TECHNICAL REPORT

TR-321
Public Wi-Fi Access in Multi-service Broadband Networks

Issue: 01
Issue Date: November2015

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	9 November 2015	11 November 2015	Bo Wang, China Telecom Kenneth Wan, Alcatel-Lucent	Original

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

Editor	Bo Wang	China Telecom	wangbo@chinatelecom.com.cn
	Kenneth Wan	Alcatel-Lucent	kenneth.wan@alcatel-lucent.com
Architecture and Migration	David Allan	Ericsson	david.i.allan@ericsson.com
	David Thorne	BT	david.j.thorne@bt.com
WA Directors			

Table of Contents

List of Figures

List of Tables

Executive Summary

Wi-Fi has recently become widely available as an access technology in homes, enterprises and hot spots expanding the set of devices that can utilize fixed access as well as permitting offloading of data traffic from the mobile network. This Technical Report specifies architectures and solutions to incorporate Wi-Fi access technology into existing Broadband Forum networks.

1 Purpose and Scope

1.1 Purpose

Since the introduction of Wi-Fi on mobile devices, there has been interest in incorporating so called 'public Wi-Fi' into Broadband Forum's multi-service broadband architecture. The rise in smart phone usage at public hotspots has increased this interest. As the popularity of Wi-Fi enabled devices to provide access to the Internet and other data services rises, applications are increasingly being developed to be independent of access type. Operators are looking to provide network capabilities that offer better user experience on mobile devices, and there is a need to find more efficient ways for the network to support mobile devices.

1.2 Scope

The TR-321 covers use cases, physical and logical architecture and functional and nodal requirements for public Wi-Fi access. The architecture includes data, control and management, as well as functional decomposition and placement into network nodes. Functional and nodal requirements are considered for the following: Wi-Fi Access Points (AP), Access Controllers (AC) and Broadband Network Gateways (BNG). The scope also includes interactions with the Authentication Authorization Accounting (AAA) server and the portal server.

TR-321 covers requirements for:

- Simplifying AP requirements by placing more functions into the AC and/or BNG
- Network architectures to support different use cases and new service offerings such as location based service, wholesale/retail, and mobility
- Authentication models
- Subscriber management and traffic management
- Architecture based nodal requirements

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 be 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-069	*CPE WAN Management Protocol*	BBF	2013
[2]	TR-101	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011
[3]	TR-145	*Multi-service Broadband Network Functional Modules and Architecture*	BBF	2012
[4]	TR-177	*IPv6 in the context of TR-101*	BBF	2010

[5]	TR-178	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	2014
[6]	TR-203	*Interworking between Next Generation Fixed and 3GPP Wireless Networks*	BBF	2012
[7]	TR-291	*Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access*	BBF	2014
[8]	802.1X	*Port Based Network Access Control*	IEEE	2004
[9]	802.11i	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications* *Amendment 6: Medium Access Control (MAC) Security Enhancements*	IEEE	2004
[10]	RFC 1701	*Generic Routing Encapsulation (GRE)*	IETF	1994
[11]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[12]	RFC 2784	*Generic Routing Encapsulation (GRE)*	IETF	2000
[13]	RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	IETF	2000
[14]	RFC 2866	*RADIUS Accounting*	IETF	2000
[15]	RFC 3579	*RADIUS Support For Extensible Authentication Protocol (EAP)*	IETF	2003
[16]	RFC 3580	*IEEE 802.1X RADIUS Usage Guidelines*	IETF	2003
[17]	RFC 3748	*Extensible Authentication Protocol (EAP)*	IETF	2004
[18]	RFC 5415	*Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*	IETF	2009
[19]	RFC 5416	*Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11*	IETF	2010

2.3 Definitions

The following terminology is used throughout this Technical Report.

AC (Access Controller) The network entity that provides wireless termination point access to the network infrastructure in the data plane, control plane, and management plane.

Standalone AC architecture	An architecture in which all the Wi-Fi traffic (data, control and management) is forwarded to the AC to be processed, and the AC is separate from the BNG.
Distributed AC architecture	An architecture in which the Wi-Fi data traffic is forwarded to another node to process, while the AC only processes Wi-Fi control and management traffic, and the AC is separate from the BNG.
BNG integrated AC architecture	An architecture in which the AC is integrated within the BNG.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AC	Access Controller
AKA	Authentication and Key Agreement
AP	Access Point
BNG	Broadband Network Gateway
BSSID	Basic Service Set Identifier
CAPEX	Capital Expenditure
CAPWAP	Control And Provisioning of Wireless Access Points
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EUD	End User Device
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identification Number
MAC	Media Access Control
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAT	Network Address Translation
OPEX	Operating Expense
PMK	Pairwise Master Key
QoS	Quality of Server
RADIUS	Remote Authentication Dial In User Service

RFC	Request For Comments
RG	Residential Gateway
RSSI	Received Signal Strength Indicator
SIM	Subscriber Identity Module
SLAAC	Stateless Address AutoConfiguration
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TR	Technical Report
UDP	User Datagram Protocol
URL	Universal Resource Locator
USIM	Universal Subscriber Identity Module
VLAN	Virtual Local Area Network
WA	Work Area
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report proposes several public Wi-Fi network architectures with different distribution of the AC function. As a result, the impact on energy consumption will vary. In the particular case of integrating the AC function into the BNG or deploying a centralized AC co-located with the BNG, the total number of ACs is expected to go down. This provides an opportunity to lower the overall power consumption of the network.

3.2 IPv6

The architectures specified in this Technical Report can facilitate the migration to IPv6. An AP and AC without native IPv6 support can be configured as a layer 2 bridge. End device address requests are tunneled directly to the BNG. The BNG can then perform DHCPv6 and SLAAC address assignment. In addition, the BNG processes end device ICMPv6 messages such as router solicits and neighbor solicits to help resolve the default gateway address.

3.3 Security

TR-321 can enhance the security of Wi-Fi deployments. The document outlines the use of IEEE 802.11i to encrypt the wireless channel between the end user device and the AP. A new requirement in section 5.7 prevents the AP broadcasting, unicast flooding, and multicasting end device packets on the LAN segment. As a result, end device traffic is forwarded directly to the WAN interface of the AP. This can help improve security and reduce potential malicious attacks on the subscriber, as the subscriber MAC and IP address are never exposed to others.

3.4 Privacy

Architecture that utilizes IEEE 802.11i to encrypt subscriber data to the AP ensures privacy in the physical layer air space. Further, a new AP requirement, which tunnels subscriber traffic directly to and from the AP WAN interface, isolates subscriber traffic from each other at layer 2. This requirement prevents any possibility of packet eavesdropping between Wi-Fi devices.

The architecture that utilizes IEEE 802.11i to encrypt subscriber data to the AP ensures privacy in the physical layer air space. Further, a new AP requirement, which tunnels subscriber traffic directly to and from the AP WAN interface, isolates each subscriber's traffic at layer 2. This requirement prevents packet eavesdropping between Wi-Fi devices.

4 Introduction

As the use of smart mobile devices continues to show vast growth, it puts tremendous strain on the mobile network. Network operators are faced with various engineering challenges when scaling the mobile network such as: shortage of spectrum, placement of additional antennas, and the oversubscription ratio that can be used (especially in highly populated area). Besides engineering challenges, service providers face the prospect of significant CAPEX investment and installation costs, for example purchasing spectrum, installation of antennas, and new equipment. There is also the prospect of higher OPEX as the network size and traffic increases. In an effort to address these challenges, service providers have been considering using Wi-Fi to move traffic off the mobile network onto the fixed broadband network. Wi-Fi is an obvious choice as it is a standard feature on smart mobile devices. These devices have also implemented Wi-Fi authentication methods such as EAP-SIM/AKA, making the authentication process seamless for the end user. As a result, the end user can transition from the mobile network to a Wi-Fi network with little or no service interruption.

Many service providers offer Wi-Fi as part of their basic broadband service. Subscribers can utilize their service provider's public Wi-Fi to avoid mobile data roaming charge or in areas with slower or weak mobile data coverage. Another popular use of public Wi-Fi is for visitors from other countries who can purchase public Wi-Fi service to avoid international roaming charges. These public Wi-Fi services are rather different to legacy Wi-Fi "hotspots" (e.g. single AP in a café) as they cover a relative large geographic area (e.g. a downtown area) and may offer QoS capabilities.

Wi-Fi only provides the physical access, end devices still require authentication and address assignment. This document provides use cases, architecture requirements and nodal requirements for the AP, the AC and the BNG for public Wi-Fi access.

5 Use Cases for Public Wi-Fi Access

5.1 Wi-Fi Hotspots for Public Wireless Access

Operators may deploy Wi-Fi networks in public places for their own subscribers - as well as those of their roaming partners - in order to offer an access service. Wi-Fi enabled end user devices with or without (U)SIMs, such as smart phones, tablets and laptops can connect to that Wi-Fi network. The Wi-Fi network is deployed as an extension of the fixed network, and can help relieve mobile network congestion.

In places with Wi-Fi deployment, subscribers need to be authenticated before they can access the Internet. The authentication methods used by operators include portal and IEEE 802.1X authentication. There may be multiple SSIDs configured by multiple operators each of which may require different authentication types, for example, one open SSID for the subscribers using portal authentication and one secure SSID for subscribers using IEEE 802.1X authentication.

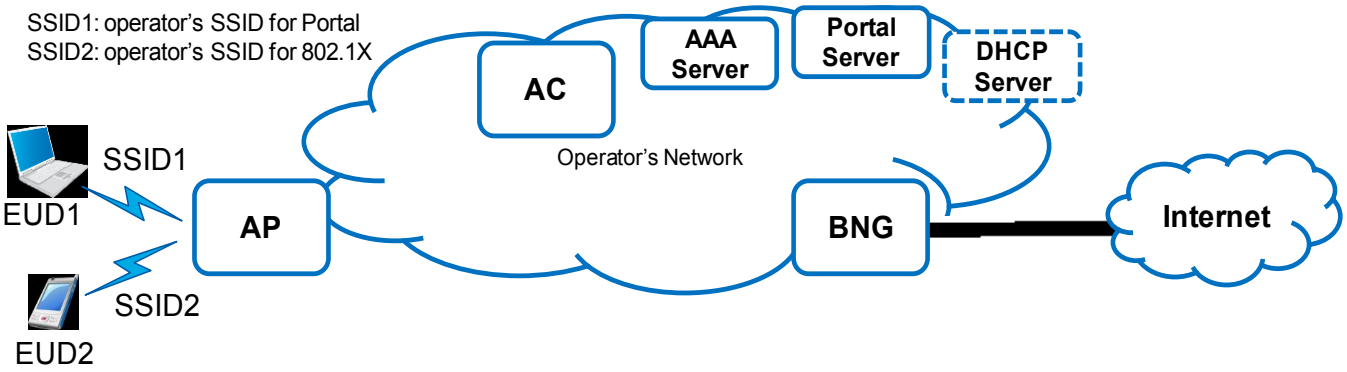


Figure 1 - Wi-Fi hotspots for public wireless access

5.2 Interworking of Wi-Fi and the 3GPP Network

A subscriber using a mobile phone in a public place may need to access the Internet irrespective of the access type. In this case, the operator may need to deploy a Wi-Fi network following the requirements in TR-203 and TR-291; the mobile devices can then roam between networks. To achieve this public Wi-Fi needs to support uniform authentication methods (i.e. EAP-SIM/AKA/AKA'), 3GPP routed traffic, and Wi-Fi offloading.

