Network Working Group
Request for Comments: 1385

Z. Wang
University College London

November 1992

EIP: The Extended Internet Protocol
A Framework for Maintaining Backward Compatibility

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Summary

The Extended Internet Protocol (EIP) provides a framework for solving the problem of address space exhaustion with a new addressing and routing scheme, yet maintaining maximum backward compatibility with current IP. EIP can substantially reduce the amount of modifications needed to the current Internet systems and greatly ease the difficulties of transition. This is an "idea" paper and discussion is strongly encouraged on Big-Internet@munnari.oz.au.

Introduction

The Internet faces two serious scaling problems: address exhaustion and routing explosion [1-2]. The Internet will run out of Class B numbers soon and the 32-bit IP address space will be exhausted altogether in a few years time. The total number of IP networks will also grow to a point where routing algorithms will not be able to perform routing based a flat network number.

A number of short-term solutions have been proposed recently which attempt to make more efficient use of the the remaining address space and to ease the immediate difficulties [3-5]. However, it is important that a long term solution be developed and deployed before the 32-bit address space runs out.

An obvious approach to this problem is to replace the current IP with a new internet protocol that has no backward compatibility with the current IP. A number of proposals have been put forward: Pip[7], Nimrod [8], TUBA [6] and SIP [14]. However, as IP is really the cornerstone of the current Internet, replacing it with a new "IP" requires fundamental changes to many aspects of the Internet system (e.g., routing, routers, hosts, ARP, RARP, ICMP, TCP, UDP, DNS, FTP).

Migrating to a new "IP" in effect creates a new "Internet". The

development and deployment of such a new "Internet" would take a very large amount of time and effort. In particular, in order to maintain interoperability between the old and new systems during the transition period, almost all upgraded systems have to run both the new and old versions in parallel and also have to determine which version to use depending on whether the other side is upgraded or not.

Let us now have a look at the detailed changes that will be required to replace the current IP with a completely new "IP" and to maintain the interoperability between the new and the old systems.

1) Border Routers: Border routers have to be upgraded and to provide address translation service for IP packets across the boundaries. Note that the translation has to be done on the outgoing IP packets as well as the in-coming packets to IP hosts.

2) Subnet Routers: Subnet Routers have to be upgraded and have to deal with both the new and the old packet formats.

3) Hosts: Hosts have to be upgraded and run both the new and the old protocols in parallel. Upgraded hosts also have to determine whether the other side is upgraded or not in order to choose the correct protocol to use.

4) DNS: The DNS has to be modified to provide mapping for domain names and new addresses.

5) ARP/RARP: ARP/RARP have to be modified, and upgraded hosts and routers have to deal with both the old and new ARP/RARP packets.

6) ICMP: ICMP has to be modified, and the upgraded routers have to be able to generate both both old and new ICMP packets. However, it may be impossible for a backbone router to determine whether the packet comes from an upgraded host or an IP host but translated by the border router.

7) TCP/UDP Checksum: The pseudo headers may have to be modified to use the new addresses.

8) FTP: The DATA PORT (PORT) command has to be changed to pass new addresses.

In this paper, we argue that an evolutionary approach can extend the addressing space yet maintain backward compatibility. The Extended Internet Protocol (EIP) we present here can be used as a framework by which a new routing and addressing scheme may solve the problem of address exhaustion yet maintain maximum backward compatibility to

current IP.

EIP has a number of very desirable features:

1) EIP allows the Internet to have virtually unlimited number of network numbers and over 10**9 hosts in each network.

2) EIP is flexible to accommodate most routing and addressing schemes, such as those proposed in Nimrod [8], Pip [7], NSAP [9] and CityCodes [10]. EIP also allows new fields such as Handling Directive [7] or CI [11] to be added.

3) EIP can substantially reduce the amount of modifications to current systems and greatly ease the difficulties in transition. In particular, it does not require the upgraded hosts and subnet routers to run two set of protocols in parallel.

