Grundlagen: Rechnernetze und verteilte Systeme

Elfte Woche: 2./6. Juli 2018

NAT, DNS

Leo Glavinić
netze@eo.gl
eo.gl/netze

Inhalt

1. Network Address Translation (NAT, Schicht 4)

2. Domain Name System (DNS, Schicht 7)

1. Network Address Translation

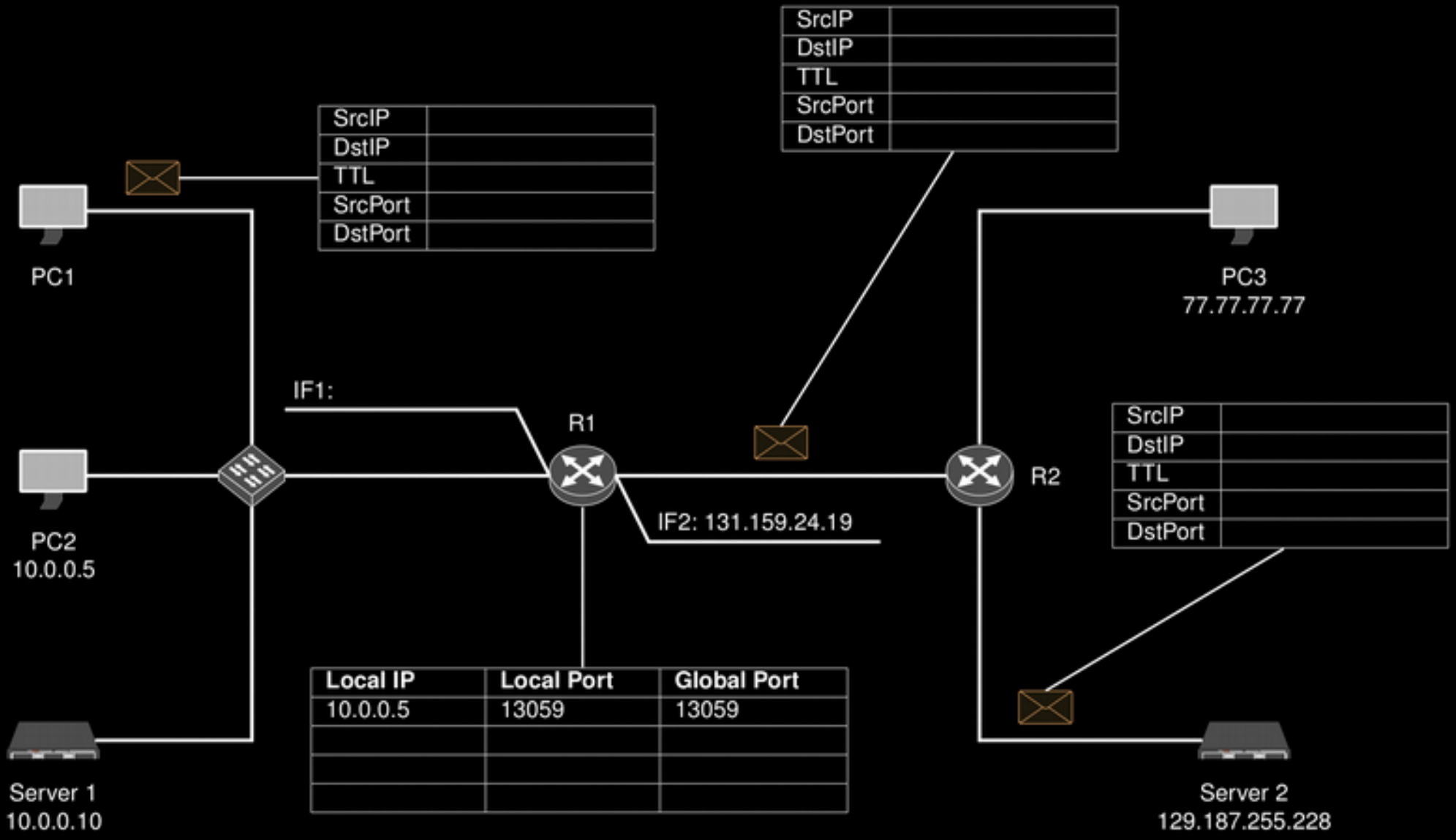
Zuordnung zwischen öffentlichen und privaten IP-Adressen: Abbildungstabelle bei NAT-fähigen Routern (lokaler Port → globaler Port)

In diesem Beispiel: R1 mit NAT (private IP auf Interface 1, öffentliche IP auf Interface 2), R2 ohne NAT

PC2 hat bereits mit Server 2 kommuniziert → bereits vorhandener Eintrag

Bei Uneindeutigkeit: sinnvolle Werte wählen!

