nslookup — Professional Cheat Sheet

> **Compact professional reference** for `nslookup` — interactive and non-interactive DNS lookup utility available on Windows, macOS and many Linux distributions. Quick flags, record types, examples, and troubleshooting tips for DNS reconnaissance and debugging.

---

1) At-a-glance

- **Tool:** `nslookup` — query DNS servers for resource records (A, AAAA, MX, NS, SOA, TXT, PTR, SRV, CNAME, etc.).
- **Use cases:** Simple DNS record checks, reverse lookups, testing a specific DNS server, basic zone transfer attempts (AXFR), and quick debugging when `dig` is unavailable.
- **Note:** Behavior and flags differ slightly between Windows and Unix implementations; interactive mode is similar across platforms.

---

2) Modes of use

- **Non-interactive (one-shot):** `nslookup <name> [server]` e.g. `nslookup example.com 8.8.8.8`.
- **Interactive:** start with `nslookup` (or `nslookup -`) then issue commands like `server`, `set type=MX`, `ls -d example.com`.

---

3) Common command syntax (non-interactive)

```
nslookup hostname [server]
# Examples
nslookup example.com                # query default resolver
nslookup example.com 8.8.8.8        # query Google public DNS
nslookup -type=MX example.com 1.1.1.1
```

Windows: `nslookup -type=MX example.com 8.8.8.8` (order of flags may vary).

---

4) Interactive mode quick reference

Start:

```
nslookup
> server 8.8.8.8       # change server
> set type=AAAA        # change query type
> example.com          # query
> set debug            # verbose response + additional info
> exit
```

Useful interactive commands: - `server <address>` or `ls` to list records (ls requires server permission and may be limited). - `set type=<RR>` (A, AAAA, MX, NS, SOA, TXT, PTR, SRV, CNAME) - `set class=<class>` (IN, CH, HS) — default is IN (Internet) - `set port=<port>` — change destination port (for non-standard DNS ports) - `set vc` — use TCP (sometimes `-vc` on non-interactive variants) - `set debug` / `set d2` — more verbose output - `set recurse` / `set norecurse` — control recursion flag

---

5) Common query examples

A and AAAA records

```
nslookup -type=A example.com
nslookup -type=AAAA example.com
```

MX (mail exchangers)

```
nslookup -type=MX example.com
```

NS (name servers)

```
nslookup -type=NS example.com
```

TXT (SPF / DKIM / verification)

```
nslookup -type=TXT example.com
```

PTR (reverse DNS)

```
nslookup -type=PTR 1.2.3.4.in-addr.arpa
# or simpler (non-interactive):
nslookup 1.2.3.4
```

SRV (services like _ldap._tcp)

```
nslookup -type=SRV _ldap._tcp.example.com
```

SOA (start of authority)

```
nslookup -type=SOA example.com
```

Zone transfer attempt (AXFR)

```
# Interactive: set type=AXFR then 'ls -d example.com' (many servers deny AXFR)
nslookup
> server ns1.example.com
> set type=AXFR
> example.com
```

---

6) Troubleshooting & useful tips

- **Use a specific DNS server** to rule out resolver cache: `nslookup host 1.1.1.1`.
- **Compare authoritative vs recursive:** query the authoritative NS directly (use `server <ns-ip>`), and compare with your recursive resolver.
- **Check TTL and caching:** look at `TTL` values returned; cached answers may persist until TTL expiry.
- **Use TCP** if UDP responses are truncated or blocked: `set vc` or `nslookup -vc`.
- **Verbosity:** `set debug` or `set d2` shows full response including authority and additional sections.
- **Reverse lookup caveat:** a successful PTR record doesn't guarantee hostname authenticity; PTR is controlled by the IP owner.
- **Zone transfers:** AXFR is often blocked; if allowed and used without permission, it may be illegal—use only on targets you own or are authorized to test.

---

7) Differences vs `dig` (quick note)

- `dig` provides richer, script-friendly output and fine control for DNS diagnostics; prefer `dig` for complex tasks. Use `nslookup` for quick checks and on systems where `dig` is missing.

---

8) One-liners & cheat commands

```
# Query A record using Google DNS
nslookup example.com 8.8.8.8

# Query MX records (Cloudflare DNS)
nslookup -type=MX example.com 1.1.1.1

# Reverse lookup
nslookup 93.184.216.34

# Query authoritative name server directly
nslookup example.com ns1.example.net

# Use TCP (when UDP truncated)
nslookup -vc example.com 8.8.8.8   # depending on build
```

---

9) Quick checklist when DNS seems broken

1. Try a known public resolver (8.8.8.8 / 1.1.1.1) to rule out local DNS cache.
2. Query authoritative NS to see authoritative data.
3. Use `set debug` to inspect additional/authority sections.
4. Check TTLs and propagation if records recently changed.
5. Ensure firewall allows DNS (UDP/TCP 53) between you and the server.

This cheat sheet is for network diagnostics, security testing and DNS troubleshooting. Always get authorization before performing intrusive DNS operations like zone transfers.