5. Secure Remote Access

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

November 1, 2020

Securing Remote Access Virtual Private Networks

Disscussion

Private vs. Non-Private Networks

Offices in several cities:

- Internet – problems with confidentiality, integrity, authentication
- MPLS – how to connect home/mobile users?

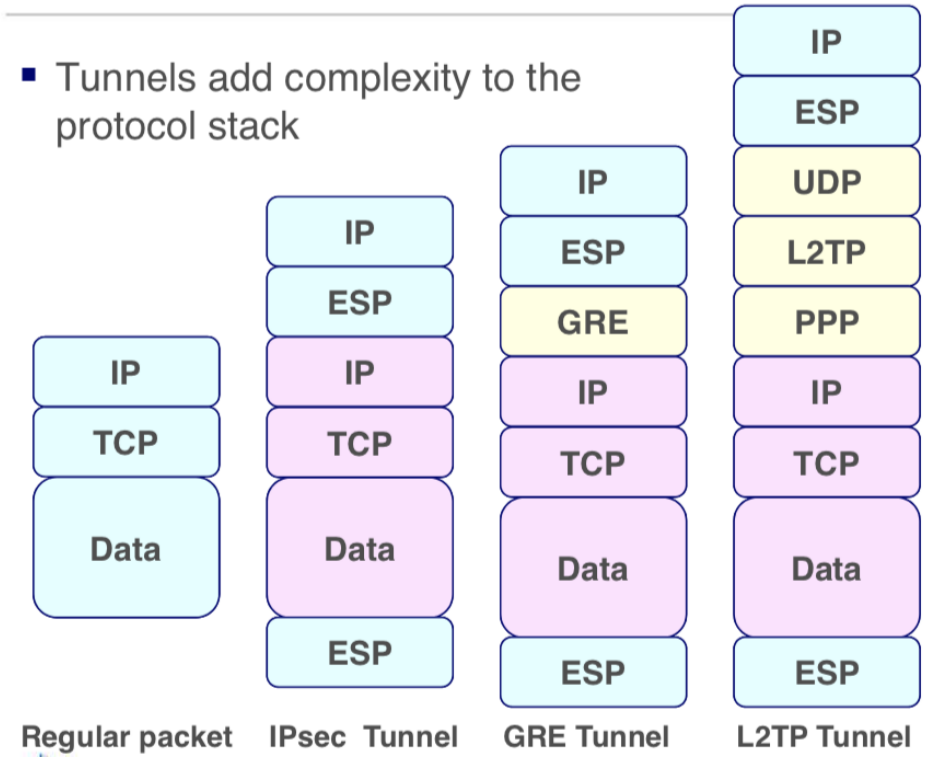
Virtual Private Networks #1

1. Even with the ability to sniff my packets on the Internet, you can't tell what I'm sending.
2. They can't modify my packets without me knowing it.
3. They can't send me traffic and have me think it came from one of my sites.
4. They can drop some of my packets, but they can't drop a class of packets (Because of #1)

Virtual Private Networks #2

Basic Idea:

- **Tunnelling & Encryption**
- GRE/L2TP
- IPsec/IKE
- SSL



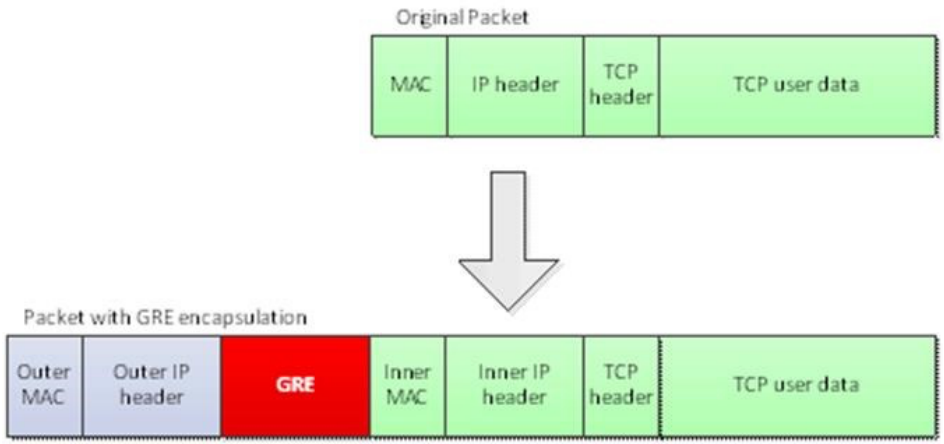
GRE/L2TP

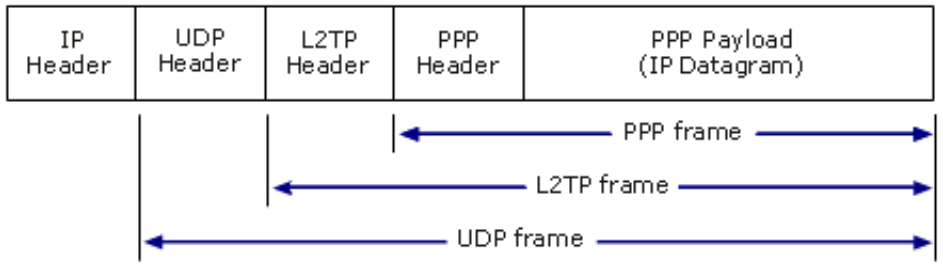
GRE – Generic Routing and Encapsulation adds a simple header to traffic, and has its own protocol number (47)

- Used mainly by Cisco for site-2-site VPNs.

L2TP – Layer-2 Transport Protocol establishes a point-2-point protocol (PPP) link over UDP port 1701.

- Used mainly for remote access in Windows, Mac, iOS, Android





IPSec #1

- To establish a secure IPSEC connection two nodes must execute a key agreement protocol.
  - The sub-protocol of IPSEC that handles key negotiations is called IKE (Internet Key Exchange).
- First, assume two nodes have agreed on keys (via IKE) and see how they proceed to protect their communication via IPSEC
- An IPsec protected connection is called a security association.
  - IPsec is a level-3 protocol (runs on top of IP), and below TCP/UDP
  - Security associations may either be end-to-end or link-to-link.
- Two modes of encapsulating IPsec data into an IP packet define two modes of operation:
  - Transport mode and tunnel mode

IPSec #2

Authentication Header (AH)

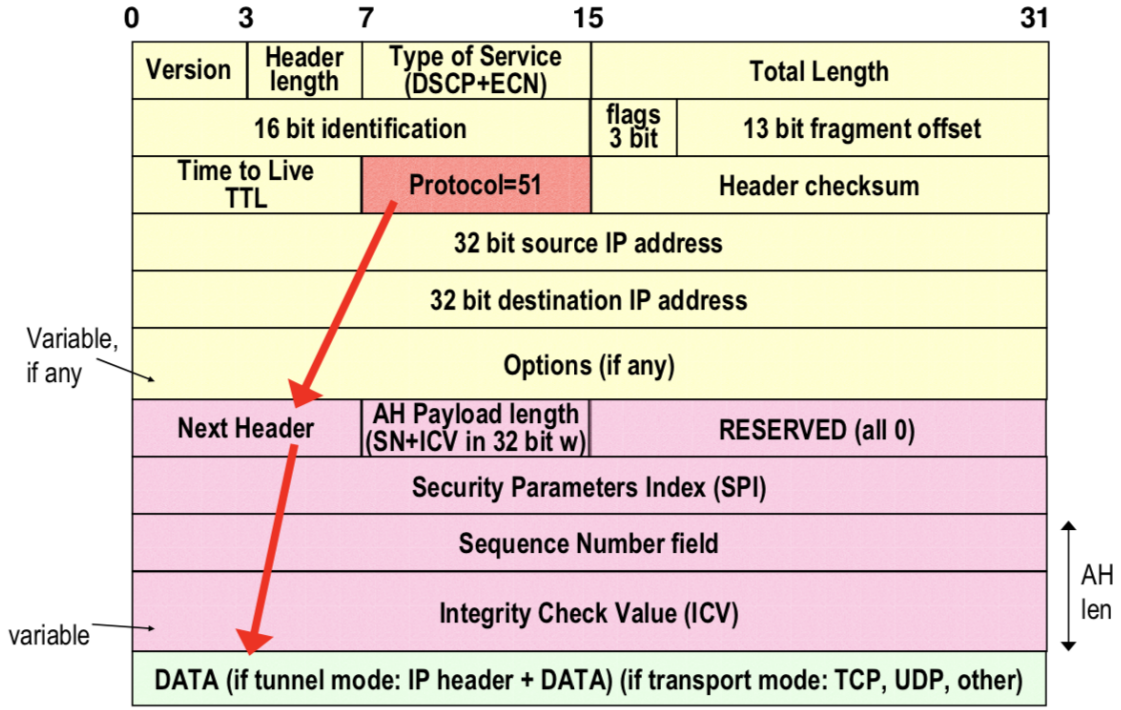
- Provides packet authentication using a keyed MAC function
- Ensures that the packet actually came from the peer with which you exchanged keys, was not modified, and was not replayed.

