

Juniper Networks, Inc.
v.
Monarch Networking Solutions, Inc.

Monarch's Trial Presentation

IPR2024-00485
US Patent No. 8,451,844

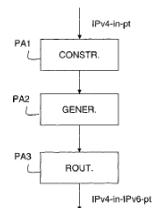
The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- Ground 1:
 - Li-2 is not prior art
 - A POSITA would not combine Li and Li-2
- Ground 2:
 - There is no evidence of simultaneous invention
- Ground 3:
 - Li and Wu would not have been combined
 - Wu does not teach the claimed constructed destination address

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains

 US008451844B2	
(12) United States Patent Boucadair et al.	(10) Patent No.: US 8,451,844 B2 (45) Date of Patent: May 28, 2013
(54) METHOD OF RECEIVING A DATA PACKET COMING FROM AN IPV4 DOMAIN IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND ASSOCIATED ACCESS EQUIPMENT	(56) References Cited
(75) Inventors: Mohamed Boucadair , Rennes (FR); Jean-Luc Grimault , Mondeville (FR)	U.S. PATENT DOCUMENTS 7,245,622 B2 * 7/2007 Huisman 370/392 7,551,632 B2 * 6/2009 Thibert et al. 370/401 2005/0236553 A1 * 12/2005 Wetterwald et al. 370/466
(73) Assignee: France Telecom , Paris (FR)	FOREIGN PATENT DOCUMENTS JP 1 420 559 A1 5/2004 WO WO 2004/039014 A1 5/2004 WO WO 2007/099248 A2 9/2007
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 278 days.	OTHER PUBLICATIONS Afili et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt Jul. 6-8, 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (Jul. 6, 1999). Carpenter et al., "RFC 3056. Connection of IPv6 Domains via IPv4 Clouds," Network Group Request for Comments, pp. 1-23 (Feb. 1, 2001). Park et al., "Network Address Translation—Protocol Translation (NAT-PT), draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (Oct. 22, 2005). Shin et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6 th International Conference on Advanced Communication Technology, Phoenix Park, Korea, Feb. 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (Feb. 9, 2004).
(21) Appl. No.: 13/001,850	* cited by examiner
(22) PCT Filed: Jun. 16, 2009	<i>Primary Examiner</i> — Hong Cho
(86) PCT No.: PCT/FR2009/051148 § 371 (c)(1), (2), (4) Date: Dec. 29, 2010	(74) <i>Attorney, Agent, or Firm</i> — Drinker Biddle & Reath LLP
(87) PCT Pub. No.: WO2010/004156 PCT Pub. Date: Jan. 14, 2010	(57) ABSTRACT A method of receiving a data packet from an IPv4 domain in an IPv6 domain, the data packet comprising an IPv4 destination address and a destination port number. The method comprises the following steps: constructing an IPv6 destination address by concatenating an operator prefix, the IPv4 destination address, and the destination port number; generating an IPv6 data packet from the IPv6 constructed destination address and the received IPv4 data packet; and routing the generated IPv6 data packet in the IPv6 domain using the IPv6 constructed destination address, the constructed address belonging to a range of IPv6 addresses routable to an interconnection equipment of the IPv6 domain with the IPv4 destination address.
(65) Prior Publication Data US 2011/0110374 A1 May 12, 2011	10 Claims, 5 Drawing Sheets
(30) Foreign Application Priority Data Jun. 30, 2008 (FR) 08 54398	
(51) Int. Cl. H04L 12/28 (2006.01)	
(52) U.S. Cl. USPC 370/393; 370/401	
(58) Field of Classification Search USPC 370/389, 392, 393, 401, 466 See application file for complete search history.	



Juniper Exhibit 1001, page 1

The IPv6 data packet is routed in the IPv6 domain as far as an equipment interconnecting the IPv6 domain and an IPv4 domain. *The method of the invention generates from this IPv6 data packet an IPv4 data packet that the IPv4 domain will be able to route to its destination.*

With the mechanism of the invention for constructing an IPv6 address from an IPv4 address, it is possible to retrieve the IPv4 address on which the IPv6 constructed address is based. It is therefore not necessary to store a table for translating IPv4 addresses to IPv6 addresses or to maintain states relating to sessions in an equipment interconnecting the IPv4 and IPv6 domains. *Thus the invention makes it possible to route an IPv4 data packet in the form of an IPv6 data packet via an equipment interconnecting the IPv6 domain with an IPv4 domain and to route the packet to its final destination* using the payload contained in the packet received by said interconnecting equipment to its destination without having recourse to state tables that are laborious to maintain.

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains



US008451844B2

(12) United States Patent Boucadiar et al.

(10) Patent No.: **US 8,451,844 B2**
(45) Date of Patent: **May 28, 2013**

(54) **METHOD OF RECEIVING A DATA PACKET COMING FROM AN IPV4 DOMAIN IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND ASSOCIATED ACCESS EQUIPMENT**

(75) Inventors: **Mohamed Boucadiar**, Rennes (FR);
Jean-Luc Grimaud, Mondeville (FR)

(73) Assignee: **France Telecom**, Paris (FR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 278 days.

(21) Appl. No.: **13/001,850**

(22) PCT Filed: **Jun. 16, 2009**

(86) PCT No.: **PCT/FR2009/051148**

§ 371 (c)(1),
(2), (4) Date: **Dec. 29, 2010**

(87) PCT Pub. No.: **WO2010/004156**

PCT Pub. Date: **Jan. 14, 2010**

(65) **Prior Publication Data**

US 2011/0110374 A1 May 12, 2011

(30) **Foreign Application Priority Data**

Jun. 30, 2008 (FR) 08 54398

(51) **Int. Cl.**
H04L 12/28 (2006.01)

(52) **U.S. Cl.**
USPC 370/393; 370/401

(58) **Field of Classification Search**
USPC 370/389, 392, 393, 401, 466
See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS
7,245,622 B2 * 7/2007 Huisma 370/392
7,551,632 B2 * 6/2009 Thibert et al. 370/401
2005/0236553 A1 * 12/2005 Wetterwald et al. 370/466

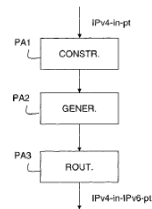
FOREIGN PATENT DOCUMENTS
JP 1 420 559 A1 5/2004
WO WO 2004/039014 A1 5/2004
WO WO 2007/099248 A2 9/2007

OTHER PUBLICATIONS
Afili et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt Jul. 6-8, 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (Jul. 6, 1999).
Carpenter et al., "RFC 3056. Connection of IPv6 Domains via IPv4 Clouds," Network Group Request for Comments, pp. 1-23 (Feb. 1, 2001).
Park et al., "Network Address Translation-Protocol Translation (NAT-PT), draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (Oct. 22, 2005).
Shin et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6th International Conference on Advanced Communication Technology, Phoenix Park, Korea, Feb. 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (Feb. 9, 2004).

* cited by examiner
Primary Examiner — Hong Cho
(74) Attorney, Agent, or Firm — Drinker Biddle & Reath LLP

(57) **ABSTRACT**
A method of receiving a data packet from an IPv4 domain in an IPv6 domain, the data packet comprising an IPv4 destination address and a destination port number. The method comprises the following steps: constructing an IPv6 destination address by concatenating an operator prefix, the IPv4 destination address, and the destination port number; generating an IPv6 data packet from the IPv6 constructed destination address and the received IPv4 data packet; and routing the generated IPv6 data packet in the IPv6 domain using the IPv6 constructed destination address, the constructed address belonging to a range of IPv6 addresses routable to an inter-connection equipment of the IPv6 domain with the IPv4 destination address.

