VLAN Security

3B04

Andreas Aurand
Network Consultant

HP NWCC

DECUS Symposium 2003

Agenda

- **Warum Ethernet Security ? Mögliche Angriffsszenarien**
- **MAC-Angriffe**
  - MAC Flooding
  - MAC Spoofing
  - Port Security
  - IEEE 802.1X Port Authentication
- **ARP Spoofing**
  - ARP Cache Poisoning
  - Private VLANs
  - VLAN ACLs
  - Sticky ARP
  - ARP Inspection
- **VLAN Hopping**
- **Spanning Tree Angriffe**

Warum Ethernet Security ?

Angriffsszenarien

Passwort Sniffing

Router VTY ACLs umgehen

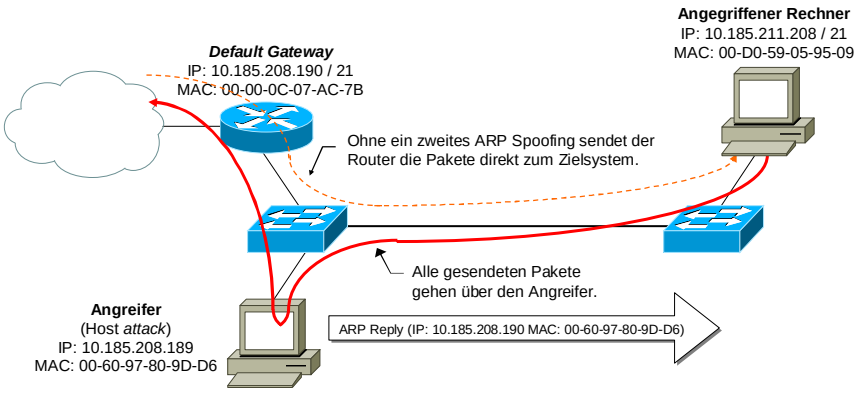
MitM-Attacke mit DNS Spoofing

DHCP Starvation

Ziel eines Angreifers

- **Gesendete Pakete mitprotokollieren**
  - Passwörter
  - Sensitive Informationen
- **Verbindungen über den eigenen Rechner umleiten**
  - Man-in-the-Middle-Attacke (MitM)
    - Verschlüsselte Verbindungen knacken
    - Informationen modifizieren
  - Session Hijacking
- **Denial-of-Service-Angriffe (DoS)**
  - Auf wichtige Server (z.B. DHCP- oder DNS-Server)
  - Auf wichtige Infrastrukturkomponenten (Router, Firewall, Switch)

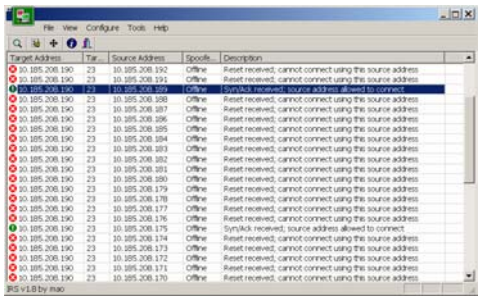
Passwort Sniffing

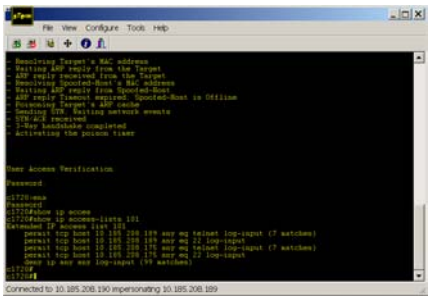



```
attack:~ # dsniff -cn
dsniff: listening on eth0
-----------------
10/28/02 13:16:15 tcp 10.185.211.208.2137 -> 10.204.208.33.23 (telnet)
ena
c
exit
```

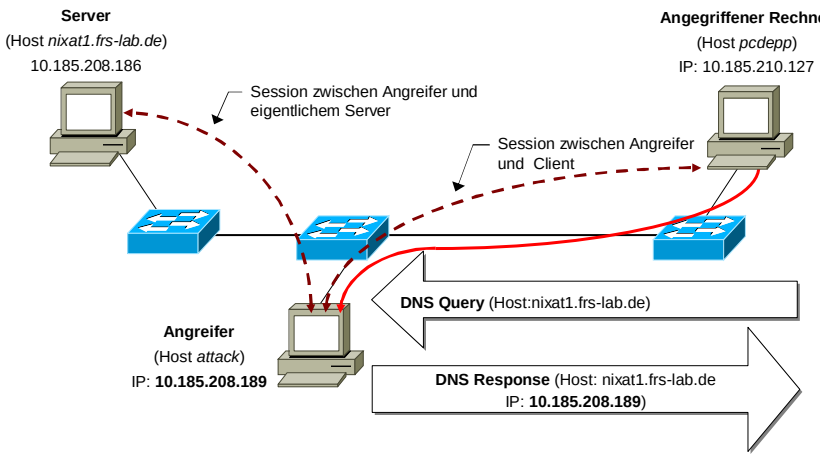

Router VTY ACLs umgehen

- IP und ARP Spoofing ermöglicht, dass Angreifer ACLs umgeht, mit denen Zugriff auf Router/Firewall eingeschränkt ist
  - (Source) IP Spoofing
    - Angreifer probiert verschiedene Adressen als IP-Quelladressen aus
  - ARP Spoofing
    - ARP Cache auf dem Router wird modifiziert um eine Antwort zu bekommen

