ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

# Communication Systems

## PPP

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer


# Copyright Warning

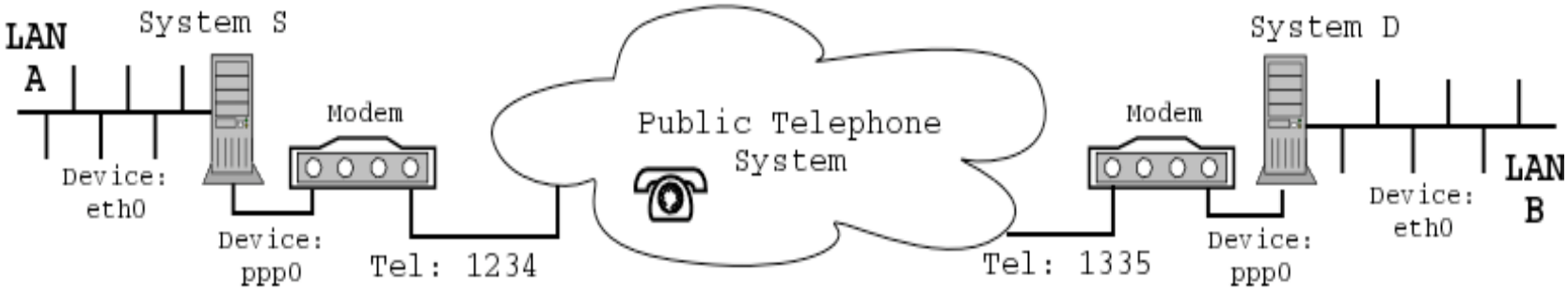
- This lecture has already been stolen
- If you copy it again please ask the author
  - Prof. Dr. Gerhard Schneider
- like I did

# Other Physical and Higher Level Protocols

- By now our host is connected to the IP world through LAN technology like Ethernet
- Not suitable for WAN access like dial-in from home
  - Longer distances than just a few 100 meters
  - Other kind of traffic (very few packets between stations directly, mostly gateway, outward traffic)
- In the beginning: Modem dial-in via telephony network
  - Remember (or look it up at home) the networks taxonomy: switched versus packet orientated networks, typically point-to-point connections
- Typically ADSL, TV Cable or ISDN used for private, small offices Internet uplink

# Other Physical and Higher Level Protocols

- Modem, ISDN, cellular or alike connections offer unstructured bitstream transport
- Local delivery with point-to-point connections is easy, just send the packet to the other end of the connection
  - Modem – addressing is done other ways:
    - Device number of serial port, telephone number of the telephone system, ...
    - Same game as for Ethernets – mapping is needed



# Point-to-Point-Protocol

- Point-to-Point Protocol (PPP) data link protocol used to establish a direct connection between two networking nodes
  - Distinguish between single packets
  - Can additionally provide connection authentication
  - Can provide compression and transmission encryption
- Predecessors were Serial Line Internet Protocol (SLIP) or Telco standards such as Link Access Protocol Balanced (LAPB) part of the deprecated X.25 protocol suite
- Basic features of PPP
  - Multiple network layer protocols
  - Automatic self configuration
  - Looped link detection via magic numbers in control protocol

# Point-to-Point-Protocol

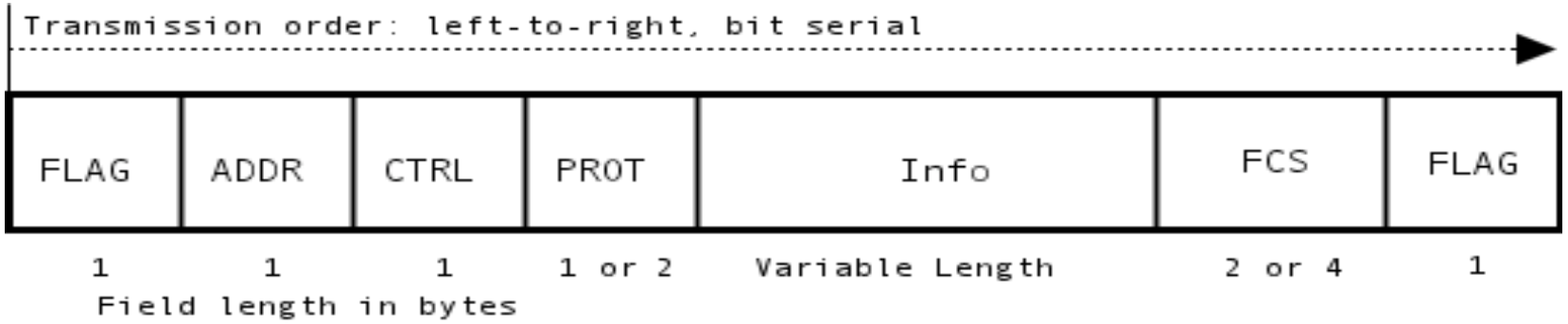
- Multiple network layer protocols
  - Can handle multiple network layer protocols (different IP, NetBIOS, IPX, ...)
  - Separate Network Control Protocol (NCP) for every higher layer protocol, e.g. IP Control Protocol (IPCP)
- Automatic self configuration
  - Link Control Protocol (LCP) for automated configuration of interfaces at each end of connection: datagram size, escaped characters, magic numbers
  - Optional: selecting authentication method like PAP (password authentication protocol – rather insecure and thus deprecated) or CHAP (Challenge-handshake authentication protocol mostly in use today) or EAP (Extensible Authentication Protocol)

