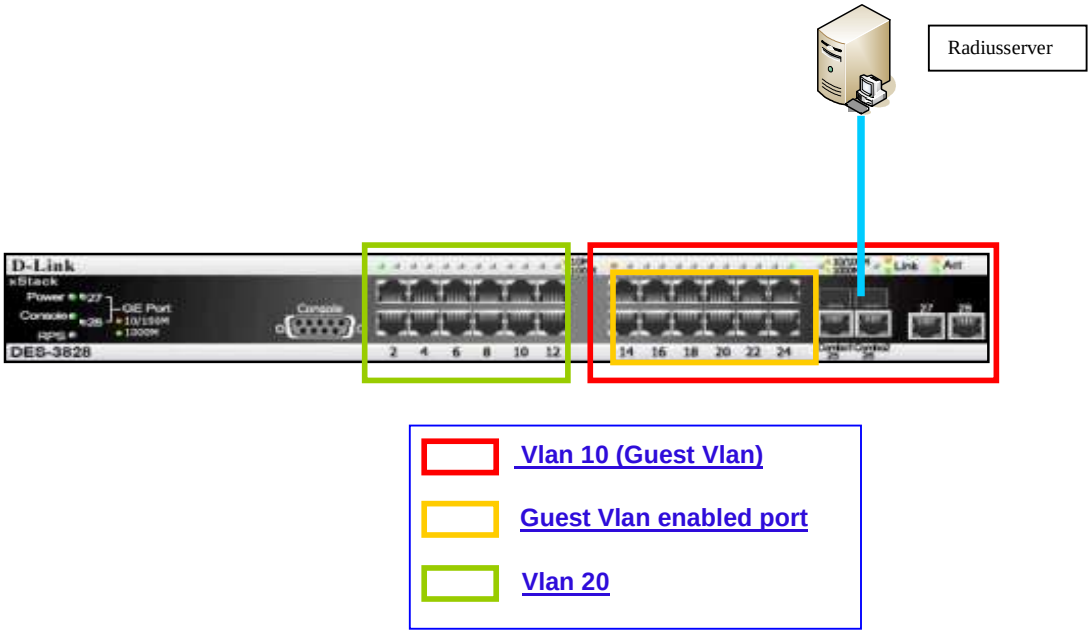
Diese Anleitung beschreibt die Einrichtung eines portbasierenden Gäste-VLAN anhand einer Radiusauthentifizierung

Die Aufgabe eines portbasierenden Gäste-VLAN anhand einer Radiusauthentifizierung ist es Benutzer anhand eines Usernamen und Kennwort am Switch zu authentifizieren und somit den Zugang zum internen Netzwerk zu gestatten. Wenn die Authentifizierung nicht erfolgreich stattfinden konnte, soll der Benutzer nur eine begrenzten Netzwerkzugriff erhalten.



In VLAN 10 (rot) [Port 13-28] befinden sich alle Devices, welche bei einer fehlerhafte Authentifizierung erreicht werden können. Dieses VLAN soll den beschränkten Netzwerkbereich definieren. Somit sollten hier keine firmeninternen Server aktiv sein

An die „Guest VLAN enabled Ports“ (gelb) [Port 13-24] werden generell alle PC´s angeschlossen, welche sich über die Radius authentifizieren sollen.

In VLAN 20 (grün) [Port 1-12] befindet sich das interne Netzwerk. Nur mit einer gültigen Radiusauthentifizierung soll hier der Zugriff gewährleistet werden.

Ein Anwendungsbeispiel wäre das einstecken eines Notebooks an Port 13.
Sollte noch keine Authentifizierung am Radiusserver stattgefunden haben oder der Zugriff wg. eines falschen Kennworts verboten worden sein, so befindet sich das Notebook in VLAN 10 und hat somit auch nur Zugriff auf Netzwerkdevices in VLAN 10 (somit Port 13 – Port 18).