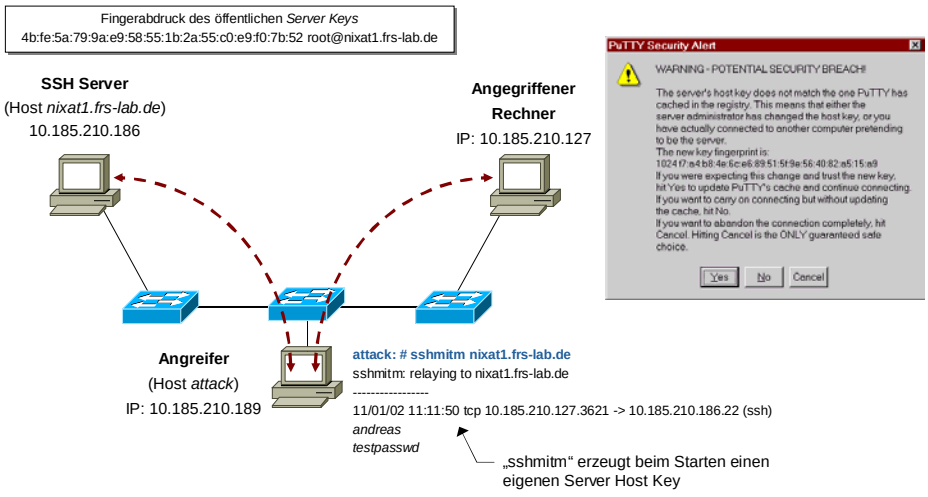




DNS Spoofing



SSH MitM-Attacke



DHCP Starvation

- Ein Angreifer "*spooft*" den DHCP Packet Exchange
  - Fordert alle verfügbaren IP-Adressen vom Servers an
- Server kann neuen Clients keine Adresse mehr zuweisen
  - DoS-Attacke auf den DHCP-Server.

```
attack# DHCPGobbler -g
Detecting DHCP service for gobble attack
DHCP server at 192.168.1.190 offering 192.168.1.101 with
subnet mask 255.255.255.0 gateway 192.168.1.1 and DNS 10.185.208.34
192.168.1.101 gobbled using MAC 0:28:c:a8:5e:a7
192.168.1.102 gobbled using MAC 0:a8:25:24:5e:51
192.168.1.103 gobbled using MAC 0:48:c4:b3:a9:a0
192.168.1.104 gobbled using MAC 0:3c:63:ab:41:f3
192.168.1.105 gobbled using MAC 0:73:92:a7:75:1b
192.168.1.106 gobbled using MAC 0:ca:44:1a:73:a2
192.168.1.107 gobbled using MAC 0:4a:ca:67:ee:29
192.168.1.108 gobbled using MAC 0:77:f1:7d:2b:9b
192.168.1.109 gobbled using MAC 0:5d:d7:1:88:99
192.168.1.110 gobbled using MAC 0:33:d:8:db:2
....
```

Angreifer muss für jeden *DHCP Packet Exchange* eine andere MAC-Adresse verwenden

