



Technical Report

TR-497

Public Wi-Fi user authentication and data local forwarding technical requirements

Issue: 01

Issue Date: June 2024

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
01	June 2024	Bo Gao, China Telecom Lei Zhou, New H3C	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor: Bo Gao, China Telecom
Lei Zhou, New H3C

Work Area Director(s): David Sinicrope, Ericsson
Jonathan Newton, Vodafone

Project Stream Leader(s): Jonathan Newton, Vodafone

Table of Contents

Executive Summary	7
1 Purpose and Scope	8
1.1 Purpose	8
1.2 Scope	8
2 References and Terminology	9
2.1 Conventions	9
2.2 References	9
2.3 Definitions	10
2.4 Abbreviations	11
3 Technical Report Impact	12
3.1 Energy Efficiency	12
3.2 Security	12
3.3 Privacy	12
4 Networking Architecture	13
4.1 AP access AC through Internet	13
4.2 AP access AC through Dedicated Line	14
4.3 AP access AC pool through dedicated line	15
4.4 Call Flows	16
4.4.1 AP Access AC through Internet	16
4.4.2 AP access AC through a dedicated VLAN	18
4.4.3 AP Access AC Pool through Dedicated Line	19
5 User Authentication	21
5.1 Portal Authentication	21
5.1.1 User Address Assignment	21
5.1.2 AC Redirect Portal Authentication	22
5.1.3 AP Redirect Portal Authentication	25
5.1.4 Users Are Offline Normally	27
5.1.5 The User Is Offline Abnormally	27
5.2 802.1X Authentication	29
5.2.1 PEAP Authentication	29
5.2.2 EAP-SIM/AKA Authentication	33
6 Nodal Requirements	35
6.1 AP Requirements	35
6.2 AC Requirements	36
6.3 APADS Requirements	38
6.4 Portal Server Requirements	38
6.5 AAA Server Requirements	38

Table of Figures

Figure 1 AP access AC network through the Internet	13
Figure 2 AP accessing AC through dedicated line	14
Figure 3 AP access AC pool through dedicated line	15
Figure 4 Call flow of AP accessing AC through Internet	17
Figure 5 Call flow of AP accessing AC through dedicated line	18
Figure 6 Call flow of assigning AC to AP	19
Figure 7 Call flow of AP access AC pool through dedicated line	20
Figure 8 Call flow of Gateway assigns IP address for EUD	21
Figure 9 Call flow of AC assigns IP address for EUD	22
Figure 10 AC is responsible for redirecting the Portal authentication call flow	24
Figure 11 AP is responsible for redirecting the Portal authentication process	26
Figure 12 User's normal offline detection process	27
Figure 13 Detection process of abnormal offline users on the wired side	28
Figure 14 Detection flow of abnormal offline user at the air interface side	28
Figure 15 PEAP authentication call flow	30
Figure 16 User-initiated offline	31
Figure 17 AAA-initiated offline	32
Figure 18 User abnormal offline call flow	32
Figure 19 EAP-SIM authentication call flow	33
Figure 20 EAP-SIM authentication call flow	34

Table of Tables

Table 1 AP requirements for different authentication scenarios.....	36
Table 2 AC requirements for different authentication scenarios	37
Table 3 APADS requirements for different authentication scenarios	38
Table 4 Portal Server requirements for different authentication scenarios	38
Table 5 AAA Server requirements for different authentication scenarios	39

Executive Summary

This document defines the network architecture and technical requirements for Wi-Fi users to be authenticated by access controller (AC) and local forwarding of user data, so that Wi-Fi devices developed by device manufacturers can meet the requirements of Wi-Fi networking and operation requirements. This document is to focus on the requirements and use case aligned and complementary to TR-321.

According to the deployment location of AC defined in Section 4 of this document, this document defines three architectural models for the access point (AP) to connect to the AC:

- 1: AP accesses AC network through the Internet;
- 2: AP accesses AC through dedicated line;
- 3: AP accesses AC pool through dedicated line.

Based on the three Wi-Fi networking architectures, the call flows for AP accesses to AC are defined respectively to meet the networking mode in which Wi-Fi user traffic is forwarded locally and users are centrally managed by AC.

Two Wi-Fi user authentication methods are specified: Portal authentication and 802.1X authentication. Portal authentication includes both AP redirection and AC redirection. 802.1X authentication includes PEAP authentication and EAP SIM/AKA authentication.

This document specifies the requirements for each network element including AC, AP, Access Point Address Distribution System (APADS), AAA server & Portal Server for each Wi-Fi architecture model and user authentication method.

1 Purpose and Scope

1.1 Purpose

This document aims to define the network architecture and technical requirements for Wi-Fi users to be uniformly authenticated by AC and local forwarding of user data, so that Wi-Fi devices developed by device manufacturers can meet the requirements of Wi-Fi networking and operation requirements. This document is to focus on the requirements and use case aligned and complementary to TR-321.

1.2 Scope

This document extends TR-321 architecture 3 (Distributed AC Architecture) to allow users to be authenticated and managed at the AC, but adding support for user data to be forwarded locally.

The following three aspects are within the scope of this document:

Networking scenarios:

1. The AC is deployed on the core of the metropolitan area network connected to the AP through the Internet.
2. The AC is deployed on the edge of the metropolitan area network or on the access network side connected to the AP via dedicated lines.

User authentication operation process related the following use cases:

1. User address allocation operation process.
2. User association process.
3. User online operation process.
4. User offline operation process.

Device functional requirement:

1. AP functional requirement
2. AC functional requirement
3. APADS functional requirement
4. AAA functional requirement
5. Portal server functional requirement

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found in RFC 2119.

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-101	<i>Migration to Ethernet-Based Broadband Aggregation</i>	BBF	2006
[2] TR-321	<i>Public Wi-Fi Access in Multi-service Broadband Networks</i>	BBF	2015
[3] 802.1Q	<i>Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11</i>	IEEE	2009
[4] 802.1X	<i>Port-Based Network Access Control</i>	IEEE	2020
[5] 802.11i	<i>Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements</i>	IEEE	2004
[6] RFC1994	<i>PPP Challenge Handshake Authentication Protocol (CHAP)</i>	IETF	1996

[7]	RFC2131	<i>Dynamic Host Configuration Protocol</i>	IETF	1997
[8]	RFC2516	<i>A Method for Transmitting PPP Over Ethernet (PPPoE)</i>	IETF	1999
[9]	RFC2759	<i>Microsoft PPP CHAP Extensions</i>	IETF	2000
[10]	RFC2865	<i>Remote Authentication Dial In User Service (RADIUS)</i>	IETF	2000
[11]	RFC3748	<i>Extensible Authentication Protocol (EAP)</i>	IETF	2004
[12]	RFC4186	<i>Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)</i>	IETF	2006
[13]	RFC4187	<i>Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)</i>	IETF	2006
[14]	RFC5176	<i>Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)</i>	IETF	2008
[15]	RFC5246	<i>The Transport Layer Security (TLS) Protocol</i>	IETF	2008
[16]	RFC5415	<i>Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification</i>	IETF	2009
[17]	RFC5416	<i>IEEE Standard for Local and metropolitan area networks-Bridges and Bridged Networks</i>	IETF	2014

2.3 Definitions

The following terminology is used throughout this Technical Report.

Term	Definition
Access controller (AC)	The network entity that provides wireless termination point access to the network infrastructure in the data plane, control plane, and management plane
Business gateway	Gateway is used for business network to connect WAN network
Business rules	Business rules refer to a set of EUD-related information that the AC sends to the AP after the EUD authentication has been passed. This information includes the EUD authentication success notification, the EUD rate limit, the forwarding method (whether it's local forwarding or centralized forwarding), VLAN information, and more. In essence, business rules are the collective term for the EUD-related information that the AC issues to the AP
Gateway	Gateway in this document includes Business Gateway and Residential Gateway
Portal server	Web site or an app that enables user authentication through web pages.
Detection message	A detection message is a type of TCP message (TCP keep alive) that the Portal server periodically sends to the End User Device (EUD) after the user Portal authentication is successful. This message prompts a reply from the EUD, enabling the Portal server to determine whether the EUD is online Note: TCP Keep Alive is defined in the IETF RFC 1122, section 4.2.3.6, "TCP Keep-Alives".
Heartbeat information	Portal Server's detection messages and EUD's reply messages are collectively referred to as heartbeat information

Residential gateway	Gateway is used for home network to connect WAN network
Wi-Fi Hotspot	A site that offers public access to packet data services (e.g., the Internet) via a Wi-Fi access network

2.4 Abbreviations

This Technical Report uses the following abbreviations:

Term	Definition
AAA	Authentication, Authorization, Accounting
APADS	Access Point Address Distribution System
AC	Access Controller
AP	Access Point
BNG	Broadband Network Gateway
CAPWAP	Control and Provisioning of Wireless Access Points
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EUD	End User Device (Refer to TR-321)
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NM	Network Management
MAC	Media Access Control
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PPPoE	Point-to-Point Protocol Over Ethernet
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

3 Technical Report Impact

3.1 Energy Efficiency

This document proposes several AP access AC methods and AC deployment mode of Wi-Fi network architecture. Therefore, the impact on energy consumption will vary. In the network architecture where AC is centrally deployed to form an AC pool, the total number of ACs is expected to decrease. This provides an opportunity to reduce the overall power consumption of the network.

3.2 Security

This document addresses user authentication which has implications for network security. User authentication mechanisms in this document ensure authorized users can access the Internet and unauthorized users aren't allowed to access the internet. The following security mechanisms are implemented during the authentication process defined in this document:

1. IEEE 802.11i can be used for port authentication to ensure the security of data transmission.
2. The PEAP authentication process uses a TLS tunnel to protect the username and password during the user authentication process. (Refer to IETF RFC 2759).
3. EAP-SIM/AKA Authentication is used for generating air interface encryption parameters to protect the security of the data transmission. (Refer to IETF RFC 3748 and RFC 4186).

These above mechanisms help improve security and reduce potential malicious attacks on the subscriber.

3.3 Privacy

Any issues regarding privacy are not affected by TR-497.

4 Networking Architecture

Depending upon the deployment location of the AC defined in Section 4 of this document, there are two methods for the AP to access the AC:

1. The AC is deployed in the cloud, and the AP accesses the AC through the Internet;
2. The AC is deployed on the access network. For example, AC is attached to the BNG, and the AP accesses the AC through a dedicated line.

4.1 AP access AC through Internet

The gateway (supporting NAT optionally) is deployed at the hotspot, and the gateway accesses the BNG through the access network. The AP is deployed at the hotspot and connected to the gateway. The AP has been pre-configured with AC's address or domain name. The AC is deployed in the cloud and can be accessed through the internet. See Figure 1.

