UAT for DNS

for

DNS and NTP Modernization project for ROBI

Submitted By

BDCOM Online Limited

Document Version: [1.0]

Date: [04/08/2014]

UAT FOR DNS

The Domain Name System (**DNS**) is a standard technology for managing the names of Web sites and other Internet domains. DNS is an Internet service that translates domain names into IP addresses. Because domain names (example - robi.com.bd) are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.robi.com.bd might translate to 202.134.12.106.

Reverse DNS lookup (also known as rDNS) is a process to determine the hostname associated with a given IP address.Typically, the DNS is used to determine what IP address is associated with a given hostname; so to reverse resolve a known IP address is to lookup what the associated hostname for it. A reverse lookup is often referred to simply as reverse resolving, or more specifically reverse DNS lookups. The most common uses of the reverse DNS are:

1. Anti-spam
2. Network troubleshooting
3. Avoid spammers and phishers using a forward confirmed reverse DNS etc

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

There are various ways to do the testing DNS server resolution. The total procedure given below:

Objective	**Forward Traffic Test**:host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of its command line arguments and options.
Test Procedure	**host -vt any robi.com.bd ns1.robi.com.bd**
Sample Output	Trying "robi.com.bd" Using domain server: Name: ns1.robi.com.bd Address: 202.134.13.4#53 Aliases: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8162 ;; flags: qr aa rd; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 4 ;; QUESTION SECTION:

	;robi.com.bd. IN ANY ;; ANSWER SECTION: robi.com.bd. 86400 IN SOA ns1.aktel.com. hostmaster.robi.com.bd. 2014270701 10800 3600 604800 10800 robi.com.bd. 86400 IN TXT "v=spf1 mx ip4:202.134.12.68 ip4:202.134.12.69 mx:mail.robi.com.bd mx:mail.messaging.microsoft.com ~all mx:include:spf.protection.outlook.com ~all" robi.com.bd. 86400 IN MX 0 robi-com-bd.mail.protection.outlook.com. robi.com.bd. 86400 IN MX 10 mail.robi.com.bd. robi.com.bd. 86400 IN MX 20 ms14373886.msv1.invalid.outlook.com. robi.com.bd. 86400 IN A 202.134.12.106 robi.com.bd. 86400 IN NS ns2.aktel.com. robi.com.bd. 86400 IN NS ns4.robibazar.com. robi.com.bd. 86400 IN NS ns1.aktel.com. ;; ADDITIONAL SECTION: mail.robi.com.bd. 86400 IN A 202.134.12.68 mail.robi.com.bd. 86400 IN A 202.134.12.69 ns1.aktel.com. 14400 IN A 202.134.13.4 ns2.aktel.com. 86400 IN A 202.134.12.13 **Received 500 bytes from 202.134.13.4#53 in 182 ms**
Original Output	root@dns0:~# host -vt any google.com Trying "google.com" ;; Truncated, retrying in TCP mode. Trying "google.com" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29965 ;; flags: qr rd ra; QUERY: 1, ANSWER: 28, AUTHORITY: 4, ADDITIONAL: 4 ;; QUESTION SECTION: ;google.com. IN ANY ;; ANSWER SECTION: google.com. 86399 IN SOA ns1.google.com. dns-admin.google.com. 2014021800 7200 1800 1209600 300 google.com. 3599 IN TXT "v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all" google.com. 599 IN MX 50 alt4.aspmx.l.google.com. google.com. 599 IN MX 10 aspmx.l.google.com. google.com. 599 IN MX 20 alt1.aspmx.l.google.com. google.com. 599 IN MX 30 alt2.aspmx.l.google.com. google.com. 599 IN MX 40 alt3.aspmx.l.google.com. google.com. 86399 IN TYPE257 \# 19 0005697373756573796D616E7465632E636F6D google.com. 299 IN A 114.130.6.53

	google.com. 299 IN A 114.130.6.57 google.com. 299 IN A 114.130.6.59 google.com. 102185 IN NS ns3.google.com. google.com. 102185 IN NS ns2.google.com. google.com. 102185 IN NS ns4.google.com. google.com. 102185 IN NS ns1.google.com. ;; AUTHORITY SECTION: google.com. 102185 IN NS ns1.google.com. google.com. 102185 IN NS ns4.google.com. google.com. 102185 IN NS ns3.google.com. google.com. 102185 IN NS ns2.google.com. ;; ADDITIONAL SECTION: ns1.google.com. 274986 IN A 216.239.32.10 ns2.google.com. 274985 IN A 216.239.34.10 ns3.google.com. 274986 IN A 216.239.36.10 ns4.google.com. 274986 IN A 216.239.38.10 **Received 749 bytes from 10.101.11.23#53 in 1 ms**
Result	pass
Remarks	Query From DNS1.
Signature BDCOM	
Signature ROBI	

