Huawei S Series Switches with the Versatile Routing Platform Software Version 5

Interoperability with the Cisco Identity Services Engine (ISE)

Tolly Report #216161
Commissioned by
Huawei Technologies Co., Ltd

December 2016

Huawei Technologies Co., Ltd

S Series Switches

Interoperability with the Cisco Identity Services Engine (ISE)

Tested October 2016

Executive Summary

Huawei commissioned Tolly to verify the Huawei S series switches' interoperability with the Cisco Identity Services Engine (ISE) for authentication and more.

The complete list of devices tested is available in Table 1. Device support for each individual test case is provided in the test results (Table 2) and further details in the test case descriptions.

Huawei S Series Switches Under Test

Device Under Test	S/W Version	Platform Version	Hardware Model
Huawei S12700	Huawei Versatile Routing Platform Software VRP (R) software, Version 5.160 (S12700 V200R010C00SPC300)	VRP (R) software, Version 5.160	12704
Huawei S5720	Huawei Versatile Routing Platform Software VRP (R) software, Version 5.160 (S5720 V200R010C00SPC300)	VRP (R) software, Version 5.160	S5720-32C-HI-24S

Cisco Identity Services Engine (ISE)

Product	Version
Identity Services Engine (ISE)	Version 2.0.0.306 ADE-OS Version 2.3.0.187

Source: Tolly, October 2016

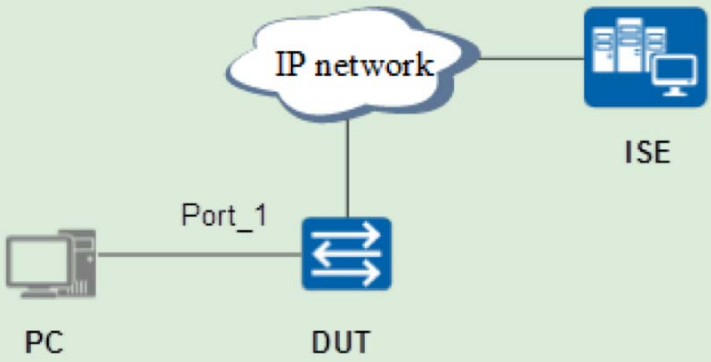
Table 1

Huawei S Series Switches Interoperability with the Cisco ISE Test Results

Authentication Protocol		**Generic RADIUS Attributes**	
✔	PAP/CHAP	✔	Framed-IP-Address On-demand DHCP IP address
✔	EAP-MD5	✔	Framed-Pool On-demand DHCP Pool
✔	PEAP	✔	NAS-Port
✔	EAP-TLS	**Others**	
✔	EAP-TTLS	✔	Post-rejection Authentication Once a client is rejected by ISE, authenticate certain VLAN to it
✔	EAP-FAST	✔	Time-based Authentication Policy
Authentication Method		**Change of Authorization (CoA)**	
✔	Wired MAC Authentication	✔	Session Re-authentication
✔	Wired 802.1X Authentication	✔	Session Termination
✔	Wireless MAC Authentication	✔	CoA Port Customization in ISE Huawei S switches use port 3799 for CoA. The CoA destination port can be changed to 3799 in Cisco ISE for interoperability
✔	Wireless 802.1X Authentication	**Endpoint Profiling**	
✔	Wired and Wireless Web Portal Authentication Huawei S Switch as the Portal Server	✔	with DHCP Packets e.g. DHCP Option60: Vendor Class Identifier
✔	Wired and Wireless Web Portal Authentication Cisco ISE as the Portal Server	✔	with MAC Addresses e.g. Organizationally Unique Identifier (OUI) in the MAC Address
✔	Wired Mixed Authentication e.g. MAC and 802.1X Authentication	✔	with HTTP Packets e.g. User-Agent attribute in the HTTP packet
✔	Wireless Mixed Authentication e.g. MAC and Web Portal Authentication	✔	with RADIUS Packets e.g. CallingStationID attribute in RADIUS
Authentication Policy		✔	Network Scan (NMAP)
Built-in Attributes		**Other**	
✔	Dynamic VLAN Assign one existing VLAN to the user with the VLAN number	✔	Posture Assessment with the Cisco ISE and the Cisco NAC Appliance Agent
✔	Dynamic ACL Assign one existing ACL to the user with the ACL number	✔	Guest Management Guest self-registration and authentication
Huawei Attributes		✔	BYOD BYOD device self-registration and authentication
✔	Dynamic ACL Rule Create a new ACL rule with the HW-Data-Filter attribute		
✔	Dynamic UCL Group Assign one existing UCL group to the user with the HW-UCL-Group attribute and the UCL group's name		
✔	Dynamic CAR CIR (rate limiting) create a new CAR CIR rule with the HW-Input-Committed-Information-Rate attribute or/and the HW-Output-Committed-Information-Rate attribute		
✔	Service Scheme Assign one existing service scheme to the user with Huawei's HW-Service-Scheme attribute and the service scheme's name		

Source: Tolly, October 2016

Table 2

Test 1.1	PAP/CHAP Authentication
Objective	Verify the 802.1X authentication method with the PAP/CHAP authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as CHAP. # dot1x-access-profile name tolly dot1x authentication-method chap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the CHAP mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template tolly radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 # 3. Configure the aaa scheme on the switch. # authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly authentication-scheme tolly accounting-scheme tolly radius-server tolly # 4. Configure the 802.1X authentication profile on the device. # authentication-profile name tolly dot1x-access-profile tolly access-domain tolly dot1x force #

Test Results

5. Configure the DHCP server on the device, and enable dot1x authentication on the correspondent interface.

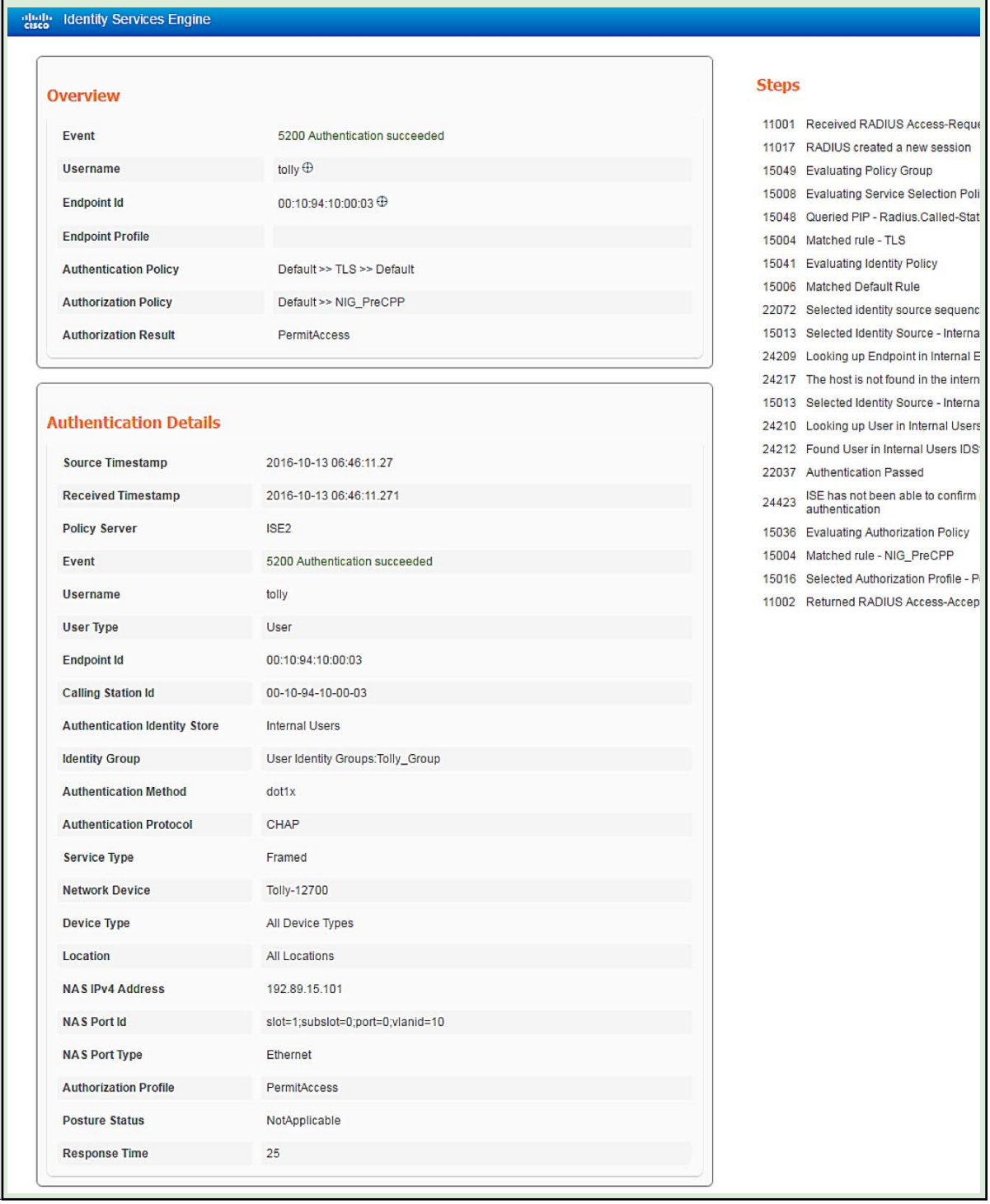
```
#
interface Vlanif4090
ip address 192.89.6.202 255.255.255.0
dhcp select interface
interface GigabitEthernet1/1/0
port link-type hybrid
port hybrid pvid vlan 4090
port hybrid untagged vlan 4090
authentication-profile tolly
#
```

6. The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16093                          192.89.17.109    3c97-0ed9-bd91 Pre-authen
 16094  tolly                   -                0010-9410-0003 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 16094

Basic:
  User ID                       : 16094
  User name                     : tolly
  Domain-name                   : tolly
  User MAC                      : 0010-9410-0003
  User IP address               : -
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : XGigabitEthernet1/0/0
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/10
  User access time              : 2016/10/13 14:46:47
  User accounting session ID    : s127000100000000010d352bf0003ede
  Option82 information          : -
  User access type              : 802.1x
  Terminal Device Type          : Data Terminal

AAA:
  User authentication type      : 802.1x authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None

[Tolly_auth]
```

Test Results	**Authentication Details** **Source Timestamp** 2016-10-13 06:46:11.27 **Received Timestamp** 2016-10-13 06:46:11.271 **Policy Server** ISE2 **Event** 5200 Authentication succeeded **Username** tolly **User Type** User **Endpoint Id** 00:10:94:10:00:03 **Calling Station Id** 00-10-94-10-00-03 **Authentication Identity Store** Internal Users **Identity Group** User Identity Groups:Tolly_Group **Authentication Method** dot1x **Authentication Protocol** CHAP **Service Type** Framed **Network Device** Tolly-12700 **Device Type** All Device Types

Test Results



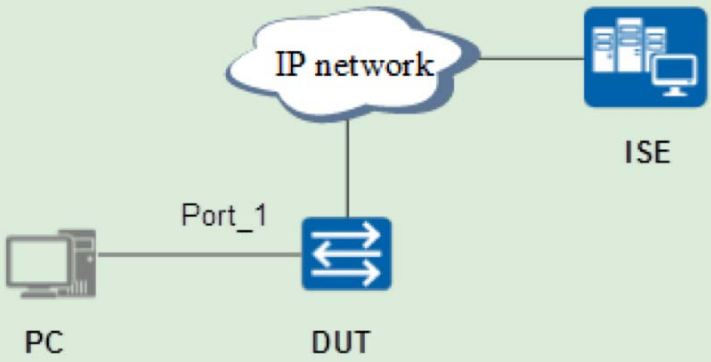
Test Results

Other Attributes

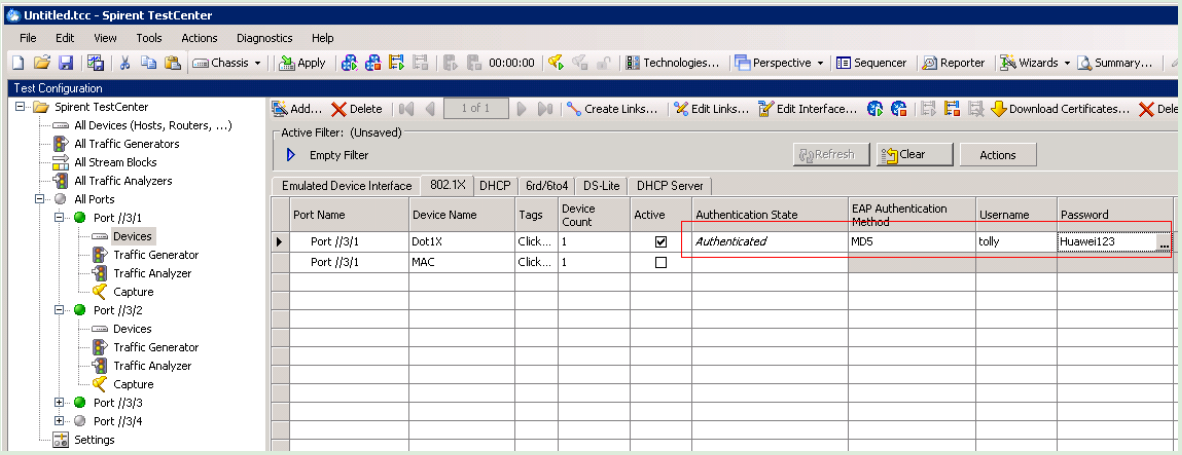
ConfigVersionId	111
DestinationPort	1812
Protocol	Radius
NAS-Port	16777226
Framed-Protocol	PPP
Vendor Specific	00:00:07:db:3b:06:57:fe:01:4d:3c:23:32:35:35:2e:32:35:35:2e:32:35:35:2e:32:35:35:20:30:30:3a:31:30:3a:39:34:3a:31:30:3a:30:30:3a:30:33:1a:06:00:00:3e:de:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
Acct-Session-Id	s12700010000000000010d352bf0003ede
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	8ade1f15-aef1-4a9a-8158-d02e835179db
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
AcsSessionID	ISE2/265353892/2665
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	Guest Users
SelectedAuthenticationIdentityStores	Tander
SelectedAuthenticationIdentityStores	test.com
SelectedAuthenticationIdentityStores	Initial_Scope
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	AD1
AuthorizationPolicyMatchedRule	NIG_PreCPP
CPMSessionID	c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE
EndPointMACAddress	00-10-94-10-00-03
ISEPolicySetName	Default
AllowedProtocolMatchedRule	TLS
IdentitySelectionMatchedRule	Default
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	tolly
NAS-Identifier	s12700
Device IP Address	192.89.15.101
Called-Station-ID	54:39:DF:C9:9A:E0

Result

State	ReauthSession:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE
Class	CACS:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE:ISE2/265353892/2665
LicenseTypes	5

Test 1.2	EAP-MD5
Objective	Verify the 802.1X authentication method with the EAP-MD5 authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as EAP. # dot1x-access-profile name tolly dot1x authentication-method eap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the EAP-MD5 mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results



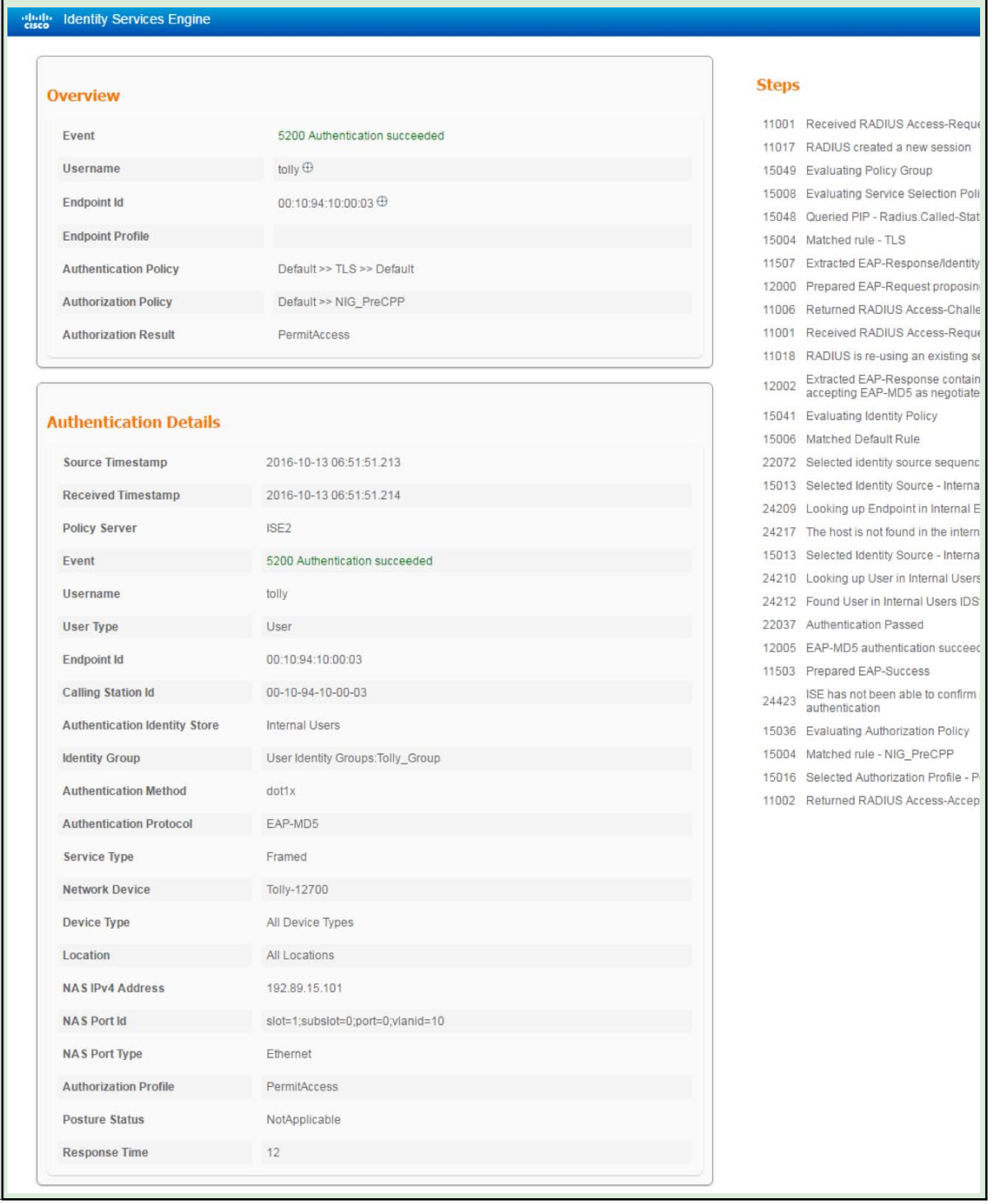

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                  IP address       MAC            Status
 ------------------------------------------------------------------------------
 16097                            192.89.17.109    3c97-0ed9-bd91 Pre-authen
 16098  tolly                     -                0010-9410-0003 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]
[Tolly_auth]
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 16098

Basic:
  User ID                        : 16098
  User name                      : tolly
  Domain-name                    : tolly
  User MAC                       : 0010-9410-0003
  User IP address                : -
  User vpn-instance              : -
  User IPv6 address              : -
  User access Interface          : XGigabitEthernet1/0/0
  User vlan event                : Success
  QinQVlan/UserVlan              : 0/10
  User access time               : 2016/10/13 14:52:26
  User accounting session ID     : Tolly_auth0100000000000101a103c0003ee2
  Option82 information           : -
  User access type               : 802.1x
  Terminal Device Type           : Data Terminal

AAA:
  User authentication type       : 802.1x authentication
  Current authentication method  : RADIUS
  Current authorization method   : -
  Current accounting method      : None
```

Test Results

Authentication Details

Source Timestamp	2016-10-13 06:51:51.213
Received Timestamp	2016-10-13 06:51:51.214
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	tolly
User Type	User
Endpoint Id	00:10:94:10:00:03
Calling Station Id	00-10-94-10-00-03
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group
Authentication Method	dot1x
Authentication Protocol	EAP-MD5
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1;subslot=0;port=0;vlanid=10

Test Results



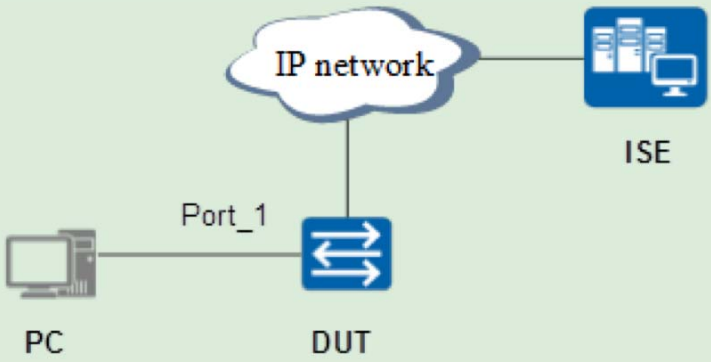
Test Results

Other Attributes

ConfigVersionId	112
DestinationPort	1812
Protocol	Radius
NAS-Port	16777226
Framed-Protocol	PPP
Framed-MTU	1500
Login-IP-Host	0.0.0.0
State	64CPMSessionID=c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5Hlxe4HhBWxpmpyVPE;29SessionID=ISE2/265353892/2668;
Vendor Specific	00:00:07:db:3b:06:57:fe:01:4d:3c:23:32:35:35:2e:32:35:35:2e:32:35:35:2e:32:35:35:20:30:30:3a:31:30:3a:39:34:3a:31:30:3a:30:30:3a:30:33:1a:06:00:00:3e:e2:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	8ade1f15-aef1-4a9a-8158-d02e835179db
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
AcsSessionID	ISE2/265353892/2668
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	Guest Users
SelectedAuthenticationIdentityStores	Tander
SelectedAuthenticationIdentityStores	test.com
SelectedAuthenticationIdentityStores	Initial_Scope
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	AD1
AuthorizationPolicyMatchedRule	NIG_PreCPP
CPMSessionID	c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5Hlxe4HhBWxpmpyVPE
EndPointMACAddress	00-10-94-10-00-03
ISEPolicySetName	Default
AllowedProtocolMatchedRule	TLS
IdentitySelectionMatchedRule	Default
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	tolly
NAS-Identifier	s12700
Device IP Address	192.89.15.101
Called-Station-ID	54:39:DF:C9:9A:E0

Result

State	ReauthSession:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5Hlxe4HhBWxpmpyVPE
Class	CACS:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5Hlxe4HhBWxpmpyVPE:ISE2/265353892/2668
LicenseTypes	5

Test 1.3	PEAP
Objective	Verify the 802.1X authentication method with the PEAP authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as EAP. # dot1x-access-profile name tolly dot1x authentication-method eap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the PEAP mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results

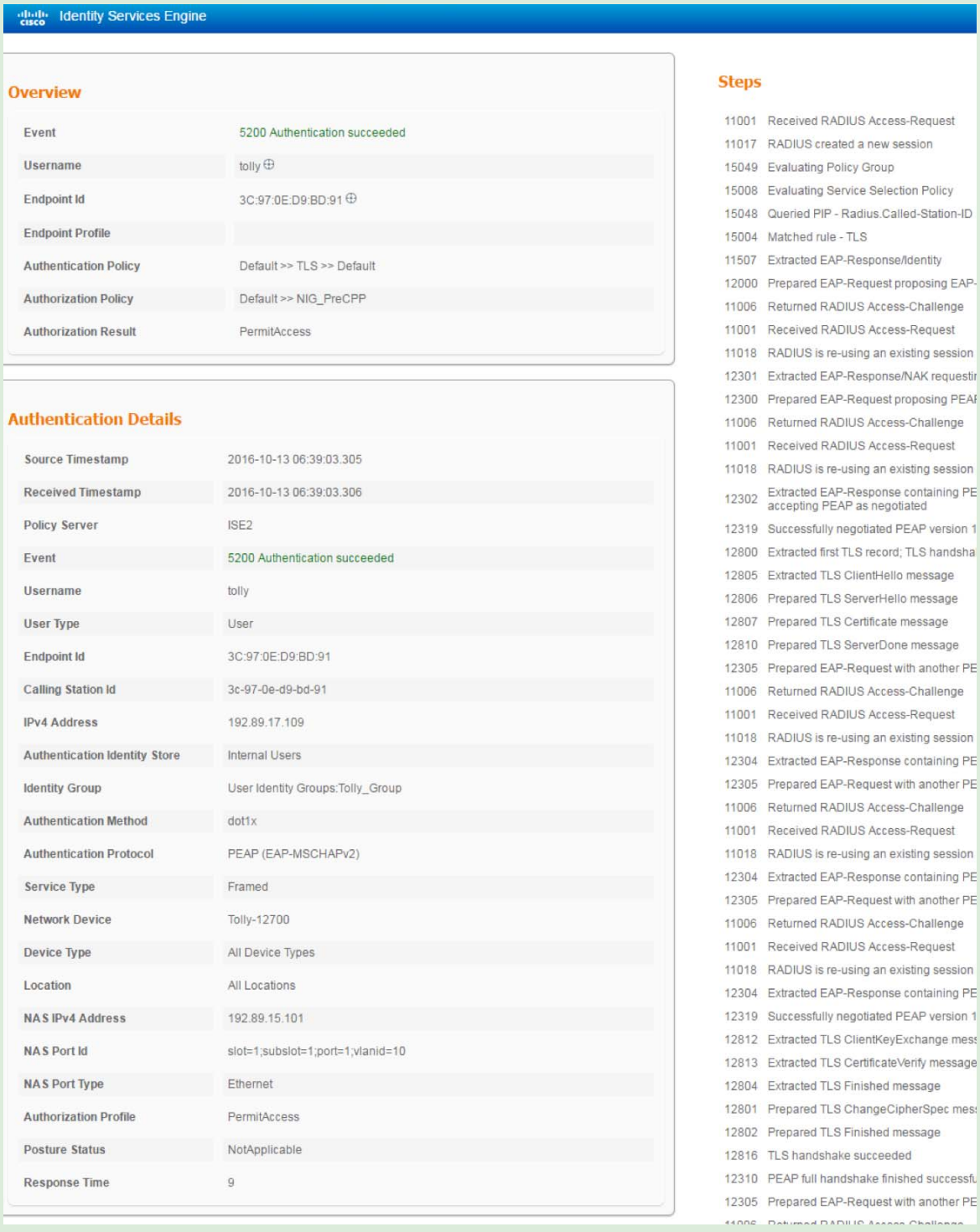
```
[Tolly_auth-aaa]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16086  tolly                    192.89.17.109    3c97-0ed9-bd91 Success
 16087  10-51-72-14-C8-6U        30.1.1.254       1051-7214-c86U Pre-authen
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth-aaa]dis access-user  us
[Tolly_auth-aaa]dis access-user  user
[Tolly_auth-aaa]dis access-user  user-id 16086

Basic:
  User ID                        : 16086
  User name                      : tolly
  Domain-name                    : tolly
  User MAC                       : 3c97-0ed9-bd91
  User IP address                : 192.89.17.109
  User vpn-instance              : -
  User IPv6 address              : -
  User access Interface          : GigabitEthernet1/1/1
  User vlan event                : Success
  QinQVlan/UserVlan              : 0/10
  User access time               : 2016/10/13 14:37:52
  User accounting session ID     : Tolly_auth01101000000010f1dd0c0003ed6
  Option82 information           : -
  User access type               : 802.1x
  Terminal Device Type           : Data Terminal

AAA:
  User authentication type       : 802.1x authentication
  Current authentication method  : RADIUS
  Current authorization method   : -
  Current accounting method      : None
```

Test Results

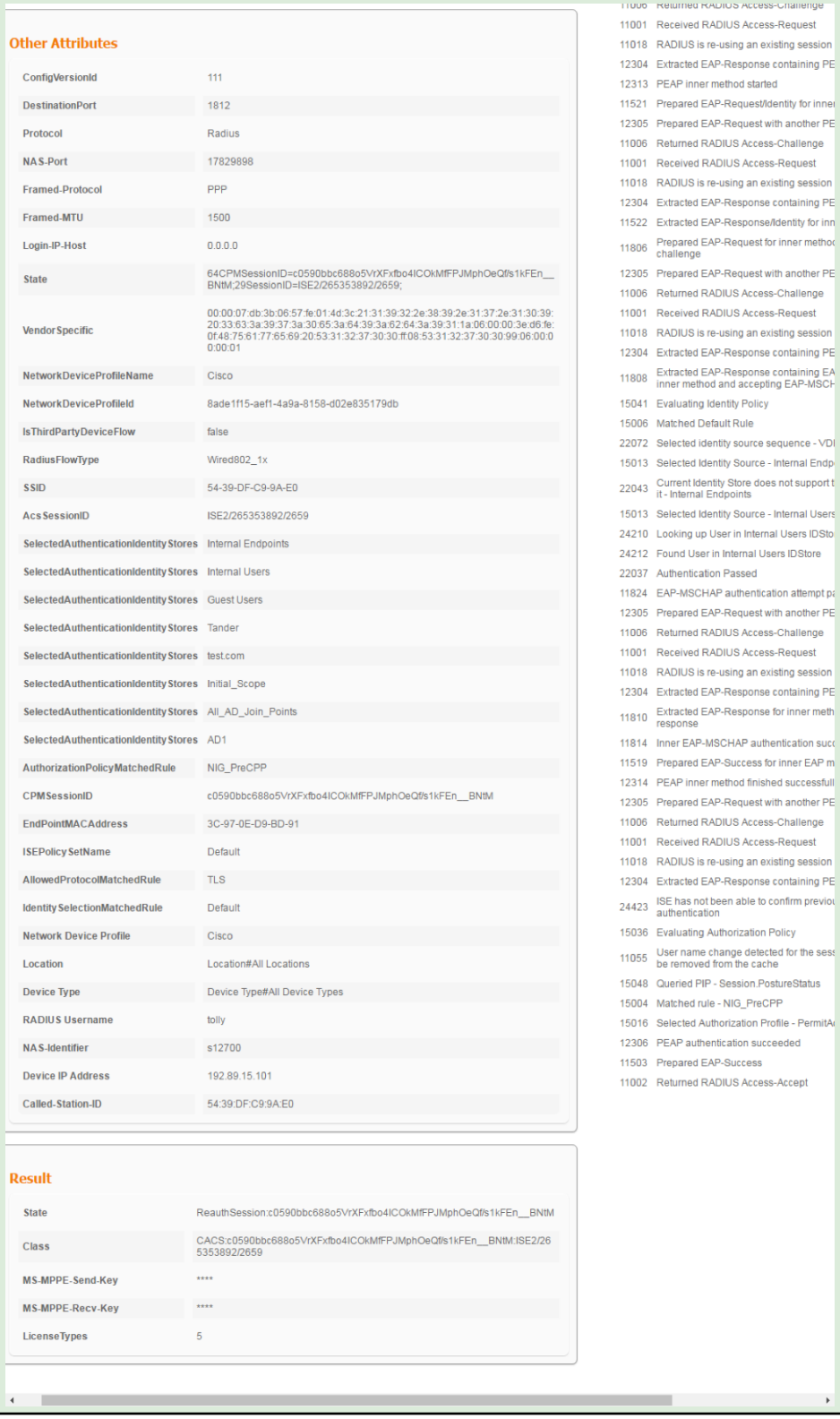
Authentication Details

Source Timestamp	2016-10-13 06:39:03.305
Received Timestamp	2016-10-13 06:39:03.306
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	tolly
User Type	User
Endpoint Id	3C:97:0E:D9:BD:91
Calling Station Id	3c-97-0e-d9-bd-91
IPv4 Address	192.89.17.109
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1;subslot=1;port=1;vlanid=10

Test Results



Test Results



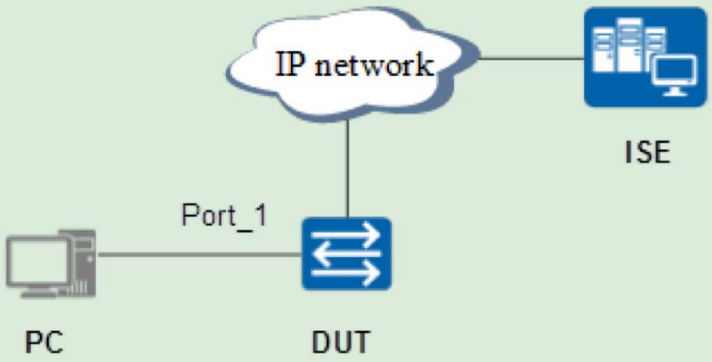
Other Attributes

ConfigVersionId	111
DestinationPort	1812
Protocol	Radius
NAS-Port	17829898
Framed-Protocol	PPP
Framed-MTU	1500
Login-IP-Host	0.0.0.0
State	64CPMSessionID=c0590bbc688o5VrXFxfbo4ICOkMfFPJMphOeQf/s1kFEn__BNtM;29SessionID=ISE2/265353892/2659;
Vendor Specific	00:00:07:db:3b:06:57:fe:01:4d:3c:21:31:39:32:2e:38:39:2e:31:37:2e:31:30:39:20:33:63:3a:39:37:3a:30:65:3a:64:39:3a:62:64:3a:39:31:1a:06:00:00:3e:d6:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	8ade1f15-aef1-4a9a-8158-d02e835179db
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
AcsSessionID	ISE2/265353892/2659
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	Guest Users
SelectedAuthenticationIdentityStores	Tander
SelectedAuthenticationIdentityStores	test.com
SelectedAuthenticationIdentityStores	Initial_Scope
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	AD1
AuthorizationPolicyMatchedRule	NIG_PreCPP
CPMSessionID	c0590bbc688o5VrXFxfbo4ICOkMfFPJMphOeQf/s1kFEn__BNtM
EndPointMACAddress	3C-97-0E-D9-BD-91
ISEPolicySetName	Default
AllowedProtocolMatchedRule	TLS
IdentitySelectionMatchedRule	Default
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	tolly
NAS-Identifier	s12700
Device IP Address	192.89.15.101
Called-Station-ID	54:39:DF:C9:9A:E0

Result

State	ReauthSession:c0590bbc688o5VrXFxfbo4ICOkMfFPJMphOeQf/s1kFEn__BNtM
Class	CACS:c0590bbc688o5VrXFxfbo4ICOkMfFPJMphOeQf/s1kFEn__BNtM:ISE2/265353892/2659
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	5

