White Paper

Cisco Prime Network Registrar - DNS in Mobile Networks

IP communications between service providers today are starting to evolve to support services other than General Packet Radio Service (GPRS) roaming. These new services rely upon Domain Name System (DNS) for inter-Public Land Mobile Network Multimedia Messaging Service (PLMN MMS) delivery and IP Multimedia Subsystem (IMS) interworking. Therefore, it is of utmost importance for service providers to choose the most resilient and reliable DNS solution to ensure that their customers experience seamless roaming and uninterrupted internet connectivity.

This document is intended to provide guidelines and technical information for those who need to set up or maintain DNS servers for inter-service-provider services with Cisco Prime™ Network Registrar.

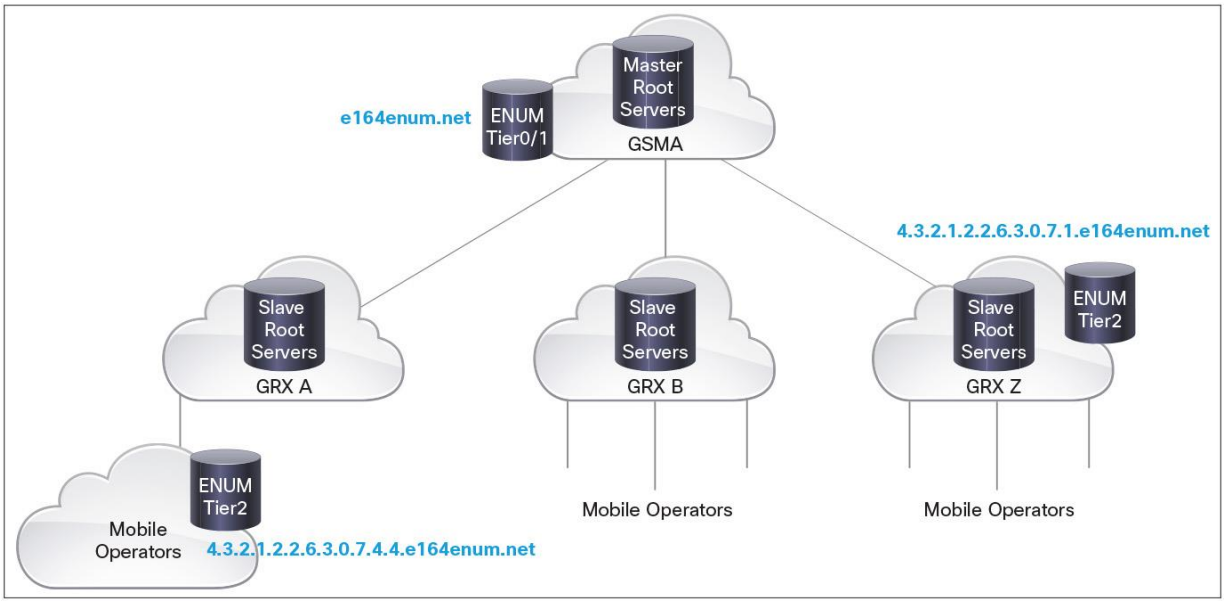
DNS as Used in an MPC/EPC Network[1]

The Domain Name System is critical to such services as GPRS roaming, inter-PLMN MMS delivery, and IMS interworking. DNS is defined in many IETF RFC documents; the most notable ones are IETF RFC 1034 [1] and IETF RFC 1035 [2]. The DNS on the inter-PLMN IP backbone network (known as the "GRX/IPX") is completely separate from the DNS on the Internet. This is purposely done to add an extra layer of security to the GRX/IPX network and the nodes within it.

The GRX/IPX root DNS servers that network operators see are known as "secondary" root DNS servers and are commonly provisioned by a service provider's GRX/IPX service provider. See Figure 1. However, operators themselves can provision these secondary root DNS servers if they so wish by making a copy of the GRX root server records in their own network. The “primary” root DNS servers are managed by the GSM Association (GSMA) and have no relationship to the 13 root name servers `([a-m].root-servers.net.)` used by all Internet DNS users.

[1] http://www.gsma.com/newsroom/wp-content/uploads/2012/11/IR.67-v8.0.pdf

Figure 1. Typical DNS Setup in a GSMA Network



Having a consistent naming convention makes tracing and troubleshooting easier as well as easing the maintenance of a service provider's DNS. The following convention is recommended to achieve these goals:

Service provider nodes should have names for each interface with the following format:

```
<city>-<type>-<nbr>
```

Where:

- <city> is the name, or shortened name, of the city/town (or closest, where applicable) where the node is located
- <type> describes the device type and should be one of the following for GRX/IPX-connected hosts:
  - dns (DNS/ENUM servers)
  - ggsn
  - sgsn
  - rtr (router)
  - fw (firewall)
- <nbr> is a running number of similar devices at the same city (for DNS servers, use 0 to indicate the primary DNS server)

Support for IPv4 and IPv6 on service provider DNS name servers is twofold: the ability to serve data relating to IPv4 and IPv6 addresses and connectivity to and from the name server. For configuration information in a name server, IPv4 and IPv6 information can coexist together. Service providers just need to make sure that the name server software used is capable of supporting the relevant resource records (RRs) required. The A RR is used to hold IPv4 address information and the AAAA RR is used for IPv6 address information.

GPRS provides for a packet-switched bearer in Global System for Mobile Communications (GSM)/Universal Mobile Telecommunications Service (UMTS) networks. Packets are tunneled between core network nodes that may or may not be in different PLMNs, using the GPRS Tunneling Protocol (GTP) as defined in 3GPP TS 29.060 [24].

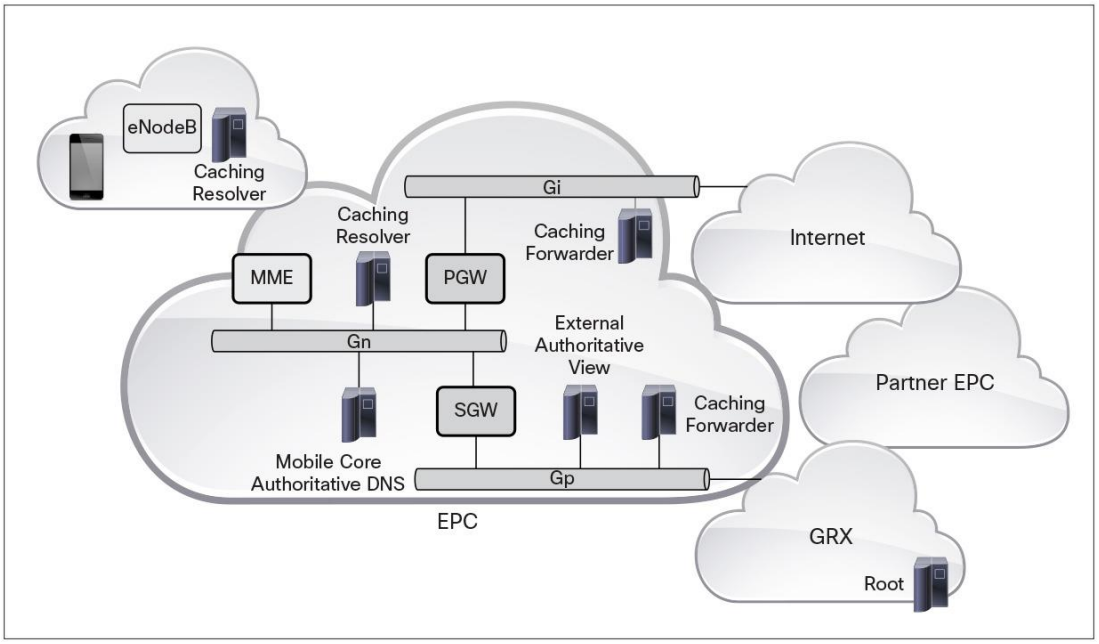
Packet Data Protocol (PDP) context activations occur between the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN). PDP contexts are activated to an Access Point Name (APN) either provided by the mobile station (MS) or derived by the network (such as when the MS instructs the SGSN to use a "default" APN). It is the APN that determines to which interface on which GGSN the PDP context is to be established.

An SGSN (serving gateway [SGW]) and a GGSN (packet data network gateway [PGW]) can be located in either the Home PLMN (HPLMN) or Visited PLMN (VPLMN). Both are in the same network when the subscriber is in the HPLMN and also when the subscriber is roaming in a VPLMN and is using a GGSN in the VPLMN (vGGSN). However, the SGSN and GGSN are in different networks when the subscriber is roaming but using a GGSN in the HPLMN (hGGSN).

GPRS roaming means the extension of packet-switched services offered in the Home PLMN to Visited PLMNs with which the HPLMN has a predefined commercial roaming agreement.

The necessary DNS queries for resolving an APN in order to activate a PDP context are described below. Note that the authoritative DNS server is usually located in the same PLMN as the GGSN, but can be located elsewhere, for example, in the HPLMN's GRX/IPX provider's network (due to the HPLMN outsourcing the authoritative DNS server). Figure 2 shows an architectural representation of several DNS functions in a 3GPP Evolved Packet System (EPS) network and the relation between a DNS server and components of the network described earlier.

Figure 2. DNS Model for Mobile Networks



The GSM Association recommends use of a commercial DNS name server for such mobile services. By choosing a commercial DNS product such as Cisco Prime Network Registrar, service providers can satisfy client roaming needs both today and tomorrow by using the product's built-in features, including but not limited to DNS High Availability, DNS Views, and VoLTE ENUM (E.164 Number Mapping), with a single DNS product architecture.

Cisco Prime Network Registrar - Introduction

Cisco Prime Network Registrar is part of the Cisco Prime portfolio of OSS and network management solutions. The Cisco Prime portfolio of IT and service provider management offerings empowers organizations to more effectively manage their networks and the services they deliver. Built on a service-centered foundation, Cisco Prime supports integrated lifecycle management through an intuitive workflow-oriented user experience, providing A-to-Z management for evolved programmable networks, mobility, video, cloud, and managed services.

Cisco Prime Network Registrar provides integrated, scalable, reliable DNS, Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM) (DDI) services for both IPv4 and IPv6. The solution supports dual-stack environments to manage both IPv4 and IPv6 seamlessly. The IPAM rich GUI includes megamenu selections that show both IPv4 and IPv6 in one window, allowing users to maintain their dual-stack environment as well as their DNS settings without switching applications or context within the application.

Cisco Prime Network Registrar includes the following integrated components and their respective services - all supporting both IPv4 and IPv6:

- An authoritative DNS server for IP address translation and service delivery
- A DNS caching server that supports DNS Security Extensions (DNSSEC) and is designed to prevent cache poisoning and other attacks
- A single DHCP server for device network access
- A powerful, comprehensive IPAM system to automate and manage all IP address requirements

Cisco Prime Network Registrar DNS Benefits

- **Fast and scalable:** The recursive, extremely fast, DNS caching server offers significant acceleration of DNS queries.
- **Reliable:** Support for High-Availability DNS (HA-DNS) promotes continuous business operations.
- **Cloud support:** Multitenant capabilities help enable cloud-based DNS services (including DNS Views) by providing subscribers with secure IP address management and self-service control.
- **Easy to deploy and low risk:** Cisco Prime Network Registrar can be deployed as a preconfigured virtual appliance and will run on any VMware ESXi-capable server - simplifying installation, lowering deployment risks, and reducing startup costs.

Configuring Cisco Prime Network Registrar DNS for Mobility Applications

Creating Zones

The first step toward creating resource records in the DNS server is to create a zone for the domain name for which Cisco Prime Network Registrar will provide services. A DNS zone is a portion of a domain name space using the Domain Name System for which administrative responsibility has been delegated.

For example: 'epc.mncxxx.mccxxx.3gppnetwork.org'

In the above example, we have a zone that has traversed several levels into the root domain (which is '3gppnetwork.org'). In order to simplify the zone such that we can accommodate more subdomains under the root domain, we could create subzones (also known as subdomains or child zones). Subzones allow you to organize zone data into manageable pieces.

Creating Resource Records

In a typical mobile (3G, 4G) service provider network, the following three types of resource records will be created in the DNS server:

- A record (32-bit)/AAAA record (128-bit) - Hostname to IP address mapping.
- SRV record (service locator) - Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.
- NAPTR record (naming authority pointer) - Allows regular expression-based rewriting of domain names, which can then be used as uniform resource identifiers (URIs), further domain names to lookups, and so on.

DNS A Records

A records, or "address records," are detailed in RFC 1035. An A record returns an IPv4 address. It is most commonly used to map hostnames to an IPv4 address. Each A (or AAAA) record can have its own TTL (time to live) parameter specified. TTLs are set by an authoritative nameserver for a particular resource record. When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL.

The essential contents of the address records is as follows:

```
<Hostname>A      <IPV4- Address>
<Hostname>AAAA   <IPV6- Address>
```

DNS SRV Records

DNS resource records for specifying the location of services (DNS SRV) are described in RFC-2782.

Clients can ask for a specific service/protocol for a specific domain and get back the names of any available servers.

The format of the SRV RR is as follows:

```
'_Service._Proto.Name   TTL  Class   SRV   Priority  Weight  Port  Target'
```

NAPTR Records

The name authority pointer (NAPTR) is used by the DNS client to reference supported application interface types in 3GPP 23.003. The S-NAPTR (Straightforward NAPTR) rewrite process is controlled by flags that provide information on how to communicate with the host at the domain name that was the result of the rewrite. If DNS returns multiple NAPTR resource records, those can be prioritized using embedded order and preference values defined by the DNS administrator.

The format of an NAPTR record is as follows (an example):

```
cisco.com.apn IN NAPTR 1  5  "a"  "x-3gpp-pgw:x-s5-gtp"   ""
nodes1.pgw.3gppnetwork.org
```

Where:

- 1 is the order and 5 is the preference.
- “a” is the terminal flag, which indicates that an A record is next.
- The text following “a” is the service parameter used to filter the DNS response.
- The last bit of text (nodes1.pgw.3gppnetwork.org) is a replacement expression that points to the corresponding A record.

Since NAPTR records are a proposed standard, RFC 3403, Cisco Prime Network Registrar only validates their numeric record fields. However, the proposed standard requires a value for each field, even if it is null (""), and there are no preset values.

The concept of S-NAPTR also simplifies the use of NAPTR by limiting the terminal flags only to “A” and “S”. If the terminal flag is “S”, then the next DNS query is made for SRV records by using the replacement field as the target. The result of the SRV query is a list of SRV records with port number, target, preference, weight, and so on.

In summary, S-NAPTR uses:

- Only “S” and “A” as terminal flags (NAPTR RFC defines more flags)
- Replacement expressions and not regular expressions

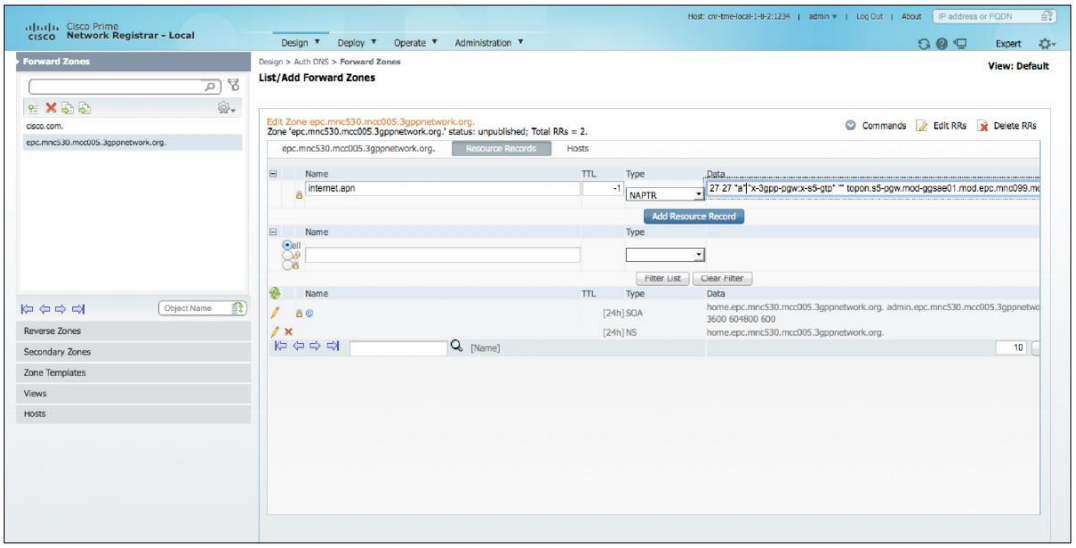
The Mobile Management Entity (MME) uses a DNS query of type "NAPTR" to identify the SGW that needs to handle the subscriber's bearer. The NAPTR query includes a Tracking Area Identity Fully Qualified Domain Name (TAI FQDN). The MME constructs the TAI FQDN as defined in subclause 19.4.2.3 of 3GPP TS 23.003.

If the terminal flag was “A”, then the next DNS query is made for A records by using the replacement field as the target. The result of the A query should give the IP address of GW (gateway) offering the required service over the desired protocol.

For each node type in Evolved Packet Core (EPC) that can be queried for information using the S-NAPTR procedure, the authoritative DNS server for a given domain should be provisioned with a unique domain name for each EPC node or other identifier that is explicitly specified by a procedure in this specification (for example, one based on APN, TAI, GUTI, and so on) and corresponding NAPTR records.

Figure 3 shows the creation of an NAPTR RR using the Cisco Prime Network Registrar GUI.

Figure 3. Adding an NAPTR Resource Record in Cisco Prime Network Registrar



Node Selection Using DNS

DNS in LTE Summary

This subsection aims to summarize the key DNS-related information relevant for LTE deployments. This can be used as reference information in the context of DNS design and Cisco Prime Network Registrar configuration.

LTE APN Fully Qualified Domain Name

The APN-FQDN is derived from an APN as follows:

- The APN consists of an APN Network Identifier (APN NI -> APN Name) and an APN Operator Identifier (APN OI -> Operator GPRS Domain).
- The APN-FQDN is obtained from the APN by inserting the labels "apn.epc" between the APN NI and the default APN OI, and by replacing the label "gprs" at the end of the default APN OI with the label “3gppnetwork.org". “APN-NI.mnc<MNC>.mcc<MCC>.gprs” would be translated into “APN-NI.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org”.

Several entries of this record type are kept in DNS for APN queries by MME.

APN should be in the form “<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org” in Cisco Prime Network Registrar.

TAI Fully Qualified Domain Name

The TAI FQDN is constructed as:

```
“tac-lb<TAC-low-byte>.tac-hb<TAC-high-
byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org”.
```

Several numbers of records of this kind are kept in DNS for DNS queries by MME for SGW selection.

The tracking area code (TAC) is a 16-bit integer. <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and <TAC-low-byte > is the hexadecimal string of the least significant byte.

DNS Call Flow

The DNS call flow mechanism is based on the 3GPP standards defined in the following:

- TS 23.401, TS 23.060 for node selection principles
- TS 23.003 for node identifiers
- TS 29.303 for DNS procedures

3GPP node selection uses S-NAPTR records. S-NAPTR is a stripped down version of NAPTR procedures that simplifies and reduces complexity associated with the regular NAPTR procedures.

If the terminal flag is “S”, the replacement field is the target of the DNS query for an SRV record.

If the flag is “A”, the replacement field is the target of the DNS query for an address record.

The information below showcases the configuration of a Cisco Prime Network Registrar DNS server in a typical 3G/4G LTE environment.

SGW and PGW Node Selection

The MME needs to select the SGW and PGW for the user equipment (UE) that is requesting access to a specific APN. The APN used is either obtained by the MME from the user subscriber record coming from the Home Subscriber Server (HSS) or is the APN provided by the UE. This APN name will be required in order for the MME to identify which PGW offers such service.

SGW List Retrieval

MME will use TAI information (UE location) to identify the closest SGW for this tracking area. The MME will contact the DNS in order to identify the SGW supporting that TAI.

The MME will then filter the ones associated to the application x-3gpp-sgw and service x-s5-gtp. The result of this will be the list of the candidate SGWs (Candidate A list from 3GPP 29.303).

NAPTR Records

For TAC 1, the first entry SGW with lower order (order 10) will be selected. The second SGW entry/node will be used only if the first node is down.

For TAC 2, the first entry SGW with lower order (order 10) will be selected. The second SGW entry/node will be used only if the first node is down.

Note: The NAPTR order will be used after gateway selection based on topology or colocation selection.

For the PGW, the DNS entries associated to the APN are as follows:

```
internet.apn     IN     NAPTR  27 27 "a" "x-3gpp-pgw:x-s5-gtp" "" topon.s5-
pgw.ggsabc.loc.epc.mncxxx.mccxxx.3gppnetwork.org.
```

The associated A records for the SGWs to be assigned are:

```
topon.s5-pgw.ggsabc.loc        IN     A      x.x.x.x
```

PGW List Retrieval

The MME will contact the DNS in order to find the mapping between the APN and the PGW. For the DNS query, the MME will use the APN-FQDN. In a simplified form, the DNS may hold various records (S-NAPTR) for the APN-FQDN on which the subscriber wants to connect.

The MME will filter the ones associated to the application x-3gpp-pgw and service x-s5-gtp. The result of this will be the list of the candidate PGWs (Candidate B list from 3GPP 29.303).

ENUM Records

Creating separate E.164 Number Mapping (ENUM) domains simplifies the management of the NAPTR ENUM. It simplifies to a great extent the setup and management of E.164 numbers and how available services are connected to the E.164 numbers. When you create an ENUM zone and add the corresponding E.164 numbers, Cisco Prime Network Registrar automatically creates a forward zone and the respective NAPTR resource records.

Cisco Prime Network Registrar also has ENUM interfaces in the GUI that simplify editing of the ENUM records.

Call Flow Mechanism

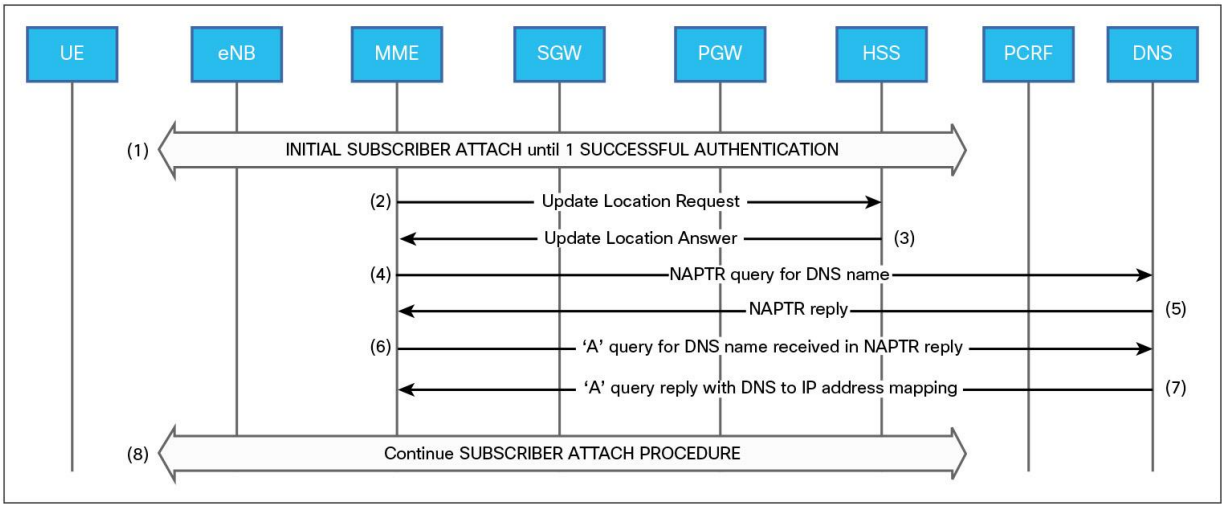
As a subscriber attempts to access the Mobile Packet Core (MPC)/EPC network using the attach procedure, the MME needs to determine the SGW and the PGW that will handle the subscriber's bearer traffic. The MME in such a network would be configured to use the services of the Cisco Prime Network Registrar DNS server in order to determine the SGW and/or PGW IP address for a particular subscriber attach request.

The following sections explain the different options available for SGW and PGW selection and how the base configuration changes with those options.

The steps listed below and Figure 4 illustrate the DNS call flow.

1. The initial Attach call flow is the same as the Session Attach with Default Bearer call flow until a successful authentication is made.
2. The MME sends an Update Location Request to the HSS.
3. The MME is configured to use DNS to identify the IP address of the SGW:
    a. The MME uses a DNS query of type "NAPTR to identify the SGW that needs to handle the subscriber's bearer.
    b. The NAPTR query includes a TAI FQDN. The MME shall construct the TAI FQDN as defined in subclause 19.4.2.3 of 3GPP TS 23.003. The TAI FQDN shall be constructed as:
        i. tac-lb<TAC-low-byte>.tac-hb<TAC-highbyte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
        ii. In our example, the NAPTR query included the TAI FQDN of tac-lb0c.tachb00.tac.epc.mnc156.mcc123.3gppnetwork.org.
4. DNS replies to the NAPTR query with Flag=A, Service=x-3gpp-sgw:x-s5-gtp, and Replacement=sgw1.3gppnetwork.org.
    a. This tells the MME to use the SGW "sgw1.3gppnetwork.org" for this subscriber's bearer.
5. MME sends a query to DNS to resolve sgw1.3gppnetwork.org.
6. The DNS server resolves the DNS query and returns the SGW IP address.
7. The rest of the call flow is the same as the Session Attach with Default Bearer call flow.

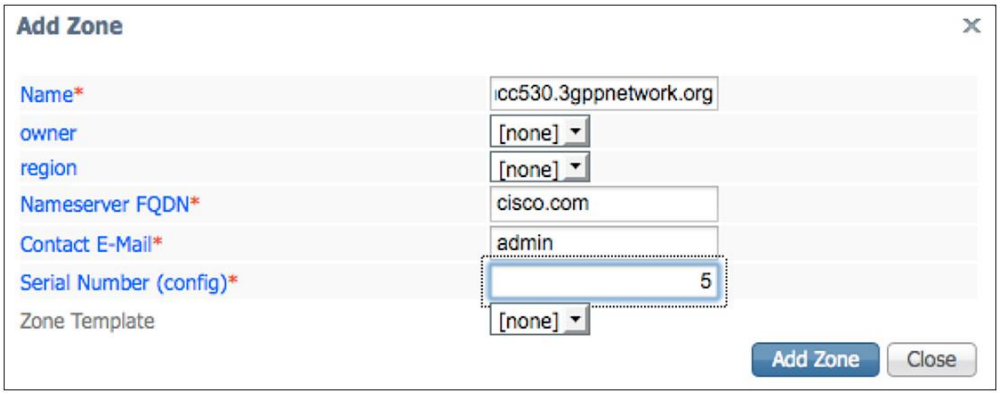
Figure 4. Cisco Prime Network Registrar - MME Call Flow



To configure the SGW in the Cisco Prime Network Registrar DNS server, per instructions mentioned earlier on creating zones and resource records, these steps should be followed:

1. Create a zone (see Figure 5).

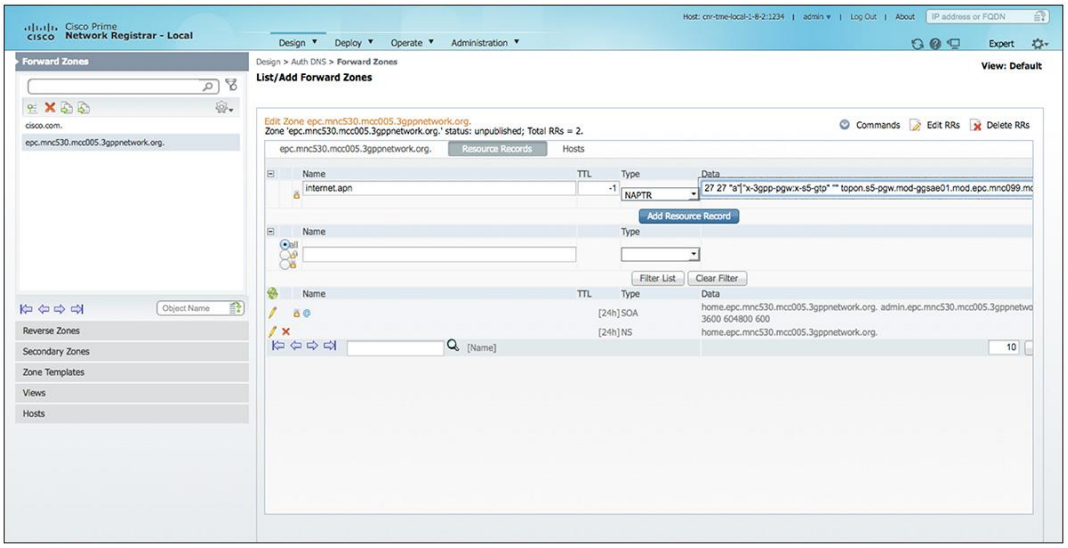
Figure 5. Zone Creation - Call Flow



2. Create an NAPTR resource record (see Figure 6).

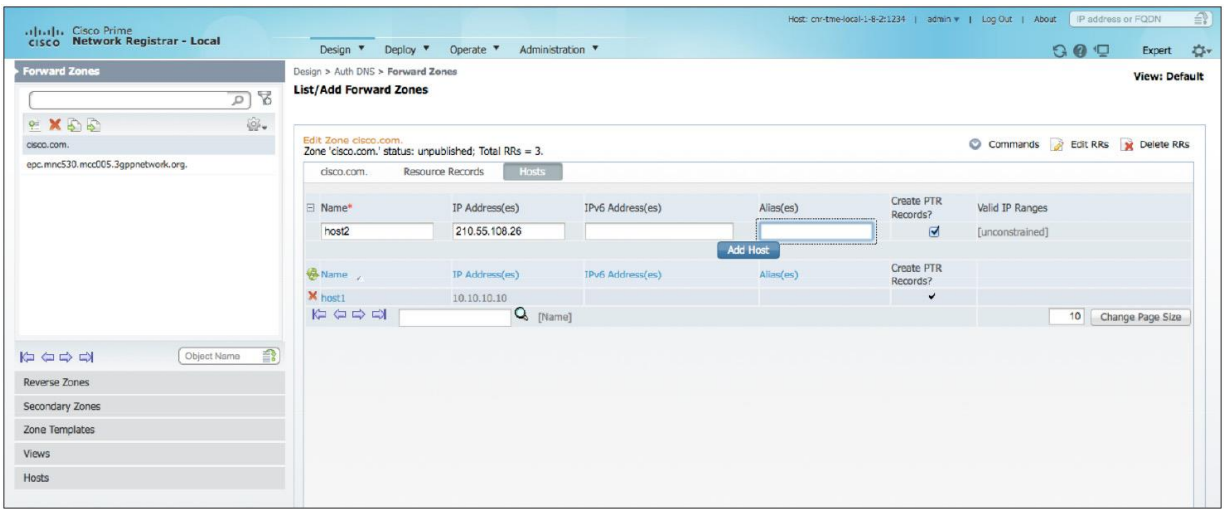
```
Name = tac-lb64.tac-hb00.tac.epc.mncxxx.mccxxx.3gppnetwork.org.
TTL = 24h
Type = NAPTR
Data = 10 27 "a" "x-3gp-sgw:x-s5-gtp" "" topon.s11-
sgw.locggsae01.loc.epc.mncxxx.mccxxx.3gppnetwork.org.
```

Figure 6. NAPTR RR Creation - Call Flow



3. Create other RRs.
4. Add hosts to the zone (see Figure 7).

Figure 7. Hosts - Call Flow



The preceding data translates into the following:

- When the MME sends an NAPTR record query, the MME queries for the TAI FQDN name (tac-lb0c.tac-hb00.tac.epc.mnc156.mcc123.3gppnetwork.org).
- When the query arrives, Cisco Prime Network Registrar retrieves the created NAPTR resource record and sends the configured information, where x-3gpp-sgw:x-s5-gtp is the Service field, indicating an SGW service over an S5 interface; sgw1.3gppnetwork.org is the Replacement field; “a” is the flag indicating that the next lookup should be of type A.

- After the MME receives the reply to the NAPTR query, the MME sends an A query asking DNS to resolve the Replacement field (sgw1.3gppnetwork.org).
- Cisco Prime Network Registrar, upon receiving the A query, looks up the IP address of "sgw1.3gppnetwork.org" created in the previous steps and sends the IP address in a reply.

DNS is usually available on the Gn/Gp interface and is used to resolve the APN for PDP context activation and to resolve the IP address of the old SGSN during the Inter-SGSN routing area update.

Cisco Prime Network Registrar Jumpstart for Mobility

Cisco Prime Network Registrar Jumpstart is a high-performing physical appliance that can be configured for DNS services and DHCP services for both IPv4 and IPv6 addresses.

The solution includes the following:

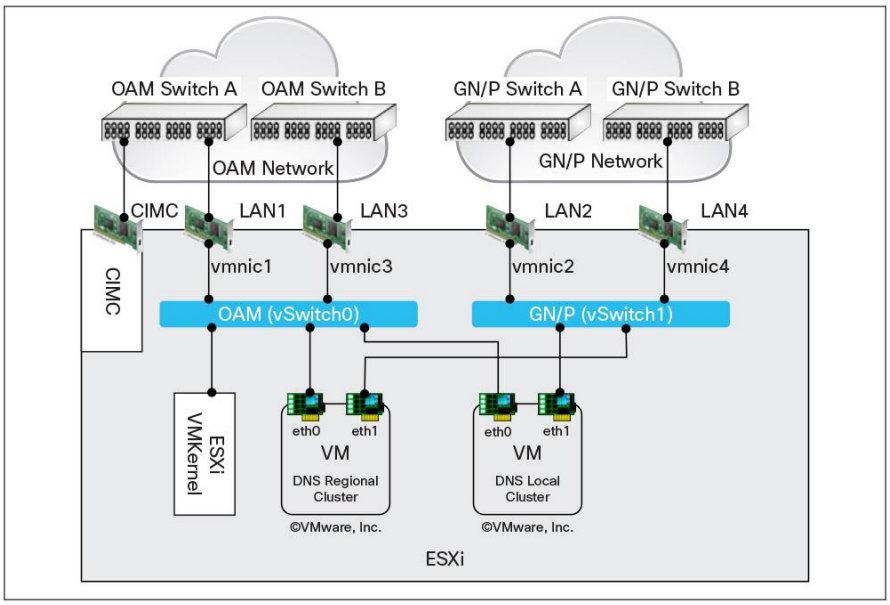
- Cisco Prime Network Registrar DNS: A single DNS server for IP address translation and service delivery that supports both IPv4 and IPv6 - preinstalled on the appliance
- Cisco Prime Network Registrar DNS Caching: A DNS caching server that supports DNS Security Extensions to prevent cache poisoning and other attacks and provides validation that DNS data has been signed - preinstalled on the appliance
- Cisco Prime Network Registrar DHCP: A single DHCP server for device network access that supports both IPv4 and IPv6 - preinstalled on the appliance
- Cisco Unified Computing System™ (Cisco UCS®) C220 M3: High-density, two-socket, one rack-unit (RU) rack-mount server
- VMware ESXi: VMware virtualization technology - preinstalled on the appliance

The Cisco Prime Network Registrar software is preinstalled as a virtual machine in the appliance.

In a typical mobile service provider environment, there need to be redundant network interfaces as well as separate connections to the operation, administration, and maintenance (OAM) network as well as the packet core network. Cisco Prime Network Registrar Jumpstart comes in very handy in such instances, as it has an inbuilt VMware hypervisor environment, which can contain several virtual machines (for individual Cisco Prime Network Registrar components).

These two pairs of interfaces can be configured with an Ethernet bonding mechanism to provide fault tolerance and load balancing with network interface cards (NICs). With Ethernet bonding, two NICs are dedicated for each network to which the DNS connects. One of these interfaces is marked as primary, and the other interface is marked as secondary. In the event of a failure of the primary interface, the system will automatically switch to using the secondary interface. Figure 8 showcases an example setup.

Figure 8. Cisco Prime Network Registrar **Jumpstart Setup Example**



Cisco Prime Network Registrar DNS Security

The intent of this section is to describe the different security options on the Cisco Prime Network Registrar DNS platform, their advantages, and their disadvantages.

Zone Transfers

Cisco Prime Network Registrar enables transfer of zone information among DNS authoritative servers. Using this option, administrators will not have to update all DNS servers within a managed network. Cisco Prime Network Registrar can restrict zone transfers by setting the restrict-xfer attribute to true (the present value is false) on the primary server. The restrict-xfer-acl setting has to be made accordingly.

Notify Option

Cisco Prime Network Registrar's notify capability allows the DNS server to send information to other computers to inform them that a modification of a zone file has been performed.

Transaction Security

With Cisco Prime Network Registrar, it is possible to define a key for transactions in order to cryptographically authenticate and verify zone data as well as to authorize in order to verify the client. It can be used for zone transfers and dynamic updates. This key will only be established for transfer zones from primary DNS to secondary.

Radius Authentication

Cisco Prime Network Registrar includes a RADIUS client component, which is integrated with the authentication and authorization module of the Central Configuration Management (CCM) server[2]. When external authentication is enabled, the CCM server handles attempts to log in through the web UI, software development kit (SDK), or command-line interface (CLI), by issuing a RADIUS request to a RADIUS server that is selected dynamically from

[2] Central Configuration Management server - the core service between DNS and users who log in to Cisco Prime Network Registrar.

the configured list. The RADIUS server that most recently responded successfully to a request is always preferred. If the RADIUS server validates the login request, access is granted, and the CCM server creates an authorized session with the group assignments specified by the RADIUS server.

Cisco Prime Access Registrar

Cisco Prime Access Registrar is the leading Cisco® RADIUS and Diameter authentication, authorization, and accounting (AAA) server for the service provider market. It supports service provider deployment of access services by centralizing AAA information and simplifying provisioning and management. Cisco Prime Access Registrar is a standards-based RADIUS/Diameter and proxy RADIUS/Diameter server designed for high performance, extensibility, and integration with external data stores and systems. It provides an ideal solution for service providers with wide-area broadband (WiMax), wide-area mobile Code Division Multiple Access (CDMA), GPRS, Universal Mobile Telecommunications Service, 1xRTT, 1xEV-DOrA, wired and wireless local-area networks (Wi-Fi, WiMax), dial-up, and DSL services.

For More Information

For more information about Cisco Prime Network Registrar, please visit http://www.cisco.com/go/networkregistrar or contact your local account representative.

To download a copy of Cisco Prime Network Registrar 8.x for evaluation, please contact your Cisco account representative and discover the benefits of this powerful solution with a no cost evaluation license.

For more information on Cisco Prime Access Registrar go to http://www.cisco.com/go/accessregistrar.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-731488-00 05/14