CoA - Change Of Authorization

Mist
AI is in the AIR™

Why CoA

- The RADIUS protocol, defined in [RFC2865], does not support unsolicited messages sent from the RADIUS server to the Network Access Server (NAS).

- However, there are many instances in which it is desirable for changes to be made to session characteristics, without requiring the NAS to initiate the exchange.

- For example, it may be desirable for administrators to be able to terminate user session(s) in progress. Alternatively, if the user changes authorization level, this may require that authorization attributes be added/deleted from user sessions.

- To overcome these limitations, several vendors have implemented additional RADIUS commands in order to enable unsolicited messages to be sent to the NAS. These extended commands provide support for Disconnect and Change-of-Authorization (CoA) packets.

Messages

1. Disconnect Message
   a. Session Termination

AVP: Acct-Terminate-Cause
Value: Admin-Reset

```
+----------+                                +----------+
|          |   Disconnect-Request           |          |
|          |   <--------------------        |          |
|   NAS    |                                |   DAC    |
|          |   Disconnect-ACK/NAK           |          |
|          |   --------------------->       |          |
+----------+                                +----------+
```

1844	2018-11-20 18:46:49.328865	192.168.8.11	192.168.8.57	RADIUS	146	Disconnect-Request id=9
1845	2018-11-20 18:46:49.341454	192.168.8.57	192.168.8.11	RADIUS	86	Disconnect-ACK id=9

```
▶ Frame 1844: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_2e:21:c5 (5c:5b:35:2e:21:c5)
▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.57
▶ User Datagram Protocol, Src Port: 11474, Dst Port: 3799
▼ RADIUS Protocol
    Code: Disconnect-Request (40)
    Packet identifier: 0x9 (9)
    Length: 104
    Authenticator: a6e95d87167098b954e5e472db344cb0
    [The response to this request is in frame 1845]
  ▼ Attribute Value Pairs
    ▶ AVP: t=NAS-IP-Address(4) l=6 val=192.168.8.57
    ▶ AVP: t=Calling-Station-Id(31) l=19 val=68-EC-C5-09-2E-69
    ▼ AVP: t=Acct-Terminate-Cause(49) l=6 val=Admin-Reset(6)
        Type: 49
        Length: 6
        Acct-Terminate-Cause: Admin-Reset (6)
    ▼ AVP: t=Event-Timestamp(55) l=6 val=Nov 20, 2018 10:46:49.000000000 PST
        Type: 55
        Length: 6
        Event-Timestamp: Nov 20, 2018 10:46:49.000000000 PST
    ▶ AVP: t=Message-Authenticator(80) l=18 val=2701a9e759fa25f15d56e1a50f4ab250
    ▶ AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
```

Messages

2. CoA: Session Re-authentication
   AVP: Vendor Specific (Cisco-AVP)
   Value: Reauthenticate

RFC 5176 Dynamic Authorization Extensions to RADIUS

```
+----------+                                +----------+
|          |      CoA-Request               |          |
|          |<-------------------            |          |
|   NAS    |                                |   DAC    |
|          |     CoA-ACK/NAK                |          |
|          |------------------------------> |          |
+----------+                                +----------+
```

3888	2018-12-13 21:27:13.578009	10.2.15.254	10.2.10.13	RADIUS	271 CoA-Request id=37
3889	2018-12-13 21:27:13.583400	10.2.10.13	10.2.15.254	RADIUS	86 CoA-ACK id=37
3890	2018-12-13 21:27:13.585375	10.2.10.13	10.2.15.254	RADIUS	205 Access-Request id=1
3892	2018-12-13 21:27:13.599993	10.2.15.254	10.2.10.13	RADIUS	286 Access-Accept id=1