Objective	**Forward Traffic Test** :To perform a reverse lookup
Test Procedure	**host -vt ptr 202.134.13.4 ns2.robi.com.bd**
Sample Output	Trying "4.13.134.202.in-addr.arpa" Using domain server: Name: ns2.robi.com.bd Address: 202.134.12.13#53 Aliases: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51419 ;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3 ;; QUESTION SECTION: ;4.13.134.202.in-addr.arpa. IN PTR

	;; ANSWER SECTION: 4.13.134.202.in-addr.arpa. 86400 IN PTR ns1.aktel.com. 4.13.134.202.in-addr.arpa. 86400 IN PTR ns1.aktelbd.com. ;; AUTHORITY SECTION: 13.134.202.in-addr.arpa. 86400 IN NS ns3.aktel.com. 13.134.202.in-addr.arpa. 86400 IN NS ns1.aktel.com. 13.134.202.in-addr.arpa. 86400 IN NS ns2.aktel.com. ;; ADDITIONAL SECTION: ns1.aktel.com. 14400 IN A 202.134.13.4 ns2.aktel.com. 86400 IN A 202.134.12.13 ns3.aktel.com. 86400 IN A 202.134.13.2 **Received 194 bytes from 202.134.12.13#53 in 182 ms**
Original Output	root@dns0:~# host -vt ptr 216.239.38.10 Trying "10.38.239.216.in-addr.arpa" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20501 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4 ;; QUESTION SECTION: ;10.38.239.216.in-addr.arpa. IN PTR ;; ANSWER SECTION: 10.38.239.216.in-addr.arpa. 86400 IN PTR ns4.google.com. ;; AUTHORITY SECTION: 38.239.216.in-addr.arpa. 86400 IN NS ns4.google.com. 38.239.216.in-addr.arpa. 86400 IN NS ns2.google.com. 38.239.216.in-addr.arpa. 86400 IN NS ns3.google.com. 38.239.216.in-addr.arpa. 86400 IN NS ns1.google.com. ;; ADDITIONAL SECTION: ns1.google.com. 274789 IN A 216.239.32.10 ns2.google.com. 274788 IN A 216.239.34.10 ns3.google.com. 274789 IN A 216.239.36.10 ns4.google.com. 274789 IN A 216.239.38.10 **Received 204 bytes from 10.101.11.23#53 in 719 ms**
Result	pass
Remarks	Query From DNS1.
Signature BDCOM	
Signature ROBI	

Objective	**Forward Traffic Test** :Nslookup is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain
Test Procedure	**nslookup** **> server ns1.robi.com.bd** **Default server: ns1.robi.com.bd** **Address: 202.134.13.4#53** **> set type=any** **> robi.com.bd**
Sample Output	Server: ns1.robi.com.bd Address: 202.134.13.4#53 robi.com.bd origin = ns1.aktel.com mail addr = hostmaster.robi.com.bd serial = 2014270701 refresh = 10800 retry = 3600 expire = 604800 minimum = 10800 robi.com.bd text = "v=spf1 mx ip4:202.134.12.68 ip4:202.134.12.69 mx:mail.robi.com.bd mx:mail.messaging.microsoft.com ~all mx:include:spf.protection.outlook.com ~all" robi.com.bd mail exchanger = 0 robi-com-bd.mail.protection.outlook.com. robi.com.bd mail exchanger = 10 mail.robi.com.bd. robi.com.bd mail exchanger = 20 ms14373886.msv1.invalid.outlook.com. Name: robi.com.bd Address: 202.134.12.106 robi.com.bd nameserver = ns4.robibazar.com. robi.com.bd nameserver = ns1.aktel.com. robi.com.bd nameserver = ns2.aktel.com.
Original Output	root@dns0:~# nslookup Internal Query > server dns0.robi.com.bd Default server: dns0.robi.com.bd Address: 10.101.11.22#53 > set type=any > robi.com.bd Server: dns0.robi.com.bd Address: 10.101.11.22#53 robi.com.bd text = "v=spf1 mx ip4:202.134.12.68 ip4:202.134.12.69 mx:mail.robi.com.bd mx:mail.messaging.microsoft.com ~all

	mx:include:spf.protection.outlook .com ~all" robi.com.bd mail exchanger = 0 robi-com-bd.mail.protection.outlook.com. robi.com.bd mail exchanger = 10 mail.robi.com.bd. robi.com.bd mail exchanger = 20 ms14373886.msv1.invalid.outlook.com. Name: robi.com.bd Address: 202.134.12.106 robi.com.bd origin = dns0.robi.com.bd mail addr = root.robi.com.bd serial = 6 refresh = 3600 retry = 1800 expire = 2419200 minimum = 3600 robi.com.bd nameserver = dns0.robi.com.bd. robi.com.bd nameserver = dns2.robi.com.bd. robi.com.bd nameserver = dns1.robi.com.bd. robi.com.bd nameserver = dns3.robi.com.bd. Out world Query : root@dns0:~# nslookup > server 10.101.11.22 Default server: 10.101.11.22 Address: 10.101.11.22#53 > set type=any > www.google.com ;; connection timed out; no servers could be reached >
Result	pass
Remarks	Master DNS cannot query outer world in our project requirements.
Signature BDCOM	
Signature ROBI	

