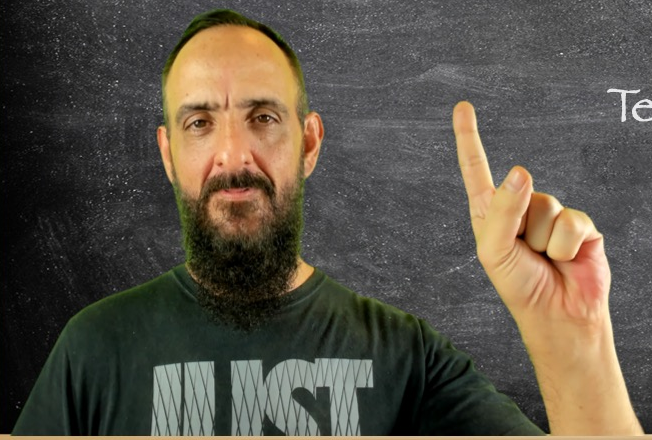
IMPLANTAÇÃO DE SOLUÇÕES BNG-BRAS PARA INTERNET BANDA-LARGA COM PPPOE E IPOE



Leonardo Furtado
Tech Talk | Redes & Telecom

nic.br
Núcleo de Informação e Coordenação do Ponto BR

https://cursoseventos.nic.br/
Semana de Capacitação On-line
27 a 30 de setembro de 2021

AGENDA

- Introdução
- Sobre o palestrante
- Modalidades de produtos de Internet para consumidores
- O que são soluções de BNG
- A arquitetura de uma solução BNG típica
- Dissecando os componentes de uma solução BNG típica

X

AGENDA

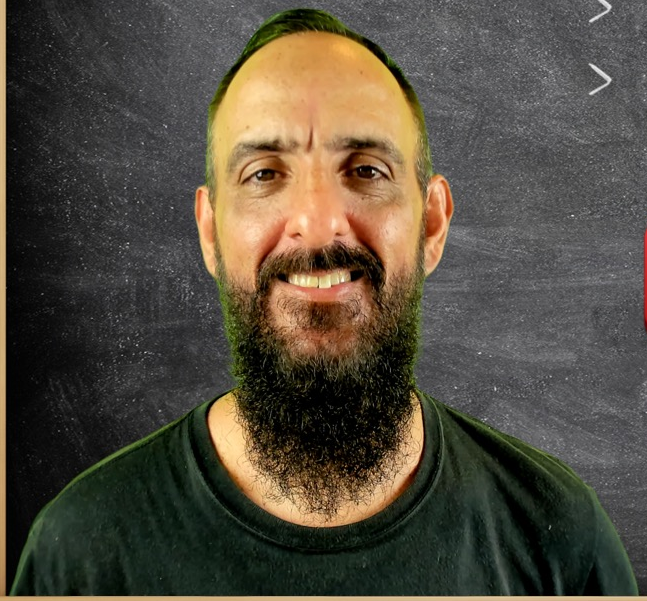
- Como funciona o PPPoE
- Como funciona o IPoE
- Como funciona o RADIUS
- Diferenças entre os cenários PPPoE e IPoE
- Como é feita uma integração básica entre BNG e RADIUS
- Estudo de caso: demonstração de uma solução BNG em pilha dupla!

SOBRE O PALESTRANTE

- Sou Arquiteto de Soluções, Engenheiro de Redes, e Instrutor e Facilitador.
- Em adição, atuo pelo High Touch Delivery Learning Services / Cisco Advanced Services' Education, lecionando clientes Cisco em diversos países sobre as tecnologias e plataformas determinantes para as arquiteturas Carrier Ethernet e NGN de última geração.
- Possuo formação em Ciência da Computação e 26 anos de experiência em diversos segmentos de mercado e verticais tecnológicas, de routing & switching, wireless, segurança e colaboração, até Service Providers e Data Centers, sendo estes dois últimos meus segmentos de maior especialidade e interesse.
- Atuação em empresas com perfil de missão crítica, tais como a New York Stock Exchange (NYSE/Euronext), instituições financeiras e operadoras de telecomunicações.

X

SOBRE O PALESTRANTE

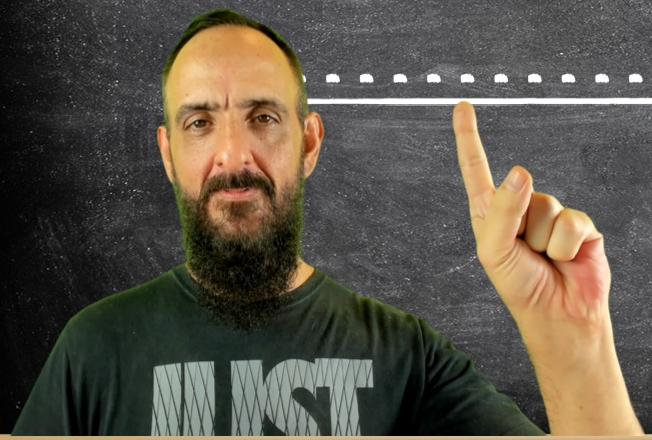


- Mantenho uma comunidade online pela plataforma do Discord.
- Reunindo quase 4.000 aficcionados pelos temas de redes e telecom.
- Mantenho um canal no YouTube contendo dicas, minicursos, tutoriais, e eventos ao vivo com especialistas renomados!

/LeonardoFurtadoNYC

X

COMO FUNCIONA O PPPOE?



Voltando no tempo: como surgiram os protocolos de comunicação ponto-a-ponto

- A expansão do uso de computadores pessoais no início dos anos 80...
- ... e a necessidade pelo compartilhamento de serviços de arquivos e de impressão...
- ... mesmo que ainda por métodos rudimentares de comunicação...
- ... impulsionou o desenvolvimento de protocolos, programas e procedimentos para a troca destes serviços sobre uma *conexão serial*.

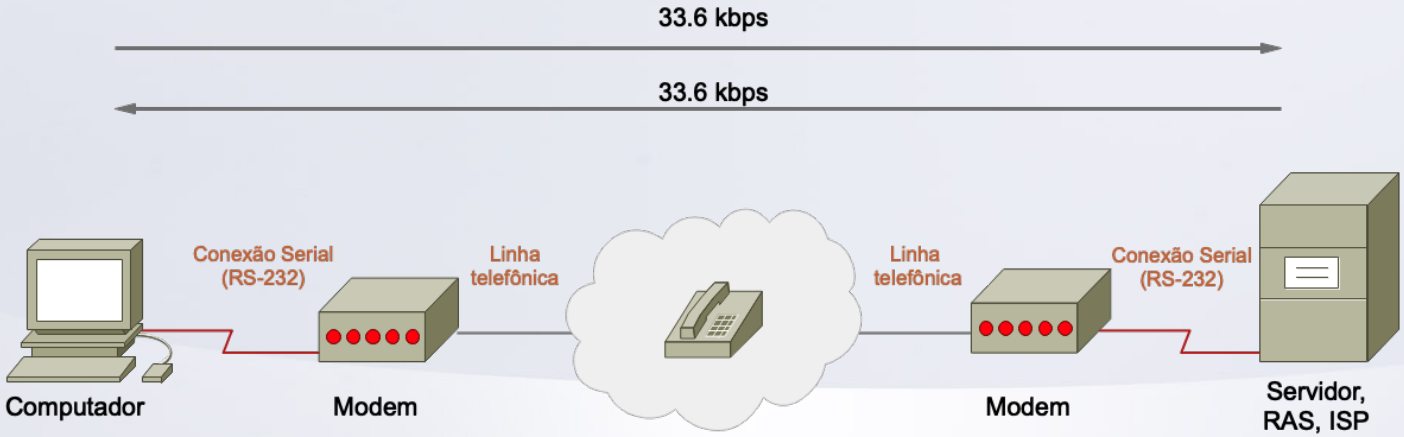
Voltando no tempo: como surgiu os protocolos para comunicação ponto-a-ponto (cont.)

- Algumas destas tecnologias contemplavam:
  - Kermit (Columbia University)
  - Xmodem, Ymodem, Zmodem
- A primeira rede baseada em pacotes foi a ARPAnet (DARPA), sobre circuitos dedicados.
- Posteriormente, as portas PSN passaram a suportar o protocolo X.25.
- E o TCP/IP estava despontando nos anos 80.
- Em 1983 foi mandatório o uso do TCP/IP por todos os computadores conectados à ARPAnet.

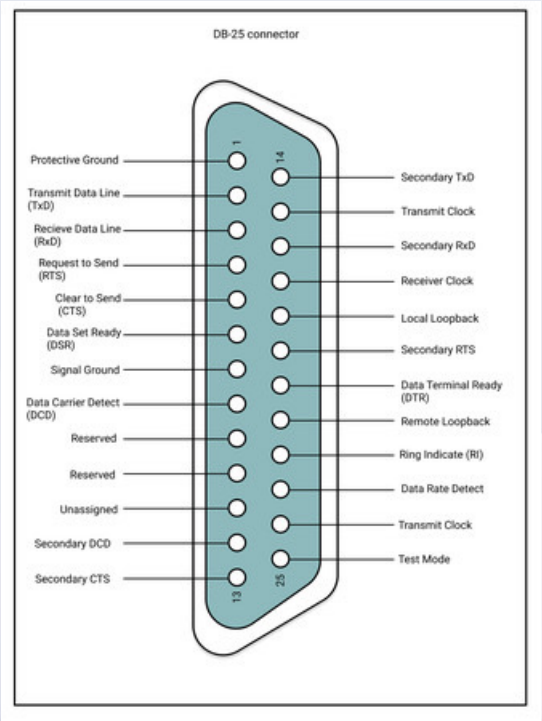
O surgimento do SLIP!

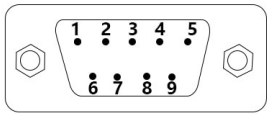
- O protocolo Serial Line Internet Protocol (SLIP) foi definido como método para redes TCP/IP sobre circuitos dedicados e conexões seriais.
  - O SLIP ficou popularizado como método para interconexão de computadores suportando TCP/IP sobre estes tipos de conexões.
  - Dentre as conexões, obviamente, a linha telefônica (POTS), ou seja, surgia aí o dial-up networking!

