



Netzwerkgrundlagen für CTF-Player





Agenda

- Grundlagen
 - TCP/IP / OSI-Layer
 - Netzdesign
 - Routing + Firewalls
 - Troubleshooting
- Workshop
 - Applied Grundlagen ;)





End System A



End System B

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data Link layer
Physical layer

Application-specific protocols
Data representation formats
Dialog control
End-to-end data transport
Routing
Next-neighbor error and flow control
Physical data transfer

7
6
5
4
3
2
1

Physical link





Funktionsaufruf durch den Anwender	AH + Daten	7 Application
Umwandlung der Daten ein eigenes Format	PH + AH + Daten	6 Presentation
Verbindungen zwischen den Endsystemen	SH + PH + AH + Daten	5 Session
Datenpaket wird einer Anwendung zugeordnet	TH + SH + PH + AH + Daten	4 Transport
Erstmalige logische Adressierung der Endgeräte	IH + TH + SH + PH + AH + Daten	3 Network
Physikalische Adressierung mit Fehlererkennung, Fehlerbehebung und Datenflusskontrolle	DH + IH + TH + SH + PH + AH + Daten	2 Data Link
Definition der elektrischen, mechanischen und funktionalen Schnittstelle zum Übertragungsmedium	PhH + DH + IH + TH + SH + PH + AH + Bits	1 Physical





- MAC-Adresse: 00:50:56:C0:00:01
- Eindeutige Adresse einer Netzwerkkarte
- Ablauf wenn A mit B kommunizieren will:
 - A schreit an alle: Hey, wer ist B?
 - Nur B antwortet: Hier ich, meine MAC-Adresse ist DE:AD:BE:EF:00:00





- IP-Adresse: 192.168.42.1
 - Private IP-Adressen (RFC 1918)
 - 10.0.0.0/8
 - 192.168.0.0/16
 - 172.16.0.0/23
 - Öffentliche IP-Adresse
- Netzbereiche: 192.168.42.0/24
- Subnetzmasken: 192.168.42.0 255.255.255.0





- Übersetzt Namen in IP-Adressen
 - hlab.informatik.uni-mannheim.de => 134.155.88.197





- Transmission Control Protocol
 - Das Protokoll das normalerweise für Verbindungen benutzt wird
 - “Verwaltungsoverhead”
 - Ports: 1-65535





- User Datagram Protocol
 - Verbindungslos
 - Keine Garantie, dass ein Paket auch ankommt
 - Ports: 1-65535





