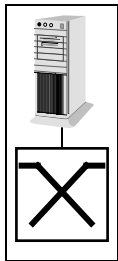


# Netze und Protokolle für das Internet



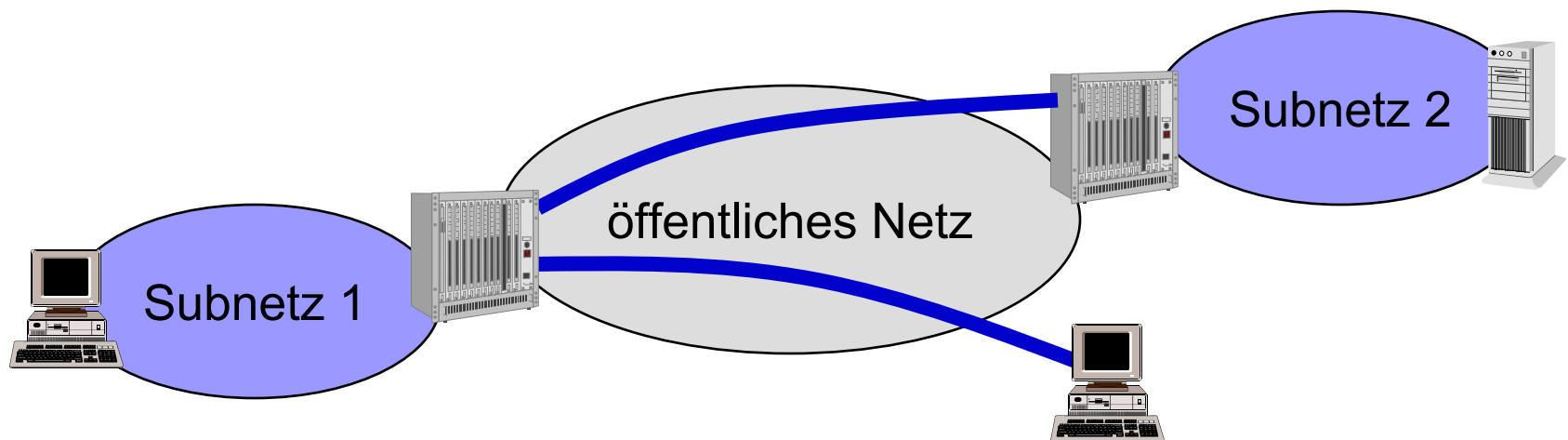
## 8. Virtuelle Private Netze

# Inhalt

- Virtuelle Private Netze
- Layer-2- und Layer-3-VPNs
- Virtuelle Private Netze mit MPLS
- Entfernter VPN-Zugriff
  - L2TP und RADIUS
- IP Security
  - Sicherheitsassoziation
  - Authentication Header
  - Encapsulation Security Payload
  - Internet Key Exchange
- VPNs und Firewalls

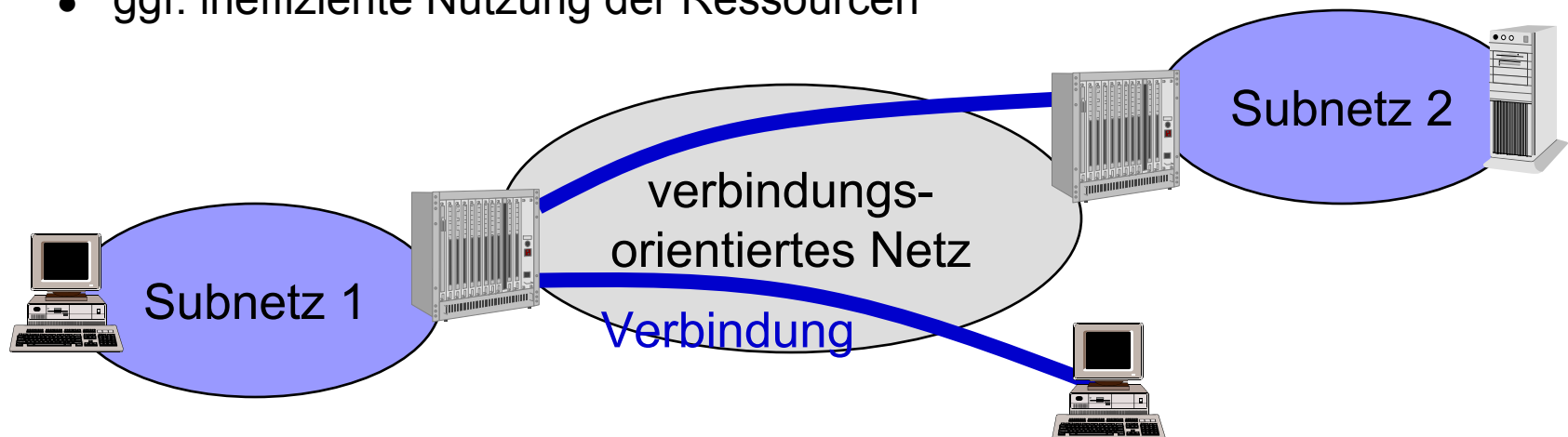
# Virtuelle Private Netze

- Ein Virtuelles Privates Netz (VPN) ist ein über einer öffentlichen Kommunikationsinfrastruktur für den privaten Gebrauch einer Organisation etabliertes Netz.
- 2 Adressierungsebenen
  - Physikalische (geographische) Adressen
  - Logische Adressen
- Hauptanwendungen
  - Verbindung entfernter Subnetze einer Organisation
  - entfernter Zugriff von Mitarbeitern auf das private Netz einer Organisation



