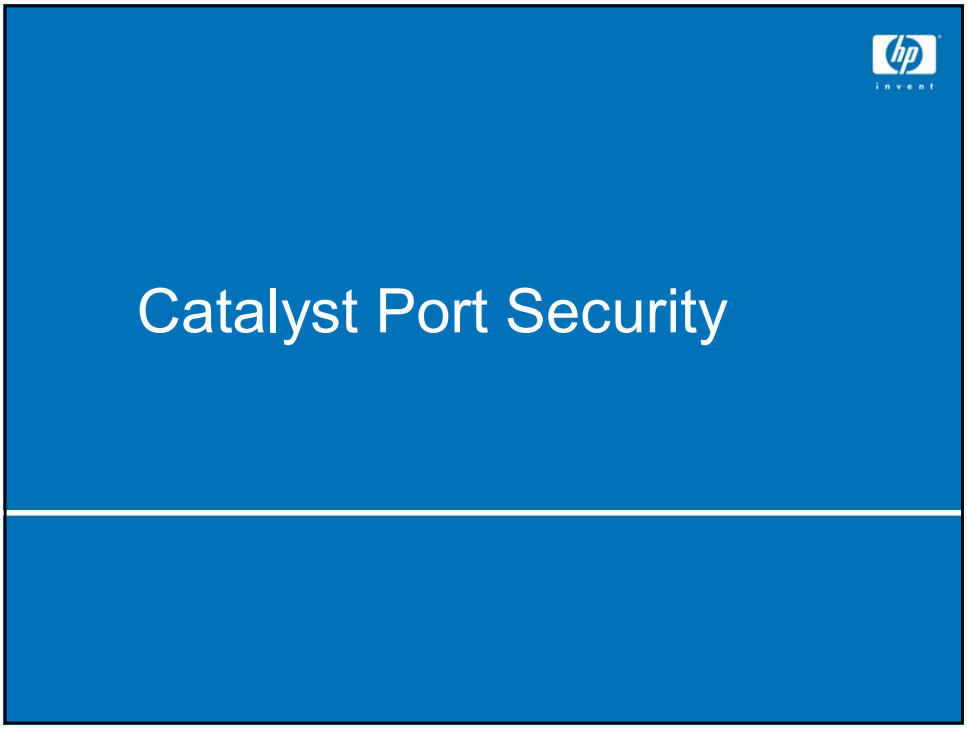
Cisco LAN Security

2B04

Andreas Aurand
Network Consultant NWCC, HP

Agenda

- **Catalyst Port Security**
- **Private VLANs**
  - VLAN ACLs
  - ARP Inspection
- **DHCP Snooping**
- **Konfiguration von Switch Ports**



Port Security

- Schutz vor gefälschten MAC-Adressen
  - Switch lässt nur eine definierte Anzahl von MAC-Adressen pro Port zu
  - Schutz gegen MAC Flooding, MAC Spoofing, (DHCP Starvation)
- CatOS-Konfiguration

```
set port security mod/port enable
set port security mod/port violation restrict | shutdown
set port security mod/port maximum 1
[ set port security mod/port unicast-flood disable ]
```

- IOS-Konfiguration

```
errdisable recovery cause psecure-violation
errdisable recovery interval 300
interface name
  switchport mode access
  switchport port-security
  switchport port-security violation restrict | shutdown
  switchport port-security maximum 1
  [ switchport block unicast ]
```

April 21, 2004 Andreas Aurand, HP Network Competence Center 4

Port Security – Secure MAC Address

- Switch trägt dynamisch gelernte **sichere MAC-Adressen** als statische MAC-Adressen in CAM-Tabelle ein
  - Switch übernimmt Adressen automatisch in seine Konfiguration
  - Adresse kann nicht mehr überschrieben werden

CatOS> (enable) show port security 3/15

```
* = Configured MAC Address
Port   Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
------ -------- --------- ------------- -------- -------- ------- -------
 3/15  enabled  shutdown              0        0        1 disabled      24
Port   Num-Addr Secure-Src-Addr     Age-Left Last-Src-Addr     Shutdown/Time-Left
------ -------- ------------------ -------- ----------------- ------------------
 3/15          1 00-04-c1-7d-d6-54        - 00-04-c1-7d-d6-54       no          -
```