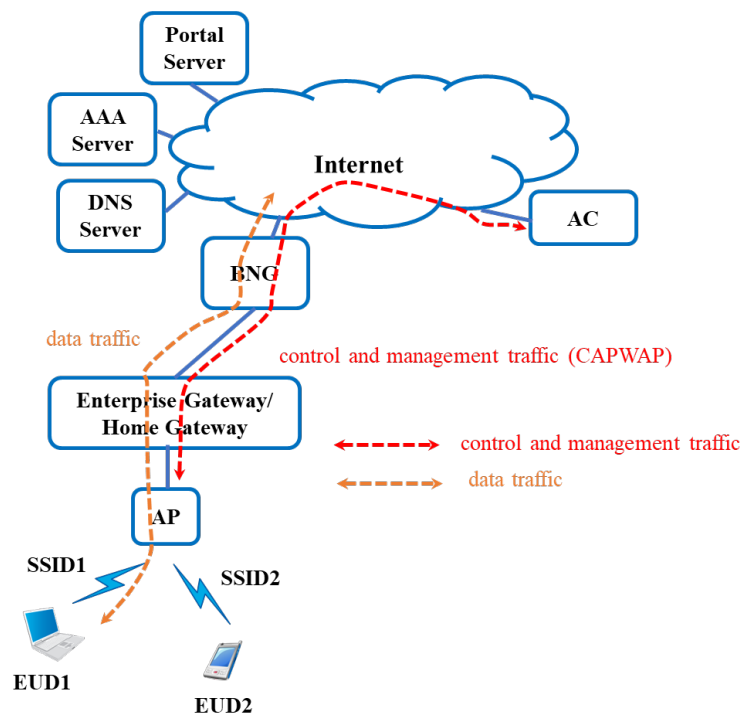


Figure 1 AP access AC network through the Internet

The main process is as follows:

1. The gateway connects to the BNG by PPPoE and is assigned an IP address through standard broadband procedures such as those defined in TR-10.
2. After the gateway is assigned an IP address, the gateway can access the Internet.
3. After the AP is powered on, the AP sends a DHCP request to the gateway.
4. The gateway assigns a private IP address to the AP, and the AP can access the Internet. Note: the gateway is responsible for NAT conversion of the AP private network address.
5. The AP obtains the AC IP address according to the pre-configured AC IP address in AP or through the pre-configured AC domain name in AP. Then the AP communicates with the AC to establish a CAPWAP tunnel.
6. The AC sends the configuration to the AP by CAPWAP, and the AP configures its parameters according to the received configuration refer to IETF RFC 5415.
7. The AP broadcasts the specified SSID in the configuration.
8. The Wi-Fi EUD associates with the specified SSID.

9. The AP management traffic and control traffic are tunneled to the AC through CAPWAP; the user's data traffic is transmitted from the AP to the Internet through the gateway. The user data passes through the BNG to the Internet without transiting through the AC.

4.2 AP access AC through Dedicated Line

The AP is deployed at the hotspot, and the AP accesses the BNG through the access network. Each AP is assigned a specified management VLAN and data VLAN in advance. Control and management traffic is transmitted in the management VLAN, and data traffic is transmitted in the data VLAN. These two VLANs are between the AP and the BNG.

The AC is connected to the BNG directly, or through an Ethernet Network. AC access Internet, Portal Server, and AAA Server through the BNG. The AC has a built-in DHCP server, which is responsible for allocating private IP addresses for the AP, and at the same time, sending AC addresses to the AP through the DHCP Option field. See Figure 2.

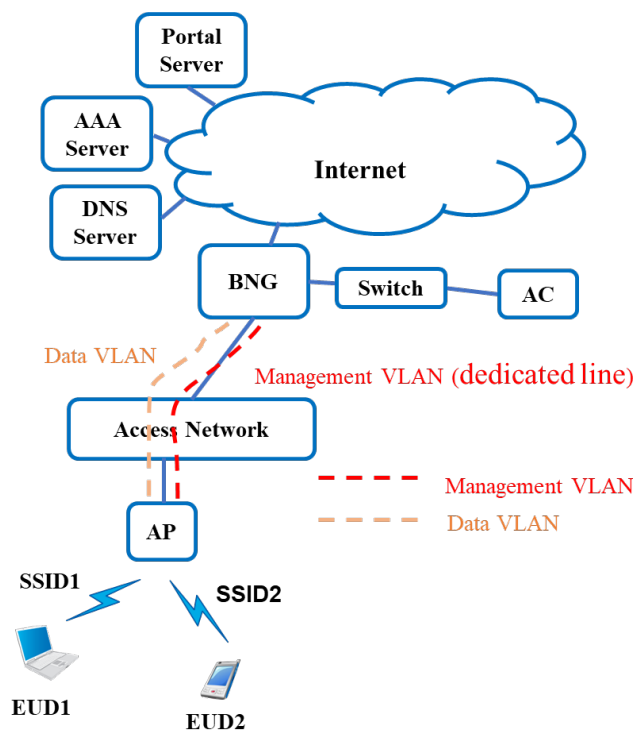


Figure 2 AP accessing AC through dedicated line

In order for the AP management traffic to be routed to the AC, firstly the management traffic is sent on the dedicated management VLAN, then the BNG will route the AP management traffic to the AC.

The main process is as follows:

1. The AP initiates a DHCP request.
2. The BNG relays the DHCP request to the AC.
3. The AC (with a built-in DHCP server) sends DHCP reply with the AC's IPv4 only or IPv6 address only or both IPv4 address and IPv6 address specified in RFC 4517 in the DHCP Options to the AP. The AP communicates and registers with the AC according to the AC address received via DHCP (refer to RFC5417). AP and AC establish CAPWAP tunnel.
4. The AC sends the configuration to the AP through CAPWAP tunnel, which is applied by the AP.
5. The AP broadcasts the specified SSID in the configuration.

6. The Wi-Fi EUD associates with the specified SSID.
7. The AP management traffic and control traffic are tunneled to the AC through CAPWAP. The user's data traffic is transmitted from the AP to the Internet through the BNG. The user data passes through the BNG to the Internet without transiting through the AC.

Note1: Step 3 For the IPv4 DHCP Option field of the AC, see Chapter 2 of IETF RFC 5417.

Note2: Step 3 For the IPv6 DHCP Option field of the AC, see Chapter 3 of IETF RFC 5417.

4.3 AP access AC pool through dedicated line

The AP is deployed at the hotspot, and the AP accesses the BNG through the access network. Each AP is assigned a specified management VLAN and data VLAN in advance. The management VLANs of different APs can be the same or different, and the data VLANs of different APs can be the same or different. That is, a VLAN may be dedicated to one AP, or shared among multiple Aps. Control and management traffic is transmitted in the management VLAN, and data traffic is transmitted in the data VLAN. These two VLANs are between AP and the BNG.

The AC is centrally deployed to form an AC pool. Each BNG is connected to the AC pool through the switch, so that each the AC and the BNG can communicate with each other and the AP can flexibly access any AC in the AC pool. The AP Address Distribution System (APADS) is connected to the switch to assign IP addresses and AC addresses to the online APs. See Figure 3.

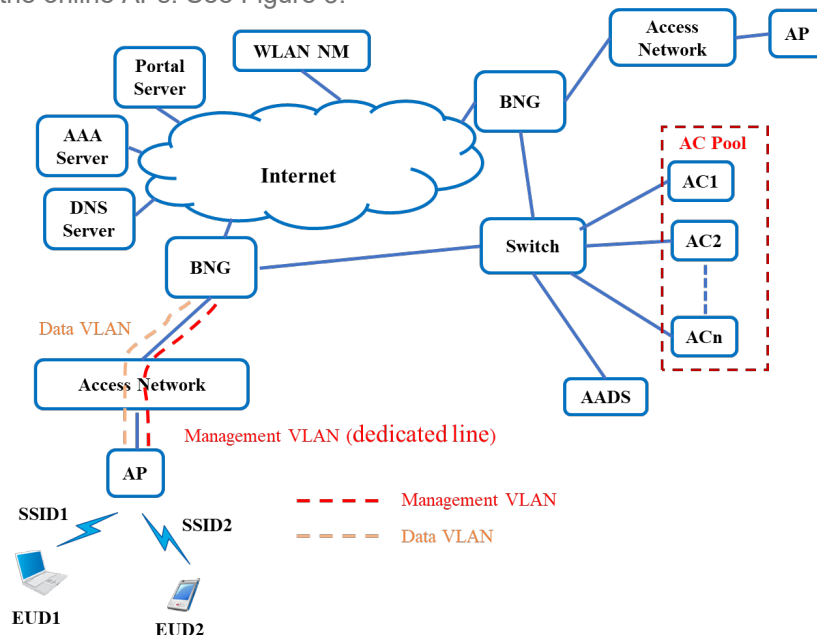


Figure 3 AP access AC pool through dedicated line

WLAN Network Management (NM) selects the appropriate AC for the AP according to comprehensive factors such as the number of APs accessed by each AC in the AC pool, the number of users accessed, and the CPU utilization of the AC. The corresponding relationship between the AP attribute information and the pre-allocated AC information is used as the configuration data and distributed to the APADS for keeping the two in sync with each other. The AP in the configuration data is called the registered AP. The configuration data includes AP attribute information and AC information, wherein the AP attribute information includes the MAC address and a serial number of the AP; The AC information includes the AC address list (the IP address of the primary AC and the IP addresses of the standby ACs). At the same time, the WLAN NM sends the AP attribute information to the corresponding AC.

AC accesses the Internet, Portal Server, AAA Server and WLAN NM through the BNG. The APADS is responsible for assigning private IP network addresses to the AP, and carrying AC addresses specified in RFC 4517 in the DHCP Options to the AP.

According to pre-configured AP's management VLAN, the BNG relays the AP's DHCP packets to APADS. Communication between the AP and the APADS as well as between the AP and the AC is forwarded through the BNG by routing.

The main process is as follows:

1. The AP sends a DHCP request, DHCP request contains AP attribute information: AP MAC address and serial number.
2. The BNG relays the DHCP request to the APADS.
3. The APADS receives the DHCP packets relayed by the BNG and analyzes the AP attribute information, that is, the MAC address and a serial number of the AP
4. The APADS compares the attribute information of the resolved AP with the attribute information of the AP registered in the configuration data. There are three comparison methods as follows, and one of them is selected for comparison according to needs: 1) The MAC addresses of two APs are used for comparison; 2) The serial numbers of two APs are used for comparison; 3) The MAC addresses of the two APs are used in combination with the serial numbers for comparison.
5. If the APADS successfully compares the received AP attribute information with the registered AP attribute information in the configuration data, that is, the received AP is a registered AP. Then the AC information corresponding to the registered AP is obtained from the configuration data, that is, the AC address list. If the comparison fails, the AP received by the APADS is a non-registered AP.
6. For a registered AP that is successfully matched, the APADS assigns a private IP network address to the AP, and sends the AC addresses list to the AP in the DHCP Options field. For non-registered APs that fail to match, the APADS discards the received DHCP Request message, or assigns the implementation-specified IP address to prevent the non-registered APs from repeatedly sending DHCP Request messages.
7. The AP communicates and registers with the AC according to the AC address received. AP and AC establish the CAPWAP tunnel.
8. The AC sends the configuration to the AP through CAPWAP tunnel, and the AP configures itself with this configuration accordingly.
9. The AP broadcasts the specified SSID in the configuration.
10. The Wi-Fi EUD associates with the specified SSID.
11. The AP management traffic and control traffic are tunneled to the AC through CAPWAP. The user's data traffic is transmitted from the AP to the Internet through the BNG. The user data passes through the BNG to the Internet without transiting through the AC.

4.4 Call Flows

4.4.1 AP Access AC through Internet

The networking of AP accessing AC through the Internet is shown in Figure 1. The gateway can access the Internet by obtaining the IP address assigned by the BNG. After obtaining the private network IP address from the gateway through DHCP, the AP accesses the Internet through the gateway. The AP communicates with the AC deployed in the cloud and establishes a CAPWAP tunnel. Figure 4 is a call flow of AP access AC through the Internet.