MAC-Angriffe

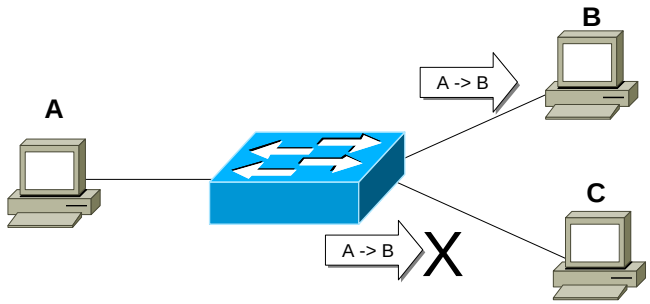
MAC Flooding

MAC Spoofing

Port Security

IEEE 802.1X Port Authentication

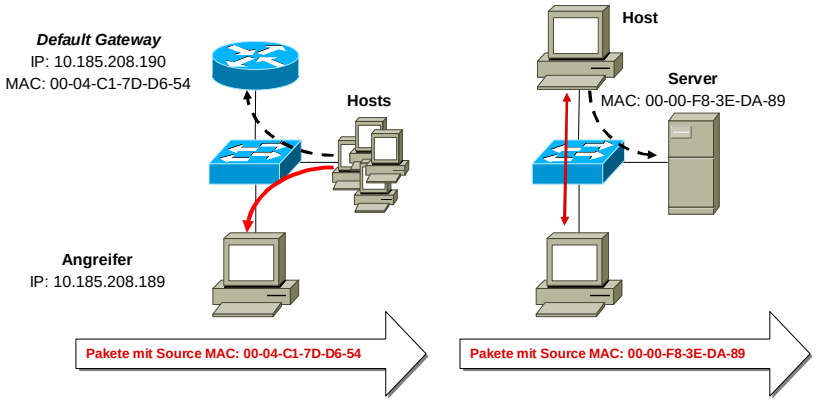
MAC Flooding



- MAC-Adresse eines Pakets ist in **MAC-Adress-Tabelle** vorhanden
  - Frame wird nur an entsprechenden Port weitergeleitet
- MAC-Adresse ist nicht in der MAC-Adress-Tabelle vorhanden
  - **Frame wird über alle Ports geflutet (auch über Trunk Ports)**
- Ziel eines Angreifers: Tabelle auf dem Switch zum Überlauf bringen
  - „**macof**“: generiert bis zu 155.000 unterschiedliche MAC-Adresse pro Minute

MAC Spoofing

- Angreifer verwendet die MAC-Adresse eines bekannten Rechers um alle Pakete zu diesem Hosts zu seinem System unzulenken.
- Keine Weiterleitung der Daten an das eigentliche Zielsystem möglich
  - Übernahme der Serverfunktionalität (z.B. HTTP) oder DoS-Angriff



Schutzmechanismen – Port Security

- **Konfiguration**
  set port security *mod/port* enable
  [set port security *mod/port* unicast-flood disable]
  set port security *mod/port* maximum 1
  set port security *mod/port* **violation** restrict | shutdown
- **Violation Shutdown** (Standardverhalten)
  - Bei Verletzung der Port Security wird Port auf „shutdown“ gesetzt
    - set port security *mod/port* shutdown *time* legt Zeitdauer fest
- **Violation Restrict**
  - Bei Verletzung der Port Security werden Pakete von „unsicheren“ Hosts verworfen, Port bleibt aber oben
- **Verletzung der Sicherheit eines Ports**
  - Mehr MAC-Adressen an einem Port als erlaubt
  - Source-Adresse ist bereits Secure MAC-Adresse eines anderen Port
    - Port geht auch bei „violation restrict“ in Shutdown

Schutzmechanismen – Port Security

- Dynamisch gelernte *Secure-MAC-Adressen* werden als statische MAC-Adressen in CAM Tabelle eingetragen
  - Switch übernimmt Adressen automatisch in seine Konfiguration:

CatOS> (enable) show port security 3/15

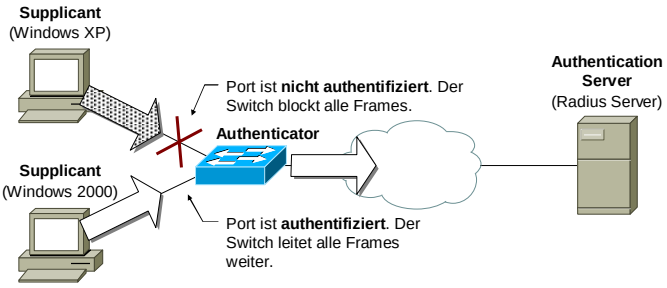
```
* = Configured MAC Address
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
 3/15  enabled  shutdown             0        0        1 disabled      24
Port  Num-Addr Secure-Src-Addr     Age-Left Last-Src-Addr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

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
10    00-30-69-b7-b6-de  X          3/13
Total Matching CAM Entries Displayed  =2
```

IEEE 802.1X Port Authentication

- Client-Server-Protokoll zur direkten Übertragung von Authentifizierungs-informationen über Layer 2
- Clients, die sich mit einem LAN verbinden wollen, müssen sich zuerst authentisieren
  - Die Übertragung der EAP-Daten zwischen *Supplicant* (Client) und *Authenticator* erfolgt mittels **EAPOL** (Ethernet-Protokoll 0x88-8E)
  - Der Authenticator leitet die EAP-Daten dann über RADIUS an den *Authentication Server* weiter



IEEE 802.1X Port Authentication

- IEEE 802.1X Konfiguration auf dem Switch

```
set radius server 192.168.1.185 auth-port 1812 primary
set radius server 192.168.1.210 auth-port 1645
set radius key ABC
#
set dot1x system-auth-control enable
set dot1x guest-vlan 999
set port dot1x 3/37-3/48  port-control auto
```

Console> (enable) show dot1x

```
PAE Capability           Authenticator Only
Protocol Version         1
system-auth-control      enabled
max-req                  2
quiet-period             60 seconds
re-authperiod            3600 seconds
server-timeout           30 seconds
supp-timeout             30 seconds
tx-period                30 seconds
guest-vlan               999
```

