

Netzwerktechnologien und multimediale Teledienste


Netzwerke/Basistechnologien




Universität
Potsdam
Institut für
Informatik

Routing / Interworking

Prof. Dr. Ing. Klaus Rebensburg


Netzwerktechnologien und multimediale Teledienste

Worum geht's?



Universität
Potsdam
Institut für
Informatik

Routing / Inter-Networking


Dienste sollen von einem Ort an beliebigen anderen Orten zur Verfügung gestellt werden. oder (profaner)

Es sollen **Datenpakete** zwischen zwei (oder mehr) Programmen an **geographisch unterschiedliche Orte** (mit bestimmten **Dienstgütern** /Qualitäten) übertragen werden.

Forwarding von Paketen wäre die Sicht eines Netzknotens zum nächsten


Die Lenkung der Ströme kann **fest(statisch), alternativ oder adaptiv(dynamisch)** sein.

2


Netzwerktechnologien und multimediale Teledienste

Worum geht's?

Beispiel : Voice over IP (VoIP)

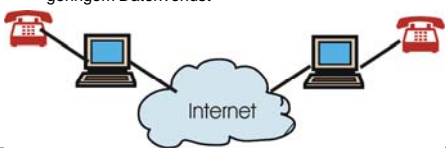


Universität
Potsdam
Institut für
Informatik

Anforderungen:

ein **logischer Datenkanal** zwischen zwei Telefonierenden mit

- definierter Bandbreite
- geringem Delay
- geringer Varianz der Datenpakete
- geringem Datenverlust



3



Worum geht´s? Beispiel : Voice over IP (VoIP)

Netzwerktechnologien
und multimediale
Teledienste



Bandbreite

Wenn die Bandbreite nicht reicht,
dann klingt Sprache dumpf und ist unverständlich
Heutige Sprachcodierer mit ihren Kompressionsverfahren und
Sprachpausenunterdrückung verringern die zu übertragende
Bandbreite auf eine Brutto-Bandbreite von ca. 17 kBit/s.

Zeitliche Verzögerungen (Delay)

Grosse Verzögerungen machen eine verständliche
Kommunikation zwischen Gesprächspartnern unmöglich.

Universität
Potsdam
Institut für
Informatik

4



Worum geht´s bei QoS? Beispiel : Voice over IP (VoIP)

Netzwerktechnologien
und multimediale
Teledienste



Zeitliche Varianz (Jitter)

Das menschliche Ohr reagiert empfindlich auf zeitliche
Asynchronitäten bei der Sprachkommunikation.
Irritationen sind die Folge.

Paketverluste

Paketverluste hört man.
Der Algorithmus der Sprachcodierer lässt es zu, mit geringen
Informationsverlusten eine gleichbleibende Sprachqualität zu
liefern.

Universität
Potsdam
Institut für
Informatik

5

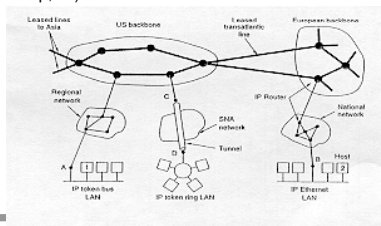


Wo ist das Problem?

Netzwerktechnologien
und multimediale
Teledienste



Es existiert eine historisch gewachsene und extrem heterogene
Netzwerkinfrastruktur verteilt über den ganzen Globus.
Wir haben gleichzeitig eine standardisierte Protokollwelt durch
die Internetprotokolle (TCP,UDP,IP,...) und Dienste (telnet, ftp,
http,)



Universität
Potsdam
Institut für
Informatik

6

Wo ist das Problem?



Früher bestand das vorrangige Problem darin, Standardprotokolle überall auf den jeweiligen meist festen **Netzwerkstrukturen** benutzen zu können und die Prinzipien für das **Verteilen der Pakete** im Netz zu etablieren

Heute ist das zusätzliche Problem,

- dieses auch drahtlos zu tun,
- Dieses auch mobil zu tun,
- dieses mit den erforderlichen **Qualitäten** zu können.

Wie wird das Problem gelöst?



Verbindung der verschiedenen Netzwerkinseln zu einer umfassenden Netzwerkinfrastruktur

1. Kabel + Übertragungsverfahren
 2. Netzwerkprotokolle
 3. Komponenten
2. Bereitstellung eines Identifikationsschemas für Prozesse auf beliebigen Rechnern im Netz sowie die nötigen Datentransportmechanismen: Internetprotokolle
1. TCP, UDP, IP
 2. Routingprotokolle
 - RIP
 - OSPF

Wie wird das Problem gelöst?



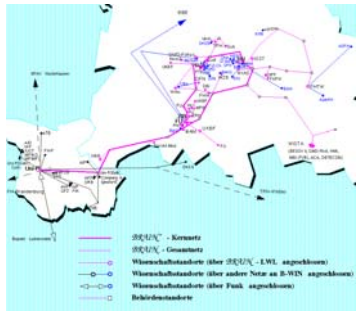
3. Bereitstellung der darauf basierenden Dienste und Qualitätssicherungsprotokolle

- Dienste
- RSVP



Z.B. Kabel+Übertragungsverfahren Die BRAIN Infrastruktur

Netzwerktechnologien
und multimediale
Tele Dienste



Berlin
Research
and
Information
Network

Universität
Potsdam
Institut für
Informatik

10



Netzwerktechnologien

Netzwerktechnologien
und multimediale
Tele Dienste



Technologien im Einsatz (heterogen):

- Ethernet (10 Mbit/s, 100 Mbit/s, 1 Gbit/s)
- FDDI (100 Mbit/s)
- ATM (155 Mbit/s, 622 Mbit/s, 2,5 Gbit/s),
- Token Ring / High Speed Token Ring (HSTR) (10 Mbit/s, 1 Gbit/s)

Universität
Potsdam
Institut für
Informatik

11



Netzwerkcomponenten Netzverkopplung

Netzwerktechnologien
und multimediale
Tele Dienste



Router, Bridges oder Gateways **verbinden** nicht nur Netze, sie können auch zur **logischen Separierung** von Netzen dienen. Die Aufteilung von großen Netzen in Subnetze verbessert die **Verfügbarkeit**, da ein Fehler nur einen begrenzten Bereich des Netzes betrifft und dort schneller lokalisiert werden kann. Bei zunehmender Anzahl von Netzstationen werden (interne) Antwortzeiten unakzeptabel und eine Subnetzbildung zur **Lasttrennung** wird notwendig. Der **Schutz von sensiblen Informationen** kann ein weiterer Grund zur Segmentierung von Netzen sein, damit diese nicht auf dem Gesamtnetz verfügbar sind.

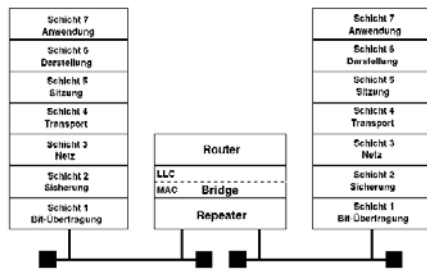
Universität
Potsdam
Institut für
Informatik

12



Um sich vor **externen Angreifern** zu schützen, kann es sinnvoll sein, Pakete **nur** vom **sicheren** ins **unsichere** Netz zuzulassen.

Zum Schutz von vertraulichen Daten kann es andererseits sinnvoll sein, keine Pakete vom sicheren ins unsichere Netz zuzulassen.