11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PE
12313	PEAP inner method started
11521	Prepared EAP-Request/Identity for inne
12305	Prepared EAP-Request with another PE
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PE
11522	Extracted EAP-Response/Identity for inn
11806	Prepared EAP-Request for inner metho challenge
12305	Prepared EAP-Request with another PE
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PE
11808	Extracted EAP-Response containing EA inner method and accepting EAP-MSCH
15041	Evaluating Identity Policy
15006	Matched Default Rule
22072	Selected identity source sequence - VDI
15013	Selected Identity Source - Internal Endp
22043	Current Identity Store does not support t it - Internal Endpoints
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDSto
24212	Found User in Internal Users IDStore
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt pa
12305	Prepared EAP-Request with another PE
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PE
11810	Extracted EAP-Response for inner meth response
11814	Inner EAP-MSCHAP authentication succ
11519	Prepared EAP-Success for inner EAP m
12314	PEAP inner method finished successfull
12305	Prepared EAP-Request with another PE
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PE
24423	ISE has not been able to confirm previou authentication
15036	Evaluating Authorization Policy
11055	User name change detected for the sess be removed from the cache
15048	Queried PIP - Session.PostureStatus
15004	Matched rule - NIG_PreCPP
15016	Selected Authorization Profile - PermitA
12306	PEAP authentication succeeded
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

Test 1.4	EAP-TLS
Objective	Verify the 802.1X authentication method with the EAP-TLS authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as EAP. # dot1x-access-profile name tolly dot1x authentication-method eap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the EAP-TLS mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results

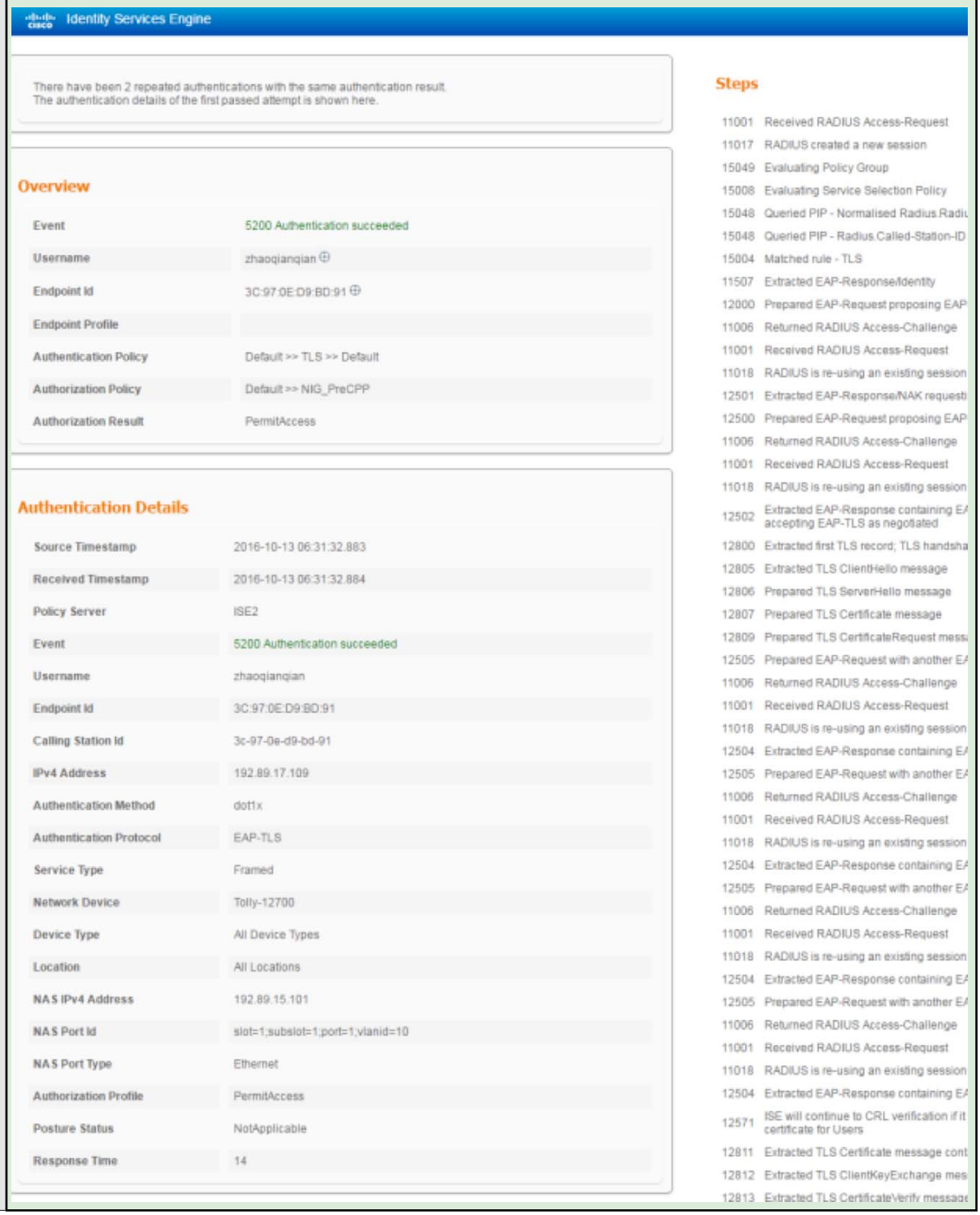
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16063  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
[Tolly_auth]
[Tolly_auth]
[Tolly_auth]dis access-user  su
[Tolly_auth]dis access-user  su
[Tolly_auth]dis access-user  us
[Tolly_auth]dis access-user  user
[Tolly_auth]dis access-user  user-id 16063

Basic:
  User ID                          : 16063
  User name                        : zhaoqianqian
  Domain-name                      : tolly
  User MAC                         : 3c97-0ed9-bd91
  User IP address                  : 192.89.17.109
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet1/1/1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/10
  User access time                 : 2016/10/13 10:40:20
  User accounting session ID       : Tolly_auth01101000000010c9abaa0003ebf
  Option82 information             : -
  User access type                 : 802.1x
  Terminal Device Type             : Data Terminal

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test Results

Authentication Details

Source Timestamp	2016-10-13 06:31:32.883
Received Timestamp	2016-10-13 06:31:32.884
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	zhaoqianqian
Endpoint Id	3C:97:0E:D9:BD:91
Calling Station Id	3c-97-0e-d9-bd-91
IPv4 Address	192.89.17.109
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1:subslot=1:port=1:vlanid=10

Test Results



Identity Services Engine

There have been 2 repeated authentications with the same authentication result.
The authentication details of the first passed attempt is shown here.

Overview

Event	5200 Authentication succeeded
Username	zhaoqianqian ⊕
Endpoint Id	3C:97:0E:D9:BD:91 ⊕
Endpoint Profile	
Authentication Policy	Default >> TLS >> Default
Authorization Policy	Default >> NIG_PreCPP
Authorization Result	PermitAccess

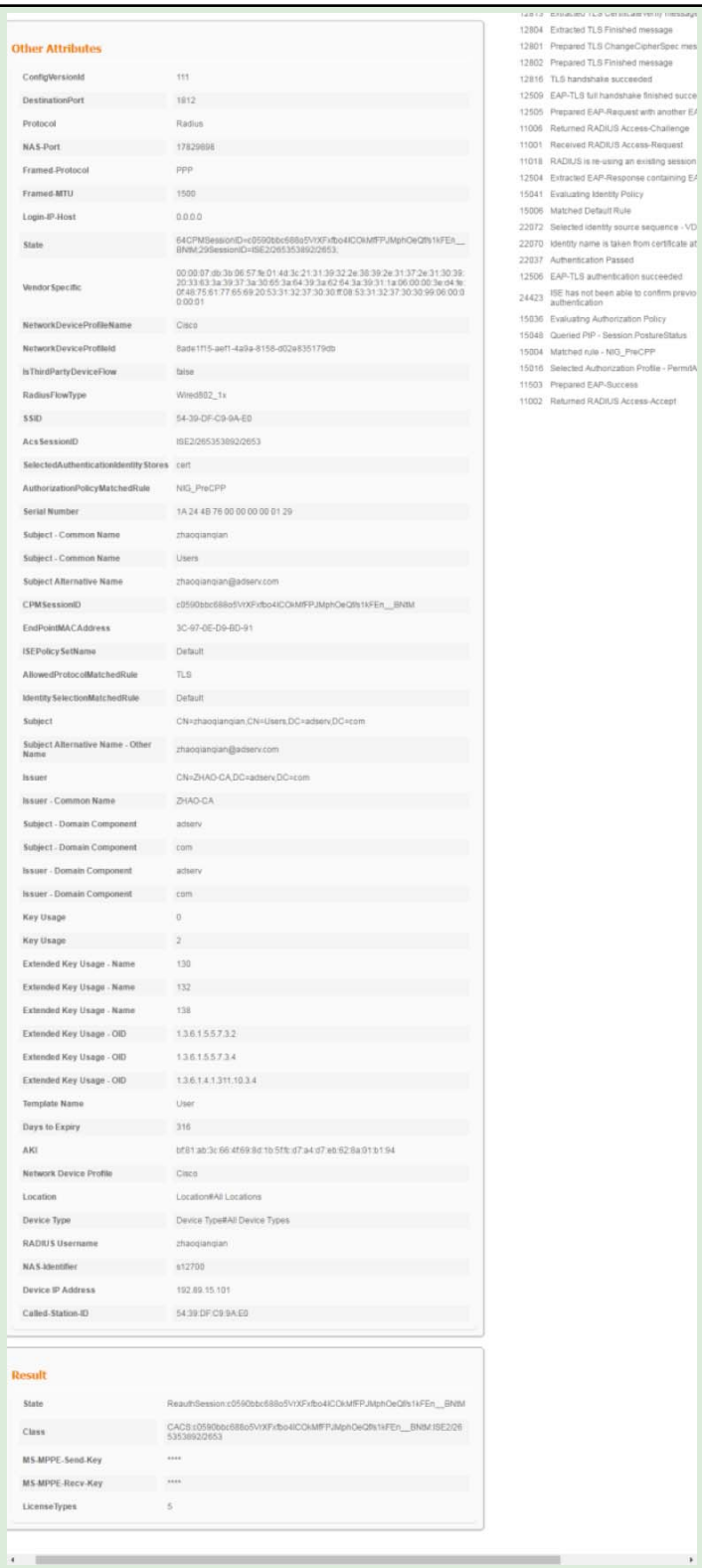
Authentication Details

Source Timestamp	2016-10-13 06:31:32.883
Received Timestamp	2016-10-13 06:31:32.884
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	zhaoqianqian
Endpoint Id	3C:97:0E:D9:BD:91
Calling Station Id	3c-97-0e-d9-bd-91
IPv4 Address	192.89.17.109
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1;subslot=1;port=1;vlanid=10
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Posture Status	NotApplicable
Response Time	14

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Normalised Radius.Radiu
15048	Queried PIP - Radius.Called-Station-ID
15004	Matched rule - TLS
11507	Extracted EAP-Response/Identity
12000	Prepared EAP-Request proposing EAP
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12501	Extracted EAP-Response/NAK requesti
12500	Prepared EAP-Request proposing EAP
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12502	Extracted EAP-Response containing E accepting EAP-TLS as negotiated
12800	Extracted first TLS record; TLS handsha
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12809	Prepared TLS CertificateRequest mess
12505	Prepared EAP-Request with another E
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing E
12505	Prepared EAP-Request with another E
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing E
12505	Prepared EAP-Request with another E
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing E
12505	Prepared EAP-Request with another E
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12504	Extracted EAP-Response containing E
12571	ISE will continue to CRL verification if it certificate for Users
12811	Extracted TLS Certificate message cont
12812	Extracted TLS ClientKeyExchange mes
12813	Extracted TLS CertificateVerify message

Test Results



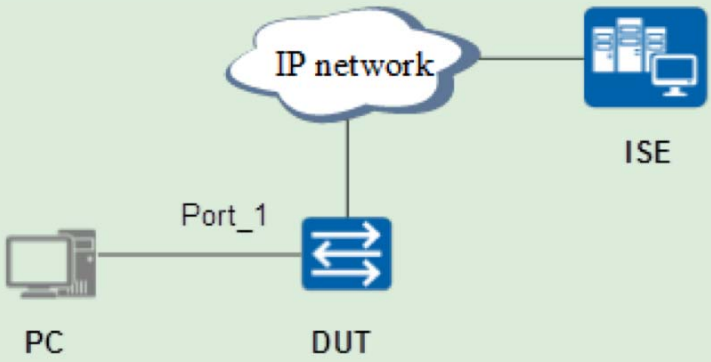
Other Attributes

ConfigVersionId	111
DestinationPort	1812
Protocol	Radius
NAS-Port	17829898
Framed-Protocol	PPP
Framed-MTU	1500
Login-IP-Host	0.0.0.0
State	64CPMSessionID=c0590bbc688a5VrXFxfbo4ICOkMfFPJMphOeQfls1kFEn__BNtM:29SessionID=ISE2/265353892/2653;
Vendor Specific	00:00:07:db:3b:06:57:fe:01:4d:3c:21:31:39:32:2e:38:39:2e:31:37:2e:31:30:39:20:33:63:3a:39:37:3a:30:65:3a:64:39:3a:62:64:3a:39:31:1a:06:00:00:3e:04:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	8ade1f15-aef1-4a9a-8158-d02e835179db
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
AcsSessionID	ISE2/265353892/2653
SelectedAuthenticationIdentityStores	cert
AuthorizationPolicyMatchedRule	NIG_PreCPP
Serial Number	1A 24 4B 76 00 00 00 00 01 29
Subject - Common Name	zhaoqianqian
Subject - Common Name	Users
Subject Alternative Name	zhaoqianqian@adserv.com
CPMSessionID	c0590bbc688a5VrXFxfbo4ICOkMfFPJMphOeQfls1kFEn__BNtM
EndPointMACAddress	3C-97-0E-D9-BD-91
ISEPolicySetName	Default
AllowedProtocolMatchedRule	TLS
IdentitySelectionMatchedRule	Default
Subject	CN=zhaoqianqian,CN=Users,DC=adserv,DC=com
Subject Alternative Name - Other Name	zhaoqianqian@adserv.com
Issuer	CN=ZHAO-CA,DC=adserv,DC=com
Issuer - Common Name	ZHAO-CA
Subject - Domain Component	adserv
Subject - Domain Component	com
Issuer - Domain Component	adserv
Issuer - Domain Component	com
Key Usage	0
Key Usage	2
Extended Key Usage - Name	130
Extended Key Usage - Name	132
Extended Key Usage - Name	138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2
Extended Key Usage - OID	1.3.6.1.5.5.7.3.4
Extended Key Usage - OID	1.3.6.1.4.1.311.10.3.4
Template Name	User
Days to Expiry	316
AKI	bf:81:ab:3c:66:4f:69:8d:1b:5f:fc:d7:a4:d7:e6:62:8a:91:b1:94
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	zhaoqianqian
NAS-Identifier	s12700
Device IP Address	192.89.15.101
Called-Station-ID	54:39:DF:C9:9A:E0

Result

State	ReauthSession:c0590bbc688a5VrXFxfbo4ICOkMfFPJMphOeQfls1kFEn__BNtM
Class	CACS:c0590bbc688a5VrXFxfbo4ICOkMfFPJMphOeQfls1kFEn__BNtM:ISE2/265353892/2653
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	5

12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec mes
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12509 EAP-TLS full handshake finished succe
12505 Prepared EAP-Request with another EA
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EA
15041 Evaluating Identity Policy
15006 Matched Default Rule
22072 Selected identity source sequence - VD
22070 Identity name is taken from certificate at
22037 Authentication Passed
12506 EAP-TLS authentication succeeded
24423 ISE has not been able to confirm previo authentication
15036 Evaluating Authorization Policy
15048 Queried PIP - Session.PostureStatus
15004 Matched rule - NIG_PreCPP
15016 Selected Authorization Profile - PermitA
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept

Test 1.5	EAP-TTLS
Objective	Verify the 802.1X authentication method with the EAP-TTLS authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as EAP. # dot1x-access-profile name tolly dot1x authentication-method eap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the EAP-TTLS mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results

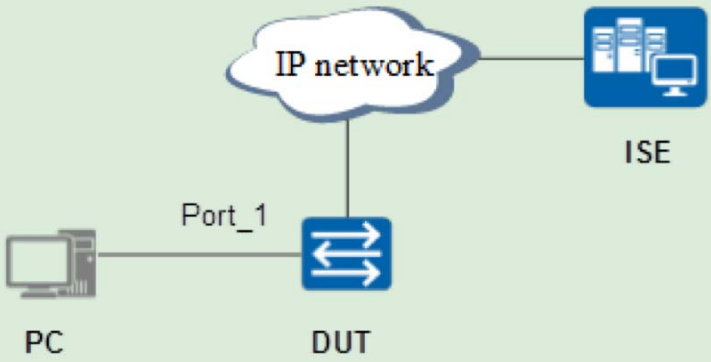
```
[Tolly_auth]dis access-user user-id 165

Basic:
  User ID                          : 165
  User name                        : zhangcong
  Domain-name                      : tolly_mac
  User MAC                         : 2400-ba06-c843
  User IP address                  : 172.168.10.246
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/1720
  User access time                 : 2016/11/03 20:48:46
  User accounting session ID       : Tolly_a0002000000172068d9fd00000a5
  Option82 information             : -
  User access type                 : 802.1x
  AP name                          : AP6010DN_SLAM
  Radio ID                         : 0
  AP MAC                           : dcd2-fc9a-8ac0
  SSID                             : tolly
  Online time                      : 46(s)
  Push URL content                 : https://172.168.10.2:8443/portal/gateway?ses
                                     sionID=aca80a02wymbotXIzs5UCtaq46ElhaGGByuXk
                                     mqIgMcMnMhrPZA&portal=0d56f8f0-6d90-11e5-978
                                     e-005056bf2f0a&action=nsp&token=bffbed3f133e
                                     73609725eec28c719cbf
  Redirect acl                     : 3001

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test Results

Authentication Policy	Default >> Dot1x-Peap >> Default
Authorization Policy	Default >> BYOD_IOS_NSP
Authorization Result	Peap_Author_NSP

Authentication Details

Source Timestamp	2016-11-03 16:08:20.962
Received Timestamp	2016-11-03 16:08:20.962
Policy Server	ise-a
Event	5200 Authentication succeeded
Username	zhangcong
User Type	User
Endpoint Id	24:00:BA:06:C8:43
Calling Station Id	24-00-ba-06-c8-43
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Employee
Authentication Method	dot1x
Authentication Protocol	EAP-TTLS (EAP-MSCHAPv2)
Service Type	Framed
Network Device	S5720HI

Test 1.6	EAP-FAST
Objective	Verify the 802.1X authentication method with the EAP-FAST authentication protocol when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure the Huawei switch 802.1X authentication mode as EAP. # dot1x-access-profile name tolly dot1x authentication-method eap # 4. Enable 802.1X authentication globally and on the interface Port_1. 5. Use the PC to initiate the 802.1X authentication in the EAP-FAST mode, and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results

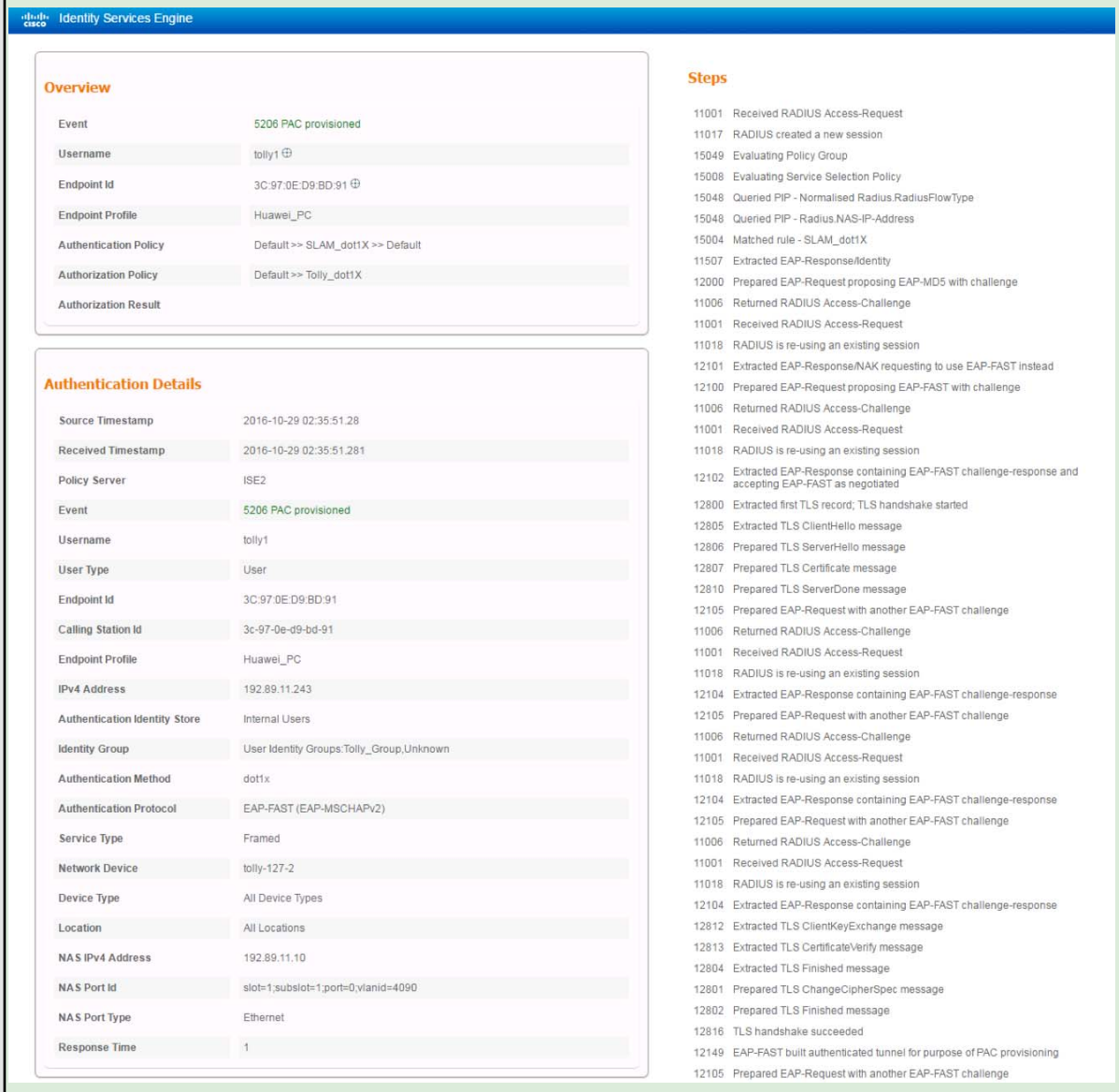
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16194  tolly1                   -                3c97-0ed9-bd91 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 16094

Basic:
  User ID                          : 16194
  User name                        : tolly1
  Domain-name                      : tolly
  User MAC                         : 0010-9410-0003
  User IP address                  : -
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : XGigabitEthernet1/0/0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/10
  User access time                 : 2016/10/14 15:46:47
  User accounting session ID       : Tolly_auth0100000000010d352bf0003ede
  Option82 information             : -
  User access type                 : 802.1x
  Terminal Device Type             : Data Terminal

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]
```

Test Results

Authentication Details

Source Timestamp	2016-10-29 02:35:51.28
Received Timestamp	2016-10-29 02:35:51.281
Policy Server	ISE2
Event	5206 PAC provisioned
Username	tolly1
User Type	User
Endpoint Id	3C:97:0E:D9:BD:91
Calling Station Id	3c-97-0e-d9-bd-91
Endpoint Profile	Huawei_PC
IPv4 Address	192.89.11.243
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group,Unknown
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	tolly-127-2
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.11.10

Test Results



Overview

Event	5206 PAC provisioned
Username	tolly1
Endpoint Id	3C:97:0E:D9:BD:91
Endpoint Profile	Huawei_PC
Authentication Policy	Default >> SLAM_dot1X >> Default
Authorization Policy	Default >> Tolly_dot1X
Authorization Result	

Authentication Details

Source Timestamp	2016-10-29 02:35:51.28
Received Timestamp	2016-10-29 02:35:51.281
Policy Server	ISE2
Event	5206 PAC provisioned
Username	tolly1
User Type	User
Endpoint Id	3C:97:0E:D9:BD:91
Calling Station Id	3c-97-0e-d9-bd-91
Endpoint Profile	Huawei_PC
IPv4 Address	192.89.11.243
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group,Unknown
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	tolly-127-2
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.11.10
NAS Port Id	slot=1;subslot=1;port=0;vlanid=4090
NAS Port Type	Ethernet
Response Time	1

Steps

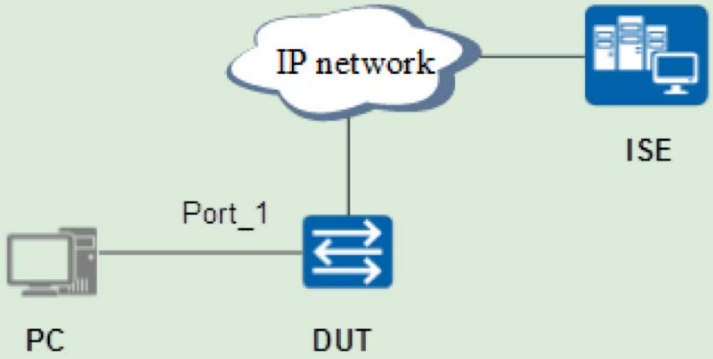
```
11001  Received RADIUS Access-Request
11017  RADIUS created a new session
15049  Evaluating Policy Group
15008  Evaluating Service Selection Policy
15048  Queried PIP - Normalised Radius.RadiusFlowType
15048  Queried PIP - Radius.NAS-IP-Address
15004  Matched rule - SLAM_dot1X
11507  Extracted EAP-Response/Identity
12000  Prepared EAP-Request proposing EAP-MD5 with challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12101  Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100  Prepared EAP-Request proposing EAP-FAST with challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12102  Extracted EAP-Response containing EAP-FAST challenge-response and
       accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
12810  Prepared TLS ServerDone message
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
12105  Prepared EAP-Request with another EAP-FAST challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12104  Extracted EAP-Response containing EAP-FAST challenge-response
12812  Extracted TLS ClientKeyExchange message
12813  Extracted TLS CertificateVerify message
12804  Extracted TLS Finished message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message
12816  TLS handshake succeeded
12149  EAP-FAST built authenticated tunnel for purpose of PAC provisioning
12105  Prepared EAP-Request with another EAP-FAST challenge
```

Test Results

Other Attributes

ConfigVersionId	81
DestinationPort	1812
Protocol	Radius
NAS-Port	17829882
Framed-Protocol	PPP
Framed-MTU	1500
Login-IP-Host	0.0.0.0
State	64CPMSessionID=c0590bbcYAHGFu5hV8PoPomYpx4i_uorIMevIUuDqBbAaWviC6g;28SessionID=ISE2/266937011/146;
Vendor Specific	00:00:07:db:3b:06:58:04:e4:c4:3c:21:31:39:32:2e:38:39:2e:31:31:2e:32:34:33:20:33:63:3a:39:37:3a:30:65:3a:64:39:3a:62:64:3a:39:31:1a:06:00:00:4a:3a:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
NetworkDeviceProfileName	NIG_HW
NetworkDeviceProfileId	01112297-aae6-4faa-9f0d-ea313a34bfe1
IsThirdPartyDeviceFlow	true
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
Acs Session ID	ISE2/266937011/146
SelectedAuthenticationIdentity Stores	Internal Users
AuthorizationPolicyMatchedRule	Tolly_dot1X
IssuedPacInfo	Issued PAC type=Tunnel V1A with expiration time: Fri Jan 27 02:35:51 2017
CPMSessionID	c0590bbcYAHGFu5hV8PoPomYpx4i_uorIMevIUuDqBbAaWviC6g
EndPointMACAddress	3C-97-0E-D9-BD-91
EapChainingResult	No chaining
ISEPolicy SetName	Default
AllowedProtocolMatchedRule	SLAM_dot1X
Identity SelectionMatchedRule	Default
HostIdentityGroup	Endpoint Identity Groups:Unknown
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	anonymous
NAS-Identifier	Tolly_auth
Device IP Address	192.89.11.10
Called-Station-ID	54:39:DF:C9:9A:E0

11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12125	EAP-FAST inner method started
11521	Prepared EAP-Request/Identity for inner EAP method
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11522	Extracted EAP-Response/Identity for inner EAP method
11806	Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041	Evaluating Identity Policy
15006	Matched Default Rule
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - tolly1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt passed
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11810	Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814	Inner EAP-MSCHAP authentication succeeded
11519	Prepared EAP-Success for inner EAP method
12128	EAP-FAST inner method finished successfully
12966	Sent EAP Intermediate Result TLV indicating success
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12126	EAP-FAST cryptobinding verification passed
12161	Cannot provision Authorization PAC when the stateless session resume is disabled
12200	Approved EAP-FAST client Tunnel PAC request
24423	ISE has not been able to confirm previous successful machine authentication
15036	Evaluating Authorization Policy
15004	Matched rule - Tolly_dot1X
15016	Selected Authorization Profile -
12964	Sent EAP Result TLV indicating success
12169	Successfully finished EAP-FAST tunnel PAC provisioning/update
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
11401	Prepared RADIUS Access-Reject after the successful in-band PAC provisioning
11504	Prepared EAP-Failure
11003	Returned RADIUS Access-Reject

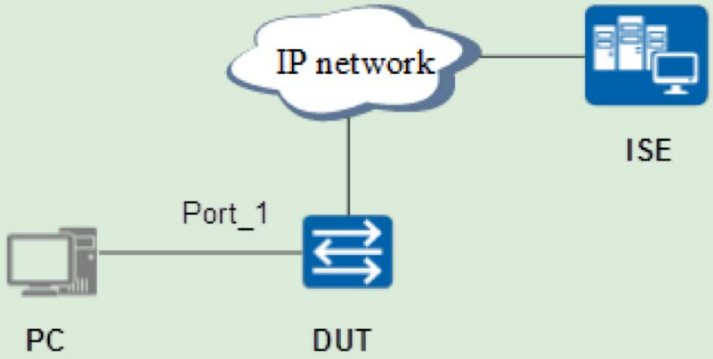
Test 2.1	Wired MAC Authentication
Objective	Verify the MAC authentication method for a wired PC when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. Add the PC's MAC address to the user list. 3. Configure the Huawei switch's MAC authentication profile. 4. Connect the PC to the Huawei S Switch and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

Test Results	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the Huawei switch 802.1X authentication mode as EAP. # radius-server template tolly_mac radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 radius-attribute set Service-Type 10 # domain tolly_mac authentication-scheme tolly authorization-scheme tolly radius-server tolly_mac # 3. Configure the aaa scheme. # aaa authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly_mac authentication-scheme tolly accounting-scheme tolly radius-server tolly_mac #

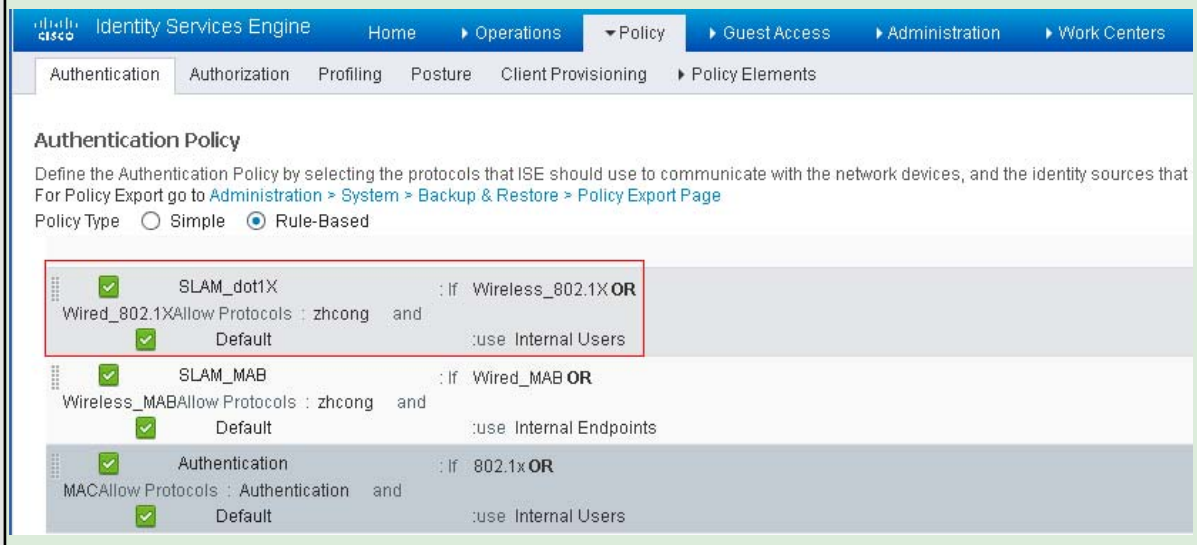
Test Results	4. Configure the MAC authentication profile on the device. # mac-access-profile name tolly mac-authen username macaddress format with-hyphen normal uppercase authentication-profile name tolly_mac mac-access-profile tolly access-domain tolly_mac # 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. # interface Vlanif4090 ip address 192.89.11.10 255.255.255.0 dhcp select interface # interface XGigabitEthernet1/0/0 port link-type hybrid port hybrid pvid vlan 4090 port hybrid untagged vlan 4090 authentication-profile tolly_mac # 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed.

