HowTo: Einstellung Time-Based Access an einem D-Link Wireless Switch (DWS)

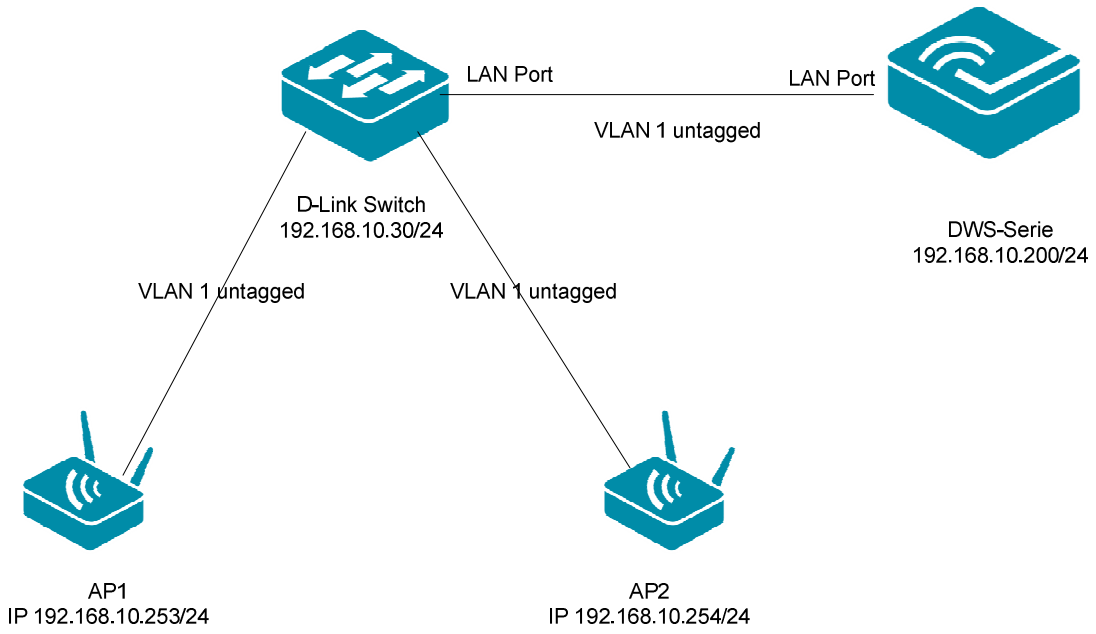
[Voraussetzungen]

1. DWS-4026/3160 mit aktueller Firmware
   - *DWS-4026/ 3160 mit Firmware (FW) 4.1.0.2 und höher*

2. Kompatibler Unified-AP mit aktueller Firmware
   - *DWL-8600AP/6600AP/3600AP am DWS-4026/3160 mit FW 4.1.0.11 und höher*

[Szenario]

Es soll eine Access Control List (ACL) auf dem D-Link Wireless Switch angelegt werden um den Zugang zum WLAN-Netz Werktäglich (Mo-Fr) nur zwischen 07:00 Uhr – 17:00 Uhr zuzulassen.



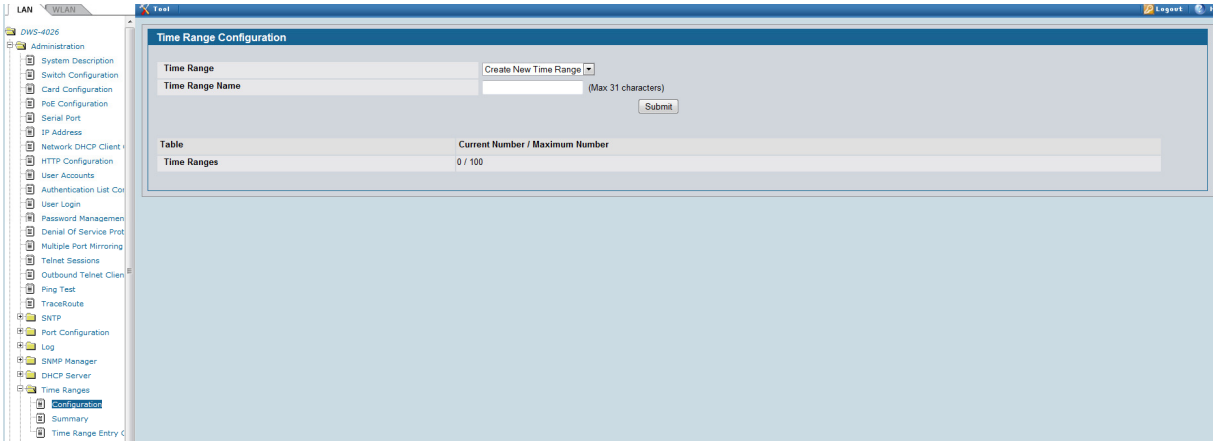
[Vorbereitung]

- ⇨ Der D-Link Wireless Switch ist bereits korrekt konfiguriert
- ⇨ Die Zeitsynchronisierung des D-Link Wireless Switch ist korrekt konfiguriert (SNTP)
- ⇨ Sollten bei Ihnen einige Menüpunkte nicht korrekt angezeigt werden, so benutzen Sie für die Konfiguration bitte einen alternativen Browser (z.B. Firefox 16)

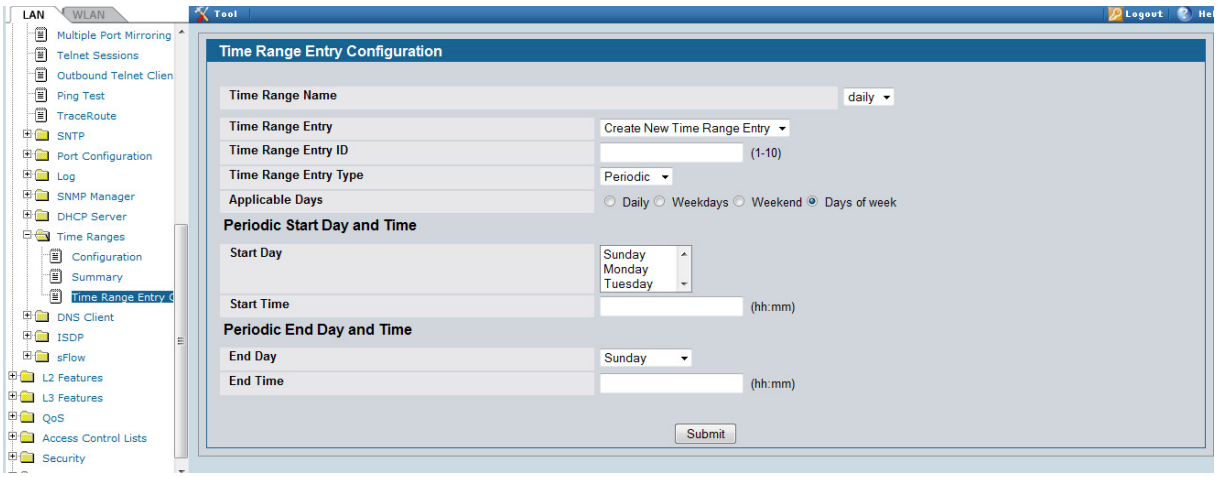
Diese Anleitung basiert auf dem DWS-4026 mit Firmware 4.1.0.11 und ist für alle Wireless Switches methodisch gleich, für die genaue Menüstruktur Ihres Wireless Switches schlagen Sie bitte im entsprechenden Handbuch nach.

[Einrichtung des D-Link Wireless Switches]

