

6.3 Routing, Gateway und Routing-Tabelle

Routing gehört zu OSI-Schicht 3.

Routing bedeutet:

IP-Pakete zwischen verschiedenen Netzwerken weiterleiten.

Ein Router entscheidet anhand der Ziel-IP-Adresse, wohin ein IP-Paket als Nächstes gesendet wird.

Dafür verwendet er eine Routing-Tabelle.

Merksatz:

Routing = Wegentscheidung für IP-Pakete.

Warum braucht man Routing?

Geräte im gleichen IP-Subnetz können direkt miteinander kommunizieren.

Geräte in unterschiedlichen IP-Subnetzen brauchen einen Router.

Beispiel:

PC A:

192.168.10.20/24

Server B:

192.168.30.50/24

Diese Geräte liegen in unterschiedlichen Netzen:

192.168.10.0/24

192.168.30.0/24

Damit die Kommunikation funktioniert, braucht man Routing.

Merksatz:

Unterschiedliche IP-Netze brauchen Routing.

Gleiches Subnetz oder anderes Subnetz?

Ein Gerät entscheidet zuerst:

Liegt das Ziel im eigenen Subnetz?

Oder liegt das Ziel in einem anderen Subnetz?

Beispiel 1:

PC:

192.168.10.20/24

Ziel:

192.168.10.50

Das Ziel liegt im gleichen Subnetz.

Direkte lokale Zustellung möglich.

Beispiel 2:

PC:

192.168.10.20/24

Ziel:

192.168.20.50

Das Ziel liegt in einem anderen Subnetz.

Standard-Gateway nötig.

Merksatz:

Gleiches Subnetz = direkt.
Anderes Subnetz = Gateway.

Standard-Gateway

Das Standard-Gateway ist der Router, den ein Gerät für Ziele außerhalb des eigenen Subnetzes verwendet.

Beispiel:

PC:
192.168.10.20/24

Standard-Gateway:
192.168.10.1

Wenn der PC ein Ziel außerhalb von 192.168.10.0/24 erreichen möchte, sendet er das Paket an das Gateway.

Merksatz:

Standard-Gateway = Ausgang in andere Netze.

Gateway muss im eigenen Subnetz liegen

Das Standard-Gateway muss für den Client lokal erreichbar sein.

Beispiel korrekt:

PC:
192.168.10.20/24

Gateway:
192.168.10.1

Beide liegen im Netz:

192.168.10.0/24

Beispiel falsch:

```
PC:
192.168.10.20/24

Gateway:
192.168.20.1
```

Das Gateway liegt nicht im eigenen Subnetz und ist für den PC nicht direkt erreichbar.

Merksatz:

Das Gateway muss im eigenen lokalen Subnetz erreichbar sein.

Router

Ein Router verbindet verschiedene IP-Netze miteinander.

Er besitzt meistens mehrere Schnittstellen.

Jede Schnittstelle gehört zu einem bestimmten Netz.

Beispiel:

Router-Schnittstelle	IP-Adresse	Netz
LAN 1	192.168.10.1/24	192.168.10.0/24
LAN 2	192.168.20.1/24	192.168.20.0/24
WAN	öffentliche IP	Internet

Der Router kann Pakete zwischen diesen Netzen weiterleiten.

Merksatz:

Router haben Schnittstellen in verschiedenen IP-Netzen.

Router und Switch unterscheiden

Gerät	typische Schicht	Aufgabe
Switch	2	leitet Frames anhand von MAC-Adressen weiter

Gerät	typische Schicht	Aufgabe
Router	3	leitet IP-Pakete zwischen Netzen weiter

Ein Switch entscheidet anhand von:

MAC-Adressen

Ein Router entscheidet anhand von:

IP-Adressen

Merksatz:

Switch = MAC.

Router = IP.

Routing-Tabelle

Eine Routing-Tabelle enthält Wege zu Zielnetzen.

Ein Router nutzt diese Tabelle, um zu entscheiden, wohin ein Paket weitergeleitet wird.

Eine Routing-Tabelle enthält typischerweise:

- Zielnetz
- Subnetzmaske oder Präfix
- nächster Hop
- Ausgangsschnittstelle
- Metrik

Merksatz:

Routing-Tabelle = Wegweiser für IP-Pakete.

