Kopplung von Netzwerken

13.1 Aktive Komponenten

Geräteübersicht

Zur Vergrößerung von Netzwerken bzw. zur Überwindung vorhandener Einschränkungen wie Längen oder Bandbreitenengpässe gibt es verschiedene Geräte unterschiedlicher Funktionalität.

Je höher die Einbindung eines Gerätes im Referenzmodell erfolgt, desto komplexer ist die in ihm realisierte Funktionalität.

Angelehnt an das OSI-Modell zeigt die folgende Tabelle eine Übersicht von aktiven Netzwerkkomponenten, auch wenn diese z. T. nicht mehr marktüblich sind.

OSI-Schicht	Netzwerkkomponenten	Kennzeichen
7	Gateway, Proxy, Application-Layer-Firewall	Protokollumsetzung auf Applikationsebene
4	Layer-4-Switch, Stateful-Inspection-Firewall	Segmentierung, Fehlerkorrektur (TCP), Portfilterung
3	Router, Multilayerswitch (Layer-3-Switch), Paketfirewall	Routing, IPv4/IPv6-Adressierung, IP-Filterung
2	Bridge, Switch, Accesspoint, Netzwerkadapter	Switching, MAC-Adressierung. Daten werden zur Übertragung in Frames (Datagramme) gepackt.
1	Repeater, Hub, Medienkonverter	Signalregenerierung, Autonegotiation, Autosensing

Sie können Netzwerkkomponenten unterschiedlicher Hersteller miteinander kombinieren. Einige Hersteller haben jedoch zusätzliche proprietäre Erweiterungen implementiert, um sich im Netzwerkmarkt abzugrenzen.

Dadurch stellt sich die Frage, ob man ein homogenes Netzwerk (alle Komponenten von einem Hersteller) oder ein heterogenes Netzwerk (Komponenten von verschiedenen Herstellern) aufbaut.

Den ersten Punkt sollten Sie in Betracht ziehen, wenn Sie Netzwerke konzipieren und einen einheitlichen Standard für die Wartung und das Management bevorzugen. Der zweite Punkt findet Anwendung, sofern Sie in Teilbereichen Ihres Netzwerkes besondere (manchmal nicht standardkonforme) Lösungen benötigen.

13.2 Repeater und Hub (Schicht 1)

Repeater

Ein Repeater verbindet physikalische Medien (auf Layer 1 des OSI-Referenzmodells), um die vorgegebenen Längenbeschränkungen des Mediums zu erweitern.

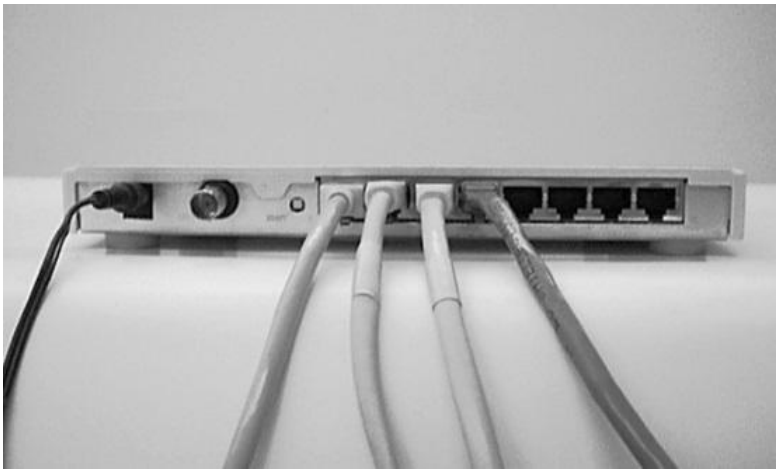
Er ist ein Signalregenerator zwischen Ein- und Ausgangsport. Repeater werden auch als Link Extender bezeichnet.

Verbindet ein Repeater unterschiedliche Medien (z. B. Twisted-Pair-Kabel mit Lichtwellenleitern), spricht man von einem Medienkonverter.

Hub (veraltet)

Ein Hub (englisch für „Nabe“, „Mittelpunkt“) ist ein zentraler Verteiler, basierend auf einer klassischen Bus-Topologie. Er wird auch als Kabelkonzentrator bezeichnet. Ein Hub arbeitet wie ein Repeater auf der Schicht 1 des OSI-Modells und wird deshalb auch Multiportrepeater genannt.

Eine solche Anschlussstelle wird als Port bezeichnet (hier z.B. ein 8-Port-Hub).



Hubs finden in aktuellen Netzwerken keine Anwendung mehr, da sie vollständig durch Switches ersetzt wurden. Zudem müssen sich bei Hubs alle angeschlossenen Geräte die verfügbare Bandbreite teilen.

