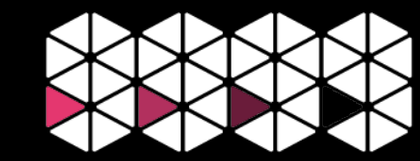


Quad9

Quad9:
A Free, Secure DNS Resolver

Nishal Goburdhan
Internet Infrastructure Analyst
Packet Clearing House
nishal@pch.net

What is the Domain Name System?

The Domain Name System (DNS) is the "phone book" of the Internet. It translates domain names like www.example.net into Internet Protocol addresses, like 93.184.216.34.

Every device that uses the Internet, whether it be a desktop computer, laptop, mobile phone, or an IoT device like a smart thermostat, television, or security camera, requires a DNS Recursive Resolver to perform this translation function.

All of this happens transparently to most Internet users.

The Domain Name System: Not so good for Cyber Crime and Privacy

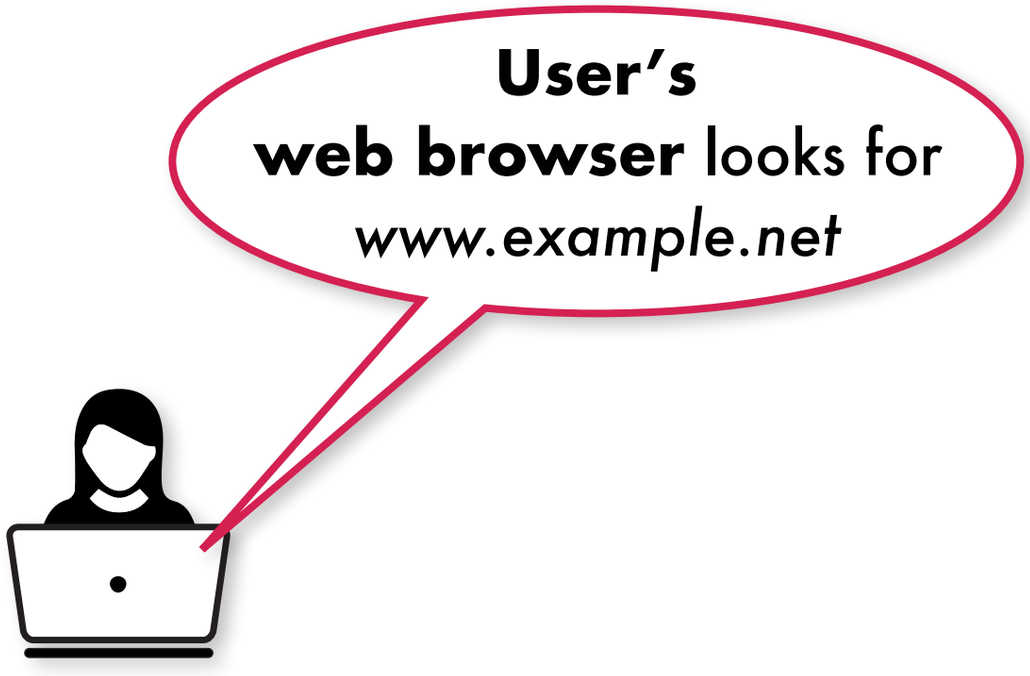
Since every Internet device is critically dependent on the Domain Name System the DNS is a very attractive target for criminals.

When the DNS is not sufficiently secured, it gives criminals easy inroads into every Internet-connected device.

This affects not just your computer and mobile phone, but your thermostat and television and refrigerator.

The DNS is thus a critical weak point which needs to be improved and reinforced through technical means.

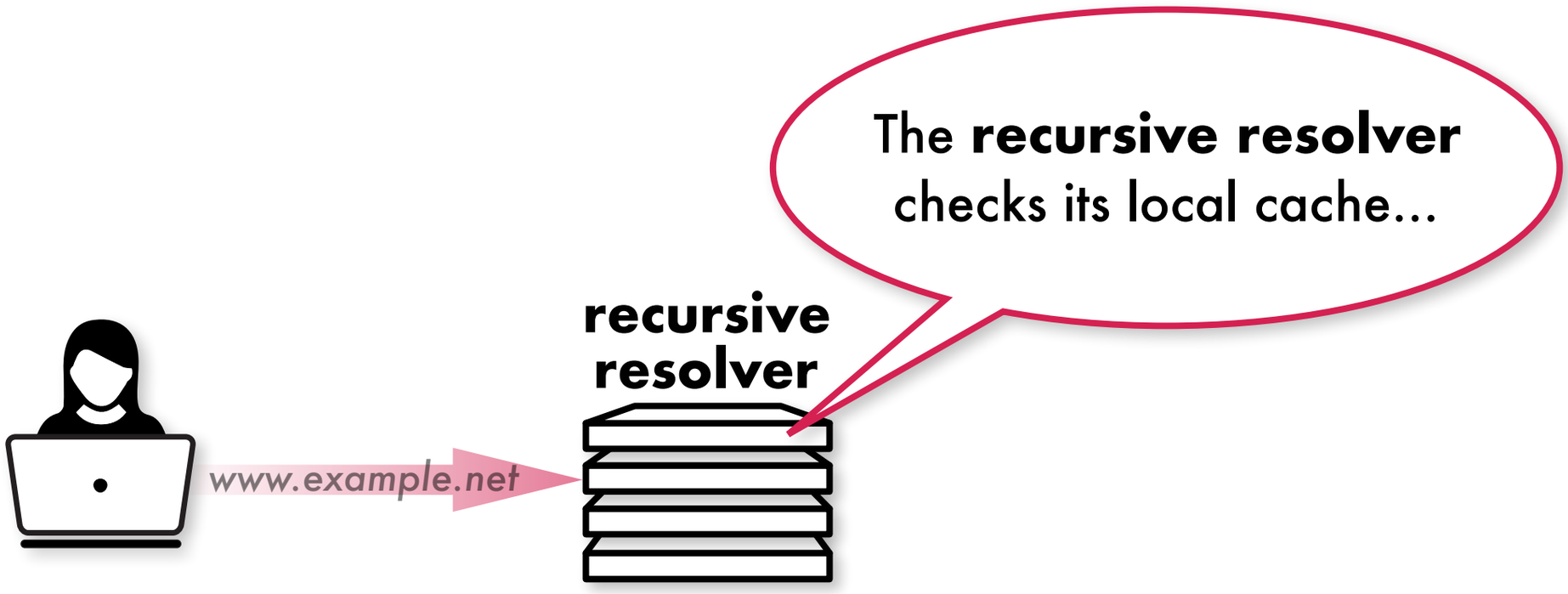
Overview of the Domain Name System



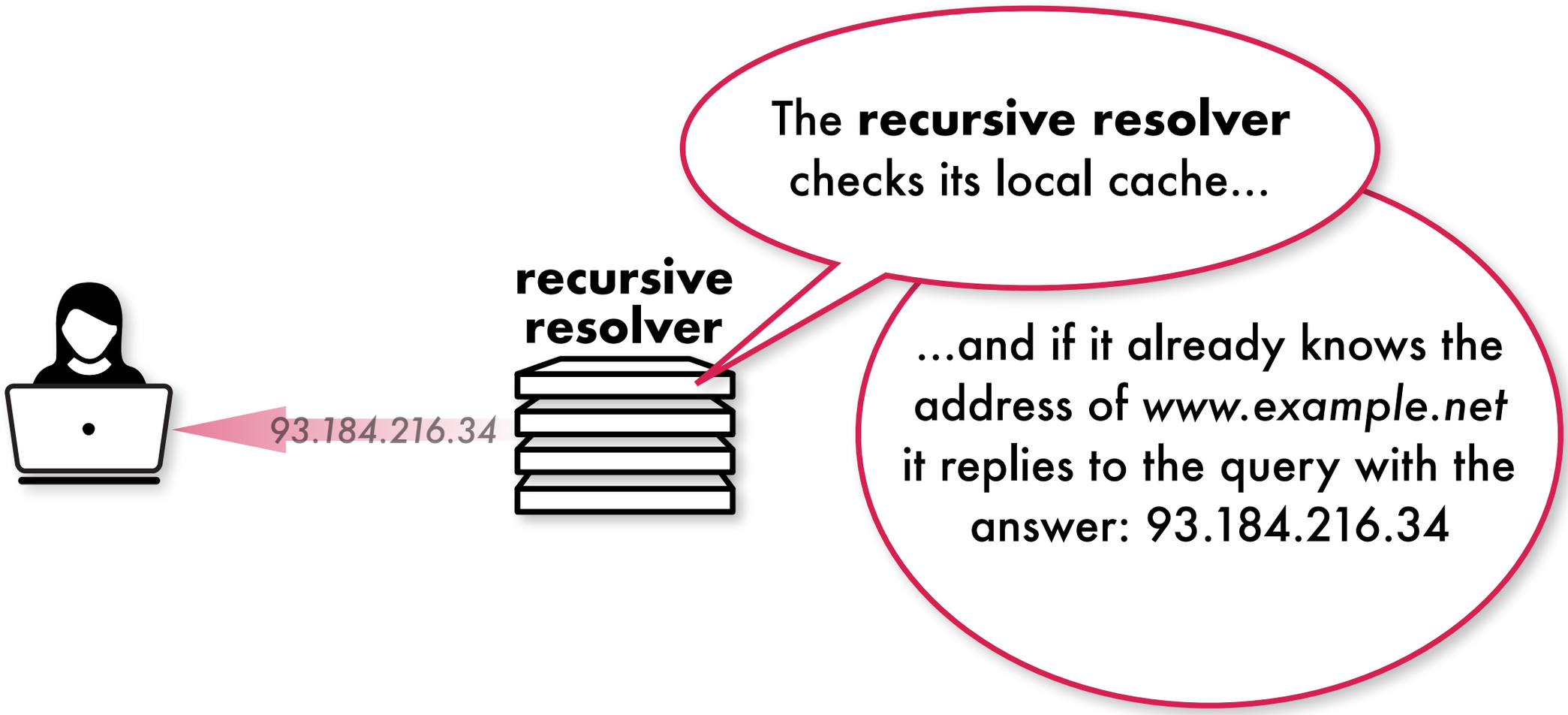
Overview of the Domain Name System

User's
computer sends a query
for *www.example.net*
to a **recursive resolver**

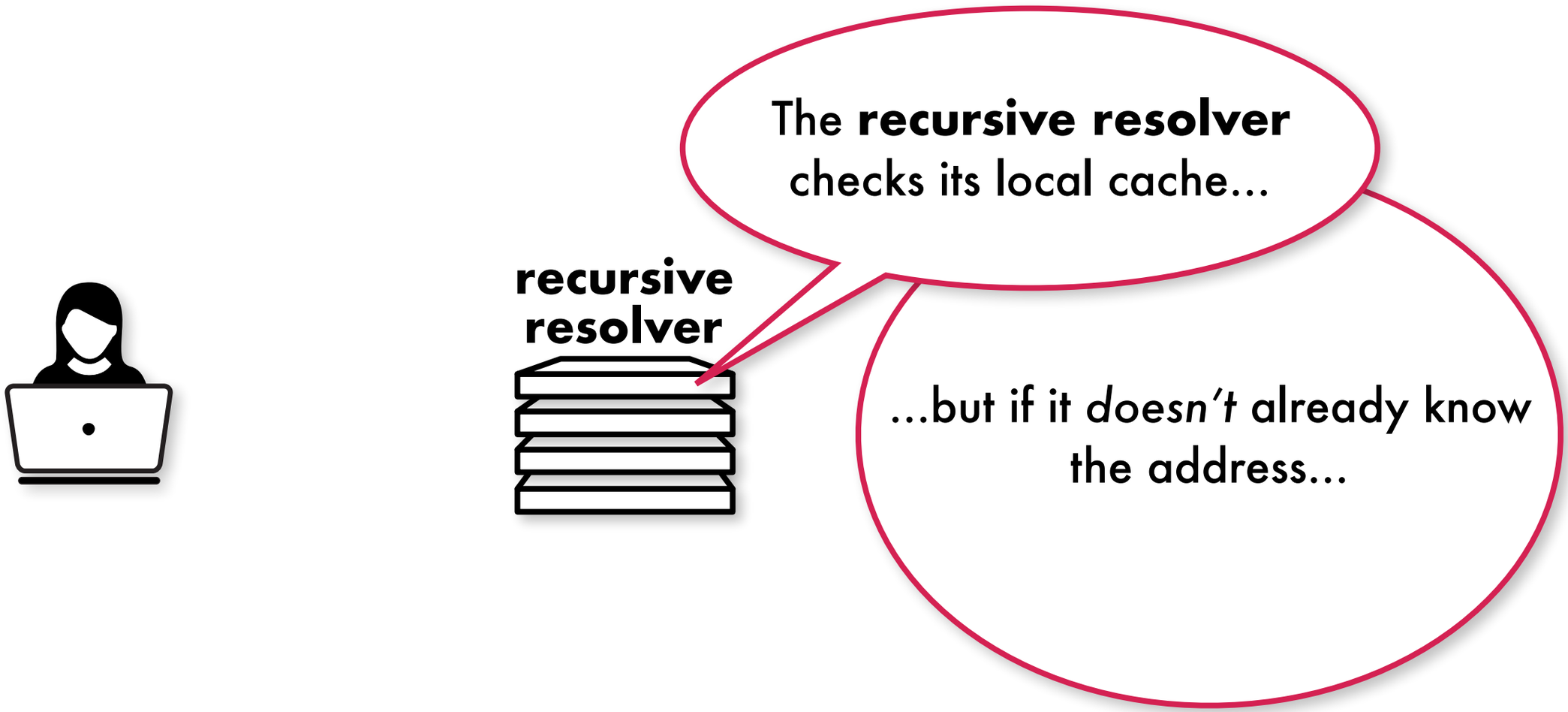
Overview of the Domain Name System



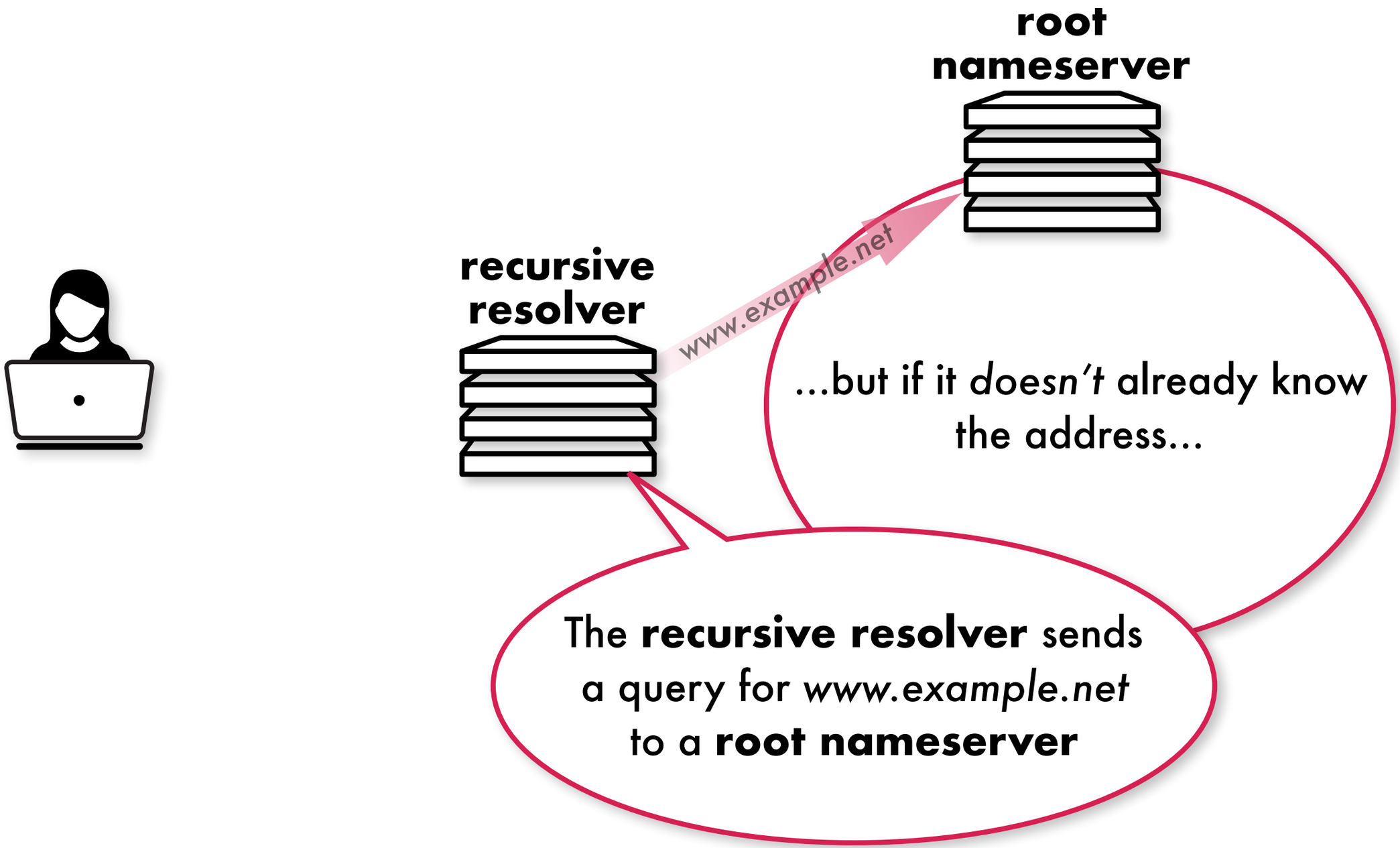
Overview of the Domain Name System



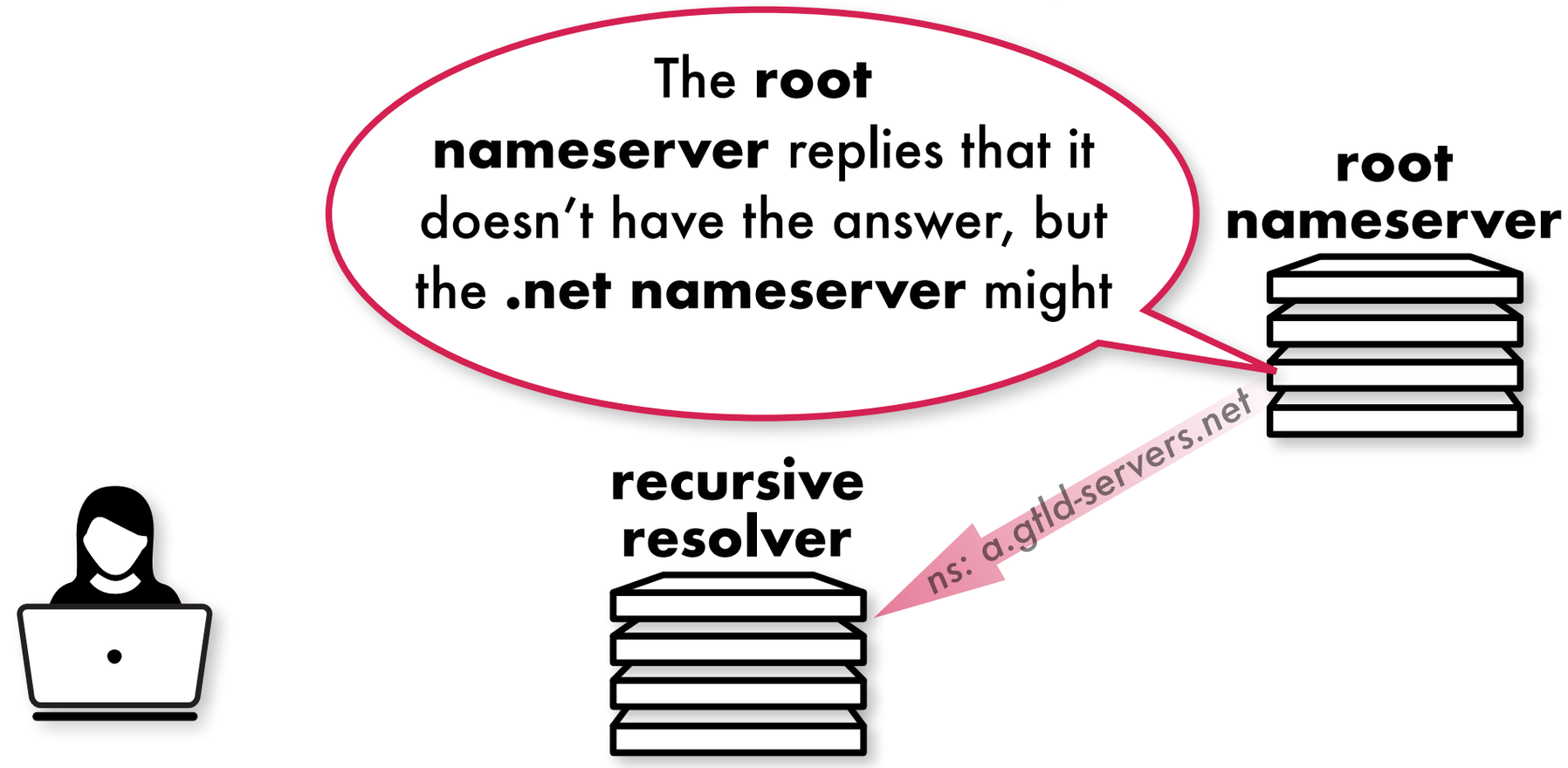
Overview of the Domain Name System



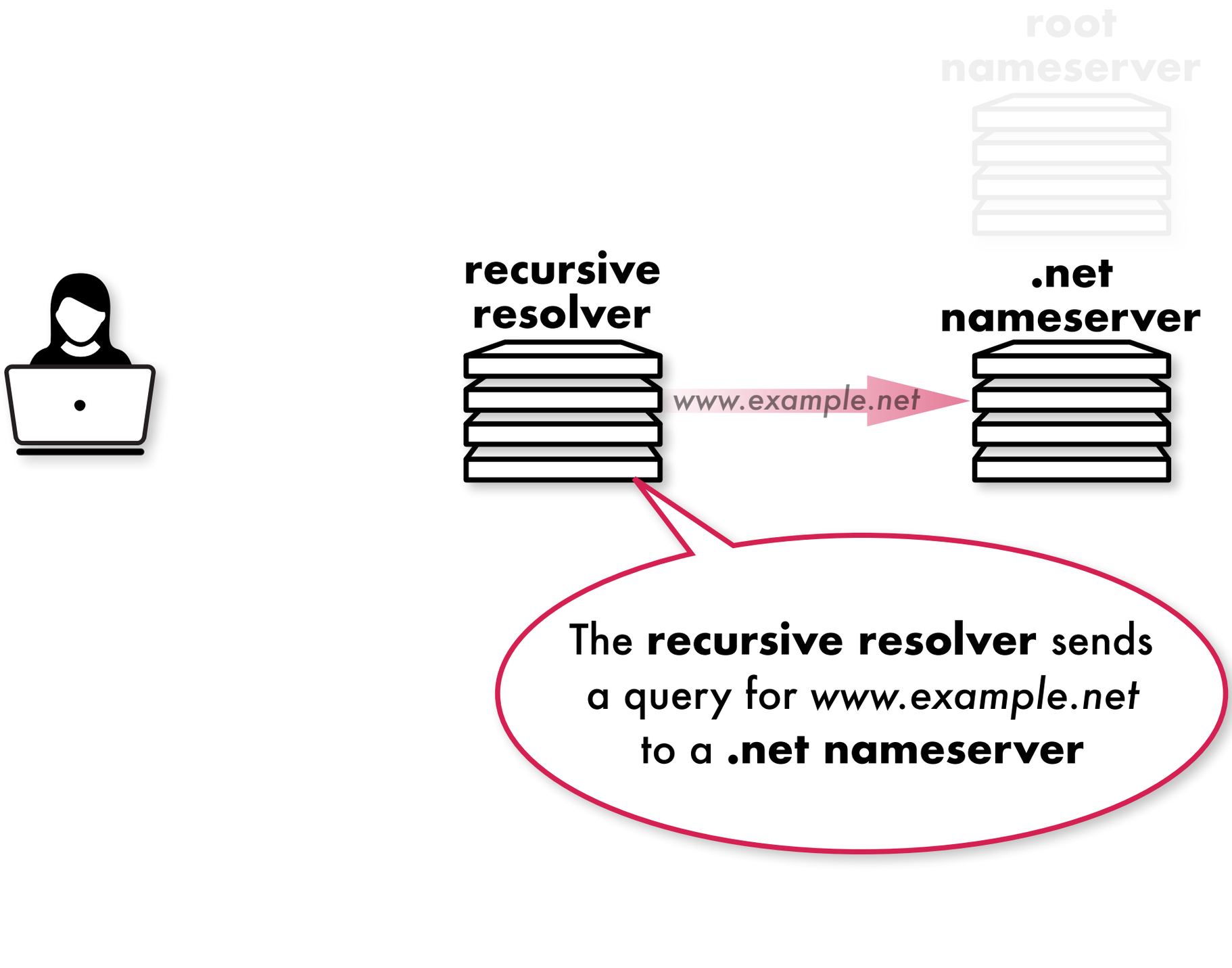
Overview of the Domain Name System



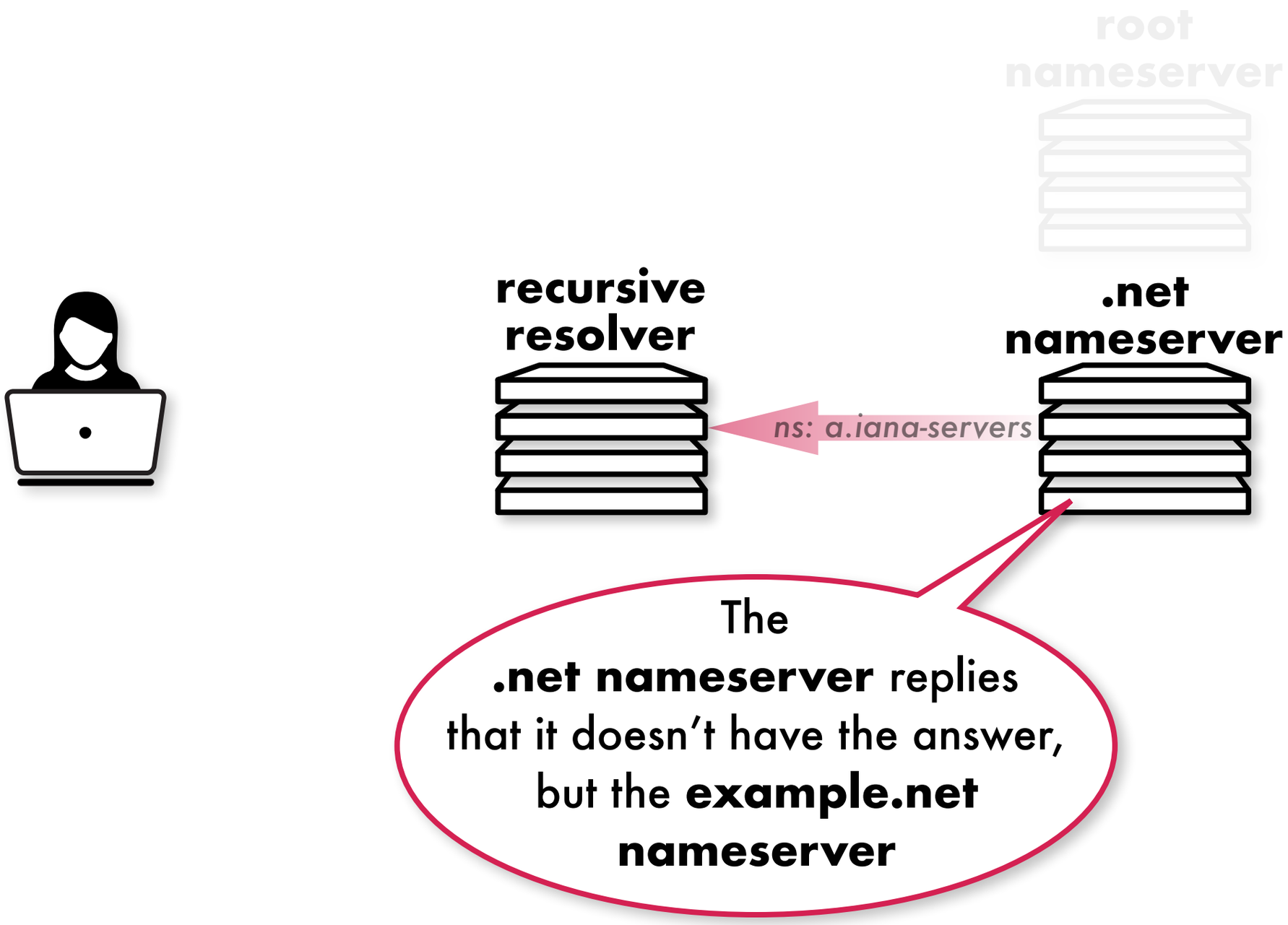
Overview of the Domain Name System



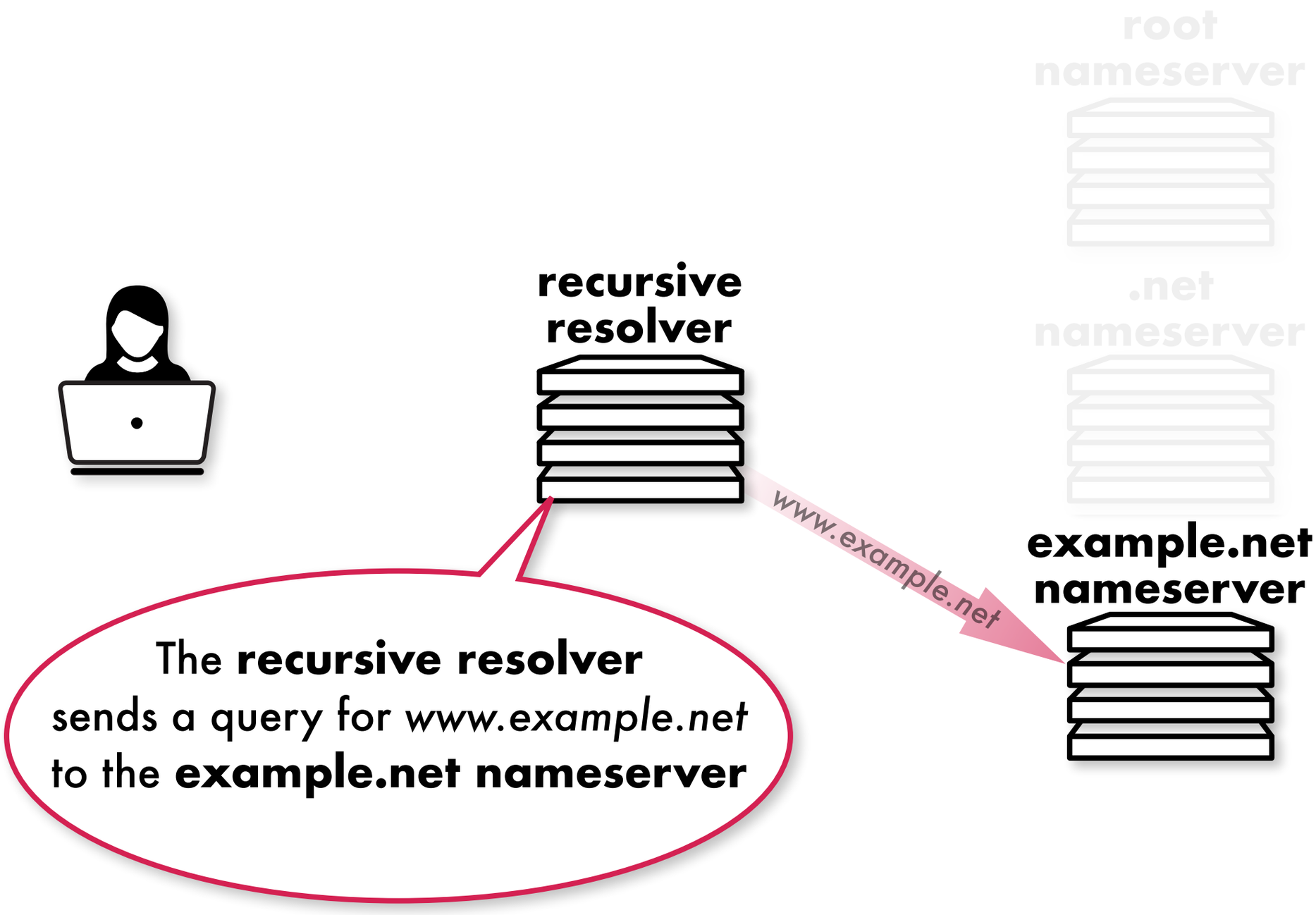
Overview of the Domain Name System



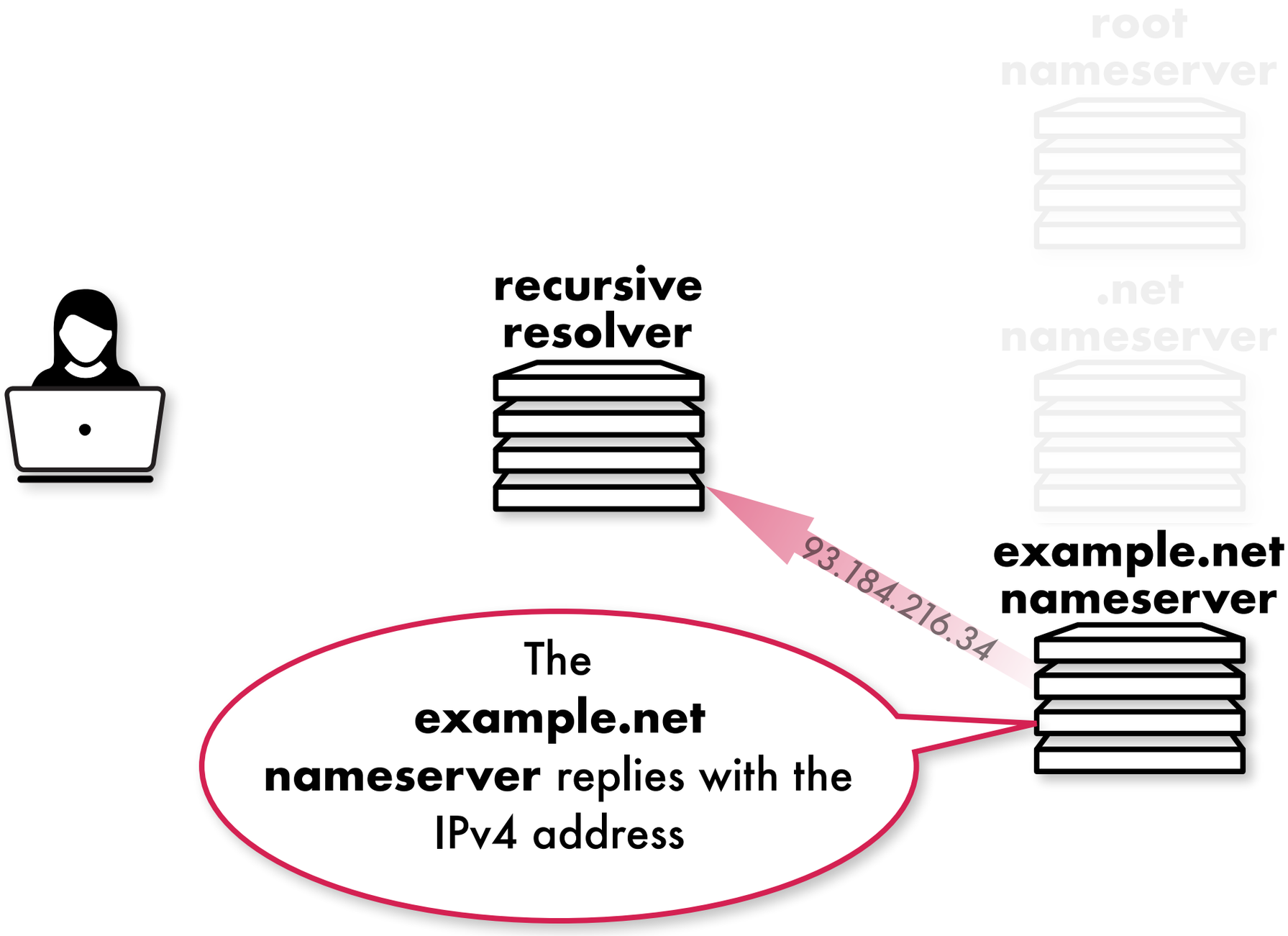
Overview of the Domain Name System



Overview of the Domain Name System

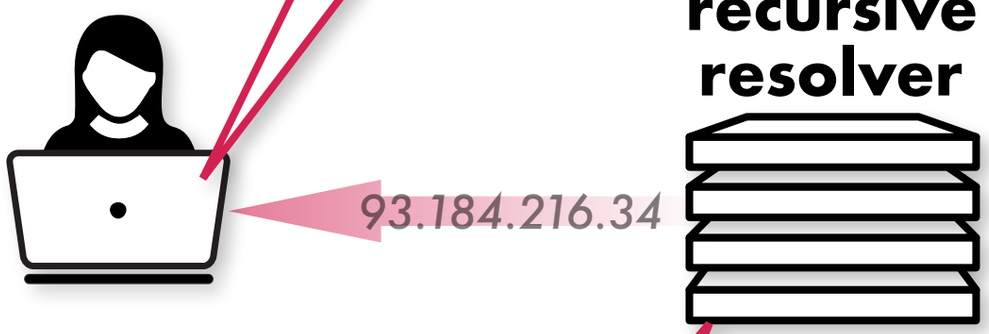


Overview of the Domain Name System



Overview of the Domain Name System

The **user's computer** passes the IPv4 address to the **user's web browser**



The **recursive resolver** replies to the **user's computer** with the IPv4 address 93.184.216.34

Overview of the Domain Name System

So What are the Problems with this System?

So What are the Problems with this System?

The connection between the user and the recursive resolver exposes the IP address of the user, which is considered regulated Personally Identifiable Information (PII) in many jurisdictions.

The domain names that the user's computer is querying for constitute a rich "click trail" of information about the user's browsing history, email, all of the software on their computer that's checking for updates, and all of the malicious software that's infected their machine.

So What are the Problems with this System?

If the recursive resolver is a single machine, or a cluster of machines that share common fate, simple power or network outages can leave large communities of users unable to utilize their Internet connections.

Even when users are already using recursive resolvers that are broadly anycast, the failure of a local node often results in users' queries being backhauled to other continents.

So What are the Problems with this System?

The maximum performance a user can receive is limited by the distance between the user and the recursive resolver: the further away, the slower the user's performance will be.

Also, the further away the recursive resolver is, the more surveillance regimes the user's traffic is likely to be exposed to in transit.

So What are the Problems with this System?

A malicious computer posing as a recursive resolver can provide inauthentic answers, compromising the user's computer or online transactions.

And even a correct recursive resolver can be tricked into providing inauthentic answers to the user.

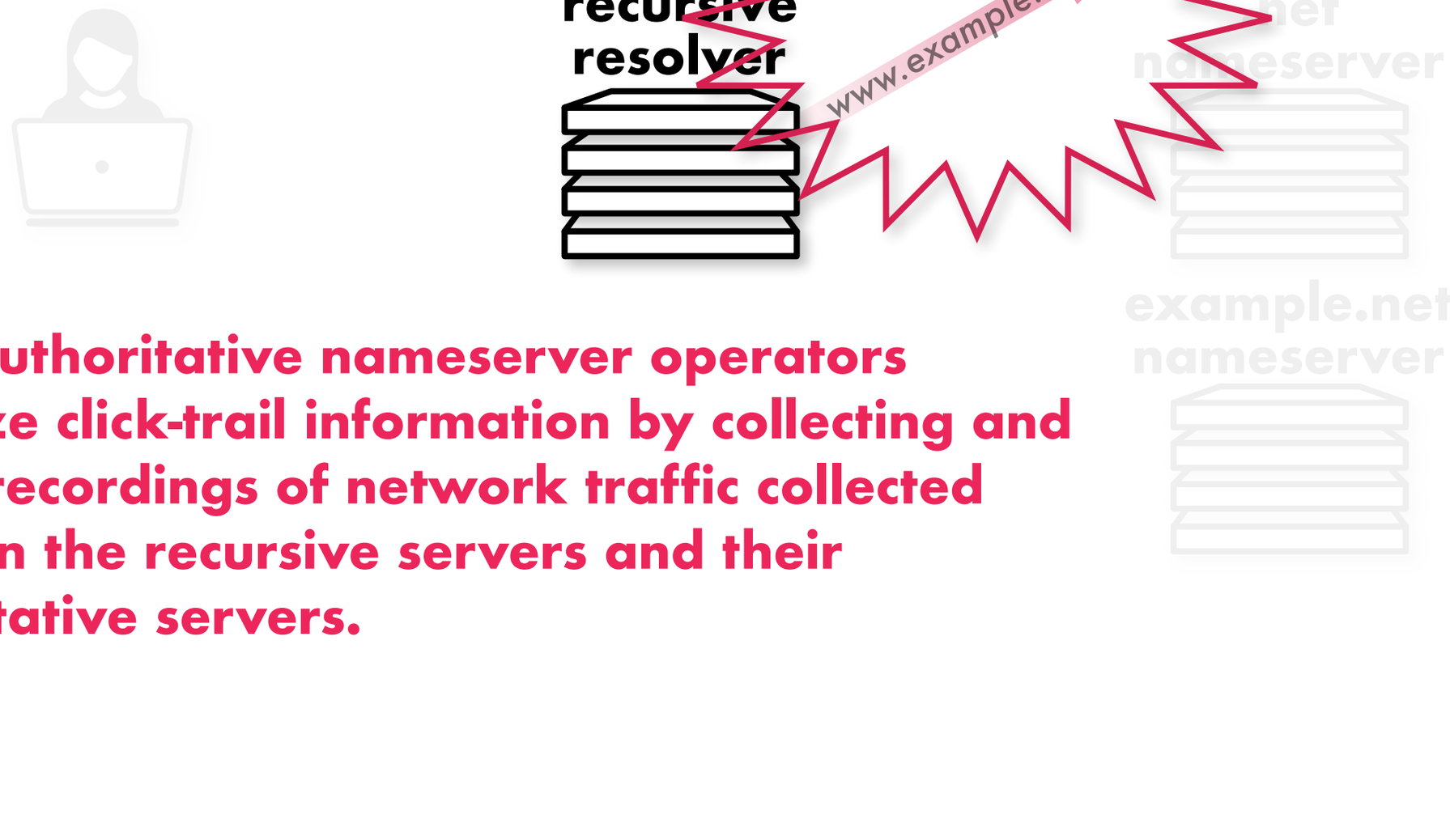
So What are the Problems with this System?

When a recursive resolver has a "cache miss" performance takes another huge hit as the resolver begins querying authoritative servers that are far away and potentially slow to respond.

Many commercial recursive resolver operators intentionally pass user IP address information onward to authoritative server operators.

So What are the Problems with this System?

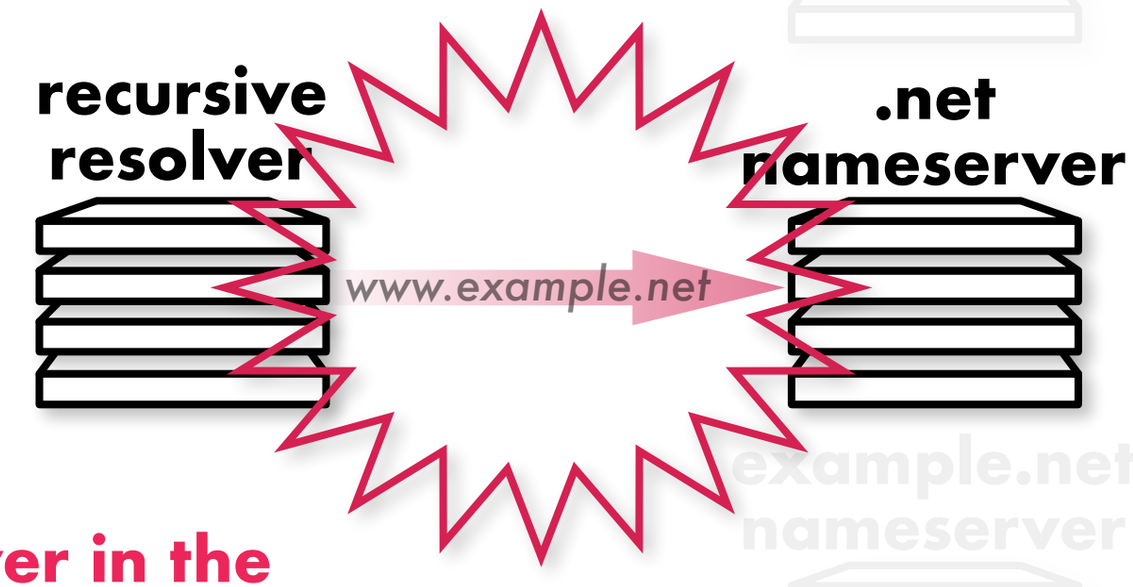
Recursive resolvers leak far more information to authoritative servers than is necessary to answer queries. In this example, a query to a root nameserver need not include the "www.example" portion of the domain name.



Many authoritative nameserver operators monetize click-trail information by collecting and selling recordings of network traffic collected between the recursive servers and their authoritative servers.

So What are the Problems with this System?

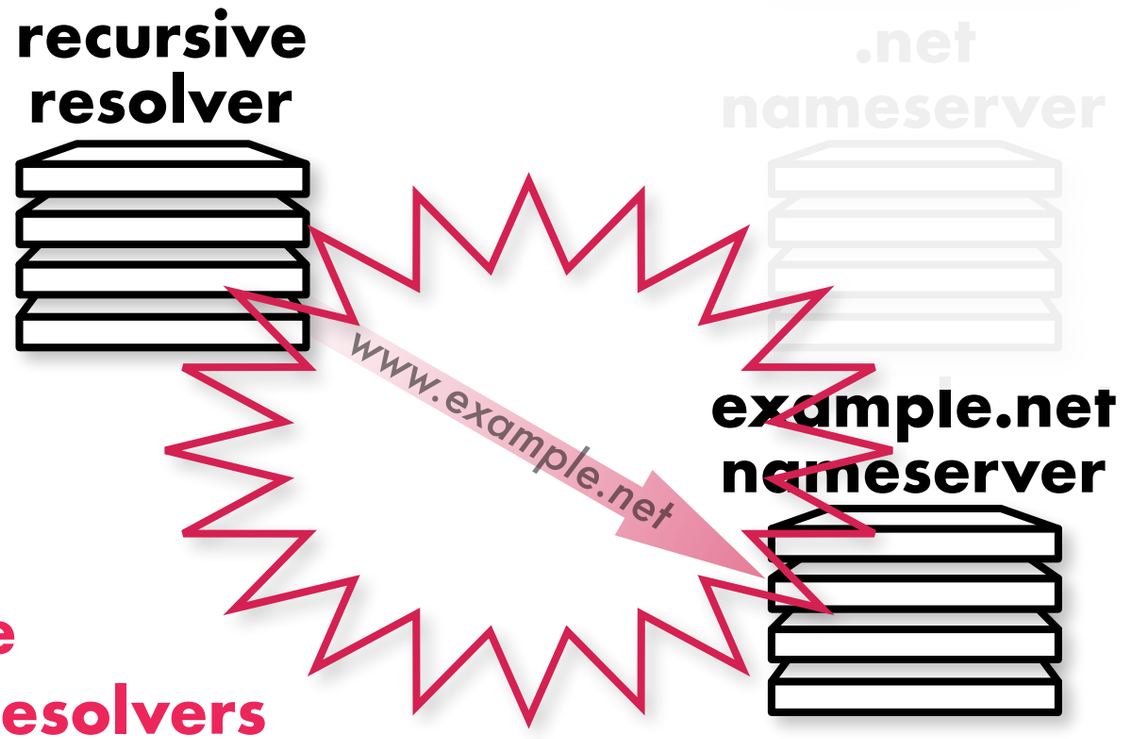
As the recursive resolver continues to query authoritative servers, the performance degrades still further.



Any authoritative nameserver in the recursion chain which fails to provide cryptographic authentication of the DNS data (DNSSEC) precludes the authentication of any domain names further downstream.

So What are the Problems with this System?

Every additional authoritative server in the chain is another potential weak link which could be compromised and caused to provide malicious data to the end user.



Attacks against authoritative servers can leave recursive resolvers unable to obtain answers on users' behalf.

Quad9: Collaboration Between Internet Industry Leaders

IBM

GLOBAL CYBER ALLIANCE

PCH
Packet Clearing House

IBM is providing threat intelligence to protect Quad9 users, the 9.9.9.9 IP address, and funding to ensure the sustainability of the system.

IBM Security is a global provider of security software and services

- 8,000 employees in 130 countries

IBM believes collaborative defense is critical to fight cybercrime

- IBM X-Force Exchange
- IBM Security App Exchange

IBM X-Force world renowned threat research and intelligence

- 40 billion analyzed web pages and images
- 17 million spam and phishing attacks daily
- Over 1 million malicious IP addresses

GLOBAL CYBER ALLIANCE

GCA originated the Quad9 project and is providing funding to ensure the sustainability of the system.

Global Cyber Alliance initiated Quad9 as a way of increasing public trust in the Internet infrastructure and enhancing global cybersecurity by improving Internet users' defense-in-depth.

PCH

Packet Clearing House

PCH provides Quad9's operational infrastructure and funding to ensure the sustainability of the system.

Packet Clearing House sees Quad9 as a logical component of PCH's responsibility for supporting the security and stability of critical Internet infrastructure.

Quad9 derives huge synergies of privacy, performance, and security by being colocated with PCH's global DNS infrastructure and twenty five years of experience operating the largest DNS infrastructure in the world.

Together, IBM, GCA, and PCH Introduce Today:

Quad9

Together, IBM, GCA, and PCH Introduce Today:

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security.

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security. Privacy.

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security. Privacy. Transparency.

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security. Privacy. Transparency. Simplicity.

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security. Privacy. Transparency. Simplicity.

Together, IBM, GCA, and PCH Introduce Today:

9.9.9.9

Global Public Recursive Resolver

Security. Privacy. Transparency. Simplicity.

How Quad9
is addressing
DNS problems

Security

Threat-intelligence feeds from
many security companies allow Quad9
to protect users from malicious connections.

Unlike other recursive resolvers, Quad9's comprehensive
infrastructure allows fewer opportunities for "man in the middle" attacks.

To protect users from fraudulent DNS replies, Quad9 performs DNSSEC
cryptographic validation of DNS answers it receives from other sources.

Quad9 doesn't just protect your desktop and laptop computers and your
mobile devices, it also protects vulnerable "Internet of Things" devices which
can't be protected with anti-virus software and may never receive security patches.

Quad9 uses and contributes improvements back to open-source, publicly-vetted software.

How Quad9 is addressing DNS problems

Privacy

Quad9 doesn't collect or store any Personally Identifiable Information (PII), including IP addresses. We don't have accounts or profiles or ask who you are.

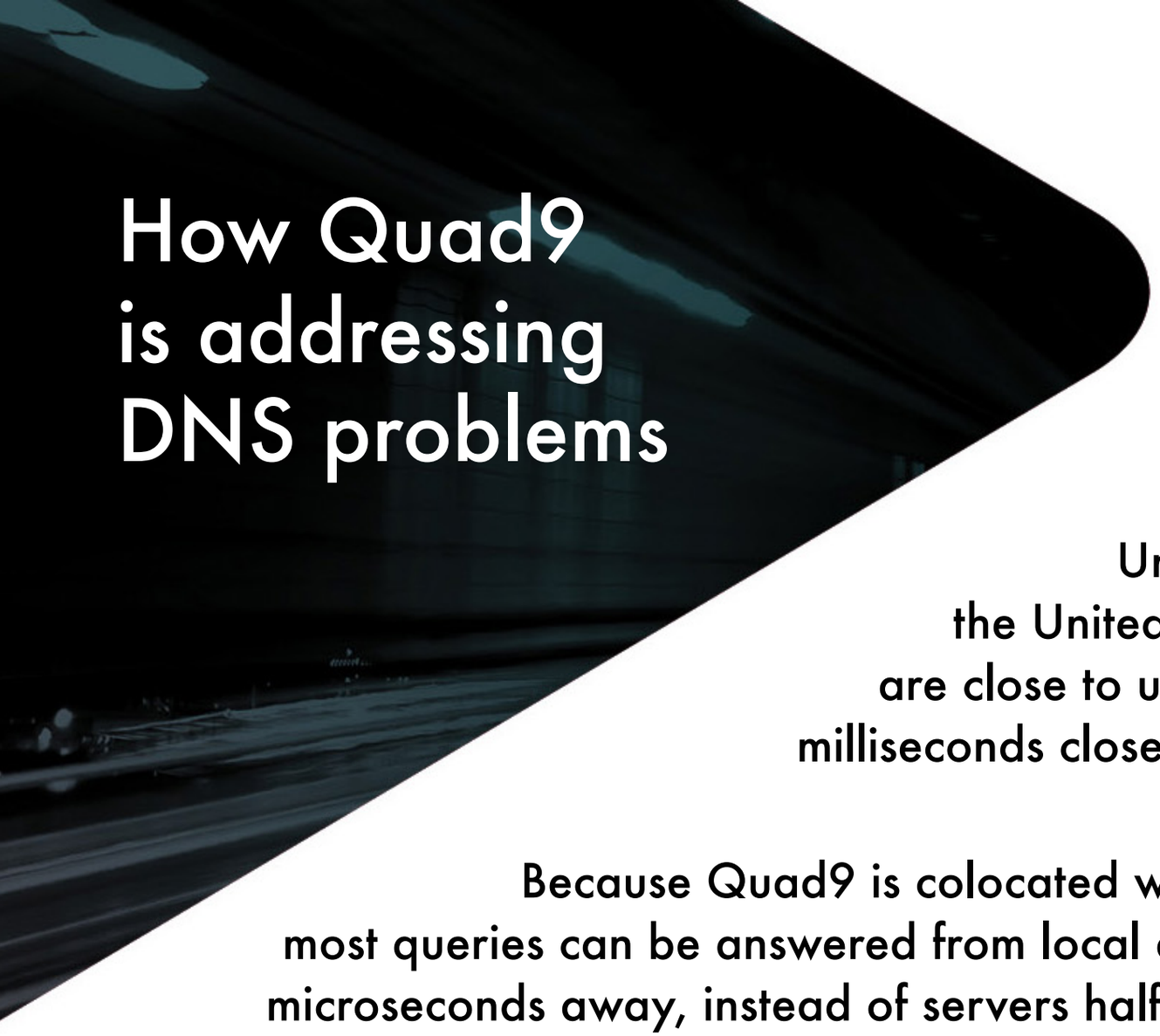
Quad9 supports user-to-server encryption of DNS queries.

Since we don't collect personal information, it can't be sold or stolen.

One of Quad9's key differentiators is that as a transparent, grant-funded public-benefit not-for-profit organization, there is neither room in our model nor a reason to try to profit from our position of trust. PCH has twenty five years of experience and continuous growth operating Internet critical infrastructure under this model.

Because Quad9 shares the PCH DNS infrastructure platform, all root and most TLD queries can be answered locally within the same stack of servers, without passing query onward and making it vulnerable to interception and collection by others.

When Quad9 does have to pass a query onward to a server outside of our control, unlike other recursive resolvers, we use a variety of techniques to ensure that the very minimum necessary information leaves our network and users' privacy is maximized.



How Quad9 is addressing DNS problems

Performance Differentiators

Unlike other recursive resolvers which focus on the United States and Western Europe, Quad9 servers are close to users throughout the world, often hundreds of milliseconds closer to users in Africa, Latin America, and Asia.

Because Quad9 is colocated with PCH's global anycast DNS infrastructure, most queries can be answered from local authoritative servers in the same server stack microseconds away, instead of servers halfway around the world with a thousand times more delay. Quad9 is the only recursive resolver colocated back-to-back with a comprehensive array of root and TLD nameservers.

Unlike other recursive resolvers, Quad9 servers are hosted directly within Internet Exchange Points (IXPs) in all cities. They have direct peering interconnections with thousands of Internet service provider networks globally. This ensures equal access and equal performance for users of all Internet service providers, both large and small. We will not reinforce the position of market-dominant carriers.

How Quad9
is addressing
DNS problems

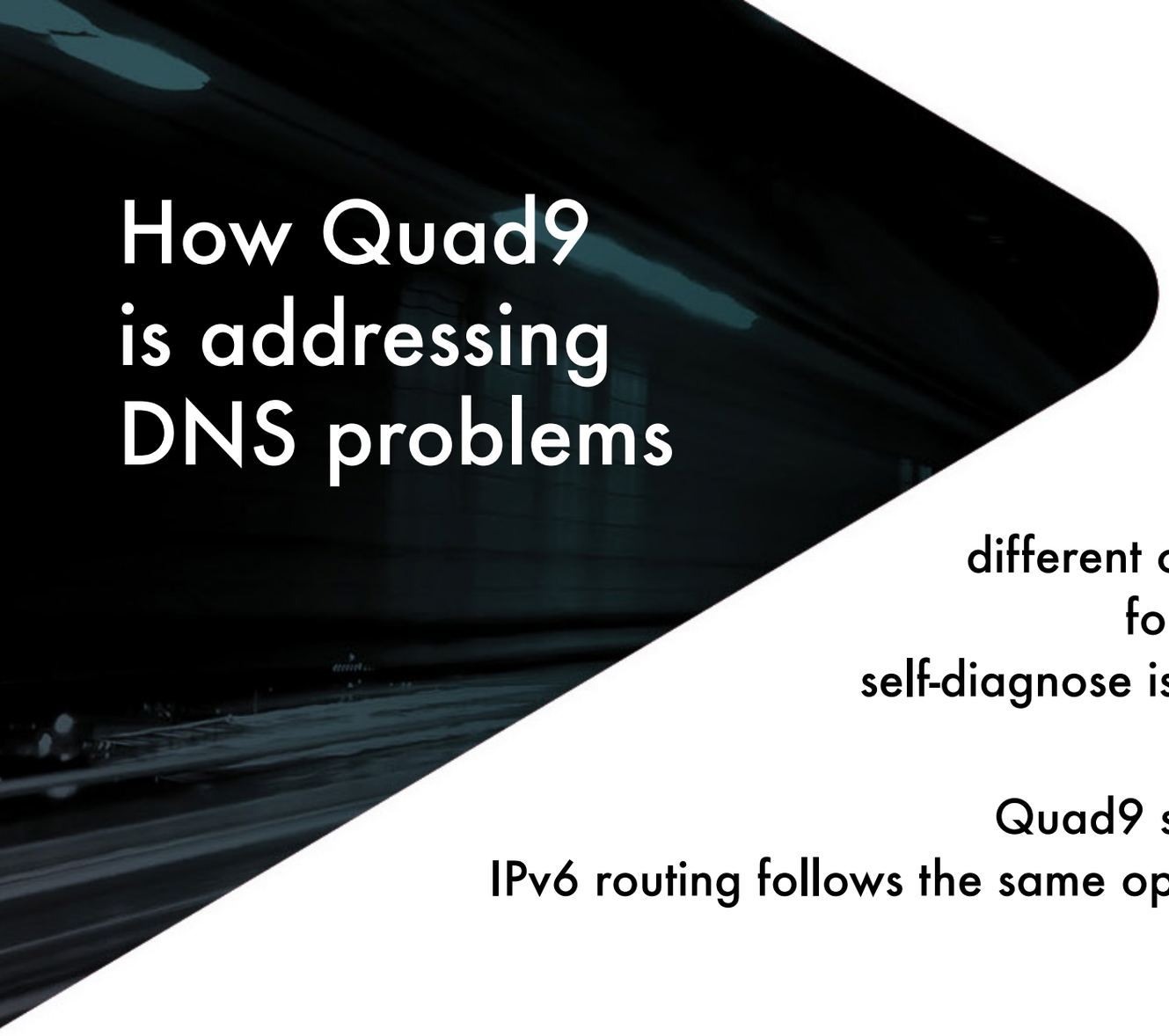
Transparency

Quad9 is the only global recursive resolver that's owned and operated by a not-for-profit organization. The regulatory rules which govern non-profits protect the public interest and ensure transparency of governance and finance.

Quad9 is committed to transparency in policy, as well as technical operations and finance. We have a major effort underway to comprehensively define and publicly document our privacy and law-enforcement-compliance policy.

An effort of this global scale uncovers complex interactions between incompatible legal regimes in the many dozens of countries in which we operate. As a part of our transparency efforts, we're committed to documenting both our compliance efforts and the conflicts between incompatible legal and regulatory regimes that we encounter. We aim to encourage governments to protect users' privacy within their jurisdictions.

Our foremost guiding principle is to protect Internet users from malicious actors, whether the threat be from malware or fraud or the nonconsensual monetization of their privacy.



How Quad9
is addressing
DNS problems

Features

Quad9 provides alternate IP addresses with
different combinations of features, so users can choose
for themselves which protections they want and
self-diagnose issues related to enhanced privacy or security.

Quad9 supports native IPv6 everywhere, all the time.
IPv6 routing follows the same optimum paths as IPv4, it's not an afterthought.

Quad9 provides security, not censorship.
We block connections based on criminal threats to users, not on the nature of content.

Quad9 has a white-listing system to protect users from false-positive
blocking of legitimate connections by threat intelligence providers.

Quad9 is designed not only to defend its users, but also to protect authoritative
DNS servers from DDoS and help domain operators weather attacks.

Feature Selection Matrix

		Malware Blocklist	NXDOMAIN Only	Send EDNS Client Subnet	DNSSEC Validation
Primary	9.9.9.9	●			●
No Features	9.9.9.10			●	
CDN-Friendly	9.9.9.11	●		●	●
IoT-Friendly	9.9.9.12	●	●		●

Today's public introduction marks the culmination of a one year long pilot.

Nearly a million users
and more than one hundred
organizations on six continents
have been using the service
since November of last year.

Today's public introduction marks the culmination of a one year long pilot.

Nearly a million users
and more than one hundred
organizations on six continents
have been using the service
since November of last year.

Today's public introduction marks the culmination of a one year long pilot.

Their stories tell the value of Quad9.

Spectrum Internet
Cardiff, Wales

50,000 Home and
Small Enterprise users

"As an ISP, we're in a unique position to help a wide range of Internet users address cyber-security issues.

That's why we are really excited about bringing Quad9 to our customers.

Quad9's unique transparent, best-practices structure has given us the confidence to provide this additional layer of security to all of our products as a free, opt-in service."

Universidade Eduardo Mondlane
Maputo, Mozambique

30,000 academic users

"As a university, we have to be particularly careful about the technologies that we invest in. We care intimately about cost, performance, security, ease of use, and privacy for our students.

Quad9 was a perfect fit for us, as it easily checked all those boxes with no additional complexity in our workflow. It literally 'just works' in the background, and we rest assured that our users have an additional layer of protection!"

"We're using Quad9 across all of the companies that rely on us for IT support, mostly medium enterprise and manufacturing companies in the American midwest.

Adding secure DNS gives them an additional layer of defense-in-depth protection, and Quad9's privacy policies mean that we don't have to give anything up in exchange."

Enterprise Systems Solutions, Inc.

Loveland, United States

1,000 small and medium-enterprise users

"After we started using Quad9,
we saw a 50% reduction
in anti-virus alerts and a 30% reduction
in the number of hits on our
Intrusion Detection System.

Quad9 is an indispensable part
of our defense-in-depth."

A U.S. State Government

5,000 government users

“Thusa Connect provides IT support to Enterprise and SMMEs in South Africa. Our customers are concerned with security, reliability, and performance.

Before, many of them were using Google’s DNS resolvers, but Quad9 has much better geographic diversity generally, and particularly here in South Africa.

With the added benefits of the great security features and the reliability we’ve experienced, it was an easy decision to switch our customers to Quad9.”

Thusa Connect
Durban, South Africa

7,000 medium enterprise users

Key Facts About Quad9

Not-for-profit, transparent, public-benefit organization

Exclusive focus on public DNS service

Industry-leading experts in DNS and IP content delivery

No collection or monetization of user information

Served from 100 cities on 6 continents today, more soon

Easily-memorable 9.9.9.9 address

Mission: Quad9 exists to improve the security, performance, and privacy of all users of the Internet by delivering free and open DNS recursive resolution