Network Working Group
Request for Comments: 3761
Obsoletes: 2916
Category: Standards Track

P. Faltstrom
Cisco Systems, Inc.
M. Mealling
VeriSign

April 2004

The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

Status of this Memo

Copyright Notice

Abstract

This document discusses the use of the Domain Name System (DNS) for storage of E.164 numbers. More specifically, how DNS can be used for identifying available services connected to one E.164 number. It specifically obsoletes RFC 2916 to bring it in line with the Dynamic Delegation Discovery System (DDDS) Application specification found in the document series specified in RFC 3401. It is very important to note that it is impossible to read and understand this document without reading the documents discussed in RFC 3401.

Table of Contents

1. Introduction

This document discusses the use of the Domain Name System (DNS) for storage of E.164 numbers. More specifically, how DNS can be used for identifying available services connected to one E.164 number. It specifically obsoletes RFC 2916 to bring it in line with the Dynamic Delegation Discovery System (DDDS) Application specification found in the document series specified in RFC 3401 [6]. It is very important to note that it is impossible to read and understand this document without reading the documents discussed in RFC 3401 [6].

Through transformation of International Public Telecommunication Numbers in the international format [5], called within this document E.164 numbers, into DNS names and the use of existing DNS services like delegation through NS records and NAPTR records, one can look up what services are available for a specific E.164 in a decentralized way with distributed management of the different levels in the lookup process.

The domain "e164.arpa" is being populated in order to provide the infrastructure in DNS for storage of E.164 numbers. In order to facilitate distributed operations, this domain is divided into subdomains. Holders of E.164 numbers which want to be listed in DNS should contact the appropriate zone administrator according to the

policy which is attached to the zone. One should start looking for this information by examining the SOA resource record associated with the zone, just like in normal DNS operations.

Of course, as with other domains, policies for such listings will be controlled on a subdomain basis and may differ in different parts of the world.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

All other capitalized terms are taken from the vocabulary found in the DDDS algorithm specification found in RFC 3403 [2].

1.2. Use for these mechanisms for private dialing plans

This document describes the operation of these mechanisms in the context of numbers allocated according to the ITU-T recommendation E.164. The same mechanisms might be used for private dialing plans. If these mechanisms are re-used, the suffix used for the private dialing plan MUST NOT be e164.arpa, to avoid conflict with this specification. Parties to the private dialing plan will need to know the suffix used by their private dialing plan for correct operation of these mechanisms. Further, the application unique string used SHOULD be the full number as specified, but without the leading '+', and such private use MUST NOT be called "ENUM".

1.3. Application of local policy

The Order field in the NAPTR record specifies in what order the DNS records are to be interpreted. This is because DNS does not guarantee the order of records returned in the answer section of a DNS packet. In most ENUM cases this isn't an issue because the typical regular expression will be '!^.*$!' since the first query often results in a terminal Rule.

But there are other cases (non-terminal Rules) where two different Rules both match the given Application Unique String. As each Rule is evaluated within the algorithm, one may match a more significant piece of the AUS than the other. For example, by using a non-terminal NAPTR a given set of numbers is sent to some private-dialing-plan-specific zone. Within that zone there are two Rules that state that if a match is for the entire exchange and the service is SIP related then the first, SIP-specific rule is used. But the other Rule matches a longer piece of the AUS, specifying that for

some other service (instant messaging) that the Rule denotes a departmental level service. If the shorter matching Rule comes before the longer match, it can 'mask' the other rules. Thus, the order in which each Rule is tested against the AUS is an important corner case that many DDDS applications take advantage of.

In the case where the zone authority wishes to state that two Rules have the same effect or are identical in usage, then the Order for those records is set to the same value. In that case, the Preference is used to specify a locally over-ridable suggestion by the zone authority that one Rule might simply be better than another for some reason.

For ENUM this specifies where a client is allowed to apply local policy and where it is not. The Order field in the NAPTR is a request from the holder of the E.164 number that the records be handled in a specific way. The Preference field is merely a suggestion from that E.164 holder that one record might be better than another. A client implementing ENUM MUST adhere to the Order field but can simply take the Preference value "on advisement" as part of a client context specific selection method.

2. The ENUM Application Specifications

This template defines the ENUM DDDS Application according to the rules and requirements found in [7]. The DDDS database used by this Application is found in [2] which is the document that defines the NAPTR DNS Resource Record type.

ENUM is only applicable for E.164 numbers. ENUM compliant applications MUST only query DNS for what it believes is an E.164 number. Since there are numerous dialing plans which can change over time, it is probably impossible for a client application to have perfect knowledge about every valid and dialable E.164 number. Therefore a client application, doing everything within its power, can end up with what it thinks is a syntactically correct E.164 number which in reality is not actually valid or dialable. This implies that applications MAY send DNS queries when, for example, a user mistypes a number in a user interface. Because of this, there is the risk that collisions between E.164 numbers and non-E.164 numbers can occur. To mitigate this risk, the E2U portion of the service field MUST NOT be used for non-E.164 numbers.

2.1. Application Unique String

The Application Unique String is a fully qualified E.164 number minus any non-digit characters except for the '+' character which appears at the beginning of the number. The "+" is kept to provide a well understood anchor for the AUS in order to distinguish it from other telephone numbers that are not part of the E.164 namespace.

For example, the E.164 number could start out as "+44-116-496-0348". To ensure that no syntactic sugar is allowed into the AUS, all non-digits except for "+" are removed, yielding "+441164960348".

2.2. First Well Known Rule

The First Well Known Rule for this Application is the identity rule. The output of this rule is the same as the input. This is because the E.164 namespace and this Applications databases are organized in such a way that it is possible to go directly from the name to the smallest granularity of the namespace directly from the name itself.

Take the previous example, the AUS is "+441164960348". Applying the First Well Known Rule produces the exact same string, "+441164960348".

2.3. Expected Output

The output of the last DDDS loop is a Uniform Resource Identifier in its absolute form according to the 'absoluteURI' production in the Collected ABNF found in RFC2396 [4].

2.4. Valid Databases

At present only one DDDS Database is specified for this Application. "Dynamic Delegation Discovery System (DDDS) Part Three: The DNS Database" (RFC 3403) [2] specifies a DDDS Database that uses the NAPTR DNS resource record to contain the rewrite rules. The Keys for this database are encoded as domain-names.

The output of the First Well Known Rule for the ENUM Application is the E.164 number minus all non-digit characters except for the +. In order to convert this to a unique key in this Database the string is converted into a domain-name according to this algorithm:

1. Remove all characters with the exception of the digits. For example, the First Well Known Rule produced the Key "+442079460148". This step would simply remove the leading "+", producing "442079460148".

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.