

PSU Mac 2011 Talk Notes

- General Notes
 - Command-line Tools
 - Testing services
- Out of the box support
- Firewall
- DNS
 - Restrict access to recursive DNS
 - IPv6 DNS records
- Web
- Mail
 - Dovecot
 - Postfix

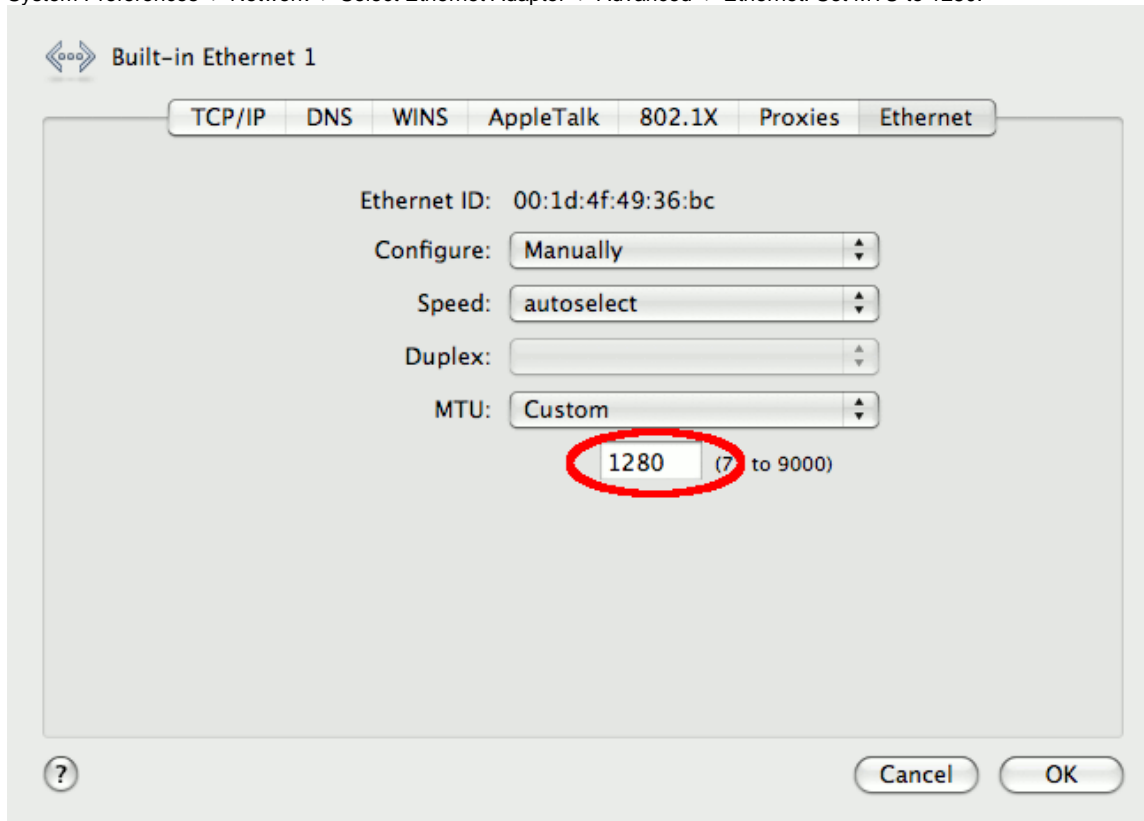
General Notes

The [IPv6 Rosetta Stone](#) page can be helpful. It lists common IPv6-related network commands for multiple operating systems.

On OS X Server, Server Admin does not support IPv6. All IPv6-related setup must be done from the command line.

It is very important that you [change your interface MTU to 1280](#). You can do this from System Preferences:

System Preferences -> Network -> Select Ethernet Adaptor -> Advanced -> Ethernet. Set MTU to 1280.



Or you can set it from the command line:

```
sudo networksetup -setMTU 'Ethernet' 1280
```

Command-line Tools

Not all commands support IPv6. The `ifconfig` and `networksetup` support IPv6. The `changeip` and `ipconfig` commands do not.