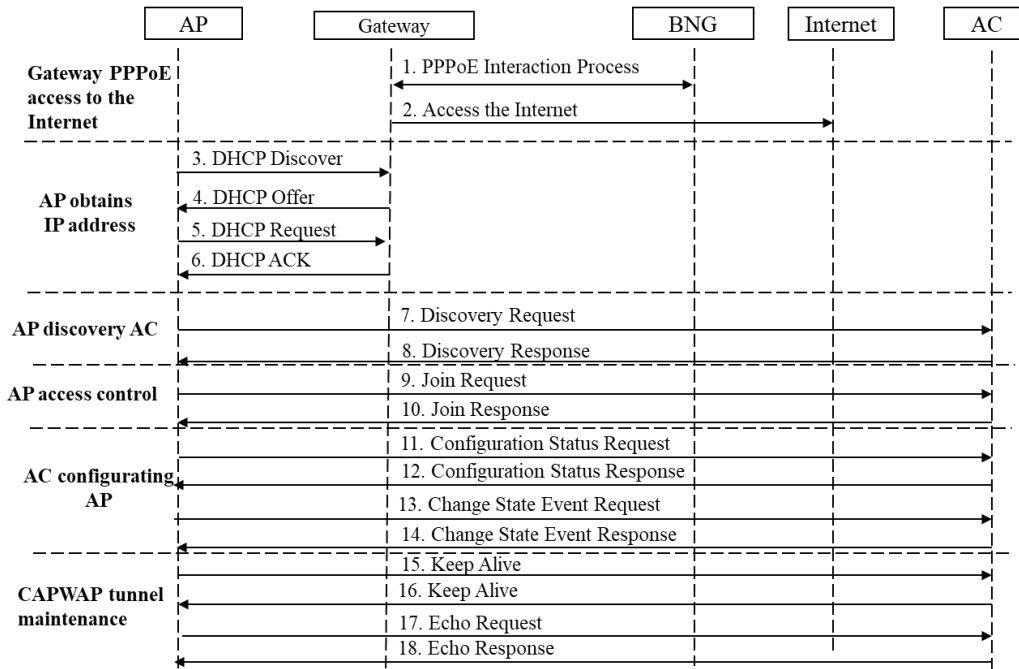


Figure 4 Call flow of AP accessing AC through Internet

1. The gateway sends a PPPoE request to the BNG. After the PPPoE authentication is successful, the BNG assigns an IP address to the gateway.
2. The gateway can access the Internet after obtaining an IP address.
3. The AP sends a DHCP Discover to the gateway.
4. The gateway replies with a DHCP Offer.
5. The AP sends a DHCP Request.
6. The gateway replies with DHCP ACK. Through steps 3 to 6, the AP obtains the private network IP address allocated by the gateway.
7. The AP sends a Discovery Request to the AC.
8. The AC replies a Discovery Response to the AP. In steps 7 to 8, the AP discovers the AC.
9. The AP sends a Join Request to the AC.
10. The AC replies Join Response to the AP. In steps 9 to 10, the AP joins the AC.
11. The AP sends a Configuration Status Request to the AC.
12. The AC replies Configuration Status Response to the AP.
13. The AP sends a Change State Event Request to the AC.
14. The AC replies Change State Event Response to the AP. In steps 11 to 14, the AC sends the configuration to the AP.
15. The AP sends Keep Alive to the AC.
16. The AC sends Keep Alive to the AP.
17. The AP sends an Echo Request to the AC.
18. The AC replies Echo Response to the AP. In steps 15 to 18, the CAPWAP tunnel between the AP and the AC is maintained.

Note1: Refer to IETF RFC2516 for the process of steps 1.

Note2: Refer to IETF RFC2131 for the process of steps 3 to 6.

Note3: Refer to IETF RFC5415 for the process of steps 7 to 18.

4.4.2 AP access AC through a dedicated VLAN

See Figure 2 for the networking of AP accessing AC through a dedicated line. After the AP is powered on, it initiates a DHCP request. The BNG relays the DHCP request of the AP to the AC according to the management VLAN configured by the AP. The AC (with a built-in DHCP server) assigns a private IP network address to the AP and sends the AC's address to the AP through the DHCP Option. The AP communicates with the AC according to the obtained AC address and establishes a CAPWAP tunnel. **Figure 5** is a call flow of AP accessing AC through dedicated line.

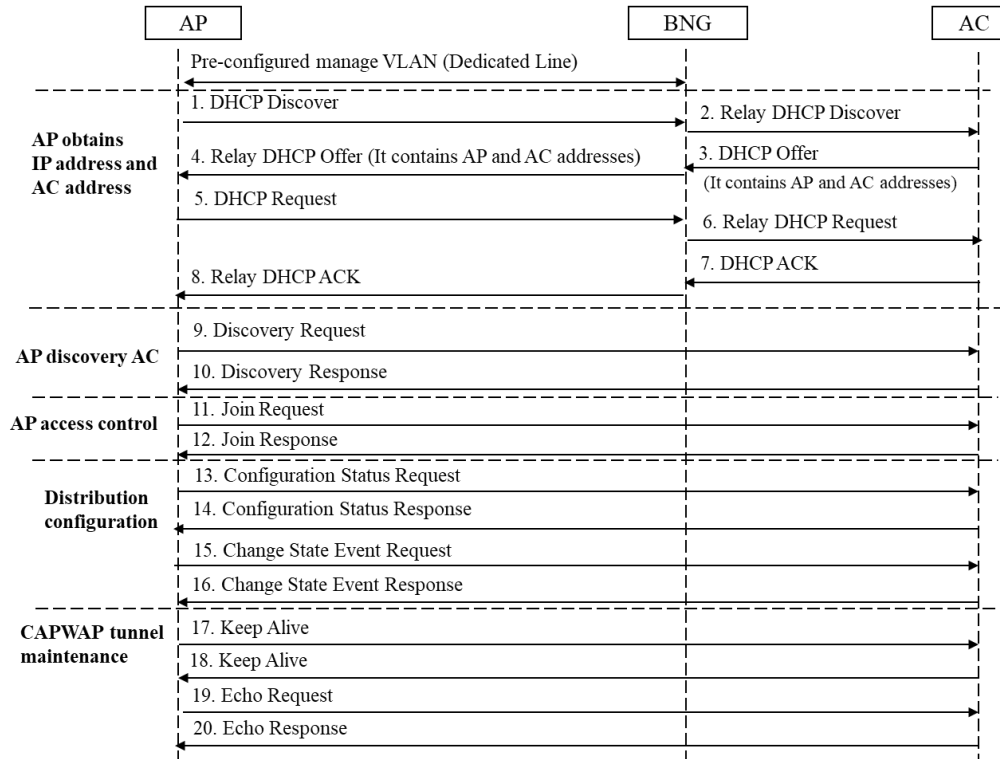


Figure 5 Call flow of AP accessing AC through dedicated line

1. The AP initiates a DHCP Discover Request to the BNG.
2. The BNG relays the received DHCP Discover Request to the AC in the management VLAN preconfigured for the AP.
3. AC replies with a DHCP Offer. The DHCP Offer carries the AP address and the AC address (IPv4 and/or IPv6 address is carried in the DHCP Option field).
4. The BNG relays the DHCP Offer to the AP.
5. After receiving the AP address and AC address, the AP responds DHCP Request to BNG.
6. The BNG relays the DHCP Request to the AC.
7. The AC replies with a DHCP ACK.
8. The BNG relays the DHCP ACK to the AP. In steps 1 to 8, the AP obtains the private IP network address and the AC address allocated by the AC.
9. The AP sends a Discovery Request to the AC.
10. The AC replies Discovery Response to AP. In steps 9 to 10, the AP discovery AC.
11. The AP sends a Join Request to the AC.
12. The AC replies Join Response to AP. In steps 11 to 12, the AP joins the AC.
13. The AP sends a Configuration Status Request to the AC.
14. The AC replies Configuration Status Response to the AP.
15. The AP sends a Change State Event Request to the AC.

16. The AC replies Change State Event Response to the AP. In steps 13 to 16, the AC sends the configuration to the AP.
17. The AP sends Keep Alive to the AC.
18. The AC sends Keep Alive to the AP.
19. The AP sends an Echo Request to the AC.
20. The AC replies Echo Response to AP. In steps 17 to 20, the CAPWAP tunnel between the AP and the AC is maintained.

Note1: Refer to IETF RFC2131 and RFC5417 for the process of steps 1 to 8.

Note2: Refer to IETF RFC5415 for the process of steps 9 to 20.

4.4.3 AP Access AC Pool through Dedicated Line

4.4.3.1 Call flow of assigning AC to AP

For multiple APs case, AC selection principal is as follows:

1. Multiple APs in the same continuous coverage area correspond to the same AC to ensure that EUD can achieve seamless roaming between different APs.
2. The AP is assigned the appropriate AC based on factors such as the current traffic load, CPU processing load, and the number of connected APs.

Figure 6 is a call flow of assigning AC to AP.

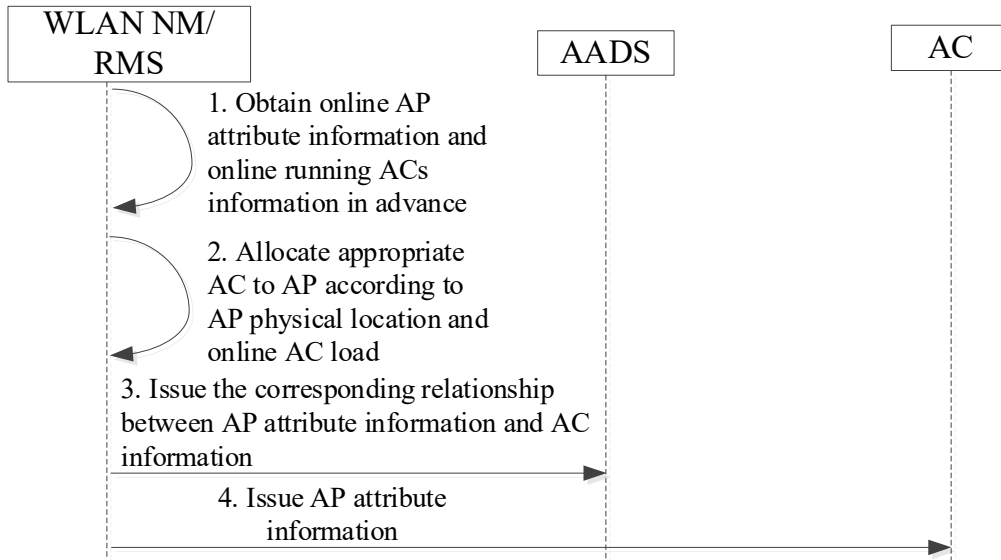


Figure 6 Call flow of assigning AC to AP

1. The WLAN NM obtains the AP attribute information to be online in advance, including the MAC address, serial number, physical location, and other information of the AP. At the same time, The WLAN NM obtains the information of each AC current online.
2. Allocate appropriate AC to AP according to AP's physical location and online AC load.
 - a According to the physical location of the AP, the APs in the same area are ensured to correspond to the same AC, to meet the seamless roaming of the EUD when the EUD moves outside the usable range of one AP and connects to a different AP.
 - b If there is no AP with continuous coverage in the same area, the appropriate AC is selected for the AP, according to the number of access APs, the number of access users, the CPU utilization of each AC and other factors.

3. The WLAN NM sends AP attribute information (including the MAC address and a serial number of the AP) and AC information (including the IP address of the primary AC and the IP addresses of the standby ACs) to the APADS. The corresponding relationship between AP attribute information and AC information is used as the configuration data of the APADS, and the AP is a registered AP.
4. The WLAN NM sends the AP attribute information to the corresponding AC at the same time.

4.4.3.2 Call flow of AP access AC pool through dedicated line

See Figure 3 for the networking of the AC pool. After the AP is powered on, the AP initiates a DHCP Discover. The BNG relays the DHCP Discover of the AP to the APADS according to the management VLAN configured by the AP. APADS analyzes the DHCP Discover message, obtains the AP attribute information, and compares it with the registered AP in the configuration data. If the comparison is successful, the obtained AP is considered as a registered AP, otherwise it is considered as a non-registered AP.

For registered AP, the APADS assigns a private IP network address to the AP and sends the AC address list (the primary AC address and the standby AC addresses) to the AP through the DHCP Option. The AP communicates with the primary AC according to the obtained AC address and establishes a CAPWAP tunnel. **Figure 7** is a call flow of AP access AC pool through dedicated line.

For non-registered AP, APADS discards the received DHCP message, or assigns the specified IP address to prevent the non-registered AP from repeatedly sending DHCP Request messages.

