# Comments & Discussions on ExIP (Extended IPv4)
# Following
# "IPv6 – Is There a Better Way?"
# Whitepaper on Viodi.com

September 18, 2015 at 8:25 am

New comment on your post "IPv6 - Is There a Better Way?"
Author: Napsterbater (IP: 38.66.197.240, 38.66.197.240)
E-mail: bojack1437@gmail.com
URL:
Comment:
Except a ton of devices and software would have to be updated to work with "ExIP", which none are capable of right now, while there are ton of IPv6 devices and software already out there, so you would have to basically start over on deploying the new specification.

You can see all comments on this post here:
http://viodi.com/2015/05/22/ipv6-is-there-a-better-way/#comments

Permalink: http://viodi.com/2015/05/22/ipv6-is-there-a-better-way/comment-page-1/#comment-52522

Reply

- Abraham Y. Chen

  September 18, 2015 at 9:08 am

  Yes, for the long term, new Edge Routers should be developed and deployed. On the other hand, if you recognize the fact that the SPR (Semi-Public Router) is an adjunct device to the current router architecture, the immediate deployment will be "stealth". Initially, SPR will be installed only where it is needed. And, to start with, the hardware modules already exist. Only firmware simplification effort is needed. ….

  Reply

  ○

> On 2015-09-18 12:21, Napsterbater wrote:
>
> September 18, 2015 at 9:21 am
>
> You are basically talking about CGNAT, which is already in use, it sucks. If behind one you lose the ability to receive connections from anyone in the world. And why develop new routers to handle new methods when a tone of devices and routers already handle IPv6.
>
> Even in your picture you have a router with the same subnet on two interfaces, a router cant have 192.168.2.0 which must be part of a /16 on the external interface then have 192.168.2.*** on the internal, routing doesn't work that way. If you can't even understand that, how should we feel about anything else you are proposing.

On Sat, Sep 19, 2015 at 3:50 PM, Abraham Y. Chen <aychen@avinta.com> wrote:
Hi, Napsterbater:

0) You might have looked at my proposal from a somewhat sophisticated angle. The fact of the matter is, the SPR (Semi-Public Router) concept is rather Simple and Straightforward. On the other hand, we made observations on a couple unpublicized facts that help to formulate the SPR.

1) "CGNAT": The proposed SPR is a rudimentary router. It has nothing to do with the CGNAT, not even the NAT commonly practiced in an RG (Residential Gateway). So, unlike a router equipped with NAT, SPR is very "transparent" in terms of initiating a session. It does not block a requesting packet, no matter which direction it comes from.

2) "a router can't have 192.168.2.0 which must be part of a /16 on the external interface then have 192.168.2.*** on the internal,": You might be referring to how a common RG router works that appears to be restricted to a single level routing within 192.168/16. RG is a "terminal" device as far as the Internet routing goes. It is slightly different from the general scheme of router hierarchy which is based on dividing the 32 bits of the IPv4 number into two parts, the network segment and the host identification. (The division used to be by the octet. Now, the division line is at the bit level.) Even under 192.168/16, consumer RG routers are mostly operating with 192.168.0/24, 192.168.1/24 or 192.168.2/24 (Occasionally, I have seen a couple products operating with 192.168.10/24.) which means that the manufacturers have already made one level of "manual routing through factory default" within 192.168/16, by preferring one of several network segments identified by 192.168.n/24 (where "n" equals to 0, 1, 2 or 10). Normally, either one of these works fine with a subnet mask of 255.255.255.0. However, if several hosts on the same physical network infrastructure are assigned with IP addresses belonging to more than one of these network segments, they can not network properly. Upon configured with 255.255.252.0 as the subnet mask, those hosts with n =

0, 1, 2 will be able to communicate. Those on 192.168.10/24 will only be able to join in when the subnet mask is further relaxed to 255.255.240.0. This is the principle of making SPR to route at 192.168.n/24 level and leave the existing RGs to route at the fourth octet level which is what they have been doing anyway.

Hope I am making some sense for you.

