The PULP

HUGE this month:

General Meeting: July 15th

We'll figure it out when we get there.

See you there!

East Hartford Public Library
Main St. & Central Ave., East Hartford, CT.

Q&A Session: 7:00 PM–7:30 PM
Meeting starts at: 7:30 PM

Contents:

Member of Association of Personal Computer User Groups APCUG

UGC

Apple User Group

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATIONS
East Hartford Public Library
Main & Central Avenue
in the Lion's Room(downstairs)

Wethersfield Public Library 500 Silas Deane Hwy., Wethersfield, CT

Editors Corner

Happy Summer.

Do you have one of those new-fangled cars with the wireless key system and a pushbutton starter? Then you might want to be aware of where you park it. The FCC is investigating reports of "Electronic Bermuda Triangles" or focused interference. In these areas, car alarms will randomly go off and some will refuse to start.

One (semi)documented area is a five block area around the Empire State Building, another is in downtown Tampa . See the article--

(http://www.tampabay.com/news/transportation/article467048.ece)

This month we will begin incorporating articles from "Tidbits". Here is the approriate copyright citation and a link to the full text. (http://creativecommons.org/licenses/by-nc-nd/3.0/).

Stuart Rabinowitz
Editor-in-Chief

A Little Computer Quiz

by Stuart Rabinowitz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

1 Any fans of 'Alias' out there, remember back to the first season and the character of Burnett--what was Burnett's job?
2 Who played the role?
3 In November, 1995 a 'well known' TV news anchor announced their resignation and intention to write for "PCWorld" magazine. Who was it?
4 What (now much larger) social website launched on February 4, 2004?
5 Who started it?
6 Where did it get started?

Answers to June, 2008 Quiz

1 In 1998 Apple introduced the first iMac, what color was it?
A It was Bondi Blue
2 In December, 1977 the first commercially installed local area network was installed, where?
A It was installed at Chase Manhattan Bank in New York
3 What type of network was it?
A It was an Attached Resource Computer (ARCnet) and was passed on a token scheme
4 What company developed/sold it?
A It was sold by, the now out of business, Datapoint Corp.
5 What was the original project name?
A Internally it was called 'internet'.
6 At what speed did it operate?
A The original network speed was 2.5Mbit/sec

Does Your Network Have a Public IP Address?
by Glenn Fleishman <glenn@tidbits.com>
article link: <http://db.tidbits.com/article/9661>

I pose the question in the headline based on the early feedback from readers of my new book, "Take Control of Back to My Mac," which covers using Mac OS X 10.5 Leopard plus the .Mac service (soon to be called MobileMe) for remotely accessing files on and remotely controlling the screens of Macs you manage or own.

<http://www.takecontrolbooks.com/back-to-my-mac.html?14@@!pt=TB934>

The trouble with Back to My Mac, in comparison with Skype and LogMeIn, is that Back to My Mac requires a publicly routable IP address on either a computer that's to be reachable or a router to which one or more computers with Back to My Mac are connected.

The question I've heard from multiple readers is, "I'm not a network engineer. How do I figure out if I have such an IP address?"

There's a short non-answer and a long answer. The short non-answer is that I can't give you a good short answer because the Internet is broken. The current system of public and private networks, designed in part to get around a shortage in the current IP addressing system, doesn't allow easy end-to-end connections. For the long answer, read on. (I expand on the short non-answer in the last section, too.)

Public IP versus Private IP -- Let me back up to explain what a public IP address really is. The Internet is Balkanized through something called Network Address Translation (NAT), which allows a single public IP address that's reachable, or _routable_, from any other computer on the Internet to act as a kind of proxy for 1, 1,000, or 1,000,000 private IP addresses. A gateway mediates traffic between the public address and the private one. (You can read more about NAT in "Punch Through NAT with Port Map's Port Forwarding," 2008-04-16.)

<http://db.tidbits.com/article/9568>

If a computer on which you want to enable Back to My Mac has a public IP address - as do some computers in my office network - then Back to My Mac works without a hitch. It allows any other computers that you log into with your .Mac account name and password, and on which you enable Back to My Mac in the .Mac system preference pane, to access that publicly addressed computer. (If you have a public IP that's assigned to individual computers, you probably already know that you do, because you're likely paying your ISP more for that privilege.)

Where a computer is on a private network, using a range of addresses that can be reached only through a router, Back to My Mac has to perform a NAT end-run using one of two widely available protocols that let a privately addressed computer punch through the NAT gateway with the router's assistance. Those protocols are NAT-PMP (NAT Port Mapping Protocol), an open standard used exclusively by Apple, and UPnP (Universal Plug and Play), another standard used widely by other routers and supported by Apple and Microsoft for various services.

