



XROADS NETWORKS

---

Network Appliance How To Guide: DNS Delegation

# How To Guide

## DNS Delegation (The Simple Redundancy Solution)

The key requirement when performing DNS based network redundancy and load balancing is the ability to control the domain information for the servers that require the network continuity service.

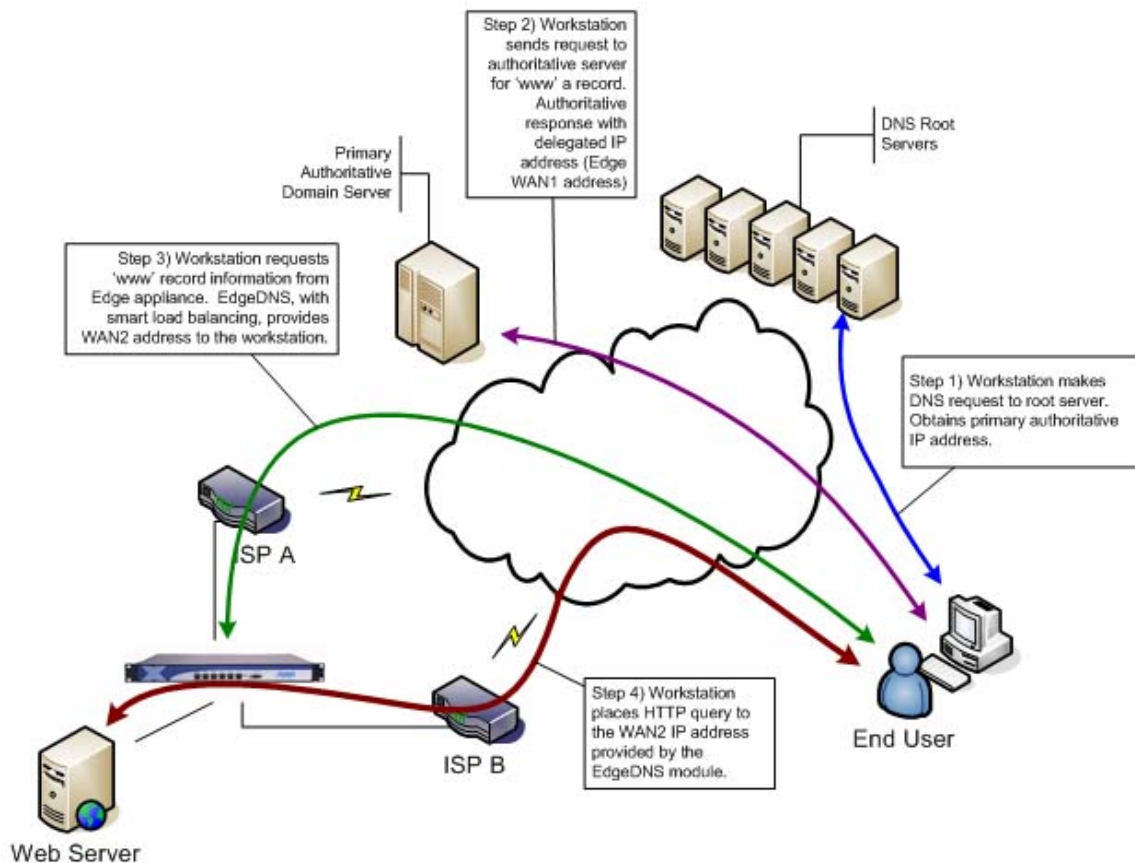
The problem with this key requirement is that many organizations do not wish to transfer their DNS zone information to a single device which could become a single point of failure for their entire domain.

The solution to this problem is called delegation and is essentially the ability to tell the master DNS server that when a specific servers information is requested, forward those requests, and only those requests to an external DNS server for resolution.

The configuration of this delegation process is fairly simple. We have outlined two examples below. One is from a BIND DNS implementation, the other is from Windows XP DNS Server.

### How It Works

The diagram below provides an overview of how DNS delegation works, and show the various steps involved with a workstation requesting delegated DNS record info.



## BIND DNS Example

The BIND DNS server provides a simple method to delegate individual server information via a standard zone file. An example zone file is provided below with the modified server information.

```
@   IN  SOA  abc.com.  hostmaster.abc.com. (
                                1      ; serial
                                3h     ; refresh
                                1h     ; retry
                                1w     ; expire
                                1h )   ; negative caching TTL

    IN  NS   ns1
    IN  NS   ns2

    IN  MX   10  mail

ns1   IN  A   10.10.10.10
ns2   IN  A   10.10.10.20
mail  IN  A   10.20.20.50

### Old Configuration

www   IN  A   10.20.20.50

### Updated Configuration

edge1 IN  A   xxx.xxx.xxx.xxx
edge2 IN  A   yyy.yyy.yyy.yyy
www   IN  NS  edge1.abc.com.
www   IN  NS  edge2.abc.com.
      IN  MX  20 mail2
mail2 IN  A   10.50.50.20
```

Where the xxx.xxx.xxx.xxx and yyy.yyy.yyy.yyy are the actual WAN1 and WAN2 IP addresses of the Edge device which is providing the redundancy services for the “web” server.

