PPP

The point-to-point protocol

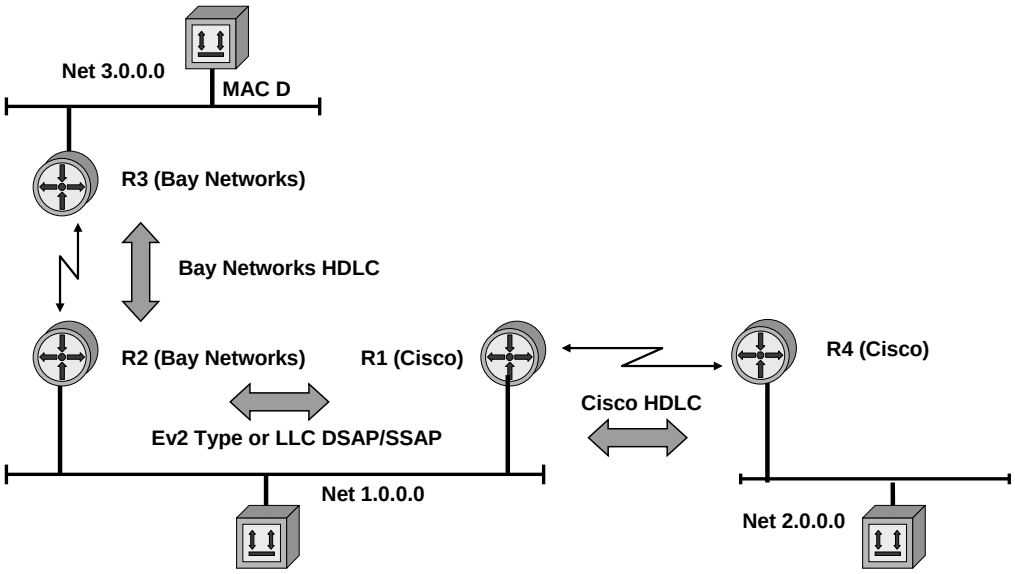
PPP versus SLIP

- PPP
  - Where is PPP used
  - What is the task of LCP
  - What is the task of NCP
- SLIP
  - Serial Line IP
  - Predecessor of PPP
  - We don't even think of it today

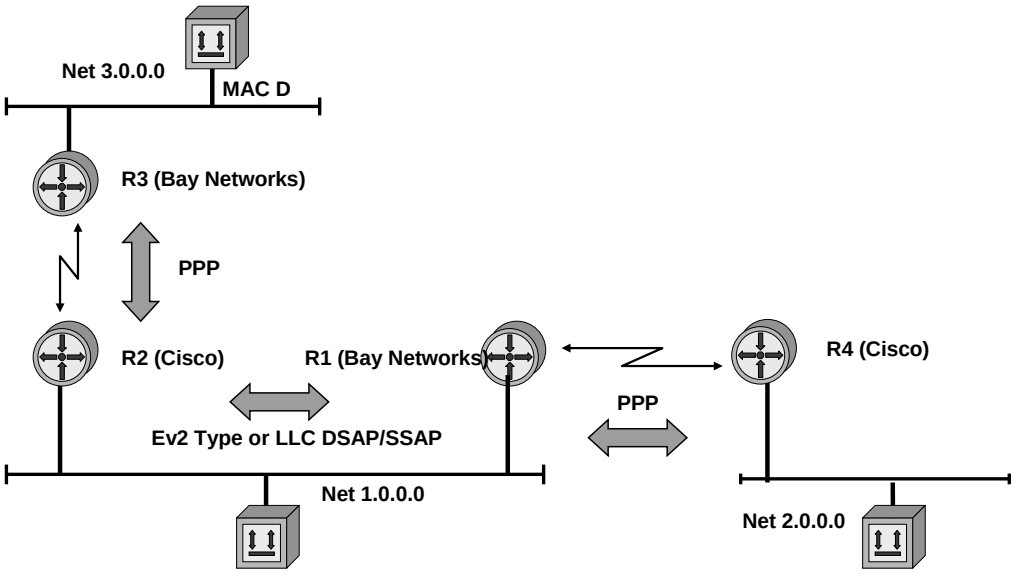
Reasons for Point-to-Point Protocol (PPP)

- **Communication between router of different vendors on a LAN was possible**
  - from the very beginning
    - Remember: Ethernet V2 Protocol Type field or LLC-DSAP/SSAP fields carry information about the protocol stack (e.g. IP or IPX or SAN or NetBEUI or AppleTalk)
- **Communication between router of different vendors on a serial line was not possible**
    - because of the proprietary “kind of HDLC” encapsulation method used by different vendors
- **PPP standardizes multiprotocol encapsulation on a serial line**
    - hence interoperability is the main focus

