Seminararbeit für das Proseminar IT/RAK

Netzwerkkomponenten: Hub, Bridge, Router, Firewall, ...

Ihre Lehrveranstaltungsnummer: 401212/2

Ihr Lehrveranstaltungsleiter: Prof. Dr. Roland Wismüller

Tragen Sie hier ihre Gruppendaten ein:

Name	Matrikelnummer
Max Steigerwald	9847008
Stefan Steigerwald	0047351

INHALTSVERZEICHNISS

Abstract

Wir wollen dem Leser in dieser Arbeit einen Überblick über Netzwerkkomponenten wie Kabeln, Router, Hub, Switches, Bridges, Firewalls und Gateways geben.
Diese Netzwerkkomponenten sind schon im alltäglichem Computerleben eingebetet und werden von manchen Menschen einfach nur als Selbstverständlichkeit wahrgenommen. Für unerfahrene User (wie z.B. Computerspieler, die übers LAN spielen oder normale Internetsurfer) sind das einfach nur Geräte die im Hintergrund und unsichtbar sind. Doch hinter diesen Geräten steckt viel mehr und sie verlangen nach Installation, Konfiguration und Wartung.

1. Einleitung / Introduction

Der Zusammenschluss von mehreren Computern und Peripheriegeräten zu Netzen gewinnt immer mehr an Bedeutung. War es damals das LAN was explosionsartig gestiegen ist, so ist es heutzutage das WLAN, das vor allem in Unternehmen und Privat Bereich eingesetzt wird.
Unter LAN (Local Area Network) bezeichnet man Lokale Netzte, die nur über einen begrenzten Raum gehen. Das gleiche gilt auch für WLAN (Wireless Local Network), was allerdings kabellos funktioniert.
Unter WAN (Wide Area Network) versteht man Weitverkehrsnetze, die für weite Entfernungen ausgelegt sind. Diese einzelnen Netze können über Router und Gateways miteinander verbunden werden und dabei auch öffentliche Kommunikationsnetze nutzen.
Um ein funktionstüchtiges Ethernet schaffen zu können bedarf es einiger Regeln. Man darf z.B. nicht beliebig lange Kabeln verwenden oder beliebig viele Hubs hintereinander schalten. Wird eine dieser Regeln nicht eingehalten, so kann es zu Problemen kommen.
Viele dieser Probleme lassen sich schon im Vorfeld vermeiden, indem man sich Wissen über den Aufbau von Ethernet und Netzwerken, sowie über die ISO/OSI Schichtenmodelle aneignet.
Das Grundprinzip von Ethernet baut auf CSMA/CD auf. Diese Abkürzung steht für „Carrier Sense Multiple Access with Collision Detection“. Aus CSMA/CD leiten sich auch die Regeln für das Design eines Ethernet-Netzwerks ab.
Carrier Sense heisst, dass eine Station vor dem Sendeversuch zuerst einmal eine gewisse Zeitspanne lauscht, ob nicht jemand gerade sendet oder senden will. Diese Zeitspanne wird auch Interframe Gap genannt. Es darf aber nur gesendet werden wenn das Medium frei ist.
Multiple Access bedeutet, dass eine Station direkt nach dem Senden eines Pakets wieder auf das Medium zugreifen darf, um weitere Daten zu senden. Bei Verfahren wie Token Ring, muss sie warten, bis sie wieder die Sende-Benachrichtigung in Forum eines Tokens erhält.
Wenn beim Ethernet zwei Stationen am Medium lauschen (Carrier Sense genannt) und dann gleichzeitig senden, muss diese Situation erkannt werden und alle sendenden Stationen müssen daraufhin eine *Collision Detection* durchführen. Eine Kollision wird dadurch erkannt, dass sich die elektrischen Signale der Übertragung überlagern. Hier wird dann ein JAM-Signal ausgesendet, das allen angeschlossenen Stationen anzeigt, dass das Paket ungpltig ist. Der Netzwerkbereich, auch Collision Domain genannt, breitet das JAM Signal aus.

2. Methodik

Um an Informationen über das Netzwerk im Allgemeinen und über Netzwerkkomponenten zu kommen, haben wir uns der Suchmaschine Google und Astalavista bedient – also großteils aus dem Internet. Des Weiteren haben wir auch Informationen aus Büchern der TU Wien Bibliothek und der Hauptbibliothek Wien.

3. Kabel

Um ein Ethernet überhaupt erstmal möglich machen zu können, bedarf es nach dem Herzstück, dem Kabel (Die kabellose Variante eines LANS wird WLAN genannt).
Für die Klassifikation von Kabeln und die Setzung von Standarts ist die *Electronic Industry Association und Telecommunication Industry Association (EIA/TIA)* zuständig.
Es werden 3 Arten von Kabeln unterschieden:

3.1 Coax Kabel

Alle Coax Kabelsysteme rufen eine Bus Topologie hervor und lassen sich mithilfe von Repeatern ausdehnen. Jedoch darf das Netzsegment max. 185m bei 10Base2 und 500m bei 10Base5 lang sein. Schuld an dieser Eingrenzung ist die Protokoll- und Kollisionsbehandlungs- Struktur.

10Base2:
dieses Kabelsystem ruft eine Bus Topologie hervor und ist wegen der niedrigeren Kosten vor allem in kleineren Netzwerken weit verbreitet. Es ist ausserdem bestens zum Verbinden zweier Rechner über das Ethernet geeignet. Die maximale Segmentlänge beträgt 185m und der minimale Länge beträgt 0.5m. An den Bus werden die Ethernet-Devices mit Hilfe von T-Stücken zusammengeschlossen.

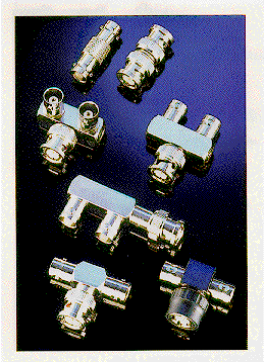

Abbildung 1: T-Stück

10Base5:
Bei diesem Kabeltyp ist die maximale Segmentlänge auf 500m beschränkt. Er wurde bei Ethernets das erste Kabel, das Gebrauch gefunden hat, und wird jetzt aber kaum noch eingesetzt. Laut Ethernetspezifikation ist eine maximale Weglänge von 2.5km erlaubt, die durch eine maximale Anzahl von 4 Repeatern, was 5 10Base5 Segmenten entspricht, erreicht wird – was aber auch schon das Limit ist.