1. Network Address Translation



1. Network Address Translation

a. Passende IP-Adressen für PC1 und IF1 von R1 mit Subnetz 10.0.0.0/24

z.B.:
PC1: 10.0.0.1
R1 IF1: 10.0.0.254

1. Network Address Translation

b. Aufbau von HTTP-Verbindung PC1 → Server2; Paketinformationen an den drei Stellen ausfüllen, NAT-Tabelle von R1 vervollständigen

Zwischen PC1 und R1
SrcIP: Private IP-Adresse von PC1, s. Aufg. a
DstIP: 129.187.255.228 (Server 2)
TTL: Beliebig
SrcPort: Beliebig zwischen 1024 und 65535
DstPort: 80 (Well known port für HTTP)

1. Network Address Translation

b. Aufbau von HTTP-Verbindung PC1 → Server2; Paketinformationen an den drei Stellen ausfüllen, NAT-Tabelle von R1 vervollständigen

Zwischen R1 und R2
SrcIP: 131.159.24.19 (Öffentliche IP von R1)
DstIP: 129.187.255.228 (Server 2)
TTL: Vorherige TTL minus eins
SrcPort: Gleich, sofern nicht bereits belegt
DstPort: 80 (Well known port für HTTP)

1. Network Address Translation

b. Aufbau von HTTP-Verbindung PC1 → Server2; Paketinformationen an den drei Stellen ausfüllen, NAT-Tabelle von R1 vervollständigen

Zwischen R2 und Server 2
TTL: Noch mal dekrementiert
Alles andere bleibt gleich, da R2 kein NAT kann

1. Network Address Translation

b. Aufbau von HTTP-Verbindung PC1 → Server2; Paketinformationen an den drei Stellen ausfüllen, NAT-Tabelle von R1 vervollständigen

Neuer Eintrag in NAT-Tabelle von R1
Local IP: Private IP von PC1
Local Pt: Als SrcPort gewählte Portnummer
Global Pt: Gleich wie Local Port, falls nicht belegt

1. Network Address Translation

c. Antwort Server 2 → PC1

Zwischen Server 2 und R2:
SrcIP: 129.187.255.228 (Server 2)
DstIP: 131.159.24.19 (öffentliche IP von R1)
TTL: Beliebig
SrcPort: 80 (HTTP)
DstPort: SrcPort aus Aufg. b

1. Network Address Translation

c. Antwort Server 2 → PC1

Zwischen R2 und R1:
TTL wird dekrementiert, Rest bleibt gleich (weil kein NAT)

1. Network Address Translation

c. Antwort Server 2 → PC1

Zwischen R1 und PC1:
SrcIP: 129.187.255.228 (Server 2)
DstIP: Private IP von PC1
TTL: Nochmal runter
SrcPort: 80 (HTTP)
DstPort: Siehe Zuordnung in NAT-Tabelle

1. Network Address Translation

d. Aufbau einer TCP-Verbindung Server 1 → Server 2 auf Port 80, Absender-Port 13059; Problem bei NAT und Lösung?

Kollision mit erstem Eintrag in NAT-Tabelle: Bei Antwort von Server 2 keine mögliche Unterscheidung mehr zwischen PC1 und Server 2 als Empfänger

Lösung: NAT-Router prüft vor Erzeugung neuer Einträge, ob Portnummer bereits verwendet wird und wählt ggf. neue Nummer aus

1. Network Address Translation

e. R1 erhält von PC3 ein Paket an 131.159.24.19:13059. Was passiert?

R1 übersetzt Zieladresse gemäß NAT-Tabelle und leitet Paket an PC2 weiter, obwohl der ursprüngliche Eintrag für Server 2 angelegt wurde → Empfang von unerwartetem Paket bei PC2

Wir merken uns: NAT ist keine Firewall!

1. Network Address Translation

f. Problem für PC2 bei zufälligem Paket mit TCP-Payload auf einem Port mit bestehender Verbindung?

Wahrscheinlich andere Absender-IP und Source Port
→ gehört nicht zur Verbindung

Bei zufälliger Übereinstimmung: Sequenznummer fällt mit hoher Wahrscheinlichkeit nicht in das aktuelle Empfangsfenster

1. Network Address Translation

g. Weitere Unterscheidungskriterien im NAT-Router

Globale IP, Remote IP, Remote Port, Protokollnummer (TCP oder UDP)

1. Network Address Translation

hi. Problem bei Echo Request PC1 → Server 2;
Lösung hierfür?

ICMP ohne Portnummern → NAT-Router kann keinen Eintrag erzeugen, Antwort wird verworfen

Bei ICMP-Paketen könnte NAT-Router zusätzlich zur Protokollnummer den ICMP-Identifier als Portnummernersatz speichern; dann muss Router aber immer zwischen den IP-Protokollen (TCP, UDP, ICMP, ...) unterscheiden

1. Network Address Translation

j. Problem bei TTL-Exceeded-Nachrichten, die am NAT-Router ankommen und zum Empfänger weitergeleitet werden sollen? Lösung?

TTL-Exceeded-Nachrichten sind eigene ICMP-Nachrichten, deren Identifier nicht in der NAT-Tabelle steht; keine Zuordnung zum Empfänger möglich

Solche Nachrichten enthalten aber noch einen IP-Header und die ersten acht Payload-Bytes des auslösenden Pakets → Zustellung möglich

1. Network Address Translation

k. Klappt eine HTTP-Verbindung PC3 → Server 1?

PC3 kann das Paket nicht direkt an die Adresse 10.0.0.10 adressieren, weil privat → nicht geroutet

Wenn PC3 die öffentliche IP von R1 kennt, hinter dem sich Server 1 befindet, kann das Paket zwar an diese IP adressieren; R1 hat aber keinen passenden Eintrag in der NAT-Tabelle

1. Network Address Translation

I. Lösung dieses Problems in NAT

Portforwarding (statische Weiterleitung) im NAT eintragen; damit kann Server 1 auf der IP von R1 von außen auf Port 80 erreicht werden

2. Domain Name System (DNS)

Zentrale Aufgabe: Abbildung menschlich lesbarer Namen auf IP-Adressen für Wegwahl auf der Netzwerkschicht

Fully Qualified Domain Name (FQDN): zum Beispiel netze.eo.gl.

2. Domain Name System (DNS)

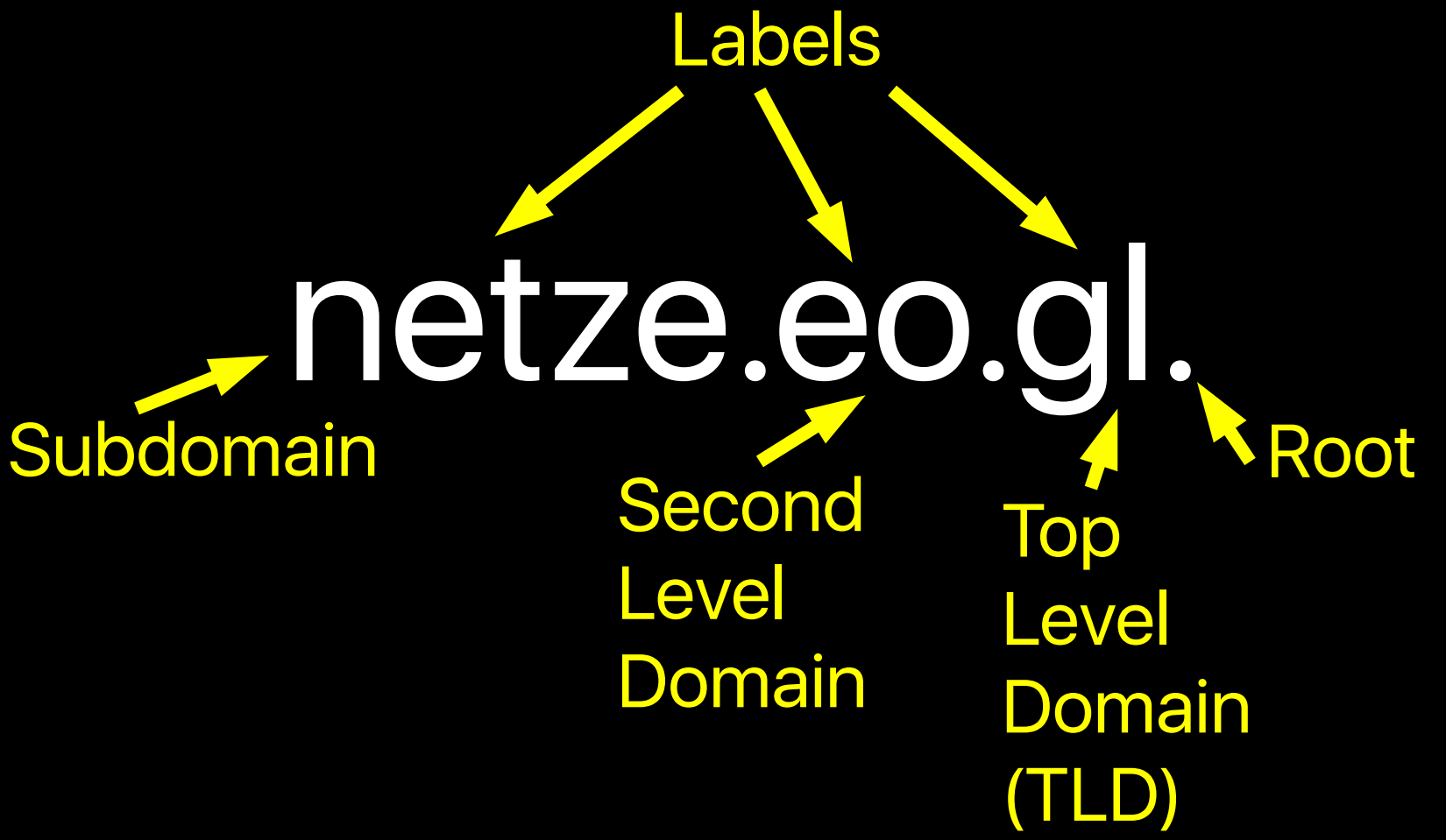
a. Unterschied zwischen FQDN und nicht voll-qualifiziertem Domainnamen

FQDN endet mit Punkt, also der Wurzel des gesamten Name Spaces

Nicht-qualifizierter Domain Name kann eigenes Label sein oder geordnete Liste von durch Punkte getrennten Labels (relativ zu einer anderen Wurzel als .)

2. Domain Name System (DNS)

b. Einzelne Bestandteile des FQDN



2. Domain Name System (DNS)

PC1 nutzt seinen Router als Resolver, dieser nutzt Google-Resolver unter IP 8.8.8.8; dieser ist gerade neu gestartet worden und bietet rekursive Namensauflösung an

Autoritative Nameserver für jeweilige Zonen:

Zone	autoritativer Nameserver
.	d.root-servers.net.
com., net.	a.gtld-servers.net.
google.com.	ns1.google.com.
grnvs.net.	bifrost.grnvs.net.

2. Domain Name System (DNS)

c. Unterschied zwischen Resolver und Nameserver

Nameserver: autoritativ für eine oder mehrere Zonen, besitzen also eine gültige Kopie der ganzen Zone

Resolver: Extraktion der benötigten DNS-Informationen aus einer Reihe von Anfragen an die Nameserver und Rückgabe an den anfragenden Client

2. Domain Name System (DNS)

d. Funktion von d.root-servers.net und a.gtld-servers.net

Root-Nameserver kennt die Nameserver, die für die einzelnen TLDs verantwortlich sind; a.gtld-servers.net kennt wiederum die zuständigen Nameserver für alle Second-Level-Domains unter net

2. Domain Name System (DNS)

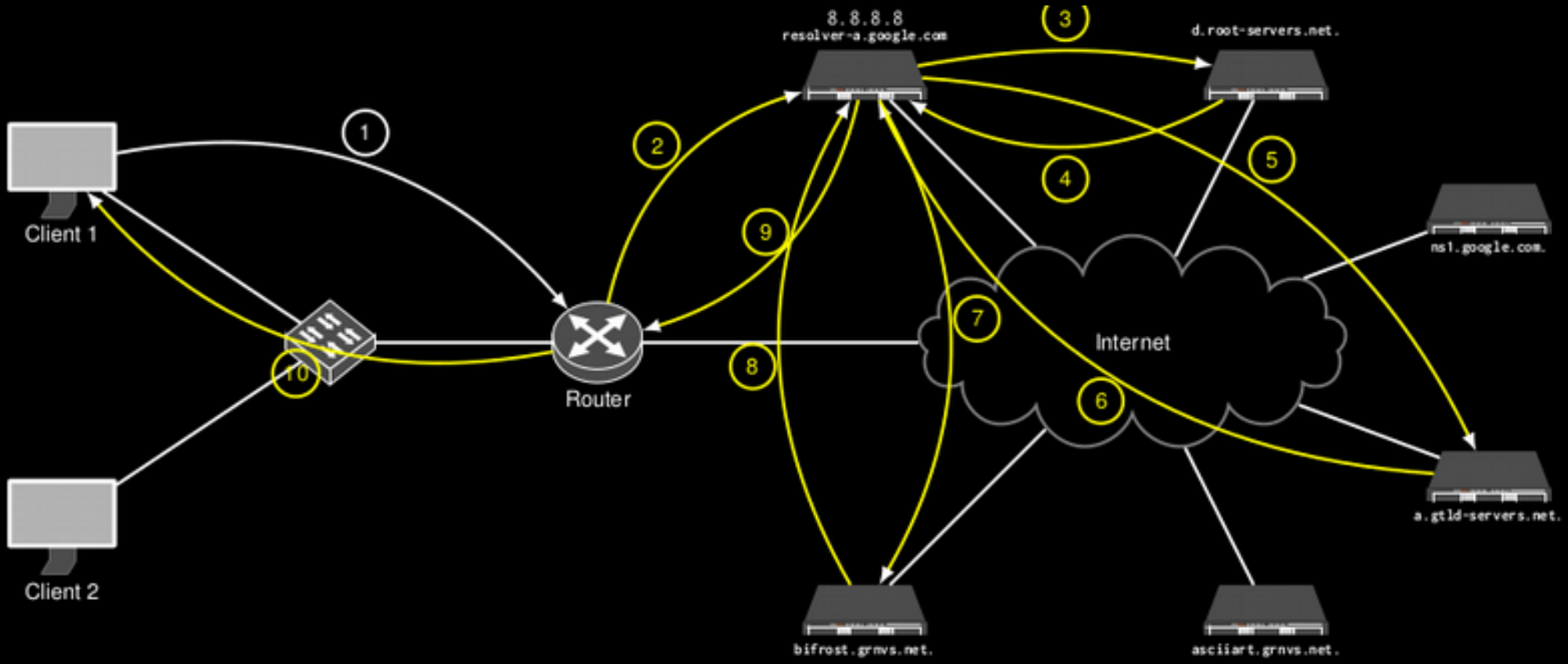
e. Unterschied zwischen iterativer und rekursiver Namensauflösung

Rekursiv: DNS-Anfrage wird an Resolver gestellt; dieser sendet das endgültige Ergebnis zurück

Iterativ: autoritative Nameserver der einzelnen Zonen werden schrittweise angefragt

2. Domain Name System (DNS)

f. DNS-Requests/-Responses in die Abbildung einzeichnen, wenn PC1 auf asciiart.grnvs.net. zugreift



2. Domain Name System (DNS)

g. Sicherstellung, dass kein bösartiger Nameserver Anfragen für andere Domänen beantwortet

Nur indirekte Sicherheit: bei der iterativen Namensauflösung werden stets nur die jeweils autoritativen Nameserver kontaktiert → eventuelle bösartige Nameserver werden also nie abgefragt

Man-in-the-middle-Angriffe sind aber trotzdem möglich (Abfang und Modifikation von DNS-Responses) → Kryptographie!

3. Kompression: Huffman-Code

„Hausaufgabe“