Exemplo de comunicação serial ponto-a-ponto com o protocolo SLIP



Exemplos de pinouts de conectores seriais DB25 e DB9





DB9 Male

Pin	Deiscription	Name
1	Data Carrier Detect	DCD
2	Receive(rx) Data	RXD
3	Transmit(tx) Data	TXD
4	Data Terminal Ready	DTR
5	Ground	GND
6	Data Set Ready	DSR
7	Request To Send	RTS
8	Clear to send	CTS
9	Ring Indicator	RI

O funcionamento das conexões seriais

Modem Cable - Straight Cable DB9 to DB9

DTE to DCE Connections

DTE Device (Computer) DB9		Signal Direction	DCE Device (Modem) DB9	
Pin# DB9 RS-232 Signal Names			Pin# DB9 RS-232 Signal Names	
#1 Carrier Detector (DCD)	CD	→	#1 Carrier Detector (DCD)	CD
#2 Receive Data (Rx)	RD	←	#2 Receive Data (Rx)	RD
#3 Transmit Data (Tx)	TD	→	#3 Transmit Data (Tx)	TD
#4 Data Terminal Ready	DTR	→	#4 Data Terminal Ready	DTR
#5 Signal Ground/Common (SG)	GND	—	#5 Signal Ground/Common (SG)	GND
#6 Data Set Ready	DSR	←	#6 Data Set Ready	DSR
#7 Request to Send	RTS	→	#7 Request to Send	RTS
#8 Clear to Send	CTS	←	#8 Clear to Send	CTS
#9 Ring Indicator	RI	←	#9 Ring Indicator	RI
Soldered to DB9 Metal - Shield	FGND	—	Soldered to DB9 Metal - Shield	FGND

Null-modem cable DTE - DTE (computer-to-computer)

DTE device	DB9		DB9	DTE device
1 Carrier Detection (DCD)	CD		CD	1 Carrier Detection (DCD)
2 Receive Data (Rx)	RD		RD	2 Receive Data (Rx)
3 Transmit Data (Tx)	TD		TD	3 Transmit Data (Tx)
4 Data Terminal Ready	DTR		DTR	4 Data Terminal Ready
5 Signal Ground/Common (SG)	GND		GND	5 Signal Ground/Common (SG)
6 Data Set Ready	DSR		DSR	6 Data Set Ready
7 Request to Send	RTS		RTS	7 Request to Send
8 Clear to Send	CTS		CTS	8 Clear to Send
9 Ring Indicator	RI		RI	9 Ring Indicator
Shield	FGND		FGND	Shield

Modem to Modem - Crossover Cable DB25 to DB25

DCE to DCE Connections

DCE Device (Modem) DB25		Signal Direction	DCE Device (Modem) DB25	
Pin# DB25 RS-232 Signal Names			Pin# DB25 RS-232 Signal Names	
#1 Shield to Frame Ground	FGND	—	#1 Shield to Frame Ground	FGND
#2 Transmit Data (Tx)	TD	→	#2 Transmit Data (Tx)	TD
#3 Receive Data (Rx)	RD	←	#3 Receive Data (Rx)	RD
#4 Request to Send	RTS	→	#4 Request to Send	RTS
#5 Clear to Send	CTS	←	#5 Clear to Send	CTS
#6 Data Set Ready	DSR	→	#6 Data Set Ready	DSR
#7 Signal Ground/Common (SG)	GND	—	#7 Signal Ground/Common (SG)	GND
#8 Carrier Detector (DCD)	CD	→	#8 Carrier Detector (DCD)	CD
#20 Data Terminal Ready	DTR	→	#20 Data Terminal Ready	DTR
#22 Ring Indicator	RI	←	#22 Ring Indicator	RI

Note: "Null Modem" cable for DTE to DTE also connects pins #6 & #8 together on each side simulating Carrier (CD)
Signal directions are reversed when devices are DTE to DTE.

Como surgiu o protocolo PPP?

- Apesar do SLIP ter sido o método popular e relativamente fácil de implementar, possuia diversas limitações:
  - Suportava apenas o TCP/IP.
  - Não suportava a negociação de parâmetros de comunicação:
    - Detecção de erros
    - Correção de erros
    - Compressão
- O sucessor do protocolo SLIP foi o *Point-to-Point Protocol* (PPP), publicado no RFC1134 no ano de 1989!

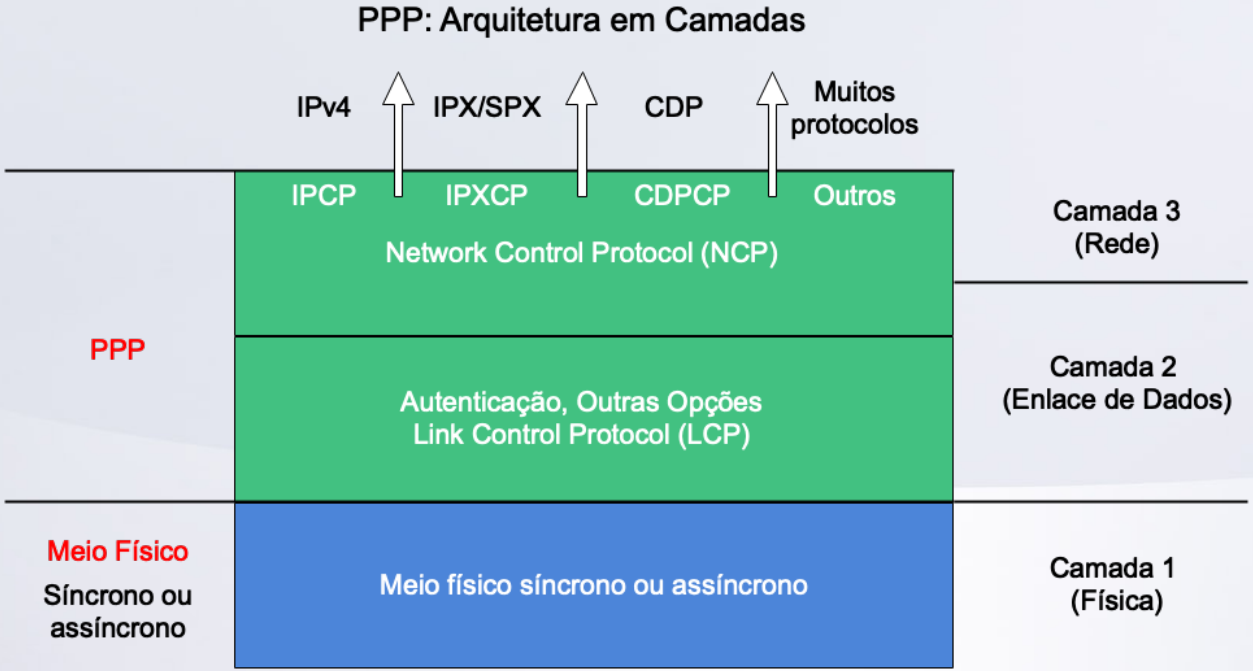
Sobre o Point-to-Point Protocol (PPP)

- O PPP foi desenvolvido devido a necessidade de um padrão de Internet para o encapsulamento e envio de datagramas sobre conexões seriais ponto-a-ponto.
  - Datagrama = bloco de dados, similar aos pacotes em uma rede PSN.
    - E redes TCP/IP dependem exclusivamente da entrega de datagramas IP (ou "pacotes")!
- O PPP abstrai todas as informações e procedimentos (números, portas, etc.) da infraestrutura por onde opera.

Recursos introduzidos pelo PPP

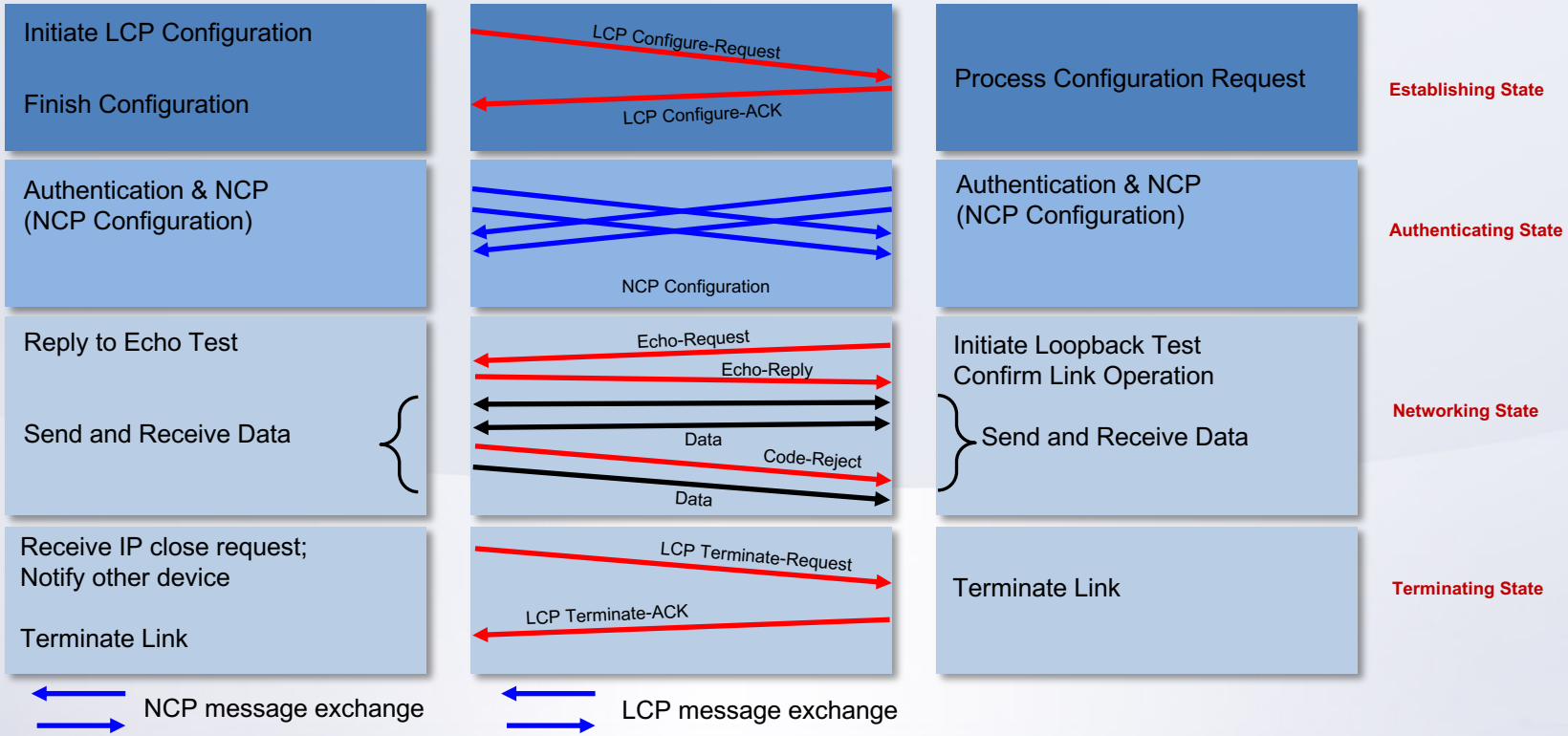
- O PPP oferece os seguintes mecanismos:
  - Multiplexação de diversos protocolos de redes.
  - Configuração dos enlaces, com seus mecanismos de negociação entre as duas partes.
  - Detecção de erros.
  - Recursos adicionais tais como compressão e algum regime de criptografia.
  - Negociação dos endereços de rede (ex: IP).
  - Autenticação.
  - Suporte a multilink.