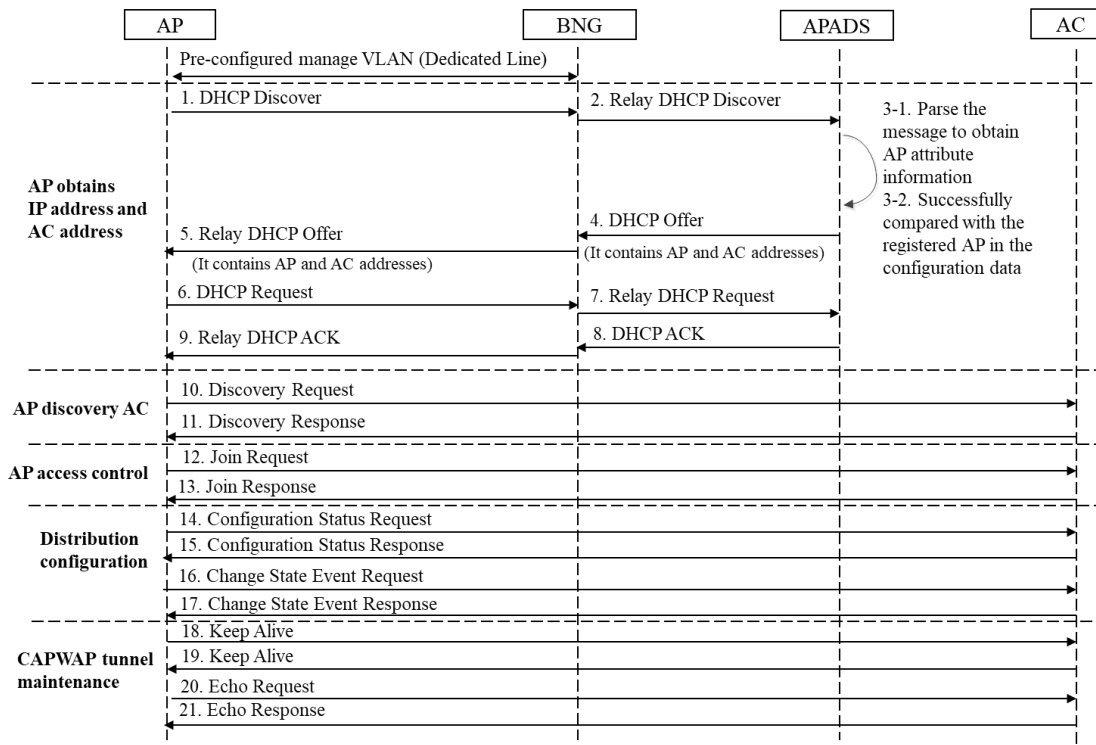


Figure 7 Call flow of AP access AC pool through dedicated line

1. The AP initiates a DHCP Discover Request to the BNG.
2. The BNG relays the received DHCP Discover Request to the APADS in the management VLAN preconfigured for the AP.
3. APADS analyzes DHCP Discover message and successfully compares the acquired AP attribute information with the registered AP in the configuration data.
4. APADS replies with a DHCP Offer. The DHCP Offer carries the AP address and the AC addresses (IPv4 and/or IPv6 address is carried in the DHCP Option field).

5. The BNG relays the DHCP Offer to the AP.
6. After receiving the AP address and AC addresses, the AP replies with a DHCP Request.
7. The BNG relays the DHCP Request to the APADS.
8. The APADS replies with a DHCP ACK.
9. The BNG relays the DHCP ACK to the AP. In steps 1 to 9, the AP obtains the IP address and AC information (AC address list) allocated by the APADS.
10. The AP sends a Discovery Request to the AC.
11. The AC replies Discovery Response to AP. In steps 10 to 11, the AP discovers AC.
12. The AP sends a Join Request to the AC.
13. The AC replies Join Response to AP. In steps 12 to 13, the AP joins the AC.
14. The AP sends a Configuration Status Request to the AC.
15. The AC replies Configuration Status Response to the AP.
16. The AP sends a Change State Event Request to the AC.
17. The AC replies Change State Event Response to the AP. In steps 14 to 17, the AC sends the configuration to the AP.
18. The AP sends Keep Alive to the AC.
19. The AC sends Keep Alive to the AP.
20. The AP sends an Echo Request to the AC.
21. The AC replies Echo Response to AP. In steps 18 to 21, the CAPWAP tunnel between the AP and the AC is maintained.

Note1: Refer to IETF RFC2131 and RFC5417 for the process of steps 1 to 9.

Note2: Refer to IETF RFC5415 for the process of steps 10 to 21.

5 User Authentication

In many scenarios, the device using Wi-Fi needs to be authenticated. The common authentication methods are Portal authentication based on the web page, PEAP authentication and EAP authentication based on 802.1x.

Based on the two access modes of AP accessing AC through the Internet and a dedicated line, the EUD address assignment and authentication process are given respectively.

For the local forwarding method of user data, there are two redirection technologies: one is AC responsible for user redirection and the other is AP responsible for user redirection.

For the portal authentication, the channel between Portal Server and AC can be encrypted (CHAP authentication) and unencrypted (PAP authentication).

5.1 Portal Authentication

5.1.1 User Address Assignment

In the AP accesses the AC through the Internet networking scenario shown in section 4.1. The gateway (with a built-in DHCP server) directly assigns a private IP address to the EUD. Figure 8 is the EUD address assignment call flow of AP accessing AC through the Internet.

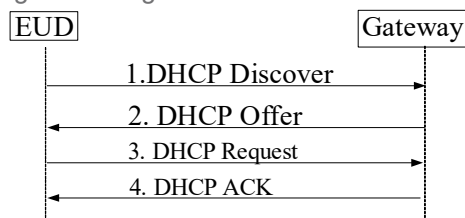


Figure 8 Call flow of Gateway assigns IP address for EUD

1. The EUD sends the DHCP Discover to the gateway through the AP.
2. The gateway replies with a DHCP Offer. DHCP Offer contains IP address, lease time, and other configuration information assigned to the EUD.
3. The EUD sends a DHCP request to the Gateway.
4. The gateway replies DHCP ACK to EUD.

Note: Refer to IETF RFC2131 for IP address allocation.

Since different gateways may assign the same private IP address to the EUD, the user identity attribute should be identified with "IP address+ MAC address" in AC, Portal Server, and AAA.

In the AP accesses the AC through the dedicated line networking scenario, the AC (with a built-in DHCP server) directly assigns the IP address to the EUD. Figure 9 is the EUD address assignment call flow of AP accessing AC through a dedicated line.

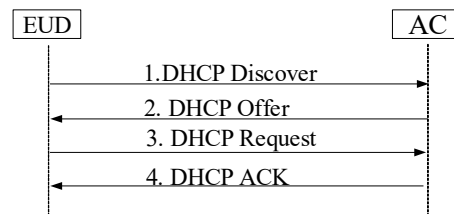


Figure 9 Call flow of AC assigns IP address for EUD

1. The EUD sends the DHCP Discover to the AC through the AP.
2. The AC replies with a DHCP Offer. DHCP Offer contains the IP address, lease term, and other configuration information assigned to the EUD.
3. The AP sends a DHCP Request to the AC.
4. The gateway replies DHCP ACK to the EUD.

AC can uniformly plan the IP address pool and assign different IP address to EUDs, the user identity attribute should be identified with the IP address in AC, Portal Server, and AAA. BNG is the first gateway and would be served as DHCP relay.

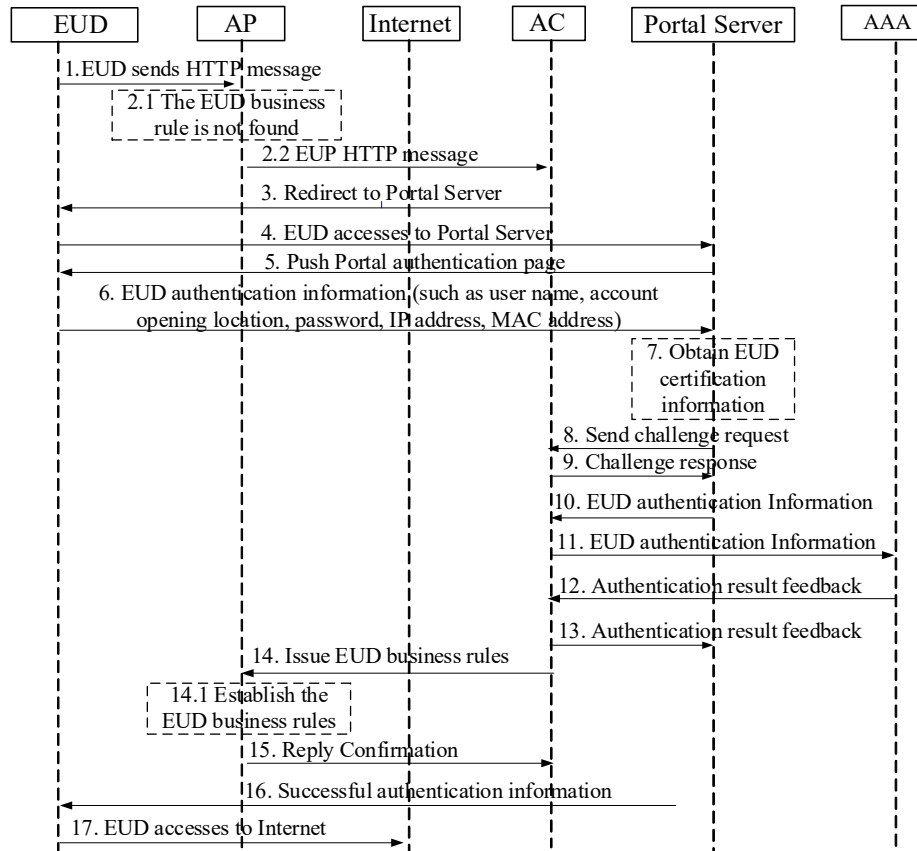
5.1.2 AC Redirect Portal Authentication

After the EUD is powered on, it is associated with the SSID initiated by the specified AP, that is, the AP provides wireless access to the EUD. The IP address is obtained automatically through a DHCP request. The AP must not forward non-HTTP traffic to BNG when the user is not authenticated.

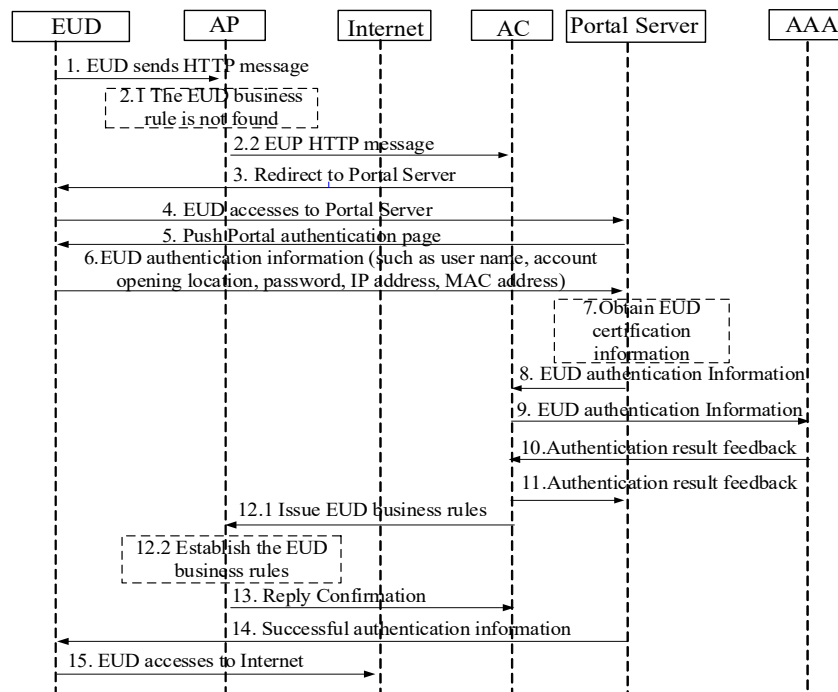
When the EUD sends an HTTP message to access the Internet, the AP forwards the user's HTTP message to the AC through the AP-AC tunnel, and the AC redirects the EUD to the Portal Server.

