Hewlett Packard
Enterprise

802.1X/MAC/WEB Auth Use Cases and Lessons Learned

Taken from POC activity

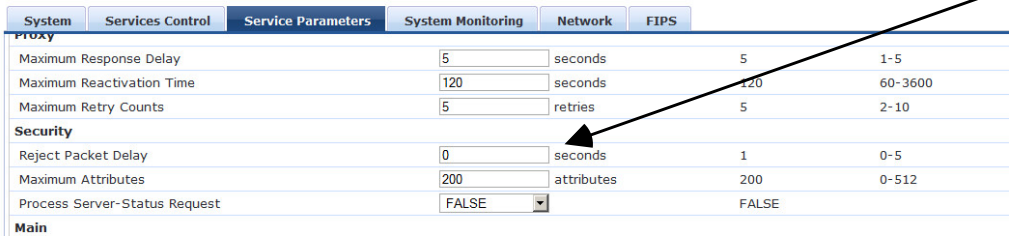
Serge BAIKOFF
System Engineer
HPE MASE/ CCIE #7639
Email: serge.baikoff@hpe.com

Comware v7 – Features Update

RADIUS Probe-on Feature (R3109P14/5130EI; R1120/5130HI/5500HI)

radius-server test-profile abc username admin interval 10
radius scheme cppm
 primary authentication x.x.x.x key cipher c3$ test-profile abc

CPPM 'Reject Packet Delay' !!!!



RADIUS Server Load Sharing (R3109P14/5130EI; R1120/5130HI/5500HI)

radius-server test-profile abc username admin interval 10
radius scheme cppm
 primary authentication x.x.x.x key cipher c3$ test-profile abc
 secondary authentication x.x.x.x key cipher c3$ test-profile abc weight 100
 algorithm loading-share enable

Hewlett Packard Enterprise

Comware v7 – Features Update – Critical Voice VLAN (1/2)

802.1X Critical Voice VLAN (R3109P14 / 5130EI)

interface GigabitEthernetx/x/x
dot1x critical-voice-vlan
undo voice-vlan mode auto
voice-vlan XXX enable

When a reachable RADIUS server is detected, the device removes 802.1X voice users from the critical voice VLAN. The port sends a unicast EAP-Request/Identity packet to each 802.1X voice user that was assigned to the critical voice VLAN to trigger authentication.

MAC-Authentication Critical Voice VLAN (R3109P14 / 5130EI)

interface GigabitEthernetx/x/x
mac-authentication critical-voice-vlan
undo voice-vlan mode auto
voice-vlan XXX enable

- Enable LLDP both globally and on the port
- Enable voice VLAN on the port

Authentication status	VLAN manipulation
A voice user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	The device assigns the port to the 802.1X critical voice VLAN.
A voice user in the 802.1X Auth-Fail VLAN fails authentication because all the RADIUS servers are unreachable.	The port is still in the 802.1X Auth-Fail VLAN.
A voice user in the 802.1X guest VLAN fails authentication because all the RADIUS servers are unreachable.	The device removes the port from the 802.1X guest VLAN and assigns the port to the 802.1X critical voice VLAN.

Comware v7 – Features Update – Critical Voice VLAN (2/2)

The critical VLAN feature takes effect when MAC/DOT1X authentication is performed only through RADIUS servers. If a MAC/DOT1X authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN

```
domain xxx
 authentication lan-access radius-scheme xx
 authorization lan-access radius-scheme xx
 accounting lan-access radius-scheme xx
```

*So do not configure **local** authentication/authorization/accounting fallback for Critical VLAN or Voice VLAN to make it works !*

Hewlett Packard Enterprise

Comware v7 – Features Update

MAC-Authentication Multi-VLAN mode (R3109P14 / 5130EI)

interface GigabitEthernetx/x/x
mac-authentication host-mode multi-vlan

The MAC authentication multi-VLAN mode prevents an authenticated online user from service interruption caused by VLAN changes on a port. When the port receives a packet sourced from the user in a VLAN not matching the existing MAC-VLAN mapping, the device neither logs off the user nor reauthenticates the user. The device creates a new MAC-VLAN mapping for the user, and traffic transmission is not interrupted.

