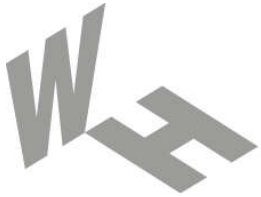


Westfälische Hochschule

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Routing-Protokolle

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Inhalt

- Ziele, Einordnung und Übersicht
- Router
- Routing-Verfahren
- Routing-Protokolle
- Zusammenfassung

Inhalt

- **Ziele, Einordnung und Übersicht**
- Router
- Routing-Verfahren
- Routing-Protokolle
- Zusammenfassung

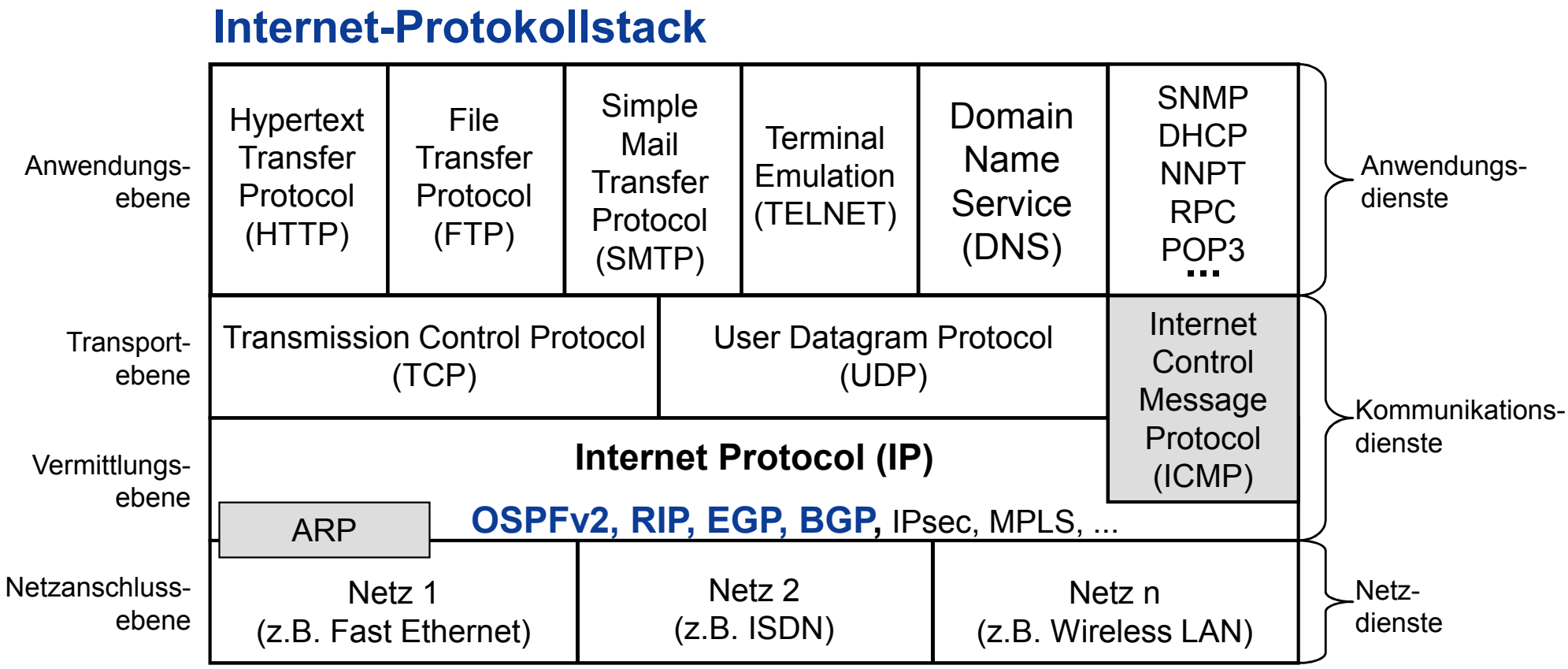
Routing-Protokolle
→ Ziele

- Gutes Verständnis für die Notwendigkeit und die Möglichkeiten eines Teils des Konfigurationsmanagements im Bereich des Netzwerkmanagements.

- Guten Sachverstand und Überblick für die wichtigsten Routing-Verfahren und -Protokolle in den TCP/IP-Kommunikationsarchitekturen.

- Erlangen der Kenntnisse über die Aufgaben, Prinzipien und Mechanismen von Routing-Algorithmen und -Protokollen.

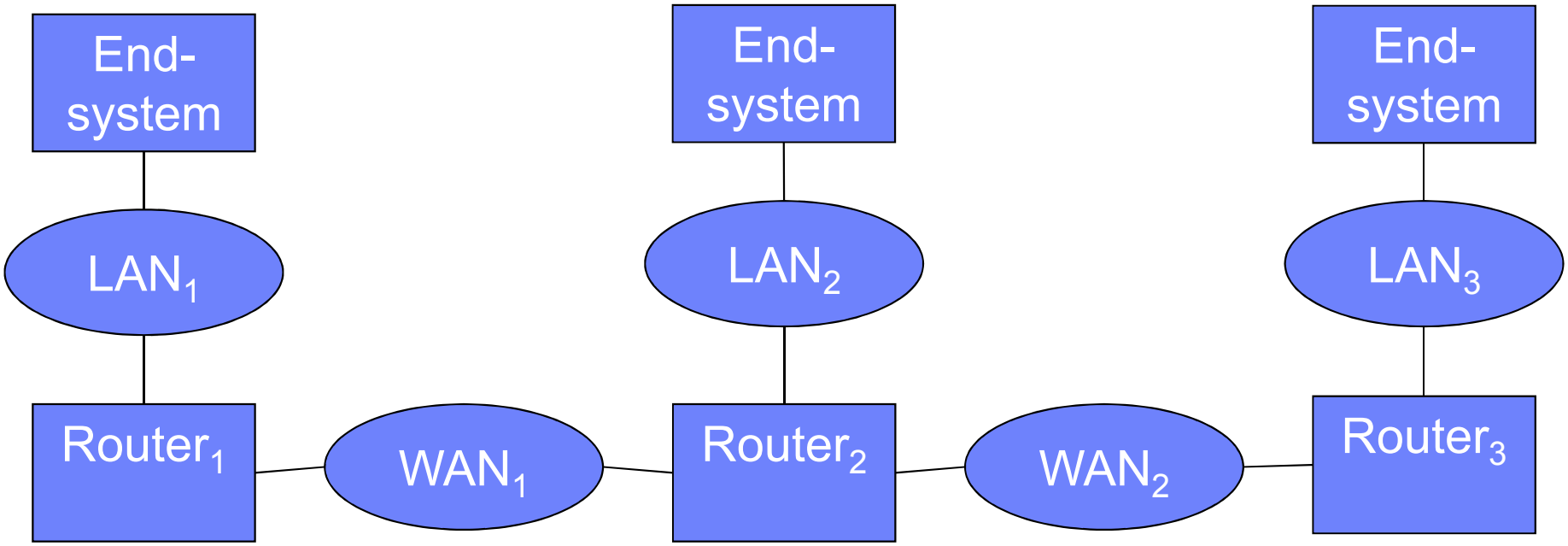
Routing-Protokolle
→ Einordnung



Inhalt

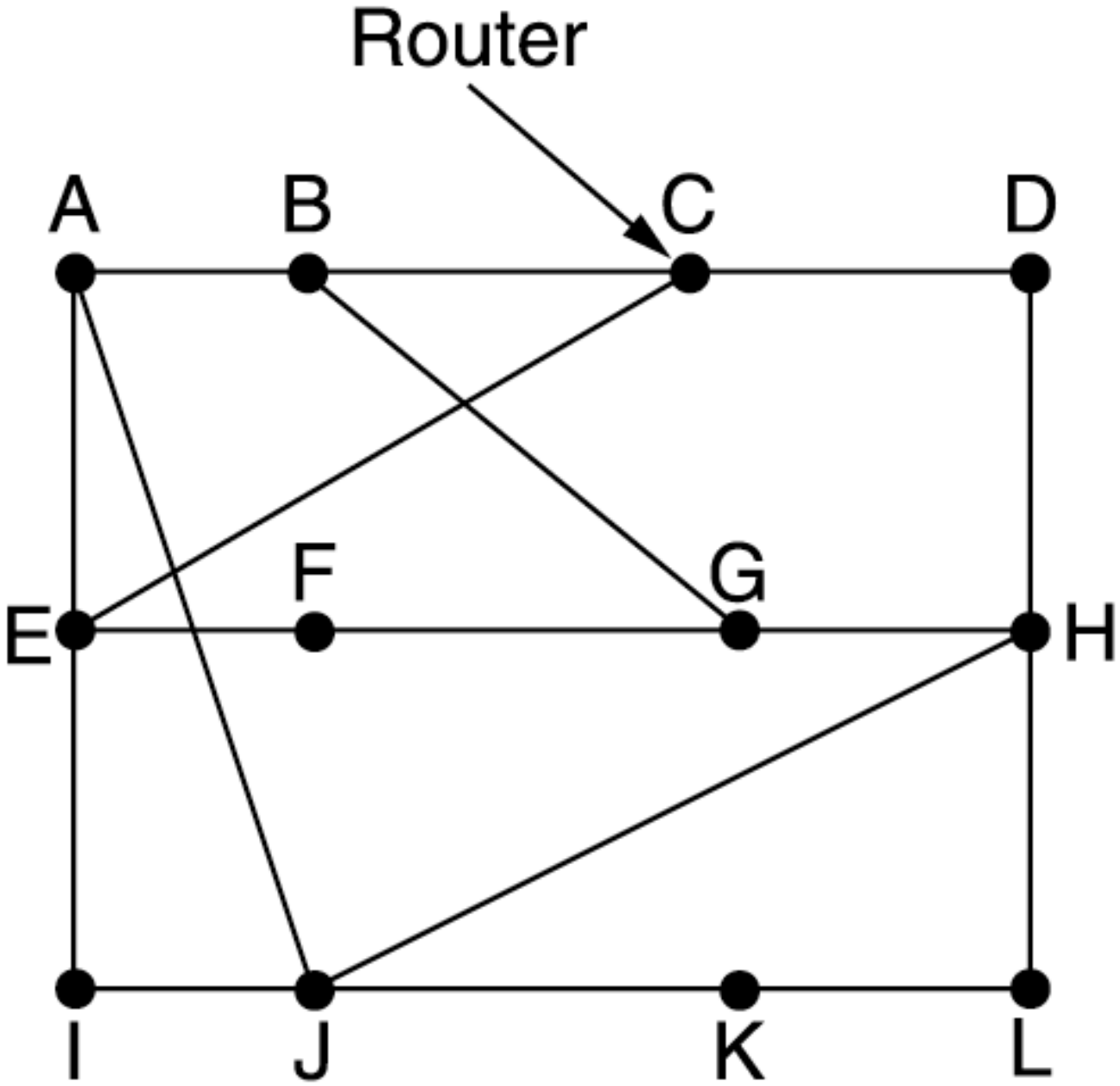
- Ziele, Einordnung und Übersicht
- **Router**
- Routing-Verfahren
- Routing-Protokolle
- Zusammenfassung

Router
→ Einsatzzweck



- Ein Router koppelt das Netz mit unterschiedlichen Netzadressen auf der Vermittlungsschicht zu entfernten Endsystemen über ein oder mehrere WANs.
- Mit Hilfe von IP-Adressen und den dazugehörigen Routing-Protokollen baut ein Router die dazugehörigen Routing-Tabellen auf.
- Bei den meisten Routern geschieht dieser Aufbau automatisch nach dem Einschalten des Routers.

Router
→ Beispiel eines Teilnetzes



Router
→ Aufgaben

- Kopplung über Schicht 3 des OSI-Referenzmodells

- **Wegewahl** anhand weltweit eindeutiger, hierarchischer Netzwerkadressen
  - meist IP-Adressen
  - Adressen werden in speziellen Tabellen gehalten
  - durch Hierarchie weltweite Zuordnung der Adressen möglich
  - Voraussetzung für optimale Wegewahl

- Segmentieren und Reassemblieren von Schicht-3-Datenpaketen zur Anpassung an unterschiedliche maximale Paketgrößen auf Schicht 2

Router

- **Weitere Aufgaben:**
  - Sicherheitsmechanismen zur Regelung von Netzzugriffen abhängig von der Netzwerkadresse.

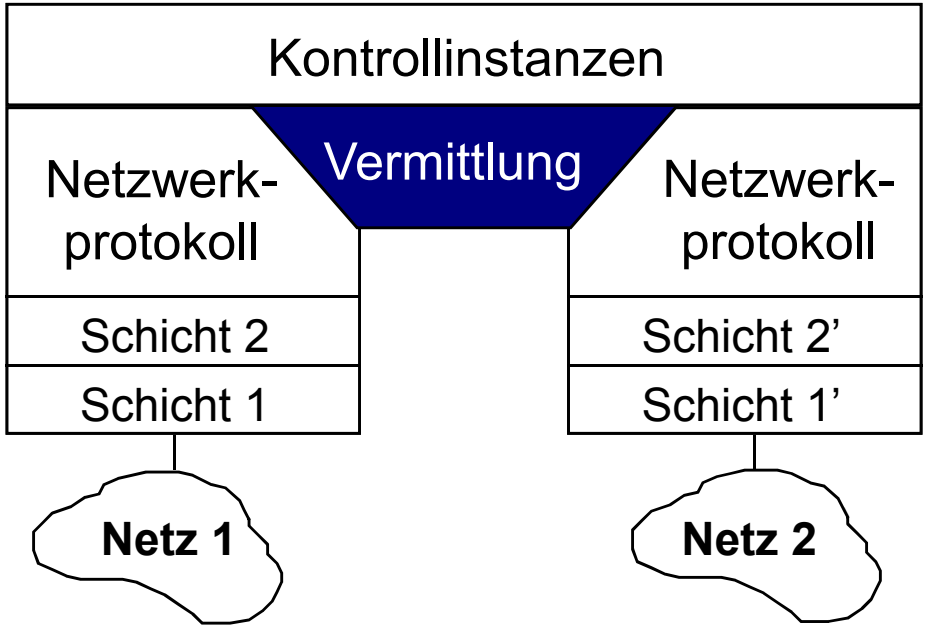
    Firewalling: anhand von Quell- bzw. Zieladressen kann über eine Weiterleitung der Pakete entschieden werden (Packet-Filter-Funktionen)

  - automatische Begrenzung von Schicht-2-Broadcasts

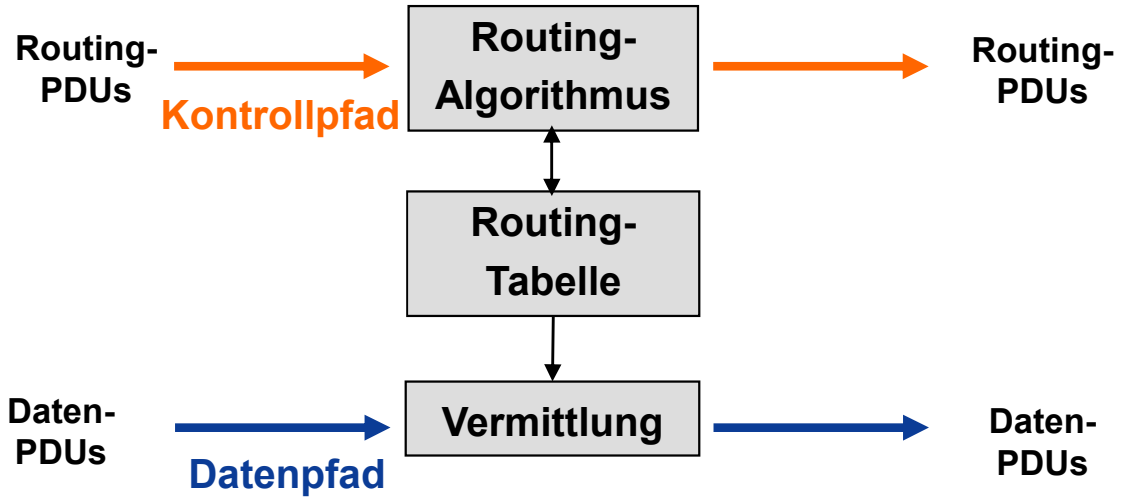
- Router sind eine der leistungsfähigsten Netzwerkkomponenten mit Datendurchsätzen im **Multi-Gigabit-Bereich**

Router
→ Architektur - wesentliche Merkmale

- Für jedes Netzwerk eine eigene Schicht-1- und Schicht-2-Instanz
- Netzwerkprotokoll ist in der Regel für alle Netzwerke gleich (z.B. IP-Router)
- Wegwahl anhand der global eindeutigen Netzwerkadressen
- Vermittlungskomponente verbindet die Netzwerkprotokollinstanzen; sie realisiert die Weiterleitungsfunktion
- Kontrollinstanzen implementieren beispielsweise Routing-Protokolle, Protokolle zur Fehleranzeige und Managementprotokolle (ICMP)



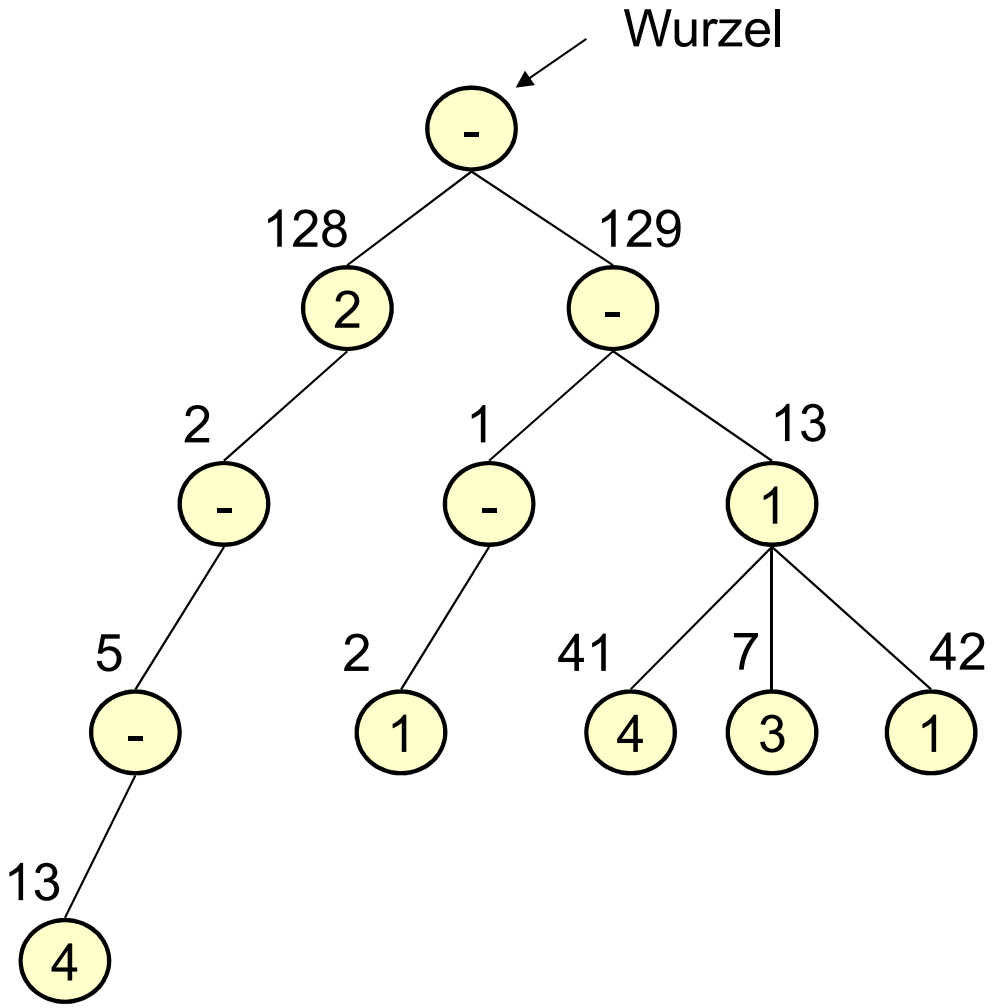
Router
→ Kontroll- und Datenpfad



- **Datenpfad auf Netzwerkschicht**
- **Kontrollpfad darüber**
- Gewinnung von Routinginformationen durch das **Routing-Protokoll**
- **Routing-Algorithmus** verwaltet die Routing-Tabelle (Eintragen, Ändern, Löschen von Einträgen)
- **Routing-Tabelle** enthält Routinginformationen
- Wegewahl bei der Vermittlung wird anhand der Routing-Tabelle durchgeführt

Router
→ Prinzip einer Routing-Tabelle

Zieladresse	Ausgang
129.13.*.*	1
128.*.*.*	2
129.1.2.*	1
129.13.41.*	4
129.13.42.*	1
129.13.7.*	3
128.2.5.13	4



- Beispiel einer vereinfachten Routing-Tabelle:
  - Suche nach dem am besten passenden **Präfix**
  - Weiterleitung der Pakete an die den jeweiligen Präfixen zugeordneten Ausgänge

Inhalt

- Ziele, Einordnung und Übersicht
- Router
- **Routing-Verfahren**
- Routing-Protokolle
- Zusammenfassung

Router
→ Routing-Verfahren (1/3)

- **Aufgaben des Routingverfahrens**
  - Treffen der Entscheidung, auf welcher Übertragungsleitung ein eingehendes Paket weitergeleitet werden soll
- **Ziele**
  - niedrige bis mittlere Paketverzögerungszeit
  - hoher Netzdurchsatz
- **Ansatzpunkt**
  - Übertragen eines Pakets von einem Quellrechner zu einem Zielrechner über den Weg mit den geringsten „Kosten“.
  - **Mögliche Metriken** sind z.B.: ***Anzahl der Hops***, ***finanzielle Kosten***, ***Verläßlichkeit***, ***Durchsatz***, ***Bandbreite*** und ***Verzögerung***.

