ÜBUNG 11

Packet Forwarding

NETZWERKTECHNIK / SEMESTER 3 UND 4

1

AGENDA

01 LAYER 2/3 FORWARDING UND ROUTING

02 FORWARDING ARCHITEKTUREN

03 ZUSAMMENFASSUNG

tgm

2

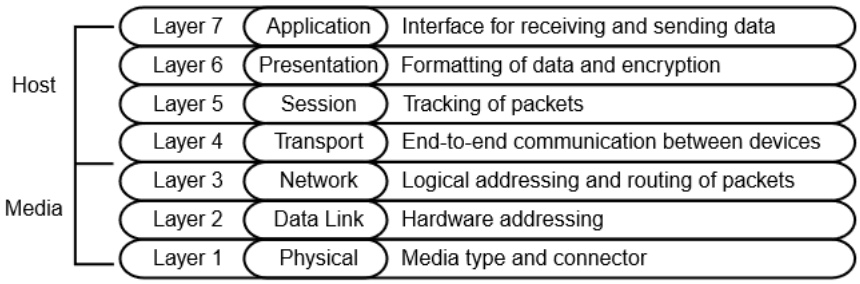
01

Layer 2/3 Forwarding und Routing

3

OSI Modell

TCP/IP basiert auf dem Open Systems Interconnection (OSI)-Modell, das aus sieben Schichten besteht, wie in der Abbildung gezeigt.

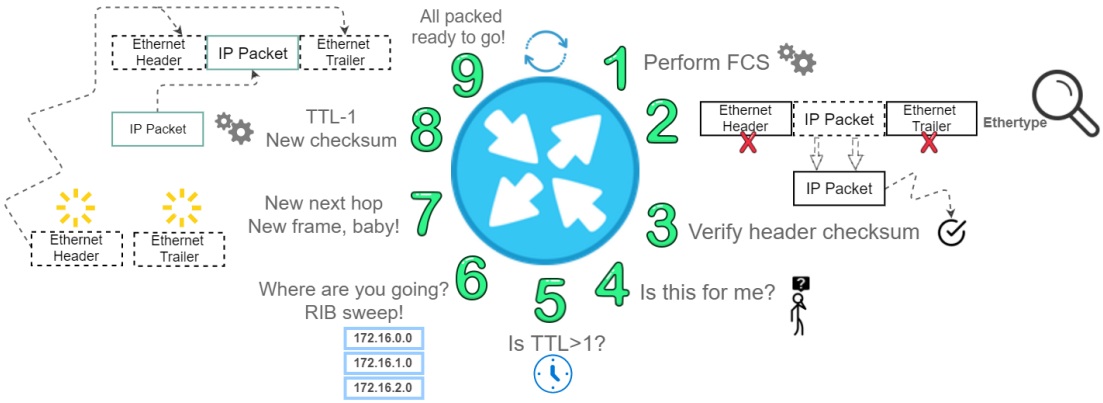


[Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

4

NETZWERKTECHNIK / SEMESTER 3 und 4

„Forwarding“ Prozess in einem Router



[Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

5

NETZWERKTECHNIK / SEMESTER 3 und 4

„Forwarding“ Prozess in einem Router

1. **Der Router empfängt ein Frame und prüft die empfangene Frame-Prüfsequenz (FCS)**, um sicherzustellen, dass er es verarbeiten kann. Bei Abweichungen wird das Frame verworfen.
2. Ist die FCS-Prüfung erfolgreich, prüft der Router den **Ethernet-Typ des Pakets** und extrahiert es.
3. Nach der Extraktion des Pakets hängen die folgenden Aktionen von der IP-Version des Pakets ab: **Bei IPv4 wird die Header-Prüfsumme überprüft**; ein Paket mit falscher Prüfsumme wird verworfen. Bei IPv6 wird diese Prüfung übersprungen, da der Header eines IPv6-Pakets keine Prüfsumme enthält.
4. **Der Router prüft, ob die Zieladresse des Pakets mit einer der auf seinen Schnittstellen konfigurierten IP-Adressen im Status „aktiv, Leitungsprotokoll aktiv“ übereinstimmt.** Bei Übereinstimmung ist der Router das endgültige Ziel des Pakets und verarbeitet es lokal.
5. Stimmt die Zieladresse mit keiner der konfigurierten Schnittstellen im Status „aktiv, Leitungsprotokoll aktiv“ überein, **beginnt das Routing. Damit dies möglich ist, muss die TTL größer als 1 sein.** Der Router prüft, ob die TTL größer als 1 ist. Wenn ja, kann das Paket weitergeleitet werden; andernfalls wird es verworfen und der Absender mit einer ICMP-Nachricht „Zeitüberschreitung“ benachrichtigt.

[Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

6

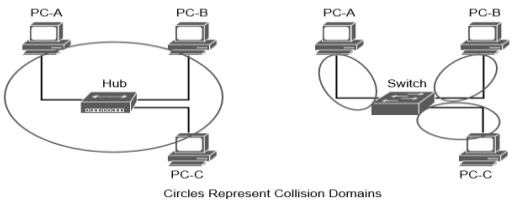
„Forwarding“ Prozess in einem Router

6. Jetzt geht es ans Routing! – Der Router prüft seine Routing-Tabelle und **sucht nach der längsten Präfixübereinstimmung** für die Zieladresse im Paket.
7. Sobald der nächste Hop und die ausgehende Schnittstelle in der Routing-Tabelle gefunden wurden, **benötigt der Router die Sicherungsschichtinformationen des nächsten Hops**, um einen neuen Frame zu erstellen und das Paket zustellen zu können. Er verwendet Mechanismen wie **ARP** – es gibt viele weitere –, um Schicht-3-Informationen Schicht-2-Informationen zuzuordnen.
8. Da das Paket weitergeleitet wird, wird die **TTL um eins reduziert**. Dadurch ändert sich der Inhalt des IP-Headers (TTL), und die **IPv4-Prüfsumme wird neu berechnet**.
9. Schließlich **kapselt das Routing das verarbeitete Paket in den neu erstellten Datenlink-Header und -Trailer ein**. Und schon haben wir einen neuen Frame, den wir direkt versenden können!

tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

Layer 2 Forwarding und Kollisionsdomänen

- Die **Sicherungsschicht (Data Link Layer, DSL)** ist für die Adressierung unterhalb des IP-Protokollstapels zuständig, um die Kommunikation zwischen Hosts zu steuern.
- Ethernet verwendet üblicherweise **MAC-Adressen (Media Access Control)**, während andere DSL-Protokolle wie Frame Relay ein völlig anderes Verfahren zur Adressierung auf Schicht 2 nutzen.
- Kollisionsdomänen:
  - **Ethernet-Geräte verwenden CSMA/CD** (Carrier Sense Multiple Access/Collision Detection), um sicherzustellen, dass in einer Kollisionsdomäne immer nur ein Gerät gleichzeitig sendet.
  - Geräte können daher nur gleichzeitig Daten senden oder empfangen (**Halbduplex-Betrieb**).



tgm [Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

Kollisionsdomänen auf einem Hub vs. Switch

- **Unbekanntes Unicast-Flooding** tritt auf, wenn ein Paket eine Ziel-MAC-Adresse enthält, die nicht in der MAC-Adresstabelle des Switches vorhanden ist. Der Switch leitet das Paket über alle Switch-Ports weiter.
- **Broadcast-Verkehr** ist Netzwerkverkehr, der für alle Hosts im LAN bestimmt ist und über alle Switch-Port-Schnittstellen weitergeleitet wird.
- **Netzwerk-Broadcasts überschreiten keine Layer-3-Grenzen** (von einem Subnetz zum anderen).

