# Teil 1 – Wissenschaftliche Zusammenfassung der Vorlesung „RDP und DMVPN“

## 1. Einleitung und thematischer Rahmen

Die Vorlesung widmet sich der Konzeption, Funktionsweise und praktischen Umsetzung von **Dynamic Multipoint Virtual Private Networks (DMVPN)** im Kontext moderner **Weitverkehrsnetze (WANs)**. Aufbauend auf früheren Konzepten wie **MPLS** und **Frame Relay** wird die Frage behandelt, wie sich flexible, skalierbare und dynamisch konfigurierbare Overlays über bestehende Netzwerkinfrastrukturen realisieren lassen.

Das Ziel ist die Schaffung einer **dynamischen, sicheren und selbstorganisierenden Kommunikationsstruktur** zwischen dezentralen Standorten – insbesondere im Umfeld von **Cloud-Architekturen**, **SD-WAN**-Lösungen und **mobilen Netzwerken**.

---

## 2. Historischer Kontext und konzeptionelle Grundlagen

Der Professor stellt DMVPN in eine historische Entwicklungslinie von **Frame Relay → MPLS → SD-WAN**. Bereits im Frame-Relay-Zeitalter existierte das **Hub-and-Spoke-Modell**, bei dem ein zentraler Knoten (Hub) die Kommunikation mehrerer Außenstellen (Spokes) vermittelte. Dieses Prinzip wird im DMVPN erneut aufgegriffen, jedoch um dynamische und verschlüsselte Tunnelbildung erweitert.

Eine zentrale Analogie ist der Vergleich mit **Mobilfunknetzarchitekturen**: Die Base Stations (entsprechend den Branches) kommunizieren über das **Mobile Switching Center (MSC)** als Hub. In älteren Netzen führte dies zu ineffizienten Kommunikationswegen, da auch lokale Verbindungen über das MSC geleitet wurden. DMVPN überwindet dieses Prinzip durch **direkte Spoke-to-Spoke-Kommunikation**, wodurch Engpässe und Latenzen reduziert werden.

---

## 3. Architektur von DMVPN

### 3.1 Grundaufbau

DMVPN kombiniert **Generic Routing Encapsulation (GRE)**, **Next Hop Resolution Protocol (NHRP)** und optional **IPsec** zu einem mehrschichtigen Overlay-Netzwerk. Die Basiskomponenten sind:

- **Hub:** zentrale Kontrollinstanz, verwaltet NHRP-Datenbank und Redirects
- **Spokes:** Außenstellen, die sich dynamisch registrieren und Tunnel aufbauen

- **Overlay Network:** logisches Multipoint-GRE-Netz (MGRE), optional verschlüsselt
- **Underlay Network:** physische Transportebene, oft das öffentliche Internet

### 3.2 Funktionsweise

Jeder Spoke baut initial einen Tunnel zum Hub auf und registriert seine IP- und Netzparameter über **NHRP Registration Messages**. Bei Bedarf einer Verbindung zu einem anderen Spoke fragt der Client den Hub nach der Zieladresse. Der Hub kann dann:

1. Die Verbindung selbst weiterleiten (*Hub-and-Spoke-Kommunikation*), oder
2. Ein **Redirect Message** senden, damit die Spokes direkt miteinander kommunizieren (*Spoke-to-Spoke*).

Routing-Protokolle wie **OSPF** oder **BGP** werden anschließend über die Tunnel gefahren. Das Overlay dient somit ausschließlich als Transportmedium – analog zum Label-Switching in MPLS.

---

## 4. Das Next Hop Resolution Protocol (NHRP)

NHRP ist das zentrale Steuerprotokoll im DMVPN. Es stammt ursprünglich aus der Frame-Relay-Welt und wurde für IP-basierte Netzwerke adaptiert. Seine Hauptaufgabe besteht in der **Auflösung logischer Next-Hops** in physische Adressen im Overlay.