# Point-to-Point-Protocol

- Link Control Protocol (LCP) for initiating / terminating connections
  - Allowing hosts to negotiate connection options
  - Supports both byte- and bit-oriented encodings
- Network Control Protocol (NCP) for negotiating network-layer information
  - Network address, compression options, DNS, ...
- PPP data frame format
  - Flag of 0111 1110
  - Address 1111 1111
  - Control 0000 0011

# Point-to-Point-Protocol

- PPP data frame format (cont.)
  - First and/or second byte: kind of payload packet (e.g. LCP, NCP, IP, IPv6, IPX, AppleTalk, ...)
  - Information field contains PPP payload with a MTU negotiated between both sides (default is MTU of 1500 Bytes); Padding (if needed)
  - Frame check of 2 or 4 Bytes (standard CRC)
  - Flag 0111 1110



# Point-to-Point-Protocol

- PPP byte stuffing
  - Problem: How to distinguish bit patterns of frame delimitors from data within payload?
  - What happens if 0111 1110 appears within Info field?
  - Cannot require upper layer protocols to avoid this pattern
  - Uses “byte stuffing” - adding of additional bytes into the stream
  - Defines a  special control escape of 0111 1101
  - If any 0111 1110 appears (beside the flag itself) it is preceeded by the control escape pattern

# Point-to-Point-Protocol

- PPP states / phases
  - Link Dead - phase occurs when the link fails, or one side finished the connection (e.g. user ending his or her dialup connection)
  - Link Establishment Phase
    - Phase is active when Link Control Protocol negotiation is attempted
    - If successful control goes to authentication phase (if disired) or directly to Network Layer Protocol phase
  - Authentication Phase (optional): Authentication of each other before a connection is established
  - Network Layer Protocol Phase: Active when each desired Network Control Protocols are invoked
    - Data transport for all protocols which are started

# Point-to-Point-Protocol

- PPP states / phases (cont.)
  - Link Termination Phase for closing down connections
    - On authentication failure
    - Too many checksum errors
    - If link suddenly fails
    - If user decides to shut down connection. Tries a graceful shutdown on any active connection)
- Multiclass PPP for running more than one PPP over the same connection
- Extensions like PPTP
  - VPN like connection for layer 2 (thus able to handle multi network layer protocols, different e.g. compared to IPsec)
  - Insecure in the first version

