# Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

## Summer 2015
## Chapter 06: Link Level Security
## Module 02: Wired Networks


**Prof. Dr.-Ing. Matthias Hollick**

**Technische Universität Darmstadt**
**Secure Mobile Networking Lab - SEEMOO**
**Department of Computer Science**
**Center for Advanced Security Research Darmstadt - CASED**

**Mornewegstr. 32**
**D-64293 Darmstadt, Germany**
**Tel.+49 6151 16-70922, Fax. +49 6151 16-70921**
**http://seemoo.de or http://www.seemoo.tu-darmstadt.de**

**Prof. Dr.-Ing. Matthias Hollick**
**matthias.hollick@seemoo.tu-darmstadt.de**

CASED

# Learning Objectives

Why network access authentication? Why on the link layer?

Technological perspective on wired network link layer security

- Technologies include
  - IEEE 802.1X
  - Point-to-Point Protocol (PPP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)

Module is structured accordingly

Chapter 06, Module 02

SECURE MOBILE NETWORKING

# Towards Network Access Authentication

# What is Network Access Authentication?

A mechanism by which access to the network is restricted to authorized entities

- Identities used are typically userIDs

Once authenticated, the session needs to be authorized

- Authorization can include things like VLANID, rate limits, filters, tunneling, etc.

What could be problems?

# What could be Problems?

Each user on a multi-user machine does not need to authenticate once the link is up, so this doesn't guarantee that only the authenticated user is accessing the network

Hijacking by external attacker

- To prevent hijacking, you need per-packet authentication as well
- Encryption orthogonal to authentication
- Per-packed MIC based on key derived during the authentication process, linking each packet to the identity claimed in the authentication

- Some existing protocols do not support MIC (e.g. PPP and WEP!)

# Network Access Alternatives

Network access authentication has already been implemented at various layers

PHY/MAC

- Example: 802.11b
- Pros: no MAC or TCP/IP changes required (all support in firmware)
- Cons: requires firmware changes in NICs and NASes to support new auth methods, requires NAS to understand new auth types, slows delivery of bug fixes (e.g. WEP v1.0), hard to integrate into AAA

MAC

- Examples: PPP , 802.1X
- Pros: no firmware changes required for new auth methods, easier to fix bugs, easy to integrate into AAA, no network access needed prior to authentication, extensible (RFC 2284)
- Cons: requires MAC layer changes unless implemented in driver

# Network Access Alternatives (cont'd)

IP + App-Level Gateway

- Examples: hotel access (based on ICMP re-direct to access web server)
- Pros: no client MAC or TCP/IP changes required (for ICMP re-direct method)
- Cons: Doesn't work for all apps, no mutual authentication, partial network access required prior to auth, need to find access control server if not at first hop, typically not extensible, may not derive encryption keys, no accounting (no logoff)

UDP/TCP/Application

- Examples: Proprietary token card protocols
- Pros: No client MAC or TCP/IP changes required – can be implemented purely at the application layer
- Cons: requires client software, partial network access required prior to auth, need to find access control server if not at first hop, typically not extensible, no accounting (no logoff)

# Why Do Auth at the Link Layer?

It's fast, simple, and inexpensive

- Most popular link layers support it: PPP, IEEE 802
- Cost matters if you're planning on deploying 1 million ports!

Client doesn't need network (services) access to authenticate

- No need to resolve names, obtain an IP address prior to auth

In a multi-protocol world, doing auth at link layer enables authorizing all protocols at the same time

- Doing it at the network layer would mean adding authentication within IPv4, IPv6, AppleTalk, IPX, SNA, NetBEUI
- Would also mean authorizing within multiple layers
- Result: more delay

# IEEE 802.1X

# What is IEEE 802.1X?

The IEEE standard for authenticated and auto-provisioned LANs.

- Ratified June 2001, Based on EAP, IETF RFC 2284

A framework for authentication and key management

- IEEE 802.1X derives keys which can be used to provide per-packet authentication, integrity and confidentiality
- Typically used along with well-known key derivation algorithms (e.g. TLS, SRP, etc.)
- IEEE 802.1X does not mandate security services – can do authentication, or authentication & encryption
- Encryption alone not recommended (but that's what WEP does)
  - For IPSec has been thoroughly discussed
  - See http://www.cs.columbia.edu/~smb/papers/badesp.ps
  - See http://eprint.iacr.org/2007/125.pdf

# What IEEE 802.1X is not

Purely a wireless standard – it applies to all IEEE 802 technologies (e.g. Ethernet First Mile applications)

PPP over Ethernet (PPPOE) – only supports EAP authentication methods (no PAP or CHAP), packets are not encapsulated

A cipher – not a substitute for WEP, RC4, DES, 3DES, AES, etc.

- But 802.1X can be used to derive keys for any cipher

A single authentication method

- But 802.1X can support many authentication methods without changes to the AP or NIC firmware

# A History of IEEE 802.1X

SECURE MOBILE NETWORKING

The idea started with customers who wanted to control access to a public network

- Universities, government agencies

Existing approaches were inadequate

- Customers wanted something that could be implemented inexpensively – on existing switches
- Customers wanted to utilize existing network access infrastructure (RADIUS, LDAP, etc.)
- PPPOE – too much overhead
- VPN – too many interoperability issues
- DHCP – designed for addressing and configuration, not access control

Concept developed by 3Com, HP, and Microsoft

- A small group wrote the spec and built prototypes
- Consensus and running code! Not designed by committee!