Interoperability without PPP



Interoperability with PPP



Today's Main Focus of PPP

- **Providing Dial-In connectivity for IP systems**
  - using modems and Plain Old Telephone Network (POTS)
    - PPP
  - using ISDN
    - PPP over transparent B-channel
  - using ADSL (Asymmetric Digital Subscriber Line)
    - PPPoE (PPP over Ethernet)
    - PPPoA (PPP over ATM)
  - using Dial-In VPN technology
    - Microsoft PPTP (Point-to-Point Tunneling Protocol)
    - Cisco L2F (L2 Forwarding Protocol)
    - L2TP (Layer2 Tunneling Protocol), RFC

Introduction (1)

- **Goal of PPP**
  - **Convey datagrams over a serial link**
  - **Both synchronous or asynchronous serial links are supported**
  - **Both bit or byte oriented transmissions are supported**
- **Basically, PPP consists of**
  - **One Link Control Protocol (LCP)**
  - **Several Network Control Protocols (NCPs)**

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

1. A method for encapsulating multi-protocol datagrams.
2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
3. A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

Introduction (2)

- HDLC is basis for encapsulation
  - Only framing and error detection necessary
  - Only simple unnumbered information frames (UI)
- PPP supports full-duplex links only (!)
- PPP Frame = Datagram + 2-8 bytes extra header
  - Extra header consists of HDLC header and PPP header
- Byte Stuffing: Data dependent overhead!

Overhead

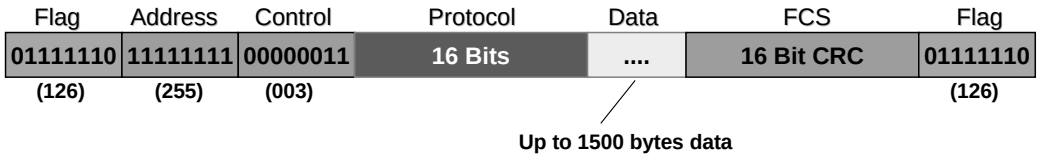
Only 8 additional octets are necessary to form the encapsulation when used with the default HDLC framing. In environments where bandwidth is at a premium, the encapsulation and framing may be shortened to 2 or 4 octets.

Byte Stuffing

If the flag byte (126) occurs in the data field it has to be escaped using the escape byte 125, while byte 126 is transmitted as a two byte sequence (125, 94) and the escape byte itself is transmitted as (125, 93).

Data Link Layer: HDLC

- Address 11111111 means "all stations"
  - PPP does not assign individual station addresses
- Only the control field 00000011 is used
  - Unnumbered Information (UI) command
- Protocol field identifies datagram
  - Already part of PPP, not HDLC (!)



Up to 1500 bytes data

(C) Herbert Haas 2005/03/11 9

Protocol: The True PPP Field

The most important field is the protocol field, which has two octets and its value identifies the datagram encapsulated in the Information field of the packet.

PPP Header Compression

If protocol field compression is enabled, the protocol field is reduced from 2 to 1 byte. Since the first two bytes are always constant, that is the address byte (always 255) and the control byte (always 003), PPP also supports address-and-control-field-compression, which omits these bytes.

Byte Stuffing

If the flag byte (126) occurs in the data field it has to be escaped using the escape byte 125, while byte 126 is transmitted as a two byte sequence (125, 94) and the escape byte itself is transmitted as (125, 93).

Protocol Field

0xxx – 3xxx	**L3 protocol type**
4xxx – 7xxx	**L3 protocol type without associated NCPs**
8xxx – bxxx	**Associated NCPs for protocols in range 0xxx – 3xxx**
cxxx – fxxx	**LCP, PAP, CHAP, ...**

0021	IP
002b	Novell IPX
002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
8021	IP-NCP (IPCP)
802b	IPX-NCP (IPXCP)

Important Examples

c021	Link Control Protocol (LCP)
c023	Password Auth. Protocol (PAP)
c025	Link Quality Report
c223	Challenge Handshake Auth. Protocol (CHAP)

(C) Herbert Haas 2005/03/11 10

Protocol Field Values

Protocol field values in the "0***" to "3***" range identify the network-layer protocol of specific packets, and values in the "8***" to "b***" range identify packets belonging to the associated Network Control Protocols (NCPs), if any. Protocol field values in the "4***" to "7***" range are used for protocols with low volume traffic which have no associated NCP. Protocol field values in the "c***" to "f***" range identify packets as link-layer Control Protocols (such as LCP).

All these numbers are controlled by the IANA (see RFC-1060).

