Status of IPv6 in Linux

by Dr. Peter Bieringer

12th International Linux System Technology Conference
October 11-14, 2005
at University of Hamburg, Germany

IPv6

Contents

- About me
- Status of IPv6 support in Linux
- Status of IPv6 support in applications
- Configuring IPv6 on a Linux box
- Configuring IPv6 in applications
- Summary & Outlook
- Further Information

About me (or who I am)

- Living in Munich (Germany)
- Employee of *AERAsec Network Services and Security GmbH* (since 2000)
  - focussing on IT security and network consulting
  - trainer for IPv6, TCP/IP and others
- Co-founder and core member of *Deep Space 6*
- Member of the German IPv6 Task Force

My IPv6-related time line

- 1993: First contact with the Internet
- 1996: Got in touch with IPv6
- 1997: *IPv6 & Linux - HowTo*, *initscripts-ipv6*
- 1999: *IPv6 & Linux - Current Status*
- 2001: *Linux IPv6 HOWTO*, *ipv6calc*
- 2002: Co-founded *Deep Space 6*

Status of IPv6 support in Linux

IPv6 support in Linux

- Several components need IPv6 support in Linux
  - Kernel
    - Networking
      - e.g. interface configuration, routing, sockets
    - Firewalling
  - C-Library
    - resolver functions
      - resolve IPv6 addresses
    - RPC (portmapper)
  - Security extensions
    - TCP-Wrapper

IPv6 support in Linux

- Several components need IPv6 support in Linux (cont'd)
  - Server applications
    - Have to understand IPv6 addresses in configurations
    - Have to use IPv6 server socket (either selected by configuration or by default)
    - Should proper log IPv6 addresses
  - Client applications
    - Have to understand IPv6 addresses in input
    - Have to understand AAAA records during DNS resolving
    - Should use IPv6 socket, if AAAA record is in DNS available
      - Should have an option to force IPv6 or IPv4 connection if both addresses are available

History of IPv6 in Linux - Kernel

- History of IPv6 implementation in Linux kernel
  - First rudimentary in version 2.1.8 (1996)
  - 2.2.19+ worked relatively stable, but less features
  - 2.4.x works relatively stable, some more features
  - In October 2000 the USAGI team was founded with focus of implementing all required features into the kernel
    - URL: http://www.linux-ipv6.org/
  - USAGI team submitted patches for 2.5.x series
    - Some of them backpatched to 2.4.x series
  - Awarded with *IPv6 Ready Logo*™ (Phase 1)
    - USAGI snapshot 20040119 (and later)
    - For router and host role

Status of IPv6 in Linux - Kernel

- Ongoing development for 2.6.x series by USAGI team and others, e.g.
  - Fixing problems reported by TAHI Conformance Test Report
    - Goal is getting the *IPv6 Ready Logo*™ (Phase 2)
  - Completing IPsec support
  - Stateful IPv6 netfilter (connection tracking)
  - Multicast routing
  - Implementing Avanced API (RFC 3493)
  - Mobile IPv6 http://www.mobile-ipv6.org/

Note: USAGI kernel patch (20050912) diffstat:

91 files changed, 10283 insertions(+), 451 deletions(-)

~ 50 % related to IPv6 connection tracking

Status of IPv6 in Linux – IPv6 IPsec

- USAGI and Netdev team ported code of *BSD KAME project to Linux
  - Replaces KLIPS code of FreeS/WAN
  - Features IPv4 and IPv6 support
- IKE daemons *racoon* and *pluto*
  - Both are IPv6 capable
  - *racoon* was also taken from KAME project, intention was replacing *pluto* (from the FreeS/WAN project) because of its complex code base
  - *pluto* was extended to support native IPsec of 2.6.x kernels
    - now maintained by *Openswan* http://www.openswan.org/

Firewalling in IPv6 is very important...

...there is no implicit „protection“ anymore!

Reasons for IPv6 Firewalling

- Firewalling in IPv6 is very important, because
  - Client gets a global IPv6 address by design
    in case if a global prefix is available
    - quickly happen by autoconfiguration after receiving a router advertisement (RA)
  - Unlike in IPv4, no hiding NAT on border routers is possible
    - In IPv6, NAT was left out from design (see also RFC 2993)
    - But hiding NAT in IPv4 does not solve all security problems...think about tunneling via HTTPS (HTTP CONNECT), DNS or ICMP payload

  Without protection, any non-local listening service can be accessed from remote!

