Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

Bundesverwaltungsamt

– Bundesstelle für Informationstechnik –

IT-Dienstleistungszentrum des Bundes

IPv6-ÖV-Workshop

Workshop-Modul A:

IPv4/IPv6-Übergangstechniken

16. Dezember 2013

Nutzungshinweise

- Nutzung und Weitergabe unter folgenden Voraussetzungen:

Creative Commons 3.0, Deutschland Lizenz (CC BY-NC 3.0)
<http://creativecommons.org/licenses/by-nc/3.0/de/>

- Namensnennung
  Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen.
- Keine kommerzielle Nutzung
  Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.

- Unter Verwendung der OSA Icon Library: http://www.opensecurityarchitecture.org

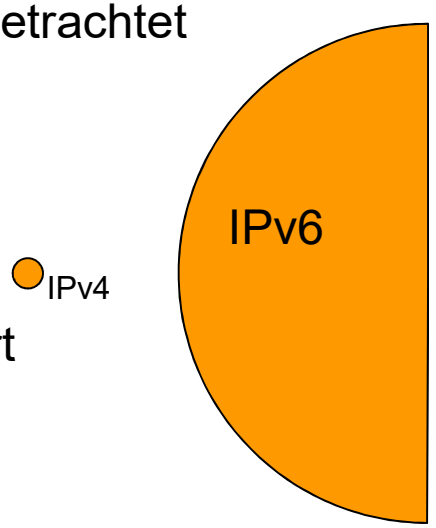
Übersicht

- Motivation und Ziel
  - Sichtweisen und Akteure
- Vorstellung von Übergangstechnologien
  - Dual Stack, Tunnel, Protokollumsetzung
  - weitere Lösungen zur Migration
  - weitere Techniken der Migrationsphase
- Migrationsszenarien der ÖV
- Zusammenfassung

Motivation

- IPv6 ist nicht abwärtskompatibel zu IPv4
  - Design-Entscheidung: Altlasten loswerden
  - Übergangstechniken wurden bei IPv6-Entwurf schon mitbetrachtet

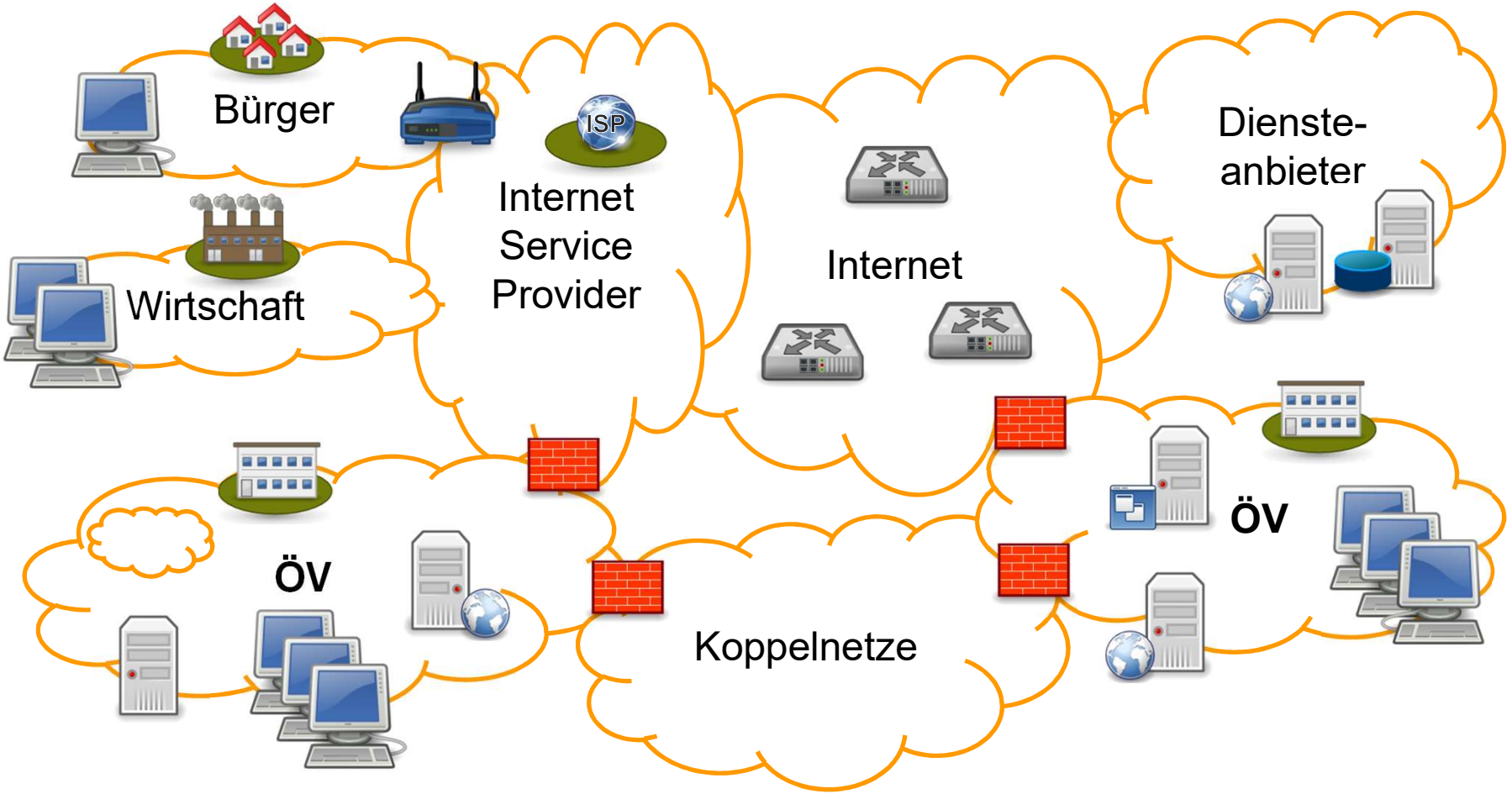
- IPv4 und IPv6
  - Kleine Unterschiede im Prinzip, Große in der Anwendung
  - gleiche *Art und Weise* der Adressierung,
    aber Adressraum bei IPv6 um *Größenordnungen* erweitert
  - vollständige Adressumsetzung (1:1) nicht möglich!



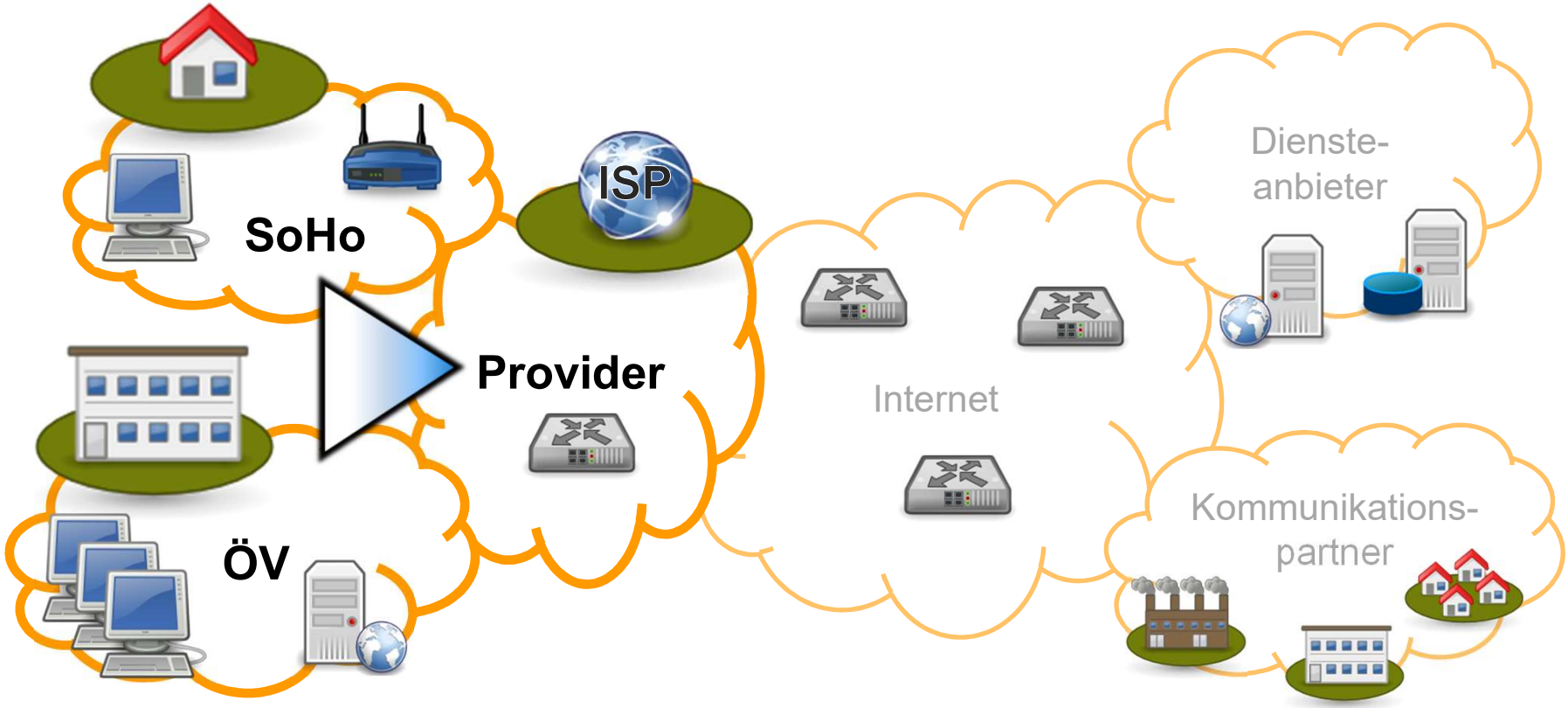
- Konsequenz: Übergangstechniken notwendig
  - Techniken und passende Anwendungsszenarien werden hier vorgestellt

- Sichtweisen: Intranet, Internet-Zugang und Auswirkungen durch Provider

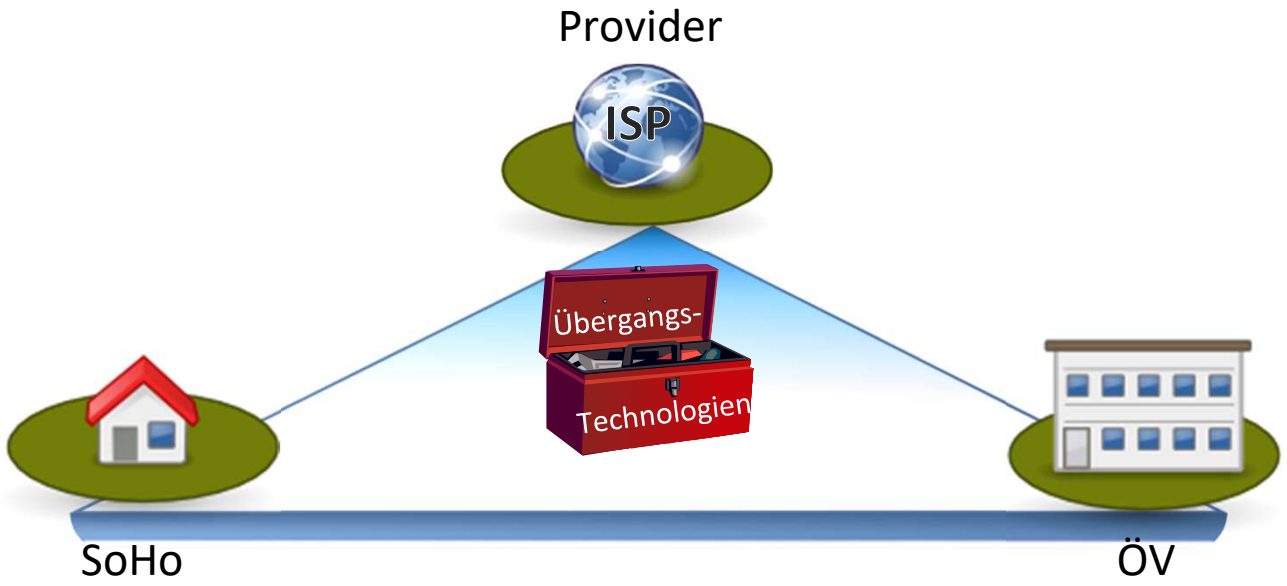
IPv6 kommt überall…



… auch bei Akteuren im Anschlussbereich



Sichtweisen der Akteure



- Auswirkungen von Übergangstechnologien auf Kunden des Providers (ISP)
  - Nutzbarkeit eingesetzter Technologie für Anwendungen der Kunden
- Rückwirkungen von Kunden auf ISP
  - IPv4- / IPv6-Verkehrsanteile beeinflussen direkt die Kosten des ISP

Ziel dieses Moduls

- Darstellung der relevanten IPv4/IPv6-Übergangstechniken
- Betrachtung je Einsatzgebiet
  - beim Provider (Anschlussbereich)
  - beim Endkunden (lokales Netz)
- Bewertung dieser Techniken & Analyse der Konsequenzen
  - bei Endkunden-Einsatz („SoHo“)
  - bei ÖV-Einsatz („Verwaltung“)
  - bei ISP-Einsatz (Auswirkungen auf Kunden) („Provider“)

- Darstellung ergänzender Verfahren, z. B. Carrier Grade NAT
- Warnung vor problematischen Verfahren:

Internet Service Provider (ISP)

- Verschiedene Provider-Typen
  - Traditionelle ISPs mit großem IPv4-Adressvorrat (z.B. Deutsche Telekom)
  - neue Anbieter, ggf. mit neuen Zugangstechniken (z.B. Kabelnetzbetreiber)

- Herausforderungen der Provider
  - nahtlose Umstellung („muss funktionieren“)
  - Investition in neue Systeme (beim Provider, ggf. beim Kunden)
  - unabhängig von IPv6 - Preisdruck auf Geschäftsmodell „reiner IP-Zugang“

- ÖV-Sicht: Unterschied Standard-Produkte / kundenspezifische Verträge
  - Standard-Produkte sind ggf. problematisch, da bei manchen Übergangstechniken der Datenverkehr der ÖV mitgelesen werden kann
  - mit kundenspezifischen Verträgen kann ein Provider auch sensible Techniken zur Dienstleistungserbringung nutzen

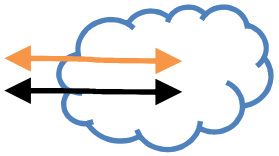
Motivationen der Provider

- Motivation für den Übergang IPv4 → IPv6 in kabelgebundenen ISP-Netzen
  - IPv4-Adressen sparen
  - IPv6 / private IPv4-Adressen für ISP-eigene Dienste („managed services“) nutzen
  - wirtschaftlich sinnvolle Übergangstechniken einsetzen

- Motivation für den Übergang und die Nutzung von IPv6 im Anwendungsgebiet Mobilfunk
  - vollwertiger Internet-Anschluss wird vom Kunden (noch) nicht erwartet
    - höhere Akzeptanz von Einschränkungen durch Übergangstechniken
  - „always on“ – permanente Erreichbarkeit / Nutzung der IP-Adresse
  - private IPv4-Netze reichen nicht aus (Class A ~16 Mio. IPv4-Adressen)

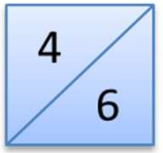
Verschiedene Ansätze für den Übergang

- Dual Stack („IPv4 und IPv6 parallel“)
  - Geräte sind über beide Protokolle gleichzeitig erreichbar, automatische / konfigurierbare Auswahl
  - physikalische Trennung oder Nutzung virtueller LANs

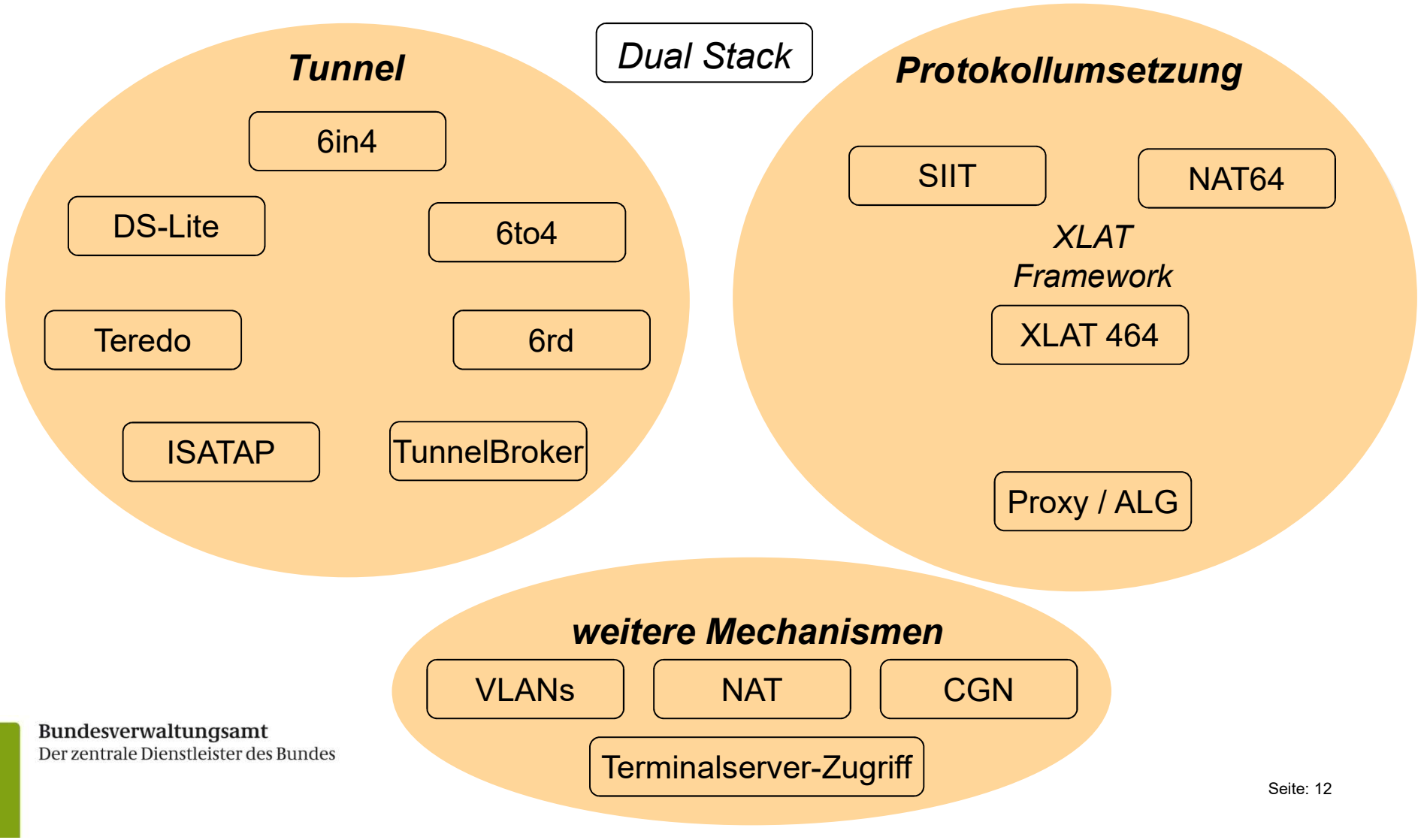


- Tunnel („Verbindung von IPv6-Inseln“)
  - Anbindung einzelner IPv4- bzw. IPv6-Inseln
  - Verbindung zwischen mehreren IPv4- bzw. mehreren IPv6-Inseln

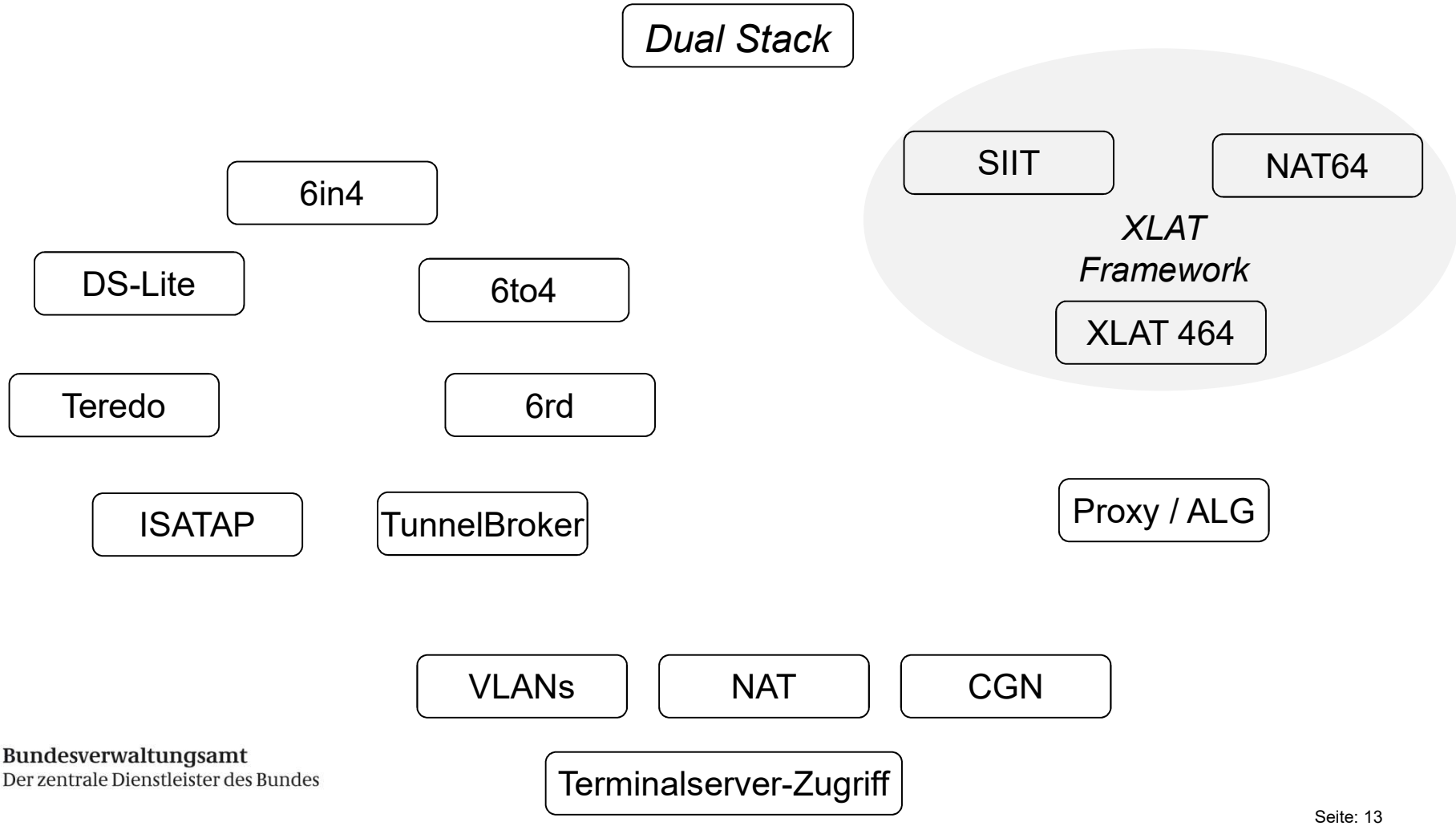
- Protokollumsetzung
  - auf Netzwerkebene: zwischen IPv4-only- und IPv6-only
  - auf höheren Ebenen: durch Application Layer Gateways (ALGs)



Übersicht Übergangstechniken



Übersicht Übergangstechniken - XLAT



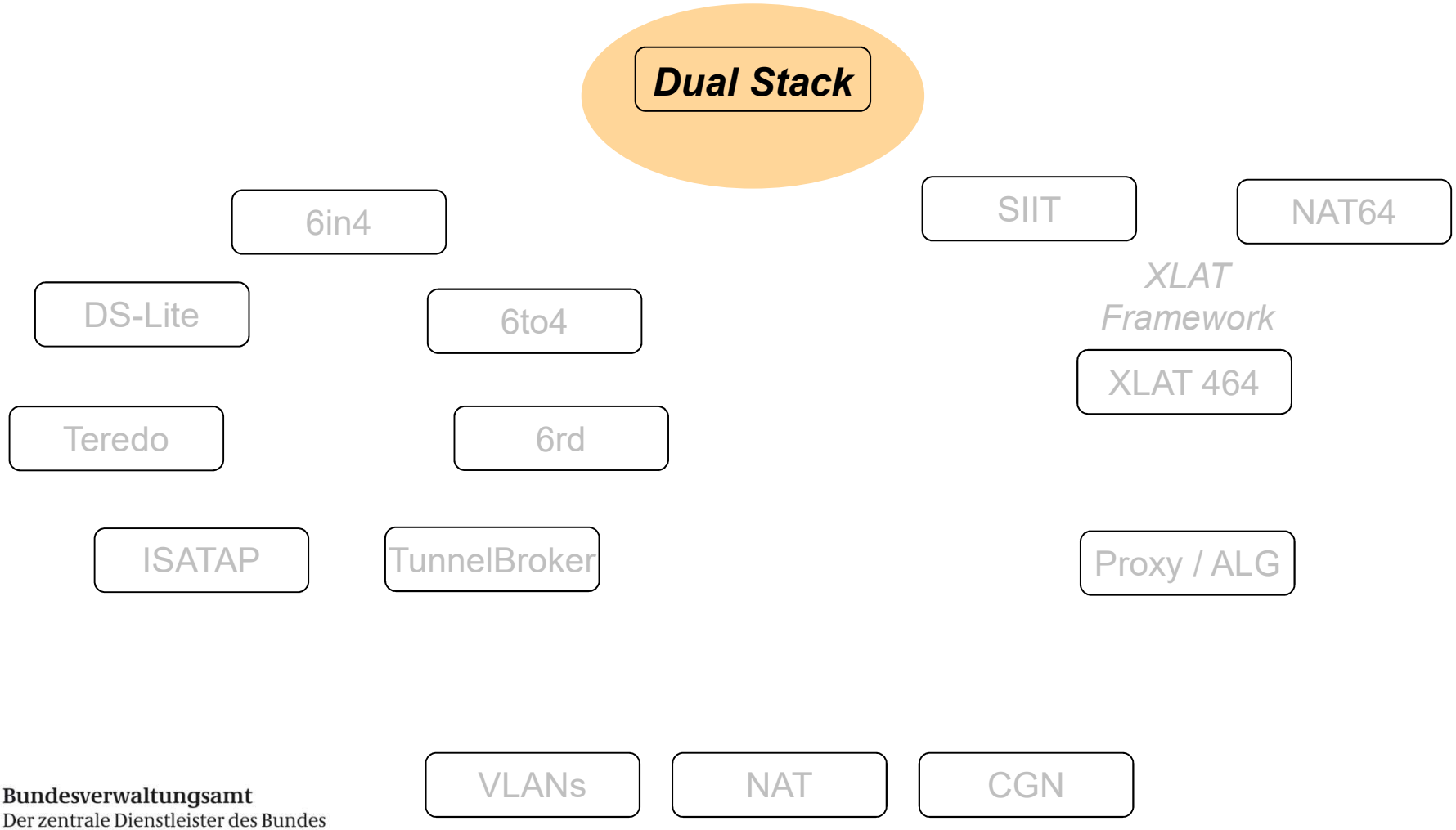
Anmerkung

- es gibt nicht „die eine“ ideale Umsetzung, sondern eine Reihe von Methoden
  - beispielhafte Vorstellung hier ohne Anspruch auf Vollständigkeit
  - Entwicklung neuer Kombinationen

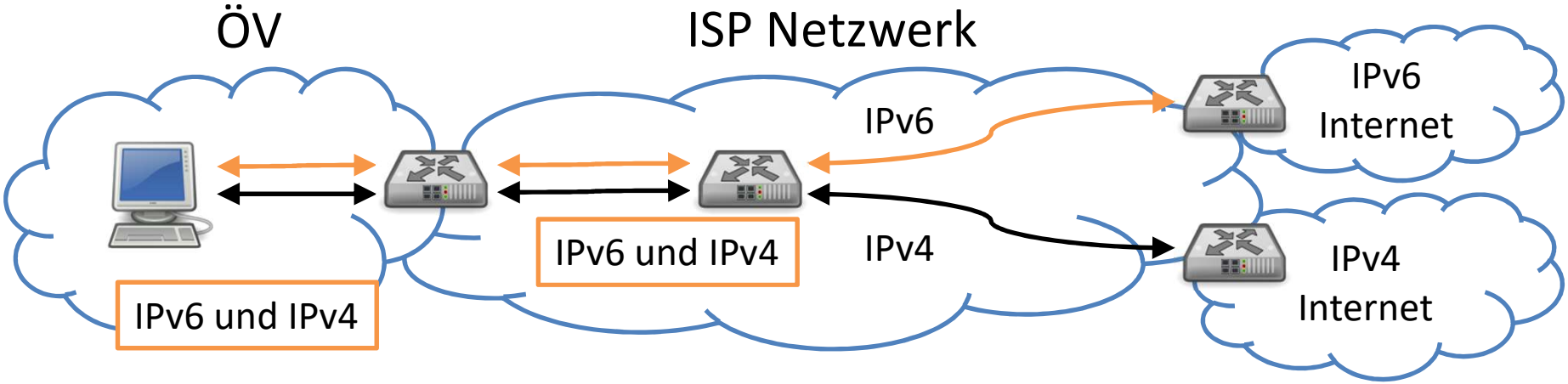
- typische Dilemmas (⤫), z. B. bei Protokollumsetzung:

Protokollumsetzung auf …		
Netzwerk-Schicht	theoretisch sehr universell, völlig unabhängig von Anwendungen	funktioniert nicht für alle genutzten Protokolle, (Einzelfallbetrachtung notwendig)
Anwendungs-Schicht	sehr zuverlässig für begrenztes Einsatzszenario, kann vorher getestet werden	nur für einzelne Anwendungen, Proxy muss vorher installiert sein

Übersicht Übergangstechniken – Dual Stack



Dual Stack - Mechanismus



- paralleler Betrieb von IPv4 und IPv6
- universeller Einsatz, im …
  - Intranet (bei Anwendungen, Servern, Arbeitsplätzen)
  - Internet-Zugang / beim Dienstangebot
  - Backbone (heute schon Standard)

Dual Stack - Details

- keine Übergangstechnologie im engeren Sinne, sondern Verbindung zwischen IPv4- und IPv6-Internet an Endsystemen (Endgerät, Server)
- Parallelbetrieb an Stelle von Interoperabilität zwischen IPv4 und IPv6
- Einbeziehung aller Infrastruktur-Komponenten nötig
- Ziel: alle Systeme werden mit / für beiden Versionen auf Schicht 3 (Netzwerkschicht, „IP-Layer“) betrieben
  - Anwendung oberhalb IP davon unabhängig, bspw. über TCP, HTTP

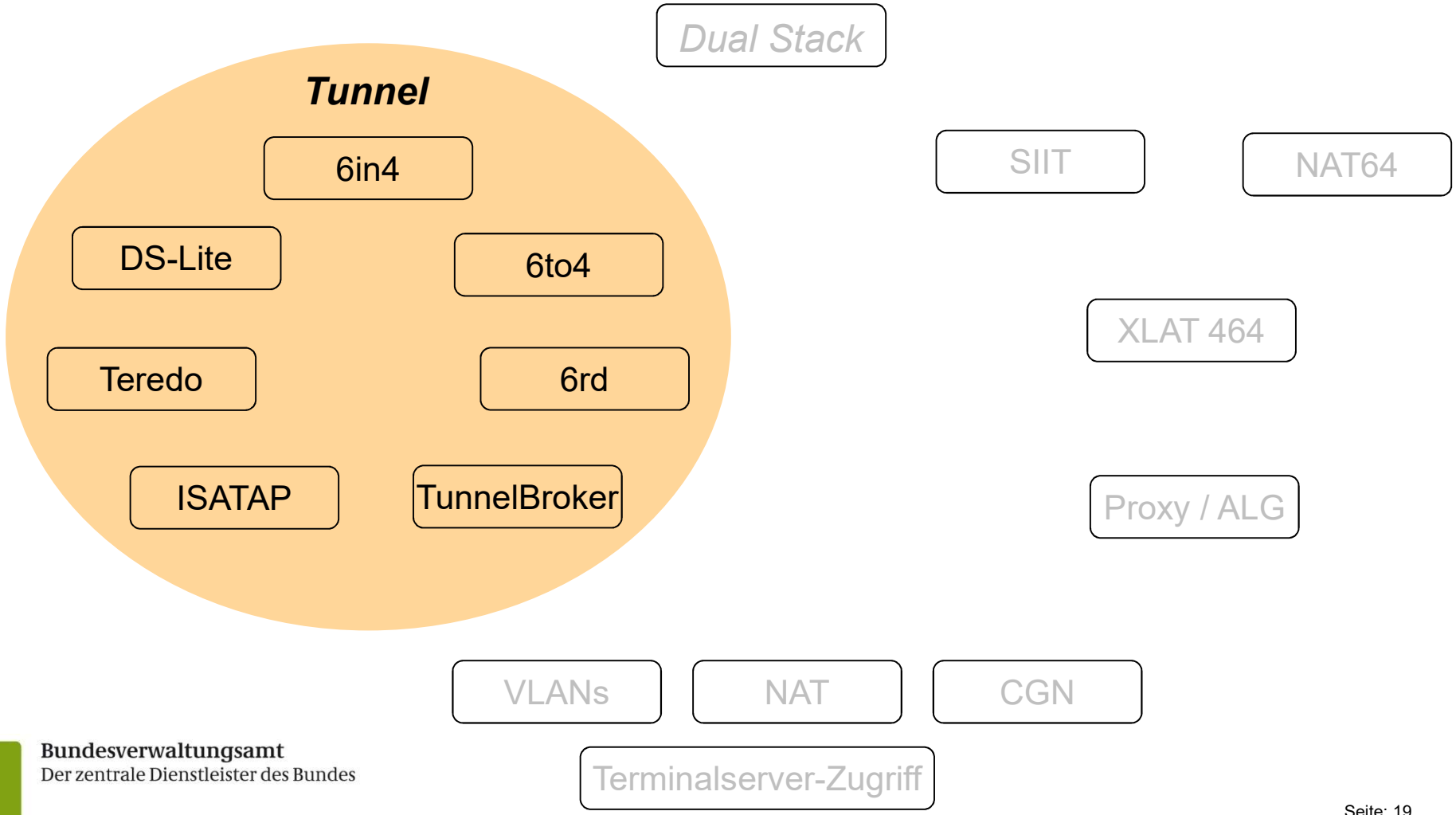
- Beim Netzwerk-Management ggf. noch IPv4- / IPv6-only Nutzung möglich
  - bei Einsatz von IPv6 sind die IPv6-MIBs nötig

- Auswahl IPv4/v6 durch Betriebssystem bzw. Anwendung, z. B. Browser
  - genutzte IP-Version im Einzelfall nicht immer vorhersehbar

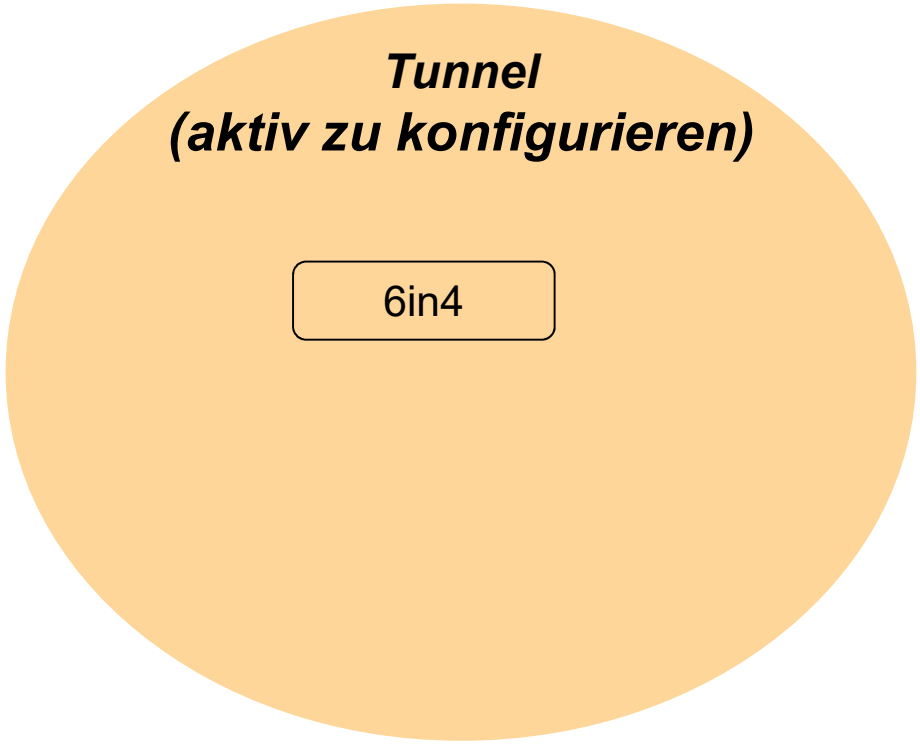
Dual Stack - Bewertung

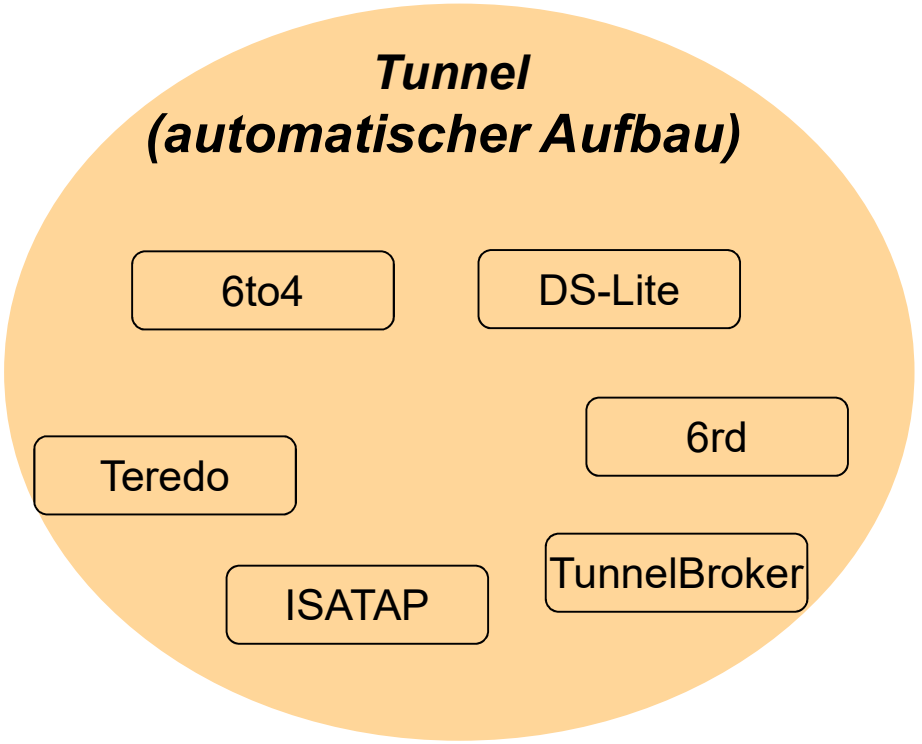
- schrittweise Einführung möglich → Orientierung an Netzgrenzen
  - bis Dienstangebot (Web-Server) oder bis Proxy / ALG
- sauberer Netzaufbau nötig, da sonst Sicherheitslücken entstehen
  - Zuschnitt von Sub-Netzen in IPv6 orientiert an IPv4
    → vergleichbare, übersichtliche Zugriffssteuerung (ACLs)
  - Chance für optimierte Strukturen mit IPv6-only
- Basisinfrastruktur muss komplett verfügbar sein
  - Verschlechterung von Antwortzeiten bei Ausfall von IPv6 möglich
    - wenn IPv6-Verbindungsversuch scheitert, IPv4-Nutzung erst nach Timeout
  - Migrationsreihenfolge muss beachtet werden (Netze, Geräte)
  - Auswahl der Protokollversion pro Verbindung nicht immer transparent
- **Nutzbarkeit**: sowohl für ISP, ÖV und Endkunden sinnvoll
  - verringerter Aufwand durch *Teilmigration* ausgewählter Subnetze

Übergangstechniken - Tunnel

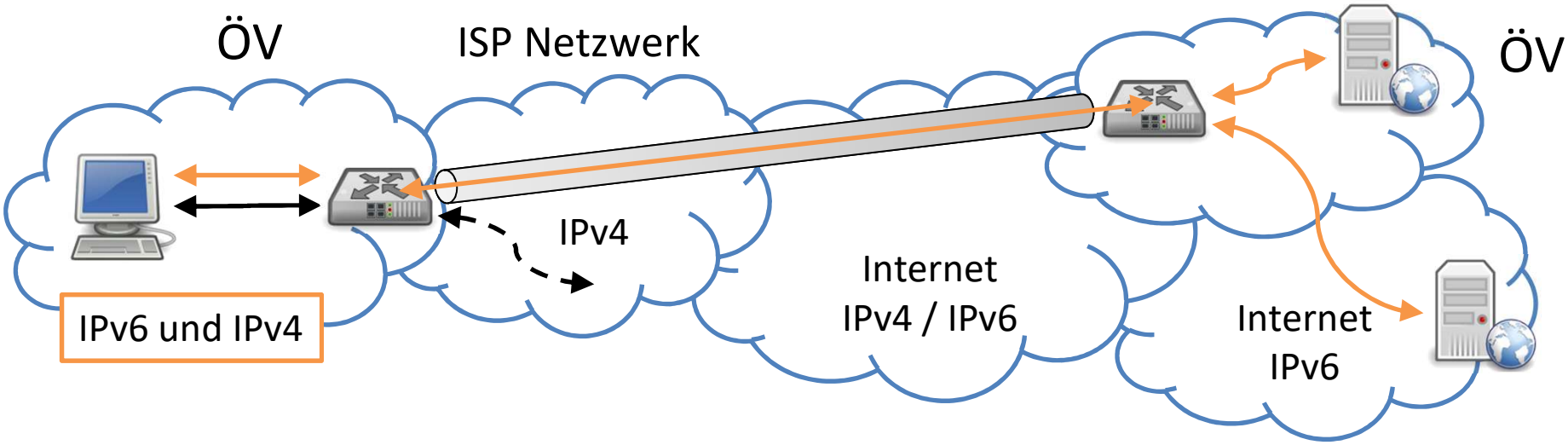


Tunneltechniken





6in4 – Mechanismus



- Übertragung von IPv6-Pakten über ein IPv4-Netz
- Konfiguration statischer Tunnel: einfach, eindeutig, aber skaliert nicht
- Statischer Tunnel, wird auch von einigen → Tunnelbrokern verwendet

6in4 – Details

- RFC 4213 – Basic Transition Mechanisms for IPv6 Hosts and Routers
- Technisch sehr einfach:
  - direkt auf den IPv4-Header folgt das IPv6-Paket
  - als Protokollnummer im IPv4-Header wird 41 verwendet
- Endpunkt kann Router oder Host sein

- mögliche Probleme:
  - Max. Paketgröße (MTU)
    durch den zusätzlichen IPv4-Header wächst die Paketgröße
  - NAT (Network Address Translation)
    ggf. muss Paket Forwarding umkonfiguriert werden

- ähnliche Möglichkeiten
  - GRE – Generic Router Encapsulation (CISCO)
  - AYIYA – Anything In Anything
    umgeht das NAT-Problem, wird daher von dem Tunnelbroker SixXS verwendet

6in4 – Bewertung

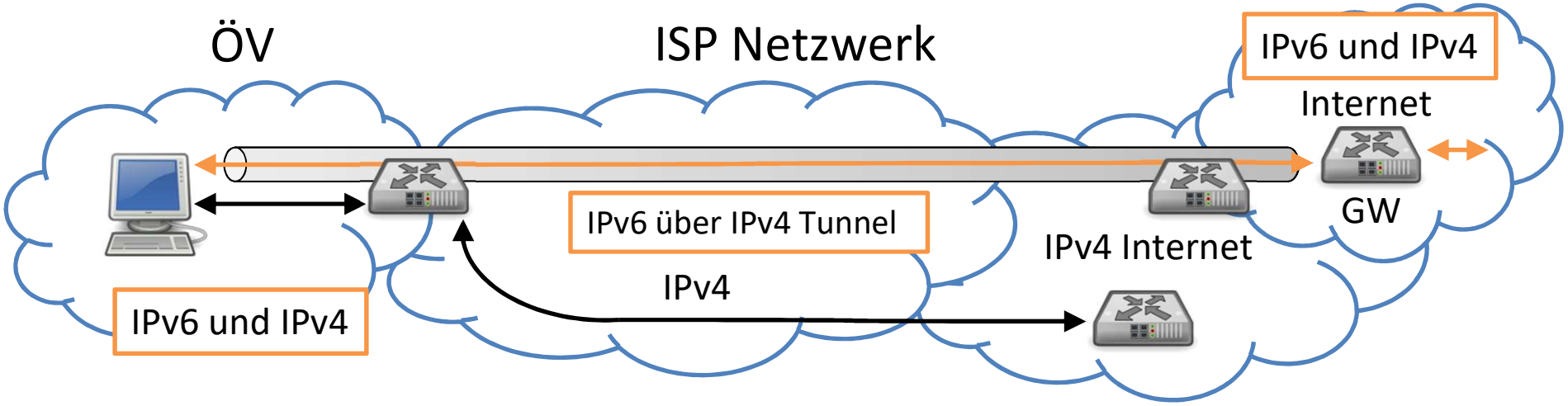
- Statischer Tunnel
  - keine Verschlüsselung oder weitere Sicherheitseigenschaften
  - manuelles Management
    - Übersichtlich für die einzelne Kopplung zwischen Routern
    - zu komplex in großen Szenarien, ggf. NAT-Probleme bei Endnutzern
- Transparent über verschiedene IPv4-Netze, ggf. nicht über Middleboxes

Management zu aufwendig, statt dessen Verwendung von automatischen Tunneln durch Tunnelbroker-Konzept

einfachste Möglichkeit zur Verknüpfung von IPv6-Inseln, über beliebige (IPv4-)Infrastrukturen dazwischen

IPv4-Pakete werden transparent weitergeleitet, normalerweise kein Einfluss durch den ISP

6to4 – Mechanismus



- Verbindung Dual-Stack-fähiger Klienten über Gateways ins IPv6-Internet
- Gateway im Internet wird aus einem öffentlichen Pool gewählt
- keine IPv6-Unterstützung beim Provider (ISP) notwendig

6to4 – Details

- RFC 3056 – Connection of IPv6 Domains via IPv4 Clouds
- Host oder Router baut Tunnel zu öffentlichem Gateway auf

- Adressierung:
  - Öffentliche IPv4-Adresse wird auf /48 IPv6-Netz abgebildet
  - IPv6-Adresse mit Präfix 2002 und hexadezimal notierter IPv4-Adresse

http://commons.wikimedia.org/wiki/File:6to4_adresse.png

- Transport:
  - IPv6-Paket wird über Tunnel an 6to4-Relay geschickt
  - Rückweg nicht zwingend über das gleiche Relay (öffentliche IPv4-Adr.)

- Sicherheitshinweise in RFC 3964 – Security Considerations for 6to4

6to4 – Bewertung

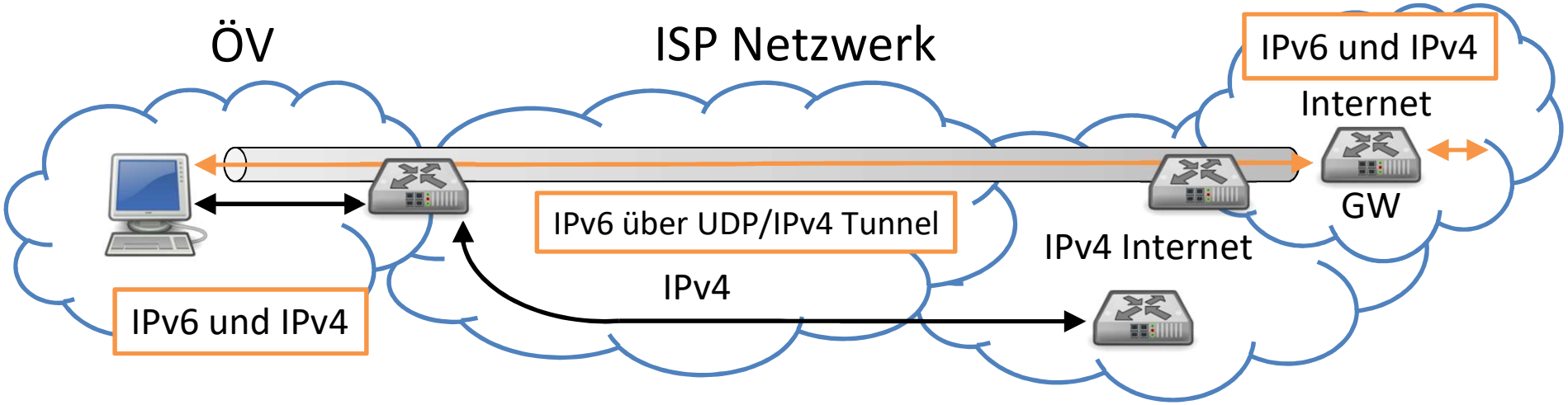
- Sicherheit bei 6to4 als kritisch zu betrachten, da Gateway im Internet „zufällig“ ausgewählt wird und daher nicht unter Kontrolle der ÖV ist
- schlechte Performance für IPv6 möglich,
  - je nach Auswahl des Gateways, z. B. bei großer Entfernung von ÖV
- 6to4 ist anfällig für Angriffe
  - eingehender Verkehr wird aufgrund des Protokolls von beliebigen 6to4-Gateways im Internet akzeptiert

„Notlösung“, wenn keine andere (Tunnel-)Technik einen notwendigen Zugang zum IPv6-Internet ermöglicht

Da 6to4 hier ein Sicherheitsrisiko darstellt: keinesfalls nutzen!

leitet 6to4-(Tunnel-)Verkehr üblicherweise durch, verwenden die Technik aber selbst nicht

Teredo – Mechanismus



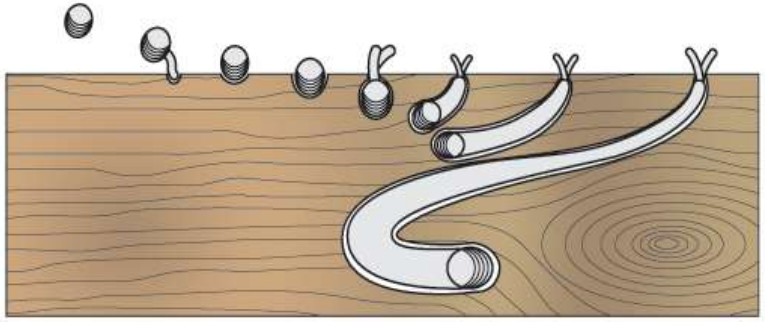
- Klienten bauen Tunnel auf, mithilfe von öffentlichen Teredo-Servern
- keine IPv6-Unterstützung im ÖV-Intranet nötig, nur auf den Klienten
- nutzt öffentlichen Tunnelendpunkt („Teredo-Relay“) im IPv6-Internet

Teredo – Details

- RFC 4380 – Teredo:
  Tunneling IPv6 over UDP through Network Address Translations (NATs)
- speziell für PCs in privaten Netzen hinter NAT, Verwendung von UDP
- Gegenseite im IPv6-Internet: Öffentliche Teredo-Server

- Zweck: Nutzung von automatischem Tunnel, wenn sonst kein IPv6 vorhanden ist
- Problem: Firewall im (DSL-) Router wird wirkungslos / durchtunnelt, Endsystem steht dann ohne Schutz im IPv6-Internet
- Empfehlung an Systemadministratoren: UDP-Port 3544 sperren

- Juli 2013:
  - Microsoft testet Teredo-Abschaltung
    (Quelle: http://heise.de/-1916499)
  - Xbox One verwendet weiterhin Teredo



http://commons.wikimedia.org/wiki/File:Schiffsbohrwurm_bohrt.png

Teredo – Googles Sicht

http://www.google.de/ipv6/statistics.html, Abruf: 18.8.2013

Teredo – Bewertung

- Klienten bauen selbstständig Verbindungen auf, das ist kritisch, da ….
  - zentrale Filter- und Schutzmechanismen können ausgehebelt werden
  - fremde Systeme (hinter Teredo-GW) erhalten ggf. Zugriff ins Intranet

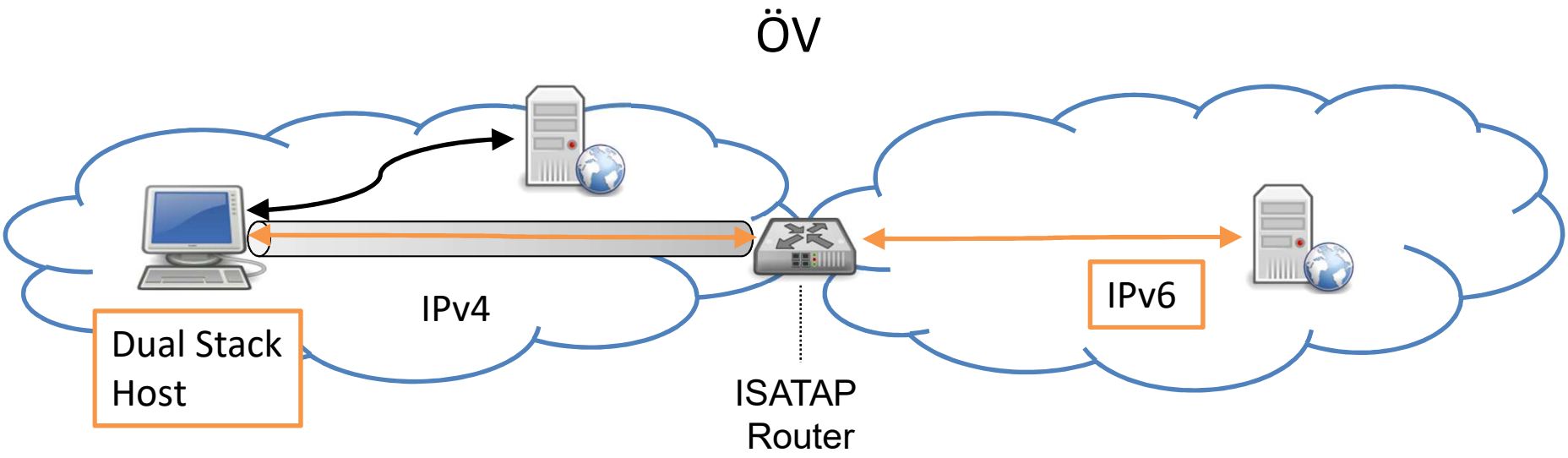
„Notlösung“, wenn keine andere (Tunnel-)Technik
einen notwendigen Zugang zum IPv6-Internet ermöglicht

hebelt u. U. Sicherheitsmechanismen aus:

- Sicherheitsrisiko - keinesfalls nutzen!
- im Betriebssystem abschalten, in Infrastruktur Port blockieren

leitet Teredo-(Tunnel-)Verkehr üblicherweise durch,
verwendet die Technik aber selbst nicht

ISATAP – Mechanismus



- Nutzung innerhalb einer Organisation
  - wenn Netze noch nicht Dual-Stack-fähig sind / wenige Hosts existieren
- Nutzung von IPv4 als Link Layer für IPv6
  - darüber dann Neighbor Discovery, um Router für Host zu konfigurieren
- IPv6-Adresse wird aus der lokalen IPv4-Adresse gebildet

ISATAP – Details

- RFC 5214 – Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- Nutzung eines speziellen EUI-64-Formats, das von ISATAP-Komponenten erkannt wird
  - IPv4-Adresse ist in Interface Identifier enthalten:
    `FE80::5EFE:<IPv4-Adresse>` (für private IPv4-Adressen)
- Vorteil: Es wird kein Multicast im IPv4-Netz benötigt (vgl. 6over4)
- Neigbor Discovery wird anders verwendet, da kein Multicast verfügbar
  - Auffinden der Router über DNS über **`isatap.example.com`**
  - Router werden direkt angesprochen, ob sie verfügbar sind

ISATAP – Bewertung

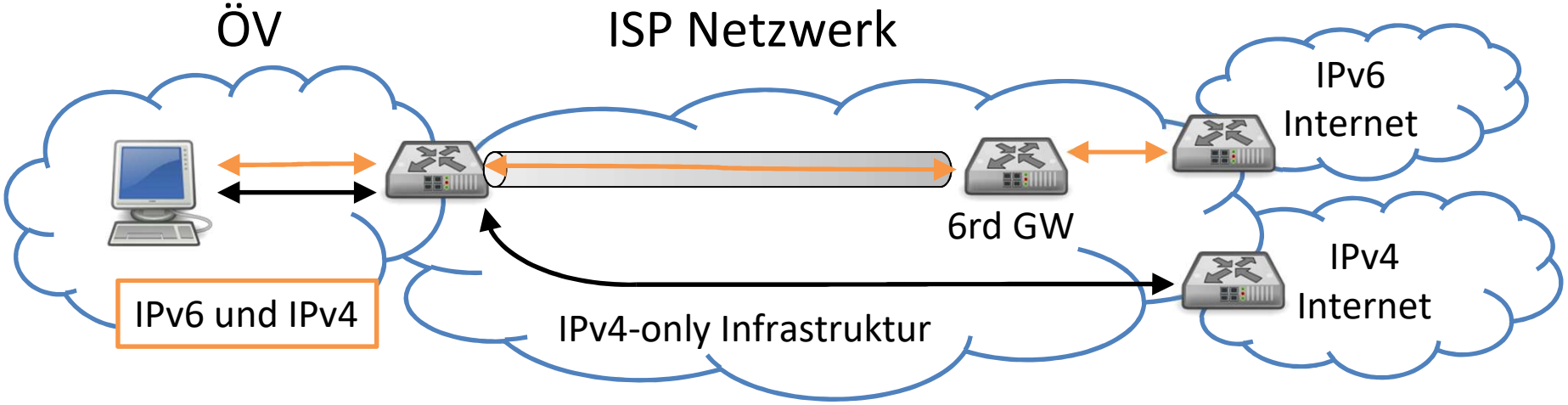
- Methode zum Betreiben weniger Dual-Stack-Hosts in einer IPv4-Umgebung
  - Einsatz während der frühen Phase der IPv6-Migration
- inzwischen sind ausreichend Dual-Stack-Netzwerk-Komponenten verfügbar
  - Empfehlung: wo *IPv4 und IPv6* benötigt werden Dual-Stack verwenden

nicht verwendbar für einzelne oder kleine lokale Netze

sollte nicht verwendet werden

nicht üblich / keine Auswirkung

6rd: IPv6 Rapid Deployment – Mechanismus



- Provider-Technologie: Kunden bekommt IPv6 über IPv4-Infrastruktur des Providers
  - Weiterentwicklung von 6to4: *GW jetzt im Providernetz*, nicht öffentlich
- Entwicklung des französischen Providers „free“
  - kurze Einführungszeit, war deutlich sichtbar in der Google-IPv6-Statistik für Europa

http://www.google.de/ipv6, Januar 2013

6rd – Details

- RFC 5969 – IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification

- Providertechnologie
  - Kunde bekommt IPv6 über eine bestehende IPv4-Infrastruktur
    - Schnelles Ausrollen von IPv6 durch den Provider möglich
  - Kunde behält IPv4 und bekommt (eingeschränktes) IPv6
    - IPv6 wird zum Kunden über IPv4 getunnelt

- 6rd basiert auf der Idee von 6to4
  - IPv6-GW stehen unter Kontrolle des Providers
  - Nutzung der IPv6-Adressen des Providers → verbesserte Erreichbarkeit

6rd – Bewertung

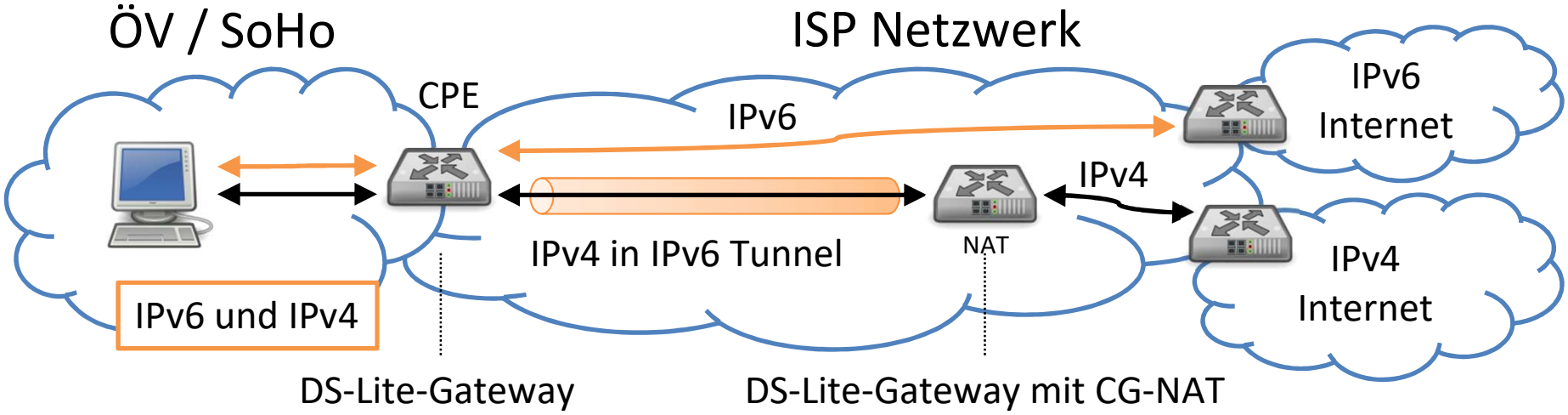
- Provider-Technik, spielt innerhalb einer ÖV keine Rolle
- ermöglicht es ISP, IPv6 anzubieten, ohne nativen IPv6-Support
- aus Sicht des Kunden (ÖV) „so gut wie natives IPv6“, wenn alles funktioniert
  - Vorteil zu 6to4: 6rd-GWs sind unter Kontrolle des Providers
- nicht optimal, da IPv6-Pakete im ISP-Netzwerk getunnelt werden
  - besser den Provider dazu bewegen, natives IPv6 anzubieten

wird nicht lokal genutzt, dort Dual-Stack oder IPv6-only
ermöglicht Zugang zu IPv6 über den Provider

wird nicht im Intranet genutzt; bei Nutzung beim Provider: ggf. langsamerer Zugang zu ext. IPv6-Netzen mit nativem IPv6
keine Nutzung des Adresspools der LIR *de.government* möglich

kann 6rd als Brückentechnologie anbieten, Vorteile für die Kunden

DS-Lite – Mechanismus



- Provider-Technologie: Kunden bekommt IPv6 und eingeschränktes IPv4
  - IPv6 wird nativ vom Provider zur Verfügung gestellt, wie bei Dual-Stack
  - IPv4 über Carrier Grade NAT bereitgestellt, Einschränkung zu Dual-Stack

DS-Lite – Details

- RFC 6333 – Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

- Providertechnologie:
  - Kundenanschluss (CPE) verwendet nur IPv6 auf Providerseite
    - Vereinfachung des Management des Anschlusses
  - Kunde bekommt IPv6 und (eingeschränktes) IPv4
    - IPv4 für Kunden verfügbar, auch bei knappen IPv4-Adressraum des Providers
  - Provider setzt Carrier Grade NAT (CGN) ein
    - erhöhter Aufwand beim Provider, technologische Sackgasse

- CGN: Qualitätsnachteile für den IPv4-Internet-Zugang
  - Erreichbarkeit von außen nicht ohne weiteres möglich (→ Port Forwarding)
  - Teilen einer IPv4-Adresse kann Qualität verschlechtern
    (insbesondere bei hoher Anzahl von TCP-Verbindungen mehrerer Nutzer)

DS-Lite – Bewertung

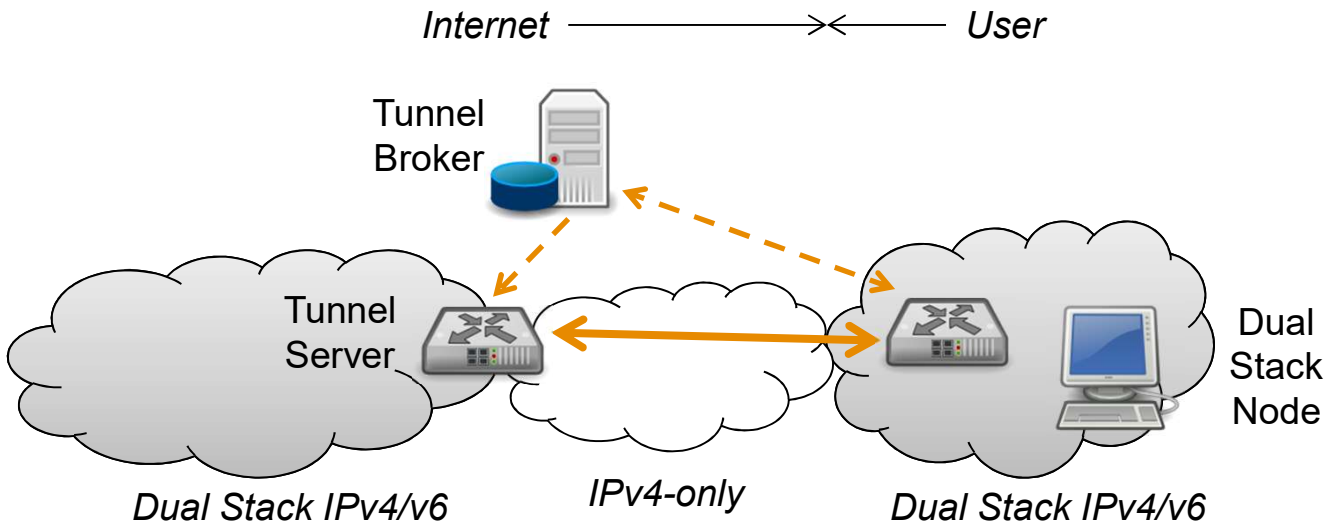
- allgemein: DS-Lite ist eine Providertechnik mit nativem IPv6 und geteiltem IPv4, um die Zahl der genutzten öffentlichen IPv4-Adressen zu reduzieren
- Carrier Grade NAT Einsatz beim Provider
  - Nachteile für den Kunden (IPv4-Erreichbarkeit von außen, Qualität)

Endkunde kann IPv4 und IPv6 von einem ISP bekommen, der DS-Lite nutzt; Endkunde nutzt lokal dann Dual-Stack

statt DS-Lite besser natives IPv4 und IPv6 vom Provider verlangen, da DS-Lite (durch Nutzung von CG-NAT) einen schwerwiegenden Eingriff in IPv4 bedeutet

kann DS-Lite nutzen, bei vorhandener IPv6-Infrastruktur

Tunnel Broker – Mechanismus



- Ziel: Konfiguration eines IPv6-in-IPv4-Tunnels
- Tunnel Broker übernimmt für Nutzer Aushandlung und Aufbau des Tunnels
- Tunnel wird zwischen einem Knoten beim Nutzer (Netzwerk oder Endsystem) und einem Tunnel-Server beim Tunnel-Anbieter aufgebaut

Tunnel Broker – Details

- RFC 3053 – IPv6 Tunnel Broker
- Bestandteile des Tunnelbrokers
  - Tunnel Broker – Zugangskontrolle und Konfiguration
  - Tunnel Server – Dual-Stack-Knoten als Tunnel-Endpunkt in IPv6

- Tunnel Setup Request läuft zwischen
  Klient (Gateway oder Perimeter-Router) und Tunnel Broker
- nutzt TSP (Tunnel Setup Protocol), TIC (Tunnel Information and Control Protocol) oder webbasierten Zugriff
- benötigt starke Absicherung (AAA + Transportverschlüsselung),
  damit keine „ungewollten Gäste“ Tunnel über den Broker aufbauen können
- Option:
  TLS für Transport Security, LDAP und signierte Client-Zertifikate für AAA

Tunnel Broker – Bewertung

- Übergangstechnik zur Erleichterung der Migration zu IPv6, wenn …
  - … IPv6 (Dual Stack) bei eigenem Provider noch nicht verfügbar ist und
  - … Erfahrungen im lokalen (Test-)Netz gesammelt werden sollen oder
  - … gleichartige IPv6-Komponenten frühzeitig genutzt werden sollen.
- Vorteil: Beschleunigung der Migration durch Parallelisierung, Aufbau und Nutzung von IPv6 können bereits vor dem nativen IPv6-Zugang starten.

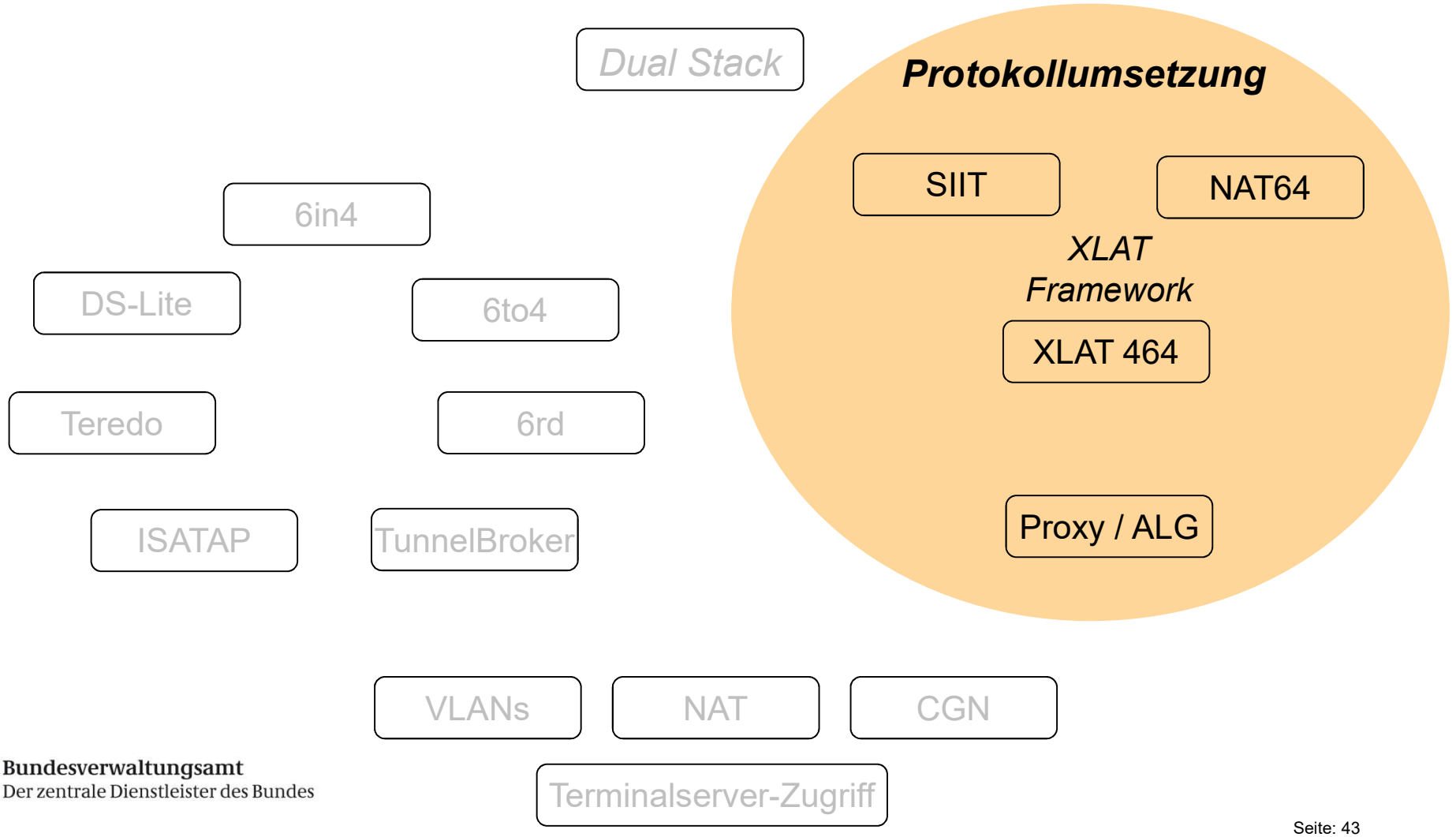
Zielgruppe des Konzepts Tunnelbroker –
kleineren Einheiten wird ein Zugang zu IPv6 ermöglicht

Angebot von Tunnelbroker durch ÖV / Dienstleister (RZ) als Dienstleistung

- sicherer Zugang zu IPv6 für SoHo oder kleinere ÖV
- beschleunigte Einführung von IPv6

kann diesen Dienst anbieten (bekannte Anbieter: SixXS, Hurricane Electric)

Übergangstechniken - Protokollumsetzung



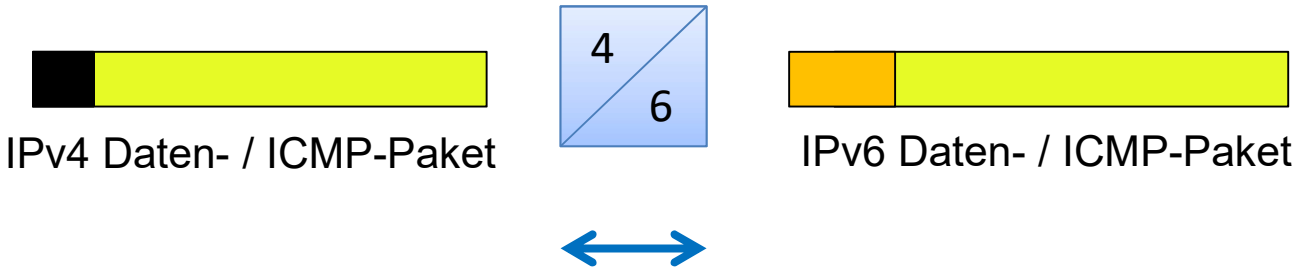
Protokollumsetzung

- Protokollumsetzung
  - auf Netzwerkschicht:
    - SIIT, NAT64, XLAT
  - (auf Transportschicht)
  - auf Anwendungsschicht:
    - Proxy, Reverse-Proxy

universelle Protokollumsetzung schwierig, daher wird Umsetzung auf verschiedenen Protokollschichten genutzt

- ohne Protokollumsetzung
  - Dual-Stack
    - vermeidet Protokollumsetzung, stattdessen Parallelbetrieb
    - Betriebssystem / Anwendung sucht passende IP-Protokoll-Version aus

SIIT – Mechanismus



- Verfahren zur Umsetzung von IPv6- und IPv4-Header-Feldern
  - bidirektionale Umsetzung zwischen IPv4 ←→ IPv6 (stateless)
  - Schwierigkeit: Checksummen in Protokollen, Informationsverlust

- Netzwerk-Präfix oder „Well-Known Prefix“: **`64:ff9b::/96`**
  `192.0.2.33` → `64:ff9b::192.0.2.33`
  - Präfix ist neutral in Bezug auf die Checksumme des Transportprotokolls

SIIT – Details

- RFC 6145 – IP/ICMP Translation Algorithm
  (die aktuelle Version, siehe nächste Seite für vorherige RFCs)
- RFC 6052 – IPv6 Addressing of IPv4/IPv6 Translators

- Beschreibung der Umsetzung einzelner Header-Felder in die jeweils andere Protokollversion, Beispiel:

Version	6
Traffic Class	TOS-Feld
Flow Label	0
Payload Length	Länge_aus_IPv4-Header - (IPv4-Header + IPv4-Options)
…	

Adressumsetzung gemäß RFC 6052

- Umsetzung von ICMP-Paketen, ggf. neue Transport Layer Checksum nötig

SIIT – Grundlagen

- SIIT wird als Baustein für die Protokollumsetzung verwendet, meist in Verbindung mit anderen Techniken

- ein Mechanismus des XLAT-Frameworks
  - RFC 6144 – Framework for IPv4/IPv6 Translation

- erster Ansatz war Verfahren „NAT-PT“
  - RFC 2765 – Stateless IP/ICMP Translation Algorithm (SIIT)
  - RFC 2766 – Network Address Translation - Protocol Translation (NAT-PT)
    - Umsetzung von IPv6-only Netz zur Erreichbarkeit der IPv4-Welt
  - RFC 4966 – Reasons to Move … (NAT-PT) to Historic Status
    - Gründe, u.a.: NAT-typisch (IP-Adressen innerhalb des Protokolls werden nicht behandelt), komplexes DNS (DNS ALG fängt IPv6-DNS-Anfragen ab und setzt sie um)

SIIT – Bewertung

- SIIT ist ein Baustein bei der Protokollumsetzung
  - in Kombination mit anderen Verfahren (→ XLAT464)
  - meist manuell konfiguriert
    (z. B. IPv4-Adresse des Geräts, Adressbereiche für die Umsetzung)

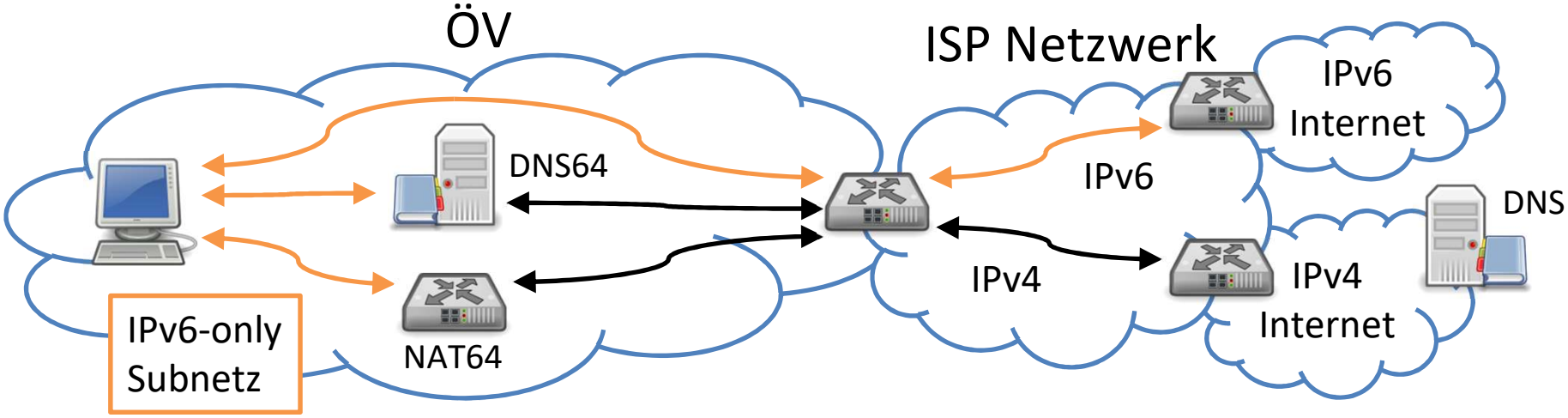
für SoHo-Intranets zu komplex

- keine Notwendigkeit aufgrund niedriger Anzahl gleichartiger Systeme
- Keine Einschränkung bei Einsatz von SIIT bei Provider zu erwarten

möglicher Baustein für die Migration in Rechenzentren und bei Providern

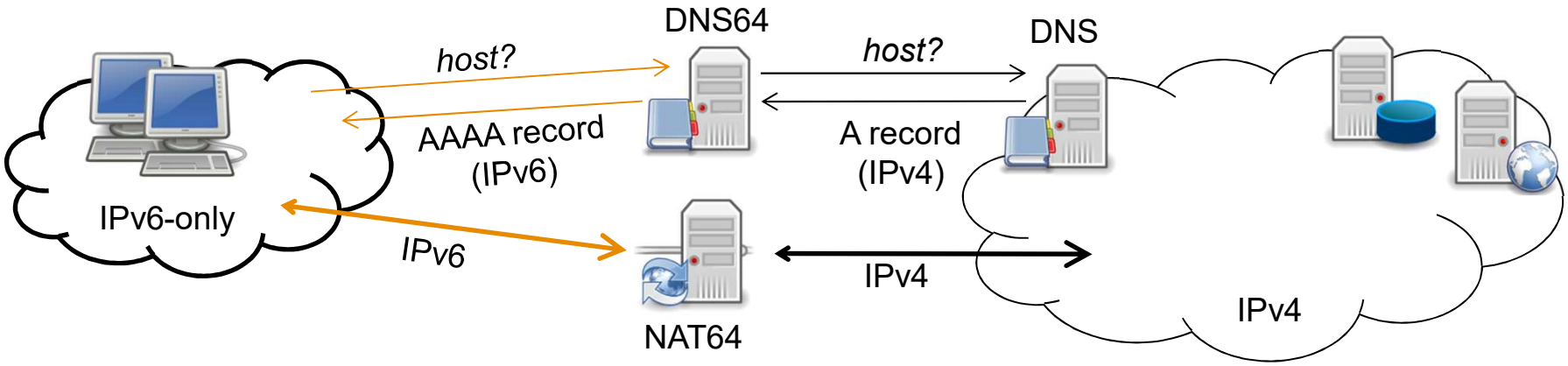
- Vorteil „stateless“-Umsetzung: Skalierbarkeit, Load Balancing möglich
- sinnvoll nutzbar, wenn Szenario Umsetzung auf IP-Schicht erlaubt

NAT64 – Mechanismus 1/2



- Technik, die Endsystemen in (neuen) IPv6-only Umgebungen erlaubt, zusätzlich auch auf IPv4-Systeme im Intranet und Internet zuzugreifen
- funktioniert nur mit Diensten, welche sich über Namen (URI/URL oder Hostname) ansprechen lassen, nicht bei nur numerischer IPv4-Adresse
- benötigt zwingend einen DNS64-Server und NAT64-Gateway im Intranet

NAT64 – Mechanismus 2/2



- Umsetzung von IP-Adressen:
  - IPv6-Adresse kann IPv4-Adresse komplett enthalten (Hinweg)
  - Zuordnung IPv4- zu IPv6-Adresse muss gespeichert werden (Rückweg)
- Grundlage: Verwendung von DNS-Namen
  - Bildung eines künstlichen AAAA-Eintrag (aus A-Eintrag)

NAT64 – Details

- RFC 6146 – Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers

- Einbettung der IPv4-Adresse in eine IPv6-Adresse
  - reserviertes Präfix für IPv6-Adressen: **`64:ff9b::/96`**

    `192.0.2.1` → **`64:ff9b::192.0.2.1`**
  - umgekehrte Zuordnung nicht eindeutig, daher muss die NAT-Funktion über die Verbindungen Buch führen (stateful NAT notwendig)

- Ablauf für Zugriff auf IPv4-only Dienst im Internet:
  1. Anfrage von IPv6-Endgerät nach einer Adresse über DNS
  2. lokales DNS64 setzt öffentliche IPv4-Adresse in IPv6-Adresse um
  3. Endgerät nutzt gebildete IPv6-Adresse
  4. NAT64 setzt Adresse nach IPv4 um, verwendet nur eine IPv4-Adresse

NAT64 – Bewertung

- allgemein: Zugriff für IPv6-only-Endsysteme auch auf IPv4-Systeme außerhalb des IPv6-only-Netzbereichs

für SoHo-Intranets zu komplex, universelle Umsetzung nicht garantiert

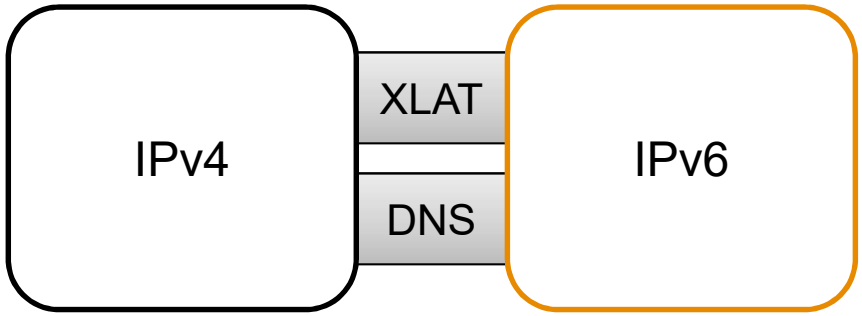
- Nutzung von Dual-Stack

gute Technik für neu geplante, aufzubauende IPv6-only-Teilnetze

- verringert ggf. Aufwand zur Pflege dieser Teilnetze (nur IPv6)
- Aufbau von IPv6-only-Teilnetzen noch kritisch,
  da IPv4-Dienste nicht mehr zu 100% funktionieren (z. B. NAT-Probleme)
  → Im Zweifelsfall besser Dual-Stack nutzen
- außerdem nützliche Technik zum Ansprechen von IPv4-Altsystemen

Technik wird alleine in Providernetzen nicht genutzt (→ XLAT464)

XLAT Framework



- XLAT Framework: Systematische Betrachtung der IP4/IPv6-Umsetzung
- 4 Fälle
  a. IPv6 Netz – IPv4 Internet
  b. IPv4 Netz – IPv6 Internet
  c. IPv6 Netz – IPv4 Netz
  d. IPv6 Internet – IPv4 Internet
- 2 Möglichkeiten, welche Seite die Kommunikation initiiert

} 8 Szenarien

XLAT-Szenarien

- RFC 6144 – Framework for IPv4/IPv6 Translation

- Szenarien (*grau – weniger relevant*):
  1. von IPv6-Netz ins IPv4-Internet – z.B. neuer IPv6-only Provider
  2. vom IPv4-Internet in ein IPv6-Netz – z.B. neuer IPv6-only Dienstanbieter
  3. vom IPv6-Internet in ein IPv4-Netz – z.B. bestehende IPv4-Dienste
  4. *vom IPv4-Netz ins IPv6-Internet – z.B. Weiterbetrieb IPv4 aufgrund technischer / ökonomischer Gründe*
  5. von IPv6-Netz in IPv4-Netz – z.B. innerhalb Organisation, wie 1.
  6. von IPv4-Netz in IPv6-Netz – z.B. innerhalb Organisation, wie 2.

  7. *vom IPv6-Internet ins IPv4-Internet – „Idealfälle der Umsetzung“…*
  8. *vom IPv4-Internet ins IPv6-Internet – (Adressbereiche zu unterschiedlich)*

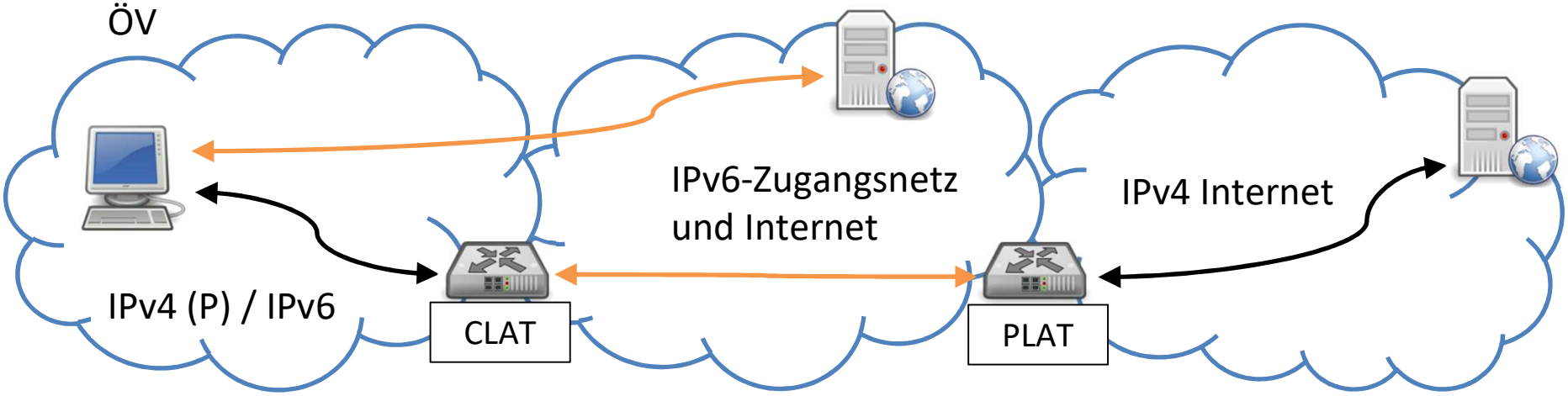
  … ergeben leider technisch und wirtschaftlich keinen Sinn

XLAT-Techniken

- Umsetzung zwischen IPv4 und IPv6-Adressen

- Stateless NAT64 / SIIT, siehe RFC 6145
  - Initiierung der Kommunikation von IPv4 oder IPv6-Seite
  - keine Zustandsinfo zu Verbindung oder Session, Behandlung per Paket
- Stateful NAT64, siehe RFC 6146
  - Initiierung der Kommunikation von IPv6-Seite
    oder mit statischer Abbildung von IPv4- auf IPv6-Adressen
  - Speichert Zustandsinfo über die Verbindungen
- Unterstützung durch DNS64
  - RFC 6147 – DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
  - 2 Methoden: Statische DNS Records oder dynamische Umsetzung statischer DNS Records (Ergänzung um Präfix aus IPv6-Netz)

XLAT464 – Mechanismus



- Bereitstellung von IPv4-Basisfunktionalität über IPv6-Zugangsnetzwerk
- Übergangstechnologie zur sparsamen Verwendung von IPv4-Adressen
- Einsatz im Mobilfunk, bei IPv6-Infrastruktur und wenigen IPv4-Adressen

XLAT464 – Details

- RFC 6877 – 464XLAT: Combination of Stateful and Stateless Translation

- Kombination von
  - Stateless XLAT / RFC 6145: CLAT (Customer Side Translator)
    - Umsetzung 1:1 private IPv4-Adressen zu globalen IPv6-Adressen
  - Stateful XLAT / RFC 6146: PLAT (Provider Side Translator)
    - Umsetzung n:1 globale IPv6-Adressen zu globalen IPv4-Adressen

- Motivation
  - sparsame Verwendung von IPv4-Adressen
  - Verwendung einfacher IPv6-Infrastruktur, schnelle Einführung
  - geringere Komplexität als NAT444
    - trotzdem kein vollwertiger IPv4 / Dual-Stack-Ersatz

XLAT464 – Bewertung

- Provider-Technologie
  - Kombination von Technologien aus dem „XLAT-Baukasten“
- Typische Übergangstechnik mit Schwerpunkt auf IPv6-Infrastruktur

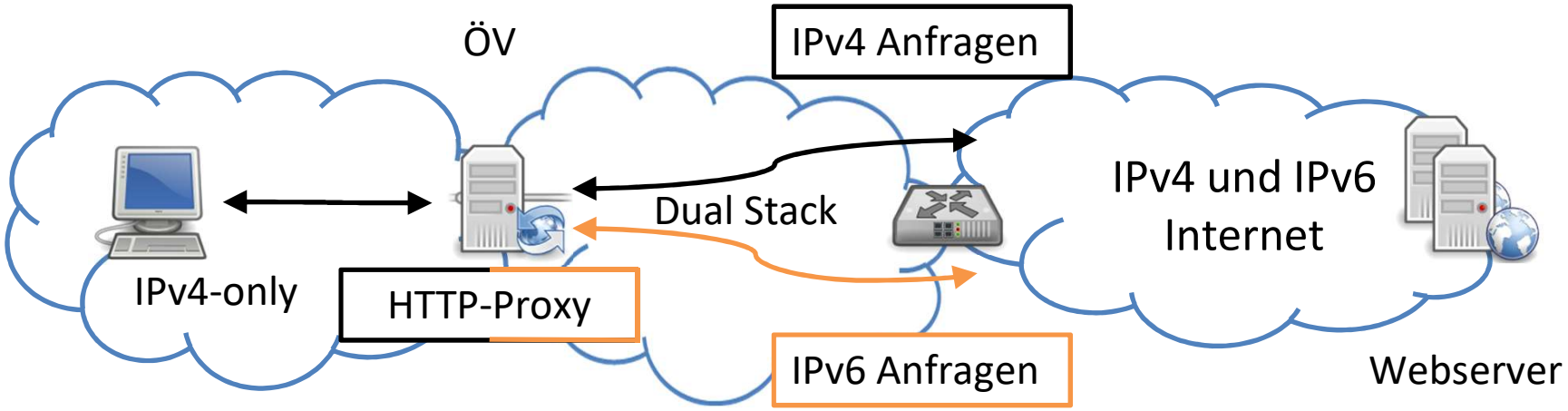
bei Nutzung über Provider ggf. Einschränkungen bei IPv4 durch NAT, Standardanwendung werden wenig beeinflusst

nicht nutzbar für Verwaltungen, auch nicht über Provider
Erreichbarkeit von außen und Universalität von Anschluss problematisch
→ hierfür besser Dual-Stack nutzen

Providertechnologie, Vorteile:

- schneller Aufbau von Infrastrukturen / sparsame Verwendung von IPv4
- besonders geeignet für neue Kabelnetz- und Mobilfunk-Provider

http(s) Proxy – Mechanismus



- Mögliche Übergangslösung für Zugriff aus einer IPv4-only-Umgebung ins IPv4- und IPv6-Internet (bzw. aus neuem IPv6-only)
- vorhandener Dienst und dessen Server müssen nicht angepasst werden
- relativ geringer Aufwand; Proxy-Technologie und Lösungen ausgereift
- Brückentechnologie vor Einführung von IPv6 im Intranet

http(s) Proxy – Details

- möglicher Schritt in einer Migrationsstrategie:
  - Teilmigration vom Internet-Anschluss bis zum Proxy
  - keine Änderung der internen Netze
- Umsetzung durch Proxy / allgemeinerer Fall verwendet ALG
- Umgekehrter Fall genauso möglich:
  - Zugriff von IPv6-only-Arbeitsplätzen mit definiertem Funktionsumfang auf bestehende IPv4-Dienste über Proxy / ALG
- kann auch intern zur Verbindung von Neu- und Altsystemen genutzt werden

http(s) Proxy – Bewertung

- Zusatznutzung von vorhandenem Proxy, ggf. Proxy als Brückentechnik
  - nur einsetzbar für „proxybare“ Protokolle wie z. B. http, ftp, smtp, pop3
  - Einsatzszenarien müssen getestet werden, keine Universallösung

normalerweise wird kein Proxy eingesetzt, Einsatz ist aber möglich

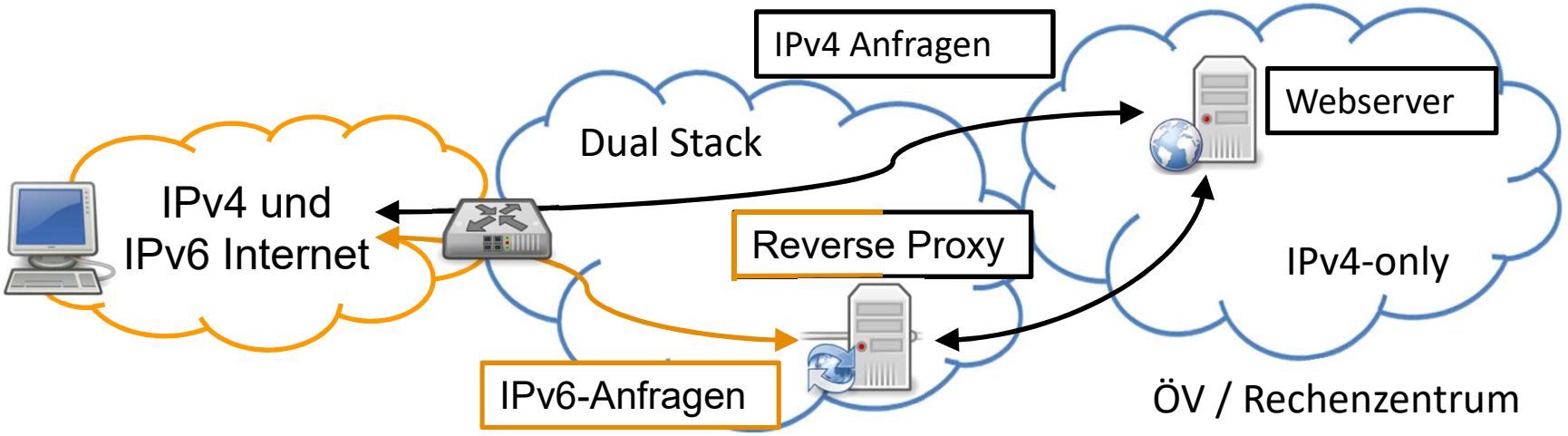
Nutzung von bestehendem Proxy oder ALG

- sinnvolle, bereits bestehende Netzgrenze für Teilmigration
- Einsatz von neuem Proxy als Brückentechnik sinnvoll
- ggf. interne Nutzung zum Zugriff auf nicht migrierbare Alt-IPv4-Systeme

Proxy könnte als Dienst angeboten werden

- Vertraulichkeit der Kommunikation(sbeziehungen) muss gewahrt bleiben

Reverse Proxy für http(s) – Mechanismus



- zusätzlicher Reverse Proxy, um Inhalte eines IPv4-only Webservers auch im IPv6-Internet abrufbar zu machen
- Konfiguration des bestehenden Webservers kann dabei zumeist komplett unverändert erhalten bleiben.
- Brückentechnologie, bis der Webserver auch Dual-Stack-tauglich ist.

Reverse Proxy für http(s) – Details

- möglicher Schritt in einer Migrationsstrategie:
  - schnelle Migration der Web-Inhalte, Sichtbarkeit im IPv6-Web
  - keine Änderung des eigentlichen Webservers
  - Voraussetzung: IPv6 steht durch Provider zur Verfügung
- für andere Dienste theoretisch genauso möglich, weniger üblich
- Teilmigration auch an vergleichbaren Übergängen:
  - Load Balancer
  - Dual-Stack-Webserver & IPv4-only Backend-Systeme (Datenbank)
- ggf. später: IPv4-Zugang über Proxy, Dienst steht nativ unter IPv6 bereit
  - Lastbetrachtung / Abschätzung des IPv6-Wachstums nötig

Reverse Proxy für http(s) – Bewertung

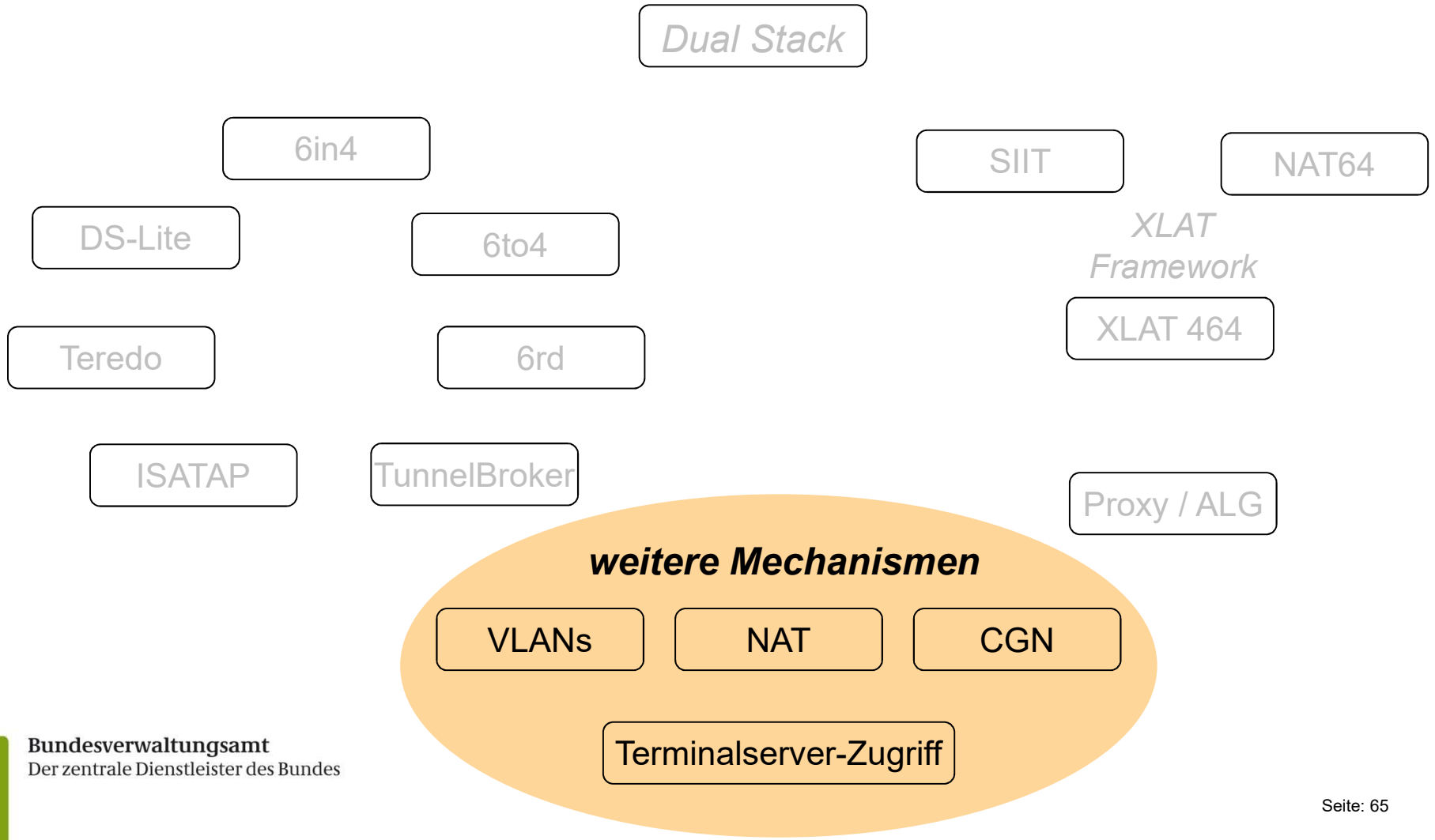
- Brückentechnik: IPv4-only Webserver wird über IPv6 erreichbar
  - … wenn ein IPv6-Zugang besteht
- nur einsetzbar für „proxybare“ Protokolle wie z. B. http, ftp, smtp und pop3.

SoHo bietet normalerweise keine Dienste an, Einsatz ist aber möglich

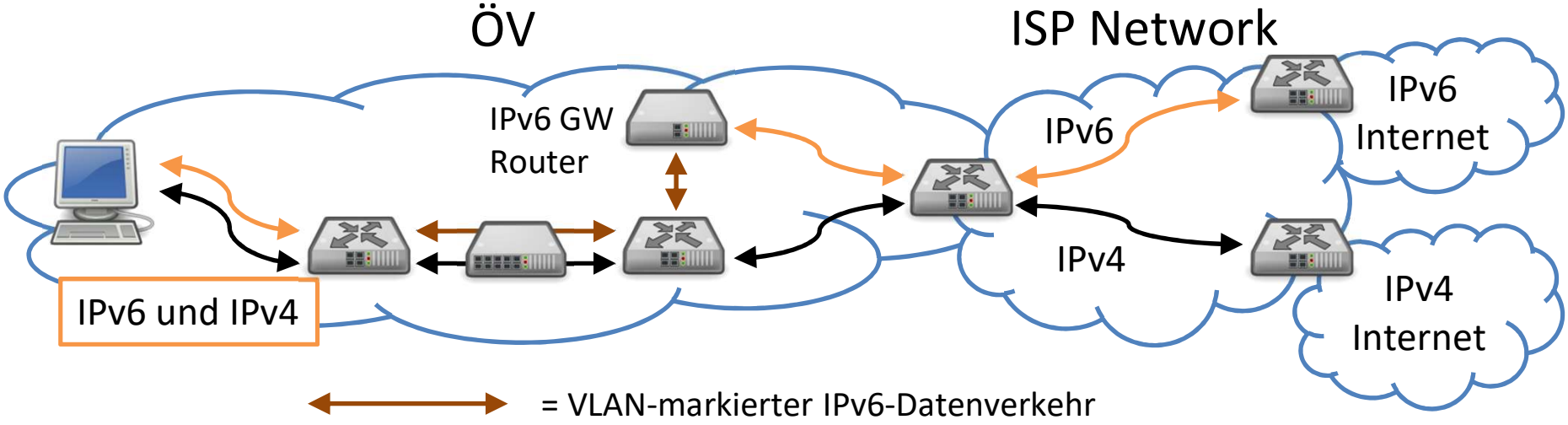
gute Brückentechnik für schnelle Verfügbarkeit von IPv6-Angeboten

Nutzung als Übergangstechnik für eigene Hosting-Angebote
ggf. Betrieb von Reverse Proxy als Dienstleistung für externe Server

Übergangstechniken – weitere Mechanismen



Nutzung von Layer2-VLANs – Mechanismus



- Übergangstechnik, für große Intranets
  mit VLAN-Tagging und ohne IPv6-fähige Switche/Router
- ist eine Brückentechnik auf dem Weg zu DualStack-Betrieb
- unabhängig von der Art und Weise, wie der ISP IPv6 zur Verfügung stellt

Nutzung von Layer2-VLANs – Details

- RFC4554 – Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks

- Einsatz als Übergangstechnik,
  - wenn VLANs bereits im LAN benutzt werden
  - und noch keine Dual-Stack-fähigen Router vorhanden

- geeignet zur frühen Nutzung von IPv6 ohne IPv6-Infrastruktur

Nutzung von Layer2-VLANs – Bewertung

- Technik unnötig, wenn im Intranet IPv6-fähige Router zur Verfügung stehen

Technik nicht sinnvoll in kleinen Infrastrukturen wie SoHo anwendbar

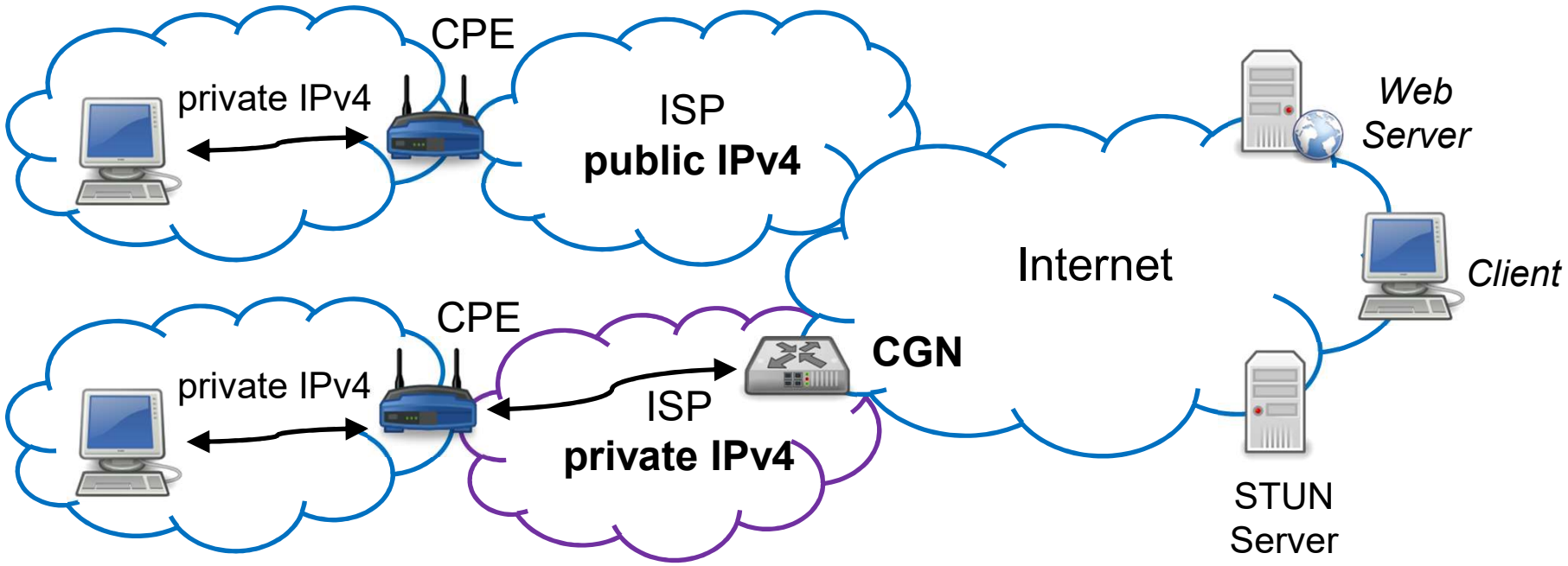
- gleich Dual-Stack nutzen

Technik nicht allgemein empfohlen, da hoher Aufwand für Brückentechnik

- gleich Dual-Stack nutzen
- ggf. zur Lösung spezieller Probleme nutzbar

Einsatz der Technik im eigenen LAN möglich (Provider routet dann Verkehr zwischen Netzen unterschiedlich bzgl. IPv4 und IPv6)

Privates NAT vs. Carrier Grade NAT – Mechanismus



- Carrier Grade NAT (CGN), Large Scale NAT (LSN), NAT444
- Einsatz beim ISP / bei Mobilfunk-Providern für IPv4
- reine IPv4-Lösung, angewendet aufgrund der IPv4-Adressknappheit

Carrier Grade NAT – Details

- Problem: Provider hat nicht mehr genug öffentliche IPv4-Adressen verfügbar
- einzige nur-IPv4-Lösung:
  - Vergabe privater IPv4-Adressen durch den ISP an seine Kunden …
  - … und Adressumsetzung (NAT) zwischen Kunden und Internet

- CG-NAT-Probleme:
  - Verbindungsaufbau nur von innen nach außen (zum Internet hin)
  - Zustand aller aktiven Verbindungen muss im NAT-Gateway des ISPs gehalten werden (für alle Kunden)
  - Kunde nicht mehr durch public IP identifizierbar (IP-Adresse wird geteilt)
  - Port-Forwarding für Kunden benötigt Konfiguration auf Gateway des ISP

- Private IPv4-Adressen: Im Heimnetz/Intranet nach RFC1918 und beim ISP nach RFC 6598 (verschiedene Adressbereiche aufgrund Routing)

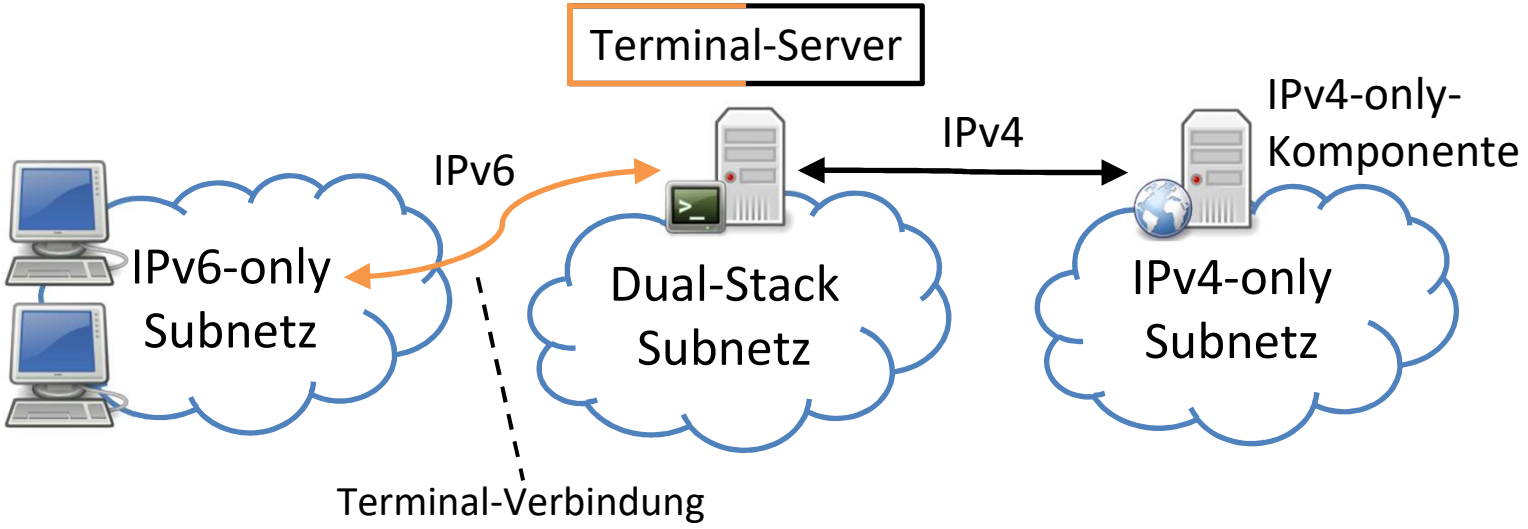
Carrier Grade NAT – Bewertung

- Erreichbarkeit von außen mit CGN sehr kompliziert
  - Portfreigaben müssten das Intranet verlassen und zum Provider geschickt werden
    - standardisierte und proprietäre Mechanismen (PCP, über Webportal)
    - zumindest teilweise Aufdecken der internen Netzstruktur

- Probleme bei der Skalierung von CGN
  - an einer Stelle muss für viele „Anschlüsse“ der Zustand gehalten werden
  - bei weiterem Datenwachstum (zu erwarten) muss weiter in „Sackgassen-Technologie“ investiert werden
  - Wachstum /Skalierung sollte über IPv6-Nutzung abgefangen werden

- CGN-Fazit:
  - als spezielle Lösung (z. B. im Mobilfunk) einsetzbar, ansonsten überwiegt das Potential zur Schaffung neuer Probleme

Zugang zu IPv4-Komponenten via Terminal-Server – Mechanismus



- „Legacy“-Dienste, ohne Möglichkeit zur Aktualisierung / IPv6-Umstellung
  - Dienst nur mit einer IPv4-only Klienten-Software erreichbar
- IPv6-only Klienten Alt-Dienste über Terminal-Lösung nutzen
- Lösung funktioniert auch für proprietäre Protokolle über IPv4
  - Unterschied zu Proxy-Lösungen, wo das Protokoll bekannt sein muss

Zugang zu IPv4-Komponenten via Terminal-Server – Details

- benötigt neue Infrastrukturkomponenten
- bietet dafür aber eine gute Lösung für Software bzw. Netzkomponenten (z. B. Steuerung), die nicht mehr nach IPv6 portiert werden können
- durch die Terminal-Server-Lösung sind diese „Legacy-Systeme“ dann trotzdem auch von Dual-Stack- und IPv6-only-Klienten nutzbar

Zugang zu IPv4-Komponenten via Terminal-Server – Bewertung

Einsatz möglich, aber hoher Aufwand

Terminal-Server sind hier z. T. schon im Einsatz
Lösung speziell für neue, IPv6-only Netze möglich

Interve Verwendung möglich, aber nicht für Kunden des ISPs

Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

Bewertungen & Empfehlungen

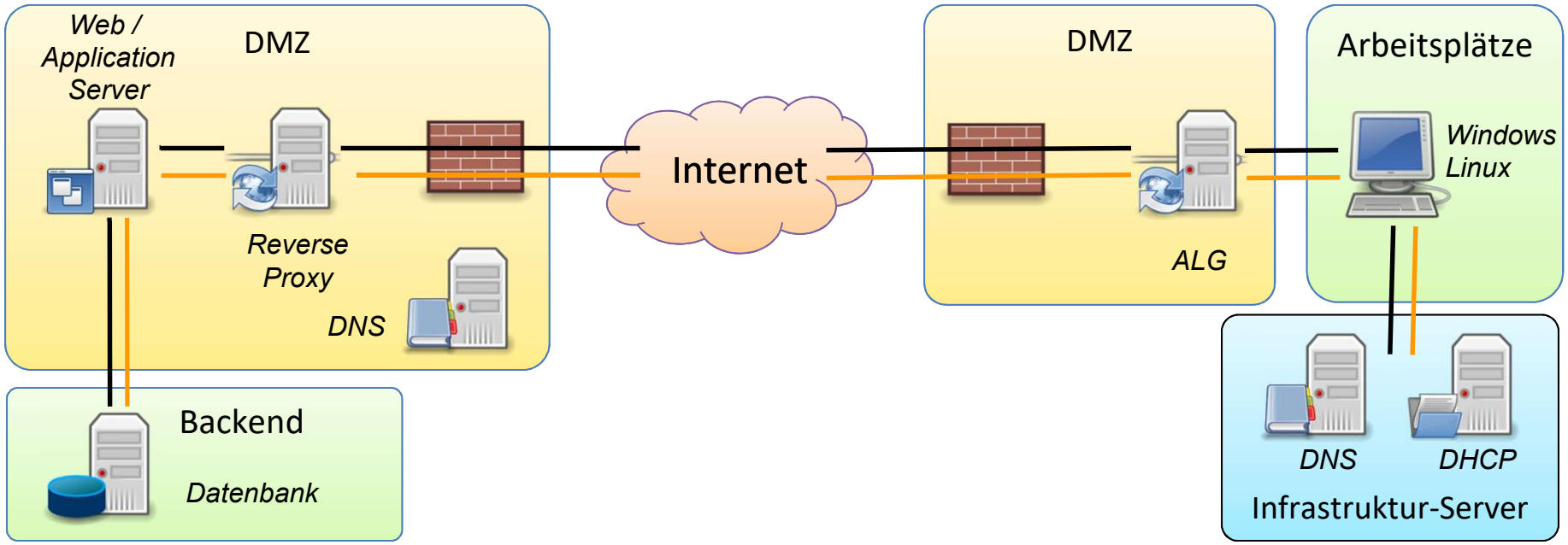
	SoHo	ÖV	ISP
Dual Stack	++	++	++
6in4	(→ Tunnelbroker)	+	
Teredo / 6to4	- (Sicherheit)	-- (Sicherheit)	
ISATAP		-	
DS-Lite / CGN	+ (über ISP)	- (über ISP)	+ (spart IPv4)
6rd	+ (über ISP)	- (über ISP)	+ (ermöglicht IPv6)
ÖV-Tunnelbroker	+	+ (Nutzer/Anbieter)	(ggf. Dienstanbieter)
NAT64 & DNS64	- (Aufwand)	+	
XLAT464	+ (über ISP)	- (über ISP)	+ (für neue ISP)
Proxy / ALG	+	++	- (ggf. Dienstanbieter)
Reverse Proxy		++	(ggf. Dienstanbieter)
L2-VLAN		-	
SIIT		+	+

Migrationsszenarien der ÖV

Empfohlener Einsatz von Übergangstechnologien in der ÖV

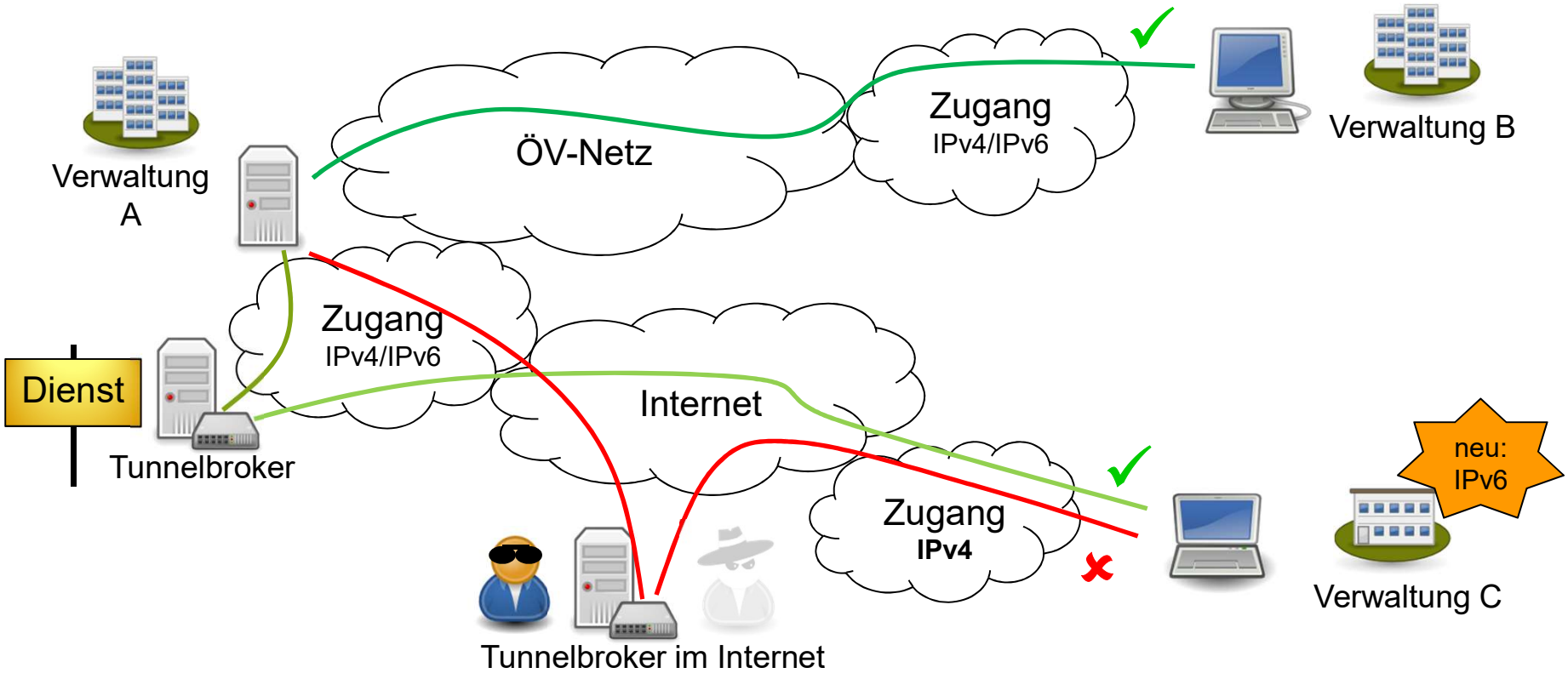
- Anbindung Internet: Dual-Stack, Proxy, Tunnelbroker
- Unterstützung von Alt-Anwendungen: Protokollumsetzung, Proxy, Tunnel
- Einbindung einer Außenstelle: VPN-Tunnel
- IPv6 über Koppelnetze
- IPv6-only für neue Netze / Anwendungen
  - der Blick nach vorn… in eine hoffentlich nicht allzu ferne Zukunft
- Verwaltungsübergreifende Kommunikation benötigt gemeinsame und abgestimmte IPv6-Policies

Szenario: Internet-Anbindung



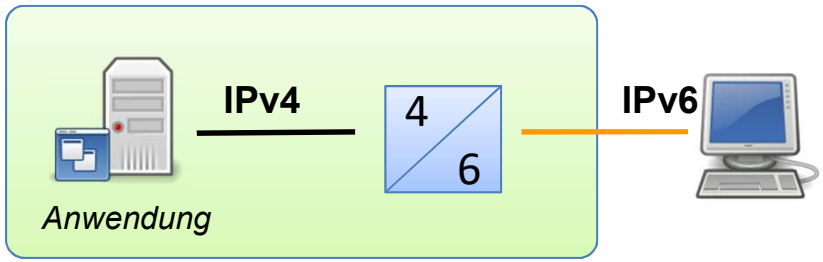
- zwei Teilbereiche, hier getrennt dargestellt: Dienste und Arbeitsplätze
- Vollständige Migration oder Teilmigration an Verbindungs- / Netzgrenzen
- Proxy bzw. ALG in der Praxis als Grenze / interne Netze sind abgegrenzt

Szenario: Tunnelbroker

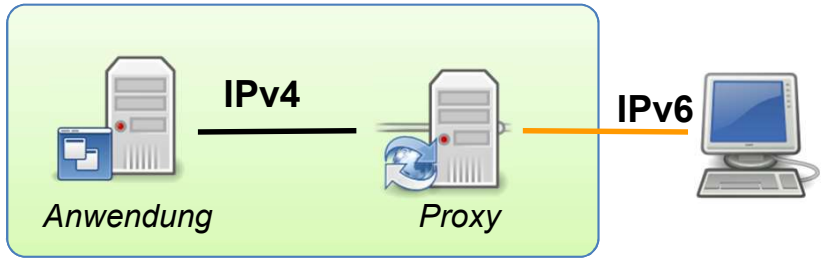


- Ziel: Sichere Kommunikation zwischen IPv6-Nutzern in der Migrationsphase

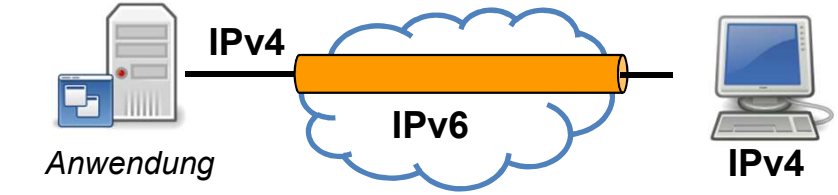
Szenario: Unterstützung von Alt-Anwendungen



- generelle Protokollumsetzung

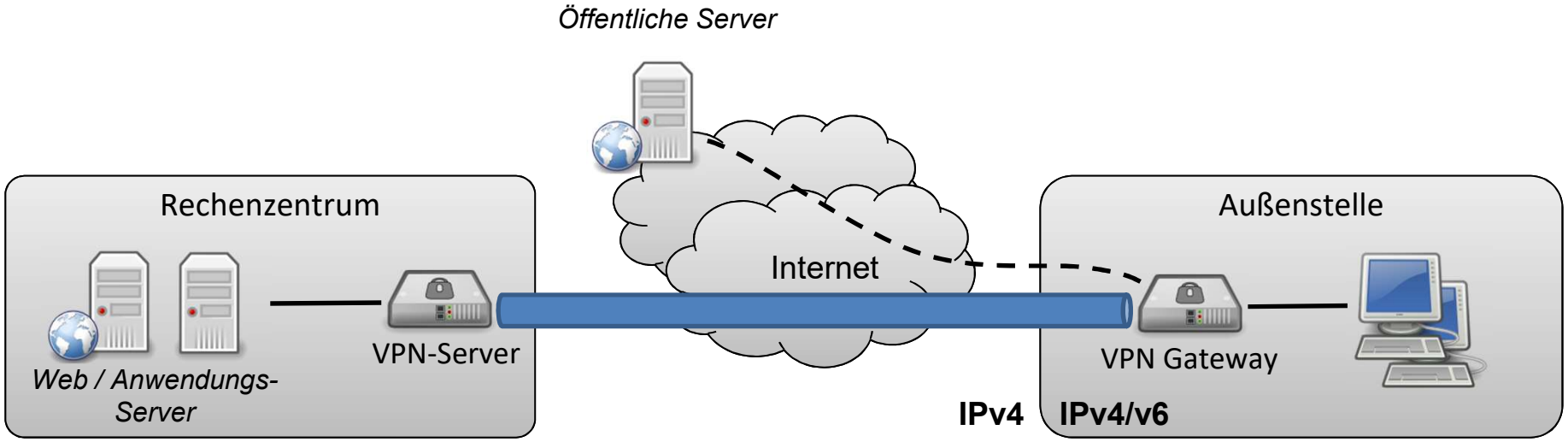


- anwendungsspezifische Protokollumsetzung mit Proxy



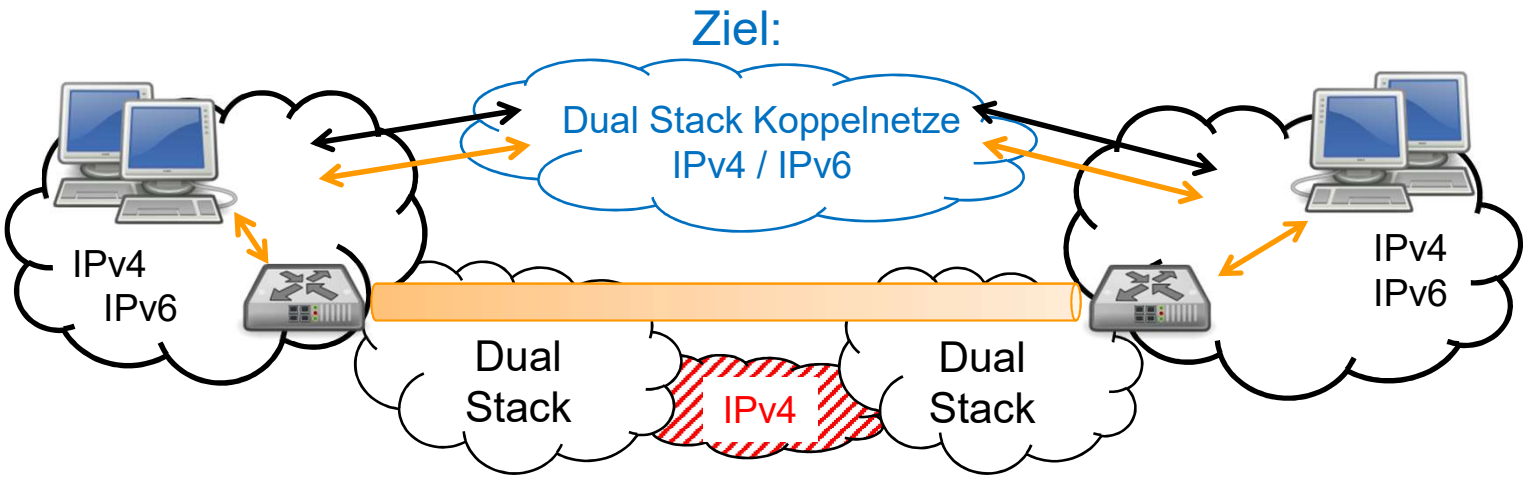
- Verwendung eines Tunnels über neue IPv6-only Netze oder Komponenten

Szenario: Anbindung einer Außenstelle



- Fallunterscheidung:
  IPv4/v6 außerhalb des Tunnels, IPv4/v6 innerhalb des Tunnels
- Kommunikation über VPN-Tunnel und/oder Nutzung direkter Internet-Zugriff
- mögliche Probleme: Routing der Außenstelle, MTU bei Tunneln, …

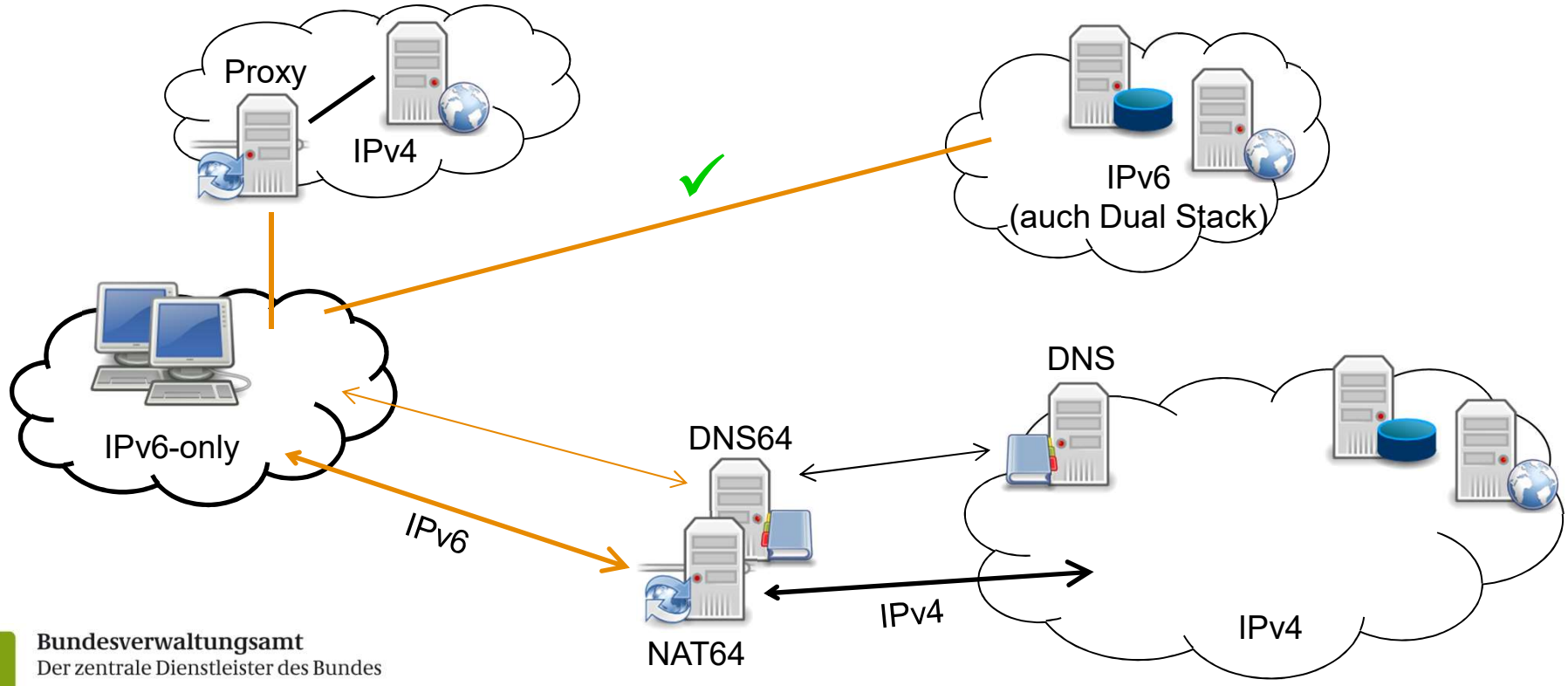
Szenario: Koppelnetze



- Ziel für Koppelnetze:
  - Angebot von Dual Stack Betrieb, wie alle Backbones
  - Übergangsphase, insbesondere über mehrere Netze: IPv6-Tunnel
- typische statische Tunnel:
  - 6in4 (RFC 4213 – Protokollnummer im IP-Header: 41(„proto 41 tunnel“)
  - GRE (Generic Router Encapsulation) von CISCO – Protokollnummer: 47
- Verwendung bestehender MPLS-Infrastruktur von Weitverkehrsnetzen

Szenario: IPv6-only für neue Netze

- Idee: Beim Aufbau ganz neuer Netze nur noch IPv6 einsetzen
  - Netze werden einfacher, kein Dual-Stack mehr
- Problem: Zugriff auf alte IPv4-Systeme → z. B. mittels Proxy oder NAT64



Zusammenfassung

- Migration von IPv4 zu IPv6 bedeutet Aufwand
  - sorgfältig planen, incl. Schulungen
  - passende, situationsgerechte Übergangstechnik auswählen
  - weitere Entwicklungen einplanen, Wachstum berücksichtigen

- die „eine beste“ Übergangstechnik gibt es nicht
  - viele Techniken und Kombinationen verfügbar, Auswahl ist individuell
  - Problematisch sind kurzfristige und spezielle Lösungen
    - Protokollumsetzung durch Proxy für Alt-Anwendungen
      → OK, wenn Anwendungsbereich genau bekannt ist

    - Einsatz von Carrier Grade NAT am universellen Internet-Zugang
      → lassen sich wirklich alle Auswirkungen auf bestehende und kommende Anwendungen schon vorher abschätzen?

- Informationen & Kontakt

Bundesstelle für Informationstechnik (BIT) –
Der zentrale IT-Dienstleister der Bundesverwaltung

Local Internet Registry (LIR) de.government

http://www.lir.bund.de

LIR@bva.bund.de