Your IP: **217.120.90.198** ASN: **9143** [AtHome-Benelux-BV (----------)] Near: Netherlands

Tools

DNSreport for twswireless.com

Generated by www.DNSreport.com **at 20:38:05 GMT on 21 Jan 2008.**

Email link to results

Category	Status	Test Name	Information
Parent	PASS	Missing Direct Parent check	OK. Your direct parent zone exists, which is good. Some domains (usually third or fourth level domains, such as example.co.us) do not have a direct parent zone ('co.us' in this example), which is legal but can cause confusion.

	INFO	NS records at parent servers	Your NS records at the parent servers are:
			`ns1.smallbizconcepts.nl. [80.69.65.224 (NO GLUE)] [NL]`
			`ns2.smallbizconcepts.nl. [84.244.144.194 (NO GLUE)] [NL]`
			[These were obtained from k.gtld-servers.net]

	PASS	Parent nameservers have your nameservers listed	OK. When someone uses DNS to look up your domain, the first step (if it doesn't already know about your domain) is to go to the parent servers. If you aren't listed there, you can't be found. But you are listed there.
	WARN	Glue at parent nameservers	WARNING. The parent servers (I checked with k.gtld-servers.net.) are not providing glue for all your nameservers. This means that they are supplying the NS records (host.example.com), but not supplying the A records (192.0.2.53), which can cause slightly slower connections, and may cause incompatibilities with some non-RFC-compliant programs. This is perfectly acceptable behavior per the RFCs. This will usually occur if your DNS servers are not in the same TLD as your domain (for example, a DNS server of "ns1.example.**org**" for the domain "example.**com**"). In this case, you can speed up the connections slightly by having NS records that are in the same TLD as your domain.
	PASS	DNS servers have A records	OK. All your DNS servers either have A records at the zone parent servers, or do not need them (if the DNS servers are on other TLDs). A records are required for your hostnames to ensure that other DNS servers can reach your DNS servers. Note that there will be problems if your DNS servers do not have these same A records.

NS	INFO	NS records at your nameservers	Your NS records at your nameservers are:
			`ns2.networkconcepts.nl. [84.244.144.194] [TTL=85147]`
			`ns1.networkconcepts.nl. [80.69.65.224] [TTL=85147]`

	PASS	Open DNS servers	OK. Your DNS servers do not announce that they are open DNS servers. Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances that of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack (so it is good that your DNS servers do not appear to be open DNS servers).
	PASS	Mismatched glue	OK. The DNS report did not detect any discrepancies between the glue provided by the parent servers and that provided by your authoritative DNS servers.
	PASS	No NS A records at nameservers	OK. Your nameservers do include corresponding A records when asked for your NS records. This ensures that your DNS servers know the A records corresponding to all your NS records.
	WARN	All nameservers report identical NS records	WARNING: Your nameservers report somewhat different answers for your NS records (varying TTL, for example).
	PASS	All nameservers respond	OK. All of your nameservers listed at the parent nameservers responded.
	PASS	Nameserver name validity	OK. All of the NS records that your nameservers report seem valid (no IPs or partial domain names).
	PASS	Number of nameservers	OK. You have 2 nameservers. You must have at least 2 nameservers (RFC2182 section 5 recommends at least 3 nameservers), and preferably no more than 7.
	FAIL	**Lame nameservers**	ERROR: You have one or more lame nameservers. These are nameservers that do NOT answer authoritatively for your domain. This is bad; for example, these nameservers may never get updated. The following nameservers are lame: 84.244.144.194

	FAIL	**Missing (stealth) nameservers**	FAIL: You have one or more missing (stealth) nameservers. The following nameserver(s) are listed (at your nameservers) as nameservers for your domain, but are not listed at the parent nameservers (therefore, they may or may not get used, depending on whether your DNS servers return them in the authority section for other requests, per RFC2181 5.4.1). You need to make sure that these stealth nameservers are working; if they are not responding, you may have serious problems! The DNSreport will not query these servers, so you need to be very careful that they are working properly.
			`ns2.networkconcepts.nl.`
			`ns1.networkconcepts.nl.`
			This is listed as an ERROR because there are some cases where nasty problems can occur (if the TTLs vary from the NS records at the root servers and the NS records point to your own domain, for example).

