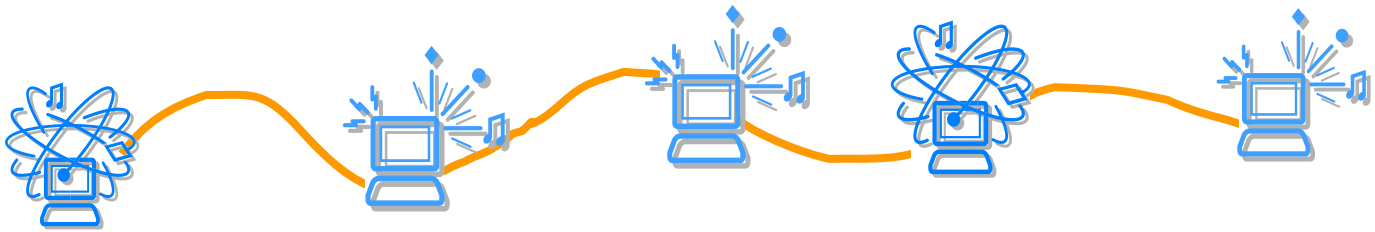
Mecanismos de *tunneling* – PPPoE, PPPoA

RFC 2516 - *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2364 - *PPP Over AAL5*



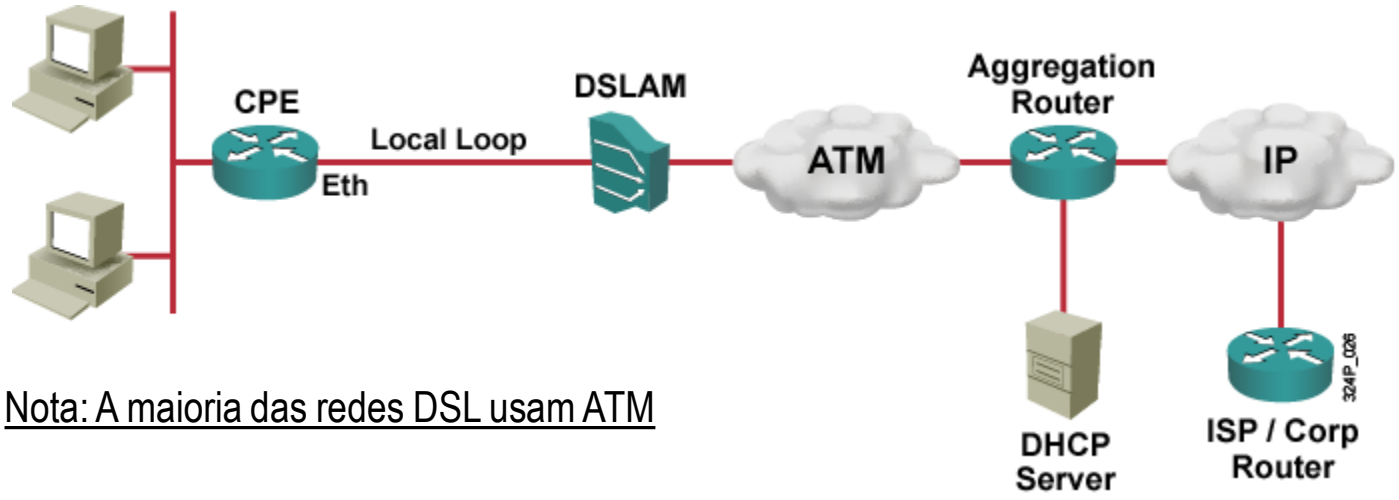
Segurança em Redes de Computadores

Redes de Comunicação

Porquê PPPoE?

- As formas tradicionais de aceder à Internet eram lentas devido a utilizarem ligações série via modem sobre linhas telefónicas comutadas. O PPP foi criado para correr directamente sobre estas ligações.
- Com o advento da Internet de banda larga com acesso através de tecnologias como o ADSL e modems para rede de cabo deu-se um grande incremento na largura de banda disponível para os utilizadores. Isto permitiu a existência de vários equipamentos interligados entre si através de redes locais como a Ethernet e ligados à Internet através de dispositivos com muito maior largura de banda.
- Infelizmente a Ethernet é não orientada à ligação e não tem suporte, como o PPP tem, para autenticação dos utilizadores, atribuição de endereço, compressão, etc. A forma de resolver esta falta sem desenvolver outro protocolo novo foi pôr o PPP a correr sobre Ethernet.
- **O PPPoE foi criado para conseguir o melhor de ambos os mundos – conseguir ligar um conjunto de equipamentos do utilizador final a um débito elevado, e usar mecanismos existentes e bem conhecidos para estabelecer sessões mantendo as interfaces de utilizador.**

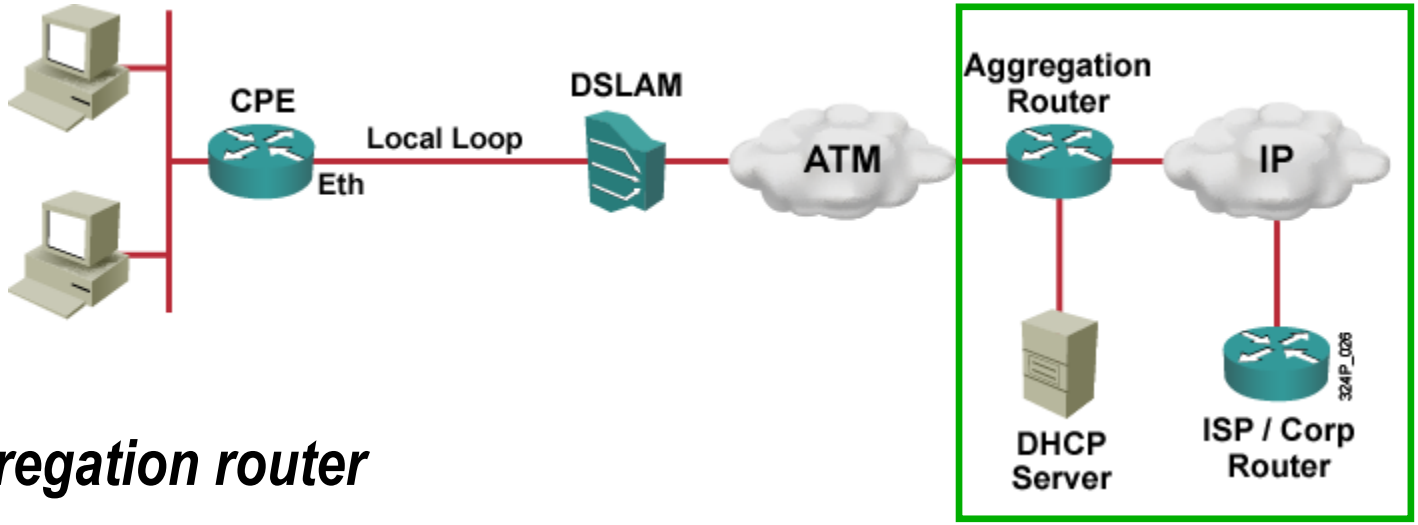
Transmissão através de ADSL



Nota: A maioria das redes DSL usam ATM

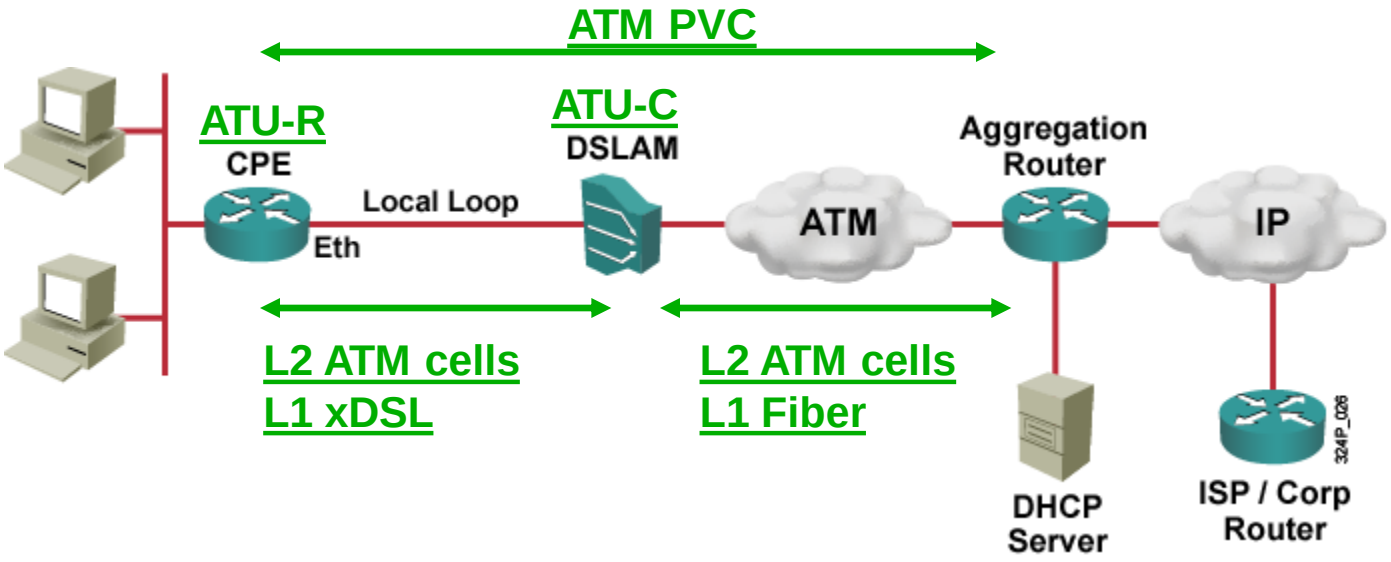
- O xDSL fornece os recursos para a ligação ao nível da camada 1
- **DSLAM**:
  - *Switch* ATM que inclui as placas ATU-C (placas de interface xDSL)
  - Termina o lado do operador do *loop* local
  - Comuta tráfego sobre a rede ATM para um *router* agregador

Transmissão através de ADSL



- ***Aggregation router***
  - Primeiro ponto onde o tráfego da camada 3 é examinado
- Há três formas de encapsular pacotes IP sobre uma ligação série (fisica ou virtual), como, por exemplo, sobre ATM/xDSL:
  - **RFC 1483/2684 *Bridged***
  - **PPP *over* Ethernet (PPPoE)**
  - **PPP *over* ATM (PPPoA)**