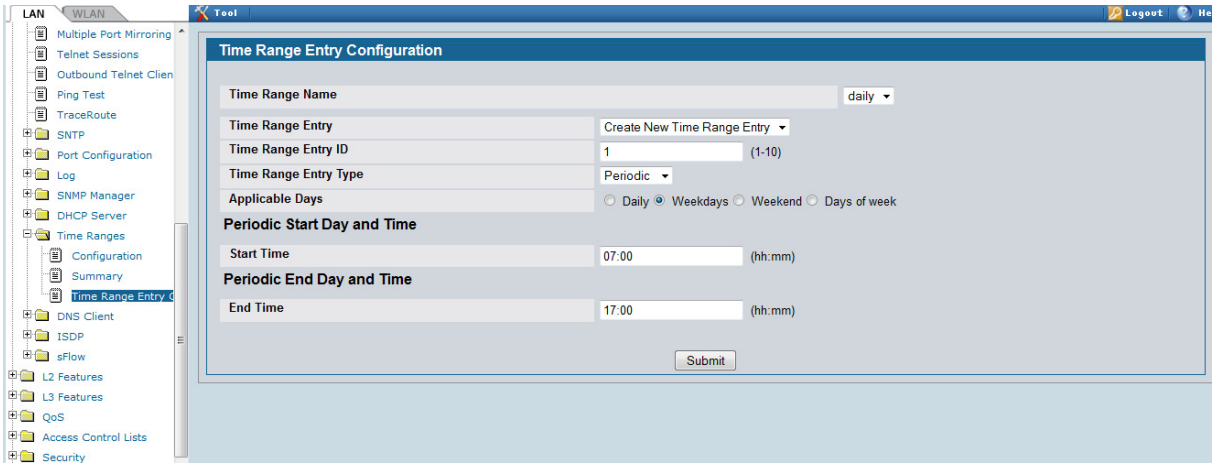
1.) Anlegen der Time-Range, hierzu klicken Sie bitte auf „LAN -> Administration -> Time Range -> Configuration“
   a. zum Erstellen einer Time-Range wählen Sie bitte „Create New Time Range“ aus und tragen den Namen für Ihre Time-Range ein (z.B. „daily“)
   b. bestätigen Sie die Eingabe mit dem Button „Submit“

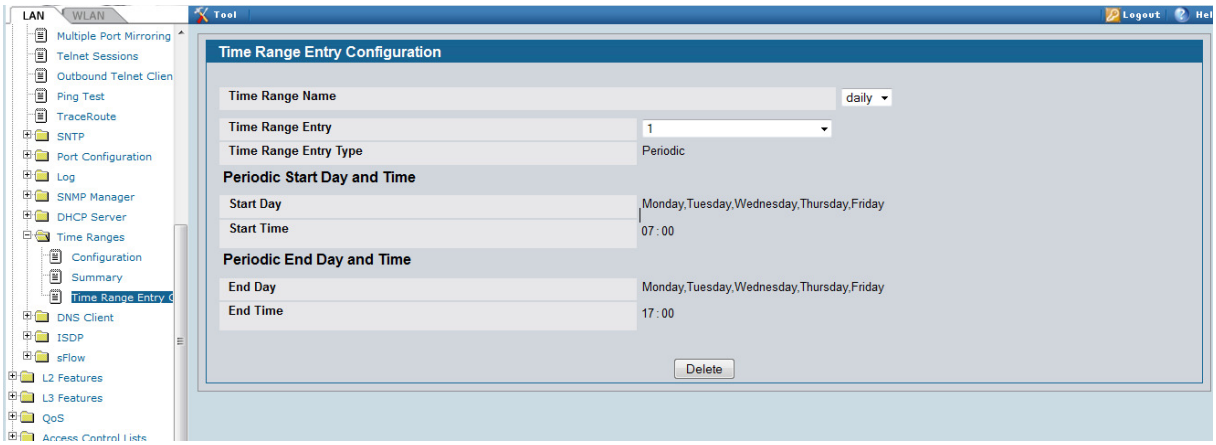


2.) Anpassen der Time-Range, hierzu klicken Sie bitte auf „LAN -> Administration -> Time Range -> Time Range Entry Configuration“
   a. sollten Sie mehrere Time-Ranges unter Punkt 1. Angelegt haben, so können Sie diese unter „Time Range Name“ auswählen
   b. Passen Sie nun die restlichen Einstellungen der Time-Range Ihren Vorgaben entsprechend an und bestätigen die Eingabe mit dem Button „Submit“



