

Reverse Lookup

Objective:

Converts IP address into Name. This is to verify the authenticity of the sender (server). For example, let us assume a mail server mail.xyz.com wants to send mail. The recipient server can determine whether mail.xyz.com is actually mail.xyz.com (Not anyone else pretending to be mail.xyz.com), by doing a reverse lookup of the sender's IP address. If it matches with the name then the sender is who it claims to be.

How does reverse lookup work:

Reverse lookup is done through the DNS as the normal name to IP address resolution is done with one minor difference. An authoritative reverse resolution can only be done by the DNS, which is registered to be the owner of those IP addresses (Your ISP). Similar to domain registration, the IP addresses are registered by American Registry for Internet Numbers (<http://www.arin.net>). ARIN's database contains information about the owner (company etc.) and the name servers, which will reverse resolve those ranges. The ISP may further delegate a smaller range within its allocated IP addresses to another DNS. The authoritative DNS for an IP range contains an entry for each IP address in the following form:

129.20.113.207.in-addr.arpa PTR node1.jagat.com.

Which means, an address 207.113.20.129 is called node1.jagat.com.

How do I setup my server to reverse resolve:

Determine who owns the IP address you are using

Go to ARIN's website, <http://ws.arin.net/cgi-bin/whois.pl>.

Enter the IP address. For example, for 207.113.20.129 you may get the following output:

```
Search results for: 207.113.20.129

OrgName:      Internet Online Services
OrgID:        IOS
Address:      294 State Street
City:         Hackensack
StateProv:    NJ
PostalCode:   07601
Country:      US

NetRange:     207.113.0.0 - 207.113.127.255
CIDR:         207.113.0.0/17
NetName:      IOSNET-5
NetHandle:    NET-207-113-0-0-1
Parent:       NET-207-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS.IDT.NET
NameServer:   NOC.IOS.COM
NameServer:   AUTH2.NS.IDT.NET
Comment:
RegDate:      1996-05-13
Updated:      1996-06-04

TechHandle:   IOS-NOC-ARIN
TechName:     IDT Corp
TechPhone:    +1-201-928-2889
TechEmail:    domreg@corp.idt.net

# ARIN WHOIS database, last updated 2003-05-05 20:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Use NSLOOKUP to determine whether the owner of the IP address has a PTR entry for your address

```
C:\>nslookup
*** Can't find server name for address 192.168.5.41: Non-existent
domain
Default Server:  cdr-dns.molam.com
Address:  192.168.5.40

> server ns.idt.net
Default Server:  ns.idt.net
Address:  198.4.75.100

> set type=ptr
> 207.113.20.129
Server:  ns.idt.net
```

```
Address: 198.4.75.100
```

```
129.20.113.207.in-addr.arpa name = node1.jagat.com <<<ENTRY EXISTS>>  
20.113.207.in-addr.arpa nameserver = ns.idt.net  
20.113.207.in-addr.arpa nameserver = noc.ios.com  
ns.idt.net internet address = 198.4.75.100  
noc.ios.com internet address = 198.4.75.69  
>
```

The commands are highlighted in bold. If the entry do not exist then the ISP/Owner should provide these entries or delegate to a name server.

Create a name resolution entry for the PTR record

This entry should exist in the DNS of the domain, used in the PTR record. In the example above the PTR record points to node1.jagat.com. The name server for the domain jagat.com should contain an entry for node1.jagat.com to resolve to 207.113.20.129.

Note that it is quite possible the reverse resolution does not involve the domain jagat.com in reverse resolution. It is up to your ISP/Owner of the address to determine how they want to handle the reverse resolution.