BEST PRACTICE - NAC AUF ARUBA SWITCHES

Rollenbasierte Konzepte mit Aruba OS Switches in Verbindung mit ClearPass – Vorstellung Mobile First Features
Agenda

1. Overview
2. 802.1X Authentication
3. MAC Authentication
4. Web Authentication with Clearpeass
5. User Roles
Overview
Network Access Security
User Experience

1. Sets up role based access policy groups & assigns rules and access profiles:
   - Set rules
     - Time
     - Location
     - Device ID
     - Client integrity status
   - To trigger each policy profile
     - ACL
     - VLAN
     - QoS
     - BW limit

2. Put users in appropriate access policy group
Network Access Security
User Experience cont.

1. Sets up role based access policy groups & assigns rules and access profiles:
   - Set rules
     - Time
     - Location
     - Device ID
     - Client integrity status
   - To trigger each policy profile
     - ACL
     - VLAN
     - QoS
     - BW limit

2. Put users in appropriate access policy group
Client Authentication Possibilities

- Three methods to authenticate at the “edge”
  - IEEE 802.1X
  - Web Authentication
  - MAC Authentication

- 0008A2-1C99C6: no client software required – sends MAC address

- Using 802.1X client software

- Using web browser only
802.1X Authentication
Naming differences

**IETF RADIUS naming**
- Access Client
- Network Access Server (NAS)
- RADIUS Server

**IEEE 802.1X naming**
- Client
- Policy Enforcement Point
- Policy Decision Point
- Supplicant
- Authenticator
- Authentication Server
Authentication Flow

Supplicant | Authenticator | Authentication Server

Authenticator relays packets between supplicant and authentication server

RADIUS

802.1X
Authenticator relays packets between supplicant and authentication server
IEEE 802.1X

802.1X introduces Port-States

- Unauthorized—no authorized client has connected to the port
- When a port is in the unauthorized state, only EAP traffic is allowed.
IEEE 802.1X

- 802.1X introduces Port-States
  - Authorized—connected client has supplied valid credentials
- When a port is in the authorized state, traffic is forwarded normally.
Standard 802.1X behavior with multiple clients per port

– 802.1X-2004 assume one client per switch port
– Protocol on LAN uses multicast address

=> Port based authentication

– Problem:
  – Piggy back attack relatively easy
  – First client on the port open it also for subsequent clients, e.g. IP phone connected on the same port would open the port for the cascaded client.
ArubaOS-Switch solution with multiple 802.1X clients per port

- Successful authentication by a client opens port for traffic with the clients source MAC address only
- All authenticated clients must use the same untagged VLAN
- Associated instance in the switch use only the associated source MAC address as destination address for 802.1X packets (will prevent confusion of other 802.1X clients connected to the same port)
- An 802.1X client instance must be able to receive unicast 802.1X packets
- Supports up to 32 802.1X clients per port
- A client-limit needs to be configured to activate this mode
What if the RADIUS Server is not reachable?

– Option 1 (default):
  – New clients don’t get authenticated => no access to network
  – If reauthentication occurs on already authenticated clients they are deauthenticated => no access to network

```
5406zl(config)# aaa authentication port-access eap-radius none
```

– Option 2 (authorized):
  – New clients will be allowed without authentication to succeed
  – If reauthentication occurs on already authenticated clients will be put in authenticated state

```
5406zl(config)# aaa authentication port-access eap-radius authorized
```

– Option 3 (cached-reauth):
  – New clients don’t get authenticated => no access to network
  – If reauthentication occurs on already authenticated clients will stay authenticated

```
5406zl(config)# aaa authentication port-access eap-radius cached-reauth
```
RADIUS Server Availability Tracking

– This feature tracks the availability of radius servers configured on the switch. It helps to minimize the waiting period for new clients in the unauth-vid(Guest Vlan) when authentication fails because of service is not available and for previously authenticated clients in unauth-vid(Guest Vlan) when re-authentication fails because of service is not available during re-authentication period.

```
switch(config)# radius-server tracking <enable | disable>
switch(config)# radius-server tracking user-name <USER-NAME>
```

– Once the feature is enabled, radius control task sends access-request of PAP with test user name and empty password to all radius servers for every 5 minutes. If access-accept/access-reject is received, it will treat the server as alive. If time out happens then the server will be treated as dead based on the configured retry count and time out values. When all the servers are dead in that server-group, it informs the clients (802.1x, web-auth, mac-auth) about the failure. It is up to the clients to decide whether to ignore the request when unauth vid is not set or gets authenticated if cached-reauth is configured.
Order of VLAN assignments

