Content

Chapter 1 Centralized Forwarding

1.1 Overview of Centralized Forwarding

1.1.1 Introduction to Centralized Forwarding

In real network environment, many enterprises or operator customers need to monitor all flow in network to guarantee the security; the centralized forwarding can make all flow centralize to AC (wireless controller) to achieve the centralized control of flow instead of local forwarding to every AP to deal with flow, the latter cannot monitor the flow in network.

Besides, many wireless users have the demand of roaming (roaming from one AP to another AP), and many applications request that IP address is not changed after roaming, such as IP phones. For the situation of the layer 3 roaming, our centralized forwarding can be supported. And it is hardware forwarding which can satisfy the flow demand.

Centralized forwarding uses CAPWAP tunnel protocol (centralized tunnel) to package user data. The outer layer of CAPWAP packets uses UDP protocol; it makes wireless data can be transmitted between AC and AP by passing through IP network. Then the wireless network deployment is very flexible. Deploying wireless network based on existing IP network is in particular, wireless deployment can be conducted at the case of keeping original network not changing.

1.1.2 Centralized Tunnel Creating

After AP and AC are associated, a centralized tunnel will be created between them (this tunnel use the IPv4 address to create first. If IPv4 routing is not passed, IPv6 address can be used). The addresses of the start point and end point are the IP addresses of AC and AP respectively. But the data is still through VLAN to conduct local forwarding. Only after enabling centralized forwarding of a VLAN (add this VLAN to the VLAN table of the tunnel forwarding), the packets of this VLAN can be forwarded through the centralized tunnel.

Through binding the QoS Policy to the vlan which is enabled the centralized forwarding, can conduct the QoS controlling to the user data packets.

1.1.3 Deleting of Centralized Tunnel

When AP and AC are disassociated, TLS security connection will be disassociated. Then the centralized tunnel deleting will be triggered. When TLS is connected to timeout on AP, TLS security connection will be disassociated. Then the centralized tunnel deleting

will be triggered.

1.2 Centralized Forwarding Configuration

1. Add VLAN into tunnel VLAN list

Command	Explanation
Wireless Global Mode	
l2tunnel vlan-list <*1-4094*> **no l2tunnel vlan-list <*1-4094*>**	Add a VLAN to tunnel VLAN list, all user packets which belong to this VLAN are forwarded through centralized tunnel. The no command deletes a VLAN from tunnel VLAN list.

2. Clear statistic information of port

Command	Explanation
Admin Mode	
clear counter [interface wlan <*ifname*>]	Clear statistic information of the appointed tunnel port. If the port is not appointed, clear statistic information of all ports.

3. Enable/disable error debug information of centralized forwarding

Command	Explanation
Admin Mode	
debug wireless cl2tunnel error <*FF-FF-FF-FF-FF-FF*> **no debug wireless cl2tunnel error <*FF-FF-FF-FF-FF-FF*>**	Enable debug of error information of centralized forwarding. The parameter of FF-FF-FF-FF-FF-FF if the MAC address of AP opposite to tunnel. No command disables the debug.

4. Enable/disable internal debug information of centralized forwarding

Command	Explanation
Admin Mode	
debug wireless cl2tunnel internal-info <*FF-FF-FF-FF-FF-FF*> **no debug wireless cl2tunnel internal-info <*FF-FF-FF-FF-FF-FF*>**	Enable the debug information of internal configuration, tunnel creating and deleting of centralized forwarding. The parameter of FF-FF-FF-FF-FF-FF if the MAC address of AP opposite to tunnel. No command disables the debug.

1.3 IPv4 Centralized Forwarding Configuration Examples
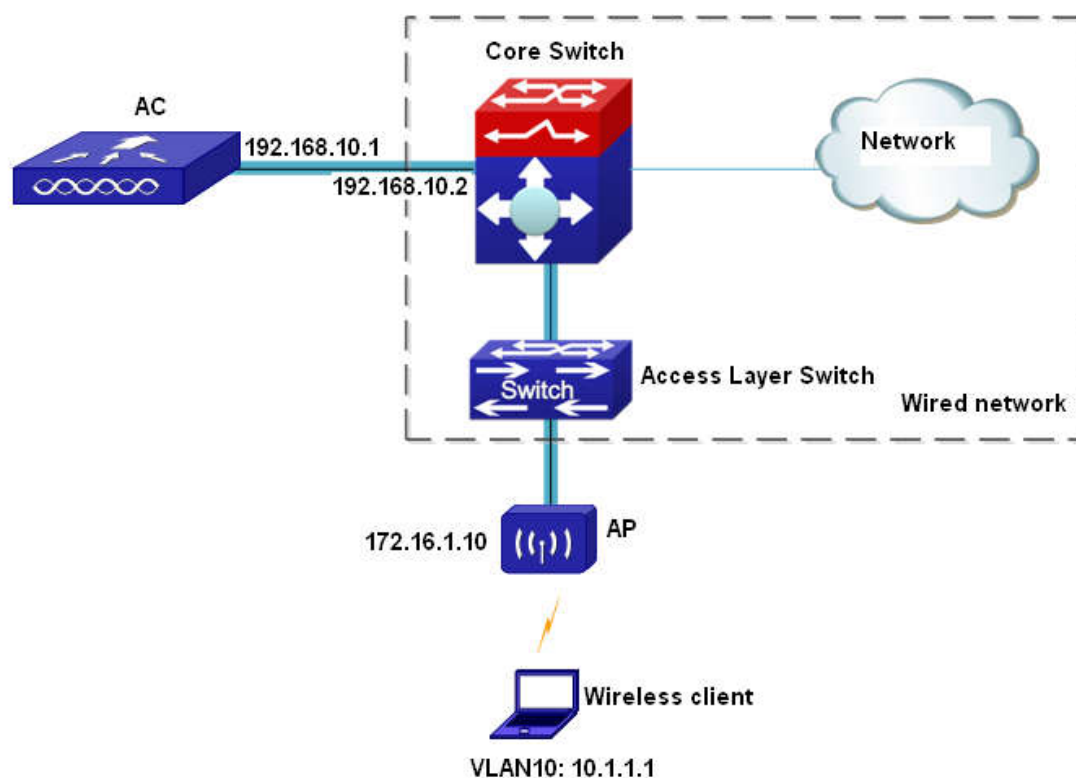
Case Topology:

Fig 1-1 IPv4 Centralized Forwarding Configuration Topology

Introduction to Case:

As shown in Fig 1-1, AC connects to the core switch of wired network through the method of bypath, AP connects to the access layer switch. Wireless client belongs to VLAN10 and adopts centralized forwarding. The default router should be added on AC, the next hop is the interface address of the core switch as 192.168.10.2.

Configuration Process:

AC configuration:

AC(config)#vlan 10

AC(config-vlan10)#exit

AC(config) #interface vlan 10

AC(config -if-vlan10) #ip address 10.1.1.254 255.255.255.0

AC(config -if-vlan10) #exit

AC(config) #interface vlan 1

AC(config -if-vlan1) #ip address 192.168.10.1 255.255.255.0

AC(config) #ip route 0.0.0.0/0 192.168.10.2

AC(config) #wireless

AC(config-wireless)#enable

AC(config-wireless)#l2tunnel vlan-list 10

1.4 IPv6 Centralized Forwarding Configuration Examples
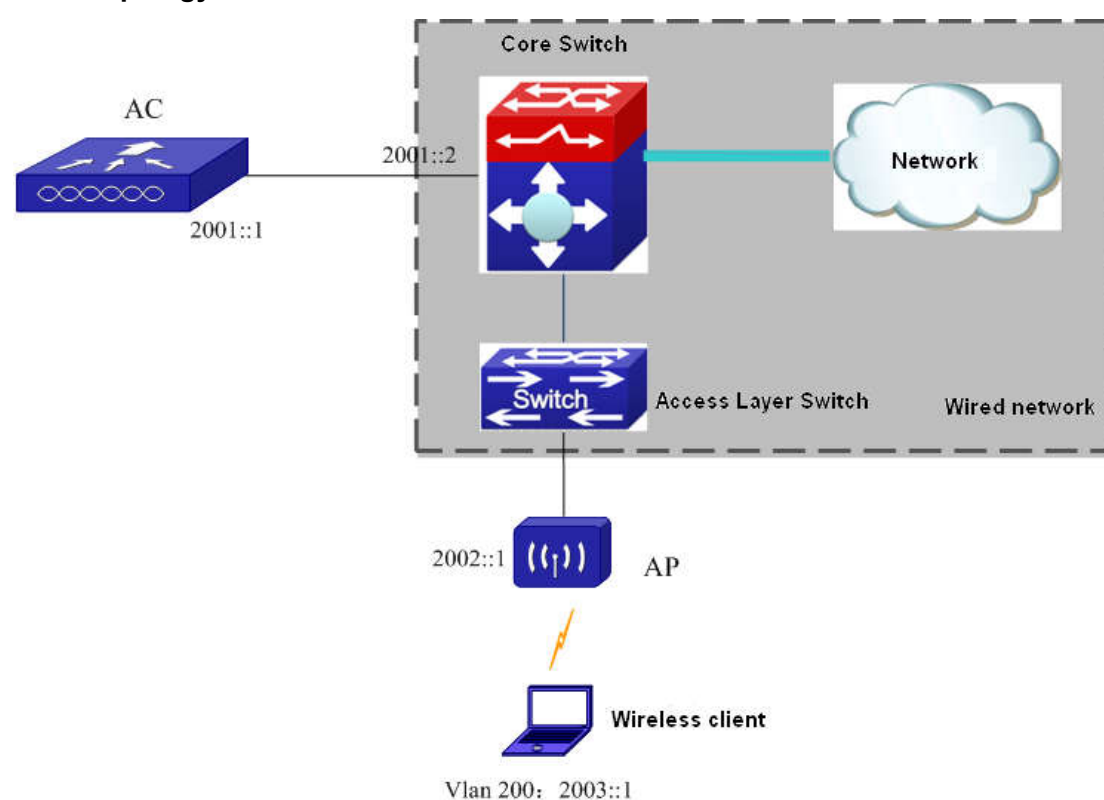
Case Topology:

Fig 1-2 IPv4 Centralized Forwarding Configuration Topology

Introduction to Case:

As shown in Fig 1-2, AC connects to the core switch of wired network through the method of bypath, AP connects to the access layer switch. Wireless client belongs to VLAN200 and adopts centralized forwarding. The default router should be added on AC, the next hop is the interface address of the core switch as 2001::2.

Configuration Process:

AC Configuration:

AC(config)#vlan 200

AC(config-vlan200)#exit

AC(config) #interface vlan 200

AC(config -if-vlan200) #ipv6 address 2003::FFFF/64

AC(config -if-vlan200) #exit

AC(config) #interface vlan 1

AC(config -if-vlan1) #ipv6 address 2001::1/64

AC(config) #ipv6 route ::/0 2001::2

AC(config) #wireless

AC(config-wireless)#enable

AC(config-wireless)#l2tunnel vlan-list 200

1.5 Centralized Forwarding Troubleshooting

When centralized forwarding does not transmit data correctly, please inspect the error with the following steps:

☞ Through **ping**, make sure the link between AC and AP is normal.

☞ Through **show wireless l2tunnel tunnel-list** command, check if the tunnel is created correctly.

☞ Through **show wireless l2tunnel vlan-list** command, check if the relevant data VLAN has been added into tunnel vlan-list.

☞ Through **show mac-address-table vlan** command, check if the MAC address of user is studied normally.

☞ Through **show arp** command, check if ARP table is normal.

Chapter 2   Distributed Forwarding

2.1 Introduction to Distributed Forwarding

Distributed forwarding is based on local forwarding, after the wireless client starts up layer3 roaming, the forwarding method is distributed forwarding. Data tags a tunnel (distributed tunnel) between two APs (one AP is before roaming and another one is after roaming), then the AP associated after roaming send data back to the AP associated before roaming. At last, the AP associated before roaming forwards data.

The principle of distributed forwarding: On the basis of ensuring VLAN forwarding normal, enable distributed forwarding on-off. The wireless user roams from an AP to another AP which does not belong to the same network segment (as shown in ① of Fig 2-1). For ensuring not to redistribute IP address for roaming user, AC will notify these two APs to create a distributed layer 2 tunnel (as shown in ② of Fig 2-1). Then the association AP after wireless user roaming (Assoc-AP) will send the data to the association AP (Home-AP) before client roaming through the distributed tunnel and Home-AP will forwards it. It can ensure that the IP address of wireless user will not change when there happens layer 3 roaming and the flow will not suspend.
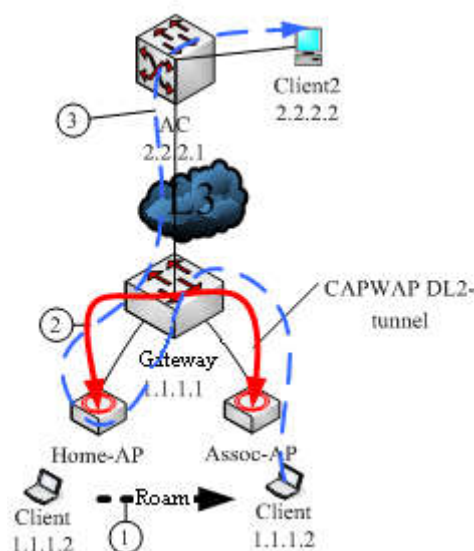

Fig 2-1 distributed tunnel creating and data forwarding

The advantages of distributed forwarding: distributed layer 2 tunnel solves the problem of wireless clients layer 3 roaming under the local forwarding mode and it does not have to forward all data to AC, so it reduces AC load effectively.

The disadvantages of distributed forwarding: distributed forwarding is conducted on AP, through layer 2 distributed tunnel supporting the layer 3 roaming of client; AP forwarding function will be affected. On the other hand, if Home-AP has error, layer 3 roaming will fail.

2.2 Distributed Forwarding Configuration

1. Enable/disable distributed layer2 tunnel function

Command	Explanation
Network Configuration Mode	
[no] dist-tunnel	Enable/disable distributed layer2 tunnel function.

2. Configure MaxClients of Home-AP

Command	Explanation
Wireless Global Mode	
dist-tunnel max-client <*1-8000*> **no dist-tunnel max-client**	Configure the maximum number of roaming clients of Home-AP. The no command will restore the default value as 128.

3. Configure IdleTimeout of Home-AP

Command	Explanation
Wireless Global Mode	
dist-tunnel idle-timeout <*30-3600*> **no dist-tunnel idle-timeout**	Configure the tunnel idle timeout value of Home-AP; the no command will restore the default value as 120s.

4. Configure MaxTimeout of Home-AP

Command	Explanation
Wireless Global Mode	
dist-tunnel max-timeout <*30-86400*> **no dist-tunnel max-timeout**	Configure Home-AP tunnel timeout value, the no command will restore the default value as 7200s.

5. Configure MaxMcastRepl of Home-AP

Command	Explanation
Wireless Global Mode	

dist-tunnel mcast-repl *<1-1024>* no dist-tunnel mcast-repl	Configure Home-AP multicast copying value; the no command will restore the default value as 128.

6. Enable/disable internal debug information of distributed layer2 tunnel

Command	Explanation
Admin Mode	
debug wireless dl2tunnel internal-info *<FF-FF-FF-FF-FF-FF>* no debug wireless dl2tunnel internal-info *<FF-FF-FF-FF-FF-FF>*	Enable/disable the distributed layer 2 interior tunnel debugging information.

7. Enable/disable internal error information of distributed layer2 tunnel

Command	Explanation
Admin Mode	
debug wireless dl2tunnel error *<FF-FF-FF-FF-FF-FF>* no debug wireless dl2tunnel error *<FF-FF-FF-FF-FF-FF>*	Enable/disable distributed layer 2 interior tunnel error information.

8. Clear roaming information of roaming user

Command	Explanation
Admin Mode	
clear wireless detected-client [*<macaddr>*] roam-history	Clear the roaming informations of roaming users. With no parameters, clear roaming informations of all roaming users.

2.3 Distributed Forwarding Configuration Examples
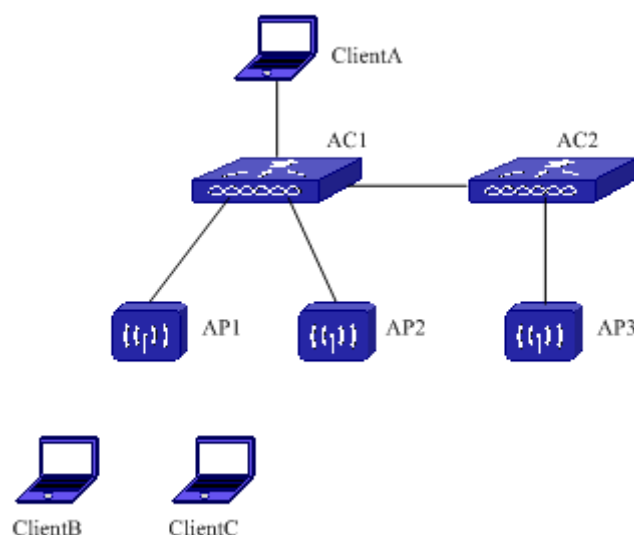
Configuration Topology:

Fig 2-2 Distributed Forwarding Configuration Topology

Introduction to Case:

As shown in Fig 2-2:

1. AC1 and AC2 make up cluster.

2. AP1 and AP2 associated with AC1, AP3 is associated with AC2.

3. Data forwarding adopts distributed forwarding mode.

Configuration Process:

1. Configure network and ssidap1 on AC, apply profile 1 on AP1.

AC> enable

AC# config

AC(config)# wireless

AC(config-wireless)# network 1

AC(config-network)# ssid ssidap1

AC(config-network)# dist-tunnel

AC(config-network)#vlan 11

AC(config-network)# exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)# enable

AC(config-ap-profile-radio)# vap 1

AC(config- ap-profile-vap)# network 1

AC(config-ap-profile-vap)# enable

AC(config- ap-profile-vap)# end

AC# wireless ap profile apply 1

2. Configure network and ssidap2 on AC1, apply profile 2 on AP2.

AC(config-wireless)# network 2

AC(config-network)# ssid ssidap2

AC(config-network)# dist-tunnel

AC(config-network)#vlan 12

AC(config-network)# exit

AC(config-wireless)#ap profile 2

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)# enable

AC(config-ap-profile-radio)# vap 2

AC(config- ap-profile-vap)# network 2

AC(config-ap-profile-vap)# enable

AC(config- ap-profile-vap)# end

AC# wireless ap profile apply 2

3. Configure network and ssidap3 on AC2, apply profile 1 on AP3.

AC> enable

AC# config

AC(config)# wireless

AC(config-wireless)# network 1

AC(config-network)# dist-tunnel

AC(config-network)# ssid ssidap3

AC(config-network)#vlan 13

AC(config-network)# exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)# enable

AC(config-ap-profile-radio)# vap 1

AC(config- ap-profile-vap)# network 1

AC(config-ap-profile-vap)# enable

AC(config- ap-profile-vap)# end

AC# wireless ap profile apply 1

2.4 Distributed Forwarding Troubleshooting

☞ Make sure that wired network is connected correctly.

☞ Make sure that distributed tunnel is enabled on both sides of Home-AP and Assoc-AP.

☞ Make sure that Home-AP and Assoc-AP are in different network segment. If

Home-AP and Assoc-AP are in the same network segment, distributed tunnel will not be enabled even if the vlan before and after roaming are different.