Like in very modern IPv4 world

firewalling on

border AND **host**

is also required for IPv6

In addition use TCP-Wrapper configuration for increasing security!

Status of IPv6 firewalling in Linux

- TCP-Wrapper
  - Patch is available for (latest) version 7.6
    - Mostly included in distributed binaries
- Packet filtering
  - Modern Linux kernel contains netfilter firewalling
    - ipchains was replaced 2001 in 2.3.x series
    - User-space tool for IPv6: ip6tables
    - Development
      - Netfilter team with help by USAGI team

Status of IPv6 netfilter in Linux

- Connection tracking
  - Vanilla kernels (until at least 2.6.13.1) only supports stateless IPv6 packet filtering (like old ipchains for IPv4)
  - Already available in USAGI extension, but waiting to be included in vanilla kernel
  - Work is ongoing to abstract the connection tracking code for common use with IPv4 and IPv6 (scheduled for 2.6.15)
- General
  - Already very useful to protect a host
  - GUI tools (e.g. fwbuilder until at least 2.0.8) still miss IPv6 support - scripts have to be used instead (examples and tool sets are available)

Example of IPv6 netfilter rules in Linux

- Minimal ruleset (for use with *ip6tables-restore*):

```
*filter
:INPUT DROP [12:440]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [12:440]
-A INPUT -s ::/0 -d ::/0 -p tcp -m tcp --dport 512:65535 ! --tcp-flags
  SYN,RST,ACK SYN -j ACCEPT
-A INPUT -s ::/0 -d ::/0 -p udp -m udp --dport 512:65535 -j ACCEPT
-A INPUT -p icmpv6 -j ACCEPT
-A INPUT -m limit --limit 5/min -j LOG
-A INPUT -j DROP
COMMIT
```

- Allow incoming SSH from anywhere:

```
-A INPUT -p tcp --dport 22 -j ACCEPT
```

- More hints available at:

  http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/chapter-firewalling-security.html

DNS IPv6 status – resolver

- IPv6 address query support
  - GNU C-Library since version 2.1
  - dietlibc
- Resolver able to use IPv6 transport for queries
  - GNU C-Library since version 2.2
  - dietlibc since version 0.10
- RPC bind (portmapper)
  - GNU C-Library: status currently unknown
  - dietlibc: not planned

DNS IPv6 status - server

- Support of „AAAA“ record
  - BIND since version 4.9.5
- Native IPv6 transport of queries
  - BIND8 since version 8.4.0
  - BIND9
  - djbdns (with patch from Felix Leitner – experimental)
- Note:
  - No changes are required for the reverse lookup (PTR), each nibble of the expanded IPv6 address is separated by a dot, same mechanism as on IPv4 is used

Status of IPv6 support in applications

IPv6-ready daemons/clients

List is not exhaustive, see for more:

http://www.deepspace6.net/docs/ipv6_status_page_apps.html

- SSH: OpenSSH
- HTTP: Apache2, thttpd, Mozilla, konqueror, lynx, w3m
- FTP: proftpd, vsftpd, pure-ftpd, lftp
- E-Mail: postfix, sendmail, exim, courier, courier-imap, dovecot, solidpop3d, mutt, ximian-evolution
- LDAP: openldap
- Routing: quagga, zebra, MRTd

Configuring IPv6 on a Linux box...

...some scenarios

Enable IPv6 on Linux client

- General: enable IPv6 in kernel
  - Usually, current distributed kernel binaries are IPv6 enabled
- Activate IPv6 by loading the kernel module „ipv6“
  - Manual:

```
# modprobe ipv6
```

  - After next reboot (current Debian and Fedora Core already contain this by default)

Kernel 2.4.x:

```
# echo "alias net-pf-10 ipv6"
>>/etc/modules.conf
```

Kernel 2.6.x:

```
# echo "alias net-pf-10 ipv6"
>>/etc/modprobe.conf
# depmod -a
```

Enable IPv6 on Linux client

- Prerequisites:
  - Native IPv6 connectivity is available on the link
  - A router sends advertisements (RA)
- Autoconfiguration does the rest for you:
  - adds IPv6 address using the prefix received by the RA

```
# ip -6 addr show dev eth0 scope global
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qlen 1000
    inet6 2001:db8:0123:4567:210:b5ff:fe01:2345/64
  scope global dynamic
       valid_lft 298sec preferred_lft 198sec
```