c. In diesem Screenshot sehen Sie die Beispieleinstellungen für dieses Scenario

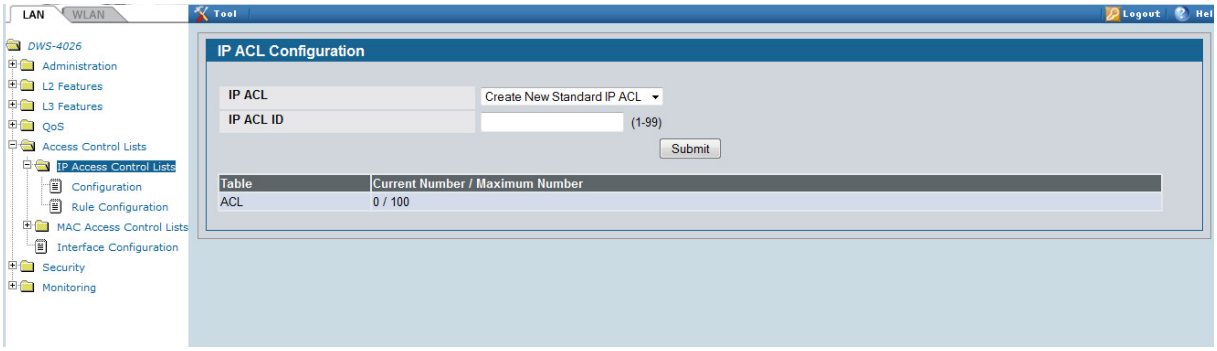




Hier können Sie auch nicht mehr verwendete Time-Ranges mittels des Button „Delete“ löschen.

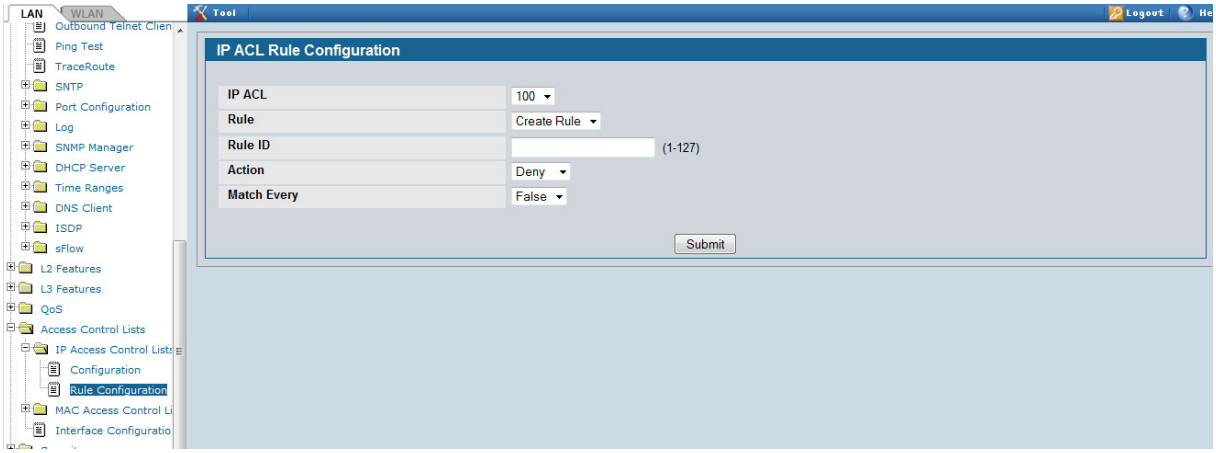
3.) Anlegen einer Access Control List (ACL), hierzu klicken Sie bitte auf „LAN -> Access Control Lists -> IP Access Control Lists“

a. wählen Sie zum anlagen einer ACL bitte “Create New Extended IP ACL” aus und vergeben Sie der ACL eine ACL ID im vorgegebenen Bereich (100-199) und bestätigen die Eingabe mit dem Button „Submit“

