



DNS Setup

Domain Name System (DNS) is a system used in the Internet for translating names of network nodes into addresses. This appendix describes how to set up DNS services for use with your Cisco SIP proxy server (Cisco SPS).

Starting with Cisco SPS 2.1, you should set up your DNS services with naming-authority pointer record (NAPTR) records and server (SRV) records based on RFC 3263 guidelines. Doing so ensures high scalability, availability, security, and interoperability of your service deployments.

Different levels of DNS records are used as shown in [Figure D-1](#).

Figure D-1 DNS Record Levels

```
|
|--service-1 [SRV] gives an ordered list of targets to contact
|                   | for service-1 in the domain. We'll call this
|                   | list the "SRV records list."
|
|                   |--server-1 [A] gives a list of network addresses for the target.
|                   | We'll call this list the "A records list."
|                   |
|                   |--IP-1 1st network address to contact for service-1
|                   | in domain
|                   |--IP-2 2nd network address to contact for service-1
|                   | in domain
|                   |
|                   | :
|                   | :
|                   |
|                   |--server-2
|                   |
|                   | :
|                   | :
|
|----service-2
|
| :
| :...service-N
| :
```

Use DNS records for the following purposes:

- Naming-authority pointer (NAPTR) records—Use to set up different services in the domain. RFC 3263 defines each transport support on Session Initialization Protocol (SIP) as a different service. Hence, SIP over Transmission Control Protocol (TCP), SIP over User Datagram Protocol (UDP), and SIP over Transport Layer Security Protocol (TLS) are three different services, with three different NAPTR records.

- Server resource (SRV) records—Use to provide contacts for the specific domain services. An SRV lookup for a specific service results in an ordered list of SRV records. You can therefore assign your preferred contacts for the service the highest priority and your backups a lower priority.

Let each SRV record correspond to an individual farm (not farm member). This helps in the smart-failover mechanism, as suggested in RFC 3263. There should be a unique and single fully qualified domain name (FQDN) for each farm, which should be returned in the query results.

- A records—Use to provide IP addresses for specific contacts or individual farm members. Multiple A records can point to the IP address of each proxy server. For example, the FQDN for a farm in SRV records can point to a list of IP addresses, each of which also points to individual host names of each farm member.

Sample Configuration: NAPTR Records

Following is an example of a DNS configuration for domain cisco.com for a setup that has two Cisco SPS farms. The primary farm is farm1.cisco.com; the backup farm is farm2.cisco.com.

```

;;; NAPTR records for sip services
;           order pref flags service      regexp  replacement
  IN NAPTR 50   50   "s"  "SIPS+D2T"    ""      _sips._tcp.cisco.com.
  IN NAPTR 90   50   "s"  "SIP+D2T"     ""      _sip._tcp.cisco.com.
  IN NAPTR 100  50   "s"  "SIP+D2U"     ""      _sip._udp.cisco.com.

;;; SRV records for each sip service
;
;           Priority Weight Port Target
_sips._tcp.cisco.com SRV      10      1    5061 farm1.cisco.com.
                   SRV      20      1    5061 farm2.cisco.com.
_sip._tcp.cisco.com  SRV      10      1    5060 farm1.cisco.com.
                   SRV      20      1    5060 farm2.cisco.com.
_sip._udp.cisco.com  SRV      10      1    5060 farm1.cisco.com.
                   SRV      20      1    5060 farm2.cisco.com.

;;; A records for the contacts mentioned in SRV records
farm1      IN A          10.4.175.126  ;; proxy1
           IN A          10.4.175.127  ;; proxy2
farm2      IN A          10.4.175.128  ;; proxy3
           IN A          10.4.175.129  ;; proxy4

;;; A records for the well known names of the hosts
proxy1     IN A          10.4.175.126
proxy2     IN A          10.4.175.127
proxy3     IN A          10.4.175.128
proxy4     IN A          10.4.175.129

```

In this example, the proxy-server domain is cisco.com, and therefore the proxy-server configuration directive ProxyDomain is also set to cisco.com. Similarly, the proxy-server farm FQDNs are farm1.cisco.com and farm2.cisco.com, and therefore the directive ServerName is also set to one of the two values, as appropriate.

You can use Cisco SPS to support multiple virtual domains. In such deployments, the virtual domain owners might configure their NAPTR DNS records such that the domain suffix in the NAPTR replacement field points to a DNS SRV entry in the actual server domain instead of their own domain. The domain suffixes in the NAPTR replacement field need not match the domain of the original query. However, for backward compatibility with RFC 2543, such domains must maintain SRV records for the domain of the original query, even if the NAPTR record points to a different domain.

As an example, if the SIP+D2T service field above contained the TCP SRV replacement value _sip._tcp.example.com, an SRV record must also exist at the domain cisco.com. The SRV query string _sip._tcp.cisco.com should return the contact as the actual FQDN in the example.com domain. Since RFC 2543 clients may not support NAPTR lookup, they look up the SRV records for the domain

cisco.com directly. Clients whose queries are not answered fail. Again, to maintain maximum compatibility with upstream stateless proxies, we recommend that you assign different weights to SRV records with equal priority.

For NAPTR records with SIPS protocol fields, if Cisco SPS uses a site certificate, the domain name of the NAPTR query and the domain name in the replacement field must both be valid according to the site certificate handed out by Cisco SPS in the TLS exchange. Similarly, the domain name in the SRV query and the domain name in the target in the SRV record must both be valid according to the same site certificate. This ensures correct trust credentials with upstream clients.