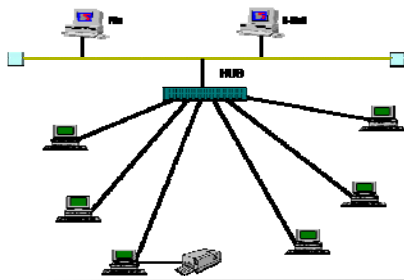


- HUB
- (Multiport-) Repeater
- Bridge
- Switch
- Router
- Access-Router
- Brouter
- Gateway



Wiederholung: Was ist ein HUB?

Ein Hub ist ein logischer Zwischenpunkt, ein Vermittlungsknoten in einem LAN. Das Wort Hub wird häufig auch synonym für **Sternkoppler** benutzt. Hubs haben als Basisfunktionen die **Aufbereitung von Signalamplituden**, Kollisionserkennung und Signalweiterleitung zu Hubs niedrigerer Ordnung und Endgeräten.





Ein (**Multiport**) **Repeater** kopiert Ethernet-Frames zwischen den verschiedenen Segmenten einer Collision-Domain hin und her. Repeater sind Verstärker, die auf **Layer 1** des OSI-Modells arbeiten und die Signale verstärken. Kollidieren Signale auf einem Segment, so **trennt** ein Repeater die beiden Segmente, damit sich die Kollision nicht auf alle Segmente ausdehnt. Mit Repeatern kann die maximale Länge eines Kabelsegmentes **verlängert** werden. Wegen der zeitlichen Rahmenbedingungen von Ethernet dürfen max. 2 Repeater in einer Strecke zwischen 2 Systemen vorhanden sein. Vorteil: Kollisionsminderung.

Wiederholung: Was ist eine Bridge?



Eine Bridge verbindet zwei Netze, die in der Regel dasselbe **Logical Link Control Protokoll (LLC)** benutzen, aber unterschiedliche Medium Access Control Protokolle.

Eine Bridge kann z. B. ein Ethernet mit einem Token-Ring-Netz verbinden.

Eine Bridge ist in der Lage, alle im Netz vorkommenden Adressen zu erlernen und Routingtabellen aufzubauen.

Eine Bridge übermittelt nur Daten, die in ein anderes Netzsegment gesendet werden sollen, wodurch eine Lasttrennung möglich ist (store and forward-Prinzip)

Weitere Filtermechanismen erlauben die Einführung von Zugriffskontrollen.

Filter können sich auf Ziel- oder Quelladressen oder Protokolltypen beziehen.

Wiederholung: Was ist ein Switch ?



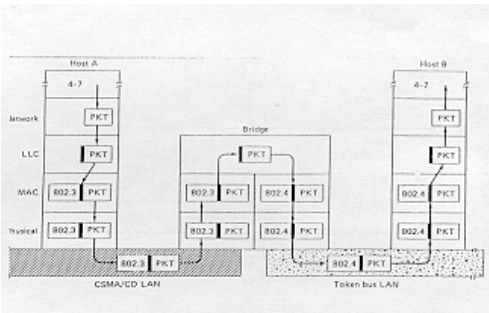
Ein Switch ist (oft) eine Multiport-Bridge

Performance Probleme bei Fast Ethernet/Gigabit-Switches

Vorteile:

- Unterteilung von Netzen in überschaubare Einheiten, erleichterte Isolierung von Fehlern,
- Lasttrennung (Performanceverbesserung),
- Implementierung von Subnetzen mit unterschiedlichen Sicherheitsstufen,
- Zugriffskontrolle auf MAC-Ebene möglich,
- Filterung von nichtautorisierten Datenpaketen.

Was ist eine Bridge / Switch ?





- **Route** Weg eines Datenpaketes vom Sender zum Empfänger.
- Den Prozess der Wegwahl nennt man Routing
- Der Weg kann statisch vorbestimmt sein, oder dynamisch den Bedingungen im Netz angepasst sein.
- Intelligente Wegwahl ist notwendig in Netzen (Maschen/Schleifen mit gewichteten Kanten)



Spanning-Tree ist ein Verfahren zur Schleifenunterdrückung in Brücken - gekoppelten Netzen. Bei diesem Verfahren werden **physikalisch redundante** Netzstrukturen ermittelt und in eine **zyklenfreien Struktur** abgebildet.

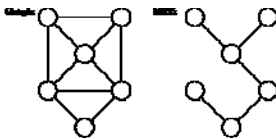


Minimum Spanning Tree

Eine Anwendung für den Union/Find-Algorithmus ist der Minimum Spanning Tree (MST).

Ein Spannbaum ist eine minimale Menge von Kanten eines Graphen, die alle Knoten des Graphen verbindet.

Beispiel:





Algorithmus von Prim

Ein schnellerer Algorithmus (als der von Kruskal) zur Berechnung des MST ist der Algorithmus von Prim.

Starte mit einem Knoten.

Wähle die billigste Kante, die den bisher aufgebauten Baum mit dem Rest verbindet.

genauer:

Initialisiere einen Baum mit dem Knoten A

Initialisiere Heap mit den Nachbarn von A

REPEAT

entferne den billigsten Knoten x aus dem Heap

füge x dem Baum hinzu

update den Heap

UNTIL heap_is_empty



Ein Router „kopiert“ IP-Pakete zwischen verschiedenen IP-Segmenten hin und her.

Dabei können dort unterschiedliche MAC-Layer verwendet werden (Ethernet, FDDI, PPP, ATM,...)

Der Router wirkt auf dem Network-Layer

Access-Router vermitteln Datenpakete über Telefonnetz inkl. der Authentifizierung der Einwählenden.

Weitere Verwirrungen: Brouter sind Bridging-Router



- Eine Netzwerkkomponente, die mehrere Rechnernetze koppelt;
- Bei ihm eintreffende Netzwerk-Pakete eines Protokolls werden auf Basis von Layer-3-Informationen analysiert
- und zum vorgesehenen Zielnetz (Ziel-Subnetze) weitergeleitet oder *geroutet*.



- **Medienunabhängig :**
die Schnittstellen eines Routers sind Teile unterschiedlicher Netze (wie Token Ring, Ethernet, WLAN – aber auch ISDN oder ATM).
Ein Router kann auch über eine einzige Schnittstelle verfügen und vermittelt dann das Protokoll zwischen unterschiedlichen logischen Netzwerken auf demselben physikalischen Medium (auch *router on a stick* genannt).
- **Protokollabhängigkeit**
ein Router leitet nur ihm bekannte Protokolle der Schicht 3 des OSI-Referenzmodells weiter.
Ein Router, der mehrere Protokolle weiterleitet (z. B. IP und IPX), heißt **Multi-Protocol-Router**.



- Kombinationen verschiedener Komponenten
- DSL-Modem (oder genauer gesagt ADSL-Modem) & Router = **ADSL-Router** oder **DSL-Router** bezeichnet.
Das heißt, keine vollständigen Router, nur Internetzugangs-Systeme nur mit aktiviertem PPPoE oder PPPoA sowie NAT-Routing (oder IP-Masquerading).
Oft DSL-Router, auch wenn über ein externes Modem per ADSL mit dem Internet verbunden.
 - Kombination aus Access Point und Router = **WLAN-Router** .
(wenn es einen WAN-Port gibt).
Routing zwischen WLAN und WAN
(und falls vorhanden auch zwischen LAN und WAN).
Fehlt WAN-Port, dann gelogen, da reine Access Points auf OSI-Ebene 2 arbeiten und somit Bridges und keine Router sind.
Häufig WLAN-Router keine vollwertigen Router,
Oft gleiche Einschränkungen wie DSL-Router (PPPoE, NAT – siehe oben).