CatOS> (enable) show cam static

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ---------------------------------------
10    00-04-c1-7d-d6-54  X          3/15
Total Matching CAM Entries Displayed  = 1
```


Port Security – was passiert

- ***Violation Shutdown*** (Standardverhalten)
  - Bei Verletzung der Port Security wird Port auf „*shutdown*“ gesetzt
  - set port security *mod/port* shutdown *time* legt Zeitdauer fest
  - Ohne *shutdown time* muss Port manuell aktiviert werden
- ***Violation Restrict***
  - Bei Verletzung der Port Security werden Pakete von „unsicheren“ Hosts verworfen, Port bleibt aber oben
- **Verletzung der Sicherheit eines Ports**
  - Switch sieht mehr MAC-Adressen an einem Port als erlaubt
  - Quelladresse ist bereits *Secure MAC Address* eines anderen Port
    - Der Port geht in diesem Fall auch bei *violation restrict* auf „*shutdown*“

Port Security – was passiert

- SYSLOG-Meldung

  c6506> (enable) show logging buffer

```
%SECURITY-1-PORTSHUTDOWN:Port 3/13 shutdown due to security violation
```

- Port-Informationen

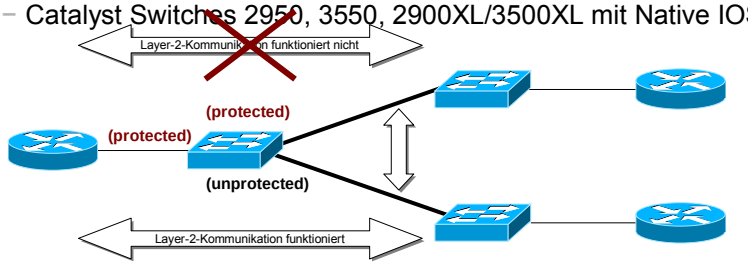
  c6506> (enable) show port security 3/13

```
* = Configured MAC Address
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- --------- --------- ------------ -------- -------- -------- -------
 3/13  enabled   restrict             0        0        1 disabled      22

Port  Num-Addr Secure-Src-Addr     Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- -----------------  -------- ----------------- ------------------
 3/13        0                 -        - 00-04-c1-7d-d6-54       yes          -

Port  Flooding on Address Limit
----- --------------------------
 3/13                   Enabled
```


Private VLANs und Protected Ports

Protected Ports

- „Abgeschwächtes“ privates VLAN
  - Verhindert direkte Layer-2-Kommunikation zwischen geschützten Ports
  - Gilt nur für lokalen Switch
  - Catalyst Switches 2950, 3550, 2900XL/3500XL mit Native IOS



- Konfiguration

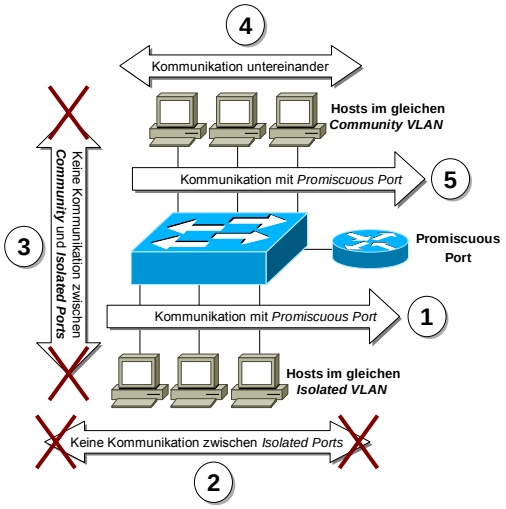
```
Interface name
 switchport protected
```


Private VLANs – Übersicht

- PVLANs trennen auf Layer-2-Ebene den Datentransfer innerhalb eines VLANs
  - keine Host-zu-Host Kommunikation mehr zwischen bestimmten Ports möglich
- Das eigentliche VLAN (***Primary VLAN***) wird aufgeteilt in
  - ***Promisuous Ports***
  - ***Isolated Ports***
  - ***Community Ports***
  - zusammen als ***Secondary VLAN*** bezeichnet.
- Private VLANs sind nicht auf einzelne Switches beschränkt, sie können sich über mehrere Switches erstrecken

Private VLANs – Übersicht

- ***Isolated Ports*** können nur mit ***Promiscuous Ports*** kommunizieren **(1)**. Nicht mit anderen Isolated **(2)** oder Community Ports **(3)**.
- ***Community Ports*** können mit anderen *Community Ports* des gleichen Community VLAN **(4)** sowie mit *Promiscuous Ports* **(5)** kommunizieren
- Ports an Switches, die keine privaten VLANs unterstützen, können nur untereinander und mit dem *Promiscuous Port* kommunizieren.



Private VLAN - Konfiguration

- Catalyst 6000, 4000, 2980G, 2948G und 4912G
  - **VTP ausschalten** (oder VTP Version 3)

