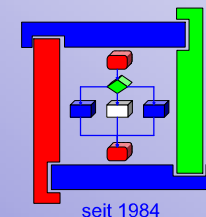


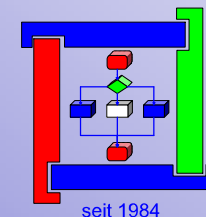
# THEMA

“Verbesserung des Quality of Service  
und der Sicherheitsaspekte beim  
Einsatz von heterogenen  
Netzwerken“



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# Einführung

Die verschiedenen neuen Technologien und Techniken in der IT-Branche haben zu einer starken Veränderung der Kommunikationsstrukturen geführt. Sowohl die Art und Weise der Kommunikation als auch die Form der Kommunikation wurden weiterentwickelt.

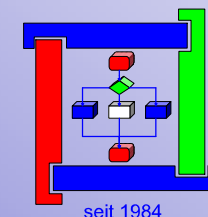
Eine schnelle Informationsbeschaffung aktueller Informationen in höchster Qualität wird für Entscheidungsprozesse immer bedeutsamer. Gänzlich neue Berufsfelder ergeben sich daraus.

Durch Netzwerke LANs und WANs, wie das Internet, können diese Möglichkeiten / Dienste auf globaler Ebene angeboten werden.

Einführung (neue Formen der Kommunikation)

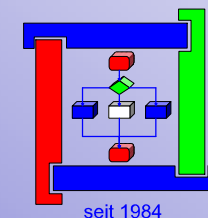
3 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- **Historische Betrachtungen**
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# Historie

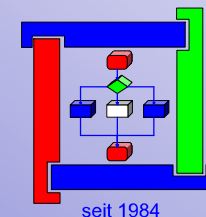
Die Entwicklungen seit den Anfängen 1962 Rand Corporation bis zu heutig existierenden Netzwerkstrukturen.

- 1969 ARPA (Advanced Research Projects Agency)
- Die TCP/IP-Protokolle (1973) wurden 1983 als militärische Standards (MIL STD) übernommen
- 1986 weniger als 6000 Rechner im „Internet“
- 1991 mehr als 600.000 Rechner im „Internet“
- 1995 ca. 60 Mio. Rechner im „Internet“
- 2000 ca. 300 Mio. User im „Internet“ weltweit
- Dieses explosionsartige Wachstum verdeutlicht den enormen Bedarf an Netzwerkdiensten.

## Historische Betrachtungen

### 5 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Zielsetzungen der Rand Corporation

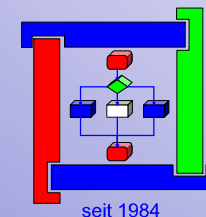
Entwicklung eines Systems, welches die folgenden Kriterien erfüllen soll:

- Hardware- und Betriebssystem-unabhängig
- dezentrale Verwaltung
- redundante Übertragungswege
- übergreifende Dienste (email, ftp, telnet)
- selbstkonfigurierend
- paketvermittelnd

Historische Betrachtungen

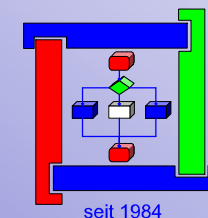
6 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- **Begriffsdefinitionen**
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# LAN / MAN

## **LAN**

Local Area Network,

lokales Netzwerk, welches von der Ausdehnung her auf eine Grundstücksgrenze beschränkt ist.

Meist wird in LANs nur eine Architektur verwendet (z.B. Ethernet).

## **MAN**

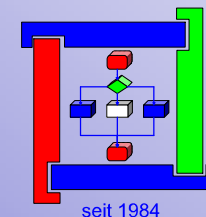
Metropolitan Area Network,

Netzwerk, welches von der Ausdehnung her auf eine Stadt begrenzt ist. Charakteristisch ist die Verwendung eines Backbones zur Verbindung mehrerer Gebäude (Campus-Netzwerk).

## Begriffsdefinitionen

8 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



seit 1984



# WAN

## **WAN**

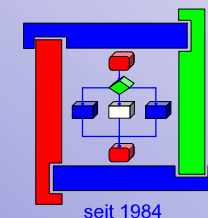
Wide Area Network,

Ein Netzwerk, welches sich über Landesgrenzen hinweg ausdehnt und öffentliche Leitungen zur Verbindung der verschiedenen Teilnetzwerke verwendet. Es verbindet international oder global meist unter Einsatz der TCP/IP-Technologien.

Begriffsdefinitionen

9 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Internet / Intranet

## ***Internet***

Das Internet ist derzeit der weltweit größte Netzverbund, der jedem Teilnehmer eine nahezu grenzenlose Informations- und Kommunikationsinfrastruktur zur Verfügung stellt.

## ***Intranet***

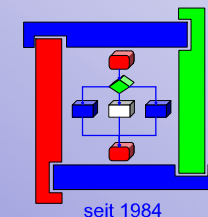
Firmenbezogenes Netzwerk, welches TCP/IP-Technologien verwendet, aber nur für eine geschlossene Benutzergruppe zur Verfügung steht.

---

## Begriffsdefinitionen

10 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Verschiedene Netzwerktypen

## Server basierte Netzwerke

- Client-Server: ein besonders zuverlässiges Gerät (Server, Dienstgeber) stellt seine speziellen Fähigkeiten in Form von Diensten oder Services (Zugriff auf Massenspeicher, Peripheriegeräte) der Allgemeinheit (Client-Stationen, Dienstenehmer) zur Verfügung.

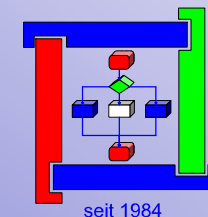
## Peer-to-Peer Netzwerke

- Jede Arbeitsstation (PC) kann sowohl Server- als auch Client-Funktionen übernehmen. Sie kann in dem Netz nicht nur als Empfänger, sondern auch als Sender von Daten für die restlichen Teilnehmer fungieren.

## Begriffsdefinitionen

11 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



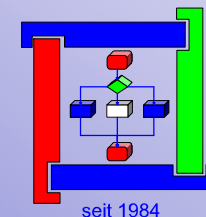
# Protokoll

Ein **Protokoll** ist die Summe aller Regeln, die zum Datenaustausch zwischen zwei Kommunikationspartnern eingehalten werden müssen.

Begriffsdefinitionen

12 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Aufgaben von Protokollen

## Protokolle haben folgende Aufgaben:

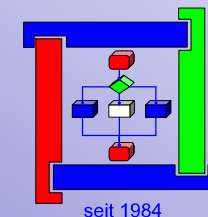
- Reihenfolge
- Adressierung
- Fehlererkennung und -korrektur
- Synchronisation

Wir unterscheiden zwischen ***paketvermittelnden*** und ***leitungsvermittelnden*** Netzwerken.

## Begriffsdefinitionen

13 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



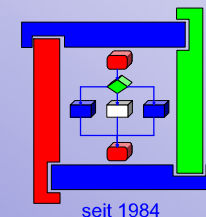
# Merkmale von TCP/IP

- offener Protokollstandard, frei verfügbar, hardware- und betriebssystem-unabhängig
- unabhängig von physikalischer Netzwerk-Hardware
- einheitliches Adressierungsschema, selbst bei extrem großen Netzwerken (Internet) ist der Zugriff auf Hosts eineindeutig möglich
- zum Teil selbstkonfigurierend
- standardisierte High-Level-Protokolle für konsistente, weit verbreitete Benutzerdienste (email, ftp, telnet).

## Begriffsdefinitionen

14 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Adressierung

## Adressierung

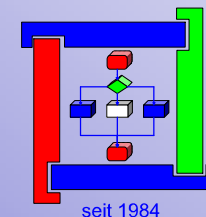
IP-Adressen (Internet-Adressen), die jeden Host im Netzwerk eindeutig kennzeichnen, sorgen für die Zustellung der Daten an den richtigen Host (4 Byte groß).

IP-Adressen sind gegenüber den **physikalischen** Hardware-Adressen von Netzwerkkarten **logische** Adressen.

Begriffsdefinitionen

15 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Adressierung

*Eine IP-Adresse besteht aus einem:*

- *Netzwerkteil*
- *Hostteil*

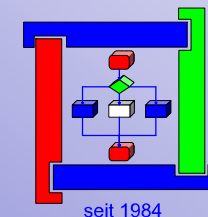
Allerdings ist das Format dieser beiden Teile ist nicht immer gleich. Die Anzahl der zur Identifikation des Netzwerks verwendeten Adreßbits und die Anzahl der Kennzeichnung des Hosts verwendeten Bits hängen vom Längenpräfix der Adresse ab.

