DNS zone transfer

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/DNS_zone_transfer#mw-head)[Jump to search](https://en.wikipedia.org/wiki/DNS_zone_transfer#searchInput)

**DNS zone transfer**, also sometimes known by the inducing DNS query type **AXFR**, is a type of [DNS](https://en.wikipedia.org/wiki/Domain_Name_System) [transaction](https://en.wikipedia.org/wiki/Database_transaction). It is one of the many mechanisms available for administrators to [replicate](https://en.wikipedia.org/wiki/Distributed_database) DNS databases across a set of [DNS servers](https://en.wikipedia.org/wiki/DNS_server).

A zone transfer uses the [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) for transport, and takes the form of a [client–server](https://en.wikipedia.org/wiki/Client%E2%80%93server) transaction. The client requesting a zone transfer may be a secondary server requesting data from a primary server, historically referred to as [*master* and *slave*](https://en.wikipedia.org/wiki/Master/slave_(technology)).[[1]](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_note-1) The portion of the database that is replicated is a [zone](https://en.wikipedia.org/wiki/DNS_zone).



**Contents**

* [1Operation](https://en.wikipedia.org/wiki/DNS_zone_transfer#Operation)
* [2Limitations](https://en.wikipedia.org/wiki/DNS_zone_transfer#Limitations)
* [3Operational problems](https://en.wikipedia.org/wiki/DNS_zone_transfer#Operational_problems)
  + [3.1Serial number changes](https://en.wikipedia.org/wiki/DNS_zone_transfer#Serial_number_changes)
  + [3.2Serial number comparisons](https://en.wikipedia.org/wiki/DNS_zone_transfer#Serial_number_comparisons)
  + [3.3Multiple resource records](https://en.wikipedia.org/wiki/DNS_zone_transfer#Multiple_resource_records)
  + [3.4Exposure of data](https://en.wikipedia.org/wiki/DNS_zone_transfer#Exposure_of_data)
* [4See also](https://en.wikipedia.org/wiki/DNS_zone_transfer#See_also)
* [5References](https://en.wikipedia.org/wiki/DNS_zone_transfer#References)
* [6External links](https://en.wikipedia.org/wiki/DNS_zone_transfer#External_links)
  + [6.1Security standards information](https://en.wikipedia.org/wiki/DNS_zone_transfer#Security_standards_information)
  + [6.2Related Request for Comments](https://en.wikipedia.org/wiki/DNS_zone_transfer#Related_Request_for_Comments)

Operation[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=1)]

Zone transfer consists of a preamble, followed by the actual data transfer. The preamble comprises a lookup of the [Start of Authority](https://en.wikipedia.org/wiki/Start_of_Authority) (SOA) resource record for the "zone apex", the node of the DNS namespace that is at the top of the "zone". The fields of this SOA resource record, in particular the "serial number", determine whether the actual data transfer need to occur at all. The client compares the serial number of the SOA resource record with the serial number in the last copy of that resource record that it has. If the serial number of the record being transferred is greater, the data in the zone are deemed to have "changed" (in some fashion) and the secondary proceeds to request the actual zone data transfer. If the serial numbers are identical, the data in the zone are deemed not to have "changed", and the client may continue to use the copy of the database that it already has, if it has one.

The actual data transfer process begins by the client sending a query (opcode 0) with the special query type AXFR (value 252) over the TCP connection to the server. The server responds with a series of response messages, comprising all of the resource records for every domain name in the "zone". The first response comprises the SOA resource record for the zone apex. The other data follows in no specified order. The end of the data is signaled by the server repeating the response containing the SOA resource record for the zone apex.

Some zone transfer clients perform the SOA lookup of the preamble using their system's normal DNS query resolution mechanism. These clients do not open a TCP connection to the server until they have determined that they need to perform the actual data transfer. However, since TCP can be used for normal DNS transactions, as well as for zone transfer, other zone transfer clients perform the SOA lookup preamble over the same TCP connection as they then (may) perform the actual data transfer. These clients open the TCP connection to the server before they even perform the preamble.

The preceding describes full zone transfer. Incremental zone transfer differs from full zone transfer in the following respects:

* The client uses the special QTYPE IXFR (value 251) instead of the AXFR QTYPE.
* The client sends the SOA resource record for the zone apex that it currently has, if any, in the IXFR message, letting the server know which version of the "zone" it believes to be current.
* Though the server may respond in the normal AXFR manner with the full data for the zone, it may also instead respond with an "incremental" data transfer. This latter comprises the list of changes to the zone data, in zone serial number order, between the version of the zone that the client reported to the server as having and the version of the zone that is current at the server. The changes comprise two lists, one of resource records that are deleted and one of resource records that are inserted. (A modification to a resource record is represented as a deletion followed by an insertion.)

