Die Rolle von PTR Abfragen bei Mailservern

Willkommen im Wahnsinn!

Disclaimer:

An diesem Dokument haben nur echte Experten mitgeschrieben. Dies wurde von anderen Experten verifiziert.

Die Einleitung

Die Ausgangssituation zum besseren Verständnis:

Ein Kunde kann an eine Domain keine Emails schicken.

Der Admin des empfangenen Mailservers, macht einen nicht vorhandenen „RDNS“ Eintrag dafür verantwortlich, denn der Absenderserver haben muß.

Die Einleitung

Wie man sich dabei täuschen kann,

erfahren Sie gleich!

Die Einleitung

„Führende IT-Spezis Deutschlands“*

behaupten übrigens,

dass Mailserver einen „RDNS“ Eintrag haben müssen.

*) Begriffsklärung „Spezi, der“ → https://www.bayrisches-woerterbuch.de/spezl-der-spezi/

Die Einleitung

Was ist denn ein „RDNS“ Eintrag überhaupt?

Die Einleitung

„RDNS“ ist kein DNS Eintrag,

sondern eine Verfahrensbeschreibung,

wie man eine IP zu einem Domainnamen auslösen kann.

Siehe* **https://de.wikipedia.org/wiki/Reverse_DNS**

Die Einleitung

Experten nennen das einen **PTR** Record :)

Die Einleitung

Experten nennen das einen **PTR** Record :)

Steht so übrigens auch in dem Wikipediaeintrag* drin ;)

*) „Führende IT Spezis Deutschlands“ verlinken dieses Dokument, haben es aber scheinbar nicht zu ende nicht gelesen.

Die Einleitung

Wo kommt das mit den PTR Records für Mailserver her?

Die Einleitung

„Führende IT-Spezis Deutschlands“

empfehlen

„Anti-Spam-**Empfehlungen** für SMTP-MTAs“

https://www.rfc-editor.org/rfc/rfc2505

Die Einleitung

„Führende IT-Spezis Deutschlands“

empfehlen

„Anti-Spam-**Empfehlungen** für SMTP-MTAs“ von 1999

https://www.rfc-editor.org/rfc/rfc2505

Die Einleitung

Einleitung RFC 2505

„Die Absicht ist, dass diese Empfehlungen dazu beitragen werden, **die Spam-Situation zu bereinigen**, wenn sie auf genügend SMTP-MTAs im Internet angewendet werden, und dass sie als Richtlinien für die verschiedenen MTA-Anbieter dienen sollten. Wir sind uns darüber im Klaren, dass dies nicht die endgültige Lösung ist, **aber wenn diese Empfehlungen von allen SMTP-MTAs im Internet übernommen und verwendet würden, würde sich die Situation erheblich verbessern** und Zeit für die Entwicklung einer längerfristigen Lösung entstehen. Im Abschnitt "Zukünftige Arbeiten" werden einige Ideen vorgeschlagen, die Teil einer solchen langfristigen Lösung sein könnten. Es könnte jedoch sehr gut sein dass die endgültige Lösung eher sozialer, politischer oder rechtlicher Natur ist, und nicht technischer Natur ist.“ (1999)

Das hat ja richtig gut geklappt mit der Spambekämpfung :D

Die Einleitung

Man „**muß**“ also bestenfalls einen **PTR** haben,

weil andere Anbieter die RFC auch umgesetzt haben.

Ist halt empfohlene „**Best Practise**“.

Die Einleitung

Wie sinnvoll das noch ist,

wo 2024 alle Endkunden Anschlüsse PTR Records haben,

die das **1999** nicht hatten,

sei mal dahin gestellt.

Die Einleitung

Disclaimer:

Natürlich haben hier alle Server einen PTR und prüfen auch,

ob die sendende IP-Adresse einen PTR hat :)

Die Abfrage war beim Exim Mailserver schon out-of-the-box dabei ;)

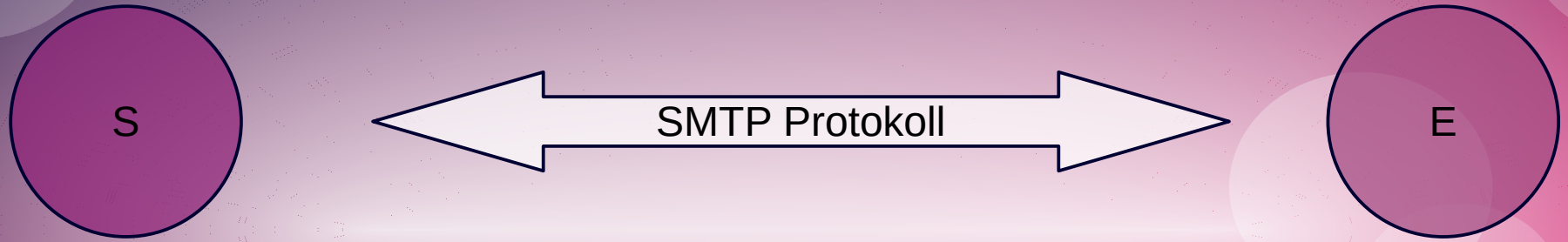
Die Rolle von PTR Abfragen bei Mailservern

„Ein Wunder, dass wir Emails verschicken konnten.“

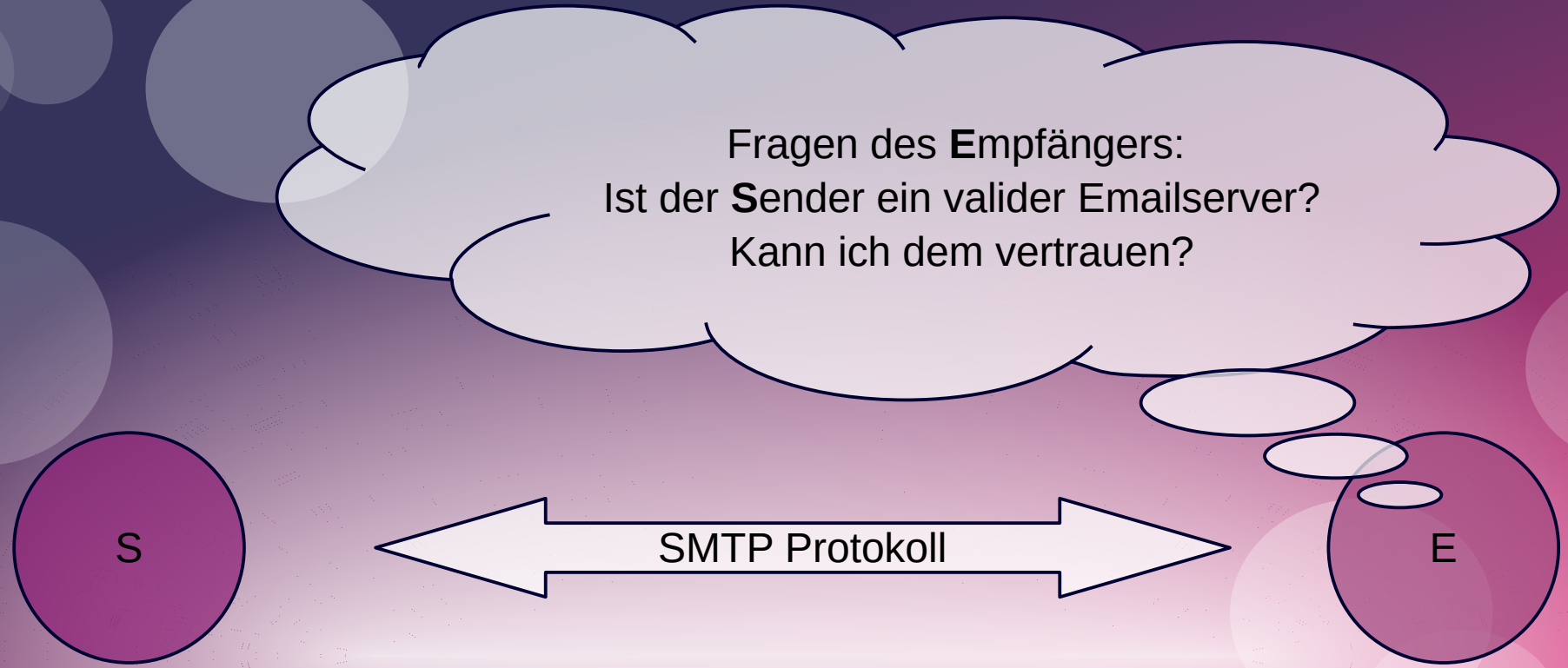
Sanford Wallace
(Spam König)

Wir brauchen … Mailserver!

Die sprechen SMTP (RFC 821 ff.) untereinander



„Ist das ein Profi?“



PTR Tests von Mailserver

Um das zu beantworten,
führen sehr viele Mailserver einen Test
der sendenden IP Adresse durch,
ob diese einen **PTR** Record hat.

(In Microsoftkreisen spricht man auch von RDNS)

PTR Tests von Mailserver

Die prüfen aber auch,
ob es den Absender dort überhaupt gibt
und viele andere Dinge.

PTR Tests sind nur einer von vielen Tests.

PTR Tests von Mailserver

Ein **PTR** ist ein DNS Eintrag, der eine IP auf einen Domainnamen zeigen lässt.

„**Full-Circle-PTR**“

Ein **FCPTR** wäre ein passendes Duo aus PTR und IN A der Domain und IP:

domain.de => 1.2.3.4 => domain.de

PTR Tests von Mailserver

Da wir immer noch im **D**omain **N**ame **S**ervice unterwegs sind,
müssen wir aus der IP einen Domainnamen machen:

Beispiel:

93.246.80.144 wird zu 144.80.246.93**.in-addr.arpa.**

PTR Tests von Mailserver

Beispiele:

Variante A – Delegation eines Class-C Netzes /24

$ host 93.246.80.144
144.80.246.93.in-addr.arpa domain name **pointer p5df65090.dip0.t-ipconnect.de**.

Variante B – CNAME Delegation einen Class-C Subnetzes /27

$ host 83.246.80.144
144.80.246.83.in-addr.arpa is an alias for 144.128/27.80.246.83.in-addr.arpa.
144.128/27.80.246.83.in-addr.arpa domain name **pointer s129.resellerdesktop.de**.

Für mehr Infos siehe RFC 2317/1998 - https://datatracker.ietf.org/doc/html/rfc2317

PTR Tests von Mailserver

Das war einfach?

PTR Tests von Mailserver

Ja, weil alles geklappt hat!