```
CatOS> (enable) set vtp mode transparent
```

  - ***Primary VLAN*** **definieren**

```
CatOS> (enable) set vlan 51 pvlan-type primary
```

  - ***Isolated VLAN*** **definieren**

```
CatOS> (enable) set vlan 151 pvlan-type isolated
```

  - ***Community VLAN*** **definieren**

```
CatOS> (enable) set vlan 251 pvlan-type community
```

  - ***Isolated Ports*** **definieren**

```
CatOS> (enable) set pvlan 51 151 3/40-3/48
```

  - ***Community Ports*** **definieren**

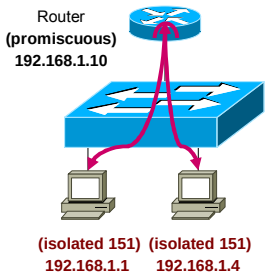
```
CatOS> (enable) set pvlan 51 251 3/29,3/42
```

  - ***Promiscuous Ports*** **definieren**

```
CatOS> (enable) set pvlan mapping 51 151 3/2
CatOS> (enable) set pvlan mapping 51 251 3/2
```

Private VLANs – Intrasubnetz Routing

- Host-Routen, die auf Router am *Promiscuous Port* zeigen
  - Host sendet Daten zuerst an Router, der leitet Pakete dann an das Zielsystem weiter
- **Lösung: ACLs**

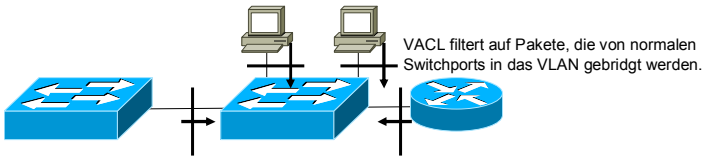


route add –host 192.168.1.1 gw 192.168.1.10

route add –host 192.168.1.4 gw 192.168.1.10

VLAN ACL

- Bei Layer-2-geswitchten Paketen wird **VLAN ACL** nur auf das **Input VLAN** angewandet.
  - Überprüfung gegen Access-Liste erfolgt auf dem Port, an dem Switch das Paket zum erstem Mal empfängt.



- VACL für **Primary *VLAN***
  - Daten, die Switch **vom Promiscuous Port** annehmen soll
- VACL für **Secondary *VLANs***
  - Applikationen, die an **Isolated** und **Community Ports** freigeben sind

VLAN ACL - Konfiguration

- Intrasubnetz-Routing über *Promiscuous Port* ausschalten

```
set security acl ip PVLAN51 permit icmp host 192.168.1.10 any
set security acl ip PVLAN51 permit tcp host 192.168.1.10 eq telnet host 192.168.1.4
set security acl ip PVLAN51 deny ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
set security acl ip PVLAN51 permit ip any any
```

- Applikationen für *Isolated Port* freigeben
  - HTTP und Telnet zum Host 192.168.1.1 von Systemen außerhalb 192.168.1.0 / 24