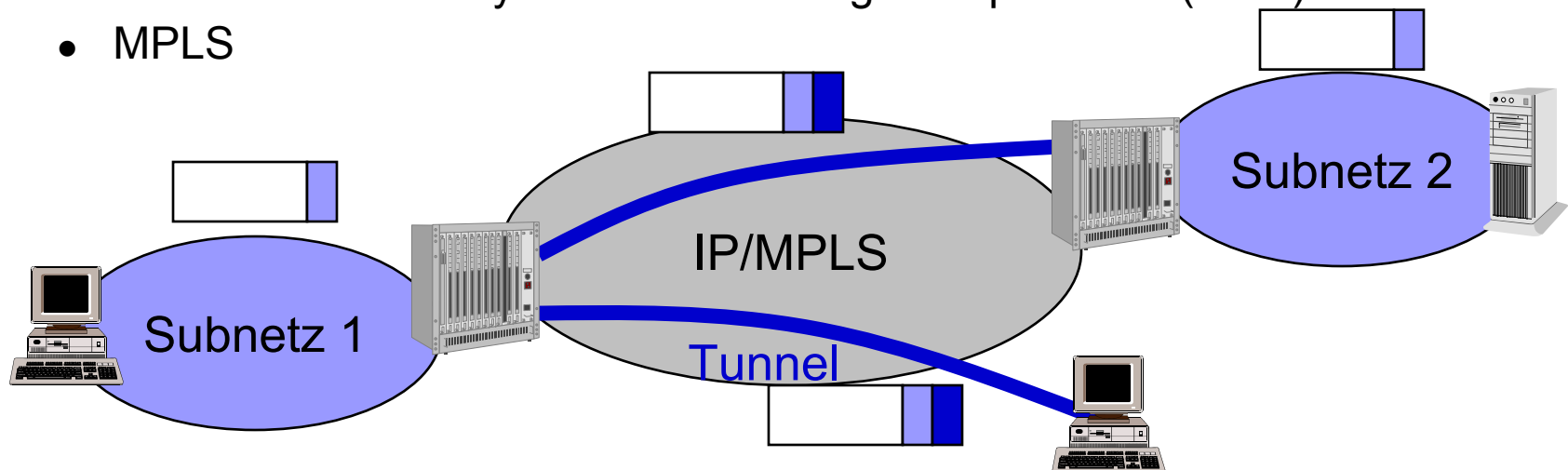
# Layer-2-VPNs

- Systeme eines logischen (IP-)Subnetzes werden über eine (meist verbindungsorientierte) Netztechnologie verbunden.
- Beispiele
  - ATM, ISDN, Frame Relay zur Verbindung von Routern und Bridges
- Vorteil
  - Dienstgütenunterstützung
- Nachteile
  - homogene Zugangsnetze erforderlich
  - Management von zwei unterschiedlichen Netztechnologien
  - ggf. ineffiziente Nutzung der Ressourcen

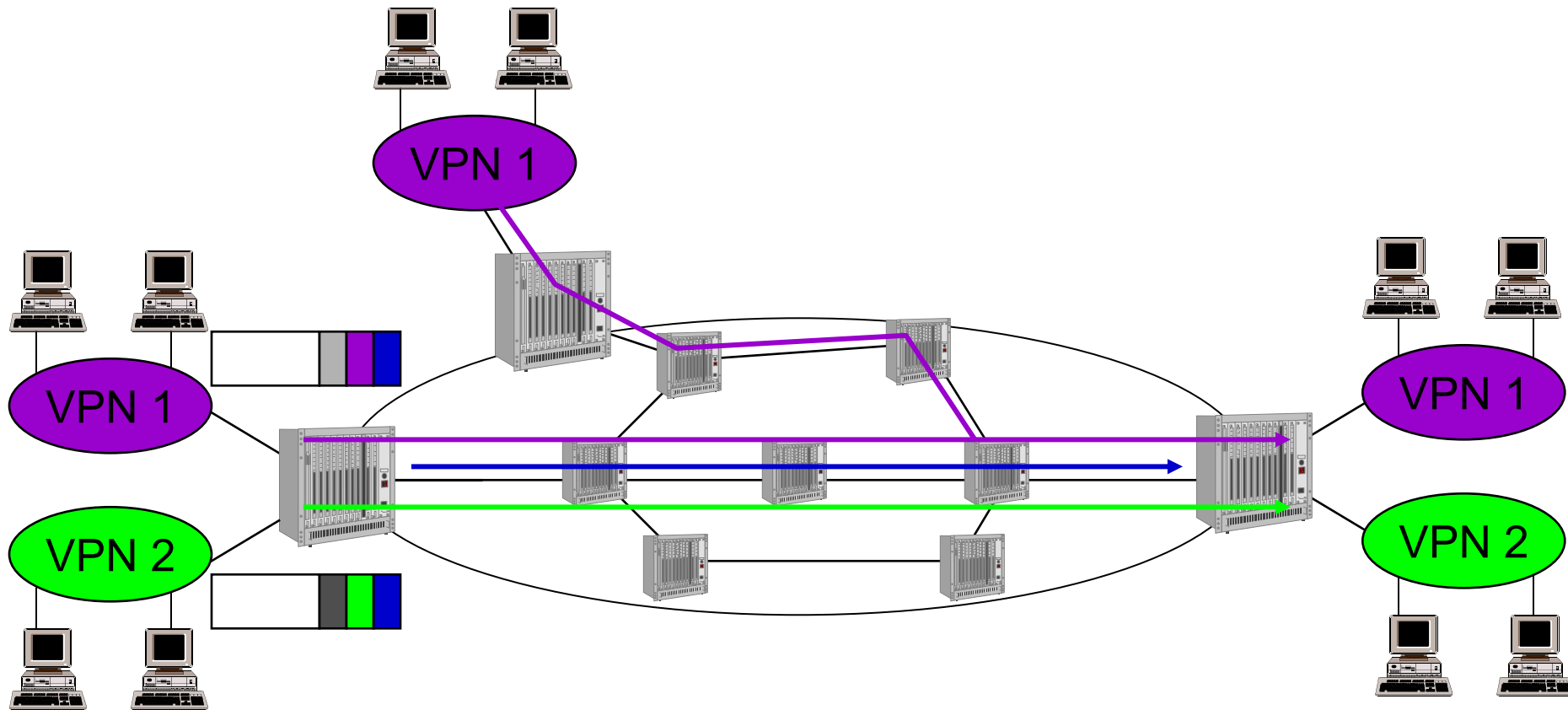


# Layer-3-VPNs

- Internet als geteiltes öffentliches Netz
- Private Pakete werden eingekapselt und über Tunnel übertragen.
- Vorteile
  - erlaubt heterogene Zugangsnetze
  - preiswerte Internet-Technologie (hauptsächlich Kosten f. Internet-Zugang)
- Probleme
  - Sicherheit → IP Security
  - Dienstgüten → Differentiated Services
- Einkapselungsverfahren
  - IP-in-IP / IP Security / Generic Routing Encapsulation (GRE)
  - MPLS