Die Rolle von PTR Abfragen bei Mailservern

Aus der Kategorie: „Was kann da schon schief gehen?“

namenloser Windowsadmin
(gottesfürchtig)

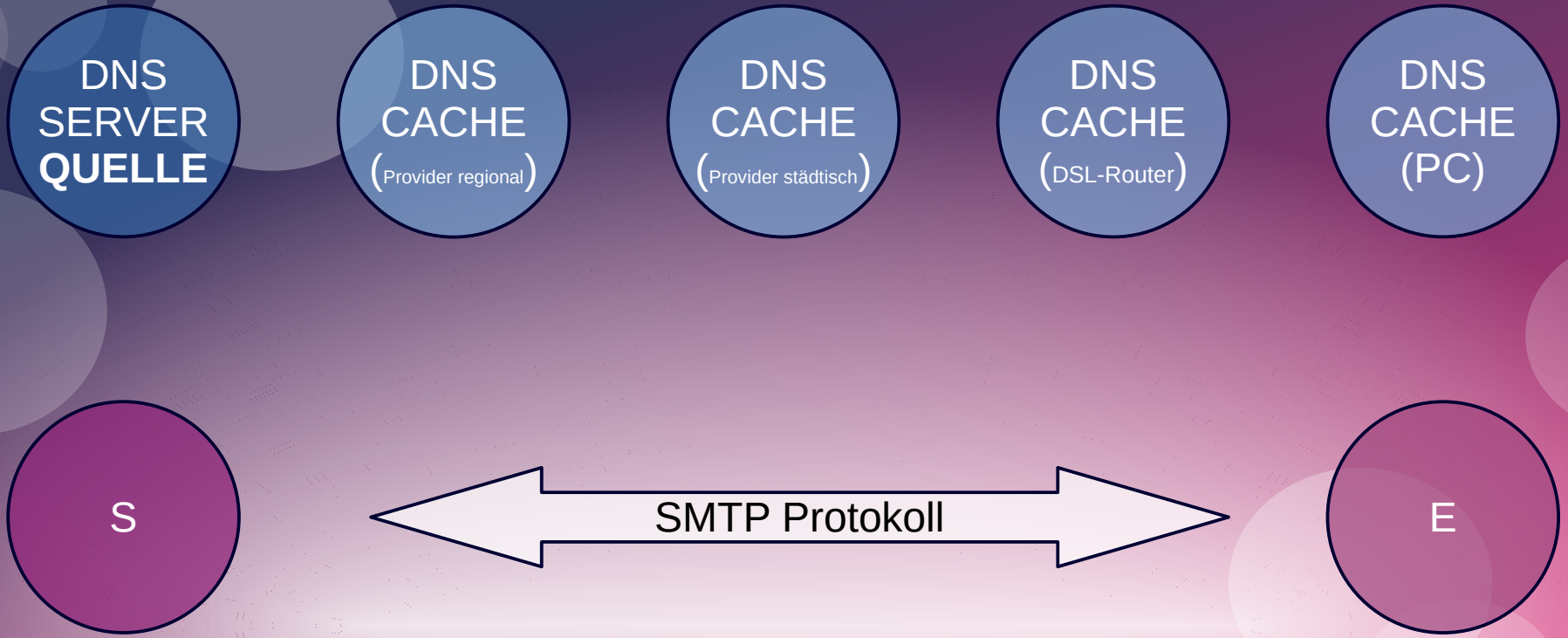
PTR Tests von Mailserver

Hinweis:

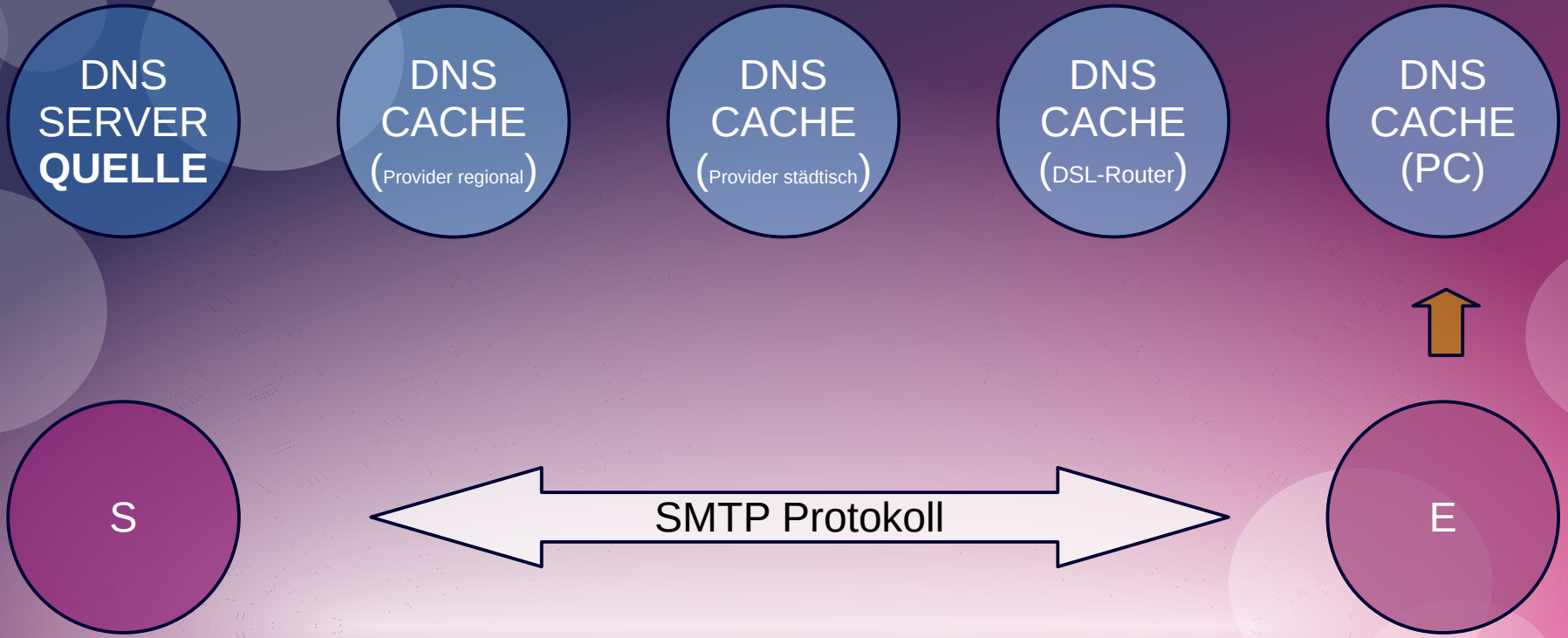
In den nachfolgenden Grafiken,

steht der Mailserver im Büro.