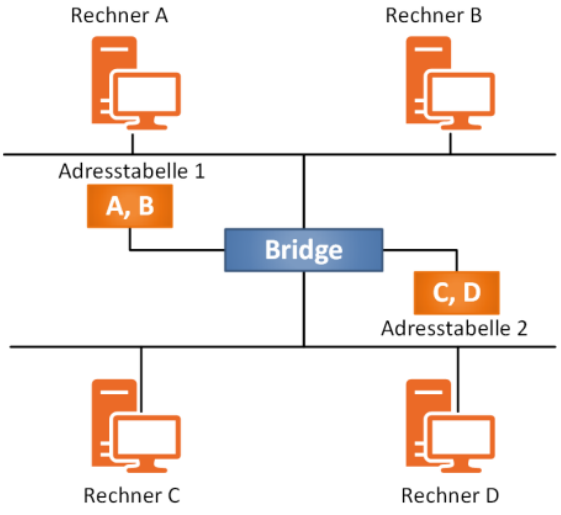
OSI-Einordnung und Beschreibung

Repeater und Hubs arbeiten auf der Schicht 1 des OSI-Modells, d. h., sie regenerieren nur die Bitströme, die über die Medien gesendet werden, haben aber keinen Einblick in den Inhalt der Informationen.

13.3 Bridge (Schicht 2)

Definition

Eine Bridge verbindet lokale Netzwerk-Segmente miteinander. Sie verfügt über zwei Ports und arbeitet auf der Schicht 2 des OSI-Modells. Dabei leitet sie die Frames anhand der MAC-Adresse Informationen weiter.



Im Unterschied zu Repeater oder Hub kann eine Bridge unterschiedliche Übertragungsraten und unterschiedliche Zugriffsverfahren auf den Ports umsetzen.

Arbeitsweise

Eine Bridge transportiert Datenframes anhand ihrer MAC-Adressen zwischen den angeschlossenen Segmenten. In der Abbildung oben rechts sieht man die Aufteilung eines Netzwerkes in zwei Segmente (eines mit Rechner A und B und ein weiteres mit Rechner C und D).

Die MAC-Adresse bzw. die Ethernet-Adresse ist die Adresse der Netzwerk-Schnittstelle (vgl. Kapitel 11). Für diese Aufgabe verwaltet die Bridge für jeden Port Adresstabellen (Forwarding Database, FDB), in denen die MAC-Adressen der angeschlossenen Stationen eingetragen sind. In der Praxis wird allerdings kaum noch eine Bridge verwendet, da ein Switch (vgl. Kapitel 13.4) flexibler ist.

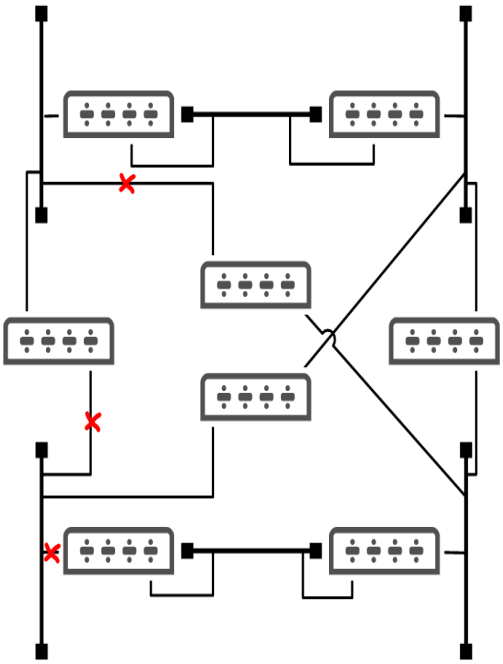
Learning Bridge

Als „Learning Bridge“ wird eine Bridge bezeichnet, die ihre Adresstabellen automatisch aufbaut und während des Betriebs selbständig aktualisiert.

Mit diesen Adresstabellen trägt eine Bridge dazu bei, den Netzverkehr zwischen den einzelnen Segmenten zu reduzieren.

Spanning-Tree-Algorithmus

Bei Bridges wird sehr häufig das Spanning-Tree-Protokoll (STP) eingesetzt. Spanning Tree ist ein Verfahren zur Unterdrückung von Schleifen in Netzwerken, die sich ergeben, wenn redundante Wege zu gleichen Netzwerkzielen existieren.



Gibt es mehrere Wege zwischen Sender und Empfänger, können Frames, wie in einer Schleife (Loop), immer wieder von einer Bridge zur nächsten weitergereicht werden. Dieses x-malige Weiterreichen führt dazu, dass das Netz durch Überlastung zum Stillstand kommt.

Spanning Tree legt in einem Netz einen eindeutigen Weg zwischen Sender und Empfänger über Bridges fest und blockiert redundante Verbindungen innerhalb des Normalbetriebs.

Dieses Protokoll findet auch bei Switches Anwendung. Neben dem Protokoll Spanning Tree (IEEE 802.1D) gibt es die beschleunigten Versionen Rapid Spanning Tree (IEEE 802.1W) und Multiple Spanning Tree (IEEE 802.1S). Beim Meshing (nach IEEE 802.1aq) definieren geeignete Switches dennoch Schleifen zur Redundanz und für höhere Übertragungsraten. Ein Beispiel ist die Topologie Maschennetz.