LCP

- **Link Control Protocol (LCP)**
  - **Setup, configure, test and terminate PPP connection**
  - **Supports various environments**
- **LCP negotiates**
  - **Encapsulation format options**
  - **Maximal packet sizes**
  - **Identification and authentification of peers (!)**
  - **Determination of proper link functionality**

In order to be sufficiently versatile to be portable to a wide variety of environments, PPP provides a Link Control Protocol (LCP). The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, authenticate the identity of its peer on the link, determine when a link is functioning properly and when it is defunct, detect a looped-back link and other common misconfiguration errors, and terminate the link.

Types of LCP Packets

- **There are three classes of LCP packets:**
  - class 1: Link Configuration packets used to establish and configure a link
    - Configure-Request (code 1, details in option field), Configure-Ack (code 2), Configure-Nak (code 3, not supported option) and Configure-Reject (code 4, not supported option)
  - class 2: Link Termination packets used to terminate a link
    - Terminate-Request (code 5) and Terminate-Ack (code 6)
  - class 3: Link Maintenance packets used to manage and debug a link
    - Code-Reject (code 7, unknown LCP code field), Protocol-Reject (code 8, unknown PPP protocol field), Echo-Request (code 9), Echo-Reply (code 10) and Discard-Request (code 11)

LCP and PPP Connection

- **LCP**
  - supports the establishment of the PPP connection and allows certain configuration options to be negotiated
- **PPP connection is established in four phases**
  - phase 1: link establishment and configuration negotiation
    - done by LCP (note: deals only with link operations, does not negotiate the implementation of network layer protocols)
  - phase 2: optional procedures that were agreed during negotiation of phase 1 (e.g. CHAP authentication or compression)
  - phase 3: network layer protocol configuration negotiation done by corresponding NCP´s
    - e.g. IPCP, IPXCP, …
  - phase 4: link termination

PPP Phases

- **task of phase 1**
  - LCP is used to automatically
    - agree upon the encapsulation format options
    - handle varying limits on sizes of packets
    - detect a looped-back link and other common configuration errors (magic number for loopback detection)
  - options which may be negotiated
    - maximum receive unit
    - authentication protocol
    - quality protocol
    - Protocol-Field-Compression
    - Address-and-Control-Field-Compression
    - these options are described in RFC 1661 (except authentication protocols)

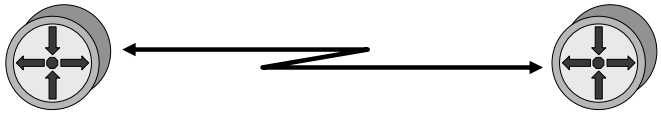
PPP Phases

- **task of phase 1 (cont.)**
  - options which may be negotiated but implementations are specified in other RFCs
    - PPP link quality protocol (RFC 1989)
    - PPP compression control protocol (RFC 1962)
    - PPP compression STAC (RFC 1974)
    - PPP compression PREDICTOR (RFC 1978)
    - PPP multilink (RFC 1990)
    - PPP callback (draft-ietf-pppext-callback-ds-01.txt)
    - PPP authentication CHAP (RFC 1994)
    - PPP authentication PAP (RFC 1334)
    - PPP Extensible Authentication Protocol (EAP), RFC 2284

PPP Phases

- **task of phase 2**
  - providing of optional facilities
    - authentication, compression initialization, multilink, etc.
- **task of phase 3**
  - network layer protocol configuration negotiation
    - after link establishment, stations negotiate/configure the protocols that will be used at the network layer; performed by the appropriate network control protocol
    - particular protocol used depends on which family of NCPs is implemented
- **task of phase 4**
  - link termination
    - responsibility of LCP, usually triggered by an upper layer protocol of a specific event

PPP Link Operation Example



Phase 1

Configure Request

Configure ACK

Configure Request

Configure ACK

LCP Operations (several LCP options are exchanged and accepted options acknowledged)

Phase 3

Configure Request IP

Configure ACK

Configure Request IP

Configure ACK

NCP Operations for IPCP

Exchange Traffic

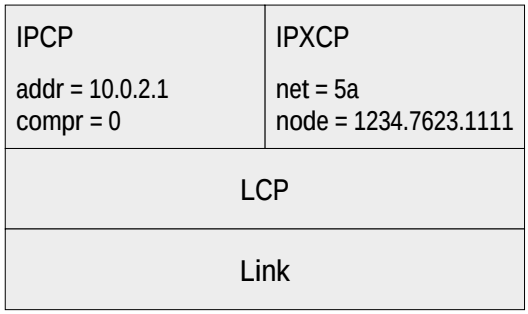
Phase 4

Terminate Request

Terminate ACK

Network Control Protocol

- one per upper layer protocol (IP, IPX…)
- each NCP negotiates parameters appropriate for that protocol
- NCP for IP (IPCP)
  - IP address, Def. Gateway, DNS Server, TTL, TCP header compression can be negotiated
  - Similar functionality as DHCP for LAN



