

**A New Scheme for the Compression of Domain Names**  
**draft-ietf-dnsind-local-compression-05.txt**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Comments should be sent to the author or the DNSIND WG mailing list <namedroppers@internic.net>.

Abstract

The compression of domain names in DNS messages was introduced in [[RFC1035](#)]. Although some remarks were made about applicability to future defined resource record types, no method has been deployed yet to support interoperable DNS compression for RR types specified since then.

This document summarizes current problems and proposes a new compression scheme to be applied to future RR types which supports interoperability. Also, suggestions are made how to deal with RR types defined so far.

**1. Conventions used in this document**

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 [\[RFC2119\]](#).

Domain names herein are for explanatory purposes only and should not be expected to lead to useful information in real life [\[RFC2606\]](#).

## 2. Background

Domain name compression was introduced in [\[RFC1035\]](#), [section 4.1.4](#), as an optional protocol feature and later mandated by [\[RFC1123\]](#), [section 6.1.2.4](#). The intent was to reduce the message length, especially that of UDP datagrams, by avoiding repetition of domain names or even parts thereof.

A domain name is internally represented by the concatenation of label strings, where the first octet denotes the string length, not including itself. The null string, consisting of a single octet of zeroes, is the representation of the root domain name and also terminates every domain name.

As labels may be at most 63 characters long, the two most significant bits in the length octet will always be zero. Compression works by overloading the length octet with a second meaning. If the two MSB have the value '1', the remainder of the length octet and the next octet form a compression pointer, which denotes the position of the next label of the current domain name in the message:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 1  1|                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
      OFFSET

```

It is important that these pointers always point backwards.

Compression may occur in several places. First, the owner name of an RR may be compressed. The compression target may be another owner name or a domain name in the RDATA section of a previous RR. Second, any domain name within the RDATA section may be compressed and the target may be part of the same RR, being the owner name or another domain name in the RDATA section, or it may live in a previous RR, either as its owner or as a domain name in its RDATA section. In fact, due to the chaining feature, combinations of the above may occur.

## 3. Problems

While implementations shall use and must understand compressed domain names in the RDATA section of "well known" RR types (those initially defined in [\[RFC1035\]](#)), there is no interoperable way of applying

compression to the RDATA section of newer RRs:

Quote from [\[RFC1123\]](#), section 6.1.3.5:

Compression relies on knowledge of the format of data inside a particular RR. Hence compression must only be used for the contents of well-known, class-independent RRs, and must never be used for class-specific RRs or RR types that are not well-known. The owner name of an RR is always eligible for compression.

DNS records in messages may travel through caching resolvers not aware of the particular RR's type and format. These caches cannot rearrange compression pointers in the RDATA section simply because they do not recognize them. Handing out these RRs in a different context later will lead to confusion if the target resolver tries to uncompress the domain names using wrong information. This is not restricted to intermediate caching but affects any modification to the order of RRs in the DNS message.

#### 4. Local Compression

We often observe a certain locality in the domain names used as owner and occurring in the RDATA section, e.g. in MX or NS RRs but also in newer RR types [\[RFC1183\]](#):

```
host.foo.bar.example RP adm.foo.bar.example adm.persons.bar.example
```

So, to still profit from compression without putting interoperability at risk, a new scheme is defined which limits the effect of compression to a single RR.

In contrast to the usual method of using offsets relative to the start of a DNS packet we start counting at the RR owner or calculate pointers relative to the start of the RDATA to avoid context sensitivity. We use an additional compression indicator for a two octet local pointer:

```
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 1  0 |                               OFFSET                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

The "10" bits will indicate the use of local compression and distinguish it from conventional compression, plain labels and EDNS label codes [\[EDNS0\]](#). Two types of pointers need to be specified: those pointing into the owner name and those pointing into RDATA.

A) Pointers into the owner name are interpreted as the ordinal label number (starting at 0 for the topmost label, the TLD). This way we avoid the need for extra decompression of the owner name during

message composition or decomposition.

The highest possible value of a compression pointer pointing into the owner name is 254. The value 255 is reserved for future use.

- B) Pointers into the RDATA section start at the fixed value 256 for the first octet and have a maximum value of 16383 limiting possible targets to the first 16128 octets. The actual offset relative to the start of RDATA is determined by subtracting 256 from the value of the pointer.

Local pointers MUST point to a previous occurrence of the same name in the same RR. Even domain names in another RR of the same type cannot serve as compression targets since the order of RRs in an RRSets is not necessarily stable. The length of the compressed name(s) MUST be used in the length calculation for the RDLENGTH field.

#### Example

Consider a DNS message containing two resource records, one CNAME RR and one XMPL RR, undefined and meaningless so far, with an RDATA section consisting of two domain names:

```
ab.foo.example  IN  CNAME  bar.example
bar.example     IN  XMPL   a.foo.example  foo.example
```

In a message this appears as follows (randomly starting at octet 12):

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
12 |           2           |           a           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
14 |           b           |           3           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
16 |           f           |           o           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
18 |           o           |           7           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
20 |           e           |           x           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
22 |           a           |           m           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
24 |           p           |           l           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
26 |           e           |           0           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

10 octets skipped (TYPE, CLASS, TTL, RDLENGTH)

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
38 |           3           |           b           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
40 |           a           |           r           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
42 | 1  1|           19           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The XMPL RR with local compression applied:

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
44 | 1 1 |           38           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

10 octets skipped (TYPE, CLASS, TTL, RDLENGTH)

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
56 |           1           |           a           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
58 |           3           |           f           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
60 |           o           |           o           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
62 | 1  0|           0           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
64 | 1  0|           258          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

The first local pointer at position 62 points to the topmost label "example" of the XMPL RR's owner.

The second local pointer at position 64 represents the "foo.example" and points backwards into the RDATA section, third octet, at absolute position 58. Note that with conventional compression this example message would have occupied less space.

## 5. Interaction with DNSSEC

The security extensions to DNS [[RFC2535](#)] mandate that domain names in RDATA be signed only in expanded, lower case format. For RR types using local compression the specification is changed as follows:

Resource Records subject to local compression MUST be stored, signed, transmitted and verified in locally compressed form. Name expansion or canonicalization MUST NOT be performed on the RDATA section for signing or verification.

This way RR type transparency can be achieved, since domain names in

the RDATA section are treated as arbitrary data and can be cached and verified by resolvers not aware of the particular RR type. Old RR types subject to conventional or no compression are not affected by this change.

Wildcard owners may serve as compression targets only in their fixed part. Even if a particular query asks for a domain name which could be used to compress the RDATA part more efficiently, this MUST NOT be done. Otherwise signatures would be invalidated.

Currently slave servers store zones in text format and re-encode the data into wire format, e.g. after a restart. This encoding must be unique to ensure signature validity. To achieve this, local compression MUST be applied optimally, i.e. every domain name must be compressed as far as possible and each local compression pointer must point to the earliest available target (including the owner).

## **6. Interaction with Binary Labels**

When constructing local compression pointers into the owner name, every one-bit label is counted as a label. This way the compression and decompression is independent of the actual bit-string representation.

For local compression pointers into the RDATA section, only bit-string labels may serve as targets, not single one-bit labels. Bit-string labels may be adjusted to increase compression efficiency [BINLABELS, [section 3.1](#)]

The internal representation of a domain name has a maximum length of 255 [RFC 1035]. Any label consists of at least two octets, leading to at most 127 labels per domain name plus the terminating zero octet, which does not qualify as a compression target. With the introduction of binary labels a domain name can consist of up to 1904 labels (all one-bit labels). This document restricts the possible compression targets in an owner name to the topmost 255 labels. This limit was chosen to be consistent with [RFC2535], [section 4.1.3](#).

## **7. Old RR types and deployment**

Although differences in RDATA sections by class have not yet been reported and the concept of classes did not really spread, we are just considering the IN class here.