```
set security acl ip IsolatedPVLAN151 deny ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
set security acl ip IsolatedPVLAN151 permit tcp host 192.168.1.1 eq 80 any
set security acl ip IsolatedPVLAN151 permit tcp host 192.168.1.1 eq 23 any
```

- VACLs aktivieren

```
commit security acl all
!
set security acl map IsolatedPVLAN151 151
set security acl map PVLAN51 51
```

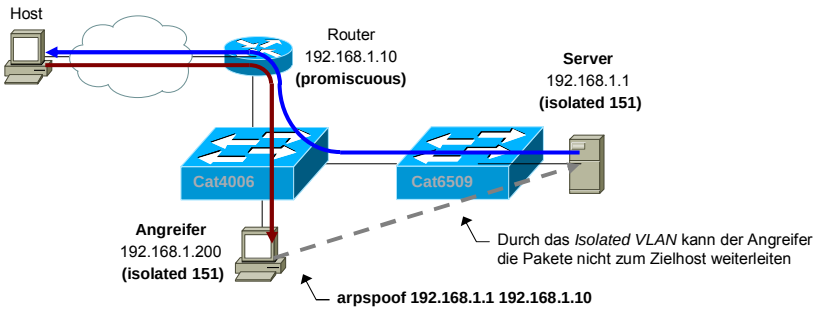

Router ACL

- Nicht alle Switches unterstützen VACLs
  - ACL direkt auf dem Router konfigurieren

```
interface GigabitEthernet4
  description -- Router Port fuer Subnetz 192.168.1.0/24 --
  ip address 192.168.1.10 255.255.255.0
  ip access-group DenyLocalForwarding in
!
ip access-list extended DenyLocalForwarding
  permit icmp any host 192.168.1.10
  permit tcp host 192.168.1.4 host 192.168.1.10 eq telnet
  deny ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
  permit ip any any
!
end
```

ARP Spoofing auf Promiscuous Port

- PVLAN-Schutzmechanismen erlauben weiterhin ***ARP Spoofing*** auf Systeme am ***Promiscuous Port***
  - Angreifer kann Pakete nicht mehr an das Zielsystem weiterleiten
- Daher „lediglich“ DoS-Attacken möglich



Mögliche Schutzmaßnahmen

- Statische MAC-Einträge auf Router
  - Vorsicht: manche Betriebssysteme überschreiben statische ARP-Einträge (z.B. Windows)
  - Skaliert schlecht
- ***Sticky ARP***
  - Catalyst 6000 Serie mit MSFC-Routerkarte (ab V12.1(8a)EX)
- ***ARP Inspection***
  - Catalyst 6500 Serie mit SUP2 und PFC2 (ab V7.5)
- ***Dynamic ARP Inspection (DAI)***
  - Catalyst 4500 mit Native IOS (ab V12.1(19)EW)
- ***DHCP Secured Address Assignment***
  - IOS Router (ab V12.2(15)T)

Sticky ARP

- MSFC (Router-Karte im Switch) überschreibt keine ARP-Einträge von Hosts aus privaten VLANs
- Angreifer kann *ARP Cache* auf der MSFC-Karte nicht mehr verändern

Sticky ARP Eintrag

```
c6509msfc# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            1   0050.3edb.04c1  ARPA   Vlan51 pv 151
Internet  192.168.1.2            0   0050.3edb.04e1  ARPA   Vlan51 pv 251

c6509msfc# show logging
%IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: 192.168.1.3,
hw: 0030.9497.0e21 by hw: aa00.0400.0102
```

- VLAN Interface für *Primary VLAN* auf MSFC definieren

```
ip sticky-arp
interface Vlan51
  ip address 192.168.1.11 255.255.255.0
```

- Schnittstelle zur MSFC auf Switch als *Promiscuous Ports* definieren

