Raceless network configuration

Questions and questions

Vadim Zhukov <zhuk@openbsd.org>

What's the all fuss is about?

- How do you switch to another network?
  - by running ifconfig a few times, or running it once with a couple of command line parameters?
  - by putting those calls behind a script/config file?
- Anyway, you're doomed

How it really works

- So you have a network interface. How to manage it?

How it really works

- So you have a network interface. How to manage it?
- ioctl() calls, right. But how much?

How it really works

- So you have a network interface. How to manage it?
- ioctl() calls, right. But how much?
- Lots of them.

The ioctl madness

```
SIOCS80211NWID
SIOCS80211WEPKEY
SIOCS80211WPAPSK
SIOCS80211POWER
SIOCS80211CHANNEL
SIOCS80211BSSID
SIOCS80211TXPOWER
SIOCS80211WPAPARMS
SIOCS80211FLAGS
```

- Do you think that's all?

The ioctl madness

- Do you know what happens when you set up your WPA parameters?
  - Enable WPA itself? – SIOCS80211WPAPARMS
  - Set allowed WPA version? – SIOCS80211WPAPARMS
  - Set allowed ciphers list? – SIOCS80211WPAPARMS

The ioctl madness

- Do you know what happens when you set up your WPA parameters?
  - Enable WPA itself? – SIOCS80211WPAPARMS
  - Set allowed WPA version? – SIOCS80211WPAPARMS
  - Set allowed ciphers list? – SIOCS80211WPAPARMS
  - Set WPA key? – oh, it's different: SIOCS80211WPAPSK

The ioctl madness

- Do you know what happens when you set up your WPA parameters?
  - Enable WPA itself? – SIOCS80211WPAPARMS
  - Set allowed WPA version? – SIOCS80211WPAPARMS
  - Set allowed ciphers list? – SIOCS80211WPAPARMS
  - Set WPA key? – oh, it's different: SIOCS80211WPAPSK
- Yes, all of them do operate on the same structure.

Philosophy question

- A few hours ago you've exited you hotel (or other home) and went to the conference.
- At some later point in time you arrived here.
- Where were you in between?
  - Would you say to someone: “Let's meet in the hotel hall”?
  - Would you say to someone: “I'm on the Track C”?

Switching between networks

- So, a couple of ioctl() calls are made, forming many intermediate states.
- But the packets do still flow!
- Do you really want to send data from old connections via the new one?
  - Note: it won't work anyway as you'll get different address.

What do others do?

- Cisco IOS does a really good job here.

What do others do?

- Cisco IOS does a really good job here.
- But it can't run KDE.

What do others do?

- Recent Windows versions do have netsh.
- But the API it uses is awful.
  - Put interface down and up by a simple function call? Are you kidding?
- But GUI is good.

What do others do?

- Red Hat Linux is usually called enterprise solution.
- If the “enterprise” means “we do the same shit as others, but you may pay for it”, I'll agree.
- /etc/sysconfig/network-scripts/ifcfg-* do not differ too much from /etc/hostname.* (or /etc/ifconfig.*, whatever).
- Network Manager does a GUI, though.

What do others do?

