BROADBAND REMOTE ACCESS SERVER

Saw Yan Paing
CCIE #57007

Broadband Remote Access Server (BRAS)

- BRAS are an essential part of broadband topologies to control subscriber access
- BRAS is the access point for subscribers, through which they connect to the broadband network. When a connection is established between BNG and Customer Premise Equipment(CPE),the subscriber can access the broadband services provided by the Network Service Provider(NSP) or Internet Service Provider(ISP).
- BRAS establishes and manages subscriber sessions. When a session is active, BNG aggregates traffic from various subscriber sessions from an access network , and routes it to the network of the service provider.
- BRAS is deployed by the service provider and is present at the first aggregation point in the network, such as the edge router.
- BRAS effectively manages subscriber access, and subscriber management functions such as:
    - Authentication, Authorization and Accounting of subscriber sessions
    - Address assignment
    - Security
    - Policy management
    - Quality of Service(QoS)

BRAS or BNG?

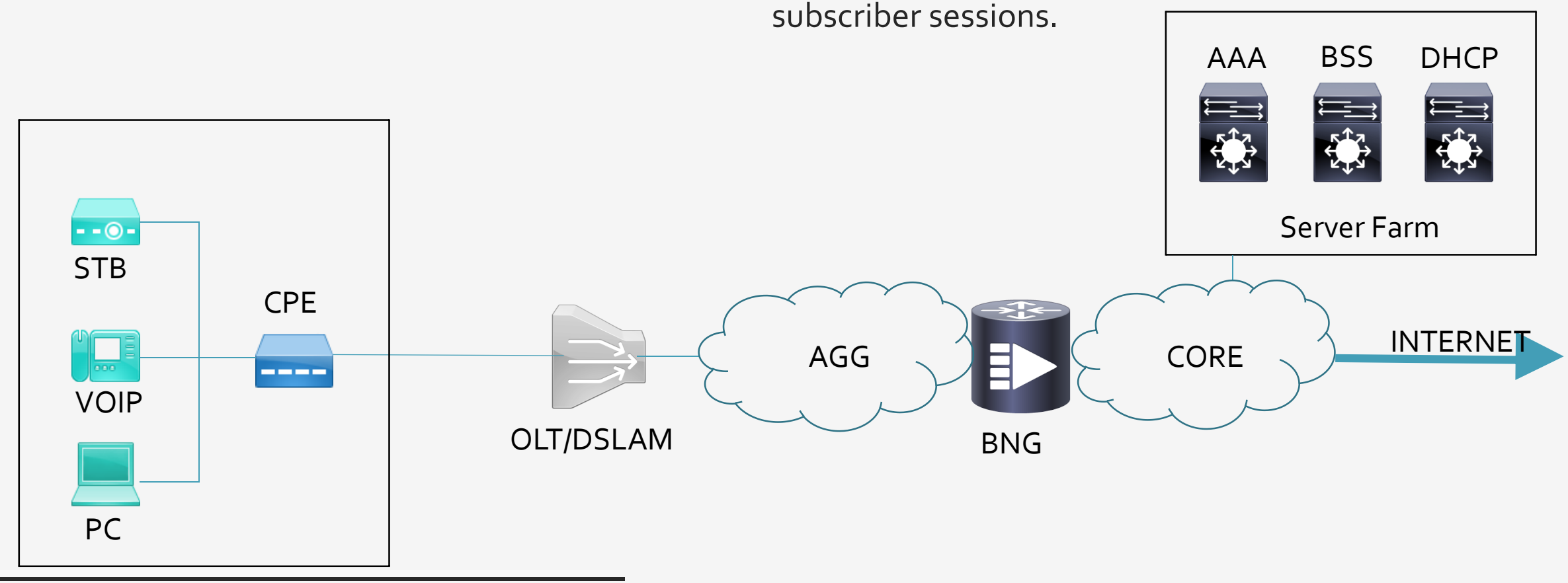
- BRAS (Broadband Remote Access Server) was the term previously used, it is now BNG (Broadband Network Gateway). There is no functional difference.

Task of BRAS/BNG

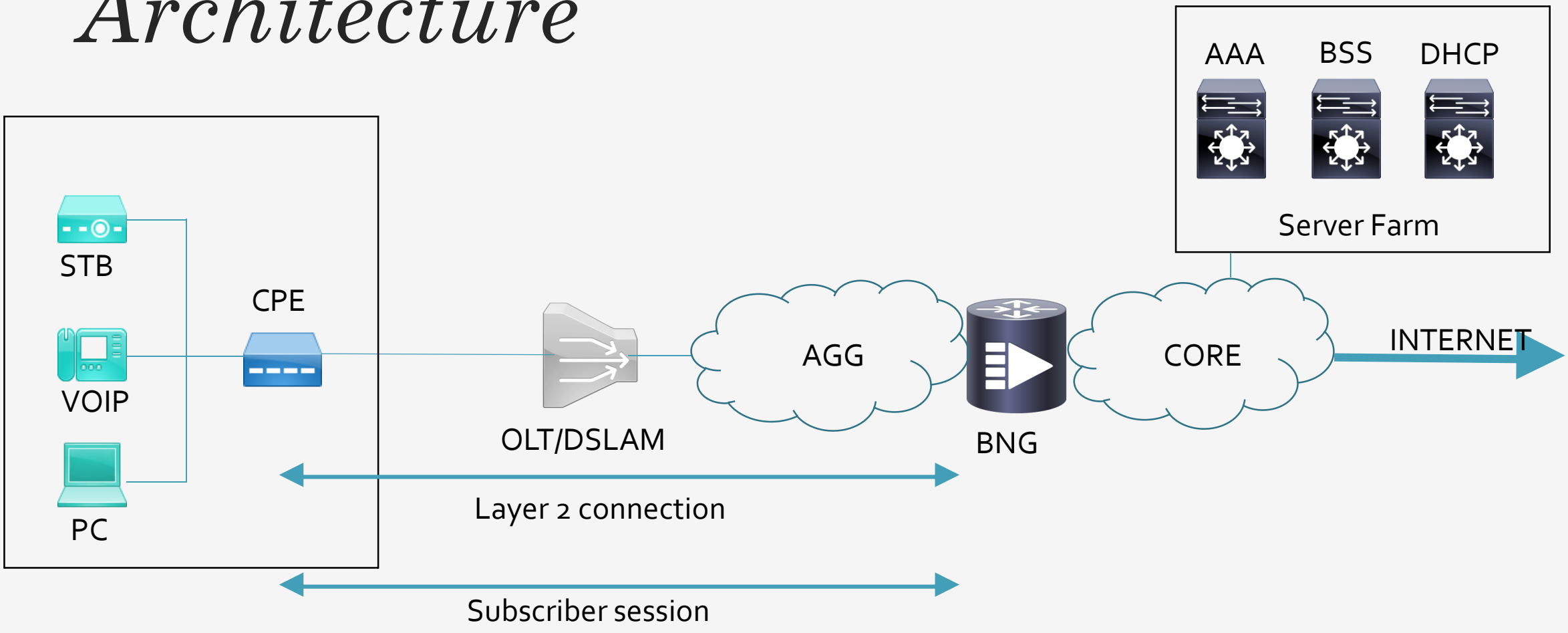
- Connecting with the Customer Premise Equipment (CPE) that needs to be served broadband services.
- Establishing subscriber sessions using IPoE or PPPoE protocols
- Aggregates the circuit from one or more link access devices (provides aggregate capabilities for IP,PPP,ATM, etc.)
- Interacting with the AAA server that authenticates subscribers, and keeps an account of subscriber sessions.
- Interacting with the DHCP server to provide IP address to clients.
- Enforce quality of service (QoS) polices
- Provide Layer 3 connectivity and routes IP traffic through on ISP backbone network to the Internet

BNG Architecture

- The goal of the BNG architecture is to enable the BNG router to interact with peripheral devices(like CPE)and servers(like AAA and DHCP),in order to provide broadband connectivity to subscribers and manage subscriber sessions.