```
c6509> (enable) set pvlan mapping 51 151 15/1
```

April 21, 2004 Andreas Aurand, HP Network Competence Center 19

ARP Inspection

- ARP-Pakete werden von Switch-CPU überprüft
  - ***ARP Binding Filter*** (MAC und IP-Adresse im ARP Paket)
  - ARP-Paket mit **ungültigen MAC- und IP-Adressen**
  - **Vergleich der MAC-Adresse** im Ethernet-Header und im ARP-Paket

April 21, 2004 Andreas Aurand, HP Network Competence Center 20

ARP Inspection

- ***ARP Binding Filter***

IP-Address im *ARP Header* — MAC-Address im *ARP Header*

set security acl ip *name* permit|deny **arp-inspection host *ip-addr mac-addr*** [log]
set security acl ip *name* permit|deny **arp-inspection host *ip-addr* any** [log]
set security acl ip *name* permit|deny **arp-inspection *ip-addr mask* any** [log]
set security acl ip *name* permit|deny **arp-inspection any any** [log]

- **Vergleich** MAC-Adresse im Ethernet-Header mit ARP-Paket
  - Paket verwerfen
    - set security acl **arp-inspection match-mac enable drop**
  - Nur SYSLOG-Meldung generieren
    - set security acl **arp-inspection match-mac enable**

ARP Inspection

- Paket auf **ungültige** MAC- oder IP-Adressen überprüfen
  - **MAC-Adressen**
    - 00-00-00-00-00-00
    - Alle Multicast-Adressen
    - Broadcast (FF-FF-FF-FF-FF-FF)
  - **IP-Adressen**
    - 0.0.0.0
    - Alle IP-Multicast-Adressen (224.x.x.x – 239.x.x.x)
    - Broadcast (255.255.255.255); verhindert ***Gratuitous ARP***
  - **Paket verwerfen**
    - set security acl **arp-inspection address-violation enable drop**
  - **Nur Log-Meldung generieren**
    - set security acl **arp-inspection address-violation enable**

DHCP Secured IP Address Assignment

- Modifikation der MAC-Adressen von DHCP-Clients im *ARP Cache* des Routers nicht mehr möglich
  - Ab IOS **V12.2(15)T** verfügbar
- Router muss DHCP-Server des LANs sein
  - DHCP Datenbank kann extern abgespeichert werden

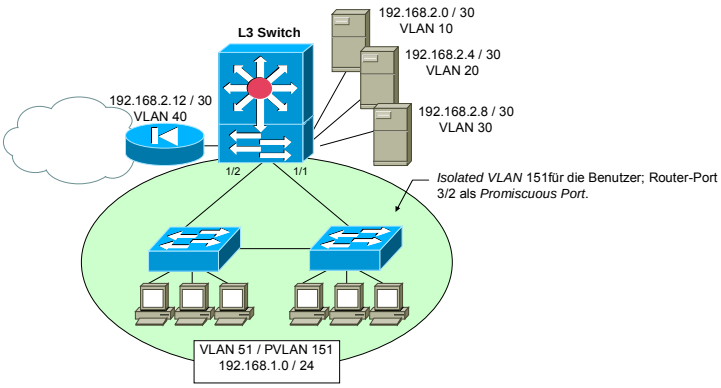
```
ip dhcp pool LAN
  network 10.185.208.0 255.255.248.0
  default-router 10.185.208.66
  update arp
```

