The DNS Records Cheat Sheet

WebsiteSetup.org · a printable reference for your zone file

DNS is the phone book of the internet. The full set of records for one domain is a zone. Each record has a type, a name or host ("@" means the root of your domain), and a value, plus a TTL: the seconds other servers may cache it before checking again.

Record types at a glance

Type	What it does	Example value	When you use it
A	Name to IPv4 address	`203.0.113.25`	Point a domain at a server
AAAA	Name to IPv6 address	`2001:db8::1`	Same as A, for IPv6
CNAME	Alias one name to another	`yourdomain.com.`	Point www or a subdomain
MX	Mail servers for the domain	`1 smtp.google.com.`	Receive email
TXT	Free text machines read	`v=spf1 ... ~all`	Verification, SPF, DKIM, DMARC
NS	Authoritative servers for zone	`ns1.example-dns.com.`	Delegate DNS to a provider
SOA	Start and settings of the zone	`ns1... admin... serial`	Created for you automatically
PTR	IP back to a name (reverse)	`mail.yourdomain.com.`	Reverse DNS, set by IP owner
SRV	Service to a host and port	`10 5 5060 sip.example.com.`	VoIP, chat, similar services
CAA	Which CAs may issue certs	`0 issue "letsencrypt.org"`	Lock down cert issuance
ALIAS/ANAME	CNAME-like at the apex	`target.host.com.`	Point a bare domain at a host

Record types in one line each

A maps a name to an IPv4 address. `A @ 203.0.113.25`

AAAA maps a name to an IPv6 address.

CNAME aliases one name to another; points to a name, never an IP.

MX names mail servers by priority; must target a real hostname.

TXT stores plain text: verification, SPF, DKIM, DMARC.

SPF (a TXT) lists who may send mail as you. `~all` soft-fails the rest.

DKIM (a TXT) holds a public key to verify mail signatures.

DMARC (a TXT at `_dmarc`) sets policy and asks for reports.

NS names the authoritative servers for the zone.

SOA marks the start of authority; managed for you.

PTR is reverse DNS, set by whoever owns the IP.

SRV points a service to a host and port.

CAA restricts which CAs may issue certificates.

ALIAS/ANAME gives CNAME behavior at the root.

TTL in 30 seconds

TTL is the seconds a resolver caches a record. Default 3600 (one hour). About 24 hours before a host migration, drop it to 300 so changes propagate fast, then raise it back to 3600 afterward.

Practical recipes

Point a domain to a host

```
A     @     203.0.113.25
CNAME www   yourdomain.com.
```

Apex cannot be a CNAME

RFC 1034 bars a CNAME beside the apex SOA and NS. Use ALIAS/ANAME or Cloudflare CNAME flattening. This does not let MX point at a CNAME; MX needs a real hostname.

```
ALIAS @   target.host.com.
```

Email deliverability (Google Workspace)

```
MX    @                  1 smtp.google.com.
TXT   @                  v=spf1 include:_spf.google.com ~all
TXT   google._domainkey  v=DKIM1; k=rsa; p=<key from Admin console>
TXT   _dmarc             v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
```

SPF = who may send. DKIM = signature. DMARC = policy plus reports. Roll DMARC p=none : quarantine : reject over weeks.

Verify domain ownership

```
TXT   @   google-site-verification=Abc123Xyz...
```

Restrict cert issuance

```
CAA   @   0 issue "letsencrypt.org"
```

Host migration without downtime

```
# ~24h before: lower TTL on A @ to 300
# at cutover: point A @ to the new IP
A   @   198.51.100.40
# after it settles: raise TTL back to 3600
```

Mistakes and gotchas

Propagation is not a fixed 24 to 48 hour timer; it is old TTL plus resolver caching. Lowering TTL first is the real lever. Only one SPF record per domain (two `v=spf1` TXT = PermError). SPF has a 10-DNS-lookup limit; too many `include:` = PermError. PTR is set by your host, not your zone. Mind the trailing dot: `example.com.` is fully qualified. On Cloudflare, orange = proxied, grey = DNS-only.