Technical Impacts of DNS Privacy and Security on Network Service Scenarios

ATIS-I-0000079 | April 2020

Abstract

The domain name system (DNS) is a key network function used to resolve domain names (e.g., atis.org) into routable addresses and other data. Most DNS signalling today is sent using protocols that do not support security provisions (e.g., cryptographic confidentiality protection and integrity protection). This may create privacy and security risks for users due to on-path nodes being able to read or modify DNS signalling.

In response to these concerns, particularly for DNS privacy, new protocols have been specified that implement cryptographic DNS security. Support for these protocols is being rapidly introduced in client software (particularly web browsers) and in some DNS servers.

The implementation of DNS security protocols can have a range of positive benefits, but it can also conflict with important network services that are currently widely implemented based on DNS. These services include techniques to mitigate malware and to fulfill legal obligations placed on network operators. This report describes the technical impacts of DNS security protocols in a range of network scenarios. This analysis is used to derive recommendations for deploying DNS security protocols and for further industry collaboration. The aim of these recommendations is to maximize the benefits of DNS security support while reducing problem areas.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address network reliability, 5G, robocall mitigation, smart cities, artificial intelligence-enabled networks, distributed ledger/blockchain technology, cybersecurity, IoT, emergency services, quality of service, billing support, operations and much more. These priorities follow a fast-track development lifecycle from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org. Follow ATIS on Twitter and on LinkedIn.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE: The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

ATIS-I-0000079

Copyright © 2020 by Alliance for Telecommunications Industry Solutions

All rights reserved.

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information, contact ATIS at (202) 628-6380. ATIS is online at http://www.atis.org.

Table of Contents

1 Introduction 1

2 Executive Summary 1

3 Implications and Recommendations 3

4 Current ISP DNS Services and Features 5

5 DNS Protocols 9

6 Scenarios 15

7 Conclusion 31

8 Acronyms and Abbreviations 32

Appendix 1 – Organizational and Customer Communications and Talking Points 33

1 Introduction

The domain name system (DNS) provides an essential function for distributed applications of resolving human-readable names into network routable IP addresses. As such, DNS provides a bridge between the application domain and the network domain. The ubiquitous nature of DNS means it has also become a platform for distributing application-specific information such as domain-based message authentication, reporting and conformance (DMARC) email security policy.

Given the key role that DNS plays in network routing and operation, the network domain has employed DNS in support of local services, network optimization, fulfillment of legal requirements and to enhance the online security of network users.

The dual role of DNS—as an internet-wide database and a network service function—potentially creates tension between application and network interests, with contrasting perspectives in different technical communities. Encrypted DNS protocols such as DNS over HTTPS (DoH) and DNS over Transport Layer Security (TLS) (DoT) are now being rolled out, which brings the different perspectives about the role of DNS into sharp focus. Encrypted DNS protocols can increase user privacy and security, but deployments should consider the public and private network impacts because they may have deleterious impacts on the overall network operation and robustness.

This report will identify some of the most important public and private network scenarios that involve DNS network features and analyze the technical impacts of DNS privacy protocols. The focus will be on the client-to-server (including stub-to-recursive-resolver) interface. Based on this analysis, recommendations for how to deploy and operate DoH and DoT will be generated.

2 Executive Summary

Client operating systems and applications are rapidly introducing support for the encrypted DNS protocols DoT and DoH. These protocols provide integrity protection and confidentiality for DNS requests and responses between the client and the responding DNS server. This can improve user privacy and security in all deployment scenarios. Encrypted DNS protocols are a useful addition to the network security toolkit.

Given the important and diverse role of DNS in network operations and policy enforcement, any changes to DNS behavior in clients should be studied for impacts on the complete networked system. Measures should be taken, if necessary, to maintain the best possible service. In the case of support for DoT and DoH, there are impacts on systems in three main areas:

- The absence of industry norms for how to deploy and operationalize encrypted DNS in servers and clients is leading to the adoption of piecemeal solutions that differ in each implementation. This is creating a confusing situation, which risks a range of service problems or security loopholes due to incompatible assumptions in different implementations. In some cases, this may lead to users finding services or devices that fail to operate. They may also find that there is no single point of contact capable of understanding and resolving service problems due to the complex interactions between the different components.
- Some clients are disregarding DNS server provisioning information received from the network, e.g., in Dynamic Host Configuration Protocol (DHCP), and instead selecting their own DNS servers. These clients can disrupt a range of network services, including security and legally

required services, that are implemented in Internet Service Provider (ISP) and managed private network DNS servers today.

- The support of confidentiality in DoT and DoH may prevent operation of any network services implemented in "middleboxes" that rely on DNS queries and responses being in clear text. This could include implementations of network security features (e.g., malware detection and blocking), as well as the implementation of government and legal requirements in public networks and network policy controls in managed private networks.

The rapid changes to DNS require technical, organizational and educational responses from stakeholders. To help understand the impacts of encrypted DNS protocols and to recommend options, we have described and analyzed a number of key scenarios that represent typical network deployments and user experiences. Based on this analysis, we have made specific recommendations for different stakeholder groups that are described in section 3.

A key issue is that, for most end users, DNS is a service that should "just work." They do not wish to configure DNS services in devices or networks. Therefore, many users will rely on the automatic configuration of systems and guided user interface choices to set their DNS configurations. This makes it difficult for systems to adequately account for differences in user requirements and scenarios. Different assumptions about what is in the "best interests" of the user is one cause of the piecemeal approach to encrypted DNS deployment. Users should be provided with clear and honest advice about the implications of any changes made in devices, products or services.

In many of the scenarios we have studied, the ATIS identified and defined concept of a "same-provider" DNS protocol upgrade, discussed in section 5.6.1, is consistent with the principle of "least surprise" for users. Several leading client implementations are already adopting this approach, which could be a good basis for further developments.

A feature common to several scenarios (e.g., home/residential, enterprise and public Wi-Fi) is the use of private IP addresses on the Local Area Network (LAN) and the use of local DNS servers that are accessed by a private IP address. We believe that deploying DoT and DoH in this situation is difficult due to the lack of agreed approaches to certificate handling and same-provider protocol upgrade. More collaboration between stakeholders is required to generate good deployment options for DoT and DoH in networks with this type of IP addressing.

Currently, both clients and servers are taking their own piecemeal approaches to how the deploy DoT and DoH and select the DNS server to use. We recommend that all stakeholders move rapidly to provide better guidance on best practices for DoT and DoH deployment and server selection to reduce complexity and improve the user experience. This should consider the different use cases and network scenarios found in the industry and recognize the full extent of variety in the social, legal and technical context in which networks are used. At a minimum, solutions should be developed that work effectively in the scenarios described in this document. As an industry, we should deliver DoT and DoH in ways that enhance user experience and service quality.

3 Implications and Recommendations

3.1 Implications and Recommendations for End Users in Home Networks

Deployment of encrypted DNS protocols in clients and networks currently is piecemeal and uncoordinated. This situation risks having users find unexpected and hard-to-comprehend changes to their network experience. In the worst case, users may find services or devices stop functioning because of DNS configuration problems. With different actors introducing encrypted DNS in different ways, users that experience problems will lack a clear point of contact to help them in debugging and resolving issues.

Some users, by their own actions, or by using services provided by their ISP, use DNS to apply security and content policies within their home network. Users should be aware that introducing DoT or DoH may disrupt these services.

Appendix 1 contains some guidance for ISPs about how to structure user communication and support.

3.2 Implications and Recommendations for Wireline ISPs

We recommend that ISPs understand the impact of DoT and DoH on their systems, prepare strategies to cover their introduction in clients and consider the advantages of supporting DoT and DoH on their infrastructure. This includes gaining an understanding of the current practices in DNS clients and how these may impact ISP networks. Appendix 1 contains some guidance for ISPs about how to develop a strategy.

Where clients have implemented a same-provider DNS protocol upgrade strategy, ISPs that offer DoT or DoH support should work with individual client vendors to enroll their systems to make a same-provider upgrade to their DoT or DoH services available.

3.3 Implications and Recommendations for Client Devices (Operating Systems and Applications)

Support for DoT and DoH in clients can offer users security advantages, but also risks disruption to internet services. In the absence of industry norms, we recognized that clients have had to take a piecemeal approach to introducing DoT and DoH. We recommend that clients develop their approach considering the scenarios and use cases described in this document and in collaboration with network providers and other stakeholders. The same-provider DNS protocol upgrade strategy has considerable advantages in most of the scenarios we have discussed and seems to be more compatible with the principle of least surprise for users.

Where clients request user input to perform DNS configuration, we recommend that the information communicated is helpful, fair and technically accurate.

We recommend that clients recognize that DNS-based policy controls can be valuable to users in home networks and privately managed networks (e.g., enterprise networks). We recommend that these policy controls are honored by clients when introducing DoT and DoH support.

3.4 Implications and Recommendations for Enterprises and Other Managed Private Networks

Managed private networks may use DNS for a range of purposes, including policy enforcement, malware detection and management, and split-horizon naming. Private networks should form a strategy about

how to support these services when clients use DoT or DoH. This may include the use of endpoint management to apply proprietary configurations to DoT and DoH clients.

Development of industry standards for DNS discovery and best practices that meet enterprise and other managed private network requirements would simplify the secure management of enterprise networks.

Managed private networks may have a requirement to disable DNS queries from clients that do not support the necessary management features and do not honor the network's indicated DNS provider. This may require the development and filtering of solutions for unauthorized DoT and DoH clients within the enterprise network.

3.5 Implications and Recommendations for Governments, Regulators and Law Enforcement

Nations use DNS as a mechanism to support law enforcement information gathering and content filtering according to local regulations. In many countries, the implementation burden of these requirements is focused on ISPs that operate in the governed territory.

The introduction of DoT and DoH has the potential to disrupt DNS-based policy and information-gathering mechanisms. It may also reduce the visibility and control available to ISPs because more DNS traffic will be routed directly to public DNS providers. Governments, regulators and law enforcement should evaluate the changing environment and consider technical and legal responses. For DNS-based mechanisms, these could include:

- Extension of legal requirements to DNS providers other than national ISPs.
- Establishing voluntary agreements with DNS client developers and public DNS providers.

Increased use of encrypted DNS and changes to the client routing of DNS queries might mean that DNS-based mechanisms are insufficient to meet national requirements. If so, then other technical options beyond DNS may need to be fully investigated.

3.6 Implications and Recommendations for Public DNS Services

Public DNS servers that support DoT or DoH are likely to experience an increase in traffic due to direct routing of DNS queries by DoT or DoH clients that do not implement a same-provider strategy.