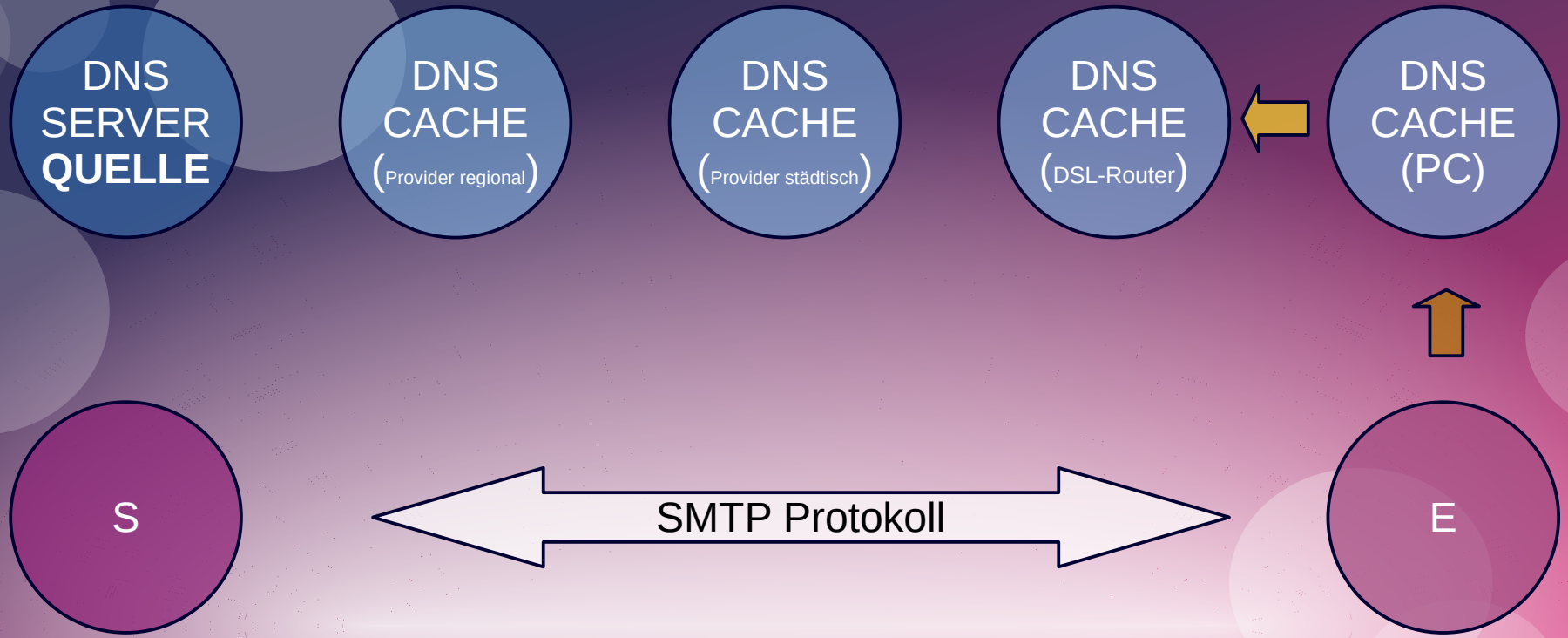
PTR Abfragen von E über diverse Cache



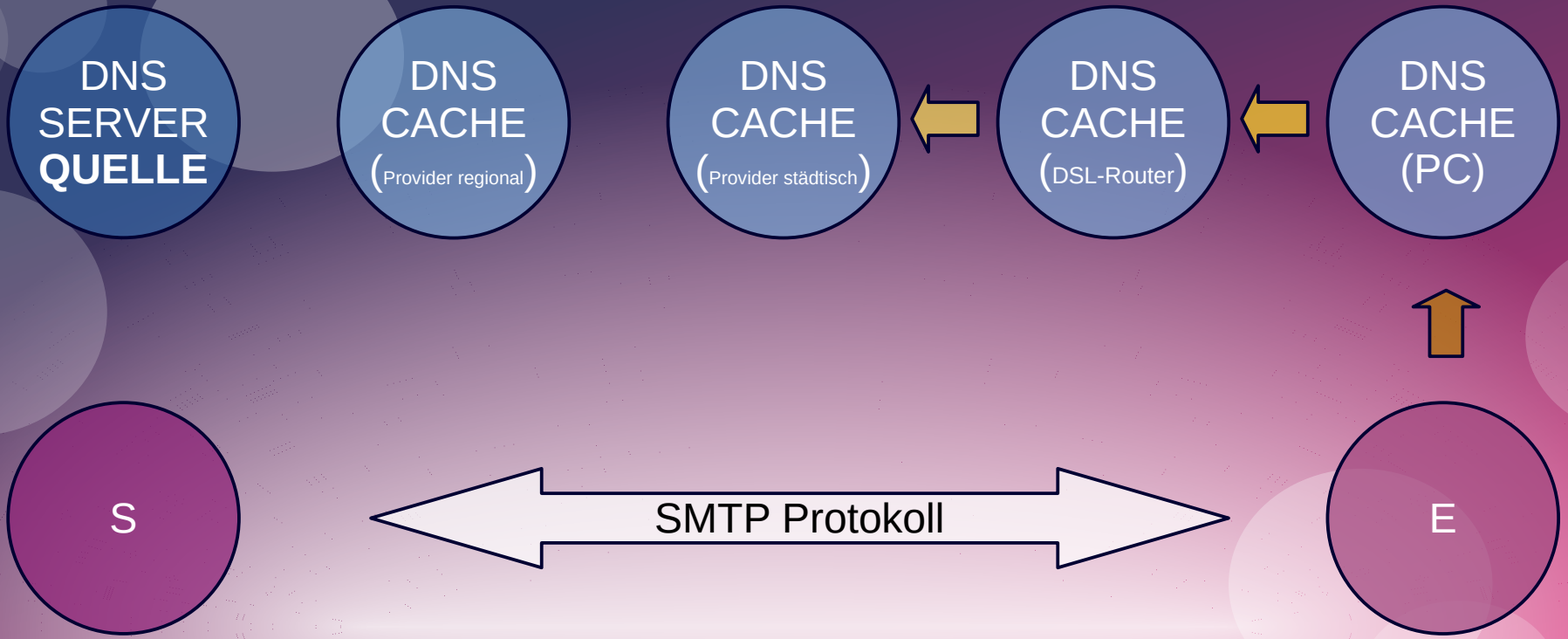
PTR Abfragen von E über diverse Cache



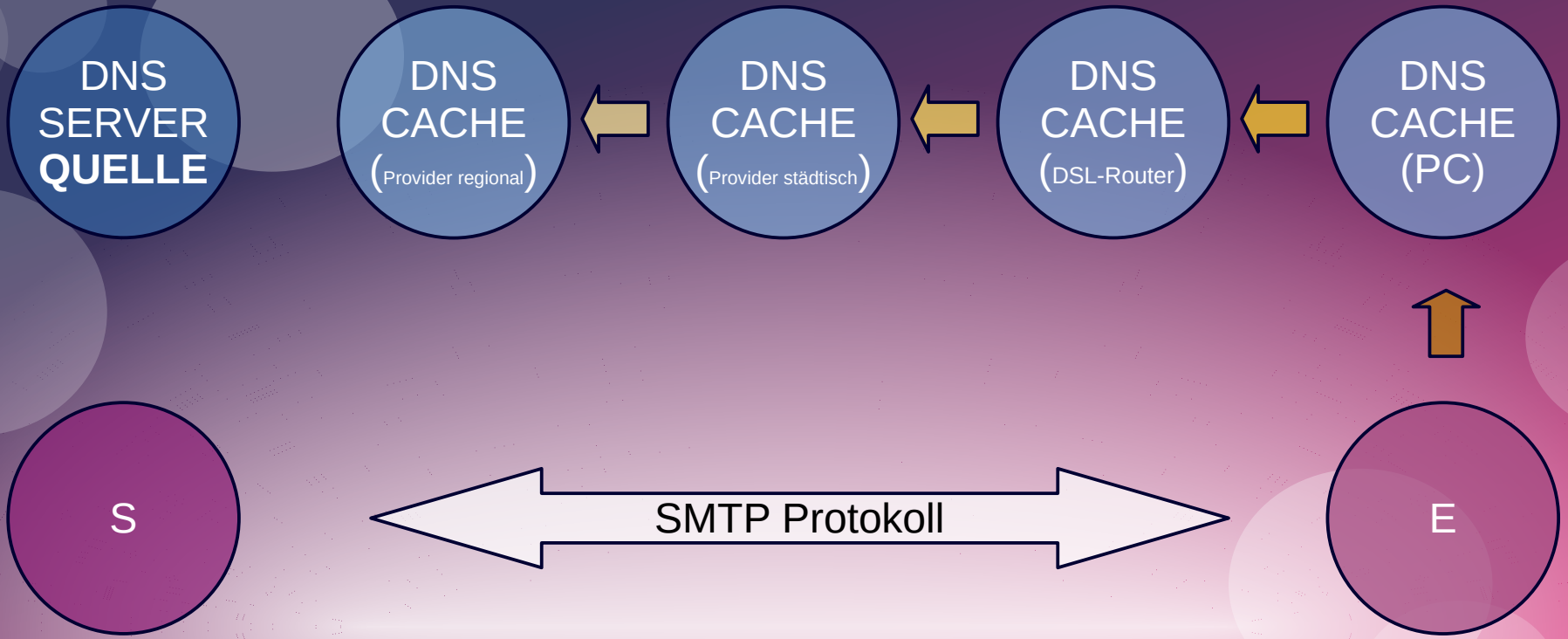
PTR Abfragen von E über diverse Cache



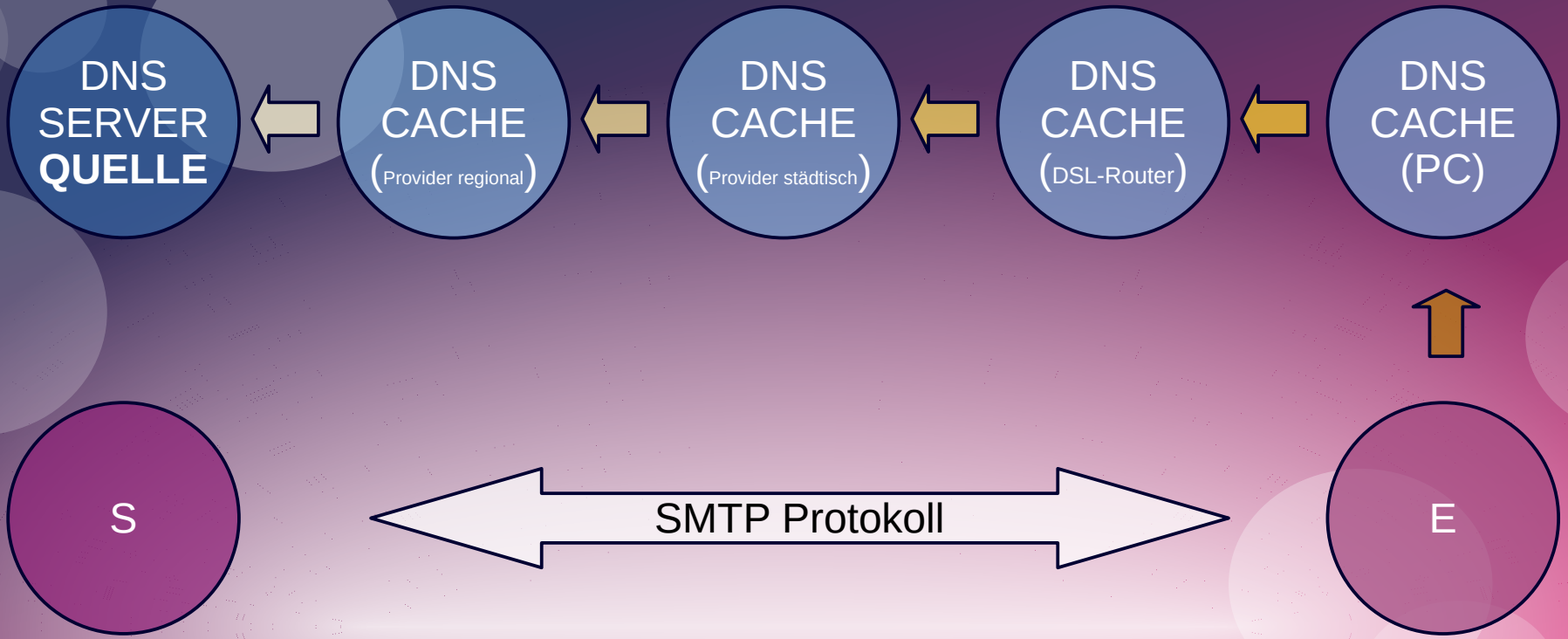
PTR Abfragen von E über diverse Cache



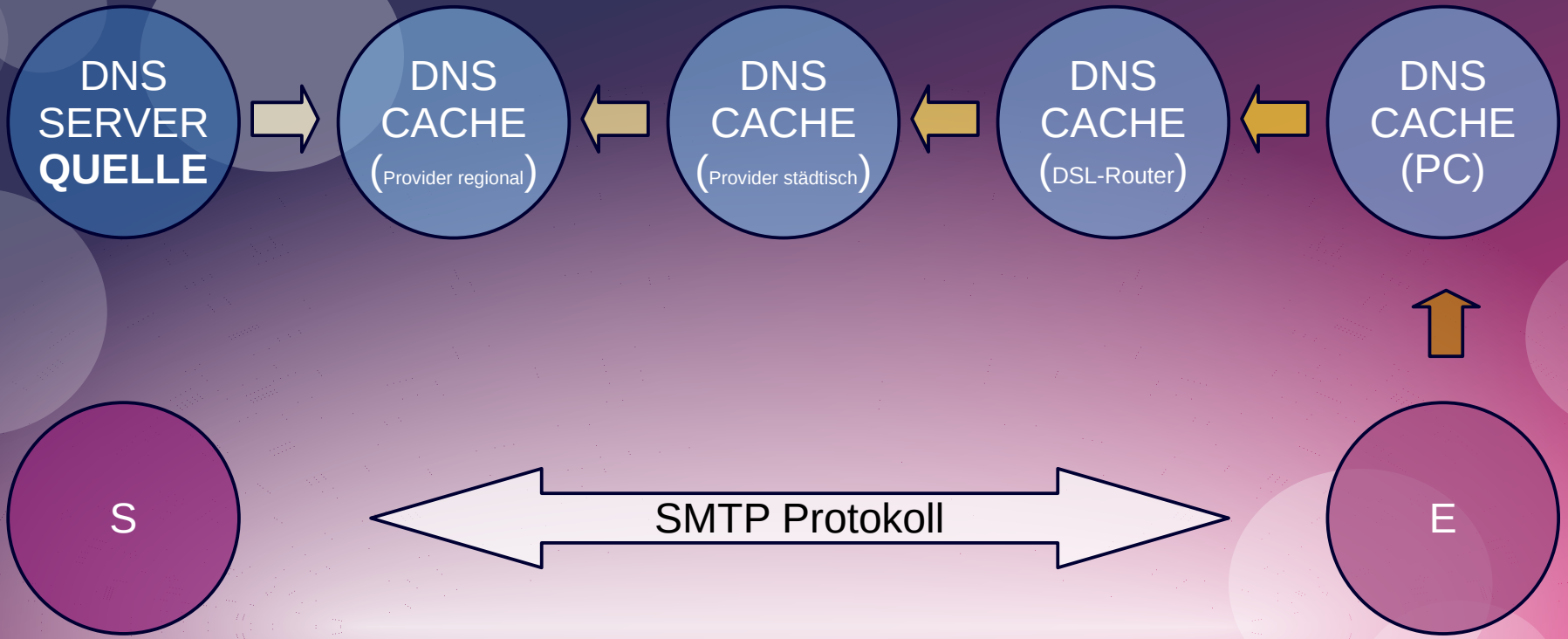
PTR Abfragen von E über diverse Cache



