Complete DNS Learning Journey - Reference Documentation

A comprehensive guide covering BIND9 DNS infrastructure from basics to enterprise implementation

Table of Contents

DNS Fundamentals

Core DNS Concepts

- **Forward DNS**: Domain name to IP address resolution
- **Reverse DNS**: IP address to domain name resolution
- **Authoritative DNS**: Server that holds the actual zone data
- **Recursive DNS**: Server that queries other servers on behalf of clients

DNS Record Types

```
A # IPv4 address mapping
AAAA # IPv6 address mapping
CNAME # Canonical name (alias)
MX # Mail exchange
NS # Name server
PTR # Pointer record (reverse DNS)
SOA # Start of Authority
TXT # Text records
```

Zone Files Structure

- **SOA Record**: Defines zone parameters (serial, refresh, retry, expire)
- **NS Records**: Specify authoritative name servers
- **Glue Records**: Required when NS points to hosts within the same zone
- **Serial Numbers**: Track zone changes (format: YYYYMMDDNN)

BIND9 Installation & Basic Setup

Ubuntu Installation

```
sudo apt update
sudo apt install bind9 bind9utils bind9-doc
```

Service Management

```
sudo systemctl start bind9
sudo systemctl enable bind9
sudo systemctl status bind9
sudo systemctl reload bind9 # Reload config without restart
sudo systemctl restart bind9 # Full restart `
```

Configuration File Structure

```
text/etc/bind/ ├── named.conf # Main config (includes others) ├── named.conf.options # Server options and logging ├── named.conf.local # Local zone definitions ├── named.conf.default-zones # Default zones (root, localhost) ├── zones/ # Zone files directory └── keys/ # TSIG keys directory
```

Basic Options Configuration

```
options { directory "/var/cache/bind"; recursion no; # For authoritative servers listen-on { 127.0.0.1; 192.168.1.10; }; allow-query { any; }; allow-transfer { none; }; # Security default version "Not Disclosed"; # Hide version hostname "Not Disclosed"; # Hide hostname };
```

Zone Configuration

Forward Zone Example

```
zone "example.com" { type primary; file "/etc/bind/zones/db.example.com"; allow-transfer { 192.168.1.11; }; also-notify { 192.168.1.11; }; };
```

Zone File Format

```
$TTL 604800 @ IN SOA ns1.example.com. admin.example.com. ( 2024082401 ; Serial (YYYYMMDDNN) 604800 ; Refresh (1 week) 86400 ; Retry (1 day) 2419200 ; Expire (4 weeks) 604800 ) ; Negative Cache TTL (1 week)
```

; Name servers IN NS ns1.example.com. IN NS ns2.example.com.

; A records ns1 IN A 192.168.1.10 ns2 IN A 192.168.1.11 www IN A 192.168.1.100 mail IN A 192.168.1.50

; CNAME records smtp IN CNAME mail.example.com. ftp IN CNAME www.example.com.

; MX records IN MX 10 mail.example.com. `

Reverse Zone Configuration

zone "1.168.192.in-addr.arpa" { type primary; file "/etc/bind/zones/db.192.168.1"; };

Reverse Zone File

$TTL 604800 @ IN SOA ns1.example.com. admin.example.com. (2024082401 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800) ; Negative Cache TTL

```
IN  NS  ns1.example.com.
IN  NS  ns2.example.com.
```

10 IN PTR ns1.example.com. 11 IN PTR ns2.example.com. 100 IN PTR www.example.com. 50 IN PTR mail.example.com.

Split-Horizon DNS (Views)

ACL Definition

acl "internal-network" { 192.168.1.0/24; 172.16.0.0/12; 127.0.0.1; };

acl "external-network" { !192.168.1.0/24; # Not internal any; };

View Configuration

view "internal" { match-clients { internal-network; }; recursion yes; # Allow recursion for internal

```
zone "example.com" {
    type primary;
    file "/etc/bind/zones/db.example.com.internal";
};
```

};

view "external" { match-clients { any; }; recursion no; # No recursion for external

```
zone "example.com" {
    type primary;
    file "/etc/bind/zones/db.example.com.external";
};
```

};

Internal vs External Zone Content

Internal Zone (shows all hosts):

```
www IN A 192.168.1.100 mail IN A 192.168.1.50 db IN A 192.168.1.200 # Internal only admin IN A 192.168.1.150 # Internal only
```

External Zone (limited public hosts):

```
www IN A 203.0.113.100 # Public IP mail IN A 203.0.113.50 # Public IP
```

No internal hosts exposed

Security Implementation

TSIG Key Generation

Generate TSIG key

```
sudo tsig-keygen -a hmac-sha256 zone-xfer > /etc/bind/keys/zone-xfer.key
```

Key file content example

```
key "zone-xfer" { algorithm hmac-sha256; secret "base64secretstring=="; };
```

TSIG Key Usage

Include key in configuration

```
include "/etc/bind/keys/zone-xfer.key";
```

Use key for zone transfers

```
zone "example.com" { type primary; file "/etc/bind/zones/db.example.com"; allow-transfer { key "zone-xfer"; 192.168.1.11; }; allow-update { key "zone-xfer"; }; };
```

Security Options

```
options { // Hide server information version "Not Disclosed"; hostname "Not Disclosed"; server-id "Not Disclosed";
```

```
// Rate limiting (DDoS protection)
rate-limit {
    responses-per-second 10;
    referrals-per-second 5;
    nodata-per-second 5;
    nxdomains-per-second 5;
    errors-per-second 5;
    all-per-second 20;
    window 15;
    slip 2;
};

// Response minimization
minimal-any yes;
minimal-responses yes;
```

};

Zone Transfers & Replication

Primary Server Configuration

zone "example.com" { type primary; file "/etc/bind/zones/db.example.com"; allow-transfer { key "zone-xfer"; 192.168.1.11; }; also-notify { 192.168.1.11; }; # Notify secondary };

Secondary Server Configuration

zone "example.com" { type secondary; file "/var/cache/bind/db.example.com.slave"; masters { 192.168.1.10 key "zone-xfer"; }; allow-notify { 192.168.1.10; }; };

Zone Transfer Types

- **AXFR**: Full zone transfer (all records)
- **IXFR**: Incremental transfer (only changes)
- **NOTIFY**: Notification of zone changes

Manual Zone Transfer Testing

Test AXFR from authorized host

dig @192.168.1.10 example.com AXFR

Test from unauthorized host (should fail)

dig @192.168.1.10 example.com AXFR

Dynamic DNS (DDNS)

Server Configuration

zone "example.com" { type primary; file "/etc/bind/zones/db.example.com"; allow-update { key "zone-xfer"; }; allow-update-forwarding { none; }; };

DDNS Client Updates

Create update script

```
cat > /tmp/ddns-update.txt << EOF server 192.168.1.10 key zone-xfer hmac-sha256:base64secret== zone example.com update add newhost.example.com 300 A 192.168.1.250 send EOF
```

Execute update

```
nsupdate -v /tmp/ddns-update.txt
```

Alternative: Use key file

```
nsupdate -k /etc/bind/keys/zone-xfer.key /tmp/ddns-update.txt
```

DDNS Update Types

Add record

```
update add hostname.example.com 300 A 192.168.1.100
```

Delete specific record

```
update delete hostname.example.com A 192.168.1.100
```

Delete all records for name

```
update delete hostname.example.com
```

Replace record (delete then add)

```
update delete hostname.example.com A update add hostname.example.com 300 A 192.168.1.200
```

Journal Files

- Created automatically: db.example.com.jnl
- Track incremental changes
- Must be writable by bind user
- Used for IXFR replication

Logging & Monitoring

Comprehensive Logging Configuration

```
logging { // Log channels channel general_log { file "/var/log/named/general.log"
versions 3 size 5m; severity info; print-time yes; print-severity yes; print-category
yes; };
```

```
channel security_log {
    file "/var/log/named/security.log" versions 3 size 5m;
    severity info;
    print-time yes;
    print-severity yes;
    print-category yes;
};

channel transfer_log {
    file "/var/log/named/transfer.log" versions 3 size 5m;
    severity info;
    print-time yes;
    print-severity yes;
    print-category yes;
};

channel update_log {
    file "/var/log/named/update.log" versions 3 size 5m;
    severity info;
    print-time yes;
    print-severity yes;
    print-category yes;
};

// Category assignments
category default        { general_log; };
category general        { general_log; };
category security       { security_log; };
category update         { update_log; };
category update-security { security_log; };
category xfer-in        { transfer_log; };
category xfer-out       { transfer_log; };
category notify         { transfer_log; };
```

```
};
```

Log Analysis Commands

Monitor logs in real time

```
sudo tail -f /var/log/named/general.log
```

Search for security events

```
grep -i "denied|refused|unauthorized" /var/log/named/*.log
```

DDNS update analysis

```
grep "update.approved|update.denied" /var/log/named/general.log
```

Zone transfer statistics

```
grep "AXFR|IXFR" /var/log/named/transfer.log
```

Error analysis

```
grep "ERROR|WARN" /var/log/named/general.log
```

File Permissions & Security

Secure File Ownership

Configuration files (read-only)

```
sudo chown -R root:bind /etc/bind/ sudo chmod 755 /etc/bind/ sudo chmod 644
/etc/bind/named.conf*
```

TSIG keys (restricted access)

```
sudo chown root:bind /etc/bind/keys/ sudo chmod 750 /etc/bind/keys/ sudo chmod 600
/etc/bind/keys/*.key
```

Zone files (DDNS zones need bind ownership)

```
sudo chown -R bind:bind /etc/bind/zones/ sudo chmod 755 /etc/bind/zones/ sudo chmod
644 /etc/bind/zones/db.*
```

Cache and working directories

```
sudo chown -R bind:bind /var/cache/bind/ sudo chmod 755 /var/cache/bind/
```

Log directories

```
sudo chown -R bind:bind /var/log/named/ sudo chmod 755 /var/log/named/
```

Permission Verification Script

```
#!/bin/bash echo "=== BIND9 Permission Audit ==="
```

```
echo "Config directory:" ls -ld /etc/bind/
```

```
echo "Zone files:" ls -l /etc/bind/zones/
```

```
echo "Key files:" ls -l /etc/bind/keys/
```

```
echo "Journal files:" ls -l /etc/bind/zones/*.jnl 2>/dev/null || echo "No journal files"
```

```
echo "Cache directory:" ls -ld /var/cache/bind/
```

Troubleshooting Guide

Configuration Validation

Check main configuration syntax

```
sudo named-checkconf
```

Check specific zone file

```
sudo named-checkzone example.com /etc/bind/zones/db.example.com
```

Check all zones

```
sudo named-checkconf -z
```

Common Error Resolution

Zone Transfer Failures

Symptoms: Secondary not updating

Check: TSIG key mismatch, firewall, notify settings

Fix: Verify key consistency, check port 53 TCP/UDP

Manual transfer test

```
dig @primary-ip zone-name AXFR
```

DDNS Update Failures

Symptoms: "update failed: SERVFAIL"

Common causes:

1. Permission issues (journal file creation)

2. TSIG key mismatch

3. Zone not configured for updates

Fix permissions

```
sudo chown bind:bind /etc/bind/zones/db.zone-name sudo rm -f /etc/bind/zones/*.jnl
sudo systemctl reload bind9
```

View/ACL Issues

Symptoms: Wrong records returned

Debug: Check client IP against ACL

Fix: Review ACL definitions and view order

Test from specific IP

```
dig @dns-server +short hostname
```

Diagnostic Commands

Show current configuration

```
sudo rndc status sudo rndc dumpdb -cache sudo rndc stats
```

Flush cache

sudo rndc flush

Reload zones

sudo rndc reload sudo rndc reload zone-name

Check listening ports

sudo netstat -tulpn | grep :53 sudo ss -tulpn | grep :53

Best Practices & Optimization

Security Hardening

1. **Disable unnecessary features**
    - Turn off recursion on authoritative servers
    - Hide version information
    - Implement rate limiting
2. **Access Control**
    - Use TSIG keys for all transfers
    - Implement ACLs for query restrictions
    - Regular key rotation
3. **Monitoring**
    - Enable comprehensive logging
    - Monitor for failed authentication attempts
    - Set up log rotation

Performance Optimization

options { // Memory management max-cache-size 128M; max-ncache-size 32M;

```
// TTL limits
max-cache-ttl 86400;    # 1 day max
max-ncache-ttl 10800;   # 3 hours negative cache

// Performance tuning
minimal-any yes;
minimal-responses yes;

// Statistics
memstatistics-file "/var/log/named/memstats.log";
statistics-file "/var/log/named/stats.log";
```

```
};
```

Operational Procedures

1. **Configuration Changes**
   - Always backup before changes
   - Use named-checkconf before reload
   - Test in staging environment
2. **Zone Updates**
   - Increment serial numbers consistently
   - Use YYYYMMDDNN format
   - Document all changes
3. **Key Management**
   - Store keys securely
   - Implement key rotation schedule
   - Separate keys for different functions

Testing & Validation

Functionality Tests

Basic resolution

```
dig @dns-server hostname.domain.com dig @dns-server domain.com MX dig @dns-server domain.com NS
```

Reverse DNS

```
dig @dns-server -x 192.168.1.100
```

Zone transfers

```
dig @dns-server domain.com AXFR
```

Dynamic updates

```
nsupdate -k keyfile update-script
```

Security Validation

Test ACL restrictions

```
dig @dns-server hostname.domain.com # From different networks
```

TSIG authentication

```
dig @dns-server domain.com AXFR # Without key (should fail)
```

Rate limiting

Multiple rapid queries from same IP

Version hiding

```
dig @dns-server version.bind chaos TXT
```

Load Testing

Use dig with multiple queries

```
for i in {1..100}; do dig @dns-server test$i.domain.com & done
```

Monitor performance

```
sudo rndc stats cat /var/log/named/stats.log
```

Enterprise Implementation Checklist

Pre-Production

- Security review completed
- Performance testing done
- Backup/recovery procedures tested
- Monitoring setup verified
- Documentation completed

Production Deployment

- Primary server configured and tested

- Secondary server configured and tested
- Zone transfers working
- DDNS functionality verified
- Logging operational
- Security controls validated

Post-Deployment

- Monitor logs for issues
- Performance baseline established
- Team training completed
- Maintenance procedures documented
- Emergency procedures tested

Useful Commands Reference

Service Management

```
sudo systemctl start|stop|restart|reload bind9 sudo systemctl status bind9 sudo rndc reload [zone] sudo rndc stats sudo rndc flush
```

Testing Commands

```
dig @server hostname [type] nslookup hostname server host hostname server named-checkconf [-z] named-checkzone zone-name zone-file nsupdate [-k keyfile] [-v] [script]
```

Log Commands

```
tail -f /var/log/named/general.log grep "pattern" /var/log/named/*.log journalctl -u bind9 -f
```

This documentation serves as a comprehensive reference for implementing DNS infrastructure using BIND9. Keep it updated as your knowledge and implementations evolve.

Created: Deba Dey **Last Updated:** August 2025**Version:** 1.0