# 802.1X Security Philosophy

SECURE MOBILE NETWORKING

Approach: a flexible security framework

- Implement security framework in upper layers
- Enable plug-in of new authentication, key management methods without changing NIC or Access Point
- Leverage main CPU resources for cryptographic calculations

How it works

- Security conversation carried out between supplicant and authentication server
- NIC, Access Point acts as a pass through device

Advantages

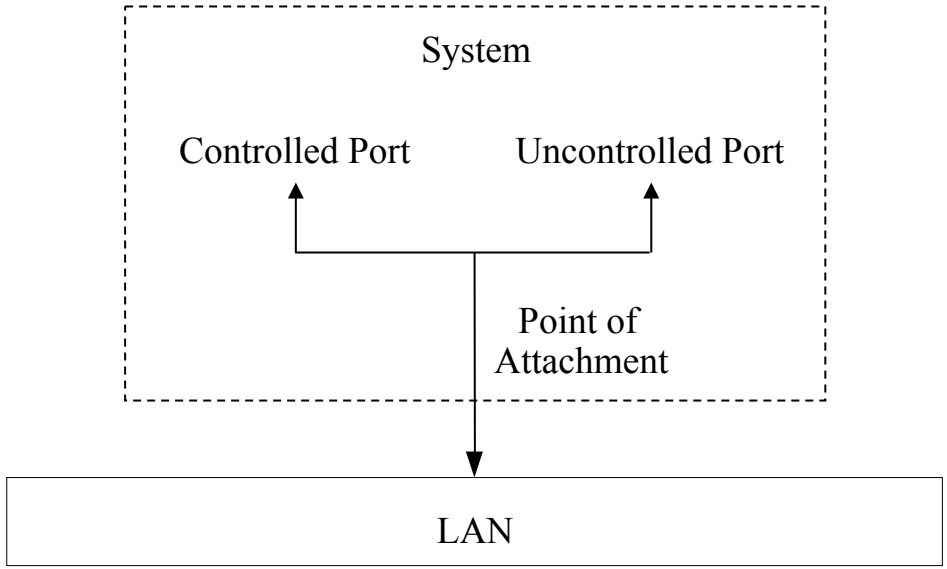
- Decreases hardware cost and complexity
- Enables customers to choose their own security solution
- Can implement the latest, most sophisticated authentication and key management techniques with modest hardware
- Enables rapid response to security issues

# IEEE 802.1X working

# IEEE 802.1X: Controlled and Uncontrolled Ports

IEEE 802.1X introduces the notion of two logical ports:

- the uncontrolled port allows to authenticate a device
- the controlled port allows an authenticated device to access LAN services



# IEEE 802.1X: Roles

Three principal roles are distinguished:

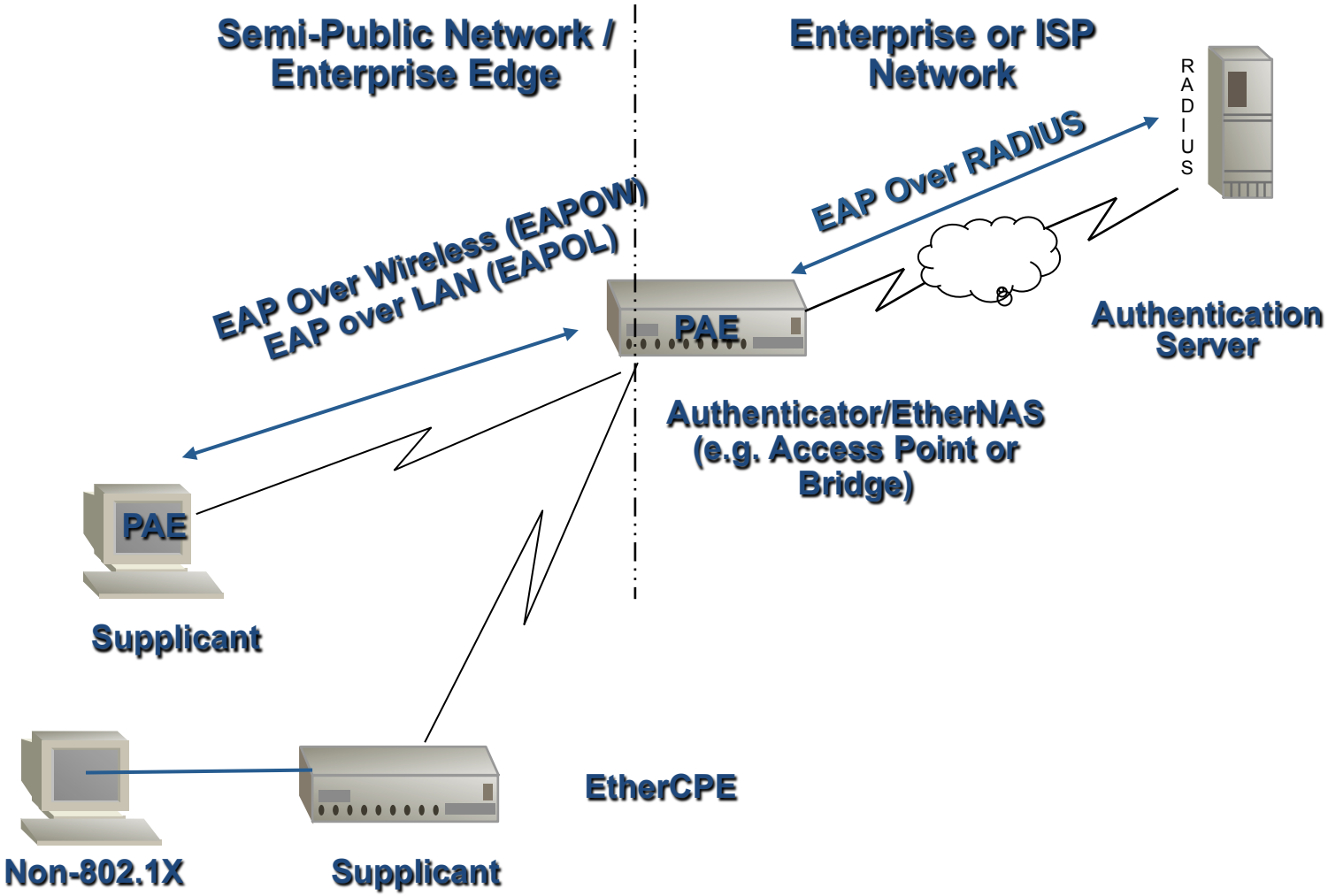
- A device that wants to use the service offered by an IEEE 802.1X LAN acts as a supplicant requesting access to the controlled port
- The point of attachment to the LAN infrastructure (e.g. a MAC bridge) acts as the authenticator demanding the supplicant to authenticate itself
- The authenticator does not check the credentials presented by the supplicant itself, but passes them to his authentication server for verification