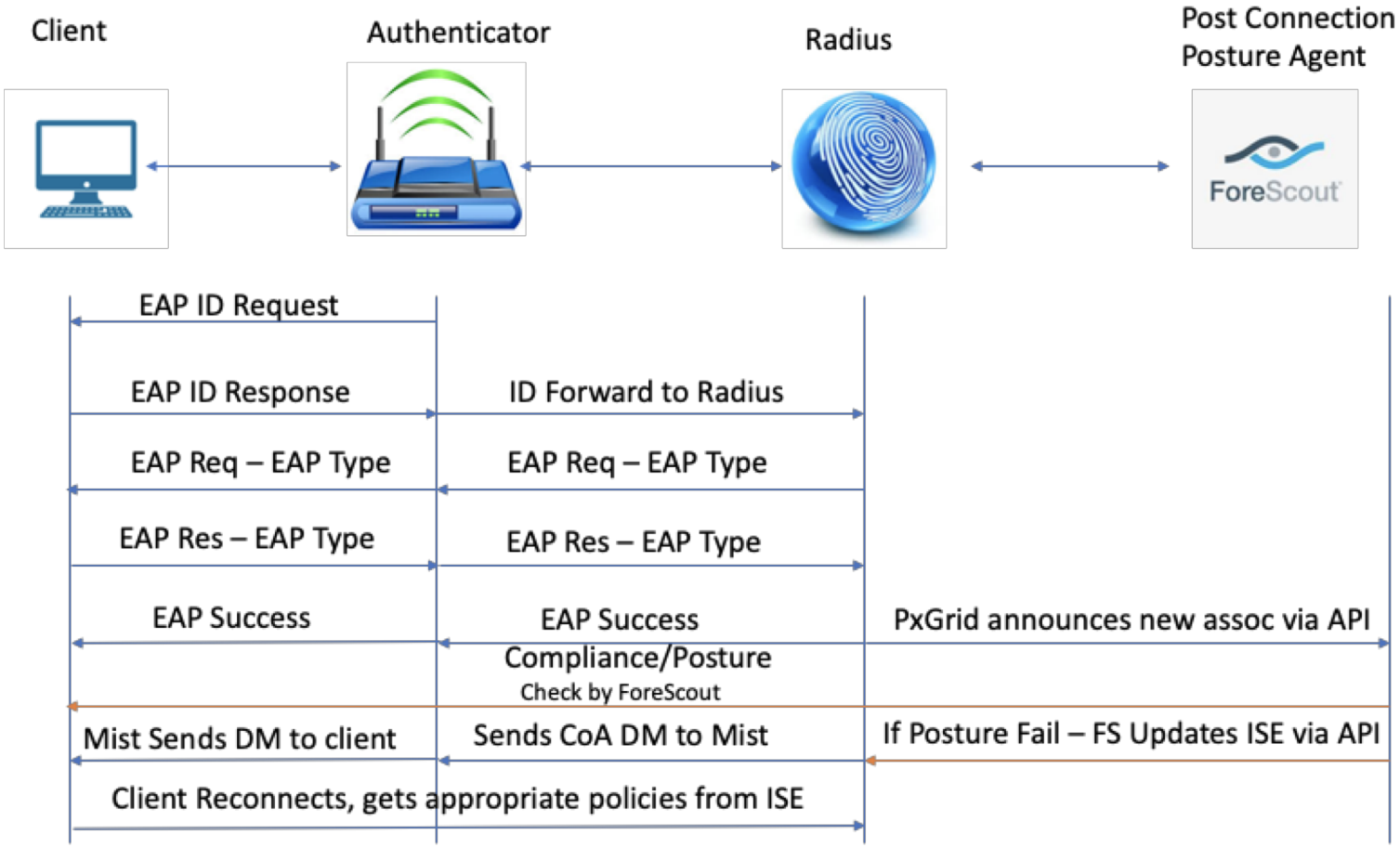
```
▶ Frame 3888: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits)
▶ Ethernet II, Src: Microsof_b2:e8:0e (00:15:5d:b2:e8:0e), Dst: Mist_3e:d2:28 (5c:5b:35:3e:d2:28)
▶ Internet Protocol Version 4, Src: 10.2.15.254, Dst: 10.2.10.13
▶ User Datagram Protocol, Src Port: 21779, Dst Port: 3799
▼ RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x25 (37)
    Length: 229
    Authenticator: 8224d751dab908cccc8fe58124fd140d
    [The response to this request is in frame 3889]
  ▼ Attribute Value Pairs
    ▶ AVP: t=NAS-IP-Address(4) l=6 val=10.2.10.13
    ▶ AVP: t=Calling-Station-Id(31) l=19 val=F0-18-98-57-5D-E4
    ▶ AVP: t=Event-Timestamp(55) l=6 val=Dec 13, 2018 13:27:13.000000000 PST
    ▶ AVP: t=Message-Authenticator(80) l=18 val=27bc61454f9bcc5339beb12f16e43ded
    ▼ AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
        Type: 26
        Length: 43
        Vendor ID: ciscoSystems (9)
      ▶ VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
    ▼ AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
        Type: 26
        Length: 41
        Vendor ID: ciscoSystems (9)
      ▶ VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
    ▼ AVP: t=Vendor-Specific(26) l=76 vnd=ciscoSystems(9)
        Type: 26
        Length: 76
        Vendor ID: ciscoSystems (9)
      ▶ VSA: t=Cisco-AVPair(1) l=70 val=audit-session-id=0a020ffeCTLnZbHwvQwBBLHh606hq/tfezmNVnP9NWDx8Deke64
```