Encapsulated Security Protocol (ESP)

- Provides packet authentication and encryption.
- Uses a keyed MAC and an encryption function.
- Ensures your traffic cannot be read en route.

Authentication Header

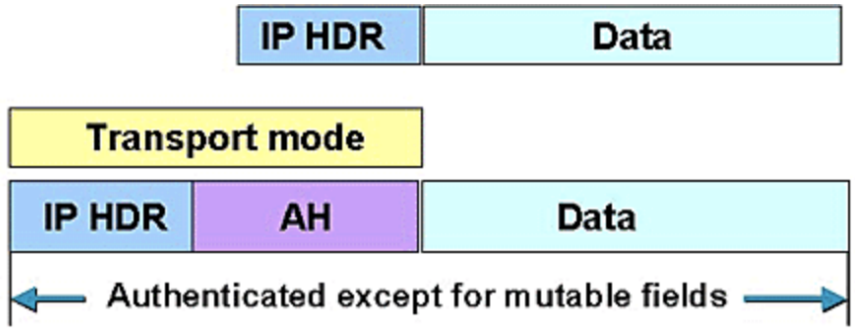
Sequence number
(no seq. no. in IP header)
prevents replays of
authenticated packets



Transport Mode — Layers 4–7

Transport mode:

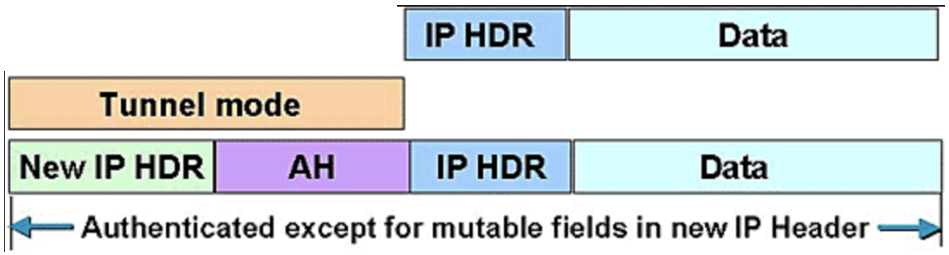
- was designed to save bandwidth in end-to-end associations
- payload is typically encrypted and authenticated
- IP header is unencrypted, and may or may not be authenticated



Tunnel Mode — Layers 3–7

Tunnel mode:

- protects both the payload and IP header of the original packet
- if encryption is used between gateways in tunnel mode, then it reduces information for traffic analysis



SSL VPNs

- In its simplest form, an SSL VPN is a portal that gives the user access to company resources though a web interface:
  - Email
  - Intranet
  - Fileshares, anything
- Advantages over IPsec tunnels
  - Clientless – all you need is a browser
  - Web-based authentication
  - It's HTTPS and most firewalls allow HTTPS

SSL VPN access

- **Clientless** — Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to access in a web browser, such as Internet access, databases, and online tools that employ a web interface.
- **Thin client (port-forwarding Java applet)** — Thin-client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and SSH.
- **Tunnel mode** — Full-tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN Client (next-generation SSL VPN Client) for SSL VPN. Full tunnel client mode delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application.