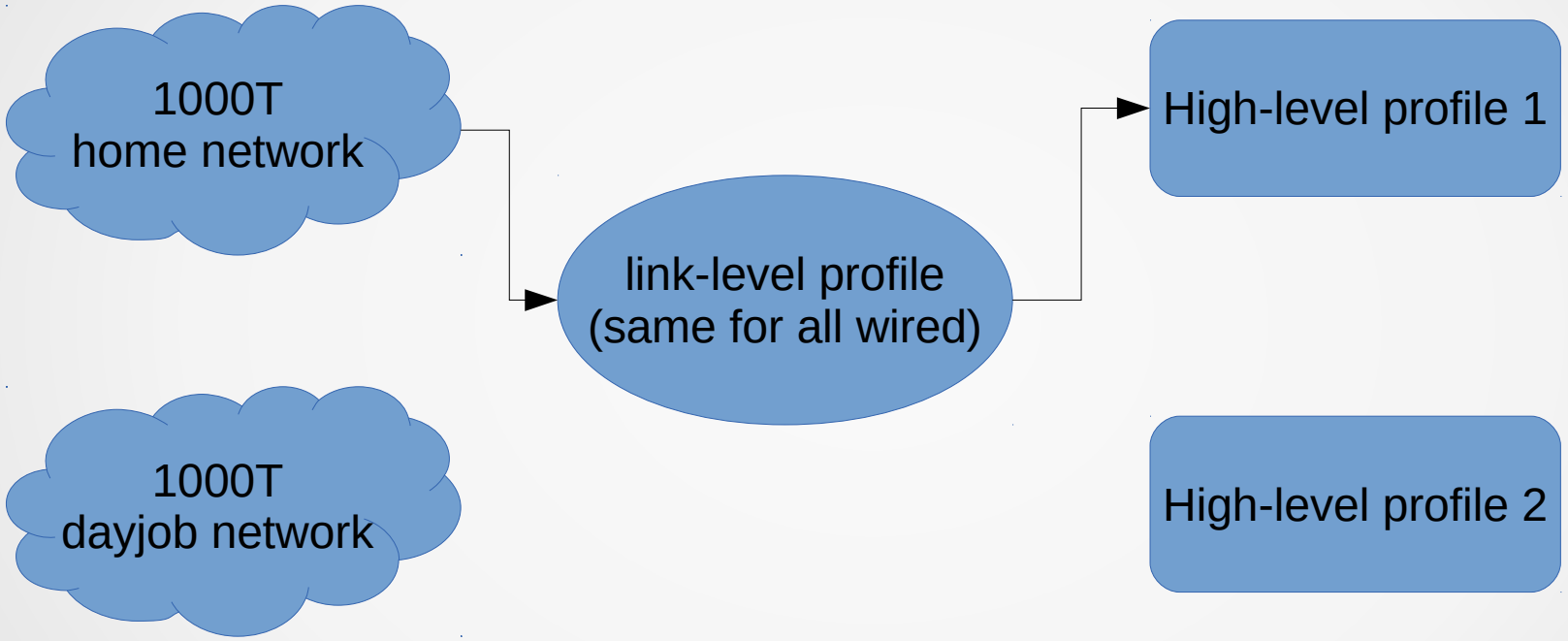
- Solaris has a perfect network profiles architecture.
- The 802.11 part isn't that promising, though.
- Can't comment on GUI.

Proposal 1

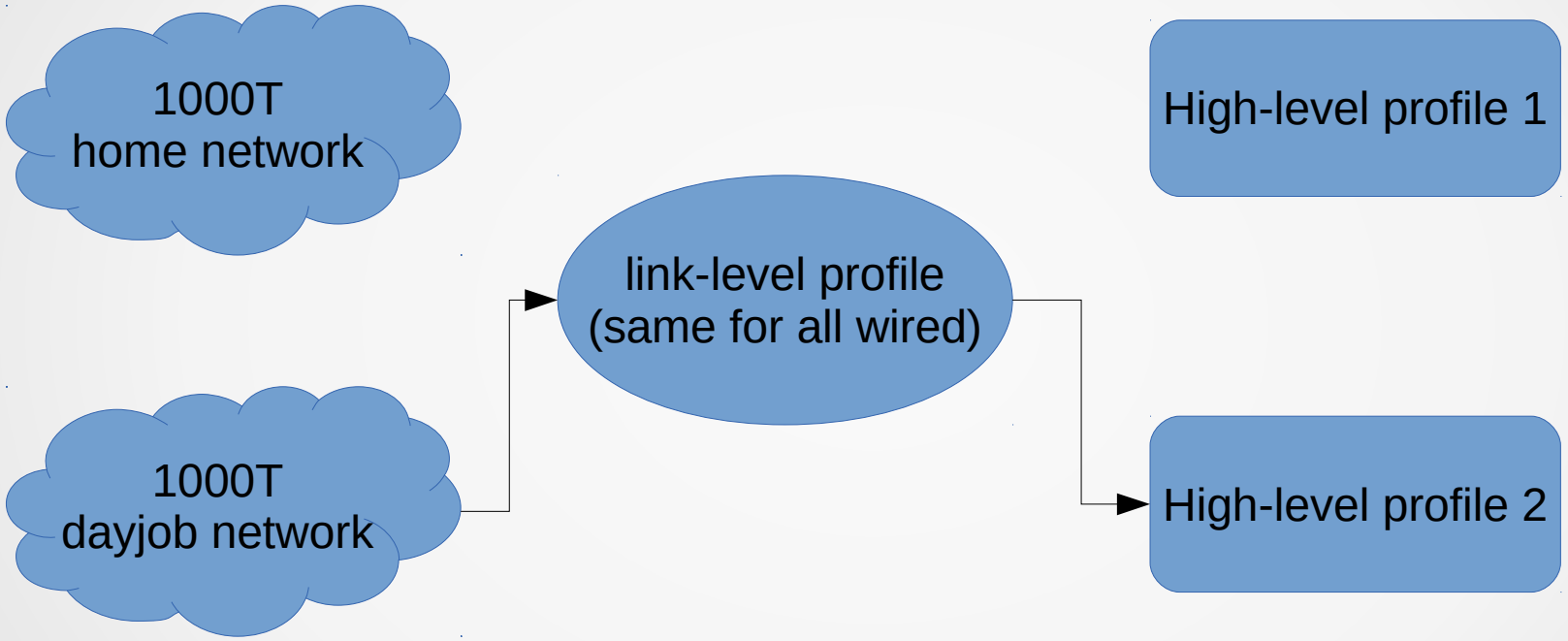
- Implement some sort of network profiles that will list all known and trusted (by us) networks.
  - In particular, keys/passwords will be kept.
  - Absolutely needed by wireless communications.
  - Could be used by wired one, too, but will likely need a help from dhclient(8).
    - Should there be more than one profile level?