13.4 Switch (Schicht 2)

Definition

Ein Switch (engl. für „Schalter“) ist quasi eine Multiport-Bridge, welche die Vorteile einer Bridge auf mehrere Ports überträgt.

Durch Schalten („switchen“) von Verbindungen ist es für miteinander kommunizierende Geräte so, als ob sie direkt miteinander verbunden wären.

Per Kaskadierung lässt sich mit Switchen eine Vergrößerung der Gesamtportanzahl ermöglichen. Dabei bilden diese Verbindungen einen Flaschenhals für den Datenverkehr, und die Latenzzeit erhöht sich. Dieses Problem wird mit Stacking gelöst (vgl. Kapitel 12.4). Vor allem bei einer Kaskadierung können sehr viele Geräte miteinander verbunden sein, daher verfügen bereits einfache Desktop-Switches über internen Speicherplatz für 1000 und mehr MAC-Adressen.

19"-Switches: Managed ., Unmanaged und Webinterface des Managed Switches

Sogenannte Managed Switches können konfiguriert werden (meist per Webinterface). Desktop-Switches sind in der Regel unmanaged und damit nicht konfigurierbar, aber dafür sofort einsetzbar. Managed Switches benötigen eine eigene IP-Adresse zur Konfiguration.

Arbeitsweise

Damit ein Switch schnell die Frames zwischen den Ports vermitteln kann, muss er über eine interne Verdrahtung (Backplane) mit sehr hoher Geschwindigkeit verfügen.

Ein Switch kann im Prinzip mit einer Telefonanlage verglichen werden, bei der zeitlich begrenzt zwischen kommunizierenden Telefonen eine exklusive Verbindung besteht. Die für diese Verbindung benutzten Ports können so mit ihrer maximalen Geschwindigkeit arbeiten.

Bei serverbasierten Netzwerken, bei denen nahezu alle Arbeitsstationen Daten vom gleichen Server benötigen, ist dies für die Verbindung zum Server nicht mehr der Fall. Kollisionen werden dabei durch die Flusskontrolle der Übertragung vermieden.

Flusskontrolle der Übertragung

Im Duplexmodus wird durch Pause-Frames den sendewilligen Geräten signalisiert, eine Pause per Flow-Control nach IEEE 802.3x einzulegen, falls der Port mit der Leitung zum Empfänger bereits mit der Übertragung von einem anderen Frame belegt ist.

Bei Priority Flow Control (PFC nach IEEE 802.1p von 1998, bzw. Priority based Flow Control nach IEEE 802.1Qbb ab 2008) wird auf OSI-Layer 2 von einem Switch ein 3 Bit großes Feld (PCP, Priority Code Point) in das 4 Byte lange VLAN-Tag des Ethernet-Frames eingefügt.

Etliche Switches haben die Funktion Auto-VoIP, mit der sie automatisch VoIP-Pakete erkennen und passende VLAN-Tags generieren.

Prioritäten können auch von Einträgen im IP-Header auf Layer 3 stammen, die dort als Differentiated Service Codepoint (DSCP)-Flag bzw. Type of Service (ToS) bekannt sind. Diese Einstellungen bleiben auf dem gesamten Weg bis zum Empfänger erhalten. Ein derartiger Switch (Layer-3-Switch bzw. Smart-Switch genannt) kann daher Ethernet-Frames bis zum IP-Header auf Layer 3 auspacken, um die eingebetteten Information auszuwerten.

Mit Traffic Shaping beschleunigt sich die gesamte Übertragung, und damit verbessern sich auch Verbindungen von sensiblen Anwendungen wie VoIP. Etliche Managed Switches und DSL-Router (z. B. viele Fritz!Boxen) verwenden diese Technik, die auf VLAN-Tags verzichtet.

Die verschiedenen Modi der Weiterleitung

Sowohl bei einem Switch als auch bei einer Bridge haben sich grundsätzlich folgende drei Verfahren etabliert, wobei die Ports zwischen den Verfahren nach Bedarf umschalten können. Dies hängt von den angeschlossenen Stationen und der Ausstattung der Komponente ab.

Cut-Through

Beim Fast-Forward-Modus beginnt der Switch sofort mit dem Weiterleiten (Forward) der Daten zur Ziel-MAC-Adresse, nachdem er die Zieladresse gelesen hat. Diese befindet sich am Anfang des Ethernet-Frames.

Beim Fragment-Free-Modus prüft der Switch erst, ob der Frame die minimale Länge von 64 Byte hat, indem er die ersten 64 Bytes liest. Erst danach leitet er den Frame weiter (Forward). Kürzere Frames verwirft er. In beiden Modi von Cut-Through müssen die Ports gleiche Übertragungsraten und Übertragungsmedien haben. Anderenfalls weicht der Switch auf Store-and-Forward aus (wie z. B. beim Übergang von Twisted-Pair auf Glasfaser).

Der Nachteil dieser beiden Modi ist, dass bei der Übertragung nicht auf fehlerhafte oder unvollständige Frames geprüft wird. Dafür ist die Geschwindigkeit höher als im Store-and-Forward-Modus.

