       Considerations around Transport Header Confidentiality, Network
        Operations, and the Evolution of Internet Transport Protocols

Abstract

   To protect user data and privacy, Internet transport protocols have
   supported payload encryption and authentication for some time. Such
   encryption and authentication are now also starting to be applied to
   the transport protocol headers. This helps avoid transport protocol
   ossification by middleboxes, mitigate attacks against the transport
   protocol, and protect metadata about the communication. Current
   operational practice in some networks inspect transport header
   information within the network, but this is no longer possible when
   those transport headers are encrypted.

   This document discusses the possible impact when network traffic uses
   a protocol with an encrypted transport header. It suggests issues to
   consider when designing new transport protocols or features.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are candidates for any level of Internet
   Standard; see Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc9065.

Table of Contents

1. Introduction

   The transport layer supports the end-to-end flow of data across a
   network path, providing features such as connection establishment,
   reliability, framing, ordering, congestion control, flow control,
   etc., as needed to support applications. One of the core functions
   of an Internet transport is to discover and adapt to the
   characteristics of the network path that is currently being used.

   For some years, it has been common for the transport-layer payload to
   be protected by encryption and authentication but for the transport-
   layer headers to be sent unprotected. Examples of protocols that
   behave in this manner include Transport Layer Security (TLS) over TCP
   [RFC8446], Datagram TLS [RFC6347] [DTLS], the Secure Real-time
   Transport Protocol [RFC3711], and tcpcrypt [RFC8548]. The use of
   unencrypted transport headers has led some network operators,
   researchers, and others to develop tools and processes that rely on
   observations of transport headers both in aggregate and at the flow
   level to infer details of the network's behaviour and inform
   operational practice.

   Transport protocols are now being developed that encrypt some or all
   of the transport headers, in addition to the transport payload data.
   The QUIC transport protocol [RFC9000] is an example of such a
   protocol. Such transport header encryption makes it difficult to
   observe transport protocol behaviour from the vantage point of the

network. This document discusses some implications of transport header encryption for network operators and researchers that have previously observed transport headers, and it highlights some issues to consider for transport protocol designers.

As discussed in [RFC7258], the IETF has concluded that Pervasive Monitoring (PM) is a technical attack that needs to be mitigated in the design of IETF protocols. This document supports that conclusion. It also recognises that [RFC7258] states, "Making networks unmanageable to mitigate PM is not an acceptable outcome, but ignoring PM would go against the consensus documented here. An appropriate balance will emerge over time as real instances of this tension are considered." This document is written to provide input to the discussion around what is an appropriate balance by highlighting some implications of transport header encryption.

Current uses of transport header information by network devices on the Internet path are explained. These uses can be beneficial or malicious. This is written to provide input to the discussion around what is an appropriate balance by highlighting some implications of transport header encryption.

2. Current Uses of Transport Headers within the Network

In response to pervasive surveillance [RFC7624] revelations and the IETF consensus that "Pervasive Monitoring Is an Attack" [RFC7258], efforts are underway to increase encryption of Internet traffic. Applying confidentiality to transport header fields can improve privacy and can help to mitigate certain attacks or manipulation of packets by devices on the network path, but it can also affect network operations and measurement [RFC8404].

When considering what parts of the transport headers should be encrypted to provide confidentiality and what parts should be visible to network devices (including unencrypted but authenticated headers), it is necessary to consider both the impact on network operations and management and the implications for ossification and user privacy [Measurement]. Different parties will view the relative importance of these concerns differently. For some, the benefits of encrypting all the transport headers outweigh the impact of doing so; others might analyse the security, privacy, and ossification impacts and arrive at a different trade-off.

This section reviews examples of the observation of transport-layer headers within the network by using devices on the network path or by using information exported by an on-path device. Unencrypted transport headers provide information that can support network operations and management, and this section notes some ways in which this has been done. Unencrypted transport header information also contributes metadata that can be exploited for purposes unrelated to network transport measurement, diagnostics, or troubleshooting (e.g., to block or to throttle traffic from a specific content provider), and this section also notes some threats relating to unencrypted transport headers.

Exposed transport information also provides a source of information

that contributes to linked data sets, which could be exploited to
deduce private information, e.g., user patterns, user location,
tracking behaviour, etc. This might reveal information the parties
did not intend to be revealed. [RFC6973] aims to make designers,
implementers, and users of Internet protocols aware of privacy-
related design choices in IETF protocols.

This section does not consider intentional modification of transport
headers by middleboxes, such as devices performing Network Address
Translation (NAT) or firewalls.

2.1. To Separate Flows in Network Devices

Some network-layer mechanisms separate network traffic by flow
without resorting to identifying the type of traffic: hash-based load
sharing across paths (e.g., Equal-Cost Multipath (ECMP)); sharing
across a group of links (e.g., using a Link Aggregation Group (LAG));
ensuring equal access to link capacity (e.g., Fair Queuing (FQ)); or
distributing traffic to servers (e.g., load balancing). To prevent
packet reordering, forwarding engines can consistently forward the
same transport flows along the same forwarding path, often achieved
by calculating a hash using an n-tuple gleaned from a combination of
link header information through to transport header information.
This n-tuple can use the Media Access Control (MAC) address and IP
addresses and can include observable transport header information.

When transport header information cannot be observed, there can be
less information to separate flows at equipment along the path. Flow
separation might not be possible when a transport forms traffic into
an encrypted aggregate. For IPv6, the Flow Label [RFC6437] can be
used even when all transport information is encrypted, enabling Flow
Label-based ECMP [RFC6438] and load sharing [RFC7098].

2.2. To Identify Transport Protocols and Flows

Information in exposed transport-layer headers can be used by the
network to identify transport protocols and flows [RFC8558]. The
ability to identify transport protocols, flows, and sessions is a
common function performed, for example, by measurement activities,
Quality of Service (QoS) classifiers, and firewalls. These functions
can be beneficial and performed with the consent of, and in support
of, the end user. Alternatively, the same mechanisms could be used
to support practises that might be adversarial to the end user,
including blocking, deprioritising, and monitoring traffic without
consent.

Observable transport header information, together with information in
the network header, has been used to identify flows and their
connection state, together with the set of protocol options being
used. Transport protocols, such as TCP [RFC7414] and the Stream
Control Transmission Protocol (SCTP) [RFC4960], specify a standard
base header that includes sequence number information and other data.
They also have the possibility to negotiate additional headers at
connection setup, identified by an option number in the transport
header.

In some uses, an assigned transport port (e.g., 0..49151) can
identify the upper-layer protocol or service [RFC7605]. However,
port information alone is not sufficient to guarantee identification.
Applications can use arbitrary ports and do not need to use assigned
port numbers. The use of an assigned port number is also not limited
to the protocol for which the port is intended. Multiple sessions
can also be multiplexed on a single port, and ports can be reused by
subsequent sessions.

Some flows can be identified by observing signalling data (e.g., see
[RFC3261] and [RFC8837]) or through the use of magic numbers placed
in the first byte(s) of a datagram payload [RFC7983].

When transport header information cannot be observed, this removes
information that could have been used to classify flows by passive
observers along the path. More ambitious ways could be used to
collect, estimate, or infer flow information, including heuristics
based on the analysis of traffic patterns, such as classification of
flows relying on timing, volumes of information, and correlation
between multiple flows. For example, an operator that cannot access
the Session Description Protocol (SDP) session descriptions [RFC8866]
to classify a flow as audio traffic might instead use (possibly less-
reliable) heuristics to infer that short UDP packets with regular
spacing carry audio traffic. Operational practises aimed at
inferring transport parameters are out of scope for this document,
and are only mentioned here to recognise that encryption does not
prevent operators from attempting to apply practises that were used
with unencrypted transport headers.

The IAB [RFC8546] has provided a summary of expected implications of
increased encryption on network functions that use the observable
headers and describe the expected benefits of designs that explicitly
declare protocol-invariant header information that can be used for
this purpose.

2.3. To Understand Transport Protocol Performance

This subsection describes use by the network of exposed transport-
layer headers to understand transport protocol performance and
behaviour.

2.3.1. Using Information Derived from Transport-Layer Headers

Observable transport headers enable explicit measurement and analysis
of protocol performance and detection of network anomalies at any
point along the Internet path. Some operators use passive monitoring
to manage their portion of the Internet by characterising the
performance of link/network segments. Inferences from transport
headers are used to derive performance metrics:

Traffic Rate and Volume:
   Per-application traffic rate and volume measures can be used to
   characterise the traffic that uses a network segment or the
   pattern of network usage. Observing the protocol sequence number
   and packet size offers one way to measure this (e.g., measurements
   observing counters in periodic reports, such as RTCP [RFC3550]

[RFC3711] [RFC4585], or measurements observing protocol sequence
numbers in statistical samples of packet flows or specific control
packets, such as those observed at the start and end of a flow).

Measurements can be per endpoint or for an endpoint aggregate.
These could be used to assess usage or for subscriber billing.

Such measurements can be used to trigger traffic shaping and to
associate QoS support within the network and lower layers. This
can be done with consent and in support of an end user to improve
quality of service or could be used by the network to deprioritise
certain flows without user consent.

The traffic rate and volume can be determined, providing that the
packets belonging to individual flows can be identified, but there
might be no additional information about a flow when the transport
headers cannot be observed.

Loss Rate and Loss Pattern:
   Flow loss rate can be derived (e.g., from transport sequence
   numbers or inferred from observing transport protocol
   interactions) and has been used as a metric for performance
   assessment and to characterise transport behaviour. Network
   operators have used the variation in patterns to detect changes in
   the offered service. Understanding the location and root cause of
   loss can help an operator determine whether this requires
   corrective action.

   There are various causes of loss, including: corruption of link
   frames (e.g., due to interference on a radio link); buffering loss
   (e.g., overflow due to congestion, Active Queue Management (AQM)
   [RFC7567], or inadequate provision following traffic preemption),
   and policing (e.g., traffic management [RFC2475]). Understanding
   flow loss rates requires maintaining the per-flow state (flow
   identification often requires transport-layer information) and
   either observing the increase in sequence numbers in the network
   or transport headers or comparing a per-flow packet counter with
   the number of packets that the flow actually sent. Per-hop loss
   can also sometimes be monitored at the interface level by devices
   on the network path or by using in-situ methods operating over a
   network segment (see Section 3.3).

   The pattern of loss can provide insight into the cause of loss.
   Losses can often occur as bursts, randomly timed events, etc. It
   can also be valuable to understand the conditions under which loss
   occurs. This usually requires relating loss to the traffic
   flowing at a network node or segment at the time of loss.
   Transport header information can help identify cases where loss
   could have been wrongly identified or where the transport did not
   require retransmission of a lost packet.

Throughput and Goodput:
   Throughput is the amount of payload data sent by a flow per time
   interval. Goodput (the subset of throughput consisting of useful
   traffic; see Section 2.5 of [RFC7928] and [RFC5166]) is a measure
   of useful data exchanged. The throughput of a flow can be

determined in the absence of transport header information,
providing that the individual flow can be identified, and the
overhead known. Goodput requires the ability to differentiate
loss and retransmission of packets, for example, by observing
packet sequence numbers in the TCP or RTP headers [RFC3550].

Latency:
    Latency is a key performance metric that impacts application and
    user-perceived response times. It often indirectly impacts
    throughput and flow completion time. This determines the reaction
    time of the transport protocol itself, impacting flow setup,
    congestion control, loss recovery, and other transport mechanisms.
    The observed latency can have many components [Latency]. Of
    these, unnecessary/unwanted queueing in buffers of the network
    devices on the path has often been observed as a significant
    factor [bufferbloat]. Once the cause of unwanted latency has been
    identified, this can often be eliminated.

    To measure latency across a part of a path, an observation point
    [RFC7799] can measure the experienced round-trip time (RTT) by
    using packet sequence numbers and acknowledgements or by observing
    header timestamp information. Such information allows an
    observation point on the network path to determine not only the
    path RTT but also allows measurement of the upstream and
    downstream contribution to the RTT. This could be used to locate
    a source of latency, e.g., by observing cases where the median RTT
    is much greater than the minimum RTT for a part of a path.

    The service offered by network operators can benefit from latency
    information to understand the impact of configuration changes and
    to tune deployed services. Latency metrics are key to evaluating
    and deploying AQM [RFC7567], Diffserv [RFC2474], and Explicit
    Congestion Notification (ECN) [RFC3168] [RFC8087]. Measurements
    could identify excessively large buffers, indicating where to
    deploy or configure AQM. An AQM method is often deployed in
    combination with other techniques, such as scheduling [RFC7567]
    [RFC8290], and although parameter-less methods are desired
    [RFC7567], current methods often require tuning [RFC8290]
    [RFC8289] [RFC8033] because they cannot scale across all possible
    deployment scenarios.

    Latency and round-trip time information can potentially expose
    some information useful for approximate geolocation, as discussed
    in [PAM-RTT].

Variation in Delay:
    Some network applications are sensitive to (small) changes in
    packet timing (jitter). Short- and long-term delay variation can
    impact the latency of a flow and hence the perceived quality of
    applications using a network path. For example, jitter metrics
    are often cited when characterising paths supporting real-time
    traffic. The expected performance of such applications can be
    inferred from a measure of the variation in delay observed along a
    portion of the path [RFC3393] [RFC5481]. The requirements
    resemble those for the measurement of latency.

Flow Reordering:
    Significant packet reordering within a flow can impact time-
    critical applications and can be interpreted as loss by reliable
    transports. Many transport protocol techniques are impacted by
    reordering (e.g., triggering TCP retransmission or rebuffering of
    real-time applications). Packet reordering can occur for many
    reasons, e.g., from equipment design to misconfiguration of
    forwarding rules. Flow identification is often required to avoid
    significant packet misordering (e.g., when using ECMP, or LAG).
    Network tools can detect and measure unwanted/excessive reordering
    and the impact on transport performance.

    There have been initiatives in the IETF transport area to reduce
    the impact of reordering within a transport flow, possibly leading
    to a reduction in the requirements for preserving ordering. These
    have potential to simplify network equipment design as well as the
    potential to improve robustness of the transport service.
    Measurements of reordering can help understand the present level
    of reordering and inform decisions about how to progress new
    mechanisms.

    Techniques for measuring reordering typically observe packet
    sequence numbers. Metrics have been defined that evaluate whether
    a network path has maintained packet order on a packet-by-packet
    basis [RFC4737] [RFC5236]. Some protocols provide in-built
    monitoring and reporting functions. Transport fields in the RTP
    header [RFC3550] [RFC4585] can be observed to derive traffic
    volume measurements and provide information on the progress and
    quality of a session using RTP. Metadata assists in understanding
    the context under which the data was collected, including the
    time, observation point [RFC7799], and way in which metrics were
    accumulated. The RTCP protocol directly reports some of this
    information in a form that can be directly visible by devices on
    the network path.

In some cases, measurements could involve active injection of test
traffic to perform a measurement (see Section 3.4 of [RFC7799]).
However, most operators do not have access to user equipment;
therefore, the point of test is normally different from the transport
endpoint. Injection of test traffic can incur an additional cost in
running such tests (e.g., the implications of capacity tests in a
mobile network segment are obvious). Some active measurements
[RFC7799] (e.g., response under load or particular workloads) perturb
other traffic and could require dedicated access to the network
segment.

Passive measurements (see Section 3.6 of [RFC7799]) can have
advantages in terms of eliminating unproductive test traffic,
reducing the influence of test traffic on the overall traffic mix,
and having the ability to choose the point of observation (see
Section 2.4.1). Measurements can rely on observing packet headers,
which is not possible if those headers are encrypted, but could
utilise information about traffic volumes or patterns of interaction
to deduce metrics.

Passive packet sampling techniques are also often used to scale the

processing involved in observing packets on high-rate links. This
exports only the packet header information of (randomly) selected
packets. Interpretation of the exported information relies on
understanding of the header information. The utility of these
measurements depends on the type of network segment/link and number
of mechanisms used by the network devices. Simple routers are
relatively easy to manage, but a device with more complexity demands
understanding of the choice of many system parameters.

2.3.2. Using Information Derived from Network-Layer Header Fields

Information from the transport header can be used by a multi-field
(MF) classifier as a part of policy framework. Policies are commonly
used for management of the QoS or Quality of Experience (QoE) in
resource-constrained networks or by firewalls to implement access
rules (see also Section 2.2.2 of [RFC8404]). Policies can support
user applications/services or protect against unwanted or lower-
priority traffic (Section 2.4.4).

Transport-layer information can also be explicitly carried in
network-layer header fields that are not encrypted, serving as a
replacement/addition to the exposed transport header information
[RFC8558]. This information can enable a different forwarding
treatment by the devices forming the network path, even when a
transport employs encryption to protect other header information.

On the one hand, the user of a transport that multiplexes multiple
subflows might want to obscure the presence and characteristics of
these subflows. On the other hand, an encrypted transport could set
the network-layer information to indicate the presence of subflows
and to reflect the service requirements of individual subflows.
There are several ways this could be done:

IP Address:
    Applications normally expose the endpoint addresses used in the
    forwarding decisions in network devices. Address and other
    protocol information can be used by an MF classifier to determine
    how traffic is treated [RFC2475] and hence affects the quality of
    experience for a flow. Common issues concerning IP address
    sharing are described in [RFC6269].

Using the IPv6 Network-Layer Flow Label:
    A number of Standards Track and Best Current Practice RFCs (e.g.,
    [RFC8085], [RFC6437], and [RFC6438]) encourage endpoints to set
    the IPv6 Flow Label field of the network-layer header. As per
    [RFC6437], IPv6 source nodes "SHOULD assign each unrelated
    transport connection and application data stream to a new flow."
    A multiplexing transport could choose to use multiple flow labels
    to allow the network to independently forward subflows. [RFC6437]
    provides further guidance on choosing a flow label value, stating
    these "should be chosen such that their bits exhibit a high degree
    of variability" and chosen so that "third parties should be
    unlikely to be able to guess the next value that a source of flow
    labels will choose."

    Once set, a flow label can provide information that can help

inform network-layer queueing and forwarding, including use with IPsec [RFC6294], Equal-Cost Multipath routing, and Link Aggregation [RFC6438].

The choice of how to assign a flow label needs to avoid introducing linkages between flows that a network device could not otherwise observe. Inappropriate use by the transport can have privacy implications (e.g., assigning the same label to two independent flows that ought not to be classified similarly).

Using the Network-Layer Differentiated Services Code Point:
    Applications can expose their delivery expectations to network devices by setting the Differentiated Services Code Point (DSCP) field of IPv4 and IPv6 packets [RFC2474]. For example, WebRTC applications identify different forwarding treatments for individual subflows (audio vs. video) based on the value of the DSCP field [RFC8837]. This provides explicit information to inform network-layer queueing and forwarding, rather than an operator inferring traffic requirements from transport and application headers via a multi-field classifier. Inappropriate use by the transport can have privacy implications (e.g., assigning a different DSCP to a subflow could assist in a network device discovering the traffic pattern used by an application). The field is mutable, i.e., some network devices can be expected to change this field. Since the DSCP value can impact the quality of experience for a flow, observations of service performance have to consider this field when a network path supports differentiated service treatment.

Using Explicit Congestion Notification:
    Explicit Congestion Notification (ECN) [RFC3168] is a transport mechanism that uses the ECN field in the network-layer header. Use of ECN explicitly informs the network layer that a transport is ECN capable and requests ECN treatment of the flow. An ECN-capable transport can offer benefits when used over a path with equipment that implements an AQM method with Congestion Experienced (CE) marking of IP packets [RFC8087], since it can react to congestion without also having to recover from lost packets.

    ECN exposes the presence of congestion. The reception of CE-marked packets can be used to estimate the level of incipient congestion on the upstream portion of the path from the point of observation (Section 2.5 of [RFC8087]). Interpreting the marking behaviour (i.e., assessing congestion and diagnosing faults) requires context from the transport layer, such as path RTT.

    AQM and ECN offer a range of algorithms and configuration options. Tools therefore have to be available to network operators and researchers to understand the implication of configuration choices and transport behaviour as the use of ECN increases and new methods emerge [RFC7567].

Network-Layer Options:
    Network protocols can carry optional headers (see Section 5.1). These can explicitly expose transport header information to on-

path devices operating at the network layer (as discussed further in Section 6).

IPv4 [RFC0791] has provisions for optional header fields. IP routers can examine these headers and are required to ignore IPv4 options that they do not recognise. Many current paths include network devices that forward packets that carry options on a slower processing path. Some network devices (e.g., firewalls) can be (and are) configured to drop these packets [RFC7126]. BCP 186 [RFC7126] provides guidance on how operators should treat IPv4 packets that specify options.

IPv6 can encode optional network-layer information in separate headers that may be placed between the IPv6 header and the upper-layer header [RFC8200] (e.g., the IPv6 Alternate Marking Method [IPV6-ALT-MARK], which can be used to measure packet loss and delay metrics). The Hop-by-Hop Options header, when present, immediately follows the IPv6 header. IPv6 permits this header to be examined by any node along the path if explicitly configured [RFC8200].

Careful use of the network-layer features (e.g., extension headers can; see Section 5) help provide similar information in the case where the network is unable to inspect transport protocol headers.

2.4. To Support Network Operations

Some network operators make use of on-path observations of transport headers to analyse the service offered to the users of a network segment and inform operational practice and can help detect and locate network problems. [RFC8517] gives an operator's perspective about such use.

When observable transport header information is not available, those seeking an understanding of transport behaviour and dynamics might learn to work without that information. Alternatively, they might use more limited measurements combined with pattern inference and other heuristics to infer network behaviour (see Section 2.1.1 of [RFC8404]). Operational practises aimed at inferring transport parameters are out of scope for this document and are only mentioned here to recognise that encryption does not necessarily stop operators from attempting to apply practises that have been used with unencrypted transport headers.

This section discusses topics concerning observation of transport flows, with a focus on transport measurement.

2.4.1. Problem Location

Observations of transport header information can be used to locate the source of problems or to assess the performance of a network segment. Often issues can only be understood in the context of the other flows that share a particular path, particular device configuration, interface port, etc. A simple example is monitoring of a network device that uses a scheduler or active queue management technique [RFC7567], where it could be desirable to understand

whether the algorithms are correctly controlling latency or if
overload protection is working. This implies knowledge of how
traffic is assigned to any subqueues used for flow scheduling but can
require information about how the traffic dynamics impact active
queue management, starvation prevention mechanisms, and circuit
breakers.

Sometimes correlating observations of headers at multiple points
along the path (e.g., at the ingress and egress of a network segment)
allows an observer to determine the contribution of a portion of the
path to an observed metric (e.g., to locate a source of delay,
jitter, loss, reordering, or congestion marking).

2.4.2. Network Planning and Provisioning

Traffic rate and volume measurements are used to help plan deployment
of new equipment and configuration in networks. Data is also
valuable to equipment vendors who want to understand traffic trends
and patterns of usage as inputs to decisions about planning products
and provisioning for new deployments.

Trends in aggregate traffic can be observed and can be related to the
endpoint addresses being used, but when transport header information
is not observable, it might be impossible to correlate patterns in
measurements with changes in transport protocols. This increases the
dependency on other indirect sources of information to inform
planning and provisioning.

2.4.3. Compliance with Congestion Control

The traffic that can be observed by on-path network devices (the
"wire image") is a function of transport protocol design/options,
network use, applications, and user characteristics. In general,
when only a small proportion of the traffic has a specific
(different) characteristic, such traffic seldom leads to operational
concern, although the ability to measure and monitor it is lower.
The desire to understand the traffic and protocol interactions
typically grows as the proportion of traffic increases. The
challenges increase when multiple instances of an evolving protocol
contribute to the traffic that share network capacity.

Operators can manage traffic load (e.g., when the network is severely
overloaded) by deploying rate limiters, traffic shaping, or network
transport circuit breakers [RFC8084]. The information provided by
observing transport headers is a source of data that can help to
inform such mechanisms.

Congestion Control Compliance of Traffic:
    Congestion control is a key transport function [RFC2914]. Many
    network operators implicitly accept that TCP traffic complies with
    a behaviour that is acceptable for the shared Internet. TCP
    algorithms have been continuously improved over decades and have
    reached a level of efficiency and correctness that is difficult to
    match in custom application-layer mechanisms [RFC8085].

    A standards-compliant TCP stack provides congestion control that

is judged safe for use across the Internet. Applications
developed on top of well-designed transports can be expected to
appropriately control their network usage, reacting when the
network experiences congestion, by backing off and reducing the
load placed on the network. This is the normal expected behaviour
for IETF-specified transports (e.g., TCP and SCTP).

Congestion Control Compliance for UDP Traffic:
    UDP provides a minimal message-passing datagram transport that has
    no inherent congestion control mechanisms. Because congestion
    control is critical to the stable operation of the Internet,
    applications and other protocols that choose to use UDP as a
    transport have to employ mechanisms to prevent collapse, avoid
    unacceptable contributions to jitter/latency, and establish an
    acceptable share of capacity with concurrent traffic [RFC8085].

    UDP flows that expose a well-known header can be observed to gain
    understanding of the dynamics of a flow and its congestion control
    behaviour. For example, tools exist to monitor various aspects of
    RTP header information and RTCP reports for real-time flows (see
    Section 2.3). The Secure RTP and RTCP extensions [RFC3711] were
    explicitly designed to expose some header information to enable
    such observation while protecting the payload data.

    A network operator can observe the headers of transport protocols
    layered above UDP to understand if the datagram flows comply with
    congestion control expectations. This can help inform a decision
    on whether it might be appropriate to deploy methods, such as rate
    limiters, to enforce acceptable usage. The available information
    determines the level of precision with which flows can be
    classified and the design space for conditioning mechanisms (e.g.,
    rate-limiting, circuit breaker techniques [RFC8084], or blocking
    uncharacterised traffic) [RFC5218].

When anomalies are detected, tools can interpret the transport header
information to help understand the impact of specific transport
protocols (or protocol mechanisms) on the other traffic that shares a
network. An observer on the network path can gain an understanding
of the dynamics of a flow and its congestion control behaviour.
Analysing observed flows can help to build confidence that an
application flow backs off its share of the network load under
persistent congestion and hence to understand whether the behaviour
is appropriate for sharing limited network capacity. For example, it
is common to visualise plots of TCP sequence numbers versus time for
a flow to understand how a flow shares available capacity, deduce its
dynamics in response to congestion, etc.

The ability to identify sources and flows that contribute to
persistent congestion is important to the safe operation of network
infrastructure and can inform configuration of network devices to
complement the endpoint congestion avoidance mechanisms [RFC7567]
[RFC8084] to avoid a portion of the network being driven into
congestion collapse [RFC2914].

2.4.4. To Characterise "Unknown" Network Traffic

The patterns and types of traffic that share Internet capacity change
over time as networked applications, usage patterns, and protocols
continue to evolve.

Encryption can increase the volume of "unknown" or "uncharacterised"
traffic seen by the network. If these traffic patterns form a small
part of the traffic aggregate passing through a network device or
segment of the network path, the dynamics of the uncharacterised
traffic might not have a significant collateral impact on the
performance of other traffic that shares this network segment. Once
the proportion of this traffic increases, monitoring the traffic can
determine if appropriate safety measures have to be put in place.

Tracking the impact of new mechanisms and protocols requires traffic
volume to be measured and new transport behaviours to be identified.
This is especially true of protocols operating over a UDP substrate.
The level and style of encryption needs to be considered in
determining how this activity is performed.

Traffic that cannot be classified typically receives a default
treatment. Some networks block or rate-limit traffic that cannot be
classified.

2.4.5. To Support Network Security Functions

On-path observation of the transport headers of packets can be used
for various security functions. For example, Denial of Service (DoS)
and Distributed DoS (DDoS) attacks against the infrastructure or
against an endpoint can be detected and mitigated by characterising
anomalous traffic (see Section 2.4.4) on a shorter timescale. Other
uses include support for security audits (e.g., verifying the
compliance with cipher suites), client and application fingerprinting
for inventory, and alerts provided for network intrusion detection
and other next generation firewall functions.

When using an encrypted transport, endpoints can directly provide
information to support these security functions. Another method, if
the endpoints do not provide this information, is to use an on-path
network device that relies on pattern inferences in the traffic and
heuristics or machine learning instead of processing observed header
information. An endpoint could also explicitly cooperate with an on-
path device (e.g., a QUIC endpoint could share information about
current uses of connection IDs).

2.4.6. Network Diagnostics and Troubleshooting

Operators monitor the health of a network segment to support a
variety of operational tasks [RFC8404], including procedures to
provide early warning and trigger action, e.g., to diagnose network
problems, to manage security threats (including DoS), to evaluate
equipment or protocol performance, or to respond to user performance
questions. Information about transport flows can assist in setting
buffer sizes and help identify whether link/network tuning is
effective. Information can also support debugging and diagnosis of
the root causes of faults that concern a particular user's traffic
and can support postmortem investigation after an anomaly. Sections

3.1.2 and 5 of [RFC8404] provide further examples.

Network segments vary in their complexity. The design trade-offs for
radio networks are often very different from those of wired networks
[RFC8462]. A radio-based network (e.g., cellular mobile, enterprise
Wireless LAN (WLAN), satellite access/backhaul, point-to-point radio)
adds a subsystem that performs radio resource management, with impact
on the available capacity and potentially loss/reordering of packets.
This impact can differ by traffic type and can be correlated with
link propagation and interference. These can impact the cost and
performance of a provided service and is expected to increase in
importance as operators bring together heterogeneous types of network
equipment and deploy opportunistic methods to access a shared radio
spectrum.

2.4.7. Tooling and Network Operations

A variety of open source and proprietary tools have been deployed
that use the transport header information observable with widely used
protocols, such as TCP or RTP/UDP/IP. Tools that dissect network
traffic flows can alert to potential problems that are hard to derive
from volume measurements, link statistics, or device measurements
alone.

Any introduction of a new transport protocol, protocol feature, or
application might require changes to such tools and could impact
operational practice and policies. Such changes have associated
costs that are incurred by the network operators that need to update
their tooling or develop alternative practises that work without
access to the changed/removed information.

The use of encryption has the desirable effect of preventing
unintended observation of the payload data, and these tools seldom
seek to observe the payload or other application details. A flow
that hides its transport header information could imply "don't touch"
to some operators. This might limit a trouble-shooting response to
"can't help, no trouble found".

An alternative that does not require access to an observable
transport headers is to access endpoint diagnostic tools or to
include user involvement in diagnosing and troubleshooting unusual
use cases or to troubleshoot nontrivial problems. Another approach
is to use traffic pattern analysis. Such tools can provide useful
information during network anomalies (e.g., detecting significant
reordering, high or intermittent loss); however, indirect
measurements need to be carefully designed to provide information for
diagnostics and troubleshooting.

If new protocols, or protocol extensions, are made to closely
resemble or match existing mechanisms, then the changes to tooling
and the associated costs can be small. Equally, more extensive
changes to the transport tend to require more extensive, and more
expensive, changes to tooling and operational practice. Protocol
designers can mitigate these costs by explicitly choosing to expose
selected information as invariants that are guaranteed not to change
for a particular protocol (e.g., the header invariants and the spin

bit in QUIC [RFC9000]). Specification of common log formats and
development of alternative approaches can also help mitigate the
costs of transport changes.

2.5. To Mitigate the Effects of Constrained Networks

Some link and network segments are constrained by the capacity they
can offer by the time it takes to access capacity (e.g., due to
underlying radio resource management methods) or by asymmetries in
the design (e.g., many link are designed so that the capacity
available is different in the forward and return directions; some
radio technologies have different access methods in the forward and
return directions resulting from differences in the power budget).

The impact of path constraints can be mitigated using a proxy
operating at or above the transport layer to use an alternate
transport protocol.