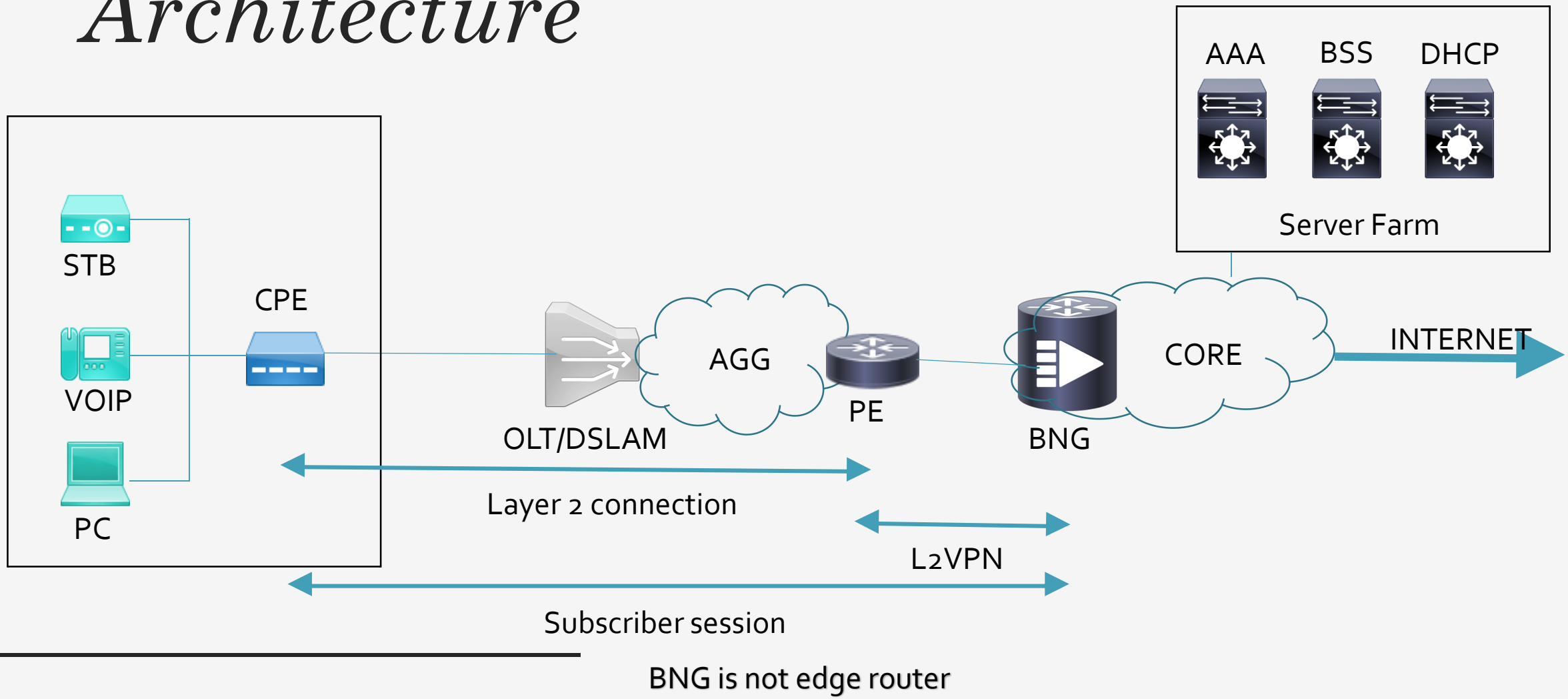


BNG Architecture



BNG as an edge router

BNG Architecture



BNG is not edge router

Establishig Subscriber Sessions

- Each subscriber (or more specifically, an application running on the CPE) connects to the network by a logical session. Based on the protocol used, subscriber sessions are classified into two types:

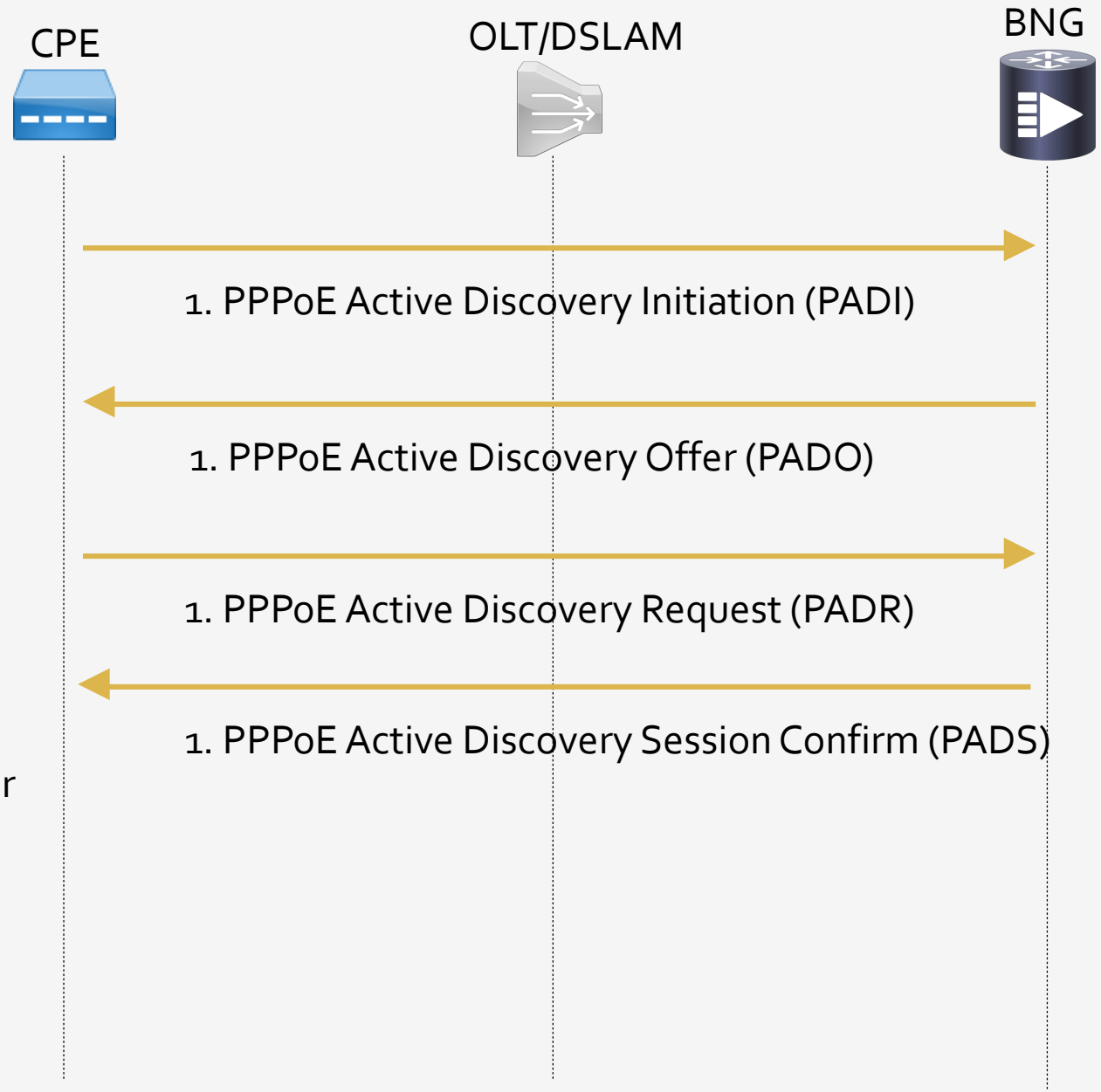
PPPoE subscriber session: The PPP over Ethernet (PPPoE) subscriber session is established using the point-to-point(PPP) protocol that runs between the CPE and BNG.

