TECHNICAL SERVICE BULLETIN (TSB)

Troubleshooting DNS Issues

ComSifter®
protect web users now!

TSB Date: January 28, 2013

IN THIS DOCUMENT

Comsift's Technical Support team receives many incident reports that culminate in discovering an issue with DNS. In the course of discussing these issues with the local network administrator, we discover that there are many misconceptions about how DNS should be configured in a network. This case study will explain some DNS fundamentals and how the ComSifter DNS should be configured.

OVERVIEW

DNS (Domain Name System) is a standard that allows Internet connected devices (humans, computers, routers, etc.) to use a human friendly nomenclature to access web services such as web sites and email. If DNS had not been created, we would all be speaking in the confusing terms of IP. Imagine that if you wanted to visit the Comsift web site; instead of entering comsift.com you would have to enter `206.188.192.7`Or, if you wanted to check your Gmail account you would have to remember `74.125.224.5`DNS removes this requirement by making the associations of human names with their IP names automatically.

HOW IT WORKS

Many technical explanations are available that explain in detail how DNS works, which are beyond the scope of this document. Rather, we will focus on how DNS affects the typical school and small business network.

1. In the simplest network, a single computer is connected to a cable/DSL modem that is connected to the Internet.
2. When the computer is turned on the DHCP client on the computer asks the network if there is a DHCP server.
3. The cable/DSL modem, running a DHCP server service, responds to the request and assigns the computer parameters that the computer must have to connect to the Internet.

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Atheros AR9285 Wireless Network Adapter
   Physical Address. . . . . . . . . : 00-26-4D-F2-C0-63
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, April 06, 2011 7:24:32 AM
   Lease Expires . . . . . . . . . . : Tuesday, April 12, 2011 2:17:49 AM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DNS Servers . . . . . . . . . . . : 192.168.10.5
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

The results of an `ipconfig/all` (via the Microsoft Windows command line) shows that a DHCP server located at `192.168.10.1` assigned the computer an IP of 192.168.10.200, a Subnet Mask of `255.255.255.0`, a Default Gateway of `192.168.10.1`, and most important for our discussion—a DNS server at `192.168.10.5`.

4. The computer now has enough information to connect to the Internet.
5. The user opens a browser and enters `comsift.com`. The browser then asks the operating system (OS) to lookup `comsift.com`.

CONTINUED

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com

6. The OS first looks in its internal DNS cache to see if it has a current entry (this is very fast, only requiring 1/1000th of a second). If not, it then looks in the internal Host file to see if there is a matching entry (less than a 1/100th of a second). If not, the OS then makes a DNS request over Port 53 to the DNS server defined in step 3 (1/100th to 1/50th of a second). The DNS server looks up the DNS name in its database and returns the associated IP. The OS then returns the IP to the Browser. The browser then makes a request to the Internet using the real IP of `comsift.com` and the Comsift home page appears in the browser. All of this happens in 1–2 seconds.

Let's now expand the network from a single computer to many computers connected by a local area network (LAN). In this scenario, instead of a computer directly connected to the Cable/DSL modem—a router is connected to the modem—a distribution switch is the connected to the router-and many computers are connected the switch.

DNS works exactly the same in this scenario. The router may be configured to perform DHCP services instead of the Cable/DNS modem. The big difference-instead of one computer making a DNS request, many computers will be making requests.

Note: Beware of consumer-grade (home) routers in large networks (20 or more computers). A router's main function is to route traffic. If it is busy doing this task, and is then asked to forward DNS requests—it may result in a slowdown on the network.

HOW DOES THE COMSIFTER FIT INTO THIS PICTURE?

The ComSifter is no different than any other device on the network. It needs to know the IP of a requested web page. The ComSifter must also request a DNS lookup. This lookup is separate from the lookup described above. When the ComSifter does a lookup it uses the DNS server that was configured when the ComSifter's network settings were configured.

BEST PRACTICES

In general, there are two types of networks. Networks that are part of a domain, and those that are not.

Non-domain network (networks without a server)
Non-domain networks are best served using the DNS settings given by the Internet Service Provider (ISP). You may be tempted to use your router for DNS, or even the ComSifter—but both of these are DNS forwarders. They will forward the DNS request to the next DNS server—and this adds a small amount of delay to the lookup. A worst-case scenario would be the client computer asking the ComSifter for DNS, the ComSifter asking the router for DNS, the router then asks the ISP for DNS.

