

Reverse DNS in IPv6 for Internet Service Providers

Abstract

In IPv4, Internet Service Providers (ISPs) commonly provide IN-ADDR.ARPA information for their customers by prepopulating the zone with one PTR record for every available address. This practice does not scale in IPv6. This document analyzes different approaches and considerations for ISPs in managing the IP6.ARPA zone.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8501>.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Reverse DNS in IPv4	3
1.2.	Reverse DNS Considerations in IPv6	4
2.	Alternatives in IPv6	4
2.1.	Negative Response	4
2.2.	Wildcard Match	5
2.3.	Dynamic DNS	5
2.3.1.	Dynamic DNS from Individual Hosts	6
2.3.2.	Dynamic DNS through Residential Gateways	7
2.3.3.	Automatic DNS Delegations	7
2.3.4.	Generate Dynamic Records	8
2.3.5.	Populate from DHCP Server	8
2.3.6.	Populate from RADIUS Server	8
2.4.	Delegate DNS	9
2.5.	Dynamically Generate PTR When Queried ("On the Fly")	9
3.	Manual User Updates	10
4.	Considerations and Recommendations	10
5.	Security and Privacy Considerations	11
5.1.	Using Reverse DNS for Security	11
5.2.	DNS Security with Dynamic DNS	11
5.3.	Considerations for Other Uses of the DNS	12
5.4.	Privacy Considerations	12
5.5.	User Creativity	12
6.	IANA Considerations	12
7.	References	12
7.1.	Normative References	12
7.2.	Informative References	14
	Acknowledgements	14
	Author's Address	15

1. Introduction

[RFC1912] recommended that "every Internet-reachable host should have a name" and says "Failure to have matching PTR and A records can cause loss of Internet services similar to not being registered in the DNS at all". While the need for a PTR record and for it to match is debatable as a best practice, some network services (see Section 4) still do rely on PTR lookups, and some check the source address of incoming connections and verify that the PTR and A records match before providing service.

Individual Internet users on the residential or consumer scale, including small and home businesses, are constantly connecting to or moving around the Internet. For large ISPs who serve residential users, maintenance of individual PTR records is impractical.

Administrators at ISPs should consider whether customer PTR records are needed, and if so, evaluate methods for responding to reverse DNS queries in IPv6.

1.1. Reverse DNS in IPv4

ISPs that provide access to many residential users typically assign one or a few IPv4 addresses to each of those users and populate an IN-ADDR.ARPA zone with one PTR record for every IPv4 address. Some ISPs also configure forward zones with matching A records so that lookups match. For instance, if an ISP Example.com aggregated 192.0.2.0/24 at a network hub in one region, the reverse zone might look like:

1.2.0.192.IN-ADDR.ARPA. IN PTR 1.string.region.example.com.

2.2.0.192.IN-ADDR.ARPA. IN PTR 2.string.region.example.com.

3.2.0.192.IN-ADDR.ARPA. IN PTR 3.string.region.example.com.

.

.

.

254.2.0.192.IN-ADDR.ARPA. IN PTR 254.string.region.example.com.

The conscientious Example.com might then also have a zone:

1.string.region.example.com. IN A 192.0.2.1

2.string.region.example.com. IN A 192.0.2.2

3.string.region.example.com. IN A 192.0.2.3

.

.

.

254.string.region.example.com. IN A 192.0.2.254

Many ISPs generate PTR records for all IP addresses used for customers, and many create the matching A record.

1.2. Reverse DNS Considerations in IPv6

A sample entry for 2001:0db8:0f00:0000:0012:34ff:fe56:789a might be:

```
a.9.8.7.6.5.e.f.f.f.4.3.2.1.0.0.0.0.0.0.0.f.0.8.b.d.0.1.0.0.2
.IP6.ARPA.  IN PTR 1.string.region.example.com.
```

ISPs will often delegate an IPv6 prefix to their customers. Since 2^{80} possible addresses could be configured in a single /48 zone alone, it is impractical to write a zone with every possible address entered, even with automation. If 1000 entries could be written per second, the zone would still not be complete after 38 trillion years.

Furthermore, it is often impossible to associate hostnames and addresses, since the 64 bits in the Interface Identifier portion of the address are frequently assigned using Stateless Address Autoconfiguration (SLAAC) [RFC4862] when the host comes online, and they may be short-lived.