4) EIP requires no changes to all assigned IP addresses and subnet structures in local are networks. and requires no modifications to ARP/RARP, ICMP, TCP/UDP checksum.

5) EIP can greatly ease the difficulties of transition. During the transition period, no upgrade is required to the subnet routers. EIP hosts maintain full compatibility with IP hosts within the same network, even after the transition period. During the transition period, IP hosts can communicate with any hosts in other networks via a simple translation service.

In the rest of the paper, IP refers to the current Internet Protocol and EIP refers to the Extended Internet Protocol (EIP is pronounced as "ape" - a step forward in the evolution :-).

Extended Internet Protocol (EIP)

The EIP header format is shown in Figure 1 and the contents of the header follows.

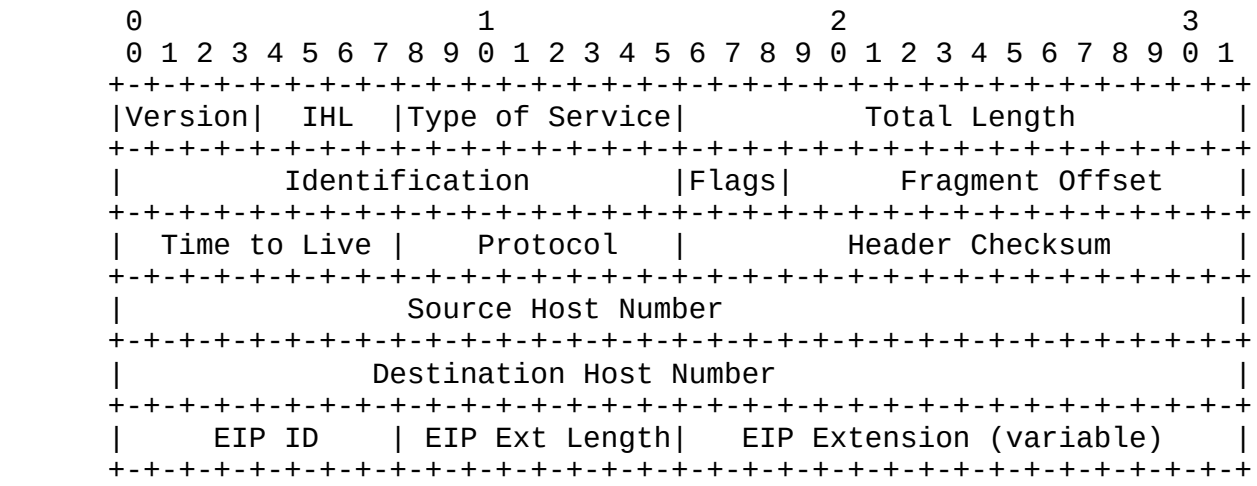

Figure 1: EIP Header Format

Version: 4 bits

The Version field is identical to that of IP. This field is set purely for compatibility with IP hosts. It is not checked by EIP hosts.

IHL: 4 bits

Internet Header Length is identical to that of IP. IHL is set to the length of EIP header purely for compatibility with IP. This field is not checked by EIP hosts. see below the EIP Extension Length field for more details)

Type of Service: 8 bits

The ToS field is identical to that of IP.

Total Length: 16 bits

The Total Length field is identical to that of IP.

Identification: 16 bits

The Identification field is identical to that of IP.

Flags: 3 bits

The Flags field is identical to that of IP.

Fragment Offset: 13 bits

The Fragment Offset field is identical to that of IP.

Time to Live: 8 bits

The Time to Live field is identical to that of IP.

Protocol: 8 bits

The Protocol field is identical to that of IP.

Header Checksum: 16 bits

The Header Checksum field is identical to that of IP.

Source Host Number: 32 bits

The Source Host Number field is used for identifying the source host but is unique only within the source network (the equivalent of the host portion of the source IP address).