---

Begriffsdefinitionen

16 Vorlesung - FHDW

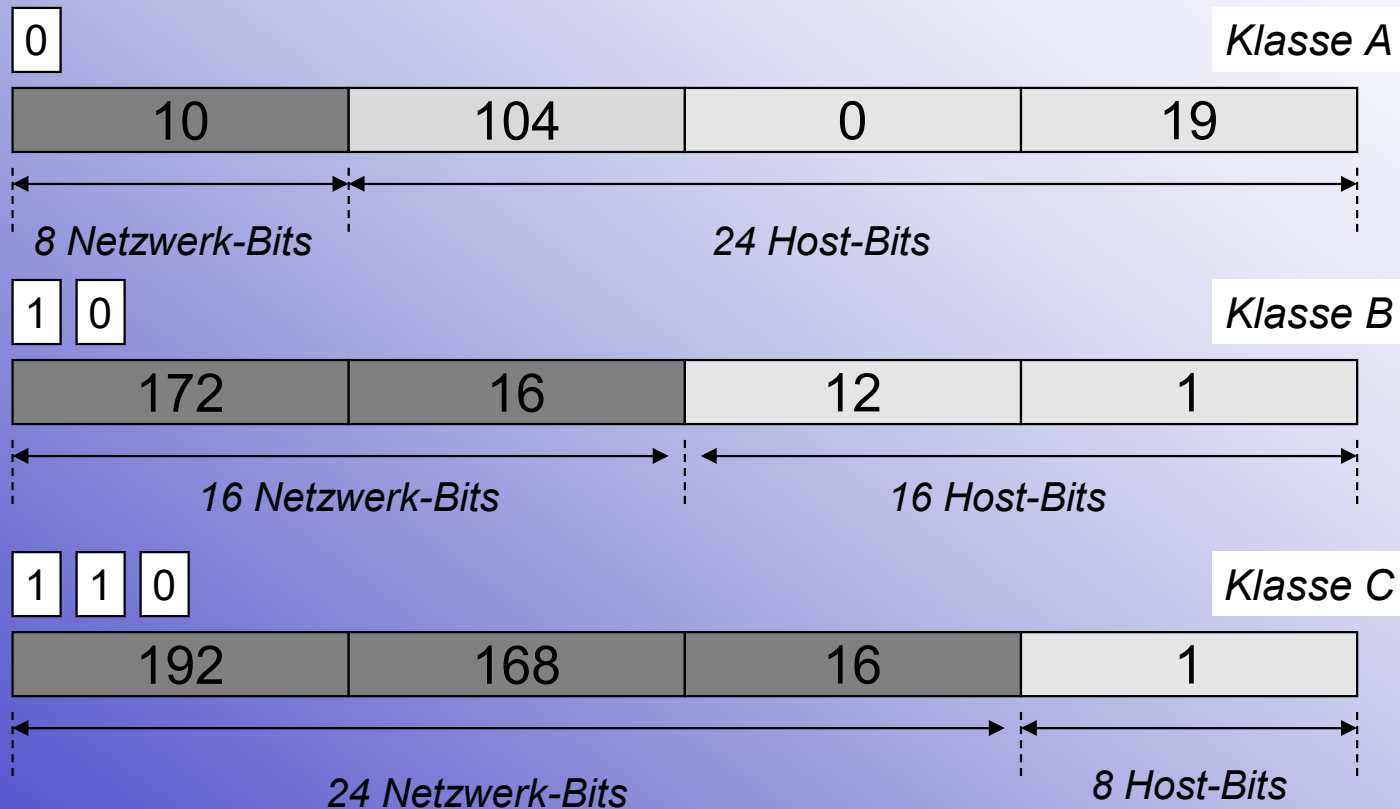
© Dr. G. Hellberg August 2000





# Adressierung

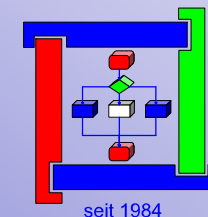
## Die Struktur von IP-Adressen



## Begriffsdefinitionen

17 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



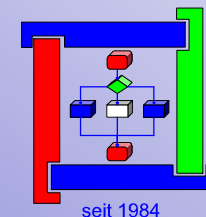
# ISO / OSI - Referenzmodell

ISO-OSI	Benutzer	NetWare	TCP/IP-Protokolle	DOD-Modell		
7 Anwendung	Programme Betriebs- systeme	Betriebs- systeme Anwender- programme und Utilities	FTP	HTTP	Telnet	Prozeß / Anwendung
6 Darstellung			SMTP	NFS	Andere	
5 Kommunikations- steuerung			<b>TCP / UDP</b>			
4 Transport	Logische Verbindung (Adressierung)	IPX und SPX				ICMP
3 Vermittlung			physikalischer Transport und Kontrolle	Ethernet Arcnet Token Ring	IP	BOOTP
2 Sicherung	Ethernet				Token Ring	
1 Bitübertragung	FDDI			Andere		

## Begriffsdefinitionen

18 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Kopplungselemente

**Kopplungselemente** sind Einheiten zur Verbindung von physikalischen Netzwerksegmenten. Es können vier verschiedene Haupttypen unterschieden werden.

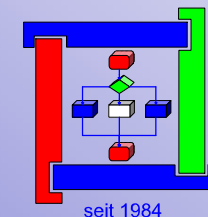
- ④ **Gateway** = Protokollumsetzung (TCP/IP, IPX/SPX)
- ③ **Router** = verschiedene Architekturen, aber gleiches Protokoll
- ② **Bridge** = Filter, bildet Kollisionsdomänen aus
- ① **Repeater** = Signalverstärker (Nutz- und Störsignal)