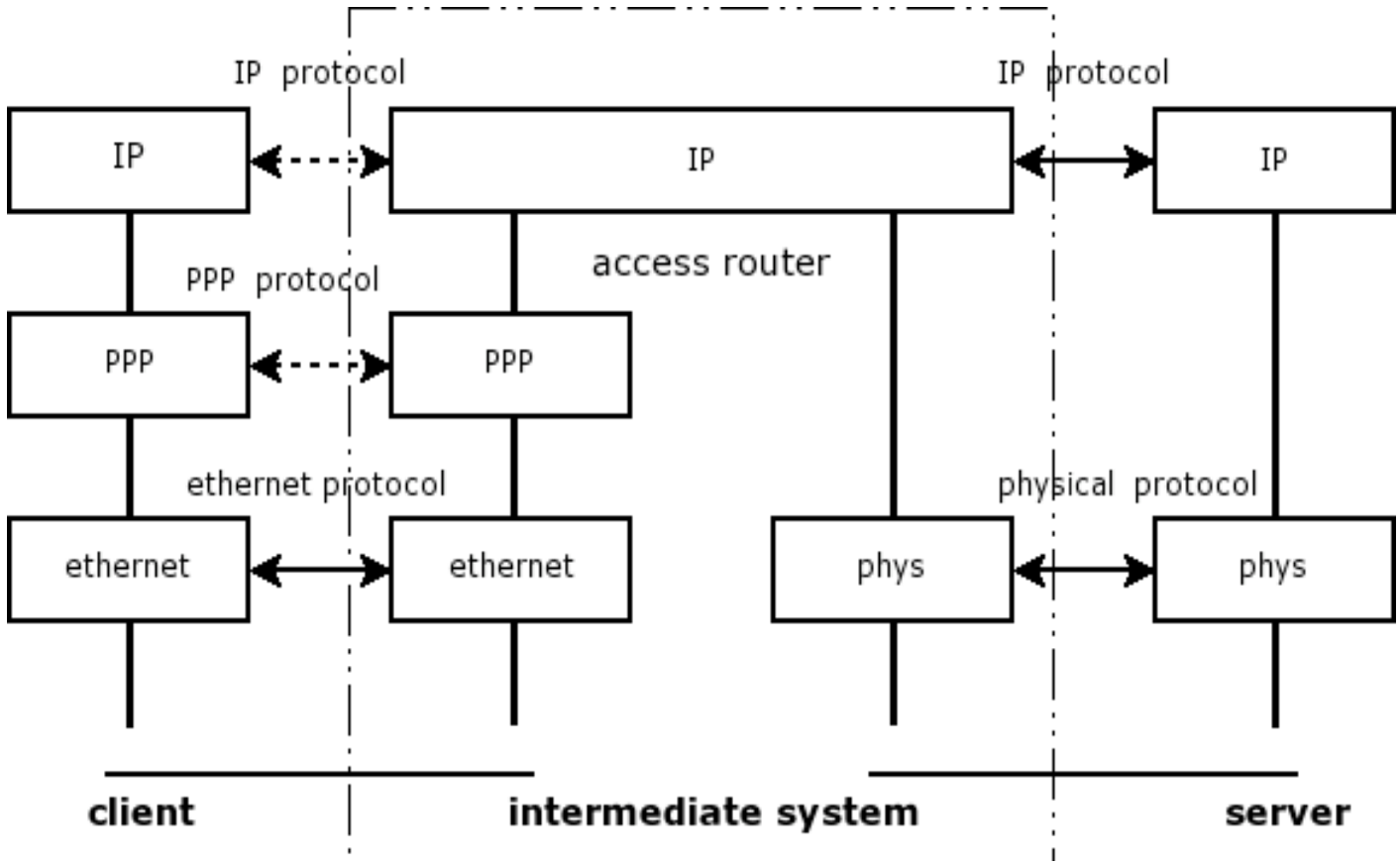
# Datagram Delivery for IPv4

- Routing table will look a little bit different (compared to LAN e.g. Ethernet connection, check in practical part)
  - Netmask is 255.255.255.255 (just one address in network)
  - Addresses do not have to share the same prefix (!)
  - e.g. 80.43.112.34 for the local machine and 217.67.12.33 for the providers gateway
    - Seen with modem, ISDN, PPPoE (ADSL) connections for individuals toward end user ISPs
  - Default gateway is just the machine at the other end of connection or just oneself (if special address of 10.64.64.64 was assigned for the gateway)
- Extension of PPP for Ethernet, (ATM) on DSL

# PPPoE

- PPP over Ethernet (PPPoE) is PPP (designed for serial communications) that has been adapted to an Ethernet network
- PPPoE turns multi-access Ethernet (last lectures) into a dedicated poin-to-point link
- Offers speedy access between two well-defined points, and its traffic can be monitored/authenticated
- PPPoE provides the ability to connect a network of hosts over a simple bridging access device (DSL or cable modem) to a remote access concentrator
- Each host utilizes its own PPP stack (check it for modem or cellular connections on your machine) and the user is presented with a familiar interface