Regards,

Abe (2015--09-19 15:50)

On 2015-09-21 17:36, Napsterbater wrote:
You make no sense at all. None of this solve the fact of running out of IPv4 address.
----------------------------------
Napsterbater
bojack1437@gmail.com

On Tue, Sep 22, 2015 at 12:03 AM, Abraham Y. Chen <aychen@avinta.com> wrote:
Hi, Napsterbater:

0) Thanks for your candid comment. Yes, the IPv4 public address pool is running out according to the conventional wisdom that was based the original thinking of the Internet design.

1) However, if we look hard at what is the real purpose of such address pool, we can then search for existing (old) techniques that may be mimicked to deal with the need, while not breaking the IPv4 protocol (rules).

2) The fact that the three reserved private network address blocks, 10/8, 172.16/12 and 192.168/16 allow individuals to have so many identification numbers locally, (16M, 1M and 64K, respectively) yet not visible from Internet provides the basic clue to the ExIP solution. That is, all we need to do is to make part of such pool publicly assignable while not affecting the existing IPv4 based Internet operation. Then, the IPv4 address pool shortage issue becomes moot.

3) It turns out that the proposed Internet SPR is very much the same as the telephony PABX (Public Automatic Branch eXchange) that has been used for over half a century by business entities to get around the PSTN (Public Switched Telephone Network) phone number shortage. The difference is that the telephony numbering rule is flexible and open-ended because it grew longer as the service expanded from local to state, to country, and now to international. For Internet, the IPv4 numbering length was fixed at 32 bits from the start. So, it has a limit. However, if we treat the reserved private network

address blocks utilized by SPR as PABX extension numbers, we can apply significant, although finite, multiplication factors to each of the IPv4 addresses. This is the fundamental realization as analyzed by the simple math in Section 2 of the following whitepaper:

http://avinta.com/phoenix-1/home/IPv6Myth&InternetVsPSTN.pdf

3) The key trick here is that the SPR is making use of the addresses that existing Internet Core and Edge Routers are not allowed to act upon. Through SPR, however, each IPv4 public address becomes the focal point of 256 publicly assignable identification addresses.

4) For sure, this analogy is not apparent at the first look. It is based upon an in-depth appreciation of telephony switching concepts and numbering plans followed by a lot of soul searching efforts to dream up this proposal that is rather unorthodox, if examined from IT centric views.

5) If you could, I would urge you to browse through other whitepapers on Avinta's website:

A. The following provide you a chronological transition of our philosophical thinking started from focusing on extending PSTN and progressed to Internet:

http://avinta.com/aboutavinta-1/home/aahome.htm

B. The following are recent whitepapers that address both fields with the goal to converge the two:

http://avinta.com/phoenix.htm

Based on the first three documents, we realized the strong similarity between Internet and PSTN. What got your attention are those among the last three documents. They are kind of derivatives of derivatives. So, it will take some effort to see through. But, I do look forward to your further comments.

Regards,

Abe (2015-09-22 00:03)

On 2015-09-22 00:21, Napsterbater wrote:
My friends over at dslreports.com is what lead me to your site, specifically this thread http://www.dslreports.com/forum/r30299384-IPv6-Is-There-a-Better-Way

Even if your idea had a plausible chance of working, the world is already going IPv6, it has a 15+ year head start over this, you are still gonna have to upgrade most of the internet to work with this, Windows, Linux, Android, IOS (Apple) are all IPv6 ready, that's probably 99% of end user devices and servers, not to mention all of the routers and switches and firewalls that are already IPv6 aware, even if those features are not being used currently.

--------------------------------
Napsterbater
bojack1437@gmail.com

On Tue, Sep 22, 2015 at 11:11 AM, Abraham Y. Chen <aychen@avinta.com> wrote:
Hi, Napsterbater:

1) "My friends over at dslreports.com is what lead me to your site.": Thanks for clarifying where you came from. And, appreciate very much for copy-&-paste our exchanges to that website for sharing. I hope this thread of discussion will be productive.

