Teil 1 – Wissenschaftlich-detaillierte Zusammenfassung der Vorlesung *MPLS III & BGP*

1. Einleitung und thematischer Rahmen

Die Unterrichtseinheit widmet sich der **Verknüpfung von MPLS und BGP** im Rahmen moderner Provider- und Backbone-Netzwerke. Aufbauend auf den vorherigen Modulen (DMVPN, OSPF, MPLS-2) zeigt der Professor die **Rolle von BGP als Policy-Engine im MPLS-Backbone**, und erläutert, wie Pfadwahl, Filterung, Compliance und internationale Routingpolitik ineinandergreifen.

Während MPLS die **technische Ebene der Paketweiterleitung (Data Plane)** bereitstellt, stellt BGP die **politisch und wirtschaftlich gesteuerte Control Plane** dar. Es geht also nicht mehr nur um technische Effizienz, sondern um gezielte Pfadsteuerung, Priorisierung und Filterung von Traffic zwischen autonomen Systemen (AS).

---

2. Rückblick und Ausgangspunkt

Der Unterricht beginnt mit dem Hinweis, dass nach dem Abschluss der GRE-/DMVPN-Übungen die **MPLS-Tunnel zwischen Edges** künftig nicht mehr manuell aufgebaut werden – die Rolle dieser Tunnel übernimmt das MPLS-Label-Switching selbst. Anschließend folgt ein **„Ausflug nach BGP“**, bei dem sowohl die theoretischen Grundlagen als auch praktische Attribute behandelt werden.

BGP (Border Gateway Protocol) ist ein **Pfadvektorprotokoll**, das anders als Interior Gateway Protocols (IGPs) nicht auf Metriken wie Hop Count oder Bandbreite basiert, sondern auf **politischen, wirtschaftlichen oder organisatorischen Präferenzen**.

Der Professor formuliert es so:

> „Bei BGP zählt nicht die kürzeste oder schnellste Verbindung – sondern die gewollte.“

---

3. BGP im Kontext von MPLS und Internetstruktur

BGP ist das Protokoll, das **autonome Systeme (AS)** miteinander verbindet. Diese AS sind logische Verwaltungseinheiten von Providern, Konzernen oder großen Organisationen. Das globale Internet besteht also aus einem Netzwerk von Netzwerken, wobei jedes AS seine eigenen **Policies**, **Peering-Vereinbarungen** und **Routing-Präferenzen** definiert.

3.1 Policy-based Routing

Die Auswahl eines Pfades folgt **nicht technischen**, sondern **ökonomisch-politischen Kriterien**. Beispiel:

> Die Telekom Austria routet Traffic Richtung Westen (z. B. nach Übersee) über *British Telecom* statt über die *Deutsche Telekom*, da beide Unternehmen über die gemeinsame Tochter „Datacom Information Systems“ verbunden sind – ein Konzerninteresse.

Damit BGP solche **Präferenzen** ausdrücken kann, nutzt es **Pfadmanipulation durch Attribute**, z. B. `Local Preference`, `AS-Path`, `MED`, oder `Community`.

---

4. Struktur und Attribute von BGP

BGP-Implementierungen (nach RFC 1771 ff., aktuell BGPv4) beruhen auf **Pfadvektor-Mechanismen** mit **inkrementellen Updates** – d. h. Router tauschen nur geänderte Routen aus. In der Praxis kann der Neustart eines Core-Routers mit 1,6 Millionen Routen **mehrere Stunden dauern**, bis die Routing-Tabellen vollständig konvergieren.

