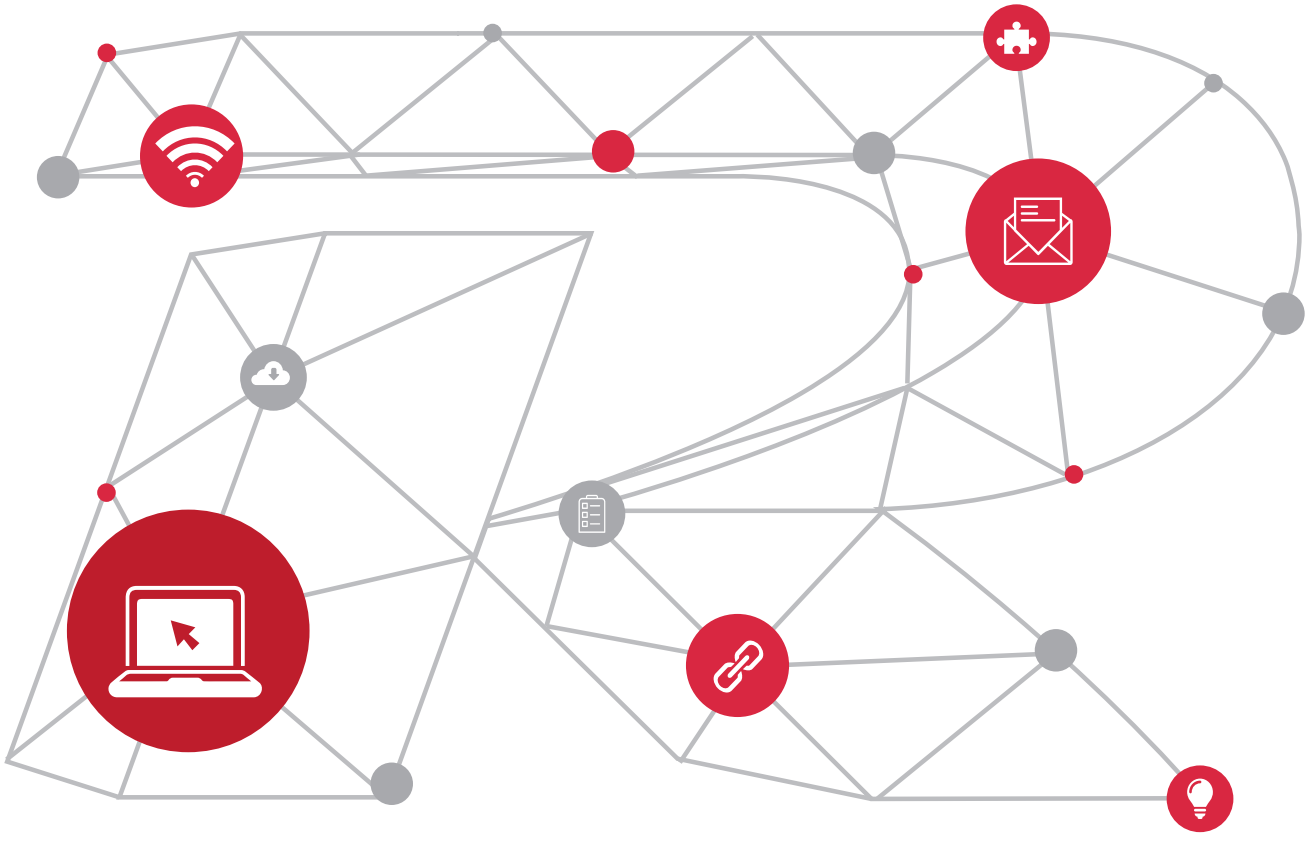
Ruijie WLAN Roaming

White Paper



Contents

Introduction

This document describes Layer-2 and Layer-3 user roaming implemented in the fit Access Point (AP) architecture, analyzes features of the Ruijie solution, and provides a comparison with existing technical standards and technical solutions of other vendors.

• Basic Concepts

Terminology	Description
Roaming	When a STA moves to the border of the coverage areas of two basic service sets (BSSs), the STA associates with a new AP and disassociates from the original AP.
Layer-2 roaming	A wireless STA roams within one VLAN subnet and its IP address keeps unchanged.
Layer-3 roaming	A wireless STA roams between different VLAN subnets and its IP address keeps unchanged.
Fast roaming	After a wireless STA associates with an access controller (AC) for the first time, a fast handover can be implemented upon roaming, so that voice and video communication of the user are little affected (with the roaming connection setup time shorter than 50 ms).
Visitor	Access requirements of some users should be met with certain restrictions. Such users are called wireless visitors. In a campus network (for example, intranet of an enterprise), partners or visitors may access the Internet or other extranets by using wireless network resources of the campus network.
HA	Short for home agent. When a wireless STA associates with an AC in a mobility group, the AC becomes the HA of the wireless STA.
FA	Short for foreign agent. An AC that is not the HA of a wireless STA and to which the wireless STA is connecting is referred to as an FA.
HAC	Short for home AC, that is, the AC with which a STA associates for the first time.
HAP	Short for home AP, that is, the AP with which a STA associates for the first time.
FAC	Short for foreign AC, that is, currently associated AC after STA roaming.