NCPs

- **Network Control Protocols (NCPs)**
  - **Helper to establish various network protocols**
  - **IP uses "IPCP"**
- **Typical tasks**
  - **Assignment and management of IP addresses**
  - **Compression and authentication**

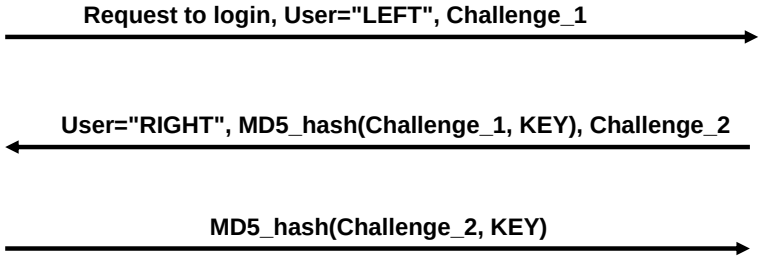
Point-to-Point links tend to exacerbate many problems with the current family of network protocols. For instance, assignment and management of IP addresses, which is a problem even in LAN environments, is especially difficult over circuit-switched point-to-point links (such as dial-up modem servers). These problems are handled by a family of Network Control Protocols (NCPs), which each manage the specific needs required by their respective network-layer protocols.

NCPs have been developed for all important network layer protocols such as IP, which uses the IP Control Proocol (IPCP).

There are also NCPs designed to enable compression and authentication.

CHAP – The Challenge Handshake Authentication Protocol

- Supports 1-way and 2-way authentication
- Periodically verifies the identity of the remote node using a three-way handshake
- Relies on MD5 hash (regarded as weak today)
  - Offline dictionary attacks possible!
- Still widely used



Microsoft's MSCHAPv2 is even worse

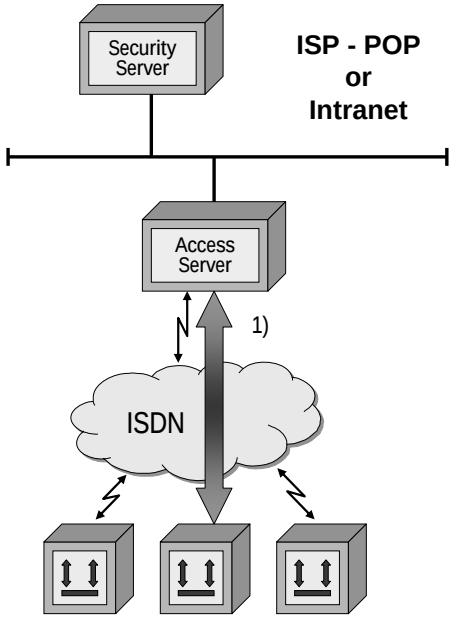
PPP today

- Is still a usual choice when carrying IP packets over high-speed serial lines
- Several flavors for different media
  - PPPOE (over Ethernet)
  - PPPOA (over ATM)
  - PPTP (Tunnel PPP through a IP network)
  - POS – Packet over SONET/SDH
- See RFC 1661, 1662

PPP as Dial-In Technology

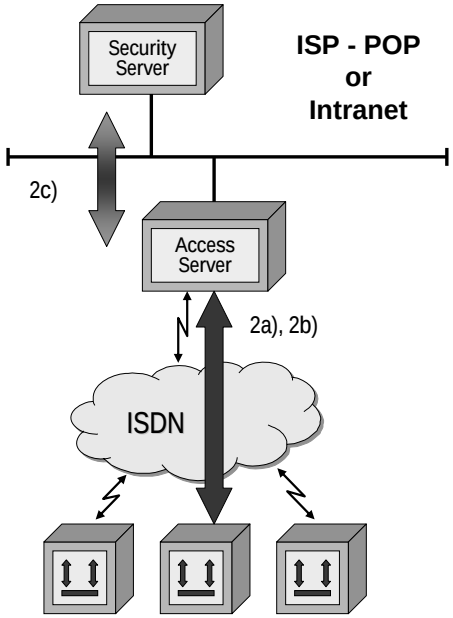
- **Dial-In:**
  - Into a corporate network (Intranet) of a company
    - Here the term RAS (remote access server) is commonly used to describe the point for accessing the dial-in service
  - Into the Internet by having an dial-in account with an Internet Service Provider (ISP)
    - Here the term POP (point-of-presence) is used to describe the point for accessing the service