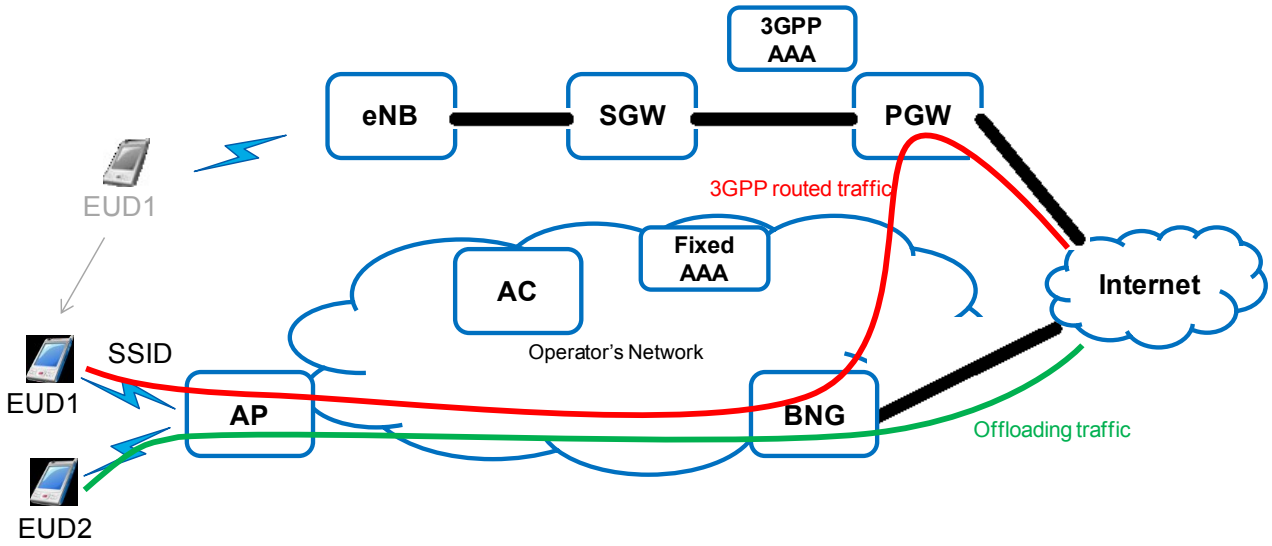


Figure 2 - Interworking of Wi-Fi and 3GPP network

5.3 Wholesale Wi-Fi

A network operator may provide Wi-Fi wholesale services to other network operators such as virtual network operators or Internet service providers. The Wi-Fi wholesale traffic can be routed to the subscribers home network or directly to the Internet according to the agreement between the network operator and the wholesale customer.

There are two wholesale variants, described below.

5.3.1 Home Routed Model of Operation

In the home routed model, the network owner operator (Operator A in Figure 3) routes the wholesale traffic belonging to subscribers of the retail operator to their home network.

Figure 3 shows an example of the home routed model. Operator A provides Wi-Fi wholesale services to operator B. EUD2, belonging to an operator B subscriber, can access the Wi-Fi service via operator A's Wi-Fi network. The traffic is routed back to operator B's network (i.e. the EUD2's home network). In this model, operator B is responsible for authenticating and accounting of EUD2.

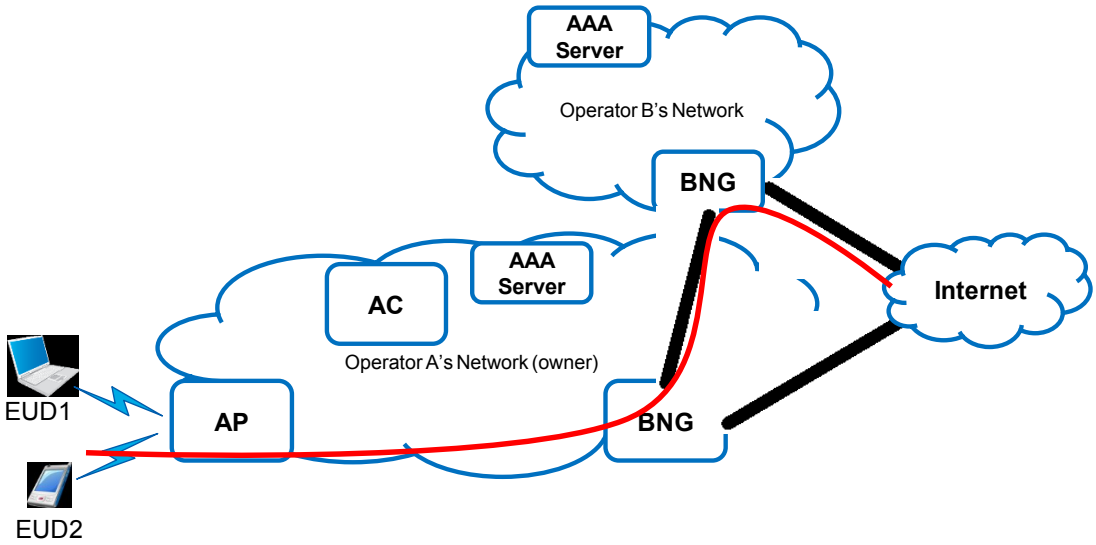


Figure 3 - Wi-Fi wholesale (home routed model)

5.3.2 Local Breakout Model of Operation

In the local breakout model, the network operator routes the wholesale traffic to the Internet locally. The local breakout model is usually preferred when the retail operator does not a Wi-Fi network, or when the retail operator requests the wholesale operator to provide Internet connection directly.

Figure 4 shows an example of the local breakout model Operator A provides a Wi-Fi wholesale service to operator B. EUD2, belonging to an Operator B subscriber, can access the Wi-Fi service via operator A's Wi-Fi network. The traffic is routed directly to the Internet. In this model, EUD2 obtains an IP address in the visited network (i.e. Operator A's network). The subscriber's authentication and accounting information is conveyed to Operator B.

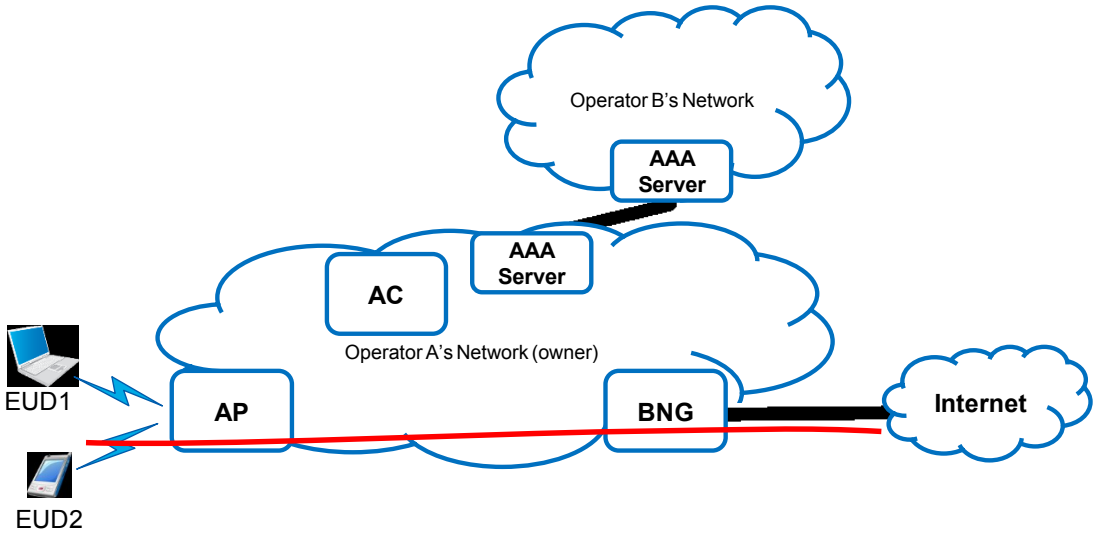


Figure 4 - Wi-Fi wholesale (local breakout model)

5.4 Community Wi-Fi

A fixed network operator can have an agreement with their subscribers to share their RG/AP. In this case, the RG/AP can advertise multiple SSIDs. Private SSIDs dedicated to the subscriber are used for home network access, and the operator's common SSID is used for public access. A visiting friend or a subscriber passing by can access the Internet using the operator's SSID. Community Wi-Fi is different from the hotspot use cases, the AC is not a mandatory requirement to manage the RG/APs. To support mobility, the RG/APs must meet the requirements in TR-291 section 6.1, 7.4, and 10.1.

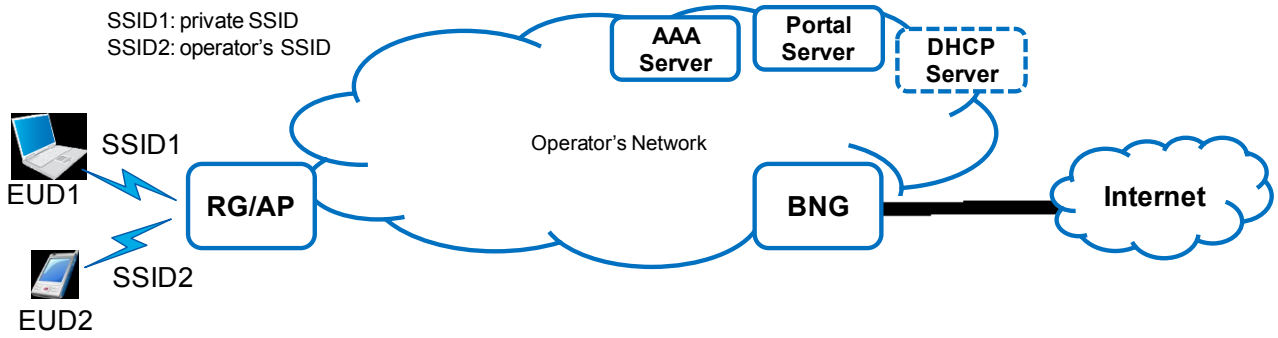


Figure 5 - RG-hosted Wi-Fi hotspots

5.5 Location Based Service

There are two location methods, geo-location based which is very precise, and network topology based, which only provides a rough estimate. Geo-location provides the exact longitude and latitude of an EUD. Network topology based location only positions the EUD as within the coverage area of a given AP.

To obtain the geo-location of an EUD, several APs are used to triangulate it. The APs only provide signal strength and other EUD related information, the calculation of the EUD's exact location is performed by a back-end location server. The EUD's geo-location will be updated periodically. The back-end location server defines the APs' information update interval.