```
show ip dhcp server statistics
Memory usage          14027
Address pools         1
Database agents       0
Automatic bindings    1.
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    1
```

Anzahl der "gesicherten" ARP-Einträge auf dem DHCP-Server, die nicht mehr modifiziert werden können.

Layer-3-Trennung

- Schutz gegen die meisten Layer-2-Attacken
- Separates VLAN für jedes wichtige System
- Restlichen Hosts kommen in ein privates VLAN



Schutzmaßnahmen gegen IP-basierende Angriffe

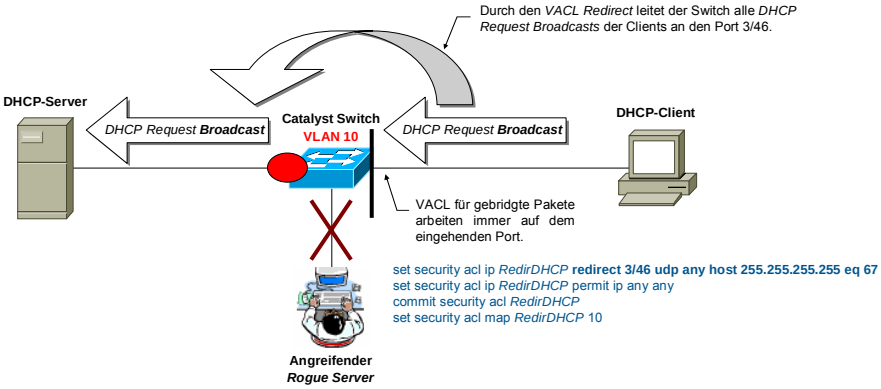
Schutz gegen DHCP-Angriffe

- **DHCP Starvation**
  - ***Port Security*** als Schutzmechanismus
  - kann man aber auch umgehen
- **DHCP Rogue Server**
  - ***VLAN ACL Redirects***
  - ***DHCP Snooping*** (Catalyst 4500 ab V12.1(12))

April 21, 2004 Andreas Aurand, HP Network Competence Center 26

VLAN ACL Redirects

- Die ***Redirect VACL*** leitet die als Broadcast gesendeten *DHCP Requests* der Clients nur an den Port des DHCP-Servers weiter
- **Nachteil**: Alle Switches des IP-Subnetzes müssen VACLs unterstützen, ansonsten ist kein vollständiger Schutz möglich



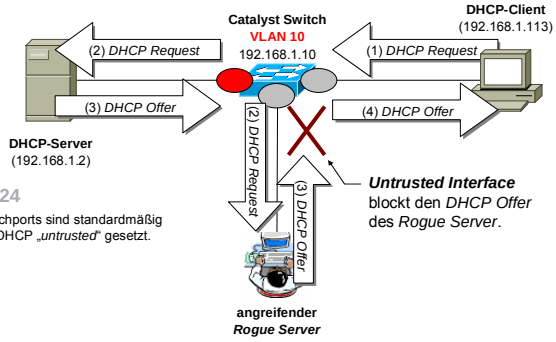
DHCP Snooping

- Switch unterscheidet der zwischen vertrauenswürdigen (***trusted***) und nicht vertrauenswürdigen (***untrusted***) Schnittstellen
- Auf nicht vertrauenswürdigen Schnittstellen sind **keine DHCP-Server-zum-Client-Pakete** (d.h. ***BOOTP Replies***) erlaubt

```
ip dhcp snooping
ip dhcp snooping vlan 10
!
interface fastethernet0/1
  switchport mode access
  switchport access vlan 10
  ip dhcp snooping trust
!
interface range fastethernet0/2 – 24
  switchport mode access
  switchport access vlan 10
  ip dhcp snooping limit rate 10
```

Switchports sind standardmäßig auf DHCP „*untrusted*" gesetzt.

Rate Limiting für normale Schnittstellen (DHCP-Pakete pro Sekunde)



Schutz gegen IP-Spoofing

- Definition von entsprechenden Filter
  - Anti-IP-Spoofing Mechanismen auf dem Perimeter-Router geblockt.
- ***IP Source Guard***
  - Funktionalität im Zusammenhang mit *DHCP Snooping*
  - Switch lässt auf einem ***untrusted Port*** zuerst nur DHCP-Pakete durch und blockt alle anderen IP-Pakete.
  - Erzeugt ***per-Port ACL*** für zugewiesene IP-Adresse bzw. für Kombination von IP- und MAC-Adresse

```
ip dhcp snooping
ip dhcp snooping vlan 10
ip dhcp snooping information option
interface name
no ip dhcp snooping trust
  ip verify source vlan dhcp-snooping [ port-security ]
  switchport port-security limit rate invalid-source-mac # | none
  switchport port-security violation shutdown | restrict
```

Überprüfung der MAC- und IP-Adresse

Angabe, bei vielen ungültigen Paketen die *Port Security* greift.

April 21, 2004 Andreas Aurand, HP Network Competence Center 29

Schutz gegen HSRP-Angriffe

- **MD5-Authentisierung** der HSRP-Pakete
  - Ab der IOS Version V12.3(2)T verfügbar
  - Potentieller Angreifer kann das verwendete Passwort nicht erkennen
  - Router ignorieren HSRP-Pakete ohne eine gültige MD5-Prüfsumme
- Konfiguration auf den Routern