[RFC1912] is an Informational RFC that says "PTR records must point back to a valid A record" and further that the administrator should "Make sure your PTR and A records match." Herein are considerations for how to follow this advice for AAAA and PTR records.

2. Alternatives in IPv6

Several options exist for providing reverse DNS in IPv6. All of these options also exist for IPv4, but the scaling problem is much less severe in IPv4. Each option should be evaluated for its scaling ability, compliance with existing standards and best practices, and availability in common systems.

2.1. Negative Response

Some ISP DNS administrators may choose to provide only an NXDOMAIN response to PTR queries for subscriber addresses. In some ways, this is the most accurate response, since no name information is known about the host. However, providing a negative response to PTR queries does not satisfy the expectation in [RFC1912] for entries to match. Users of services that are dependent on a successful lookup will have a poor experience. For instance, some web services and Secure Shell (SSH) connections wait for a DNS response, even NXDOMAIN, before responding. For the best user experience, then, it is important to return a response, rather than time out with no answer. On the other hand, external mail servers are likely to reject connections, which might be an advantage in fighting spam.

When evaluating this option, DNS administrators should consider the uses for reverse DNS records and the number of services affecting the number of users.

2.2. Wildcard Match

The use of wildcards in the DNS is described in [RFC4592], and their use in IPv6 reverse DNS is described in [RFC4472].

While recording all possible addresses is not scalable, it may be possible to record a wildcard entry for each prefix assigned to a customer. Consider also that "inclusion of wildcard NS RRSets in a zone is discouraged, but not barred". [RFC4592]

This solution generally scales well. However, since the response will match any address in the wildcard range (/48, /56, /64, etc.), a forward DNS lookup on the response given will not be able to return the same hostname. This method therefore fails the expectation in [RFC1912] that forward and reverse will match. DNSSEC [RFC4035] scalability is limited to signing the wildcard zone, which may be satisfactory.

2.3. Dynamic DNS

One way to ensure that forward and reverse records match is for hosts to update DNS servers dynamically once interface configuration is complete (whether by SLAAC, DHCPv6, or other means), as described in [RFC4472]. Hosts would need to provide both AAAA and PTR updates and would need to know which servers would accept the information.

This option should scale as well or as poorly as IPv4 dynamic DNS (DDNS) does. Dynamic DNS may not scale effectively in large ISP networks that have no single master name server, but a single master server is not best practice. The ISP's DNS system may provide a point for Denial-of-Service attacks, including many attempted DDNS updates. Accepting updates only from authenticated sources may mitigate this risk, but only if authentication itself does not require excessive overhead. No authentication of dynamic DNS updates is inherently provided. Implementers should therefore consider use of TSIG [RFC2845], or at least ingress filtering, so that updates are only accepted from customer address space from internal network interfaces. They should also rate limit the number of updates from a customer per second and consider impacts on scalability. UDP is allowed per [RFC2136], so connection reliability is not assured, though the host should expect an ERROR or NOERROR message from the server; TCP provides transmission control, but the updating host would need to be configured to use TCP.

Administrators may want to consider user creativity if they provide hostnames, as described in Section 5.5, "User Creativity".

There is no assurance of uniqueness if multiple hosts try to update with the same name ("mycomputer.familyname.org"). There is no standard way to indicate to a host what server it should send DDNS updates to; the master listed in the SOA is often assumed to be a DDNS server, but this may not scale.

2.3.1. Dynamic DNS from Individual Hosts

In the simplest case, a residential user will have a single host connected to the ISP. Since the typical residential user cannot configure IPv6 addresses or resolving name servers on their hosts, the ISP should provide address information conventionally -- i.e., using their normal combination of Router Advertisements (RAs), DHCP, etc. The ISP should also provide a DNS Recursive Name Server and Domain Search List as described in [RFC3646] or [RFC8106]. In determining its Fully Qualified Domain Name (FQDN), a host will typically use a domain from the Domain Search List. This is an overloading of the parameter; multiple domains could be listed, since hosts may need to search for unqualified names in multiple domains without necessarily being a member of those domains. Administrators should consider whether the Domain Search List actually provides an appropriate DNS suffix(es) when considering use of this option. For the purposes of dynamic DNS, the host would concatenate its local hostname (e.g., "hostname") plus the domain(s) in the Domain Search List (e.g., "customer.example.com"), as in "hostname.customer.example.com".