By subverting NAT, these two protocols enable a router that has a public IP address to make services on private computers available publicly. It's a secondary problem to let other computers know precisely which ports - a kind of numbered cubbyhole on an IP address, in this case the address of the router - are used by whatever game, remote access service, IP phone, or other software that has engaged NAT-PMP or UPnP.

Apple plays nice with networks by using these two protocols. LogMeIn, Skype, and other remote connection and voice-over-IP programs use their own techniques to link computers that can't be reached via public IP addresses. Skype, for instance, uses "supernodes," which are computers with a logged-in Skype user, a high bandwidth connection, and a reachable address. Supernodes are chosen dynamically by the Skype system, and they engender varying degrees of concern and irritation from network administrators. (Skype 3 for Windows has a checkbox to disable becoming a supernode; the current Mac release, 2.7, does not.)

<https://secure.logmein.com/>

<http://www.skype.com/>

Your Network's Layout -- The next piece in figuring out whether you have a publicly reachable IP is looking at how your broadband network is set up. Most of us at home have a cable, DSL, or fiber modem that connects to some incoming wire, and has one or more local Ethernet jacks, and optionally Wi-Fi.

Some broadband modems act as full-fledged routers: they assign private addresses to networked computers and let you configure firewall and other network settings. Others act like bridges: they enable the ISP to assign you an address (which can be public or private, and either dynamic or static) and relay traffic from the ISP's network to yours.

With a modem that acts as a router, you may be unable to use Back to My Mac because that modem controls access to the network. If the modem doesn't support or allow you to enable UPnP, you're stuck using manual port mapping (if supported), which lets you set up only one computer to be reachable via Back to My Mac. (I cover the ugly details of port mapping in my book. It gets rather involved.)

I have this kind of modem in my home, for Qwest DSL service, and I'm stuck because it's made by 2Wire. Although Qwest gives me a public IP address, 2Wire does not offer UPnP support in any of its modems; its customers are ISPs, typically DSL providers who don't wish to allow users to make public services from networked computers available, largely due to security and control reasons.

A theoretical malicious program could use UPnP or NAT-PMP to open a tunnel to itself from other agents in the outside world, and become, for instance, a mail server delivering spam or any of a number of other activities. So there's some justification for disabling UPnP, but it should be left up to the user, since viruses can work without enabling direct port mapping.

With the second kind of modem, the one that bridges a network, you can connect your AirPort Extreme Base Station or other gateway to the broadband modem, obtain what's typically a publicly reachable IP address, enable the automatic port mapping option (NAT-PMP or UPnP), and then Bob's your uncle: Back to My Mac typically works. Many broadband networks are set up this way, and it's one of the best cases in which to use Back to My Mac.

Now, how can you tell which type of modem you have, and how can you tell whether you have a public IP address? Let's get into that next.

Reach Out and IP Someone -- We start with the broadband modem. Can you view your modem's configuration by connecting to it over your local network via a Web browser? If not, then you find yourself in one of two situations:

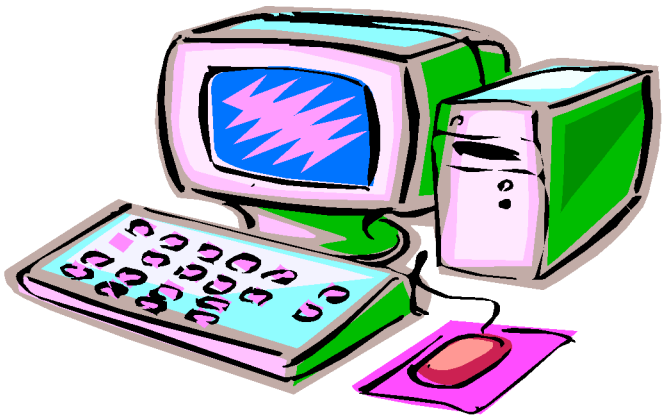
* The modem is a bridge, and you still need to determine whether or not devices you plug into it obtain or can be assigned a public IP address.

* Your modem has a configuration locked down by your ISP, and you can neither enable UPnP if available nor use manual port mapping if UPnP is unavailable. In this second case, you're out of luck with Back to My Mac.

If you can connect to your broadband modem via a Web browser, do so (this may require a password, which may require a call to your ISP), and see what the summary screen or status screen tells you about the modem's Wide Area Network (WAN) connection - the modem's connection back to the ISP's network.

That screen should provide you the address the modem is using. In some cases, you'll see just one number; with my Qwest modem, I see both a private address in Qwest's network and a separate public address to which Qwest connects my modem, both of them clearly labeled.