2) "Even if your idea had a plausible chance of working,": Good, It sounds that you are beginning to suspect that there might be some merits behind the SPR and have the interest in digging deeper into it. For second opinion, you may want to have a closer look at the EnIP (Enhanced IPv4) work that our paper refers to. It is an independent idea with a slightly different approach and performance. But, it uses the same IPv4 Option mechanism that has been around since day one.

3) "the world is already going IPv6, it has a 15+ year head start over this.": Talking about history, well, SPR is not a new development but an adjunct enhancement to IPv4 that has as long history as the Internet itself which was started around 1983. The trouble being, IPv6 tries to replace IPv4, instead of to enhance it. That is why it takes so much effort but still moves slowly, and has a hard time to earn the heart of the mass.

4) "you are still gonna have to upgrade most of the Internet to work with this.": No, my statement to this aspect is a definitive negative. Please review the configuration definition of the SPR and its operation examples. We approached this general subject from the fundamental system engineering principles and disciplines that require minimum perturbation to an existing functional system for any purpose of expansion or enhancement. In this case, truly nothing in Internet is affected. To put in another way, the SPR may operate as a "stealth" building block as far as the Internet Core and Edge Routers are concerned. Even the RG does not need much simplification at all. Of course, in the long run, the SPR function should be integrated into the new ER design to consolidate the physical hardware. But, the last step is definitely optional during the initial deployment.

5) "all of the routers and switches and firewalls that are already IPv6 aware, even if those features are not being used currently.": Correct. However, are we obligated to use

them simply because the big guys have built them? Why not use something simpler and we are familiar with, particularly if everything promised by IPv6 is achievable by Extended IPv4? I know at least one major software company (through a senior staff) decided to have the IPv6 "capability" in their products just to be compatible, but, has no intention to promote it.

6) What we are talking about is actually the tip of an iceberg. For example, please look at the spelling of SPR (Semi-Public Router). Do you see any other way to spell this abbreviation out? The answer is actually embedded in our white-papers. ;-) Once you figured this out, we have a lot more to talk about.

7) To facilitate our conversation, I have taken the liberty to submit my Bio as attached. You may find a copy of the same on LinkedIn.com as well. If you could tell me a bit about yourself, it may expedite our conversation by being able to use more common expressions.

Regards,

Abe (2015-09-22 11:10)

On 2015-09-22 13:26, Napsterbater wrote:
2: Not at all, and I have heard of and looked at "EnIP" before, it also make no sense to try and use at this point in time.

3: Sure IPv4 has been around, since 1983, but you are basically proposing IPv4v2 (ver. 2), this is just as much of a replacement as IPv6 is, because a host using EnIP or your proposal cant really talk to a host not using it and vice versa, it has the same downside of IPv6 in that respect.

4: Again this makes no sense.

5: Because without them this has no chance anyways.

6:?

7: Again? Speak as actual network engineers would and it wouldn't be a problem.
----------------------------------
Napsterbater
bojack1437@gmail.com

On Wed, Sep 23, 2015 at 9:33 AM, Abraham Y. Chen <aychen@avinta.com> wrote:
Hi, Napsterbater:

1) Re: Ur. Pt. 2: The reason that I mentioned EnIP is because it similarly utilizes the Option mechanism in IPv4 header to be stealth through the Internet. I did not want to

comment on its actual technique, because it is rather involved if you follow through its deployment strategy. It also implicitly abandons the common RG characteristics. So, the hosts need be upgraded as well. ExIP basically tries to avoid these issues by focusing the implementation efforts in the SPR, so that the kick-off may be smoother.