Few other CoA Messages which are not applicable to us:

a. Session termination with Port-Shut (Not Applicable for us)
b. Session termination with Port-Bounce (Not applicable for us)

CoA Applications/Use Cases

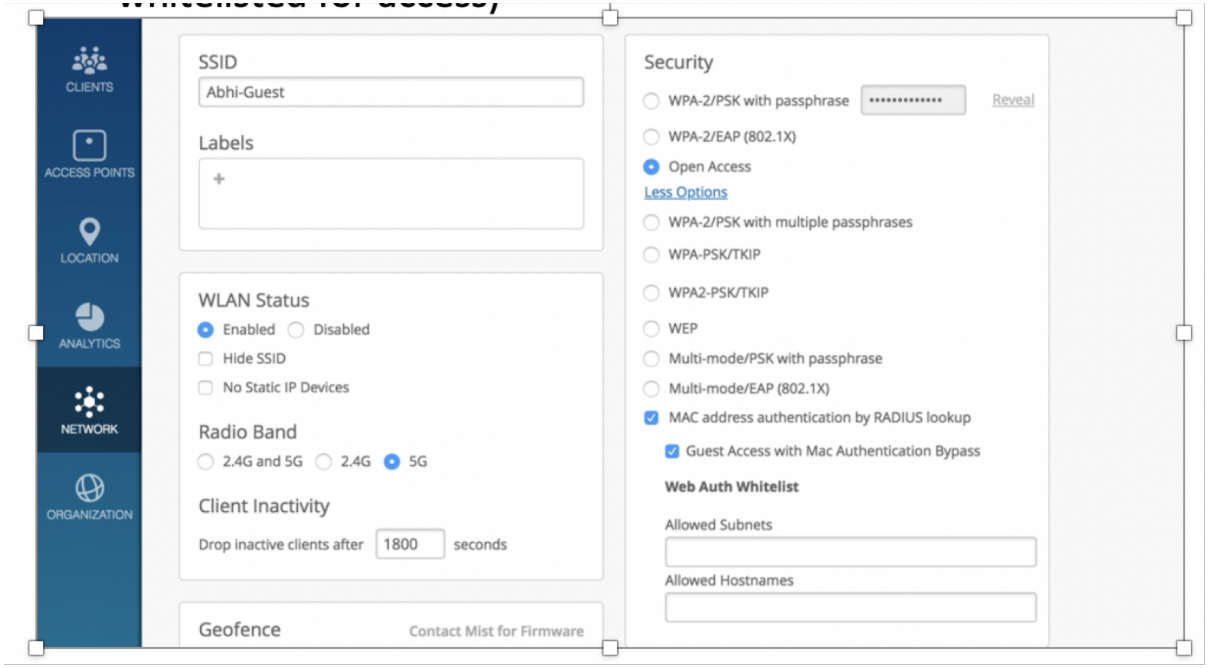
Disconnect Message: Posturing

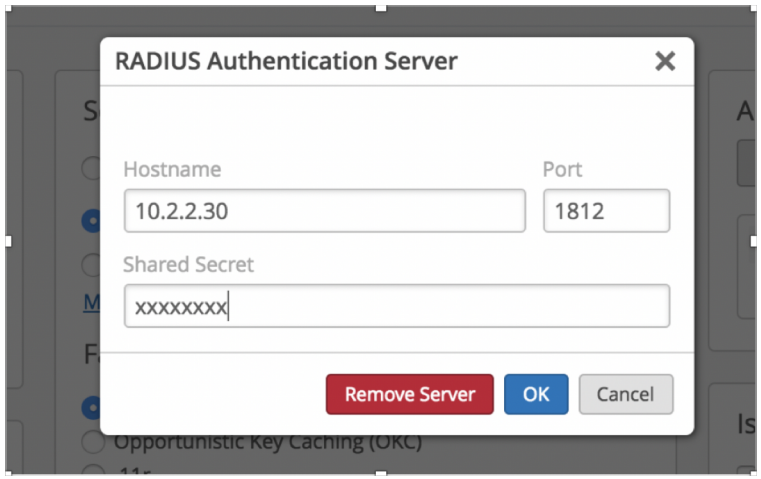


CoA Applications/Use Cases

CoA-ReAuth Message: Guest Access

a) Configuration from Mist





Guest Access: Access-Request1

No.	Time	Source	Destination	Length	Protocol	Size	TX Rate	RSSI	Channel	Info
239	2018-08-17 17:52:51.457672	172.24.89.150	155.64.42.55	208	RADIUS	208				Access-Request(1) (id=0, l=166)
240	2018-08-17 17:52:51.464048	155.64.42.55	172.24.89.150	643	RADIUS	643				Access-Accept(2) (id=0, l=601)
1266	2018-08-17 17:53:26.048774	155.64.42.55	172.24.89.150	271	RADIUS	271				CoA-Request(43) (id=5, l=229)
1267	2018-08-17 17:53:26.094516	172.24.89.150	155.64.42.55	86	RADIUS	86				CoA-ACK(44) (id=5, l=44)
1268	2018-08-17 17:53:26.114376	172.24.89.150	155.64.42.55	208	RADIUS	208				Access-Request(1) (id=1, l=166)
1269	2018-08-17 17:53:26.121090	155.64.42.55	172.24.89.150	643	RADIUS	643				Access-Accept(2) (id=1, l=601)

```
▶ Frame 239: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
▶ Ethernet II, Src: Cisco_ff:fd:94 (00:08:e3:ff:fd:94), Dst: Cisco_6c:d6:c0 (2c:33:11:6c:d6:c0)
▶ Internet Protocol Version 4, Src: 172.24.89.150, Dst: 155.64.42.55
▶ User Datagram Protocol, Src Port: 55567, Dst Port: 1812