Upon authorization, a port will be assigned to a VLAN in order of priority:

1. VLAN from the user’s RADIUS profile, if defined
2. Authorized VLAN, if configured for the port
3. Underlying VLAN configured for the port

If a port is used to authenticate multiple users
- VLAN assignment is on a first-come, first-served basis
- First authenticated client dictates untagged VLAN assignment
- Subsequent clients must be authorized for the same VLAN or they will be denied access

Unauthorized users will either have no access or can be placed in an unauthorized VLAN.
802.1X authentication: Switch-to-switch

802.1X-aware switch can operate as an authenticator on some ports and a supplicant using EAP-MD5 on others. Supplicant mode can be used to provide security between uplinks.

- Enable port as supplicant with no parameters
- Reissue the command with parameters to set username and password

```
Edge_1(config)# aaa port-access supplicant 10
Edge_1(config)# aaa port-access supplicant 10 identity edge01 secret
Enter secret: ********
Repeat secret: ********
```
Dynamically assign multiple VLANs on a port via RADIUS

- RADIUS attributes according to:
  - RFC3580: The RADIUS server can assign the untagged VLAN ID
  - RFC4675: The RADIUS server can assign untagged and multiple tagged VLAN IDs

Fixed VLAN configuration for uplink port:
```
...  
vlan 1
  name Management
  untag 10
vlan 2
  name Data
  tag 10
vlan 3
  name Voice
  tag 10
...  
```
## RFC 4675 – Radius Attribute Types

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>Egress-VLANID</td>
</tr>
<tr>
<td>57</td>
<td>Ingress-Filter</td>
</tr>
<tr>
<td>58</td>
<td>Egress-VLAN-Name</td>
</tr>
<tr>
<td>59</td>
<td>User-Priority-Table</td>
</tr>
</tbody>
</table>
## Egress-VLANID

<table>
<thead>
<tr>
<th>Tag Indication</th>
<th>PAD</th>
<th>VLANID</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Bits</td>
<td>12 Bits</td>
<td>12 Bits</td>
</tr>
</tbody>
</table>

- **0x31** = tagged
- **0x32** = untagged

(always 0x000)

0x001 .. 0xffe

Example: 0x31000011 = VLAN 17, tagged
## Egress-VLAN-Name

<table>
<thead>
<tr>
<th>Tag Indication</th>
<th>Vlan Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Bits</td>
<td>UTF-8 encoded, &lt;= 10646 characters</td>
</tr>
</tbody>
</table>

"1" = tagged
"2" = untagged

Example "1student" = VLAN student, tagged
Clearpass RADIUS Attributes
Possibility 1 using Egress-VLANID

- HP-Port-Auth-Mode-Dot1x=1
- HP-Port-Client-Limit-MA=0
- VLAN 1 untagged
  HEX 0x32000001 = DECIMAL 838860801
  Egress-VLANID=838860801
- VLAN 2 tagged
  HEX 0x31000002 = DECIMAL 822083586
  Egress-VLANID=822083586
- VLAN 3 tagged
  HEX 0x31000003 = DECIMAL 822083587
  Egress-VLANID=822083587
Clearpass RADIUS Attributes using Egress-VLAN-Name
Possibility 2 using Egress-VLAN-Name

- HP-Port-Auth-Mode-Dot1x=1
- HP-Port-Client-Limit-MA=0
- VLAN 1 untagged, name Management
  Egress-VLAN-Name= 2Management
- VLAN 2 tagged, name Data
  Egress-VLAN-Name= 1Data
- VLAN 3 tagged, name Voice
  Egress-VLAN-Name= 1Voice
Port-Access Controlled-Directions Support Wake-on-LAN functionality

Suppliant

Authenticator

– In an unauthorized state the traffic is allowed from the switch port towards the client. This support Wake-on-LAN functionality.

5406zl(config)# aaa port-access a4-a16 controlled-direction in
MAC-based VLAN (MBV) Support for multiple untagged VLANs

– Allows multiple users and devices that connect on the same port to operate in different untagged VLANs:
  – More flexibility for connecting users and endpoints
  – More granular control

5406zl(config)# aaa port-access a4-a16 mbv enable
MAC-based VLAN (MBV) table

– The port uses a table to map MAC addresses to untagged VLANs.