- Software-Router multifunktional, aber I/O Beschränkungen.
- PCI-Bus mit 32-Bit Busbreite und ...-MHz-Taktung
- Über einen solchen Bus lassen sich bis 1.000 MBit/s leiten;
- Netzwerkpakete passieren den PCI-Bus allerdings zweimal, (Karte-PCI-Arbeitsspeicher-CPU-Arbeitsspeicher-PCI-Karte)
- Reduktion dann auf ca 500 MBit/s



- Statisch
- Zentralisiert (adaptiv)
- Isoliert
 - Broadcast Routing
 - Hot Potato
 - Backward Learning
 - Delta-Routing
- Verteilt adaptiv
- Distance Vector
- Link State
- Hierarchisch
- Inter Domain (EGP)/Intra Domain



Internet Routingprotokolle:

- RIP, RIP2: IGP, Distance-Vector, Unicast
- IGRP: IGP, Distance-Vector, Unicast
- OSPF: IGP/EGP, Link-State, Unicast (Shortest Path First)
- EIGRP: IGP/EGP, Hybrid Distance-Vector/Link State, Unicast
- BGP EGP, AS Pathes, Unicast
- DVMRP IGP/EGP, Distance-Vector, Multicast



- Gleichzeitige Nutzung von Routing-Protokolle aus verschiedenen Klassen:
- **Interior Gateway Protocols (IGPs)** tauschen Routing-Informationen in einem einzelnen autonomen System.
 - IGRP/EIGRP (Interior Gateway Routing Protocol/ Enhanced IGRP)
 - OSPF (Open Shortest Path First)
 - IS-IS (Intermediate System to Intermediate System)
 - RIP (Routing Information Protocol)
 - **Exterior Gateway Protocols (EGPs)** Routing zwischen autonomen Systemen.
 - BGP (Border Gateway Protocol: ist weltweit de-facto-Standard.
 - EGP (altes Exterior Gateway Protocol für Verbindung Internet-Backbones)
 - **Ad hoc Routing-Protokolle** n Netzen mit wenig oder keiner Infrastruktur
 - OLSR im mobilen Bereich.
 - AODV in kleineren Netzen mit hauptsächlich statischem Traffic



Übersicht/Zusammenfassung Routing-Protokolle

Routing-Protokoll	Routing-Algorithmus	Shortest Path-Algorithmus	Einsatz	Metrik	Anmerkungen
BGP	Path-Vector	Bellman-Ford	EGP	Policies	de Facto-Standard, verhindert Schleifen
RIP	DV	Bellman-Ford	IGP	Hop-Count	Count-to-Infinity-Problem
OSPF	LS	Dijkstra	IGP	*	hierarchisches Routing
IS-IS	LS	Dijkstra	IGP	*	ISO-Standard, vglb. mit OSPF
EIGRP	DV	DUAL	IGP	*	Cisco-Standard

*) verschiedene (teilweise kombinierbare) Metriken

Die Sicht darüber: Was ist ein Gateway?



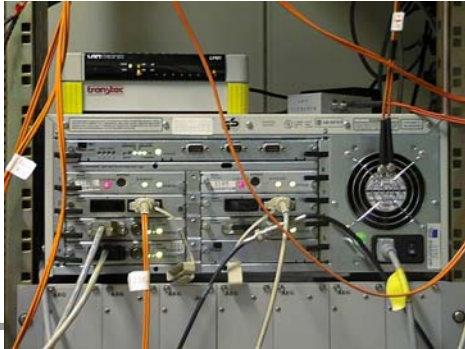
Gateways sind Protokoll-Konverter auf höheren Ebenen, die letztlich alles in alles konvertieren können.

WEB-Proxy, Email-Proxy,

Der Gateway wirkt auf den höheren Layern (>3)

3Com & HP Ethernet Switches







Architecture	Catalyst 6000 Series	Catalyst 6500 Series
Backplane Bandwidth	32 Gbps	32 to 256 Gbps
Number of Gigabit Ethernet ports	130	130
Number of 100FX Ethernet ports	192	192
Number of 10/100 Ethernet ports	384	384



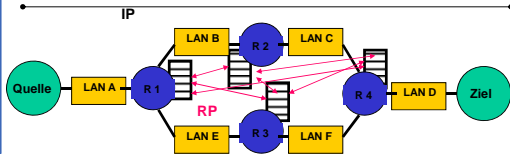
- Übertragungsprotokolle
 - TCP, UDP, IP, IPv6
- IP - Routingprotokolle
 - Prinzip des Routings
 - Schicht 2 Routing
 - Schicht 3 Routing
 - Routing Protokolle
 - VPN's
 - VLAN's



- **TCP, UDP**
sind Transportprotokolle der OSI-Schicht 4
 - **IP, IPV6**
sind Netzwerkprotokolle der OSI-Schicht 3
- IP bildet **zusammen mit diversen Routing Protokollen** die Grundlage für das Internet.



- IP überträgt Datenpakete zwischen Rechnern basierend auf **Routingtabellen**
- **Router** haben mehrere Interfaces
senden IP-Pakete in Abhängigkeit von der Routing-Tabelle in verschiedene Netzsegmente
- **Routingprotokolle** manipulieren Routing-Tabellen entsprechend gewünschter Strategien,





IPv6 ist eine neue Generation des IP-Protokolls der Internet-Schicht, welches von der IPhG, der Internet-Protocol-next-Generation Group entwickelt wurde aufgrund folgender praktischer Probleme:

- Die maximal verfügbare Anzahl von Adressen reicht nicht aus, da maximal 32 Bit für die Adressierung der Host-Rechner benutzt werden können.
- 32 Bit-Adressierung reicht in großen Netzen nicht aus, um die erforderlichen Subnetze zu verwalten.



Übertragungsprotokolle IPv6 warum?

Netzwerktechnologien
und multimediale
Tele Dienste



- Die bisherige Version IP4 erzeugt **exponentiell wachsende Routingtabellen**, die von den Routern vollständig kaum noch ökonomisch zu verarbeiten sind.
- Nicht alle Router unterstützen sämtliche Protokolle, um das gesamte Leistungsspektrum von IP auszunutzen, da sie dann vermutlich sehr langsam wären.

Aufgrund dieser Probleme und anderen neuen Anforderungen an das Internet Protokoll haben die verschiedenen Initiativen folgende Merkmale herausgearbeitet, die für das neue IPv6 gelten sollen:

Universität
Potsdam
Institut für
Informatik

43



Übertragungsprotokolle IPv6 Header

Netzwerktechnologien
und multimediale
Tele Dienste



- Die Header des neuen IPv6 haben im Vergleich zu den variablen **Protokollkopflängen** des alten IP4 eine **konstante Länge**. Dies bewirkt eine wesentlich größere Verarbeitungsgeschwindigkeit
- Für spezielle Anwendungen existieren sog. Extensionsheader, die dem Basisheader im Sinne einer verketteten Liste folgen
- Extensionheader sind z.B. Sourcerouteheader, über die der Weg, den ein IP - Paket gehen soll, festgelegt werden kann oder Authentication Header, die der Authentifizierung aller nachfolgenden Header und deren Nutzdaten dienen (Signatur).