# PPPoE principle

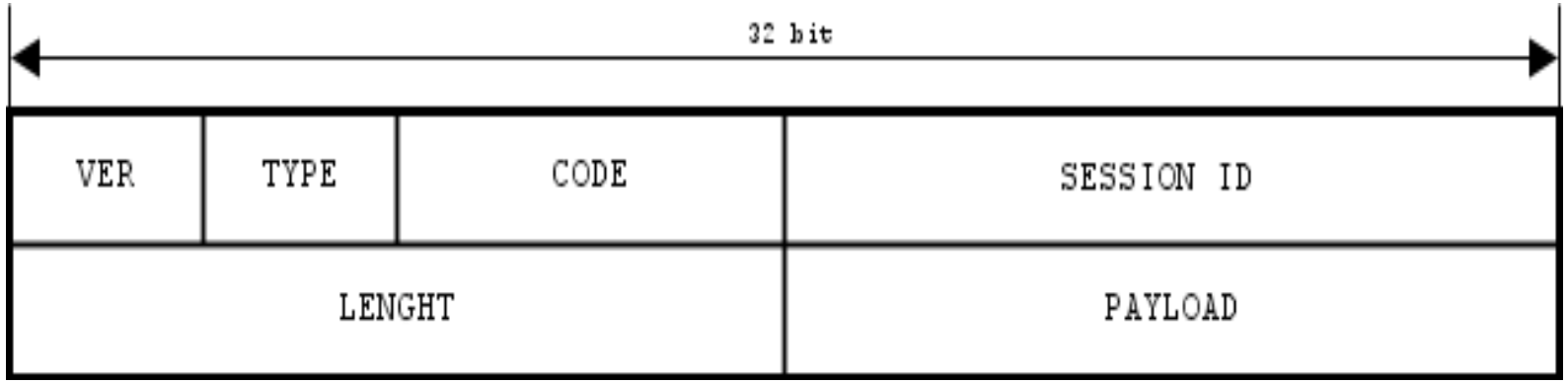


# PPPoE

- For point-to-point connection over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier
- PPPoE includes a discovery protocol to do this (practical part)
- So, it is possible to run more than one PPPoE session over one DSL link and
  - Many providers can offer services over same infrastructure
- Under Linux – “roaring penguin” PPPoE services (practical part)
  - Provide tools for analyzing of PPPoE links
- Try multiple links with the DSL service provider (depends on your DSL base provider, multiple links possible, but bandwidth is the same)

# PPPoE header

- VER field is four bits : 0x1
- TYPE field is four bits : 0x1
- CODE field is eight bits: Discovery and PPP Session
- SESSION_ID field is 16 bits
- Length and payload (data)



# PPPoE operation

- PPPoE Discovery phase:
  - PADI (PPPoE Active Discovery Initiation) Packet
    - The frame is sent to the broadcast Ethernet address
    - (MAC: 0xffffffff code: 0x09 SESSION_ID: 0x0000)
- At the Access-Concentrator (AC)
  - PADO (PPPoE Active Discovery Offer) Packet
    - The frame is sent to the client's Ethernet address
    - code: 0x07 SESSION_ID: 0x0000
  - PADR (PPPoE Discovery Request)
    - The client picks an access concentrator (if more than one responded) and sends a packet to it's Ethernet address.
    - ( code: 0x19 SESSION_ID: 0x0000 )