Beispiel einer Routing-Tabelle

Vereinfachte Routing-Tabelle:

Zielnetz	Präfix	Nächster Hop	Schnittstelle
192.168.10.0	/24	direkt verbunden	LAN 1
192.168.20.0	/24	direkt verbunden	LAN 2
10.10.0.0	/16	192.168.20.254	LAN 2
0.0.0.0	/0	Provider-Router	WAN

Bedeutung:

192.168.10.0/24 liegt direkt an LAN 1.
 192.168.20.0/24 liegt direkt an LAN 2.
 10.10.0.0/16 ist über 192.168.20.254 erreichbar.
 Alles andere geht über die Default Route.

Merksatz:

Jede Route beschreibt einen Weg zu einem Zielnetz.

Direkt verbundene Route

Eine direkt verbundene Route entsteht, wenn eine Router-Schnittstelle eine IP-Adresse aus diesem Netz hat.

Beispiel:

Router-Interface:
 192.168.10.1/24

Dann kennt der Router direkt:

192.168.10.0/24

Für dieses Netz braucht der Router keinen nächsten Router.

Merksatz:

Direkt verbunden = Netz liegt an eigener Schnittstelle.

Statische Route

Eine statische Route wird manuell eingetragen.

Beispiel:

Zielnetz:
10.20.30.0/24

nächster Hop:
192.168.10.254

Der Administrator legt also fest:

Pakete zu 10.20.30.0/24 gehen über 192.168.10.254.

Vorteile:

- einfach bei kleinen Netzen
- gut kontrollierbar
- kein Routing-Protokoll nötig

Nachteile:

- manuelle Pflege
- fehleranfällig bei Änderungen
- keine automatische Anpassung bei Ausfällen

Merksatz:

Statische Route = manuell eingetragener Weg.

Dynamische Route

Dynamische Routen werden automatisch über Routing-Protokolle gelernt.

Beispiele für Routing-Protokolle:

- RIP
- OSPF
- BGP

Router tauschen dabei Informationen über erreichbare Netze aus.

Vorteile:

- automatische Anpassung
- besser für größere Netze
- alternative Wege möglich

Nachteile:

- komplexer
- muss richtig geplant werden
- braucht Absicherung

Merksatz:

Dynamische Route = automatisch gelernter Weg.

Default Route

Eine Default Route wird verwendet, wenn keine genauere Route passt.

IPv4-Schreibweise:

0.0.0.0/0

Bedeutung:

alle IPv4-Ziele

Beispiel:

Wenn der Router das Zielnetz nicht genauer kennt,
sendet er das Paket an den Provider-Router.

Merksatz:

Default Route = Route für alles Unbekannte.

Warum ist die Default Route wichtig?

Ohne Default Route kennt ein Router oder Client nur bestimmte Netze.

Ein normaler Client kennt meistens:

eigenes Subnetz
Standard-Gateway

Für Internetziele braucht der Client sein Gateway.

Der Router braucht wiederum oft eine Default Route Richtung Internet.

Merksatz:

Ohne Default Route funktionieren unbekannte externe Ziele nicht.

Nächster Hop

Der nächste Hop ist das nächste Gerät auf dem Weg zum Ziel.

Meistens ist das ein Router.

Beispiel:

Zielnetz:
10.10.0.0/16

nächster Hop:
192.168.20.254

Der Router sendet das Paket an 192.168.20.254, damit es von dort weitergeleitet wird.

Merksatz:

Nächster Hop = nächster Router auf dem Weg.

Ausgangsschnittstelle

Die Ausgangsschnittstelle ist die Schnittstelle, über die ein Paket den Router verlässt.

Beispiele:

LAN
WAN
VLAN 10
VLAN 20
SFP-Port
Tunnel-Interface

Bei direkt verbundenen Netzen reicht oft die Ausgangsschnittstelle.

Bei entfernten Netzen wird häufig ein nächster Hop angegeben.

Merksatz:

Ausgangsschnittstelle = Port oder Interface, über das das Paket weitergeht.

Metrik

Die Metrik ist ein Wert zur Bewertung einer Route.

Wenn mehrere Wege zum gleichen Ziel vorhanden sind, kann die Metrik bei der Auswahl helfen.

Eine kleinere Metrik bedeutet häufig:

bevorzugter Weg

Die genaue Bedeutung hängt vom Routing-Verfahren ab.

Merksatz:

Metrik = Bewertung eines Weges.