<table>
<thead>
<tr>
<th>MAC address</th>
<th>Assigned Untagged VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000c6000001</td>
<td>VLAN 10</td>
</tr>
<tr>
<td>0000c6000002</td>
<td>VLAN 20</td>
</tr>
</tbody>
</table>

Policy:
- 0000c6000001 = VLAN 10
- 0000c6000002 = VLAN 20
Additional considerations

– Broadcasts and multicasts from one client’s VLAN will be received by all clients.
– **Mixed-mode** is required if you want unauthenticated and authenticated clients on the port.
MAC Authentication
MAC authentication overview

• Instead of client interactively entering username and password credentials, the device’s learned MAC address is used
  – Switch sends device’s MAC address to the RADIUS server as the username and password
  – User database accessed by RADIUS server has “user” entries with username and password set to device MAC address
  – No client device configuration necessary and no interactive logon session is involved
Problem: password complexity rule in MS AD prohibits MAC authentication account setup

– Problem:
  – When you want to use MAC authentication a username=MAC-address and a password=MAC-address needs to be configured in the AD. In a normal customer environment the AD password complexity rules prohibit those combination to be setup in the AD.

– Solutions:
  – Per AD group password complexity rule: Supported in Windows 2008
  – Change password with the feature called "MAC Authentication Global Password" on ArubaOS-Switch Switch Series (K.14.31)

```
switch(config)# aaa port-access mac-based password <string>
```

```
Switch(config)# show port-access mac-based config
Port Access MAC-Based Configuration
  MAC Address Format : no-delimiter
  MAC password : &sF95@1
  Unauth Redirect Configuration URL :
  Unauth Redirect Client Timeout (sec) : 1800
  Unauth Redirect Restrictive Filter : Disabled
  Total Unauth Redirect Client Count : 0
...```

Multi-user authentication

– 802.1X, MAC auth and Web auth are parallel events.

– If either MAC auth or Web auth succeeds then the other authentication like MAC or Web (if in progress) is ended.

– 802.1X authorization (VLAN, ACLs, etc..) of the same client has always precedence over MAC auth.
Web Authentication with Clearpeass
Clearpass portal
Existing ArubaOS-switch Web-auth mechanisms

- Existing ArubaOS-switch Web-auth services
  - Switch local web-auth
  - Switch local web-auth with external pages
  - MAC-auth with web-auth fallback
  - BYOD HTTP redirect

- None of the above was valid for Clearpass
  - BYOD HTTP redirect is close match
    - but requires switch local configuration
    - different URL redirect options

- New feature: Clearpass portal redirect support
  - Clearpass will deliver the redirect URL in RADIUS attribute to switch
  - Supports different portals based on different authentication scenario’s
Clearpass captive portal HTTPS
Clearpass portal
Client HTTPS connection

– User can make initial HTTPS connection
  – Example: user has homepage set to https://www.hpe.com
  – Switch can terminate HTTPS connection and redirect user to Captive portal (HTTP 302)
  – User will **always** get a certificate warning:
    – Original URL which user attempted to reach does not match the IP/DNS name of the switch
    – Changing the redirect certificate on the switch will not change this behavior

– Administrator can use switch self-signed or external certificate
  – Switch supports new certificate application type: captive portal
ClearPass Integration Features

– Server Initiated Captive Portal using VSA
  – Ability to send a URL string dynamically using a VSA to support a Captive Portal workflow for guest access.

– Port Bounce VSA
  – Ability to send a VSA to shutdown a port from 0-60 seconds to facilitate VLAN changes.

– Consolidated Client View
  – Enhance the switch per-auth type CLI client view to provide consolidated client view with all auth types.

– New RADIUS Dictionary
  – Update existing ClearPass dictionary for HP Enterprise including new VSAs for PVOS integration.
Captive Portal - Overview

Initial Authentication

Captive Portal redirect and user registration

Final Authentication
Captive Portal - Initial Authentication

- **Client**
  - Auth - 802.1x/MAC
  - The ACL is applied to this client allowing DNS, DHCP and HTTP/S traffic to ClearPass and sending all other HTTP/S traffic to the CPU

- **Switch**
  - RADIUS Access-Request
  - RADIUS Access-Accept

- **ClearPass**
  - The Access-Accept will include: URL and ACL
  - 
  - DHCP/DNS Request
  - DHCP/DNS Reply

- **DHCP/DNS**
  - Forward all HTTP/S traffic to ClearPass: permit in tcp from any to <clearpass_ip> 80, 443
  - Steal all HTTP/S traffic to CPU: deny in tcp from any to any 80, 443 cpy
  - Forward all DNS/DHCP traffic: permit in udp from any to any 53, 67