Where only network topology based location is required, this is simply based on the knowledge of the AP identity (e.g. AP MAC or AP based VLAN) and location. The network topology based location is first obtained after an EUD successfully authenticates. Subsequent updates are done when the EUD moves between APs.

Based on the location information, the operator can offer location based service to their subscribers, such as advertisements and assisting with emergency services (e.g. fire, rescue).

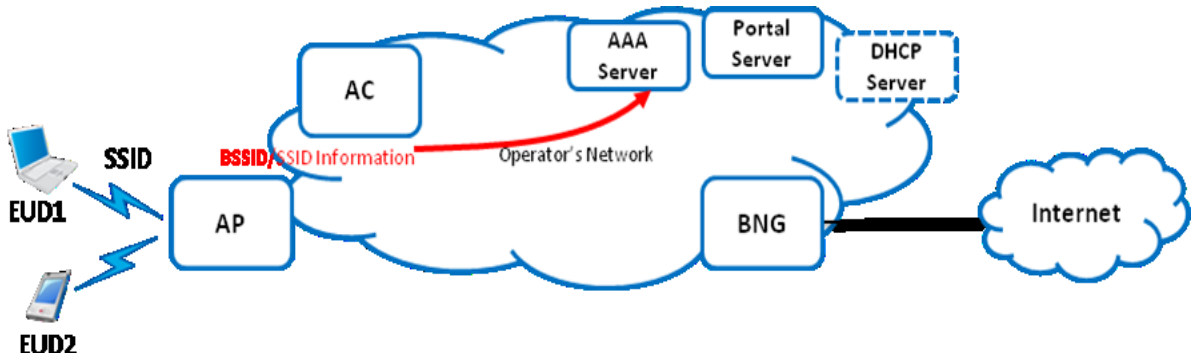


Figure 6 - Location based service in public Wi-Fi network

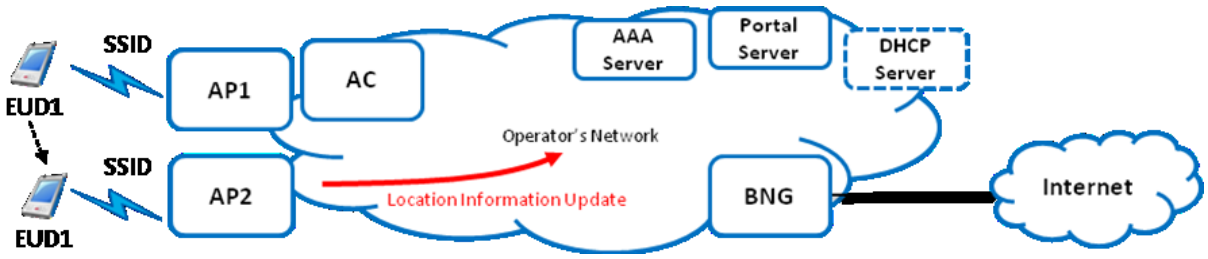


Figure 7 - Location reporting during handover

5.6 Unauthenticated IPv4 Wi-Fi Subscribers

Public Wi-Fi is a very dynamic type of service where every second many subscriber sessions are created and deleted. People regularly search for 'free' Internet access through open SSIDs but then find themselves landing on a portal login page. This makes it difficult to use private/public addresses and accounting records for these "unauthenticated" subscribers.

The BNG needs to employ techniques to reduce resource consumption by "unauthenticated" subscribers (see R-31 to R-34 in section 8.2).

5.7 Public Wi-Fi NAT

Service providers already have several private pools of addresses to maintain and manage; these are for wireless/wireline equipment, device management and the subscriber addresses themselves. The addition of public Wi-Fi creates the need for yet another private IP address pool. To optimize the utilization of private addreses and reduce management overhead, all Wi-Fi subscribers could be assigned the same private address. This provides additional benefits such as security (allowing only a single address while filtering others) and EUD mobility (where the default gateway is always the same). However, this will then require this common address to be translated by a layer 2 aware NAT.

5.8 Wi-Fi Mobility support within a BNG

The BNG acts as the IP gateway for the EUD device. The APs and ACs provide pure layer 2 transport between the EUD and the BNG. The goal is to achieve seamless AP to AP mobility for both the standalone and distributed AC architectures.

In the standalone AC architecture, depicted in Figure 8, the AC notices that the EUD is moving from AP to AP. The AC ensures that the EUD data traffic remains on the same logical interface on the BNG. From the perspective of the EUD, it has moved between two different APs; however, from the BNG perspective, there was no data path change. To ensure seamless mobility, the best practice is to reuse the same Ethernet interface or encapsulated tunnel to minimize the interruption for the EUD. Further, if required, the AC should translate the VLAN for the same SSID. The protocol stack is shown in section 6.4. With the AC handing off the EUD traffic to the BNG using both the same port and same VLAN, the BNG will not detect a mobility event.

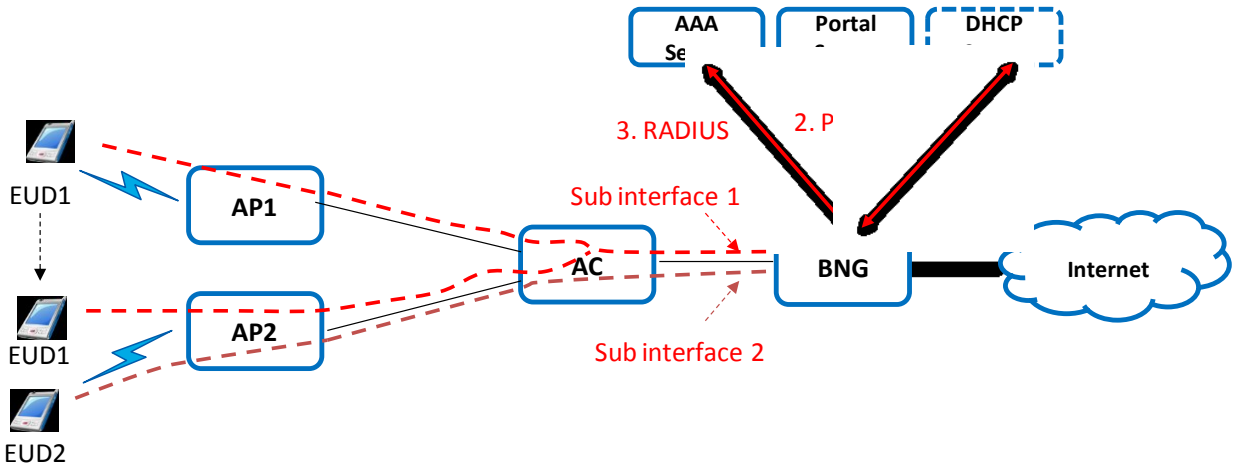


Figure 8 - Wi-Fi mobility in the standalone AC architecture

In the distributed AC architecture, depicted in Figure 9, EUD mobility between APs will result in the subscriber moving to a different BNG interface. EUD traffic might arrive at the BNG with a layer 3 encapsulation, or in native Ethernet. In mobility, this means the same subscriber using different fields in the encapsulation, or a different Ethernet port. The BNG must be able to accept the subscriber traffic with minimal interruption. On a traditional BNG, this is equivalent to a subscriber moving to a new home, taking the RG with him/her.

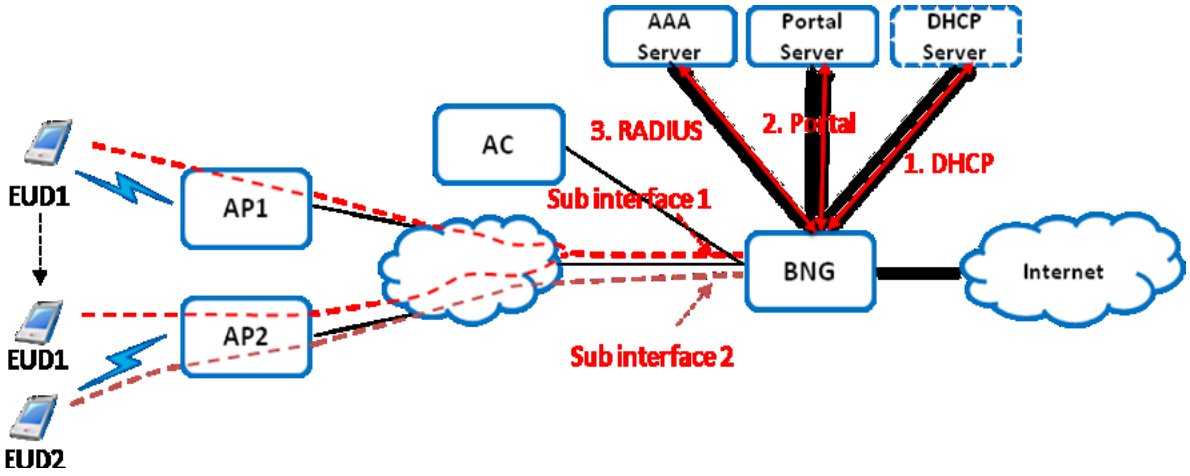


Figure 9 - Wi-Fi mobility in the distributed AC architecture

6 Public Wi-Fi Access Network Architecture

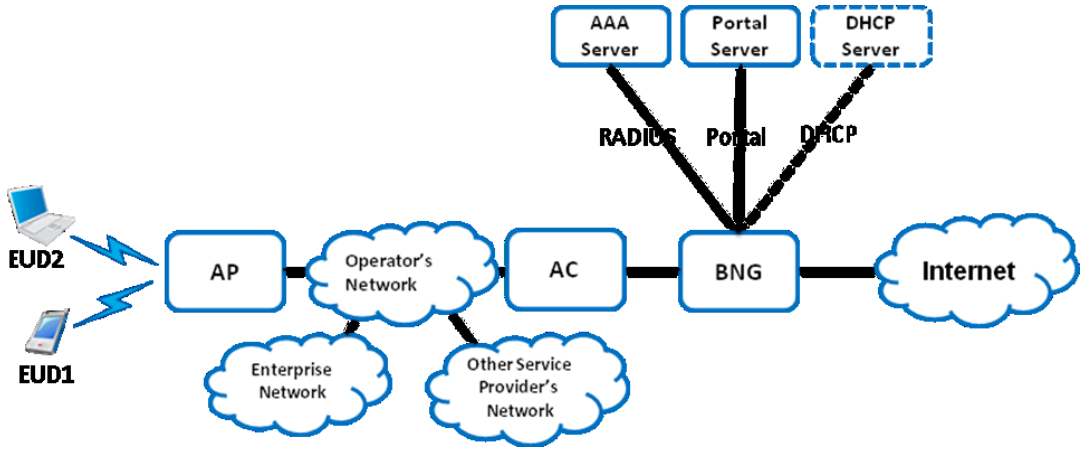
This section describes public Wi-Fi network architectures which are aligned with TR-101, TR-145 and TR-178 architectural principles.

