



REICHMAN JORGENSEN
LEHMAN & FELDBERG LLP

SILICON VALLEY • NEW YORK • ATLANTA • WASHINGTON, D.C.

Patent Owner's Presentation
IPR2023-00923
U.S. Patent No. 7,266,682

Meta Platforms, Inc. v. VL Collective IP LLC
September 10, 2024

Statutory Grounds for Challenges

Ground	Assertion	Petitioned Claims
1	Obvious under § 103 in view of Handley in combination with Basturk	1-21, 23, 25-28
2	Obvious under § 103 in view of PacketCable in combination with Handley	1-28
3	Obvious under § 103 in view of PacketCable in combination with Basturk	1-28
4	Obvious under § 103 in view of Handley in combination with Basturk and PacketCable	22, 24

'682 Patent

Title: Method and System for Transmitting Data from a Transmitter to a Receiver and Transmitter and Receiver Therefor

Inventor: Martin Euchner

Original Assignee: Siemens Aktiengesellschaft

Priority Date: January 18, 2000

US00726682B2

(12) **United States Patent**
Euchner

(10) **Patent No.:** US 7,266,682 B2
(45) **Date of Patent:** Sep. 4, 2007

(54) **METHOD AND SYSTEM FOR TRANSMITTING DATA FROM A TRANSMITTER TO A RECEIVER AND TRANSMITTER AND RECEIVER THEREFOR**

(75) **Inventor:** Martin Euchner, Munich (DE)
(73) **Assignee:** Siemens Aktiengesellschaft, Munich (DE)
(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(h) by 675 days.

(21) **Appl. No.:** 10/181,564
(22) **PCT Filed:** Jan. 5, 2001
(86) **PCT No.:** PCT/DE01/00021
§ 371 (c)(1),
(2), (4) **Date:** Jul. 18, 2002
(87) **PCT Pub. No.:** WO01/54371
PCT Pub. Date: Jul. 26, 2001

(65) **Prior Publication Data**
US 2003/0005284 A1 Jan. 2, 2003

(30) **Foreign Application Priority Data**
Jan. 18, 2000 (DE) 100 01 855

(51) **Int. Cl.** H04L 29/00 (2006.01)
(52) **U.S. Cl.** 713/152; 713/151; 713/161; 713/168
(58) **Field of Classification Search** 713/151-153, 713/160-162, 168, 178; 726/4, 27
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
4,375,097 A * 2/1983 Ulug 370/400
5,345,507 A * 9/1994 Herzberg et al. 380/28
5,602,918 A * 2/1997 Chen et al. 713/153
5,917,830 A * 6/1999 Chen et al. 370/487
6,061,796 A * 5/2000 Chen et al. 726/15
6,158,011 A * 12/2000 Chen et al. 726/15
6,229,821 B1 * 5/2001 Bhargava et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,660 B1 * 12/2001 Patel 713/193
6,366,961 B1 * 4/2002 Subbiah et al. 709/238
6,396,840 B1 * 5/2002 Rose et al. 370/401
6,918,034 B1 * 7/2005 Sengodan et al. 713/160

FOREIGN PATENT DOCUMENTS
WO 99/11019 3/1999

OTHER PUBLICATIONS
Perkins et al., "RTP Payload for Redundant Audio Data", Network Working Group, Sep. 1997, pp. 1-10.*
(Continued)
Primary Examiner—Kambiz Zand
Assistant Examiner—Tongoc Trnn
(74) Attorney, Agent, or Firm—Stuss & Halsey LLP

(57) **ABSTRACT**
Data from a transmitter is extended to include authentication data on the application level by an application protocol. The authentication data is used by the receiver to determine whether the transmitter is known by the receiver. If the transmitter is known by the receiver, the data is accepted. If not, the data is rejected.

28 Claims, 3 Drawing Sheets

```
graph TD
    subgraph Transmitter [308]
        301[Create authentication data on application layer and append the PCUS]
        302[ ]
    end
    subgraph Receiver [307]
        303[Check the authentication data]
        304[Process data]
        305[Reject data]
        306[ ]
    end
    301 --> 302
    302 --> 303
    303 --> 304
    303 --> 305
    304 --> 306
    305 --> 306
```

EX1001 ('682 Patent) at 1; Paper 3 (Petition) at 4; Paper 26 (POR) 2-5



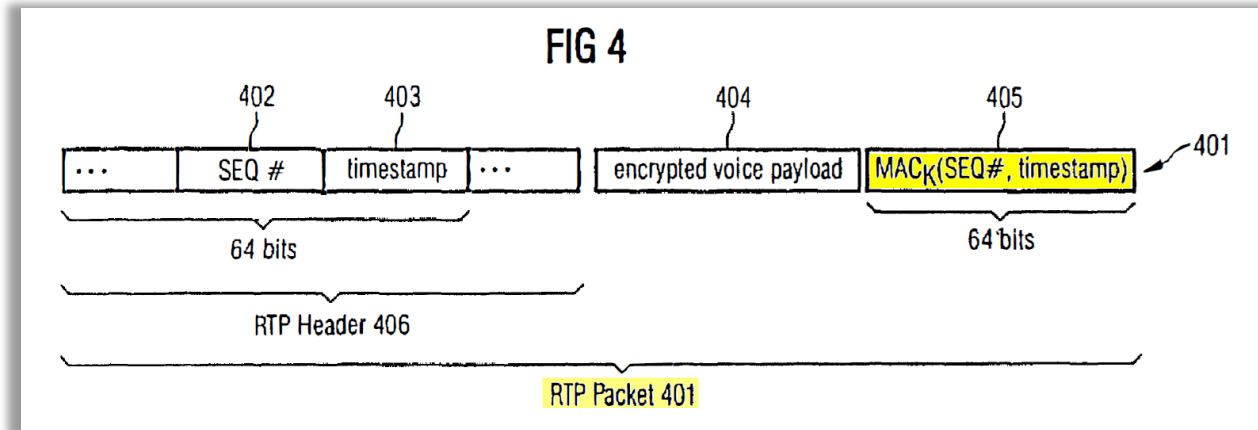
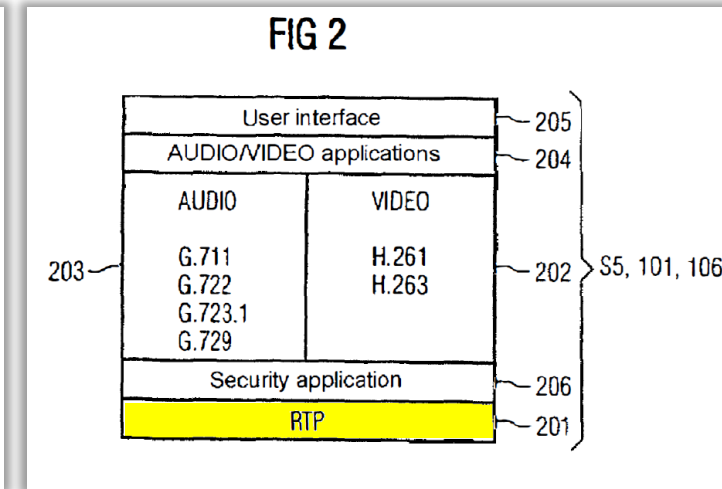
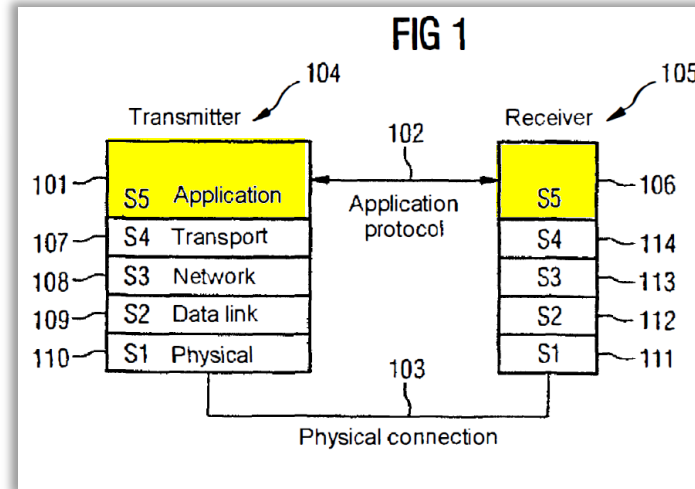
Method and System for Transmitting Data from a Transmitter to a Receiver and Transmitter and Receiver Therefor

1. A method for transmitting data from a transmitter to a receiver, comprising:

providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.



EX1001 ('682 Patent) at Claim 1, Figs. 1-2, 4; Paper 26 (POR) at 3-5

'682 Patent

OVERVIEW OF THE '682 PATENT



The '682 Patent Addresses Problems Related to Real-Time A/V Data Transmission

Security of Real-Time Communication

A communication system is subject to a multiplicity of possible attacks which can target, inter alia, the content of the messages interchanged in the communication system or the availability of the communication system. Taking the example of Internet telephony, then it is firstly important for the content of the telephone conversation not to be able to be monitored by an unauthorized third party, and secondly it is also necessary for the third party not to be able to initiate countless calls, and hence for him not to interfere with the receiver and unnecessarily encumber the communication system. Such attacks are also called denial-of-service attacks. Possible examples of such attacks are mass data or mass messages which are automatically generated and sent to one or more receivers, where they significantly encumber availability and performance. In the Internet telephony example, it is at least unwanted for an Internet telephone to ring incessantly and hence not only to load the network unnecessarily but also to distract the receiver's attention. It is likewise perceived to be disruptive if an attacker interferes with the flow of communication between transmitter and receiver by sending unauthorized voice data.

To fend off attacks on a private communication network, "firewalls" are often used which ensure, in particular, that the private communication network is separated from public networks. However, it is a simple matter for an attacker to send his meaningless (mass) data to addressees within the private network as well, that is to say behind the firewall. There, these data are decoded and possibly reproduced. Thus, the effect achieved by the attacker is that, by way of example, the reproduction of such meaningless data produces nothing but annoying audio interference or noise and hence restricts the bandwidth and availability of the private network. In the extreme case, part or all of the private communication network can even crash.

EX1001 ('682 Patent) at 2:44–3:10; Paper 26 (POR) at 2



The '682 Patent Addresses Problems Related to Real-Time A/V Data Transmission

The “IPSEC” Protocol had flaws

One approach to holding off unwanted data is provided by the IPSEC protocol described S. Kent, R. Atkinson; IP Authentication Header, Internet Engineering Task Force, RFC2402, 1998 and S. Kent, R. Atkinson; IP Encapsulating Security Payload (ESP), Internet Engineering Task Force, RFC2406, 1998. In this case, data packets of the Internet protocol (IP data packets) can be encapsulated and can be protected in terms of confidentiality and/or integrity (implicit sender authentication). In addition, the IPSEC protocol affords a key management method using a “cookie” mechanism (see D. Harkins, D. Carrel, The Internet Key Exchange (IKE), Internet Engineering Task Force, RFC2409, 1998), which can be used to fend off the mass data attacks (denial-of-service attacks) discussed above during the key management phase. The cookie mechanism involves linking fast

ment phase. The cookie mechanism involves linking fast one-way hash functions (e.g. SHA-1), random numbers and IP addresses to one another. However, the first “cookie” transmitted from the transmitter to the receiver is not protected, which results in a security gap. In addition, the IPSEC cookie method is not suitable for ensuring protection against such unwanted mass data on the application layer (for the application protocol) under real-time conditions as well. However, the OSI layer structure means that a drawback for IPSEC is, among other things, that it is not possible to link IPSEC to the security functions of an application layer in this manner.

EX1001 ('682 Patent) at 3:16–41; Paper 26 (POR) at 2-3



The '682 Patent Addresses Problems Related to Real-Time A/V Data Transmission

RTP did not have authentication/integrity features

B. Security Considerations

RTP suffers from the same security liabilities as the underlying protocols. For example, an impostor can fake source or destination network addresses, or change the header or payload. Within RTCP, the CNAME and NAME information may be used to impersonate another participant. In addition, RTP may be sent via IP multicast, which provides no direct means for a sender to know all the receivers of the data sent and therefore no measure of privacy. Rightly or not, users may be more sensitive to privacy concerns with audio and video communication than they have been with more traditional forms of network communication [24]. Therefore, the use of security mechanisms with RTP is important. These mechanisms are discussed in Section 9.

RTP-level translators or mixers may be used to allow RTP traffic to reach hosts behind firewalls. Appropriate firewall security principles and practices, which are beyond the scope of this document, should be followed in the design and installation of these devices and in the admission of RTP applications for use behind the firewall.

EX1008 at 72

9.2 Authentication and Message Integrity

Authentication and message integrity are not defined in the current specification of RTP since these services would not be directly feasible without a key management infrastructure. It is expected that authentication and integrity services will be provided by lower layer protocols in the future.

EX1008 at 50

Paper 26 (POR) at 2-3



The Innovative Technique of the '682 Patent

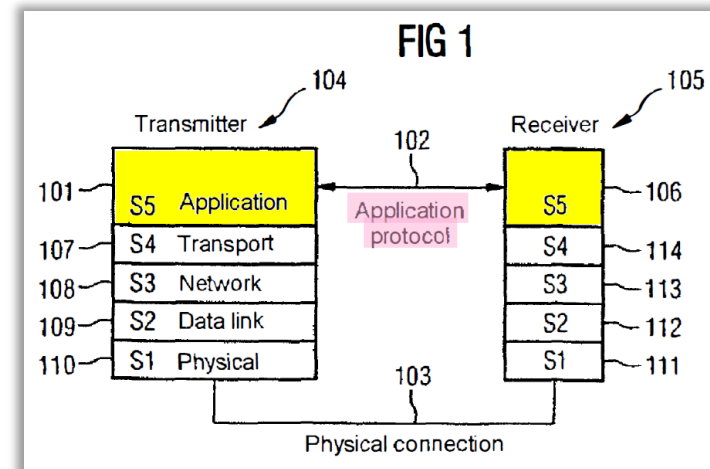
The OSI Model

has a different functionality (in terms of abstraction). In the OSI model, layer 1 corresponds to a physical layer, where data and messages are transmitted from the transmitter to the receiver using a physical protocol. In layer 2, a data link layer is provided, and a data link protocol is used for transmission from layer 2 of the transmitter to layer 2 of the receiver. In a similar manner, layer 3, a network layer, uses a network protocol between transmitter and receiver, and layer 4, a transport layer, uses a transport protocol. In the OSI model, layer 5 corresponds to a session layer using a session protocol, layer 6 corresponds to a presentation layer using a presentation protocol, and layer 7 corresponds to an application layer using an application protocol. In practice, many applications do not always permit exact nomination of strict boundaries specifically between the upper protocol layers, particularly layers 5 to 7. By way of example, within the context of Internet telephony, i.e. use of the telephone service using the medium of the Internet, the three layers above the transport layer 4 combine to form an “application layer” for which, in a similar way to in the implementation above, an “application protocol” is used.

EX1001 ('682 Patent) at 1:19-45

When referring to application layer below, this denotes the layers above the transport layer (layers above 4). The application protocol also denotes the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.

EX1001 ('682 Patent) at 2:6-11



EX1001 ('682 Patent) Fig. 1

Paper 26 (POR) at 4, 14-15

The Innovative Technique of the '682 Patent

Inserting authentication data into RTP packets as an application protocol on an application layer

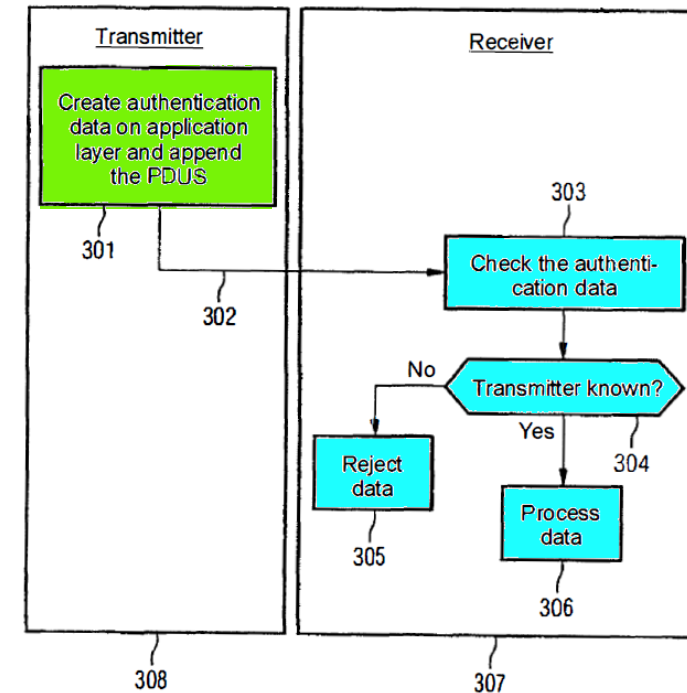
SUMMARY OF THE INVENTION

An object of the invention is to transmit data from a transmitter to a receiver, with the receiver ensuring that the data are not unwanted data arising from a denial-of-service attack, for example.

First, the object is achieved by specifying a method for transmitting data from a transmitter to a receiver, in which the transmitter extends the data by authentication data using an application protocol on the application layer. The authentication data are used by the receiver to ascertain whether it knows the transmitter. If the receiver knows the transmitter, the data are accepted, otherwise the data are rejected.

FIG. 3 is a flowchart for transmitting data from the transmitter 308 to the receiver 307. In block 301, authentication data are produced on the application layer, and the protocol data unit (PDU) relevant to the application protocol is appended. In accordance with the arrangements of the application protocol, the data, including the authentication data, are transmitted to the receiver 307 (see connection 302). This is done using the functionalities or services available under the application protocol. In block 303, the authentication data are checked in the receiver 307 and there is a test (in block 304) to determine whether the transmitter 308 is known to the receiver 307. If this is not the case, the procedure branches to block 305 and the data are rejected. If the transmitter 308 is known to the receiver 307, the procedure branches to block 306 and the data are processed further. The authentication between transmitter and receiver was successful, and the transmitted data are not unwanted mass data.

FIG 3



EX1001 ('682 Patent) at 7:6-23, Fig. 3; Paper 26 (POR) at 3

The Innovative Technique of the '682 Patent

Inserting authentication data into RTP packets as an application protocol on an application layer

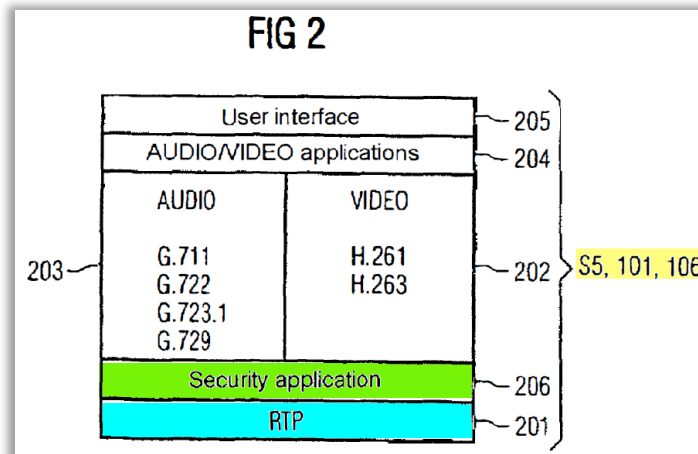
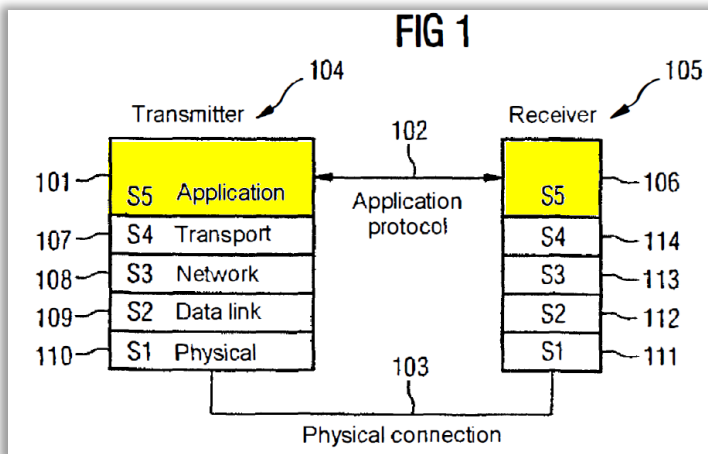


FIG. 2 is a block diagram of an application layer with possible protocols, based on an application concerning the transmission of media data (audio and video data). Thus, 101 and 106 represent the application layer (layer 5) shown in FIG. 1 for the transmitter 104 and the receiver 105. This application layer is in turn divided into a plurality of sublayers. Thus, directly above the layer 4 is the real time transport protocol (RTP) 201. This protocol allows voice and/or picture data to be transmitted in real time from one to possibly a plurality of points (addressees). A layer 206 contains a security application which compiles security functions of the application layer; associated security protocols provide for services such as

- User authentication,
- Access control
- Confidentiality,
- Integrity
- Binding nature of the application data, and
- Accounting.

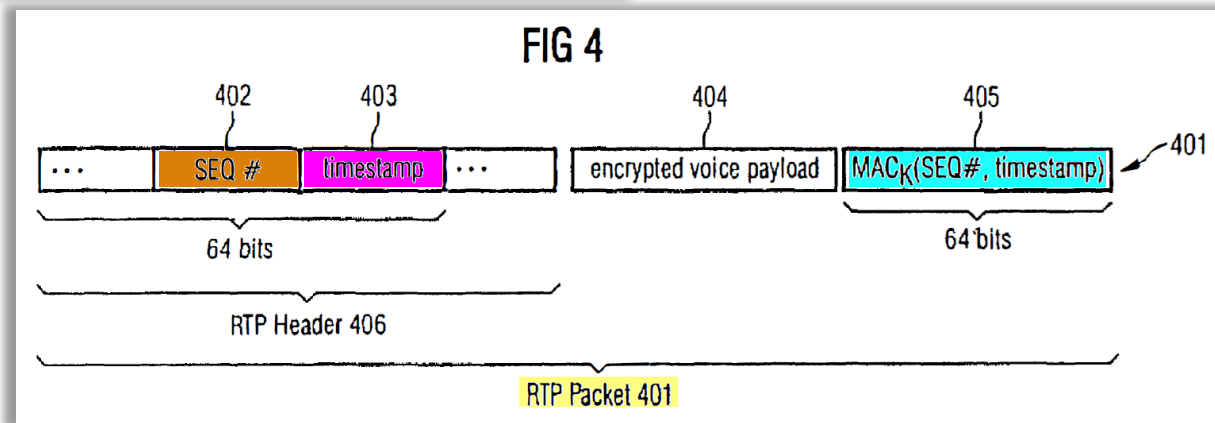
EX1001 ('682 Patent) Figs. 1-2, 6:33-51; Paper 26 (POR) at 4

The Innovative Technique of the '682 Patent

Inserting authentication data into RTP packets as an application protocol on an application layer

FIG. 4 shows a protocol data unit (PDU) of the application protocol with authentication data. What is shown in FIG. 4 is a protocol data unit (PDU) of the real time transport protocol (RTP, see 201 in FIG. 2) 401. Such an RTP packet 401 comprises an RTP header 406, encrypted media data 404 and authentication data 405. The RTP header 406 comprises, inter alia, a sequence number 402 and a timestamp 403. Both the transmitter and the receiver know a shared secret K, in this case indicated as a key, which is used to generate a message authentication code (MAC), on the basis of the sequence number 402 and the timestamp 403 (see field 405). An advantage with respect to encryption using a DES algorithm, for example, is a field length of 64 bits.

As already described, such a packet sent by the transmitter is authenticated at the receiver end such that (in relation to the application layer) a message authentication code is generated by field 402 (sequence number) and field 403 (timestamp) on the basis of the key (K) known to the receiver. If this message authentication code is the same as the field 405, then the arriving RTP packet 401 is a data packet coming from a known transmitter, and the data are processed, for example displayed or stored. In the other case, unauthenticated data are involved, the transmitter is unknown to the receiver and the entire RTP packet is rejected.



EX1001 ('682 Patent) at 7:24-36;
Paper 26 (POR) at 4-5

The Innovative Technique of the '682 Patent

Benefits of authenticating RTP packets in the application layer

As stated above, depending on the protocol structure (cf. OSI model), data in each protocol layer have their own transparency with regard to this protocol layer, i.e. the services in protocol layers beneath are performed (without being seen by the current protocol layer). Advantageously, data packets on the application layer, in particular, are free of the administrative data associated with layers beneath, i.e. the data packets in the application layer have, besides the administrative information for the application layer, only the data which are actually to be communicated. Accordingly, authentication in the application layer is particularly advantageous, because the data packets themselves, in contrast to

layers beneath, are of significantly reduced size. This small size has an advantageous effect on real time and availability of the entire communication system. If the receiver knows the transmitter, i.e. particularly if the transmitter is successfully authenticated with respect to the receiver, the message from the transmitter is accepted, in particular the data are stored. Otherwise, i.e. if the receiver does not know the transmitter, the data are rejected, i.e. buffering does not take place. This is particularly advantageous if such a decision is made automatically.

EX1001 ('682 Patent) at 3:55-4:10; Paper 26 (POR) at 4

The Innovative Technique of the '682 Patent

Benefits of authenticating RTP packets in the application layer

In particular, available security functions and keys on the application layer can advantageously be allocated to the individual application users. This can advantageously be linked to the application data in a filter function outlined above. Special functions at the application level, such as picture and/or sound compression methods, can advantageously be combined with security functions in the application layer, which makes it possible to increase the end systems' performance and reduces the implementation complexity; this also applies to the aforementioned filtering mechanism.

EX1001 ('682 Patent) at 4:11-22

The described authentication mechanism in the application layer allows transmitters and receivers which know one another to be separated from transmitters which are not known by the receiver and from which the receiver does not accept any messages either. This allows an attack of the type described in the introduction ("denial-of-service" attack) to be effectively prevented, i.e. unwanted mass data are actually rejected when arriving at the transmitter.

EX1001 ('682 Patent) at 4:22-30

Claim 1 of the '682 Patent

1. A method for transmitting data from a transmitter to a receiver, comprising:

providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.