2) Re: Ur. Pt. 3: "you are basically proposing IPv4v2 (ver. 2)": No. I believe that ExIP would be just like one of the "experiments" that have been assigned Option numbers during the past several decades (See URL below.). The Option information is part of the IPv4 header handled payload by design. There may be some extra processing, such as message exchanges for the extra information necessary to carry out these option functions. But, the protocol itself is not affected by the inclusion of any of these options. So, these even could not be qualified as IPv4 v1.1 yet.

http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml

3) Re: Ur. Pt. 3: " because a host using EnIP or your proposal cant really talk to a host not using it and vice versa,": This is true for the full deployment, because there is no free lunch and there is no magician in the tech world. We are not pretending that we have a silver bullet that can fix everything in one shot. The general philosophy that we follow is to keep the working system (the current IPv4 based Internet) undisturbed while introducing the enhancement (the ExIP). I can not speak for EnIP. Right from the beginning, we were very conscientious about this issue. This is why our plan proposes focusing everything related to ExIP to be within the SPR module. So that this is an optional add-on equipment for those who want to enjoy the benefits ahead of the mass. The general strategy is to put the SPR capability into new web servers. Then, the public can access it by having the SPR on the originating end which would be transparent to the end user / host. From consumers' perspective, this is basically a "bulletin board access" mode that the Internet is mostly being used for. Once the SPRs become popular, ExIP aware hosts may begin to address one another in a peer-to-peer manner.

4) Re: Ur. Pts. 4, 5: Correct, at the first look. You may change your opinion once we have cleared the next topic.

5) Re: Ur. Pt. 6?: Hint: Where does the octet used for the address extension operation come from?

6) Re: Ur. Pt. 7: Good. We should have no trouble to discuss the current topics. On the other hand, you may have to excuse my limited network vocabulary because I was primarily trained as a traditional telecommunications guy who gravitated to telephony systems, home networking, and now getting involved with the Internet. Sometimes, I may have the correct concept but use the incorrect terminology. Please excuse me. Thanks.

Regards,

Abe (2015-09-23 09:33)

On 2015-09-23 15:30, Napsterbater wrote:
Here is a good response from http://www.dslreports.com/forum/r30311098-

"This is a feeble attempt at partially solving the problem.  Any way you slice it, addresses are running out.  The only problem this solves is eliminating NAPT, thus restoring end-to-end connectivity.  This is nothing more than a weird, nonstandard form of IPIP tunnelling.

As I've seen on some sites, it seems awfully presumptive that all you have to do is insert around 4000 lines of code in your router (as opposed to 100x as much for IPv6 implementation) and everything is just hunkey-doorey.  There is around a 10 or so year IPv6 client code head start (e.g., Web browsers, Wireshark, just about anything you can imagine which is dual stack).  Without also implementing some sort of IPv6EnIP gateway, there's an AWFUL lot more development required than a few thousand lines of code in a router.  You might as well just implement IPv6 while you're at it instead of just a specific IPv6/EnIP gateway.  After all, it would seem to rely on AAAA records.

What about those unfortunate protocols, such as FTP, SIP, and SDP, which have IPv4 dotted quads embedded in them?  Howya gonna cope with that?

It seems the whole presumption is that almost all the other protocols (like ARP, DHCP, etc.) need minor or no updates.  I just can't see it.  It looks like much of it presumes the extra 32 bits of addressing get inserted or excised at something like a CPE router.  We are running out of the ability to address those individually already.  It's tough for me to conceive how this operates by slicing up an existing IPv4 address among multiple ISP customers.  IMHO, the far better solution is explicit assignment of 64 (or sometimes fewer) address bits to CPE, as is being done now with prefix delegation.

If you examine IANA's site, option 26 is not yet assigned, so any site referring to it as being an "existing option" speaks about it in a pure and not applied (like maths) way.  Sure, the number 26 exists, and it's not imaginary, but that doesn't mean a whole lot until IANA recognizes it.  Not only that, I'm going to guess IPv4 option handling isn't one of those things which gets a lot of testing coverage.

In short, it's a cute idea which is just yet another time, effort, and money waster by those who want to hang on to their old IPv4 ways and resist the change to IPv6 for questionable reasons.  It is perhaps best exempified from the draft RFC itself:
In order to maintain backward compatibility with old IPv4 systems, it is important that the EnIP Source Address is an allowed private address.  Otherwise, that address becomes a routable address outside of an autonomous system and there is a potential for routing ambiguity.

