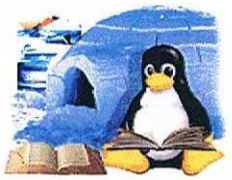
Linux basic

netzwerk

Version 2005-11-29

DipLInf. (FH) Bernd Schwägerl
DipLInf. (FH) Stefan Edenhofer



Netzwerkeinstellungen abfragen und einstellen (IPv4)

Netzwerk-Interface-Card (NIC):	
ifconfig	Abfrage der aktuellen Einstellungen für alle Schnittstellen
ifconfig [schnittstelle] [adresse] [parameter]	
ifconfig eth0 172.17.21.11 netmask 255.255.255.0 broadcast 172.17.21.255	
Die wichtigsten Parameter	
broadcast [BC-Adresse]	Broadcastadresse setzen
down	Schnittstelle deaktivieren
mtu [Zahl]	Maximale Transfer Unit setzen
netmask [MASK]	Netzmaske setzen
up	Schnittstelle aktivieren
Routing:	
arp -n	ARP-Tabelle (MAC-IP-Zuweisung) anzeigen ohne Namensauflösung (-n).
route -n	Abfrage der aktuellen Routinginformationen ohne Namensauflösung (-n).
route [add|del] [-net|-host] [Ziel] netmask [NM] gw [Gateway] dev [IF]	
route add -net 172.16.1.0 netmask 255.255.255.0 gw 172.17.21.1 dev eth0	
Aktivieren des Routings :	
echo "1" > /proc/sys/net/ipv4/ip_forward	
Deaktivieren des Routings:	
echo "0" > /proc/sys/net/ipv4/ip_forward	
Anzeigen, ob Routing aktiviert wurde (0=nein/1=ja):	
cat /proc/sys/net/ipv4/ip_forward	
Weitere wichtige Optionen für den Befehl route:	
metric [METRIK]	Mit der Metrik werden die "Kosten" der Strecke festgelegt. Je höher die Metrik, umso weniger "gern" wird diese Strecke (route) genutzt.
mss [MAXSIZE]	Die maximale Fragmentgröße (Paketgröße) - wird eventuell benötigt zwischen unterschiedlichen Topologien/Medien. Dies ist auch für einige (schlechte) Firewalls eventuell notwendig.
ACHTUNG! Jegliche Information, die Sie mit diesen Tools setzen, wird nach einem Reboot nicht mehr zur Verfügung stehen! Daher müssen diese in ein Startskript (siehe Shellprogrammierung)	
SuSE-Konfigurationsfiles	/etc/sysconfig/network/ifcfg....

Wichtige Tools, die man kennen sollte

ping	Testen der Erreichbarkeit
-c [Anzahl]	(count) Anzahl der Pings
-n	(nummerisch) Keine Namensauflösung
traceroute -n	Weg eines Pakets - im Internet meist sinnlos, da keine Rückantwort (*) kommt. (-n ohne Namensauflösung)
tcpdump -i [NIC]	Ist ein sehr spärlicher Netzwerksniffer.
ssh	SSL verschlüsselter Remotezugang
scp [user1]@[host1]:[absPfad] [user2]@[host2]:[absPfad]	
	verschlüsseltes Remotekopieren (siehe shell)

Namensauflösung (nslookup / dig)

Achtung! nslookup wird durch dig abgelöst!	
nslookup	Öffnet nslookup interaktiv und konnektiert an den im System angegebenen Nameserver
set q=[TYP]	(siehe Ressource Records)
server [IP/NAME]	Diesen Server befragen
dig -t [TYP] @[NServer]	Den Server NServer nach dem Ressource Record TYP befragen.

Ressource Records (TYP) für nslookup und dig

SOA	Verwaltungsinfos
A	Adresseintrag (NAME -> IP)
NS	Nameserver
CNAME	Aliasnamen
PTR	Adresseintrag (IP -> NAME)
MX	MaileXchanger - Mailserver
HINFO	Hostinfos (falls gesetzt)
TXT	Kommentare
ALL	(fast) alles - (QueryType - aber eigentlich KEIN Ressource Record)

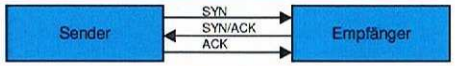
Anzeige Netzwerkrelevanter Infos (netstat) (ausführlich -v)

netstat -s	Statistische Protokollinformationen
netstat -c	Fortlaufende Anzeige
netstat -l	Empfangsbereite Sockets
netstat -a	Sende- und Empfangssckets
netstat -p	Mit Programmen

TCP-Header

1. Byte	2. Byte
Source Port (Dienstkennung)	
Destination Port (Dienstkennung)	
Sequenz Nummer (4 Byte)	
Sequenz Nummer (4 Byte)	
Acknowledge Nummer (4 Byte)	
Acknowledge Nummer (4 Byte)	
Daten Offset	Reserviert (6 Bit) | Flags (6 Bit)
Window (Puffergröße des Empfängers)	
Checksumme (Prüfsumme Header UND Daten)	
Urgent Pointer (Zeigt auf "vorrangig zu bearbeitende Daten")	
Options (Immer 32 Bit-Vielfaches)	
Options + Padding ("Füllung")	
Dateninhalt	

Erfolgreiche TCP-Verbindung (3-way-handshake)



TCP-Flags:	
URG	1 = Urgent Pointer-Feld muß gelesen werden („vorrangig" zu bearbeitende Daten)
ACK	1 = Acknowledge Number-Feld muß gelesen werden
PSH	1 = Daten müssen unverzüglich an den entsprechenden Dienst weitergeleitet werden
RST	1 = Verbindung soll beendet werden
SYN	1 = Verbindung soll aufgebaut werden
FIN	1 = Zeigt endgültigen Verbindungsabbau

netcat / nc

netcat, bzw. nc ermöglicht die Kommunikation mit einer tcp- oder udp-Verbindung über stdin/out, beispielsweise aus einem Shellscript heraus.
Abfrage von Klartextprotokollen (Beispiel für HTTP)
printf 'GET / HTTP/1.0\r\n\r\n' | netcat -w [TIMEOUT] [SERVER] [PORT]
Umleiten von lokalen Ports auf Remoterechner (siehe auch rinetd)
Eintrag in /etc/inetd.conf (Port <-> Programmzuordnung!): [L-Port] stream tcp nowait [User] nc nc -w 5 [R-host] [R-port]
Mit netcat / nc lassen sich Shellprogramme als Daemon nutzen. netcat muss mit der Option (-DGAPING_SECURITY_HOLE compiliert sein.
nc -l -p [PORT] -e [Pfad zu einem Shellskript]

Ihre Zusätze

Gängige TCP-Ports

(TCP) 20	Datenkanal FileTransferProtocol (FTP)
(TCP) 21	Kontrollkanal FileTransferProtocol (FTP)
(TCP) 22	Secure Login
(TCP) 23	telnet
(TCP) 25	Simple Mail Transfer Protocol (SMTP)
(TCP/UDP) 53	DomainNameService (DNS)
(TCP) 80	HyperTextTransferProtocol (HTTP)
(TCP) 110	PostOfficeProtocol 3 (POP3)
(TCP) 443	https
Die bekannten Dienst / Port - Zuordnung finden sich in /etc/services	