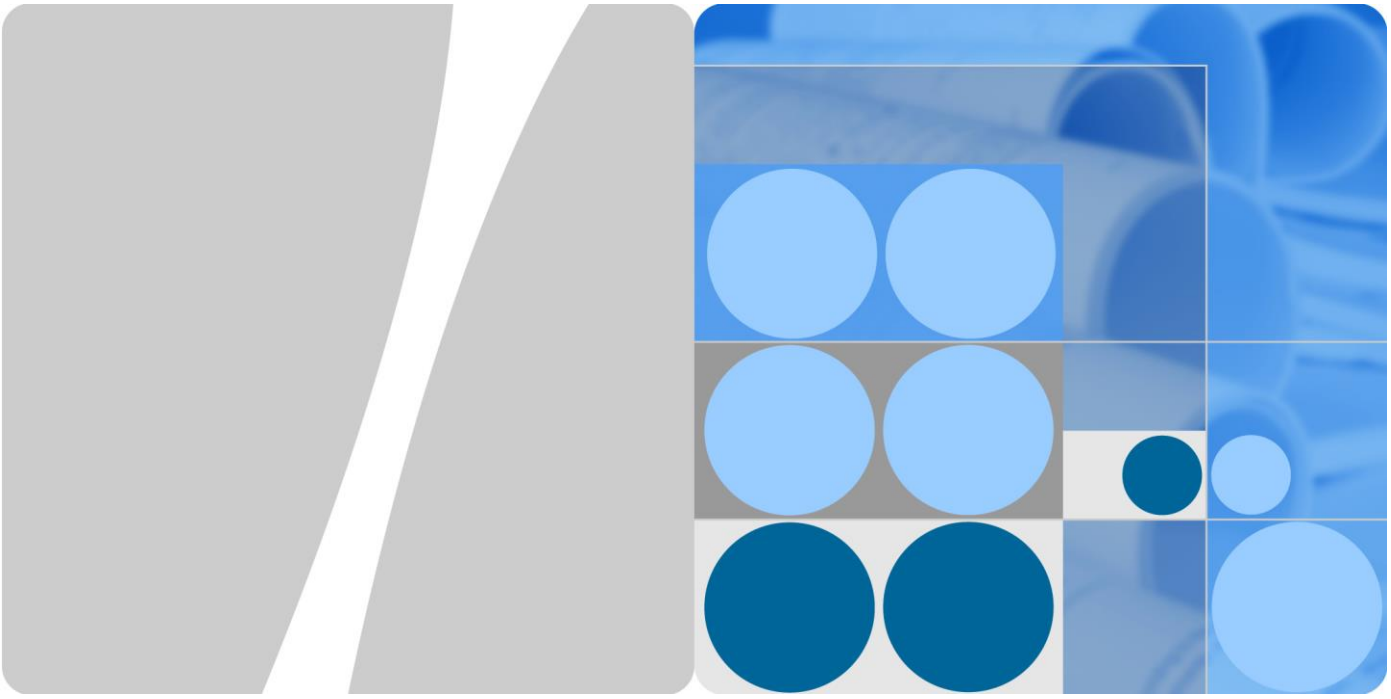


Agile Controller-Campus
V100R002C10

Permission Control Technical White Paper

Issue 01

Date 2016-04-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 Overview

1.1 Background

As enterprises are more informationized, network connections are made available in every corner of their offices. Their own staff and partners may usually bring laptops to office and connect to the LAN, which is challenging information security. Connections to the LAN from external unauthorized terminals may bring security threats like computer viruses and may even provide channels for stealing confidential information. In addition, as WLAN is mature and smart terminals are widely used, more enterprises are allowing their staff to bring their own smart devices to use in office, with intentions to address staff's individual needs and improve their productivity while reducing expenses in mobile terminals for office work. WLAN applications leave significant information security risks for enterprises.

To safeguard accesses to enterprises' networks, Huawei provides the Agile Controller solution to implement a unified permission control policy, which interworks with the permission control devices to control accesses from the inside and outside network.

1.2 Technical Features

Huawei Agile Controller provides network permission control solutions to meet diversified needs of customer networks. It provides IEEE 802.1X permission control for a wired LAN, security gateway-based permission control for a core network, and IEEEE 802.11i-based 802.1X permission control and portal-based guest permission control for a wireless network.

To address the need of complex network policies in the BYOD scenario, it provides flexible authentication and authorization policy management, which supports permission control policies in multiple dimensions and therefore suits diversified service control requirements. Huawei Agile Controller supports authorization and authentication policies in the following dimensions:

- User: It tells user identifies and applies different rules of authorization accordingly on the access devices.

- Location: It uses the IP address, wireless SSID, and AP MAC address as indications of the locations where the terminals are attempting on accesses, and applies location-varied authorization rules accordingly on the access devices.
- Time: It tells time periods and applies different authorization accordingly on the access devices.
- Terminal type: It identifies device types and applies different authorization rules accordingly on the access devices.
- Terminal security compliance: It tells whether terminals comply with security rules and applies different authorization rules accordingly on the access devices.