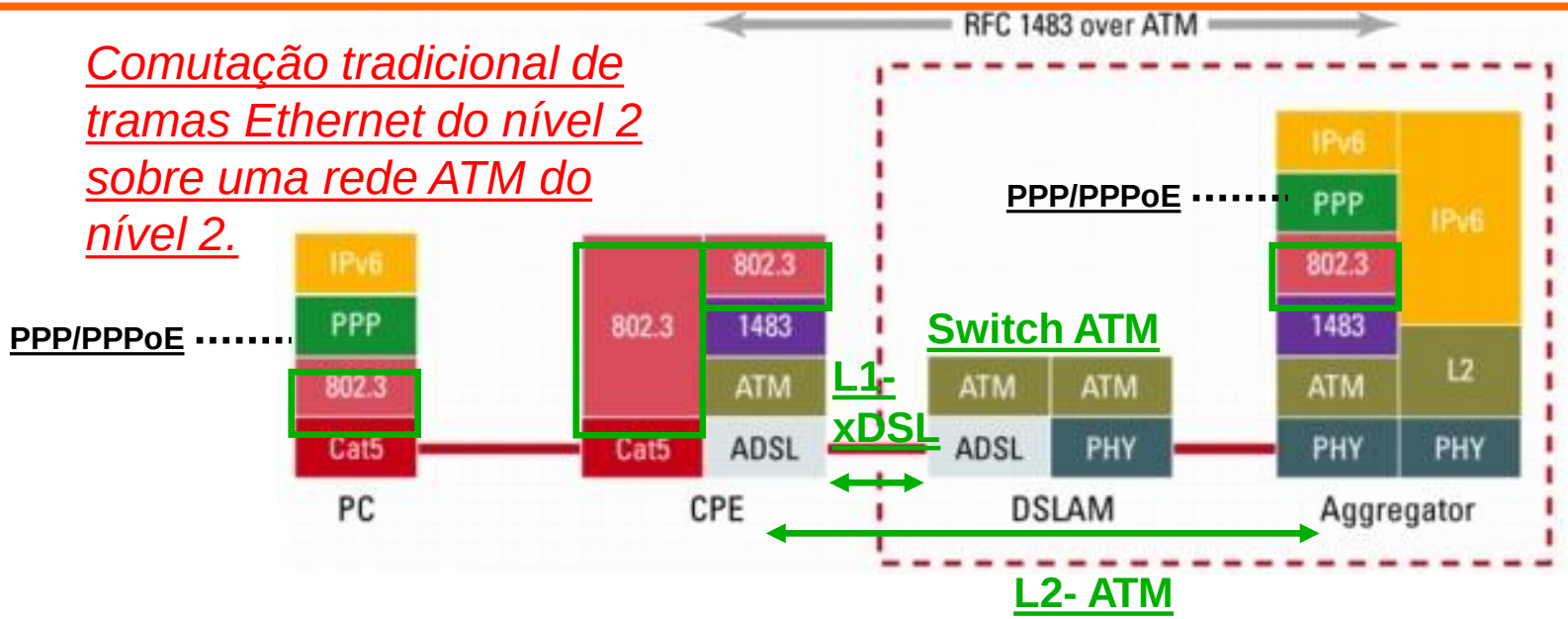
RFC 1483/2684 *Bridged*



- Define o transporte de um ou de múltiplos protocolos sobre um simples circuito virtual ATM.
- Usa xDSL do ATU-R para o ATU-C na camada 1 para enviar e receber células ATM.
- Do DSLAM para o *aggregation router* pode incluir fibra no anel da camada 1 para suportar a a rede baseada em ATM.

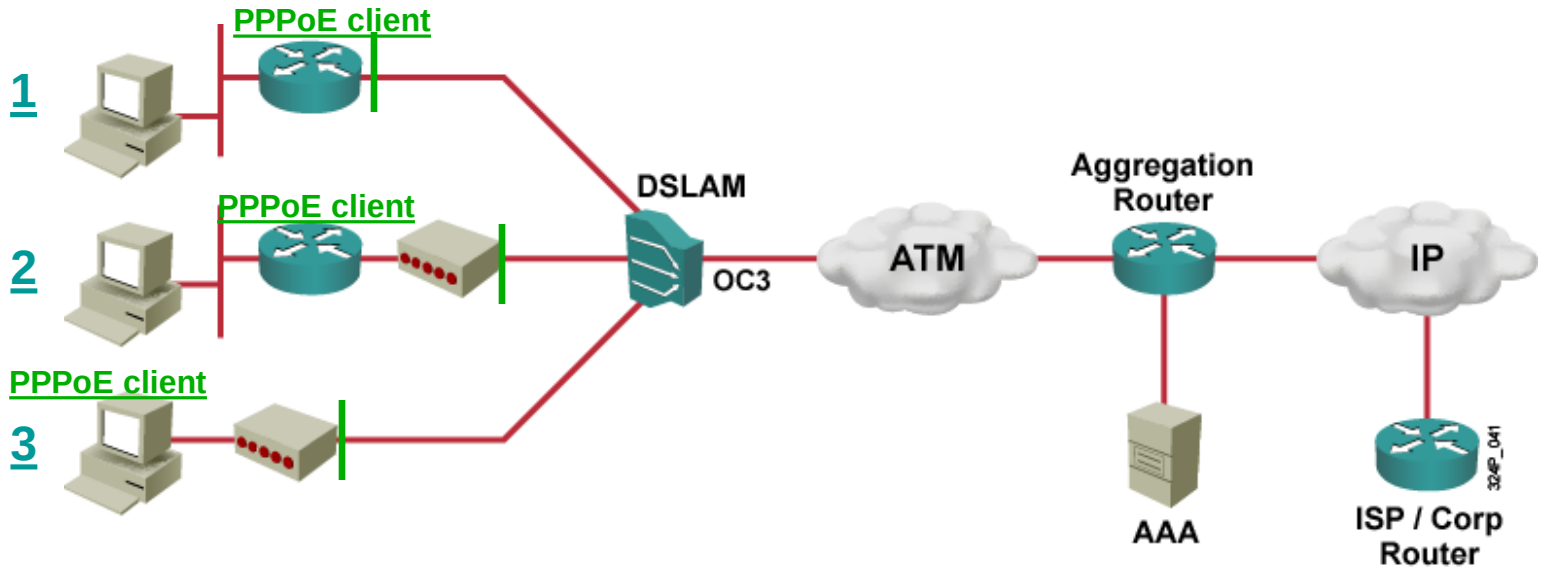
- **Possibilita a criação de um PVC ATM entre o modem xDSL e o *aggregation router*.**

RFC 1483/2684 *Bridged*



- É utilizado um PVC ATM para transportar tramas Ethernet (RFC 1483/2684 *Bridging*).
- O DSLAM essencialmente comporta-se como um *switch* ATM.
- Se o CPE (modem xDSL) tiver uma interface ATM esta ligação ainda usa o xDSL como camada 1.
  - Mas ao nível da camada 2 estabelece um PVC ATM directamente com o *aggregate router* (PPPoA).
- O CPE faz *bridging* sobre ATM das tramas Ethernet entre o PC do utilizador e *aggregation router*. As tramas Ethernet transportam tramas PPP, permitindo isto levar as funcionalidades do PPP até aos PC.

PPPoE – PPP *over* Ethernet

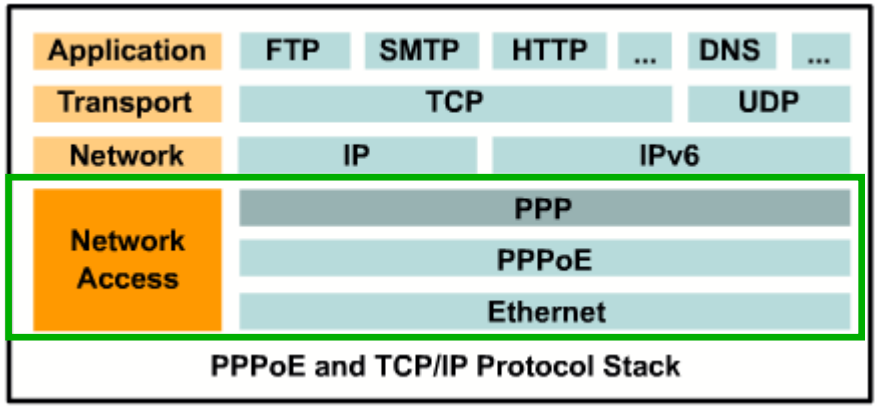


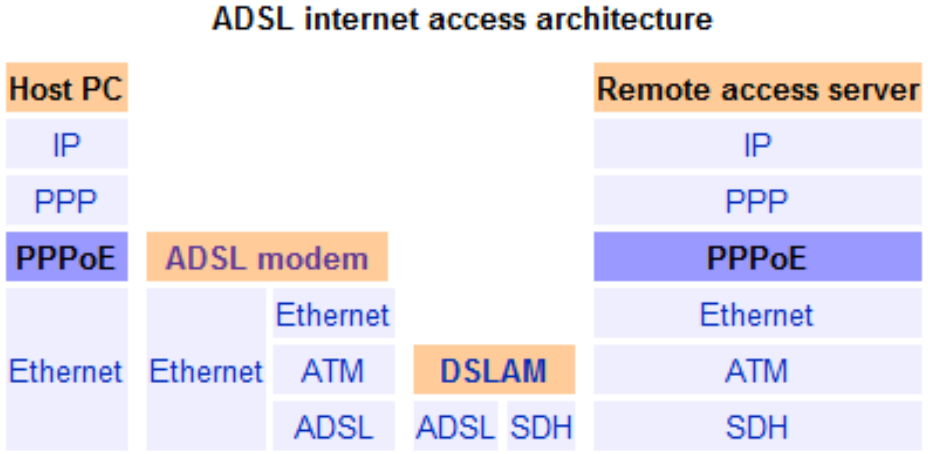
Maneiras de utilizar o xDSL e o PPPoE:

1. *Router* como cliente PPPoE e a terminar a ligação xDSL
2. Modem a terminar a ligação xDSL e o *router* como cliente PPPoE
3. Modem a terminar a ligação xDSL e o PC do utilizador como cliente PPPoE

As funcionalidades do PPP vão até onde em cada caso?

PPPoE





O *Point-to-Point over Ethernet* (**PPPoE**) é um **protocolo para encapsular tramas PPP em tramas Ethernet**.

Oferece as facilidades do PPP como:

- **Autenticação**
- **Compressão**

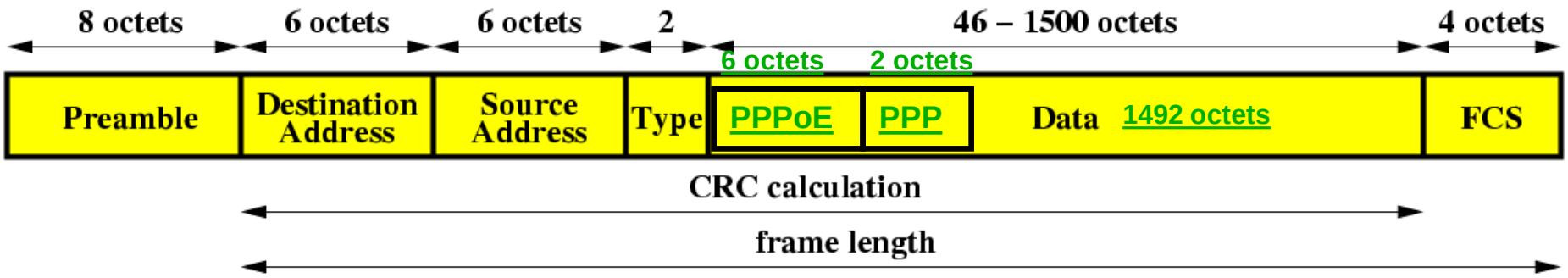
PPPoE

- A atribuição de endereço IP ao cliente PPPoE utiliza o **IP Control Protocol** (**IPCP**)
  - Permite que o dispositivo envie um mensagem IPCP *Configure-Request* para especificar o endereço IP que pretende utilizar ou requisitar que lhe seja fornecido um endereço.
- Utilizado com autenticação ***Password Authentication Protocol*** (**PAP**) ou ***Challenge Handshake Authentication Protocol*** (**CHAP**) ou **outros protocolo sobre *Extensible Authentication Protocol*** (**EAP**).
- O *aggregation router* autentica os utilizadores usando:
  - Base de dados local, ou
  - Servidor AAA (TACACs ou RADIUS)

PPPoE (PPP *over* Ethernet)

- **O protocolo PPP está concebido para ligar ponto a ponto (*data link*).**
- Quando o terminal se encontra numa rede partilhada a ligação ponto a ponto tem de ser estabelecida de outro modo.
  - **Como descobrir um concentrador de acessos?**
    - O protocolo PPPoE estabelece uma túnel entre o terminal e o concentrador de acessos, através do qual, os pacotes de PPP são transportados.
- O protocolo PPPoE tem duas fases distintas (RFC 2516):
  - **Fase de descoberta**: Identificação por parte do cliente do endereço MAC do servidor e estabelecimento de uma sessão PPPoE (SESSION_ID). Esta fase permite ao cliente descobrir todos os concentradores de acesso.
    - A trama Ethernet vai marcada com ETHER_TYPE= **0x8863**.
  - **Fase de sessão PPP**: Fase de transporte de informação PPP através da rede Ethernet entre o cliente e o concentrador de acessos.
    - A trama Ethernet vai marcada com ETHER_TYPE= **0x8864**.

