Academy-Day-2016

FH Bielefeld

Demo-Lab-Vorschlag zu CCNA 6: Layer 2 Sicherheit

Agenda:

- Kurzer Überblick neuer CCNA-6 Inhalte
- Layer 2 Switche und Sicherheit
- L2- Sicherheitsmechanismen allgemein
- Einfache DHCP-Attacken
- "Yersinia Framework" für Cisco-Attackierungen
- DHCP-Snooping und Konfiguration

Kurzer Überbilick neuer CCNA-6 Inhalte

ICND-1 / CCENT	**Intro to Networks**	**R&S Essentials**
	• Extended Traceroute	• Host-Routes
	• Debugging	• Devices Discovery, NTP
	• Troubleshooting	• Password Recovery
ICND-2 / CCNA	**Scaling Networks**	**Connecting Networks**
	VTP, Extended VLAN, DTP	WAN-Topol., PPPoE, eBGP,
	Troubleshooting Multi VLAN, Switch Stacking, HSRP	DMVPN, IPv6 ACL, QoS, LAN-Sec, SDN
	Troubleshooting Multi. OSPF	SNMPv3, SPAN, Cloud, Using IP SLA, Networkpro.

• Kurzer Überbilick neuer CCNA-6 Inhalte

4.6: LAN Security

4.6.1: LAN Security Best Practices

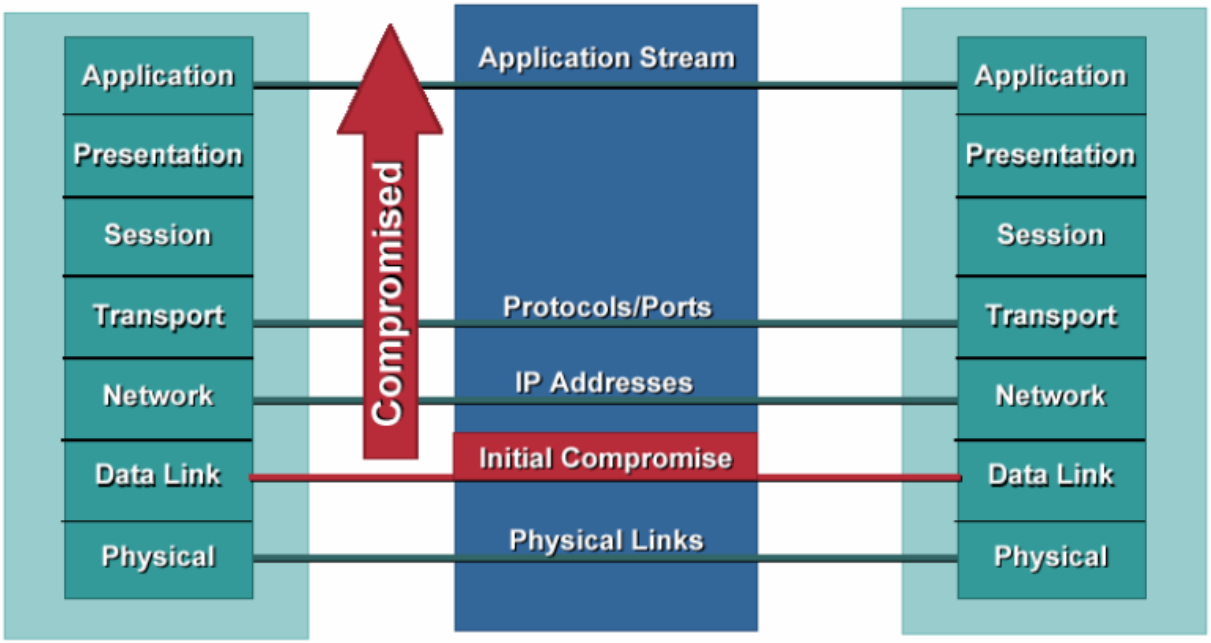
- 4.6.1.1: DHCP Snooping
- 4.6.1.2: AAA with RADIUS and TACACS+
- 4.6.1.3: 802.1X
- 4.6.1.4: Activity - Identify the Security Best Practice

Layer 2 Switche und Sicherheit

The Domino Effect

Cisco.com

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as your weakest link
- When it comes to networking, layer 2 can be a VERY weak link



l2-security-bh.ppt

© 2002, Cisco Systems, Inc. All rights reserved.

Natürlich sind alle Layer betroffen!

Layer 2 Switche und Sicherheit

- Layer 2- und Layer 3- Switche sind ebenfalls, wie Router attackierbar mit den selben / ähnlichen Angriffen
- Jedoch haben sie ihre eigenen “Attack-Techniken”:

  - **Sniffing**
  - **MAC address spoofing, Table-overflow**
  - **DTP-Attacken**
  - **Spanning Tree Protocol Manipulation**
  - **LAN-Storms**
  - **VLAN-Hopping……und DHCP-Attacken**

Layer 2 Switche und Sicherheit

Allgemeine Best Practices für VLAN's und Trunking!

- Benutze immer eine eigene VLAN-ID für Trunk's!
- Schalte ungenutzte Ports aus, setze sie in ein ungenutztes VLAN!
- "Sei paranoid": benutze nicht VLAN 1 für irgendwas!
- Schalte "Auto-Trunking" an "User-Ports" aus (DTP off)!
- Konfiguriere ausdrücklich Trunks an Infrastruktur-Ports!
- Benutze PC Voice VLAN Access bei Telefonen, die es können!