Name	Kabeltyp	Beschreibung
Koax (Kupfer)	RG-58/U	sehr billig, daher teilweise für Ethernet eingesetzt
	RG-58A/U	Thinwire Ethernet, 10Base2
	RG-58C/U	Thinwire Ethernet, 10Base2
	RG-59	Kabelfernsehen

Tabelle 1: Koax Kabel

3.2 Twisted Pair Kupfer-Kabel

Das für LANs am meisten verbreiteste Kabel ist ohne Frage das Twisted Pair kurz TP genannt. Hierbei handelt es sich um paarweise miteinander verdrillte Kupferleiter.
Es gibt jedoch verschiedene Kategorien, wie viele Paare das Kabel nun hat und wie gut sie voneinander abgeschirmt sind. Für 10Mbps Netzte werden meistens die TP Kabel der Kategorie UTP-3 eingesetzt. Für Netzwerke die auf 100Mbps werden Kabeln aus der UTP-5 Kategorie eingesetzt. Die Anschlüsse dieser Kabeln werden RJ-45 Stecker genannt und ähneln sehr den gewöhnlichen ISDN Telefon Steckern.

Abbildung 2: RJ-45 Stecker und Steckdose

3.3 Crossoverkabel

Sind für die Verbindung zweier Hubs oder direkt Verbindung zweier Computer über ihre NICs (Network Interface Cards). Hubs werden dann miteinander verbunden wenn man ihre Rechneranschlüsse erhöhen will. Es lässt sich jedoch nur eine begrenzte Zahl an Hubs miteinander verbinden.

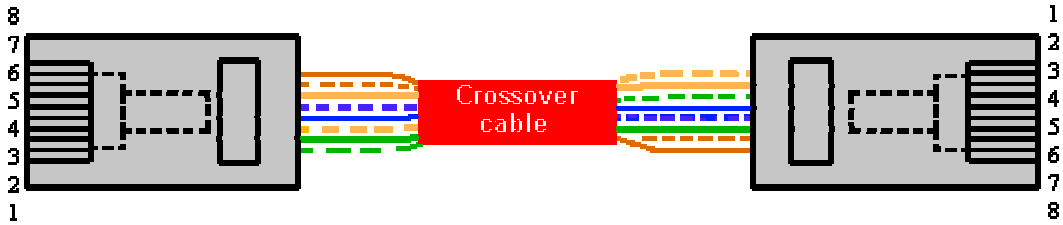

Abbildung 3: Crossoverkabel

10BaseT:
Bei dieser Verkabelung ist eine Baum- oder Sternverkabelung notwendig.

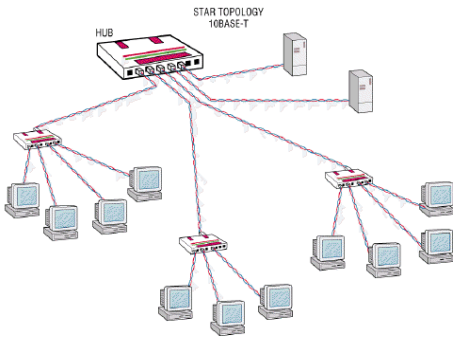

Abbildung 4: Sternverkabelung

Hierbei reicht ein Kabel der Kategorie UTP-3 und die und die Sterntopologie (siehe Abbildung) mit Hub, Switches, Routern, etc ist leichter zu administrieren als ein Bus-Netzwerk.

Name	Kabeltyp	Spezifikations-Typ	Beschreibung
Twisted Pair (Kupfer)	STP (Shield Twisted Pair)	IBM Typ 1/9	4- und 16-MBit Token Ring
	UTP-1 (Unshield Twisted Pair)	EIA/TIA-586 Kategorie 1	Analoge Sprachübertragung
	UTP-2	EIA/TIA-586 Kategorie 2	IBM-Verkabelung Typ 3 EIA-232
	UTP-3	EIA/TIA-586 Kategorie 3	10BaseT, 100BaseT4, 4-MBit Token Ring, ISDN
	UTP-4	EIA/TIA-586 Kategorie 4	16-MBit Token Ring
	UTP-5	EIA/TIA-586 Kategorie 5	100BaseTx, ATM (155Mbps)

Tabelle 2: Twisted Pair Kabel

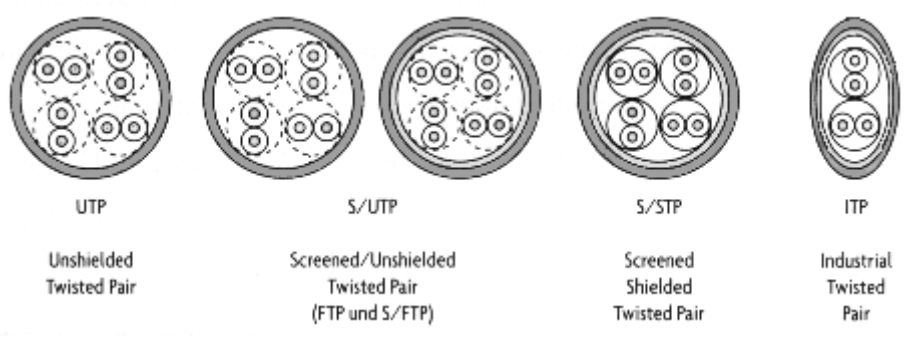

Abbildung 5: Querschnitt von Twisted Pair Kabeln

3.4 Glasfaserkabel

Glasfaserkabel bieten die beste Geschwindigkeit und ermöglichen auch größere Distanzen bei LANs. Da sie aber jedoch nicht sehr billig sind, spezielle Hardware wie z.B. Transeiver und Switches benötigen und nach einer nicht ganz unproblematischen Handhabung verlangen, werden sie meistens nur in Backbones eingesetzt. In kleineren 10Mbps Netzten werden sie nur eingesetzt wenn die Distanz, die die TP Kabeln bieten, zu kurz sind.
Das *Fiber Distributed Data Interface* (FDDI) ist eine „High Performance“ Token-Ring Technologie und kann die Daten mit 100Mbps bei einer Entfernung von 200km übertragen.
Eine Alternative zum FDDI wäre der *Asynchronous Transfer Mode* (ATM) wo sogar eine Übertragung von 665Mbps erreicht werden können und mit den billigeren Kupferkabeln sogar 155Mbps.