Zone transfer is entirely client-initiated. Though servers can send a NOTIFY message to clients (that they have been informed about) whenever a change to the zone data has been made, the scheduling of zone transfers is entirely under the control of the clients. Clients schedule zone transfers initially, when their databases are empty, and thereafter at regular intervals, in a pattern controlled by the values in the "refresh", "retry", and "expire" fields in the SOA resource record of the zone apex.

Limitations[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=2)]

Though it is standardized, full-zone transfer being described as one of the possible database replication mechanisms in [RFC 1034](https://tools.ietf.org/html/rfc1034) and [RFC 5936](https://tools.ietf.org/html/rfc5936) (incremental zone transfer described in [RFC 1995](https://tools.ietf.org/html/rfc1995)), zone transfer is the most limited of those database replication mechanisms. Zone transfer operates in terms of "[wire format](https://en.wikipedia.org/wiki/Wire_protocol)" resource records, *i.e.* resource records as they are transferred using the DNS protocol. However, the schema of wire format resource records may not be identical to the database schema used by the [back ends](https://en.wikipedia.org/wiki/Back-end_database) of the DNS servers themselves.

Operational problems[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=3)]

**Serial number changes**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=4)]

The preamble portion of zone transfer relies on the serial number, and *only* the serial number, to determine whether a zone's data have changed, and thus whether the actual data transfer is required. For some DNS server packages, the serial numbers of SOA resource records are maintained by administrators by hand. Every edit to the database involves making two changes, one to the record being changed and the other to the zone serial number. The process requires accuracy: the administrator may forget to change the serial number or change it incorrectly (reduce it). [RFC 1912](https://tools.ietf.org/html/rfc1912) (section 2.2 SOA records) recommends using the value YYYYMMDDnn as the number (YYYY=year, MM=month, DD=day, nn=revision number). This won't overflow until the year 4294.

Some DNS server packages have overcome this problem by automatically constructing the serial number from the last modification timestamp of the database file on disk. This is the case for [djbdns](https://en.wikipedia.org/wiki/Djbdns), for example. The operating system ensures that the last modification timestamp is updated whenever an administrator edits the database file, effectively automatically updating the serial number, and thus relieving administrators of the need to make two edits (in two different places) for every single change.

Furthermore, the paradigm of database replication for which the serial number check (and indeed zone transfer itself) is designed, which involves a single central DNS server holding the primary version of the database with all other DNS servers merely holding copies, simply does not match that of many modern DNS server packages. Modern DNS server packages with sophisticated database back ends such as [SQL](https://en.wikipedia.org/wiki/SQL) servers and [Active Directory](https://en.wikipedia.org/wiki/Active_Directory) allow administrators to make updates to the database in multiple places (such systems employ [multi-master replication](https://en.wikipedia.org/wiki/Multi-master_replication)), with the database back end's own replication mechanism handling the replication to all other servers. This paradigm simply does not match that of a single, central, monotonically increasing number to record changes, and thus is incompatible with zone transfer to a large extent. Modern DNS server packages with sophisticated database back ends often will create a "shim" serial number, simulating the existence of a single central place where updates are made, but this is at best imperfect.

Fortunately, for this and several reasons outlined later, DNS servers that use such sophisticated database back ends in general rarely use zone transfer as their database replication mechanism in the first place, and usually instead employ the vastly superior distributed database replication mechanisms that the back ends themselves provide.

**Serial number comparisons**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=5)]

Serial number comparisons are intended to use [Serial Number Arithmetic](https://en.wikipedia.org/wiki/Serial_Number_Arithmetic) as defined in [RFC 1982](https://tools.ietf.org/html/rfc1982). However, this was not clearly specified in [RFC 1034](https://tools.ietf.org/html/rfc1034), resulting in not all clients perform the serial number check, in the preamble, in the same way. Some clients check merely that the serial number supplied by the server is different from that known by the client, or non-zero. Other clients check that the serial number supplied by the server is within a given range of the serial number already known by the client. Yet other clients still perform the latter check and additionally check that the serial number supplied by the server is not zero.