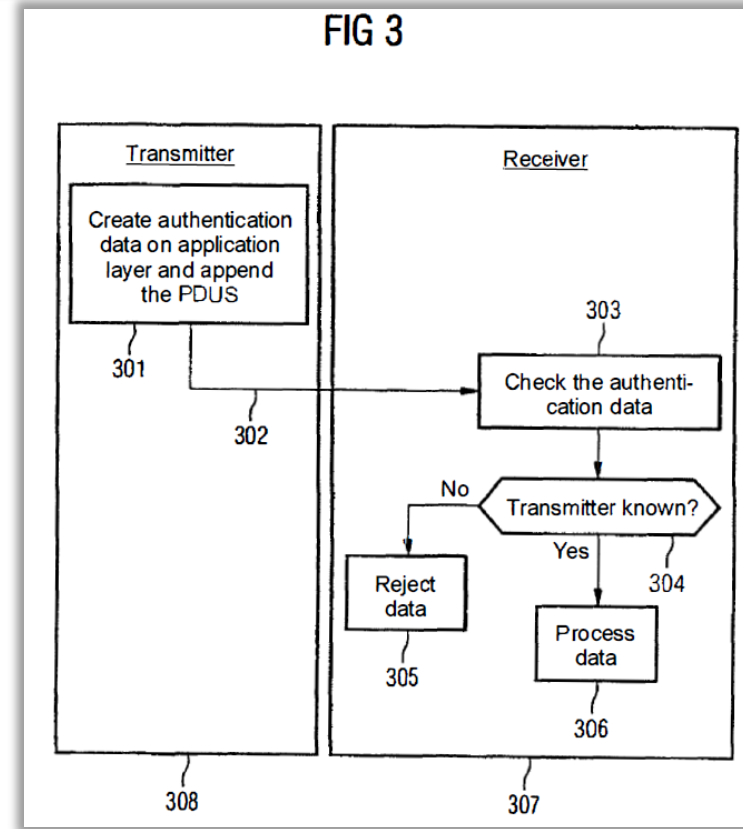


FIG. 3 is a flowchart for transmitting data from the transmitter 308 to the receiver 307. In block 301, authenti-

EX1001 ('682 Patent) at 7:6-7

Paper 26 (POR) at 3

Claim 1 of the '682 Patent

1. A method for transmitting data from a transmitter to a receiver, comprising:

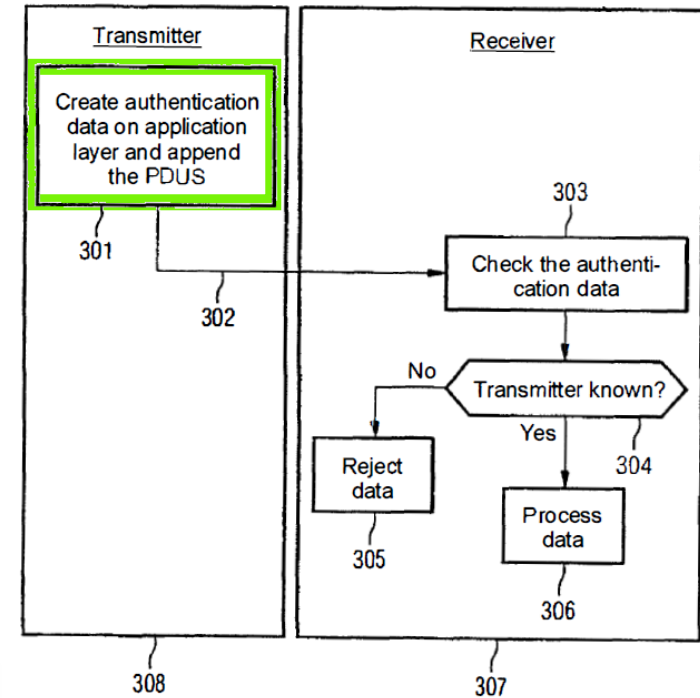
providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.

transmitter 308 to the receiver 307. In block 301, authentication data are produced on the application layer, and the protocol data unit (PDU) relevant to the application protocol is appended. In accordance with the arrangements of the application protocol, the data, including the authentication data, are transmitted to the receiver 307 (see connection 302). This is done using the functionalities or services available under the application protocol. In block 303, the

FIG 3



EX1001 ('682 Patent) Fig. 3

EX1001 ('682 Patent) at 7:6-22

Paper 26 (POR) at 3

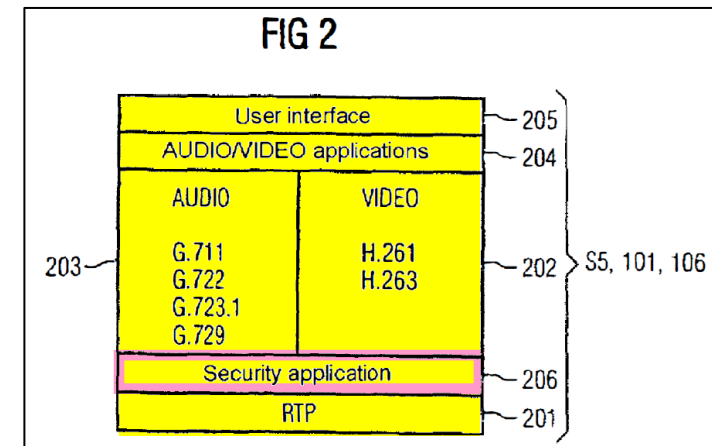
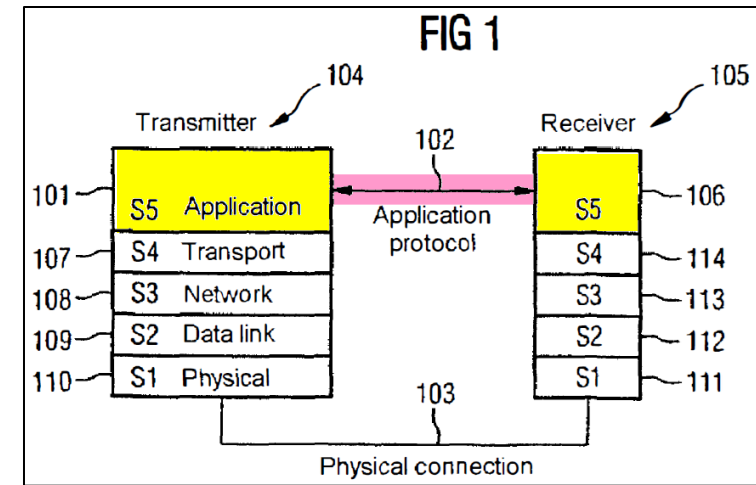
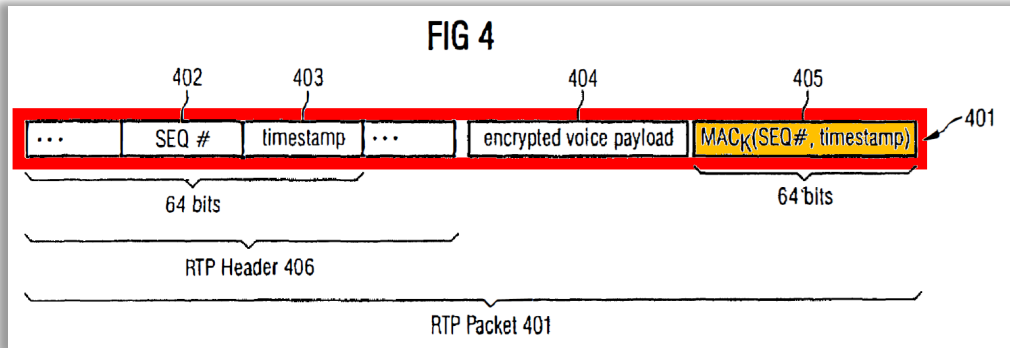
Claim 1 of the '682 Patent

1. A method for transmitting data from a transmitter to a receiver, comprising:

providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.



EX1001 ('682 Patent) at 7:6-23, 7:24-48, Figs. 1-4; Paper 26 (POR) at 3-5

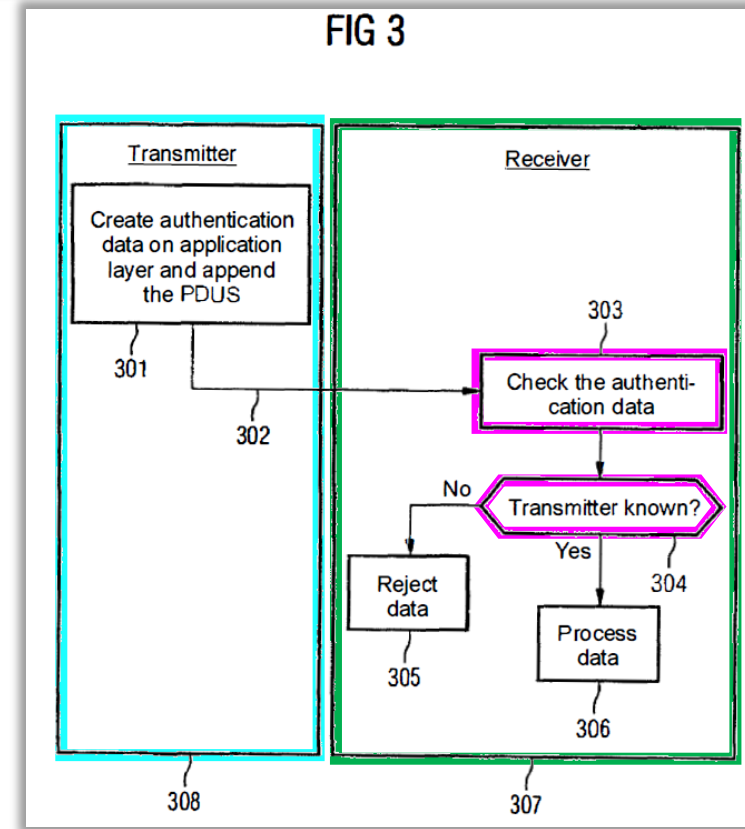
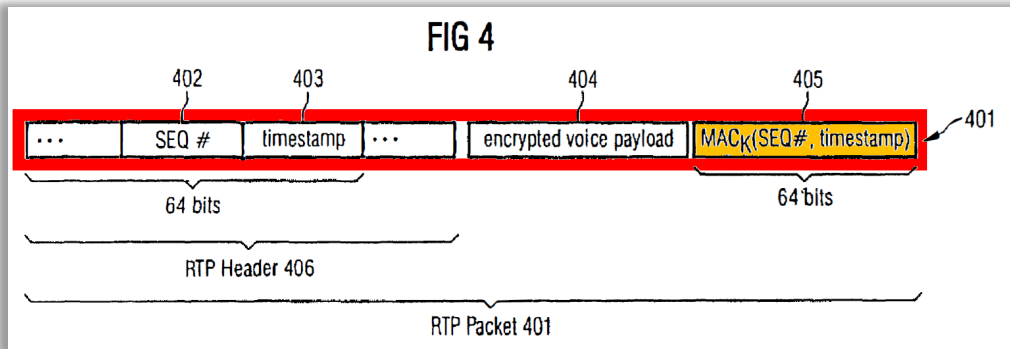
Claim 1 of the '682 Patent

1. A method for transmitting data from a transmitter to a receiver, comprising:

providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.



available under the application protocol. In block 303, the authentication data are checked in the receiver 307 and there is a test (in block 304) to determine whether the transmitter 308 is known to the receiver 307. If this is not the case, the

EX1001 ('682 Patent) at 7:6-23, Figs. 3 and 4; Paper 26 (POR) at 3-5

Claim 1 of the '682 Patent

1. A method for transmitting data from a transmitter to a receiver, comprising:

providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

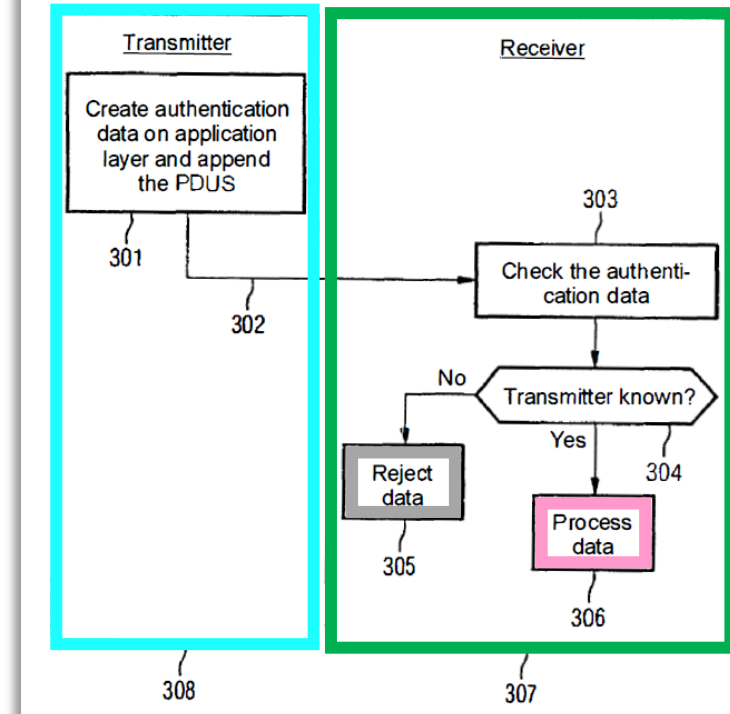
ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.

308 is known to the receiver 307. If this is not the case, the procedure branches to block 305 and the data are rejected. If the transmitter 308 is known to the receiver 307, the procedure branches to block 306 and the data are processed further. The authentication between transmitter and receiver was successful, and the transmitted data are not unwanted mass data.

EX1001
('682 Patent)
at 7:6-23

FIG 3



EX1001
('682 Patent)
Fig. 3

receiver. If this message authentication code is the same as the field 405, then the arriving RTP packet 401 is a data packet coming from a known transmitter, and the data are processed, for example displayed or stored. In the other case, unauthenticated data are involved, the transmitter is unknown to the receiver and the entire RTP packet is rejected.

EX1001
('682 Patent)
at 7:24-48

CLAIM CONSTRUCTION

Claim Construction

Claim 1

1. A method for transmitting data from a transmitter to a receiver, comprising:

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

[1.4] accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.

EX1001 ('682 patent), at claim 1



Claim Construction

Term	Patent Owner's Construction	Petitioners' Construction ¹
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

¹ See Paper 3 (Petition) at 9 and Paper 37 (Reply) at 1.



Claim Construction: “application layer” & “application protocol”

The OSI Model

The transmission of data is known, by way of example, on the basis of the OSI reference model as described in Andrew S. Tanenbaum, Computer-Netzwerke; Wolfram's Fachverlag, Attenkirchen 1992, pages 17-32. The OSI reference model (OSI model for short) from the International Standards Organization (ISO) has seven layers, each of which has a different functionality (in terms of abstraction). In the OSI model, layer 1 corresponds to a physical layer, where data and messages are transmitted from the transmitter to the receiver using a physical protocol. In layer 2, a data link layer is provided, and a data link protocol is used for transmission from layer 2 of the transmitter to layer 2 of the receiver. In a similar manner, layer 3, a network layer, uses a network protocol between transmitter and receiver, and layer 4, a transport layer, uses a transport protocol. In the OSI model, layer 5 corresponds to a session layer using a session protocol, layer 6 corresponds to a presentation layer using a presentation protocol, and layer 7 corresponds to an application layer using an application protocol. In practice,

EX1001 ('682 Patent) at 1:19-45

application layer using an application protocol. In practice, many applications do not always permit exact nomination of strict boundaries specifically between the upper protocol layers, particularly layers 5 to 7. By way of example, within the context of Internet telephony, i.e. use of the telephone service using the medium of the Internet, the three layers above the transport layer 4 combine to form an “application layer” for which, in a similar way to in the implementation above, an “application protocol” is used.

EX1001 ('682 Patent) at 1:19-45

Paper 26 (POR) at 14-15 (citing EX2004 ¶62)

Claim Construction: “application layer” & “application protocol”

The '682 Patent

When referring to application layer below, this denotes the layers above the transport layer (layers above 4). The application protocol also denotes the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.

EX1001 ('682 Patent) at 2:6-11

“Because a patent is a fully integrated written instrument, we have long emphasized the importance of the specification in claim construction. Thus, if the specification reveals a special definition given to a claim term by the inventor, then **the inventor’s lexicography governs**, even if it differs from the term’s ordinary meaning.”

David Netzer Consulting Eng’r LLC v. Shell Oil Co., 824 F.3d 989, 994 (Fed. Cir. 2016) (cleaned up; emphasis added)



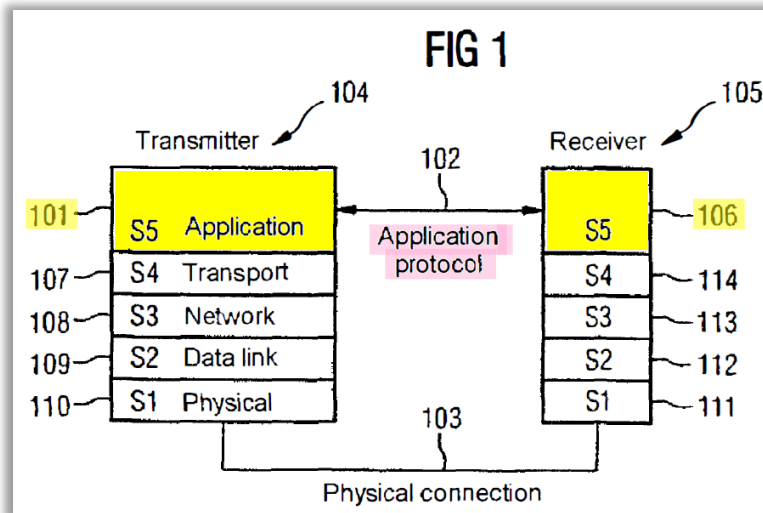
Paper 26 (POR) at 12, 15-16 (citing EX2004 ¶63)

Claim Construction: “application layer” & “application protocol”

The '682 Patent

FIG. 1 is a block diagram of a protocol architecture (protocol stack) for a communication system in the layer model;

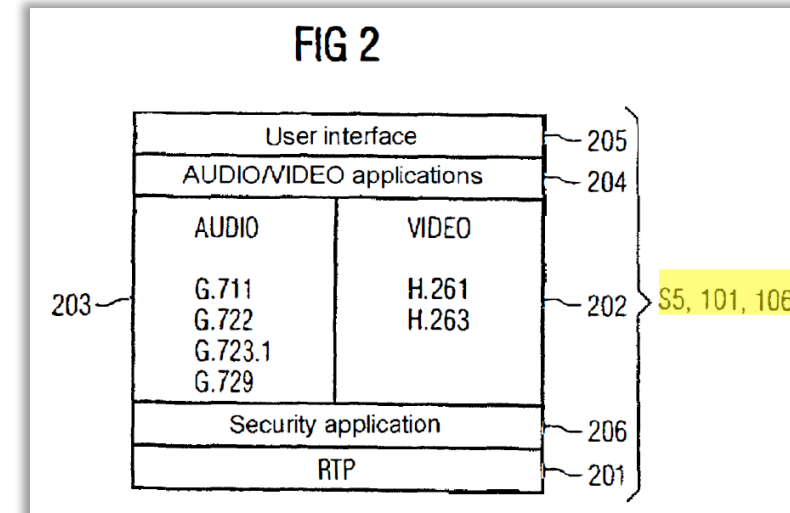
EX1001 ('682 Patent) at 5:65-67



EX1001 ('682 Patent) Fig. 1

FIG. 2 is a block diagram of an application layer with possible protocols;

EX1001 ('682 Patent) at 6:1-2



EX1001 ('682 Patent) Fig. 2

Paper 26 (POR) at 16 (citing EX2004, ¶64)

'682 Patent

HANDLEY IS NOT PRIOR ART



Handley is not prior art.

Petitioners' only public accessibility theory is that Handley (EX1005) published in Computer Networks journal on February 11, 1999

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

59. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the Computer Networks journal. Handley provides an

EX1003 (Houh Decl.) ¶59

Paper 26 (POR) at 18-19; Paper 44 (Sur-Reply) at 5



Handley is not prior art.

The Board instituted based on Petitioners' sole theory that Handley (EX1005) published in Computer Networks journal on February 11, 1999

We agree with Petitioner that there is a reasonable likelihood that Dr. Houh's sworn testimony that Handley was published on February 11, 1999 in the Computer Networks journal is true. Ex. 1003 ¶¶ 59, 327. We agree with Petitioner that there is a reasonable likelihood that the Computer Networks Journal is an established publisher because the Board routinely accepts articles from this Journal. Paper 14, 1 (citing *Resideo Tech. v.*

Paper 16 at 15

15, 1–2. However, the mere fact that Petitioners cited, and the Board recognized, Computer Networks in two separate cases is evidence that artisans of ordinary skill had access to the publication. Further, Handley

We agree with Petitioner that there is a reasonable likelihood that a person of ordinary skill, exercising reasonable diligence, would have found Handley in the Computer Networks Journal. *Id.* The Petition and supporting evidence, taken together, provide more “than mere notice pleading.” *Hulu* at 13. Therefore, on this record, we are sufficiently persuaded that there is a reasonable likelihood that Handley qualifies as a printed publication. We do not opine at this stage of the proceeding as to the

Paper 16 at 15-16

Paper 26 (POR) at 20



Handley is not prior art.

The Petition's evidence is insufficient: no indicia of publication

Very large conferences on the Internet: the Internet Multimedia Conferencing Architecture and the MBONE.

M. Handley, J. Crowcroft and C. Bormann

Abstract

In this paper we provide an overview of multimedia conferencing on the Internet. The protocols mentioned are all specified elsewhere as internet-drafts or RFCs. Each RFC gives details of the protocol itself, how it works and what it does. This document attempts to provide the reader with an overview of how the components fit together and of some of the assumptions made, as well as some statement of direction for those components still in a nascent stage.

1 Introduction

The Internet is not currently very good at carrying audio and video. This is hardly surprising as it was not designed or engineered with real-time traffic in mind, but there has recently been a great deal of interest in using the Internet for telephony services. Part of this has come from pricing anomalies that make internet telephony somewhat artificially cheaper than traditional telephone services, but this is not the whole story. The Internet itself is improving to better handle traffic such as audio and video, and in the medium term, the internet should be able to provide good quality realtime multimedia services, although such quality improvements are likely to incur additional charges.

However, the real interest in using the internet for audio and video should come from the prospect for a single ubiquitous communications network that not only allows traditional telephony services, but also video, shared collaboration tools, and through IP Multicast, multi-party conferences and multimedia sessions that scale from small group meetings through to television sized audiences. In principle, this may lead to a "democratization" of telecommunication services, where licenses to broadcast are not required to control physical access to the limited broadcast medium (although they may still be required for political reasons).

It is far from clear what services will eventually emerge using such communications capabilities. We can only say that the technical capability to have large numbers of sessions ranging in audience from hundreds to millions of participants, largely unlimited by geographic boundaries, will lead to services and social structures that do not exist today. However, we can describe the basic technologies that are likely to bring about such changes, and in this paper we attempt to provide such an overview. We leave it to the reader to imagine the uses to which this technology will be put.

2 The Technology

In conjunction with computers, the term "conferencing" is often used in two different ways: firstly, to refer to bulletin boards and mail list style asynchronous exchanges of messages between multiple users; secondly, to refer to synchronous or so-called "real-time" conferencing, including audio, video, shared whiteboards and other applications. This paper is about the architecture for this latter application in an Internet environment.

1

Meta 1005
p. 1

“One of the Flashpoint manuals is marked ‘an unpublished work and is considered a trade secret belonging to the copyright holder.’ The second manual is not marked with any indicium of either publication or secrecy. There was no evidence as to the source, publication, or public accessibility of either manual. The district court found that ‘no witness testified, nor was any evidence presented, that either of these documents was ever published or disseminated to the public.’”

ResQNet.com, Inc. v. Lansa, Inc., 594 F.3d 860, 865-66 (Fed. Cir. 2010)



EX1005 (Handley) at 1

Paper 26 (POR) at 21-22



Handley is not prior art.

The Petition's evidence is insufficient: conclusory argument and testimony

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

59. Handley (EX1005) – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the Computer Networks journal. *Handley* provides an

EX1003 (Houh Decl.) ¶59

“Attorney argument is not evidence.”

Icon Health & Fitness, Inc. v. Strava, Inc., 849 F.3d 1034, 1043 (Fed. Cir. 2017)

“Conclusory expert testimony does not qualify as substantial evidence.”

TQ Delta, LLC v. Cisco Sys., 942 F.3d 1352, 1358 (Fed. Cir. 2019)



Paper 26 (POR) at 19, 21-22



Handley is not prior art.

The Petition does not explain how the POSITA would locate Handley

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

59. Handley (EX1005) – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the Computer Networks journal. *Handley* provides an

EX1003 (Houh Decl.) ¶59

“A reference is considered publicly accessible ‘upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’”

Jazz Pharms., Inc. v. Amneal Pharms., LLC, 895 F.3d 1347, 1355 (Fed. Cir. 2018)



Paper 26 (POR) at 19, 22



Handley is not prior art.

Petitioners forfeited their opportunity to argue public accessibility in Reply

A. Handley Qualifies as Prior Art

PO contends the Petition does not show *Handley* (EX1005) qualifies as prior art. POR, 18-23. Since the filing of the POR, the Board granted Petitioners' Motion to Submit Supplemental Information. *See* Paper 28. There, the Board confirmed that *Handley* was publicly accessible by February 11, 1999, thus, confirming *Handley* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art. Paper 28, 3.

Paper 37 (Reply) at 2

We also determine that by failing to argue in the papers that any particular claim element lacks support in the '777 provisional, Petitioner waived such arguments.⁹

⁹ At the hearing, Petitioner requested to introduce new arguments into the record concerning the support provided by Patent Owner in the Sur-reply. Tr. 64:15–67:23. We allowed Petitioner to advance the arguments, but did not rule at that time whether they were improper new arguments. *Id.* at 64:15–65:23. We determine that these arguments are improper new arguments that should have been advanced in the Reply.

Unified Patents, LLC v. Gesture Technology Partners, LLC, IPR2021-00917, Paper 31 at 33 (PTAB Nov. 21, 2022)

Paper 44 (Sur-Reply) at 2



Handley is not prior art.

Petitioners forfeited their opportunity to argue public accessibility in the Petition

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

We find that Petitioner has not satisfied its burden to show that Mann is analogous art to the '924 patent. As noted above, **Petitioner waived all arguments related to the question of “reasonably pertinent to the particular problem” and only addresses the “field of endeavor.”** Though it may be sufficient to provide no or minimal analysis in the Petition concerning analogous art, including field of endeavor (*see e.g.*, IPR2021-00564, Paper 58, 24–25), **Petitioner’s Reply did not provide any additional analysis as to why the identified field of endeavor is correct or supported by the '924 patent or Mann (*see Reply 24*).** Rather, Petitioner merely asserts that its different characterizations of the disclosure of the '924 patent are the field of endeavor for the '924 patent. *Id.* As noted above, the asserted fields of endeavor with respect to Amir and Aviv do not cover Mann.

Apple, Inc. v. Gesture Technology Partners, LLC, IPR2021-00923, Paper 27 at 13-14 (PTAB Dec. 2, 2022)

Paper 44 at 2-3



Handley Is Not Prior Art

“The burden of production cannot be met without some combination of citing the relevant record evidence with specificity and explaining the significance of the produced material in briefs.”

Parus Holdings, Inc. v. Google LLC, 70 F.4th 1365, 1372 (Fed. Cir. 2023)

Paper 44 (Sur-Reply) at 2-3

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the Computer Networks journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

A. Handley Qualifies as Prior Art

PO contends the Petition does not show *Handley* (EX1005) qualifies as prior art. POR, 18-23. Since the filing of the POR, the Board granted Petitioners’ Motion to Submit Supplemental Information. *See* Paper 28. There, the Board confirmed that *Handley* was publicly accessible by February 11, 1999, thus, confirming *Handley* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art. Paper 28, 3.

Paper 37 (Reply) at 2

Paper 44 (Sur-Reply) at 2-3



Handley is not prior art.

The Board did not rule that Handley is prior art

A. Handley Qualifies as Prior Art

PO contends the Petition does not show *Handley* (EX1005) qualifies as prior art. POR, 18-23. Since the filing of the POR, the Board granted Petitioners' Motion to Submit Supplemental Information. See Paper 28. There, the Board confirmed that *Handley* was publicly accessible by February 11, 1999, thus, confirming *Handley* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art, Paper 28, 3.

Paper 37 (Reply) at 2

Further, regardless of whether Petitioner could have submitted the supplemental information earlier, the purpose of 37 C.F.R. § 42.123(a) is to allow filing of evidence relevant to a claim. Petitioner is not taking a wait and see approach to submitting supplemental information. Patent Owner raised publication issues with respect to Exhibits 1005 and 1007 in its Preliminary Response, and Petitioner responded with the Motion. Moreover, Patent Owner is able to argue any publication or evidentiary issues collectively with respect to Exhibits 1005, 1007, and 1016–1028 in the normal course of scheduled briefing.

Paper 28 at 6

Paper 44 (Sur-Reply) at 3



Handley is not prior art.

Petitioners' motion arguments and evidence are not incorporated into their Reply

A. Handley Qualifies as Prior Art

PO contends the Petition does not show *Handley* (EX1005) qualifies as prior art. POR, 18-23. Since the filing of the POR, the Board granted Petitioners' Motion to Submit Supplemental Information. See Paper 28. There, the Board confirmed that *Handley* was publicly accessible by February 11, 1999, thus, confirming *Handley* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art, Paper 28, 3.

Paper 37 (Reply) at 2

We decline Petitioner's invitation to consider arguments presented in papers outside of the Petition and Petitioner's Reply. We treat Petitioner's request that we consider arguments only presented in the Opposition to the Motion to Amend as a request for incorporation by reference. However, our rules prohibit "incorporat[ion] by reference from one document into another document." 37 C.F.R. § 42.6(a)(3) (2019); see also *DeSilva v. DiLeonardi*, 181 F.3d 865, 866–67 (7th Cir. 1999) (Incorporation "by reference amounts to a self-help increase in the length of the [] brief[.]" and "is a pointless imposition on the court's time. A brief must make all arguments accessible to the judges, rather than ask them to play archeologist with the record.")). Petitioner has not persuasively argued why we should not apply Rule 42.6(a)(3) in these circumstances. See 37 C.F.R. § 42.5(b) (2019) ("The Board may waive or suspend a requirement of parts 1, 41, and 42 and may place conditions on the waiver or suspension."). Although Petitioner may have intended to make the argument in both Petitioner's Reply and the Opposition to the Motion to Amend (Tr. 58–59), it did not do so.⁸

Apple Inc. v. Qualcomm Inc., IPR2018-01279, Paper 45 at 17-18 (PTAB Jan. 2, 2020)

Paper 44 (Sur-Reply) at 3-4



Handley is not prior art.

Considering Petitioners' motion arguments would “eviscerate all page limits”

A. Handley Qualifies as Prior Art

PO contends the Petition does not show *Handley* (EX1005) qualifies as prior art. POR, 18-23. Since the filing of the POR, the Board granted Petitioners' Motion to Submit Supplemental Information. See Paper 28. There, the Board confirmed that *Handley* was publicly accessible by February 11, 1999, thus, confirming *Handley* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art, Paper 28, 3.

Paper 37 (Reply) at 2

“Further, Parus’s suggestion that patent owners need only submit evidence—regardless how voluminous or argumentative—would eviscerate all page limits for patent owners while maintaining restrictions on petitioners. See 37 C.F.R. § 42.24.”

Parus Holdings, Inc. v. Google LLC, 70 F.4th 1365, 1372 (Fed. Cir. 2023)

Before addressing the substance of Petitioner’s arguments, we note that page 1 of the Motion to Exclude directs us to a separate document, Paper 31, which “further explains the nature of the objections.” Paper 46, 1. Page 11 of the Motion to Exclude contains similar references to arguments set forth in Paper 31. See Paper 46, 11. Our Rules unambiguously foreclose such attempts to incorporate by reference arguments from other documents. 37 C.F.R. § 42.6(a)(3) (2018) (“Arguments must not be incorporated by reference from one document into another document.”). Accordingly, we disregard these references to Paper 31 and consider only the arguments set forth in the Motion to Exclude.

In-Depth Geophysical Inc. v. ConocoPhillips Co., IPR2019-00850, Paper 56 at 35 (PTAB Sept. 3, 2020)

Paper 44 (Sur-Reply) at 3-4



Handley is not prior art.

The Board should not consider the supplemental information

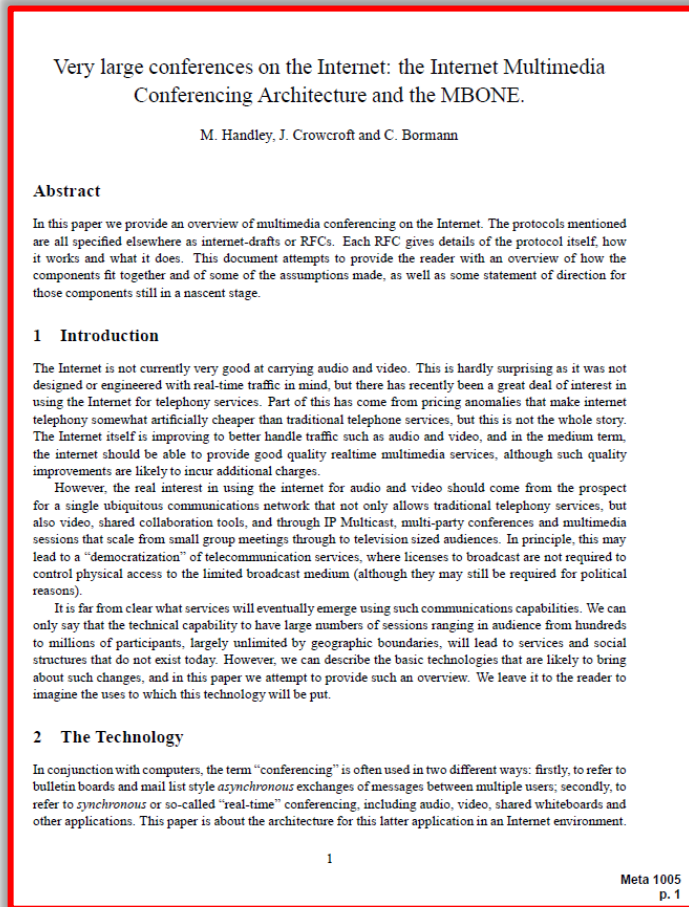
“But it is still a system that is predicated on a petition followed by a trial in which the petitioner bears the burden of proof. Given that framework, we find no support for the PTO’s position that the Board is free to adopt arguments on behalf of petitioners that could have been, but were not, raised by the petitioner during an IPR. Instead, the Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.”

In re Magnum Oil Tools Int’l, Ltd., 829 F.3d 1364, 1381 (Fed. Cir. 2016)

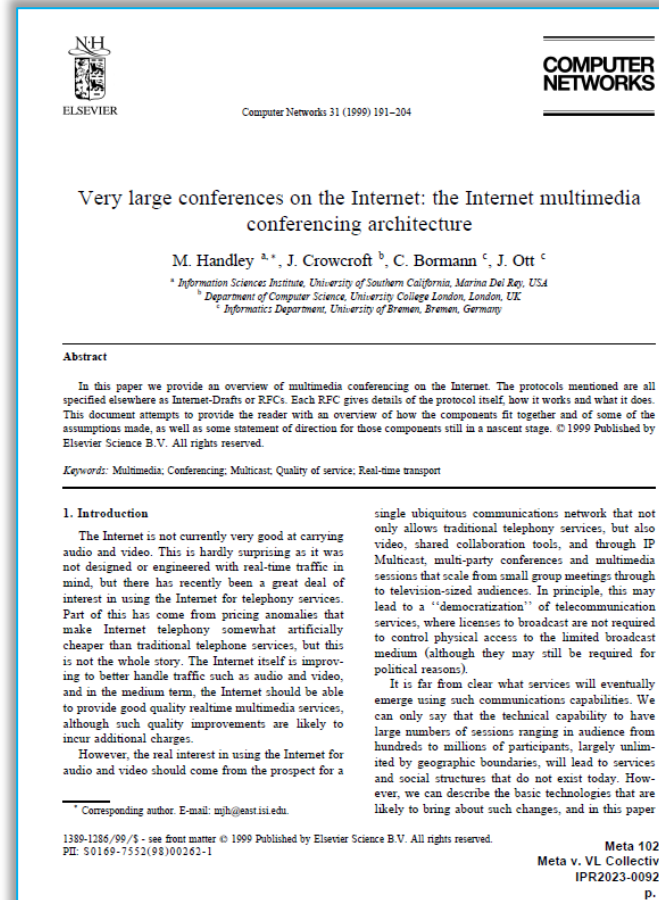


Handley is not prior art.

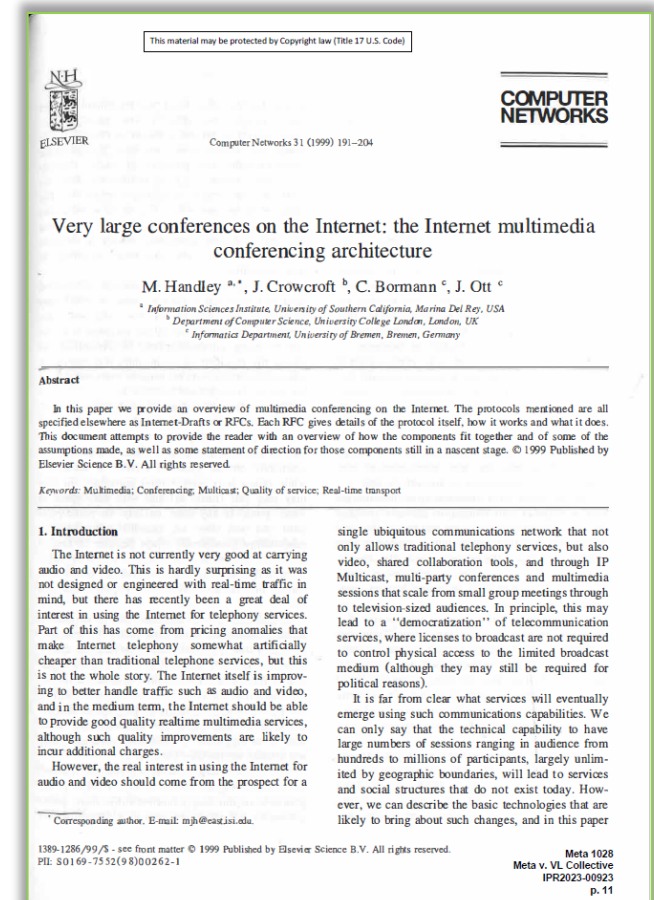
Handley (EX1005) is not what published in Computer Networks



EX1005 (Handley)



EX1027



EX1028



Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

Very large conferences on the Internet: the Internet Multimedia Conferencing Architecture and the MBONE.

M. Handley, J. Crowcroft and C. Bormann



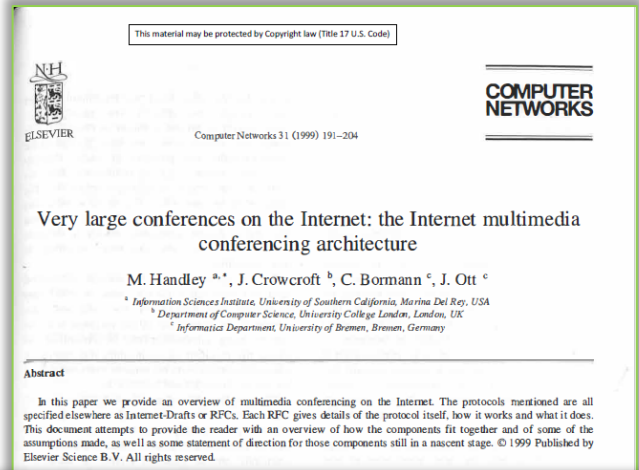
Computer Networks 31 (1999) 191–204

COMPUTER NETWORKS

Very large conferences on the Internet: the Internet multimedia conferencing architecture

M. Handley ^{a,*}, J. Crowcroft ^b, C. Bormann ^c, J. Ott ^c

^a Information Sciences Institute, University of Southern California, Marina Del Rey, USA
^b Department of Computer Science, University College London, London, UK
^c Informatics Department, University of Bremen, Bremen, Germany



Very large conferences on the Internet: the Internet multimedia conferencing architecture

M. Handley ^{a,*}, J. Crowcroft ^b, C. Bormann ^c, J. Ott ^c

^a Information Sciences Institute, University of Southern California, Marina Del Rey, USA
^b Department of Computer Science, University College London, London, UK
^c Informatics Department, University of Bremen, Bremen, Germany

It is far from clear what services will eventually emerge using such communications capabilities. We can only say that the technical capability to have large numbers of sessions ranging in audience from hundreds to millions of participants, largely unlimited by geographic boundaries, will lead to services and social structures that do not exist today. However, we can describe the basic technologies that are likely to bring about such changes, and in this paper

1389-1286/99/\$ - see front matter © 1999 Published by Elsevier Science B.V. All rights reserved.
PII: S0169-7552(98)00262-1

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 11

EX1005 (Handley)

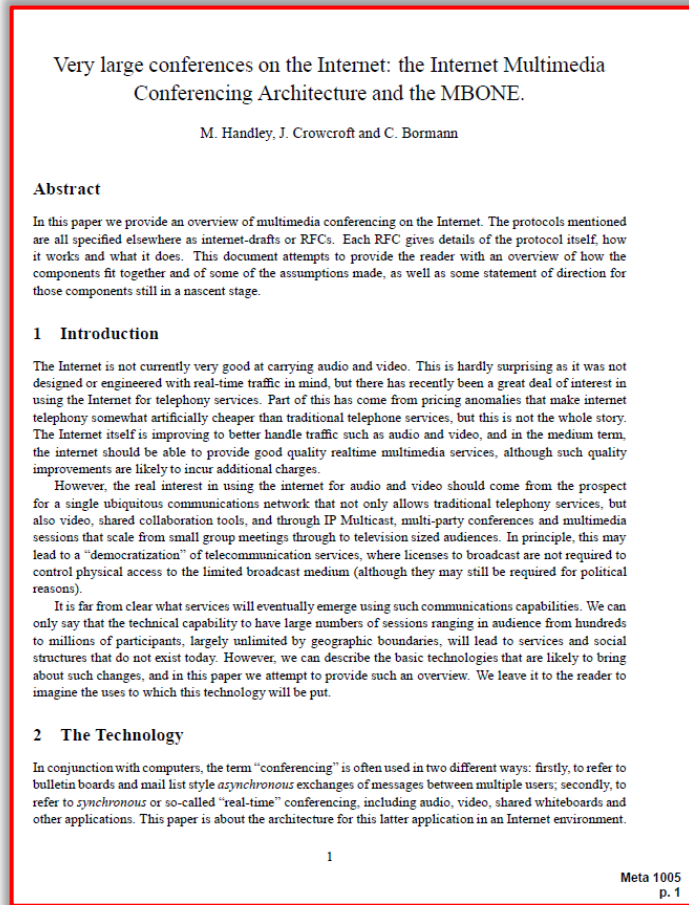
EX1027

EX1028

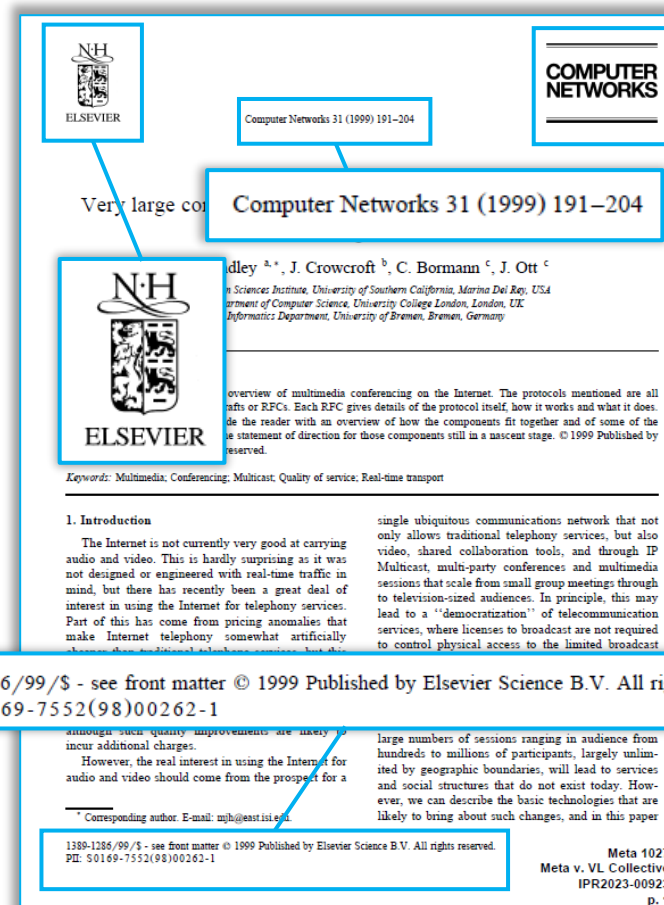


Handley is not prior art.

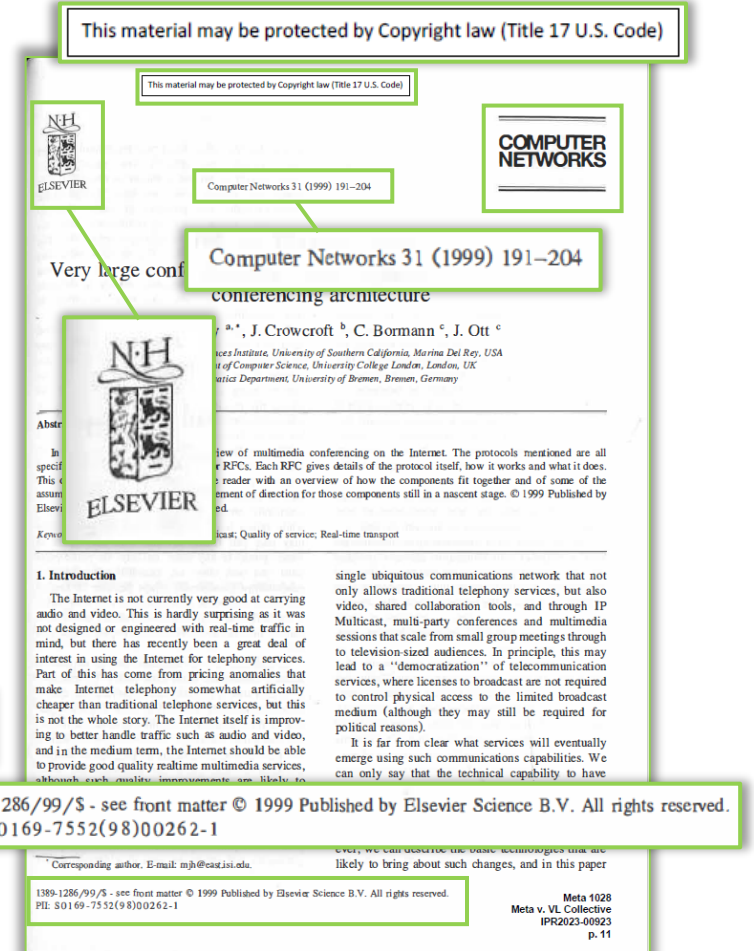
Handley (EX1005) is not what published in Computer Networks



EX1005 (Handley)



EX1027



EX1028

Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

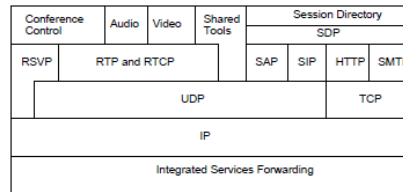


Figure 1: Internet multimedia conferencing protocol stacks

- Senders just send to the group
- Receivers express an interest in receiving data sent to the group

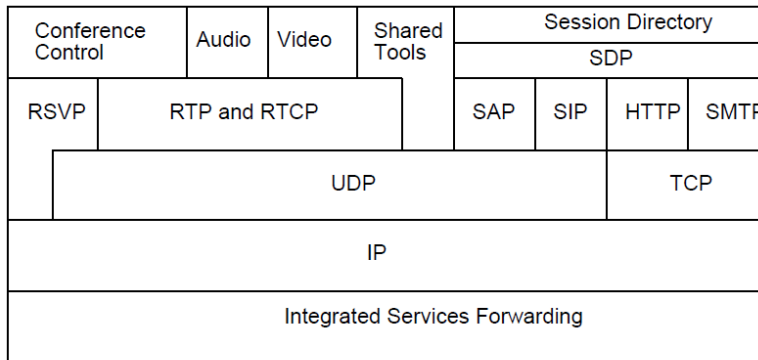


Figure 1: Internet multimedia conferencing protocol stacks

group can be encapsulated (either unicast or multicast) between on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers

3

Meta 1005
p. 3

EX1005 (Handley)

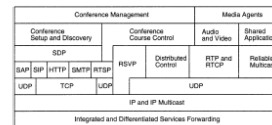


Fig. 1. Internet multimedia conferencing protocol stacks.

fashion for specific tasks to produce a complete conference.

3. Multicast traffic distribution

detailed information on multicast routing, see [1,5,7,8,22]. Typically, as a group with s senders and r receivers increases in size, state in routers scales $O(s)$ or $O(1)$ depending on the routing scheme in use. This state may be in on-tree routers for newer so-called sparse-mode algorithms such as PIM, or in off-tree routers for older so-called dense-mode algorithms such as DVMRP. Thus the most scalable current multicast routing algorithms require $O(1)$ state in on-tree routers, and hence the total routing state scales $O(g)$ in a router that is on-tree for g groups. We can also envisage multicast routing schemes which require less than $O(g)$ state¹, but the requirement is not currently urgent, so none of these have yet been implemented.

The level of indirection introduced by the IP class D address denominating the group solves the distributed systems binding problem, by pushing this

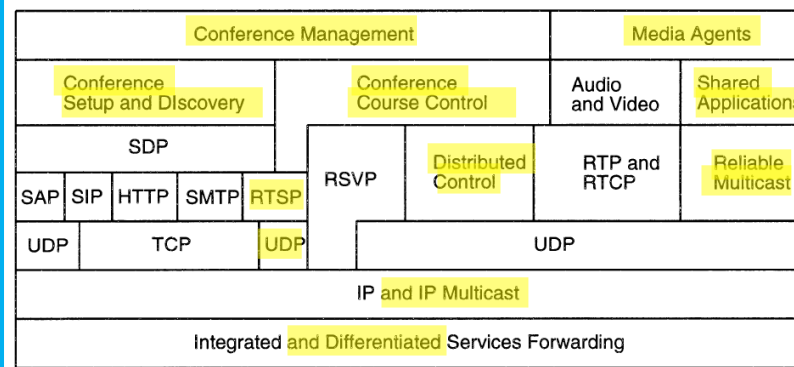


Fig. 1. Internet multimedia conferencing protocol stacks.

routing will not be discussed in detail here. For more on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers.

Meta 1027
Meta v. VL Collective
IPR2023-00923
p. 3

EX1027

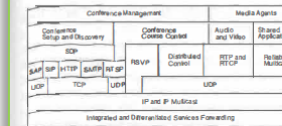


Fig. 1. Internet multimedia conferencing protocol stacks.

fashion for specific tasks to produce a complete conference.

3. Multicast traffic distribution

detailed information on multicast routing, see [1,5,7,8,22]. Typically, as a group with s senders and r receivers increases in size, state in routers scales $O(s)$ or $O(1)$ depending on the routing scheme in use. This state may be in on-tree routers for newer so-called sparse-mode algorithms such as PIM, or in off-tree routers for older so-called dense-mode algorithms such as DVMRP. Thus the most scalable current multicast routing algorithms require $O(1)$ state in on-tree routers, and hence the total routing state scales $O(g)$ in a router that is on-tree for g groups. We can also envisage multicast routing schemes which require less than $O(g)$ state¹, but the requirement is not currently urgent, so none of these have yet been implemented.

The level of indirection introduced by the IP class D address denominating the group solves the distributed systems binding problem, by pushing this task down into routing: given a multicast address

IP multicast provides efficient many-to-many data

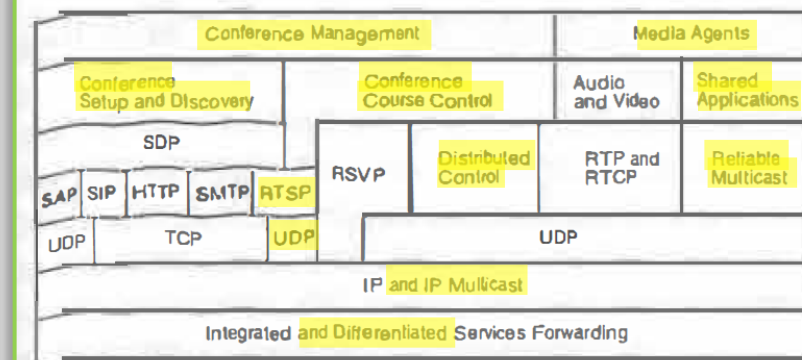


Fig. 1. Internet multimedia conferencing protocol stacks.

several solutions do exist and therefore multicast routing will not be discussed in detail here. For more on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers.

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 13

EX1028

Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

playback and recording of a session into an archive and record it.

7 Conference

There are two basic session types: a session invitation, and a session record. Session invitation is provided using a session invitation protocol such as SIP.

7.1 Session

The rendezvous "broadcasts" session information to provide an advertisement, port addresses, port session. The session and the session. This mechanism provides additional information in sessions in this manner, and

7.2 Session

Not all sessions invite a user to join a session or a multicast session to join the session. As users are a user in a location rather than responses, such as the session conference. SIP care whether the information to know what sort of by no means is conference are

8 Security

There is a temporary traffic visits so that a multicast session to join a multicast

Figure 6: Internet multimedia conferencing lifecycles

12

Meta 1005
p. 12

M. Handley et al. / Computer Networks 31 (1999) 191–204 201

session invitation. A session is provided using a session invitation protocol such as SIP.

7.1. Session distribution

The rendezvous sessions is a multicast "broadcasts" session information to provide an advertisement, port addresses, port session. The session and the session. This mechanism provides additional information in sessions in this manner, and

8.1. Authentication and key distribution

Key distribution is closely tied to authentication. Conference or session directory keys can be securely distributed using public-key cryptography on a one-to-one basis (by e-mail, a directory service, or by an explicit conference setup mechanism), but this is only as good as the certification mechanism used to certify that a key given by a user is the correct public key for that user. Such certification mechanisms [3] are however not specific to conferencing, and it looks likely that certificates such as those provided by PGP will be most widely used in the near term. Session keys can be distributed using encrypted Session Descriptions carried in SIP session invitations, or in encrypted session announcements as described below. Neither of these mechanisms provide for changing keys during a session as might be required in some tightly coupled sessions, but they are probably sufficient for many used in the context of lightweight sessions. Even without privacy requirements in the conference policy, strong authentication of a user is required if making a network reservation results in usage based billing.

7.2. Session invitation

Not all sessions that are advertised explicitly invite a user to join a session or a multicast session to join the session. As users are a user in a location rather than responses, such as the session conference. SIP care whether the information to know what sort of by no means is conference are

8.2. Encrypted session announcements

Session Directories can make encrypted session announcements using private key encryption, and carry the encryption keys to be used for each of the conference media streams in the session. Whilst this does not solve the key distribution problem, it does allow a single conference to be announced more than once to more than one key-group, where each group holds a different session directory key, so that the two groups can be brought together into a single conference without having to know each other's keys.

8.3. Secured "broadcasts"

While private-key encryption is sufficient to exclude non-members from sending or receiving multicast conference traffic, it does mean that all members

9. Summary

This document is an attempt to gather together in one place the set of assumptions behind the design of the Internet Multimedia Conferencing architecture, and the services that are provided to support it. Fig. 6 shows an example time sequence involved in setting up a light-weight session between two sites. In this case, site A creates a session advertisement, and some time later starts sending a media stream even though there may be no receiver at that time. Some time later, site B joins the session (the multicast routing protocol here is PDM), and starts to receive the traffic. At the earliest opportunity site B also makes an RSVP reservation to ensure the flow quality is satisfactory. This example should be taken as illustrative only—there are different ways to join

Meta 1027
Meta v. VL Collective
IPR2023-00923
p. 12

M. Handley et al. / Computer Networks 31 (1999) 191–204 202

session invitation. A session is provided using a session invitation protocol such as SIP.

7.1. Session distribution

The rendezvous sessions is a multicast "broadcasts" session information to provide an advertisement, port addresses, port session. The session and the session. This mechanism provides additional information in sessions in this manner, and

8.1. Authentication and key distribution

Key distribution is closely tied to authentication. Conference or session directory keys can be securely distributed using public-key cryptography on a one-to-one basis (by e-mail, a directory service, or by an explicit conference setup mechanism), but this is only as good as the certification mechanism used to certify that a key given by a user is the correct public key for that user. Such certification mechanisms [3] are however not specific to conferencing, and it looks likely that certificates such as those provided by PGP will be most widely used in the near term. Session keys can be distributed using encrypted Session Descriptions carried in SIP session invitations, or in encrypted session announcements as described below. Neither of these mechanisms provide for changing keys during a session as might be required in some tightly coupled sessions, but they are probably sufficient for many used in the context of lightweight sessions. Even without privacy requirements in the conference policy, strong authentication of a user is required if making a network reservation results in usage based billing.

7.2. Session invitation

Not all sessions that are advertised explicitly invite a user to join a session or a multicast session to join the session. As users are a user in a location rather than responses, such as the session conference. SIP care whether the information to know what sort of by no means is conference are

8.2. Encrypted session announcements

Session Directories can make encrypted session announcements using private key encryption, and carry the encryption keys to be used for each of the conference media streams in the session. Whilst this does not solve the key distribution problem, it does allow a single conference to be announced more than once to more than one key-group, where each group holds a different session directory key, so that the two groups can be brought together into a single conference without having to know each other's keys.

8.3. Secured "broadcasts"

While private-key encryption is sufficient to exclude non-members from sending or receiving multicast conference traffic, it does mean that all members

9. Summary

This document is an attempt to gather together in one place the set of assumptions behind the design of the Internet Multimedia Conferencing architecture, and the services that are provided to support it. Fig. 6 shows an example time sequence involved in setting up a light-weight session between two sites. In this case, site A creates a session advertisement, and some time later starts sending a media stream even though there may be no receiver at that time. Some time later, site B joins the session (the multicast routing protocol here is PDM), and starts to receive the traffic. At the earliest opportunity site B also makes an RSVP reservation to ensure the flow quality is satisfactory. This example should be taken as illustrative only—there are different ways to join

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 22

EX1005 (Handley)

EX1027

EX1028



Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

playback and record functionality. A client can specify that an RTSP server plays a recorded multimedia session into an existing multicast-based conference, or can specify that the server should join the conference and record it.

7 Conference Setup

There two basic forms of conference discovery mechanism. These are session advertisement and session invitation. Session advertisements are provided using a session directory, and inviting a user to join a session is provided using a session invitation protocol such as SIP or H.323.

7.1 Session Directories

The rendezvous mechanism for many light-weight sessions is a multicast based session directory. This "broadcasts" session descriptions[8] to all the potential session participants. These session descriptions provide an advertisement that the session will exist, and also provide sufficient information including multicast addresses, ports, media formats and session times so that a receiver of the session description can join the session. The session description protocol (SDP) describes the content and format of a multimedia session, and the session announcement protocol (SAP) is used to distribute it to all potential session recipients.

This mechanism can also be applied to advertised tightly coupled sessions, and only requires that additional information about the mechanism to use to join the session is given. However, as the number of sessions in the session directory grows, we expect that only larger-scale public sessions will be announced in this manner, and smaller, more private sessions will tend to use direct invitation rather than advertisement.

7.2 Session Invitation

Not all sessions are advertised, and even those that are advertised may require a mechanism to explicitly invite a user to join a session. Such a mechanism is required regardless of whether the session is a lightweight session or a more tightly coupled session, although the invitation system must specify the mechanism to be used to join the session.

As users are mobile, it is important that such an invitation mechanism is capable of locating and inviting a user in a location independent manner. Thus user addresses need to be used as a level of redirection rather than routing a call to a specific terminal. The invitation mechanism should also provide for alternative responses, such as leaving a message or being referred to another user, should the invited user be unavailable.

The Session Initiation Protocol provides a mechanism whereby a user can be invited to participate in a conference. SIP does not care whether the session is already ongoing, or is just being created, and it doesn't care whether the conference is a small tightly coupled session or a huge broadcast - it merely conveys the information to a user inviting them to participate and provides enough information for them to be able to know what sort of session to expect. Thus although SIP can be used to make telephone-style calls, it is by no means restricted to that style of conference. Possible places for SIP to be used in different styles of conference are shown in figure 6.

8 Security

There is a temptation to believe that multicast is inherently less private than unicast communication since the traffic visits so many more places in the network. In fact, this is not the case except with broadcast and prune type multicast routing protocols[3]. However, IP multicast does make it simple for a host to anonymously join a multicast group and receive traffic destined to that group without the other senders' and receivers'

200

M. Handley et al. / Computer Networks 31 (1999) 191–204

model is orthogonal to issues of quality of service and network resource reservation, and it is also orthogonal to the mechanism for discovering the conference [25].

Light-weight sessions are multicast based multimedia conferences that lack explicit conference membership control and explicit conference control mechanisms. Typically a lightweight session consists of a number of many-to-many media streams supported using RTP and RTCP using IP multicast.⁵ Typically, the only conference control information needed during the course of a light-weight session is that distributed in the RTCP session information, i.e. an approximate membership list with some attributes per member.

Tightly coupled conferences may also be multicast based and use RTP and RTCP, but in addition they have an explicit conference membership mechanism and may have an explicit conference control mechanism that provides facilities such as floor control.

The most widely used tightly coupled conference control protocols suitable for Internet use are those belonging to the ITU's H.323 family [17]. However it should be noted that this is inappropriate for large sessions where scaling problems will be introduced by the conference control mechanisms.

In order to try and address this, the ITU is currently standardising H.332, which is essentially a small tightly coupled H.323 conference with a larger lightweight-sessions-style conference listening in as passive participants. It is not yet clear whether H.332 will see large scale acceptance, as its benefits over a simple lightweight session are not terribly obvious. It seems likely that lightweight sessions combined with stream authentication (Section 8.3) might be a more appropriate solution for many potential users.

6.1. Controlling multimedia servers

The Real-Time Stream-control Protocol (RTSP) [28] provides a standard way to remote control a

⁵ There is some confusion on the term session, which is sometimes used for a conference and sometimes for a single media stream transported by RTP. In this paper, we prefer to use the less ambiguous term conference except where existing protocols use the term session.

multimedia server. While primarily aimed at web-based media-on-demand services, RTSP is also well suited to provide VCR-like controls for audio and video streams, and to provide playback and record functionality of RTP data streams. A client can specify that an RTSP server plays a recorded multimedia session into an existing multicast-based conference, or can specify that the server should join the conference and record it.

6.2. Protocols for non-A/V applications

Applications other than audio and video have evolved in Internet conferencing, e.g. Imm [4], Web [9], NTE [10]. Such applications can be used to substitute for meeting aids in physical conferences (whiteboards, projectors) or replace visual and auditory cues that are lost in teleconferences (e.g., a speaker list application); they also can enable new styles of joint work.

Most non-A/V applications have in common that the application protocol is about establishing and updating a shared state. Loss of information is often not acceptable, so some form of multicast reliability is required. The applications' requirements differ: Some applications make per-participant additions to the shared state that are orthogonal to each other (e.g., whiteboards), some evolve a more closely inter-related common state (e.g., additions to a speaker list must be properly sequenced). Some applications can make use of added bandwidth/react to congestion in an elastic way, others transport data that, although not strictly real-time, is time-critical.

In the IRTF research group on Reliable Multicast [15], work is in progress on common protocol elements that can be used in such applications. At the time of writing, some aspects of reliable multicast are not well-understood, such as the proper way to provide congestion control in a multicast environment. As congestion control is considered an essential element, standards track protocols are not expected before this can be solved.

7. Conference setup

There are two basic forms of conference discovery mechanism. These are session advertisement and

200

M. Handley et al. / Computer Networks 31 (1999) 191–204

model is orthogonal to issues of quality of service and network resource reservation, and it is also orthogonal to the mechanism for discovering the conference [25].

Light-weight sessions are multicast based multimedia conferences that lack explicit conference membership control and explicit conference control mechanisms. Typically a lightweight session consists of a number of many-to-many media streams supported using RTP and RTCP using IP multicast.⁵ Typically, the only conference control information needed during the course of a light-weight session is that distributed in the RTCP session information, i.e. an approximate membership list with some attributes per member.

Tightly coupled conferences may also be multicast based and use RTP and RTCP, but in addition they have an explicit conference membership mechanism and may have an explicit conference control mechanism that provides facilities such as floor control.

The most widely used tightly coupled conference control protocols suitable for Internet use are those belonging to the ITU's H.323 family [17]. However it should be noted that this is inappropriate for large sessions where scaling problems will be introduced by the conference control mechanisms.

In order to try and address this, the ITU is currently standardising H.332, which is essentially a small tightly coupled H.323 conference with a larger lightweight-sessions-style conference listening in as passive participants. It is not yet clear whether H.332 will see large scale acceptance, as its benefits over a simple lightweight session are not terribly obvious. It seems likely that lightweight sessions combined with stream authentication (Section 8.3) might be a more appropriate solution for many potential users.

6.1. Controlling multimedia servers

The Real-Time Stream-control Protocol (RTSP) [28] provides a standard way to remote control a

⁵ There is some confusion on the term session, which is sometimes used for a conference and sometimes for a single media stream transported by RTP. In this paper, we prefer to use the less ambiguous term conference except where existing protocols use the term session.

multimedia server. While primarily aimed at web-based media-on-demand services, RTSP is also well suited to provide VCR-like controls for audio and video streams, and to provide playback and record functionality of RTP data streams. A client can specify that an RTSP server plays a recorded multimedia session into an existing multicast-based conference, or can specify that the server should join the conference and record it.

6.2. Protocols for non-A/V applications

Applications other than audio and video have evolved in Internet conferencing, e.g. Imm [4], Web [9], NTE [10]. Such applications can be used to substitute for meeting aids in physical conferences (whiteboards, projectors) or replace visual and auditory cues that are lost in teleconferences (e.g., a speaker list application); they also can enable new styles of joint work.

Most non-A/V applications have in common that the application protocol is about establishing and updating a shared state. Loss of information is often not acceptable, so some form of multicast reliability is required. The applications' requirements differ: Some applications make per-participant additions to the shared state that are orthogonal to each other (e.g., whiteboards), some evolve a more closely inter-related common state (e.g., additions to a speaker list must be properly sequenced). Some applications can make use of added bandwidth/react to congestion in an elastic way, others transport data that, although not strictly real-time, is time-critical.

In the IRTF research group on Reliable Multicast [15], work is in progress on common protocol elements that can be used in such applications. At the time of writing, some aspects of reliable multicast are not well-understood, such as the proper way to provide congestion control in a multicast environment. As congestion control is considered an essential element, standards track protocols are not expected before this can be solved.

7. Conference setup

There are two basic forms of conference discovery mechanism. These are session advertisement and

11

Meta 1005
p. 11

10

Meta 1005
p. 10

EX1005 (Handley)

EX1027

Meta 1027
Meta v. VL Collective
IPR2023-00923
p. 10

EX1028

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 20



Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

rates sometimes seen with video. The use of public-key cryptography for this purpose has not yet been standardised, but some such mechanism will clearly be needed before the MBone becomes an acceptable environment for commercial broadcasters.

9 Summary

This document is an attempt to gather together in one place the set of assumptions behind the design of the Internet Multimedia conferencing architecture, and the services that are provided to support it.

Figure 7 shows the time sequence involved in setting up a light-weight session between two sites. In this case, site A creates a session advertisement, and some time later starts sending a media stream even though there may be no receiver at that time. Some time later, site B joins the session, and starts to receive the traffic. At the earliest opportunity site B also makes an RSVP reservation to ensure the flow quality is satisfactory.

10 Acknowledgments

Acknowledgments are due to the End-to-End Research Group, the Int-serv, RSVP, MMUSIC and AVT working groups of the IETF, and discussion with colleagues at UCL. The earliest clear exposition of the ideas here was presented at ACM SIGCOMM 1994 in London by Van Jacobson.

References

- [1] A. Ballardie, P. Francis, J. Crowcroft, "An Architecture for Scalable Inter-Domain Multicast Routing", ACM SIGCOMM 1993, pp 85-95
- [2] CCITT (Consultative Committee on International Telegraphy and Telephony). "Recommendation X.509: The Directory - Authentication Framework." 1988.
- [3] S. Deering, C. Partridge, D. Waitzman, "Distance Vector Multicast Routing Protocol", RFC 1075, Nov 1988.
- [4] Steve Deering "Multicast Routing in Internetworks and Extended LANs", ACM SIGCOMM 88, August 1988, pp 55-64 and "Host Extensions for IP Multicasting", RFC 1112
- [5] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C-G. Liu, L. Wei "An Architecture for Wide Area Multicast Routing" ACM SIGCOMM 1994, London October 1994, ACM CCR Vol 24, No. 4, 126-135
- [6] Estrin, Farinacci, Helmy, Thaler, Deering, Handley, Jacobson, Liu, Sharma, Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2117.
- [7] S. Floyd, V. Jacobson, S. McCane, C-G. Liu, L. Zhang, "A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing" ACM SIGCOMM 1995, pp 342-356
- [8] M. Handley, V. Jacobson "SDP: Session Description Protocol" INTERNET-DRAFT, Dec 1997.
- [9] M. Handley, D. Thaler, D. Estrin, "The Internet Multicast Address Allocation Architecture", INTERNET-DRAFT, Dec 1997.
- [10] V. Handman, A. Sasse, M. Handley, A. Watson, "Reliable Audio for Use over the Internet" Proc INET '95, Hawaii, Internet Society, Reston, VA, 1995.

14

Meta 1005
p. 14

EX1005 (Handley)

M. Handley et al. / Computer Networks 31 (1999) 191-204 203

8.2. Encrypted session announcements

Session Directories can make encrypted session announcements using private key encryption, and carry the encryption keys to be used for each of the conference media streams in the session. Whilst this does not solve the key distribution problem, it does allow a single conference to be announced more than once to more than one key-group, where each group holds a different session directory key, so that the two groups can be brought together into a single conference without having to know each other's keys.

9. Summary

This document is an attempt to gather together in one place the set of assumptions behind the design of the Internet Multimedia Conferencing architecture, and the services that are provided to support it.

Fig. 6 shows an example time sequence involved in setting up a light-weight session between two sites. In this case, site A creates a session advertisement, and some time later starts sending a media stream even though there may be no receiver at that time. Some time later, site B joins the session (the multicast routing protocol here is PIM), and starts to receive the traffic. At the earliest opportunity site B also makes an RSVP reservation to ensure the flow quality is satisfactory. This example should be taken as illustrative only—there are different ways to join

coupled conferences, joining there too. This architecture that is subject of active *initiated services* for now great promise to relative to individual scales well to large large numbers of some the subject of a few years. *Multis* are still a re-ear several schemes. *Layered codecs* references to scale in the join and leave perform receiver-ill being examined. *Reliable mul-* the next few years tion work in this congestion control complete security could be very desir-

Meta 1027
Meta v. VL Collective
IPR2023-00923
p. 12

sessions, and different ways to get improved quality of service.

The lightweight sessions model for Internet multimedia conferencing may not be appropriate for all conferences, but for those sessions that do not require tightly-coupled conference control, it provides an elegant style of conferencing that scales from two participants to millions of participants. It achieves this scaling by virtue of the way that multicast routing is receiver driven, keeping essential information about receivers local to those receivers. Each new participant only adds state close to them in the network. It also scales by not requiring explicit conference join mechanisms; if everyone were to need to know exactly who is in the session at any time, the scaling would be severely adversely affected. RTCP provides membership information that is accurate when the group is small, and increasingly only a statistical representation of the membership as the group grows. Security is handled through the use of encryption rather than through the control of data distribution.

Acknowledgements

Acknowledgments are due to the End-to-End Research Group, the Int-serv, RSVP, MMUSIC and AVT working groups of the IETF, and discussion

Meta 1027
Meta v. VL Collective
IPR2023-00923
p. 13

EX1027

M. Handley et al. / Computer Networks 31 (1999) 191-204 203

8.2. Encrypted session announcements

Session Directories can make encrypted session announcements using private key encryption, and carry the encryption keys to be used for each of the conference media streams in the session. Whilst this does not solve the key distribution problem, it does allow a single conference to be announced more than once to more than one key-group, where each group holds a different session directory key, so that the two groups can be brought together into a single conference without having to know each other's keys.

9. Summary

This document is an attempt to gather together in one place the set of assumptions behind the design of the Internet Multimedia Conferencing architecture, and the services that are provided to support it.

Fig. 6 shows an example time sequence involved in setting up a light-weight session between two sites. In this case, site A creates a session advertisement, and some time later starts sending a media stream even though there may be no receiver at that time. Some time later, site B joins the session (the multicast routing protocol here is PIM), and starts to receive the traffic. At the earliest opportunity site B also makes an RSVP reservation to ensure the flow quality is satisfactory. This example should be taken as illustrative only—there are different ways to join

conferences, here too. Architecture that ect of active *services* for at promise to to individual well to large numbers of he subject of years. *Mult-* are still a re-vel schemes *layered codecs* es to scale in in and leave orm receiving examined. *Reliable mul-* text few years work in this tion control *lete security* e very desir-

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 22

sessions, and different ways to get improved quality of service.

The lightweight sessions model for Internet multimedia conferencing may not be appropriate for all conferences, but for those sessions that do not require tightly-coupled conference control, it provides an elegant style of conferencing that scales from two participants to millions of participants. It achieves this scaling by virtue of the way that multicast routing is receiver driven, keeping essential information about receivers local to those receivers. Each new participant only adds state close to them in the network. It also scales by not requiring explicit conference join mechanisms; if everyone were to need to know exactly who is in the session at any time, the scaling would be severely adversely affected. RTCP provides membership information that is accurate when the group is small, and increasingly only a statistical representation of the membership as the group grows. Security is handled through the use of encryption rather than through the control of data distribution.

Acknowledgements

Acknowledgments are due to the End-to-End Research Group, the Int-serv, RSVP, MMUSIC and AVT working groups of the IETF, and discussion

Meta 1028
Meta v. VL Collective
IPR2023-00923
p. 23

EX1028



Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

¹ with IP encapsulation, not all on-tree routers need hold the state for a group whose traffic they are forwarding - traffic for the group can be encapsulated (either unicast or multicast) between on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers

² Note that a conference policy that restricts conference membership can be implemented using encryption and restricted distribution of encryption keys, of which more later.

³ There is some confusion on the term session, which is sometimes used for a conference and sometimes for a single media stream transported by RTP. In this paper, we prefer to use the less ambiguous term conference except where existing protocols use the term session.

EX1005 (Handley)

¹ With IP encapsulation, not all on-tree routers need hold the state for a group whose traffic they are forwarding—traffic for the group can be encapsulated (either unicast or multicast) between on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers.

¹ With IP encapsulation, not all on-tree routers need hold the state for a group whose traffic they are forwarding—traffic for the group can be encapsulated (either unicast or multicast) between on-tree routers nearer the edge of the network, reducing some of the state burden on backbone routers.

² For slow links, a set of mechanisms has been defined that helps minimize serialisation and link access delays [2,18].

² For slow links, a set of mechanisms has been defined that helps minimize serialisation and link access delays [2,18].

¹ With reservations there may be ways to avoid this too, but they're somewhat more difficult given the more specific nature of a reservation.

³ With reservations there may be ways to avoid this too, but they're somewhat more difficult given the more specific nature of a reservation.

⁵ There is some confusion on the term session, which is sometimes used for a conference and sometimes for a single media stream transported by RTP. In this paper, we prefer to use the less ambiguous term conference except where existing protocols use the term session.

⁵ There is some confusion on the term session, which is sometimes used for a conference and sometimes for a single media stream transported by RTP. In this paper, we prefer to use the less ambiguous term conference except where existing protocols use the term session.

⁴ Note that a conference policy that restricts conference membership can be implemented using encryption and restricted distribution of encryption keys, of which more later.

⁴ Note that a conference policy that restricts conference membership can be implemented using encryption and restricted distribution of encryption keys, of which more later.

EX1027/EX1028

Handley is not prior art.

Handley (EX1005) is not what published in Computer Networks

References

- [1] A. Ballardie, P. Francis, J. Crowcroft, "An Architecture for Scalable Inter-Domain Multicast Routing", ACM SIGCOMM 1993, pp 85-95
- [2] CCITT (Consultative Committee on International Telegraphy and Telephony). "Recommendation X.509: The Directory - Authentication Framework." 1988.
- [3] [11] ITU "Recommendation H.320", ITU, Geneva
- [4] [12] ITU "Recommendation T.124 - Generic Conference Control", ITU, Geneva.
- [13] V. Jacobson "Congestion Avoidance and Control", ACM SIGCOMM 88, August 1988
- [14] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, Feb 1993
- [15] S. McCanne, V. Jacobson and M. Vetterli, "Receiver-driven Layered Multicast". ACM SIGCOMM, August 1996, Stanford, CA, pp. 117-130.
- [16] S. McCanne, M. Vetterli, "Joint Source/Channel Coding for Multicast Packet Video". Proceedings of the IEEE International Conference on Image Processing, October, 1995. Washington, DC.
- [17] J. Moy, "Multicast Extensions to OSPF", RFC 1584, March 1994.
- [18] National Institute of Standards and Technology (NIST), "FIPS Publication 46-1: Data Encryption Standard", January 22, 1988
- [19] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992
- [20] Schooler, E., A Distributed Architecture for Multimedia Conference Control, ISI Research Report ISI/RR-91-289, November 1991. [ftp://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps](http://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps)
- [21] Schulzrinne, H., "Personal Mobility for Multimedia Services in the Internet" IMDS'96, March 4-6 1996. [ftp://ftp.fokus.gmd.de/pub/step/papers/Schu9603:Personal.ps.gz](http://ftp.fokus.gmd.de/pub/step/papers/Schu9603:Personal.ps.gz)
- [22] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson "RTP: A Transport Protocol for Real-Time Applications" RFC 1889.
- [23] D. Thaler, D. Estrin, D. Meyer, "Border Gateway Multicast Protocol", INTERNET-DRAFT, Oct 1997.

with colleagues at UCL. The earliest clear exposition of some of the ideas here was presented at ACM SIGCOMM 1994 in London by Van Jacobson.

References

- [1] A. Ballardie, P. Francis, J. Crowcroft, An architecture for scalable inter-domain multicast Routing, ACM SIGCOMM 1993, pp. 85-95.
- [2] C. Bormann, Providing Integrated Services over Low-bitrate Links, Internet-Draft draftietf-isil-islow-03.txt, Work in Progress, March 1998.
- [3] CCITT (Consultative Committee on International Telegraphy and Telephony), Recommendation X.509: The Directory - Authentication Framework, 1988.
- [4] W. Dang, Reliable file transfer in the multicast domain, University of Hawaii Technical Report, August 1993.
- [5] S. Deering, C. Partridge, D. Waitzman, Distance Vector Multicast Routing Protocol, IETF RFC 1075, November 1988.
- [6] S. Deering, Multicast routing in inter-networks and extended LANs, ACM SIGCOMM 88, August 1988, pp. 55-64 and Host Extensions for IP Multicasting, IETF RFC 1112.
- [7] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C.-G. Liu, L. Wei, An architecture for wide area multicast routing, ACM SIGCOMM 1994, London, October 1994, Computer Communications Review 24 (4) (1994) 126-135.
- [8] Estrin, Farinacci, Helmy, Thaler, Deering, Handley, Jacobson, Liu, Sharma, Wei, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, IETF RFC 2117.
- [9] S. Floyd, V. Jacobson, S. McCanne, C.-G. Liu, L. Zhang, A reliable multicast framework for light-weight sessions and application level framing, ACM SIGCOMM 1995, pp. 342-356.
- [10] M. Handley, J. Crowcroft, Network Text Editor (NTE): A scalable shared text editor for the Mbone, Proc. ACM SIGCOMM 97, Cannes, France, 1997.
- [11] M. Handley, V. Jacobson, SDP: Session Description Protocol, IETF RFC 2327, April 1998.
- [12] M. Handley, H. Schulzrinne, E. Schooler, SIP: Session Initiation Protocol, IETF Internet-Draft, Work in Progress.
- [13] M. Handley, D. Thaler, D. Estrin, The Internet Multicast

Address Allocation Architecture, IETF Internet-Draft, Work in Progress.

- [14] V. Hardman, A. Sasse, M. Handley, A. Watson, Reliable audio for use over the Internet, Proc INET '95, Hawaii, Internet Society, Reston, VA, 1995.
- [15] IRTF Research Group on Reliable Multicast, <http://www.east.isi.edu/RMRG/>.
- [16] ITU, Recommendation H.320: Narrow-band Visual Telephone Systems and Terminal Equipment, ITU, Geneva, July 1997.
- [17] ITU, Recommendation H.323: Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-guaranteed Quality of Service, ITU, Geneva, November 1996.
- [18] V. Jacobson, Congestion avoidance and control, ACM SIGCOMM 88, August 1988.
- [19] J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, IETF RFC 1421, February 1993.
- [20] S. McCanne, V. Jacobson, M. Vetterli, Receiver-driven layered multicast, ACM SIGCOMM, Stanford, CA, August 1996, pp. 117-130.
- [21] S. McCanne, M. Vetterli, Joint source/channel coding for multicast packet video, Proc. IEEE Int. Conf. on Image Processing, Washington, DC, October 1995.
- [22] J. Moy, Multicast Extensions to OSPF, IETF RFC 1584, March 1994.
- [23] National Institute of Standards and Technology (NIST), FIPS Publication 46-1: Data Encryption Standard, January 22, 1988.
- [24] R. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, April 1992.
- [25] E. Schooler, A distributed architecture for multimedia conference control, ISI Research Report ISI/RR-91-289, November 1991. [ftp://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps](http://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps)
- [26] H. Schulzrinne, Personal mobility for multimedia services in the Internet, IMDS'96, March 4-6, 1996.
- [27] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson RTP: A Transport Protocol for Real-Time Applications, IETF RFC 1889.
- [28] H. Schulzrinne, A. Rao, R. Lanphier, Real Time Streaming Protocol (RTSP), IETF RFC 2326, April 1998.
- [29] K. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoglu, D. Estrin, M. Handley, The MASC/BGMP architecture for inter-domain multicast routing, Proc. ACM SIGCOMM 98, Vancouver, Canada, September 1998.

with colleagues at UCL. The earliest clear exposition of some of the ideas here was presented at ACM SIGCOMM 1994 in London by Van Jacobson.

References

- [1] A. Ballardie, P. Francis, J. Crowcroft, An architecture for scalable inter-domain multicast Routing, ACM SIGCOMM 1993, pp. 85-95.
- [2] C. Bormann, Providing Integrated Services over Low-bitrate Links, Internet-Draft draftietf-isil-islow-03.txt, Work in Progress, March 1998.
- [3] CCITT (Consultative Committee on International Telegraphy and Telephony), Recommendation X.509: The Directory - Authentication Framework, 1988.
- [4] W. Dang, Reliable file transfer in the multicast domain, University of Hawaii Technical Report, August 1993.
- [5] S. Deering, C. Partridge, D. Waitzman, Distance Vector Multicast Routing Protocol, IETF RFC 1075, November 1988.
- [6] S. Deering, Multicast routing in inter-networks and extended LANs, ACM SIGCOMM 88, August 1988, pp. 55-64 and Host Extensions for IP Multicasting, IETF RFC 1112.
- [7] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C.-G. Liu, L. Wei, An architecture for wide area multicast routing, ACM SIGCOMM 1994, London, October 1994, Computer Communications Review 24 (4) (1994) 126-135.
- [8] Estrin, Farinacci, Helmy, Thaler, Deering, Handley, Jacobson, Liu, Sharma, Wei, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, IETF RFC 2117.
- [9] S. Floyd, V. Jacobson, S. McCanne, C.-G. Liu, L. Zhang, A reliable multicast framework for light-weight sessions and application level framing, ACM SIGCOMM 1995, pp. 342-356.
- [10] M. Handley, J. Crowcroft, Network Text Editor (NTE): A scalable shared text editor for the Mbone, Proc. ACM SIGCOMM 97, Cannes, France, 1997.
- [11] M. Handley, V. Jacobson, SDP: Session Description Protocol, IETF RFC 2327, April 1998.
- [12] M. Handley, H. Schulzrinne, E. Schooler, SIP: Session Initiation Protocol, IETF Internet-Draft, Work in Progress.
- [13] M. Handley, D. Thaler, D. Estrin, The Internet Multicast

Address Allocation Architecture, IETF Internet-Draft, Work in Progress.

- [14] V. Hardman, A. Sasse, M. Handley, A. Watson, Reliable audio for use over the Internet, Proc INET '95, Hawaii, Internet Society, Reston, VA, 1995.
- [15] IRTF Research Group on Reliable Multicast, <http://www.east.isi.edu/RMRG/>.
- [16] ITU, Recommendation H.320: Narrow-band Visual Telephone Systems and Terminal Equipment, ITU, Geneva, July 1997.
- [17] ITU, Recommendation H.323: Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-guaranteed Quality of Service, ITU, Geneva, November 1996.
- [18] V. Jacobson, Congestion avoidance and control, ACM SIGCOMM 88, August 1988.
- [19] J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, IETF RFC 1421, February 1993.
- [20] S. McCanne, V. Jacobson, M. Vetterli, Receiver-driven layered multicast, ACM SIGCOMM, Stanford, CA, August 1996, pp. 117-130.
- [21] S. McCanne, M. Vetterli, Joint source/channel coding for multicast packet video, Proc. IEEE Int. Conf. on Image Processing, Washington, DC, October 1995.
- [22] J. Moy, Multicast Extensions to OSPF, IETF RFC 1584, March 1994.
- [23] National Institute of Standards and Technology (NIST), FIPS Publication 46-1: Data Encryption Standard, January 22, 1988.
- [24] R. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, April 1992.
- [25] E. Schooler, A distributed architecture for multimedia conference control, ISI Research Report ISI/RR-91-289, November 1991. [ftp://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps](http://ftp.isi.edu/pub/hpcc-papers/mmcc/mmcc.ps)
- [26] H. Schulzrinne, Personal mobility for multimedia services in the Internet, IMDS'96, March 4-6, 1996.
- [27] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson RTP: A Transport Protocol for Real-Time Applications, IETF RFC 1889.
- [28] H. Schulzrinne, A. Rao, R. Lanphier, Real Time Streaming Protocol (RTSP), IETF RFC 2326, April 1998.
- [29] K. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoglu, D. Estrin, M. Handley, The MASC/BGMP architecture for inter-domain multicast routing, Proc. ACM SIGCOMM 98, Vancouver, Canada, September 1998.

EX1005 (Handley)

EX1027

EX1028



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Presentation of Patent Owner

Paper 44 (Sur-Reply) at 5

47

Handley is not prior art.

Crowcroft confirms “differences” and different “versions”

16. An online version of EX1028 is available at Elsevier’s ScienceDirect website (EX1027).⁸ I have compared the articles in EX1027 and EX1028 and found them fully identical. Elsevier’s ScienceDirect states that EX1027 was available online as of June 9, 1999.⁹ Further, I have performed a side-by-side comparison of EX1005 to EX1027 and EX1028 and confirm the substance is virtually identical. While slight differences are apparent, they do not detract from the underlying technical teachings of the article. In my opinion, as a co-author, the technical substance of EX1005, EX1027, and EX1028 are identical.

EX1016 (Crowcroft Decl.) ¶16

17. It was common practice for me, as an author and academic, to upload papers, publications, and articles to my personal academic website as well as the FTP server prior to formal publication. As background, the authors of EX1005 were all active participants in the Internet Engineering Task Force (IETF) working on Internet Standards. Draft versions of these documents, like EX1005, were frequently exchanged and updated as part of that work, and typically made available through public FTP (later WWW) servers. It was also part of the culture to publish more research-oriented versions of the work as papers in the regular academic press (conferences and journals). The Internet standards process has always promoted open access to work, and much of communications research has followed that convention.

EX1016 (Crowcroft Decl.) ¶17

Paper 44 (Sur-Reply) at 5-6



Handley is not prior art.

Houh confirms EX1005 is a different “version”

13. I understand from personal knowledge and experience, as an academic and author myself, and based on knowledge provided to me by colleagues in the field, including publishers, other academics, and librarians, that authors routinely post articles or papers on their personal or academic websites prior to submitting them to conferences and journals or during the process of journal publication. These versions, typically linked to a web page maintained by the author and publicly available free of charge, are the basis for the published versions. These published versions may contain additional edits and citations as requested by editors or publishers. In my opinion, this is the scenario that occurred with respect to EX1005. I have reviewed Dr. Crowcroft’s declaration, EX1016, and my opinion is consistent with his understanding of the series of events leading to the publication of EX1027 and EX1028. Namely, Dr. Crowcroft posted EX1005 on his academic website, which was subsequently edited by the publisher before being formally published in COMPUTER NETWORKS Volume 31, Issue 3, and is virtually identical in substance as well as identical for the portions relied upon in the petition and my declaration.

EX1017 (Houh Supp. Decl.) ¶13

Paper 44 at 6



Handley is not prior art.

Alternative “UCL website” and “FTP” theories are waived

“Before the Board, Samsung did not argue that the WD4 reference was publicly accessible because it was discussed at the Torino meeting or disseminated at the Geneva meeting. ... Thus, Samsung waived any separate argument on appeal that the WD4 reference was publicly accessible because it was disseminated at the Torino or Geneva meetings.”

Samsung Elecs. Co. v. Infobridge Pte. Ltd., 929 F.3d 1363, 1369-70 (Fed. Cir. 2019)



“We agree with Patent Owner that Petitioner’s argument in Section II.C. of its opening brief is a new argument or theory of public disclosure that was not raised in the Petition and, therefore, is waived. See *Ariosa*, 805 F.3d at 1367. As the Federal Circuit found, Samsung argued in the Petition that WD4 was publicly accessible because it was uploaded to the JCT-VC and MPEG websites and emailed to the JCT-VC listserv. See *Samsung*, 929 F.3d at 1369–1373. ... We determine that this is a new argument or theory because the argued dissemination is not based on the listserv email, but on post-listserv email ‘secondary distribution’ that may have occurred with respect not only to WD4, but also ‘other versions of Working Draft 4.’ Accordingly, Petitioner’s new ‘public dissemination’ argument is waived.”

Samsung Elecs. Co. v. Infobridge Pte., Ltd., IPR2017-00099, Paper 43 at 42 (PTAB Nov. 13, 2020)



Handley is not prior art.

The Petition does not argue disclosure by “UCL website” or “FTP”

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the *Computer Networks* journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

59. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the *Computer Networks* journal. Handley provides an

EX1003 (Houh Decl.) ¶59

Paper 44 (Sur-Reply) at 7; Paper 26 (POR) at 19



Handley is not prior art.

Liquidia does not support consideration of theories not disclosed in the petition

accessible. PO Resp. 11–18. The argument that Voswinckel JESC was publicly presented is not a change in theory from the Petition, because Petitioner presented this argument in the Petition. Pet. 22. As to both Voswinckel JESC and Voswinckel JAHA, Petitioner’s Reply evidence showing citation to the references in other publicly accessible documents is merely additional evidence supporting Petitioner’s original theory that a person of ordinary skill in the art could have located the references. Accordingly, we find that the following arguments made by Petitioner are not untimely: (1) that Voswinckel JESC was presented publicly, (2) that Voswinckel JESC was referenced in a publicly accessible document, and (3) that Voswinckel JAHA was referenced in a publicly accessible document.

Liquidia Technologies, Inc. v. United Therapeutics Corp., IPR2021-00406, Paper 78 at 10 (PTAB Jul. 19, 2022)



“As the Board recognized, Liquidia’s IPR petition asserted that each of the Voswinckel abstracts was publicly presented or published at least one year before the priority date of the ’793 patent, making each of them printed publications within the meaning of § 102(b). ...

“ ... As the Board observed, Liquidia’s arguments were not inconsistent with, and therefore not new over, the grounds raised in its IPR petition—that the Voswinckel abstracts were publicly accessible prior to the critical date.”

United Therapeutics Corp. v. Liquidia Techs., Inc., 2023 WL 8794633, at *3 (Fed. Cir. Dec. 20, 2023)



Paper 44 (Sur-Reply) at 7

Handley is not prior art.

Disclosure by “UCL website” or “FTP” is *inconsistent* with the Petition’s theory

1. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, published February 11, 1999, in the *Computer Networks* journal. Handley is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 4

59. **Handley (EX1005)** – *Very Large Conferences on the Internet: The Internet Multimedia Conferencing Architecture and the MBONE*, was published February 11, 1999, in the *Computer Networks* journal. Handley provides an

EX1003 (Houh Decl.) ¶59

Examples of indications that a new issue has been raised in a reply include new evidence necessary to make out a *prima facie* case for the patentability or unpatentability of an original or proposed substitute claim, such as newly raised rationale to combine the prior art references that was not expressed in the petition. See *Intelligent Bio-Sys., Inc. v. Illumina*

Consolidated Trial Practice Guide (Nov. 2019) at 74

“In these circumstances, we find that the Board did not err in refusing the reply brief as improper under 37 C.F.R. § 42.23(b) because IBS relied on an entirely new rationale to explain why one of skill in the art would have been motivated to combine Tsien or Ju with a modification of Zavgorodny.”

Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd., 821 F.3d 1359, 1369–70 (Fed. Cir. 2016)

Paper 44 (Sur-Reply) at 7-8; Paper 26 (POR) at 19



Handley is not prior art.

The “UCL website” and “FTP” theories fail to meet Petitioners’ burden

“A reference is considered publicly accessible if it was ‘disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’ As petitioner, Blizzard had the burden to prove Lin is a printed publication.”

Acceleration Bay, LLC v. Activision Blizzard Inc., 908 F.3d 765, 772
(Fed. Cir. 2018) (cleaned up).

“The Board then correctly noted that ‘public accessibility’ requires more than technical accessibility.”

Acceleration Bay, LLC v. Activision Blizzard Inc., 908 F.3d 765, 773-74
(Fed. Cir. 2018).

Handley is not prior art.

Petitioners fail to show the POSITA would have located Handley on the UCL website

“In the present case, the Board found that Groupon had failed to carry its burden of establishing that an interested party exercising reasonable diligence would have located Ratsimor. We agree. Groupon has provided no evidence that Ratsimor was disseminated to the interested public before the critical date other than testimony from Dr. Joshi that it was ‘publicly available around November 2003.’ Even if we assume that Ratsimor was available online on Dr. Ratsimor’s personal page before the critical date, Groupon does not point to any evidence indicating that Ratsimor was viewed or downloaded. Further, in contrast to *Voter Verified*, the present case lacks any testimonial evidence that a person interested in e-commerce and peer-to-peer marketing would be independently aware of the web address for Dr. Ratsimor’s personal page. In other words, there was no evidence that the ordinarily skilled artisan would know of Dr. Ratsimor’s personal webpage or its web address.”

Blue Calypso, LLC v. Groupon, Inc., 815 F.3d 1331, 1349-50 (Fed. Cir. 2016).

Handley is not prior art.

Petitioners fail to show the POSITA would have located Handley on the FTP

“The record on summary judgment does not show that an **anonymous user skilled in the art in 1997** would have gained access to the FTP server and would have freely navigated through the directory structure to find the Live Traffic paper.”

SRI Int’l, Inc. v. Internet Sec. Sys., Inc., 511 F.3d 1186, 1196-97 (Fed. Cir. 2008)

Handley is not prior art.

Petitioners' evidence is insufficient as a matter of law

“Taken together, these cases suggest that a work is not publicly accessible if the only people who know how to find it are the ones who created it. This is why *SRI* focused on the knowledge of those outside the authoring organization and why *Bayer* discounted the knowledge of various professors on a faculty committee reviewing student theses. To hold otherwise would disincentivize collaboration and depart from what it means to publish something.”

Samsung Elecs. Co. v. Infobridge Pte. Ltd., 929 F.3d 1363, 1372 (Fed. Cir. 2019)

Handley Is Not Prior Art

The “teachings” of Handley are not printed publications

“In *MIT*, a paper delivered orally to the First International Cell Culture Congress was considered a ‘printed publication.’ In that case, as many as 500 persons having ordinary skill in the art heard the presentation, and at least six copies of the paper were distributed. The key to the court’s finding was that actual copies of the presentation were distributed. The court did not consider the issue of indexing. The *MIT* court determined the paper in question to be a “printed publication” but did not limit future determinations of the applicability of the “printed publication” bar to instances in which copies of a reference were actually offered for distribution. *MIT*, 774 F.2d at 1108–10.⁴”

“⁴ With regard to scientific presentations, it is important to note that an entirely oral presentation at a scientific conference that includes neither slides nor copies of the presentation is without question not a “printed publication” for the purposes of 35 U.S.C. § 102(b). ...”

In re Klopfenstein, 380 F.3d 1345, 1349 (Fed. Cir. 2004)

Paper 44 (Sur-Reply) at 9-10



Handley is not prior art.

EX1027 and EX1028 cannot stand in for Handley

“Based on this record, we conclude that substantial evidence supports the Board’s determination that Zodiac did not satisfy its burden of establishing that **the version of the Orange Book in the record** was publicly accessible. The nature of the Orange Book focuses our inquiry on whether **the version of the Orange Book containing the relevant schematic** was publicly accessible. ... In short, nothing in the record demonstrates that “persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence” could have located **the relevant version of the Orange Book** before the priority date. *See In re Lister*, 583 F.3d at 1311.”

B/E Aerospace, Inc. v. C & D Zodiac, Inc., 709 F. App’x 687, 698 (Fed. Cir. 2017)

PACKETCABLE IS NOT PRIOR ART

PacketCable Is Not Prior Art

Petition

3. **PacketCable (EX1007)** – *PacketCable 1.0 Architecture Framework Technical Report*, published December 1, 1999. PacketCable is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 3 (Petition) at 5

C. PacketCable

61. PacketCable (EX1007) – *PacketCable 1.0 Architecture Framework Technical Report*, was published December 1, 1999. Cable Television

EX1003 (Houh Decl.) ¶61

Paper 26 (POR) at 40; Paper 44 (Sur-Reply) at 10



PacketCable Is Not Prior Art

Reply

PO's contention that the Petition does not show *PacketCable* (EX1007) qualifies as prior art defies *PacketCable's* indicia, Dr. Hall-Ellis' Declaration, and the Board's findings. POR, 40-42. *PacketCable* includes reliable indicia of publication on its face, including a 1999 copyright date, a December 1, 1999 release date, and consecutive "12/01/99" footer date stamps. Regardless of whether

Paper 37 (Reply) at 2-3

release date, and consecutive "12/01/99" footer date stamps. Regardless of whether *PacketCable* is a technical report or standard, it states "[t]his *PacketCable* technical report is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry." EX1007, 1. As described in Petitioners' Reply to POPR, a standard's purpose is to be adopted and infers public accessibility. See Paper 14, 3. The Board found *PacketCable's* indicia "further corroborate Petitioner's sufficient showing for institution that CableLabs intended to disseminate the document at least to the listed member companies of the project and artisans of ordinary skill in those companies seeking to design and/or sell applicable networks." Paper 16, 27. Dr. Hall-Ellis, "a librarian with over 50 years of experience," confirmed *PacketCable* was publicly available no later than December 1, 1999. See, e.g., EX1019; Paper 16, 18. *PacketCable* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 44 (Sur-Reply) at 12-13



PacketCable Is Not Prior Art

Notice

This PacketCable **technical report** is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

EX1007 at 1

“Instead, Groupon argues that an internet search engine would have been able to locate the report. But **that argument does not allow us to automatically infer** that Dr. Ratsimor’s webpage was ‘indexed . . . (through search engines or otherwise)’ and thus **locatable** by a search engine. *See Voter Verified*, 698 F.3d at 1381. **The record is devoid of any evidence** that a query of a search engine before the critical date, using any combination of search words, would have led to Ratsimor appearing in the search results.”

Blue Calypso, LLC v. Groupon, Inc., 815 F.3d
1331, 1349-50 (Fed. Cir. 2016)

Paper 26 at 42; Paper 44 (Sur-Reply) at 10-11



PacketCable is not prior art.

Hall-Ellis's 12/1/1999 "release date" theory fails to meet Petitioners' burden

to design and/or sell applicable networks." Paper 16, 27. Dr. Hall-Ellis, "a librarian with over 50 years of experience," confirmed *PacketCable* was publicly available no later than December 1, 1999. *See, e.g.*, EX1019; Paper 16, 18. *PacketCable* is at least pre-AIA 35 U.S.C. §§102(a) and 102(b) prior art.

Paper 37 at 2-3

18. Exhibit 1007 is a document titled *PacketCable™ 1.0 Architecture Framework Technical Report* prepared by the Cable Television Laboratories staff. The document is identified as PKT-TR-ARCH-V01-991201 (as shown on the cover of Exhibit 1007) and the "Document Status Sheet" (as indicated on page 3 of Exhibit 1007). The "Document Status Sheet" indicates a December 1, 1999, release date.

20. Exhibit 1007 is a true and correct copy in a condition that creates no suspicion about its authenticity. Based on the date recorded in the document, it is my opinion that the document titled *PacketCable™ 1.0 Architecture Framework Technical Report* was available to the public by at least December 1, 1999.

EX1019 (Hall-Ellis Decl.) ¶¶18, 20

Paper 44 (Sur-Reply) at 10-11



PacketCable is not prior art.

Hall-Ellis's only evidence of accessibility is the *current* CableLabs website

19. Exhibit 1007 is a true and accurate copy of the document titled *PacketCable™ 1.0 Architecture Framework Technical Report* that was and issued “... for the benefit of the cable industry” (page 1). The technical report is available from the Cable Television website.⁶ I obtained the document filed as Exhibit 1007 from the Cable Television website. Specifically, the text of the document titled *PacketCable™ 1.0 Architecture Framework Technical Report* is complete; no pages are missing, and the text on each page appears to flow seamlessly from one page to the next; further, there are no visible alterations to the document. Exhibit 1007 was found within the custody of the issuing agency – a place where, if authentic, a copy of this federal document would likely be.

6

<https://community.cablelabs.com/wiki/plugins/servlet/cablelabs/alfresco/download?id=bddae471-01dd-43c8-8e59-d6547fcf4ffd>

“Groupon has provided no evidence that Ratsimor was disseminated to the interested public before the critical date”

Blue Calypso, LLC v. Groupon, Inc., 815 F.3d
1331, 1349 (Fed. Cir. 2016)

EX1019 (Hall-Ellis Decl.) ¶19

Paper 44 (Sur-Reply) at 11



PacketCable is not prior art.

Hall-Ellis checked but found no evidence of online availability at the relevant time

14 Q. Well, my question was, do you have
15 any evidence that PacketCable was available on a
16 website as of December 1st, 1999?

17 A. Only the website for the company.
18 So, nothing else, no.

19 Q. Well, did you try to -- have you
20 ever heard of the Wayback Machine?

21 A. I am very familiar with the Wayback
22 Machine. The websites that are on it are

1 archived, something is currently on the internet,
2 it is not in the Wayback Machine.

3 Q. Did you ever check if the
4 PacketCable reference was on the Wayback Machine
5 as of December 1st, 1999?

6 A. I always check.

7 Q. And was it there?

8 A. No.

EX2009 (Hall-Ellis Dep. Tr.) at 25:14-26:8

Paper 44 (Sur-Reply) at 11



PacketCable is not prior art.

Hall-Ellis checked but found no evidence of online availability at the relevant time

13 Q. Okay. And have you seen any
14 evidence whatsoever that PacketCable reference
15 was online in 1999 other than the date printed on
16 the paper?

17 A. I do see on their current website
18 the revision of this document and an indication
19 that December 1st, 1999, was the release date of
20 the document that we are describing as 1007.

EX2009 (Hall-Ellis Dep. Tr.) at 28:13-20

7 Q. Okay. And you know that PacketCable
8 wasn't on the Wayback Machine on December 1st,
9 1999, correct?

10 MR. BAKER: Objection, asked and
11 answered.

12 THE WITNESS: That is correct.

EX2009 (Hall-Ellis Dep. Tr.) at 32:7-12



PacketCable is not prior art.

Hall-Ellis checked but found no evidence of online availability at the relevant time

22 Q. Okay. And have you seen any
1 evidence specifically showing that in 1999 Cable
2 Television Laboratories was publishing its
3 documents online?

4 A. I have seen nothing to the contrary.

5 Q. Could you please answer my question?

6 A. I have seen nothing to the contrary.

7 That is my answer.

8 Q. Have you seen anything affirmatively
9 supporting that in 1999 Cable Television
10 Laboratories was releasing its documents online?

11 A. I think I have answered that. And I
12 have nothing else to say about that.

13 Q. Okay. I am understanding from that
14 that you have no evidence. But please correct me
15 if I'm wrong.

16 A. I have nothing else to say about
17 that.

EX2009 (Hall-Ellis Dep. Tr.) at 29:22-30:17

Paper 44 (Sur-Reply) at 11



PacketCable is not prior art.

Hall-Ellis performed a “pretty thorough search” but found no evidence of availability anywhere at the relevant time

13 Q. Besides the Wayback Machine, did you
14 do any other investigation to try to determine if
15 PacketCable was available on a website back in
16 December, 1999?

17 A. Yes, I did.

18 Q. What did you do?

19 A. I know it is not in WorldCat. I
20 know that typing the title of the document into a
21 web browser brings up this site. And that is
22 where it is at Cable Labs.

1 And it is not anywhere else that I
2 can find.

3 So, you know, I do a pretty thorough
4 search for documents, that is my practice, that
5 is my procedure. I write about what I can
6 identify, not what I can't identify.

7 Q. What is WorldCat?

8 A. WorldCat is the public interface for
9 the OCLC bibliographic database.

10 Q. Okay. And why would you search
11 WorldCat?

12 A. If this item were in a library,
13 anywhere in the world in any language, the
14 probability is about 99 percent that it would be
15 in that database, and it is not there.

EX2009 (Hall-Ellis Dep. Tr.) at 36:13-37:15

Paper 44 (Sur-Reply) at 11



PacketCable Is Not Prior Art

PacketCable Was Not Catalogued, Indexed, or in a Library

9 Q. Are you aware of any indexing or
10 cataloguing of PacketCable in December 1999?

11 A. I think I said before, I looked in
12 WorldCat. This is not the kind of document you
13 would find in a library.

14 You might find it in a corporate
15 library, which would be closed to the public, for
16 people doing work that would be embargoed or
17 would be held as corporate confidential, you
18 might find it in those places.

19 But again, there would be a reason
20 for that. I think we talked about money has a
21 role in all of this.

22 But in a general library, no. This
1 is not the kind of document. If it were in a
2 library, it would probably not be there now
3 anyway because this document had been superceded.

4 And because of that, unless
5 libraries have more space than any I know, the
6 newer version would have replaced the older
7 version. So there would only be a newer one
8 available.

9 Q. What do you mean this -- well, thank
10 you for explaining your answer. But, I think I
11 understood you to agree that there was no
12 indexing or cataloguing of PacketCable back in
13 December 1999.

14 A. No, because I looked. And I can
15 find records for materials from the 19th century
16 in WorldCat, and I can't find this.

17 So, no. No cataloguing, no
18 indexing, and no library presence that I can
19 identify.

EX2009 (Hall-Ellis Dep. Tr.) at 50:9-51:19

Paper 44 (Sur-Reply) at 11



PacketCable is not prior art.

Hall-Ellis' opinion is based on the word "release"

18. Exhibit 1007 is a document titled *PacketCable™ 1.0 Architecture Framework Technical Report* prepared by the Cable Television Laboratories staff. The document is identified as PKT-TR-ARCH-V01-991201 (as shown on the cover of Exhibit 1007) and the "Document Status Sheet" (as indicated on page 3 of Exhibit 1007). The "Document Status Sheet" indicates a December 1, 1999, **release date**.

EX1019 (Hall Ellis Decl.) ¶18

8 Q. **And so is Page 3 of PacketCable, is**
9 **that your basis for saying in Paragraph 18 that**
10 **there is indicated December 1st, 1999 release**
11 **date?**
12 A. Well, that is certainly is the first
13 indication of the date.
14 And it makes sense. And, to me, it
15 is highly likely that the organization knows the
16 date it released the document. **And they have**
17 **stated that, therefore, that date to me makes**
18 **sense.**

EX2009 (Hall-Ellis Dep. Tr.) at 17:8-18 Paper 44 (Sur-Reply) at 11-12

PKT-TR-ARCH-V01-991201 PacketCable™ 1.0 Architecture Framework Technical Report

Document Status Sheet

Document Control Number: PKT-TR-ARCH-V01-991201
Document Title: PacketCable™ 1.0 Architecture Framework Technical Report
Revision History: D01-991201: **release**
Date: December 1, 1999

EX1007 at 3



PacketCable is not prior art.

PacketCable does not say what “release” means

19 Q. Okay. And what is, does the
20 PacketCable reference say anything about what it
21 means for the document to be released?
22 A. Well, it doesn't say that
1 specifically.

EX2009 (Hall-Ellis Dep. Tr.) at 17:19-18:1

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis has no personal knowledge of CableLabs' release policies/process

4 Q. Do you have any personal knowledge
5 of the policies for releasing technical documents
6 of Cable Television Laboratories?

7 A. That is an interesting question.
8 When I got this document, I took a look at the
9 website of this organization for a couple of
10 reasons.

11 One is they are down the road from
12 me about 30 miles. They are not very far away.

13 And they are not particularly
14 interested in interacting with the public but
15 they have been around quite a long time.

16 And their work is critical in the
17 cable television industry.

18 So, I did some reading about them,
19 although I have not worked there.

EX2009 (Hall-Ellis Dep. Tr.) at 19:4-19

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis has no personal knowledge of CableLabs' release policies/process

21 You don't have any personal
22 knowledge of Cable Television Laboratories'
1 processes for releasing its technical documents,
2 correct?
3 A. No.
4 Q. And that is true today and that was
5 also true in 1999, correct?
6 A. I'm not sure I had heard of this
7 place in 1999.

8 Q. And you are not, you don't have
9 personal knowledge of Cable Television
10 Laboratories' processes for releasing technical
11 documents back in 1999, correct?
12 A. The only information I have about
13 that, which I think I have already said, is based
14 on their description of their mission and their
15 work as expressed on their internet site.

EX2009 (Hall-Ellis Dep. Tr.) at 37:21-38:15

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis did not research CableLabs' release procedures

9 Q. Okay. Okay. And let me ask you,
10 did you do any research into what PacketCable's
11 procedures were for releasing technical documents
12 in the 1999-2000 time frame?
13 A. Specifically -- well, we are dancing
14 around the issue. So I would say specifically to
15 that question, no.

EX2009 (Hall-Ellis Dep. Tr.) at 20:9-15

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis does not know who or how many people wrote PacketCable

9 Q. Okay. Do you know who at Cable
10 Television Laboratories wrote this document?
11 A. No, an individual, no, I don't.
12 Q. Do you know how many people wrote
13 this document, I say this document, let me say --
14 A. No.
15 Q. And let me re-ask that a little
16 better to make sure I get a better answer.
17 We are going to be talking a lot
18 about this PacketCable reference which is
19 Exhibit 1000 --
20 A. No, I don't know.

EX2009 (Hall-Ellis Dep. Tr.) at 11:9-20

10 Q. But, do you know how many people
11 wrote the PacketCable reference?
12 A. I do not know.
13 Q. Okay. And your knowledge about who
14 prepared PacketCable comes from what is written
15 in PacketCable, correct?
16 A. I believe they know that. And yes,
17 they are forthcoming and putting that information
18 on the front of the document.
19 Q. And it is not that you have any of
20 your own personal knowledge about who drafted
21 PacketCable, correct?
22 A. I do not know who did it, no.

EX2009 (Hall-Ellis Dep. Tr.) at 12:10-22

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis does not know of any CableLabs members

18 Q. Do you know who the member companies
19 of Cable Television Laboratories were in
20 December 1999?
21 A. No.
22 Q. Do you know any people who were
1 members of Cable Television Laboratories in
2 December 1999?
3 MR. BAKER: Objection, outside of
4 the scope of direct.
5 THE WITNESS: I do not. And it is
6 my understanding this is an institutional
7 organizer, organizational membership group,
8 not individuals per se.

EX2009 (Hall-Ellis Dep. Tr.) at 30:18-31:8

Paper 44 (Sur-Reply) at 12



PacketCable is not prior art.

Hall-Ellis' speculation about the release of PacketCable is insufficient

“The government urges us that it is appropriate in this case to presume that the manuscript information was added to the Westlaw and Dialog databases prior to the critical date because the critical date was more than a year after the certificate of registration was granted. However, absent any evidence pertaining to the general practices of the Copyright Office, Westlaw, and Dialog, or the typical time that elapses between copyright registration, inclusion in the Copyright Office's automated catalog, and subsequent incorporation into one of the commercial databases, any presumption along those lines would be pure speculation.”

In re Lister, 583 F.3d 1307, 1317 (Fed. Cir. 2009)

PacketCable is not prior art.

Hall-Ellis' speculation about the release of PacketCable is insufficient

“Although there was testimony that it was the general practice at IADR meetings for presenters to hand out abstracts to interested attendees, the lack of substantial evidence of actual availability of the Abstract adequately supports the court’s conclusion that dissemination of the Abstract was not established. That holding is affirmed.”

Norian Corp. v. Stryker Corp., 363 F.3d 1321, 1330 (Fed. Cir. 2004)

PacketCable is not prior art.

No evidence PacketCable was locatable by the POSITA before January 18, 2000

11 Do you know what I'm referring to
12 when I say the person of ordinary skill in the
13 art?
14 A. I do know that term, yes.

EX2009 (Hall-Ellis Dep. Tr.) at 52:11-14

13 Q. Were you -- did you have the
14 qualifications of a person of ordinary skill in
15 the art as of December 1999?
16 A. Oh, no, I have never had these, no.
17 Q. Okay.
18 A. No.

EX2009 (Hall-Ellis Dep. Tr.) at 55:13-18

Paper 44 (Sur-Reply) at 13



PacketCable is not prior art.

No evidence the POSITA would have been directed to PacketCable

20 Q. Did you find any evidence of other
21 websites or resources directing people to the
22 PacketCable reference as of December 1999?

1 A. I did not look for that and I had no
2 reason to do so.

3 Q. Okay. And I think this is
4 probably -- it is obvious from what you say, but
5 I will ask it anyway, you didn't look for that
6 type of evidence and you are also not aware of
7 any of that type of evidence, correct?

8 A. That is correct.

EX2009 (Hall-Ellis Dep. Tr.) at 51:20-52:8

Paper 44 (Sur-Reply) at 13



PacketCable is not prior art.

PacketCable's copyright date does not indicate public accessibility

accessible by a particular date. As discussed above, the September 2012 date, like the legend copyright notice, sheds virtually no light on whether the document was publicly accessible prior to November 1, 2012. Additional evidence thus is necessary to support a showing of public accessibility. See, e.g., *Ford Motor Co. v. Cruise Control Techs. LLC*, Case IPR2014-00291, slip op. at 9–10 (PTAB June 29, 2015) (Paper 44) (discussing evidence of public accessibility that supported a finding that a reference was a prior art printed publication).

In-Depth Geophysical, Inc. v. Conocophillips Co.,
IPR2019-00849, Paper 14 at 9-11 (PTAB Sept. 6, 2019)

12 Q. Is there any other investigative
13 work that you did that is not in your
14 supplemental declaration that we haven't already
15 discussed?
16 A. No. I, I generally look in, you
17 know, a pretty standard list of places.
18 And this one just doesn't appear in
19 things like, when it is not in WorldCat and it is
20 not in the database at the copyright office. And
21 it is only one site that comes up on a web
22 browser.

EX2009 (Hall-Ellis Dep. Tr.) at 57:12-22

Paper 44 (Sur-Reply) at 13



Ground 1: Obviousness over Handley + Basturk

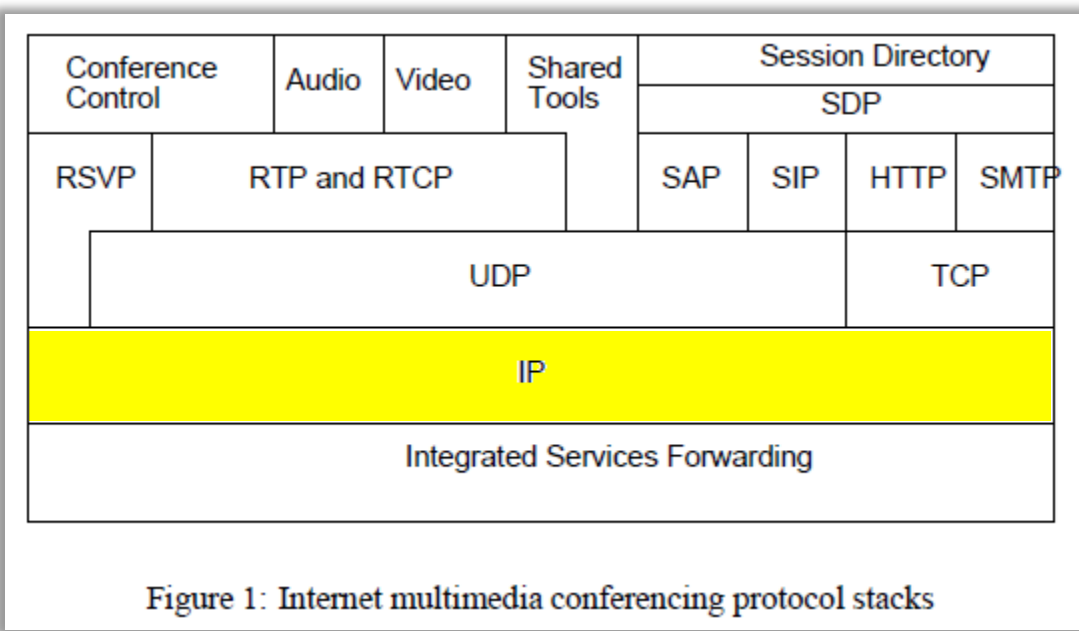
Ground	Assertion	Petitioned Claims
1	Obvious under § 103 in view of Handley in combination with Basturk	1-21, 23, 25-28
2	Obvious under § 103 in view of PacketCable in combination with Handley	1-28
3	Obvious under § 103 in view of PacketCable in combination with Basturk	1-28
4	Obvious under § 103 in view of Handley in combination with Basturk and PacketCable	22, 24

Paper 3 (Petition) at 5



Handley: Overview

IP Multicast distribution through “routers”



EX1005 (Handley) at 3

3 Multicast Traffic Distribution

IP multicast provides efficient many-to-many data distribution in an internet environment. It is easy to view IP multicast as simply an optimisation for data distribution, and indeed this is the case, but IP multicast can also result in a different way of thinking about application design. To see why this might be the case, examine the IP multicast service model, as described by Van Jacobson[7]:

EX1005 (Handley) at 2

- Senders just send to *the group*
- Receivers express an interest in receiving data sent to *the group*
- Routers conspire to deliver data from senders to receivers

With IP multicast, the group is indirectly identified by a single IP class-D multicast address.

Several things are important about this service model from an architectural point of view. *Receivers do not need to know who or where the senders are* to receive traffic from them. *Senders never need to know who the receivers are.* Neither senders or receivers need care about the network topology as the network optimises delivery.

EX1005 (Handley) at 3

Handley: Overview

“real-time” traffic v. “non-real-time” traffic

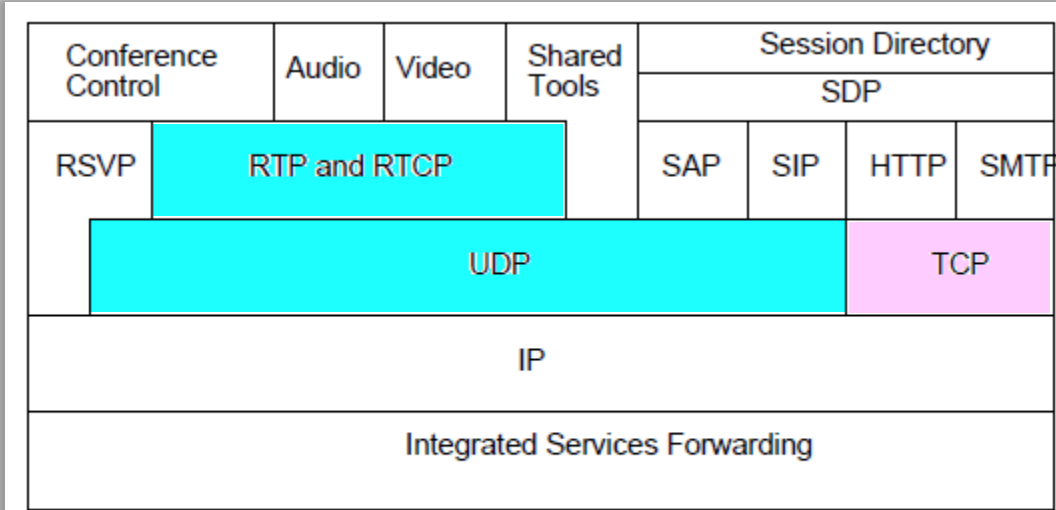


Figure 1: Internet multimedia conferencing protocol stacks

EX1005 (Handley) at 3

4.1 Non-best effort service

Real-time internet traffic is defined as datagrams that are delay sensitive. It could be argued that all datagrams are delay sensitive to some extent, but for these purposes we refer only to datagrams where exceeding an end-to-end delay bound of a few hundred milliseconds renders the datagrams useless for the purpose they were intended. For the purposes of this definition, TCP traffic is normally not considered to be real-time traffic, although there may be exceptions to this rule.

EX1005 (Handley) at 5

Although best-effort services can support real-time traffic, classifying real-time traffic separately from non-real-time traffic and giving real-time traffic priority treatment ensures that real-time traffic sees minimum delays. Non-real-time TCP traffic tends to be elastic in its bandwidth requirements, and will then tend to fill any remaining bandwidth.

EX1005 (Handley) at 5

5.2 RTP

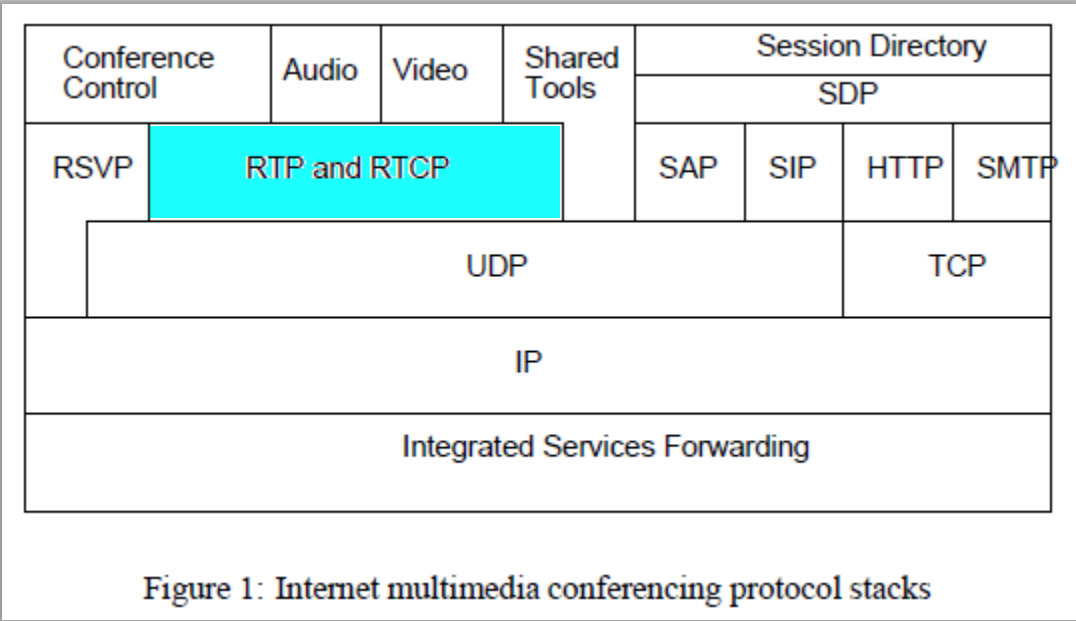
The transport protocol for real-time flows is RTP[22]. This provides a standard format packet header which gives media specific timestamp data, as well as payload format information and sequence numbering amongst other things. RTP is normally carried using UDP. It does not provide or require any connection setup, nor does it provide any enhanced reliability over UDP. For RTP to provide a useful media flow, there

EX1005 (Handley) at 8

Paper 26 (POR) at 5-6

Handley: Overview

No authentication at the RTP packet level



EX1005 (Handley) at 3

5.2 RTP

The transport protocol for real-time flows is RTP[22]. This provides a standard format packet header which gives media specific timestamp data, as well as payload format information and sequence numbering amongst other things. RTP is normally carried using UDP. It does not provide or require any connection setup, nor does it provide any enhanced reliability over UDP. For RTP to provide a useful media flow, there

EX1005 (Handley) at 8

RTP specifies a standard way to encrypt RTP and RTCP packets using private key encryption schemes such as DES[18]. It also specifies a standard mechanism to manipulate plain text keys using MD5[19] so that the resulting bit string can be used as a DES key. This allows simple out-of-band mechanisms such as privacy-enhanced mail to be used for encryption key exchange.

EX1005 (Handley) at 12

EX1006, 4 n. 3. But the combination Petitioners put forth does not duplicate functions because Handley does not disclose the use of a MAC or signatures and any checksums in different protocol layers used in Handley are not for the purpose of authentication. EX1033, ¶39.

Paper 37 (Reply) at 14

Paper 26 (POR) at 6; Paper 44 (Sur-Reply) at 19-21

Basturk: Overview

Basturk's transport level protocol provides transport level security

Abstract

We argue that the increasingly widespread use of networks is leading to new security concerns such as *secure delivery* which are most naturally associated with the transport level and best addressed by the design of *secure transport protocols*. We present general methods for such a design which are directed at optimizing performance on a *high speed* network. Our work reflects the experience gained in designing and implementing a particular secure transport protocol.

EX1006 (Basturk) at 1

Paper 26 (POR) at 6



Basturk: Overview

Basturk's transport level protocol provides transport level security

1 Introduction

As we entrust more and more of our communication to networks, the concern with security increases. This paper begins by arguing that the *nature* of the security guarantees which users will need and expect is changing. In particular, new requirements, like *secure delivery*, are emerging. In contrast to traditional security features which tend to be purely application level, the new ones are most naturally identified with the transport level. We suggest the design of secure transport protocols as the most effective way of filling all needs, and present a general method to transform a given transport protocol into a secure one. The design puts particular emphasis on maintaining the level

EX1006 (Basturk) at 3

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure. To this end, we distinguish security features according to the layer of the communication structure to which they are most naturally associated. We found that the traditional features are mostly application level, while the new ones we deem necessary are transport level.

EX1006 (Basturk) at 3

Paper 26 (POR) at 6-7

Basturk: Overview

Basturk's transport level protocol provides transport level security

TRANSPORT LEVEL SECURITY. In this design, the application passes its key *a* to the transport module, and leaves to the latter the task of applying any cryptographic functions or taking other security steps. The advantage is that the transport module can compute a signature which covers not only the data but also (relevant parts of) the transport header which it creates, particularly the byte sequence numbers. It can also sign the acknowledgments messages which exist only at the transport level. As we will see, these possibilities are key to the provision of secure delivery.

EX1006 (Basturk) at 4-5

Paper 26 (POR) at 7



Basturk: Overview

Basturk's protocol requires a transport-level session key α

ELEMENTS OF THE SOLUTION. The design will be specified in full in the body of the paper, but here is a brief sketch. The secure transport protocol has two phases, the *initialization* phase and the *steady state*. In the former, an *entity authentication and key exchange* protocol is executed. This authenticates the parties and yields them a *session key α* . In the steady state, if the integrity option is selected, both data integrity and secure delivery are provided by attaching to each packet a signature, computed under key α , and taken over some portions of the header and the data payload. Note that acknowledgments, which have no data, are also signed. If confidentiality is desired, the data is encrypted, also under α . See the rest of the paper for more details on which parts of the header must be signed and which left in the clear; why the design guarantees secure delivery; and also for explanations on why a session key is needed when the parties already share the long lived key a .

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. Applications using the regular transport protocol should not have to be modified at all.

EX1006 (Basturk) at 5

Paper 26 (POR) at 6-8



Basturk: Overview

“transport machines” M_A and M_B apply the cryptographic functions

CONNECTION INITIATOR INTERFACE. Now suppose A wishes to initiate a connection with B , with whom it shares LL-key a . It interfaces with a local piece of software to which it passes the identity B and the key a . It can also control the nature and strength of the security to be provided by specifying some options which will be discussed below. This software creates for her an entity we call her *secure transport machine* and denote by M_A . Once initialized, A can send (and receive) data via the secure transport machine just as it would via the original (insecure) version. That is, when it wants to send a message m , it passes it to the secure transport machine, and the latter is responsible for relaying the message, applying any necessary cryptographic functions to it, taking care of retransmission, and in general providing all transport facilities.

EX1006 (Basturk) at 8

Paper 26 (POR) at 7-8



Basturk: Overview

“transport machines” M_A and M_B generate/verify the MAC under session key α ; the application never sees it

- (1) **Initialization:** Authentication and session key exchange. When A initializes M_A (by passing it B 's identity and the shared key a) the machine initiates and executes an authentication and key exchange protocol with M_B . Specifically, the protocol used is the one chosen by the initiator in the options specified above. This protocol results in the distribution of a new (fresh) session key α while making sure that this key is authentic (ie. known only to M_A and M_B).
- (2) **Steady state:** Initialization completed, M_A is ready to receive data from the application A and send it to B ; similarly, M_B is ready to receive data from M_A and pass it to B .
 - (2.1) *Integrity via signing.* If the integrity option is selected then data is signed by M_A under the session key α (a signature is also called a MAC, or message authentication code). The signature covers not only the data payload but also the transport header (as explained later). On receiving a signed packet, M_B uses α to verify the signature.
 - (2.2) *Confidentiality via encryption.* If the confidentiality option is selected then the data payload is encrypted by M_A under the session key α . On receiving a packet, M_B uses α to decrypt the payload and then passes the plaintext to B .

EX1006 (Basturk) at 9-10

Notice that only the transport machines M_A and M_B know about the session key. A and B never see it.

EX1006 (Basturk) at 10

Paper 26 (POR) at 7-8



Basturk: Overview

Computing a MAC adds latency; “on-the-fly” minimizes this latency

The provision of security is bound to somewhat degrade performance, but the goal is to keep this impact at a minimum. A first generic step towards minimizing the perceived performance

EX1006 (Basturk) at 6

There are, however, performance issues that are common to any security option, and their impact should also be minimized. Performance degradations caused by the provision of security have two major causes: additional flows and increased processing. Additional flows are typically required for authentication purposes during the initial phases of a connection. Increased processing is the result of the computational requirements of security functions such as signature generation and verification, and encryption/decryption. We now review the design implications of both, and identify the components they impact most.

EX1006 (Basturk) at 6-7

The main one is that all computations should be performed in the most timely fashion possible. In other words, while an increase in the amount of computation is unavoidable, it is important to ensure that nothing slows down or delays this additional processing. In all instances we would like all computations to be carried out “on-the-fly” as data is being transmitted or received. This minimizes latency.

EX1006 (Basturk) at 7

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Basturk: Overview

“on-the-fly” processing depends on two major components

tations and verifications to dedicated hardware. The ability to achieve such on-the-fly processing depends on two major components. The first is the latency in retrieving the information needed to perform the necessary computations. The second is the nature of the computations themselves. The first component is most relevant at the receiver, while the second is equally important at both the transmitter and the receiver.

EX1006 (Basturk) at 12-13

verification process should be kept to a minimum. A first step in achieving this is to allow context retrieval to be performed as quickly as possible by specifying early on in the packet all the required information. While rapid context retrieval certainly helps it does not eliminate all initial latency, and it is therefore still important to allow computations to start even before the full context has been retrieved. Finally, latency can also be kept small by ensuring that computations are of minimal complexity while meeting our security requirements.

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Basturk: Overview

“context”

Both signature computation and encryption/decryption rely on the use of secret information (key) shared by the two communicating parties. Retrieval of this information is, therefore, necessary for such processing. While one can assume its immediate availability when transmitting data, it must typically be retrieved upon receipt of a packet and this context retrieval step can introduce latency. It is, therefore, useful to design security functions, in particular signature computation, which allow processing to start immediately upon arrival of data, without waiting for the associated context retrieval to complete.

EX1006 (Basturk) at 8

associated connection context. The context contains information such as the shared session key, the counter value of the last accepted packet, the type of cryptographic function used, etc., which are central to the verification of a packet integrity. Some delay is obviously unavoidable when

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Basturk: Overview

Two rules for on-the-fly's two major components

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

EX1006 (Basturk) at 13

First, all data used to generate the signature is present in the packet. Let's illustrate with an example from the AKE protocols. In such challenge response protocols, it is common that one party (say B) proves his identity by signing a challenge R_A sent by A . In such a case, rather than returning $\langle R_A, \sigma \rangle$ with $\sigma = \text{MAC}_\alpha(R_A)$, party B could return just the short tag σ ; after all, A already knows R_A (it is in A 's context) so why waste bandwidth sending it? The reason for preferring to send the full $\langle R_A, \sigma \rangle$ is that signature verification can begin without waiting for the outcome of context retrieval. On the other hand, the cost of resending R_A is minimal since bandwidth is not that expensive at these speeds. In general, this translates into the following packet format: a signed packet will be of the form $\langle D, \sigma \rangle$ where σ is a signature of packet D under key α .

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Basturk: Overview

Two rules for on-the-fly's two major components

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

EX1006 (Basturk) at 13

Second, MAC computations are kept simple and can start prior to context retrieval. In particular, we rely on MAC implementations of the form $\text{MAC}_\alpha(m) = f_\alpha(h(m))$, where h is a (hash) function depending neither on α nor on the cryptographic primitive chosen in the initial options. The use of such an implementation will enhance performance in our setting as MAC computation does not have to wait for α and the cryptographic function to be retrieved from the context; we can begin computing $h(m)$ straight away. By the time we need to compute f_α the key α and cryptographic function will have been retrieved. In addition, since h can be chosen to be a standard hash function and only f_{α} needs to involve more computationally intensive cryptographic functions, the overall cost of signature generation/verification can be kept low.

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Basturk: Overview

Three design rules for “timely and on-the-fly” security computations

To summarize, our requirement for timely and on-the-fly security computations translates into three specific design rules:

- (1) Signature computation starts before the retrieval of connection context;
- (2) Packets are independently encrypted;
- (3) Hardware utilization is facilitated wherever possible.

EX1006 (Basturk) at 8

Paper 26 (POR) at 8-9; Paper 44 (Sur-Reply) at 15-16



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Petitioners argue that “on-the-fly” computations are performed in parallel with “packet” transmission

remove the jitter added by the network.” EX1005, 8. Similarly, *Basturk* discloses, “[i]deally, we want signatures to be computed and verified on-the-fly; i.e., MAC generation should be carried out as data transmissions proceeds rather than before these operations have completed” because “[t]he goal is to avoid slowing down the regular flow of data.” EX1006, 12 (cleaned up).

Paper 3 (Petition) at 11

When read correctly, a POSITA would have understood *Basturk*’s “on-the-fly” teachings means, in part, the process of computing the MAC in parallel to the transmission of the packet. EX1033, ¶¶11-14. Notably, Dr. Stubblebine failed to

Paper 37 (Reply) at 5

slowing down the regular flow of data.” EX1006, 12 (cleaned up). For example, the data transmission occurs faster using on-the-fly signature computation because the signature computation is done in parallel with the transmission of the packet, and then the computed signature is placed at the end of the packet just as the transmission is completing. Compare this to where the signature is computed

EX1003 (Houh Decl.) ¶65

6 But it -- by following these design
7 rules, it doesn't introduce any additional
8 latency over what is already there in a system,
9 because it can be done in parallel to the -- an
10 on-the-fly, which I have shown in my third
11 supplemental declaration with some charts, how
12 that can be done in parallel to the actual
13 transmission of a packet.

EX2010 (Houh Dep. Tr.) at 65:6-13

Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Petitioners argue that “on-the-fly” computations are performed in parallel with “packet” transmission

17 It is like jumping on the train, the
18 last car in the train as it is leaving the
19 station.

EX2010 (Houh Dep. Tr.) at 98:17-19

16 Q. So, in your train leaves the station
17 analogy, anything that left the station is
18 analogous to anything that has already been
19 transmitted over the network; is that right?
20 MR. BRIT: Objection to form.
21 Mischaracterizes the prior testimony. And
22 incomplete hypothetical.
1 THE WITNESS: Yes, I mean, I'm
2 assuming you can't run instantly, you know,
3 from the back of the train forward, you know,
4 down the tube of the tracks or wherever. Or
5 down the tracks to get on the first car,
6 right, that actually takes some time and I'm
7 assuming you -- it has already been
8 transmitted.

EX2010 (Houh Dep. Tr.) at 99:16-100:8

11 And that -- and then, because you
12 put the trailer, the MAC, the signature in
13 the trailer as suggested -- as taught,
14 actually, explicitly taught on Page 16, then
15 you can stuff that generated signature at the
16 end of the packet just as the last bytes of
17 the trailer need to be transmitted.

18 That is what Basturk is referring to
19 when it refers to on-the-fly. And that is --
20 that is -- that is how I have written up all
21 of my supplemental declarations.

22 And even the original one is really
1 based on that on-the-fly teaching interpreted
2 correctly in that as Dr. Stubblebine
3 misinterprets.

EX2010 (Houh Dep. Tr.) at 74:11-75:3

Paper 44 (Sur-Reply) at 16



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

“on-the-fly” computes in parallel with context retrieval, not actual packet transmission

latency. It is, therefore, useful to design security functions, in particular signature computation, which allow processing to start immediately upon arrival of data, without waiting for the associated context retrieval to complete.

EX1006 (Basturk) at 8

signatures and counters be kept to a minimum. Ideally, we want signatures to be computed and verified on-the-fly; i.e., MAC generation (verification) should be carried out as data transmissions (receptions) proceeds rather than before (after) these operations have completed. The goal is to avoid slowing down the regular flow of data, and allow the possible off-load of signature computations and verifications to dedicated hardware. The ability to achieve such on-the-fly processing depends on two major components. The first is the latency in retrieving the information needed to perform the necessary computations. The second is the nature of the computations themselves. The first component is most relevant at the receiver, while the second is equally important at both the transmitter and the receiver.

EX1006 (Basturk) at 8

First, all data used to generate the signature is present in the packet.

A already knows R_A (it is in A 's context) so why waste bandwidth sending it? The reason for preferring to send the full $\langle R_A, \sigma \rangle$ is that signature verification can begin without waiting for the outcome of context retrieval. On the other hand, the cost of resending R_A is minimal since

Second, MAC computations are kept simple and can start prior to context retrieval.

EX1006 (Basturk) at 13

Paper 26 (POR) at 24-25; Paper 44 (Sur-Reply) at 15-16



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Under Petitioners' theory, "on-the-fly" operations happen *below* the application layer

5 And especially, you know, doing
6 things in parallel with the transmission,
7 specifically computing the signature while in
8 parallel with transmission.
9 And that is clearly at a lower
10 layer.

EX2010 (Houh Dep. Tr.) at 117:5-10

14 So, but, you know, if you have to
15 sign things at the application layer and you
16 are not actually computing them until you are
17 doing it on the fly in parallel with
18 transmission, then that is clearly a lower
19 layer.

EX2010 (Houh Dep. Tr.) at 117:14-19

1 And, and that is what
2 Dr. Stubblebine's misinterpretation of on-the-fly
3 and the strict OSI layering is doing. It is
4 introducing unnecessary latency because if you
5 have to compute the signature at a higher level
6 before passing it down, then you have to do it
7 where you could have done it on-the-fly. And as
8 Basturk is teaching, you are doing it on-the-fly
9 in parallel with the transmission of a packet.

EX2010 (Houh Dep. Tr.) at 66:1-9

4 And, therefore, under
5 Dr. Stubblebine's interpretation of the very
6 strict boundaries between the OSI layers
7 where you are forced to do the MAC
8 computation before you move the whole packet
9 down to the lower layers for processing, you
10 are forced to suffer the latency of the -- of
11 a MAC generation.

EX2010 (Houh Dep. Tr.) at 109:4-11

Paper 44 (Sur-Reply) at 16-17



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Under Petitioners' theory, "on-the-fly" operations happen at the physical layer

108. Basturk's context retrieval process is not "the transmission of the packet," as Dr. Houh suggests. EX1003 ¶ 65 (emphasis added). Indeed, Dr. Houh's interpretation of Basturk is inaccurate, as a POSITA would understand that "packets" or Protocol Data Units (PDUs) at higher layers are encapsulated by the next lower layer, and the data is not "transmitted" bit-by-bit until the data reaches the physical layer (in conjunction with the link layer). See §§ VI.A (OSI) and VI.E (Ethernet). As such, PDUs are passed up and down the layers of a protocol stack

EX2004 (Stubblebine Decl.) ¶108

52. Ethernet, a protocol operating at the physical layer and link layer (ISO Layers 1 & 2), is designed to process incoming frames bit by bit as they are received as the unit of exchange at the physical layer is the bit. See EX1014 at 32, 142-143.

EX2004 (Stubblebine Decl.) ¶52

14 Q. What is the transmission speed here?

15 A. The transmission speed that I am
16 referring to is the network to which this device
17 was attached that has a rate at which the data
18 can be transmitted onto the network.

19 So, if you are attached to a
20 100-megabit Ethernet, then you can transmit onto
21 that 100-megabit Ethernet at about 100 megabits.

22 So, that is -- when the data is
1 being transmitted, it would go out at a certain
2 rate and that is whatever the rate of the network
3 to which the device attached is running.

EX2010 (Houh Dep. Tr.) at 109:4-11

Paper 26 (POR) at 25; Paper 44 (Sur-Reply) at 17



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Petitioners' disregard for layer distinctions is inconsistent with the patent's lexicography

As Dr. Houh explains, these strict boundary requirements between layers do not exist. EX1033, ¶¶22-28. The '682 Patent itself states, “[i]n practice, many applications *do not always permit exact nomination of strict boundaries* specifically between the upper protocol layers, particularly layers 5 to 7.” EX1001, 1:37-45. This discussion of the merging of layers 5-7 belies PO's strict boundary requirements. POR, 25; EX1033, ¶22.

Paper 37 (Reply) at 5-6

PO sets forth a claim construction for “application layer,” and “application protocol.” POR, 14. Even under PO's proposed claim constructions, it does not render any asserted reference inapplicable, nor does it change that those references either disclose and/or render obvious all Challenged Claims. EX1033, ¶10.

Paper 37 (Reply) at 1

application layer using an application protocol. In practice, many applications do not always permit exact nomination of strict boundaries specifically between the upper protocol layers, particularly layers 5 to 7. By way of example, within

EX1001 ('682 Patent) at 1:19-45

When referring to application layer below, this denotes the layers above the transport layer (layers above 4). The application protocol also denotes the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer.

EX1001 ('682 Patent) at 2:6-11

Paper 44 (Sur-Reply) at 18; Paper 26 at 14-18



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

“on-the-fly” does not motivate the claimed invention

“This testimony is generic and bears no relation to any specific combination of prior art elements. It also fails to explain why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does*. See *KSR*, 550 U.S. at 418, 127 S.Ct. 1727 (“[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements *in the way the claimed new invention does* ... because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.”).”

ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc., 694 F.3d 1312, 1328 (Fed. Cir. 2012)



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Basturk teaches *not* modifying the application layer

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure. To this end, we distinguish security features according to the layer of the communication structure to which they are most naturally associated. We found that the traditional features are mostly application level, while the new ones we deem necessary are transport level.

EX1006 (Basturk) at 3

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. Applications using the regular transport protocol should not have to be modified at all.

EX1006 (Basturk) at 5

Paper 26 (POR) at 25-26



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify Handley in view of Basturk

Basturk's speed and efficiency benefits are inapplicable to Handley

EX1001, cl. 1; EX1003, ¶64. A POSITA would have been motivated to use Basturk's "on-the-fly" signature computation with Handley's internet conferencing architecture due to the known communication benefits, which include faster data transmission, reduced jitter, and reductions in computing power. EX1003, ¶64.

Paper 3 (Petition) at 10

remove the jitter added by the network." EX1005, 8. Similarly, *Basturk* discloses, "[i]deally, we want signatures to be computed and verified on-the-fly; i.e., MAC generation should be carried out as data transmissions proceeds rather than before these operations have completed" because "[t]he goal is to avoid slowing down the regular flow of data." EX1006, 12 (cleaned up).

Paper 3 (Petition) at 11

EX1006, 4 n. 3. But the combination Petitioners put forth does not duplicate functions because Handley does not disclose the use of a MAC or signatures and any checksums in different protocol layers used in *Handley* are not for the purpose of authentication. EX1033, ¶39.

Paper 37 (Reply) at 14

Paper 44 (Sur-Reply) at 19



Motivation to Combine: Basturk's reliable transport protocol is incompatible with Handley's use of RTP

Basturk has reliability features like TCP

TRANSPORT LEVEL SECURITY FEATURES: SECURE DELIVERY. **Secure delivery**, roughly speaking, is a guarantee to the sender *A* that his message was received by *B* and not intercepted and destroyed by the adversary. It **is essentially an extension of the standard transport level *reliability* feature** to the more adversarial setting we are discussing, which is why it seems most natural to view it as a transport level feature.

EX1006 (Basturk) at 4

Reliability:

The TCP must **recover from data that is damaged, lost, duplicated, or delivered out of order** by the internet communication system. This is achieved by assigning a **sequence number** to each octet transmitted, and requiring a positive **acknowledgment (ACK)** from the receiving TCP. If the ACK is not received within a **timeout interval**, the data is **retransmitted**. At the receiver, the sequence numbers are used to correctly order segments that may be received out of order and to eliminate duplicates. Damage is handled by adding a checksum to each segment transmitted, checking it at the receiver, and discarding damaged segments.

EX2006 (TCP) at 10

Paper 26 (POR) at 26-27



Motivation to Combine: Basturk's reliable transport protocol is incompatible with Handley's use of RTP

Basturk has reliability features like TCP

Secure delivery is guaranteed because the ACKs include sequence numbers and are signed.

Note that the signature also provides error detection, so that no CRC or error detection code is required. Replaying of packets from one session into another is not possible because each session has a different session key.

EX1006 (Basturk) at 12

Reliability:

The TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the internet communication system. This is achieved by assigning a sequence number to each octet transmitted, and requiring a positive acknowledgment (ACK) from the receiving TCP. If the ACK is not received within a timeout interval, the data is retransmitted. At the receiver, the sequence numbers are used to correctly order segments that may be received out of order and to eliminate duplicates. Damage is handled by adding a checksum to each segment transmitted, checking it at the receiver, and discarding damaged segments.

EX2006 (TCP) at 10

Paper 26 (POR) at 27-28

Motivation to Combine: Basturk's reliable transport protocol is incompatible with Handley's use of RTP

Basturk's "extension" of transport level reliability is the *addition* of security

15 Q. So, when Basturk calls secure
16 delivery an extension of the standard transport
17 level reliability feature, by extension Basturk
18 means adding security, right?

19 MR. BRIT: Objection to form.

20 THE WITNESS: Well, it can extend
21 existing protocols to mitigate or eliminate
22 the threat posed by adversaries in the
1 network that may, you know, intercept or
2 destroy packets and fool the sender into
3 thinking that the data has actually been
4 received.

5 So, it is simply an extension to
6 existing protocols. And the features in
7 Basturk are, I would say, orthogonal to the
8 features provided by a protocol such as TCP.
9 That is, they can be used in
10 conjunction with each other, and the
11 extensions discussed in Basturk are, are --
12 can provide additional security functions
13 or -- well, sorry. I'm not sure I -- I don't
14 use that word the same way as --
15 But, it can provide the ability to
16 detect such malicious activity by adversaries
17 in the network.
18 And so, that is how it can extend
19 other existing protocols such as TCP.

EX2010 (Houh Dep. Tr.) at 126:15-127:19

Paper 44 (Sur-Reply) at 18-19



Motivation to Combine: Basturk's reliable transport protocol is incompatible with Handley's use of RTP

Handley teaches away from combining reliability protocols with RTP

Real-time internet traffic is defined as datagrams that are delay sensitive. It could be argued that all datagrams are delay sensitive to some extent, but for these purposes we refer only to datagrams where exceeding an end-to-end delay bound of a few hundred milliseconds renders the datagrams useless for the purpose they were intended. For the purposes of this definition, TCP traffic is normally not considered to be real-time traffic, although there may be exceptions to this rule.

EX1005 (Handley) at 4-5

traffic.” EX1005 at 5. A POSITA would have understood that Handley considers TCP traffic to be non-real-time because of the delay associated with its reliability features. A POSITA would understand that this is why Handley implements real-time RTP traffic over UDP, which is not a reliable delivery protocol, and distinguishes between real-time traffic (RTP over UDP) from non-real-time traffic (traffic over TCP) for prioritized processing. See § IX.A.2, *supra*; EX2007 at 1

EX2004 (Stubblebine Decl.) ¶113

service provided.” EX1005 at 4-5. Handley suggests a modified routing model where “real-time” non-TCP traffic (as defined) is segregated from and prioritized over non-real-time TCP traffic. See EX1005 at 5. According to Handley, its approach of “classifying real-time traffic separately from non-real-time traffic and giving real-time traffic priority treatment ensures that real-time traffic sees minimum delays.” EX1005 at 5.

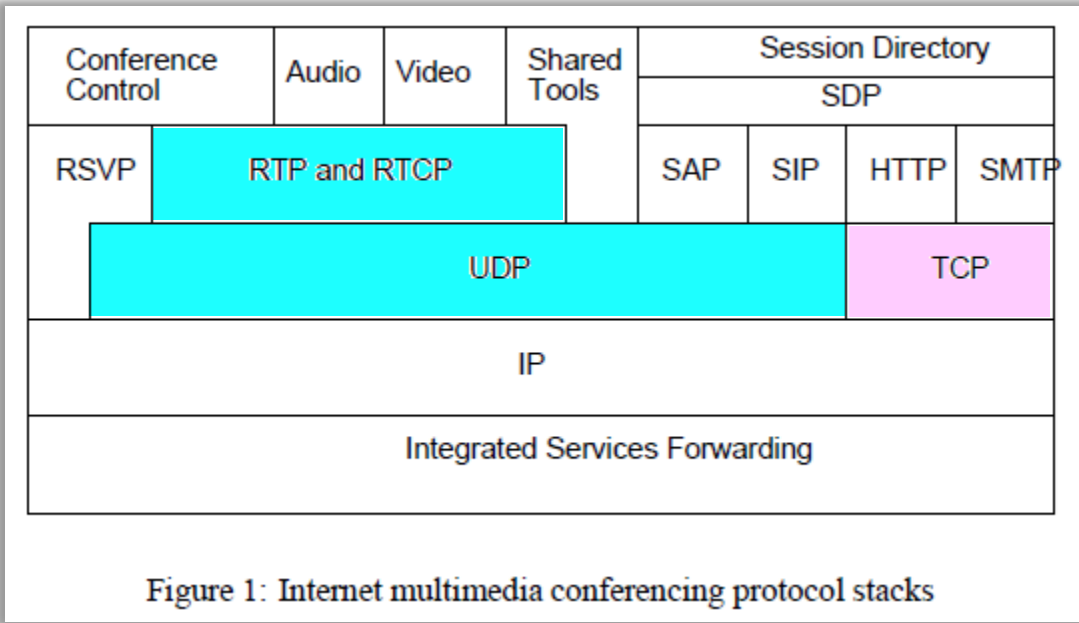
EX2004 (Stubblebine Decl.) ¶70 (§ IX.A.2)

Paper 26 (POR) at 28-29



Motivation to Combine: Basturk’s reliable transport protocol is incompatible with Handley’s use of RTP

Handley teaches away from combining reliability protocols with RTP



EX1005 (Handley) at 3

4.1 Non-best effort service

Real-time internet traffic is defined as datagrams that are delay sensitive. It could be argued that all datagrams are delay sensitive to some extent, but for these purposes we refer only to datagrams where exceeding an end-to-end delay bound of a few hundred milliseconds renders the datagrams useless for the purpose they were intended. For the purposes of this definition, TCP traffic is normally not considered to be real-time traffic, although there may be exceptions to this rule.

EX1005 (Handley) at 5

Although best-effort services can support real-time traffic, classifying real-time traffic separately from non-real-time traffic and giving real-time traffic priority treatment ensures that real-time traffic sees minimum delays. Non-real-time TCP traffic tends to be elastic in its bandwidth requirements, and will then tend to fill any remaining bandwidth.

EX1005 (Handley) at 5

5.2 RTP

The transport protocol for real-time flows is RTP[22]. This provides a standard format packet header which gives media specific timestamp data, as well as payload format information and sequence numbering amongst other things. RTP is normally carried using UDP. It does not provide or require any connection setup, nor does it provide any enhanced reliability over UDP. For RTP to provide a useful media flow, there

EX1005 (Handley) at 8

Paper 26 (POR) at 6, 28-29

Motivation to Combine: Basturk's reliable transport protocol is incompatible with Handley's use of RTP

Basturk's protocol is unsuitable for Handley's multicast network

115. Furthermore, A POSITA would have understood that because Basturk's protocol is a reliably delivery protocol like TCP, it would be unsuitable for use with Handley which relies on a multicast network for delivery of packets. Applications relying on multicast delivery networks can easily scale to many receivers because the senders do not need to do any additional work when a new receiver joins (or leaves) a multicast group. The same applies to broadcast delivery. Furthermore, a POSITA would understand that a multicast delivery is incompatible with a reliable delivery protocol such as TCP or any protocol based on TCP or that has similar functionality. This is because TCP is a connection-oriented protocol, which means it establishes a direct connection between two endpoints before data can be sent, where the sender and receiver know who each other are. EX2006 at 11

EX2004 (Stubblebine Decl.) ¶115

With IP multicast, the group is indirectly identified by a single IP class-D multicast address.

Several things are important about this service model from an architectural point of view. Receivers do not need to know who or where the senders are to receive traffic from them. Senders never need to know who the receivers are. Neither senders or receivers need care about the network topology as the network optimises delivery.

EX1005 (Handley) at 3

Paper 26 (POR) at 29-30



Handley + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Handley does not disclose RTP packet level authentication

RTP specifies a standard way to encrypt RTP and RTCP packets using private key encryption schemes such as DES[18]. It also specifies a standard mechanism to manipulate plain text keys using MD5[19] so that the resulting bit string can be used as a DES key. This allows simple out-of-band mechanisms such as privacy-enhanced mail to be used for encryption key exchange.

EX1005 (Handley) at 12

9.2 Authentication and Message Integrity

Authentication and message integrity are not defined in the current specification of RTP since these services would not be directly feasible without a key management infrastructure. It is expected that authentication and integrity services will be provided by lower layer protocols in the future.

EX1008 (RTP) at 50

Paper 26 (POR) at 31-32



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Basturk does not disclose authentication at the RTP packet level

A POSITA would have appreciated that although *Basturk* does not explicitly disclose RTP, RTP’s secure transport protocol is compatible with *Handley’s* internet conferencing architecture. EX1003, ¶66. For example, *Basturk* discloses

Paper 3 (Petition) at 11

Paper 26 (POR) at 31-32



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Basturk teaches away from modifying Handley’s application layer

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to **add security functionality in a way which is consistent with, and best matches, the existing communication structure**. To this end, we

EX1006 (Basturk) at 3

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. **Applications using the regular transport protocol should not have to be modified at all.**

EX1006 (Basturk) at 5

Paper 26 (POR) at 30-31



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Basturk teaches away from modifying Handley’s application layer

³ An implicit assumption is that the application is not performing its own acknowledgments and retransmission, but, more naturally, relying on the transport for these features. Indeed, asking the application to duplicate these transport functions is usually poor design in that it belies the layered communication structure, and would also adversely affect performance.

EX1006 (Basturk) at 4

The manner in which security against replay is guaranteed illustrates well an advantage of security at the transport level. Sequencing is a standard and already present transport function. We simply exploit its presence. Had we wanted to prevent replay at the application level we would had to implement sequencing with transport level counters and provide for our own checking and retransmission, thereby not only making implementation significantly harder but duplicating the transport functionality and degrading performance.

EX1006 (Basturk) at 12

Paper 26 (POR) at 30-31



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Handley + Basturk does teach or suggest RTP packet level authentication as an *application* protocol on an *application* layer

EX1006, 4 n. 3. But the combination Petitioners put forth does not duplicate functions because *Handley* does not disclose the use of a MAC or signatures and any checksums in different protocol layers used in *Handley* are not for the purpose of authentication. EX1033, ¶39.

Paper 37 (Reply) at 14

initiator in the options specified above. This protocol results in the distribution of a new (fresh) *session key* α while making sure that this key is authentic (ie. *known only to M_A and M_B*).

EX1006 (Basturk) at 9

Integrity via signing. If the integrity option is selected then *data is signed by M_A under the session key α (a signature is also called a MAC, or message authentication code)*. The signature covers not only the data payload but also the transport header (as explained later). On receiving a signed packet, M_B uses α to verify the signature.

EX1006 (Basturk) at 9

Notice that *only the transport machines M_A and M_B know about the session key. A and B never see it.*

EX1006 (Basturk) at 10

Paper 44 (Sur-Reply) at 19



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

**Patent Owner does not apply an “overly strict” interpretation of “application layer”;
Petitioners ignore the patent’s lexicography**

18 But RTP packets are encapsulated
19 inside UDP packets typically. They are
20 encapsulated inside IP packets, that may be also
21 encapsulated inside Ethernet frames or layer
22 frames. But the point here is that it doesn't
1 matter what PDU he is talking about, one PDU or
2 the other.

EX2010 (Houh Dep. Tr.) at 153:3-154:2

16 But an RTP packet as a whole, the
17 header and the data would be carried inside a
18 UDP packet.
19 So, at a different layer, there is
20 the whole RTP packet including the header is
21 a PDU in a higher layer protocol like UDP
22 which encapsulates RTP.
1 BY MR. EKLEM:
2 Q. Okay.
3 A. And similarly the UDP, whole UDP
4 portion of the packet is encapsulated within an
5 IP packet.

EX2010 (Houh Dep. Tr.)
at 153:3-154:2

Paper 44 (Sur-Reply) at 21



Handley + Basturk [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Under Petitioners’ theory, “on-the-fly” computations are done at the “lower” physical layer

5 And especially, you know, doing
6 things in parallel with the transmission,
7 specifically computing the signature while in
8 parallel with transmission.
9 And that is clearly at a lower
10 layer.

EX2010 (Houh Dep. Tr.) at 117:5-10

14 So, but, you know, if you have to
15 sign things at the application layer and you
16 are not actually computing them until you are
17 doing it on the fly in parallel with
18 transmission, then that is clearly a lower
19 layer.

EX2010 (Houh Dep. Tr.) at 117:14-19

14 Q. What is the transmission speed here?
15 A. The transmission speed that I am
16 referring to is the network to which this device
17 was attached that has a rate at which the data
18 can be transmitted onto the network.
19 So, if you are attached to a
20 100-megabit Ethernet, then you can transmit onto
21 that 100-megabit Ethernet at about 100 megabits.
22 So, that is -- when the data is
1 being transmitted, it would go out at a certain
2 rate and that is whatever the rate of the network
3 to which the device attached is running.

EX2010 (Houh Dep. Tr.) at 109:4-11

Paper 44 (Sur-Reply) at 17, 19-21



Handley + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Under Petitioners’ theory, Handley does not disclose this element

EX1006, 4 n. 3. But the combination Petitioners put forth does not duplicate functions because *Handley* does not disclose the use of a MAC or signatures and any checksums in different protocol layers used in *Handley* are not for the purpose of authentication. EX1033, ¶39.

Paper 37 (Reply) at 14

Paper 44 (Sur-Reply) at 20-21



Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Basturk’s “on-the-fly” is not enabled by placing the signature in a trailer

tations and verifications to dedicated hardware. The ability to achieve such on-the-fly processing depends on two major components. The first is the latency in retrieving the information needed to perform the necessary computations. The second is the nature of the computations themselves. The first component is most relevant at the receiver, while the second is equally important at both the transmitter and the receiver.

EX1006 (Basturk) at 12-13

verification process should be kept to a minimum. A first step in achieving this is to allow context retrieval to be performed as quickly as possible by specifying early on in the packet all the required information. While rapid context retrieval certainly helps it does not eliminate all initial latency, and it is therefore still important to allow computations to start even before the full context has been retrieved. Finally, latency can also be kept small by ensuring that computations are of minimal complexity while meeting our security requirements.

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9, 34-36; Paper 44 (Sur-Reply) at 20-21

Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Basturk’s two rules for on-the-fly’s two major components do not require a trailer

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

EX1006 (Basturk) at 13

First, all data used to generate the signature is present in the packet. Let’s illustrate with an example from the AKE protocols. In such challenge response protocols, it is common that one party (say B) proves his identity by signing a challenge R_A sent by A . In such a case, rather than returning $\langle R_A, \sigma \rangle$ with $\sigma = \text{MAC}_\alpha(R_A)$, party B could return just the short tag σ ; after all, A already knows R_A (it is in A ’s context) so why waste bandwidth sending it? The reason for preferring to send the full $\langle R_A, \sigma \rangle$ is that signature verification can begin without waiting for the outcome of context retrieval. On the other hand, the cost of resending R_A is minimal since bandwidth is not that expensive at these speeds. In general, this translates into the following packet format: a signed packet will be of the form $\langle D, \sigma \rangle$ where σ is a signature of packet D under key α .

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9, 34-36

Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Basturk’s two rules for on-the-fly’s two major components do not require a trailer

These different requirements have been incorporated in our design, where the goal of minimal latency is reflected in the following two rules.

EX1006 (Basturk) at 13

Second, MAC computations are kept simple and can start prior to context retrieval. In particular, we rely on MAC implementations of the form $\text{MAC}_\alpha(m) = f_\alpha(h(m))$, where h is a (hash) function depending neither on α nor on the cryptographic primitive chosen in the initial options. The use of such an implementation will enhance performance in our setting as MAC computation does not have to wait for α and the cryptographic function to be retrieved from the context; we can begin computing $h(m)$ straight away. By the time we need to compute f_α the key α and cryptographic function will have been retrieved. In addition, since h can be chosen to be a standard hash function and only f_{α} needs to involve more computationally intensive cryptographic functions, the overall cost of signature generation/verification can be kept low.

EX1006 (Basturk) at 13

Paper 26 (POR) at 8-9, 34-36

Basturk’s three design rules for on-the-fly do not require a trailer

To summarize, our requirement for timely and on-the-fly security computations translates into three specific design rules:

- (1) Signature computation starts before the retrieval of connection context;
- (2) Packets are independently encrypted;
- (3) Hardware utilization is facilitated wherever possible.

EX1006 (Basturk) at 8

Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

The “inserting” of 1.2 is how the “providing” of 1.1 is done

Claim 1

1. A method for transmitting data from a transmitter to a receiver, comprising:

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and

[1.4] accepting, by the receiver, the whole RTP packet payload, if the receiver knows the transmitter, and otherwise rejecting the whole RTP packet payload.

EX1001 ('682 patent), at claim 1

Paper 44 (Sur-Reply) at 19-21



Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Under Petitioner’s theory, “on-the-fly” insertion into a trailer happens as the packet is actually transmitted onto the network

17 It is like jumping on the train, the
18 last car in the train as it is leaving the
19 station.

EX2010 (Houh Dep. Tr.) at 98:17-19

16 Q. So, in your train leaves the station
17 analogy, anything that left the station is
18 analogous to anything that has already been
19 transmitted over the network; is that right?

20 MR. BRIT: Objection to form.

21 Mischaracterizes the prior testimony. And
22 incomplete hypothetical.

1 THE WITNESS: Yes, I mean, I'm
2 assuming you can't run instantly, you know,
3 from the back of the train forward, you know,
4 down the tube of the tracks or wherever. Or
5 down the tracks to get on the first car,
6 right, that actually takes some time and I'm
7 assuming you -- it has already been
8 transmitted.

EX2010 (Houh Dep. Tr.) at 99:16-100:8

11 And that -- and then, because you
12 put the trailer, the MAC, the signature in
13 the trailer as suggested -- as taught,
14 actually, explicitly taught on Page 16, then
15 you can stuff that generated signature at the
16 end of the packet just as the last bytes of
17 the trailer need to be transmitted.

18 That is what Basturk is referring to
19 when it refers to on-the-fly. And that is --
20 that is -- that is how I have written up all
21 of my supplemental declarations.

22 And even the original one is really
1 based on that on-the-fly teaching interpreted
2 correctly in that as Dr. Stubblebine
3 misinterprets.

EX2010 (Houh Dep. Tr.) at 74:11-75:3

Paper 44 (Sur-Reply) at 16



Handley + Basturk [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Under Petitioner’s theory, “on-the-fly” insertion into a trailer happens at the physical layer, not the application layer

5 And especially, you know, doing
6 things in parallel with the transmission,
7 specifically computing the signature while in
8 parallel with transmission.
9 And that is clearly at a lower
10 layer.

EX2010 (Houh Dep. Tr.) at 117:5-10

14 So, but, you know, if you have to
15 sign things at the application layer and you
16 are not actually computing them until you are
17 doing it on the fly in parallel with
18 transmission, then that is clearly a lower
19 layer.

EX2010 (Houh Dep. Tr.) at 117:14-19

14 Q. What is the transmission speed here?
15 A. The transmission speed that I am
16 referring to is the network to which this device
17 was attached that has a rate at which the data
18 can be transmitted onto the network.

19 So, if you are attached to a
20 100-megabit Ethernet, then you can transmit onto
21 that 100-megabit Ethernet at about 100 megabits.

22 So, that is -- when the data is
1 being transmitted, it would go out at a certain
2 rate and that is whatever the rate of the network
3 to which the device attached is running.

EX2010 (Houh Dep. Tr.) at 109:4-11

Paper 44 (Sur-Reply) at 17, 19-21



Handley + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



Ground 2: Obviousness over PacketCable + Handley

Ground	Assertion	Petitioned Claims
1	Obvious under § 103 in view of Handley in combination with Basturk	1-21, 23, 25-28
2	Obvious under § 103 in view of PacketCable in combination with Handley	1-28
3	Obvious under § 103 in view of PacketCable in combination with Basturk	1-28
4	Obvious under § 103 in view of Handley in combination with Basturk and PacketCable	22, 24

Paper 3 (Petition) at 5



PacketCable: Overview

PacketCable clients are MTAs

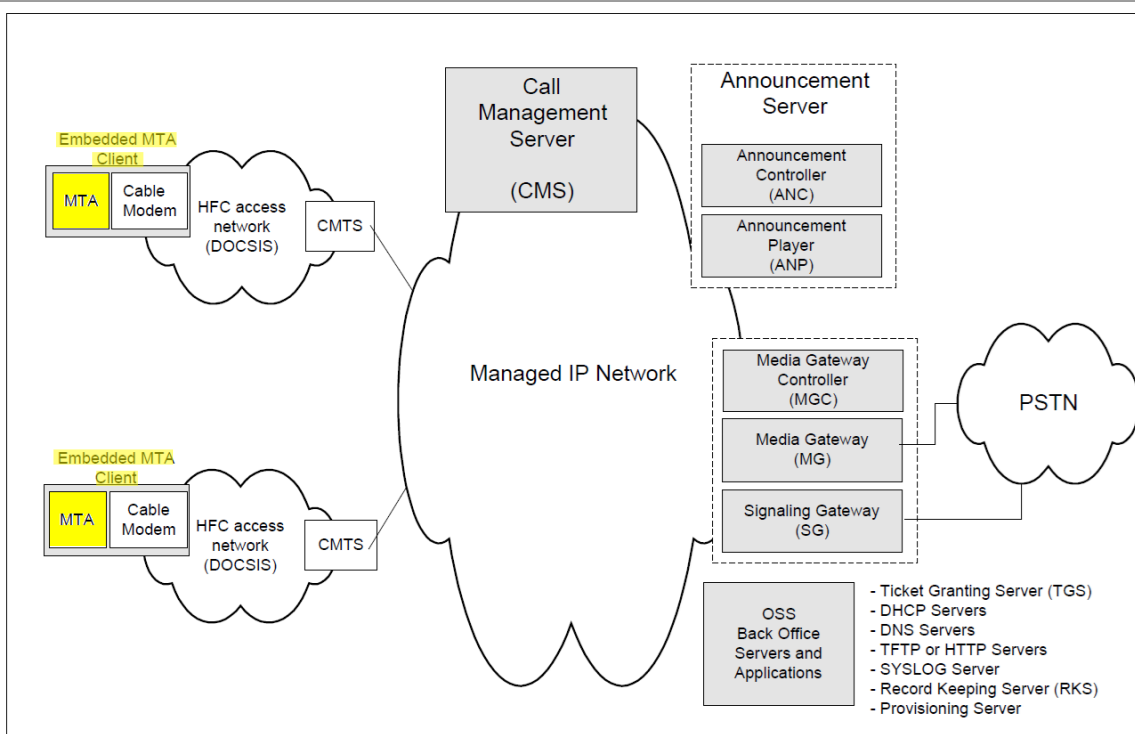


Figure 1. PacketCable Reference Architecture

3.1 Multimedia Terminal Adapter (MTA)

An MTA is a PacketCable client device that contains a subscriber-side interface to the subscriber's CPE (e.g., telephone) and a network-side signaling interface to call control elements in the network. An MTA provides codecs and all signaling and encapsulation functions required for media transport and call signaling.

MTAs reside at the customer site and are connected to other PacketCable network elements via the HFC access network (DOCSIS). PacketCable 1.0 MTAs are required to support the Network Call Signaling (NCS) protocol.

An embedded MTA (E-MTA) is a single hardware device that incorporates a DOCSIS 1.1 cable modem as well as a PacketCable MTA component. Figure 4 shows a representative functional diagram of an E-MTA.

EX1007 (PacketCable) at 18

PacketCable 1.0 specifications only require support for embedded MTAs. Throughout this report, unless otherwise noted, the term MTA refers to an embedded MTA.

EX1007 (PacketCable) at 19

EX1007 (PacketCable) at 12

Paper 26 (POR) at 9-10

PacketCable: Overview

RTP is used to transport media streams

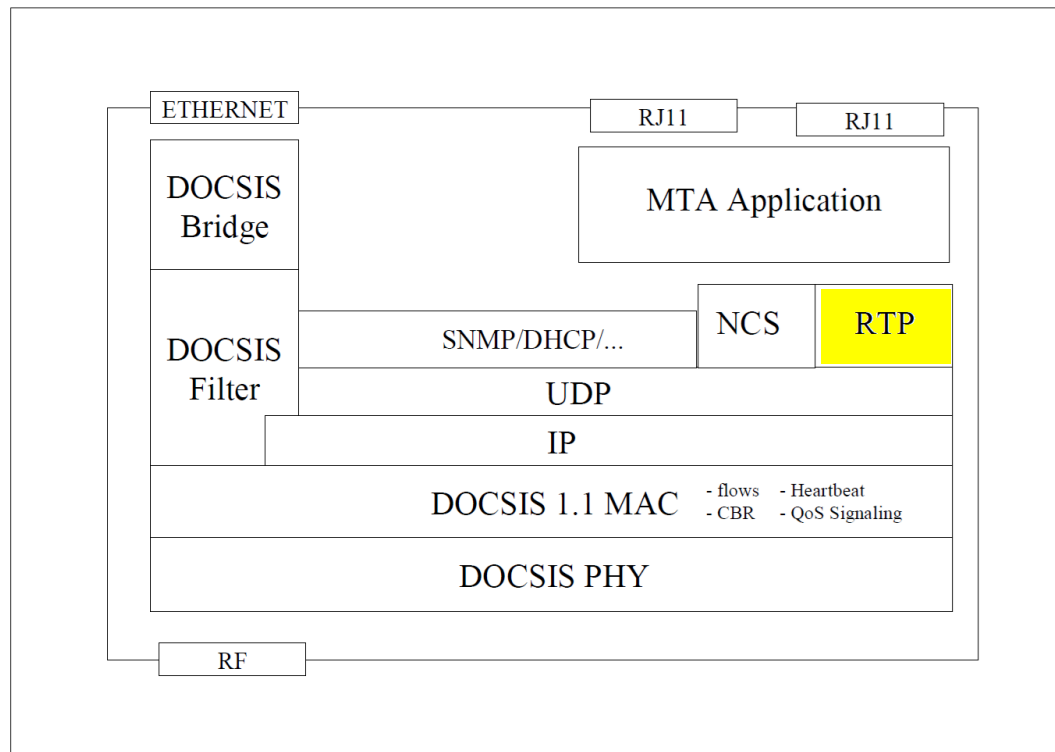


Figure 4. E-MTA Conceptual Functional Architecture

The IETF standard RTP (RFC 1899 - Real-Time Transport Protocol) is used to transport all media streams in the PacketCable network[32]. PacketCable utilizes the RTP profile for audio and video streams as defined in RFC 1990[35].

EX1007 (PacketCable) at 31

EX1007 (PacketCable) at 12

Paper 26 (POR) at 9-11

PacketCable: Overview

RTP is used to transport media streams

End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. An MMH-based MAC (Message Authentication Code) optionally provides message integrity. Keys are distributed by the CMS to the two endpoints.

EX1007 (PacketCable) at 45

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet's unencrypted header and encrypted payload.

EX1007 (PacketCable) at 47

9.2 Authentication and Message Integrity

Authentication and message integrity are not defined in the current specification of RTP since these services would not be directly feasible without a key management infrastructure. It is expected that authentication and integrity services will be provided by lower layer protocols in the future.

EX1008 (RTP) at 50

Paper 26 (POR) at 44, 46



PacketCable + Handley Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



PacketCable + Handley [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Petitioners identify no RTP authentication functions implemented in the MTA application

52. Further, it was known that RTP operates on the session and application layer in the OSI Model, which are often combined with the application layer for purposes of describing an application layer. For example, the original RTP specification, RFC 1889, teaches that “RTP represents a new style of protocol following the principles of application level framing and integrated layer processing,” meaning some protocol functions are implemented in the application. EX1008, 3-4. Additionally, the Complaint in the associated litigation states “the

EX1003 (Houh Decl.) ¶52

RTP represents a new style of protocol following the principles of application level framing and integrated layer processing proposed by Clark and Tennenhouse [1]. That is, RTP is intended to be malleable to provide the information required by a particular application and will often be integrated into the application processing rather than being implemented as a separate layer. RTP is a protocol framework

EX1008 (RTP) at 4

the two endpoints.” *Id.* As described in Ground I, Element [1.1], a POSITA would have understood (1) that manipulating RTP packets, e.g., implementing RC4 or adding a MAC, results in authentication at the packet level and (2) RTP packets are created at the application layer because RTP is an application protocol. EX1003, ¶174. As such, *PacketCable* discloses this element. *Id.*, ¶174.

Paper 3 (Petition) at 45

Paper 26 (POR) at 43; Paper 44 (Sur-Reply) at 22-23



PacketCable + Handley [1.1]: “providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer”

Term	Patent Owner’s Construction	Petitioners’ Construction
“application layer”	“the layers above the transport layer (layers above 4)”	n/a
“application protocol”	“the protocol for communication between a transmitter application layer situated above the transport layer and a receiver application layer situated above the transport layer”	n/a

Petitioners identify no RTP authentication functions implemented in the MTA application

pkt-s6	MTA – MTA	End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. An MMH-based MAC (Message Authentication Code) optionally provides message integrity. Keys are distributed by the CMS to the two endpoints.
--------	-----------	--

EX1007 (PacketCable) at 45

The IETF standard RTP (RFC 1899 - Real-Time Transport Protocol) is used to transport all media streams in the PacketCable network[32]. PacketCable utilizes the RTP profile for audio and video streams as defined in RFC 1990[35].

EX1007 (PacketCable) at 31

[32] “RTP: A Transport Protocol for Real-Time Application,” IETF RFC 1889.

EX1007 (PacketCable) at 57

9.2 Authentication and Message Integrity

Authentication and message integrity are not defined in the current specification of RTP since these services would not be directly feasible without a key management infrastructure. It is expected that authentication and integrity services will be provided by lower layer protocols in the future.

EX1008 (RTP) at 50

Paper 26 (POR) at 44; Paper 44 (Sur-Reply) at 22-23



No Hindsight Reasoning

“However, ‘[t]he inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight. What matters is the path that the person of ordinary skill in the art would have followed, as evidenced by the pertinent prior art.’”

Millennium Pharms., Inc. v. Sandoz Inc., 862 F.3d 1356, 1367 (Fed. Cir. 2017)



Paper 44 (Sur-Reply) at 22-23

PacketCable + Handley Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Petitioners do not show that PacketCable discloses this element

Further, *PacketCable* discloses that the “MAC computation spans the packet’s unencrypted header and encrypted payload.” EX1007, 47. A POSITA would have understood and found obvious that placement of authentication data in the middle of the packet payload would negatively impact performance, cause packet fragmentation issues, and complicate the implementation of networking software. EX1003, ¶178. As such, a POSITA would have avoided such placement. *Id.*, ¶178. With this knowledge, a POSITA would have understood available authentication data placement options to include either at the beginning or the end of the payload. Further, a POSITA would have understood that the authentication

Paper 3 (Petition) at 45)

Paper 26 at 45; Paper 44 (Sur-Reply) at 23



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

PacketCable is completely silent as to the location of the MAC

147. Based on the above portions of PacketCable, a POSITA would have understood that PacketCable does not disclose “inserting, at the transmitter, authentication data at end of a whole RTP packet payload,” as required by this claim element. While PacketCable mentions that “[e]ach RTP packet may include an optional message authentication code (MAC)” and that “MAC computation spans the packet’s unencrypted header and encrypted payload,” a POSITA would not have understood this to disclose (explicitly or inherently) inserting the optional MAC “at end of a whole RTP packet payload.” EX1007 at 47. **PacketCable is completely silent as to where in an RTP packet the optional MAC would be inserted. Indeed, Dr. Houh does not show that PacketCable discloses placing the MAC at any of the theoretical locations he suggests.** See EX1003 ¶ 178.

EX2004 (Stubblebine Decl.) ¶147

End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. **An MMH-based MAC (Message Authentication Code) optionally provides message integrity.** Keys are distributed by the CMS to the two endpoints.

EX1007 (PacketCable) at 45

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. **The MAC computation spans the packet’s unencrypted header and encrypted payload.**

EX1007 (PacketCable) at 47

Paper 26 at 46; Paper 44 (Sur-Reply) at 23



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

PacketCable’s silence is consistent with RTP’s lack of authentication

148. PacketCable’s non-disclosure of Element [1.2] is consistent with a POSITA’s understanding of the RTP protocol specification, which explicitly does not define an authentication service, and instead states that “[a]uthentication and message integrity are not defined in the current specification of RTP” and teaches that “[i]t is expected that authentication and integrity services will be provided by lower layer protocols in the future.” EX1008 at 50 (emphasis added). That is, the RTP specification does not disclose inserting a MAC “at end of a whole RTP packet payload,” and, in fact, contemplates authentication and integrity services would be provided by lower layer protocols instead. A person of ordinary skill in the art would therefore have understood that PacketCable does not disclose (explicitly or inherently) “inserting, at the transmitter, authentication data at end of a whole RTP packet payload.”

EX2004 (Stubblebine Decl.) ¶148

9.2 Authentication and Message Integrity

Authentication and message integrity are not defined in the current specification of RTP since these services would not be directly feasible without a key management infrastructure. It is expected that authentication and integrity services will be provided by lower layer protocols in the future.

EX1008 (RTP) at 50

PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Dr. Houh does not dispute that RTP does not define a trailer or that there is space in the RTP header

10 Q. So, you don't dispute in your
11 supplemental declaration that RTP does not define
12 a trailer, correct?

13 MR. BRIT: Objection to form. Lacks
14 foundation.

15 THE WITNESS: What I am rebutting
16 with respect to Dr. Stubblebine's statements
17 is why this header field extension is also
18 not -- I am rebutting his statements about
19 placing the additional information in the
20 header, at least I think in this paragraph.

EX2010 (Houh Dep. Tr.) at 148:10-20

67. Dr. Stubblebine further states that “RTP does not define a trailer and instead defines a mechanism for placing additional information in the header, as explained above.” EX2004, ¶154. He implies that this teaches away from putting the MAC at the end of an RTP packet. But Dr. Stubblebine ignores that the RTP RFC specifically states “[n]ote that this header extension is intended only for limited use. Most potential uses of this mechanism would be better done another way, using the methods described in the previous section.” EX1008, 15. Dr. Stubblebine does not consider better ways of storing the MAC other than in the RTP header RTP header extension even though the RTP RFC explicitly urges the reader to do so. EX1008, 14 (“Additional information that is required for a particular payload format, such as a video encoding, should be carried in the payload section of the packet.”).

EX1033 (Houh Decl.) ¶67

Paper 44 (Sur-Reply) at 23



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Information would be easier to find in the RTP header

150. Dr. Houh does not identify any negative impacts to “performance” that would result from placing, for example, a MAC in “in the middle” of a packet payload or even in the middle of a packet header. In the context of RTP, a POSITA would have understood that RTP provides a header extension mechanisms to allow additional data to be placed in the header. *See* § VI.B.3, *supra*. A POSITA would have understood that the RTP header is comprised of fixed-length or length-determinable portions (including the extended portion), making it computationally easier (and thus more efficient) to find the data there as opposed to the payload area, which is of a variable (and undefined) length and would require more computational resources to find the data there. *See* § VI.B.3, *supra*.

EX2004 (Stubblebine Decl.) ¶150

43. The RTP header includes an extension bit “X” that, when set, means that “the fixed header is followed by exactly one header extension” to support additional information. EX1008 at 14-15.

extension (X): 1 bit
If the extension bit is set, the fixed header is followed by exactly one header extension, with a format defined in Section 5.3.1.

EX1008 at 11

EX2004 (Stubblebine Decl.) ¶43 (in § VI.B.3)

Paper 26 (POR) at 47-48; Paper 44 (Sur-Reply) at 24



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Information would be easier to find in the RTP header

packet payload (which has a variable and undefined length). EX1003, ¶178. A POSITA would have understood that data can be found more quickly in an area with defined and/or fixed-length (or easily-determinable-length) fields, such as a header. And, as explained above, RTP provides mechanisms for placing additional data in the header (e.g., in a header extension), which is advantageously “less expensive to process because it is not conditional nor in a variable location.” See EX1008 at 14-15; §§ VI.B.3 and X.A.2.b, *supra*. Moreover, a POSITA would have known and considered that RTP looks for information in the header to check for validity issues, including “to verify that incoming packets have been correctly decrypted.” EX1008 at 59; See § VI.B.3, *supra*.

EX2004 (Stubblebine Decl.) ¶152

43. The RTP header includes an extension bit “X” that, when set, means that “the fixed header is followed by exactly one header extension” to support additional information. EX1008 at 14-15.

extension (X): 1 bit
If the extension bit is set, the fixed header is followed by exactly one header extension, with a format defined in Section 5.3.1.

EX1008 at 11

EX2004 (Stubblebine Decl.) ¶43 (in § VI.B.3)

44. RTP looks for information in the header to check for validity issues, including “to verify that incoming packets have been correctly decrypted.” EX1008 at 59.

A.1 RTP Data Header Validity Checks

An RTP receiver should check the validity of the RTP header on incoming packets since they might be encrypted or might be from a different application that happens to be misaddressed. Similarly, if encryption is enabled, the header validity check is needed to verify that incoming packets have been correctly decrypted, although a failure of the header validity check (e.g., unknown payload type) may not necessarily indicate decryption failure.

EX1008 at 59

EX2004 (Stubblebine Decl.) ¶44 (in § VI.B.3)

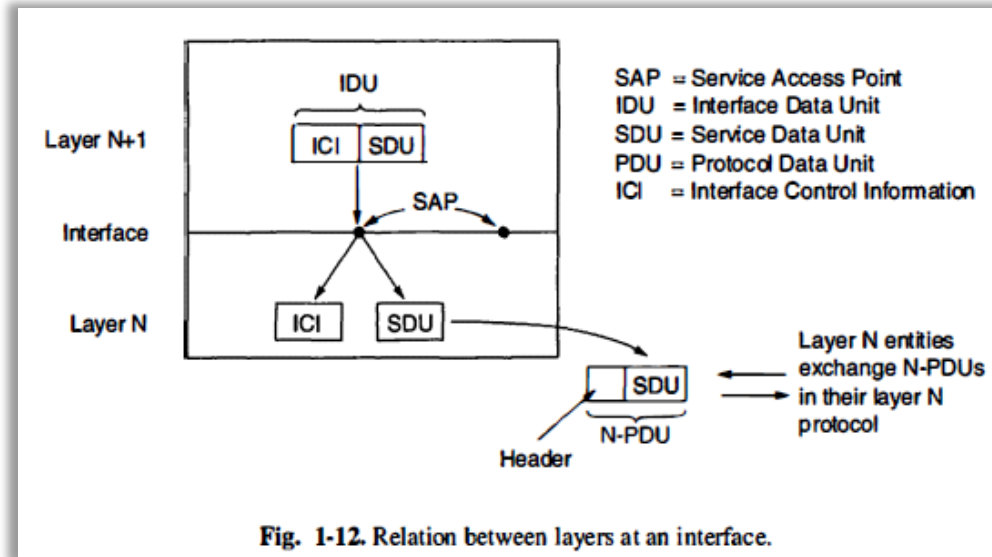
Paper 26 (POR) at 48-49; Paper 44 (Sur-Reply) at 24



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Petitioners identify no “fragmentation” issues

In order to transfer the SDU, the layer n entity may have to fragment it into several pieces, each of which is given a header and sent as a separate PDU (Protocol Data Unit) such as a packet. The PDU headers are used by the peer entities



EX1009 (Tanenbaum) at 43-44

21 But, in this case what I am talking
22 about is that if one were to put the MAC in
1 the middle of the data portion of a single
2 packet, that there is -- it would become two
3 portions.

EX2010 (Houh Dep. Tr.) at 145:21-146:3

16 But these are reasons why a POSITA
17 would not want to locate the data in the
18 middle of the data portion of a single
19 packet. They would not locate the MAC or
20 signature there.

EX2010 (Houh Dep. Tr.) at 147:16-20

Paper 26 (POR) at 48; Paper 44 (Sur-Reply) at 23-24

PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

The use of checksum services in lower layers does not motivate the use of a trailer in the RTP packet

155. Furthermore, as explained above, RTP can rely on the underlying UDP protocol for providing checksum services, EX1008 at 3; § X.A.2.b, *supra*, thus a POSITA would not have been motivated to include a trailer at the end of an RTP packet based on the use of checksums in lower layer protocols. RTP also looks for information in the *header* to check for validity issues, including “to verify that incoming packets have been correctly decrypted,” EX1008 at 59, which further demonstrates that a POSITA would not have been motivated to add a trailer to an RTP packet based on the location of error checking data in a lower level protocol. See § X.A.2.b, *supra*.

EX2004 (Stubblebine Decl.) ¶150

37. According to the RTP specification, RTP “provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video.” EX1008 at 3. The RTP protocol indicates that “[a]pplications typically run RTP on top of UDP to make use of its multiplexing and checksum services....” EX1008 at 3.

This memorandum specifies the real-time transport protocol (RTP), which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, timestamping and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols (see Section 10). RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network.

EX1008 at 3

EX2004 (Stubblebine Decl.) ¶37

Paper 26 (POR) at 49; Paper 44 (Sur-Reply) at 24



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Adding a trailer does not avoid the need for storing the packet in memory

156. I also disagree with Dr. Houh’s general suggestion that a POSITA would have understood that “the authentication data would go at the end of the whole RTP packet payload because it would reduce the latency of delivering the packet *since* placing the authentication data at the beginning of the payload requires storing the packet, computing the authentication data, transmitting the packet to the network” I disagree with Dr. Houh’s concern about “storing the packet”. For example, all PDU components need to be stored at least in temporary memory as the PDU is being prepared for passing down the protocol stack to the next layer. A POSITA would not have been motivated to add a trailer to end of the whole RTP packet payload based to avoid storing the packet. I further disagree that “computing the authentication data” would motivate the use of a trailer. The same authentication process would be used to compute the authentication data if the authentication data were placed in the header or the beginning of the packet payload. Thus, a POSITA would not have been motivated to add a trailer to end of the whole RTP packet based on computing the authentication data.

EX2004 (Stubblebine Decl.) ¶156

Paper 26 (POR) at 49-50; Paper 44 (Sur-Reply) at 24



PacketCable + Handley [1.2]: “by inserting, at the transmitter, authentication data at end of a whole RTP packet payload”

Adding a trailer does not reduce transmission delay

Further, a POSITA would have understood and found obvious that placing authentication at the end of the payload would allow the transmitter to transmit data while simultaneously computing the checksum and prevent any unnecessary transmission delay by having to first compute the checksum and then transmit the payload. EX1003, ¶178. Thus, a POSITA would have understood and found obvious that placing authentication at the end of the whole RTP packet payload would be the best solution to increase transmission speeds and decrease memory usage needed to encrypt and decrypt the data. *Id.*, ¶178. A POSITA would have

Paper 3 (Petition) at 47

159. Simply put, Dr. Houh’s arguments regarding “placement of authentication at the end of the whole RTP packet payload” are inaccurate because bit-by-bit transmission occurs at the physical layer (not at the RTP packet level), and the location of authentication data within the higher layer PDUs (such as an RTP packet) would not make that transmission faster as Dr. Houh suggests.

EX2004 (Stubblebine Decl.) ¶158-159

Paper 26 (POR) at 50-51; Paper 44 (Sur-Reply) at 24



PacketCable + Handley Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



PacketCable + Handley: Claims 22 and 24

Petitioners' Reply arguments are untimely and improper

Examples of indications that a new issue has been raised in a reply include new evidence necessary to make out a *prima facie* case for the patentability or unpatentability of an original or proposed substitute claim, such as newly raised rationale to combine the prior art references that was not expressed in the petition. See *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369–70 (Fed. Cir. 2016) (holding that the Board did not err in refusing the reply brief as improper under 37 C.F.R. § 42.23(b) because petitioner relied on an entirely new rationale to explain why one of skill in the art would have combined the references at issue). It is also improper for a reply to present new evidence (including new expert testimony) that could have been presented in a prior filing, for example newly cited prior art references intended to “gap-fill” by teaching a claim element that was not present in the prior art presented with the petition. See *Genzyme Therapeutic Prods. Ltd. v. Biomarin Pharm. Inc.*, 825 F.3d 1360, 1365–69 (Fed. Cir. 2016) (proper for Board to rely on prior art references submitted with petitioner’s reply to establish the state of the art at the time of the invention in response to patent owner arguments).

Consolidated Trial Practice Guide
(Nov. 2019) at 74-75

Paper 26 (POR) at 54;
Paper 44 (Sur-Reply at 24-25)



Ground 3: Obviousness over PacketCable + Basturk

Ground	Assertion	Petitioned Claims
1	Obvious under § 103 in view of Handley in combination with Basturk	1-21, 23, 25-28
2	Obvious under § 103 in view of PacketCable in combination with Handley	1-28
3	Obvious under § 103 in view of PacketCable in combination with Basturk	1-28
4	Obvious under § 103 in view of Handley in combination with Basturk and PacketCable	22, 24

Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify PacketCable in view of Basturk

Basturk teaches away from modifying the application layer

Our discussion of security features which follows takes the perspective of a designer and architect of a secure communications medium. It reflects the need to add security functionality in a way which is consistent with, and best matches, the existing communication structure. To this end, we distinguish security features according to the layer of the communication structure to which they are most naturally associated. We found that the traditional features are mostly application level, while the new ones we deem necessary are transport level.

EX1006 (Basturk) at 3

COMPATIBILITY. Usually, applications are written on top of an existing transport protocol before any security is included in it. We want to assure *compatibility* of a secure version of this protocol with the regular non-secure version. The secure transport protocol then becomes a superset of the regular transport protocol. Applications using the regular transport protocol should not have to be modified at all.

EX1006 (Basturk) at 5

Paper 26 (POR) at 30-31, 55



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify PacketCable in view of Basturk

Basturk teaches away from modifying the application layer

³ An implicit assumption is that the application is not performing its own acknowledgments and retransmission, but, more naturally, relying on the transport for these features. Indeed, asking the application to duplicate these transport functions is usually poor design in that it belies the layered communication structure, and would also adversely affect performance.

EX1006 (Basturk) at 4

The manner in which security against replay is guaranteed illustrates well an advantage of security at the transport level. Sequencing is a standard and already present transport function. We simply exploit its presence. Had we wanted to prevent replay at the application level we would had to implement sequencing with transport level counters and provide for our own checking and retransmission, thereby not only making implementation significantly harder but duplicating the transport functionality and degrading performance.

EX1006 (Basturk) at 12

Paper 26 (POR) at 30-31, 55



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify PacketCable in view of Basturk

Basturk’s reliability protocols is incompatible with PacketCable for the same reasons as Handley

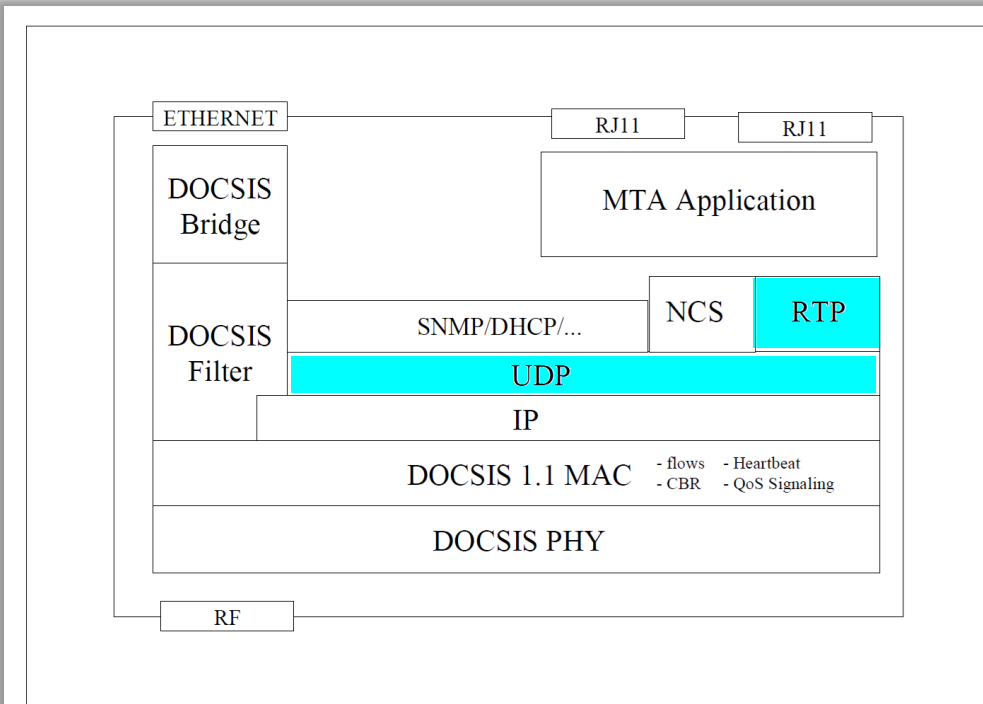


Figure 4. E-MTA Conceptual Functional Architecture

EX1007 (PacketCable) at 20

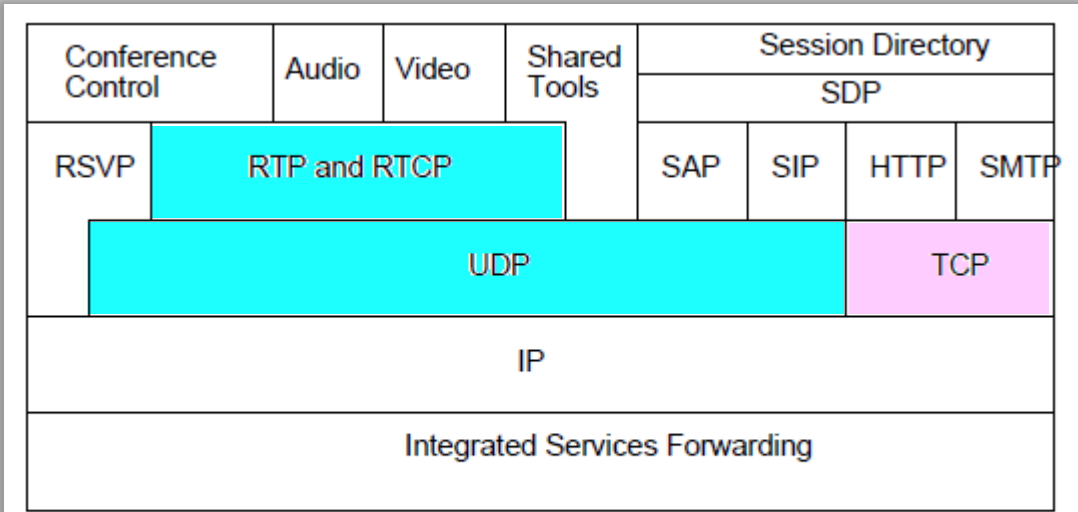


Figure 1: Internet multimedia conferencing protocol stacks

EX1005 (Handley) at 3

Paper 26 (POR) at 55-56



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify PacketCable in view of Basturk

Preliminary context retrieval is unavoidable in PacketCable; “on-the-fly” is not possible

173. According to PacketCable’s security framework, “[t]he MAC computation spans the packet’s unencrypted header and encrypted payload.” EX1007 at 47. Thus, the MAC computation—whether the MMH algorithm of PacketCable or Basturk’s algorithm, cannot even begin to be processed on the transmitter until encryption of the encrypted payload happens. To perform the encryption, context retrieval must necessarily take place prior to the start of any MAC computation over the encrypted payload. This is so even with Basturk’s MAC algorithm (which requires no key to compute the hash portion of the MAC computation) because even the portion that requires no key is computed over the entire encrypted data. A context retrieval is necessary to retrieve the key used to encrypt the payload data. Thus, the basic security structure of the PacketCable design means “on-the-fly” cannot be achieved on the packet transmission side, and thus no purported benefits of “on-the-fly” can be realized.

EX2004 (Stubblebine Decl.) ¶173

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet’s unencrypted header and encrypted payload.

EX1007 (PacketCable) at 47

Paper 26 (POR) at 57-58



Motivation to Combine: The POSITA Would Not Have Been Motivated to Modify PacketCable in view of Basturk

Preliminary context retrieval is unavoidable in PacketCable; “on-the-fly” is not possible

Here we see there are two phases of the algorithm. The first is in the “For $i=1$ to k ” loop. The second component starting with “Reduce...” operates on the results of the first portion (i.e., SumHigh and SumLow). Note that the first phase requires access to both a portion of the message, e.g. $msg[i]$ as well as a portion of the cryptographic key, e.g. $key[i]$ for every block of the message $m[1]$ to $m[k]$. Thus, to even begin processing the secure MAC algorithm based on MMH the cryptographic key is necessary.

177. As such, a context retrieval would be required before processing any portion of the message using the secure MAC based on MMH. Consequently, the delay associated with context retrieval would be unavoidable in PacketCable, meaning that “on-the-fly” cannot be achieved.

EX2004 (Stubblebine Decl.) ¶¶ 176-1773

Each RTP packet may include an optional message authentication code (MAC). The MAC algorithm can also be negotiated, although the only one that is currently specified is MMH. The MAC computation spans the packet’s unencrypted header and encrypted payload.

EX1007 (PacketCable) at 47

A pseudo-code for MMH on such machine may be as follows

MMH(msg, key)

1. $SumHigh = SumLow = 0$
2. For $i = 1$ to k
3. load $msg[i]$
4. load $key[i]$
5. $\langle ProdHigh, ProdLow \rangle = msg[i] * key[i]$
6. $SumLow = SumLow + ProdLow$
7. $SumHigh = SumHigh + ProdHigh + carry$
8. Reduce $\langle SumHigh, SumLow \rangle \bmod 2^{32} + 15$ and then $\bmod 2^{32}$

EX2008 (Halevi) at 9

Paper 26 (POR) at 57-58



PacketCable + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



PacketCable + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



PacketCable + Basturk Do Not Disclose or Render Obvious Every Element

Missing Claim Elements

[1.1] providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer

[1.2] by inserting, at the transmitter, authentication data at end of a whole RTP packet payload

[1.3] ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data

EX1001 ('682 patent), at claim 1



Ground 4: Obviousness over Handley + PacketCable + Basturk

Ground	Assertion	Petitioned Claims
1	Obvious under § 103 in view of Handley in combination with Basturk	1-21, 23, 25-28
2	Obvious under § 103 in view of PacketCable in combination with Handley	1-28
3	Obvious under § 103 in view of PacketCable in combination with Basturk	1-28
4	Obvious under § 103 in view of Handley in combination with Basturk and PacketCable	22, 24

Ground 4: Obviousness over Handley + PacketCable + Basturk

Petitioners' Reply arguments are untimely and improper

Examples of indications that a new issue has been raised in a reply include new evidence necessary to make out a *prima facie* case for the patentability or unpatentability of an original or proposed substitute claim, such as newly raised rationale to combine the prior art references that was not expressed in the petition. See *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369–70 (Fed. Cir. 2016) (holding that the Board did not err in refusing the reply brief as improper under 37 C.F.R. § 42.23(b) because petitioner relied on an entirely new rationale to explain why one of skill in the art would have combined the references at issue). It is also improper for a reply to present new evidence (including new expert testimony) that could have been presented in a prior filing, for example newly cited prior art references intended to “gap-fill” by teaching a claim element that was not present in the prior art presented with the petition. See *Genzyme Therapeutic Prods. Ltd. v. Biomarin Pharm. Inc.*, 825 F.3d 1360, 1365–69 (Fed. Cir. 2016) (proper for Board to rely on prior art references submitted with petitioner’s reply to establish the state of the art at the time of the invention in response to patent owner arguments).

Consolidated Trial Practice Guide
(Nov. 2019) at 74-75

Paper 26 (POR) at 54;
Paper 44 (Sur-Reply at 24-25)