Huawei Agile Controller also provides authentication and authorization based on combinations of these dimensions to address the complex needs in the BYOD scenario.

2 Permission Control for Terminals

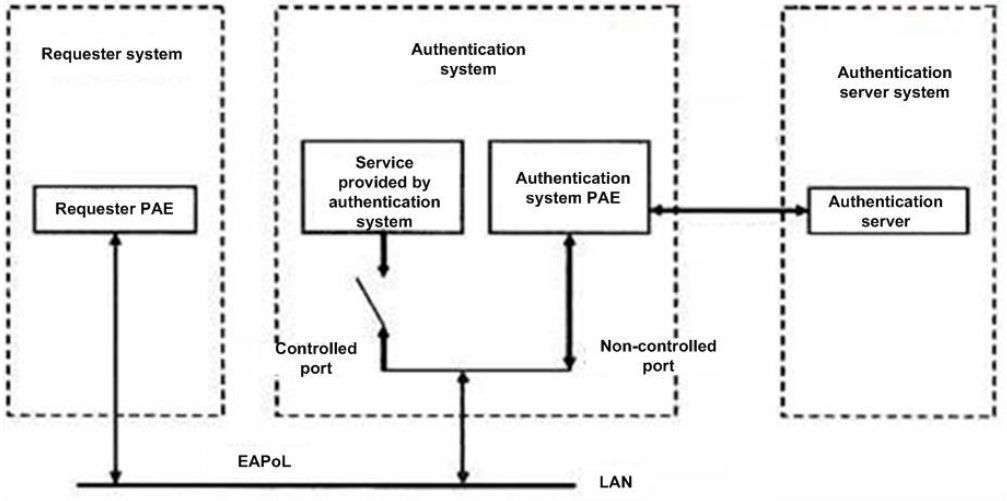
2.1 IEEE 802.1X Entry Control

IEEE 802 protocols are dominant in the LAN domain and the LAN defined in the traditional IEEE 802 protocol does not authorize accesses and allows any user connected to the switch to access resources on the LAN, leaving security risks.

IEEE 802.1X is a port-based network permission control protocol and it authorizes devices that are attempting on accesses at switch ports. If the user device connected to a switch port passes the authorization, it can access resources on the LAN; if it fails to pass the authorization, it cannot access any LAN resources, or in other words, it is physically disconnected from the LAN.

The IEEE 802.1X system has three components: requester (user access device), authentication unit (permission control unit), and authorization server. Figure 2-1 shows the IEEE 802.1X system architecture.

Figure 2-1 IEEE 802.1X system architecture

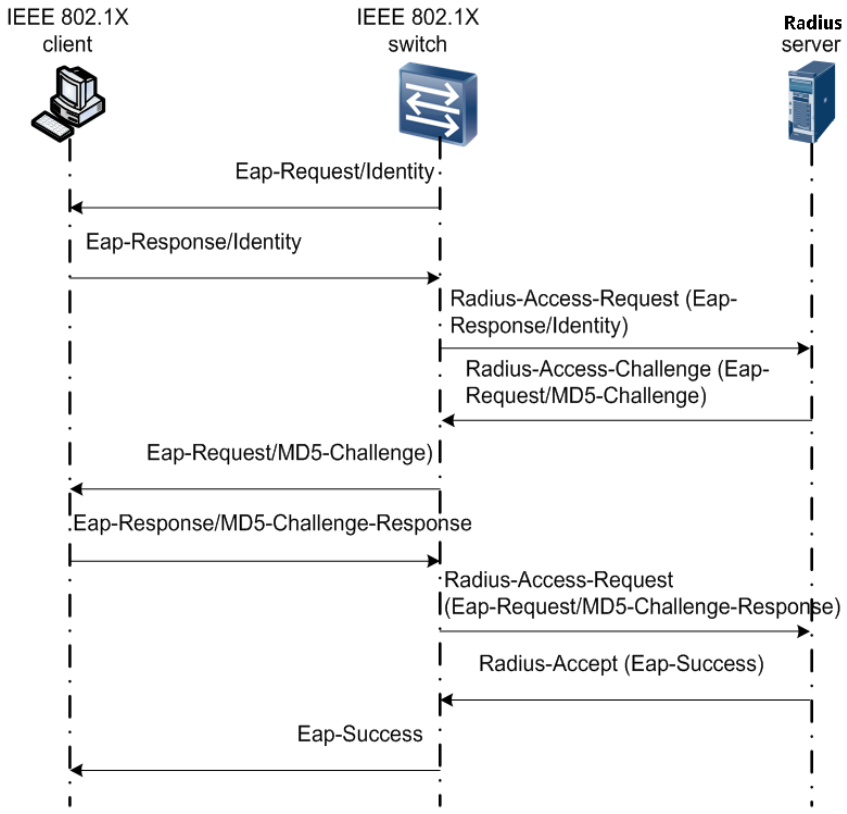


The requester refers to the terminal for IEEE 802.1X authorization and the requester port access entity (PAE) refers to the IEEE 802.1X client installed on the terminal. The authentication unit usually refers to an IEEE 802.1X switch or wireless AP/AC. The authentication server usually refers to a Radius server. In Huawei Agile Controller solution, the authentication server refers to the Agile Controller server.