Test Results

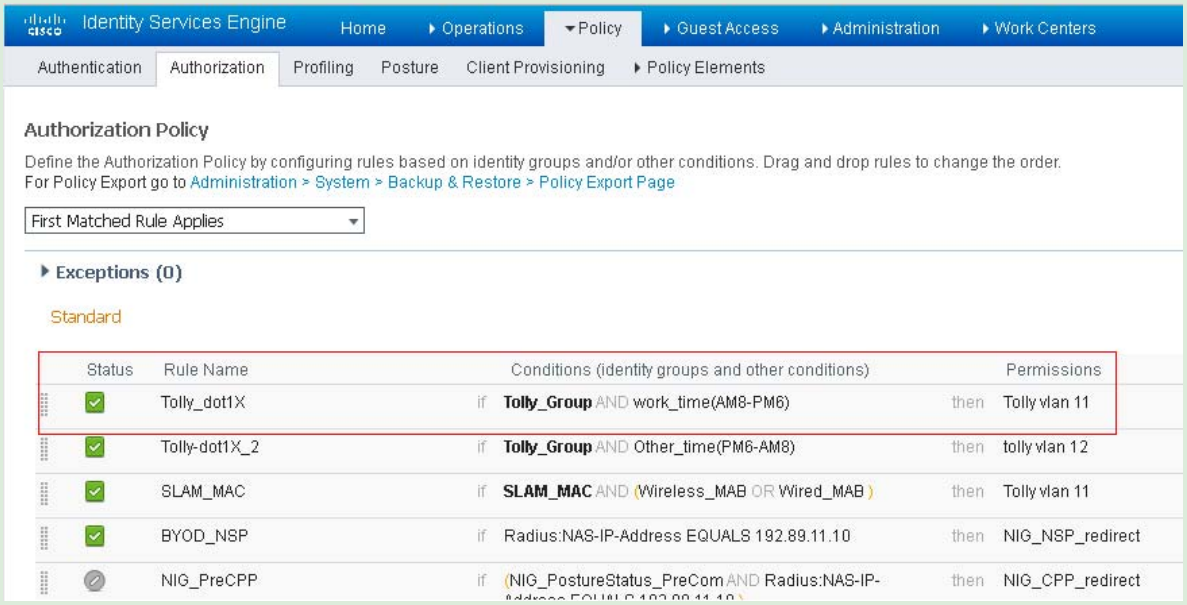
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16063  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
 16069  00-10-94-00-00-22        10.1.1.11        0010-9400-0022 Success
 ------------------------------------------------------------------------------
 Total: 3, printed: 3
[Tolly_auth]
[Tolly_auth]dis access-user user-id 16069

Basic:
  User ID                       : 16069
  User name                     : 00-10-94-00-00-22
  Domain-name                   : tolly_mac
  User MAC                      : 0010-9400-0022
  User IP address               : 10.1.1.11
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : XGigabitEthernet1/0/0
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/10
  User access time              : 2016/10/13 13:40:49
  User accounting session ID    : Tolly_auth0100000000000103f739b0003ec5
  Option82 information          : -
  User access type              : MAC
  Terminal Device Type          : Data Terminal

AAA:
  User authentication type      : MAC authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None
```

Test 2.2	Wired 802.1X Authentication
Objective	Verify the 802.1X authentication method for a wired PC when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the Huawei S switch to ensure that the Huawei switch and the Cisco ISE server communicate with each other at Layer 3. 2. Create the Cisco ISE server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. Add the PC's MAC address to the user list. 3. Configure the Huawei switch's 802.1X authentication profile. 4. Connect the PC to the Huawei S Switch and expected result 1 is displayed. 
Pass Criteria	The PC is authenticated to have network access.

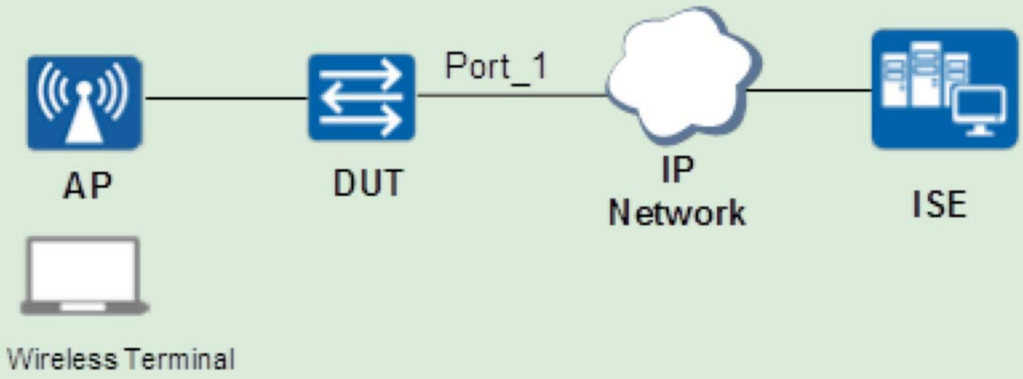
Test Results	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template tolly radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 # 3. Configure the aaa scheme. # aaa authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly authentication-scheme tolly accounting-scheme tolly radius-server tolly # 4. Configure the 802.1X authentication profile on the device. # dot1x-access-profile name tolly authentication-method eap authentication-profile name tolly dot1x-access-profile tolly access-domain tolly dot1x force #

Test Results	5. Configure the DHCP server on the device, and enable dot1x authentication on the correspondent interface. # interface Vlanif4090 ip address 192.89.6.202 255.255.255.0 dhcp select interface interface GigabitEthernet1/1/0 port link-type hybrid port hybrid pvid vlan 4090 port hybrid untagged vlan 4090 authentication-profile tolly # 6. Enter the correct user name and password on the device for authentication. Check the user address and authentication information, and expected result 1 is displayed. 

Test Results

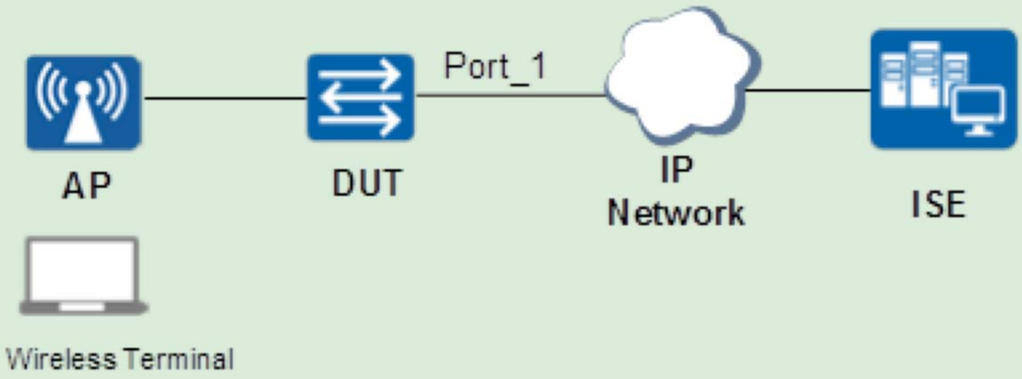



```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
 19142  tolly1                   11.1.1.252       0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user user-id 19142

Basic:
  User ID                       : 19142
  User name                     : tolly1
  Domain-name                   : tolly
  User MAC                      : 0010-9400-0011
  User IP address               : 11.1.1.252
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : XGigabitEthernet1/0/0
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/11
  User access time              : 2016/10/15 16:43:11
  User accounting session ID    : Tolly_a0100000000040901f97550004ac6
  Option82 information          : -
  User access type              : 802.1x
  Terminal Device Type          : Data Terminal
  Dynamic VLAN ID               : 11

AAA:
  User authentication type      : 802.1x authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None
```

Test 2.3	Wireless MAC Authentication
Objective	Verify the MAC authentication method for a wireless client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server profile and aaa profile on the switch. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. In the WLAN view, configure the security and SSID profiles. Bind the security and authentication profiles, service WLAN, forwarding mode, and SSID profile to the VAP profile. Configure the AP Group and bind it to the VAP profile. 7. The terminal accesses the wireless network through the SSID. Expected result 1 is displayed. 
Pass Criteria	The wireless laptop is authenticated to have network access.

Test Results

```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16302  6C-72-E7-72-DC-81        192.89.11.249    6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
<Tolly_auth>dis access-user user-id 16302

Basic:
  User ID                          : 16302
  User name                        : 6C-72-E7-72-DC-81
  Domain-name                      : tolly_mac
  User MAC                         : 6C-72-E7-72-DC-81
  User IP address                  : 192.89.11.249
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/14 16:26:53
  User accounting session ID       : Tolly_a01000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  AP name                          : AP5030DN_SLAM
  Radio                            : 1
  AP MAC                           : 1051-7214-C860
  SSID                             : tolly
  Online time                      : 27(s)
  DHCP option ID                   : 12
  DHCP option content              : Summer
  DHCP option ID                   : 55
  DHCP option content              : \001y\003\006\017w\374
  Push URL content                 : https://192.89.11.188:port/portal/gateway?se
                                     ssionId=c0590bbcD4f22QyTOuqj/h8YzPq8svV3Mf12
                                     WRRYGrO5EjEJVXO&portal=0ce17ad0-6d90-11e5-97
                                     8e-005056bf2f0a&action=cwa&token=89096284743
                                     2f0edc14a7106d568ece6
  Redict acl                       : 3001

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
```

Test 2.4	Wireless 802.1X Authentication
Objective	Verify the 802.1X authentication method for a wireless client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server profile and aaa profile on the switch. 4. Configure the aaa scheme. 5. Configure the 802.1X authentication profile on the device. 6. Configure the DHCP server on the device, and enable dot1x authentication on the correspondent interface. 7. In the WLAN view, configure the security and SSID profiles. Bind the security and authentication profiles, service WLAN, forwarding mode, and SSID profile to the VAP profile. Configure the AP Group and bind it to the VAP profile. 8. The user accesses the wireless network through the SSID, and enters the user name and password for authentication. Expected result 1 is displayed. 
Pass Criteria	The wireless laptop is authenticated to have network access.

Test Results

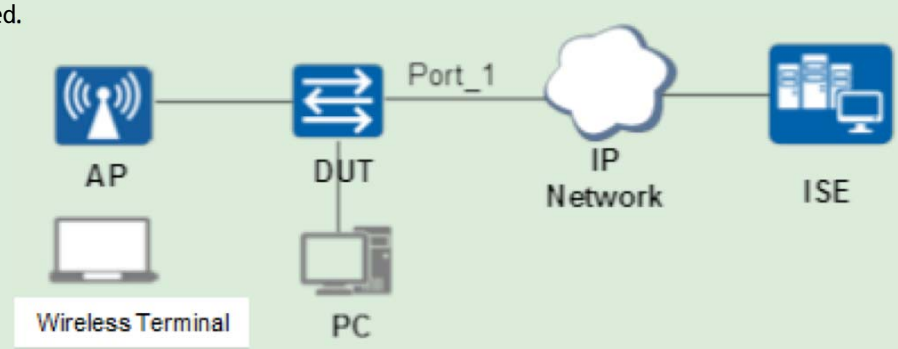
```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16304  tolly                   11.1.1.252       6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
<Tolly_auth>dis access-user user-id 16304

Basic:
  User ID                          : 16304
  User name                        : tolly
  Domain-name                      : tolly
  User MAC                         : 6C-72-E7-72-DC-81
  User IP address                  : 11.1.1.252
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/11
  User access time                 : 2016/10/14 16:30:36
  User accounting session ID       : Tolly_a01000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : 802.1x
  AP name                          : AP5030DN_SLAM
  Radio                            : 1
  AP MAC                           : 1051-7214-C860
  SSID                             : tolly
  Online time                      : 14(s)
  DHCP option ID                   : 12
  DHCP option content              : Summer
  DHCP option ID                   : 55
  DHCP option content              : \001y\003\006\017w\374
  Dynamic VLAN ID                  : 11

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test Results

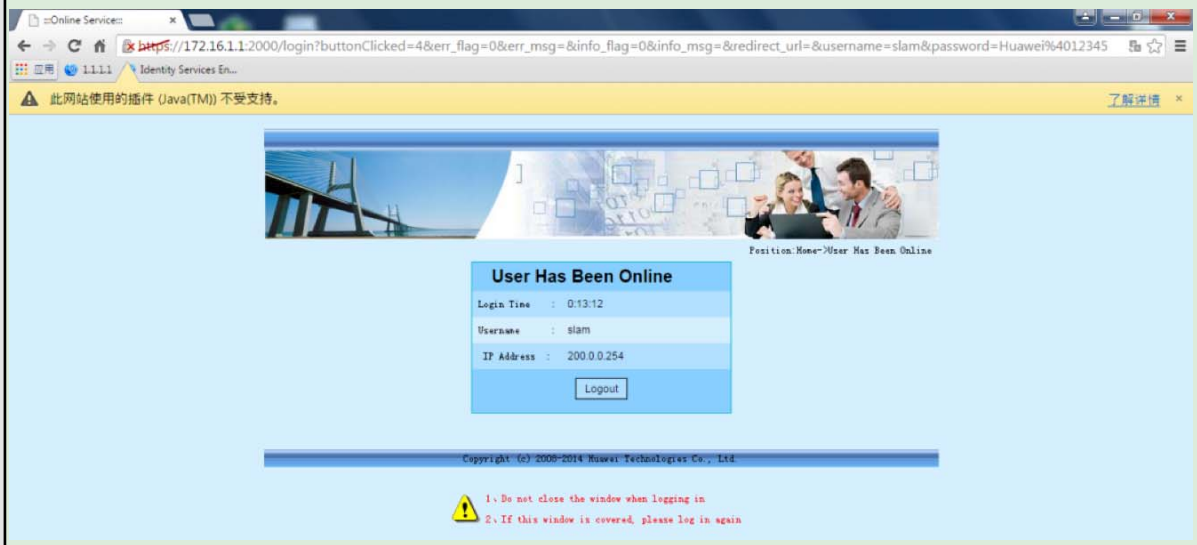
CPMSessionID	c0590bbcD4f22QyTOuqj/h8YzPq8svV3mfl2WRRYGrO5EjEJVX0
EndPointMACAddress	6C-72-E7-72-DC-81
ISEPolicySetName	Default
AllowedProtocolMatchedRule	Tolly_dot1X
IdentitySelectionMatchedRule	Default
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	tolly
NAS-Identifier	s12700
Device IP Address	192.89.11.10
Called-Station-ID	D8-49-0B-B7-DF-80:tolly

Result

State	ReauthSession:c0590bbcD4f22QyTOuqj/h8YzPq8svV3mfl2WRRYGrO5EjEJVX0
Class	CACS:c0590bbcD4f22QyTOuqj/h8YzPq8svV3mfl2WRRYGrO5EjEJVX0:ISE2/265746011/154
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 11
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	1

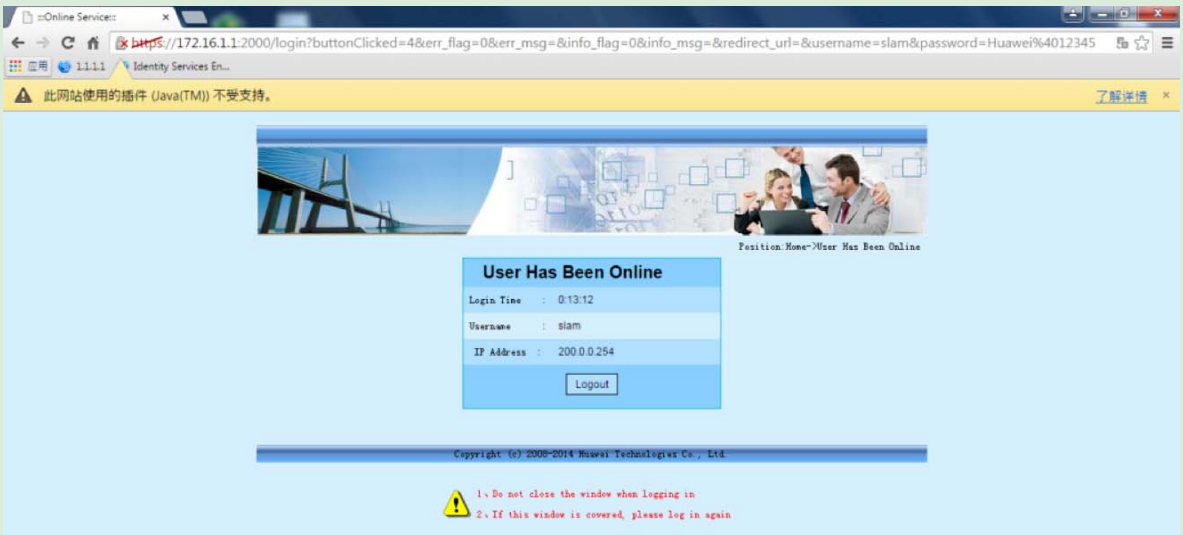
Test 2.5	Wired and Wireless Web Portal Authentication (Huawei S Switch as the Portal Server)
Objective	Verify the web portal authentication method for a wired client and a wireless client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. The web portal is hosted on the Huawei S switch.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server profile and aaa profile on the switch. 4. Configure the aaa scheme. 5. Load the ipsec.pem and ipseckey.pem certificates to the security file, and configure the ssl profile. 6. Configure the built-in Portal server on the switch, and obtain the URL address on the ISE server. 7. Configure the Portal authentication profile. 8. Configure the DHCP server on the device. 9. In the WLAN view, configure the security and SSID profiles. Bind the security and authentication profiles, service WLAN, forwarding mode, and SSID profile to the VAP profile. Configure the AP Group and bind it to the VAP profile. 10. The user accesses the wireless network through the SSID. Open a webpage and enter any address in the address bar. Expected result 1 is displayed. 11. Configure the Portal authentication profile on the correspondent interface. The user accesses the network in wired mode. Open a webpage and enter any address in the address bar on the PC. Expected result 1 is displayed. 
Pass Criteria	The wired PC and the wireless laptop are both authenticated to have network access.

Test Results

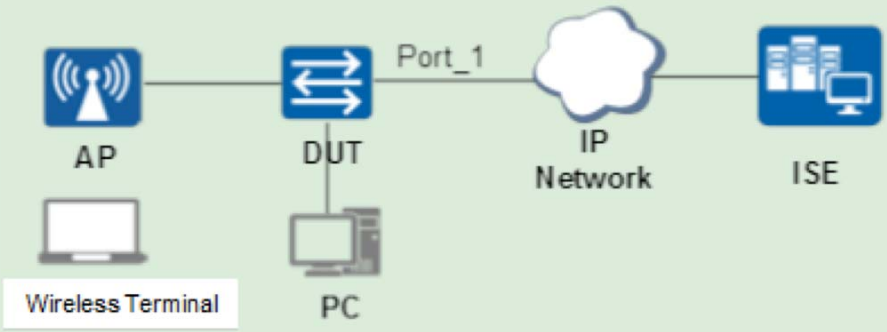



```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 111  slam                       200.0.0.246      b853-ac75-c38f Success
 112  6C-72-E7-72-DC-81          200.0.0.253      6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
<Tolly_auth>dis access-user user-id 111

Basic:
  User ID                       : 111
  User name                     : slam
  Domain-name                   : slam_ise
  User MAC                      : b853-ac75-c38f
  User IP address               : 200.0.0.246
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : Wlan-Dbss1
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/200
  User access time              : 2001/11/02 02:15:01
  User accounting session ID    : Tolly_a01000000004090a8741d0004acd
  Option82 information          : -
  User access type              : WEB
  AP name                       : AP5030DN_SLAM
  Radio                         : 1
  AP MAC                        : 1051-7214-C860
  SSID                          : SSID_Cisco_ISE
  Online time                   : 80(s)
  Web-server IP address         : 172.16.1.1

AAA:
  User authentication type      : WEB authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : RADIUS
```

Test Results




```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 41     slam                     200.0.0.252      f0de-f1e0-aeb2 Success
 42     b853ac75c38f             200.0.0.251      b853-ac75-c38f Pre-authen
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user u
[Tolly_auth]dis access-user user-id 41

Basic:
  User ID                       : 41
  User name                     : slam
  Domain-name                   : slam_ise
  User MAC                      : f0de-f1e0-aeb2
  User IP address               : 200.0.0.252
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : GigabitEthernet0/0/19
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/200
  User access time              : 2001/11/03 18:37:40
  User accounting session ID    : Tolly_a00019000000200a75e750000029
  Option82 information          : -
  User access type              : WEB
  Terminal Device Type          : Data Terminal
  Web-server IP address         : 172.16.1.1

AAA:
  User authentication type      : WEB authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : RADIUS
```

Test 2.6	Wired and Wireless Web Portal Authentication (Cisco ISE Server as the Portal Server)
Objective	Verify the web portal authentication method for a wired client and a wireless client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. The web portal is hosted on the Cisco ISE server.
Procedure	1. All devices are working properly. The test environment has been set up according to the networking diagram. 2. Related configuration has been completed on the ISE authentication server. 3. Configure the switch's IP address so that the switch can communicate with the ISE server. 4. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 5. Configure the RADIUS server on the switch. 6. Configure the aaa profile. 7. Configure the MAC authentication profile. 8. Configure the CoA authorization server. 9. Configure the ACL redirection on the switch. 10. Users access the network in wired mode for MAC authentication. Expected result 1 is displayed. 11. Open a web page and access any website. Enter the user name and password for authentication. Expected result 2 is displayed. 
Pass Criteria	1. When the user accesses the network for MAC authentication, the server delivers URL and redirection ACL. Open a browser and enter any IP address in the address bar, the page is redirected to the Portal authentication page. 2. After entering the user name and password, the user passes the Portal authentication successfully.

Test Results

```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16305  F0-DE-F1-E0-AE-B2        192.89.11.248    f0de-f1e0-aeb2 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1

<Tolly_auth>dis access-user user-id 16305

Basic:
  User ID                          : 16305
  User name                        : F0-DE-F1-E0-AE-B2
  Domain-name                      : tolly_mac
  User MAC                         : f0de-f1e0-aeb2
  User IP address                  : 192.89.11.248
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet0/0/4
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/28 16:10:46
  User accounting session ID       : Tolly_a0100000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  Push URL content                 : https://192.89.11.188:8443/portal/gateway?se
                                     ssionId=c0590bbct6OyL70wsnEHgXOlbGavZyRTs2IE
                                     _fzxbif8zL_uEmk&portal=0ce17ad0-6d90-11e5-97
                                     8e-005056bf2f0a&action=cwa&token=20558beb1f5
                                     6e1ac449017966929fe40
  Terminal Device Type             : Data Terminal
  Redirect acl                     : 3001

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test Results

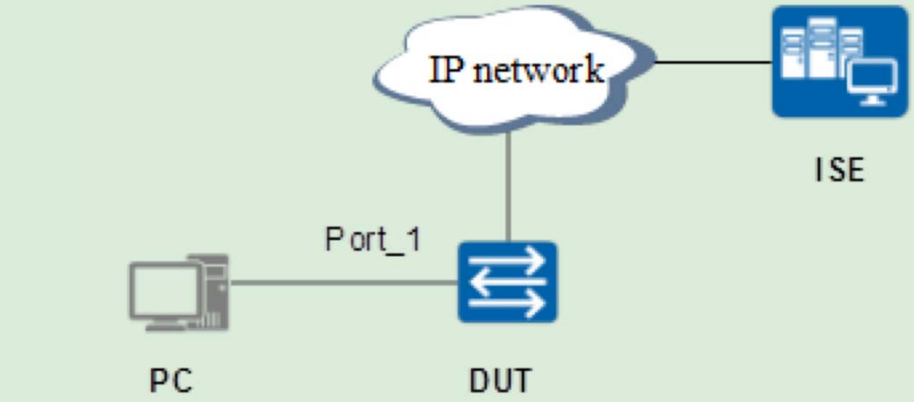
```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16306  tolly                    192.89.11.248    f0de-f1e0-aeb2 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1

<Tolly_auth>dis access-user user-id 16306

Basic:
  User ID                          : 16306
  User name                        : tolly
  Domain-name                      : tolly_mac
  User MAC                         : f0de-f1e0-aeb2
  User IP address                  : 192.89.11.248
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet0/0/4
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/28 16:10:46
  User accounting session ID       : Tolly_a0100000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  Terminal Device Type             : Data Terminal

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test Results

```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16302  6C-72-E7-72-DC-81       192.89.11.249    6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
<Tolly_auth>dis access-user user-id 16302

Basic:
  User ID                          : 16302
  User name                        : 6C-72-E7-72-DC-81
  Domain-name                      : tolly_mac
  User MAC                         : 6C-72-E7-72-DC-81
  User IP address                  : 192.89.11.249
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/14 16:26:53
  User accounting session ID       : Tolly_a01000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  AP name                          : AP5030DN_SLAM
  Radio                            : 1
  AP MAC                           : 1051-7214-C860
  SSID                             : tolly
  Online time                      : 27(s)
  DHCP option ID                   : 12
  DHCP option content              : Summer
  DHCP option ID                   : 55
  DHCP option content              : \001y\003\006\017w\374
  Push URL content                 : https://192.89.11.188:port/portal/gateway?se
                                     ssionId=c0590bbcD4f22QyTOuqj/h8YzPq8svV3Mf12
                                     WRRYGrO5EjEJVXO&portal=0ce17ad0-6d90-11e5-97
                                     8e-005056bf2f0a&action=cwa&token=89096284743
                                     2f0edc14a7106d568ece6
  Redict acl                       : 3001

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
```

Test Results

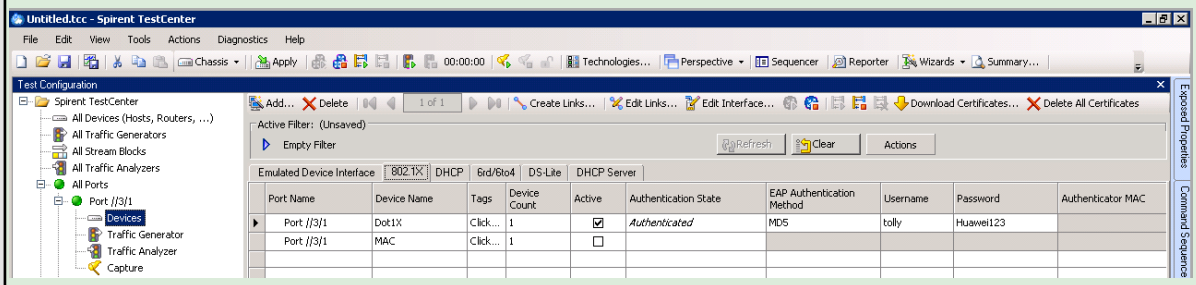
```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                  IP address       MAC            Status
 ------------------------------------------------------------------------------
 16303  tolly                     192.89.11.249    6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
<Tolly_auth>dis access-user user-id 16303

Basic:
  User ID                          : 16303
  User name                        : tolly
  Domain-name                      : tolly_mac
  User MAC                         : 6c72-e772-dc81
  User IP address                  : 192.89.11.249
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2001/11/02 02:16:01
  User accounting session ID       : Tolly_a01000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  AP name                          : AP5030DN_SLAM
  Radio                            : 1
  AP MAC                           : 1051-7214-C860
  SSID                             : SSID_Cisco_ISE
  Online time                      : 14(s)
  DHCP option ID                   : 12
  DHCP option content              : Summer
  DHCP option ID                   : 55
  DHCP option content              : \001y\003\006\017w\374

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

Test 2.7	Wired Mixed Authentication
Objective	Verify the mixed MAC and 802.1X authentication methods for a wired client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. The web portal is hosted on the Cisco ISE server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the MAC authentication and dot1x authentication profiles on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. Use the tester interface as the user terminal to connect to the DUT and enable the MAC-authenticated and 802.1X-authenticated ports. Expected result 1 is displayed  Simulated by Spirent TestCenter
Pass Criteria	Create two device users on the Spirent TestCenter interface for MAC authentication and 802.1X authentication respectively. After passing the authentication, the user obtains the IP address. The device shows that the authentication succeeds.

Test Results	Configuration Steps: 1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template tolly radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 # radius-server template tolly_mac radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 radius-attribute set Service-Type 10 # domain tolly_mac authentication-scheme tolly authorization-scheme tolly radius-server tolly_mac #

Test Results	3. Configure the aaa scheme. # aaa authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly_mac authentication-scheme tolly accounting-scheme tolly radius-server tolly_mac domain tolly authentication-scheme tolly accounting-scheme tolly radius-server tolly # 4. Configure the MAC authentication and dot1x authentication profiles on the device. # mac-access-profile name tolly mac-authen username macaddress format with-hyphen normal uppercase dot1x-access-profile name tolly authentication-method eap dot1x-access-profile tolly mac-access-profile tolly access-domain tolly dot1x force access-domain tolly_mac mac-authen force access-domain tolly force #

Test Results	5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. # interface Vlanif4090 ip address 192.89.11.10 255.255.255.0 dhcp select interface # interface XGigabitEthernet1/0/0 port link-type hybrid port hybrid pvid vlan 4090 port hybrid untagged vlan 4090 authentication-profile tolly # 6. Use the tester interface as the user terminal to connect to the DUT and enable the MAC-authenticated and 802.1X-authenticated ports. Expected result 1 is displayed Results: Create two device users on the tester interface for MAC authentication and 802.1X authentication respectively. After passing the authentication, the user obtains the IP address. The device shows that the authentication succeeds.

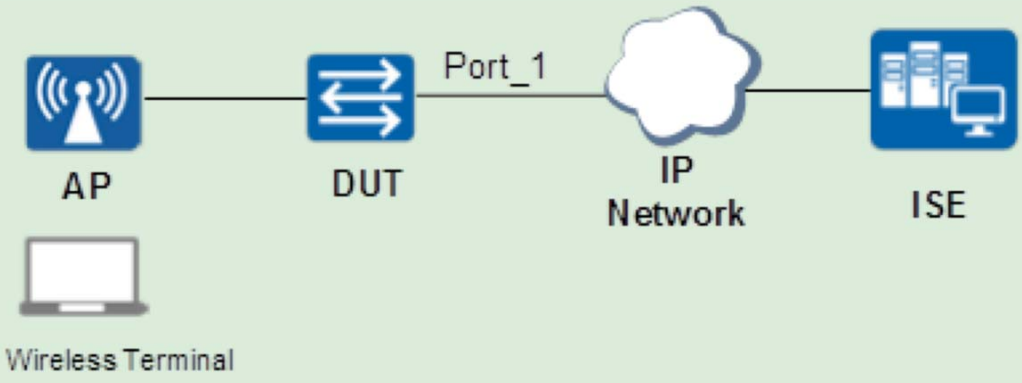



```
[Tolly_auth]dis access-user
--------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
--------------------------------------------------------------------------------
16080  00-10-94-00-00-22        10.1.1.11        0010-9400-0022 Success
16081  tolly                    -                0010-9410-0003 Success
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Test Results

```
[Tolly_auth-XGigabitEthernet1/0/0]di th
#
interface XGigabitEthernet1/0/0
 port link-type hybrid
 port hybrid pvid vlan 4090
 port hybrid untagged vlan 4090
 authentication-profile tolly
#
```

```
[Tolly_auth-authen-profile-tolly]di th
#
authentication-profile name tolly
 dot1x-access-profile tolly
 mac-access-profile tolly
 access-domain tolly dot1x force
 access-domain tolly_mac mac-authen force
 access-domain tolly force
 authentication event authen-fail action authorize vlan 10
#
```

Test 2.7	Wireless Mixed Authentication
Objective	Verify the mixed MAC and Web Portal authentication methods for a wired client when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. The web portal is hosted on the Cisco ISE server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server profile and aaa profile on the switch. 4. Configure the MAC authentication and Portal authentication profiles on the device. 5. Configure the DHCP server on the device, and enable combined MAC authentication and Portal authentication on the correspondent interface. 6. In the WLAN view, configure the security and SSID profiles. Bind the security and authentication profiles, service WLAN, forwarding mode, and SSID profile to the VAP profile. Configure the AP Group and bind it to the VAP profile. 7. The wireless terminal accesses the network through the SSID for MAC authentication. Expected result 1 is displayed. 8. For users who fail to pass the MAC authentication, allow them to perform the Portal authentication. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The user opens the browser and enters any IP address for Portal authentication. Enter the user name and password, and the device shows that the authentication succeeds.

