V6home:
Deploying Dual Stack E-mail

Lawrence E. Hughes
Chairman & CTO, InfoWeapons

lhughes@infoweapons.com (legacy)
lhughes@v6home.org (Dual Stack Postfix/Dovecot)
lhughes@hughesnet.org (Dual Stack Exchange 2007)

Once you get a dual stack network going, what next?

- With most Operating Systems supporting IPv6 today, it is no longer rocket science to deploy a dual stack network, complete with DNS (especially with a dual stack DNS appliance).
- It is not *that* difficult to get Internet Information Server or Apache to provide web content over IPv6, and most web applications pretty much get a “free ride” once the web server supports dual stack.
- The next major application that most people think of is Internet e-mail. If you read the relevant documentation, you discover:
  - Exchange Server 2007 (running on Windows Server 2008) has IPv6 support.
  - Most open-source mail server applications (Postfix, Dovecot, etc) have IPv6 support.
  - Most e-mail clients (e.g. Outlook, Windows Live Mail) have IPv6 support.
- Making webmail (Exchange OWA or Squirrelmail) available over IPv6 is not difficult – these are just web applications. Making SMTP, POP3 and IMAP protocols work over IPv6 *is a bit more of a challenge*.

What is the advantage of using IPv6 for email?

- The big win currently is the ability to do client access from anywhere (that has IPv6 connectivity) without having to have one of the scarce, precious IPv4 “static external” (real) addresses for every email server in your organization.
- The mail gateway for your organization will still need one of these precious IPv4 addresses, to exchange mail with other legacy mail servers over SMTP, but in a typical organization there might be many internal servers where the user accounts live. With IPv6 (combined with TLS), your remote users (road warriors or employees at home) can easily access *any* mail server without using up lots of IPv4 addresses, or having to use some VPN solution (almost certainly through NAT, which eliminates the only IETF approved VPN technology, IPsec).
- What with free tunneled IPv6 service available from several vendors (he.net, gogonet.com, etc.) you can get IPv6 service on pretty much any client computer today, over existing IPv4 service (even if you are buried behind NAT). Chances are your current email client supports IPv6 today.
- Of course, as IPv6 proliferates, there will be some mail servers and networks that are IPv6 only, so you will need to support IPv6 to use mail in those. If you attend IETF meetings, you will still be able to communicate when they turn off IPv4!

Exchange 2007

- If you search Google for “Exchange 2007 IPv6” you find almost exclusively information on how to *turn off* IPv6. It seems few network engineers have had much luck getting it to work over IPv6. Good news! I have it running dual stack nicely at my home (my address there is *lhughes@hughesnet.org*).
- The first thing you discover is that Exchange 2007 *does not run on Windows Server 2008*. You must obtain *Exchange Server 2007 SP1*. Fortunately, you can avoid the classic “chicken and egg” problem as Exchange Server 2007 SP1 is a full install, not just an update. Even better, your Exchange Server 2007 license key works fine on Exchange Server 2007 SP1.
- So, deploy Windows Server 2008 and enable IPv6. This is not difficult, and there is a fair amount of help on the Internet. Given that most of the world is still running legacy (IPv4) networks, it is critical that you deploy *dual stack*, not pure IPv6. Your server is going to have to accept mail from, and forward mail to, lots of legacy (IPv4 only) mail servers for some time to come (at least the gateway mail server must support IPv4).
- However, you can make *your* server dual stack and access it via SMTP, POP3, IMAP4 or webmail over IPv6. You can of course, also do server to server transfers over IPv6 with any other dual stack mail servers out there.