PPPoE e MTU

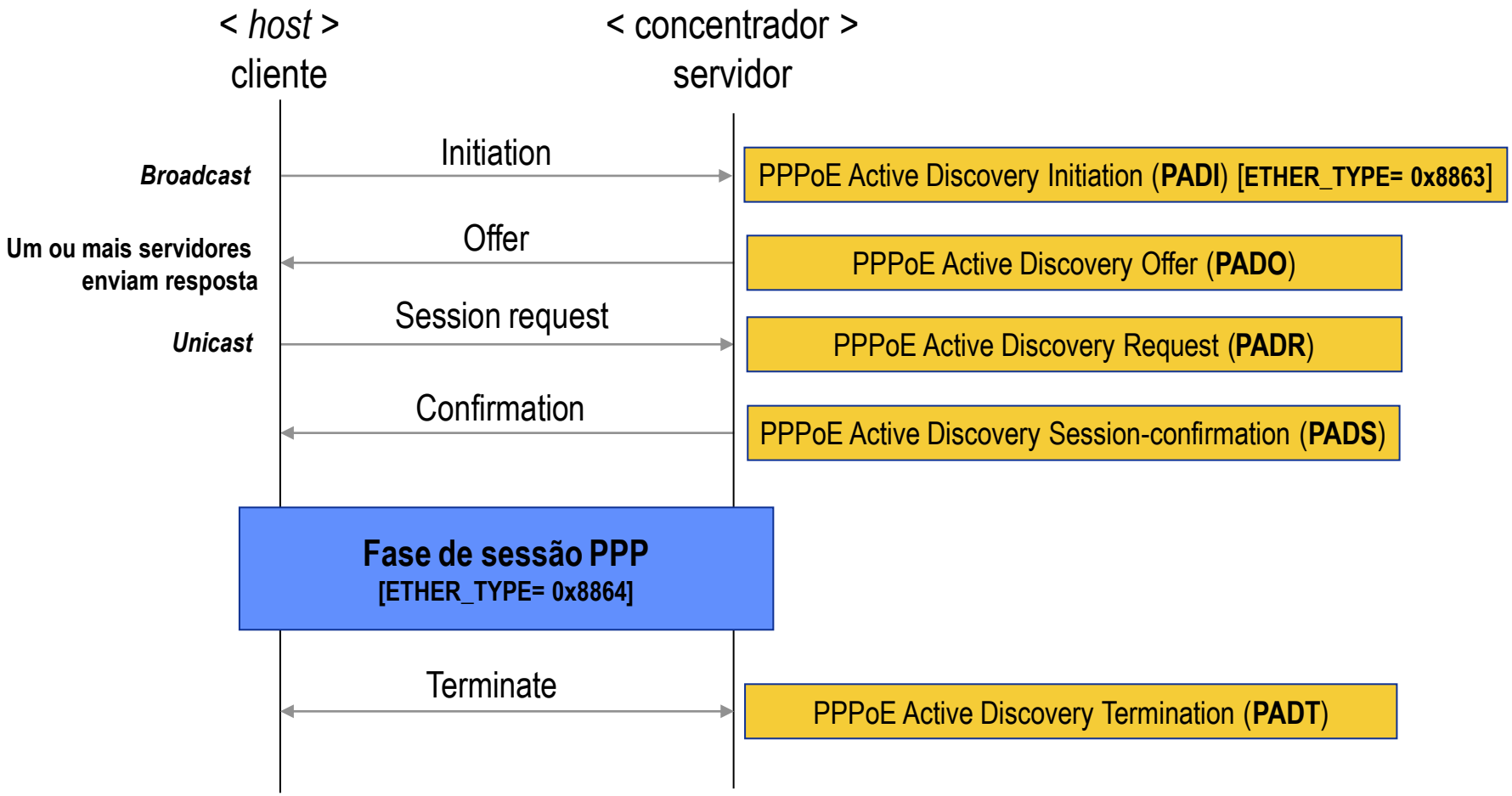


Como especificado no **RFC 2516**, a opção ***Maximum Receive Unit* (MRU)** não deve ser maior que **1492 bytes** porque:

- A Ethernet tem uma dimensão máxima para a carga de 1500 octetos.
- O cabeçalho do PPPoE tem 6 octetos
- O *protocol ID* do PPP tem 2 octetos
- O *Maximum Transmission Unit* (MTU) do PPP não deve exceder (1500 – 6 - 2) **1492 bytes**.

PPPoE: Fases de descoberta e de sessão

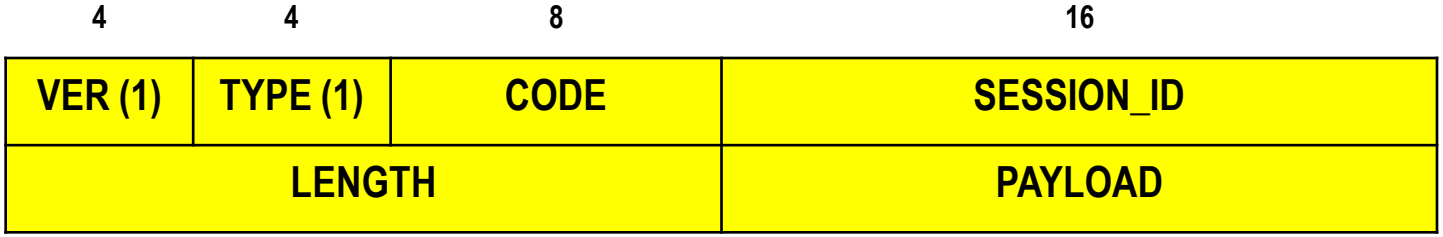
O PPPoE utiliza um *4-way handshake* para o estabelecimento de uma sessão.



PPPoE: Tipos de mensagens

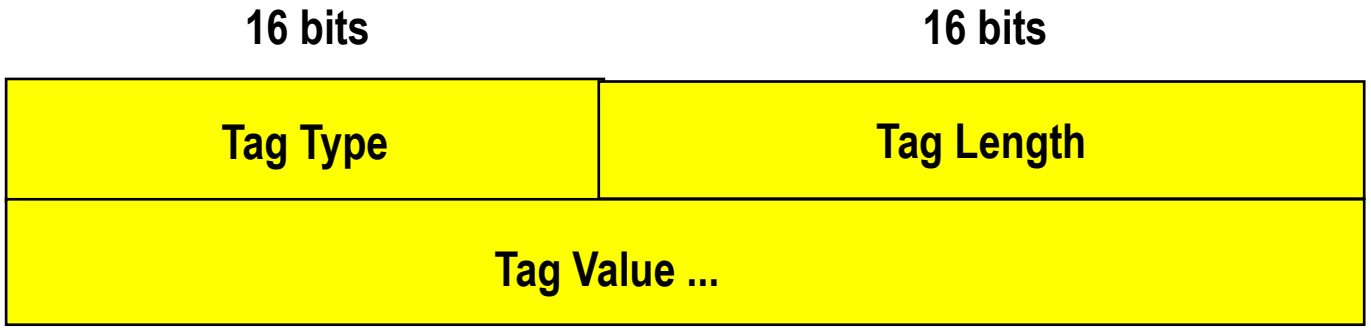
- ***PPPoE Active Discovery Initiation* (PADI)**: Enviado pelo cliente para descobrir um servidor de PPPoE através de uma trama Ethernet de *broadcast*.
- ***PPPoE Active Discovery Offer* (PADO)**: Enviado pelos vários servidores para o cliente indicando a oferta do serviço PPPoE.
- ***PPPoE Active Discovery Request* (PADR)**: Resposta do cliente a um servidor pedindo o estabelecimento da ligação PPPoE.
- ***PPPoE Active Discovery Session-Confirmation* (PADS)**: Confirmação do servidor **com um SESSION_ID gerado para aquela ligação PPPoE**.
- ***PPPoE Active Discovery Termination* (PADT)**: Para terminar a ligação PPPoE.

Mensagem PPPoE



PPPoE: Fase de descoberta

- Nesta fase o cliente descobre, utilizando ***broadcast***, o servidor de acessos criando uma sessão identificada pelo seu endereço MAC e pelo MAC do concentrador de acessos e pelo SESSION_ID. É o concentrador de acessos que define o valor do SESSION_ID no pacote PADS.
- O campo ETHER_TYPE das tramas Ethernet que transportam pacotes PPPoE da fase de descoberta é colocado a **0x8863**.
- Nesta fase os pacotes PPPoE transportam como carga (*payload*) *tags* no formato **TLV (*Type*, *Length*, *Value*)**