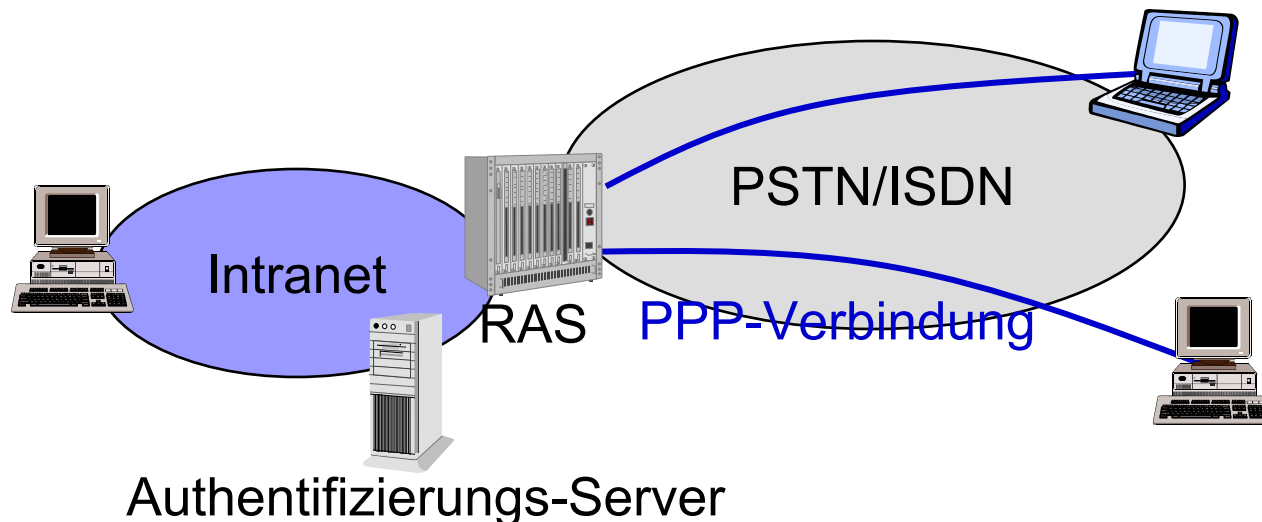


# Virtuelle Private Netze mit MPLS



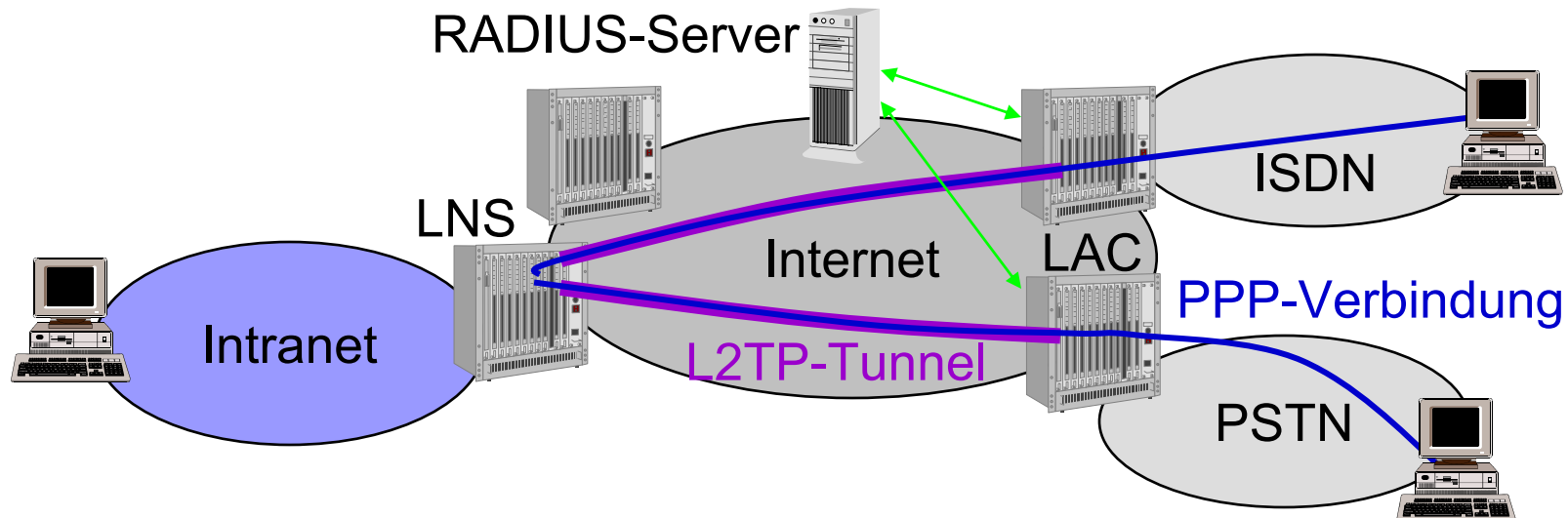
# Traditioneller entfernter VPN-Zugriff

- Etablieren von PPP-Verbindungen (z.B. über Weitverkehrsnetze) vom Client zum Remote Access Server (RAS)
- PPP: Point-to-Point Protocol
- Authentifizierung durch separaten Authentifizierungs-Server