Destination Host Number: 32 bits

The Destination Host Number field is used for identifying the destination host but is unique only within the destination network (the equivalent of the host portion of the destination IP address).

EIP ID: 8 bits

The EIP ID field equals to 0x8A. The EIP ID value is chosen in such a way that, to IP hosts and IP routers, an EIP appears to be an IP packet with a new IP option of following parameters:

COPY	CLASS	NUMBER	LENGTH	DESCRIPTION
1	0	TBD	var	

Option: Type=TBD

EIP Extension Length: 8 bits

The EIP Extension Length field indicates the total length of the EIP ID field, EIP Extension Length field and the EIP Extension field in octets. The maximum length that the IHL field above can specify is 60 bytes, which is considered too short in future. EIP hosts actually use the EIP Extension Length field to calculate the total header length:

The total header length = EIP Extension Length + 20.

The maximum header length of an EIP packet is then 276 bytes.

EIP Extension: variable

The EIP Extension field holds the Source Network Number, Destination Network Number and other fields. The format of the Extension field is not specified here. In its simplest form, it can be used to hold two fixed size fields as the Source Network Number and Destination Network Number as the extension to the addressing space. Since the Extension field is variable in length, it can accommodate almost any routing and addressing schemes. For example, the Extension field can be used to hold "Routing Directive" etc specified in Pip [7] or "Endpoint IDs" suggested in Nimrod [8], or the "CityCode" [10]. It can also hold other fields such as the "Handling Directive" [7] or "Connectionless ID" [11].

EIP achieves maximum backward compatibility with IP by making the extended space appear to be an IP option to the IP hosts and routers.

When an IP host receives an EIP packets, the EIP Extension field is safely ignored as it appears to the IP hosts as an new, therefore an unknown, IP option. As a result, there is no need for translation for in-coming EIP packets destined to IP hosts and there is also no need for subnet routers to be upgraded during the transition period see later section for more details).

EIP hosts or routers can, however, determine whether a packet is an IP packet or an EIP packet by examining the EIP ID field, whose position is fixed in the header.

The EIP Extension field holds the Source and Destination Network Numbers, which are only used for communications between different networks. For communications within the same network, the Network Numbers may be omitted. When the Extension field is omitted, there is little difference between an IP packet and an EIP packet. Therefore, EIP hosts can maintain completely compatibility with IP hosts within one network.

In EIP, the Network Numbers and Host Numbers are separate and the IP address field is used for the Host Number in EIP. There are a number of advantages:

1) It maintains full compatibility between IP hosts and EIP hosts for communications within one network. Note that the Network Number is not needed for communications within one network. A

host can omit the Extension field if it does not need any other information in the Extension field, when it communicates with another host within the same network.

2) It allows the IP subnet routers to route EIP packet by treating the Host Number as the IP address during the transition period, therefore the subnet routers are not required to be updated along the border routers.

3) It allows ARP/RARP to work with both EIP and IP hosts without any modifications.

4) It allows the translation at the border routers much easier. During the transition period when the IP addresses are still unique, the network portion of the IP addresses can be directly extracted and mapped to EIP Network Numbers.

Modifications to IP Systems

In this section, we outline the modifications to the IP systems that are needed for transition to EIP. Because of the similarity between the EIP and IP, the amount of modifications needed to current systems are substantially reduced.

1) Network Numbers: Each network has to be assigned a new EIP Network Number based on the addressing scheme used. The mapping between the IP network numbers and the EIP Network Numbers can be used for translation service (see below).

2) Host Numbers: There is no need for assigning EIP Host Numbers. All existing hosts can use their current IP addresses as their EIP Host Numbers. New machines may be allocated any number from the 32-bit Host Number space since the structure posed on IP addressing is no longer necessary. However, during the transition, allocation of EIP Host Numbers should still follow the IP addressing rule, so that the EIP Host Numbers are still globally unique and can still be interpreted as IP addresses. This will allow a more gradual transition to EIP (see below).