Store-and-Forward

Bei diesem Modus speichert der Switch den Frame vollständig zwischen, bevor er ihn zum Zielport weiterschickt. Store-and-Forward muss verwendet werden, wenn zwischen Quell- und Zielport unterschiedliche Übertragungsraten verwendet werden, z. B. von 1 Gbit/s nach 100 Mbit/s. Beim Zwischenspeichern überprüft der Switch die Daten auf Fehler anhand der im Ethernetframe vorhandenen FCS-Prüfsumme. Somit werden fehlerhafte Frames nicht weitergeleitet, was jedoch eine längere Latenzzeit zur Folge hat.

Error-Free-Cut-Through

Dies ist eine Mischform aus den vorgenannten Modi, zwischen denen der Switch je nach Qualität der Datenübertragung (Fehlerrate etc.) wechseln kann. Somit können je nach Situation die Vorteile aller oben genannten Modi kombiniert werden. Diesen Modus nennt man auch Adaptive Switching.

Interne Switcharchitektur

Auch bei der internen Behandlung der Frames gibt es bei Switches unterschiedliche Methoden. So bestehen bei einem Cross-Bar-Switch dedizierte Verbindungen zwischen allen Ports, was einen maximalen Datendurchsatz garantiert. Sobald der Weg zwischen Quelle und Ziel bekannt ist, werden die Daten über die entsprechende Verbindung weitergeleitet, ohne von anderem Datenverkehr behindert oder blockiert zu werden. Ein Nachteil dieser Methode liegt in der schlechteren Skalierbarkeit bei steigender Portzahl.

Beim Cell-Backplane-Switch kommunizieren alle Ports über einen schnellen internen Bus. Der Switch zerlegt die Frames in kleinere Zellen und fügt jeder Zelle einen Header mit der Adresse des Zielports hinzu. Dort werden die Zellen zwischengespeichert, zum Ausgangsframe zusammen gesetzt und endgültig an das Ziel weitergeleitet.

Weitere Entwicklungen

Etliche Hersteller bieten Hochleistungs-Switches an, die nicht nur auf der Schicht 2 des OSI Modells arbeiten, wie dies bei einem klassischen Switch der Fall ist, sondern auf Schicht 3 und höher handelt es sich um Multilayer-Switches.

Layer-3-Switching

In einem Netzwerk ohne Priority Flow Control sind prioritätsgesteuerte Übertragungen nur dann auf Layer 2 möglich, wenn der Switch nicht nur die ankommenden Frames weiterleitet, sondern zusätzlich auf Layer 3 die IP-Header analysiert und sie auf ToS-Attribute bzw. das DSCP-Flag untersucht (siehe „Flusskontrolle“ weiter oben). Von daher kommt der Ausdruck Layer-3-Switch.

Routing kommt erst dann hinzu, wenn ein zusätzliches Routermodul in ein derartiges Gerät eingebaut ist. In diesem Fall handelt es sich um ein Multifunktionsgerät. Ein Switch allein verbindet keine unterschiedlichen Netzwerke. Dennoch wird der Ausdruck „Layer-3-Switch“ oft fälschlicherweise als Synonym für Router benutzt.

Layer-4-Switching

Auf der Schicht 4 des OSI-Modells sind die Portnummern angesiedelt (vgl. Kapitel 11.2). Beim Layer-4-Switching stehen somit die Paket-Informationen der Schicht 4 zur Verfügung, sodass z. B. ein Administrator über Zugriffsregeln (Access Control List (ACL)) festlegen kann, welcher Verkehr vom Switch behandelt wird. Der Switch kann damit, abhängig von der Anwendung (deren Portnummer), eine Entscheidung über den Weitertransport eines Datenpaketes treffen und damit Datenverkehr filtern oder priorisieren. Damit können Sie eine einfache Paketfirewall einrichten.

Layer-7-Switching

Switche, die bis hinauf zur Schicht 7 arbeiten, können neben der Portnummer weitere Angaben, wie z. B. eine Web-Adresse, für die Steuerung des Datenverkehrs nutzen. Insbesondere auf dem Gebiet der Bereitstellung von Daten für Webanfragen werden solche Geräte eingesetzt.

Sie dienen im Rahmen von Serverfarmen dazu, gleichzeitige Anfragen von Tausenden von Clients per Load Balancing (Lastverteilung) auf die Server zu verteilen. Häufig finden sich daher für Layer- 7-Switche auch die Begriffe Load-Balancer, Web-Switches oder Content-Switches.

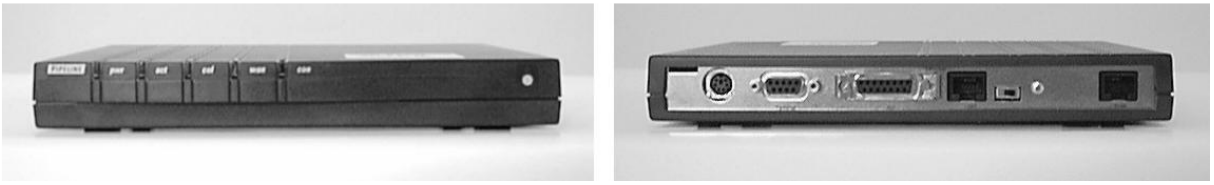
13.5 Router (Schicht 3)

Definition

Ein Router ist ein Gerät, das getrennte Netzwerke mit unterschiedlichen Adressräumen oder verschiedenen Netzwerktechnologien koppelt oder Netzwerke in Subnetze aufteilen kann. Die wesentliche Funktion ist die „Vermittlung“, oder anders gesagt, die Kenntnis der verschiedenen Netze und der Wege zu diesen Netzen.