	FAIL	**Missing nameservers 2**	ERROR: One or more of the nameservers listed at the parent servers are not listed as NS records at your nameservers. The problem NS records are: ns1.smallbizconcepts.nl. ns2.smallbizconcepts.nl.
	PASS	No CNAMEs for domain	OK. There are no CNAMEs for twswireless.com. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.

	PASS	No NSs with CNAMEs	OK. There are no CNAMEs for your NS records. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
	WARN	Nameservers on separate class C's	WARNING: We cannot test to see if your nameservers are all on the same Class C (technically, /24) range, because the root servers are not sending glue. We plan to add such a test later, but today you will have to manually check to make sure that they are on separate Class C ranges. Your nameservers should be at geographically dispersed locations. You should not have all of your nameservers at the same location. RFC2182 3.1 goes into more detail about secondary nameserver location.
	PASS	All NS IPs public	OK. All of your NS records appear to use public IPs. If there were any private IPs, they would not be reachable, causing DNS delays.
	WARN	TCP Allowed	WARNING: One or more of your DNS servers does not accept TCP connections. Although rarely used, TCP connections are occasionally used instead of UDP connections. When firewalls block the TCP DNS connections, it can cause hard-to-diagnose problems. The problem servers are: `80.69.65.224: Error [No response to TCP packets]. 84.244.144.194: Error [No response to TCP packets].`
	INFO	Nameservers versions	[For security reasons, this test is limited to members]
	FAIL	**Stealth NS record leakage**	Your DNS servers leak stealth information in non-NS requests: Stealth nameservers are leaked [ns1.networkconcepts.nl.]! Stealth nameservers are leaked [ns2.networkconcepts.nl.]! This can cause some serious problems (especially if there is a TTL discrepancy). If you must have stealth NS records (NS records listed at the authoritative DNS servers, but not the parent DNS servers), you should make sure that your DNS server does not leak the stealth NS records in response to other queries.

SOA	INFO	SOA record	Your SOA record [TTL=86400] is:
			
			`Primary nameserver: ns1.networkconcepts.nl.`
			`Hostmaster E-mail address: hostmaster.networkconcepts.nl.`
			`Serial #: 801212103`
			`Refresh: 14400`
			`Retry: 3600`
			`Expire: 604800`
			`Default TTL: 86400`

	PASS	NS agreement on SOA Serial #	OK. All your nameservers agree that your SOA serial number is 801212103. That means that all your nameservers are using the same data (unless you have different sets of data with the same serial number, which would be very bad)! Note that the DNSreport only checks the NS records listed at the parent servers (not any stealth servers).
	WARN	SOA MNAME Check	WARNING: Your SOA (Start of Authority) record states that your **master** (primary) name server is: **ns1.networkconcepts.nl.**. However, that server is not listed at the parent servers as one of your NS records! This is legal, but you should be sure that you know what you are doing.
	PASS	SOA RNAME Check	OK. Your SOA (Start of Authority) record states that your DNS contact E-mail address is: **hostmaster@networkconcepts.nl.** (techie note: we have changed the initial '.' to an '@' for display purposes).
	WARN	SOA Serial Number	WARNING: Your SOA serial number is: **801212103**. That is OK, but the recommended format (per RFC1912 2.2) is YYYYMMDDnn, where 'nn' is the revision. For example, if you are making the 3rd change on 02 May 2006, you would use 2006050203. This number **must** be incremented every time you make a DNS change.
	PASS	SOA REFRESH value	OK. Your SOA REFRESH interval is : **14400 seconds**. This seems normal (about 3600-7200 seconds is good if not using DNS NOTIFY; RFC1912 2.2 recommends a value between 1200 to 43200 seconds (20 minutes to 12 hours)). This value determines how often secondary/slave nameservers check with the master for updates.
	PASS	SOA RETRY value	OK. Your SOA RETRY interval is : **3600 seconds**. This seems normal (about 120-7200 seconds is good). The retry value is the amount of time your secondary/slave nameservers will wait to contact the master nameserver again if the last attempt failed.
	PASS	SOA EXPIRE value	OK. Your SOA EXPIRE time: **604800 seconds**. This seems normal (about 1209600 to 2419200 seconds (2-4 weeks) is good). RFC1912 suggests 2-4 weeks. This is how long a secondary/slave nameserver will wait before considering its DNS data stale if it can't reach the primary nameserver.
	PASS	SOA MINIMUM TTL value	OK. Your SOA MINIMUM TTL is: **86400 seconds**. This seems normal (about 3,600 to 86400 seconds or 1-24 hours is good). RFC2308 suggests a value of 1-3 hours. This value used to determine the default (technically, minimum) TTL (time-to-live) for DNS entries, but now is used for negative caching.