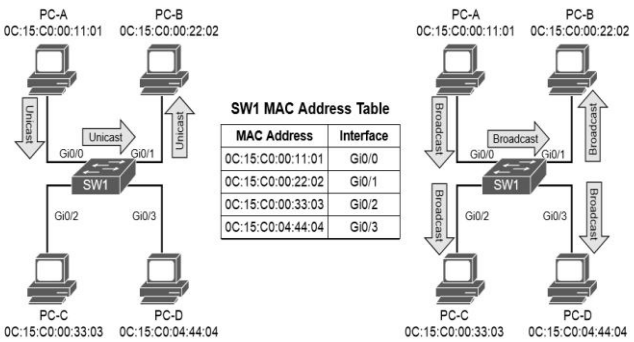
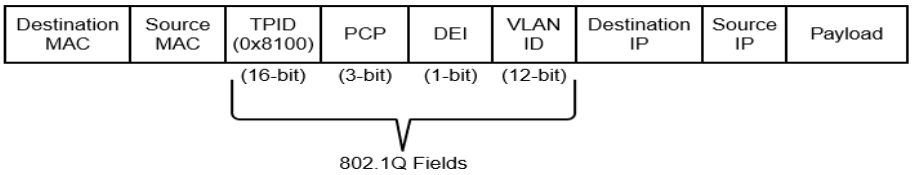


Figure 1-3 *Unicast and Broadcast Traffic Patterns*

tgm [Quelle: CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE), by Cisco Networking Academy, Cisco Press]

Virtual LANs

- Das Einfügen eines **Routers zwischen LAN-Segmenten trägt zur Verkleinerung von Broadcast-Domänen bei**.
- **Virtuelle LANs (VLANs) ermöglichen eine logische Segmentierung**, indem sie mehrere Broadcast-Domänen auf demselben Netzwerk-Switch erstellen. VLANs verbessern die Auslastung der Switch-Ports, da ein Port der benötigten Broadcast-Domäne zugeordnet werden kann und mehrere Broadcast-Domänen auf demselben Switch vorhanden sein können.
- **VLANs sind im IEEE-802.1Q-Standard definiert**. Dieser legt fest, dass dem Paketheader 32 Bit mit folgenden Feldern hinzugefügt werden: Tag-Protokollkennung (TPID), Prioritätscode (PCP), Drop-Eligible-Indikator (DEI) und VLAN-Kennung (VLAN-ID).



tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Ein VLAN erzeugen

- VLANs werden in der globalen Konfiguration erstellt.
- VLANs werden im VLAN sub-global mode benannt.
- VLANs und ihre Portzuordnung werden mit dem Befehl **show vlan [{brief | id vlan-id | name vlanname | summary}]** überprüft. Die Ausgabe ist in vier Hauptabschnitte unterteilt: VLAN-Port-Zuordnungen, System-MTU, SPAN-Sitzungen und private VLANs.

```
SW1# configure term
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 10
SW1(config-vlan)# name PCs
SW1(config-vlan)# vlan 20
SW1(config-vlan)# name Phones
SW1(config-vlan)# vlan 99
SW1(config-vlan)# name Guest
```


Optionale show vlan Schlüsselwörter

Die optionalen Schlüsselwörter des Befehls „show vlan“ bieten folgende Vorteile:

- **BRIEF** – Zeigt nur die relevanten Port-zu-VLAN-Zuordnungen an.
- **SUMMARY** – Zeigt die Anzahl der VLANs, der am VTP beteiligten VLANs und der VLANs im erweiterten VLAN-Bereich an.
- **id VLAN-ID** – Zeigt die gesamte Ausgabe des ursprünglichen Befehls, gefiltert nach der angegebenen VLAN-Nummer.
- **name VLAN-Name** – Zeigt die gesamte Ausgabe des ursprünglichen Befehls, gefiltert nach dem angegebenen VLAN-Namen.

NETZWERKTECHNIK / SEMESTER 3 und 4

Access Ports

Access-Ports sind die grundlegenden Bausteine eines Managed Switches.

- Ein **Access-Port ist genau einem VLAN zugeordnet**.
- Er leitet Datenverkehr vom angegebenen VLAN an das angeschlossene Gerät oder von diesem Gerät an andere Geräte im selben VLAN.
- Verwenden Sie den Befehl **switchport mode access**, um einen Port manuell als Access-Port zu konfigurieren.
- Mit dem Befehl **switchport access {vlan vlan-id | name vlanname}** wird dem Port ein bestimmtes VLAN zugewiesen.

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 99
SW1(config-vlan)# name Guests
SW1(config-vlan)# interface gi1/0/15
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 99
SW1(config-if)# interface gi1/0/16
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan name Guest
```

```
SW1# show running-config | begin interface GigabitEthernet1/0/15
interface GigabitEthernet1/0/15
 switchport access vlan 99
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 99
 switchport mode access
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Trunk Ports

Trunk-Ports können mehrere VLANs übertragen. Sie werden typischerweise verwendet, wenn mehrere VLANs eine Verbindung zwischen einem Switch und einem anderen Switch, Router oder einer Firewall benötigen und nur einen Port nutzen.

Trunk-Ports werden auf Catalyst-Switches statisch mit dem Befehl **switch-port mode trunk** definiert.

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gi1/0/2
SW1(config-if)# switchport mode trunk
SW1(config-if)# interface gi1/0/3
SW1(config-if)# switchport mode trunk
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Trunk Ports

Der Befehl **show interfaces trunk** liefert viele nützliche Informationen:

- Der erste Abschnitt listet **alle Trunk-Ports**, ihren Status, die Zuordnung zu einem EtherChannel und die Information, ob es sich um ein natives VLAN handelt, auf.
- Der zweite Abschnitt der Ausgabe zeigt die Liste der am **Trunk-Port zulässigen VLANs**. Der Datenverkehr an Trunk-Ports kann minimiert werden, indem VLANs auf bestimmte Switches beschränkt werden, wodurch auch Broadcast-Verkehr eingeschränkt wird.
- Der dritte Abschnitt **zeigt die VLANs an, die sich am Switch im Weiterleitungszustand befinden**. Ports im Blockierungszustand werden in diesem Abschnitt nicht aufgeführt.

```
SW1# show interfaces trunk
! Section 1 displays the native VLAN associated on this port, the status and
! if the port is associated to a EtherChannel

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/2     on               802.1q         trunking      1
Gi1/0/3     on               802.1q         trunking      1

! Section 2 displays all of the VLANs that are allowed to be transmitted across
! the trunk ports

Port        Vlans allowed on trunk
Gi1/0/2     1-4094
Gi1/0/3     1-4094

Port        Vlans allowed and active in management domain
Gi1/0/2     1,10,20,99
Gi1/0/3     1,10,20,99

! Section 3 displays all of the VLANs that are allowed across the trunk and are
! in a spanning tree forwarding state

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/2     1,10,20,99
Gi1/0/3     1,10,20,99
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Native VLANs

Im 802.1Q-Standard wird jeglicher Datenverkehr, der über einen Trunk-Port **ohne 802.1Q-VLAN-Tag gesendet oder empfangen wird, dem nativen VLAN zugeordnet**.

- Das standardmäßige native VLAN ist VLAN 1.
- Wenn ein Switch zwei Access-Ports als Access-Ports konfiguriert und VLAN 10 zugeordnet hat – d. h., ein Host ist an einen Trunk-Port mit dem nativen VLAN 10 angeschlossen –, kann dieser Host mit den an die Access-Ports angeschlossenen Geräten kommunizieren.
- **Das native VLAN muss auf beiden Trunk-Ports übereinstimmen**, da der Datenverkehr sonst unbeabsichtigt die VLANs wechseln kann. Obwohl die Verbindung zwischen Hosts möglich ist (vorausgesetzt, sie befinden sich in unterschiedlichen VLANs), führt dies bei den meisten Netzwerktechnikern zu Verwirrung und ist keine Best Practice.
- **Ein natives VLAN ist eine portspezifische Konfiguration** und wird mit dem Befehl **switchport trunk native vlan vlan-id** geändert.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Allowed VLANs

Der Befehl **switchport trunk allowed vlan vlan-ids** legt die VLANs fest, die über die Verbindung übertragen werden dürfen. Beispiel 1-7 zeigt eine Konfiguration zur Beschränkung der VLANs, die den Trunk-Port Gi1/0/2 für die VLANs 1, 10, 20 und 99 passieren dürfen.

- Die vollständige Befehlssyntax **switchport trunk allowed {vlan-ids | all | none | add vlan-ids | remove vlan-ids | except vlan-ids}** bietet umfangreiche Möglichkeiten mit einem einzigen Befehl.
- Das optionale Schlüsselwort `**all**` aktiviert alle VLANs, während `**none**` alle VLANs vom Trunk-Link entfernt.
- Das Schlüsselwort `**add**` fügt weitere VLANs zu den bereits aufgeführten hinzu, und das Schlüsselwort `**remove**` entfernt das angegebene VLAN aus den bereits für diesen Trunk-Link identifizierten VLANs.