10 Claims, 5 Drawing Sheets



Juniper Exhibit 1001, page 1

EX1001, Page 1

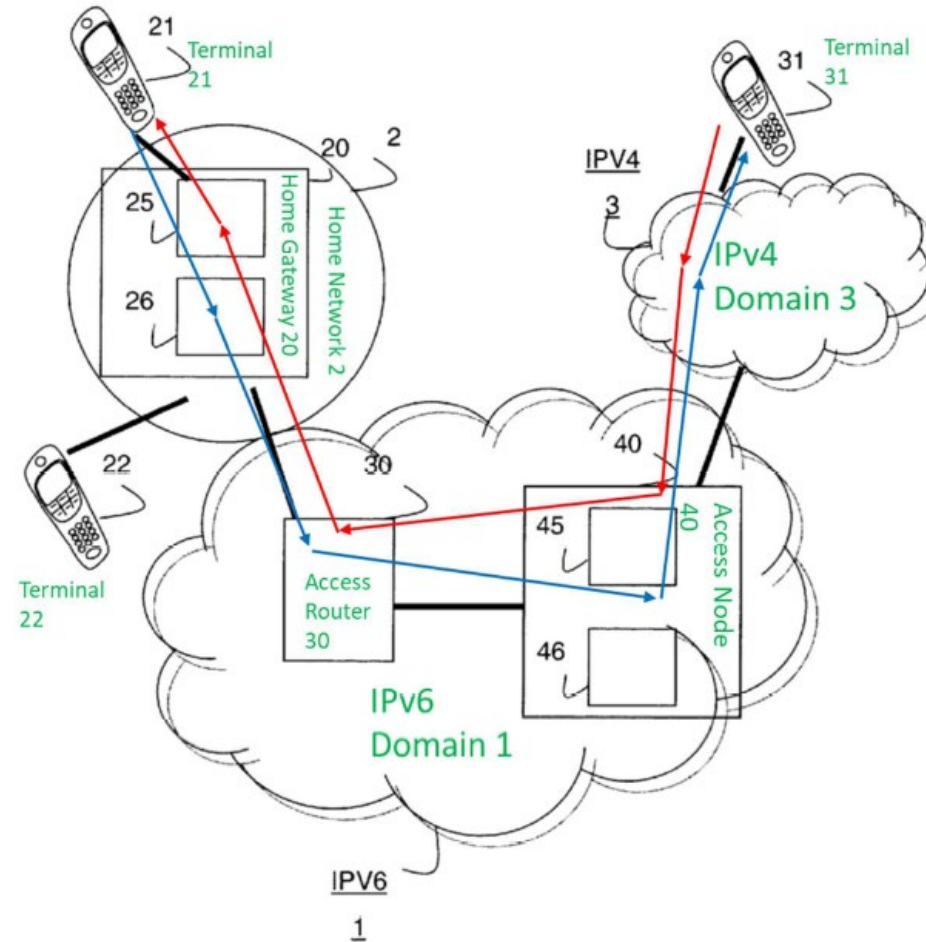
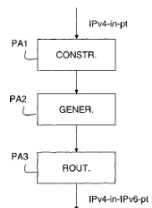


FIG. 1

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains

 US008451844B2	
(12) United States Patent Boucadair et al.	(10) Patent No.: US 8,451,844 B2 (45) Date of Patent: May 28, 2013
(54) METHOD OF RECEIVING A DATA PACKET COMING FROM AN IPV4 DOMAIN IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND ASSOCIATED ACCESS EQUIPMENT	(56) References Cited
(75) Inventors: Mohamed Boucadair , Rennes (FR); Jean-Luc Grimault , Mondeville (FR)	U.S. PATENT DOCUMENTS 7,245,622 B2 * 7/2007 Huisman 370/392 7,551,632 B2 * 6/2009 Thibert et al. 370/401 2005/0236553 A1 * 12/2005 Wetterwald et al. 370/466
(73) Assignee: France Telecom , Paris (FR)	FOREIGN PATENT DOCUMENTS JP 1 420 559 A1 5/2004 WO WO 2004/039014 A1 5/2004 WO WO 2007/099248 A2 9/2007
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 278 days.	OTHER PUBLICATIONS Afili et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt Jul. 6-8, 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (Jul. 6, 1999). Carpenter et al., "RFC 3056. Connection of IPv6 Domains via IPv4 Clouds," Network Group Request for Comments, pp. 1-23 (Feb. 1, 2001). Park et al., "Network Address Translation—Protocol Translation (NAT-PT), draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (Oct. 22, 2005). Shin et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6 th International Conference on Advanced Communication Technology, Phoenix Park, Korea, Feb. 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (Feb. 9, 2004).
(21) Appl. No.: 13/001,850	* cited by examiner <i>Primary Examiner</i> — Hong Cho (74) <i>Attorney, Agent, or Firm</i> — Drinker Biddle & Reath LLP
(22) PCT Filed: Jun. 16, 2009	(57) ABSTRACT A method of receiving a data packet from an IPv4 domain in an IPv6 domain, the data packet comprising an IPv4 destination address and a destination port number. The method comprises the following steps: constructing an IPv6 destination address by concatenating an operator prefix, the IPv4 destination address, and the destination port number; generating an IPv6 data packet from the IPv6 constructed destination address and the received IPv4 packet; and routing the generated IPv6 data packet in the IPv6 domain using the IPv6 constructed destination address, said constructed address belonging to a range of IPv6 addresses routable to an interconnection equipment of the IPv6 domain with the IPv4 destination address.
(86) PCT No.: PCT/FR2009/051148 § 371 (c)(1), (2), (4) Date: Dec. 29, 2010	10 Claims, 5 Drawing Sheets
(87) PCT Pub. No.: WO2010/004156 PCT Pub. Date: Jan. 14, 2010	
(65) Prior Publication Data US 2011/0110374 A1 May 12, 2011	
(30) Foreign Application Priority Data Jun. 30, 2008 (FR) 08 54398	
(51) Int. Cl. H04L 12/28 (2006.01)	
(52) U.S. Cl. USPC 370/393; 370/401	
(58) Field of Classification Search USPC 370/389, 392, 393, 401, 466 See application file for complete search history.	



Juniper Exhibit 1001, page 1

1. A method of receiving a data packet from an *IPv4 domain* in an *IPv6 domain*, said data packet comprising an IPv4 destination address and a destination port number, said method comprising the following steps:

constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number;

generating an IPv6 data packet from the IPv6 constructed destination address and the received IPv4 packet; and

routing the generated IPv6 data packet in the IPv6 domain using the IPv6 constructed destination address, said constructed address belonging to a range of IPv6 addresses routable to an interconnection equipment of the IPv6 domain with the IPv4 destination address.

EX1001 at 14:29-42 (Claim 1)

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains

A domain is defined by control:

“A telecommunications network administered by an operator is also referred to as a domain.”

EX1001 at 1:30-31

“This kind of access equipment therefore interconnects the IPv6 domain to which it belongs and to a neighboring IPv4 domain. The neighboring IPv4 domain may be a public network managed by an operator or a private network, either a home network or a business network. ”

EX1001 at 4:39-43

(12) **United States Patent**
Boucadair et al.

(10) **Patent No.: US 8,451,844 B2**
(45) **Date of Patent: May 28, 2013**

(54) **METHOD OF RECEIVING A DATA PACKET COMING FROM AN IPV4 DOMAIN IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND ASSOCIATED ACCESS EQUIPMENT**

(75) **Inventors:** Mohamed Boucadair, Rennes (FR); Jean-Luc Grimault, Mondeville (FR)

(73) **Assignee:** France Telecom, Paris (FR)

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 278 days.

(21) **Appl. No.:** 13/001,850

(22) **PCT Filed:** Jun. 16, 2009

(86) **PCT No.:** PCT/FR2009/051148
§ 371 (c)(1),
(2), (4) Date: Dec. 29, 2010

(87) **PCT Pub. No.:** WO2010/004156
PCT Pub. Date: Jan. 14, 2010

(65) **Prior Publication Data**
US 2011/0110374 A1 May 12, 2011

(30) **Foreign Application Priority Data**
Jun. 30, 2008 (FR) 08 54398

(51) **Int. Cl.**
H04L 12/28 (2006.01)

(52) **U.S. Cl.**
USPC 370/393; 370/401

(58) **Field of Classification Search**
USPC 370/389, 392, 393, 401, 466
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,245,622 B2 * 7/2007 Huisma 370/392
7,551,632 B2 * 6/2009 Thibert et al. 370/401
2005/0236553 A1 * 12/2005 Wetterwald et al. 370/466

FOREIGN PATENT DOCUMENTS

JP 1 420 559 A1 5/2004
WO WO 2004/039014 A1 5/2004
WO WO 2007/099248 A2 9/2007

OTHER PUBLICATIONS

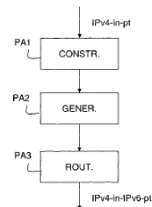
Afilil et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt Jul. 6-8, 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (Jul. 6, 1999).
Carpenter et al., "RFC 3056. Connection of IPv6 Domains via IPv4 Clouds," Network Group Request for Comments, pp. 1-23 (Feb. 1, 2001).
Park et al., "Network Address Translation—Protocol Translation (NAT-PT), draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (Oct. 22, 2005).
Shin et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6th International Conference on Advanced Communication Technology, Phoenix Park, Korea, Feb. 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (Feb. 9, 2004).