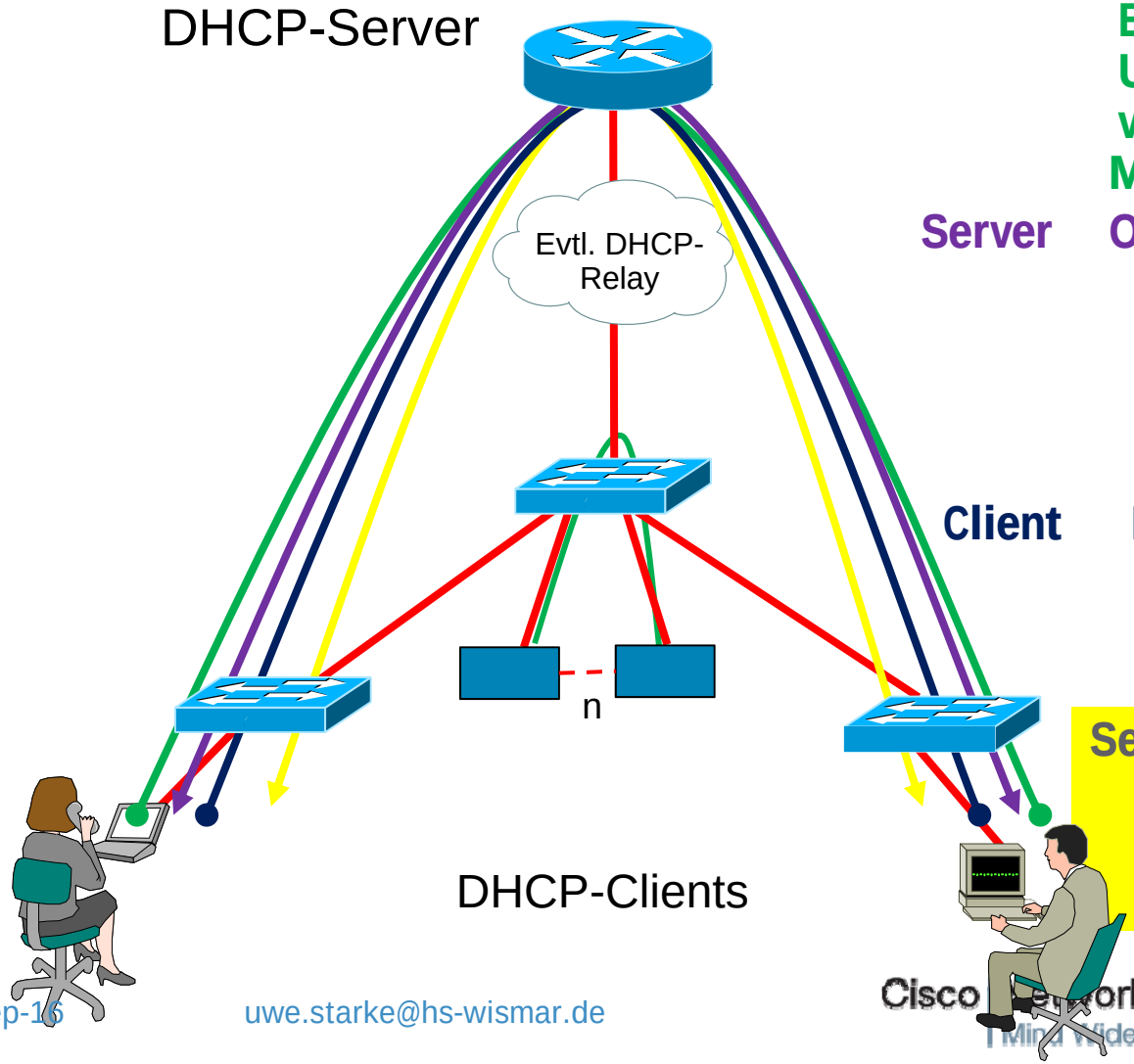
Einfache DHCP-Attacken

Welche Attack-Varianten kennt ihr?

DHCP- Starvation (arbeitet mit andern Attacken zusammen)

Faked-Spoofed DHCP-Server (Voraussetzung für spätere Attacken)

Normale DHCP-Arbeitsweise



Client DHCP- Discover
Broadcast im L2 und L3;
UDP-SrcPort 68 zu Dst-Port 67
verschieden Opt. Im Bootp z.B.
MAC, Mess.Typ, Hostname

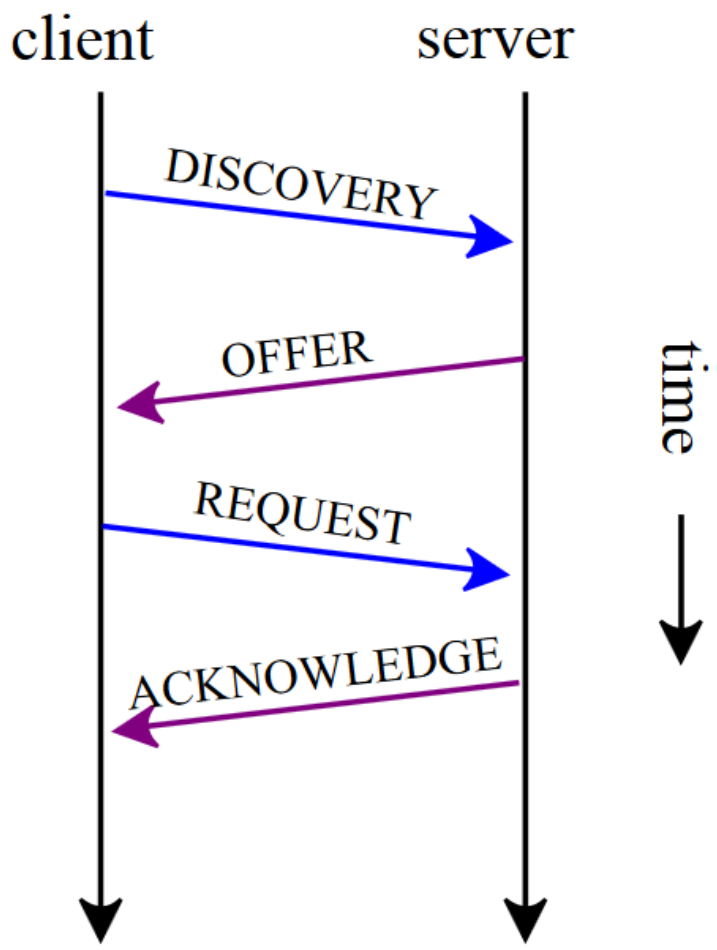
Server Offer
L2/3 Broadcast vom
Server UDP von 67 an
68, offer eines IP-
Konfigvorschlags

Client Request
L2/3 Broadcast, UDP 68/67
Request der offerd IP-Konfig.

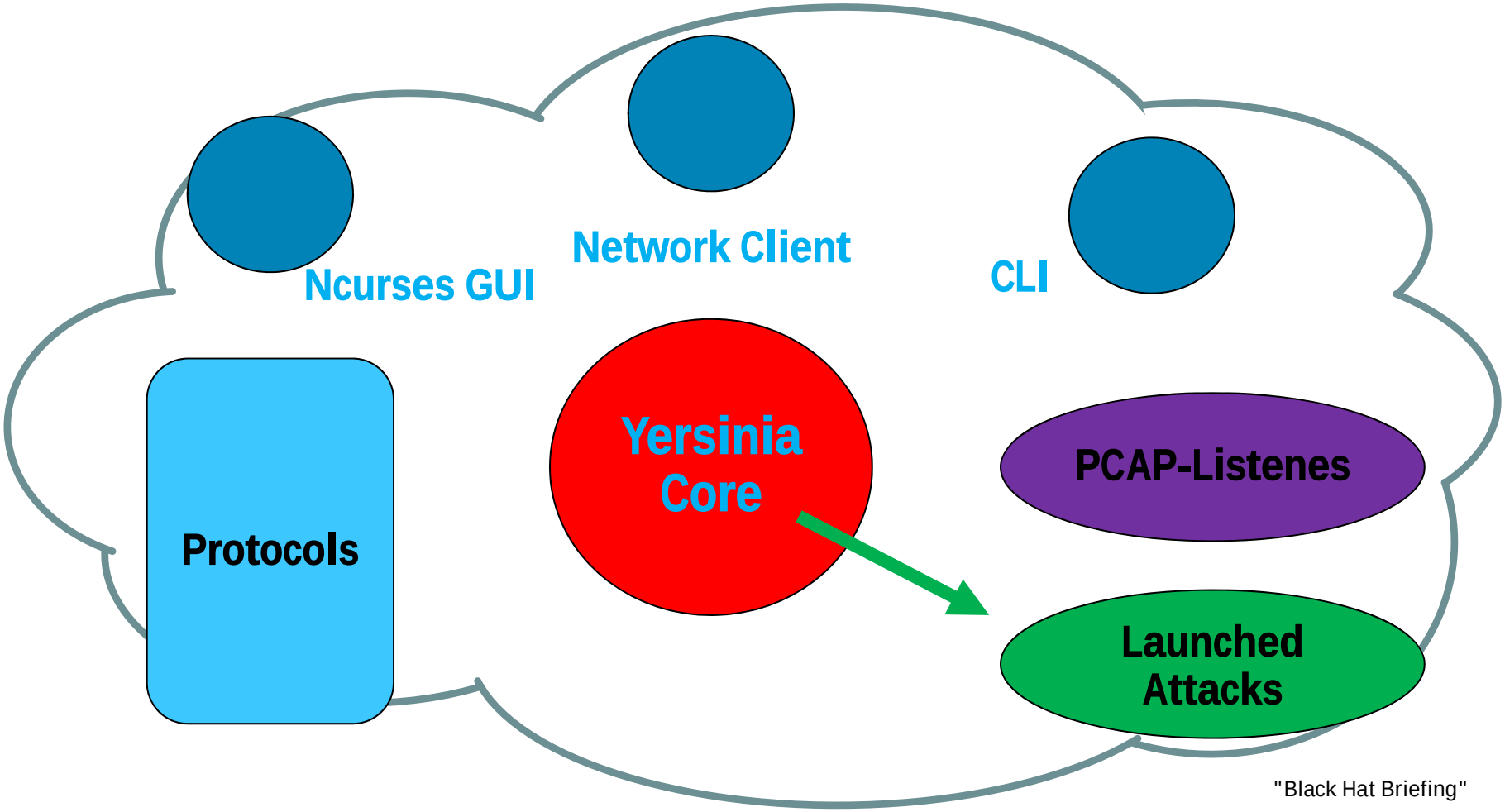
Server DHCP-ACK
L2/3 Broadcast
UDP 67/68, ACK für
IP-Konfig

Normale DHCP-Arbeitsweise

- Flow kurz



Yersinia Framework für Layer 2 attack! Short intro.



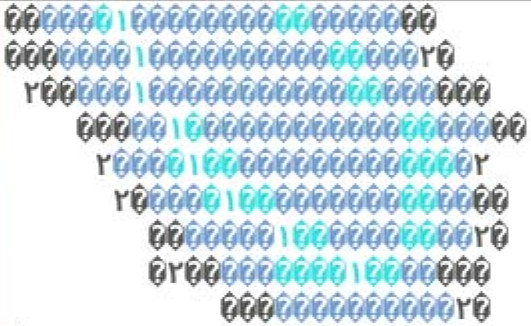
"Black Hat Briefing"

Yersinia Framework für Layer 2 attack!

Short intro

- Layer 2 Attacks
  - ARP Poisoning
  - CAM Flooding and more
- Multithreaded: multiple user, multiple attacken
  - Analyze and watch your packets
  - Edit each protocol‘s field
  - Learn the packets and replay them with modifications
  - Capture network data in wireshark-format (pcap)
- Support for protocols
  - STP, CDP, DTP, DHCP, HSRP, 802.1Q, VTP

Yersinia Framework für Layer 2 attack! Short intro.



```
by Slay & tomac

http://www.yersinia.net
 yersinia@yersinia.net


Prune your MSTP, RSTP, STP trees!!!!

Usage: yersinia [-hVGIDd] [-l logfile] [-c conffile] protocol [protocol_options]
       -V   Program version.
       -h   This help screen.
       -G   Graphical mode (GTK).
       -I   Interactive mode (ncurses).
       -D   Daemon mode.
       -d   Debug.
       -l logfile   Select logfile.
       -c conffile  Select config file.
  protocol   One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@yersinia.net>
```

Yersinia Framework für Layer 2 attack!
Short intro. /cont

```
root@uwe-nix: ~
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
root@uwe-nix:~# yersinia -I

 yersinia 0.7.3 by Slay & tomac - STP mode                                [13:43:43]
                RootId          BridgeId        Port            Iface Last seen

                  Notification window
                  Warning: interface eth0 selected as the default one

                  Press any key to continue

          Total Packets: 0          STP Packets: 0          MAC Spoofing [X]
 You've got a message
 STP Fields
          Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
          Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
          BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

Yersinia Framework für Layer 2 attack! Short intro. /cont

```
Available commands
h       Help screen
x       eXecute attack
i       edit Interfaces
ENTER   information about selected item
v       View hex packet dump
d       load protocol Default values
e       Edit packet fields
f       list capture Files
s       Save packets from protocol
S       Save packets from all protocols
L       Learn packet from network
M       set Mac spoofing on/off
l       List running attacks
K       Kill all running attacks
c       Clear current protocol stats
C       Clear all protocols stats
g       Go to other protocol screen
Ctrl-L  redraw screen
w       Write configuration file
a       About this proggie
q       Quit (bring da noize)
```

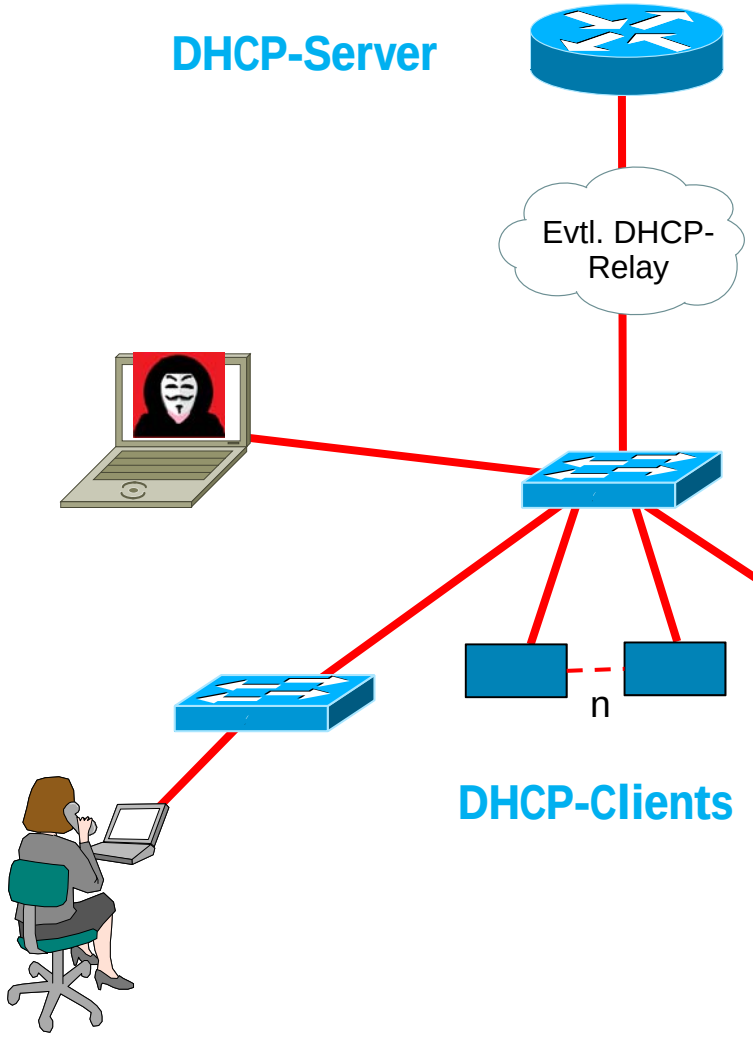
Yersinia Framework für Layer 2 attack!
Short intro. /cont

```
Choose protocol mode
CDP     Cisco Discovery Protocol
DHCP    Dynamic Host Configuration Protocol
802.1Q  IEEE 802.1Q
802.1X  IEEE 802.1X
DTP     Dynamic Trunking Protocol
HSRP    Hot Standby Router Protocol
ISL     Inter-Switch Link Protocol
MPLS    MultiProtocol Label Switching
STP     Spanning Tree Protocol
VTP     VLAN Trunking Protocol

ENTER to select  -  ESC/Q to quit
```

DHCP Attack- Topologie

Starvation Attack (*Angriff durch Aushungern)*



 # yersinia –I -> g – für Protocols

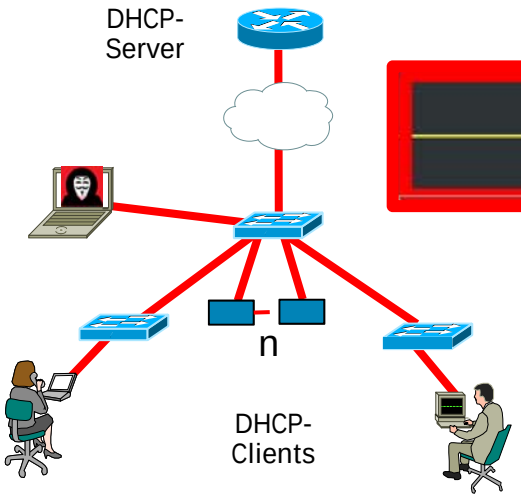
```
Choose protocol mode
CDP    Cisco Discovery Protocol
DHCP   Dynamic Host Configuration Protocol
802.1Q IEEE 802.1Q
```

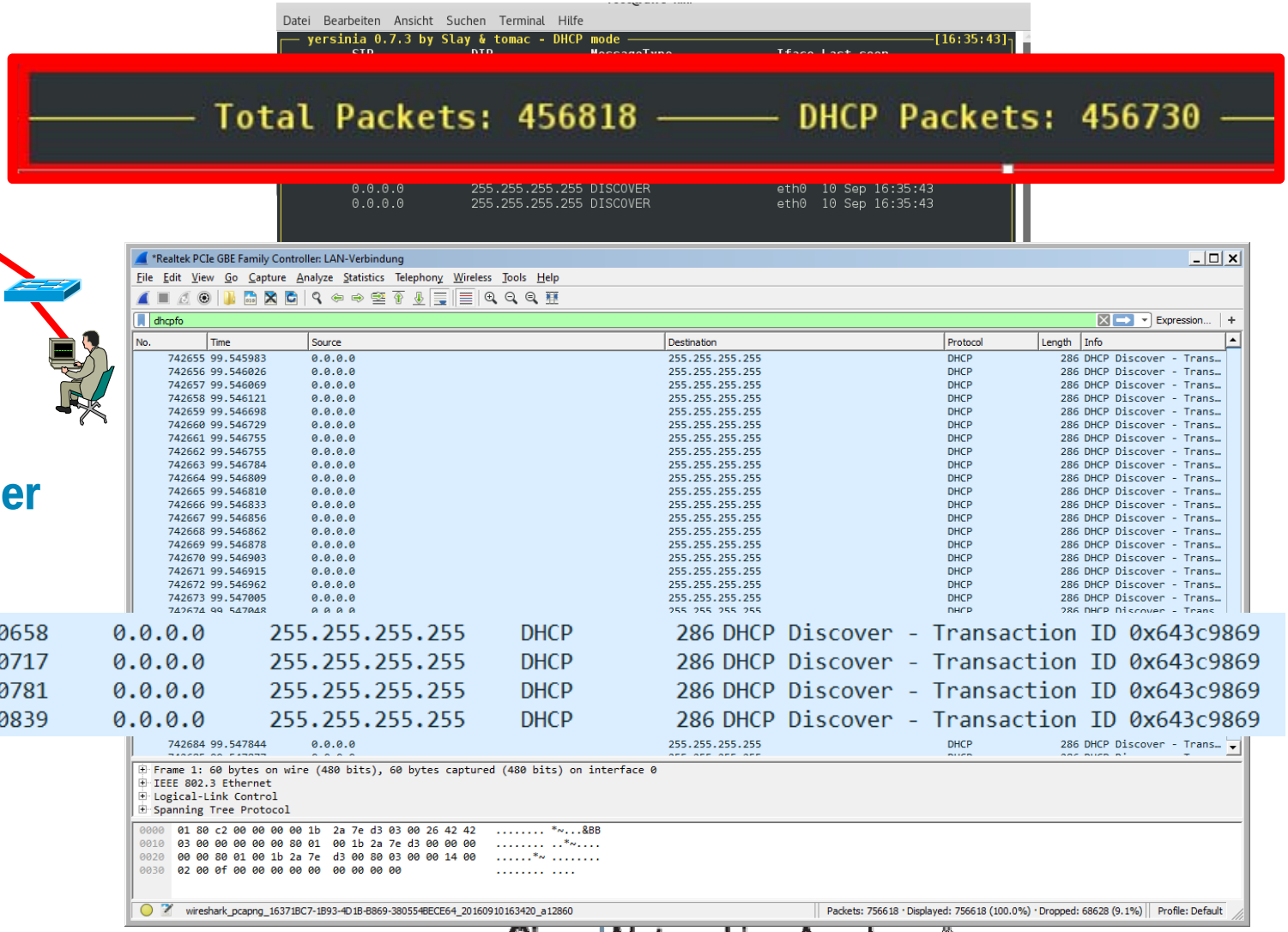
dann ein "x"

```
Attack Panel
No  DoS  Description
0        sending RAW packet
1   X    sending DISCOVER packet
2        creating DHCP rogue server
3   X    sending RELEASE packet
```

Welche Option ?

DHCP Attack "Starvation Attack"

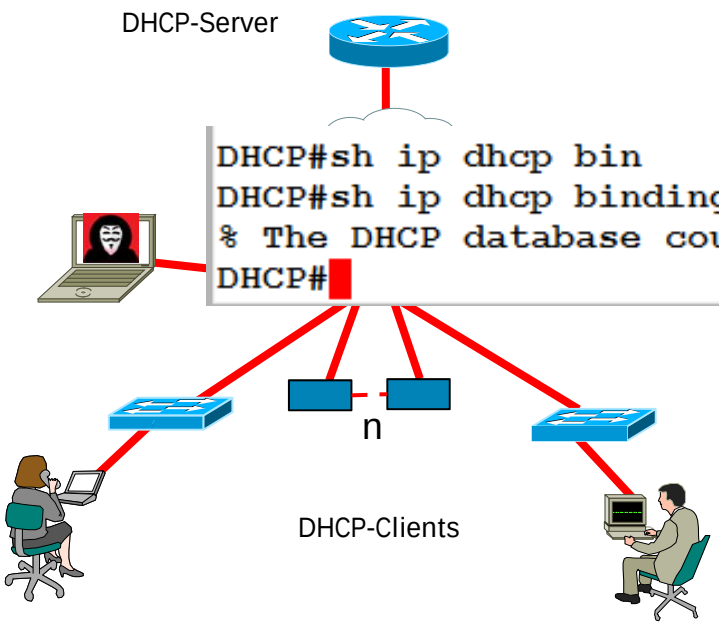




Nach Auswahl der Option 1!

702357	97.430658	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
702358	97.430717	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
702359	97.430781	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
702360	97.430839	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

DHCP Attack "Starvation Attack"




```
DHCP#sh ip dhcp bin
DHCP#sh ip dhcp binding
% The DHCP database could not be locked. Please retry the command later.
DHCP#
```

COM3 - PuTTY

10.0.0.14	7efb.4d52.d147	Jan 01 1970 12:51 AM	Automatic
10.0.0.15	c8d2.d62c.eb04	Jan 01 1970 12:51 AM	Automatic
10.0.0.16	66bc.5469.6e2d	Jan 01 1970 12:52 AM	Automatic
10.0.0.17	92f4.672f.9ee2	Jan 01 1970 12:52 AM	Automatic
10.0.0.18	986b.810f.9f40	Jan 01 1970 12:52 AM	Automatic
10.0.0.19	96e5.1842.cc8c	Jan 01 1970 12:52 AM	Automatic
10.0.0.20	7ae6.7704.574a	Jan 01 1970 12:52 AM	Automatic
10.0.0.21	ceb3.790f.3114	Jan 01 1970 12:52 AM	Automatic
10.0.0.22	2cc5.b638.b360	Jan 01 1970 12:52 AM	Automatic
10.0.0.23	06b1.941f.404e	Jan 01 1970 12:52 AM	Automatic
10.0.0.24	aee0.7f0c.8a3a	Jan 01 1970 12:52 AM	Automatic
10.0.0.25	5480.6846.ab2c	Jan 01 1970 12:52 AM	Automatic
10.0.0.26	bc9f.af65.2735	Jan 01 1970 12:52 AM	Automatic
10.0.0.27	b4e3.662e.a13a	Jan 01 1970 12:52 AM	Automatic
10.0.0.28	b8c5.6b74.cb39	Jan 01 1970 12:52 AM	Automatic
10.0.0.29	262c.471b.1625	Jan 01 1970 12:52 AM	Automatic
10.0.0.30	f2a2.9c4e.69c7	Jan 01 1970 12:52 AM	Automatic
10.0.0.31	d637.441e.726f	Jan 01 1970 12:52 AM	Automatic
10.0.0.32	96e7.8740.3b96	Jan 01 1970 12:52 AM	Automatic
10.0.0.33	ca28.5812.a250	Jan 01 1970 12:52 AM	Automatic
10.0.0.34	ee03.5942.916c	Jan 01 1970 12:52 AM	Automatic
10.0.0.35	c2f7.c02c.8210	Jan 01 1970 12:52 AM	Automatic
10.0.0.36	86fe.4928.eea9	Jan 01 1970 12:52 AM	Automatic
10.0.0.37	4663.4901.cdff	Jan 01 1970 12:52 AM	Automatic

Welches Kommando im Router? (Anzeige DHCP – Tabelle)

Router#sh ip dhcp bindings

Der gesamte Adressbereich sollte ausgeschöpft sein!

DHCP Attack "Starvation Attack"

- Vielzahl von gefälschten MAC-Adressen fordern vom Server IP-Adressen an -> bis Vorrat verbraucht ist -> berechtigte User erhalten keine IP
- Angriff ist begrenzt auf die Broadcast-Domäne
- Freigabe der Lease-Adressen nach Servereingriff
- Angriff nur aus lokalen LAN, es sei denn man nutzt VLAN-Hopping?
- Möglichkeit des Einsatzes eines Rogue-DHCP-Servers -> „Man in the Middle“, Sniffing....

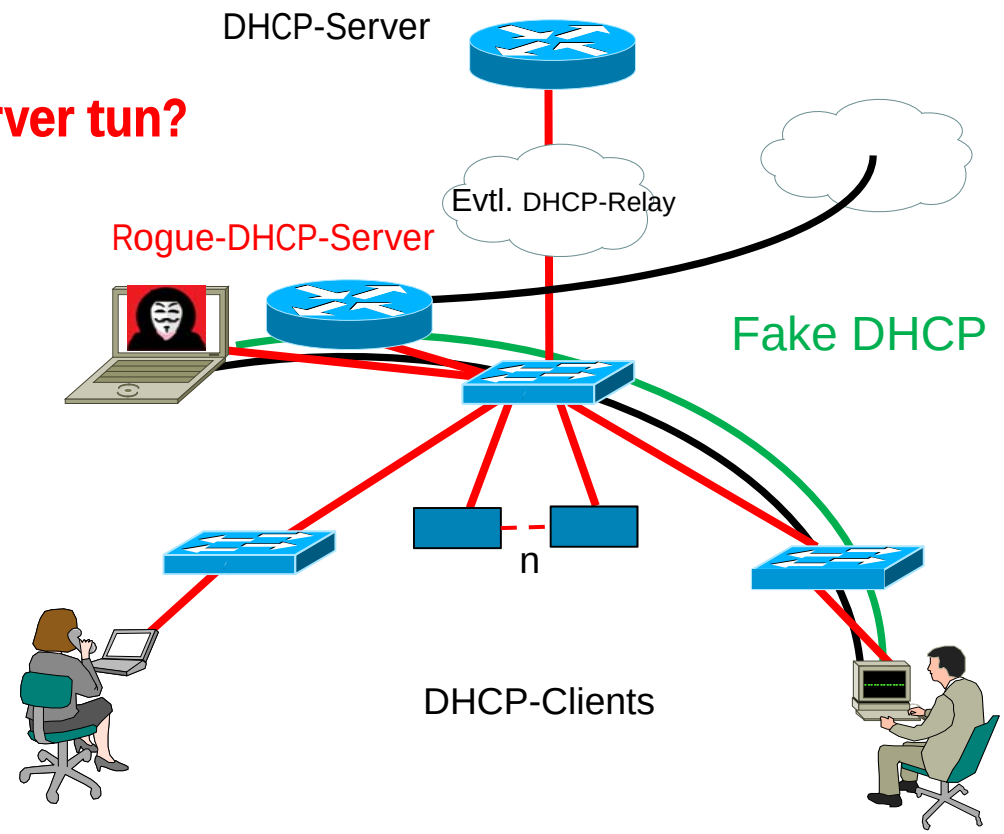
Verhinderung!

Port-Security und / oder DHCP-Snooping

DHCP Attack "Rogue DHCP-Server"

Was kann nun der falsche DHCP-Server tun?

1. **Falsches Default-Gateway, Attacker ist das Gateway!**
2. **Falscher DNS-Server!**
3. **Falsche IP-Adresse!**



Angriff ist begrenzt auf die Broadcast-Domäne!

DHCP Attack "Rogue DHCP-Server"

```
Attack parameters

        Server ID 192.168.100.100
         Start IP 192.168.100.101
           End IP 192.168.100.099
Lease Time (secs) 12345670
Renew Time (secs) 12345670
      Subnet Mask 255.255.255.000
           Router 192.168.100.100
       DNS Server 123.456.789.123
           Domain Fake

ESC/Q to abort - ENTER to continue
```

Angriff ist begrenzt auf die Broadcast-Domäne!

Verhinderung von DHCP-Attacken

Port-Security (wie bekannt), ist nicht immer eine gute Lösung in größeren Netzen, an Up-Links, Trunks!

Besser dann DHCP Snooping!

4.6.1.1: DHCP Snooping

A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. DHCP spoofing is dangerous because clients can be leased IP information such as malicious DNS server addresses, malicious default gateways and malicious IP assignments.

Security best practices recommend using DHCP snooping to mitigate DHCP spoofing attacks.

DHCP snooping builds and maintains a database called the DHCP Snooping Binding Database (also known as the DHCP Snooping Binding Table). This database includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on each untrusted switch port or interface. The network administrator must define what ports are to be trusted. By combining the information in the DHCP Snooping Binding Database with the trusted ports, the switch is able to filter DHCP messages from untrusted sources.

When DHCP snooping is enabled on an interface or VLAN, and a switch receives a DHCP packet on an untrusted port, the switch compares the source packet information with that held in the DHCP Snooping Binding Database. The switch will deny packets containing any of the following information:

- Unauthorized DHCP server messages coming from an untrusted port
- Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits
- DHCP relay-agent packets that include option-82 information coming from an untrusted port.

Note: Option 82 provides additional security and is used to send information about DHCP clients to the DHCP server. However, an untrusted port should not be receiving option-82 packets.

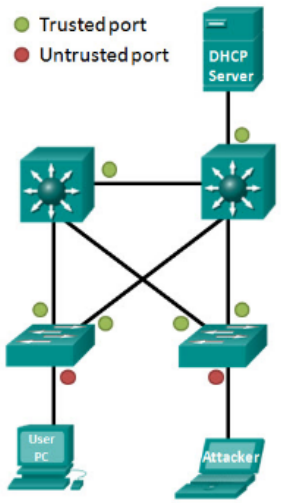
In a large network, the DHCP Snooping Binding Database may take time to build after it is enabled. For example, it could take 2 days for DHCP snooping to complete the database if DHCP lease time is 4 days.

DHCP snooping recognizes two types of ports:

- **Trusted DHCP ports** - Only ports connecting to upstream DHCP servers should be trusted. These ports should lead to legitimate DHCP servers replying with DHCP offer and DHCP Ack messages. Trusted ports must be explicitly identified in the configuration.
- **Untrusted ports** - These ports connect to hosts that should not be providing DHCP server messages. By default, all switch ports are untrusted.

Figure 1 provides a visual example of how DHCP snooping ports should be assigned on a network.

Figure 1: Identifying Trusted and Untrusted DHCP Snooping Ports



CCNA 6 Bridge-Kurse:

Leider sehr wenig im neuen Curriculum.Es gibt leider auch keine Praktika!

DHCP Snooping!

- Was ist das?
  - Ähnlich einer "Firewall", zwischen DHCP-Clients und den/m DHCP-Server
  - Unterschieden wird zwischen „trusted und untrusted“ Informationen
  - Bildung einer „snooping binding database“
  - Bestimmung welcher Switchport darf auf DHCP-Requests antworten (trusted - untrusted Ports)
  - Trusted Ports können alle DHCP-Messages durchlassen
  - Untrusted -> nur Requests, muss nicht extra konfiguriert werden

DHCP Snooping!

Was ist das?

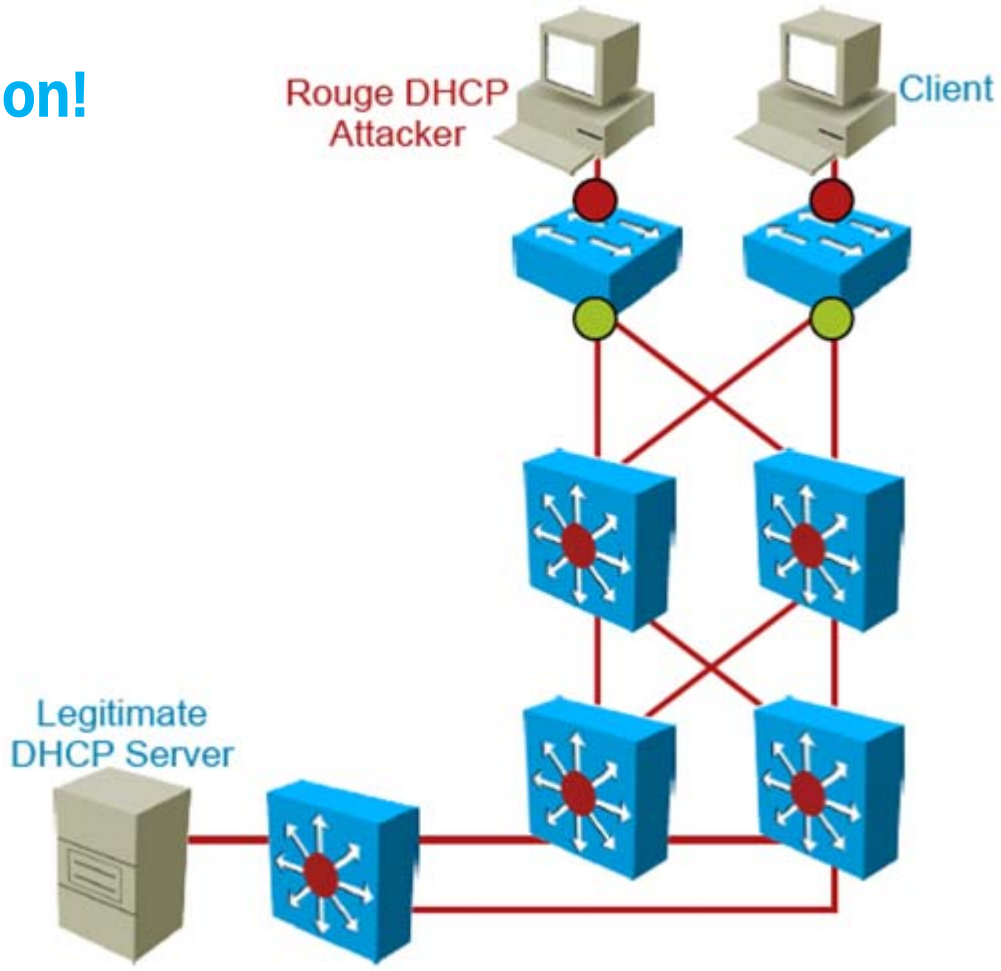
- Trusted Ports in Richtung des DHCP-Servers
- Sendet ein Host, an einem untrusted Port, eine Antwort auf einen Request (Discover) -> Port geht in error-disable
- Untrusted Ports dürfen keine Serverantworten wie:
  - DHCPOFFER; DHCPACK oder DHCPNAK senden
- Bindig-Tabelle wird an untrusted Ports gebildet mit:
  - Client-MAC
  - IP-Adresse
  - Lease-Time
  - VLAN-ID und Port-ID von welcher der Client nach einer Adresse fragte

DHCP Snooping!

Infrastrukturkonfiguration!

Trusted Ports

Untrusted Ports



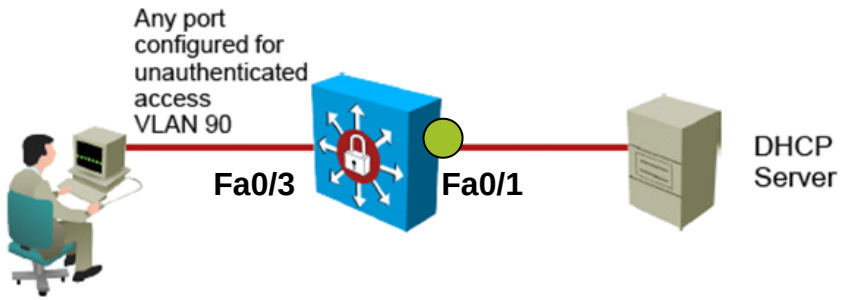
Konfiguration DHCP Snooping

Step	Commands
1.	Enable DHCP snooping globally: Switch(config)# **ip dhcp snooping**
2.	Enable DHCP Option 82: Switch(config)# **ip dhcp snooping information option**
3.	Configure DHCP server interfaces or uplink ports as trusted: Switch(config-if)# **ip dhcp snooping trust**
4.	Configure the number of DHCP packets per second (pps) that are acceptable on the port: Switch(config-if)# **ip dhcp snooping limit rate** *rate*
5.	Enable DHCP snooping on specific VLANs: Switch(config)# **ip dhcp snooping vlan** *number* **[***number***]**
6.	Verify the configuration: Switch# **show ip dhcp snooping**

Option evt. ausschalten!

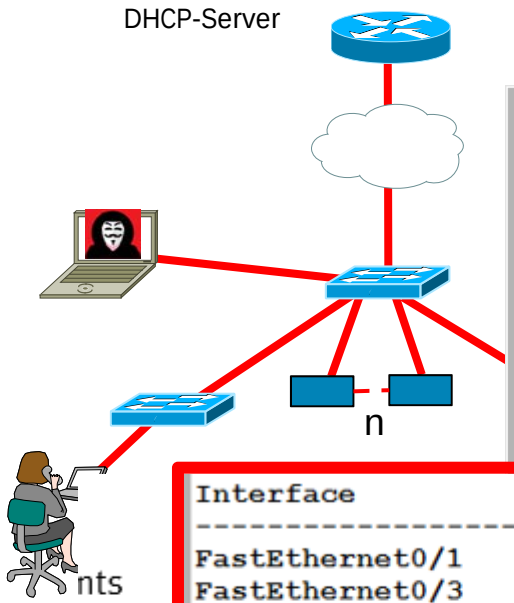
Konfiguration DHCP Snooping

```
no aaa new-model
ip subnet-zero
!
ip dhcp snooping vlan 1
ip dhcp snooping
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 ip dhcp snooping limit rate 200
 ip dhcp snooping trust
!
Interface Fastethernet0/3
 ip dhcp snooping limit rate 20
```



Verhindert Starvation!

Auswirkung nach der Konfiguration



COM3 - PuTTY

```
Snooping>ena
Snooping#sh ip dhcp snoo
Snooping#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/1              yes         200
FastEthernet0/3              no          20
Snooping#sh ip dhcp snooping bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:29:02:6B:46   10.0.0.3         86008       dhcp-snooping  1     FastEthernet0/3
3C:97:0E:68:CF:E3   10.0.0.2         85968       dhcp-snooping  1     FastEthernet0/3
Total number of bindings: 2
```

Eintrag der aktiven über DHCP- konfigurierten PC's!

Auswirkung nach der Konfiguration bei erneuter Attacke!

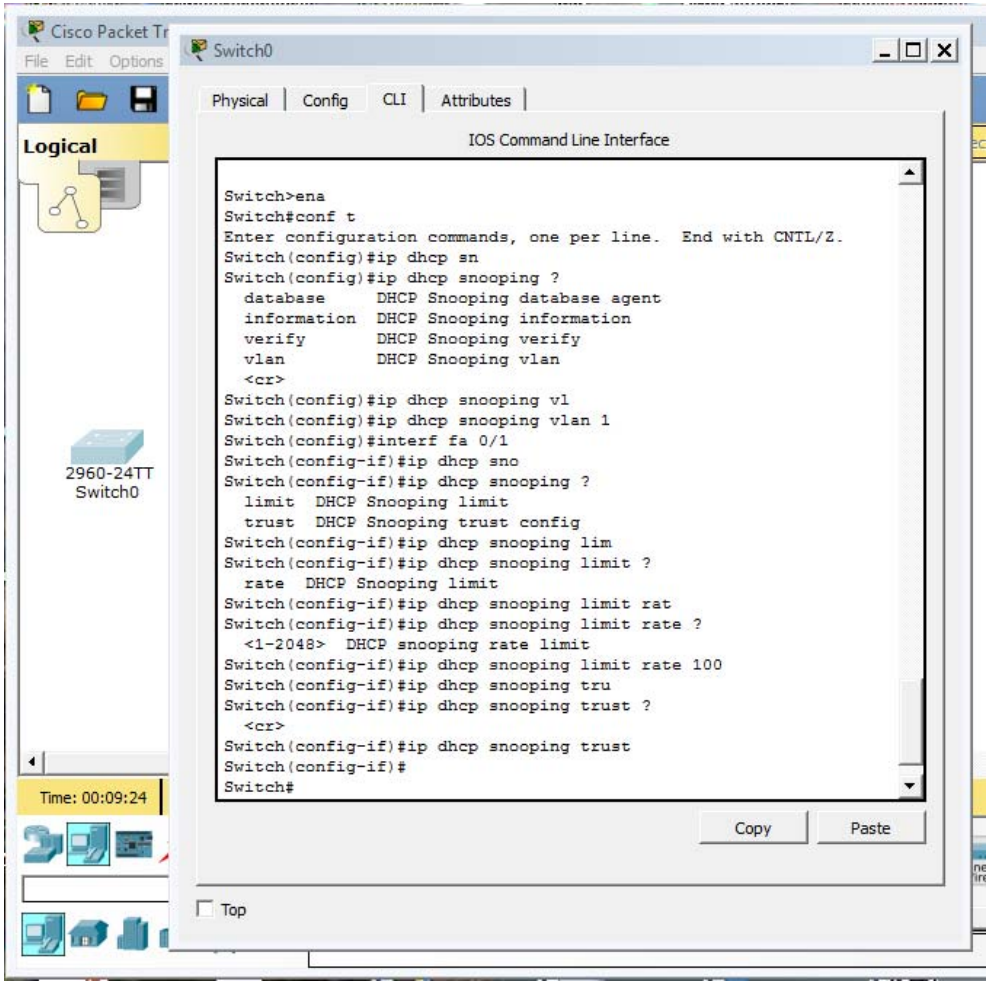
DHCP-Server

COM3 - PuTTY

```
  event    DHCP Snooping event
  packet   DHCP Snooping packet

Snooping#deb ip dhcp snooping ev
Snooping#deb ip dhcp snooping event
DHCP Snooping Event debugging is on
Snooping#
01:10:21: DHCP_SNOOPING: exceeded rate limit 20pps on Fa0/3
01:10:21: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 20 DHCP
 packets on interface Fa0/3
01:10:21: DHCP_SNOOPING_SW: perform error disable for interface (Fa0/3)
01:10:21: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Fa0/3, putting Fa0/3 in err-
disable state
Snooping#
01:10:21: DHCP_SNOOPING: exceeded rate limit 20pps on Fa0/3
01:10:21: DHCP_SNOOPING: exceeded rate limit 20pps on Fa0/3
Snooping#
01:10:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
 down
Snooping#
01:10:23: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
Snooping#
01:10:39: DHCP_SNOOPING: checking expired snoop binding entries
Snooping#
```

Konfiguration DHCP Snooping am PTracer



Simple Konfiguration möglich!

DHCP-Attacken können durch Snooping verhindert werden!

- DHCP Starvation können mit Portsecurity und DHCP-Snooping "rate-limit" an untrusted Ports verhindert werden!
- Rogue DHCP-Server kann durch Snooping an untrusted Ports verhindert werden.
- VLAN-Konfiguration -> alle Ports im VLAN sind untrusded

Was ist aber mit anderen Attackierungen?
z.B. ARP-Spoofing, IP-Spoofing

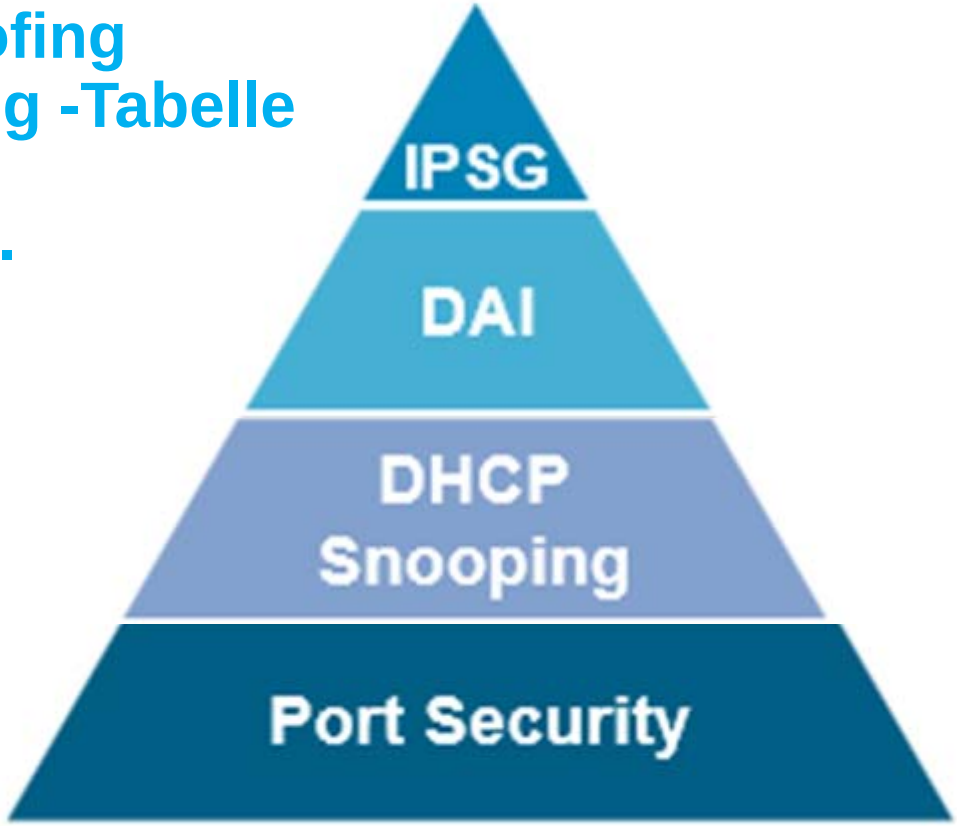
Weitere Feature im Zusammenhang mit Snooping!

Verhindert IP Address-Spoofing
Nutzung der Snooping -Tabelle

Verhindert MAC-Spoofing u. Poisoning bei Nutzung der Snooping-Tabelle

Verhindert DHCP-Client-Server-Attacken

Verhindert MAC-flooding, und auch DHCP-Starvation



DAI Commands

Command	Description
Switch(config)# **ip arp inspection vlan** *vlan_id* [*vlan_id*]	Enables DAI on a VLAN or range of VLAN's.
Switch(config-if)# **ip arp inspection trust**	Enables DAI on an interface and sets the interface as a trusted interface.
Switch(config)# **ip arp inspection validate** {[*src-mac*] [*dst-mac*] [*ip*]}	Configures DAI to drop ARP packets when the IP addresses are invalid, or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header.

Configuring IP Source Guard

Step	Commands
1.	Switch(config)# **ip dhcp snooping**
2.	Switch(config)# **ip dhcp snooping vlan** *number [number]*
3.	Switch(config-if)# **ip verify source vlan dhcp-snooping** or Switch(config-if)# **ip verify source vlan dhcp-snooping port-security**
4.	Switch(config-if)# **switchport portsecurity limit rate** *invalid-source-mac N*
5.	Switch(config)# **ip source binding** ***ipaddr*** **ip vlan** *number* **interface** *interface-id*

Danke für die Aufmerksamkeit!

Vielleicht gibt es noch Fragen?