In many cases, one or both endpoints are unaware of the
characteristics of the constraining link or network segment, and
mitigations are applied below the transport layer. Packet
classification and QoS methods (described in various sections) can be
beneficial in differentially prioritising certain traffic when there
is a capacity constraint or additional delay in scheduling link
transmissions. Another common mitigation is to apply header
compression over the specific link or subnetwork (see Section 2.5.1).

2.5.1. To Provide Header Compression

Header compression saves link capacity by compressing network and
transport protocol headers on a per-hop basis. This has been widely
used with low bandwidth dial-up access links and still finds
application on wireless links that are subject to capacity
constraints. These methods are effective for bit-congestive links
sending small packets (e.g., reducing the cost for sending control
packets or small data packets over radio links).

Examples of header compression include use with TCP/IP and RTP/UDP/IP
flows [RFC2507] [RFC6846] [RFC2508] [RFC5795] [RFC8724]. Successful
compression depends on observing the transport headers and
understanding the way fields change between packets and is hence
incompatible with header encryption. Devices that compress transport
headers are dependent on a stable header format, implying
ossification of that format.

Introducing a new transport protocol, or changing the format of the
transport header information, will limit the effectiveness of header
compression until the network devices are updated. Encrypting the
transport protocol headers will tend to cause the header compression
to fall back to compressing only the network-layer headers, with a
significant reduction in efficiency. This can limit connectivity if
the resulting flow exceeds the link capacity or if the packets are
dropped because they exceed the link Maximum Transmission Unit (MTU).

The Secure RTP (SRTP) extensions [RFC3711] were explicitly designed
to leave the transport protocol headers unencrypted, but

authenticated, since support for header compression was considered important.

2.6. To Verify SLA Compliance

Observable transport headers coupled with published transport specifications allow operators and regulators to explore and verify compliance with Service Level Agreements (SLAs). It can also be used to understand whether a service is providing differential treatment to certain flows.

When transport header information cannot be observed, other methods have to be found to confirm that the traffic produced conforms to the expectations of the operator or developer.

Independently verifiable performance metrics can be utilised to demonstrate regulatory compliance in some jurisdictions and as a basis for informing design decisions. This can bring assurance to those operating networks, often avoiding deployment of complex techniques that routinely monitor and manage Internet traffic flows (e.g., avoiding the capital and operational costs of deploying flow rate-limiting and network circuit breaker methods [RFC8084]).

3. Research, Development, and Deployment

Research and development of new protocols and mechanisms need to be informed by measurement data (as described in the previous section). Data can also help promote acceptance of proposed standards specifications by the wider community (e.g., as a method to judge the safety for Internet deployment).

Observed data is important to ensure the health of the research and development communities and provides data needed to evaluate new proposals for standardisation. Open standards motivate a desire to include independent observation and evaluation of performance and deployment data. Independent data helps compare different methods, judge the level of deployment, and ensure the wider applicability of the results. This is important when considering when a protocol or mechanism should be standardised for use in the general Internet. This, in turn, demands control/understanding about where and when measurement samples are collected. This requires consideration of the methods used to observe information and the appropriate balance between encrypting all and no transport header information.

There can be performance and operational trade-offs in exposing selected information to network tools. This section explores key implications of tools and procedures that observe transport protocols but does not endorse or condemn any specific practises.

3.1. Independent Measurement

Encrypting transport header information has implications on the way network data is collected and analysed. Independent observations by multiple actors is currently used by the transport community to maintain an accurate understanding of the network within transport area working groups, IRTF research groups, and the broader research

community. This is important to be able to provide accountability
and demonstrate that protocols behave as intended; although, when
providing or using such information, it is important to consider the
privacy of the user and their incentive for providing accurate and
detailed information.

Protocols that expose the state of the transport protocol in their
header (e.g., timestamps used to calculate the RTT, packet numbers
used to assess congestion, and requests for retransmission) provide
an incentive for a sending endpoint to provide consistent
information, because a protocol will not work otherwise. An on-path
observer can have confidence that well-known (and ossified) transport
header information represents the actual state of the endpoints when
this information is necessary for the protocol's correct operation.

Encryption of transport header information could reduce the range of
actors that can observe useful data. This would limit the
information sources available to the Internet community to understand
the operation of new transport protocols, reducing information to
inform design decisions and standardisation of the new protocols and
related operational practises. The cooperating dependence of
network, application, and host to provide communication performance
on the Internet is uncertain when only endpoints (i.e., at user
devices and within service platforms) can observe performance and
when performance cannot be independently verified by all parties.

3.2. Measurable Transport Protocols

Transport protocol evolution and the ability to measure and
understand the impact of protocol changes have to proceed hand-in-
hand. A transport protocol that provides observable headers can be
used to provide open and verifiable measurement data. Observation of
pathologies has a critical role in the design of transport protocol
mechanisms and development of new mechanisms and protocols and aides
in understanding the interactions between cooperating protocols and
network mechanisms, the implications of sharing capacity with other
traffic, and the impact of different patterns of usage. The ability
of other stakeholders to review transport header traces helps develop
insight into the performance and the traffic contribution of specific
variants of a protocol.

Development of new transport protocol mechanisms has to consider the
scale of deployment and the range of environments in which the
transport is used. Experience has shown that it is often difficult
to correctly implement new mechanisms [RFC8085] and that mechanisms
often evolve as a protocol matures or in response to changes in
network conditions, in network traffic, or to application usage.
Analysis is especially valuable when based on the behaviour
experienced across a range of topologies, vendor equipment, and
traffic patterns.

Encryption enables a transport protocol to choose which internal
state to reveal to devices on the network path, what information to
encrypt, and what fields to grease [RFC8701]. A new design can
provide summary information regarding its performance, congestion
control state, etc., or make explicit measurement information

available. For example, [RFC9000] specifies a way for a QUIC
endpoint to optionally set the spin bit to explicitly reveal the RTT
of an encrypted transport session to the on-path network devices.
There is a choice of what information to expose. For some
operational uses, the information has to contain sufficient detail to
understand, and possibly reconstruct, the network traffic pattern for
further testing. The interpretation of the information needs to
consider whether this information reflects the actual transport state
of the endpoints. This might require the trust of transport protocol
implementers to correctly reveal the desired information.

New transport protocol formats are expected to facilitate an
increased pace of transport evolution and with it the possibility to
experiment with and deploy a wide range of protocol mechanisms. At
the time of writing, there has been interest in a wide range of new
transport methods, e.g., larger initial window, Proportional Rate
Reduction (PRR), congestion control methods based on measuring
bottleneck bandwidth and round-trip propagation time, the
introduction of AQM techniques, and new forms of ECN response (e.g.,
Data Centre TCP, DCTCP, and methods proposed for Low Latency Low Loss
Scalable throughput (L4S)). The growth and diversity of applications
and protocols using the Internet also continues to expand. For each
new method or application, it is desirable to build a body of data
reflecting its behaviour under a wide range of deployment scenarios,
traffic load, and interactions with other deployed/candidate methods.

3.3. Other Sources of Information

Some measurements that traditionally rely on observable transport
information could be completed by utilising endpoint-based logging
(e.g., based on QUIC trace [Quic-Trace] and qlog [QLOG]). Such
information has a diversity of uses, including developers wishing to
debug/understand the transport/application protocols with which they
work, researchers seeking to spot trends and anomalies, and to
characterise variants of protocols. A standard format for endpoint
logging could allow these to be shared (after appropriate
anonymisation) to understand performance and pathologies.

When measurement datasets are made available by servers or client
endpoints, additional metadata, such as the state of the network and
conditions in which the system was observed, is often necessary to
interpret this data to answer questions about network performance or
understand a pathology. Collecting and coordinating such metadata is
more difficult when the observation point is at a different location
to the bottleneck or device under evaluation [RFC7799].

Despite being applicable in some scenarios, endpoint logs do not
provide equivalent information to on-path measurements made by
devices in the network. In particular, endpoint logs contain only a
part of the information to understand the operation of network
devices and identify issues, such as link performance or capacity
sharing between multiple flows. An analysis can require coordination
between actors at different layers to successfully characterise flows
and correlate the performance or behaviour of a specific mechanism
with an equipment configuration and traffic using operational
equipment along a network path (e.g., combining transport and network

measurements to explore congestion control dynamics to understand the
implications of traffic on designs for active queue management or
circuit breakers).

Another source of information could arise from Operations,
Administration, and Maintenance (OAM) (see Section 6). Information
data records could be embedded into header information at different
layers to support functions, such as performance evaluation, path
tracing, path verification information, classification, and a
diversity of other uses.

In-situ OAM (IOAM) data fields [IOAM-DATA] can be encapsulated into a
variety of protocols to record operational and telemetry information
in an existing packet while that packet traverses a part of the path
between two points in a network (e.g., within a particular IOAM
management domain). IOAM-Data-Fields are independent from the
protocols into which IOAM-Data-Fields are encapsulated. For example,
IOAM can provide proof that a traffic flow takes a predefined path,
SLA verification for the live data traffic, and statistics relating
to traffic distribution.

4. Encryption and Authentication of Transport Headers

    There are several motivations for transport header encryption.

    One motive to encrypt transport headers is to prevent network
    ossification from network devices that inspect well-known transport
    headers. Once a network device observes a transport header and
    becomes reliant upon using it, the overall use of that field can
    become ossified, preventing new versions of the protocol and
    mechanisms from being deployed. Examples include:

    * During the development of TLS 1.3 [RFC8446], the design needed to
       function in the presence of deployed middleboxes that relied on
       the presence of certain header fields exposed in TLS 1.2
       [RFC5426].

    * The design of Multipath TCP (MPTCP) [RFC8684] had to account for
       middleboxes (known as "TCP Normalizers") that monitor the
       evolution of the window advertised in the TCP header and then
       reset connections when the window did not grow as expected.

    * TCP Fast Open [RFC7413] can experience problems due to middleboxes
       that modify the transport header of packets by removing "unknown"
       TCP options. Segments with unrecognised TCP options can be
       dropped, segments that contain data and set the SYN bit can be
       dropped, and some middleboxes that disrupt connections can send
       data before completion of the three-way handshake.

    * Other examples of TCP ossification have included middleboxes that
       modify transport headers by rewriting TCP sequence and
       acknowledgement numbers but are unaware of the (newer) TCP
       selective acknowledgement (SACK) option and therefore fail to
       correctly rewrite the SACK information to match the changes made
       to the fixed TCP header, preventing correct SACK operation.

In all these cases, middleboxes with a hard-coded, but incomplete, understanding of a specific transport behaviour (i.e., TCP) interacted poorly with transport protocols after the transport behaviour was changed. In some cases, the middleboxes modified or replaced information in the transport protocol header.

Transport header encryption prevents an on-path device from observing the transport headers and therefore stops ossified mechanisms being used that directly rely on or infer semantics of the transport header information. This encryption is normally combined with authentication of the protected information. [RFC8546] summarises this approach, stating that "[t]he wire image, not the protocol's specification, determines how third parties on the network paths among protocol participants will interact with that protocol" (Section 1 of [RFC8546]), and it can be expected that header information that is not encrypted will become ossified.

Encryption does not itself prevent ossification of the network service. People seeking to understand or classify network traffic could still come to rely on pattern inferences and other heuristics or machine learning to derive measurement data and as the basis for network forwarding decisions [RFC8546]. This can also create dependencies on the transport protocol or the patterns of traffic it can generate, also resulting in ossification of the service.

Another motivation for using transport header encryption is to improve privacy and to decrease opportunities for surveillance. Users value the ability to protect their identity and location and defend against analysis of the traffic. Revelations about the use of pervasive surveillance [RFC7624] have, to some extent, eroded trust in the service offered by network operators and have led to an increased use of encryption. Concerns have also been voiced about the addition of metadata to packets by third parties to provide analytics, customisation, advertising, cross-site tracking of users, customer billing, or selectively allowing or blocking content.

Whatever the reasons, the IETF is designing protocols that include transport header encryption (e.g., QUIC [RFC9000]) to supplement the already widespread payload encryption and to further limit exposure of transport metadata to the network.

If a transport protocol uses header encryption, the designers have to decide whether to encrypt all or a part of the transport-layer information. Section 4 of [RFC8558] states, "Anything exposed to the path should be done with the intent that it be used by the network elements on the path."

Certain transport header fields can be made observable to on-path network devices or can define new fields designed to explicitly expose observable transport-layer information to the network. Where exposed fields are intended to be immutable (i.e., can be observed but not modified by a network device), the endpoints are encouraged to use authentication to provide a cryptographic integrity check that can detect if these immutable fields have been modified by network devices. Authentication can help to prevent attacks that rely on sending packets that fake exposed control signals in transport

headers (e.g., TCP RST spoofing). Making a part of a transport
header observable or exposing new header fields can lead to
ossification of that part of a header as network devices come to rely
on observations of the exposed fields.

The use of transport header authentication and encryption therefore
exposes a tussle between middlebox vendors, operators, researchers,
applications developers, and end users:

*   On the one hand, future Internet protocols that support transport
    header encryption assist in the restoration of the end-to-end
    nature of the Internet by returning complex processing to the
    endpoints. Since middleboxes cannot modify what they cannot see,
    the use of transport header encryption can improve application and
    end-user privacy by reducing leakage of transport metadata to
    operators that deploy middleboxes.

*   On the other hand, encryption of transport-layer information has
    implications for network operators and researchers seeking to
    understand the dynamics of protocols and traffic patterns, since
    it reduces the information that is available to them.

The following briefly reviews some security design options for
transport protocols. "A Survey of the Interaction between Security
Protocols and Transport Services" [RFC8922] provides more details
concerning commonly used encryption methods at the transport layer.

Security work typically employs a design technique that seeks to
expose only what is needed [RFC3552]. This approach provides
incentives to not reveal any information that is not necessary for
the end-to-end communication. The IETF has provided guidelines for
writing security considerations for IETF specifications [RFC3552].

Endpoint design choices impacting privacy also need to be considered
as a part of the design process [RFC6973]. The IAB has provided
guidance for analysing and documenting privacy considerations within
IETF specifications [RFC6973].

Authenticating the Transport Protocol Header:
    Transport-layer header information can be authenticated. An
    example transport authentication mechanism is TCP Authentication
    Option (TCP-AO) [RFC5925]. This TCP option authenticates the IP
    pseudo-header, TCP header, and TCP data. TCP-AO protects the
    transport layer, preventing attacks from disabling the TCP
    connection itself and provides replay protection. Such
    authentication might interact with middleboxes, depending on their
    behaviour [RFC3234].

    The IPsec Authentication Header (AH) [RFC4302] was designed to
    work at the network layer and authenticate the IP payload. This
    approach authenticates all transport headers and verifies their
    integrity at the receiver, preventing modification by network
    devices on the path. The IPsec Encapsulating Security Payload
    (ESP) [RFC4303] can also provide authentication and integrity
    without confidentiality using the NULL encryption algorithm
    [RFC2410]. SRTP [RFC3711] is another example of a transport

protocol that allows header authentication.

Integrity Check:
    Transport protocols usually employ integrity checks on the
    transport header information. Security methods usually employ
    stronger checks and can combine this with authentication. An
    integrity check that protects the immutable transport header
    fields, but can still expose the transport header information in
    the clear, allows on-path network devices to observe these fields.
    An integrity check is not able to prevent modification by network
    devices on the path but can prevent a receiving endpoint from
    accepting changes and avoid impact on the transport protocol
    operation, including some types of attack.

Selectively Encrypting Transport Headers and Payload:
    A transport protocol design that encrypts selected header fields
    allows specific transport header fields to be made observable by
    network devices on the path. This information is explicitly
    exposed either in a transport header field or lower layer protocol
    header. A design that only exposes immutable fields can also
    perform end-to-end authentication of these fields across the path
    to prevent undetected modification of the immutable transport
    headers.

    Mutable fields in the transport header provide opportunities where
    on-path network devices can modify the transport behaviour (e.g.,
    the extended headers described in [PLUS-ABSTRACT-MECH]). An
    example of a method that encrypts some, but not all, transport
    header information is GRE-in-UDP [RFC8086] when used with GRE
    encryption.

Optional Encryption of Header Information:
    There are implications to the use of optional header encryption in
    the design of a transport protocol, where support of optional
    mechanisms can increase the complexity of the protocol and its
    implementation and in the management decisions that have to be
    made to use variable format fields. Instead, fields of a specific
    type ought to be sent with the same level of confidentiality or
    integrity protection.

Greasing:
    Protocols often provide extensibility features, reserving fields
    or values for use by future versions of a specification. The
    specification of receivers has traditionally ignored unspecified
    values; however, on-path network devices have emerged that ossify
    to require a certain value in a field or reuse a field for another
    purpose. When the specification is later updated, it is
    impossible to deploy the new use of the field and forwarding of
    the protocol could even become conditional on a specific header
    field value.

    A protocol can intentionally vary the value, format, and/or
    presence of observable transport header fields at random
    [RFC8701]. This prevents a network device ossifying the use of a
    specific observable field and can ease future deployment of new
    uses of the value or code point. This is not a security

mechanism, although the use can be combined with an authentication mechanism.

Different transports use encryption to protect their header information to varying degrees. The trend is towards increased protection.

5. Intentionally Exposing Transport Information to the Network

A transport protocol can choose to expose certain transport information to on-path devices operating at the network layer by sending observable fields. One approach is to make an explicit choice not to encrypt certain transport header fields, making this transport information observable by an on-path network device. Another approach is to expose transport information in a network-layer extension header (see Section 5.1). Both are examples of explicit information intended to be used by network devices on the path [RFC8558].

Whatever the mechanism used to expose the information, a decision to expose only specific information places the transport endpoint in control of what to expose outside of the encrypted transport header. This decision can then be made independently of the transport protocol functionality. This can be done by exposing part of the transport header or as a network-layer option/extension.

5.1. Exposing Transport Information in Extension Headers

At the network layer, packets can carry optional headers that explicitly expose transport header information to the on-path devices operating at the network layer (Section 2.3.2). For example, an endpoint that sends an IPv6 hop-by-hop option [RFC8200] can provide explicit transport-layer information that can be observed and used by network devices on the path. New hop-by-hop options are not recommended in [RFC8200] "because nodes may be configured to ignore the Hop-by-Hop Options header, drop packets containing a Hop-by-Hop Options header, or assign packets containing a Hop-by-Hop Options header to a slow processing path. Designers considering defining new hop-by-hop options need to be aware of this likely behavior."

Network-layer optional headers explicitly indicate the information that is exposed, whereas use of exposed transport header information first requires an observer to identify the transport protocol and its format. See Section 2.2.

An arbitrary path can include one or more network devices that drop packets that include a specific header or option used for this purpose (see [RFC7872]). This could impact the proper functioning of the protocols using the path. Protocol methods can be designed to probe to discover whether the specific option(s) can be used along the current path, enabling use on arbitrary paths.

5.2. Common Exposed Transport Information

There are opportunities for multiple transport protocols to consistently supply common observable information [RFC8558]. A

common approach can result in an open definition of the observable
fields. This has the potential that the same information can be
utilised across a range of operational and analysis tools.

5.3. Considerations for Exposing Transport Information

   Considerations concerning what information, if any, it is appropriate
   to expose include:

   * On the one hand, explicitly exposing derived fields containing
      relevant transport information (e.g., metrics for loss, latency,
      etc.) can avoid network devices needing to derive this information
      from other header fields. This could result in development and
      evolution of transport-independent tools around a common
      observable header and permit transport protocols to also evolve
      independently of this ossified header [RFC8558].

   * On the other hand, protocols and implementations might be designed
      to avoid consistently exposing external information that
      corresponds to the actual internal information used by the
      protocol itself. An endpoint/protocol could choose to expose
      transport header information to optimise the benefit it gets from
      the network [RFC8558]. The value of this information for
      analysing operation of the transport layer would be enhanced if
      the exposed information could be verified to match the transport
      protocol's observed behavior.

   The motivation to include actual transport header information and the
   implications of network devices using this information has to be
   considered when proposing such a method. [RFC8558] summarises this
   as:

   | When signals from endpoints to the path are independent from the
   | signals used by endpoints to manage the flow's state mechanics,
   | they may be falsified by an endpoint without affecting the peer's
   | understanding of the flow's state. For encrypted flows, this
   | divergence is not detectable by on-path devices.

6. Addition of Transport OAM Information to Network-Layer Headers

   Even when the transport headers are encrypted, on-path devices can
   make measurements by utilising additional protocol headers carrying
   OAM information in an additional packet header. OAM information can
   be included with packets to perform functions, such as identification
   of transport protocols and flows, to aide understanding of network or
   transport performance or to support network operations or mitigate
   the effects of specific network segments.

   Using network-layer approaches to reveal information has the
   potential that the same method (and hence same observation and
   analysis tools) can be consistently used by multiple transport
   protocols. This approach also could be applied to methods beyond OAM
   (see Section 5). There can also be less desirable implications from
   separating the operation of the transport protocol from the
   measurement framework.

6.1. Use of OAM within a Maintenance Domain

OAM information can be restricted to a maintenance domain, typically owned and operated by a single entity. OAM information can be added at the ingress to the maintenance domain (e.g., an Ethernet protocol header with timestamps and sequence number information using a method such as 802.11ag or in-situ OAM [IOAM-DATA] or as a part of the encapsulation protocol). This additional header information is not delivered to the endpoints and is typically removed at the egress of the maintenance domain.

Although some types of measurements are supported, this approach does not cover the entire range of measurements described in this document. In some cases, it can be difficult to position measurement tools at the appropriate segments/nodes, and there can be challenges in correlating the downstream/upstream information when in-band OAM data is inserted by an on-path device.

6.2. Use of OAM across Multiple Maintenance Domains

OAM information can also be added at the network layer by the sender as an IPv6 extension header or an IPv4 option or in an encapsulation/ tunnel header that also includes an extension header or option. This information can be used across multiple network segments or between the transport endpoints.

One example is the IPv6 Performance and Diagnostic Metrics (PDM) destination option [RFC8250]. This allows a sender to optionally include a destination option that carries header fields that can be used to observe timestamps and packet sequence numbers. This information could be authenticated by a receiving transport endpoint when the information is added at the sender and visible at the receiving endpoint, although methods to do this have not currently been proposed. This needs to be explicitly enabled at the sender.

7. Conclusions

Header authentication and encryption and strong integrity checks are being incorporated into new transport protocols and have important benefits. The pace of the development of transports using the WebRTC data channel and the rapid deployment of the QUIC transport protocol can both be attributed to using the combination of UDP as a substrate while providing confidentiality and authentication of the encapsulated transport headers and payload.

This document has described some current practises, and the implications for some stakeholders, when transport-layer header encryption is used. It does not judge whether these practises are necessary or endorse the use of any specific practise. Rather, the intent is to highlight operational tools and practises to consider when designing and modifying transport protocols, so protocol designers can make informed choices about what transport header fields to encrypt and whether it might be beneficial to make an explicit choice to expose certain fields to devices on the network path. In making such a decision, it is important to balance:

User Privacy:
   The less transport header information that is exposed to the
   network, the lower the risk of leaking metadata that might have
   user privacy implications. Transports that chose to expose some
   header fields need to make a privacy assessment to understand the
   privacy cost versus benefit trade-off in making that information
   available. The design of the QUIC spin bit to the network is an
   example of such considered analysis.

Transport Ossification:
   Unencrypted transport header fields are likely to ossify rapidly,
   as network devices come to rely on their presence, making it
   difficult to change the transport in future. This argues that the
   choice to expose information to the network is made deliberately
   and with care, since it is essentially defining a stable interface
   between the transport and the network. Some protocols will want
   to make that interface as limited as possible; other protocols
   might find value in exposing certain information to signal to the
   network or in allowing the network to change certain header fields
   as signals to the transport. The visible wire image of a protocol
   should be explicitly designed.

Network Ossification:
   While encryption can reduce ossification of the transport
   protocol, it does not itself prevent ossification of the network
   service. People seeking to understand network traffic could still
   come to rely on pattern inferences and other heuristics or machine
   learning to derive measurement data and as the basis for network
   forwarding decisions [RFC8546]. This creates dependencies on the
   transport protocol or the patterns of traffic it can generate,
   resulting in ossification of the service.

Impact on Operational Practice:
   The network operations community has long relied on being able to
   understand Internet traffic patterns, both in aggregate and at the
   flow level, to support network management, traffic engineering,
   and troubleshooting. Operational practice has developed based on
   the information available from unencrypted transport headers. The
   IETF has supported this practice by developing operations and
   management specifications, interface specifications, and
   associated Best Current Practices. Widespread deployment of
   transport protocols that encrypt their information will impact
   network operations unless operators can develop alternative
   practises that work without access to the transport header.

Pace of Evolution:
   Removing obstacles to change can enable an increased pace of
   evolution. If a protocol changes its transport header format
   (wire image) or its transport behaviour, this can result in the
   currently deployed tools and methods becoming no longer relevant.
   Where this needs to be accompanied by development of appropriate
   operational support functions and procedures, it can incur a cost
   in new tooling to catch up with each change. Protocols that
   consistently expose observable data do not require such
   development but can suffer from ossification and need to consider
   if the exposed protocol metadata has privacy implications. There

is no single deployment context; therefore, designers need to
consider the diversity of operational networks (ISPs, enterprises,
DDoS mitigation and firewall maintainers, etc.).

Supporting Common Specifications:
   Common, open, transport specifications can stimulate engagement by
   developers, users, researchers, and the broader community.
   Increased protocol diversity can be beneficial in meeting new
   requirements, but the ability to innovate without public scrutiny
   risks point solutions that optimise for specific cases and that
   can accidentally disrupt operations of/in different parts of the
   network. The social contract that maintains the stability of the
   Internet relies on accepting common transport specifications and
   on it being possible to detect violations. The existence of
   independent measurements, transparency, and public scrutiny of
   transport protocol behaviour helps the community to enforce the
   social norm that protocol implementations behave fairly and
   conform (at least mostly) to the specifications. It is important
   to find new ways of maintaining that community trust as increased
   use of transport header encryption limits visibility into
   transport behaviour (see also Section 5.3).

Impact on Benchmarking and Understanding Feature Interactions:
   An appropriate vantage point for observation, coupled with timing
   information about traffic flows, provides a valuable tool for
   benchmarking network devices, endpoint stacks, and/or
   configurations. This can help understand complex feature
   interactions. An inability to observe transport header
   information can make it harder to diagnose and explore
   interactions between features at different protocol layers, a side
   effect of not allowing a choice of vantage point from which this
   information is observed. New approaches might have to be
   developed.

Impact on Research and Development:
   Hiding transport header information can impede independent
   research into new mechanisms, measurements of behaviour, and
   development initiatives. Experience shows that transport
   protocols are complicated to design and complex to deploy and that
   individual mechanisms have to be evaluated while considering other
   mechanisms across a broad range of network topologies and with
   attention to the impact on traffic sharing the capacity. If
   increased use of transport header encryption results in reduced
   availability of open data, it could eliminate the independent
   checks to the standardisation process that have previously been in
   place from research and academic contributors (e.g., the role of
   the IRTF Internet Congestion Control Research Group (ICCRG) and
   research publications in reviewing new transport mechanisms and
   assessing the impact of their deployment).

Observable transport header information might be useful to various
stakeholders. Other sets of stakeholders have incentives to limit
what can be observed. This document does not make recommendations
about what information ought to be exposed, to whom it ought to be
observable, or how this will be achieved. There are also design
choices about where observable fields are placed. For example, one

location could be a part of the transport header outside of the
encryption envelope; another alternative is to carry the information
in a network-layer option or extension header. New transport
protocol designs ought to explicitly identify any fields that are
intended to be observed, consider if there are alternative ways of
providing the information, and reflect on the implications of
observable fields being used by on-path network devices and how this
might impact user privacy and protocol evolution when these fields
become ossified.

As [RFC7258] notes, "Making networks unmanageable to mitigate PM is
not an acceptable outcome, but ignoring PM would go against the
consensus documented here." Providing explicit information can help
avoid traffic being inappropriately classified, impacting application
performance. An appropriate balance will emerge over time as real
instances of this tension are analysed [RFC7258]. This balance
between information exposed and information hidden ought to be
carefully considered when specifying new transport protocols.

8. Security Considerations

   This document is about design and deployment considerations for
   transport protocols. Issues relating to security are discussed
   throughout this document.

   Authentication, confidentiality protection, and integrity protection
   are identified as transport features by [RFC8095]. As currently
   deployed in the Internet, these features are generally provided by a
   protocol or layer on top of the transport protocol [RFC8922].

   Confidentiality and strong integrity checks have properties that can
   also be incorporated into the design of a transport protocol or to
   modify an existing transport. Integrity checks can protect an
   endpoint from undetected modification of protocol fields by on-path
   network devices, whereas encryption and obfuscation or greasing can
   further prevent these headers being utilised by network devices
   [RFC8701]. Preventing observation of headers provides an opportunity
   for greater freedom to update the protocols and can ease
   experimentation with new techniques and their final deployment in
   endpoints. A protocol specification needs to weigh the costs of
   ossifying common headers versus the potential benefits of exposing
   specific information that could be observed along the network path to
   provide tools to manage new variants of protocols.

   Header encryption can provide confidentiality of some or all of the
   transport header information. This prevents an on-path device from
   gaining knowledge of the header field. It therefore prevents
   mechanisms being built that directly rely on the information or seeks
   to infer semantics of an exposed header field. Reduced visibility
   into transport metadata can limit the ability to measure and
   characterise traffic and conversely can provide privacy benefits.

   Extending the transport payload security context to also include the
   transport protocol header protects both types of information with the
   same key. A privacy concern would arise if this key was shared with
   a third party, e.g., providing access to transport header information

to debug a performance issue would also result in exposing the transport payload data to the same third party. Such risks would be mitigated using a layered security design that provides one domain of protection and associated keys for the transport payload and encrypted transport headers and a separate domain of protection and associated keys for any observable transport header fields.

Exposed transport headers are sometimes utilised as a part of the information to detect anomalies in network traffic. As stated in [RFC7258], "While PM is an attack, other forms of monitoring that might fit the definition of PM can be beneficial and not part of any attack, e.g., network management functions monitor packets or flows and anti-spam mechanisms need to see mail message content." This can be used as the first line of defence to identify potential threats from DoS or malware and redirect suspect traffic to dedicated nodes responsible for DoS analysis, for malware detection, or to perform packet "scrubbing" (the normalisation of packets so that there are no ambiguities in interpretation by the ultimate destination of the packet). These techniques are currently used by some operators to also defend from distributed DoS attacks.

Exposed transport header fields can also form a part of the information used by the receiver of a transport protocol to protect the transport layer from data injection by an attacker. In evaluating this use of exposed header information, it is important to consider whether it introduces a significant DoS threat. For example, an attacker could construct a DoS attack by sending packets with a sequence number that falls within the currently accepted range of sequence numbers at the receiving endpoint. This would then introduce additional work at the receiving endpoint, even though the data in the attacking packet might not finally be delivered by the transport layer. This is sometimes known as a "shadowing attack". An attack can, for example, disrupt receiver processing, trigger loss and retransmission, or make a receiving endpoint perform unproductive decryption of packets that cannot be successfully decrypted (forcing a receiver to commit decryption resources, or to update and then restore protocol state).

One mitigation to off-path attacks is to deny knowledge of what header information is accepted by a receiver or obfuscate the accepted header information, e.g., setting a nonpredictable initial value for a sequence number during a protocol handshake, as in [RFC3550] and [RFC6056], or a port value that cannot be predicted (see Section 5.1 of [RFC8085]). A receiver could also require additional information to be used as a part of a validation check before accepting packets at the transport layer, e.g., utilising a part of the sequence number space that is encrypted or by verifying an encrypted token not visible to an attacker. This would also mitigate against on-path attacks. An additional processing cost can be incurred when decryption is attempted before a receiver discards an injected packet.

The existence of open transport protocol standards and a research and operations community with a history of independent observation and evaluation of performance data encourage fairness and conformance to those standards. This suggests careful consideration will be made

over where, and when, measurement samples are collected. An
appropriate balance between encrypting some or all of the transport
header information needs to be considered. Open data and
accessibility to tools that can help understand trends in application
deployment, network traffic, and usage patterns can all contribute to
understanding security challenges.

The security and privacy considerations in "A Framework for Large-
Scale Measurement of Broadband Performance (LMAP)" [RFC7594] contain
considerations for Active and Passive measurement techniques and
supporting material on measurement context.

Addition of observable transport information to the path increases
the information available to an observer and may, when this
information can be linked to a node or user, reduce the privacy of
the user. See the security considerations of [RFC8558].

9. IANA Considerations

This document has no IANA actions.

10. Informative References

[bufferbloat]
           Gettys, J. and K. Nichols, "Bufferbloat: Dark Buffers in
           the Internet", Communications of the ACM, Vol. 55, no. 1,
           pp. 57-65, DOI 10.1145/2063176.2063196, January 2012,
           <https://doi.org/10.1145/2063176.2063196>.

[DTLS]   Rescorla, E., Tschofenig, H., and N. Modadugu, "The
           Datagram Transport Layer Security (DTLS) Protocol Version
           1.3", Work in Progress, Internet-Draft, draft-ietf-tls-
           dtls13-43, 30 April 2021,
           <https://datatracker.ietf.org/doc/html/draft-ietf-tls-
           dtls13-43>.

[IOAM-DATA]
           Brockners, F., Bhandari, S., and T. Mizrahi, "Data Fields
           for In-situ OAM", Work in Progress, Internet-Draft, draft-
           ietf-ippm-ioam-data-12, 21 February 2021,
           <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-
           ioam-data-12>.

[IPV6-ALT-MARK]
           Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R.
           Pang, "IPv6 Application of the Alternate Marking Method",
           Work in Progress, Internet-Draft, draft-ietf-6man-ipv6-
           alt-mark-06, 31 May 2021,
           <https://datatracker.ietf.org/doc/html/draft-ietf-6man-
           ipv6-alt-mark-06>.

[Latency] Briscoe, B., Brunstrom, A., Petlund, A., Hayes, D., Ros,
           D., Tsang, I., Gjessing, S., Fairhurst, G., Griwodz, C.,
           and M. Welzl, "Reducing Internet Latency: A Survey of
           Techniques and Their Merits", IEEE Communications Surveys
           & Tutorials, vol. 18, no. 3, pp. 2149-2196, thirdquarter

                    2016, DOI 10.1109/COMST.2014.2375213, November 2014,
                    <https://doi.org/10.1109/COMST.2014.2375213>.

[Measurement]
                    Fairhurst, G., Kuehlewind, M., and D. Lopez, "Measurement-
                    based Protocol Design", European Conference on Networks
                    and Communications, Oulu, Finland., June 2017.

[PAM-RTT]   Trammell, B. and M. Kuehlewind, "Revisiting the Privacy
                    Implications of Two-Way Internet Latency Data", Passive
                    and Active Measurement, March 2018.

[PLUS-ABSTRACT-MECH]
                    Trammell, B., "Abstract Mechanisms for a Cooperative Path
                    Layer under Endpoint Control", Work in Progress, Internet-
                    Draft, draft-trammell-plus-abstract-mech-00, 28 September
                    2016, <https://datatracker.ietf.org/doc/html/draft-
                    trammell-plus-abstract-mech-00>.

[QLOG]   Marx, R., Niccolini, L., and M. Seemann, "Main logging
                    schema for qlog", Work in Progress, Internet-Draft, draft-
                    ietf-quic-qlog-main-schema-00, 10 June 2021,
                    <https://datatracker.ietf.org/doc/html/draft-ietf-quic-
                    qlog-main-schema-00>.

[Quic-Trace]
                    "QUIC trace utilities", Commit 413c3a4,
                    <https://github.com/google/quic-trace>.

[RFC0791]   Postel, J., "Internet Protocol", STD 5, RFC 791,
                    DOI 10.17487/RFC0791, September 1981,
                    <https://www.rfc-editor.org/info/rfc791>.

[RFC2410]   Glenn, R. and S. Kent, "The NULL Encryption Algorithm and
                    Its Use With IPsec", RFC 2410, DOI 10.17487/RFC2410,
                    November 1998, <https://www.rfc-editor.org/info/rfc2410>.

[RFC2474]   Nichols, K., Blake, S., Baker, F., and D. Black,
                    "Definition of the Differentiated Services Field (DS
                    Field) in the IPv4 and IPv6 Headers", RFC 2474,
                    DOI 10.17487/RFC2474, December 1998,
                    <https://www.rfc-editor.org/info/rfc2474>.

[RFC2475]   Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z.,
                    and W. Weiss, "An Architecture for Differentiated
                    Services", RFC 2475, DOI 10.17487/RFC2475, December 1998,
                    <https://www.rfc-editor.org/info/rfc2475>.

[RFC2507]   Degermark, M., Nordgren, B., and S. Pink, "IP Header
                    Compression", RFC 2507, DOI 10.17487/RFC2507, February
                    1999, <https://www.rfc-editor.org/info/rfc2507>.

[RFC2508]   Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP
                    Headers for Low-Speed Serial Links", RFC 2508,
                    DOI 10.17487/RFC2508, February 1999,
                    <https://www.rfc-editor.org/info/rfc2508>.

[RFC2914] Floyd, S., "Congestion Control Principles", BCP 41,
           RFC 2914, DOI 10.17487/RFC2914, September 2000,
           <https://www.rfc-editor.org/info/rfc2914>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition
           of Explicit Congestion Notification (ECN) to IP",
           RFC 3168, DOI 10.17487/RFC3168, September 2001,
           <https://www.rfc-editor.org/info/rfc3168>.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and
           Issues", RFC 3234, DOI 10.17487/RFC3234, February 2002,
           <https://www.rfc-editor.org/info/rfc3234>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
           A., Peterson, J., Sparks, R., Handley, M., and E.
           Schooler, "SIP: Session Initiation Protocol", RFC 3261,
           DOI 10.17487/RFC3261, June 2002,
           <https://www.rfc-editor.org/info/rfc3261>.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation
           Metric for IP Performance Metrics (IPPM)", RFC 3393,
           DOI 10.17487/RFC3393, November 2002,
           <https://www.rfc-editor.org/info/rfc3393>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V.
           Jacobson, "RTP: A Transport Protocol for Real-Time
           Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550,
           July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC
           Text on Security Considerations", BCP 72, RFC 3552,
           DOI 10.17487/RFC3552, July 2003,
           <https://www.rfc-editor.org/info/rfc3552>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K.
           Norrman, "The Secure Real-time Transport Protocol (SRTP)",
           RFC 3711, DOI 10.17487/RFC3711, March 2004,
           <https://www.rfc-editor.org/info/rfc3711>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302,
           DOI 10.17487/RFC4302, December 2005,
           <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",
           RFC 4303, DOI 10.17487/RFC4303, December 2005,
           <https://www.rfc-editor.org/info/rfc4303>.

[RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey,
           "Extended RTP Profile for Real-time Transport Control
           Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585,
           DOI 10.17487/RFC4585, July 2006,
           <https://www.rfc-editor.org/info/rfc4585>.

[RFC4737] Morton, A., Ciavattone, L., Ramachandran, G., Shalunov,
           S., and J. Perser, "Packet Reordering Metrics", RFC 4737,

                  DOI 10.17487/RFC4737, November 2006,
                  <https://www.rfc-editor.org/info/rfc4737>.

[RFC4960]   Stewart, R., Ed., "Stream Control Transmission Protocol",
            RFC 4960, DOI 10.17487/RFC4960, September 2007,
            <https://www.rfc-editor.org/info/rfc4960>.

[RFC5166]   Floyd, S., Ed., "Metrics for the Evaluation of Congestion
            Control Mechanisms", RFC 5166, DOI 10.17487/RFC5166, March
            2008, <https://www.rfc-editor.org/info/rfc5166>.

[RFC5218]   Thaler, D. and B. Aboba, "What Makes for a Successful
            Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008,
            <https://www.rfc-editor.org/info/rfc5218>.

[RFC5236]   Jayasumana, A., Piratla, N., Banka, T., Bare, A., and R.
            Whitner, "Improved Packet Reordering Metrics", RFC 5236,
            DOI 10.17487/RFC5236, June 2008,
            <https://www.rfc-editor.org/info/rfc5236>.

[RFC5426]   Okmianski, A., "Transmission of Syslog Messages over UDP",
            RFC 5426, DOI 10.17487/RFC5426, March 2009,
            <https://www.rfc-editor.org/info/rfc5426>.

[RFC5481]   Morton, A. and B. Claise, "Packet Delay Variation
            Applicability Statement", RFC 5481, DOI 10.17487/RFC5481,
            March 2009, <https://www.rfc-editor.org/info/rfc5481>.

[RFC5795]   Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust
            Header Compression (ROHC) Framework", RFC 5795,
            DOI 10.17487/RFC5795, March 2010,
            <https://www.rfc-editor.org/info/rfc5795>.

[RFC5925]   Touch, J., Mankin, A., and R. Bonica, "The TCP
            Authentication Option", RFC 5925, DOI 10.17487/RFC5925,
            June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC6056]   Larsen, M. and F. Gont, "Recommendations for Transport-
            Protocol Port Randomization", BCP 156, RFC 6056,
            DOI 10.17487/RFC6056, January 2011,
            <https://www.rfc-editor.org/info/rfc6056>.

[RFC6269]   Ford, M., Ed., Boucadair, M., Durand, A., Levis, P., and
            P. Roberts, "Issues with IP Address Sharing", RFC 6269,
            DOI 10.17487/RFC6269, June 2011,
            <https://www.rfc-editor.org/info/rfc6269>.

[RFC6294]   Hu, Q. and B. Carpenter, "Survey of Proposed Use Cases for
            the IPv6 Flow Label", RFC 6294, DOI 10.17487/RFC6294, June
            2011, <https://www.rfc-editor.org/info/rfc6294>.

[RFC6347]   Rescorla, E. and N. Modadugu, "Datagram Transport Layer
            Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347,
            January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6437]   Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme,

                    "IPv6 Flow Label Specification", RFC 6437,
                    DOI 10.17487/RFC6437, November 2011,
                    <https://www.rfc-editor.org/info/rfc6437>.

[RFC6438]   Carpenter, B. and S. Amante, "Using the IPv6 Flow Label
            for Equal Cost Multipath Routing and Link Aggregation in
            Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011,
            <https://www.rfc-editor.org/info/rfc6438>.

[RFC6846]   Pelletier, G., Sandlund, K., Jonsson, L-E., and M. West,
            "RObust Header Compression (ROHC): A Profile for TCP/IP
            (ROHC-TCP)", RFC 6846, DOI 10.17487/RFC6846, January 2013,
            <https://www.rfc-editor.org/info/rfc6846>.

[RFC6973]   Cooper, A., Tschofenig, H., Aboba, B., Peterson, J.,
            Morris, J., Hansen, M., and R. Smith, "Privacy
            Considerations for Internet Protocols", RFC 6973,
            DOI 10.17487/RFC6973, July 2013,
            <https://www.rfc-editor.org/info/rfc6973>.

[RFC7098]   Carpenter, B., Jiang, S., and W. Tarreau, "Using the IPv6
            Flow Label for Load Balancing in Server Farms", RFC 7098,
            DOI 10.17487/RFC7098, January 2014,
            <https://www.rfc-editor.org/info/rfc7098>.

[RFC7126]   Gont, F., Atkinson, R., and C. Pignataro, "Recommendations
            on Filtering of IPv4 Packets Containing IPv4 Options",
            BCP 186, RFC 7126, DOI 10.17487/RFC7126, February 2014,
            <https://www.rfc-editor.org/info/rfc7126>.

[RFC7258]   Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an
            Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May
            2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7413]   Cheng, Y., Chu, J., Radhakrishnan, S., and A. Jain, "TCP
            Fast Open", RFC 7413, DOI 10.17487/RFC7413, December 2014,
            <https://www.rfc-editor.org/info/rfc7413>.

[RFC7414]   Duke, M., Braden, R., Eddy, W., Blanton, E., and A.
            Zimmermann, "A Roadmap for Transmission Control Protocol
            (TCP) Specification Documents", RFC 7414,
            DOI 10.17487/RFC7414, February 2015,
            <https://www.rfc-editor.org/info/rfc7414>.

[RFC7567]   Baker, F., Ed. and G. Fairhurst, Ed., "IETF
            Recommendations Regarding Active Queue Management",
            BCP 197, RFC 7567, DOI 10.17487/RFC7567, July 2015,
            <https://www.rfc-editor.org/info/rfc7567>.

[RFC7594]   Eardley, P., Morton, A., Bagnulo, M., Burbridge, T.,
            Aitken, P., and A. Akhter, "A Framework for Large-Scale
            Measurement of Broadband Performance (LMAP)", RFC 7594,
            DOI 10.17487/RFC7594, September 2015,
            <https://www.rfc-editor.org/info/rfc7594>.

[RFC7605]   Touch, J., "Recommendations on Using Assigned Transport

                    Port Numbers", BCP 165, RFC 7605, DOI 10.17487/RFC7605,
                    August 2015, <https://www.rfc-editor.org/info/rfc7605>.

[RFC7624]   Barnes, R., Schneier, B., Jennings, C., Hardie, T.,
            Trammell, B., Huitema, C., and D. Borkmann,
            "Confidentiality in the Face of Pervasive Surveillance: A
            Threat Model and Problem Statement", RFC 7624,
            DOI 10.17487/RFC7624, August 2015,
            <https://www.rfc-editor.org/info/rfc7624>.

[RFC7799]   Morton, A., "Active and Passive Metrics and Methods (with
            Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799,
            May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC7872]   Gont, F., Linkova, J., Chown, T., and W. Liu,
            "Observations on the Dropping of Packets with IPv6
            Extension Headers in the Real World", RFC 7872,
            DOI 10.17487/RFC7872, June 2016,
            <https://www.rfc-editor.org/info/rfc7872>.

[RFC7928]   Kuhn, N., Ed., Natarajan, P., Ed., Khademi, N., Ed., and
            D. Ros, "Characterization Guidelines for Active Queue
            Management (AQM)", RFC 7928, DOI 10.17487/RFC7928, July
            2016, <https://www.rfc-editor.org/info/rfc7928>.

[RFC7983]   Petit-Huguenin, M. and G. Salgueiro, "Multiplexing Scheme
            Updates for Secure Real-time Transport Protocol (SRTP)
            Extension for Datagram Transport Layer Security (DTLS)",
            RFC 7983, DOI 10.17487/RFC7983, September 2016,
            <https://www.rfc-editor.org/info/rfc7983>.

[RFC8033]   Pan, R., Natarajan, P., Baker, F., and G. White,
            "Proportional Integral Controller Enhanced (PIE): A
            Lightweight Control Scheme to Address the Bufferbloat
            Problem", RFC 8033, DOI 10.17487/RFC8033, February 2017,
            <https://www.rfc-editor.org/info/rfc8033>.

[RFC8084]   Fairhurst, G., "Network Transport Circuit Breakers",
            BCP 208, RFC 8084, DOI 10.17487/RFC8084, March 2017,
            <https://www.rfc-editor.org/info/rfc8084>.

[RFC8085]   Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage
            Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085,
            March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[RFC8086]   Yong, L., Ed., Crabbe, E., Xu, X., and T. Herbert, "GRE-
            in-UDP Encapsulation", RFC 8086, DOI 10.17487/RFC8086,
            March 2017, <https://www.rfc-editor.org/info/rfc8086>.

[RFC8087]   Fairhurst, G. and M. Welzl, "The Benefits of Using
            Explicit Congestion Notification (ECN)", RFC 8087,
            DOI 10.17487/RFC8087, March 2017,
            <https://www.rfc-editor.org/info/rfc8087>.

[RFC8095]   Fairhurst, G., Ed., Trammell, B., Ed., and M. Kuehlewind,
            Ed., "Services Provided by IETF Transport Protocols and

              Congestion Control Mechanisms", RFC 8095,
              DOI 10.17487/RFC8095, March 2017,
              <https://www.rfc-editor.org/info/rfc8095>.

   [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", STD 86, RFC 8200,
              DOI 10.17487/RFC8200, July 2017,
              <https://www.rfc-editor.org/info/rfc8200>.

   [RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6
              Performance and Diagnostic Metrics (PDM) Destination
              Option", RFC 8250, DOI 10.17487/RFC8250, September 2017,
              <https://www.rfc-editor.org/info/rfc8250>.

   [RFC8289] Nichols, K., Jacobson, V., McGregor, A., Ed., and J.
              Iyengar, Ed., "Controlled Delay Active Queue Management",
              RFC 8289, DOI 10.17487/RFC8289, January 2018,
              <https://www.rfc-editor.org/info/rfc8289>.

   [RFC8290] Hoeiland-Joergensen, T., McKenney, P., Taht, D., Gettys,
              J., and E. Dumazet, "The Flow Queue CoDel Packet Scheduler
              and Active Queue Management Algorithm", RFC 8290,
              DOI 10.17487/RFC8290, January 2018,
              <https://www.rfc-editor.org/info/rfc8290>.

   [RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of
              Pervasive Encryption on Operators", RFC 8404,
              DOI 10.17487/RFC8404, July 2018,
              <https://www.rfc-editor.org/info/rfc8404>.

   [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol
              Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,
              <https://www.rfc-editor.org/info/rfc8446>.

   [RFC8462] Rooney, N. and S. Dawkins, Ed., "Report from the IAB
              Workshop on Managing Radio Networks in an Encrypted World
              (MaRNEW)", RFC 8462, DOI 10.17487/RFC8462, October 2018,
              <https://www.rfc-editor.org/info/rfc8462>.

   [RFC8517] Dolson, D., Ed., Snellman, J., Boucadair, M., Ed., and C.
              Jacquenet, "An Inventory of Transport-Centric Functions
              Provided by Middleboxes: An Operator Perspective",
              RFC 8517, DOI 10.17487/RFC8517, February 2019,
              <https://www.rfc-editor.org/info/rfc8517>.

   [RFC8546] Trammell, B. and M. Kuehlewind, "The Wire Image of a
              Network Protocol", RFC 8546, DOI 10.17487/RFC8546, April
              2019, <https://www.rfc-editor.org/info/rfc8546>.

   [RFC8548] Bittau, A., Giffin, D., Handley, M., Mazieres, D., Slack,
              Q., and E. Smith, "Cryptographic Protection of TCP Streams
              (tcpcrypt)", RFC 8548, DOI 10.17487/RFC8548, May 2019,
              <https://www.rfc-editor.org/info/rfc8548>.

   [RFC8558] Hardie, T., Ed., "Transport Protocol Path Signals",
              RFC 8558, DOI 10.17487/RFC8558, April 2019,

                    <https://www.rfc-editor.org/info/rfc8558>.

[RFC8684]   Ford, A., Raiciu, C., Handley, M., Bonaventure, O., and C.
            Paasch, "TCP Extensions for Multipath Operation with
            Multiple Addresses", RFC 8684, DOI 10.17487/RFC8684, March
            2020, <https://www.rfc-editor.org/info/rfc8684>.

[RFC8701]   Benjamin, D., "Applying Generate Random Extensions And
            Sustain Extensibility (GREASE) to TLS Extensibility",
            RFC 8701, DOI 10.17487/RFC8701, January 2020,
            <https://www.rfc-editor.org/info/rfc8701>.

[RFC8724]   Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC.
            Zúñiga, "SCHC: Generic Framework for Static Context Header
            Compression and Fragmentation", RFC 8724,
            DOI 10.17487/RFC8724, April 2020,
            <https://www.rfc-editor.org/info/rfc8724>.

[RFC8837]   Jones, P., Dhesikan, S., Jennings, C., and D. Druta,
            "Differentiated Services Code Point (DSCP) Packet Markings
            for WebRTC QoS", RFC 8837, DOI 10.17487/RFC8837, January
            2021, <https://www.rfc-editor.org/info/rfc8837>.

[RFC8866]   Begen, A., Kyzivat, P., Perkins, C., and M. Handley, "SDP:
            Session Description Protocol", RFC 8866,
            DOI 10.17487/RFC8866, January 2021,
            <https://www.rfc-editor.org/info/rfc8866>.

[RFC8922]   Enghardt, T., Pauly, T., Perkins, C., Rose, K., and C.
            Wood, "A Survey of the Interaction between Security
            Protocols and Transport Services", RFC 8922,
            DOI 10.17487/RFC8922, October 2020,
            <https://www.rfc-editor.org/info/rfc8922>.

[RFC9000]   Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based
            Multiplexed and Secure Transport", RFC 9000,
            DOI 10.17487/RFC9000, May 2021,
            <https://www.rfc-editor.org/info/rfc9000>.

Acknowledgements

Authors' Addresses

Godred Fairhurst
University of Aberdeen
Department of Engineering
Fraser Noble Building
Aberdeen, Scotland
AB24 3UE
United Kingdom

Email: gorry@erg.abdn.ac.uk
URI: http://www.erg.abdn.ac.uk/

Colin Perkins
University of Glasgow
School of Computing Science
Glasgow, Scotland
G12 8QQ
United Kingdom

Email: csp@csperkins.org
URI: https://csperkins.org/