WINS Lookup by DNS server (WINS-Lookup)

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.

Abstract

WINS Lookup is a system that provides a limited gateway between the Domain Name System [RFC 1034] and the Windows Internet Name System [WINS]. Using WINS Lookup, a DNS server can resolve A and PTR type queries for names registered exclusively in WINS. This document describes the WINS Lookup system and the format of the WINS and WINSR resource records.
Introduction

The Domain Name System is a distributed hierarchical database of names. A DNS server updates the DNS database and responds to the queries addressed to it. Similar to the DNS server, the Windows Internet Naming Service (WINS) provides support for registering in and querying a database that contains mapping of the NetBIOS names to the IP addresses. WINS protocol is based and fully compatible with the protocols defined for NBNS [NBNS]. WINS Lookup is a system that provides a limited gateway between the Domain Name System and the Windows Internet Name System. Using WINS Lookup, a DNS server can resolve A and PTR type queries for names registered in WINS. This document describes the WINS Lookup system and the format of the WINS and WINSR resource records. WINS lookup allows clients that are DNS-aware but WINS-unaware (hereafter referred to as "DNS-only" clients) to resolve the names of hosts registered with WINS.

Although DNS [RFC 1034] may seem similar to WINS, there are differences between them. The main difference is that DNS has the concept of hierarchy, which allows the administration and replication of the database to be broken up into zones. WINS supports a flat name space, without the concept of hierarchy and requires each WINS server to maintain a complete database of entries through replication.

The DNS and WINS servers provide complementary name resolution services in the mixed environment of the DNS- and WINS-aware clients. WINS-aware (but DNS-unaware) clients (hereafter referred to as "WINS-only" clients) register their names with the WINS servers (not DNS servers). The "DNS-only" clients that need to resolve the names registered only with WINS servers will not be able to find these names in the DNS database. WINS lookup allows these "DNS-only" clients to resolve the names of "WINS-only" clients, by advising the DNS server to submit unresolved queries to WINS servers.

WINS Lookup overview

WINS lookup is enabled for the zones that contain WINS or WINSR records at the root of the zones. Using WINS Lookup, a DNS server can resolve A and PTR type queries for names and IP addresses registered only in WINS, but not in DNS. The following example demonstrates the protocol for the name resolution involving WINS lookup.
Step 1
At bootstrap the "WINS-only" client registers its name to IP address mapping only with WINS server. As an example we assume that the NetBIOS name of the "WINS-only" client is "winsclient" and its IP address 10.1.2.3.

Step 2
The DNS client requires name-to-IP address resolution for the name "winsclient.example.com." and submits a DNS A query to the DNS server authoritative for the zone "example.com." (The diagram is simplified by showing the query directly submitted to the DNS server authoritative for the name "example.com." In general, this query may be recursively sent to multiple DNS servers prior to arriving to the authoritative server, according to the [RFC 1034].)
Step 3
The authoritative DNS server does not contain an A record for the name "winsclient.example.com.". In this case the server checks if it contains WINS resource record for the zone "example.com." (format of the record is described in the following section). If such record does not exist then the DNS server returns "Name Error" (RCODE 3) (hereafter referred to as NXDOMAIN) as described in [RFC 1035] Section 4.1.1. If such record does exist, then the DNS server submits a query for the name "winsclient" to the WINS server, whose IP address is specified in the WINS resource record. If WINS resource record contains more than one IP address, then the queries are submitted one at a time to every IP address in the order specified in the WINS record until the query is resolved. Query is submitted to the next WINS server if the previous queries were not positively resolved or the previous WINS servers did not respond within specific time period.

Step 4
If WINS server contains the queried name, it resolves the query and returns the response to the DNS server.

Step 5
If the query was resolved by a WINS server, the DNS server constructs the response to the original A type query using the response from WINS server and returns it to the client. The TTL value of the constructed record is set to the value specified in the Cache Timeout field of the WINS record. If the WINS servers didn’t positively resolve the query for the name "winsclient", then the DNS server returns NXDOMAIN to the client. In both cases the DNS server caches the response for the time specified in the Cache Timeout field of the WINS record.

If the DNS client sent a non A type query for the "winsclient.example.com.", and the authoritative DNS server does not contain such name it MUST NOT return NXDOMAIN. If the same client cached such negative result and the next moment it needs to resolve A query for the same "winsclient.example.com." name, it would find NXDOMAIN in its cache prior to submitting the A query. The resolver would assume that the name does not exist. As was shown above this is not true, since the WINS contains this name and the authoritative DNS server contains the WINS resource record. There are two ways for a DNS server that implements WINS lookup to handle this situation: First: if a zone contains a WINS record, then before returning NXDOMAIN a DNS server must check the appropriate WINS server(s) to find if such name exists. If it does exist then the DNS server should return a response (hereafter referred to as NODATA) with empty Answer records.
and Authority sections, which indicates that the name exists, but no RRs of the requested type are present. If it does not exist, then DNS server returns NXDOMAIN.

Second: if a zone contains a WINS record, then a DNS server must return NODATA.

The first solution is more strict, but it involves extra querying WINS server every time a DNS server receives a non A type query for non-existing name in the authoritative zone, that contains a WINS record. At the same time, since non A type queries compose only a minor portion of all queries, extra querying WINS servers has no significant impact on performance and network load.