Arquitetura por camadas do PPP



Lista completa de protocolos suportados pelo PPP:
https://www.iana.org/assignments/ppp-numbers/ppp-numbers.xhtml

O estabelecimento de um link PPP



O formato de um frame PPP

Frame PPP

1	1	1	2	Variável	2 ou 4
Flag	Address	Control	Protocol	Data	FCS

Flag: um único byte (01111110) indicando o início ou fim de um frame. Valor 0x7E.
Address: Um único byte contendo uma sequência binária de 11111111. Valor 0xFF.
Control: um único byte (00000011) para chamada de transmissão de dados em um frame não sequenciados. Valor 0x03.
Protocol: dois bytes identificando o protocolo encapsulado pelo campo de dados. Alguns exemplos:
- **IP**: 0x0021
- **IPCP**: 0x8021
- **IPV6CP**: 0x8057
- **LCP**: 0xC021
- **PAP**: 0xC023
- **CHAP**: 0xC223

Data: zero ou mais bytes contendo os dados de protocolos de camadas superiores.
FCS: normalmente, 16 bits (2-byte)

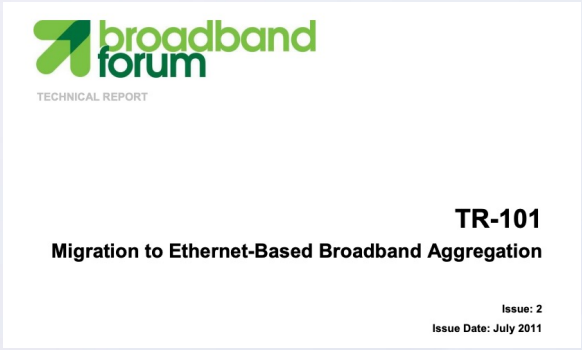
Alguns exemplos de códigos de mensagens do PPP

Códigos do LCP	
0x01	Configure-request
0x02	Configure-ack (acknowledge)
0x03	Configure-nak (negative acknowledge)
0x04	Configure-reject
0x05	Terminate-request
0x06	Terminate-ack (acknowledge)
0x07	Code-reject
0x08	Protocol-reject
0x09	Echo-request
0x0a	Echo-reply
0x0b	Discard-request

Códigos do NCP para o IPCP	
0x01	Configure-request
0x02	Configure-ack (acknowledge)
0x03	Configure-nak (negative acknowledge)
0x04	Configure-reject
0x05	Terminate-request
0x06	Terminate-ack (acknowledge)
0x07	Code-reject

A utilização do PPP para conectividade de Internet banda-larga

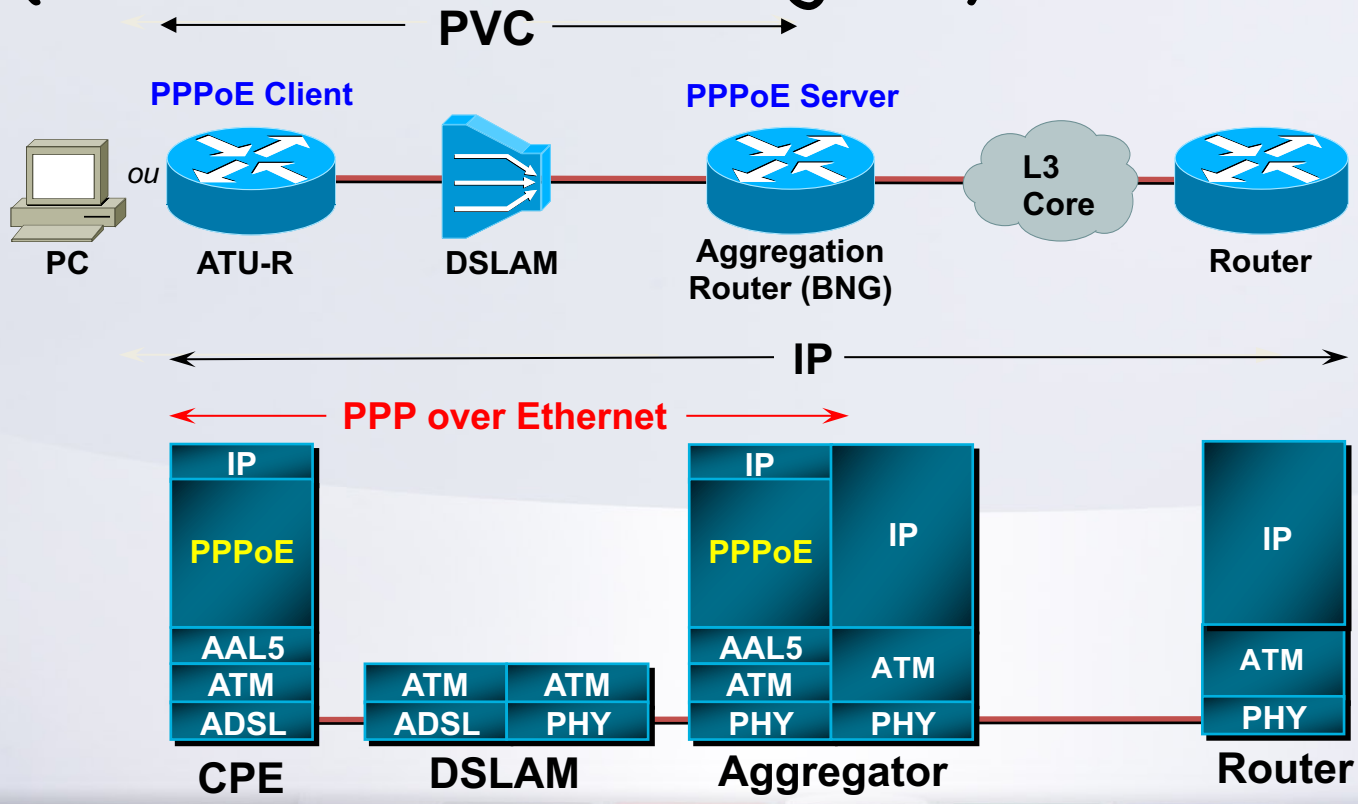
- O PPP por muitos anos tem sido o protocolo de controle de sessão predominante para conectividade banda-larga.
  - Em primeiro momento, em conexões dial-up.
  - Posteriormente, com a chegada do Digital Subscriber Line (DSL), e até mesmo em alguns casos com SONET/SDH:
    - PPP over ATM (PPPoA)
    - PPP over Ethernet (PPPoE)
    - PPP over SONET/SDH (POS)
- Por um bom tempo o PPP era o único mecanismo de transporte permitido pelo DSL Forum
  - DSL Forum's Technical Report 101 (TR-101), Migration to Ethernet-Based DSL Aggregation
- RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE).
- OBS: posteriormente, o IPoE passou a ser suportado para o DSL.



Por que o PPPoE foi (ou ainda é) necessário?

- Com a chegada da conectividade de Internet banda-larga, em especial com o advento das tecnologias xDSL...
- ... era exigido estabelecer sessões com os assinantes para os seguintes procedimentos:
  - Estabelecimento do link.
  - Estabelecimento de uma sessão lógica, onde cada uma pudesse ser unicamente rastreada.
  - Autenticação e autorização do assinante.
  - Identificação do assinante.
  - Monitoramento da rede, especificamente da conexão lógica.

O funcionamento básico do PPPoE (cenário clássico ou legado)



Alguns exemplos de códigos de mensagens do PPPoE

Pacotes durante o estágio de PPPoE Discovery (EtherType 0x8863)

Code	Mensagem	Session-ID
0x09	PPPoE Active Discovery Initiation (**PADI**)	0x0000
0x07	PPPoE Active Discovery Offer (**PADO**)	0x0000
0x19	PPPoE Active Discovery Request (**PADR**)	0x0000
0x65	PPPoE Active Discovery Session Confirmation (**PADS**)	Valor único produzido para a sessão ou 0x0000
0xA7	PPPoE Active Discovery Terminate (**PADT**)	Valor único da sessão em questão

Pacotes durante o estágio de PPPoE Session (EtherType 0x8864)

Code	Mensagem	Session-ID
0x00	Dados do pacote IP do assinante	Valor único que foi produzido para a sessão

O funcionamento básico do PPPoE

PADI (*broadcast*)

PADO (*unicast*)

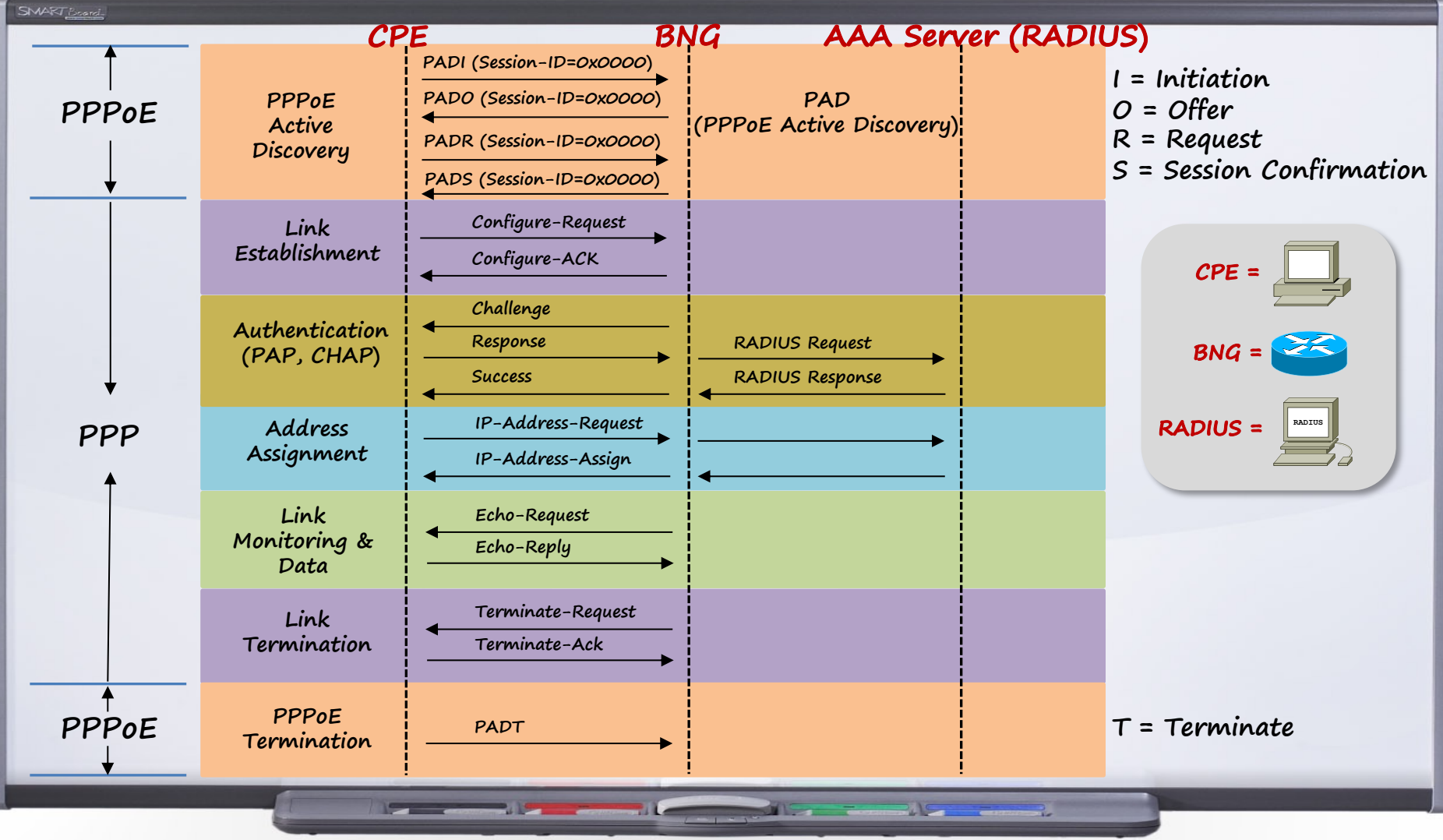
PADR (*unicast*)

PADS (Session ID) (*unicast*)

LCP / Authenticate / NCP (Regular PPP)

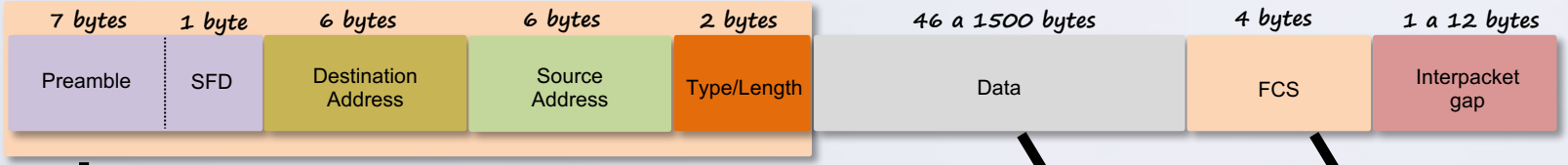
.
.
.