IPoE subscriber session: The IP over Ethernet (IPoE) subscriber session is established using IP protocol that runs between the CPE and BNG; IP addressing is done using the DHCP protocol.

PPPoE

- PPPoE was designed for managing how data is transmitted over Ethernet networks, and it allows a single server connection to be divided between multiple clients, using Ethernet. As a result, multiple clients in shared network can connect to the same server from the Internet Service Provider and get access to the internet, at the same time, in parallel. To simplify, PPPoE is a modern version of the old dial-up connections, which were popular in the 80s and the 90s.
- P2P protocol over ethernet encapsulating PPP frames in Ethernet frames (Src MAC, Dst MAC).
- Old days used mainly with ADSL services (most common PPPOE over ATM)
- Offers standard PPP features such as authentication, encryption, and compression
- PPPoE has two distinct stages as defined in RFC 2516:
    - Discovery stage
    - PPP session stage

PPPoE Call Flow



Discovery stage

- The discovery stage allows the PPPoE client (end-user PC/ router / Modern) to discover all PPPoE servers and then select one to use.

- The host must identify the MAC address of the peer and establish a PPPoE session

Ethertype : 0x8863

PPPoE Call Flow

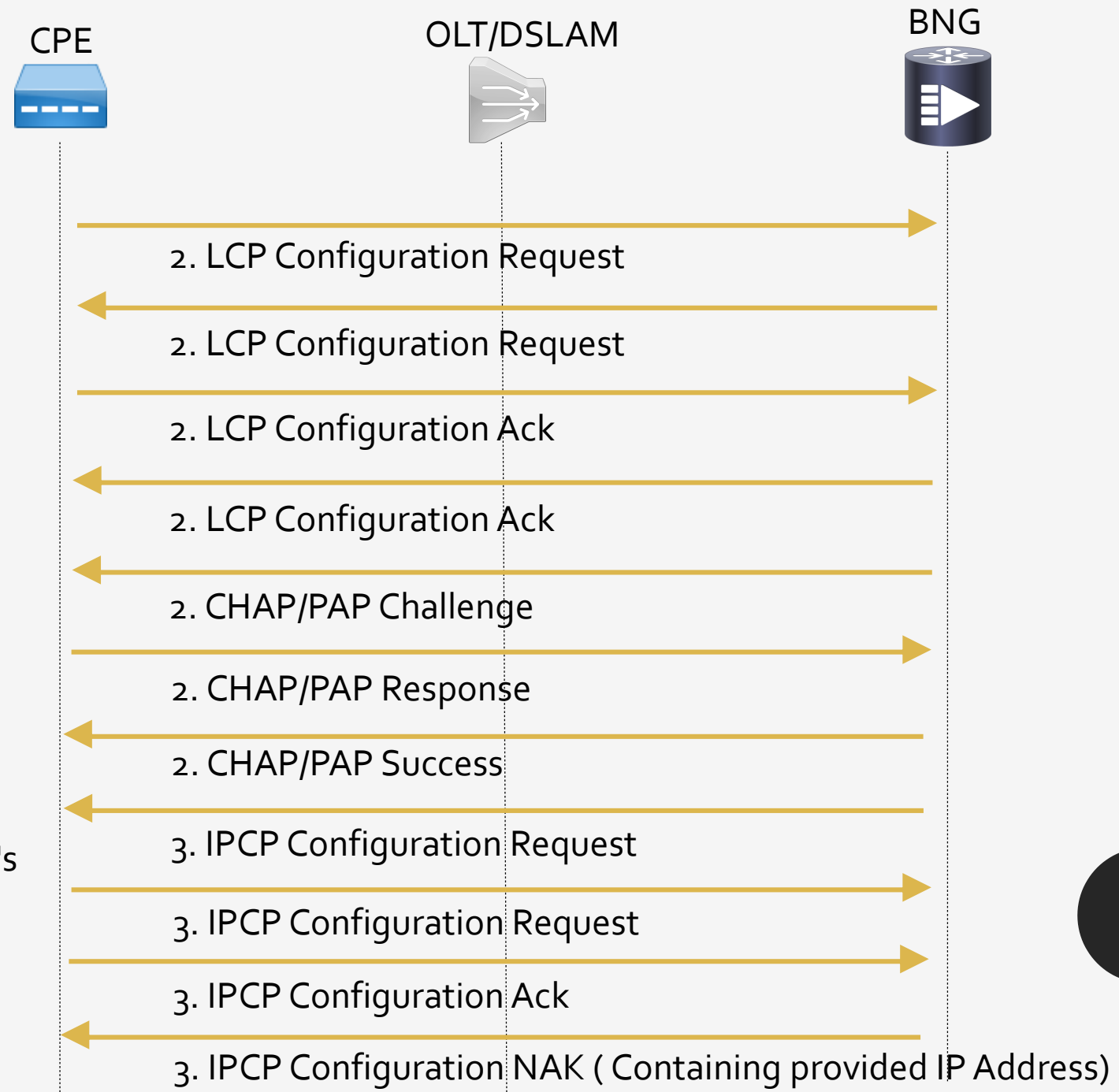
Session stage

- PPP normal operation (LCP,NCP(IPCP))