The second solution may be suitable for those implementers who don’t like the idea of extra querying the WINS servers. Returning NODATA instead of NXDOMAIN has no negative effects.

WINS Reverse Lookup
Step 1
In case when the DNS client needs to resolve the PTR query for the 3.2.1.10.in-addr.arpa corresponding to the IP address of the "WINS-only" client, it submits the query to the DNS server. This query is submitted to the authoritative for the name DNS server.

Step 2
Since this IP address belongs to the "WINS-only" client, the authoritative DNS server does not contain the PTR record for the specified name. Instead, if the authoritative zone contains the WINSR resource record (specified below) the DNS server sends to the computer with the IP address 10.1.2.3 a NetBIOS node adapter status [NBNS] query.

Step 3
The computer responds to the DNS server with its NetBIOS name, "winsclient".

Step 4
The DNS server concatenates this NetBIOS name, "winsclient", with the domain name specified in the WINSR resource record, "example.com.", as "winsclient.example.com.", constructs the response to the original PTR query using this concatenated name and sends it back to the client. The TTL value of the constructed record is set to the value specified in the Cache Timeout field of the WINSR record. The DNS server caches the response for the time specified in the Cache Timeout field of the WINSR record.

WINS Resource Record

The WINS record is compatible with Resource Record (RR) format described in [RFC 1034]. The WINS record type is assigned a value of 65281 (TBD). The WINS record has the following components:

- **owner**: is the DNS name of the zone for which the WINS lookup is enabled
- **class**: Standard DNS meaning [RFC 1035]
- **type**: WINS Identifies a WINS Lookup

Expires April 2000
TTL

Standard DNS meaning [RFC 1035]

Flag

32 bit integer that specifies whether the record must be included into the zone replication. It may have only two values: 0x00000000 and 0x00010000 corresponding to the replication and no-replication (local record) flags respectively.

Lookup Timeout

32 bit integer that indicates how long (in seconds) a DNS server, using WINS Lookup, waits for response from a WINS server before the DNS server returns the NXDOMAIN to its client.

Cache Timeout

32 bit integer that indicates how long (in seconds) a DNS server may cache a WINS response and specifies the TTL value of the A record that the DNS server constructs to respond to the client’s A query.

WINS Servers

list of space-separated IP addresses of the WINS servers to be queried by the DNS server

The following line represents the format of the WINS record in the zone database file:

```<domain> [TTL] IN WINS [Flag] L<Lookup Timeout> C<Cache Timeout> <IP address of WINS server>```

Example:

```
example.com. IN WINS LOCAL L5 C3600 10.0.0.1
```

WINS Reverse Lookup Resource Record

The WINSR record type is assigned a value of 65282 (TBD). The format of the WINSR record is similar to the WINS record and has the following components:

owner is the DNS name of the zone for which the WINS reverse lookup is enabled

class Standard DNS meaning [RFC 1035]

type WINSR Identifies a WINS Reverse Lookup
TTL          Standard DNS meaning [RFC 1035]

Flag         32 bit integer that specifies whether the record must be included into the zone replication. It may have only two values: 0x00000000 and 0x00010000 corresponding to the replication and no-replication (local record) flags respectively

Lookup Timeout 32 bit integer that indicates how long (in seconds) a DNS server, using WINS Reverse Lookup, waits for response for the adapter status lookup

Cache Timeout 32 bit integer that indicates how long (in seconds) a DNS server, using WINS Reverse Lookup, may cache the response and specifies the TTL value of the PTR record that the DNS server constructs to respond to the client’s PTR query

Domain Name   domain name to be appended to the NetBIOS names returned in response to the NetBIOS node adapter status lookup

The following line represents the format of the WINSR record in the zone database file:

```
<domain> [<TTL>] IN WINSR [<Flag>] L<Lookup Timeout>
C<Cache Timeout> <domain to append to returned NetBIOS names>
```

Example:

```
0.0.10.in-addr.arpa. IN WINSR L5 C3600 example.com.
```

Special Issues

Flag field in the WINS and WINSR resource records allows disabling replication of these records to the secondary copies of the zones. It could be used in the mixed environment of the DNS servers when some servers do not support WINS and/or WINSR records while others do. Even if all DNS servers in the enterprise support WINS record, this feature could be useful in case if the DNS servers authoritative for the same zone, containing WINS records, are separated by large physical distances. In this situation an administrator may prefer to direct WINS queries to the local WINS servers, rather than one specified in the WINS record on the primary DNS server, and modify/add/delete the WINS records directly on the secondary zones.
Security Consideration

Authors believe that the WINS lookup does not introduce new security problems. The DNS and WINS servers and databases are subjected to the same attacks as without WINS Lookup facility.

Acknowledgements

The authors of this document would like to thank Stuart Kwan for his contribution to this document.

IANA Considerations.

Authors would like to ask the IANA to reserve the mnemonics WINS and WINSR and decimal values 65281 and 65282 for the WINS and WINSR resource records.

References

[NBNS] Â’PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODSÂ¶ RFC 1001, March, 1987;

Author’s Addresses:

James Gilroy                                  Levon Esibov
Microsoft Corporation                         Microsoft Corporation
One Microsoft Way                             One Microsoft Way
Redmond, WA  98052                            Redmond, WA  98052
USA                                           USA
<jamesg@microsoft.com>                        <levone@microsoft.com>