Router
→ Routing-Verfahren (2/3)

- **Ort des Routing-Verfahrens:**
  - **Zentral** in einem Netzkontrollzentrum (Routing Control Center, RCC)
  - **Dezentral**, d.h. verteilt auf die Vermittlungsknoten (Router)

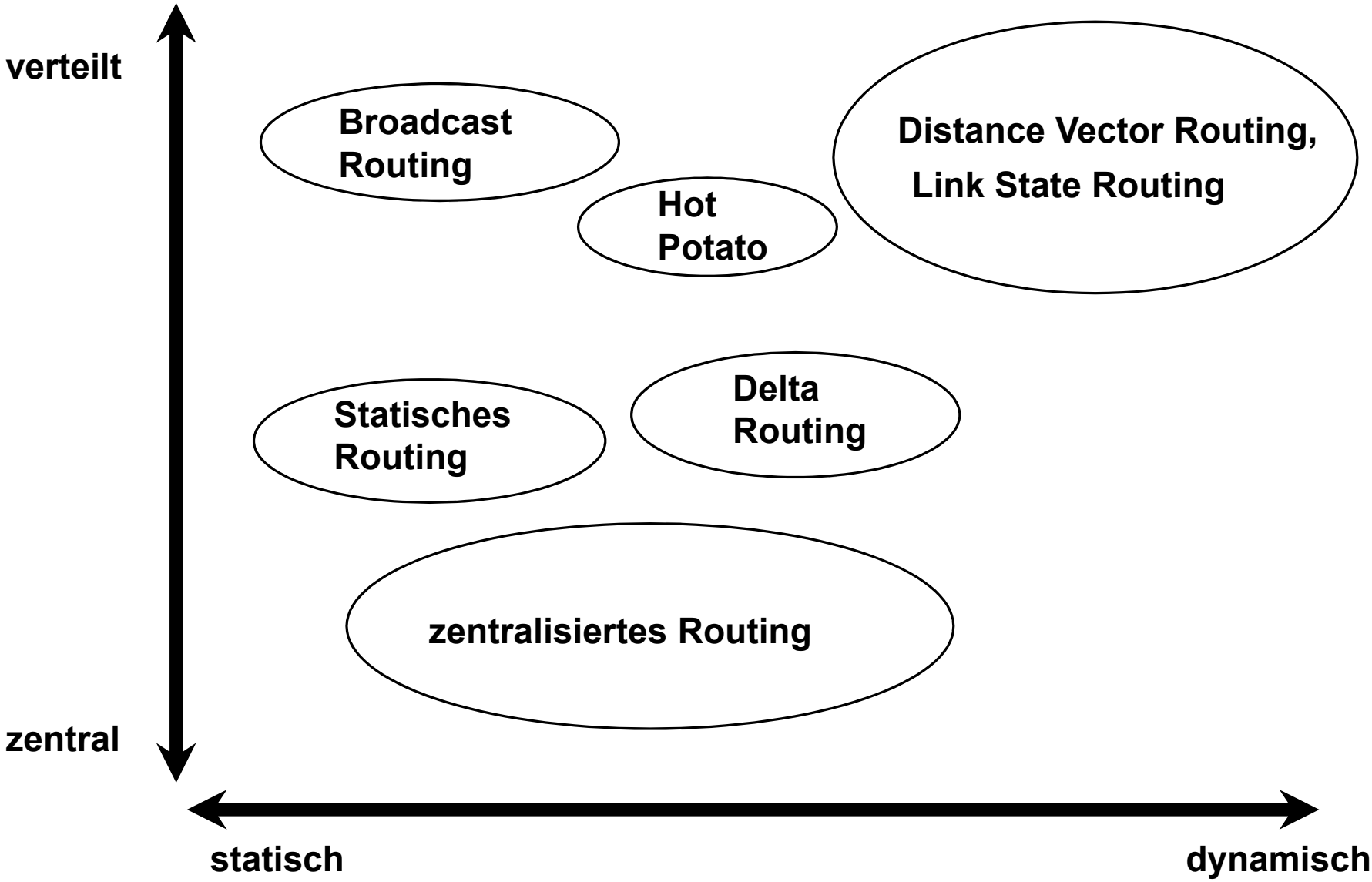
- **Dynamik des Routing-Verfahrens:**
  - **Nicht adaptiv (statisch):** die Routing-Tabellen in den Vermittlungsknoten bleiben über längere Zeit konstant (verglichen mit Verkehrsänderungen)
  - **Adaptiv (dynamisch):** Routing-Entscheidungen hängen vom Zustand des Netzes ab (Topologie, Lastverhältnisse), und passen sich schnell an.
    Für die Wegewahl sind Veränderungen der Topologie oder die aktuelle Auslastung einer Leitung entscheidend.
    Für die Berücksichtigung des momentanen Netzzustandes ist ein Informationsaustausch zwischen den Knoten notwendig.

Router
→ Routing-Verfahren (3/3)

- **Zeitpunkt der Wegwahlentscheidung:**
  - Datenübertragung mit Hilfe einzelner Datagramme: erneute Wegewahl für jedes einzelne IP-Paket
  - Verbindungsorientierte Datenübertragung (z.B. Telefonnetz): einmalige Wegewahl, alle nachfolgende Datenpakete folgen diesem Weg

- **Art der Informationsbeschaffung:**
  - Jeder **Knoten entscheidet isoliert** (*Isolated Routing*, hierunter fallen z.B. Broadcast Routing, Hot Potato, ...) ohne Informationsaustausch mit anderen Routern
  - Benachbarte **Knoten tauschen Informationen aus**
  - Informationen betreffen nicht nur lokale Bereiche, sondern sind übergreifend und **werden zentral gesammelt**

Router
→ Übersicht der Routing-Verfahren



Statisches Routing (1/2)

- Statische Routing ist ein einfaches nicht adaptives Verfahren, welches von vielen kleinen stabilen IP-Netzen benutzt wird.

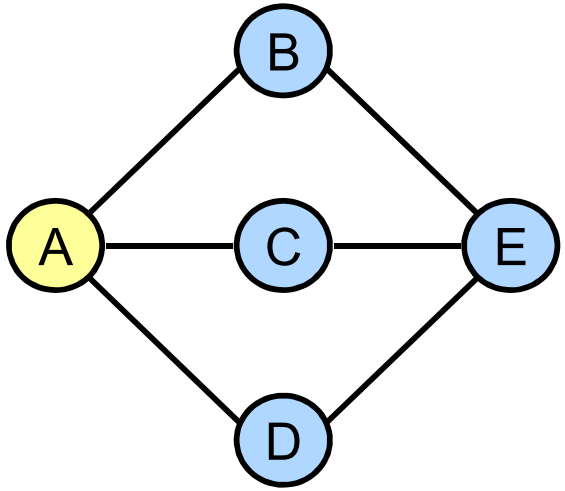
- **Verfahren:**
  - Jeder Knoten unterhält eine Tabelle mit einer Zeile für jeden möglichen Zielknoten.
  - Der komplette Inhalt dieser Tabellen wird statisch in jedem Router konfiguriert.
  - Eine Zeile enthält z.B. n Einträge, welche die beste, zweitbeste, etc. Übertragungsleitung für dieses Ziel ist, zusammen mit einer **relativen Gewichtung entsprechend der Kapazität** der jeweiligen Leitung.
  - Vor der Weiterleitung eines Pakets wird eine Zufallszahl gezogen und eine der Alternativen anhand der Gewichtung ausgewählt

Statisches Routing (2/2)

- Beispiel:
  - Ziehen einer Zufallszahl x, mit $0.99 \geq x \geq 0.00$
  - Falls $x < 0.6$ dann Weiterleiten nach B
  - Falls $0.9 \geq x \geq 0.6$ dann Weiterleiten nach C
    sonst Weiterleiten nach D

Tabelle in Knoten A

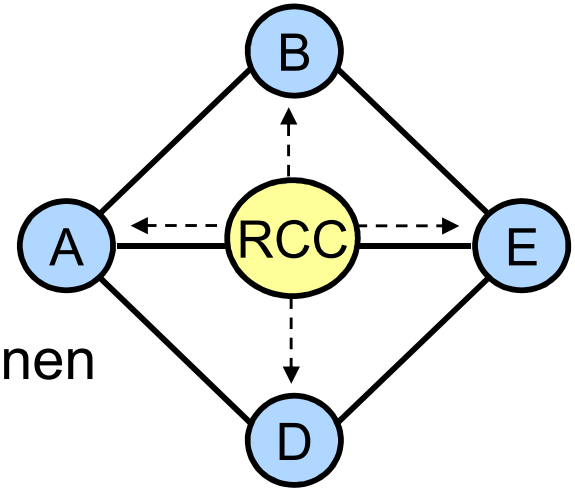
Ziel	1. Wahl		2. Wahl		3. Wahl	
	Kn	Gew	Kn	Gew	Kn	Gew
E	B	0,6	C	0,3	D	0,1
⋮						



- Statisches Routing ist ein mächtiges Werkzeug, um das Routing-Verhalten in einem Netzwerk präzise zu kontrollieren.
- Wenn jedoch regelmäßige Änderungen in der Topologie auftreten, kann der hierfür erforderliche Aufwand der manuellen Neukonfiguration ein statisches Routing undurchführbar machen.

Zentralisiertes Routing

- Ist ein adaptives Routingverfahren.
- **Verfahren:**
  - Im Netz gibt es ein Routing Control Center (RCC)
  - Jeder Knoten sendet periodisch Zustandsinformationen an das RCC, z.B.:
    - Liste aller aktiven Nachbarn
    - Aktuelle Längen der Warteschlangen
    - Umfang an Verkehr, der seit dem letzten Bericht abgewickelt wurde
  - RCC sammelt diese Zustandsinformationen und berechnet aufgrund dieser Kenntnis über das gesamte Netz die optimalen Wege zwischen allen Knoten (z.B. kürzeste Wege)
  - Jeder Knoten trifft seine Routing-Entscheidungen anhand der ihm zugewiesenen Routing-Tabelle vom RCC



Zentralisiertes Routing

- **Vorteile:**
  - Im Prinzip hat das RCC die vollständige Übersicht, und damit können perfekte Entscheidungen getroffen werden.
  - Die Router müssen keine aufwendigen Routing-Berechnungen durchführen.

- **Nachteile:**
  - Für große Netze dauert die Routing-Berechnung sehr lang.
  - Der Ausfall des RCCs lähmt das ganze Netz, dadurch ist eine Redundanz durch Back-up Rechner dringend erforderlich.
  - Es sind globale Inkonsistenzen möglich, da Router nahe dem RCC neue Routing-Tabellen wesentlich früher erhalten, als weiter entfernte Knoten.
  - Eine starke Belastung des RCCs durch die zentrale Funktion.

Hot Potato

- Hot Potato ist ein isoliertes Routing, d.h. es findet keinerlei Austausch mit den Nachbarknoten bezüglich der Wegwahlinformation statt.
- **Verfahren:**
  - Jeder Knoten versucht, eingehende Pakete so schnell wie möglich weiterzuleiten (bildhaft, wie eine heiße Kartoffel).
  - Die Übertragungsleitung mit der kürzesten Warteschlange wird für die Weiterleitung genutzt.
  - Hierbei kann es jedoch zu sehr großen Umwegen kommen (kürzeste Warteschlange ist i.d.R. nicht der kürzeste Weg!).
- **Varianten:**
  - Auswahl der besten Übertragungsleitung nach statischem Verfahren, solange deren Warteschlange unter einer bestimmten Schwelle bleibt.
  - Auswahl der Übertragungsleitung mit kürzester Warteschlange, falls deren statisches Gewicht nicht zu niedrig ist.

Broadcast Routing (1/2)
→ Fluten (Flooding)

- Broadcast Routing wird auch Fluten (Flooding) genannt.
- Ist ein statisches, isoliertes und einfaches Routingverfahren, d.h. auch hier findet keinerlei Austausch mit den Nachbarknoten bezüglich der Wegwahlinformation statt.
- **Verfahren:**
  - Jedes eingehende Paket wird auf allen Übertragungsleitungen (Ausgangsleitungen) weitergeleitet, außer auf derjenigen, auf er es eingetroffen ist.
  - Probleme:
    - Beim Flooding werden viele Paketduplikate erstellt (Paketflut).
    - Diese Zahl kann unendlich sein (z.B. durch Zirkulieren), wenn nicht Maßnahmen ergriffen werden, um diese einzudämmen.

Broadcast Routing (2/2)
→ Fluten (Flooding)

- **Maßnahmen zur Eindämmung der Flut:**
  - Erkennung von Duplikaten durch die Numerierung der Pakete.
  - Kontrolle der Lebensdauer eines Pakets durch Zählen der zurückgelegten Teilstrecken (hops).
    - Initialisierung eines hop-Zählers im Paket durch minimale bzw. maximale Weglänge zwischen Quelle und Ziel.
    - Dekrementieren des Zählers um 1 in jedem Knoten.
    - Bei Erreichen von 0 Verwerfung des Pakets.

- **Varianten:**
  - Selektives Fluten bedeutet, dass Weiterleitung nicht auf allen, sondern nur auf einigen Ausgangsleitungen durchgeführt wird.
  - Random Walk bedeutet die zufällige Auswahl einer Ausgangsleitung.

Distance Vector Routing
→ Übersicht

- Distance Vector Routing ist ein **verteiltes, adaptives Routing.**
- Jeder Knoten tauscht periodisch Routing-Informationen mit jedem Nachbarn aus.
- Typischerweise unterhält jeder Knoten eine Routing-Tabelle, die für jeden anderen Knoten im Netz einen Eintrag enthält, beispielsweise über:
  - bevorzugte Übertragungsleitungen
  - Schätzung über Zeit oder Entfernung zu diesem Knoten.
- Distance Vector Routing wurde früher als RIP (Routing Information Protocol) im Internet viel benutzt.

Distance Vector Routing
→ Verfahren

- Jeder Router speichert eine Tabelle mit den besten Entfernungen (z.B. Anzahl der hops, Verzögerung in ms) zu jedem Ziel und dem dazugehörigen Ausgang.
- Diese Tabelle wird periodisch mit den Nachbarn austauscht.

- **Bewertung:**
  - Die Ansprüche an den Router sind sehr gering, da er nur den jeweiligen nächsten Hop kennen muss.
  - Allerdings stabilisieren sich die Routing-Tabellen im Netz nur sehr langsam, wenn sich Veränderungen in den Routern ergeben („count-to-infinity“-Problematik).

Distance Vector Routing
→ Beispiel (1/4)

- Als Beispiel nehmen wir an, dass die Übertragungszeit als Maß verwendet wird und der Router die Übertragungszeit zu allen seinen Nachbar-Router kennt (mit Hilfe von ECHO-Paketen).
- Einmal alle T s sendet jeder Router an jeden Nachbarn eine Liste mit den geschätzten Übertragungszeiten zu jedem Ziel.
- Das heisst auch, jeder Router empfängt eine Liste seiner Nachbarn.
- Nehmen wir an, dass eine Tabelle gerade vom **Nachbarn-Router X** eingetroffen ist, wobei **Xy** die Schätzung von **X** ist, wie lange der Weg zu **Router Y** dauert.
- Wenn der Router weiß, dass die Übertragung zu **X m** ms dauert, weiß er auch, dass er **Router Y** über **X** in **Xy+m** ms erreichen kann.
- Wenn man dies für jeden Nachbarknoten berechnet, kann ein Router herausfinden, welche Schätzung am besten zu sein scheint, und diese mit der zugehörigen Leitung dann in seiner neuen Routing-Tabelle verwendet.

Distance Vector Routing
→ (2/4) - Liste der geschätzten Übertragungszeiten

- Die ersten vier Spalten zeigen die von den Nachbarn von Router J eingegangenen Übertragungsvektoren.

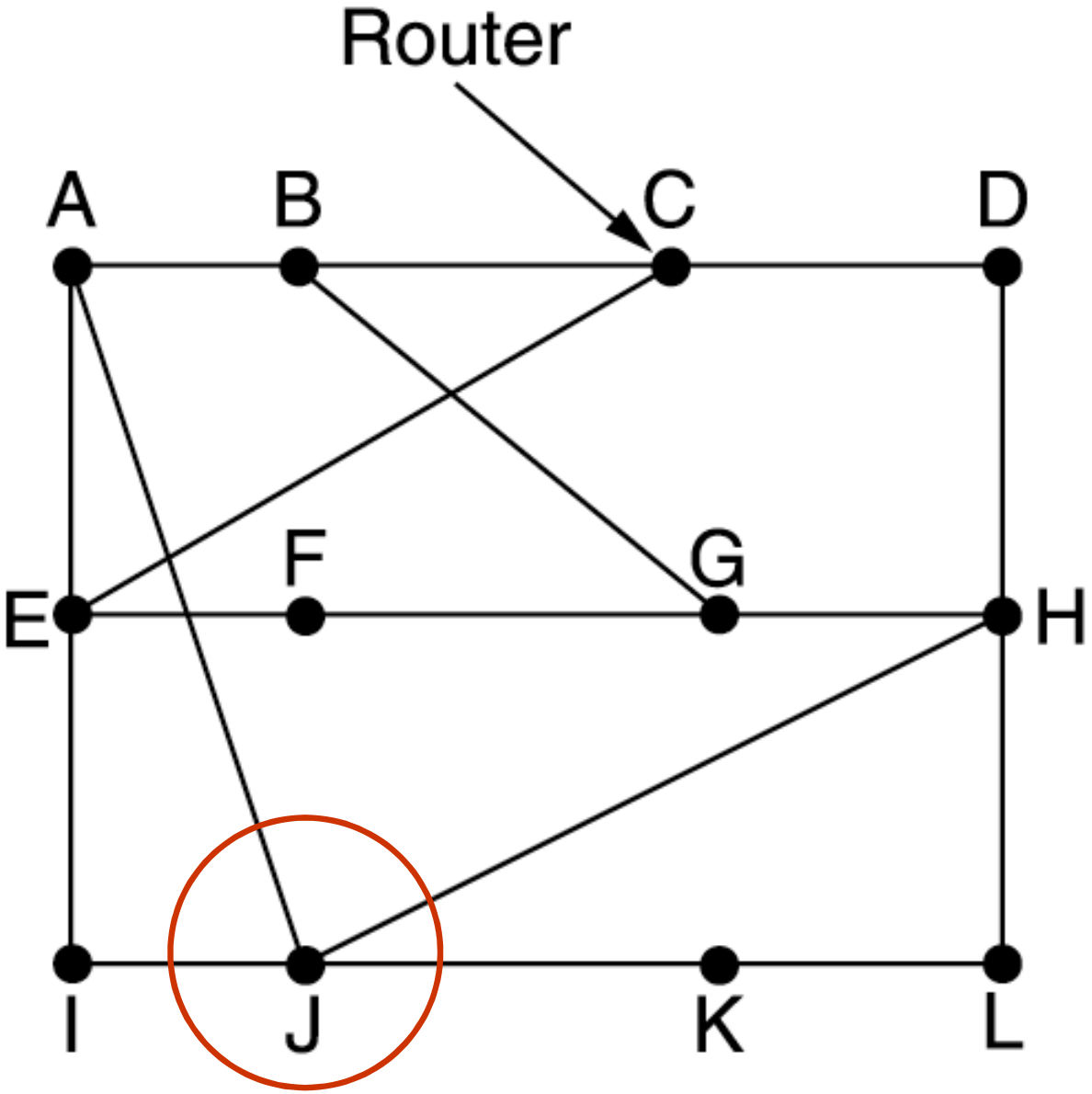
- J selber schätzt die Übertragungszeit:
  - zu A auf 8 ms,
  - zu I auf 10 ms,
  - zu H auf 12 ms und
  - zu K auf 6 ms.