MX	INFO	MX Record	Your 3 MX records are:
			
			`30 mx143.emailfiltering.com. [TTL=7200] IP=195.2.244.43 [TTL=531] [GB]`
			`10 mx141.emailfiltering.com. [TTL=7200] IP=194.116.198.81 [TTL=617] [GB]`
			`20 mx142.emailfiltering.com. [TTL=7200] IP=194.116.199.81 [TTL=531] [GB]`

	PASS	Low port test	OK. Our local DNS server that uses a low port number can get your MX record. Some DNS servers are behind firewalls that block low port numbers. This does not guarantee that your DNS server does not block low ports (this specific lookup must be cached), but is a good indication that it does not.
	PASS	Invalid characters	OK. All of your MX records appear to use valid hostnames, without any invalid characters.
	PASS	All MX IPs public	OK. All of your MX records appear to use public IPs. If there were any private IPs, they would not be reachable, causing slight mail delays, extra resource usage, and possibly bounced mail.
	PASS	MX records are not CNAMEs	OK. Looking up your MX record did not just return a CNAME. If an MX record query returns a CNAME, extra processing is required, and some mail servers may not be able to handle it.
	PASS	MX A lookups have no CNAMEs	OK. There appear to be no CNAMEs returned for A records lookups from your MX records (CNAMEs are prohibited in MX records, according to RFC974, RFC1034 3.6.2, RFC1912 2.4, and RFC2181 10.3).
	PASS	MX is host name, not IP	OK. All of your MX records are host names (as opposed to IP addresses, which are not allowed in MX records).
	PASS	Multiple MX records	OK. You have multiple MX records. This means that if one is down or unreachable, the other(s) will be able to accept mail for you.
	PASS	Differing MX-A records	OK. I did not detect differing IPs for your MX records (this would happen if your DNS servers return different IPs than the DNS servers that are authoritative for the hostname in your MX records).
	PASS	Duplicate MX records	OK. You do not have any duplicate MX records (pointing to the same IP). Although technically valid, duplicate MX records can cause a lot of confusion, and waste resources.