# IEEE 802.1X: Roles

Accessing a LAN with IEEE 802.1X security measures:

- Prior to successful authentication the supplicant can access the uncontrolled port:
  - The port is uncontrolled in the sense, that it allows access prior to authentication
  - However, this port allows only restricted access
- Authentication can be initiated by the supplicant or the authenticator
- After successful authentication the controlled port is opened

# 802.1X Topologies



# IEEE 802.1X Security Protocols and Message Exchange

IEEE 802.1X does not define its own security protocols, but advocates the use of existing protocols:

- The Extensible Authentication Protocol (EAP) may realize basic device authentication [RFC 2284]
- If negotiation of a session key during authentication is required, the use of the PPP EAP TLS Authentication Protocol is recommended [RFC 2716]
- Furthermore, the authentication server is recommended to be realized with the Remote Authentication Dial In User Service (RADIUS) [RFC 2865]

Exchange of EAP messages between supplicant and authenticator is realized with the EAP over LANs (EAPOL) protocol:

- EAPOL defines the encapsulation techniques that shall be used in order to carry EAP packets between supplicant port access entities (PAE) and Authenticator PAEs in a LAN environment
- EAPOL frame formats have been defined for various members of the 802.x protocol family, e.g. EAPOL for Ethernet, ...
- Between supplicant and authenticator RADIUS (or Diameter) messages may be used

# What is EAP?

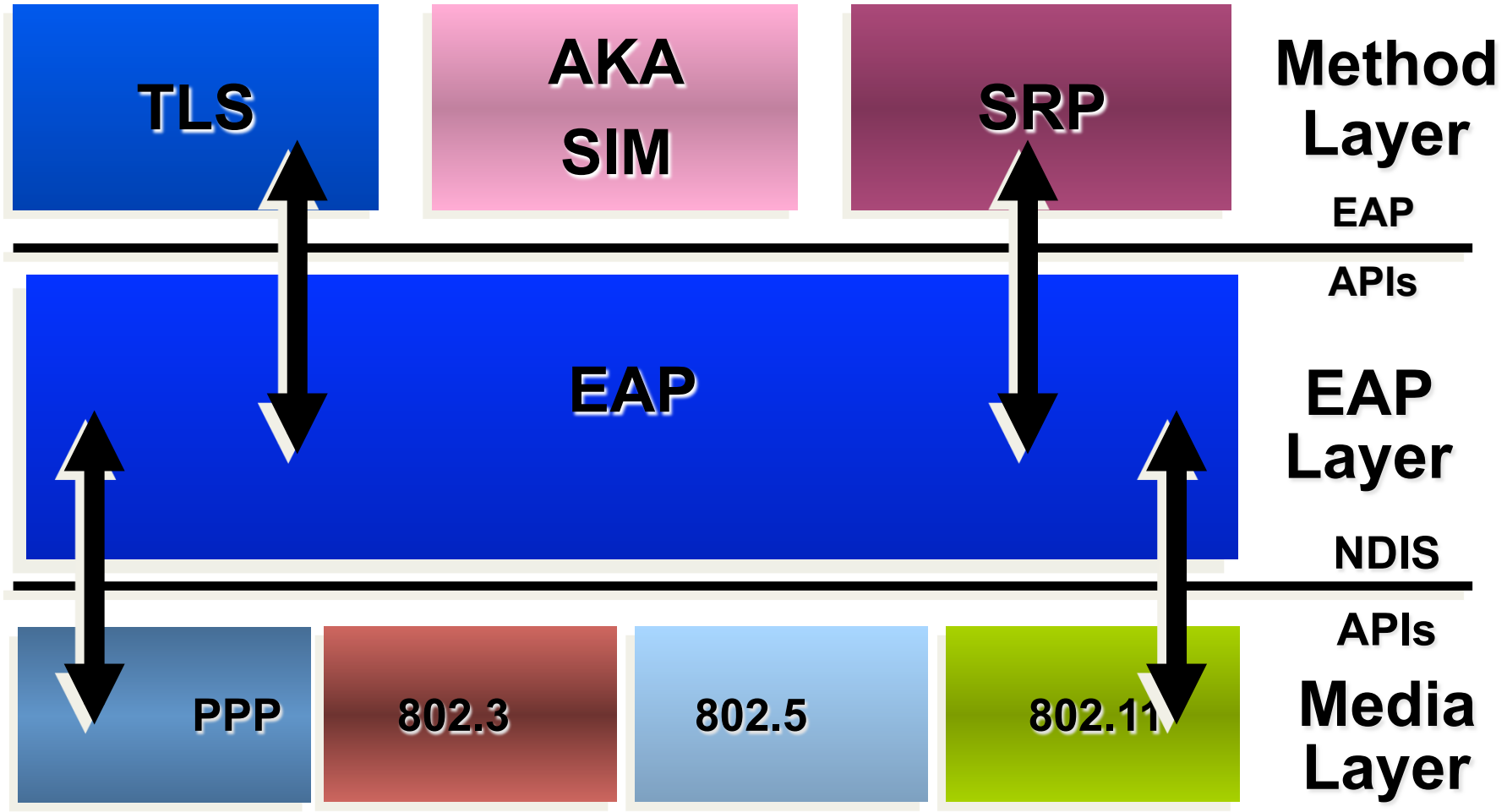
The Extensible Authentication Protocol (RFC 2284)