Longest Prefix Match

Wenn mehrere Routen passen, wählt der Router die genaueste Route.

Das nennt man:

Longest Prefix Match

Beispiel:

Route	passt für Ziel 192.168.10.50?
192.168.0.0/16	ja
192.168.10.0/24	ja
192.168.10.48/28	ja
0.0.0.0/0	ja

Die genaueste Route ist:

192.168.10.48/28

Warum?

/28 hat den längsten passenden Präfix.

Merksatz:

Genaueste passende Route gewinnt.

Default Route und Longest Prefix Match

Die Default Route passt immer.

Aber sie ist am wenigsten genau.

Beispiel:

Route	Präfix
192.168.10.0/24	/24
192.168.0.0/16	/16
0.0.0.0/0	/0

Für das Ziel:

192.168.10.20

wird die /24-Route gewählt.

Die Default Route wird nur verwendet, wenn keine genauere Route passt.

Merksatz:

Default Route ist der letzte Ausweg.

Routing-Entscheidung Schritt für Schritt

Ein Router arbeitet vereinfacht so:

1. IP-Paket kommt an.
2. Router liest die Ziel-IP-Adresse.
3. Router sucht passende Route in der Routing-Tabelle.
4. Genaueste passende Route wird gewählt.
5. Router bestimmt nächsten Hop oder Ausgangsschnittstelle.
6. Router erstellt einen neuen lokalen Frame.
7. Paket wird weitergeleitet.

Merksatz:

Router entscheidet nach Ziel-IP,
nicht nach Ziel-MAC des alten Frames.

Was passiert mit dem Ethernet-Frame am Router?

Ein Router trennt Schicht-2-Abschnitte.

Wenn ein Frame beim Router ankommt, passiert vereinfacht:

Der Router entfernt den alten Ethernet-Frame.
Das IP-Paket wird geprüft.
Der Router entscheidet den nächsten Weg.
Für den nächsten Abschnitt wird ein neuer Ethernet-Frame erstellt.

Dabei ändern sich:

Quell-MAC-Adresse
Ziel-MAC-Adresse

Grundsätzlich gleich bleiben:

Quell-IP-Adresse
Ziel-IP-Adresse

Ausnahme:

NAT oder PAT kann IP-Adressen verändern.

Merksatz:

Router erneuert den Frame,
aber routet das IP-Paket weiter.

ARP beim Routing

Auch Router brauchen lokale MAC-Adressen.

Wenn ein Router ein Paket zum nächsten Hop senden soll, muss er die MAC-Adresse des nächsten Hops kennen.

Dafür verwendet er bei IPv4 ARP.

Beispiel:

nächster Hop:
192.168.20.254

Der Router fragt per ARP:

Wer hat 192.168.20.254?

Merksatz:

Routing entscheidet den Weg,
ARP findet die lokale MAC für den nächsten Abschnitt.

Routing zwischen VLANs

VLANs trennen auf Schicht 2.

Wenn Geräte in unterschiedlichen VLANs kommunizieren sollen, braucht man Routing.

Das nennt man:

Inter-VLAN-Routing

Beispiel:

VLAN 10:
192.168.10.0/24

VLAN 20:
192.168.20.0/24

Kommunikation zwischen VLAN 10 und VLAN 20 benötigt eine Schicht-3-Komponente.

Merksatz:

VLAN zu VLAN braucht Routing.

Router-on-a-Stick

Router-on-a-Stick ist eine Methode für Inter-VLAN-Routing.

Dabei gibt es eine Trunk-Verbindung zwischen Switch und Router.

Über diesen Trunk laufen mehrere VLANs.

Der Router nutzt logische Unterinterfaces.

Beispiel:

Unterinterface	VLAN	Gateway-IP
G0/0.10	VLAN 10	192.168.10.1
G0/0.20	VLAN 20	192.168.20.1
G0/0.30	VLAN 30	192.168.30.1

Merksatz:

Router-on-a-Stick = Routing mehrerer VLANs über einen Router-Trunk.

Layer-3-Switch

Ein Layer-3-Switch kann Switching und Routing kombinieren.

Er arbeitet:

auf Schicht 2 als Switch
und
auf Schicht 3 als Router

Er kann zwischen VLANs routen, ohne dass ein separater Router nötig ist.

Dafür nutzt er oft virtuelle Schnittstellen.