PADT (*unicast*)

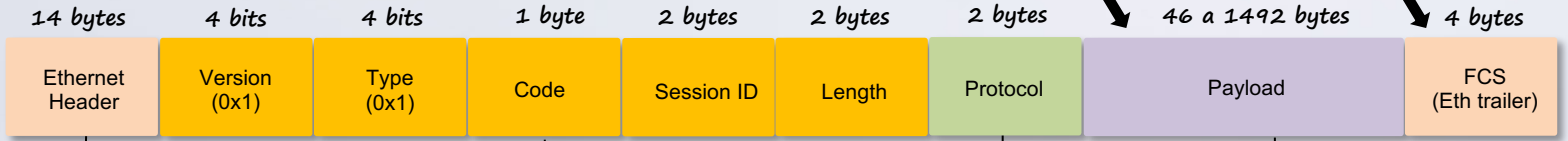

CPE
BNG
AAA Server (RADIUS)
PPPoE
PPP
PPPoE
PPPoE Active Discovery
PADI (Session-ID=0x0000)
PADO (Session-ID=0x0000)
PADR (Session-ID=0x0000)
PADS (Session-ID=0x0000)
PAD (PPPoE Active Discovery)
Link Establishment
Configure-Request
Configure-ACK
Authentication (PAP, CHAP)
Challenge
Response
Success
RADIUS Request
RADIUS Response
Address Assignment
IP-Address-Request
IP-Address-Assign
Link Monitoring & Data
Echo-Request
Echo-Reply
Link Termination
Terminate-Request
Terminate-Ack
PPPoE Termination
PADT
I = Initiation
O = Offer
R = Request
S = Session Confirmation
CPE =
BNG =
RADIUS =
RADIUS
T = Terminate

Formato do quadro Ethernet e pacote PPPoE

Quadro Ethernet II original (sem VLAN tag)



Formato do pacote PPPoE



- MAC de destino
- MAC de origem
- VLAN Tags (opcional)
- EtherType
  - **0x8863 (PPPoE Discovery)**
  - **0x8864 (PPPoE Session)**

PPPoE Header (6 bytes)

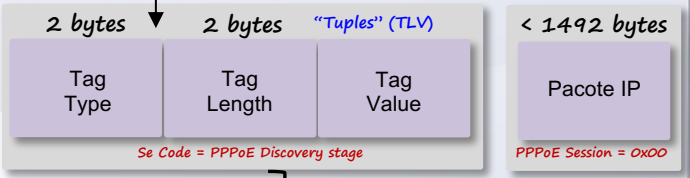
Discovery stage:
- 0x09 PADI
- 0x07 PADO
- 0x19 PADR
- 0x65 PADS
- 0xA7 PADT

Session stage:
- 0x00

Se Code = PPPoE Session stage

- IP: 0x0021
- IPCP: 0x8021
- LCP: 0xC021
- PAP: 0xC023
- CHAP: 0xC223
- Outros...

... ou ...



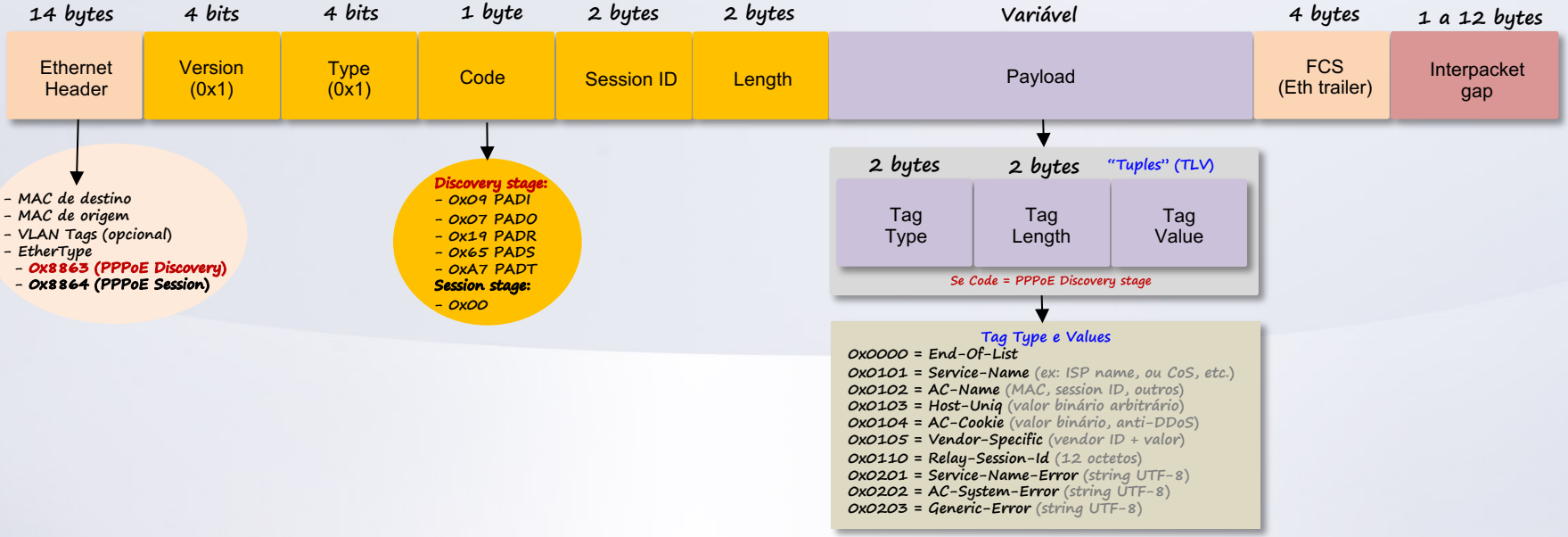
PPP Header (2 bytes) | **Pacote IP (< 1492 bytes)**

Ethernet Frame

Até 1518 bytes originais, ou 1522 bytes (IEEE 802.1q / 802.3ac), ou 1526 bytes (IEEE 802.1ad)

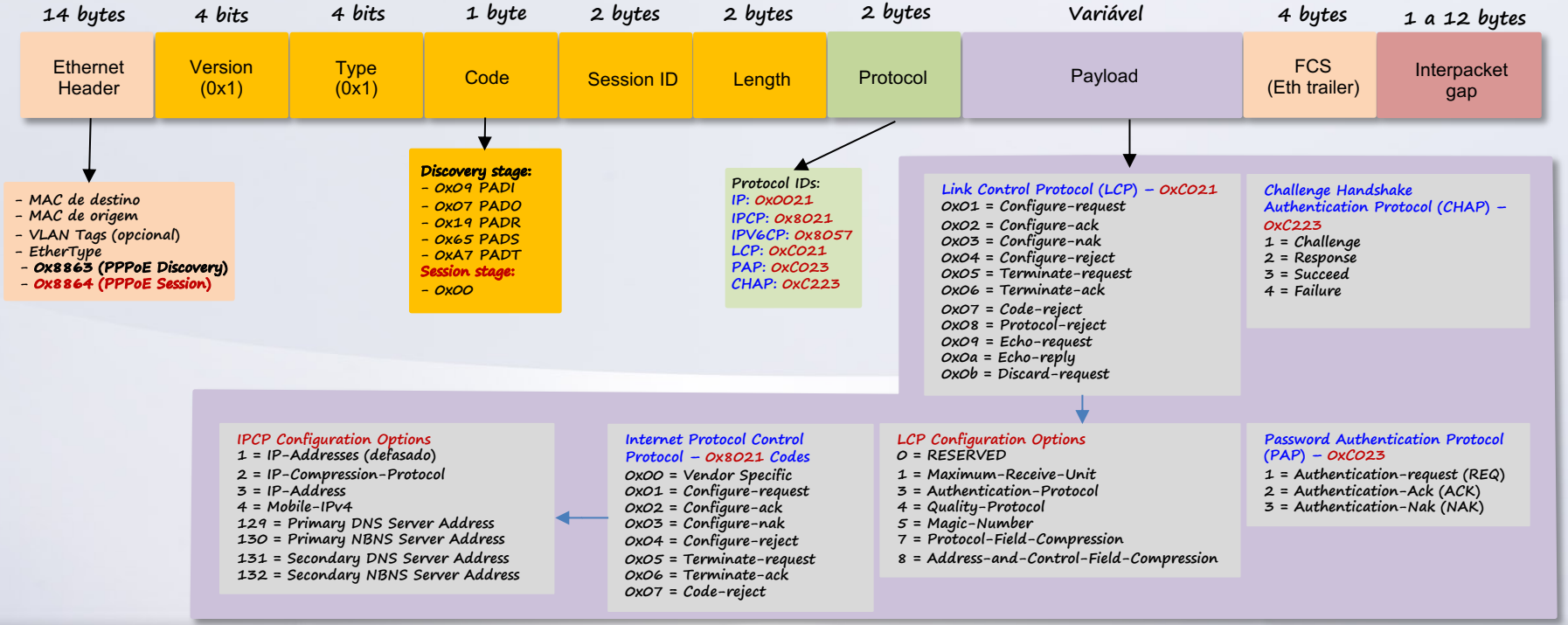
Procedimentos do protocolo PPPoE (PPPoE Discovery Stage)

Formato do pacote PPPoE

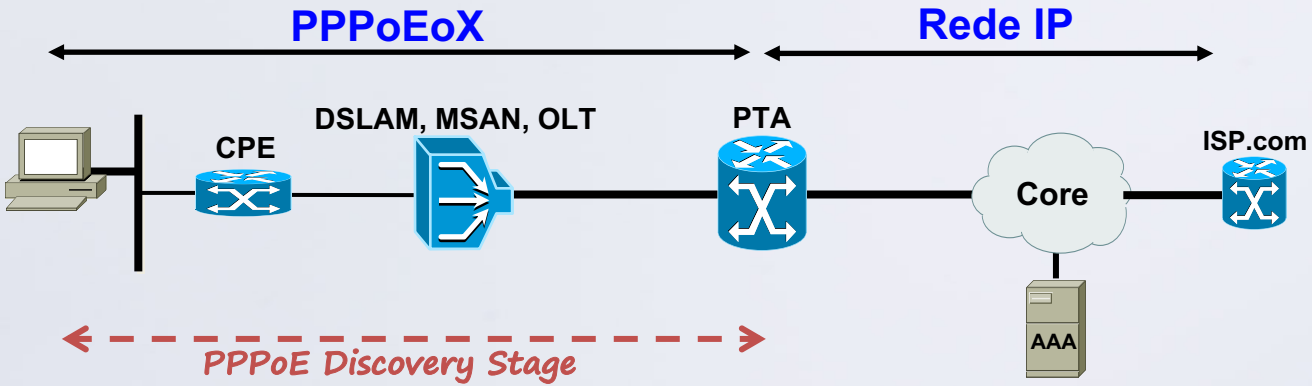


Procedimentos do protocolo PPP (PPPoE Session Stage)