It is better to use the ISP's DNS for all lookups.

Note: Beware of using third-party DNS servers that are not provided by your ISP (such as Google, Verizon, etc.). Typically, your ISP will have DNS servers physically located close to your network. When you use other DNS servers, you do not know where they are located, which can add a large amount of delay to each lookup.

Note: Beware of free content-filtering DNS services. As with the third-party servers described above, it is unknown as to where the servers are physically located and large delays can be added to lookups. Many free DNS content-filtering services do not offer much in the way of administrative control or advanced abilities to filter content.

Note: Do not use a third-party "filtering service" for the ComSifter's DNS settings. The ComSifter must have a non-filtered DNS to operate properly.

CONTINUED

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com

Note: Comsift ships all ComSifter models with a default DNS setting of `4.2.2.1` (Verizon). This allows a ComSifter to be plugged in and successfully connect to the Internet before you have configured it to your network. You should change this as soon as possible to your ISP's DNS server or your domain's DNS server.

Domain Networks (networks with a server)
Domains are specialized networks and are typically under the control of a server called a Domain Controller (DC). In the case of a Microsoft Windows DCs, a requirement for the proper operation of the domain is for all client computers to use the domain controller for DNS.

Note: It is a best practice for the ComSifter to also use the DC for DNS.

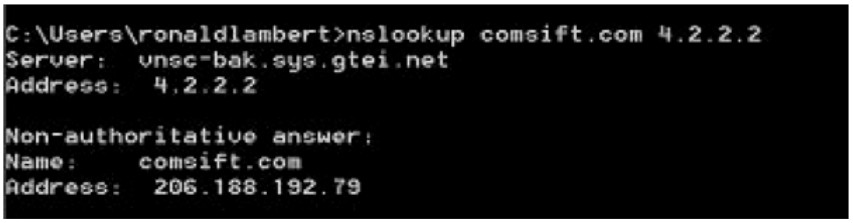
Microsoft has an excellent best practices paper at the following location: `http://support.microsoft.com/kb/825036`

All Networks
Learn to use DNS tools. All recent Microsoft OS offerings include `nslookup` from the command line `(Start > Run > cmd)`.

A simple `nslookup` will use the client computer DNS settings as shown below:

In this example, we see a query for `comsift.com` resulted in our default DNS server (`192.168.10.5`) responding with a lookup (`206.188.192.79`).

If the query fails, try using an alternate DNS server as shown below:



In this example, we queried `4.2.2.2` for a lookup for `comsift.com`. We did not use our default DNS server.
Using the above two tests we can quickly determine if our primary DNS is failing—if the first test failed, but the second test passed, then we can conclude that something is wrong with our DNS server.

Find out how fast your DNS server responds. The faster the DNS server responds to a lookup, the faster a user will see the requested web page.

In general, a properly operating DNS system will respond as follows:
- A LAN-based DNS server (such as a domain controller DNS server) will respond in 1-5 milliseconds (ms).
- An ISP-based DNS server will respond in 30-50ms.

CONTINUED

Gibson Research offers a free DNS speed test that may be downloaded at: `http://www.grc.com/dns/benchmark.htm`. This tool will test the speed of all your configured DNS servers and compare them with other well-known DNS servers.

LEARN THE FEEL OF A SLOW DNS SERVER

Although many network issues may cause delays or slowdowns, there are some symptoms that point to DNS.

Go to a fast-loading web site such as `google.com`. This site should load within 1–3 seconds. If the site takes 6–12 seconds to load, you may be experiencing a DNS timeout. It takes six (6) seconds for a primary DNS server to timeout and, depending on the OS, it may try twice before moving to the secondary DNS server.

WHAT IS COMSIFT smartDNS?

All ComSifter models include smartDNS—a feature that insures your ComSifter uses the fastest available (configured) DNS server.

When configuring the ComSifter, you are given the opportunity to define two (2) or more DNS servers that the ComSifter will use. Typically, a primary and a secondary are defined. Every 15 minutes the ComSifter runs a series of tests to determine the response time of each of the DNS servers. If the secondary DNS server is faster by more than 200ms, a flag is set. If the same condition continues for 45 minutes (3 tests), the ComSifter will switch DNS servers, using the secondary as the primary. This ensures that the ComSifter is using the fastest DNS server available. The switch will also provide a message to any defined email recipients `(Maintenance > Utilities > Email Notification Parameters > Email address of second recipient)`.