```
SW1# show run interface gi1/0/1
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 1,10,20,99
 switchport mode trunk
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

MAC Address Table

Die MAC-Adresstabelle **dient der Identifizierung der Switch-Ports und VLANs**, denen ein Gerät zugeordnet ist.

Ein **Switch erstellt die MAC-Adresstabelle, indem er die Quell-MAC-Adresse des empfangenen Datenverkehrs analysiert**. Diese Informationen werden anschließend verwaltet, um die Kollisionsdomäne (Punkt-zu-Punkt-Kommunikation zwischen Geräten und Switches) zu verkleinern, indem die Menge an unbekanntem Unicast-Flooding reduziert wird.

Die MAC-Adresstabelle wird mit dem Befehl **show mac address-table [address mac-address | dynamic | vlan vlan-id]** angezeigt.

Die optionalen Schlüsselwörter dieses Befehls bieten folgende Vorteile:

- **address mac-address** – Zeigt Einträge an, die der angegebenen MAC-Adresse entsprechen. Dieser Befehl kann bei Switches mit Hunderten von Ports hilfreich sein.
- **dynamic** – Zeigt Einträge an, die dynamisch gelernt wurden und nicht statisch festgelegt oder im Switch fest gespeichert sind.
- **vlan vlan-id** – Zeigt Einträge an, die dem angegebenen VLAN entsprechen.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

MAC Address Table

- Der Befehl **mac address-table static mac-address vlan vlan-id {drop | interface interface-id}** fügt einen manuellen Eintrag hinzu, der einem bestimmten Switch-Port zugeordnet oder eingehender Datenverkehr verworfen werden kann.
- Der Befehl **clear mac address-table dynamic [{address mac-address | interface interface-id | vlan vlan-id}]** leert die MAC-Adresstabelle des gesamten Switches.
- **Die MAC-Adresstabelle befindet sich im inhaltsadressierbaren Speicher (CAM).** Der CAM nutzt aufgrund seiner Suchtechniken einen Hochgeschwindigkeitsspeicher, der schneller als der typische Arbeitsspeicher (RAM) ist.
- **CAM arbeitet intern wie eine große Hardware-Suchmaschine**. Wenn der Switch eine MAC-Adresse sucht:
  - Er legt die Adresse an das CAM-Feld an.
  - Alle CAM-Einträge werden parallel abgefragt.
  - Der eine passende Eintrag liefert ein Match-Signal zurück, also:1 = Treffer (MAC-Adresse gefunden); 0 = kein Treffer
  - Die Ausgabe ist also ein Binärmuster, aus dem dann der Index des passenden Ports ermittelt wird.

```
SW1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0081.c4ff.8b01    DYNAMIC     Gi1/0/2
   1    189c.5d11.9981    DYNAMIC     Gi1/0/3
   1    189c.5d11.99c7    DYNAMIC     Gi1/0/3
   1    7070.8bcf.f828    DYNAMIC     Gi1/0/17
   1    70df.2f22.b882    DYNAMIC     Gi1/0/2
   1    70df.2f22.b883    DYNAMIC     Gi1/0/3
   1    bc67.1c5c.9304    DYNAMIC     Gi1/0/2
   1    bc67.1c5c.9347    DYNAMIC     Gi1/0/3
  99    189c.5d11.9981    DYNAMIC     Gi1/0/3
  99    7069.5ad4.c228    DYNAMIC     Gi1/0/15
  10    0087.31ba.3980    DYNAMIC     Gi1/0/9
  10    0087.31ba.3981    DYNAMIC     Gi1/0/9
  10    189c.5d11.9981    DYNAMIC     Gi1/0/3
  10    3462.8800.6921    DYNAMIC     Gi1/0/8
  10    5067.ae2f.6480    DYNAMIC     Gi1/0/7
  10    7069.5ad4.c220    DYNAMIC     Gi1/0/13
  10    e8ed.f3aa.7b98    DYNAMIC     Gi1/0/12
  20    189c.5d11.9981    DYNAMIC     Gi1/0/3
  20    7069.5ad4.c221    DYNAMIC     Gi1/0/14
Total Mac Addresses for this criterion: 19
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

19

NETZWERKTECHNIK / SEMESTER 3 und 4

Status des Switchport

Die Überprüfung der Konfiguration eines Switch-Ports kann hilfreich sein; allerdings überschreiben einige an anderer Stelle in der Konfiguration gespeicherte Befehle die für die Schnittstelle festgelegte Konfiguration.

- Der Befehl **show interfaces interface-id switchport** liefert alle relevanten Informationen zum Status eines Switch-Ports.
- Der Befehl **show interfaces switchport** zeigt dieselben Informationen für alle Ports des Switches an.

```
SW1# show interfaces gi1/0/5 switchport
Name: Gi1/0/5
! The following line indicates if the port is shut or no shut
Switchport: Enabled
Administrative Mode: dynamic auto
! The following line indicates if the port is acting as static access port, trunk
! port, or if is down due to carrier detection (i.e. link down)
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
! The following line displays the VLAN assigned to the access port
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

```
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

20

NETZWERKTECHNIK / SEMESTER 3 und 4

Status des Interfaces

Der Befehl **show interface status** ist ein weiterer nützlicher Befehl, um den Status von Switch-Ports übersichtlich und einfach anzuzeigen.

- **Port** – Zeigt die Schnittstellen-ID oder den Portkanal an.
- **Name** – Zeigt die konfigurierte Schnittstellenbeschreibung an.
- **Status** – Zeigt „Verbunden“ für Verbindungen an, die erkannt und hergestellt wurden. „Nicht verbunden“ wird angezeigt, wenn keine Verbindung erkannt wurde, und „err-deaktiviert“, wenn ein Fehler aufgetreten ist und der Switch die Weiterleitung von Datenverkehr über diesen Port deaktiviert hat.

```
SW1# show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/2   SW-2 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW-3 Gi1/0/1       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/5                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/6                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/7   Cube13.C           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/8   Cube11.F           connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/9   Cube10.A           connected    10         a-full  a-100 10/100/1000BaseTX
Gi1/0/10                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/11                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/12  Cube14.D Phone     connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/13  R1-G0/0/0          connected    10         a-full a-1000 10/100/1000BaseTX
Gi1/0/14  R2-G0/0/1          connected    20         a-full a-1000 10/100/1000BaseTX
Gi1/0/15  R3-G0/1/0          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/16  R4-G0/1/1          connected    99         a-full a-1000 10/100/1000BaseTX
Gi1/0/17                     connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/18                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/19                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/21                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/22                     notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/23                     notconnect   routed       auto   auto 10/100/1000BaseTX
Gi1/0/24                     disabled     4011         auto   auto 10/100/1000BaseTX
Te1/1/1                      notconnect   1            full    10G SFP-10GBase-SR
Te1/1/2                      notconnect   1            auto   auto unknown
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Status des Interfaces

- **VLAN** – Zeigt die VLAN-Nummer der Access-Ports an. Trunk-Verbindungen werden als Trunk angezeigt, und als Layer-3-Schnittstellen konfigurierte Ports werden als geroutet angezeigt.
- **Duplex** – Zeigt den Duplexmodus des Ports an. Bei automatischer Duplex-Aushandlung wird ein „a-“ vorangestellt.
- **Geschwindigkeit** – Zeigt die Portgeschwindigkeit an. Bei automatischer Portgeschwindigkeit wird ein „a-“ vorangestellt.
- **Typ** – Zeigt den Schnittstellentyp des Switch-Ports an. Bei einem festen RJ-45-Kupferport enthält die Beschreibung „TX“ (z. B. 10/100/1000BASE-TX). SFP-Ports (Small Form-Factor Pluggable) werden mit dem SFP-Modell aufgeführt, sofern ein Treiber in der Software vorhanden ist; andernfalls wird „Unbekannt“ angezeigt.

