DNS Tools Cheatsheet

A quick reference guide to common DNS tools for network administration and troubleshooting. This cheat sheet provides commands and examples for querying DNS records, diagnosing DNS issues, and managing DNS zones.

Basic DNS Query Tools

dig (Domain Information Groper)

`dig` is a powerful command-line tool for querying DNS name servers. It can retrieve various DNS records and is available on most Unix-like operating systems.

Basic Syntax:

```
dig [options] name [query type] [query class]
```

Common Options:

- `+trace`: Trace the delegation path from the root nameservers.
- `+short`: Display only the IP address.
- `@server`: Specify the DNS server to query.
- `-x ip_address`: Perform a reverse DNS lookup.

Examples:

- Get the A record for example.com:
  `dig example.com A`
- Get the MX record for example.com:
  `dig example.com MX`
- Trace the DNS resolution for example.com:
  `dig +trace example.com`
- Query a specific DNS server:
  `dig @8.8.8.8 example.com`
- Reverse lookup for an IP address:
  `dig -x 8.8.8.8`

nslookup (Name Server Lookup)

`nslookup` is another command-line tool for querying DNS name servers. It's simpler than `dig` but still useful for basic DNS lookups.

Basic Syntax:

```
nslookup [options] name [server]
```

Common Usage:

- Enter interactive mode by typing `nslookup` without arguments.
- Set the query type: `set type=record_type` (e.g., `set type=MX`).
- Query a name: `name` (e.g., `example.com`).
- Specify a server: `server server_address` (e.g., `server 8.8.8.8`).

Examples:

- Get the A record for example.com:
  `nslookup example.com`
- Get the MX record for example.com:
  `nslookup -type=MX example.com`
- Query a specific DNS server:
  `nslookup example.com 8.8.8.8`

Advanced DNS Analysis Tools

host

`host` is a simple utility for performing DNS lookups. It is often used to quickly retrieve the IP address associated with a domain name or to perform reverse lookups.

Basic Syntax:

```
host [options] name [server]
```

Common Options:

- `-t type`: Specify the record type to query (e.g., `A`, `MX`, `NS`).
- `-a`: Perform a query for all record types.
- `-l zone_name`: Perform a zone transfer for the specified zone.
- `-v`: Enable verbose output.

Examples:

- Get the A record for example.com:
  `host example.com`
- Get the MX record for example.com:
  `host -t MX example.com`
- Perform a reverse lookup:
  `host 8.8.8.8`
- Query a specific DNS server:
  `host example.com 8.8.8.8`

dnsperf & zonefetch

`dnsperf` is a DNS performance testing tool that measures the performance of DNS servers by simulating client queries. `zonefetch` is used to fetch DNS zone data for testing purposes.

Basic Usage:

- `dnsperf -s server_ip -d query_file`
- `zonefetch example.com`

Key dnsperf Options:

- `-s server_ip`: Specify the IP address of the DNS server to test.
- `-d query_file`: Specify the file containing DNS queries.
- `-l duration`: Specify the duration of the test in seconds.
- `-c clients`: Specify the number of concurrent clients.
- `-q queries`: Specify the maximum number of queries to send.

Example:

- Test the performance of a DNS server using a query file:
  `dnsperf -s 8.8.8.8 -d queries.txt -l 10 -c 20`
- Fetch DNS zone data for example.com:
  `zonefetch example.com > example.com.zone`

PowerShell DNS Tools (Windows)

Resolve-DnsName

`Resolve-DnsName` is a PowerShell cmdlet used to perform DNS queries. It provides similar functionality to `dig` and `nslookup` on Unix-like systems.

Basic Syntax:

```
Resolve-DnsName [-Name] <String> [[-Type] <String>] [-Server <String>]
```

Common Parameters:

- `-Name`: Specifies the DNS name to resolve.
- `-Type`: Specifies the DNS record type to query (e.g., `A`, `MX`, `NS`).
- `-Server`: Specifies the DNS server to query.
- `-DnsOnly`: Use only DNS to resolve the name.

Examples:

- Get the A record for example.com:
  `Resolve-DnsName -Name example.com -Type A`
- Get the MX record for example.com:
  `Resolve-DnsName -Name example.com -Type MX`
- Query a specific DNS server:
  `Resolve-DnsName -Name example.com -Server 8.8.8.8`

Get-DnsClientCache

`Get-DnsClientCache` is a PowerShell cmdlet that retrieves the contents of the DNS client cache on a Windows system.

Basic Syntax:

```
Get-DnsClientCache
```

Common Usage:

- View all entries in the DNS client cache:
  `Get-DnsClientCache`
- Filter the cache entries by name:
  `Get-DnsClientCache | Where-Object {$_.Name -like "*example.com*"}`
- Clear the DNS client cache (requires administrative privileges):
  `Clear-DnsClientCache`

Example:

- Retrieve and display the DNS client cache:
  `Get-DnsClientCache | Format-Table -AutoSize`

Common DNS Record Types

Record Types

A (Address) Record:

Maps a domain name to an IPv4 address.

Example:

```
example.com.   3600  IN  A   192.0.2.1
```

AAAA (Quad-A) Record:

Maps a domain name to an IPv6 address.

Example:

```
example.com.   3600  IN  AAAA   2001:db8::1
```

CNAME (Canonical Name) Record:

Creates an alias for a domain name. Points one domain name to another.

Example:

```
www.example.com.   3600  IN  CNAME   example.com.
```

MX (Mail Exchange) Record:

Specifies the mail server responsible for accepting email messages on behalf of a domain.

Example:

```
example.com.   3600  IN  MX  10 mail.example.com.
```

NS (Name Server) Record:

Delegates a DNS zone to a specific name server.

Example:

```
example.com.   86400  IN  NS   ns1.example.com.
```

TXT (Text) Record:

Contains arbitrary text data, often used for verification or SPF records.

Example:

```
example.com.   3600  IN  TXT   "v=spf1 mx -all"
```

SOA (Start of Authority) Record:

Specifies administrative information about a DNS zone, including the primary name server, the responsible party's email, and refresh intervals.

Example:

```
example.com.   3600  IN  SOA   ns1.example.com. admin.example.com. (2023102601 3600 1800 604800 3600)
```