You can tell whether this WAN address is public or



private by looking at its first few numbers. Current IP addresses - using the ancient IPv4 numbering system - have four numbers separated by dots, like 10.0.0.1. If the WAN port's IP address starts with 192.168 or 10., or begins with 172. followed by the numbers 16 to 31, it's a private address. (Examples: 192.168.0.1, 10.0.0.1, 172.16.5.1.) You'll need to contact your ISP to see if you can get a public address.

If the number doesn't fit any of those patterns, it should be a public address, and should be generally reachable.

Now, if you can't connect to your broadband modem from the local network or if you want to ensure the address you're looking at for the WAN port is truly public, you can use a Web site that tries to tell you your current IP address; WhatIsMyIPAddress.com is one of many examples. These sites tell you what they believe the address is of the router or computer that sent the request. However, if your network is nested in one or more layers of NAT, the page shows the IP address of an ISP's router.

<http://whatismyipaddress.com/>

Visit that link. Does it match the configuration screen (if any) of the broadband modem? If so, you're almost certainly set to go.

If not, or if that doesn't apply, you can try at least one technique to see if the router is reachable: the command-line tool ping. Make a note of the address from the Web page and leave your home or office. Using Mac OS X from another network, launch Terminal (in Applications/Utilities); under Windows, launch the Command Prompt program in the Applications folder. At the prompt type:

ping -c 10 address

replacing _address_ with the IP address that you copied. Do you see a few lines in response in the Terminal like this one?

64 bytes from 34.33.111.253: icmp_seq=0 ttl=127 time=10.564 ms

That means the modem is responding to an "are you alive" request over the Internet, and is likely reachable.

Let's put this all together.

Back into Back to My Mac -- If, in any of the cases above, you believe or know that you have a public IP address connected to a modem or router that can use NAT-PMP or UPnP, or that you have used manual port mapping to enable access to one computer via Back to My Mac, turn on Back to My Mac and see if you can reach the computer from outside your local network. (You can't properly test Back to My Mac with two computers on the same local network, since Leopard doesn't offer any visual indication to show whether a computer in the Shared list in the Finder sidebar is available via Bonjour over the local network or via Back to My Mac over the Internet.)

If that doesn't work, or you determine you don't have a public IP address, there's nothing more you can do on your own; it's time to call your ISP if you want any hope of making Back to My Mac work.

To recap, Back to My Mac should work on a network in which one of these conditions is met:

* Your ISP has assigned your modem a public IP address _and_ it supports either UPnP or manual port mapping.

* Your ISP bridges their network across the modem, providing a public IP address for your router, which supports NAT-PMP, UPnP, or manual port mapping.

Back to My Mac won't work on a network in which either of these conditions are true:

* Your ISP doesn't provide a public IP address to your modem or your router.

* You can't configure UPnP, NAT-PMP, or manual port mapping on your modem or router.

If your network should allow proper Back to My Mac functioning, and you still get a yellow dot (in Mac OS X 10.5.3) in the .Mac preference pane's Back to My Mac view (see "Back to My Mac Communicates Faults in 10.5.3," 2008-05-29) then you either need to read my book, or try an alternative like LogMeIn Free for Mac or Timbuktu plus Skype. I have advised many TidBITS readers to try these alternatives because their networks simply won't work with Back to My Mac.

<http://db.tidbits.com/article/9636>
<http://www.netopia.com/software/products/tb2/tb2_skype.html>

The Future with IPv6 -- As I said at the outset, the Internet is broken. IPv4 addresses are in short

supply and running out. But take heart: IPv6 is IPv4's replacement, has vastly more potential addresses (4 billion to the fourth power, versus 4 billion), and is designed and implemented in a way that will restore much of the end-to-end principle of the Internet. This introduces more security concerns, but also makes it much more likely that network services will just work.

IPv6 isn't a simple migration; every single device on the Internet must support the new protocol and deal with the long, perhaps eternal, transition from IPv4. Mac OS X and Windows have supported IPv6 for years, but DSL and cable modems have lagged even as other components of broadband networks have been upgraded. Comcast, for instance, uses IPv6 for its vast internal routing network, because they simply couldn't obtain enough IPv4 numbers for their needs. (You can read more about this in a recent article I wrote for the Economist, "Your Number's Up.")

<http://www.economist.com/science/tq/displaystory.cfm?story_id=11482493>

I bring up IPv6 not to complicate your understanding, but because Apple has enabled IPv6 in two key places that have to do with your network and Back to My Mac. IPv6 can be tunneled over existing IPv4 networks, which means that data addresses using the new scheme can be wrapped within packages addressed with the old.