Diese heißen je nach System zum Beispiel:

SVI
VLAN-Interface
Routing-Interface

Merksatz:

Layer-3-Switch = Switch mit Routing-Funktion.

Firewall als Gateway

In vielen Netzwerken ist eine Firewall das Standard-Gateway für VLANs.

Beispiel:

	VLAN	Gateway auf Firewall
	VLAN 10	192.168.10.1
	VLAN 20	192.168.20.1
	VLAN 30	192.168.30.1

Vorteil:

Die Firewall kann den Verkehr zwischen VLANs kontrollieren.

Beispiel:

Gäste dürfen ins Internet.

Gäste dürfen nicht auf Server.

Mitarbeiter dürfen auf bestimmte Serverdienste.

Merksatz:

Firewall als Gateway verbindet Routing mit Zugriffskontrolle.

Routing und Firewall unterscheiden

Routing entscheidet:

Wohin soll ein Paket weitergeleitet werden?

Firewall entscheidet:

Darf dieses Paket weitergeleitet werden?

Beide Funktionen können im gleichen Gerät sitzen.

Beispiel:

Eine Firewall routet zwischen VLANs
und prüft dabei Regeln.

Merksatz:

Routing findet den Weg.
Firewall erlaubt oder blockiert.

NAT und Routing unterscheiden

Routing leitet Pakete zwischen Netzen weiter.

NAT verändert IP-Adressen.

Beispiel Routing:

Paket wird von VLAN 10 ins Internet weitergeleitet.

Beispiel NAT:

private Quell-IP 192.168.10.20 wird zur öffentlichen IP des Routers übersetzt.

Merksatz:

Routing leitet weiter.
NAT übersetzt Adressen.

PAT und Internetzugang

PAT ist eine häufige Form von NAT.

PAT steht für:

Port Address Translation

Viele interne Geräte teilen sich eine öffentliche IPv4-Adresse.

Beispiel:

```
PC 1:  
192.168.10.20  
  
PC 2:  
192.168.10.30
```

Beide nutzen nach außen dieselbe öffentliche IP-Adresse.

Der Router unterscheidet die Verbindungen über Port-Zuordnungen.

Merksatz:

PAT ermöglicht vielen privaten Geräten gemeinsamen Internetzugang über eine öffentliche IP.

Routing-Schleife

Eine Routing-Schleife entsteht, wenn Router Pakete im Kreis weiterleiten.

Beispiel:

```
Router A sendet zu Router B.  
Router B sendet zurück zu Router A.
```

Folge:

Das Paket kreist im Netz,
bis die TTL abläuft.

Merksatz:

Routing-Schleife = Paket läuft auf Schicht 3 im Kreis.

TTL bei Routing-Schleifen

TTL steht für:

Time To Live

Jeder Router verringert die TTL eines IP-Pakets.

Wenn TTL 0 erreicht, wird das Paket verworfen.

Zweck:

IP-Pakete sollen nicht endlos im Netz kreisen.

Merksatz:

TTL begrenzt Routing-Schleifen.

Traceroute und Routing

Traceroute nutzt TTL-Verhalten, um den Weg zu einem Ziel sichtbar zu machen.

Je nach Betriebssystem heißt der Befehl:

```
tracert  
tracroute  
tracpath
```

Traceroute zeigt:

welche Router auf dem Weg liegen
und
wo die Verbindung möglicherweise stoppt.

Merksatz:

Traceroute hilft beim Prüfen des Routing-Wegs.

Ping und Routing

Ping kann helfen zu prüfen, ob ein Ziel per IP erreichbar ist.

Ping nutzt typischerweise ICMP Echo Request und Echo Reply.

Wenn Ping nicht funktioniert, kann das viele Ursachen haben:

- Ziel aus
- falsche IP-Adresse
- falsches Gateway
- fehlende Route
- Firewall blockiert ICMP
- Routing-Problem
- Schicht-1- oder Schicht-2-Problem

Merksatz:

Ping prüft Erreichbarkeit,
aber erklärt nicht allein die Ursache.

Typische Routing-Fehler

Typische Fehler sind:

- falsches Standard-Gateway
- fehlende Default Route
- fehlende Route zum Zielnetz
- falscher nächster Hop
- Gateway nicht erreichbar
- falsche Subnetzmaske
- Routing-Schleife
- asymmetrisches Routing
- Firewall blockiert Verkehr
- NAT falsch konfiguriert

Merksatz:

Routing-Fehler betreffen Wege zwischen IP-Netzen.