6.1 Architecture 1: Standalone AC Architecture

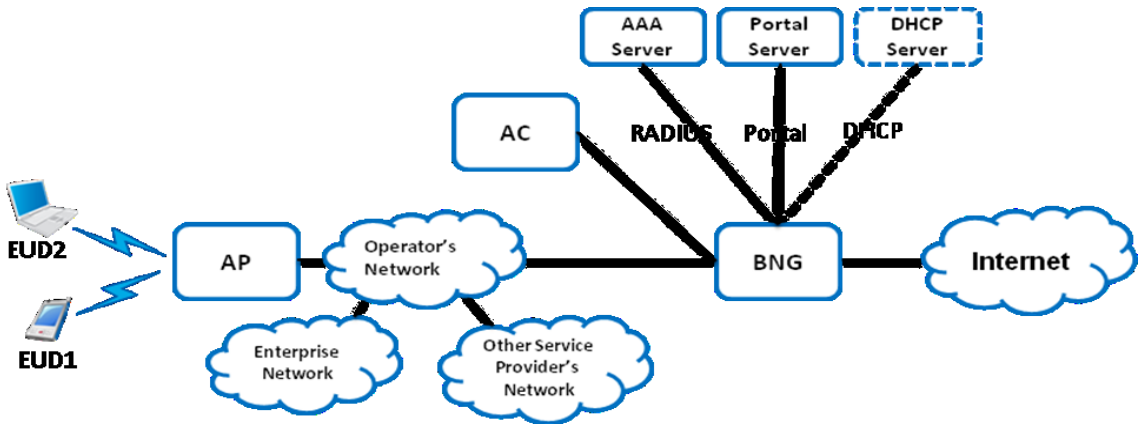
In the standalone AC architecture (shown in Figure 10), all of AP's traffic including control, management and Wi-Fi data traffic (with the Internet as the destination) is first aggregated at the AC. The AC then forwards the traffic towards the BNG. Since the AC is on the data path, the AC can provide additional QoS and filtering treatment to the subscriber traffic. A single physical AP can advertise multiple SSIDs for different Wi-Fi providers or different services. For example, enterprise traffic can be offloaded locally via a specific SSID.

There are several assumptions in this architecture:

- The AC is responsible for control and management of the APs.
- The AC is not responsible for IP address assignment of EUDs.
- The BNG manages traffic on a per subscriber basis.
- The AC location can vary:
  - The AC can be deployed closer to the APs than the BNG if there is a high density of APs deployed.
  - The AC can be co-located with the BNG.
- The AC can communicate with the AAA directly, or via a RADIUS proxy (e.g. BNG).
- The AP needs to support multiple SSIDs.
- Different authentication methods (e.g. IEEE 802.1X, web portal) need to be supported for different SSIDs.
- Different SSIDs can be used to connect to different networks such as other service providers' and enterprise networks.



(a) AC deployed in close proximity to the APs



(b) AC co-located with BNG

Figure 10 - Architecture 1: standalone AC architecture

6.2 Architecture 2: BNG Integrated AC Architecture

In the BNG integrated AC architecture (shown in Figure 11), the AC functionality is incorporated within the BNG. All of the AP's traffic including control, management and subscriber data traffic (with the Internet as the destination) are aggregated at the integrated AC and BNG node. This architecture can provide a single point of control and management, and the access network architecture can be simplified. A single physical AP can advertise multiple SSIDs for different Wi-Fi providers or different services. For example, enterprise traffic can be offloaded locally via a specific SSID.

There are several assumptions in this architecture:

- The AC is responsible for control and management of APs.
- The AC/BNG node manages traffic on a per subscriber basis.
- The AP needs to support multiple SSIDs.
- Different authentication methods (e.g. IEEE 802.1X, web portal) need to be supported for different SSIDs.
- Different SSIDs can be used to connect to different service providers or enterprise networks.

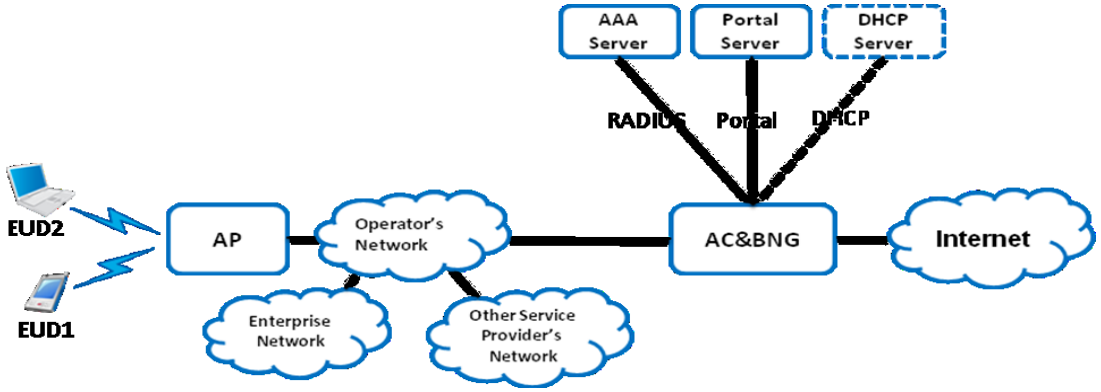


Figure 11 - Architecture 2: BNG integrated AC architecture

6.3 Architecture 3: Distributed AC Architecture

In the distributed AC architecture (shown in Figure 12), only APs' control and management traffic is forwarded to the AC, while the Wi-Fi data traffic (with the Internet as the destination) is forwarded straight to the BNG, via either a tunnel or an Ethernet link. In this architecture, the AC is not on the data path, so there is no requirement on the data processing and forwarding capability of the AC. The AC can be deployed in a more centralized location to manage a higher number of APs that are spread across different geographic locations, which will also facilitate AC virtualization when migrating to NFV. A single physical AP can advertise multiple SSIDs for different Wi-Fi providers or different services. For example, enterprise traffic can be offloaded locally via a specific SSID.

There are several assumptions in this architecture:
- The AC is responsible for control and management of APs.
- The BNG manages traffic on a per subscriber basis.
- The AP needs to support multiple SSIDs.
- Different authentication methods (e.g. IEEE 802.1X, web portal) need to be supported for different SSIDs.
- Different SSIDs can be used to connect to different service providers or enterprise networks.

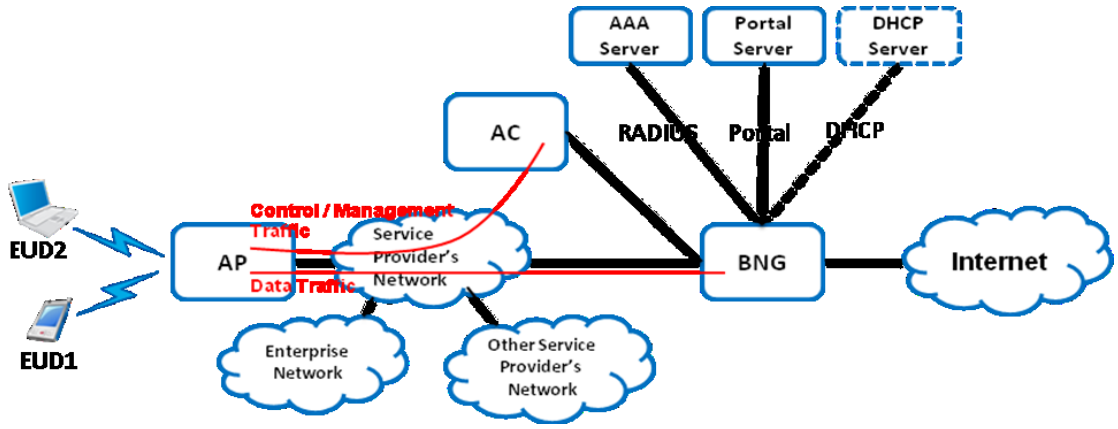


Figure 12 - Architecture 3: distributed AC architecture

6.4 Protocol Stack

An AP in close proximity to the BNG can bridge subscriber traffic to the BNG via native Ethernet. There are use cases where the BNG is placed closer to the core of the network to aggregate a large number of APs. As a result, there are two different protocol stacks depending on the placement of the BNG and the APs.

6.4.1 Protocol Stack 1: Native Ethernet

A high concentration of APs may be in close proximity to the BNG such as in a sports stadium or a shopping center. The subscriber traffic can be simply bridged from the AP to the BNG. The AC or the AP inserts a VLAN on the subscriber packet to identify the SSID that the subscriber is using.

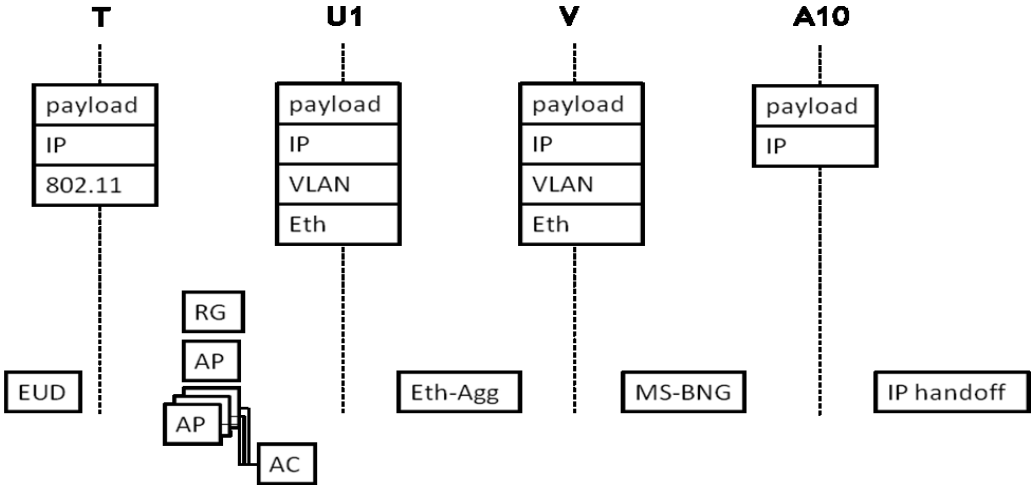


Figure 13 - Protocol stack 1: native Ethernet transport

Note: In the standalone AC architecture, the AC is on the data path, and the protocol stack on the U1 interface is provided by the AC. In the distributed AC architecture, the AC is not on the data path, so the protocol stack on the U1 interface is provided by the AP or the RG.

6.4.2 Protocol Stack 2: Layer 3 Tunneling

In cases such as community Wi-Fi, APs can be widely dispersed. Operators might choose to place the BNG towards the network core in order to aggregate hundreds of thousands of APs. In this architecture, an IP network might exist between the APs and the BNG. Therefore, all subscriber traffic are required to be bridged between the AP and the BNG over an IP network. To bridge subscriber traffic over an IP network, native Ethernet frames are encapsulated in an L3 tunnel (e.g. IP-GRE). The AC or the AP will first insert a VLAN on the subscriber packet to identify the SSID that the subscriber is using. Afterwards, an IP-GRE header encapsulates the subscriber frame along with the inserted VLAN ID.