Hmmm....sort of like the ULA concept?  Site local scope?  These sorts of issues are already fairly well hashed out in IPv6.  My advice is to embrace the change and not fight it so much."

----------------------------------

Napsterbater
bojack1437@gmail.com

On Thu, Sep 24, 2015 at 10:49 AM, Abraham Y. Chen <aychen@avinta.com> wrote:
Hi, Napsterbater:

0)    Thanks for forwarding rchandra's comments. However, he digressed from critiquing Avinta's ExIP work to promoting IPv6. With so many specific terms in his writing, I must profess that I am not equipped to follow up on his trend of thoughts. It would truly be wasting both of our times. Please excuse me.

1)    On the other hand, it looks that you guys are very much intimately familiar with IPv6. Maybe this is a good opportunity for me to ask a few dumb questions which have been puzzling me since I stumbled onto studying the IPv4 address shortage subject, etc. The following are what I could not find straight answers in my search. Please guide me to the proper information source, so that I will not carry on my incorrect impressions.

2)    It seems that IPv6 is not backward compatible with IPv4. It does not have a simple conversion rule. IPv6 is not a superset of IPv4. It even can not encapsulate IPv4 packets. So, gateways between the two are necessary. This seems to be extremely odd for upgrading a working system. Are these true and is there any good explanation?

3)    Based on Cisco's prediction, there will be 50 billion IoTs by year 2020. Any approach that has the potential to handle multiple folds of this number deserves to be a candidate to be considered, especially something, such as IPv4, has been working fine up to now. Why do we want to waive a big banner to promote IPv6 with an implied end outcome of killing IPv4? What is the purpose of the zillions address pool? The 32 bit dot decimal format of IPv4 is already beyond most people's brain power. The 128 bit HEX formatted IPv6 may be only recognizable by machines. Is this really necessary or is it for "confuse the enemy"? (In case you have not heard of, this is an expression in military discipline. Keep everything neat and concise so that your team can work with your. Otherwise, your comrades will likely be confused before facing the enemy.)

4)    IPv6 is being promoted as having better security capability than IPv4. However, I have not found any evidence of supporting such. I did come across a quotation that seems to cast some doubt on this:

   Why the Internet of Things Needs IPv6:

http://www.govtech.com/policy-management/Why-the-Internet-of-Things-Needs-IPv6.html

And like all tech implementations, security is another issue – neither IPv6 nor IPv4 protect against denial of service attacks, for example. “Switching from one protocol to the other or running them both in parallel does not solve that problem, which simply means we have many other things to worry about,” Cerf said.

Could you kindly clarify this for me?

5) "15 years of work with thousands upon thousands lines of code" is very impressive. But, with only a small percentage of Internet traffic beginning to use IPv6, isn't it the time to review why it takes so long to get something going? Did we start from the correct footing? Could it be done better? Is there any such analysis document available for share?

6) Lastly, let's come back to where we started with. Putting marketing potential and implementation effort aside, do you see any technical issue with ExIP's numbering plan (reclaiming the third octet of 192.168/16 for public routing) and stealthily passing (tunneling?) through the Internet (utilizing the IP header Option mechanism)? For a technical topic, its baseline needs be cleared for all parties before getting to the next two levels. Jumping onto the marketing aspects as the conclusion with a long free-hand essay does not settle the discussion.

Regards,

Abe (2015-09-24 10:48)

On 2015-09-24 12:12, Napsterbater wrote:
2) No its not, just as what you suggest is not really backwards compatible either, at-least for the endpoints., and it can be encapsulated in IPv4, 6in4 does this, this is for 6to4 works, as well as tunnels, a lot of tunnel brokers like HE.net and Sixxs use this, as well as a lot of other people/companies to connect 2 IPv6 networks across IPv4 only networks.