Fehlerbild: Gateway nicht erreichbar

Mögliche Ursachen:

- Gateway-IP falsch eingetragen
- Gateway liegt nicht im eigenen Subnetz
- falsches VLAN
- Router-Interface down
- ARP zum Gateway funktioniert nicht
- Schicht-1-Problem
- Schicht-2-Problem

Prüfung:

- IP-Adresse prüfen.
- Subnetzmaske prüfen.
- Gateway prüfen.
- ARP-Eintrag prüfen.
- VLAN prüfen.
- Link prüfen.

Merksatz:

Gateway-Probleme können Schicht 2 oder Schicht 3 betreffen.

Fehlerbild: Internet funktioniert nicht

Wenn ein Client das Internet nicht erreicht, kann ein Routing-Problem vorliegen.

Mögliche Ursachen:

- falsches Gateway
- Gateway nicht erreichbar
- DNS funktioniert nicht
- Default Route fehlt
- NAT fehlt
- Firewall blockiert
- Provider-Verbindung gestört
- IP-Konfiguration falsch

Wichtig:

DNS-Problem und Routing-Problem unterscheiden.

Beispiel:

Ping auf 8.8.8.8 funktioniert,
aber www.example.com nicht.

Dann ist Routing wahrscheinlich grundsätzlich möglich, aber DNS könnte das Problem sein.

Merksatz:

IP-Ziel testen,
danach DNS prüfen.

Fehlerbild: Ein Netz erreicht anderes Netz nicht

Beispiel:

VLAN 10 erreicht VLAN 20 nicht.

Mögliche Ursachen:

- Inter-VLAN-Routing fehlt
- Gateway-IP fehlt
- falsche Firewall-Regel
- falsche Route
- VLAN nicht korrekt angebunden
- Subnetzmaske falsch
- Rückroute fehlt

Merksatz:

Kommunikation zwischen Netzen braucht Hin- und Rückweg.

Rückroute

Eine Rückroute ist der Weg zurück zum Absendernetz.

Kommunikation braucht nicht nur einen Hinweg, sondern auch einen Rückweg.

Beispiel:

Netz A sendet zu Netz B.

Netz B muss Antwortpakete zurück zu Netz A senden können.

Wenn die Rückroute fehlt, sieht es so aus, als ob das Ziel nicht antwortet.

Merksatz:

Ohne Rückroute keine funktionierende Antwort.

Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

Hinweg und Rückweg nehmen unterschiedliche Pfade.

Das ist nicht immer ein Fehler.

Aber es kann problematisch sein, wenn Firewalls oder zustandsbehaftete Prüfungen beteiligt sind.

Warum?

Eine Firewall erwartet oft,
dass sie beide Richtungen einer Verbindung sieht.

Merksatz:

Asymmetrisches Routing kann Firewalls stören.

Routing und Dokumentation

Routing sollte sauber dokumentiert werden.

Wichtige Informationen:

- Netze
- Subnetze
- Gateways
- Routing-Tabellen
- Default Routes
- Firewall-Zonen
- VLAN-Zuordnung
- NAT-Regeln
- WAN-Verbindungen

Merksatz:

Ohne Dokumentation wird Routing-Fehlersuche schnell unübersichtlich.

Einordnung in das OSI-Modell

Thema	Schicht
Ethernet-Frame	2
MAC-Adresse	2
VLAN	2
IP-Adresse	3
IP-Paket	3
Routing	3
Router	3
Gateway	3
Routing-Tabelle	3
ICMP	3
TCP-Port	4
DNS	7

Merksatz:

MAC/VLAN = Schicht 2.

IP/Routing = Schicht 3.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet Routing?
- Welche Aufgabe hat ein Router?
- Was ist eine Routing-Tabelle?
- Was ist eine Default Route?
- Was bedeutet 0.0.0.0/0?
- Was ist ein Standard-Gateway?
- Wann wird ein Gateway benötigt?
- Was ist ein nächster Hop?
- Was bedeutet Longest Prefix Match?
- Was ist der Unterschied zwischen statischem und dynamischem Routing?
- Was ist Inter-VLAN-Routing?
- Was ist Router-on-a-Stick?
- Was ist ein Layer-3-Switch?
- Was ist eine Routing-Schleife?
- Warum ist TTL wichtig?
- Warum braucht Kommunikation auch eine Rückroute?