Terminology	Description
FAP	Short for foreign AP, that is, currently associated AP after STA roaming.
MTI tunnel	Extension tunnel compliant with the Control and Provisioning of Wireless Access Points (CAPWAP) protocol, which is used to transmit roaming control packets and data packets between an FAC and an HAC or between an FAP and an HAP.
Fast roaming STA	A wireless STA that associates with a mobility group and supports the fast roaming service (RSN+802.1x).
Roam-out STA	When a roaming wireless STA is connecting to an AC other than the HA in a mobility group, the wireless STA is a roam-out STA to the HA.
Roam-in STA	When a roaming wireless STA is connecting to an AC (FA) other than the HA in a mobility group, the wireless STA is a roam-in STA to the FA.
Intra-AC roaming	Intra-AC roaming occurs when a wireless STA roams from an AP of an AC to another AP of the same AC.
Inter-AC roaming	Inter-AC roaming occurs when a wireless STA roams from an AP of an AC to another AP of a different AC.

• Background

A wireless local area network (WLAN) is a local area network (LAN) that uses radio waves rather than conducting wires or cables as the data transmission media. The transmission distance is generally only dozens of meters. The trunk paths of WLANs usually use wired cables. WLAN users access WLANs via one or more wireless APs. WLANs have been widely applied in business districts, universities, airports, and other public areas. The most universal WLAN standards are the IEEE 802.11 series standards.

With the widespread application of wireless networks, users raise increasingly high requirements for mobility in accessing networks. The coverage area of an AP is limited. The communication quality deteriorates as a STA moves farther from an AP. For this, the roaming function is developed to expand the moving scope of a STA. The roaming function ensures that the IP address keeps unchanged and data services are not interrupted when a STA moves from the signal coverage area of one AP to that of another. One key feature of the roaming function is to ensure that user services are not interrupted. If a STA goes offline from AP 1 with services interrupted, and then goes online on AP 2 and obtains an IP address, this is not roaming. User services are not interrupted at the macro level. In actual situations, a few packets are lost during roaming due to multiple factors, for example, the signal strength is weak or signal hollow holes exist in overlapped coverage areas of two APs, a new AP is found by scanning upon channel switching in STA roaming, a STA needs to be disassociated from an original AP and associated with a new AP, or key re-negotiation or even re-authentication is required after a STA is associated with a new AP. An important objective of roaming is to reduce packet loss during roaming and ensure that a delay and stuttering in upper-layer services cannot be perceived, and service experience is satisfactory during STA mobility.

Roaming is transparent and seamless for users, that is, users and their applications will not perceive the occurrence of roaming. For applications such as VoWLAN, the data communication interruption duration must be shorter than 50 ms (interval perceptible to human beings) during handovers. These requirements greatly challenge existing technologies. How to effectively implement seamless roaming for users who are using wireless networks (especially WLANs) is an issue to be urgently settled by device vendors.

• Implementation Status Quo

The IEEE has launched two fast roaming 802.11 standards: 802.11f (abolished) and 802.11r. The latter was published on May 9, 2008 and requires support from both clients and APs. Currently, no vendor has implemented this standard yet. In addition, the network-layer Mobile IP/IPv6 technology defined by the Internet Engineering Task Force (IETF) is conducive to the implementation of Fast BSS Transition (FBT) for roaming users. Further study is required to combine it with WLAN technologies to implement fast roaming.

Mainstream vendors (such as Cisco and H3C) use the Layer-2 roaming mode and the fit AP architecture described below, in combination with client information sharing inside a mobility group, to shorten the Extensible Authentication Protocol (EAP) authentication time during roaming, in an effort to achieve fast roaming.

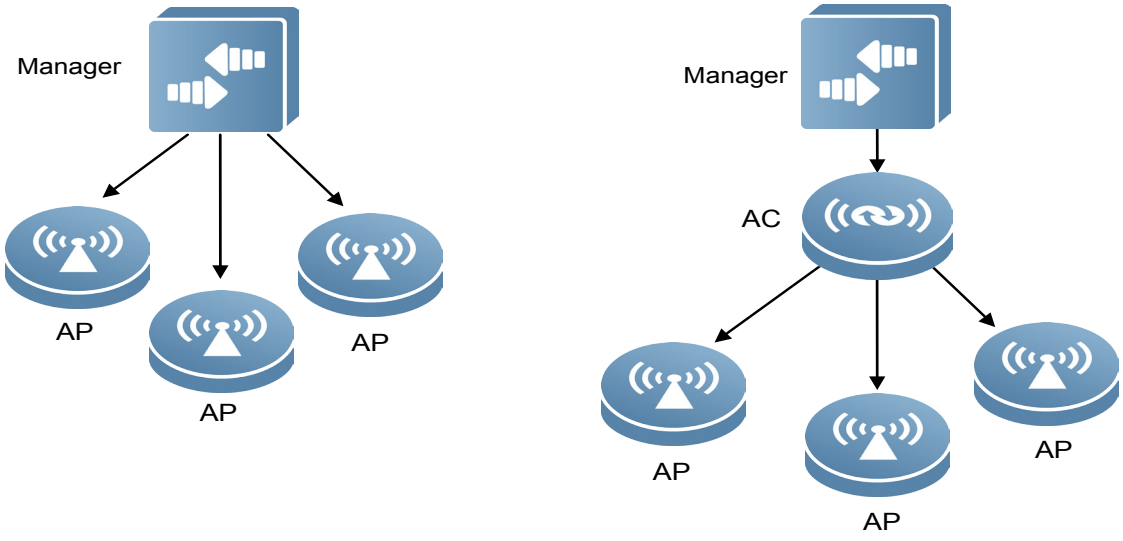
• Market Prospect

Users have increasingly high requirements for multimedia application. Implementing fast roaming for WLAN users gives strong support to the Ruijie overall WLAN solution and will significantly enhance the competitive edge of the Ruijie solution.