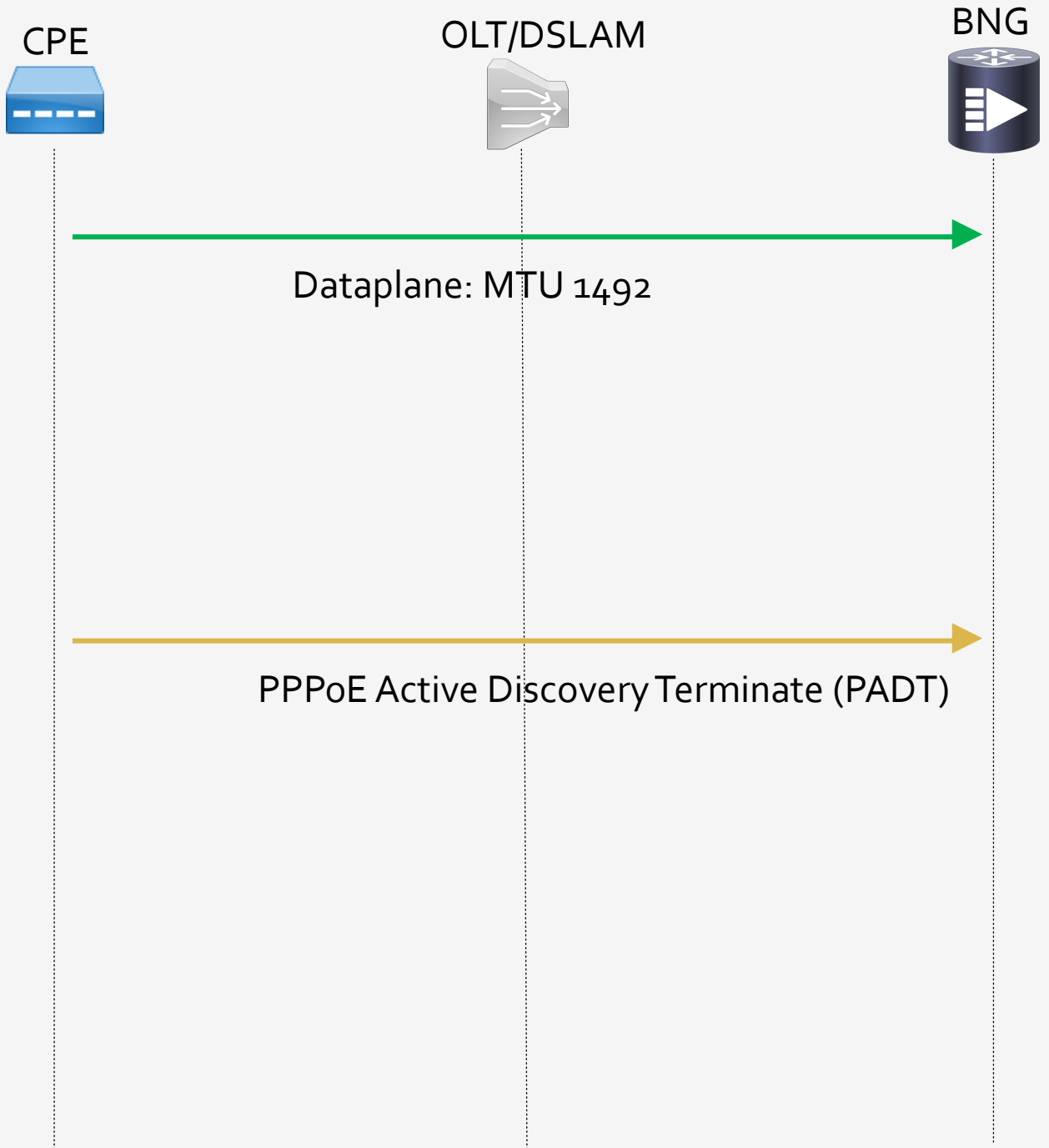
- data plane: each PPPoE Session ID attached to virtual access interface on BRAS/BNG

Ethertype : ox8864

After the PPPoE session has established,
- with Ethertype ox8864 and all the messages will include inside PPPOE header the session ID (and that's for PPP session stage and data plane)



PPPoE Call Flow



PADT (PPPoE Active Discovery Terminate): can send this message by PPPoE client or the PPPoE server to terminate the session.

Notes:

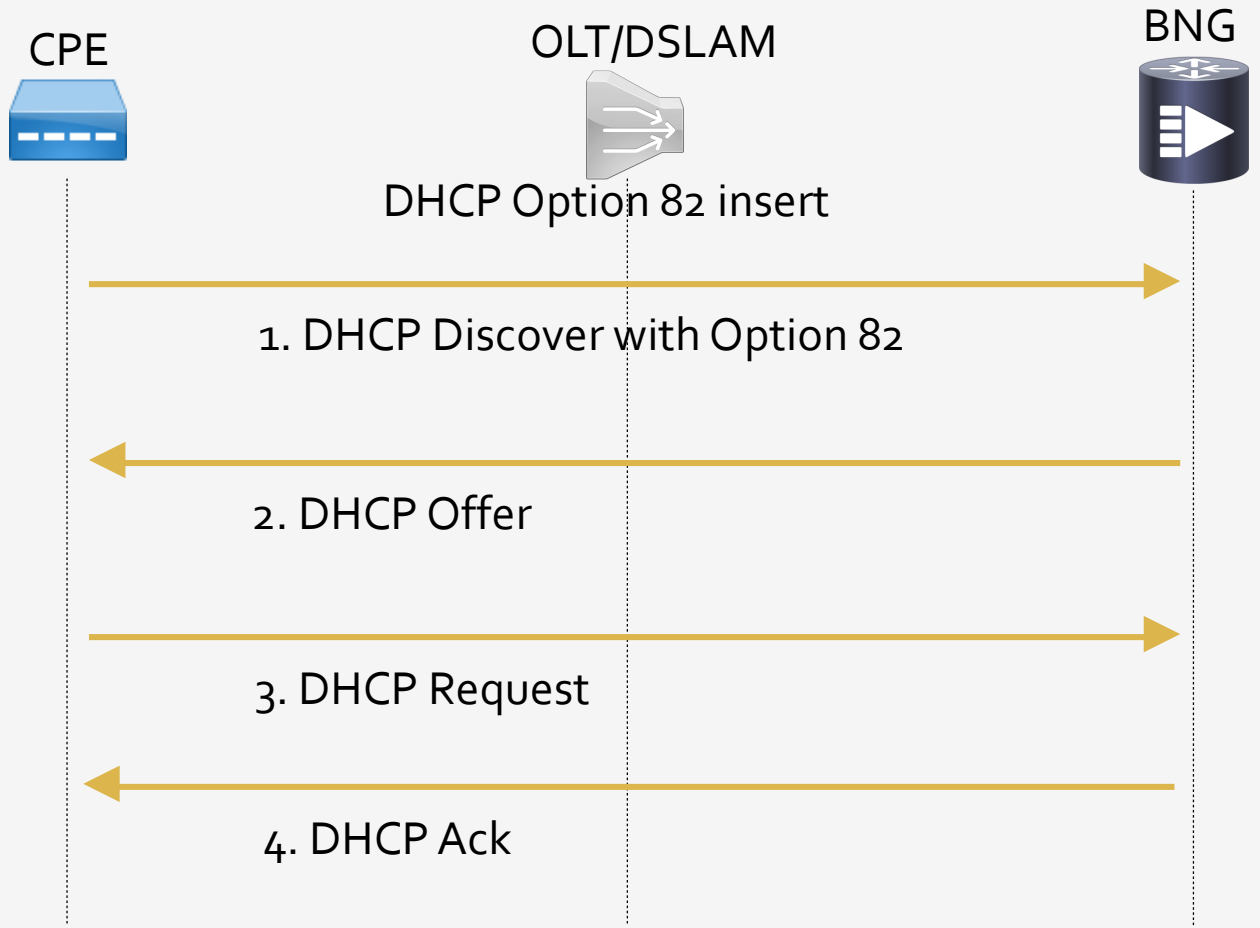
-maximum payload size for Ethernet is 1500 octets
- PPPoE header is 6 octets
- PPP protocol ID is 2 octets

So PPP maximum transmission unit (MTU) must not greater than (1500-8)=1492 bytes

IPoE

- IPoE is essentially DHCP-triggered subscriber interfaces.
- Users are "authenticated" through the use of DHCPv4/v6 **Option-82** inserting their Circuit-ID into their initial DHCP Discovery - this identifies the physical location of the user based on the tail that they are connected to (this would be done at an aggregation switch between the xPON network and whatever backhaul gets them to their ISP of choice).
- The ISP will then service the DHCP request (if the Circuit-ID can be mapped to a valid user via RADIUS), provide an IP (and hopefully prefix-delegation if they're offering IPv6) and then create a logical interface representing that subscriber that you they apply their filtering/rate-shaping to and start grabbing stats from.
- Session lifecycle based on DHCP Lease Tracking and Split Lease
- Authentication methods
    - DHCP Option82
    - DHCP Option 60
    - Vlan Encap

IPoE Call Flow



IPoE does not establish a session between the endpoints, and therefore does not have a unique, permanent subscriber identifier . Therefore, the IP address must be used to identify the subscriber, and steps must be taken to ensure that the IP address assigned to a subscriber does not change, or that the network adapts as the IP address changes .