RAS Operation 1



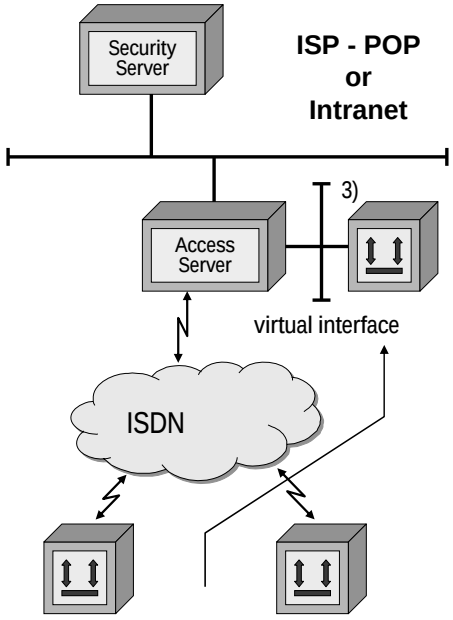
- **remote PC places ISDN call to access server, ISDN link is established (1)**

RAS Operation 2



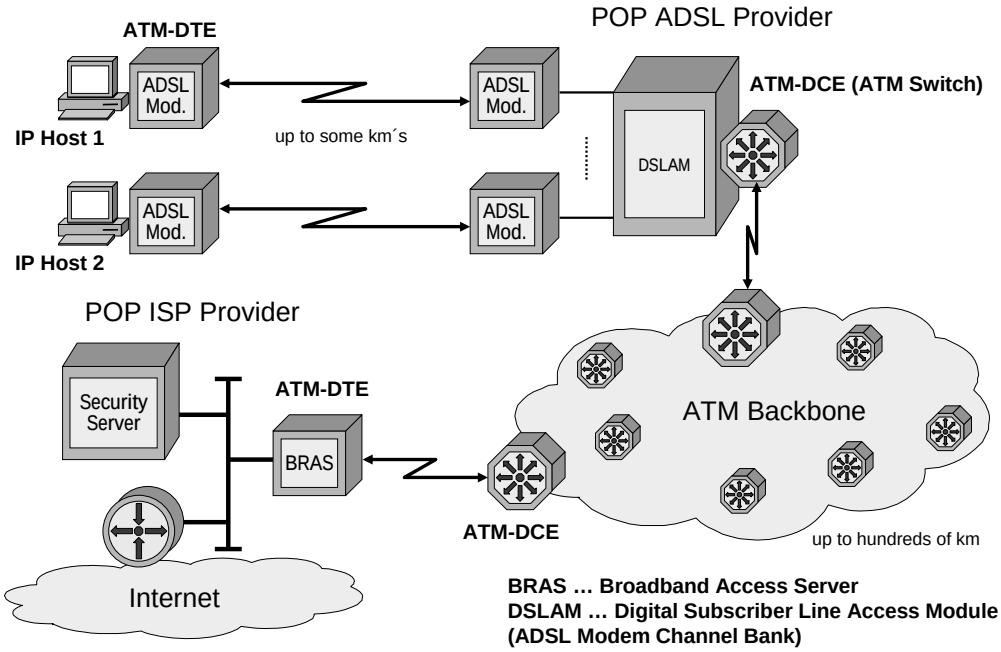
- **PPP link (multiprotocol over serial line) is established**
  - LCP Link Control Protocol (2a)
    - establishes PPP link plus negotiates parameters like authentication CHAP
  - authentication
    - CHAP Challenge Authentication Protocol to transport passwords (2b)
    - verification maybe done by central security server (2c) -> Radius, TACACS, TACACS+