**Hauptfunktionen:**

- **Registration:** Spokes melden sich beim Hub an und teilen mit, welche Subnetze über sie erreichbar sind.
- **Resolution Request/Reply:** Anfrage zur Erreichbarkeit eines Zielnetzes.
- **Redirect:** Hub informiert über eine direkte Route zwischen zwei Spokes.
- **Purge:** Aktualisierung oder Löschung veralteter Einträge.

NHRP ist somit funktional vergleichbar mit einem ARP-Dienst auf WAN-Ebene und bildet die Grundlage für dynamische Tunnelbildung.

---

## 5. Phasen (Modes) von DMVPN

Der Professor unterscheidet drei Phasen, die aufeinander aufbauen, aber unabhängig voneinander existieren können.

**Phase 1 – Statische Hub-and-Spoke-Struktur**

- Jeder Spoke besitzt einen festen GRE-Tunnel zum Hub (*point-to-point*).
- Kommunikation zwischen Spokes erfolgt ausschließlich über den Hub.
- Vorteil: einfach, stabil, für kleine Netze geeignet.
- Nachteil: keine direkte Spoke-to-Spoke-Kommunikation, ineffizient bei großem Datenverkehr.

**Phase 2 – Dynamische Spoke-to-Spoke-Tunnel**

- Verwendung von **Multipoint-GRE (mGRE)** und NHRP für dynamische Tunnel.
- Der Hub fungiert nur noch als Vermittlungsinstanz für Adressauflösung.
- Routing erfolgt direkt zwischen Spokes.
- Voraussetzung: Anpassung der OSPF-Network-Types, um Split-Horizon-Probleme zu vermeiden.

**Phase 3 – Redirect-gestützte Kommunikation**

- Hub sendet Redirects an Spokes, um dynamisch optimale Pfade zu erstellen.
- Routing-Tabellen werden automatisch aktualisiert.
- Optional: IPsec-Verschlüsselung („Phase 3+“) mit dynamischer Schlüsselverhandlung über IKEv2.
- Entspricht dem in der Industrie gebräuchlichen SD-WAN-Standard.

---

## 6. OSPF und Routing-Integration

Da DMVPN auf Layer 3 arbeitet, ist die Routing-Integration zentral. Der Professor erläutert ausführlich die **Anpassung von OSPF-Network-Types**:

| Typ | Beschreibung | Verwendung im DMVPN |
|---|---|---|
| Point-to-Point | Default-Typ | Phase 1 |
| Point-to-Multipoint | mehrere Spokes, keine Broadcasts | Phase 2 |
| Broadcast | simuliert LAN-ähnliches Verhalten | Alternative zu Non-Broadcast |
| Non-Broadcast (NBMA) | explizite Nachbarangabe erforderlich | Phase 3, erweiterte Kontrolle |

Um **Split Horizon** zu vermeiden, wird auf den Spokes die **Interface Priority auf 0** gesetzt, damit der Hub als **Designated Router (DR)** fungiert. Die Timer für Hello- und Dead-Intervalle müssen auf beiden Seiten synchron konfiguriert werden.

Ein wichtiger praktischer Hinweis betrifft die Befehlskombination

`clear ip ospf process`

um alte Adjazenzen nach Konfigurationsänderungen zu löschen.

---

## 7. Sicherheitsaspekte und Verschlüsselung

Ab Phase 3 wird typischerweise eine **IPsec-Integration** mit IKEv2 eingesetzt, um dynamische Tunnels zu verschlüsseln. Bei Prüfungsaufgaben gilt die Kombination „**Phase 3 + IPsec**“ als idealer Zielzustand („Best Practice Level“). Eine optionale PKI-Integration dient der automatisierten Zertifikatsverwaltung.

