Teil 1 – Wissenschaftlich-detaillierte Zusammenfassung der Vorlesung *MPLS I & II*

1. Einführung und Kontext

Die Unterrichtseinheit führt in die Grundlagen, Architektur und Designphilosophie von **Multiprotocol Label Switching (MPLS)** ein – eine Schlüsseltechnologie moderner Weitverkehrs- und Provider-Netze. Der Professor beschreibt MPLS als eine **Zwischenschicht zwischen Layer 2 (Ethernet)** und **Layer 3 (IP)** – also als *„Layer 2.5“* –, die sowohl Switching- als auch Routing-Eigenschaften kombiniert.

Das Ziel von MPLS ist die **effiziente Weiterleitung von Datenströmen** (Traffic Engineering) bei gleichzeitiger **Skalierbarkeit, Redundanz und Quality of Service (QoS)**. MPLS wird damit zum Fundament vieler moderner Konzepte, etwa von **SD-WAN**, **L3VPNs**, und **Carrier-Backbones**.

---

2. Historischer und ökonomischer Hintergrund

2.1 Vom Mainframe zur Cloud und zurück

Der Professor zeichnet einen historischen Bogen: In den 1960ern dominierten **zentralisierte Mainframe-Systeme**; Benutzer arbeiteten über „dumme Terminals“. In den 1990ern erfolgte die **Dezentralisierung** durch Arbeitsplatz-PCs und verteilte Systeme. Damit stieg die Notwendigkeit, Standorte effizient zu verbinden.

Heute pendelt die Industrie wieder zurück zu **zentralisierten Rechenzentren (Cloud)** – allerdings unter neuen Begriffen. MPLS bildet das Rückgrat dieser modernen „Mainframes“. Nach großen Cloud-Ausfällen (z. B. Apple-Zutrittskontrolle, Voestalpine-Hochofen) vollzieht sich erneut eine Bewegung **zurück zu On-Prem-IT**, um Kontrolle, Datenschutz und Ausfallsicherheit zu gewährleisten.

> „Cloud ist gut, aber On-Prem ist besser – weil On-Prem kontrolliere ich selbst.“

---

3. MPLS als Overlay und Netzwerklogik

MPLS ist ein **Overlay-Netzwerk**, das sich über ein bestehendes **Ethernet-Underlay** legt. Innerhalb dieses Overlays werden **Labels** anstelle von IP-Adressen zur Weiterleitung verwendet. MPLS-Knoten bilden so ein logisches, durch Labels identifiziertes **Virtual Circuit Network**.

> „Man kann sich MPLS vorstellen wie einen gigantischen Switch – jedes Interface ist ein Port dieses logischen Switches."

Innerhalb der MPLS-Domäne erfolgt die Weiterleitung *label-basiert* (Switching), während außerhalb wieder klassisches IP-Routing gilt.

---

4. Netzwerktopologien und Marktentwicklung

- Früher: *Hub-and-Spoke*-Architekturen (Frame Relay).
- Heute: **Full-Mesh-MPLS-Backbones** mit dynamischem Traffic Engineering.
- Provider verlieren zunehmend Kunden, weil Firmen nicht mehr nur Internet-Connectivity, sondern **MPLS-Connectivity** wünschen.

Beispiel:

> Microsoft errichtet derzeit drei Rechenzentren in Österreich (Münchendorf, Heidenreichstein, Litz). Diese werden an das eigene Microsoft-MPLS-Backbone angebunden, um Kunden direkten Zugang zum globalen Cloud-Core zu ermöglichen.

---

5. Grundkomponenten einer MPLS-Domäne

Begriff	Bedeutung
Label Switching Router (LSR)	Router im MPLS-Core, der auf Basis von Labels weiterleitet
Provider Edge (PE)	Eintrittspunkt des Kundenverkehrs in die MPLS-Domäne
Customer Edge (CE)	Kundenseitiger Router, spricht i. d. R. kein MPLS
Ingress Router	Erster MPLS-fähiger Router einer Verbindung
Egress Router	Letzter MPLS-fähiger Router einer Verbindung
Label	20-Bit-Feld zur Identifikation einer Forwarding Equivalence Class
MPLS Domain / Autonomous System	Logischer Verwaltungsbereich, meist deckungsgleich mit einem AS

---

6. Funktionsprinzip und Label-Switching

6.1 Label-Mechanismus

Ein MPLS-Label ist eine kurze Kennung, die vom Ingress-Router vergeben und entlang des Pfades durch Label-Swapping ersetzt wird. Ein Router, der ein Paket

erhält, **liest nicht den IP-Header**, sondern **das Label**, sucht die passende Eintragung in der **Label Forwarding Information Base (LFIB)**, tauscht das Label aus und leitet weiter.

Dieser Mechanismus reduziert die Komplexität der Layer-3-Analyse und steigert die Performance erheblich.

---

7. Forwarding Equivalence Class (FEC)

Alle Pakete, die denselben **Pfad und dieselben Weiterleitungsparameter** teilen, gehören zur gleichen *Forwarding Equivalence Class*. Damit genügt es, einmal den optimalen Pfad zu berechnen; danach werden alle zugehörigen Pakete gleich behandelt.

> „Ein Router hat 20 Interfaces – also auch nur 20 Forwarding Equivalence Classes. Alles andere ist Overhead."

