Expose your Raspberry Pi on Any Network

[Originalartikel](#)

[Backup](#)

<html> <p>Everyone’s talking about the Internet of Things (IoT) these days. If you are a long-time Hackaday reader, I’d imagine you are like me and thinking: “so what?” We’ve been building network-connected embedded systems for years. Back in 2003, I wrote a book called Embedded Internet Design — save your money, it is way out of date now and the hardware it describes is all obsolete. But my point is, the Internet of Things isn’t a child of this decade. Only the name is.</p> <p>The big news — if you can call it that — is that the network is virtually everywhere. That means you can connect things you never would have before. It also means you get a lot of data you have to find a reason to use. Back in 2003, it wasn’t always easy to get a board on the Internet. The TINI boards I used (later named MxTNI) had an Ethernet port. But your toaster or washing machine probably didn’t have a cable next to it in those days.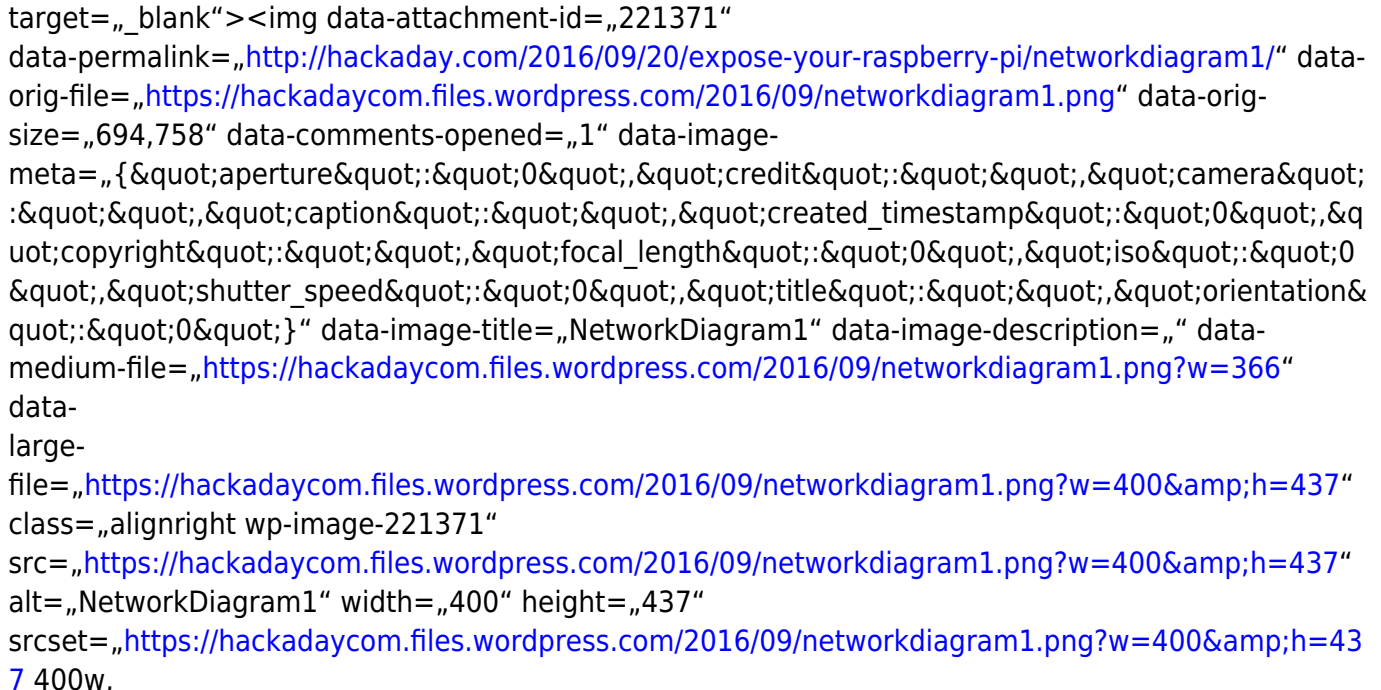</p> <p>Today boards like the Raspberry Pi, the Beagle Bone, and their many imitators make it easy to get a small functioning computer on the network — wired or wireless. And wireless is everywhere. If it isn’t, you can do 3G or 4G. If you are out in the sticks, you can consider satellite. All of these options are cheaper than ever before.</p> <h2>The Problem</h2> <p>There’s still one problem. Sure, the network is everywhere. But that network is decidedly slanted at letting you get to the outside world. Want to read CNN or watch Netflix? Sure. But turning your computer into a server is a little different. Most low-cost network options are asymmetrical. They download faster than they upload. You can’t do much about that except throw more money at your network provider. But also, most inexpensive options expose one IP address to the world and then do Network Address Translation (NAT) to distribute service to local devices like PCs, phones, and tablets. What’s worse is, you share that public address with others, so your IP address is subject to change on a whim.</p> <p>What do you do if you want to put a Raspberry Pi, for example, on a network and expose it? If you control the whole network, it isn’t that hard. You usually use some kind of dynamic DNS service that lets the Pi (or any computer) tell a well-known server its current IP address (see figure below).</p> <p/> <p><img data-attachment-id=„221371“ data-permalink=„http://hackaday.com/2016/09/20/expose-your-raspberry-pi/networkdiagram1/“ data-orig-file=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png“ data-orig-size=„694,758“ data-comments-opened=„1“ data-image-meta=„{"aperture":"0","credit":"","camera":"","caption":"","created_timestamp":"0","copyright":"","focal_length":"0","iso":"0","shutter_speed":"0","title":"","orientation":"0"}“ data-image-title=„NetworkDiagram1“ data-image-description=„“ data-medium-file=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=366“ data-large-file=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=400&h=437“ class=„alignright wp-image-221371“ src=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=400&h=437“ alt=„NetworkDiagram1“ width=„400“ height=„437“ srcset=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=400&h=437 400w,