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA	JI	JH	JK
	Verzög. ist 8	Verzög. ist 10	Verzög. ist 12	Verzög. ist 6

Von den vier Nachbarn von J erhaltene Vektoren

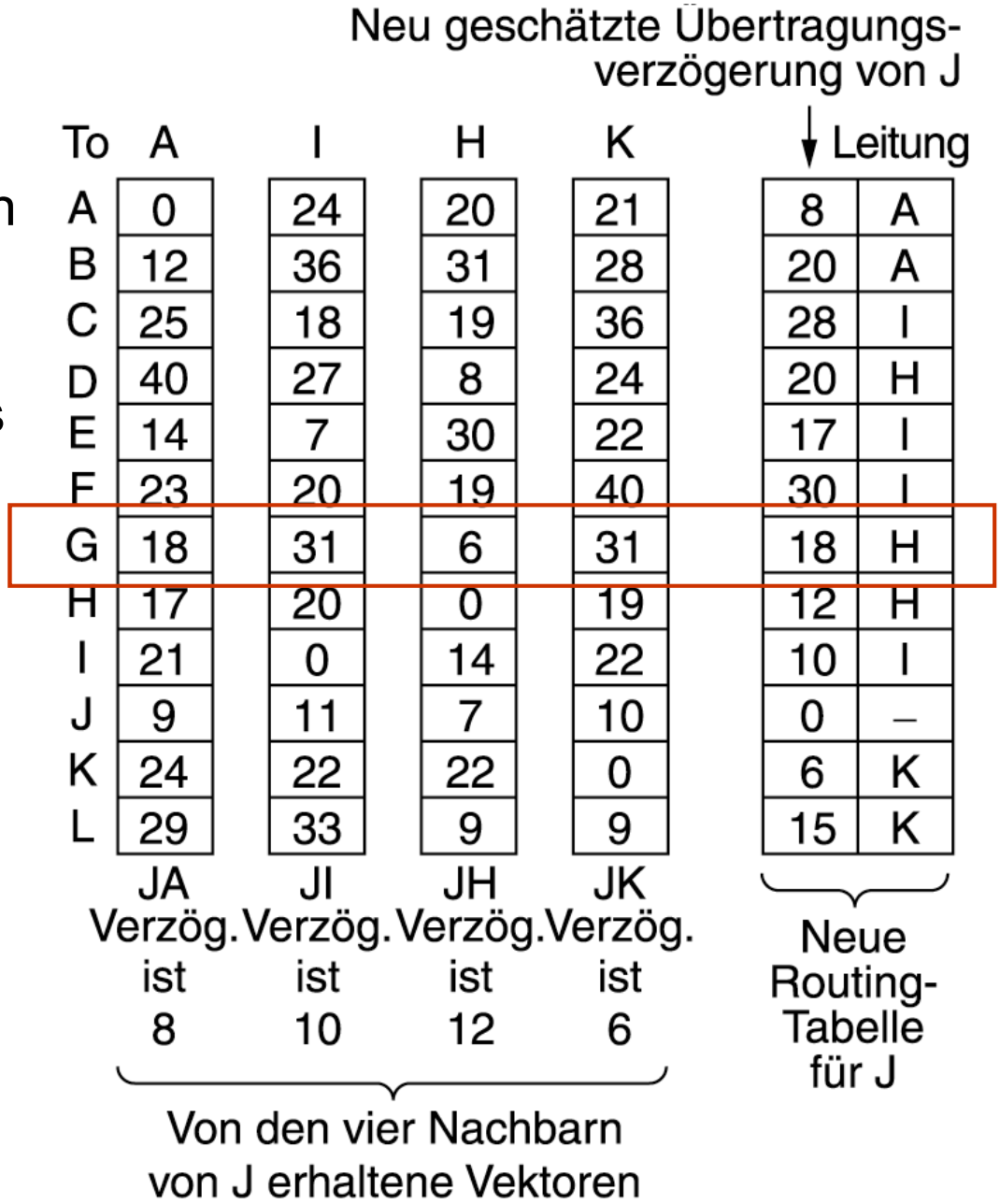
Distance Vector Routing
→ Beispiel (3/4)

- Beispiel-Teilnetz



Distance Vector Routing
→ (4/4) Berechnung des neuen Weg zu Router G

- J weiss, dass er A in 8 ms erreichen kann.
- A behauptet, G in 18 ms erreichen zu können.
- Daraus schließt J, dass er mit einer Übertragungszeit von 26 ms zu G rechnen muss, wenn er das Paket für G nach A überträgt.
- Weitere Berechnungen:
  - über I 41 (31+10) ms
  - **über H 18 (6+12) ms**
  - über K 37 (31+6) ms
- Über H ist der schnellest Weg zu G, aus diesem Grund trägt J in seine Routing-Tabelle H ein.
- Die gleiche Berechnung wird für alle anderen Ziele durchgeführt.



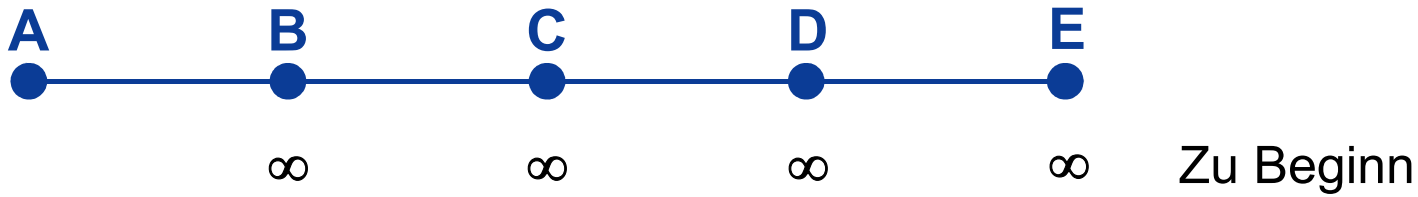
Distance Vector Routing
→ Count-to-Infinity-Problem (1/6)

- Distance Vector Routing funktioniert theoretisch, hat in der Praxis aber einen großen Nachteil.
- Der Algorithmus führt zwar zur richtigen Lösung, schafft das aber sehr langsam.
- Insbesondere reagiert er schnell auf gute Nachrichten, aber sehr träge auf schlechte Nachrichten.
- Nehmen wir an, der beste Weg eines Routers zu Ziel X ist lang.
- Meldet Nachbar A beim nächsten Mal plötzlich eine kürzere Übertragungszeit zu X, schaltet der Router einfach um, indem er Leitungen A verwendet, um den Datentransfer an X zu senden.
- Die gute Nachricht wird mit einem einzigen Austausch im Vektor verarbeitet.

Distance Vector Routing
→ Count-to-Infinity-Problem (2/6)

- Um zu sehen, wie schnell sich gute Nachrichten verbreiten, betrachten wir das (lineare) Teilnetz mit fünf Knoten, bei dem das Maß für die Übertragung die Anzahl der Teilstecken ist.

- Wir nehmen an, dass A anfänglich nicht in Betrieb ist und dies alle anderen Router wissen.
- Mit anderen Worten, sie haben alle die Übertragung nach A als unendlich registriert.



- Schaltet sich A wieder zu, erfahren das die anderen Router über den Vektoraustausch.
- Wir nehmen an, dass alle Router gleichzeitig den Vektoraustausch durchführen.

Distance Vector Routing
→ Count-to-Infinity-Problem (3/6)

- Zum Zeitpunkt des ersten Austausches erfährt B, dass sein linker Nachbar eine Übertragungszeit von 1 zu A hat.
- B trägt in seine Routing-Tabelle ein, dass A **eine** Teilstrecke nach links entfernt liegt.
- Alle anderen Router glauben noch, dass A ausgeschaltet ist.
- An diesem Punkt sehen die Einträge in der Routing-Tabelle für A noch folgendermaßen aus:

B	C	D	E	
∞	∞	∞	∞	Zu Beginn
1	∞	∞	∞	Nach 1. Austausch

- Beim nächsten Mal erfährt C, dass B einen Pfad von Länge 1 zu A hat.
- Folglich aktualisiert C seine Routing-Tabelle auf 2, was D und E aber erst später erfahren.

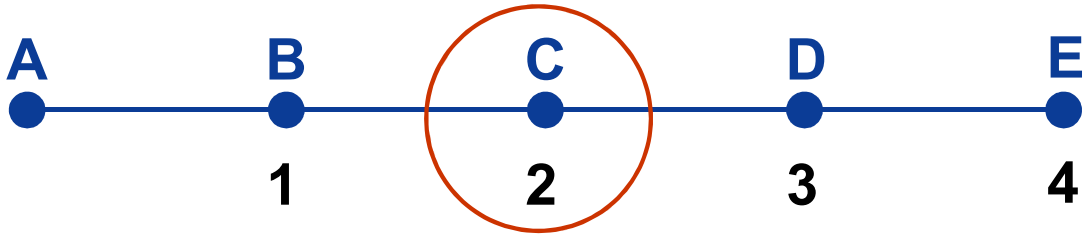
Distance Vector Routing
→ Count-to-Infinity-Problem (4/6)

B	C	D	E	
∞	∞	∞	∞	Zu Beginn
1	∞	∞	∞	Nach 1. Austausch
1	**2**	∞	∞	Nach 2. Austausch
1	**2**	**3**	∞	Nach 3. Austausch
1	**2**	**3**	**4**	Nach 4. Austausch

- Die gute Nachricht verbreitet sich in der Geschwindigkeit von einer Teilstrecke pro Austausch.
- In einem Teilnetz, dessen längster Pfad ein Länge von N Teilstrecken hat, tauschen alle innerhalb von N die Nachrichten über neu zugeschaltete Router und Leistungen aus.

Distance Vector Routing
→ Count-to-Infinity-Problem (5/6)

- Was passiert nun, wenn A ausfällt oder die Leitung zwischen A und B unterbrochen wird, was aus der Sicht von B das Gleiche ist?



Zu Beginn

- Beim ersten Paketaustausch hört B überhaupt nichts von A.
- C teit aber mit, dass er einen Pfad der Länge 2 zu A hat.
- B weiß nicht, dass dieser Pfad über ihn, B, zu A führt.
- Deshalb denkt B, er könne A über C mit einer Pfadlänge von 3 erreichen und aktualisiert seine Tabelle.
- Beim nächsten Austausch erfährt C, dass alle seine Nachbarn behaupten, einen Pfad der Länge 3 zu A zu haben.
- Er wählt einen aus und setzt seine Entfernung zu A auf 4.
- Diese Spiel setzt sich weiter fort, bis irgendwann alle Router den Wert ∞ für die Entfernung zu A in der Tabelle haben.
- Wie lange dies geschieht, hängt vom numerischen Wert von ∞ ab.

Distance Vector Routing
→ Count-to-Infinity-Problem (6/6)

B	C	D	E	
1	2	3	4	Zu Beginn
3	2	3	4	Nach 1. Austausch
3	4	3	4	Nach 2. Austausch
5	4	5	4	Nach 3. Austausch
5	6	5	6	Nach 4. Austausch
7	6	7	6	Nach 5. Austausch
7	8	7	8	Nach 6. Austausch
...	...	...	...	...
∞	∞	∞	∞	Nach ∞. Austausch

- Bei diesem Beispiel wird deutlich, dass sich schlechte Nachrichten langsam verbreiten.
- Die Zahl der benötigten Übertragungen hängt davon ab, auf welchen Wert ∞ gesetzt wurde.
- Daher wird ∞ auf den längsten Pfad+1 gesetzt.
- Als Metrik kann nicht die Verzögerung verwendet werden, da es hier keine definierte Obergrenze gibt.

Link State Routing
→ Übersicht (1/2)

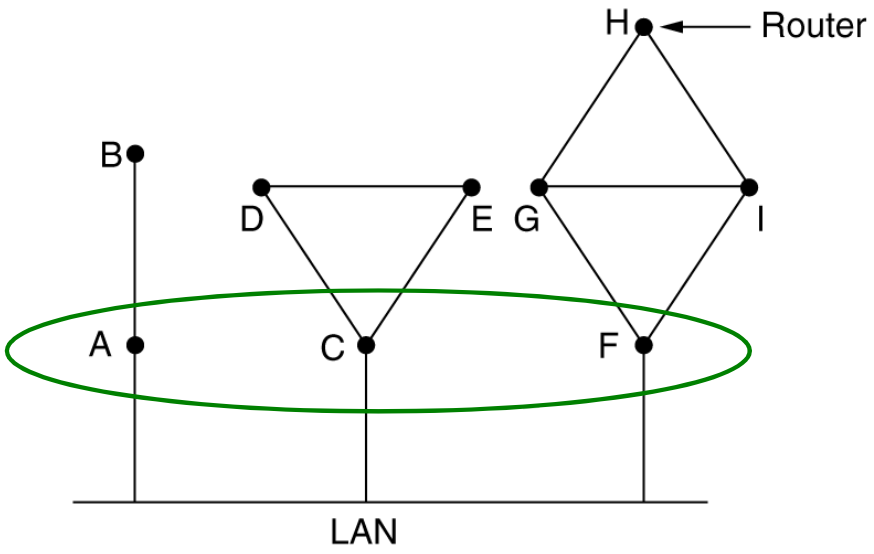
- Link State Routing ist ein verteiltes und adaptives Routing-Verfahren.
- Der Name Link State (Zusand der Verbindung) beschreibt die Tatsache, dass bei diesem Routing-Verfahren jeder Router die Topologie des kompletten Netzes kennt, an das er angeschlossen ist.
- Damit kann ein Router den besten Weg eines Datenpaketes selbst ermitteln.
- Dazu müssen die Router die Informationen des Netzes in geeigneter Weise in ihrer Datenbank speichern.
- Das Link State Routing stellt im Gegensatz zum Distance Vector Routing **sehr hohe Ansprüche an die Rechnerleitung und Speicherressourcen der Router**.
- Dafür stabilisiert sich die Routing-Tabelle bei einer Veränderung aber sehr viel schneller.

Link State Routing
→ Übersicht (2/2)

- Das Link State Routing besteht aus fünf Schritten:
  - **1.** Die **Nachbarn und deren Netzadressen ermitteln** (Hello-Paket)
  - **2.** Die **Übertragungszeit oder die Kosten** zu jedem seiner Nachbarn **messen** (ECHO-Paket)
  - **3.** Ein **Paket zusammenstellen**, in dem alles steht, was gelernt wurde
  - **4.** Dieses **Paket an alle anderen Router senden** (Flooding)
  - **5.** Den **kürzesten Pfad zu allen anderen Routern berechnen** (SPF-Algorithmus (Shortest Path First Algorithmus) von E. W. Dijkstra)

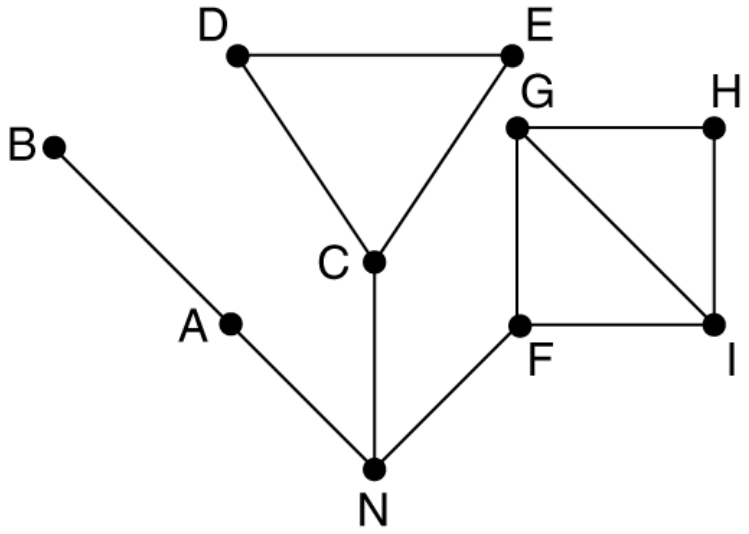
Link State Routing
→ 1. Ermittlung der Nachbar-Router (1/2)

- Nach dem Start muss ein Router als erstes ermitteln, wer seine Nachbarn sind.
- Hierzu sendet er ein spezielles HELLO-Paket auf jede Punkt-zu-Punkt-Leitung.
- Der Router am anderen Ende muss eine Antwort zurücksenden, durch die er seine Identität bekannt gibt.
- Diese Namen müssen global eindeutig sein.
- Sind zwei oder mehrere Router an ein LAN angeschlossen, ist die Situation etwas komplizierter.



Link State Routing
→ 1. Ermittlung der Nachbar-Router (2/2)

- Ein Möglichkeit, das LAN zu modellieren, ist, es selbst als Knoten zu betrachten.



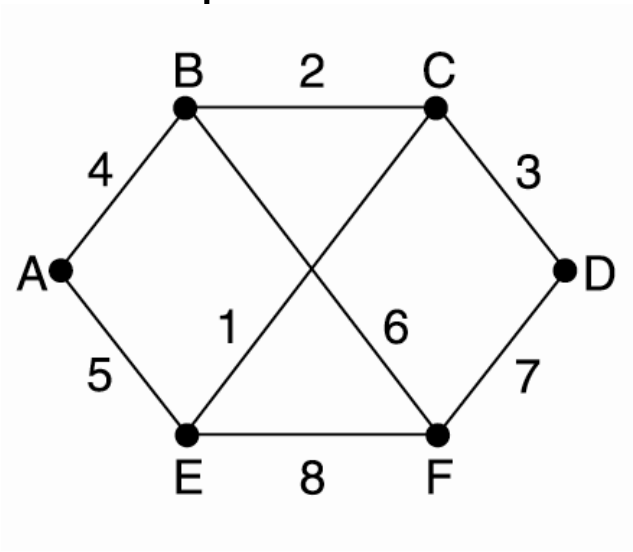
- Hier wird ein neuer künstlicher Knoten N eingeführt, an dem A, C und F angeschlossen sind.
- Die Tatsache, dass man im LAN von A nach C gelangen kann, ist hier durch den Pfad A-N-C dargestellt.

Link State Routing
→ 2. Ermittlung der Leitungskosten

- Das Link State Routing setzt voraus, dass jeder Router die Übertragungszeit zu seinen Nachbarn kennt oder zumindestens einen guten Schätzwert dafür hat.
- Der direkteste Weg, diese Übertragungszeit zu ermitteln, ist das Aussenden eines speziellen ECHO-Pakets.
- Die andere Seite muss es sofort wieder zurücksenden.
- Durch Messen der Hin- und Rückreisezeit, geteilt durch zwei, kann der sendende Router die Übertragungszeit vernünftig abschätzen.
- Besse Ergebnisse werden erzielt, wenn der Test mehrmals wiederholt und dann der Durchschnitt gebildet wird.

Link State Routing
→ 3. Link-State-Pakete erstellen (1/2)

- Nachdem die erforderlichen Informationen für den Austausch erfasst wurden, muss jeder Router im nächsten Schritt ein Paket mit allen Daten zusammenstellen.
- Das Paket beginnt mit der Identität des Senders, gefolgt von einer Folgenummer und dem Alter sowie einer Liste der Nachbarn mit den entsprechenden Verzögerung.



Link-State-Pakete

A	
Folge-Nr.	
Alter	
B	4
E	5

B	
Folge-Nr.	
Alter	
A	4
C	2
F	6

C	
Folge-Nr.	
Alter	
B	2
D	3
E	1

D	
Folge-Nr.	
Alter	
C	3
F	7

E	
Folge-Nr.	
Alter	
A	5
C	1
F	8

F	
Folge-Nr.	
Alter	
B	6
D	7
E	8

Link State Routing
→ 3. Link-State-Pakete erstellen (2/2)

- Das Erstellen von Link-State-Paketen ist einfach.
- Der schwierige Teil ist die Frage, wann sie erstellt werden sollen.
- Eine Möglichkeit ist, sie periodisch aufzubauen, d.h. in regelmäßigen Abständen.
- Eine Alternative ist die Erstellung, wenn ein bestimmtes wichtiges Ereignis eintritt, z.B. der Ausfall oder die Aufnahme einer Leistung oder eines benachbarten Routers oder eine erhebliche Änderung der Eigenschaften.

Link State Routing
→ 4. Link-State-Pakete verteilen (1/3)

- Der schwierigere Teil des Algorithmus ist die zuverlässige Verteilung der Link-State-Pakete.
- Bei der Verteilung und Installation der Pakete ändern die Router, die sie als erstes erhalten, ihre Wege.
- Folglich werden in verschiedenen Routern eventuell unterschiedliche Versionen der Toplogie verwendet, was zu Inkonsistenzen, Schleifen, unerreichbaren Rechnern und anderen Problemen führen kann.
- Das Basiskonzept des Verteilungsalgorithmus ist die Anwendung von Flooding zur Verteilung der Link-State-Pakete.
- Jedes Paket enthält eine Folgenummer, die bei jedem neu ausgesendeten Paket erhöht wird.
- Die Router vermerken alle Paare (Quell-Router, Folgenummer), die sie sehen.
- Kommt ein neues Link-State-Paket an, wird es mit der Paketliste verglichen.