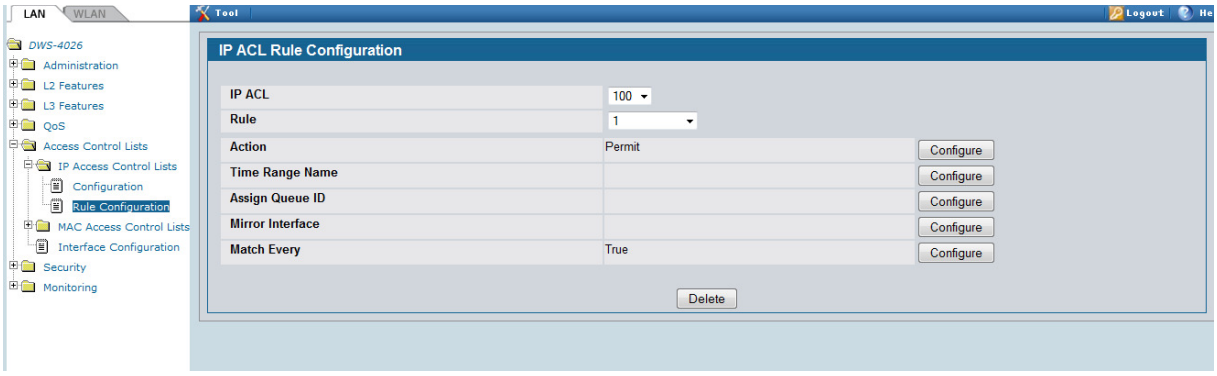


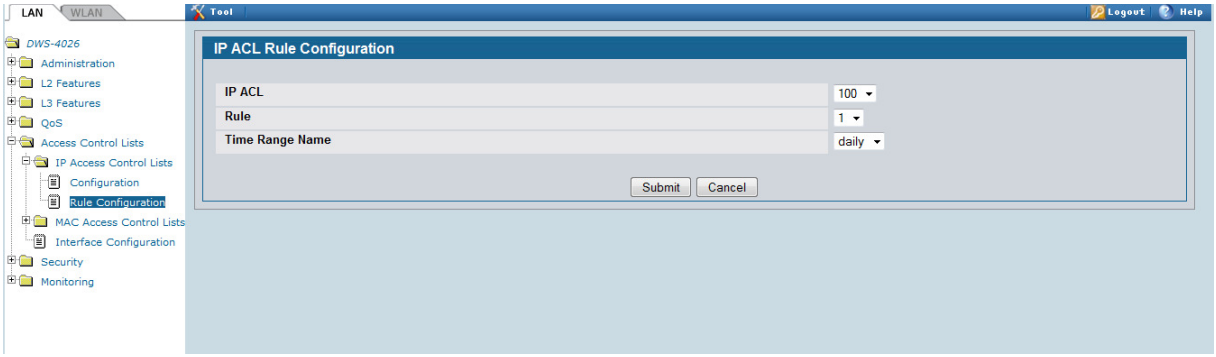
4.) Anpassen einer Access Control List (ACL), hierzu klicken Sie bitte auf „LAN -> Access Control Lists -> IP Access Control Lists“

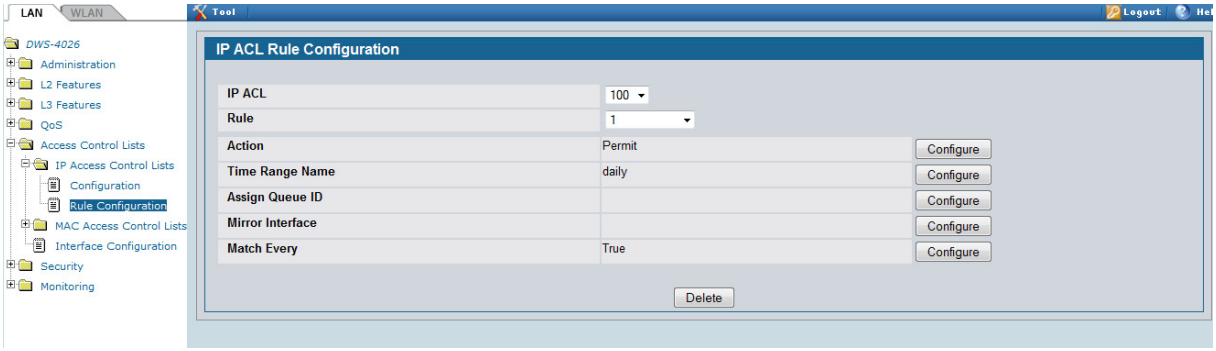
a. sollten Sie unter Punkt 3 mehrere ACLs angelegt haben, so können Sie diese hier unter “IP ACL” auswählen
b. zum Bearbeiten der angelegten IP ACL legen Sie bitte eine Regel „Rule ID“ an
c. bitte wählen Sie, ob die IP ACL Rule ein „Deny“ (Verbieten) oder „Permit“ (Erlauben) sein soll
d. bitte wählen Sie, ob diese IP ACL Rule auf alle Datenpakete angewendet werden soll „True“ oder „False“ (für eine genau Bedeutung dieser Einstellung schlagen Sie bitte im Handbuch nach)
e. bestätigen Sie Ihre Konfiguration mit dem Button „Submit“