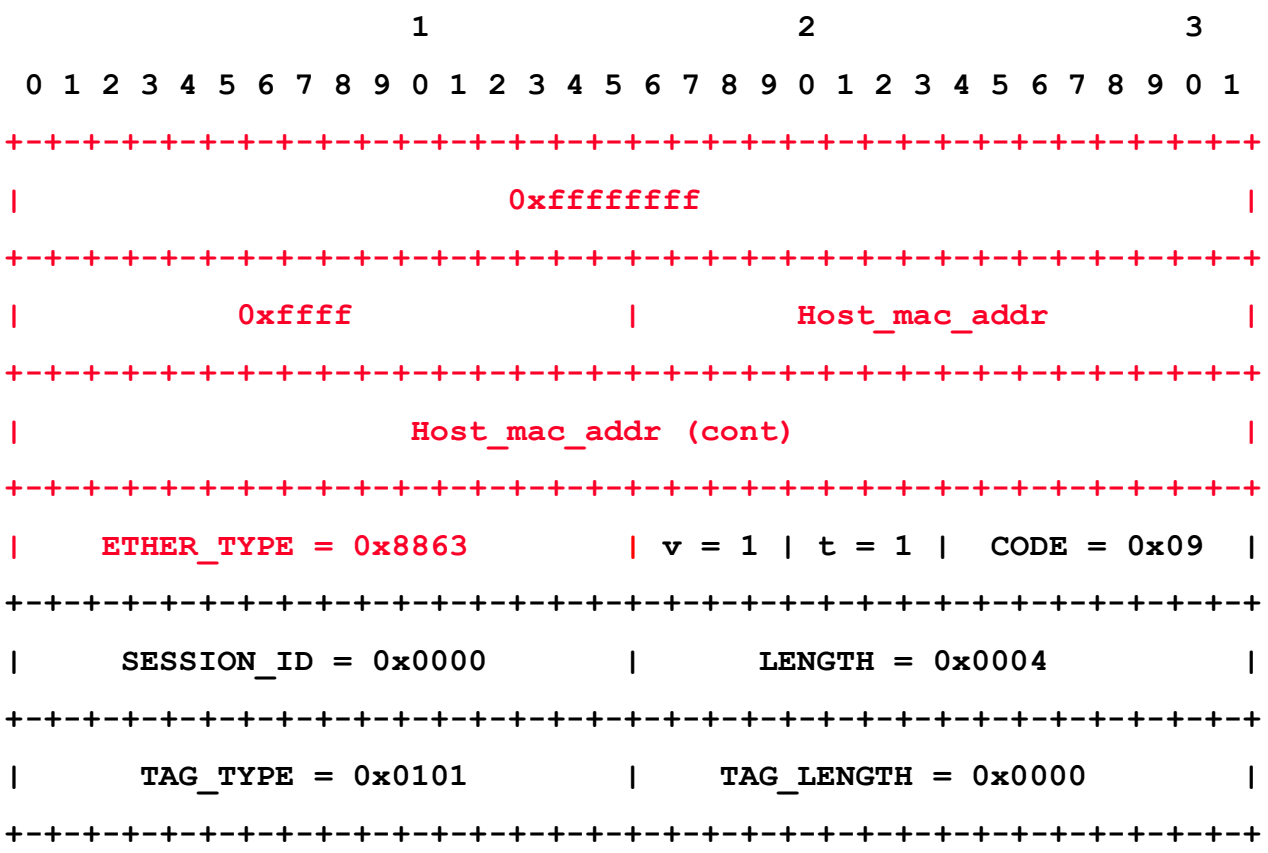
Dimensão variável

PPPoE: Tipos de *tags* e respectivos valores

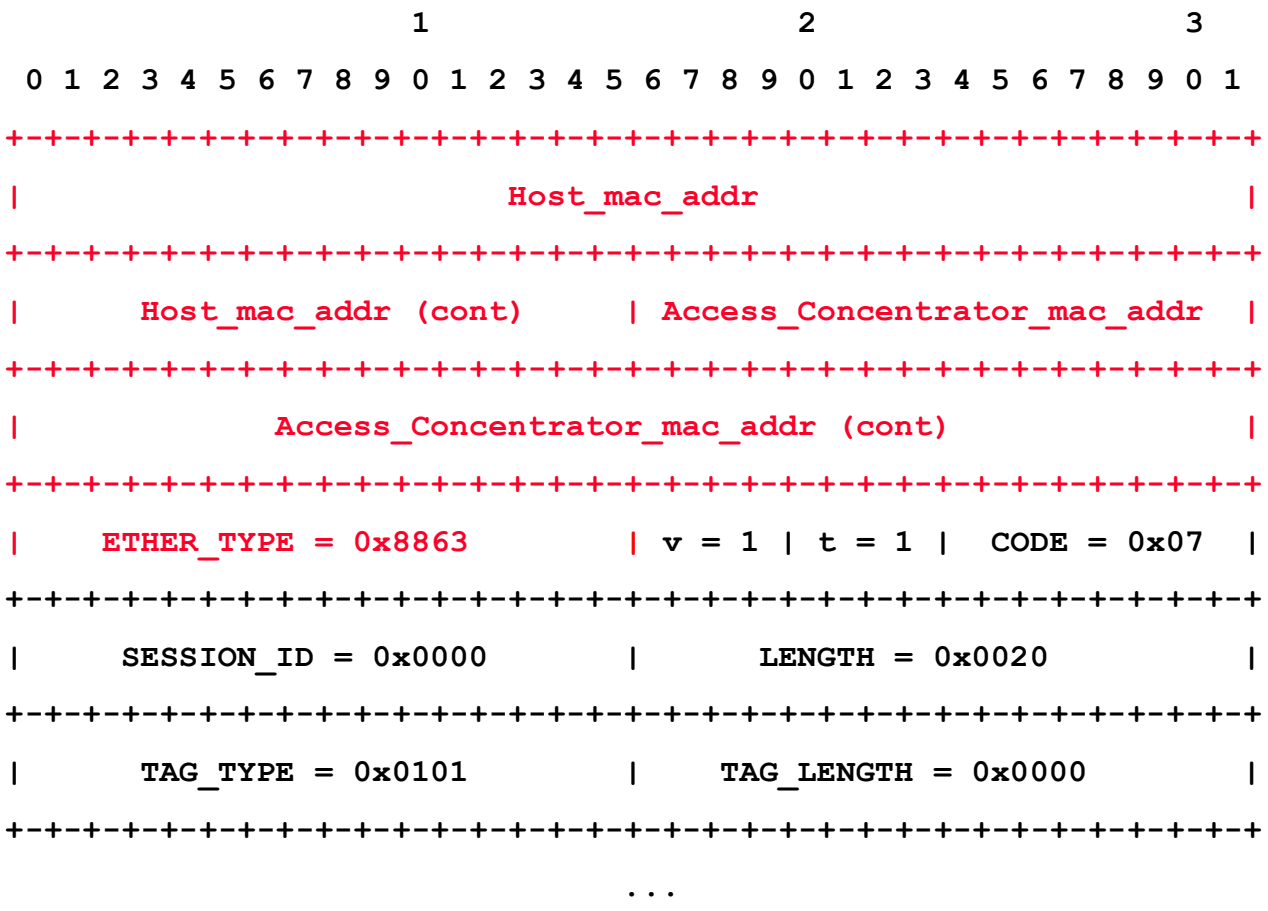
- 0x0000 End-Of-List — Última *tag* do pacote PPPoE
- 0x0101 Service-Name — Nome do serviço pretendido. Nulo => qq
- 0x0102 AC-Name — Identificação do concentrador de acessos (AC)
- 0x0103 Host-Uniq — Utilizado pelo *host* para identificar o AC
- 0x0104 AC-Cookie — Defesa contra alguns ataques DoS
- 0x0105 Vendor-Specific — Específica do vendedor. A evitar.
- 0x0110 Relay-Session-Id — A utilizar pelos *relay agent*
- 0x0201 Service-Name-Error — Erro no Service-name
- 0x0202 AC-System-Error — Erro no concentrador de acessos
- 0x0203 Generic-Error — Erro genérico

- O *tag length* e o *tag value* variam conforme o tipo de *tag.*

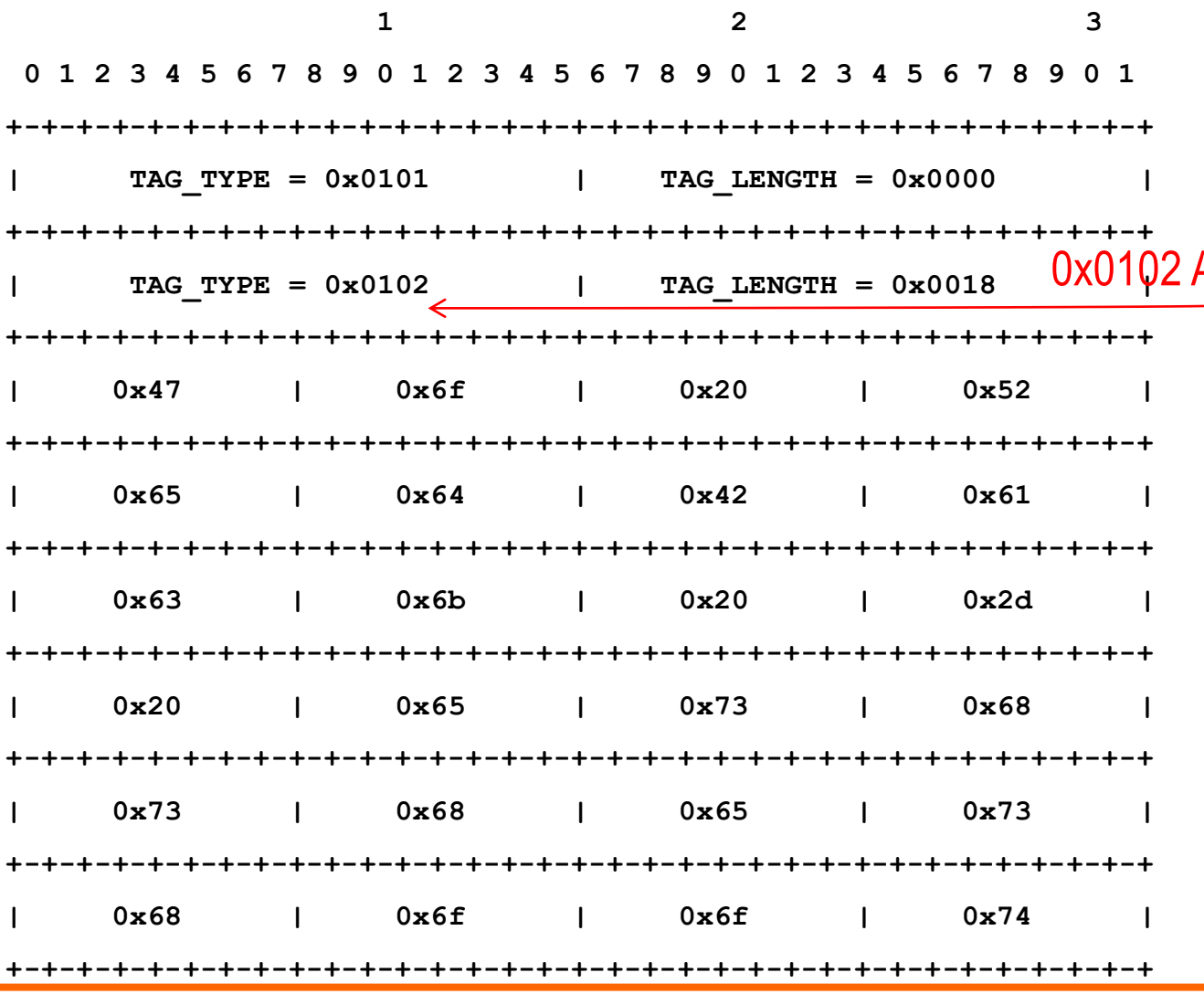
PPPoE: Trama Ethernet com a mensagem PADI



PPPoE: Trama Ethernet com a mensagem PADO (1)



PPPoE: Pacote PADO (2)