```
interface FastEthernet0
 ... ... ...
  standby ip 10.185.208.222
  standby priority 101
  standby preempt
  standby authentication md5 key-string fdjfot0ertujklfg
```

April 21, 2004 Andreas Aurand, HP Network Competence Center 30

Schutzmaßnahmen gegen VLAN Hopping und STP-Attacken

VLAN Hopping

- **Niemals VLAN 1 verwenden**
  - gilt für Trunk und Access Ports
- **Eigenes *Native VLAN* für Trunk-Verbindungen**
- **DTP auf normalen Switchports ausschalten**
- **Unbenutzte Ports ausschalten und in unbenutztes VLAN legen**

Catayst OS

- Trunk Ports

  CatOS> (enable) **set vlan 500** *mod/ports*
  CatOS> (enable) **set trunk** *mod/ports* **on**

- Access Ports

  CatOS> (enable) **set vlan 10** *mod/ports*
  CatOS> (enable) **set trunk** *mod/port* **off**

oder

  CatOS> (enable) **set port** mod/ports **host**

Cisco Integrated IOS

- Trunk Ports

  interface *name*
  switchport trunk native vlan 500
  switchport mode trunk

- Access Ports

  interface *name*
  switchport access vlan 10
  switchport mode access

oder

  switchport host

April 21, 2004 Andreas Aurand, HP Network Competence Center 32

Spanning-Tree-Attacken

- Normale Switchports
  - Catalyst OS
    ```
    set spantree portfast bpdu-guard enable
    set spantree portfast mod/port enable
    ```
  - IOS
    ```
    spanning-tree portfast bpduguard
    interface name
      spanning-tree portfast
    ```
- Trunk Ports zu Switches, die keine *Root Bridge* werden dürfen
  - Calatyst OS
    ```
    set trunk mod/port on
    set spantree guard root mod/port
    ```
  - IOS
    ```
    interface name
      spanning-tree guard root
      switchport mode trunk
    ```

April 21, 2004 Andreas Aurand, HP Network Competence Center 33

BPDU Guard – was passiert

- SYSLOG-Meldung

```
Cat2950# show logging
%SPANTREE-2-RX_PORTFAST: Received BPDU on PortFast enabled port.
Disabling FastEthernet0/9.
%PM-4-ERR_DISABLE: bpduguard error detected on Fa0/9,putting Fa0/1 in err-disable state
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/9, changed state to down
```

- Port-Informationen

```
Cat2950# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (Vlan_1)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Protected: false
Voice VLAN: none (Inactive)
Appliance trust: none
```

BPDU Guard setzt den Port auf „down“.

April 21, 2004 Andreas Aurand, HP Network Competence Center 34

Root Guard – was passiert

- SYSLOG-Meldung

Cat2950# show logging

```
%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/9 on VLAN1.
```

- Port-Informationen

„*Root Guard*“ setzt den Port auf „broken“

Cat2950# show interface fa0/9 switchport

```
Port 1 (FastEthernet0/9) of VLAN1 is broken (Root Inconsistent)
   Port path cost 100, Port priority 128, Port Identifier 128.1.
   Designated root has priority 0, address 000a.415e.4580
   Designated bridge has priority 32768, address 0009.b7f7.e70a
   Designated port id is 128.1, designated path cost 62
   Timers: message age 1, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 1608, received 27
   Root guard is enabled
```

April 21, 2004 Andreas Aurand, HP Network Competence Center 35

Zusammenfassung

VLANs bieten KEINE erhöhte Sicherheit !

Weitere Sicherheitseinstellungen sind notwendig !

April 21, 2004 Andreas Aurand, HP Network Competence Center 36

Links

- Cisco SAFE Layer 2 Application Note
  - http://www.cisco.com/go/safe
- Securing Networks with Private VLANs and VLAN ACLs
  - http://www.cisco.com/warp/public/473/90.shtml
- Catalyst Secure Template
  - http://www.qorbit.net/documents/catalyst-secure-template.htm

Fragen