Test Results

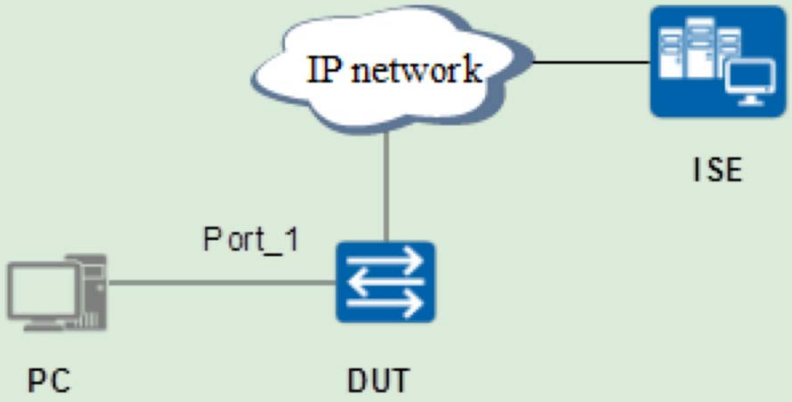
1. The user goes online for MAC authentication, and obtains the correspondent VLAN address.

```
<Tolly_auth>dis access-user user-id 112

Basic:
  User ID                          : 112
  User name                        : 6C-72-E7-72-DC-81
  Domain-name                      : slam_ise
  User MAC                         : 6c72-e772-dc81
  User IP address                  : 200.0.0.253
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : Wlan-Dbss1
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/200
  User access time                 : 2001/11/02 02:16:01
  User accounting session ID       : Tolly_a01000000004090a8741d0004acd
  Option82 information             : -
  User access type                 : MAC
  AP name                          : AP5030DN_SLAM
  Radio                            : 1
  AP MAC                           : 1051-7214-C860
  SSID                             : SSID_Cisco_ISE
  Online time                      : 57(s)

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : RADIUS
```

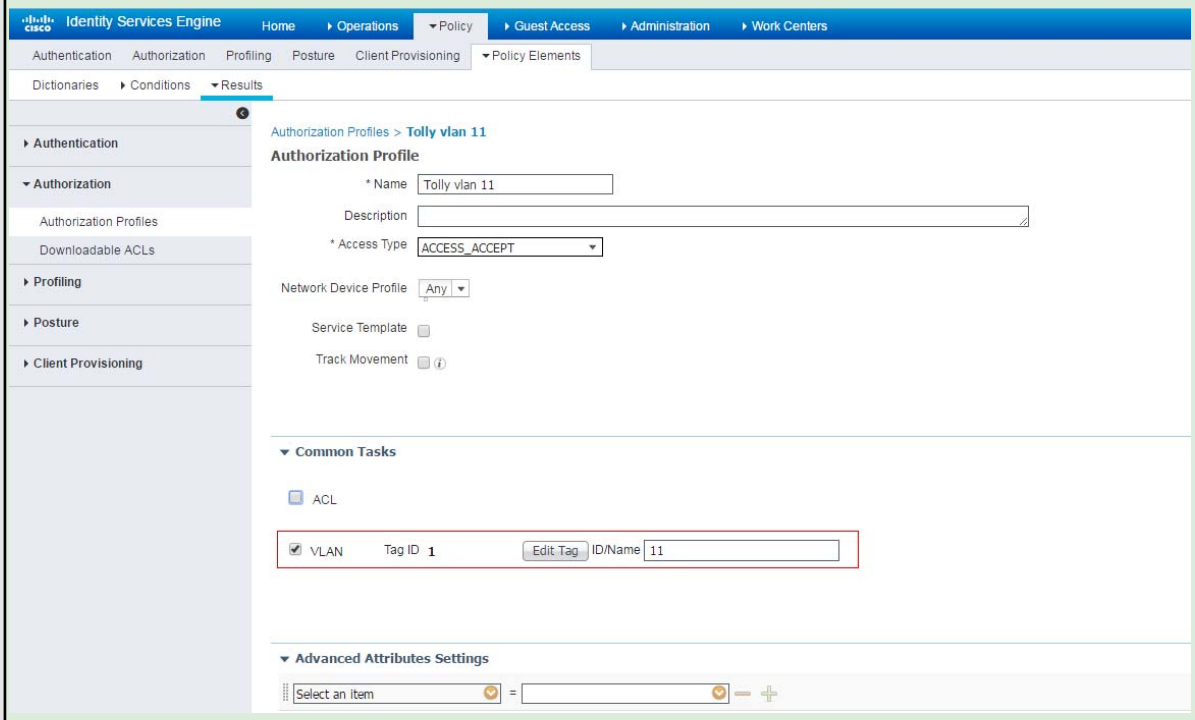
Test Results

2. The user goes online for Portal authentication, and obtains the correspondent VLAN address.

```
<Tolly_auth>dis access-user
 ------------------------------------------------------------------------------
 UserID Username                  IP address       MAC            Status
 ------------------------------------------------------------------------------
 111  slam                      200.0.0.246      b853-ac75-c38f Success
 112  6C-72-E7-72-DC-81         200.0.0.253      6c72-e772-dc81 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
<Tolly_auth>dis access-user user-id 111

Basic:
  User ID                           : 111
  User name                         : slam
  Domain-name                       : slam_ise
  User MAC                          : b853-ac75-c38f
  User IP address                   : 200.0.0.246
  User vpn-instance                 : -
  User IPv6 address                 : -
  User access Interface             : Wlan-Dbss1
  User vlan event                   : Success
  QinQVlan/UserVlan                 : 0/200
  User access time                  : 2001/11/02 02:15:01
  User accounting session ID        : Tolly_a01000000004090a8741d0004acd
  Option82 information              : -
  User access type                  : WEB
  AP name                           : AP5030DN_SLAM
  Radio                             : 1
  AP MAC                            : 1051-7214-C860
  SSID                              : SSID_Cisco_ISE
  Online time                       : 80(s)
  Web-server IP address             : 172.16.1.1

AAA:
  User authentication type          : WEB authentication
  Current authentication method     : RADIUS
  Current authorization method      : -
  Current accounting method         : RADIUS
```

Test 3.1	Built-in Authentication Attribute: Dynamic VLAN
Objective	Verify the built-in authentication attribute Dynamic VLAN when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Configure the authorization policy on the ISE server: Deliver the dynamic VLAN11. Create VLAN11 on the device, and configure VLANIF11 as the DHCP IP address pool. 5. Use the PC to initiate the 802.1X authentication, and expected result 1 is displayed. 
Pass Criteria	The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. Dynamic VLAN11 and IP address can be obtained.

Test Results	1. Configure the dynamic VLAN11 authorization in the ISE server authorization policy.



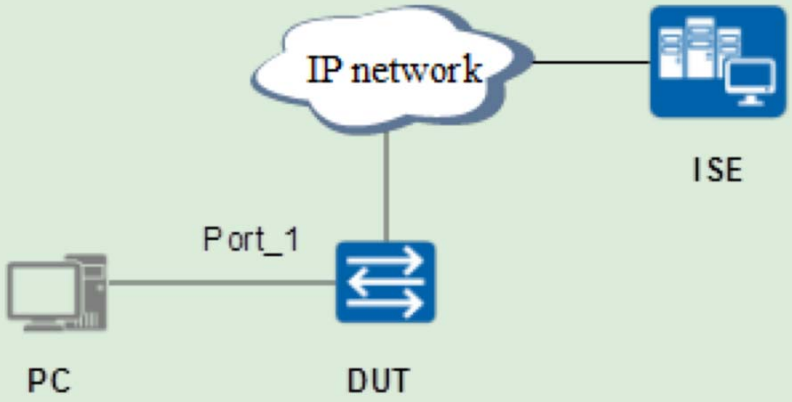
Test Results

2. Create VLAN11 on the device. The device goes online after passing the authentication successfully, and obtains the dynamic VLAN11.

```
[Tolly_auth-Vlanif11]di th
#
interface Vlanif11
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
return
[Tolly_auth-Vlanif11]ip pool vlan11
[Tolly_auth-ip-pool-vlan11]di th
#
ip pool vlan11
 gateway-list 11.1.1.1
 network 11.1.1.0 mask 255.255.255.0
 dns-list 11.1.1.1
#
```

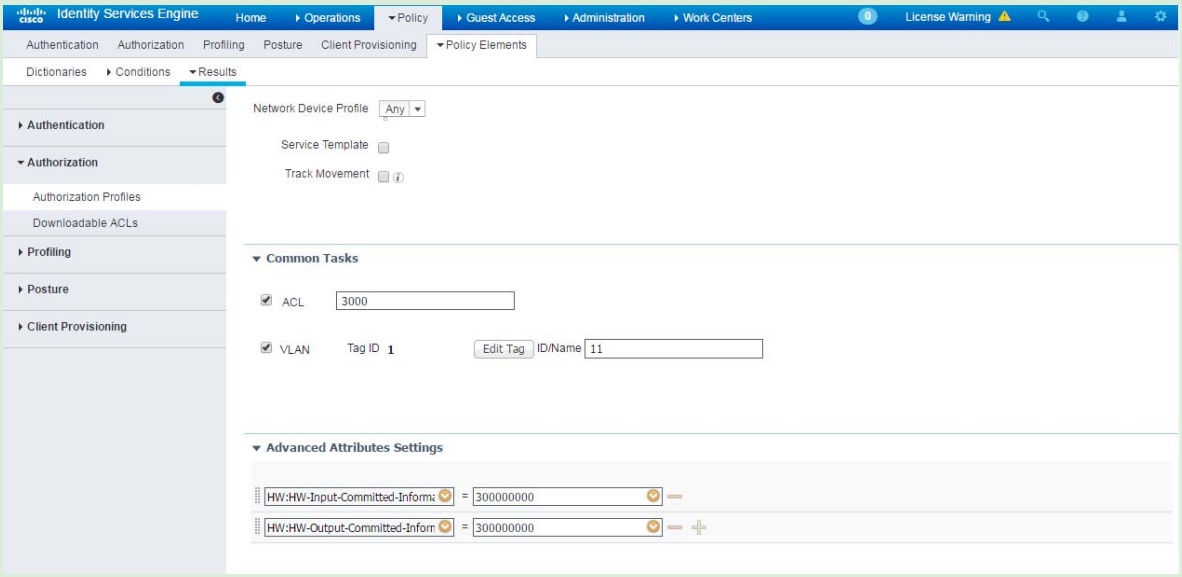
```
[Tolly_auth]dis access-user
--------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
--------------------------------------------------------------------------------
19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
19141  tolly1                   11.1.1.252       0010-9400-0011 Success
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

```
[Tolly_auth]dis access-user
--------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
--------------------------------------------------------------------------------
19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
19142  tolly1                   11.1.1.252       0010-9400-0011 Success
--------------------------------------------------------------------------------
Total: 2, printed: 2
[Tolly_auth]dis access-user user-id 19142

Basic:
  User ID                       : 19142
  User name                     : tolly1
  Domain-name                   : tolly
  User MAC                      : 0010-9400-0011
  User IP address               : 11.1.1.252
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : XGigabitEthernet1/0/0
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/11
  User access time              : 2016/10/15 16:43:11
  User accounting session ID    : Tolly_a0100000000040901f97550004ac6
  Option82 information          : -
  User access type              : 802.1x
  Terminal Device Type          : Data Terminal
  Dynamic VLAN ID               : 11

AAA:
  User authentication type      : 802.1x authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None
```

Test 3.2	Built-in Authentication Attribute: Dynamic ACL
Objective	Verify the built-in authentication attribute Dynamic ACL when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Configure the ACL 3000 authorization on the ISE server, and configure the correspondent ACL 3000 description 3000.in on the device. 5. Use the PC to initiate the 802.1X authentication, and expected result 1 is displayed. 6. Use the tester to send packets to the destination address 100.1.1.10, and expected result 2 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. Result 2: The tester sends packets to the destination address 100.1.1.10, and the traffic is denied.

Test Results

1. Configure the ACL 3000 dynamic authorization in the ISE server authorization policy.



2. Configure the ACL 3000 on the device.

```
[Tolly_auth-acl-adv-3000]di th
#
acl number 3000
 description 3000.in
 rule 5 deny ip destination 100.1.1.10 0
#
return
[Tolly auth-acl-adv-3000]_
```

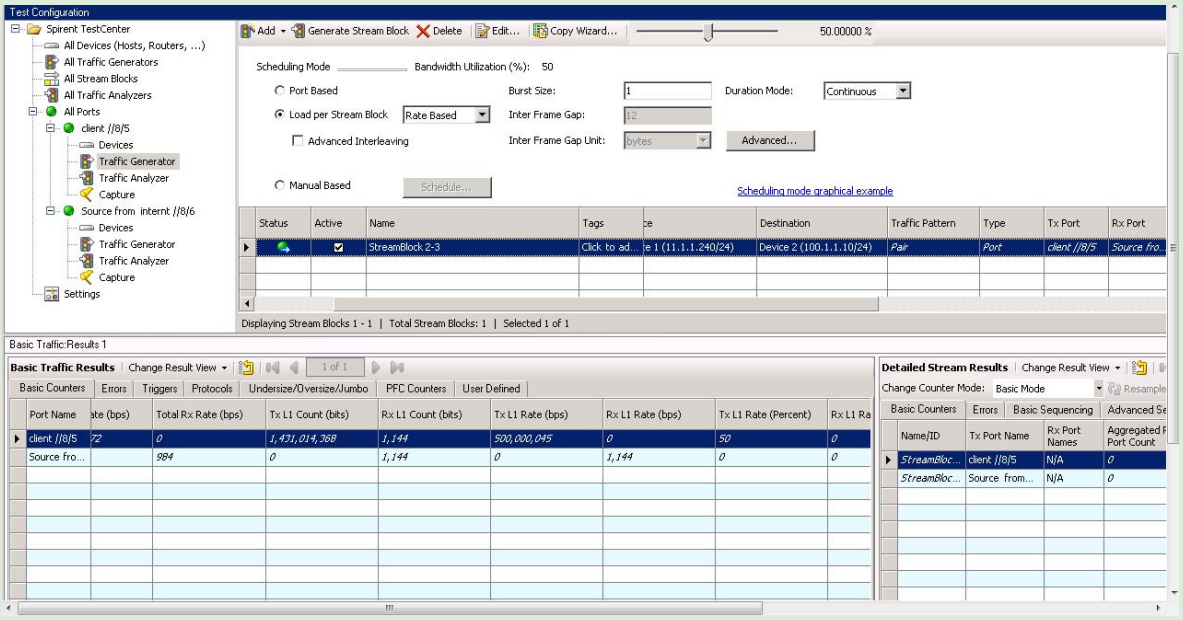
Test Results

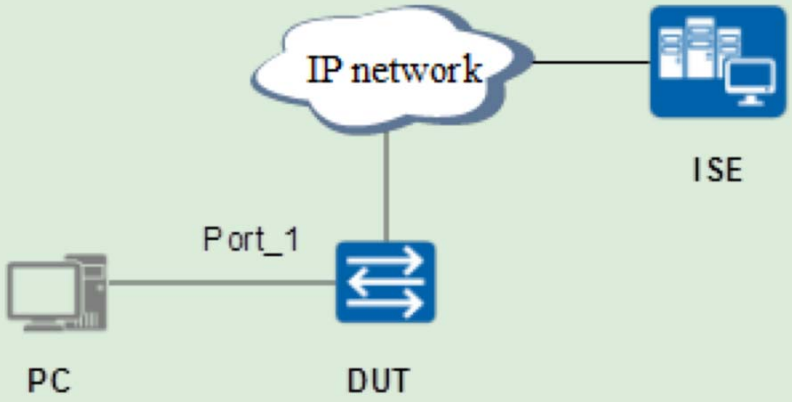
3. The device goes online after passing the authentication successfully, and obtains the dynamic ACL.

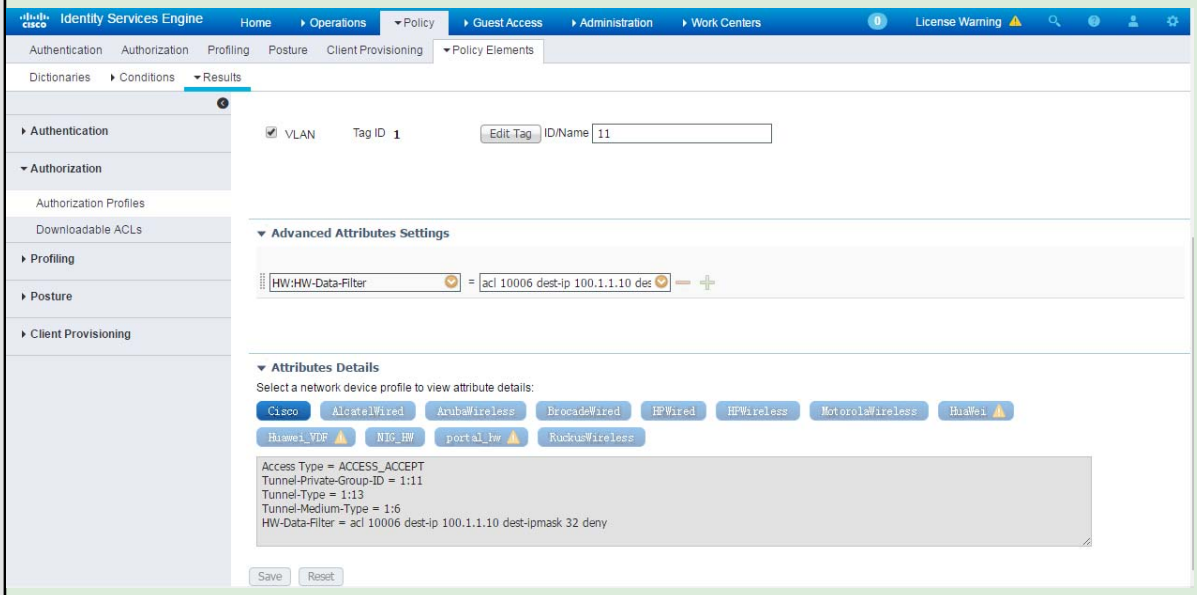
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16027  F0-DE-F1-E0-AE-B2       192.89.11.253    f0de-f1e0-aeb2 Success
 16028  tolly1                  -                0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 16028

Basic:
  User ID                          : 16027
  User name                        : tolly1
  Domain-name                      : tolly
  User MAC                         : 0010-9400-0011
  User IP address                  : -
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : XGigabitEthernet1/0/0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/11
  User access time                 : 2016/10/13 16:23:36
  User accounting session ID       : Tolly_a01000000004090cb7e280004ac4
  Option82 information             : -
  User access type                 : 802.1x
  Terminal Device Type             : Data Terminal
  Dynamic VLAN ID                  : 11
  Dynamic ACL number(Effective)    : 3000

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]
```

Test Results

4. The tester sends packets to the destination address 100.1.1.10, and the traffic is denied.



Test 3.3	Huawei Authentication Attribute: Dynamic ACL Rule
Objective	Verify the Huawei authentication attribute Dynamic ACL Rule when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. Huawei attributes can be imported to the Cisco ISE server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Configure the DACL authorization on the ISE server. 5. Use the PC to initiate the 802.1X authentication, and expected result 1 is displayed. 6. Use the tester to send packets to the destination address 100.1.1.10, and expected result 2 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. Result 2: The tester sends packets to the destination address 100.1.1.10, and the traffic is denied.

Test Results	1. Configure the DACL dynamic authorization in the ISE server authorization policy. 

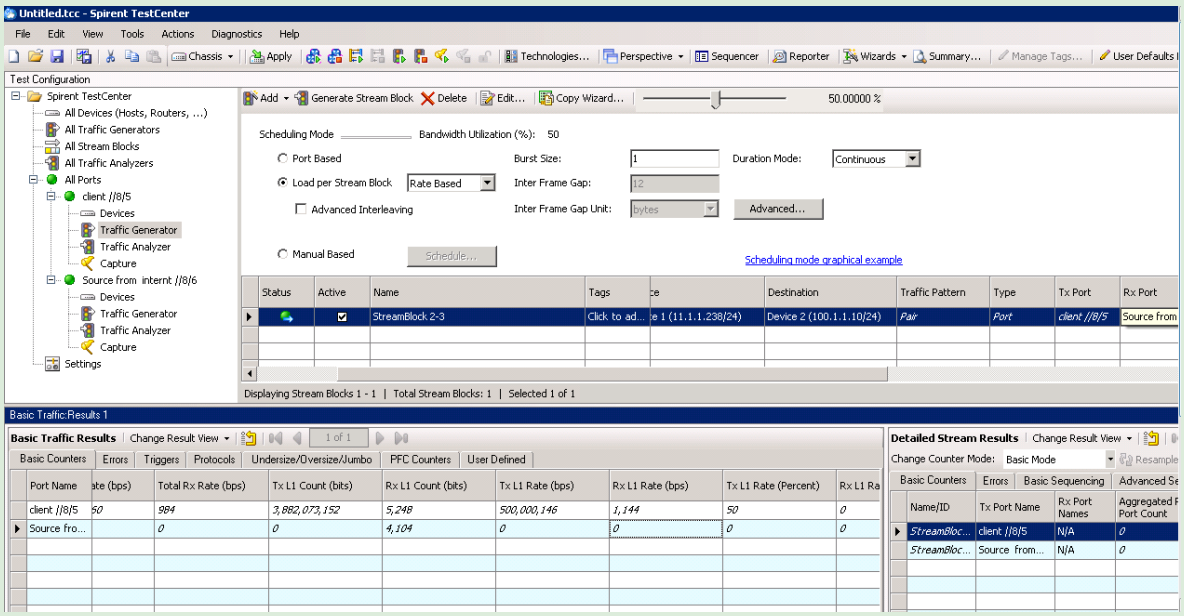
Test Results

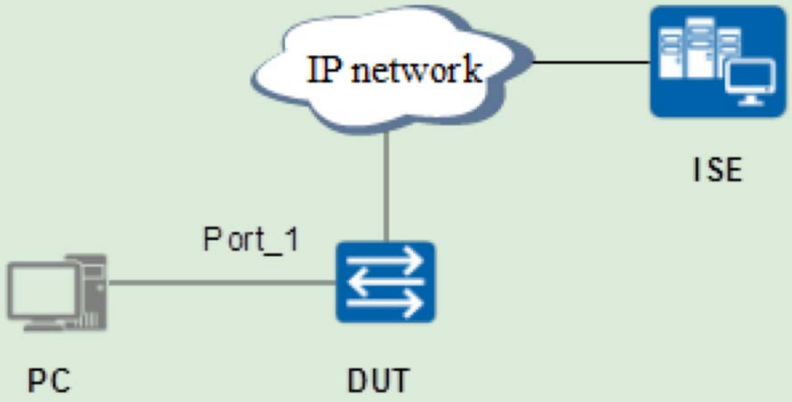
2. The device goes online after passing the authentication successfully, and obtains the dynamic DACL.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
 19143  tolly1                   11.1.1.251       0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]
[Tolly_auth]dis access-user user-id 19143

Basic:
  User ID                       : 19143
  User name                     : tolly1
  Domain-name                   : tolly
  User MAC                      : 0010-9400-0011
  User IP address               : 11.1.1.251
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : XGigabitEthernet1/0/0
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/11
  User access time              : 2016/10/15 17:02:21
  User accounting session ID    : Tolly_a0100000000409010a2e10004ac7
  Option82 information          : -
  User access type              : 802.1x
  Terminal Device Type          : Data Terminal
  Dynamic VLAN ID               : 11
  Dynamic ACL desc(Effective)   :
   No. 0: acl 10006 dest-ip 100.1.1.10 dest-ipmask 32 deny

AAA:
  User authentication type      : 802.1x authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None

[Tolly_auth]
```

Test Results

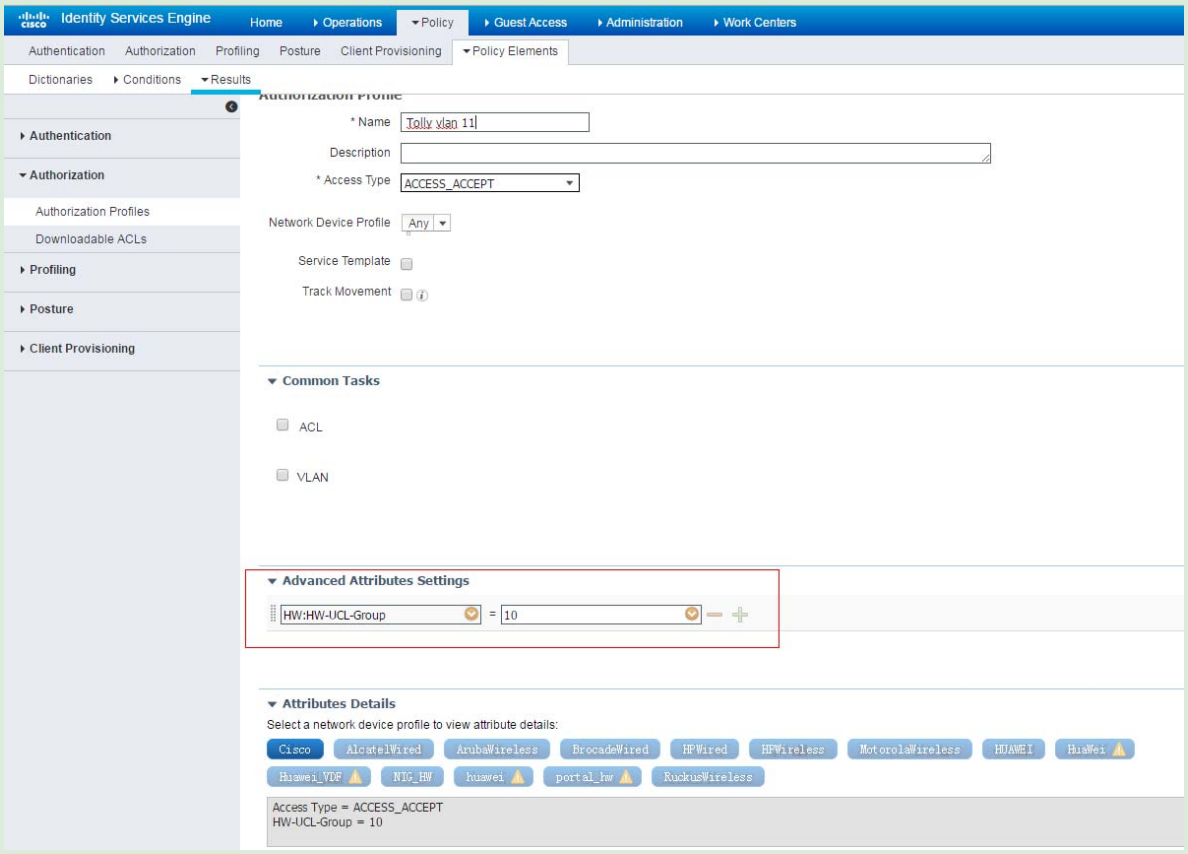
3. The tester sends packets to the destination address 100.1.1.10, and the traffic is denied.



Test 3.4	Huawei Authentication Attribute: Dynamic UCL Group
Objective	Verify the Huawei authentication attribute Dynamic UCL Group when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. Huawei attributes can be imported to the Cisco ISE server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Configure the UCL-group 10 authorization on the ISE server, and create UCL-group 10 on the device. Create and bind ACL 6000 to UCL-group 10. 5. Use the tester as a host to initiate the 802.1X authentication, and expected result 1 is displayed. 6. Use the tester to send traffic that matches ACL6000, and expected result 2 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. The device can obtain the UCL-group 10. Result 2: The tester sends traffic that matches ACL6000, and the traffic is denied.

Test Results

1. Configure the UCL-group 10 dynamic authorization in the ISE server authorization policy.



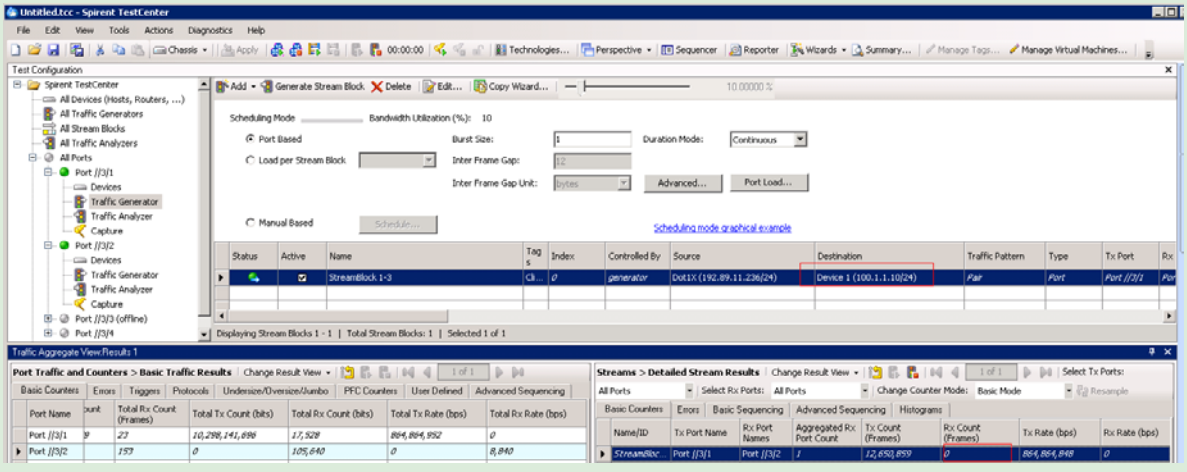
Test Results	2. Configure UCL-group 10 on the device. Create ACL 6000, bind it to UCL-group 10, and apply it.
	`[Tolly_auth]ucl-group 10 name tolly`
	`[Tolly_auth]acl 6000`
	`Info: When the ACL that is referenced by SACL is modified, the SACL will be dynamically updated. During the update, these SACL will become invalid temporarily.`
	`[Tolly_auth-acl-ucl-6000]di th`
	`#`
	`acl number 6000`
	`rule 5 deny ip source ucl-group name tolly destination 100.1.1.10 0`
	`#`
	`return`
	`[Tolly_auth-acl-ucl-6000]_`
	`[Tolly_auth]traffic-filter inbound acl 6000`

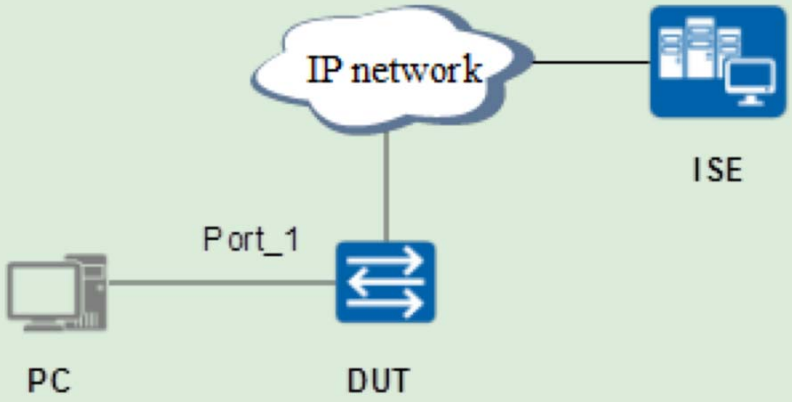
Test Results

3. The user goes online after passing the authentication, and obtains the UCL-group successfully.

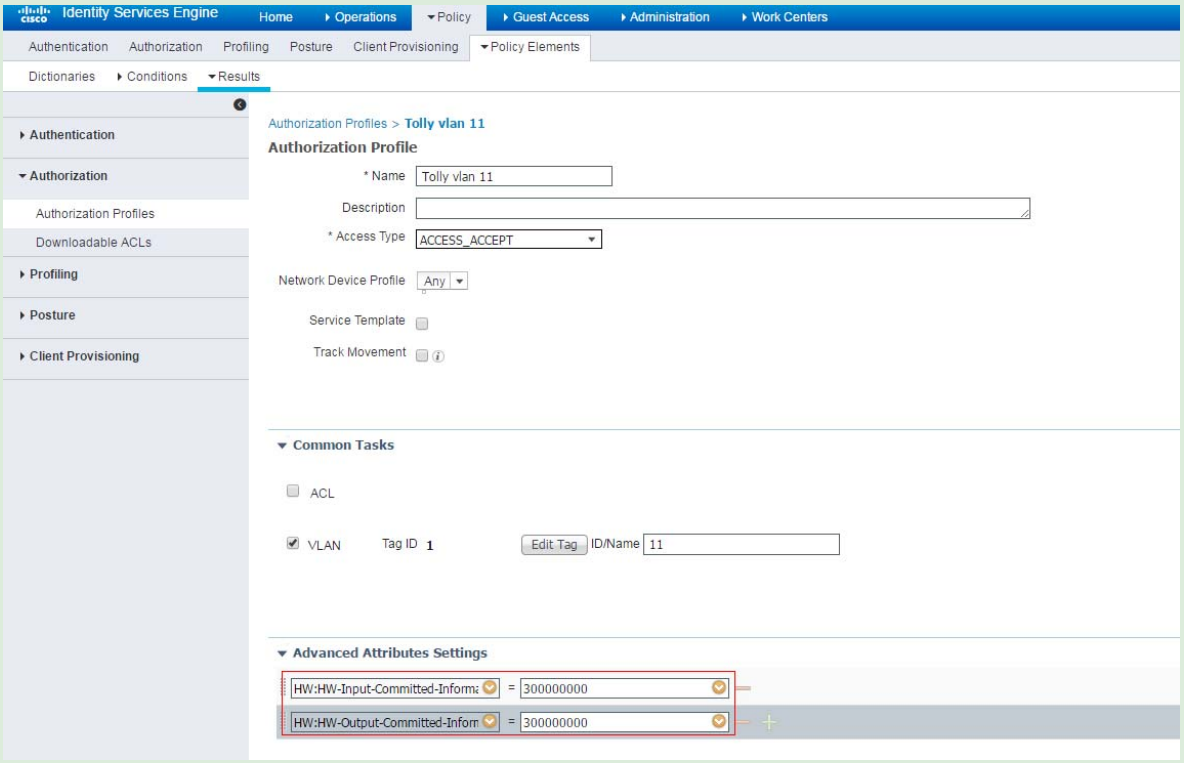
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
 19148  tolly1                   192.89.11.237    0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 19148

Basic:
  User ID                          : 19148
  User name                        : tolly1
  Domain-name                      : tolly
  User MAC                         : 0010-9400-0011
  User IP address                  : 192.89.11.237
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : XGigabitEthernet1/0/0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/14 15:31:17
  User accounting session ID       : Tolly_a01000000004090c10b650004acc
  Option82 information             : -
  User access type                 : 802.1x
  Terminal Device Type             : Data Terminal
  Dynamic group index(Effective)   : 10
  Dynamic group name(Effective)    : tolly

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

4. The tester sends traffic that matches ACL6000, and the traffic is denied.



Test 3.5	Huawei Authentication Attribute: Dynamic CAR CIR (Rate Limiting)
Objective	Verify the Huawei authentication attribute Dynamic CAR CIR when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. Huawei attributes can be imported to the Cisco ISE server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Configure the upstream and downstream CAR authorization on the ISE server. 5. Use the PC to initiate the 802.1X authentication, and expected result 1 is displayed. 6. Use the tester to send upstream and downstream test traffic, and expected result 2 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. Result 2: The tester sends upstream and downstream traffic that is limited to a certain rate.

Test Results	1. Configure upstream and downstream CAR dynamic authorization in the ISE server authorization policy; the CAR is limited to 300 Mbit/s.



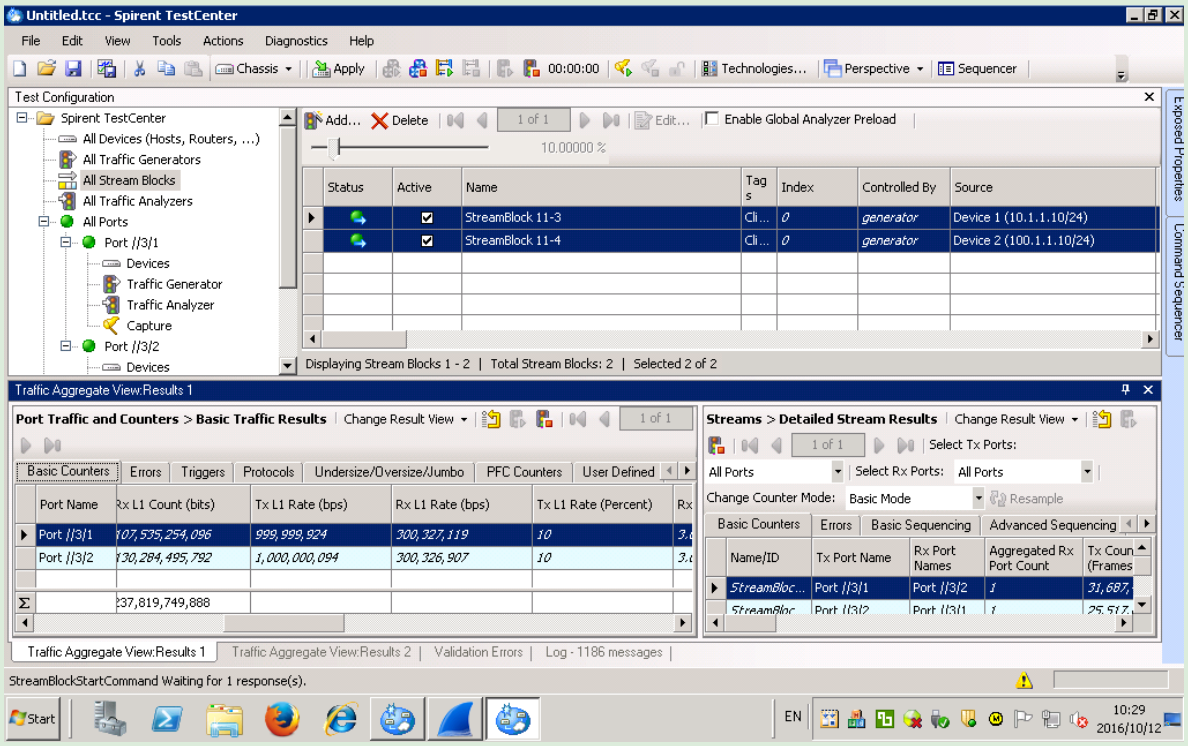
Test Results

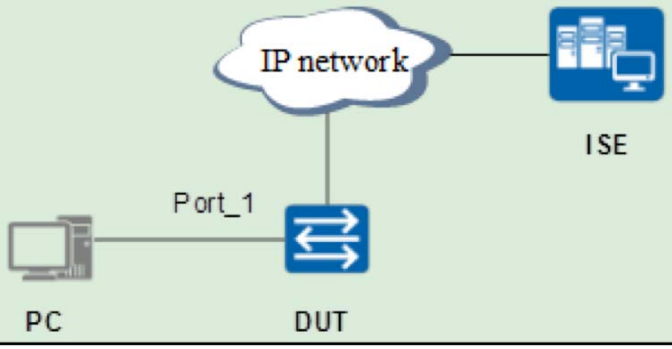
2. The device goes online after passing the authentication successfully, and obtains the authorized CAR.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19127  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
 19144  tolly1                   11.1.1.250       0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
 Number of user-group car : 1
```

```
[Tolly_auth]dis access-user user-id 19144

Basic:
  User ID                         : 19144
  User name                       : tolly1
  Domain-name                     : tolly
  User MAC                        : 0010-9400-0011
  User IP address                 : 11.1.1.250
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : XGigabitEthernet1/0/0
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/11
  User access time                : 2016/10/15 17:15:32
  User accounting session ID      : Tolly_a0100000000409042892b0004ac8
  Option82 information            : -
  User access type                : 802.1x
  Terminal Device Type            : Data Terminal
  Dynamic VLAN ID                 : 11
  User inbound CAR CIR(Kbps)      : 300000
  User inbound CAR PIR(Kbps)      : 300000
  User inbound CAR CBS(Byte)      : 56400000
  User inbound CAR PBS(Byte)      : 56400000
  User inbound data flow(Packet)  : 0
  User inbound data flow(Byte)    : 0
  User outbound CAR CIR(Kbps)     : 300000
  User outbound CAR PIR(Kbps)     : 300000
  User outbound CAR CBS(Byte)     : 56400000
  User outbound CAR PBS(Byte)     : 56400000
  User outbound data flow(Packet) : 1
  User outbound data flow(Byte)   : 78

AAA:
  User authentication type        : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : None
```

Test Results	3. The tester sends upstream and downstream test traffic at a rate of 1000 Mbit/s, and the traffic is limited to 300 Mbit/s.