Formato do pacote PPPoE



Revisão do setup da sessão PPPoE



PPPoE Discovery Stage

1 Host inicia sessão PPP com nome de usuário

Estágio negociação do LCP

Estágio de autenticação

2 Assinante autenticado pelo roteador local ou pelo servidor RADIUS

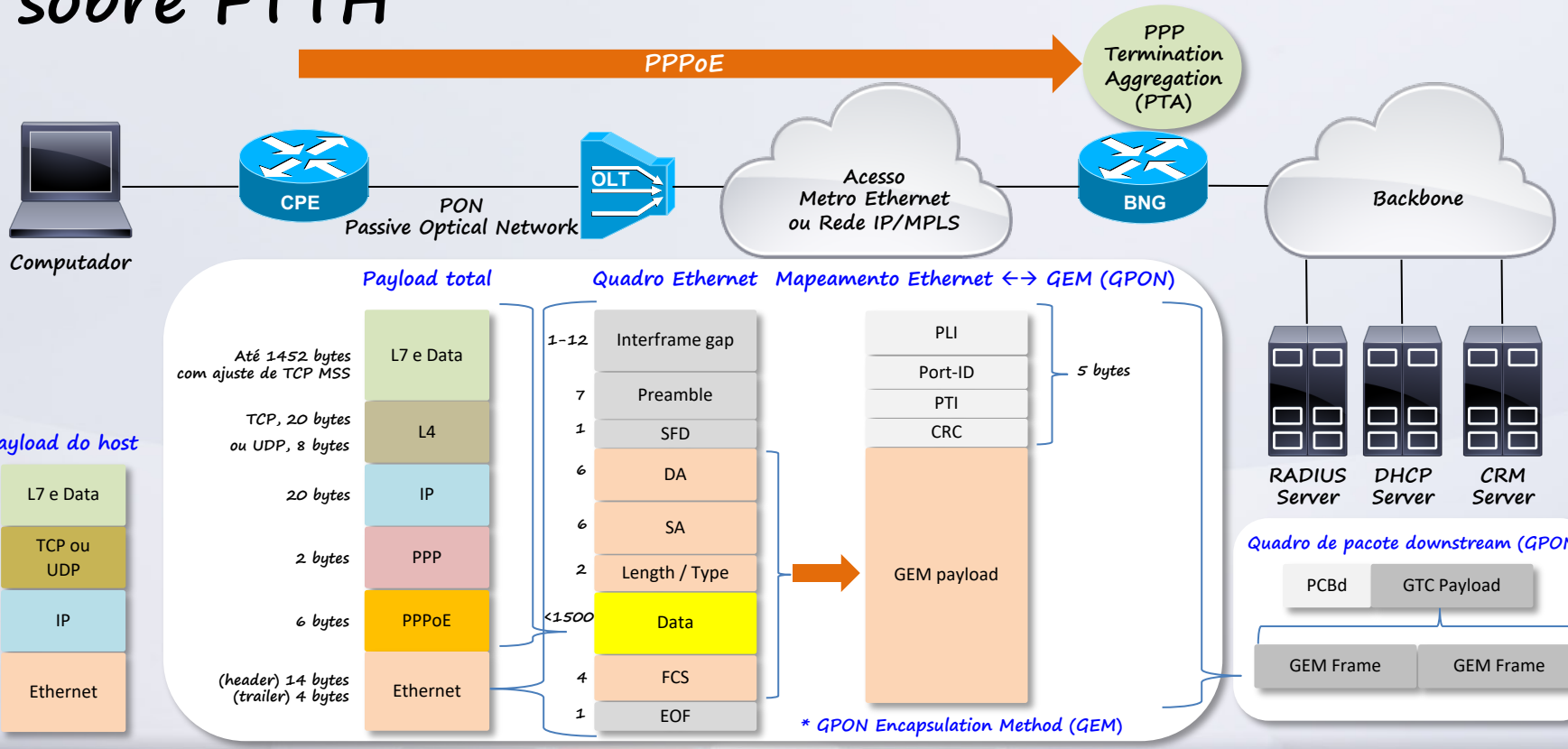
Estágio de negociação do NCP

3 Endereço IP alocado ao host usando negociação IPCP

4 O usuário pode acessar o serviço

Sessão estabelecida

O funcionamento de uma sessão PPPoE típica sobre FTTH



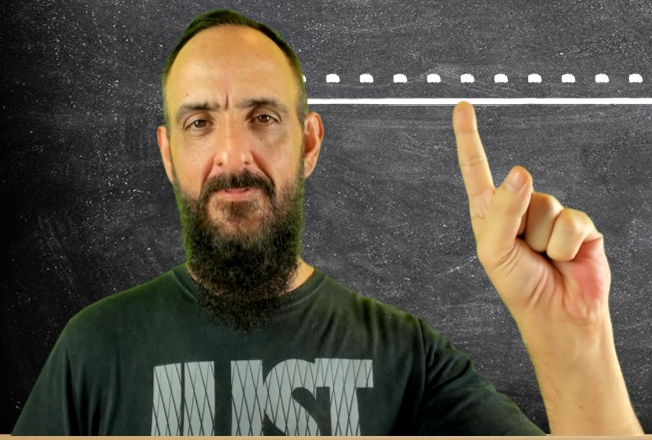
Requerimentos de sessões para assinantes

- O requisito mais fundamental para oferecer serviço de banda larga é o estabelecimento de uma sessão de rede para cada assinante, e de forma que possa ser usada para controlar o acesso à rede. O estabelecimento desta sessão consiste em várias fases:
  1. Autenticação do usuário – uma vez que o link é estabelecido, a identidade do usuário deve ser validada (autenticado) antes que o assinante tenha acesso à rede.
  2. Atribuição de endereço – uma vez autenticado, o usuário deve receber um endereço IP e demais parâmetros para que consiga acessar os serviços de rede.
  3. Controle de acesso – a rede deve autorizar quais recursos (serviços) de rede o usuário pode usar. Isso pode ser tão simples quanto limitar a velocidade de acesso à Internet com base no contrato estabelecido com o cliente.
  4. Monitoramento da conexão – cada conexão deve ser monitorada para garantir que o assinante ainda esteja conectado à rede.

Requerimentos de sessões para assinantes

- O PPPoE e IPoE são as duas técnicas principais disponíveis para executar essas tarefas.
  - IPoE também é às vezes referido como "DHCP", uma vez que esse protocolo desempenha um papel fundamental no estabelecimento da sessão IPoE.
- Abordemos, então, o IPoE na sequência!

COMO FUNCIONA O IPOE?



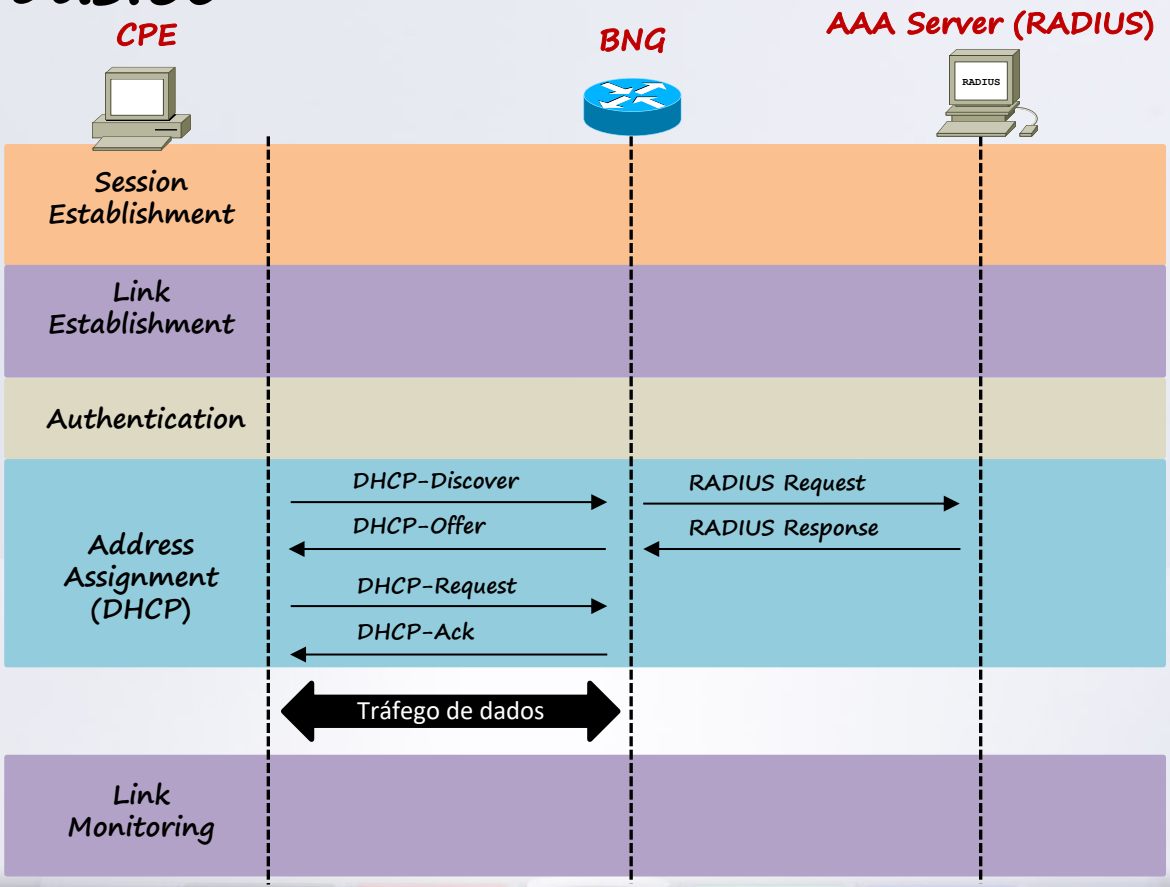
Introdução ao IPoE

- Resumidamente, o IPoE é um método de fornecimento de tráfego para os assinantes sem o uso do encapsulamento PPP.
- É uma alternativa mais recente que o PPPoE, e depende principalmente do DHCP, que foi originalmente projetado para atribuir endereços IP para dispositivos de conectados em LANs.
  - Inicialmente, o DHCP não era adequado para este procedimento devido a ausência de suporte a autenticação e monitoramento da sessão do assinante.
  - No entanto, extensões DHCP e outros protocolos (ex: EAP) ou procedimentos podem ser combinados para fornecer estes recursos que até então existiam somente para o PPPoE.

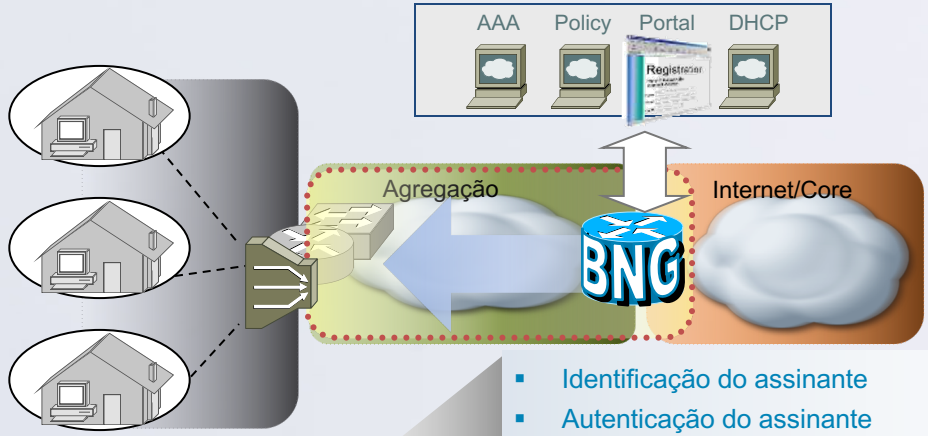
Introdução ao IPoE

- **Estabelecimento da sessão IPoE**
  - Na verdade, não há "exatamente" um conceito de sessão como no PPPoE! Consequentemente, não há um identificador único nativo para cada assinante.
    - O endereço IP atribuído deverá ser utilizado para identificar o assinante.
- **Autenticação do assinante IPoE**
  - O IPoE carece de procedimentos nativos de login/autenticação, tal como o CHAP do PPP/PPPoE.
  - Sendo assim, o IPoE depende de informações sobre a conexão de rede do assinante para poder identificar, admitir o assinante, e determinar os serviços disponíveis para o assinante.