▼ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 166
    Authenticator: b0d3e5b86fa3f3809c63ade4179aa727
    [The response to this request is in frame 240]
  ▼ Attribute Value Pairs
    ▼ AVP: l=14 t=User-Name(1): f48c507eb0c6
        Type: 1
        Length: 14
        User-Name: f48c507eb0c6
    ▼ AVP: l=18 t=User-Password(2): Encrypted
        Type: 2
        Length: 18
        User-Password (encrypted): 2d4a4987a89674cda41683a4f2561295
    ▶ AVP: l=6 t=Service-Type(6): Call-Check(10)
    ▶ AVP: l=35 t=Called-Station-Id(30): 5C-5B-35-20-0B-83:SYMC-Guest_test
    ▶ AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
    ▶ AVP: l=19 t=Calling-Station-Id(31): F4-8C-50-7E-B0-C6
    ▶ AVP: l=24 t=Connect-Info(77): CONNECT 11Mbps 802.11b
    ▶ AVP: l=6 t=NAS-IP-Address(4): 172.24.89.150
    ▶ AVP: l=18 t=Message-Authenticator(80): 17d233522f93491677a37bc7122993b6
```

Guest Access: ISE Policy

ISE Policy Stage 1:

If user not found, continue by providing limited access and Splash Page

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits
Search				
	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP	48

Wi-Fi_Guest_Access	AND	IdentityGroup·Name EQUALS Endpoint Identity Groups:HotSpot_Endpoints Wireless_MAB	PermitAccess	Select from list	0	
Wi-Fi_Redirect_to_Guest_Login		Wireless_MAB	Guest_Access	Select from list	47	
Basic_Authenticated_Access		Network_Access_Authentication_Passed	PermitAccess	Select from list	0	
Default			DenyAccess	Select from list	0	