---

## Begriffsdefinitionen

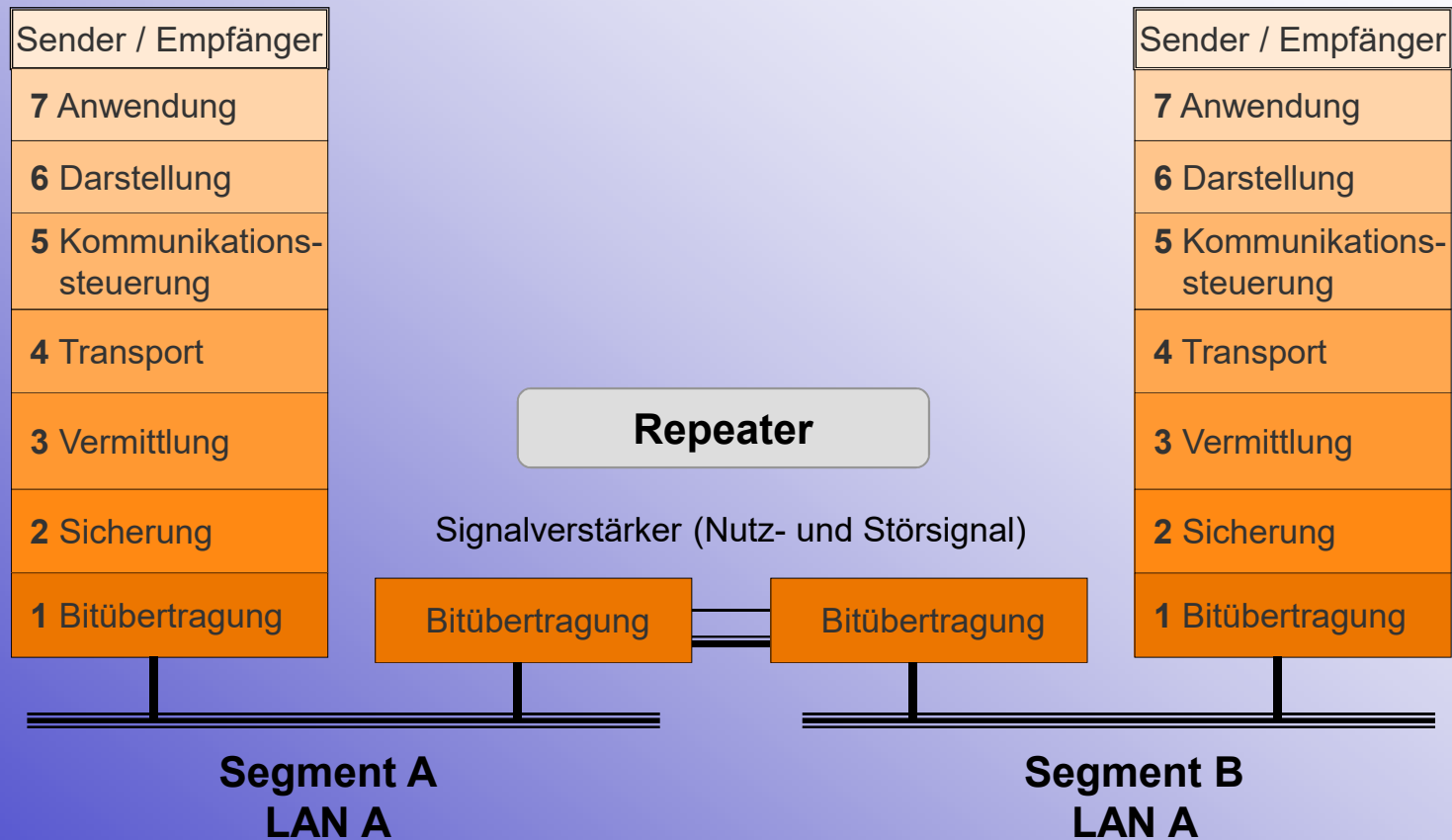
19 Vorlesung - FHDW

© Dr. G. Hellberg August 2000

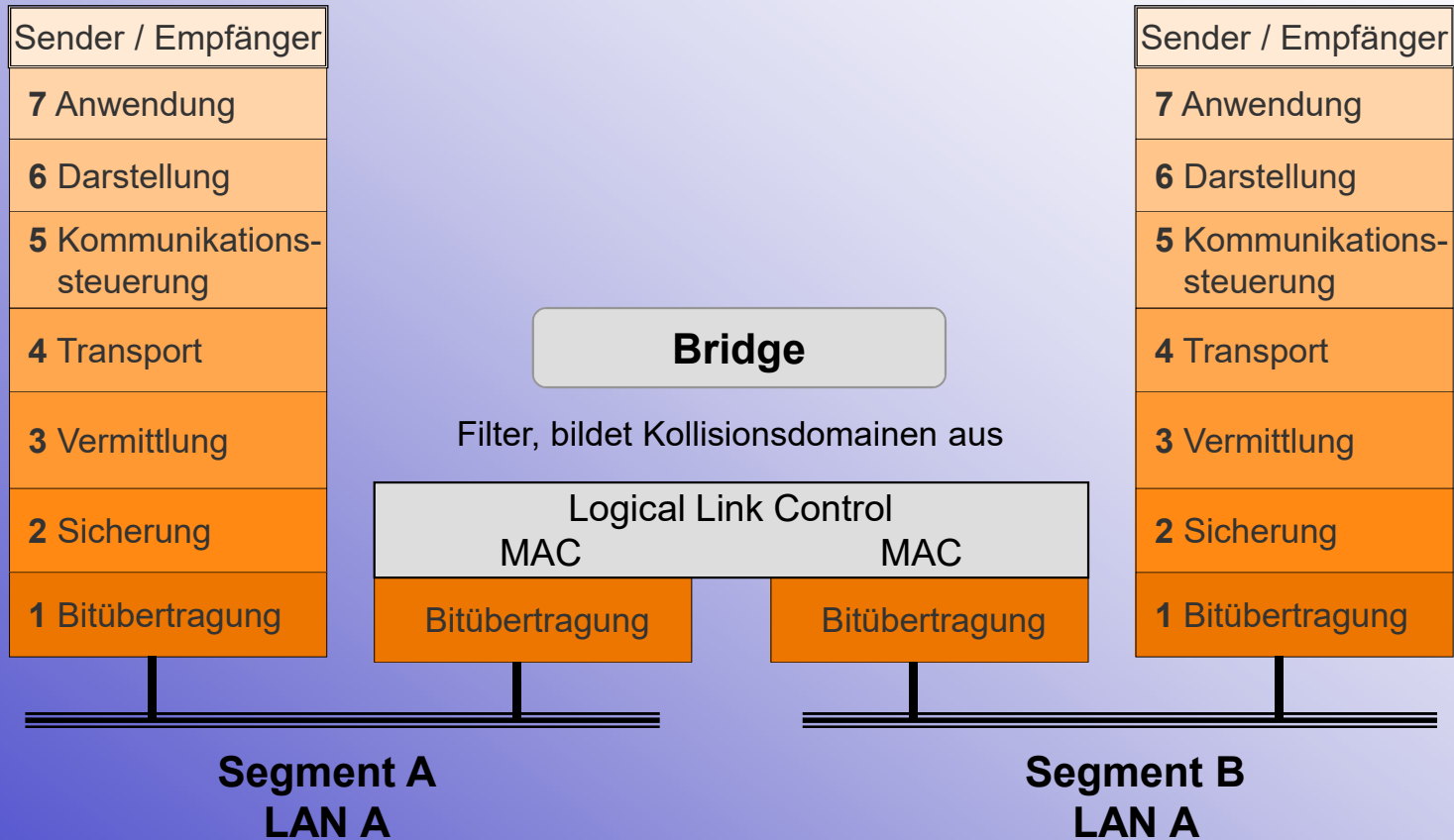


seit 1984

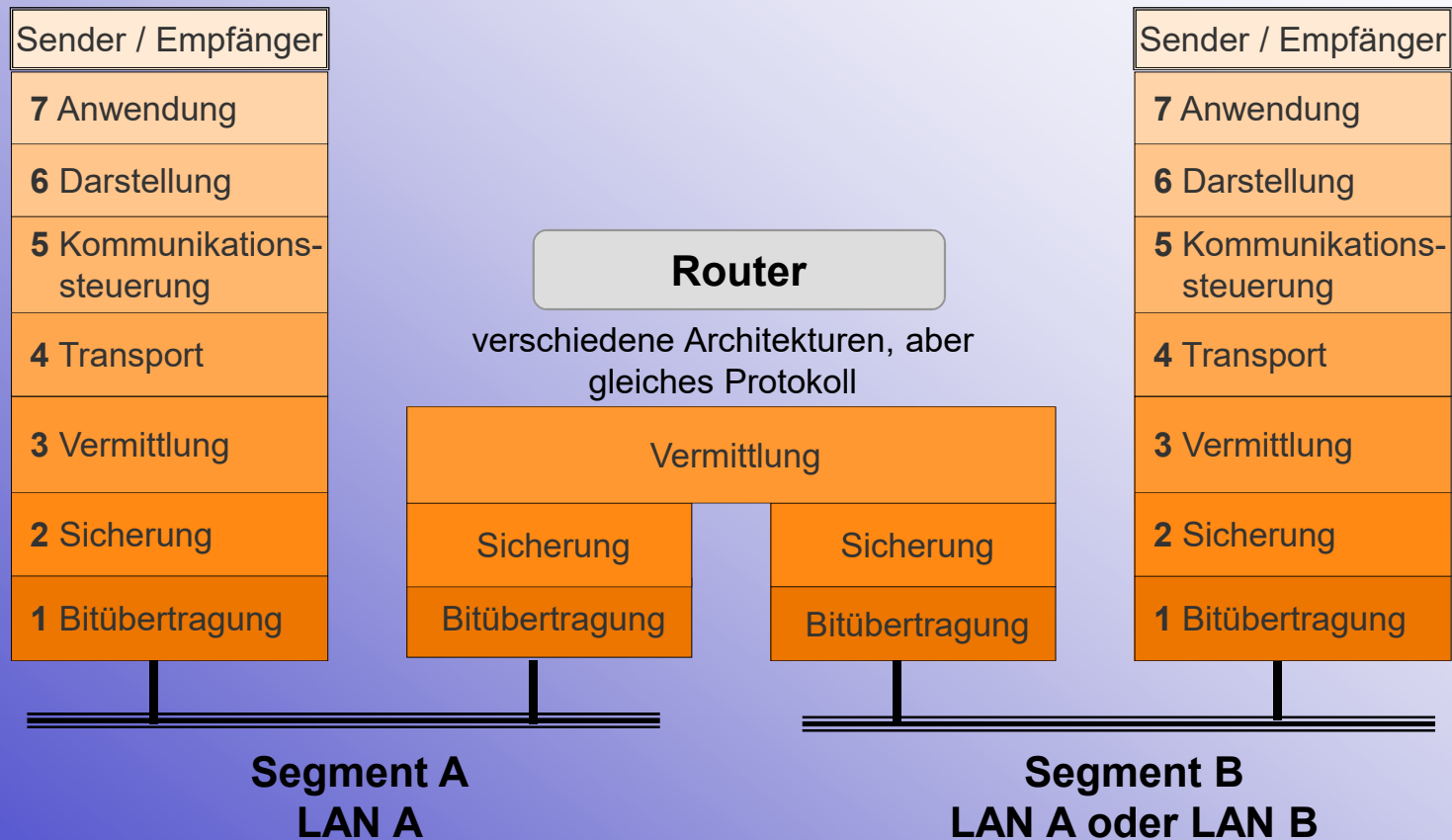
# Repeater im OSI-Modell



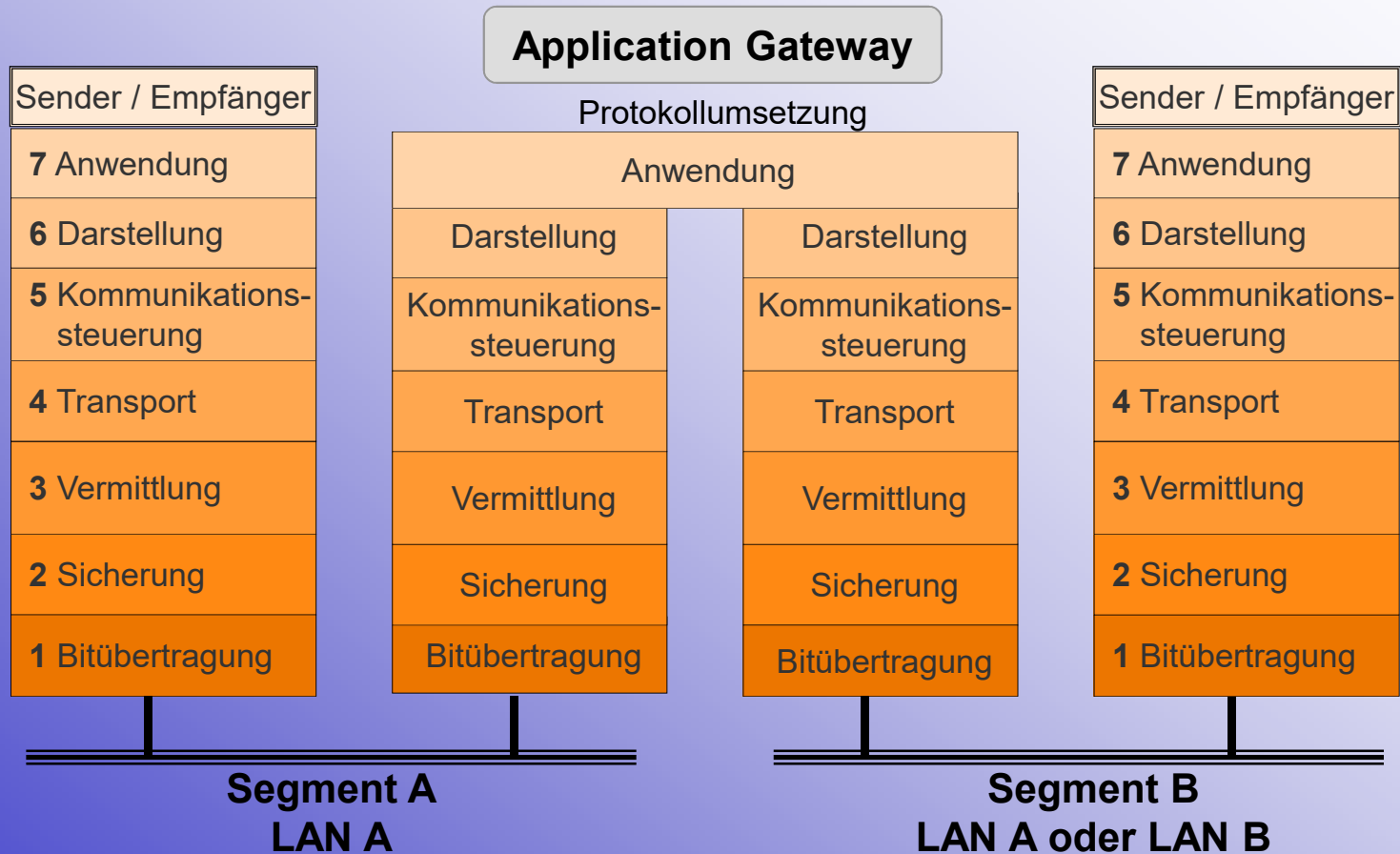
# Bridge im OSI-Modell



# Router im OSI-Modell



# Gateway im OSI-Modell



# Router und Routing

**Router** und **Routing-Protokolle**, dienen der dynamischen Suche nach geeigneten Wegen im Internet. Sie sind grundlegend für den Betrieb von TCP/IP.

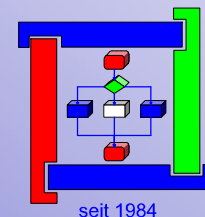
**Routing-Information** setzt zwei Routen fest: von der Quell- zur Zielmaschine und zurück.

Der Rückweg ist gewöhnlich die Umkehr des Hinwegs. Andernfalls spricht man von **asymmetrischen Routing**, welches meist aus sicherheitstechnischer Sicht bedenklich ist.

Begriffsdefinitionen

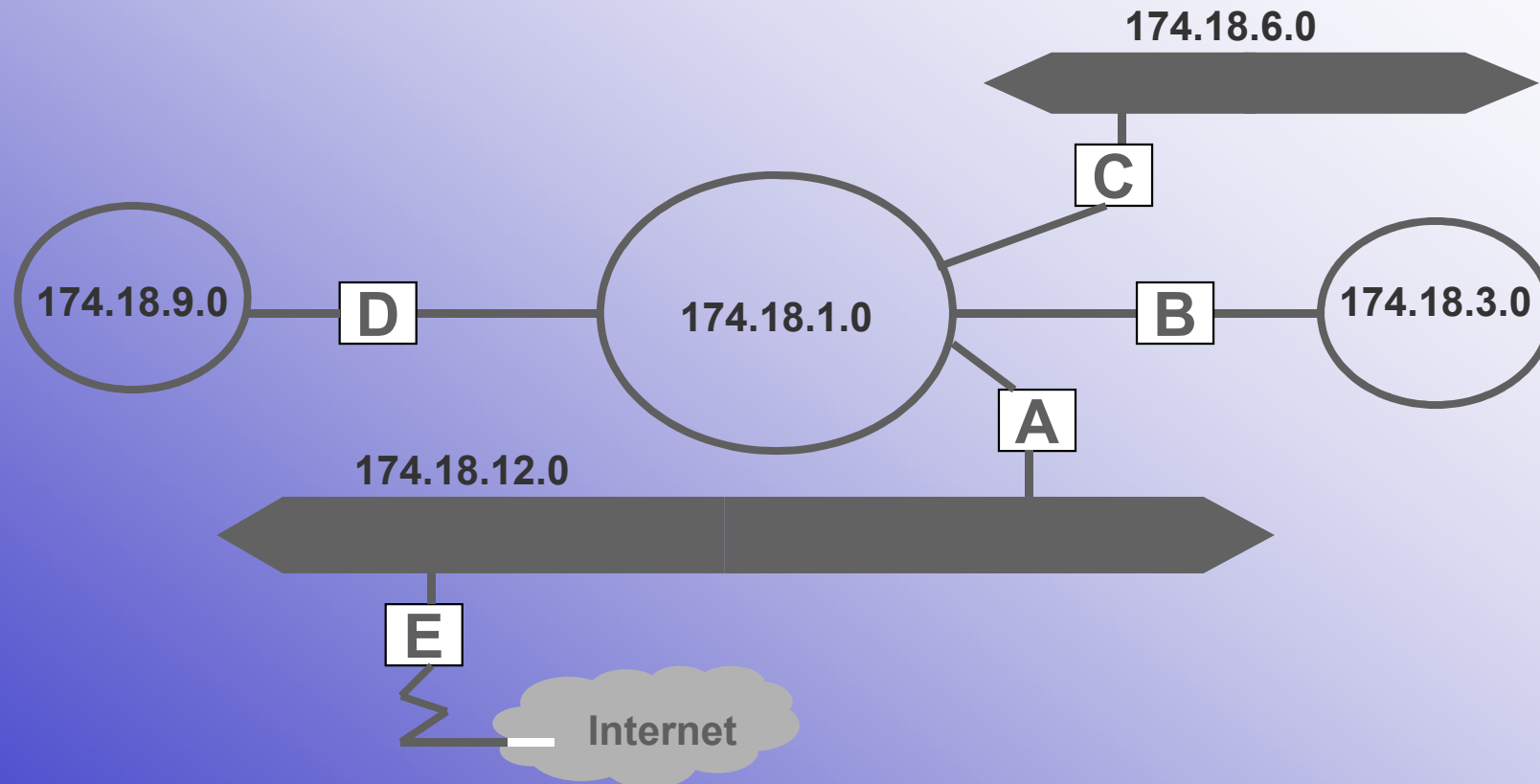
24 Vorlesung - FHDW

© Dr. G. Hellberg August 2000





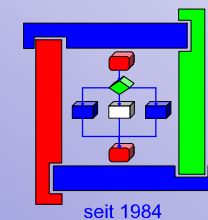
# Routing und Subnetze



Begriffsdefinitionen

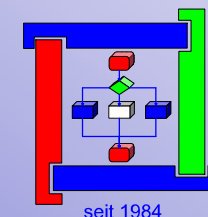
25 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



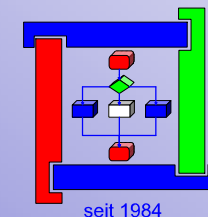
# Motivation für den Einsatz von Netzwerken

- Ausgangssituation: Ressourcen-Sharing (z.B. gemeinsame Benutzung von Druckern)
- Großrechner (Mainframes) mit „dummen Terminals“; anderes Extrem: 1981 IBM PC XT als „Insellösung“; Kombination beider Vorteile => Netzwerke
- Bedürfnis nach flexibleren Kommunikationsstrukturen

Vor- / Nachteile / Nutzen von Netzwerken

27 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



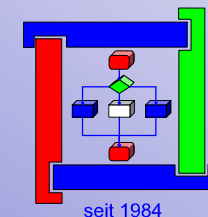
# Nachteile von Einzelplatzlösungen

- Pflege und Wartung von Programmen und Daten müssen auf mehreren Rechnern durchgeführt werden
- Datenbestände können nicht gemeinsam von mehreren Anwendern genutzt werden
- gleichzeitiges Ändern von Daten in einer Datei ist nicht möglich
- teure Peripheriegeräte müssen für jeden Rechner angeschafft werden, obwohl sie nicht optimal ausgelastet werden.

Vor- / Nachteile / Nutzen von Netzwerken

28 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



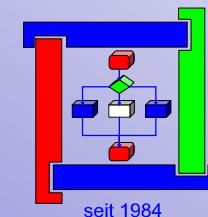
# Vorteile von Netzwerken

- Handhabung (Updates einfacher, Arbeiten mit denselben Programmversionen, automatische Backups usw.)
- Sicherheit
- Standardisierung (Formulare, Programmversionen, Daten usw.)
- geringere Kosten (Lizenzgebühren für Software, Ressourcen-Sharing wie z.B. Drucker)
- Gemeinsamer Zugriff auf Informationen (Konsistenz, Integrität und damit auch Geschwindigkeit)

Vor- / Nachteile / Nutzen von Netzwerken

29 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



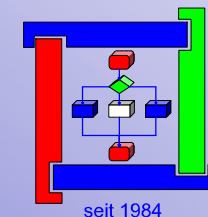
# Nachteile von Netzwerken

- Befall des Systems durch Viren (auch gesamtes Netz)
- eventuell höherer Administrationsaufwand
- höhere Anschaffungskosten
- Schwierigkeiten der Kopplung von verschiedenen Systemen
- Zugriff auf sensitive Daten durch unbefugte Benutzer
- Manipulation bzw. Zerstörung von Daten durch unbefugte Benutzer

Vor- / Nachteile / Nutzen von Netzwerken

30 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



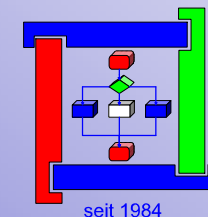
# Stellung des Netzwerkes

- Zugriff aller Benutzer auf gemeinsame Programme und Daten
  - zentrale Auftragsabwicklung
  - zentrale, konsistente Daten und Arbeitsabläufe
- Sicherheit
  - physikalisch (intelligente Plattenverwaltung)
  - zentrale, regelmäßig und automatisch erfolgende Datensicherung z.B. mittels Streamer
  - logische und programmtechnische Sicherheit durch die Verwendung von Benutzergruppen und Paßwörtern
- Anbindung an andere Betriebssysteme und Software
- Optimale Ausnutzung von Ressourcen (z.B. Drucker)

Vor- / Nachteile / Nutzen von Netzwerken

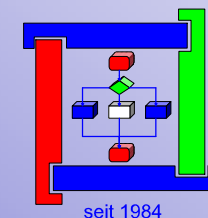
31 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- **Bereitstellung von Diensten (email, ftp, www)**
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick





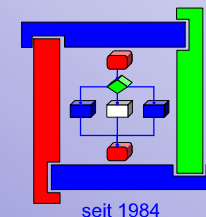
# Dienste im Internet

- Elektronische Post (Email, SMTP)
- Übertragung von Dateien (ftp)
- Terminal-Zugang (telnet) und ferne Ausführung von Kommandos
- Usenet-News
- World Wide Web (Web-Server)
- Dienste für Echtzeit-Konferenzsysteme (Video)
- Name-Service (DNS)
- Dienste zur Netzverwaltung (SNMP)
- Netzweit verteilte Dateisysteme (File-Server)
- Druckdienste (Print-Server)
- Datenbankdienste

Bereitstellung von Diensten

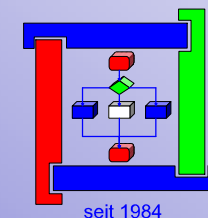
33 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- **Marktübersicht von NOS**
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# Marktübersicht von NOS

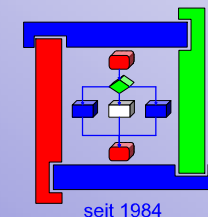
Die Merkmale der folgenden drei NOS (networking operating systems) werden beispielhaft in Kurzform dargestellt:

- Windows NT 4.0 Server
- Novell Netware 5.x
- Unix (Linux Suse 6.x)

Marktübersicht von NOS

35 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Windows NT 4.0 Server

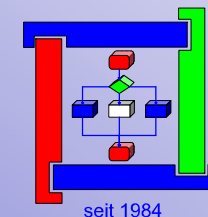
Merkmale von Windows NT 4.0 Server:

- Multiuser
- Multitasking
- Multithreading
- Multiprozessorfähig
- Domainen-Konzept
- Digital-Cluster
- GUI
- Haupteinsatzgebiet im Bereich der Applikationsserver

Marktübersicht von NOS

36 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Novell Netware 5.x

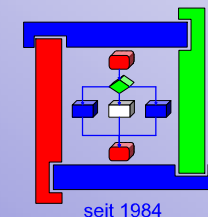
Merkmale von Novell-Netware 5.x:

- Multiuser
- Multitasking
- Multithreading
- Multiprozessorfähig
- NDS (Novell Directory Services)
- Cluster
- GUI (console-one)
- Applikationen wie z.B. Oracle, Groupwise, etc.

Marktübersicht von NOS

37 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Unix (Linux Suse 6.x)

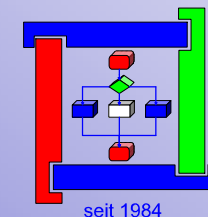
Merkmale von Unix (Linux Suse 6.x):

- Multiuser
- Multitasking
- Multithreading
- Multiprozessorfähig
- Cluster
- GUI (X-Windows, KDE)
- TCP/IP direkt implementiert
- 30 Jahre auf diversen Plattformen verfügbar
- System von Programmierern für Programmierer
- als Server- und als Client-Betriebssystem einsetzbar
- für Firewall-Systeme gut geeignet (Quellcode)

Marktübersicht von NOS

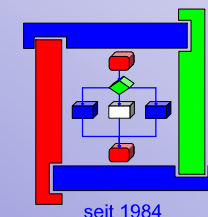
38 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# Risiken beim Einsatz von Netzwerken

Die folgenden **Aspekte** werden berücksichtigt:

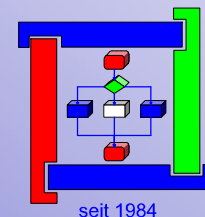
- Datensicherheit
- Datenschutz
- Viren
- Darstellung verschiedener Sicherheitskonzepte

Einige kurze Bemerkungen zu den rechtlichen Aspekten der Datenverarbeitung ergänzen die Ausführungen.

Risiken beim Einsatz von Netzwerken

40 Vorlesung - FHDW

© Dr. G. Hellberg August 2000





# Ausgangssituation zu Firewalls

Was ist eine **Firewall**, und welche Vorteile bringt sie?

Bietet die Möglichkeit der Beschränkung der Kommunikation zwischen dem Internet und dem internen Netz.

Einrichtung am effektivsten Punkt, dem Anschlußpunkt des internen Netzwerkes an das Internet.

Die Wahrscheinlichkeit, daß Angreifer von außen in Ihre internen Systeme und Netze eindringen läßt sich verringern.

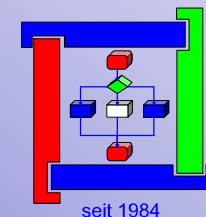
Interne Benutzer werden davon abhalten, Systeme zu gefährden, indem sie sicherheitsrelevante Informationen wie unverschlüsselte Paßwörter oder vertrauliche Daten nach außen geben.

---

Risiken beim Einsatz von Netzwerken

41 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Ausgangssituation zu Firewalls

Die **Firewall** ist jedoch nur ein Teil des Plans zur Realisierung eines Sicherheitskonzeptes.

**Was wollen Sie schützen?**

**Welche Sicherheitsphilosophie wird eingesetzt?**

Beim Anschluß an das Internet müssen drei Dinge beachtet werden:

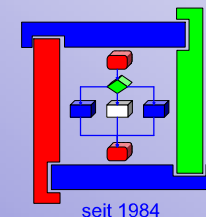
- Daten (Vertraulichkeit, Integrität, Verfügbarkeit)
- Ressourcen
- Image

---

Risiken beim Einsatz von Netzwerken

42 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Ausgangssituation zu Firewalls

## **Kosten**

Firewalls gibt es nicht umsonst, es entsteht Aufwand für:

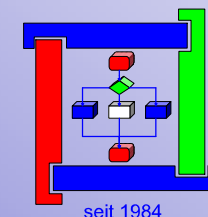
- Anschaffung und Wartung der Hardware,
- Entwicklung / Anschaffung und Wartung der Software,
- Installation und Personalschulung,
- kontinuierliche Administration und Troubleshooting,
- Geschäftseinbußen und Widrigkeiten durch blockierte Dienste oder Störungen in der Firewall,
- Verzicht auf die Dienste oder Annehmlichkeiten einer offenen Anbindung.

---

Risiken beim Einsatz von Netzwerken

43 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Ausgangssituation zu Firewalls

## **Kosten**

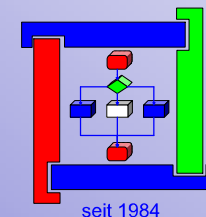
Sollte auf den Einsatz einer Firewall verzichtet werden, können folgende Kosten auftreten:

- nötige Maßnahmen zur Bekämpfung eines erfolgreichen Einbruchs und zum Wiederanlauf des Betriebs, inklusive Geschäftseinbußen,
- juristische und andere Konsequenzen wegen der Duldung oder Unterstützung von Hackern.

Risiken beim Einsatz von Netzwerken

44 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Definitionen zu Firewalls

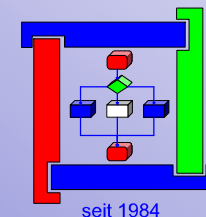
Wir definieren eine Ansammlung von Komponenten zwischen zwei Netzen kollektiv als **Firewall**, wenn folgende Bedingungen erfüllt sind:

- Jeglicher Verkehr zwischen innen und außen muß die Firewall passieren.
- Nur der im Sicherheitskonzept vorgesehene Verkehr wird durchgeschleust.
- Die Firewall selbst ist immun gegen Angriffe.

Risiken beim Einsatz von Netzwerken

45 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

## *Definition Firewall-Gateways*

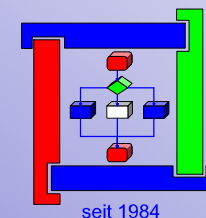
Eine **Firewall** besteht im allgemeinen aus verschiedenen Komponenten **Filter** - manchmal auch Screens genannt - schleusen nur ganz bestimmte Klassen von Verkehr durch und blockieren den anderen.

Ein **Gateway** besteht aus einer oder mehreren Maschinen, die als Relais für bestimmte, durch Filter blockierte Dienste dienen. Das Gateway-Datennetzsegment wird oft auch *demilitarisierte Zone* (DMZ) genannt. Ein Gateway in der DMZ wird häufig durch einen *internen Gateway* ergänzt.

Risiken beim Einsatz von Netzwerken

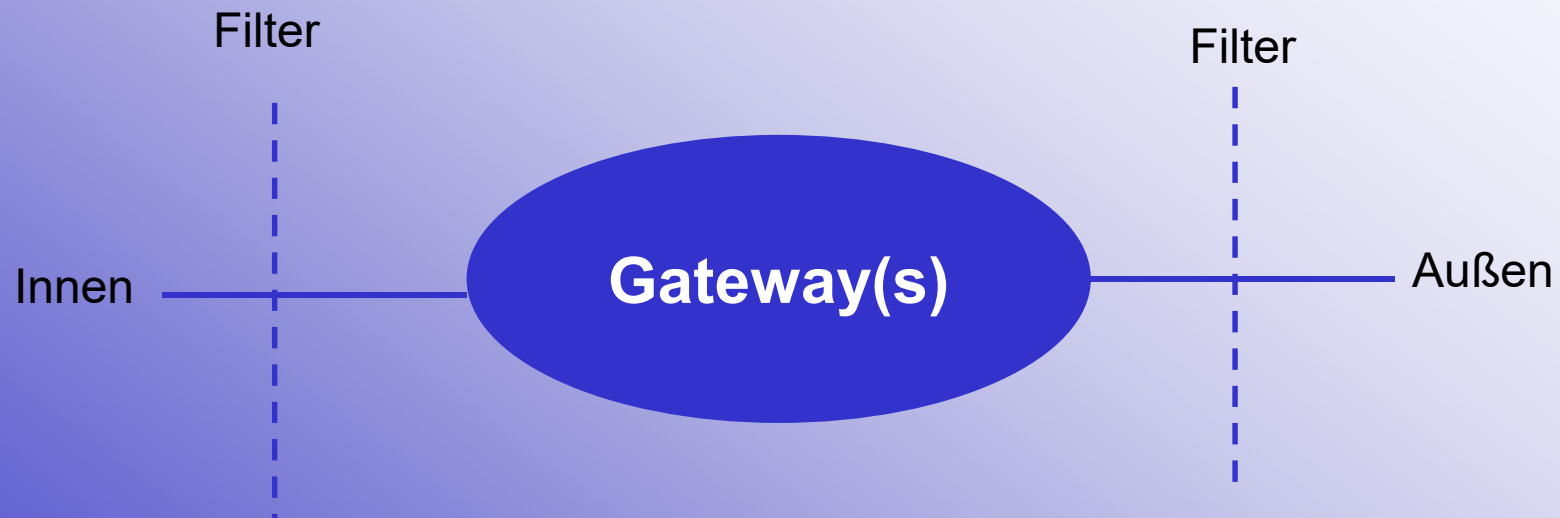
46 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

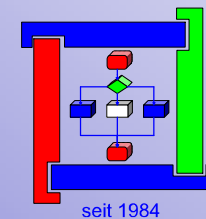
## Schema einer Firewall



Risiken beim Einsatz von Netzwerken

47 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

*Drei Hauptkategorien von Firewalls werden unterschieden:*

- Paketfilter
- Vermittler- oder Transportschicht-Gateway (circuit gateway)
- Anwendungsschicht-Gateway (application gateway)

Meist werden mehrere Typen gleichzeitig eingesetzt.

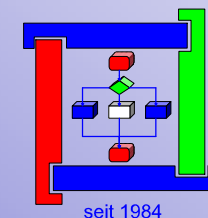
Wir werden im folgenden einige Architekturen für Firewalls betrachten.

---

Risiken beim Einsatz von Netzwerken

48 Vorlesung - FHDW

© Dr. G. Hellberg August 2000

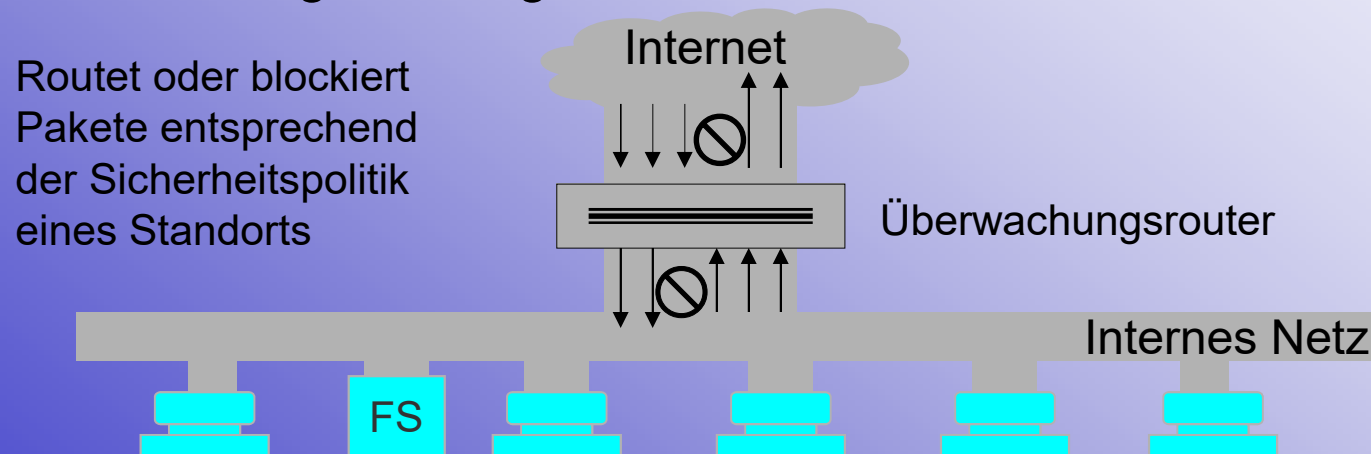




# Sicherheit

## *Paketfilterung*

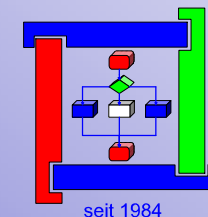
Paketfilter-Systeme routen Pakete zwischen internen und externen Rechnern, gehen dabei aber selektiv vor. Sie lassen bestimmte Pakettypen passieren oder blockieren sie auf eine Art, die die Sicherheitspolitik eines Standortes widerspiegelt. Der in einem Paketfilter-Firewall verwendete Routertyp wird Überwachungsrouter genannt.



## Risiken beim Einsatz von Netzwerken

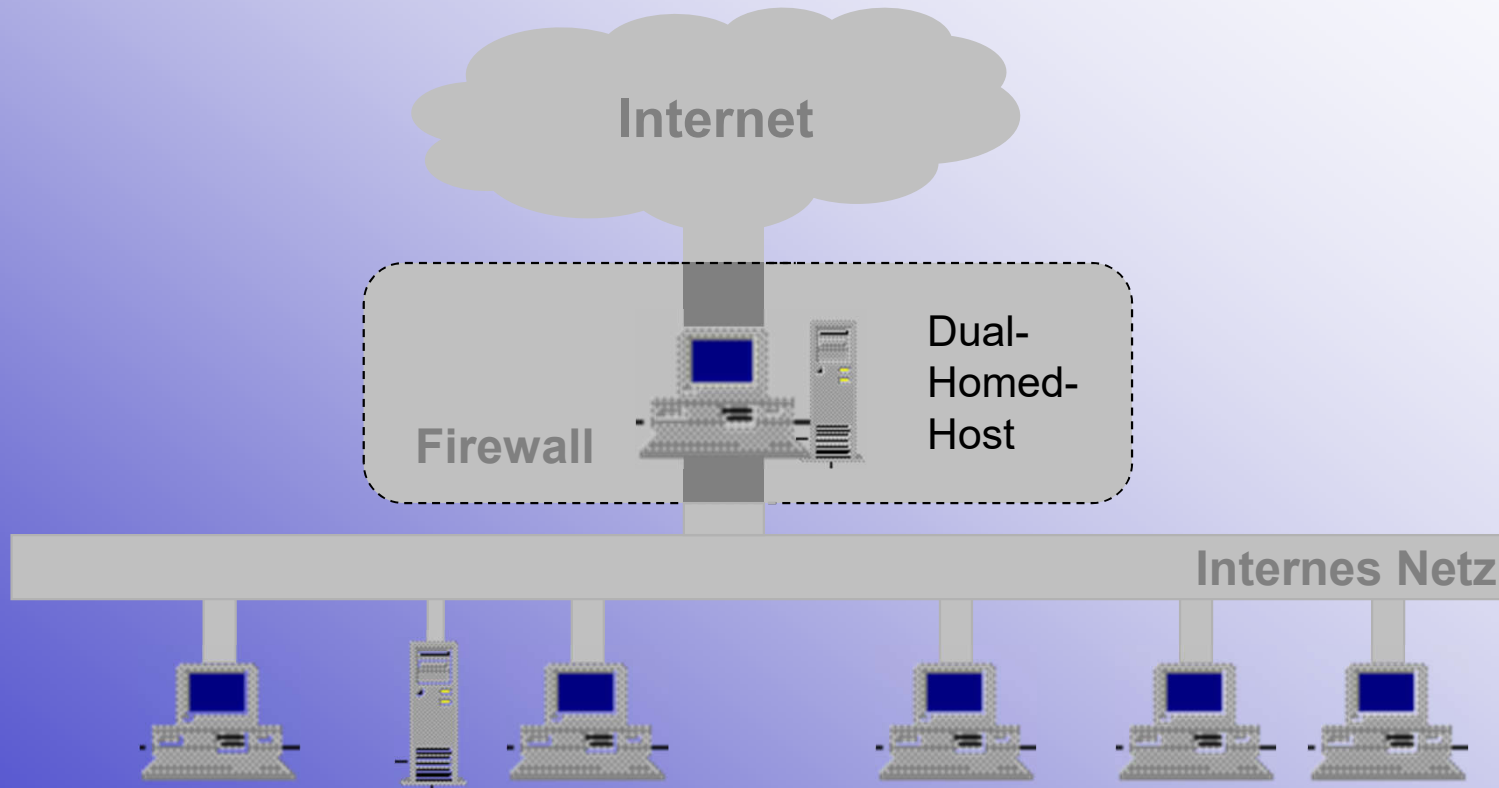
49 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

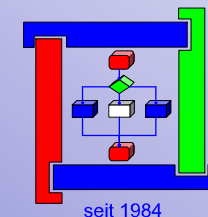
## Architektur mit Dual-Homed-Host



Risiken beim Einsatz von Netzwerken

50 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Definitionen zu Firewalls

## **Grenznetz**

Ein Netz, das zwischen ein geschütztes und ein externes Netz eingefügt wird, um eine weitere Schutzschicht zu schaffen. Ein Grenznetz wird manchmal auch DMZ genannt, das für *De-Militarisierte Zone* steht (nach einer Zone, die Nord- und Südkorea trennt).

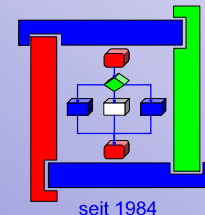
## **Proxy-Server**

Ein Programm, das stellvertretend für interne Clients mit externen Servern kommuniziert. Proxy-Clients unterhalten sich mit den Proxy-Servern, die bestätigte Client-Anfragen an die eigentlichen Server weiterleiten und die Antworten zurück an die Clients übermitteln.

## Risiken beim Einsatz von Netzwerken

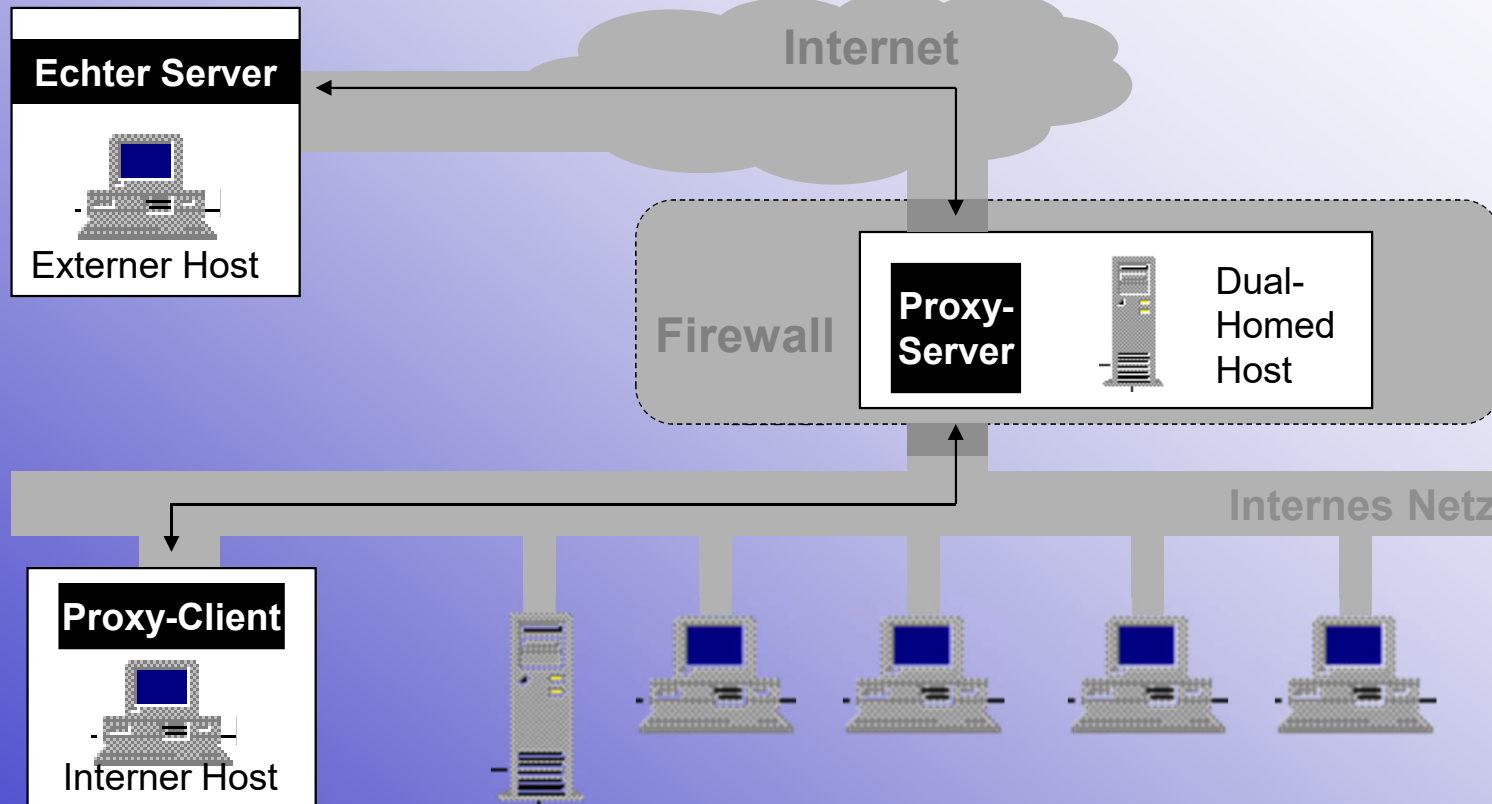
51 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

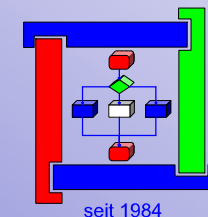
*Proxy-Dienste bei einem Dual-Homed-Host.*



Risiken beim Einsatz von Netzwerken

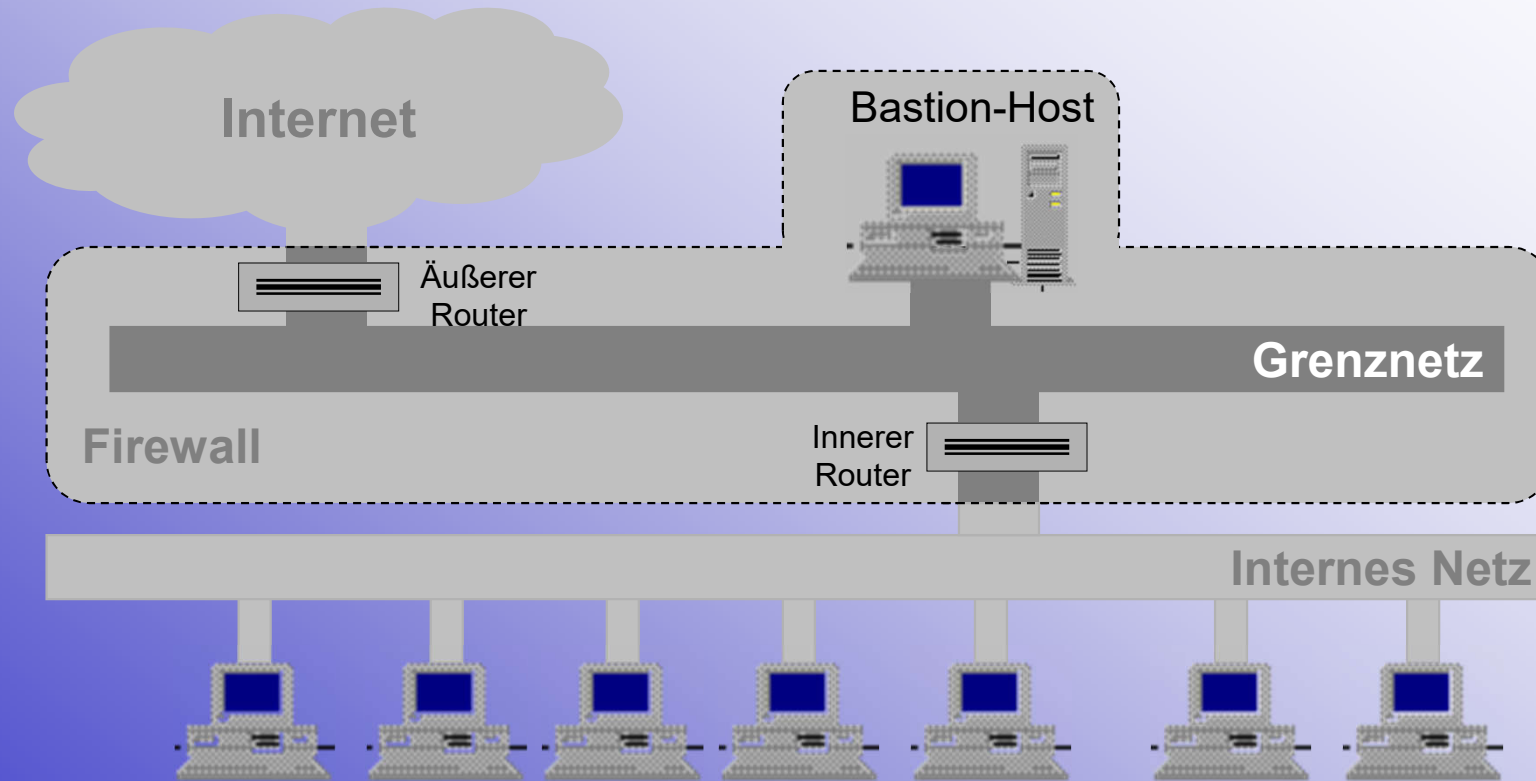
52 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

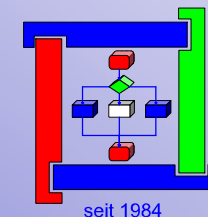
## Architektur mit überwachtem Teilnetz (und zwei Routern)



Risiken beim Einsatz von Netzwerken

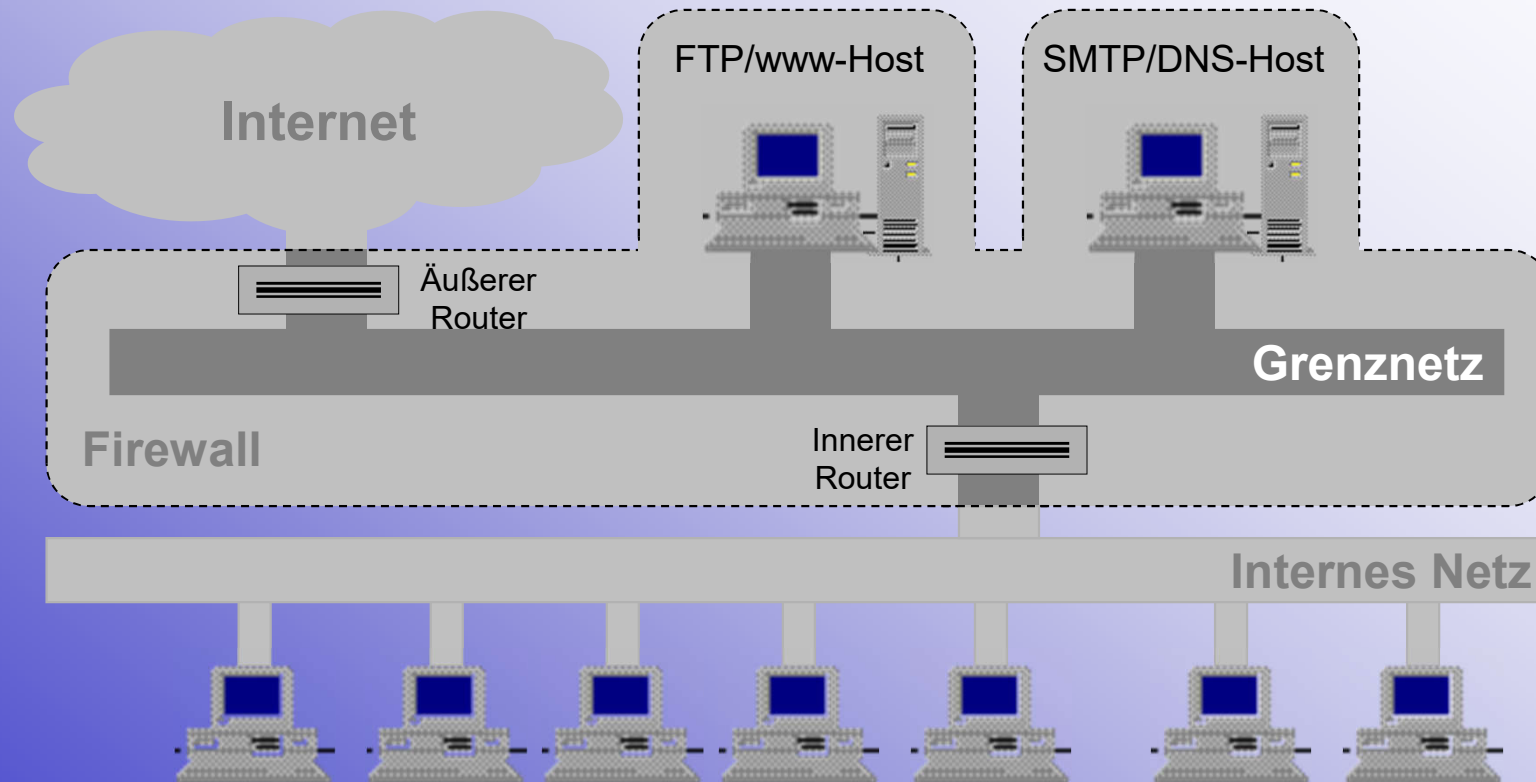
53 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

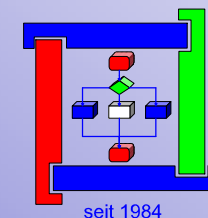
## Architektur mit zwei Bastion-Hosts



## Risiken beim Einsatz von Netzwerken

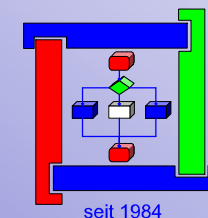
54 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- **Aktuelle Entwicklungen**
- Zusammenfassung / Ausblick



# Aktuelle Entwicklungen

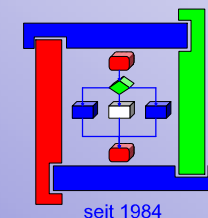
Mit den zusammenfassenden Betrachtungen wird ein Ausblick unter Berücksichtigung der aktuellen Entwicklungen gegeben.

- Neue Technologien LWL, Satelliten, Gigabit-Netz
- sinkende Kosten für Technologien
- höherwertige Dienste (Quality of Service)
- steigende Anzahl von Anwendern
- neue Einsatzbereiche (Data-Ware-House, Virtuelle Welten)

Aktuelle Entwicklungen

56 Vorlesung - FHDW

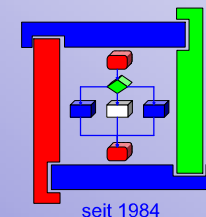
© Dr. G. Hellberg August 2000





# Gliederung

- Einführung (neue Formen der Kommunikation)
- Historische Betrachtungen
- Begriffsdefinitionen
- Vorteile / Nachteile / Nutzen von Netzwerken
- Bereitstellung von Diensten (email, ftp, www)
- Marktübersicht von NOS
- Risiken beim Einsatz von Netzwerken (Viren, Datenschutz, Firewall, Rechtliche Aspekte)
- Aktuelle Entwicklungen
- Zusammenfassung / Ausblick



# Zusammenfassung / Ausblick

Schwerpunktmäßig wurden in der Vorlesung folgende Punkte behandelt:

Nach einigen grundlegenden Begriffsdefinitionen (Kopplungselemente usw.) wurden die Vor- und Nachteile von Netzwerken diskutiert.

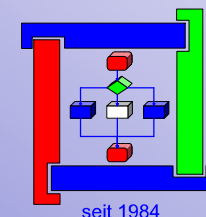
Danach wurden die einzelnen Dienste / Protokolle anhand des ISO/OSI-Referenzmodells und TCP/IP erläutert und in Beziehung zu aktuellen Betriebssystemen gesetzt.

Im Anschluß wurde schwerpunktmäßig auf die Risiken beim Einsatz von Netzwerken und auf den Aufbau von Sicherheitskonzepten eingegangen.

Zusammenfassung / Ausblick

58 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Zusammenfassung / Ausblick

Der Einsatz von globalen, heterogenen Netzwerken führt dazu, daß die Netzwerksicherheit immer mehr Relevanz bekommt.

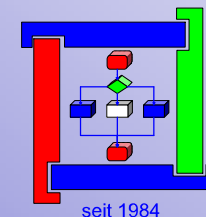
Die zur Verfügung gestellten Dienste stellen immer höhere Anforderungen an die IT-Technologien und -Verfahren.

Dem Anwender soll dieses durch eine möglichst einfache Schnittstelle zur Verfügung gestellt werden.

Zusammenfassung / Ausblick

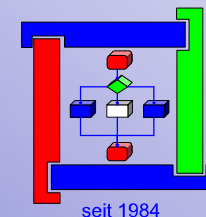
59 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Quellennachweise

- Einrichten von Internet Firewalls, D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly International Thomson Verlag, 1. Auflage 1996
- Firewalls und Sicherheit im Internet, William R. Cheswick, Steven M. Belovin, Addison-Wesley, 1. Auflage 1996
- TCP/IP Netzwerk-Administration, Craig Hunt, O'Reilly Verlag, 2. aktualisierte und erweiterte Auflage 1998
- Lexikon Lokale Netze, Klaus Lipinski, International Thomson Publishing, 1998
- Computertechnologie und Managementpraxis: Datenbanken und Objekte, Wolf Dietrich Nagel, Addison-Wesley, 1. Auflage 1992



# Definitionen zu Firewalls

## **Firewall**

Eine oder mehrere Komponenten, die den Zugriff zwischen einem geschützten Netz und dem Internet oder zwischen beliebigen anderen Netzen beschränken.

## **Host**

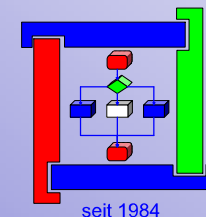
Ein Computersystem, das an ein Netz angeschlossen ist.

---

Risiken beim Einsatz von Netzwerken

61 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Definitionen zu Firewalls

## ***Bastion-Host***

Ein Computersystem, das besonders geschützt werden muß, da es für Angriffe prädestiniert ist - in der Regel, weil es dem Internet offensteht und eine wichtige Anlaufstelle für Benutzer interner Netze ist. Der Bastion-Host hat seinen Namen von den stark befestigten Vorsprüngen auf den Außenmauern mittelalterlicher Burgen.

## ***Dual-Homed-Host***

Ein für verschiedene Aufgaben ausgelegtes Computersystem mit mindestens zwei Netzchnittstellen.

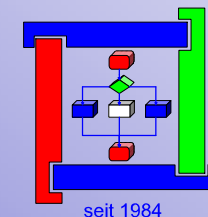
## ***Paket***

Die elementare Kommunikationseinheit im Internet.

## Risiken beim Einsatz von Netzwerken

62 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Definitionen zu Firewalls

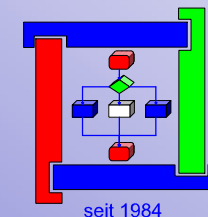
## ***Paketfilterung***

Die Aktion, bei der ein Gerät den Datenfluß von und zu einem Netz selektiv steuert. Paketfilter lassen Pakete nur passieren oder halten sie auf, was meist beim Routing zwischen zwei Netzen geschieht (normalerweise zwischen dem Internet und einem internen Netz). Für die Paketfilterung stellen Sie einen Satz von Regeln auf, in dem festgelegt ist, welche Pakettypen zugelassen sind und welche aufgehalten werden, z.B. Pakete von einer bestimmten IP-Adresse oder einem bestimmten Port. Paketfilterung kann auf einem Router, einer Bridge oder einem einzelnen Host stattfinden. Sie wird manchmal auch als Screening bezeichnet.

Risiken beim Einsatz von Netzwerken

63 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Definitionen zu Firewalls

## **Grenznetz**

Ein Netz, das zwischen ein geschütztes und ein externes Netz eingefügt wird, um eine weitere Schutzschicht zu schaffen. Ein Grenznetz wird manchmal auch DMZ genannt, das für *De-Militarisierte Zone* steht (nach einer Zone, die Nord- und Südkorea trennt).

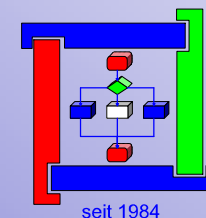
## **Proxy-Server**

Ein Programm, das stellvertretend für interne Clients mit externen Servern kommuniziert. Proxy-Clients unterhalten sich mit den Proxy-Servern, die bestätigte Client-Anfragen an die eigentlichen Server weiterleiten und die Antworten zurück an die Clients übermitteln.

## Risiken beim Einsatz von Netzwerken

64 Vorlesung - FHDW

© Dr. G. Hellberg August 2000





# Definitionen zu Firewalls

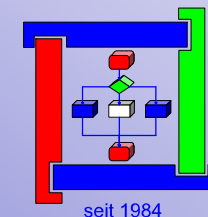
## ***Proxy-Dienste,***

sind spezielle Anwendungs- und Serverprogramme, die auf einem Firewall-Host ablaufen: entweder auf einem Dual-Homed-Host mit einer Schnittstelle zum internen und einer zum externen Netz oder auf einem anderen Bastion-Host, der Zugang zum Internet hat und von den internen Rechnern aus angesprochen werden kann. Diese Programme greifen die Benutzeranfragen nach Internet-Diensten wie FTP oder Telnet auf und leiten sie an die eigentlichen Dienst weiter, sofern sie mit einer Sicherheitspolitik des Standorts vereinbar sind. Die Proxies stellen Ersatzverbindungen her und fungieren als Gateways zu den Diensten. Deshalb werden Proxies manchmal auch *Application-Level-Gateways* genannt.

Risiken beim Einsatz von Netzwerken

65 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

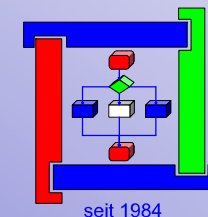
## **Architektur mit Dual-Homed-Host**

Eine Architektur mit Dual-Homed-Host wird um den Dual-Homed-Host herum aufgebaut. Dies ist ein Computer, der über mindestens zwei Netzanschlüsse verfügt. Ein solcher Host ist als Router zwischen den Netzen einsetzbar, an die die Schnittstellen angeschlossen sind, da er IP-Pakete von Netz zu Netz routen kann. Für die Firewall Architektur mit Dual-Homed-Host jedoch aktivieren Sie diese Routing-Funktion. IP-Pakete werden somit nicht direkt von einem Netz (dem Internet) in das andere Netz (das interne, geschützte Netz) geroutet. Systeme innerhalb des Firewalls und Systeme außerhalb (im Internet) können jeweils mit einem Dual-Homed-Host, aber nicht direkt miteinander kommunizieren. Der IP-Verkehr zwischen ihnen wird vollständig blockiert.

## Risiken beim Einsatz von Netzwerken

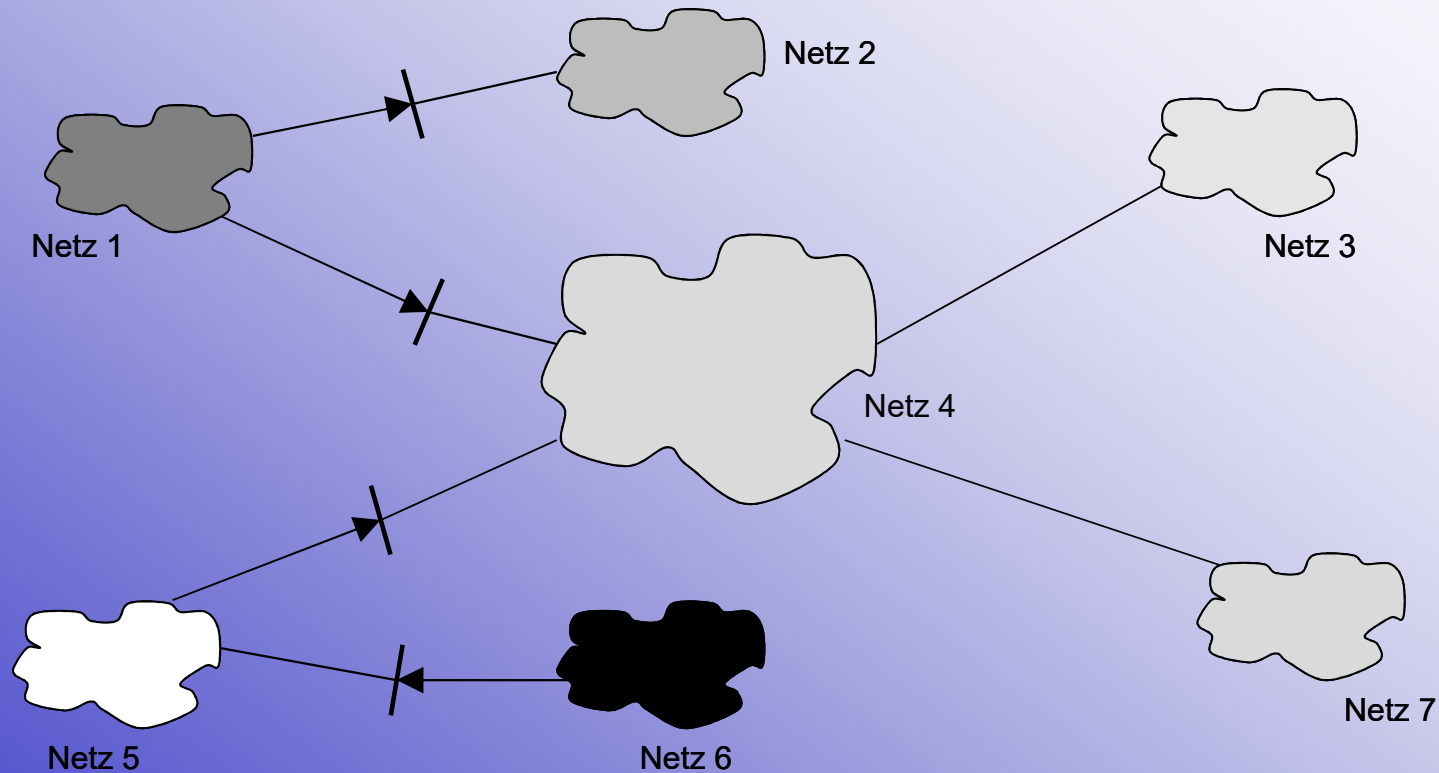
66 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

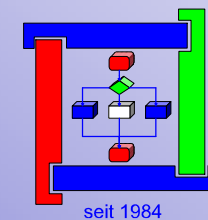
## Anordnung von Firewalls



## Risiken beim Einsatz von Netzwerken

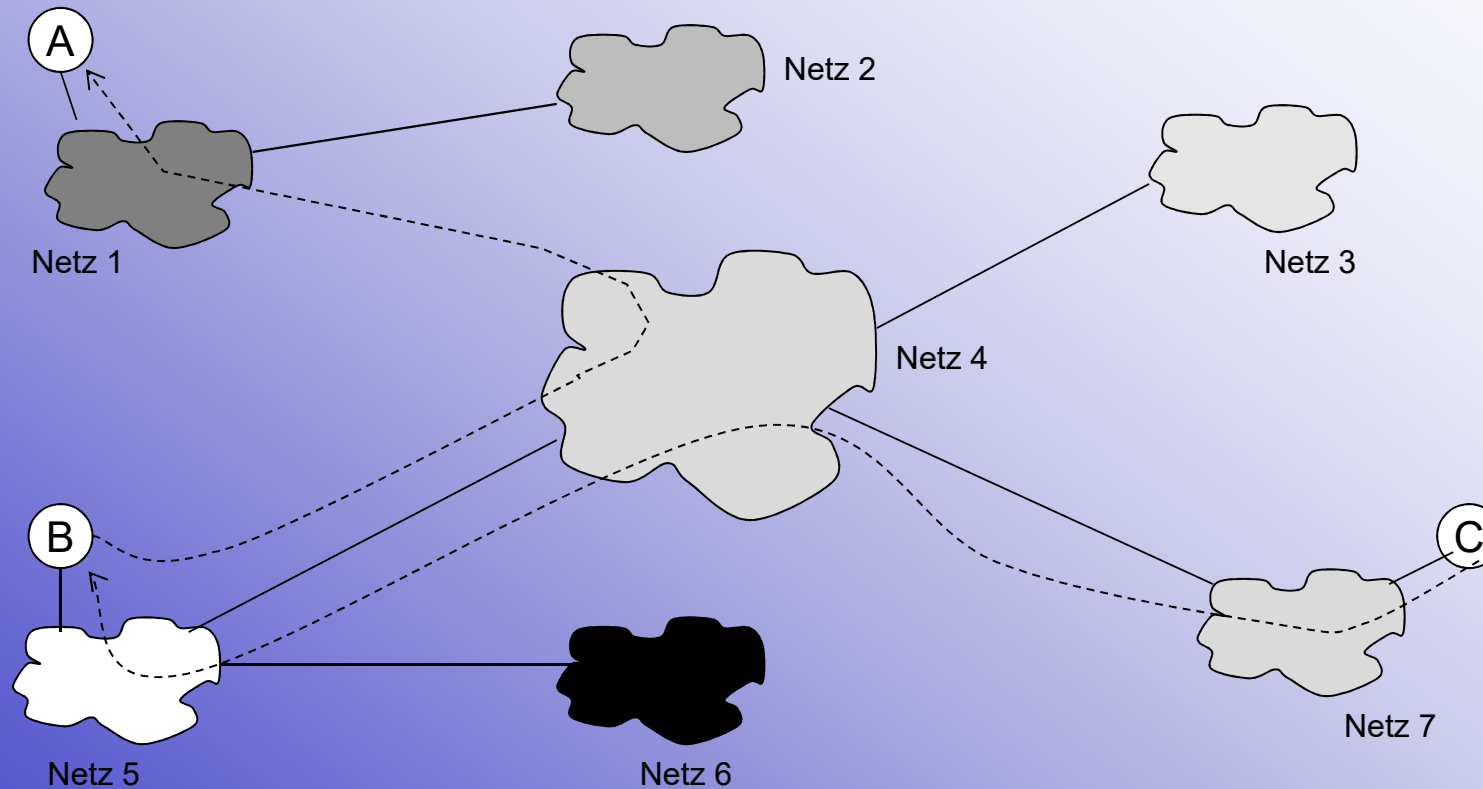
67 Vorlesung - FHDW

© Dr. G. Hellberg August 2000



# Sicherheit

## Beispiel für transitives Vertrauen



Risiken beim Einsatz von Netzwerken

68 Vorlesung - FHDW

© Dr. G. Hellberg August 2000