SW1# show interface status

Port   Name   Status   Vlan   Duplex Speed Type
Gi1/0/1   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/2   SW-2 Gi1/0/1   connected   trunk   a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW-3 Gi1/0/1   connected   trunk   a-full a-1000 10/100/1000BaseTX
Gi1/0/4   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/5   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/6   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/7   Cube13.C   connected   10   a-full a-1000 10/100/1000BaseTX
Gi1/0/8   Cube11.F   connected   10   a-full a-1000 10/100/1000BaseTX
Gi1/0/9   Cube10.A   connected   10   a-full a-100 10/100/1000BaseTX
Gi1/0/10   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/11   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/12 Cube14.D Phone   connected   10   a-full a-1000 10/100/1000BaseTX
Gi1/0/13 R1-G0/0/0   connected   10   a-full a-1000 10/100/1000BaseTX
Gi1/0/14 R2-G0/0/1   connected   20   a-full a-1000 10/100/1000BaseTX
Gi1/0/15 R3-G0/1/0   connected   99   a-full a-1000 10/100/1000BaseTX
Gi1/0/16 R4-G0/1/1   connected   99   a-full a-1000 10/100/1000BaseTX
Gi1/0/17   connected   1   a-full a-1000 10/100/1000BaseTX
Gi1/0/18   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/19   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/20   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/21   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/22   notconnect   1   auto   auto 10/100/1000BaseTX
Gi1/0/23   notconnect   routed   auto   auto 10/100/1000BaseTX
Gi1/0/24   disabled   4011   auto   auto 10/100/1000BaseTX
Te1/1/1   notconnect   1   full   10G SFP-10GBase-SR
Te1/1/2   notconnect   1   auto   auto unknown

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Layer 3 Forwarding und Local Network Forwarding

Ein Teil der Layer-3-Weiterleitungslogik findet vor der Layer-2-Weiterleitung statt.

Es gibt zwei Hauptmethoden für die Layer-3-Weiterleitung:

- Weiterleitung von Datenverkehr **an Geräte im selben Subnetz**
- Weiterleitung von Datenverkehr **an Geräte in einem anderen Subnetz**

Lokale Netzwerkweiterleitung

- Zwei Geräte im selben Subnetz kommunizieren lokal. Da die Daten mit ihrer IP-Adresse gekapselt sind, erkennt das Gerät, dass sich das Ziel im selben Netzwerk befindet. Das Gerät muss jedoch noch die Layer-2-Informationen in das Paket kapseln. **Es kennt seine eigene MAC-Adresse, aber zunächst nicht die MAC-Adresse des Ziels.**
- Die **ARP-Tabelle (Address Resolution Protocol) ermöglicht die Zuordnung von Layer-3-IP-Adressen zu Layer-2-MAC-Adressen**, indem sie die IP-Adresse eines Hosts und seine zugehörige MAC-Adresse speichert.
- Die ARP-Tabelle kann mit dem Befehl **show ip arp [mac-address | ip-address | vlan vlan-id | interface-id]** angezeigt werden. Optionale Schlüsselwörter ermöglichen das Filtern der Informationen.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

23

NETZWERKTECHNIK / SEMESTER 3 und 4

Packet Routing

Pakete müssen geroutet werden, wenn sich zwei Geräte in unterschiedlichen Netzwerken befinden. Da die Daten mit ihrer IP-Adresse gekapselt sind, erkennt ein Gerät, dass sich sein Ziel in einem anderen Netzwerk befindet und geroutet werden muss.

Das Gerät **prüft seine lokale Routingtabelle**, um die IP-Adresse des nächsten Hops zu ermitteln. Diese kann auf verschiedene Weisen ermittelt werden:

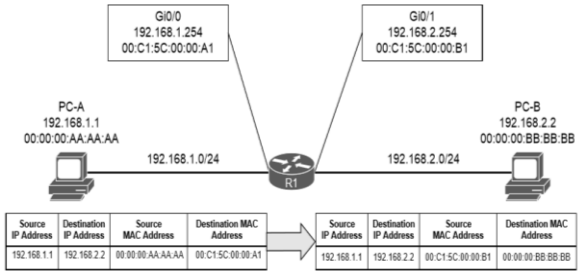
- Über einen **statischen Routeneintrag** erhält es das Zielnetzwerk, die Subnetzmaske und die IP-Adresse des nächsten Hops.
- Ein **Standardgateway** ist eine vereinfachte statische Standardroute, die lediglich die lokale IP-Adresse des nächsten Hops für den gesamten Netzwerkverkehr anfordert.
- Routen können auch von **Routingprotokollen** gelernt werden.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

24

Packet Routing

- **Das Quellgerät muss die entsprechenden Layer-2-Header (Quell- und Ziel-MAC-Adresse) hinzufügen.** Die Ziel-MAC-Adresse wird für die Next-Hop-IP-Adresse benötigt.
- Das Gerät sucht den **Eintrag für die Next-Hop-IP-Adresse in der ARP-Tabelle** und verwendet die dort angegebene MAC-Adresse als Ziel-MAC-Adresse.
- Im nächsten Schritt wird das Datenpaket zur **Verarbeitung und Weiterleitung an Layer 2** gesendet.
- Der nächste Router empfängt das Paket anhand der Ziel-MAC-Adresse.
  - Er **analysiert die Ziel-IP-Adresse**, sucht den entsprechenden Netzwerkeintrag in seiner **Routing-Tabelle und identifiziert die ausgehende Schnittstelle**.
  - Anschließend **ermittelt er die MAC-Adresse des Zielgeräts** (oder die MAC-Adresse des nächsten Hops, falls eine Weiterleitung erforderlich ist).

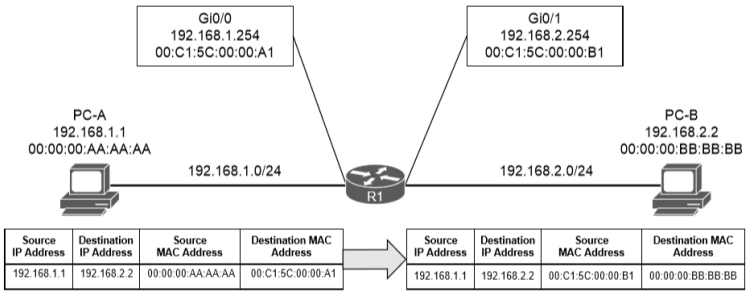


[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

25

Packet Routing

Schließlich **ändert der Router die Quell-MAC-Adresse in die MAC-Adresse seiner ausgehenden Schnittstelle** und die **Ziel-MAC-Adresse in die MAC-Adresse des Zielgeräts** (bzw. des nächsten Routers).



[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

26

NETZWERKTECHNIK / SEMESTER 3 und 4

IP Adresszuordnung

Bei beiden Versionen muss einer Schnittstelle eines Routers oder Multilayer-Switches eine IP-Adresse zugewiesen werden, damit dieser Pakete weiterleiten kann.

- Eine Schnittstelle mit konfigurierter IP-Adresse und aktivem Status trägt das **zugehörige Netzwerk in die Routing-Tabelle (Routing Information Base [RIB]) des Routers ein**.
- Verbundene Netzwerke oder Routen haben eine **administrative Distanz (AD) von null**.
- **Es ist möglich, mehrere IPv4-Netzwerke an dieselbe Schnittstelle anzuschließen**, indem man mit dem Befehl **ip address ip-address subnet-mask secondary** eine sekundäre IPv4-Adresse an diese Schnittstelle anlegt.
- IPv6-Adressen werden mit dem Schnittstellenkonfigurationsbefehl **ipv6 address ipv6-address/prefix-length** zugewiesen.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface gi0/0/0
R1(config-if)# ip address 10.10.10.254 255.255
R1(config-if)# ip address 172.16.10.254 255.255.255.0 secondary
R1(config-if)# ipv6 address 2001:db8:10::254/64
R1(config-if)# ipv6 address 2001:DB8:10:172::254/64
R1(config-if)# interface gi0/0/1
R1(config-if)# ip address 10.20.20.254 255.255.255.0
R1(config-if)# ip address 172.16.20.254 255.255.255.0 secondary
R1(config-if)# ipv6 address 2001:db8:20::254/64
R1(config-if)# ipv6 address 2001:db8:20:172::254/64
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

27

NETZWERKTECHNIK / SEMESTER 3 und 4

Routed Subinterfaces

- Es ist möglich, die Schnittstelle eines Switches als Trunk-Port zu konfigurieren und logische Subinterfaces auf einem Router zu erstellen.
- Ein Subinterface wird erstellt, indem ein Punkt und ein numerischer Wert angehängt werden. Anschließend muss das VLAN mit dem Befehl **encapsulation dot1q vlan-id** dem Subinterface zugeordnet werden.