Objective	**Forward Traffic Test** :To perform a reverse lookup
Test Procedure	**nslookup** **> server 202.134.13.4** **Default server: 202.134.13.4** **Address: 202.134.13.4#53** **> set type=any** **> 202.134.12.13**
Sample Output	Server: 202.134.13.4 Address: 202.134.13.4#53

	13.12.134.202.in-addr.arpa name = ns2.aktel.com. 13.12.134.202.in-addr.arpa name = ns2.aktelbd.com.
Original Output	root@dns0:~# nslookup > server 10.101.11.22 Default server: 10.101.11.22 Address: 10.101.11.22#53 > set type=any > 98.139.183.24 ;; connection timed out; no servers could be reached
Result	pass
Remarks	Master DNS cannot query outer world in our project requirements.
Signature BDCOM	
Signature ROBI	

Objective	**Forward Traffic Test** :dig (*domain information groper*) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.
Test Procedure	**dig robi.com.bd**
Sample Output	; <<>> DiG 9.7.3 <<>> robi.com.bd ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53635 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3 ;; QUESTION SECTION: ;robi.com.bd. IN A ;; ANSWER SECTION: robi.com.bd. 83897 IN A 202.134.12.106 ;; AUTHORITY SECTION: robi.com.bd. 76885 IN NS ns1.aktel.com. robi.com.bd. 76885 IN NS ns2.aktel.com. robi.com.bd. 76885 IN NS ns4.robibazar.com. ;; ADDITIONAL SECTION: ns1.aktel.com. 4885 IN A 202.134.13.4 ns2.aktel.com. 76885 IN A 202.134.12.13

	ns4.robibazar.com. 77012 IN A 202.134.12.97 ;; Query time: 0 msec ;; SERVER: 210.4.77.180#53(210.4.77.180) ;; WHEN: Sun Aug 3 13:12:11 2014 ;; MSG SIZE rcvd: 166
Original Output	> ^Croot@dns0:~# dig prothom-alo.com ; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> prothom-alo.com ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9651 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3 ;; QUESTION SECTION: ;prothom-alo.com. IN A ;; ANSWER SECTION: prothom-alo.com. 3600 IN A 199.83.134.216 prothom-alo.com. 3600 IN A 199.83.135.155 ;; AUTHORITY SECTION: prothom-alo.com. 3600 IN NS dns2.bdcom.com. prothom-alo.com. 3600 IN NS dns1.bdcom.com. prothom-alo.com. 3600 IN NS ns.prothom-alo.com. ;; ADDITIONAL SECTION: ns.prothom-alo.com. 172799 IN A 174.122.238.194 dns1.bdcom.com. 172799 IN A 210.4.77.180 dns2.bdcom.com. 172799 IN A 210.4.77.181 ;; Query time: 617 msec ;; **SERVER: 10.101.11.23#53(10.101.11.23)** ;; WHEN: Thu Sep 11 11:41:14 2014 ;; MSG SIZE rcvd: 174
Result	pass
Remarks	Query From DNS1.
Signature BDCOM	
Signature ROBI	

Objective	**Forward Traffic Test** :Dns trace report
Test Procedure	**dig +trace robi.com.bd**
Sample Output	; <<>> DiG 9.7.3 <<>> +trace robi.com.bd ;; global options: +cmd