RAS Operation 3



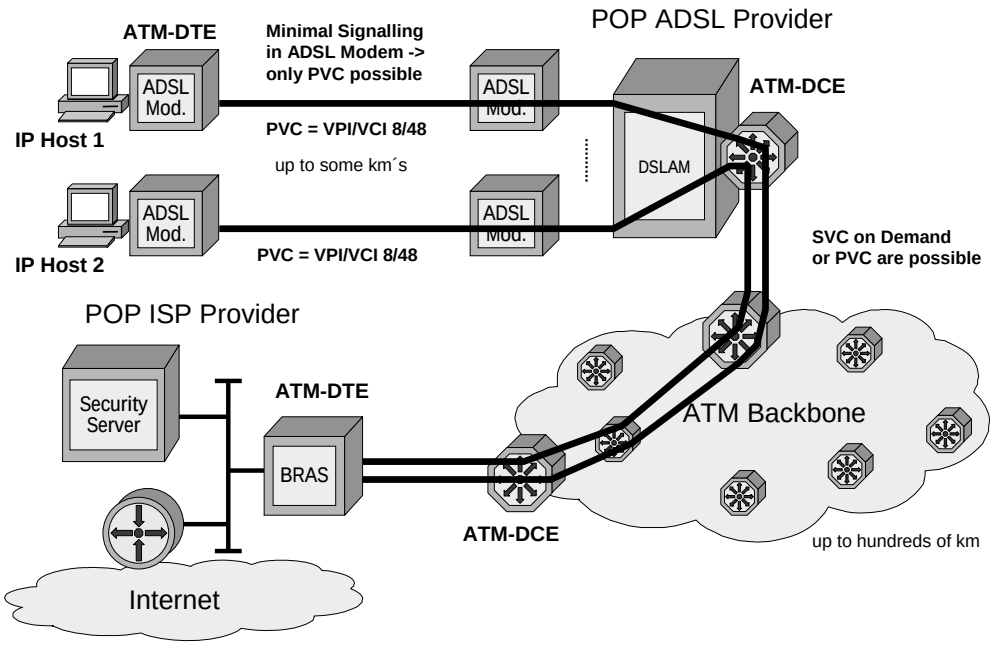
- **PPP NCP (Network Control Protocol) IPCP**
  - assigns IP address, Def. GW, DNS to remote PC
- **remote PC appears as**
  - device reachable via virtual interface (3), IP host Route
- **optionally**
  - filter could be established on that virtual interface
    - authorization
  - accounting can be performed
    - actually done by security server (AAA server)
    - TACACS, Radius

ADSL: Physical Topology

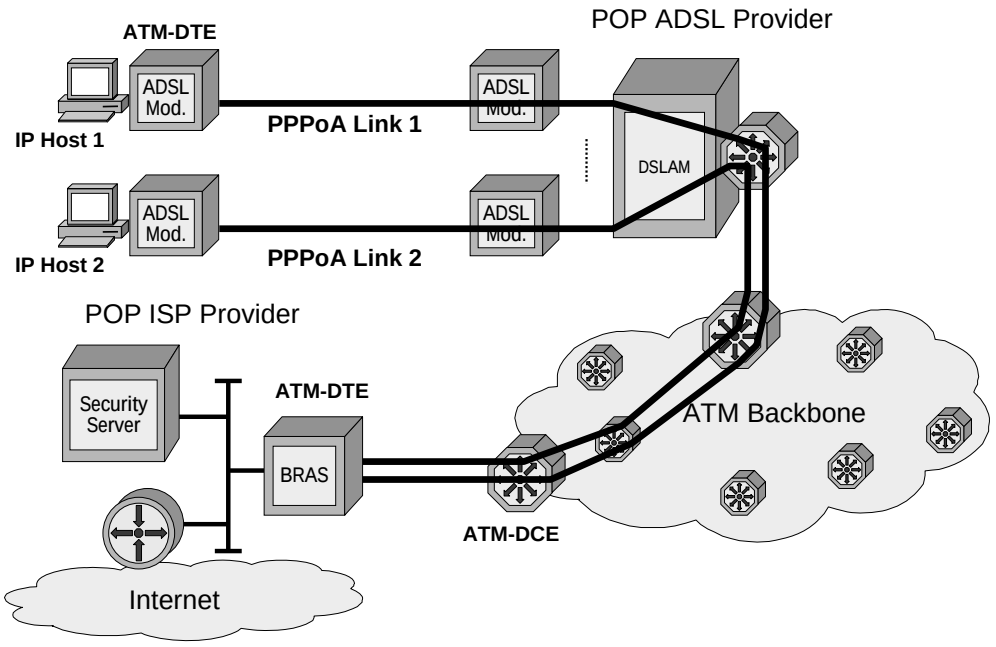


BRAS … Broadband Access Server
DSLAM … Digital Subscriber Line Access Module (ADSL Modem Channel Bank)