  - adds default route to the address of the router which is received also by the RA

```
# ip -6 route show default
default via fe80::280:c8ff:fea9:abcd dev eth0  proto
  kernel  metric 1024
```

Enable IPv6 on Linux client

- Prerequisites:
  - Native IPv6 connectivity is available on the link
  - No router sends advertisements
- Manual setup
  - Add an IPv6 address to the interface

```
# ip -6 addr add 2001:0DB8::2/64 dev eth0
# ip link set dev eth0 up
```

  - Add static route to a router

```
# ip -6 route add ::/0 via 2001:0DB8::1
```

    - Note that support of manual setup of default route in IPv6 does not work on earlier kernels (use `2000::/3` instead)

IPv6 on Linux client - 6to4 tunneling

- Prerequisites:
  - Global routable IPv4 address on one interface (eth?, ppp?)
- Manual setup
  - Generate 6to4 prefix

```
# ipv6calc -q --action conv6to4 192.0.2.1
  2002:c000:201::
```

  - Create a tunnel interface

```
# ip tunnel add tun6to4 mode sit ttl 64 remote any
  local 192.0.2.1
# ip link set dev tun6to4 up
```

IPv6 on Linux client - 6to4 tunneling

- Manual setup (cont'd)
  - Add 6to4 IPv6 address to the interface (example suffix ::1)

```
# ip -6 addr add 2002:c000:201::1/16 dev tun6to4
```

  - Add static route through device to IPv4 anycast address of 6to4 relays

```
# ip -6 route add ::/0 via ::192.88.99.1 dev tun6to4
  metric 1
```

    - Note if your implementation don't like the compatible address `::192.88.99.1`, try `2002:c058:6301::1` instead

- Further information:
  - http://staff.csc.fi/~psavola/residential.html (how 6to4 works)

IPv6 on Linux client - static tunneling

- Prerequisites:
  - Global routable IPv4 address on one interface (eth?, ppp?)
    - Static IPv4 address in normal cases
    - Dynamic IPv4 address can be used using heartbeat protocols
      - E.g. by SixXS Tunnel Broker, URL: http://www.sixxs.net/ 
  - IPv4 address of remote tunnel server
- Manual setup
  - Create a tunnel interface

```
# ip tunnel add sit1 mode sit ttl 64 remote 192.0.2.254
  local 192.0.2.1
# ip link set dev sit1 up
```

  - Add static route through device

```
# ip -6 route add ::/3 dev sit1 metric 1
```

IPv6 on Linux router

- IPv6 enabled router
  - Can supply native IPv6 connectivity for a local network
  - Supply autoconfiguration for clients by using
    - Router Advertisement Daemon *radvd*
    - DHCPv6 server *dhcp6s* 
  - Can provide upstream connectivity via tunneling
  - Should have IPv6 firewalling configured
    - Remember: no NAT is available in IPv6 for „auto-protection“ on layer 3 and 4 (IPv6 and ICMP/TCP/UDP)!

IPv6 on Linux router

- Manual setup
  - IPv6 configuration of at least 2 devices (e.g. LAN and tunnel interface)
  - IPv6 forwarding needs to be enabled

```
# sysctl -w net.ipv6.conf.all.forwarding=1
```

  - Provide autoconfiguration information for clients
    - Router Advertisement Daemon *radvd*
      - Configuration file: /etc/radvd.conf
    - DHCPv6 server *dhcp6s*
      - Configuration file: /etc/dhcp6s.conf
    - More hints available at:
      http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/chapter-autoconfiguration.html

Permanent IPv6 setup in Linux

- Depends on support in the used Linux distribution
  - Red Hat migrated *initscripts-ipv6* extension into their *initscripts* package
    - *initscripts-ipv6* is probably the fullest featured one ;-)
  - Some other vendors (e.g. Debian, SuSE) use different configuration file and rc-script structures
    - *initscripts-ipv6* extension cannot be used here :-(

Permanent IPv6 setup in Linux

- Description of permanent IPv6 setup
  - Fedora/Red Hat Linux and others which using *initscripts*
    - File: /usr/share/doc/initscripts-<version>/sysconfig.txt
    - *initscripts-ipv6* homepage: http://www.deepspace6.net/projects/initscripts-ipv6.html
  - Debian and clones
    - Craig Small's web page http://people.debian.org/~csmall/ipv6/setup.html
  - SuSE
    - File: /usr/share/doc/packages/sysconfig/README

