

Vertiefung Rechnertechnik und -netzwerke

Fahrplan

1. Wir bauen was.
2. Wir tricksen es aus.
3. Wir verstehen es.

1 Einführung: TCP/IP in der Praxis

- Als Administrator (`root`) anmelden
- Netzwerk-Automatismen ausschalten

1 Einführung: TCP/IP in der Praxis

- Als Administrator (`root`) anmelden
- Netzwerk-Automatismen ausschalten
- `ifconfig`: Netzwerkanschlüsse konfigurieren, IP-Adressen zuweisen
- `ping`: Erreichbarkeit prüfen
- `arp`: Zuordnung zwischen Hardware- und IP-Adressen abrufen
- `nc -l 1234` oder `nc -p 1234 -l`: auf TCP-Port 1234 „lauschen“
- `nc 10.1.1.9 1234`: Mit dem Rechner `10.1.1.9` auf TCP-Port 1234 kommunizieren

1 Einführung: TCP/IP in der Praxis

- Als Administrator (`root`) anmelden
- Netzwerk-Automatismen ausschalten
- `ifconfig`: Netzwerkanschlüsse konfigurieren, IP-Adressen zuweisen
- `ping`: Erreichbarkeit prüfen
- `arp`: Zuordnung zwischen Hardware- und IP-Adressen abrufen
- `nc -l 1234` oder `nc -p 1234 -l`: auf TCP-Port 1234 „lauschen“
- `nc 10.1.1.9 1234`: Mit dem Rechner `10.1.1.9` auf TCP-Port 1234 kommunizieren
- `echo 1 > /proc/sys/net/ipv4/ip_forward`: Rechner mit zwei Netzwerkanschlüssen soll durchreichen
- `route`: Routing-Tabelle konfigurieren
- Rechner in Teilnetz `10.1.1.0` mit Maske `255.255.255.0`, wenn: Rechner-IP-Adresse & `255.255.255.0 == 10.1.1.0`
- Default-Gateway: für Teilnetz `0.0.0.0` mit Maske `0.0.0.0`

1 Einführung: TCP/IP in der Praxis

- E-Mail versenden mit `nc` auf Port 25
Protokoll: SMTP

1 Einführung: TCP/IP in der Praxis

- E-Mail versenden mit `nc` auf Port 25
Protokoll: SMTP
- Web-Surfen mit `nc` auf Port 80:
Protokoll: HTTP

1 Einführung: TCP/IP in der Praxis

- E-Mail versenden mit `nc` auf Port 25
Protokoll: SMTP
- Web-Surfen mit `nc` auf Port 80:
Protokoll: HTTP
- Manueller Webserver: `nc -p 80 -l`

1 Einführung: TCP/IP in der Praxis

- E-Mail versenden mit `nc` auf Port 25
Protokoll: SMTP
- Web-Surfen mit `nc` auf Port 80:
Protokoll: HTTP
- Manueller Webserver: `nc -p 80 -l`
- Der Webserver kann der IP-Adresse und dem HTTP-Dialog etliche Informationen über den Besucher entnehmen.

2 Schichtenmodelle

2 Schichtenmodelle

2.1 Das DoD-Schichtenmodell

Department of Defense

Nr.	Name	Beispiele
4	Anwendung	HTTP, SMTP, SSH, OpenVPN, FTP, LDAP, NCP, AppleTalk AFP
3	Transport	UDP, TCP, SPX, AppleTalk ATP
2	Internet	IP, IPX, NetBEUI, AppleTalk DDP
1	Netzzugang	Ethernet, FDDI, Profibus, ARCNET, Token Ring, LocalTalk

