Change of authorization

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Identity-Based Networking Services supports change of authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.

Information about change of authorization

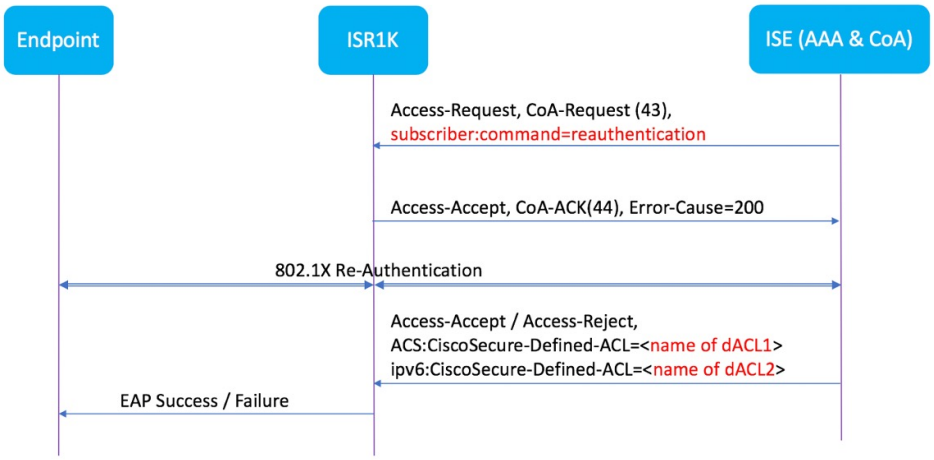
Change of authorization reauthentication procedure

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. The main steps in this procedure are:

- Authentication
- Posture Assessment
- CoA Re-Authentication
- Network Access Authorization

When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server, such as a Cisco Identity Secure Engine (ISE) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

The RADIUS CoA provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changed on user or user group in RADIUS server, administrators can initiate RADIUS CoA process from RADIUS server to re-authenticate or re-authorize new policy



By default, the RADIUS interface is enabled on the device. However, some basic configuration is required for the following attributes:

- Security and Password
- Accounting

After posture assessment is succeessful, full network access is pushed down to the device for specific client through CoA re-authentication command based on its compliance state derived from last assessment. It is optional to enforce downloadable ACLs with Permit-ALL or limited access to certain resources to corresponding clients. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

Change of authorization requests

Change of Authorization (CoA) is a critical part of a solution to initiate re-authenticate or re-authorization to an endpoint's network access based on its posture assessment result.

The network topology below shows a typical Cisco 8100 Series Secure Routers as a branch router in a network for secure access with ISE and other network services deployed in Campus or Data Center.

CoA is critical part of the solution to initiate re-authenticate or re-authorization to endpoint's network access based on its posture assessment result. Downloadable ACL is the Target/Purpose of the entire solution. The per-client basis customized security policies are achieved by it.

Restrictions for change of authorization

- Most of CoA and posture features heavily rely on HW TCAMs, such as Downloadable ACL (dACL), Redirect ACL (RACL) and SISF-based device tracking, which can only be supported on Cisco 8100 Series Secure Routers.

- Port ACL (PACL) is not supported on Cisco 8100 Series Secure Routers.
- IPv6 Access Control Entry (ACE) is not supported.
- IPv4 ACE can neither support IPv4 option header nor IP fragment match.
- IPv4 ACE can support TCP/UDP L4 port# match, but only with eq (=) or any (*) match. gt (>), lt (<) or range (A-to-B) is not supported.
- For C8130-G2:
  - Scale up to 128 dACL ACEs and up to 64 RACL ACEs are shared between all switchports.
  - IPv4 ACE L4 match can only support TCP/UDP port# match.
- For C8140-G2, C8151-G2, C8161-G2:
  - Scale up to 2048 dACL ACEs and up to 512 RACL ACEs shared between all switchports.
  - IPv4 ACE L4 match can only support TCP/UDP port# match, and L4 Flags with match-all (no match-any) option.
- SISF-based device tracking policy can support IPv4 address glean (using security-level glean) and tracking (using tracking enable).
- Multi-auth per user VLAN assignment is not supported.
- NEAT/CISP is not supported.

How to configure change of authorization

Essential dot1x|SANet configuration

Procedure

Example:

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
 server name coa
radius server coa
 address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
 key cisco123
policy-map type control subscriber simple_coa
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
interface gigabitethernet0/1/0
 switchport access vlan 22
 switchport mode access
```

```
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
service-policy type control subscriber simple_coa
```

Configure change of authorization

```
aaa server radius dynamic-author
 client
 server-key ******
 auth-type any
 ignore server-key
ip access-list extended redirect_acl
 20 deny udp any eq bootps any
 25 deny udp any eq domain any
 30 deny udp any any eq bootpc
 40 deny udp any eq bootpc any
 50 deny ip any host %{ise.ip}
 60 permit tcp any any eq www
 70 permit tcp any any eq 443
device-tracking tracking
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
interface 0/1/0
 device-tracking attach-policy tracking_test
```

Configuration examples for change of authorization

Check if the RADIUS server is active

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.10.10.1, auth-port 1812, acct-port 1813, hostname host
     State: current UP, duration 188755s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

Device tracking policy

```
Device# show aaa group radius coa3 **** port 1813 new-code
User successfully authenticated
USER ATTRIBUTES
username             0   "coa3"
```

To check if the parameters are enabled:

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
```

```
Gi0/1/1              PORT  tracking_test        Device-tracking vlan all
Gi0/1/2              PORT  tracking_test        Device-tracking vlan all
Gi0/1/3              PORT  tracking_test        Device-tracking vlan all
Gi0/1/4              PORT  tracking_test        Device-tracking vlan all
```

To check the SISF table:

```
Device# show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
Network Address        Link Address       Interface  vlan  prlvl    age    state       Time
 left
ARP 10.11.22.20       0050.5683.3f97      Gi0/1/4     22    0005    11s   REACHABLE
295 s
```

To check if the access-session is authenticated and autorized:

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
            Interface:  GigabitEthernet0/1/7
               IIF-ID:  0x0DB9315A
          MAC Address:  b496.913d.4f9b
         IPv6 Address:  Unknown
         IPv4 Address:  10.10.22.27
            User-Name:  coa2
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  611C4B0A00000053F483D7B0
      Acct Session ID:  Unknown
               Handle:  0x21000049
       Current Policy:  POLICY_COA
   Server Policies:  Filter-ID: Filter_ID_COA2
   Method status list:  Method           State
                        dot1x           Authc Success
```