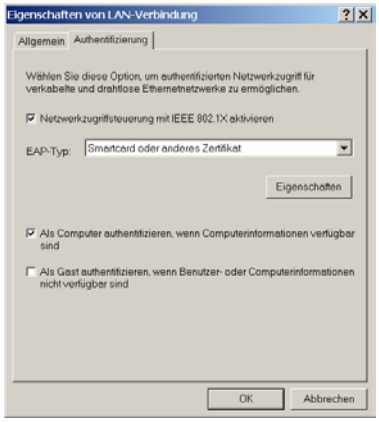
Console> (enable) show port dot1x 3/37

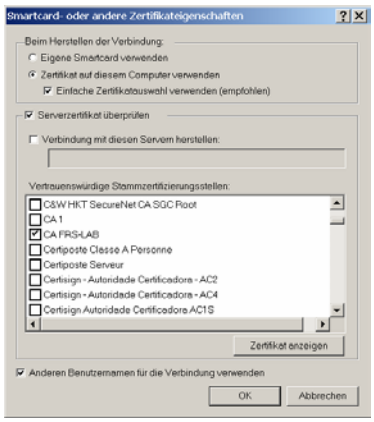
```
Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- ------------
 3/37 authenticated       idle       auto                authorized

Port  Port-Mode     Re-authentication
----- ------------ -----------------
 3/37 SingleAuth     enabled
```

IEEE 802.1X Port Authentication

- IEEE 802.1X Konfiguration unter Windows 2000
  - Authentifizierung über EAP-MD5, EAP-TLS oder EAP-PEAP
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=6b78edbe-d3ca-4880-929f-453c695b9637&DisplayLang=en





ARP Spoofing

ARP Cache Poisoning

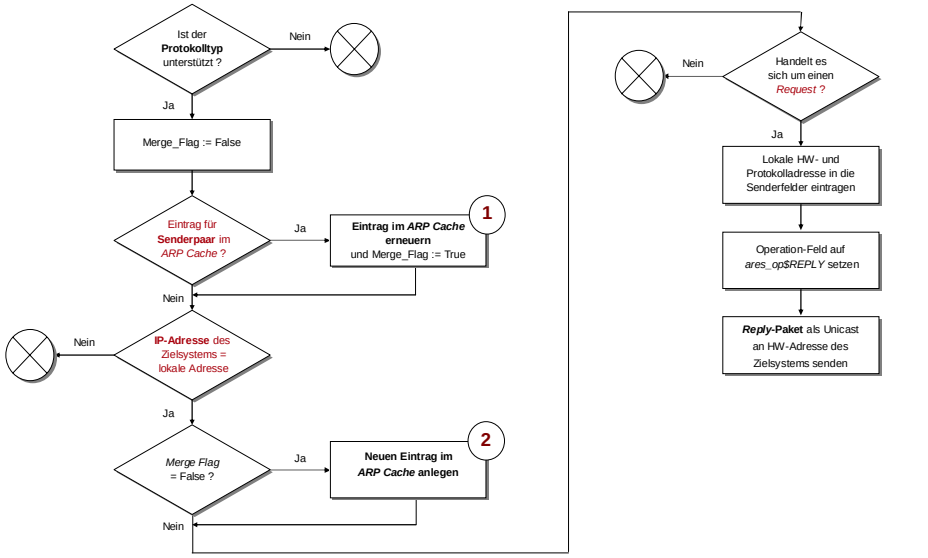
Private VLANs

VLAN ACLs

Sticky ARP

ARP Inspection

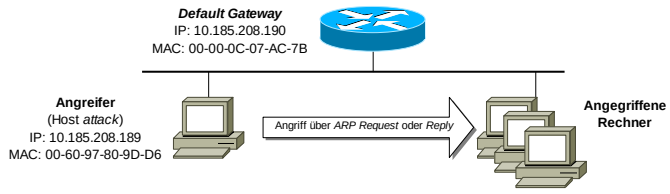
Wie funktioniert der ARP Cache überhaupt ?



Wann wird der ARP Cache verändert ?

- Empfänger ändert **bestehenden Eintrag** im *ARP Cache* immer ab **(1)**
  - Ziel-IP-Adresse im ARP-Paket muss nicht mit der lokalen Adresse übereinstimmen
- Empfänger erzeugt **neuen Eintrag** im *ARP Cache* nur, falls die Ziel-IP-Adresse des ARP-Pakets mit der lokalen Adresse übereinstimmt **(2)**
- Durch „gefälschte“ ARP-Pakete können bestehende Einträge im ARP Cache modifiziert und neue Einträge hinzufügt werden
  - ***ARP Spoofing*** oder ***ARP Cache Poisoning***.
  - Ermöglicht Denial-of-Service- und Man-in-the-Middle-Attacken
- ***Gratuitous ARP***
  - Modifikation des *ARP Cache* durch einen *ARP Reply*
    - Als Broadcast gesendet, wird bestehender Eintrag auf allen Systemen geändert
      - attack# arpspoof 10.185.208.190
    - Häufig benutzt, um ARP-Eintrag des Default Gateway auf Hosts zu modifizieren