* cited by examiner

Primary Examiner — Hong Cho
(74) *Attorney, Agent, or Firm* — Drinker Biddle & Reath LLP

(57) **ABSTRACT**
A method of receiving a data packet from an IPv4 domain in an IPv6 domain, the data packet comprising an IPv4 destination address and a destination port number. The method comprises the following steps: constructing an IPv6 destination address by concatenating an operator prefix, the IPv4 destination address, and the destination port number; generating an IPv6 data packet from the IPv6 constructed destination address and the received IPv4 data packet; and routing the generated IPv6 data packet in the IPv6 domain using the IPv6 constructed destination address, the constructed address belonging to a range of IPv6 addresses routable to an interconnection equipment of the IPv6 domain with the IPv4 destination address.

10 Claims, 5 Drawing Sheets



Juniper Exhibit 1001, page 1

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains

A “domain” is “a network or subnetwork and its address space that are under common control.”

“One key aspect of a “domain” is the concept of common control. The '844 Patent's specification recognizes this concept and states that “[a] telecommunications network administered by an operator is also referred to as a domain.” EX1001 at 1:30-31 (emphasis added). In other words, a domain is only understood in the context of the party the administers it: networks administered by different operators are different domains. The specification highlights the difference between a private domain (a network that is controlled or administered by a homeowner or business entity) and a domain operated by a service provider. *Id.* at 1:32-50; 4:41-43 (“The neighboring IPv4 domain may be a public network managed by an operator or a private network, either a home network or a business network.”).”

EX2015 ¶¶ 46-47

A domain is defined by control:

“Domain The part of a computer network in which the data processing resources are under common control. That's the formal technical definition.”

EX2003 at 3

“domain (1) That part of a computer network in which the data processing resources are under common control. ”

EX2004 at 4

'844 Patent: Enabling Communications Between IPv4 and IPv6 Domains

- Petitioner defined domain as “a group of computers that merely share something in common.”
 - Reply 4 (quotation omitted)

1. A method of receiving a data packet from an IPv4 ~~domain~~ [group of computers] in an IPv6 ~~domain~~ [group of computers], said data packet comprising....

EX1001, 14:29-30 (Claim 1, annotated)

- This definition has no limits and even includes subnets

“An IPv6 address has two parts:
a left-hand part (the prefix) that *identifies a subnetwork of the domain*;
a right-hand part that identifies a machine connected to the subnetwork.”

EX1001 at 6:25-29 (annotated)

The '844 Patent

Key Points

- **All Grounds:**
 - **Li does not disclose separate IPv4 and IPv6 domains**
- Ground 1:
 - Li-2 is not prior art
 - A POSITA would not combine Li and Li-2
- Ground 2:
 - There is no evidence of simultaneous invention
- Ground 3:
 - Li and Wu would not have been combined
 - Wu does not teach the claimed constructed destination address

Li's Figure 7 Is A Single Domain

Li's Figure 1 and Figure 7 share the same **domains** and the same **components**

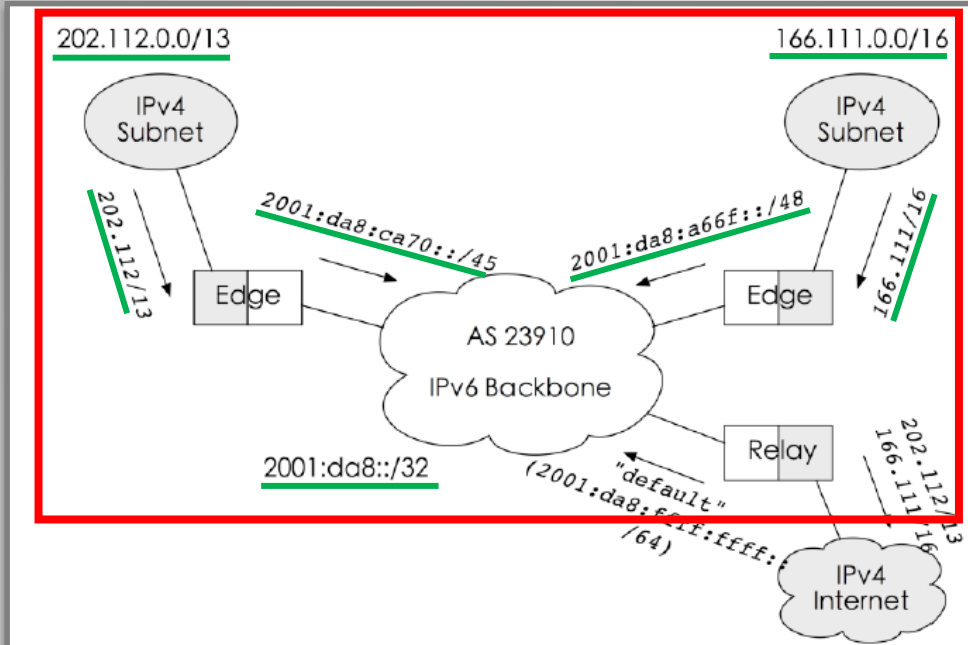


Figure 1. Intra-domain IPv4-over-IPv6 transition

EX1037 Fig. 1 (Annotated)

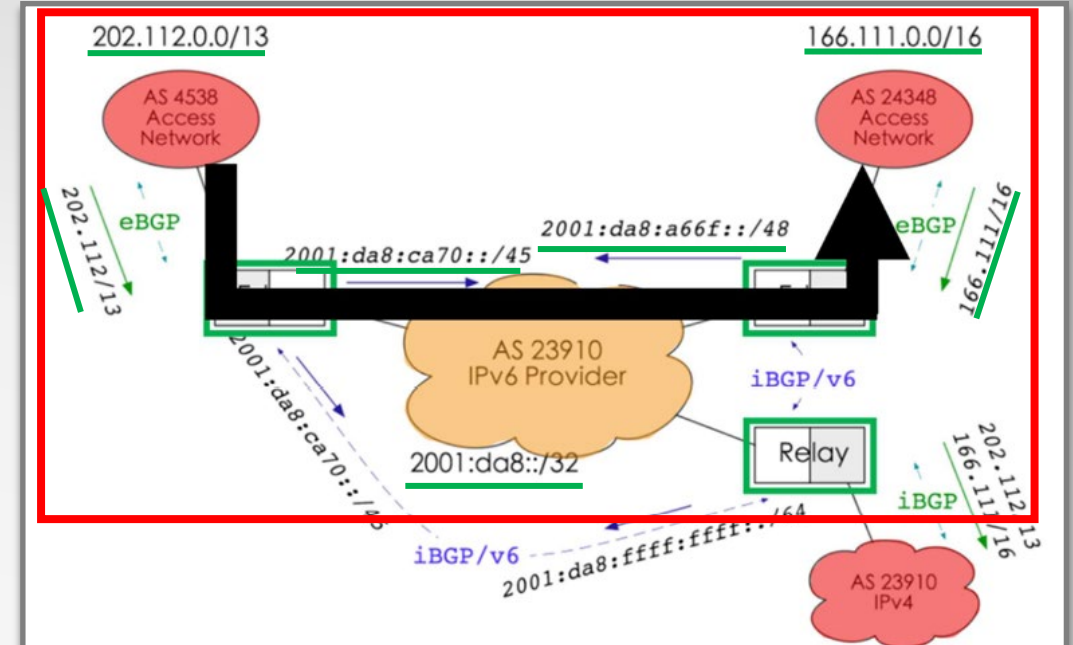


Figure 7. IPv4-over-IPv6 transition for access networks

Pet. 17 (EX1037 Fig. 7 Annotated)

Li Explains That Figure 7 Refers to The Intra Domain Environment

Forwarding IPv4 Traffic in Pure IPv6 Backbone with Stateless Address Mapping

Maoke Chen, Xing Li
CERNET, Network Research Center
Tsinghua University
Beijing, P. R. China
{mk, xing}@cernet.edu.cn

Ang Li
Dept. of Electronic Engineering
Tsinghua University
Beijing, P. R. China
auron@ns.foxit.edu.cn

Yong Cui
Dept. of Computer Science
Tsinghua University
Beijing, P. R. China
cy@csnet1.cs.tsinghua.edu.cn

Abstract—As the IPv6 networks rapidly deployed, the transition problem has been changed. Because the transition of applications is a steady process with a far longer duration in comparison to the transition of infrastructure, providers cannot give up the duty of serving IPv4 traffic for the time being. On the other hand, operating a dual-stack backbone is highly costing for large-scale deployment of new networks. In this paper, a new technique of forwarding IPv4 traffic in IPv6-only backbone is developed. Rather than the ever-existing tunneling approaches, the proposed one is automatic and stateless for end nodes, without explicit tunneling. The route entries for delivering IPv4 traffic are well aggregated on the borders of IPv6 autonomous systems. This makes the technique suitable for large-scale deployment in an inter-domain networking environment.

Keywords—IPv6; transition; automatic tunneling; routing

I. INTRODUCTION

Transition is one of the most significant problems in deploying an emerging network technology. Since the IP plays the role of engine in the Internet architecture, migrating networks from IPv4 to IPv6 is very difficult and complicated. In the past decade after the IPv6 protocol specification was defined, a series of techniques were developed to solve the issues of transition, including both translation and tunneling approaches [1-8]. Among them, Tunnel Broker [6] and 6to4 [7,8] are highlighted in the real deployment because of their ability of handling tunnel requests automatically.

However, these do not terminate all the obstacles of transition. Since native IPv6 networks are rapidly deployed over the world, the problem is changing unconsciously. In the early stage of IPv6 deployment, there are IPv6 islands dispersed among the ocean of IPv4 networks and therefore connectivity of IPv6 clouds is the major issue. Currently, native IPv6 infrastructures are established in large-scale and the connectivity becomes less serious. On the other hand, however, the applications and resources are still concentrated in the IPv4 networks. Although the IPv6 programming interface has been well defined since several years ago [9, 10], the application porting process are far slower than what is expected. Theoretically, porting an application from IPv4 to IPv6-enabled version is not a big burden. But this is often untrue in practice. Besides the socket interface should be modified, data structures and message formats, once involving IP addresses, should be reshaped as well. This often challenges the compatibility of an application protocol and its implementation

details. Even if programmers are fully encouraged to do the porting, there is still an obstacle at migrating the running services. Anyway, at this stage, interoperability of applications in dual-protocol environment has, replacing connectivity, become the sharpest issue of the IPv4-IPv6 transition.

Dual-stack is a feasible solution for application transition but not suitable for large-scale deployment of new networks, esp. in developing countries where the scale of next generation Internet might be as tens or hundreds times as that of current. Firstly, as the IPv4 address space has been half and more exhausted, it is almost impossible to get such a huge amount of address resources for new deployments. E.g. for the next generation Internet project in China, if each citizen would hold one permanent global address in average, then about 73 blocks of class A are needed. Secondly, a single-stack backbone is more economical than a dual-stack one. Single-stack routers consume less processing power and memory, and single-stack networks are less costing in operation and maintenance. Thirdly, the funding bodies, e.g. government, ministries and etc., sees deployment of IPv6 as a national strategy and single-stack obviously much more encourages the transition from traditional IPv4 to new IPv6 Internet.

Therefore, carrying IPv4 traffic in pure IPv6 backbone is a significant problem of current stage of transition. The generic encapsulation for IPv6 stack has been defined [11]. Tunnel broker approach can be applied for the IPv4-over-IPv6 case without any difficulty to accelerate the effect of access service provision. However, there is not a scalable solution as is stateless to end-systems, just like the 6to4 for IPv6-over-IPv4 case. Furthermore, if not all the tunnel brokers communicate each other and exchange the route information, they may cause IPv4 routing non-optimized and cause a great waste of network resources. However, meshed tunneling among the brokers is not scalable too. Lack of a scalable approach hampers the deployment of IPv6-only backbones.

In this paper, a new technique of forwarding IPv4 traffic in pure IPv6 backbone is proposed. In order to provide a transparent environment for users to run their IPv4 applications and to have accesses to the existing IPv4 content services, IPv4 packets are mapped into IPv6 (or vice versa) automatically at the edge of the IPv6 backbone, with the help of BGP routing tables. The rest parts of the paper are organized as follows. Section II discusses the functional requirements to the architecture design. Section III illustrates the basic design, which is suitable for transition in an intra-domain environment.

“In this section, we extend the scheme to two models: 1) stub autonomous systems are connected to an IPv6 backbone, *as customer networks of the latter, and only have accesses to IPv4 hosts within the scope controlled by the provider*; 2)”

Figure 7 is model 1

“Meanwhile, the relay router advertises the special prefix with “0xFFFFFFFF” for all the IPv4 networks *outside the scope of the provider’s administration.*”

“Indeed, the BGP RIB provides a way of automatically distributing the list. Actually, the scenario in Fig. 5 can be seen as an alternative for that in Fig. 1, as long as each IPv4 *subnet* are configured with BGP and assigned with a private AS number.”

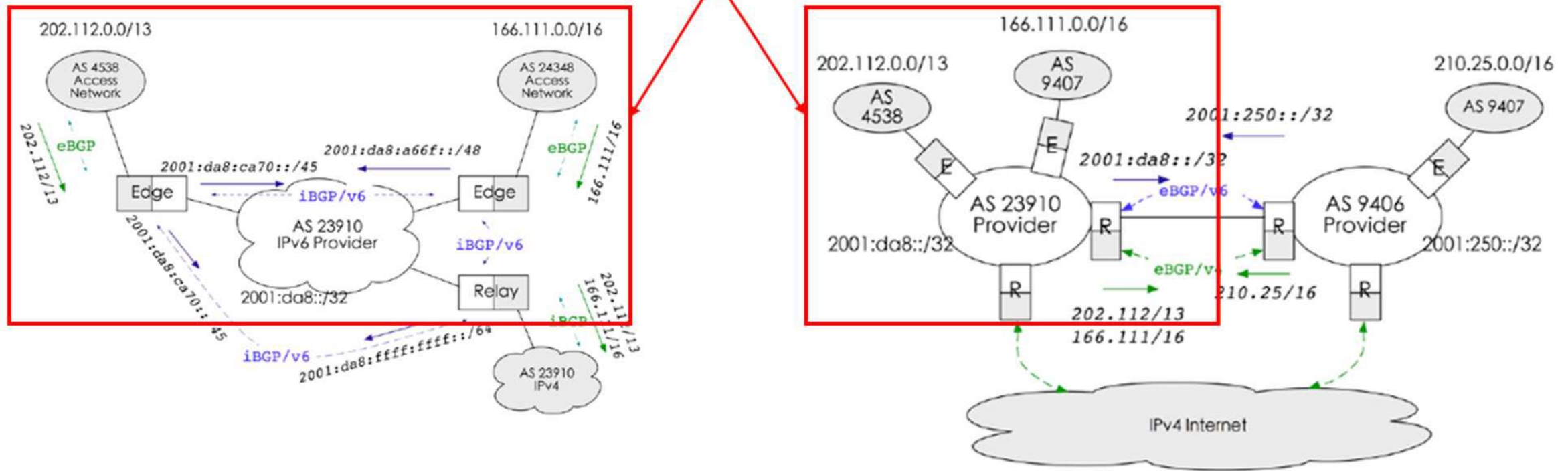
Petitioner Cannot Rely On Li's Other Figures

- The Petition did not discuss Figures 8, 10, or 11
 - These embodiments cannot be raised for the first time in Reply
 - *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1367-68 (Fed. Cir. 2015)
 - *MModal LLC v. Nuance Communications, Inc.*, 846 F. App'x 900, 906 (Fed. Cir. 2021)
- The Reply and Declaration do not explain how Li teaches the invention
 - Petitioner to provide an element-by-element analysis

Figures 8, 10, and 11 do not teach the claims

Figures 8, 10, and 11 include the same domain as Figs. 1 and 7

The same single domain



Sur-reply 11 (EX1037 Figs 7, 8
(annotated))

The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- **Ground 1:**
 - **Li-2 is not prior art**
 - A POSITA would not combine Li and Li-2
- Ground 2:
 - There is no evidence of simultaneous invention
- Ground 3:
 - Li and Wu would not have been combined
 - Wu does not teach the claimed constructed destination address

Li-2 Is Not Prior Art

- Public accessibility requires that a POSITA could locate it using reasonable diligence

“A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that [POSITAs] *exercising reasonable diligence*, can locate it.”

SRI Int’l, Inc. v. Internet Sec. Sys., Inc., 511 F.3d 1186, 1194 (Fed. Cir. 2008) (emphasis added)

- Mere availability is not public accessibility:

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

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

A POSITA Would Not Have Found Li-2

- Li-2 was not published by the IETF
- Li-2 was not announced to the public
- The directory containing Li-2 was not indexed or searchable
- There is no evidence the staging directory was online during the relevant period
- There is no evidence anyone ever saw Li-2, other than its authors
- Li-2 was only in the staging directory for at most 9 days before the priority date

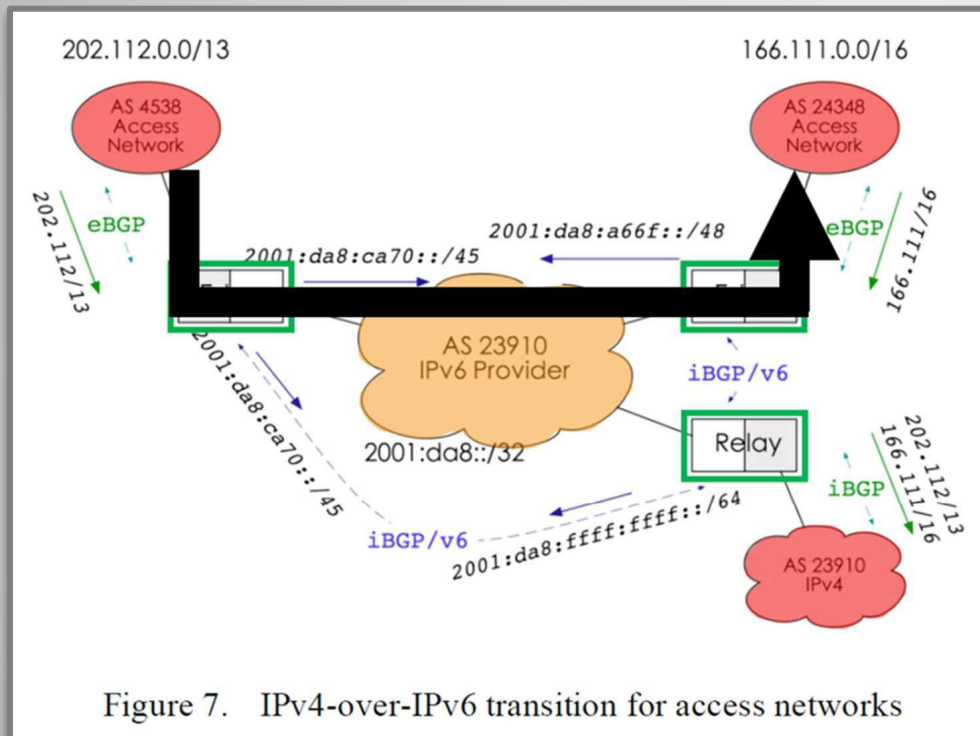
The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- **Ground 1:**
 - Li-2 is not prior art
 - **A POSITA would not combine Li and Li-2**
- Ground 2:
 - There is no evidence of simultaneous invention
- Ground 3:
 - Li and Wu would not have been combined
 - Wu does not teach the claimed constructed destination address

Li-2 Is Not An Extension Of Li

- **Li**: IPv4 hosts within an IPv4 network communicating with other IPv4 hosts across an IPv6-only network.
- **Li-2**: enabling hosts within an IPv6-only network to communicate with IPv4 hosts.



IVI Routing

```
(Global ) ---- IPv4-2 ----- IPv6-2 ---- (Global )
(IPv4   ) --|R1|-----|IVI gateway|-----|R2|---- (IPv6   )
(network) ---- IPv4-1 ----- IPv6-1 ---- (network)
```

Figure 2

EX1038 Fig. 2

Pet. 17 (EX1037 Fig. 7 Annotated)

The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- Ground 1:
 - Li-2 is not prior art
 - A POSITA would not combine Li and Li-2
- **Ground 2:**
 - **There is no evidence of simultaneous invention**
- Ground 3:
 - Li and Wu would not have been combined
 - Wu does not teach the claimed constructed destination address

Petitioner Misapplies The “Simultaneous Invention” Concept

- When the instances of alleged simultaneous invention do not disclose the claimed invention, they are not evidence of simultaneous invention.

“[E]vidence of simultaneous invention cannot alone show obviousness.”

Regents of the Univ. of Cal. v. Broad Inst., Inc., 903 F.3d 1286, 1295-96 (Fed. Cir. 2018)

“Simultaneous invention may serve as evidence of obviousness when considered in light of all of the circumstances.”

Regents of the Univ. of Cal. v. Broad Inst., Inc., 903 F.3d 1286, 1295 (Fed. Cir. 2018)

The “Simultaneous Inventions” Are Not The Claimed Invention

- The IVI References do not describe the entire claimed invention
 - Petitioner only addressed claims 1 and 3
 - These references do not describe a destination port number
- The Bush References cannot render obvious the claims
 - The Reply does not identify what Petitioner relies on in the thus Bush Paper
 - The Bush Presentation does not describe constructing an IPv6 address or extracting information from one
 - The Bush References never use a port number in an IPv6 address

The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- Ground 1:
 - Li-2 is not prior art
 - A POSITA would not combine Li and Li-2
- Ground 2:
 - There is no evidence of simultaneous invention
- **Ground 3:**
 - **Li and Wu would not have been combined**
 - Wu does not teach the claimed constructed destination address

Wu's "Silkroad" Solution

- Silkroad clients communicate via a Silkroad tunnel with assistance from a Silkroad server

[19] State Intellectual Property Office of PRC



[12] Patent Application Publication

[51] Int. Cl.

H04L 12/28

H04L 29/06 H04Q 3/00

H04Q 3/545

[21] Application No.: 03158973.1

[43] Publication Date: September 1st, 2004

[11] Patent NO.:

[22] Application Date: September 17th, 2003

[21] Application No.: 03158973.1

[71] Applicant: The Institute of Computing Technology of

the Chinese Academy of Sciences
Address: No. 6, Kexueyuan South Road,
Zhongguancun, Haidian District, Beijing
100080

[72] Inventor: WU Xianguo, LIU Min, ZHANG Tianle,
SHI Jinglin, LI Zhongcheng

[74] Patent agency: China Science

Trademark

Agent: ZHOU Guo

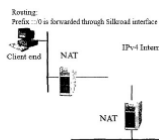
Claims: 6 pages
Specification: 8 pages
Drawings: 5 pages

[54] Title of Invention

An automatic tunnel method capable of traversing
network address translation

[57] Abstract

The present invention involves the field of Internet
technology, a kind of automatic tunnel method capable
of traversing NAT (Network Address Translation), i.e.
this tunnel technology allows the tunnel body to have
any type and any number of NAT, it is a kind of new
tunnel technology in the transition period from IPv4
Internet to IPv6 Internet. The aim is to make the
IPv6/IPv4 dual-stack nodes within NAT field to obtain
the global end-to-end IPv6 connection. By using this
tunnel technology, the IPv6/IPv4 dual-stack nodes
within NAT field will communicate with the IPv6 nodes
outside NAT field through the intermediate server, and
will communicate with other the IPv6/IPv4 dual-stack
nodes within NAT field.



Published by Intellectual Property Publishing House, Juniper E

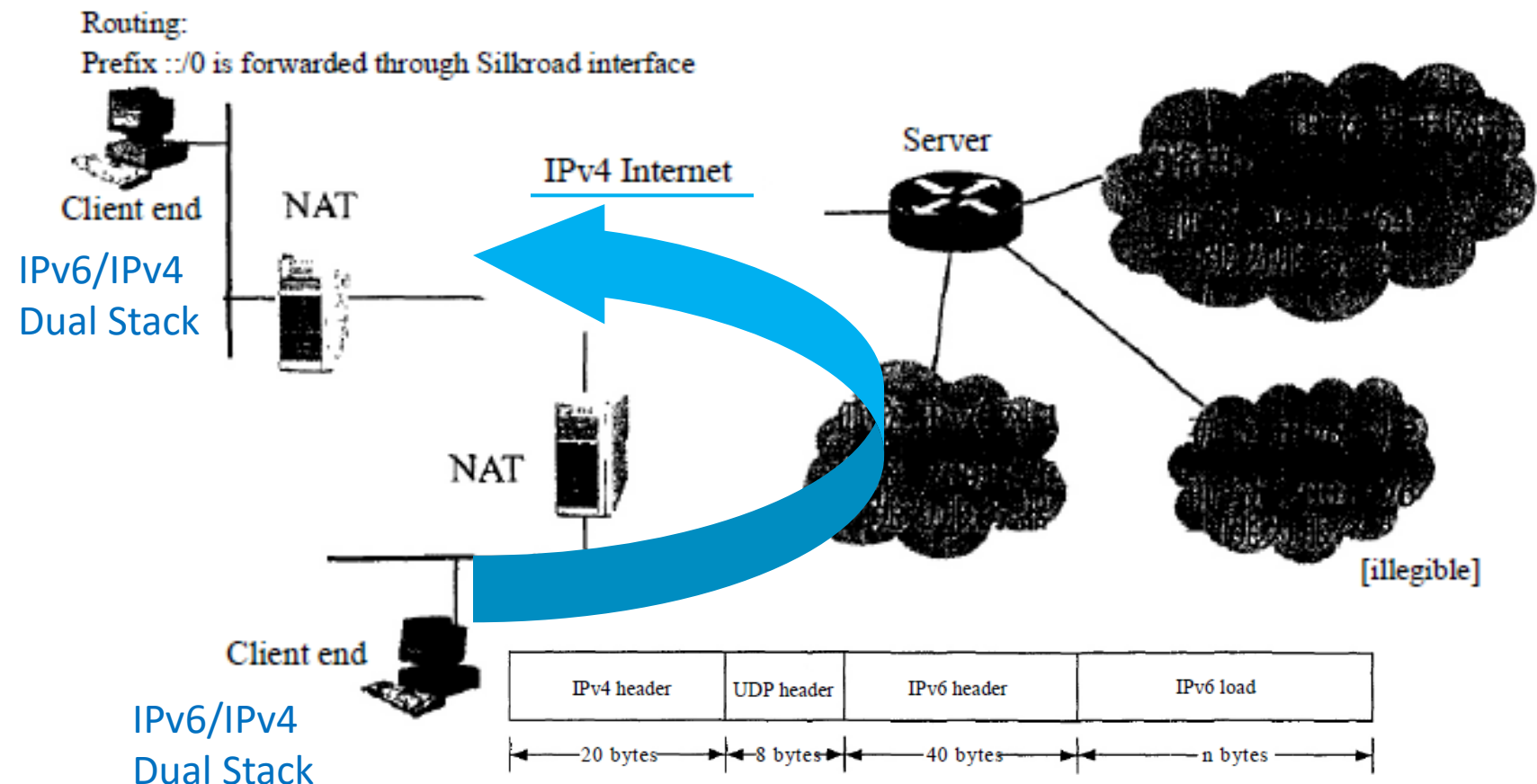


Fig. 4

Fig. 2

Wu's "Silkroad" Solution

- Wu uses initialization packets and maintaining packets to maintain state tables

"In order to maintain the mapping relation in NAT, e.g. "cone" NAT's <source address, source port, destination address, destination port>. The client end needs to send data packet to NAT periodically, we call such data packet as the maintaining packet, as shown in Attached Fig. 3."

EX1039 at 12

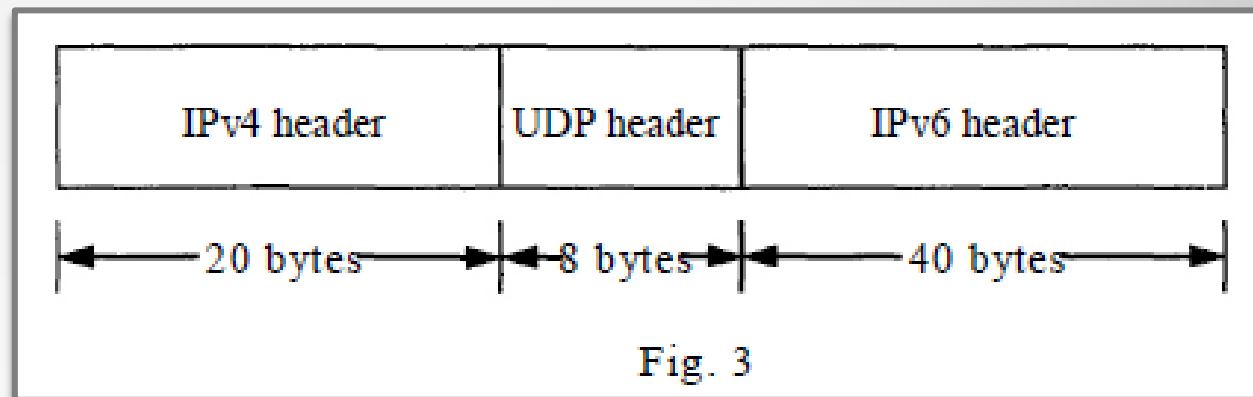


Fig. 3

EX1039 Fig. 3

[19] State Intellectual Property Office of PRC

[51] Int. Cl.

H04L 12/28

[12] Patent Application Publication

H04L 29/06 H04Q 3/00

H04Q 3/545



[21] Application No.: 03158973.1

[43] Publication Date: September 1st, 2004

[11] Patent NO.: CN 1525699A

[22] Application Date: September 17th, 2003

[21] Application No.: 03158973.1

[71] Applicant: The Institute of Computing Technology of the Chinese Academy of Sciences
Address: No. 6, Kexueyuan South Road,
Zhongguancun, Haidian District, Beijing
100080

[74] Patent agency: China Science Patent & Trademark Agent Ltd.
Agent: ZHOU Guocheng

[72] Inventor: WU Xianguo, LIU Min, ZHANG Tianle,
SHI Jinglin, LI Zhongcheng

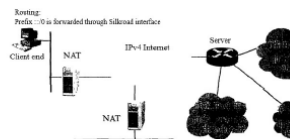
Claims: 6 pages
Specification: 8 pages
Drawings: 5 pages

[54] Title of Invention

An automatic tunnel method capable of traversing network address translation

[57] Abstract

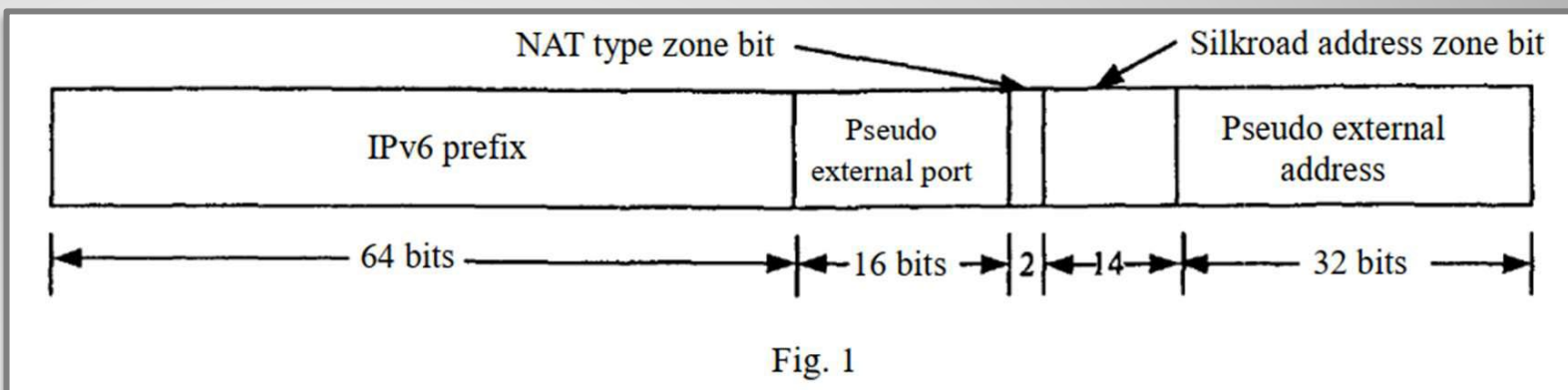
The present invention involves the field of Internet technology, a kind of automatic tunnel method capable of traversing NAT (Network Address Translation), i.e. this tunnel technology allows the tunnel body to have any type and any number of NAT, it is a kind of new tunnel technology in the transition period from IPv4 Internet to IPv6 Internet. The aim is to make the IPv6/IPv4 dual-stack nodes within NAT field to obtain the global end-to-end IPv6 connection. By using this tunnel technology, the IPv6/IPv4 dual-stack nodes within NAT field will communicate with the IPv6 nodes outside NAT field through the intermediate server, and will communicate with other the IPv6/IPv4 dual-stack nodes within NAT field.



ISSN 1008-4274

Wu's "Silkroad" Solution

- Silkroad address includes a "Pseudo external port" assigned by the server during initialization:



“♦ Pseudo external port:

The external port (NAT-mapped port) and 0xFFFF and/or the subsequent 16-bit numerical value. The SilkRoad client end send an initialized data packet to the server after it is started, the UDP port of this packet is mapped to a different port when it passes NAT, we call it as the external port.

The server obtains this port from the received initialized data packet.”

[19] State Intellectual Property Office of PRC

[51] Int. Cl.

H04L 12/28

[12] Patent Application Publication

H04L 29/06 H04Q 3/00

H04Q 3/545

[21] Application No.: 03158973.1

[43] Publication Date: September 1st, 2004

[11] Patent NO.: CN 1525699A

[22] Application Date: September 17th, 2003

[21] Application No.: 03158973.1

[71] Applicant: The Institute of Computing Technology of the Chinese Academy of Sciences
Address: No. 6, Kexueyuan South Road,
Zhongguancun, Haidian District, Beijing
100080

[74] Patent agency: China Science Patent & Trademark Agent Ltd.
Agent: ZHOU Guocheng

[72] Inventor: WU Xianguo, LIU Min, ZHANG Tianle,
SHI Jinglin, LI Zhongcheng

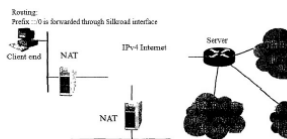
Claims: 6 pages
Specification: 8 pages
Drawings: 5 pages

[54] Title of Invention

An automatic tunnel method capable of traversing network address translation

[57] Abstract

The present invention involves the field of Internet technology, a kind of automatic tunnel method capable of traversing NAT (Network Address Translation), i.e. this tunnel technology allows the tunnel body to have any type and any number of NAT, it is a kind of new tunnel technology in the transition period from IPv4 Internet to IPv6 Internet. The aim is to make the IPv6/IPv4 dual-stack nodes within NAT field to obtain the global end-to-end IPv6 connection. By using this tunnel technology, the IPv6/IPv4 dual-stack nodes within NAT field will communicate with the IPv6 nodes outside NAT field through the intermediate server, and will communicate with other the IPv6/IPv4 dual-stack nodes within NAT field.



ISSN 1008-4274

Wu's "Silkroad" Solution

[19] State Intellectual Property Office of PRC

[51] Int. Cl.
H04L 12/28



[12] Patent Application Publication

H04L 29/06 H04Q 3/00
H04Q 3/545

[21] Application No.: 03158973.1

[43] Publication Date: September 1st, 2004

[11] Patent NO.: CN 1525699A

[22] Application Date: September 17th, 2003

[21] Application No.: 03158973.1

[71] Applicant: The Institute of Computing Technology of
the Chinese Academy of Sciences
Address: No. 6, Kexueyuan South Road,
Zhongguancun, Haidian District, Beijing
100080

[74] Patent agency: China Science Patent &
Trademark Agent Ltd.
Agent: ZHOU Guocheng

[72] Inventor: WU Xianguo, LIU Min, ZHANG Tianle,
SHI Jinglin, LI Zhongcheng

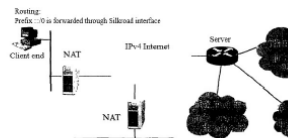
Claims: 6 pages
Specification: 8 pages
Drawings: 5 pages

[54] Title of Invention

An automatic tunnel method capable of traversing
network address translation

[57] Abstract

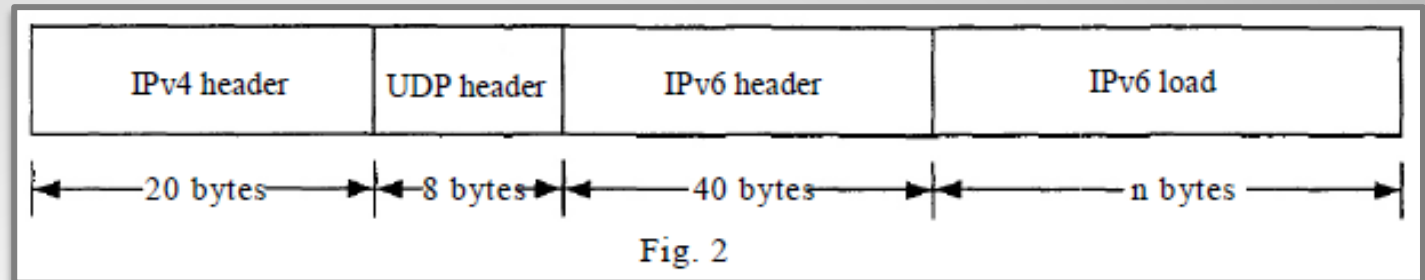
The present invention involves the field of Internet
technology, a kind of automatic tunnel method capable
of traversing NAT (Network Address Translation), i.e.
this tunnel technology allows the tunnel body to have
any type and any number of NAT, it is a kind of new
tunnel technology in the transition period from IPv4
Internet to IPv6 Internet. The aim is to make the
IPv6/IPv4 dual-stack nodes within NAT field to obtain
the global end-to-end IPv6 connection. By using this
tunnel technology, the IPv6/IPv4 dual-stack nodes
within NAT field will communicate with the IPv6 nodes
outside NAT field through the intermediate server, and
will communicate with other the IPv6/IPv4 dual-stack
nodes within NAT field.



ISSN 1008-4274

Published by Intellectual Property Publishing House, Juniper Exhibit 1039, page 2

- The Silkroad data packet is an IPv6 data packet encapsulated in IPv4:



“● IPv4 header:

The source IPv4 address is the IPv4 address of the client end (private address), the destination IPv4 address is the IPv4 address of the server (if the destination is the ordinary IPv6 node) or the external address of the client end mapped by NAT (if the destination is another client end).

● UDP header:

The source port is 5188, the destination port is 5188 (if the destination is the ordinary IPv6 node) or the external port of the client end mapped by NAT of the counterparty (if the destination is another client end).

● IPv6 header:

It includes the source IPv6 address and the destination IPv6 address, wherein at least one is the SilkRoad address.”

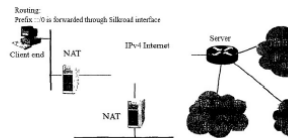
A POSITA Would Not Look To Wu To Modify Li



[54] Title of Invention
An automatic tunnel method capable of traversing
network address translation

[57] Abstract

The present invention involves the field of Internet technology, a kind of automatic tunnel method capable of traversing NAT (Network Address Translation), i.e. this tunnel technology allows the tunnel body to have any type and any number of NAT, it is a kind of new tunnel technology in the transition period from IPv4 Internet to IPv6 Internet. The aim is to make the IPv6/IPv4 dual-stack nodes within NAT field to obtain the global end-to-end IPv6 connection. By using this tunnel technology, the IPv6/IPv4 dual-stack nodes within NAT field will communicate with the IPv6 nodes outside NAT field through the intermediate server, and will communicate with other the IPv6/IPv4 dual-stack nodes within NAT field.