IPv6 is now configured on the Linux box...

now let's look for support in applications

IPv6-enabling of DNS

- BIND server „named“ (http://www.isc.org/products/BIND/)
  - Adjust listen option in configuration file (usually */etc/named.conf*) section `options {...}`

```
listen-on-v6 { any; };
```

- glibc resolver (http://www.gnu.org/software/libc/libc.html)
  - For sending queries via IPv6 (supported since version 2.2), specify IPv6 address in */etc/resolv.conf*

```
# ns.ripe.net
nameserver 2001:610:240:0:53::193
nameserver 193.0.0.193
```

  - Sometimes it’s necessary to enable AAAA queries on host-to-address resolution in configuration file */etc/nsswitch.conf*

```
hosts:      files dns6
```

IPv6-enabling of SSH

- SSH
  - OpenSSH server „sshd“ (http://www.openssh.org/)
    - Configuration file, usually */etc/ssh/sshd_config*
      - Adjust listen option

```
...
Listen ::
...
```

  - OpenSSH client „ssh“
    - Use command line option to force IPv6 connect

```
# ssh -6 ::1
```

IPv6-enabling of HTTP

- HTTP

  - Apache2 webserver (http://httpd.apache.org/)
    - Configuration file, usually /etc/httpd/conf/httpd.conf
      - Extend listen option

```
Listen 192.0.2.1:80
Listen [2001:DB8::1]:80
```

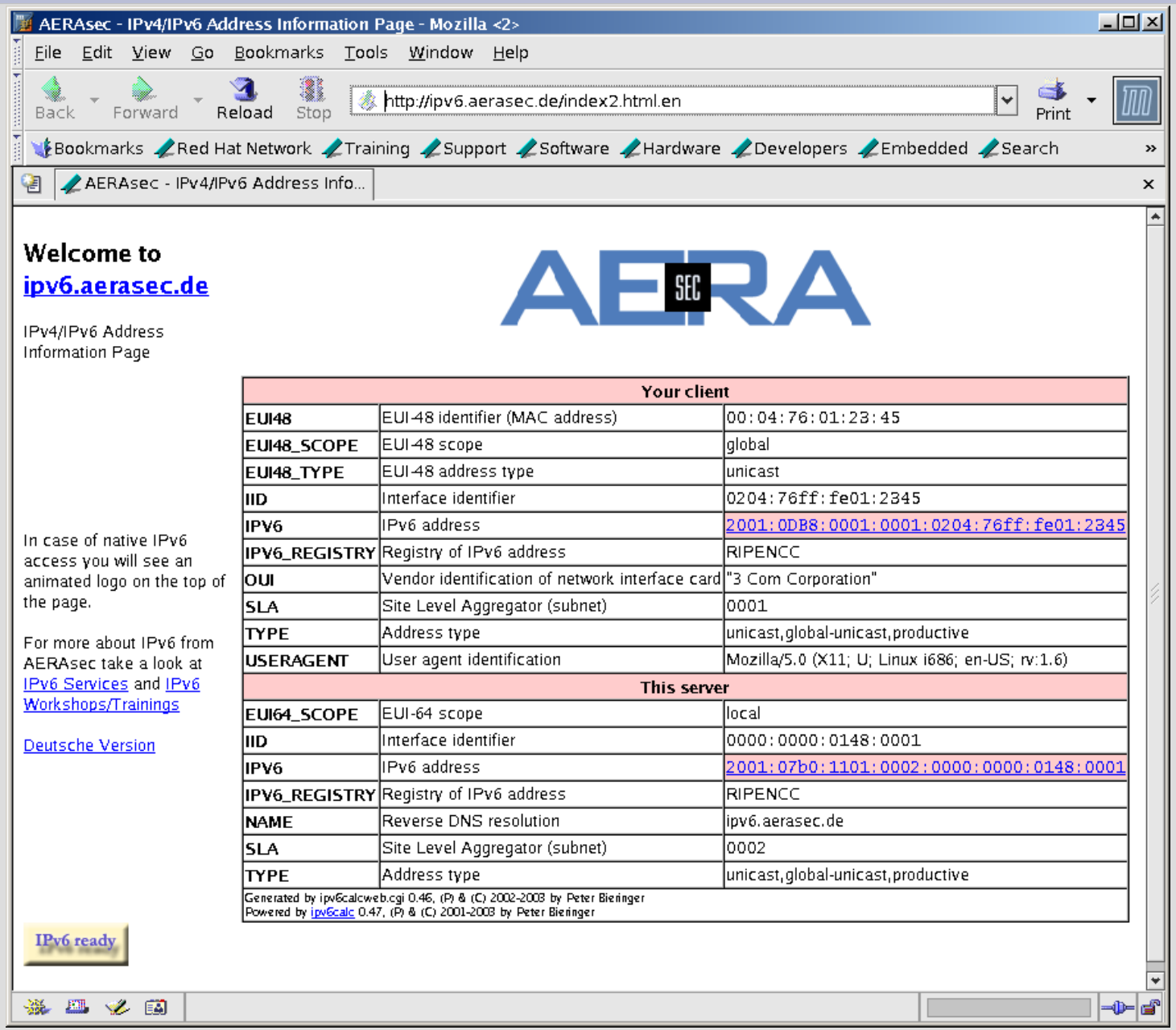
      - Extend virtual host option, if required

```
<VirtualHost [2001:DB8::1]:80 192.0.2.1:80>
</VirtualHost>
```