• WLAN Architecture

The WLAN access speed increases from the initial 1 Mbit/s to the current 54 Mbit/s since the IEEE802.11 standard was launched in 1997. The release of the IEEE802.11a/b/g/n standards dramatically drives WLAN expansion. WLANs not only serve as a supplement to wired networks but also evolve towards large-scale deployment and independent networking, and even replace wired networks in some places. The conventional WLAN architecture (fat AP architecture) can no longer meet large-scale networking requirements and vendors unveil their own solutions. In addition, the IETF also sets up a CAPWAP work group to study solutions to large-scale WLAN deployment. One centralized WLAN fit AP architecture (as shown in Figure 1) is proposed and adopted by vendors progressively.

Figure 1



• Roaming Standards

Network Roaming at Single Link Layer (802.11)

In WLAN roaming standards, the IEEE proposes IEEE 802.11f, that is, the Inter-Access Point Protocol (IAPP), to support the STA mobility. This protocol defines information relevant to the communication, exchange, and handover between APs, for STAs to roam between multiple APs in the same subnet. The 802.11f standard defines a system composed of a STA, multiple APs, a Distribution Service (DS), an AC, and a Remote Authentication Dial In User Service (RADIUS) server, to implement the STA handover between APs in the same extended service set (ESS). When a handover is necessary for a STA due to wireless link factors, the STA must complete re-authentication and re-association with a new AP before communicating with the new AP. IAPP is an upper-layer protocol above the IP layer. To secure communication between APs, IAPP-compliant APs should register with the RADIUS server so that secure communication connections are set up between APs. Information exchanged between APs and the RADIUS server include the mapping from BSS IDs to IP addresses of APs. The RADIUS server sends keys to the APs to secure the communication between APs. When a STA needs a handover, it needs to send an association/re-association message to a new AP, which should exchange information with the RADIUS server to implement the mapping from the BSS ID to the IP address of the new AP. Then, the RADIUS server sends a key to the AP. The AP needs to exchange messages with the RADIUS server for each STA handover, resulting in a long handover delay. For this, the 802.11 committee found the TGr group to study the FBT, with the aim of developing the FBT technology that supports delay-sensitive services. IEEE 802.11f was abolished on February 3, 2006.

The TGr group proposed the finalized 802.11r standard in 2005. This standard was formally approved in the summer in 2008. In comparison with 802.11f, 802.11r does not restrict APs to be in the same subnet, but proposes new authentication protocols, new key management protocols, and faster PTK algorithms, and resource reservation prior to association/re-association, to minimize the verification and handover time, thereby achieving seamless connections between hot spots. The core of 802.11r is to utilize the currently associated AP to send FBT requests to a new target AP directly or in wireless mode before a STA re-associates with the new target AP, and to optimize the key distribution procedure and reduce the required time, in an effort to reduce the interruption duration caused by the roaming handover. The main mechanisms are as follows:

1. Handover capability definition, used to achieve resource configuration before or during re-association between a STA and an AP.
2. Resource reservation mechanism: Various resources including Quality of Service (QoS) and relevant security parameters are used to achieve the communication with the target AP via a wireless network or via the current AP and DS prior to association.
3. New key management framework, used to establish the unique pairwise master key security association (PMKSA) between a STA and an AP.
4. New roaming protocol, used to calculate a pairwise transient key (PTK) during or before re-association.

802.11r has just been approved (formally approved on May 9, 2008). No 802.11r-complaint client and network device are available in the market yet until this document is written. Data shows that the latest Windows 7 will support 802.11r. In addition, 802.11r is based on the fat AP architecture. How to implement 802.11r in the fit AP architecture (RFC 4118) needs to be further analyzed and studied.

Network Roaming Across Link Layers (Wired, 802.11 Wireless, and Cellular Networks)

Global mobile devices are predicted to increase at an annual rate of about 50%. The quantity of mobile devices will reach about 80 million in 2011 (and will be larger if 3G mobile terminals are included). With the coming of the all-IP era, the IP technology plays an increasingly important role in supporting mobility. In addition to roaming standards for 802.11 WLANs, Mobile IPv4/IPv6 is dedicated to implementing roaming from a higher layer. Mobile IPv4/IPv6 supports device mobility on the IP-based Internet, without considering that the link layer is in a wired network, wireless network, or cellular network.

Mobile IPv4

The core protocol of Mobile IPv4 is RFC 3344, which defines how to enable a node to keep its fixed home address while moving on the Internet. IETF has launched 24 Mobile IPv4-relevant RFC standards, with the core of RFC 3344. A large number of drafts are under research and the content involves tunnel encapsulation, security, Authentication, Authorization and Accounting (AAA), network management, network address translation (NAT), and applicability. The standardization of Mobile IPv4 has basically ended except some "minor" issues concerning deployment, such as protocol optimization and extension, safety protection, AAA, and enterprise network.

The applicability and specific problems of Mobile IP in the wireless environment are another hot issue to be studied. The current study focuses on inter-domain routing, network access flag extension, private IPv4 addresses, positioning and privacy, and service quality.

The basic idea of the Mobile IP protocol is to separate the IP address flag from the addressing function, and use two IP addresses for identification. The IP address that identifies a mobile host is the local agent address and the IP address that identifies the current position of the host is the care of address (CoA).

The following communication entities are often involved in the Mobile IP protocol: mobile node (MN), home network (HN), foreign network (FN), home agent (HA), foreign agent (FA), and CoA. The most basic principle is as follows: An MN registers with the HA, and a data channel set up between the HA and an FA routes data packets. A CoA is a temporary IP address obtained when an MN roams to an FN. It provides a channel for the communication between the MN and the HN and is the destination of the channel. Therefore, obtaining a correct CoA is a key step. There are two modes for obtaining a CoA: One is that an MN uses the IP address of an FA as the CoA for registration. The FA is the destination of the channel and is responsible for receiving and decapsulating data packets, and sending the packets to the MN. This address mode enables multiple MNs to share one CoA, delivering high efficiency. The other is to assign a temporary IP address to an MN. The IP address is temporarily obtained from an FN via external protocols (such as DHCP). The MN is the destination of the channel. It independently performs decapsulation to retrieve required packets. In this mode, one CoA can be used only by one MN, delivering low efficiency. CoA is the core of data packet routing. It is a dynamic address, that is, the CoA changes as an MN moves from one subnet to another.

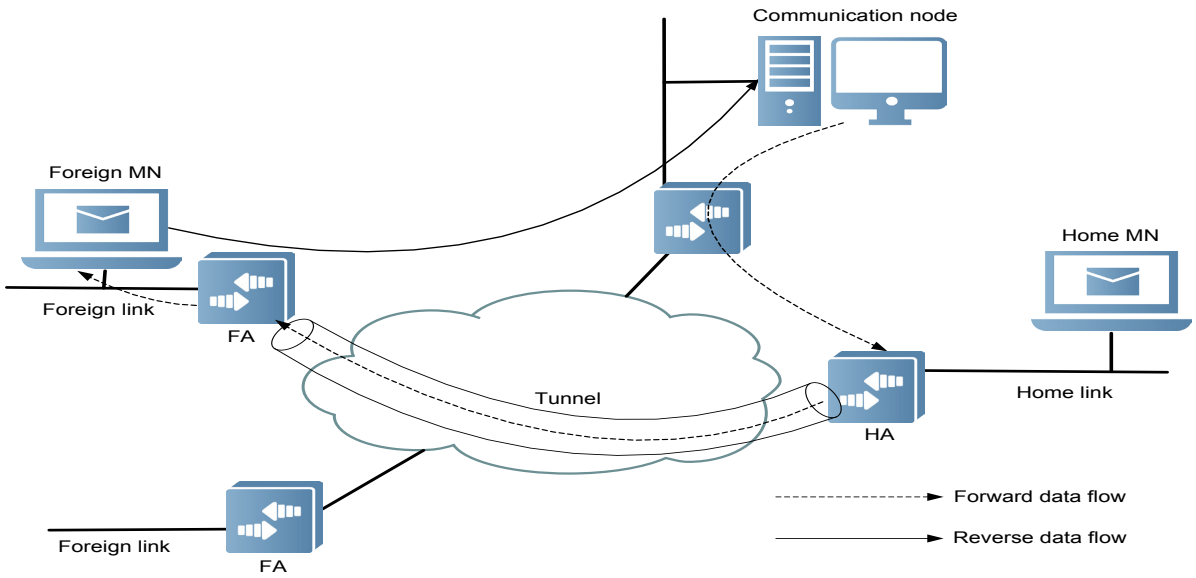
When an MN accesses a network, it must find out a mobile agent to obtain the latest CoA. There are two methods for discovering an agent: One is passive discovery, that is, an MN waits for a mobile agent to periodically broadcast agent advertisement packets. The other is active discovery, that is, an MN broadcasts an agent request packet. Both methods allow an MN to identify an agent and obtain a CoA. The second method can be used only when an MN does not receive agent advertisement packets and fails to obtain a CoA.

After obtaining a CoA, an MN must register the current CoA with the HA so that the HA accurately forwards data packets. The registration procedure varies with a network. One is that a CoA is registered via an FA: An MN sends a registration request to the FA, which processes the request and forwards it to the HA. The HA processes the registration request and sends a registration response to the FA. The FA processes the response and forwards it to the MN. The other is that an MN directly sends a registration request to an HA and the HA sends a registration response to the MN after processing.

The work process (as shown in Figure 2) of Mobile IPv4 is described as follows:

1. The HA and FA send agent advertisement messages on the network continuously to advertise their existence.
2. After receiving these messages, the MN checks that it is in the HN or FN.
3. If the MN finds that it is still in the HN, it indicates that the message is from the HA and the MN does not enable the mobility function. If the MN just returned from the FN, it sends a registration cancellation message to the HA to advertise that it returns to the HN.
4. If the MN finds that it has moved to the FN, it obtains a CoA.
5. The MN registers with the HA to indicate that the MN has left the HN, and advertises the obtained CoA to the HA.
6. After registration, all data packets destined for the MN are intercepted by the HA, which encapsulates the data packets and sends them to the FA (first CoA obtaining mode) or the MN (second CoA obtaining mode) through tunnels. If the HA sends the data packets to the FA, the FA forwards the data packets to the MN. Data packets are transmitted successfully between different subnets.
7. When the MN sends data to a common IP host, it uses the normal IP addressing method without using the HA.

Figure 2



Mobile IPv6

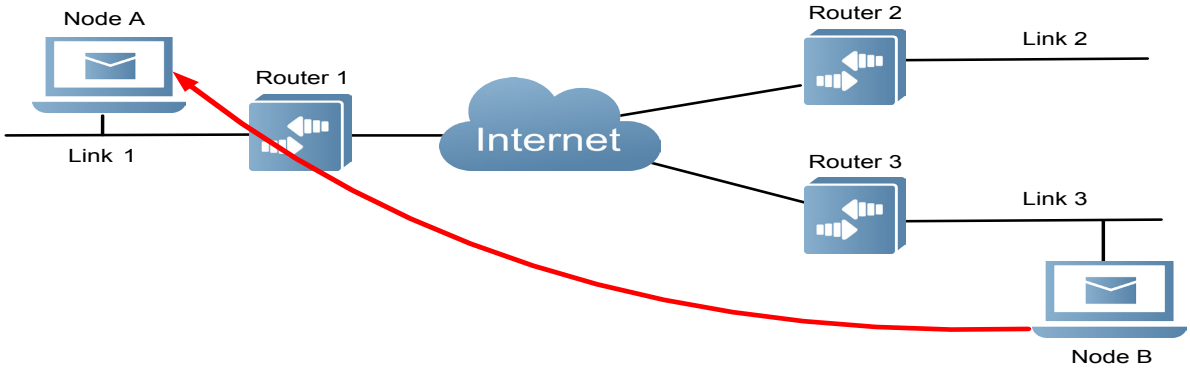
The core mobility standard is RFC3775 in IPv6 environment. In the Mobile IPv6 design, RFC3775 utilizes the IPv6 neighbor discovery and stateless automatic configuration features, with no need of FAs. It eliminates triangular routing and source address filtering in Mobile IPv4 and enhances the security. With RFC 3775 as the center, some other Mobile IPv6 informative or amendment RFC standards are further released, improving aspects such as the applicability, FBT, network AP flag, network management, security protocol (IKEv2), AAA, deployment scenarios, and Boottrap for large-scale deployment.

The optimized IPv6 design simplifies the work process of Mobile IPv6 (as shown in Figure 3).

Note

The data forwarding route is asymmetric in Mobile IPv4 roaming and a triangle is formed. As a result, roaming is not supported in the presence of some security policies (such as uPRF). Mobile IPv6 properly prevents asymmetric routes and eliminates the problems above.

Figure 3



1. Routers periodically broadcast router advertisement messages that contain the prefixes of local links. After receiving such a message, Node A learns that it has moved and obtains a new address A2 based on the new prefix via the automatic address configuration function.

2. Node A sends a message M2 to Router 1. M2 is used to notify Router 1 of the new address A2 of Node A. Subsequently, Router 1 intercepts a data packet destined for the original address A1 of Node A, uses this packet as the payload, adds an IPV6 header to it, and sends the new packet to the new address A2 of Node A. The tunneling technology is applied in this process.

3. If Node B sends a data packet to Node A but does not know that Node A has moved, Node B still sends data packets to the original address A1 of Node A.

4. When the data packet from Node B reaches Router 1, Router 1 intercepts the data packet and forwards it to the new address A2 of Node A.

5. After receiving the data packet forwarded from Router 1, Node A checks the source address of the data packet and learns that Node B wants to communicate with Node A. Then, Node A sends a data packet M3 to Node B to notify Node B of the new address A2 of Node A.

6. After receiving the data packet, Node B records the new address A2 of Node A. If Node B has other data packets to be sent to Node A, it directly sends them to the address A2 of Node A. At this point, two-way communication is implemented between Node A and Node B.

7. The establishment process of communication between other nodes and Node A is similar to the process described above.

Compared with Mobile IPv4, Mobile IPv6 has the following advantages:

* **a) With the IPv6 neighbor discovery and stateless automatic configuration features, FAs are not required.**

* **b) There are two CoAs in Mobile IPv4: configured CoA and agent CoA, which are not required in Mobile IPv6.**

* **c) Triangular routing existing in Mobile IPv4 is eliminated.**

The application of Mobile IP in WLAN roaming relies on clients. The Ruijie technical solution described below optimizes roaming in 802.11 wireless networks and does not rely on clients.

Technical Features of Ruijie WLAN Roaming Solution

• Basic Concepts

Intra-AC Roaming and Inter-AC Roaming

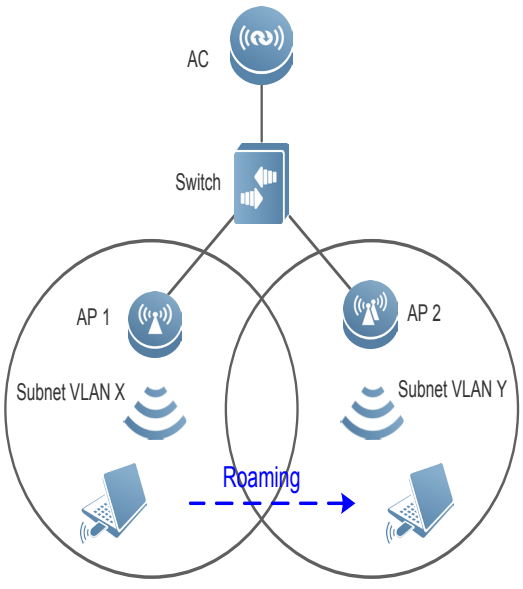
Intra-AC roaming

As shown in Figure 4, AP 1 and AP 2 are managed by the same AC. The STA goes online on AP 1 first, and re-associates with AP 2 for go-online on AP 2 during movement. The IP address of the STA keeps unchanged and services are not interrupted in this process. This is called intra-AC roaming.

AP 1 is the HAP of the STA and AP 2 is the FAP of the STA.

In special scenarios, AP 1 is AP 2 and inter-radio roaming occurs when the STA roams from Radio-1 to Radio-2 of the same AP. In actual environments, dual-band STAs that support both 2.4 GHz and 5.8 GHz bands may experience inter-radio roaming when they register with APs that support dual bands.

Figure 4



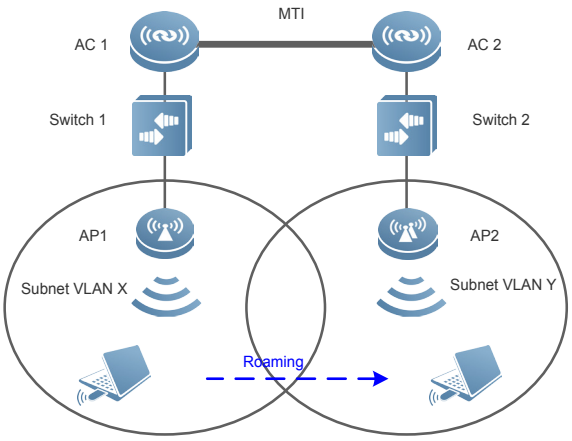
Inter-AC roaming

As shown in Figure 5, AP 1 and AP 2 are managed by AC 1 and AC 2 respectively. The STA goes online on AP 1 first, and re-associates with AP 2 for go-online on AP 2 during movement. The IP address of the STA keeps unchanged and services are not interrupted in this process. This is called inter-AC roaming.

AC 1 is the HAC of the STA and AC 2 is the FAC of the STA; AP 1 is the HAP of the STA and AP 2 is the FAP of the STA.

AC 1 exchanges STA roaming data with AC 2 through the MTI tunnel.

Figure 5



Intra-AC roaming can be considered as a special case of inter-AC roaming, in which the HAC is the FAC.

In some large WLAN networks, the data amount of APs is often very large. Not all APs can be managed by one AC, and therefore multiple ACs are needed to manage these APs. Inter-AC roaming must be supported to allow users to roam freely between different APs, thereby adapting to the scenario in which APs associated with a STA before and after roaming are not managed by the same AC.

Ruijie ACs support intra-AC roaming and inter-AC roaming by default. A mobility group or mobility list needs to be configured on ACs to support inter-AC roaming. For details, see 3.1.3 "Mobility Group and Mobility List."

Layer-2 Roaming and Layer-3 Roaming

Subnet services of APs are classified diversely in actual network planning of organizations. Roaming is classified into Layer-2 roaming and Layer-3 roaming based on subnets of services before and after roaming. In Figure 4 and Figure 5, if the subnet VLANs of services are the same before and after roaming, the roaming is Layer-2 roaming. If the subnet VLANs of services are different before and after roaming, the roaming is Layer-3 roaming.

Ruijie ACs and APs support Layer-2 roaming and Layer-3 roaming by default.

Mobility Group and Mobility List

Mobility group

The roaming scope of wireless users cannot be infinitely large in a WLAN. ACs in the moving scope of a STA can be added to a mobility group, in order to allow the STA to roam between APs served by the ACs and control and manage the roaming scope of STAs.

* **Working principle**

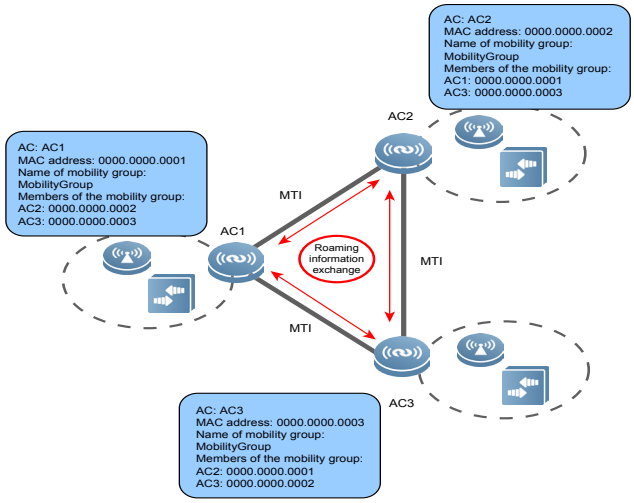
Each AC in a mobility group stores a list of other members in the mobility group (as shown in Figure 6). When a STA gains access to an AC, the AC sends an advertisement message to other ACs in the mobility group. If the STA associates with the mobility group for the first time, the initially associated AC (roam-out AC/HA) stores the STA information. When the STA roams to the coverage area of another AC, the initial AC synchronizes the STA information to the corresponding AC (roam-in AC/FA). If the STA is a roaming STA, the initially associated AC (roam-out AC/HA) synchronizes the STA information to the current AC (roam-in AC/FA) after receiving an advertisement message.

In general, information about a roaming STA is exchanged only when roaming occurs. The active information synchronization function can be used to enable ACs in a mobility group to share STA information before STA roaming occurs. In this way, the roaming re-association duration can be shortened and the roaming efficiency can be improved.

* **Mobility group topology**

The inter-AC communication establishment uses specific technologies, which shortens the required time of re-authentication with the RADIUS server after STAs roam across ACs, accelerates information authentication of roaming wireless STAs, and lays a foundation for fast seamless roaming. Figure 6 shows the work topology.

Figure 6



Mobility list

A mobility list is a supplement to a mobility group. The number of ACs in a mobility group is limited. The mobility list mechanism is introduced to extend the roaming scope of users, without affecting the roaming of normal mobility groups.

* **Difference between mobility list and mobility group**

Data exchanges of roaming STAs in the mobility list is similar to that in the mobility group. The major differences lie in that: A fast and secure roaming mechanism (PKC) is used for roaming between ACs in the mobility group; when a STA roams across mobility groups in a mobility list, the roaming STA needs to perform a complete authentication process with the AAA/RADIUS server. Therefore, in comparison with intra-group roaming, inter-group roaming is low in efficiency. The two mechanisms are common in that the roaming process is seamless and is transparent to users.

A mobility group to which an AC belongs can be specified and STAs that gain access to this AC can roam in the coverage area of the mobility group. A mobility list can further be configured on an AC, on which a mobility group is configured, and ACs in the mobility list cannot be in the same mobility group as the current AC. In this way, STAs that gain access to the current AC can roam across mobility groups.

Auto-Anchor Mobility

In the auto-anchor mobility mechanism, all STAs in a WLAN are regarded as roaming STAs, an AC is specified as an anchor AC statistically, and user data is transmitted to the anchor AC for storage through tunnels. In this way, user information is managed in a centralized manner and security policies can be implemented in a unified manner.

Working principle

The auto-anchor mobility mechanism collects user information on all ACs in a roaming group together onto the anchor AC for centralized management. All STAs associated with a common AC are regarded as roaming STAs. In comparison with the mobility group mechanism, the anchor AC serves as a roam-out AC and a common AC serves as a roam-in AC in the auto-anchor mobility mechanism. Therefore, STAs communicate with each other through the anchor AC.

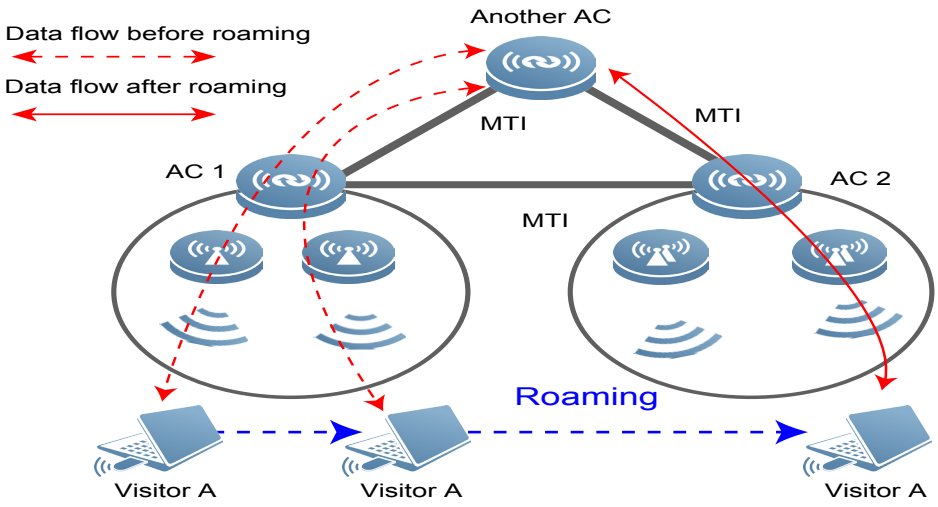
General application scenario

In a campus network (for example, intranet of an enterprise), partners or visitors may access the Internet or other extranets as wireless STA users by using wireless network resources of the campus network. The partners or visitors should be capable of moving in the campus with network service available. For this, the auto-anchor mobility mechanism based on the roaming technology is provided to meet visitor access requirements with certain restrictions.

Topology of auto-anchor mobility

In the auto-anchor mobility mechanism, ACs exchange user information with each other through tunnels established as per the mobility group or mobility list. When a user in a WLAN accesses an AC in a mobility group, if an anchor AC is configured on the WLAN, the AC sends user data to the anchor AC for processing. Figure 7 shows the work topology.

Figure 7



• Technical Principle

Roaming Judgment and Go-online Process

Roaming judgment

When an AC receives a re-association request from a STA, it judges whether roaming occurs and performs go-online processing in either of the following cases:

* **The STA entry exists in the current AC and the SSID in current association information is the same as that in re-association information.**

* **The current AC does not have the STA entry, the STA entry exists in an AC of the mobility group or mobility list, and the SSID in the entry information is the same as that in re-association information.**

Specifically, in order to prevent multi-authentication of Web authenticated users and improve user experience, an AC also performs a roaming judgment as described above and performs go-online processing when it receives an association request from a Web authenticated user.

In addition, STA go-online is considered as initial go-online and non-roaming processing.

Roaming and go-online process

When an AC receives an association/re-association request from a STA, the AC performs the following processing:

* **STA go-online: If the associated WLAN is a visitor WLAN, the AC brings the STA online.**

* **Initial go-online: non-roaming processing. If the STA online entry is not found in the current AC and other ACs in the mobility group and mobility list, or if roaming is not supported because the SSID and WLAN information in re-association information are different from those in the STA online entry, the AC performs initial go-online processing. If the STA entry exists, the AC forces the STA to go offline normally and then brings it online.**

* **Intra-AC roaming: If the AC finds the STA online entry and the STA is in the roaming state, it forces the STA to go offline due to roaming and then brings the roaming STA online normally.**

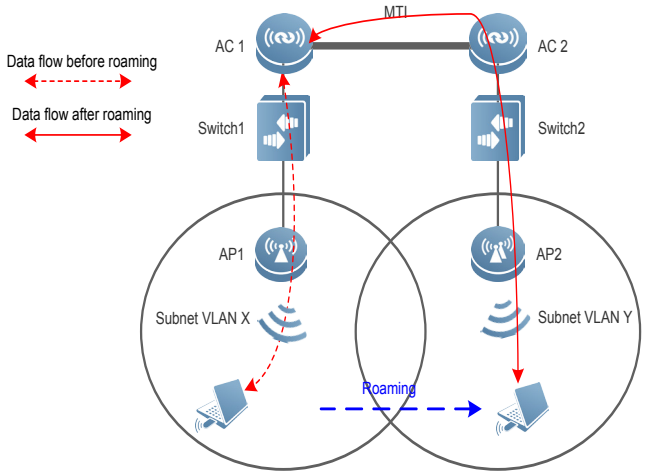
* **Inter-AC roaming: If the AC fails to find the STA online entry, it sends a roam-in request message of the STA to all ACs in the mobility group or mobility list through MTI tunnels. This message carries the re-association information of the STA, including the AP to be associated, radio, WLAN, VLAN, and SSID. After receiving the message, the HAC searches for the local STA online entry, updates the Foreign information in the STA entry, and sends the Home information of the STA to the FAC via a roam-in response message. After receiving the response message, the FAC updates the local database and completes the inter-AC roaming processing. The FAC uses a timeout mechanism for roam-in response messages. The default timeout time is 50 ms. If the FAC fails to receive a roam-in response message within 50 ms, it brings the STA online normally.**

Traffic Forwarding

Centralized forwarding

In centralized forwarding mode, the HAC is reachable to the user gateway. The traffic of roaming STAs is forwarded to the HAC, which sends out the traffic. As shown in Figure 8, the STA undergoes inter-AC (Layer-2/Layer-3) roaming. AC 1 and AC 2 serve as the HAC and FAC of the STA respectively. The IP address of the STA keeps unchanged after roaming. To ensure that the STA can still access the original subnet after Layer-3 roaming, the STA traffic needs to be forwarded to the HAC, that is, AC 1, through the MTI tunnel between ACs, so that the HAC sends out the traffic. Likewise, packets sent from the network side to the STA are first sent to the HAC, which forwards the packets to the FAC through the MTI tunnel. The FAC sends the packets to the FAP through the CAPWAP tunnel and the FAP forwards the packets to the roaming STA.

Figure 8



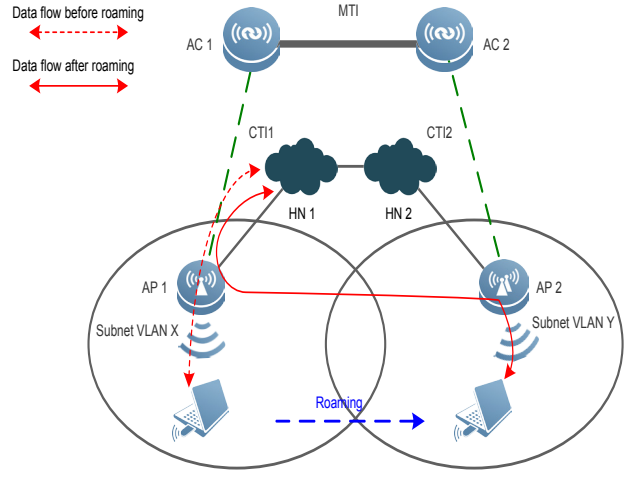
In intra-AC roaming, packet forwarding is similar to that in inter-AC roaming, and the differences are that the HAC is the FAC and the MTI tunnel between the HAC and the FAC does not exist.

Local forwarding

In local forwarding mode, the HAP is reachable to the user network. The traffic of roaming STAs must be forwarded back to the HAP, which sends out the traffic. As shown in Figure 9, the STA undergoes inter-AC Layer-2/Layer-3 roaming, and AP 1 and AP 2 serve as the HAP and FAP of the STA respectively. To ensure that the STA can still access the original network after roaming, the STA traffic must be forwarded to the HAP, which sends out the STA traffic. Likewise, packets sent from the network side to the STA are first sent to the HAP, which forwards the packets to the FAP through the MTI tunnel between the HAP and the FAP.

In intra-AC roaming, packet forwarding is similar to that in inter-AC roaming, and the differences are that the HAC is the FAC and the MTI tunnel between the HAC and the FAC does not exist.

Figure 9



Customer Benefits

Compared with conventional wired networks, the greatest advantages of WLANs lie in that STAs are free from the impact of locations of physical media, and the STAs can move freely in the WLAN coverage area, without affecting services during movement. Multiple APs are often needed in an ESS to cover a larger area. Therefore, STAs inevitably move from the coverage area of one AP to that of another, and the STA needs to be handed over from the original AP to the new AP, to obtain services from the new AP. The WLAN roaming technology ensures that services are not interrupted during handovers, minimizes packet losses, and guarantees stable and smooth service experience during STA movement.

WLAN roaming meets the following requirements:

* **Ensures unchanged IP addresses after STA roaming.**

Application-layer protocols use IP addresses and TCP/UDP to bear user services. The original IP addresses of roaming STAs must be unchanged so that the TCP/UDP connection can be uninterrupted and application-layer data can be forwarded normally.

* **Ensures that STAs can still access the home network (network accessed when the STAs go online initially) after roaming, and the services available to STAs keep unchanged. The STAs can access the home networks no matter where they roam to, and roaming is not perceived at the service layer.**

* **Prevents data packet losses during roaming and ensures user experience.**

The WLAN roaming technology ensures that users can move freely in the coverage area of WLAN signals, without interrupting services or affecting user experience during movement.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**