3) Translation Service: During the transition period when the EIP Host Numbers are still unique, an address translation service can be provided to IP hosts that need communicate with hosts in other networks cross the upgraded backbone networks. The translation service can be provided by the border routers. When a border router receives an IP packet, it obtains the Destination Network Number by looking up in the mapping table between IP network numbers and EIP Network Numbers. The border router then adds the Extension field with the Source and Destination Network

Numbers into the packet, and forwards to the backbone networks. It is only necessary to translate the out-going IP packets to the EIP packets. There is no need to translate the EIP packets back to IP packets even when they are destined to IP hosts. This is because that the Extension field in the EIP packets appears to IP hosts just an unknown IP option and is ignored by the IP hosts during the processing.

4) Border Routers: The new EIP Extension has to be implemented and routing has to be done based on the Network Number in the EIP Extension field. The border routers may have to provide the translation service for out-going IP packets during the transition period.

5) Subnet Routers: No modifications are required during the transition period when EIP Host Numbers (which equals to the IP addresses) are still globally unique. The subnet routing is carried out based on the EIP Host Numbers and when the EIP Host IDs are still unique, subnet routers can determine, by treating the EIP Host Number as the IP addresses, whether a packet is destined to remote networks or not and forward correctly. The Extension field in the EIP packets also appear to the IP subnet routers an unknown IP option and is ignored in the processing. However, subnet routers eventually have to implement the EIP Extension and carry out routing based on Network Numbers when EIP Host Numbers are no longer globally unique.

6) Hosts: The EIP Extension has to be implemented. routing has to be done based on the Network Number in the EIP Extension field, and also based on the Host Number and subnet mask if subnetting is used. IP hosts may communication with any hosts within the same network at any time. During the transition period when the EIP Host Numbers are still unique, IP hosts can communicate with any hosts in other network via the translation service.

7) DNS: A new resource record (RR) type "N" has to be added for EIP Network Numbers. The RR type "A", currently used for IP addresses, can still be used for EIP Host Numbers. RR type "N" entries have to be added and RR type "PTR" to be updated. All other entries remain unchanged.

8) ARP/RARP: No modifications are required. The ARP and RARP are used for mapping between EIP Host Numbers and physical addresses.

9) ICMP: No modifications are required.

10) TCP/UDP Checksum: No modifications are required. The pseudo

header includes the EIP Source and Destination IDs instead of the source and destination IP addresses.

11) FTP: No modifications are required during the transition period when the IP hosts can still communicate with hosts in other networks via the translation service. After the transition period, however, the "DATA Port (Port)" command has to be modified to pass the port number only and ignore the IP address. A new FTP command may be created to pass both the port number and the EIP address to allow a third party to be involved in the file transfer.

Transition to EIP

In this section, we outline a plan for transition to EIP.

EIP can greatly reduce the complexity of transition. In particular, there is no need for the updated hosts and subnet routers to run two protocols in parallel in order to achieve interoperability between old and new systems. During the transition, IP hosts can still communicate with any machines in the same network without any changes. When the EIP Host Numbers (i.e., the 32-bit IP addresses) are still globally unique, IP hosts can contact hosts in other networks via translation service provided in the border routers.

The transition goes as follows:

Phase 0:
- a) Choose an addressing and routing scheme for the Internet.
- b) Implement the routing protocol.
- c) Assign new Network Numbers to existing networks.

Phase 1:
- a) Update all backbone routers and border routers.
- b) Update DNS servers.
- c) Start translation service.

Phase 2:
- a) Update first the key hosts such as mail servers, DNS servers, FTP servers and central machines.
- b) Update gradually the rest of the hosts.

Phase 3:
- a) Update subnet routers
- b) Withdraw the translation service.

The translation service can be provided as long as the Host IDs (i.e., the 32-bit IP address) are still globally unique. When the IP

address space is exhausted, the translation service will be withdrawn and the remaining IP hosts can only communicate with hosts within the the same network. At the same time, networks can use any numbers in the 32-bit space for addressing their hosts.