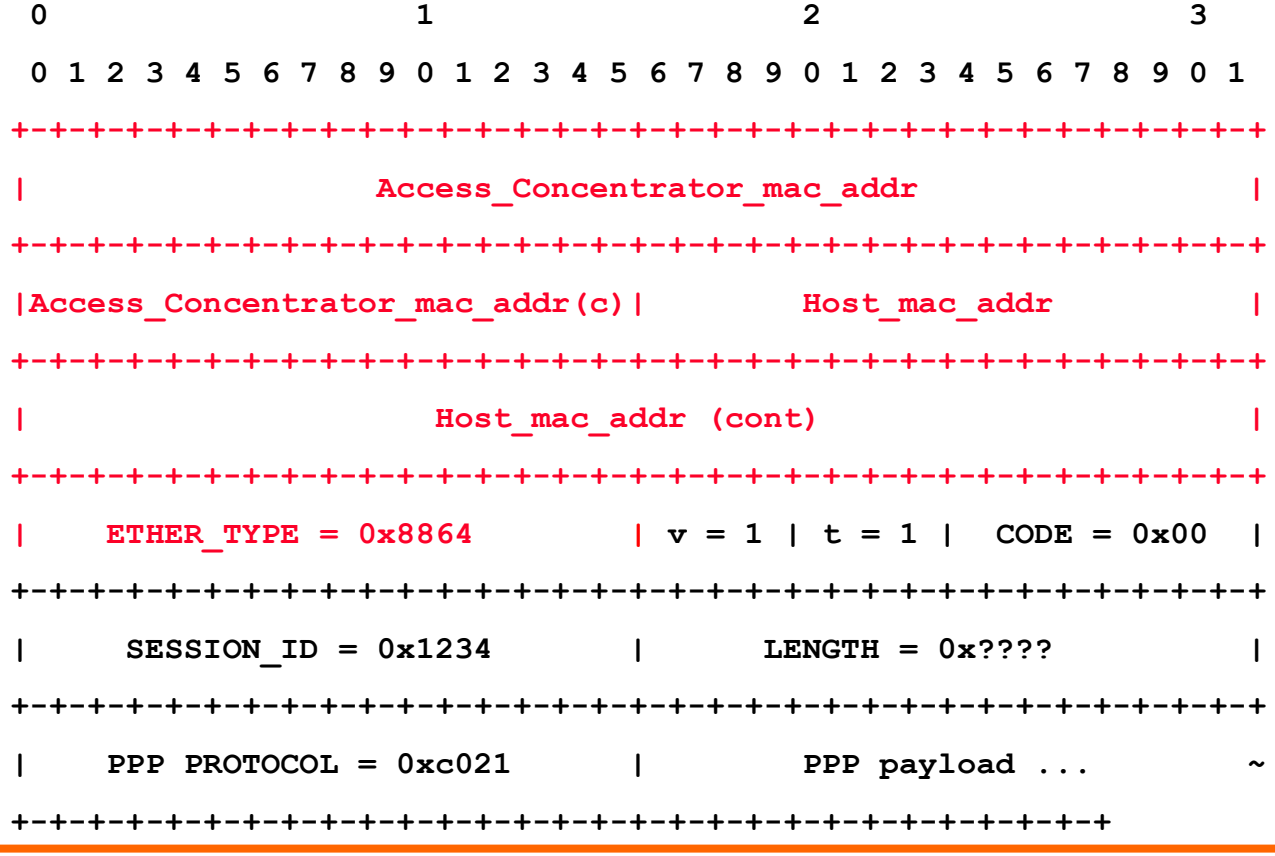


PPPoE: Fase de sessão

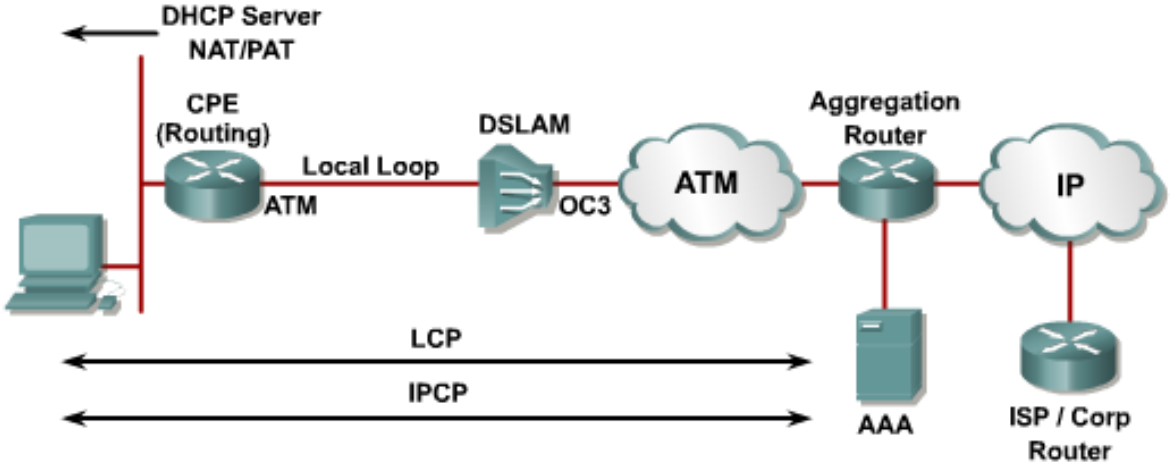
- Uma vez iniciada a sessão PPPoE os dados PPP são enviados como em qualquer encapsulação PPP.
- Todas as tramas Ethernet são *unicast*.
- O campo ETHER_TYPE é colocado a 0x8864.
- O campo *code* PPPoE deve ser 0x00.
- O SESSION_ID atribuído na fase de descoberta NÃO DEVE mudar durante toda a sessão PPPoE.
- O MTU PPP deve ser menor ou igual a 1492 bytes.
- A carga PPPoE contém uma trama PPP. A trama PPP começa com o *Protocol_ID*. Não inclui o último campo de *flags* (dado não necessitar delas de sincronismo de trama).

PPPoE: Fase de sessão – Exemplo

Pacote LCP PPP: O valor no protocolo PPP é mostrado (0xc021) mas a carga é deixada à imaginação do leitor. Este pacote é enviado do *host* para o concentrador de acessos (AC).

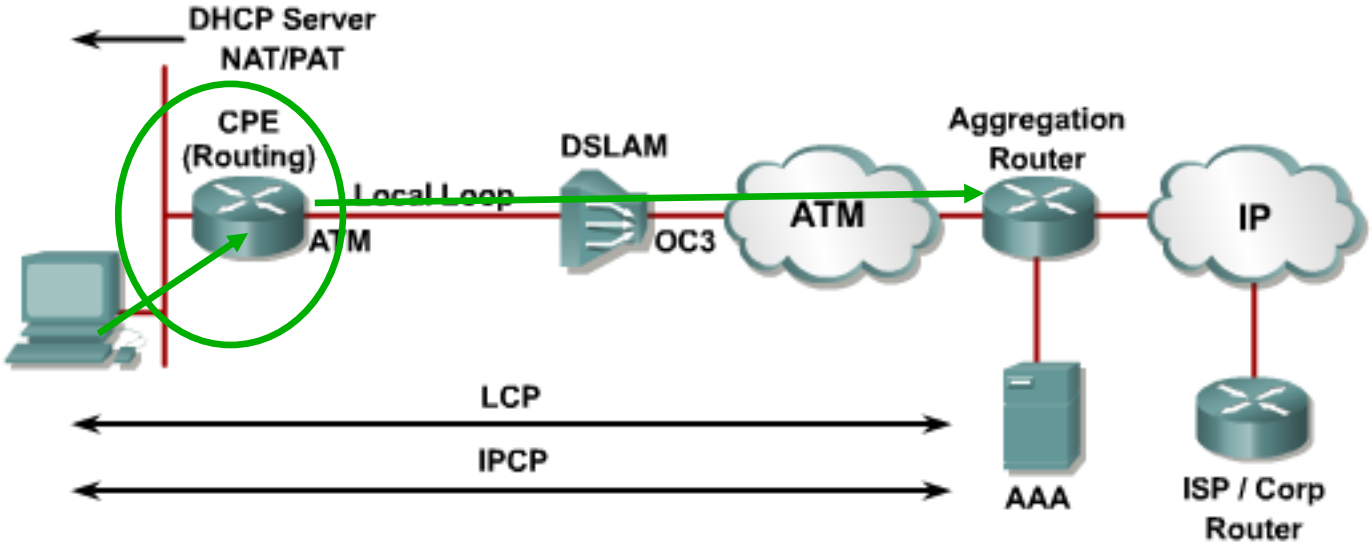


PPP over ATM (PPPoA)



- O PPPoA é utilizado principalmente em redes de cabo e xDSL.
- Fornece:
  - Autenticação, Integridade e "Confidencalidade" de alguns parametros pré-definidos
  - Compressão
- Tem um *overhead* um pouco maior que o PPPoE
- **O PPPoA tem a vantagem sobre o PPPoE de evitar a necessidade de ter um MTU menor do que o da Ethernet.**
- O PPPoA é uma solução encaminhável (nível 3), ao contrário do RFC 1483 *Bridged* e do PPPoE. Porquê?

