

Re: Lan Wifi Network

Source: <http://newsgroups.derkeiler.com/Archive/Alt/alt.internet.wireless/2005-11/msg01187.html>

- *From:* Jeff Liebermann <jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 27 Nov 2005 09:12:26 -0800
-

On 27 Nov 2005 02:02:19 -0800, "cherriesbaked"
<cherriesbaked@xxxxxxx> wrote:

>Thanks for answering, I'm gona see if your answer works with my (poor)
>knowledge of computer network... By the way, "length of connection"
>means to me info about one shutting down its computer at night or during
>the day or not.

That's going to be a problem. Deciding whether a user has intentionally disconnected or just driven out of wireless range is difficult. Most routers will retain DHCP leases for many hours after a wireless user has gone away. The ARP cache can be used to determine if a user is still there, but that comes and goes rather quickly. If your wireless network has multiple access points where users can roam between them, the question of where a user is located is added to the muddle. That's what 802.11r (fast roaming) is going to hopefully solve. It is possible to determine if a user is still connected by active means (i.e. ping their IP), but many client side personal firewalls intentionally block ICMP and UDP ping packets. All this causes problems when WISP (wireless ISP) operators want to provide metered billing (by the minute). Some have resorted to proprietary client software (Boingo) to do the job. Others require a VPN connection (T-Mobile) which can be timed. I think you're on the right track by measuring traffic instead of connect time.

>In fact, I'm looking for info that concerns only the activity of the
>network and meanwhile I hope this info can lead me to some suggestion
>like ; "is this computer downloading all night or all day long...?" I
>know for sure without being paranoid my ISP has this info and even
>further like in some explorer connect only sites that work with asp,
>java.

If all you want is aggregate (total) traffic, that's easy. Find a router or switch that has SNMP capabilities. You'll pay more but it's worth it. I use MRTG and RRDTool to query the wireless router for total traffic in both directions.

<http://www.mrtg.org>

<http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

They produce nice historical graphs of total traffic. This is most

Re: Lan Wifi Network

useful for detecting abuse and dealing with traffic failures such as RF interference because they display what is considered normal traffic patterns. User counts can also be excavated via SNMP. Digging deeper, most access point SNMP stacks will give traffic per MAC address, which can be graphed. If it's a router, it will also have the corresponding IP addresses.

You can also get traffic information by sniffing the traffic between the access point and the router. This will also have all the users MAC addresses. However, there is a gotcha. It will not show wireless to wireless traffic, which does not go through the router section and onward to the internet. If you have "client isolation" enabled in the access points, no problem as there is no client to client traffic. If you do have client to client traffic, sniffing will not work.

>What I don't want to know is what sites the computers on my small
>network are visiting? It's not my job. I just want to warn a user of
>the network I "manage", that uses too much bandwidth in a "suspect" way
>that if he keeps going on, he'll have no more connection.

Daily traffic quotas? It would be simple enough to use SNMP to accumulate daily traffic statistics from perhaps midnight to midnight. If any such traffic totals exceed an authorized value, then they get an automatic nastygram in the email. Been there, done that, and it doesn't work. The problem is that the alert appears much after the abuse has taken place. Even setting quotas on a per hour basis proved too late. It has to be caught quickly and dealt with immediately as the support phones will start ringing immediately and the NOC will not have a clue who or what is happening.

It's MUCH easier to not play policeman and simply install some form of bandwidth management or QoS that proactively prevents abuse. Time limiting is also possible such as Directway, which starts out fast, but slows down after some level of traffic threshold has passed.

I don't have a specific suggestion that would not involve replacing some of your hardware. I also have little clue as to what you have to work with and how much of it supports SNMP. I suggest you look at the various network monitoring tools available and decide what will work for you.

Also, note that your users will probably need to authenticate with a RADIUS server in order to simply identify which wireless connection belongs to which users. It's very easy to change MAC addresses and fool the NOC. That probably means a dedicated authentication server and SNMP data collector. Whether this is worth the effort for 30 users is rather dubious.

You might find the following interesting.
<http://martybugs.net/wireless/rrdtool/>

<http://martybugs.net/linux/rrdtool/traffic.cgi>

—

Jeff Liebermann jeffl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
150 Felker St #D <http://www.LearnByDestroying.com>
Santa Cruz CA 95060 <http://802.11junk.com>
Skype: JeffLiebermann AE6KS 831-336-2558

• *Follow-Ups:*

- ◆ **[Re: Lan Wifi Network](#)**
◇ *From:* cherriesbaked

• *References:*

- ◆ **[Lan Wifi Network](#)**
◇ *From:* cherriesbaked
- ◆ **[Re: Lan Wifi Network](#)**
◇ *From:* Jeff Liebermann
- ◆ **[Re: Lan Wifi Network](#)**
◇ *From:* cherriesbaked

- Prev by Date: **[Re: How can I tell if someone is using my wireless net?](#)**
- Next by Date: **[Re: Belkin Pre-N notebook card problems](#)**
- Previous by thread: **[Re: Lan Wifi Network](#)**
- Next by thread: **[Re: Lan Wifi Network](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**