2 Schichtenmodelle

2.2 Das OSI-Schichtenmodell

Open Systems Interconnection

Nr.	Name	Beispiele
7	Anwendung	HTTP, SMTP, SSH, FTP, LDAP, NCP, AppleTalk AFP
6	Darstellung	ASCII, EBCDIC, Kompression, SSL/TLS (Verschlüsselung)
5	Sitzung	RPC, SOCKS, AppleTalk ASP
4	Transport	UDP, TCP, SPX, AppleTalk ATP
3	Vermittlung	IP, ICMP, IPX, NetBEUI, AppleTalk DDP
2	Sicherung	Ethernet, FDDI, Profibus, ARCNET, Token Ring, LocalTalk, Briefftauben
1	Bitübertragung	Telefon-, Koaxial-, TP-, Glasfaser- oder sonstige Kabel, Funk, Papier

2 Schichtenmodelle

2.2 Das OSI-Schichtenmodell

Open Systems Interconnection

Nr.	Name	Beispiele
7	Anwendung	OpenPGP, S/MIME
		HTTP, SMTP, SSH, OpenVPN, FTP, LDAP, NCP, AppleTalk AFP
6	Darstellung	ASCII, EBCDIC, Kompression, SSL/TLS (Verschlüsselung)
5	Sitzung	RPC, SOCKS, AppleTalk ASP
4	Transport	UDP, TCP, SPX, AppleTalk ATP
3	Vermittlung	IP, IPsec, ICMP, IPX, NetBEUI, AppleTalk DDP
2	Sicherung	ARP
		Ethernet, FDDI, Profibus, ARCNET, Token Ring, LocalTalk, Briefftauben
1	Bitübertragung	Telefon-, Koaxial-, TP-, Glasfaser- oder sonstige Kabel, Funk, Papier