Profile levels subproposal

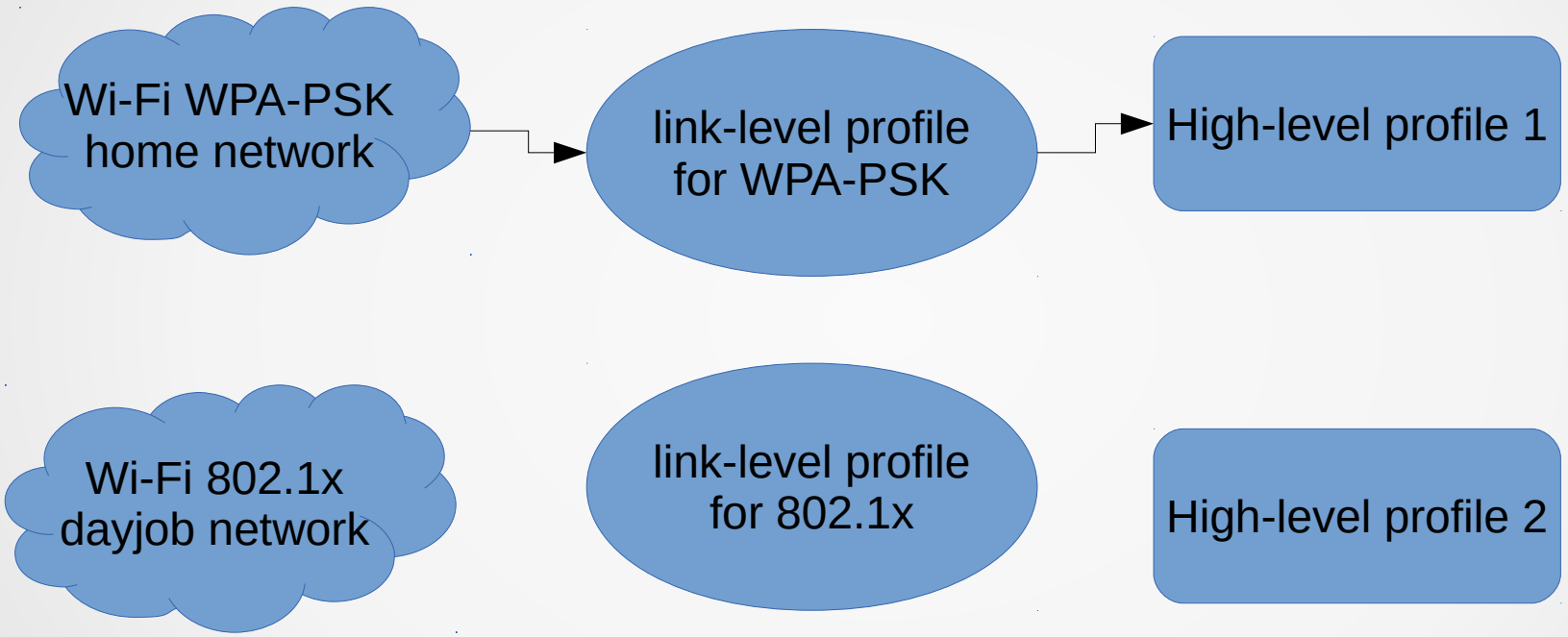
Profile levels subproposal



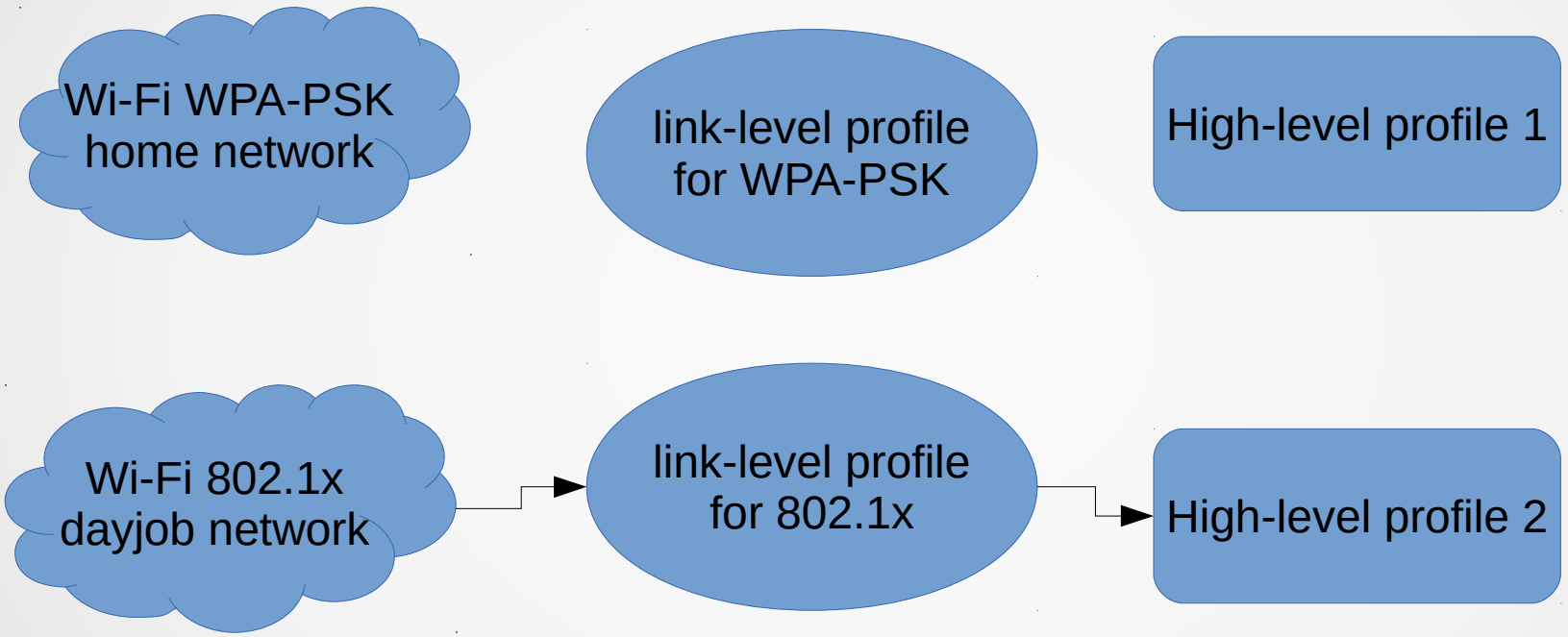
Profile levels subproposal



Profile levels subproposal



Profile levels subproposal



More than just roaming

- Unknown networks: to trust or not to trust?
  - 802.1x case: why not?
  - Other cases: the user should know better. But how to ask?