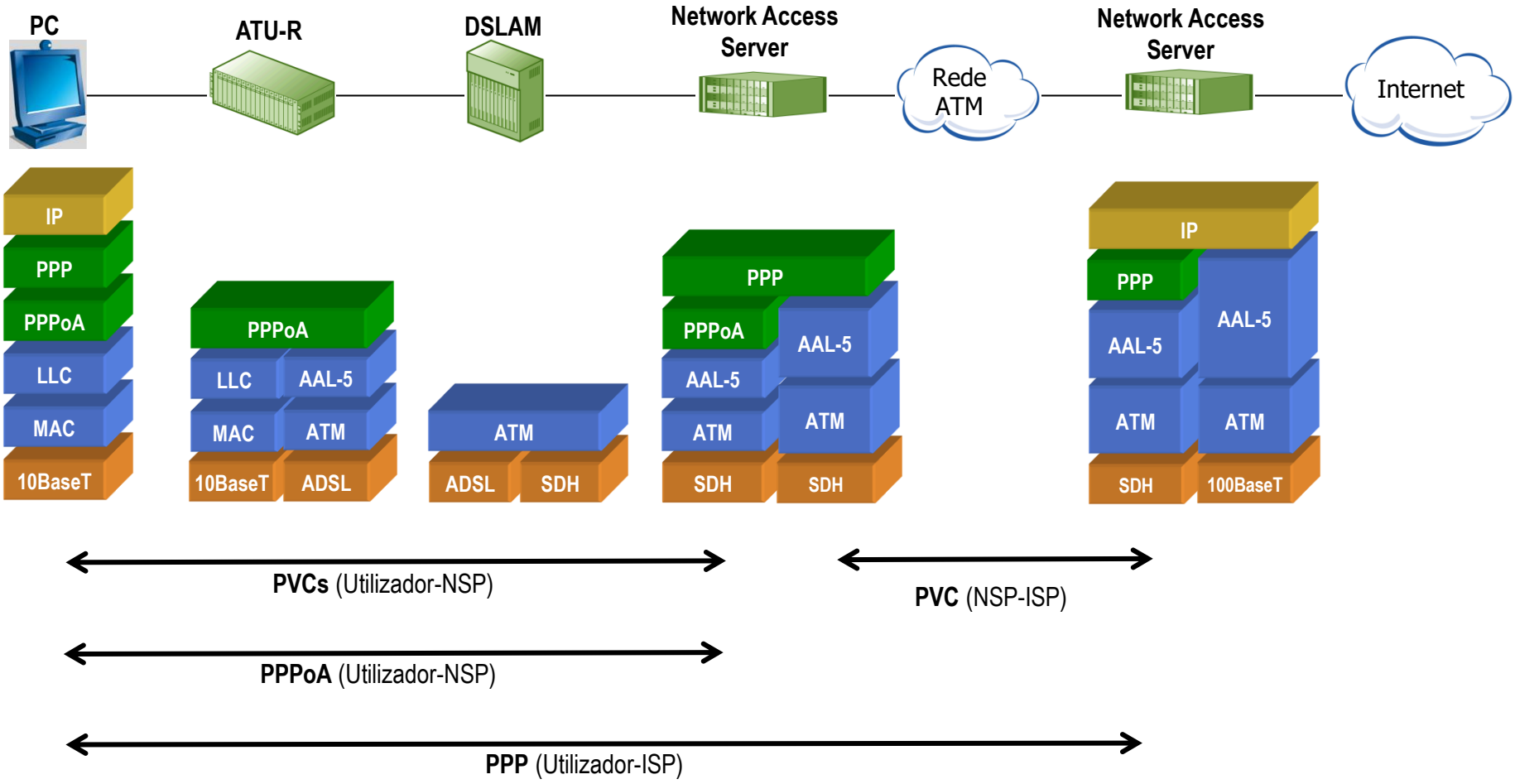
PPPoA



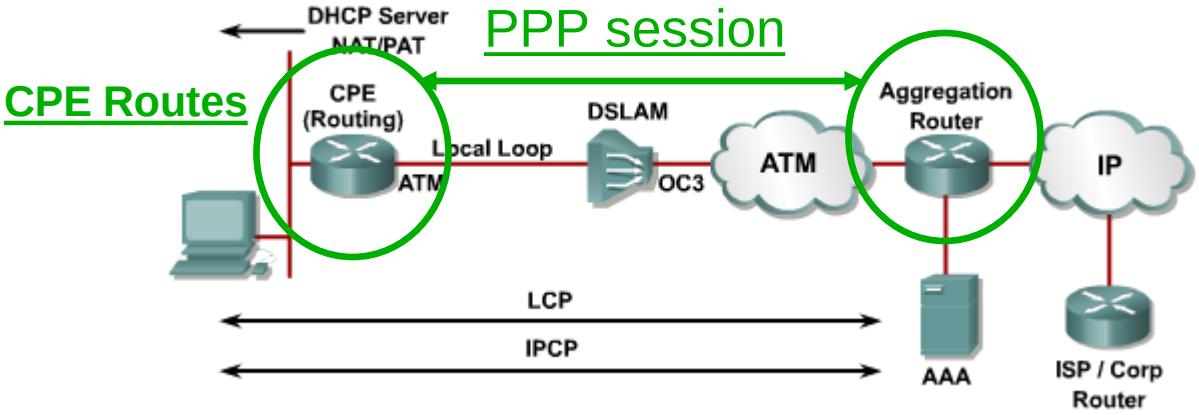
- Com o PPPoA o CPE encaminha (nível 3) os pacotes do PC do utilizador final sobre ATM para um *aggregation router.*
- Ao contrário do PPPoE, o PPPoA não requer no PC cliente software PPPoE. A terminação é no CPE.

Caso 3: Sessão PPP sobre PPPoA

Network Service Provider (NSP) com rede ATM

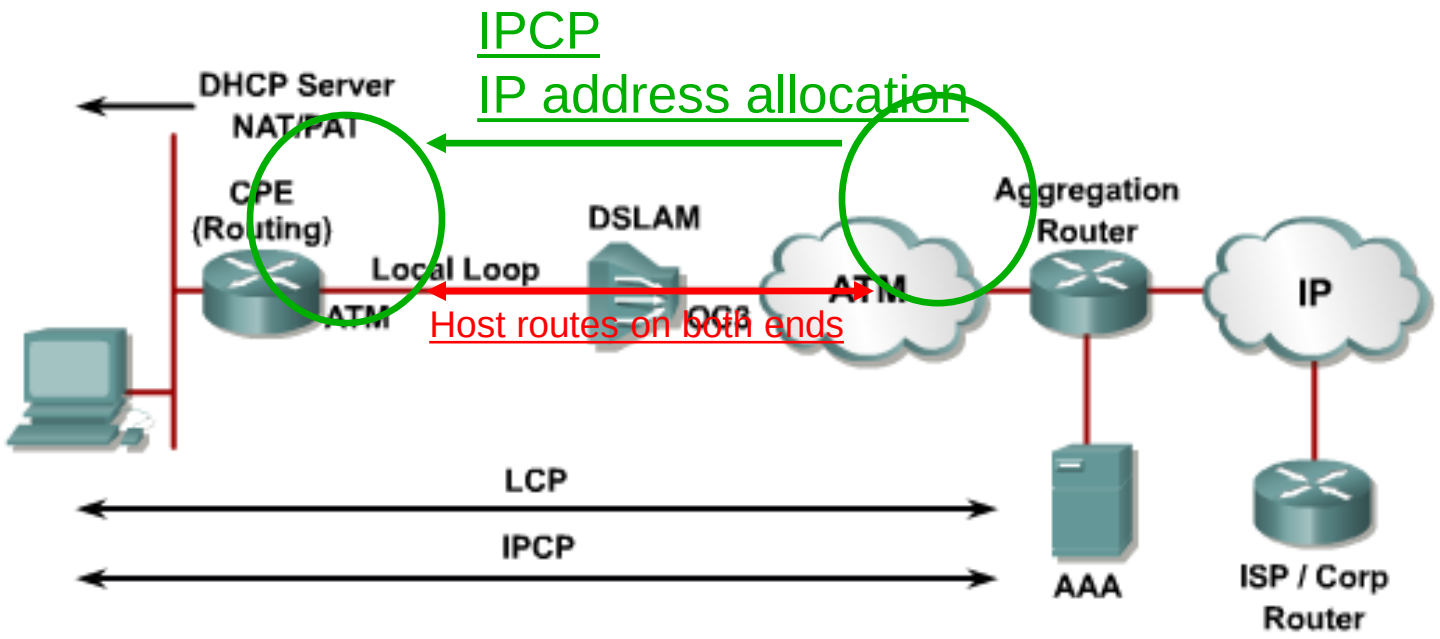


PPPoA



- A sessão PPP é estabelecida entre o CPE e o *aggregation router*.
  - O CPE deve possuir um nome de utilizador e uma *password* PPP configurados para autenticação perante o *aggregation router* onde termina a sessão PPP iniciada no CPE.
  - O *aggregation router* que autentica os utilizadores pode utilizar uma base de dados local no *aggregation router* ou um servidor AAA.
  - PAP, CHAP ou outro protocolo de autenticação suportado sobre EAP.

PPPoA



- A seguir tem lugar a negociação **IPCP** e o endereço IP é atribuído ao CPE.
- O *aggregation router* deve atribuir apenas um endereço IP ao CPE
  - O CPE pode ser configurado como servidor DHCP
  - O CPE pode usar NAT e PAT para suportar múltiplos clientes na rede servida pelo CPE.

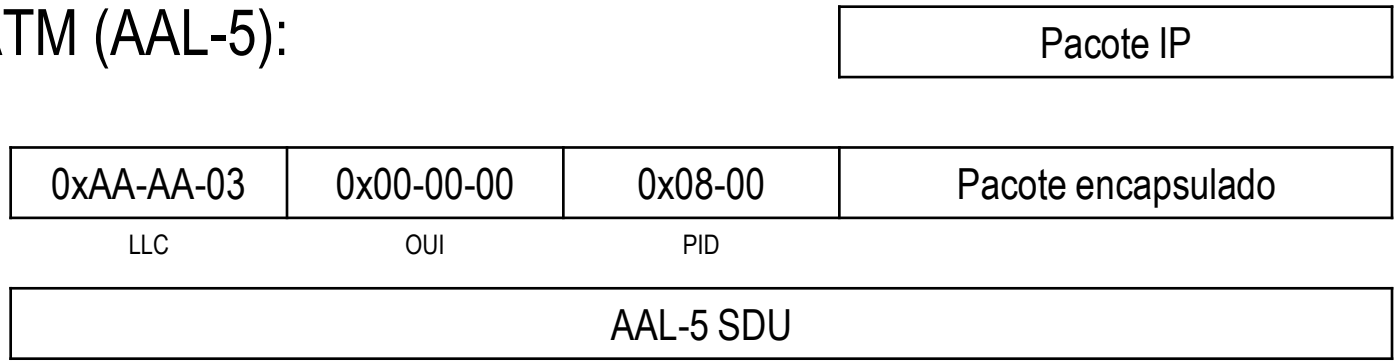
Multi-protocolos sobre AAL-5 (RFC 1483)

- Este modelo foi criado no IETF.
  - ATM é considerado como um protocolo da camada 2.
  - IP corre sobre a infra-estrutura ATM sem modificações nos *routers* e nos sistemas terminais.
  - A estrutura clássica das redes IP é preservada.
  - Encaminhamento/endereçamento IP e ATM são independentes.

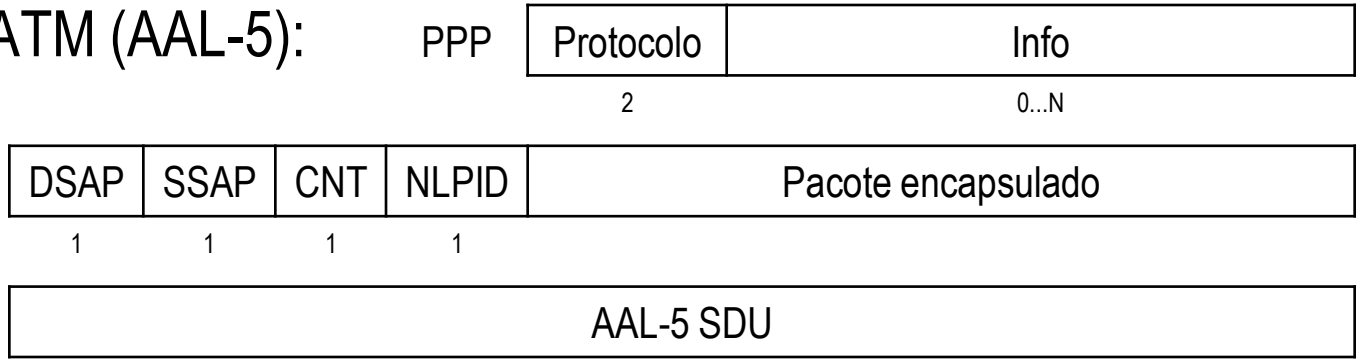
- Para correr redes IP sobre ATM levantam-se os seguintes problemas:
  - Optimização do encaminhamento
  - Resolução de endereços (RFC 1577)
  - *Multicasting*
  - Encapsulamento dos pacotes IP (RFC 1483 – Multi-protocolos sobre AAL-5)

Encapsulamento (RFC 1483)

- IP sobre ATM (AAL-5):