The following RR types with domain names in the RDATA section have been defined since [RFC1035] (Standards Track, Experimental and Informational RFCs, ignoring withdrawn types): RP [RFC1183], AFSDDB [RFC1183], RT [RFC1183], SIG [RFC2535], PX [RFC2163], NXT [RFC2535],

SRV [[RFC2052](#)], NAPTR [[RFC2168](#)], KX [[RFC2230](#)]. Some specifications do not mention DNS compression at all, others explicitly suggest it and only in part identify interoperability issues. Only the KX and SRV RR types are safe as their specifications prohibit compression.

The specification of RP, AFSDB, RT, PX, and NAPTR is hereby changed in that domain names in the RDATA section MUST NOT be compressed and MUST NOT be compression targets.

Local compression MUST NOT be used for owner names and it MUST NOT be applied to domain names in RDATA sections of any RR type defined so far.

The specification of future RR types should explicitly select the use of local compression or forbid RDATA domain name compression at all.

## **8. Security Considerations**

The usual caveats for using unauthenticated DNS apply. This scheme is believed not to introduce any new security problems. However, implementors should be aware of problems caused by blindly following compression pointers of any kind. [[RFC1035](#)] and this document limit compression targets to previous occurrences and this MUST be followed in constructing and decoding messages. Otherwise applications might be vulnerable to denial of service attacks launched by sending DNS messages with infinite compression pointer loops. In addition, pointers should be verified to really point to the start of a label (for conventional and local RDATA pointers) and not beyond the end of the domain name (for local owner name pointers).

The maximum length of 255 applies to domain names in uncompressed wire format, so care must be taken during decompression not to exceed this limit to avoid buffer overruns.

## **9. Acknowledgements**

The author would like to thank Andreas Gustafsson, Paul Vixie, Bob Halley, Mark Andrews and Thomas Narten for their review and constructive comments.

## **10. References**

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", [RFC 1034](#), STD 13, November 1987

- [RFC1035] Mockapetris,P., "Domain Names - Implementation and Specification", [RFC 1035](#), STD 13, November 1987
- [RFC1123] Braden,R., "Requirements for Internet Hosts -- Application and Support", [RFC 1123](#), STD 3, October 1989
- [RFC1183] Everhart,C., Mamakos,L., Ullmann,R., Mockapetris,P., "New DNS RR Definitions", [RFC 1183](#), October 1990
- [RFC2052] Gulbrandsen,A., Vixie,P. "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2052](#), October 1996
- [RFC2119] Bradner,S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP 14](#), March 1997
- [RFC2163] Allocchio,C., "Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)", [RFC 2163](#), January 1998
- [RFC2168] Daniel,R., Mealling,M., "Resolution of Uniform Resource Identifiers using the Domain Name System", [RFC 2168](#), June 1997
- [RFC2230] Atkinson,R., "Key Exchange Delegation Record for the DNS", [RFC 2230](#), November 1997
- [RFC2535] Eastlake,D., "Domain Name System Security Extensions", [RFC 2535](#), March 1999
- [RFC2606] Eastlake,D., Panitz,A., "Reserved Top Level DNS Names", [RFC 2606](#), [BCP 32](#), June 1999
- [EDNS0] Vixie,P., "Extension mechanisms for DNS (EDNS0)", [draft-ietf-dnsind-edns0-XX.txt](#), work in progress
- [BINLABELS] Crawford,M., "Binary Labels in the Domain Name System", [draft-ietf-dnsind-binary-labels-XX.txt](#), work in progress

## **11. Author's Address**

Peter Koch  
Universitaet Bielefeld  
Technische Fakultaet  
Postfach 10 01 31  
D-33501 Bielefeld  
Germany



INTERNET-DRAFT

DNS Compression

June 1999

+49 521 106 2902

<pk@TechFak.Uni-Bielefeld.DE>

Koch

Expires December 1999

[Page 9]