Universität
Potsdam
Institut für
Informatik

44



Übertragungsprotokolle IPv6 Adressen

Netzwerktechnologien
und multimediale
Tele Dienste



- Neue **Adressstruktur** mit einer Breite von 128 Bit. Die Adressen können dann auch etwas über den Standort des Empfängers aussagen und nicht mehr nur irgendeine Kombination von vier 8-Bit-Zahlen darstellen.
- Die Adresse enthält dann Informationen über die Adressverteilungsautorität, den Provider, den Kunden, im Falle des Falles das benutzte Subnet und das Interface, das Endgerät.
- Die letzten 32 Bit werden für die Abwärtskompatibilität zu IP4 reserviert.

Universität
Potsdam
Institut für
Informatik

45



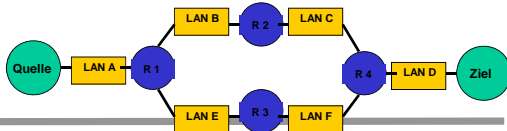
Aus diesen Erweiterungen ergeben sich auch **neue Anwendungsmöglichkeiten**. So u.a.:

- Unicast (wie bisher, ein Empfänger),
- Multicast (mehrere bestimmte Empfänger sind möglich) und
- Anycast (irgendeinen Empfänger aus einer bestimmten Gruppe von Empfängern)
- Encryption (Verschlüsselung der Nutzdaten)
- Encapsulation (Einkapselung von alten Protokolle, somit Abwärtskompatibilität)
- Realtime Dataflow (für Massenwendungen der Zukunft, Pakete mit variablen Prioritäten)



Ein Router empfängt Pakete von einem physikalischen Netz und überträgt sie auf ein anderes.

- Alle für das Routing erforderlichen Informationen sind in jedem IP-Paket enthalten. Der Router muss allerdings wissen,
- welche Netze angeschlossen sind (Netznummer, Netzmaske)
 - welche anderen Netze über welche "Gateways" (nächster Router, der direkt erreichbar ist) erreichbar sind
 - wohin Pakete zu senden sind, für die kein direktes Routing möglich ist





IP-Routing Tabelle enthält „Next-Hop“ Information, d.h. grundsätzlich Zeilen der Art (N, R) wobei:

- N: IP Adresse eines Zielnetzwerkes oder einer Zielstation
R: IP Adresse des „nächsten“ Routers entlang des Pfades zum Ziel der über ein direkt angeschlossenes Schicht 2 Netzwerk erreicht werden kann

Beispiel für eine Routingtabelle:

Netznummer	Netzmaske	Ziel
193.174.12.0	255.255.255.240	eth0
194.121.202.160	255.255.255.248	s10
194.174.11.176	255.255.255.240	gw 193.174.12.10
default		gw 193.174.12.1



IP Routing ist allgemein in zwei Paketzustellarten unterteilbar:

- **direkte Paketzustellung**
- **indirekte Paketzustellung**



Schicht 2 zu Schicht 2:

- direkte Versendung eines Pakets über ein einzelnes, zusammenhängendes Schicht 2 Netzwerk
- IP Pakete werden in Schicht 2 Pakete verpackt
- IP-Adressen werden in Schicht 2 Adressen umgesetzt (Adressauflösung; Mechanismen: ARP, direktes Mapping, Punkt-zu-Punkt)
- Bsp.: direkte Zustellung über Ethernet, FDDI, ATM, V.24



Abgeschlossene Routingeinheiten / z.B.

Intranets:

- **AS = Administrativ „abgeschlossene“ Einheiten in einem Internet**
- **d.h. abgeschlossen im Sinne der Verteilung von interner IP-Routinginformationen**
- **typische AS: IP Provider Netzwerke**
- **Routen innerhalb eines AS werden nicht an andere AS propagiert**
- **es gibt keine Default-Routen zwischen AS**



Richtungen und Distanzen im DVA:

- jeder Router der am Routingprozess teilnimmt, unterhält eine Tabelle mit „Richtungen“ und „Distanzen“ für alle möglichen anderen Ziele
- alle bekannten Ziele/Distanzen werden zeitlich periodisch benachbarten Routern „angezeigt“ (d.h. per broad-, multi- oder unicast Paketen)
- aus den regelmäßig empfangenen Paketen konstruiert bzw. aktualisiert der DVA, die Einträge für die Routing Tabelle (d.h. die mit der kleinsten Distanz zu dem jeweiligen Ziel)



- Routing Updates werden nur an benachbarte Router an direkt angeschlossenen Segmenten („direkte Links“) versendet
- jeder Router kennt immer nur den „Next Hop“ für jedes mögliche Ziel
- verwendete Distanzen in D.V.A.'s: „Metriken“; z.B. Zahl der „Hops“ zum Ziel, oder administrativ festgesetzte oder protokollspezifische Werte
- „beste“ Distanz (Metrik 0): normalerweise direkte Links bei Änderungen werden sofort Updates gesendet (z.B. wenn ein Interface ausfällt)
- Routen, für die eine bestimmte Zeitlang kein Update empfangen wurde, werden entfernt; optional abschaltbar



Vorteile:

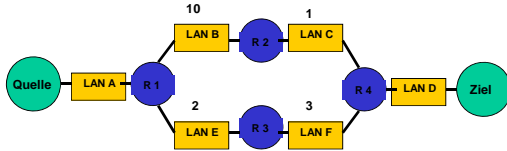
- Wartung tyischerweise relativ leicht
- weit verbreitet, auf vielen Plattformen verfügbar (d.h. insbesondere RIP)

Nachteile:

- skalieren sich schlecht für große Netzwerke
- Updates pflanzen sich nur langsam fort
- es können daher Routing-Schleifen auftreten
- Routing-Update-Pakete können bei vielen Zielen sehr groß werden

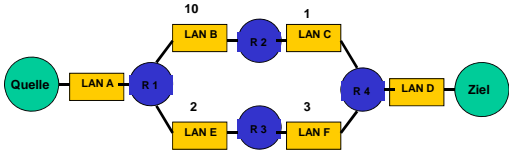


- Beispiel: Routing Tabellen für
1. Nach dem Start aller Systeme
 2. Nach dem Eintrag der Abstands-Werte aller Systeme
 3. Nach dem Austausch der Routing Tabellen



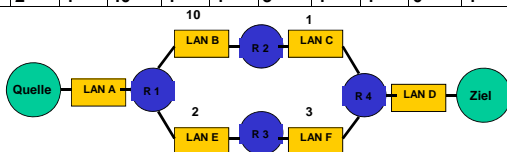
1. Nach dem Start aller Systeme

Router 1			Router 2			Router 3			Router 4		
Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über
1	0	1	1	?	1	1	?	1	1	?	2
2	?	2	2	0	2	2	?	4	2	?	2
3	?	3	3	?	3	3	0	3	3	?	3
4	?	2	4	?	4	4	?	4	4	0	4



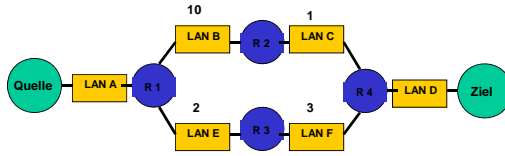
2. Nach dem Feststellen des Abstands zum Nachbarn

Router 1			Router 2			Router 3			Router 4		
Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über
1	0	1	1	10	1	1	2	1	1	?	2
2	10	2	2	0	2	2	?	4	2	1	2
3	2	3	3	?	3	3	0	3	3	3	3
4	?	2	4	10	4	4	3	4	4	0	4



3. Nach dem Austausch der Routingtabellen

Router 1			Router 2			Router 3			Router 4		
Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über	Nach	Dauer	über
1	0		1	6	4	1	2	1	1	5	3
2	6	3	2	0	2	2	4	4	2	1	2
3	2	3	3	4	4	3	0	3	3	3	3
4	6	3	4	10	4	4	3	4	4	0	4