Link State Routing
→ 4. Link-State-Pakete verteilen (2/3)

- Ist es neu, wird es an alle Leitungen außer derjenigen, auf der es eingegangen ist, ausgegeben.
- Ist es ein Duplikat, wird es verworfen.
- Ist die Folgenummer eines Paketes niedriger als das höchste bisher erfasste, wird das Paket als veraltet abgelehnt.
- Um z.B. ausgefallene Router berücksichtigen zu können, wird das Alter eines Pakets mit aufgenommen (z.B. 60s) und pro Sekunde um 1 reduziert.
- Ist das Alter gleich null, werden die Informationen im Router verworfen.
- Kommt ein neues Paket alle zehn Sekunden an, „veraltet“ ein Paket nur, wenn ein Router ausfällt.
- Das Feld Alter wird von jedem Router auch während des anfänglichen Flooding-Verfahrens um 1 reduziert, um sicherzustellen, dass kein Paket verloren geht und ewig weiterlebt (ein Paket mit dem Alter null wird verworfen).

Link State Routing
→ 4. Link-State-Pakete verteilen (3/3)

- Als Schutz vor Fehlern auf dem Routern/den Router-Leitungen werden alle Link-State-Pakete bestätigt.
- **Beispiel eines Paketpuffer für den Router B**

muss übertragen werden → Sende-Flags ACK-Flags **← muss bestätigt werden**

Quelle	Folge-Nr.	Alter	A	C	F	A	C	F	Daten
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	← da, von A und F gekommen, muss nur an C gesendet werden
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

- Jede Zeile entspricht einem kürzlich angenommenen, aber noch nicht voll verarbeiteten Link-State-Paket.
- In der Tabelle werden der Ursprung des Paketes, die Folgenummer, das Alter und Sende- und Bestätigungs-Flags erfasst.

Link State Routing
→ 5. Berechnung neuer Wege (1/5)

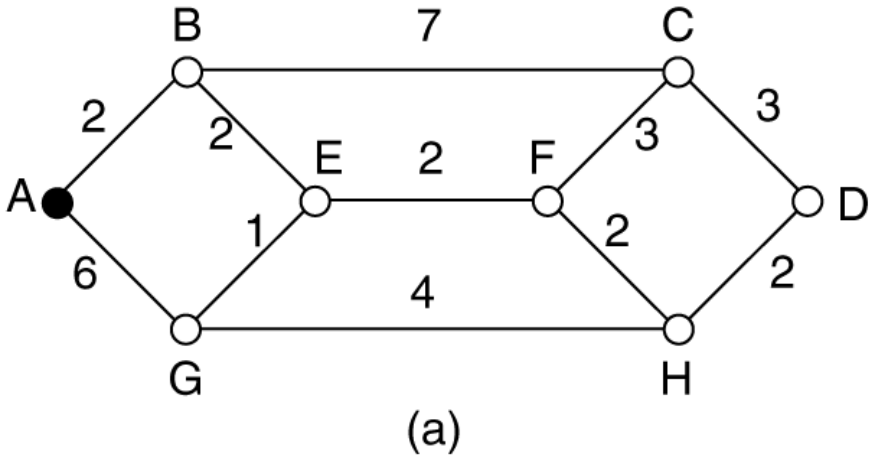
- Nachdem ein Router eine vollständige Menge an Link-State-Paketen angesammelt hat, kann er den Graphen für das Teilnetz aufbauen, weil alle Verbindungen vertreten sind.
- Die Verbindungen werden zweimal dargestellt, je einmal für eine Richtung.
- Die zwei Werte können getrennt verwendet werden, oder aber man berechnet einen Durchschnitt davon.
- Jetzt kann mit einem passenden Algorithmus der kürzeste Pfad zu allen möglichen Zielen ermittelt werden.
- Die Ergebnisse werden in die Routing-Tabelle eingeführt und der Normalbetrieb aufgenommen.
- Bei einem Teilnetz mit n Routern, die je k Nachbarn haben, ist der zum Ablegen der Eingangsdaten erforderliche Speicher proportional zu kn.
- Bei großen Teilnetzen kann der Speicherplatz aber auch die Berechnungszeit problematisch sein.
- Das **OSPF-Protokoll** ist das am häufigste verwendete Routing-Protokoll im Internet und setzt einen Link-State-Algorithmus ein.

Link State Routing
→ 5. Berechnung neuer Wege (2/5)

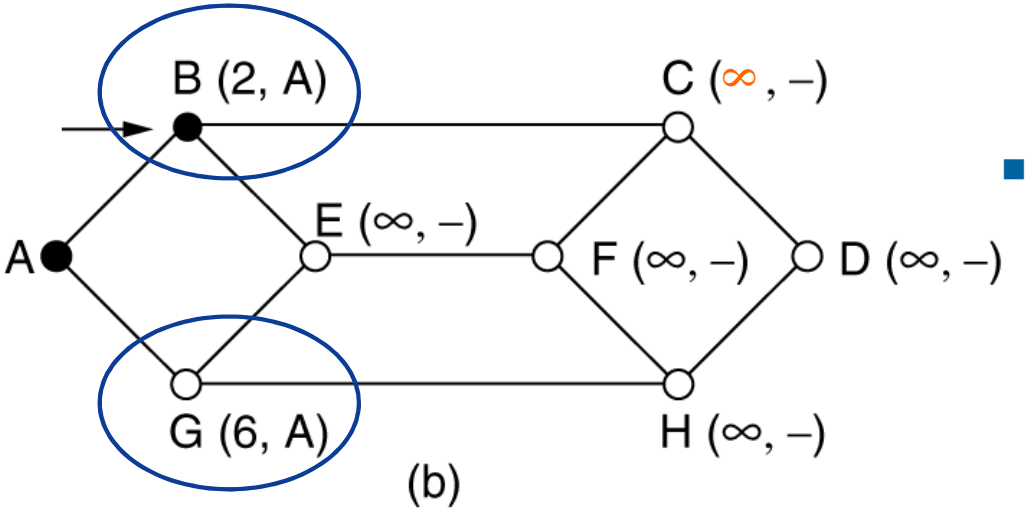
- Berechnung des kürzesten Pfades nach dem SPF-Algorithmus (Shortest Path First Algorithmus) von E. W. Dijksatra.
- Jeder Knoten wird mit seiner Entfernung vom Quellknoten auf dem besten bekannten Pfad beschriftet.
- Anfangs ist kein Pfad bekannt, so dass alle Knoten die Bezeichnung „unendlich“ tragen.
- Je weiter der Algorithmus fortschreitet und Pfade gefunden werden, desto mehr kann sich die Beschriftung ändern und jeweils besser Pfade anzeigen.
- Eine Beschriftung kann povisorisch oder permanent sein.
- Zunächst sind alle Beschriftungen provisorisch.
- Wird festgestellt, dass eine Beschriftung den kürzestmöglichen Pfad von Quelle zu einem Knoten angibt, wird sie permanent gesetzt und danach nie mehr geändert.

Link State Routing
→ 5. Berechnung neuer Wege (3/5)

- Gesucht wird der kürzeste Weg von A nach D.



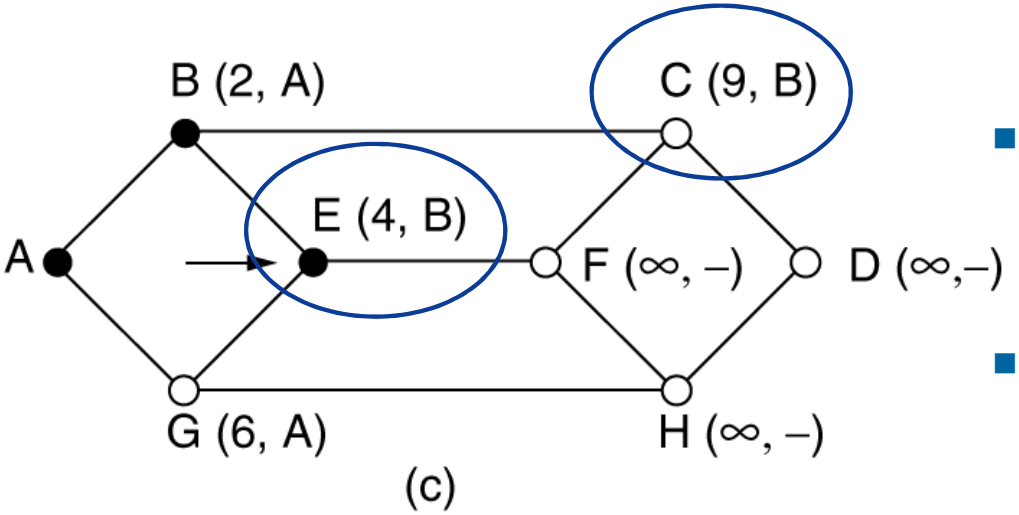
(a)



(b)

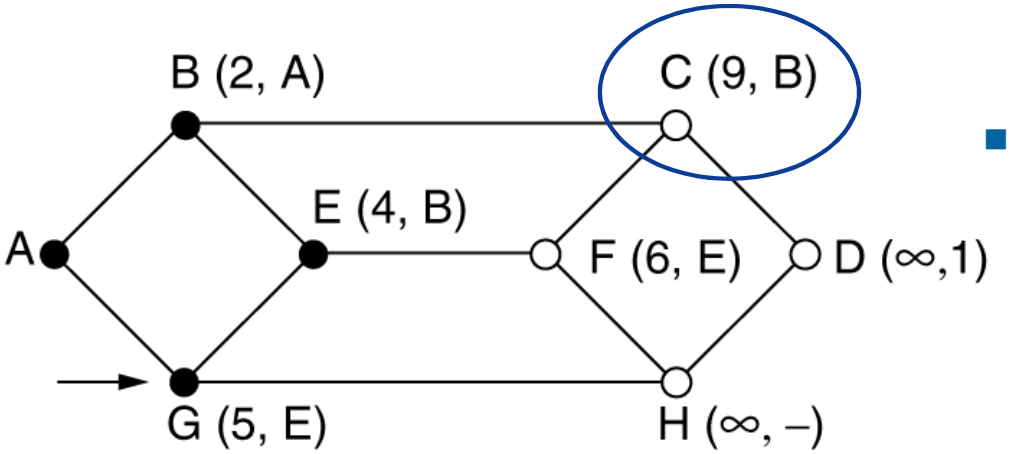
- Im Graphen sind die Gewichtung in Entfernung (1,2,3,...) eingetragen.
- Als erstes wird der Knoten A als permanent markiert.
- Nun wird von A jeder benachbarte Knoten mit der Entfernung beschriftet.

Link State Routing
→ 5. Berechnung neuer Wege (4/5)



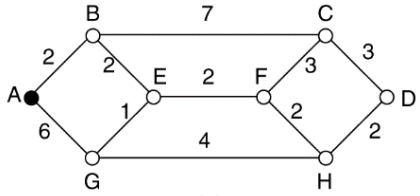
(c)

- Nun wird von B jeder benachbarte Knoten mit der Entfernung beschriftet.
- Da der Weg von A nach E über B der kürzeste ist, wird dieses als permanent markiert.



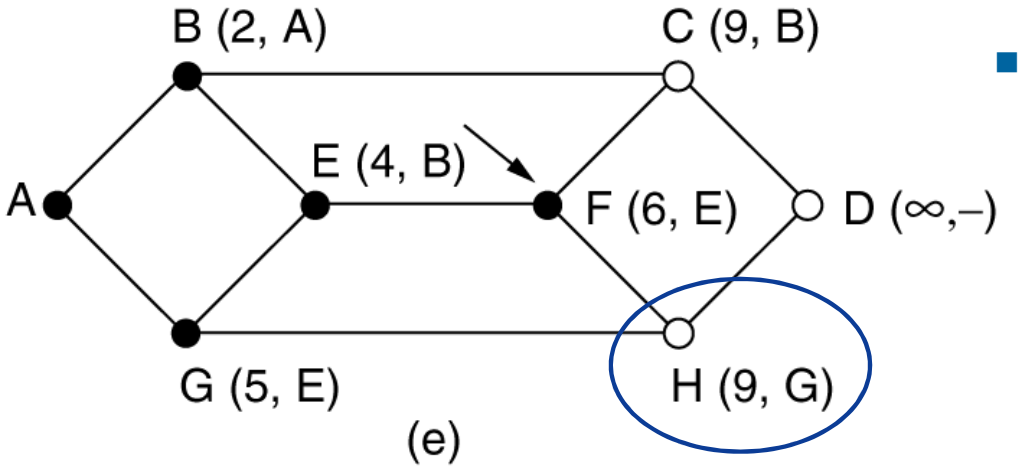
(d)

- Nun wird von E jeder benachbarte Knoten mit der Entfernung beschriftet.

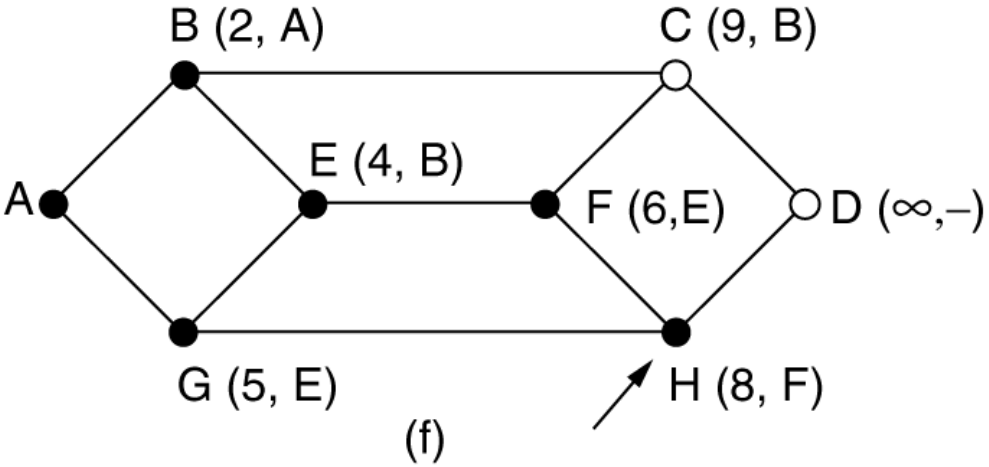


(a)

Link State Routing
→ 5. Berechnung neuer Wege (5/5)



- Nun wird von G jeder benachbarte Knoten mit der Entfernung beschriftet.



- usw.
- Die Komplexität des Algorithmus ist im besten Fall O(n*log n), wobei n die Anzahl der Verbindungen ist.

Inhalt

- Ziele, Einordnung und Übersicht
- Router
- Routing-Verfahren
- **Routing-Protokolle**
- Zusammenfassung

Grundlagen
→ Autonome Systeme (1/2)

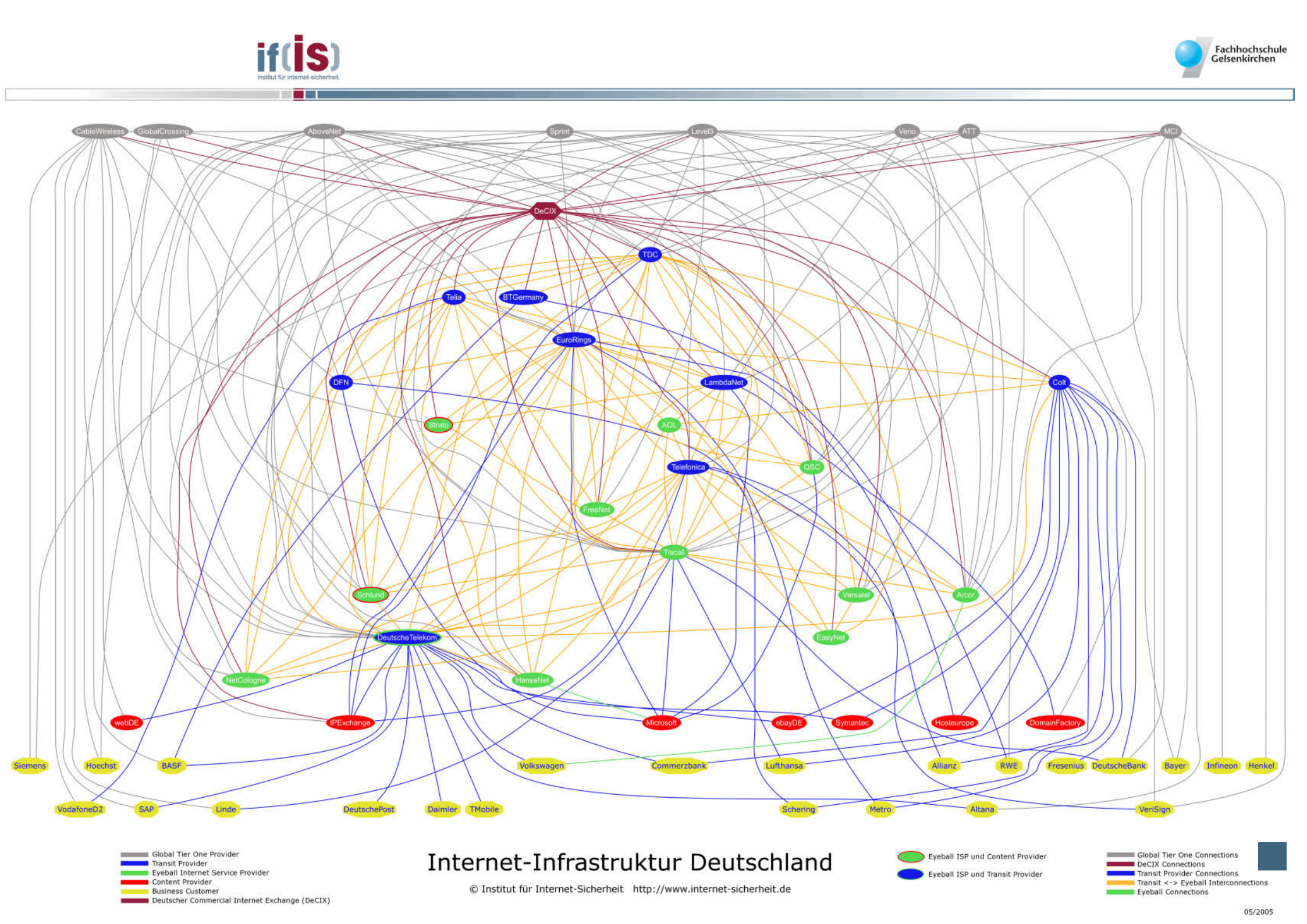
- Ein **Autonomes System (AS)** ist eine **Ansammlung von IP-Netzen** welche als Einheit verwaltet werden

- **Autonome Systeme** stehen unter einer gemeinsamen **administrativen Verwaltung** wie beispielsweise eines Internet Service Providers, einer Firma oder einer Universität

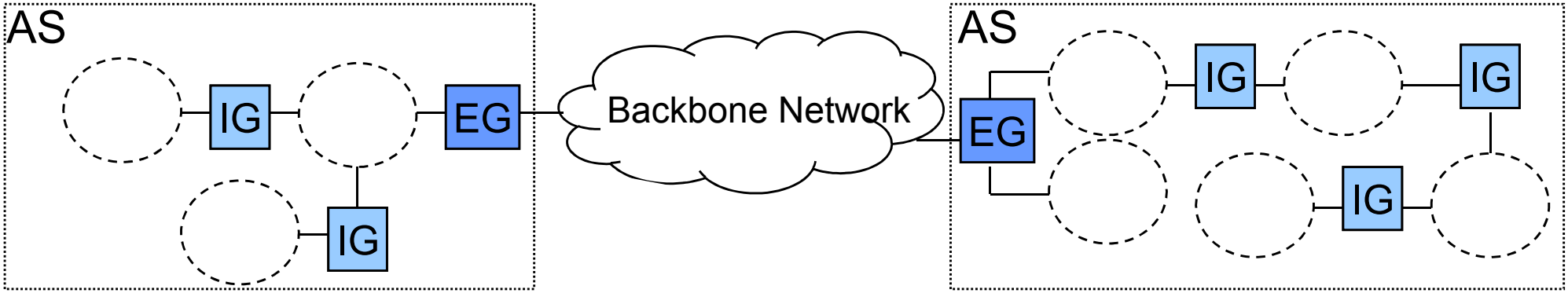
- Jedes **AS** hat eine **eindeutige AS-Nummer** (ASN bzw. AS-ID)
  - AS-IDs sind 16 bit lang, was 65.536 möglichen AS entspricht
  - **Öffentliche AS-IDs** liegen im Bereich **1 bis 64.511**
  - **Private AS-IDs** liegen im Bereich **64.512 bis 65.535**
  - Die **IANA** verwaltet die **Zuteilung** der AS-Nummern