Portal Server forwards the EUD authentication information to AAA for authentication through AC. If the authentication is successful, the Portal Server pushes the authentication success information to the EUD. If the authentication fails, the Portal Server pushes the authentication failure information to the EUD.

The Portal Server sends the detection message to the user periodically, and the EUD needs to reply to the Portal Server when receiving the detection message. The heartbeat information of the EUD is received by the Portal Server, indicating that the EUD is online.



a) The Portal Server and AC adopt CHAP authentication



b) Portal Server and AC adopt PAP authentication

Figure 10 AC is responsible for redirecting the Portal authentication call flow

Figure 10-a) The Portal Server and AC use CHAP authentication.

1. EUD sends an HTTP message.
2. After receiving the HTTP message sent by the EUD, the AP forwards the HTTP message of the EUDP to the AC.
3. AC redirects EUD to Portal Server.
4. EUD accesses to Portal Server.
5. Portal Server pushes the Portal authentication page to EUD.
6. EUD fills in authentication information, such as user name, account opening location, password, IP address, and MAC address. EUD clicks the authentication button on the authentication page to send EUD authentication information.
7. Portal Server obtains EUD authentication information
8. Portal Server sends challenge request to AC.
9. AC reply challenge response.
10. Portal Server sends EUD authentication information to AC.
11. AC forwards EUD authentication information to AAA.
12. AAA feeds back the EUD certification results to AC.
13. AC feeds back the authentication results to Portal Server.
14. AC issues EUD business rules to AP; AP establishes the EUD business rules.
15. AP replies and confirms to AC.
16. Portal Server pushes authentication success information to EUD.
17. EUD is allowed to access the Internet through filter rule change on AP.

Note1: Refer to IETF RFC1994 for the process of steps 8 to 9.

Note2: Refer to IETF RFC5176 for the process of steps 11 to 12.

Figure 10-b) Portal Server and AC adopt PAP authentication based on Figure 10-a), step 8 (Portal Server sends a challenge request to AC), and step 9 (AC replies to a challenge response) are omitted. Step 6 to step 9 is used for PAP authentication (Refer to IETF RFC1334). The EUD name and password as clear text are delivered from the portal server to AC.

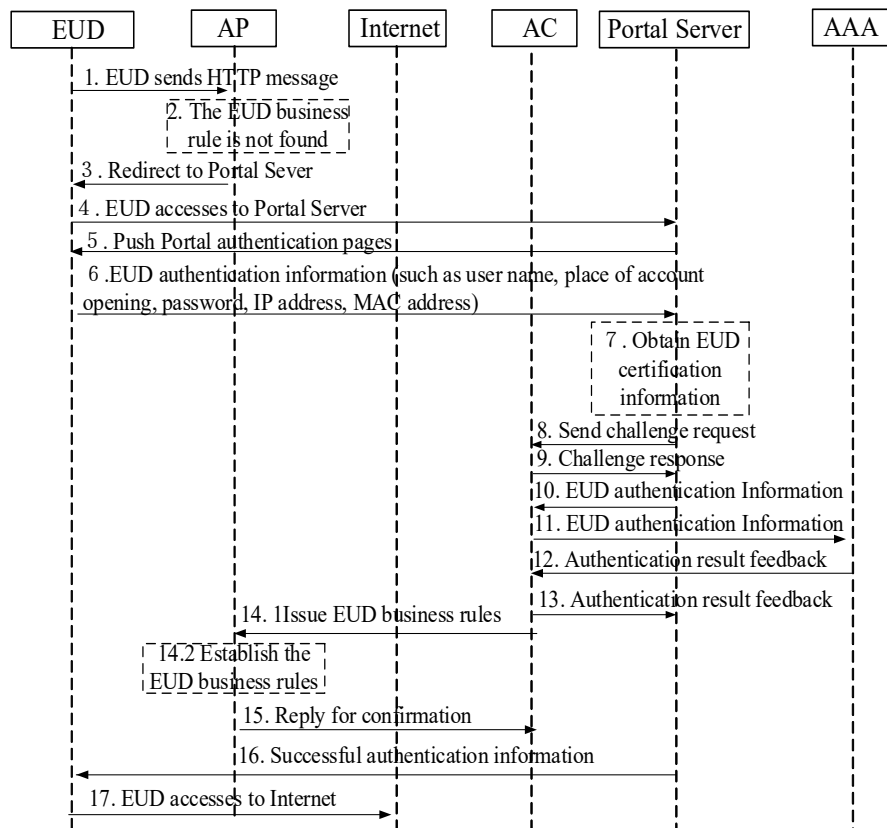
When the AP receives the HTTP message sent by the EUD, if it finds the EUD business rule, it will directly follow the business rule and skip the process of redirecting to Portal Server authentication.

When the AP accesses the AC networking scenario through the Internet, the EUD authentication information must carry the MAC address information, because the identity information of the EUD is the combination of the IP address and the MAC address to avoid duplication of the EUD private network IP address.

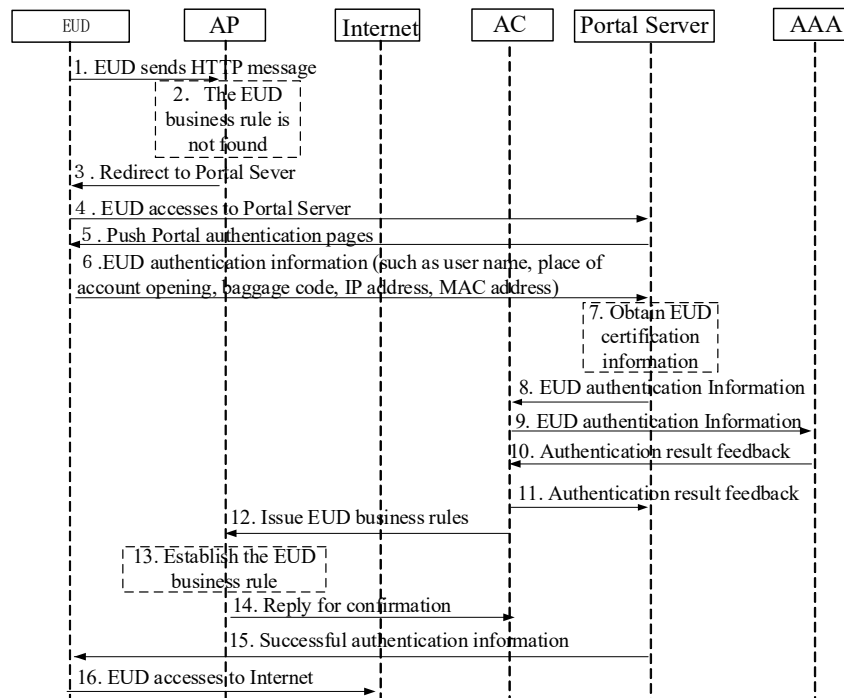
When the AP accesses the AC networking scenario through the dedicated line, the EUD authentication information carries the MAC address information as an option.

5.1.3 AP Redirect Portal Authentication

Since the user data is forwarded locally, the AP can also take the place of the AC to be responsible for user redirection for Portal authentication. The other processes are consistent with the AC responsible for redirecting the Portal authentication process shown in Figure 11.



a) The Portal Server and AC adopt CHAP authentication



b) The Portal Server and AC adopt PAP authentication

Figure 11 AP is responsible for redirecting the Portal authentication process

Figure 11-a) The Portal Server and AC use CHAP authentication.

1. EUD opens any webpage and sends an HTTP message.
2. After receiving the HTTP message of the EUD, the AP does not detect the EUD business rule locally.
3. AP redirects EUD to Portal Server.
4. EUD accesses to Portal Server.
5. Portal Server pushes the Portal authentication page to EUD.
6. EUD fills in authentication information, such as user name, account opening location, password, IP address, and MAC address. EUD clicks the authentication button on the authentication page to send EUD authentication information.
7. Portal Server obtains EUD authentication information
8. Portal Server sends challenge request to AC.
9. AC reply challenge response.
10. Portal Server sends EUD authentication information to AC.
11. AC forwards EUD authentication information to AAA.
12. AAA will feed back the EUD certification results to AC
13. AC feeds back the authentication results to Portal Server.
14. AC issues EUD business rules to AP; AP establishes the EUD business rules.
15. AP replies and confirms to AC.
16. Portal Server pushes authentication success information to EUD.
17. EUD is allowed to access the Internet.

Note1: Refer to IETF RFC1994 for the process of steps 8 to 9.

Note2: Refer to IETF RFC5176 for the process of steps 11 to 12.

For Portal Server and AC adopt PAP authentication shown in Figure 11-b) all of steps are the same as above Figure 11-a) except that step 8 (Portal Server sends a challenge request to AC) and step 9 (AC replies to a challenge response) are omitted. Steps 6 to 9 are used for PAP authentication (Refer to IETF RFC1334). The EUD name and password as clear text are delivered from the portal server to AC.

When the AP receives the HTTP message sent by the EUD, if it finds the EUD business rule, it will directly handle it according to the business rule and skip the process of redirecting to Portal Server authentication.

5.1.4 Users Are Offline Normally

When the EUD initiates the offline procedure, the user sends a logoff request to the Portal Server. The Portal Server receives the logoff request initiated by the EUD and notifies the AC to perform the user logoff operation, that is, the Portal Server forwards the user logoff request message to the AC, the AC sends the request message to AAA to stop accounting, and the AC notifies the AP to delete the user's business rules, as shown in Figure 12.

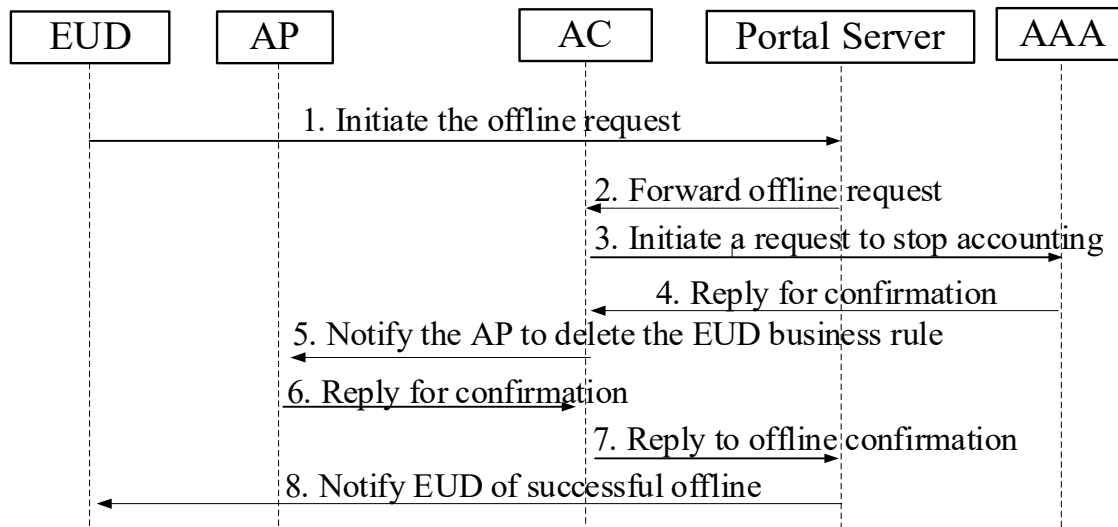


Figure 12 User's normal offline detection process

1. The EUD initiates an offline request to the Portal Server.
2. The Portal Server forward the EUD's offline request to the AC.
3. AC initiates the EUD's stop accounting request to AAA.
4. AAA reply acknowledgement to AC.
5. AC notifies AP to delete the EUD's service rule.
6. The AP replies with an acknowledgement.
7. The AC replies to the Portal Server with the EUD offline confirmation.
8. The Portal Server notifies the EUD of successful disconnection.