Test 3.6	Huawei Authentication Attribute: Service Scheme; Generic RADIUS Attribute: Framed-IP-Address (On-demand DHCP IP Address) Generic RADIUS Attribute: Framed-Pool (On-demand DHCP Pool)
Objective	Verify the Huawei authentication attribute HW-Service-Scheme, the generic RADIUS attribute Framed-IP-Address and the generic RADIUS attribute Framed-Pool when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server. Huawei attributes can be imported to the Cisco ISE server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure PPP authentication on the device so that the host can access the network after passing PPPoE authentication. 4. Configure HW-Service-Scheme: pppoe authorization on the ISE server. Create Service-Scheme: pppoe in the AAA view. Bind Service-Scheme to the address pool vlan44. 5. After the PC dials in through PPPoE authentication, expected result 1 is displayed. 6. Add the service scheme pppoe in the default domain. Configure the frame-ip-address attribute in the ISE authorization policy, and assign fixed IP addresses to users. Expected result 2 is displayed. 7. Add the service scheme pppoe in the default domain. Configure the frame-pool attribute in the ISE authorization policy, and assign the IP address pool to users. Expected result 3 is displayed. 
Pass Criteria	Result 1: The tested device displays authentication statistics information, which indicates that the PPP authentication succeeds. The device can obtain addresses from the VLAN44 IP address pool. Result 2: The PC goes online after passing authentication successfully, and obtains the fixed IP address assigned by the ISE server. Result 3: The PC goes online after passing authentication successfully, and obtains the IP address from the IP address pool delivered by the ISE server.

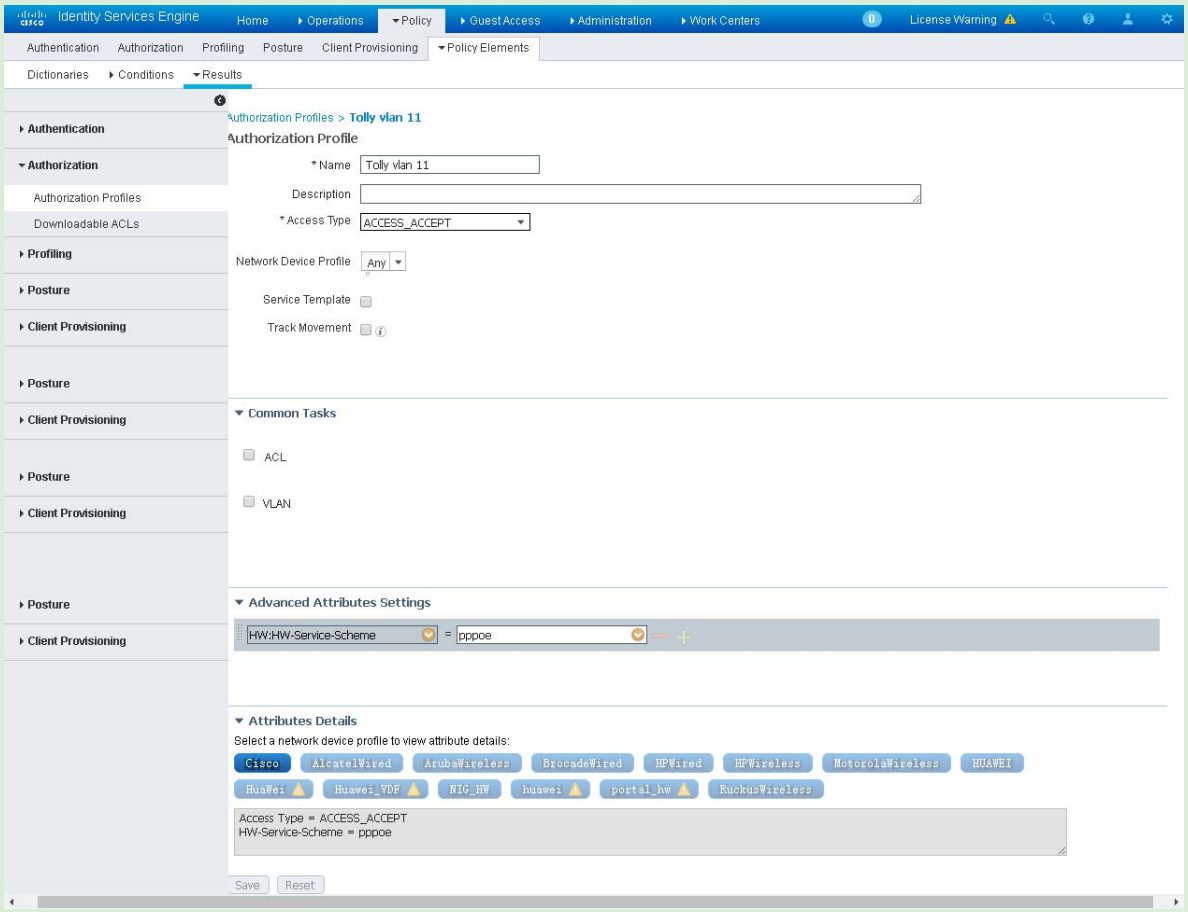
Test Results	Configuration: 1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Configure PPP authentication on the device so that the host can access the network after passing PPPoE authentication. # interface Virtual-Template1 ppp keepalive retransmit 4 ppp mru 1400 ppp authentication-mode pap ppp timer negotiate 5 ip address 44.4.4.1 255.255.255.0 # # interface Vlanif44 pppoe-server bind virtual-template 1 # # ip pool vlan44 gateway-list 44.4.4.1 network 44.4.4.0 mask 255.255.255.0 #

Test Results	4. Configure HW-Service-Scheme: pppoe authorization on the ISE server. Create Service-Scheme: pppoe in the AAA view. Bind Service-Scheme to the address pool vlan44. # ip pool vlan44 gateway-list 44.4.4.1 network 44.4.4.0 mask 255.255.255.0 # # aaa service-scheme pppoe ip-pool vlan44 domain default authentication-scheme radius radius-server tolly # 5. After the PC dials in through PPPoE authentication, expected result 1 is displayed. 6. Add the service scheme pppoe in the default domain. Configure the frame-ip-address attribute in the ISE authorization policy, and assign fixed IP addresses to users. Expected result 2 is displayed. # aaa service-scheme pppoe ip-pool vlan44 domain default authentication-scheme radius radius-server tolly service-scheme pppoe # 7. Add the service scheme pppoe in the default domain. Configure the frame-pool attribute in the ISE authorization policy, and assign the IP address pool to users. Expected result 3 is displayed.

Test Results

Results:

1. Configure HW-Service-Scheme: pppoe authorization on the ISE server.



Test Results

2. Configure the service scheme pppoe in the AAA view, and bind vlan44 IP address pool to pppoe. The user goes online after passing authentication successfully, and obtains the pppoe service scheme and IP address.

```
[Tolly_auth-aaa]di th
#
aaa
 authentication-scheme default
 authentication-scheme radius
  authentication-mode radius
 authentication-scheme tolly
  authentication-mode radius
 authorization-scheme default
 authorization-scheme tolly
 accounting-scheme default
 accounting-scheme tolly
  accounting-mode radius
 service-scheme pppoe
  ip-pool vlan44
 service-scheme tolly
 domain default
  authentication-scheme radius
  radius-server tolly
```

Test Results

```
[Tolly_auth-aaa]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16016  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91 Success
 81555  tolly                    44.4.4.253       f0de-f1e0-aeb2 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth-aaa]
[Tolly_auth-aaa]
[Tolly_auth-aaa]dis access-user us
[Tolly_auth-aaa]dis access-user user
[Tolly_auth-aaa]dis access-user user-id 81555

Basic:
  User ID                         : 81555
  Session ID                      : 4
  User name                       : tolly
  Domain-name                     : tolly
  User MAC                        : f0de-f1e0-aeb2
  User IP address                 : 44.4.4.253
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : GigabitEthernet1/1/5
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/44
  User access time                : 2016/10/13 18:40:27
  User accounting session ID      : Tolly_a01105000000044b45f610013e93
  Option82 information            : -
  User access type                : PPP
  Dynamic service scheme          : pppoe

AAA:
  User authentication type        : PPP authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : None

[Tolly_auth-aaa]
```

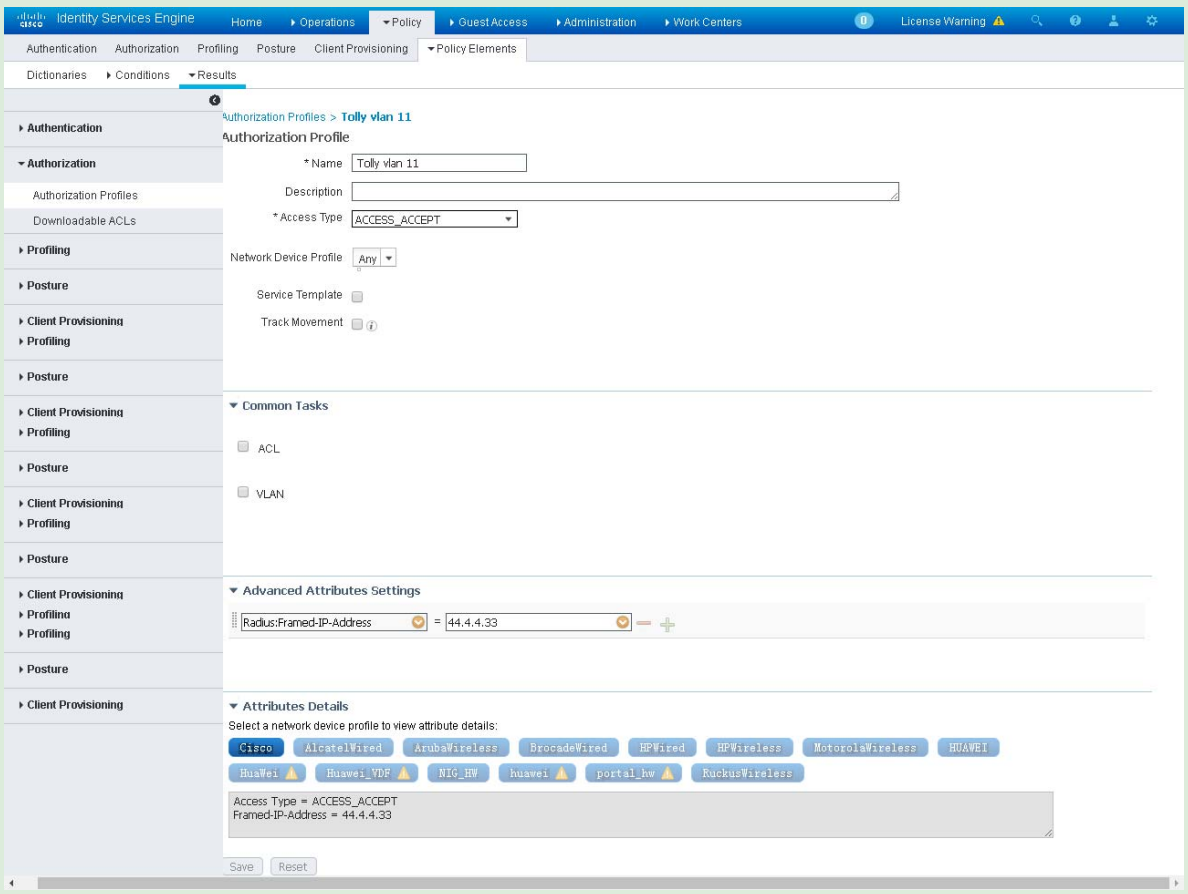
Test Results

3. Configure the frame-ip-address attribute in the ISE authorization policy, and users can obtain fixed IP addresses.

```
[Tolly_auth-aaa-domain-default]di th
#
 domain default
  authentication-scheme radius
  service-scheme pppoe
  radius-server tolly
#
```

```
 UserID Username                 IP address       MAC            Status
 -------------------------------------------------------------------------------
 16016  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91 Success
 81553  tolly                    44.4.4.33        f0de-f1e0-aeb2 Success
 -------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user user-id 81553

Basic:
  User ID                       : 81553
  Session ID                    : 2
  User name                     : tolly
  Domain-name                   : tolly
  User MAC                      : f0de-f1e0-aeb2
  User IP address               : 44.4.4.33
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : GigabitEthernet1/1/5
  User vlan event               : Success
  QinQVlan/UserVlan             : 0/44
  User access time              : 2016/10/13 18:11:30
  User accounting session ID    : Tolly_a011050000000448825990013e91
  Option82 information          : -
  User access type              : PPP
  Dynamic service scheme        : pppoe

AAA:
  User authentication type      : PPP authentication
  Current authentication method : RADIUS
  Current authorization method  : -
  Current accounting method     : None

[Tolly_auth]
```

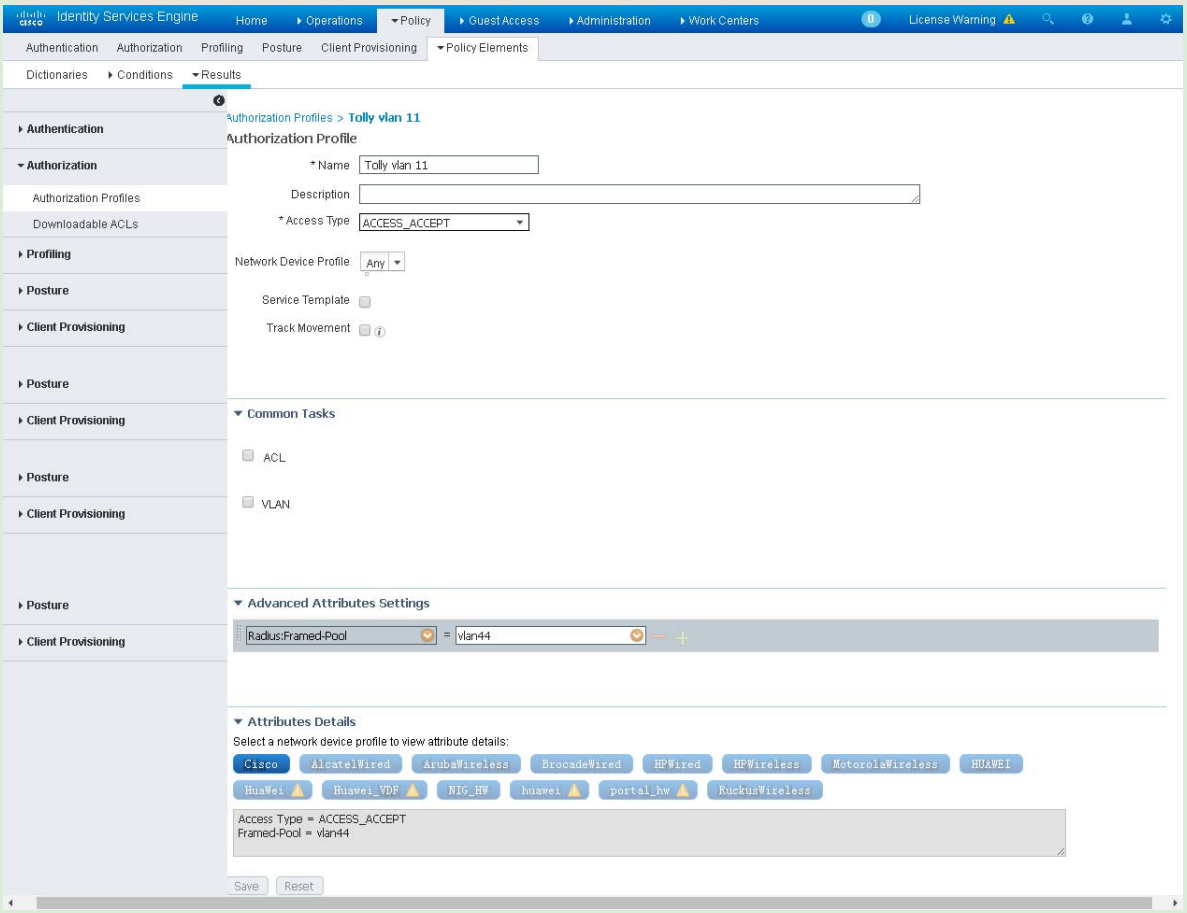
Test Results



Test Results

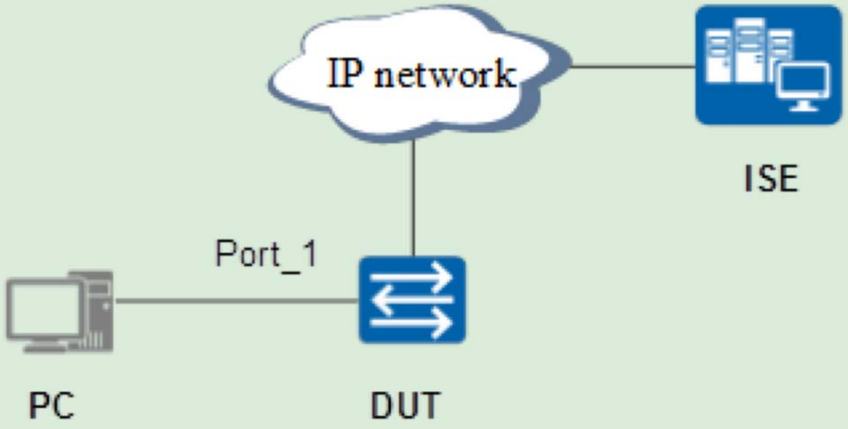
4. Configure the frame-pool attribute in the ISE authorization policy, and users can obtain IP addresses from the assigned IP address pool.

```
[Tolly_auth-aaa-domain-default]di th
#
 domain default
  authentication-scheme radius
  service-scheme pppoe
  radius-server tolly
#
```



Test Results

```
 ------------------------------------------------------------------------------
 16016  3C-97-0E-D9-BD-91       192.89.11.243    3c97-0ed9-bd91 Success
 81554  tolly                  44.4.4.254       f0de-f1e0-aeb2 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user user-id 81554

Basic:
  User ID                          : 81554
  Session ID                       : 3
  User name                        : tolly
  Domain-name                      : tolly
  User MAC                         : f0de-f1e0-aeb2
  User IP address                  : 44.4.4.254
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet1/1/5
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/44
  User access time                 : 2016/10/13 18:27:48
  User accounting session ID       : Tolly_a01105000000044707a450013e92
  Option82 information             : -
  User access type                 : PPP
  Dynamic service scheme           : pppoe

AAA:
  User authentication type         : PPP authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]
```

Test 3.7	Generic RADIUS Attribute: NAS-Port
Objective	Verify the generic RADIUS attribute NAS-Port when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Use the PC to initiate the 802.1X authentication, and expected result 1 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the PC passes authentication successfully. The access user's physical port number can be viewed on the ISE server through the NAS-Port attribute.

Test Results

1. The tested device displays 802.1X authentication statistics information, which indicates that the PC passes authentication successfully. The access user's physical port number can be viewed on the ISE server through the NAS-Port attribute.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 16093                          192.89.17.109    3c97-0ed9-bd91 Pre-authen
 16094  tolly                   -                0010-9410-0003 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 16094

Basic:
  User ID                          : 16094
  User name                        : tolly
  Domain-name                      : tolly
  User MAC                         : 0010-9410-0003
  User IP address                  : -
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : XGigabitEthernet1/0/0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/10
  User access time                 : 2016/10/13 14:46:47
  User accounting session ID       : s127000100000000000010d352bf0003ede
  Option82 information             : -
  User access type                 : 802.1x
  Terminal Device Type             : Data Terminal

AAA:
  User authentication type         : 802.1x authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]
```

Test Results

Authentication Details

Source Timestamp	2016-10-13 06:46:11.27
Received Timestamp	2016-10-13 06:46:11.271
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	tolly
User Type	User
Endpoint Id	00:10:94:10:00:03
Calling Station Id	00-10-94-10-00-03
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group
Authentication Method	dot1x
Authentication Protocol	CHAP/MD5
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1;subslot=0;port=0;vlanid=10
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Posture Status	NotApplicable
Response Time	25

Test Results

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	tolly
Endpoint Id	00:10:94:10:00:03
Endpoint Profile	
Authentication Policy	Default >> TLS >> Default
Authorization Policy	Default >> NIG_PreCPP
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2016-10-13 06:46:11.27
Received Timestamp	2016-10-13 06:46:11.271
Policy Server	ISE2
Event	5200 Authentication succeeded
Username	tolly
User Type	User
Endpoint Id	00:10:94:10:00:03
Calling Station Id	00-10-94-10-00-03
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:Tolly_Group
Authentication Method	dot1x
Authentication Protocol	CHAP/MD5
Service Type	Framed
Network Device	Tolly-12700
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.89.15.101
NAS Port Id	slot=1;subslot=0;port=0;vlanid=10
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Posture Status	NotApplicable
Response Time	25

Steps

11001	Received RADIUS Access-Reque
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Poli
15048	Queried PIP - Radius.Called-Stat
15004	Matched rule - TLS
15041	Evaluating Identity Policy
15006	Matched Default Rule
22072	Selected identity source sequenc
15013	Selected Identity Source - Interna
24209	Looking up Endpoint in Internal E
24217	The host is not found in the intern
15013	Selected Identity Source - Interna
24210	Looking up User in Internal Users
24212	Found User in Internal Users IDS
22037	Authentication Passed
24423	ISE has not been able to confirm authentication
15036	Evaluating Authorization Policy
15004	Matched rule - NIG_PreCPP
15016	Selected Authorization Profile - P
11002	Returned RADIUS Access-Accep

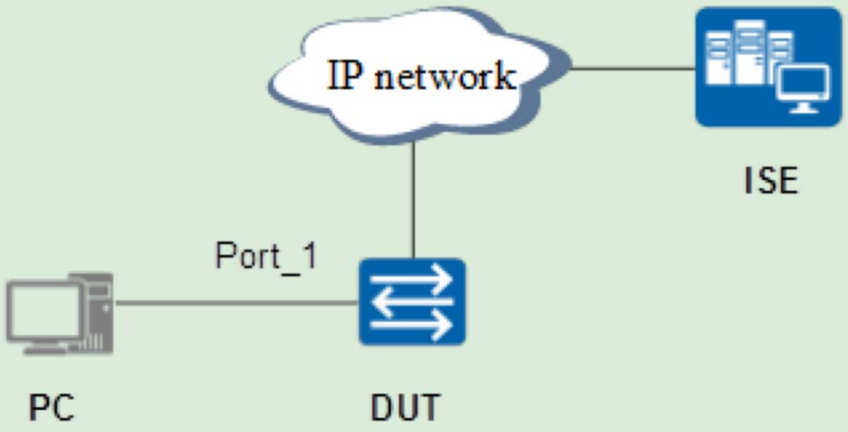
Test Results

Other Attributes

ConfigVersionId	111
DestinationPort	1812
Protocol	Radius
NAS-Port	16777226
Framed-Protocol	PPP
Vendor Specific	00:00:07:db:3b:06:57:fe:01:4d:3c:23:32:35:35:2e:32:35:35:2e:32:35:35:2e:32:35:35:20:30:30:3a:31:30:3a:39:34:3a:31:30:3a:30:30:3a:30:33:1a:06:00:00:3e:de:fe:0f:48:75:61:77:65:69:20:53:31:32:37:30:30:ff:08:53:31:32:37:30:30:99:06:00:00:00:01
Acct-Session-Id	s1270001000000000010d352bf0003ede
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	8ade1f15-aef1-4a9a-8158-d02e835179db
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	54-39-DF-C9-9A-E0
AcsSessionID	ISE2/265353892/2665
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	Guest Users
SelectedAuthenticationIdentityStores	Tander
SelectedAuthenticationIdentityStores	test.com
SelectedAuthenticationIdentityStores	Initial_Scope
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	AD1
AuthorizationPolicyMatchedRule	NIG_PreCPP
CPMSessionID	c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE
EndPointMACAddress	00-10-94-10-00-03
ISEPolicySetName	Default
AllowedProtocolMatchedRule	TLS
IdentitySelectionMatchedRule	Default
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
RADIUS Username	tolly
NAS-Identifier	s12700
Device IP Address	192.89.15.101
Called-Station-ID	54:39:DF:C9:9A:E0

Result

State	ReauthSession:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE
Class	CACS:c0590bbc2OUgWwZvhOmzN1gmTKdsaaNzO5HIxe4HhBWxpmpyVPE:ISE2/265353892/2665
LicenseTypes	5

Test 3.8	Post-rejection Authentication
Objective	Verify the post-rejection authentication when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure DUT to ensure that DUT and RADIUS server communicate with each other at Layer 3. 2. Create a RADIUS server profile and configure the related parameters, including IP address of the authentication server, port number, the RADIUS server key, and the retransmission time. Create an authentication scheme, and configure the authentication mode as RADIUS. Configure a domain name, and apply the authentication scheme to the domain. 3. Enable 802.1X authentication globally and on the interface Port_1. 4. Enter the correct user name and password on the PC to initiate 802.1X authentication. Expected result 1 is displayed. 5. Configure the event on the device that if authentication fails, authorize VLAN10 to users. Configure VLANIF10 IP address pool. 6. Enter the wrong password for authentication on the PC. Expected result 2 is displayed. 
Pass Criteria	Result 1: The tested device displays 802.1X authentication statistics information, which indicates that the authentication succeeds. Result 2: The PC authentication fails, and the PC obtains the VLANIF10 IP address.

Test Results

1. Enter the correct user name and password, and the PC can go online after passing the authentication successfully.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19007  F0-DE-F1-E0-AE-B2        192.89.11.253    f0de-f1e0-aeb2 Success
 19006  tolly1                   192.89.11.239    0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 19006

Basic:
  User ID                         : 19006
  User name                       : tolly1
  Domain-name                     : tolly
  User MAC                        : 0010-9400-0011
  User IP address                 : 192.89.11.239
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : XGigabitEthernet1/0/0
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/4090
  User access time                : 2016/10/14 14:28:39
  User accounting session ID      : Tolly_a0100000000004090ffe9630004aca
  Option82 information            : -
  User access type                : 802.1x
  Terminal Device Type            : Data Terminal

AAA:
  User authentication type        : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : None

[Tolly_auth]
```

Test Results

2. Configure the event on the device that if authentication fails, authorize VLAN10.

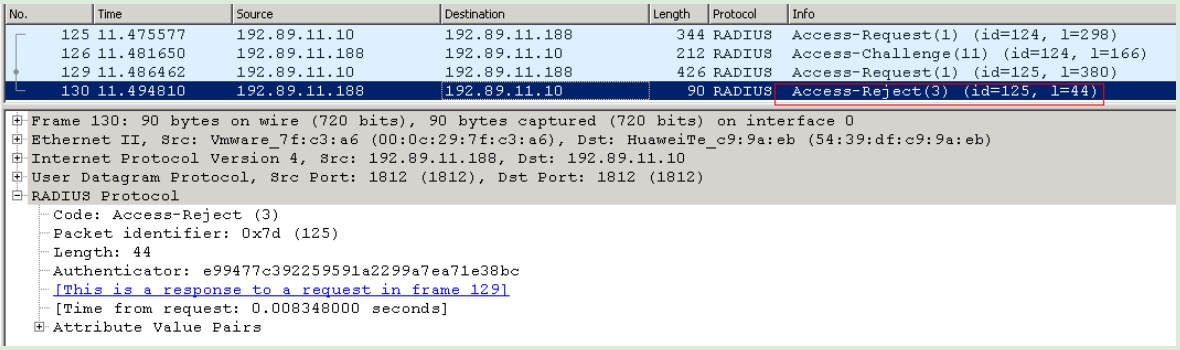
```
[Tolly_auth-authen-profile-tolly_1x]di th
#
authentication-profile name tolly_1x
 dot1x-access-profile tolly
 portal-access-profile tolly
 access-domain tolly
 access-domain tolly force
 authentication event authen-fail action authorize vlan 10
#
```

```
[Tolly_auth-Vlanif10]di th
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 10.1.1.1
#
```

```
[Tolly_auth-XGigabitEthernet1/0/0]di th
#
interface XGigabitEthernet1/0/0
 port link-type hybrid
 port hybrid pvid vlan 4090
 port hybrid untagged vlan 4090
 authentication-profile tolly_1x
 port-mirroring to observe-port 1 inbound
 port-mirroring to observe-port 1 outbound
#
```

Test Results

3. The PC authentication fails, and the PC obtains the VLANIF10 IP address.

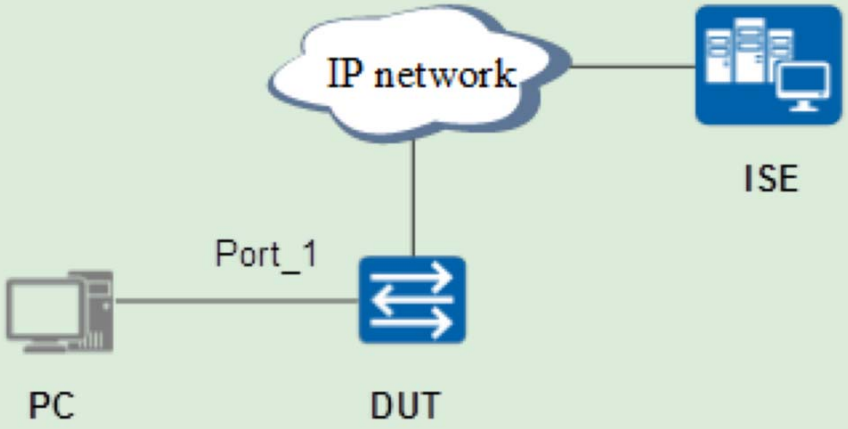


No.	Time	Source	Destination	Length	Protocol	Info
125	11.475577	192.89.11.10	192.89.11.188	344	RADIUS	Access-Request(1) (id=124, l=298)
126	11.481650	192.89.11.188	192.89.11.10	212	RADIUS	Access-Challenge(11) (id=124, l=166)
129	11.486462	192.89.11.10	192.89.11.188	426	RADIUS	Access-Request(1) (id=125, l=380)
130	11.494810	192.89.11.188	192.89.11.10	90	RADIUS	Access-Reject(3) (id=125, l=44)

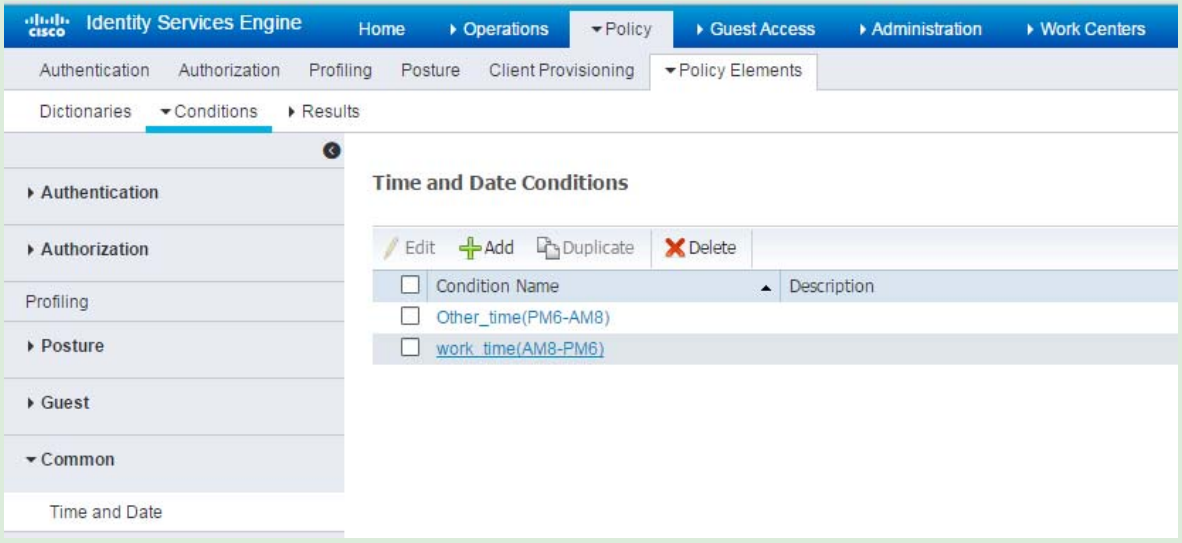
```
Frame 130: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: Vmware_7f:c3:a6 (00:0c:29:7f:c3:a6), Dst: HuaweiTe_c9:9a:eb (54:39:df:c9:9a:eb)
Internet Protocol Version 4, Src: 192.89.11.188, Dst: 192.89.11.10
User Datagram Protocol, Src Port: 1812 (1812), Dst Port: 1812 (1812)
RADIUS Protocol
    Code: Access-Reject (3)
    Packet identifier: 0x7d (125)
    Length: 44
    Authenticator: e99477c392259591a2299a7ea71e38bc
    [This is a response to a request in frame 129]
    [Time from request: 0.008348000 seconds]
  Attribute Value Pairs
```