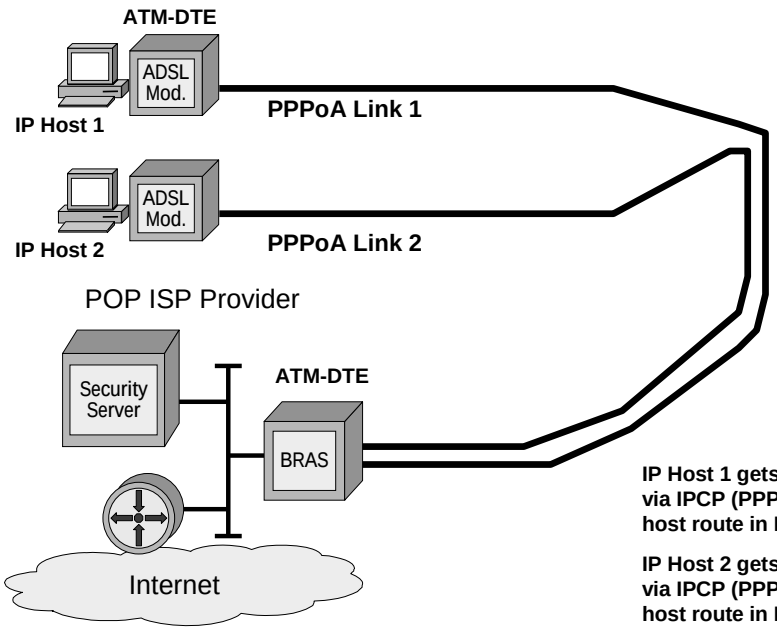
ADSL: ATM Virtual Circuits



ADSL: PPP over ATM (PPPoA)



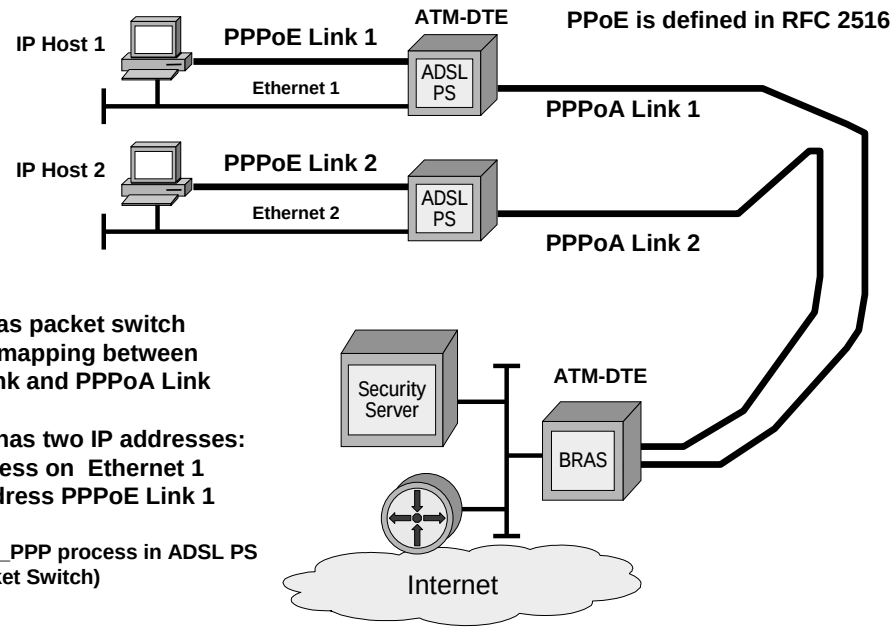
ADSL: PPP over ATM (PPPoA), IPCP



IP Host 1 gets global IP address via IPCP (PPP-NCP), appears as host route in BRAS

IP Host 2 gets global IP address via IPCP (PPP-NCP), appears as host route in BRAS

ADSL: PPP over Ethernet (PPPoE)

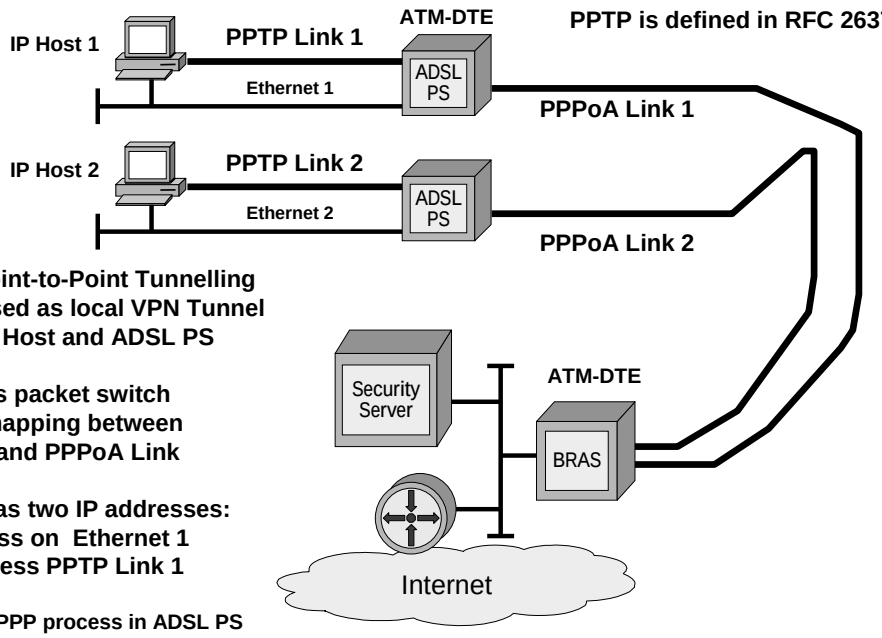


ADSL PS as packet switch performs mapping between PPPoE Link and PPPoA Link

IP Host 1 has two IP addresses:
local address on Ethernet 1
global address PPPoE Link 1

note: Relay_PPP process in ADSL PS (PS ... Packet Switch)