- Provides a flexible link layer security framework
- Simple encapsulation protocol
  - No dependency on IP
  - ACK/NAK, no windowing, no fragmentation support
- Few link layer assumptions
  - Can run over any link layer (PPP, 802, etc.)
  - Does not assume physically secure link
    - Methods provide security services
  - Assumes no re-ordering
  - Can run over lossy or lossless media
    - Retransmission responsibility of authenticator

EAP methods based on IETF standards

- Transport Level Security (TLS) , Secure Remote Password (SRP)
- GSS_API (including Kerberos)

# EAP Architecture



# What is RADIUS?

Remote Access Dial In User Service

Supports authentication, authorization, and accounting for network access

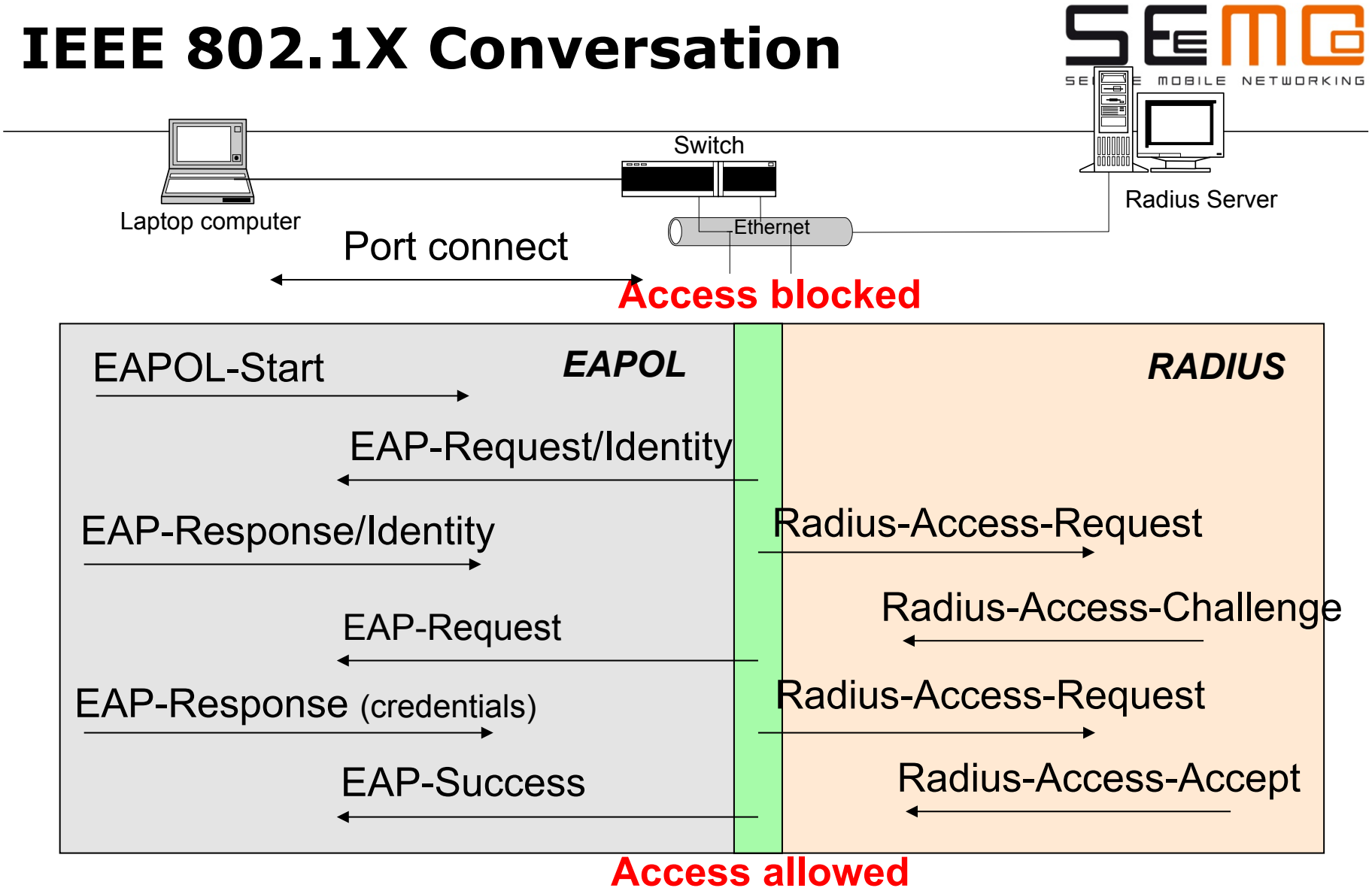
- Physical ports (analog, ISDN, IEEE 802)
- Virtual ports (tunnels, wireless)