5.1.5 The User Is Offline Abnormally

EUD abnormal logoff refers to the user's disconnection from the network without active logoff, including user shutdown, restart, leaving the Wi-Fi coverage area or network failure.

There are two methods to detect abnormal offline users.

5.1.5.1 Wired Side Detection Method

The Portal Server sends the detection message to the user periodically. If the Portal Server does not receive the user's response message (also called heartbeat message) for more than a predetermined number of consecutive times, it determines that the user is offline abnormally. The Portal Server sends the user's abnormal offline information to AC, which logs the user off and notifies the AP to delete the user's business rules and notifies AAA to stop user accounting. Figure 13 is detection call flow of abnormal offline users on the wired side.

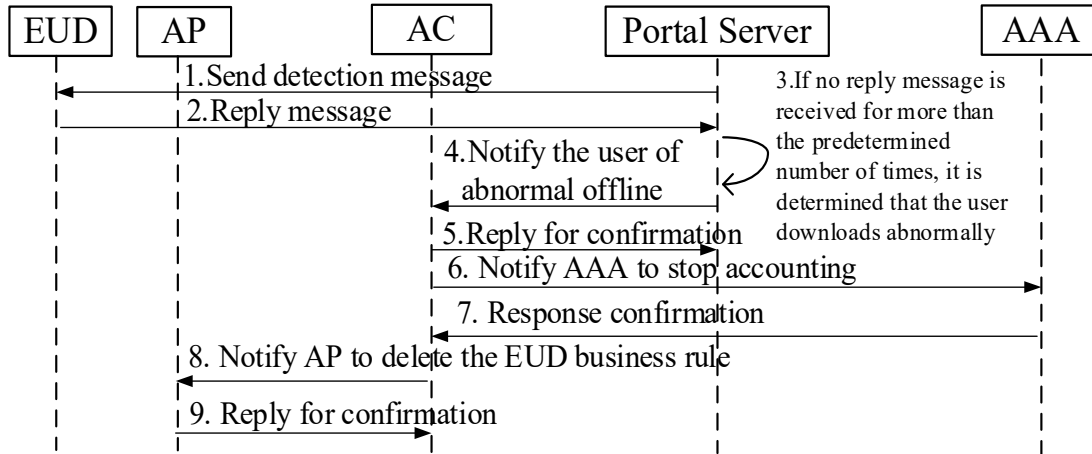


Figure 13 Detection process of abnormal offline users on the wired side

1. The Portal Server periodically sends detection messages to the EUD.
2. The EUD replies to the Portal Server with a message.
3. Portal Server determines that the EUD is abnormally offline if no reply message is received more than a configured number of times.
4. The Portal Server notifies the AC that the EUD is offline abnormally.
5. AC replies to Portal Server with an acknowledgement.
6. AC notifies AAA to stop billing of the EUD.
7. AAA replies to AC to confirm.
8. AC notifies AP to delete the EUD business rule.
9. AP replies to AC to confirm.

Note: Refer to IETF RFC2131 for IP address release.

5.1.5.2 Air Interface Detection Method

When the AP receives the disassociation message sent by the user or does not receive any message (including management frame message and data frame message) from the user within the predetermined time, it determines that the user is offline abnormally, as shown in Figure 14.

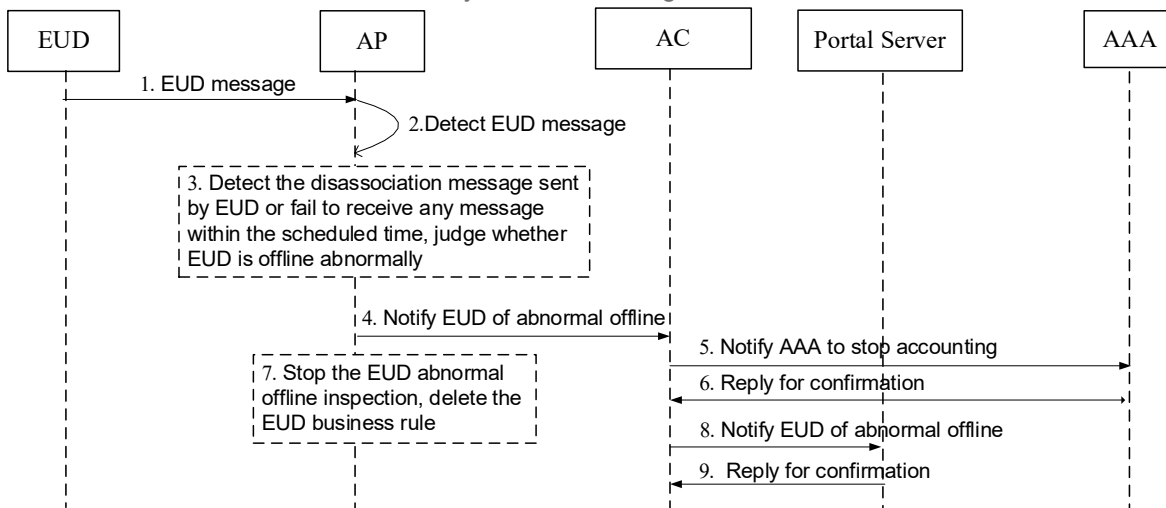


Figure 14 Detection flow of abnormal offline user at the air interface side

1. The EUD sends a message to the AP.
2. AP detects the EUD message

3. The AP detects the de-association message sent by the EUD or does not receive any message within the scheduled time and determines that the EUD is abnormally offline.
4. The AP notifies the EUD of the abnormal disconnect.
5. The AC notifies AAA to stop the billing of the EUD.
6. AAA replies to AC to confirm.
7. The AP stops the EUD's abnormal offline detection and removes the EUD service rule.
8. AC notifies the Portal Server of the abnormal disconnect.
9. Portal Server replies with a confirmation.

5.2 802.1X Authentication

5.2.1 PEAP Authentication

5.2.1.1 User online process

The EUD uses PEAP authentication for the online process. The EUD carries out the authentication process, after the EUD has executed authentication initialization and established a TLS channel. And then it will complete the Wi-Fi association and IP address acquisition process. The Wi-Fi association is out scope of this document and the IP address acquisition process is already described in section 5.1.1.

The authentication process for user access consists of 3 steps:

1. Authentication initialization process
2. TLS tunnel establishment process
3. Authentication process

Figure 15 is PEAP authentication call flow.

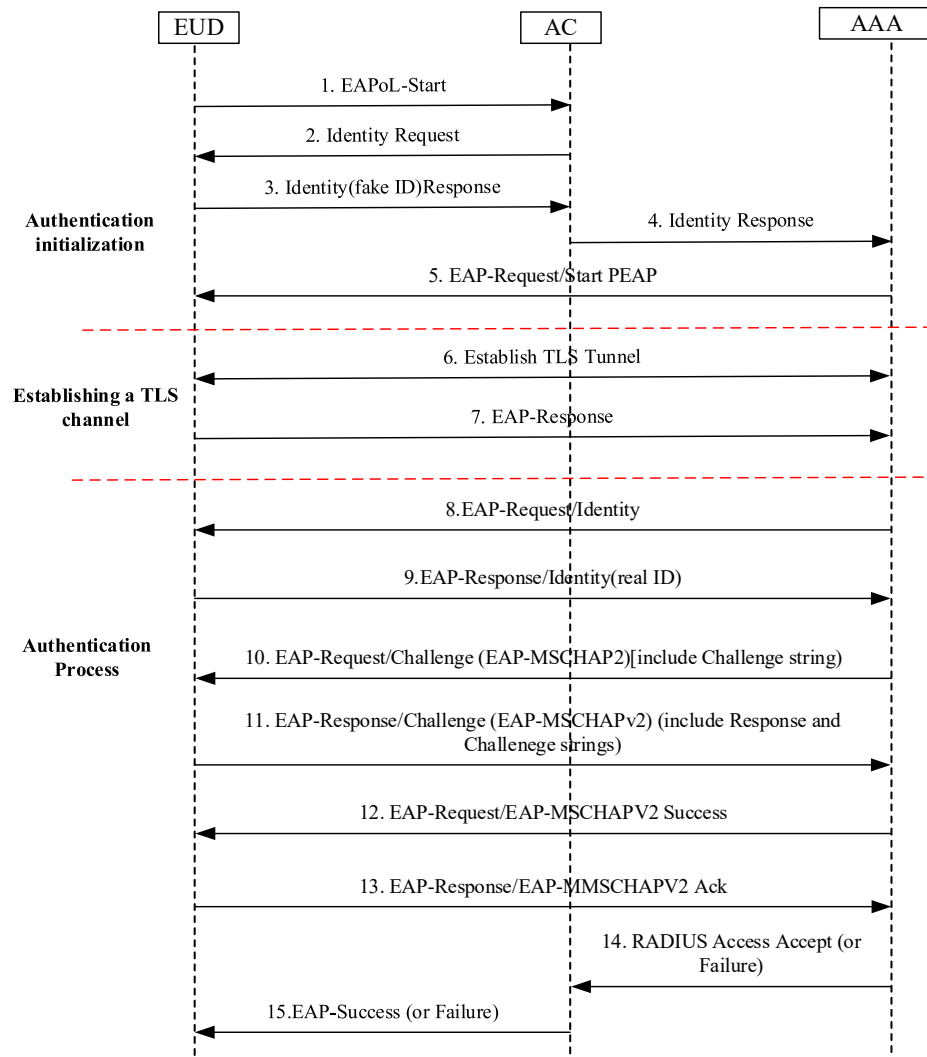


Figure 15 PEAP authentication call flow

1. After EUD associates with Wi-Fi hotspot enabled with EAP-PEAP authentication method, the EUD sends an EAPoL-Start message to the AC to start the PEAP authentication process.
2. The AC sends an Identity Request message to the EUD requesting the EUD to send the user information.
3. The EUD responds with an Identity Response to the AC's request.
4. The AC sends the Identity Response to AAA in the EAP over RADIUS message format, with the relevant RADIUS attributes.
5. AAA receives the Identity Response from the AC, determines the use of EAP-PEAP authentication according to the configuration, and starts the EAP-PEAP authentication.
6. AAA sends its Server Certificate to EUD, to start the TLS channel establishment.
7. After EUD validates AAA certificate, the EUD and AAA establish a TLS tunnel, following authentication process is occur in this TLS tunnel.
8. AAA sends EAP message to AC, AC extracts the EAP domain from the RADIUS message and encapsulates it into an EAP-request message and sends it to the EUD, in this step it's an Identity Request.
9. After receiving the message, the EUD replies with EAP-response, AC extracts the message and encapsulates as RADIUS EAP message, and sends it to AAA, in this step it's the Identity Response with the real identity of EUD.

10. The AAA will send a RADIUS access challenge message to the AC after obtaining the access identifier of the EUD. Upon receiving this message, the AC will decapsulate the message and send the EAP-Request/EAP-MSCHAPv2(Challenge) in the message to the EUD, where Challenge message contains the Server-Challenge generated by the AAA.
11. The EUD performs the calculation and sends a Response message to the AC. After receiving the message, AC encapsulates it in an Access-Request and passes it to the AAA. The Response message contains the Peer-Challenge and a response message which generated as a response to Server-Challenge by calculation based on the user's password, user name, Peer-Challenge and Server-Challenge.
12. The AAA authenticates the EUD by using the same algorithm on the AAA to calculate an answer based on the user password, user name, Peer-Challenge and Server-Challenge. If successfully authenticated, a Success-Request message is sent to the AC, which contains the answer. After receiving the message, the AC decapsulates it and sends the Success-Request in the message to the EUD, requesting the user to authenticate the AAA'.
13. The EUD verifies the AAA by using the same algorithm with the user password, user name, Peer-Challenge, Server-Challenge response, and then matching it with the response in the Success-Request sent by the AAA. If the match is successful, the EAP-Request/EAP-MSCHAPv2 (Success-Response) message is sent to the AC, and after the AC receives it, the message is encapsulated into an Access-Request message and passed to the AAA.
14. If the AAA receives the Success-Response message, it means the authentication is successful and the AAA sends the Access accept message to the AC.
15. The AC sends an EAP-success message to notify the EUD of successful authentication after receiving the accept message.