Related Work

A recent proposal called IPAE by Hinden and Crocker also attempts to minimize the modifications to the current IP system yet to extend the addressing space [12]. IPAE uses encapsulation so that the extended space is carried as IP data. However, it has been found that the 64 bits IP data returned by an ICMP packet is too small to hold the Global IP addresses. Thus, when a router receives an ICMP generated by an old IP host, it is not able to convert it into a proper ICMP packet. More details can be found in [13].

Discussions

EIP does not necessary increase the header length significantly as most of the fields in the current IP will be still needed in the new internet protocol. There are debates as to whether fragmentation and header checksum are necessary in the new internet protocol but no consensus has been reached.

EIP assumes that IP hosts and routers ignore unknown IP option silently as required by [15,16]. Some people have expressed some concerns as to whether current IP routers and hosts in the Internet can deal with unknown IP options properly.

In order to look into the issues further, we carried out a number of experiments over the use of IP option. We selected 35 hosts over 30 countries across the Internet. A TCP test program (based on ttcp.c) then transmitted data to the echo port (tcp port 7) of each of the hosts. Two tests were carried out for each host, one with an unknown option (type 0x8A, length 40 bytes) and the other without any options.

It is difficult to ensure that the conditions under which the two tests run are identical but we tried to make them as close as possible. The two tests (test-opt and test-noopt) run on the same machine a Sun4) in parallel, i.e., "test-opt& ; test-noopt&" and then again in the reverse order, i.e., "test-noopt& ; test-opt&", so each test pair actually run twice. Each host was ping'ed before the tests so that the domain name information was cached before the name lookup.

The experiments were carried out at three sites: UCL, Bellcore and Cambridge University. The tcp echo throughput (KB/Sec) results are

listed in Appendix.

The results show that the IP option was dealt with properly and there is no visible performance difference under the test setup.

References

[1] Chiappa, N., "The IP Addressing Issue", Work in Progress, October 1990.

[2] Clark, D., Chapin, L., Cerf, V., Braden, R., and R. Hobby, "Towards the Future Architecture", RFC 1287, MIT, BBN, CNRI, ISI, UCDavis , December 1991.

[3] Solensky, F. and F. Kastenholz, "A Revision to IP Address Classifications", Work in Progress, March 1992.

[4] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Supernetting: an Address Assignment and Aggregation Strategy", RFC 1338, BARRNet, cisco, Merit, OARnet, June 1992.

[5] Wang, Z., and J. Crowcroft, "A Two-Tier Address Structure for the Internet: a solution to the problem of address space exhaustion", RFC 1335, University College London, May 1992.

[6] Callon, R., "TCP and UDP with Bigger Addresses (TUBA), a Simple Proposal for Internet Addressing and Routing", RFC 1347, DEC, June 1992.

[7] Tsuchiya, P., "Pip: The 'P' Internet Protocol", Work in Progress, May 1992

[8] Chiappa N., "A New IP Routing and Addressing Architecture", Work in Progress, 1992.

[9] Colella, R., Gardner, E., and R. Callon, "Guidelines for OSI NSAP Allocation in the Internet" RFC 1237, NIST, Mitre, DEC, July 1991.

[10] Deering, S., "City Codes: An Alternative Scheme for OSI NSAP Allocation in the Internet", Work in Progress, January 1992.

[11] Clark, D., "Building routers for the routing of tomorrow", in his message to Big-Interent@munnari.oz.au, 14 July 1992.

[12] Hinden, R., and D. Crocker, "A Proposal for IP Address Encapsulation (IPAE): A Compatible Version of IP with Large Addresses", Work in Progress, July 1992.

[13] Partridge, C., "Re: Note on implementing IPAE", in his message to Big-Interent@munnari.oz.au, 17 July 1992.

[14] Deering, S., "SIP: Simple Internet Protocol", Work in Progress, September 1992.