2.1.1 Wired IEEE 802.1X Permission Control

The following uses IEEE 802.1X EAP-MD5 authentication as an example to show the authentication process.

Figure 2-2 IEEE 802.1X EAP-MD5 authentication



Authentication process:

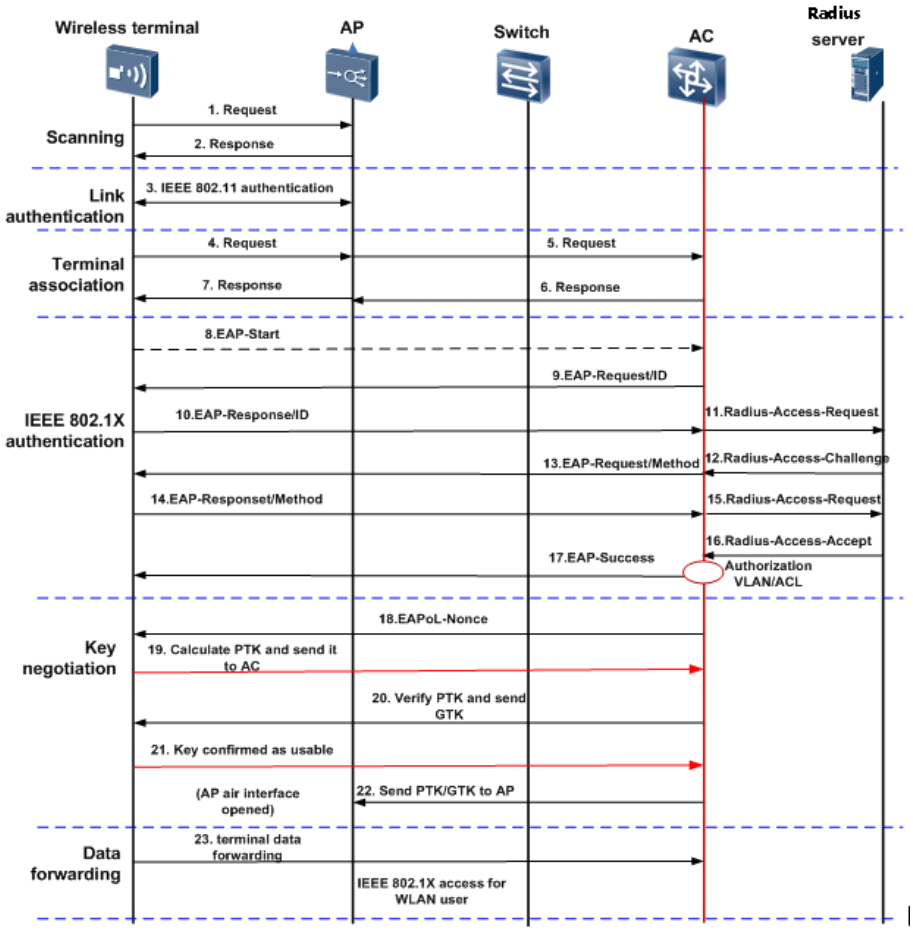
1. When the terminal connected to a switch port is powered on, the switch periodically sends an IEEE 802.1X authentication request to the terminal: Eap-Request/Identity.
2. After receiving the request, the IEEE 802.1X client on the terminal sends a response message (Eap-Response/Identity) with the authentication user account to the switch.
3. The switch forwards the received response message over Radius protocol packets to the Agile Controller server.
4. The Agile Controller Radius server sends the Eap-Request/MD5-Challenge message to the switch using the Radius protocol based on the selected authentication protocol (EAP-MD5).
5. The switch forwards the Eap-Request/MD5-Challenge message to the terminal.
6. After receiving the Eap-Request/MD5-Challenge message, the terminal calculates an EAP-MD5 response message according to the EAP-MD5 protocol.
7. The switch forwards the Eap-Request/MD5-Challenge-Response message from the terminal using the Radius protocol.
8. The Agile Controller server receives the response message and verifies the user account and password as required by the MD5 protocol. If they are verified as correct, the Agile Controller server sends a Radius-Accept message with the EAP-SUCCESS message to the switch.
9. After receiving the Radius-Accept message from the Agile Controller server, the switch opens the port (authenticated) and forwards the EAP-SUCCESS message to the terminal.

10. After receiving the EAP-SUCCESS message, the terminal finishes the authentication and starts the following services, for example, getting an IP address using DHCP.

2.1.2 Wireless IEEE 802.1X Permission Control

Wireless IEEE 802.1X permission control involves more interactions than wired IEEE 802.1X permission control, from enabling WLAN to getting an IP address.

Figure 2-3 Wireless IEEE 802.1X permission control



- Scanning for WLANs

  The terminal scans for WLANs. A WLAN list is named SSID.