Einordnung und Arbeitsweise

Die einfachste Form eines Routers ist ein PC mit mehreren Netzwerkadaptern, die jeweils Kontakt zu unterschiedlichen Netzwerken haben. Die Funktion „IP Forwarding“ muss dabei aktiviert sein, sonst erfolgt keine Weiterleitung der Pakete.



SOHO-Router (Vorder- und Rückseite)

Router arbeiten auf der Schicht 3 (Network/Vermittlung) des OSI-Modells. Das bedeutet, dass sie Netzwerke mit unterschiedlichen Topologien der darunter liegenden Schichten 1 und 2 verbinden können. Allerdings müssen alle beteiligten Netzwerke die gleiche Art der Adressierung ihrer Datenpakete verwenden, d. h. die gleichen Protokolle auf Schicht 3. Ist dies der Fall, z. B. beim Einsatz von IP-Adressen im Netzwerk, dann kann ein Router ankommende Frames bearbeiten und an ein anderes Netzwerk übergeben.

Dazu muss ein Router das IP-Paket des empfangenen Frames auf Schicht 3 auspacken, um aus dem IP-Header die IP-Adresse des Ziels zu ermitteln. Das IP-Paket selbst packt er nach der Ermittlung des weiteren Weges in einen neu erstellten Frame und schickt diesen über die entsprechende Schnittstelle in ein anderes Netzwerk weiter. Dieser Vorgang kostet Zeit, und so ist der Router im Normalfall langsamer als Switch oder Bridge.

Multiprotokollfähig

Ein wichtiges Unterscheidungskriterium von Routern ist die Frage, ob es sich bei dem Gerät um einen Einzelprotokoll- oder Multiprotokoll-Router handelt. Ein Router, der nur ein Protokoll kennt, ist lediglich in der Lage, Netzwerke mit gleichem Protokoll zu verbinden. (z. B. IPv4).

Ist der Router multiprotokollfähig, beherrscht er mehrere Protokolle, ohne diese zu vermischen (z. B. IPv4 und IPv6). Dies heißt aber nicht, dass ein Multiprotokoll-Router ein

Protokoll direkt in ein anderes umwandeln kann, sondern nur, dass er in der Lage ist, unterschiedliche Protokolle weiterzuleiten.

Tunneling

Mittels Tunneling können die Datenpakete eines Protokolls in den Nutzdaten (Payload) eines anderen Protokolls transportiert werden. Dies wird nötig, wenn ein Netzwerk überbrückt werden muss. Am Ende der Übertragung bzw. am Ende des „Tunnels“ wird der Transportrahmen entfernt, wodurch das Paket wieder in seinen ursprünglichen Zustand gebracht wird.

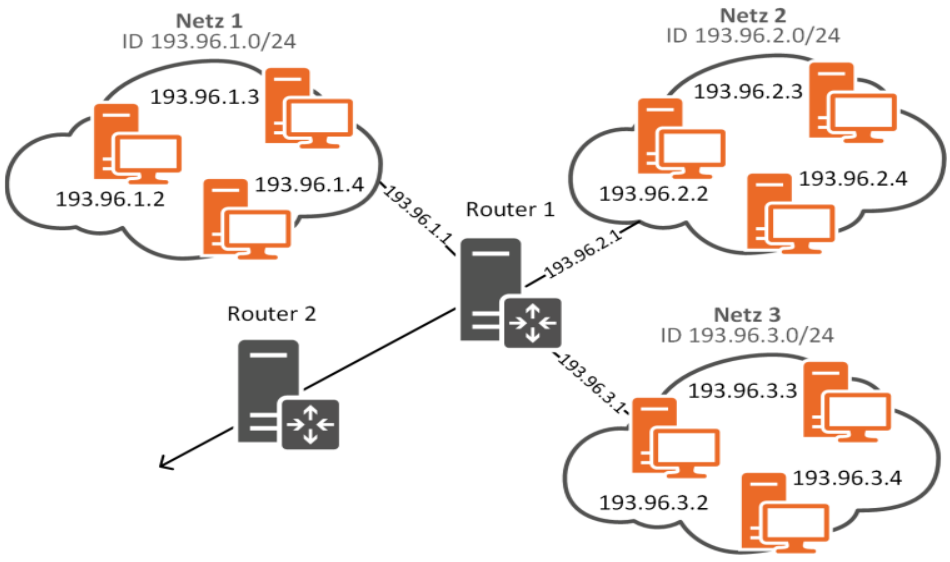
Ein Beispiel für solch ein Verfahren könnte der Transport von IPv6-Paketen über ein reines IPv4-Netzwerk sein. Damit können zwei IPv6-Netzwerke über ein IPv4-Netz gekoppelt werden. Beispiele für solche Verfahren sind 4in6, 6in4, Teredo.