Grundlagen
→ Autonome Systeme (2/2)

- Durch **Verbinden** der **Autonomen Systeme** entsteht das **Internet**
  - Es gibt ca. 60.000 AS im Internet (Stand 2016)
  - Telekom (AS 3320) ist mit ca. 800 anderen AS verbunden
- Jedes **Autonome System** kann ein oder mehrere **IP-Adress-bereiche verwalten**
  - Telekom verwaltet ca. 314 IP-Adressbereiche (Summe: IP-Adr. 33 Mio.)
    - Bsp. 80.128.0.0/11 (CIDR Notation)
- AS schließen oft **Service Level Agreements** untereinander ab
  - Um Peering und Paid-Peering zu regulieren
- Ein gutes Tool, um sich Verbindungen zwischen AS anzusehen
  - **AS-Analyzer** http://www.internet-sicherheit.de


CableWireless
GlobalCrossing
AboveNet
Sprint
Level3
Verio
ATT
MCI
DeCIX
TDC
Telia
BTGermany
EuroRings
DFN
LambdaNet
Colt
Strato
AOL
Telefonica
QSC
FreeNet
Tiscali
Schlund
Versatel
Arcor
EasyNet
DeutscheTelekom
NetCologne
HanseNet
webDE
IPExchange
Microsoft
ebayDE
Symantec
Hosteurope
DomainFactory
Siemens
Hoechst
BASF
Volkswagen
Commerzbank
Lufthansa
Allianz
RWE
Fresenius
DeutscheBank
Bayer
Infineon
Henkel
VodafoneD2
SAP
Linde
DeutschePost
Daimler
TMobile
Schering
Metro
Altana
VeriSign
Global Tier One Provider
Transit Provider
Eyeball Internet Service Provider
Content Provider
Business Customer
Deutscher Commercial Internet Exchange (DeCIX)
Internet-Infrastruktur Deutschland
© Institut für Internet-Sicherheit http://www.internet-sicherheit.de
Eyeball ISP und Content Provider
Eyeball ISP und Transit Provider
Global Tier One Connections
DeCIX Connections
Transit Provider Connections
Transit <-> Eyeball Interconnections
Eyeball Connections
05/2005

Routing-Protokolle
→ Übersicht



- **Autonomes System (AS):**
  - Netz(e) unter einheitlicher Verwaltung.
  - Ein AS kann aus sehr vielen Netzen bestehen, die wiederum intern mit Routern verbunden sind.
- **Interior Gateway (IG):**
  - Interner Router eines autonomen Systems (AS)
- **Exterior Gateway (EG):**
  - Router am Rande eines autonomen Systems (AS)

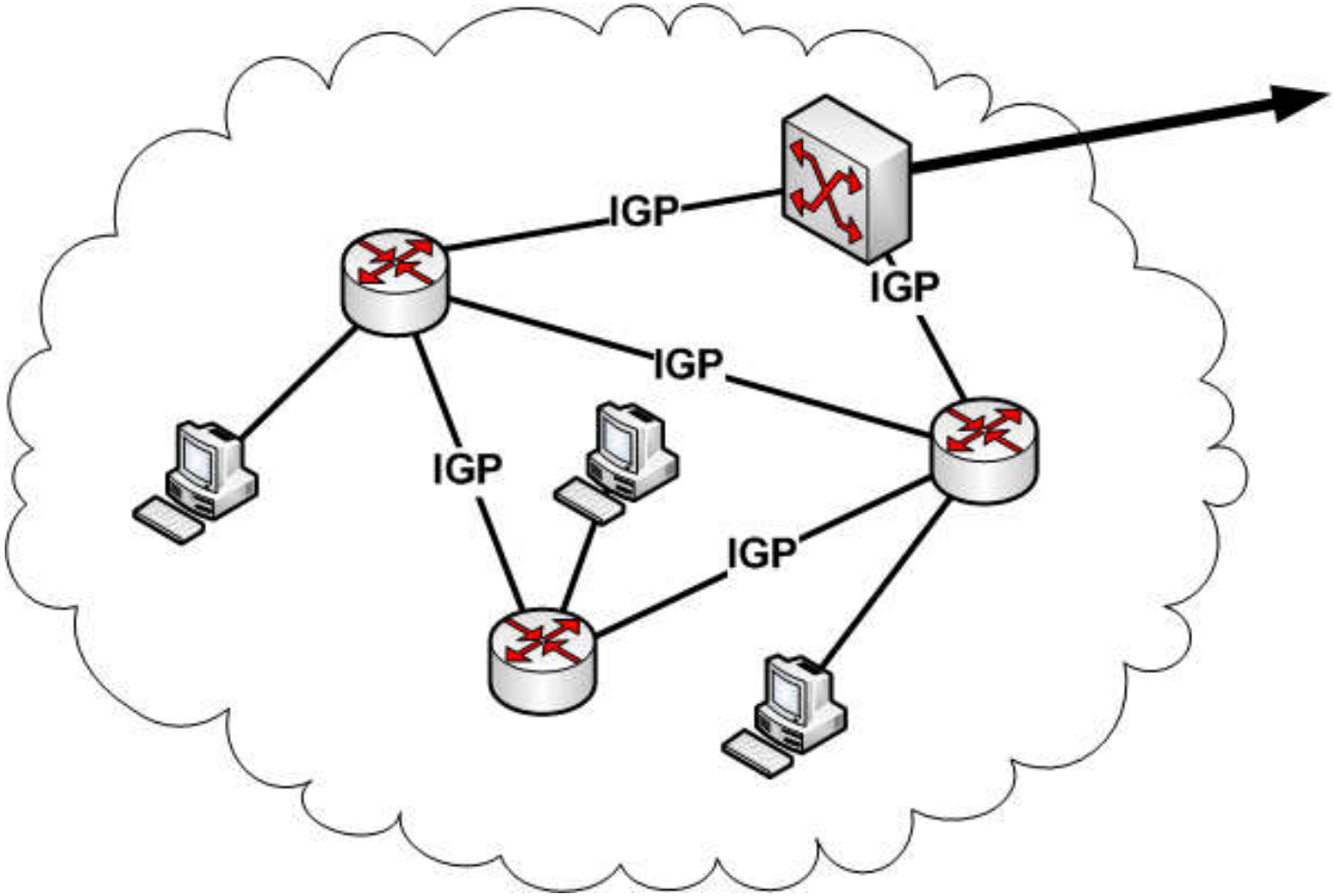
Routing-Protokolle
→ Interior Gateway Protocol (IGP)

- Grundsätzlich unterscheidet man zwei Arten von Routing-Protokollen.
  - **Interior Gateway Protocol (IGP)**
  - **Exterior Gateway Protocol (EGP)**

- Ein **Interior Gateway Protocol (IGP)** wird innerhalb eines Netzes (autonomen Systems) eingesetzt.
- Das bekannteste IGP war das ***Router Information Protocol (RIP)***, welches aufgrund seiner Einschränkungen und Probleme durch das ***Open Shortest Path First (OSPF)*** abgelöst wird.
- Ein internes Gateway-Protokoll muss lediglich Pakete so effizient wie möglich von der Quelle zum Ziel befördern.
- Es muss sich um keinerlei besondere Regeln kümmern.

Grundlagen
→ Interior Gateway Protocol (IGP)

- Routing innerhalb eines AS findet durch ein IGP Protokoll statt



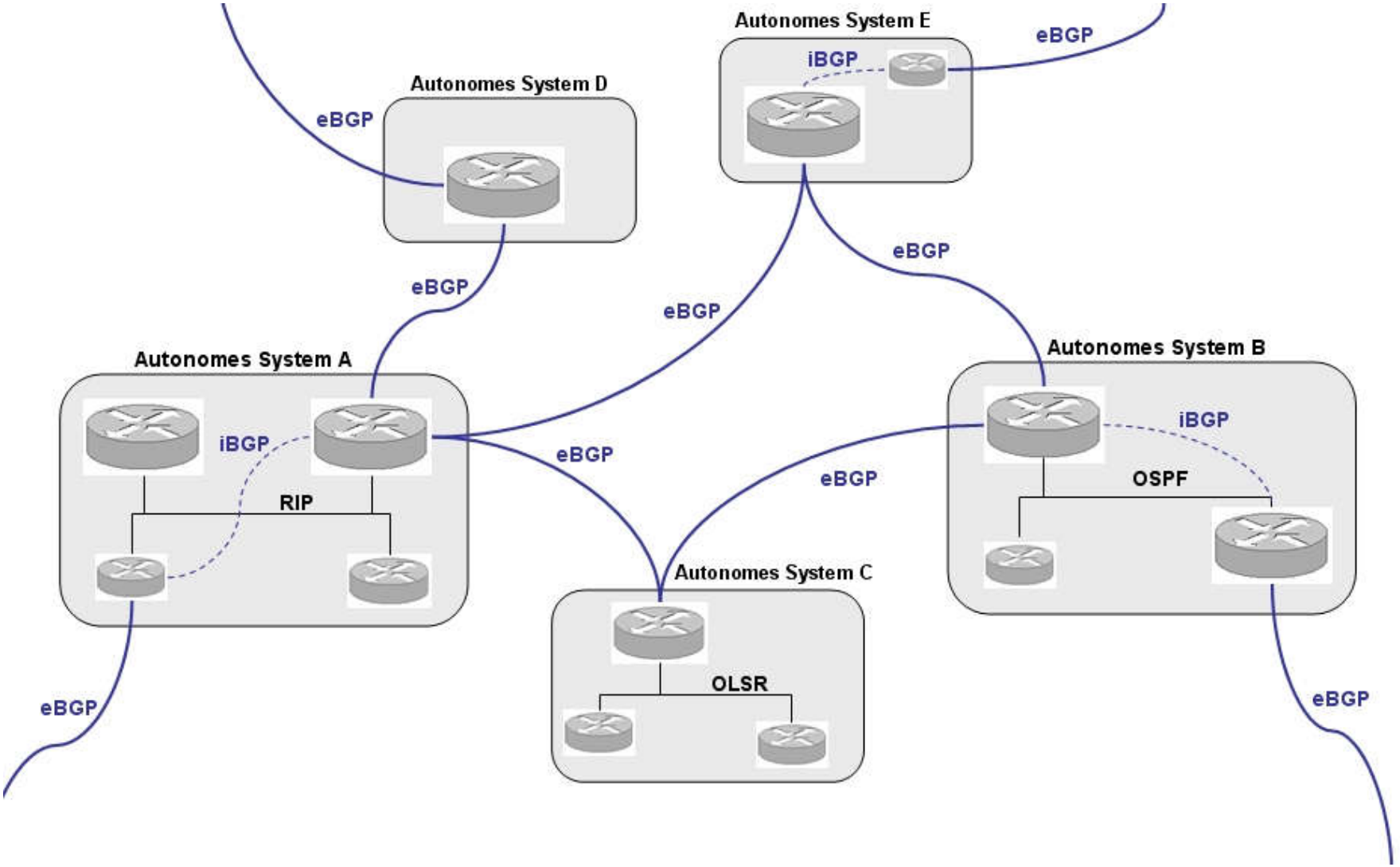
Routing-Protokolle
→ Exterior Gateway Protocol (EGP)

- Zur Kommunikation ***zwischen Routern*** von autonomen Netzen wird ein **Exterior Gateway Protocol (EGP)** eingesetzt.
- Das seit 1984 bestehende Protokoll EGP wurde mittlerweile weitgehend durch das ***Border Gateway Protocol (BGP)*** abgelöst.
- Bei Exterior Gateways müssen besondere Regeln beachtet werden.
- Z.B. ist ein Unternehmen nicht willens, Pakete auf dem Transit von einem fremden autonomen System zu einem anderen fremden autonomen System zu befördern, obwohl es auf dem kürzesten Weg zwischen den beiden fremden Systemen liegt.
- Anderseits ist es vielleicht bereit, Transitverkehr für seine Nachbarn oder bestimmte andere autonome Systeme zu übernehmen, falls sie für diesen Dienst bezahlen.
- Telekommunikationsgesellschaften stellen ihre Übertragungsdienste gerne zur Verfügung, nicht aber fremden Parteien.

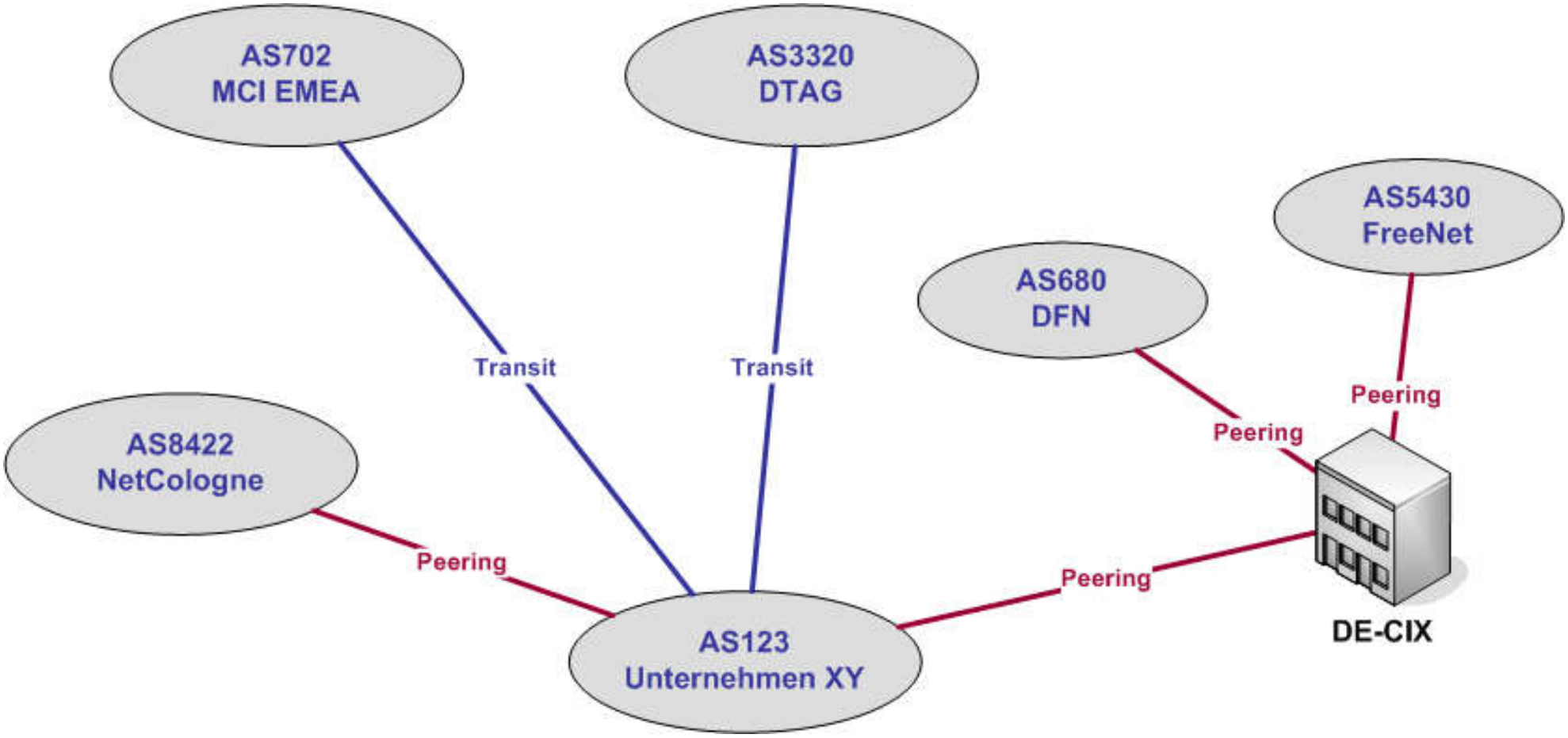
BGP (Border Gateway Protocol)
→ Überblick, Aufgaben

- Die Aufgabe von BGP ist, die Organisation und Durchführung der Wegewahl zwischen autonomen Systemen (AS) unter Berücksichtigung besonderer politischer, wirtschaftlicher oder sicherheitsbezogener Regeln.
- Beispiele für besondere Regel:
  - Datenverkehr soll nie durch bestimmte autonome System fließen.
  - Vom Pentagon ausgehender Datenverkehr darf nie über Irak übertragen werden.
  - Albanien darf nur durchquert werden, wenn es keine Alternative zum Ziel gibt.
  - Datenverkehr, der bei IBM beginnt und endet, darf nicht über Microsoft führen.
  - usw.
- Regeln und Maßnahmen werden normalerweise manuell in jedem BGP-Router konfiguriert (oder mit Hilfe eines Scripts aufgenommen).
- Sie sind nicht Teil des Protokolls.

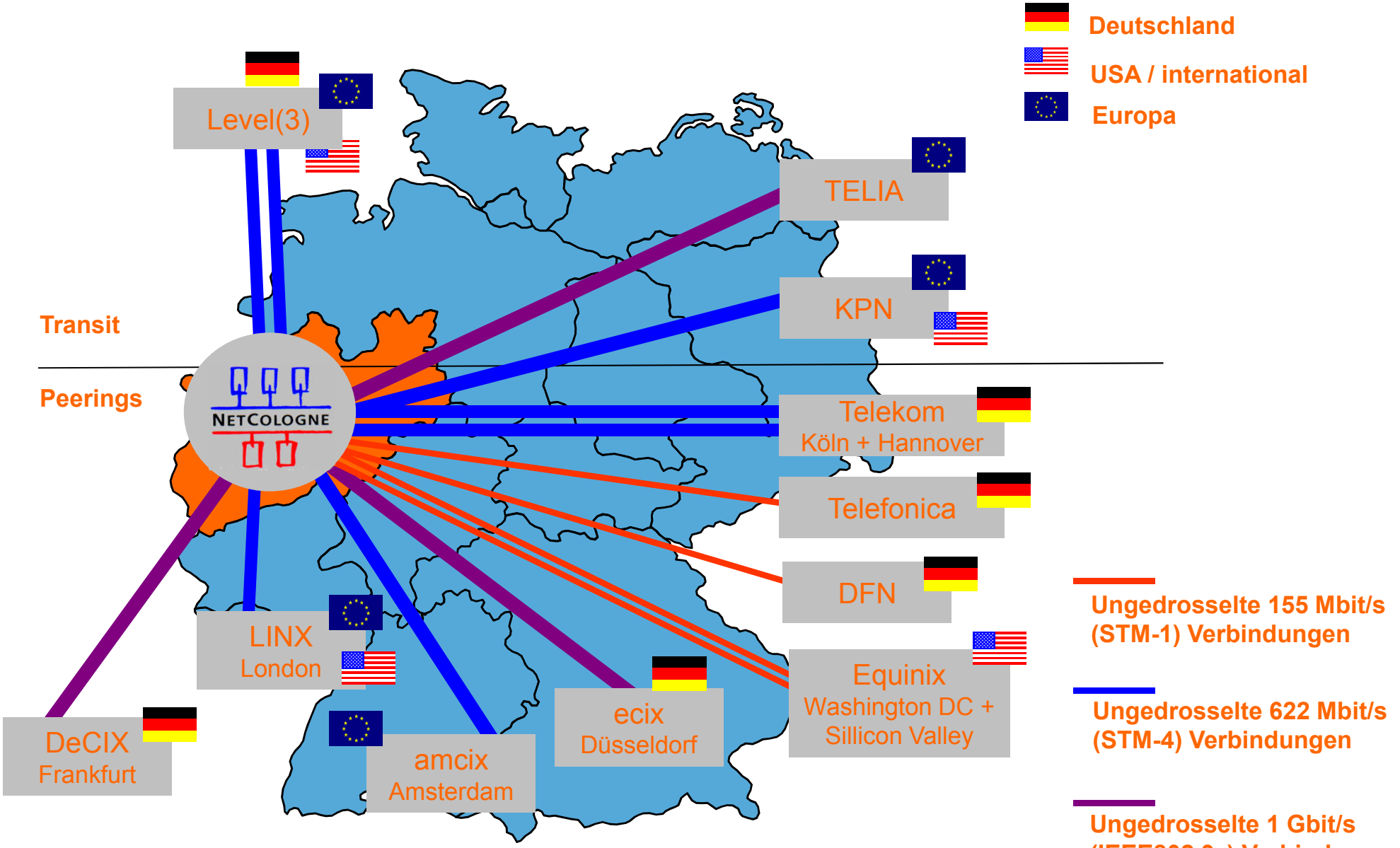
Autonome Systeme
→ Übersicht



Autonome Systeme
→ Strategien und Notwendigkeiten der Provider



NetColone
→ Beispiel: Internet Anbindung



Grundlagen
→ Border Gateway Protocol (BGP) (1/3)