# Entfernter VPN-Zugriff über Konzentrator

- Layer 2 Tunneling Protocol (L2TP) erlaubt Tunneln von Layer-2-Protokollen (z.B. PPP) über IP
- Lokale Verbindungen zwischen Client und L2TP Access Concentrator (LAC)
- Authentifizierung über RADIUS-Server
- Weiterleiten der PPP-Pakete über L2TP-Tunnel zwischen LAC und L2TP Network Server (LNS)



# L2TP

- LNS und LAC tauschen L2TP-Kommandos und Antworten zum Etablieren, Aufrechterhalten und Terminieren von Tunnels und Sessions aus.
- Alle L2TP-Pakete werden in UDP eingekapselt.
- Einkapseln von mehreren PPP-Verbindungen (= Sessions) in einen L2TP-Tunnel
- Anwendung von IP-Security-Protokollen zur Authentifizierung und Verschlüsselung

flags	version	length
tunnel ID		call ID
Ns		Nr

# Remote Authentication Dial-In User Service

- RADIUS erlaubt das Überprüfen von Authentifizierungsinformationen durch einen zentralen Server (Request- / Reply-Nachrichten)
- Datenbank enthält
  - Passwörter (Authentifizierung)
  - Zugriffsrechte (Autorisierung)
  - Netzbenutzungsinformationen (Accounting)
- RADIUS-Server kann weitere Informationen (z.B. Passwörter) verlangen.
- LAC kann Accounting-Informationen (z.B. Beginn und Ende einer Verbindung) an RADIUS-Server senden.

# IP Security

- Authentifizierung
  - Sender-Authentifizierung
    - Überprüfen, ob empfangenes Paket wirklich durch den ausgegebenen Sender gesendet wurde
  - Datenintegrität
    - Überprüfen, ob die Daten auf dem Pfad vom Sender zum Empfänger manipuliert wurden
- Verschlüsselung
  - vertraulicher Datenaustausch

# IPSec-Protokolle

- Entwicklung mit IPv6, spätere Integration in IPv4
- Protokolle
  - Authentication Header (AH)
    - Sender-Authentifizierung, Datenintegrität
  - Encapsulating Security Payload (ESP)
    - Verschlüsselung
  - Internet Key Exchange (IKE)
    - Schlüsselmanagement

# Sicherheitsassoziation

- Sender und Empfänger müssen Menge gemeinsamer Parameter vereinbaren

→ Sicherheitsassoziation (SA)

= logische, unidirektionale Verbindung zwischen Sender und Empfänger

- Identifikation einer Sicherheitsassoziation durch
  - IP-Zieladresse
  - Security-Parameter-Index (SPI, 32-Bit-String)
  - IPSec Protokoll (ESP/AH)

# Parameter einer Sicherheitsassoziation

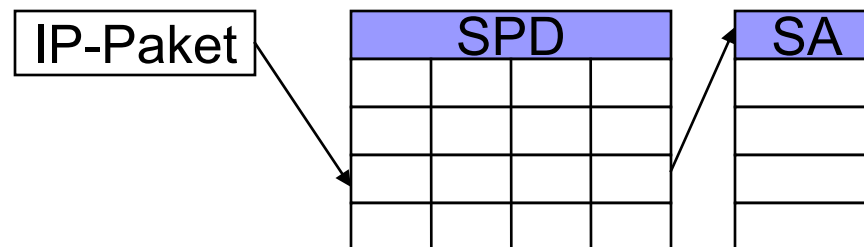
- Sequenznummernzähler zur Generierung der Sequenznummer in AH- oder ESP-Header
- Sequenznummernüberlaufanzeige
- Anti-Replay-Fenster (Sliding Window für Sequenznummer)
- AH-Information (z.B. Authentifizierungsalgorithmus, Schlüssel, Schlüssellebenszeit, ...)
- ESP-Information (Verschlüsselungs- und Authentifizierungsalgorithmus, Schlüssel, Schlüssellebenszeit, Initialisierungsdaten)
- Lebenszeit der Sicherheitsassoziation
- IPSec-Protokollmodus (Transport, Tunnel)
- Pfad-MTU

# Security Policy Database (SPD)

- SPD definiert Untermenge von IP-Verkehr (SPD-Eintrag) und bildet diesen auf eine Sicherheitsassoziation ab.
- SPD-Eintrag = Menge von Protokollfeldern von IP und darüber liegenden Protokollen (Selektoren)
  - IP-Adressen, IPv4 ToS, IPv6 Traffic Class, IPv6 Flow Label, Transportprotokoll
  - Port-Nummern
  - IPSec-Protokoll
  - UserID
  - Sensitivitätslevel

# IPSec-Paketverarbeitung

- Verarbeitung von ausgehenden Paketen
  1. Finden eines geeigneten SPD-Eintrags basierend auf Selektoren
  2. Bestimmen der SA und des dazugehörigen SPI
  3. Erforderliche IPSec-Verarbeitung (AH oder ESP)
- Empfangene Pakete werden anhand des SPI auf eine Sicherheitsassoziation abgebildet.



# Authentication Header

- zur Authentifizierung und Datenintegrität aller IP-Header-Felder, die sich auf dem Weg zwischen Sender und Empfänger nicht ändern
- Default-Algorithmus für Authentifizierungsdaten: Keyed MD5 berechnet 128-Bit-Wert über
  - nicht änderbare IP-Header-Felder des Pakets
  - den AH-Header ausser Authentifizierungsdaten
  - höhere Protokolle und Daten und
  - einem geheimen Schlüssel