https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=229&h=250 229w,
https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png?w=366&h=400 366w,
https://hackadaycom.files.wordpress.com/2016/09/networkdiagram1.png 694w" sizes="(max-width:
400px) 100vw, 400px"/></p> <p>That well-known server answers DNS requests (the thing that
converts hackaday.com into a real IP address). Now anyone can find your Pi. If you have a firewall in
hardware and/or software (and it is a good bet that you do), you’ll also have to open the
firewall port and tell the NAT router that you want to service traffic on the given port.</p> <h2
style="clear:none;">Alien Networks</h2> <p>That’s fine if you are at home and you control
all of your network access and hardware. But suppose you don’t know for sure where your
system will deploy. For example, perhaps you will use your box at different traffic intersections over a
3G modem. Or maybe you have built a smart picture frame to put in a hospital or nursing home and
you want access over the institution’s WiFi.</p> <p>Granted, you can handle that as a
system design problem. For the hypothetical picture frame, maybe it checks a web server on the
public Internet periodically for new content. Sure. You can do that. Until you need to ssh into the box
to make some updates. Sometimes you just need to get to the box in question.</p>
<h2>Solutions</h2> <p>There are a few options for cases like this. <a
href="http://www.neorouter.com/products-nrfree" target="_blank">NeoRouter has software for
many platforms that can create a virtual private network (VPN) that appears to be a new network
interface where all the participants are local. If my desktop computer has a NeoRouter IP of 10.0.0.2
and my Pi has 10.0.0.9 then I can simply ssh over to that IP address. It doesn’t matter if the Pi
is halfway around the world. The traffic will securely traverse the public Internet as though the two
computers were directly connected with no firewalls or anything else between them.</p>
<p>Honestly, that sounds great, but I found it a little difficult to set up. It also isn’t terribly
useful by itself. You need to run some kind of server like a Web server. You also need a NeoRouter
server on the public Internet with an open port.</p> <h2>A Better Answer</h2> <p>What I wound
up using was a service called Pagekite. The
software is all open source
and there is a reasonable amount of free use on their servers. I would go on to set the whole thing up
on my own servers (I’ll talk about that next time). For right now, though, assume you are
happy to use their server.</p> <p>If you go to the Pagekite web site, they have a really
simple “flight plan” to get you started:</p> <pre>curl -s https://pagekite.net/pk/ |
sudo bash pagekite.py 80 yourname.pagekite.me</pre> <p><a
href="https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png"
target="_blank"><img data-attachment-id="223780"
data-permalink="http://hackaday.com/2016/09/20/expose-your-raspberry-pi/networkdiagram2-redo/"
data-orig-file="https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png" data-
orig-size="753,720" data-comments-opened="1" data-image-
meta="{"aperture":"0","credit":"","camera"
:"","caption":"","created_timestamp":"0",&q
uot;copyright":"","focal_length":"0","iso":"0
","shutter_speed":"0","title":"","orientation&
quot;:"0"}" data-image-title="networkdiagram2-redo" data-image-description="" data-
medium-file="https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png?w=400
&h=382"
data-
large-file="https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png?w=654"
class="alignleft size-medium wp-image-223780"
src="https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png?w=400&h=
382" alt="networkdiagram2-redo" width="400" height="382"