Tunneling-Protokolle ermöglichen grundsätzlich nur eine erhöhte Sicherheit während der Übertragung, wenn sie auf Tunnel-Kryptografie aufsetzen. Hierzu werden u. a. die Protokolle Layer 2 Tunneling Protocol (L2TP) / IPsec, OpenVPN, und weitere verwendet.

Routing-Tabellen

Die Hauptfunktion eines Routers besteht in der Pfadbestimmung (Routing) für IP-Pakete zum Zielnetzwerk. Dazu verwenden Router sogenannte Routing-Tabellen (eine für jedes Routing protokoll), in denen die an dem Router direkt angeschlossenen Netzwerke (inkl. Netzmasken) und Wege zu benachbarten Netzen hinterlegt sind. Empfängt der Router ein IP-Paket und hat die geforderte Zieladresse ermittelt, muss er den weiteren Weg bestimmen.

Der Router prüft erst anhand der Einträge in den Routing-Tabellen, ob das Gerät mit der Ziel-Adresse direkt angeschlossen ist. Dann kann der Router das IP-Paket in einen neuen Frame packen und diesen direkt zum Ziel weiterleiten. Anderenfalls wird er das Paket an einen anderen Router weiterschicken. Dieser nächste Router, der auch als „Next Hop“ bezeichnet wird, versucht dann auf seine Weise das Paket weiter zuzustellen. Eine wichtige Voraussetzung dafür ist, dass die Time to live (TTL) des Pakets noch nicht den Wert 0 erreicht hat. Bei der TTL handelt es sich um einen Zähler, der von jedem Router reduziert wird, nachdem das Routing stattgefunden hat.



Default-Router

Nicht jeder Router kann die Wege zu allen Netzen kennen. Daher wurde als Lösung der Default-Router eingeführt. Alle Pakete, für die das Zielnetz unbekannt ist, werden einfach an den Default-Router weitergeleitet.

Jedes IP-fähige Gerät besitzt intern eine statische Routing-Tabelle. Dort ist in jedem Fall das eigene Netzwerk mit dessen Netzmaske eingetragen. Zusätzlich gibt es meistens einen Eintrag (die Default-Route) für unbekannte Wege zum Ziel.

Alle weiteren Einträge müssen beim statischen Routing manuell (z. B. vom Administrator) angelegt werden. Beim dynamischen Routing tauschen die Router ihre Routeninformationen miteinander aus und generieren die entsprechenden Tabellen selbst.

Ein Router trifft seine Routingentscheidung in folgender Reihenfolge:

1. Er prüft zunächst anhand der Einträge in den Routing-Tabellen und den dazugehörigen Netzmasken, ob sich die Zieladresse in einem direkt angeschlossenen Netzwerk befindet. Falls ja, ermittelt er die MAC-Adresse (Ethernet-Adresse) des Ziels über das Protokoll ARP und erzeugt ein Paket mit der MAC-Adresse des gewünschten Geräts.
2. Ist das Zielnetz über einen benachbarten Router zu erreichen, entscheidet der Router anhand seiner Metrik (Maß für die Güte einer Verbindung), welches der richtige Weg zum Ziel ist. Das kann z. B. der Weg mit der größten Bandbreite oder aber auch der Weg mit den geringsten Kosten sein. Weitere mögliche, zur Auswahl stehende Wege können durch statische Routing-Einträge vorgegeben sein oder sind Wege, die der Router mithilfe eines dynamischen Routing-Protokolls erlernt hat. Anhand dieser Wahl leitet er das IP-Paket zum nächsten passenden Router (Next Hop), indem er es in einem neuen Frame an dessen MAC-Adresse schickt.
3. Gibt es weder einen passenden Eintrag in der statischen noch in einer dynamischen Routing-Tabelle, ist der Weg zum Ziel unbekannt. In diesem Fall leitet der Router das IP-Paket an die MAC-Adresse des Routers, der als Default-Router (auch Gateway of Last Resort genannt) eingetragen ist. Dieser kümmert sich um die weitere Zustellung.
4. Findet er in der genannten Reihenfolge keinen verwertbaren Eintrag, so verwirft er das Paket und sendet die Nachricht „Zielnetz nicht erreichbar“ an den Absender.

Dynamische Routingprotokolle

Eine Alternative zur statischen Konfiguration von Routern schaffen dynamische Routingprotokolle, mit deren Hilfe Router benachbarte Netzwerke kennen lernen. Das Ergebnis könnte die Wegewahl auf Basis der kürzesten Verbindung, der aktuellen Lastsituation oder der günstigsten Verbindungskosten sein.