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config-if)# int g0/0/1.10
R2(config-subif)# encapsulation dot1Q 10
R2(config-subif)# ip address 10.10.10.2 255.255.255.0
R2(config-subif)# ipv6 address 2001:db8:10::2/64
R2(config-subif)# int g0/0/1.99
R2(config-subif)# encapsulation dot1Q 99
R2(config-subif)# ip address 10.20.20.2 255.255.255.0
R2(config-subif)# ipv6 address 2001:db8:20::2/64
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

28

NETZWERKTECHNIK / SEMESTER 3 und 4

Switched Virtual Interfaces

- Mit Catalyst-Switches lässt sich einer **virtuellen Switch-Schnittstelle (SVI), auch VLAN-Schnittstelle genannt**, eine IP zuweisen.
- Eine SVI wird konfiguriert, indem das VLAN auf dem Switch definiert und anschließend die VLAN-Schnittstelle mit dem Befehl **interface vlan vlan-id** festgelegt wird.
- Damit die SVI aktiv ist, muss dem Switch eine Schnittstelle zugeordnet sein, die dem entsprechenden VLAN zugeordnet und aktiv ist. Bei Multilayer-Switches können die SVIs zum Routing von Paketen zwischen VLANs verwendet werden, ohne dass ein externer Router erforderlich ist.

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface Vlan 10
SW1(config-if)# ip address 10.10.10.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:10::1/64
SW1(config-if)# no shutdown
SW1(config-if)# interface vlan 99
SW1(config-if)# ip address 10.99.99.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:99::1/64
SW1(config-if)# no shutdown
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Routed Switchport

- Manche Netzwerkdesigns beinhalten eine **Punkt-zu-Punkt-Verbindung zwischen Switches für das Routing**. Wenn beispielsweise ein Switch eine Verbindung zu einem Router herstellen muss, wird üblicherweise ein Transit-VLAN (z. B. VLAN 2001) eingerichtet, der Port, der mit dem Router verbunden ist, diesem VLAN zugeordnet und anschließend ein SVI für VLAN 2001 erstellt. Es besteht jedoch immer die Möglichkeit, dass VLAN 2001 an anderer Stelle im Layer-2-Bereich existiert oder dass Spanning Tree die Topologie beeinflusst.
- Alternativ kann der Multilayer-Switch-Port mithilfe des Befehls **no switchport** in der Schnittstellenkonfiguration von einem Layer-2-Switch-Port in einen gerouteten Switch-Port umgewandelt werden. Anschließend kann ihm eine IP-Adresse zugewiesen werden.

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int gi1/0/14
SW1(config-if)# no switchport
SW1(config-if)# ip address 10.20.20.1 255.255.255.0
SW1(config-if)# ipv6 address 2001:db8:20::1/64
SW1(config-if)# no shutdown
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Überprüfen der IP Adressen (IPv4)

- IPv4-Adressen können mit dem Befehl **show ip interface [brief | Schnittstellen-ID | VLAN VLAN-ID]** angezeigt werden.
- Die Ausgabe dieses Befehls enthält: MTU, DHCP-Relay, ACLs und die primäre IP-Adresse.
- Das optionale Schlüsselwort `brief` zeigt die Ausgabe in komprimierter Form an.

```
SW1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES manual up                    up
Vlan10                 10.10.10.1      YES manual up                    up
Vlan99                 10.99.99.1      YES manual up                    up
GigabitEthernet0/0     unassigned      YES unset  down                  down
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   unassigned      YES unset  up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
```

```
SW1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 10.10.10.1      YES manual up                    up
Vlan99                 10.99.99.1      YES manual up                    up
GigabitEthernet1/0/14  10.20.20.1      YES manual up                    up
GigabitEthernet1/0/23  192.168.1.1     YES manual down                  down
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Überprüfen der IP Adressen (IPv6)

- Die gleichen Informationen lassen sich für IPv6-Adressen mit dem Befehl **show ipv6 interface [brief | interface-id | vlan vlan-id]** anzeigen.
- Genau wie bei IPv4-Adressen kann ein CLI-Parser verwendet werden, um die Informationen auf das Relevante zu reduzieren.

```
SW1# show ipv6 interface brief
! Output omitted for brevity
Vlan1                  [up/up]
    FE80::262:ECFF:FE9D:C547
    2001:1::1
Vlan10                 [up/up]
    FE80::262:ECFF:FE9D:C546
    2001:DB8:10::1
Vlan99                 [up/up]
    FE80::262:ECFF:FE9D:C55D
    2001:DB8:99::1
GigabitEthernet0/0     [down/down]
    unassigned
GigabitEthernet1/0/1   [down/down]
    unassigned
GigabitEthernet1/0/2   [up/up]
    unassigned
GigabitEthernet1/0/3   [up/up]
    unassigned
GigabitEthernet1/0/4   [down/down]
    unassigned
GigabitEthernet1/0/5   [down/down]
    Unassigned
```