O IPoE básico



Posicionamento do BNG em ambientes ISP

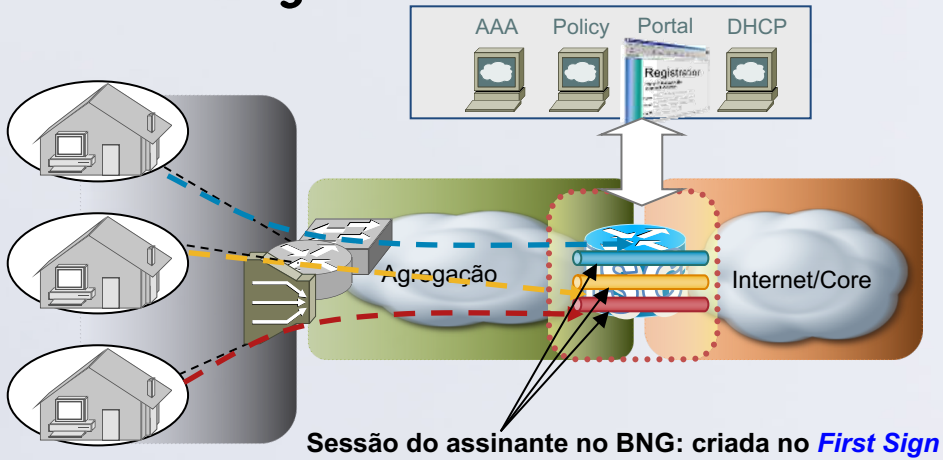


- Implantado no acesso ou na borda de serviços
- Comunica-se com outros dispositivos para controlar todos os aspectos do acesso do assinante na rede
- Único ponto de contato

- Identificação do assinante
- Autenticação do assinante
  - PPP CHAP/PAP
  - Transparent Auto Logon (TAL)
  - Web Logon
  - RADIUS
- Determinação e aplicação dos serviços do assinante
- Atualização dinâmica de serviços
- Gerenciamento do ciclo de vida da sessão
  - Estabelecimento
  - Configuração
  - Terminação

Baseado em:
- Quem é o usuário
- Onde ele está
- Como se comporta
- O que ele demanda

Identificação do assinante no IPoE



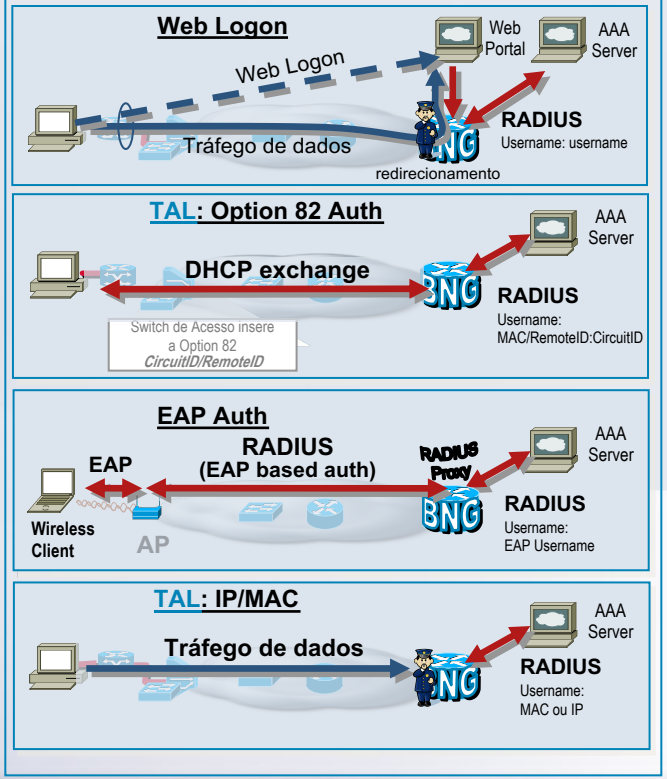
Sessão do assinante no BNG: criada no *First Sign Of Life* (FSOL)

Relação N:1 entre sessão e interface

	FSOL	
Sessões PPP	Pedido de chamada PPP	
Sessões IP	Pacote recebido com endereço IP ou MAC de origem desconhecido	*Sessão IP iniciada por IP ou MAC*
	DHCP Discover	*Sessão IP iniciada por DHCP*
	RADIUS Request	*Sessão IP iniciada por RADIUS*

Autenticação do assinante no IPoE

Cenários comuns com IPoE



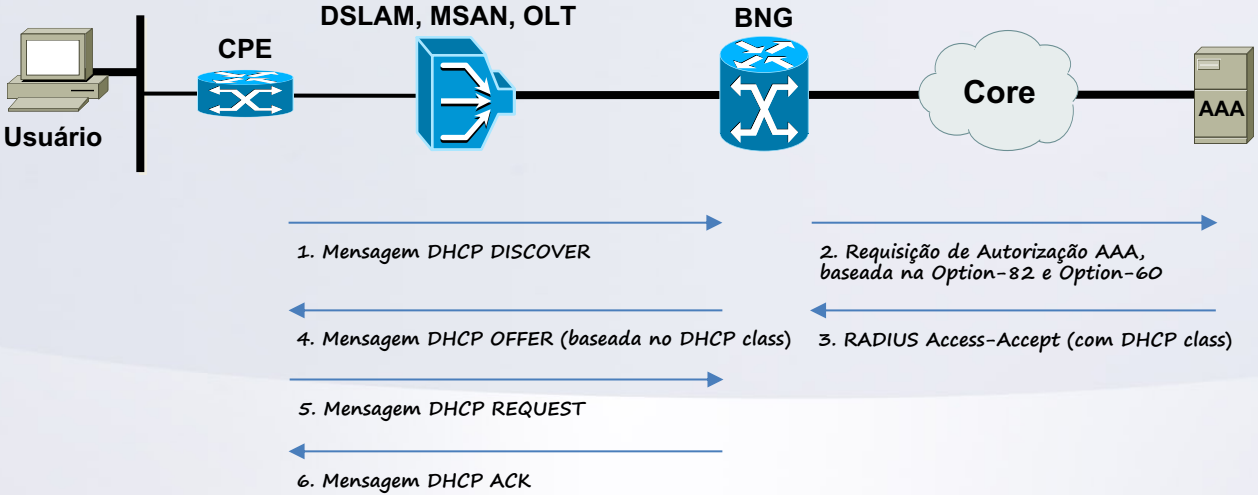
- O tráfego do usuário é redirecionado para um portal web para login
- As credenciais do usuário são passadas para BNG/ISG
- O BNG/ISG usa as credenciais para autenticar o usuário com o servidor AAA
- Aplicável a todos os tipos de sessão

- O switch de Acesso insere a Option 82 (Circuit e Remote ID) nas solicitações de DHCP
- O BNG/ISG autentica usando uma combinação de Circuit e Remote ID
- Ou o dispositivo do cliente encaminha a Option 60 (RFC 2132) para o BNG
- A sessão no BNG/ISG deve ser iniciada por DHCP

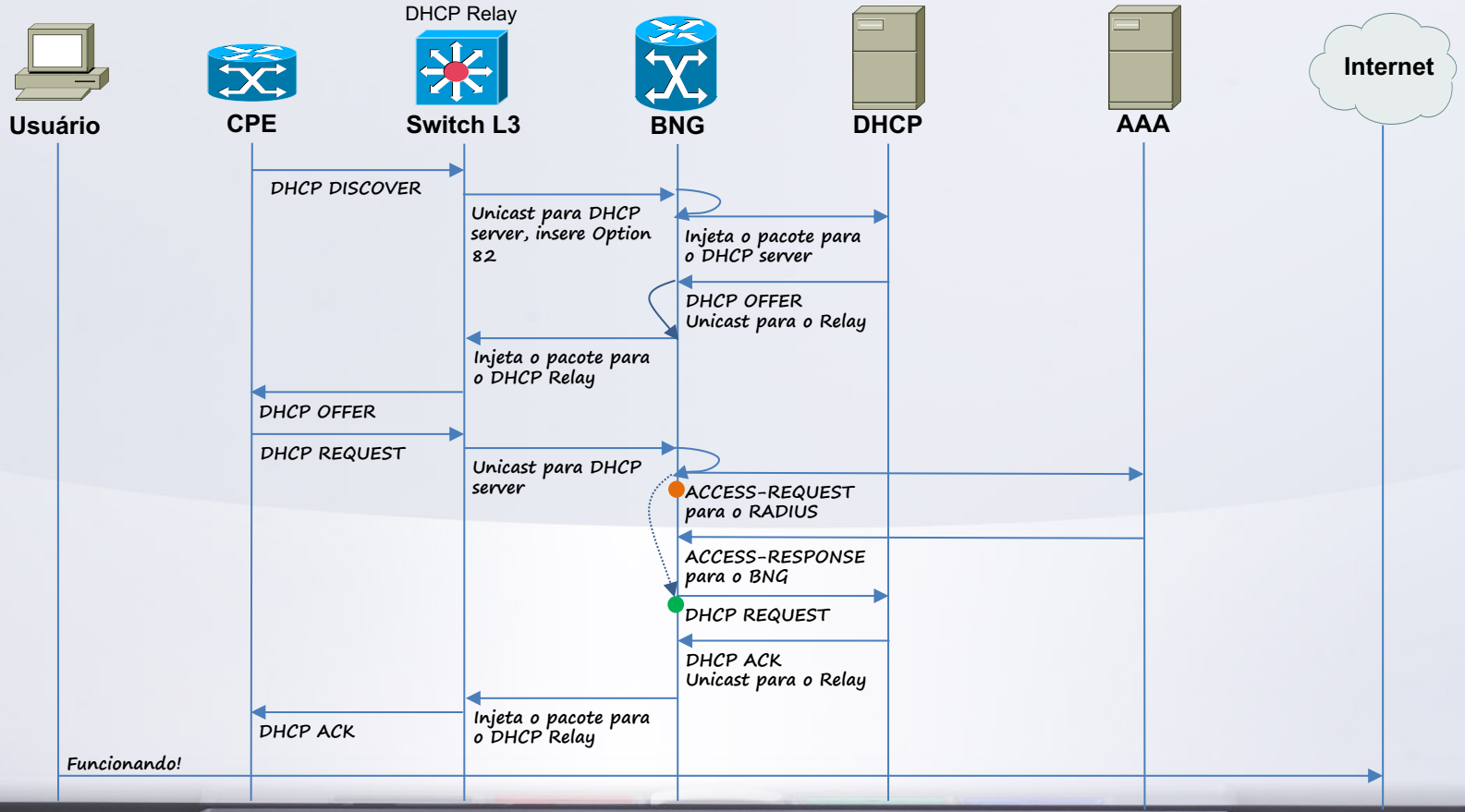
- O usuário inicia a autenticação EAP com Ponto de Acesso (AP)
- O BNG/ISG personifica o servidor RADIUS para o AP e o cliente RADIUS para o servidor real
- O BNG/ISG aprende o status de autenticação da sessão por meio do proxy de mensagens RADIUS entre o cliente RADIUS real e o servidor
- A sessão no BNG/ISG deve ser iniciada por RADIUS

- O ISG autentica usando identificadores de tráfego do assinante (IP / MAC de origem)
- Normalmente usado em topologias com assinantes conectados L2 para oferecer suporte a clientes com endereço IP estático ou em topologias roteadas por IP

