DNSSEC w/o Humans?

Ólafur Guðmundsson ogud@shinkuro.com
Bob Novas bob@shinkuro.com
Shinkuro Inc.

Icann-44 Prague June 2012

DNSSEC validation where?

Where	What is protected	Managed
ISP	All customers	Staff
Office / Enterprise DNS resolver	The systems using that resolver	Staff
End system	All applications on the system	User
Application	That particular application	User

What's missing?

Unmanaged DNSSEC validators

DNSSEC +

- Protects the whole home/office network !
  - Possible ?
  - Fast enough ?
- What about configuration ?
- Looking for inexpensive 99% solution

1. We did it in Open-WRT and DD-WRT
2. Unbound faster than DnsMasq, most of the time
   1. Upto 4000 q/s vs 800 q/s
   2. 200+ validations/second
3. DNSSEC-Trigger does most of the configuration work, we provide wrapper for environment and schedule

Leverage

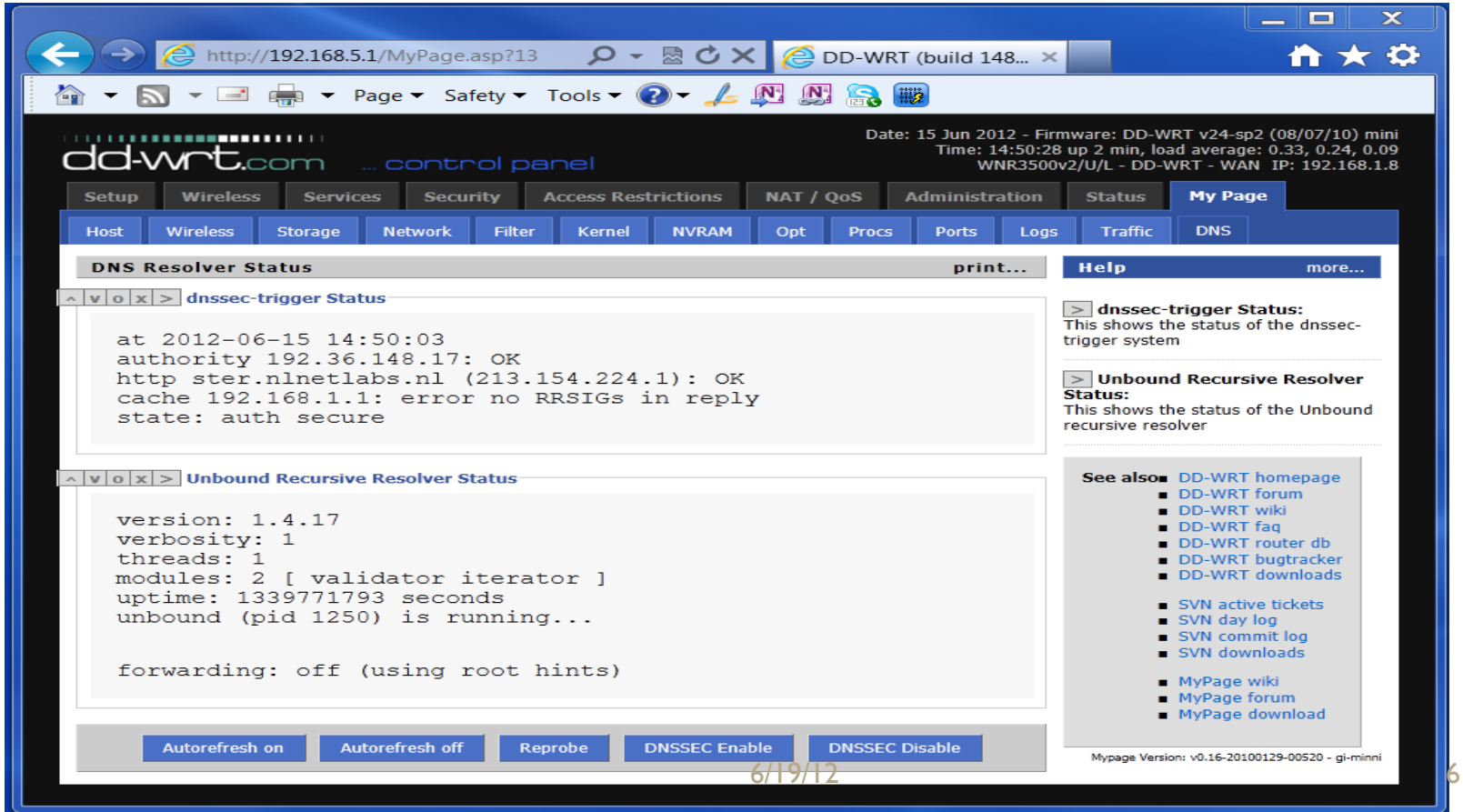
- ISP DNS infrastructure when possible
  - Forward queries when ISP DNS "good enough"
    - FCC-A grade == DNSSEC validation
    - FCC-B grade == DNSSEC records passed
- Open Source software
  - Unbound
  - Dnssec-trigger
  - Open-wrt and DD-wrt