Bei erfolgreicher Authentifizierung wird der Port automatisiert auf VLAN 20 umgestellt. Somit kann dann auf Komponenten im firmeninternen Netzwerk (Port 1- Port 12) zugegriffen werden

Um die Einrichtung der Radiusauthentifizierung durchzuführen sollten über die Konsole (hyperterminal) folgende Befehle eingegeben werden.

```
## Factory Reset des Switches
reset system

## Löschen des default VLAN´s an Port 1-28
config vlan default delete 1-28

## Erstellen eines VLAN 10 und die Zuweisung an Port 13 - 28
create vlan v10 tag 10
config vlan v10 add untagged 13-28

## Erstellen eines VLAN 20 und die Zuweisung an Port 1 - 12
create vlan v20 tag 20
config vlan v20 add untagged 1-12

## Konfiguration der IP Adresse des Switches und Zuweisung des VLAN 10
config ipif System ipaddress 192.168.0.1/24 vlan v10

## Aktivierung und Konfiguration der Radiusauthentifizierung
enable 802.1x
create 802.1x guest_vlan v10
config 802.1x guest_vlan ports 13-24 state enable
config 802.1x capability ports 13-24 authenticator

## Konfiguration der IP des Radius Servers
config radius add 1 192.168.0.10 key 123456 default
```

Im Test wurde Free-Radius in Version 1.1.1-r0-0-1 genutzt.
Die IP Adresse des Radiusservers ist in diesem Fall 192.168.0.10.

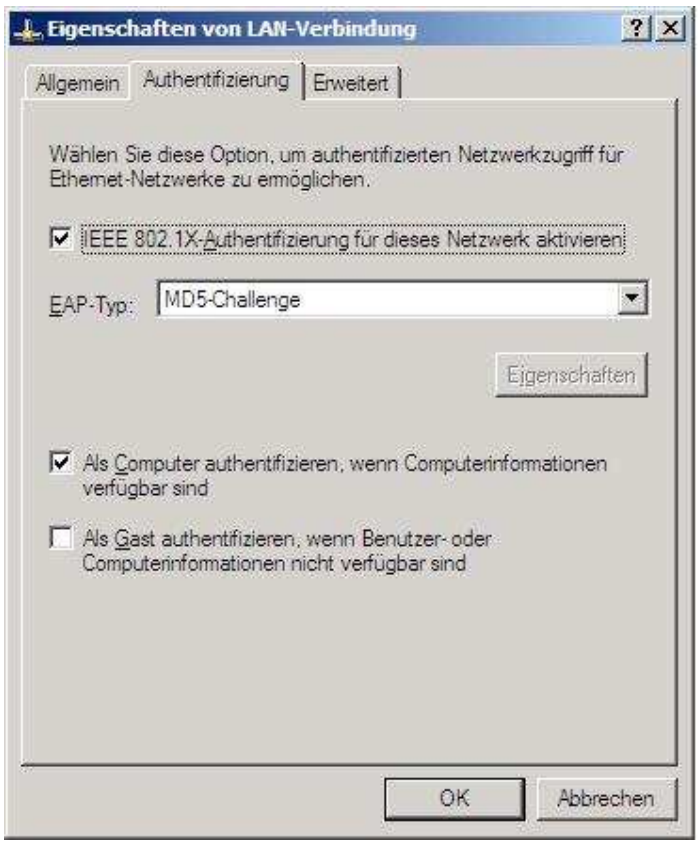
Folgende Zeilen wurden in der Datei clients.conf hinzugefügt:

```
client 192.168.0.0/24 {
        secret          = 123456
        shortname       = Dlink
}
```

Folgende Zeilen wurden in der Datei users.conf hinzugefügt:

```
test    User-Password == "test"
                Tunnel-Type = "VLAN",
                Tunnel-Medium-Type = "IEEE-802",
                Tunnel-Private-Group-Id = "20"
```

In den Eigenschaften der Netzwerkkarte sollte unter dem Reiter „Authentifizierung“ ein Haken am Menüpunkt „IEEE 802.1X-Authentifizierung für dieses Netzwerk aktivieren“ gesetzt werden. Als „EAP-Typ:“ muss „MD5-Challenge“ ausgewählt werden.



Sobald nun das Netzwerkkabel des Notebooks in den Switch an einen „guest VLAN enabled Port“ eingesteckt wird, wird der User aufgefordert den Benutzennamen und das Kennwort einzugeben. Der Benutzername lautet „test“ und das Kennwort lautet „test“.

Sobald die Authentifizierung erfolgreich durch den Radiusserver durchgeführt wurde ist eine Kommunikation in VLAN 20 möglich. Sollte die Authentifizierung wg. beispielsweise einem falschen Kennwort fehlschlagen, so befindet sich das Notebook weiterhin in VLAN 10.