Typische Prüfungsfallen

Routing gehört zu Schicht 3.

Router leiten IP-Pakete weiter,
keine Ethernet-Frames über mehrere Netze.

Switches leiten Frames anhand von MAC-Adressen weiter.

Router entscheiden anhand von IP-Adressen.

Gateway wird nur für Ziele außerhalb des eigenen Subnetzes benötigt.

Das Standard-Gateway muss im eigenen Subnetz liegen.

Default Route = 0.0.0.0/0.

Genaueste passende Route gewinnt.

Direkt verbundene Netze brauchen keinen nächsten Hop.

Kommunikation braucht Hinweg und Rückweg.

Fehlende Rückroute kann wie ein Zielproblem aussehen.

Routing ist nicht NAT.

Routing ist nicht Firewall.

VLAN zu VLAN braucht Routing.

TTL begrenzt Routing-Schleifen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Routing	Weiterleitung von IP-Paketen zwischen Netzen
Router	Gerät zur Verbindung verschiedener IP-Netze
Routing-Tabelle	Tabelle mit Wegen zu Zielnetzen
Zielnetz	Netz, zu dem ein Paket geleitet werden soll
Nächster Hop	nächster Router auf dem Weg
Ausgangsschnittstelle	Interface, über das das Paket weitergeht
Metrik	Bewertung eines Weges
Direkt verbunden	Netz liegt an eigener Schnittstelle
Statische Route	manuell eingetragene Route
Dynamische Route	automatisch gelernte Route
Default Route	Route für unbekannte Ziele
Longest Prefix Match	genaueste passende Route gewinnt
Standard-Gateway	Router für Ziele außerhalb des eigenen Netzes
Inter-VLAN-Routing	Routing zwischen VLANs
Router-on-a-Stick	Inter-VLAN-Routing über Router-Trunk
Layer-3-Switch	Switch mit Routing-Funktion
NAT	Übersetzung von IP-Adressen

Begriff	Kurze Erklärung
PAT	NAT mit Port-Zuordnung
Routing-Schleife	Paket läuft auf Schicht 3 im Kreis
TTL	begrenzt Lebensdauer eines IP-Pakets
Rückroute	Weg zurück zum Absendernetz
asymmetrisches Routing	Hin- und Rückweg sind unterschiedlich

IHK-sichere Kurzformulierung

Routing ist die Weiterleitung von IP-Paketen zwischen unterschiedlichen IP-Netzen und gehört zu OSI-Schicht 3. Ein Router entscheidet anhand der Ziel-IP-Adresse und seiner Routing-Tabelle, wohin ein Paket weitergeleitet wird. Befindet sich ein Ziel nicht im eigenen Subnetz, sendet ein Client das Paket an sein Standard-Gateway. Die Default Route 0.0.0.0/0 wird verwendet, wenn keine genauere Route vorhanden ist. Bei mehreren passenden Routen gilt das Longest Prefix Match, also die genaueste passende Route gewinnt. Für funktionierende Kommunikation müssen Hinweg und Rückweg vorhanden sein.

Merksätze

Routing = Schicht 3.

Routing = IP-Pakete zwischen Netzen weiterleiten.

Router entscheidet anhand der Ziel-IP.

Switch entscheidet anhand der Ziel-MAC.

Routing-Tabelle = Wegweiser für IP-Pakete.

Gateway = Ausgang in andere Netze.

Gleiches Subnetz = direkt.

Anderes Subnetz = Gateway.

Gateway muss im eigenen Subnetz liegen.

Direkt verbunden = eigene Schnittstelle im Zielnetz.

Statische Route = manuell.

Dynamische Route = automatisch gelernt.

Default Route = 0.0.0.0/0.

Default Route = letzter Ausweg.

Longest Prefix Match = genaueste Route gewinnt.

Nächster Hop = nächster Router.

Router erneuert den Ethernet-Frame.

IP-Paket wird weitergeroutet.

MAC ändert sich pro Abschnitt.

IP bleibt grundsätzlich erhalten.

VLAN zu VLAN braucht Routing.

Routing findet den Weg.

Firewall entscheidet erlaubt oder blockiert.

NAT übersetzt Adressen.

TTL begrenzt Routing-Schleifen.

Kommunikation braucht Hinweg und Rückweg.