Allows centralized administration and accounting

IETF status

- Proposed standard
  - RFC 2865, RADIUS authentication/authorization
  - RFC 2618-2621, RADIUS MIBs
- Informational
  - RFC 2866, RADIUS accounting
  - RFC 2867-8, RADIUS Tunneling support
  - RFC 2869, RADIUS extensions,  RFC 3162, RADIUS for IPv6

# IEEE 802.1X Conversation



# Point-to-Point Protocols

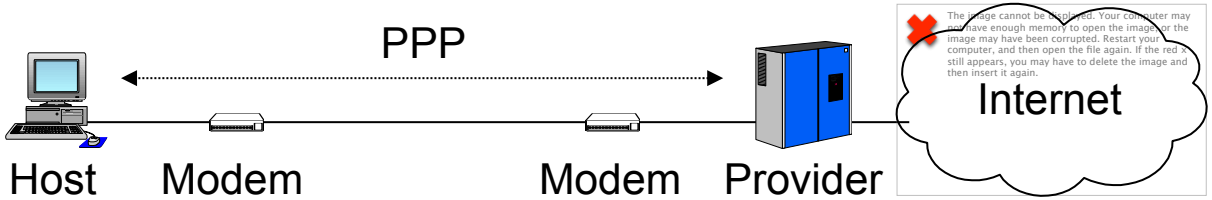
# Point-to-Point Protocol: Purpose and Tasks

Parts of the Internet rely on point-to-point connections:

- Wide area network (WAN) connections between routers
- Historical: dial-up connections of hosts

Protocols for this purpose:

- Point-to-Point Protocol (PPP): successor to SLIP, supports IP, IPX, ...




PPP [RFC 1661/1662]:

- Layer-2 frame format with frame delimitation and error detection
- Control protocol (Link Control Protocol, LCP) for connection establishment, -test, -negotiation, and -release
- Separate Network Control Protocols (NCP) for supported Layer-3 protocols

# Point-to-Point Protocol: A Typical PPP Connection

Usage Scenario “Internet access of a PC via modem”:

- User calls *Internet service provider (ISP)* via modem and establishes a “physical” connection via the plain old telephone service (POTS)
- Caller sends multiple LCP-packets in PPP-frames to chose desired PPP-parameters
- Security specific negotiation (see below)
- Exchange of NCP-packets to configure network layer:
  - e.g. configuration of IP including dynamic allocation of an IP address via Dynamic Host Configuration Protocol (DHCP)
- Caller may use arbitrary Internet services like any other host with a fixed connection to the Internet
- For connection termination the allocated IP address and the network layer connection are released
- The layer-2 connection is released via LCP and the modem closes down the “physical” connection

# Point-to-Point Protocol: Security Services

The original version of PPP [RFC 1661] suggests the optional run of an authentication protocol after the link establishment phase:

- If required, authentication is demanded by one peer entity via an LCP Configuration-Request at the end of the link establishment phase
- Originally, two authentication protocols have been defined:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- Meanwhile, an extensible protocol has been defined:
  - Extensible Authentication Protocol (EAP)
  - PPP EAP Transport Level Security Protocol (PPP-EAP-TLS)

Furthermore, encryption can be negotiated after authentication:

- Protocols:
  - Encryption Control Protocol (ECP) for negotiation
  - PPP DES Encryption Protocol (DESE)
  - PPP Triple DES Encryption Protocol (3DESE)

# Point-to-Point Protocol: Authentication Protocols

SECURE MOBILE NETWORKING

Password Authentication Protocol (PAP):

- The protocol is very simple (no crypto) (RFC 1334):
  - Authenticator, demands the peer entity to authenticate with PAP
  - Peer entity sends peer ID and password
  - Authenticator checks correctness (authenticate-ack/-nack)

Challenge Handshake Authentication Protocol (CHAP):

- Simple challenge-response protocol (RFC 1334, RFC 1994):
  - Prerequisite: authenticator and peer entity share a secret
  - Authenticator (A) sends challenge with *identifier*, a random number $r_A$, and its name to the peer entity (B): $A \rightarrow B: (1, identifier, r_A, A)$
  - Peer entity computes cryptographic hash function over its name, the shared secret $K_{A,B}$ and the challenge random number $r_A$ and sends the following message: $B \rightarrow A: (2, identifier, H(B, K_{A,B}, r_A), B)$
  - Authenticator re-computes the hash value, answers with a *success* message (RFC 1994 specifies, that MD5 must be supported)

# Point-to-Point Protocol: Authentication Protocols (2)

Extensible Authentication Protocol (EAP):

- EAP is an general protocol for PPP authentication which supports multiple authentication methods [RFC2284 -> RFC 3748 & updated by RFC 5247]
- The main idea behind EAP is to provide a common protocol to run more elaborate authentication methods than “1 question + 1 answer”
- The protocol provides basic primitives:
  - Request, Response: further refined by type field + type specific data
  - Success, Failure: to indicate the result of an authentication exchange
- Variety of methods are supported
  - LEAP, EAP-TLS, EAP-MD5, EAP-PSK, EAP-TTLS, EAP-IKEv2, EAP-FAST, EAP-SIM, EAP-AKA, EAP-GTC, EAP-OTP, etc.
  - EAP-MD5 - MD5 Challenge (this corresponds to CHAP)
  - EAP-OTP - One-Time Password (OTP): defined in [RFC2289]
  - EAP-GTC - Generic Token Card
  - Etc.