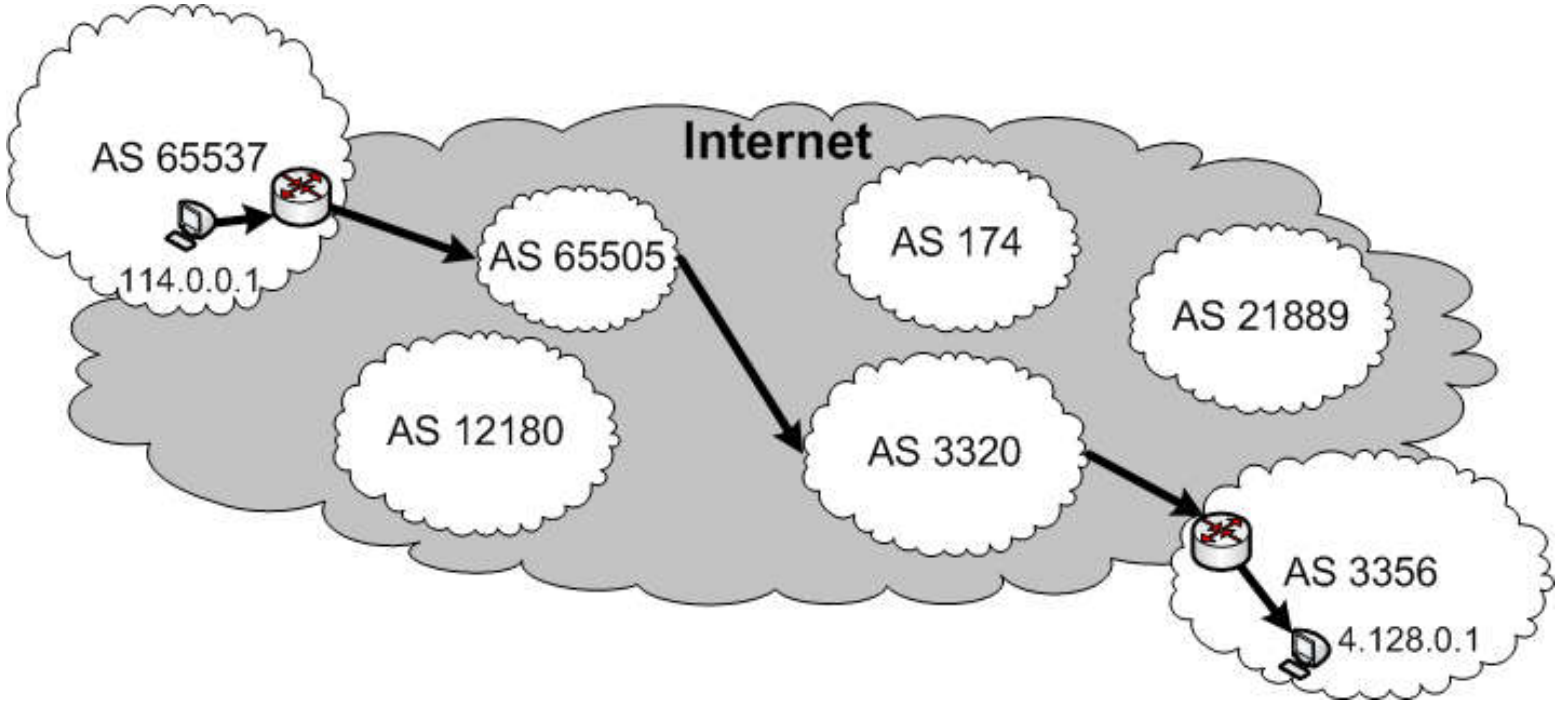
- Routing der obersten Ebene des Internets durch BGP

- BGP ist ein **Pfad Vektor Protokoll**
  - Alle **Wege** zu allen Routern werden per **Flooding** verbreitet
  - Alle Router die diese Wege empfangen haben, **errechnen** mit diesen Informationen die **besten Wege** zu allen anderen Routern im Netz. Dann verbreiten Sie ihre besten Wege per Flooding weiter.
  - Jeder Router hängt sich dabei an den Weg dran
  - Der Name des Weges wird im BGP **AS-Path** genannt

- Wofür wird immer der ganze Weg (AS-Path) mitgeschickt ?
  - Um das **Count-To-Infinity** Problem zu vermeiden
  - Um **Schleifen** im Netz zu **vermeiden**

Grundlagen
→ Border Gateway Protocol (BGP) (2/3)

- Beispiel eines AS-Path



Das IP-Paket muss die AS **65505 3320 3356** (AS-Path) durchlaufen um ans Ziel zu kommen

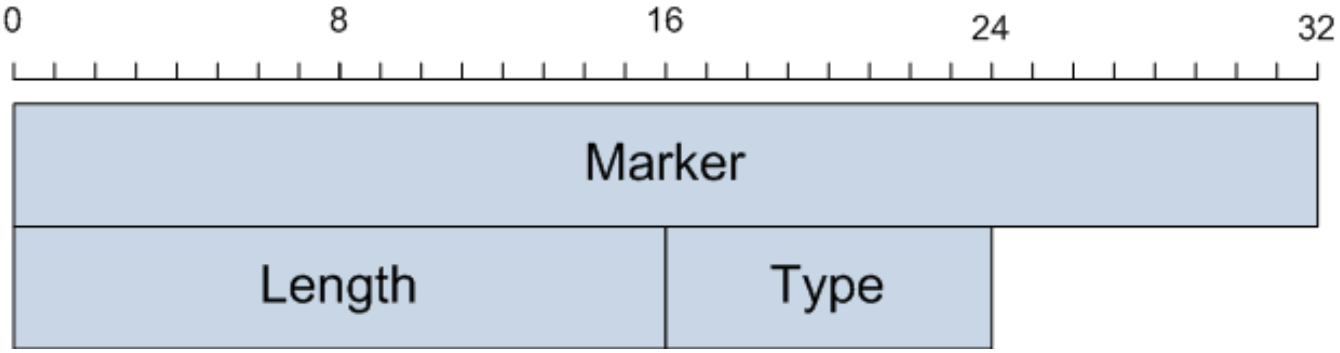
Grundlagen
→ Border Gateway Protocol (BGP) (3/3)

- **Router** die per **BGP** kommunizieren werden **BGP-Speaker** genannt
- BGP-Speaker **kommunizieren über** den **TCP Port 179**
- Jeder **BGP-Speaker** hält **zu jedem** seiner **Nachbarn** eine **TCP-Session** aufrecht
- **Standardmäßig** findet **keine Verschlüsselung** des TCP Datenstroms statt (kann jedoch aktiviert werden)

BGP Nachrichten

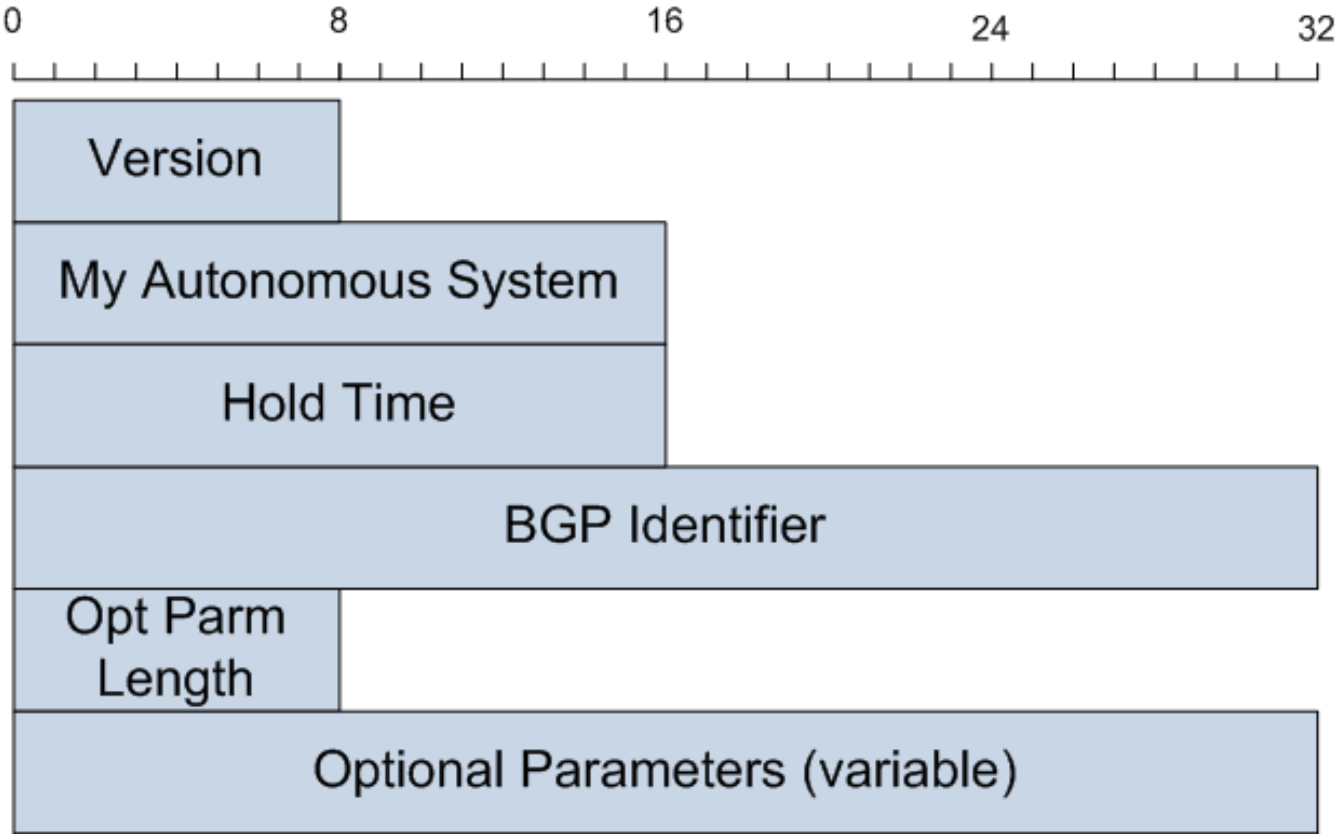
- BGP-Speaker kommunizieren über 4 Nachrichten miteinander
  - OPEN
    - **Öffnet** eine **BGP-Session** mit einem anderen BGP-Speaker
  - UPDATE
    - Dient zum **Verteilen neuer Routen** und gleichzeitig zum **Löschen** von nicht mehr routbaren **Routen**
  - NOTIFICATION
    - **Beendet eine Session** und gibt Fehler- bzw. Statuscodes an. Alle Routen, die über diese beendete Verbindung empfangen wurden, müssen nun gelöscht werden
  - KEEP ALIVE
    - Zur regelmäßigen **Überprüfung, ob der Verbundene Router noch online ist**, oder ob die Session unterbrochen ist und die **Routen** über den verbundenen Router somit **ungültig geworden** sind

BGP Protokoll
→ Header



- Marker (32 bit)
  - 4 Oktetten auf 1 gesetzt aus kompatibilitäts Gründen
- Length (16 bit)
  - Länge der gesamten BGP-Nachricht inklusive Header
- Type (8 bit)
  - Typ der Nachricht
    1 - OPEN
    3 - NOTIFICATION
    2 - UPDATE
    4 - KEEPALIVE

BGP Protokoll
→ OPEN – Nachricht (1/2)

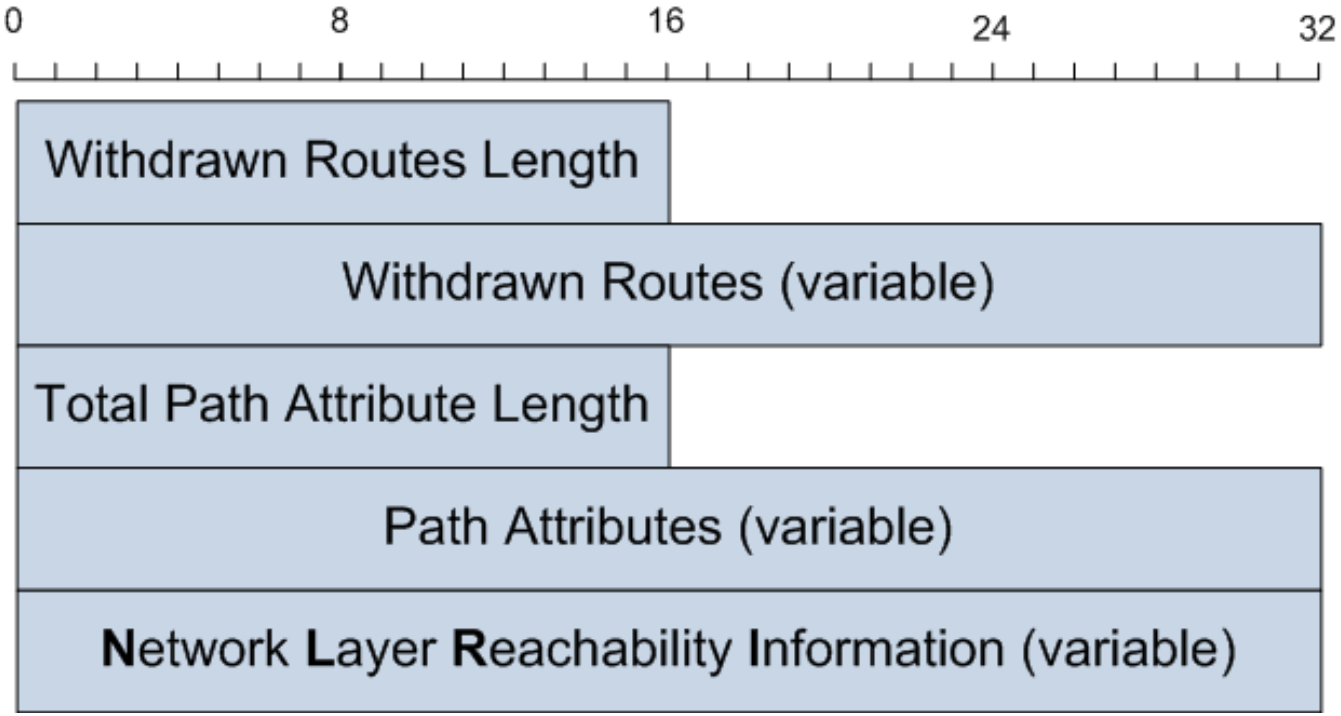


- Version (8 bit)
  - Version des BGP Protokolls (aktuell 4 – für Version 4)

BGP Protokoll
→ OPEN – Nachricht (2/2)

- My Autonomous System (16 bit)
  - AS - Nummer des Senders der OPEN Nachricht
- Hold Time (16 bit)
  - Maximale Anzahl in Sekunden die zwischen KEEPALIVE bzw. UPDATE Nachrichten verstreichen dürfen
- BGP Identifier (32 bit)
  - IP-Adresse die den Sender der OPEN Messsage identifiziert (muss nicht die IP-Adresse sein, von der das OPEN kam)
- Optional Parameters Length (8 bit)
  - Länge der Optionalen Parameter
- Optional Parameters (variable Länge)
  - Optionale Parameter (bsp. Fähigkeiten des BGP Routers)

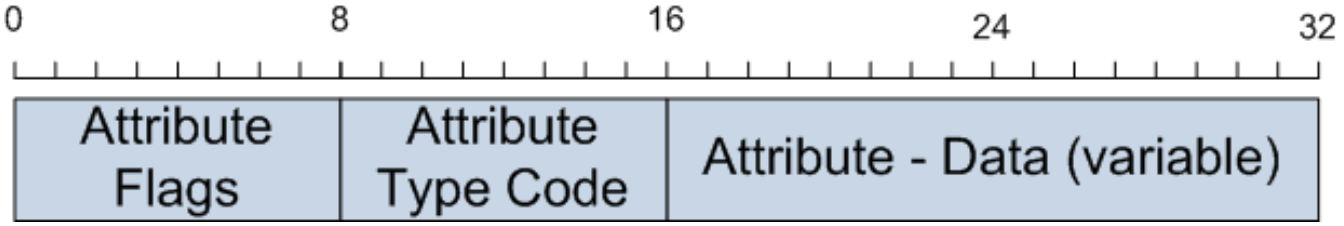
BGP Protokoll
→ UPDATE – Nachricht (1/3)



- Withdrawn Routes Length (16 bit)
  - Länge/Anzahl der Routen die über den Sender des Updates nicht länger erreichbar sind

BGP Protokoll
→ UPDATE – Nachricht (2/3)

- Withdrawn Routes (variable Länge)
  - Routen die über den Sender des Updates nicht mehr erreicht werden können.
  - Tupel des Typs (Length, Prefix) – Bsp. (24, 10.0.1) für 10.0.1.0/24
- Total Path Attributes Length (16 bit)
  - Gesamtanzahl der folgenden Pfad Attribute
- Path Attributes

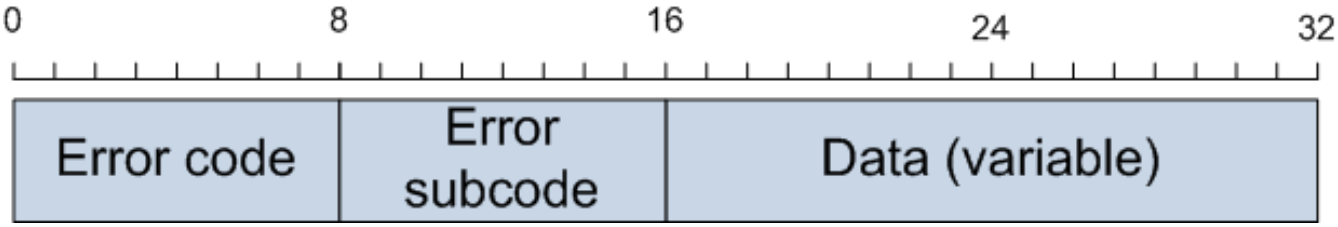


  - Attribute Flags (8 bit)
    - Geben an, ob Attribut optional ist und ob die Länge des Attributs 8 oder 16 bit ist

BGP Protokoll
→ UPDATE – Nachricht (3/3)

- Path Attributes (Fortsetzung)
  - Attribute Type Code
    - Stellt den Typ des Attributs dar. Wichtige Typen sind:
    - 1 - Origin (Herkunft der Route)
    - 2 - AS-Path (Pfad der AS bis zum Quell-AS)
    - 3 - Next Hop (Die IP-Adresse des letzten AS im AS-Path)
    - …
  - Attribute Data
    - Der eigentliche Inhalt des Attributs
- Network Layer Reachability Information (NLRI) (variabel)
  - Neue Routen die mit diesem Update verbreitet wurden
  - Tupel des Typs (Length, Prefix) – Bsp. (24, 10.0.1) für 10.0.1.0/24

BGP Protokoll
→ NOTIFICATION – Nachricht

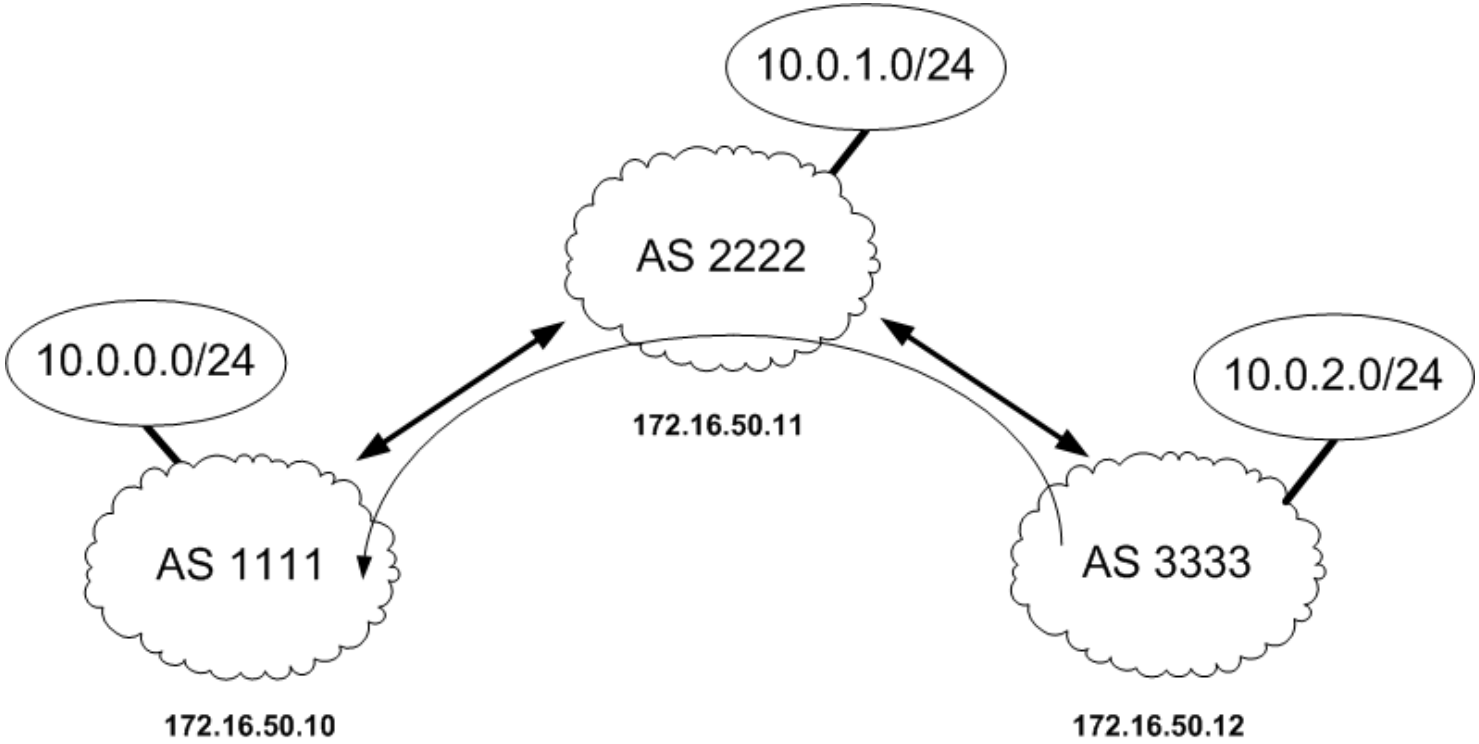


- Error Code (8 bit)
  - 1 = Message Header Error
    2 = OPEN Message Error
    3 = UPDATE Message Error
    4 = Hold Timer Expired
    5 = Finite State Machine Error
    6 = Cease
- Error Subcode (8 bit)
  - Subcodes für die Errorcodes 1-3
  - Beispiel bei Errorcode 2 - Subcode 1 Unsupported Version Number
- Data (variabel)
  - Hängt von Error Code und Subcode ab und gibt weitere Informationen zu der Ursache des Fehlers

BGP Protokoll
→ KEEPALIVE – Nachricht

- Bei der KEEPALIVE Nachricht wird **lediglich der Header** mit dem **Type = 4** (KEEPALIVE) gesendet
- **KEEPALIVE** Nachrichten sind durchaus **sicherheitsrelevant**, da durch **verzögern** von KEEPALIVE Nachrichten (durch Beispielsweise einen DOS - Angriff) die **Erreichbarkeit** von bestimmten Routen **gefährdet** ist.