	. 508806 IN NS l.root-servers.net. . 508806 IN NS m.root-servers.net. . 508806 IN NS i.root-servers.net. . 508806 IN NS g.root-servers.net. . 508806 IN NS c.root-servers.net. . 508806 IN NS j.root-servers.net. . 508806 IN NS d.root-servers.net. . 508806 IN NS f.root-servers.net. . 508806 IN NS h.root-servers.net. . 508806 IN NS b.root-servers.net. . 508806 IN NS e.root-servers.net. . 508806 IN NS k.root-servers.net. . 508806 IN NS a.root-servers.net. ;; Received 496 bytes from 210.4.77.180#53(210.4.77.180) in 0 ms bd. 172800 IN NS surma.btcl.net.bd. bd. 172800 IN NS jamuna.btcl.net.bd. bd. 172800 IN NS dns.bd. ;; Received 145 bytes from 2001:7fe::53#53(i.root-servers.net) in 217 ms robi.com.bd. 86400 IN NS ns2.aktel.com. robi.com.bd. 86400 IN NS ns1.aktel.com. ;; Received 106 bytes from 203.112.194.231#53(jamuna.btcl.net.bd) in 1 ms robi.com.bd. 86400 IN NS ns1.aktel.com. robi.com.bd. 86400 IN NS ns2.aktel.com. robi.com.bd. 86400 IN NS ns4.robibazar.com. ;; Received 166 bytes from 202.134.13.4#53(ns1.aktel.com) in 207 ms
Original Output	root@dns0:~# dig +trace protho-alo.com ; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> +trace protho-alo.com ;; global options: +cmd . 3600000 IN NS I.ROOT-SERVERS.NET. . 3600000 IN NS H.ROOT-SERVERS.NET. . 3600000 IN NS C.ROOT-SERVERS.NET. . 3600000 IN NS E.ROOT-SERVERS.NET. . 3600000 IN NS L.ROOT-SERVERS.NET. . 3600000 IN NS B.ROOT-SERVERS.NET. . 3600000 IN NS F.ROOT-SERVERS.NET. . 3600000 IN NS D.ROOT-SERVERS.NET. . 3600000 IN NS K.ROOT-SERVERS.NET. . 3600000 IN NS M.ROOT-SERVERS.NET. . 3600000 IN NS G.ROOT-SERVERS.NET. . 3600000 IN NS A.ROOT-SERVERS.NET. . 3600000 IN NS J.ROOT-SERVERS.NET. ;; Received 228 bytes from 10.101.11.22#53(10.101.11.22) in 65262 ms

	com. 172800 IN NS c.gtld-servers.net. com. 172800 IN NS k.gtld-servers.net. com. 172800 IN NS h.gtld-servers.net. com. 172800 IN NS d.gtld-servers.net. com. 172800 IN NS a.gtld-servers.net. com. 172800 IN NS i.gtld-servers.net. com. 172800 IN NS b.gtld-servers.net. com. 172800 IN NS m.gtld-servers.net. com. 172800 IN NS g.gtld-servers.net. com. 172800 IN NS l.gtld-servers.net. com. 172800 IN NS f.gtld-servers.net. com. 172800 IN NS j.gtld-servers.net. com. 172800 IN NS e.gtld-servers.net. ;; Received 504 bytes from 192.5.5.241#53(192.5.5.241) in 67767 ms protho-alo.com. 172800 IN NS dns10.parkpage.foundationapi.com. protho-alo.com. 172800 IN NS dns11.parkpage.foundationapi.com. ;; Received 127 bytes from 192.48.79.30#53(192.48.79.30) in 11190 ms protho-alo.com. 300 IN A 209.99.40.222 ;; Received 48 bytes from 199.79.61.222#53(199.79.61.222) in 307 ms
Result	pass
Remarks	
Signature BDCOM	
Signature ROBI	

Objective	**IPV6 Compatibility Test** :
Test Procedure	vim /var/lib/named/etc/bind/named.conf.options
Sample Output	//acl "loopback_v6" { // listen-on-v6 { 2403:4000:0:2::3; ::1; }; // "robi_v6"; // "loopback_v6"; }; max-cache-size 30M; query-source address * port 53; query-source-v6 address * port 53;
Original Output	acl "loopback" {

	127.0.0.1;
	};
	//acl "loopback_v6" {
	// ::1;
	//};
	
	options {
	directory "/var/cache/bind";
	
	// If there is a firewall between you and nameservers you want
	// to talk to, you may need to fix the firewall to allow multiple
	// ports to talk. See http://www.kb.cert.org/vuls/id/800113
	
	// If your ISP provided one or more IP addresses for stable
	// nameservers, you probably want to use them as forwarders.
	// Uncomment the following block, and insert the addresses replacing
	// the all-0's placeholder.
	
	// forwarders {
	// 0.0.0.0;
	// };
	
	allow-transfer { 10.101.11.23; 10.101.11.24; 10.16.49.58; 192.168.80.30;
	192.168.90.4; 202.134.12.13; 202.134.13.4; };
	datasize 100M;
	dump-file "named_dump.db";
	interface-interval 0;
	listen-on { 10.101.11.22; 127.0.0.1; };
	// listen-on-v6 { 2403:4000:0:2::3; ::1; };
	allow-recursion {
	"robi_private";
	"robi_public";
	// "robi_v6";
	// "other_ROBI";
	"loopback";
	// "loopback_v6";
	};
	max-cache-size 30M;
	query-source address * port 53;
	query-source-v6 address * port 53;
	statistics-file "named.stats";
	version "This is not the port you're looking for.";
	zone-statistics yes;

Result	passed
Remarks	
Signature BDCOM	
Signature ROBI	