Notice for the “mail” server we simply added a secondary “mail2” record, as MX records have a built-in ability to provide load balancing and failover.

## Windows XP DNS Server Example

Windows uses a simple delegation wizard for setting up individual server delegations. This process is provided as a general overview. A more detailed description can be found within the Microsoft documentation.

### Delegating Zones

DNS provides the option of dividing up the namespace into one or more zones, which can then be stored, distributed, and replicated to other DNS servers. When deciding whether to divide your DNS namespace to make additional zones, consider the following reasons to use additional zones:

- A need to delegate management of part of your DNS namespace to another location or department within your organization.
- A need to divide one large zone into smaller zones for distributing traffic loads among multiple servers, improve DNS name resolution performance, or create a more fault-tolerant DNS environment.
- A need to extend the namespace by adding numerous subdomains at once, such as to accommodate the opening of a new branch or site.

If, for any of these reasons, you could benefit from delegating zones, it might make sense to restructure your namespace by adding additional zones. When choosing how to structure zones, you should use a plan that reflects the structure of your organization.

When delegating zones within your namespace, be aware that for each new zone you create, you will need delegation records in other zones that point to the authoritative DNS servers for the new zone. This is necessary both to transfer authority and to provide correct referral to other DNS servers and clients of the new servers being made authoritative for the new zone.

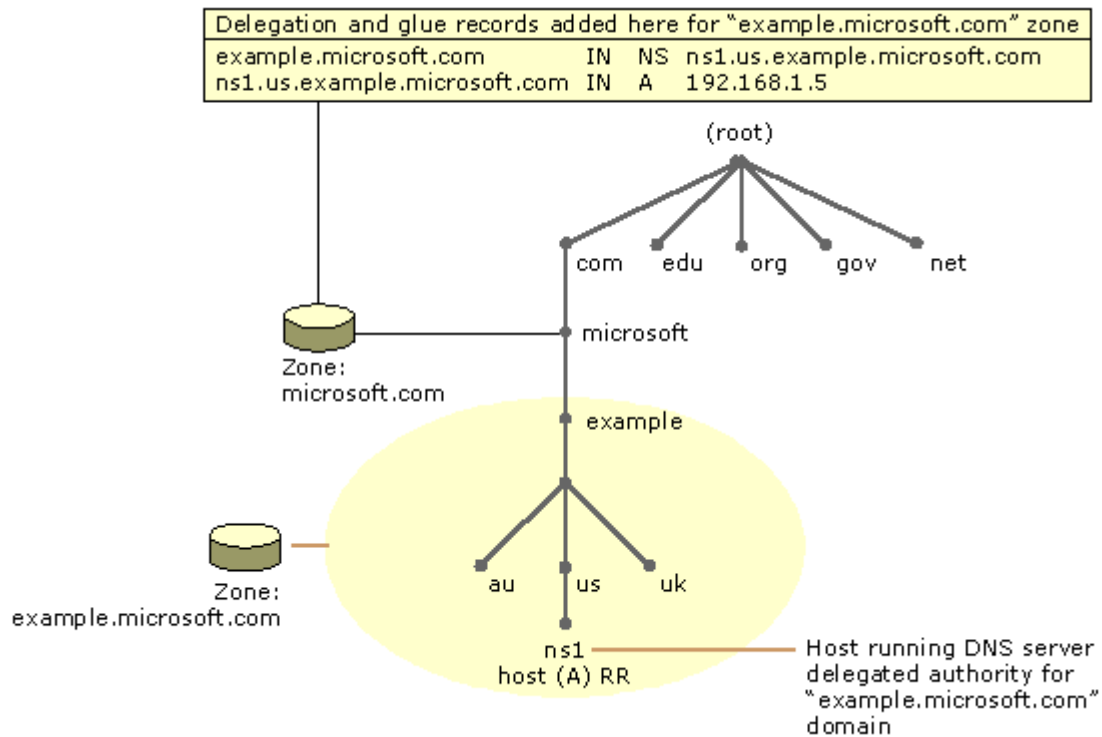
When a standard primary zone is first created, it is stored as a text file containing all resource record information on a single DNS server. This server acts as the primary master for the zone. Zone information can be replicated to other DNS servers to improve fault tolerance and server performance.

When structuring your zones, there are several good reasons to use additional DNS servers for zone replication:

1. Added DNS servers provide zone redundancy, enabling DNS names in the zone to be resolved for clients if a primary server for the zone stops responding.
2. Added DNS servers can be placed so as to reduce DNS network traffic. For example, adding a DNS server to the opposing side of a low-speed WAN link can be useful in managing and reducing network traffic.
3. Additional secondary servers can be used to reduce loads on a primary server for a zone.