```
SW1# show ipv6 interface brief | exclude unassigned|GigabitEthernet
Vlan1                  [up/up]
    FE80::262:ECFF:FE9D:C547
    2001:1::1
Vlan10                 [up/up]
    FE80::262:ECFF:FE9D:C546
    2001:DB8:10::1
Vlan99                 [up/up]
    FE80::262:ECFF:FE9D:C55D
    2001:DB8:99::1
```

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

02

Forwarding Architekturen

Layer 2 vs. Layer 3 Switching

- Switch within VLANs.
- Filter traffic based on layer 2

Layer 2 Switch

- Switch within VLANs.
- Route between VLANs.
- Filter traffic based on layer 2 or 3.

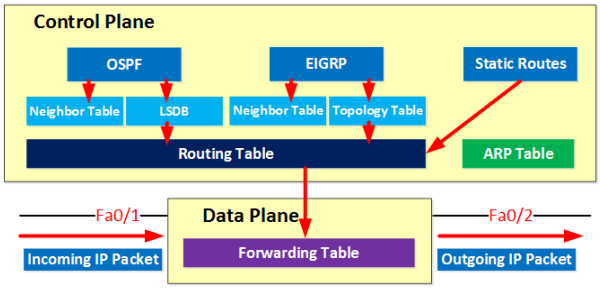
Multilayer switch

tgm [Quelle: https://networklessons.com/switching/cef-cisco-express-forwarding - letzter Abruf 12.2.2026]

NETZWERKTECHNIK / SEMESTER 3 und 4

Multilayer Switches – Seperation of Duties

- Bei Multilayer-Switches gibt es eine **Aufgabentrennung**.
- Wir müssen eine Tabelle für die MAC-Adressen erstellen, eine Routing-Tabelle füllen, ARP-Anfragen bearbeiten, prüfen, ob ein IP-Paket mit einer Zugriffsliste übereinstimmt usw. und unsere IP-Pakete weiterleiten.
- Diese Aufgaben sind auf die **Steuerungsebene (Control Plane, CSI) und die Datenebene (Data Plane, DP)** aufgeteilt.
- Ein **Beispiel**:
  - Die Steuerungsebene ist für den Austausch von Routing-Informationen mithilfe von Routing-Protokollen und den Aufbau einer Routing- und einer ARP-Tabelle zuständig.
  - Die Datenebene ist für die eigentliche Weiterleitung der IP-Pakete verantwortlich.

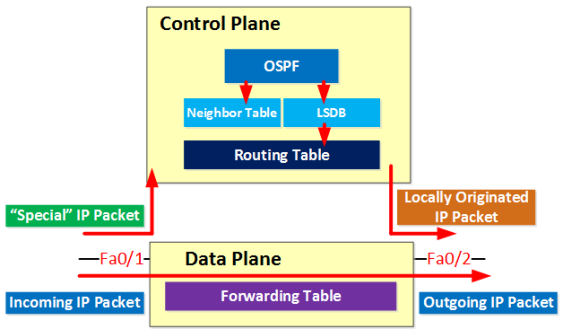


[Quelle: https://networklessons.com/switching/cef-cisco-express-forwarding - letzter Abruf 12.2.2026]

NETZWERKTECHNIK / SEMESTER 3 und 4

Multilayer Switches – Seperation of Duties

- Die **meisten IP-Pakete können von der Datenebene** weitergeleitet werden.
- Es gibt jedoch einige „**spezielle" IP-Pakete**, die nicht direkt von der Datenebene weitergeleitet werden können und **daher an die Steuerungsebene gesendet werden**.
  - IP-Pakete, die für eine der IP-Adressen des Multilayer-Switches bestimmt sind.
  - Routing-Protokolldatenverkehr wie OSPF, EIGRP oder BGP.
  - IP-Pakete, bei denen bestimmte Optionen im IP-Header gesetzt sind.
  - IP-Pakete mit abgelaufener TTL (Time-to-Live).



[Quelle: https://networklessons.com/switching/cef-cisco-express-forwarding - letzter Abruf 12.2.2026]

NETZWERKTECHNIK / SEMESTER 3 und 4

Weiterleitungsverfahren (Switching Paths) in Routern, mit denen Pakete von einem Eingangs- an einen Ausgangsport übergeben werden

Process Switching (Prozessumschaltung) - Dies ist die älteste und langsamste Methode.

- **Funktionsweise: Jedes einzelne Paket wird von der Haupt-CPU (Route Processor) analysiert.** Die CPU schlägt in der Routing-Tabelle (RIB) nach, bestimmt den nächsten Hop (ARP-Tabelle) und schreibt den MAC-Header um.
- **Nachteil: Hohe CPU-Last, sehr langsam**, da keine Informationen zwischengespeichert werden.
- **Einsatz: Wird heute nur noch verwendet, wenn CEF oder Fast Switching nicht unterstützt werden** oder für spezifische Pakete, die an den Router selbst gerichtet sind ("Punted Packets").

Fast Switching (Schnellumschaltung) - Ein "cache-basiertes" Verfahren, das schneller als Process Switching ist.

- **Funktionsweise: Das erste Paket eines Datenstroms (Flow) wird via Process Switching verarbeitet.** Das Ergebnis dieser Entscheidung (Ausgangsinterface, MAC-Header) wird im "Fast Switch Cache" gespeichert. Alle folgenden Pakete für dasselbe Ziel werden direkt aus diesem Cache weitergeleitet, ohne die CPU erneut zu belasten.
- **Nachteil: Der Cache wird "reaktiv" aufgebaut** (erst wenn Daten fließen). Cache-Einträge müssen regelmäßig gelöscht werden (Aging), was die CPU belastet. Es ist "per-destination" (zielbasiert), nicht "per-packet".
- **Einsatz: Veraltet**, bei modernen IOS-Versionen oft durch CEF ersetzt.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

37

NETZWERKTECHNIK / SEMESTER 3 und 4

Weiterleitungsverfahren (Switching Paths) in Routern, mit denen Pakete von einem Eingangs- an einen Ausgangsport übergeben werden

Cisco Express Forwarding (CEF) - Die modernste, effizienteste und standardmäßige Methode auf aktuellen Cisco-Geräten.

- **Funktionsweise: CEF ist "proaktiv". Es wartet nicht auf den ersten Paketfluss**, sondern erstellt Tabellen basierend auf der Routing-Tabelle (RIB) und der ARP-Tabelle im Voraus.
  - FIB (Forwarding Information Base): Spiegelt die Routing-Tabelle, optimiert für Hardware-Suche.
  - Adjacency Table: Enthält die Layer-2-Informationen (MAC-Adressen) für die nächsten Hops.
- **Vorteil: Extrem schnell** (Hardware-basiert/ASIC), kaum CPU-Last, unterstützt "per-packet" Load Balancing.
- **dCEF (Distributed CEF): Bei High-End-Routern wird die FIB/Adjacency-Tabelle auf die Linecards heruntergeladen**, sodass die zentrale CPU gar nicht mehr am Switching beteiligt ist.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

38

NETZWERKTECHNIK / SEMESTER 3 und 4

Process Switching

- Prozessvermittlung, auch **Software-Vermittlung** oder langsamer Pfad genannt, ist ein Vermittlungsmechanismus, bei dem die Allzweck-CPU eines Routers für die Paketvermittlung zuständig ist.
- **Folgende Pakettypen erfordern Softwareverarbeitung**:
  - Pakete, die vom Router gesendet oder an ihn adressiert sind (mittels Kontrollverkehr oder Routing-Protokollen),
  - Pakete, die für die Hardware zu komplex sind (IP-Pakete mit IP-Optionen),
  - Pakete, die zusätzliche, aktuell unbekannte Informationen erfordern (z. B. ARP).
- Software-Vermittlung ist **deutlich langsamer als Hardware-Vermittlung**.
- Der NetIO-Prozess ist darauf ausgelegt, **nur einen sehr geringen Anteil des Systemverkehrs zu verarbeiten**. **Pakete werden, wann immer möglich, per Hardware vermittelt.**

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

39

NETZWERKTECHNIK / SEMESTER 3 und 4

Process Switching

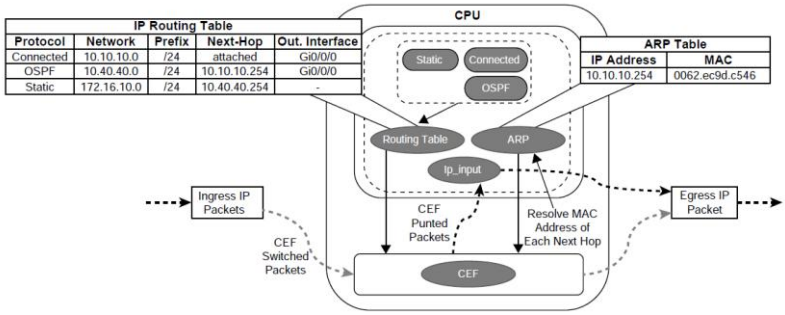
- **Früher Mechanismus (späte 80er):** Router-CPU verarbeitet **jedes Paket vollständig einzeln** („per-packet processing“).
- **Ablauf**: Für jedes Paket wurde die komplette Forwarding-Prozedur erneut durchlaufen (Routing-Lookup, ARP-Lookup, Frame-Rewrite etc.).
- **Hauptproblem**: Zwei zeitintensive Schritte dominierten:
  - Suchen der Route und des Next Hops im Routing-Table (inkl. rekursiver Lookups)
  - Auflösen der Layer-3-zu-Layer-2-Adresse (z. B. ARP)
- **Frame Rewrite**: Beim Weiterleiten muss der Data-Link-Header neu aufgebaut werden → einer der rechenintensivsten Schritte.
- Limitierungen:
  - Hoher CPU-Aufwand durch vollständige Einzelverarbeitung
  - Wachsende Netzlast machte Process Switching zunehmend ineffizient
  - Router wurden zum **Flaschenhals**