- Authenticating links

  Authentication was designed for the earliest WLAN. This authentication is called link authentication, because a WLAN link has not been established yet.

  A link may be authenticated as follows:

  - Wired equivalent privacy (WEP): It derives from an RSA data encryption technique named RC4 and addresses more complex security needs. WEP authentication is weak. It had been abandoned after it was cracked a long time ago.
  - Now, WEP authentication is applicable for individual use only, though it is not formally forbidden. For WEP authentication, a pre-shared key (PSK) has to be

configured on the permission control device and terminal, and it has to be made public to the entire enterprise, which voids the key.

- Open system: no authentication.

  Link authentication does not provide sufficient security capabilities for WLAN. Then the WiFi Alliance designed IEEE 802.11i to secure accesses for enterprise and individuals. Specifically, no link authentication is performed but IEEE 802.11i authentication is performed on the established WiFi Layer 2 link.

- Setting up a terminal connection to AP

  The terminal sets up a connection to the AP/AC so that it can receive extensible authentication protocol (EAP) packets from the latter.

- Performing IEEE 802.1X authentication

  For both wired and wireless IEEE 802.1X authentications, a network device sends an Eap-Request/Identity message to start the authentication process. To secure IEEE 802.1X authentication in the wireless environment, the WiFi Alliance recommends the following authentication protocols:

  - EAP-TLS: used for certificate-based authentication.
  - EAP-PEAP: used for password-based authentication. As an embedded protocol, EAP-PEAP first uses EAP-TLS to set up a communication tunnel and then transfers other EAP protocols over the TLS tunnel.
  - EAP-TTLS: used for password-based authentication. As an embedded protocol, EAP-TTLS first uses EAP-TLS to set up a communication tunnel and then transfers other EAP protocols over the TLS tunnel.

- Negotiating on a key

  After the IEEE 802.1X authentication is successful, the Agile Controller sends a Radius-Accept packet with MPPE-KEY (used for link-layer key negotiation) to the AC/AP. Then the AC/AP negotiates on a link key with the access device based on the received MPPE-KEY. This negotiation process is usually called four handshakes.

- Getting an IP address and forwarding data

  After the key negotiation succeeds, the terminal attempts to get an IP address using DHCP and, after that, forwards data.

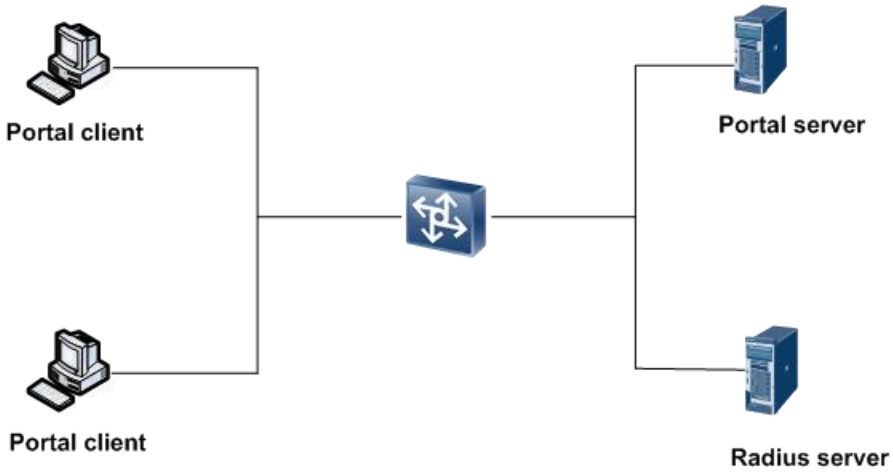
2.2 Portal Permission Control

On a traditional network, users with LAN accesses can access LAN devices or resources. To reinforce security controls and operation of network resources, user accesses have to be controlled in many cases. For example, for APs in some public or residential areas, or within an enterprise, the network access service provider allows only the users who have paid to access, by providing an account and password to each user. In addition, some enterprises may provide key resources of their own for external users that pass authentication to access.

The current permission controls like IEEE 802.1x and PPPoE require cooperation with the client, and are effective only at the access layer. Portal authentication provides flexible permission controls while eliminating the need to install a client. Specifically, it controls accesses at the access layer and key data entries that require protection. The Agile Controller solution provides Portal authentication for permission controls.

A portal client, server, broadband access server (BAS), and Radius server are involved in Portal authentication. The following shows the components of a Portal authentication system.