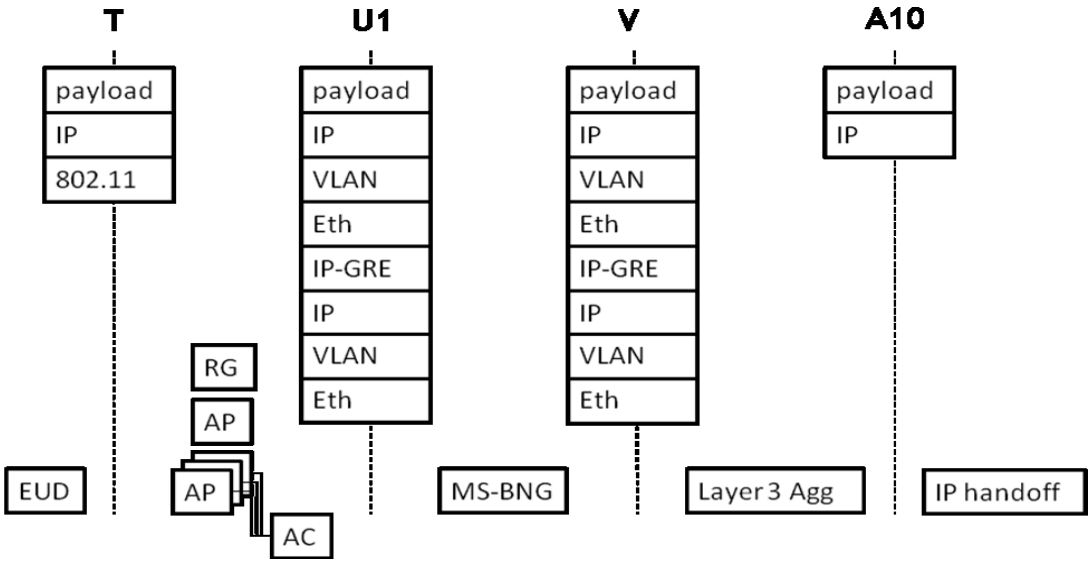


Figure 14 - Protocol stack 2: layer 3 tunneling

Note: In the standalone AC architecture, the AC is on the data path, and the protocol stack on the U1 interface is provided by the AC. In the distributed AC architecture, the AC is not on the data path, so the protocol stack on the U1 interface is provided by the AP or the RG.

7 Authentication Techniques

7.1 IEEE 802.1X Authentication

7.1.1 Scenario 1: the AC and the BNG are Separated, the AC is the Authenticator, the BNG Acts as RADIUS Proxy

In this scenario (shown in Figure 15), the AC is the IEEE 802.1X authenticator, and the BNG is the RADIUS proxy. In the network, the BNG is the service gateway. The BNG is aware of the EUD's information, and is responsible for IP address assignment and traffic management on a per subscriber basis. Key exchange and IP address assignment procedures are initiated after the successful EAP session establishment. The authentication flow for scenario 1 is shown in Figure 16.

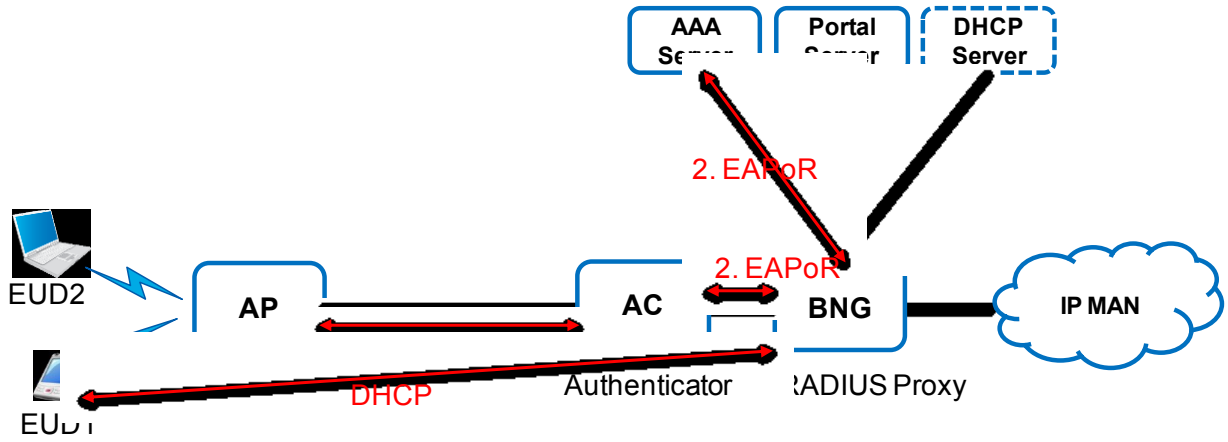


Figure 15 - Scenario 1 of IEEE 802.1X authentication

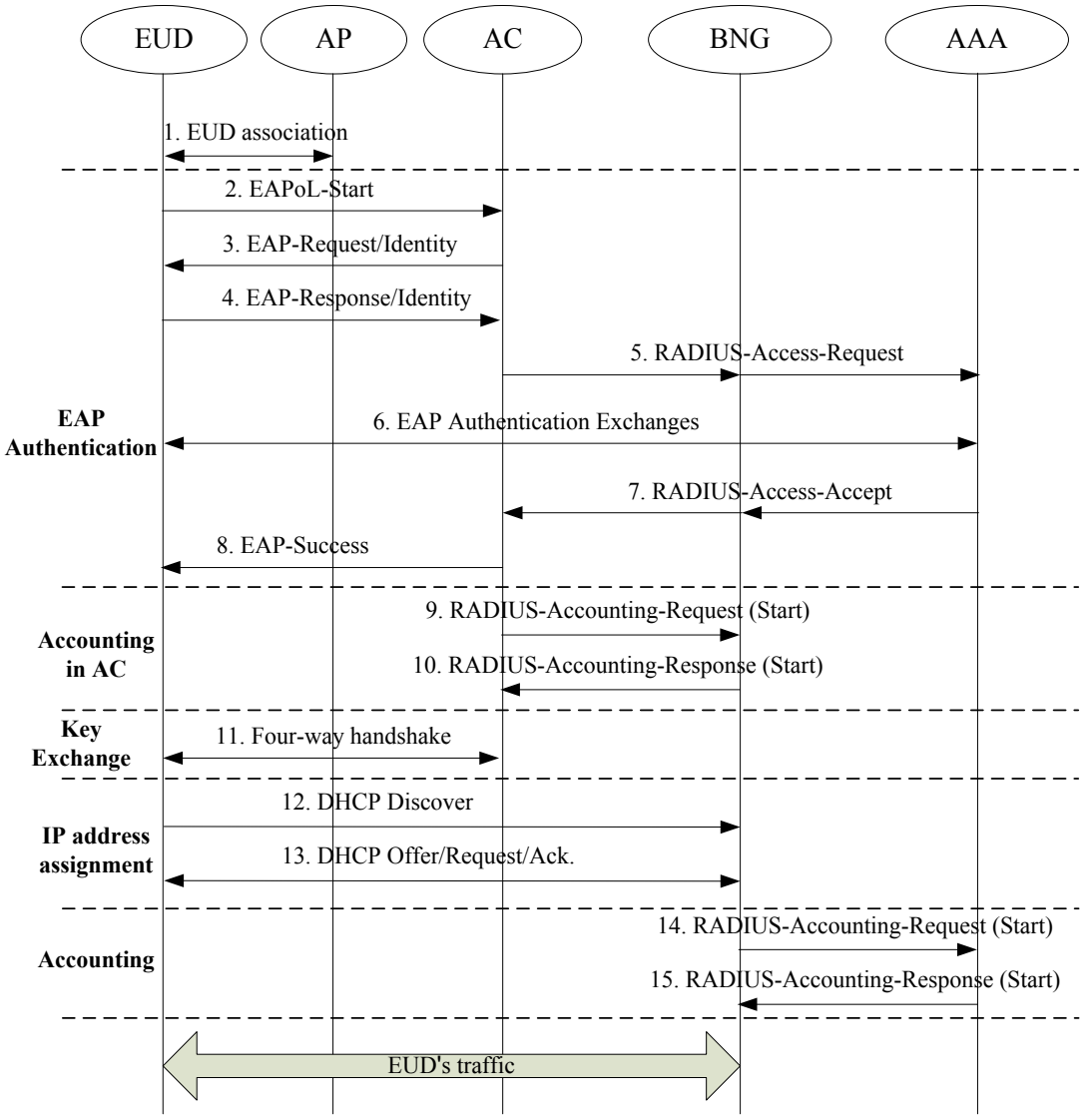


Figure 16 - Authentication flows for scenario 1 of IEEE 802.1X authentication

7.1.2 Scenario 2: the AC and the BNG are Separated, the AC is the Authenticator, the BNG is not the RADIUS Proxy

In this scenario (shown in Figure 17), the AC is the IEEE 802.1X authenticator, and the BNG is not the RADIUS proxy. The BNG is the service gateway. The BNG is responsible for IP address assignment, and traffic management on a per subscriber basis. It is assumed that the BNG can obtain EUD's authentication information from the AAA. Key exchange and IP address assignment procedures are initiated after the successful EAP session. The authentication flow for scenario 2 is shown in Figure 18.