3) Because in the long run 1 network is easier then two, but two are required until there is enough penetration of IPv6, and the reason for it being so big, 1) why make it "just big enough" for now and run into this problem again. Make it huge and not have this problem ever again, or at least for a very long time. and 2) it allow better subnetting, allowing one organization to need only 1 subnet for everything instead of needing multiple unconnected subnets which also help keep the BGP6 table size in check, unlike what has happened with the BGP4 table size.

4) You are right, this is false. At one point IPv6 required that IPSEC be supported, some people took this to mean IPSEC be used for all connections. This is false. IPEC is not even required anymore. IPv6 is not more secure then IPv4.

5) The problem is businesses, they wont upgrade anything until they see a financial reason to, Facebook found that their site and apps work better with IPv6 on networks that had IPv4 and IPv6, so they have upgraded their entire backend to be dual statck IPv4 and IPv6, Google has done the same, but most ISP don't care about upgrading because its not something they can advertise because 95+% of customers don't care or even know what IPv4 or IPv6 is.

6) No. because that is not how routing works, you can’t just change the rules like that, its fundamentally flawed.

---------------------------------

Napsterbater
bojack1437@gmail.com

On 2015-09-27 11:13, Abraham Y. Chen wrote:

Hi, Napsterbater:

1) Re: Ur. Pts. 2) - 5): Thanks for confirming my speculations. At the minimum, I would recommend that IPv6 camp should reach out with a clear set of characteristics, capabilities, agenda and goal, etc. for the "outsiders" to appreciate what IPv6 is and isn't, as well as IPv6 team's efforts.

2) Re: Ur. Pt. 6): Let's go through the exercise of "Divide and conquer" on this, since I posted a two-part question, but you made a categorical conclusion without respective comments.

3) "The Option mechanism used by ExIP": Since EnIP reported that their live test packets did go through Internet, even though their Option number (26) was not assigned by IETF (Isn't this the real beauty of this mechanism?), would you say that this part should be usable by ExIP?

4) "Numbering plan used by ExIP: The idea of making use of the third octet of 192.168/16 for ExIP comes from telephony's PBX technology. Based on what I have seen in products, I presumed that logically it should work for the hierarchical network routing setup being considered, just as in the telephony switching system like PSTN. Since you seem to disapprove this subnetting or layering technique, I went through a bit more study in the networking field. Here are some references that I found:

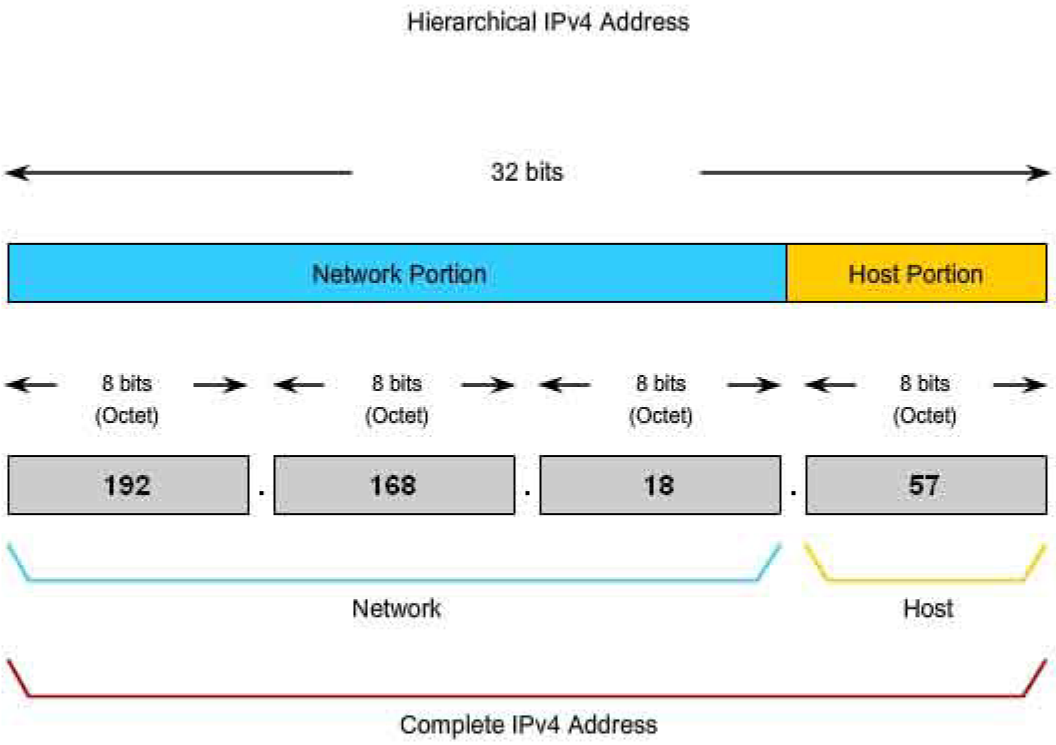
A. Halfway down on the following webpage, I found a description that matches well with the ExIP numbering plan for SPR, because it uses 192.168.18/24 as the example! For your convenience, I copied-&-pasted the relevant portion of the text below. I further highlighted two sentences in the middle of the second paragraph, because they seem to apply to ExIP directly. Even the keyword "***extended***" is in here.