Example: Delegating a subdomain to a new zone

As shown in the following graphic, when a new zone for a subdomain (example.microsoft.com) is created, delegation from the parent zone (microsoft.com) is needed.



In this example, an authoritative DNS server computer for the newly delegated example.microsoft.com subdomain is named based on a derivative subdomain included in the new zone (ns1.us.example.microsoft.com). To make this server known to others outside of the new delegated zone, two RRs are needed in the microsoft.com zone to complete delegation to the new zone.

These RRs include:

- An NS RR to effect the delegation. This RR is used to advertise that the server named ns1.us.example.microsoft.com is an authoritative server for the delegated subdomain.
- An A RR (also known as a [glue record](#) ) is needed to resolve the name of the server specified in the NS RR to its IP address. The process of resolving the host name in this RR to the delegated DNS server in the NS RR is sometimes referred to as [glue chasing](#)

## Edge Appliance Configuration (Example)

The process for creating a delegated record within Edge appliance requires the creation of a domain, equal to the delegated URL. If the URL is [www.abc.com](http://www.abc.com), a domain would need to be created with that full URL name as seen below.

The screenshot shows the 'Inbound DNS Resolution' configuration page. On the left is a dark blue sidebar with menu items: 'Inbound DNS Resolution: ?', 'Authoritative Domains: ?', 'Zone Transfer: ?', and 'Domain Parameters: ?'. The main content area has a 'Domain Settings' dropdown menu. Below it is a text input field containing 'www.abc.com' with a help icon and the text '(Enter A Domain Name, Example: abc.com)'. A note below reads: 'NOTE: The root servers must be redirected to the Edge router in order to enable the DNS functionality.' Under 'Zone Transfer', there are radio buttons for 'Enable' and 'Disable' (selected), with the text '(Enable zones transfers for this domain.)'. Under 'Domain Parameters', there are three text input fields: '30' (TTL - The number of seconds that this zone may be cached, '0' means no cache), '30' (Refresh - The number of seconds after which nameservers should check to see if this zone has changed), and '86400' (Expire - If the Edge cannot be reached, all information is invalidated after 'expire' seconds). At the bottom are four buttons: 'Reset', 'Add / Update', 'List Domains', and 'Restart DNS'.

## Creating Global Records

With the domain created, a global 'a' record must be created for the URL. This global record is created by selecting the URL from the domain drop-down and leaving the host name field blank.

Then, select the WAN link to associate (another record would need to be created for WAN2 in this case) and enter the external and internal IP addresses of the server.

The screenshot shows the 'Inbound DNS Resolution' configuration page for creating a record. The sidebar is the same as in the previous screenshot. The main content area has a 'HostRecords' dropdown menu. Below it is a 'Authoritative Domain' dropdown menu containing 'www.abc.com' with the text '(Domain name associated with the host)'. The 'Host Name' field is empty, and the 'Host Name' dropdown is set to 'WAN1' with the text '(Enter host name [example: www] and bound to an interface)'. The 'Host Address / URL' field contains '10.20.20.50' with the text '(Enter an ip address or cname for this host, cname must end with \'.')' and a checkbox for 'OR Click for dynamic WAN addressing'. The 'Internal Address' field contains '192.168.168.50' with the text '(Enter the LAN IP address for this record, 'A' records only)'. The 'Record Type' dropdown is set to 'A' with the text '(Host Type)'. The 'Time-To-Live' field contains '30' with the text '(TTL determines how long this record is cached by DNS clients)'. The 'Load Balancing' field contains '1' with the text '(Used for load balancing server records, lower numbers are provided first more often [1 - 9999])'. Below this are radio buttons for 'Disabled' (selected) and 'Enabled' with the text '(Enables SMART Load Balancing for this DNS entry, only enable for 'A' records)'. At the bottom is a 'Host Status' dropdown menu set to 'ACTIVE' with the text '(Host Status)'. At the very bottom are three buttons: 'Reset', 'Add / Update', and 'View Hosts >>'.

## Confirm Records

Add another global 'a' record for WAN2+ and then confirm that all of the records have been entered correctly list select the 'View Domain' button. The Host Name should start with a '.' period, which designated that this 'a' record is global.

Once the WAN ports have been activated the status for each active port will be set to 'on' or '1'. The load balancing LB will be set to whatever value was given in the 'Load Balancing' field when creating the 'a' record.

www.abc.com.  (Select A Domain)

| Select                | Host Name                                                                                      | Type                                                                                | Address                                                                                       | L.B. | Interface                                                                                | Status | Internal       |
|-----------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------|--------|----------------|
| <input type="radio"/> |  www.abc.com. |  A |  10.20.20.50 |      |  wan1 |        | 192.168.168.50 |
| <input type="radio"/> |  www.abc.com. |  A |  10.50.50.20 |      |  wan2 |        | 192.168.168.20 |

**Notes:**