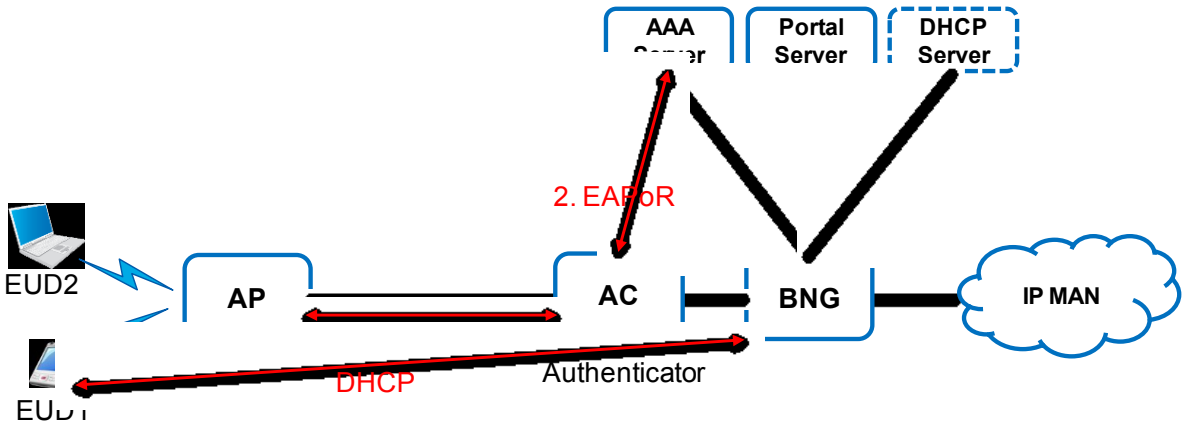


Figure 17 - Scenario 2 of IEEE 802.1X authentication

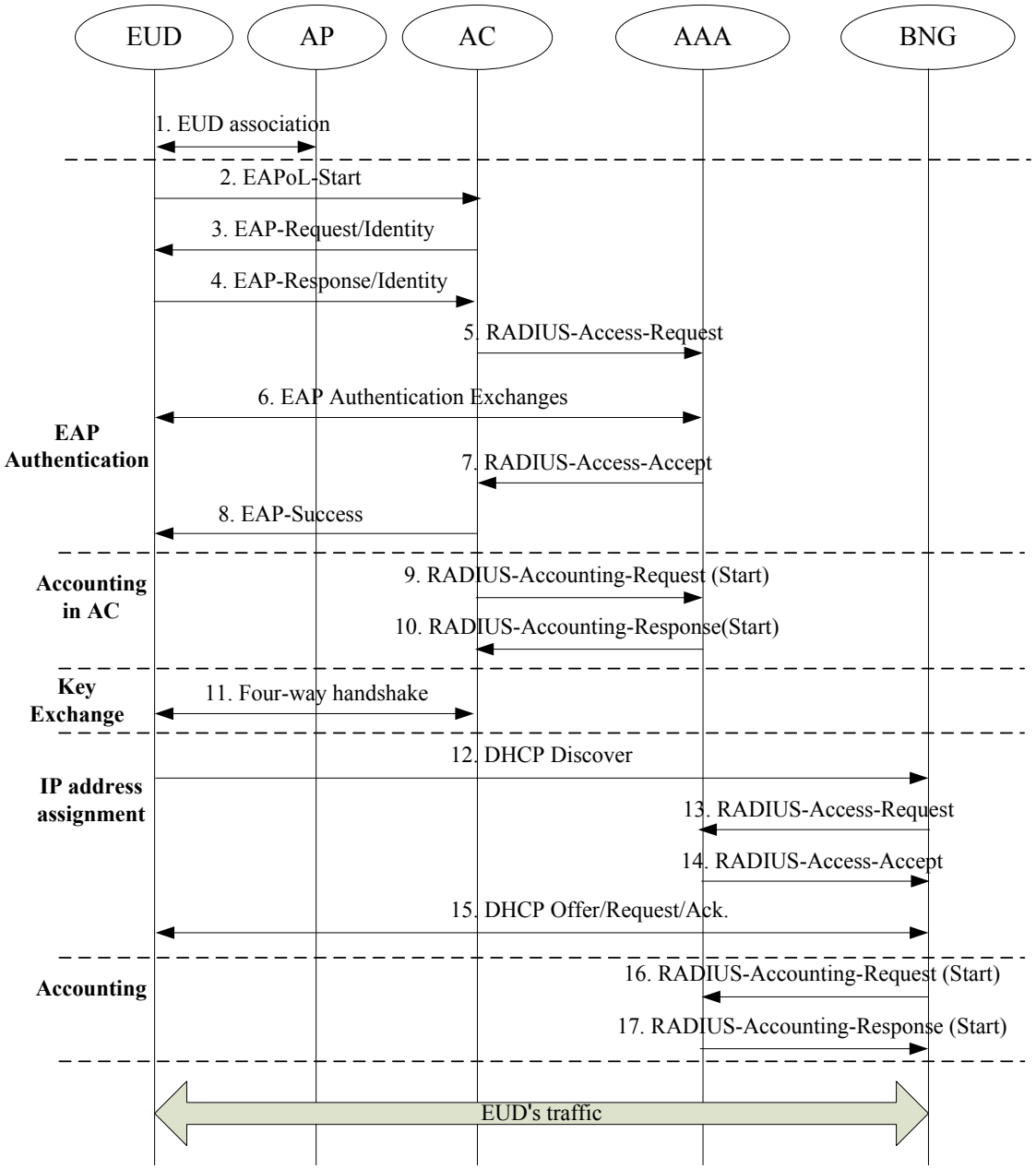


Figure 18 - Authentication flows for scenario 2 of IEEE 802.1X authentication

7.1.3 Scenario 3: the AC and the BNG are Separated, the BNG Acts as the Authenticator

In this scenario (shown in Figure 19), the BNG is the IEEE 802.1X authenticator. The BNG is responsible for IP address assignment, and traffic management on a per subscriber basis. The AC needs to acquire the PMK based on IEEE 802.11i requirements in the key exchange via RADIUS packets. The authentication flow for scenario 3 is shown in Figure 20.

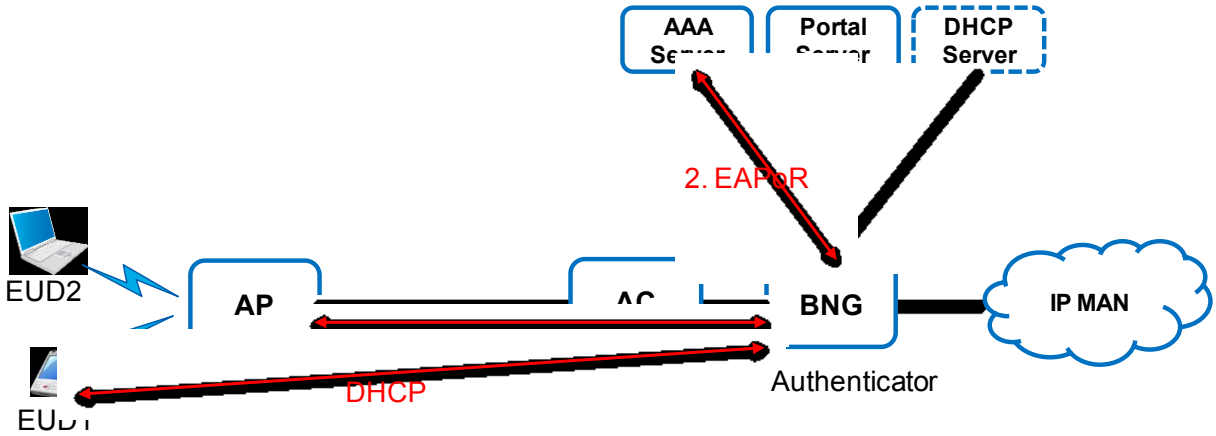


Figure 19 - Scenario 3 of IEEE 802.1X authentication

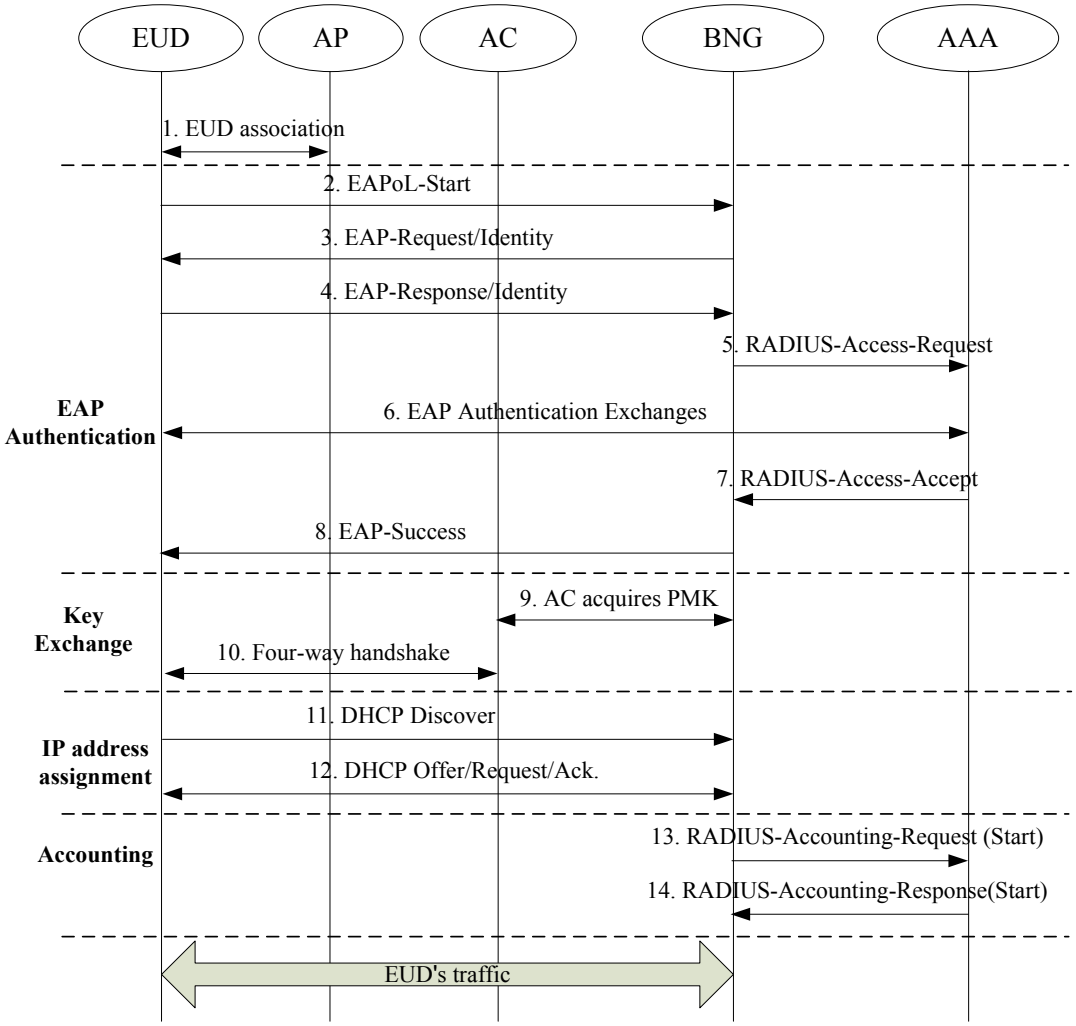


Figure 20 - Authentication flows for scenario 3 of IEEE 802.1X authentication

7.1.4 Scenario 4: the AC and the BNG are Integrated

In this scenario (shown in Figure 21), the AC is integrated with the BNG, as the IEEE 802.1X authenticator. The integrated AC and BNG node is responsible for IP address assignment, and traffic management on a per subscriber basis. Key exchange and IP address assignment procedures are initiated after the successful EAP session. The authentication flow for scenario 4 is shown in Figure 22.