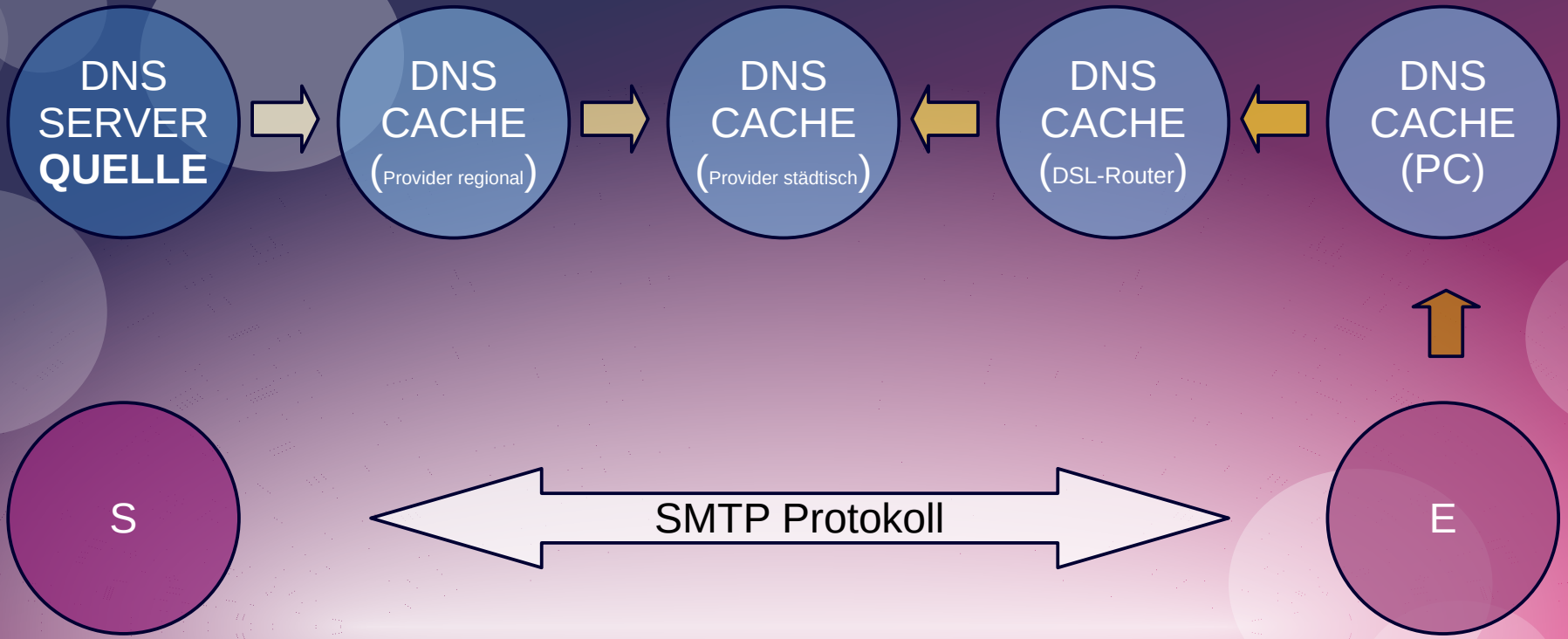
PTR Abfragen von E über diverse Cache



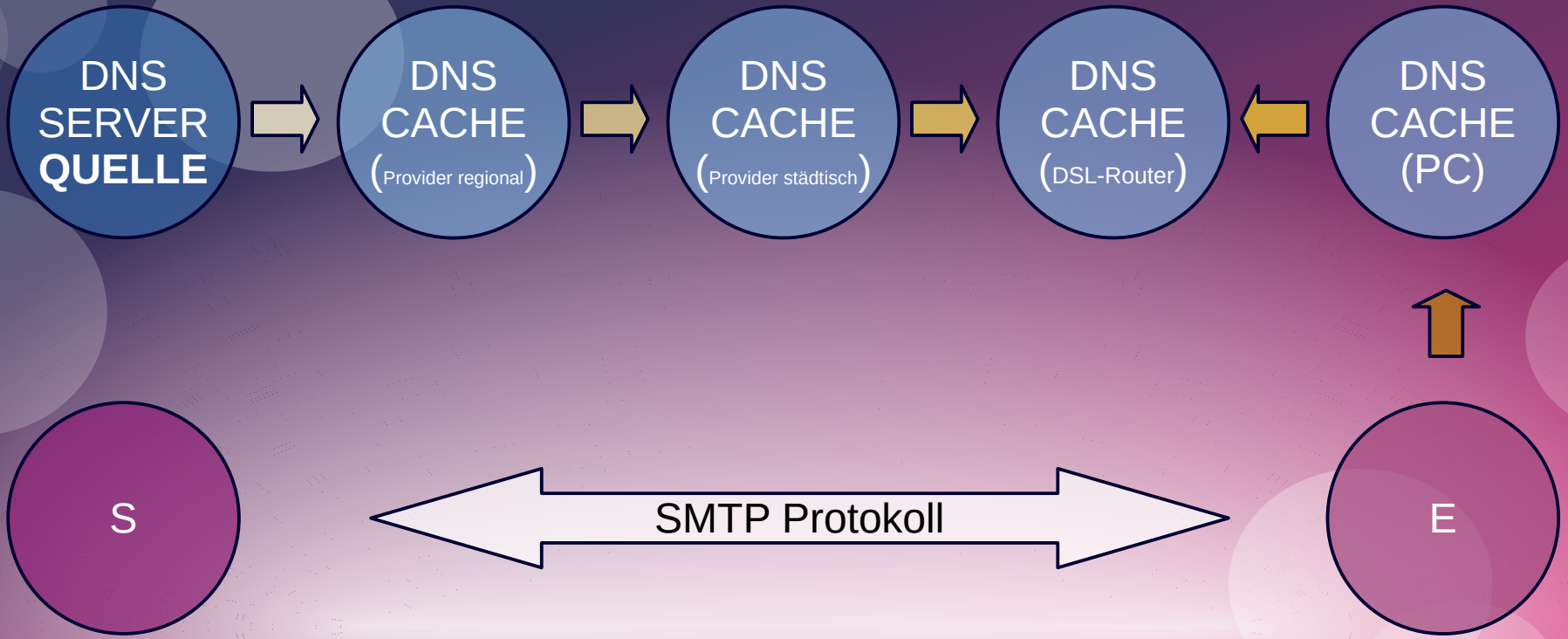
PTR Abfragen von E über diverse Cache



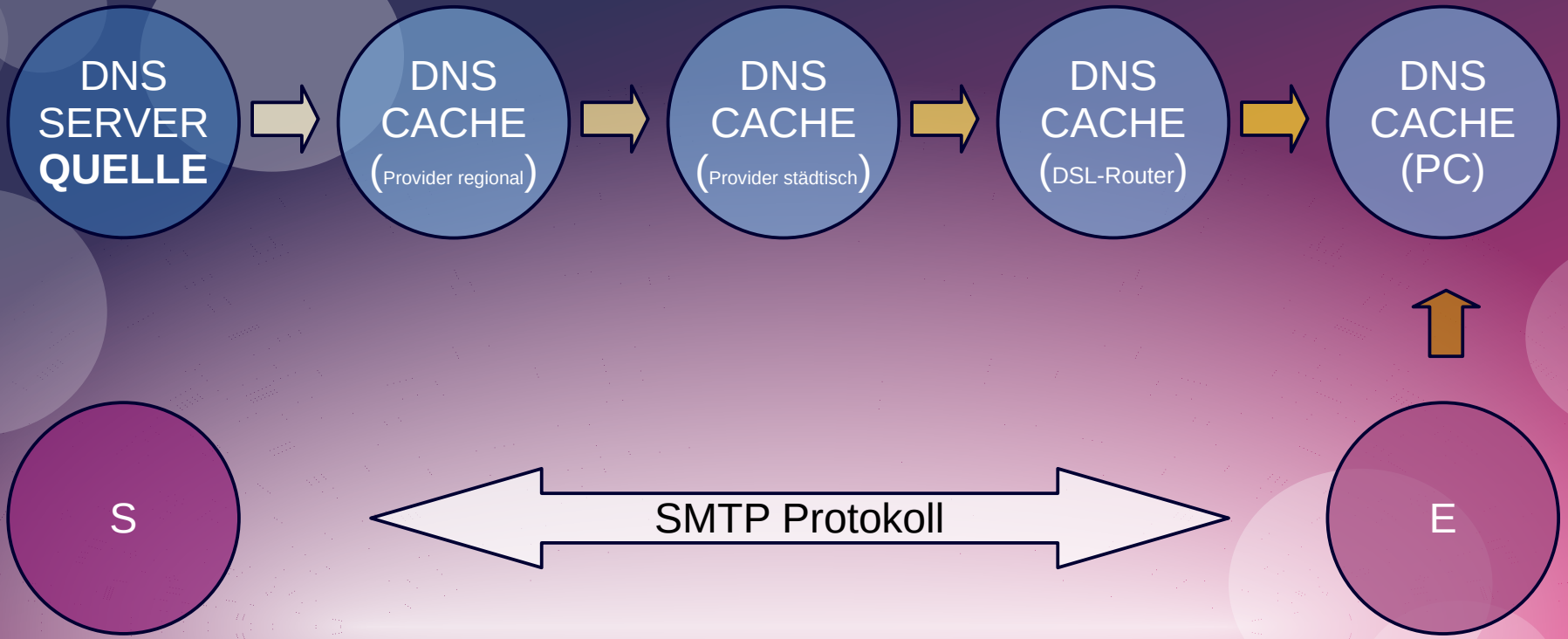
PTR Abfragen von E über diverse Cache



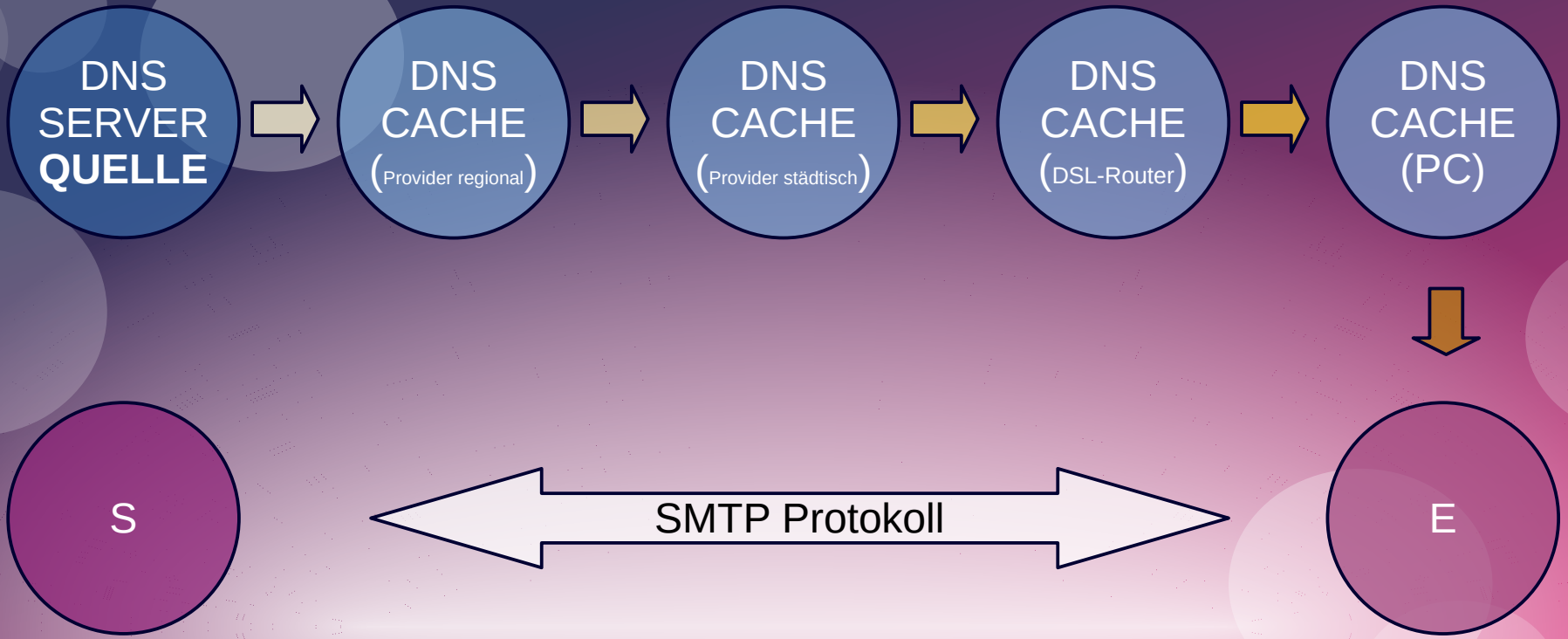
PTR Abfragen von E über diverse Cache



PTR Abfragen von E über diverse Cache



PTR Abfragen von E über diverse Cache



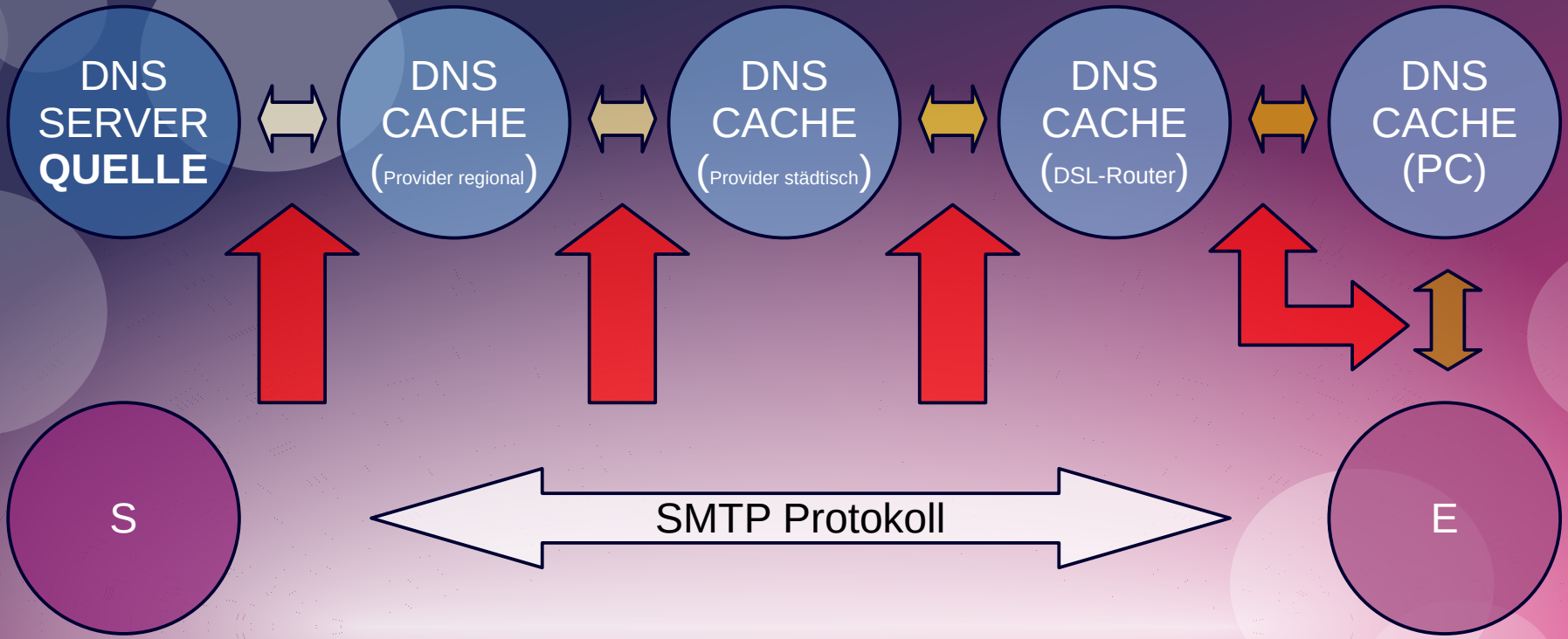
Das Netz ist nicht perfekt

„Was kann da schon schiefgehen!“

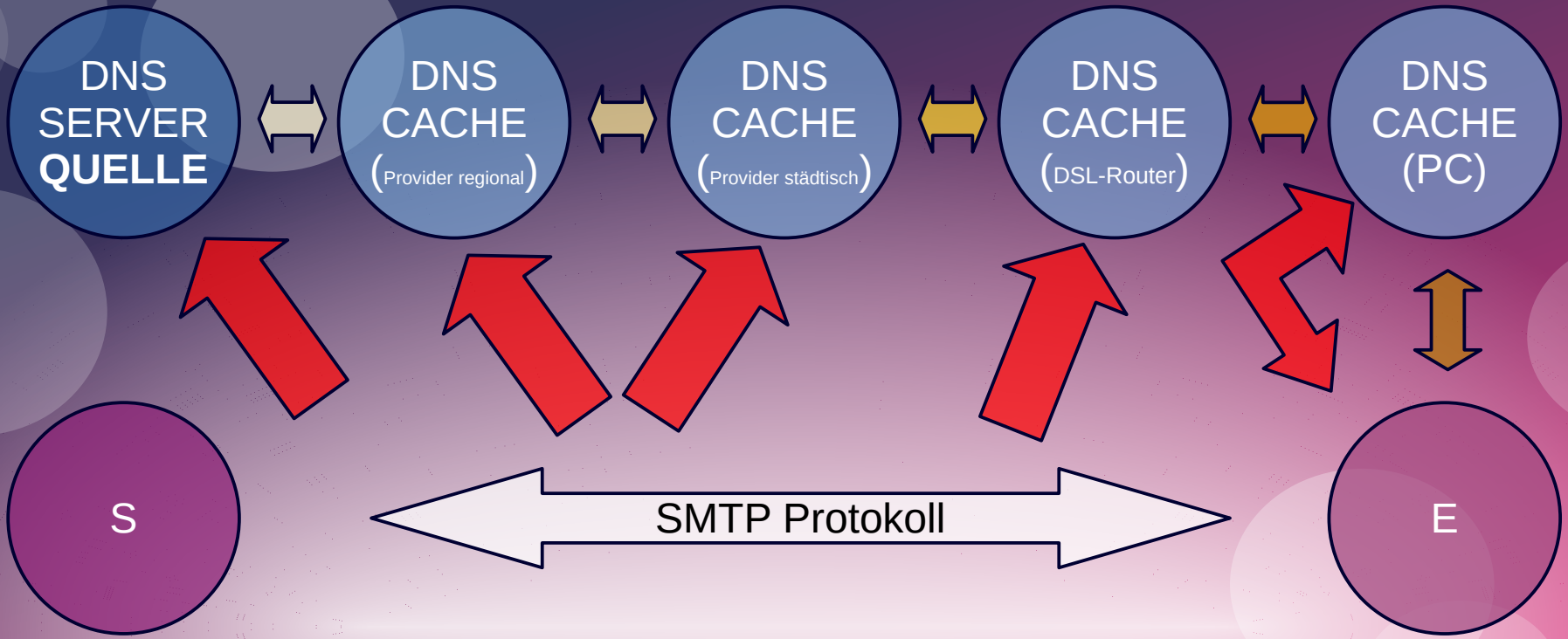
Das Netz ist nicht perfekt

Alles!

Wahrscheinlichste Fehlerquellen!



Wahrscheinlichste Fehlerquellen!



Das Netz ist nicht perfekt

Natürlich sähe die Lage in einem Rechenzentrum nicht viel anders aus.

Als Serverbetreiber hätte man aber auch die Option den RZ DNS zu übergehen und das Resolving selbst zu machen.

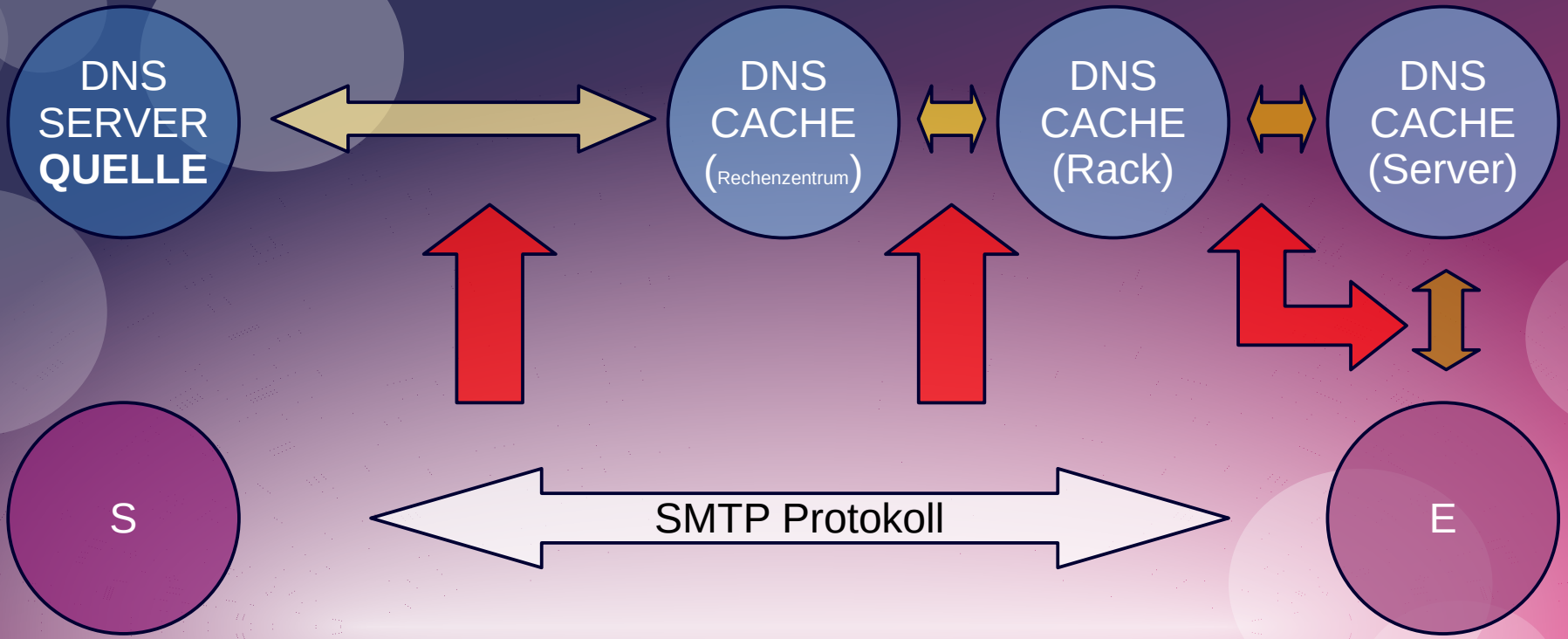
Das Netz ist nicht perfekt

Die **PTR** Abfrage wird über eine

Kette von **DNS Caches** durchgeführt,

die für Netzwerkstörungen anfällig ist.

Wahrscheinlichste Fehlerquellen!



UDP geht als erstes verloren

DNS Anfragen werden auch heute noch oft mit UDP durchgeführt, was bei Netzwerkstörungen als erstes von einem betroffenen Router gedroppt werden darf.

Das ist per se auch nicht schlimm.

Das Netz ist nicht perfekt

Temporäre Störungen dieser Ketten treten täglich

millionenfach auf.

Das Netz ist nicht perfekt

Nicht tragisch, denn

die Dienste können damit umgehen!

Ich frage einfach nochmal...

Ein **DNS-Resolver**, der macht die PTR Auflösung, schickt mehrere Pakete los.

Erst wenn alle Pakete unbeantwortet bleiben, erfolgt eine negative Antwort.

Keine Antwort, Keine Email!

Der empfangene Mailserver lehnt jetzt aufgrund der nicht erfolgten Antwort die Email ab.

z.B. mit „Host 1.2.3.4 lacks reverse DNS“

ABER

Das wäre noch nicht schlimm.

Die Störung könnte ja weg sein..

Nach einigen Minuten oder Stunden,
wenn die nächste Email geschickt wird,
versuchen es die DNS Cache erneut.

...oder doch nicht?

„Schlimm“ wird es erst, wenn die Störung tagelang anhält und das eine andere Ursache hat, als man denken würde:

NEGATIVE CACHING

Oh Oh

oder noch schlimmer:

Die DNS-Cache-Software hat sich verhaspelt

Der kleine GAU

Ein Negative Caching läuft nach einer Zeitspanne von Stunden,Tagen oder Wochen ab, dann **versucht es das Cache neu**.

Es verhindert, dass das Cache unsinnige Anfragen wieder und **wieder** und **WIEDER!** stellt.

Der Super-GAU

Wenn die Cache-Server Software z.B. BIND beim Negative Caching stolpert, und das kommt gelegentlich vor, dann wird das Cache NIE WIEDER neu nachfragen!

Der Super-GAU

Da kann der PTR Record so korrekt in der DNS-Zone eingetragen sein,
wie man möchte.

Die Email kommt nicht mehr an.

Die Rolle von PTR Abfragen bei Mailservern

„Selbst ist der Fachmann!“
namenloser Linuxadmin
(glaubt an Linus Torvals)

Wie können wir das selbst prüfen?

Tests mit **Linux**:

Der einfache Test des benutzten DNS-Caches des Pcs/Servers:

$ host 83.246.80.144
144.80.246.83.in-addr.arpa is an alias for 144.128/27.80.246.83.in-addr.arpa.
144.128/27.80.246.83.in-addr.arpa domain name pointer **s129.resellerdesktop.de**.

Damit sehen wir NUR die Antwort von dem eingestellten DNS Cache,

nicht was der zuständige DNS-Server wirklich sagt.

Wichtig, wenn keine Antwort kommt!

Wie können wir das selbst prüfen?

Fragen wir mal die ROOT-Nameserver nach dem PTR Record für die IP 83.246.80.144:

```
# dig  +trace PTR  144.80.246.83.in-addr.arpa
…
;; Received 327 bytes from 2001:13c7:7002:3000::14#53(ns3.lacnic.net) in 194 ms

144.80.246.83.in-addr.arpa. 86400 IN    CNAME 144.128/27.80.246.83.in-addr.arpa.
128/27.80.246.83.in-addr.arpa. 86400 IN      NS  ns2.resellerdesktop.de.
128/27.80.246.83.in-addr.arpa. 86400 IN      NS  c1.resellerdesktop.de.
;; Received 133 bytes from 185.136.98.195#53(pns03.dcsix.net) in 7 ms
```

Freundlicherweise bekommen wir die zuständigen Nameserver auch mitgeteilt.

Wie können wir das selbst prüfen?

Weil wir einen **CNAME** bekommen haben für eine Delegation nach RFC 2317,

müssen wir nochmal fragen:

```
# dig  +trace PTR  144.128/27.80.246.83.in-addr.arpa
…
128/27.80.246.83.in-addr.arpa. 86400 IN      NS  ns2.resellerdesktop.de.
128/27.80.246.83.in-addr.arpa. 86400 IN      NS  c1.resellerdesktop.de.
;; Received 115 bytes from 185.136.96.195#53(pns01.dcsix.net) in 7 ms

144.128/27.80.246.83.in-addr.arpa. 300 IN PTR  s129.resellerdesktop.de.
;; Received 99 bytes from 83.246.67.243#53(c1.resellerdesktop.de) in 0 ms
```

Wie können wir das selbst prüfen?

Jetzt für **Windows**:

```
# nslookup -query=ptr 144.128/27.80.246.83.in-addr.arpa.
Server:         83.246.80.131
Address:        83.246.80.131#53

Non-authoritative answer:
144.128/27.80.246.83.in-addr.arpa  name = s129.resellerdesktop.de.
```

Authoritative answers can be found from:
…

WICHTIG: NSLOOKUP zeigt an, welches Cache es gefragt hat.

Wie können wir das selbst prüfen?

Jetzt für **Windows** und wir fragen den zuständigen Server ab:

nslookup -query=ptr 144.128/27.80.246.83.in-addr.arpa. **c1.resellerdesktop.de**
Server: **c1.resellerdesktop.de**
Address: 83.246.67.243#53

144.128/27.80.246.83.in-addr.arpa name = **s129.resellerdesktop.de**.

Den zuständigen DNS-Server und die Schreibweise des PTR Records entnehmen wir hier einfach der Linuxausgabe, mit NSLOOKUP ist das sehr aufwändig, aber es geht ;)

Die Lehre die wir ziehen sollten...

Merke:

Erst den zuständigen DNS-Server fragen,
dann Rückschlüsse auf die Fehlerursache ziehen.

Die Rolle von PTR Abfragen bei Mailservern

„Und jetzt? Wie fixen wir das?“

Unbekannter Admin #2
(Kakteen-Experte)

Es könnte so einfach sein...

Einfach mal das „unwillige“ Cache neustarten.

Es könnte so einfach sein...

Wirkt Wunder!

Die Rolle von PTR Abfragen bei Mailservern

„Gibt es noch andere Möglichkeiten?“

Unbekannter Admin #1
(Whiskey-Experte)

Es könnte so einfach sein...

Natürlich:

Der Softwarestack des Mailservers, oder eines beteiligten Caches, könnte mit der Antwort „CNAME“ auf die Frage nach „PTR“ unzufrieden sein und das als „Gibt es nicht“ werten.

Es könnte so einfach sein...

Die Folgen wären die gleichen,
als wenn ein Cache eine Störung gehabt hätte,
oder es tatsächlich keinen PTR gäbe.

Die Rolle von PTR Abfragen bei Mailservern

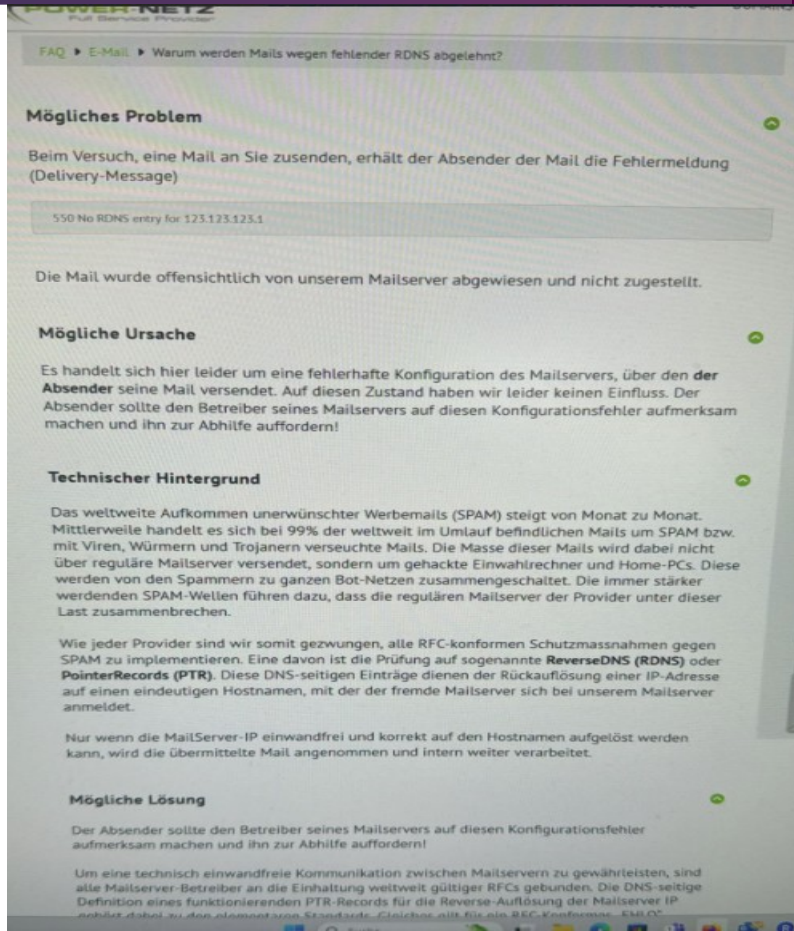
„Vertrauen Sie mir, ich weiß was ich tue!“

Sledge Hammer
(Experte beim LAPD)

Was Experten zu „Experten“ macht

Das nebenstehende Handyfoto wurde uns von einem „Experten“ zu gespielt.

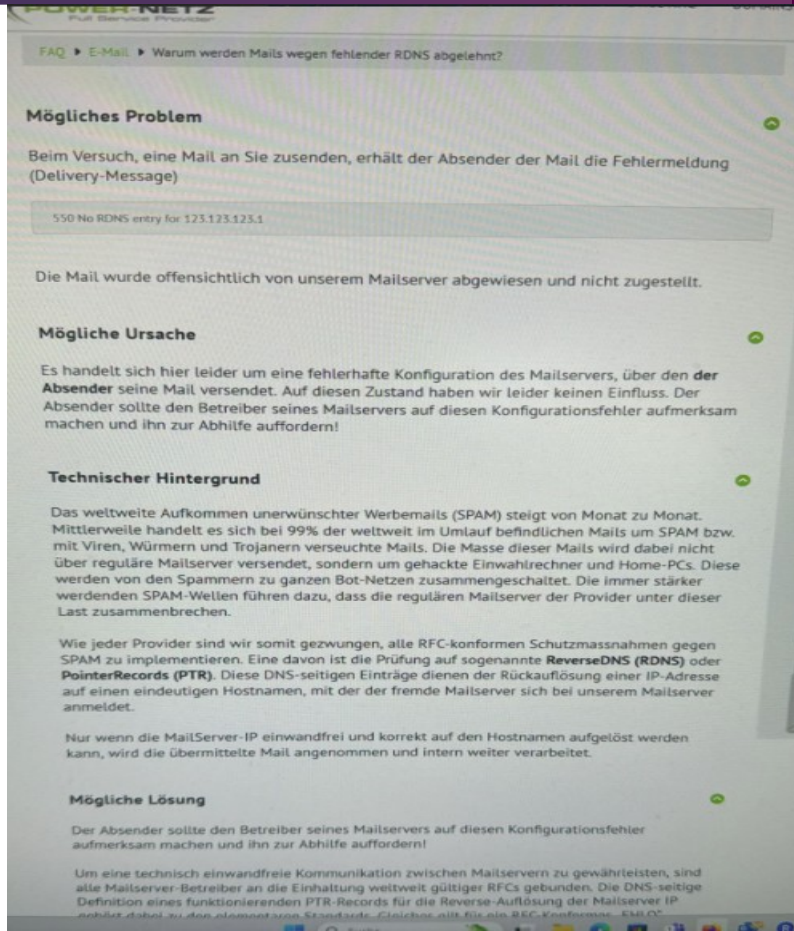
Wir sollen gefälligst tun, was in dieser Bibel steht und das Problem so lösen!



Was Experten zu „Experten“ macht

„Natürlich“ hätten wir auch den Link zur Webseite akzeptiert.

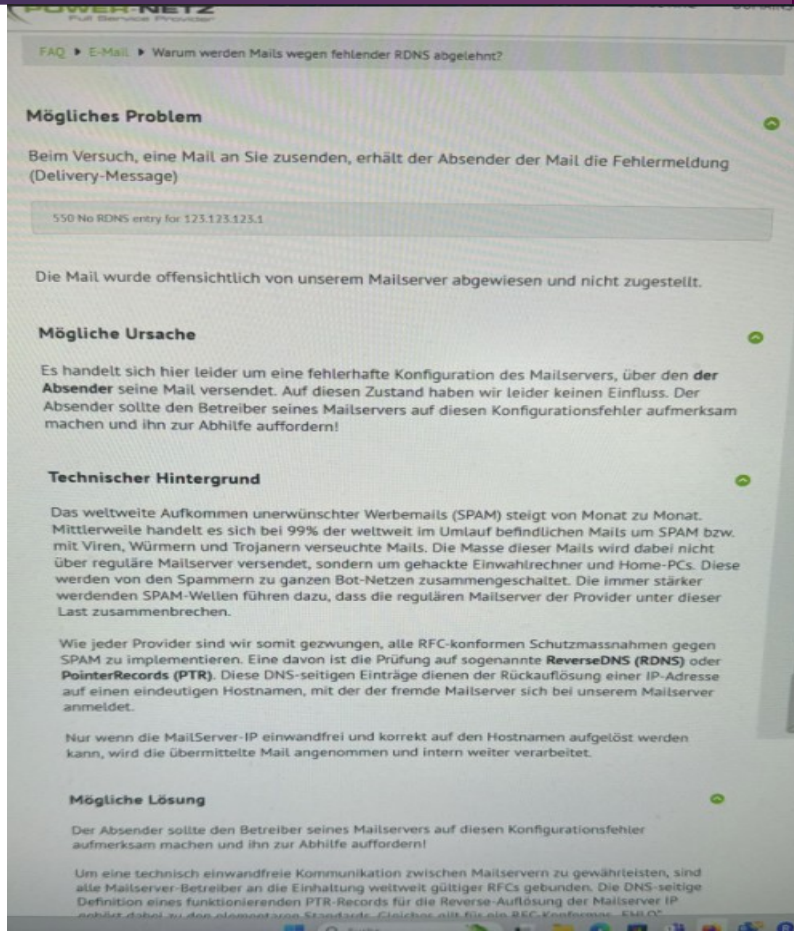
Schade nur, dass die *Möglich*keiten* dieser Webseite unbeachtet blieben ;)



*) „Führende IT Spezis Deutschlands“ haben es aber scheinbar nicht gelesen oder verstanden. Sonst wäre Ihnen **möglich**erweise das „möglich“ aufgefallen.

Was Experten zu „Experten“ macht

Nach nur 5 Stunden Schuldzuweisungen und falsch informierter und verstandener „führenden IT Spezis Deutschlands“ per WhatsApp, Email und Telefon platzte dann dem Kunden der Kragen und er beendete die weitere Kommunikation.

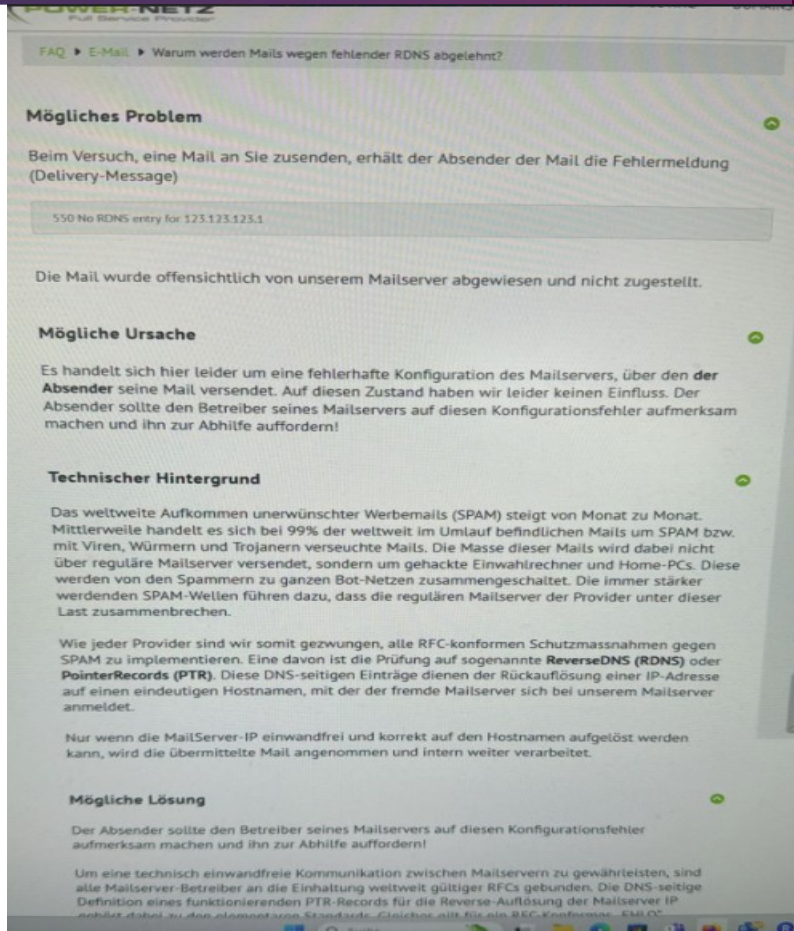


Was Experten zu „Experten“ macht

Der COO der rechts zitierten Firma lies noch am selben Tag mitteilen:

„Hallo …

vielen Dank für den Hinweis. Bei nächster Gelegenheit werden wir den Beitrag komplett überarbeiten.„ :D



FAQ ▸ E-Mail ▸ Warum werden Mails wegen fehlender RDNS abgelehnt?

Mögliches Problem

Beim Versuch, eine Mail an Sie zusenden, erhält der Absender der Mail die Fehlermeldung (Delivery-Message)

550 No RDNS entry for 123.123.123.1

Die Mail wurde offensichtlich von unserem Mailserver abgewiesen und nicht zugestellt.

Mögliche Ursache

Es handelt sich hier leider um eine fehlerhafte Konfiguration des Mailservers, über den **der Absender** seine Mail versendet. Auf diesen Zustand haben wir leider keinen Einfluss. Der Absender sollte den Betreiber seines Mailservers auf diesen Konfigurationsfehler aufmerksam machen und ihn zur Abhilfe auffordern!

Technischer Hintergrund

Das weltweite Aufkommen unerwünschter Werbemails (SPAM) steigt von Monat zu Monat. Mittlerweile handelt es sich bei 99% der weltweit im Umlauf befindlichen Mails um SPAM bzw. mit Viren, Würmern und Trojanern verseuchte Mails. Die Masse dieser Mails wird dabei nicht über reguläre Mailserver versendet, sondern um gehackte Einwahlrechner und Home-PCs. Diese werden von den Spammern zu ganzen Bot-Netzen zusammengeschaltet. Die immer stärker werdenden SPAM-Wellen führen dazu, dass die regulären Mailserver der Provider unter dieser Last zusammenbrechen.

Wie jeder Provider sind wir somit gezwungen, alle RFC-konformen Schutzmassnahmen gegen SPAM zu implementieren. Eine davon ist die Prüfung auf sogenannte **ReverseDNS (RDNS)** oder **PointerRecords (PTR)**. Diese DNS-seitigen Einträge dienen der Rückauflösung einer IP-Adresse auf einen eindeutigen Hostnamen, mit der der fremde Mailserver sich bei unserem Mailserver anmeldet.

Nur wenn die MailServer-IP einwandfrei und korrekt auf den Hostnamen aufgelöst werden kann, wird die übermittelte Mail angenommen und intern weiter verarbeitet.

Mögliche Lösung

Der Absender sollte den Betreiber seines Mailservers auf diesen Konfigurationsfehler aufmerksam machen und ihn zur Abhilfe auffordern!

Um eine technisch einwandfreie Kommunikation zwischen Mailservern zu gewährleisten, sind alle Mailserver-Betreiber an die Einhaltung weltweit gültiger RFCs gebunden. Die DNS-seitige Definition eines funktionierenden PTR-Records für die Reverse-Auflösung der Mailserver IP

Am gleichen Tag

„Morgens, halb Zehn in Deutschland“

Mailversand an den Zielkontakt:

2024-02-29 **09:47:27** 1rfc4d-00000009Qpy-0OIc ** [HIDDEN] R=dnslookup T=remote_smtp H=mailgw.[DOMAIN] [HIDDEN] X=TLS1.3:TLS_AES_256_GCM_SHA384:256 CV=yes: SMTP error from remote mail server after RCPT TO:<HIDDEN@DOMAIN>: **550 Missing RDNS entry.**

Am gleichen Tag

„550 Missing RDNS entry.“

Ist die monierte Fehlermeldung des empfangenen Mailservers.

Die Rolle von PTR Abfragen bei Mailservern

Einen Tag später

Einen Tag später

Kurz vor 5: „... da kommt ja eine Mail am Ziel an!“

2024-03-01 **16:48:18** 1rg4UD-0000000GUup-1NS5 =>
gibts.nicht.weil.test@[DOMAIN] R=dnslookup T=remote_smtp H=mailgw.
[DOMAIN] [HIDDEN] X=TLS1.3:TLS_AES_256_GCM_SHA384:256 CV=yes
C="250 OK id=1rg52T-0006Km-1U"
2024-03-01 **16:48:18** 1rg4UD-0000000GUup-1NS5 **Completed**

Einen Tag später

Na so was … !

Die Rolle von PTR Abfragen bei Mailservern

PASSIVE DNS TESTING

Einen Tag später

Wir müßten mal die DNS Cache fragen,
welches von denen keine Antwort bekommen hat.

Leider kennen wir die nicht.

PASSIVE DNS SCANNING

Und wir können die DNS Cache des Mailservers
und des Telekom Rechenzentrums nicht direkt abfragen,
weil die das natürlich nur aus dem eigenen Netz erlauben.

Machen wir nicht anders ;)

PASSIVE DNS SCANNING

Da müssen wir wohl **andere** Methoden auffahren!

PASSIVE DNS SCANNING

Schritt 1:

Aufklärung

PASSIVE DNS SCANNING

1. Frage:

Wer wird unseren Server überhaupt fragen?

PASSIVE DNS SCANNING

1. Antwort:

Der letzte/äußerste DNS Cache in der Kette.

PASSIVE DNS SCANNING

2. Frage:

Wird der uns überhaupt fragen?

Wir nehmen ja schließlich an, dass Negative Caching im Spiel ist.

PASSIVE DNS SCANNING

2. Antwort:

Negative Caching kann es entweder für einen Eintrag geben, entweder für den RR selbst oder den Nameserver des RR.

Kann man von außen nicht wissen.

PASSIVE DNS SCANNING

Wie haben wir das also gemacht?

In dem wir von einem nie für den Mailversand genutzten **anderen** Mailserver eine Email an den aufzuklärenden Mailserver geschickt haben.

Schritt 1 einer Validitätsprüfung ist ja: **PTR** Record anfordern ;)

PASSIVE DNS SCANNING

Also können wir den DNS Server

des empfangenen Mailservers identifizieren:

15:13:27.208869 IP **217.237.149.168**.4794 > 85.214.124.40.53: 1841 [1au] PTR? 158.128/27.80.246.83.in-addr.arpa. (62)

15:13:27.210673 IP 85.214.124.40.53 > **217.237.149.168**.4794: 1841*- 1/0/1 PTR s164.resellerdesktop.de. (99)

Bekannt als : h-dns-a05.isp.t-ipnet.de.

(T- wie in TELEKOM-IPNET)

PASSIVE DNS SCANNING

Leider können wir das Cache **von außen** nicht direkt fragen,

es antwortet nur Servern in seinem Netzsegment.

PASSIVE DNS SCANNING

Macht nichts :D

Wir wollen eh die **ganze** Kette checken!

PASSIVE DNS SCANNING

Schritt 2:

Noch eine EMail vom „Mailserver ohne PTR“ senden :)

PASSIVE DNS SCANNING

Bitte Uhrzeit merken!

2024-03-01 **16:07:45** 1rg4UD-0000000GUup-1NS5 <= security@s129.resellerdesktop.de H=localhost (localhost.localdomain) [127.0.0.1] P=esmtp S=521

2024-03-01 **16:07:45** 1rg4UD-0000000GUup-1NS5 H=mailgw.[DOMAIN] [HIDDEN]: SMTP error from remote mail server after end of data: **451 Temporary local problem, please try again!**

16:07:45

PASSIVE DNS SCANNING

SMTP Antwort: „451 Temporary local problem, please try again!“

„Ah, Greylisting getriggert!“

und was war dazu nötig?

PASSIVE DNS SCANNING

Na die PTR Abfrage natürlich!

und da wir den Server von dem es kommen mußte kennen:

16:07:45.488045 IP **217.237.149.168**.62991 > 85.214.124.40.53: 27103 [1au] PTR? 144.128/27.80.246.83.in-addr.arpa. (62)

16:07:45.488987 IP 85.214.124.40.53 > **217.237.149.16**8.62991: 27103*- 1/0/1 **PTR s129.resellerdesktop.de.** (99)

Konnten wir den Zugriff von den hunderten Anderen gleichartigen Zugriffen auf unseren DNS identifizieren. THX TCPDUMP!

Die Rolle von PTR Abfragen bei Mailservern

Schlußfolgerungen

„Logik ist Dein Freund“

PASSIVE DNS SCANNING

Das beweist,

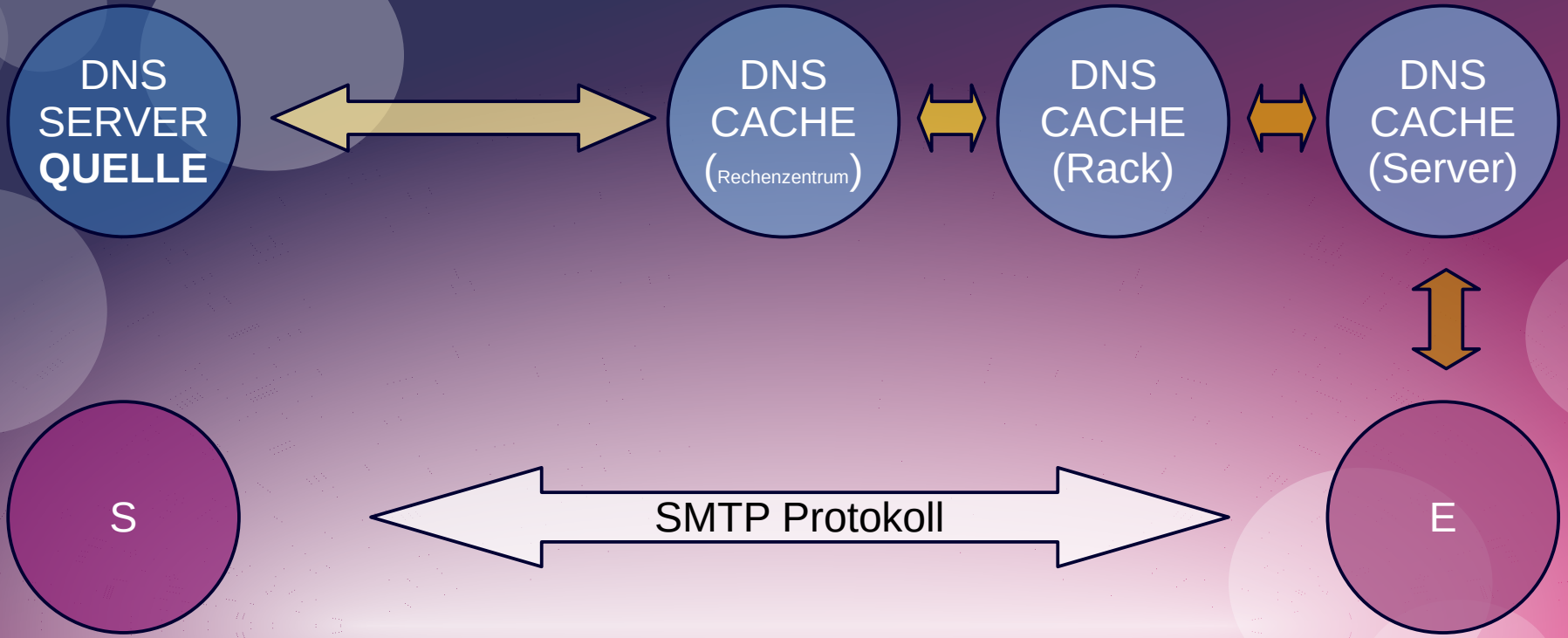
das der PTR min. bis zum DTAG Cache gelangt ist.

(und das es den PTR auch gibt ;))

PASSIVE DNS SCANNING

Erinnert Ihr Euch noch an diese Grafik?

DNS CACHE KETTE



PASSIVE DNS SCANNING

Damit das Telekom DNS-Cache

unseren Server abfragen kann,

muß der Mailserver sein Cache fragen,

das dann sein Cache fragt usw.

PASSIVE DNS SCANNING

Die ganze Kette **muß** funktioniert haben,

sonst hätten wir den Zugriff nicht gesehen.

PASSIVE DNS SCANNING

Damit ist logisch bewiesen,

daß die Cache alle einwandfrei funktioniert haben.

PASSIVE DNS SCANNING

Heute!

PASSIVE DNS SCANNING

GESTERN,

hat min. eines nicht funktioniert.

PASSIVE DNS SCANNING

Wir haben nämlich nichts geändert :D

PASSIVE DNS SCANNING

Zwei Möglichkeiten:

das Negative Caching ist abgelaufen (worden)

oder

ein „Experte“ hat sein DNS Cache rebootet :)

PASSIVE DNS SCANNING

Das „worden“ muß ich erklären:

Wenn eines der Cache den ZielDNS im Negative Caching hatte,

weil es ja keine Antwort bekam,

kann, muß aber nicht, eine Abfrage nach einem anderen PTR

beim gleichen ZielDNS die Blockade lösen.

Die Rolle von PTR Abfragen bei Mailservern

DANKE :)