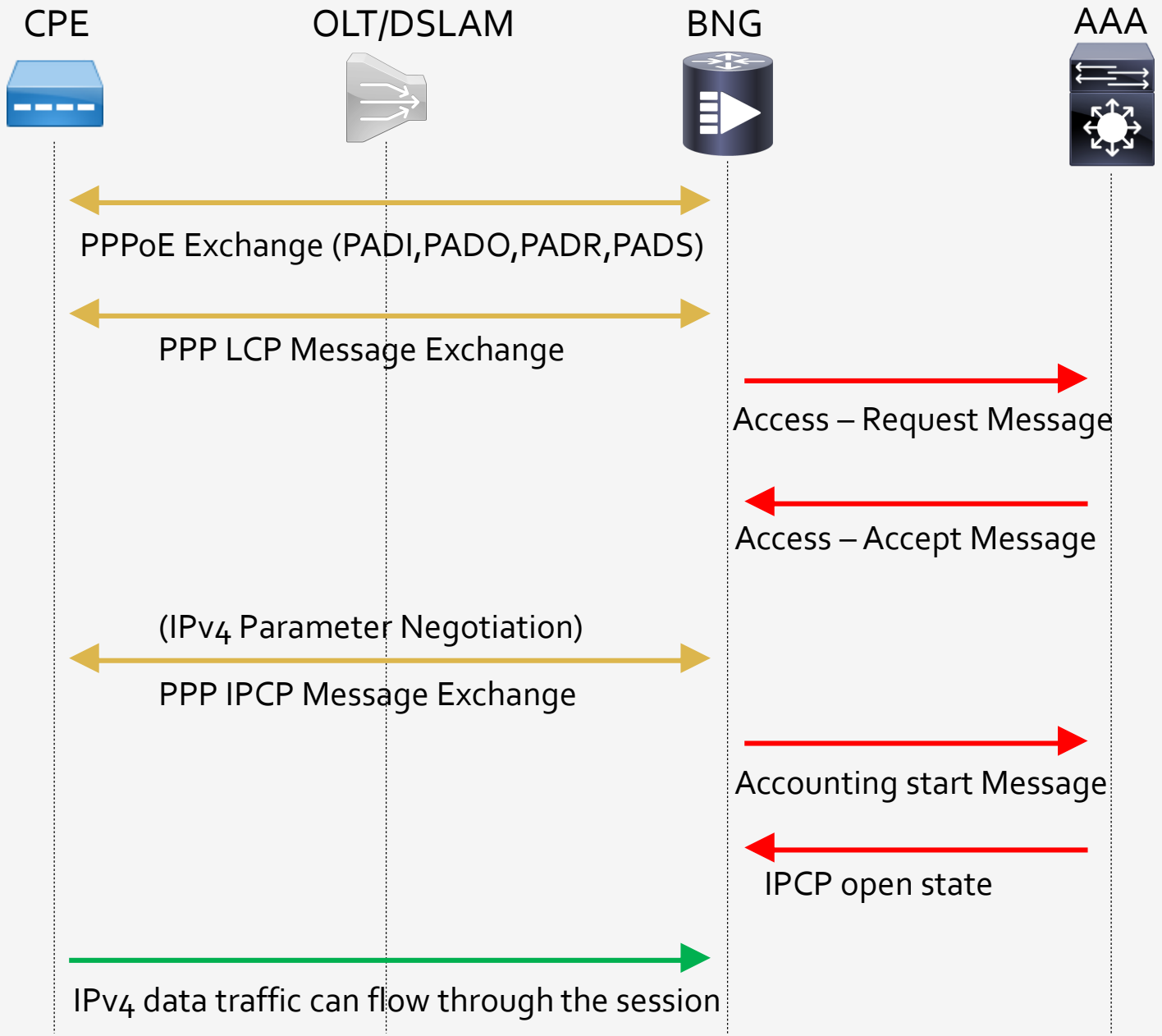
PPPoE vs IPoE

Feature	PPPoX	IPoE
Session Establishment	PPP session-identifier uniquely identifies subscriber connection	Connectionless—use IP address as customer identifier
Subscriber Authentication	Triggered by automated login using CHAP, PAP or other EAP-supported method	Triggered by incoming DHCP Discover packet
Authentication Server	RADIUS	DHCP (some implementations allow use of RADIUS)
Address Assignment	DHCP (with DHCP Relay) based on subscriber login	DHCP (with DHCP Relay), based on physical port, VLAN or VC
Monitoring	LCP echo commands provide Integrated keep-alive mechanism	Using DHCP Proxy allows DHCP lease renewal requests to function as keep-alive
Additional Strengths	Wholesale support; IPv6 support	Point to multipoint support
Additional Weaknesses	Overhead on each packet (8 bytes)	Re-authenticate whenever IP address changes. (Using DHCP Proxy mitigates this issue)