# Point-to-Point Protocol: Authentication Protocols (3)

Generic Token Card:

- Basically, a challenge response dialogue
- A token card is used to compute a response to a challenge:
  - The challenge is presented to the user who has to type it to his token card device
  - The token card computes and displays the response
  - The user enters the response into the system that sends it as an answer to the challenge message

PPP-EAP-TLS:

- TLS stands for Transport Layer Security [RFC 2246]
- Thus, the authentication dialogue of TLS is run

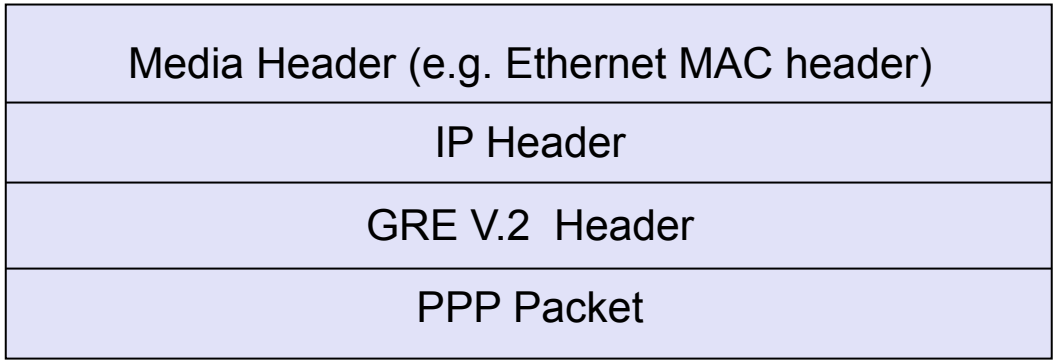
After link establishment and authentication: encryption can be negotiated using Encryption Control Protocol (ECP) [RFC1968]

# Point to Point Tunneling Protocol (PPTP)

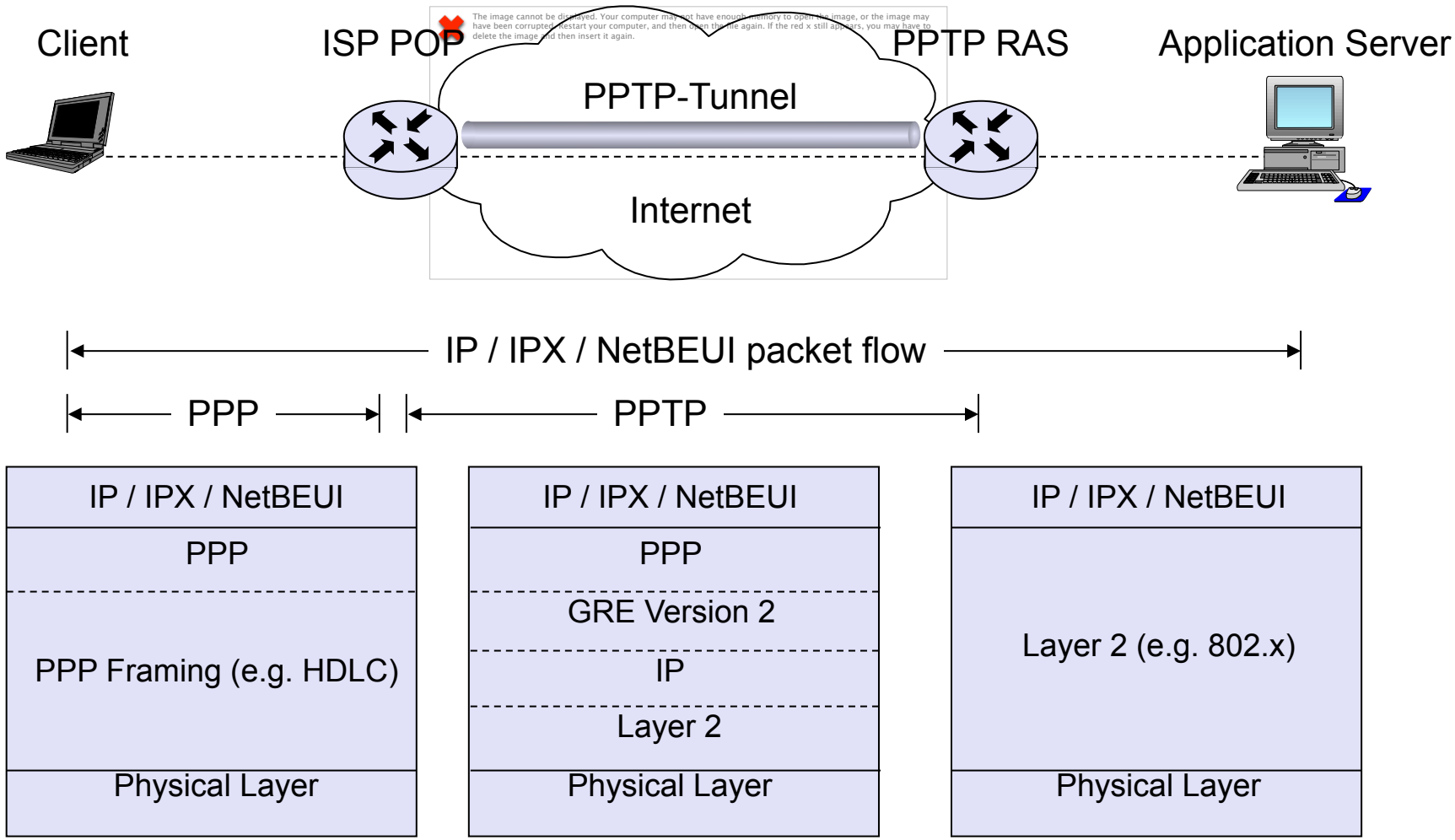
PPP designed to be run between “directly” connected entities, that is entities which share a layer-2 connection