Guest Access: Authz Policy

Authorization Profiles

Downloadable ACLs

- Profiling
- Posture
- Client Provisioning

Common Tasks

Centralized Web Auth | ACL: ACL_WEBAUTH_REDIRECT | Value: Sponsored Guest Portal (defau

- [x] Display Certificates Renewal Message
- [x] Static IP/Host name/FQDN: 10.2.15.254
- [ ] Suppress Profiler CoA for endpoints in Logical Profile

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect-acl=ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://10.2.15.254:port/portal/gateway?sessionId=SessionIdValue&portal=f079c670-7159-11e7-a355-005056aba474&daysToExpiry=value&action=cwa
```

Guest Access: Access-Accept1

```
310 2018-08-17 17:43:22.978274   192.168.8.42   192.168.8.11   204 RADIUS   204   Access-Request(1) (id=12, l=162)
311 2018-08-17 17:43:23.015352   192.168.8.11   192.168.8.42   581 RADIUS   581   Access-Accept(2) (id=12, l=539)
473 2018-08-17 17:43:27.902296   192.168.8.42   192.168.8.11   204 RADIUS   204   Access-Request(1) (id=13, l=162)
474 2018-08-17 17:43:27.949698   192.168.8.11   192.168.8.42   572 RADIUS   572   Access-Accept(2) (id=13, l=530)
951 2018-08-17 17:43:40.457216   192.168.8.11   192.168.8.42   271 RADIUS   271   CoA-Request(43) (id=53, l=229)
952 2018-08-17 17:43:40.459947   192.168.8.42   192.168.8.11    86 RADIUS    86   CoA-ACK(44) (id=53, l=44)

▶ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_0e:02:b7 (5c:5b:35:0e:02:b7)
▶ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.42
▶ User Datagram Protocol, Src Port: 1812, Dst Port: 48218
▼ RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xc (12)
    Length: 539
    Authenticator: b65d47cb334340e451b8815bac804ac0
    [This is a response to a request in frame 310]
    [Time from request: 0.037078000 seconds]
  ▼ Attribute Value Pairs
    ▼ AVP: l=19 t=User-Name(1): 68-EC-C5-09-2E-69
        Type: 1
        Length: 19
        User-Name: 68-EC-C5-09-2E-69
    ▶ AVP: l=67 t=State(24): 526561757468536573737369 6f6e3a63306138303830623631...
    ▶ AVP: l=78 t=Class(25): 434143533a63306138303830623631547452515f53356c5f...
    ▶ AVP: l=18 t=Message-Authenticator(80): fe260cbc9ae1cdc036963d2cabbb09b4
    ▼ AVP: l=45 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 45
        Vendor ID: ciscoSystems (9)
      ▶ VSA: l=39 t=Cisco-AVPair(1): url-redirect-acl=ACL_WEBAUTH_REDIRECT
    ▼ AVP: l=217 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 217
        Vendor ID: ciscoSystems (9)
      ▶ VSA: l=211 t=Cisco-AVPair(1): url-redirect=https://192.168.8.11:8443/portal/gateway?sessionId=c0a8080b61TtRQ_S5l_Tna7LS4PeAZBQ4kmT6DGDXXPChRXUDm8&portal=f0ae43f0-7159-1
```

Guest Access: URL-Direct

At this stage, client is able to procure an IP.

- The client should initiate an HTTP transaction – by logging into the browser and trying to reach an external URL

- Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server

- The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.

- Once the client provides necessary info on the URL, **the radius server now installs this client's mac address in its database** and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.

Guest Access: CoA Request

No.	Time	Source	Destination	Length	Protocol	Size	TX Rate	RSSI	Channel	Info
474	2018-08-17 17:43:27.949698	192.168.8.11	192.168.8.42	572	RADIUS	572				Access-Accept(2) (id=13, l=530)
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86				CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204	RADIUS	204				Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286				Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=54, l=229)