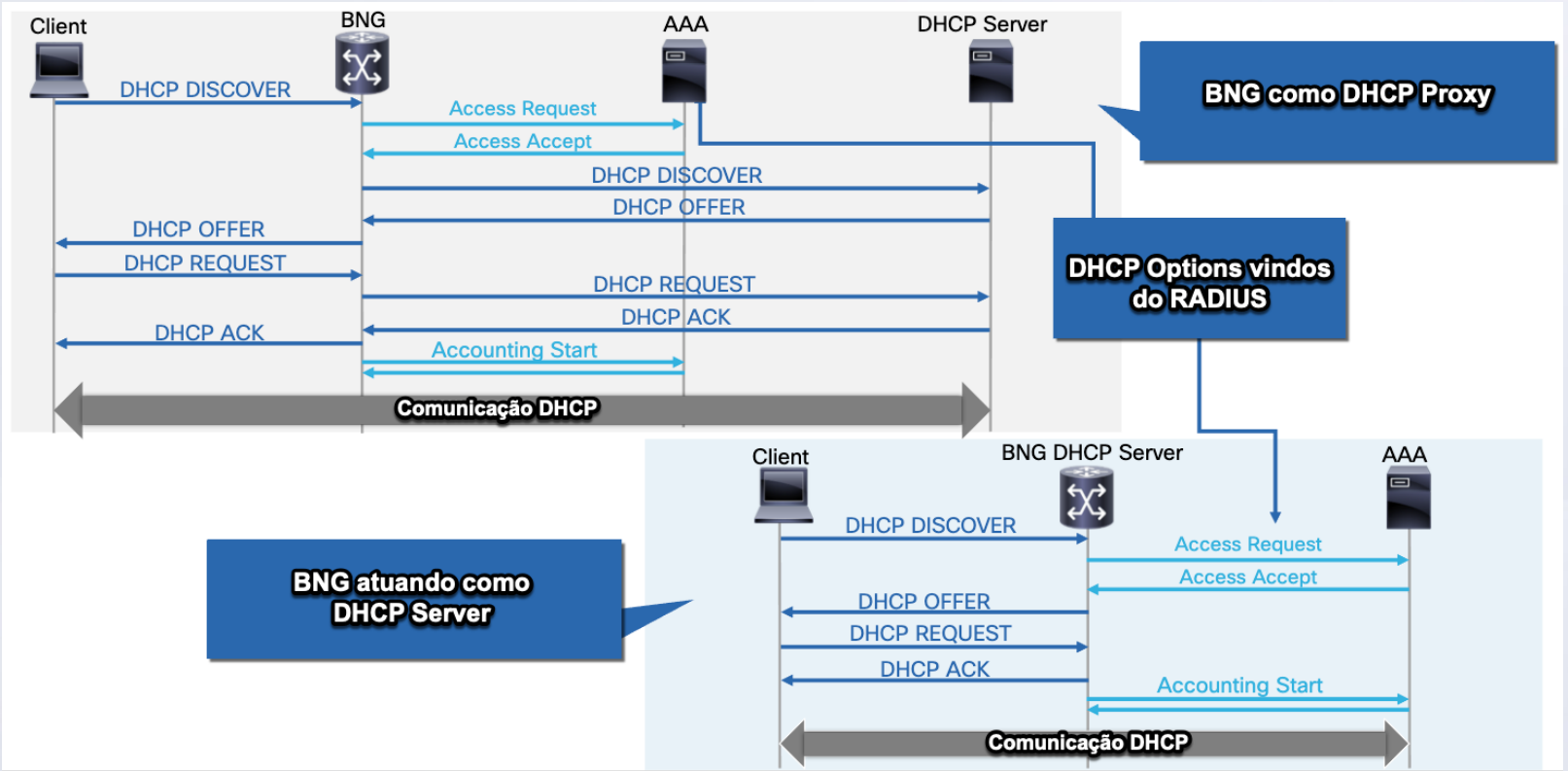
Sessões de assinantes iniciadas por DHCP, com o BNG atuando como DHCP server



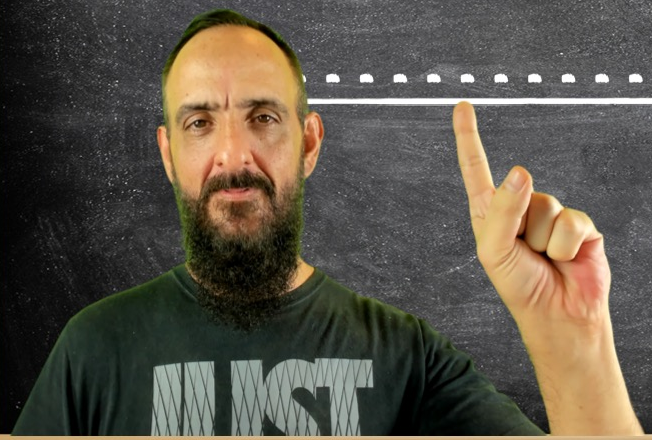
Sessões de assinantes iniciadas por DHCP



Sessões de assinantes iniciadas por DHCP



COMO FUNCIONA O RADIUS?

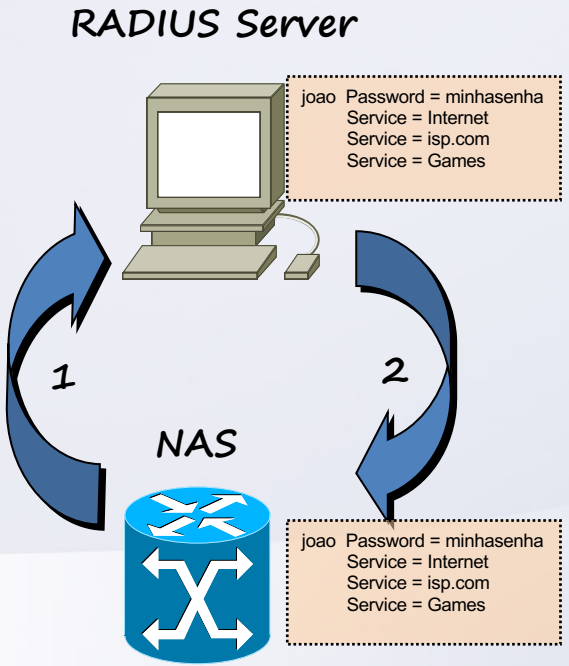


Conhecendo o AAA

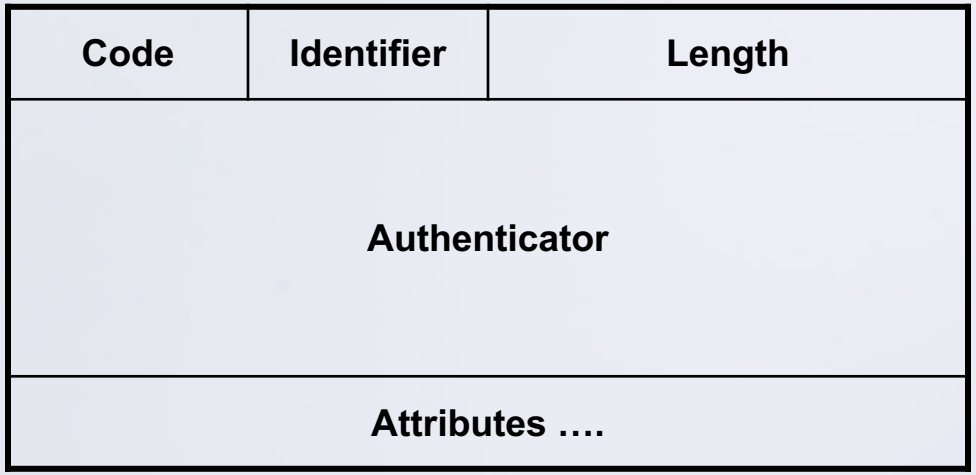
- **A**uthentication
  - Confirmação da identidade da entidade (ex: usuário, dispositivo)
- **A**uthorization
  - Implementação dos serviços autorizados, tais como o que pode ser acessado, tempo de vida da sessão, banda contratada, etc.
- **A**ccounting
  - Manutenção de registros de auditoria da sessão.

Operação do RADIUS

- O servidor escuta o serviço na porta UDP port 1812/1645 (RFC 2865)
- O NAS (BNG) envia mensagens Access-Request (1)
- O servidor processa a requisição
- O servidor encaminha mensagens Access-Accept ou Access-Reject (2)



Mensagens do RADIUS



Code:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response

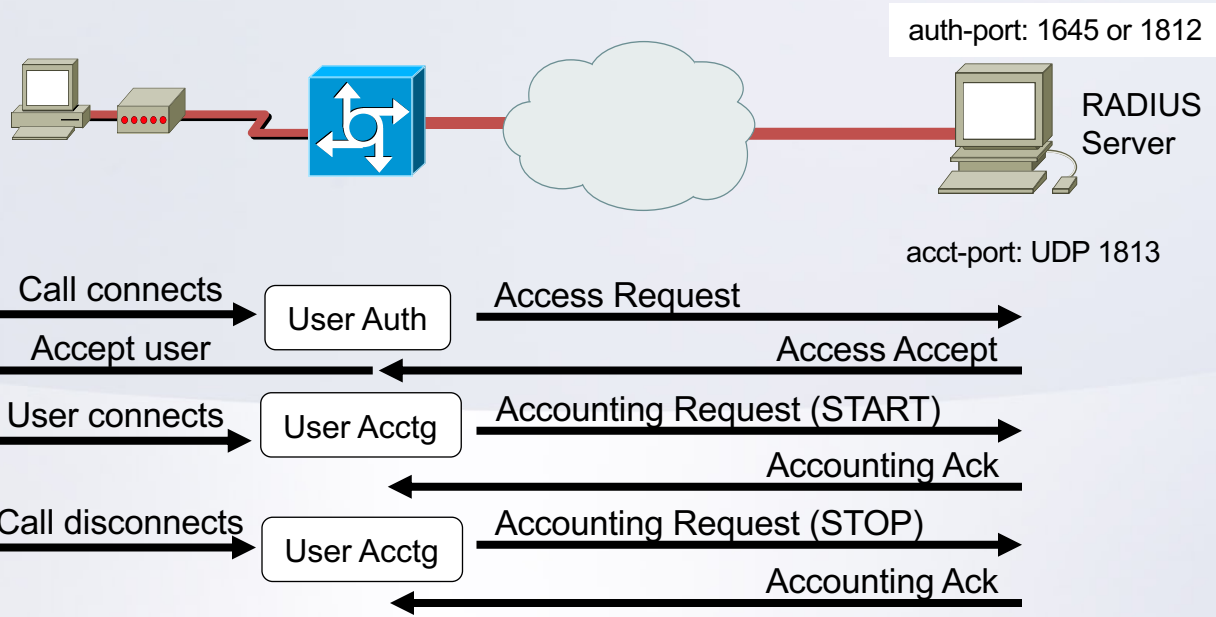
Radius – AV Pairs

Type	Length	Value ….
Value ….		