„Routing Information Protocol“

- IGP
- Distance-Vector Protokoll
- war erstes verfügbares IGP
- ursprünglich sehr weit verbreitet durch Distribution mit BSD Unix (*routed* Software)
- entwickelt für relativ kleine Netzwerke
- immer noch sehr weit verbreitet, nahezu auf jeder Plattform implementiert

RIP Festlegungen

- als Distanz (Metrik) wird die Zahl der „Hops“ zum Ziel verwendet (**Maximum: 15 „Hops“**)
- Metrik 16 = „unendlich“, d.h. RIP ist nicht geeignet für Netzwerke mit mehr 15 Routern in einem Pfad
- RIP's D.V.A. sendet standardmäßig alle 30 Sek. ein RIP-Update mit allen bekannten Routen (Zieladresse, Distanz)
- empfängt ein RIP Router mehrere Routen zum gleichen Ziel bekommt die mit der kleinsten Metrik die höchste Präferenz



- nach standardmäßig 180 Sekunden wird angenommen, daß eine Route nicht mehr verfügbar ist, wenn **kein Update** empfangen wurde
- RIP sendet dann selber einen Request und fragt nach der Route; nach 270 Sekunden ohne Antwort wird die **Route entfernt**
- lernt RIP, daß eine Topologie-Änderung aufgetreten ist, wartet es nicht bis zum nächsten periodischen Route-Updating-Zeitpunkt, sondern **sendet sofort** (*Triggered Update*)



RIP Optionen:

- *optional*: Hold-Down: Änderungen zu einmal aktualisierten Routen (d.h. „gerade aktualisierten“) werden erst wieder nach einer gewissen Zeit akzeptiert
- *optional*: Split Horizon und Poison Reverse Algorithmen um möglichen Routing-Loops entgegenzusteuern



RIP Vorteile, Nachteile:

- Vorteil und Nachteile, wie bei allen D.V. Protokollen
- weiterer Nachteil: Benutzung der simplen Hop-Metrik erlaubt keine Unterscheidung zwischen unterschiedlich guten physikalischen Verbindungen

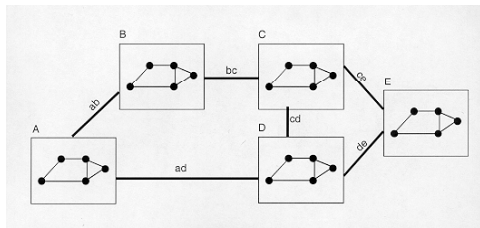


Link-State Algorithmus (LSA)

- jeder Router, der am Routingprozess teilnimmt, unterhält eine komplette Topologieinformation (Link-Status) über das „betrachtete“ Netzwerk, d.h. die entsprechende administrative Einheit
- d.h. jeder Router kennt jeden anderen Router und die an diesen angeschlossenen Netzwerke (Link-Graph)

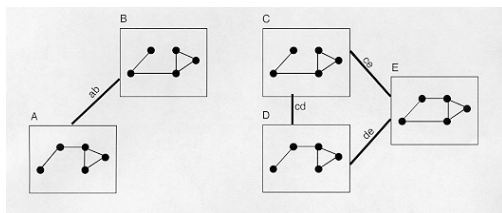


Netz im stabilen Zustand



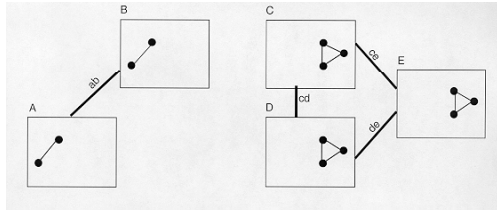


Links bc und ad sind ausgefallen





Nach einer Nachrichtenrunde





Prinzip:

- Ermittlung aller direkten Nachbar-Router
- jeder Router testet aktiv und zeitlich periodisch den Status aller benachbarten Router (d.h. direkte Links)
- die gesamte Link-Status Information werden zeitlich periodisch *allen* anderen beteiligten Routern im Netzwerk „angezeigt“
- Link-Status-Info spezifiziert keine Routen, sondern gibt jeweils an, ob Kommunikation jeweils zwischen Paaren von Routern möglich ist



Buchführung:

- Zustellung der Link-Status-Info mittels broad-, multi-, oder unicast Paketen
- beim Empfang einer Link-Status-Nachricht aktualisiert ein Router seine eigene Topologie Datenbasis, indem Links als „up“ bzw. „down“ markiert werden
- werden Änderungen bei Links festgestellt, werden mit dem *Dijkstra Algorithmus* die betroffenen Routen neu berechnet und die eigene IP Routingtabelle aktualisiert



Vorteile:

- jeder Router berechnet seine Routingtabelle unabhängig von anderen, mit der originalen Link-Status-Info des „anzeigenden“ Routers
- d.h. keine Abhängigkeit von den Berechnungen von „Zwischen“-Routern
- Probleme leichter zu finden
- Größe der Pakete hängt nicht von der Zahl der gerouteten Netzwerke ab (d.h. L.S.A.'s skalieren sich besser)
- Link-Status kann zusätzliche Information, wie Qualität des Links („cost“) enthalten, dadurch optimale Pfadwahl möglich



Nachteile:

- meist aufwendiger zu warten
- meist höhere Rechnerleistung auf dem Router erforderlich bei großen „Gebieten“



„Open Shortest Path First“

- als IGP entworfen, ist aber in der Lage, Routen mit anderen AS auszutauschen, daher auch teilweise ein EGP
- entwickelt von der IETF Ende der 80iger Jahre
- sollte RIP ersetzen
- offener Standard, auf allen wichtigen Router Plattformen implementiert, aber seltener in End-systemen als RIP



OSPF ist klassisches Link-State-Protokoll

- erfordert administrative Unterteilung des Netzwerkes in eine Routing Hierarchie
- ein zentraler OSPF „Backbone“ verbindet eine Zahl von „Areas“
- Areas sollten administrativ so gestaltet werden, dass inter-Area Kommunikation möglichst selten ist



Router mit OSPF:

- Router die Areas über ihre Interfaces verbinden heißen „Border Area“ Router
- die Kommunikation zwischen Areas kann nur über die Backbone Area erfolgen (Area 0; kann aber *virtuell* sein)
- Border Area Router unterhalten Link-Status-Datenbasen für alle Areas in denen sie Teil-nehmer sind
- die Topologie eines Areas ist unsichtbar für alle anderen Areas (*intra-Area* vs. *inter-Area* Routing)



Festlegungen:

- Intra-Area Router haben alle die gleiche Topologie-Datenbasis
- an LAN-Segmenten wählt OSPF einen Router als „Designated“ Router und einen als seinen Backup aus um Link-State-Info für dieses LAN in der entsprechenden OSPF Area zu verbreiten
- Router die ihre Datenbasen abgeglichen haben werden in OSPF „Adjacencies“ genannt
- OSPF operiert wie ein klassisches Link-State-Protokoll



weitere Features:

- **Route Aggregation**
 - Zusammenfassung von Routen mit gleichem Präfix (*classless*)
 - kann Größe der Routing Tabelle und Protokoll Traffic erheblich minimieren
- **Type of Service Routing**
 - mehrfache Routen zum gleichen Ziel installierbar, für verschiedene Servicetypen (Pfadwahl dann durch Felder IP-Header)



