

Anleitung zur Einrichtung von MAC basierter Authentifizierung am Beispiel eines DGS-3120/3420/3620-Stack Switches.

Aufgabe:

An Ports 2:1-48 des DGS-3x20 Stack(aktuelle Firmware) 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 Version 1.1.7 R 0.0.2) welcher an Port 1:16 (VLAN 1 untagged) des DGS-3120 angeschlossen ist. Port 1:24 des Switches ist der Uplink in das Netzwerk (VLAN 1, 2 & 3 werden tagged über Port 1:24 übertragen)
Das Standardpasswort für die Radiusauthentifizierung ist in diesem Beispiel die MAC Adresse des sich authentifizierenden Clients.

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

```
config ipif System ipaddress 192.168.10.190/24  
  
<- ändert die IP Adresse des IP Interface System auf  
192.168.10.19/24
```

3.) zuweisen des Uplinkports (Port 1:24 tagged) sowie des Radiusports

```
config vlan default add tagged 24 <- weist Port 24 dem default VLAN tagged zu  
config vlan VLAN2 add tagged 24 <- weist Port 24 dem VLAN 2 tagged zu  
config vlan VLAN3 add tagged 24 <- weist Port 24 dem VLAN 3 tagged zu
```

4.) konfigurieren & aktivieren des Radius Server

```
config radius add 1 192.168.10.20 key 123456 default  
<- definiert den Radiusserver 1 mit der IP 192.168.10.210  
und dem Shared Secret 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 2:1-48 <- weist die zu authentifizierenden Ports dem GuestVLAN zu
config mac_based_access_control ports 2:1-48 state enable <- aktiviert die GuestVLAN Ports
config mac_based_access_control method radius <- definiert die zu verwendende Authentifizierungsmethode
config mac_based_access_control password_type client_mac_address <- definiert das Passwort für alle zu authentifizierenden Clients
```

Damit der DGS-3x10 Stack Anfragen an den RADIUSserver (freeradius) senden darf, muss folgender Eintrag in der Datei „client.conf“ des RADIUSserver existieren:

```
client 192.168.10.19/24                <- 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 == "001346360DFD"    <- definiert den Usernamen anhand der MAC-Adresse und das Passwort „001346360DFD“ 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 == "00D059272101 "            <- definiert den Usernamen anhand der MAC-Adresse und das Passwort „00D059272101“ für diesen User

Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-Id = "3"                <- definiert die VLAN ID "3" des Clients
```

Bitte kommentieren Sie in „users.conf“ folgende 2 Einträge aus (# davorsetzen)

```
DEFAULT    Auth-Type = System
            Fall-Through = 1
```

Bitte beachten Sie, dass diese RADIUSserverkonfiguration nur als Beispiel dient. Für die Installation und Konfiguration des RADIUSservers für Ihr Netzwerk können wir leider keine Unterstützung liefern.