Skriptum: Unterbrechungsfreier Domänenwechsel und IP-Range-Wechsel – Fokus auf Mail-Services (DNS & E-Mail-Infrastruktur)

Thema: Wie sorgt man bei einem Domänenwechsel (z. B. `corp.at` → `firma.at`) oder IP-Range-Wechsel (ISP-Wechsel) dafür, dass **Mail-Services unterbrechungsfrei** weiterlaufen? **Beispiel-Domäne:** `corp.at` → `firma.at` (beide extern gehostet, z. B. bei Cloudflare oder anderem Public DNS Provider)

---

1. Grundlagen: Was steht in einer DNS-Zone?

1.1. Wichtige DNS-Record-Typen (für Mail & Web)

Record	Zweck	Beispiel (`corp.at`)	Bemerkung
MX	Mail Exchange – zeigt auf **MTA** (Mail Transfer Agent)	`MX 10 mail.corp.at.`	**Kein IP direkt!** → verweist auf A-Record
A	Address – IP zu Hostname	`mail.corp.at. IN A 80.90.100.1`	Wird vom MX benötigt
A (Web)	Webserver	`server10.corp.at. IN A 80.90.100.2`	
CNAME	Canonical Name – Alias	`www.corp.at. IN CNAME server10.corp.at.`	**Kein zweiter A-Record auf gleiche IP!** → nicht standardkonform
SOA	Start of Authority	`corp.at. IN SOA ns1.hostingprovider.at. ...`	Zeigt auf **Primary DNS** (Read-Write)
NS	Name Server	`corp.at. IN NS ns1.hostingprovider.at.`	Für Primary + Secondary
PTR	Pointer (Reverse Lookup)	`1.100.90.80.in-addr.arpa. IN PTR mail.corp.at.`	**Vertrauenswürdig!** Wird vom **ISP** verwaltet

Record	Zweck	Beispiel (`corp.at`)	Bemerkung
SPF (TXT)	Sender Policy Framework	`corp.at. IN TXT "v=spf1 ip4:80.90.100.1 -all"`	Anti-Spam: Welche IPs dürfen für Domäne senden?

Wichtig: Bei **MX, SOA, NS** steht **immer der volle FQDN** (nicht abgekürzt wie bei A/CNAME). BIND ergänzt **nicht** automatisch die Domain!

---

2. E-Mail-Infrastruktur: Die 3 Rollen (MUA, MTA, MDA)

Rolle	Name	Protokoll	Aufgabe	Server-Typ
MUA	**Mail User Agent**	–	Client (Outlook, Thunderbird)	Konfiguriert MTA + MDA
MTA	**Mail Transfer Agent**	**SMTP**	Versendet & empfängt Mails zwischen Servern	**SMTP-Server**
MDA	**Mail Delivery Agent**	**IMAP/POP3**	Speichert Mails im Postfach	**Postfach-Server**

2.1. Protokolle im Detail

Protokoll	Vollname	Aufgabe	Besonderheit
SMTP	Simple Mail Transfer Protocol	Mail-Versand (MTA → MTA)	
POP3	Post Office Protocol v3	Abruf → **löscht** vom Server	Veraltet, unsicher
IMAP (IMAP4)	Internet Message Access Protocol	Abruf → **bleibt auf Server**	Datenbank-basiert, Struktur, Abfragen

Heutiger Standard: IMAP (POP3 fast vergessen)

---

3. Wie funktioniert Mail-Zustellung? (Schritt-für-Schritt)

Ablauf:

1. **MUA** schickt Mail an **konfigurierten MTA** (SMTP-Server).
2. **MTA** liest **To: user@htl.at** → extrahiert **Domain: htl.at**.
3. **MTA** fragt DNS: `MX für htl.at?`
   - Antwort: `mail.corp.at` + **A-Record** (DNS schickt beides mit).
4. **MTA** sendet SMTP an `mail.corp.at` (IP aus A-Record).
5. Ziel-MTA empfängt → leitet an **MDA** weiter (oft gleicher Server).
6. **MUA** holt per **IMAP** vom MDA.

MX zeigt immer auf MTA (SMTP-Server), nie direkt auf MDA!

---

4. Vertrauen & Anti-Spam: Warum PTR & SPF?

4.1. Reverse Lookup (PTR) – Vertrauenswürdig

- **Empfänger-MTA** prüft:
  1. IP des Senders → **PTR-Abfrage** → `mail.corp.at`
  2. Vergleicht mit **From-Domäne** in Mail
- **PTR wird vom ISP verwaltet → vertrauenswürdig**
- **MX kann jeder ändern → nicht vertrauenswürdig**

4.2. SPF (Sender Policy Framework)

- TXT-Record: Welche IPs dürfen für `@corp.at` senden?
- Beispiel: `v=spf1 ip4:80.90.100.1 include:_spf.google.com -all`
- Moderne Alternative bei Office 365, etc.

---

5. Szenario 1: Domänenwechsel (`corp.at` → `firma.at`)

Ziel: Kein Mail-Verlust, keine Unterbrechung

Lösung: Parallele DNS-Einträge + Mail-Server-Konfiguration

Schritt 1: DNS (Forward Zone bei Hoster)

```
firma.at.         IN MX 10 mail.firma.at.
mail.firma.at.    IN A  80.90.100.1
www.firma.at.     IN CNAME server10.firma.at.
server10.firma.at. IN A  80.90.100.2
```

Schritt 2: Mail-Server konfigurieren

- **Akzeptiert Mails für beide Domänen:**
  - `corp.at`
  - `firma.at`
- **Mehrere virtuelle Domains** möglich

Schritt 3: Reverse Lookup (beide ISPs!)

- **Alter ISP:** `1.100.90.80.in-addr.arpa → mail.corp.at`
- **Neuer ISP:** `1.100.90.80.in-addr.arpa → mail.firma.at` **(oder beide!)**

Schritt 4: SPF-Record erweitern

```
firma.at. IN TXT "v=spf1 a:mail.corp.at -all"
```

Schritt 5: TTL beachten

- Standard: **4 Stunden**
- **Nach 4–6 Stunden weltweit propagiert**
- **Keine Forwarder-Chains** → max. 2–3 Hops

  Risiko: Greylisting, wenn PTR nicht passt → **beide PTRs kurzzeitig lassen!**

---

6. Szenario 2: IP-Range-Wechsel (ISP-Wechsel, keine Domainänderung)

Gegeben:

- Alte IP: `80.90.100.1` (alter ISP)
- Neue IP: `192.168.200.1` (neuer ISP)
- Domain: `corp.at` bleibt

Änderungen in 3 Zonen:

Zone	Wo?	Was ändern?
Forward Lookup	DNS-Hoster	`mail.corp.at A → 192.168.200.1`
Reverse Lookup (alt)	Alter ISP	**PTR beibehalten!**
Reverse Lookup (neu)	Neuer ISP	`1.200.168.192.in-addr.arpa → mail.corp.at`

Unterbrechungsfrei durch:

1. Temporäre zweite A-Record (Forward)

```
mail.corp.at. 3600 IN A 80.90.100.1   ; alt
mail.corp.at. 3600 IN A 192.168.200.1 ; neu
```

→ **Beide IPs antworten**

2. Alter ISP: SMTP-Redirect

- **Standard-Service**: Alter ISP nimmt Mails auf alter IP entgegen → **leitet weiter** an neue IP
- **Kein Speichern nötig**

3. PTR beibehalten (alter ISP)

- Für **gecachte Abfragen** und **Anti-Spam**

4. SPF erweitern

```
corp.at. IN TXT "v=spf1 ip4:80.90.100.1 ip4:192.168.200.1 -all"
```

> **Nach 1–2 Tagen:** Alte IP & PTR löschen (wenn nicht mehr benötigt)

---

7. DNS-Caching & TTL

Konzept	Erklärung
TTL	Time To Live – im SOA-Record → Standard: **4 Stunden**
Caching	Jeder DNS-Server speichert Antworten
Wann neu abgefragt?	Nach Ablauf der TTL
Weltweite Propagation	Max. **TTL + 1–2 Stunden** (keine langen Forwarder-Chains)

> **Tipp:** TTL vor Umstellung auf **1 Stunde** senken → schnelleres Update

---

8. DNS-Abfragen: Rekursiv vs. Iterativ

Typ	Ablauf	Vorteil	Nachteil
Rekursiv	Client → Forwarder → Forwarder → ... → Antwort	Einfach, nutzt Cache	Belastet Forwarder
Iterativ	Client → Root → TLD → Authoritative → Antwort	**Erste Hand**, genau	Mehr Aufwand

Root-Server werden entlastet durch **Caching + rekursive Abfragen**

---

9. Primary vs. Secondary DNS

Typ	Schreibrecht?	Replikation
Primary	**Read-Write**	Master-Zone
Secondary	**Read-Only**	**Zonentransfer** vom Primary

Active Directory: Multi-Master → **alle gleich Klassisches DNS:** Single-Master (Primary)

---

10. Zusammenfassung: Checkliste für unterbrechungsfreien Wechsel

Aufgabe	Domänenwechsel	IP-Wechsel
Neue Forward-Zone anlegen	J (firma.at)	N
MX + A-Records setzen	J	J (A ändern)
Mail-Server: Domains hinzufügen	J	N
PTR bei altem ISP beibehalten	J	J
PTR bei neuem ISP setzen	J	J
SPF erweitern	J	J
SMTP-Redirect (alter ISP)	N	J
TTL senken	J	J
Warten: 4–6 Stunden	J	J

Merksätze des Professors

„MX zeigt immer auf MTA, nie auf IP direkt.“ „PTR ist vertrauenswürdig – wird vom ISP verwaltet.“ „SPF ist die moderne Lösung für Office 365 & Co.“ „Kein zweiter A-Record auf gleiche IP – dafür gibt's CNAME.“ „TTL = 4 Stunden → weltweit max. 6 Stunden bis Update.“ „Alter ISP macht SMTP-Redirect – Standard-Service!“ „Primary = Read-Write, Secondary = Read-Only via Zonentransfer.“ „Rekursiv = Bequem, Iterativ = Genau.“