**Multiple resource records**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=6)]

Originally, in the actual data transfer each set of resource records for a single domain name and type was transferred in a separate response message from the server to the client. However, this is inefficient, and some DNS server software implemented optimizations, geared at allowing the response compression mechanism in the DNS protocol to reduce the total bandwidth requirements of data transfers, such as:

* performing "additional section processing" to include any "glue" resource record sets in the same response as an NS, SRV, or MX resource record set
* collecting all of the resource record sets relating to a single domain name together and sending them, if they fit, in a single response

Some clients were written to expect *only* the original response format, and would fail to perform data transfer if such optimizations were employed. Several DNS server packages thus have a configuration setting allowing administrators to specify the use of "single answer format" responses for those clients that require it.

**Exposure of data**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=7)]

The data contained in a DNS zone may be sensitive from an operational security aspect. This is because information such as server hostnames may become public knowledge, which can be used to discover information about an organization and even provide a larger [attack surface](https://en.wikipedia.org/wiki/Attack_surface). In June 2017 the registrar responsible for Russian top-level-domains accidentally enabled DNS zone transfers via AXFR which led to 5.6 million records being accidentally exposed.[[2]](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_note-2)

In 2008 a court in North Dakota, USA, ruled that performing a zone transfer as an unauthorized outsider to obtain information that was not publicly accessible constitutes a violation of North Dakota law.[[3]](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_note-3)

See also[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=8)]

* [List of DNS record types](https://en.wikipedia.org/wiki/List_of_DNS_record_types)

References[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=9)]

* 1. [**^**](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_ref-1) *Fujiwara, Kazunori; Sullivan, Andrew; Hoffman, Paul.*[*"DNS Terminology"*](https://tools.ietf.org/html/rfc8499.html)*. tools.ietf.org. Retrieved 2020-06-21.*
  2. [**^**](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_ref-2) [*"Wrong Bind Configuration Exposes the Complete List of Russian TLD's to the Internet"*](https://securitytrails.com/blog/russian-tlds)*. SecurityTrails Blog. 2018-03-14. Retrieved 2018-04-10.*
  3. [**^**](https://en.wikipedia.org/wiki/DNS_zone_transfer#cite_ref-3) [*"Anti-spammer fined for accessing DNS records of private network"*](http://www.h-online.com/security/news/item/Anti-spammer-fined-for-accessing-DNS-records-of-private-network-735841.html)*. The H. 18 January 2008.*
* [*"How the AXFR protocol works"*](http://cr.yp.to/djbdns/axfr-notes.html)*. Internet publication, D. J. Bernstein. Retrieved February 15, 2005.*
* [*"Understanding zones and zone transfer"*](https://technet.microsoft.com/en-us/library/cc781340(WS.10).aspx)*. Microsoft Windows Server 2003 product documentation. Retrieved 2011-11-27.*
* [*"How DNS Support for Active Directory Works"*](https://technet.microsoft.com/en-us/library/cc759550(WS.10).aspx)*. Microsoft Windows Server 2003 product documentation. Retrieved 2011-11-27.*
* [*"DNS zone replication in Active Directory"*](https://technet.microsoft.com/en-us/library/cc779655(WS.10).aspx)*. Microsoft Windows Server 2003 product documentation. Retrieved 2011-11-27.*
* *McClure, Stuart; Scambray, Joel; Kurtz, George (2009). Hacking Exposed: Network Security Secrets & Solutions (6th ed.). McGraw-Hill.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-07-161374-3*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-07-161374-3)*.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=10)]

**Security standards information**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=11)]

* [CAPEC-291 DNS Zone Transfers](http://capec.mitre.org/data/definitions/291.html)
* [CVE-1999-0532 A DNS server allows zone transfers.](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0532)
* [CWE-16 Configuration](http://cwe.mitre.org/data/definitions/16.html)
* [CWE-276 Incorrect Default permissions](http://cwe.mitre.org/data/definitions/276.html)

**Related Request for Comments**[[edit](https://en.wikipedia.org/w/index.php?title=DNS_zone_transfer&action=edit&section=12)]

* [RFC 5936](https://tools.ietf.org/html/rfc5936) DNS Zone Transfer Protocol (defines AXFR, updates [RFC 1034](https://tools.ietf.org/html/rfc1034) Domain Names - Concepts and Facilities, and [RFC 1035](https://tools.ietf.org/html/rfc1035) Domain Names - Implementation and Specification)
* [RFC 1995](https://tools.ietf.org/html/rfc1995) Incremental Zone Transfer in DNS
* [RFC 1996](https://tools.ietf.org/html/rfc1996) A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
* [draft-ietf-dnsext-axfr-clarify DNS Zone Transfer Protocol (AXFR)](http://tools.ietf.org/html/draft-ietf-dnsext-axfr-clarify) [internet draft](https://en.wikipedia.org/wiki/Internet_draft)