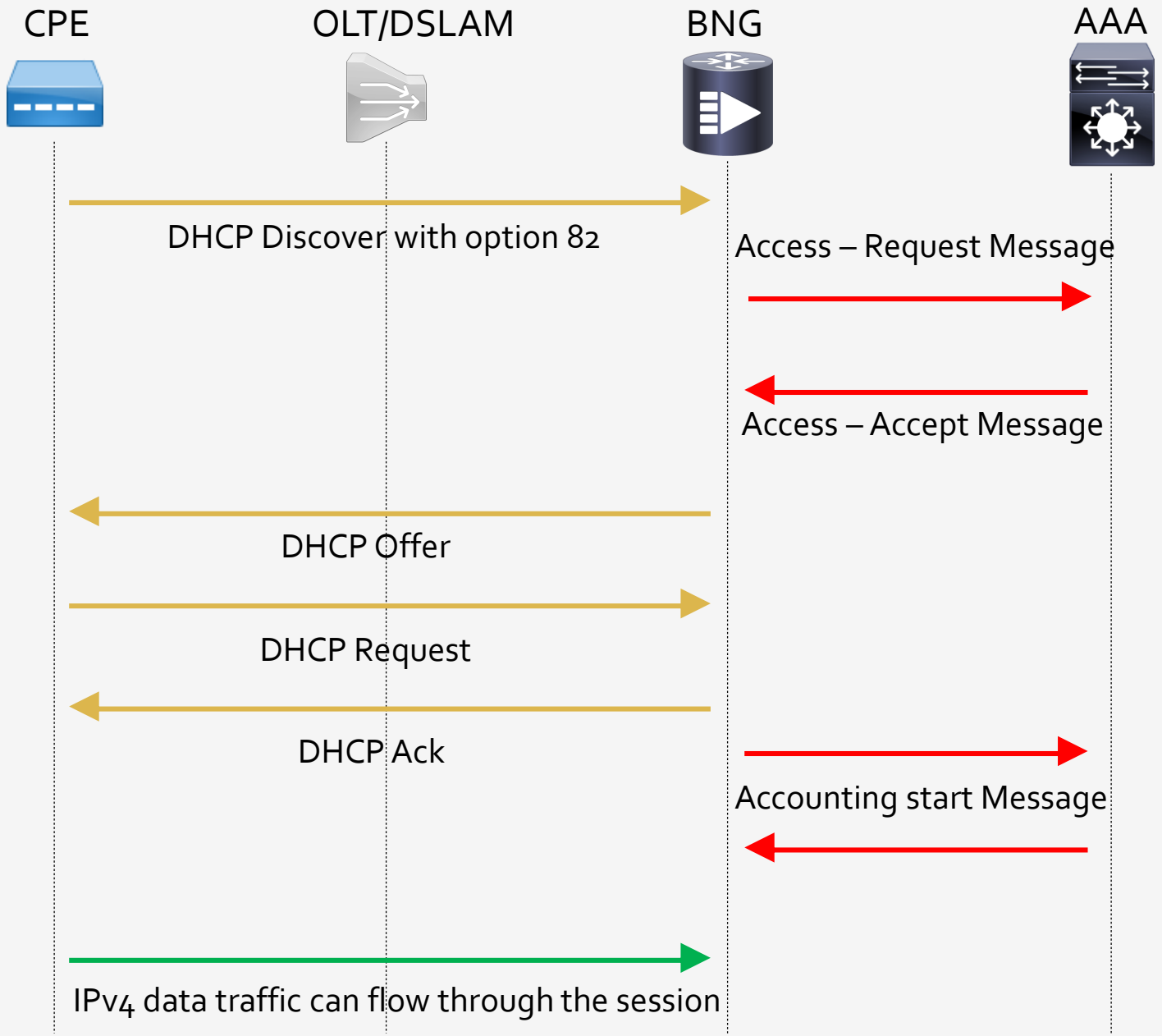
Interacting with the RADIUS Server

- BNG relies on an external Remote Authentication Dial-In User Service (RADIUS) server to provide subscriber Authentication, Authorization, and Accounting (AAA) functions. During the AAA process, BNG uses RADIUS to:
    - authenticate a subscriber before establishing a subscriber session
    - authorize the subscriber to access specific network services or resources
    - track usage of broadband services for accounting or billing
- The RADIUS server contains a complete database of all subscribers of a service provider, and provides subscriber data updates to the BNG in the form of **attributes** within RADIUS messages. BNG, on the other hand, provides session usage (accounting) information to the RADIUS server.
- BNG supports connections with more than one RADIUS server to have fail over redundancy in the AAA process. For example, if RADIUS server A is active, then BNG directs all messages to the RADIUS server A. If the communication with RADIUS server A is lost, BNG redirects all messages to RADIUS server B.
- During interactions between the BNG and RADIUS servers, BNG performs load balancing in a round-robin manner. During the load balancing process, BNG sends AAA processing requests to RADIUS server A only if it has the bandwidth to do the processing. Else, the request is send to RADIUS server B.

Interacting with the RADIUS Server



Interacting with the RADIUS Server



RADIUS MESSAGE TYPES

- **Access – Request**

  Authentication requests from NAS to server

- **Access – Challenge**

  Request from server to NAS, asking for additional info from user

- **Access – Accept**

  Response from server to NAS accepting the user session

- **Access – Reject**

  Response from server to NAS rejecting the user session

- **Accounting – Request**

  The NAS sends accounting information to the server

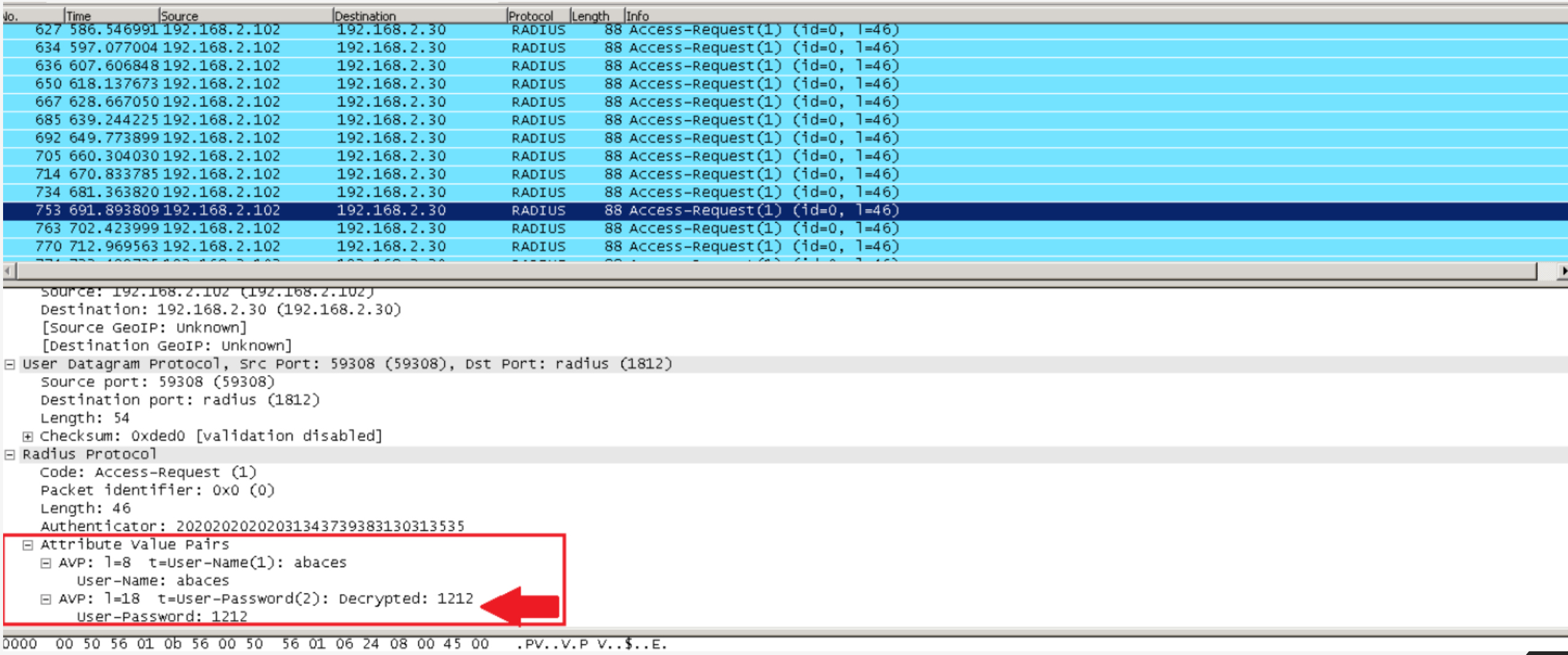
- **Accounting – Response**

  The server ACKs the acct packet to the NAS

RADIUS ATTRIBUTES

- Common Attributes (AVP)
  - User-Name
  - User-Password
  - NAS-IP-Address
  - NAS-Port
  - Service-Type
  - NAS-Identifier
  - Framed-Protocol
  - Vendor-Specific
  - Calling-Station-ID
  - Called-Station-Id

Range	Registration Procedures
1-191	IETF Review
192-240	Reserved for Private Use
224-240	Implementation Specific
241-246 (extended space, Unassigned)	IETF Review
241-246 (extended space, Reserved)	Standards Action
247-255	Reserved


No. Time Source Destination Protocol Length Info
627 586.546991 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
634 597.077004 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
636 607.606848 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
650 618.137673 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
667 628.667050 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
685 639.244225 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
692 649.773899 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
705 660.304030 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
714 670.833785 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
734 681.363820 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
753 691.893809 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
763 702.423999 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
770 712.969563 192.168.2.102 192.168.2.30 RADIUS 88 Access-Request(1) (id=0, l=46)
Source: 192.168.2.102 (192.168.2.102)
Destination: 192.168.2.30 (192.168.2.30)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 59308 (59308), Dst Port: radius (1812)
Source port: 59308 (59308)
Destination port: radius (1812)
Length: 54
Checksum: 0xded0 [validation disabled]
Radius Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 46
Authenticator: 20202020202031343739383130313535
Attribute Value Pairs
AVP: l=8 t=User-Name(1): abaces
User-Name: abaces
AVP: l=18 t=User-Password(2): Decrypted: 1212
User-Password: 1212
0000 00 50 56 01 0b 56 00 50 56 01 06 24 08 00 45 00 .PV..V.P V..$..E.