Captive Portal – ClearPass Configuration

– A ClearPass enforcement profile needs to be created to enable captive portal re-direction.
– The enforcement profile uses HP-Captive-Portal-URL VSA and several NAS-Filter-Rule entries.
The redirect occurs from an ACL rule - any HTTP/S traffic not destined for ClearPass is sent to the CPU, resulting in a 302 redirect being sent back to the client.

Parameters list = Client MAC, Client IP, Client URL, Timestamp

A hash of the captive portal redirect URL and the above parameters are included in the Parameter List if the URL hash key is configured.
Port Bounce

– No explicit command is needed to enable this on the switch
– A pre-defined enforcement profile is included in ClearPass 6.5.5 and higher.
  – The default port shutdown is 12 seconds.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Radius: IETF</td>
<td>User-Name</td>
<td>%{Radius: IETF:User-Name}</td>
</tr>
<tr>
<td>2. Radius: IETF</td>
<td>Calling-Station-Id</td>
<td>%{Radius: IETF:Calling-Station-Id}</td>
</tr>
<tr>
<td>3. Radius: IETF</td>
<td>NAS-Port</td>
<td>%{Radius: IETF:NAS-Port}</td>
</tr>
<tr>
<td>6. Radius: HP</td>
<td>HP-Port-Bounce-Host</td>
<td>12</td>
</tr>
</tbody>
</table>
Captive Portal – Final Authentication

Client

Switch

ClearPass

Wait configured time for authentication to complete

Client traffic

RADIUS Access-Request

RADIUS Access-Accept

Apply new attributes

HTTP to Original URL

The Access-Accept may include: VLAN, QoS, Rate-Limit, ACL

Internet
User Roles
User roles introduction

– New AAA model, similar to role-based access on Aruba Mobility Switch

– User roles defined locally on switch
  – Groups a set of attributes applied to user session
    – VLAN, User Policy (QOS, ACLs and rate limits), Re-authentication period or Captive Portal profile
    – E.g. define roles for Guest, Printer, Corporate, Contractor

– User role assigned by
  – RADIUS assigned attribute
User roles provide user based QOS

- Each switch role can contain a user traffic policy
- Traffic policy can control per traffic class:
  - Permit/deny of traffic
  - QOS action
  - Rate limiter
- Previously, RADIUS server could apply a COS value per user session, but it would be a single value for all the traffic of this user.
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPPM</td>
<td>ClearPass Policy Manager, RADIUS Server</td>
</tr>
<tr>
<td>VSA</td>
<td>RADIUS Vendor-specific attribute</td>
</tr>
<tr>
<td>LMA</td>
<td>Switch Local MAC Authentication</td>
</tr>
<tr>
<td>OUI</td>
<td>Organization Unique Identifier</td>
</tr>
<tr>
<td>CoA</td>
<td>RADIUS Change of Authorization</td>
</tr>
<tr>
<td>WMA</td>
<td>RADIUS based Web/MAC Authentication</td>
</tr>
</tbody>
</table>
New AAA Model

– Switch Global feature
  – Replaces the current authentication scheme for entire switch
  – Every device is assigned a user role

– Advantage
  – Access switch can now show online users and their roles
  – Roles abstracts details of configuration
User role assignment

– New model
  – unauthenticated device state does not exist anymore
  – unauthenticated devices now assigned the Initial role

– Active on all ports with authentication enabled
  – No impact on ports without port-security

– All devices are assigned a user role
  – Unauthenticated devices: the Initial user role
  – Authenticated devices can obtain role from:
    – VSA (Vendor Specific Attribute) provided by the ClearPass RADIUS server
User role assignment based on RADIUS VSA

– RADIUS Server like ClearPass sends user role to switch
  – Attribute set in Access-accept or Change of Authorization (CoA) packet
– Attribute is HPE Vendor Specific Attribute 25
  – ClearPass 6.5 and earlier: administrator can add attribute manually
  – ClearPass 6.6: included by default as HPE-User-Role
    – Dictionary updated to Hewlett-Packard-Enterprise
– Method applicable for these authentication methods:
  – 802.1x
  – MAC Authentication with RADIUS server
User role assignment based on RADIUS VSA

- ClearPass updated HP (11) RADIUS dictionary with string attribute 25 (HP-User-Role)

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>HP (11)</th>
<th>Type</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. HP-Egress-VLANID</td>
<td>64</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>9. HP-Management-Protocol</td>
<td>26</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>10. HP-Nas-Filter-Rule</td>
<td>61</td>
<td>string</td>
<td>in out</td>
</tr>
<tr>
<td>11. HP-Nas-Rules-IPV6</td>
<td>63</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>12. HP-Port-Auth-Mode-Dot1x</td>
<td>13</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>13. HP-Port-Bounce-Host</td>
<td>23</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>14. HP-Port-Client-Limit-Dot1x</td>