The basic idea of PPTP is to extend the protocol’s reach over the entire Internet by defining transport of PPP PDUs in IP packets

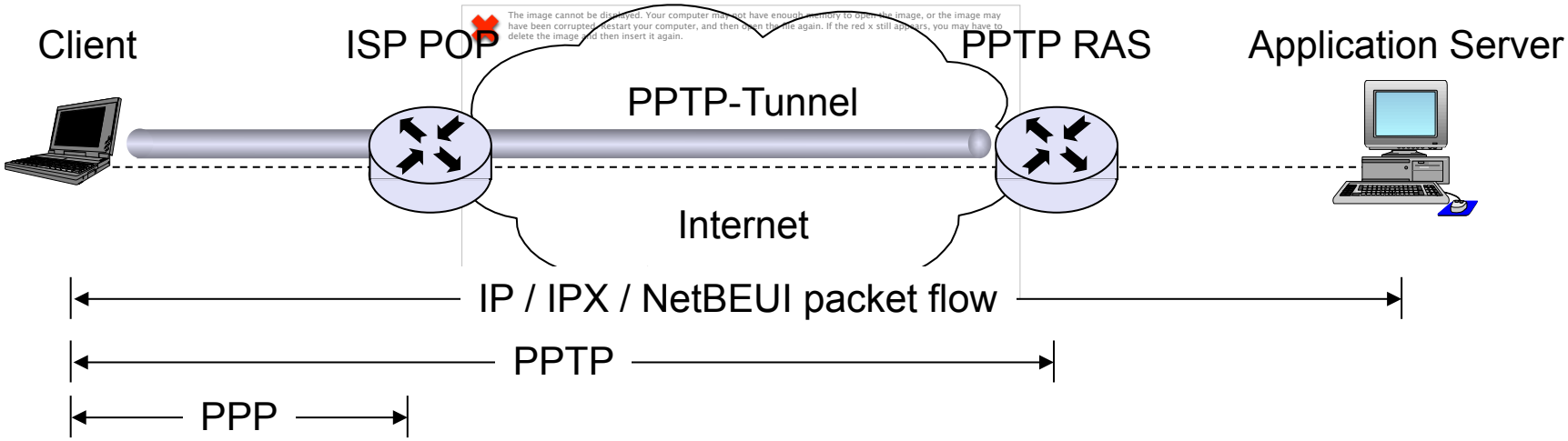
- Payload of PPTP PDUs are PPP packets (without layer-2 specific fields like HDLC flags, bit insertion, control characters, CRC error check values, etc.)
- PPP packets are encapsulated in GRE packets (generic routing encapsulation) that themselves are encapsulated in IP packets:



# PPTP: Compulsory Tunneling Protocol Layers



# PPTP: Voluntary Tunneling Protocol Layers

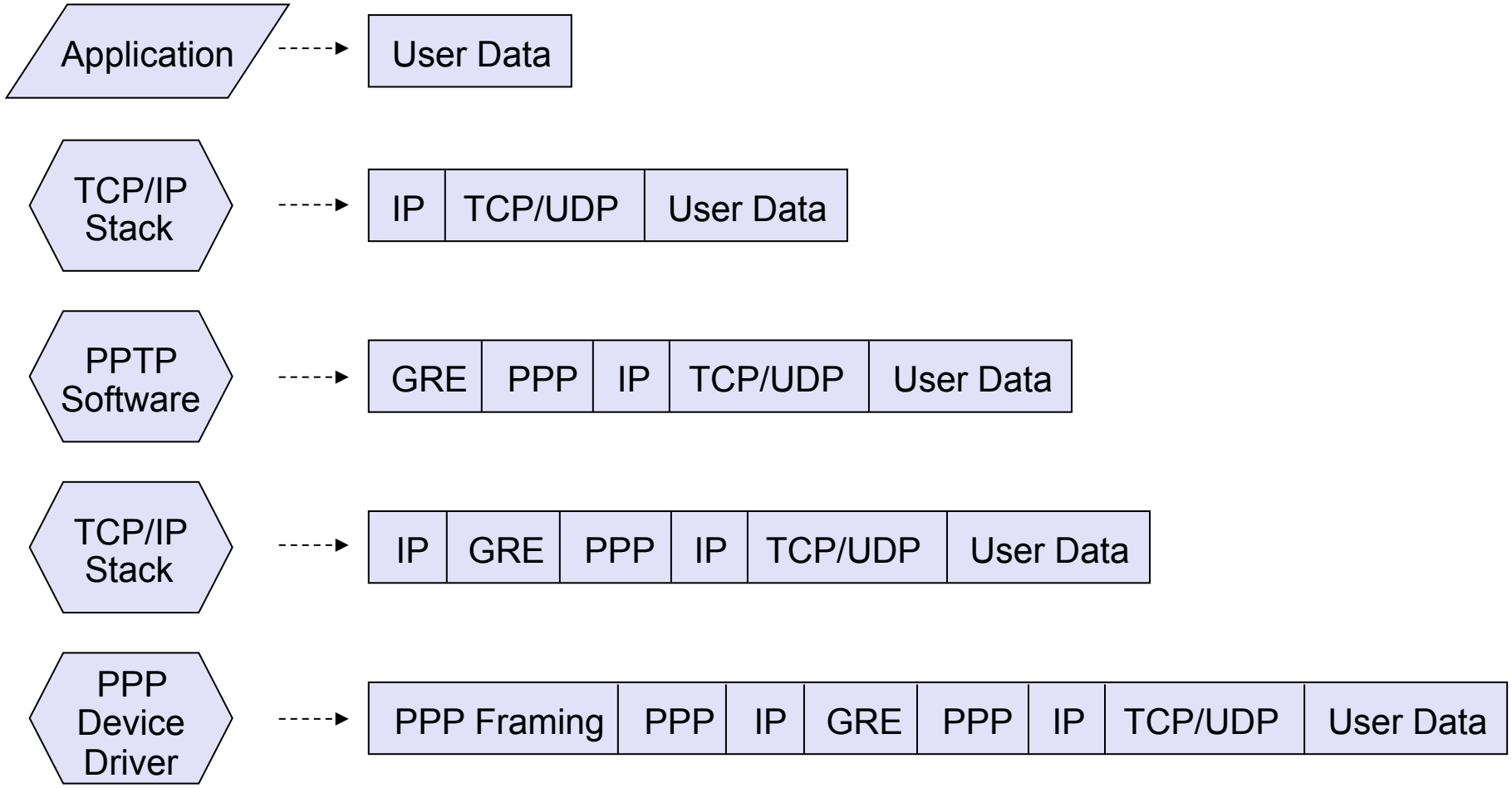



| IP / IPX / NetBEUI |
|---|
| PPP |
| GRE Version 2 |
| IP |
| PPP |
| PPP Framing (HDLC) |
| Physical Layer |

| IP / IPX / NetBEUI |
|---|
| PPP |
| GRE Version 2 |
| IP |
| Layer 2 |
| Physical Layer |

| IP / IPX / NetBEUI |
|---|
| Layer 2 (e.g. 802.*) |
| Physical Layer |

# PPTP: Voluntary Tunneling Packet Construction at Client



# PPTP / PPP Proprietary Extensions & Some "History"

PPTP has been largely deployed as a consequence of Microsoft's support for it:

- Developed with Microsoft's active involvement, [RFC2637]
- Microsoft implemented it as a part of its Remote Access Service (RAS)

Microsoft further specified "proprietary" extensions for PPP:

- Microsoft PPP CHAP Extensions [RFC2433]
- Microsoft Point to Point Encryption Protocol [RFC3078]

However, a series of vulnerabilities have been discovered in PPTP version 1 and also in an improved version 2 [SM98a, SMW99a]:

- A general consensus to adopt PPTP as a standard protocol could not be reached in the IETF working groups
- Furthermore, a similar protocol (Layer 2 Forwarding, L2F) had been proposed by Cisco as a competing approach
- As a consequence, a compromise was found to merge the advantages of both proposals into one single protocol Layer 2 Tunneling Protocol (L2TP)
  - L2TPv3 is published as proposed standard RFC 3931, UDP port 1701 is used, can be combined with IPSec

# Comparison of PPTP and L2TP

Both protocols:

- use PPP to provide an initial envelope for user packets
- extend the PPP model by allowing the layer-2 and the PPP endpoints to reside on different devices
- support voluntary and compulsory tunneling

Underlying network:

- PPTP requires an IP network to transport its PDUs
- L2TP supports different technologies: IP (using UDP), Frame Relay permanent virtual circuits (PVCs), X.25 virtual circuits (VCs), or ATM VCs

PPTP can only support a single tunnel between end points, L2TP allows for the use of multiple tunnels between end points

- E.g. L2TP allows to create different tunnels for different qualities of service

Both protocols provide for header compression:

- With header compression L2TP operates with 4 bytes of overhead, as compared to 6 bytes for PPTP

L2TP provides for tunnel authentication, while PPTP does not

# Additional References (1)


[IEEE04] IEEE. Standards for Local and Metropolitan Area Networks: Standard for Port Based Network Access Control. IEEE.

- A 2015 veriosn exists, but is not yet publicly available

[RFC1661] W. Simpson. The Point-to-Point Protocol (PPP). RFC 1661, 1994.

[RFC1994] W. Simpson. PPP Challenge Handshake Authentication Protocol (CHAP). RFC 1994 (obsoletes RFC 1334), 1996.

[RFC2284] L. Blunk, J. Vollbrecht. PPP Extensible Authentication Protocol (EAP).
RFC 2284, 1998.

[RFC2289] N. Haller, C. Metz, P. Nesser, M. Straw. A One-Time Password System.
RFC 2289, 1998.


Updated and newer versions of most of these protocols exist

# Additional References (2)


[RFC2341] A. Valencia, M. Littlewood, T. Kolar. Cisco Layer Two Forwarding Protocol (L2F). RFC 2341, 1998.

[RFC2637] K. Hamzeh, G. Pall , W. Verthein, J. Taarud, W. Little, G. Zorn. Point-to-Point Tunneling Protocol (PPTP). RFC 2637, 1999.

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. Layer Two Tunneling Protocol (L2TP). RFC 2661, 1999.

[RFC2828] R. Shirey. Internet Security Glossary. RFC 2828, 2000.

[SM98a] B. Schneier, Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). Proceedings of the 5th ACM Conference on Communications and Computer Security, ACM Press, pp. 132-141, 1998.

[SMW99a] B. Schneier, Mudge, D. Wagner. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MSCHAPv2). Counterpane Systems, 1999.

# Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Some other slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- B. Aboba (Microsoft Research)

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6
- [Stallings2015] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2015, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

# Copyright Notice

# Contact


**Prof. Dr.-Ing. Matthias Hollick**
**Department of Computer Science**

**SEEMOO**
**Mornewegstr. 32**
**64293 Darmstadt/Germany**
matthias.hollick@seemoo.tu-darmstadt.de

**Phone +49 6151 16-70920**
**Fax +49 6151 16-70921**
**www.seemoo.tu-darmstadt.de**