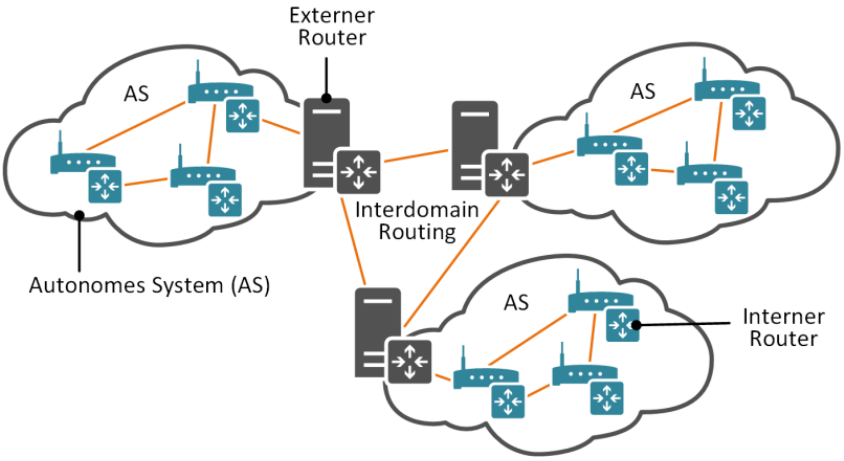
Interne/externe dynamische Routingprotokolle

Interne Routingprotokolle werden ausschließlich im Intranet, also im LAN selbst bzw. innerhalb von Autonomen Systemen, eingesetzt. Typische Vertreter sind die Standardprotokolle Routing Information Protocol (RIP) und Open Shortest Path First(OSPF). Externe Routingprotokolle finden Anwendung im WAN, also im Internet und zwischen

Autonomen Systemen. Ein Beispiel hierfür ist das Border Gateway Protocol (BGP), obwohl auch OSPF hierfür geeignet ist.

Autonomes System

Würde jeder Router alle verfügbaren Netze lernen, so käme er schnell an seine Grenzen. Aus diesem Grunde hat man Autonome Systeme (AS) eingeführt. Ein Router in einem AS erkennt nur seine Nachbarnetze.



Der Vorteil von AS besteht darin, dass die internen Router nur einen Teil der Netze kennen müssen und demzufolge ihre Routingentscheidung effizienter treffen können. Externe Router (auch Border-Router genannt) übernehmen die Vermittlung zwischen den AS. Vorrangig vernetzen sich ISP auf diese Weise (Interdomain Routing).

RIP

RIP war das erste dynamische Standardprotokoll. Es arbeitet nach dem Distanz-Vektor-Algorithmus, d. h., die Wegewahl wird anhand der geringsten Anzahl der Router (Hops) zwischen Quell- und Zielnetz getroffen. Dazu verschickt jeder Router seine Routinginformationen im 30-Sekundentakt an seine Nachbarn.

OSPF

Das Protokoll Open Shortest Path First (OSPF) ist ebenfalls ein dynamisches Routing-Protokoll und basiert auf der Link State Database. In dieser Datenbank sind alle benachbarten Router bzw. deren Link-Status enthalten, für die Aktualisierung der Datenbank der Router untereinander sind feste Regeln definiert.

Das OSPF-Protokoll berechnet die Güte eines Weges zu einem benachbarten Router anhand der Leitungskosten, d. h., je höher die verfügbare Bandbreite der Hops zwischen Quell- und Zielnetz ist, desto geringer sind die Kosten und desto günstiger ist der Weg dorthin.

BGP

Das Border Gateway Protocol (BGP) nutzt den Path-Vektor-Algorithmus, der ähnlich dem Distanz-Vektor-Algorithmus arbeitet. Jedoch können hierbei keine Routingschleifen auftreten. Es kann sowohl innerhalb eines Autonomen Systems als iBGP (internal BGP) als auch zwischen AS als eBGP (external BGP) eingesetzt werden.

Load Balancing

Die meisten Routing-Protokolle ermöglichen ein sogenanntes Load Balancing, was bedeutet, dass alternative Wege zur Zieladresse verwendet werden können. Load Balancing heißt, dass bei zwei gleichwertigen Wegen (gleiche Metrik) die Datenströme wechselseitig auf beide Wege verteilt werden.

13.6 Firewall

Sowohl zum Schutz des lokalen Netzes (Intranet) als auch zwischen Intranet und Internet ist heute die Filterung durch eine Firewall unabdingbar. Eine Firewall kann in Abhängigkeit von ihrem Funktionsumfang ein- und ausgehenden Datenverkehr auf den Layern 2 bis 7 des OSI Modells anhand festgelegter Regeln filtern. Dabei sind nur drei Aktionen erlaubt.

- Allow, der Verkehr wird über die Firewall durchgelassen.
- Deny, die Firewall verwirft die ankommenden Daten, wobei der Sender keine oder die Nachricht „Time Out“ bekommt.
- Reject, die Daten werden von der Firewall abgewiesen und der Sender erhält eine Fehlermitteilung.