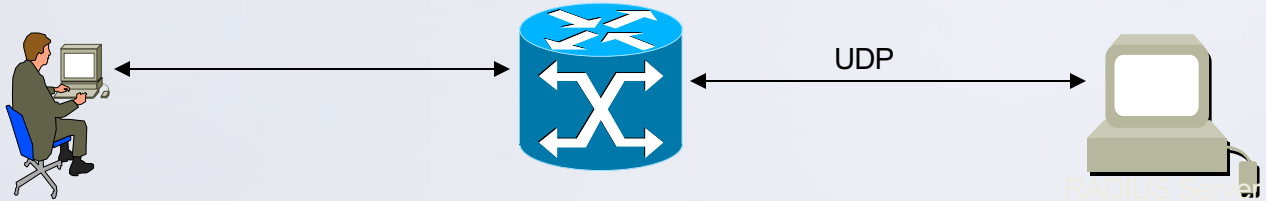
Vendor Specific:

Type = 26	Length	Vendor-Id Cisco = 9, Ascend = 529
Vendor Id (cont)		String

Radius – RFC 2865



Um exemplo de sessão simples com procedimento pelo RADIUS



Access-Request

(Username, Encrypted Password, NAS ID, NAS Port, etc.)

(ex: joao@isp.com, $%^&*#$, PPP)

Access-Accept / Access-Reject

(Contém Reply Attributess, ex:User-Service = Framed,

protocol type, IP Address, access lists, routes, policies de QoS, etc.)

(Ex: Framed/PPP, IP, 192.168.1.10)

Packet Type = Accounting-Request

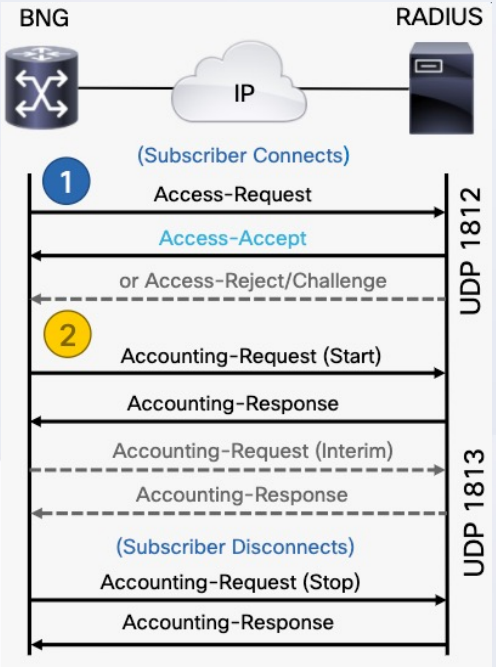
(Contém Accounting Attributes)

Packet Type = Accounting-Response

(Reconhecimento de que a contabilidade foi registrada)

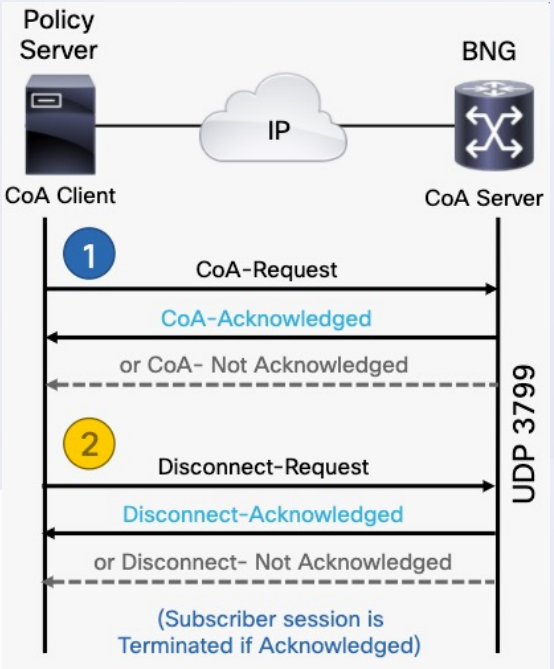
Funcionamento básico do RADIUS com o BNG

- Processo em dois estágios, com troca de pacotes pelo UDP:
  1. A autenticação e autorização são combinadas num único procedimento.
     - Autorização é opcional
     - Se houver autorização, AV-Pairs recebidos na mensagem Access-Accept são aplicados para a sessão.
     - Se não houver configuração de autorização, o roteador simplesmente ignora.
  2. Accounting ocorre no segundo estágio.
     - Apenas se a autenticação tiver sido bem sucedida.
     - O accounting também é opcional.

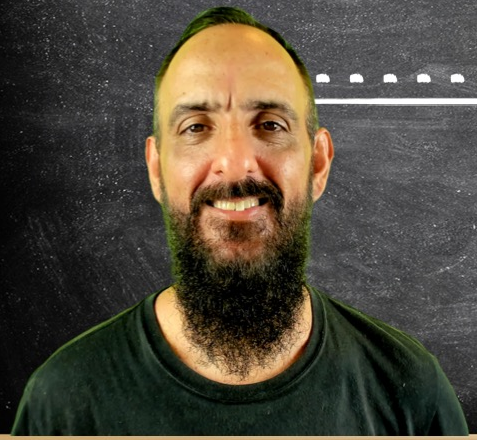


Extensões para operações de autorização do RADIUS

- Configurações adicionais podem ser idealizadas para fornecer funcionalidades e facilidades para o projeto:
  1. Change of Authorization (CoA)
     - Usado para controle dinâmico de políticas.
       - Adição e remoção de serviços para a sessão, "on the fly".
     - O BNG responde com um Ack positivo ou negativo, e aplica as políticas de acordo.
  2. Disconnect Message (DM)
     - Também conhecido por Packet of Disconnect (PoD).
     - Se reconhecido, a sessão do assinante é terminada, e o assinante é desconectado.



DIFERENÇAS ENTRE OS CENÁRIOS COM PPPOE E IPOE



Comparativos entre PPPoE e IPoE

Requerimento da Sessão	PPP / PPPoE - Session	IP-Session
Endpoint da Sessão do Assinante	PPPoE/PPP client	Múltiplas opções – comum: Device (“Identification”)
Autenticação do Assinante	PPP LCP Auth.Phase (PAP, CHAP,..)	MAC/Line-Authentication, soluções de Portal, DHCP-Auth
Isolamento do Assinante	Encapsulamento PPP por sessão	L3: Session Controller, ACLs, VRFs L2: VLAN, private VLAN
Identificação do Assinante e da Sessão	Session ID	Múltiplas opções (Interface, MAC, IP-address,…)
Endereçamento IP	PPP NCP	DHCP, SLAAC, DHCPv6 IAPD …
Manutenção da Sessão – Keepalive	PPP LCP	Múltiplas opções (ARP ping, ICMP ping, …)
Start/Stop da Sessão	PPP LCP	Múltiplas opções (Chegadas de pacotes, DHCP,…)
Encapsulamento do Tráfego	PPPoE, PPP	Nenhum
Encaminhamento do Tráfego	Ponto a ponto	Ponto a ponto & Multiponto
Wholesale	PPP/L2TP	L3: VRF L2: VLAN, EoMPLS PW
Mobilidade do Assinante	Reestabelecimento da sessão PPP	Transparent Autologon, Soluções de Portal

Iniciação dinâmica de sessão

- As sessões dos assinantes são iniciadas ao "primeiro sinal de vida" (FSOL)
- O FSOL dependerá do tipo de sessão

Sessões PPP - FSOL

- Recebimento do PADR
  - Session-start event
- Estabelecimento da sessão em 2 estágios
  - Session-start
  - Session-activate
- Assinante identificado por MAC + PPP session ID

Sessões IP- FSOL

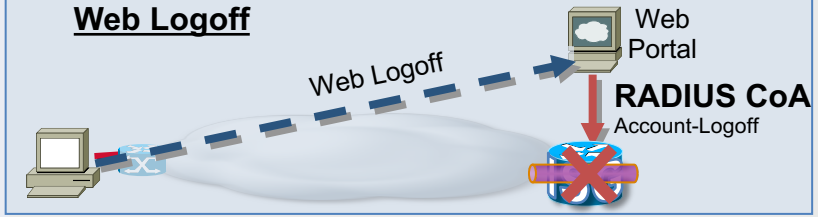
- DHCP Discover message
  - Session-start event
- Estabelecimento de sessão de estágio único
- Assinante identificado por endereço MAC ou conforme sinalizado pelo Option 82
- O BNG pode ser DHCP ou Proxy
  - DHCP proxy = DHCP relay que:
    1. cria e mantém os DHCP bindings
    2. Representa o servidor do ponto de vista do cliente

Terminação da sessão IPoE

Sessões IP

Tempo de inatividade, expiracão

Web Logoff

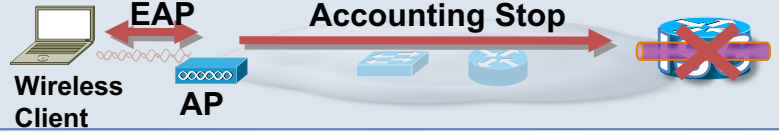


RADIUS (Packet Of Disconnect)

Falha do keepalive do ICMP, ou timeout de ARP

ICMP para sessões L3/routed
ARP para sessões conectadas em L2

RADIUS



DHCP

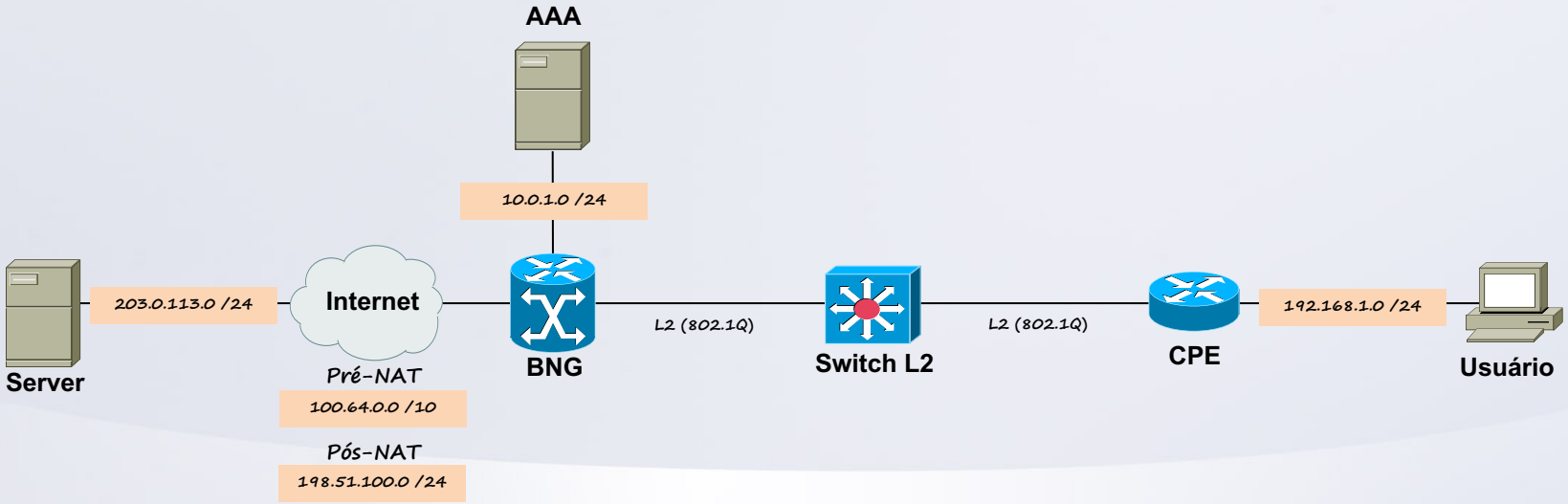
Apenas para sessões iniciadas por DHCP

ESTUDO DE CASO: UMA SOLUÇÃO (PROJETO) TÍPICO DE BNG COM MULTISSERVIÇOS

Estudo de Caso
BNG com PPPoE e CGNAT

Baseado em plataform Cisco ASR 1000

Topologia do Laboratório



OBRIGADO!!

/LeonardoFurtadoNYC

Https://discord.gg/leonardofurtado