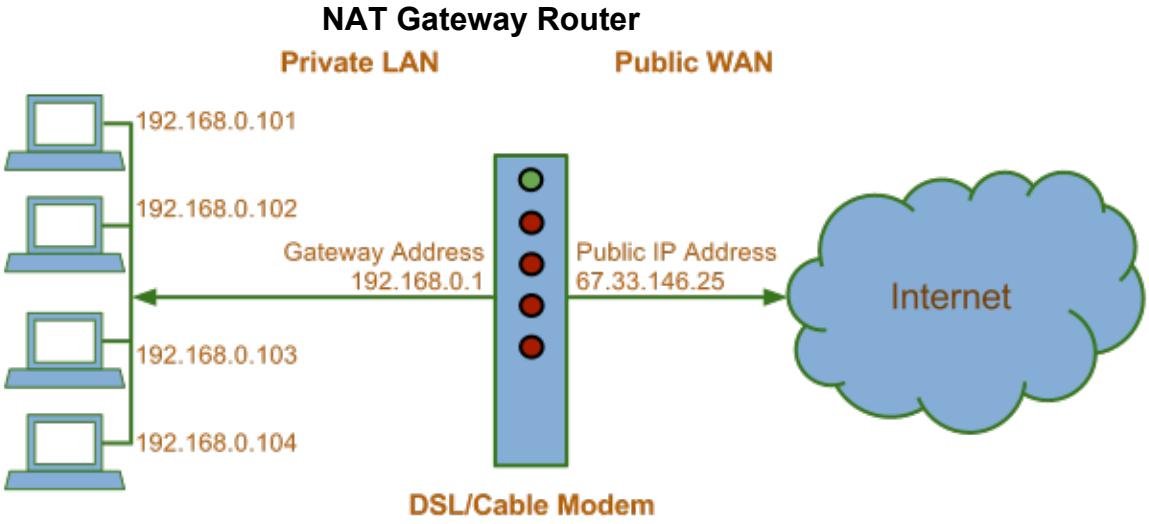
My name is RAParker. I own a Newton and a Mac.

My Newton is wireless and it accesses the Internet securely using WEP. I'll wait for just a minute while the naysayers warm up and begin typing their responses.

Understanding NAT

There are several private IP address ranges which were set aside to help preserve the limited number of public IP addresses. These private address ranges are classified as non-routable over the Internet. Generally, broadband routers will use NAT, or Network Address Translation, to allow a single network device (the router) to act as an Internet Gateway for the other (and usually multiple) network clients. The NAT gateway helps network clients on a private LAN to open connections to the Internet by sharing the single public IP address, translating the source and destinations of the data packets on the fly, depending on which client on local network made the request.



When a client on the private LAN requests an address located on the Internet, the request is forwarded to the NAT gateway. The gateway changes the source address of outgoing packets to match the IP address of the public facing (WAN Port) of the gateway. The router then forwards the outgoing packets further on to their destination over the Internet.

At first this is a one-way connection. After a client makes the initial connection, the source of the outgoing connections are tracked by the gateway, essentially creating an active connection state within the gateway's NAT table. Upon returning, the incoming packets are compared against the NAT table. The destination addresses of the packets are re-translated using the NAT table and then forwarded back to the client which originally requested the packet.

Important Security Note: If an incoming packet is not in the gateway's NAT table, it is considered unsolicited and immediately dropped.