ADSL: PPTP over Ethernet (Microsoft VPN)



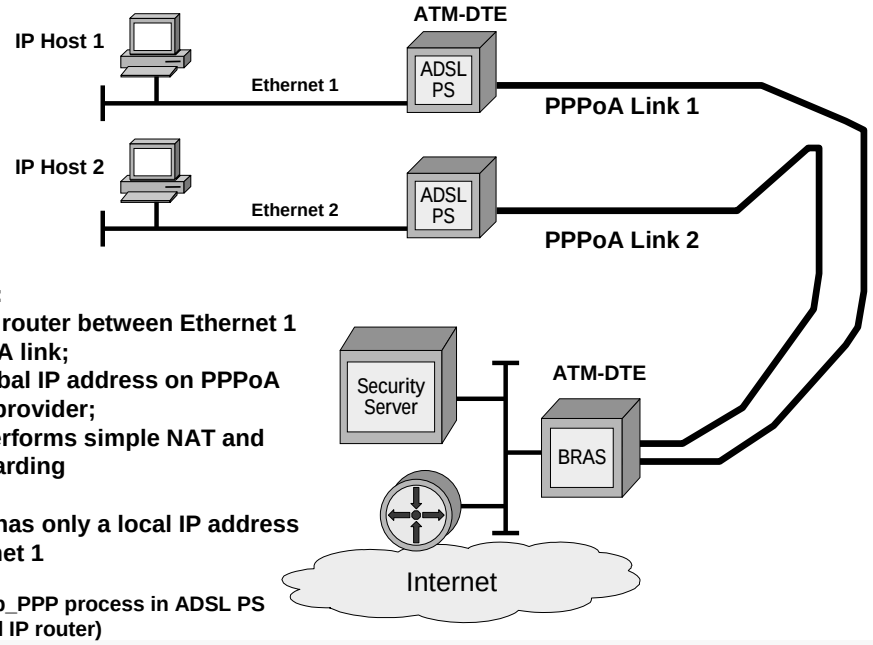
PPTP … Point-to-Point Tunnelling Protocol used as local VPN Tunnel between IP Host and ADSL PS

ADSL PS as packet switch performs mapping between PPTP Link and PPPoA Link

IP Host 1 has two IP addresses:
local address on Ethernet 1
global address PPTP Link 1

note: Relay_PPP process in ADSL PS

ADSL: Routed PPPoA

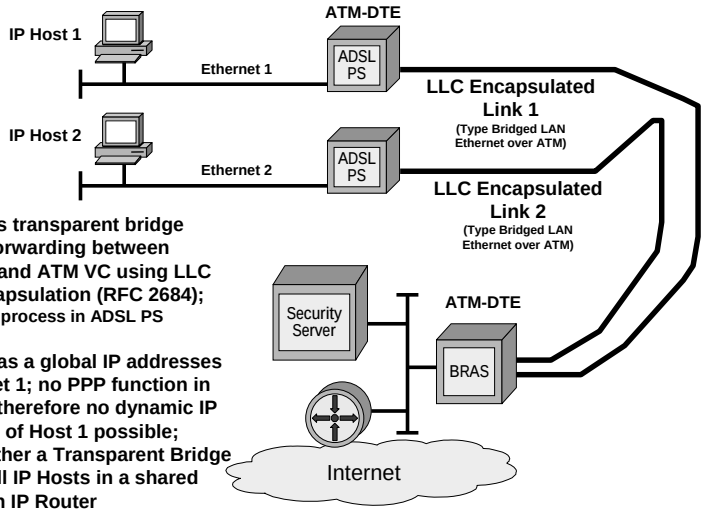


ADSL PS :
acts as IP router between Ethernet 1 and PPPoA link;
gets a global IP address on PPPoA link from provider;
usually performs simple NAT and DNS forwarding

IP Host 1 has only a local IP address on Ethernet 1

note: Dialup_PPP process in ADSL PS (PS is a real IP router)

ADSL: Ethernet Approach



ADSL PS as transparent bridge performs forwarding between Ethernet 1 and ATM VC using LLC bridge encapsulation (RFC 2684);
note: Bridge process in ADSL PS

IP Host 1 has a global IP addresses on Ethernet 1; no PPP function in BRAS and therefore no dynamic IP addressing of Host 1 possible;
BRAS is either a Transparent Bridge grouping all IP Hosts in a shared media or an IP Router