RADIUS ATTRIBUTES

IETF Attributes Versus VSAs

RADIUS Internet Engineering Task Force(IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server.

Because IETF attributes are standard, the attribute data is predefined and well known ; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

RADIUS vendor-specific attributes(VSAs) derived from one IETF attribute-vendor-specific(attribute26).

Attribute26 allows a vendor to create an additional255 attributes however they wish. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behindattribute26;thus, the newly created attribute is accepted if the user accepts attribute26.

Value	Description	Data Type	Reference
1	User-Name	text	[RFC2865]
2	User-Password	string	[RFC2865]
3	CHAP-Password	string	[RFC2865]
4	NAS-IP-Address	ipv4addr	[RFC2865]
5	NAS-Port	integer	[RFC2865]
6	Service-Type	enum	[RFC2865]
7	Framed-Protocol	enum	[RFC2865]
8	Framed-IP-Address	ipv4addr	[RFC2865]
9	Framed-IP-Netmask	ipv4addr	[RFC2865]
10	Framed-Routing	enum	[RFC2865]
11	Filter-Id	text	[RFC2865]
12	Framed-MTU	integer	[RFC2865]
13	Framed-Compression	enum	[RFC2865]
14	Login-IP-Host	ipv4addr	[RFC2865]
15	Login-Service	enum	[RFC2865]
16	Login-TCP-Port	integer	[RFC2865]
17	Unassigned		
18	Reply-Message	text	[RFC2865]
19	Callback-Number	text	[RFC2865]
20	Callback-Id	text	[RFC2865]
21	Unassigned		
22	Framed-Route	text	[RFC2865]
23	Framed-IPX-Network	ipv4addr	[RFC2865]
24	State	string	[RFC2865]
25	Class	string	[RFC2865]
26	**Vendor-Specific**	**vsa**	**[RFC2865]**
27	Session-Timeout	integer	[RFC2865]
28	Idle-Timeout	integer	[RFC2865]
29	Termination-Action	enum	[RFC2865]

Vendor Specific Attribute VSA(26)

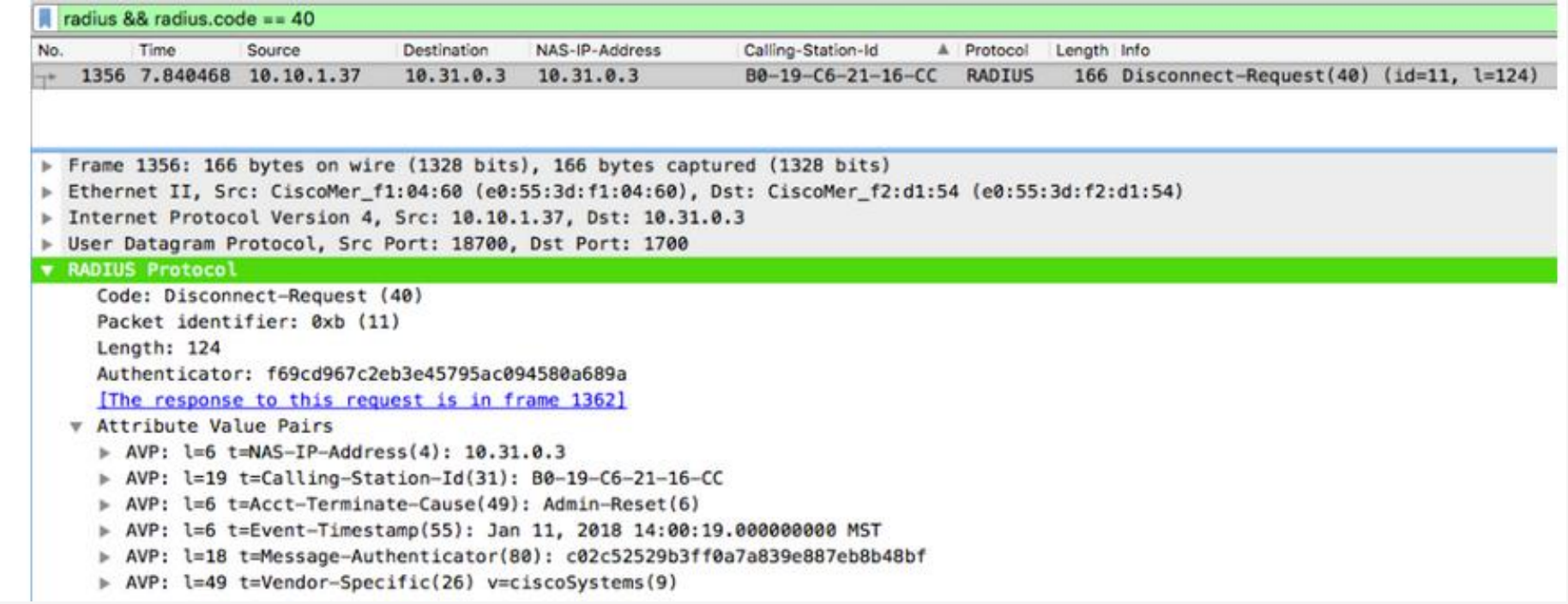
- Vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute(attribute26). Attribute26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.
- Attribute26 contains these three elements:
    - Type
    - Length
    - String(also known as data)
        - Vendor-ID
        - Vendor-Type
        - Vendor-Length
        - Vendor-Data

VSA(26) Cisco Vendor-ID 9 “cisco-avpair”

Name	Value	Type	Present in AAA message type
access-loop-encapsulation	binary	1	Access-accept, Accounting-request
accounting-list	string	1	Access-accept, CoA, Accounting-request
acct-input-gigawords-ipv4	integer	1	Accounting-request
acct-input-octets-ipv4	integer	1	Accounting-request
acct-input-packets-ipv4	integer	1	Accounting-request
acct-input-gigawords-ipv6	integer	1	Accounting-request
acct-input-octets-ipv6	integer	1	Accounting-request
if-handle	integer	1	Accounting-request
inacl	string	1	Access-accept
intercept-id	integer	1	Access-accept
ip-addresses	string	1	Access-request, Accounting-request
ipv4-unnumbered **Note** This AVPair is preferred for BNG in Cisco IOS XR Software, and it is equivalent to the ip-unnumbered AVPair in Cisco IOS Software.	string	1	Access-accept
ipv6_inacl	string	1	Access-accept, CoA
ipv6_outacl	string	1	Access-accept, CoA