[15] Braden, R., Editor, "Requirements for Internet Hosts -- Communication Layers", RFC 1122, ISI, October 1989.

[16] Almquist, P., Editor, "Requirements for IP Routers", Work in Progress, October 1991.

Appendix

Throughput Test from UCL (sartre.cs.ucl.ac.uk)

Destination Host	test-noopt	test-opt
oliver.cs.mcgill.ca	1.128756	1.285345
oliver.cs.mcgill.ca	1.063096	1.239709
bertha.cc.und.ac.za	0.094336	0.043917
bertha.cc.und.ac.za	0.075681	0.057120
vnet3.vub.ac.be	2.090622	2.228181
vnet3.vub.ac.be	1.781374	1.692740
itdsrv1.ul.ie	1.937596	2.062579
itdsrv1.ul.ie	1.928313	1.936784
sunic.sunet.se	11.064797	11.724055
sunic.sunet.se	10.861720	10.840306
pascal.acm.org	2.463790	0.810133
pascal.acm.org	1.619088	0.860198
iti.gov.sg	1.565320	1.983795
iti.gov.sg	1.564788	1.921803
rzusuntk.unizh.ch	9.903805	11.335920
rzusuntk.unizh.ch	9.597806	10.678098
funet.fi	9.897876	9.382925
funet.fi	10.487118	11.023745
odin.diku.dk	5.851407	5.482946
odin.diku.dk	5.992257	6.243283
cphkvx.cphk.hk	0.758044	0.844406
cphkvx.cphk.hk	0.784532	0.745606
bootes.cus.cam.ac.uk	28.341705	29.655824
bootes.cus.cam.ac.uk	24.804125	23.240990
pesach.jct.ac.il	1.045922	1.115802
pesach.jct.ac.il	1.330429	0.978184
sun1.sara.nl	10.546733	11.500778
sun1.sara.nl	9.624833	10.214136
cocos.fuw.edu.pl	1.747777	1.702324
cocos.fuw.edu.pl	1.676151	1.716435

apple.com	4.449559	4.145081
apple.com	6.431675	5.520443
gorgon.tf.tele.no	1.199810	1.374546
gorgon.tf.tele.no	0.508642	0.993261
kogwy.cc.keio.ac.jp	3.626448	3.249590
kogwy.cc.keio.ac.jp	3.913777	4.094849
exu.inf.puc-rio.br	1.913925	1.795235
exu.inf.puc-rio.br	1.154936	1.114775
inria.inria.fr	2.299561	0.599665
inria.inria.fr	1.219282	0.873672
kum.kaist.ac.kr	0.252704	0.254199
kum.kaist.ac.kr	0.236196	0.172367
sunipc1.labein.es	1.398777	1.243588
sunipc1.labein.es	0.876177	0.602964
wifosv.wsr.ac.at	0.531153	0.803387
wifosv.wsr.ac.at	0.773935	0.557798
uunet.uu.net	7.813556	6.764543
uunet.uu.net	7.969203	6.657325
infnsun.aquila.infn.it	2.321197	2.402477
infnsun.aquila.infn.it	2.400196	2.695016
muttley.fc.ul.pt	0.545775	0.434672
muttley.fc.ul.pt	0.284124	0.266017
dmssyd.syd.dms.csiro.au	2.734685	2.857545
dmssyd.syd.dms.csiro.au	1.168154	1.462789
hamlet.caltech.edu	2.552804	2.897286
hamlet.caltech.edu	3.839141	2.407945
sztaki.hu	0.294196	0.403697
sztaki.hu	0.236260	0.388755
menvax.restena.lu	0.465066	0.515361
menvax.restena.lu	0.358646	0.511985
nctu.edu.tw	0.484372	0.816722
nctu.edu.tw	0.705733	1.109228
xalapa.lania.mx	0.899529	0.822544
xalapa.lania.mx	1.150058	0.881713
truth.waikato.ac.nz	1.438481	1.993749
truth.waikato.ac.nz	1.325041	1.833999

Throughput Test from Bellcore (latour.bellcore.com)

Destination Host	test-noopt	test-opt
oliver.cs.mcgill.ca	1.820014	2.128104
oliver.cs.mcgill.ca	1.979981	1.866815
bertha.cc.und.ac.za	0.099289	0.035877
bertha.cc.und.ac.za	0.118627	0.103763
vnet3.vub.ac.be	0.368476	0.694463
vnet3.vub.ac.be	0.443269	0.644050
itdsrv1.ul.ie	0.721444	0.960068
itdsrv1.ul.ie	0.713952	0.953275
sunic.sunet.se	2.989907	2.956766
sunic.sunet.se	2.100563	2.010292
pascal.acm.org	2.487185	3.896253
pascal.acm.org	1.944085	4.269323
iti.gov.sg	2.401733	2.735445
iti.gov.sg	2.950990	2.793121
rzusuntk.unizh.ch	4.094820	3.618023
rzusuntk.unizh.ch	2.952650	2.245001
funet.fi	6.703408	5.928008
funet.fi	7.389722	5.815122
odin.diku.dk	2.094152	2.450695
odin.diku.dk	5.362362	4.690722
cphkvx.cphk.hk	0.092698	0.106880
cphkvx.cphk.hk	0.496394	0.681994
bootes.cus.cam.ac.uk	2.632951	2.631322
bootes.cus.cam.ac.uk	3.717170	1.335914
pesach.jct.ac.il	0.684029	0.921621
pesach.jct.ac.il	0.390263	1.095265
sun1.sara.nl	3.186035	2.325166
sun1.sara.nl	3.053797	3.081236
cocos.fuw.edu.pl	0.154405	0.124795
cocos.fuw.edu.pl	0.120283	0.105825
apple.com	12.588979	12.957880
apple.com	13.861733	12.211125
gorgon.tf.tele.no	1.280217	1.112675
gorgon.tf.tele.no	0.243205	0.631096
kogwy.cc.keio.ac.jp	6.249789	5.075968
kogwy.cc.keio.ac.jp	3.387490	4.583511
exu.inf.puc-rio.br	2.089536	2.233711
exu.inf.puc-rio.br	2.476758	2.249439
inria.inria.fr	0.653974	0.866246
inria.inria.fr	0.739127	1.130521
kum.kaist.ac.kr	1.541682	1.312546
kum.kaist.ac.kr	0.906632	1.042793
sunipc1.labein.es	0.101496	0.091456
sunipc1.labein.es	0.054245	0.101585

wifosv.wsr.ac.at	1.044443	0.369528
wifosv.wsr.ac.at	0.596935	0.870377
uunet.uu.net	9.530348	8.999789
uunet.uu.net	8.941888	6.075660
infnsun.aquila.infn.it	1.619418	1.569645
infnsun.aquila.infn.it	1.156780	1.158000
muttley.fc.ul.pt	0.353632	0.416126
muttley.fc.ul.pt	0.221522	0.155505
dmssyd.syd.dms.csiro.au	3.433901	3.272839
dmssyd.syd.dms.csiro.au	3.408975	3.130188
hamlet.caltech.edu	5.367756	6.325031
hamlet.caltech.edu	4.828718	5.676571
sztaki.hu	0.301120	0.362481
sztaki.hu	0.253222	0.519892
menvax.restena.lu	0.364221	0.480789
menvax.restena.lu	0.456882	0.580778
nctu.edu.tw	0.246523	1.199412
nctu.edu.tw	0.423476	0.630833
xalapa.lania.mx	0.748642	0.607284
xalapa.lania.mx	0.716781	0.643030
truth.waikato.ac.nz	2.197595	2.072601
truth.waikato.ac.nz	2.489748	2.186684

Throughput Test from Cam U (cus.cam.ac.uk)