Once it learns its address and has a resolving name server, the host must perform an SOA lookup on the IP6.ARPA record to be added in order to find the owner and eventually the server that is authoritative for the zone (which might accept dynamic updates). Several recursive lookups may be required to find the longest prefix that has been delegated. The DNS administrator must designate the Primary Master Server for the longest match required. Once found, the host sends dynamic AAAA and PTR updates using the concatenation defined above ("hostname.customer.example.com").

In order to use this alternative, hosts must be configured to use dynamic DNS. This is not default behavior for many hosts, which is an inhibitor for a large ISP. This option may be scalable, although registration following an outage may cause significant load, and hosts using privacy extensions [RFC4941] may update records daily. It is up to the host to provide matching forward and reverse records and update them when the address changes.

2.3.2. Dynamic DNS through Residential Gateways

Residential customers may have a gateway, which may provide DHCPv6 service to hosts from a delegated prefix. ISPs should provide a DNS Recursive Name Server and Domain Search List to the gateway, as described above and in [RFC3646] and [RFC8106]. There are two options for how the gateway uses this information. The first option is for the gateway to respond to DHCPv6 requests with the same DNS Recursive Name Server and Domain Search List provided by the ISP. The alternate option is for the gateway to relay dynamic DNS updates from hosts to the servers and domain provided by the ISP. Host behavior is unchanged; the host sends the same dynamic updates, either to the ISP's server (as provided by the gateway) or to the gateway for it to forward. The gateway would need to be capable of and configured to use dynamic DNS.

2.3.3. Automatic DNS Delegations

An ISP may delegate authority for a subdomain, such as "customer12345.town.AW.customer.example.com" or "customer12345.example.com", to the customer's gateway. Each domain thus delegated must be unique within the DNS. The ISP may also then delegate the IP6.ARPA zone for the prefix delegated to the customer, as in (for 2001:db8:f00::/48) "0.0.f.0.8.b.d.0.1.0.0.2.IP6.ARPA". Then, the customer could provide updates to their own gateway, with forward and reverse. However, individual hosts connected directly to the ISP rarely have the capability to run DNS for themselves; therefore, an ISP can only delegate to customers with gateways capable of being authoritative name servers. If a device requests a DHCPv6 Prefix Delegation, that may be considered a reasonably reliable indicator that it is a gateway, rather than an individual host. It is not necessarily an indicator that the gateway is capable of providing DNS services and therefore cannot be relied upon as a way to test whether this option is feasible. In fact, this kind of delegation will not work for devices complying with [RFC6092], which includes the requirement, "By DEFAULT, inbound DNS queries received on exterior interfaces MUST NOT be processed by any integrated DNS resolving server".

If the customer's gateway is the name server, it provides its own information to hosts on the network, as described in [RFC2136], which is often done for enterprise networks.

An ISP could provide authoritative responses as a secondary server to the customer's master server. For instance, the home gateway name server could be the master server, with the ISP providing the only published NS authoritative servers.

To implement this alternative, users' residential gateways must be capable of acting as authoritative name servers capable of dynamic DNS updates. There is no mechanism for an ISP to dynamically communicate to a user's equipment that a zone has been delegated, so user action would be required. Most users have neither the equipment nor the expertise to run DNS servers, so this option is unavailable to the residential ISP.

2.3.4. Generate Dynamic Records

An ISP's name server that receives a dynamic forward or reverse DNS update may create a matching entry. Since a host capable of updating one is generally capable of updating the other, this should not be required, but redundant record creation will ensure that a record exists. ISPs implementing this method should check whether a record already exists before accepting or creating updates.

This method is also dependent on hosts being capable of providing dynamic DNS updates, which is not default behavior for many hosts.

2.3.5. Populate from DHCP Server

An ISP's DHCPv6 server may populate the forward and reverse zones when the DHCP request is received if the request contains enough information [RFC4704].

However, this method will only work for a single host address (IA_NA); the ISP's DHCP server would not have enough information to update all records for a prefix delegation. If the zone authority is delegated to a home gateway that used this method, the gateway could update records for residential hosts. To implement this alternative, users' residential gateways would have to support the FQDN DHCP option and would have to either have the zones configured or send DDNS messages to the ISP's name server.