Open Source e-mail Servers

- The first choice is which open source Operating System to deploy it on (religion alert!!) My first choice is FreeBSD (which has been IPv6 Ready Gold certified the longest, and has the Kame reference stack), but OpenBSD and NetBSD have the same stack. Linux has lagged a bit behind *BSD, but even it has now achieved IPv6 Ready Gold certification. You should be OK with any of these. MacOS is basically Darwin underneath, which is a branch off of FreeBSD, so it also has the Kame stack. For other choices, you may have to do some research. Use what you know best.
- I believe all open source e-mail SMTP MTA's (Sendmail, Qmail, Exim, Postfix, etc.) currently have support for IPv6. I happen to like Postfix, so that is what I chose, and it works fine, although some of the IPv6 configuration took a bit of digging to find.
- Likewise, I believe that all open source POP3/IMAP access servers (Cyrus, Courier, Dovecot, etc.) today support IPv6. I happen to like Dovecot. It works fine.
- Again, webmail is basically just a web application. Get Apache running dual stack and you get a free ride here. I found Squirrelmail to be suitable. Your mileage may vary.
- There is a good "how-to" on deploying FreeBSD + Postfix + Dovecot + Squirrelmail, with accounts kept in MySQL. See http://www.purplehat.org. All that remains is IPv6.

Supporting IPv6 in Open Source packages

- First make sure the underlying Operating System supports IPv6. For FreeBSD, include the changes to files in /etc as described further on. Of course, you should use addresses appropriate for your network, not my addresses. Because these are servers, you must have globally routable addresses, for both IPv4 and IPv6.
- When building packages, such as Postfix, Dovecot and Apache 2.2, be sure to check the “IPv6” option in any *configure* screens, and make the changes described further on to the Postfix and Dovecot configure files.
- Verify operation of the components over IPv6 by using telnet to port 25 for SMTP, port 110 for POP3 and port 143 for IMAP. If your dual stack DNS is already working, use domain names. If not, use numeric IPv6 addresses. See examples further on.
- Installing a digital certificate for SSL/TLS operation is not affected at all by use of IPv6 – follow normal procedure.
- In your gateway firewall, it is actually simpler to allow IPv6 traffic through to inside nodes, than doing BINAT with IPv4 – no NAT to complicate things – no “missing ARP” problem requiring virtual IPs! If you don’t have an IPv6 compliant firewall you can wrap your own using FreeBSD and pf (books are available to help with this). InfoWeapon’s *SolidWall* easily handled everything I needed including tunneled IPv6.

Supporting IPv6 on FreeBSD

 # IPv4 and IPv6 config in /etc/rc.conf

```
hostname="us1.v6home.org"

ifconfig_age0="inet 172.20.0.13  netmask 255.255.0.0"
defaultrouter="172.20.0.1"

ipv6_enable="YES"
ipv6_ifconfig_age0="2001:418:5403:3000::d prefixlen 64"
ipv6_defaultrouter="2001:418:5403:3000::1"
```

 # IPv4 and IPv6 config in /etc/hosts

```
127.0.0.1               localhost localhost.v6home.org
172.20.0.13             us1.v6home.org us1
172.20.0.13             us1.v6home.org.

::1                     localhost localhost.v6home.org
2001:418:5403:3000::d   us1.v6home.org us1
2001:418:5403:3000::d   us1.v6home.org.
```

 # IPv4 and IPv6 config in /etc/resolv.conf – point to your DNS servers

```
search v6home.org
nameserver 172.20.0.11
nameserver 172.20.0.12
nameserver 2001:418:5403:3000::c
nameserver 2001:418:5403:3000::d
```

IPv6 specific configuration for Postfix and Dovecot

In /usr/local/etc/postfix/main.cf (no IPv6 specific items in master.cf)

```
# inet_protocols to set IPv4 and/or IPv6 support
# "ipv4", "ipv6", "ipv4, ipv6" or "all"
inet_protocols = all

mynetworks = 127.0.0.0/8, 172.20.0.0/16, [ipv6:::1/128], [ipv6:2001:418:5403:3000::/64]
```

In /usr/local/etc/dovecot.conf:

```
# A space separated list of IP or host addresses where to listen in for
# connections. "*" listens in all IPv4 interfaces. "[::]" listens in all IPv6
# interfaces. Use "*, [::]" for listening both IPv4 and IPv6.
listen = *, [::]
```