- **Ergebnis**: Der Bedarf nach höherer Performance führte zur Entwicklung von **Fast Switching.**

tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

40

Process Switching

- Die Routingtabelle, auch Routing Information Base (RIB) genannt, wird aus Informationen dynamischer Routingprotokolle sowie direkt verbundenen und statischen Routen erstellt.
- Die ARP-Tabelle basiert auf Informationen des ARP-Protokolls.



[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Fast Switching

- **Caching-Prinzip:** Erste Anfrage wird vollständig verarbeitet, Ergebnisse (Route, Next Hop, Layer-2-Header) werden im Cache abgelegt.
- **„Route once, switch many“:** Nur das erste Paket wird process-switched, alle folgenden nutzen die gespeicherten Cache-Informationen → deutlich schneller.
- **Cache-Inhalt:**
  - Ziel-IP
  - Next-Hop-Adresse
  - vollständiger Layer-2-Frame-Header
- **Vorteile**: Schnellere Weiterleitung, weniger CPU-Belastung.
- **Nachteile**:
  - Hohe Last auf Routing-Änderungen → Cache-Einträge müssen gelöscht werden
  - Bei Traffic-Bursts zu neuen Zielen fällt Router auf langsames Process Switching zurück
  - Eingeschränkte Lastverteilung (nur Interface der ersten Lookup-Entscheidung wird genutzt)
- **Fazit**: Große Verbesserung gegenüber Process Switching – aber mit wachsenden Netzwerken unzureichend → führte ab 1996 zur Entwicklung moderner Verfahren (z. B. CEF).

[Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

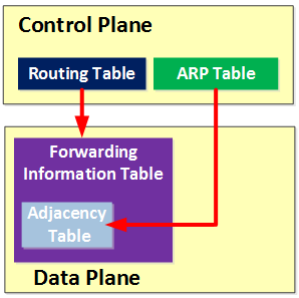
Warum Fast Switching nicht ausreichte

- **Caching steigert Performance**, aber: Das Erstellen eines Cache-Eintrags **bleibt CPU-intensiv**.
- **Fast Switching Limitierung**: Auch wenn spätere Pakete schnell weitergeleitet werden, ist das Erstellen des ersten Cache-Eintrags rechenaufwendig.
- **Leistungshürde**: Um Software-Router weiter zu beschleunigen und die Implementierung in Hardware zu erleichtern, musste der gesamte Forwarding-Ablauf neu gedacht werden.
- **Komplexeste Schritte des Packet Forwarding**:
  - **Best Path Selection**: Routing-Lookup + Bestimmung der ausgehenden Schnittstelle
  - **Frame Rewrite**: Neuer Aufbau des Data-Link-Headers – einer der teuersten Schritte
- Fazit: Die Engpässe in Routing-Lookup und Frame Rewrite zeigten klar, dass reine Cache-Optimierung nicht ausreicht → der Weg zu **CEF** (Cisco Express Forwarding) wurde notwendig.

tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

CEF (Express Forwarding)

- Cisco Express Forwarding (CEF) ist ein **proprietärer Switching-Mechanismus von Cisco**. Er ist der Standard-Switching-Mechanismus aller Cisco-Plattformen, die **spezialisierte anwendungsspezifische integrierte Schaltungen (ASICs) und Netzwerkprozessoren (NPUs) für hohen Paketdurchsatz (hardwarebasierte Router) verwenden**.
- Der **ternäre inhaltsadressierbare Speicher (TCAM)** eines Switches ermöglicht den Abgleich und die Auswertung eines Pakets anhand mehrerer Felder.
- Die TCAM-Einträge werden im **VMR-Format (Value, Mask, Result)** gespeichert.
  - Der Wert gibt die zu durchsuchenden Felder an, z. B. IP-Adresse und Protokoll.
  - Die Maske gibt das relevante Feld an, das abgefragt werden soll.
  - Das Ergebnis gibt die Aktion an, die bei einer Übereinstimmung von Wert und Maske ausgeführt werden soll.
- **TCAM arbeitet in Hardware** und bietet dadurch eine schnellere Verarbeitung und Skalierbarkeit als prozessbasiertes Switching.



tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Von Process Switching zur FIB (Forwarding Information Base)

Problem im Process Switching:

- Jeder Paket-Forwarding-Vorgang durchläuft komplett die Routing-Tabelle (RIB).
- Nutzung **Longest Prefix Match** → lineare Suche von /32 bis /0.
- Rekursion notwendig: Viele Routen enthalten nur Next Hop → erneute RIB-Lookups.
- RIB gibt **keine Frame-Rewrite-Infos** aus → ARP/L2-Lookup zusätzlich notwendig.
- Ergebnis: Viele Iterationen, hoher CPU-Aufwand, wiederholt für jedes Paket.

Ineffizienz des RIB-Lookups:

- Linear, potenziell mehrere hunderttausend Einträge.
- Worst Case: Erst die Default Route am Ende passt.
- Routing-Tabellen sind zum **Speichern**, **nicht zum schnellen Suchen** gemacht.

Lösungsidee -Optimierte Lookup-Struktur:

- Keine linearen Suchvorgänge mehr.
- Keine Rekursion zu Next-Hop-Routen.
- **Lookup muss einmalig, direkt, ohne weitere Tabellen, ohne Iteration erfolgen.**

Die **Forwarding Information Base (FIB):**

- Wird automatisch aus der RIB erzeugt.
- Alle Routen werden rekursiv vollständig aufgelöst (bis zur direkt angeschlossenen Next-Hop-Schnittstelle).
- **Ergebnis: Eine einzige Lookup-Operation liefert: Zielpräfix, Next Hop, Outgoing Interface, Frame-Rewrite-Information**

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

NETZWERKTECHNIK / SEMESTER 3 und 4

Verwendung von "Bäumen" für Routing und Prefix Lookup

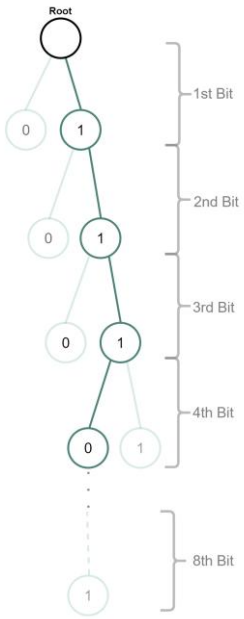
Ziel im Routing: Für jede eingehende Ziel-IP → längstes übereinstimmendes Präfix finden („Longest Prefix Match").

„Baum" als Lösung (FIB-Struktur):

- **Jeder Bit des Präfixes = eine Ebene im Baum**
- IPv4: max. 32 Ebenen (bzw. 33 inkl. Root)
- Lookup folgt den Bits der Ziel-IP Schritt für Schritt
- Aufwand: maximal 32 Vergleiche, egal wie viele Präfixe gespeichert sind

Beispiel:

- Ziel-IP beginnt mit 11100001 (dezimal: 225) → Baum verfolgt Bitfolge
- Vollständiger 8-Bit-Match → exakte Route
- Kürzerer Match, z. B. 1110xxxx → längstes existierendes Präfix wird gewählt



tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

NETZWERKTECHNIK / SEMESTER 3 und 4

Adjacency Table

Router kennen oft **tausende bis hunderttausende Ziele, aber nur wenige direkte Nachbarn**.

Viele FIB-Einträge nutzen deshalb **dieselben** Weiterleitungsinformationen.

Merksatz: FIB wählt den Weg – die Adjacency sagt, wie der Frame gebaut wird.

Grundidee:

- Statt für jedes Ziel die Frame-Rewrite-Information neu zu berechnen oder pro Ziel zu cachen, erstellt der Router die notwendigen Weiterleitungsdaten **einmal pro Nachbar**.

Vorgehen des Routers:

- RIB kennt alle Next-Hop-IP-Adressen
- Layer-3-zu-Layer-2-Zuordnung (z. B. ARP, ND) wird vorab durchgeführt
- Aus diesen Informationen wird eine komplette Weiterleitungsstruktur erzeugt
- Diese landet in einer eigenen Datenbank: der Adjacency-Tabelle

Inhalt einer Adjacency:

- Ausgangsinterface zum Next Hop
- Vollständiger, vorgefertigter Layer-2-Header (Frame Rewrite)
- Optional: zusätzliche Verwaltungsinformationen

tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

47

NETZWERKTECHNIK / SEMESTER 3 und 4

Beispiel mit Subinterfaces in der Adjacency Table

Die oben ausgegebenen Informationen entsprechen vollständigen, vorkonfigurierten Datenverbindungsschichtinformationen, die vom Router sofort verwendet werden können.