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19002  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91 Success
 19007  tolly123                 10.1.1.250       0010-9400-0011 Fail-authorized
 ------------------------------------------------------------------------------
```

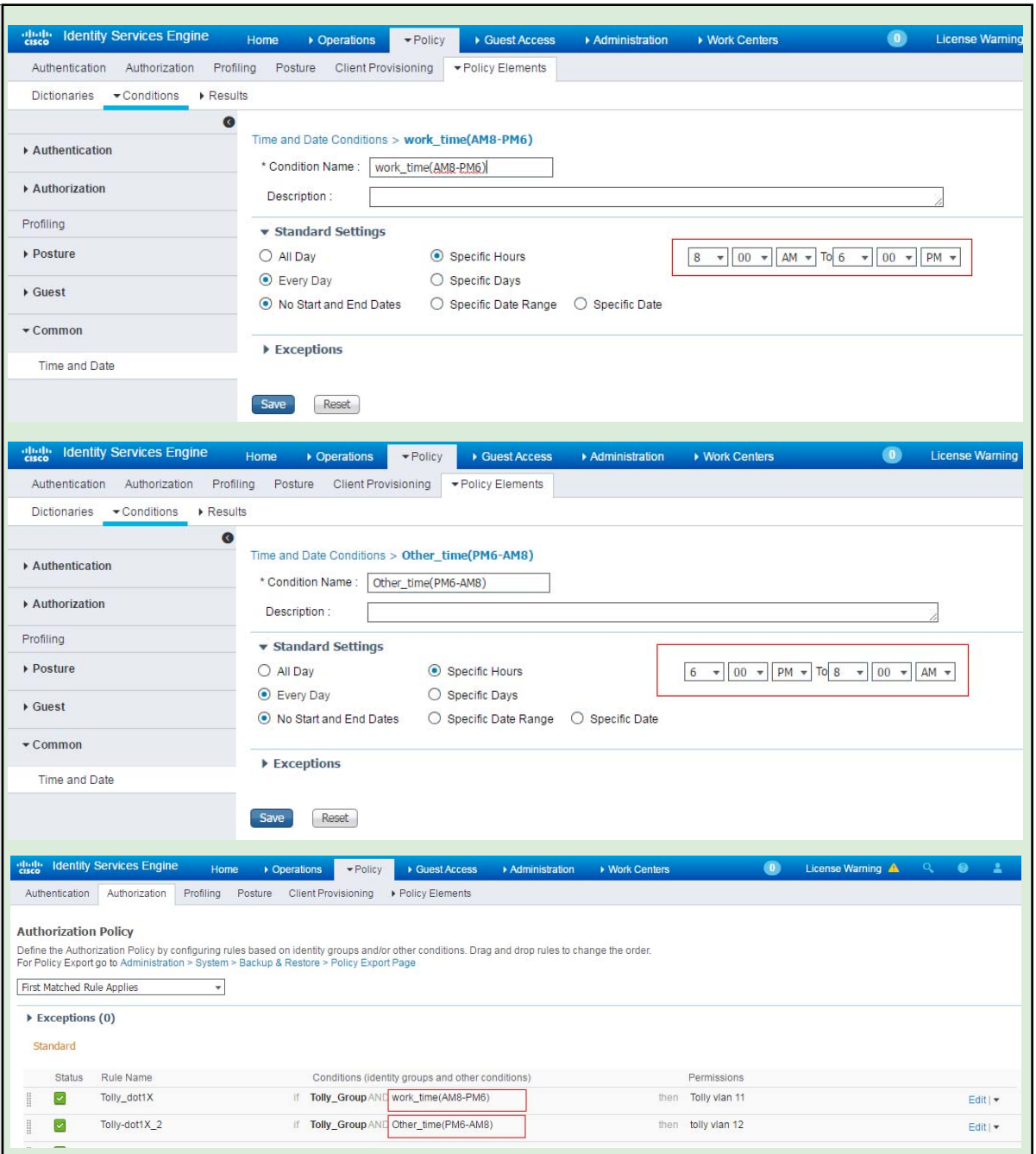
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19002  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91 Success
 19007  tolly123                 10.1.1.250       0010-9400-0011 Fail-authorized
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis acc
[Tolly_auth]dis access-user user-id 19007

Basic:
  User ID                         : 19007
  User name                       : tolly123
  Domain-name                     : -
  User MAC                        : 0010-9400-0011
  User IP address                 : 10.1.1.250
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : XGigabitEthernet1/0/0
  User vlan event                 : Fail-authorized
  QinQVlan/UserVlan               : 0/10
  User access time                : 2016/10/14 14:35:57
  Option82 information            : -
  User access type                : None
  Terminal Device Type            : Data Terminal
  Dynamic VLAN ID                 : 10

AAA:
  User authentication type        : No authentication
  Current authentication method   : None
  Current authorization method    : Local
  Current accounting method       : None
```

Test 3.9	Time-based Authentication Policy
Objective	Verify the time-based authentication when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the 802.1X authentication profile on the device. 5. Configure the DHCP server on the device, and enable dot1x authentication on the correspondent port. 6. Enter the correct user name and password on the device for authentication. Check the user address and authentication information, and expected result 1 is displayed. 7. Configure time ranges on the ISE server. Authorization policies vary with different time periods. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: Users obtain different authorization policies based on time periods.

Test Results	Configuration 1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template tolly radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 # 3. Configure the aaa scheme. # aaa authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly authentication-scheme tolly accounting-scheme tolly radius-server tolly # 4. Configure the 802.1X authentication profile on the device. # dot1x-access-profile name tolly authentication-method eap authentication-profile name tolly dot1x-access-profile tolly access-domain tolly dot1x force #

Test Results	5. Configure the DHCP server on the device, and enable dot1x authentication on the correspondent port. # interface Vlanif4090 ip address 192.89.6.202 255.255.255.0 dhcp select interface interface GigabitEthernet1/1/0 port link-type hybrid port hybrid pvid vlan 4090 port hybrid untagged vlan 4090 authentication-profile tolly # 6. Enter the correct user name and password on the device for authentication. Check the user address and authentication information, and expected result 1 is displayed. 7. Configure time ranges on the ISE server. Authorization policies vary with different time periods. Test Results: 1. Configure different time ranges and two dot1x authorization policies on the ISE server. Users obtain different authorization policies based on their login time periods. 

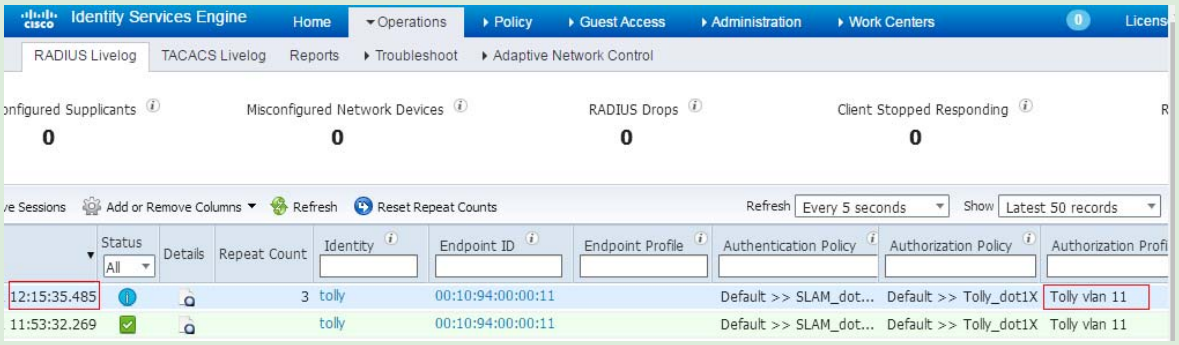
Test Results

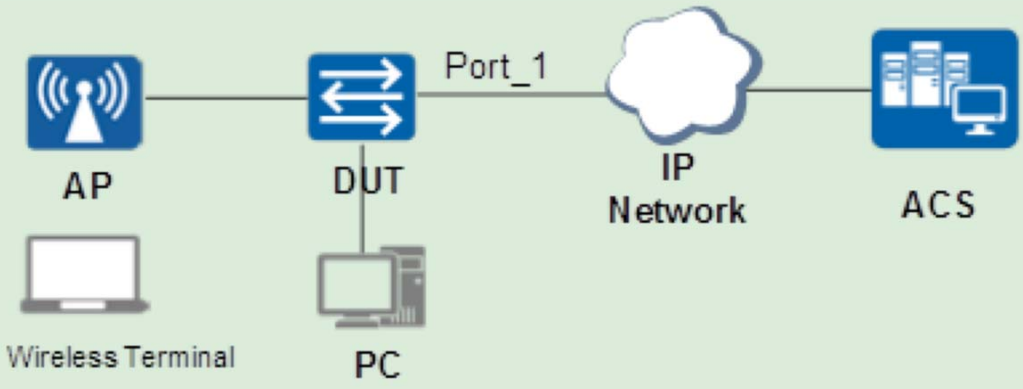


Test Results

2. A user goes online after passing the dot1x authentication, and obtains the correspondent authorization policy based on the login time period.

```
[Tolly_auth]dis access-user
--------------------------------------------------------------------------------
UserID Username                 IP address       MAC             Status
--------------------------------------------------------------------------------
16016  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91  Success
16020  tolly                    -                0010-9400-0011  Success
--------------------------------------------------------------------------------
Total: 2, printed: 2
```



Test 4.1	Change of Authorization (CoA): Session Re-authentication
Objective	Verify session re-authentication when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server on the switch. 4. Configure the aaa profile. 5. Configure the MAC authentication profile. 6. Configure the CoA authorization server. 7. Configure the redirection ACL on the switch. 8. Users access the network in wired mode for MAC authentication. Expected result 1 is displayed. 9. Open a web page and access any website. Enter the user name and password for authentication. Expected result 2 is displayed. 
Pass Criteria	Result 1: When the user accesses the network for MAC authentication, the server delivers URL and redirection ACL. Open a browser and enter any IP address in the address bar, the page is redirected to the guest management page. Result 2: After entering the user name and password, the user passes the Portal authentication successfully.

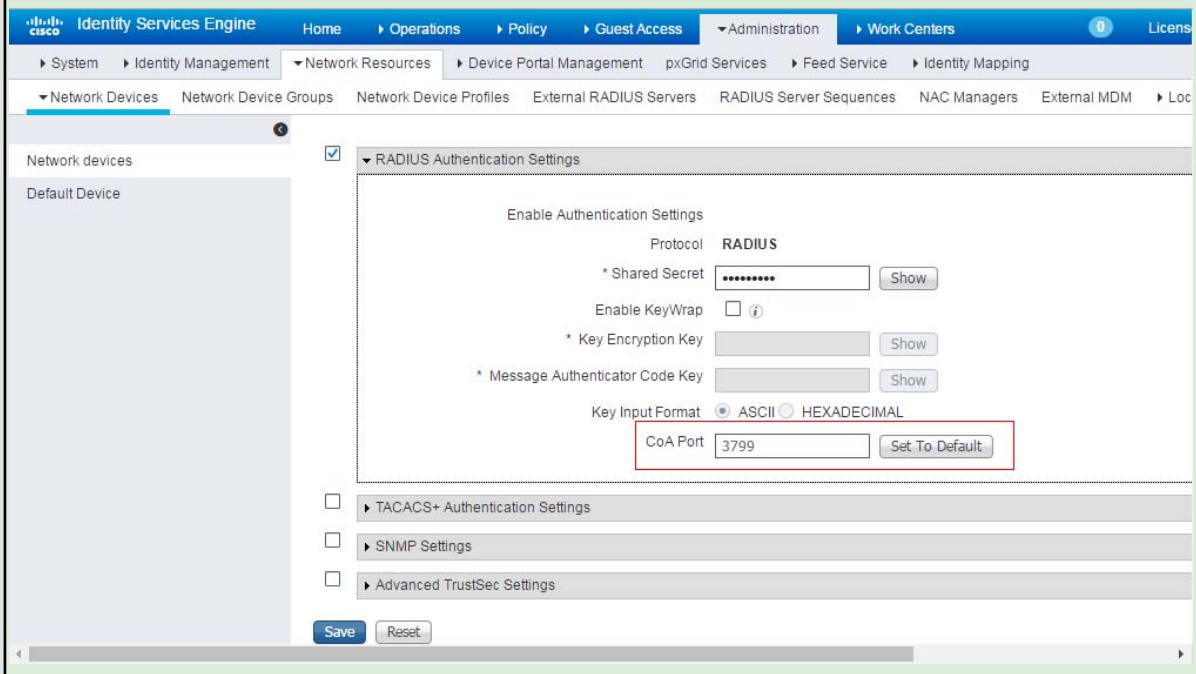
Test Results

1. Configure the RADIUS authorization server, and enable the device to respond to and process ISE CoA packets. On the ISE server, change the CoA port number of the access device to 3799 (change the destination port number in the 1.6.3 case).

   #

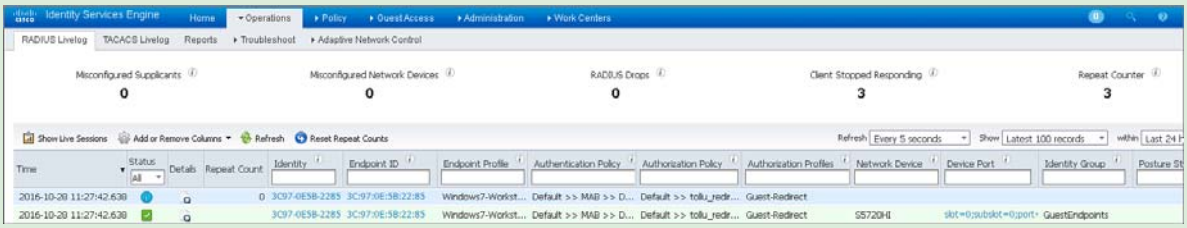
   radius-server authorization 192.89.11.188 shared-key cipher huawei123

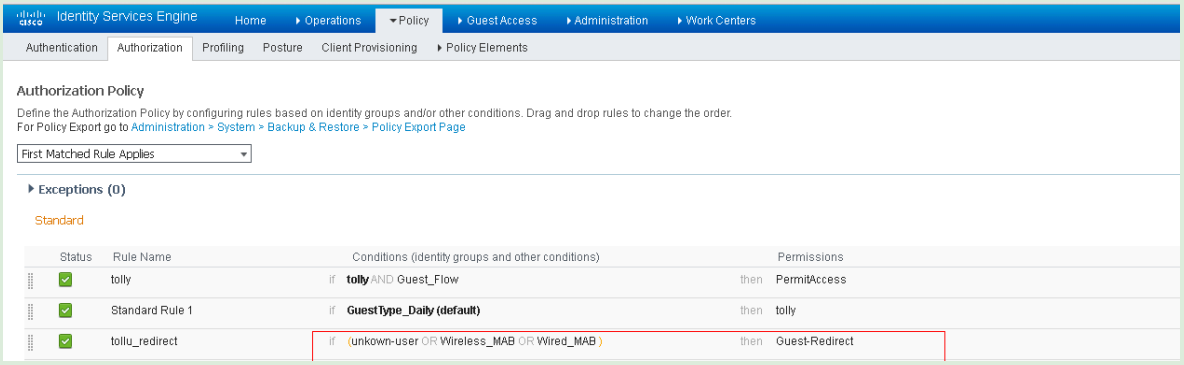
   #



Test Results

2. When a new user accesses the network, he must pass the MAC authentication first. After the authentication succeeds, the page is redirected to the guest management page. A user can log in to the system using a registered account or a new user can register an account first.



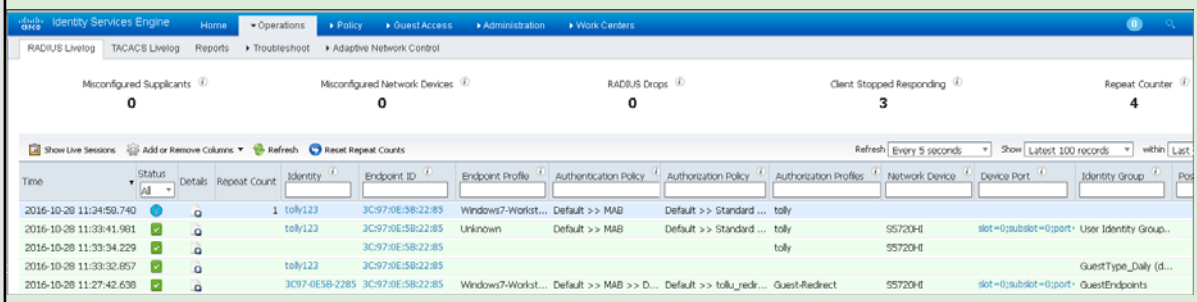


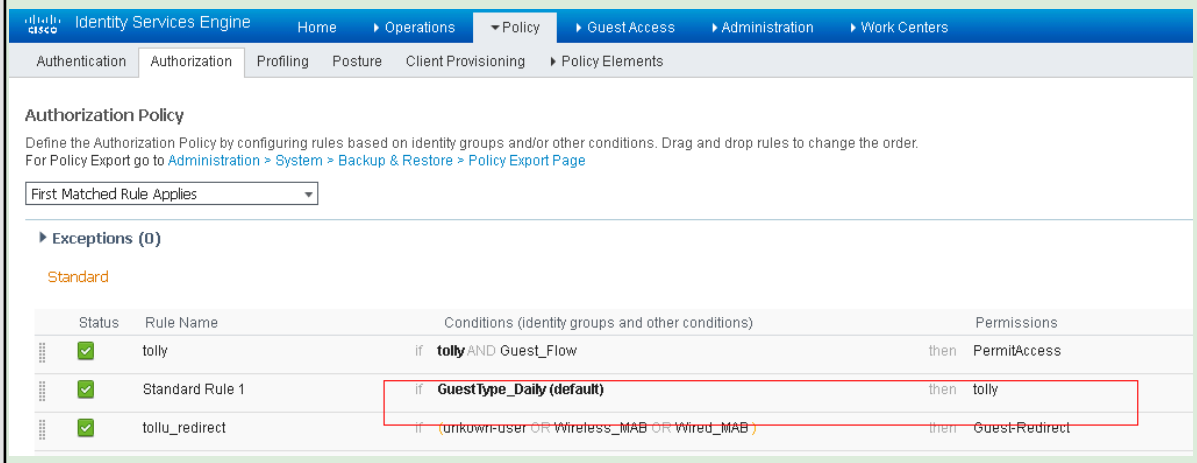
3. After a user registers an account, the system disconnect the user through CoA. The user should log in again using the new account.
4. After new users log in to the system, the server authorizes new policies to users so that they can obtain new permissions.

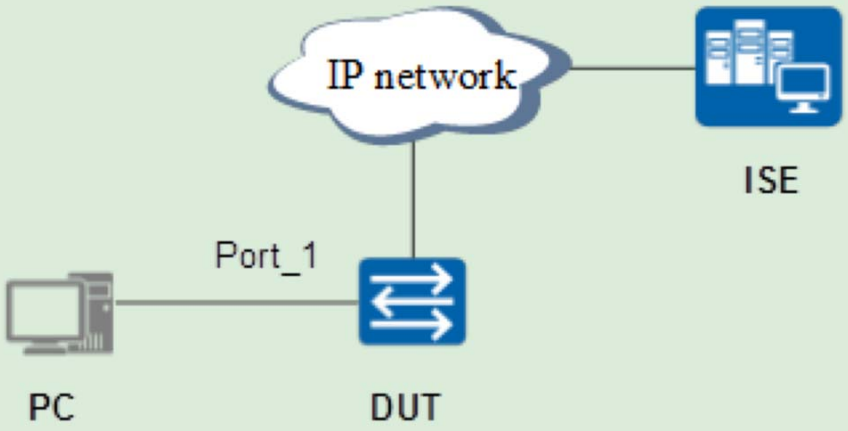
Test Results

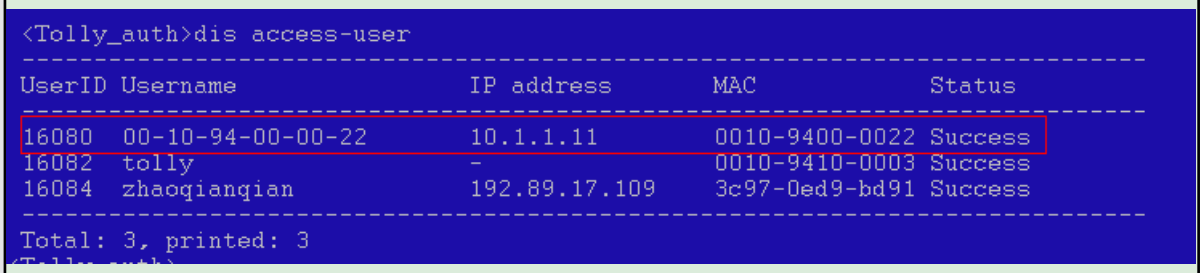
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 185    tolly123                172.168.10.252   3c97-0e5b-2285 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 185

Basic:
  User ID                          : 185
  User name                        : tolly123
  Domain-name                      : tolly_mac
  User MAC                         : 3c97-0e5b-2285
  User IP address                  : 172.168.10.252
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet0/0/19
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/1720
  User access time                 : 2016/10/28 16:15:12
  User accounting session ID       : Tolly_a00019000001720a2f0ea00000b9
  Option82 information             : -
  User access type                 : MAC
  Terminal Device Type             : Data Terminal
  Dynamic ACL number(Effective)    : 3004
  Session Timeout                  : 65595(s)
  Termination Action               : OFFLINE

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]_
```

Test Results





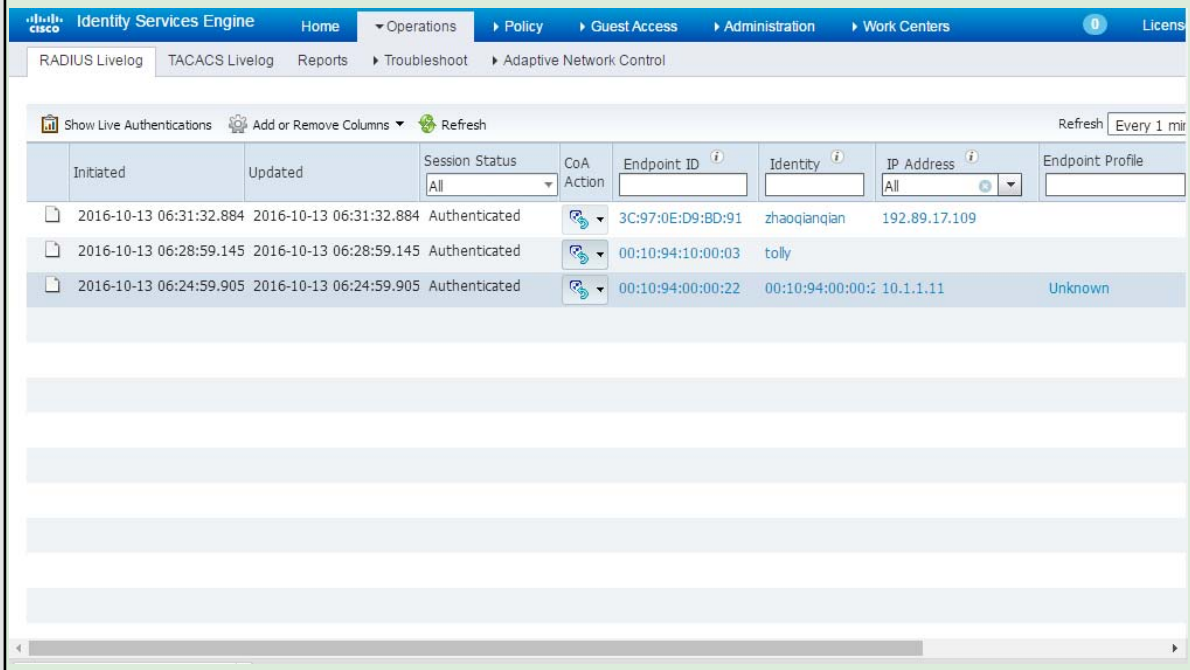
Test 4.2	CoA: Session Termination
Objective	Verify session termination when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the MAC authentication profile on the device. 4. Configure the DHCP server on the device, and enable MAC authentication on the correspondent port. 5. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 6. Configure the RADIUS authorization server on the device and use the ISE server to disconnect online users. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: Online users are disconnected from the network by the ISE server, and online user entries are deleted from the device.

Test Results	1. The user goes online after passing the MAC authentication successfully, and obtains the correspondent IP address. 

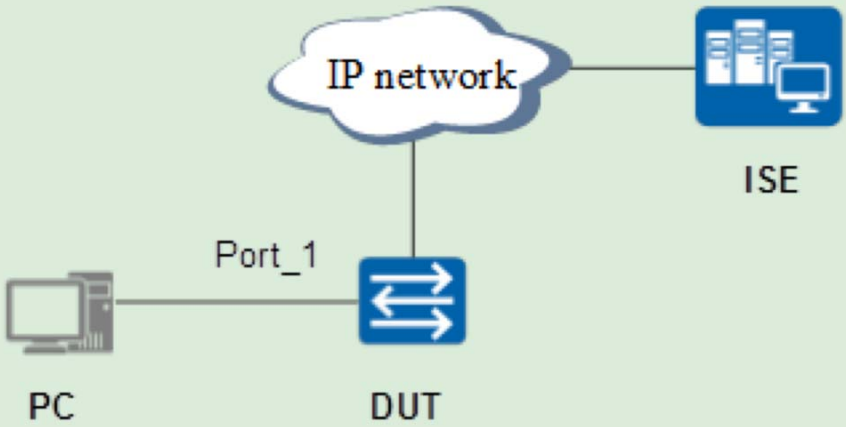
```
<Tolly_auth>dis access-user
------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
------------------------------------------------------------------------------
16080  00-10-94-00-00-22        10.1.1.11        0010-9400-0022 Success
16082  tolly                    -                0010-9410-0003 Success
16084  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
------------------------------------------------------------------------------
Total: 3, printed: 3
```

Test Results

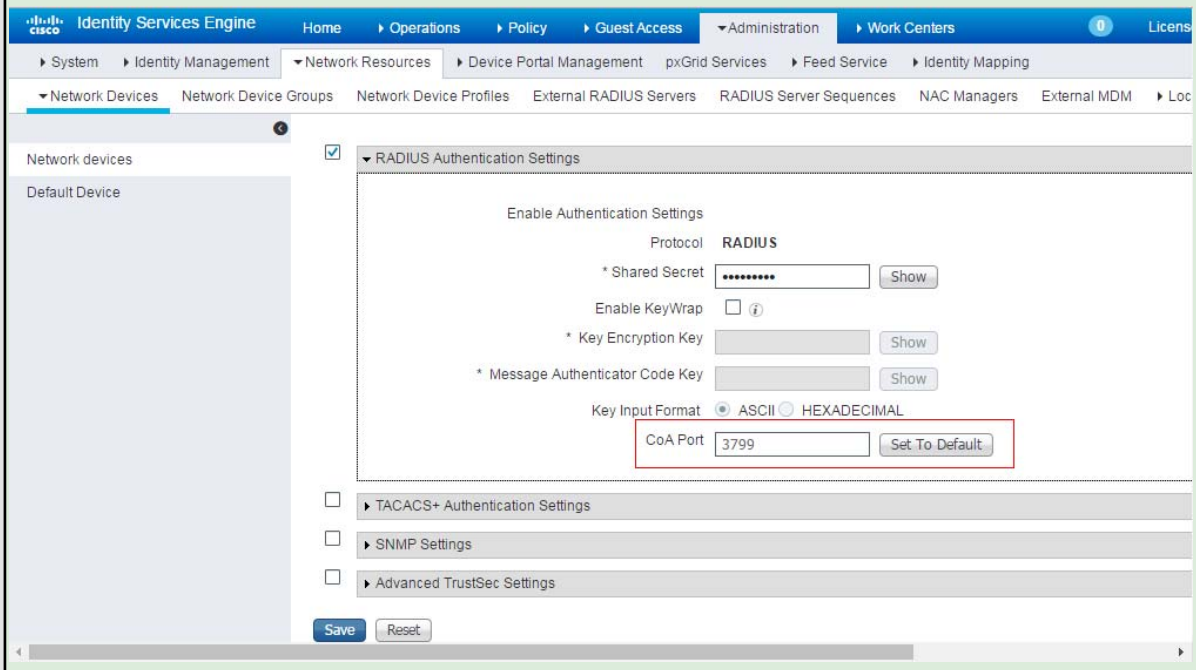
2. Online users are disconnected from the network by the ISE server, and online user entries are deleted from the device.