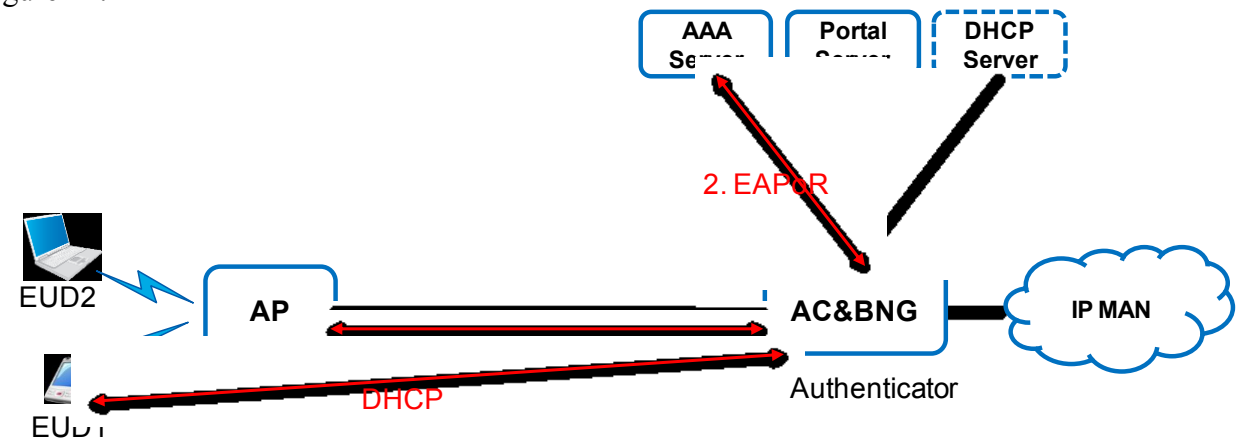


Figure 21 - Scenario 4 of IEEE 802.1X authentication

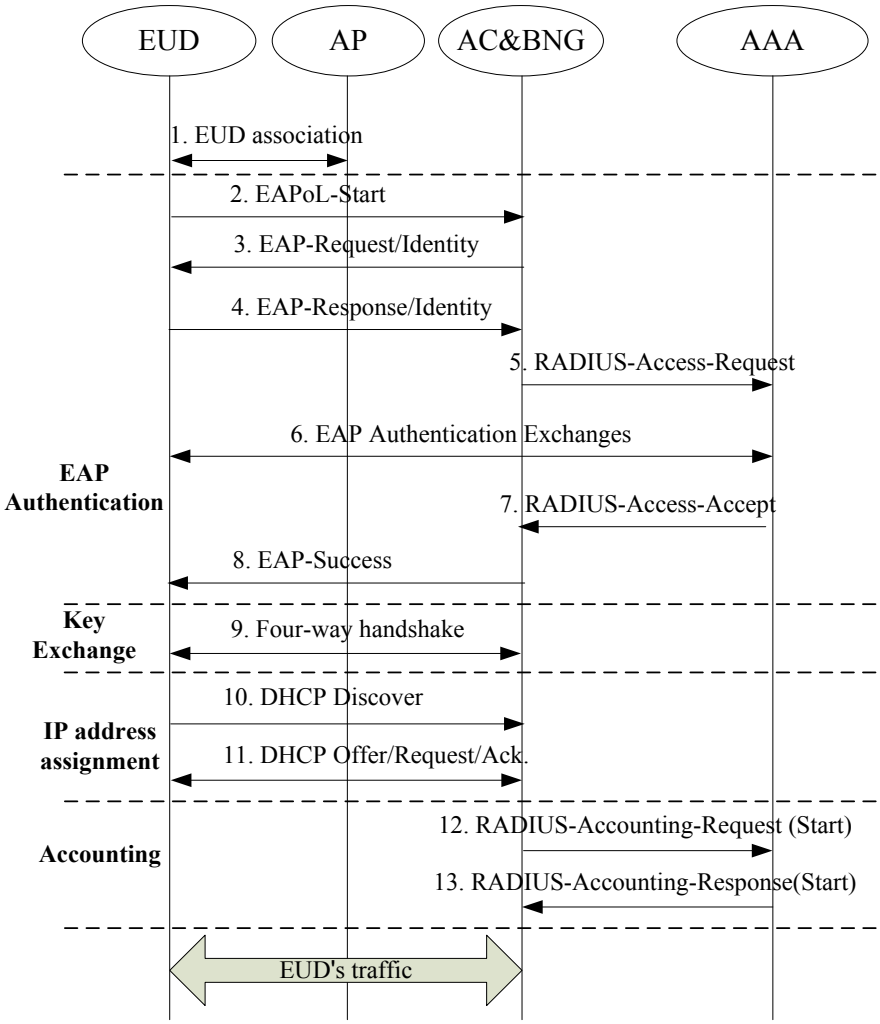


Figure 22 -Authentication flows for scenario 4 of IEEE 802.1X authentication

7.2 Portal Authentication

In portal authentication, a subscriber is identified by an operator-assigned username and password. .

7.2.1 Scenario 1: the AC and the BNG are Separated

When the AC and the BNG are separated, the BNG is responsible for IP address assignment and traffic management on a per subscriber basis.

The BNG is responsible for redirecting the HTTP traffic of the EUD to the portal server before the EUD is successfully authenticated. The subscriber needs to input the username and password in the portal page provided by the portal server. After successful authentication, traffic is forwarded in the normal manner.

The AAA is responsible for authentication and accounting. Additionally, the AAA provides the policy and QoS configuration of the EUD to the BNG as part of the RADIUS Access Accept message.

Re-authentication may be required after a specified period of time or a volume quota.

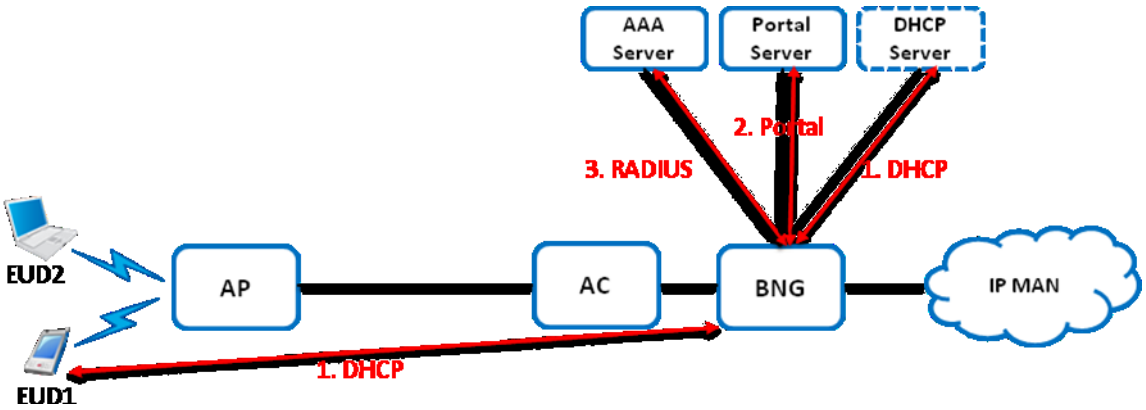


Figure 23 - Scenario 1 of portal authentication

7.2.2 Scenario 2: the AC and the BNG are Integrated

When the AC is integrated with the BNG, the AC/BNG is responsible for IP address assignment and traffic management on a per subscriber basis, and redirecting the HTTP traffic of the EUD to the portal server before the user is successfully authenticated. The subscriber needs to input the username and password in the portal page provided by portal server. After successful authentication, traffic is forwarded in the normal manner.

The AAA is responsible for authentication and accounting. Additionally, the AAA provides the policy and QoS configuration of the EUD to the BNG as part of the RADIUS Access Accept message.

Re-authentication may be required after a specified period of time or when a volume quota is reached.

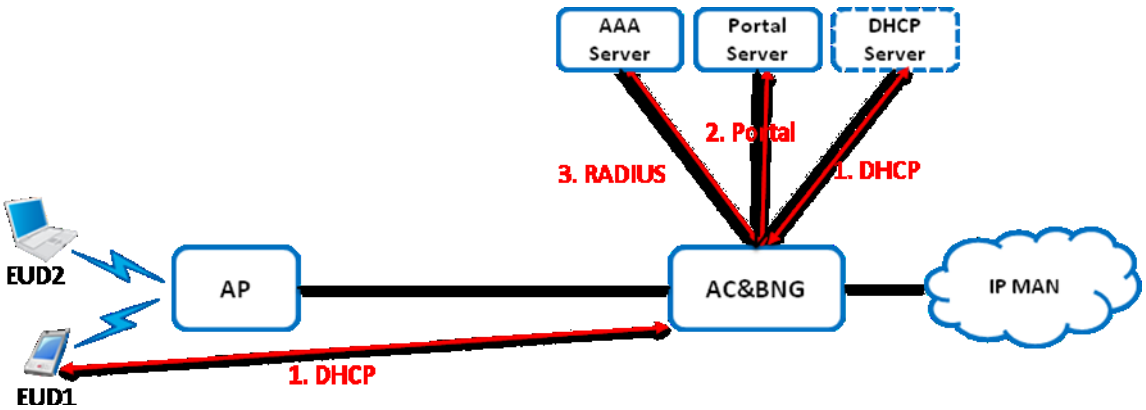


Figure 24 - Scenario 2 of portal authentication

7.2.3 Authenticated Portal Subscribers

A suggested best practice is that once the subscriber is authenticated, they should not be redirected to a sign-in portal until their credit is exhausted

Once the EUD is away from the AP or has gone into sleep mode, the subscriber session can time out and the subscriber record will be purged from the BNG. If the EUD reconnects, then the AAA should have sufficient information to determine if the subscriber requires portal re-direction for authentication. The AAA should be able to provide a known authenticated subscriber Internet access immediately, without portal authentication.

8 Nodal Requirements

8.1 AP Requirements

[R-1] The AP MUST support multiple SSIDs. **M**

[R-2] The AP MUST relay customer Ethernet frames to an AC in the standalone AC architecture.

[R-3] The AP MUST relay customer Ethernet frames to a BNG in the distributed AC architecture.

[R-4] 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. **M**

[R-5] The AP MUST prevent local switching of user traffic. **M**

[R-6] The AP MUST support a stateless IPv4 or IPv6 tunneling mechanism. The tunnel protocol stack is specified in section 6.4. **M**

[R-7] 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. **M**

Requirements R-8 and R-9 apply to different scenarios of IEEE 802.1X and portal authentication.

Table 1 - AP requirements for different authentication scenarios

	IEEE 802.1X authentication				Portal authentication	
	Scenario 1 (separated AC and BNG, AC - authenticator, BNG - RADIUS proxy)	Scenario 2 (separated AC and BNG, AC - authenticator, BNG - not RADIUS proxy)	Scenario 3 (separated AC and BNG, BNG - authenticator)	Scenario 4 (integrated AC and BNG)	Scenario 1 (separated AC and BNG)	Scenario 2 (integrated AC and BNG)
R-8			x		x	
R-9	x	x	x		x	

[R-8] The AP MUST support a DHCP relay function and insert the BSSID and SSID into DHCP option 82 during IP address allocation or renewal of an EUD. **M**

To support Wi-Fi mobility within the BNG, requirement R-9 applies to the different APs under the same BNG in the distributed AC architecture.

[R-9] In the distributed AC architecture, the AP MUST place all traffic from a given SSID in the same VLAN. **M**

8.2 BNG Requirements

[R-10] The BNG MUST support IPv4 and IPv6 GRE stateless tunneling. **M**

Before traffic is sent over TCP, TCP will first negotiate the payload size for bi-directional traffic. This is known as the maximum segment size (MSS). The MSS size can be changed to avoid fragmentation between routers.

[R-11] The BNG MUST support TCP MSS adjust for Wi-Fi subscribers' TCP traffic.