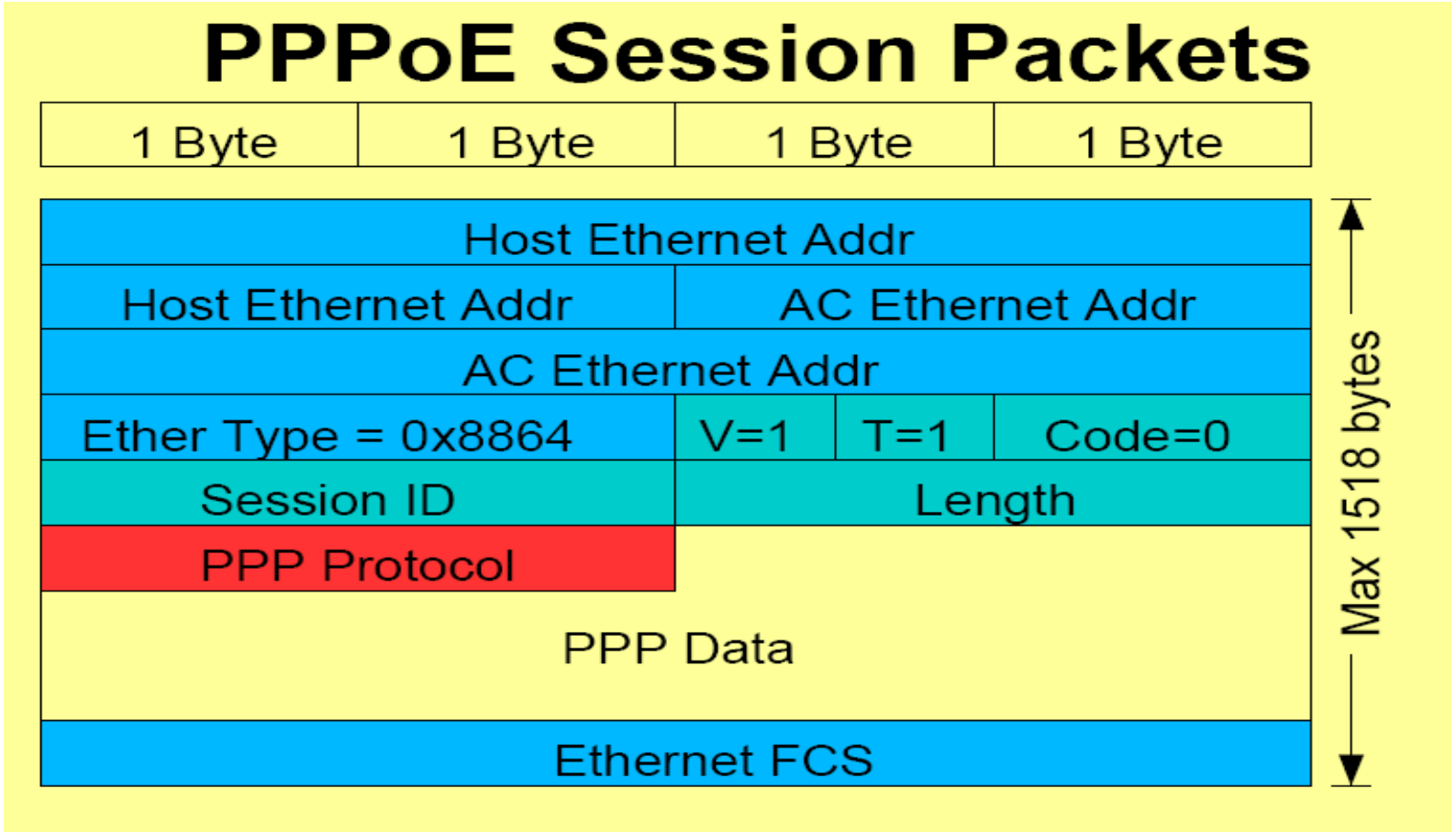
# PPPoE operation

- PADC (PPPoE Active Session Confirmation)
  - The access concentrator sends a packet
  - ( code: 0x65 SESSION_ID: 0x0000 )
- PADT (PPPoE Active Discovery Terminate)

- After initialisation: PPPoE Session
  - Normal PPP session
  - See protocol stacking in wireshark
  - Packets are transmitted over Ethernet instead of a serial link