```
R3#show adjacency detail
Protocol Interface Address
<omitted for brevity>
...
IP Ethernet2/3.100 192.168.23.2(7)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 0
Encap length 18
CA022904003BCA0320A4003B810000640800
ARP
```

CA022904003B - Destination MAC address - R2 Ethernet 2/3's MAC address

CA0320A4003B - Source MAC address - R3 Ethernet 2/3's MAC address

8100 - Ethertype of the 802.1Q header

0 - Class of Service (0) and Discard Eligibility Indicator (0)

064 - VLAN Tag - 100 (064 in Hex = 100 in decimal)

0800 - Ethertype of the original L2 header

tgm [Quelle: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKKGEA4/demystifying-cef - letzter Abruf 12.2.2026]

48

Zusammenfassung

Adjacency Table – Grundprinzip:

- Enthält genau die Informationen, die der Router zum Weiterleiten eines Pakets benötigt: Ausgangsinterface, vollständiger vorgefertigter Layer-2-Header (Frame Rewrite)
- Für untagged, tagged oder spezielle Interfaces (z. B. Tunnel) werden jeweils passende Adjacency-Einträge erzeugt

CEF besteht aus zwei zentralen Bausteinen:

FIB = Wo geht das Paket hin?

Adjacency Table = Wie wird es weitergeleitet?

Arbeitsweise von CEF:

- **FIB**: Enthält alle IP-Präfixe aus der RIB, optimiert für extrem schnelle Lookups (**Software: Trie-Struktur; Hardware: TCAM**).
- **FIB-Lookup**: Ziel-IP → FIB liefert direkten Pointer zur passenden Adjacency.
- **Adjacency**: Liefert sofort nutzbare Weiterleitungsdaten (Interface + Frame-Rewrite)→ Paket kann sofort gesendet werden – ohne Rekursion, ohne ARP-Lookup, ohne erneutes Frame-Rewrite.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

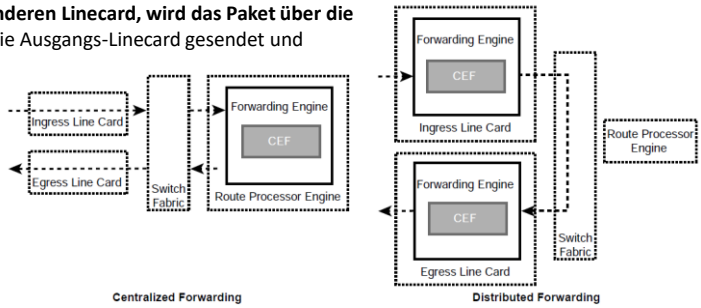
Zentralisiertes und verteiltes Forwarding

- Wenn ein **Routenprozessor (RP) mit einer Weiterleitungs-Engine ausgestattet ist**, die alle Paketvermittlungsentscheidungen trifft, spricht man von einer **zentralisierten Weiterleitungsarchitektur**.
  - Bei einer zentralisierten Weiterleitungsarchitektur wird ein auf der Eingangsleitungskarte empfangenes Paket an die Weiterleitungs-Engine des RP weitergeleitet. Diese prüft die Paket-Header, bestimmt, dass das Paket über einen Port der Ausgangsleitungskarte gesendet werden soll, und leitet es zur Weiterleitung an diese weiter.
- Sind die **Leitungskarten hingegen mit Weiterleitungs-Engines ausgestattet**, die Paketvermittlungsentscheidungen ohne Eingriff des RP treffen, spricht man von einer **verteilten Weiterleitungsarchitektur**.

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Zentralisiertes und verteiltes Forwarding

- In einer verteilten Weiterleitungsarchitektur wird ein **auf der Eingangs-Linecard empfangenes Paket an die lokale Weiterleitungs-Engine weitergeleitet**.
- Die Weiterleitungs-Engine führt eine Paket-Lookup durch und leitet das Paket über eine **lokale Schnittstelle weiter**, falls die Ausgangsschnittstelle lokal ist.
- Befindet sich die **Ausgangsschnittstelle auf einer anderen Linecard, wird das Paket über die Switch-Fabric** (auch Backplane genannt) direkt an die Ausgangs-Linecard gesendet und umgeht dabei den RP (Remote Point).



[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Software CEF

Die **Software CEF (auch bekannt als Software Forwarding Information Base)** besteht aus folgenden Komponenten:

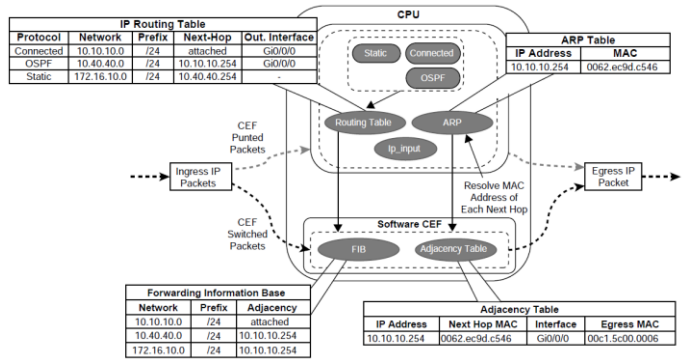
- **Forwarding Information Base (FIB)** – Die FIB wird direkt aus der Routing-Tabelle erstellt und enthält die Next-Hop-IP-Adresse für jedes Ziel im Netzwerk. Sie bildet die Weiterleitungsinformationen der IP-Routing-Tabelle ab. Bei einer Routing- oder Topologieänderung im Netzwerk wird die IP-Routing-Tabelle aktualisiert, und diese Änderungen werden in der FIB abgebildet. CEF verwendet die FIB für IP-Zielpräfix-basierte Switching-Entscheidungen.
- **Adjacency Tabelle** – Die Adjacency Tabelle, auch bekannt als **Adjacency Information Base (AIB)**, enthält die direkt verbundenen Next-Hop-IP-Adressen und die zugehörigen Next-Hop-MAC-Adressen sowie die MAC-Adresse der Ausgangsschnittstelle. Die Adjazenztabelle wird mit Daten aus der ARP-Tabelle oder anderen Layer-2-Protokolltabellen gefüllt.

[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Software CEF

Beim Empfang eines IP-Pakets wird die FIB auf einen gültigen Eintrag geprüft.

- **Fehlt ein Eintrag**, handelt es sich um eine „abgeleitete“ Adjacency in CEF. Das bedeutet, dass das Paket an die **CPU weitergeleitet** werden muss, da CEF es nicht verarbeiten kann.
- **Gültige FIB-Einträge werden weiterverarbeitet**, indem die Adjacency Tabelle für die Ziel-IP-Adresse jedes Pakets geprüft wird.
- **Fehlende Adjacency Einträge rufen den ARP-Prozess auf.** Nach erfolgreicher ARP-Auflösung kann der vollständige CEF-Eintrag erstellt werden.



[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

Hardware CEF

- **ASICs** ermöglichen zwar sehr hohe Paketraten, ihre Funktionalität ist jedoch eingeschränkt, da sie **fest auf bestimmte Aufgaben ausgelegt sind**. Router verfügen über NPUs, die die mangelnde Flexibilität von ASICs überwinden sollen.
- **NPUs sind programmierbar** und ihre Firmware lässt sich leicht austauschen.
- Die Paketvermittlung in verteilten Architekturen erfolgt über **Distributed CEF (dCEF)**.
- dCEF ist ein Mechanismus, bei dem die CEF-Datenstrukturen **auf die weiterleitenden ASICs und die CPUs aller Linecards heruntergeladen werden**, sodass diese an der Paketvermittlung teilnehmen können. Dadurch findet die Vermittlung auf verteilter Ebene statt, was den Paketdurchsatz des Routers erhöht.

Hinweis:

- Eine **NPU (Network Processing Unit)** ist ein spezialisierter Prozessor, der für das Hochgeschwindigkeits-Verarbeiten von Netzwerkverkehr entwickelt wurde.
- Ein **ASIC (Application Specific Integrated Circuit)** ist ein speziell entwickelter Chip, der für eine ganz bestimmte Aufgabe optimiert ist

[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

03

Zusammenfassung

55

Schlüsselbegriffe

Key Terms	
Access port	Forwarding Information Base (FIB)
Address Resolution Protocol (ARP)	MAC address table
Broadcast Domain	native VLAN
Cisco Express Forwarding (CEF)	process switching
collision domain	Routing Information Base (RIB)
content addressable memory (CAM)	trunk port
Layer 2 forwarding	ternary content addressable memory (TCAM)
Layer 3 forwarding	virtual LAN (VLAN)

[Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]

56

Kommandoreferenz

Task	Command Syntax
Define a VLAN	**vlan** vlan-id **name** vlanname
Configure and interface as a trunk port	**switchport mode trunk**
Configure an interface as an access port assigned to a specific VLAN	**switchport mode access** **switchport access** {**vlan** vlan-id | **name** name}
Configure a static MAC address entry	**mac address-table static mac-address vlan** vlan-id **interface** interface-id
Clear MAC addresses from the MAC address table	**clear mac address-table dynamic [{address** mac-address | **interface** interface-id | **vlan** vlan-id}]

Kommandoreferenz

Task	Command Syntax
Assign an IPv4 address to an interface	**ip address** ip-address subnet-mask
Assign a secondary IPv4 address to an interface	**ip address** ip-address subnet-mask **secondary**
Assign an IPv6 address to an interface	**ipv6 address** ipv6-address/prefix-length
Modify the SDM database	**sdm prefer {vlan | advanced}**
Display the interfaces that are configured as a trunk port and all the VLANs that they permit	**show interfaces trunk**

Kommandoreferenz

Task	Command Syntax
Display the list of VLANs and their associated ports	**show vlan [{brief | id** vlan-id | name vlanname | **summary}]**
Display the MAC address table for a switch	**show mac address-table [address** mac-address | **dynamic | vlan** vlan-id]
Display the current interface state, including duplex, speed, and link state	**show interfaces**
Display the Layer 2 configuration information for a specific switchport	**show interfaces** interface-id **switchport**
Display the ARP table	**show ip arp** [mac-address | ip-address **| vlan** vlan-id | interface-id].
Displays the IP interface table	**show ip interface [brief** | interface-id | **vlan** vlan-id]
Display the IPv6 interface table	**show ipv6 interface [brief** | interface-id | **vlan** vlan-id]

tgm [Quelle: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition, Ciscopress]