In this example, you can see that `ifconfig` and `networksetup` display the IPv6 addresses on the machine:

```
$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1280
    ether 00:16:cb:ae:aa:b8
    inet6 fe80::216:cbff:feae:aab8%en0 prefixlen 64 scopeid 0x5
    inet6 2610:8:6c00:a::217 prefixlen 64
    inet 146.186.110.217 netmask 0xffffffc0 broadcast 146.186.110.255
    media: autoselect (1000baseT <full-duplex,flow-control>)
    status: active

$ networksetup -getinfo 'Built-in Ethernet 1'
Manual Configuration
IP address: 146.186.110.217
Subnet mask: 255.255.255.192
Router: 146.186.110.193
IPv6: Manual
IPv6 IP address: 2610:0008:6c00:000a:0000:0000:0000:0217
IPv6 Router: 2610:0008:6c00:000a:0000:0000:0000:0001
IPv6 Prefix Length: 64
Ethernet Address: 00:16:cb:ae:aa:b8$
```

Here you can see that `ipconfig` and `changeip` do not support IPv6:

```
$ ipconfig getifaddr en0
146.186.110.217

$ sudo changeip -checkhostname

Primary address      = 146.186.110.217

Current HostName     = petite.et.its.psu.edu
DNS HostName         = petite.et.its.psu.edu

The names match. There is nothing to change.
dirserv:success = "success"
```

Testing services

The `telnet` command can be used to check if a service is answering on IPv4 or IPv6. Here, I telnet to a mail server (on SMTP port 25). Use the `-4` flag to connect over IPv4. The `-6` flag connects over IPv6.

```

$ telnet -4 smtp.et-test.psu.edu 25
Trying 128.118.27.7...
Connected to www.et-test.psu.edu.
Escape character is '^]'.
220 www.et-test.psu.edu ESMTP Sendmail 8.13.8/8.13.8; Fri, 13 May 2011 09:01:30 -0400
EHLO foobar
250-www.et-test.psu.edu Hello [146.186.110.217], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI
250-STARTTLS
250-DELIVERBY
250 HELP
QUIT
221 2.0.0 www.et-test.psu.edu closing connection
Connection closed by foreign host.

$ telnet -6 smtp.et-test.psu.edu 25
Trying 2610:8:6800:1::7...
Connected to www.et-test.psu.edu.
Escape character is '^]'.
220 www.et-test.psu.edu ESMTP Sendmail 8.13.8/8.13.8; Fri, 13 May 2011 09:01:39 -0400
EHLO foobar
250-www.et-test.psu.edu Hello [IPv6:2610:8:6c00:a::217], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH GSSAPI
250-STARTTLS
250-DELIVERBY
250 HELP
QUIT
221 2.0.0 www.et-test.psu.edu closing connection
Connection closed by foreign host.

```

Out of the box support

After configuring an IPv6 address (and changing the MTU!), basic OS X Server services will support IPv6. Here, Open Directory, AFP, SSH, Remote Desktop, and Web all support IPv6.

```

$ netstat -af inet6 | grep LISTEN
tcp46      0      0 *.http          *.*          LISTEN
tcp6       0      0 *.afpovert     *.*          LISTEN
tcp46      0      0 *.vnc-server   *.*          LISTEN
tcp6       0      0 *.kerberos     *.*          LISTEN
tcp6       0      0 *.ldap         *.*          LISTEN
tcp6       0      0 *.ssh          *.*          LISTEN
tcp6       0      0 localhost.ipp  *.*          LISTEN

```

The `netstat` command lists which services are listening on IPv6.

Unfortunately, the OS X Server firewall will block access to these services over IPv6. In the next section, we discuss how to fix the firewall.

Firewall

The IPv6 firewall on OS X Server is seriously broken. The Server Admin utility does not support IPv6 firewall rules, and it will overwrite any IPv6 rules you manually create (with the now-working `ip6fw`). To prevent Server Admin from overwriting IPv6 rules, edit `/etc/ipfilter/ip_address_groups.plist`, and change these settings:

```
/etc/ipfilter/ip_address_groups.plist  
  
<key>IPv6Mode</key>  
<string>NoRules</string>  
<key>IPv6Control</key>  
<false/>
```

If you use an external firewall appliance, this is all you have to do (aside from setting the firewall rules!). If you use the OS X Server firewall, you must make more fixes. IPv6 firewall rules are managed by the `ip6fw` utility. Unfortunately, this command is broken in Snow Leopard – it isn't 64-bit clean and does not function properly. You need to remove the 64-bit build and force the system to use the 32-bit build:

```
sudo ditto /sbin/ip6fw /sbin/ip6fw.orig  
sudo ditto --arch i386 /sbin/ip6fw /sbin/ip6fw.i386  
sudo mv /sbin/ip6fw.i386 /sbin/ip6fw
```

Finally, OS X Server does not provide a way to load custom `ip6fw` rules at boot. You can install a [third-party package](#) to get this functionality:

```
cd /tmp  
curl -LO http://blog.atariwiki.strotmann.de/roller/cas/resource/ip6fw-load.pkg  
sudo installer -pkg ip6fw-load.pkg -target /
```

Edit `/etc/ip6fw.conf` to set custom rules. Do not modify rules below 20100, as this could break ICMPv6 functionality.

DNS

To configure BIND to answer on IPv6, edit `/etc/named.conf`. Make the `controls` section look like this:

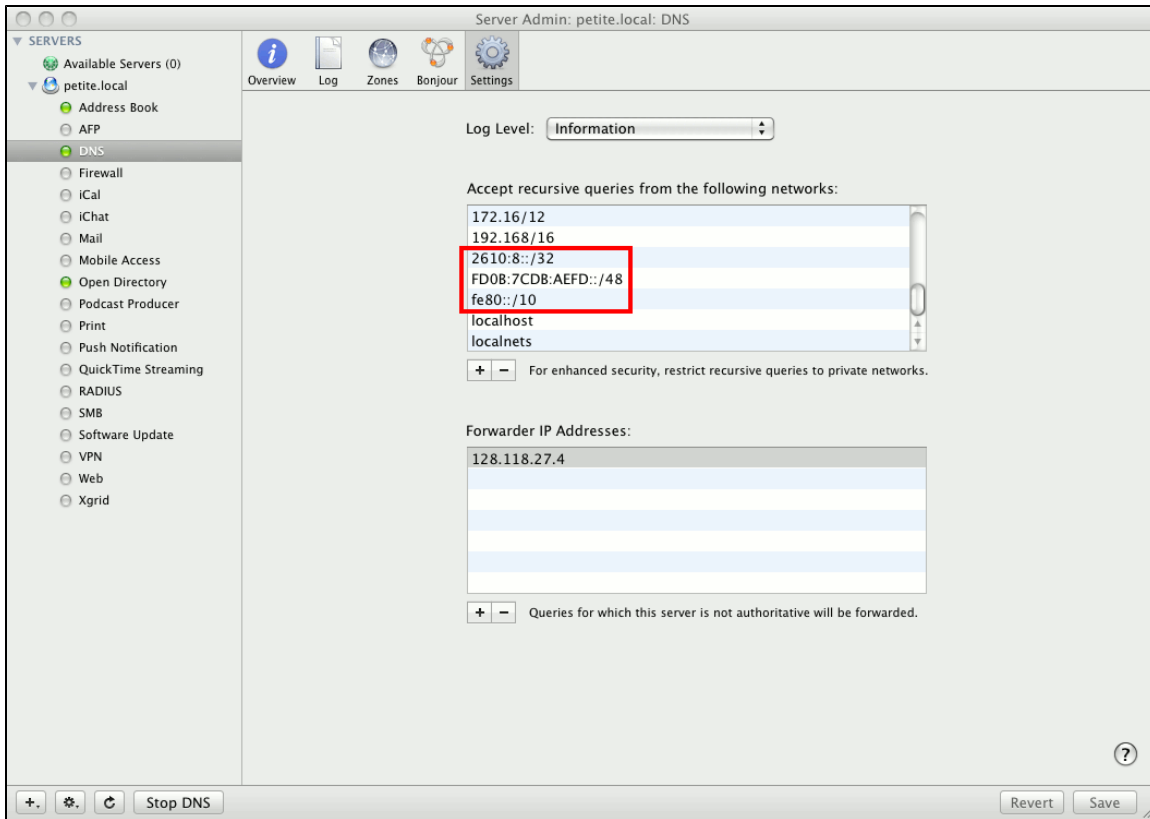
```
/etc/named.conf  
  
controls {  
    inet 127.0.0.1 port 54 allow { any; } keys { "rndc-key"; };  
    inet ::1 port 54 allow { any; } keys { "rndc-key"; };  
};
```

In the `options` section, add:

```
/etc/named.conf  
  
listen-on-v6 {any; };
```

Restrict access to recursive DNS

Penn State DNS admins are required to restrict access to recursive DNS to Penn State IP addresses. Update your ACL to include IPv6. Unlike everything else, you can do this from the Server Admin GUI:



Then restart the DNS service.

IPv6 DNS records

OS X Server's Server Admin tool does not support IPv6, and Server Admin overwrites all zone files. So it's not possible to add forward and reverse entries for IPv6 on OS X Server. You'll have to use another DNS services. Alternatively, you could forgo using Server Admin's GUI to modify zone files.

Web

To dual-stack a WebAccess-protected web site, edit the relevant configuration file, and insert this line:

```
CosignCheckIP never
```

Mail

Dovecot

edit `/etc/dovecot/dovecot.conf`, append:

```
/etc/dovecot/dovecot.conf  
listen = *,[::]
```

Postfix

edit `/etc/postfix/main.cf`, append:

/etc/postfix/main.cf

```
inet_protocols = all
```

Be sure to contact TNS to request they open a hole for TCP port 25 for your IPv6 address.