  - Mozilla/Firefox web client (http://www.mozilla.org/)

    - IPv6 support in current distributed binaries enabled by default
    - Most proxies don't support IPv6 to client at the moment, so specify not to use any proxy
      - For IPv6 connectivity tests try e.g. http://ipv6.aerasec.de/

IPv6-enabling of HTTP



IPv6-enabling of SMTP/POP3/IMAP4

- SMTP
  - Postfix server (http://www.postfix.org/)
    - Native IPv6 support since 2.2.x
    - Enable IPv6 for client and server by option in *main.cf*

      ```
      inet_protocols = all
      ```
    - Dedicated bind address for client can be specified in *main.cf*

      ```
      smtp_bind_address6 = 2001:db8:0123:4567::123:1
      ```
    - Dedicated listen address can be specified in *master.cf*

      ```
      [::1]:smtp  inet  n  -  n  -  -  smtpd -v
      ```

IPv6-enabling of SMTP/POP3/IMAP4

- POP3/IMAP4
  - dovecot (http://www.dovecot.org/)
    - Supports IPv6 out-of-the-box
    - Dedicated listen address configuration *dovecot.conf*

```
imap_listen = [::1]
pop3_listen = [::1]
```

  - courier-imap (http://www.courier-mta.org/imap/)
    - Supports IPv6 if compiled on an IPv6 enabled system
    - Configuration file, usually */usr/lib/courier-imap/etc/{imapd,pop3d}*

`ADDRESS=0` (default)

Summary & Outlook

Summary & Outlook

- Linux kernel
  - Ongoing coding by USAGI/netdev team to reach the 100% compatibility and add missing features
  - Stateful firewalling already developed and waits for integration into vanilla kernel
- Distribution support
  - Permanent setup capabilities and features depending on implementation
  - Application with native IPv6 support in source code mostly distributed IPv6 enabled, sometimes even if only patches are availalbe

Summary & Outlook

- Application support
  - Unix/Linux
    - Around 200 are ported or patch available
    - Major missing ones for IPv6-only networking:
      - common used syslog daemons
      - RPC for e.g. NFS (Linux specific issue, no forecast)
        - GNU C-Library: status unknown (currently none)
        - *dietlibc*: no IPv6 support planned
      - *squid* (no forecast, outdated patch, *privoxy* with patch can used instead/as cache-peer)
      - *amanda* (no forecast)
      - *coda* (first occurance of IPv6 support in 6.0.4)
    - Conclusion
      - For Internet usage mostly all applications are IPv6-enabled
      - For Intranet usage still some important application missing

Summary & Outlook

- Major question:
  - When can we deploy an Linux based IPv6-only network?
- Answer:
  - Still not 100% at the moment
  - Good: Internet usage
    - Browsing, e-Mail
  - Poor: Intranet support
    - Common used RPC/NFS, syslog to remote, caching proxies

Further Information

IPv6 & Linux related information

- *Linux IPv6 HOWTO*
  - Focus: extensive information about IPv6 on Linux
  - Currently available in the following languages:

 English (since beginning)  German (since February 2003)

 French (since May 2003)  Italian (since March 2004)