Paketfilter

Paketfilter stellen eine einfache Variante einer Firewall dar. Hierbei wird der Header der Layer-3-Protokolle (z. B. IP-Header, ICMP-Header) bzw. der Layer-4-Protokolle (TCP-Header, UDP-Header) überprüft und in Abhängigkeit der eingestellten Filter-Regeln eine Aktion ausgelöst. Aufgrund der geringen Komplexität ergibt sich ein guter Datendurchsatz (Performance). Nachteilig ist jedoch, dass u. a. der Missbrauch von Protokollfunktionen (z. B. Fragmentierungs-Attacken oder Buffer Overflow) möglich ist. Zudem ist eine Verschleierung durch Verwendung erlaubter Ports für auf Port x nicht erlaubte bzw. vorgesehene Anwendungen möglich, ohne dass der Paketfilter diese unerwünschten Daten herausfiltern kann.

Stateful Inspection Firewall

Sie ist eine Weiterentwicklung des Paketfilters. Zusätzlich ist sie jedoch in der Lage, sich aktuelle Status- und Kontextinformationen zu merken bzw. diese bei der Filterung zu berücksichtigen.

Damit lässt sie (wie z. B. in den meisten DSL-Routern vorhanden) nur Antwort-Pakete auf Anfragen ins Internet in das interne Netz zurück passieren, während sie alle anderen Pakete aus dem Internet blockiert. Über Ausnahmeregeln können bestimmte Verbindungen dennoch erlaubt werden. Auf diese Weise kann z. B. eine Fragmentierungs-Attacke verhindert oder ein manipulierter Verbindungsaufbau erkannt und unterbunden werden.

Durch spezielle Filterregeln kann zudem ein Schutz vor etlichen Denial of Service (DoS-Attacken) erreicht werden, indem die Anzahl der Verbindungsaufnahmen pro Sekunde begrenzt wird. Dos-Attacken zielen auf die Verfügbarkeit des Systems durch Überflutung mit Anfragen.

Application Level Firewalls (ALF) /Proxy-Server

Die Application Level Firewall arbeitet auf Layer 7 des OSI-Modells und wird zwischen Client und Server geschaltet. Sie fungiert in Richtung Client als stellvertretender Server und gegenüber dem Server als stellvertretender Client. Für jeden Dienst wird eine eigene Applikation (Proxy) benötigt. Über generische Proxys kann man jedoch einige Dienste zusammenfassen. Der Proxy überwacht den kompletten Verkehr bis zur Applikationsebene, und die vor dem Proxy liegenden Netze sind von „außen“ nicht sichtbar. Durch die hohe Komplexität hat eine ALF eine geringere Systemperformance.

Weitere Firewalltypen

Die folgenden Typen beinhalten die oben beschriebenen Implementierungsverfahren:

- Transparent Firewall – Sonderform der Stateless oder Stateful Inspection Firewall, filtert ab Layer 2 und verhält sich im Netzwerk transparent gegenüber den Kommunikationspartnern. Diese sehen in der Firewall quasi nur einen Router ohne dahinterliegendes Netzwerk.
- Personal Firewall/Desktop Firewall – wird nicht im Netz, sondern auf den Endsystemen als Programm/ Dienst installiert (bzw. ist bereits in das Betriebssystem integriert) und stellt eine Mischung aus Paketfilter und Stateless oder Stateful Inspection Firewall dar. Zudem können auf dem Endsystem installierte Programme von der Firewall berücksichtigt werden.
- Application Inspection/Next Generation Firewall – untersucht den Datenstrom auf Applikationsebene, erkennt unterschiedliche Anwendungen und kann Sicherheitsrichtlinien auf Applikations- und Nutzerebene umsetzen.
- Unified Threat Management (UTM) – steht für zentrale Sicherheit für das gesamte Netzwerk. Damit wird versucht, verschiedene Schutzfunktionen unter einem Dach zu vereinen. Wichtige Bestandteile davon sind ein Intrusion Detection System, Contentfilter und Virus- sowie Spam- und Surf Protection.

Das Thema Network Address Translation (NAT) spielt bei Firewalls eine wichtige Rolle im Bezug darauf, wie die Firewall gegenüber anderen Netzwerkteilnehmern in Erscheinung tritt.

13.7 Gateway (Schicht 7)

Vermittlung auf allen Schichten

Gateways verbinden Netzwerke mit völlig unterschiedlichen Protokollen und Adressierungen, sie stehen als Oberbegriff für die Vermittlung und Umwandlung auf allen 7 Schichten des OSI-Modells.

Ein Gateway kann damit inkompatible Netze miteinander verbinden und im Extremfall eine ankommende Nachricht bis auf Schicht 7 entpacken, um sie dann für das andere Netz passend wieder bis auf Schicht 1 zu verpacken. Ein Gateway wandelt also real ein Protokoll in ein anderes um.

Der Begriff Gateway wird teilweise auch als Synonym für Router verwendet.

13.8 Multifunktionsgeräte

Viele Geräte enthalten mehrere Komponenten. Man spricht in diesem Zusammenhang von Multifunktionsgeräten (siehe Bild rechts, DSL-Router mit Access Point und Switch mit 4 LAN-Ports). Ein derartiges Gerät kann auch als Gateway (zum Internet) angesehen werden.