Deploying a dual stack host firewall with pf

```
# host based firewall using pf in FreeBSD, file /etc/pf.conf - protect us1

block in all
pass out all

email_ports = "{ smtp, pop3, imap, pop3s, imaps }"
web_ports = "{ http, https }"
ldap_ports = "{ ldap, ldaps }"
ssh_ports = "{ ssh }"
dns_ports = "{ domain }"

pass in quick proto icmp6 all
pass in quick proto icmp all

pass in inet proto tcp to any port $email_ports
pass in inet proto tcp to any port $web_ports
pass in inet proto tcp to any port $ldap_ports
pass in inet proto tcp to any port $ssh_ports
pass in inet proto { tcp, udp } to any port $dns_ports

pass in inet6 proto tcp to any port $email_ports
pass in inet6 proto tcp to any port $web_ports
pass in inet6 proto tcp to any port $ldap_ports
pass in inet6 proto tcp to any port $ssh_ports
pass in inet6 proto { tcp, udp } to any port $dns_ports
```

DNS records for v6home (BIND 9.x) – part 1

```
; Origin added to names not ending in a dot:
; v6home.org
;

@ IN SOA atlcolodns1.infoweapons.com. it.infoweapons.com. (
                15            ; Serial
                3h            ; Refresh
                1h            ; Retry
                1w            ; Expire
                1h         )  ; Negative caching TTL

;
; NS
;
@       3h IN NS  ns1.v6home.org.
@       3h IN NS  ns1.v6home.org.
@       3h IN NS  ns2.v6home.org.
@       3h IN NS  ns2.v6home.org.
@       IN NS  atlcolodns1.infoweapons.com.

;
; NS glue records
;
ns1.v6home.org.  3h IN A  204.2.248.2
ns1.v6home.org.  3h IN AAAA  2001:0418:5403:0000:0000:0000:0000:0002
ns2.v6home.org.  3h IN AAAA  2001:0418:5403:0000:0000:0000:0000:0003
ns2.v6home.org.  3h IN A  204.2.248.3
```

DNS records for v6home (BIND 9.x) – part 2

```
; MX Records
;
@       3h IN MX  1 us1.v6home.org.

;
; Addresses for the canonical names
;
mailroute            3h IN A    204.2.248.50
mailroute            3h IN AAAA 2001:0418:5403:3000:0000:0000:0000:000d
ns1                  3h IN A    204.2.248.2
ns1                  3h IN AAAA 2001:0418:5403:0000:0000:0000:0000:0002
ns2                  3h IN A    204.2.248.3
ns2                  3h IN AAAA 2001:0418:5403:0000:0000:0000:0000:0003
us1                  3h IN AAAA 2001:0418:5403:3000:0000:0000:0000:000d
@                    3h IN AAAA 2001:0418:5403:3000:0000:0000:0000:000d
us1                  3h IN A    122.52.125.245
@                    3h IN A    122.52.125.245
```

DNS Details for E-mail Servers

- You need to register your nameservers to the DNS Top Level Domain servers (e.g. those that are authoritative for .org, .com, .net). Your domain registrar must support this for IPv6. Some do today, some don't. One that does is *godaddy.com*, where v6home.org was obtained. They support "registration" of your nameservers on both IPv4 and IPv6. See their "domain manager" to accomplish this.
- You will need to publish the IPv4 and IPv6 addresses of your mail server, as well as an MX record that points to it (contains the server's FQDN). Your DNS server should accept lookup queries over both IPv4 and IPv6.
- Many e-mail servers will do a reverse DNS lookup (even for IPv6), so you will need to have your ISP (or someone) publish both IPv4 and IPv6 PTR records for your mail server. You can also have the ISP delegate your block of addresses to you so you can publish reverse records yourself, which is what we did. Contact your ISP for details. See typical IPv6 reverse records in the following slide.
- DNS appliances (like SolidDNS) will greatly simplify creation and management of both IPv4 and IPv6 resource records and reverse zones.

Reverse DNS Records for 2001:418:5403:3000::/64

```
; Origin added to names not ending in a dot:
; 0.0.0.3.3.0.4.5.8.1.4.0.1.0.0.2.ip6.arpa
;

@ IN SOA atlcolodns1.infoweapons.com. it.infoweapons.com. (
                11            ; Serial
                3h            ; Refresh
                1h            ; Retry
                1w            ; Expire
                1h         )  ; Negative caching TTL

;
; NS
;
@       IN NS  atlcolodns1.infoweapons.com.

;
; DNSKEY
;

;
; Addresses point to canonical names
;

d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  mailroute.v6home.org.
d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  us1.v6home.org.
d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  v6home.org.
```

Protocol handshake with Exchange 2007

```
$ telnet ws1.hughesnet.org 25
Trying 2001:418:5403:3000::b...
Connected to hughesnet.local.
Escape character is '^]'.
220 ws1.hughesnet.org Microsoft ESMTP MAIL Service ready at Mon, 16 Nov 2009 15:03:36 +0800
EHLO x.com
250-ws1.hughesnet.org Hello [2001:418:5403:3000::d]
250-SIZE
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-AUTH NTLM
250-8BITMIME
250-BINARYMIME
250 CHUNKING
quit
221 2.0.0 Service closing transmission channel


$ telnet ws1.hughesnet.org 110
Trying 2001:418:5403:3000::b...
Connected to ws1-v6.hughesnet.local.
Escape character is '^]'.
+OK The Microsoft Exchange POP3 service is ready.
quit
+OK Microsoft Exchange Server 2007 POP3 server signing off.
```

Protocol handshake to Postfix and Dovecot

```
$ telnet us1.v6home.org 25
Trying 2001:418:5403:3000::d...
Connected to us1.hughesnet.org.
Escape character is '^]'.
220 us1.v6home.org ESMTP Postfix
EHLO x.com
250-us1.v6home.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
```

```
$ telnet us1.v6home.org 110
Trying 2001:418:5403:3000::d...
Connected to us1.hughesnet.org.
Escape character is '^]'.
+OK Dovecot ready.
quit
+OK Logging out
Connection closed by foreign host.
```

Mail Headers from Message that traversed IPv6

```
Received: from us1.v6home.org (2001:418:5403:3000::d) by ws1.hughesnet.org
 (2001:418:5403:3000::b) with Microsoft SMTP Server (TLS) id 8.1.393.1; Thu, 5
 Nov 2009 12:01:08 +0800
Received: from LEH (unknown [IPv6:2001:418:5403:2410:e409:f84d:c2d4:d91b])
     (using TLSv1 with cipher AES128-SHA (128/128 bits))    (No client certificate
 requested)     by us1.v6home.org (Postfix) with ESMTPSA id 2DCC03BA84E     for
 <lhughes@hughesnet.org>; Thu,  5 Nov 2009 12:00:03 +0800 (PHT)
From: "Lawrence E. Hughes" <lhughes@v6home.org>
To: "Lawrence E. Hughes" <lhughes@hughesnet.org>
Date: Tue, 3 Nov 2009 09:47:17 +0800
Subject: v6home to hughesnet
```

v6home – an online community for IPv6 aficionados

- The deployment of Postfix/Dovecot and Squirrelmail was done as part of **v6home**, which is a new online community for anyone deploying IPv6 networks or network applications.
- v6home includes a free IPv6 email account and use of phpbb (a discussion forum web application), Wordpress (a blog platform) and MediaWiki (a groupware web application). When you register in phpbb that automatically registers you with the other applications and creates an e-mail account for you on Postfix / Dovecot / Squirrelmail (all with the same credentials). All accounts are kept in MySQL. It is running on FreeBSD 7.2 amd64, and uses pf as a host based firewall.
- To join v6home, surf to *https://us1.v6home.org* and click on the *phpbb* icon.
- We used the new InfoWeapons SolidWall dual stack firewall with 6in4 tunneling to protect the network and tunnel in IPv6 from our colo (where we have direct IPv6 service from NTT America). We publish all v6home DNS records with a pair of InfoWeapons' SolidDNS servers (in our colo), and even sign them using DNSSEC. Contact me if you would like an "organizational" account on these servers to publish your resource records. We can also provide commercial grade hosted dual stack email with web management and dual stack web hosting.

Thank You for Listening
Any questions?