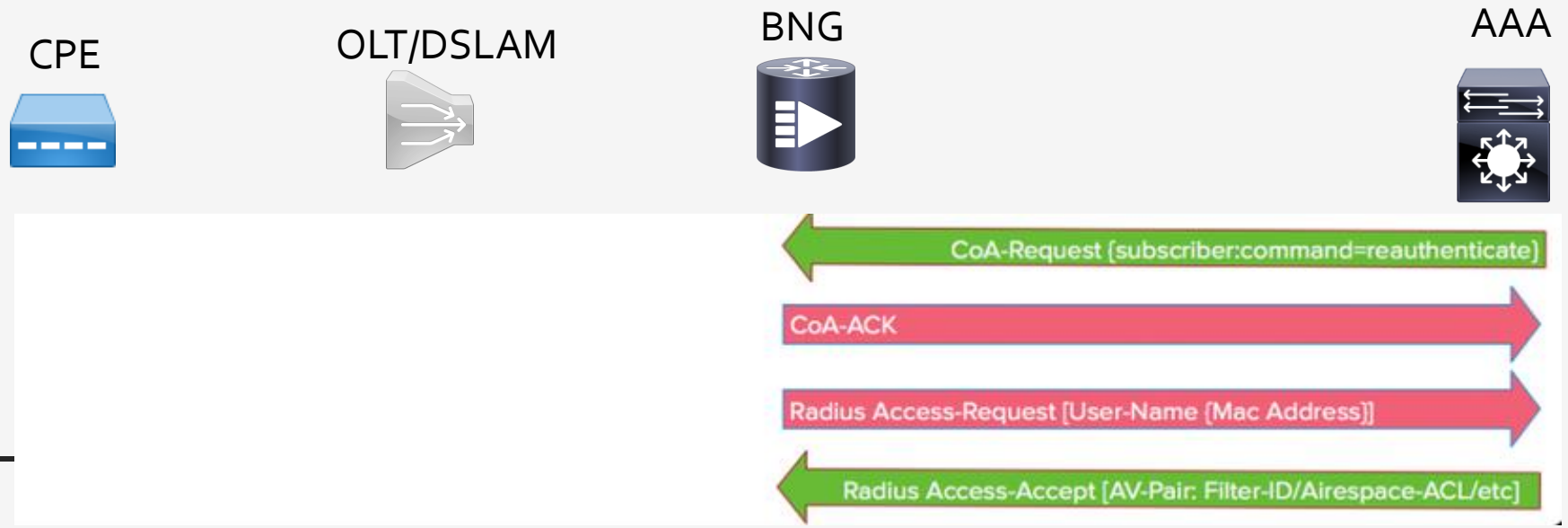
RADIUS AVP	Value	Type	Action
subscriber:command=account-logon	string	1	account logon
subscriber:command=account-logoff	string	1	account logoff
subscriber:command=account-update	string	1	account update
subscriber:sa=<service-name>	string	1	service activate
subscriber:sd=<service-name>	string	1	service de-activate

VSA(26) Cisco Vendor-ID 9 "cisco-avpair"

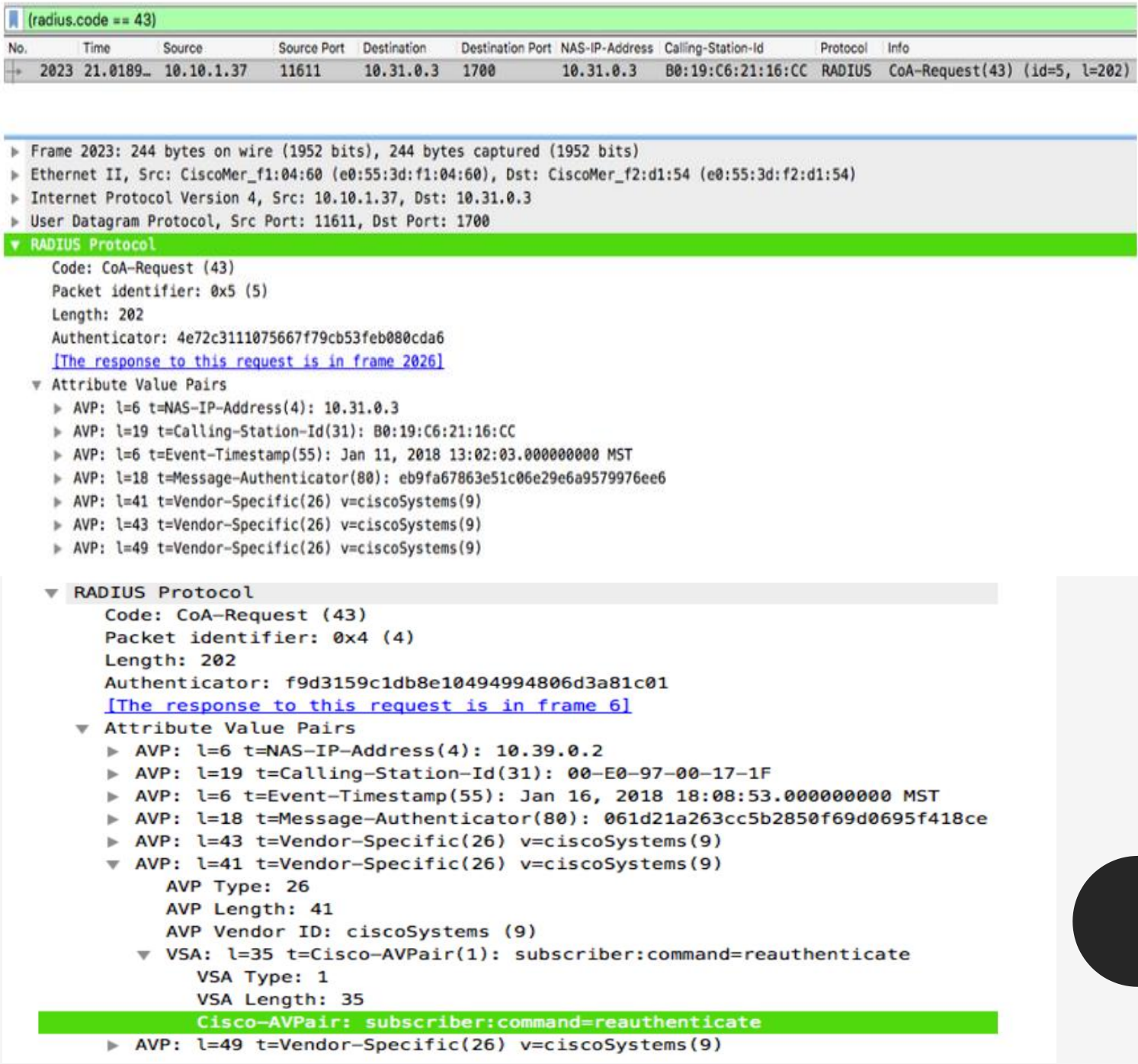


RADIUS CoA (Change of Authorization)

- RADIUS Change of Authorization (RFC 3576 & RFC 5176) Allows a RADIUS server to send unsolicited messages to the Network Access Server (aka Network Access Device/Authenticator e.g. BNG) to change the connected client's authorized state.
- This could mean anything from disconnecting the client, to sending different attribute value pairs to the Authenticator to change the device's VLAN/ACL and more.



RADIUS CoA (Change of Authorization)



BNG Configuration Process

- Configuring RADIUS Server
- Activating Control Policy
- Establishing Subscriber Sessions
- Deploying QoS
- Configuring Subscriber Features
- Verifying Session Establishment

Lab Session

- TBC