



Tech Pack: ACL

Access Control List am Beispiel der
DGS-1510 Switch Serie

Dirk Böttinger | Senior Network Specialist
13.10.2023



D-LINK (Deutschland) GmbH

Schwalbacher Straße 74

65760 Eschborn

www.dlink.com

Dirk Böttinger

Senior Network Consultant

Business Development & Product Marketing

dirk.boettinger@dlink.com



Über uns



Globale Präsenz

Über 127 lokale Vertriebsniederlassungen in mehr als 56 Ländern. 20 regionale Warenlager in 15 Ländern und über 50 RMA Reparatur Zentren weltweit



Schwerpunkte

Entwicklung, Produktion und weltweiter Vertrieb



Zielgruppen

Unternehmen, Verbraucher, Telekommunikations- & Service-Provider. Öffentliche Einrichtungen wie z.B. Schulen & Behörden



Topic | Title

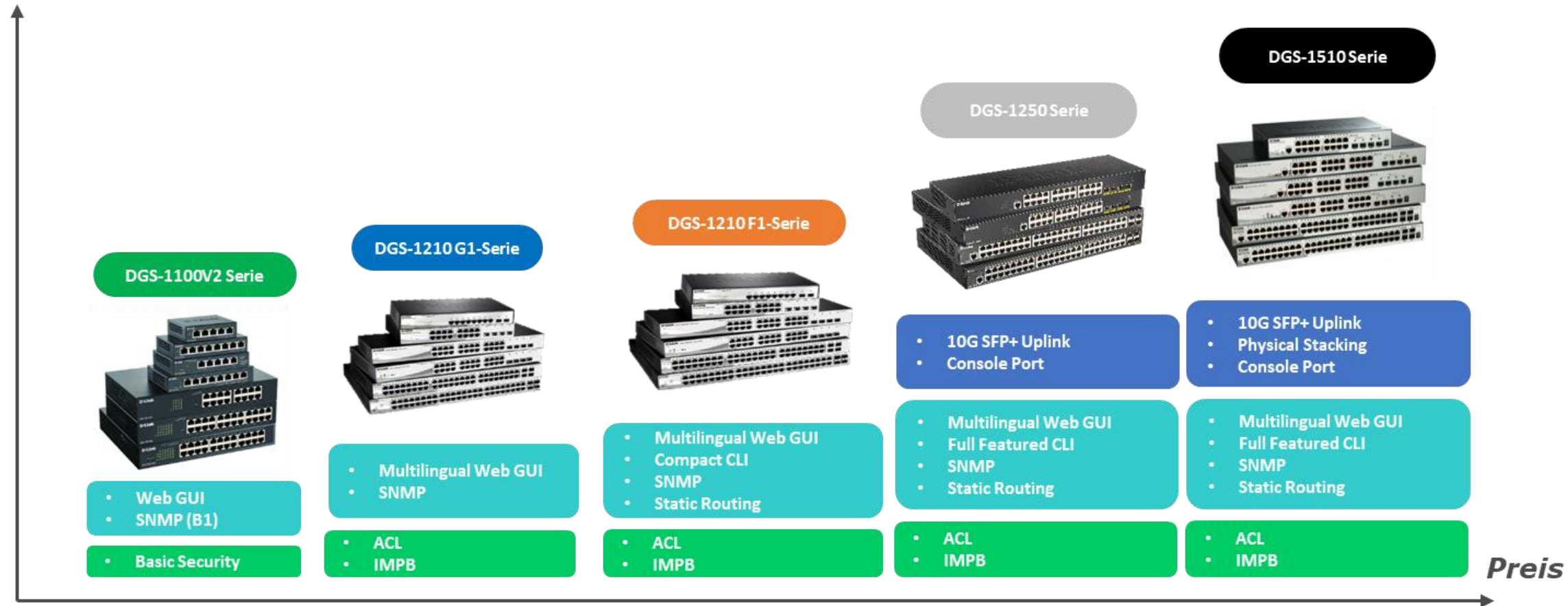
- ACL Switch Übersicht
 - Smart Managed
 - Full Managed
- ACL Grundlagen
- ACL Beispiel Routing
- ACL Beispiel Zugriffsteuerung Management
- ACL Status / Zähler