2 Schichtenmodelle

2.3 Protokollstapel

2 Schichtenmodelle

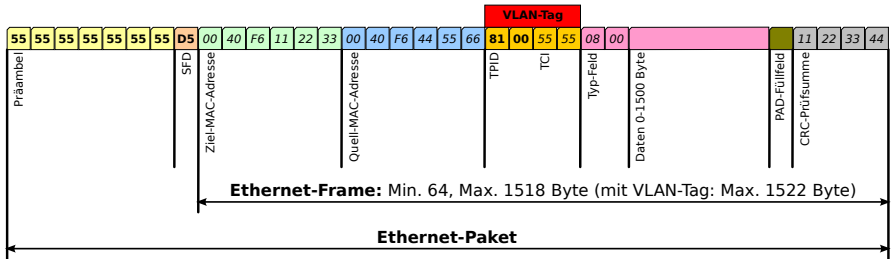
2.3 Protokollstapel

Protokollturm

2 Schichtenmodelle

2.3 Protokollstapel

Protokollturm



2 Schichtenmodelle

2.3 Protokollstapel

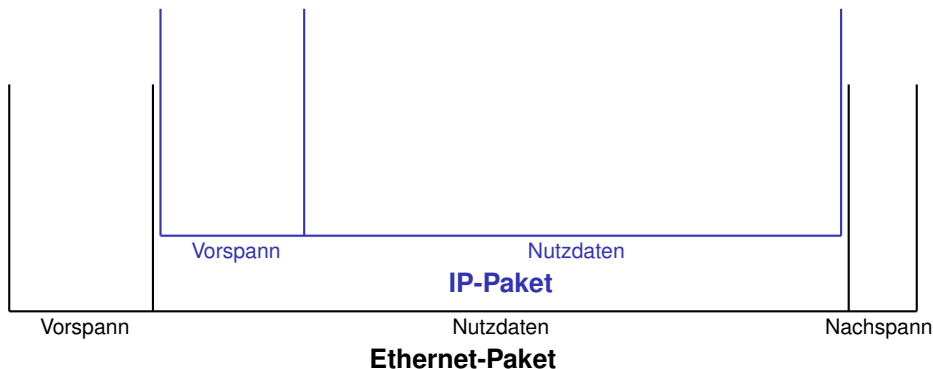
Protokollturm



2 Schichtenmodelle

2.3 Protokollstapel

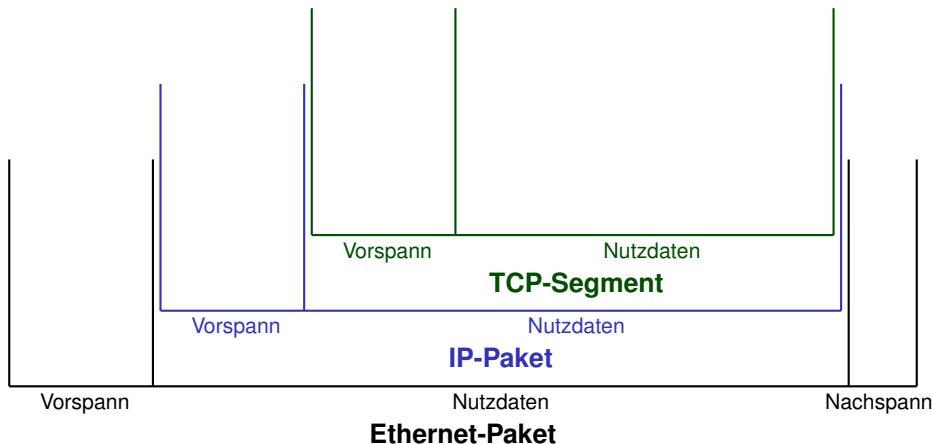
Protokollturm



2 Schichtenmodelle

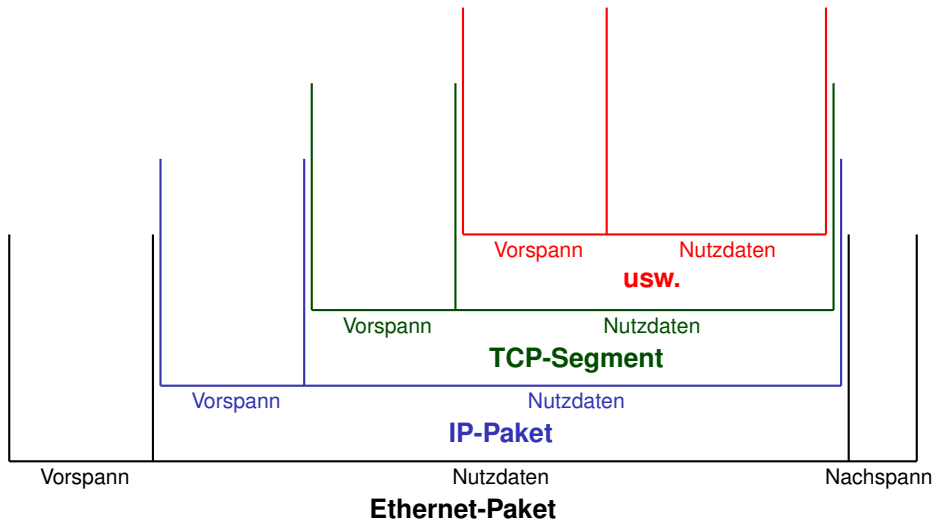
2.3 Protokollstapel

Protokollturm



2 Schichtenmodelle

2.3 Protokollstapel



2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen

2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen
- `tcpdump`: Pakete beobachten

2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen
- `tcpdump`: Pakete beobachten
- `wireshark`: Pakete analysieren

2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen

- `tcpdump`: Pakete beobachten
- `wireshark`: Pakete analysieren

→ Konfiguration untersuchen, Fehler und Angriffe erkennen

2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen

- `tcpdump`: Pakete beobachten
- `wireshark`: Pakete analysieren

—> Konfiguration untersuchen, Fehler und Angriffe erkennen

- `ettercap`: Man-in-the-Middle-Angriffe

2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen

- `tcpdump`: Pakete beobachten
- `wireshark`: Pakete analysieren

—> Konfiguration untersuchen, Fehler und Angriffe erkennen

- `ettercap`: Man-in-the-Middle-Angriffe

Warnung: Unerlaubte Anwendung ist eine Straftat!
(—> mehrjährige Freiheitsstrafe)