 Chinese (snapshot 2001)  Turkish (snapshot 2005)

URLs:

http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/ (English only)

http://mirrors.bieringer.de/ (en, de, fr, it)

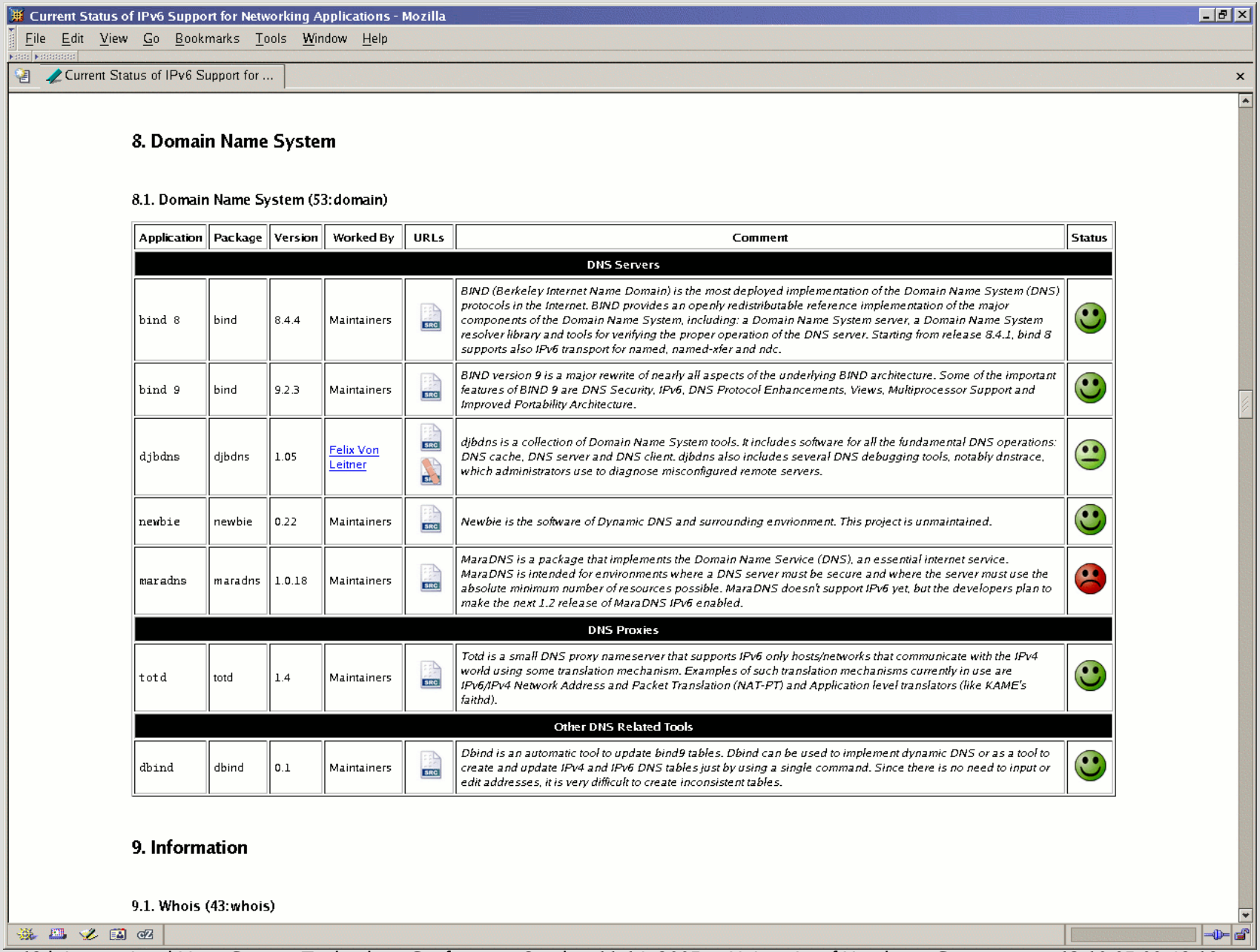
http://www.bieringer.de/linux/IPv6/ (URLs of all available languages)

IPv6 & Linux related information

- *Current Status of IPv6 Support for Networking Applications*
  - Focus: status of IPv6 in networking applications
  - Statistics (July 2, 2004):
    - Native support: 171
    - IPv6 patch available: 38
  - Contents update scheduled until end of 2005