In the case where subscriber packets are tunneled, the encapsulation will put an extra header on subscribers' IP packet. It is possible that the packet will be fragmented while tunneling to the BNG. Fragmentation and reassembly cause a lot of inefficiency. Therefore, the tunnel path should support an MTU size that usually avoids fragmentation. However, in some cases fragmentation cannot be avoided.

[R-12] The BNG MUST support reassembly of subscribers' upstream fragmented UDP/IP encapsulated tunneled traffic.

[R-13] The BNG MUST support fragmentation of subscribers' downstream UDP/IP encapsulated tunneled traffic.

[R-14] The BNG MUST support EUD mobility for both tunneled traffic and native Ethernet traffic.

[R-15] When a subscriber moves to a new AP, the BNG MUST be able to move the subscriber context to a different interface. This applies to the case where the subscriber traffic is natively bridged from the AP to the BNG.

[R-16] When a subscriber moves to a new AP, the BNG MUST accept the subscriber encapsulated packet with a new source IP. This applies to the case where the subscriber traffic is tunneled from the AP to the BNG.

[R-17] The BNG MUST be able to perform L2-aware NAT. **M**

Requirements R-18 to R-41 apply to different scenarios of IEEE 802.1X and portal authentication.

Table 2 - BNG requirements for different authentication scenarios

	IEEE 802.1X authentication				Portal authentication	
	Scenario 1 (separated AC and BNG, AC - authenticator, BNG - RADIUS proxy)	Scenario 2 (separated AC and BNG, AC - authenticator, BNG - not RADIUS proxy)	Scenario 3 (separated AC and BNG, BNG - authenticator)	Scenario 4 (integrated AC and BNG)	Scenario 1 (separated AC and BNG)	Scenario 2 (integrated AC and BNG)
R-18			x	x		
R-19	x					

R-20		x	x	x	x	x
R-21	x					
R-22	x	x	x	x		
R-23		x				
R-24		x				
R-25	x	x	x	x		
R-26				x		
R-27					x	x
R-28					x	x
R-29					x	x
R-30					x	x
R-31					x	x
R-32					x	x
R-33					x	x
R-34					x	x
R-35					x	x
R-36	x		x		x	
R-37	x		x		x	
R-38					x	x
R-39	x	x	x	x	x	x
R-40	x	x	x	x	x	x
R-41					x	x

[R-18] The BNG MUST be able to act as an IEEE 802.1X Authenticator.

[R-19] The BNG MUST support a RADIUS proxy in order to relay EAP packets to the AAA server. **M**

[R-20] The BNG MUST support a RADIUS client for Radius accounting purposes.

[R-21] The BNG MUST proxy the EAPoR packets in order to acquire the EUD information (e.g. MAC address, IMSI) for accounting and management. **M**

[R-22] The BNG MUST confirm that the EUD has been successfully authenticated before assigning an IP address.

[R-23] Upon receiving a DHCP Discover message, the BNG MUST initiate the RADIUS Access Request message based on MAC address to the AAA in order to check whether the EUD has been successfully authenticated.

[R-24] The BNG MUST be able to receive the EUD information (e.g. IMSI) for accounting and user management from the AAA.

[R-25] Upon IP address allocation, the BNG MUST send an Accounting Start Message to the AAA. **M**

[R-26] The BNG MUST support 4-way IEEE 802.11i handshake with the EUD. **M**
Note: As the AC function has been moved to the BNG, it needs to support IEEE 802.11i.

[R-27] The BNG MUST assign an IP address to an EUD independent of the EUD authentication state when using portal authentication. **M**

[R-28] The BNG MUST be able to redirect or apply a policy route to the HTTP traffic of unauthorized EUDs to the portal server for portal authentication. **M**

[R-29] The BNG MUST allow the EUD to communicate with the portal server, the DNS server, and the DHCP server even if the EUD is not authenticated. All other traffic MUST remain blocked. **M**

[R-30] The BNG MUST send an Accounting Start Message for an EUD to the AAA when the EUD has been successfully authenticated. **M**

Unauthenticated EUDs use scarce public IP addresses. These EUDs only require very few NAT outside-ports for portal login. Therefore, it is beneficial for the BNG to offer unauthenticated EUDs a small NAT outside-port range, which allows a large group of unauthenticated EUDs to share a single public IP address. Once authenticated, the EUD is assigned a larger NAT outside-port range for Internet access.

[R-31] The BNG MUST be able to change the NAT outside-port range for an authenticated Wi-Fi subscriber. **M C**

[R-32] The BNG MUST be able to enforce different QoS policies depending on the authentication state. **M**

[R-33] The BNG MUST support a variable DHCP lease time for Wi-Fi subscribers. **M C**

[R-34] The BNG MUST be able to assign the same private IP address to all Wi-Fi subscribers. **M**

[R-35] The BNG MUST be able to assign different private IP addresses to different Wi-Fi subscribers. **M**

[R-36] The BNG MUST be able to insert the BSSID and the SSID into RADIUS Called-Station-Id and report the information to the AAA during the EUD access authentication. **M**

[R-37] The BNG 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. **M**

Note: In R-36 and R-37, the BSSID and the SSID are stored in Called-Station-Id as defined in RFC 3580.

[R-38] The BNG MUST support adding EUD location information (such as the BNG identifier and port information, or the BSSID/SSID) into the URL while redirecting the HTTP traffic of an unauthenticated EUD to the portal server. **M**

[R-39] The BNG MUST support time and/or volume based credit. **M**

[R-40] The BNG MUST support prepaid credit and accepting additional credit. **M**

[R-41] The BNG MUST redirect subscribers to a portal page after credit exhaustion. **M C**

8.3 AC Requirements

The AC is the network element in a public Wi-Fi network that is responsible for the centralized control and management of APs. Some basic functions of the AC are performance monitoring and fault reporting, automatic radio channel selection and adjustment, and automatic transmit power level adjustment of the APs. The AC may also support load balancing among the neighboring APs based on subscriber numbers or traffic load.

[R-42] The AC MUST support mutual discovery and authentication between the AC and the APs. **M C**

[R-43] The AC MUST support establishment and maintenance of the control/management channel and data channel between the AC and the AP in the standalone AC architecture. **M C**

[R-44] The AC MUST support establishment and maintenance of the control/management channel between the AC and the AP in the distributed AC architecture. **M C**

Note: R-42 to R-44 can be addressed by proprietary solutions.

[R-45] The AC MUST meet the general QoS requirements for the Access Node defined in TR-101 from R64 to R79.

[R-46] The AC MUST be able to implement per SSID IEEE 802.1p and DSCP based QoS policy (including marking). **M C**

[R-47] The AC MUST support traffic scheduling on a per SSID and/or per AP basis in the standalone AC architecture.

[R-48] The AC MUST be able to control the AP's IEEE 802.1p and DSCP marking capability based on SSID.

[R-49] The AC MUST be able to configure the AP traffic scheduling on a per SSID basis.

[R-50] The AC MUST be able to limit the bandwidth for the traffic on a per SSID and per AP basis in the standalone AC architecture.

[R-51] The AC MUST be able to limit the bandwidth for the traffic on a per AP basis in the standalone AC architecture.

[R-52] The AC MUST be able to limit the number of its associated EUDs on a per SSID and per AP basis. **M**

[R-53] The AC MUST be able to limit the number of its associated EUDs on a per AP basis. **M**

[R-54] The AC MUST relay customer data traffic to the BNG in the standalone AC architecture.

[R-55] The AC MUST NOT relay IEEE 802.1X frames to the BNG if the AC is the authenticator in the distributed AC architecture.

[R-56] 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). **M**

If precise location needs to be provided, requirement R-57 applies.

[R-57] 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. **M**

[R-58] In the standalone AC architecture, when an EUD moves from one AP to another, the AC MUST send the EUD traffic to the BNG on the same interface and VLAN. **M**

Requirements R-59 to R-72 apply to different scenarios of IEEE 802.1X and portal authentication.

Table 3 - AC requirements for different authentication scenarios

	IEEE 802.1X authentication				Portal authentication	
	Scenario 1 (separated AC and BNG, AC - authenticator, BNG - RADIUS proxy)	Scenario 2 (separated AC and BNG, AC - authenticator, BNG - not RADIUS proxy)	Scenario 3 (separated AC and BNG, BNG - authenticator)	Scenario 4 (integrated AC and BNG)	Scenario 1 (separated AC and BNG)	Scenario 2 (integrated AC and BNG)
R-59	x	x		x		

R-60	x	x		x		x
R-61	x	x	x	x		
R-62				x		
R-63				x		
R-64						x
R-65						x
R-66						x
R-67						x
R-68		x		x		x
R-69	x					
R-70		x		x		x
R-71	x					
R-72						x

[R-59] The AC MUST support an IEEE 802.1X Authenticator function.

[R-60] The AC MUST support a RADIUS client.

[R-61] The AC MUST support 4-way IEEE 802.11i handshake with the EUD.

[R-62] Before assigning an IP address to the EUD, the AC MUST confirm that the EUD has been successfully authenticated.

[R-63] Upon successful IP address allocation, the AC MUST send an Accounting Start Message to the AAA.

[R-64] The AC MUST assign an IP address to an EUD using DHCP regardless of whether the EUD has been authenticated. **M**

[R-65] The AC MUST be able to redirect or policy route the HTTP traffic of unauthorized EUDs to the portal server for portal authentication. **M**

[R-66] The AC MUST block all traffic except communication to the portal server, the DNS and the DHCP server, when the EUD is unauthenticated. **M**

[R-67] The AC MUST send an Accounting Start Message for an EUD to the AAA when the EUD is authenticated successfully.

Note: In R-68 to R-71, the BSSID/SSID is stored in Called-Station-Id as defined in RFC 3580.

[R-68] 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. **M**

[R-69] The AC MUST be able to insert the BSSID and the SSID into RADIUS Called-Station-Id and report the information to the BNG during EUD authentication. **M**

[R-70] 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. **M**

[R-71] The AC MUST be able to update the BSSID and the SSID in RADIUS Called-Station-Id and report the information to the BNG when the EUD switches from one AP to another. **M**

[R-72] 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. **M**

8.4 Portal Server Requirements

[R-73] The portal server MUST support obtaining the user name and password on the portal page.

[R-74] The portal server MUST support displaying the authentication result on the portal page.

8.5 AAA Server Requirements

Table 4 - AAA requirements for different authentication scenarios

	IEEE 802.1X authentication				Portal authentication	
	Scenario 1 (separated AC and BNG, AC - authenticator, BNG - RADIUS proxy)	Scenario 2 (separated AC and BNG, AC - authenticator, BNG - not RADIUS proxy)	Scenario 3 (separated AC and BNG, BNG - authenticator)	Scenario 4 (integrated AC and BNG)	Scenario 1 (separated AC and BNG)	Scenario 2 (integrated AC and BNG)
R-75	x	x	x	x		
R-76	x	x	x	x	x	x
R-77		x				
R-78					x	x

[R-75] The AAA server MUST support IEEE 802.1X Authentication.

[R-76] 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-77] 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-78] The AAA server MUST be able to allow an authenticated subscriber to bypass portal re-authentication.

End of Broadband Forum Technical Report TR-321