```
<Tolly_auth>dis access-user
------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
------------------------------------------------------------------------------
16080  00-10-94-00-00-22        10.1.1.11        0010-9400-0022 Success
16082  tolly                    -                0010-9410-0003 Success
16084  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
------------------------------------------------------------------------------
Total: 3, printed: 3
<Tolly_auth>
<Tolly_auth>dis access-user
------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
------------------------------------------------------------------------------
16082  tolly                    -                0010-9410-0003 Success
16084  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
------------------------------------------------------------------------------
Total: 2, printed: 2
```

Test 4.3	CoA Port Customization in ISE
Objective	Verify CoA port customization when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the MAC authentication profile on the device. 4. Configure the DHCP server on the device, and enable MAC authentication on the correspondent port. 5. Connect the user terminal to the DUT and enable the MAC-authenticated port. 6. Change the CoA port number of the access device to 3799 on the ISE server. 7. Configure the RADIUS authorization server on the device and use the ISE server to disconnect online users. Expected result 1 is displayed. 
Pass Criteria	Result 1: The CoA port number is changed to 3799, and online users are disconnected.

Test Results	Configuration: 1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template mac_auth radius-server shared-key cipher Huawei@123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 radius-attribute set Service-Type 10 # 3. Configure the MAC authentication profile on the device. # mac-access-profile name mac_access_profile authentication-profile name mac_auth mac-access-profile mac_access_profile access-domain mac_auth force # 4. Configure the DHCP server on the device, and enable MAC authentication on the correspondent port. # interface Vlanif12 ip address 12.1.1.1 255.255.255.0 dhcp select interface interface GigabitEthernet0/0/2 port link-type access port default vlan 130 authentication-profile mac_auth #

Test Results	5. Connect the user terminal to the DUT and enable the MAC-authenticated port. 6. Change the CoA port number of the access device to 3799 on the ISE server. 7. Configure the RADIUS authorization server on the device and use the ISE server to disconnect online users. Expected result 1 is displayed. # radius-server authorization 192.89.11.188 shared-key cipher huawei123 # Results: 1. Change the CoA port number of the access device to 3799 on the ISE server. 

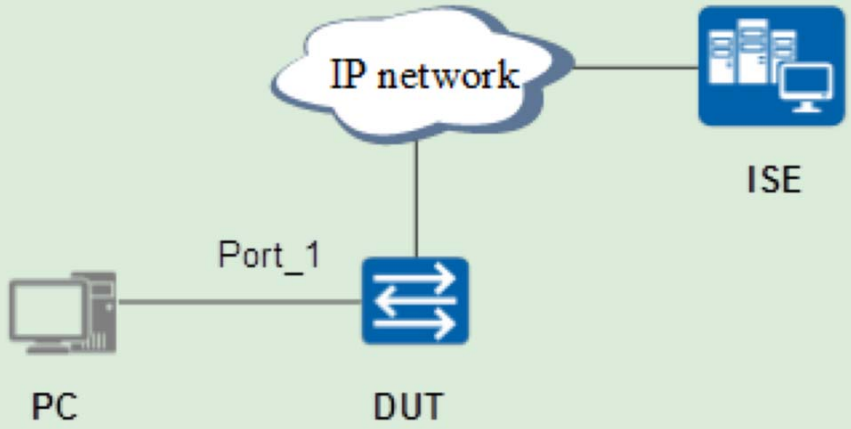
Test Results

2. The online user is disconnected from the network by the ISE server. The CoA port number of the disconnection packet sent by the RADIUS server is changed to 3799.

No.	Time	Source	Destination	Length	Protocol	Info
2041	564.018318	192.89.11.10	192.89.11.188	355	RADIUS	Access-Request(1) (id=215, l=309)
2045	564.102148	192.89.11.188	192.89.11.10	235	RADIUS	Access-Accept(2) (id=215, l=189)
2167	582.467992	192.89.11.188	192.89.11.10	151	RADIUS	Disconnect-Request(40) (id=9, l=105)
2168	582.470221	192.89.11.10	192.89.11.188	128	RADIUS	Disconnect-ACK(41) (id=9, l=82)

```
⊞ Frame 2167: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
⊞ Ethernet II, Src: Vmware_7f:c3:a6 (00:0c:29:7f:c3:a6), Dst: HuaweiTe_c9:9a:eb (54:39:df:c9:9a:eb)
⊞ Internet Protocol Version 4, Src: 192.89.11.188, Dst: 192.89.11.10
⊞ User Datagram Protocol, Src Port: 50168 (50168), Dst Port: 3799 (3799)
⊞ RADIUS Protocol
```

```
<Tolly_auth>dis access-user
------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
------------------------------------------------------------------------------
16080  00-10-94-00-00-22        10.1.1.11        0010-9400-0022 Success
16082  tolly                    -                0010-9410-0003 Success
16084  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
------------------------------------------------------------------------------
Total: 3, printed: 3
<Tolly_auth>
<Tolly_auth>dis access-user
------------------------------------------------------------------------------
UserID Username                 IP address       MAC            Status
------------------------------------------------------------------------------
16082  tolly                    -                0010-9410-0003 Success
16084  zhaoqianqian             192.89.17.109    3c97-0ed9-bd91 Success
------------------------------------------------------------------------------
Total: 2, printed: 2
```

Test 5.1	Endpoint Profiling with DHCP Packets
Objective	Verify endpoint profiling with DHCP packets when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. Configure terminal identification through DHCP on the ISE server. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The ISE server can identify terminals through DHCP.

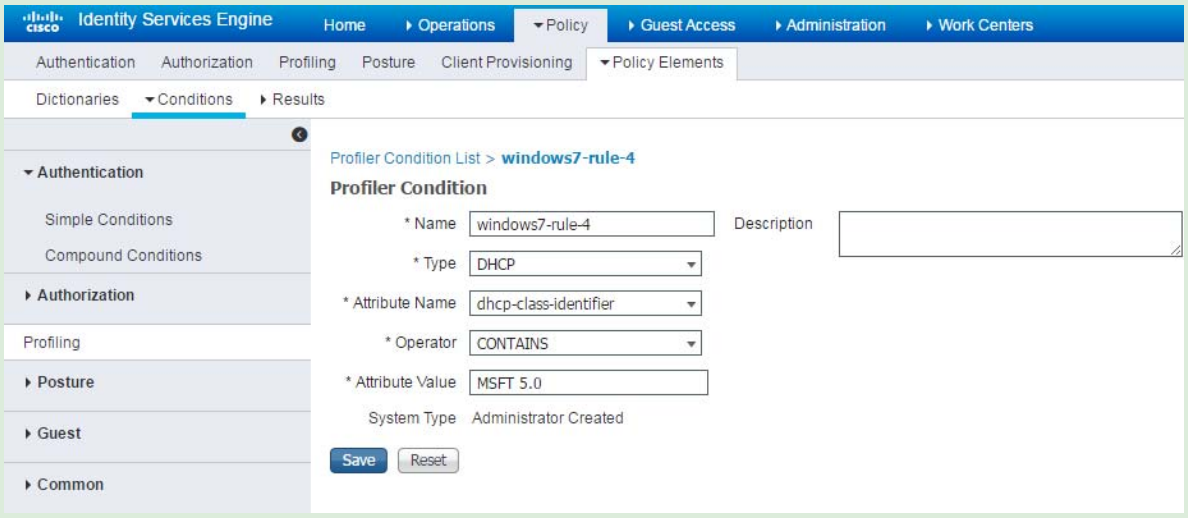
Test Results	Configuration: 1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. # radius-server template tolly_mac radius-server shared-key cipher huawei123 radius-server authentication 192.89.11.188 1812 weight 80 radius-server accounting 192.89.11.188 1813 weight 80 undo radius-server user-name domain-included calling-station-id mac-format hyphen-split mode2 radius-attribute set Service-Type 10 # domain tolly_mac authentication-scheme tolly authorization-scheme tolly radius-server tolly_mac # 3. Configure the aaa scheme. # aaa authentication-scheme tolly authentication-mode radius authorization-scheme tolly accounting-scheme tolly accounting-mode radius domain tolly_mac authentication-scheme tolly accounting-scheme tolly radius-server tolly_mac #

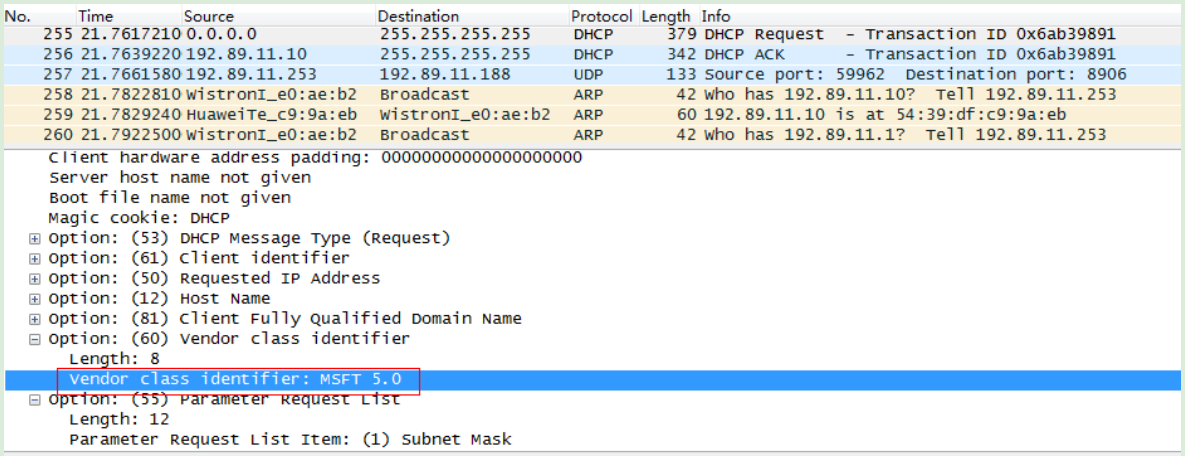
Test Results	4. Configure the MAC authentication profile on the device. # mac-access-profile name tolly mac-authen username macaddress format with-hyphen normal uppercase authentication-profile name tolly_mac mac-access-profile tolly access-domain tolly_mac # 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. # interface Vlanif4090 ip address 192.89.11.10 255.255.255.0 dhcp select interface # interface XGigabitEthernet1/0/0 port link-type hybrid port hybrid pvid vlan 4090 port hybrid untagged vlan 4090 authentication-profile tolly_mac # 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. Configure terminal identification through DHCP on the ISE server. Expected result 2 is displayed.

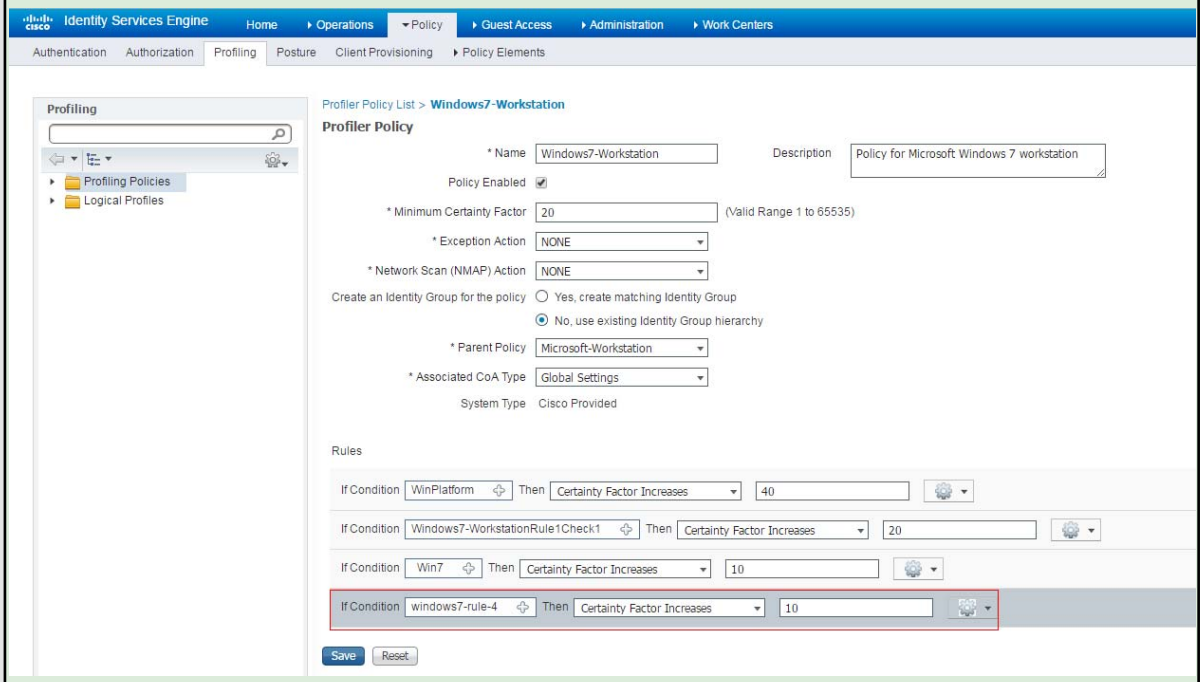
Test Results

Results:

1. Configure the DHCP attribute to identify the option field in the DHCP packets that match certain conditions.



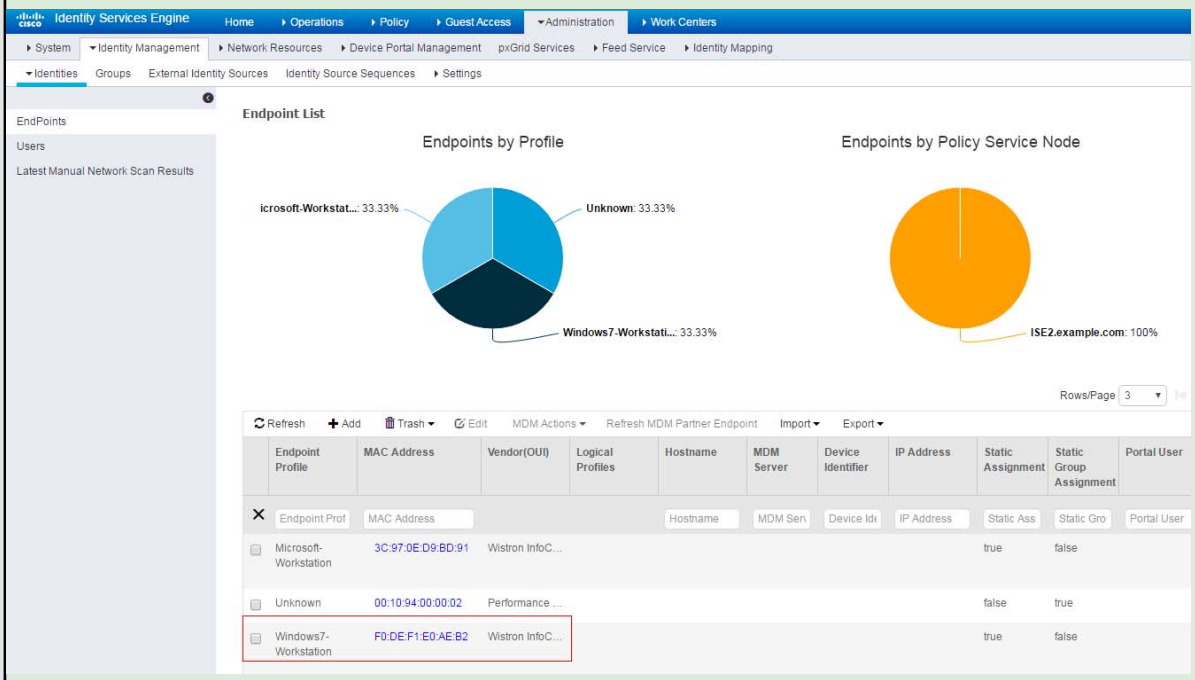


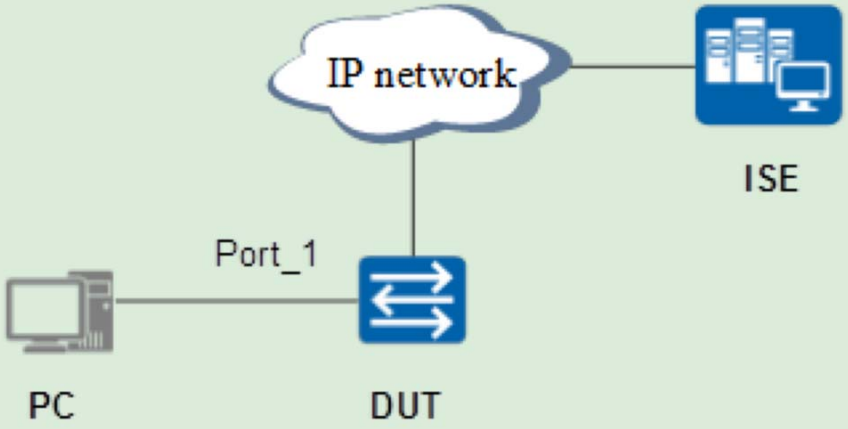
Test Results	2. Configure identification policies to invoke attribute identification conditions. 

Test Results

3. Users go online and identify terminal devices based on identification policies on the ISE server.

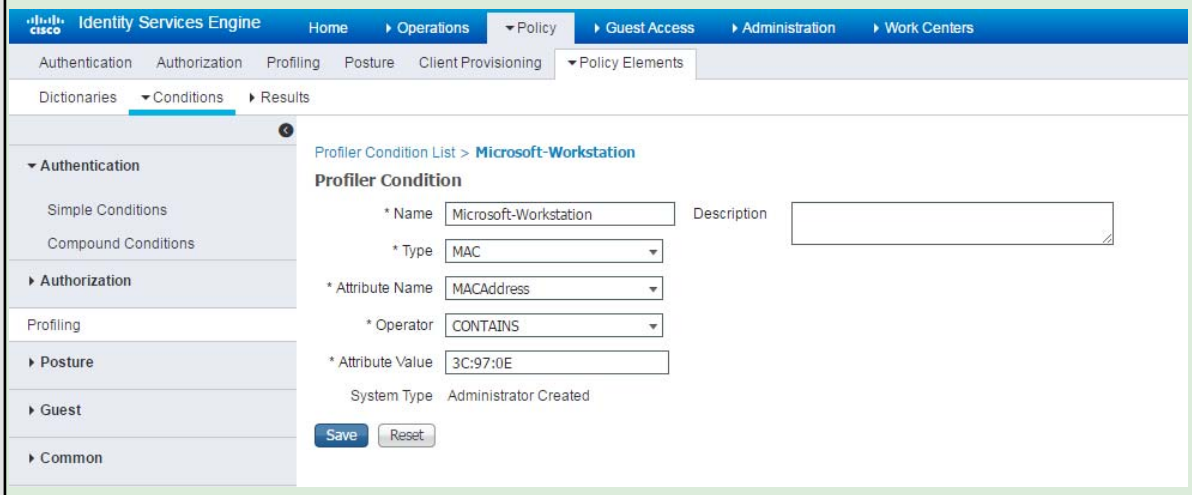
```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                  IP address       MAC            Status
 ------------------------------------------------------------------------------
 19127  F0-DE-F1-E0-AE-B2         192.89.11.253    f0de-f1e0-aeb2 Success
 19148  tolly1                    192.89.11.237    0010-9400-0011 Success
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
[Tolly_auth]dis access-user us
```

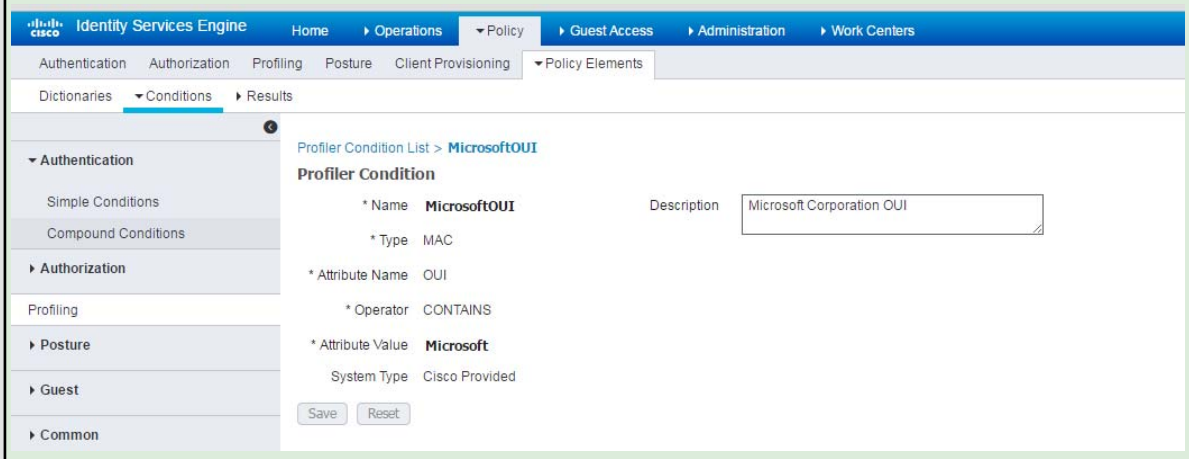


Test 5.2	Endpoint Profiling with MAC Addresses
Objective	Verify endpoint profiling with MAC addresses when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa profile on the switch. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent port. 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. Configure terminal identification through MAC address on the ISE server. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The ISE server can identify terminals through MAC addresses.

Test Results

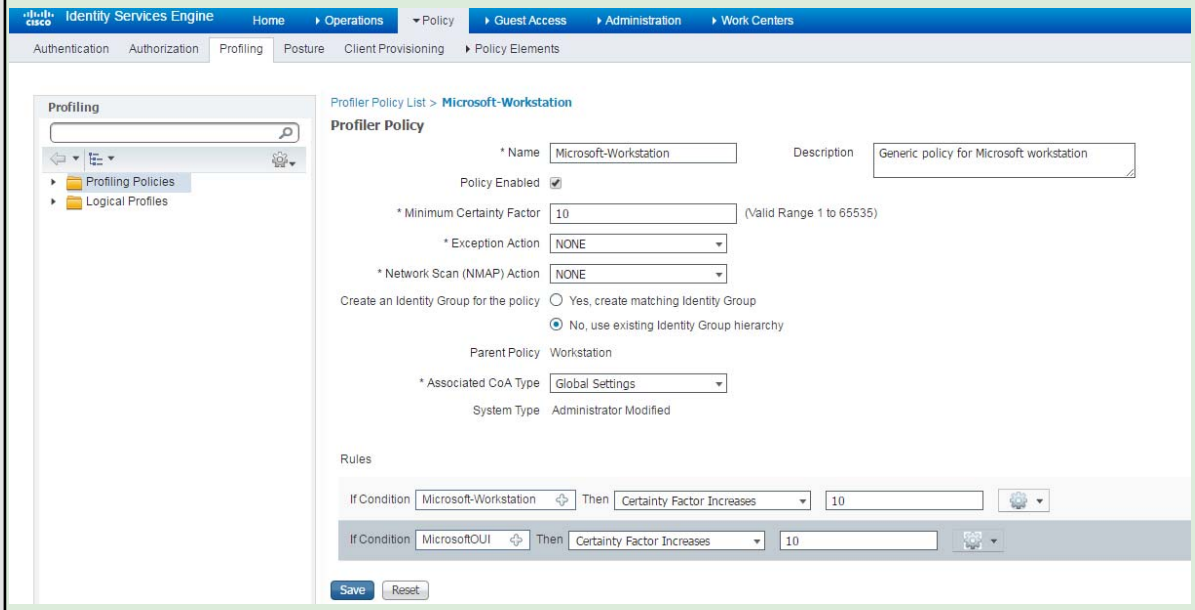
1. Configure the MAC address segment identification and specify the MAC address OUI provided by the ISE as the matching condition.





Test Results

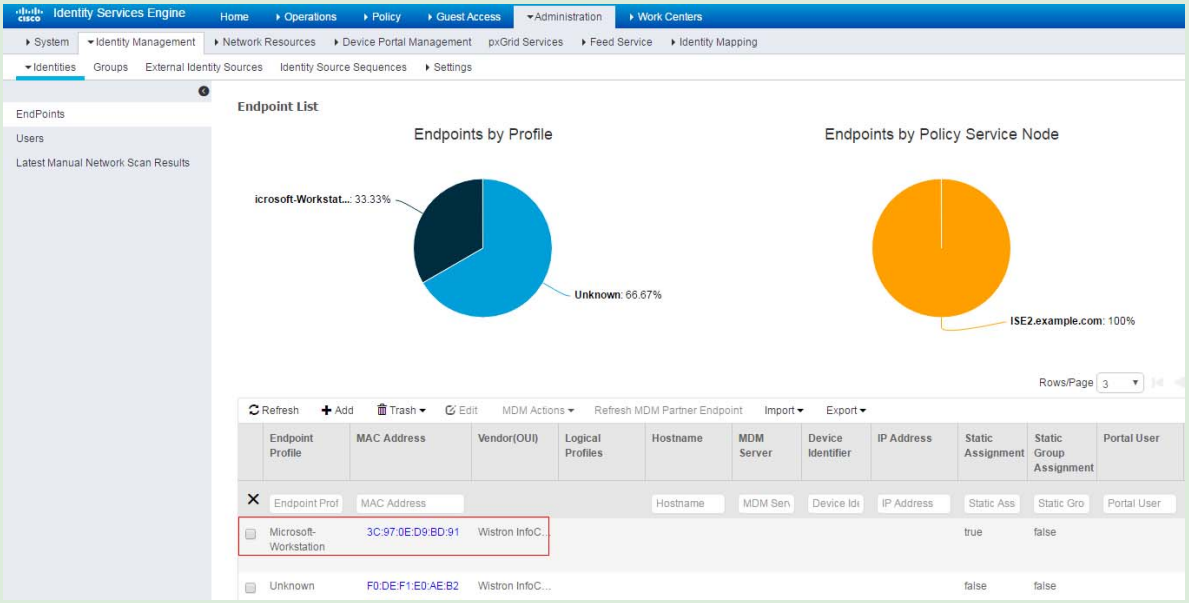
2. Configure identification policies to invoke attribute identification conditions.

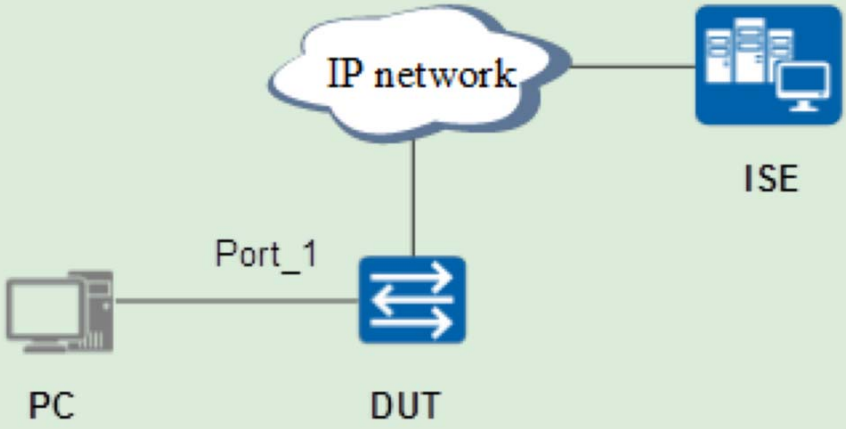


Test Results

3. Users go online and identify terminal devices based on identification policies on the ISE server.

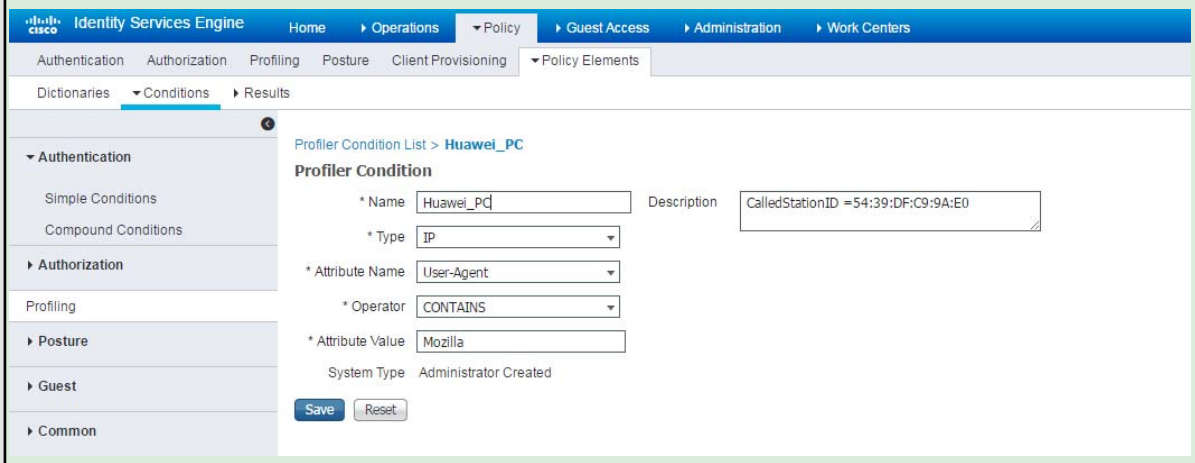
```
[Tolly_auth]dis access-user
--------------------------------------------------------------------------------
UserID Username                  IP address       MAC            Status
--------------------------------------------------------------------------------
19488  3C-97-0E-D9-BD-91         192.89.11.243    3c97-0ed9-bd91 Success
19490  tolly1                    192.89.11.173    0010-9400-0011 Success
19491  tolly                     192.89.11.253    f0de-f1e0-aeb2 Success
--------------------------------------------------------------------------------
Total: 3, printed: 3
```



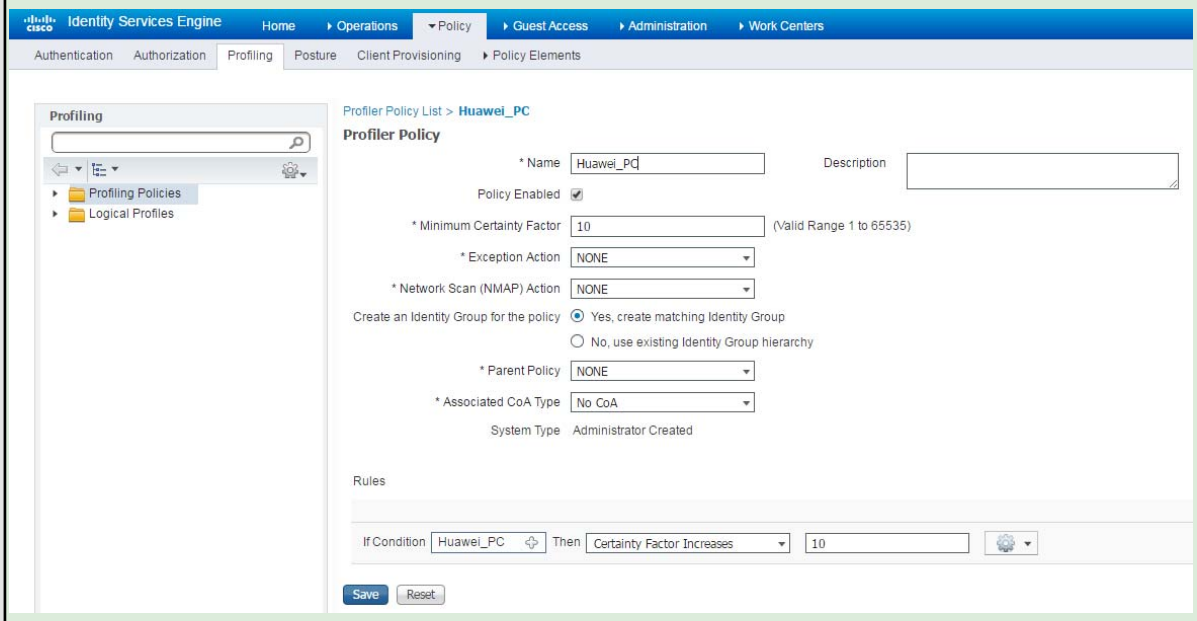
Test 5.3	Endpoint Profiling with HTTP Packets
Objective	Verify endpoint profiling with HTTP packets when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. When a user goes online after passing the MAC authentication, push the guest management page to him and allow him to exchange HTTP packets with the ISE server. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The ISE server can identify terminals through HTTP.

Test Results

1. Set the HTTP identification: User-Agent is the HTTP identifier of a device.

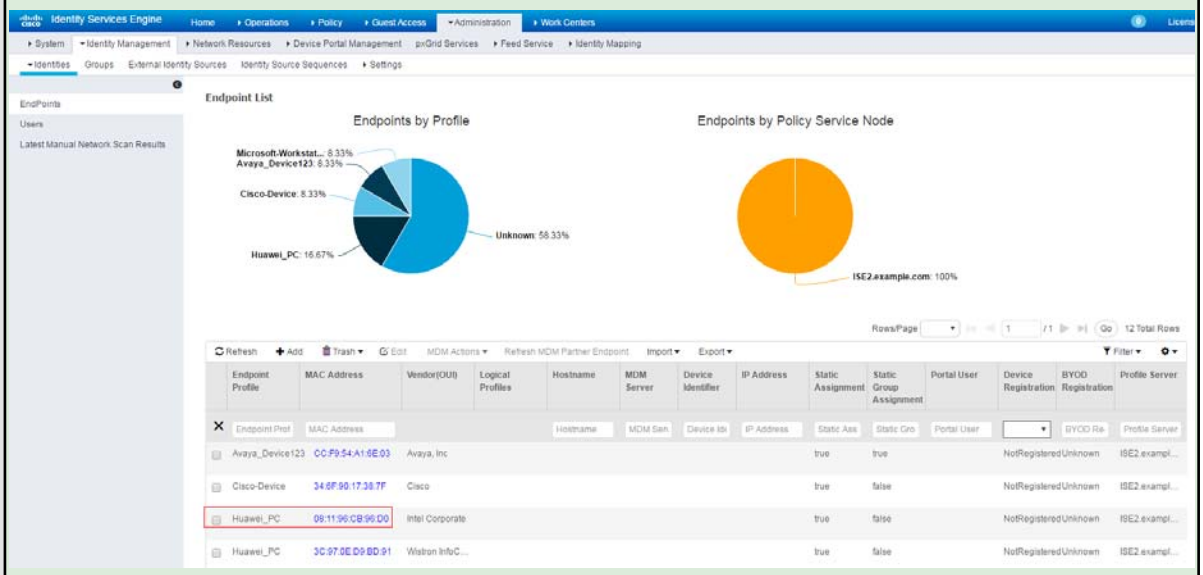


2. Configure identification policies to invoke attribute identification conditions.

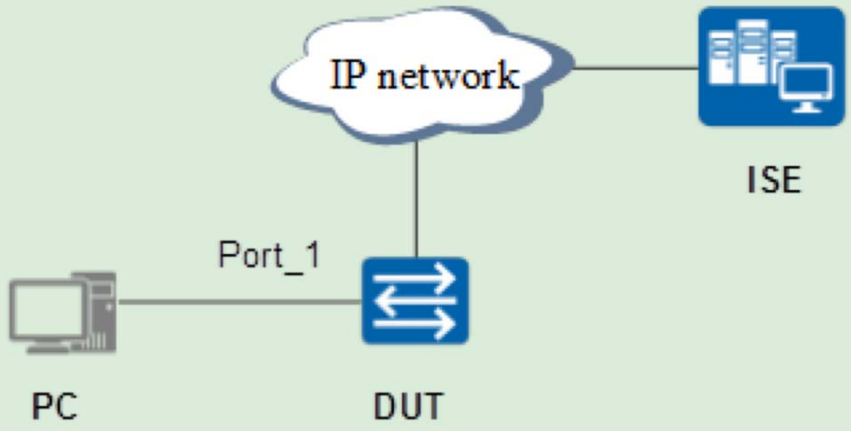


Test Results

3. Users go online and identify terminal devices based on identification policies on the ISE server.

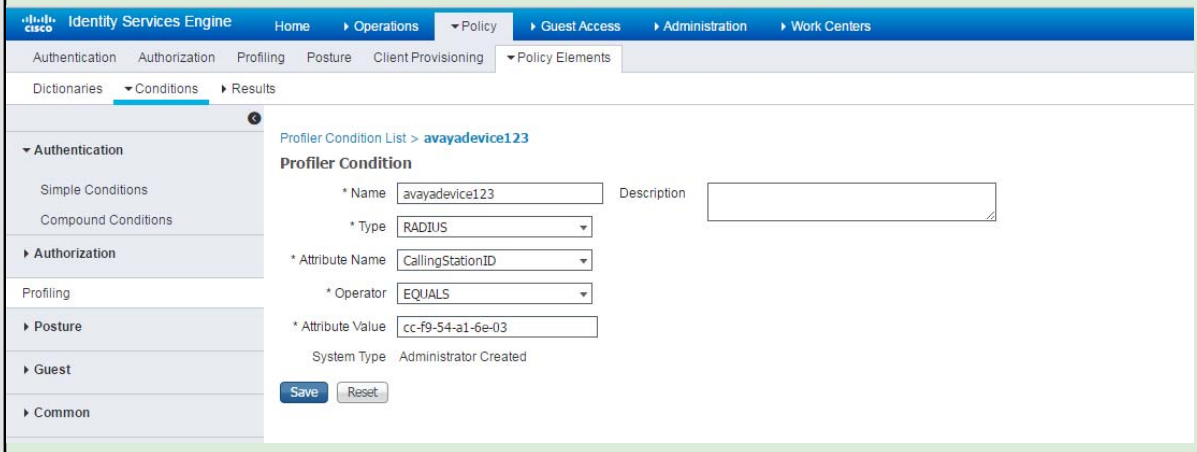