http://www.highteck.net/EN/Network/OSI_Network_Layer.html

### *Dividing the Networks - Networks from Networks*

If a large network has to be divided, additional layers of addressing can be created. Using hierarchical addressing means that the higher levels of the address are retained; with a subnetwork level and then the host level. The logical 32-bit IPv4 address is hierarchical and is made up of two parts. The first part identifies the network and the second part identifies a host on that network. Both parts are required for a complete IP address. For convenience IPv4 addresses are divided in four groups of eight bits (octets). Each octet is converted to its decimal value and the complete address written as the four decimal values separated by a dot (period), for example - 192.168.18.57

In this example, as the figure shows, the first three octets, (192.168.18), can identify the network portion of the address, and the last octet, (57) identifies the host. This is hierarchical addressing because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, rather than needing to know the location of each individual host. With IPv4 hierarchical addressing, the network portion of the address for all hosts in a network is the same. To divide a network, the network portion of the address is ***extended*** to use bits from the host portion of the address. These borrowed host bits are then used as network bits to represent the different subnetworks within the range of the original network. Given that an IPv4 address is 32 bits, when host bits are used to divide a network the more subnetworks created results in fewer hosts for each subnetwork. Regardless of the number of subnetworks created however, all 32 bits are required to identify an individual host. The number of bits of an address used as the network portion is called the prefix length. For example if a network uses 24 bits to express the network portion of an address the prefix is said to be /24. In the devices in an IPv4 network, a separate 32-bit number called a subnet mask indicates the prefix. Extending the prefix length or subnet mask enables the creation of these subnetworks. In this way network administrators have the flexibility to divide networks to meet different needs, such as location, managing network performance, and security, while ensuring each host has a unique address.



B. The following webpage has an example explaining how to break a 32 bit IPv4 address into three parts to accomplish hierarchical addressing. This is exactly what ExIP proposes to do with 192.168/16 by using its third octet to extend the basic public IPv4 network address and then use the remaining fourth octet for identifying the hosts on the private network. This article even mentioned the analogy (or parallelism) between telephony switching and network routing.

http://www.tcpipguide.com/free/t_IPSubnettingThreeLevelHierarchicalIPSubnetAddressi.htm

C. Based on the above, I found additional description about subnetting on Wikipedia which seems to also go along with the same concept that ExIP is utilizing:

https://en.wikipedia.org/wiki/Subnetwork

I look forward to your thoughts and comments.

Regards,
Abe (2015-09-27 11:13)

*************

On 2015-10-05 16:37, Abraham Y. Chen wrote:
Hi, Napsterbater:

0) Have not heard from you for awhile.

1) I am beginning to get concerned, wondering whether the cyberspace is playing tricks on us by swallowing either my MSG or your reply. Please respond to close the loop, so that we may carry on the discussion.

Regards,

Abe (2015-10-05 16:37)