4. Router

Abbildung 6: links LAN Router, rechts WLAN Router

Heutzutage sind Router Dreh-und Angelpunkt in strukturiert aufgebauten LAN- und WAN-Netzen. Ein Router verknüpft alle Netze mit unterschiedlichen Protokollen bis zur OSI -Ebene 3 miteinander(siehe *Abb.13*). Dies bedeutet, dass er auch Netze unterschiedlicher Topologien verbindet, wobei die Adressierung der OSI-Ebene 3 (Netzwerk-Protokollebene) einheitlich sein muß.
Der Router arbeitet nicht wie eine Bridge oder ein Switch mit den Adressen der MAC-Ebene. Er untersucht, bevor er ein Paket an ein abgeschlossenes LAN oder WAN weiterleitet, die Adressangaben des Pakets und leitet die Daten in Abhängigkeit seiner Routing-Tabelle weiter. Der Host muß nicht die MAC-Adresse des Empfängers wissen, um diesem eine Nachricht zu übertragen. Es genügt die Adresse der Netzwerk-Protokollebene. Die Latenzzeit der Daten im Router wird erhöht, da das Datenpaket für das Routen untersucht werden muß.
Es sei zu erwähnen, dass der Router im Gegensatz zur Bridge eine wesentlich bessere Administrierbarkeit bietet. Man kann ein LAN auch auf vielfältige Möglichkeiten logisch unterteilen.
Eine der Stärken von Routern ist die Fähigkeit, mittels Algorithmen den bestmöglichen Weg für ein Datenpaket zum Empfänger zu wählen. Dieser wird mit Hilfe der Routing-Tabelle gewählt. Unter „Routen“ versteht man das Weiterleiten von Daten.
Im Internet ist es so, dass viele Wege zu ein und dem selben Ziel führen. Im Normalfall sucht der Router immer den besten Weg aus, wenn jetzt aber mal ein Knoten in diesem „besten Weg“ ausfällt, bestimmt der Router augenblicklichst einen alternativen Weg zum Ziel. Dieses dynamische Datentransfer-Verfahren hat den Vorteil, dass Ausfälle oder Engpässe mit alternativ Routen überwunden werden, jedoch entsteht auch mehr Verwaltungsaufwand und es lässt sich nicht vorhersagen welchen Weg jedes einzelne Datenpaket einschlägt, was dann die Fehlersuche bei großen Netzen ins unermessliche hin erschweren kann.
Alle angeschlossenen Netzwerkprotokolle müssen die Fähigkeit des Routens unterstützen und vom Router verstanden werden, damit die Daten weitergeleitet werden können. Im Normalfall kann ein Router, ein oder mehrere Netzwerkprotokolle unterstützen. IP und IPX sind hier weit verbreitet. Router unterstützen aufgrund der zunehmenden Verbreitung heterogener Netze meist mehr als zwei Protokolle. Folgende Beispiele sind hier anzuführen: DECnet, AppelTalk, XNS, VINES und Apollo Domain.
Wenn Netzwerkprotokolle keine Routingfunktion unterstützen (zu erwähnen sind NetBios und LAT), müssen diese, sofern der Router auch Bridge-Funktionen unterstützt, gebridged werden. Diese Router (welche Bridge-Funktionen unterstützen) werden als BRouter (Bridge-Router) bezeichnet.
Zu erwähnende Eigenschaften von Routern sind die Filterfunktionen und die Netzwerk-Managementfunktionen. Die Netzwerk-Performance kann durch verschiedene Routing-Einstellungen verbessert werden, je nach Anforderung an das Netz. Router leiten in der Regel z.B. Broadcasts nicht weiter, daraus lässt sich schließen, dass sie eine höhere Isolation bieten.

Weiters können Router als Firewalls fungieren. Das funktioniert, indem bestimmte IP-Adressen der Zugriff auf bestimmte Netzteile verwehrt wird. Bei den meisten Routern wird die Konfiguration per Software eingestellt. Das Simple Network Management Protocol (SNMP) wird von vielen Routern heutzutage unterstützt.

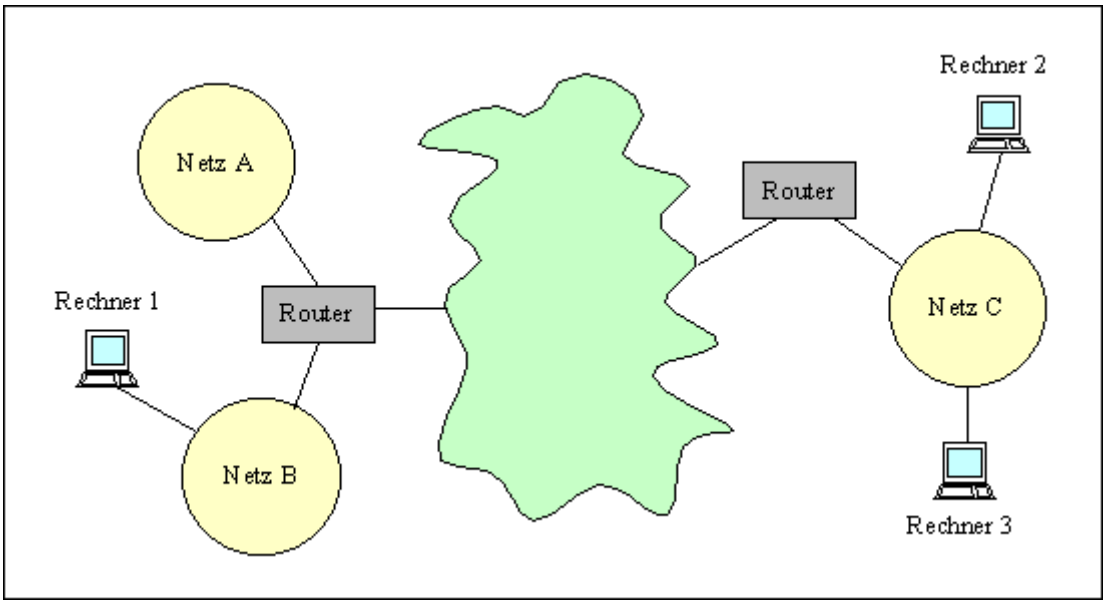

Abbildung 7: Router im Einsatz

Router sind sehr ähnlich dem PC und auch dementsprechend aufgebaut. Viele Leute bevorzugen auch einen alten Computer mit Linux als Router, der sogar noch mehr Funktionen als ein kleiner Hardeware-Router bietet. Der Aufbau von Routern sieht folgendermaßen aus:

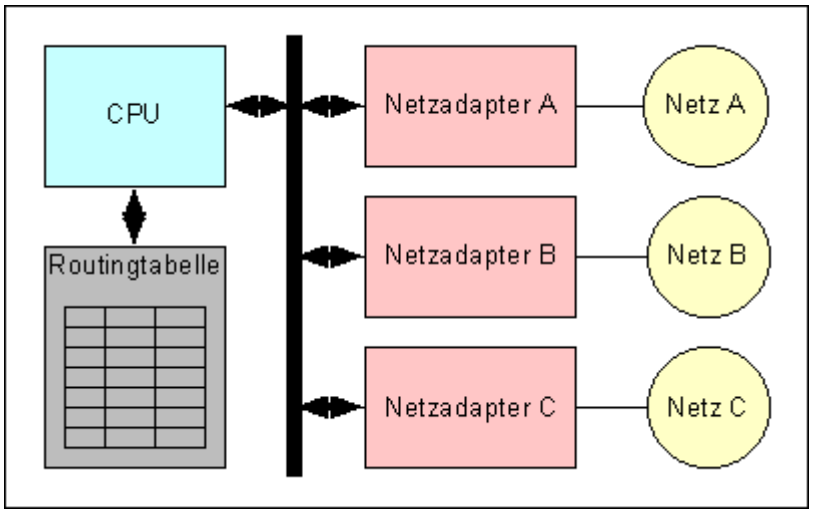

Abbildung 8: Innenleben eines Routers

Hier lässt sich erkennen, dass der Router genauso wie ein Computer auch eine CPU und einen Speicher besitzt. Im Speicher selbst liegt die Konfigurationsdatei und die Routingtabelle. Ausserdem hat er mehrere Netzadapter, die für die Verbindung der angeschlossenen Netze zuständig ist.

5. Switch

Abbildung 9: Switch mit 8 Ports

Der Hersteller Calpana hat den Begriff Switch eingeführt, welcher sich im Laufe der Zeit etablierte.
Der Switch kann LANs mit verschiedenen physikalischen Eigenschaften verbinden (Koax- mit Twisted-Pair-Netzwerken), d.h. er ist ein Gerät des OSI-Layers 2(siehe *Abb.13*). Dabei muß erwähnt werden, dass alle Protokolle höherer Ebenen (von 3 bis 7) identisch sein müssen. Dies gilt auch bei der Bridge. Ein Switch ist protokolltransparent. Da ein Switch ähnliche Eigenschaften wie eine Bridge aufweist, wird er auch als Multi-Port-Bridge bezeichnet. Jeder Port bildet ein Netzsegment. Die gesamte Netzwerk-Kapazität steht jedem dieser Segmente zur Verfügung. Daraus lässt sich schließen, dass ein Switch nicht nur die Netzwerk-Performance im Gesamtnetz, sondern auch in jedem einzelnen Segment erhöht. Vergleichbar wie eine Bridge untersucht der Switch intern jedes Paket auf die MAC-Adresse des Zielsegments und kann es dorthin direkt weiterleiten. Wenn das Paket aus dem selben Segment, für das es bestimmt ist, ist, so wird es gelöscht und nicht noch einmal übertragen. Einer der großen Vorteile eines Switches ist, dass er seine Ports direkt verschalten kann. Dies bedeutet, er kann dedizierte Verbindungen aufbauen. Der Switch ist aufgrund dieser Eigenschaften ein beliebtes Instrument um ein LAN zu unterteilen und somit die Netzwerk-Performance zu verbessern.
Ein Switch ist eigentlich nichts anderes als ein Hub nur in „intelligenter“ Form. Ein Hub schickt im Gegensatz alle Datenpakete an alle Ports weiter. Der Switch merkt sich jedoch anhand der MAC-Adresse (Ist eine eindeutige Seriennummer der Netzwerkkarte und gibt es wirklich nur einmal) der Network Interface Cards, welche Stationen an welchen Ports zu finden sind, anstatt alle Datenpakete and alle Ports zu schicken, wie es beim Hub üblich ist.
Zur Verdeutlichung sieht man anhand dieser Grafik, dass der Switch die Datenpakete nur an den Zielort überträgt. Hier überträgt PC1 seine Daten an PC3 und gleichzeitig überträgt PC3 seine Daten an PC2.

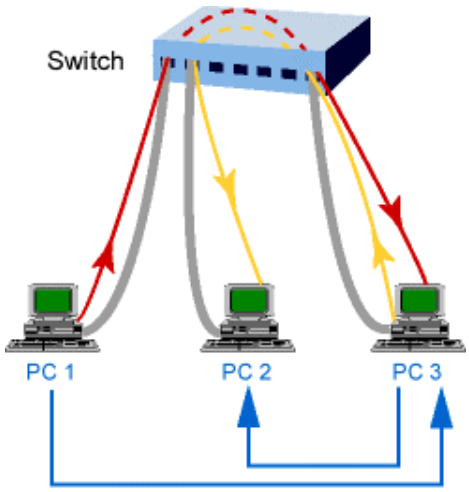

Abbildung 10: Datenpakete Versand beim Switch (vergleiche Abb.12)

Die Netztopologie muß dem Switch angepasst sein, damit man diesen gewünschten Effekt erzielen kann. Unter Umständen sollten Knoten, die viele Daten übertragen, an einen eigenen Port am Switch angeschlossen werden. D.h. die Datenlast sollte möglichst gleichmäßig auf alle Ports verteilt sein. Ein solcher Port wird oft für Server eingesetzt. Das Ziel ist die Datenmenge, die mehr als ein Segment durchlaufen muss, zu reduzieren.