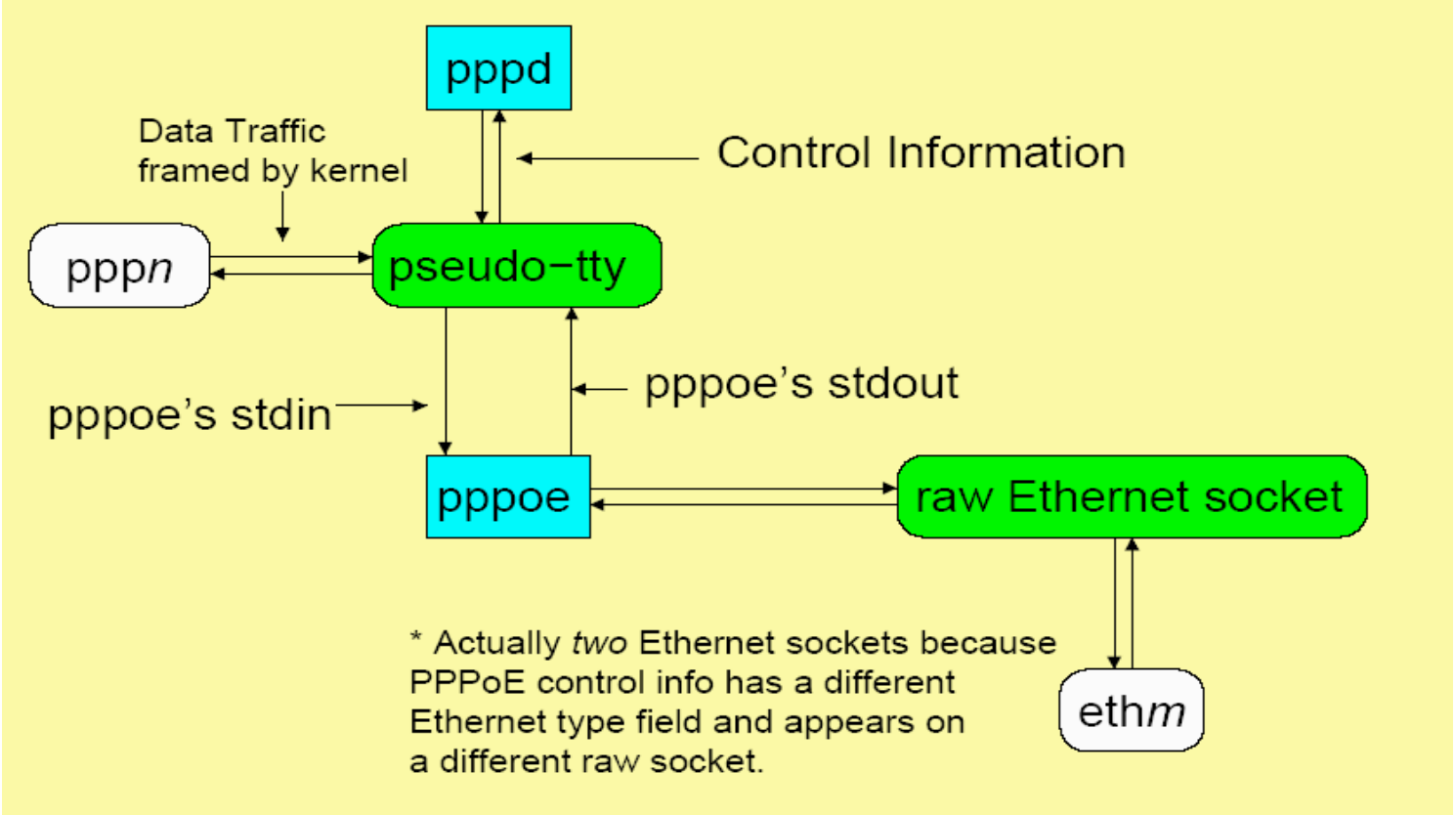
# PPPoE operation

- PPPoE Session packet format

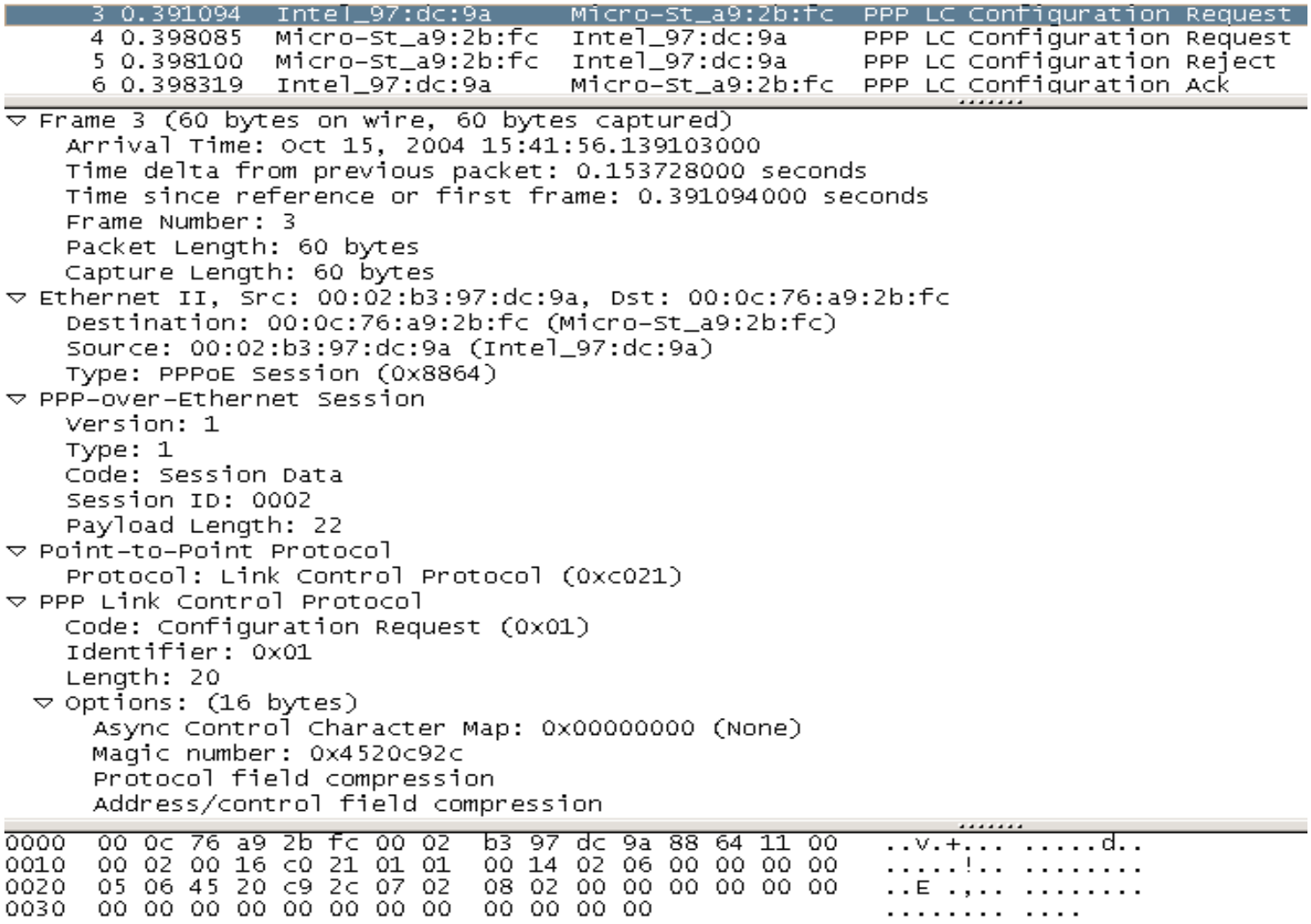


# PPPoE operation in Linux

- Setup of special network interfaces for mapping of PPP and Ethernet



# PPPoE operation – wireshark example (config request)



# PPPoE operation – ethereal example (configuration reject)

```
    3 0.391094   Intel_97:dc:9a     Micro-St_a9:2b:fc  PPP LC Configuration Request
    4 0.398085   Micro-St_a9:2b:fc  Intel_97:dc:9a     PPP LC Configuration Request
    5 0.398100   Micro-St_a9:2b:fc  Intel_97:dc:9a     PPP LC Configuration Reject
    6 0.398319   Intel_97:dc:9a     Micro-St_a9:2b:fc  PPP LC Configuration Ack
```

```
▽ Frame 5 (36 bytes on wire, 36 bytes captured)
    Arrival Time: Oct 15, 2004 15:41:56.146109000
    Time delta from previous packet: 0.000015000 seconds
    Time since reference or first frame: 0.398100000 seconds
    Frame Number: 5
    Packet Length: 36 bytes
    Capture Length: 36 bytes
▽ Ethernet II, Src: 00:0c:76:a9:2b:fc, Dst: 00:02:b3:97:dc:9a
    Destination: 00:02:b3:97:dc:9a (Intel_97:dc:9a)
    Source: 00:0c:76:a9:2b:fc (Micro-St_a9:2b:fc)
    Type: PPPoE Session (0x8864)
▽ PPP-over-Ethernet Session
    Version: 1
    Type: 1
    Code: Session Data
    Session ID: 0002
    Payload Length: 16
▽ Point-to-Point Protocol
    Protocol: Link Control Protocol (0xc021)
▽ PPP Link Control Protocol
    Code: Configuration Reject (0x04)
    Identifier: 0x01
    Length: 14
  ▽ Options: (10 bytes)
      Async Control Character Map: 0x00000000 (None)
      Protocol field compression
      Address/control field compression
```

# PPPoE operation – link control protocol (LCP)

- LCP Link Control Protocol
  - Handles authentication as in PPP
  - LCP Acknowledge
  - LCP Nak (Not Acknowledged)
  - Two modes of the authentication
    - PAP Password Authentication Protocol
    - CHAP Challenge Handshake Authentication Protocol
- Accounts check normally by a RADIUS server
  - Triple A: Authentication, Authorization & Accounting

- Machine sends a request to a AC to gain access to a particular network resource using access credentials
- AC contacts the RADIUS with Access Request message

