

Anleitung zur Einrichtung von MAC basierter Authentifizierung am Beispiel eines DGS-3200-10 Switches.

Aufgabe:

An Port 1-8 des Switches sollen sich verschiedene Clients anschließen. Diese Clients werden anhand Ihrer MAC Adresse automatisch in das korrekte VLAN (VLAN 2 oder VLAN 3) zugewiesen.

Die Authentifizierung erfolgt über einen Radius Server (in diesem Beispiel ein FreeRadius) welcher an Port 9 (VLAN 2 untagged) des DGS-3200-10 angeschlossen ist. Port 10 des Switches ist der Uplink in das Netzwerk (VLAN 2 & VLAN 3 werden tagged über Port 10 übertragen)

Das Standardpasswort für die Radiusauthentifizierung lautet in diesem Beispiel „default“. Dieses Passwort muss im Radiusserver bei jedem MAC-Adressprofil als Passwort eingetragen werden.

Diese Konfiguration sollte unbedingt über die CLI (Command Line Interface) am seriellen Port durchgeführt werden, da eine Änderung der Management-IP und des Management-VLAN zu einer kompletten Unterbrechung der Kommunikation mit dem Client führen kann!

1.) grundlegende Konfiguration des Switches (anlegen aller notwendigen VLANs)

```
create vlan VLAN2 tag 2          <- erstellt das VLAN 2 mit der VLAN ID 2
create vlan VLAN3 tag 3          <- erstellt das VLAN 3 mit der VLAN ID 3
```

2.) ändern der IP Adresse des Switches und ändern des Management(default)-VLAN

```
config ipif System ipaddress 192.168.10.200/24 vlan VLAN2 state enable
```

<- ändert die IP Adresse des IP Interface System auf 192.168.10.200/24 und weist das neue Management-VLAN „VLAN2“ zu

3.) zuweisen des Uplinkports (Port 10 tagged & Port 9 untagged) sowie des Radiusports

```
config vlan VLAN2 add untagged 9  <- weist Port 9 dem VLAN 2 untagged zu
config vlan VLAN2 add tagged 10   <- weist Port 10 dem VLAN 2 tagged zu
config vlan VLAN3 add tagged 10   <- weist Port 10 dem VLAN 3 tagged zu
```

4.) konfigurieren & aktivieren des Radius Server

```
config radius add 1 192.168.10.210 key 123456 <- definiert den Radiusserver 1 mit der IP
192.168.10.210 und dem Shared Secred Key „123456“
enable 802.1x                               <- aktiviert Radius Authentifizierung
```

5.) konfigurieren & aktivieren der MAC Zugangskontrolle

```
enable mac_based_access_control          <- aktiviert MAC based ACL
create mac_based_access_control guest_vlan default <- erstellt das GuestVLAN
                                                    im VLAN default
config mac_based_access_control guest_vlan ports 1-8 <- weist die zu authentifizierenden
                                                    Ports dem GuestVLAN zu
config mac_based_access_control ports 1-8 state enable <- aktiviert die GuestVLAN Ports
config mac_based_access_control method radius <- definiert die zu verwendende
                                                    Authentifizierungsmethode
config mac_based_access_control password default <- definiert das Passwort für alle zu
                                                    authentifizierenden Clients
```

Damit der DGS-3200-10 Anfragen an den RADIUSserver (freeradius) senden darf, muss folgender Eintrag in der Datei „client.conf“ des RADIUSserver existieren:

```
client 192.168.10.200/24    <- definiert den Radius Authenticator
secret = 123456            <- definiert das Shared Secret zwischen Radius Server und
                            Authenticator
shortname = dlink
```

Weiterhin müssen in der Datei „users.conf“ folgende Einträge existieren (pro MAC Adresse ein Eintrag):

```
001346360DFD    User-Password == "default"    <- definiert den Usernamen anhand
                            der MAC-Adresse und das
                            Passwort „default“ für diesen
                            User
                            Tunnel-Type = "VLAN",
                            Tunnel-Medium-Type = "IEEE-802",
                            Tunnel-Private-Group-Id = "2"    <- definiert die VLAN ID "2" des
                            Clients

00D059272101    User-Password == "default"    <- definiert den Usernamen anhand
                            der MAC-Adresse und das
                            Passwort „default“ für diesen
                            User
                            Tunnel-Type = "VLAN",
                            Tunnel-Medium-Type = "IEEE-802",
                            Tunnel-Private-Group-Id = "3"    <- definiert die VLAN ID "3" des
                            Clients
```