f. anschließend können Sie die IP ACL dahingehend bearbeiten, dass Sie die Time-Range auswählen, Klicken Sie hierzu bei „Time Range Name“ auf „Configure“ und wählen bei „Time Range Name“ die unter Punkt 1 angelegte Time Range „daily“ aus, bestätigen Sie die Auswahl mit dem Button „Submit“



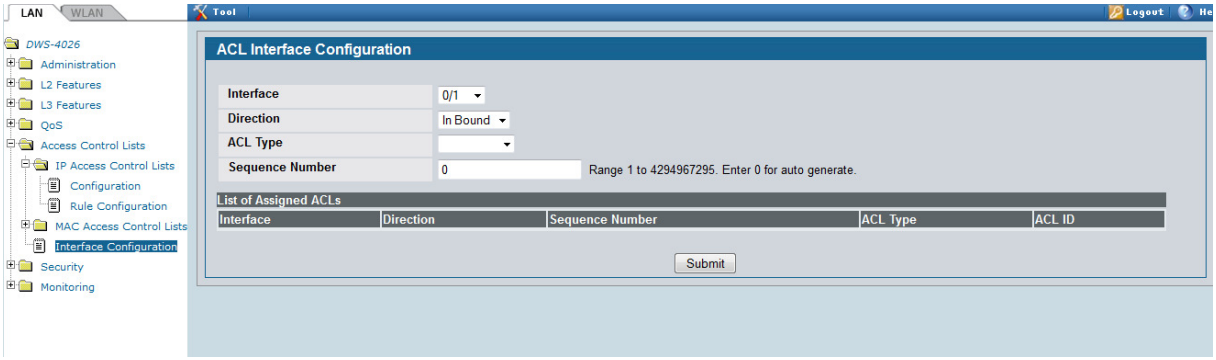


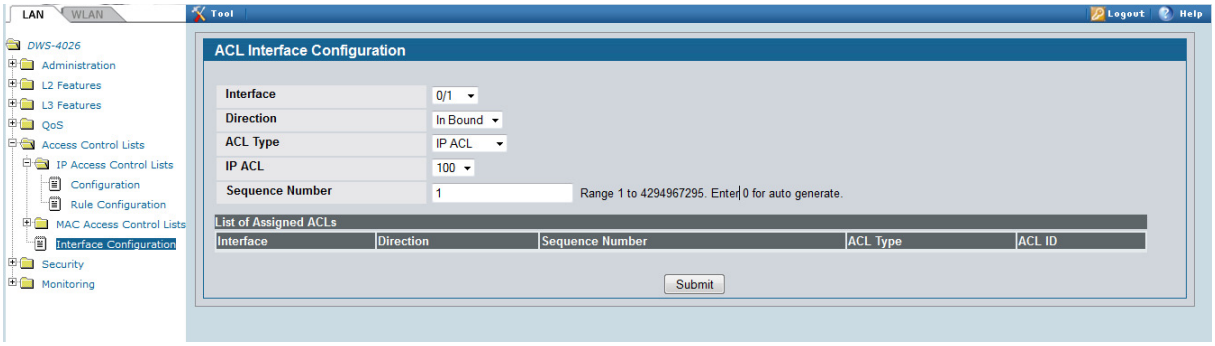


Hiermit haben Sie die ACL erfolgreich angelegt und müssen diese nur noch auf einen Port binden.

5.) Binden der ACL auf einen physikalischen Port, hierzu klicken Sie bitte auf „LAN -> Access Control Lists -> Interface Configuration“

a. wählen Sie bei Interface den physikalischen Port des D-Link Wireless Switches aus, auf dem Sie die ACL auflegen wollen
b. wählen Sie bei ACL Type Ihren ACL Typ aus (Punkt 3 IP ACL)
c. wählen Sie Ihre unter Punkt 4 angelegte Regel aus
d. mittels der „Sequence Number“ können Sie mehrere Regeln auf einem Port abbilden, diese werden der Reihenfolge nach abgearbeitet (first match)
e. bestätigen Sie Ihre Einstellungen mit dem Button „Submit“





! Die ACL wirkt auf Pakete, welche IN den D-Link Wireless Switch gehen. Daher ist es zwingend notwendig die korrekten Ports für die ACL auszuwählen.