4.1 Typen von BGP

- **eBGP** – External BGP, Austausch zwischen unterschiedlichen AS
- **iBGP** – Internal BGP, Austausch innerhalb eines AS
- **BGP Speaker** – Router, die BGP sprechen (nicht „adjacent“ im IGP-Sinn, sondern „peered“)

---

5. Zentrale BGP-Attribute

Der Professor betont fünf Attribute, die für Reifeprüfungen und Praxis entscheidend sind:

Attribut	Typ	Beschreibung	Zweck
AS-Path	Mandatory, transitive	Sequenz von AS, die eine Route durchlaufen hat	Loop Detection, Policy Enforcement
Next-Hop	Mandatory, transitive	Zieladresse des nächsten AS	Pfadauswahl, analog zu Next-Hop im IGP
Local Preference	Optional, non-transitive	Bevorzugung eingehender Pfade	Eingangs-Policy, internes Load-Balancing

Attribut	Typ	Beschreibung	Zweck
MED (Multi Exit Discriminator)	Optional, non-transitive	Auswahl eines bevorzugten Ausgangs	Ausgangs-Policy, Richtung nach außen
Community	Optional, transitive	Gruppierung mehrerer Routen	Vereinfachung der Policy-Verwaltung

5.1 AS-Path

Das **AS-Path-Attribut** dokumentiert, welche autonomen Systeme ein Paket durchlaufen hat. Es wird genutzt, um:

- Loops zu erkennen (ein AS taucht mehrfach auf),
- oder gezielt AS zu meiden oder zu bevorzugen.

Ein Beispiel politischer Anwendung:

> „Wenn ein bestimmtes AS in einem sanktionierten Land liegt (z. B. Iran oder Syrien), kann ein Provider am Exchange-Node eine Filterregel setzen, die alle Routen mit diesem AS blockiert oder depriorisiert."

Damit wird **Routing als politisches Instrument** verwendet. In Österreich wäre dies im Notstandsfall gesetzlich erlaubt.

---

6. Governance und Eingriffsrechte im Routing

Der Professor erläutert, dass der **Bundeskanzler im nationalen Notstand** (Gesundheits-, Sicherheits- oder Demokratie-Notstand) das Recht hat, in das Routing einzugreifen – bis hin zur temporären Abschaltung von Netzen. Bei COVID-19 wurde diese Kommunikationskette getestet – mit teils unerwarteten Problemen beim Wiederaufbau der Routingtabellen (Konvergenzzeit).

Aus dieser Erfahrung resultieren **staatliche Sicherheitsstrukturen**, etwa eine Stabsstelle im Innenministerium für die Koordination mit Internet Service Providern.

---

7. DNS-Traffic, Tunneling und Security Appliances

Ein längerer Exkurs behandelt **DNS-basierte Tunnels** (z. B. zur Umgehung von Sperren). Der Professor erläutert anhand der **Fortinet-Appliance**:

- DNS-Pakete werden anhand von **Signaturen, Paketgröße und Request/Response-Frequenz** analysiert.

- Systeme wie Fortinet abonnieren regelmäßig **aktualisierte Blacklists** bekannter DNS- oder TOR-Endpunkte.
- Preisrahmen: ca. **2.500 USD pro Monat und Maschine**, was zeigt, dass Security ein lukrativer Markt ist.

Dieses Beispiel verdeutlicht den **Übergang von Routing zu Security Management** – ein Aspekt, der in der Reifeprüfung zunehmend Gewicht hat.

---

8. Grafentheorie, Peering und Routing-Effizienz

Anhand der **Graphentheorie** erklärt der Professor, wie sich Peering-Entscheidungen ökonomisch motiviert treffen lassen. Das Ziel ist eine **geringe durchschnittliche Pfadlänge („Average Path Length“) $<$ 10 AS-Hops**, idealerweise gemäß dem Prinzip der „Six Degrees of Separation“.

Er verweist auf Tools wie das **Hurricane Electric BGP Toolkit**, das Echtzeitdaten zu AS-Topologien liefert. Peering-Beziehungen (z. B. am Vienna Internet Exchange, VIX) werden **täglich neu verhandelt**, abhängig von:

- erwarteter Last (z. B. Feiertage, Krisen, Sportereignisse)
- wirtschaftlichen Beziehungen
- Traffic-Statistiken zwischen AS

---

9. Bogons und Compliance-Thematik

Ein besonders praxisnaher Abschnitt widmet sich der **Haftungsproblematik durch „Bogons“** – IP-Adressen, die **nicht geroutet werden dürfen**, aber faktisch geroutet werden.