ARP Spoofing in Aktion



attack# arpspoof 10.185.208.190

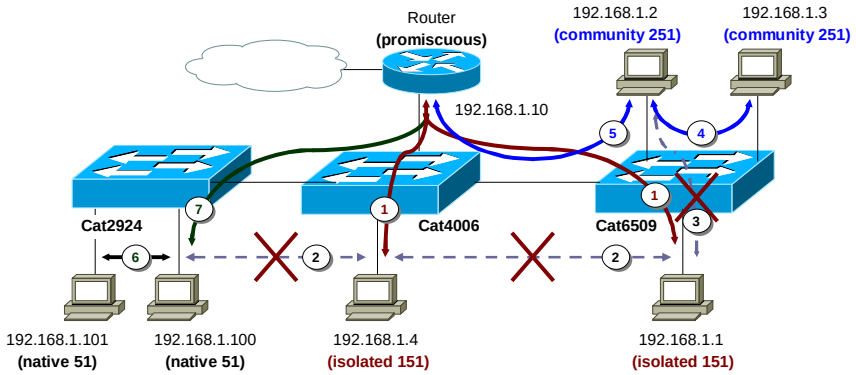
Ethernet II, Src: 00:60:97:80:9d:d6, Dst: ff:ff:ff:ff:ff:ff
Destination: ff:ff:ff:ff:ff:ff
Source: 00:60:97:80:9d:d6
Type: ARP (0x0806)
Trailer: 0000EFFDEF3CC4121700000200000000...
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: 00:60:97:80:9d:d6
Sender IP address: 10.185.208.190
Target MAC address: ff:ff:ff:ff:ff:ff
Target IP address: 0.0.0.0

D:\> arp -a

Schnittstelle: 10.185.211.208 on Interface 0x1000003

Internetadresse	Physikal. Adresse	Typ
10.185.208.190	**00-60-97-80-9d-d6**	dynamisch

Private VLANs



- **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 Private VLANs unterstützen, können nur untereinander **(6)** und mit dem Promiscuous Port kommunizieren **(7)**.

Private VLAN Konfiguration

- Catalyst 6000, 4000, 2980G, 2948G und 4912G
  - **VTP ausschalten**

    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**

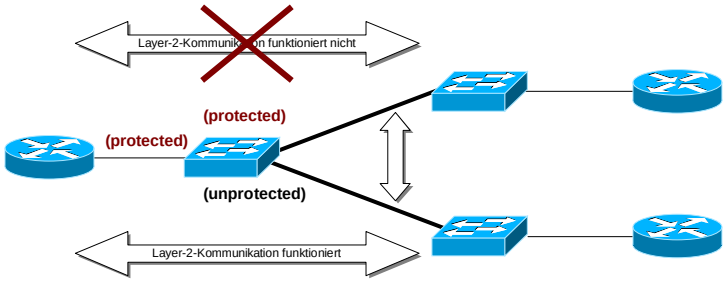
    CatOS> (enable) **set pvlan 51 251 3/29,3/42**
  - **Promiscuous Ports definieren**

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

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

Protected Ports

- Abgeschwächtes“ *Private VLAN*
  - Gelten nur für lokalen Switch und verhindern direkte Layer-2-Kommunikation zwischen geschützten Ports
  - Catalyst Switches 2950, 3550, 2900XL/3500XL mit Native IOS



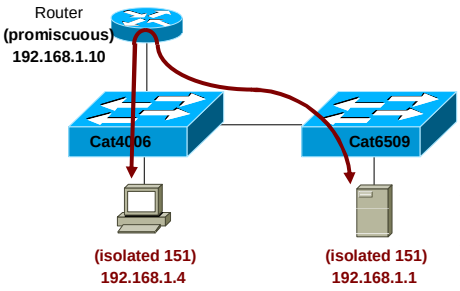
- Konfiguration

  interface *name*

  switchport protected

Problem bei Private VLANs: Host Routen

- Hostrouten an Isolated oder Community Ports möglich, die auf Router am Promiscuous Port zeigen
  - Host sendet Daten zuerst an Router, der leitet Pakete dann an das Zielsystem weiter