Note1: Step 6 refers to RFC5246;

Note2: Step 8 to step 15 refer to RFC2759 for detailed MS-CHAPv2 interaction in the inner tunnel of TLS;

Note3: For the interaction between AC and AAA, refer to RFC2865;

Note4: For the interaction between AC and EUD, refers to IEEE 802.11i.

5.2.1.2 User normal offline process

User (EUD) offline process includes user-initiated offline and network-initiated user offline. When the user is not using the Wi-Fi network, the user sends offline messages, as shown in Figure 16; the other one is AAA-initiated offline, mainly used in the prepaid user scenario, in the case of insufficient balance of the paid user, AAA initiates an offline message, as shown in Figure 17.

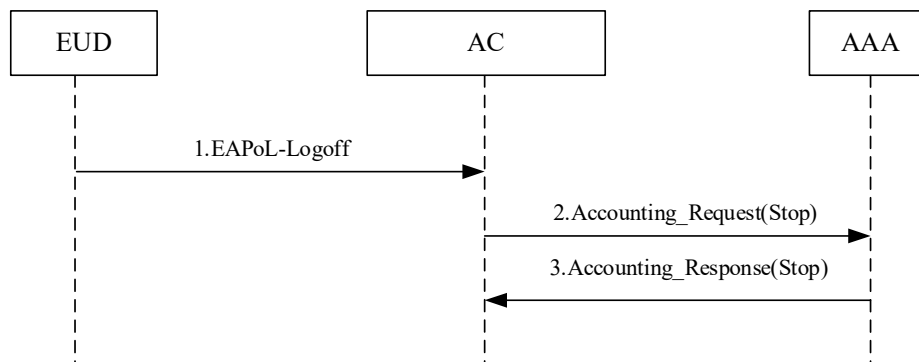


Figure 16 User-initiated offline

Figure 16 User initiated offline process.

1. The EUD actively terminates the session and initiates an EAPoL-logoff request to exit the network.
2. The AC sends an accounting stop request message to the AAA.
3. The AAA replies to the AC with a response to the accounting stop request message.

Note1: Step 1 refers to IEEE 802.1X.

Note2: Refer to RFC2865 for RADIUS Message interaction between AC and AAA.

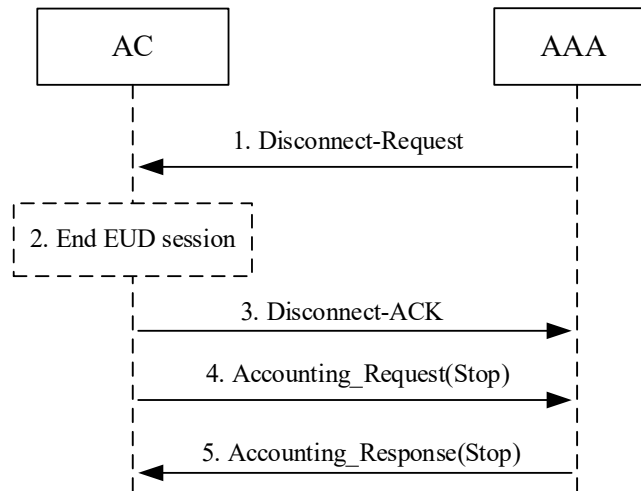


Figure 17 AAA-initiated offline

Figure 17 AAA-initiated offline process.

1. For management purposes, a user disconnect process can be initiated by the network. Disconnect-Request is initiated by the AAA to the AC.
2. The AC terminates the user session and releases the user session resources.
3. The AC replies to the Disconnect-ACK message to the AAA.
4. The AC sends an Accounting Stop Request message to the AAA.
5. The AAA replies to the AC with a response to the accounting stop request message.

Note: Refer to RFC2865 for RADIUS Message interaction between AC and AAA.

5.2.1.3 Inactive user offline process

When AC detects EUD isn't online, AC sends accounting stop request to AAA shown in Figure 18.

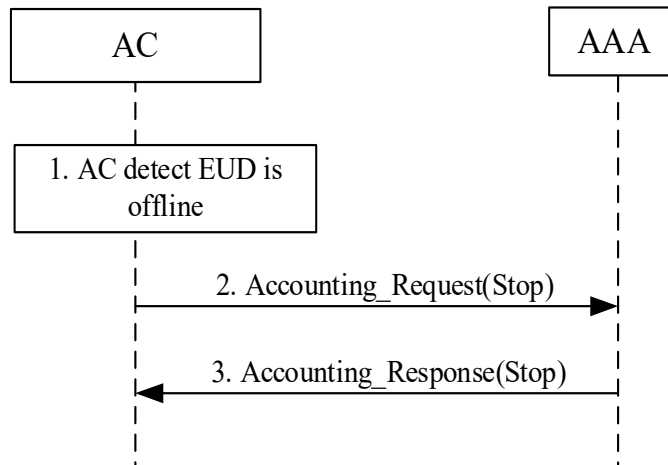


Figure 18 User abnormal offline call flow

1. The AC detects that the traffic is less than the threshold within a fixed period or detects that the user is no longer online through the Keep Alive mechanism.
2. AC sends an accounting stop request message to AAA

3. AAA responds to the AC with an accounting stop request message.

Note: Refer to RFC2865 for RADIUS Message interaction between AC and AAA.

5.2.2 EAP-SIM/AKA Authentication

5.2.2.1 EAP-SIM Authentication

EAP-SIM authentication provides authentication and key distribution mechanism based on (U)SIM card. It is a two-way authentication, that is, AAA authentication EUD, EUD also authentication AAA. The EAP-SIM authentication process is shown in Figure 19.

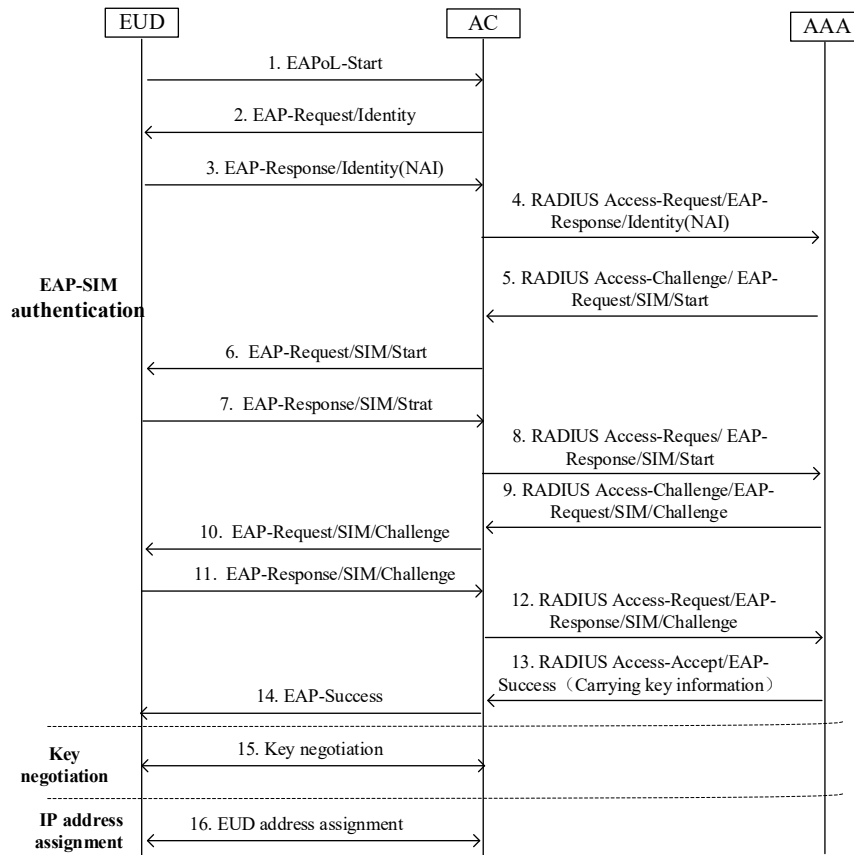


Figure 19 EAP-SIM authentication call flow

1. When the EUD initiates Wi-Fi Authentication with a Wi-Fi hotspot that has the EAP-SIM authentication method enabled, the EUD sends an EAPoL-Start message to the AC to initiate the EAP-SIM authentication process.
2. The AC sends an Identity Request message to the EUD requesting the EUD to send the user information.
3. The EUD responds with a Network Access Identity (NAI) Response to the AC's request.
4. The AC sends the Identity Response to AAA in the EAP over RADIUS message format, with the relevant RADIUS attributes.
5. The AAA receives the Identity Response from the AC, determines the use of EAP-SIM authentication according to the configuration, and start the EAP-SIM authentication.
6. The AC forwards EAP-Request/SIM/Start message to EUD.
7. The EUD responds to the request and sends EAP-Response/SIM/Start message (with NAI) to the AC.
8. The AC forwards EAP-Response/SIM/Start message (with NAI) to the AAA.

9. AAA sends EAP-Request/SIM/Challenge message according to the EUD response result.
 10. The AC forwards EAP-Request/SIM/Challenge message to the EUD.
 11. The EUD responds to the request and sends EAP-Response/SIM/Challenge message to the AC.
 12. The AC forwards EAP-Response/SIM/Challenge message to the AAA.
 13. The AAA authentication is successful and sends EAP-Success message with key information to the EUD.
 14. The AC forwards EAP-Success message (with key information) to the EUD.
 15. The AC and the AP negotiate key.
 16. The AC assigns an IP address to the EUD.
- Note1: Step 1 to step 15 refer to IETF RFC3748 and IETF RFC4186.
 Note2: Step 16 refer to section 5.1.1.
 Note3: The interaction between AC and AAA refer to RFC2865.
 Note4: The interaction between AC and EUD refers to IEEE 802.11i.

EAP-SIM and PEAP are authentication technologies based on EAP architecture, so their user offline process is the same. The normal offline process of EAP-SIM refers to section 5.2.1.2. The abnormal offline process of EAP-SIM refers to section 5.2.1.3.

5.2.2.2 EAP-AKA Authentication

EAP-AKA authentication provides authentication and key distribution mechanism based on (U)SIM card. It is a two-way authentication, that is, AAA authentication EUD, EUD also authentication AAA. The EAP-AKA authentication process is shown in Figure 20.