Die zwei Gruppen der Switch-Technologie:

- Store-and-Forward
  Das gesamte Datenpaket wird von den Switchers dieser Kategorie untersucht. Dies funktioniert folgendermaßen: Die Pakete werden kurz zwischengespeichert, daraufhin auf ihre Korrektheit und Gültigkeit überprüft und entweder verworfen oder weitergeleitet. Daraus ist ersichtlich, dass diese Methode eine hohe Latenzzeit benötigt, doch kann durch das Herausfiltern ungültiger Pakete die Netzperformance wiederum verbessert werden.

- Cut-Trough
  Die Latenzzeit (Verweilzeit) der Pakete im Switch ist bei dieser Technologie sehr kurz. Dies funktioniert folgendermaßen: Es werden nur die ersten 6 Bytes eines Pakets gelesen, um die Quell -und Zieladresse zu erfahren. Daraus folgernd können ungültige oder defekte Pakete ungehindert den Switch passieren.

Da beide Technologien Vor– und Nachteile haben, kann man nicht pauschal beantworten, ob nun die Cut-Trough- oder Store-and-Forward-Technologie für das gegebene Netz günstiger ist. Die meisten Switches heutzutage verfügen über Netzwerk-Management-Funktionen, genau wie Router und können über Simple Network Management Protocol (SNMP) per Software konfiguriert werden.

6. Hub

Abbildung 11: Hub mit 8 Ports

Der Hub wird auch als Multi-Port-Repeater bezeichnet, die in der Regel 4, 8, 12, 16, 24 und 32 Ports besitzten. Er ist das Pendant zum Repeater im Twisted-Pair verkabelten Netz. Repeater und Hubs werden zur einfachen Erweiterung der Netzausdehnung eingesetzt, da sie sehr günstig sind. Im LAN bilden Hubs zusammen mit dem Switch die Grundlage für die Baumtopologie. Der Name „Hub“ steht für fast alle Verstärkungskomponenten, die sich sternförmig vernetzen lassen. Bei einer Twisted Pair-Verkabelung ist meistens einer der Ports (meistens der letzte) also „Uplink“ aktivierbar. Somit lassen sich Hubs miteinander per

Twisted-Pair Kabel verbinden. Oder aber man greift gleich zu einem Cross-Over Kabel und geht über den normalen Port.
Die an einem Port ankommenden Signale werden von einem Hub auf alle weiteren benutzten Ports verteilt. Im Sinne der Repeaterregel gelten alle Ports eines Hubs als ein Segment. Um Übertragungsengpässe zu verringern, werden innerhalb des Hubs oft besonders breite Busse eingesetzt. Alle Stationen des Hubs teilen ein Segment des LANs, deswegen bleibt ein Segment, das über Hubs gebildet wird, ein „shared segment“. Folglich teilt er ein Netz in physikalisch unabhängige Segmente, trotzdem bleibt die logische Topologie eines Busses erhalten. Daraus ist erkennbar, dass ein Hub die Netzkapazität erhöht.
Die Hubs in der heutigen Zeit besitzen mindestens einen zusätzlichen Port, an dem ein weiteres Netzsegment angeschlossen werden kann. Über spezielle Ports lassen sich Stackable Mulitport Repeater (Hubs) zum einen großen Repeater Stack zusammenschließen.

Die zwei unterschiedlichen Methoden bei Verbindungen von Hubs:

- Die Verbindung der Hubs erfolgt über Hersteller-spezifische Busports. Hierbei sprechen wir von einer räumlichen Konzentration der Hubs, allerdings zählen die so verbundenen Hubs als ein Repeater. Es lassen sich dadurch bis zu 5 Meter überbrücken. Daraus lässt sich schließen: die maximale Entfernung bei 2 a 100m TP-Kabeln und dem Interrepeaterlink von 5m beträgt 205m zwischen den Hosts im zugehörigen Segment.

- Die Verbindung der Hubs erfolgt über Thin Wire-Kabel. Standardgemäß verfügen sie als Backbone-Anschluß über einen 10Base2-Anschluß. Es sei noch zu erwähnen, dass Hubs räumlich getrennt stehen können, wobei jeder Hub als Repeater im Sinne der Repeaterregel zählt.

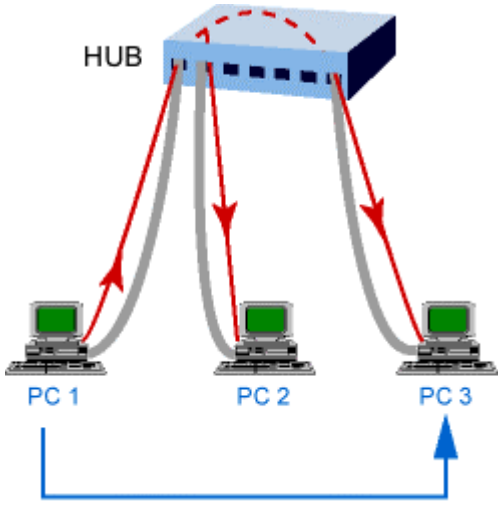

Abbildung 12: Datenpaketeversand beim Hub (vergleiche Abb.10)

Wie sich hier in *Abbildung 12* erkennen lässt leitet der Hub jedes eingehende Datenpaket an alle Ports weiter.

Manche Hersteller verleiben dem Hub Funktionen einer Bridge ein. Diese werden Bridging-Hubs genannt.