In fact, Back to My Mac takes advantage of this. Connections made with Back to My Mac use tunnels of IPv6 to transport data packets, which are wrapped in strong encryption. Back to My Mac essentially creates two IPv6 end points, one on each computer connected via Back to My Mac. Ultimately, this should enable better connectivity using more services - perhaps allowing third-party Mac developers to wire in their own services.

The other key point is that Apple has enabled IPv6 in their Draft N routers: any Wi-Fi-enabled base station released in 2007 or 2008, including the revised AirPort Express Base Station. Apple isn't supporting just IPv6 addressing - which would be like letting postal carriers know that a house has an old house number and a new house number - but is also allowing tunneling IPv6 from the local network out to IPv6 gateways on the Internet.

These gateways, run at no cost to the user, let you connect native IPv6 networks, such as those run by Apple's recent AirPort base stations, to each other using the current Internet without any need for changes by your ISP. Over time, experts and network operators have told me, IPv6 connections will expand further into the backbone of the Internet, and eventually IPv4 will primarily be tunneled inside of IPv6, instead of the reverse.

With IPv6, the idea of a public or private IP address more or less goes away, and the necessity of building and using a service like Back to My Mac drops a bit, too. You'd still want the security of Back to My Mac's authentication (proving your identity) and encryption (securing the connection), but you'll no longer need to muck about with the question of public and private IP addresses.

Mac OS X Snow Leopard to Focus on Performance, Not Features

by Adam C. Engst <ace@tidbits.com> article link: <http://db.tidbits.com/article/9651>

At the beginning of the Worldwide Developers Conference keynote, Apple announced it would provide information about the next version of Mac OS X - code-named Snow Leopard - after the keynote. Since all the content at WWDC other than the keynote is covered by non-disclosure agreements, it seemed that Apple didn't plan to talk in public about what we could expect.

However, a press release about Snow Leopard appeared late in the day revealing some details. Instead of adding marquee features like Time Machine and Spaces, Snow Leopard will instead focus on enhancing performance and reliability and lay the foundation for future features. In particular, Snow Leopard will be optimized for multi-core processors, be able to tap into the computing power of modern graphic processing units (GPUs), make it possible to address up to 16 TB of RAM, ship with QuickTime X, and provide out-of-the-box support for Microsoft Exchange 2007 in Mail, iCal, and Address Book.

<http://www.apple.com/pr/library/2008/06/09snowleopard.html>

A new technology code-named "Grand Central" will make it easier for developers to create applications that make the most of multi-core Macs, which should let people get more from those 8-core Mac Pros. Additional performance gains will come from support for Open Computing Language (OpenCL), a new language from Apple that supposedly lets any application access the gigaflops of computing power previously available only to graphics applications. Apple says that OpenCL is based on the C programming language and has been proposed as an open standard; the only hints about it up to now came in an interview with the Nvidia CEO.

<http://news.cnet.com/8301-13579_3-9962117-37.html>

QuickTime X will reportedly optimize support for modern audio and video formats for more-efficient media playback. It seems likely that QuickTime is due for a major rewrite, given how long it has been around. Finally, Safari will receive JavaScript performance enhancements that are intended to provide an enhanced user experience for Web applications, perhaps due to a new JavaScript engine called SquirrelFish that's recently seen the light of day.

<http://webkit.org/blog/189/announcing-squirrelfish>

The press release said that Snow Leopard is slated to ship "in about a year," and I'm sure more details will start leaking out as developers receive seeds. Overall, my initial reaction is that Snow Leopard is a very good move for Apple, because the focus on adding features in favor of performance has meant that Mac OS X has become increasingly poky for many users. And I suspect that people are no longer responding as favorably to long lists of features that they may or may not use - although I use them happily, none of the new features in Tiger or Leopard have radically changed the way I use my Mac. Apple touts Mac OS X as being rock-solid and easy to use (especially compared to Windows), so enhancing the engine under Leopard's hood could be just what many people are looking for in the next update.

It can be difficult to convince users to pay for better performance and more efficient workings under the hood, but perhaps Apple will charge less than the usual $129. Or, perhaps Apple will give Snow Leopard away for free, in preparation for a Mac App Store that will give Apple a cut of every Mac application sold. But that's just crazy talk... or is it?

PULP Staff

Editor Stuart Rabinowitz
Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries and BBS. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President:	George Carbonell	568–0492	george.carbonell@comcast.net
Vice President	Stuart Rabinowitz	633–9038	s.e.rabinowitz@att.net
Secretary:	Ted Bade	643–0430	tbade@cox.net
Treasurer:	Charles Gagliardi	233–0370	epencil@att.net
Director at Large:	Richard Sztaba		richer1@aol.com
Web Manager:	Bob Bonato		

Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz	633–9038	s.e.rabinowitz@att.net

July 2008

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15 General Meeting 7 PM	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		