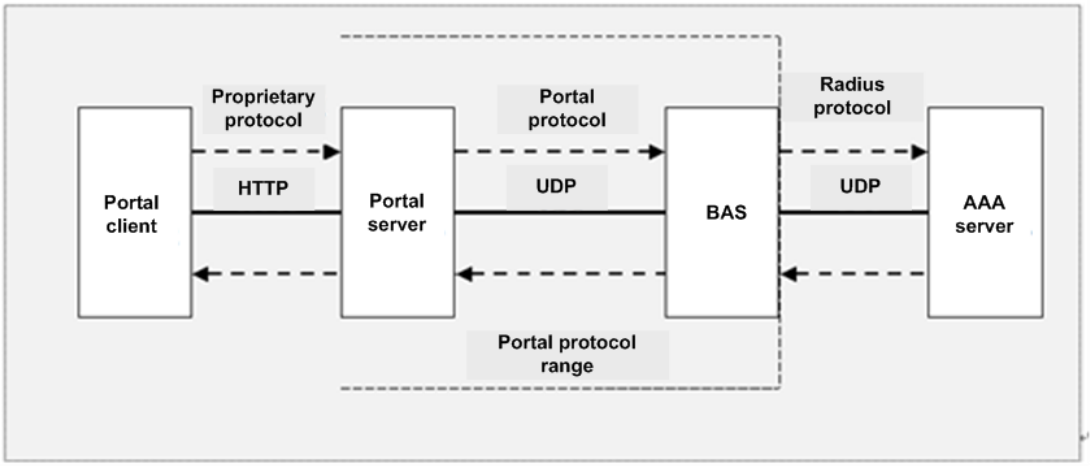
Figure 2-4 Portal authentication system components



- Portal client: It refers to a browser that runs the HTTP protocol and sends authentication requests.
- Portal server: It receives authentication requests and provides portal services and web-based authentication UIs. It exchanges the identity information of terminal with the BAS.
- BAS: It redirects HTTP authentication requests to the Portal server and exchanges information with the Portal server and Radius server to support user authentication, authorization, and billing.
- Radius server: It exchanges information with the BAS to support authorization, authentication, and billing.

Figure 2-5 shows the Portal protocol framework, which has two sections: Portal access and Radius authentication.

Figure 2-5 Portal protocol framework

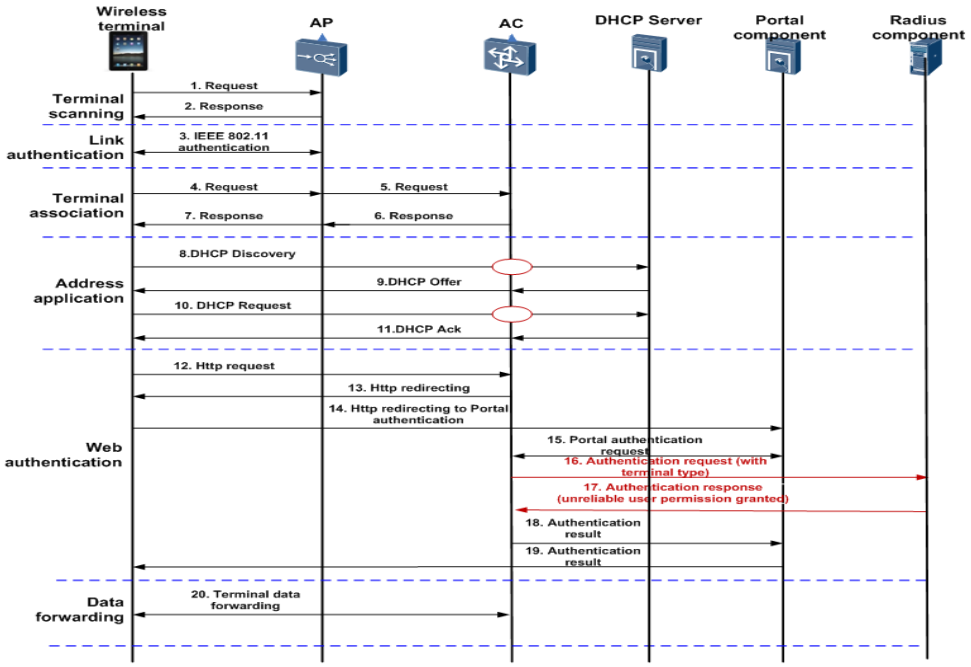


The Portal access protocol describes the protocol exchange between the Portal client and server.

- The Portal client submits authentication information using the HTTP protocol.
- The Portal server sends the authentication success/failure page to the Portal client using the HTTP protocol.
- The Portal client and server detects user online status by shaking hands.

The Portal authentication protocol describes the protocol exchange between the Portal server and BAS. It uses a client/server structure and uses the Request/Response message exchange to communicate. The following describes the Portal permission control in the wireless application.

Figure 2-6 Portal protocol framework



Portal authentication and Open system authentication are usually used together. After being associated with a wireless network, a terminal can get an IP address using DHCP without any need of extra authentication. Unlike IEEE 802.1X authentication, portal authentication does not require key negotiation between the terminal and AC/AP. In other words, the wireless link is not encrypted during Portal authentication. To secure communication between the terminal and service system, the service has to be encrypted.

During web authentication, if a terminal has not pass authentication on the AP/AC, the AP/AC will redirect traffic to the Portal component's authentication page when the terminal attempts to access the network using a browser.