The 802.11 state machine

(comments are removed for readability)

```
enum ieee80211_state {
        IEEE80211_S_INIT        = 0,
        IEEE80211_S_SCAN        = 1,
        IEEE80211_S_AUTH        = 2,
        IEEE80211_S_ASSOC       = 3,
        IEEE80211_S_RUN         = 4
};
```

Proposal 2

- Implement new network interface state, say, `IEEE80211_S_CONFIRM`
- No traffic should pass here except association-related.
- It could be good to drop connections routed through the interface before.
  - Even non-if-bound ones? Or do if-bound default?
  - What to do with datagram sockets?

Proposal 2

- Implement new network interface state, say, `IEEE80211_S_CONFIRM`
- To move on, some application should either:
  - get the list of applicable profiles (could be 0, 1 or more);
  - get the list of unknown networks (could be 0, 1 or more);
  - if desired, set up new network profile, asking user for network keys;
  - call a special ioctl() to resume operation.

Proposal 2

- Implement new network interface state, say, `IEEE80211_S_CONFIRM`
- Now the kernel looks at (probably renewed) list of network profiles and chooses first matching one.
  - Should we allow to choose non-first matching one?
  - If yes, how? It becomes too complex (read: buggy).

Proposal 2

- Implement new network interface state, say, `IEEE80211_S_CONFIRM`
- Wait, this is about 802.11!

Proposal 2

- Implement new network interface state, say, `IEEE80211_S_CONFIRM`
- Wait, this is about 802.11!
  - Embed the state machine in non-802.11 drivers?
    - Some drivers are synced with upstream from time to time, so it shouldn't add a merge pain...
  - Ideas are welcome!

Current state

- Network profiles: iteration #2.5
  - Enabled on 802.11 interfaces with special flag set.
    - no flag means things behave the traditional way
  - Allows to upload and download profiles to/from kernel;
  - A userland daemon called autonetd maintains loading profiles and performs additional actions on profile activation/deactivation

Sample autonetd.conf

```
assoc mode lazy
scan period 15
network myhome auth wpa2 " vERy SEcrEt PaSsWOrD!@#$%^&*()"
inet6="config inet6 autoconf"
network "Best Job Ever, Inc." auth 802.1x
        $inet6
        address 192.168.2.78/24
        run on assoc cmd   /sbin/route add default 192.168.2.1
        run on deassoc cmd /sbin/route delete default
defaults
        config -inet6
        no dhcp
        run async shell "echo autonetd connected to open network" \
                "\"${NWID}\" on the ${IFNAME} >>/tmp/wifi.log"
network "BestFriend_home" auth wpa 12345678
network "free wi-fi" on iwm0 open
        $inet6
        dhcp
network "MosMetro_Free" open
        inherit defaults
        captive mosmetro
```

Current state

- Network profiles: iteration #2.5
  - Enabled on 802.11 interfaces with special flag set.
    - no flag means things behave the traditional way
  - Allows to upload and download profiles to/from kernel;
  - A userland daemon called autonetd maintains loading profiles and performs additional actions on profile activation/deactivation
  - Will likely bite the dust as well as previous iterations.

Current state

- In theory, profiles could/should be loaded by utility we already have in base:
  - ifconfig
- But there is no consensus on syntax yet
  - and should it be always the whole bunch, or one-by-one?

What's next?

- Discuss the concerns with more people.
  - Everybody here is invited!
- Start implementing the IEEE80211_S_CONFIRM state.
  - When it's polished inside sys/net80211, we could start moving outside of it.

Credits and thanks

- Stefan Sperling
- Theo de Raadt
- Mark Kettenis
- Jonathan Gray
- Stuart Henderson
- and all other people who reviewed, tested and willing to help further.

Credits and thanks

- Stefan Sperling
- Theo de Raadt
- Mark Kettenis
- Jonathan Gray
- Stuart Henderson
- and all other people who reviewed, tested and willing to help further.
- EuroBSDCon organizers
  - especially Jahne Johansson for his incredible patience
- Sweden
  - for nice weather, people, trains and jam

Credits and thanks

- Stefan Sperling
- Theo de Raadt
- Mark Kettenis
- Jonathan Gray
- Stuart Henderson
- and all other people who reviewed, tested and willing to help further.
- EuroBSDCon organizers
  - especially Jahne Johansson for his incredible patience
- Sweden
  - for nice weather, people, trains and jam
- Flying Pasta Monster
  - just to be on a safe side

Questions?

Final credits

- Thank you all for allowing me to steal almost an hour of time from each of you. :)
  - This should give me a few days of life in total!