Beispiel:

> Ein Mitarbeiter der T-Systems platzierte im Rechenzentrum einen privaten Server mit einer „freien“ IP-Adresse aus einem vom Unternehmen vergebenen Adressbereich. Diese Adresse war offiziell keinem Kunden zugewiesen, jedoch global routbar. Der Server wurde für illegale Aktivitäten genutzt (Kinderpornografie).

Folgen:

- Der **Geschäftsführer** wurde strafrechtlich verurteilt wegen **Sorgfaltspflichtverletzung**,
- nicht der Administrator,
- weil kein Prozess existierte, der regelmäßig überprüfte, ob nicht zugewiesene Adressen blockiert sind.

Daraus leitet der Professor die Bedeutung von **Compliance, Prozessmanagement und Reporting** im IT-Betrieb ab:

- Unternehmen benötigen **regelmäßige Prüfprozesse** (z. B. wöchentliche Bogon-Filterung).
- Fehlende Stellvertretungsregelungen (z. B. Krankheitsfälle) führen zu Haftung.
- **Compliance Officer / Governance-Beauftragte** überwachen Prozesse, aber **Geschäftsführer bleibt haftbar**.

  „Unwissenheit schützt nicht vor Haftung. Auch nicht im Rechenzentrum."

---

10. Route Filtering und Device Hardening

Technisch wird das umgesetzt durch **Prefix-Listen** und **Access-Listen**, die RFC 1918-Adressen blockieren:

- Private Networks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
- Loopback-Adressen
- Multicast- und Broadcast-Adressen
- Class E-Testbereiche

Diese Filter gehören zu jeder **Edge-Firewall oder BGP-Edge-Router-Konfiguration** (Thema: *Device Hardening*).

---

11. Route Reflectors und iBGP-Skalierung

BGP-Router geben standardmäßig **keine via iBGP gelernte Routen** an andere iBGP-Nachbarn weiter. In großen internen Topologien führt das zu Skalierungsproblemen („Dreierkette").

Lösung:

- **Route Reflector (RR):** zentrales iBGP-Relay, das Routen weiterverteilt.
- Er funktioniert ähnlich wie der **Designated Router (DR)** bei OSPF, mit dem Vorteil reduzierter Full-Mesh-Verbindungen.

Fehlt ein RR im Szenario, **funktioniert iBGP nicht korrekt** – typischer Prüfungsfehler!

---

12. Flapping & Dampening

Route Flapping: Instabile Präfixe, die ständig erscheinen/verschwinden, führen zu hoher CPU-Last und Instabilität. **Route Dampening:** Mechanismus zur Unterdrückung solcher Präfixe über Zeitfenster. Das Ziel ist nicht höchste Aktualität, sondern maximale **Stabilität der Routing-Topologie**.

---

13. Prüfungsrelevante Themen und Lernstruktur

Der Professor kündigt ab dieser Einheit wöchentliche **Socrative-Tests** und **FAQ-Listen** an:

- Lernzielkontrolle zu BGP-Attributen, MPLS-Struktur, Compliance und Policy Routing.
- Präsentationstermine folgen, basierend auf Themen der Vorwoche.

Ziel: Kontinuierliche Lernüberprüfung und Vermeidung von „Schneeballeffekt“ kurz vor der Reifeprüfung.

Typische Prüfungsszenarien:

- BGP-Konfiguration mit Attributmanipulation (Local Pref, MED, Community)
- Prefix-Filterung und Bogon-Erkennung
- Route Reflector im iBGP
- Kombination mit MPLS-Backbone
- Fragen zu Governance, Compliance und Haftung
- Interpretation von AS-Pfaden (Loop Detection, Policy)

---

14. Fazit

Die Einheit verdeutlicht, dass moderne Netzwerke **nicht mehr rein technisch**, sondern **sozio-technisch** geprägt sind: Ökonomische, politische und rechtliche Interessen bestimmen, **wie und über wen Daten fließen**.

BGP ist damit sowohl ein Routing- als auch ein **Policy-Protokoll**, das an der Schnittstelle von Technik, Wirtschaft und Recht agiert. In Kombination mit MPLS bildet es die Grundlage für skalierbare, differenzierte und kontrollierte Provider-Backbones.