---

## 8. Praktische Umsetzung im Labor

Im Laboraufbau besteht die Topologie typischerweise aus drei Routern: einem Hub und zwei Spokes, verbunden über ein Transitnetz (Switch oder simuliertes Internet). Wichtige Konfigurationsschritte:

1. **GRE-Tunnel-Interface** mit IP-Adresse und Authentication-String
2. **NHRP-Server/Client-Definition** (NHS, NHC)
3. **mGRE-Tunnel** mit `tunnel mode gre multipoint`
4. **Routing-Protokoll (OSPF)** mit geeigneten Network-Types
5. **Überprüfung mit `show dmvpn`** zur Nachbarschaftsanalyse

In erweiterten Übungen werden über dieses Overlay zusätzlich **MPLS**, **VRFs** und **BGP-Redundanz** integriert.

---

## 9. Erweiterte Konzepte und Anwendungsfälle

- **Cloud Connectivity:** sichere dynamische Standortanbindung an Cloud-Ressourcen.
- **Mobile Networks:** Reduktion von MSC-Bottlenecks durch MSC-to-MSC-Kommunikation.
- **Industrial OT:** Einsatz von DMVPN als „Building Block“ zur Fernsteuerung industrieller Anlagen.
- **SD-WAN-Integration:** zentrale Verwaltung über Orchestrierungstools mit Zero-Touch-Deployment.

---

## 10. Prüfungsrelevante Szenarien (Reifeprüfung)

Der Professor erläutert typische Bewertungskriterien:

| Level | Beschreibung | Punktewert (implizit) |
|---|---|---|
| **Phase 1 unverschlüsselt** | Basiskonfiguration mit statischem Tunnel | Mindestanforderung |
| **Phase 2 unverschlüsselt** | Dynamische Spoke-to-Spoke-Kommunikation | fortgeschritten |
| **Phase 3 unverschlüsselt** | Redirect-Mechanismus, OSPF korrekt konfiguriert | sehr gut |
| **Phase 3 + IPsec** | Dynamische Verschlüsselung, PKI möglich | optimal |

Reifeprüfungsszenarien umfassen vollständige Netzaufbauten mit 10–20 Geräten, Kombination von DMVPN mit **MPLS**, **VRFs** und **BGP-Redundanz**, sowie zusätzliche Aufgaben zu **Logging, Monitoring (Cacti, Prometheus, Syslog)** und **Netzwerksicherheit**.

Wesentliche Bewertungskriterien:

- Funktionsfähigkeit der Konnektivität
- Korrekte Routing- und OSPF-Konfiguration
- Zeitmanagement und systematische Vorgehensweise
- Selbstständige Fehleranalyse

---

## 11. Didaktische Hinweise und „Insider“-Bemerkungen

Der Professor betont mehrfach:

- **Praxisorientiertes Üben** sei entscheidend: Schüler sollen wiederholt vollständige Topologien aufbauen.
- **Zeitmanagement**: In der Reifeprüfung (ca. 5 Stunden) entscheidet Effizienz.
- **Konfigurationsroutine**: häufige Wiederholung führt zu Stabilität.
- **„Nicht erst bei der Reifeprüfung nachschauen“** – alle Befehle und Abläufe sollen vorher beherrscht werden.
- **Eigeninitiative:** Selbständiges Arbeiten, besonders bei fehlender Lehrperson, wird erwartet.
- **„Übung ist Intelligenztest“** – Verständnis geht über bloße Befehlskenntnis hinaus.

---

## 12. Ausblick

Nach Abschluss der DMVPN-Thematik folgen:

- **MPLS mit BGP** zur Provider-Simulation

- **VRFs** zur Mehrmandantenfähigkeit (gleiche IP-Adressräume)
- **Redundanz mit BGP (MED, Weight)**
- **SD-WAN mit Fortinet Appliances**
- **Security-Härtung** (Access Control, Traffic Policing, Control/Data Plane Protection)
- **Automatisierung mit Python**, u. a. für Routersteuerung

Damit bildet DMVPN den zentralen Übergang zwischen klassischen WAN-Technologien und modernen SD-WAN- und Cloud-Infrastrukturen.