L7 VPN

OpenVPN

- Based on OpenSSL
- Uses UDP or TCP
- TUN (encapsulates from L3) or TAP (encapsulates from L2)
- various types of authentication (no, shared key, certificates)
- Topology /30 connections, P2P, subnet

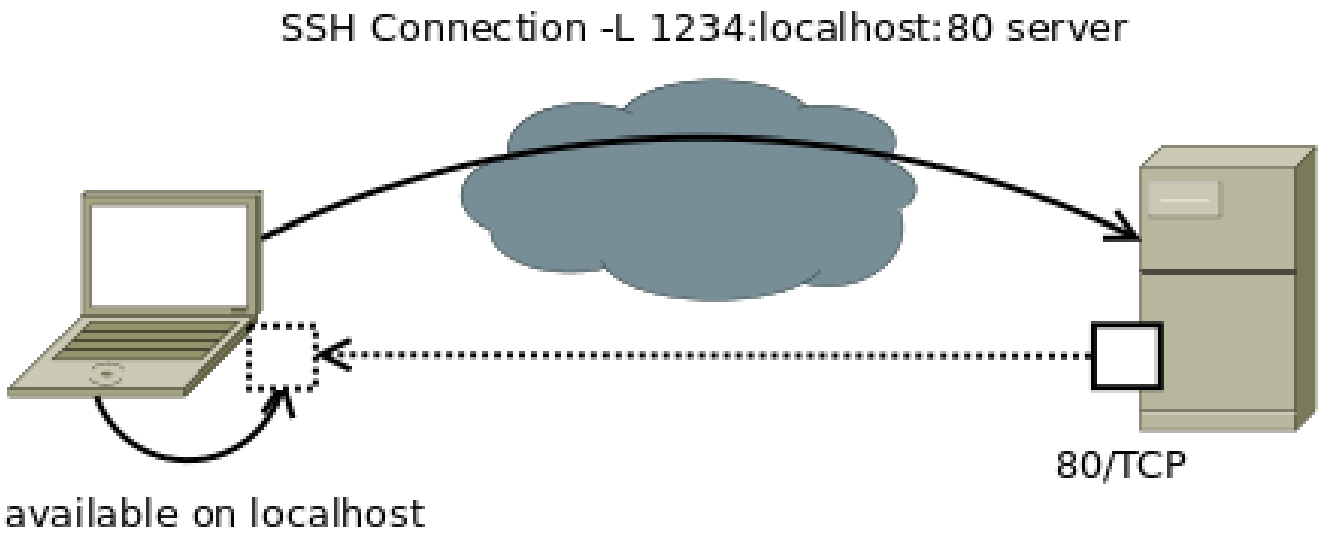
Tunneling

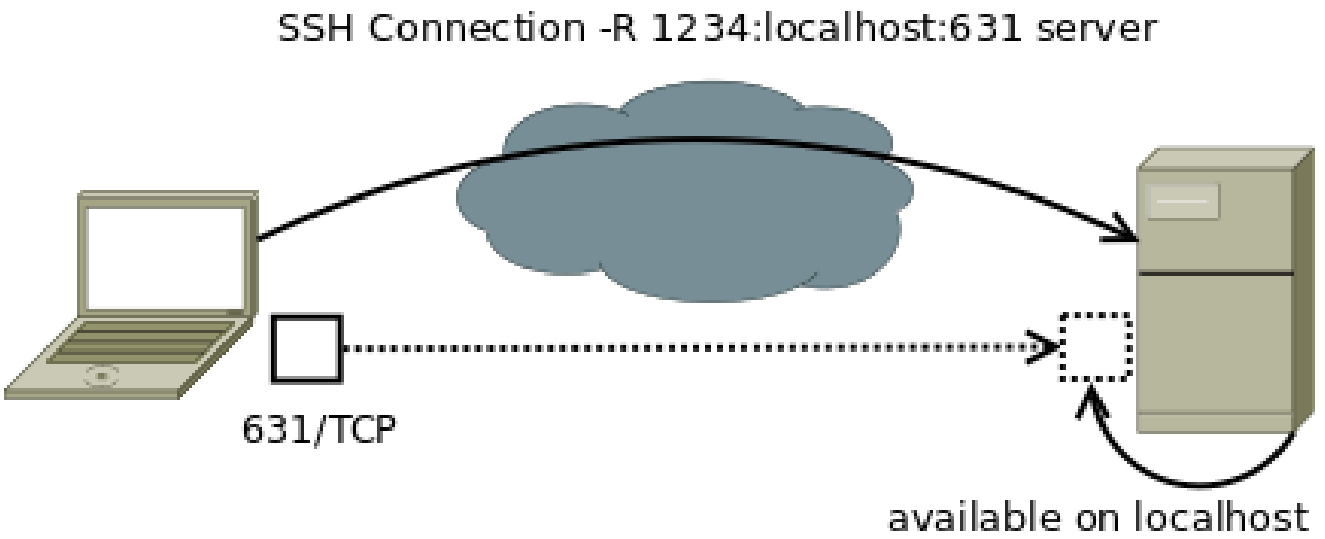
- stunnel (`https://en.wikipedia.org/wiki/Stunnel`)
- SOCKS (`https://en.wikipedia.org/wiki/SOCKS`)
- socat (`http://www.dest-unreach.org/socat/`)

```
socat - openssl-listen:12346,method=TLS1.2,key=server.key,
                                cert=server.crt,cafile=ca.crt,reuseaddr,fork
socat udp4-listen:4739,reuseaddr,fork openssl:localhost:12346,
        key=client.key,cert=client.crt,cafile=ca.crt,commonname=nemea-server
```