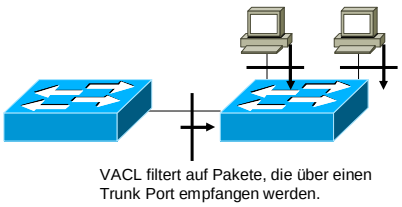
route add –host 192.168.1.1 gw 192.168.1.10

route add –host 192.168.1.4 gw 192.168.1.10

- **Lösung: VLAN ACLs**

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

VLAN ACL

- Intrasubnetz-Routing über Promiscuous Port ausschalten

  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

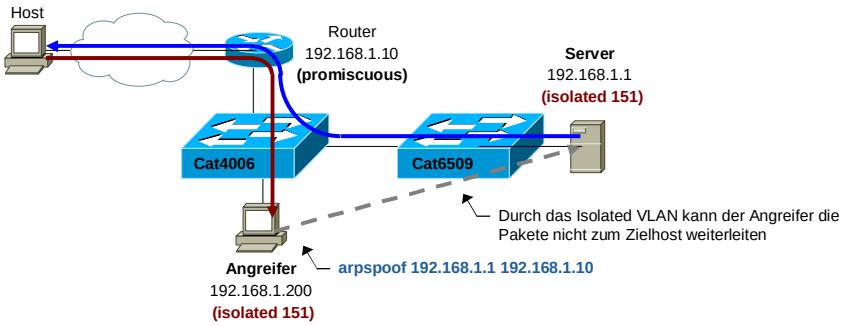
    set security acl ip *IsolatedPVLAN151* deny ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
    set security acl ip *IsolatedPVLAN151* permit tcp host 192.168.1.1 eq 80 any
    set security acl ip *IsolatedPVLAN151* permit tcp host 192.168.1.1 eq 23 any

- VACLs aktivieren

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

Problem bei Private VLANs: ARP Spoofing

- Private-VLAN-Schutzmechanismen erlauben weiterhin ARP Spoofing auf Systemen am Promiscuous Port
  - Angreifer kann Pakete nicht mehr an das Zielsystem weiterleiten
  - Daher „lediglich“DoS-Attacke möglich



- Lösung: Statische MAC-Einträge auf Router, **Sticky ARP** (nur MSFC), **ARP Inspection** (6500+SUP2+PFC2), DHCP Secured Address Assignment

Sticky ARP

- MSFC (Router-Karte im Switch) überschreibt keine ARP-Einträge von Hosts aus einem *Private VLAN*
- Angreifer kann den ARP Cache auf der MSFC nicht mehr verändern und ARP-Spoofing-Angriffe sind wirkungslos.

```
c6509msfc# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.11           -   00d0.d33a.40d4  ARPA   Vlan51
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
```

Sticky ARP Eintrag

```
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
```


ARP Inspection

- ARP-Pakete werden von Switch-CPU überprüft (ab CatOS V7.5)
  - ARP Binding (MAC und IP-Adresse im ARP Paket)
  - Gleiche MAC-Adresse im Ethernet-Header und im ARP-Paket
  - ARP Paket mit ungültigen MAC- und IP-Adressen
- ARP Binding
  - 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 any any** [log]
  - set security acl ip *name* permit/deny **arp-inspection *ip-addr mask* any** [log]
- Gleiche MAC-Adresse im Ethernet-Header und im ARP-Paket
  - Paket verwerfen
    - set security acl **arp-inspection match-mac enable drop** [log]
  - Nur Log-Meldung generieren
    - set security acl **arp-inspection match-mac enable**

ARP Inspection

- ARP-Paket mit ungültigen MAC- oder IP-Adressen
  - 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 Gratiuous ARP
  - Paket verwerfen
    - set security acl **arp-inspection address-violation enable drop** [log]
  - 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 als DHCP-Server konfiguriert werden

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

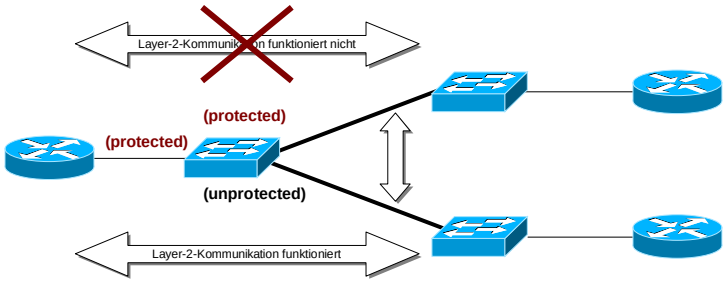
show ip dhcp server statistics

```
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.

Protected Ports

- Abgeschwächtes“ *Private VLAN*
  - Gelten nur für lokalen Switch und verhindern direkte Layer-2-Kommunikation zwischen geschützten Ports
  - Catalyst Switches 2950, 3550, 2900XL/3500XL mit Native IOS



- Konfiguration

interface *name*
switchport protected

Weitere Angriffe

VLAN Hopping

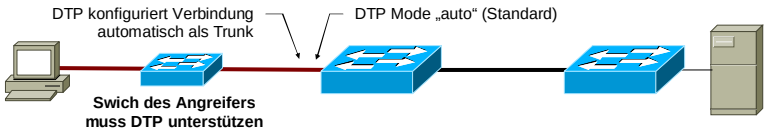
Spanning Tree Attacken

VLAN Hopping – Switch Spoofing

- Standardmäßig stehen alle Switchports auf ***Trunk Mode*** „auto“