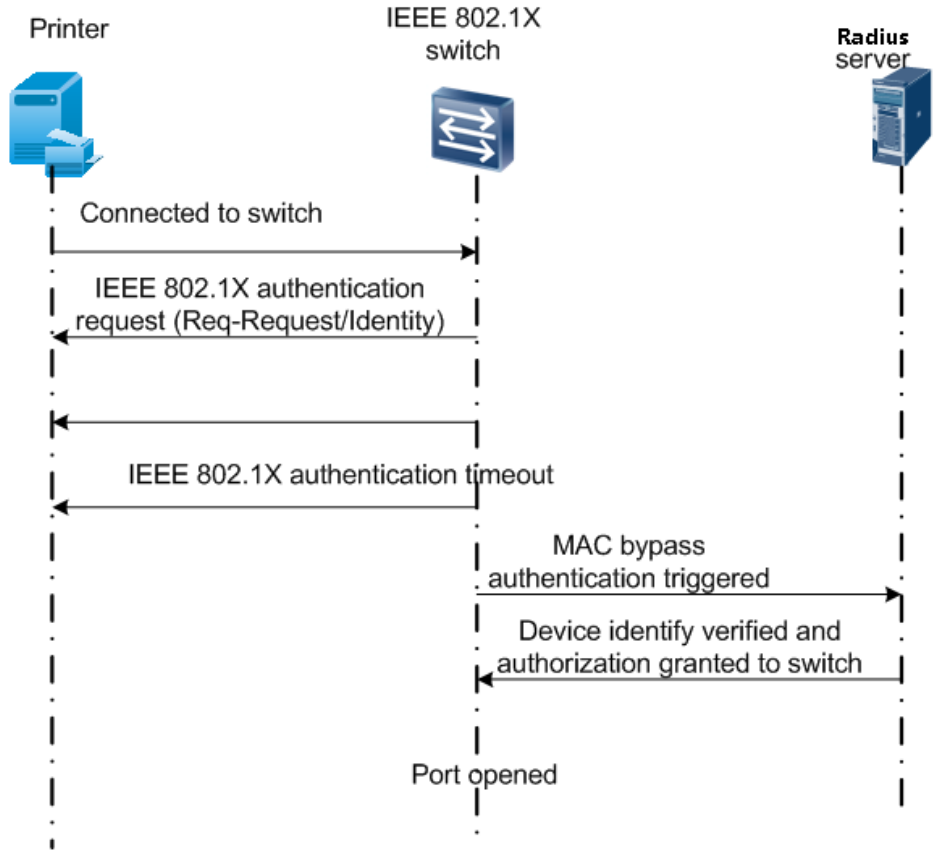
When the user enters the account and password on the authentication page, the Portal component will send Portal authentication request packets to the AC along with the user account or password. After receiving the Portal authentication request, the AC constructs Radius authentication packets and uses the packets to send the authentication request to the Radius component in the Agile Controller. Then the Radius component authenticates and authorizes the user. After receiving the authentication and authorization results, the AC/AP informs the Portal component using the Portal protocol packets. Then the Portal component informs the terminal user of the results.

2.3 MAC Bypass Permission Control

Wired IEEE 802.1X or wired Portal permission controls alone do not apply to dumb terminals such as printers, and IP phones. To resolve the issue, the Agile Controller system provides the MAC bypass permission control while interworking with network devices. Specifically, it allows dumb terminals to provide identity authentication based on devices and simplifies permission controls for dumb terminals.

Figure 2-7 shows the IEEE 802.1X + MAC bypass authentication process.

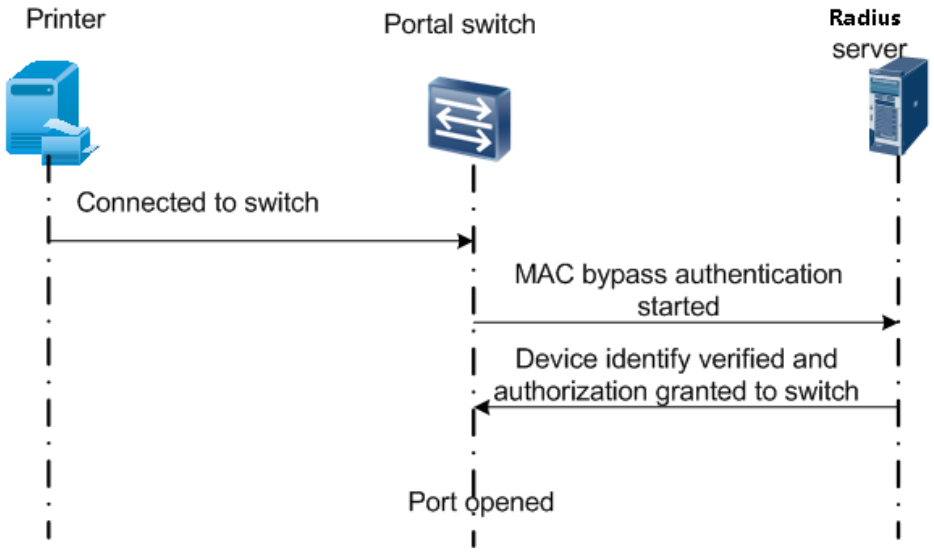
Figure 2-7 IEEE 802.1X + MAC bypass authentication



1. When a dumb terminal is connected to a switch, the switch port starts IEEE 802.1X authentication and sends an Eap-Request/Identity packet to the dumb terminal.
2. The dumb terminal does not respond. When the switch detects the authentication timeout event, it uses the dumb terminal's MAC address as the account and sends a MAC bypass authentication request to the Agile Controller server.
3. The Agile Controller server checks the identity of the dumb terminal and sends authorization information to the switch.
4. After receiving the authentication success message from the Agile Controller server, the switch opens the port.