	PASS	Reverse DNS entries for MX records	OK. The IPs of all of your mail server(s) have reverse DNS (PTR) entries. RFC1912 2.1 says you should have a reverse DNS for all your mail servers. It is strongly urged that you have them, as many mailservers will not accept mail from mailservers with no reverse DNS entry. Note that this information is *cached*, so if you changed it recently, it will not be reflected here (see the www.DNSstuff.com Reverse DNS Tool for the current data). The reverse DNS entries are: 43.244.2.195.in-addr.arpa **aix-mta-14.emailfiltering.com.** [TTL=1200] 81.198.116.194.in-addr.arpa **gse-mta-14-rx.emailfiltering.com.** [TTL=1200] 81.199.116.194.in-addr.arpa **thb-mta-14-rx.emailfiltering.com.** [TTL=1200]
Mail	WARN	Connect to mail servers	WARNING: I could not complete a connection to 66% of your mailservers. This could lead to a performance issue in your reception of mail: mx141.emailfiltering.com: The mailserver terminated the connection before the transaction was complete (state 6). This is not RFC compliant, and therefore either due to an error, or it may be the result of a non-RFC-compliant mailserver or non-RFC-compliant anti-spam program. mx142.emailfiltering.com: The mailserver terminated the connection before the transaction was complete (state 6). This is not RFC compliant, and therefore either due to an error, or it may be the result of a non-RFC-compliant mailserver or non-RFC-compliant anti-spam program.
	WARN	Mail server host name in greeting	WARNING: One or more of your mailservers is claiming to be a host other than what it really is (the SMTP greeting should be a 3-digit code, followed by a space or a dash, then the host name). If your mailserver sends out E-mail using this domain in its EHLO or HELO, your E-mail might get blocked by anti-spam software. This is also a technical violation of RFC821 4.3 (and RFC2821 4.3.1). Note that the hostname given in the SMTP greeting should have an A record pointing back to the same server. Note that this one test may use a cached DNS record. mx141.emailfiltering.com claims to be host thb-mta-14.emailfiltering.com [but that host is at 194.116.199.81 (may be cached), not 194.116.198.81]. mx142.emailfiltering.com claims to be host gse-mta-14.emailfiltering.com [but that host is at 194.116.198.81 (may be cached), not 194.116.199.81].
	PASS	Acceptance of NULL <> sender	OK: All of your mailservers accept mail from "<>". You are required (RFC1123 5.2.9) to receive this type of mail (which includes reject/bounce messages and return receipts).
	WARN	Acceptance of postmaster address	WARNING: One or more of your mailservers may not accept mail to postmaster@twswireless.com (it is generating a temporary error). Mailservers are required (RFC822 6.3, RFC1123 5.2.7, and RFC2821 4.5.1) to accept mail to postmaster. mx143.emailfiltering.com's postmaster response: >>> RCPT TO:<postmaster@twswireless.com> <<< 550 Relaying not permitted (3.7): postmaster@twswireless.com mx141.emailfiltering.com's postmaster response: >>> RCPT TO:<postmaster@twswireless.com> <<< 421 <postmaster@twswireless.com>: Deferring connection mx142.emailfiltering.com's postmaster response: >>> RCPT TO:<postmaster@twswireless.com> <<< 421 <postmaster@twswireless.com>: Deferring connection
	WARN	Acceptance of abuse address	WARNING: One or more of your mailservers does not accept mail to abuse@twswireless.com. Mailservers are expected by RFC2142 to accept mail to abuse. mx143.emailfiltering.com's abuse response: >>> RCPT TO:<abuse@twswireless.com> <<< 550 Relaying not permitted (3.7): abuse@twswireless.com
	INFO	Acceptance of domain literals	WARNING: One or more of your mailservers does not accept mail in the domain literal format (user@[0.0.0.0]). Mailservers are technically required RFC1123 5.2.17 to accept mail to domain literals for any of its IP addresses. Not accepting domain literals can make it more difficult to test your mailserver, and can prevent you from receiving E-mail from people reporting problems with your mailserver. However, it is unlikely that any problems will occur if the domain literals are not accepted (mailservers at many common large domains have this problem). mx143.emailfiltering.com's postmaster@[195.2.244.43] response: >>> RCPT TO:<postmaster@[195.2.244.43]> <<< 550 Relaying not permitted (3.7): postmaster@[195.2.244.43]
	PASS	Open relay test	OK: All of your mailservers appear to be closed to relaying. This is *not* a thorough check, you can get a thorough one here. mx143.emailfiltering.com OK: 550 Relaying not permitted (3.7): Not.abuse.see.www.DNSreport.com.from.IP.217.120.90.198@DNSreport.com
	WARN	SPF record	Your domain does not have an SPF record. This means that spammers can easily send out E-mail that looks like it came from your domain, which can make your domain look bad (if the recipient thinks you really sent it), and can cost you money (when people complain to you, rather than the spammer). You may want to add an SPF record ASAP, as 01 Oct 2004 was the target date for domains to have SPF records in place (Hotmail, for example, started checking SPF records on 01 Oct 2004).
WWW	INFO	WWW Record	Your www.twswireless.com A record is: www.twswireless.com. A 213.239.186.204 [TTL=7200] [NL]
	PASS	All WWW IPs public	OK. All of your WWW IPs appear to be public IPs. If there were any private IPs, they would not be reachable, causing problems reaching your web site.
	PASS	CNAME Lookup	OK. Some domains have a CNAME record for their WWW server that requires an extra DNS lookup, which slightly delays the initial access to the website and use extra bandwidth. There are no CNAMEs for www.twswireless.com, which is good.
	INFO	Domain A Lookup	Your twswireless.com A record is: twswireless.com. A 213.239.186.204 [TTL=5947]

Legend:

- UPDATE NOTICE November 2007:
  We have made the decision to remove the Single Point of Failure test included in DNSreport. This test was developed and enhanced over the past five years along with our other tools. The initial design of the Single Point of Failure test depended on the typical connectivity profiles prevalent at the time. As connectivity has become more robust the methodology employed makes less sense and creates more false positives. Our development team is working on an enhanced Single Point of Failure test for a future release.
- Rows with a FAIL indicate a problem that in most cases really should be fixed.
- Rows with a WARN indicate a possible minor problem, which often is not worth pursuing.
- Note that all information is accessed in real-time (except where noted), so this is the freshest information about your domain.
- Note that *automated usage* is not tolerated without the purchase of an Automated Usage plan; please only view the DNS report directly with your web browser.

Emai
link t
resul