```
[Tolly_auth]dis access-user
------------------------------------------------------------------------------
UserID Username                  IP address       MAC            Status
------------------------------------------------------------------------------
16063  zhaoqianqian              192.89.17.109    3c97-0ed9-bd91 Success
16069  08-11-96-CB-96-D0         10.1.1.11        0811-96CB-96D0 Success
------------------------------------------------------------------------------
Total: 2, printed: 2
```

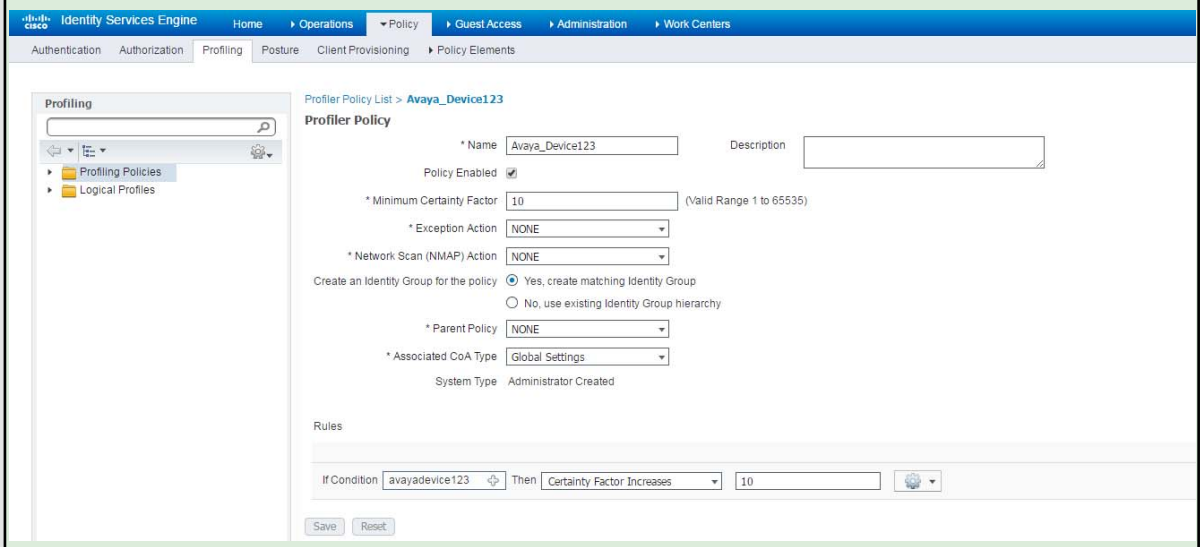
Test 5.4	Endpoint Profiling with RADIUS Packets
Objective	Verify endpoint profiling with RADIUS packets when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. Configure terminal identification through RADIUS on the ISE server. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The ISE server can identify terminals through RADIUS.

Test Results

1. Set the RADIUS identification: callingStationID is the MAC address of the device.



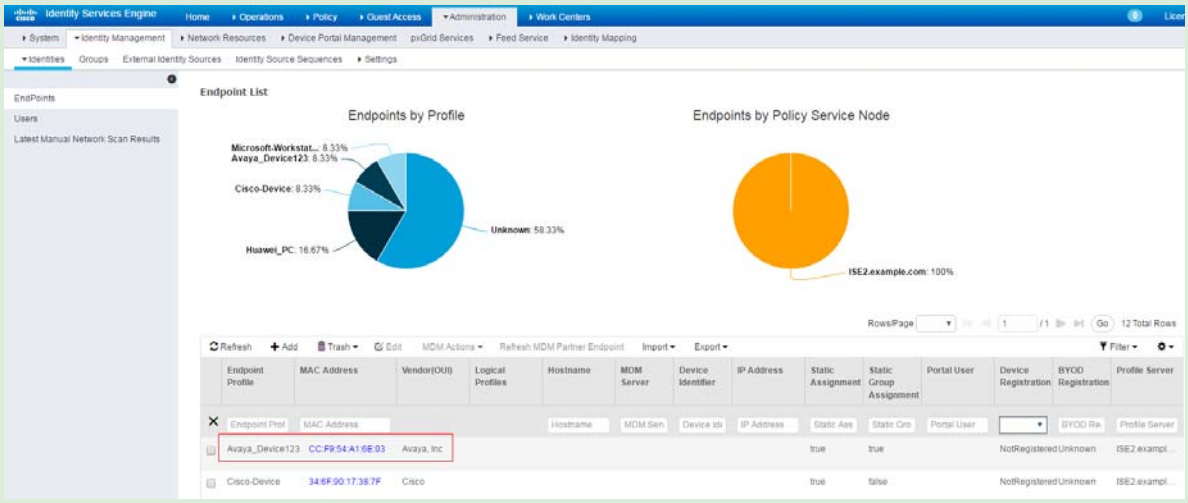
2. Configure identification policies to invoke attribute identification conditions.

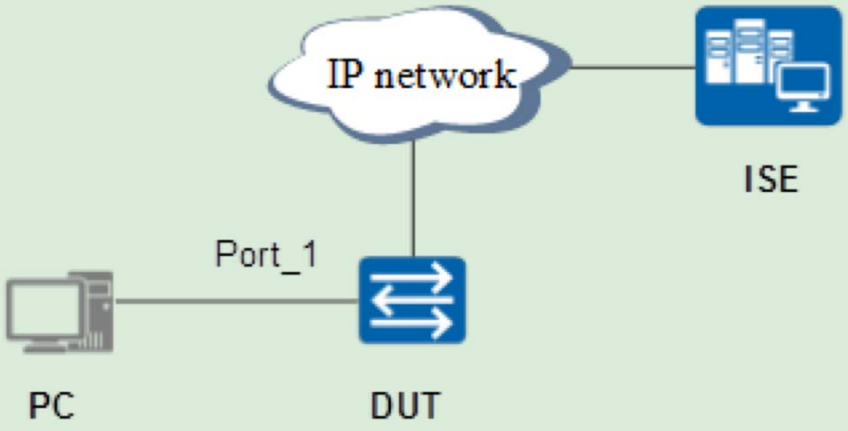


Test Results

3. Users go online and identify terminal devices based on identification policies on the ISE server.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 16169  CC-F9-54-A1-6E-03        10.1.1.11        CCF9-54A1-6E03 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```



Test 5.5	Network Scan (NMAP)
Objective	Verify network scan (NMAP) when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the RADIUS server profile and aaa profile on the switch. 3. Configure the aaa scheme. 4. Configure the MAC authentication profile on the device. 5. Configure the DHCP server on the device, and enable MAC authentication on the correspondent interface. 6. Connect the user terminal to the DUT and enable the MAC-authenticated port. Expected result 1 is displayed. 7. Set the SNMP write community password as huawei123, which matches configuration on the ISE. Configure Nmap scanning on the ISE server. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user passes the authentication successfully and obtains the correspondent IP address. The device shows that the authentication succeeds. Result 2: The ISE server identifies the device's IP address and MAC address, and identifies the terminal type based on the OUI.

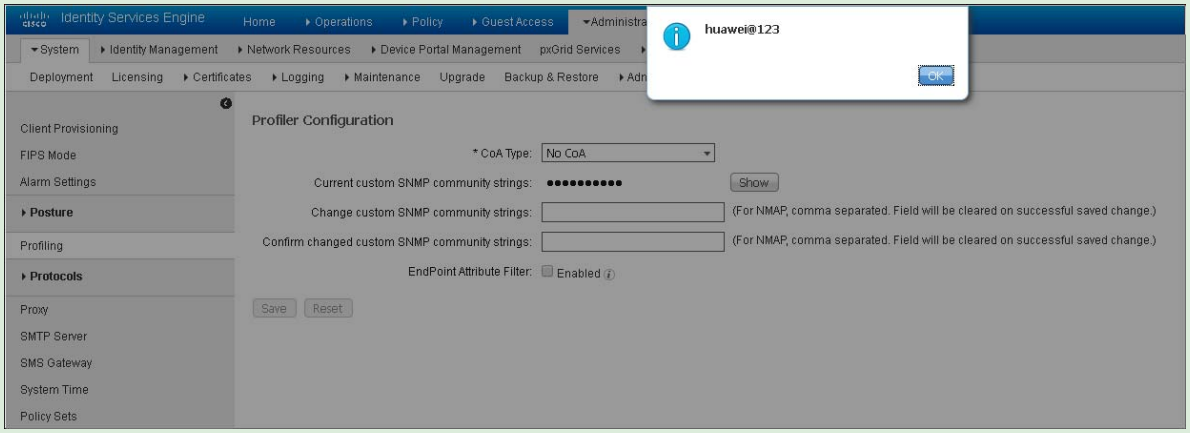
Test Results

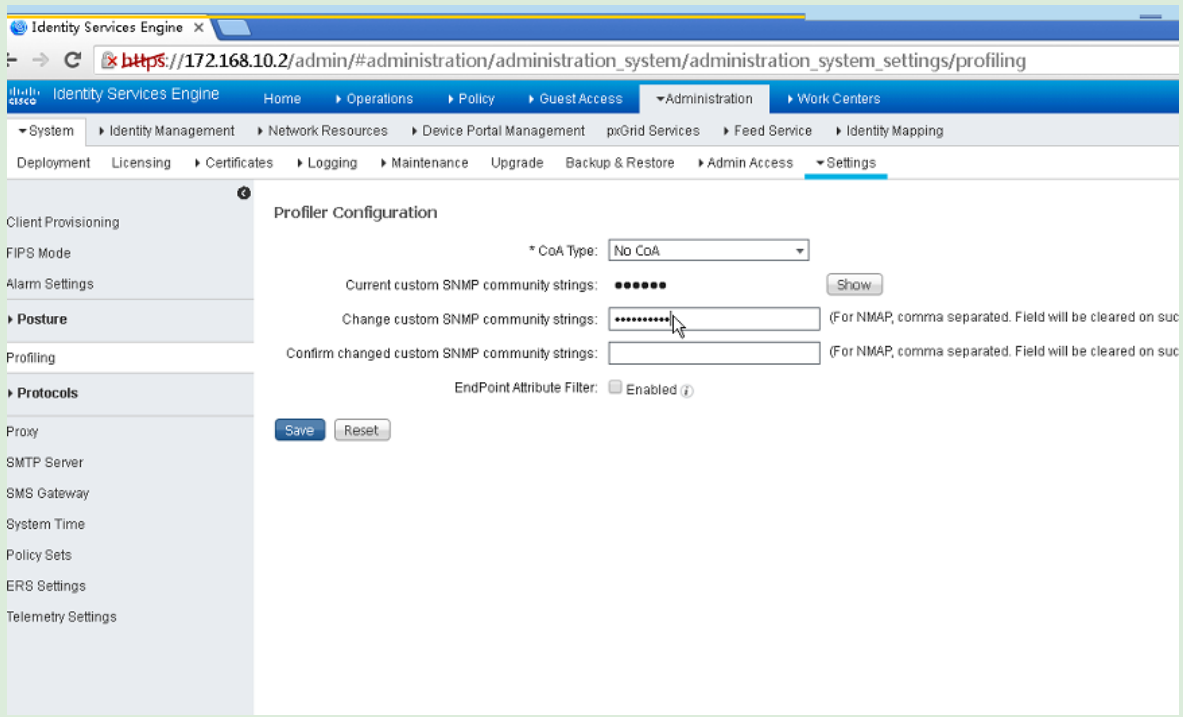
Configuration:

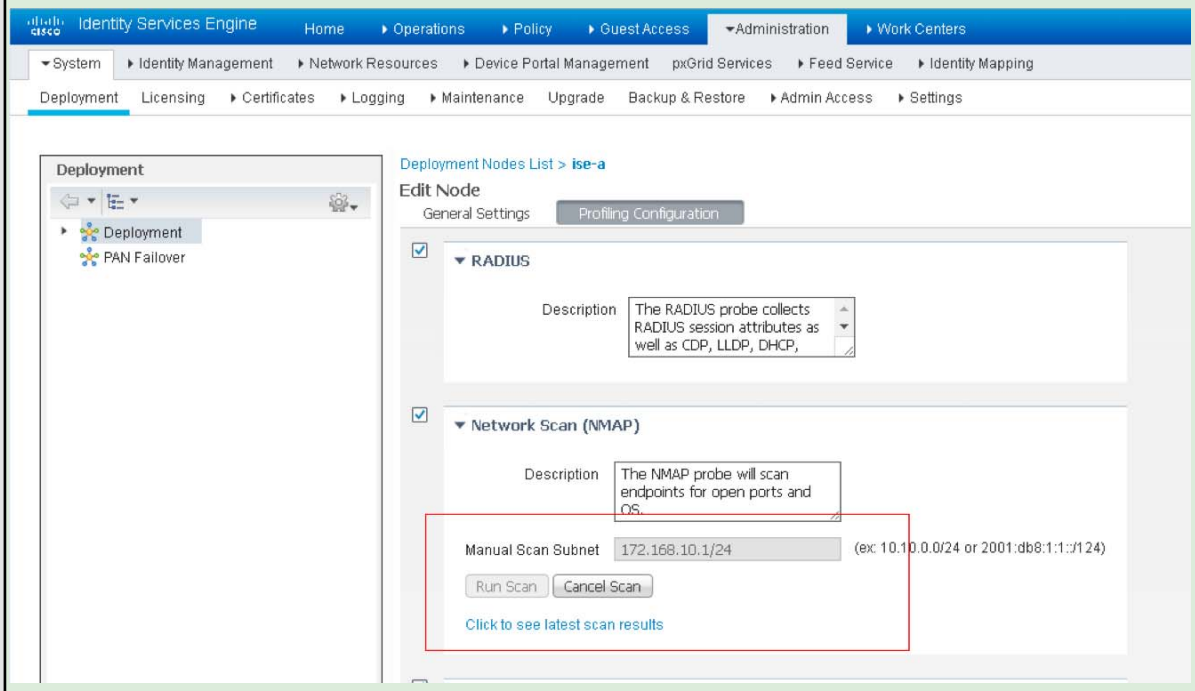
1. Configure the Huawei S switch.

```
[Tolly_auth]dis current-configuration  | include  snmp
snmp-agent
snmp-agent local-engineid 800007DB03FCE33C996AC0
snmp-agent community write cipher %^%#4VC@)IbjZ!!Uxf2YjI~Ca#_4.F;;WE@$P.9e0a+PL!
9u-v)>%'P-c#DLcTD(,nU1(kg_hXZSwR,o<xrB%^%#
snmp-agent sys-info version all
[Tolly_auth]_
```

Configure the Cisco ISE server

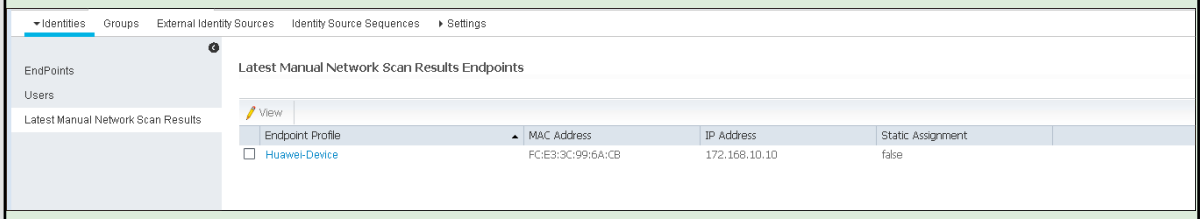


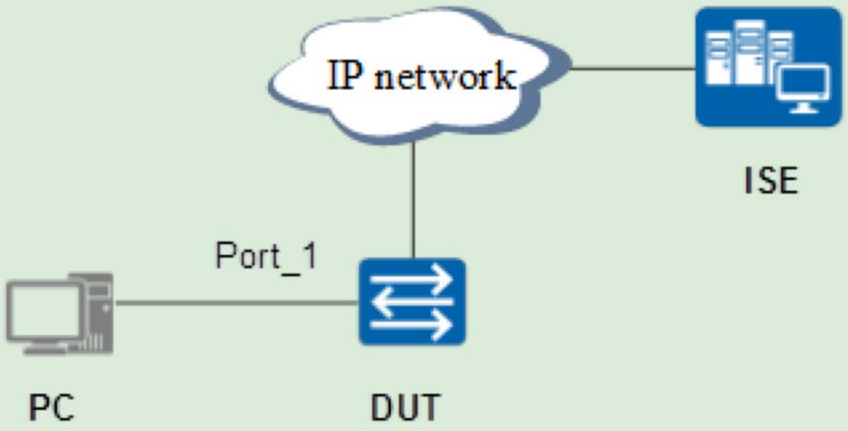




Test Results

2. Check the scanning result, and the device's IP address and MAC address are displayed. The terminal type is identified based on the OUI.



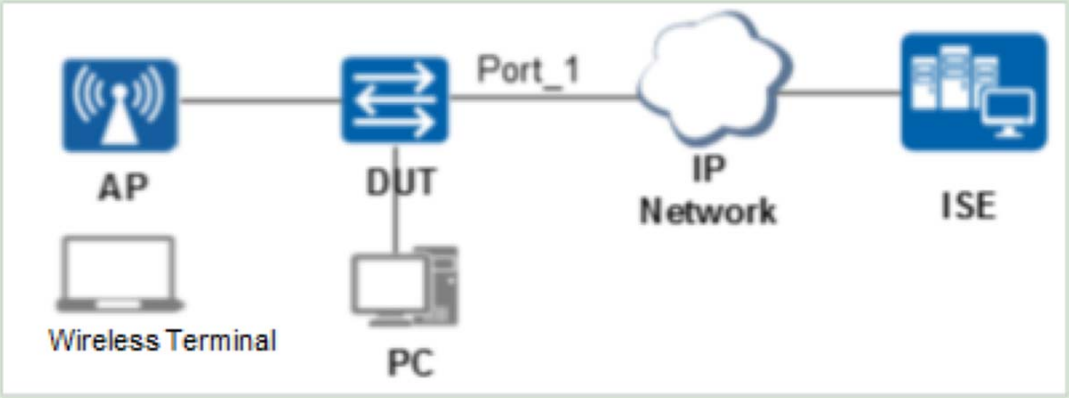
Test 6.1	Posture Assessment with the Cisco ISE and the Cisco NAC Appliance Agent
Objective	Verify posture assessment with a Huawei S switch works as the access control switch, the Cisco ISE server works as the authentication (RADIUS) server, and the Cisco NAC appliance agent.
Procedure	1. User terminals without the NAC-agent access the DUT in wired mode. Expected result 1 is displayed. 2. After the NAC-agent is installed, the agent checks the user terminals and sends the result to the ISE server. Expected result 2 is displayed. 3. The ISE server sends the CoA re-authentication to terminal devices that have passed the check. Expected result 3 is displayed. 
Pass Criteria	Result 1: The ISE server detects the lack of the NAC-agent on the device through MAC authentication, and delivers the redirection URL to the NAC-agent download page. The user terminal then downloads and installs the NAC-agent through the redirection URL. Result 2: When a terminal fails the check, the ISE server redirects the terminal to an URL for software repairing. The terminal check will not be ended until the terminal passes the check. Result 2: The device responds to CoA re-authentication, and the user's interface is authorized so that the user is granted the network access permission.

Test Results

1. After the user goes online, the server redirects the user to the URL of the cpp page.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                 IP address       MAC            Status
 ------------------------------------------------------------------------------
 19001  3C-97-0E-D9-BD-91        192.89.11.243    3c97-0ed9-bd91 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 19001

Basic:
  User ID                          : 19001
  User name                        : 3C-97-0E-D9-BD-91
  Domain-name                      : tolly_mac
  User MAC                         : 3c97-0ed9-bd91
  User IP address                  : 192.89.11.243
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet1/1/0
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/4090
  User access time                 : 2016/10/19 10:23:30
  User accounting session ID       : Tolly_a01100000000409065ccd80004a39
  Option82 information             : -
  User access type                 : MAC
  DHCP option ID                   : 12
  DHCP option content              : NJA131212947-ZO
  DHCP option ID                   : 55
  DHCP option content              : \001\017\003\006,./\037!y\371+
  DHCP option ID                   : 60
  DHCP option content              : MSFT 5.0
  Push URL content                 : https://192.89.11.188:8443/portal/gateway?se
                                     ssionId=c0590bbcYAHGFu5hV8PoPomYpx4i_uorlMev
                                     IUuDqBbAaWviC6g&portal=0d2ed780-6d90-11e5-97
                                     8e-005056bf2f0a&action=cpp&token=c618ac22017
                                     ae96df0162b0d17a4bf6a
  Terminal Device Type             : Data Terminal
  Redirect acl                     : 3001

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None
```

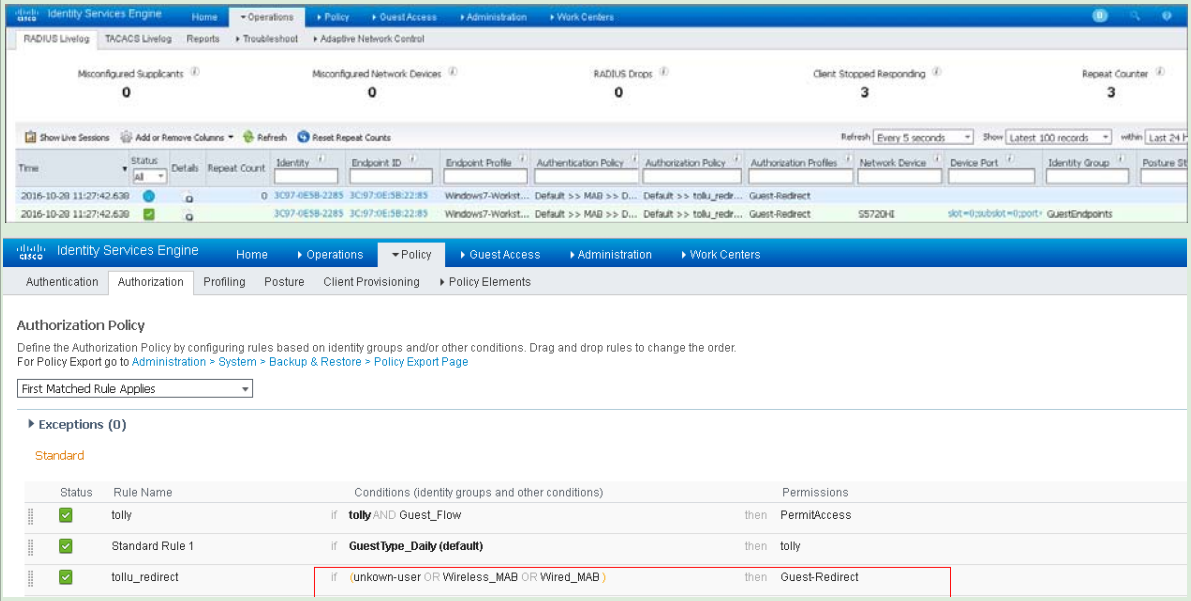
2. After opening the page, the user is redirected to the cpp page to check whether the NAC agent exists.
3. The NAC agent is installed successfully.
4. Start the NAC agent for terminal status check. Check whether the command is running. The check result shows that the command process has not been started, which indicates that the check fails.
5. Click Repair to invoke the command process and check the NAC agent again. The result shows that the check succeeds and network permissions are granted to the user.

Test 6.2	Guest Management (Guest self-registration and authentication)
Objective	Verify guest management when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server on the switch. 4. Configure the aaa profile. 5. Configure the MAC authentication profile. 6. Configure the CoA authorization server. 7. Configure the ACL redirection on the switch. 8. Users access the network in wired mode for MAC authentication. Expected result 1 is displayed. 9. Open a web page and access any website. Enter the user name and password for authentication. Expected result 2 is displayed. 
Pass Criteria	Result 1: When the user accesses the network for MAC authentication, the server delivers URL and redirection ACL. Open a browser and enter any IP address in the address bar, the page is redirected to the Portal authentication page. Result 2: After entering the user name and password, the user passes the Portal authentication successfully.

Test Results	1. When a new user accesses the network, he must pass the MAC authentication first. After the authentication succeeds, the page is redirected to the guest management page. A user can log in to the system using a registered account or a new user can register an account first.

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC            Status
 ------------------------------------------------------------------------------
 183    3C97-0E5B-2285          172.168.10.252   3c97-0e5b-2285 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 183

Basic:
  User ID                          : 183
  User name                        : 3C97-0E5B-2285
  Domain-name                      : tolly_mac
  User MAC                         : 3c97-0e5b-2285
  User IP address                  : 172.168.10.252
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet0/0/19
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/1720
  User access time                 : 2016/10/28 16:07:56
  User accounting session ID       : Tolly_a00019000001720da3e9f00000b7
  Option82 information             : -
  User access type                 : MAC
  Push URL content                 : https://172.168.10.2:8443/portal/gateway?ses
                                     sionID=aca80a02042zIxcJew_24YSREPVLLUJM1n4R3
                                     qpiGmAjkT6DrhE&portal=0ce17ad0-6d90-11e5-978
                                     e-005056bf2f0a&action=cwa&token=43584f976da7
                                     de40fb6c3c0fbd4e6983
  Terminal Device Type             : Data Terminal
  Redirect acl                     : 3001

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]_
```

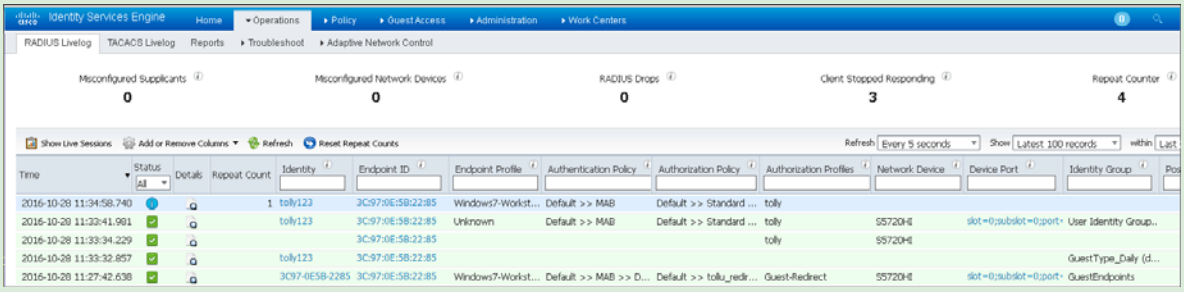
Test Results



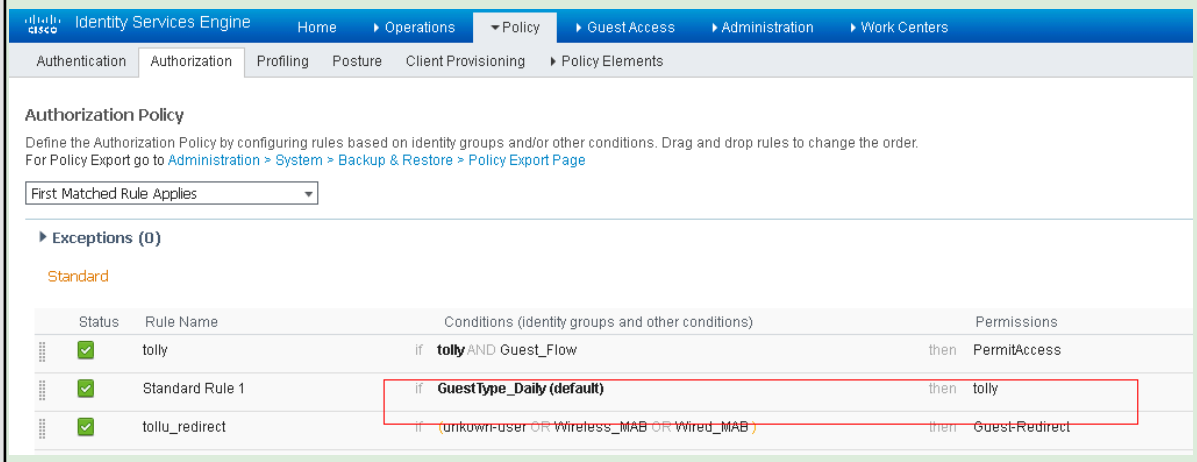
2. After a user registers an account, the system disconnect the user through CoA. The user should log in again using the new account.
3. After new users log in to the system, the server authorizes new policies to users so that they can obtain new permissions.

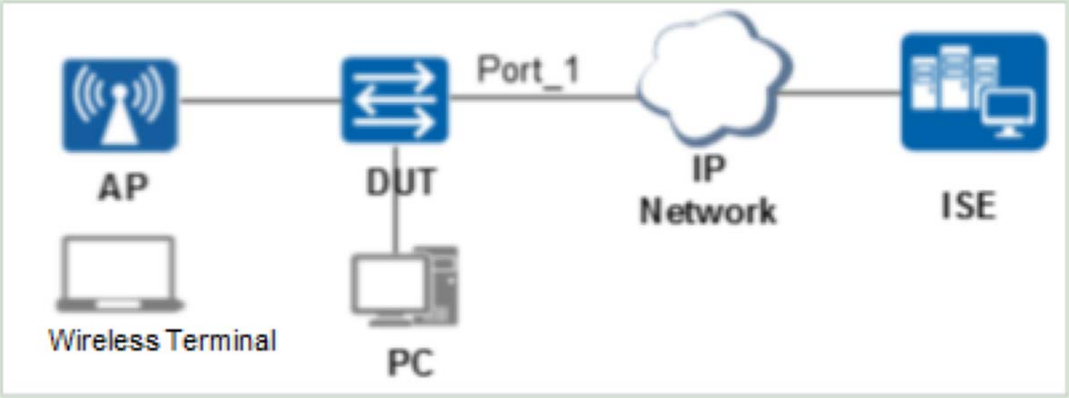
Test Results

```
[Tolly_auth]dis access-user
 ------------------------------------------------------------------------------
 UserID Username                  IP address       MAC            Status
 ------------------------------------------------------------------------------
 185    tolly123                  172.168.10.252   3c97-0e5b-2285 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
[Tolly_auth]dis access-user us
[Tolly_auth]dis access-user user
[Tolly_auth]dis access-user user-id 185

Basic:
  User ID                          : 185
  User name                        : tolly123
  Domain-name                      : tolly_mac
  User MAC                         : 3c97-0e5b-2285
  User IP address                  : 172.168.10.252
  User vpn-instance                : -
  User IPv6 address                : -
  User access Interface            : GigabitEthernet0/0/19
  User vlan event                  : Success
  QinQVlan/UserVlan                : 0/1720
  User access time                 : 2016/10/28 16:15:12
  User accounting session ID       : Tolly_a00019000001720a2f0ea00000b9
  Option82 information             : -
  User access type                 : MAC
  Terminal Device Type             : Data Terminal
  Dynamic ACL number(Effective)    : 3004
  Session Timeout                  : 65595(s)
  Termination Action               : OFFLINE

AAA:
  User authentication type         : MAC authentication
  Current authentication method    : RADIUS
  Current authorization method     : -
  Current accounting method        : None

[Tolly_auth]_
```



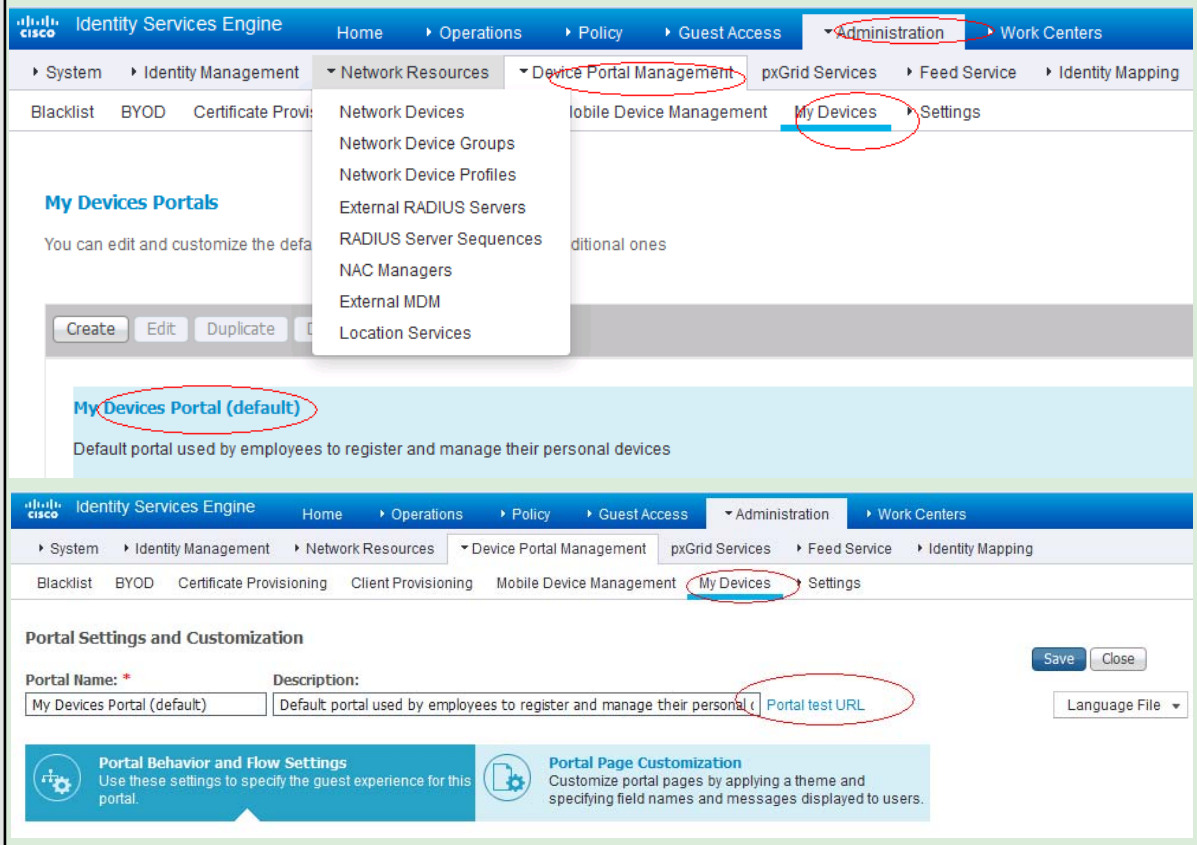
Test Results



Test 6.3	BYOD (BYOD device self-registration and authentication)
Objective	Verify BYOD when a Huawei S switch works as the access control switch and the Cisco ISE server works as the authentication (RADIUS) server.
Procedure	1. Configure the switch's IP address so that the switch can communicate with the ISE server. 2. Configure the management VLAN10, and assign IP addresses to APs. Configure network access for APs. 3. Configure the RADIUS server on the switch. 4. Configure the aaa profile. 5. Configure the MAC authentication profile. 6. Configure the CoA authorization server. 7. Configure the ACL redirection on the switch. 8. Register users on the ISE server. Expected result 1 is displayed. 9. Users access the network in wireless mode. Expected result 2 is displayed. 
Pass Criteria	Result 1: The user registers the access device on the ISE server successfully. Result 2: After entering the user name and password, the user passes the Portal authentication successfully.

Test Results

1. All internal employees must go to the specified website page (My Devices Portal) to register their own BYOD devices.



2. Enter an employee account.
3. Click Adding a Device.
4. Add a device, and the device ID must be the mobile phone's MAC address.
5. The user has registered the BYOD device successfully, and has to register again on the BYOD device when he uses the device to log in.
6. The mobile phone connects to the wireless network. After the user enters any website in the address bar of a browser, the webpage will be redirected to the ISE server's BYOD page.
7. Click Start to enter the registered user name. The ISE obtains the mobile phone's MAC address.
8. Click Continue to download the TLS certificate and configuration files from the ISE server for login.
9. After the certificate is installed, the ISE server disconnects the user through CoA. The mobile phone goes online after re-authentication and obtains the network access permission based on configuration files and the TLS certificate.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for over 25 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

216161-ivcofs15-yx-2017-02-14-VerA