- SSH
  - -L (open local port),
  - -R (open remote port),
  - -D (open local SOCKS proxy)

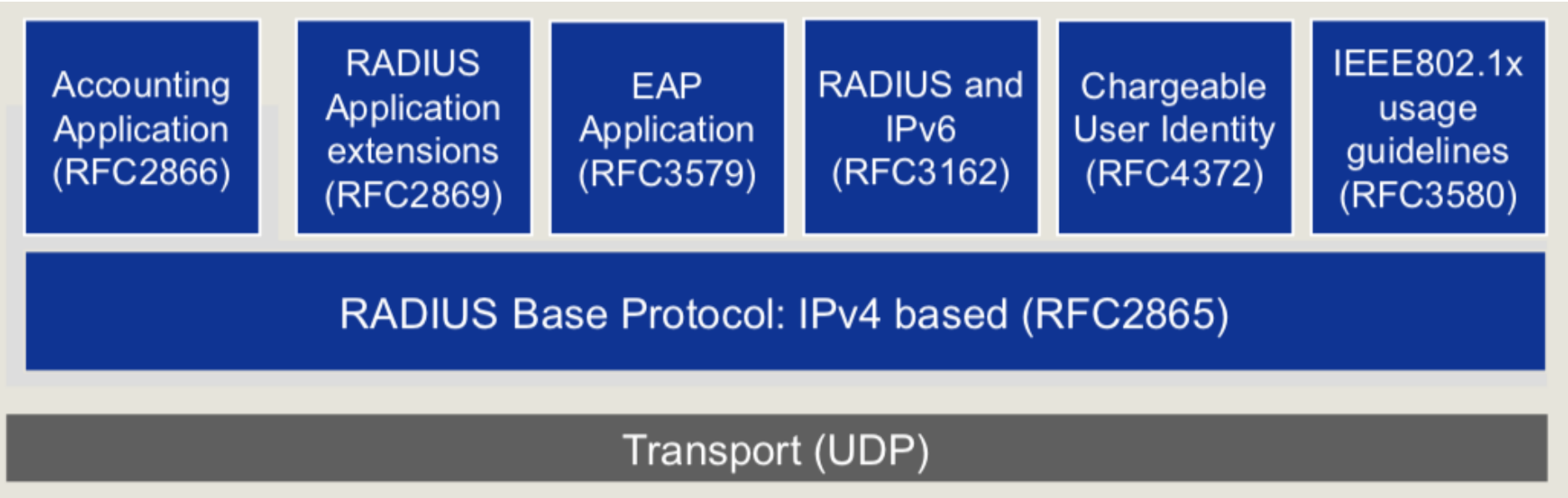
SSH Port Forwarding





RADIUS

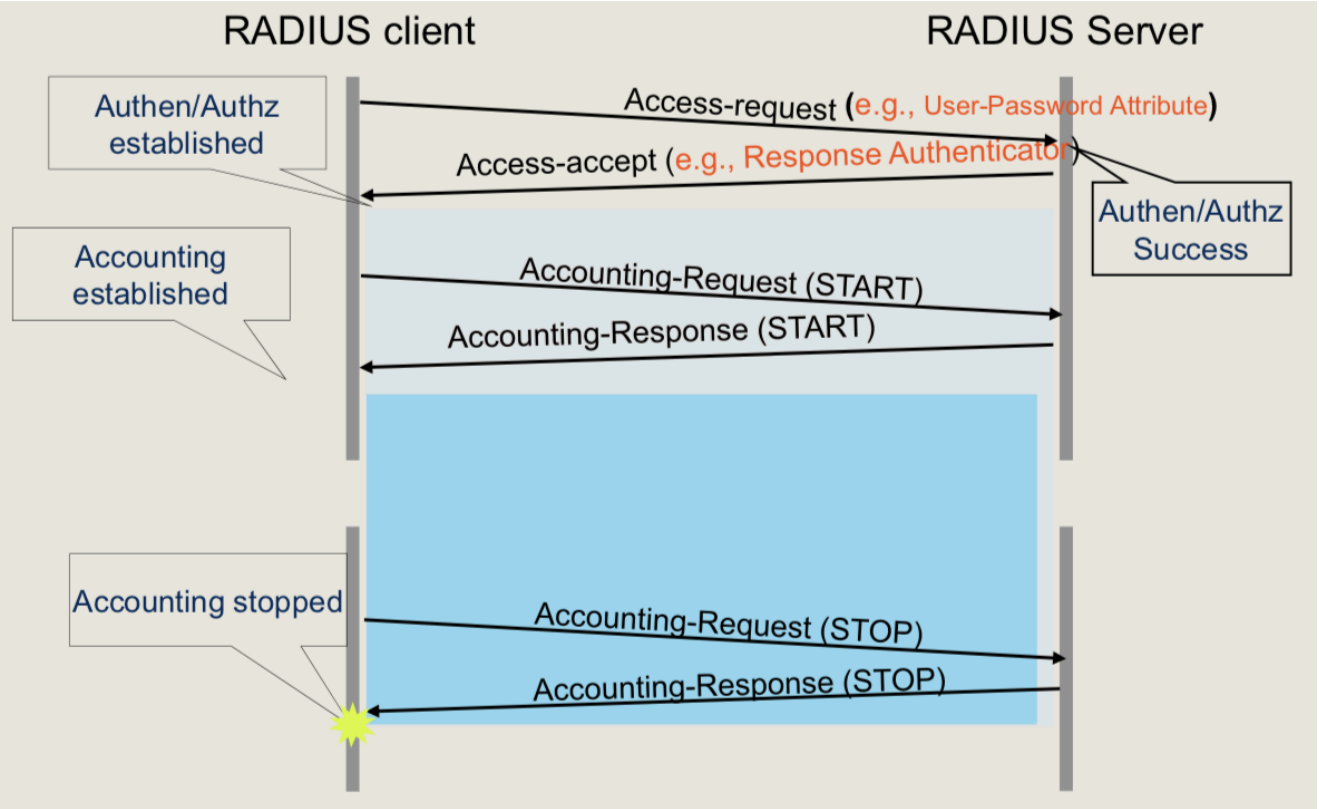
- Motivation: single user database
- Provides centralized AAA functionalities
  - Authentication
  - Authorization
  - Accounting
- Based on UDP/IP – server port 1812, client port ephemeral



RADIUS - Basic Operations

Message types:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved



Architecture

- RADIUS server
- Users DB
  - Authentication information + authentication method
- Clients DB
  - Clients allowed to communicate with the server
- Accounting DB
- Per-packet authenticated reply (using shared key)
- Encrypted user password transmission (same shared key), other info transmitted in plaintext

RADIUS and UDP

Advantages

- If request to primary authentication server fails, secondary server must be queried:
  - copy of request must be kept above transport layer
  - retransmission timers still required, above transport layer
- Stateless nature of RADIUS protocol within communication network simplifies use of UDP:
  - transport connection between client/server remains even if network failures are occurring