Figure 2-8 shows the Portal + MAC bypass authentication process.

Figure 2-8 Portal + MAC bypass authentication process



When a dumb terminal is connected to a Portal switch, the switch starts MAC bypass authentication. After that, the dumb terminal is connected to the network.

2.4 SACG Permission Control

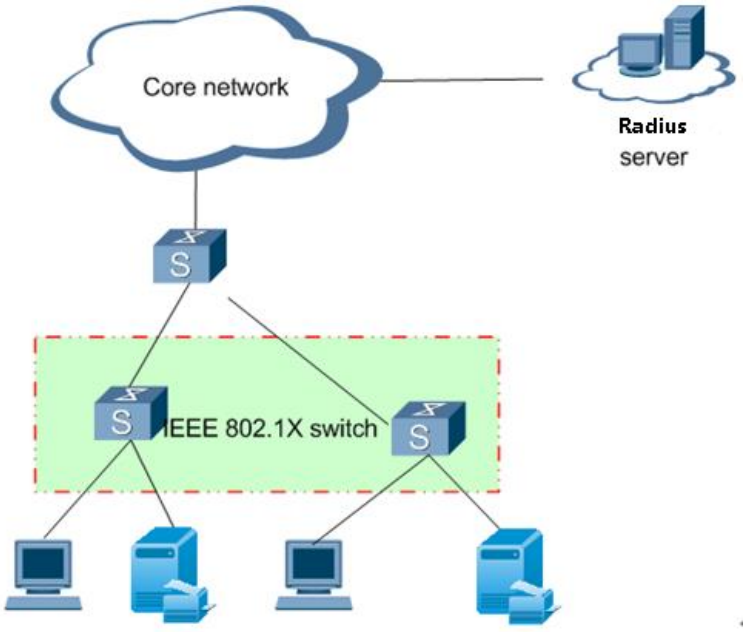
When IEEE 802.1X permission controls can hardly applied on a network, security permission control gateway (SACG) permission control may be used. SACG refers to a dedicated permission control gateway that was developed on the telecom-class firewall hardware platform. It has the following functions:

- Communicates with the Agile Controller server, synchronizes the permission control rules, and converts them into ACLs. The synchronized rules include pre-authentication domain, isolation domain, and post-authentication domain.
- Checks the authentication status of the data packets' IP address and, if the IP address has not been authenticated, applies ACLs of the pre-authentication domain to the IP address to filter data packets.
- When the terminal user passes authentication, the Agile Controller server sends post-authentication domain parameters to the permission control device. These parameters define the ACL rules.
- Filters data packets by applying the mapping ACL rules to control the access range of the terminal.

3 Typical Applications

3.1 IEEE 802.1X + MAC Bypass Permission Control

Figure 3-1 Wired IEEE 802.1X + MAC permission control



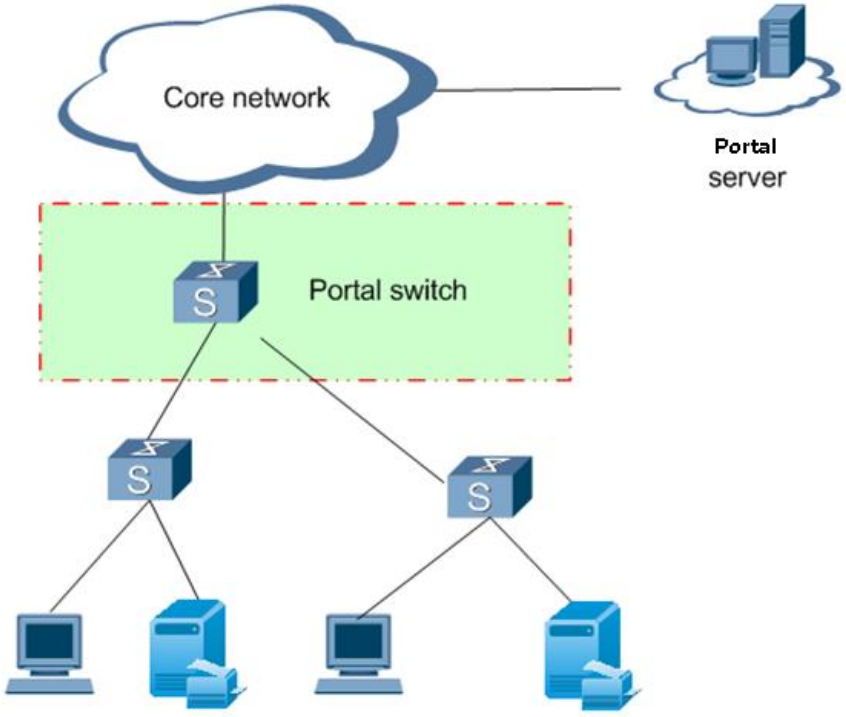
IEEE 802.1X is enabled at the switch closest to the terminal. A security agent (or the OS-carried IEEE 802.1X client) has to be deployed before the terminal accesses the network. If the switch supports guest VLAN and dynamic VLAN, the switch can be configured to allow the terminal to access the guest VLAN before it is authenticated. The guest VLAN is defined by ACLs configured on the aggregation switch. When the terminal passes IEEE 802.1X authentication, the Agile Controller server applies authorization parameters like