FECs ermöglichen die Implementierung von **Traffic Engineering**, **QoS** und **VPN-Segmentierung**.

---

8. Label Stacking und Traffic Engineering

Labels können gestapelt werden (*Label Stacking*), um **mehrere Routing-Entscheidungen im Voraus** zu kodieren. Beispielsweise kann der Ingress-Router die gesamte Pfadfolge definieren – die Zwischenrouter müssen dann nur noch den Stack abarbeiten.

Vorteil: deterministische Pfade; Nachteil: statische Konfiguration, geringe Flexibilität.

Daher wird in der Praxis meist **Label Distribution Protocol (LDP)** für dynamisches Label-Mapping eingesetzt.

---

9. Label Distribution und Routing-Integration

MPLS selbst berechnet keine Routen; es **baut auf einem bestehenden IGP** (z. B. OSPF oder Enhanced EIGRP) auf. Das Label Distribution Protocol tauscht Labels zwischen Nachbarn aus, basierend auf den IGP-Tabellen. So entsteht eine **Label-Information Base (LIB)**, aus der die **LFIB** generiert wird.

Beispielhafte Integration:

- OSPF / EIGRP bestimmen die Topologie,
- LDP vergibt und verteilt Labels entlang dieser Pfade.

Wichtig: *Split Horizon* muss beachtet werden, um doppelte Labels und Routing-Loops zu vermeiden.

---

10. Ingress, Egress und Penultimate Hop Popping (PHP)

Das **Penultimate Hop Popping** ist eine Effizienzoptimierung: Der **vorletzte Router** (Penultimate Hop) entfernt das MPLS-Label, bevor das Paket den Egress-Router erreicht. Da der Egress ohnehin nur ein mögliches Ziel hat (den Kunden-CE), wird das letzte Label nicht mehr benötigt.

> Typische Prüfungsfrage: *„Was bedeutet Penultimate Hop Popping und warum wird es eingesetzt?“*

---

11. Enhanced IGRP und Metriken

Der Professor weist auf die **„Renaissance von Enhanced IGRP“** hin, da es – anders als OSPF – **Leitungsqualität, Auslastung und Latenz** als Metriken berücksichtigt. Dies ermöglicht dynamische Pfadwahl auf Basis von *load, reliability, delay, bandwidth, MTU* (K1–K5).

Aktuelle Tendenz: Microsoft und andere Provider migrieren Backbones von OSPF auf EIGRP. Cisco integriert EIGRP daher wieder in den CCNA-Lehrplan.

---

12. Control Plane und Data Plane

Die Unterscheidung ist zentral:

Ebene	Funktion
Control Plane	Routing-, LDP-, Management- und Protokollverarbeitung
Data Plane	Tatsächliche Weiterleitung der Pakete auf Basis der LFIB

MPLS verschiebt die Belastung von der Control Plane zur Data Plane – insbesondere durch **Cisco Express Forwarding (CEF)**, das Paketinformationen cached und so mehrfaches Routing-Lookup vermeidet.

> „Wir wollen, dass die Data Plane arbeitet, während die Control Plane schläft.“

---

13. Device Architecture und SDN-Bezug

Ein moderner Enterprise-Router besteht aus:

- **Routing Table** – aus IGP/BGP berechnet
- **Forwarding Information Base (FIB)** – Kopie der Routing Table
- **Label Information Base (LIB)** – aus LDP
- **Label Forwarding Information Base (LFIB)** – Kombination aus FIB + LIB

Diese Trennung bildet die Grundlage für **Software-Defined Networking (SDN)**: Die Control Plane kann zentralisiert werden, während die Data Plane lokal weiterleitet.

Beispiel: *Nexus*-Switches mit verteilten *FEX*-Einheiten – dieselbe Logik im Campus- und WAN-Bereich.

---

14. Sicherheitsaspekte und Fehlerfälle

MPLS-Labels sind **nicht verschlüsselt**. Angriffe auf LDP oder Label-Manipulationen können ganze Backbones lahmlegen. Der Professor schildert reale Vorfälle (u. a. in Norddeutschland): Fehlkonfigurierte oder kompromittierte Router initiierten falsche Routen – das Backbone kollabierte vollständig.

Fehlerquelle oft: Techniker verwenden vorkonfigurierte Router aus Hot-Spare-Lagern (z. B. Cancom, A1), ohne sie zurückzusetzen. Folge: Routing-Konflikte, 6000 Kunden offline.

> „Wenn du einen Router tauschst, nimm nie den aus dem Regal, ohne ihn zu wipen. Sonst wipest du dein Netz."

---

15. Zusammenfassung und Ausblick

MPLS steht für:

- **Effizienz** (Label statt Lookup),
- **Skalierbarkeit** (Traffic Engineering, QoS),
- **Flexibilität** (LDP, VPN-Overlays),
- **Verwundbarkeit** (Label-Manipulation).

Zukünftige Entwicklungen:

- **Optische MPLS-Switches** (Label bleibt unverändert durch den Switch),
- **SD-WAN-Integration** (z. B. Fortinet SD-WAN, Cisco MPLS Overlay),
- **Hybrid-Architekturen** mit zentralisierter Control Plane.

> „MPLS ist kein Protokoll – es ist eine Philosophie. Und die heißt Effizienz."