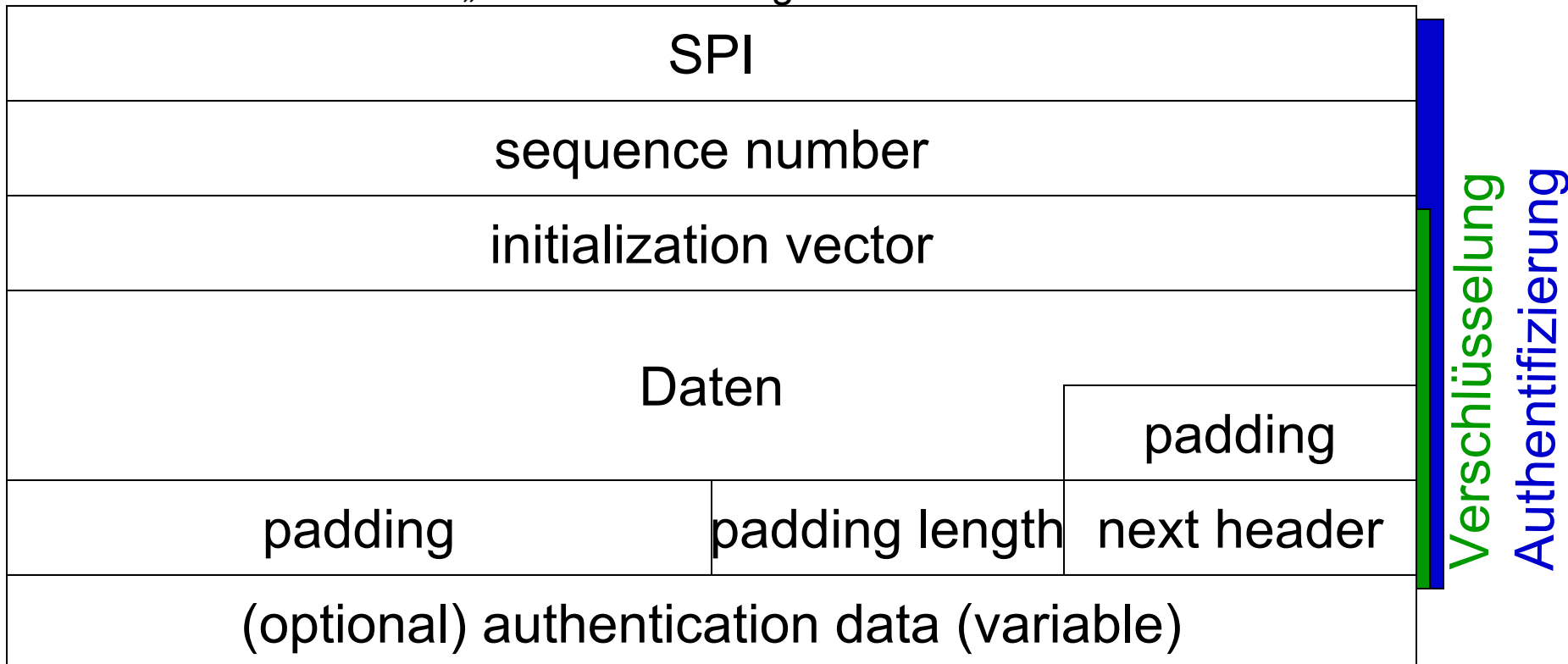
next header	payload length	reserved
SPI		
sequence number		
authentication data (n · 32 bit)		

# Schutz vor Replay-Attacken

- **Replay-Attacke**
  - Angreifer hört authentifiziertes Paket ab und sendet es später (mehrmals) zum Ziel, z.B. um einen Dienst zu beeinträchtigen.
- **Schutzmechanismus**
  - Sender initialisiert Sequenznummernzähler bei der SA-Etablierung und platziert den Wert im Sequenznummernfeld.
  - Empfänger akzeptiert nur Pakete im Fenster  $[N-W+1 \dots N]$ 
    - N = höchste empfangene Sequenznummer
    - W = Fensterbreite (default: 64)
  - Bei Erreichen des Limits von  $2^{32}-1$  wird neue SA mit neuen Schlüsseln vereinbart.

# Encapsulation Security Payload (ESP)

- Initialization Vector (32n Bit):
  - Input für Verschlüsselungsalgorithmus (Default: DES-CBC)
- Padding
  - Verschlüsselungsverfahren arbeitet auf bestimmten Blocklängen
  - Ausrichtung von Padding Length und next header
  - Verschleiern der „realen“ Paketlänge



# Padding-Feld

- Verschlüsselungsverfahren arbeitet auf einem Vielfachen einer bestimmten Anzahl von Bytes.
- Padding Length und Next Header müssen auf 32 Bit ausgerichtet werden.
- Modifizieren der „realen“ Paketlängen, um Verkehrscharakteristiken zu verschleiern.