```
▸ Frame 951: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits)
▸ Ethernet II, Src: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c), Dst: Mist_0e:02:b7 (5c:5b:35:0e:02:b7)
▸ Internet Protocol Version 4, Src: 192.168.8.11, Dst: 192.168.8.42
▸ User Datagram Protocol, Src Port: 41351, Dst Port: 3799
▾ RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x35 (53)
    Length: 229
    Authenticator: 190cded5bd49afdff47bcb87c7245d90
    [The response to this request is in frame 952]
  ▾ Attribute Value Pairs
    ▸ AVP: l=6 t=NAS-IP-Address(4): 192.168.8.42
    ▸ AVP: l=19 t=Calling-Station-Id(31): 68-EC-C5-09-2E-69
    ▸ AVP: l=6 t=Event-Timestamp(55): Aug 17, 2018 17:43:40.000000000 PDT
    ▸ AVP: l=18 t=Message-Authenticator(80): 58413c1fb15355502a0551858f0160f4
    ▾ AVP: l=43 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 43
        Vendor ID: ciscoSystems (9)
      ▸ VSA: l=37 t=Cisco-AVPair(1): subscriber:reauthenticate-type=last
    ▾ AVP: l=41 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 41
        Vendor ID: ciscoSystems (9)
      ▸ VSA: l=35 t=Cisco-AVPair(1): subscriber:command=reauthenticate
    ▾ AVP: l=76 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 76
        Vendor ID: ciscoSystems (9)
      ▸ VSA: l=70 t=Cisco-AVPair(1): audit-session-id=c0a8080b61TtRQ_S5l_Tna7LS4PeAZBQ4kmT6DGDXXPChRXUDm8
```

Guest Access: CoA ACK

951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271	CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86	CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204	RADIUS	204	Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286	Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271	CoA-Request(43) (id=54, l=229)

```
▸ Frame 952: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▸ Ethernet II, Src: Mist_0e:02:b7 (5c:5b:35:0e:02:b7), Dst: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c)
▸ Internet Protocol Version 4, Src: 192.168.8.42, Dst: 192.168.8.11
▸ User Datagram Protocol, Src Port: 3799, Dst Port: 41351
▾ RADIUS Protocol
    Code: CoA-ACK (44)
    Packet identifier: 0x35 (53)
    Length: 44
    Authenticator: de7370fd09f7d5dddceb232f33b2e51f
    [This is a response to a request in frame 951]
    [Time from request: 0.002731000 seconds]
  ▾ Attribute Value Pairs
    ▸ AVP: l=6 t=Event-Timestamp(55): Aug 17, 2018 17:43:40.000000000 PDT
    ▸ AVP: l=18 t=Message-Authenticator(80): 9013d7fde7f0d353e6c1b5de6040b0e9
```

Guest Access: Access-Accept2

No.	Time	Source	Destination	Length	Protocol	Size	TX Rate	RSSI	Channel	Info
474	2018-08-17 17:43:27.949698	192.168.8.11	192.168.8.42	572	RADIUS	572				Access-Accept(2) (id=13, l=530)
951	2018-08-17 17:43:40.457216	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=53, l=229)
952	2018-08-17 17:43:40.459947	192.168.8.42	192.168.8.11	86	RADIUS	86				CoA-ACK(44) (id=53, l=44)
953	2018-08-17 17:43:40.462132	192.168.8.42	192.168.8.11	204	RADIUS	204				Access-Request(1) (id=13, l=162)
956	2018-08-17 17:43:41.069095	192.168.8.11	192.168.8.42	286	RADIUS	286				Access-Accept(2) (id=13, l=244)
2564	2018-08-17 17:44:13.398105	192.168.8.11	192.168.8.42	271	RADIUS	271				CoA-Request(43) (id=54, l=229)