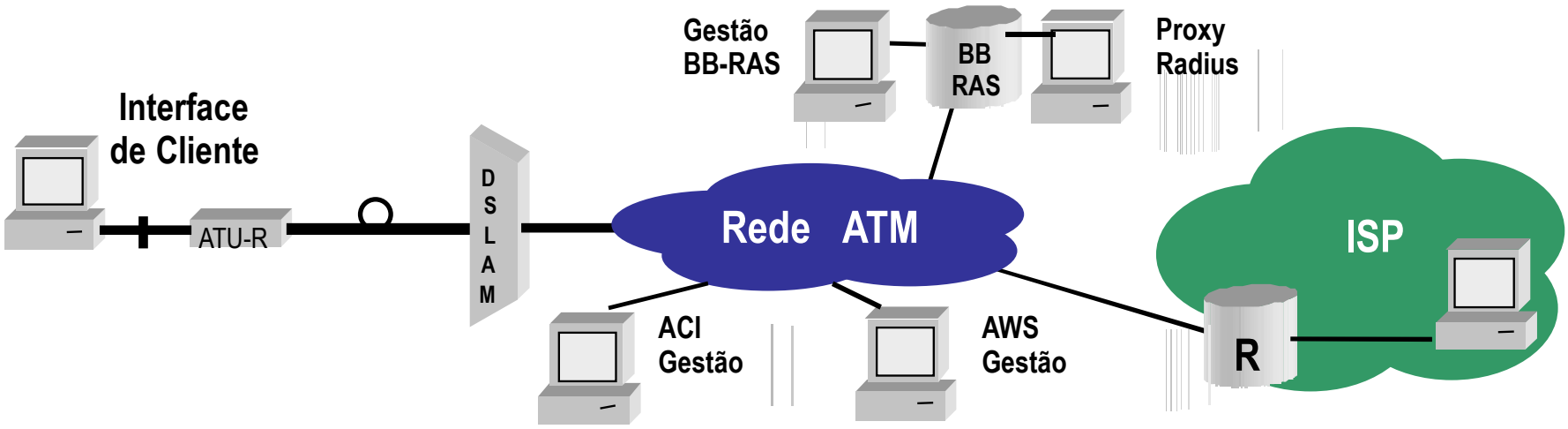


- PPP sobre ATM (AAL-5):



Exemplo: Arquitectura para acesso ADSL

- O portal de um operador é constituído por uma intranet virtual de vários servidores.
- Para o cliente são usados os modems ADSL.
- As interfaces para os ISPs são definidos de acordo com a oferta comercial de circuitos ATM do Operador.

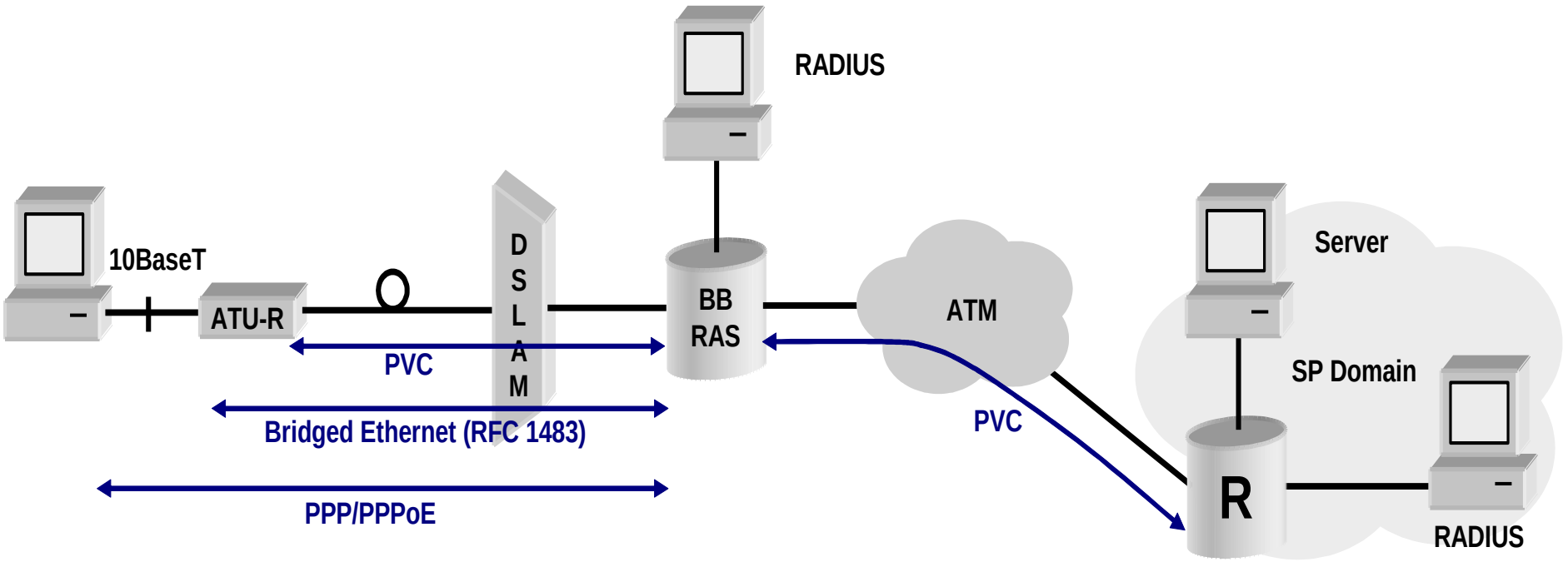


Acesso para os ISP (exemplos)

Designação genérica	IMA	E3	STM-1
Débito da Interface	N x 2,048 Mbps(N=2,3,4)	34,368 Mbps	155,520 Mbps
Interface Física	BNC 75 Ohm Coax	BNC 75 Ohm Coax	E2000 óptico monomodo short-haul (S.1.1)
Débito Máximo Disponível	7,616 Mbit/s ou 17.961 células/s	30,528 Mbit/s ou 72.000 células/s	149,760 Mbit/s ou 353.207 células/s
Nível Físico	G.703 do ITU-T	G.703 do ITU-T	G.957 do ITU-T
Estrutura da trama	IMA 1.0 do ATM Forum G.832 do ITU-T	G.832 do ITU-T	I.432 do ITU-T
Mapeamento de Células ATM	G.804 do ITU-T	G.804 do ITU-T	I.432 do ITU-T
Traffic Shaping	I.371 do ITU-T ou TM 4.0 do ATM Forum	I.371 do ITU-T ou TM 4.0 do ATM Forum	I.371 do ITU-T ou TM 4.0 do ATM Forum
Traffic Policing	I.371 do ITU-T ou TM 4.0 do ATM Forum	I.371 do ITU-T ou TM 4.0 do ATM Forum	I.371 do ITU-T ou TM 4.0 do ATM Forum