```
Console> (enable) show trunk 3/3
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/3      auto         negotiate      not-trunking  1
```

- Falls Angreifer **DTP (*Dynamic Trunking Protocol*)** unterstützt, ist Trunk-Verbindung (IEEE 802.1Q) zum Switch möglich
  - Zugriff auf alle VLANs



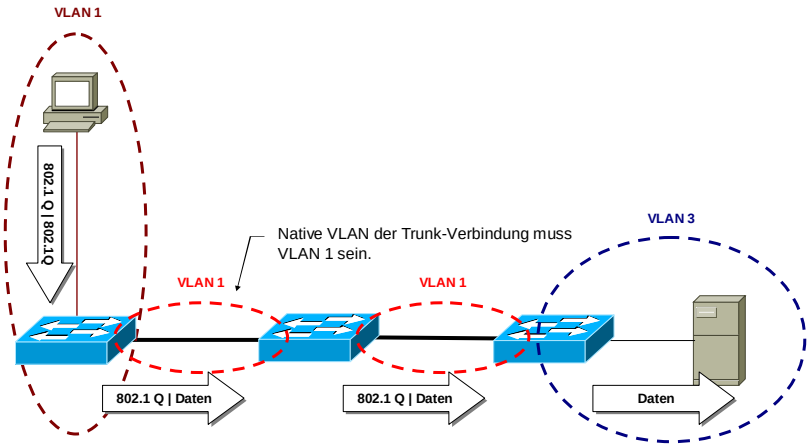
- Lösung: Trunking ausschalten

  CatOS> (enable) **set trunk *mod/port* off** oder Catos> (enable) **set trunk all off**

  IOS(config-if)# **switchport mode access**

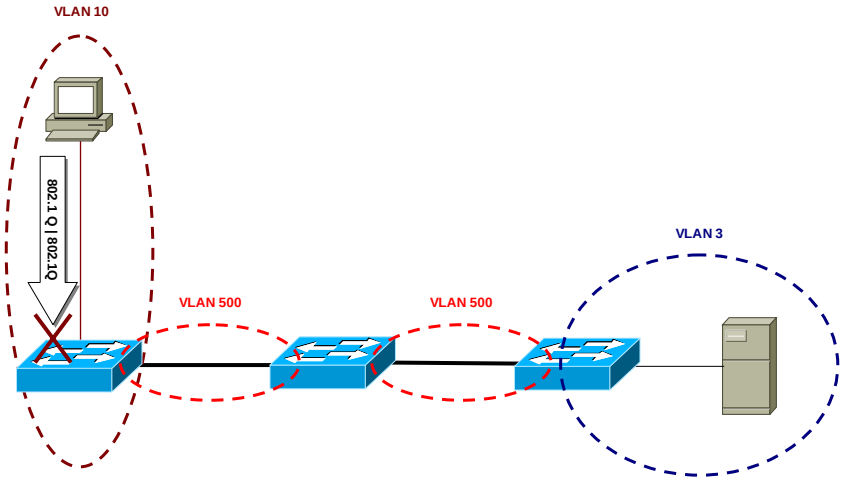
VLAN Hopping – Double Tagging

- Angreifer sendet Frame mit zwei IEEE 802.1Q VLAN Header
  - Native VLAN der Trunks und Access VLANs müssen identisch sind



VLAN Hopping – Double Tagging

- Lösung: Verschiedene VLANs für Trunk und Access Ports



VLAN Hopping – Best Practice

- **Niemals VLAN 1 verwenden** (gilt für Trunk und Access Ports)
- **Trunk-Verbindungen immer in eigenes Native VLAN**
- Unbenutzte Ports ausschalten und in unbenutztes VLAN legen
- DTP auf Access Ports ausschalten

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**

Cisco Integrated IOS

- Trunk Ports

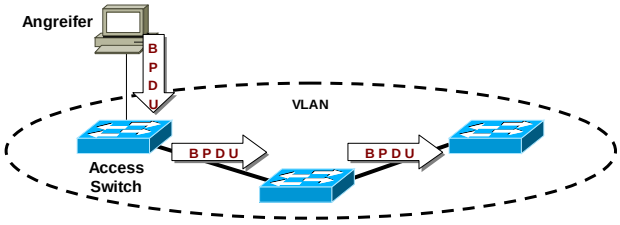
  interface *name*
  switchport trunk native vlan 500
  switchport mode trunk

- Access Ports

  interface *name*
  switchport access vlan 10
  switchport mode access

Spanning Tree Attacken

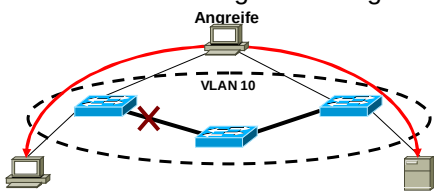
- DoS-Angriff durch Spanning-Tree-Attacke
  - Angreifer sendet *Spanning Tree Bridge PDUs* die dazu führen, dass der Spanning-Tree neu berechnet werden muss



  - Angreifer benötigt Zugang zu einem Switch
- Lösung: **Root Guard**