srcset=„https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png?w=400&h=382 400w, https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png?w=250&h=239 250w, https://hackadaycom.files.wordpress.com/2016/09/networkdiagram2-redo.png 753w" sizes=„(max-width: 400px) 100vw, 400px"/>That’s it. Honestly, you don’t know these guys so I wouldn’t suggest just piping something off the Internet into my root shell. However, it is safe. To be sure I actually redirected the script from curl into a temporary file, examined it, and then ran it. You may be able to install Pagekite from your repository, but it might be an older version. They also have common packages on GitHub and repos for many package systems (like deb packages and RPM).</p> <p>The concept behind PageKite is that of a reverse proxy. Both the remote computer and the user find the PageKite computer via DNS (see figure below). That server acts as a go-between and since nearly all networks will allow access to a web server, there should be no firewall issues.</p> <p>The last line sets up a redirect from the specified URL to your local machine on port 80. So far that isn’t much different than using NeoRouter. However, the pagekite script is kind of interesting. It can be a backend (that is, your Raspberry Pi serving up web content), or a frontend (like the server at yourname.pagekite.me). It also has a simple web server in it. So if you wanted to serve out pages from, say /home/pi/public_html you could write:</p> <pre>pagekite.py /home/pi/public_html yourname.pagekite.me +Indexes</pre> <p>There is a way to add things like this so they start when pagekite starts (read about the –add option). It all works and it works well.</p> <p>You can redirect other ports, also. There is even a way to tunnel SSH traffic, although it does require a proxy set up for the SSH client. That will depend on what ssh programs you use. Although it is a bit of trouble, it is also handy since it allows you to SSH into the remote box even on restrictive work or school networks.</p> <p>Pagekite will give you a chance to sign up the first time you run the script. However, you do need to be on a machine that can open a browser, so if you are using your Pi headless, you might want to set up the account first on another machine.</p> <p>The free account has some limits, but it does let you set up a CNAME to redirect from your own domain name. You can also create unlimited subdomains (e.g., toaster.myiot.pagekite.me, washer.myiot.pagekite.me, and alarmsystem.myiot.pagekite.me).</p> <h2>On Your Own</h2> <p>If you don’t have a public computer and you don’t have a lot of data transfer needs, the Pagekite free plan might just work for you. I didn’t want to use their domain or be subject to their quotas, so I decided to install the frontend to my own web server. The code is open source, but the documentation for making that work is not great.</p> <p>Luckily, next time, I’ll take you through the steps I took to get it all working. It isn’t that hard, but it does require a little thought, text editing, and DNS dexterity.</p> </html>

From:
https://schnipsl.qgelm.de/ - **Qgelm**

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:expose-your-raspberry-pi-on-any-network

Last update: **2021/12/06 15:24**