ACL

Access Control List

Gigabit Smart Switch Übersicht

Feature



■ DGS-1520 Switch Serie

DGS-1520-28

DGS-1520-52

DGS-1520-28MP

DGS-1520-52MP



Feature Highlights:

- 4 x 2.5G PoE ports (PoE Modelle)
- 2 x 10G RJ45
- 2 x 10G SFP+
- Stacking bis zu 8 Geräte / 80Gbps
- Redundantes Netzteil optional

Model	Port Configuration
DGS-1520-28	24*GE+2*SFP++2*10GE
DGS-1520-52	48*GE+2*SFP++2*10GE
DGS-1520-28MP	20*GE PoE+4*2.5GE PoE+2*SFP++2*10GE
DGS-1520-52MP	44*GE PoE+4*2.5GE PoE+2*SFP++2*10GE

10 Gigabit Smart Switch Übersicht

DXS-1210-10TS

8 x 100M/1000M/10GBits TP (RJ45) Port, 2 x SFP+ Slot

DXS-1210-12TC

10 x SFP+ Slot, 2 x TP / SFP+ Combo Port

DXS-1210-12TC

8 x 100M/1000M/10GBits TP (RJ45) Port, 2 x TP / SFP+ Combo Port, 2 x SFP+ Slot

DXS-1210-16TC

12 x 100M/1000M/10GBits TP (RJ45) Port, 2 x TP / SFP+ Combo Port, 2 x SFP+ Slot

DXS-1210-28T

24 x 10GbE & 4x 25G/SFP+

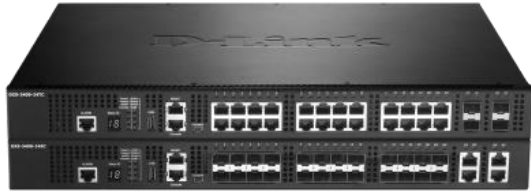
DXS-1210-28S

24 x 10SFP+



Managed Switches

DXS-3400-24TC
DXS-3400-24SC



DXS-3610-54S
DXS-3610-54T



DGS-3130-30TS
DGS-3130-30S
DGS-3130-30PS
DGS-3130-54TS
DGS-3130-54S
DGS-3130-54PS



DGS-3630-28TC
DGS-3630-28PC
DGS-3630-28SC
DGS-3630-52TC
DGS-3630-52PC



ACL Grundlagen

ACL Grundlagen

Über ACLs wird die Weiterleitung von Datenpaketen auf dem Switch beeinflusst

Haupteinsatzgebiete sind:

- Steuerung des Routing-Verhaltens

- Zugriffsteuerung des Switch Managements

- QoS Anpassung

- Blocken von unerwünschten Clients

- Blocken von unerwünschtem Traffic

ACL's ersetzen keine Firewall!

ACL Grundlagen

- ACL können erstellt werden als:
 - Layer 2 ACL (MAC Adresse)
 - Layer 3 ACL (IP Adresse)
 - Kombiniert MAC und IP
- Zusätzliche Trigger sind möglich wie z.B.:
 - Protokoll Type
 - TCP Port
 - ToS
 - TCP-Flags

ACL Grundlagen

Match IP Adresse

Quelle Any
 Host
 IP
Wildcard

Ziel Any
 Host
 IP
Wildcard

Match MAC Adresse

Quelle Any
 Host
 MAC
Wildcard

Ziel Any
 Host
 MAC
Wildcard

Match MAC Adresse

Quelle Any
 Host
 MAC
Wildcard

Ziel Any
 Host
 MAC
Wildcard

Match Port

Quelle-Port

Ziel-Port

IP-Vorrang
 DSCP (0-63)

ToS

Protokolltyp

Match IP Adresse

Quelle Any
 Host
 IP
Wildcard

Match MAC Adresse

Quelle Any
 Host
 MAC
Wildcard

Match Port

Quelle-Port

Ziel-Port

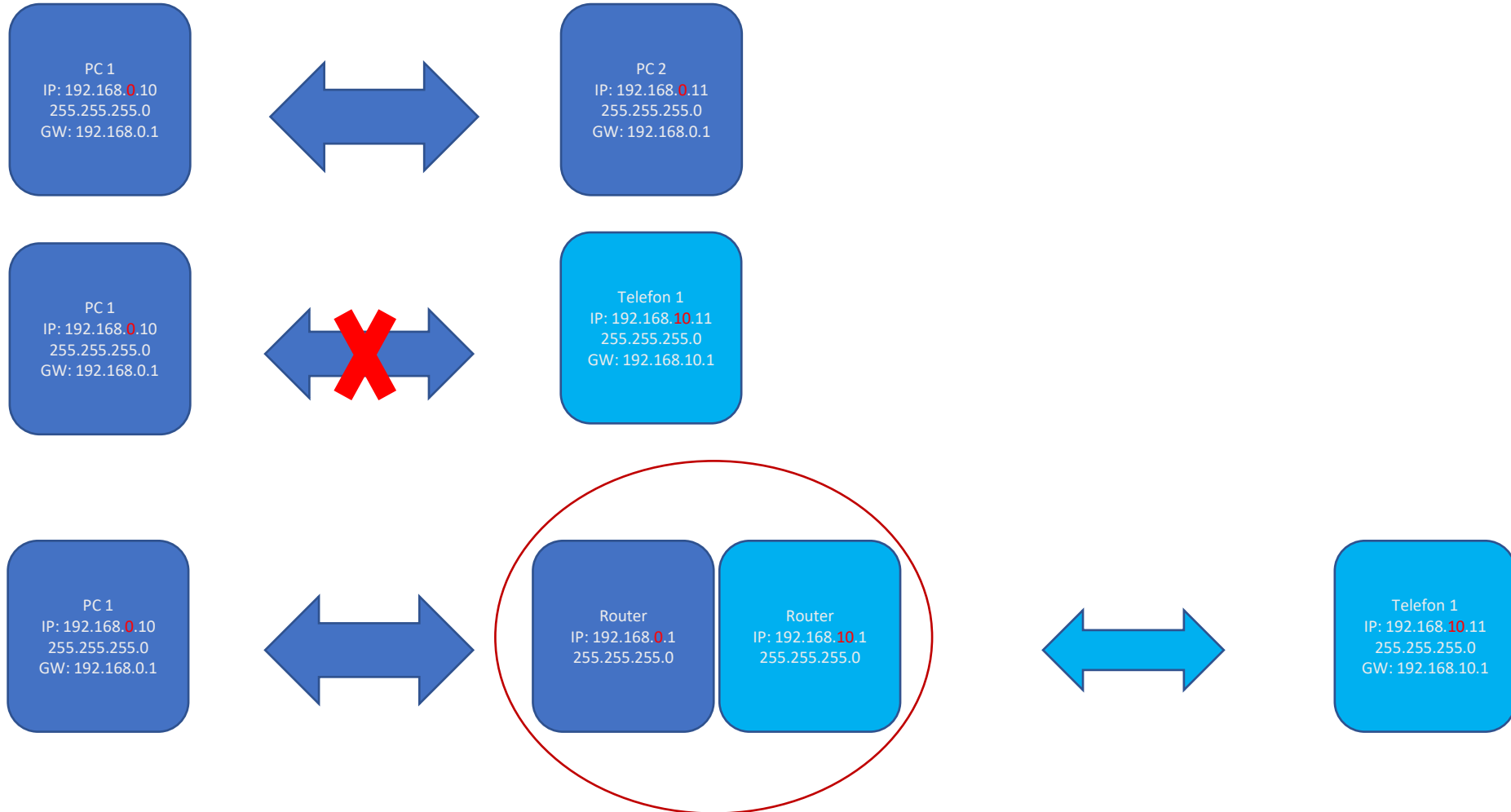
TCP-Flag

VID(1-4094)
 VLAN-Bereich

CoS

Zeitbereich

Routing



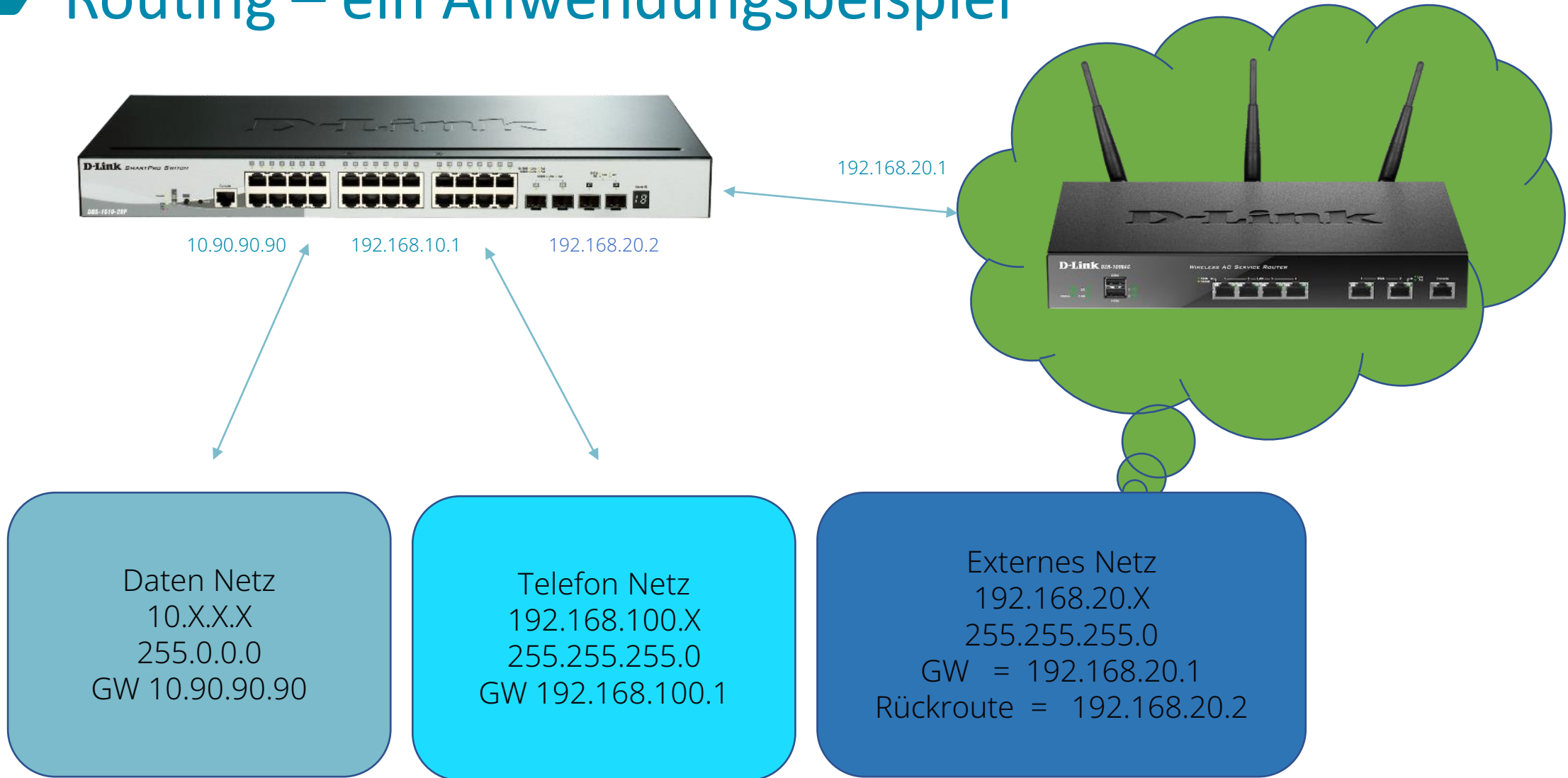
■ Konfiguration – grundsätzliches Vorgehen

- Für jedes geplante Netz ein VLAN konfigurieren
- Jedem VLAN ein IP-Netz zuweisen
 - **ACHTUNG das Routing beginnt sofort!**
- Default Gateway konfigurieren
 - Rückrouten im Gateway nicht vergessen!
- Ggf. (weitere) statische Routen anlegen
 - Notwendig wenn weitere Router verwendet werden
- Ggf. Routing über ACLs einschränken
 - Notwendig, wenn kein komplettes Routing erfolgen soll

■ Beispiel No. 1 – Routing zwischen zwei Subnetzen unterbinden

- ACHTUNG: Sobald ein Routing-fähiger Switch über mehrere IP Interfaces verfügt ist das Routing aktiviert!
- > Das Routing zwischen den Subnetzen soll verhindert werden
- > Routing zum Internet (Default Gateway) ist weiterhin aktiv

Routing – ein Anwendungsbeispiel



ACL anlegen - Routing

D-Link
Building Networks for People

D-Link SMARTPRO SWITCH
DGS-1510-20

Refresh Interval: 10 secs

Save Tools Wizard Online Help Surveillance Mode English

Fuzzy Search

- DGS-1510-20
 - System
 - Management
 - L2 Features
 - L3 Features
 - QoS
 - ACL**
 - ACL Configuration Wizard**
 - ACL Access List
 - ACL Interface Access Group
 - ACL VLAN Access Map
 - ACL VLAN Filter
 - Security
 - OAM
 - Monitoring
 - Green

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

Create

ACL Name:

Update

Note: The first character of ACL name must be a letter.

Bitte wählen Sie im Menü: ACL->ACL Configuration Wizard

Name der neuen ACL

ACL anlegen - Routing

D-Link
Building Networks for People

D-Link SMARTPRO SWITCH
DGS-1510-20

Console Fan OK Fail
Console

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 10/100M Link Act 1000M Link Act 1000M Link Act 1000M Link Act

Refresh Interval
10 secs

Save Tools Wizard Online Help Surveillance Mode English Logged in as: Administrator, ... Logout

Fuzzy Search

- DGS-1510-20
 - System
 - Management
 - L2 Features
 - L3 Features
 - QoS
 - ACL
 - ACL Configuration Wizard**
 - ACL Access List
 - ACL Interface Access Group
 - ACL VLAN Access Map
 - ACL VLAN Filter
 - Security
 - OAM
 - Monitoring
 - Green

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Which type of packet do you want to monitor?

MAC

IPv4

IPv6

Back Next

IPv4 als ACL Type auswählen

Warten auf 10.90.90.90...

ACL anlegen - Routing

D-Link
Building Networks for People

SMARTPRO SWITCH
DGS-1510-20

Refresh Interval: 10 secs

Save Tools Wizard Online Help Surveillance Mode English Logged in as: Administrator

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

Sequence No. (1-65535) Auto Assign

Protocol Type: TCP (0-255) Fragments

Assign rule criteria

IPv4 Address | Port | IPv4 DSCP | TCP Flag

Source: Any Host IP
IP: 10 . 90 . 90 . 90
Wildcard: 0 . 255 . 255 . 255

Destination: Any Host IP
IP: 192 . 168 . 100 . 1
Wildcard: 0 . 0 . 0 . 255

Time Range: 32 chars

Action: Permit Deny

Back Next

Quell und Zielnetzwerk angeben.
Achtung Format der Wildcards beachten!

Deny als Aktion auswählen um den Traffic zu unterbinden

ACL anlegen - Routing

D-Link
Building Networks for People

D-Link SMARTPro SWITCH
DGS-1510-20

Console Fan OK Fail Reset Console

Refresh Interval: 10 secs

Save Tools Wizard Online Help Surveillance Mode English Logged in as

Fuzzy Search

- DGS-1510-20
 - System
 - Management
 - L2 Features
 - L3 Features
 - QoS
 - ACL
 - ACL Configuration Wizard**
 - ACL Access List
 - ACL Interface Access Group
 - ACL VLAN Access Map
 - ACL VLAN Filter
 - Security
 - OAM
 - Monitoring
 - Green

ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> **Apply Port**

Which port(s) do you want to apply the Access-List?

From Port	To Port	Direction
eth1/0/1	eth1/0/20	In

Back Apply

Die ACL den entsprechenden Ports zuweisen

ACL anlegen - Routing

D-Link
SMARTPRO SWITCH
DGS-1510-20

Console Fan OK Fail Reset Console

Refresh Interval: 10 secs

Save Tools Wizard Online Help Surveillance Mode English Logged in as: Administrator, ... Logout

ACL Access List

ACL Type: All ID (1-14999) ACL Name: 32 chars

Total Entries: 1

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark
3999	routing	Extended IP ACL	10	10	Disabled	

routing (ID: 3999) Rule

Sequence No.	Action	Rule	Time Range	Counter
10	Deny	TCP 10.90.90.90 0.255.255...		

Übersicht der konfigurierten ACL's mit den entsprechenden Zugriffsregeln. Hier können ACL's auch manuell angelegt sowie die Regeln erweitert werden.

■ Beispiel No. 2 – Zugriff auf das Management unterbinden

- > Der Zugriff auf das Switch Management aus einem Subnetz (10.0.0.0/8) soll aus Sicherheitsgründen verhindert werden.
- > Ohne entsprechende ACL ist das Management über jedes Interface erreichbar.
- > Ein Client soll Zugriff auf das Management erhalten.

ACL Management

D-Link SMARTPRO SWITCH
DGS-1510-20

Refresh Interval: 10 secs

Save Tools Wizard Online Help Surveillance Mode English Logged in as:

Fuzzy Search

- DGS-1510-20
 - System
 - Management
 - L2 Features
 - L3 Features
 - QoS
 - ACL
 - ACL Configuration Wizard
 - ACL Access List
 - ACL Interface Access Group
 - ACL VLAN Access Map
 - ACL VLAN Filter
 - Security
 - OAM
 - Monitoring
 - Green

ACL Access List

ACL Access List

ACL Type: All | ID (1-14999) | ACL Name: 32 chars

Total Entries: 1

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	Edit	Delete
3999	routing	Extended IP ACL	10	10	Disabled			

routing (ID: 3999) Rule

Sequence No.	Action	Rule	Time Range	Counter	Delete
10	Deny	TCP 10.90.90.90 0.255.255...			

Buttons: Add ACL, Find, Add Rule, Clear All Counter, Clear Counter, Add Rule

ACL Management

D-Link
Building Networks for People

D-Link SMARTPRO SWITCH
DGS-1510-20

Refresh Interval: 10 secs

Logged in as: Administrator, ...

Add ACL Rule

Add ACL Rule

ID: 3999
ACL Name: routing
ACL Type: Extended IP ACL

Sequence No. (1-65535): [] (If it isn't specified, the system automatically assigns.)

Action: Permit Deny

Protocol Type: TCP

Match IP Address

Source: Any Host [] IP [10 . 90 . 90 . 1] Wildcard [0 . 255 . 255 . 255]

Destination: Any Host [10 . 90 . 90 . 90] IP [] Wildcard []

Match Port

Source Port: [Please Select] [] (0-65535) [Please Select] [] (0-65535)

Destination Port: [Please Select] [] (0-65535) [Please Select] [] (0-65535)

TCP Flag: ack fin psh rst syn urg

IP Precedence [Please Select] ToS [Please Select]

DSCP (0-63) [Please Select] []

Time Range: 32 chars

Back Apply

Deny / Verweigern als Aktion auswählen

Das zu sperrende Netzwerk (Quelle) sowie die Management IP des Switches (Ziel) angeben

ACL Management

D-Link SMARTPRO SWITCH
DGS-1510-20

Console Fan OK Fail Console Console

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 10/100M Link Act 1000M Link Act 1000M Link Act 1000M Link Act

Aktualisierungsintervall: 10 secs

Speichern Werkzeuge Assistent Online-Hilfe Überwachungsmodus Deutsch Angemeldet als: Administrator, ... Cie ses

Fuzzy Search

- DGS-1510-20
 - System
 - Verwaltung
 - L2 Funktionen
 - L3 Funktionen
 - QoS
 - ACL
 - ACL-Konfigurationsassistent
 - Zugriffsliste (ACL)**
 - ACL-Schnittstellen-Zugriffsgruppe
 - ACL VLAN Zugriffszuordnung
 - ACL VLAN-Filter
 - Sicherheit
 - OAM
 - Überwachung
 - Grün

Zugriffsliste (ACL)

Zugriffsliste (ACL)

ACL-Typ: ID (1-14999) ACL-Name

Gesamteinträge: 1

ID	ACL-Name	ACL-Typ	Startsequenz-Nr.	Schritt	Zählerstatus	Anmerkung	
3999	routing	Erweiterte IP ACL	10	10	Deaktiviert		<input type="button" value="Bearbeiten"/> <input type="button" value="löschen"/>

1/1 < < 1 > >

routing (ID: 3999) Regel

Laufnummer	Aktion	Regel	Zeitbereich	Zähler	
10	Verweigern	TCP 10.90.90.90 0.255.255...			<input type="button" value="löschen"/>
20	Verweigern	TCP 10.90.90.1 0.255.255...			<input type="button" value="löschen"/>

1/1 < < 1 > >

ACL Management

D-Link SMARTPRO SWITCH
DGS-1510-20

Speichern | Werkzeuge | Assistent | Online-Hilfe | Überwachungsmodus | Deutsch | Angemeldet als: Admin

Fuzzy Search

- DGS-1510-20
 - System
 - Verwaltung
 - L2 Funktionen
 - L3 Funktionen
 - QoS
 - ACL
 - ACL-Konfigurationsassistent
 - Zugriffsliste (ACL)**
 - ACL-Schnittstellen-Zugriffsgruppe
 - ACL VLAN Zugriffszuordnung
 - ACL VLAN-Filter
 - Sicherheit
 - OAM
 - Überwachung
 - Grün

Zugriffsliste (ACL)

ACL-Typ: ID (1-14999) ACL-Name Aktualisierungsintervall: 10 secs

Gesamteinträge: 1

ID	ACL-Name	ACL-Typ	Startsequenz-Nr.	Schritt	Zählerstatus	Anmerkung	
3999	routing	Erweiterte IP ACL	10	10	Deaktiviert		<input type="button" value="Bearbeiten"/> <input type="button" value="löschen"/>

1/1 < < 1 > >

routing (ID: 3999) Regel

Laufnummer	Aktion	Regel	Zeitbereich	Zähler	
10	Verweigern	TCP 10.90.90.90 0.255.255...			<input type="button" value="löschen"/>
20	Verweigern	TCP 10.90.90.1 0.255.255....			<input type="button" value="löschen"/>

1/1 < < 1 > >

Neue Regel zwischen Regel 10 und 20 einfügen.