The increasing use of public DNS services will likely bring more focus on questions about public DNS provider policies for enforcing legal requirements and their general role in internet security issues. Where public providers offer international services, these could include questions of legal jurisdiction when the client and server are in different regulatory regimes. We recommend that public DNS services monitor evolving regulations and legal requirements.

Increasing use of public DNS will centralize DNS traffic, meaning public DNS providers will become critical to internet reliability. We recommend that public DNS providers pay close attention to system robustness.

Some managed private networks may filter DoT or DoH traffic using an algorithm based on server IP address and IP port (see section 6.2.1). To avoid having this filtering cause unintended disruption to services other than DoT and DoH, we recommend that public DNS providers do not combine DoT and DoH with other unrelated services on the same IP address and IP port.

4 Current ISP DNS Services and Features

Currently, for many users, their ISP is the default provider of DNS resolution services in most scenarios (see scenarios in section 6). Many ISPs, particularly large ones, run their own DNS recursive resolvers. Some, typically smaller, ISPs may rely on DNS services from external providers.

The diversity of ISPs naturally creates a distributed DNS infrastructure where different access services use different infrastructure for DNS resolution. This diversity helps provide security and robustness for the internet as a whole.

ISPs use DNS for important applications including:

- Diagnosis and resolution of user internet connectivity problems
- Network management
- Network performance optimization
- Support for online safety of users
- Fulfillment of national legal obligations

The following table shows examples of DNS features and services that may be implemented using DNS.

Feature or Service	**Description**	**Level of Adoption**	**Comments**
Customer Care	The ISP is normally the first point of contact for users experiencing Internet connectivity issues. ISPs managing DNS helps them act as a single point of contact to fix issues and provides tools that can be used for issue diagnosis and resolution.	High	ISPs will not be able to fix internet access problems caused by external DNS resolvers.
Malware Detection	Traffic analysis of DNS can reveal emerging or spreading malware and be used to inform actions by the ISP and endpoint malware protection products.	Widely used and high importance.	
Malware Command and Control (C2) Blocking	DNS to known malware C2 endpoints is blocked by ISPs	Widely used and high importance.	

Feature or Service	Description	Level of Adoption	Comments
Parental Control	Block (e.g., return NXDOMAIN) or redirect specific hosts according to local rules/policies.	Offered by some ISPs.	Feature with user opt-in or opt-out.
Legal Requests	Block (e.g., return NXDOMAIN) or redirect specific hosts according to local rules/policies.	Widely used for a variety of legal requirements (e.g., to block illegal gambling sites, child pornography).	Requirements vary in different countries/regions. Internet Engineering Task Force (IETF) discussions suggest improving response information to offer more details about why requests are blocked. So far, the issue of legal requests for DNS blocks has been mostly directed to ISPs. However, if other DNS services (e.g., quad-X) become prominent, they may also be ordered to comply.
Global Server Load Balancing	Direct to specific address in content delivery networks (CDNs) based on user location.	Widely used and high importance.	
NXDOMAIN Redirection	Serves alternative destination or search page for domains that are not registered.	Offered by some ISPs.	May be a feature with user opt-in or opt-out capability.

Feature or Service	Description	Level of Adoption	Comments
Network Management Example 1 Management of server request floods	Handle server request floods by manipulating DNS responses to statistically gap traffic.	DNS is widely used by ISPs for network management. This example gives one application.	Important capability for at least one operator to address problems with customer premises equipment (CPE).
Network Management Example 2 Resolving problems with CPE implementations	Detect and work around incorrect use of DNS names by CPE devices.	DNS is widely used by ISPs for network management. This example gives one application.	For example, a CPE bug in the embedded DNS resolver cache caused incorrect cache hits for substantially similar domains or a query for example.com.uk would return the answer for example.com.br from the CPE cache. This was a remnant of browser prefetching. While troubleshooting real time with the customer, the ISP was able to watch the order in which the browser was sending queries to the ISP's resolver. More importantly, after the initial browser-initiated queries, we were able to see which queries were not being sent when the customer clicked on embedded links. This pointed us to cache hits on the CPE, which eventually led us to find the CPE resolver bug.

4.1 DNS Features

4.1.1 DNS64

DNS64 is a mechanism that allows end devices that support only IPv6 to reach services on devices that are accessible only by using IPv4. Figure 4.1 illustrates the operation of DNS64.

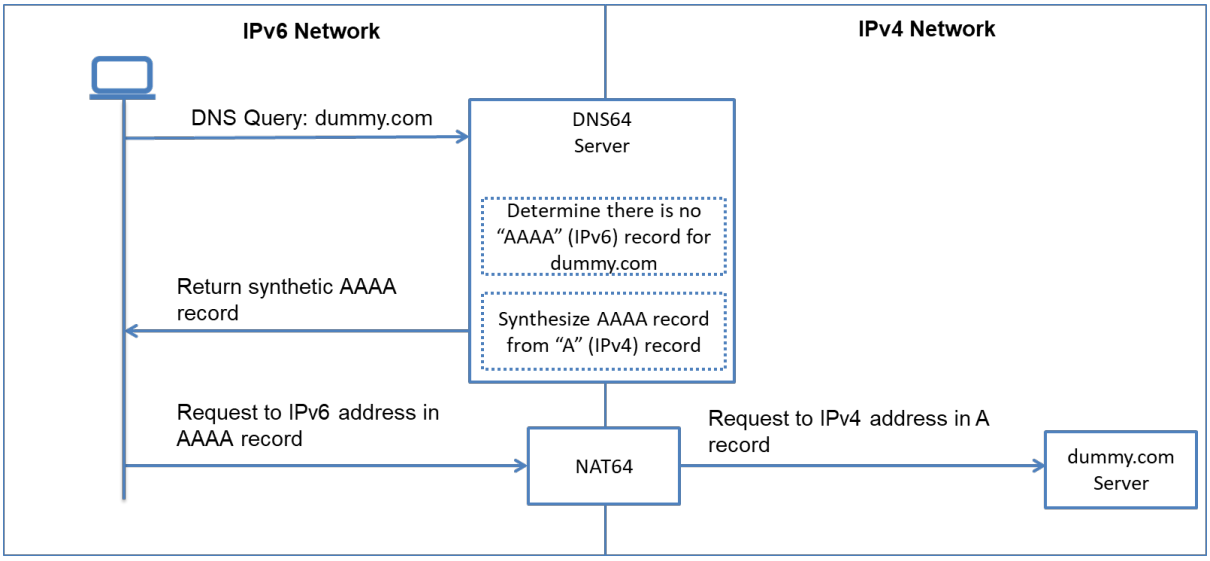

Figure 4.1 Overview of NAT64 Operation

When an IPv6 device attempts to reach a server that is accessible only over IPv4, the DNS64 server detects the lack of a DNS AAAA (IPv6 address) record. This DNS64 server creates a synthesized AAAA record based on the A record and sends this to the end device.

When the end device communicates to the IPv6 address, a NAT64 will map the address to the corresponding IPv4 address of the desired server. For the mapping to be successful, the DNS64 server and the NAT64 must use coordinated prefixes to map the external IPv4 address space into IPv6.

Because NAT64 requires coordinated provisioning with the Network Address Translation (NAT) server of the local network, this mechanism works only if the correct local DNS64 server is used. End devices or end device applications that change the DNS service (e.g., using DoH) to a DNS server other than the local server will not be able to access DNS64 services.

4.1.2 DNS for Storage of Metadata (e.g., DNS-AS)

Within private managed networks, DNS may be used as a database for storing metadata about hosts or services. An example of this is DNS-AS (https://www.dns-as.org), which "leverages DNS as an authoritative source to publish metadata as a key for common policy across networks" in the context of enterprise networks and data centers.

If systems rely on DNS metadata that is present only in a local instance of DNS (as opposed to the global DNS), then end devices or end device applications that change the DNS service (e.g., using DoH) to a DNS server other than the local server will not be able to access DNS metadata.

4.1.3 ISP DNS Privacy

One aspect of privacy is the encryption of information in protocols to prevent eavesdropping by on-path devices. Some ISPs support encrypted DNS protocols, while others do not. DNS traffic between a user and the ISP's DNS servers is routed only within the ISP's network rather than over the open Internet. Even so, it may traverse unsecure links (e.g., open Wi-Fi), so it could be vulnerable to eavesdropping and modification. Therefore, the use of encrypted DNS protocols can help improve user privacy and security.

Another aspect of privacy is the policies applied by endpoints (end devices and servers). ISPs will handle DNS data in accordance with the laws of their local geography and the contractual relationship with their users. This means that users are able to know where and how data will be handled. ISPs serve well-defined geographic areas and locate their DNS servers within their geography. This means that ISPs are able to handle user DNS resolution without creating issues of data sovereignty by not exporting data over national boundaries.

5 DNS Protocols

This section describes and compares the main DNS protocols used between end devices and DNS servers. The protocols considered are conventional, unencrypted, DNS, which we refer to as DNS53, DNS over HTTPS (DoH), DNS over TLS (DoT) and Domain Name System Security Extensions (DNSSEC).

The advantage of DNS protocols that use encryption such as DoH and DoT is that they offer users protection against malicious monitoring or modification of DNS from on-path attackers that can see DNS signalling. But at the same time, they can also disrupt benign or legally mandated network DNS features if these features are implemented using middlebox implementations. Encrypted DNS protocols may also be used to bypass the DNS infrastructure of the local network that provides services to the user. This creates a tension where solutions that are good for one scenario or threat model can be bad for another.

Note that DNS protocol encryption on its own does not offer protection against all threats. For example, only one interface (typically from the client to the first server) may be encrypted. The protocol security also does not protect against malicious activity by endpoints (DNS servers or clients). Increasing the security of DNS may lead to increased pressure from national authorities for "back doors" on endpoints as an alternative way to provide policy enforcement.

5.1 DNS53

The original, unencrypted, DNS protocol is defined in RFC1035 and is in widespread use today. Until recently, most clients and DNS servers used DNS53 only. DNS53 data is transported unencrypted and without integrity protection as UDP data on port 53. As such, it can be easily monitored, blocked or modified by middleboxes.

DNS allows many different fields to be retrieved based on the DNS name, but the initial, and still most important, application is to resolve DNS names to IP addresses. The examples in this section show this use of DNS.

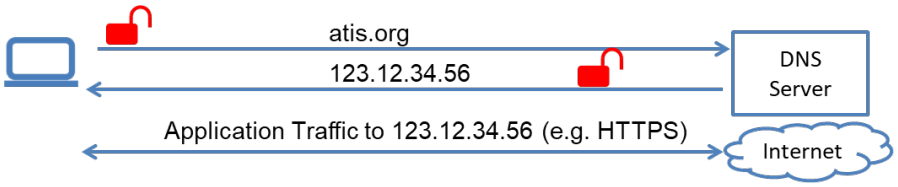

Figure 5.1 DNS53 Address Query – Simplified Example

5.2 DNSSEC

DNSSEC goes back as far as 2005 and is defined in RFC 4033, RFC 4034, RFC 2035 and other documents. The goal of DNSSEC is to provide assurance about the integrity and authenticity of DNS responses according to the domain's authoritative owner.

DNSSEC does not to provide any confidentiality protection. If confidentiality protection is required, then DNSSEC may be combined with DoT or DoH. Note that although DoT and DoH protect the integrity and confidentiality of DNS data between the end device and the first DNS server, they do not guarantee that the DNS record returned by the server is authentic. Hence the need to combine DNSSEC with DoT or DOH to ensure authenticity of data.

DNSSEC allows domain owners to sign the contents of DNS records. The client receiving a DNSSEC signed record (or a proxy acting on its behalf) can verify the record is correct by verifying the signature based on known credentials, which may be obtained using a trust anchor and authentication chain.

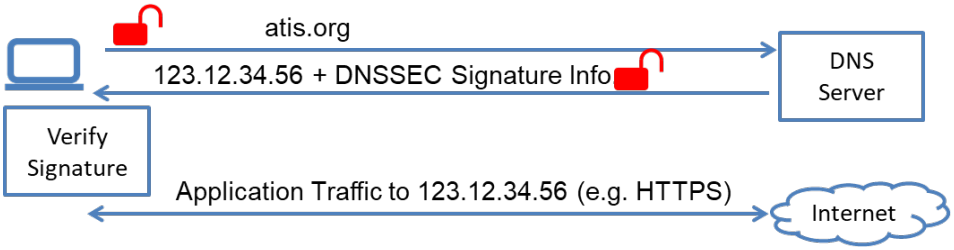

Figure 5.2 Address Query with DNSSEC and DNS53 – Simplified Example

5.3 DNS over TLS

DoT is defined in RFC7858. DoT uses TLS to add hop-by-hop cryptographic protection to DNS. According to RFC7858, DoT uses TCP on port 853. DoT has the usual security features of a TLS protocol:

- Certificate-based identity authentication of the DNS server.
- Confidentiality and integrity protection of the message contents.

The ability of middleboxes to monitor DoT will depend on the version of TLS being used and on the certificate handling policy. However, the use of the unique 853 port makes it possible for middleboxes to be aware of DoT traffic even if they are not able to see the message contents.

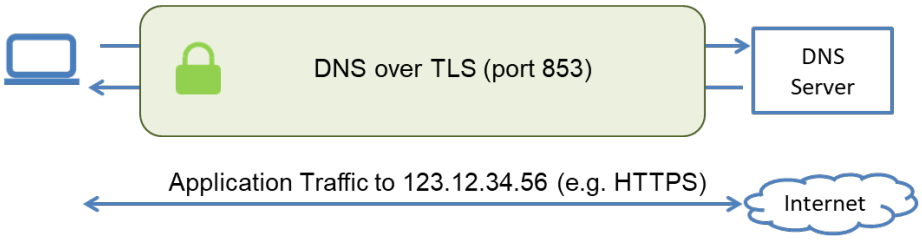

Figure 5.3 Address Query with DNS over TLS – Simplified Example

Note that it is technically easy to adapt DoT to use ports other than 853. This may be done in some implementations to bypass blocks on port 853 traffic.

5.4 DNS Over HTTPS

DoH is defined in RFC8484. DoH encapsulates DNS in HTTPS. This provides security features similar to those available in DoT. Crucially, RFC8484 defines DoH to use port number 443, which is the same port as other HTTPS traffic.

The use of port 443 means that port number cannot be used to distinguish DoH from other HTTPS traffic. Therefore, networks that wish to block DoH using a port number and IP-address-based filter will also have to block all HTTPS traffic to the same destination.

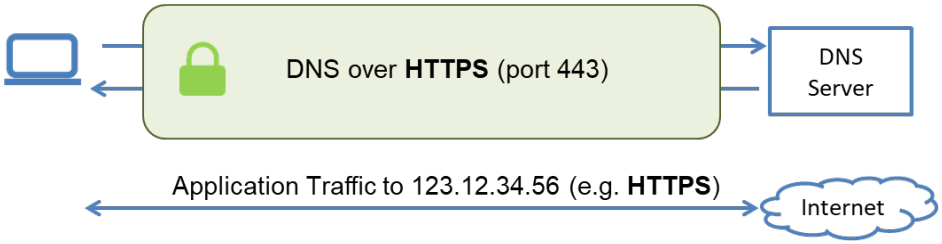

Figure 5.4 Address Query with DNS over HTTPS – Simplified Example

DoH offers a platform to allow DNS to leverage the ongoing evolution of the HTTP protocol family, including HTTP version 3 and QUIC.

5.5 Security Comparison of DNS53, DoT and DoH

The following table compares DNS53, DoT and DoH in terms of their features from a network security point of view.

Feature	DNSSEC (1)	DNS53	DoT	DoH
Wide Protocol Support	Growing	Excellent	Growing	Growing
Standard Port Number	53	53	853	442
Validation of authenticity and integrity of DNS Response compared to authoritative DNS record	Good	None	None	None

Feature	DNSSEC (1)	DNS53	DoT	DoH
Validation of integrity of data between the end device and the responding server	Good (by end-to-end validation of response authenticity)	None	Good	Good
Validation of identity of responding DNS server	None	None	Good	Good
Confidentiality protection against middlebox inspection of DNS traffic	None	None	Good	Good
Supports network monitoring of DNS queries	Yes	Yes	No	No
Tools for network inspection of DNS	Yes	Yes	No	No
Ability to bypass local DNS services without network detection	Low	Low	Medium	High
Risk of leverage by adversaries	Low	High, but can be counteracted by network filters.	High, but can be counteracted by network filters.	High and hard to counteract with network filters. (2)
Ability to bypass totalitarian network censorship	Low	Low	Limited	Good (2)

(1) DNSSEC used without other security protocols

(2) Filtering for DoH in the context of managed networks is discussed in section 6.2.1 dealing with enterprise use cases.

5.6 Discovery of DoT and DoH Resolvers and Client Configuration

As discussed in the scenarios section, many clients currently use a process of DNS resolver discovery (e.g., using DHCP) to configure their DNS resolver. This will configure a resolver that is suitable for their network context. But three issues may arise with the discovery process:

- DNS discovery protocols, especially DHCP, are not secure and may be exploited by malware to direct clients to malicious resolvers.
- Users may be unaware of the policy of the discovered resolvers and therefore may not receive the service they desire.

- There are currently no standardized solutions to discover resolvers that support protocols that offer DNS encryption such as DoT and DoH.

In order to address these issues, clients that support DoT and DoH are implementing proprietary solutions for resolver discovery and client configuration. There are several alternative implementations, but broadly there are two groups:

- Clients that implement a same-provider policy (i.e., they upgrade to DoT or DoH if available, but keep the same DNS provider as would be found using the normal discovery process).
- Clients that do not implement a same-provider policy and instead change the DNS provider from that which would be found using the normal discovery process.

5.6.1 Same-Provider DoT and DoH Clients

The goal of these clients is to retain the same DNS provider as would be found using the normal discovery process, but to opportunistically upgrade from Do53 to DoT or DoH where the provider supports these protocols. Note that the same-provider behavior applies only when the client is doing automatic DNS discovery. Most clients can also be manually configured with a DNS provider, in which case any DNS provider may be configured, and the automatic discovery process is not used.

The same-provider upgrade relies on the client maintaining a list of equivalent Do53 and DoT or DoH servers. This list may use the public IP addresses to identify the servers. When a Do53 server is discovered (e.g., using DHCP), the client will refer to its list and see if there is an equivalent DoT or DoH server listed. If so, the client will direct DNS queries to the DoT or DoH equivalent rather than to the Do53 server, a process that figure 5.6 illustrates. Same-provider upgrades may also check other policies as part of their decision-making progress (e.g., proprietary enterprise configuration policies).

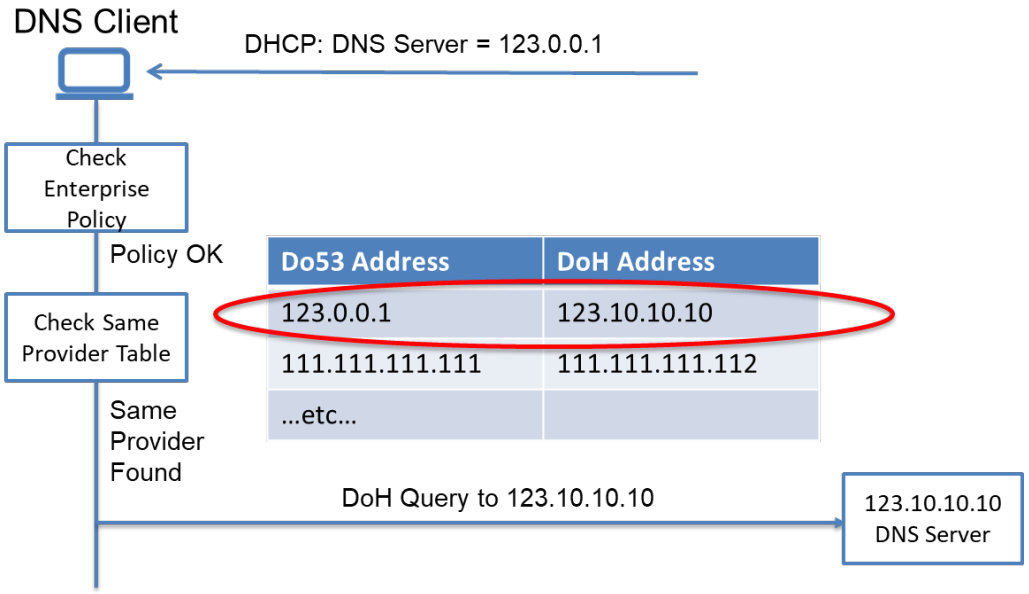

Figure 5.5 Simple Example of a Same-Provider DNS Client Upgrade Behavior

The same-provider upgrade requires the client to have access to managed data about equivalent DNS providers. Early DoT and DoH clients have this table embedded in their software and managed by the client vendor. Each client vendor has its own mechanism for building the table and deciding its contents.

For example, to be included in the table, it may be required that the DNS provider applies to the client vendor for inclusion and provides information such as:

- Proof of ownership of the Do53 and DoT services to be added.
- Information about the policy of the DNS servers in order to demonstrate compliance with rules that may be set by the client vendor for inclusion on its managed table.

Managing upgrade information in this way may be burdensome and administratively complex for both client vendors and DNS providers.

An important limitation of the same-provider upgrade strategy described above is its reliance on public IP addresses. If the discovered DNS server uses a private IP address (e.g., it is on the home gateway in a residential network, as discussed below), then this type of upgrade cannot be used.

The same-provider upgrade behavior offers the important advantage of offering encrypted DNS protocols while retaining the existing DNS service provider and, by extension, the features and policies that the provider offers. As such, an automatic upgrade to the same-provider is compatible with the principle of least surprise for users. Same-provider upgrades also maintain the current distributed nature of DNS.

However, these benefits come with a cost in terms of client complexity and a burdensome administrative process. It is unproven whether this approach is feasible to manage and maintain if a very large number of existing DNS providers decide to offer DoT or DoH.

5.6.2 DoH and DoT Clients with Change of Provider

Clients that change the DNS provider in order to use a known DoT or DoH provider will usually not use an automatic mechanism to discover local DNS servers. Instead they will be configured to use one or more DoT or DoH servers that are globally accessible. These could be, for example, a well-known quad-X DNS service.

In order to prevent changes to DNS service provider in inappropriate contexts, the client may have special policies that cause them to fall back to a discovered Do53 service rather than use a DoT or DoH service. Examples of these policies may be:

- Proprietary configuration policies for enterprise clients.
- Use of a “canary domain.”

A “canary domain” is a special domain that can be used, for example, to indicate that the network is doing special filtering based on DNS (e.g., within a school’s network). If a Do53 query to the canary domain using the discovered resolver returns a negative result (e.g., no A or AAAA record), then the client will assume that DNS filtering policies are being applied. Canary domains are currently proprietary to particular clients.

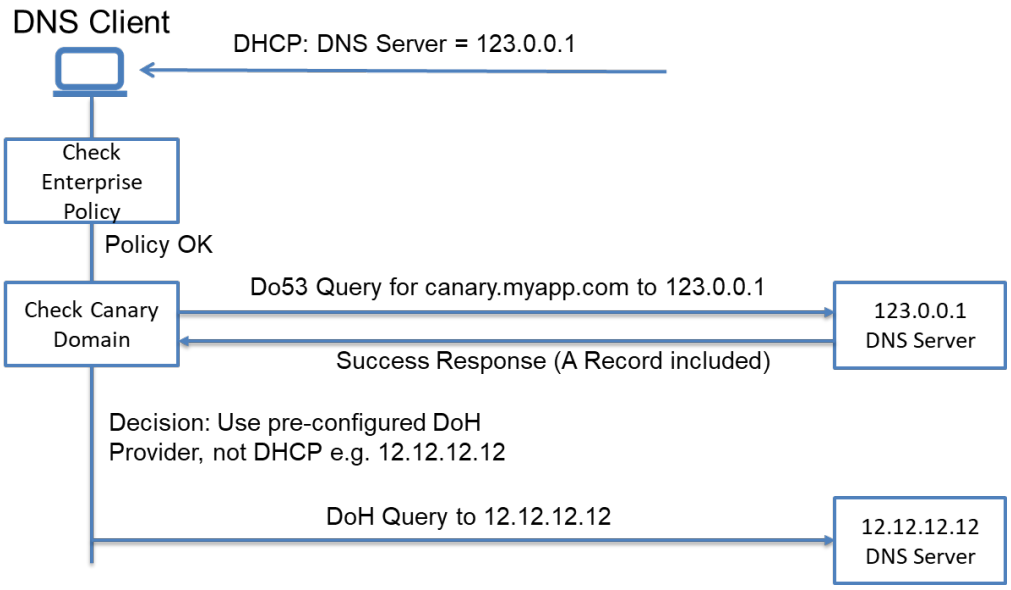

Figure 5.6 Simple Example of DoH Client with Change of DNS Provider

An extreme example of a client that uses a change of DNS provider could be malware that uses a centralized DoH service to avoid DNS-based malware monitoring and protection. When malware deliberately uses DoH to avoid DNS policies, it will obviously not perform checks against features such as enterprise policies and canary domains.

The advantages of DoT and DoH clients that implement a change of provider include:

- Users can access DoT and DoH even if the local DNS resolvers do not support it.
- Local DNS resolvers that are malicious (e.g., enforce undesirable censorship) or have poor privacy policies can be avoided.

The disadvantages of DoT and DoH clients that implement a change of provider include:

- Existing DNS servers are bypassed, which may lead to surprising and undesirable behavior for users.
- DNS-based measures to enforce democratically agreed laws and private managed network policies are avoided.
- Users are moved from a distributed to a centralized DNS infrastructure.

6 Scenarios

The scenarios will be discussed in terms of the technical system operation and the impacts on various actors. It is expected that this discussion will lead to conclusions about recommended good practices by different actors.

6.1 Home Internet Access

This section describes DNS selection in a home network. It describes the common default cases and variations that may occur.

Figure 6.1 shows the model architecture for the home network. DNS queries are often handled by a chain of proxies or resolvers so each node in the chain can insert its own policies and choose where to direct queries further down the chain. Red dots mark points in the home network where DNS behavior may be controlled.

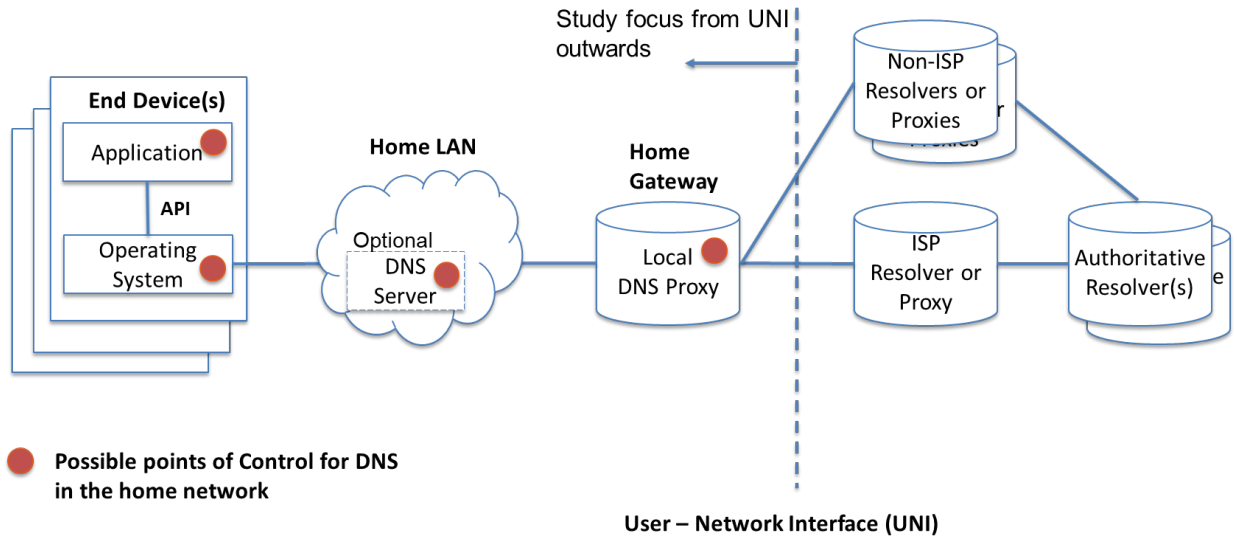

Figure 6.1 Basic Home Network DNS Architecture

Note that resolvers or proxies managed by the ISP may be accessible only via the ISP's access network and may not resolve queries from other sources. This means that the DNS servers may be visible only to clients that are connected to certain access networks. Clients cannot be statically provisioned to access such DNS servers and must change their DNS server, depending on the network context.

6.1.1 Typical Default Operation (Home Gateway with DNS)

In one typical default case, we assume that the home network administrator has taken no actions to override normal configurations and that the home gateway is configured to act as a local DNS proxy. In that case, we normally expect that:

- The local DNS proxy in the home gateway will be configured by DHCP over the UNI, or, if the gateway is provided by the ISP, by a provisioned customized configuration in the gateway. In either case the home gateway's DNS proxy is normally directed to a DNS resolver or proxy managed by the ISP.
- End devices attached to the LAN configure their DNS to refer to the local DNS proxy in the home gateway based on DHCP information on the LAN.

Applications in end devices may either perform their own DNS queries or may request that the operating system perform a query using an API. In either case, the normal default behavior will be to determine the DNS proxy configured in the end device's operating system and then direct the query there. In this case, that will direct the query to the local DNS proxy in the home gateway.

The local DNS proxy in the home gateway will receive a query from the end device and forward it to the ISP's resolver or proxy. This will respond to the query based on the ISP's configuration.

In this scenario the local DNS proxy may have a form of “split-horizon” DNS where special DNS names with only local significance are offered to refer to devices on the LAN. For example, a special-use domain such as “home.arpa” may be used. The home gateway may then have an administration page as “admin.home.arpa” and may have a file share as “share.home.arpa.” These local DNS names may be used as a subject alternate name in an HTTPS certificate for the home gateway.

6.1.2 Typical Default Operation (Home Gateways Without Local DNS)

In another typical default case, some networks or users may have a configuration where there is no local DNS proxy in the home gateway. In this case, the DHCP configuration sent by the home gateway will point to the ISP’s network-based DNS resolver or proxy. Clients on the home LAN that are configured by DHCP will direct DNS queries directly to the ISP’s resolver or proxy.

6.1.3 Primary and Secondary DNS

DNS clients typically allow a primary and secondary DNS server to be specified. The secondary server is used in case the primary is unavailable. These are normally expected to be different instances of the same DNS infrastructure. For example, in the typical default operation, the ISP may provide two addresses for different DNS resolvers or proxies, but each server supports the same DNS services and policies, and both servers are managed by the ISP.

In some configurations, the primary and secondary servers may be set to independent DNS resolvers. For example, the primary DNS server may be the ISP’s DNS, and the secondary DNS server may be a public (e.g., quad-X) DNS.

Throughout these scenarios, the different cases could apply to the primary and secondary DNS servers together or either server independently.

6.1.4 Other Variations at the Home Gateway

Home gateways may provide a range of DNS capabilities that the home network administrator can control via a configuration user interface. In cases where the home gateway is provided by the ISP, the ISP may choose which feature(s) to enable on its gateways. Examples of configuration options on home gateways include:

- Modification of the selected network DNS server(s) to override those specified in DHCP over the UNI.
- User-managed DNS services (e.g., parental controls or site blocking).
- Use of VPNs from the home gateway, including the use of DNS services via the VPN.

In the case where the home gateway applies DNS services, the home network may become an example of a managed network similar to that discussed in section 6.1.8 dealing with enterprises.

Some home gateways may be pre-configured to not use the DNS provider specified by DHCP over the UNI. Instead, they use a DNS service such as a quad-X server.

Some malware may attack the home gateway and modify its DNS behavior (e.g., to redirect popular web sites to alternatives controlled by the malware authors).

The home gateway normally also functions as a manager for local IP addresses on the home LAN and controls the LAN’s DHCP information. As such, using other DNS servers on the LAN may require changes to the home gateway behavior.

Home gateways may be provided and managed by the ISP or by individual users. If the home gateway is provided by the ISP, then there may be considerable variation in how easy and frequently the software can be updated.

6.1.5 Addition of Local DNS Servers on the home LAN

DNS servers may be added to the home LAN in a variety of ways. For example:

- Pi Hole is a home DNS server that may be run as a stand-alone server or as a process on another device. Pi Hole provides a range of DNS screening, monitoring and resolution services.
- Some home networking devices (e.g., Google Wi-Fi) apply their own DNS settings for connected end devices rather than use those from the home gateway.

Special configuration steps may be necessary so end devices can use a local DNS server on the LAN in preference to the home gateway. This could include direct configuration of individual end devices or taking control of the DHCP configuration received by end devices.

In the case where there are special DNS services in the home LAN, the home network may become an example of a managed network similar to that discussed in section 6.2 dealing with enterprises.

6.1.6 End Device Operating System DNS Configuration

In a typical end device, the operating system is responsible for managing the DNS configuration of the device, and many applications use APIs provided by the operating system to resolve DNS queries. Typically, we would expect the operating system to be configured using DHCP from the home LAN.

Operating systems can override or augment DNS configurations from DHCP in a variety of ways. This may be done using operating system administrative tools (e.g., editing the hosts file), using a CLI or by using an application or demon process. Example alternative configurations due to this kind of customization include:

- Change to the DNS provider for the device.
- Hardcoding DNS responses for specific host names (e.g., to block certain hosts).
- Using special network services that include their own DNS behavior (e.g., VPNs).
- Using device-based DNS processes that provide special handling of DNS (e.g., “stubby,” which can map unencrypted DNS queries to an encrypted alternative).

It is possible that malware on end devices may change DNS behavior for the end device, (e.g., to hijack web domains to steal user credentials).

Some devices may have operating systems that are pre-configured to use particular DNS services regardless of the DHCP configuration on the network. For example, IoT devices, home video streaming dongles and other devices that rely on proprietary cloud infrastructure may use DNS associated with their cloud service.

6.1.7 End Device Application DNS Configuration

Applications typically use configurations or APIs from the end device operating system to perform DNS queries. However, applications can do DNS using their own DNS configurations.

Some applications (e.g., Tor browsers), may use their own DNS settings as part of providing specific networking features. Applications that are tied to a particular proprietary cloud service (e.g., a home automation application) may use DNS associated with their cloud service.

Recently, there has been particular attention on moves by leading web browsers to directly implement DoH in order to encrypt DNS traffic ahead of support in some operating systems and ISPs. Web browsers have implemented different policies in terms of how to select when DoH should be active and which resolver DoH queries should be addressed to.

Misconfiguration of DNS on end devices is a possible source of problems for users. Therefore, automatic configuration will be desirable from a user experience point of view. ISPs are frequently the first point of contact when users experience connectivity issues. Increasing complexity of DNS configuration, and the use of DNS services outside the ISP, will make it harder for ISPs to address connectivity problems caused by DNS. This may be a particular issue for IoT and similar devices that are dependent on DNS, but do not provide a good user interface to manage DNS configurations.

6.1.8 Network Visitors

Home networks often receive visitors who are not part of the household that owns the network. Network owners may be concerned about the use of their network by visitors. Some home networks may provide the ability to separate “normal” and “visitor” traffic so that separate policies can be applied.

If visitors’ devices are configured to use a DNS server in the home network, the network owner can use DNS to apply policy to visitors by configuring the home gateway, or local DNS servers in the home LAN (see discussion above). However, if the operating system or individual applications on visitors’ end devices contain their own DNS configurations, these may bypass policies set by the network owner.

6.1.9 Analysis of Home Network Scenario

Figure 6.1 shows how home networks present a variety of deployment models and user requirements. As such, it is important that as DNS services evolve accommodate the full range of use cases and to appropriately accommodate user needs in the particular context of the network configuration and application requirements.

The ability of DoH and DoT to protect the confidentiality and integrity of DNS queries between the end device and the first DNS server can improve DNS security, particularly if the query is going outside the confines of the home LAN or is carried over an unsecure wireless LAN. However, it should be noted that, in a minimal deployment, these protocols protect only one interface of a more complicated system.

DNS services within the home network are one tool that the home network’s owner (acting as a network administrator) may use to set policies for their home network (see sections 6.1.4 and 6.1.5). Where the home network uses the ISP’s DNS resolver, these resolvers may offer important security protections and help support national policies (see section 4).

End devices and applications that honor policies set by networks (e.g., if the user has indicated they wish the end device to trust the home network) should be cautious about changing their DNS behavior to avoid breaking network policy implementations. One way that end devices and applications can switch to DoT or DoH (where available) without breaking network policies is to implement an opportunistic DNS protocol upgrade using a same-provider rule.

A number of applications and operating systems are developing proprietary solutions to implement opportunistic same-provider upgrades. Industry alignment around approaches and tools to help with DNS discovery and protocol upgrade decisions would help improve the consistency, range of applicability and user experience for this strategy. Without this alignment, there is a risk that the full range of scenarios are not factored into the design and users experience unexpected and confusing behavior.

A particular challenge in implementing the same-provider upgrade strategy is when the first DNS server is located on a gateway using a private IP address. This raises questions of:

- How to identify the actual DNS provider in a global context.
- How to authenticate a gateway that end devices see only as a privately addressed node.

Another aspect of same-provider upgrade strategies is the need to consider the device context. One example, as discussed in the reference architecture, is whether the ISP's DNS service is available globally or only via the ISP's access network.

Applications that use DoT, and particularly DoH, to reach external DNS servers without honoring the network configuration can prevent home network users and ISPs from applying policy and other services using DNS. How networks deal with this will depend on the importance and extent of problems caused. Some options to address DoH in managed networks are discussed in section 6.2 dealing with the enterprise case.

Use of DoT and DoH by clients in home networks may prevent ISPs using DNS to enforce legal or national requirements using DNS. This may have implications for how laws are constructed and enforced. It may also have implications for public DNS providers that may find requirements currently applied to ISPs are extended to them. These issues are discussed in the summary of the recommendations.

Standardization of tools to enable discovery of DoT and DoH servers in a context-aware manner and practices on how to make best use of these tools would benefit several groups, including client vendors, individual users, the managers of home networks and ISPs. Without this standardization, there will be a confusing and difficult-to-manage array of proprietary solutions.

6.2 Enterprise Network

6.2.1 Reference Architecture

Figure 6.2 illustrates a reference architecture for enterprise use. Many enterprises will deploy their own DNS servers. These servers may offer a split-horizon DNS, where internal DNS names are subject to special handling. Enterprises may monitor and block (or redirect) detectable DNS traffic using network monitoring capabilities. This may be particularly important in organizations (e.g., financial institutions) that are subject to strict policies on control of data.

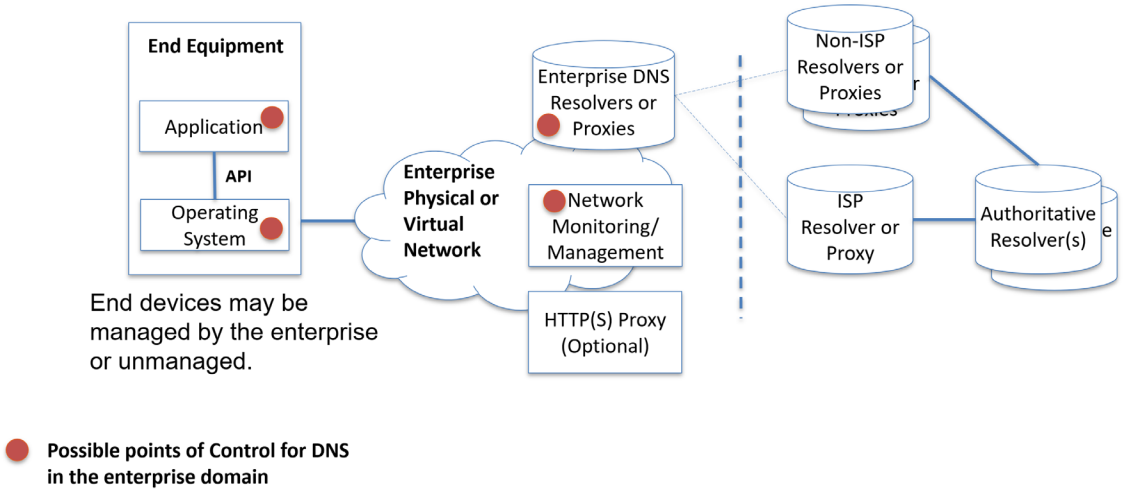

Figure 6.2 Enterprise Reference Architecture

Where the enterprise is able to manage all the end devices on its network, these devices can be an important point of control for DNS and other services. However, a solution that relies entirely on managing end devices may not be acceptable for enterprises whose Bring Your Own Device policy and IoT devices do not support enterprise policy features.

The possible points of control for DNS are discussed below.

Application Layer – Here, end users may be able to configure their applications to support a custom DNS service. Applications include traditional internet browsers, web-based applications and commercial and in-house apps.

Security risk: Poorly controlled applications do not respect enterprise domain controls. These applications may enable obfuscation of enterprise monitoring and expose the enterprise to an increased attack surface and elevated level of risk.

Mitigations:

- Ensure all enterprise applications have security controls, which allow administrators to enforce company DNS policies.
- Ensure internally developed applications implement policy compliant DNS controls.

Difficulty of DNS enforcement: High, due to inconsistent application enforcement options and mechanisms. Non-compliant applications may be difficult to locate and to enforce.

Operations System Layer – Here, end users may be able to configure the operating system to support a custom DNS service. Operating system controls have more mature policy enforcement options and a higher degree of control by enterprise administrators.

Security risk: For poorly controlled operating systems, which do not respect enterprise domain controls, the OS may enable obfuscation of enterprise monitoring and expose the enterprise to an increased attack surface and elevated level of risk. However, OS control is well documented and understood and generally available in many enterprise settings today.

Mitigations:

- Ensure all systems have OS-level controls, which allow administrators to enforce company DNS policies.
- Deny access to OS settings via policy.

Difficulty of DNS enforcement: Moderate to low due to the maturity of OS policy controls and enforcement. Additionally, identifying and assessing individual end points are well documented and scalable. However, risk is not sufficiently mitigated as unsecured/unmanaged/undiscovered end points could be using unapproved DNS solutions.

Enterprise DNS Resolvers or Proxies – Here, end users have little to no influence over the settings. The enterprise DNS resolvers and proxies are configured by enterprise administrators and, when leveraged properly, implement and enforce the desired DNS controls

Security risk: Low risk of DNS misuse. Risk is introduced due to concentrated data flows and central point of attack. However, this is an understood design risk, and DNS is not a unique use case. Remaining risk is due to poorly controlled or undocumented exfiltration points that are not controlled and monitored.

Mitigations:

- Ensure no unauthorized or undocumented exfiltration points exist.
- Secure and enforce flow through enterprise resolver and proxy.

Difficulty of DNS enforcement: Low.

6.2.2 Actors in an Enterprise Network

- Traditional network users include all enterprise personnel, with the exception of developers, that may be located within the enterprise.
- Network devices traditionally found in enterprise environments, including user end points such as phones, laptops and workstations, as well as network elements including switches, routers, proxy, IDPD and firewalls.
- Developers are users who create custom applications either for internal or external use.
- Security operations teams are responsible for monitoring and defending enterprise assets.
- Corporate legal and HR teams are responsible for developing and maintaining corporate policies that balance the need to operate and defend an enterprise and the privacy concerns of onsite personnel.
- Adversaries looking to do damage to an enterprise.

6.2.3 DNS Technology Relevance to Enterprise Actors

The following tables show the security trade offs for different DNS protocols and their likely appeal to different actors in an enterprise context.

Support for DNS53

Pros	Cons
• Complete visibility of internal and external traffic for network monitoring and management • Existing toolset to help protect enterprise services • Universal support for the protocol	• No privacy of connections • Exploit tools know and expect DNS to be available and are used

User Base	Acceptable, Encouraged or Discouraged
Traditional Network Users	Acceptable
Privacy Advocates	Discouraged
Network Devices	Acceptable
Application Developers	Acceptable
Security Operations Teams	Acceptable
Corporate Legal and HR Teams	Acceptable
Adversaries	Encouraged

Support for DoH

Pros	Cons
• Application layer control in network filters • Ensures complete privacy of DNS request content to middleboxes • More difficult to control/block when in totalitarian regimes	• Difficult to enforce security via DNS – break and inspect required on HTTPS. • Existing malware in the wild using DoH as C2 and exfiltration

User Base	Acceptable, Encouraged or Discouraged
Traditional Network Users	Acceptable
Privacy Advocates	Encouraged

Network Devices	Acceptable
Application Developers	Acceptable (generally) Encouraged (privacy-conscious Javascript applications in the browser)
Security Operations Teams	Discouraged
Corporate Legal and HR Teams	Discouraged
Adversaries	Acceptable

Support for DNS of TLS

Pros	Cons
• Transport layer control, which enables filtering at boundary devices • Ensures privacy of DNS contents	• Encrypts DNS payload, which could make enterprise security enforcement more difficult • Totalitarian regimes/censors can block the capability with greater ease.

User Base	Acceptable, Encouraged or Discouraged
Traditional Network Users	Acceptable
Privacy Advocates	Relative to Do53: Encouraged Relative to DoH: Discouraged
Network Devices	Acceptable
Developers	Acceptable
Security Operations Teams	Acceptable
Corporate Legal and HR Teams	Acceptable
Adversaries	Acceptable

6.2.4 Filtering for DoH in Managed Networks

In some contexts (e.g., for enforcing policies in managed enterprise networks), it may be appropriate for the network to apply filtering rules to prevent end devices from accessing external DoH services.

Where the network is able to apply policies directly to the end devices, this should be considered as a mechanism to manage how devices use DNS services. However, the network may also be required to

apply policies via a middlebox or firewall to devices that are connected to the network, but are not managed by the network administrator (e.g., IoT devices that do not provide a suitable management interface).

The following sections illustrate some scenarios for filtering policies that may be applied in managed networks based on IP address and port number. It is assumed that DoH prevents the managed network from inspecting the contents of DoH queries to external servers; therefore, network filtering can only be done on information contained in the IP packet header fields. In practice, other techniques, such as heuristic traffic analysis, may provide more sophisticated approaches to filtering DoH traffic.

6.2.5 DoH Server with Well-Known IP Address

Preventing access to DoH servers with well-known IP addresses can be done by maintaining a list of addresses used by well-known DoH servers and blocking traffic to port 443 on the server. This policy's consequence for users will depend on which other services the DoH server supports on port 443.

In cases where the DoH server uses port 443 only for DoH-related services, the filtering is effective and has minimal side effects, as illustrated below.

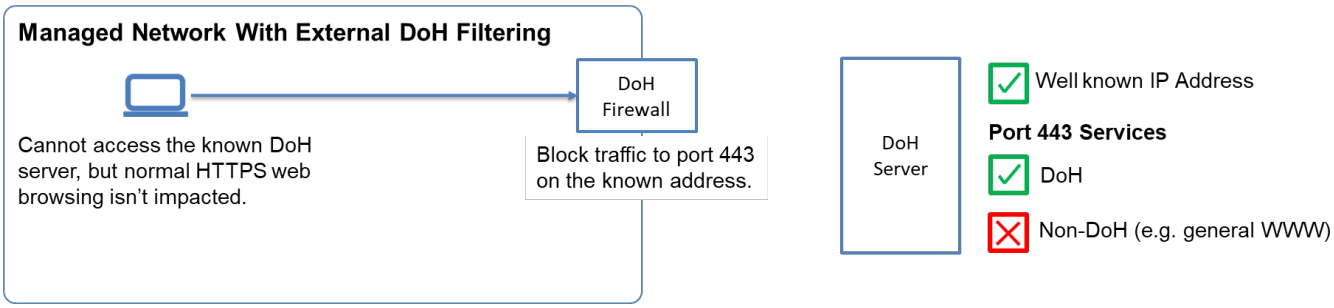

Figure 6.3 Filtering Scenario with Well-Known IP Address and DoH Services on Port 443

In cases where the DoH server uses port 443 for services that are unrelated to DoH, the filtering will have the undesirable side effect of also blocking access to other services. This could be particularly severe if the address is an anycast IP address used by a major CDN or web property because the filter may prevent access to important and popular web sites.

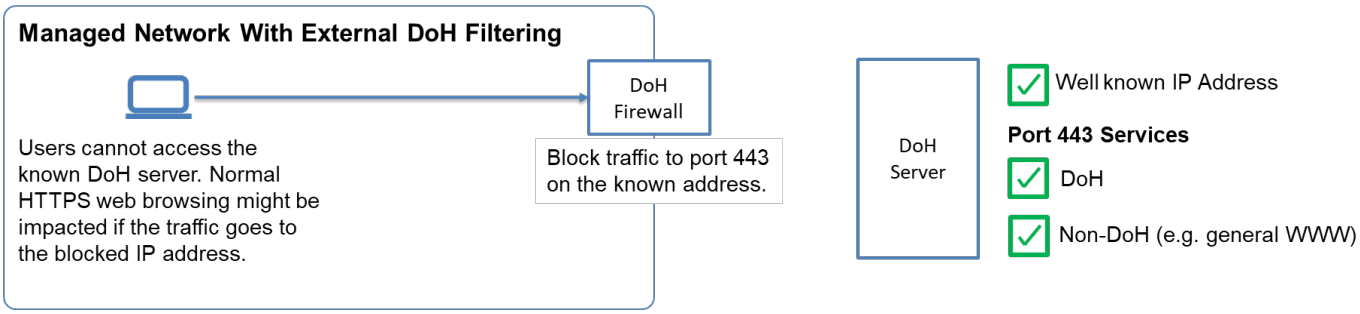

Figure 6.4 Filtering Scenario with Well-Known IP Address and Both DoH and Non-DoH Services on Port 443

If the goal is to block DoH servers that are unknown to the managed network, one solution is to allow access only to a list of known safe addresses. However, this may have a poor user experience.

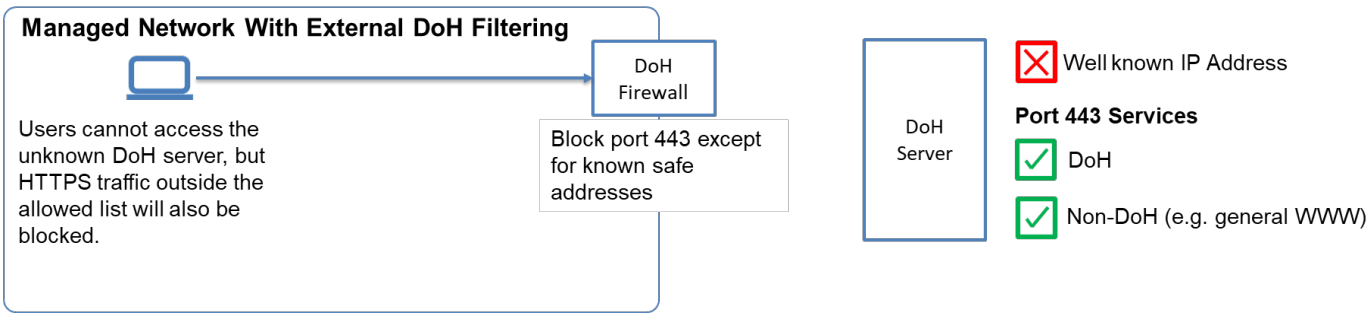

Figure 6.5 Filtering Scenario Based on a list of allowed addresses to Block Unknown DoH Servers

6.2.6 Conclusion: Enterprise Networks

Enterprise networks include those in educational institutions and other networks dedicated to particular organizations. These have strong requirements to ensure that their networks are used only for valid purposes, and to support custom features for the convenience and security of users. In some cases, these requirements may extend to legal requirements (e.g., for financial institutions to record transactions taking place on their systems).

Today, DNS is often used as a tool to implement these requirements. Specific applications of DNS include:

- The use of split-horizon DNS to support private name spaces.
- The use of DNS to control access to external sites and resources.

DNS privacy and integrity protocols such as DoT and DoH can help enterprises with information security. But they also have the potential to disrupt services that are implemented using DNS and reduce the information available to network security monitoring systems.

Clients that use a same-provider strategy for DNS protocol upgrade could be a basis for introducing DoT and DoH in a way that is compatible with enterprise requirements. However, with many enterprises using private address spaces and running their own DNS resolvers, the determination of the DNS provider and management of information about corresponding providers will be complicated.

Clients that implement DoT or DoH using an approach that changes the provider are generally incompatible with the requirements of a private managed enterprise network. Such clients should, at least, provide tools to allow the enterprise to manage DNS settings on the endpoint and disable changes to DNS provider. As far as possible, these tools should be standardized to reduce the complexity of network management.

Enterprise networks may have a requirement to disable DNS queries from clients that do not support the necessary management features and do not honor the network's indicated DNS provider. This may require the development and filtering of solutions for unauthorized DoT and DoH clients within the enterprise network. Filtering may unintentionally block services other than DoT or DoH that share the same server IP address and port number. For this reason, we recommend that public DoT and DoH servers do not combine DoT/DoH and unrelated other services on the same port.

Developments of standards for DNS discovery and best practices that meet enterprise requirements would simplify the secure management of enterprise networks.

6.3 Mobile Network

Figure 6.6 illustrates the reference architecture for mobile services. Mobile devices often move between Wi-Fi (public or private) and cellular connectivity. Inconsistencies in DNS handling in the two environments may be visible to users.

The mobile user equipment (UE) may support "tethering," which effectively creates a private Wi-Fi network around the UE, with the UE acting as the gateway and the mobile network providing internet connectivity. Within the tethered network, the discussions of private residential networks and enterprise networks in the preceding section may be relevant. This section focuses on UEs rather than tethered devices.

Note that for UEs roaming between networks, the exact network topology will depend on how the roaming agreement is implemented between the home and visited network.

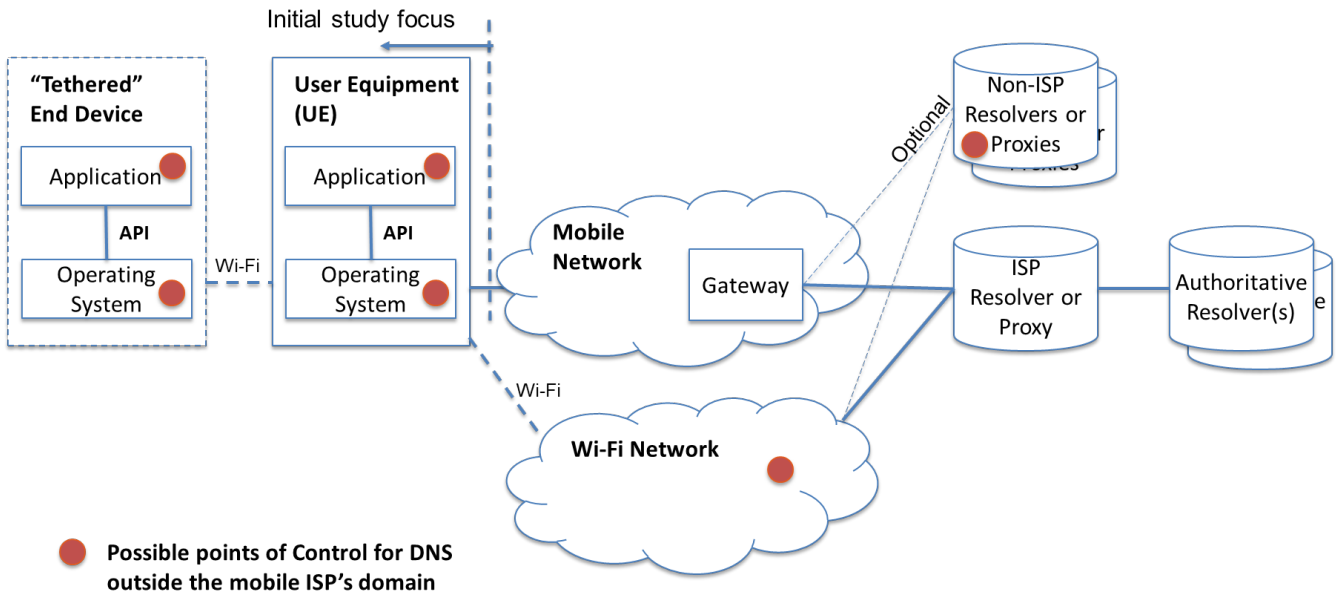

Figure 6.6 Reference Architecture for Mobile Networks

6.3.1 Typical Default Operation

In a typical default operation, a UE connected to the mobile network will receive DNS configuration information either via protocol configuration options (PCO) in mobile signalling or by DHCP through the mobile network IP tunnel. These will typically point to a DNS resolver managed by the mobile network operator.

As with wired networks, the DNS service may be used for policy management and network operational services.

6.3.2 Alternative Configurations

Many UEs allow their DNS services to be configured differently from that set by the mobile network. For example:

- Built-in operating system features that attempt to "normalize" DNS behavior across multiple access technologies.

- From the device administrator via the device preferences, or using a configuration application.
- Using special network services (e.g., VPNs).
- Via firmware or special configuration for embedded and IoT devices.

In some cases, UEs may allow network operators to configure end device policies over DNS settings in the UE.

6.3.3 Conclusion: Mobile Network

Like wireline ISPs, mobile network operators may use DNS for a variety of operational services and enforcement of legal policies. Many of the issues created by changes to DNS that are discussed in the home internet access scenario will apply to mobile networks, too.

The geographic mobility of mobile phones and the support of international roaming means that optimization of CDN content location may need to take account of the UE's current location.

International roaming means that several countries may be involved in issues of legal policy enforcement and support of national requirements for user privacy. These need to be taken in to account when using DNS to implement features.

It is recommended that standards are developed to support the discovery and selection of DNS services that accommodate the needs of mobile networks.

6.4 Public Wi-Fi with Captive Portal

Many organizations provide public Wi-Fi services on their premises. This is often accompanied by the use of a "captive portal," which requires uses to log on or accept the terms of service before they are able to connect to the internet. In the absence of standards, the implementation of these services uses proprietary techniques. To alleviate some of the problems associated with proprietary implementations, the IETF CAPPORT working group is developing a standard architecture and protocols for captive portal support.

6.4.1 Reference Architecture

Figure 6.7 illustrates the reference architecture for the public Wi-Fi with a captive portal.

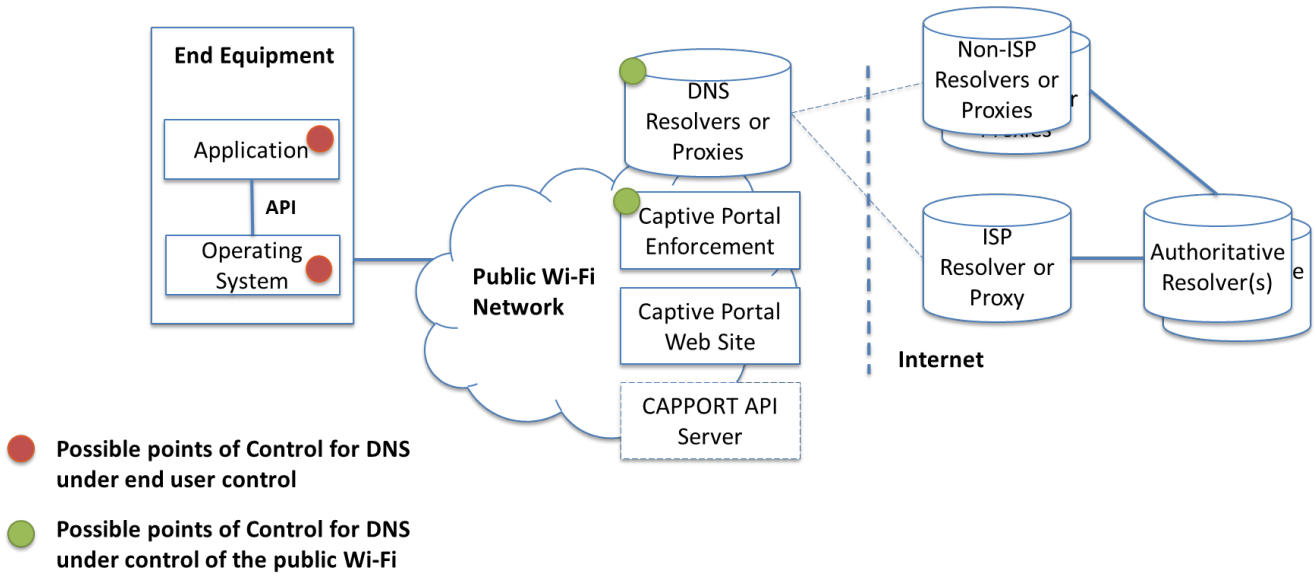

Figure 6.7 Reference Architecture for Public Wi-Fi with Captive Portal

The public Wi-Fi network is expected to provide its own DNS resolver or proxy. The captive portal enforcement will apply policies for routing data between the public Wi-Fi and the internet. The captive portal web site will provide a user interface to allow users to perform the required actions to enable internet connectivity. If the IETF CAPPORT architecture is implemented, then a CAPPORT API server will also be present. All these functions need to act in coordination to deliver the correct service to the end user.

Public Wi-Fi networks frequently use a private IP address space for end devices and servers within the network.

6.4.2 Normal Operation

On initial network attachment, devices are kept "captive" in the network and can access only special services within the captive network, and possibly a few chosen external sites (e.g., the network owner's web site).

Web requests from captive devices are redirected to the captive portal web site. From there, users may register with the network to allow their device to escape captivity.

End devices are provisioned by the network (e.g., using DHCP) to access a DNS server chosen by the network administrator. The chosen DNS server may have special features to support the public Wi-Fi, such as:

- Web request redirection to a captive portal.
- Policy enforcement of allowed external site access when in captive and non-captive modes.
- User behavior tracking and analytics (subject to local laws and practices).

Access to the public internet is unlikely to be solely controlled by the DNS server. The captive portal enforcement will apply policies based on IP address.

6.4.3 Normal Operation with IETF CAPPORT

The CAPPORT project in IETF aims to provide a mechanism to implement captive portal behavior without the network having to do man-in-the-middle (MITM) interception of web traffic. It aims to avoid the undesirable security consequences of pervasive MITM of traffic, and to be compatible with the emerging security protocols, such as TLS1.3, DoT and DoH.

Figure 6.8 shows the general operation concept in CAPPORT.

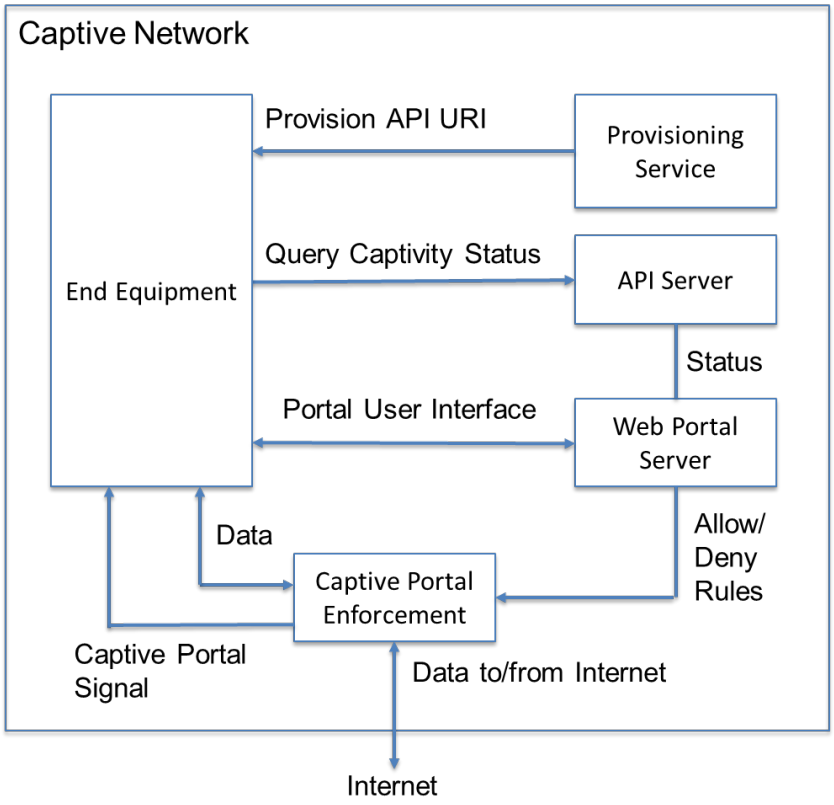

Figure 6.8 IETF CAPPORT Overview

When the end device attaches to the network, it receives provisioning information that contains a URI for a CAPPORT API server. This could be done in a DHCP message. The end device can signal to this URI and receive information about its captivity status and the address of the captive web portal.

Using the captive web portal, users can register with the network and allow their device to escape captivity. The captivity status will be communicated to the captive portal enforcement, allowing it to apply the correct policy.

6.4.4 Analysis

In this scenario, users may have a low level of trust in the network. In the worst case, the network may attempt to use its on-path position to inject malicious or unwanted content. The low trust may mean users prefer to bypass the public Wi-Fi DNS to connect to an external DNS server instead (e.g., using DoH). This choice may create service problems for the user or the public Wi-Fi, such as:

- This may defeat some policy enforcement (e.g., specific site blocking) within the public Wi-Fi.

- Use of the internal DNS may be necessary for web redirect to the captive portal web page.
- While a device is captive, external DNS traffic may be blocked by the captive portal enforcement.
- Even when a device has escaped captivity, certain protocols or external IP addresses may be blocked by the captive portal enforcement, which could prevent DoT or DoH access to external DNS servers from working.

In the absence of specific guidance, proprietary solutions for captive portals have been developed that may embed assumptions about client behavior. CAPPORT is attempting to make captive networks more consistent, but roll-out will take many years.

6.4.5 Conclusion: Public Wi-Fi with Captive Portal

In a low-trust situation such as public Wi-Fi, users may prefer using a centralized rather than local DNS server. Doing so may improve user privacy and security. But depending on the precise configuration, it also may prevent access to network features, including access to the captive network portal to log-on to the network).

Clients may want to use different DNS strategies based on the network context and level of trust in the attached network. Therefore, clients should consider how to apply different policies for DNS server selection based on the context of the access network.

Public Wi-Fi networks should assess the impact of DoT and DoH being introduced on clients and adjust their technology and policies appropriately.

Same-provider DNS protocol upgrade strategies may not work in public Wi-Fi, which uses private IP addresses for the local DNS.

DoT and DoH client deployment should be compatible with current practices for captive portals and the emerging CAPPORT approach. We recommend industry collaboration to develop such approaches.

7 Conclusion

The IETF has defined the DoT and DoH protocol specifications for encrypted DNS. However, how to deploy and operationalize these protocols is largely undefined. Important clients and DNS servers are now deploying DoT and DoH using a variety of different approaches. The use of DoT and DoH can have benefits for user security and privacy. However, the current piecemeal deployments raise complex issues for many stakeholders and thus require organizational and technical responses.

This document presents scenarios that illustrate some of the different contexts in which DNS may be used. Each scenario presents different considerations for DoT and DoH deployment. These scenarios should be used to guide decision-making by clients and servers deploying DoT and DoH. They can also be used by organizations impacted by DoT and DoH to help formulate their strategy.

We have enumerated key recommendations for different stakeholders in section 3. We encourage collaboration among all stakeholders to create technical standards and best practices for the deployment of DoT and DoH that take account of the scenarios in this report.

8 Acronyms and Abbreviations

For a list of common communications terms and definitions, visit the ATIS Telecom Glossary, which is located at < https://glossary.atis.org >.

Acronyms & Abbreviations:

ATIS	Alliance for Telecommunications Industry Solutions
CDN	Content Delivery Networks
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DMARC	Domain-Based Message Authentication, Report and Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
Do53	DNS Over Port 53 (i.e., DNS without security)
DoH	DNS over HTTPS
DoT	DNS over TLS
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
LAN	Local Area Network
MITM	Main-In-The-Middle
NAT	Network Address Translation
PCO	Protocol Configuration Options
TLS	Transport Layer Security

Appendix 1 – Organizational and Customer Communications and Talking Points

Background

The domain name system (DNS) is a critical internet service that resolves human-readable domain names to IP addresses. Almost all web traffic and other Internet applications rely on DNS to allow the client to find the required server. Currently a large majority (approximately 80 percent) of DNS queries are handled by the user's ISP. This allows ISPs to use DNS to fulfil operational needs and offer services. Changes in DNS technology and implementation practices are now creating challenges and opportunities. The IETF has standardized protocols for the use of encrypted DNS: DNS over HTTPS (DoH) and DNS over TLS (DoT). These technologies can enhance the security of DNS protocols. However, they also may be implemented by browsers and mobile operating systems in a way that could dramatically change the internet architecture and have marked impacts on important DNS-based features. DoH has particular security implications because it is resistant to most approaches for interception and monitoring in the network.

Who Needs to Be Informed?

Changes to DNS can have significant impacts for ISPs and their personal and enterprise customers. Application developers and solution integrators should also be aware of the changes to make informed choices in their designs.

This section lists some of the main groups that may be impacted and highlights some of the relevant concerns.

ISP's Internal Communications Team

Goal: Solicit help in messaging other internal groups.

ISP Subscriber Customer Support Service Desks

Goal 1: Messaging to help them know questions will come and preload their answer queue to help users:

- Understand options
- Make informed choices

Goal 2: prepare processes to help debug and resolve connectivity problems due to DNS changes.

ISP Subscriber End Users (via ISP Customer Communications Teams)

Goal: Proactively explain the services that the ISPs offer and help users make informed choices that meet their needs.

ISP Enterprise Customer Support Service desks, Account Managers, Sales Representatives, etc.

Goal 1: Messaging to help them know questions will come and preload their answer queue.

Goal 2: Prepare processes to help debug and resolve connectivity problems due to DNS changes.

Enterprise Customers (via ISP Enterprise Customer Communications Teams)
Goal: Advise about new risks due to DNS changes and approaches to protect the security of their network.

ISP management team
Goal: Awareness of the fundamental nature of the change.

- What's at stake
- What could happen
- Technical and organizational responses
- Industry initiatives (e.g., ATIS, EDDI)

Q&As
The following text is possible starting points for ISPs and other DNS providers to describe some of the issues around secure DNS to different audiences. They have been written to express the technical information without over-use of detailed terminology or jargon. However, they would still need to be adjusted to suit the level of technical comprehension of the audience.
Note that the implementation plans for web browsers are subject to change. We believe the statements here are a correct reflection of the plans at the time of writing.

What are web browsers (e.g., Chrome, Firefox) changing?
Describe the changes to browser behavior in your region. Explain the consequences to users and recommended user actions (e.g., configuration recommendations).

What is your policy on DNS privacy and encrypted DNS?
This will change from company to company, but for ISPs the following points might be considered:

- Are you planning to introduce DoH or DoT on your DNS service? When? How can customers enable this?
- If you are not encrypting DNS traffic do you use other measures to prevent DNS eavesdropping – e.g., by routing DNS queries internally to your network only?
- What are your policies and relevant national requirements for DNS privacy?

Specific templates to describe DNS privacy have been proposed. For example:

- The EDDI "Disclosure Form" draft at https://github.com/Encrypted-DNS-Deployment-Initiative/Data-Policies/blob/master/disclosure-form.md
- The Internet draft draft-reddy-dprive-dprive-privacy-policy-00 https://tools.ietf.org/html/draft-reddy-dprive-dprive-privacy-policy-00. In particular, refer to section 5.2.2 of the draft.

If I enable encrypted DNS, who can still see DNS queries?
Encrypted DNS aims to protect information between the requesting client and the DNS server that responds to the request. The responding server necessarily sees the contents of the query and may, according to its privacy policies, record or share information about the query. Furthermore, the request may need to be forwarded to other DNS servers to be resolved, and these will also see information about the request.

Does DNS encryption improve the authenticity of DNS responses?

DNS encryption can prevent modification of responses between you and the server you contacted, but on its own does not guarantee authenticity. Secure web sites have a certificate that validates the owner of the site, and this can protect against impersonation. Refraining from clicking through certificate authenticity warnings on HTTPS sites is the single most powerful way to validate servers to which your browser interacts with the internet and web.