  - Switch schaltet Port ab, wenn er BPDUs empfängt, die eine *STP Root Bridge Recalculation* zur Folge haben

Spanning Tree Attacken

- Spanning Tree Topologie verändern
  - Falls Angreifer Verbindung zu mehreren Switches hat (mindestens zwei), kann er sich als *Root Bridge* in das Netzwerk einbinden
  - Durch *Spanning Tree Recalculation* werden die Wege evtl. so geändert, dass alle Pakete über den angreifenden Rechner gehen
  - Anschließend können alle Verbindungen überwacht und entsprechende MitM- oder DoS-Angriffe durchgeführt werden



- Lösung: **BPDU Guard** (nur mit PortFast Ports möglich)
  - Switch setzt **PortFast**-Schnittstelle auf „*down*“, sobald er über diesen Port ein BPDU-Paket empfängt.

Spanning Tree Attacken – Best Practice

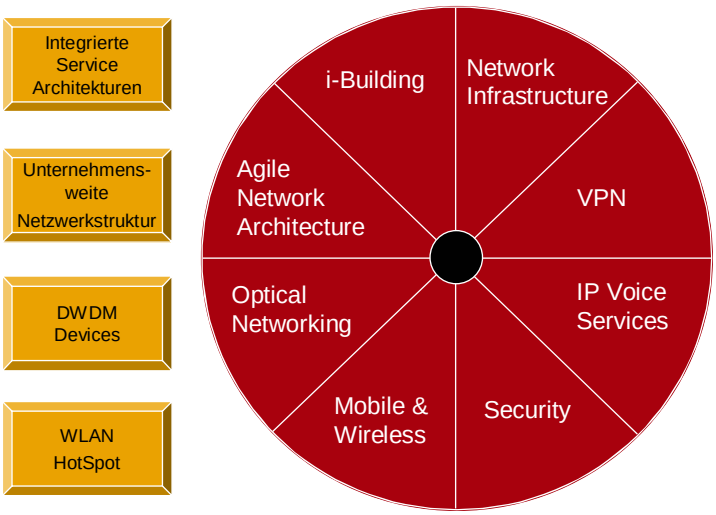
- Normale Access Ports:
  - Catalyst OS
    set spantree portfast bpdu-guard enable
    set spantree portfast *mod/port* enable
  - IOS
    spanning-tree portfast **bpduguard**
    interface *name*
      spanning-tree portfast
- Trunk Ports zu Switches, die keine Root Bridge werden dürfen:
  - Calatyst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

Zusammenfassung

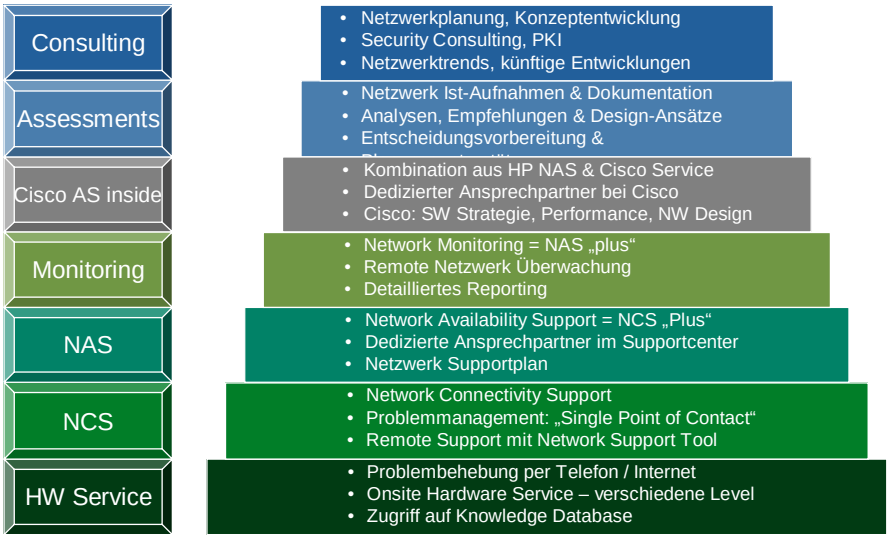
VLANs bieten KEINE erhöhte Sicherheit !

Weitere Sicherheitseinstellungen sind notwendig !

NSG Fokusthemen



Überblick HP Netzwerk Services



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
- Secure Use of VLANs: An @stake Security Assessment
  - http://www.packetfactory.net/papers/VLAN-hopping/stake_wp.pdf
- Hacking Layer 2: Fun with Ethernet Switches
  - http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf