Petitioners' Demonstrative Exhibits for Oral Argument

Meta Platforms, Inc., et al. v. VL Collective IP LLC

IPR 2023-00923

U.S. Patent No. 7,226,682

Patent Trial and Appeal Board

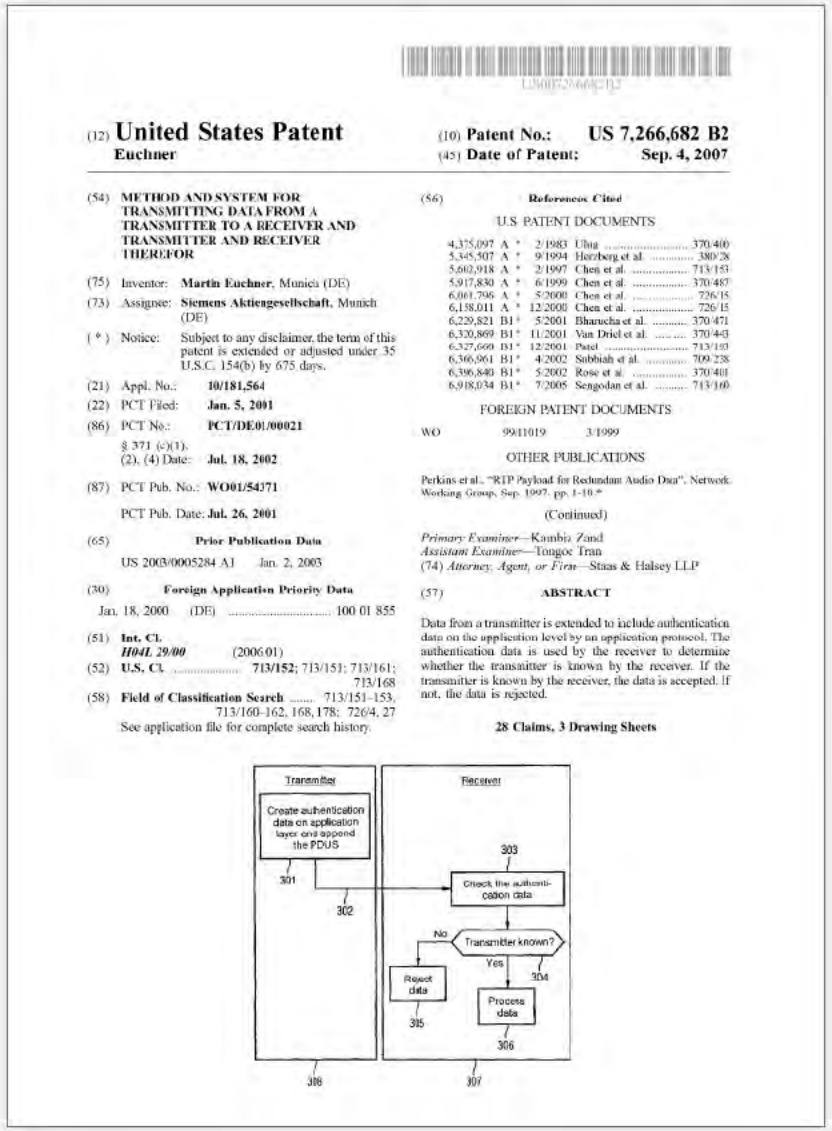
September 10, 2024

Alexandria, Virginia

U.S. Patent No. 7,266,682

IPR2023-00923

Overview



(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(b) 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 Uhra 370/400
5,345,507 A * 9/1994 Herzberg et al. 380/26
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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/463
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey LLP

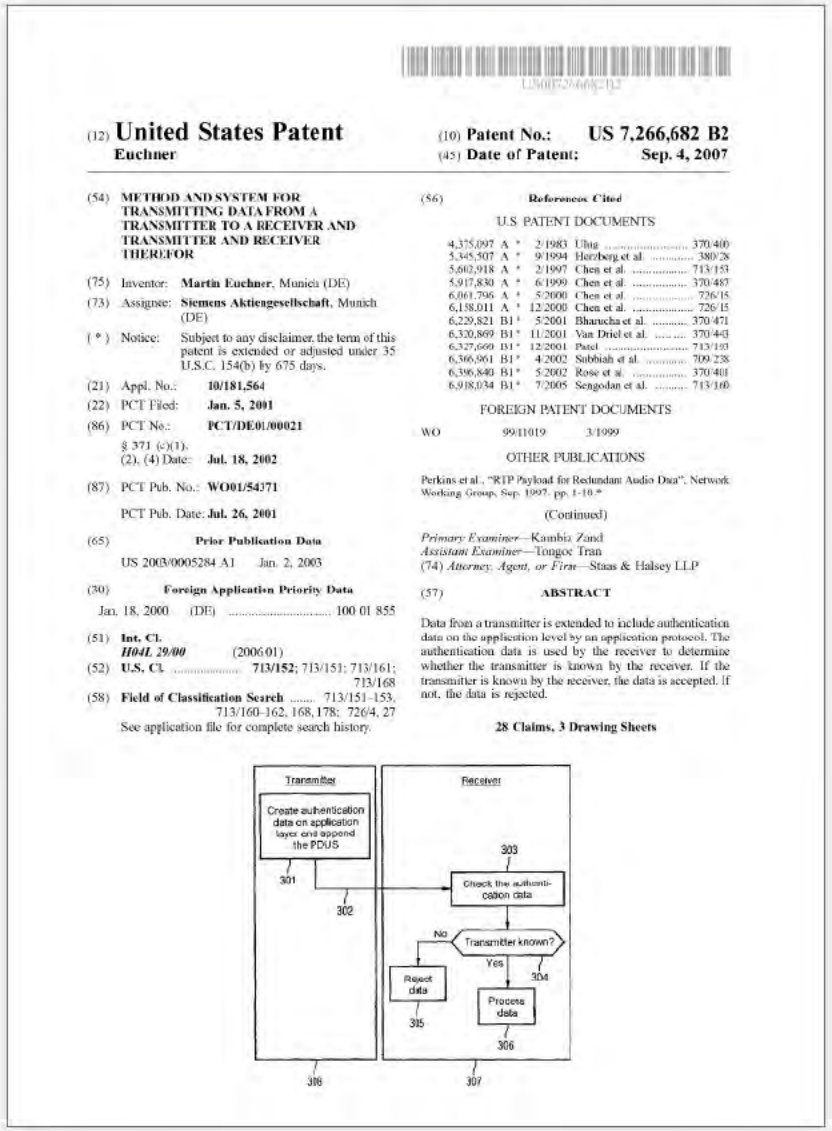
(57) **ABSTRACT**

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

1. **Background**
2. **Prior Art**
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. **Grounds**
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Overview



(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(b) 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 Uhra 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/463
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

1. **Background**
2. Prior Art
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. Grounds
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Invalidity Grounds

Ground I (Claims 1-21, 23, 25-28)

- Obvious under § 103 in view of Handley in combination with Basturk

Ground II (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Handley

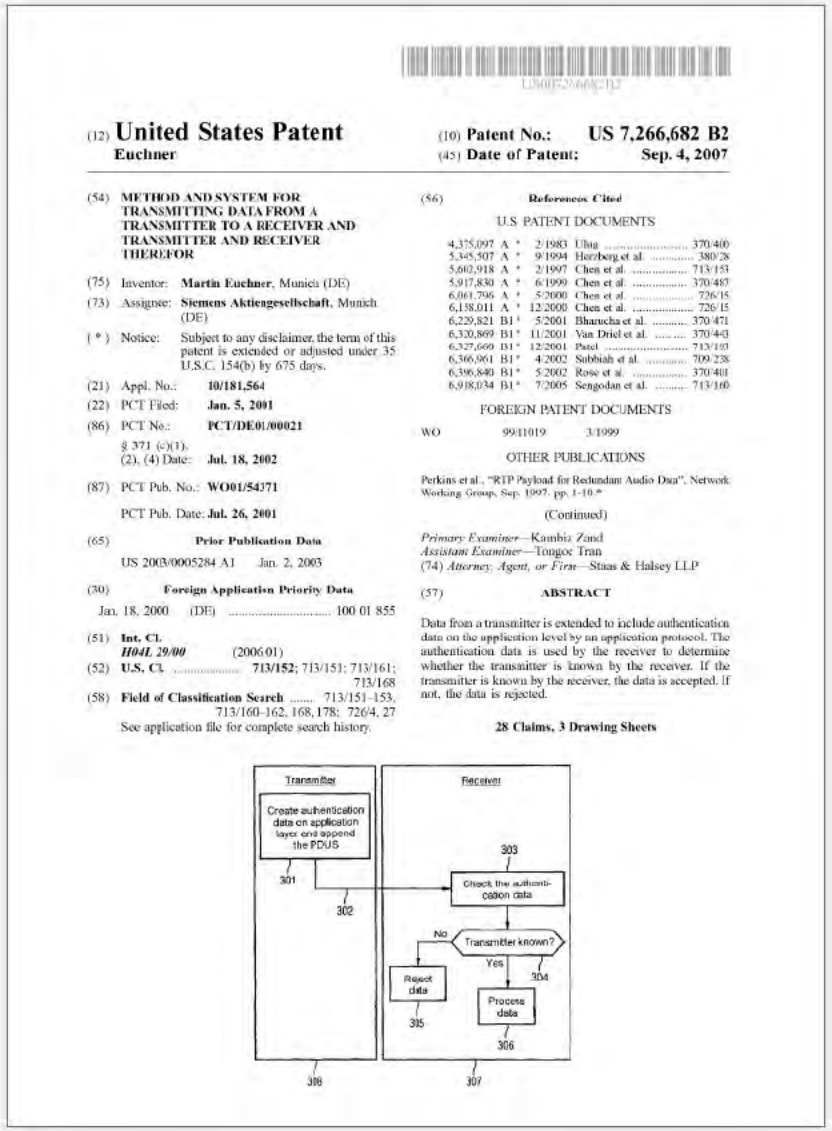
Ground III (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Basturk

Ground IV (Claims 22, 24)

- Obvious under § 103 in view of Handley in combination with Basturk and PacketCable

Overview



(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(b) 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 Uhra 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/463
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey LLP

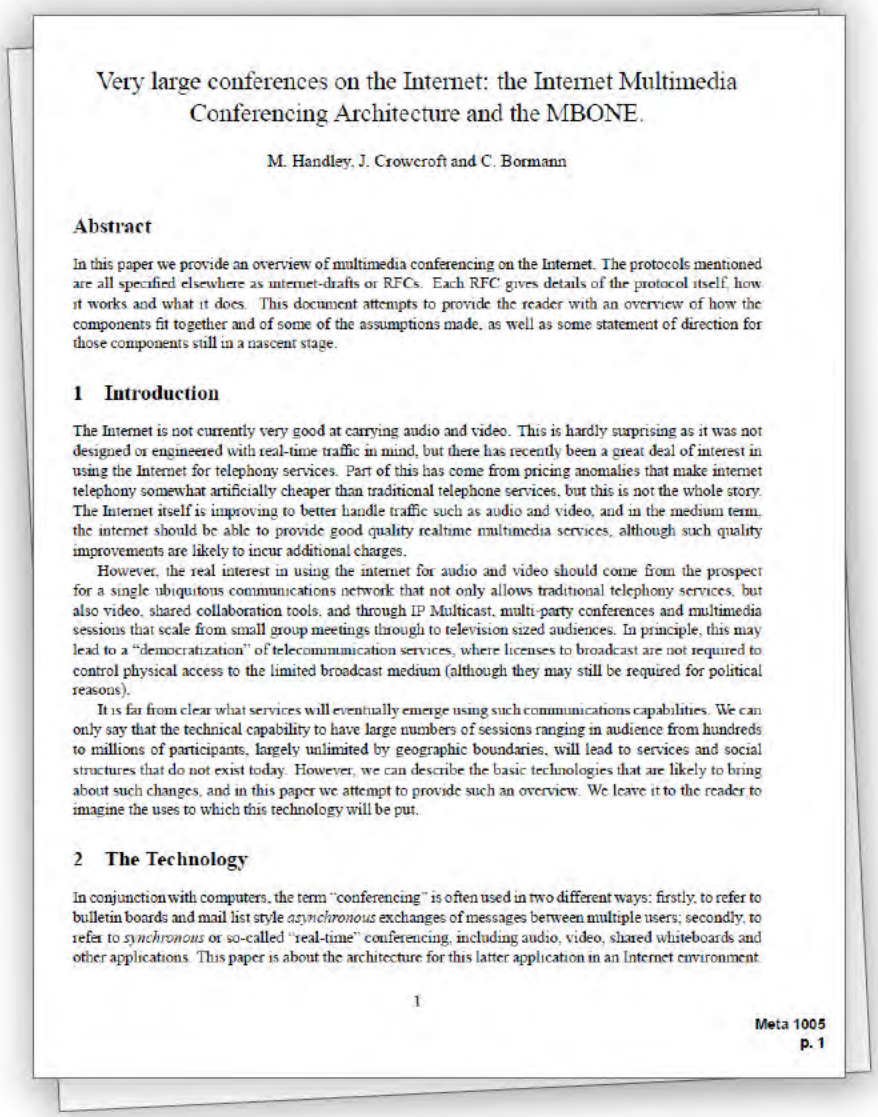
(57) **ABSTRACT**

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

1. Background
2. **Prior Art**
   a. **Handley (Ex. 1005)**
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. Grounds
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Prior Art - Handley (Ex. 1005)



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

- Handley provides an overview of "real-time" multimedia conferencing on the Internet
- Prior art reference in Grounds I, II, and IV
- Petition asserts Handley is §§ 102(a) and 102(b) prior art

Petition (Paper 3) at 4; EX1005 (Handley)

Patent Owner's Arguments re Handley (Ex. 1005) Miss the Mark

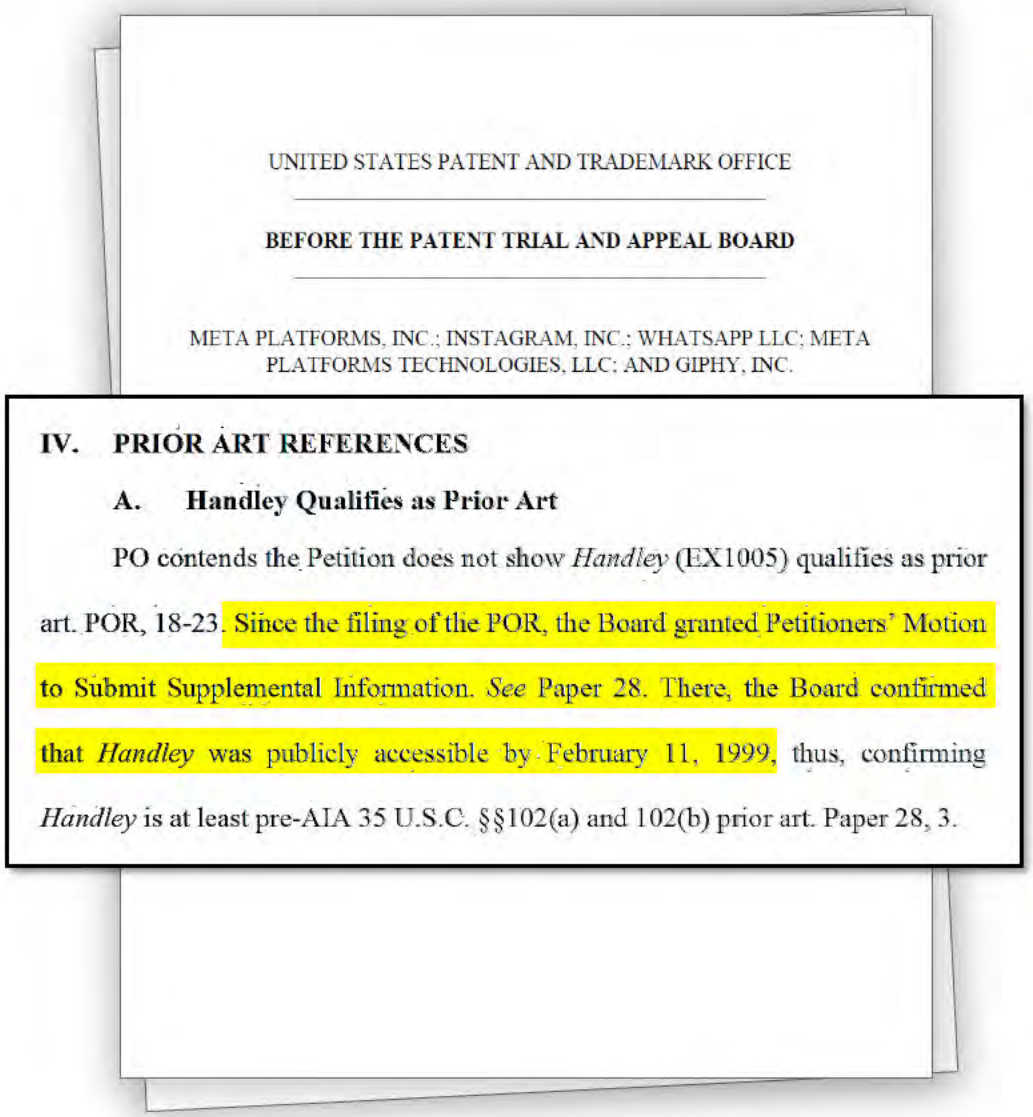
Patent Owner argues:

1. Petitioners forfeited the right to argue that Handley was publicly accessible and to rely on supplemental evidence

2. Petitioners' supplemental evidence proves that Handley is not prior art

PO Sur-Reply (Paper 44) at 2-10

Petitioner did not Forfeit its Right to Argue Handley was Publicly Accessible



UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC; META PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.

IV. PRIOR ART REFERENCES

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.

- Petitioners cited the Decision granting its Motion to Submit Supplemental Information ("Supplemental Information Decision") in their Reply
- The issue of whether Petitioners raised an alternative theory of public availability was resolved by the interlocutory Supplemental Information Decision
- The issue of Handley's public accessibility was the subject preliminary findings in the Supplemental Information Decision

Petitioners' Reply to POR (Paper 37) at 2

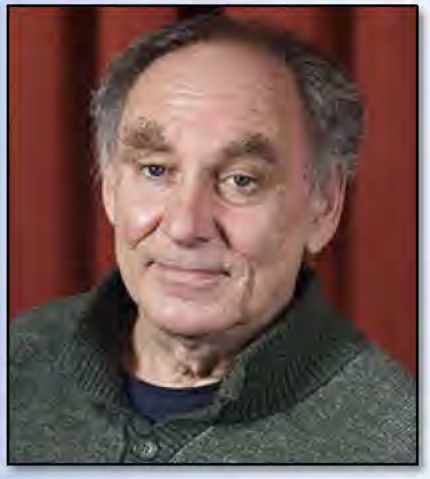
Petitioner's Motion to Submit Supplemental Information

Petitioners filed motion to submit supplemental information in support of Handley's public accessibility (Paper 21)

- Ex. 1016 – Declaration of Handley co-author, Dr. Jon Crowcroft
- Ex. 1017 – Supplemental Declaration of Dr. Henry Houh
- Ex. 1018 – Supplemental Declaration of Dr. Sylvia Hall-Ellis
- Exs. 1020-1026 – Archived websites from the Wayback Machine and a separate authenticating declaration therefrom
- Ex. 1027 – Online publication version of Handley
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Co-author of Handley (Ex. 1005) Confirms Public Availability

Co-Author of Handley (Ex. 1005)



Dr. Jon Crowcroft

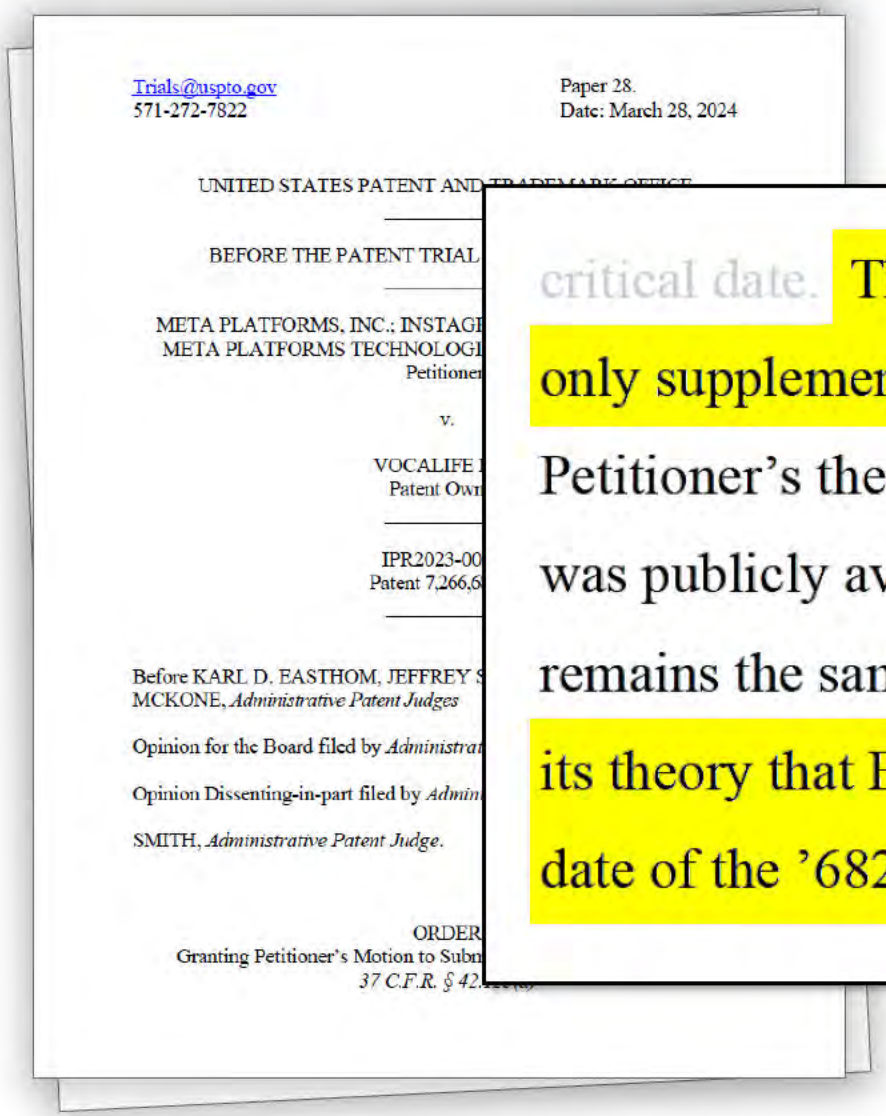
- For example, Dr. Crowcroft confirmed the public availability of Handley

II. Handley Reference

6. I am a co-author of *Very large conferences on the Internet: the Internet Multimedia Conferencing Architecture and the MBONE*. I have been informed by counsel for Petitioners that this article was used by Petitioners in IPR2023-00923 as a prior art reference. This article was labeled EX1005 by Petitioners. I have been asked to confirm the publication status and public accessibility of EX1005 and to determine whether it was publicly accessible and/or published by at least February 11, 1999. I can indeed confirm that it was.

EX1016 (Crowcroft Declaration) at ¶ 6.

Panel Decides Whether Supplemental Information Changes Theories


Trials@uspto.gov
571-272-7822

Paper 28.
Date: March 28, 2024

UNITED STATES PATENT AND

BEFORE THE PATENT TRIAL

META PLATFORMS, INC.; INSTAGR
META PLATFORMS TECHNOLOGI
Petitioner

v.

VOCALIFE
Patent Own

IPR2023-00
Patent 7,266,6

Before KARL D. EASTHOM, JEFFREY S
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administrat*

Opinion Dissenting-in-part filed by *Admin*

SMITH, *Administrative Patent Judge*.

ORDER
Granting Petitioner's Motion to Subm
37 C.F.R. § 42.

critical date. The supplemental information here does not change theories as it only supplements evidence as to the public availability of Exhibit 1005. Petitioner's theory that Exhibit 1005 is prior art to the '682 patent because it was publicly available before the effective filing date of the '682 patent remains the same. Pet. 4; Motion 4. The supplemental evidence in support of its theory that Exhibit 1005 was publicly available before the effective filing date of the '682 patent is evidence, not a new theory.

Order (Paper 28) at 6

Panel's Interlocutory Decision Governs the Trial

37 CFR § 42.71 – Decision on petitions or motions

. . .

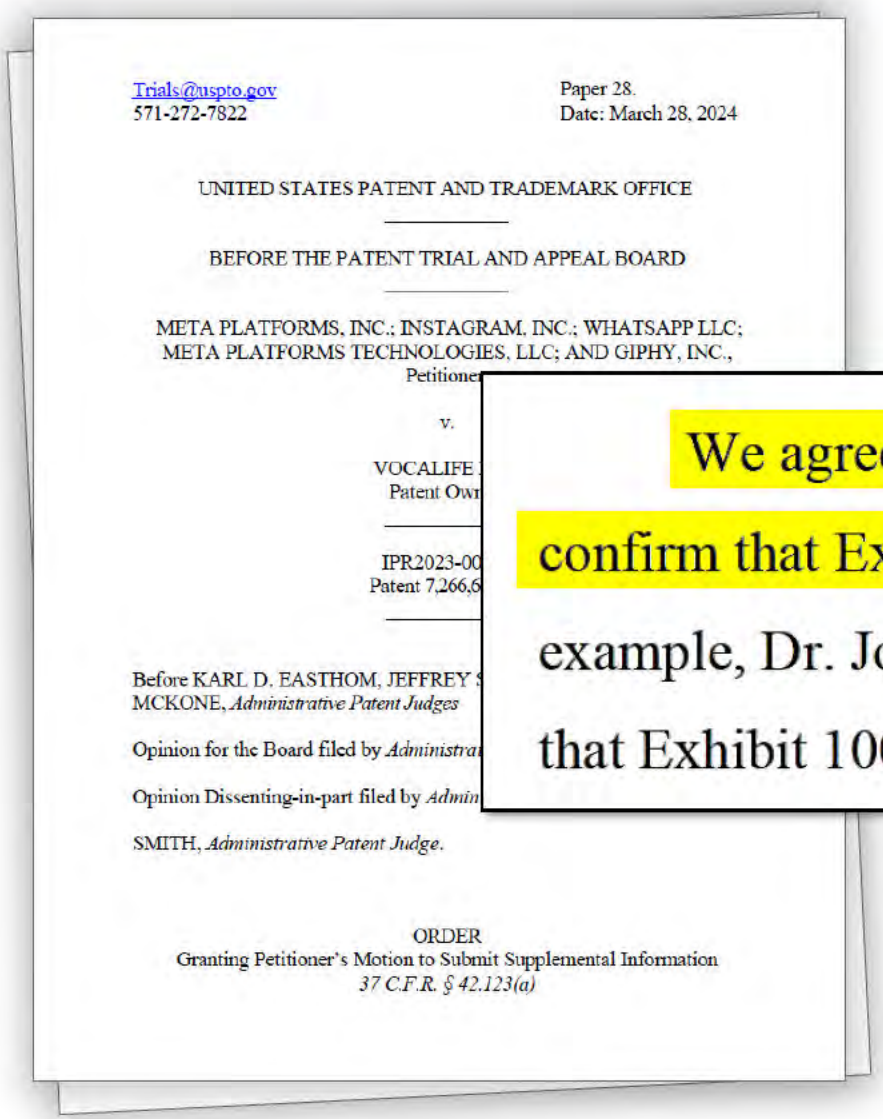
(b) Interlocutory decisions. A decision on a motion without a judgment is not final for the purposes of judicial review. If a decision is not a panel decision, the party may request that a panel rehear the decision. When rehearing a non-panel decision, a panel will review the decision for an abuse of discretion. A panel decision on an issue will govern the trial.

Panel's Interlocutory Decision Governs the Trial

77 FR 48669

Section 42.71(b) provides for interlocutory decisions. The rule makes clear that a decision short of judgment is not final, but a decision by a panel would govern the trial. Experience has shown that the practice of having panel decisions bind further proceedings has eliminated much of the uncertainty and added cost that result from deferring any final decision until the end of the proceeding.

Panel (at Least Preliminarily) Finds that Handley Publicly Accessible



Trials@uspto.gov
571-272-7822

Paper 28.
Date: March 28, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC;
META PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.,
Petitioner

v.

VOCALIFE
Patent Own

IPR2023-00
Patent 7,266,6

Before KARL D. EASTHOM, JEFFREY
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administra*

Opinion Dissenting-in-part filed by *Admin*

SMITH, *Administrative Patent Judge*.

ORDER
Granting Petitioner's Motion to Submit Supplemental Information
37 C.F.R. § 42.123(a)

We agree with Petitioner that Exhibits 1016–1018 and 1020–1028 confirm that Exhibit 1005 was publicly accessible by February 11, 1999. For example, Dr. Jon Crowcroft testifies that he is a co-author of Exhibit 1005 and that Exhibit 1005 was publicly accessible by at least February 11, 1999 on his

Order (Paper 28) at 3

PO's Reliance on *Unified Patents* is Misplaced

"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)

PO's Reliance on its Cited Case Law is Misplaced

"Petitioner only addresses the first test ('field of endeavor') and has thus waived any arguments related to the second test ('reasonably pertinent to the particular problem')."

Apple, Inc. v. Gesture Technology Partners, LLC, IPR2021-00923, Paper 27 at 11

"However, when a patent owner attempts to antedate an asserted prior art reference, the patent owner assumes a temporary burden of production" . . . "The burden of production cannot be met simply by throwing mountains of evidence at the Board without explanation or identification of the relevant portions of that evidence. One cannot reasonably expect the Board to sift through hundreds of documents, thousands of pages, to find the relevant facts."

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

"In this regard, the Reply simply states 'the record includes well over a dozen [prior art] references . . . that describe solutions for determining oxygen saturation at the wrist,' as explained by Dr. Anthony's declaration testimony and without any discussion of particular disclosures in the Exhibits. Pet. Reply 13–14 (citing Ex. 1042 ¶¶ 27–34). This improperly 'throw[s] mountains of evidence at the Board without explanation or identification of the relevant portions of that evidence.'" *Parus*, 70 F.4th at 1371.

Apple Inc. v. Masimo Corp., IPR2022-01465, Paper 73, at 85-86 (PTAB Feb. 2, 2024).

The *Seabery* Decision is on Point

"The purpose of the trial in an *inter partes* review proceeding is to give the parties an opportunity to build a record by introducing evidence—not simply to weigh evidence of which the Board is already aware."

"As noted supra, Patent Owner's argument focused on Exhibit 1003 (to the exclusion of Exhibits 1018, 1050, and all the other post-institution evidence introduced by Petitioner) ignores the ability of a Petitioner to supplement the record if appropriate. *Genzyme Therapeutic Prods.*, 825 F.3d at 1367. It overlooks also the fact that, despite minor formatting differences, there is no dispute that the text of the Aiteanu thesis is the same across the three documents"

Seabery North America v. Lincoln Global, Inc, IPR2016-00840 , Paper 60 at 9-10 (PTAB Oct. 2, 2017)

Patent Owner's Arguments re Handley (Ex. 1005) Miss the Mark

Patent Owner argues:

~~1. Petitioners forfeited the right to argue that Handley was publicly accessible and to rely on supplemental evidence~~

2. Petitioners' supplemental evidence proves that Handley is not prior art

PO Sur-Reply (Paper 44) at 2-10

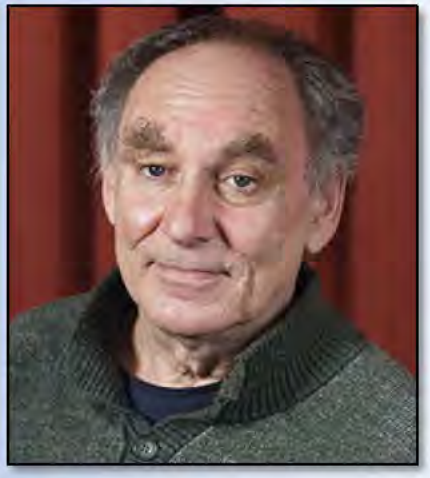
Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

- **Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft**
- Ex. 1017 – Supp. Declaration of Dr. Henry Houh
- Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis
- Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof
- Ex. 1027 – Online publication version of Handley
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Prior Art – Handley (Ex. 1005) – Ex. 1016 Declaration of Dr. Crowcroft

Co-Author of Handley (Ex. 1005)



Dr. Jon Crowcroft

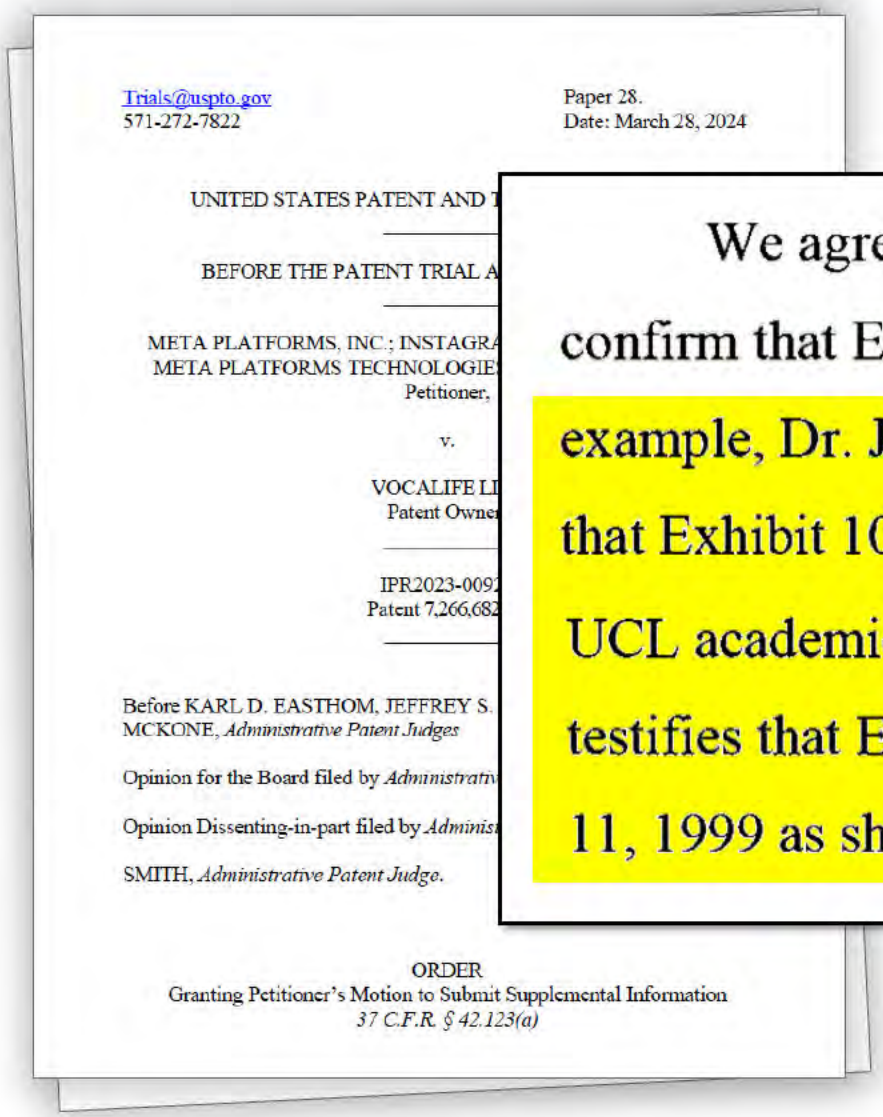
Dr. Crowcroft testified, under oath:

- Ex. 1005 was publicly accessible by at least February 11, 1999 on his UCL academic website and FTP server
- Ex. 1005 was published in Computer Networks on February 11, 1999 as shown in Exs. 1027 and 1028
- Ex. 1005 is identical to Exs. 1027 and 1028 for all intents and purposes
- It is common practice to first upload a paper, publication, or article, prior to formal publication

PO had the opportunity to cross-examine Dr. Crowcroft, but strategically chose not to

EX1016 (Crowcroft Declaration) at ¶¶ 14-17, 20

Findings Made in Supplemental Information Decision



Trials@uspto.gov
571-272-7822

Paper 28.
Date: March 28, 2024

UNITED STATES PATENT AND T

BEFORE THE PATENT TRIAL A

META PLATFORMS, INC.; INSTAGRA
META PLATFORMS TECHNOLOGIE
Petitioner,

v.

VOCALIFE LI
Patent Owne

IPR2023-009
Patent 7,266,68

Before KARL D. EASTHOM, JEFFREY S.
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administrativ*

Opinion Dissenting-in-part filed by *Adminis*

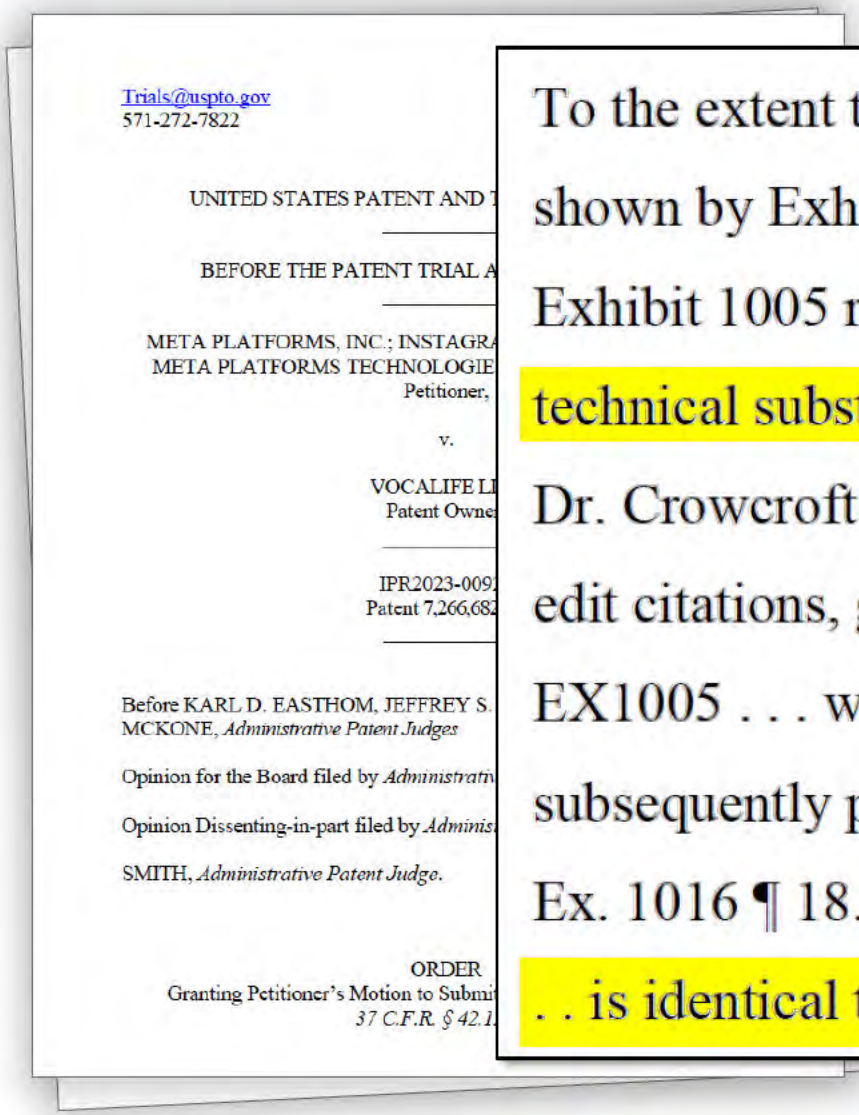
SMITH, *Administrative Patent Judge.*

ORDER
Granting Petitioner's Motion to Submit Supplemental Information
37 C.F.R. § 42.123(a)

We agree with Petitioner that Exhibits 1016–1018 and 1020–1028 confirm that Exhibit 1005 was publicly accessible by February 11, 1999. For example, Dr. Jon Crowcroft testifies that he is a co-author of Exhibit 1005 and that Exhibit 1005 was publicly accessible by at least February 11, 1999 on his UCL academic website and FTP server. Ex. 1016 ¶¶ 6, 13–14, 20. He further testifies that Exhibit 1005 was published in Computer Networks on February 11, 1999 as shown in Exhibits 1027 and 1028. Ex. 1016 ¶¶ 15–16.

Order (Paper 28) at 3-4

Findings Made in Supplemental Information Decision


Trials@uspto.gov
571-272-7822

UNITED STATES PATENT AND

BEFORE THE PATENT TRIAL A

META PLATFORMS, INC.; INSTAGRA
META PLATFORMS TECHNOLOGIE
Petitioner,

v.

VOCALIFE LI
Patent Owne

IPR2023-009
Patent 7,266,68

Before KARL D. EASTHOM, JEFFREY S.
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administrati*

Opinion Dissenting-in-part filed by *Adminis*

SMITH, *Administrative Patent Judge.*

ORDER
Granting Petitioner's Motion to Submi
37 C.F.R. § 42.1

To the extent that Exhibits 1005, 1027, and 1028 have minor differences as shown by Exhibit 2003, the differences do not bear on the subject matter of Exhibit 1005 relied on in the Petition. Dr. Crowcroft testifies that "the technical substance of EX1005, 1027, and 1028 are identical." Ex. 1016 ¶ 16. Dr. Crowcroft testifies that "it is common practice for editors and publishers to edit citations, grammar, and non-substantive text. This is what happened with EX1005 . . . where, after going through the formal publication process, it was subsequently published in Computer Networks . . . on February 11, 1999." Ex. 1016 ¶ 18. Dr. Crowcroft testifies that "the version published as EX1028 . . . is identical to EX1005 for all intents and purposes." Ex. 1016 ¶ 18.

Order (Paper 28) at 4

Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

- Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft
- **Ex. 1017 – Supp. Declaration of Dr. Henry Houh**
- Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis
- Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof
- Ex. 1027 – Online publication version of Handley
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Prior Art - Handley (Ex. 1005) – Ex. 1017 Declaration of Dr. Houh

Petitioners' Technical Expert Witness



Dr. Henry Houh

Dr. Houh testified that he:

- Personally identified and retrieved Ex. 1005
- Confirmed Ex. 1005 public accessibility by comparing Ex. 1005 to the Abstract, Introduction, and Section snippets of Ex. 1027 on Elsevier's ScienceDirect
- Compared Exs. 1027-1028 to Ex. 1005 and found that every citation to Ex. 1005 in the Petition and in his supporting declaration, Ex. 1003, was fully included in both Ex. 1027 and Ex. 1028
- Has personal knowledge and experience with academic publications and Dr. Crowcroft's declaration is consistent with Dr. Houh's understanding of the series of events leading to Exs. 1027 and 1028

EX1017 (Houh Supp. Declaration) at ¶¶ 7-9, 13

Prior Art - Handley (Ex. 1005) – Ex. 1031 Deposition of Dr. Houh

Petitioners' Technical Expert Witness



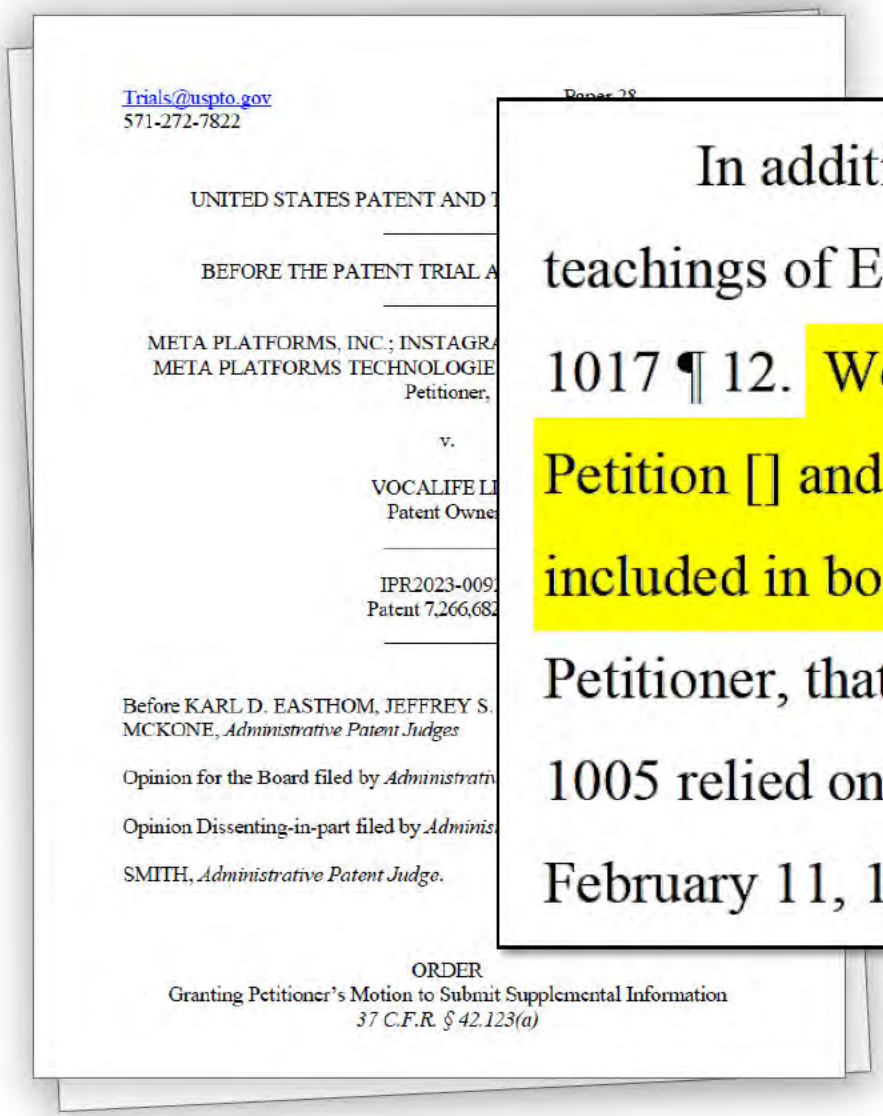
Dr. Henry Houh

Dr. Houh testified that:

- Handley was publicly accessible as of February 11, 1999 and discussed at length about (1) his supplemental declaration, (2) Exhibit 1016 (Crowcroft declaration), (3) Exhibits 1027-1028, and (4) other evidence of Handley's public accessibility

EX1029 (Houh 2/16/2024 Deposition) at pgs. 68-184

Findings Made in Supplemental Information Decision



Trials@uspto.gov
571-272-7822

Paper 28

UNITED STATES PATENT AND

BEFORE THE PATENT TRIAL A

META PLATFORMS, INC.; INSTAGRA
META PLATFORMS TECHNOLOGIE
Petitioner,

v.

VOCALIFE LI
Patent Owne

IPR2023-009
Patent 7,266,68

Before KARL D. EASTHOM, JEFFREY S.
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administrati*

Opinion Dissenting-in-part filed by *Adminis*

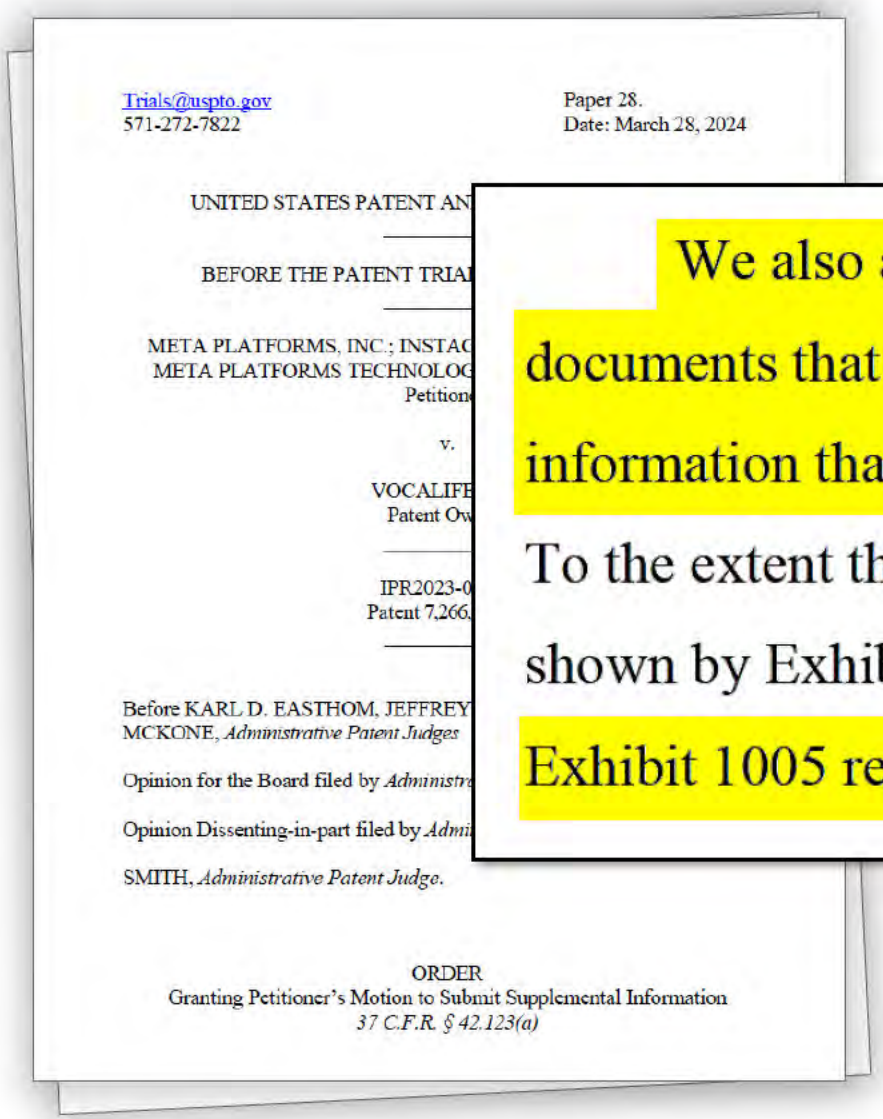
SMITH, *Administrative Patent Judge.*

ORDER
Granting Petitioner's Motion to Submit Supplemental Information
37 C.F.R. § 42.123(a)

In addition to Dr. Crowcroft's testimony, Dr. Houh testifies that the teachings of Exhibit 1005 are fully included in Exhibits 1027 and 1028. Ex. 1017 ¶ 12. We agree with Dr. Houh, that "every citation to EX1005 in [the] Petition [] and in [Dr. Houh's] supporting declaration (EX1003) [are] fully included in both EX1027 and EX1028." *Id.* Therefore, we agree with Petitioner, that Exhibits 1027 and 1028 show that the teachings of Exhibit 1005 relied on in the Petition were published in Computer Networks on February 11, 1999. *See Valve Corporation v. Ironburg Inventions LTD.*, 8

Order (Paper 28) at 4

Findings Made in Supplemental Information Decision



Trials@uspto.gov
571-272-7822

Paper 28.
Date: March 28, 2024

UNITED STATES PATENT AN

BEFORE THE PATENT TRIA

META PLATFORMS, INC.; INSTAG
META PLATFORMS TECHNOLOG
Petition

v.

VOCALIFE
Patent Ow

IPR2023-0
Patent 7,266,

Before KARL D. EASTHOM, JEFFREY
MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administr*

Opinion Dissenting-in-part filed by *Admi*

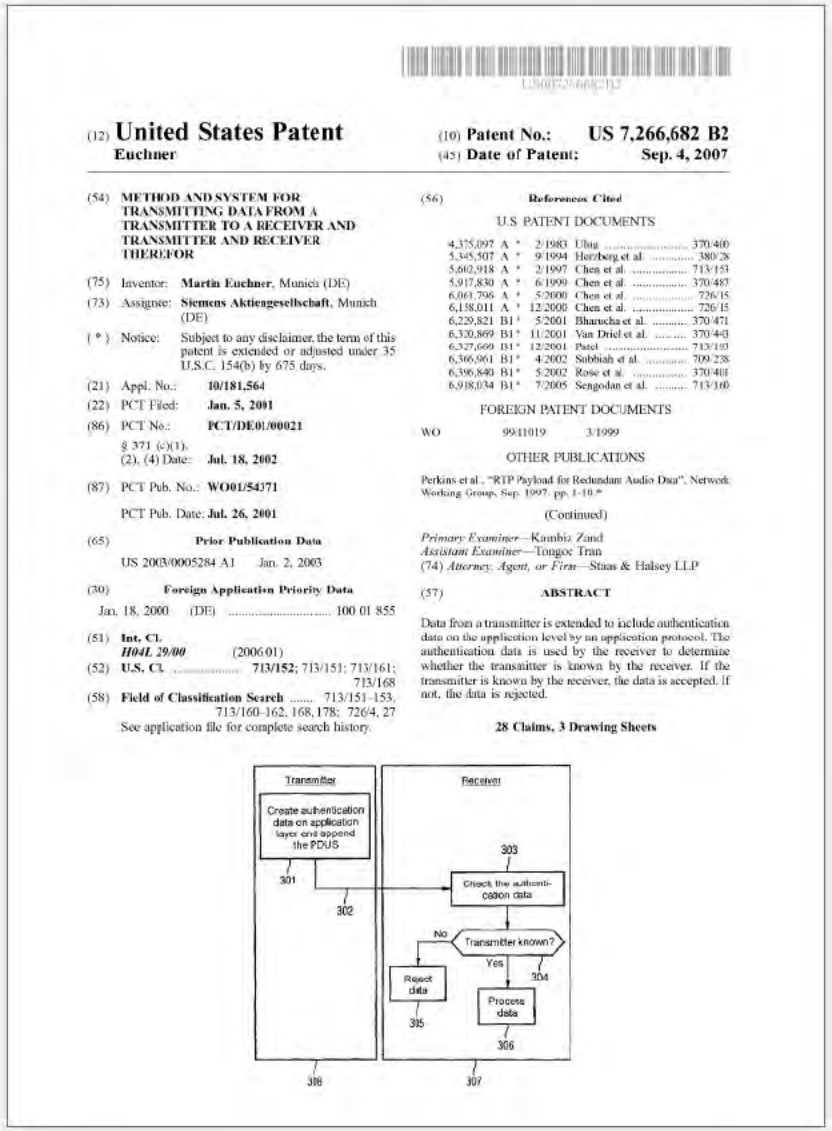
SMITH, *Administrative Patent Judge.*

ORDER
Granting Petitioner's Motion to Submit Supplemental Information
37 C.F.R. § 42.123(a)

We also agree with Petitioner that Exhibits 1027 and 1028 are not new documents that replace Exhibit 1005. Rather, these exhibits are supplemental information that provide evidence as to the public availability of Exhibit 1005. To the extent that Exhibits 1005, 1027, and 1028 have minor differences as shown by Exhibit 2003, the differences do not bear on the subject matter of Exhibit 1005 relied on in the Petition. Dr. Crowcroft testifies that "the

Order (Paper 28) at 4

Overview



(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(b) 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 Uhra 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey LLP

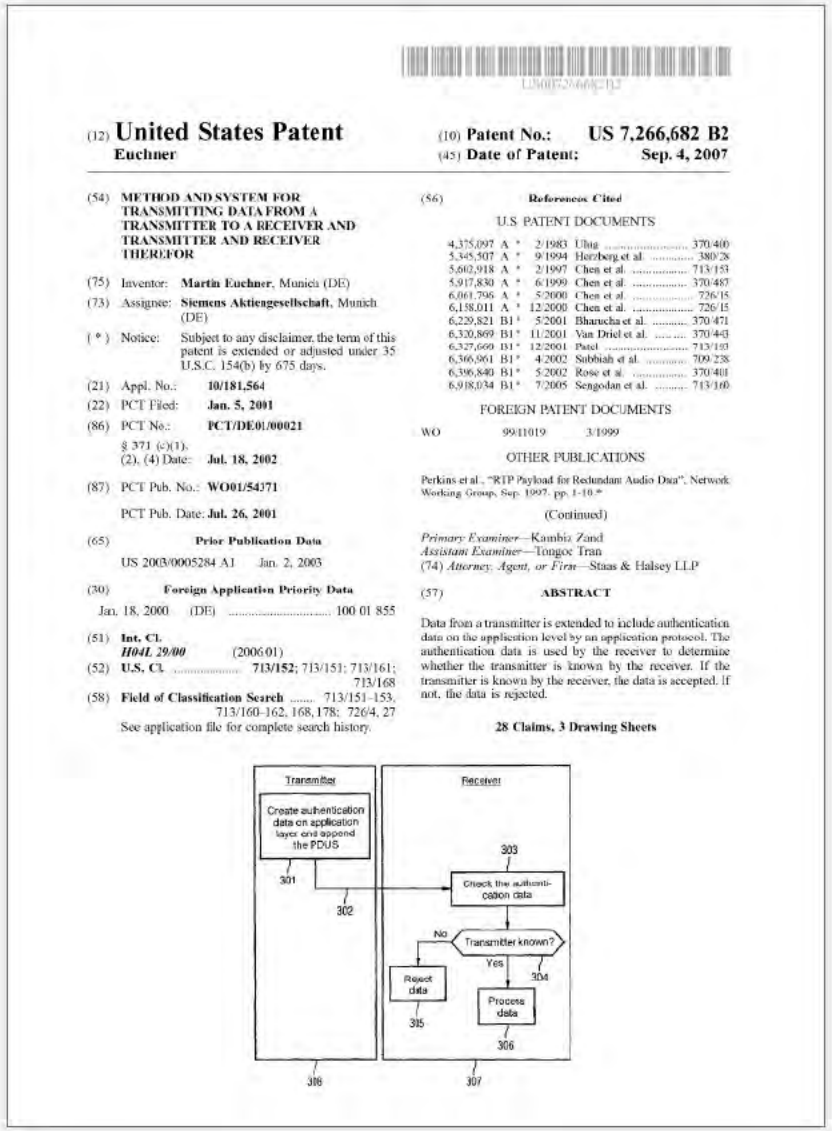
(57) **ABSTRACT**

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

1. Background
2. **Prior Art**
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. Grounds
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Overview



(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(b) 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 Uhua 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey LLP

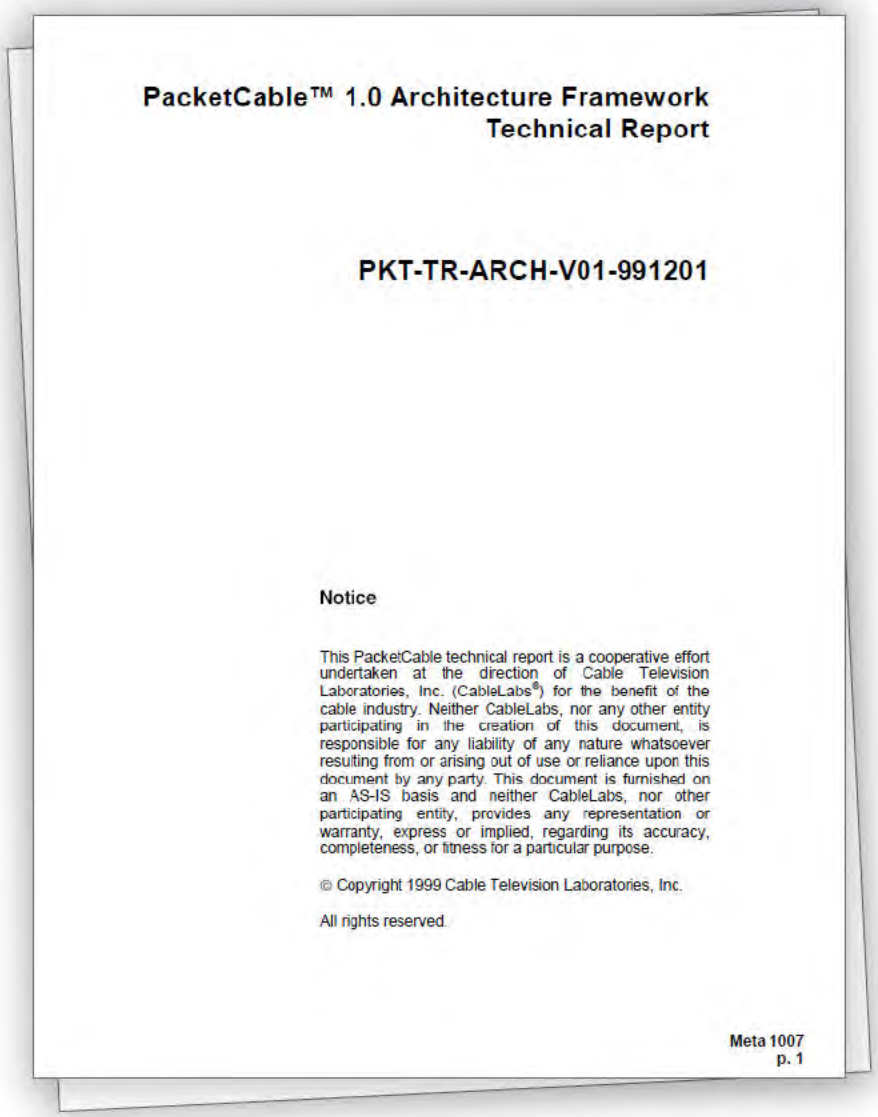
(57) **ABSTRACT**

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

1. Background
2. **Prior Art**
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. **PacketCable (Ex. 1007)**
3. Grounds
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Prior Art - PacketCable (Ex. 1007)



PacketCable™ 1.0 Architecture Framework Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

Notice

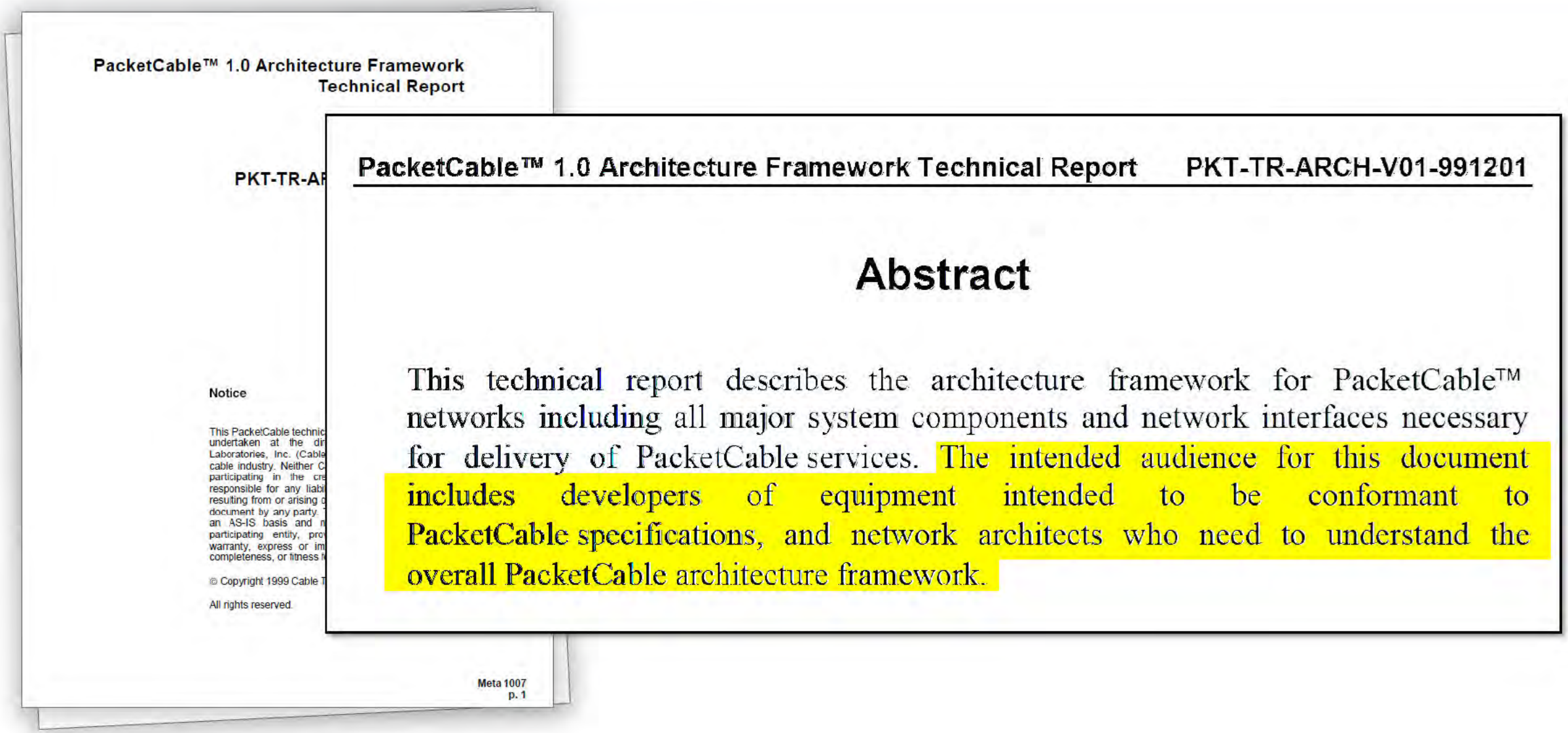
This PacketCable technical report is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of 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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

EX1007 (PacketCable) at 1

Prior Art - PacketCable (Ex. 1007)



PacketCable™ 1.0 Architecture Framework Technical Report

PKT-TR-AR

Notice

This PacketCable technic
undertaken at the dir
Laboratories, Inc. (Cable
cable industry. Neither C
participating in the cre
responsible for any liabi
resulting from or arising
document by any party.
an AS-IS basis and n
participating entity, prov
warranty, express or im
completeness, or fitness

© Copyright 1999 Cable T

All rights reserved.

Meta 1007
p. 1

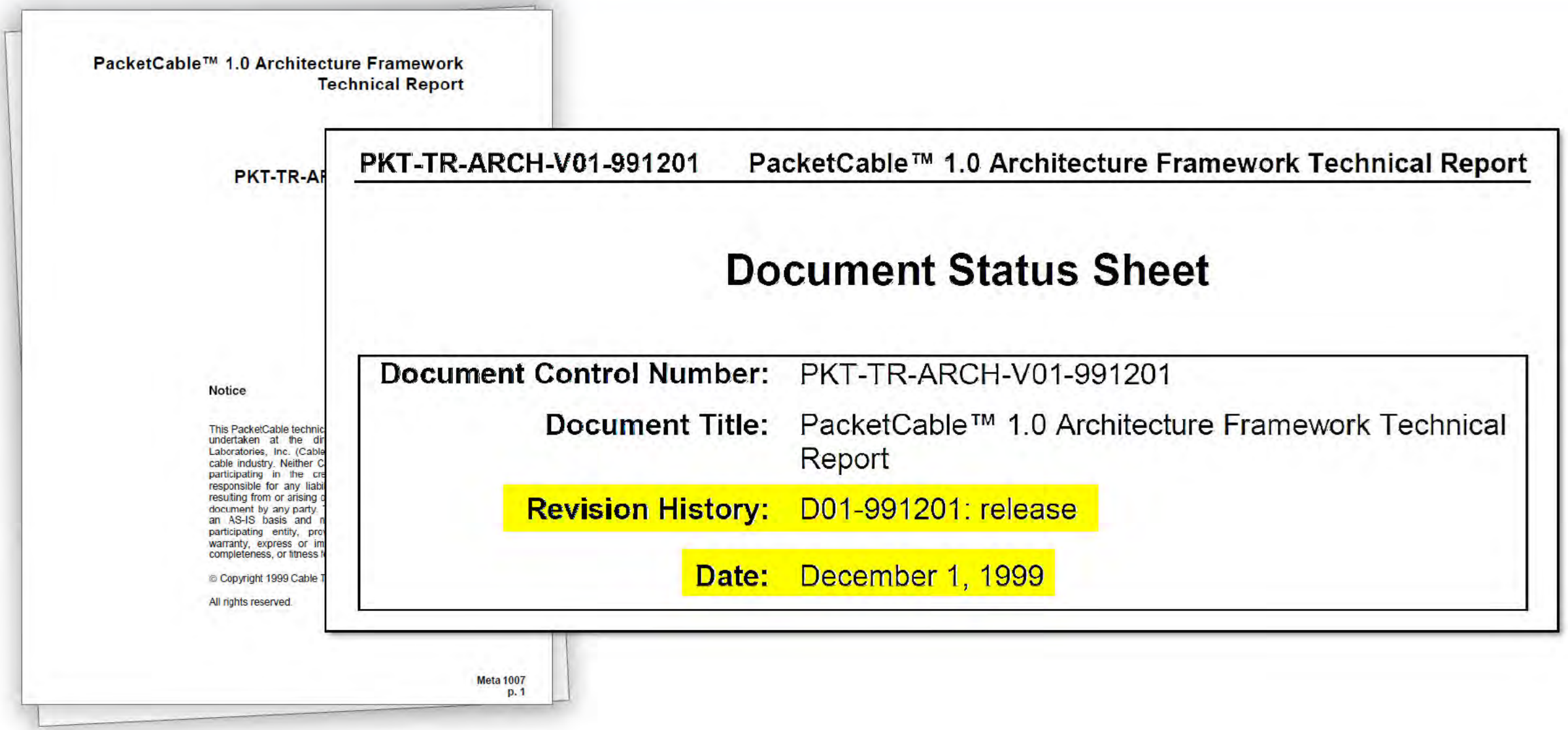
PacketCable™ 1.0 Architecture Framework Technical Report PKT-TR-ARCH-V01-991201

Abstract

This technical report describes the architecture framework for PacketCable™ networks including all major system components and network interfaces necessary for delivery of PacketCable services. The intended audience for this document includes developers of equipment intended to be conformant to PacketCable specifications, and network architects who need to understand the overall PacketCable architecture framework.

EX1007 (PacketCable) at 2

Prior Art - PacketCable (Ex. 1007)



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-AR

Notice

This PacketCable technic
undertaken at the dir
Laboratories, Inc. (Cable
cable industry. Neither C
participating in the cre
responsible for any liabi
resulting from or arising
document by any party.
an AS-IS basis and n
participating entity, pro
warranty, express or im
completeness, or fitness

© Copyright 1999 Cable T

All rights reserved.

Meta 1007
p. 1

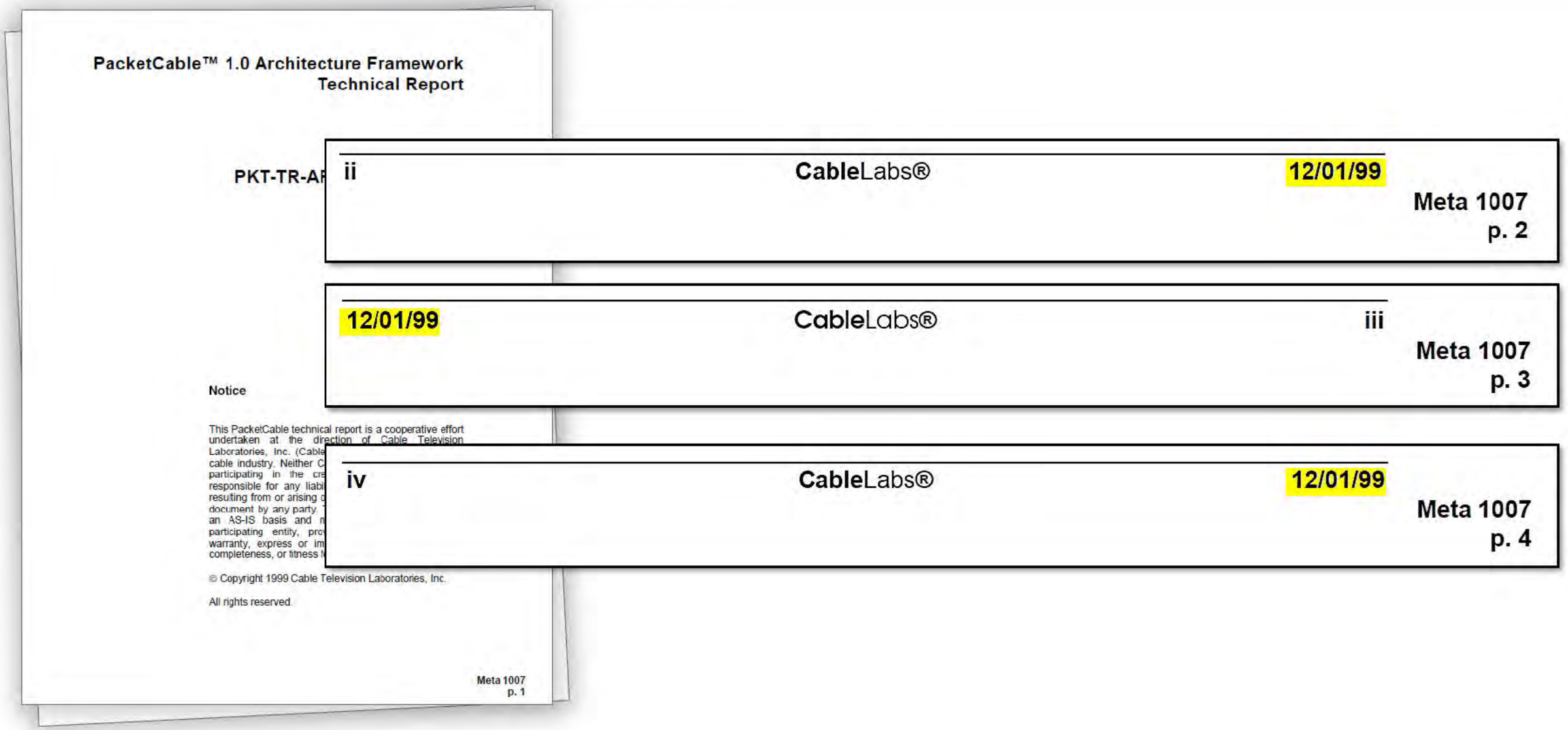
PKT-TR-ARCH-V01-991201 PacketCable™ 1.0 Architecture Framework Technical Report

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 (PacketCable) at 3

Prior Art - PacketCable (Ex. 1007)



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-AF

Notice

This PacketCable technical report is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (Cable
cable industry. Neither C
participating in the cre
responsible for any liabi
resulting from or arising
document by any party.
an AS-IS basis and n
participating entity, pro
warranty, express or im
completeness, or fitness

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

ii CableLabs® 12/01/99

Meta 1007
p. 2

12/01/99 CableLabs® iii

Meta 1007
p. 3

iv CableLabs® 12/01/99

Meta 1007
p. 4

EX1007 (PacketCable) at 2-4

Patent Owner's Arguments re PacketCable (Ex. 1007) Also Miss the Mark

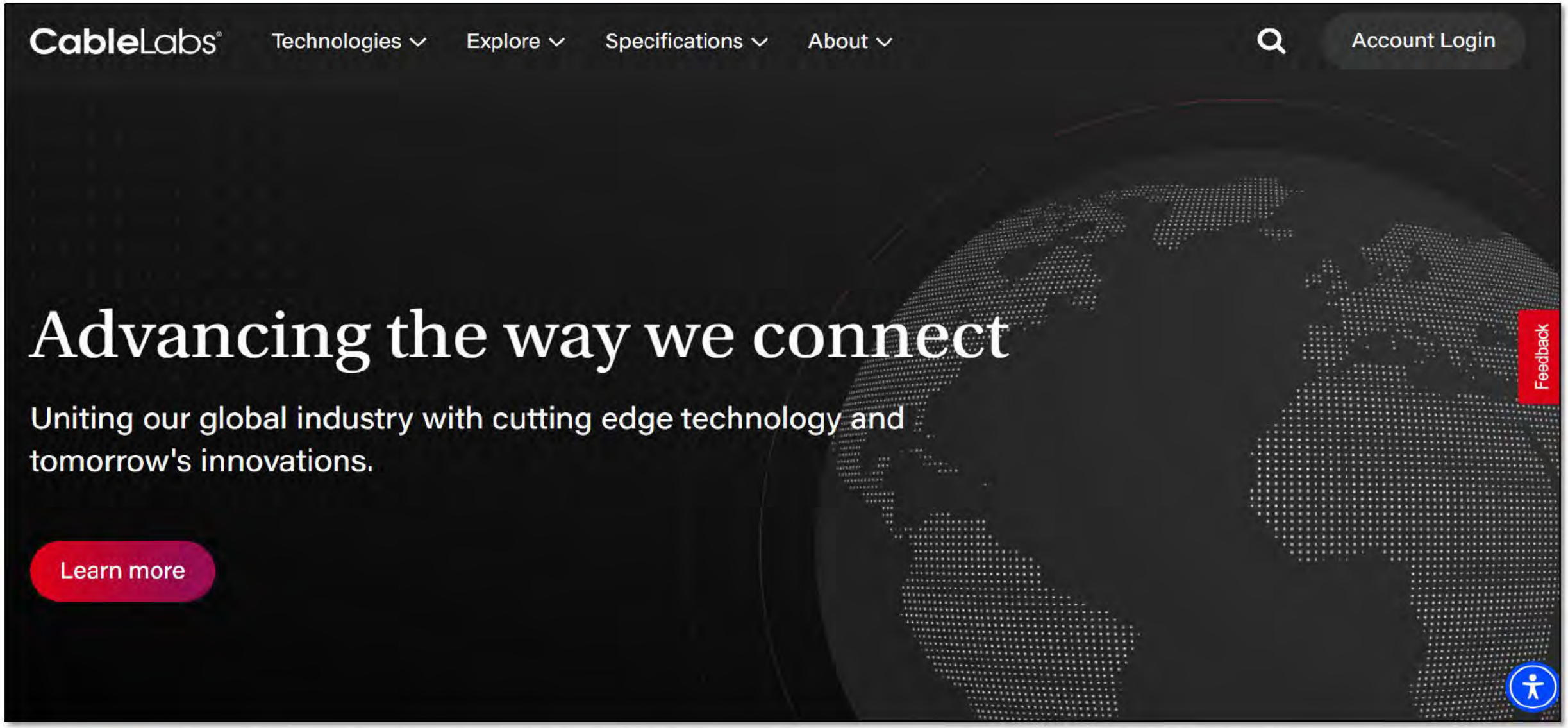
Patent Owner argues:

1. Dr. Hall-Ellis' only evidence of PacketCable's accessibility is the *present-day* CableLabs website where she found it, which says nothing about PacketCable's availability in 1999 or 2000.

2. Petitioners provide no argument or explanation as to whether or how the interested POSITA, exercising reasonable diligence, would have been able to locate PacketCable *before* January 18, 2000.

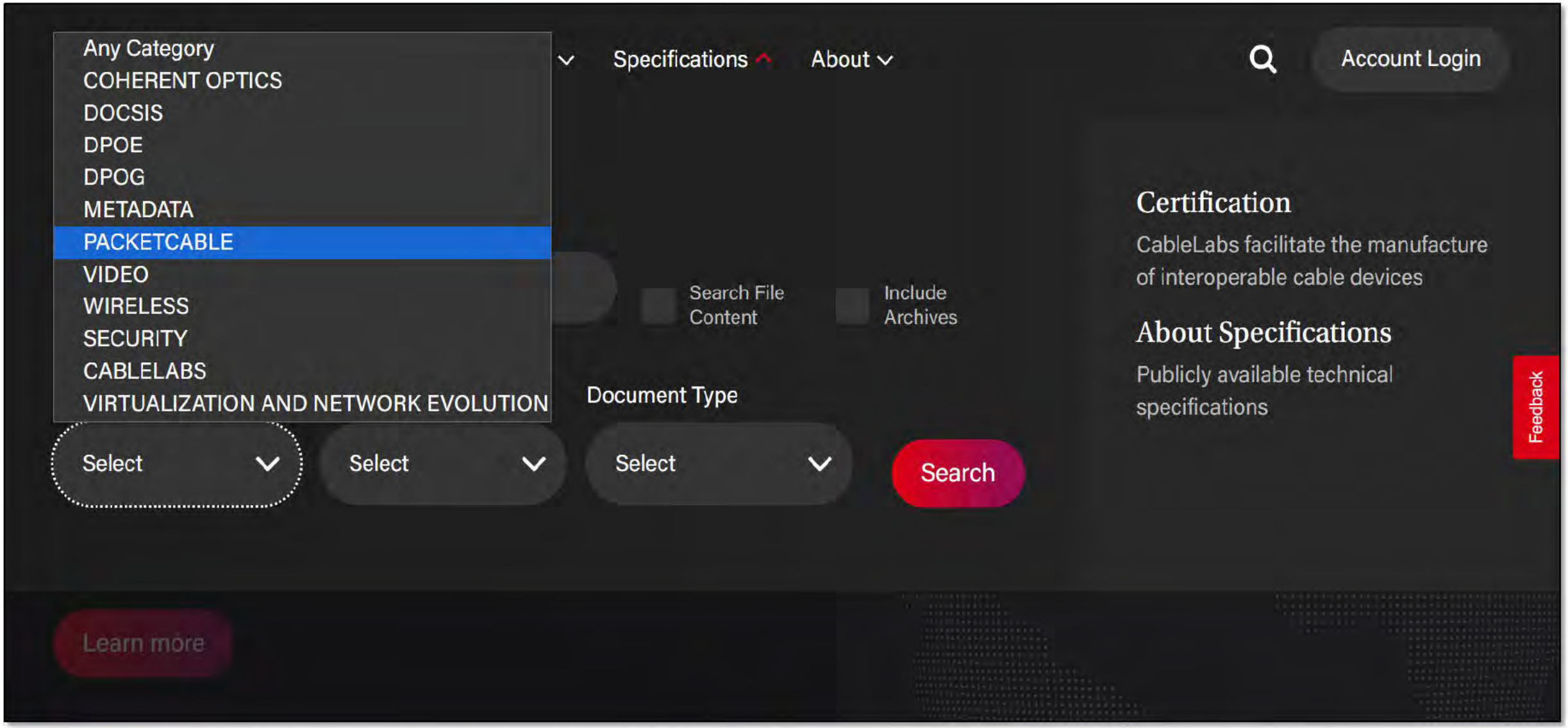
PO Sur-Reply (Paper 44) at 10-13

Prior Art - PacketCable (Ex. 1007)



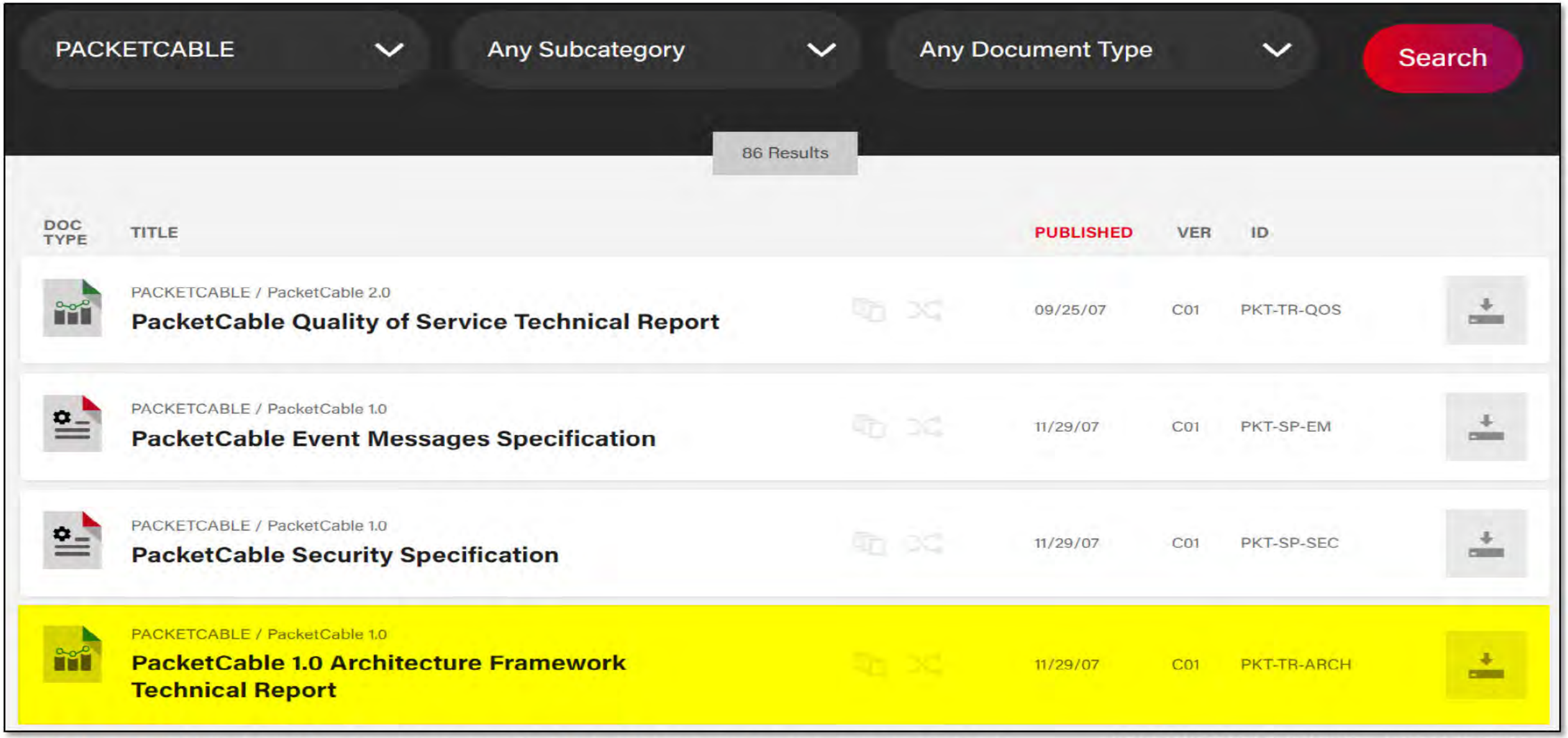
www.cablelabs.com; EX1019 (Hall-Ellis Supp. Declaration) at ¶19; EX2009 (Hall-Ellis Deposition) at 25:2-10

Prior Art - PacketCable (Ex. 1007)



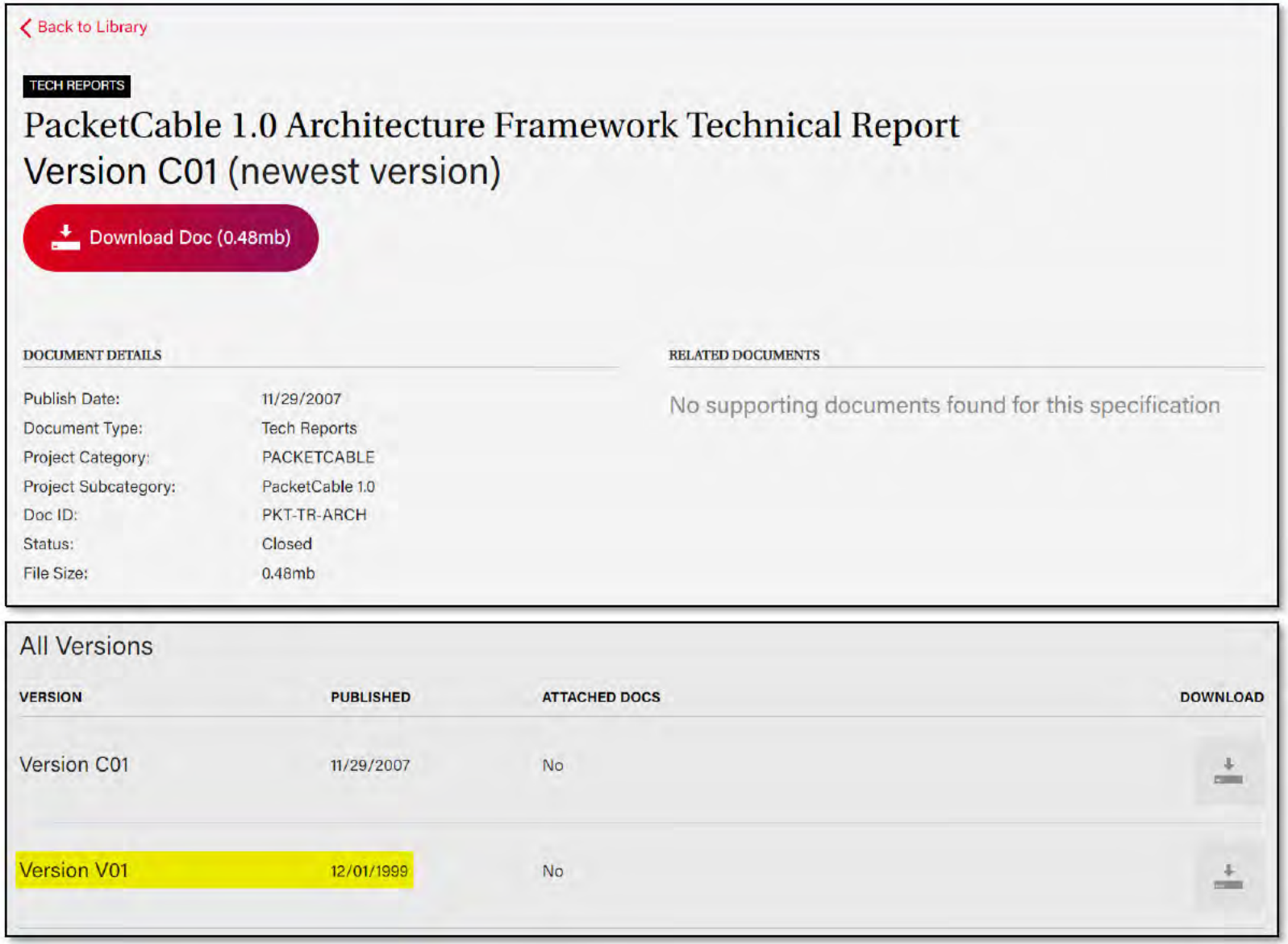
www.cablelabs.com; EX1019 (Hall-Ellis Supp. Declaration) at ¶19; EX2009 (Hall-Ellis Deposition) at 25:2-10

Prior Art - PacketCable (Ex. 1007)



www.cablelabs.com; EX1019 (Hall-Ellis Supp. Declaration) at ¶19; EX2009 (Hall-Ellis Deposition) at 25:2-10

Prior Art - PacketCable (Ex. 1007)



Back to Library

TECH REPORTS

PacketCable 1.0 Architecture Framework Technical Report
Version C01 (newest version)

Download Doc (0.48mb)

DOCUMENT DETAILS

Publish Date:	11/29/2007
Document Type:	Tech Reports
Project Category:	PACKETCABLE
Project Subcategory:	PacketCable 1.0
Doc ID:	PKT-TR-ARCH
Status:	Closed
File Size:	0.48mb

RELATED DOCUMENTS

No supporting documents found for this specification

All Versions

VERSION	PUBLISHED	ATTACHED DOCS	DOWNLOAD
Version C01	11/29/2007	No	
Version V01	12/01/1999	No	

www.cablelabs.com; EX1019 (Hall-Ellis Supp. Declaration) at ¶19; EX2009 (Hall-Ellis Deposition) at 25:2-10

Way-Back Machine Does Not Collect Everything on the Internet

Petitioners' Librarian Expert Witness



Dr. Sylvia Hall-Ellis

Dr. Hall-Ellis testified that inability to find PacketCable using the Wayback Machine "doesn't matter":

Q. Okay. So then, and then -- okay. So then why do you believe this document was on a website as of December 1st, 1999, if it is not on there on the Wayback Machine?

A. Well, remember, the Wayback Machine's purpose is not to archive things for people to use at all.

It is a way to preserve information, accurate and not accurate, for people to see because the Wayback Machine thinks it is a digital repository and I guess that is fairly accurate.

It is not the purpose of the Wayback Machine to collect everything. There are sites that don't want to be collected. Current sites are not collected.

Everything is not there. All of the links on it don't work. The deeper you go, the more the probability that something will not be operational anymore.

The Wayback Machine serves a purpose; it is not something that I rely on if I can find something different. I do use it. It is a useful tool.

But, if something isn't there, I am not always very surprised. It is okay that it is not there. It doesn't matter.

EX2003 (Hall-Ellis Deposition) at 26:9-27:13

Patent Owner's Arguments re PacketCable (Ex. 1007) Also Miss the Mark

Patent Owner argues:

~~1. Dr. Hall Ellis' only evidence of PacketCable's accessibility is the *present-day* CableLabs website where she found it, which says nothing about PacketCable's availability in 1999 or 2000.~~

2. Petitioners provide no argument or explanation as to whether or how the interested POSITA, exercising reasonable diligence, would have been able to locate PacketCable *before* January 18, 2000.

PO Sur-Reply (Paper 44) at 10-13

Patent Owner's Reliance on *Blue Calypso* is Misplaced



In Voter Verified, we found that a particular article that was available only through an on-line publication was publicly accessible. *Id.* We reached that conclusion based on "unrebutted testimony" in the record indicating that the particular on-line publication was well known to the community interested in the subject matter of the reference. *Id.* In addition, we noted that numerous related articles were also located within the same on-line publication. *Id.* These factors overcame the absence of evidence demonstrating that the website at which the article was located was indexed and thereby findable by an internet search engine. *Id.* at 1381.

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

PacketCable was Released for the Benefit of the Cable Industry

Petitioners' Librarian Expert Witness



Dr. Sylvia Hall-Ellis

Dr. Hall-Ellis testified that PacketCable:

- Was publicly available as of December 1, 1999
- "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***"

EX1019 (Hall-Ellis Supp. Declaration) at ¶¶ 19, 21

CableLabs was a Professional Organization with a Prominent Forum

Petitioners' Librarian Expert Witness



Dr. Sylvia Hall-Ellis

Dr. Hall-Ellis testified that CableLabs "released" their documents to its member companies:

Q. So, what did you learn based on reviewing the online materials about how cable television laboratories releases technical documents?

A. Well, remember they were founded in 1988. They are, according to the Internal Revenue Service, a 501(c)(6) . Which is a professional organization.

They have members which are companies and providers of cable and streaming television. And they released their documents to their members.

So, to me, that would be their public and that would make sense.

EX2003 (Hall-Ellis Deposition) at 21:10-22:1

CableLabs was a Reputable Industry Association

Petitioners' Technical Expert Witness



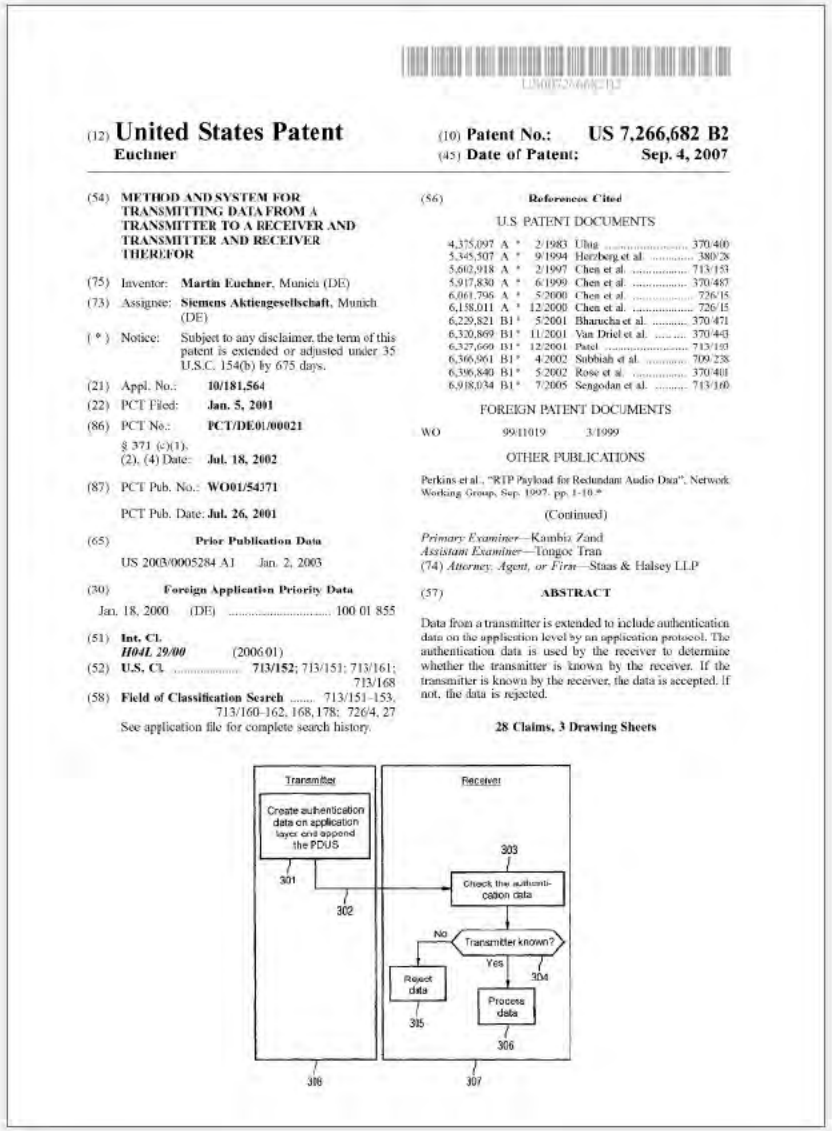
Dr. Henry Houh

Dr. Houh testified that:

- "was satisfied that in my review it was publicly available"
- "Based on my experience, these documents or types of documents from these types of groups are released both electronically and in paper form"
- Familiar with CableLabs and worked for a company in the 1990s called NBX acquired by 3Com. There, Dr. Houh made DOCSIS compliant equipment, another specification from CableLabs.
- CableLabs is a "***reputable industry association***"

EX2010 (Houh 7/19/2024 Deposition) at 172:17-20, 174:14-18, 176:14-22, 178:7-11

Overview



(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(b) 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 Uhra 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

1. Background
2. Prior Art
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. **Grounds**
   a. **Ground I**
   b. Ground II
   c. Ground III
   d. Ground IV

Claim Construction

Patent Owner's Proposed Construction

Term	Patent Owner' Construction
"application layer"	"the layers above the transport layer (layers above 4)"
"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"

PO's Response (Paper 26) at 14

Invalidity Grounds

Ground I (Claims 1-21, 23, 25-28)

- Obvious under § 103 in view of Handley in combination with Basturk

Ground II (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Handley

Ground III (Claims 1-28)

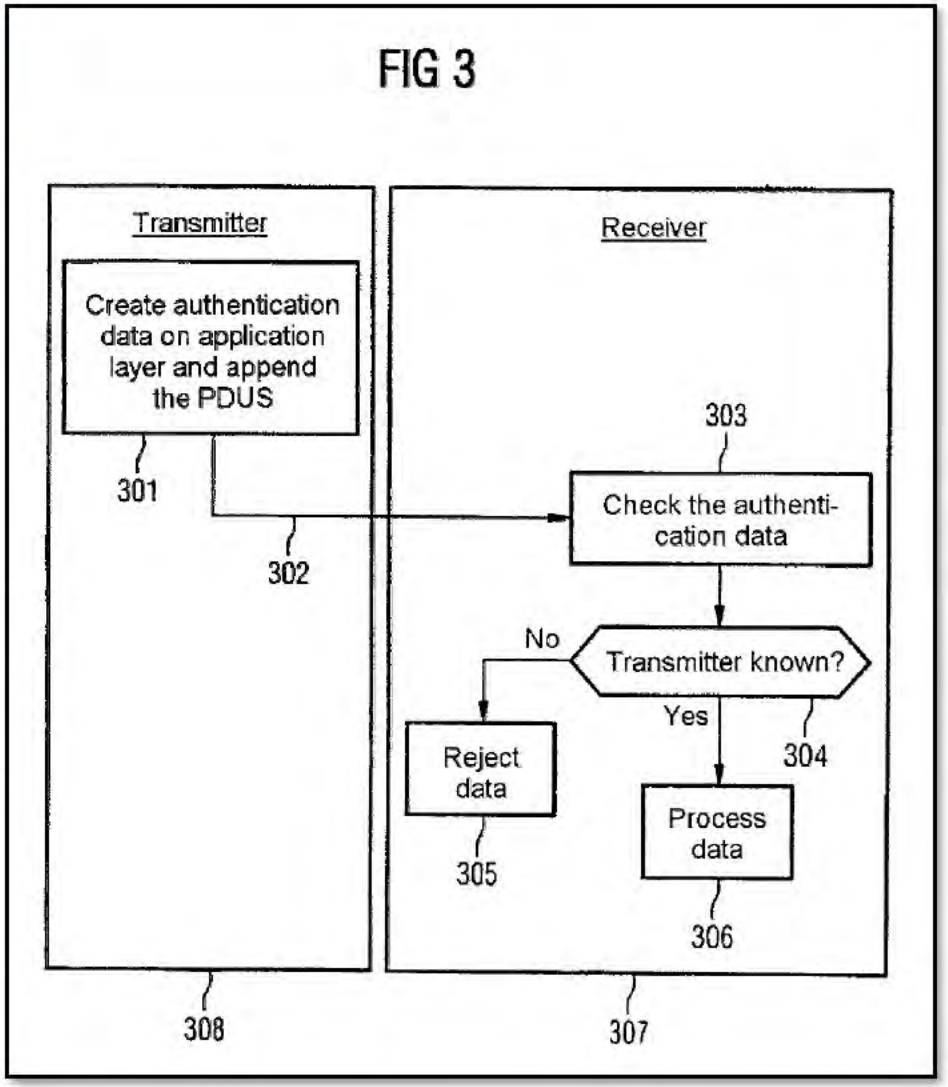
- Obvious under § 103 in view of PacketCable in combination with Basturk

Ground IV (Claims 22, 24)

- Obvious under § 103 in view of Handley in combination with Basturk and PacketCable

Ground I: Patent Owner Only Disputes Elements [1.1], [1.2], and [1.3]

Claim 1, '682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1, Fig. 3

RTP is an Application Layer Protocol

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

RTP is an Application Layer Protocol

Handley discloses RTP

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

M. Handley, J. Crowcroft and C. Bormann

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 must be sufficient capacity in the relevant traffic class to accommodate the traffic. How this capacity is ensured is independent of RTP.

EX1005 (Handley) at 1, 8

RTP follows the principles of application level framing

Network Working Group
Request for Comments: 1889
Category: Standards Track

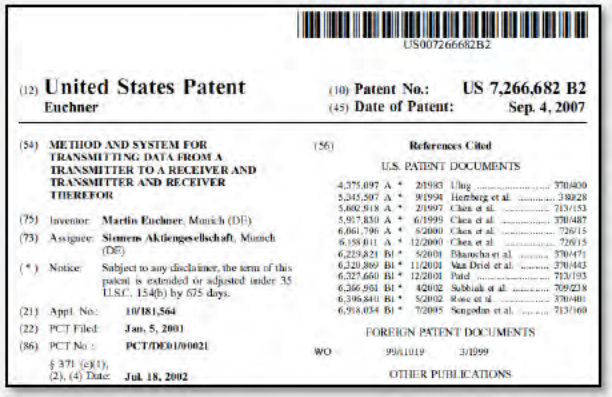
Audio-Video Transport Working Group
H. Schulzrinne
GMD Fokus
S. Casner
Precept Software, Inc.
R. Frederick
Xerox Palo Alto Research Center
V. Jacobson
Lawrence Berkeley National Laboratory
January 1996

RTP: A Transport Protocol for Real-Time Applications

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 that is deliberately not complete. This document specifies those functions expected to be common across all the applications for which RTP would be appropriate. Unlike conventional protocols in which additional functions might be accommodated by making the protocol more general or by adding an option mechanism that would require parsing, RTP is intended to be tailored through modifications and/or additions to the headers as needed. Examples are given in Sections 5.3 and 6.3.3.

EX1008 (RFC 1889 – RTP Specification) at 4

'682 Patent uses RTP at its expected location, at the application layer


US007266682B2

(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(b) 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

(56) References Cited

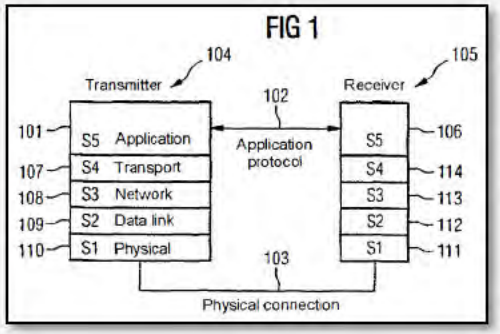
U.S. PATENT DOCUMENTS

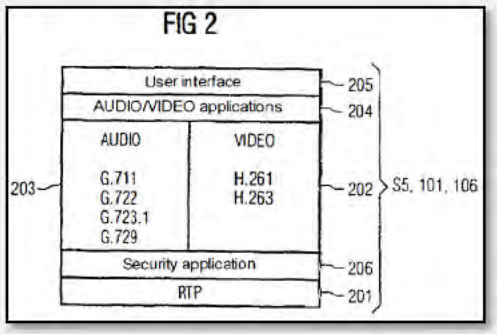
4,375,097 A * 2/1983 Ulug 370/400
5,345,597 A * 9/1994 Hertberg et al. 380/28
5,602,918 A * 2/1997 Chen et al. 713/153
5,917,830 A * 6/1999 Chen et al. 370/487
6,061,796 A * 5/2000 Chen et al. 726/15
6,158,011 A * 12/2000 Chen et al. 726/15
6,229,821 B1 * 5/2001 Bhanoo et al. 370/471
6,230,869 B1 * 11/2001 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 99/01019 3/1999

OTHER PUBLICATIONS





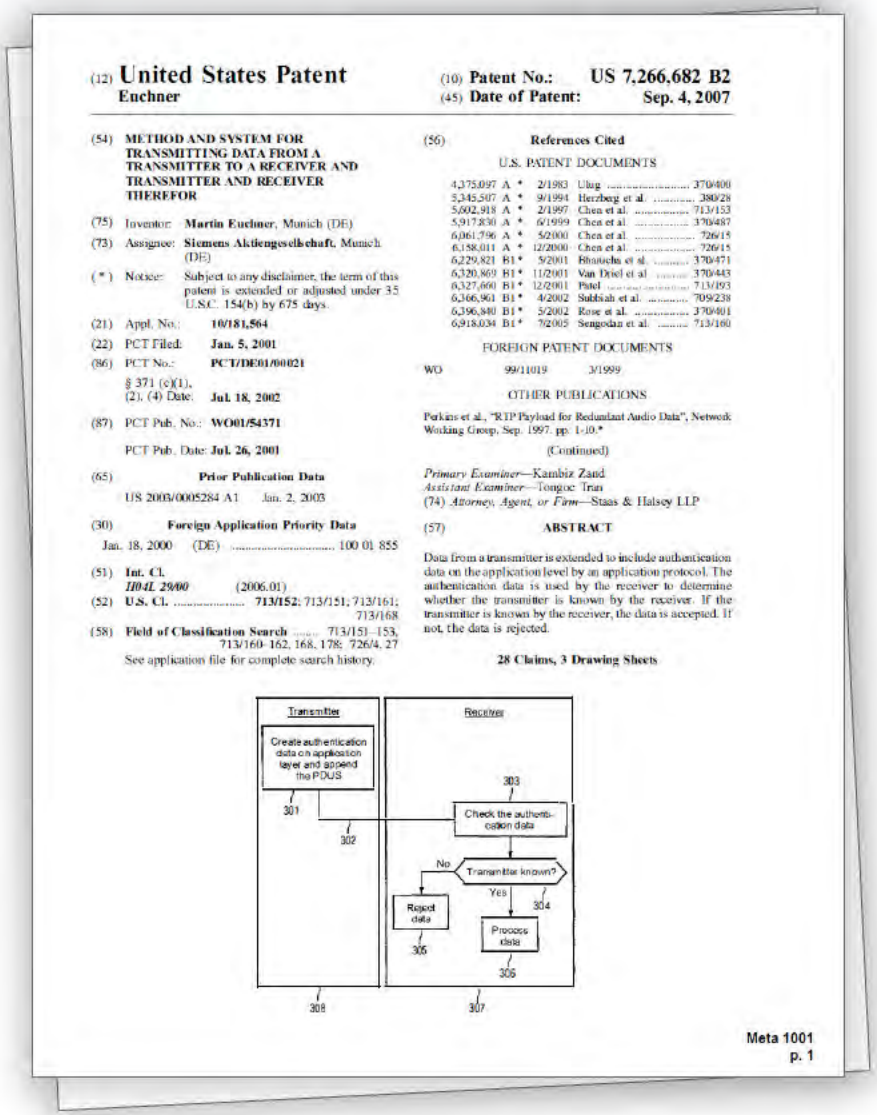
EX1001 (US 7,266,682) at Figs. 1, 2

Ground I: Handley + Basturk

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Authentication According to the '682 is Nothing New



(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(b) 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	Bhatiehe 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

Meta 1001
p. 1

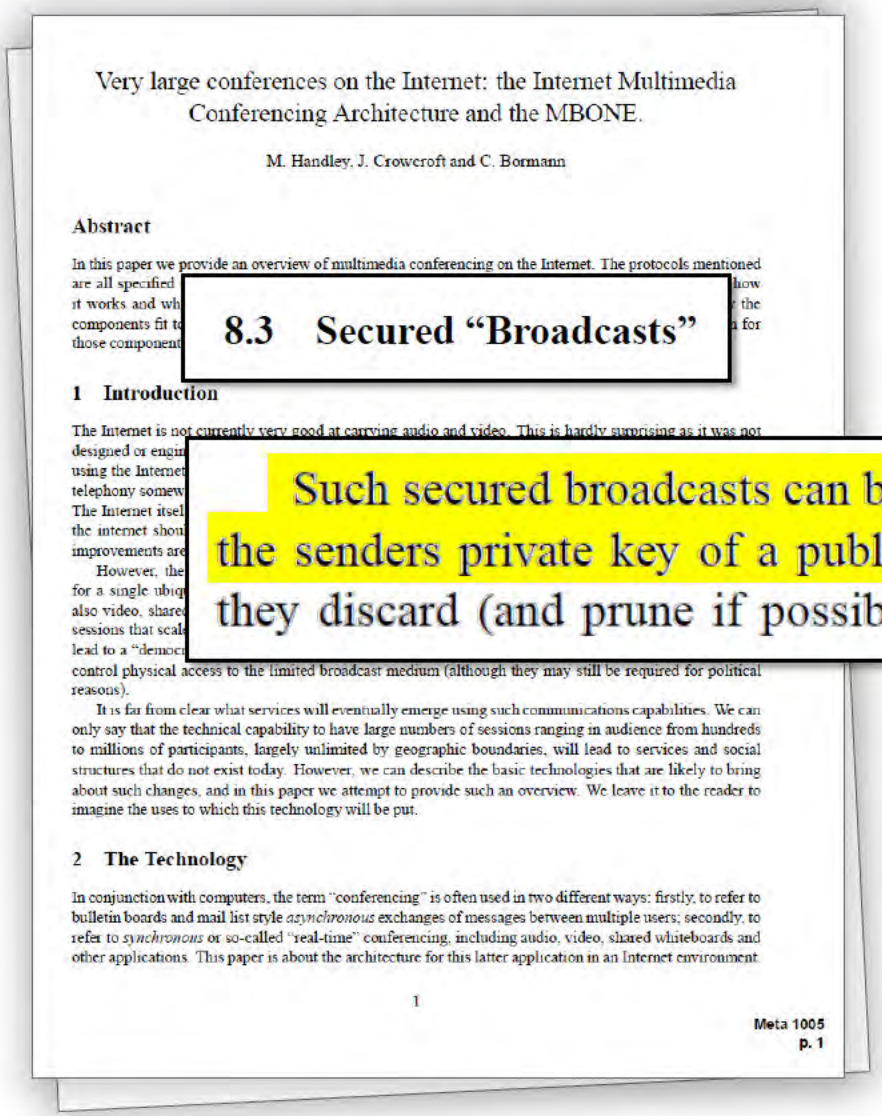
A message authentication code (MAC) is known generally and denotes a cryptographic checksum which is intended to be used to identify an alteration in a message or in data (see Christoph Ruland, Informationssicherheit in Datennetzen (which translates as Information Security in Data Networks), DATACOM-Verlag; Bergheim, 1993, pp. 61-63 and 68-79).

A one-way hash function is known from Ruland, pp. 68-79, for example. Such a one-way hash function cannot be used to calculate the correct input value for a given function value. Another feature is the absence of collision, i.e. it must not be possible to use the one-way hash function to obtain the same output value for two different input values.

In addition, an asymmetric cryptographic method (also: public key method) is known, e.g. from Ruland, pp. 73-79. Each party involved in an asymmetric cryptographic method receives two keys, a public key and a secret (or private) key.

EX1001 (US 7,266,682) at 2:12-18, 2:19-24, 2:29-32

Handley's Secure Broadcasts "sign" Each Packet



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 ... how it works and wh... the components fit t... for those component...

8.3 Secured "Broadcasts"

1 Introduction

The Internet is not currently very good at carrying audio and video. This is hardly surprising as it was not designed or engin... using the Internet ... telephony somew... The Internet itsel... the internet shou... improvements are...

However, the... for a single ubiq... also video, share... sessions that scal... lead to a "democ... 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.

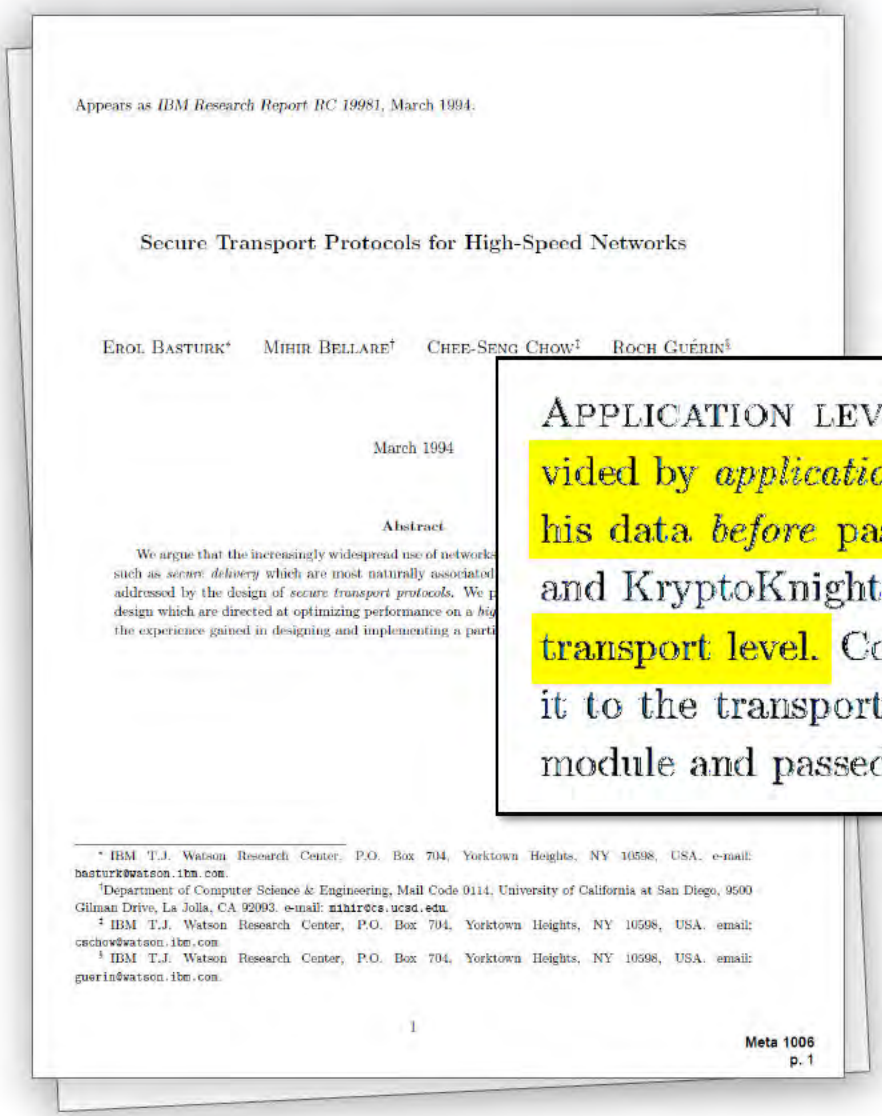
1

Meta 1005
p. 1

Such secured broadcasts can be performed by encrypting a hash (digitally signing) of each packet with the senders private key of a public-private key pair. The public key is then given to the receivers, and they discard (and prune if possible) any packets that are unsigned. The problem with this is that even

EX1005 (Handley) at 13

Basturk Authenticates at the Application Layer



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

March 1994

Abstract

We argue that the increasingly widespread use of networks
such as *secure delivery* which are most naturally associated
addressed by the design of *secure transport protocols*. We p
design which are directed at optimizing performance on a *hig*
the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.
† Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

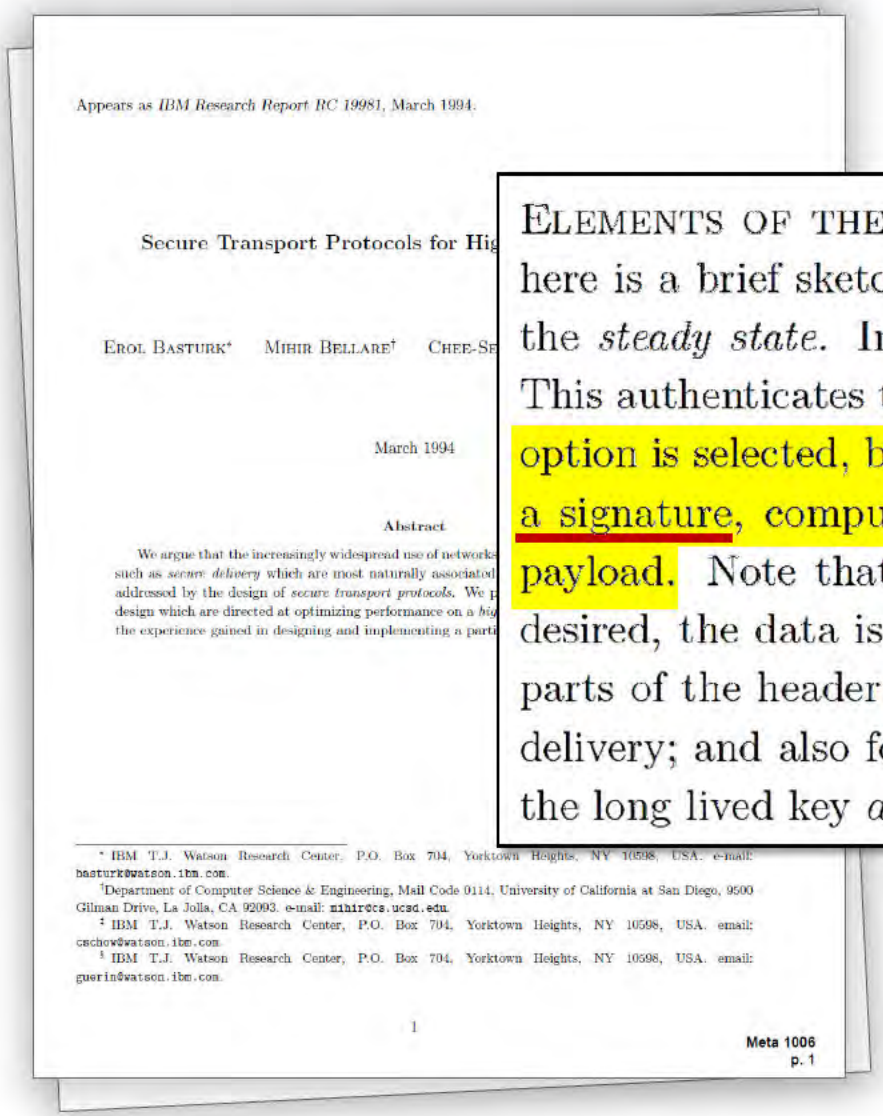
1

Meta 1006
p. 1

APPLICATION LEVEL SECURITY. Application level security features are easily (and usually) provided by *application level security*. Here the sender applies appropriate cryptographic functions to his data *before* passing it to the transport for conveyance. This is the approach of Kerberos [5] and KryptoKnight [3]. Integrity is usually guaranteed by *signing* the data before passing it to the transport level. Confidentiality is usually guaranteed by having *A encrypt* the data before passing it to the transport level, and having *B decrypt* the ciphertext which is received by his transport module and passed up to him.

EX1006 (Basturk) at 3-4

Basturk Authenticates ("signs") Each Packet at the Transport Layer



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for Hig

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks such as *secure delivery* which are most naturally associated addressed by the design of *secure transport protocols*. We p design which are directed at optimizing performance on a *big* the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

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.

EX1006 (Basturk) at 5

Ground I: Handley + Basturk

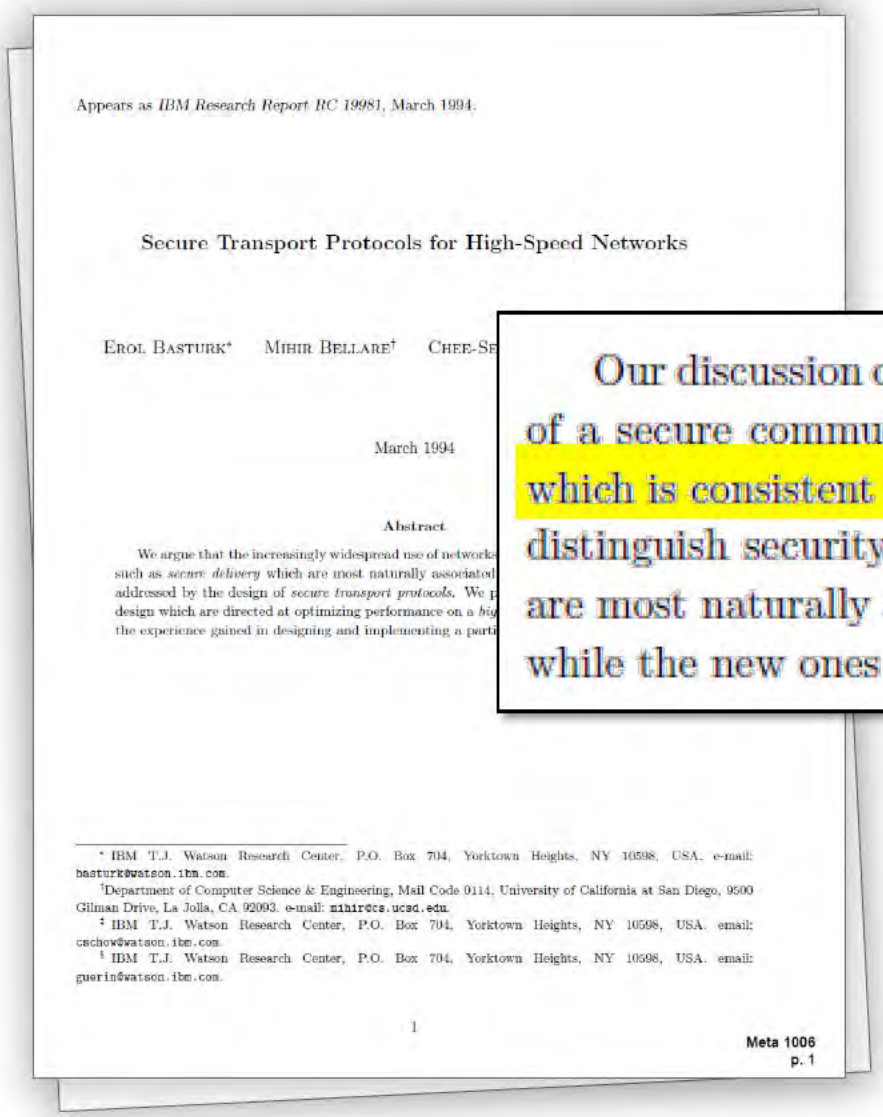
Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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.

Patent Owner makes three arguments why Element [1.1] is not obvious over Handley + Basturk

1. Basturk teaches away from modifying Handley’s application layer with Basturk’s transport protocol
2. Petitioners do not show that Handley or Basturk discloses this claim element
3. A POSITA would have not found it obvious to combine the teachings of Handley and Basturk as Petitioners suggests

EX1001 (US 7,266,682) at Claim 1, Fig. 3

Basturk Does Not Teach Away



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks such as *secure delivery* which are most naturally associated addressed by the design of *secure transport protocols*. We p design which are directed at optimizing performance on a *big* the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

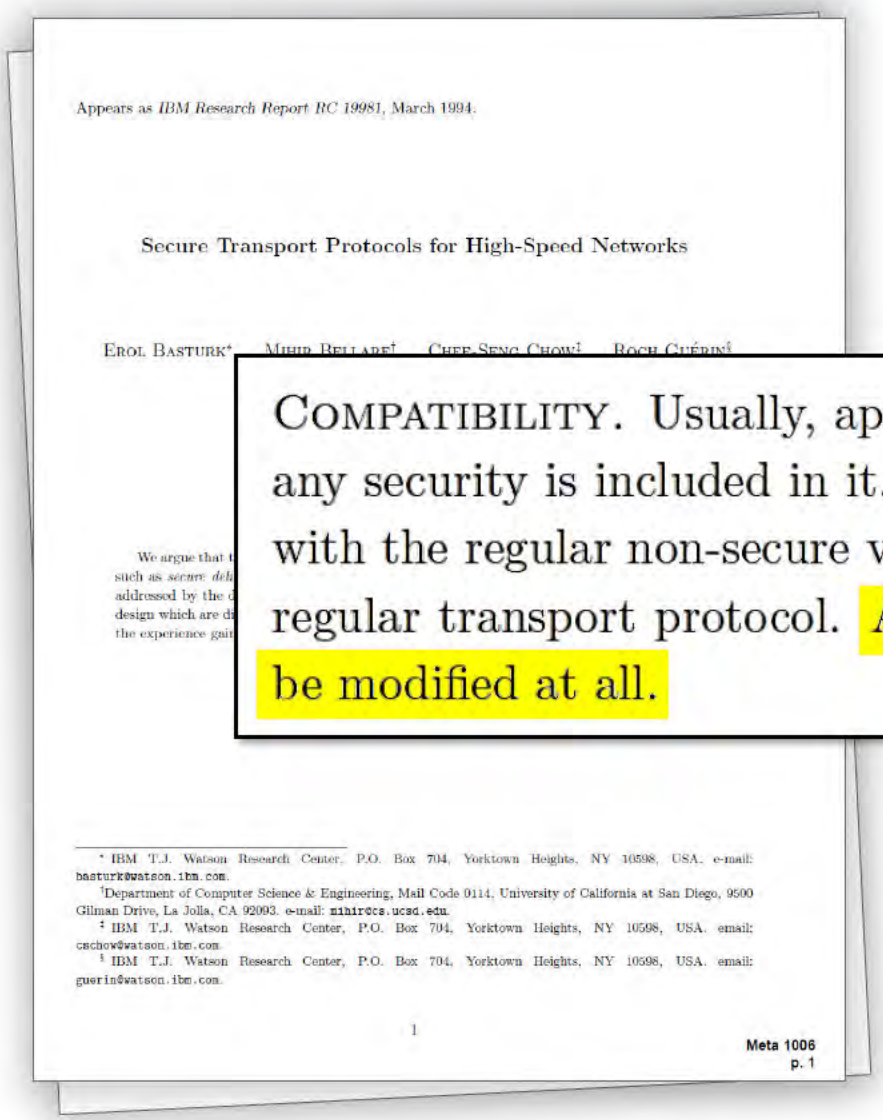
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

> 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 5

Basturk Does Not Teach Away



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

We argue that t
such as *secure del*
addressed by the
design which are d
the experience gai

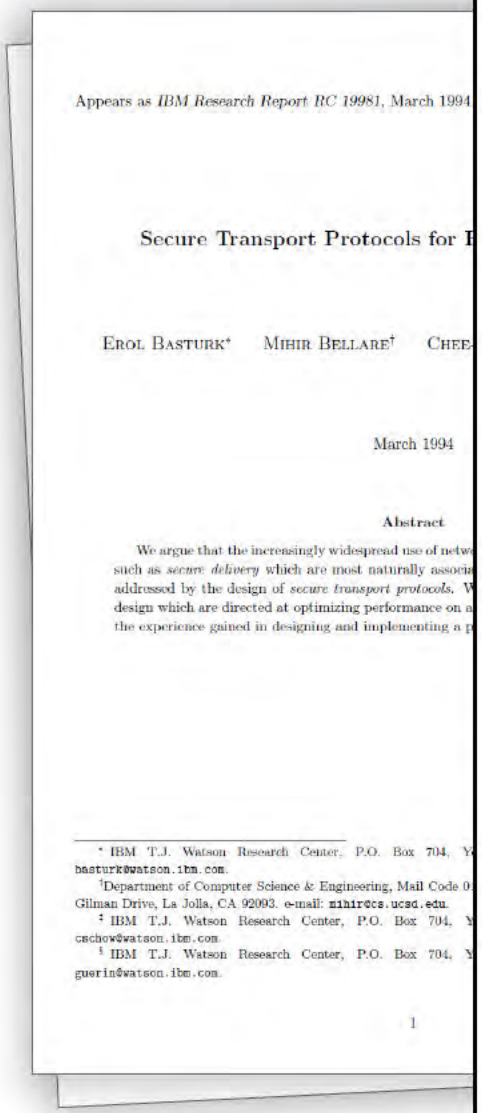
* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.
†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

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

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994

Secure Transport Protocols for I

Erol Basturk* Mihir Bellare† Chee-

March 1994

Abstract

We argue that the increasingly widespread use of netw
such as *secure delivery* which are most naturally associa
addressed by the design of *secure transport protocols*. W
design which are directed at optimizing performance on a
the experience gained in designing and implementing a p

* IBM T.J. Watson Research Center, P.O. Box 704, Y
basturk@watson.ibm.com.
†Department of Computer Science & Engineering, Mail Code 0
Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Y
cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Y
guerin@watson.ibm.com.

1

(2) *Integrity option.* If this option is selected then data integrity and secure delivery are provided. Otherwise they are not provided.

(3) *Confidentiality option.* If this option is selected then data confidentiality is provided by encryption. Otherwise, the data will be in the clear.

(4) *Basic cryptographic primitive specification.* The protocol lists a set of cryptographic primitives such as MD5 (Message Digest number 5), SHA (Secure Hash Algorithm), DES (Data Encryption Standard) and double DES, which it will use to provide both integrity and confidentiality. The application chooses which one to use.

As discussed in Section 2.1, the purpose of providing options is to allow the user to trade security for performance. We now see how this is reflected in the last three options listed above. The discussion on AKE selection is in Section 2.4.

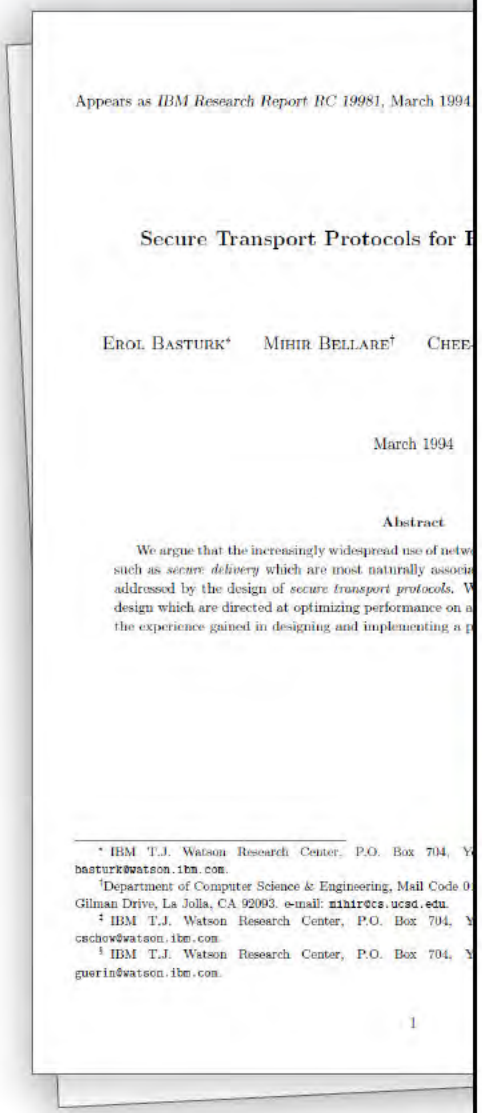
An application which wants, say, only integrity, should not be unnecessarily burdened with the performance cost inherent in providing encryption. Similarly an application wanting only confidentiality should not be burdened with the cost of signing inherent in providing integrity. So integrity and confidentiality are better made (orthogonal) options.

Cryptographic primitives exhibit a trade-off between strength and speed: more secure primitives take more time to compute. An application which needs a high level of security must be willing to pay for it in performance, and can choose a primitive which is very strong but adds to the performance cost. An application which needs just a little security can specify a weaker but faster primitive and get better performance.

EX1006 (Basturk) at 9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994

Secure Transport Protocols for I

Erol Basturk* Mihir Bellare† Chee

March 1994

Abstract

We argue that the increasingly widespread use of netw
such as *secure delivery* which are most naturally associa
addressed by the design of *secure transport protocols*. W
design which are directed at optimizing performance on a
the experience gained in designing and implementing a p

* IBM T.J. Watson Research Center, P.O. Box 704, Y
basturk@watson.ibm.com.
†Department of Computer Science & Engineering, Mail Code 0
Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Y
cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Y
guerin@watson.ibm.com.

1

(2) *Integrity option.* If this option is selected then data integrity and secure delivery are provided. Otherwise they are not provided.

(3) *Confidentiality option.* If this option is selected then data confidentiality is provided by encryption. Otherwise, the data will be in the clear.

(4) *Basic cryptographic primitive specification.* The protocol lists a set of cryptographic primitives such as MD5 (Message Digest number 5), SHA (Secure Hash Algorithm), DES (Data Encryption Standard) and double DES, which it will use to provide both integrity and confidentiality. The application chooses which one to use.

As discussed in Section 2.1, the purpose of providing options is to allow the user to trade security for performance. We now see how this is reflected in the last three options listed above. The discussion on AKE selection is in Section 2.4.

An application which wants, say, only integrity, should not be unnecessarily burdened with the performance cost inherent in providing encryption. Similarly an application wanting only confidentiality should not be burdened with the cost of signing inherent in providing integrity. So integrity and confidentiality are better made (orthogonal) options.

Cryptographic primitives exhibit a trade-off between strength and speed: more secure primitives take more time to compute. An application which needs a high level of security must be willing to pay for it in performance, and can choose a primitive which is very strong but adds to the performance cost. An application which needs just a little security can specify a weaker but faster primitive and get better performance.

EX1006 (Basturk) at 9

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness

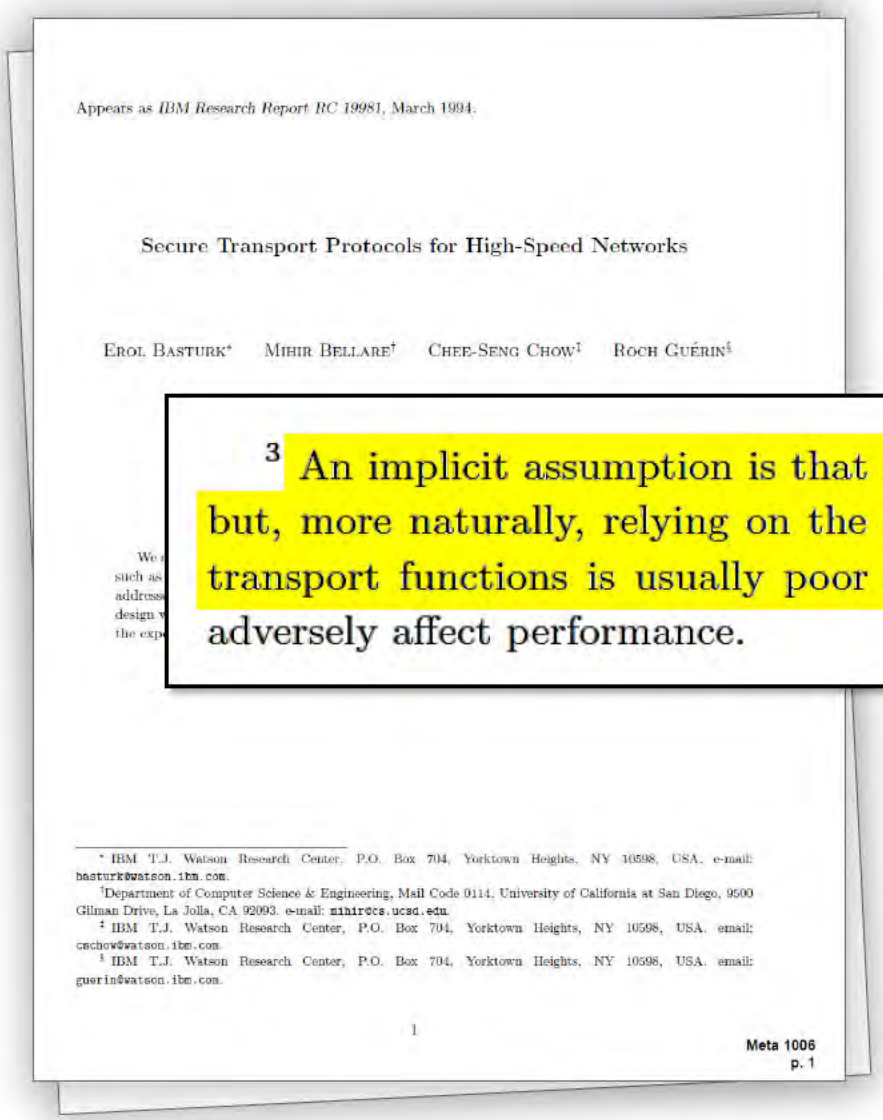


Dr. Stuart Stubblebine

> 118. A POSITA would have also understood that Basturk teaches away from modifying an application to implement its transport protocol, as Basturk indicates that it would be "poor design," "belies the layered communication structure," would "adversely affect performance," would "mak[e] implementation significantly harder," duplicate functionality" and "degrade performance." EX1006 at 4 n.3, 12. A POSITA would have understood this to teach away from and discourage implementing Basturk's transport protocol at the application layer.

EX2004 (Stubblebine Declaration) at ¶118, 101

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

[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.

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.
† Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

1

Meta 1006
p. 1

EX1006 (Basturk) at 4

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

its transport protocol." *Id.*, ¶¶117-18. However, Dr. Stubblebine takes these statements out of context. Basturk's footnote 3 states that "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, 4, n. 3. But the combination I set forth does not duplicate functions because Handley does not disclose the use of a MAC and any checksums in different protocol layers used in Handley are not for the purpose of authentication. Furthermore, I set forth the motivations a POSITA would have to make the combination above. *See* §§ IV.A-E, *supra*.

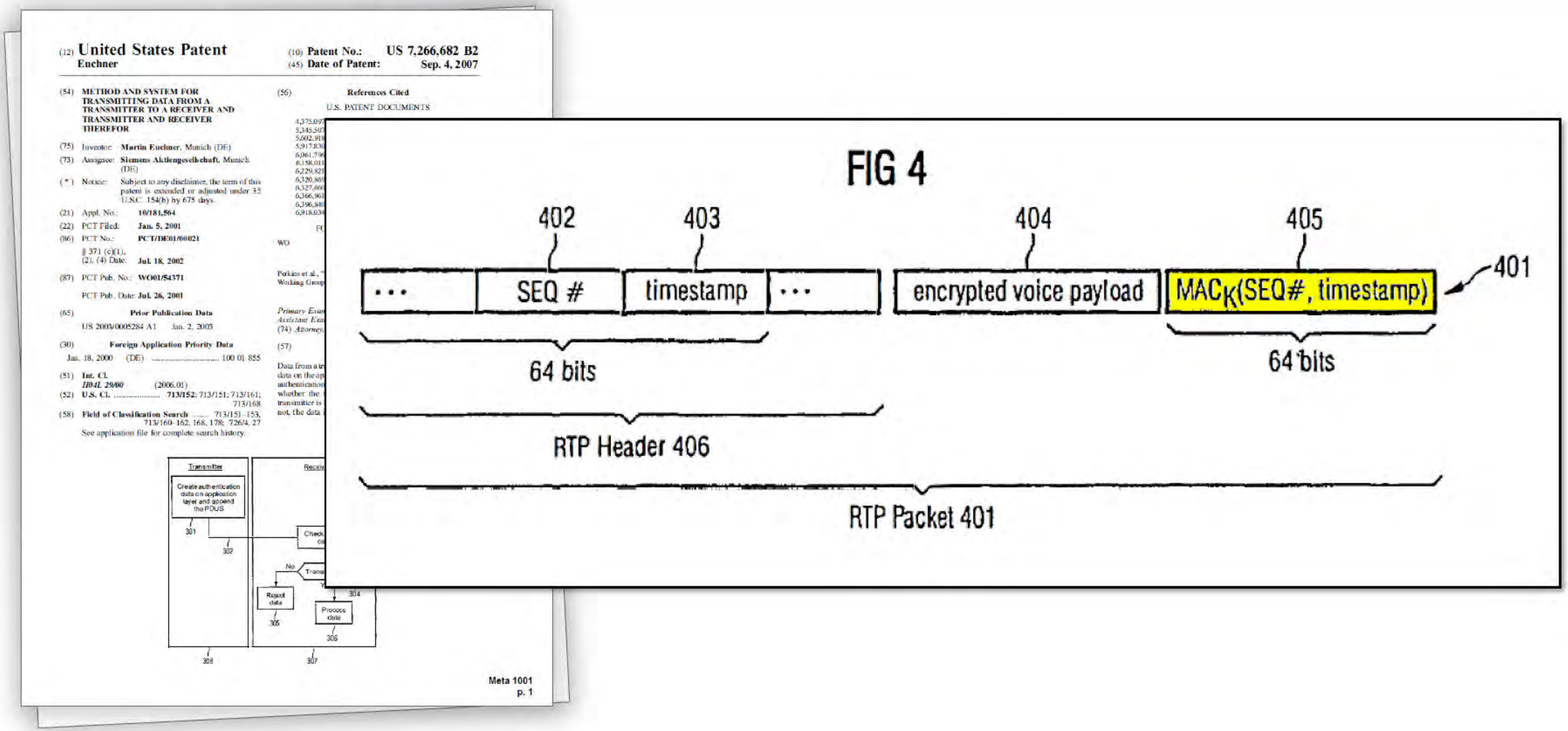
EX1006 (Basturk) at 12; EX1033 (Houh Supp. Declaration) at ¶39, 32

Ground I: Handley + Basturk

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground I: Handley + Basturk



(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(b) 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

WO

Primary Exam
Assistant Exa
(74) *Attorney,*

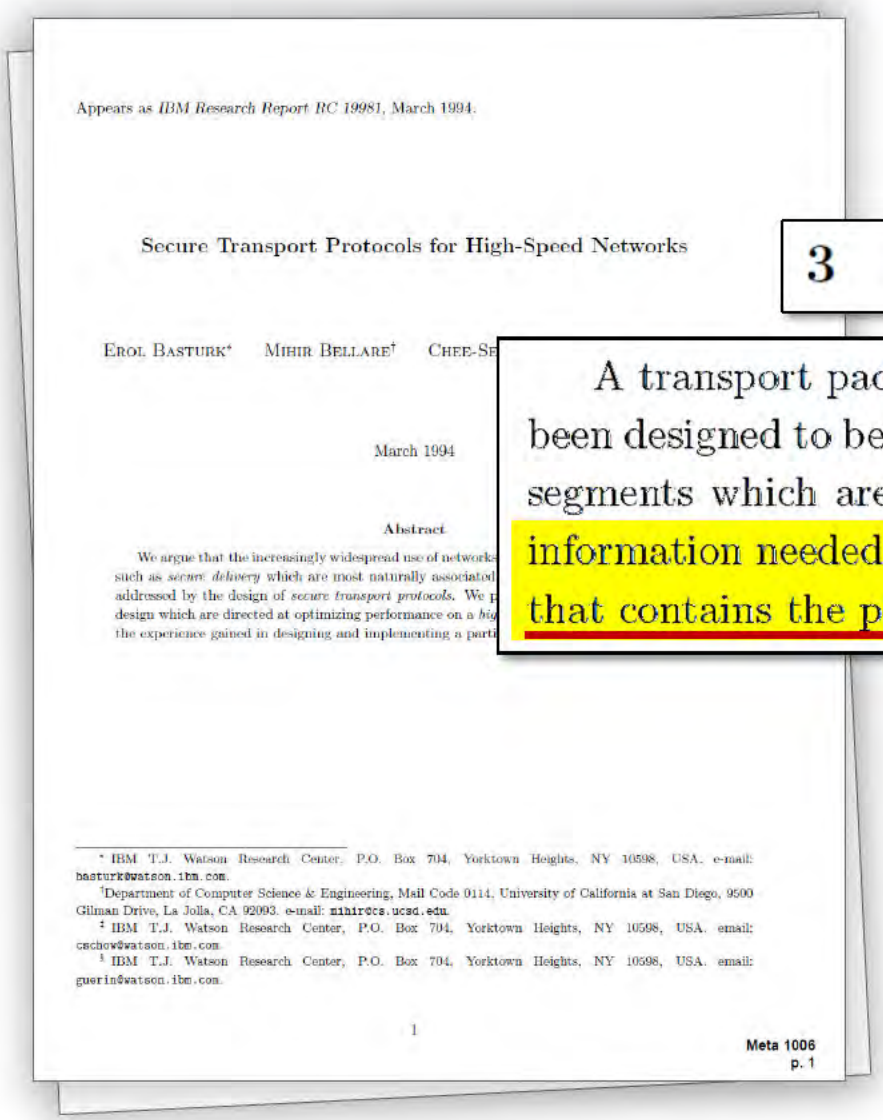
(57)

Meta 1001
p. 1

FIG 4

EX1001 (US 7,266,682) at Fig. 4

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Sh

March 1994

Abstract

We argue that the increasingly widespread use of networks
such as *secure delivery* which are most naturally associated
addressed by the design of *secure transport protocols*. We p
design which are directed at optimizing performance on a *big*
the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

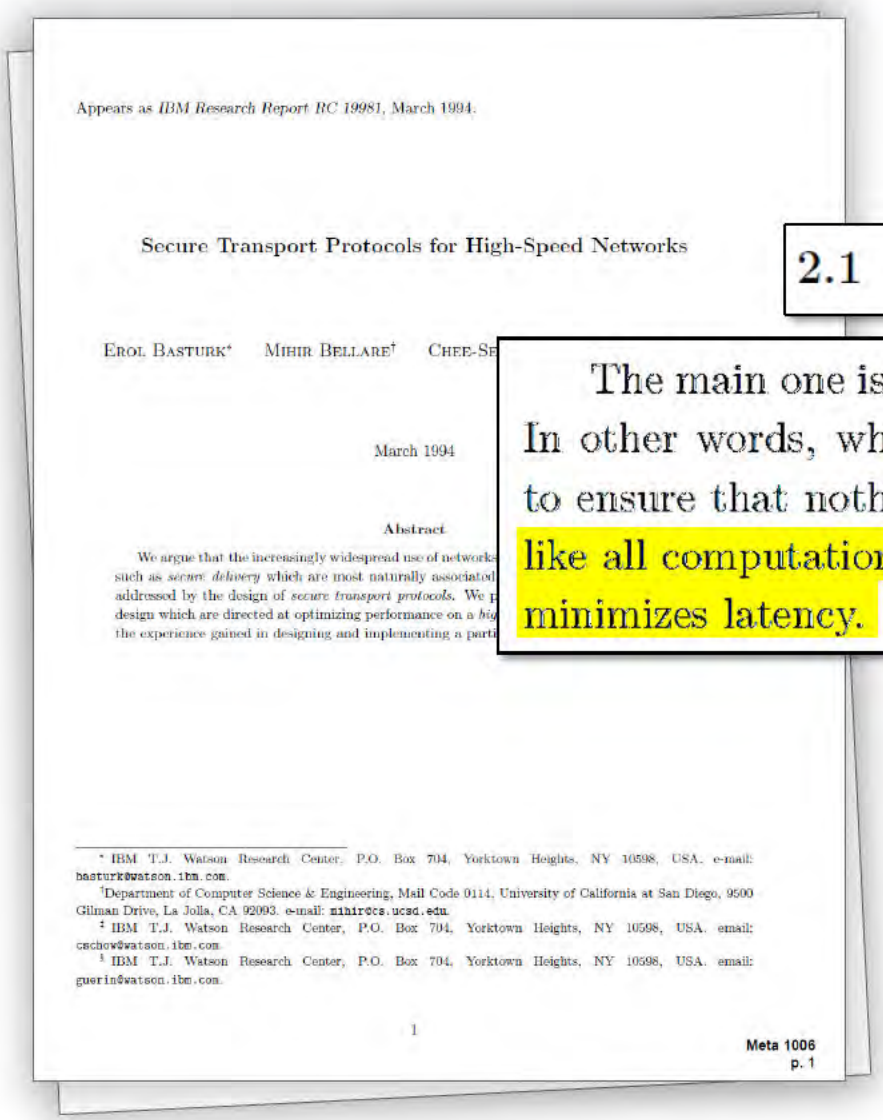
Meta 1006
p. 1

3 Implementation Overview

A transport packet consists of a header followed by data, if any. The format of the packets has been designed to be extensible. Most transport control functions are present in optional fields called segments which are part of the transport header. A security segment has been added to include information needed for authentication and confidentiality. Following data, a trailer has been added that contains the packet signature.

EX1006 (Basturk) at 16

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks such as *secure delivery* which are most naturally associated addressed by the design of *secure transport protocols*. We p design which are directed at optimizing performance on a *big* the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

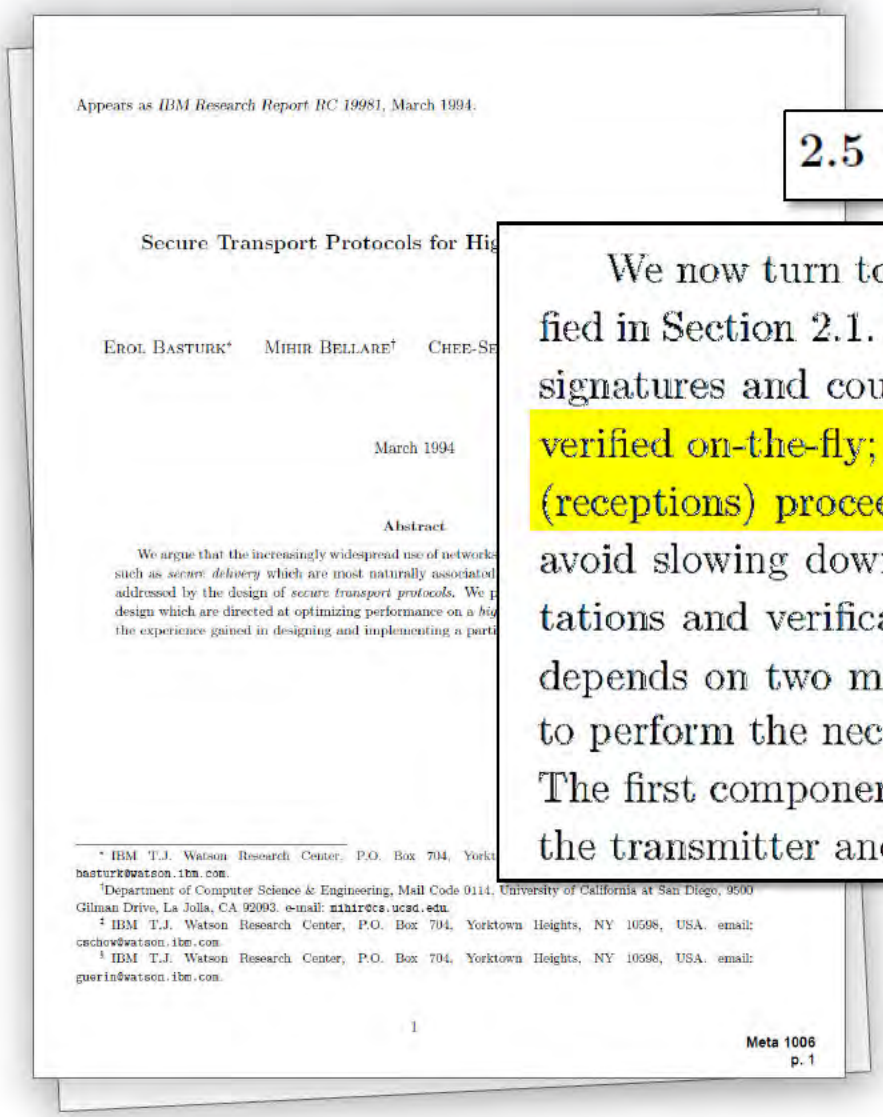
Meta 1006
p. 1

2.1 Performance Issues

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

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for Hig

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks such as *secure delivery* which are most naturally associated addressed by the design of *secure transport protocols*. We p design which are directed at optimizing performance on a *hig* the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorkt basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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 12

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.

1. Ideally, we want signatures to be computed on-the-fly; i.e., MAC **generation** should be carried out as **transmissions** proceeds rather than **before** these operations have been completed.
2. Ideally, we want signatured to be computed on-the-fly; i.e., MAC **verification** should be carried out as data **receptions** proceeds rather than **after** these operations have completed.

EX1006 (Basturk) at 12; EX1033 (Houh Supp. Declaration) at ¶12

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.

"On-the-fly" = Computing the MAC in parallel to the transmission/reception of the packet

EX1006 (Basturk) at 12; EX1033 (Houh Supp. Declaration) at ¶12

Ground I: Handley + Basturk

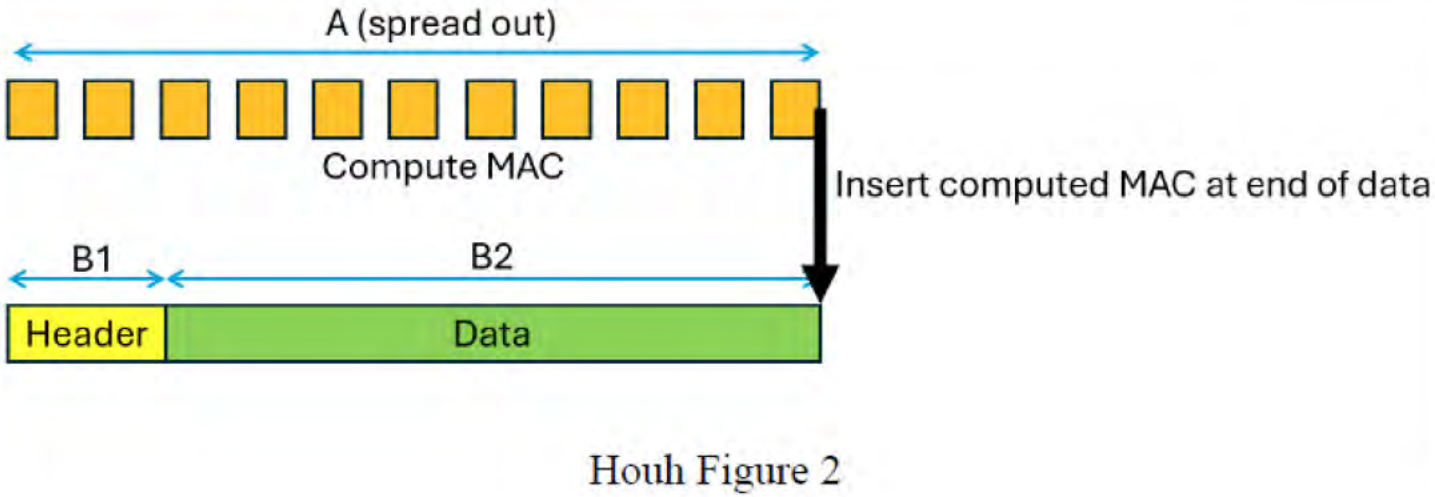
Petitioners' Technical Expert Witness



Dr. Henry Houh

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.



Houh Figure 2

EX1006 (Basturk) at 12; EX1033 (Houh Supp. Declaration) at Houh Figure 2

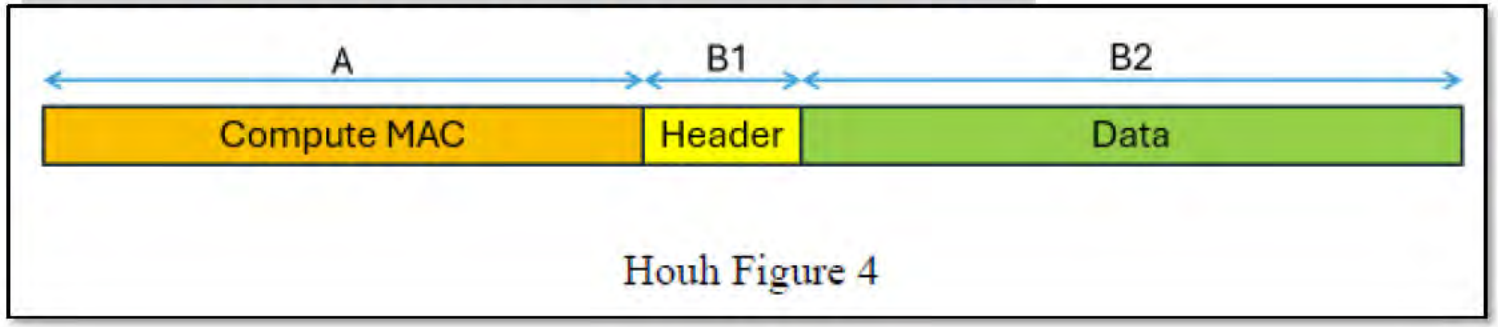
Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



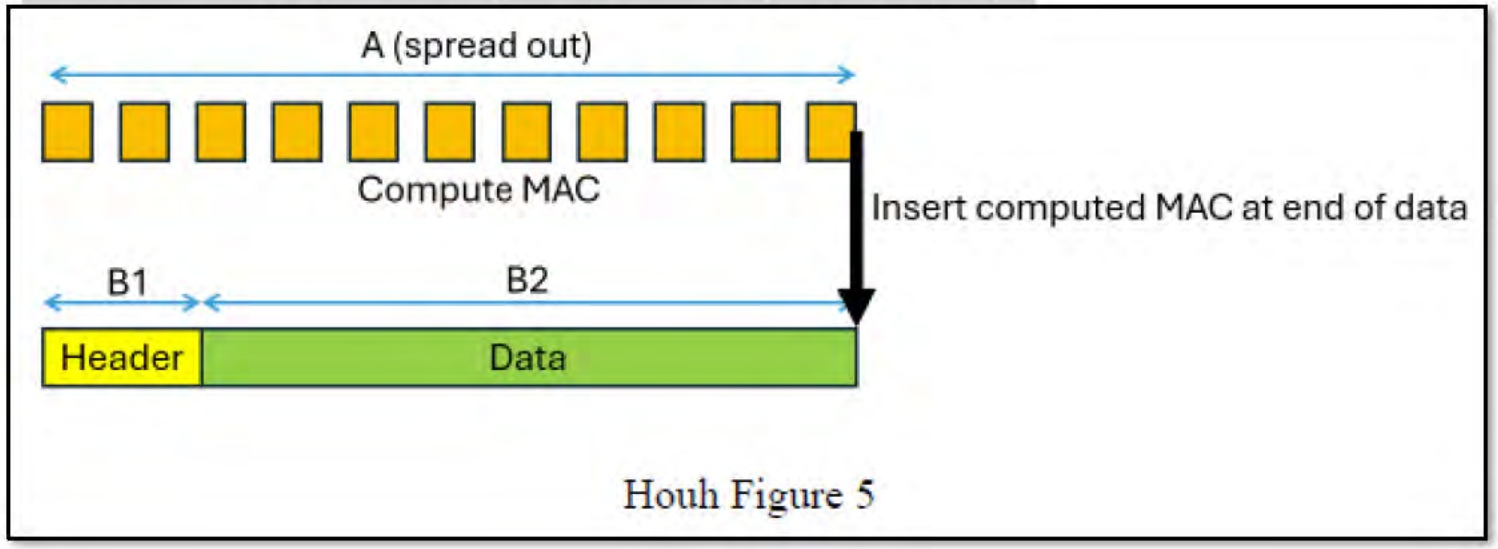
Dr. Henry Houh

Serial Computation (A + B1 + B2)



Houh Figure 4

On-the-fly Computation (B1 + B2)



Houh Figure 5

EX1033 (Houh Supp. Declaration) at Houh Figures 4, 5

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

107. Instead, Basturk is referring to starting the process of computing the style of MAC during (or in parallel with) the process of *retrieving context data* for performing cryptographic operations. In other words, Basturk is referring to starting the process of MAC computation (*i.e.*, computing a hash function portion of a particular style of MAC) while the process of *retrieving context information* for computing a cryptographic portion of the MAC is being performed. *See* § IX.B.3, *supra*. EX1006 at 8.

EX2004 (Stubblebine Declaration) at ¶107

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

85. Basturk states that "[t]he 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," known as "context" ("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"). EX1006 at 12. Basturk teaches that this context retrieval step creates latency because signature computation relies on the use of "secret information (key) shared by the two communicating parties," which is "necessary for such processing" and "must typically be retrieved upon receipt of a packet and this context retrieval step can introduce latency." EX1006 at 8. Basturk suggests reducing this context retrieval latency by putting the context information early in each packet, namely in a security segment in the packet's header. EX1006 at 12, 13, 15-16.

EX2004 (Stubblebine Declaration) at ¶85

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

March 1994

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.

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.

2.1 Performance Issues

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 12-13, 6, 11

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

March 1994

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.

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

2.5 Integrity and signatures

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.

2.1 Performance Issues

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 6, 11

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

EX1006 at 8. As seen, Basturk teaches that the latency due to retrieving the context information is upon receipt of a packet, not upon transmission of a packet, where the context information is "immediately availab[le]." *Id.* Because Basturk teaches context information is immediately available during data transmission—meaning there is no latency—Basturk's "on-the-fly" technique and goal of "minimize[ing] latency" would provide no benefit during data transmission, as there is no latency to minimize. EX1006, 7-8. In contrast, a POSITA would have understood that to minimize latency during data transmission, Basturk's "on-the-fly" teaching means that "MAC generation should be carried out as data transmission proceeds," to reduce latency introduced by MAC computations. EX1006, 7.

EX1033 (Houh Supp. Declaration) at ¶14

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

Q. Which form of latencies are you aware of in Basturk?

A. There is the latency with respect to context retrieval. It takes some time to do context retrieval. It may take some time in context retrieval.

For example, if you're in -- I -- if you're communicating with a party, like an ongoing communication, there would be no need for any significant latency with respect to context retrieval because any implementation would cache the key because this is an ongoing session.

And with ongoing session, you would know that until the connection is closed, like a TCP connection, or you're no longer -- there is an end to a TCP connection, you would know that until that occurs, you should probably keep the key. Then you can limit the time.

So I don't believe it actually reduces lateney on an ongoing basis, for example, during an interaction. That's with respect to context retrieval latency.

EX1031 (Stubblebine Deposition) at 71:1-22

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

Q Do you see evidence in Basturk which shows that on the fly does assist with context latency?
ATTORNEY EKLEM: Objection to form. And scope.
A I'm sorry. You said where it does?
Q Yes.
A Where it does?
Q Where it does assist --
A Assist?
Q -- assist with context retrieval latency.
A It's -- I think it's in here. Somewhere it says, "Put the context information early in the message."
But in most protocols, context information is already early in the message. Rarely do you put context information at the end of the message. It's normally the header that has information.
So I don't see much value at all with that little nugget of putting context information in the front of the message. If you can -- we can go through various protocols. If you have secure email, who you're communicating with is up front. If you're doing like almost -- I can't think of a protocol where you don't put context information already up in the front.
So, no, I don't see any particular advantage of -- of this paper when it comes to something we kind of already know and do.

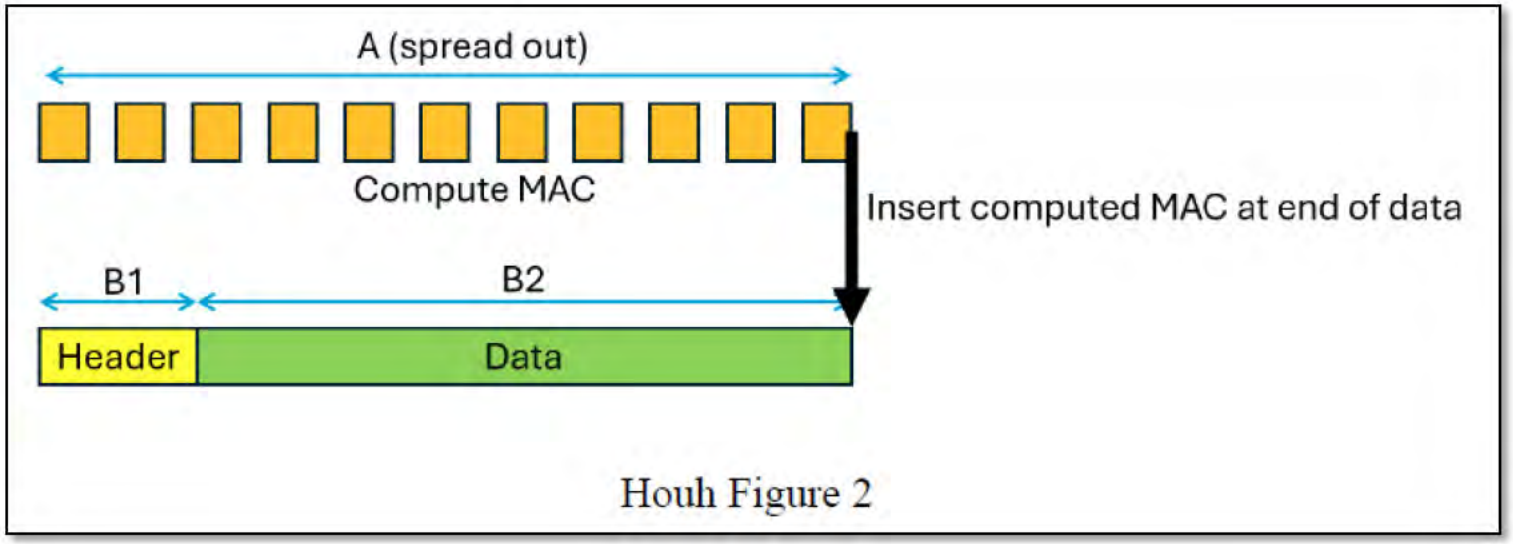
EX1031 (Stubblebine Deposition) at 78:1-79:6

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh



Houh Figure 2

"On-the-fly" = Computing the MAC in parallel to the transmission/reception of the packet

EX1033 (Houh Supp. Declaration) at Houh Figure 2, ¶15

Ground I: Handley + Basturk

Petitioner's Technical Expert Witness



Dr. Henry Houh

EX1006 at 9. A POSITA would have understood that when the MAC is computed "on-the-fly" over the data payload and transport header as data transmission of the packet proceeds, this can only be done if the MAC is placed at the end of a packet. If the MAC were placed somewhere other than at the end of the packet, the "on-the-fly" MAC computation during data transmission cannot be computed for the data in the packet that is transmitted **after** the fully computed MAC is inserted into the packet. Were the MAC located at the beginning or in the middle of the packet, the "on-the-fly" computed MAC would not be computed over the data transmitted after the MAC is inserted and, thus, cannot accurately reflect the correct MAC computed over the whole packet.

EX1033 (Houh Supp. Declaration) at ¶15

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness

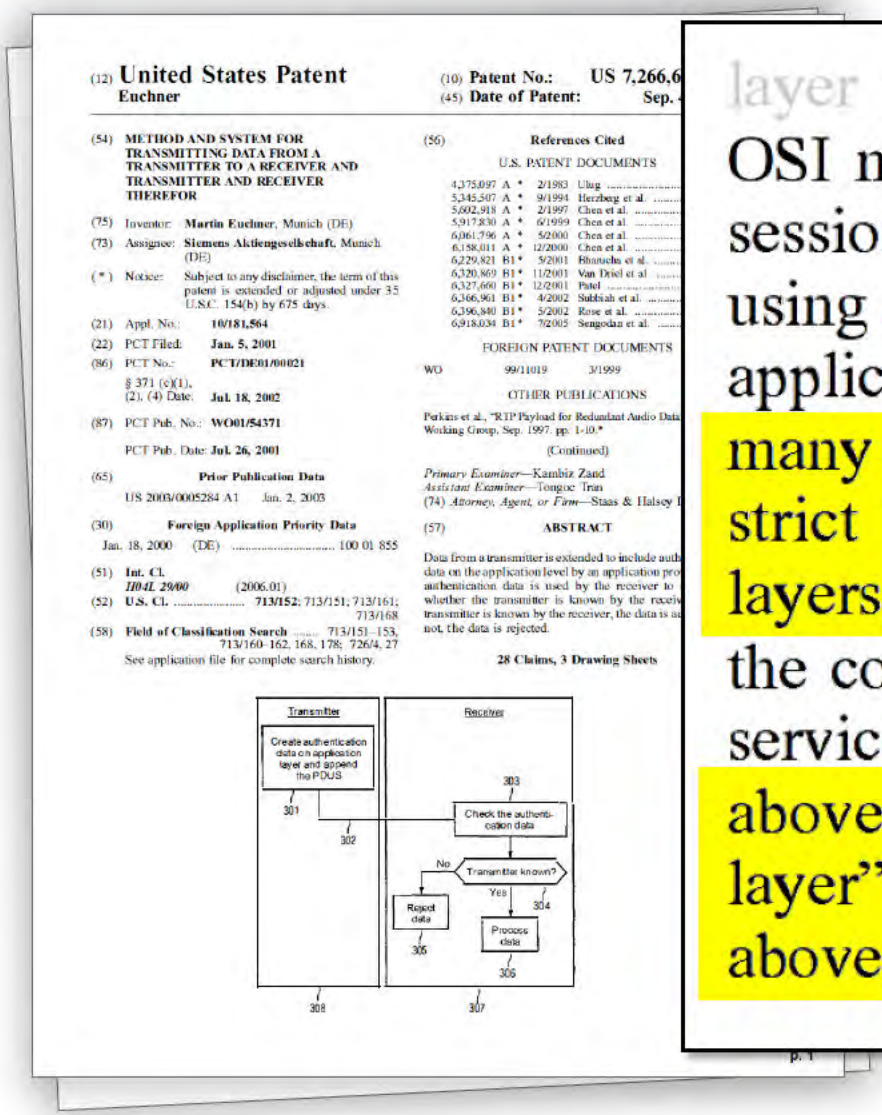


Dr. Stuart Stubblebine

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 only after PDU formation is completed, and transmission of the data doesn't occur until it reaches the physical layer (in conjunction with the link layer) where the PDU for transmission is a bit. *See* §§ VI.A (OSI) and VI.E (Ethernet). POSITA would have understood that if a packet requires information to be computed (in Dr. Houh's hypothetical, a signature), that information will always have to be computed before passing the PDU to the next layer. Thus, a POSITA would have understood that even with Basturk's "on-the-fly" processing, packets would not be passed to the next layer until all computations for that packet are complete. A POSITA would therefore

EX2004 (Stubblebine Declaration) at ¶108

Ground I: Handley + Basturk



(12) **United States Patent**
Euchner

(10) **Patent No.:** US 7,266,6
(45) **Date of Patent:** Sep.

(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(b) 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	
5,345,507	A *	9/1994	Herzberg et al.	
5,602,918	A *	2/1997	Chen et al.	
5,917,830	A *	6/1999	Chen et al.	
6,061,796	A *	5/2000	Chen et al.	
6,158,011	A *	12/2000	Chen et al.	
6,229,821	B1 *	5/2001	Bhatnchi et al.	
6,320,869	B1 *	11/2001	Van Driel et al	
6,327,660	B1 *	12/2001	Patel	
6,366,961	B1 *	4/2002	Subbiah et al.	
6,396,840	B1 *	5/2002	Rose et al.	
6,918,034	B1 *	7/2005	Sengodan et al.	

FOREIGN PATENT DOCUMENTS

WO	99/11019	3/1999

OTHER PUBLICATIONS

Perkins et al., "RTP Payload for Redundant Audio Data Working Group, Sep. 1997. pp. 1-10.*
(Continued)

Primary Examiner—Kambiz Zand
Assistant Examiner—Tongoc Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey

(57) **ABSTRACT**

Data from a transmitter is extended to include auth data on the application level by an application pro authentication data is used by the receiver to whether the transmitter is known by the receiv transmitter is known by the receiver, the data is a not, the data is rejected.

28 Claims, 3 Drawing Sheets

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 (US 7,266,682) at 1:25-45

Ground I: Handley + Basturk

Patent Owner's Technical Expert Witness

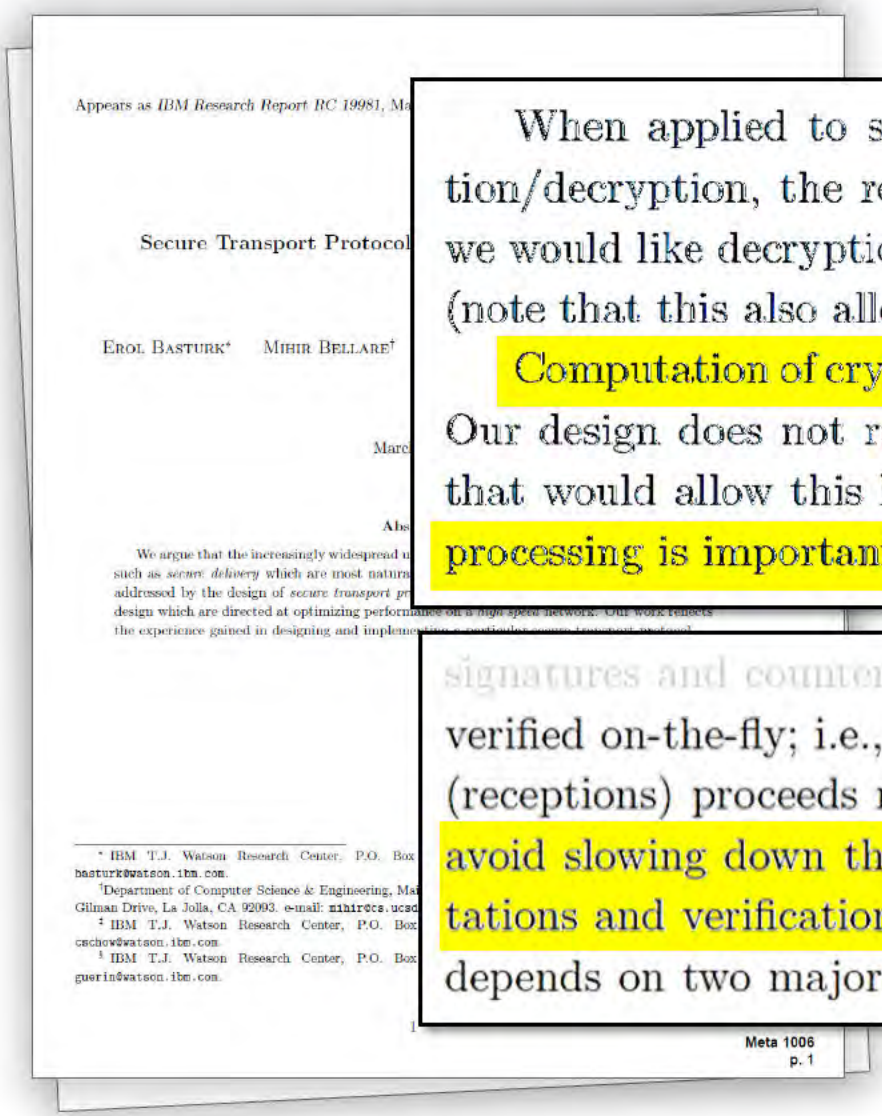


Dr. Stuart Stubblebine

128. I disagree with Dr. Houh's opinion that "the Ethernet standard … employs the same design choice reasoning to include a 'Frame Check Sequence' ('FCS') at the end of the Ethernet frame *so it can be computed during transmission and appended to the end of the frame*." EX1003 ¶ 85. In the context of Ethernet, transmission refers to generating and transmitting electromatic waves on a physical medium at ISO layer 1 (in conjunction with the link layer ISO layer 2) where the PDU is a single bit. *See* EX1014 at 32, 142-143; *see* § VI.E, *supra*.

EX2004 (Stubblebine Declaration) at ¶128

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, Ma

Secure Transport Protocol

Erol Basturk* Mihir Bellare†

Marc

Abs

We argue that the increasingly widespread u
such as *secure delivery* which are most naturs
addressed by the design of *secure transport pr*
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.

* IBM T.J. Watson Research Center, P.O. Box
basturk@watson.ibm.com.
†Department of Computer Science & Engineering, Ma
Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd
‡ IBM T.J. Watson Research Center, P.O. Box
cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box
guerin@watson.ibm.com.

When applied to security functions such as signature generation and verification or encryption/decryption, the requirement of on-the-fly processing has several implications. For example, we would like decryption of a received packet to proceed independently of that of any other packet (note that this also allows parallelization) as packets may be received out of order.

Computation of cryptographic functions can be greatly speeded up by use of dedicated hardware. Our design does not require such hardware to be available, but adopts various design principles that would allow this hardware, if available, to be exploited in the best possible way. On-the-fly processing is important in this regard as it facilitates the eventual off-loading to the hardware.

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

EX1006 (Basturk) at 7, 11

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

26. Hardware protocol accelerators allow incomplete packets, such as those including uncomputed header checksum values, to be passed from upper layers down to network interface hardware that compute and fill in these values at a lower layer in the protocol stack. Basturk specifically teaches using this kind of accelerator hardware:

EX1033 (Houh Supp. Declaration) at ¶26

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

27. Dr. Stubblebine implies that design choice reasoning at one layer cannot be applied to other layers. *See* EX2004, ¶110. I disagree. For example, the frame check sequence ("FCS") in the Ethernet protocol is a value that is appended to an Ethernet frame that is a calculation over the data in the frame itself (excluding the preamble, start frame delimiter, and the FCS itself). *See* EX1014, 26, 29. Received frames with a locally calculated FCS that do not match the value calculated at the transmitter are deemed invalid and discarded. *Id.* At the higher TCP layer, the header checksum value in the TCP header "provides a verification that the information used in processing internet datagram has been transmitted correctly" and that "[i]f the header checksum fails, the internet datagram is discarded at once by the entity which detects the error." EX1013, 9. The same reasoning at one layer

EX1033 (Houh Supp. Declaration) at ¶27

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

by the entity which detects the error." EX1013, 9. The same reasoning at one layer is applied at other layers as well. For example, the placement of the FCS at the end of the Ethernet frame enables the FCS value to be computed as the frame is transmitted and appended to the end of the frame. This concept can be applied to the check sequences or authentication sequences at another layer that are also placed at the end of that layer's PDU. The MAC can be computed "on-the-fly" and placed at the end of an RTP packet while the FCS is computed on the fly and placed at the end of an Ethernet frame. Such trailers are nested just as headers are nested.

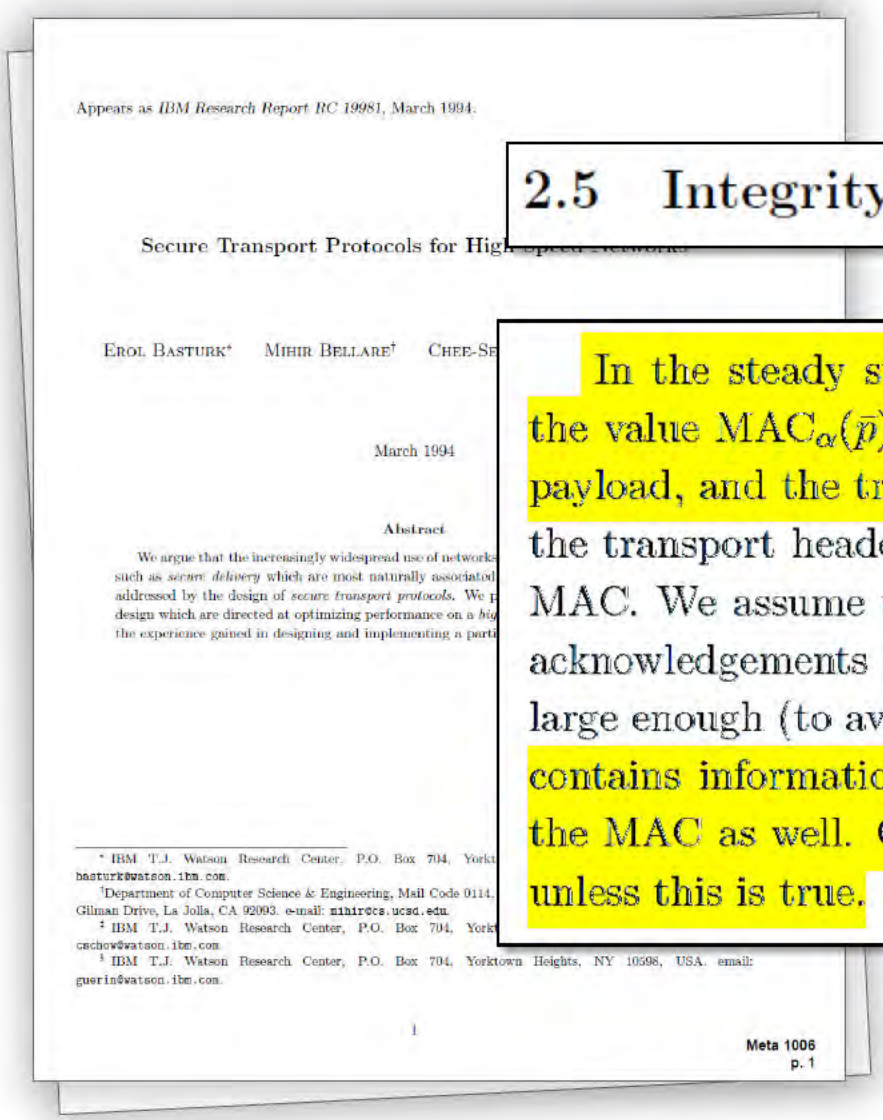
EX1033 (Houh Supp. Declaration) at ¶27

Ground I: Handley + Basturk

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground I: Handley + Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks such as *secure delivery* which are most naturally associated addressed by the design of *secure transport protocols*. We p design which are directed at optimizing performance on a *big* the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, York basturk@watson.ibm.com.

†Department of Computer Science & Engineering, Mail Code 0114, Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.

‡ IBM T.J. Watson Research Center, P.O. Box 704, York cschow@watson.ibm.com.

§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

Meta 1006
p. 1

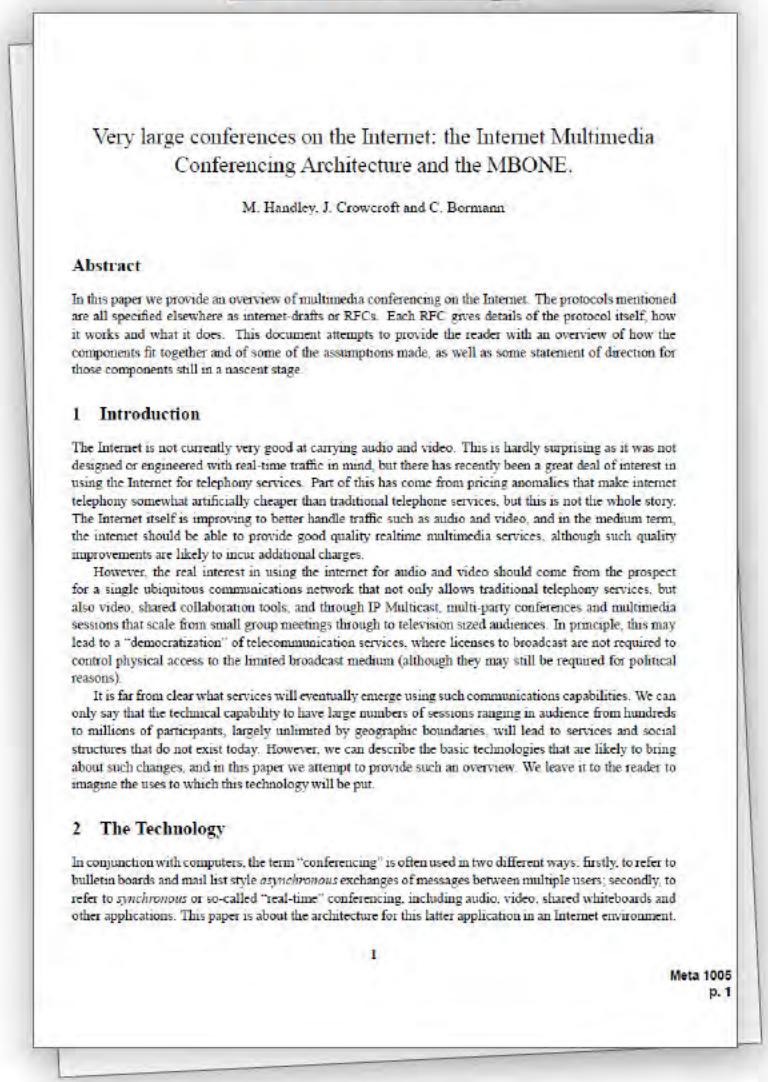
2.5 Integrity and signatures

In the steady state (integrity option assumed selected) the sender attaches to each packet p the value $\mathrm{MAC}_\alpha(\bar{p})$ where $\bar{p}$ is the subset of p which includes the transport header, the full data payload, and the trailer of the packet p. We will see that of particular importance is the fact that the transport header includes the sequence number of the packet which is thereby covered by the MAC. We assume that all packets in each direction, even those which are purely transport level acknowledgements (ACKs), can be differentiated. A simple solution is to include in each packet a large enough (to avoid wrap-around) *signature* counter. We also assume that the transport header contains information which identifies the sender so that the identity of the sender is covered by the MAC as well. On receiving p, τ the receiver checks that $\tau = \mathrm{MAC}_\alpha(\bar{p})$ and rejects the packet unless this is true.

EX1006 (Basturk) at 12

Ground I: Motivation to Combine Handley With Basturk

Handley



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.

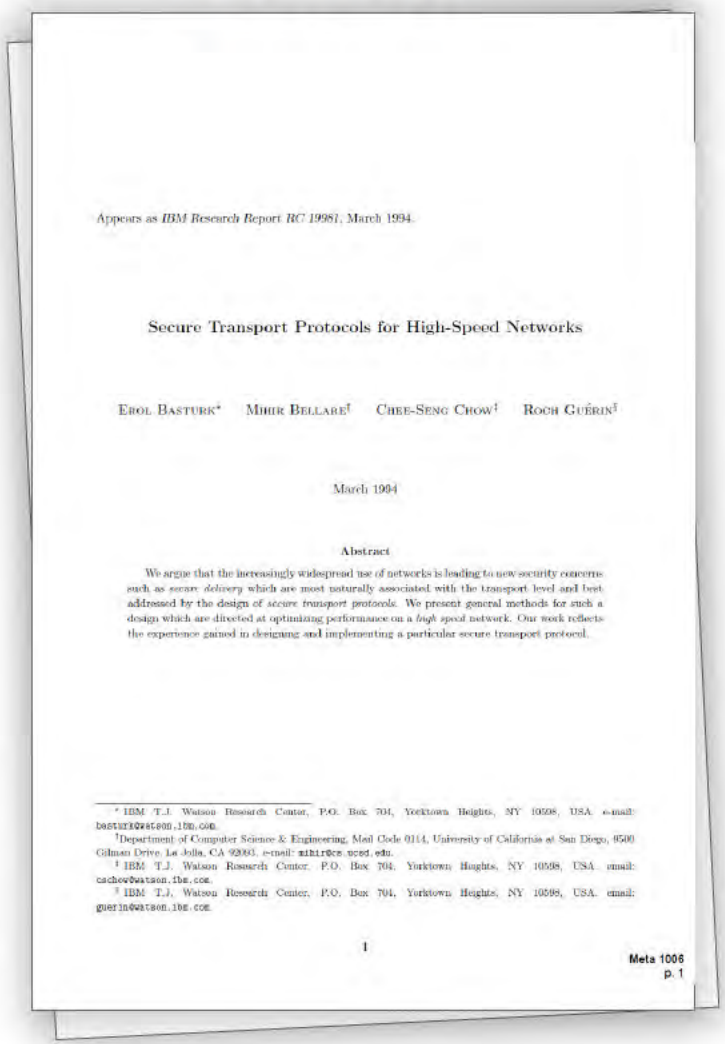
2 The Technology

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

Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Seng Chow‡ Roch Guérin§

March 1994

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.

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.
† Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

1

Meta 1006
p. 1

EX1005 (Handley) at 1; EX1006 (Basturk) at 1

Ground I: Motivation to Combine Handley With Basturk

Handley

Real-time applications such as audio and video need to be able to buffer real-time data at the receiver for sufficient time to remove the jitter added by the network and recover the original timing relationships between the media data. In order to know how long to buffer for, each packet must carry a timestamp which gives the time at the sender when the data was captured. Note that for audio and video data timing recovery, it is not necessary to know the absolute time that the data was captured at the sender, only the time relative to the other data packets.

Basturk

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.

We now turn to design issues motivated by performance. Let us recall some of the issues identified in Section 2.1. It is essential that the steady state overhead involved in computing and checking 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.

EX1005 (Handley) at 8; EX1006 (Basturk) at 7, 12-13

Ground I: Motivation to Combine Handley With Basturk

Handley

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 must be sufficient capacity in the relevant traffic class to accommodate the traffic. How this capacity is ensured is independent of RTP.

- A POSITA would have understood that RTP is commonly used for video and audio conferences as described in RFC 1889.

8 Security

8.1 Authentication and Key Distribution

8.2 Encrypted Session Announcements

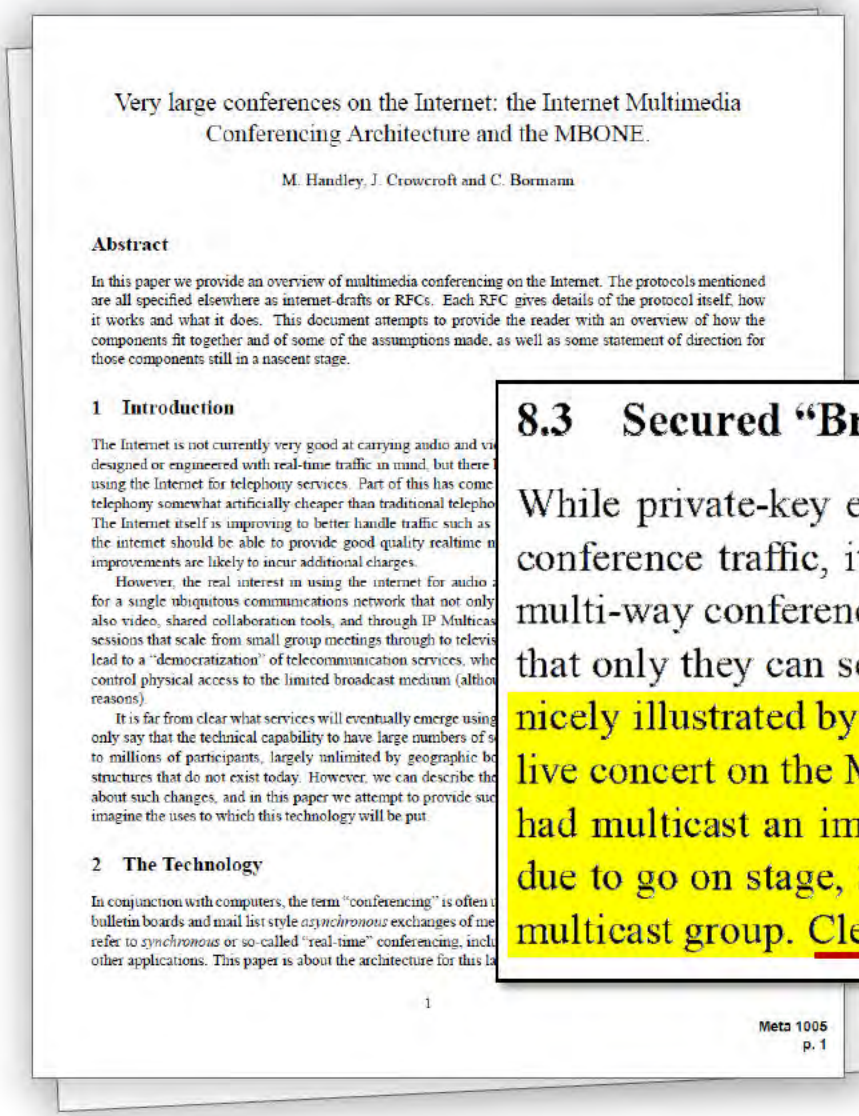
8.3 Secured "Broadcasts"

Basturk

PERFORMANCE. We take into account various *efficiency* requirements for the secure version of a transport protocol. Certain functions should be designed so that they can readily be off-loaded to hardware without impacting the original flow and processing of messages. Specifically, encryption and decryption may initially be performed in software, but, as speed increases, dedicated hardware components will almost certainly be required. For example, software encryption and decryption for secure video conferences may be feasible at low resolution. However, the provision of high resolution secure video conferences is likely to require hardware support. Our protocol should be able to operate in both environments. There are many other design aspects that need to reflect this requirement. For example, it may be worthwhile to factor into the design the eventual parallelization of certain processes, to define "intelligent" packet format for faster parsing, to allow rapid context retrieval based on simple connection-based information – all these things should be considered in order to provide greater efficiency.

EX1005 (Handley) at 8, 11-13; EX1006 (Basturk) at 3, 5,

Ground I: Motivation to Combine Handley With Basturk



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 vi
designed or engineered with real-time traffic in mind, but there
using the Internet for telephony services. Part of this has come
telephony somewhat artificially cheaper than traditional telepho
The Internet itself is improving to better handle traffic such as
the internet should be able to provide good quality realtime
improvements are likely to incur additional charges.

However, the real interest in using the internet for audio
for a single ubiquitous communications network that not only
also video, shared collaboration tools, and through IP Multicas
sessions that scale from small group meetings through to televis
lead to a "democratization" of telecommunication services, whe
control physical access to the limited broadcast medium (altho
reasons).

It is far from clear what services will eventually emerge using
only say that the technical capability to have large numbers of s
to millions of participants, largely unlimited by geographic bo
structures that do not exist today. However, we can describe th
about such changes, and in this paper we attempt to provide suc
imagine the uses to which this technology will be put.

2 The Technology

In conjunction with computers, the term "conferencing" is often
bulletin boards and mail list style *asynchronous* exchanges of me
refer to *synchronous* or so-called "real-time" conferencing, incl
other applications. This paper is about the architecture for this

1

Meta 1005
p. 1

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 of a session are equal. This is normally acceptable for multi-way conferences, but will not be acceptable for many broadcasters who require the ability to ensure that only they can send, perhaps in addition to ensuring that only their paid customers can receive. This is nicely illustrated by the multicast of the Rolling Stones concert in 1994 which was billed as being the first live concert on the Mbone. In fact, this honour goes to a little known band called Severe Tire Damage who had multicast an impromptu concert a year previously. To make their point, just before the Stones were due to go on stage, Severe Tire Damage suddenly started broadcasting one of their songs live to the same multicast group. Clearly commercial broadcasters want to avoid occurrences like this one.

EX1005 (Handley) at 13

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

111. It would not have been obvious to a POSITA to modify Handley's architecture, which uses RTP over the UDP, with Basturk's transport protocol, which "is essentially an extension of the standard transport level *reliability* feature." EX1006 at 4. A POSITA would have understood that "the standard transport level reliability feature" is a feature provided by protocols, such as the well-known Transmission Control Protocol ("TCP"). EX2006. Reliability is the ability to "recover from data that is damaged, lost, duplicated, or delivered out of order," and is achieved through timeout and retransmission policies, reordering packets received out of order based on sequence numbers, and eliminating duplicates, among other things. EX2006 at 10; *id.* at 16 ("Transmission is made reliable via the use of sequence numbers and acknowledgments."). A POSITA would have understood that the increase in reliability of TCP comes at the cost of end-to-end delay caused by its reliability features.

EX2004 (Stubblebine Declaration) at ¶111

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

112. A POSITA would also have understood that Basturk's protocol, as "an extension of the standard transport level *reliability* feature," would involve similar delays as other reliability protocols like TCP. Indeed, Basturk's protocol achieves "secure delivery" by providing acknowledgements that include sequence numbers and are signed. *See* § IX.B.1; EX1006 at 12 ("Secure delivery is guaranteed because the ACKs include sequence numbers and are signed."). A POSITA would therefore have understood that Basturk's protocol is a reliable delivery protocol like TCP and would therefore have similar end-to-end delay drawbacks.

EX2004 (Stubblebine Declaration) at ¶112

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness

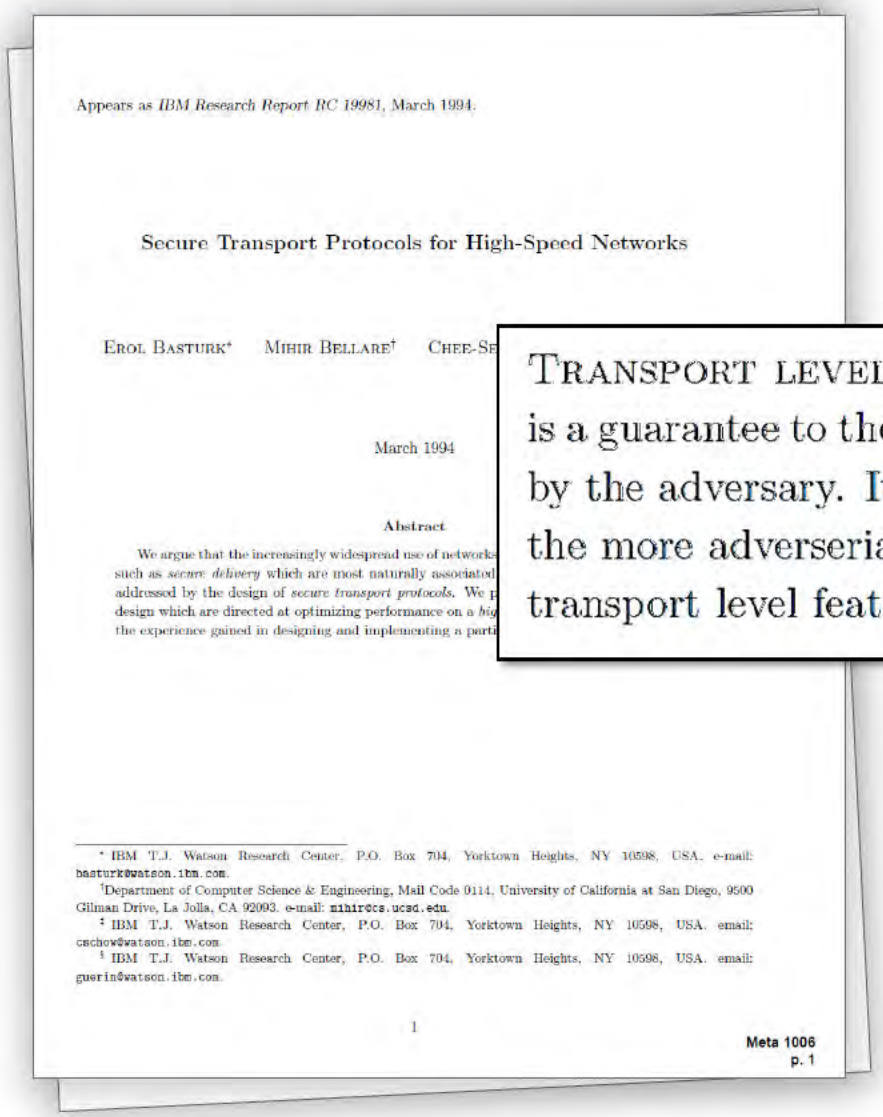


Dr. Stuart Stubblebine

113. Handley teaches away from using reliability protocols like Basturk's for transmitting RTP traffic. Handley teaches that "[r]eal-time internet traffic is defined as datagrams that are delay sensitive," such as where "where exceeding an end-to-end delay bound of a few hundred milliseconds renders the datagrams useless for the purpose they were intended." EX1005 at 4-5. Handley states that "For the purposes of this definition, TCP traffic is normally not considered to be real-time 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 ("[UDP] is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).").

EX2004 (Stubblebine Declaration) at ¶113

Ground I: Motivation to Combine Handley With Basturk



Appears as *IBM Research Report RC 19981*, March 1994.

Secure Transport Protocols for High-Speed Networks

Erol Basturk* Mihir Bellare† Chee-Se

March 1994

Abstract

We argue that the increasingly widespread use of networks
such as *secure delivery* which are most naturally associated
addressed by the design of *secure transport protocols*. We p
design which are directed at optimizing performance on a *big*
the experience gained in designing and implementing a parti

* IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. e-mail: basturk@watson.ibm.com.
†Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093. e-mail: mihir@cs.ucsd.edu.
‡ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: cschow@watson.ibm.com.
§ IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, NY 10598, USA. email: guerin@watson.ibm.com.

1

Meta 1006
p. 1

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 adverserial setting we are discussing, which is why it seems most natural to view it as a transport level feature.

EX1006 (Basturk) at 4

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

reliability feature to the more adversarial setting we are discussing." EX1006, 4. A POSITA would have understood Basturk is not teaching reliable transport features of TCP, but something totally different. Reliable delivery protocols like TCP provide the ability to "'recover from data that is damaged, lost, duplicated, or delivered out of order"' as Dr. Stubblebine notes. EX2004, ¶ 111 (quoting EX2006, 10). In contrast, TCP does not guarantee to the sender A that his message was (1) "received by B," (2) "not intercepted," by the adversary, or (3) "destroyed by the adversary."

EX1033 (Houh Supp. Declaration) at ¶30

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

Q Does TCP guarantee protocol messages are not destroyed by an adversary?

A No. There is no guarantee after it's -- after -- no, there is no guarantees.

EX1031 (Stubblebine Deposition) at 197:6-9

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

> 31. Basturk, titled "**Secure Transport Protocols** for High-Speed Networks," is focused is on ***secure*** delivery, not reliable delivery. EX1006, 1. The reliability feature described in Basturk serves the purpose of authenticating the sender of the data, which is not a feature of protocols such as TCP. *See* EX1006, 4. This reliability feature of Basturk, e.g., to sign the packets (authenticating the source of data) is orthogonal to the reliability features in protocols such as TCP, which deliver the data reliably. *Id.*

EX1033 (Houh Supp. Declaration) at ¶30

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

32. By way of further example, Basturk describes that an adversary can forge a reply that acknowledges the receipt of data by the recipient and can intercept and destroy packets while sending these forged acknowledgements. *See* EX1006, 4. The sender believes the data was received when it was not. *Id.* Basturk teaches that this is possible because the acknowledgments are not generated by an application and, thus, are not signed. *Id.* Consequently, forged messages can be erroneously accepted. *Id.* As seen in Basturk, forged data can be reliably delivered, but the delivery of forged data can be prevented by adding a signature to the data. In other words, verifying that the data came from the correct sender is orthogonal to the correct delivery of that data. Thus, the "reliability" features in Basturk (guaranteeing to the sender that its message was received, not intercepted, and not destroyed by and adversary) do not overlap with the reliability features of TCP ("recovering from data that is damaged, lost, duplicated, or delivered out of order"), which a POSITA would have known and understood. *Id.*; EX2006, 10.

EX1033 (Houh Supp. Declaration) at ¶32

Ground I: Motivation to Combine Handley With Basturk

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

who each of the receivers are. EX2006 at 11, 16. Use of such a reliable delivery protocol is further disadvantageous to the sender because the sender needs to process acknowledgement messages sent by receivers to determine if a retransmission of a message is required by a sender. *See, e.g.*, EX2006 at 10 ("If the ACK is not received within a timeout interval, the data is retransmitted."). Basturk's protocol similarly uses acknowledgements, and thus would be similarly disadvantageous and thus would not be combined with Handley for similar reasons. EX1006 at 4 ("Then, she

EX2004 (Stubblebine Declaration) at ¶116

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

> 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, 9. A POSITA would not have understood this passage to mean that "[i]ntegrity via signing" only applies to acknowledgment packets, as Dr. Stubblebine opines. *Id.* Instead, a POSITA would have understood that Basturk's plain teaching of "[i]ntegrity via signing" means any data sent is signed under the integrity option. This can include any data sent, even data that does not require acknowledgment. *Id.*

EX1033 (Houh Supp. Declaration) at ¶38

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

disagree. Basturk's secure transport protocol is not a reliable delivery protocol like TCP and does not introduce hundreds of milliseconds of delay, as Dr. Stubblebine implies. EX2004, ¶113. As described in my First Declaration, performing the MAC computation "on-the-fly" as Basturk teaches does not add any latency to the transmission because the MAC computation occurs in parallel to the transmission. EX1003, ¶¶65, 85.

EX1033 (Houh Supp. Declaration) at ¶20

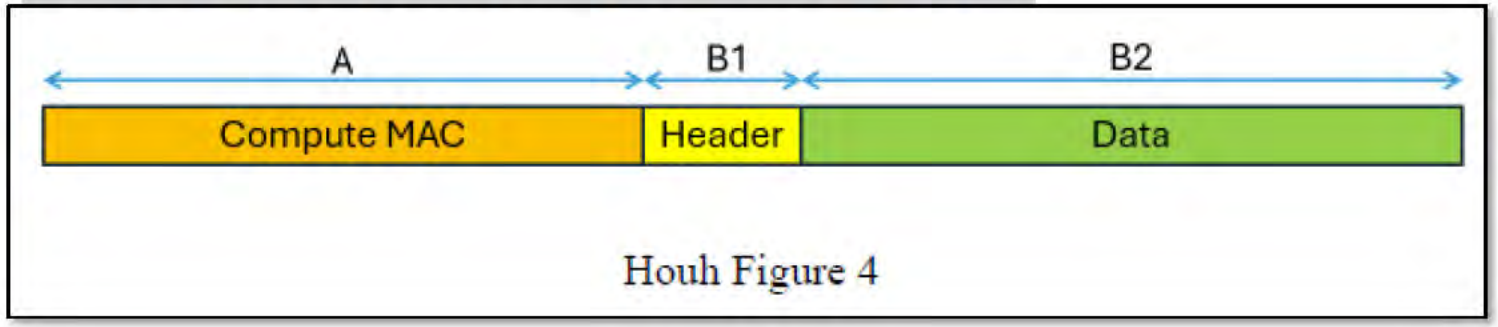
Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



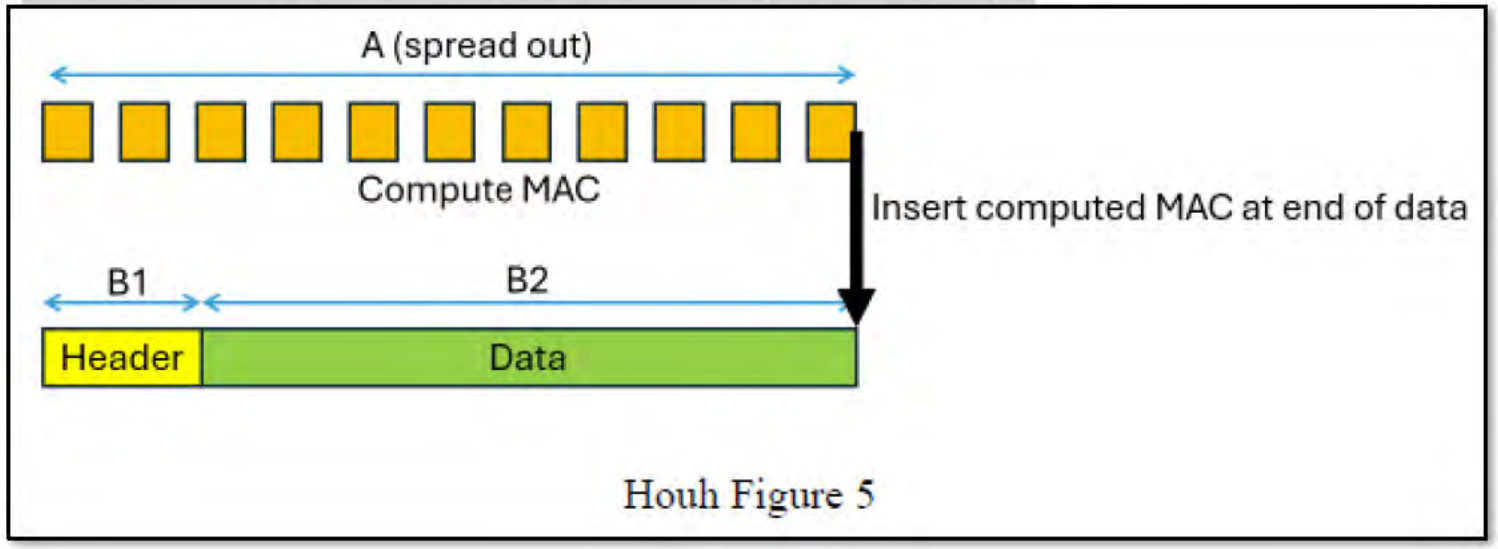
Dr. Henry Houh

Serial Computation (A + B1 + B2)



Houh Figure 4

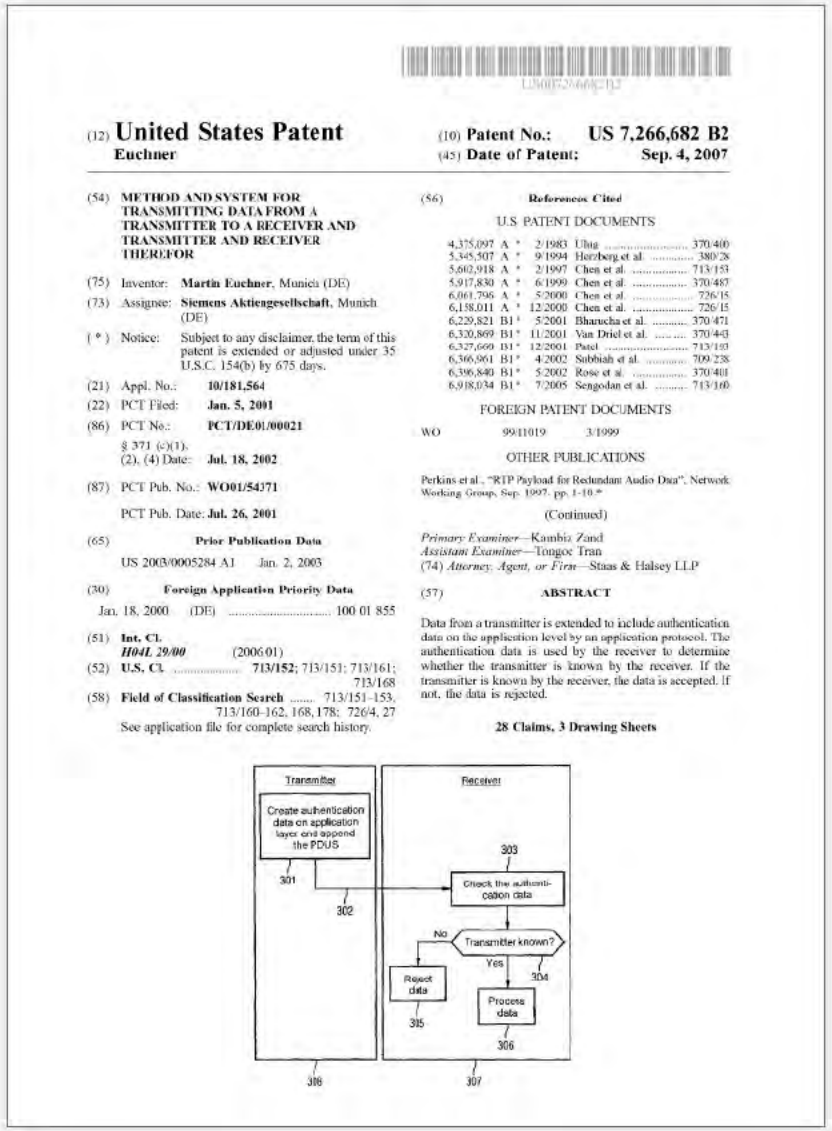
On-the-fly Computation (B1 + B2)



Houh Figure 5

EX1033 (Houh Supp. Declaration) at Houh Figures 4, 5

Overview



(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(b) 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 Uhua 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/463
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

1. Background
2. Prior Art
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. **Grounds**
   a. Ground I
   b. Ground II
   c. Ground III
   d. Ground IV

Invalidity Grounds

Ground I (Claims 1-21, 23, 25-28)

- Obvious under § 103 in view of Handley in combination with Basturk

Ground II (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Handley

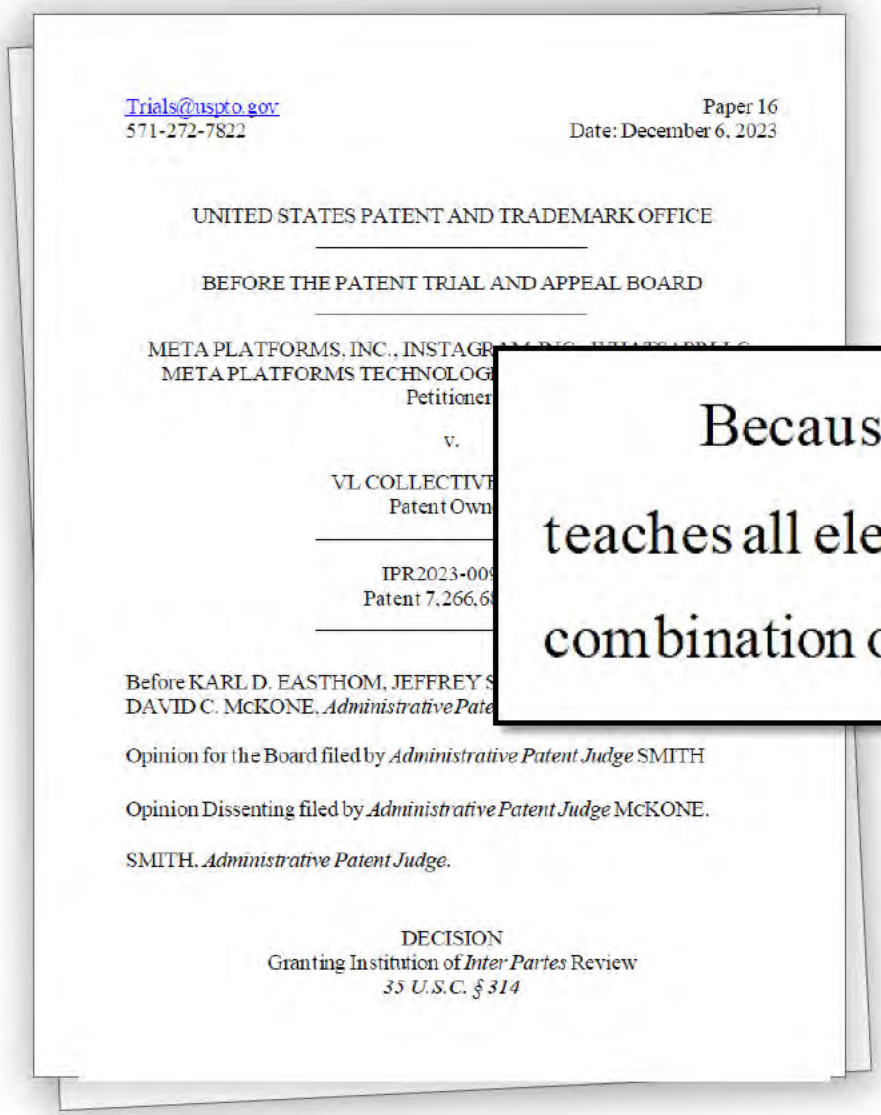
Ground III (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Basturk

Ground IV (Claims 22, 24)

- Obvious under § 103 in view of Handley in combination with Basturk and PacketCable

Invalidity Grounds



Trials@uspto.gov
571-272-7822

Paper 16
Date: December 6, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC., INSTAGR
META PLATFORMS TECHNOLOG
Petitioner

v.

VL COLLECTIVE
Patent Own

IPR2023-00
Patent 7,266,6

Before KARL D. EASTHOM, JEFFREY S
DAVID C. McKONE, *Administrative Pate*

Opinion for the Board filed by *Administrative Patent Judge* SMITH

Opinion Dissenting filed by *Administrative Patent Judge* McKONE.

SMITH, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

Because Petitioner has sufficiently shown that PacketCable alone teaches all elements of claim 1, Petitioner has sufficiently shown that the combination of PacketCable and Handley teaches claim 1. Based on

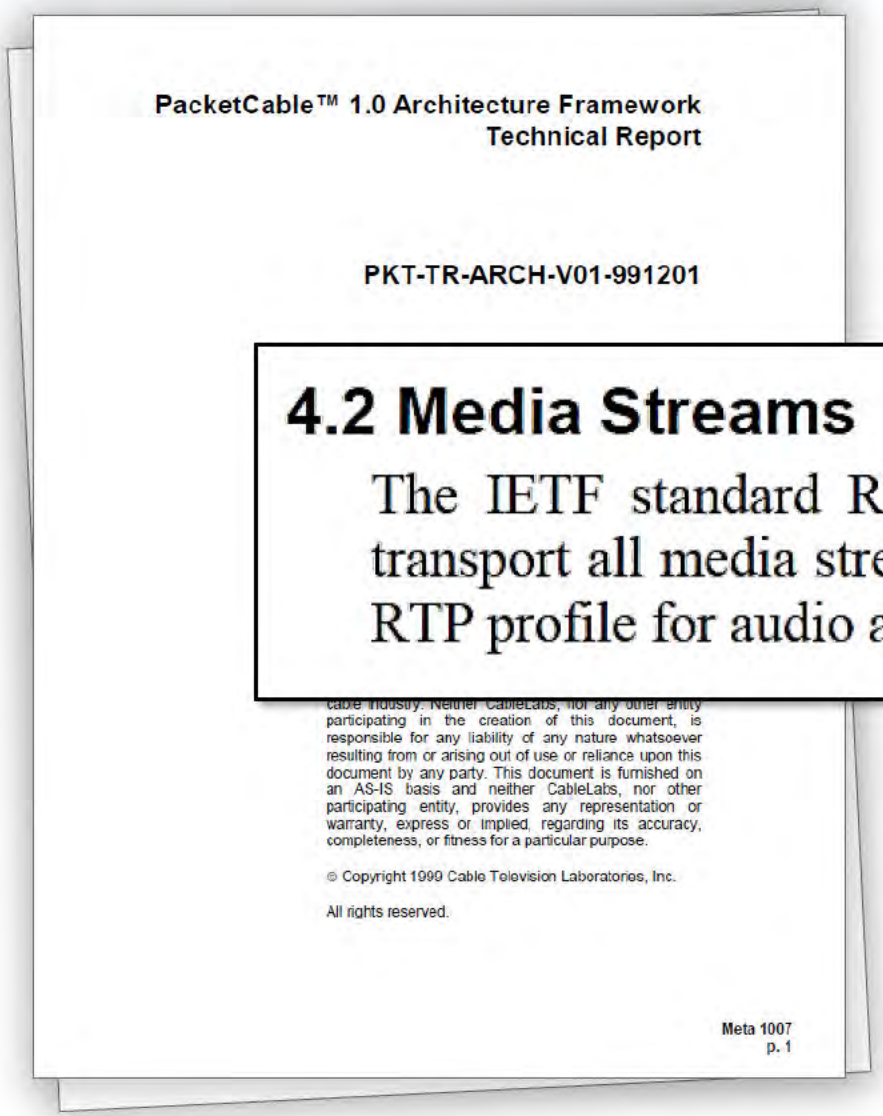
Paper 26 (Institution Decision) at 34

Ground II: PacketCable + Handley

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

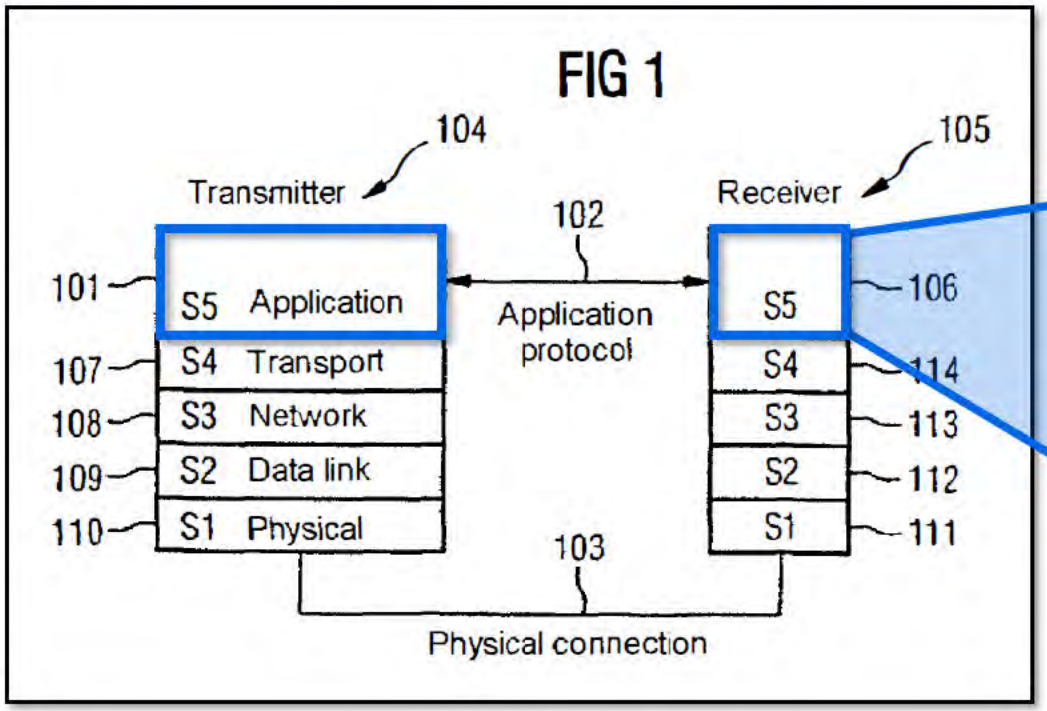
Meta 1007
p. 1

4.2 Media Streams

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 23, 37

Ground II: PacketCable + Handley



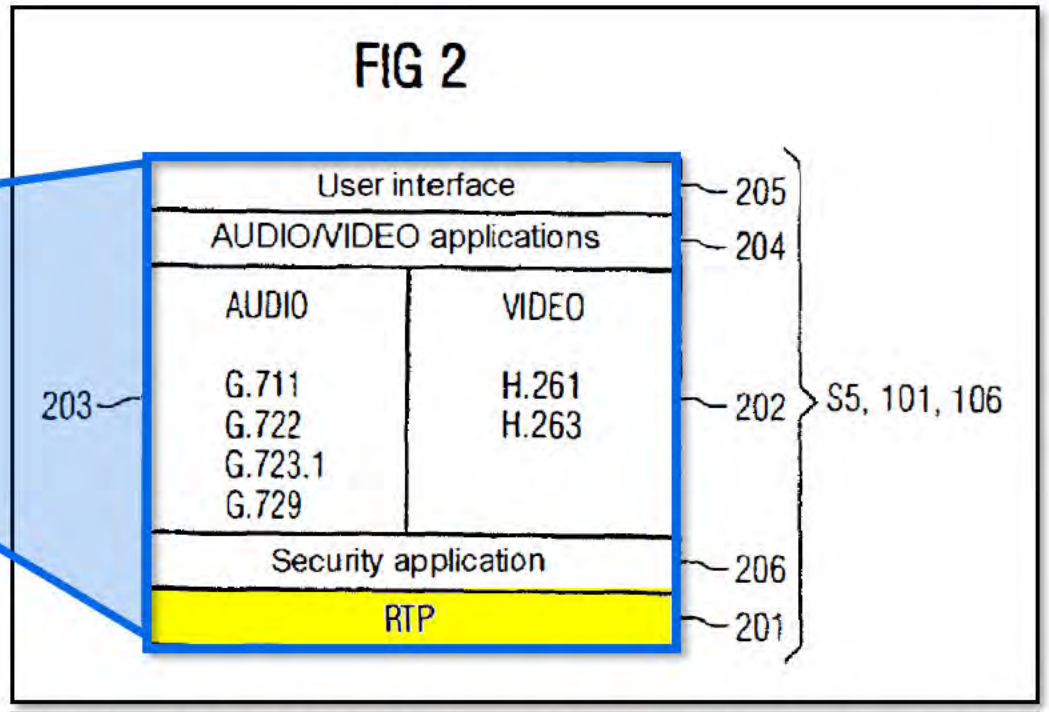


FIG. **2** is a block diagram of an application layer with possible protocols, based on an application concerning the transmission of media data (audio and video data). Thus, **101** and **106** represent the application layer (layer **5**) shown in FIG. **1** for the transmitter **104** and the receiver **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

EX1001 (US 7,266,682) at 6:33-42, Figs. 1, 2

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

142. To the contrary, as explained above, PacketCable indicates to a POSITA that MTA *devices* generally are responsible for providing secure transport services, including "Authentication, confidentiality and integrity of some messages between the MTA and other PacketCable network elements," namely those sent over the "pkt-s6" interface, which is a network interface for sending "*[e]nd-to-end media packets between two MTAs*" generally. *See* § IX.C.1, *supra*. However, PacketCable does not disclose "integration into application processing", *e.g.*, the "MTA Application." *Id.* PacketCable indicates to a POSITA that PacketCable uses the MTA device to provide secure transport services whereby "RTP packets are encrypted directly with RC4, without any additional security layers" and "[a]n MMH-based MAC (Message Authentication Code) optionally provides message integrity." EX1007 at 45. PacketCable, however, does not disclose how this

EX2004 (Stubblebine Declaration) at ¶142,

Ground I: Motivation to Combine Handley With Basturk

Petitioners' Technical Expert Witness



Dr. Henry Houh

58. Dr. Stubblebine states that "PacketCable indicates to a POSITA that MTA devices generally are responsible for providing secure transport services, including 'Authentication, confidentiality and integrity of some messages between the MTA and other PacketCable network elements.'" EX2004, ¶142. To the extent Dr. Stubblebine opines that a device performing authentication is different than an application performing authentication, that is incorrect. The authentication may be for different uses, and the device performing authentication does not preclude applications on the device from performing authentication.

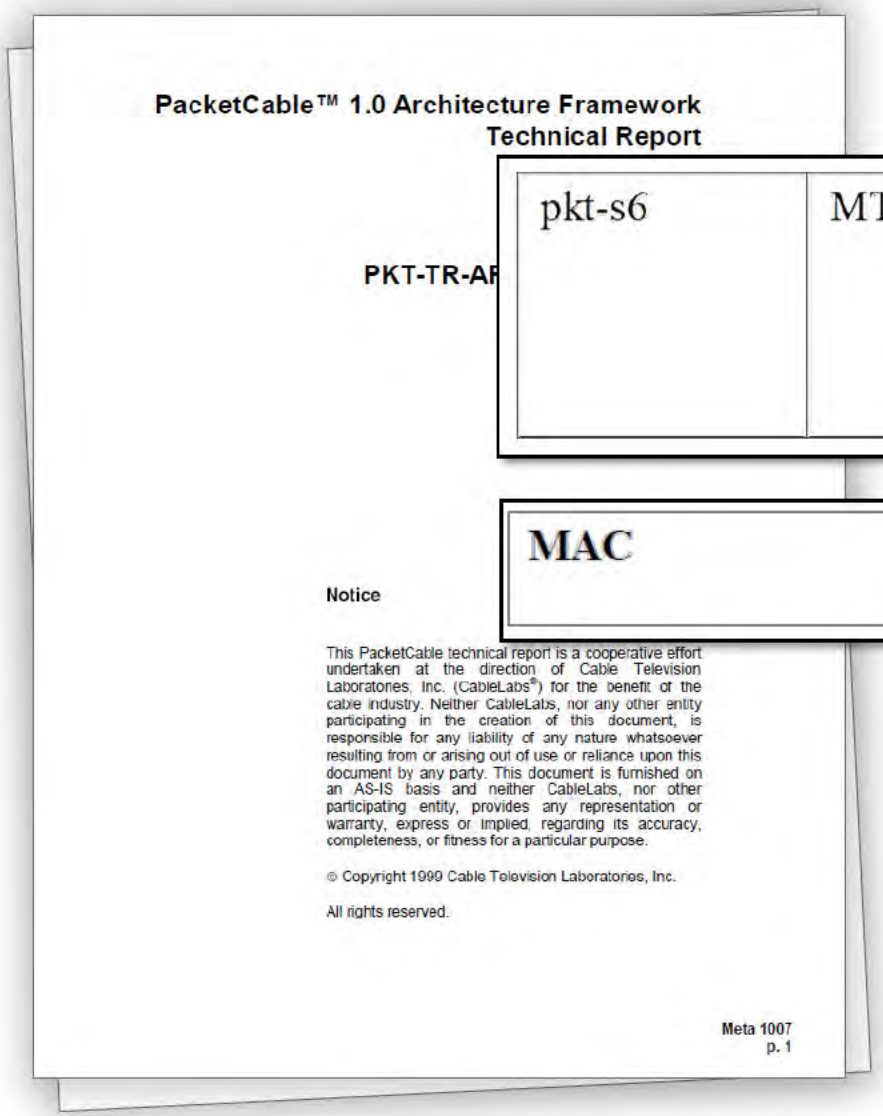
EX1033 (Houh Supp. Declaration) at ¶58, Houh Figures 4, 5

Ground II: PacketCable + Handley

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-AF

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

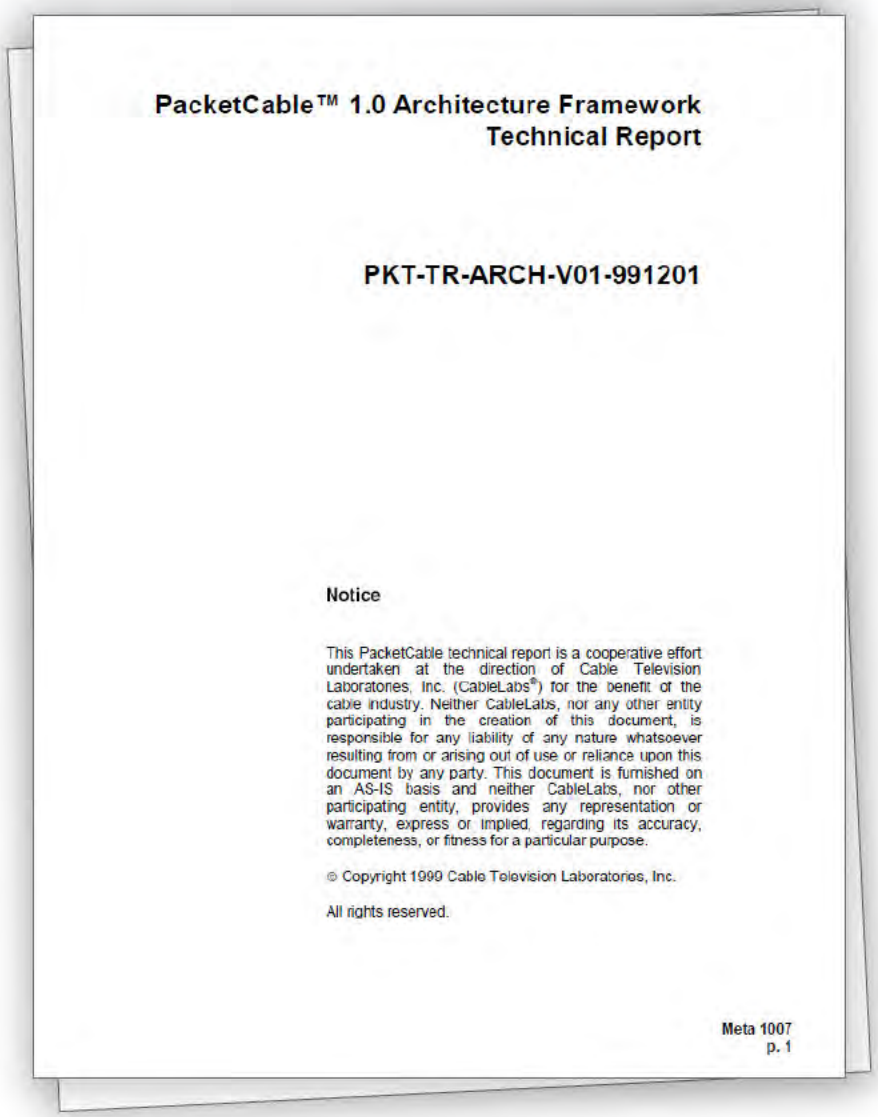
Meta 1007
p. 1

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.

MAC	Message Authentication Code - a fixed length data item that is sent together with a message to ensure integrity, also known as a MIC.

EX1007 (PacketCable) at 37, 55

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

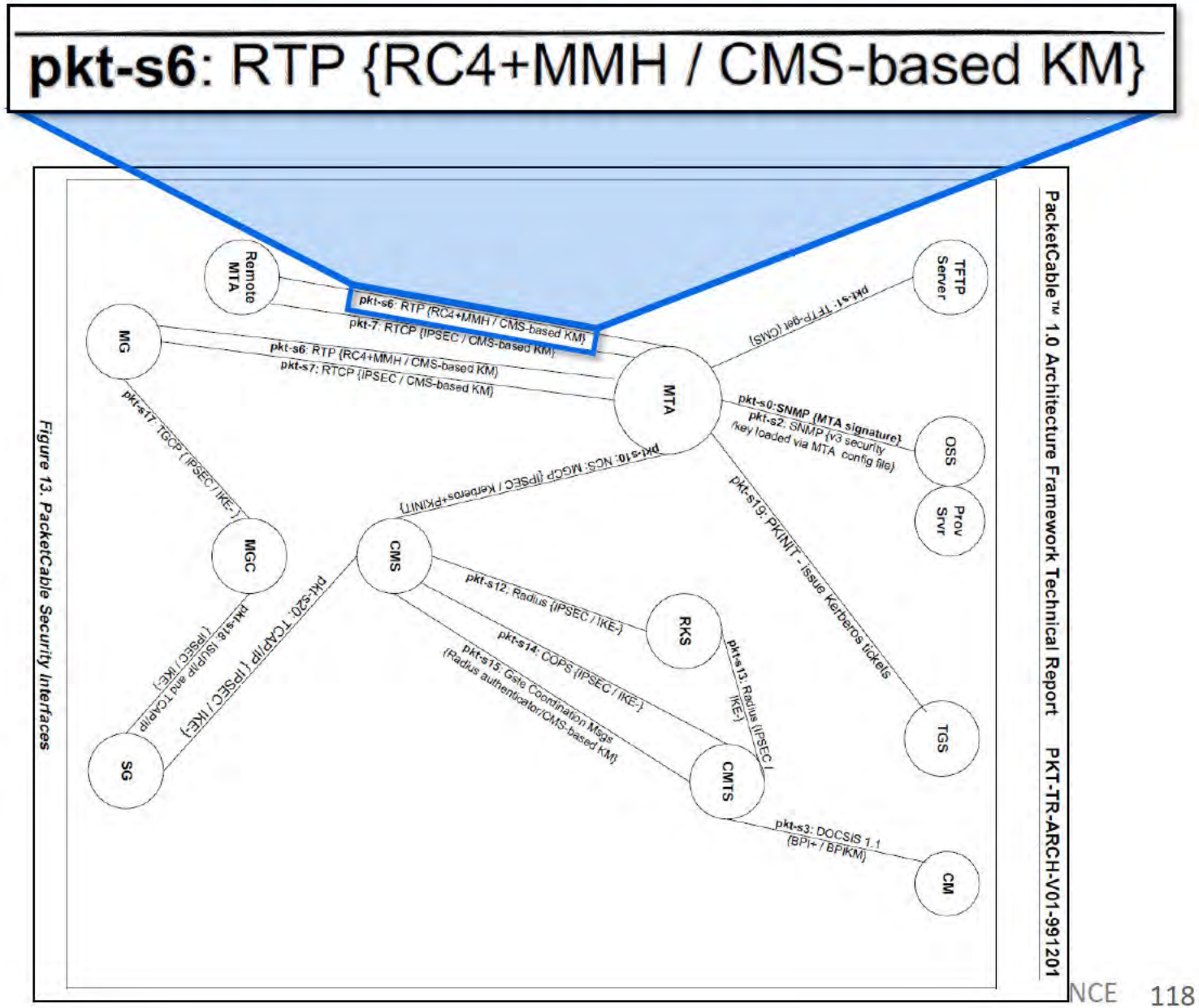


Figure 13. PacketCable Security Interfaces

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

EX1007 (PacketCable) at 44

Ground II: PacketCable + Handley

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

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 Declaration) at ¶147

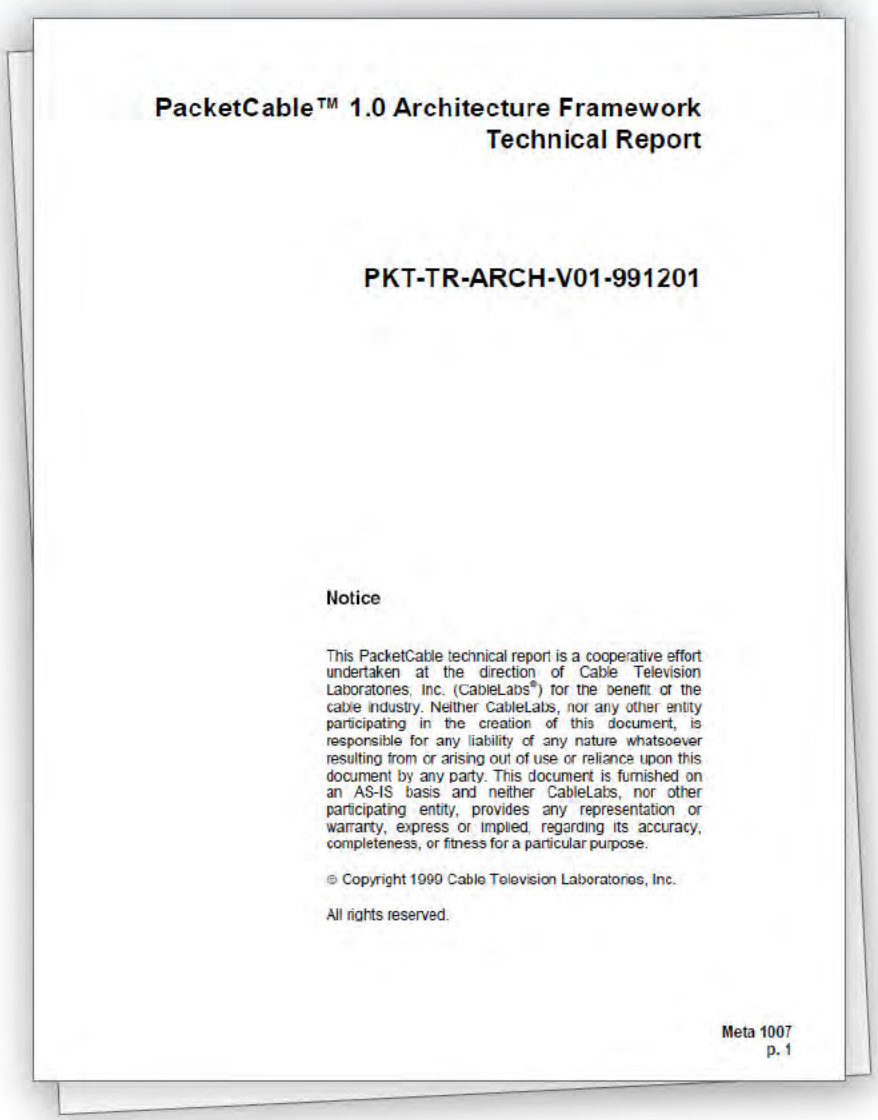
Ground II: PacketCable + Handley



"When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under § 103."

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 402 (2007).

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

Option 1: Beginning

Option 2: Middle

Option 3: End

EX1007 (PacketCable) at 1

Option 1: Beginning

Petitioners' Technical Expert Witness



Dr. Henry Houh

such as in Ethernet frames). Further, 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, and placing the authentication data at the end of the payload allows the packet to be transmitted to the network while calculating the authentication data and then adding the authentication data to the end of the payload while the packet

EX1003 (Houh Declaration) at ¶178

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

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 Declaration) at ¶152

Option 1: Beginning

Petitioners' Technical Expert Witness



Dr. Henry Houh

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 Supp. Declaration) at ¶67

Option 1: Beginning

Petitioners' Technical Expert Witness



Dr. Henry Houh

> 68. Furthermore, there can only be one header extension in an RTP packet header, so this technique cannot be used where an RTP header extension already exists. EX1008, 15 ("Only a single extension may be appended to the RTP data header."). Also, the RTP header extension is both conditional and variable length when present. *Id.*, 15 ("If the X bit in the RTP header is one, a variable-length header extension is appended to the RTP header, following the CSRC list if present."). Dr.

EX1033 (Houh Supp. Declaration) at ¶68

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

In any context, is it possible to put the MAC at the end of an RTP packet?

A So we're talking outside the scope of the -- my report in this case?

Q In general.

ATTORNEY EKLEM: Objection to form and scope.

A So outside this case -- for a protocol that's implemented, I am hesitant to say that that's where a POSITA would put a MAC. Like I keep saying, putting it in -- even in this case, but separate from the case, putting it in a fixed location in the header is -- or is the easiest way to determine the location of the MAC and the processing to location of a MAC without having to deal with variable size PDUs.

EX1031 (Stubblebine Deposition) at 234:7-22

Ground II: PacketCable + Handley

Option 1: Beginning

Petitioners' Technical Expert Witness



Dr. Henry Houh

PDUs." EX1031, 234:16-22. But this is contradictory. Put plainly, Dr. Stubblebine proposes that using the RTP header extension for the MAC avoids dealing with variable sized PDUs by proposing using the RTP header extension, which itself is variably sized and part of the PDU. In fact, Dr. Stubblebine's proposal to locate the MAC in the RTP header extension results in additional processing of variable-length data, not less. This is because using the RTP header extension introduces an additional variable-length field which was not used prior to being used for the MAC. Furthermore, packets are already variably sized – both the IP and UDP packet headers contain "length" fields. That means the variable length payload must already be dealt with and adding the MAC at the end would not result in dealing with variable size PDUs any more than is already done. But, adding an additional variable length field in the RTP does add a new variable-length field, i.e., the RTP header extension field adds more processing compared to only dealing with the variable-length IP and UDP data fields.

EX1033 (Houh Supp. Declaration) at ¶68

Ground II: PacketCable + Handley

Option 1: Beginning

Petitioners' Technical Expert Witness



Dr. Henry Houh

PDUs." EX1031, 234:16-22. But this is contradictory. Put plainly, Dr. Stubblebine proposes that using the RTP header extension for the MAC avoids dealing with variable sized PDUs by proposing using the RTP header extension, which itself is variably sized and part of the PDU. In fact, Dr. Stubblebine's proposal to locate the MAC in the RTP header extension results in additional processing of variable-length data, not less. This is because using the RTP header extension introduces an additional variable-length field which was not used prior to being used for the MAC. Furthermore, packets are already variably sized – both the IP and UDP packet headers contain "length" fields. That means the variable length payload must already be dealt with and adding the MAC at the end would not result in dealing with variable size PDUs any more than is already done. But, adding an additional variable length field in the RTP does add a new variable-length field, i.e., the RTP header extension field adds more processing compared to only dealing with the variable-length IP and UDP data fields.

EX1033 (Houh Supp. Declaration) at ¶68

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

> 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 Declaration) at ¶150.

Option 1: Beginning

Petitioners' Technical Expert Witness

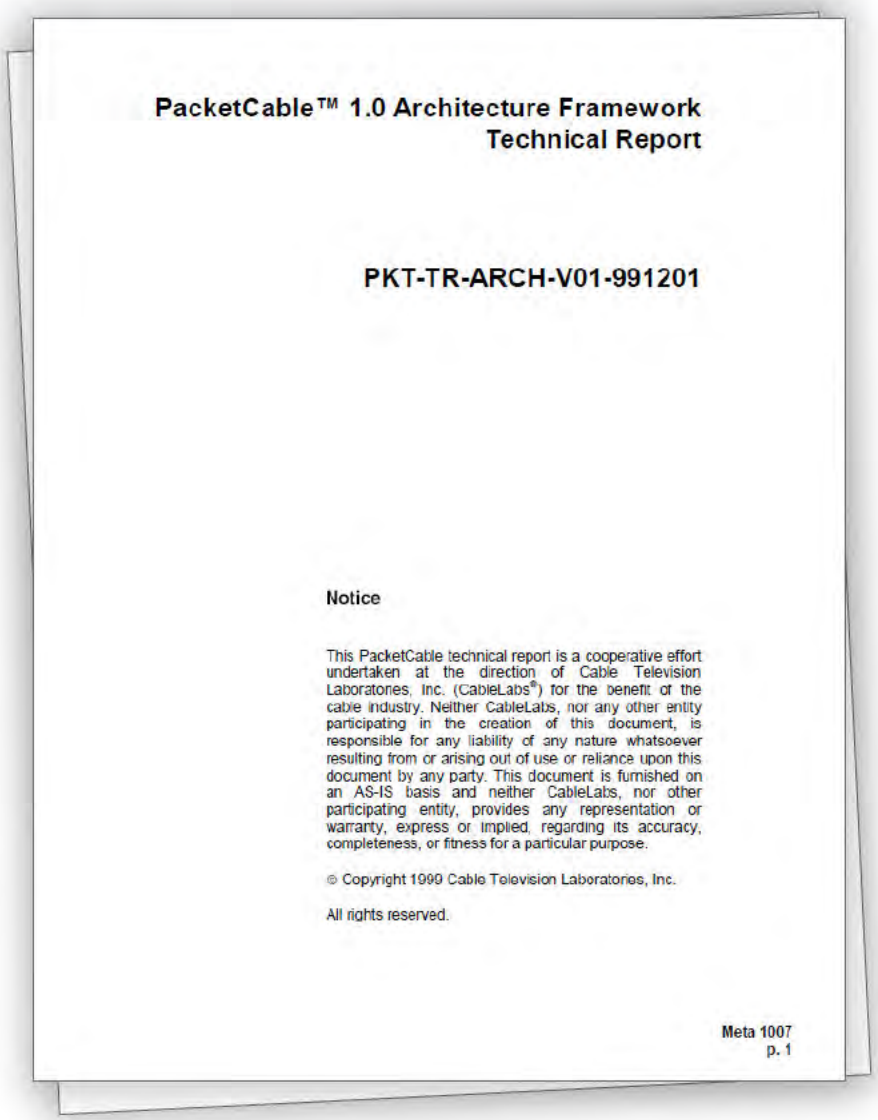


Dr. Henry Houh

comments about where if it wasn't in the header." EX1031, 219:3-13. But placing the MAC in the RTP header using the RTP header extension uses a variable length field, causing the RTP header to become a different length than normal, so it is not fixed length. And as I discuss above, IP and UDP packets are already variable length, so putting the MAC at the end does not use any more resources. This is because the end of the packet already has to be determined to know where the data ends, and knowing that the data ends with the MAC uses fewer computational resources than adding a variable-length RTP header extension at the end of the RTP header but before the data.

EX1033 (Houh Supp. Declaration) at ¶69

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

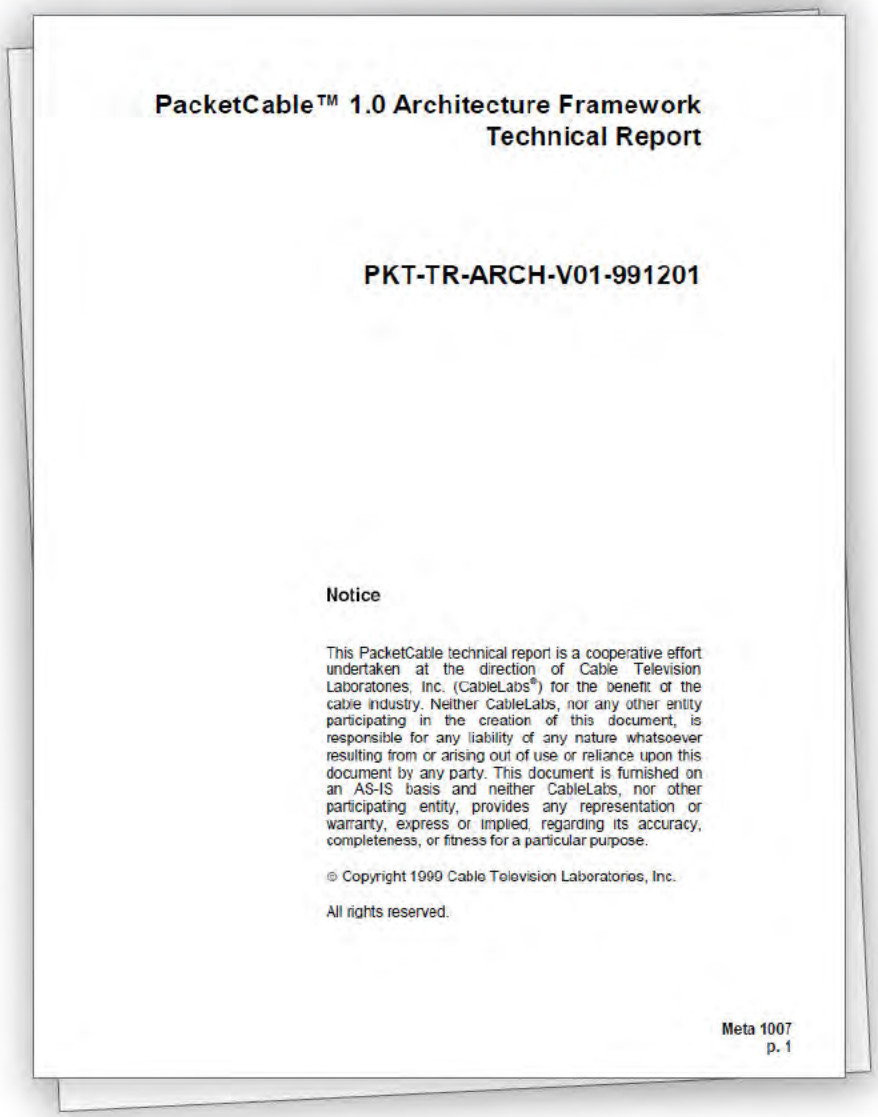
Option 1: Beginning

Option 2: Middle

Option 3: End

EX1007 (PacketCable) at 1

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

~~Option 1: Beginning~~

Option 2: Middle

Option 3: End

EX1007 (PacketCable) at 1

Option 2: Middle

Petitioners' Technical Expert Witness



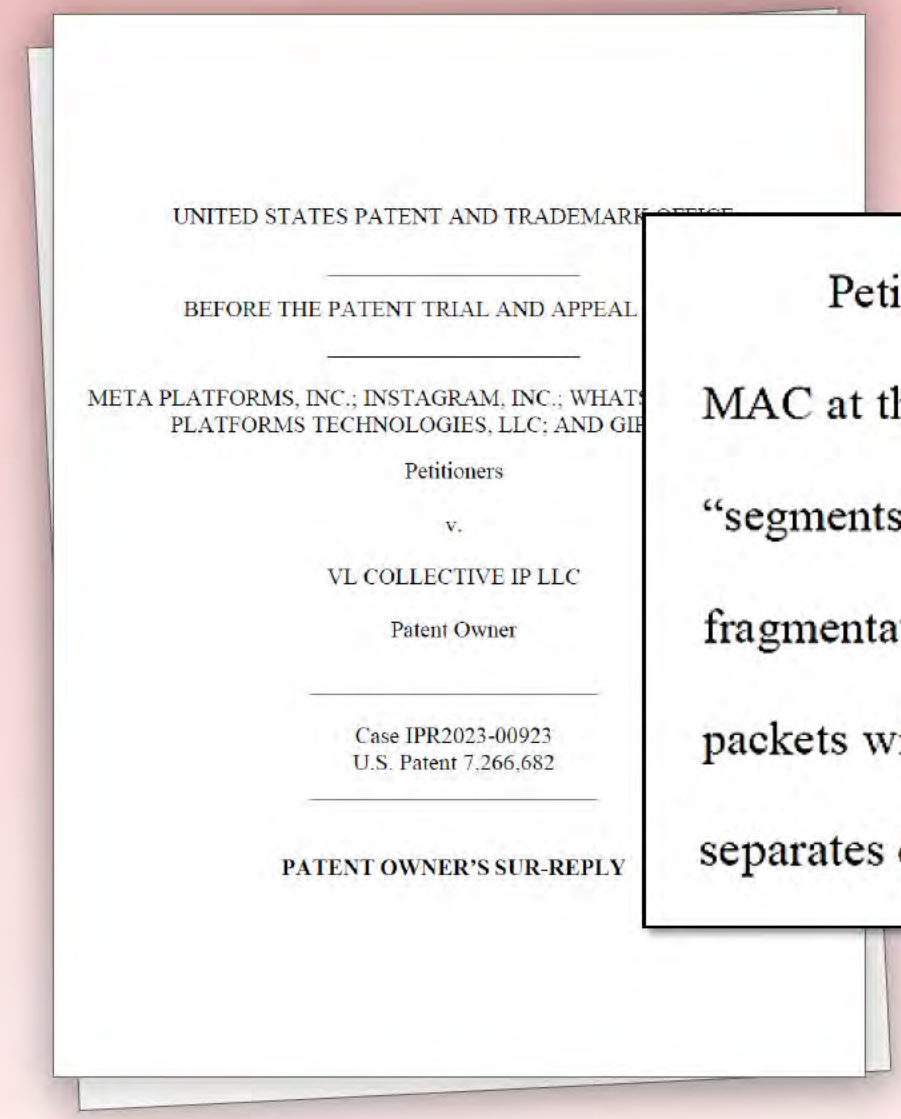
Dr. Henry Houh

178. 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, since the data in the packet would be interrupted by the authentication data, and extra data fields would be needed to identify the exact location of the authentication data within the packet data. As such, a POSITA would have avoided such placement. 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, either in a packet header (at the beginning as ubiquitous in packets) or in packet trailer (at the end which are already present in certain types of packets such as in Ethernet frames). Further, a POSITA would have understood that the

EX1003 (Houh Declaration) at ¶178

Ground II: PacketCable + Handley

Option 2: Middle



UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATS
PLATFORMS TECHNOLOGIES, LLC; AND GI

Petitioners

v.

VL COLLECTIVE IP LLC

Patent Owner

Case IPR2023-00923
U.S. Patent 7,266,682

PATENT OWNER'S SUR-REPLY

Petitioners claim to have identified fragmentation issues that favor locating a MAC at the end of an RTP packet. Reply 21. They did not. Separating data into "segments" *within a packet* by placing a MAC between them is not packet fragmentation. EX1009, 43-44 (fragmentation results in the generation of multiple packets with their own headers); EX2010, 145:21-146:3, 147:16-20 (segmentation separates data within a single packet).

PO Sur-Reply (Paper 44) at 23-24

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



Dr. Henry Houh

Option 2: Middle

63. When Dr. Stubblebine referred to "fragmentation" at his cross-examination, he appears to be limiting his view of "fragmentation" to the very specific issue of link fragmentation. *See, e.g.*, EX1031, 218:10-228:9. Link fragmentation in a network occurs when a packet exceeds the Maximum Transmission Unit ("MTU") of a link over which the packet is transmitted. For example, if the MTU of a particular link in the network is 512 bytes, and a packet is 1500 bytes, the packet must be fragmented in three units in order to be transmitted over a link. Thus, Dr. Stubblebine appears to be emphasizing and limiting his use of "fragmentation" to this scenario by focusing on the small sizes of packets. All to the exclusion of other forms of fragmentation.

EX1033 (Houh Supp. Declaration) at ¶63

Ground II: PacketCable + Handley

Option 2: Middle

Petitioners' Technical Expert Witness



Dr. Henry Houh

65. Furthermore, when Dr. Stubblebine was asked if he was familiar with the term "disk fragmentation" he said that he understood it to mean that the data in a file is stored in non-contiguous sectors on a disk: "Q. Have you ever heard of disk fragmentation? A Which? Q Disk fragmentation? ... A Like hard disk? Q. Sure. A. Yes. Q. And what is that? A. That's not something I opined on. Q. But you're familiar with it? A. I have some familiarity with it. Q. What is that general familiarity? A. There is read/write sectors on a disk, and sometimes content is distributed on have to search on multiple sectors to retrieve the entire file. Multiple noncontiguous sectors." EX1031, 220:80-229:6. Dr. Stubblebine agrees that fragmented can mean

EX1033 (Houh Supp. Declaration) at ¶65

Petitioners' Technical Expert Witness



Dr. Henry Houh

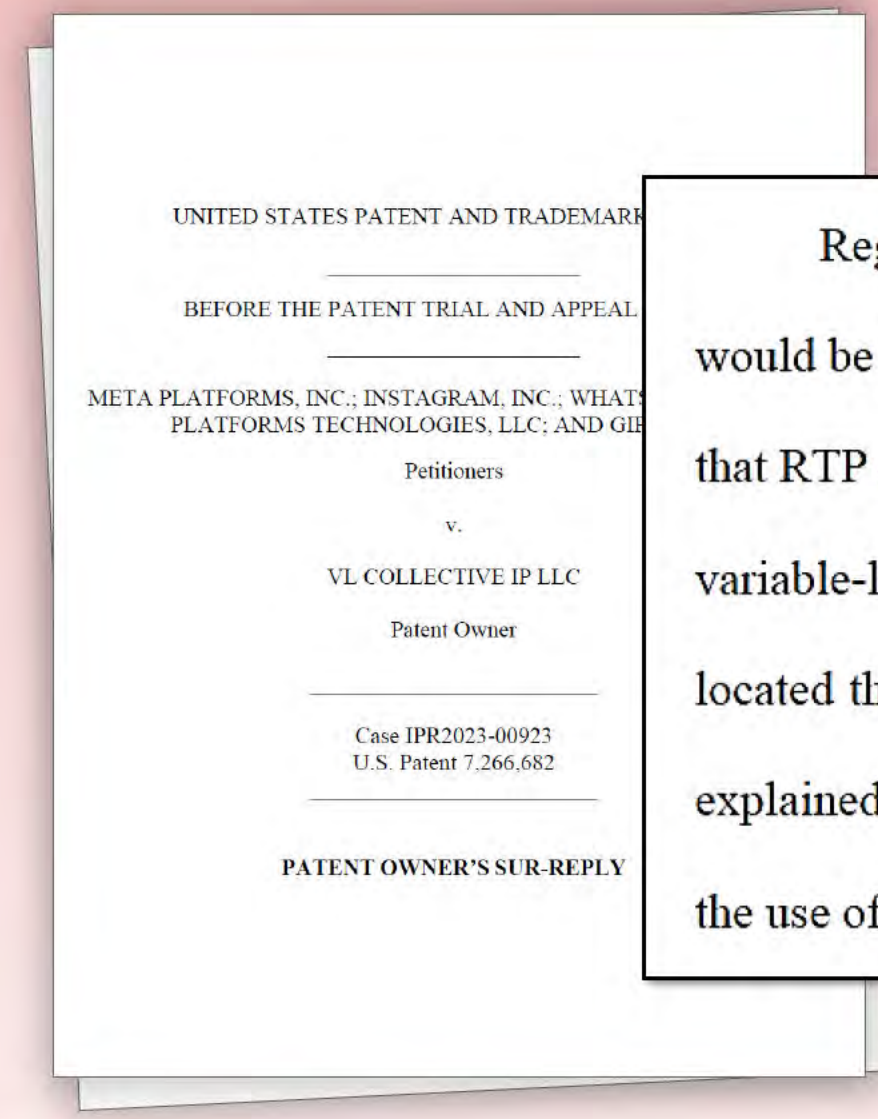
Option 2: Middle

sectors." EX1031, 220:80-229:6. Dr. Stubblebine agrees that fragmented can mean non-contiguous in the context of a disk drive. That is the sense of fragmentation as I discuss in my declaration, applied to data within a packet. When the MAC is put in the middle of a data section of the packet, it separates the data (that was originally contiguous in the packet) into two non-contiguous sections within a packet. Dr. Stubblebine appears to have an understanding of the word "fragmentation," but he chooses to re-interpret my declaration's use of "fragmentation" into his own narrow "link fragmentation" sense.

EX1033 (Houh Supp. Declaration) at ¶65

Ground II: PacketCable + Handley

Option 2: Middle



UNITED STATES PATENT AND TRADEMARK

BEFORE THE PATENT TRIAL AND APPEAL

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATS
PLATFORMS TECHNOLOGIES, LLC; AND GI

Petitioners

v.

VL COLLECTIVE IP LLC

Patent Owner

Case IPR2023-00923
U.S. Patent 7,266,682

PATENT OWNER'S SUR-REPLY

Regardless, Petitioners have not shown that their "performance" impacts would be avoided by locating the MAC at the end of an RTP packet payload, given that RTP does not define a trailer (as petitioners concede), and the RTP payload is a variable-length field, which would require additional resources to find a MAC if located there. POR, 48-49; EX2004, ¶¶41-42, 150, 152. Moreover, Patent Owner explained why Petitioners' "benefits" arguments are incorrect and do not motivate the use of a trailer. POR, 48-51.

PO Sur-Reply (Paper 44) at 24

Petitioners' Technical Expert Witness



Dr. Henry Houh

Option 2: Middle

See e.g., EX1003, ¶178. For example, I state that "the data in the packet would be interrupted by the authentication data, and extra data fields would be needed to identify the exact location of the authentication data within the packet data" as a negative impact to performance when the MAC is placed in the middle of a packet. EX1003, ¶178. Dr. Stubblebine misses or plainly fails to acknowledge that extra data in a packet means more storage is required. Extra data in a packet also means the transmission of the packet takes longer because for a fixed transmission rate, transmitting more data requires more time. I also stated that "placing authentication

EX1033 (Houh Supp. Declaration) at ¶61

Petitioners' Technical Expert Witness



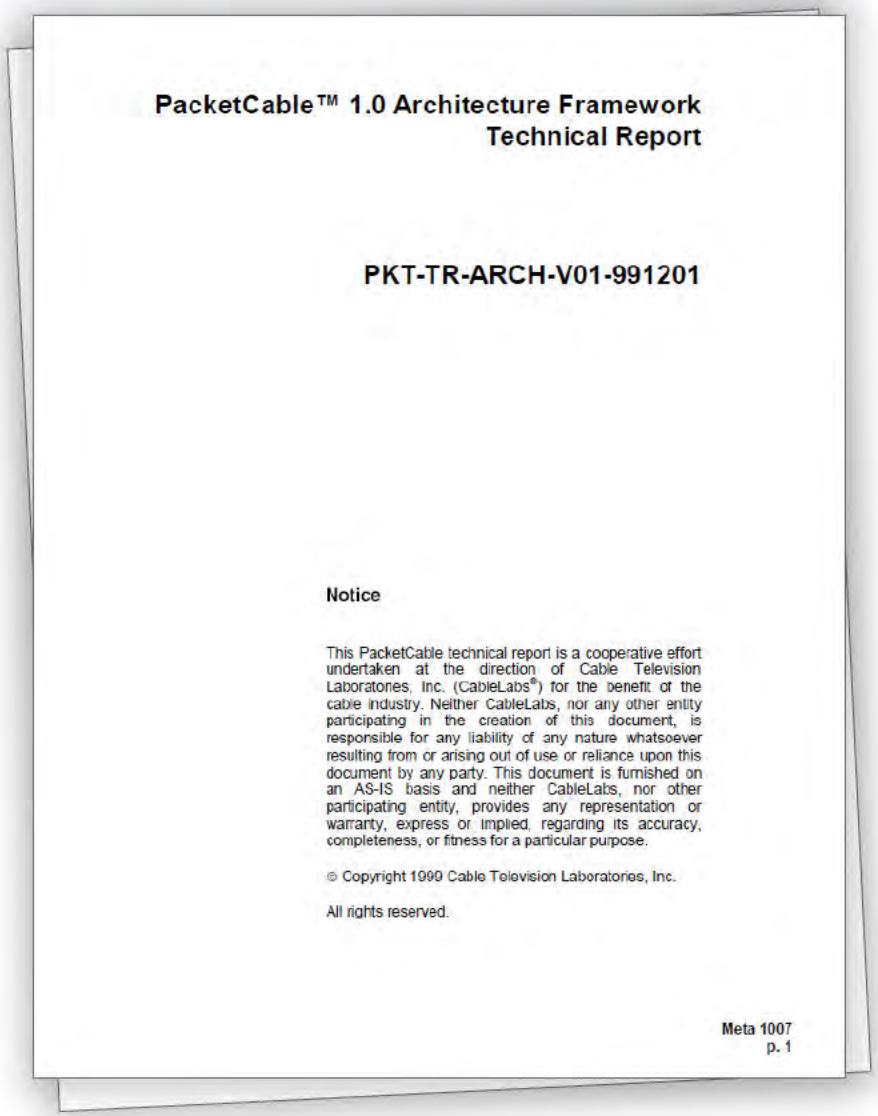
Dr. Henry Houh

Option 2: Middle

sectors." EX1031, 220:80-229:6. Dr. Stubblebine agrees that fragmented can mean non-contiguous in the context of a disk drive. That is the sense of fragmentation as I discuss in my declaration, applied to data within a packet. When the MAC is put in the middle of a data section of the packet, it separates the data (that was originally contiguous in the packet) into two non-contiguous sections within a packet. Dr. Stubblebine appears to have an understanding of the word "fragmentation," but he chooses to re-interpret my declaration's use of "fragmentation" into his own narrow "link fragmentation" sense.

EX1033 (Houh Supp. Declaration) at ¶65

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

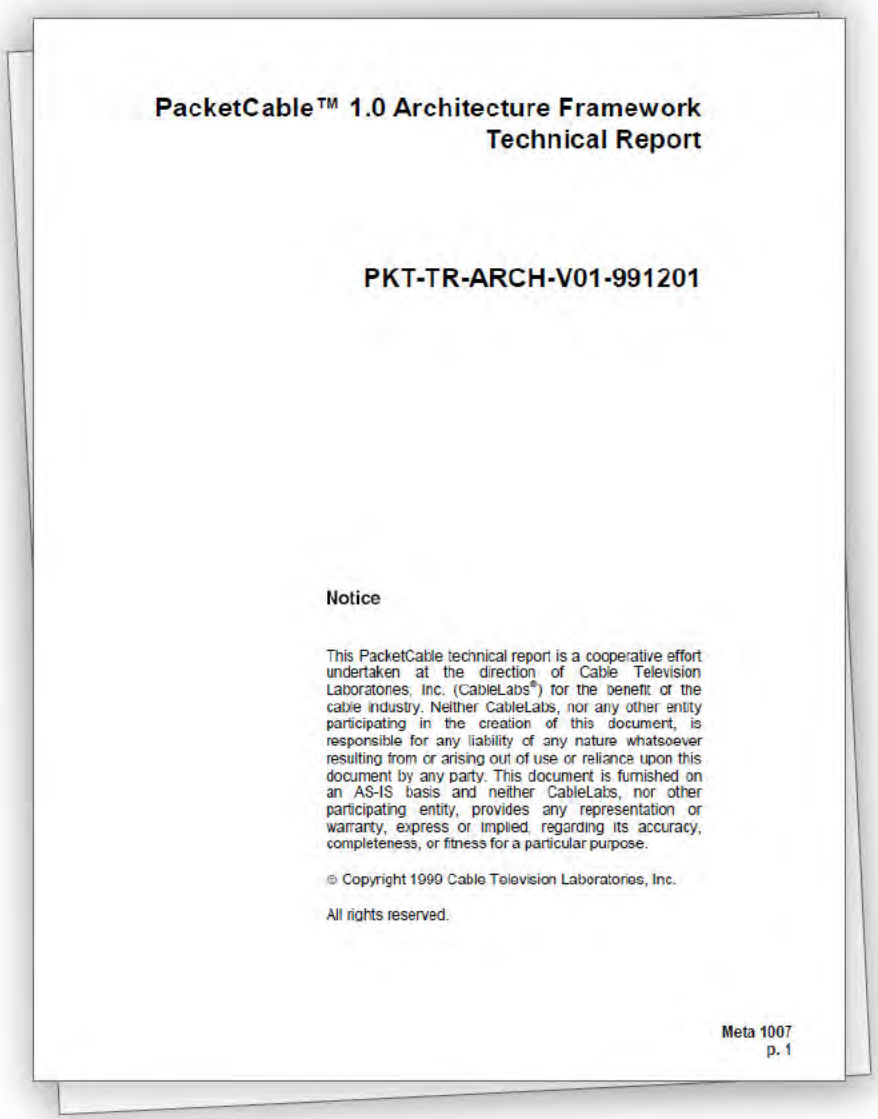
~~Option 1: Beginning~~

Option 2: Middle

Option 3: End

EX1007 (PacketCable) at 1

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

~~Option 1: Beginning~~

~~Option 2: Middle~~

Option 3: End

EX1007 (PacketCable) at 1

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



Dr. Henry Houh

Option 3: End

transmission is being completed. 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 preventing any unnecessary transmission delay by having to first compute the checksum and then transmit the payload. 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, since computations can be performed as the packet is being received. A POSITA would have appreciated that

EX1003 (Houh Declaration) at ¶178

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



Dr. Henry Houh

Option 3: End

checks. Other protocols similarly put check sequences at the end of a packet. For example, the Ethernet standard, first published in 1985, employs the same design choice reasoning to include a "Frame Check Sequence" ("FCS") at the end of the Ethernet frame so that it can be computed during transmission and appended to the end of the frame, and it can be computed upon reception to check against the FCS received and discarded if there is not a match. *See* EX1014, 43, 46, 41, 23-24, 26, 27, Fig 3-1.

EX1003 (Houh Declaration) at ¶178

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



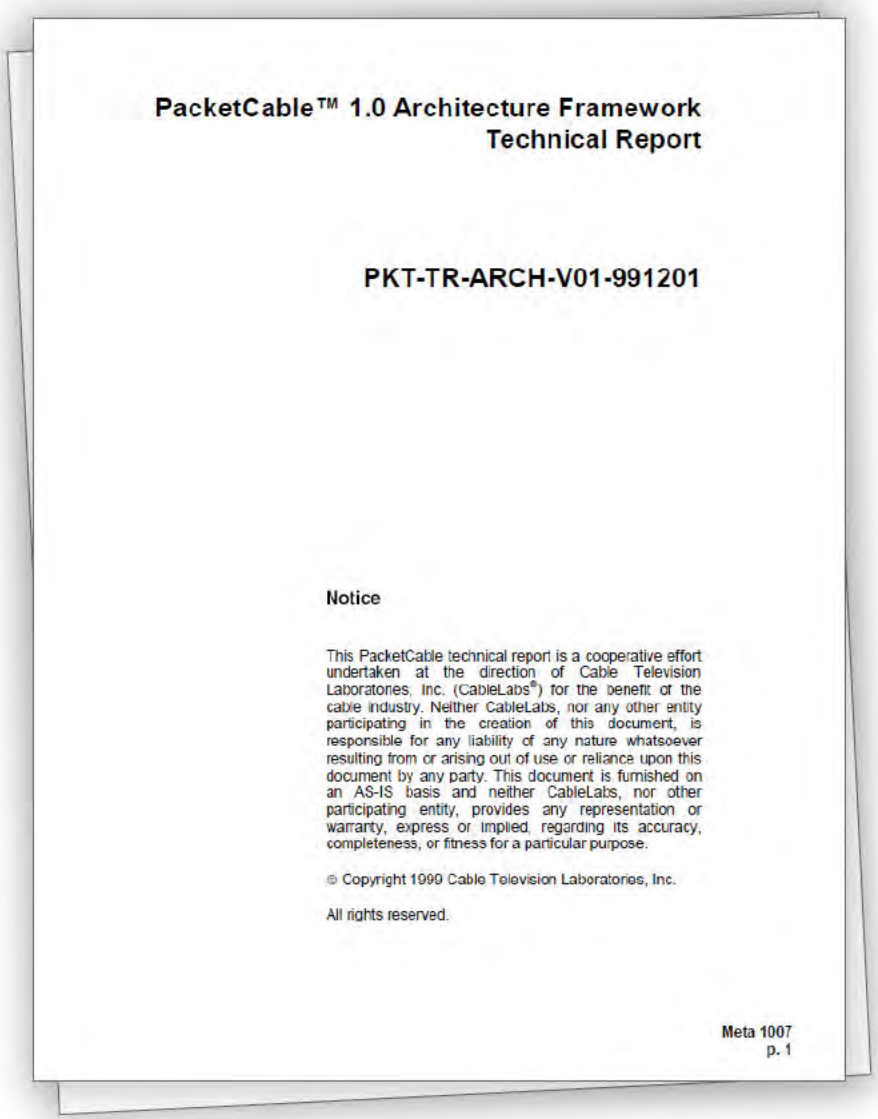
Dr. Henry Houh

Option 3: End

74. Dr. Stubblebine states that "[t]o the extent Dr. Hough [sic] is suggesting that somehow bit-by-bit processing occurs at one or more layers above the physical layer; he hasn't shown how this decreases latency in transmission at the physical layer (where transmission occurs)." EX2004, ¶161. I describe the benefits of putting the MAC at the end of a packet in my First Declaration, but I do not describe it as "bit-by-bit processing" as Dr. Stubblebine infers. *Id.* In my First Declaration, I describe performance benefits that include reducing the latency to transmit packets. *See* EX1003, ¶178. I also further explain the reasons above in Section IV.A-C and incorporate that analysis here. *See* § IV.A-C, *supra*.

EX1033 (Houh Supp. Declaration) at ¶74

Ground II: PacketCable + Handley



PacketCable™ 1.0 Architecture Framework
Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

There are only a finite number of places to place authentication in a packet:

~~Option 1: Beginning~~

~~Option 2: Middle~~

Option 3: End ✓

EX1007 (PacketCable) at 1

Ground II: PacketCable + Handley

Claim 1, ’682 Patent	
Preamble [1]	A method for transmitting data from a transmitter to a receiver, comprising:
Element [1.1]	providing transmitter-to-receiver authentication at a Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer
Element [1.2]	by inserting, at the transmitter, authentication data at end of a whole RTP packet payload;
Element [1.3]	ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data; and
Element [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 (US 7,266,682) at Claim 1

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



Dr. Henry Houh

Further, as discussed in Ground I, Elements [1.1] and [1.3], a POSITA would have understood that a receiver knows whether the transmitter is using symmetric or asymmetric encryption. If using symmetric key encryption, the transmitter and receiver will exchange secret keys prior to data transmission so the transmitter can use the secret key to encrypt the data, and the receiver can use the secret key to decrypt the data. *PacketCable* states that "[k]eys for the encryption and MAC calculation are derived from the End-End secret, which is exchanged between sending and receiving MTA as part of the call signaling." EX1007, 47. *PacketCable* discloses that a secret key is "the cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key." *Id.*, 66. A POSITA would have understood and found obvious that a receiver MTA knows the shared secret key, which it then uses with the received message to see if the computed MAC matches the MAC received from the transmitter MTA.

EX1003 (Houh Declaration) at ¶182

Ground II: PacketCable + Handley

Dependent Claims 22 and 24, ’682 Patent	
Claim 22	The method as claimed in claim 21, wherein the receiver and transmitter are each disposed in at least one of a switching node and a switching installation.
Claim 24	The method as claimed in claim 23, wherein the receiver and transmitter are each disposed in at least one of a switching node and a switching installation.

EX1001 (US 7,266,682) at Claims 22, 24

Ground II: PacketCable + Handley

PacketCable™ 1.0 Architecture Framework Technical Report

PKT-TR-ARCH-V01-991201

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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

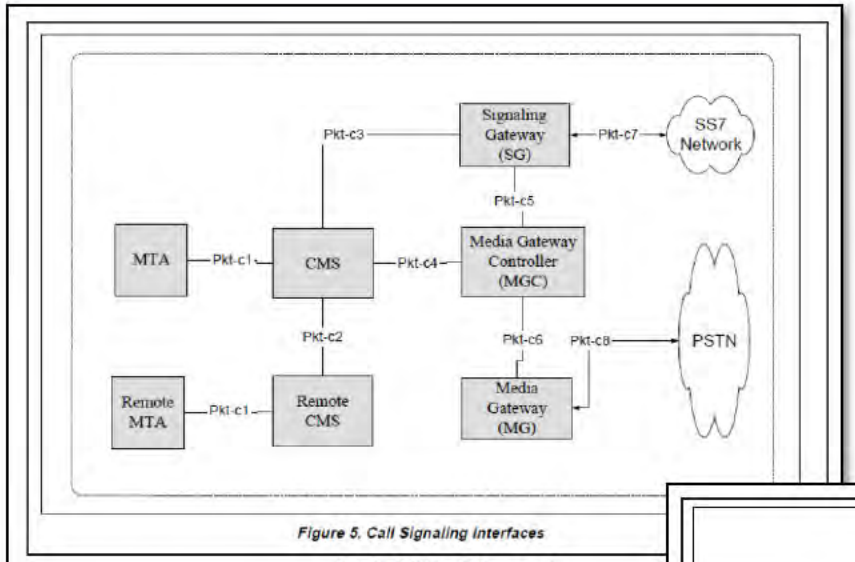


Figure 5. Call Signaling Interfaces

EX1007, Figure 5.

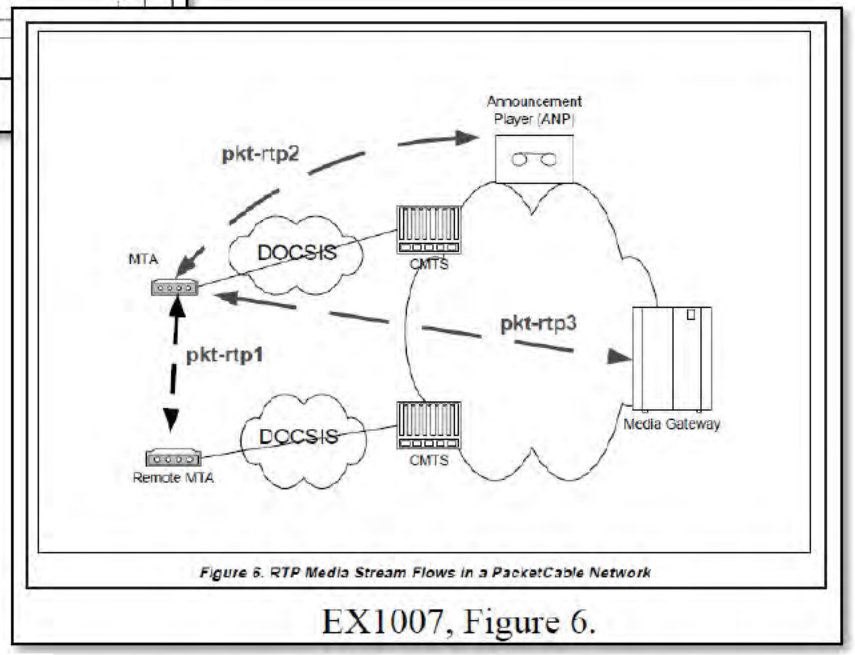


Figure 6. RTP Media Stream Flows in a PacketCable Network

EX1007, Figure 6.

EX1007 (PacketCable) at Figures 5, 6

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

167. Dr. Houh alleges that PacketCable's "media gateway" acts as a "switch," and that "[i]nclusion of a media gateway would have been obvious to a POSITA." EX1003 ¶ 224. However, Dr. Houh fails to show that PacketCable's media gateway satisfies the requirements of the "receiver" or "transmitter" of claim 1. Dr. Houh does not explain whether or how the act of switching data "between a particular IP flow and a particular PSTN port on the gateway" involves "inserting… authentication data at end of a whole RTP packet payload" (let alone "as an application protocol on an application layer") or "ascertaining, by the receiver, whether the receiver knows the transmitter based on the RTP packet level authentication data." A POSITA would have understood that IP is at a lower layer than the application layer. *See, e.g.*, EX1007 at 20.

EX2004 (Stubblebine Declaration) at ¶167.

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



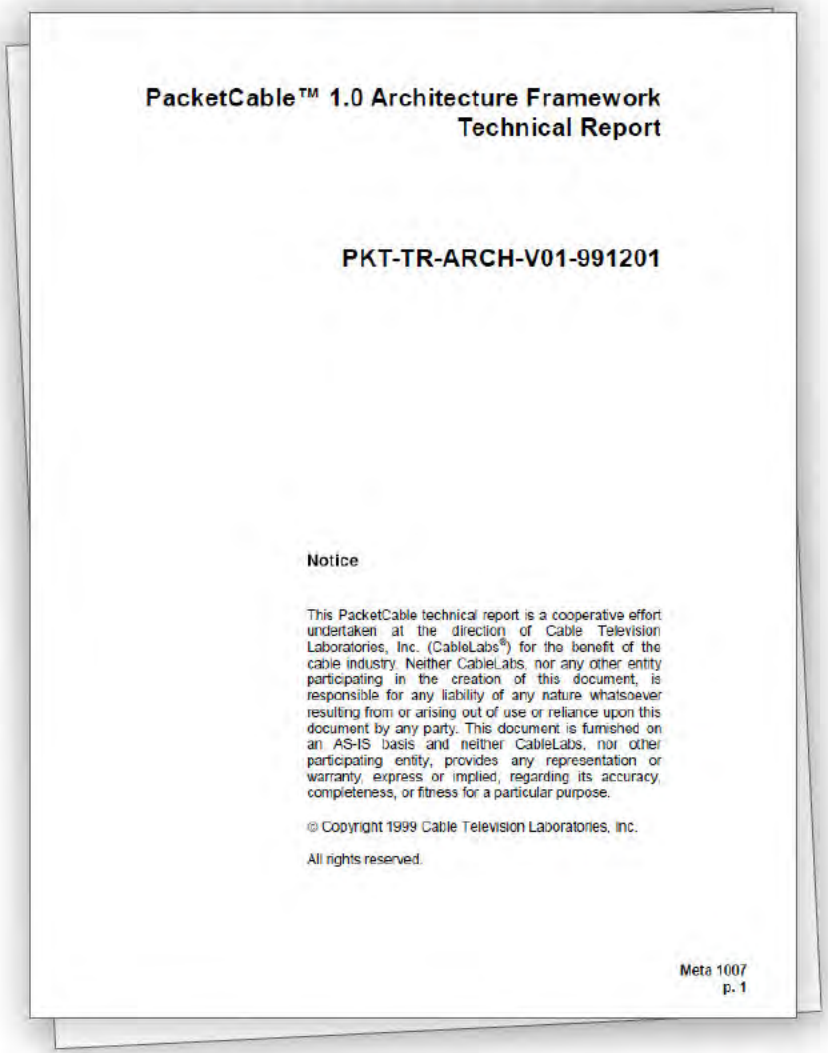
Dr. Henry Houh

packet payload'" EX2004, ¶167. I disagree. I explain in my First Declaration that a gateway "terminates the IP data side into the PSTN and ultimately acts as a switch between a particular IP flow and a particular PSTN port." EX1003, ¶224. Since the gateway terminates the IP flow, it terminates the RTP streams, and this both generates RTP packets containing data from the PSTN side of the call and receives RTP packets to convert to the PSTN format. Thus, the gateway both (1) generates RTP packets with the MAC at the end of the packet when converting call data from the PSTN into IP packets, and (2) authenticates received RTP packets by computing the MAC and comparing it to the MAC received at the end of a packet when converting call data from IP packets to the PSTN.

EX1033 (Houh Supp. Declaration) at ¶79

Ground II: Motivation to Combine PacketCable With Handley

PacketCable



PacketCable™ 1.0 Architecture Framework Technical Report

PKT-TR-ARCH-V01-991201

Notice

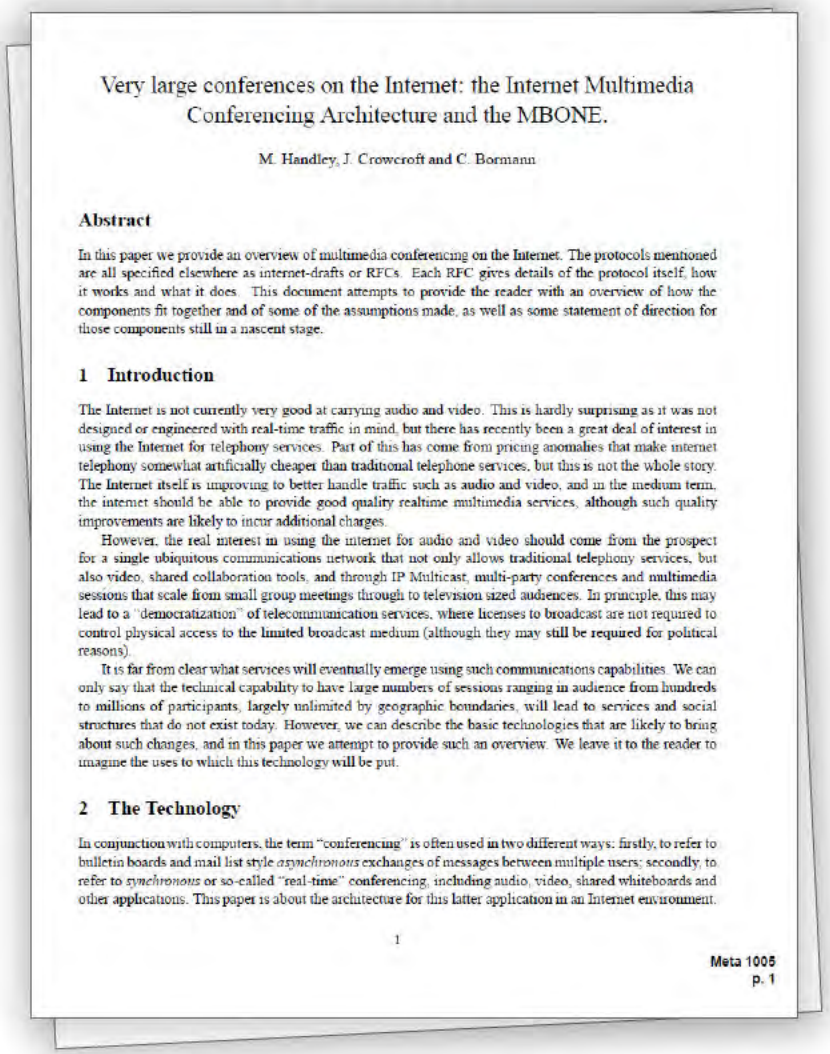
This PacketCable technical report is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of 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.

© Copyright 1999 Cable Television Laboratories, Inc.

All rights reserved.

Meta 1007
p. 1

Handley



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

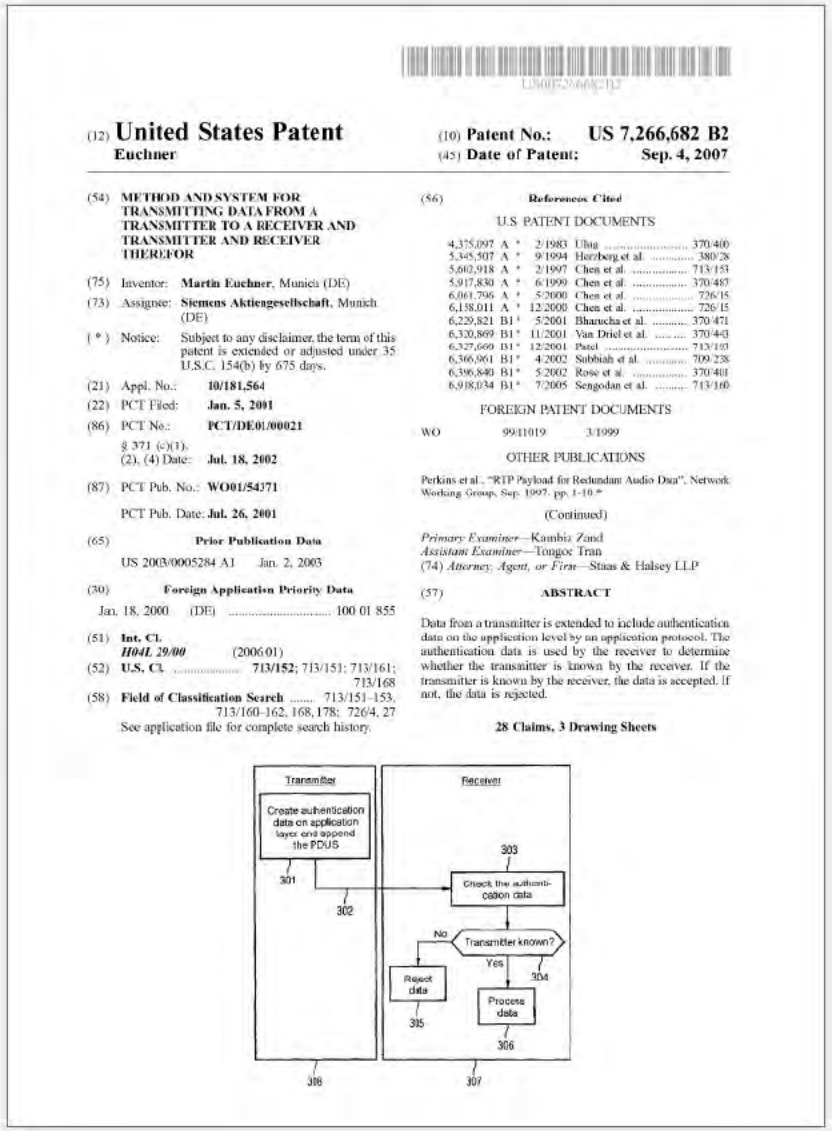
In conjunction with computers, the term "conferencing" is often used in two different ways: firstly, to refer to bulletin boards and mail list style *asynchronous* exchanges of messages between multiple users; secondly, to refer to *synchronous* or so-called "real-time" conferencing, including audio, 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

EX1007 (PacketCable) at 1; EX1005 (Handley) at 1

Overview



(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(b) 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 Uhra 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

1. Background
2. Prior Art
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. **Grounds**
   a. Ground I
   b. Ground II
   c. **Ground III**
   d. Ground IV

Invalidity Grounds

Ground I (Claims 1-21, 23, 25-28)

- Obvious under § 103 in view of Handley in combination with Basturk

Ground II (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Handley

Ground III (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Basturk

Ground IV (Claims 22, 24)

- Obvious under § 103 in view of Handley in combination with Basturk and PacketCable

Ground II: PacketCable + Handley

Patent Owner's Technical Expert Witness



Dr. Stuart Stubblebine

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

EX2004 (Stubblebine Declaration) at ¶173.

Ground II: PacketCable + Handley

Petitioners' Technical Expert Witness



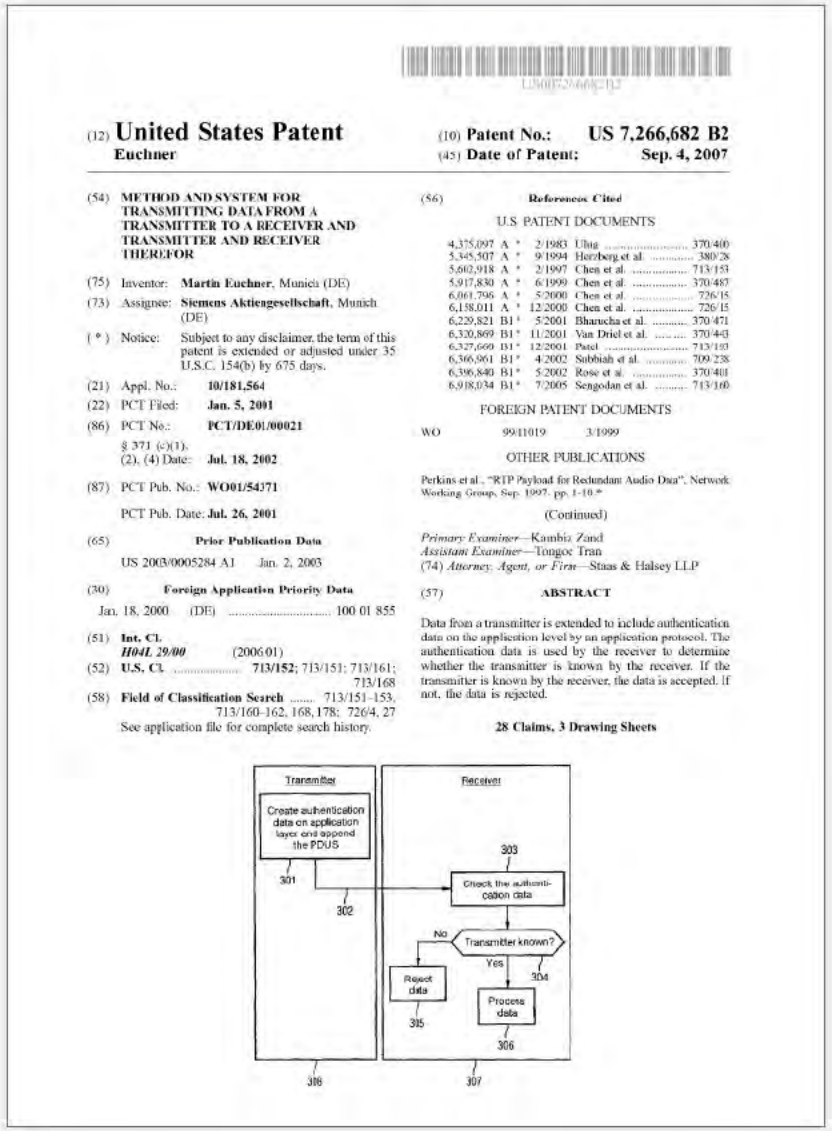
Dr. Henry Houh

> I think the paper is inaccurate when it comes to it describing latency benefits. And it essentially admits it right here when it says, "Immediately availability when transmit." So now, elsewhere in the paper, there is no issue of -- of -- elsewhere in the paper, there is supposedly an issue of latency for context retrieval. But now there isn't any for transmission. And for the same reasons there isn't any latency for transmission, there is also no latency for reception. And the reason being is, if you look -- at least one reason -- if you look at the context of -- of Basturk, it's using authenticated key exchange protocol. And this is a protocol where parties communicate to establish a key. And when that occurs, both a sender and receiver have a key in memory. And when the next packet happens, there is no context retrieval. There is -- the key is immediately available. Even if you want to call that "context retrieval," it's nothing. It's insignificant. It's already in memory.

EX1031, 148:9-149:13; *see also Id.*, 146:11-147:7. Dr. Stubblebine admits that context is immediately available on both transmission and reception, which directly contradicts his statements that "the delay associated with context retrieval would be unavoidable in PacketCable, meaning that 'on-the-fly' cannot be achieved." EX2004, ¶177.

EX1033 (Houh Declaration) at ¶83

Overview



(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(b) 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 Uhua 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 Bharucha et al. 370/471
6,320,869 B1 * 11/2001 Van Driel et al. 370/443
6,327,669 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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

1. Background
2. Prior Art
   a. Handley (Ex. 1005)
   b. Basturk (Ex. 1006)
   c. PacketCable (Ex. 1007)
3. **Grounds**
   a. Ground I
   b. Ground II
   c. Ground III
   d. **Ground IV**

Invalidity Grounds

Ground I (Claims 1-21, 23, 25-28)

- Obvious under § 103 in view of Handley in combination with Basturk

Ground II (Claims 1-28)

- Obvious under § 103 in view of PacketCable in combination with Handley

Ground III (Claims 1-28)

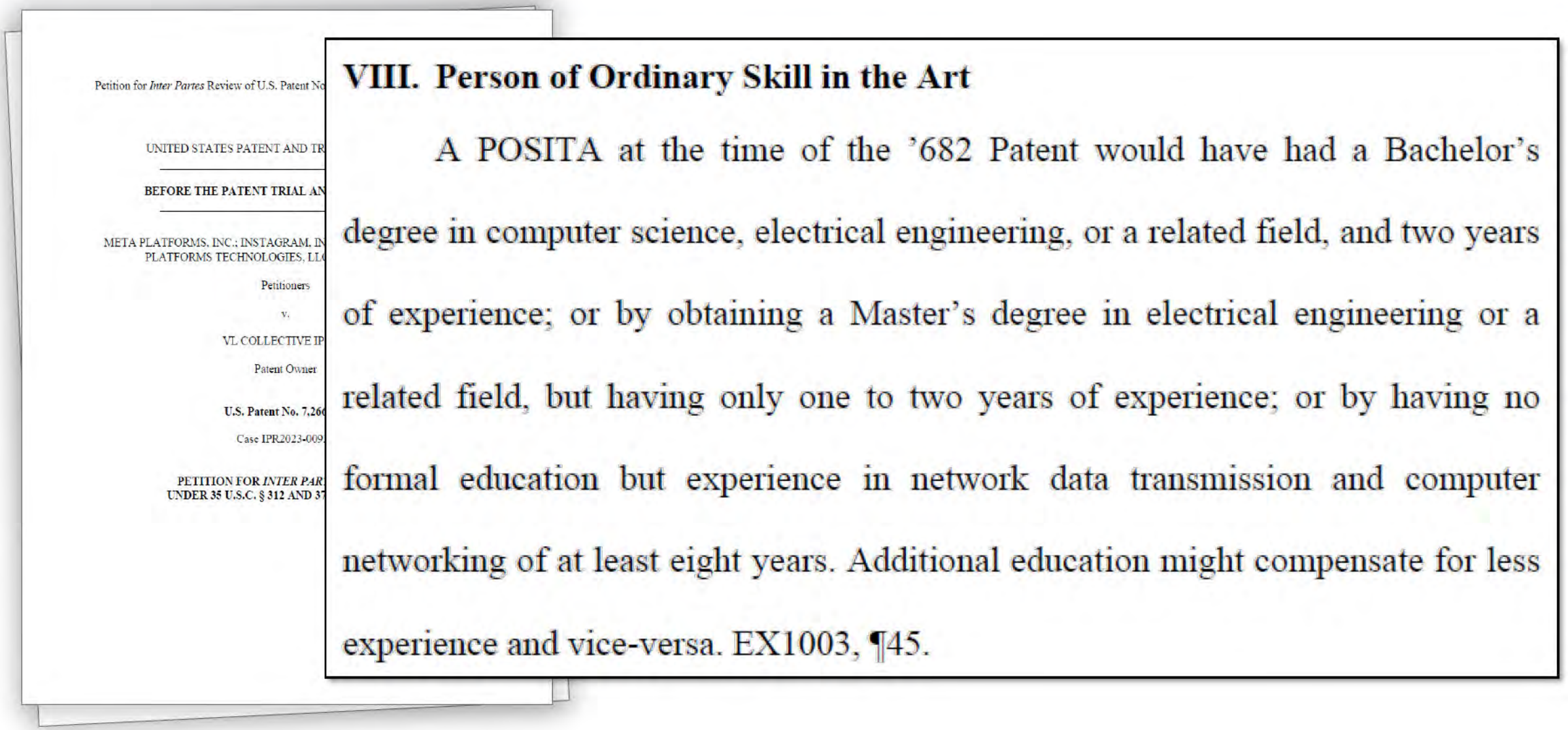
- Obvious under § 103 in view of PacketCable in combination with Basturk

Ground IV (Claims 22, 24)

- Obvious under § 103 in view of Handley in combination with Basturk and PacketCable

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Person of Ordinary Skill in the Art



Petition for *Inter Partes* Review of U.S. Patent No

UNITED STATES PATENT AND TR

BEFORE THE PATENT TRIAL AN

META PLATFORMS, INC.; INSTAGRAM, IN
PLATFORMS TECHNOLOGIES, LL

Petitioners

v.

VL COLLECTIVE IP

Patent Owner

U.S. Patent No. 7,26

Case IPR2023-009

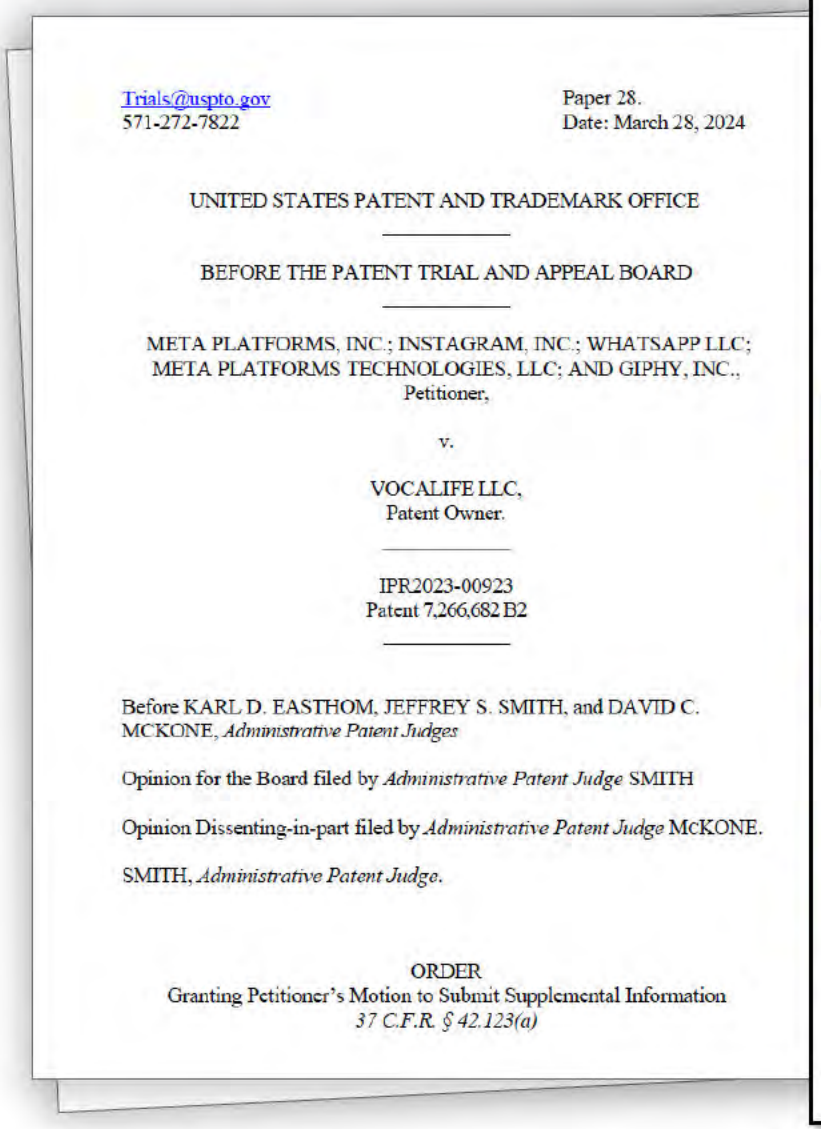
PETITION FOR *INTER PAR*
UNDER 35 U.S.C. § 312 AND 37

VIII. Person of Ordinary Skill in the Art

A POSITA at the time of the '682 Patent would have had a Bachelor's degree in computer science, electrical engineering, or a related field, and two years of experience; or by obtaining a Master's degree in electrical engineering or a related field, but having only one to two years of experience; or by having no formal education but experience in network data transmission and computer networking of at least eight years. Additional education might compensate for less experience and vice-versa. EX1003, ¶45.

Petitioner (Paper 3) at 9

Prior Art - Handley (Ex. 1005)



Trials@uspto.gov
571-272-7822

Paper 28.
Date: March 28, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC; META PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.,
Petitioner,

v.

VOCALIFE LLC,
Patent Owner.

IPR2023-00923
Patent 7,266,682 B2

Before KARL D. EASTHOM, JEFFREY S. SMITH, and DAVID C. MCKONE, *Administrative Patent Judges*

Opinion for the Board filed by *Administrative Patent Judge* SMITH

Opinion Dissenting-in-part filed by *Administrative Patent Judge* McKONE.

SMITH, *Administrative Patent Judge*.

ORDER
Granting Petitioner's Motion to Submit Supplemental Information
37 C.F.R. § 42.123(a)

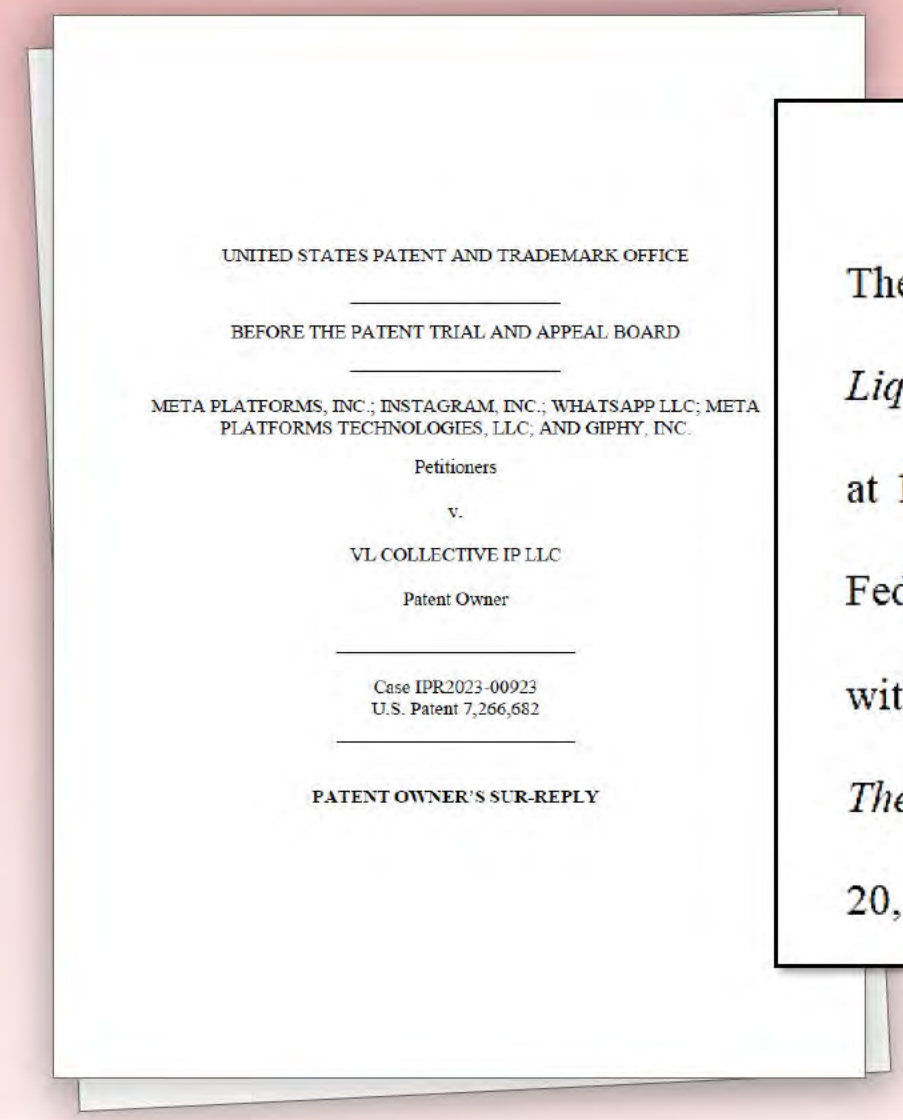
The issue here is similar to that raised in. *Liquidia,* at, where "Liquidia's IPR petition asserted that each of the Voswinckel abstracts was publicly presented or published at least one year before the priority date of the [challenged] patent, making each of them printed publications within the meaning of § 102(b)." *Liquidia*, at *4. In *Liquidia*, UTC challenged the sufficiency of the evidence for public accessibility, and Liquidia presented additional evidence in its reply under an "abstract book" theory not in the petition asserting that the abstracts were publicly presented and disseminated at a conference prior to the critical date. *Id.* at **3–4 The Board found that

. . .

The Federal Circuit held that "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." *Id.* at 8.

Order (Paper 28) at 5

Prior Art - Handley (Ex. 1005)



UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

META PLATFORMS, INC.; INSTAGRAM, INC.; WHATSAPP LLC; META PLATFORMS TECHNOLOGIES, LLC; AND GIPHY, INC.

Petitioners

v.

VL COLLECTIVE IP LLC

Patent Owner

Case IPR2023-00923
U.S. Patent 7,266,682

PATENT OWNER'S SUR-REPLY

Liquidia is distinguishable and does not support a finding of non-waiver here. The Board in *Liquidia* found the petitioner's arguments were raised in the petition. *Liquidia Technologies, Inc. v. United Therapeutics Corp.*, IPR2021-00406, Paper 78 at 10 (PTAB Jul. 19, 2022); *see id.* Paper 29 at 12-18 and Paper 44 at 2-9. The Federal Circuit agreed, stating that "Liquidia's arguments were not inconsistent with, and therefore not new over, the grounds raised in its IPR petition." *United Therapeutics Corp. v. Liquidia Techs., Inc.*, 2023 WL 8794633, at *3 (Fed. Cir. Dec. 20, 2023).

Patent Owner Sur-Reply (Paper 44) at 7

Prior Art - Handley (Ex. 1005) – Motion to Submit Supp. Info. Timeline

12/29/2023
Petitioner seeks permission to file a Motion to Submit Supp. Info.



01/04/2024
Board authorizes Petitioner to file a Motion to Submit Supp. Info.



01/18/2024
Petitioner files Motion to Submit Supp. Info.



02/13/2024
Patent Owner files opposition to Motion to Submit Supp. Info.



03/13/2024
Petitioner files Reply in support of its Motion to Submit Supp. Info.



03/28/2024
Board grants Motion to Submit Supp. Info



DECEMBER 2023 | JANUARY 2024 | FEBRUARY 2024 | MARCH 2024

Petitioners' 12/29/2023 Email to Board; Board's 01/04/2024 Email Authorization; Petitioners' Motion to Submit Supplemental Information (Paper 21); PO Opposition (Paper 25); Petitioners' Reply (Paper 27); Order (Paper 28)

Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

- Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft
- Ex. 1017 – Supp. Declaration of Dr. Henry Houh
- **Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis**
- Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof
- Ex. 1027 – Online publication version of Handley
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Prior Art - Handley (Ex. 1005) – Ex. 1018 Declaration of Dr. Hall-Ellis

Petitioners' Librarian Expert Witness



Dr. Sylvia Hall-Ellis

Dr. Hall-Ellis testified that she:

- Retrieved Ex. 1027 from Science Direct and Ex. 1028 from Kurt F. Wendt Engineering Library at the University of Wisconsin – Madison
- Found Ex. 1028 was physically published in *Computer Networks*
- Found Ex. 1027 and Ex. 1028 contain identical text
- Found Ex. 1028 to be publicly available as of February 11, 1999

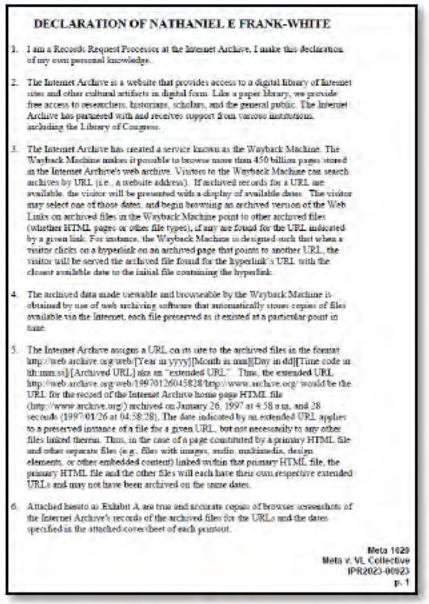
EX1018 (Hall-Ellis Declaration) at ¶¶ 37, 38, 46, 48

Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

- Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft
- Ex. 1017 – Supp. Declaration of Dr. Henry Houh
- Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis
- **Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof**
- Ex. 1027 – Online publication version of Handley
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Prior Art - Handley (Ex. 1005)



DECLARATION OF NATHANIEL E FRANK-WHITE

1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.

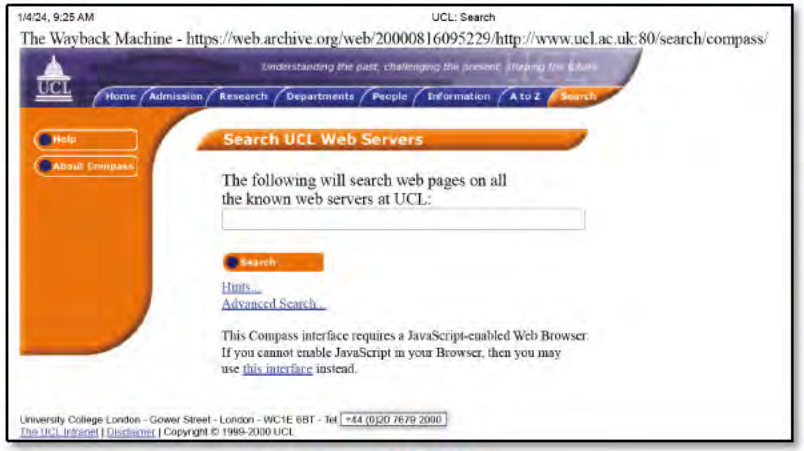
4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL], also an "extended URL." Thus, the extended URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:38 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached cover sheet of each printout.

Meta 1020
Meta v. VL Collective
IPR2023-00923
p. 1

Ex. 1020



1/4/24, 9:25 AM UCL: Search

The Wayback Machine - https://web.archive.org/web/20000816095229/http://www.ucl.ac.uk:80/search/compass/

Understanding the past, challenging the present, shaping the future

UCL

Home | Admission | Research | Departments | People | Information | A to Z | Search

Help

About Compass

Search UCL Web Servers

The following will search web pages on all the known web servers at UCL:

Search

Hints...

Advanced Search...

This Compass interface requires a JavaScript-enabled Web Browser. If you cannot enable JavaScript in your Browser, then you may use this interface instead.

University College London - Gower Street - London - WC1E 6BT - Tel +44 (0)20 7679 2000

The UCL Intranet | Disclaimer | Copyright © 1999-2000 UCL

Ex. 1021



The Wayback Machine - https://web.archive.org/web/19990210102349/http://north.east.isi.edu:80/%7Emjh/pa...

Papers, Publications and Specifications

A Thesis

On Scalable Internet Multimedia Conferencing Systems
Mark Handley
University of London PhD Thesis, Nov 1997

A Book

The World Wide Web - Beneath the Surf
Mark Handley and Jon Crowcroft
UCL Press, London, 1995, ISBN 1-85728-435-6 PB

Some Papers, Publications, and Specifications

Proxy Caching Mechanisms for Multimedia Playback Streams in the Internet
R. Rejaie, M. Handley, H. Yu, D. Estrin

Architectural Considerations for Playback of Quality Adaptive Video over the Internet
R. Rejaie, M. Handley, D. Estrin

A Dynamic Bootstrap Mechanism for Rendezvous-based Multicast Routing
D. Estrin, M. Handley, A. Helmy, P. Huang, D. Thaler
To appear in Infocom 99

RAP: An End-to-end Rate-based Congestion Control Mechanism for Realtime Streams in the Internet
R. Rejaie, M. Handley, D. Estrin
To appear in Infocom 99

Session Directories and Scalable Internet Multicast Address Allocation
M. Handley
Proc ACM Sigcomm 98, September 1998, Vancouver, Canada

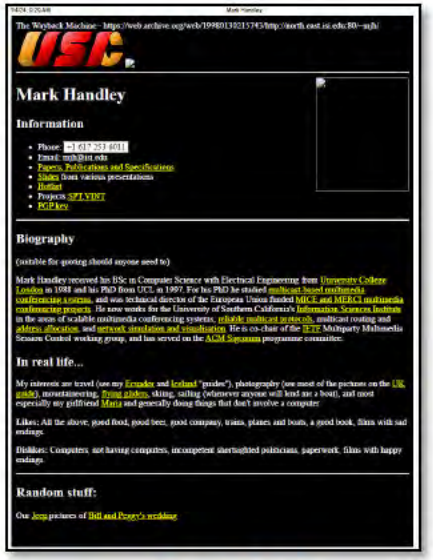
The MASC/BGMP Architecture for Inter-Domain Multicast Routing
K. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoglu, D. Estrin, M. Handley
Proc. ACM Sigcomm 98, September 1998, Vancouver, Canada

Very large conferences on the Internet: the Internet Multimedia Conferencing Architecture
M. Handley, J. Crowcroft, C. Bormann and J. Ott
To appear in Computer Networks and ISDN Systems, Special Issue on Internet Telephony

Network Text Editor (NTE): A scalable shared text editor for the MBone
Mark Handley, Jon Crowcroft,
Proceedings of ACM Sigcomm 97, Cannes, France, 1997

Meta 1022
Meta v. VL Collective
IPR2023-00923
p. 1

Ex. 1022



The Wayback Machine - https://web.archive.org/web/19980130215745/http://north.east.isi.edu:80/~mjh/

USC

Mark Handley

Information

- Phone: +1 617 253 4011
- Email: mjh@isi.edu
- Papers, Publications and Specifications
- Slides from various presentations
- Hotlist
- Projects SPI VINT
- PGP key

Biography

(suitable for quoting should anyone need to)

Mark Handley received his BSc in Computer Science with Electrical Engineering from University College London in 1988 and his PhD from UCL in 1997. For his PhD he studied multicast based multimedia conferencing systems, and was technical director of the European Union funded MICE and MERCI multimedia conferencing projects. He now works for the University of Southern California's Information Sciences Institute in the areas of scalable multimedia conferencing systems, reliable multicast protocols, multicast routing and address allocation, and network simulation and visualization. He is co-chair of the IETF Multiparty Multimedia Session Control working group, and has served on the ACM Sigcomm programme committee.

In real life...

My interests are travel (see my Ecuador and Iceland "guides"), photography (see most of the pictures on the UK guide), mountaineering, flying gliders, skiing, sailing (whenever anyone will lend me a boat), and most especially my girlfriend Maria and generally doing things that don't involve a computer.

Likes: All the above, good food, good beer, good company, trains, planes and boats, a good book, films with sad endings.

Dislikes: Computers, not having computers, incompetent shortsighted politicians, paperwork, films with happy endings.

Random stuff:

Our Jeep pictures of Bill and Peggy's wedding

Ex. 1023



The Wayback Machine - https://web.archive.org/web/19990828053320/http://www.cs.ucl.ac.uk:80/staff/jon/c...

Some of Jon's Papers - NEEDS UPDATING - Some URLs out of date!!

B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Zhang, L. Peterson, K. Ramakrishnan, S. Shenker, and J. Wroclawski "Recommendations on queue management and congestion avoidance in the internet," RFC 2309, Internet Engineering Task Force, Apr. 1998.

Fred Baker, Jon Crowcroft, Roch Guerin, Henning Schulzrinne, and Lixia Zhang. "Reservations short reservations," in *Proc. of IEEE Fifth International Workshop on Quality of Service (IWQOS 97)*, (New York, NY), May 1997.

Tony Ballardie, Paul Francis, and Jon Crowcroft, "Core based trees (CBT)," in *SIGCOMM Symposium on Communications Architectures and Protocols* (Deepinder P. Sidhu, ed.), (San Francisco, California), pp. 85-95, ACM, Sept. 1993. also in Computer Communication Review 23 (4), Oct. 1992. Path version

Tony Ballardie, Jon Crowcroft, "Multicast-Specific Security Threats and Counter-Measures in ISOC Conference on Security, 1995.

K. Carlberg and J. Crowcroft, "Building shared trees using a one-to-many virtual mechanism," *ACM Computer Communication Review*, vol. 27, pp. 3-11, Jan. 1997.

S. Chiang, Jon Crowcroft, S. Hailes, M. Handley N. Ismail, D. Lewis, and Ian Wakeman, "Multimedia application requirements for multicast communications services," in *Proceedings of the International Networking Conference (INET)*, (San Francisco, California), pp. IFB-1 - IFB-8, Internet Society, Aug. 1993.

B. Carpenter, J. Crowcroft, and Y. Rekhter, "IPv4 address behaviour today," Request for Comments (Informational) 2101, Internet Engineering Task Force, Feb. 1997.

Jon Crowcroft and M d'Inverno, "Test Based Real Time Computer Conferencing Specification, Design and Implementation," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, vol. 2, pp. 1114-1126, Apr. 1991.

Schulzrinne & Crowcroft.
href="http://www.research.att.com/jac/report/jsac13.8/guestedit/abs_guestedit.html">"Guest editorial: The global Internet," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 1366-1369, Oct. 1995.

J. Crowcroft, H. Fuchs, T. Turletti, A. Ghosh, Z. Wang, L. Vicisano, and C. Thot "RMFP: a reliable multicast framing protocol," Internet Draft, Internet Engineering Task Force, Mar. 1998. Work in progress.

J. Crowcroft and J. Onions, "Network time protocol (NTP) over the OSI remote operations service," Request for Comments (Experimental) 1165, Internet Engineering Task Force, June 1990.

J. Crowcroft and M. Ohta, "Static multicast," Internet Draft, Internet Engineering Task Force, Mar. 1998. Work in progress.

J. Crowcroft and K. Paliwoda, "A multicast transport protocol," in *SIGCOMM Symposium on Communications Architectures and Protocols*, (Stanford, California), pp. 247-256, ACM, Aug. 1988. also in em Computer Communication Review 18 (4), Aug. 1988.

Jon Crowcroft, "International Internetworking," *CommUNIcate - The InteroperabiUty Report*, vol. 2, p. Published by Advanced Computing Environments, Apr. 1991.

Meta 1024
Meta v. VL Collective
IPR2023-00923

Ex. 1024



The Wayback Machine - https://web.archive.org/web/20010217183731/http://www.cs.ucl.ac.uk:80/darpa

Index of /darpa

```
BTNORKSHOP.PPT - slides about  winsock stack management
CLOSECOM96-mcast.tex - about multicasting proceedings of nov 96 IEEE Globecom
GLOBECOM96-mcast.ps
IDMR/  - archives for IETF Working Group on Inter Domain Multicast Routing
README - this file
atm-cbr-tcp.ps.Z - draft about expected  TCP behaviour on different ATM bearer service classes
atm-congestion-mail-sample.2 - email e ATM forum about congestion
atm-end-cut-test.Sel_rep.ps.Z - report on some ATM NIC tests at UCL
atmf-ietf.doc - comparison of traffic service models for ATM and Internet
atmf-ietf.ps.Z
bulk.ps - A Draft about a multicast reliable bulk transfer protocol
bulk.ps.2
button.gif
button.ps
cats.ps - paper about sending CATS and modelling the Internet
cbq-slides.ps.Z - Slides Based Queuing wQoS at UCL
cbr-cbr-tcp.ps.Z - more notes about TCP and ATM bearer service classes
ccco-sigcom95.ps.Z - (Multimedia realtime) Conference Control Channel Protocol
ccco.ps.Z
ccco.tar.Z
charging.ps.gz - some ideas on billing.
chen2.gif
confarch.ps - a note on conference control protocol architectures
control.tar
core-dumps
dvcpmp.ps - a paper about the future prospects of the Internet
dvcpmp.ps.Z
dvr.ps.Z - a draft about protocols for distributed VR
entables.ps - a note about a network text editor
floorcoc-multimedia.ps.Z
fmulti.gif
gaga.shar - a Generic Algorithm for Genetic Algorithms
globecom-tree.ps - a different version of the Globecom report
globecom1.5.gif
globecom2.5.ps
globecom2.5.ps.gz
globecom3.5.gif
h221_encoder.tar.Z - an H221 Framing Implementation
hipl.ps - first deliverable from HIPPARCH project
ieee-collaborative-pride.txt - another draft on network pricing
ieee-telecommunications95-journal.ps.Z - a note about the Internet
ieeearticle.ps.Z - a different note about the Internet
ieee-communications-isp-priv.ps.gz - a note about ISPs
iccc-nets-pwhite.ps.Z - a paper about RSVP
iccc-tos95-ch4.ps.Z a paper about Core Based Tree style multicast routing
internetmmconvergence - more html notes about IP and ATM service models
isp-atmm.ps.Z - what is new about ATM
isp-atmp.ps.Z - what is on about ATM
ip-atm.txt - a report about how ATM did not work at all well for IP
ipc-conf.ps
ipj-cent.ps - paper about state of multicast in 1999
isdn-mbone-report.ps - using ISDN for the Mbone
janetvid.ps.Z - experiences with video over the JANET netwrk
jbvcast.tar.Z - casting java...
jntvid1.ps.Z
jntvid2.ps.Z
jpd - paul dourish's thesis.
jsac-group.ps.Z
```

Ex. 1025



The Wayback Machine - https://web.archive.org/web/19981203112130/http://www.cs.ucl.ac.uk:80/staff/jon/

Jon Crowcroft

contact

Phone (DDI): +44 171 380 7296
Fax: +44 171 387 1397
Email: J.Crowcroft at cs.ucl.ac.uk

(this "here", as always, is under decommission)

projects

- BT final Management of Multiservice Networks (mom) and earlier one mobwells, MMPM/TEW, MANIC, MCHB and Layered Infrastructure.
- Esprit HIPPARCH, High Performance Protocol Architectures, had 3 workshops in June 1995.
- ACTS CESAS, COnvergence Internet-ATM-Satellite
- Ranging also final x.desc emailing project in the department.
- Nimbus (UK and Canada) also finals some Internet Telephony and IETF activities.
- IIP final UNIS and Saleem Bhatti's work on QPDANA under the Internet Research Institute
- The EU ACTS Project, Flowthru
- A DARPA funded project on multicast multimedia and multiservices.
- Mmetrics on Mobile Qos
- Some Past Projects

Next year IEEE JWOS is at UCL, which should be interesting. I keep a list of various calls for papers, while a list of papers are on our ftp server, while some of mine are getable via Houssine Sellimi-ssn's excellent online bibliography

teaching

undergraduate

- IM10 - Computer Architectures based mainly on Patterson&Hennessy.

trends mm 98/99 timetable, (alumni, see here)

- TS9

telecoms mm and mmcn & timetable and modules

- data networks & protocols
- distributed systems for beginners* Additional notes on objects, java, corba and multicast

Meta 1026
Meta v. VL Collective
IPR2023-00923

Ex. 1026

Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

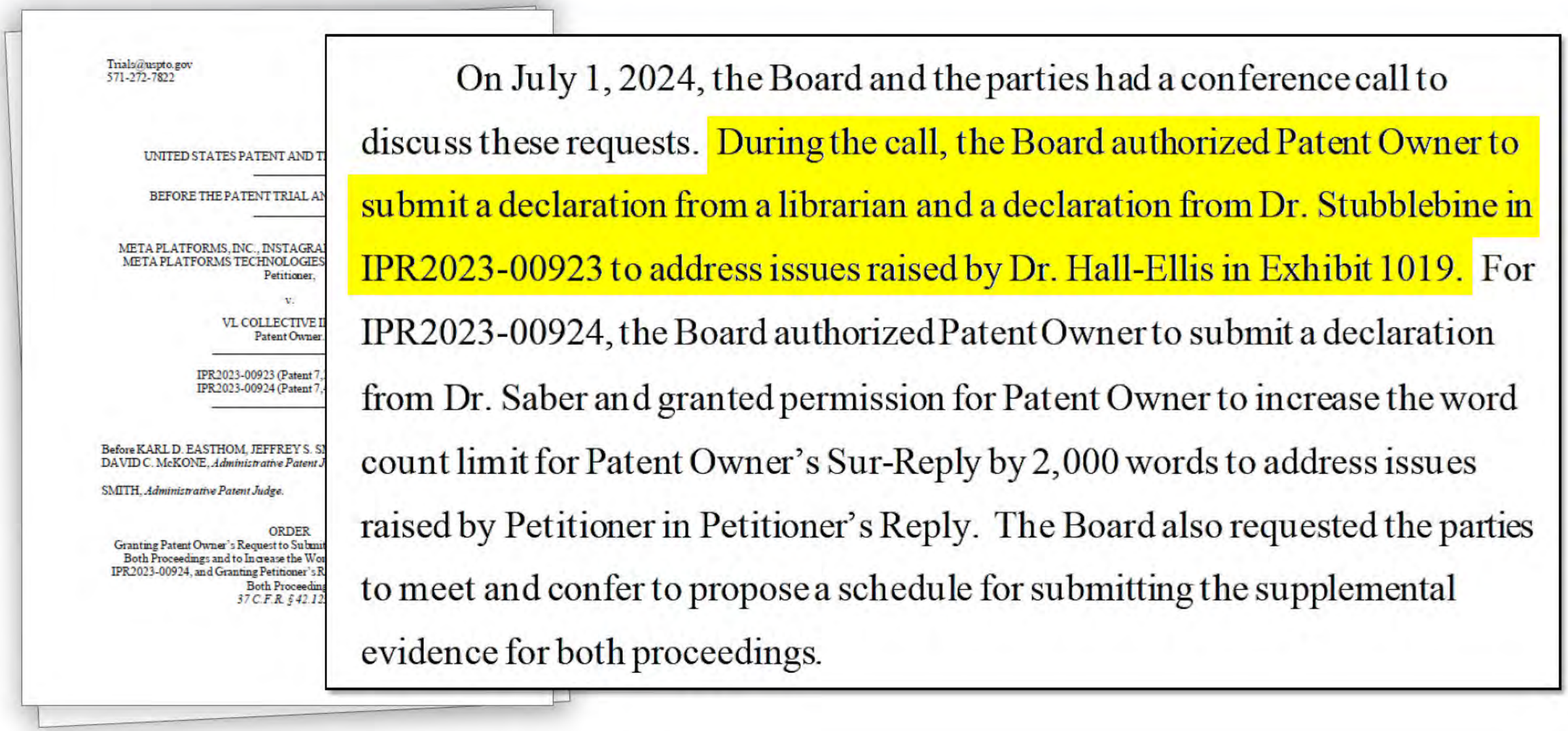
- Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft
- Ex. 1017 – Supp. Declaration of Dr. Henry Houh
- Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis
- Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof
- **Ex. 1027 – Online publication version of Handley**
- Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3

Prior Art - Handley (Ex. 1005)

Petitioners filed motion to submit supplemental information regarding Handley's public accessibility (Paper 21)

- Ex. 1016 – Declaration of Handley co-author Dr. Jon Crowcroft
- Ex. 1017 – Supp. Declaration of Dr. Henry Houh
- Ex. 1018 – Supp. Declaration of Dr. Sylvia Hall-Ellis
- Exs. 1020-1026 – Archived websites from Wayback Machine and authenticating declaration thereof
- Ex. 1027 – Online publication version of Handley
- **Ex. 1028 – Scanned physical copy of Handley from Computer Networks Vol. 31, Issue 3**

Prior Art - Handley (Ex. 1005)



Trials@uspto.gov
571-272-7822

UNITED STATES PATENT AND T

BEFORE THE PATENT TRIAL AN

META PLATFORMS, INC., INSTAGRA
META PLATFORMS TECHNOLOGIES
Petitioner,

v.

VL COLLECTIVE I
Patent Owner.

IPR2023-00923 (Patent 7,
IPR2023-00924 (Patent 7,

Before KARL D. EASTHOM, JEFFREY S. S
DAVID C. McKONE, *Administrative Patent J*

SMITH, *Administrative Patent Judge.*

ORDER
Granting Patent Owner's Request to Submit
Both Proceedings and to Increase the Wo
IPR2023-00924, and Granting Petitioner's R
Both Proceeding
37 C.F.R. § 42.12

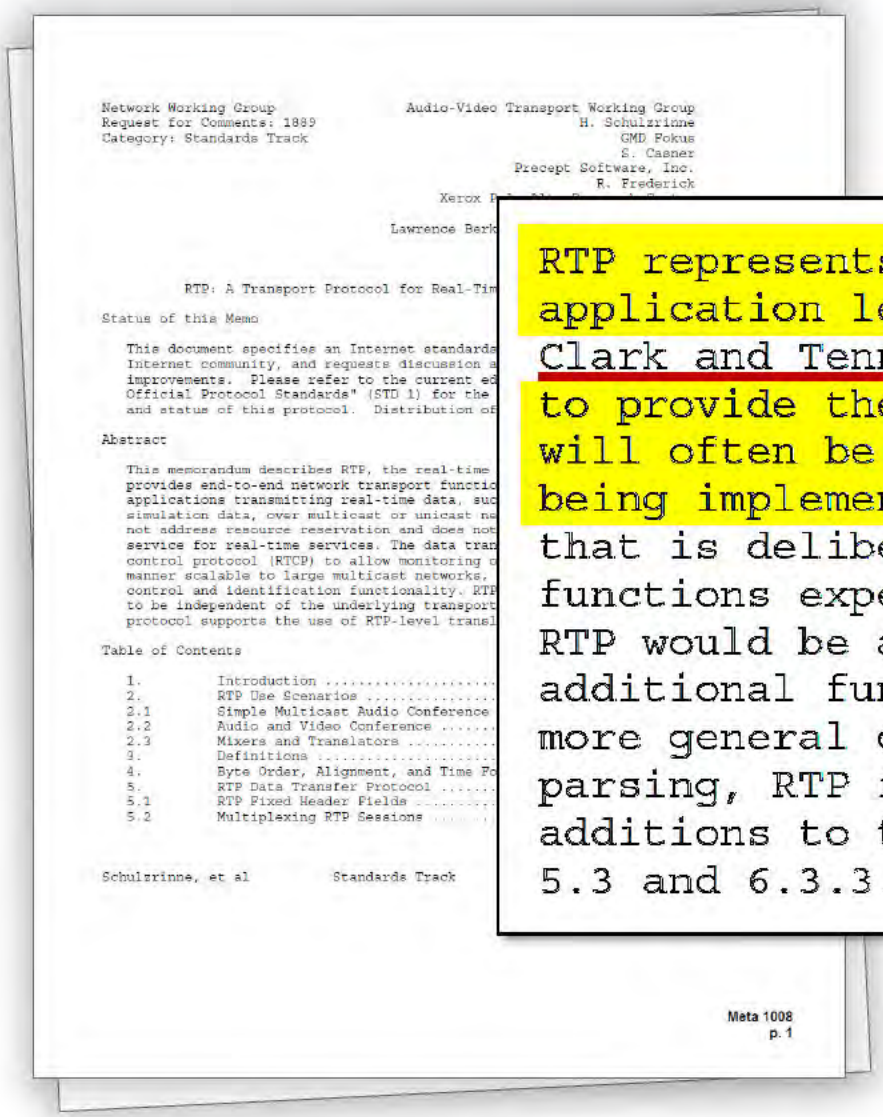
On July 1, 2024, the Board and the parties had a conference call to discuss these requests. During the call, the Board authorized Patent Owner to submit a declaration from a librarian and a declaration from Dr. Stubblebine in IPR2023-00923 to address issues raised by Dr. Hall-Ellis in Exhibit 1019. For IPR2023-00924, the Board authorized Patent Owner to submit a declaration from Dr. Saber and granted permission for Patent Owner to increase the word count limit for Patent Owner's Sur-Reply by 2,000 words to address issues raised by Petitioner in Petitioner's Reply. The Board also requested the parties to meet and confer to propose a schedule for submitting the supplemental evidence for both proceedings.

Order (Paper 41) at 2

Prior Art - Handley (Ex. 1005)

- Patent Owner ***did not*** submit a librarian expert declaration
- Patent Owner ***did not*** submit a supplemental declaration from Dr. Stubblebine

Ground I: Handley + Basturk



Network Working Group
Request for Comments: 1889
Category: Standards Track

Audio-Video Transport Working Group
H. Schulzrinne
GMD Fokus
S. Casner
Precept Software, Inc.
R. Frederick
Xerox
Lawrence Berk

RTP: A Transport Protocol for Real-Tim

Status of this Memo

This document specifies an Internet standards
Internet community, and requests discussion a
improvements. Please refer to the current ed
Official Protocol Standards" (STD 1) for the
and status of this protocol. Distribution of

Abstract

This memorandum describes RTP, the real-time
provides end-to-end network transport functio
applications transmitting real-time data, suc
simulation data, over multicast or unicast ne
not address resource reservation and does not
service for real-time services. The data tran
control protocol (RTCP) to allow monitoring o
manner scalable to large multicast networks,
control and identification functionality. RTP
to be independent of the underlying transport
protocol supports the use of RTP-level transl

Table of Contents

1. Introduction .....
2. RTP Use Scenarios .....
2.1 Simple Multicast Audio Conference
2.2 Audio and Video Conference .....
2.3 Mixers and Translators .....
3. Definitions .....
4. Byte Order, Alignment, and Time Fo
5. RTP Data Transfer Protocol .....
5.1 RTP Fixed Header Fields .....
5.2 Multiplexing RTP Sessions .....

Schulzrinne, et al Standards Track

Meta 1008
p. 1

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 that is deliberately not complete. This document specifies those functions expected to be common across all the applications for which RTP would be appropriate. Unlike conventional protocols in which additional functions might be accommodated by making the protocol more general or by adding an option mechanism that would require parsing, RTP is intended to be tailored through modifications and/or additions to the headers as needed. Examples are given in Sections 5.3 and 6.3.3.

EX1008 (RFC 1889 – RTP Specification) at 4

Ground I: Handley + Basturk

Petitioners' Technical Expert Witness



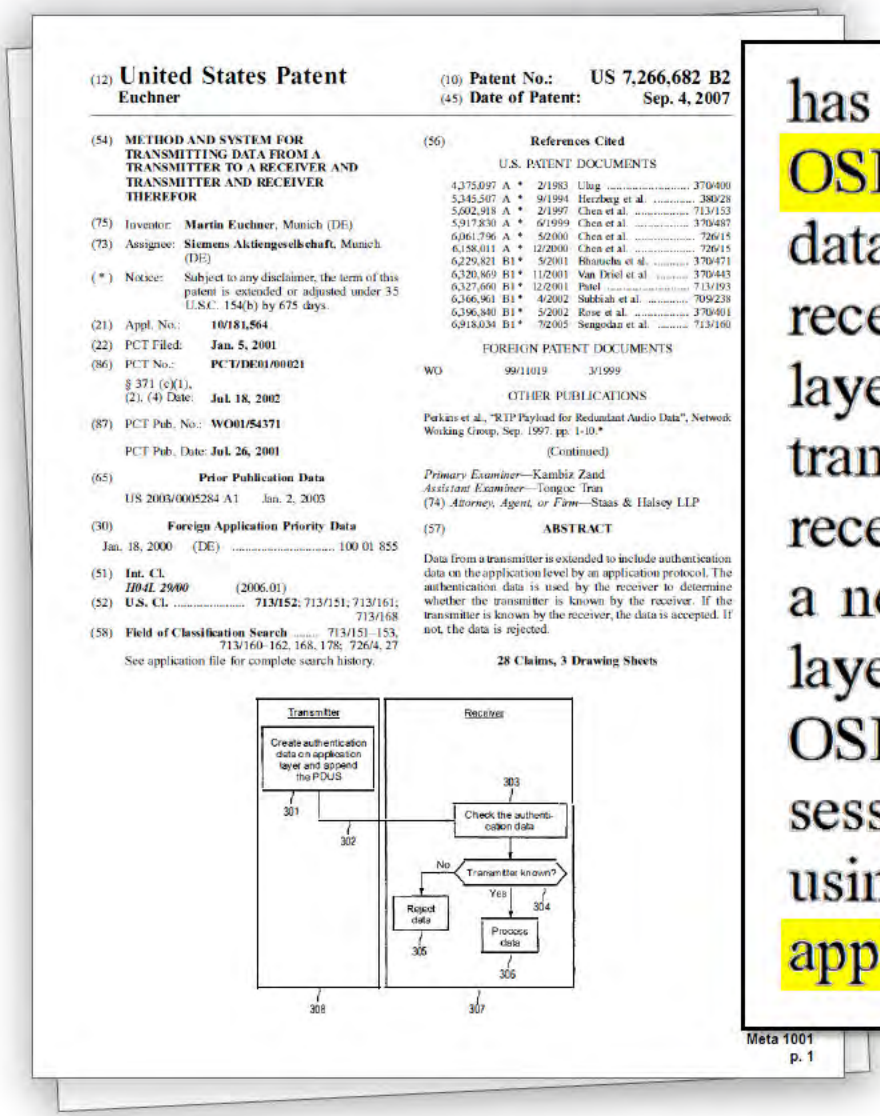
Dr. Henry Houh

77. Next, RTP utilizes the known OSI Model and, as described above in Section IV.G.1, RFC 1889 describes RTP as "represent[ing] a new style of protocol following the principles of application level framing and integrated layer processing." EX1008, 4. A POSITA would have understood and found obvious that because RTP follows the principles of application level framing and integrated layer processing and that the RTP packets are created at the application layer and RTP is an application protocol. *See* EX1015.[4] Thus, *Handley* teaches "Real Time Transport Protocol (RTP) packet level as an application protocol on an application layer" due to its disclosure of RTP. EX1001, cl. 1.

[4] This is the seminal Application Layer Framing paper, and I was a member of the research group headed by both Dr. Clark and Dr. Tennenhouse. The research group later split into two research groups, and I remained with Dr. Tennenhouse, who was also my Ph.D. Thesis advisor.

EX1003 (Houh Supp. Declaration) at ¶77, n.4

Ground I: Handley + Basturk



(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(b) 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 Bhatiehs 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 Tran
(74) *Attorney, Agent, or Firm*—Staas & 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.

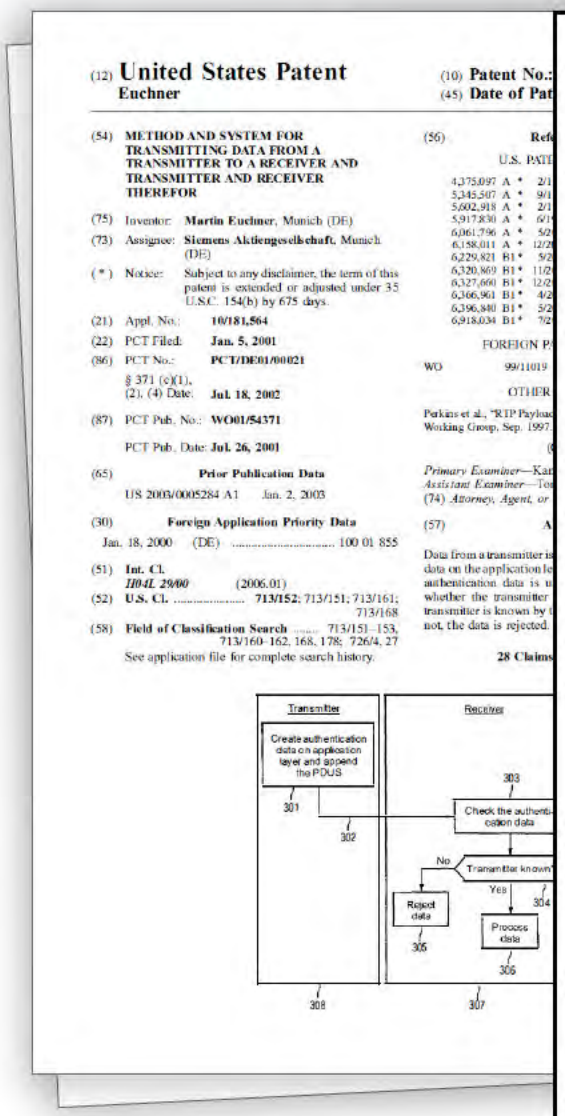
28 Claims, 3 Drawing Sheets

Meta 1001
p. 1

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 (US 7,266,682) at 1:25-37

Ground I: Handley + Basturk



(12) **United States Patent**
Euchner

(10) **Patent No.:**
(45) **Date of Pat**

(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(b) 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

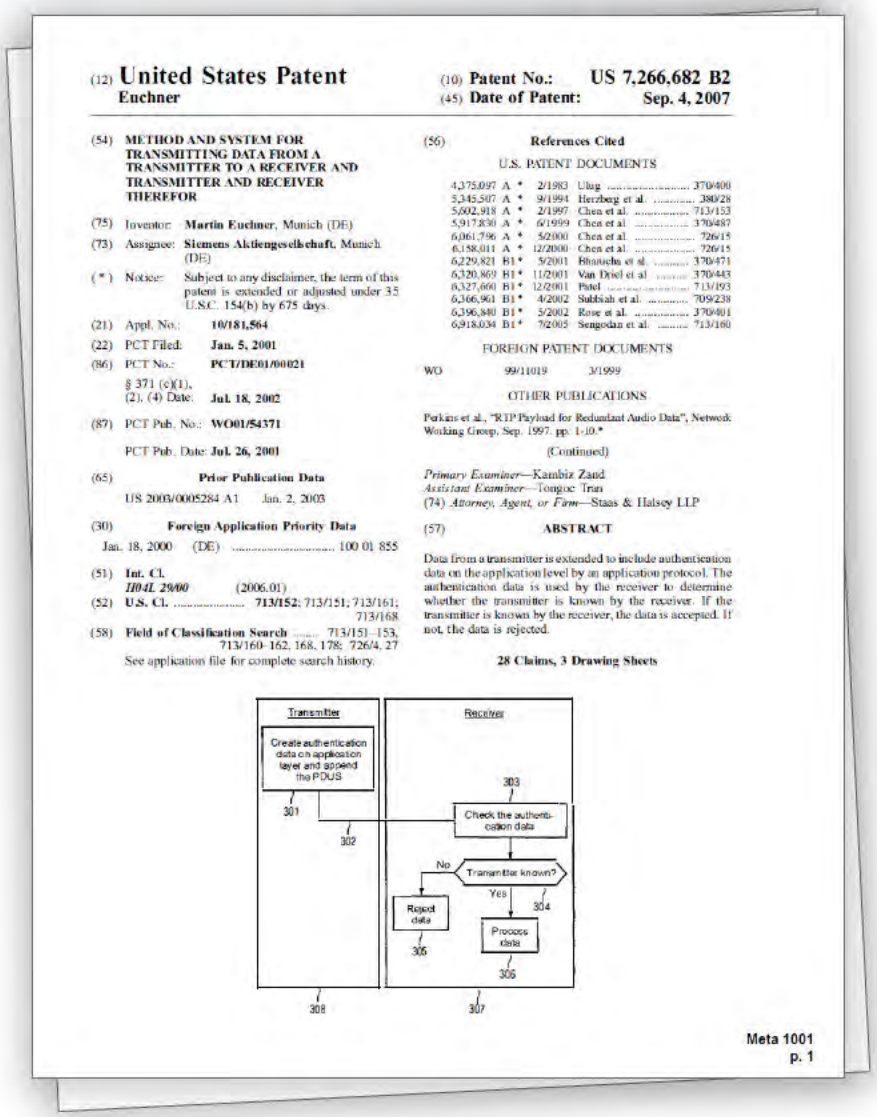
(58) **Field of Classification Search** 713/151–153, 713/160–162, 168, 178; 726/4, 27
See application file for complete search history.

(56) **Ref**
U.S. PAT
4,375,097 A * 2/1
5,345,507 A * 9/1
5,602,918 A * 2/1
5,917,830 A * 6/1
6,061,796 A * 5/2
6,158,011 A * 12/2
6,229,821 B1 * 5/2
6,320,869 B1 * 11/2
6,327,660 B1 * 12/2
6,366,961 B1 * 4/2
6,396,840 B1 * 5/2
6,918,034 B1 * 7/2
FOREIGN P
WO 99/11019
OTHER
Perkins et al., "RTP Payloa
Working Group, Sep. 1997
Primary Examiner—Kat
Assistant Examiner—Te
(74) *Attorney, Agent, or*
(57) A
Data from a transmitter is
data on the application le
authentication data is u
whether the transmitter
transmitter is known by
not, the data is rejected.
28 Claims

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 (US 7,266,682) at 1:25-45

Ground I: Handley + Basturk



(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(b) 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	Bhatiecha 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)

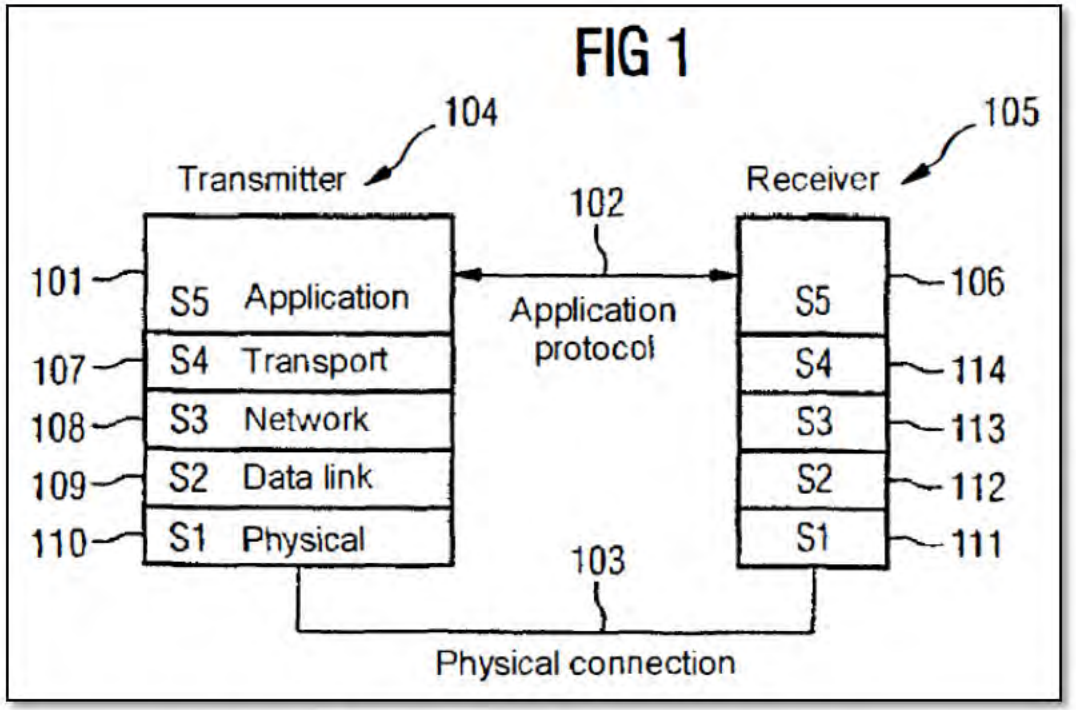
Primary Examiner—Kambiz Zand
Assistant Examiner—Tongoc Tran
(74) *Attorney, Agent, or Firm*—Staas & Halsey LLP

(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

Meta 1001
p. 1

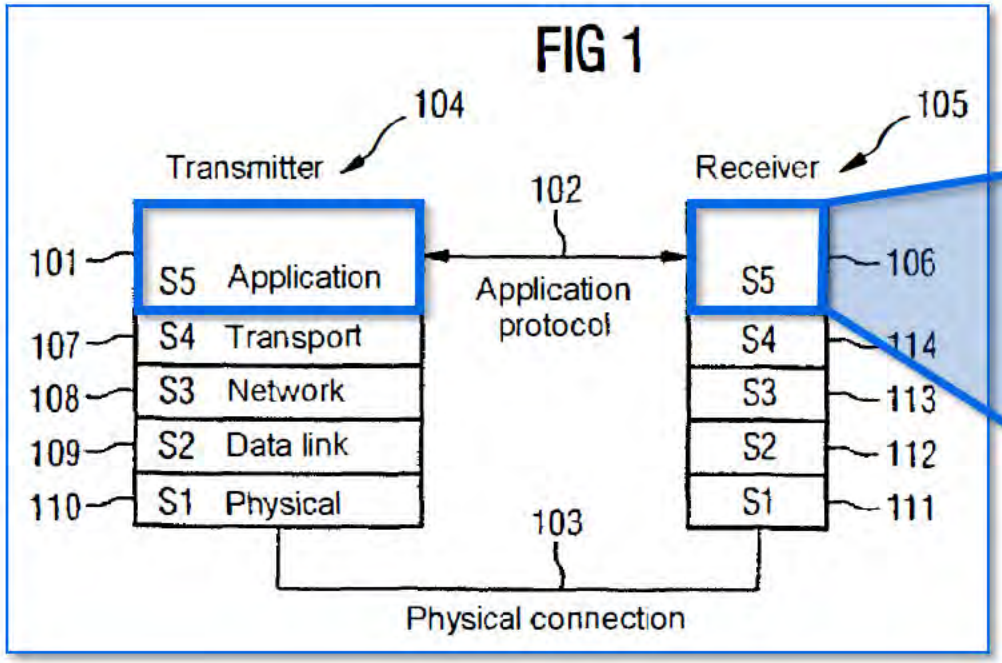


DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram of a protocol architecture (protocol stack) for a communication system in the layer model, following the OSI model mentioned above. A transmitter **104** and a receiver **105** interchange messages via a physical connection **103**. Both the transmitter **104** and the

EX1001 (US 7,266,682) at Fig. 1, 6:12-16

Ground I: Handley + Basturk



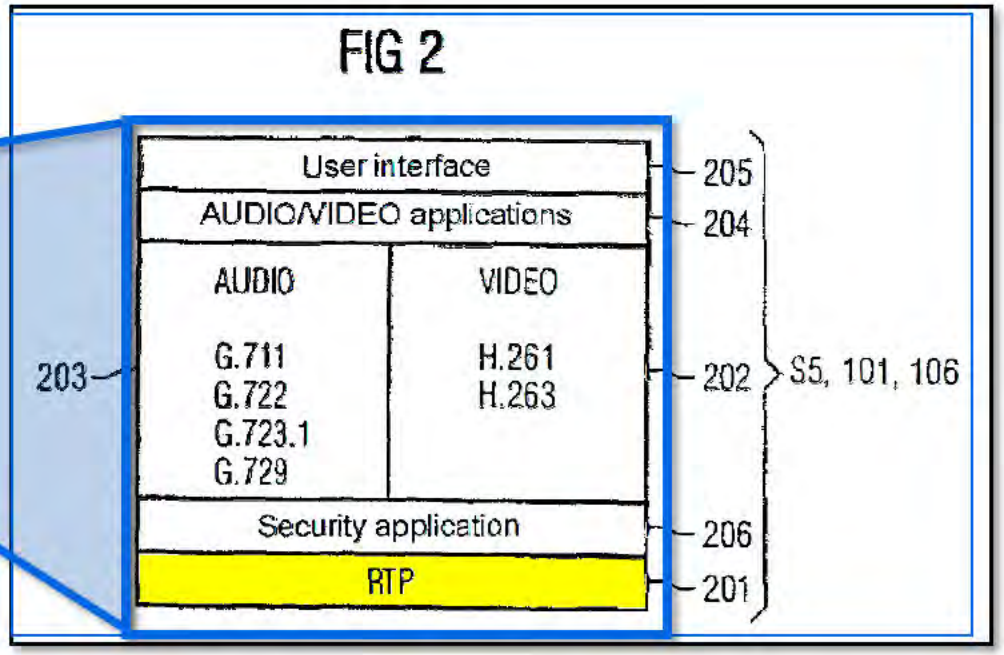


FIG. **2** is a block diagram of an application layer with possible protocols, based on an application concerning the transmission of media data (audio and video data). Thus, **101** and **106** represent the application layer (layer **5**) shown in FIG. **1** for the transmitter **104** and the receiver **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

EX1001 (US 7,266,682) at 6:33-42, Figs. 1, 2

Ground I: Handley + Basturk

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

M. Handley, J. Crowcroft and C. Bormann

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 must be sufficient capacity in the relevant traffic class to accommodate the traffic. How this capacity is ensured is independent of RTP.

EX1005 (Handley) at 1, 8