Load Balancing

- bei mehrfachen Routen zum gleichen Ziel mit gleicher „Cost“ kann OSPF Traffic über diese Pfade gleich verteilen

Authentication

- Routing Pakete können mit verschiedenen Verfahren authentifiziert werden



Am Markt:

- **unterschiedlichste Routingsoftware für verschiedenste Plattformen am Markt**
- **sehr weit verbreitet sind:**
 - Cisco IOS; Betriebssystem nahezu der gesamten Cisco Router und Switch Produktpalette, große Zahl von unterstützten Routingprotokollen
 - gated Software; auf nahezu allen Unix'en vorhanden, unterstützt alle wichtigen Routingprotokolle, einschließlich RIP, OSPF und BGP



Routingsoftware ff. 1

Netzwerktechnologien
und multimediale
Teledienste



Universität
Potsdam
Institut für
Informatik

- Moderne Routingsoftware gestattet üblicherweise sehr weitgehende administrative Eingriffe
- z.B. das Erlauben oder Verboten bestimmter Routen
 - das Festlegen von administrativen „Weights“, d.h. z.B. Bevorzugung bestimmter Routen
 - das Akzeptieren von Updates nur von bestimmten Nachbar Routern
 - peer-to-peer Betrieb (d.h. z.B. kein RIP-Broadcast) passiv (nur „Lernen“, kein aktives Anzeigen)
 - konfigurierbaren Routenaustausch zwischen allen auf dem gleichen System laufenden Routing Protokollen

79



Dienste mit Qualitäten (QoS) und Qualitätssicherungsprotokolle

Netzwerktechnologien
und multimediale
Teledienste



Universität
Potsdam
Institut für
Informatik

- Dienste
- Dienstgüte
- Protokolle

80



Dienste

Netzwerktechnologien
und multimediale
Teledienste



Universität
Potsdam
Institut für
Informatik

- Email
- WWW
- FTP
- Telnet
- Mbone
- Videoconference
- und alle anderen 1.700 Internetdienste

81



Die herkömmlichen Algorithmen und Protokolle gestatten keinen isochronen Fluß der Paketströme, da sie eine erhebliche Varianz beim Datenverkehr (delay, jitter) erzeugen und bieten keine Garantien für Dienstgüten („best effort“ Netze)

Gründe:

- Fehlersicherung durch Übertragungswiederholungen
- Flußkontrolle (z.B. sliding window)

Also sind neue Protokolle erforderlich.



Anwendungsbezogene Qualitäten:

Bandbreite :

Wie viele Bit/s können übertragen werden

Verkehrsart :

Konstante Bitrate (CBR), Variable Bitrate (VBR)

Verzögerung (delay) :

Wie lange dauert die Übertragung eines Paketes

Varianz der Verzögerung (jitter) :

Wie gleichmäßig kommen die Pakete an ?

Verlustrate (loss rate) :

Wie viele Pakete gehen verloren ?



Die Dienstgüte ist eine **Parametrisierung von Protokollen** zur Bestimmung des Übertragungsverhaltens.

Das OSI-Referenzmodell definiert bestimmte Protokoll-Dienste, die von der Vermittlungsschicht der übergeordneten Transportschicht angeboten werden.

Bei den OSI-Protokollen der Transportschicht werden mit dem Verbindungsaufbau Dienstgüteparameter vereinbart.

Es wird von der initialisierenden Transportinstanz eine Liste vorgeschlagen, die entweder von der gerufenen Transportinstanz akzeptiert oder verändert wird.



Typische Dienstgütemerkmale sind:

- Verbindungsaufbauverzug,
- Störungswahrscheinlichkeit des Aufbaus,
- Durchsatz,
- Transitverzug,
- Restfehlerrate,
- Störungswahrscheinlichkeit des Transfers,
- Abbauverzug,
- Störungswahrscheinlichkeit des Abbaus,
- Schutz der Transportverbindung,
- Priorität von Transportverbindungen und
- Rücksprung aus einer Transportverbindung.



Die Dienstgüte kann für verschiedene Dienste und Netze **unterschiedlich** definiert sein.

Bei ATM werden mit der Dienstgüte die Service-Parameter einer ATM-Verbindung spezifiziert. Dazu gehören u.a. die Zellenverlustrate und die Zellenverzögerung.



Wie wird sichergestellt, daß die Dienstgütemerkmale eingehalten werden ?

Entweder durch ein **Class of Service (CoS)**-Konzept:

Beispiel: Das Kennzeichnen der Sprachpakete mit einer speziellen Signalisation (IP Precedence), ermöglicht, dass die aktiven Netzkomponenten diese Pakete gegenüber Datenpaketen priorisiert behandeln und sofort weiterleiten.

Oder durch ein **Quality of Service (QoS)**-Konzept:

Beispiel: Mit Hilfe des Resource Reservation Protocol (RSVP) wird über die ganze Übertragungsstrecke der Sprachverbindung Kapazität in den Routern reservieren.



Dienstgüte-Protokolle

Netzwerktechnologien
und multimediale
Teledienste



Die Router bedienen sich dabei diverser interner **Warteschlangen-Mechanismen**, um Sprachpakete vorrangig zu behandeln und dadurch mit möglichst hoher Bandbreite durch das Netzwerk zu übertragen. Es wird zwischen Mechanismen zur optimalen Flusststeuerung (Weighted Fair Queuing) und Mechanismen zur vorbeugenden Verhinderung von Blockierungen (Random Early Detection) unterschieden. Router der verschiedenen Hersteller können dabei auch proprietäre Warteschlangen-Verfahren verwenden.

Universität
Potsdam
Institut für
Informatik



Dienstgüte-Protokolle RSVP

Netzwerktechnologien
und multimediale
Teledienste



Einen Ansatz, QoS auch innerhalb IP-basierender Netze bereitzustellen, stellt das **Resource ReSerVation Protocol (RSVP)** dar.

Die Entwicklung von RSVP wird seit 1993 von der Internet Engineering Task Force (IETF) vorangetrieben. Das Ziel ist die QoS-Sensitivierung von TCP/IP unter Beibehaltung der bestehenden Protokollstrukturen.

Anders als bei ATM sollte RSVP von Beginn an eine dynamische Allokierung von Ressourcen von Unicast- und Multicast-Verbindungen bei gleichzeitiger Minimierung der notwendigen Bandbreite ermöglichen.

Beide Verbindungsarten, Unicast und Multicast, sollen im weiteren unter dem Oberbegriff RSVP-Sitzung zusammengefasst werden.

Universität
Potsdam
Institut für
Informatik



Dienstgüte-Protokolle RSVP

Netzwerktechnologien
und multimediale
Teledienste



Der QoS einer RSVP-Sitzung ist keine statische Größe, sondern kann auftretenden Änderungen während einer Sitzung angepasst werden.

Weiterhin ist die Anzahl der an einer Sitzung teilnehmenden Hosts variabel. Maschinen können einer laufenden Sitzung zugeschaltet werden oder sie verlassen. Dieser hohe Grad an Flexibilität spiegelt sich in den von ATM grundsätzlich verschiedenen Eigenschaften des RSVP-Protokolls wieder:

Simplex Protokoll

Ressourcen werden unidirektional alloziert. Up- und Down-Stream sind somit bzgl. ihres QoS voneinander entkoppelt.

Universität
Potsdam
Institut für
Informatik



Dienstgüte-Protokolle RSVP

Netzwerktechnologien
und multimediale
Tele Dienste



Receiver orientiert

Die Reservierung der Ressourcen wird nicht vom Sender sondern durch den Empfänger (Receiver) einer Verbindung eingeleitet. Dies ermöglicht den Einsatz heterogener Receiver innerhalb einer Sitzung.