Wichtige Eigenschaften von Hubs:

- Datenpakete können immer nur hintereinander den Hub passieren, also niemals zusammen
- Hubs haben eine Geschwindigkeit von 10Mbps oder 10/100Mbps bei Dual Speed Hubs
- Sie wissen nicht, an welchem Port welche Station angeschlossen ist und können es auch nicht erlernen. Sie können auch nicht konfiguriert werden sowie Router
- Billiger als Switches

7. Gateway

Gateways ermöglichen die Verbindung von völlig unterschiedlichen Netzen, außerdem decken sie alle sieben Schichten des OSI-Referenzmodells ab(siehe *Abb.13*). Sollen zwei inkompatible Netztypen miteinander verbunden werden, so werden Gateways eingesetzt. Es ist eine LAN-WAN Kopplung möglich oder eine LAN-WAN-LAN Kopplung.
IPX-IP Gateways auf Novell-Servern oder TCP/IP-Systeme mit DECnet-Hosts. Gateways können auch Softwaremodule sein und müssen nicht unbedingt reine Hardwarelösungen sein. Der Vorteil der Hardware besteht darin, dass sie schneller ist, allerdings ist sie unflexibler. Die Latenzzeit der Daten ist sehr hoch. Tunneling wird von Gateways nicht unterstützt, da das jeweilige Protokoll real in ein anderes umgesetzt wird.
Der Gateway ist ein aktiver Netzknoten und die Adressierung erfolgt von beiden Seiten aus. Er kann auch immer nur 2 Netze miteinander verbinden und niemals mehr. Von großer Bedeutung für Gateways ist das Routing über die Netzgrenzen hinaus. Es werden zwei Typen unterschieden:

- Medienkonvertierende Gateways (Sie stellen bei gleichem Übertragungsverfahren die Verbindung zwischen unterschiedlichen Prokollen, der unteren Ebene her, wo Router nicht mehr ausreichen würden.
- Protokollkonvertierende Gateways (Sie sind für die unterschiedlichen Protokolle der Ebenen 3 und 4 zuständig(siehe *Abb.13*))

Die Unterschiede zwischen Router und Gateway:
Ein Gateway ist ein Netzwerk-Device der Ebene 7 und ein Router der Ebene 3(siehe *Abb.13*). Irrtümlicherweise wird ein Router häufig mit einem Gateway verwechselt. Da der Begriff „Gateway“ in den Eingabemasken von PC TCP/IP-Software falsch verwendet wird, ist die Verwechslung vollkommen. Die erwähnten Eingabemasken verlangen meist anstelle einer Routeradresse, für den anzumeldenden Host, eine Gateway-Adresse.

8. Bridge

Die Bridge verbindet LANS mit verschiedenen physikalischen Eigenschaften. Zu erwähnende Beispiele sind Coax-mit Twisted-Pair-Netzwerken. Die Protokolle der höheren Ebenen (von 3 bis 7) müssen miteinander konform sein. Die Bridge ist in der IEEE 802.1D grundlegend beschrieben und ist protokolltransparent. Ein LAN, das mittels Bridge erweitert wurde, bildet nach außen hin weiter eine Einheit.
Die Bridge ist stark in ihrer Leistungsfähigkeit eingeschränkt LANs logisch zu unterteilen, da sie die MAC-Adressen der Datenpakete interpretiert, und nicht im Gegensatz zum Router mit

höheren Protokollen (Internet-Protocol-IP) arbeitet. Die Brigde ist auf MAC-Adressen angewiesen (Gegensatz zum Router). In der Regel ist eine Bridge im Bezug auf die Latenzzeit schneller, allerdings bieten heutzutage viele Router auch Bridge-Funktionalitäten an und sind nicht wesentlich teurer. Allgemein gesagt sind Brigde für kleine Netzstrukturen geeignet.
Folgende wichtige Merkamale einer Bridge:

- Durchsatzsteigerung:
  Die Netzperformance wird erhöht, indem in den durch Bridges getrennten Netzsegmenten unterschiedliche Daten gleichzeitig transferriert werden.

- Ausfallsicherheit:
  Störungen von der einen Seite der Bridge können nicht auf die andere Seite gelangen

- Datensicherheit:
  Informationen, die zwischen Knoten auf der einen Seite der Bridge ausgetauscht werden, können nicht auf der anderen Seite der Bridge abgehört werden. Als Beispiel hiefür sind Benutzerpasswörter, die Terminal-Server und Terminal-Rechner übertragen werden.

- Vermeidung von Netzwerkschleifen:
  Da eine Bridge den so genannten Spanning Tree Algorithmus unterstützt, ist es möglich, Ring-oder Schleifenkonfigurationen im Netz zu erlauben. Im Gegensatz zu „dummen“ Repeatern oder Hubs, kommunizieren Bridges. Diese stellen über den Algorithmus sicher, dass bei mehreren redundanten Verbindungen immer nur eine Gerade aktiv ist. Dadurch werden kreisende Pakete im Netz verhindert.

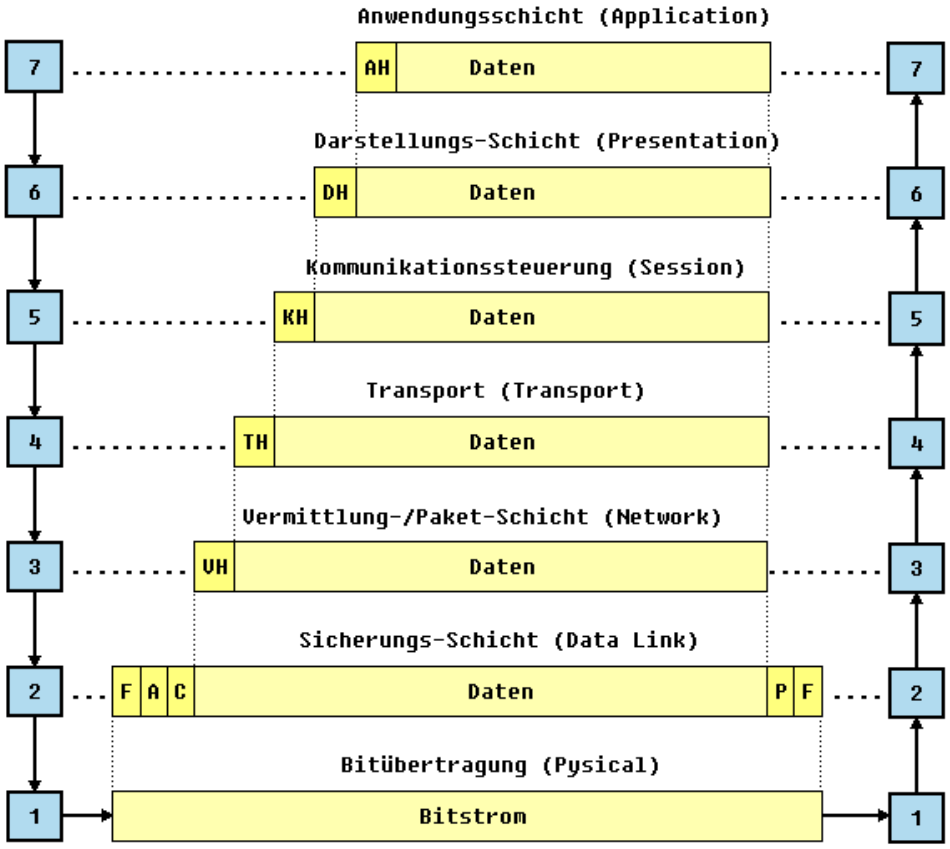

Abbildung 13: OSI Schichtenmodell

9. Firewall

Die Notwendigkeit einer Firewall für firmen Netze als auch private Netze nimmt von Tag zu Tag zu. Hacker haben die Möglichkeit durch gezielte Attacken von außen Rechner in firmen als auch privat Netzen lahm zulegen, als auch an wichtige Daten zu kommen.
Eine Art wie sich dieses Problem „verringern“ lässt sind die Firewalls, die aber auch ständig gewartet und konfiguriert werden müssen. Aber auch dann sind sie kein 100 Protzentiger Schutz gegen Angriffe von Außen.
Meistens versteht man unter einer Firewall einen eigenen Rechner (meistens ein Linux Rechner), der als eine Art Schnittstelle zwischen Intranet und WLAN fungiert und überwacht den ein- und ausgehenden Datenverkehr.
Firewalls werden aber auch als Softwarelösungen angeboten (zB. Norton Firewall, Blackice etc.) und in Routern eingebaut (siehe *Abb.6*).
Die Kofiguration der Firewall im Router geschieht sehr leicht:

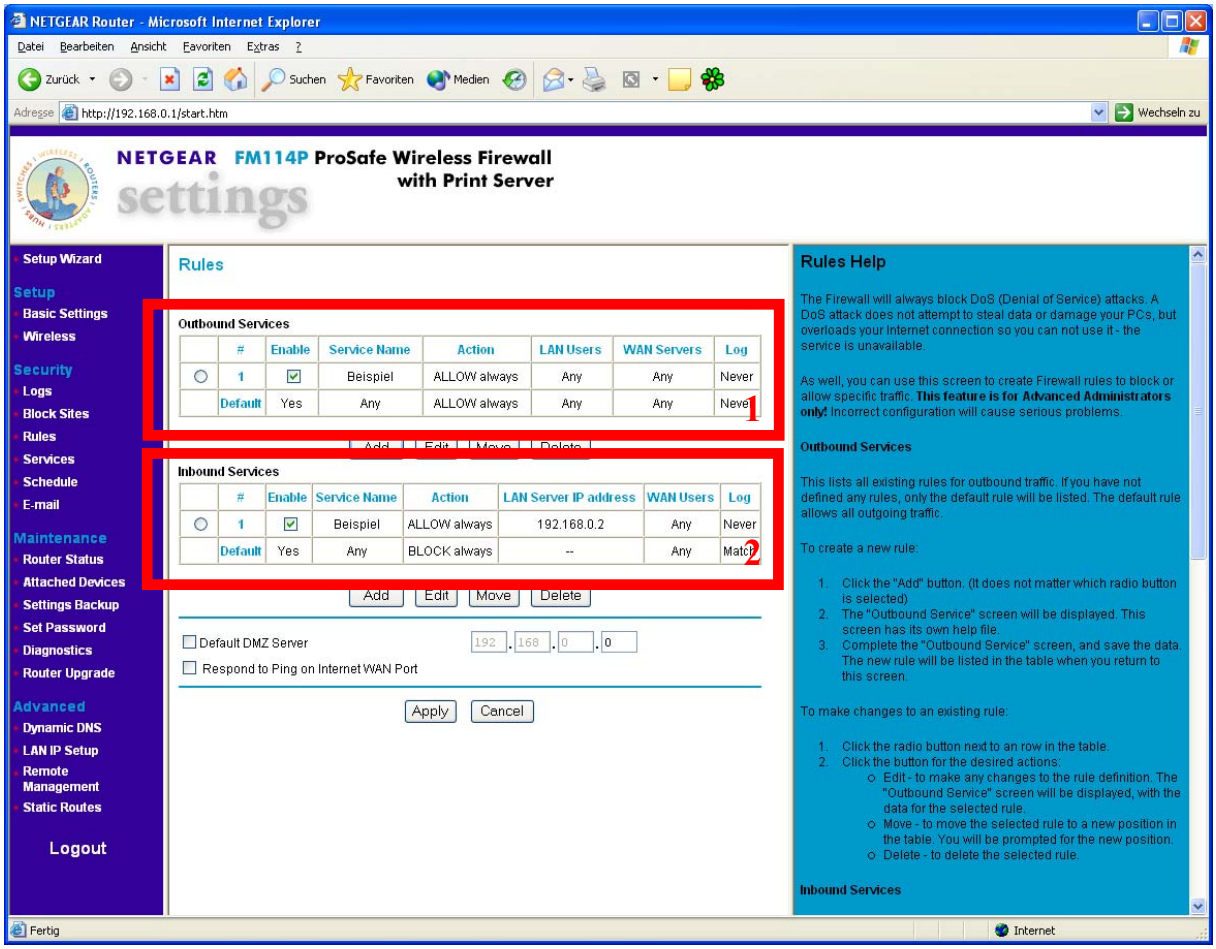

Abbildung 14: Konfiguration der Firewall eines Netgear FM114P Routers

In *Abb.14* sieht man wie das Konfigurationsfenster eines Netgear-Routers ausschaut. Zu diesem Fenster kommt man per Web-Browser, indem man die IP-Adresse des Routers angibt. (Im Normalfall ist die Adresse 192.168.0.1 und 192.168.0.x ist dann für die an dem Router hängenden Computer). Bei manchen Routern kommt man zu der Konfiguration jedoch nur per Telnet, weil kein GUI angeboten wird.
Im roten *Fenster Nr. 1* werden die Outbound Services festgelegt. Der Outbound Service ist zuständig für den Verkehr der nach draussen geht. Hier lassen sich z.B. bestimmte IP Adresse sperren die nicht ins Internet gehen dürfen.

Im *roten Fenster Nr.2* werden die Inbound Services festgelegt. Der Inbound Service verwaltet den Verkehr der von draußen nach drinnen geht. Hier kann man bestimmte Ports (TCP und UDP) festlegen, die durch die Firewall zu einer bestimmten IP-Adresse gelassen werden.

Eine Firewall kann auf zwei Arten installiert werden:

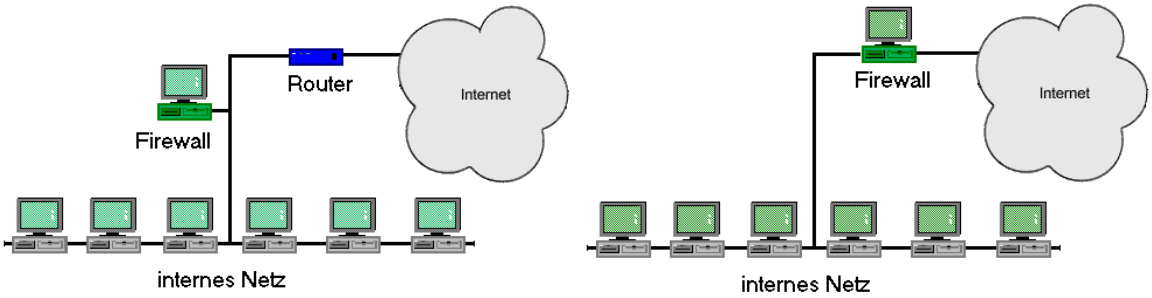

Abbildung 15: Firewall auf 2 Arten

In *Abb.15 links* ist die Firewall zwischen dem internen Netz und dem Router installiert.
Hier wird die Firewall in das lokale Netz eingebunden und dem Router wird gesagt, dass alle Datenpakete nur an die Firewall weitergegeben werden. Die Firewall ist somit auch als einziges System nach außen hin sichtbar.
In *Abb.15 rechts* ist die Firewall zwischen dem internen Netz und dem WAN geschaltet. Hier ist die Firewall mit zwei NICs ausgerüstet, damit das interne und das externe Netz durch den Rechner getrennt wird. Hier werden nur erlaubte Datenpakete durch die Firewall geroutet.

Egal ob Software- oder Hardware-Firewall gibt es 2 Arten, auf die eine Firewall konfiguriert werden kann:

- „Es ist alles erlaubt, was nicht verboten ist“
  Hier werden bestimmte Dienste (tftp, nfs) ausgeschlossen. Er ist sehr benutzerfreundlich, weil neue Dienste automatisch erlaubt sind, jedoch ist er aber auch gefährlich, da der Administrator die Datentransfers ständig im Auge haben muss und gegebenenfalls gleich Gegenmaßnamen treffen.

- „Es ist alles verboten, was nicht erlaubt ist“
  Diese Art ist sehr benutzerunfreundlich, weil alle Dienste automatisch geblockt werden und wenn ein Benutzer einen Dienst nutzen will, so muss er es extra beantragen. Jedoch ist diese Art besonders sicher, weil der Zugriff auf alle unbekannten Ports automatisch gesperrt wird. Somit werden Sicherheitslücken im Betriebssystem und in Anwendungsprogrammen geblockt.

Es gibt 3 Arten von Firewalls:

- Paketfilter überprüfen hier die Quell- und Zieladresse (die IP-Adresse und den TCP/UDP Port) und entscheiden dann ob es weiter darf oder nicht. Von Vorteil ist die Transparenz für den User, wobei diese Transparenz auch von Nachteil ist, weil die Paketfilter nicht zwischen Nutzern und deren Rechten unterscheiden kann. Es gibt jedoch auch intelligente Paketfilter die den Inhalt der Pakete zusätzlich analysieren und erkennen des weiteren die Zulässigkeit von Verbindungen, die einfache Paketfilter nicht erlauben würden.

- Circuit Level Gateways sind vergleichbar mit Paketfiltern, arbeiten jedoch auf einer anderen Ebene des Protokollstacks. Die Verbindungen durch solch ein Gateway erscheinen einer entfernten Maschine, als bestünden sie mit dem Firewall-Host und lassen somit Informationen über geschützte Netzwerke verbergen.

- Application Gateways (Proxy), stellen ein anderes Firewall-Konzept dar. Für jede zulässige Anwendung wird auf dem FIrewall-Host ein eigenes Gateway-Programm installiert. Jedoch verlangt das Proxy-Programm oftmals nach einer Authentifizierung vom Client. Hier fungiert der Proxy dann als Stellvertreter für den Client und führt alle seine Aktionen im LAN aus. Damit lassen sich sowohl benutzerspezifische Zugangsprofile erstellen als auch zulässige Verbindungen anwendungsbezogen vornehmen.

10. Zusammenfassung

Wir hoffen, dass wir euch mit dieser Arbeit, die Netzwerkkomponenten ein wenig näher bringen konnten und hoffen verdeutlicht zu haben, dass hinter den stillschweigenden und unsichtbaren Maschinen im Hintergrund mehr steckt.
Auch in Zukunft wird sich im Netzwerkbereich noch eine Menge tun. So werden z.B immer schnellere und zuverlässigere Netzverbindungen auf den Markt kommen, WLAN wird auch in Österreich nachziehen in punkto Geschwindigkeit mit Amerika und das wichtigste ist, dass immer mehr Geräte im Haushalt vernetzt werden. So wird man Heizung, Licht, Kühlschrank, Klimaanlage, Toaster etc über den Computer steuern können.

11. Bibliographie

[1] Andrew Tanenbaum: Computer Networks, Prentice Hall. Kap. 4.4, 5.4 (*)

[2] Firewalls: http://www.knopper.net/firewall/firewall.html

[3] Google Suchmaschine: http://www.google.at/

[4] Grundlagen Computernetze: http://www.netzmafia.de/skripten/netze/index.html

[5] Skript an der Uni Bielefeld:
http://www.rvs.uni-bielefeld.de/~mblume/seminar/ss97/ethernet

[6] tecChannel: http://www.tecchannel.de

[7] World of Windows Networking: http://www.wown.com/