Haben Sie Ihre APs direkt an den D-Link Wireless Switch angeschlossen, so wählen Sie bitte diese Ports aus. In diesem Beispiel sind die APs an einem weiteren Switch im Netzwerk angeschlossen, so dass der Uplink ausgewählt werden muss.

!! Bitte beachten Sie bei der Konfiguration auf dem Uplink, dass außerhalb der „Permit“ Zeit kein Zugriff auf den Switch erfolgen kann.

Hier empfiehlt es sich vorab eine weitergehende ACL zu erstellen, damit der Zugriff weiterhin auf den Switch zu administrationszwecken gegeben ist.

!!! Der D-Link Wireless Switch DWS-3160 hat keine explizites „DENY ANY“ als Default Einstellung. Daher müssen Sie für den DWS-3160 beim Punkt 4.) eine weitere Regel anlegen, welche ein „DENY“ und Match Every = TRUE enthält.

Beispiel für die ACL mittels CLI am DWS-3160 (*Time Range Name „time“ Startzeit 08:00 Uhr, Endzeit 16:00 Uhr, täglich => ACL aktiv auf Ports 1-3 des DWS-3160*)

„

config time_range time hours start_time 8:0:0 end_time 16:0:0 weekdays Sun,Mon,Tue,Wed,Thu,Fri,Sat

create access_profile profile_id 1 profile_name 1 ip source_ip_mask 0.0.0.0 destination_ip_mask 0.0.0.0
config access_profile profile_id 1 add access_id 1 ip source_ip 0.0.0.0 destination_ip 0.0.0.0 port 1-6 permit counter enable time_range time
config access_profile profile_id 1 add access_id 2 ip source_ip 0.0.0.0 destination_ip 0.0.0.0 port 1-3 deny

“

Sie können anhand des Log prüfen, ob die ACL korrekt aktiviert und deaktiviert wird.

<13> OCT 26 05:02:51 192.168.10.200-1 TIMERANGE[83054600]: timerange_control.c(139) 4395 %% Sending TIMERANGE_EVENT_END notification for time-range daily for QOS_ACL component
<13> OCT 26 05:02:51 192.168.10.200-1 TIMERANGE[83054600]: timerange_control.c(139) 4396 %% Sending TIMERANGE_EVENT_END notification for time-range daily for POE component
<14> OCT 26 05:02:51 192.168.10.200-1 ACL[141779656]: acl.c(10442) 4397 %% Successful installation of ACL 100, Rule 1 as deactivated in hardware for time based ACL rule associated with time range daily on which there is a L7_TIMERANGE_EVENT_DEACTIVATE notification
<13> OCT 26 11:05:08 192.168.10.200-1 TIMERANGE[83054600]: timerange_control.c(139) 4400 %% Sending TIMERANGE_EVENT_START notification for time-range daily for QOS_ACL component
<13> OCT 26 11:05:08 192.168.10.200-1 TIMERANGE[83054600]: timerange_control.c(139) 4401 %% Sending TIMERANGE_EVENT_START notification for time-range daily for POE component
<14> OCT 26 11:05:08 192.168.10.200-1 ACL[141779656]: acl.c(10421) 4402 %% Successful installation of ACL 100, Rule 1 as activated in hardware for time based ACL rule associated with time range daily on which there is a L7_TIMERANGE_EVENT_ACTIVATE notification

Wenn APs nicht direkt am D-Link Wireless Switch angeschlossen sind, gilt folgendes zu beachten:

- *Clients, welche sich VOR Ablauf der „Permit“ Zeit am WLAN angemeldet haben können weiterhin kommunizieren.*
- *Dies ist der Tatsache geschuldet, dass nur die Authentifizierung der Clients am D-Link Wireless Switch erfolgt, der Datenverkehr jedoch direkt am Access-Switch ausgeschleust wird. Hier ist evtl. eine Designanpassung notwendig.*