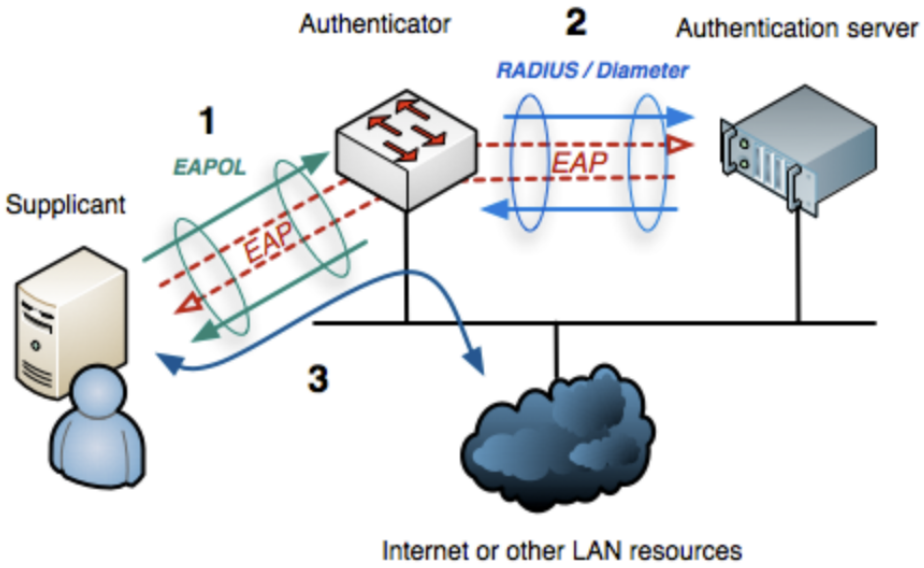
Disadvantages

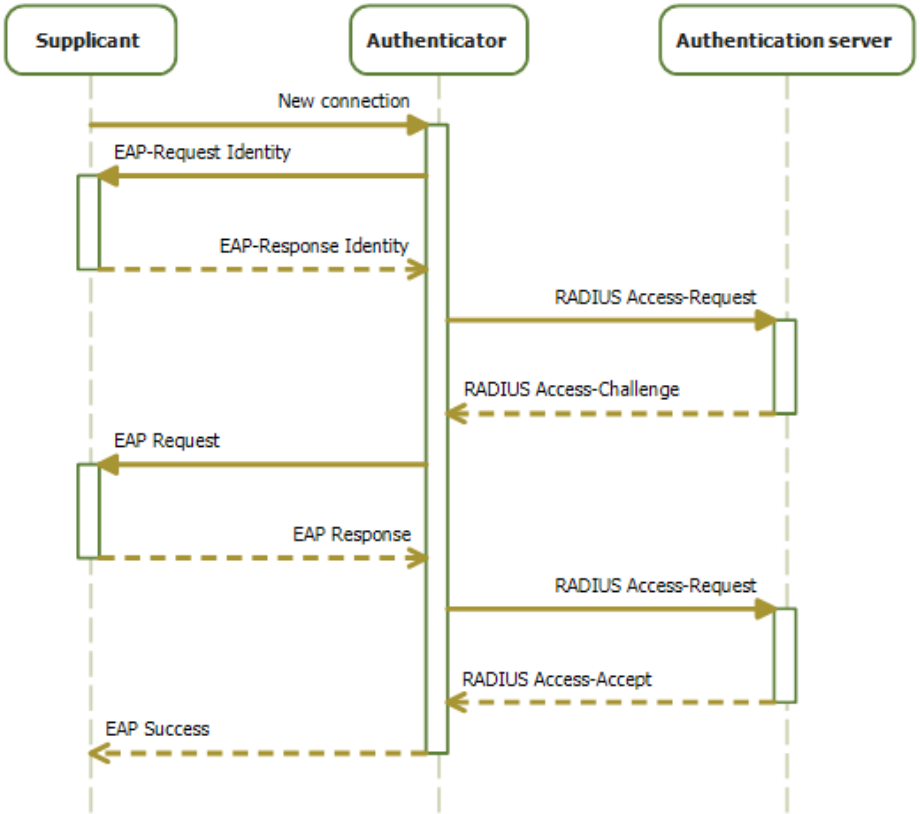
- Transport is not reliable (layer above transport has to take care of packet losses)
- TCP adapt to network congestion, while UDP does not

RADIUS Weaknesses

- Vulnerable to message sniffing and modification
- Clear-text protocol - privacy issues
- Access-Request not authenticated
  - MITM possible, access request forgery possible
- Various attacks presented
  - Shared secret attacks
  - Offline dictionary attacks
  - PRNG attacks

RADIUS - Use in 802.1x Authentication





References

- William Stallings: Data and Computer Communications
- Yoav Nir: Lecture on PKI, SSL and VPN (Information Security – Theory vs. Reality)
- Aiko Pras et. Al: Lecture on AAA protocols
- Giuseppe Bianchi: Lectures on Handling Remote Access: RADIUS; RADIUS limits and extensions
- Giuseppe Binachi: Lecture on IPSec Basics
- Phil Scott: Lecture on Virtual Private Networks
- Wikipedia: RADIUS, 802.1x

Questions?