Goal: detect and turn on DNSSEC by default: Issues seen

- *Routers clock does not have battery backup*
  - Wait for time to sync before enabling DNSSEC
- *No writeable file system (DD-WRT)*
  - Use NVRAM variables instead of files to persist user configuration
  - Sym link some files to writable file system (/tmp) and write the file at startup from the configuration in nvram
  - Run **unbound-anchor** on every boot
- *Address can be dynamic or static*
  - Extend DNSSEC-trigger to deal with static addresses
- Network connection down/changes
  - DNSSEC-Trigger Reprobe every 5 minutes
  - Disable DNSSEC when network goes down

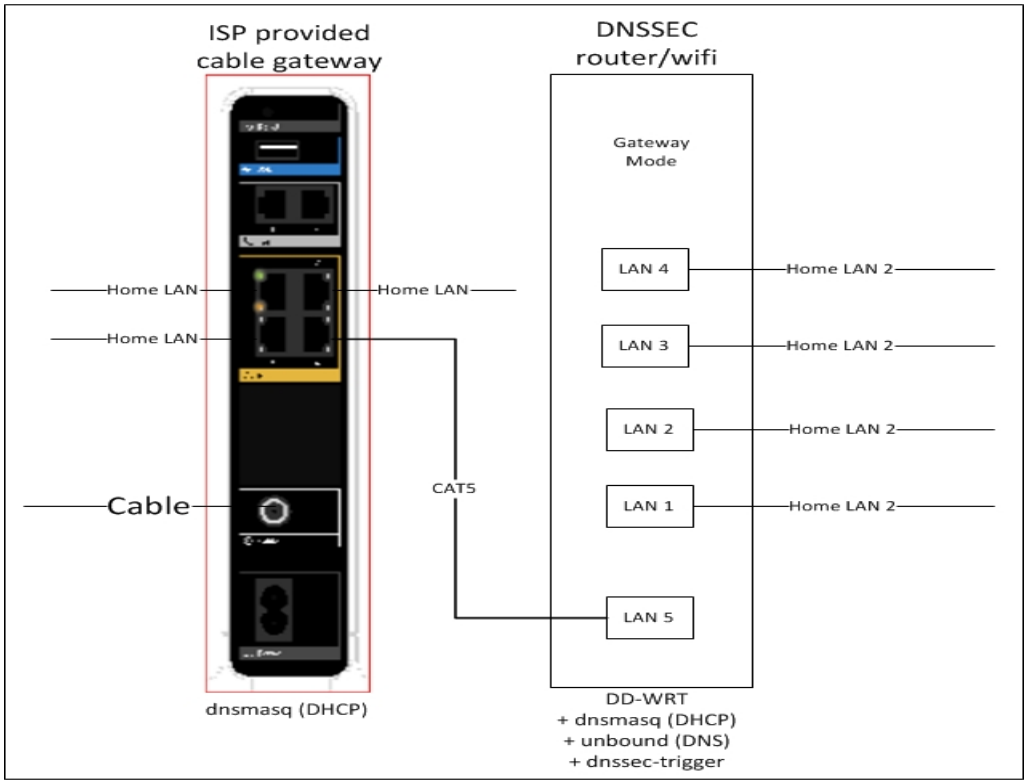
How much to expose in UI?

- Not at all ? Only status ? Full configuration ?



How to use?

- Connect directly to internet or



Next steps

- Add Authorative zone support with DNS updates
  - Looking at options
- Make distributions available for download
  - Test in adverse networks
- Work with vendors to incorporate in products

Backup slides

Home routers/gateways

- Inexpensive, Low power requirement, frequently do DNS
- DNS is proxy i.e. forwards queries to ISP
- Computing power is limited but sufficient.
- Most humans plug in and do minimal changes if any
  - Change wireless network name and passphrase

Test environment

- Buffalo WZR-HP-G3000N
- Netgear WNR3500L

	Buffalo	Netgear
CPU	AR7242 + AR9280 + AR8316	Broadcom 4718A
Static Ram	32	8
Ram	64	32
Wireless Network	BGN	BG
Disk	None	none
Cost	$70	$30 refurbished

Quick Performance test

- Buffalo running Open-WRT
  - DNSMasq and Unbound both forwarding to local servers
  - we used parallel queries to stress test resolvers, all queries resolve on local net
  - Netgear had similar performance

	DNSMasq	Unbound
Recursive Cold, no cache reuse	700 q/s	700 q/s
Recursive Warm with cache reuse	700 q/s	4000 q/s
DNSSEC validations no cache reuse	X	140 q/s
Remote DNSSEC test serial queries	5 q/s	7 q/s