Simulation eines Mini-Internets

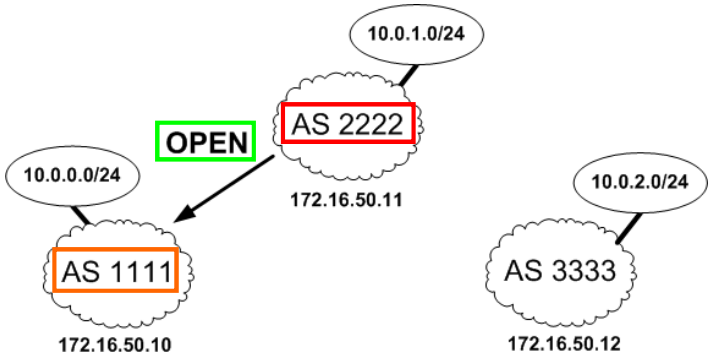


- Jedes AS routet einen bestimmten Netzbereich (AS 1111 routet beispielsweise den Netzbereich 10.0.0.0/24)
- AS 2222 erhält alle Routing Infos, AS 3333 nur die von AS 2222
- AS 1111 erhält Routing Infos von AS 2222 und AS 3333

Prokokollmitschnitt BGP
→ OPEN Message (1/2)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
⊞ Frame 4 (115 bytes on wire, 115 bytes captured)
⊞ Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_05:5d:e5 (00:0c:29:05:5d:e5)
⊞ Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.10 (172.16.50.10)
⊞ Transmission Control Protocol, Src Port: 25158 (25158), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 49
⊟ Border Gateway Protocol
  ⊟ OPEN Message
      Marker: 16 bytes
      Length: 49 bytes
      Type: OPEN Message (1)
      Version: 4
      My AS: 2222
      Hold time: 90
      BGP identifier: 192.168.1.4
      Optional parameters length: 20 bytes
    ⊟ Optional parameters
      ⊟ Capabilities Advertisement (8 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 6 bytes
        ⊞ Multiprotocol extensions capability (6 bytes)
      ⊟ Capabilities Advertisement (4 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 2 bytes
        ⊞ Route refresh capability (2 bytes)
      ⊟ Capabilities Advertisement (8 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 6 bytes
        ⊞ Graceful Restart capability (6 bytes)
```



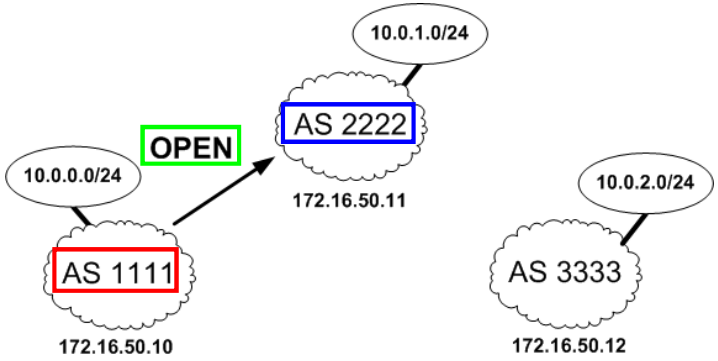
Router AS 1111 und AS 2222 werden **eingeschaltet**

AS 2222 **sendet** eine **OPEN Nachricht** an AS 1111

Prokokollmitschnitt BGP
→ OPEN Message (2/2)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
⊞ Frame 5 (115 bytes on wire, 115 bytes captured)
⊞ Ethernet II, Src: Vmware_05:5d:e5 (00:0c:29:05:5d:e5), Dst: Vmware_26:28:8a (00:0c:29:26:28:8a)
⊞ Internet Protocol, Src: 172.16.50.10 (172.16.50.10), Dst: 172.16.50.11 (172.16.50.11)
⊞ Transmission Control Protocol, Src Port: bgp (179), Dst Port: 25158 (25158), Seq: 1, Ack: 50, Len: 49
⊟ Border Gateway Protocol
  ⊟ OPEN Message
      Marker: 16 bytes
      Length: 49 bytes
      Type: OPEN Message (1)
      Version: 4
      My AS: 1111
      Hold time: 90
      BGP identifier: 192.168.1.13
      Optional parameters length: 20 bytes
    ⊟ Optional parameters
      ⊟ Capabilities Advertisement (8 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 6 bytes
        ⊞ Multiprotocol extensions capability (6 bytes)
      ⊟ Capabilities Advertisement (4 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 2 bytes
        ⊞ Route refresh capability (2 bytes)
      ⊟ Capabilities Advertisement (8 bytes)
          Parameter type: Capabilities (2)
          Parameter length: 6 bytes
        ⊞ Graceful Restart capability (6 bytes)
```

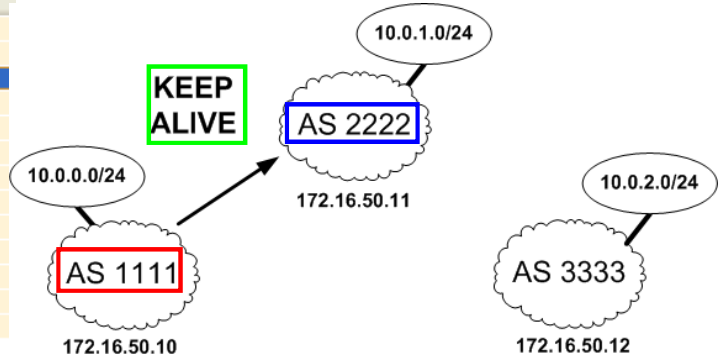


AS 1111 **sendet** eine **OPEN Nachricht** an AS 2222

Prokokollmitschnitt BGP
→ KEEPALIVE Message (1/2)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
⊞ Frame 6 (85 bytes on wire, 85 bytes captured)
⊞ Ethernet II, Src: Vmware_05:5d:e5 (00:0c:29:05:5d:e5), Dst: Vmware_26:28:8a (00:0c:29:26:28:8a)
⊞ Internet Protocol, Src: 172.16.50.10 (172.16.50.10), Dst: 172.16.50.11 (172.16.50.11)
⊞ Transmission Control Protocol, Src Port: bgp (179), Dst Port: 25158 (25158), Seq: 50, Ack: 50, Len: 19
⊟ Border Gateway Protocol
  ⊟ KEEPALIVE Message
      Marker: 16 bytes
      Length: 19 bytes
      Type: KEEPALIVE Message (4)
```

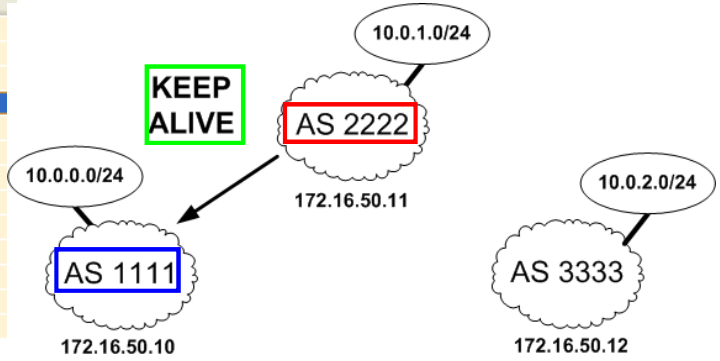


AS 1111 **quittiert** die **OPEN Nachricht** von AS 2222 mit einer **KEEPALIVE Nachricht**

Prokokollmitschnitt BGP
→ KEEPALIVE Message (2/2)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

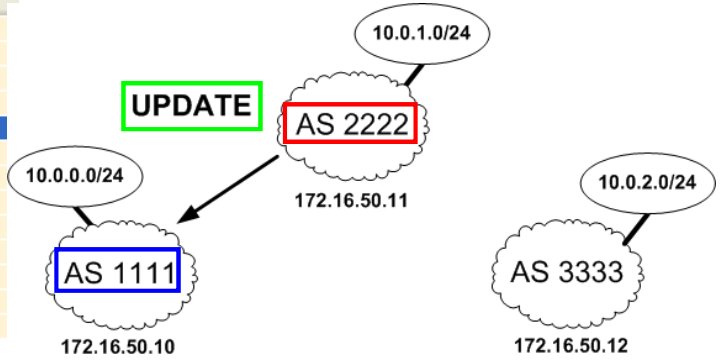
```
⊞ Frame 8 (85 bytes on wire, 85 bytes captured)
⊞ Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_05:5d:e5 (00:0c:29:05:5d:e5)
⊞ Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.10 (172.16.50.10)
⊞ Transmission Control Protocol, Src Port: 25158 (25158), Dst Port: bgp (179), Seq: 50, Ack: 69, Len: 19
⊟ Border Gateway Protocol
  ⊟ KEEPALIVE Message
      Marker: 16 bytes
      Length: 19 bytes
      Type: KEEPALIVE Message (4)
```



AS 2222 **quittiert** die **OPEN Nachricht** von AS 1111 mit einer **KEEPALIVE Nachricht**

Prokokollmitschnitt BGP
→ UPDATE Message (1/5)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

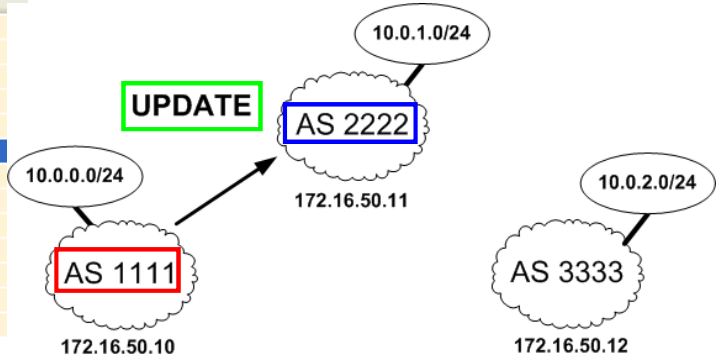



```
Frame 9 (111 bytes on wire, 111 bytes captured)
Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_05:5d:e5 (00:0c:29:05:5d:e5)
Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.10 (172.16.50.10)
Transmission Control Protocol, Src Port: 25158 (25158), Dst Port: bgp (179), Seq: 69, Ack: 69, Len: 45
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 45 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 18 bytes
  Path attributes
    ORIGIN: IGP (4 bytes)
    AS_PATH: 2222 (7 bytes)
    NEXT_HOP: 172.16.50.11 (7 bytes)
  Network layer reachability information: 4 bytes
    10.0.1.0/24
      NLRI prefix length: 24
      NLRI prefix: 10.0.1.0 (10.0.1.0)
```

AS 2222 teilt AS 1111 per **UPDATE Nachricht** seine erreichbaren Netzbereiche mit

Prokokollmitschnitt BGP
→ UPDATE Message (2/5)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message



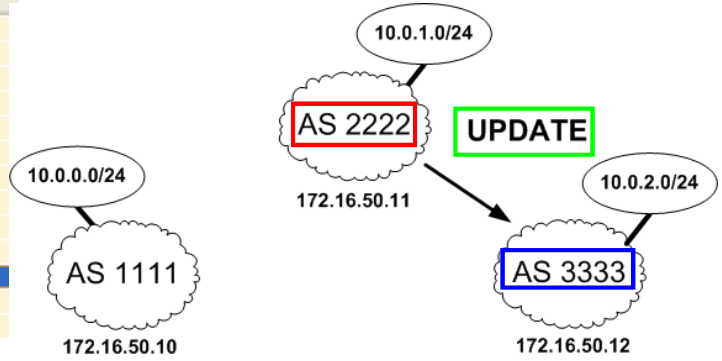

```
Frame 11 (111 bytes on wire, 111 bytes captured)
Ethernet II, Src: Vmware_05:5d:e5 (00:0c:29:05:5d:e5), Dst: Vmware_26:28:8a (00:0c:29:26:28:8a)
Internet Protocol, Src: 172.16.50.10 (172.16.50.10), Dst: 172.16.50.11 (172.16.50.11)
Transmission Control Protocol, Src Port: bgp (179), Dst Port: 25158 (25158), Seq: 69, Ack: 114, Len: 45
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 45 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 18 bytes
    Path attributes
      ORIGIN: IGP (4 bytes)
      AS_PATH: 1111 (7 bytes)
      NEXT_HOP: 172.16.50.10 (7 bytes)
    Network layer reachability information: 4 bytes
      10.0.0.0/24
        NLRI prefix length: 24
        NLRI prefix: 10.0.0.0 (10.0.0.0)
```

AS 1111 teilt AS 2222 per **UPDATE Nachricht** seine erreichbaren Netzbereiche mit

Prokokollmitschnitt BGP
→ UPDATE Message (3/5)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
⊞ Frame 20 (111 bytes on wire, 111 bytes captured)
⊞ Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_bc:b6:db (00:0c:29:bc:b6:db)
⊞ Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.12 (172.16.50.12)
⊞ Transmission Control Protocol, Src Port: bgp (179), Dst Port: 30161 (30161), Seq: 69, Ack: 69, Len: 45
⊟ Border Gateway Protocol
  ⊟ UPDATE Message
      Marker: 16 bytes
      Length: 45 bytes
      Type: UPDATE Message (2)
      Unfeasible routes length: 0 bytes
      Total path attribute length: 18 bytes
    ⊟ Path attributes
      ⊞ ORIGIN: IGP (4 bytes)
      ⊞ AS_PATH: 2222 (7 bytes)
      ⊞ NEXT_HOP: 172.16.50.11 (7 bytes)
    ⊟ Network layer reachability information: 4 bytes
      ⊟ 10.0.1.0/24
          NLRI prefix length: 24
          NLRI prefix: 10.0.1.0 (10.0.1.0)
```

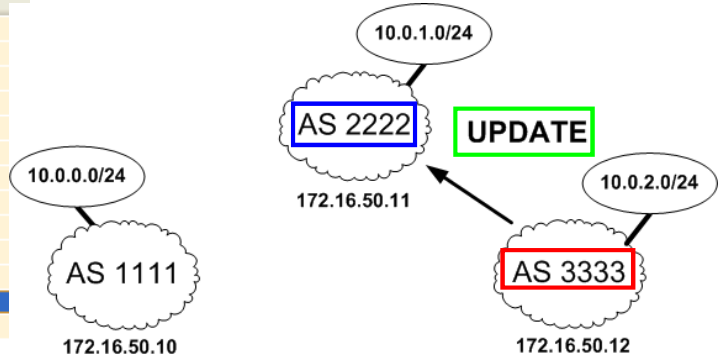


Router von AS 3333 eingeschaltet und bereits Verbindung mit AS 2222 aufgenommen

AS 2222 teilt AS 3333 per **UPDATE Nachricht** seine erreichbaren Netzbereiche mit

Prokokollmitschnitt BGP
→ UPDATE Message (4/5)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message

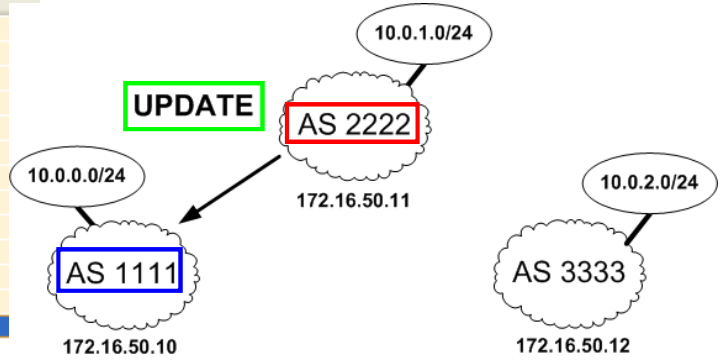



```
Frame 21 (111 bytes on wire, 111 bytes captured)
Ethernet II, Src: Vmware_bc:b6:db (00:0c:29:bc:b6:db), Dst: Vmware_26:28:8a (00:0c:29:26:28:8a)
Internet Protocol, Src: 172.16.50.12 (172.16.50.12), Dst: 172.16.50.11 (172.16.50.11)
Transmission Control Protocol, Src Port: 30161 (30161), Dst Port: bgp (179), Seq: 69, Ack: 114, Len: 45
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 45 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 18 bytes
  Path attributes
    ORIGIN: IGP (4 bytes)
    AS_PATH: 3333 (7 bytes)
    NEXT_HOP: 172.16.50.12 (7 bytes)
  Network layer reachability information: 4 bytes
    10.0.2.0/24
      NLRI prefix length: 24
      NLRI prefix: 10.0.2.0 (10.0.2.0)
```

AS 3333 teilt AS 2222 per **UPDATE Nachricht** seine erreichbaren Netzbereiche mit

Prokokollmitschnitt BGP
→ UPDATE Message (5/5)

No.	Time	Source	Destination	Protocol	Info
4	0.000741	172.16.50.11	172.16.50.10	BGP	OPEN Message
5	0.001051	172.16.50.10	172.16.50.11	BGP	OPEN Message
6	0.001273	172.16.50.10	172.16.50.11	BGP	KEEPALIVE Message
8	0.001406	172.16.50.11	172.16.50.10	BGP	KEEPALIVE Message
9	0.002338	172.16.50.11	172.16.50.10	BGP	UPDATE Message
11	0.002484	172.16.50.10	172.16.50.11	BGP	UPDATE Message
16	3.375834	172.16.50.11	172.16.50.12	BGP	OPEN Message
17	3.385134	172.16.50.12	172.16.50.11	BGP	OPEN Message
18	3.385757	172.16.50.11	172.16.50.12	BGP	KEEPALIVE Message
19	3.393030	172.16.50.12	172.16.50.11	BGP	KEEPALIVE Message
20	3.393822	172.16.50.11	172.16.50.12	BGP	UPDATE Message
21	3.402374	172.16.50.12	172.16.50.11	BGP	UPDATE Message
22	3.403805	172.16.50.11	172.16.50.10	BGP	UPDATE Message




```
Frame 22 (113 bytes on wire, 113 bytes captured)
Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_05:5d:e5 (00:0c:29:05:5d:e5)
Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.10 (172.16.50.10)
Transmission Control Protocol, Src Port: 25158 (25158), Dst Port: bgp (179), Seq: 114, Ack: 114, Len: 47
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 47 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 20 bytes
  Path attributes
    ORIGIN: IGP (4 bytes)
    AS_PATH: 2222 3333 (9 bytes)
    NEXT_HOP: 172.16.50.11 (7 bytes)
  Network layer reachability information: 4 bytes
    10.0.2.0/24
      NLRI prefix length: 24
      NLRI prefix: 10.0.2.0 (10.0.2.0)
```

AS Path hat 2 Elemente

AS 2222 teilt AS 1111 per **UPDATE Nachricht** seine von AS 3333 erhaltenen Netzbereiche mit