Abschnittsweiser QoS

Der QoS wird abschnittsweise festgelegt. Dies erlaubt in bestimmten Fällen das Verschmelzen (Merging) der Datenströme mehrerer Sender (Abschnitt.).

Universität
Potsdam
Institut für
Informatik

91



Dienstgüte-Protokolle RSVP

Netzwerktechnologien
und multimediale
Tele Dienste



Soft State

Die einer Verbindung zugeordneten Ressourcen sind innerhalb eines festgelegten Intervalls **regelmäßig zu bestätigen**. Bei Ausbleiben eines Refreshes werden sie automatisch freigegeben.

Transparenz

Das Einbinden von Strecken ohne RSVP-Unterstützung in eine RSVP-Sitzung ist aufgrund der Transparenz des Protokolls möglich.

Nutzung bestehender Routing-Mechanismen

RSVP stellt kein eigenständiges Routing-Protokoll dar, sondern nutzt bereits im Protokoll-Satz implementierte unicast oder multicast Routing-Mechanismen.

Universität
Potsdam
Institut für
Informatik

92



Dienstgüte-Protokolle RSVP

Netzwerktechnologien
und multimediale
Tele Dienste



Trotz seiner primären Ausrichtung zum Einsatz in IPv4- und IPv6-Netzen ermöglicht die Nutzung bestehender Routing-Mechanismen auch Implementierungen innerhalb IP-fremder Protokoll-Sätze.

Universität
Potsdam
Institut für
Informatik

93



Charakterisierung des Datenflusses

In Anlehnung an die von der IETF definierten Serviceklassen berücksichtigt RSVP bislang den Controlled Load Service und den Guaranteed Service. Die Spezifikation eines Datenflusses erfolgt dabei in beiden Fällen anhand des von der ITU vorgeschlagenen Leaky-Bucket Mechanismus:

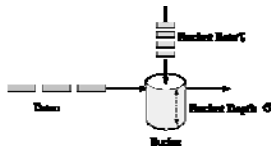


Abbildung: Leaky-Bucket Mechanismus

Die beiden zentralen Parameter einer RSVP-Nachricht sind daher die Rate mit welcher der Behälter gefüllt wird, die Token Bucket Rate [bps], und die Tiefe des Behälters, die Token Bucket Depth [bit].



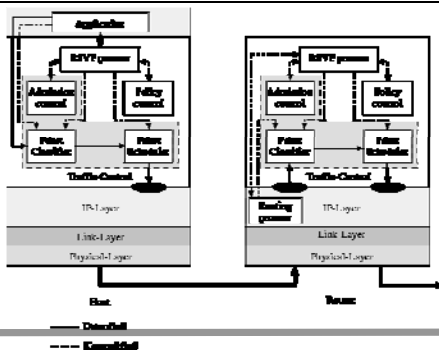
Einordnung innerhalb von TCP/IP

Zur Festlegung der RSVP-Elemente muß die Einordnung des Protokolls innerhalb von TCP/IP betrachtet werden. Bedingt durch den Rückgriff auf bereits implementierte Routing-Mechanismen sowie die Notwendigkeit eines abschnittswisen QoS ist RSVP als Protokoll der Schicht 4 des OSI-Referenzmodells einzuordnen. Trotz dieser Einordnung werden die entlang einer RSVP-Sitzung beteiligten Hosts als RSVP-Router und nicht als Gateways bezeichnet. Weiterhin ist RSVP kein Transportprotokoll sondern dient, wie ICMP, allein der Kontrolle des Datenflusses.



Für Betriebssysteme, deren Netzwerkschicht keinen direkten Datentransport über das IP-Protokoll zulässt („raw“ Network I/O) ist optional der Einsatz von RSVP über UDP vorgesehen. Die RSVP-Kontrollstruktur auf der Ebene der Transportschicht unterteilt sich in mehrere Elemente. Sowohl der einen QoS anfordernde Receiver als auch die an der Sitzung beteiligten RSVP-Router verfügen grundsätzlich über identische Protokoll-Instanzen,

- den Paket-Classifier,
- den Paket-Scheduler,
- die Admission-Control,
- die Policy-Control sowie
- den eigentlichen RSVP-Prozeß.

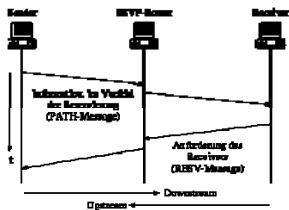




Die Admission-Control, der Paket-Classifer und der Paket-Scheduler werden in einer logischen Einheit, der Traffic-Control, zusammengefaßt. Die Aufgaben der einzelnen Instanzen sollen im folgenden betrachtet werden.



RSVP sieht eine unidirektionale Bereitstellung von Ressourcen in Abhängigkeit der Anforderung des Receivers vor (one pass). Neben den eigenen technischen Grenzen muß dieser dabei insbesondere die Leistungsfähigkeiten der Übertragungsstrecke und des Senders berücksichtigen. Einer entlang des Upstreams weitergeleiteten Anforderung des Receivers muß daher eine senderseitig generierte Nachricht im Downstreams vorausgehen:





Mit VPN-Techniken können gesicherte Verbindungen über das offene Internet zwischen einzelnen Arbeitsplätzen oder ganzen lokalen Netzen aufgebaut werden

Wozu:

- gesicherter Datentransport (Konkurrenz..)
 - LAN-Erweiterung über Internet; ISDN, X.25
 - Anschluss von Geschäftspartnern, Kunden..
- gefordert werden:
- Vertraulichkeit (Verschlüsselung)
 - Authentifizierung der beteiligten Personen
 - Standards
 - hohe Leistungsfähigkeit bei niedrigen Kosten
 - gute Administration, Schlüsselmanagement



VPN's können auf unterschiedlichen Schichten der Netzwerkprotokolle realisiert werden

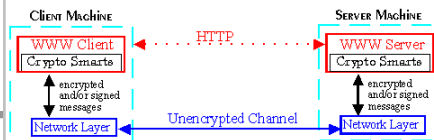
- Schicht 7
- Schicht 4
- Schicht 3
- Schicht 2



Layer-7-VPN

- Integration in Web-Browser (Netscape Navigator, MS Internet Explorer) : https - Secure HTTP
- Integration in vorhandene TCP/IP-Anwendungen geringer Installations-, Konfigurationsaufwand
- PEM (Privacy Enhanced Mail),
- PGP (Pretty Good Privacy),
- S/MIME Secure MIME für sichere EMail-Dienste

S-HTTP: Application-level Security



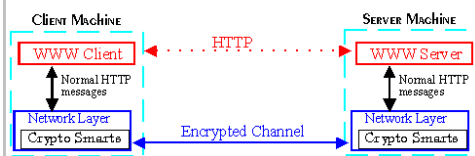


Layer-4-VPN

SSL Secure Socket Layer (Netscape):

nur TCP-, UDP-Pakete verschlüsselt

SSL: Connection-level Security





Eine Einführung in VPN's (Virtuelle Private Netze)

Netzwerktechnologien
und multimediale
Teledienste



Layer-3-VPN

umfaßt alle Pakete

Standard: (IPSec) IP Security mit

- SKIP Simple Key Management for Internet Security (skalierbar+sicher)
- ISAKMP Internet Security Association and Key Management Protocol (Standard)
 - in: IPv6, NT 5.0
 - normierte IP-Header:
 - ESP Encapsulating Security Payload (def. Paketverschlüsselung)
 - AH Auth. Header für Paketauthentifizierung