```
▶ Frame 953: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
▶ Ethernet II, Src: Mist_0e:02:b7 (5c:5b:35:0e:02:b7), Dst: Microsof_b2:e8:0c (00:15:5d:b2:e8:0c)
▶ Internet Protocol Version 4, Src: 192.168.8.42, Dst: 192.168.8.11
▶ User Datagram Protocol, Src Port: 3799, Dst Port: 1812
▼ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xd (13)
    Length: 162
    Authenticator: 1d058ee7d99027c84015a6ebaed04cf1
    [The response to this request is in frame 956]
  ▼ Attribute Value Pairs
    ▼ AVP: l=14 t=User-Name(1): 68ecc5092e69
        Type: 1
        Length: 14
        User-Name: 68ecc5092e69
    ▼ AVP: l=18 t=User-Password(2): Encrypted
        Type: 2
        Length: 18
        User-Password (encrypted): f4a417644d217877e37f2b11279f45d6
    ▶ AVP: l=6 t=Service-Type(6): Call-Check(10)
    ▶ AVP: l=6 t=NAS-IP-Address(4): 192.168.8.42
    ▶ AVP: l=31 t=Called-Station-Id(30): 5C-5B-35-00-1E-13:jon_ise_new
    ▶ AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
    ▶ AVP: l=19 t=Calling-Station-Id(31): 68-EC-C5-09-2E-69
    ▶ AVP: l=24 t=Connect-Info(77): CONNECT 11Mbps 802.11b
    ▶ AVP: l=18 t=Message-Authenticator(80): 19ef516c6a1089b9e290f69b0f0cefbc
```

Guest Access: ISE Policy 2

		Wi-Fi_Guest_Access	AND	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:HotSpot_Endpoints Wireless_MAB	× PermitAccess	Select from list	0	
		Wi-Fi_Redirect_to_Guest_Login		Wireless_MAB	× Guest_Access	Select from list	47	
		Basic_Authenticated_Access		Network_Access_Authentication_Passed	× PermitAccess	Select from list	0	
		Default			× DenyAccess	Select from list	0	

Guest Access: Access_Accept2

No.	Time	Source	Destination	Protocol	Length	Info
2185	2018-12-13 20:01:10.222473	10.2.10.13	10.2.15.254	RADIUS	205	Access-Request id=3
2186	2018-12-13 20:01:10.237153	10.2.15.254	10.2.10.13	RADIUS	552	Access-Accept id=3
4287	2018-12-13 20:01:30.510365	10.2.15.254	10.2.10.13	RADIUS	271	CoA-Request id=35
4288	2018-12-13 20:01:30.514875	10.2.10.13	10.2.15.254	RADIUS	86	CoA-ACK id=35
4289	2018-12-13 20:01:30.516758	10.2.10.13	10.2.15.254	RADIUS	205	Access-Request id=4
4290	2018-12-13 20:01:30.540528	10.2.15.254	10.2.10.13	RADIUS	275	Access-Accept id=4

```
▶ Frame 4290: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits)
▶ Ethernet II, Src: Microsof_b2:e8:0e (00:15:5d:b2:e8:0e), Dst: Mist_3e:d2:28 (5c:5b:35:3e:d2:28)
▶ Internet Protocol Version 4, Src: 10.2.15.254, Dst: 10.2.10.13
▶ User Datagram Protocol, Src Port: 1812, Dst Port: 3799
▼ RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x4 (4)
    Length: 233
    Authenticator: 0e920b47eacbe264bcc42627cc8e7788
    [This is a response to a request in frame 4289]
    [Time from request: 0.023770000 seconds]
  ▼ Attribute Value Pairs
    ▶ AVP: t=User-Name(1) l=19 val=D4-A3-3D-29-02-66
    ▼ AVP: t=State(24) l=67 val=526561757468536573737369 6f6e3a30613032306666654f6a...
        Type: 24
        Length: 67
        State: 526561757468536573737369 6f6e3a30613032306666654f6a...
    ▼ AVP: t=Class(25) l=76 val=434143533a30613032306666654f6a6c614c424976503058...
        Type: 25
        Length: 76
        Class: 434143533a30613032306666654f6a6c614c424976503058...
    ▼ AVP: t=Message-Authenticator(80) l=18 val=d85ec7c9be054b330354bff93ed841a2
        Type: 80
        Length: 18
        Message-Authenticator: d85ec7c9be054b330354bff93ed841a2
    ▼ AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
        Type: 26
        Length: 33
        Vendor ID: ciscoSystems (9)
      ▶ VSA: t=Cisco-AVPair(1) l=27 val=profile-name=Apple-iPhone
```

Enabling Airespace AVPs