Parallel processing of MAC and Dot1x authentication (R3109P14/5130EI, R1120P05/5130HI)

interface GigabitEthernetx/x/x
mac-authentication parallel-with-dot1x

With this feature enabled, when a port receives a packet from an unknown MAC address, the device immediately sends a unicast EAP-Request/Identity packet to the MAC address. After that, the device immediately processes MAC authentication without waiting for the 802.1X authentication result. Use this feature to enable a port to process MAC authentication and 802.1X authentication in a parallel manner if the port performs MAC authentication after 802.1X authentication is complete.

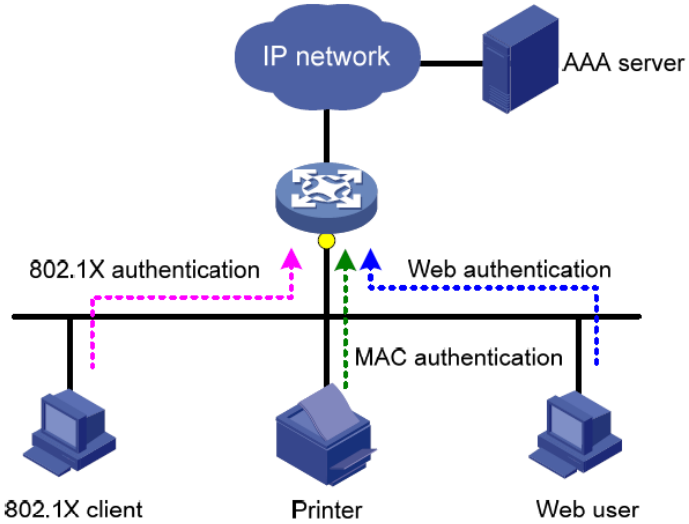
Hewlett Packard Enterprise

Comware v7 – Features Update

Triple Authentication (R3111P07 / 5130EI and Comware v5)

Triple authentication enables an access port to perform Web, MAC, and 802.1X authentication. A terminal can access the network if it passes one type of authentication.

Triple authentication is suitable for a LAN that comprises terminals that require different authentication services.
The triple authentication-enabled access port can perform MAC authentication for the printer, 802.1X authentication for the PC installed with the 802.1X client, and Web authentication for the Web user.



Hewlett Packard Enterprise

Comware v7 – Features Update

802.1X/MAC Authentication support for tagged VLAN assignement (5130EI/HI)

RFC 3580 (single untagged VLAN) Assignment
- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-Id

RFC 4675 (multiple tagged/untagged VLAN) Assignment
- Tunnel-Type
- Tunnel-Medium-Type
- Egress-VLANID

```
[5130-GigabitEthernet1/0/2]dis dot1x co
Slot ID: 1
User MAC address: 001b-4f55-cde3
Access interface: GigabitEthernet1/0/2
Username: 1111
Authentication domain: hpn.fr
Authentication method: EAP
Initial VLAN: 102
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: 101
Authorization ACL ID: N/A
Authorization user profile: N/A
Authorization URL:  N/A
Termination action: Radius-request
Session timeout period: 300 s
Online from: 2016/03/17 15:32:28
Online duration: 0h 6m 48s
```

ACL ou profile de QoS

L'attribut standard « filter-ID » est utilisé
Si il contient un numéro correspondant à une ACL, celle-ci est appliquée en entrée
Si il contient un nom, le « user-profile » correspondant est appliqué
ATTENTION si l'ACL ou le USER-PROFILE n'existent pas, l'authentification est rejetée

Hewlett Packard Enterprise

MAC&DOT1X Configuration example

```
interface GigabitEthernet2/0/34
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 3 untagged
 undo port hybrid vlan 1 untagged
 undo voice-vlan mode auto
 voice-vlan 2 enable
 mac-vlan enable
 stp edged-port
 undo dot1x multicast-trigger
 dot1x re-authenticate
 dot1x unicast-trigger
 dot1x critical vlan 3
 mac-authentication guest-vlan 3
 mac-authentication re-authenticate server-unreachable keep-online
 mac-authentication critical vlan 3
 mac-authentication critical-voice-vlan
 mac-authentication host-mode multi-vlan

 undo mac-authentication offline-detect enable
 mac-authentication parallel-with-dot1x
 port-security port-mode userlogin-secure-or-mac-ext
#
```

When the port receives a packet sourced from the user in a VLAN not matching the existing MAC-VLAN mapping, the device neither logs off the user nor reauthenticates the user

For a port to perform MAC auth before it is assigned to the 802.1X guest VLAN

Performs 802.1X authentication first. If 802.1X authentication fails, MAC authentication is performed.

CoA – Comware (1/2)

Dynamic Authorization Extensions (DAE) is an extension to Radius. It is officially documented in RFC 3576 (circa 2003). The RFC 5176 (circa 2008) is an updated version of RFC 3576.

Comware v7 (R3109P14 / 5130EI)

- *RFC 3576 Ext to RADIUS (CoA only)*
- *Configuration Example*

```
radius session-control enable
radius dynamic-author server
    client ip x..x.x key simple xxxx
    port xxx (default 3799)
```

- *What is supported*

Disconnect Message (standard DAE Disconnect Message)
Cisco-AVPair="subscriber:command=bounce-host-port“
Cisco-AVPair=""subscriber:command=disable-host-port

IETF Attribute	**User-Name**
IETF Attribute	**Calling-Station-Id**
Cisco Vendor-Specific Attribute	**Cisco-AVPair**

Hewlett Packard Enterprise

CoA – Comware (2/2)

Dynamic Authorization Extensions (DAE) is an extension to Radius. It is officially documented in RFC 3576 (circa 2003). The RFC 5176 (circa 2008) is an updated version of RFC 3576.

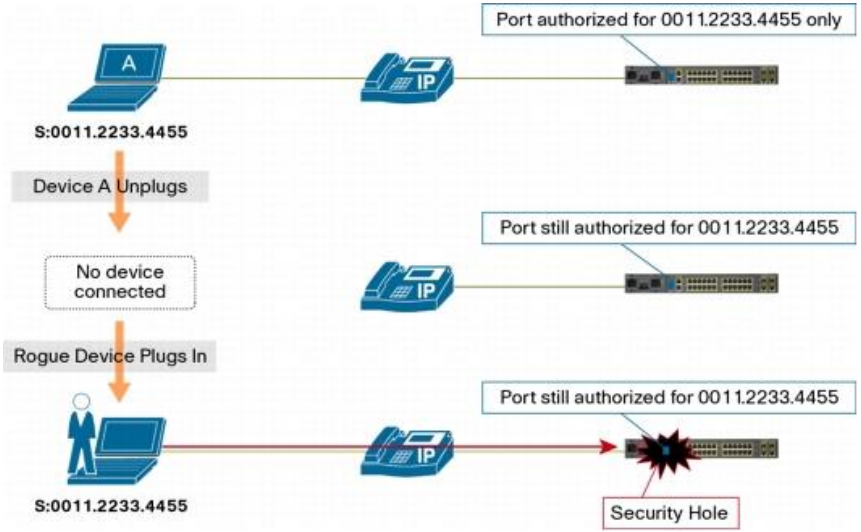
Comware v5

- *RFC 3576 Ext to RADIUS (CoA only) => Idem Comware v5 (see QS) !*
- *Configuration Example*

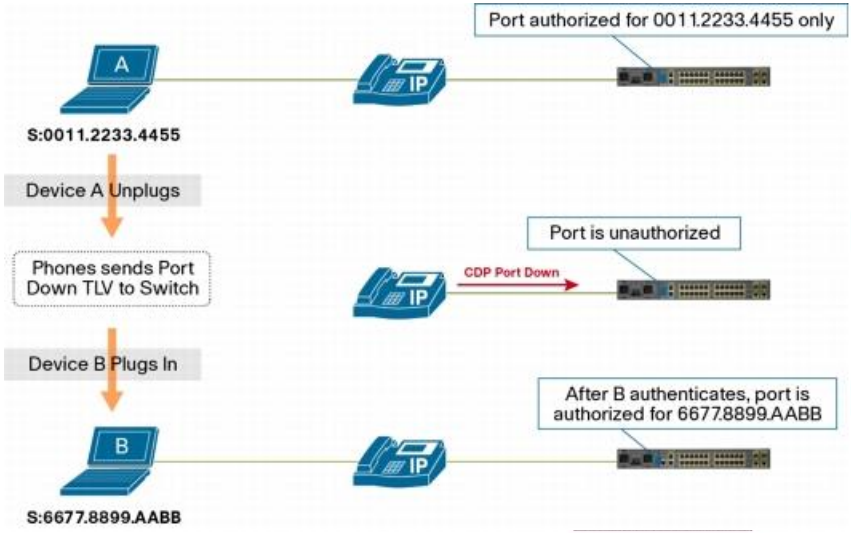
  radius session-control enable
- *What is supported*

  Disconnect Message (standard DAE Disconnect Message)

Comware v7 – MAC/802.1X/WEB



ClearPass MAC@ Spoofing

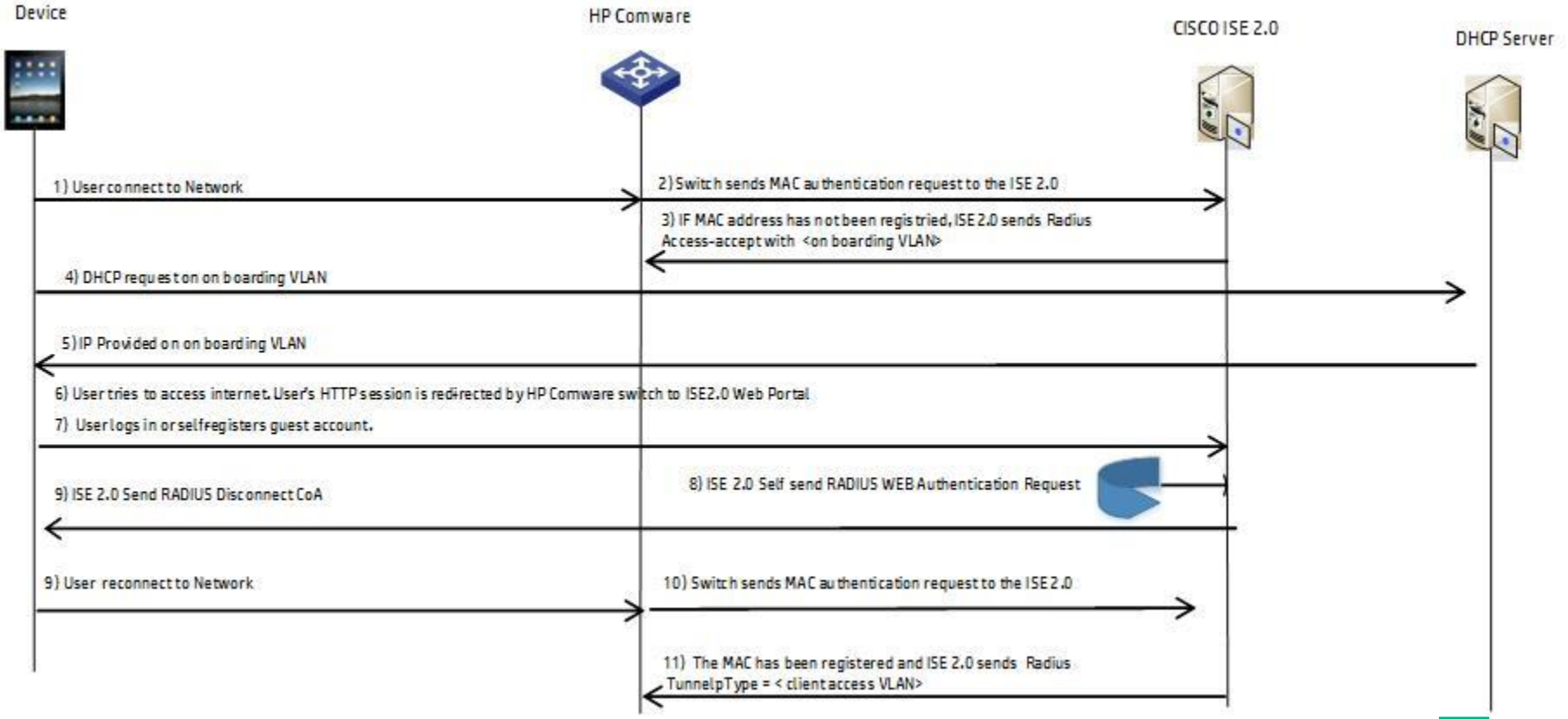


CDP Enhancement for Second Port Disconnect

- Use RADIUS to dynamically assign the best inactivity timeout value for each class of device authenticating via IEEE 802.1X or MAB
- If your phones support proxy EAPoL-Logoff, use the RADIUS-assigned inactivity timer for MAB devices

Hewlett Packard Enterprise

ISE 2.0 Central Web Auth or BYOD Onboarding



Hewlett Packard Enterprise

External Captive Portal integration (CPPM, ISE 2.0, etc..

- Cisco-av-pair=url-redirect
- url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp
- url-redirect=https://IP.ADDRESS.OF.CPG/guest/YOUR_PAGE_NAME.php?mac=%{Connection:Client-Mac-Address-Colon}

External Captive portal (Include @MAC/URL/etc..redirect)

```
portal web-server URL
 url https://10.20.40.6:8443/portal/g?p=WRLGKyWRQkjjmfAYNky7x5AQv7
 url-parameter ip source-address
 url-parameter mac source-mac
 url-parameter url original-url

interface Vlan-interfaceXXX
        portal enable method direct
        portal apply web-server URL
```


Hewlett Packard Enterprise

802.1X/MAB/WEBAUTH TIPS

- Cisco Vendor Specific Attribute (VSA): "device-traffic-class = voice" Authenticated a phone and allow access to the voice VLAN – Useful for 802.1x IP Phone Authentication
- Enable CoPP if your platform supports it to protect LLDP
- Enable Unicast EAPOL and disable EAPOL Multicast
- Configure supplicants to send EAPoL-Starts
- Same NTP source for CPPM and NAD devices
- ReAuthentication
  - Termination-Action Attribute to « RADIUS-Request »
  - Session-Timeout RADIUS Attribute (Attribute [27])
- Only use the inactivity timer if there is no other way to address the link-state issue
- Use RADIUS to dynamically assign the best inactivity timeout value for each class of device authenticating via IEEE 802.1X or MAB
- If your phones support proxy EAPoL-Logoff, rely on that feature to clear sessions for IEEE 802.1X-authenticated devices and use the RADIUS-assigned inactivity timer for MAB devices

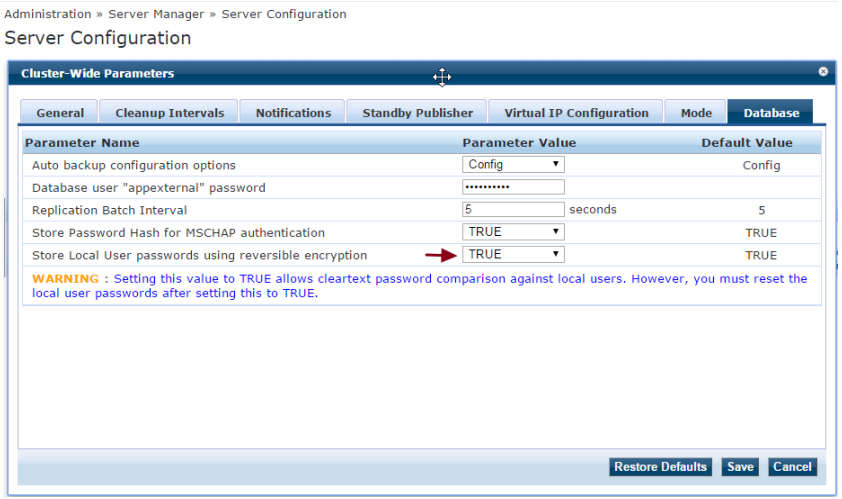
Aruba Integration Support for FlexNetwork Switches

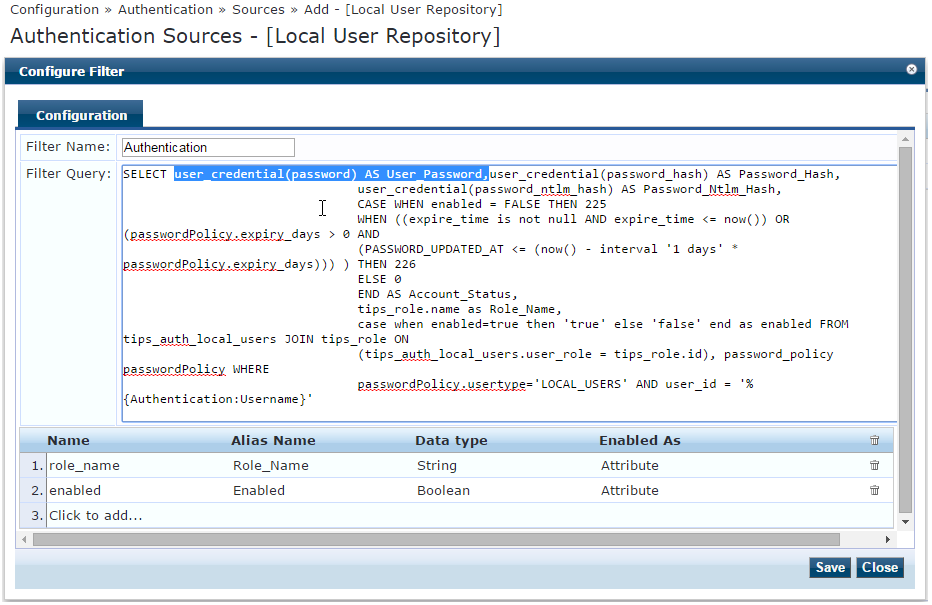
Supported
On roadmap
No support

	Comware 5	Comware 5	Comware 7	Comware 7	Comware 7	Comware 7	Comware 7
	5120 EI/SI	**5500 EI/HI**	**5130 EI**	**5130 HI**	**5510 HI**	**7500**	**10500**
Airwave Support							
Discover switches	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Basic switch monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ClearPass Support							
RADIUS-based Dynamic VLAN	Yes	Yes	Yes	Yes	Yes	Yes (Predefined VLAN)	Yes (Predefined VLAN)
RADIUS-based Dynamic ACL	Yes	Yes	Yes	Yes	Yes	Yes (Predefined ACL)	Yes (Predefined ACL)
RADIUS-based Dynamic CoS/QoS	Yes	Yes	Yes	Yes	Yes	Yes (when included w/ ACL)	Yes (when included w/ ACL)
RADIUS-based Dynamic Rate-Limiting	Yes	Yes	Yes - Use User Profile	Yes - Use User Profile	Yes - Use User Profile	Yes (when included w/ ACL)	Yes (when included w/ ACL)
RADIUS Accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RADIUS Interim Accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
802.1x	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MAC Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CoA	No Support	No Support	Yes	On the roadmap	On the roadmap	Yes	Yes
CoA Disconnect Message	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CoA Port Bounce	No Support	No Support	Yes	On the roadmap	On the roadmap	Yes	Yes
CoA Port Shutdown	No Support	No Support	Yes	On the roadmap	On the roadmap	Yes	Yes
Internal Captive Portal (RADIUS Auth)	Yes	Yes	Yes	On the roadmap	On the roadmap	Yes	Yes
External Captive Portal (include MAC address in redirect)	No Support	No Support	Yes L3 interface Only			Yes	Yes
TACACS+ Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TACACS+ Authorization	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TACACS+ Accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Concurrent MAC Auth, 802.1X Auth., & Web Auth	Yes - 5120 SI only	Yes	Yes	On the roadmap	On the roadmap	Yes	Yes

DIVERS – EAP-MD5 & ClearPass

http://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/How-to-store-local-user-password-in-clear-text-format-or-with/ta-p/248071





Hewlett Packard Enterprise

Radius VSA – H3C_WEB_URL

0927B0E48CA127262708D203015367D3_Service.xml

[acl number 3001 name CAPTIVEPORTAL
rule 10 permit tcp destination <CPPM IP> 0 destination-port eq 443
rule 20 permit tcp destination <CPPM IP> 0 destination-port eq www
rule 30 permit udp destination-port eq bootps
rule 40 permit udp destination-port eq dns
rule 50 permit udp destination-port eq bootpc

Enforcement Profiles - CW7 OnGuard Enrollment

Summary | Profile | Attributes

Profile:

Name:	CW7 OnGuard Enrollment
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:H3C	H3C_WEB_URL	=	http://cppm-es.arubalab.com/guest/onguard.php?mac=%{Connection:Client-Mac-Address-Colon}&browser=1
2.	Radius:H3C	H3C_AV_PAIR	=	url-redirect-acl=3001

Hewlett Packard Enterprise

Comware v7 RADIUS VSAs

Vendor ID	Attribute ID	Name	Description
25506 (H3C)	210	H3C_AV_PAIR: device-traffic-class=voice shell:roles=xxx url-redirect-acl=xxx url-redirect=xxx	Server-assigned voice VLAN Server-assigned user role Server-assigned ACL Server-assigned Web redirect URL
	29	H3C-Exec-Privilege	Comware Privilege Level
	250	H3C-WEB-URL	Web Redirect URL for users

Thanks!