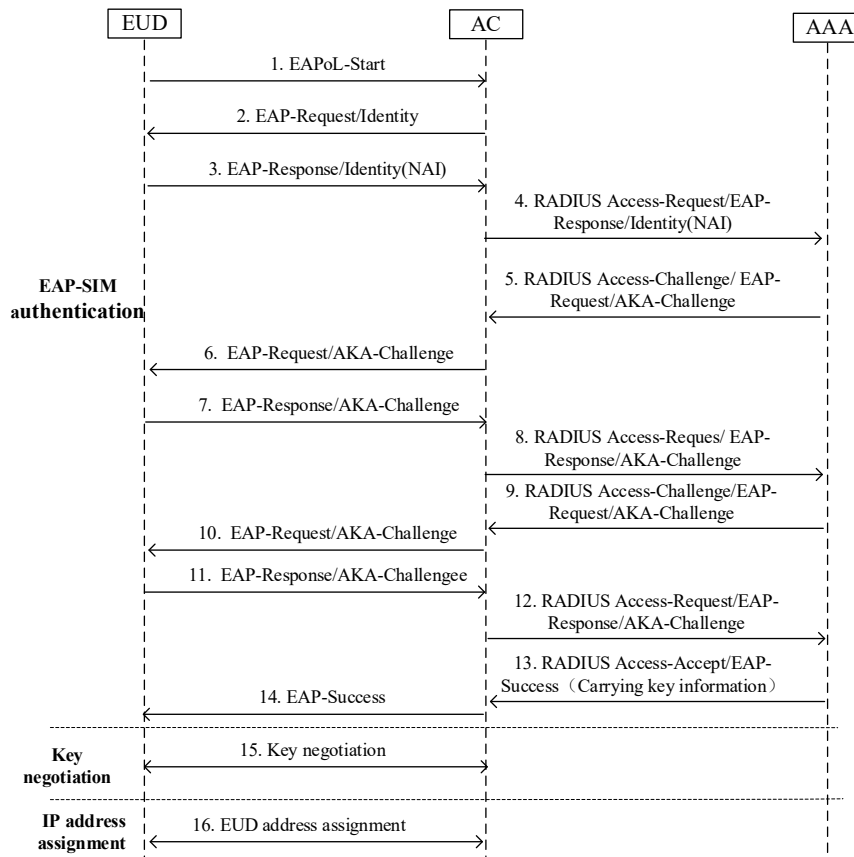


Figure 20 EAP-SIM authentication call flow

1. When the EUD initiates Wi-Fi Authentication with a Wi-Fi hotspot that has the EAP-AKA authentication method enabled, the EUD sends an EAPoL-Start message to the AC to initiate the EAP-AKA authentication process.
2. The AC sends an Identity Request message to the EUD requesting the EUD to send the user information.
3. The EUD responds with a Network Access Identity (NAI) Response to the AC's request.
4. The AC sends the Identity Response to AAA in the EAP over RADIUS message format, with the relevant RADIUS attributes.
5. The AAA receives the Identity Response from the AC, determines the use of EAP-AKA authentication according to the configuration, and start the EAP-AKA authentication.
6. The AC forwards EAP-Request/AKA-Challenge message to EUD.
7. The EUD responds to the request and sends EAP-Response/ AKA-Challenge message (with NAI) to the AC.
8. The AC forwards EAP-Response/AKA-Challenge message (with NAI) to the AAA.
9. AAA sends EAP-Request/AKA-Challenge message according to the EUD response result.
10. The AC forwards EAP-Request/AKA-Challenge message to the EUD.
11. The EUD responds to the request and sends EAP-Response/AKA-Challenge message to the AC.
12. The AC forwards EAP-Response/AKA-Challenge message to the AAA.
13. The AAA authentication is successful and sends EAP-Success message with key information to the EUD.

Note1: Step 1 to step 15 refer to IETF RFC3748 and IETF RFC4187.

Note2: Step 16 refer to section 5.1.1.

Note3: The interaction between AC and AAA refer to RFC2865.

Note4: The interaction between AC and EUD refers to IEEE 802.11i.

EAP-AKA and PEAP are authentication technologies based on EAP architecture, so their user offline process is the same. The normal offline process of EAP-AKA refers to section 5.2.1.2. The abnormal offline process of EAP-AKA refers to section 5.2.1.3.

6 Nodal Requirements

6.1 AP Requirements

- [R-1] The AP MUST support [R-1] in TR-321 "The AP MUST support multiple SSIDs".
- [R-2] The AP MUST support [R-3] in TR-321 "The AP MUST relay customer Ethernet frames to the BNG in the distributed AC architecture".
- [R-3] The AP MUST support [R-4] in TR-321 "The AP MUST be able to be configured with the BNG's tunnel address in the distributed AC architecture as specified in TR-069 or CAPWAP (RFC 5415 and RFC 5416). The tunnel protocol stack is specified in section 6.4. For additional details of the protocol stack, please refer to RFC 1701 and RFC 2784".
- [R-4] The AP MUST support [R-6] in TR-321 "The AP MUST support a stateless IPv4 or IPv6 tunneling mechanism. The tunnel protocol stack is specified in section 6.4".
- [R-5] The AP MUST support [R-7] in TR-321 "The AP MUST be able to log and report the information related to the EUD location, which includes, but is not limited to, BSSID, EUD MAC, channel, RSSI, and the collection interval".
- [R-6] The AP MUST support VLAN Trunk function. The AP can be configured with multiple VLANs on the same Ethernet port.
- [R-7] The AP MUST forward user authentication information to AC through the CAPWAP control tunnel
- [R-8] The AP MUST forward the AP management information to AC through the CAPWAP control tunnel.
- [R-9] The AP MUST forward user Ethernet frames to Gateway in local forwarding mode
- [R-10] The AP MUST support DHCP client.
- [R-11] The AP MUST support DNS client.

- [R-12] If the AP is responsible for user redirection during Portal authentication, the AP MUST support the http redirection function.
- [R-13] AP MUST support filter rule by matching on IP to redirect HTTP traffic.

Table 1 AP requirements for different authentication scenarios

	Portal authentication			802.1X authentication		
	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line
R-1	X	X	X	X	X	X
R-2	X	X	X	X	X	X
R-3	X	X	X	X	X	X
R-4	X	X	X	X	X	X
R-5	X	X	X	X	X	X
R-6		X	X		X	X
R-7	X	X	X	X	X	X
R-8	X	X	X	X	X	X
R-9	X			X		
R-10	X	X	X	X	X	X
R-11	X					
R-12	X	X	X			
R-13	X	X	X			

6.2 AC Requirements

- [R-14] The AC MUST support [R-42] in TR-321 “The AC MUST support mutual discovery and authentication between the AC and the APs”.
- [R-15] The AC MUST support [R-45] in TR-321 “The AC MUST meet the general QoS requirements for the Access Node defined in TR-101 from R64 to R79”.
- [R-16] The AC MUST support [R-46] in TR-321 “The AC MUST be able to implement per SSID IEEE 802.1p and DSCP based QoS policy (including marking)”.
- [R-17] The AC MUST support [R-48] in TR-321 “The AC MUST be able to control the AP’s IEEE 802.1p and DSCP marking capability based on SSID”.
- [R-18] The AC MUST support [R-49] in TR-321 “The AC MUST be able to configure the AP traffic scheduling on a per SSID basis”.
- [R-19] The AC MUST support [R-52] in TR-321 “The AC MUST be able to limit the number of its associated EUDs on per SSID and per AP basis”.
- [R-20] The AC MUST support [R-53] in TR-321 “The AC MUST be able to limit the number of its associated EUDs on a per AP basis”.
- [R-21] The AC MUST support [R-55] in TR-321 “The AC MUST NOT relay IEEE 802.1X frames to the BNG if the AC is the authenticator in the distributed AC architecture”.
- [R-22] The AC MUST support [R-56] in TR-321 “The AC MUST be able to provision the BNG IP address on the AP in the distributed AC architecture (see protocol stack in section 6.4)”.
- [R-23] The AC MUST support [R-57] in TR-321 “The AC MUST be able to collect from the APs information related to the EUD location, which includes BSSID, EUD MAC, channel, RSSI, and the collection time”.

- [R-24] The AC MUST support [R-59] in TR-321 “The AC MUST support an IEEE 802.1X Authenticator function”.
- [R-25] The AC MUST support [R-60] in TR-321 “The AC MUST support a RADIUS client”.
- [R-26] The AC MUST support [R-61] in TR-321 “The AC MUST support 4-way IEEE 802.11i handshake with the EUD”.
- [R-27] The AC MUST support [R-65] in TR-321 “The AC MUST be able to redirect or policy route the HTTP traffic of unauthorized EUDs to the portal server for portal authentication”.
- [R-28] The AC MUST support [R-66] in TR-321 “The AC MUST block all traffic except communication to the portal server, the DNS and the DHCP server, when the EUD is unauthenticated”.
- [R-29] The AC MUST support [R-67] in TR-321 “The AC MUST send an Accounting Start Message for a EUD to the AAA when the EUD is authenticated successfully”.
- [R-30] The AC MUST support [R-68] in TR-321 “The AC MUST be able to insert the BSSID and the SSID into RADIUS Called-Station-Id and report the information to the AAA during EUD authentication”.
- [R-31] The AC MUST support [R-70] in TR-321 “The AC MUST be able to update the BSSID and the SSID in RADIUS Called-Station-Id and report the information to the AAA when the EUD switches from one AP to another”.
- [R-32] The AC MUST support [R-72] in TR-321 “The AC MUST support adding the EUD location information (such as the AC identifier and port information, or the BSSID/SSID) into the URL while redirecting the HTTP traffic of an unauthenticated EUD to the portal server”.
- [R-33] The AC MUST support VLAN Trunk function. The AC can be configured with multiple VLANs on the same Ethernet port.
- [R-34] The AC MUST support DHCP Server.
- [R-35] The AC MUST support IPv4 or IPv6 tunneling mechanism as specified in IETF RFC 5415 and IETF RFC 5416.

Table 2 AC requirements for different authentication scenarios

	Portal authentication			802.1X authentication		
	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line
R-14	X	X	X	X	X	X
R-15	X	X	X	X	X	X
R-16	X	X	X	X	X	X
R-17	X	X	X	X	X	X
R-18	X	X	X	X	X	X
R-19	X	X	X	X	X	X
R-20	X	X	X	X	X	X
R-21				X	X	X
R-22	X	X	X	X	X	X
R-23	X	X	X	X	X	X
R-24				X	X	X
R-25	X	X	X	X	X	X
R-26				X	X	X
R-27	X	X	X			
R-28	X	X	X			

R-29	X	X	X			
R-30	X	X	X	X	X	X
R-31	X	X	X	X	X	X
R-32	X	X	X			
R-33	X	X	X	X	X	X
R-34	X	X	X	X	X	X
R-35	X	X	X	X	X	X

6.3 APADS Requirements

[R-36] The APADS MUST support DHCP Server.

[R-37] The APADS MUST determine whether an AP is a registered AP or a non-registered AP

[R-38] The APADS MUST be able to distribute AC addresses through the DHCP Option field while assigning address to a registered AP.

Table 3 APADS requirements for different authentication scenarios

	Portal authentication			802.1X authentication		
	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line
R-36			X			X
R-37			X			X
R-38			X			X

6.4 Portal Server Requirements

[R-39] The Portal Server MUST support [R-73] in TR-321 “The portal server MUST support obtaining the user name and password on the portal page”.

[R-40] The Portal Server MUST support [R-74] in TR-321 “The portal server MUST support displaying the authentication result on the portal page”.

Table 4 Portal Server requirements for different authentication scenarios

	Portal authentication			802.1X authentication		
	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line
R-39	X	X	X			
R-40	X	X	X			

6.5 AAA Server Requirements

[R-41] The AAA Server MUST support [R-75] in TR-321 “The AAA server MUST support IEEE 802.1X Authentication”.

- [R-42] The AAA Server MUST support [R-76] in TR-321 “The AAA server MUST send the policy and QoS configuration (e.g., bandwidth, time/traffic quota) to the RADIUS client (the AC or the BNG) for successfully authenticated EUDs”.
- [R-43] The AAA Server MUST support [R-77] in TR-321 “Upon receiving the RADIUS Access Request message with the MAC address of the EUD from the BNG, the AAA server MUST send the corresponding EUD information to the BNG in the RADIUS Access Accept message”.
- [R-44] The AAA Server MUST support [R-78] in TR-321 “The AAA server MUST be able to allow an authenticated subscriber to bypass portal re-authentication”.
- [R-45] The AAA server MUST support Portal Authentication.

Table 5 AAA Server requirements for different authentication scenarios

	Portal authentication			802.1X authentication		
	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line	AP Access AC through Internet	AP Access AC through Dedicated Line	AP Access AC pool through Dedicated Line
R-41	X	X	X			
R-42	X	X	X	X	X	X
R-43				X	X	X
R-44	X	X	X			
R-45	X	X	X			

End of Broadband Forum Technical Report TR-497