VLAN and ACL to the access switch to control the network access permissions of the terminal.

MAC bypass authentication will be performed for dumb terminals like printers and IP phones. When a dumb terminal is connected to the network, MAC bypass authentication is triggered by the switch.

3.2 Portal Permission Control

Figure 3-2 Portal permission control

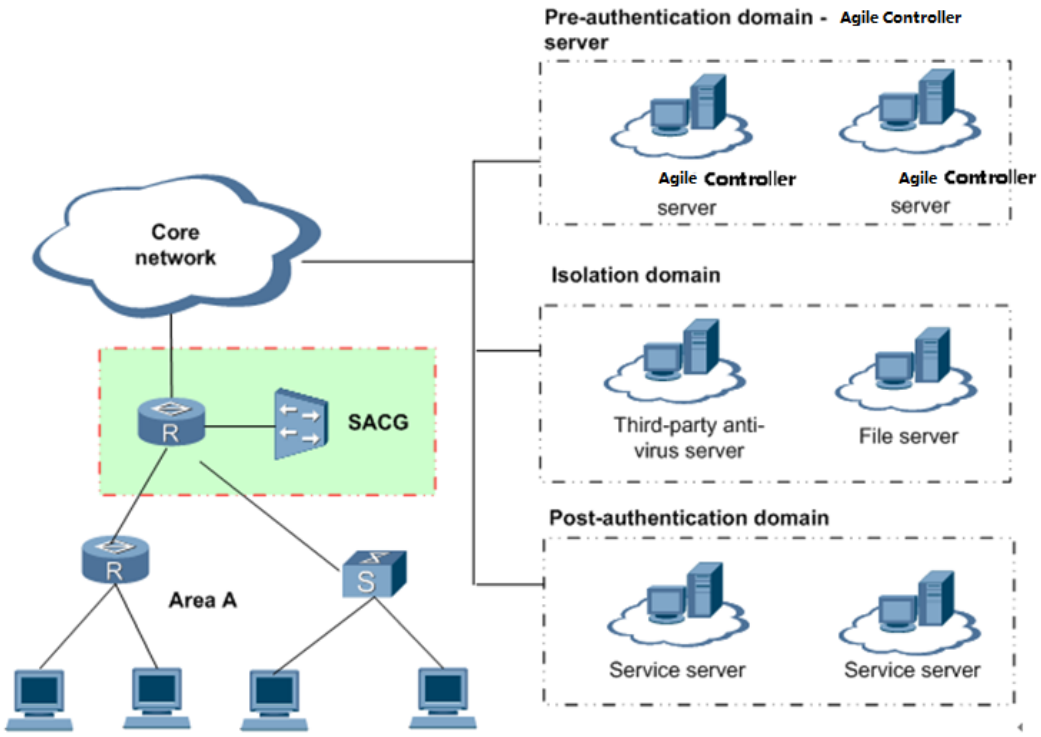


Portal + MAC bypass authentication is enabled at the gateway that connects to the terminal so that the terminal can access the network using web authentication. Alternatively, the NAC client of the Agile Controller can be installed on the terminal so that the terminal uses the client for authentication.

MAC bypass authentication will be performed for dumb terminals like printers and IP phones. When a dumb terminal is connected to the network, MAC bypass authentication is triggered.

3.3 SACG Permission Control

Figure 3-3 SACG permission control



As shown in the figure, the SACG is attached to a Layer 3 switch or router. Generally, packet redirecting is configured on the switch or policy-based routing (PBR) is configured on the router so that the upstream traffic of terminal PCs is redirected to the SACG, which filters packets and sends them back to the switch or router for normal forwarding. A service system may send data packets to the terminal PC. To ensure performance, these data packets are not redirected to the SACG, but are directly forwarded by switch or router. The SACG can be attached to the key network devices that control terminal PCs' access to service system, such as core switch or router on a Agile network or switch or router deployed right ahead of a data center.

4 References

- *RFC 2865: Remote Authentication Dial In User Service (RADIUS)*
- *RFC 2284: PPP Extensible Authentication Protocol (EAP)*
- *IEEE Std 802.1X-2001: Port-Based Network Permission Control*
- *IEEE Std 802.11i 2004: Wireless LAN Medium Permission Control (MAC) and Physical Layer (PHY) specifications*