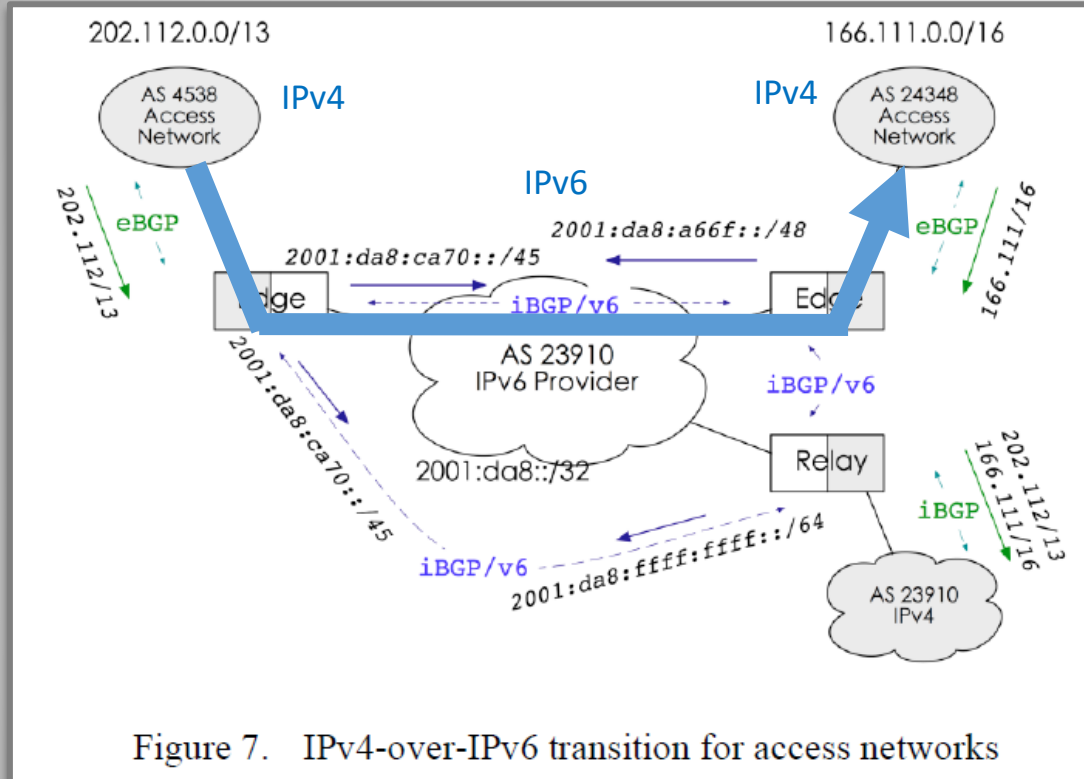


ISSN 1008-4274

- Li and Wu are directed to unrelated problems
- Wu uses a “stateful system” that would never be combined with Li

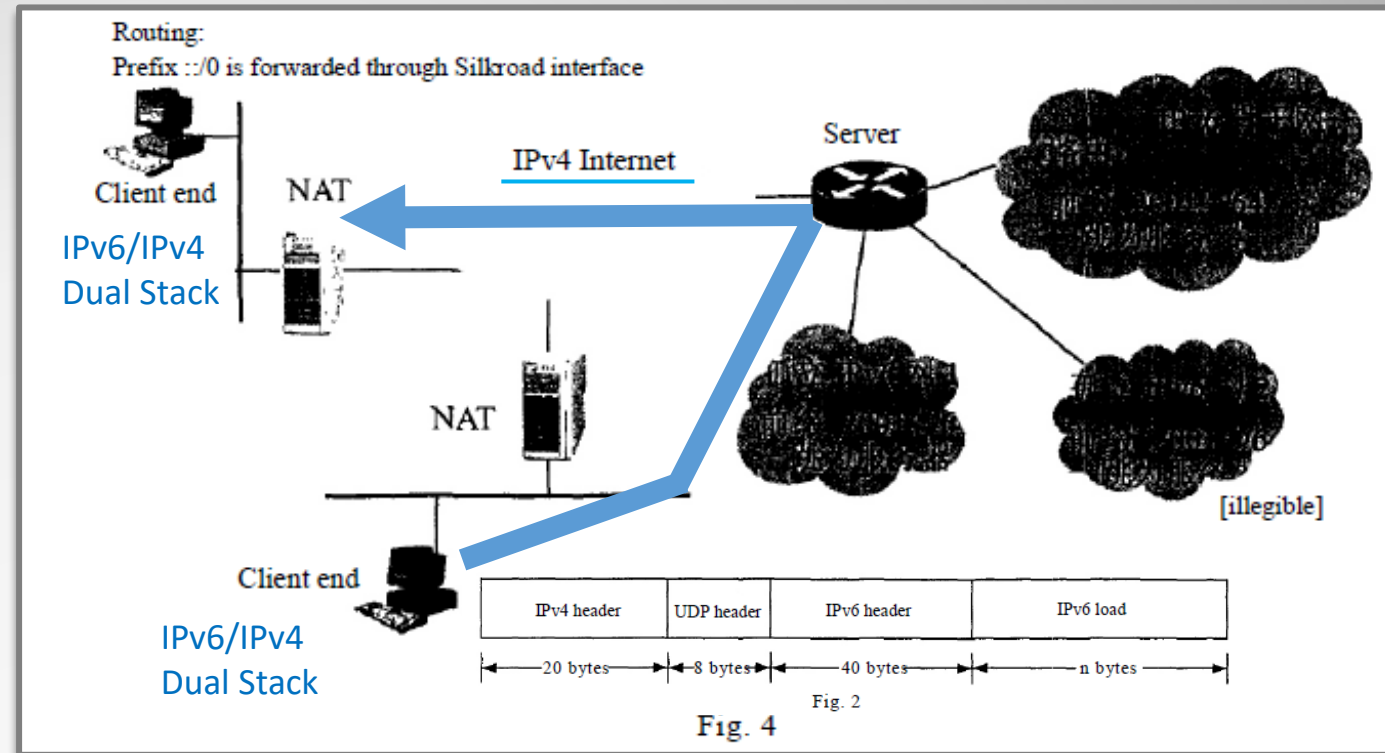
Wu And Li Address Opposite Problems

Li addresses communications between IPv4 hosts across IPv6 networks:



EX1037 Fig. 7

Wu describes transporting IPv6 packets across an IPv4 network:



EX1039 Figs. 2, 4

Wu Uses A “Stateful System” That Would Not Be Combined With Li

- Li is a stateless system:

“[T]he proposed one is automatic and stateless for end nodes, without explicit tunneling.”

EX1037, 1

- Wu is stateful:

“[The] [e]xternal port is the port mapped by NAT and 0xFFFF and/or the subsequent 16-bit numerical value.... the client end or the server will periodically send data packets to NAT to maintain such mapping relation, thus, *the NAT translation table always keeps this mapping relation....*”

EX1039, 3 (emphasis added)

Wu Uses A “Stateful System” That Would Never Be Combined With Li

- The ‘844 Patent and the art teach away from stateful systems:

“A solution based on NAT-PT that is not stateless *is not to be recommended*. This *would degrade the service provided* as value-added services linked to port forwarding configured by clients would not work”

EX1001, 13:43-46 (emphasis added)

“With the address-mapping rule commonly known within the autonomous domain, IPv4 source and destination addresses in a packet can be translated into their IPv6 version *without any explicitly stored states*, as described in Fig. 2.”

EX1037 at 3 (emphasis added)

The '844 Patent

Key Points

- All Grounds:
 - Li does not disclose separate IPv4 and IPv6 domains
- Ground 1:
 - Li-2 is not prior art
 - A POSITA would not combine Li and Li-2
- Ground 2:
 - There is no evidence of simultaneous invention
- **Ground 3:**
 - Li and Wu would not have been combined
 - **Wu does not teach the claimed constructed destination address**

Wu Does Not Describe The Claimed Destination Port Number

- A POSITA would not understand Wu’s “pseudo external port”

“[The] [e]xternal port is the port mapped by NAT and 0xFFFF and/or the subsequent 16-bit numerical value”

EX1039, 3

- Wu does not teach including a destination port number in a constructed address of an IPv6 packet

“[T]he destination port is the extracted external address”

EX1039, 16

END