# Authentifizierung durch AH bzw. ESP

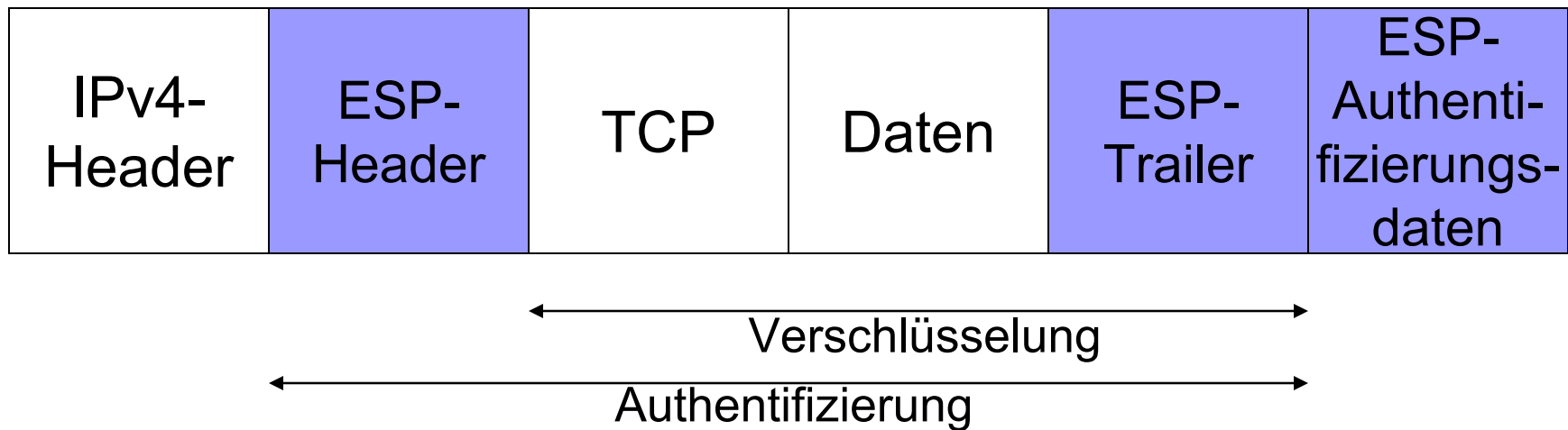
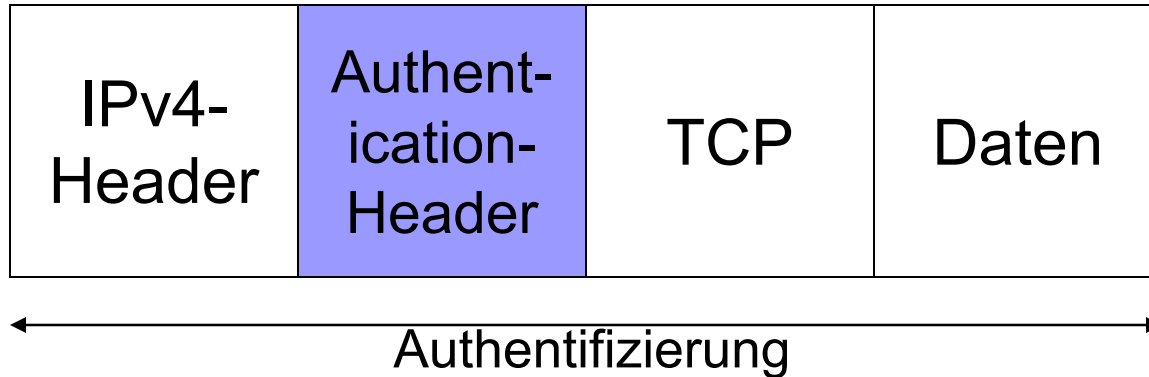
## ■ AH

- berücksichtigt (nicht änderbare) IP-Header-Felder und Nutzlast
- hauptsächlich für Authentifizierung ohne Verschlüsselung

## ■ ESP

- berücksichtigt nur ESP-Paket
- für Fälle mit Authentifizierung und Verschlüsselung
- effizienter, da Daten für Verschlüsselung und Authentifizierung integriert verarbeitet werden können.

# IPSec und IPv4

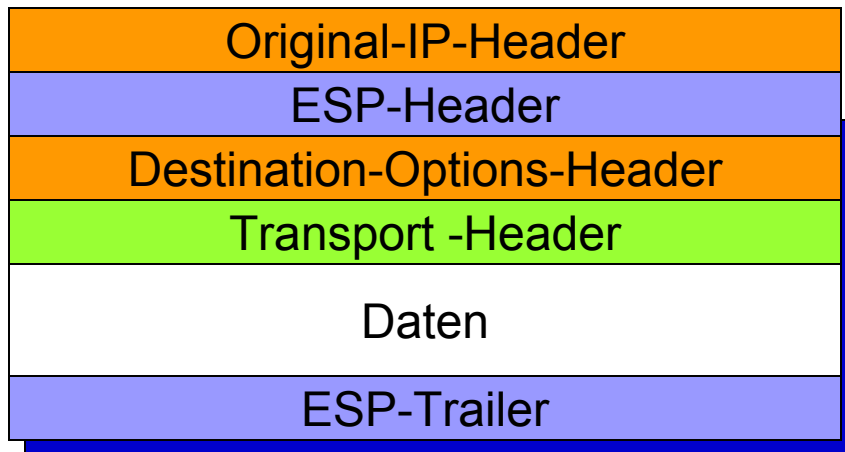


IP Security ist in IPv4 optional.

# Transport- und Tunnel-Modus

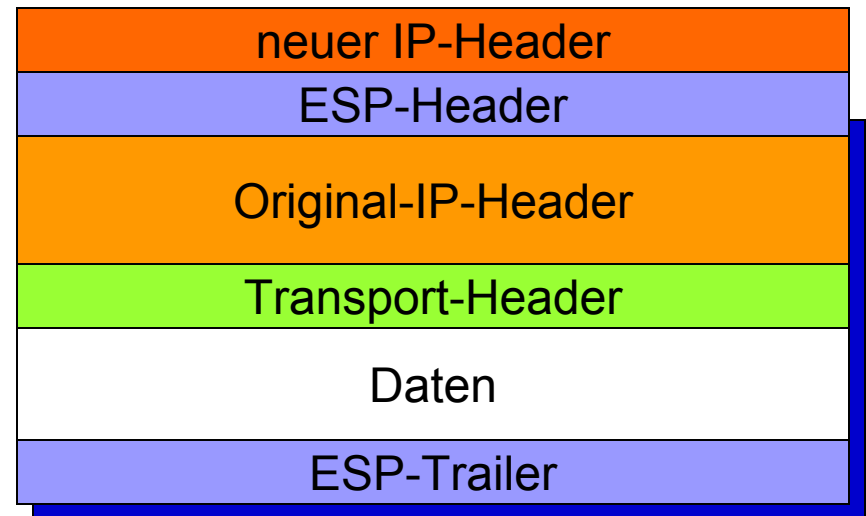
## ■ Transport-Modus

- Verschlüsselung der Ende-zu-Ende Erweiterungs-Header und des Transport-Protokoll-Pakets



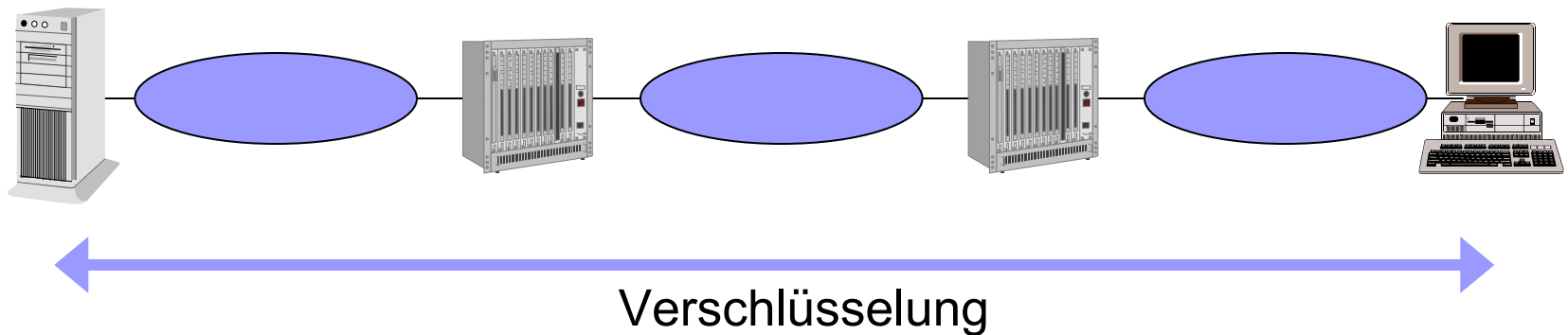
## ■ Tunnel-Modus

- Verschlüsselung eines vollständigen IP-Pakets
- Einkapseln innerhalb eines neuen IP-Pakets



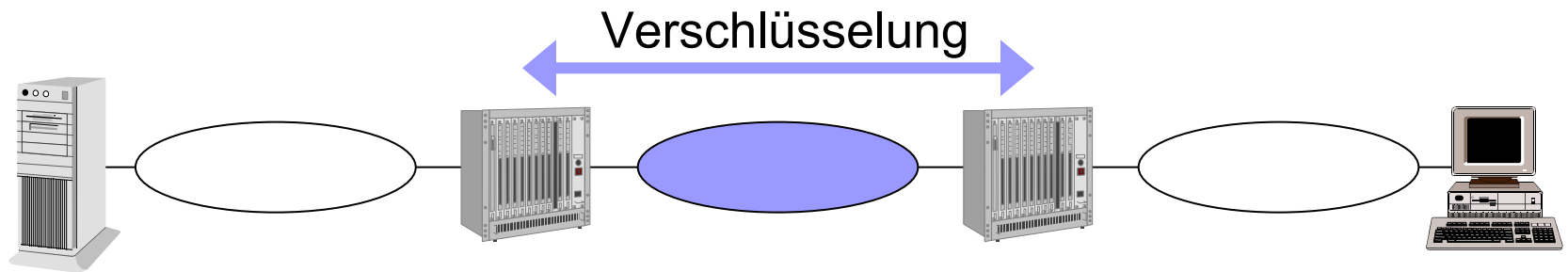
# Transport-Modus

- Ende-zu-Ende-Verschlüsselung
  - Beispiel: vertraulicher Datenaustausch zwischen zwei Benutzern

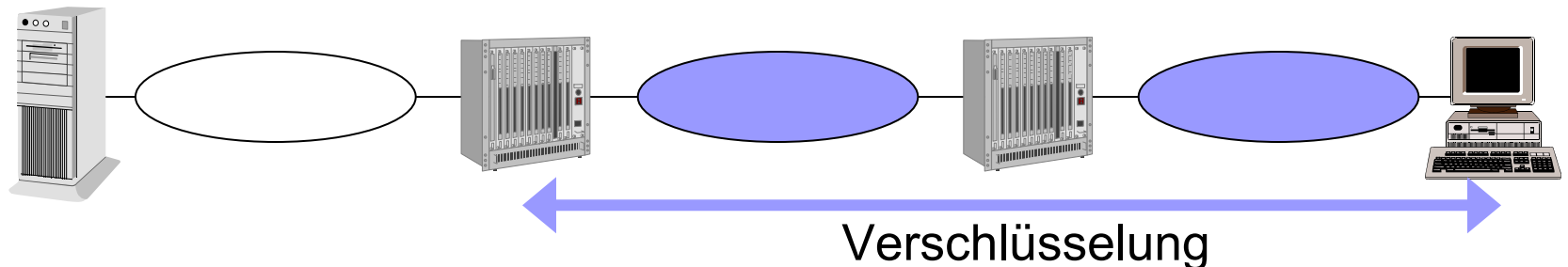


# Tunnel-Modus

- Security-Gateway zu Security-Gateway
  - Beispiel: Virtuelles Privates Netz (VPN)



- Endsystem zu Security-Gateway
  - Beispiel: Zugriff auf Firmennetz über unsichere Zugangsnetze



# Schlüsselverwaltung

- Authentifizierung und Verschlüsselung basieren auf sicherer Verteilung und Aktualisierung von Schlüsseln und Protokollparametern
- Internet Key Exchange (IKE) basiert auf
  - Internet Security And Key Management Protocol (ISAKMP)
    - Prozeduren und Paketformate zum Aufbau von Sicherheitsassoziationen
  - Untermenge von Oakley
    - Schlüsselaustauschprotokoll basierend auf Diffie-Hellman-Verfahren

# Diffie Hellman Schlüsselaustausch

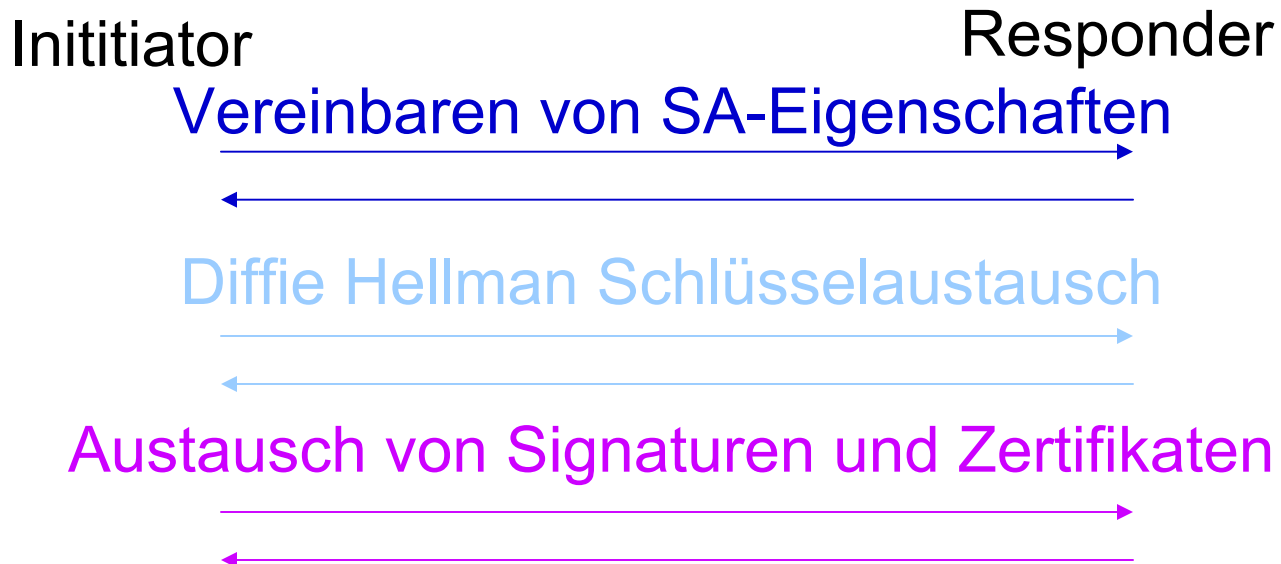
- A und B vereinbaren eine Primzahl  $p$  und einen Generator  $g$ .
- A wählt Zufallszahl  $x$ , berechnet  $n = g^x \bmod p$ , und sendet  $n$  an B
- B wählt Zufallszahl  $y$ , berechnet  $m = g^y \bmod p$ , und sendet  $m$  an A
- Schlüssel der Sitzung:  
 $z = n^y \bmod p = m^x \bmod p = g^{xy} \bmod p$
- Sicherheit durch die schwierige Berechnung von  $x$  und  $y$  („diskreter Logarithmus“)

# IKE-Phasen

- Phase 1
  - Etablieren eines sicheren primären IKE-Kanals → IKE SA
    - Vereinbaren von Sicherheitsparametern
    - Vereinbaren eines geheimen Schlüssels
    - Gegenseitige Authentifizierung der Identitäten
  - Modi
    - Main Mode
    - Aggressive Mode
    - Base Mode
- Phase 2
  - Erzeugen von allgemeinen SAs
  - Modus
    - Quick Mode

# Main Mode

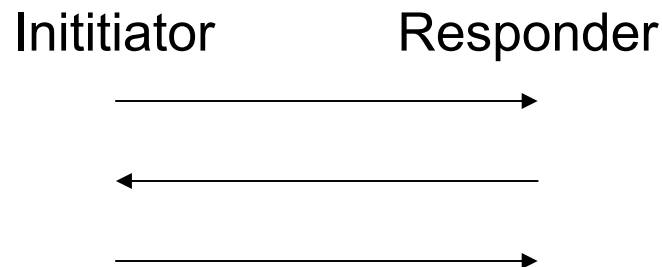
- Austausch von 3 Nachrichtenpaaren
- Authentifizierungsmöglichkeiten
  - symmetrische Verschlüsselung  
mit im Voraus vereinbartem geheimem Schlüssel
  - digitale Signaturen
  - Verschlüsselung mit öffentlichen Schlüsseln



# Aggressive und Base Mode

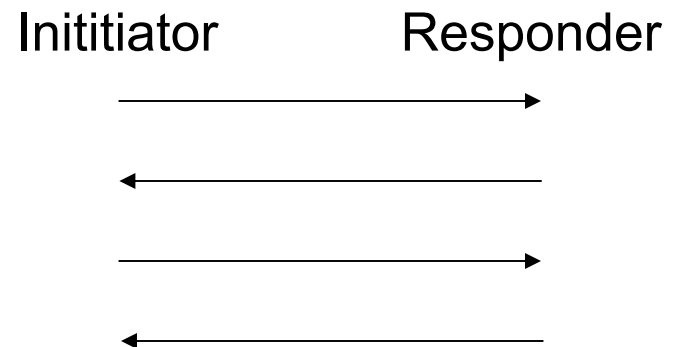
## ▪ Aggressive Mode

- Austausch von 3 Nachrichten
- Die ersten beiden Main-Mode-Nachrichten des Initiators werden in einer Nachricht zusammengefasst.
- Die 3 Main-Mode-Nachrichten des Responders werden in einer Nachricht zusammengefasst
- Authentifizierungsmöglichkeiten wie Main Mode



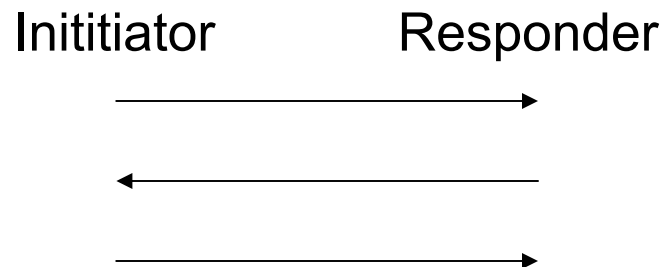
## ▪ Base Mode

- Austausch von 4 Nachrichten
- SA-Vereinbarung im 1. Nachrichtenpaar
- Diffie-Hellman-Schlüsselaustausch im 2. Nachrichtenpaar



# Quick Mode

- Phase 1 etabliert sicheren Kanal
- Etablieren von allgemeinen SAs (z.B. IPSec SAs) mit Quick-Mode
  - Initiator schlägt Parameter vor.
  - Responder wählt Parameter aus.
  - Initiator bestätigt.
- Sämtliche Nachrichten sind verschlüsselt.
- Etablieren von mehreren SAs in einem Schritt möglich.



# VPNs und Firewalls

- Etablieren von gesicherten (authentifiziert und verschlüsselt) IPSec-Tunneln zwischen Firewalls
- Firewalls akzeptieren nur Pakete von authentifizierten Systemen und entkapseln diese.