<td>10</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>15. HP-Port-Client-Limit-MA</td>
<td>11</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>16. HP-Port-Client-Limit-WA</td>
<td>12</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>17. HP-Privilege-Level</td>
<td>1</td>
<td>unsigned32</td>
<td>in out</td>
</tr>
<tr>
<td>18. HP-User-Role</td>
<td>25</td>
<td>string</td>
<td>in out</td>
</tr>
</tbody>
</table>

NOTE: The current switch release does not support ClearPass downloadable roles
User role assignment

– Original authentication precedence order is maintained for authenticated users:
  1. 802.1x RADIUS VSA
  2. MAC Authenticated RADIUS VSA

– All unauthenticated users assigned the **Initial** role:
  – Users not performing authentication
  – Users with failed authentication

**NOTE:** This applies only to switch ports with authentication enabled (802.1x and MAC authentication).
User role configuration

Elements

– User Role consists of these elements, all optional:
  – Ingress user policy (traffic filter)
  – VLAN (ID or Name)
  – Re-authentication period
    – default: 0 (no re-authentication period)
  – Captive portal profile

– Some rules apply:
  – No other RADIUS session attributes (e.g. to set VLAN, Filter ID, Filter rules or other HPE proprietary VSAs) are supported when user roles are enabled
  – RADIUS server can only use HPE VSA 25 to assign the user role name.
  – Session-timeout can be sent by the RADIUS server, but will be overwritten by User Role Re-authentication period.
  – HPE VSA 24 - Captive-portal-URL is allowed, but only when the User role has a blank (not configured) Captive portal URL or refers to the predefined “use-radius-vsa” Captive portal profile
  – Unauth-vid, auth-vid and control options cannot be used with user-roles.
User role VLAN Assignment
Order updated

– New order of VLAN assignment when User roles are enabled:
  1. VLAN from User role, if configured
     – RADIUS VSA or Initial role
  2. Apply all the configured port VLANs to the user:
     – untagged VLAN ID, if configured
     – tagged VLAN IDs of port, if configured

Which VLAN?
Initial Role

- User role assignment
  - Only applies to ports with authentication enabled
  - Every user has a role, authenticated or unauthenticated
  - Typical authentication processing should result in a role assignment

- Switch applies Initial role:
  - Failed authentications
  - Any other authentications which fail user role validation
    - User moved into Failed Initial Role state

- Admin can control role for Initial Role:
  - Administrator-defined role
  - Pre-defined role
ClearPass Captive Portal and User roles

– ClearPass Guest requires switch to redirect user to web login page
  – How does switch know to what URL user must be redirected?

– When User role feature is **disabled**:
  – ClearPass can deliver the redirect URL through the RADIUS HPE VSA 24

– When User role feature is **enabled**:
  – User Role
    – Switch configuration User Role can contain reference to name of Captive Portal Profile with static URL
      – When empty or no URL, RADIUS Based can be used
    – Switch configuration User Role can contain reference to predefined Captive Portal Profile with name “use-radius-vsa”
  – RADIUS Based
    – No other RADIUS VSA session attributes are supported when User role attribute is set
    – Exception to this rule is the Captive Portal URL, RADIUS HPE VSA 24 can still be used
User roles configuration

– Configuration steps:
  1. Enable global feature
  2. Create a User Role, optional elements:
     – Assign Captive portal
     – User Role Policy
     – Re-authentication period
     – User Role VLAN (either ID or Name)
  3. Configure user role assignment
     – RADIUS assigned, e.g. ClearPass
  4. Set Initial Role

NOTE: Captive portal profile and User Policy objects must exist when set in the User role, or role assignment will fail and user is assigned Initial Role
User roles configuration
Create a User Role

– Configuration elements
  – Re-authentication period
  – User Role VLAN ID or Name

– It is recommended to create these elements before assigning to a user role:
  – User Policy: ACL, QOS and rate limit rules
  – Captive portal profile: Redirect URL

**NOTE:** The role can refer to a non-existing User Policy or Captive Portal Profile, but the role assignment will fail in this case. User will be assigned the Initial role.
Downloadable User Roles

- Single point of policy management
  - Dynamically assigned by ClearPass at the time of authentication

- Builds on top of the existing local User Roles
  - Every user/device is assigned a User Role
  - User Role policies include QoS, VLAN, ACL, Rate Limits

- Consistent wired/wireless policy management
  - Same as WLAN AP, simplify policy configuration and management
Thank You