Destination Host	test-noopt	test-opt
oliver.cs.mcgill.ca	1.128756	1.285345
oliver.cs.mcgill.ca	1.063096	1.239709
bertha.cc.und.ac.za	0.031218	0.031221
bertha.cc.und.ac.za	0.034405	0.034925
vnet3.vub.ac.be	0.568487	0.731320
vnet3.vub.ac.be	0.558238	0.581415
itdsrv1.ul.ie	1.064302	1.284707
itdsrv1.ul.ie	0.852089	1.025779
sunic.sunet.se	7.179942	6.270326
sunic.sunet.se	5.772485	6.689160
pascal.acm.org	1.661248	1.726725
pascal.acm.org	1.557839	1.428193
iti.gov.sg	0.600616	0.926690
iti.gov.sg	0.772887	0.956636
rzusuntk.unizh.ch	3.645913	4.504969
rzusuntk.unizh.ch	1.853503	2.671272
funet.fi	4.190147	3.421110
funet.fi	2.270988	3.789678
odin.diku.dk	1.361227	0.993901
odin.diku.dk	1.977774	2.415716
cphkvx.cphk.hk	1.173451	1.298421
cphkvx.cphk.hk	1.151376	1.184210
bootes.cus.cam.ac.uk	269.589141	238.920081
bootes.cus.cam.ac.uk	331.203020	293.556436
pesach.jct.ac.il	0.343598	0.492202
pesach.jct.ac.il	0.582809	0.930958
sun1.sara.nl	1.529277	1.470571
sun1.sara.nl	0.896041	0.894923
cocos.fuw.edu.pl	0.131180	0.142239
cocos.fuw.edu.pl	0.137697	0.148895
apple.com	1.330794	0.453590
apple.com	0.856476	0.714661
gorgon.tf.tele.no	0.094793	0.099981
gorgon.tf.tele.no	0.167257	0.151625
kogwy.cc.keio.ac.jp	0.154681	0.178868
kogwy.cc.keio.ac.jp	1.095814	0.871496
exu.inf.puc-rio.br	0.454272	0.384484
exu.inf.puc-rio.br	0.705198	0.690708
inria.inria.fr	0.149511	0.150021
inria.inria.fr	0.071125	0.077257
kum.kaist.ac.kr	0.721184	0.549511
kum.kaist.ac.kr	0.250285	0.296195
sunipc1.labein.es	0.519284	0.491745
sunipc1.labein.es	0.990174	1.009475

wifosv.wsr.ac.at	0.360751	0.418554
wifosv.wsr.ac.at	0.344268	0.326605
uunet.uu.net	4.247430	3.305592
uunet.uu.net	3.139251	2.945469
infnsun.aquila.infn.it	0.480731	0.782631
infnsun.aquila.infn.it	0.230471	0.292273
muttley.fc.ul.pt	0.239624	0.334286
muttley.fc.ul.pt	0.586156	0.419485
dmssyd.syd.dms.csiro.au	3.630623	3.607504
dmssyd.syd.dms.csiro.au	1.743162	2.994665
hamlet.caltech.edu	5.897946	4.650703
hamlet.caltech.edu	5.118200	5.622022
sztaki.hu	0.338358	0.225206
sztaki.hu	0.113328	0.112637
menvax.restena.lu	0.224967	0.359237
menvax.restena.lu	0.452945	0.472345
nctu.edu.tw	2.549709	2.037245
nctu.edu.tw	2.229093	2.469851
xalapa.lania.mx	0.713586	0.810107
xalapa.lania.mx	0.612278	0.731705
truth.waikato.ac.nz	1.438481	1.993749
truth.waikato.ac.nz	1.325041	1.833999

Security Considerations

Security issues are not discussed in this memo.

Author’s Address

Zheng Wang
Dept of Computer Science
University College London
London WC1E 6BT, UK

EMail: z.wang@cs.ucl.ac.uk