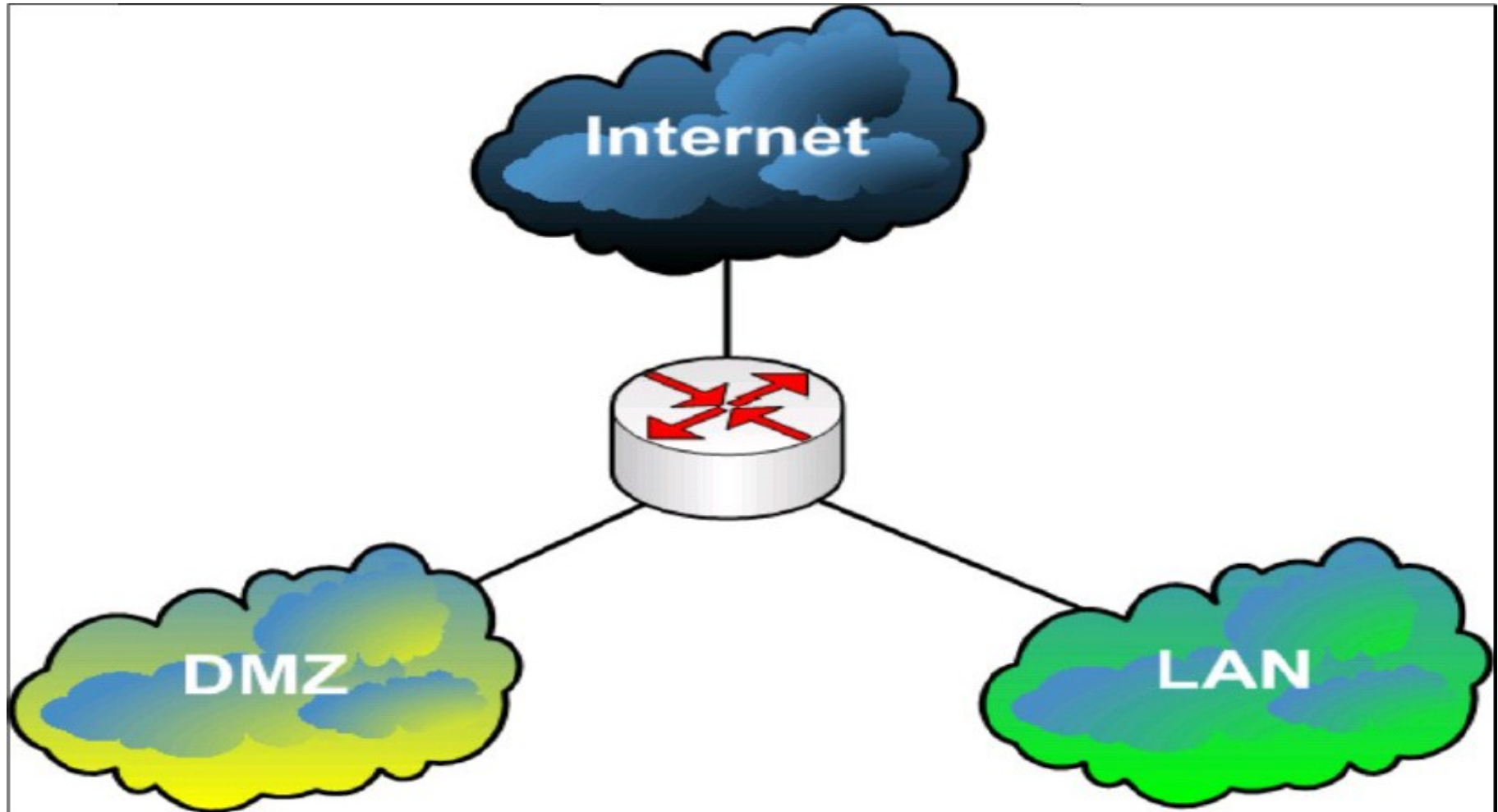
Listening Ports

- Damit eine Netzwerkverbindung zustande kommen kann, muss es sogenannte Listening Ports geben
- D.h. ein TCP- oder UDP-Port wird “abgehört”
- An diesen Port können Kommunikationspartner Netzwerkpakete senden die angenommen und verarbeitet werden.
- Pakete an geschlossene, also nicht abgehörte Ports werden einfach ignoriert.





Netzwerkdesign





- DMZ: 10.10.10.0/24, LAN: 192.168.42.0/24
- Zwei verschiedene Netzadressen
- Wir haben gelernt: Die 192.168.42.x Adressen “sehen” nur andere 192.168.42.x Adressen
- Daher muss jemand “routen”
- => Der Router ;-)





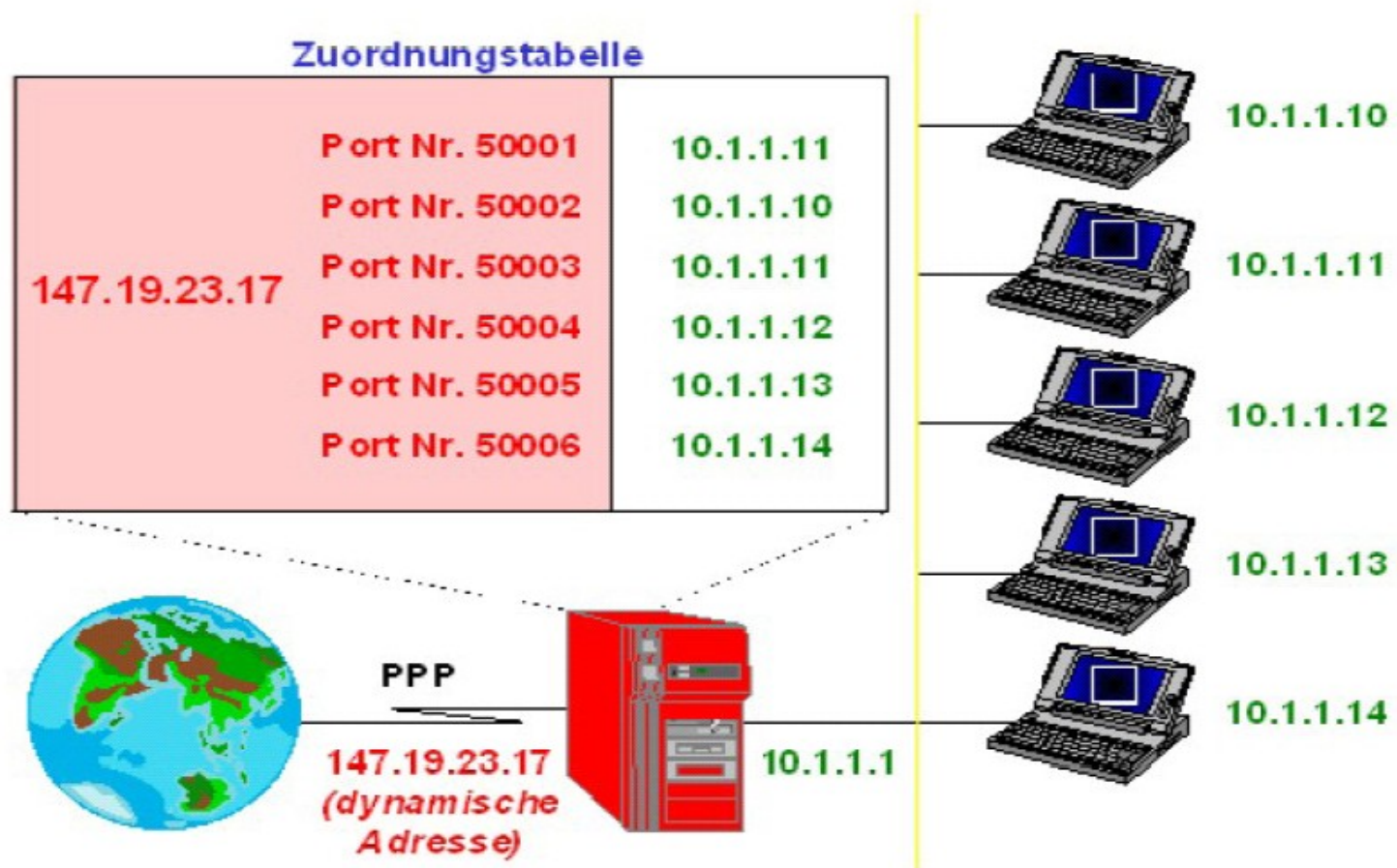
Firewall

- Router mit “mehr Intelligenz”
- Einzelne Ports können gesperrt werden
- Einzelne IP-Adressen können gesperrt werden
- IP-Bereiche können gesperrt werden





NAT





Troubleshooting

- Um ein Netzwerk zu testen, benötigen wir verschiedene Werkzeuge
- Diese werden hier vorgestellt, allerdings nur kurz mit den wichtigsten Fakten
- Quellen zu weiterführenden Informationen werden angegeben





- Ping
 - simpler Erreichbarkeitstest
 - Man ping / ping /?
- route
 - Gibt Routingtabelle aus
 - man route / route /?
- Ifconfig / ipconfig





- traceroute / tracert
 - Ermittelt “Pfad” zu anderen Rechnern
 - man traceroute / tracert /?
- netstat
 - Gibt offene Netzwerkverbindungen aus
 - man netstat / netstat /?





- netcat / nc
 - “Swiss army knife of TCP/IP”
 - Einfachster Aufbau von Verbindungen / Listening Ports
 - man nc
 - Anwendungsbeispiele:
<http://www.jfranken.de/homepages/johannes/vortraege/netcat.de.html>





- Openssh
 - Secure SHell Client
 - Remote Zugriff auf Systeme
 - Sogenannte Port-Forwardings möglich
 - man ssh
 - ssh-forwarding:
http://www.ssh.com/support/documentation/online/ssh/adminguide/32/Port_Forwarding.html





- tcpdump
 - Sämtlicher Netzwerkverkehr wird ausgegeben
 - Es kann nach bestimmten Kriterien gefiltert werden
 - man tcpdump
 - Einfacher Überblick:
 - <http://highgames.com/?set?hardwareview&view=6>





- nmap
 - Portscanner
 - Ermittelt Listening Ports auf entfernten Rechnern
 - man nmap