Prokokollmitschnitt BGP
→ Routing Information Base der AS

- RIB - AS 1111

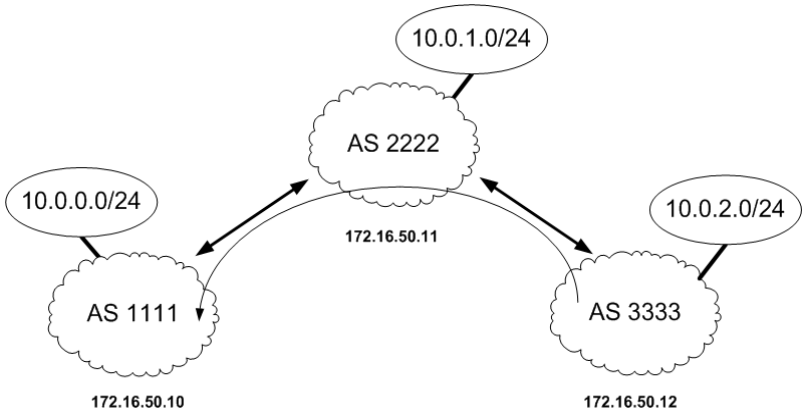
```
flags: * = Valid, > = Selected, I = via IBGP, A = Announced
origin: i = IGP, e = EGP, ? = Incomplete

flags destination          gateway           lpref   med aspath origin
AI*>  10.0.0.0/24          0.0.0.0             100     0 i
*>    10.0.1.0/24          172.16.50.11        100     0 2222 i
*>    10.0.2.0/24          172.16.50.11        100     0 2222 3333 i
```

- RIB - AS 2222

```
flags: * = Valid, > = Selected, I = via IBGP, A = Announced
origin: i = IGP, e = EGP, ? = Incomplete

flags destination          gateway           lpref   med aspath origin
*>    10.0.0.0/24          172.16.50.10        100     0 1111 i
AI*>  10.0.1.0/24          0.0.0.0             100     0 i
*>    10.0.2.0/24          172.16.50.12        100     0 3333 i
```



- RIB – AS 3333

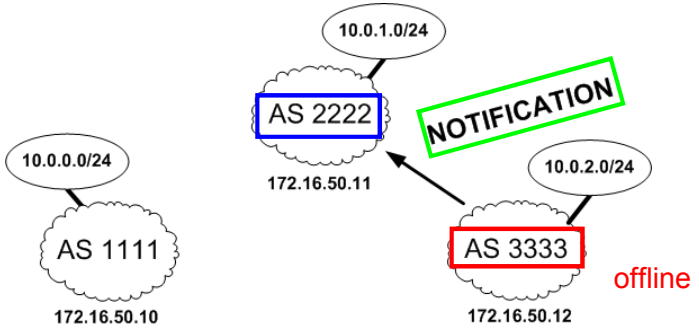
```
flags: * = Valid, > = Selected, I = via IBGP, A = Announced
origin: i = IGP, e = EGP, ? = Incomplete

flags destination          gateway           lpref   med aspath origin
*>    10.0.1.0/24          172.16.50.11        100     0 2222 i
AI*>  10.0.2.0/24          0.0.0.0             100     0 i
```

Prokokollmitschnitt BGP
→ Notification Message

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.50.12	172.16.50.11	BGP	NOTIFICATION Message
6	2.153491	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
⊞ Frame 1 (87 bytes on wire, 87 bytes captured)
⊞ Ethernet II, Src: Vmware_bc:b6:db (00:0c:29:bc:b6:db), Dst: Vmware_26:28:8a (00:0c:29:26:28:8a)
⊞ Internet Protocol, Src: 172.16.50.12 (172.16.50.12), Dst: 172.16.50.11 (172.16.50.11)
⊞ Transmission Control Protocol, Src Port: 30161 (30161), Dst Port: bgp (179), Seq: 0, Ack: 0, Len: 21
⊟ Border Gateway Protocol
  ⊟ NOTIFICATION Message
      Marker: 16 bytes
      Length: 21 bytes
      Type: NOTIFICATION Message (3)
      Error code: Cease (6)
      Error subcode: Unknown (0)
```

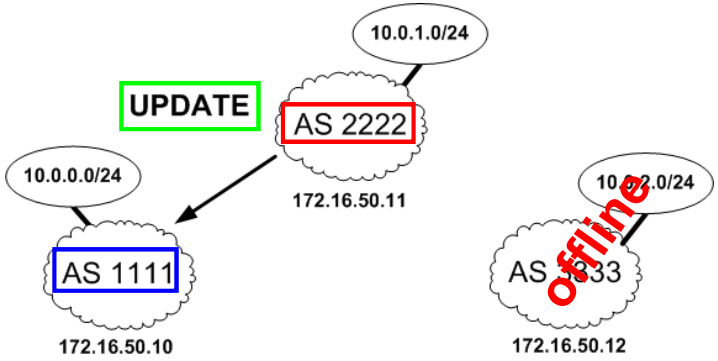


AS 3333
teilt AS 2222 per
NOTIFICATION
Nachricht mit, das der
Router offline geht

Prokokollmitschnitt BGP
→ UPDATE Message nach NOTIFICATION

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.50.12	172.16.50.11	BGP	NOTIFICATION Message
6	2.153491	172.16.50.11	172.16.50.10	BGP	UPDATE Message

```
Frame 6 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: Vmware_26:28:8a (00:0c:29:26:28:8a), Dst: Vmware_05:5d:e5 (00:0c:29:05:5d:e5)
Internet Protocol, Src: 172.16.50.11 (172.16.50.11), Dst: 172.16.50.10 (172.16.50.10)
Transmission Control Protocol, Src Port: 25158 (25158), Dst Port: bgp (179), Seq: 0, Ack: 0, Len: 27
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 27 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 4 bytes
    Withdrawn routes:
      10.0.2.0/24
        Withdrawn route prefix length: 24
        Withdrawn prefix: 10.0.2.0 (10.0.2.0)
    Total path attribute length: 0 bytes
```



AS 2222
teilt AS 1111 per
UPDATE Nachricht mit,
das über
AS 2222 der Netzbereich
10.0.2.0/24 nicht länger
erreichbar ist

Analyse der BGP-Routing-Tabelle

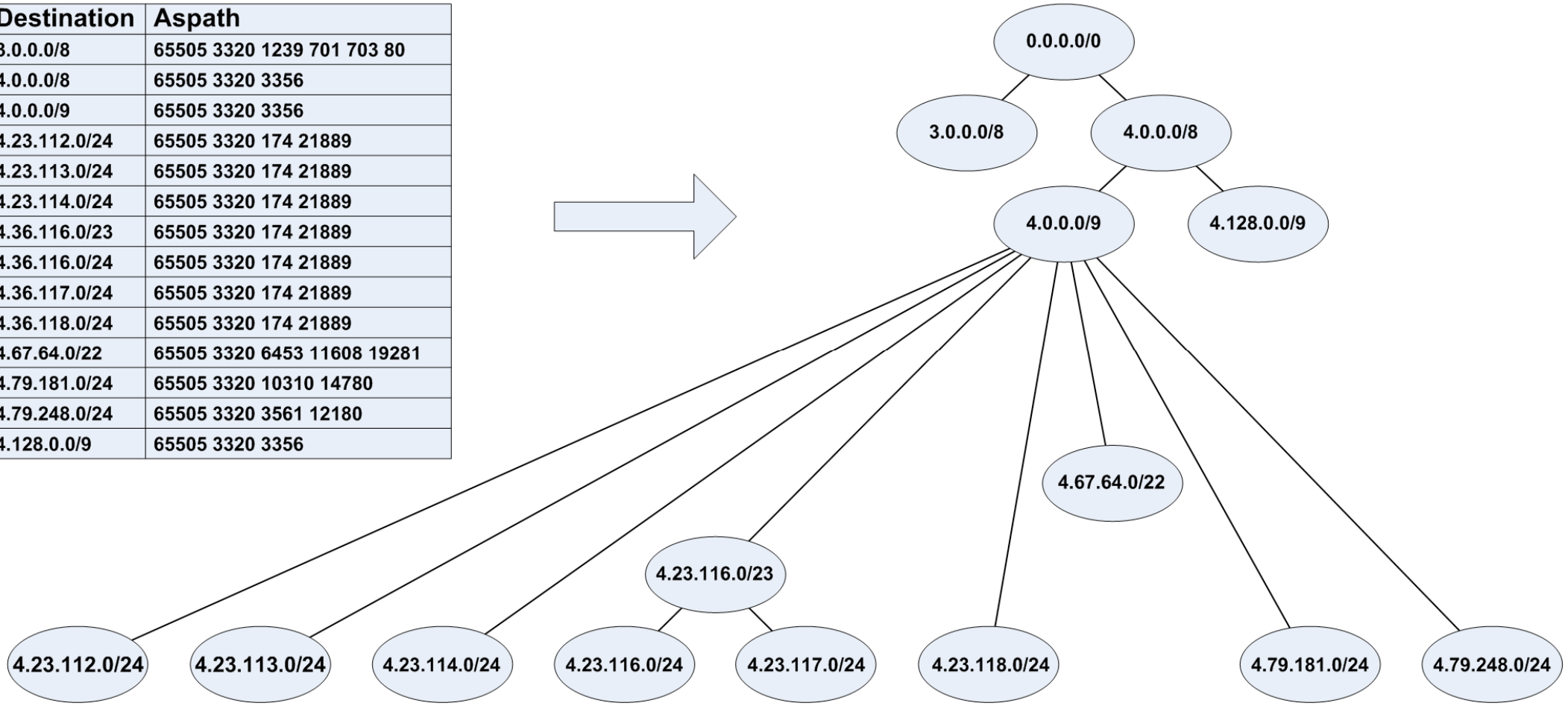
- Die ersten Zeilen einer aktuellen BGP-Routing-Tabelle
- Die Routing-Tabelle eines großen dt. Providers hat ~500.000 Einträge

Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356

Analyse der BGP-Routing-Tabelle

- Ansicht der BGP-Routing-Tabelle als Baum

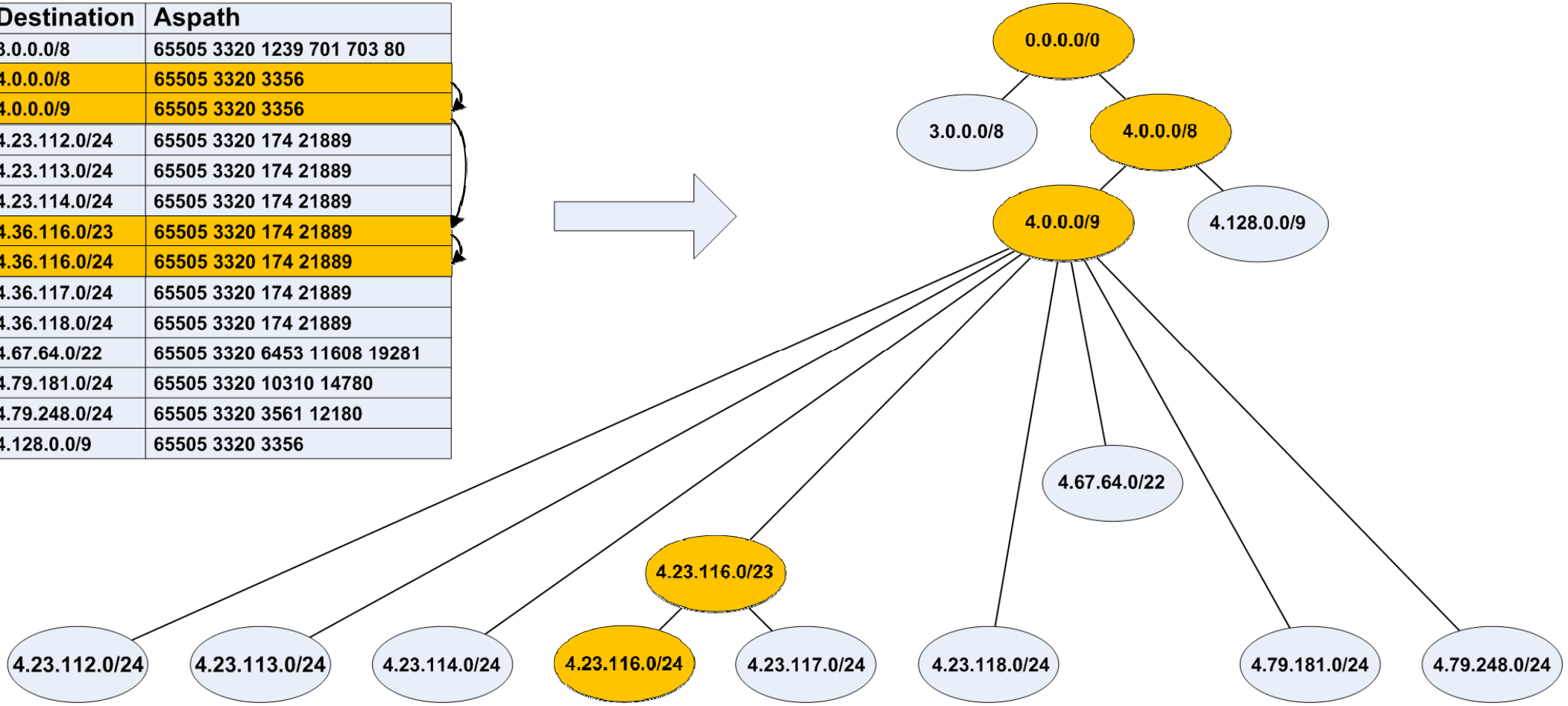
Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356



Analyse der BGP-Routing-Tabelle

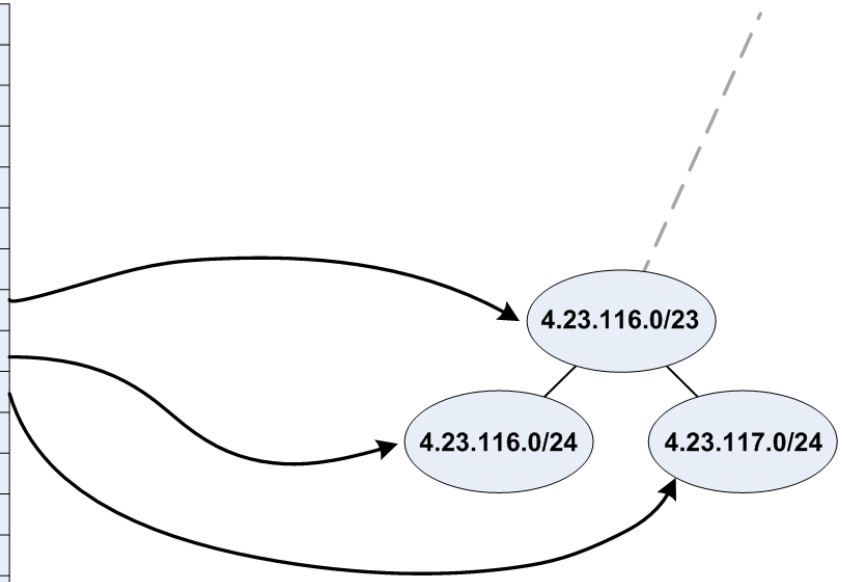
- Senden eines IP-Pakets an die IP-Adresse 4.23.116.5

Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356



Analyse der BGP-Routing-Tabelle → Redundanzen

Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356

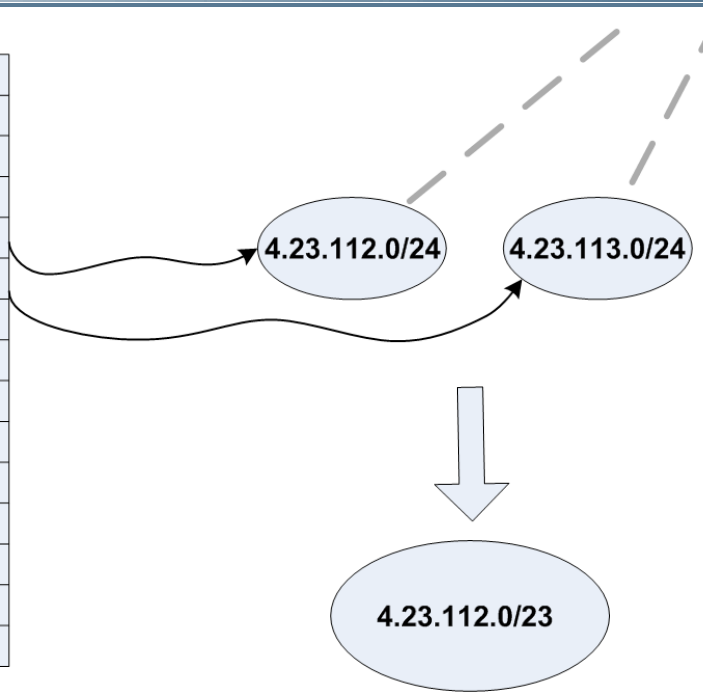


- 4.23.116.0/24 und 4.23.117.0/24 sind überflüssig, da schon 4.23.116.0/23 den gleichen Pfad liefert

- **Entfernen aller Redundanzen** aus einer aktuellen Routing-Tabelle mit 214.866 Einträgen resultierte in einer neuen Tabelle mit 176.080 Einträgen. Die **Tabelle wurde** somit **um 38.786 Einträge** (18,05%) **verkleinert**.

Analyse der BGP-Routing-Tabelle
→ Aggregation

Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356

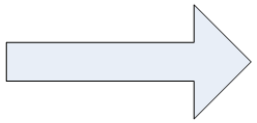


- Die Adressbereiche 4.23.112.0/24 und 4.23.113.0/24 können zu einem großen Bereich 4.23.112.0/23 aggregiert werden
- **Aggregation** der redundanzfreien Routing-Tabelle mit **176.080 Einträgen** resultierte in einer neuen Tabelle mit 138.342 Einträgen. Die **Tabelle** wurde somit **um weitere 37.738 Einträge verkleinert**. Insgesamt wurde die Tabelle um 35,6% verkleinert.

Analyse der BGP-Routing-Tabelle
→ Radundanzen und Aggregation

- Entfernen der Redundazen und Aggregation der Beispieltabelle

Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/8	65505 3320 3356
4.0.0.0/9	65505 3320 3356
4.23.112.0/24	65505 3320 174 21889
4.23.113.0/24	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.116.0/24	65505 3320 174 21889
4.36.117.0/24	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180
4.128.0.0/9	65505 3320 3356



Destination	Aspath
3.0.0.0/8	65505 3320 1239 701 703 80
4.0.0.0/7	65505 3320 3356
4.23.112.0/23	65505 3320 174 21889
4.23.114.0/24	65505 3320 174 21889
4.36.116.0/23	65505 3320 174 21889
4.36.118.0/24	65505 3320 174 21889
4.67.64.0/22	65505 3320 6453 11608 19281
4.79.181.0/24	65505 3320 10310 14780
4.79.248.0/24	65505 3320 3561 12180

Fazit

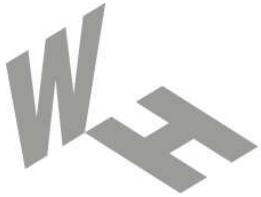
- Die Routing-Tabelle im Internet hat viele Redundanzen
  - Redundanzen können jedoch 'On The Fly' eliminiert werden
    - Ohne das Routing-Ergebnis zu verändern können Redundanzen aus der eigenen Routing-Tabelle gelöscht werden
    - Jedes AS muss dies tun, damit alle Redundanzen verschwinden
  - Auch Aggregation kann 'On the fly' durchgeführt werden
    - Erst muss ein neuer großer Bereich announced werden
    - Dann können die älteren kleinen Bereiche gelöscht werden
- Wenn sich jedes AS am Riemen reisst, kann die Routing-Tabelle durchaus verkleinert werden. (evtl. SLAs?)

Inhalt

- Ziele, Einordnung und Übersicht
- Router
- Routing-Verfahren
- Routing-Protokolle
- **Zusammenfassung**

Routing-Protokolle
→ Zusammenfassung

- Routing ist ein Teil des Konfigurationsmanagements im Bereich des Netzwerkmanagements.
- Statisches Routing ist ein mächtiges Werkzeug, um das Routing-Verhalten in einem Netzwerk präzise zu kontrollieren.
- Wenn jedoch regelmäßige Änderungen in der Topologie auftreten, kann der hierfür erforderliche Aufwand der manuellen Neukonfiguration ein statisches Routing undurchführbar machen.
- Das Border Gateway Protocol (BGP) ist das wichtigste Routing-Protokoll zur Kommunikation zwischen Routern von autonomen Systemen.
- Das Open Shortest Path First Protocol (OSPF) ist das wichtigste Routing-Protokoll zur Kommunikation innerhalb eines autonomen Systems und arbeitet mit dem Link State Routing.



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Routing-Protokolle

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de