2.3.6. Populate from RADIUS Server

A user may receive an address or prefix from a RADIUS server [RFC2865], the details of which may be recorded via RADIUS Accounting data [RFC2866]. The ISP may populate the forward and reverse zones from the accounting data if it contains enough information. This solution allows the ISP to populate data concerning allocated prefixes as per Section 2.2 (wildcards) and customer premise equipment (CPE) endpoints. However, as with Section 2.3.5, it does not allow the ISP to populate information concerning individual hosts.

2.4. Delegate DNS

For customers who are able to run their own DNS servers, such as commercial customers, often the best option is to delegate the reverse DNS zone to them, as described in [RFC2317] (for IPv4). However, since most residential users have neither the equipment nor the expertise to run DNS servers, this method is unavailable to residential ISPs.

This is a general case of the specific case described in Section 2.3.3. All of the same considerations still apply.

2.5. Dynamically Generate PTR When Queried ("On the Fly")

Common practice in IPv4 is to provide PTR records for all addresses, regardless of whether a host is actually using the address. In IPv6, ISPs may generate PTR records for all IPv6 addresses as the records are requested. Several DNS servers are capable of this.

An ISP using this option should generate a PTR record on demand and cache or prepopulate the forward (AAAA) entry for the duration of the Time to Live of the PTR. Similarly, the ISP would prepopulate the PTR following a AAAA query. To reduce exposure to a Denial-of-Service attack, state or storage should be limited. Alternatively, if an algorithm is used to generate a unique name, it can be employed on the fly in both directions. This option has the advantage of assuring matching forward and reverse entries while being simpler than dynamic DNS. Administrators should consider whether the lack of user-specified hostnames is a drawback. It may be possible to allow user-specified hostnames for some records and generate others on the fly; looking up a record before generating on the fly may slow responses or may not scale well.

DNSSEC [RFC4035] signing records on the fly may increase load; unsigned records can indicate that these records are less trusted, which might be acceptable.

Another consideration is that the algorithm used for generating the record must be the same on all servers for a zone. In other words, any server for the zone must produce the same response for a given query. Administrators managing a variety of rules within a zone might find it difficult to keep those rules synchronized on all servers.

3. Manual User Updates

It is possible to create a user interface, such as a web page, that would allow end users to enter a hostname to associate with an address. Such an interface would need to be authenticated; only the authorized user could add/change/delete entries. If the ISP changes prefixes assigned to customers, the interface would need to specify only the host bits. The backend would therefore need to be integrated with prefix assignments so that when a new prefix was assigned to a customer, the DNS service would look up user-generated hostnames, delete the old record, and create the new one.

Considerations about some records being static and others dynamic or dynamically generated (Section 2.5) and the creativity of users (Section 5.5) still apply.

4. Considerations and Recommendations

There are six common uses for PTR lookups:

Rejecting mail: A PTR with a certain string may indicate "This host is not a mail server", which may be useful for rejecting probable spam. The absence of a PTR leads to the desired behavior.

Serving ads: "This host is probably in town.province." An ISP that does not provide PTR records might affect somebody else's geolocation (also see privacy consideration about location).

Accepting SSH connections: The presence of a PTR may be inferred to mean "This host has an administrator with enough clue to set up forward and reverse DNS". This is a poor inference.

Log files: Many systems will record the PTR of remote hosts in their log files to make it easier when reading logs later to see what network the remote host uses.

Traceroute: The ability to identify an interface and name of any intermediate node or router is important for troubleshooting.

Service discovery: [RFC6763] specifies "DNS-Based Service Discovery", and Section 11 specifically describes how PTRs are used.

As a general guideline, when address assignment and name are under the same authority, or when a host has a static address and name, AAAA and PTR records should exist and match. For residential users, if these use cases are important to the ISP, the administrator will then need to consider how to provide PTR records.

The best accuracy would be achieved if ISPs delegated authority along with address delegation, but residential users rarely have domain names or authoritative name servers.

Dynamic DNS updates can provide accurate data, but there is no standard way to indicate to residential devices where to send updates, whether the hosts support DDNS, or whether it scales.

An ISP has no knowledge of its residential users' hostnames and therefore can either provide a wildcard response or a dynamically generated response. A valid negative response (such as NXDOMAIN) is a valid response if the four cases above are not essential; delegation where no name server exists should be avoided.