  URL:
  http://www.deepspace6.net/docs/ipv6_status_page_apps.html

Screenshot of Application Status



8. Domain Name System

8.1. Domain Name System (53:domain)

Application	Package	Version	Worked By	URLs	Comment	Status
DNS Servers						
bind 8	bind	8.4.4	Maintainers	SRC	*BIND (Berkeley Internet Name Domain) is the most deployed implementation of the Domain Name System (DNS) protocols in the Internet. BIND provides an openly redistributable reference implementation of the major components of the Domain Name System, including: a Domain Name System server, a Domain Name System resolver library and tools for verifying the proper operation of the DNS server. Starting from release 8.4.1, bind 8 supports also IPv6 transport for named, named-xfer and ndc.*	
bind 9	bind	9.2.3	Maintainers	SRC	*BIND version 9 is a major rewrite of nearly all aspects of the underlying BIND architecture. Some of the important features of BIND 9 are DNS Security, IPv6, DNS Protocol Enhancements, Views, Multiprocessor Support and Improved Portability Architecture.*	
djbdns	djbdns	1.05	Felix Von Leitner	SRC	*djbdns is a collection of Domain Name System tools. It includes software for all the fundamental DNS operations: DNS cache, DNS server and DNS client. djbdns also includes several DNS debugging tools, notably dnstrace, which administrators use to diagnose misconfigured remote servers.*	
newbie	newbie	0.22	Maintainers	SRC	*Newbie is the software of Dynamic DNS and surrounding envrionment. This project is unmaintained.*	
maradns	maradns	1.0.18	Maintainers	SRC	*MaraDNS is a package that implements the Domain Name Service (DNS), an essential internet service. MaraDNS is intended for environments where a DNS server must be secure and where the server must use the absolute minimum number of resources possible. MaraDNS doesn't support IPv6 yet, but the developers plan to make the next 1.2 release of MaraDNS IPv6 enabled.*	
DNS Proxies						
totd	totd	1.4	Maintainers	SRC	*Totd is a small DNS proxy nameserver that supports IPv6 only hosts/networks that communicate with the IPv4 world using some translation mechanism. Examples of such translation mechanisms currently in use are IPv6/IPv4 Network Address and Packet Translation (NAT-PT) and Application level translators (like KAME's faithd).*	
Other DNS Related Tools						
dbind	dbind	0.1	Maintainers	SRC	*Dbind is an automatic tool to update bind9 tables. Dbind can be used to implement dynamic DNS or as a tool to create and update IPv4 and IPv6 DNS tables just by using a single command. Since there is no need to input or edit addresses, it is very difficult to create inconsistent tables.*	

9. Information

9.1. Whois (43:whois)

IPv6 & Linux related information

- Older documents
  - *IPv6 & Linux – HowTo*

    http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html
  - *IPv6 & Linux - Current Status*

    http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status.html
- Others
  - *initscripts-ipv6*
    - Focus: integration of handling of permanent IPv6 setup into *initscripts* (Fedora/Red Hat Linux and clones)

    http://www.deepspace6.net/projects/initscripts-ipv6.html

    http://cvs.deepspace6.net/view/initscripts-ipv6/

    http://fedora.redhat.com/projects/additional-projects/initscripts/

Tunnel Brokers

- Common used Tunnel Brokers:
  - http://www.sixxs.net/ (NL)
    - 17 Points of Presence in Europe
    - 2 located in Germany (Easynet & M”net)
  - http://www.freenet6.net/ (CA)
  - http://tb.consulintel.euro6ix.org/
  - http://tunnelbroker.as8758.net/ (CH)

Further Information

- General IPv6 information, news and links
  - http://www.ipv6.org/
  - http://www.ist-ipv6.org/

- IPv6 Task Forces
  - http://www.ipv6tf.org/
  - http://www.eu.ipv6tf.org/
  - http://www.ch.ipv6tf.org/
  - http://www.ipv6tf.de/

Contact Information

pb@bieringer.de

http://www.bieringer.de/pb/

http://www.bieringer.de/linux/IPv6/

peter@deepspace6.net

http://www.deepspace6.net/

pbieringer@aerasec.de

http://www.aerasec.de/

http://www.aerasec.de/services/ipv6.html

http://www.aerasec.de/workshops/ipv6.html

Thank you for listening!

Q&A

Credits to
Ralf Spenneberg (invitation)
Martin Schulze (invitation)