NAT As Security

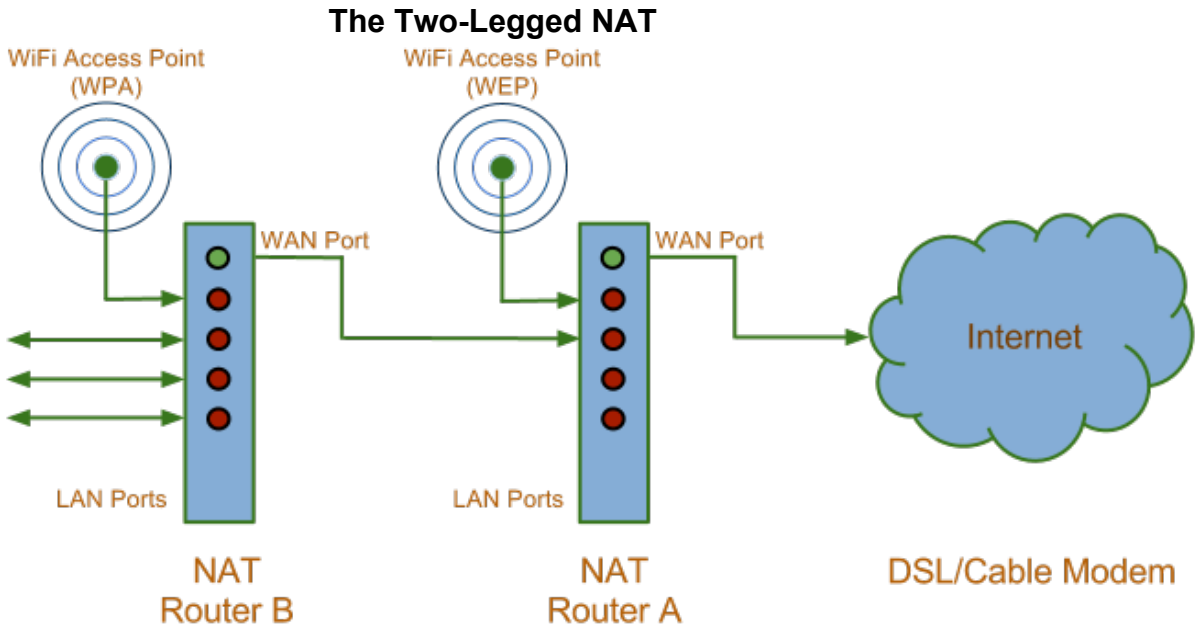
Sharing an Internet connection is not the only benefit of a NAT router. Due to the inherent design of NAT, the gateway also isolates and hides internal LANs from the Internet by using private, non-routable IP addresses. One cannot fully grasp this benefit without further study, so I will leave out the details here. But let's just say this: Network Address Translation is the single important reason that we trust our firewalls to protect us from intruders.

For further reading see:
Gibson Research Corporation - http://www.grc.com/nat/nat.htm
Tech-Faq.com - http://www.tech-faq.com/nat-network-address-translation.html
Wikipedia.com - http://en.wikipedia.org/wiki/Network_address_translation

So far, one may think this applies specifically to hardwired Ethernet connections. As mentioned in the beginning, I own an Apple Newton and my MessagePad 2100 uses a wireless adapter to connect to the Internet. Unfortunately, the wireless driver for Newton OS is limited to using WEP encryption and it is well known that WEP is crackable. Does this mean that a WEP enabled network has to be entirely insecure?

Giving WEP Another Leg Up

Understanding that NAT isolates non-routable private networks allows us to take the idea one step further. By using two NAT routers "In Series" you can isolate an insecure Wireless Access Point within its own private network. This setup provides Internet access to wireless clients and devices, which happen to be limited to WEP encryption, yet completely blocks access to the other devices behind the second NAT router. You can also provide guests with their own Internet access and still protect your private network. Take a look at this simplified diagram:

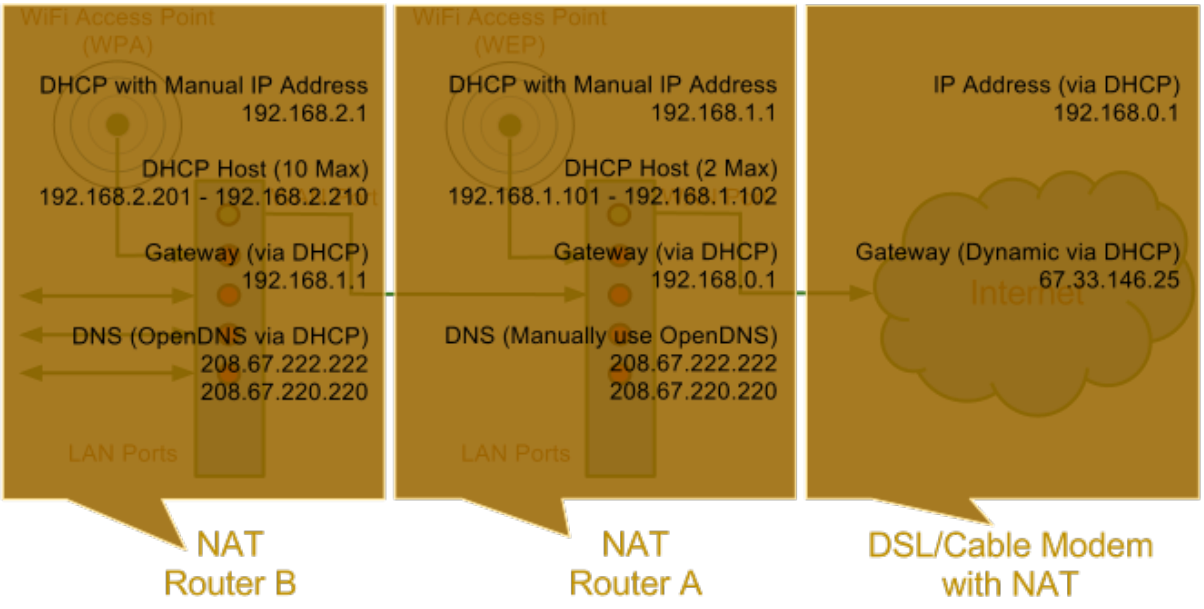


This does not eliminate the fact that an industrious neighbor can still crack the WEP encryption. But it does isolate the access point, so as to limit the intruder to Internet access only. The other private network is protected from access, probing or even snooping and discovery. Remember, the private networks on the other side of the NAT use private address space. Packets passing through the NAT are invisible to the other clients on the router, unless the packets were initially routed to that network in the first place.

Cascading DHCP With A Manual IP

Many consumer broadband routers are all-in-one devices that provide an upstream WAN port, four or more LAN ports, and a built-in WiFi Access Point. A typical default setup for a broadband router is to use DHCP to get the WAN configuration and also to use DHCP on LAN side to configure clients. Each NAT gateway/router can be both a DHCP client in addition to being a DHCP server. However, when using two routers, especially two identical models, you should pay special attention to the fact that these devices may default to using the same network and IP address. Using a combination of DHCP with manually configured IP addresses will give better control over access and setup.

Configuring Cascading NATs



Each NAT gateway adds an additional layer of protection. Each gateway acts like a one-way valve, protecting the deeper layers from unsolicited (potentially unknown or malicious) traffic. When you isolate a WiFi Access Point within its own private network, wireless clients are able to use the gateway to connect to the Internet, yet the rest of the network remains completely hidden.

The WEP problem for your Newton is solved.

Caveat Securitas

Morgan Aldridge commented, “Newtons are inherently insecure, but in such a way that makes them extremely useful and extensible. If you were able to get a nefarious package onto a Newton, it could access everything (unless you’re one of the few encrypting Notes with TheFish or one of the alternatives) and do anything. None of its transmissions to/from the outside world are encrypted and all can be intercepted: IRDA (well, not without being completely obvious, considering the extremely short range), dial-up modem (old-school, but you just have to tap the phone line), Bluetooth (Bluetooth only requires authentication or encryption and I’m pretty sure Blunt only uses the former for performance reasons), and WiFi (WEP is crackable, MAC addresses can be cloned, and ARP tables can be polluted).

But, even with all the communications options, most people will not be doing much that contains sensitive data in Newton transmissions. The best thing you can do, esp. if you live in a well populated area where bluetooth & WiFi sniffing/cracking is a possibility, it protect the rest of your devices and try to limit sensitive data that gets passed around. You’re certainly not going to be doing online banking on your Newton, but if you’re checking/sending email via IMAP/POP/SMTP then the password will be exposed. If you’re routing sensitive notes, that data will be exposed. If you’re using telnet, anything you type, including usernames & passwords, will be exposed.

If you have WiFi you should definitely be using a “guest” network/SSID or double-NAT if you’ve got other devices on the network that do have sensitive data or perform sensitive tasks so that you’re limiting their risk. It doesn’t hurt to use 128bit WEP, MAC address filtering, and a non-standard IP address range w/manual IPs. The latter will stop lazy neighbors from leeching bandwidth and will be a challenge (although probably not an overly difficult one) for budding hackers with an intrusion live CD, but will also be a big disappointment once they get in and find it a wasteland of devices like Newtons which have no open ports to probe.”