ACL Management

The screenshot shows the D-Link web interface for configuring an ACL rule. The main form is titled "ACL-Regel hinzufügen". The configuration details are as follows:

- ID: 3999
- ACL-Name: routing
- ACL-Typ: Erweiterte IP-ACL
- Laufnummer (1-65535): 15 (Ist es nicht angegeben, wird es automatisch vom System zugewiesen.)
- Aktion: Erlauben Verweigern
- Protokolltyp: TCP
- Match IP Adresse:
 - Quelle: Any Host (10.90.90.222) IP
 - Ziel: Any Host (10.90.90.90) IP
- Match Port:
 - Quell-Port: (Bitte auswählen)
 - Ziel-Port: (Bitte auswählen)
- TCP-Flag: Jack Fin Psh Rst Syn Urg
- IP-Vorrang: (Bitte auswählen)
- DSCP (0-63): (Bitte auswählen)
- ToS: (Bitte auswählen)
- Zeitbereich: 32 chars

Buttons: Back, Anwenden

Laufende Nummer zwischen 10 und 20 sowie Erlauben / Permit als Aktion auswählen

Den zugelassenen Host (Quelle) sowie die Management IP des Switches (Ziel) angeben

ACL Management

D-Link
Building Networks for People

DGS-1510-20 SMARTPRO SWITCH

Speichern Werkzeuge Assistent Online-Hilfe Überwachungsmodus Deutsch

Fuzzy Search

- DGS-1510-20
 - System
 - Verwaltung
 - L2 Funktionen
 - L3 Funktionen
 - QoS
 - ACL
 - ACL-Konfigurationsassistent
 - Zugriffsliste (ACL)**
 - ACL-Schnittstellen-Zugriffsgruppe
 - ACL VLAN Zugriffszuordnung
 - ACL VLAN-Filter
 - Sicherheit
 - OAM
 - Überwachung
 - Grün

Zugriffsliste (ACL)

Zugriffsliste (ACL)

ACL-Typ ID (1-14999) ACL-Name

Gesamteinträge: 1

ID	ACL-Name	ACL-Typ	Startsequenz-Nr.	Schritt	Zählerstatus	Anmerkung	
3999	routing	Erweiterte IP ACL	10	10	Deaktiviert		<input type="button" value="Bearbeiten"/> <input type="button" value="löschen"/>

1/1 |< < 1 > > |

routing (ID: 3999) Regel

Laufnummer	Aktion	Regel	Zeitbereich	Zähler	
10	Verweigern	TCP 10.90.90.90 0.255.255...			<input type="button" value="löschen"/>
15	Erlauben	TCP host 10.90.90.222 ho...			<input type="button" value="löschen"/>
20	Verweigern	TCP 10.90.90.1 0.255.255....			<input type="button" value="löschen"/>

1/1 |< < 1 > > |

Der Zugriff auf das Management ist nun wieder für eine IP erlaubt.

ACL – Status | Zähler

Zähler für die jeweilige ACL aktivieren

Wenn eine Regel greift wird der Zähler entsprechend erhöht.

Zähler auf folgenden Ports aktivieren
Ingress port(s): eth1/0/1

ID	ACL-Name	ACL-Typ	Startsequenz-Nr.	Schritt	Zählerstatus	Anmerkung
8000	test	Erweiterte Expert ACL	10	10	Aktiviert	

Laufnummer	Aktion	Regel	Zeitbereich	Zähler
10	Erlauben	TCP any host A8-1E-84-AA...		(Ing: 128 Pakete)



➤ Ihr persönlicher Draht zu D-Link für...

- Vertiefende Fragen
- Schulungen vor Ort
- Demogeräte
- Kostenfreie Services
- Unterstützung bei Planung und Projekten
- ... und vieles mehr

West



[Michael Bonikowski](#)

Südwest



[Sebastian Boyé](#)

Nordost



[Wolfram Obrikatis](#)

Südost



[Patrick Sychra](#)

Ihr persönlicher Ansprechpartner in der Region begleitet Sie im Projekt – von der Planung bis zur Fertigstellung und darüber hinaus.

Kurzum - für Fragen rund um Ihr Netzwerkgeschäft sind wir für Sie da.

D-Link[®]