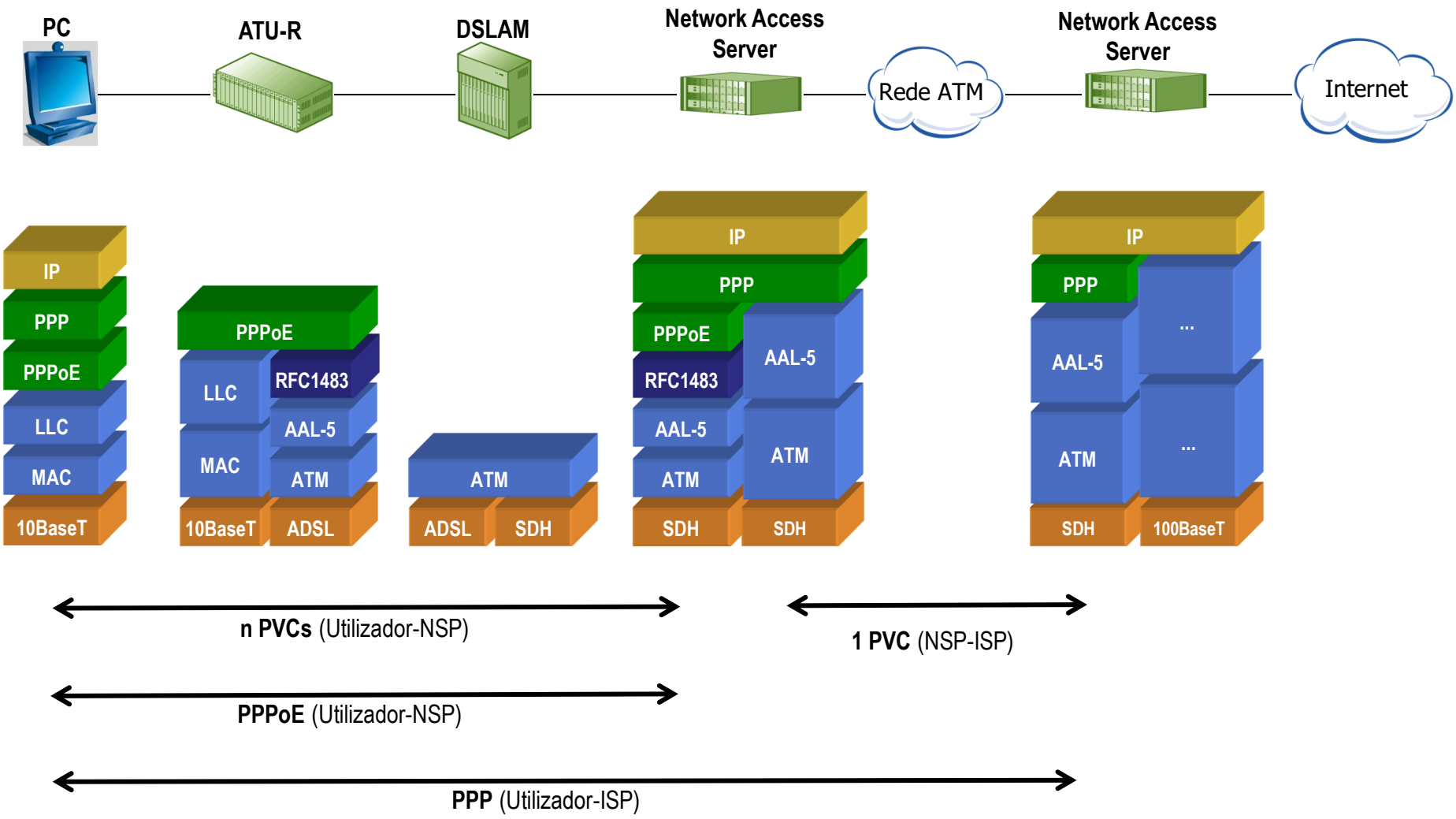
Caso 1: Sessão PPP sobre PPPoE

Network Service Provider com rede ATM



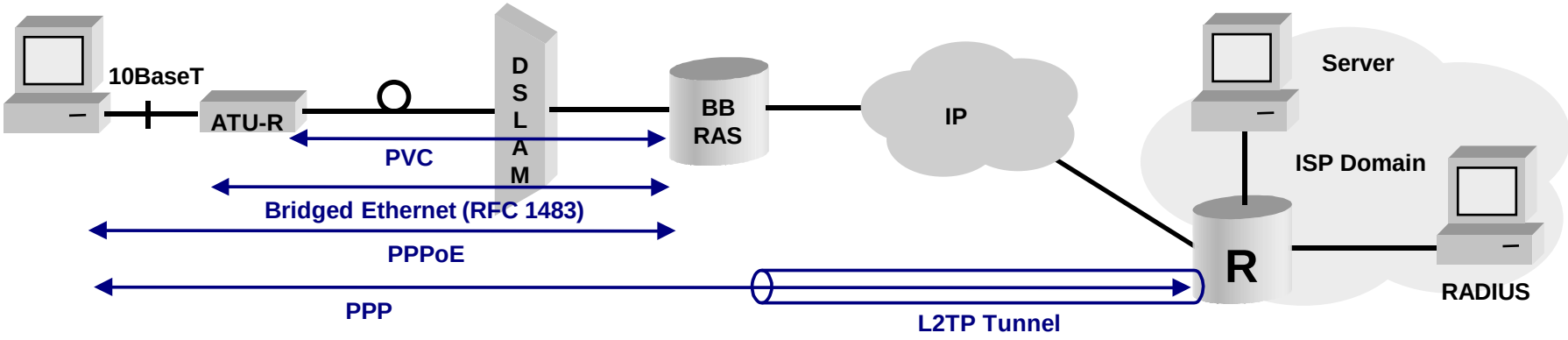
Caso 1: Sessão PPP sobre PPPoE

Network Service Provider com rede ATM



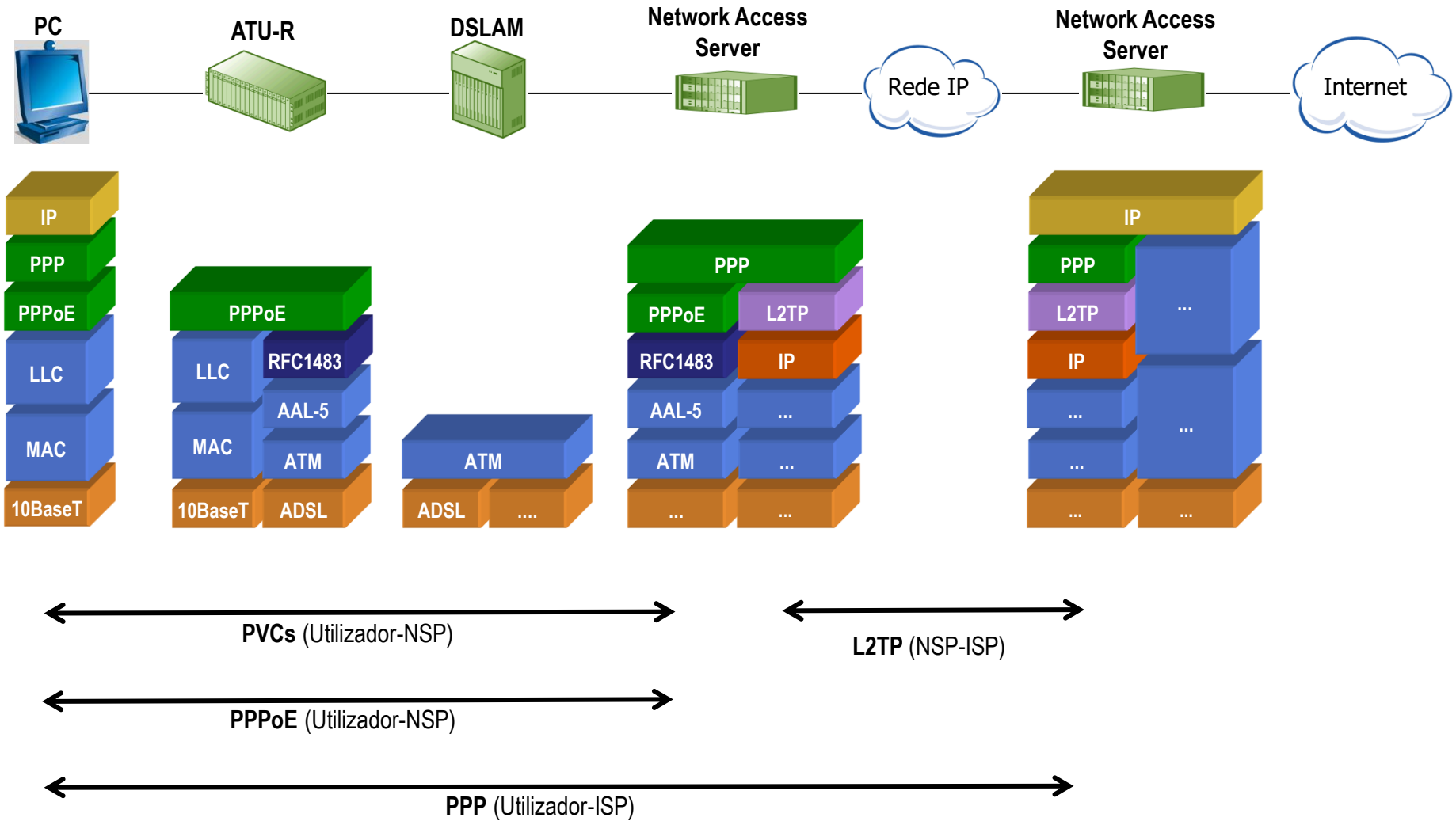
Caso 2: Sessão PPP sobre PPPoE

Network Service Provider com rede IP



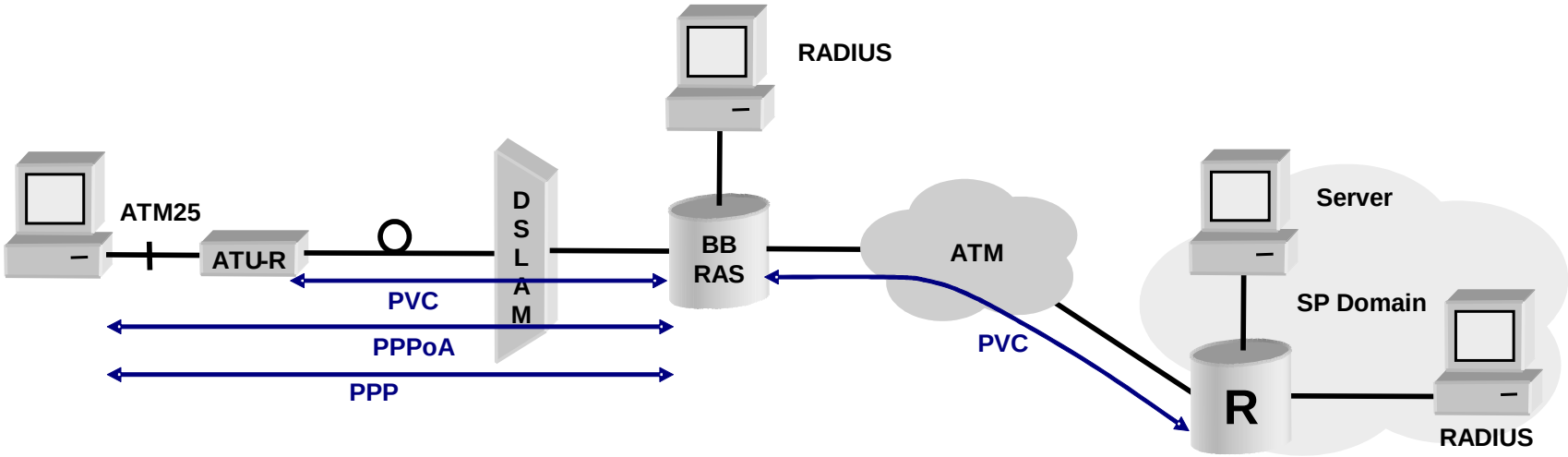
Caso 2: Sessão PPP sobre PPPoE

Network Service Provider com rede IP



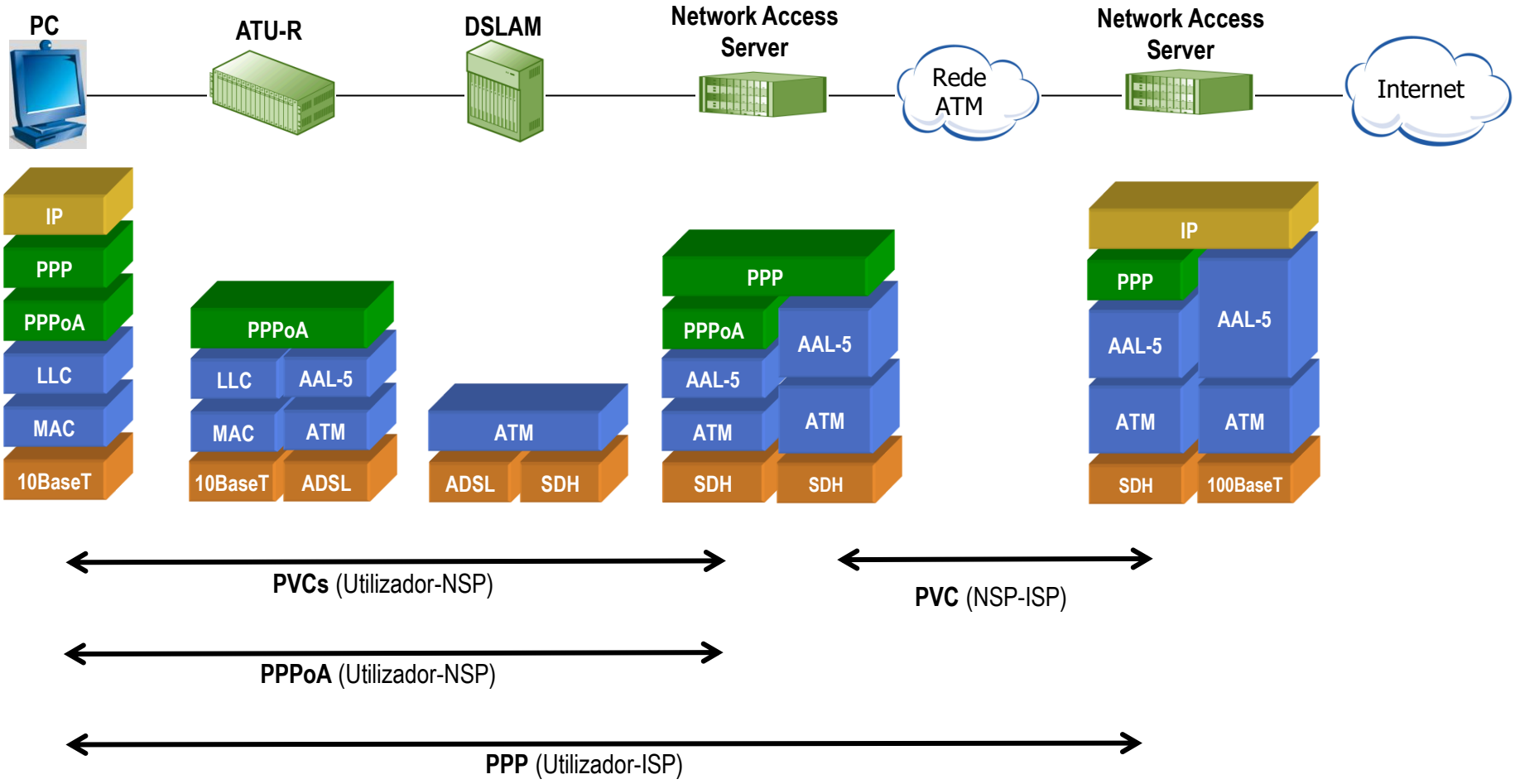
Caso 3: Sessão PPP sobre PPPoA

Network Service Provider com rede ATM



Caso 3: Sessão PPP sobre PPPoA

Network Service Provider com rede ATM



Arquitectura da rede ADSL de um operador