



Troubleshooting

Edward Lewis

edlewis@arin.net





Why Troubleshoot?

- What Can Go Wrong?
 - ◆ Misconfigured zone
 - ◆ Misconfigured server
 - ◆ Misconfigured host
 - ◆ Misconfigured network





Tools

- BIND Logging Facility
- named's built-in options
- ping and traceroute
- tcpdump and ethereal
- dig and nslookup





The Best Way To Handle Mistakes

- Assume You Will Make Them
- Prepare The Name Server via Logging





BIND Logging

- Telling named which messages to send
 - ◆ category specification
- Telling named where to send messages
 - ◆ channel specification





BIND Categories

- BIND has many categories
- Short descriptions of each can be found in the Administrator's Reference Manual (ARM)
 - ◆ Section 6.2.10.2, page 49
 - ◆ Example:

```
category dnssec {  
    dnssec_log;  
};
```





BIND channels

- BIND can use syslog
- BIND can direct output to other files

- ◆ Example:

```
channel dnssec_log {  
    file "seclog" versions 3 size 10m;  
    print-time yes;  
    print-category yes;  
    print-severity yes;  
    severity debug 3;  
};
```





So You've Set Up A Server

- What testing should be done?
- From Basic liveness
 - ◆ Is the (right) server running?
 - ◆ Is the machine set up correctly?
- To data being served
 - ◆ Has the zone loaded?
 - ◆ Have zone transfers happened?





Checking the Configuration

- To see named start, use the -g flag
 - ◆ Keeps named process in the foreground
 - ◆ Prints some diagnostics
 - ◆ But does not execute logging
- When satisfied with named's start, kill the process and start without the flag
- Other option
 - ◆ named-checkconf
 - ◆ checks syntax only





Is the Server Running?

- Once the name server is thought to be running, make sure it is
 - ◆ `dig @127.0.0.1 version.bind chaos txt`
- This makes the name server do the simplest lookup it can - its version string
- This also confirms which version you started
 - ◆ Common upgrade error: running the old version, forgetting to 'make install'





Is the Server Data Correct?

- Now that the server is the right one (executable)
 - ◆ `dig @127.0.0.1 <zone> soa`
- Check the serial number to make sure the zone has loaded
- Also test changed data in case you forgot to update the serial number
- When we get to secondary servers, this check is made to see if the zone transferred





Is the Server Reachable?

- If the dig tests fail, its time to test the environment (machine, network)
 - ◆ `ping <server machine ip address>`
- This tests basic network flow, common errors
 - ◆ Network interface not UP
 - ◆ Routing to machine not correct
- Pinging 'locally' is useful, believe it or not
 - ◆ Confirms that the IP address is correctly configured





Is the Server Listening?

- If the server does not respond, but machine responds to ping
 - ◆ look at system log files
 - ◆ telnet server 53
- Server will run even if it can't open the network port
 - ◆ logs will show this
 - ◆ telnet opens a TCP connection, tests whether port was opened at all





Is the Server Logging the Right Stuff?

- Provoking and examining the logs
 - ◆ Log files only appear when needed
 - ◆ For example, dnssec logs will start only if 'trusted-keys' are configured and are used
 - ◆ Each category is triggered differently
 - ✦ Triggers may not be obvious





Using the Tools

- named itself
- dig/nslookup
- host diagnostics
- packet sniffers





Built in to named

- named -g to retain command line
 - ◆ named -g -c <conf file>
 - ◆ keeps named in foreground
- named -d <level>
 - ◆ sets the debug output volume
 - ◆ <level>'s aren't strictly defined
 - ◆ -d 3 is popular, -d 99 gives a lot of detail





dig

- domain internet groper
 - ◆ already used in examples
 - ◆ best tool for testing
 - ◆ shows query and response syntax
 - ◆ documentation
 - ◆ `man dig`
 - ◆ `dig -help`
- Included in named distribution





Non-BIND Tools

- Tools to make sure environment is right
 - ◆ Tools to look at server machine
 - ◆ Tools to test network
 - ◆ Tools to see what messages are on the network





ifconfig

- InterFace CONFIGuration
 - ◆ `ifconfig -a`
 - ◆ shows the status of interfaces
 - ◆ operating system utility
- Warning, during boot up, `ifconfig` may configure interfaces after `named` is started
 - ◆ `named` can't open delayed addresses
- Documentation
 - ◆ `man ifconfig`





ping

- Checks routing, machine health
 - ◆ Most useful if run from another host
 - ◆ Could be reason "no servers are reached"
 - ◆ Can be useful on local machine - to see if the interface is properly configured





traceroute

- If ping fails, traceroute can help pinpoint where trouble lies
 - ◆ the problem may be routing
 - ◆ if so - it's not named that needs fixing!
 - ◆ but is it important to know...





tcpdump and ethereal

- Once confident in the environment, problems with DNS set ups may exist
- To see what is happening in the protocol, use traffic sniffers
- These tools can help debug "forwarding" of queries
- ethereal can be retrieved from
 - ◆ <http://www.ethereal.com/>