5. Security and Privacy Considerations

5.1. Using Reverse DNS for Security

Some people think the existence of reverse DNS records, or matching forward and reverse DNS records, provides useful information about the hosts with those records. For example, one might infer that the administrator of a network with properly configured DNS records was better informed, and by further inference more responsible, than the administrator of a less thoroughly configured network. For instance, most email providers will not accept incoming connections on port 25 unless forward and reverse DNS entries match. If they match, but information higher in the stack (for instance, mail source) is inconsistent, the packet is questionable. However, these records may be easily forged unless DNSSEC or other measures are taken. The string of inferences is questionable and may become unneeded if other means for evaluating trustworthiness (such as positive reputations) become predominant in IPv6.

Providing location information in PTR records is useful for troubleshooting, law enforcement, and geolocation services, but for the same reasons, it can be considered sensitive information.

5.2. DNS Security with Dynamic DNS

The security considerations for using dynamic DNS are described in [RFC3007]. DNS Security Extensions are documented in [RFC4033].

Interactions with DNSSEC are described throughout this document.

5.3. Considerations for Other Uses of the DNS

Several methods exist for providing encryption keys in the DNS. Any of the options presented here may interfere with these key techniques.

5.4. Privacy Considerations

Given the considerations in [RFC8117], hostnames that provide information about a user compromise that user's privacy. Some users may want to identify their hosts using user-specified hostnames, but the default behavior should not be to identify a user, their location, their connectivity, or other information in a PTR record.

5.5. User Creativity

Though not precisely a security consideration, administrators may want to consider what domain will contain the records and who will provide the names. If subscribers provide hostnames, they may provide inappropriate strings. Consider "ihate.example.com" or "badword.customer.example.com" or "celebrityname.committed.illegal.acts.example.com".

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

- [RFC1912] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, DOI 10.17487/RFC1912, February 1996, <<https://www.rfc-editor.org/info/rfc1912>>.
- [RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <<https://www.rfc-editor.org/info/rfc2136>>.
- [RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000, <<https://www.rfc-editor.org/info/rfc2845>>.

- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <<https://www.rfc-editor.org/info/rfc2865>>.
- [RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <<https://www.rfc-editor.org/info/rfc2866>>.
- [RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, DOI 10.17487/RFC3007, November 2000, <<https://www.rfc-editor.org/info/rfc3007>>.
- [RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003, <<https://www.rfc-editor.org/info/rfc3646>>.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <<https://www.rfc-editor.org/info/rfc4033>>.
- [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <<https://www.rfc-editor.org/info/rfc4035>>.
- [RFC4592] Lewis, E., "The Role of Wildcards in the Domain Name System", RFC 4592, DOI 10.17487/RFC4592, July 2006, <<https://www.rfc-editor.org/info/rfc4592>>.
- [RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4704, DOI 10.17487/RFC4704, October 2006, <<https://www.rfc-editor.org/info/rfc4704>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <<https://www.rfc-editor.org/info/rfc4941>>.

- [RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <<https://www.rfc-editor.org/info/rfc6763>>.
- [RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <<https://www.rfc-editor.org/info/rfc8106>>.

7.2. Informative References

- [RFC2317] Eidnes, H., de Groot, G., and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, DOI 10.17487/RFC2317, March 1998, <<https://www.rfc-editor.org/info/rfc2317>>.
- [RFC4472] Durand, A., Ihren, J., and P. Savola, "Operational Considerations and Issues with IPv6 DNS", RFC 4472, DOI 10.17487/RFC4472, April 2006, <<https://www.rfc-editor.org/info/rfc4472>>.
- [RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011, <<https://www.rfc-editor.org/info/rfc6092>>.
- [RFC8117] Huitema, C., Thaler, D., and R. Winter, "Current Hostname Practice Considered Harmful", RFC 8117, DOI 10.17487/RFC8117, March 2017, <<https://www.rfc-editor.org/info/rfc8117>>.

Acknowledgements

The author would like to thank Alain Durand, JINMEI Tatuya, David Freedman, Andrew Sullivan, Chris Griffiths, Darryl Tanner, Ed Lewis, John Brzozowski, Chris Donley, Wes George, Jason Weil, John Spence, Ted Lemon, Stephan Lagerholm, Steinar Haug, Mark Andrews, Chris Roosenraad, Fernando Gont, John Levine, and many others who discussed and provided suggestions for this document.

Author's Address

**Lee Howard
Retevia
Fairfax, VA 22032
United States of America

Email: lee.howard@retevia.net**