Universität
Potsdam
Institut für
Informatik



Eine Einführung in VPN's (Virtuelle Private Netze)

Netzwerktechnologien
und multimediale
Teledienste



Layer-2-VPN

unabhängig von Protokollen, Anwendungen

2 entstehende Standards:

PPTP:

tunnelt nach aufgenommener Verbindung alle anderen Protokolle (incl. NetBEUI, IPX)

starke Auth., Nutzdatenverschlüsselung
Windows NT, XX, Novell

L2TP:

Layer 2 Tunneling Protocol (PPTP+L2F)
starke Auth., optional ESP-Header

Universität
Potsdam
Institut für
Informatik



Eine Einführung in VLAN's 2

Netzwerktechnologien
und multimediale
Teledienste



- Der Nutzen von Virtual LAN's
- VLAN-Konzepte
 - Layer-1-VLANs
 - Layer-2-VLANs
 - Layer-3-VLANs
 - Policy-basierende VLANs

Universität
Potsdam
Institut für
Informatik



Der Begriff **VLAN (virtuelles lokales Netz)** steht für die **Trennung von physischer und logischer Netzstruktur**. D.h. die virtuellen Netze erlauben es, die physische Struktur des Netzes und seine Systeme von der organisatorischen Zugehörigkeit der Mitarbeiter (und damit von der logischen Netzstruktur) zu trennen.

Die Netzbenutzer bilden **nicht mehr** aufgrund ihres **gemeinsamen Standortes** eine Netzgruppe, sondern sie können mit den Kollegen zu einer Gruppe zusammengefasst werden, mit denen sie tatsächlich zusammenarbeiten.



Die Endgeräte der Benutzer werden zu logischen Gruppen zusammengefasst, **unabhängig von ihrem physischen Standort**, und können miteinander kommunizieren als ob sie zum selben LAN gehören.

Damit kann die Orts-Beziehung zwischen aktiven und passiven Komponenten aufgelöst oder - von höherer Ebene aus betrachtet - **eine freiere Zuordnung von Benutzern zu Netzressourcen** vorgenommen werden.



Gründe für den Zusammenschluss zu einer Interessensgruppe können organisatorischer oder technischer Art sein.

Unter dem Aspekt der Unternehmensorganisation ist es z.B. möglich, alle Mitarbeiter einer Abteilung in eine Netzgruppe zusammenzufassen, auch wenn sie auf verschiedenen Etagen verteilt sind.

Unter dem Aspekt der Arbeitsorganisation können Mitarbeiter, die gemeinsam an einem Projekt arbeiten, zu einer Netzgruppe zusammengefasst werden, auch wenn sie zu verschiedenen Abteilungen gehören. Unter Performance-Aspekten können Mitarbeiter, die besondere Anforderungen an die Bandbreite oder Quality-of-Service (QoS) stellen, zu einer Netzgruppe zusammenfassen.

Diese Anforderungen können mit Hilfe von virtuellen Netzen realisiert werden.



Durch die Zuordnung der Endgeräte zu logischen Gruppen (VLANs) beschränkt sich der Datenverkehr eines logischen Netzes auf eine Broadcastdomain. Jedes VLAN bildet also eine eigene, unabhängige Broadcastdomain, in der die Teilnehmer über geschichtete Strukturen auf Ebene 2 gekoppelt werden. Der Anwender hat u.U. die Möglichkeit, sein Endgerät an jedem beliebigen Ort innerhalb des Netzes anzuschließen, ohne daß er die Zugehörigkeit zu seinem VLAN verliert. Werden die Mitglieder eines VLANs über mehrere Switches verteilt, so steigt in der Praxis der Datenverkehr zwischen diesen Komponenten erheblich.



Aus diesem Grund muss in dem Konzept der Switches die Möglichkeit einer adäquaten Backbone-Skalierbarkeit und der Broadcast-Reduzierung integriert sein. Die Kommunikation zwischen Teilnehmer unterschiedlicher VLANs erfolgt über Router auf Ebene 3.



Zunächst besteht die Notwendigkeit, die Menge der Nutzer eines LANs in VLAN-Gruppen aufzuteilen.

Die Zuordnung der Endgeräte zu VLANs kann auf unterschiedliche Art und Weise erfolgen. Jede Variante hat hierbei andere Auswirkungen auf das Netzdesign.

Folgende Zuordnungsvarianten können gewählt werden:

- der **Switch Port**,
- die **MAC-Adresse des angeschlossenen Endgerätes**,
- das **benutzte Network-Layer Protokoll (IP, IPX, Appletalk, NetBIOS, DECnet, Banyan Vines, etc.)**,
- die **verwendeten Anwendungen (Services)**,
- die **verschiedenen Kombinationen**.



Layer-1-VLANs

Die Layer-1-VLANs oder **portbasierte-VLANs** werden von einer Reihe von Herstellern unterstützt und werden auch im zukünftigen VLAN-Standard (IEEE 802.1Q) vorgesehen. Die Layer-1-VLANs bilden die einfachste Form von virtuellen LANs und sind bekannt seit dem Aufkommen von sogenannten Portswitching- Hubs. Zuordnung der Endgeräte: die Switch-Ports sind einzelnen VLANs zugewiesen, so daß alle Stationen, die an diesem Port angeschlossen sind, automatisch diesem VLAN zugeordnet werden.



Layer-2-VLANs

Zuordnung der Endgeräte : Layer-2-VLANs werden auf **Basis von MAC-Adressen** gebildet. Jede Station (Netzkomponente, Endgerät, etc.) hat eine MAC-Adresse. Die MAC-Adresse ist eine, auf der Adapterkarte eingestellte, nicht veränderbare, eindeutige, festverdrahtete Adresse. Ein Layer-2-VLAN besteht nun aus einer Gruppe von MAC-Adressen, die jeweils eine Broadcast Domain bilden (= VLAN). Die Zuordnung der Stationen zu einem VLAN erfolgt durch Eintragung der jeweiligen Station-MAC-Adresse in die VLAN-Tabelle.



Layer-3-VLANs

Durch die **Zuordnung der Netzadresse eines Endgerätes** zu einer Gruppe entsteht die Bildung der Layer-3-VLANs. Es gibt mehrere Kriterien nach denen man VLANs bilden kann:
nach Art der Layer-3-Protokolle: IP-, IPX-VLAN, etc. Dabei befinden sich nur Anwender, die das gleiche Protokoll (z.B. IP, IPX) benutzen, in einem gemeinsamen VLAN.

nach der Subnetzbildung: z.B. IP-Subnetze. Alle Benutzer die im gleichen Subnetz angeschlossen sind, gehören auch zum selben VLAN.



Policy-basierende VLANs

Policy-basierende VLANs verwenden **logische Zuordnungen (Port, MAC, Protokoll, Netzadresse)**. Sie sind die flexibelste Form, Endgeräte zu einer Gruppe zusammenzufassen.

Zuordnung der Endgeräte :

Die Endgeräte können aufgrund ihrer Portzugehörigkeit, ihrer MAC-Adresse oder der IP-Adresse einem VLAN zugeordnet werden. Auch eine Kombination dieser Möglichkeiten können ein VLAN definieren



- Für Wizards: Jeff Doyle (CCIE), **Routing TCP/IP, Band II**. Externe Routing-Protokolle und erweitertes IP-Routing, ISBN 3-8272-6223-2, 99,95 [D]1080 Seiten, erschienen 14.12.2001