# PPPoE authentication - RADIUS

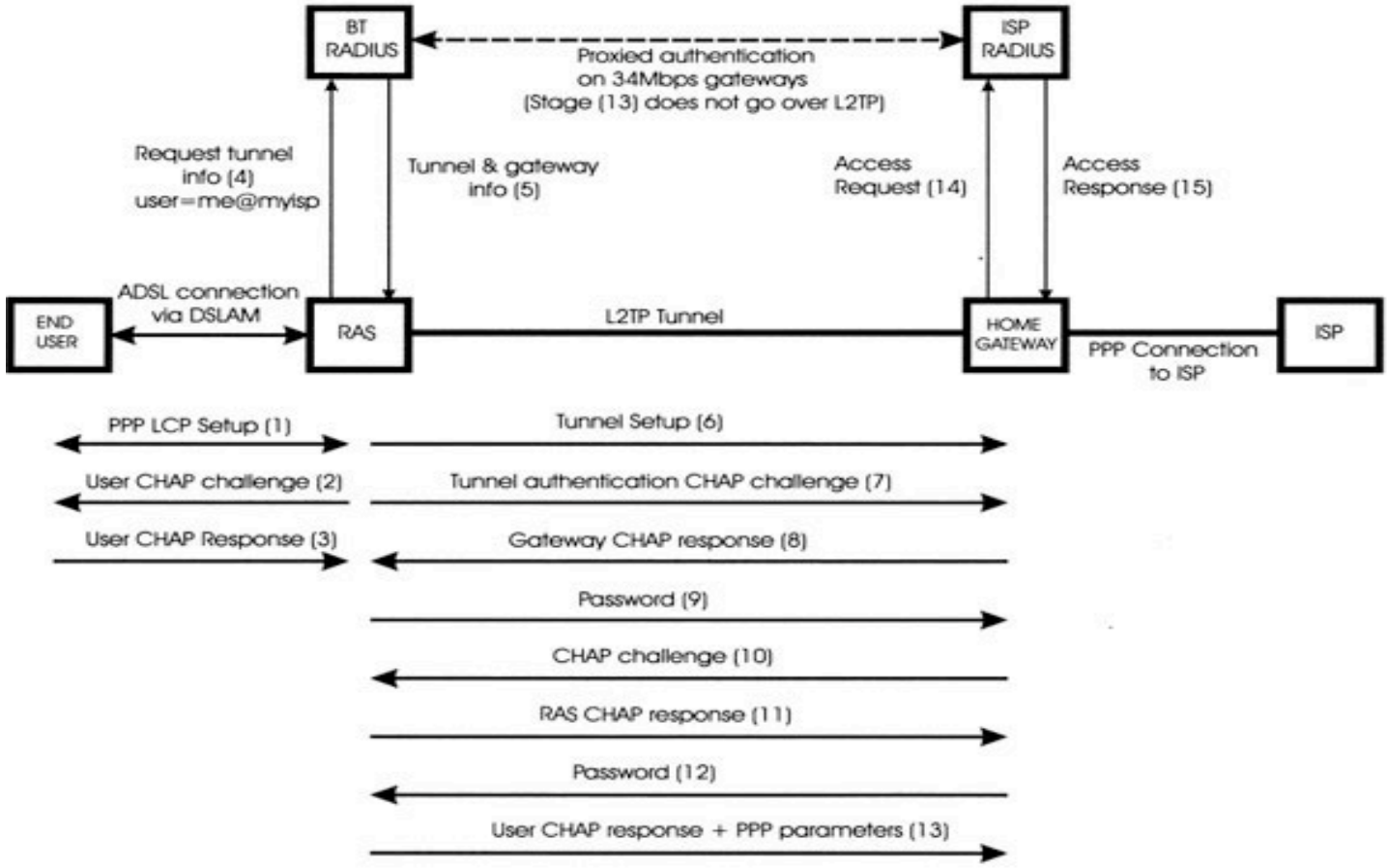
- RADIUS idea (Remote Authentication Dial In User Service)
  - Simple Network Access Servers
  - Central User Administration
  - User Roaming
  - Protection Against Sniffing (problem of packet interception)
- Typically implemented in/invoked by AC - Access Concentrator
- RADIUS – server handling the
  - User name / password
  - Challenge / response
  - Interoperation with CHAP (Challenge-handshake authentication protocol) or PAP (Password authentication protocol)

# RADIUS Functionality

- Proxy functionality: When receiving AAA (Authentication, Authorization, and Accounting) requests for a username containing a realm the server will then proxy the request to the configured home server for that domain
  - Needed e.g. several providers sharing the same physical infrastructure
  - Proxying server can add, remove or rewrite AAA requests if needed
- RADIUS uses message/response types
  - Access-Request
  - Access-Challenge – for additional tokens like PINs
  - Access-Accept – may contain several authorization parameters like IP address to be assigned or address pool, maximum length that the user may remain connected, access lists, priority queue or restrictions on a user's access, VLAN parameters
  - Access-Reject

# RADIUS protocol

- RADIUS – protocol – involved by PPP/CHAP



ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

# Communication Systems

**Christian Schindelhauer**

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe
Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG