



# network hacking

the flaws, the fear and the unexpected

# Definition Infastruktur

- Alles, was benötigt wird um IP-Pakete von einem Absender zu einem Empfänger zu transportieren:
  - Kabel
  - Switche
  - Router
  - Protokolle:
    - OSI-Layer2-Protokolle (STP, ARP, etc)
    - OSI-Layer3-Protokolle (IP, ICMP, OSPF, IS-IS, etc)
- Infrastruktur-Security betrachtet alle Parameter



# Infrastruktur als Basis

- Die Netzwerk-Infrastruktur bildet die gemeinsame Grundlage für Dienste & Applikationen:
  - Mail, Web, Active Directory, LDAP
  - Datei und Druckdienste, SAP, etc.
- Auf einer nicht-vertrauenswürdigen Infrastruktur können keine vertrauenswürdigen Dienste angeboten oder betrieben werden.



# Sicherheitsziele

- Verfügbarkeit

Die Infrastruktur sollte die gleiche Verfügbarkeit wie die Applikation mit der höchsten Verfügbarkeit haben.

# Sicherheitsziele

- Integrität

Infrastrukturprotokolle bestimmen, auf welchem Weg Informationen im Netzwerk transportiert werden. Die Integrität dieser Protokolle schützt somit die Vertraulichkeit und Integrität der transportierten Informationen indem der unautorisierte Zugriff auf die Daten während des Transports unterbunden wird.

# Sicherheitsziele

- Authentizität

Das Einbringen nicht authentifizierter Infrastruktur-Devices gefährdet die Verfügbarkeit der Infrastruktur und die Vertraulichkeit und Integrität der transportierten Daten.

# Infrastruktur wird vernachlässigt

- Infrastruktur-Sicherheit erhält heute weniger Aufmerksamkeit als noch vor einigen Jahren.
- Security wird von Trends getrieben:
  - “Web-App-Security” als Trend
  - “Client-Security” als Trend
  - “Mobile Security” als Trend
  - "Compliance" als Trend



# Infrastruktur wird vernachlässigt

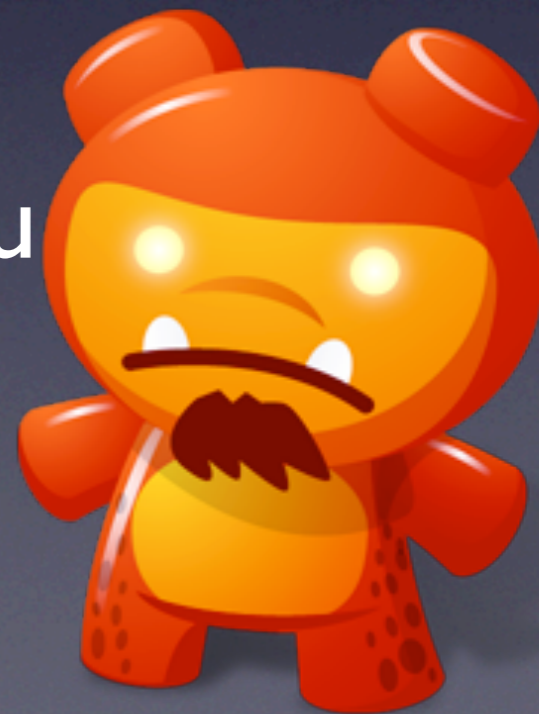


- Und hinzu kommt:
  - Netzwerk-Infrastruktur wird als “gegeben” betrachtet
  - ‘Admin-Schmerzen’: Zeit, Know-How, Budget
  - change-Mgmt, "weiß jemand was diese Kiste macht ?"
  - Oft outgesourct –mit fragwürdigen Implikationen bzgl. der Security
  - Und ausserdem:“Es läuft doch...”



# Bedrohungspotenzial

- Schlecht designte Protokolle können zum Verlust von Vertraulichkeit, Integrität, Verfügbarkeit führen.
- Implementation können BufferOverflows und ähnliche Fehler enthalten.
- Komplexität der Protokolle können zu Fehlkonfigurationen führen.

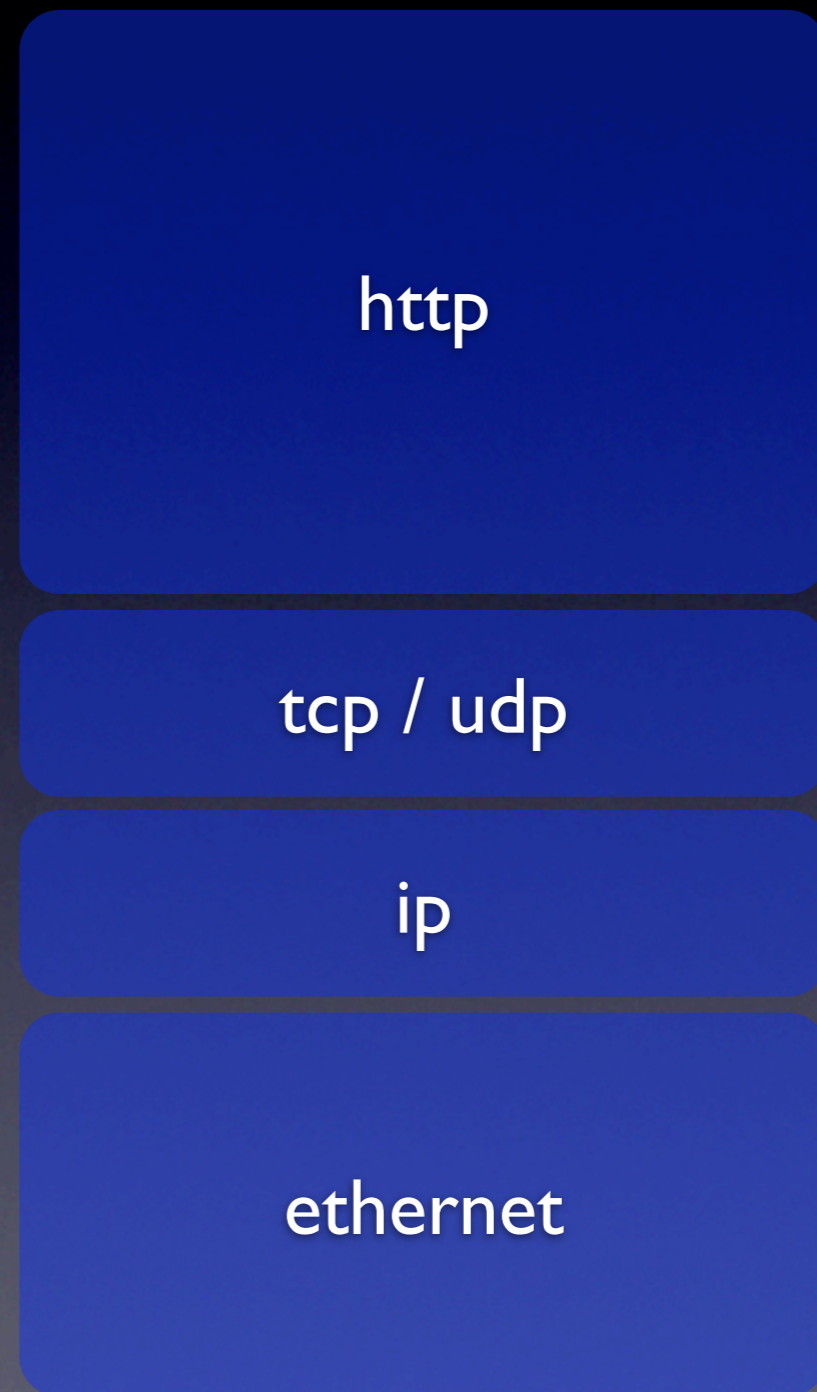
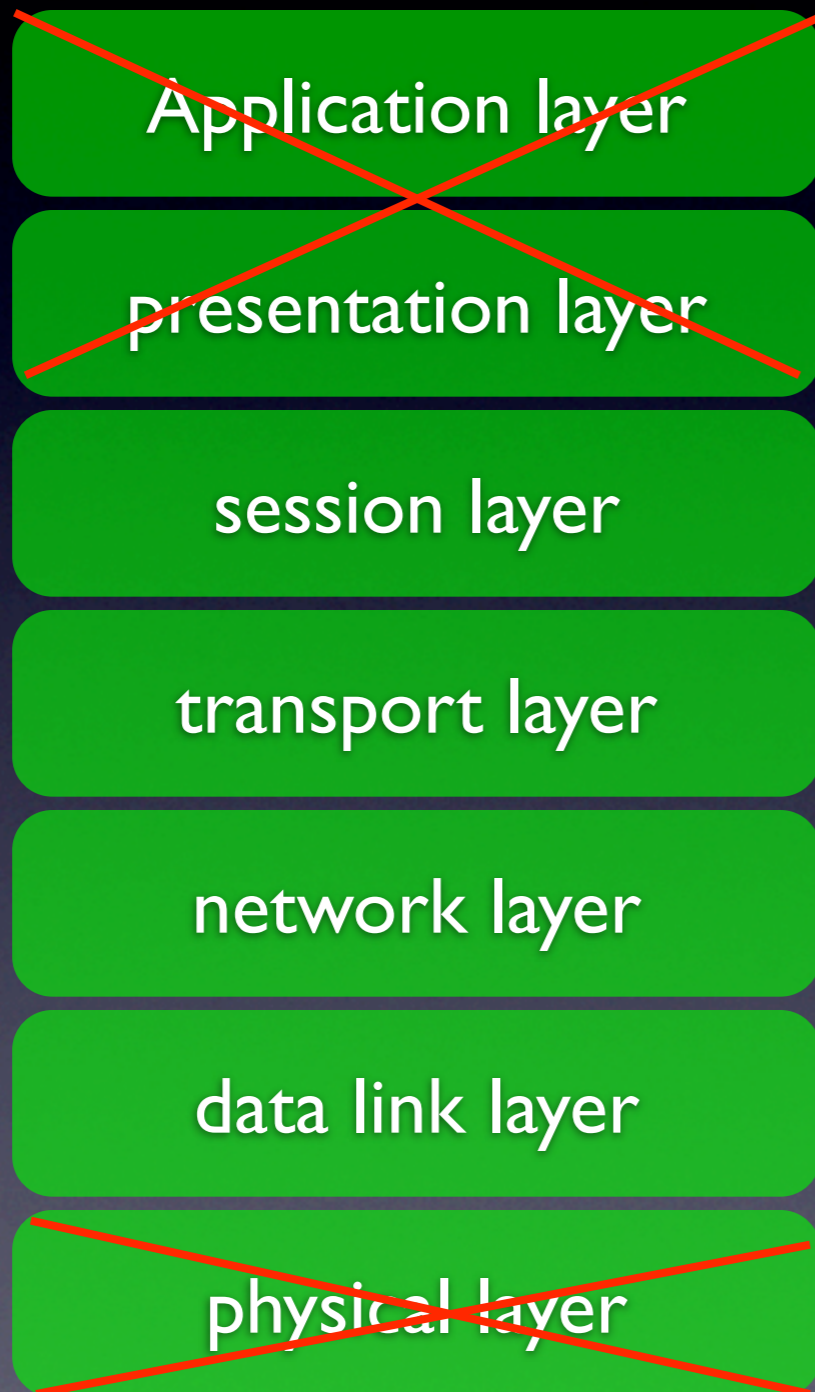


# Auswirkungen

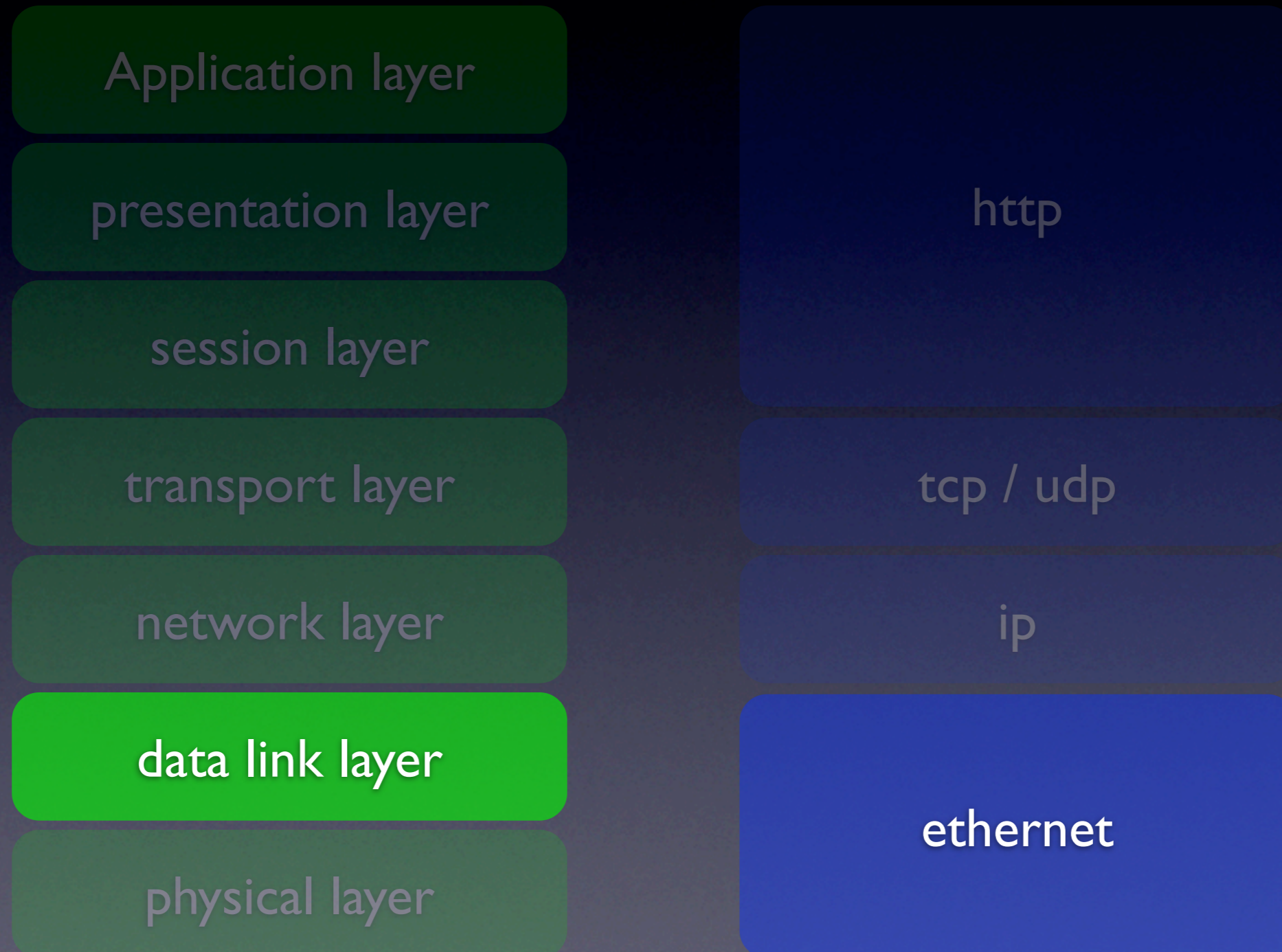
- Systemkompromittierung
  - Sniffing / Mitlesen von Daten
  - Umleiten von Verbindungen
  - Missbrauch von Ressourcen
- DOS



# iso | osi model



# layer 2 attack



# DTP

## dynamic trunking protocol

- Cisco proprietär
- Protokoll um Trunks zwischen Switchen auszuhandeln
- default aktiv
- 5 Modi Auto, On, Off, Desirable und No-Negotiate



demo  
[ yersinia ]

# VTP

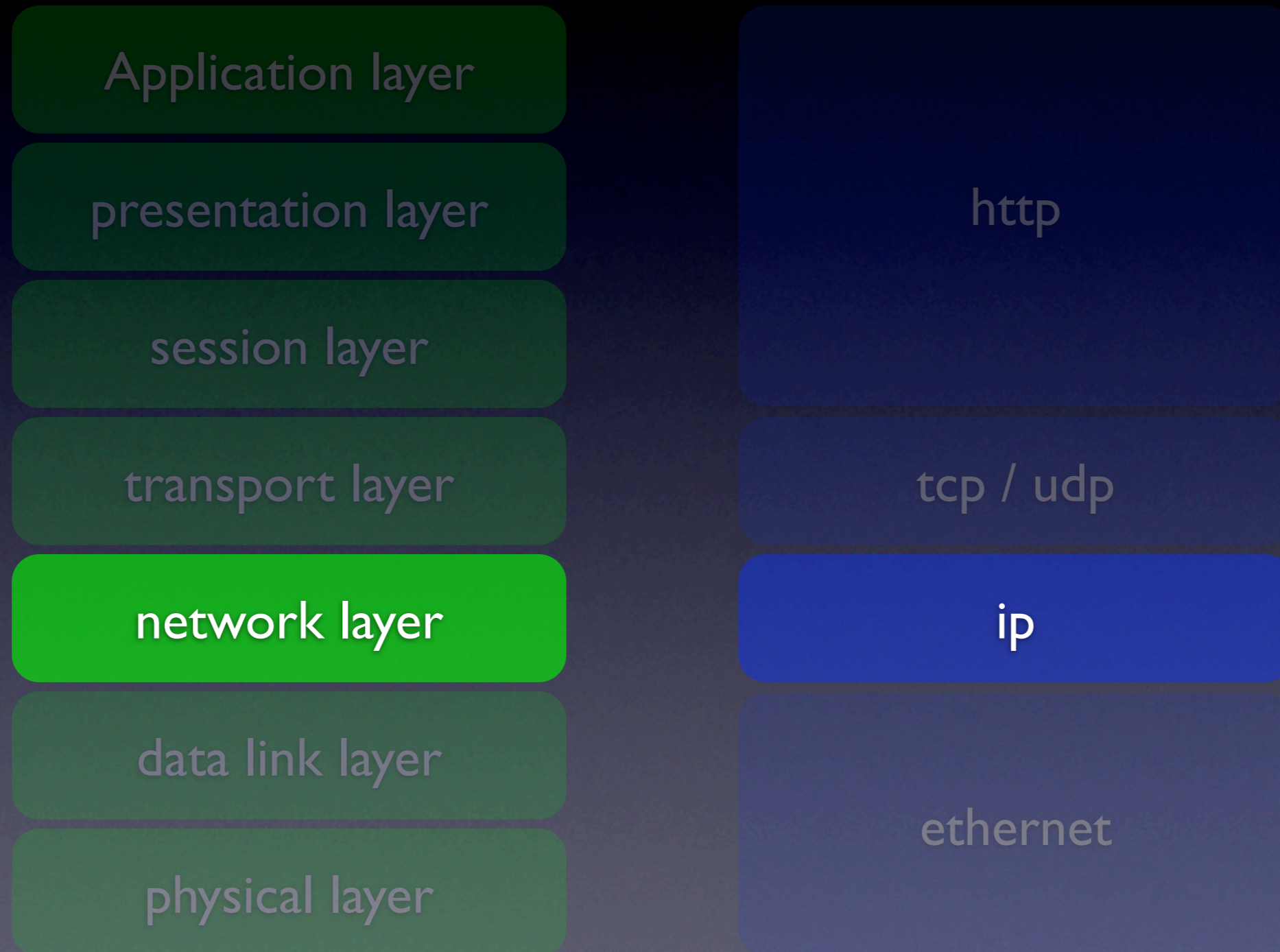
## vlan trunking protocol

- managet das Verteilen der vlans über mehrere Switche
- 3 modi client, server, transparent
- server gibt vlans über Advertisements weiter
- letzte Änderungen werden über IDs (Configuration Revision Number) über Advertisements verbreitet
- "default aktiv"



demo  
[ yersinia ]

# layer 3 attack



# OSPF

## open shortest path first

- modernes routing protokoll
- link state protocol
- infos über links werden durch LSAs ausgetauscht
- LSAs werden an alle bekannten Router geflutet
- Routingtabelle wird aus SPF Tree berechnet
- link"kosten" bewertung über Metiken

# OSPF

## open shortest path first

- per default keine Authentifizierung
  - Simple password authentication (Klartext)
  - Message Digest authentication (MD5)

# OSPF

## open shortest path first

- Angriffe von extern und intern
- Device Compromise (Kontrolle über den Router)
- Link Compromise (Kontrolle über Link)

# OSPF

open shortest path first

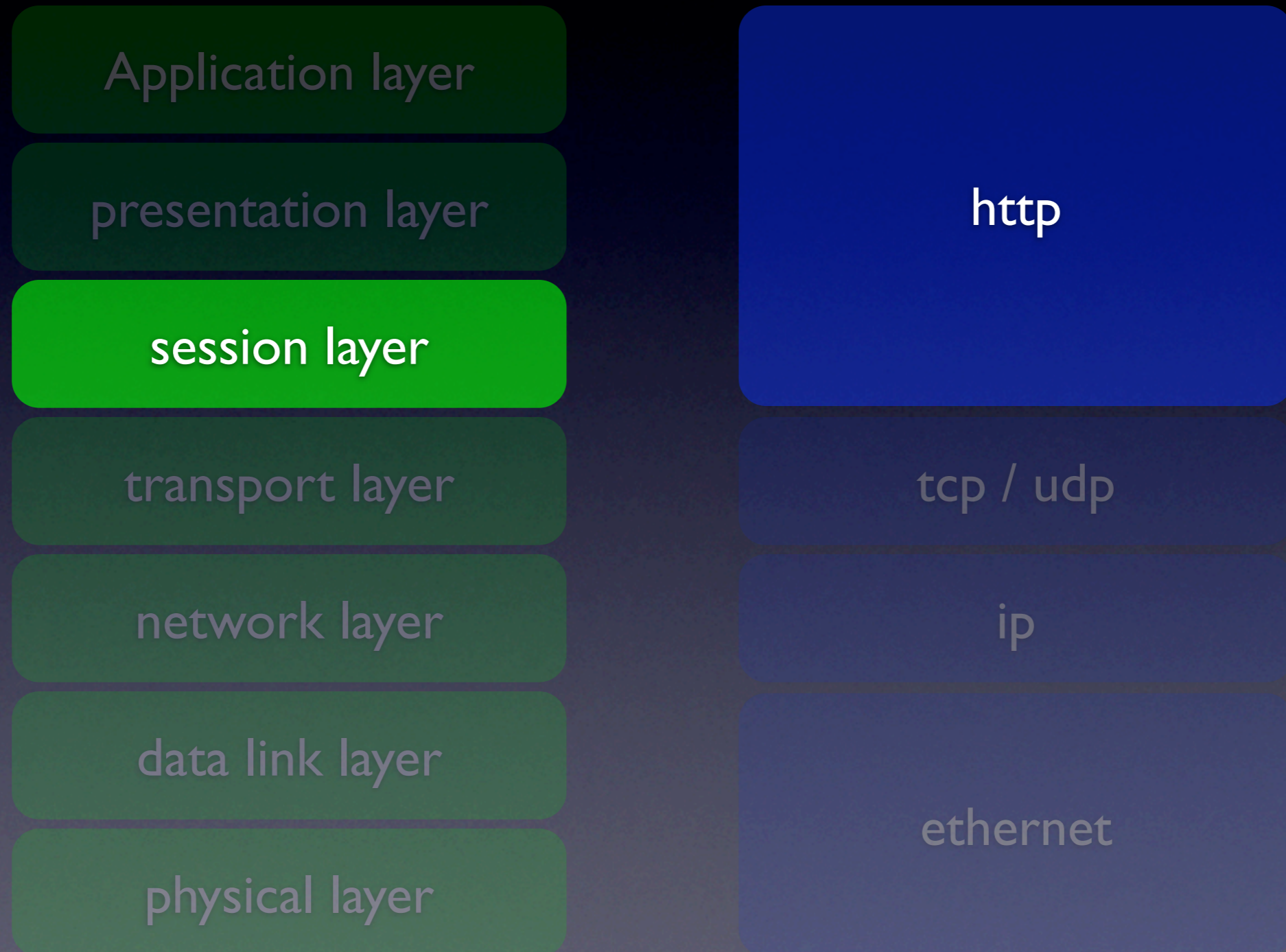
- DOS [ route > /dev/null ]
- MitM [ eavesdropping ]
- chaos [ add net, add area ]



tool

[ ospf attack shell ]

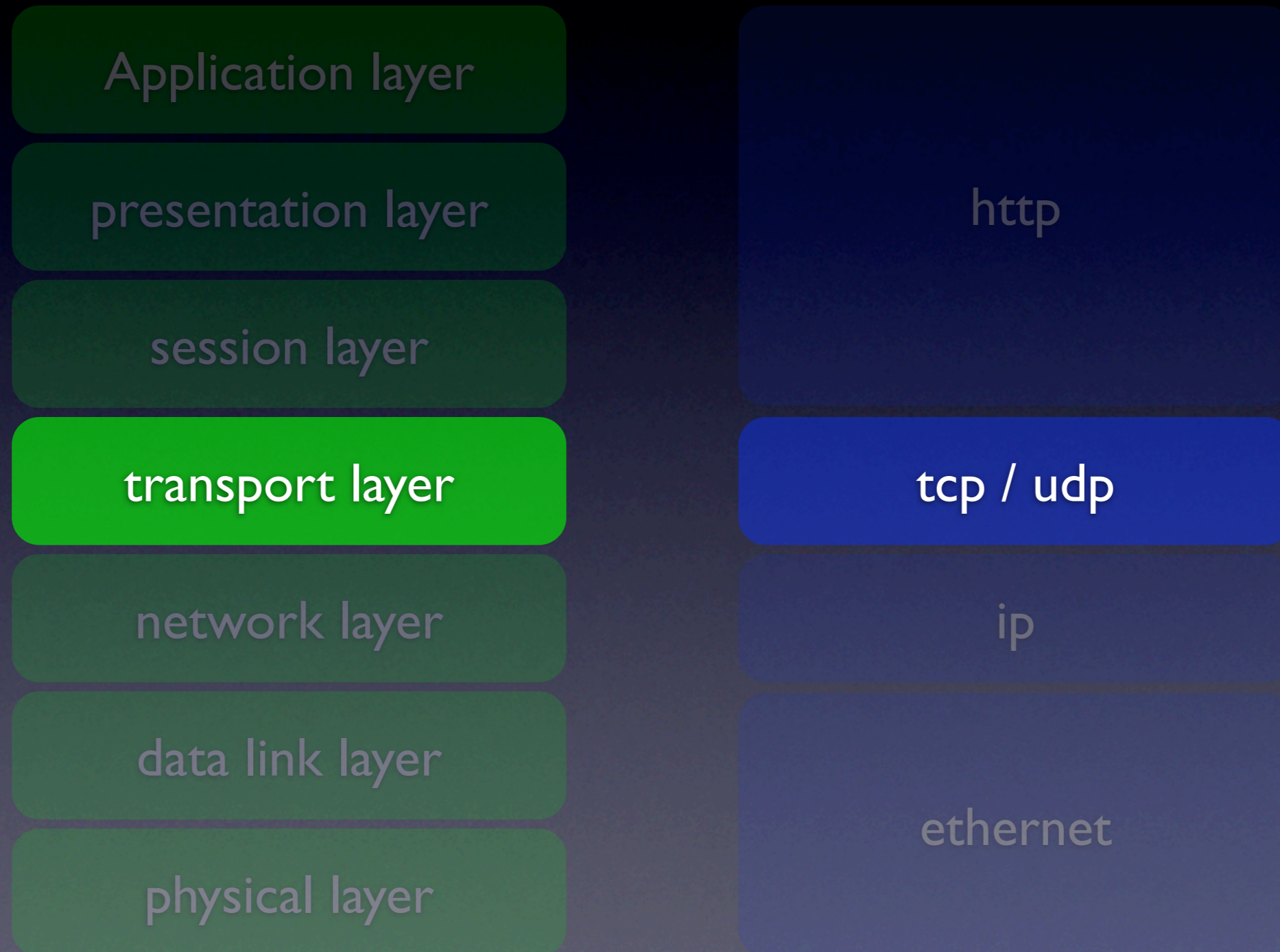
# layer 5 attack



# ssl-VPNs

- ssl bugs ;)
- client erzwingt schwache Verschlüsselung
- psk ist zu schwach
- selten client zertifikate

# layer 4 attack



# SCTP

stream control transmission protocol

- neues Transport Protokoll
- Gremium bei der IETF ist die SIGTRAN
- seit 2000 in RFC 2960, 4960 und 3286 def.
- zuverlässig und verbindungsorientiert
- UDP/TCP +



# SCTP

stream control transmission protocol

- QOS durch multiple byte-streams
- Multistreaming ( mehrere IP pro host)
- resistenz gegen synflood durch 4-way-Handshake und "cookies"
- Fluss und Überlastkontrolle ähnlich TCP
- desinged um SS7 über IP zu sprechen

# SS7

- durch CCIT als Nachfolger für SS5
- verhinderte blueboxing
- in telco Netzen, TCP/IP neben SS7 für Geräte Mgmt.
- Verfügbarkeit ( 911 112 )



# phylosophie

## "walled garden"

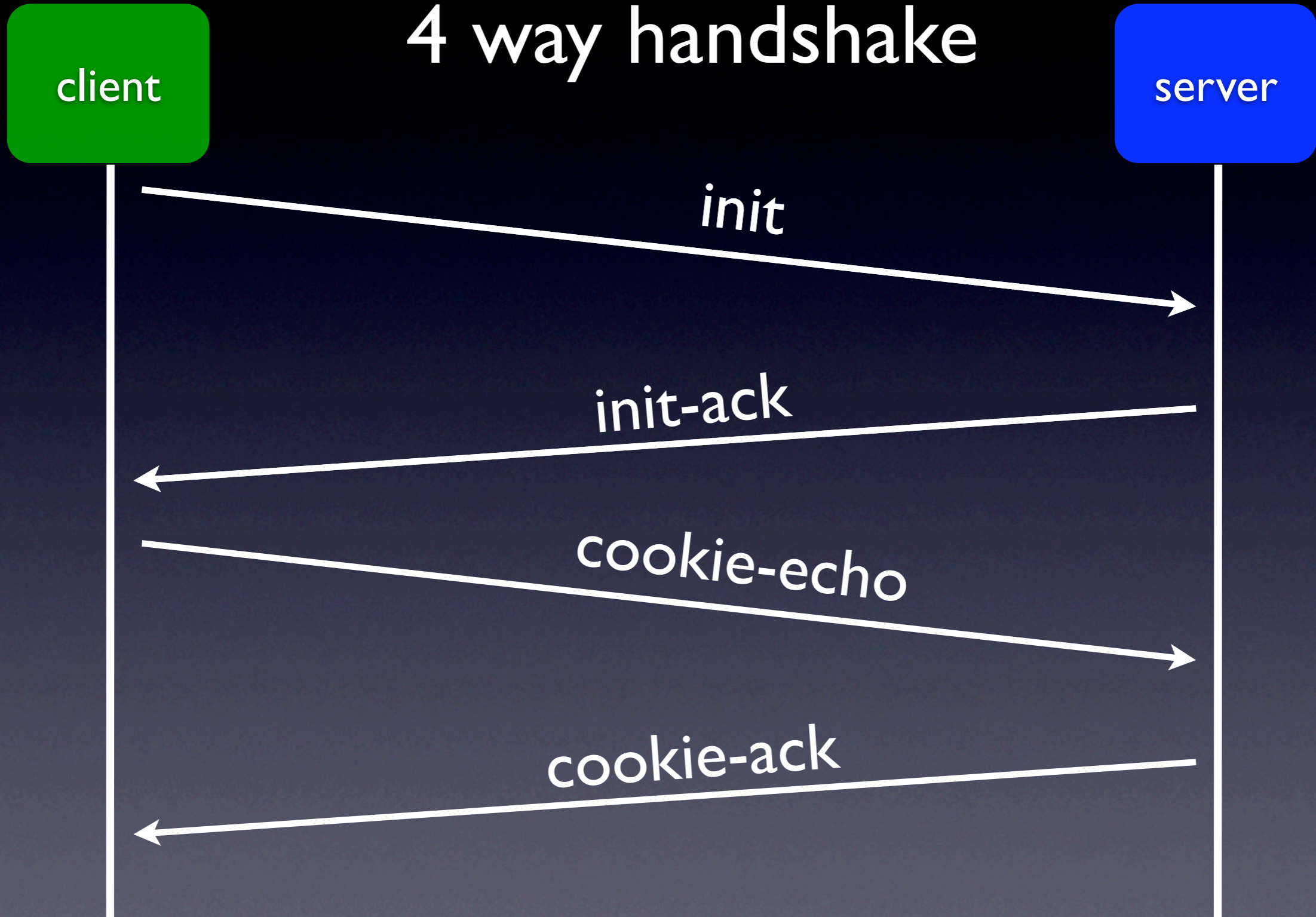
“Walled Garden - Mobile Network Operators (MNOs). At the start of 2007, probably the best example. MNOs manage closed networks - very hard to enter the garden, or leave the garden, especially as it pertains to Internet, web services, web applications. Fearful of losing customer and brand control, the MNOs opt to guard the garden as much as possible.”

# telco attacken

- SIP account hacking
  - wie "carding"
- VOIP GW hacking
  - wie "PBX hacking"
- Signaling hacking SS7 - SIGTRAN Ebene
  - zurück zur bluebox ?

# SCTP

## 4 way handshake

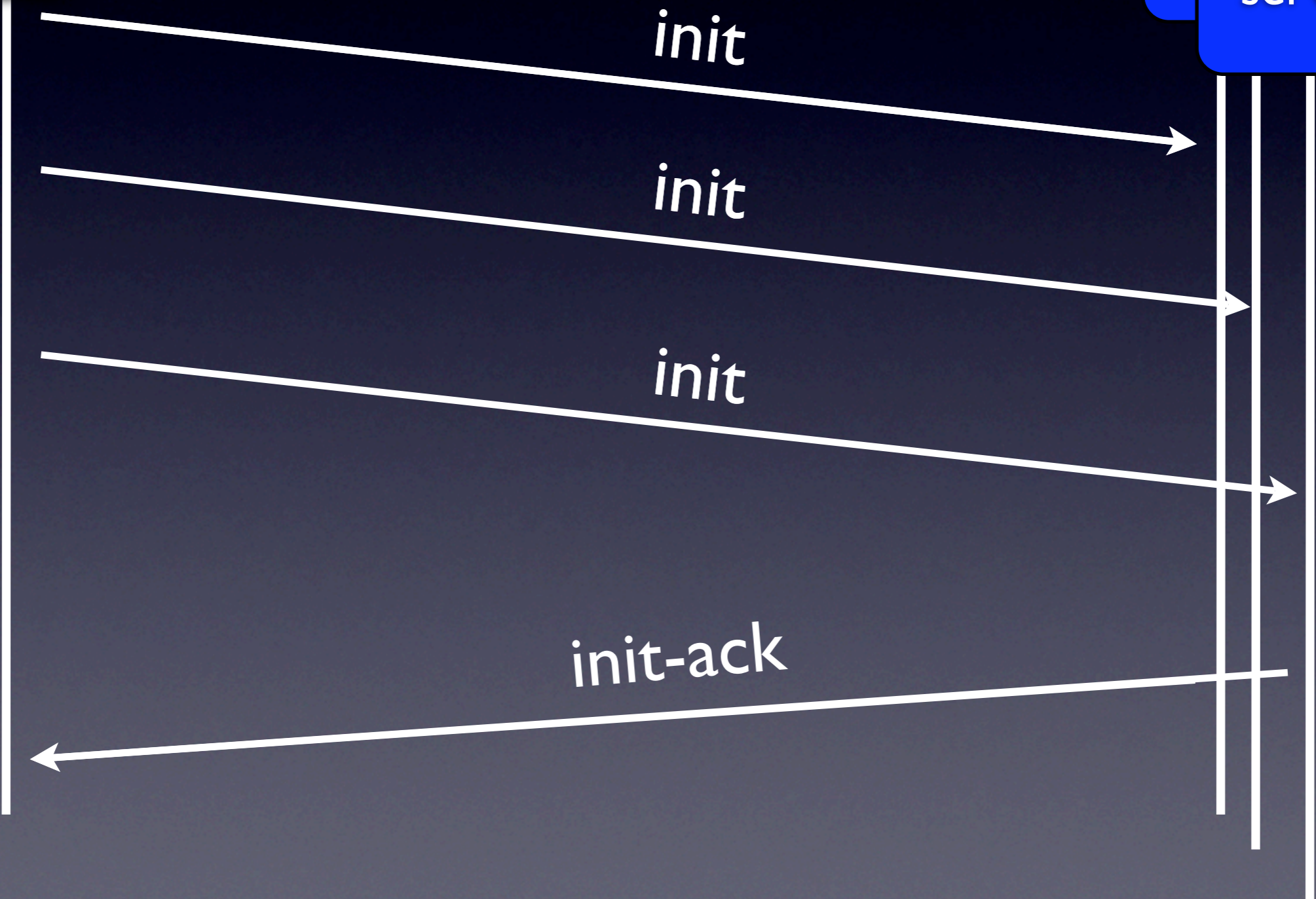
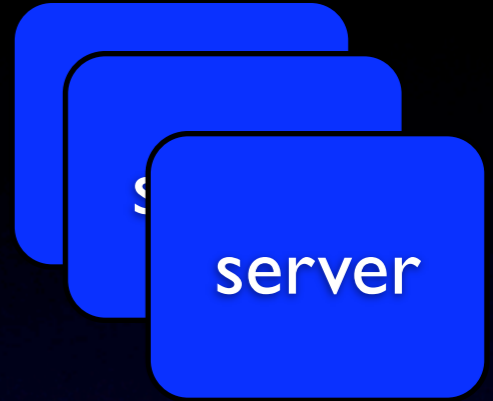


# SCTP scanning



- RFC sagt: "hosts should never answer to INIT packets on non-existing ports."
- RFC: 0, hacker: 1.
- synscans sind langsam ohne rst
  - Implementationen weichen vom RFC ab ;)

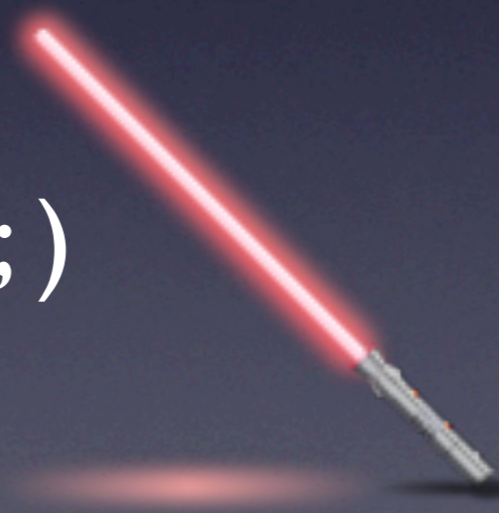
# SCTP scanning



# SCTP

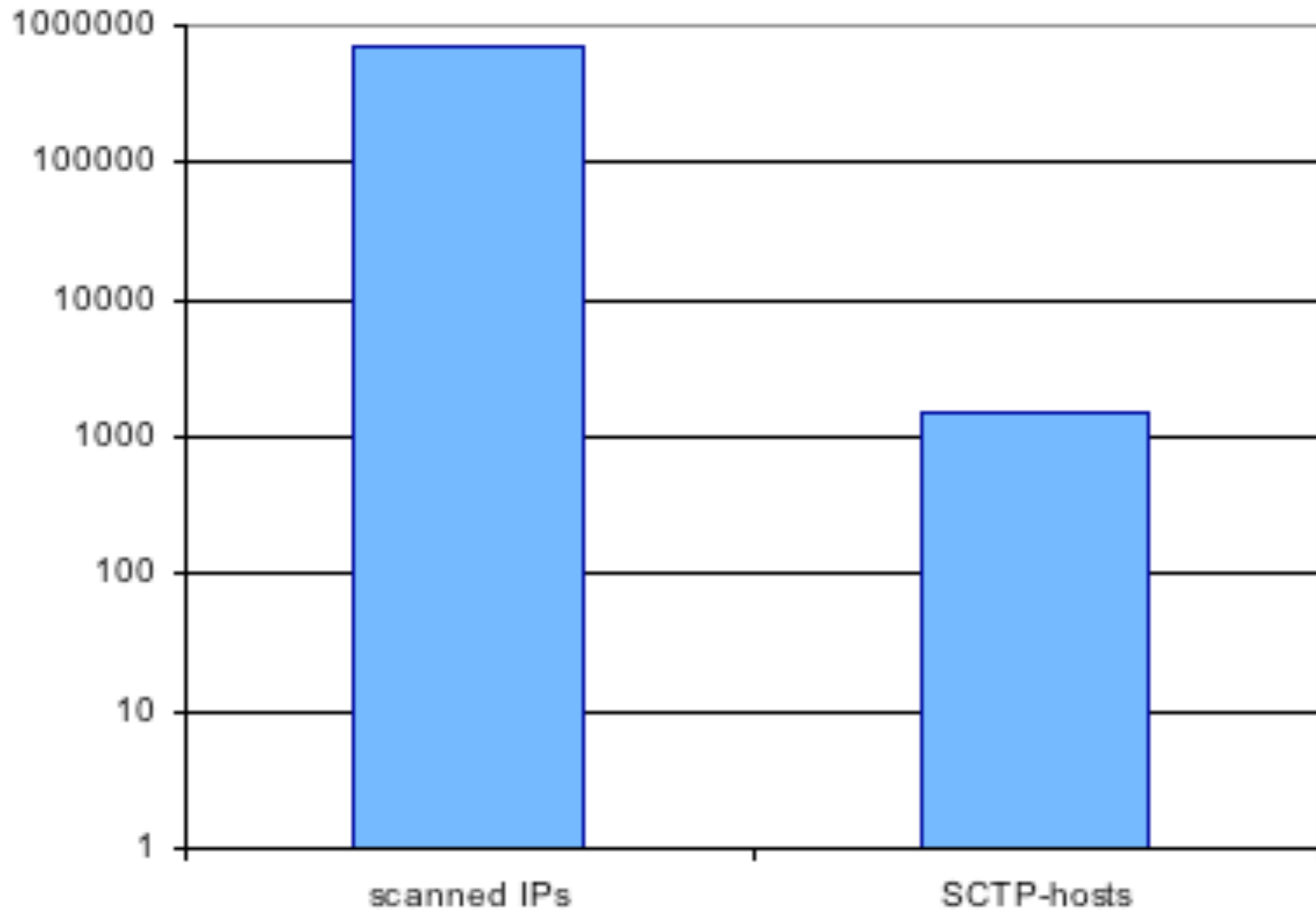
## Auswirkungen

- Wie gehen FW mit SCTP Paketen um?
- wieviele IDS sind für SCTP konfiguriert?
- schauen wir es uns an ;)



# SCTP

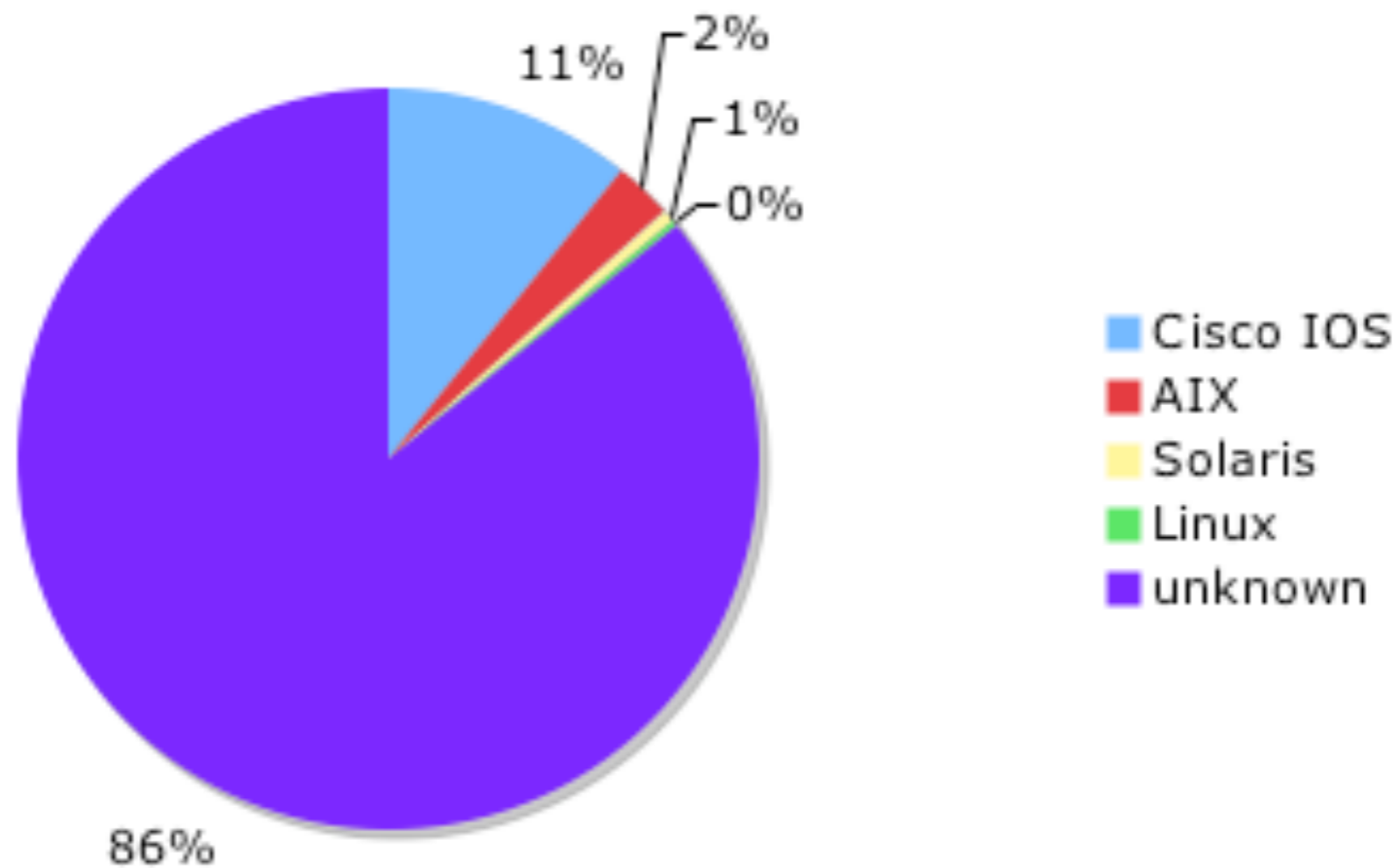
## scan results



# SCTP

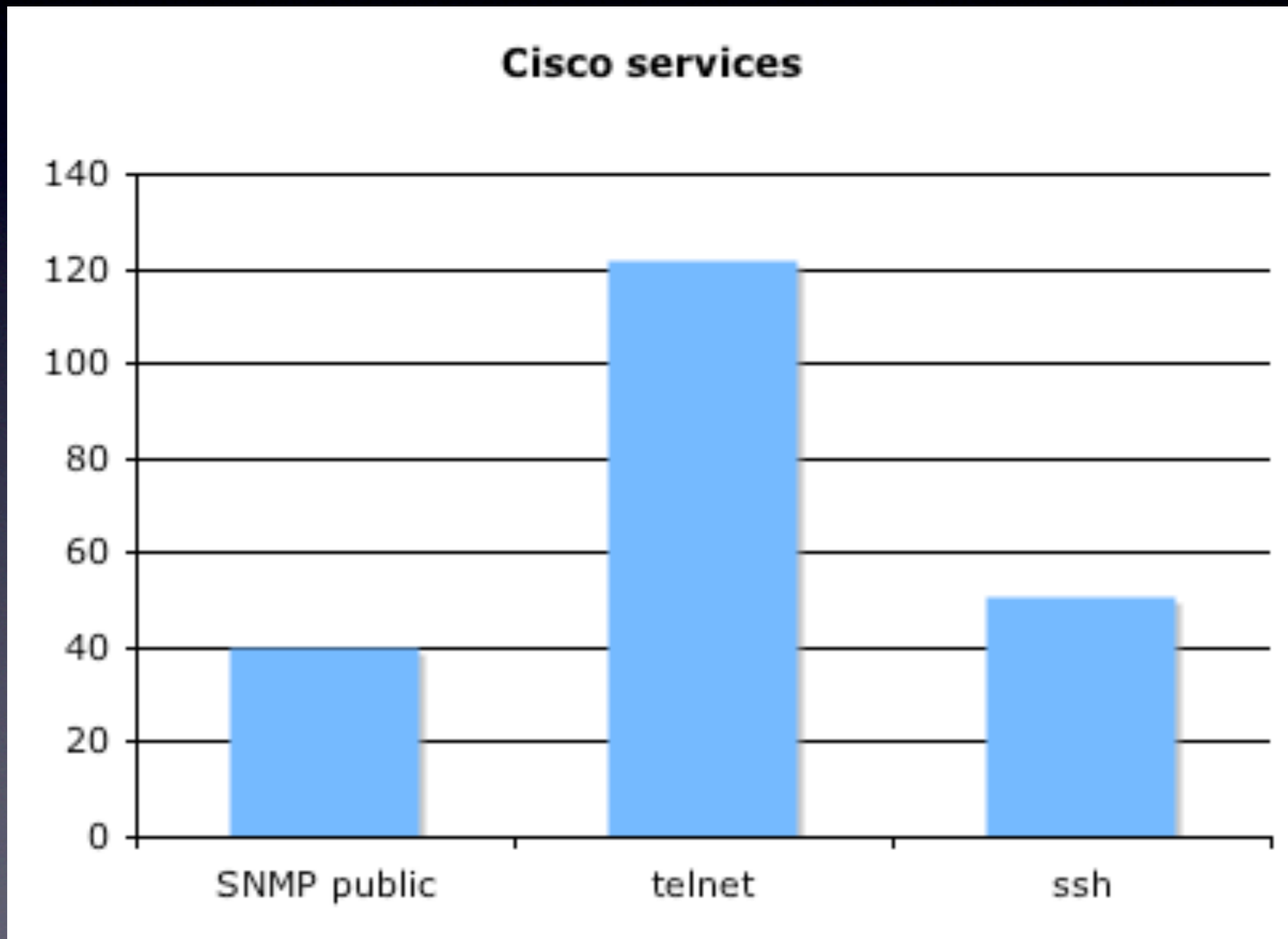
## scan results

**SCTP speaking OS**



# SCTP

## scan results



PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	Cisco SSH 1.25 (protocol 2.0)
23/tcp	open	telnet	Cisco router
79/tcp	filtered	finger	
135/tcp	filtered	msrpc	
136/tcp	filtered	profile	
137/tcp	filtered	netbios-ns	
138/tcp	filtered	netbios-dgm	
139/tcp	filtered	netbios-ssn	
445/tcp	filtered	microsoft-ds	
593/tcp	filtered	http-rpc-epmap	
1720/tcp	open	H.323/Q.931?	
4662/tcp	filtered	edonkey	
5060/tcp	open	sip?	

Service Info: OS: IOS; Device: router

80/tcp	open	http	Apache httpd 2.2.6 ((Unix) mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/4.4.4 mod_jk/1.2.25)
111/tcp	open	rpcbind	2-4 (rpc #100000)
443/tcp	open	ssl/http	Apache httpd 2.2.6 ((Unix) mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/4.4.4 mod_jk/1.2.25)
513/tcp	open	rlogin	
514/tcp	open	tcpwrapped	
587/tcp	open	smtp	Sendmail 8.13.7+Sun/8.13.7
898/tcp	open	http	Solaris management console server (Java 1.5.0_06; Tomcat 2.1; SunOS 5.10 sparc)
4045/tcp	open	nlockmgr	1-4 (rpc #100021)
5432/tcp	open	postgres?	
7100/tcp	open	font-service	Sun Solaris fs.auto
8009/tcp	open	ajp13?	
8080/tcp	open	http	Apache httpd 2.2.6 ((Unix) mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/4.4.4 mod_jk/1.2.25)
8888/tcp	open	http	Apache Tomcat 4.0.5
32771/tcp	open	status	1 (rpc #100024)
32772/tcp	open	metad	1-2 (rpc #100229)
32773/tcp	open		1-2 (rpc #100000)

2001/tcp	open	telnet	Cisco router
2002/tcp	open	telnet	Cisco router
2003/tcp	open	telnet	Cisco router
2004/tcp	open	telnet	Cisco router
2005/tcp	open	telnet	Cisco router
2006/tcp	open	telnet	Cisco router
2007/tcp	open	telnet	Cisco router
2008/tcp	open	telnet	Cisco router
2009/tcp	open	telnet	Cisco router
2010/tcp	open	telnet	Cisco router
2011/tcp	open	telnet	Cisco router
2012/tcp	open	telnet	Cisco router
2013/tcp	open	telnet	Cisco router
2014/tcp	open	telnet	Cisco router
2015/tcp	open	telnet	Cisco router
2016/tcp	open	telnet	Cisco router
2017/tcp	open	telnet	Cisco router
2018/tcp	open	telnet	Cisco router
2019/tcp	open	telnet	Cisco router
2020/tcp	open	telnet	Cisco router
2021/tcp	open	telnet	Cisco router

2000/tcp	open	canbook?
2001/tcp	open	dc?
2002/tcp	open	globe?
2003/tcp	open	cfingerd?
2004/tcp	open	mailbox?
2005/tcp	open	deslogin?
2006/tcp	open	invokator?
2007/tcp	open	dectalk?
2008/tcp	open	conf?
2009/tcp	open	news?
2010/tcp	open	search?
2011/tcp	open	raid-cc?
2012/tcp	open	ttyinfo?
2013/tcp	open	raid-am?
2014/tcp	open	troff?
2015/tcp	open	cypress?
2016/tcp	open	bootserver?
2017/tcp	open	cypress-stat?
2018/tcp	open	terminaldb?
2019/tcp	open	whosockami?
2020/tcp	open	xinupageserver?
2021/tcp	open	servexec?
2022/tcp	open	down?

Starting Nmap 4.53 ( <http://insecure.org> ) at 2008-02-15  
17:59 CEST

Strange error from connect (64):Host is down

All 1714 scanned ports on 23.42.5.666 are filtered

# Fazit



- SCTP ist interessant :)
- man kann noch interessantere hosts damit finden
- FW und IDS reagieren "anders" als bei nmap scans
- neue Spielwiese für alle denen IPv6 langsam langweilig wird.

EOF

