

DNSSEC Technology Experiment Report

Verification of Functionality and Performance

Japan Registry Services Co., Ltd.

<http://jprs.co.jp/>

2010-09-06 Ver. 1.0

(2011-11-28 English Translation)

Note about this translation

This English translation is provided only for reference. The original version of this document was written in Japanese and is available from following URI:

<<http://jprs.jp/dnssec/doc/DNSSEC-testbed-report-fpv1.0.pdf>>

Acknowledgement

This translation is contributed by [APNIC \(Asia Pacific Network Information Centre\)](#). We would like to express our sincere thanks to APNIC.

Table of Contents

- SUMMARY OF THE DNSSEC TECHNOLOGY EXPERIMENT..... 4**
- DNSSEC TECHNOLOGY EXPERIMENTAL ENVIRONMENT..... 5**
 - PSEUDO DNS TREE..... 5
 - EXPERIMENTAL METHODOLOGY..... 6
- RESULTS OF FUNCTIONALITY VERIFICATION 7**
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 1 7
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 2 9
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 3 10
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 4 12
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 5 18
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 6 34
 - VERIFICATION OF FUNCTIONALITY: CASE STUDY 7 39
- RESULTS OF PERFORMANCE VERIFICATION..... 41**
 - PERFORMANCE VERIFICATION: CASE STUDY 1 41
 - PERFORMANCE VERIFICATION: CASE STUDY 2 44
 - PERFORMANCE VERIFICATION: CASE STUDY 3 47
 - PERFORMANCE VERIFICATION: CASE STUDY 4 50
 - PERFORMANCE VERIFICATION: CASE STUDY 5 54
 - PERFORMANCE VERIFICATION: CASE STUDY 6 57

Summary of the DNSSEC Technology Experiment

When DNSSEC is deployed, digital signatures (hereinafter referred to as “signatures”) are added to DNS data. Computation cost will increase as users of DNS data have to validate signatures. Furthermore, with the addition of signatures, the size of DNS packets, which used to be restricted to a maximum size of 512 bytes for DNS, increases when combined with EDNS0. Since the size of DNS packets could exceed a regular MTU size of 1,500 bytes, depending on conditions, IP fragments need to be considered.

Such increases in DNS packet size will directly lead to an increase in DNS traffic and it will also impact DNS cache. Network devices used for the DNS packet communication could also be impacted.

Deployment of DNSSEC in a .JP zone is likely to impact not only .JP but also a suite of DNS servers linked to a root DNS server, cache DNS server, etc. as well as network access devices. In order to verify this impact beforehand to enable a smooth DNSSEC deployment, we set up an experimental environment and conducted an experiment.

Through this experiment, we obtained findings with regard to the impact on cache DNS server, authoritative DNS server, network access devices, etc. as a result of the deployment of DNSSEC.

Prior to the experiment, JPRS prepared the following two procedure manuals with the aim of verifying various behaviors which are required in order to provide DNSSEC services on each DNS server without any issues.

“DNSSEC Verification of Functionality: Procedure Manual” (Japanese only)

“DNSSEC Performance Verification: Procedure Manual” (Japanese only)

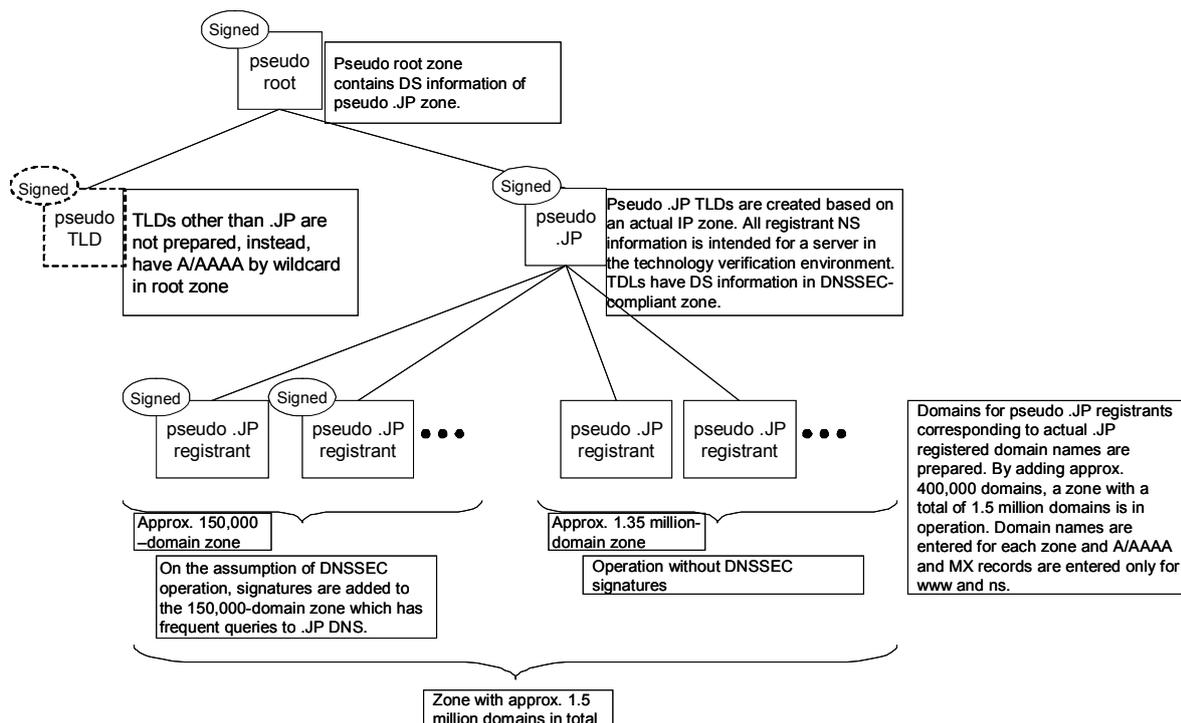
Please refer to these procedure manuals because some parts of the technical experiment were conducted in accordance with the verification procedures specified in these manuals. The manuals can be obtained from the following URL.

DNSSEC Related Information <<http://jprs.jp/dnssec/>>

DNSSEC Technology Experimental Environment

Pseudo DNS Tree

JPRS created a pseudo DNS tree as shown below based on the actual .JP domain name as an environment for the DNSSEC technology experiment.



In order to make a comparison of the environment with and without DNSSEC, JPRS also created a pseudo tree without a domain name signature in a .JP zone (the same as an ordinary DNS tree), which is not shown in the above diagram. In addition, JPRS set up a cache DNS server linked to the pseudo DNS tree.

Experimental Methodology

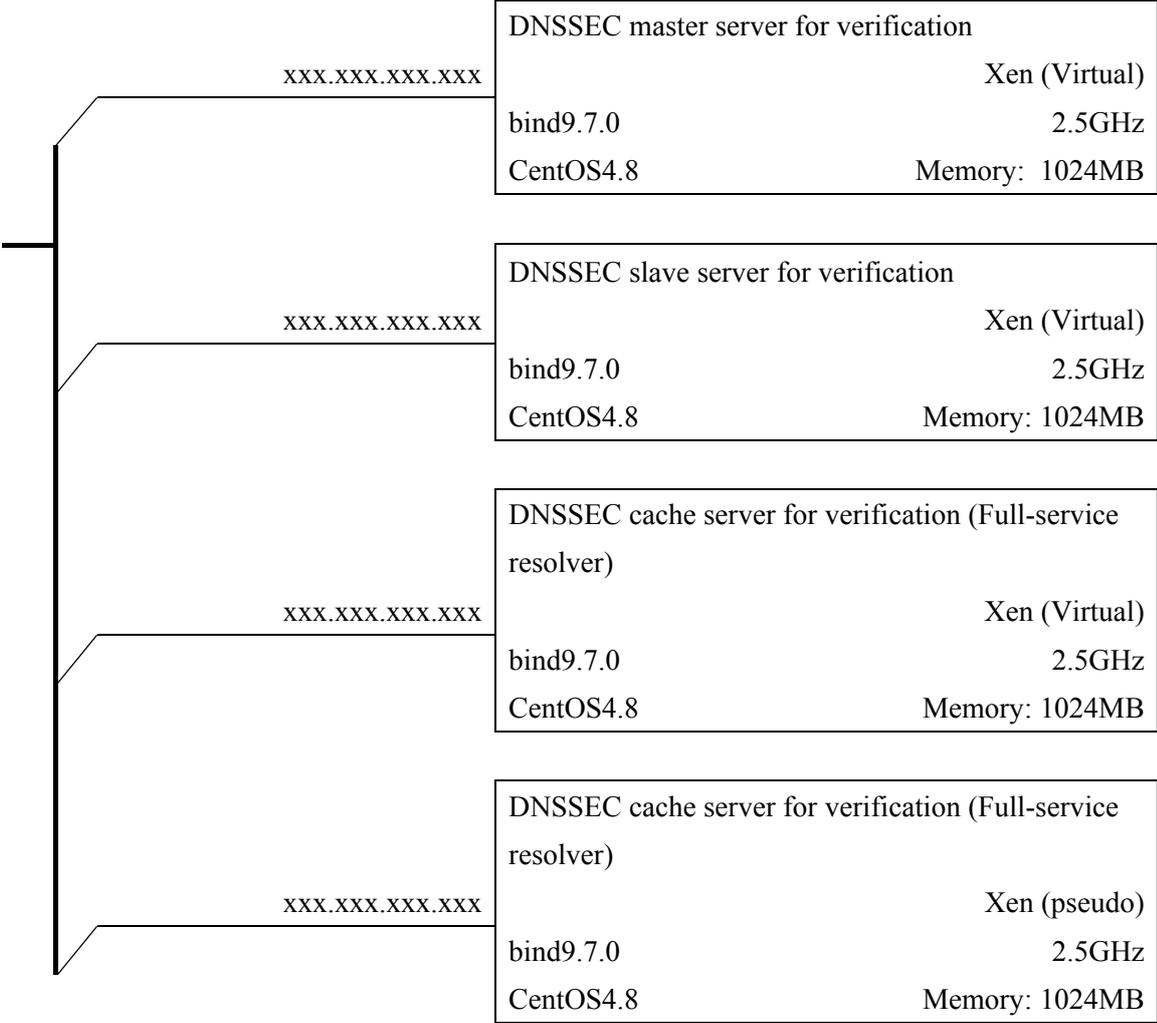
For the experiment of the cache DNS server, experiment participants used an experimental cache DNS server linked to the pseudo tree connected to the Internet, generated DNS queries by using a load generator and measured the load on the cache DNS server (response performance, CPU occupancy rate, memory usage, in/out packet size, etc.) in order to monitor changes as a result of the deployment of DNSSEC.

For the experiment of hardware devices, experiment participants used experimental devices connected to the Internet, sent and received DNS queries through the devices, and verified whether DNSSEC-compliant packets could be sent and received normally.

Results of Functionality Verification

Verification of Functionality: Case Study 1

■ Case Study 1: Experimental Environment



■ Case Study 1: Summary of Experimental Results

Verification of functionality was conducted mostly in accordance with the scenario.
 No particular issues were identified.

■ Case Study 1: Detailed Experimental Results

Although evaluation of functionality could not be conducted for the experiment with IPv6 because the experimental environment was not ready, other evaluations were conducted mostly in accordance with the scenario. No particular issues were identified.

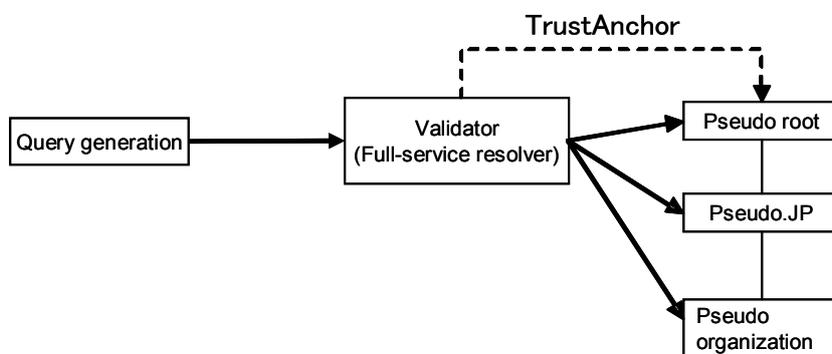
■ Case Study 1: Obtained Findings

- NSEC3 was used. The zone file size of a ZSK (1,024 bits in length) becomes approximately ten times larger when a signature is added.
- In actual operations, it is necessary to prepare a manual to address issues surrounding DNSSEC.

Verification of Functionality: Case Study 2

■ Case Study 2: Experimental Environment

Server configuration	Application
Pseudo root	BIND9.7.1-P2
Pseudo IP	queryperf (modified version)
Pseudo organization	resperf
Validator	
Query generation	



■ Case Study 2: Summary of Experimental Results

Resources changed as follows when signatures were added.

CPU usage rate:	Approx. twice as much
Memory usage:	Approx. three times as much
Network band width (query):	Approx. twice as much
Network band width (reply):	Approx. four times as much

■ Case Study 2: Obtained Findings

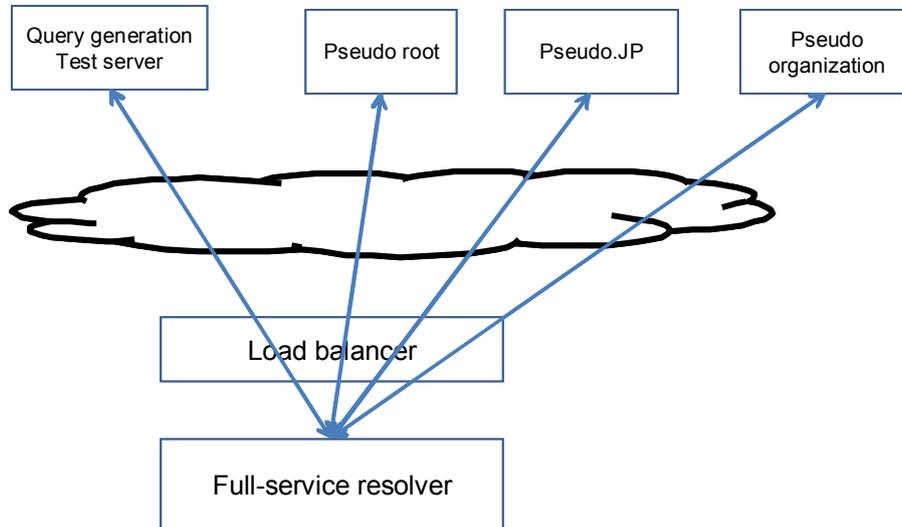
The data size accumulated in cache increased.

Not only the CPU usage rate and memory usage but also HDD resource usage increased due to key storage and ZONE signing, etc.

As a result of an increase in packet and data size, the network band width will also be restrained.

Verification of Functionality: Case Study 3

■ Case Study 3: Experimental Environment



Functionality	HW	Application	Note
Full-service resolver	SUN X2100 Solaris10	bind-9.7.0	IPv4 only
Load balancer	A10networks AX2500		IPv4 only
Query generation	SUN NetraT1	Queryperf (modified version)	IPv4 only

■ Case Study 3: Summary of Experimental Results

It was verified that tests for the following items were conducted without any issues with regard to the verification items on the full-service resolver side as well as the common items listed under “IV. Verification items” in the “DNSSEC Verification of Functionality: Procedure Manual (Ver. 1.1)” by JPRS.

2. Full-service resolver side

Verification item <F-2>: Verification of AD bits using a full-service resolver (DNSSEC-compliant)

Verification item <F-27>: Signature expiration field in the RRSIG record should indicate a time later than the current time.

Verification item <F-28>: Signature inception field in the RRSIG record should indicate a time prior to the current time.

Verification item <F-47>: Algorithm of the DS record should match that of the corresponding DNSKEY record.

Verification item <F-49>: Digest of the DS record should be hash of the key of the corresponding DNSKEY record.

Verification item <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.

Verification item <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.

Verification item <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.

Verification item <F-130>: DO bits should be set for full-service resolver (security-compliant) in recursive search irrespective of DO bits of original queries.

Verification item <F-147>: IP layer of full-service resolver (security-compliant) should be able to process fragmented UDP packets properly whether it is IPv4 or v6.

=> The experiment was conducted only for IPv4.

Verification item <F-154>: Full-service resolver (security-compliant) should have a function to incorporate at least one reliable public key or DS in its setting.

Verification item <F-194>: Self-signed DNSKEY with the REVOKE bit should be revoked.

Verification item <F-196>: Revoked DNSKEY should not be used as a trust anchor.

Verification item <F-201>: New keys should be added to the trust anchor when the time limit has passed.

Verification item <F-202>: New keys should not be added to the trust anchor before the time limit has passed.

Verification item <F-229>: The NSEC3PARAM record should exist at the top of the zone.

3. Common items

Verification item <Common-1>: It should be verified that TCP communication is not blocked.

Verification item <Common-2>: It should be verified that signed zone files are ready by BIND in the BIND setting.

Verification item <Common-3>: It should be verified that DNSSEC is enabled in the BIND setting.

Verification item <Common-4>: Verification of MTUs of communication paths by a ping command.

■ Case Study 3: Detailed Experimental Results

N/A

■ Case Study 3: Obtained Findings

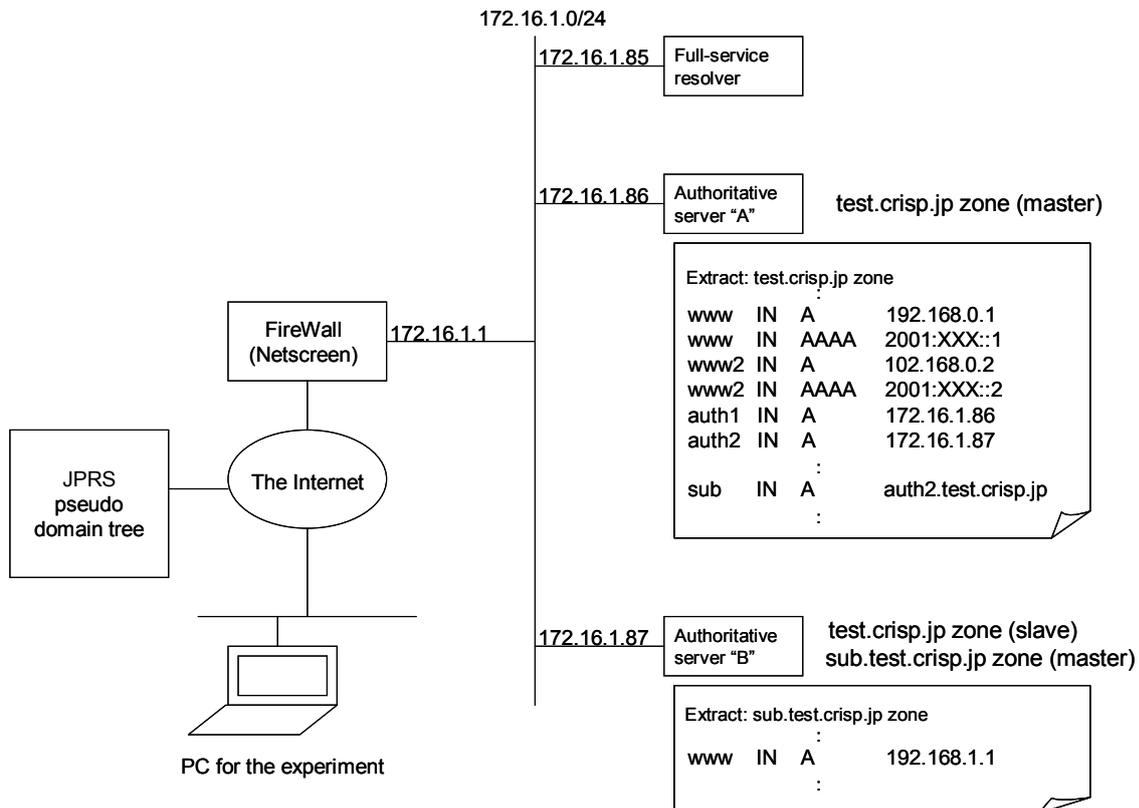
As a result of the tests conducted for each item in the aforementioned experimental environment, no particular issues were identified.

We think that there will be no functional issues in line with the deployment of DNSSEC.

Verification of Functionality: Case Study 4

■ Case Study 4: Experimental Environment

- Experimental Environment Configuration



- Software configuration:
OS: Solaris10 BIND:9.7.0-P1

■ Case Study 4: Summary of Experimental Results

The following tests were conducted based on the procedures in the “DNSSEC Verification of Functionality: Procedure Manual (Ver.1.1).”

It was verified that behaviors were within the scope of assumptions in all scenarios. In addition, conditions on the client and server sides were also verified for each scenario.

[Scenario 1] Queries to an authoritative server always fail.

[Scenario 2] Queries to an authoritative server sometimes fail.

[Scenario 3] Queries to an authoritative server get delayed.

[Scenario 4] Queries to an authoritative server result in an error.

[Scenario 5] Queries to a full-service resolver fail.

- [Scenario 6] Queries to a full-service resolver sometimes fail.
- [Scenario 7] Queries to a full-service resolver get delayed.
- [Scenario 8] Verification of queries to a full-service resolver fails.
- [Scenario 9] Queries to a full-service resolver result in an error.

■ Case Study 4: Detailed Experimental Results

Scenario 1

(i) Network issues of the testing device

Test result => No issues

(ii) Issues between the testing device and the authoritative servers

Test result => No issues

(iii) Issues with packets exceeding 512 octets

<A-85> Test result => No issues

<A-86> Test result => No issues

(Note)

UDP communication via EDNS0, switch to TCP, and fragment communication were verified for each test item.

Scenario 2

(i) The same queries result in success or failure.

Test result => No issues

(ii) Success/failure depends on the content of queries.

Covered by <A-85> of the Scenario 1 test.

(Notes)

UDP communication via EDNS0, switch to TCP, and fragment communication were verified for each test item.

It was verified that success/failure of the queries depended on the restriction of the network environment.

Scenario 3

(i) Response is also delayed for the other authoritative servers.

The test was not conducted because the preparation of the delayed network environment was not ready.

(ii) There are no issues with the other authoritative servers.

Covered by <A-85> of the Scenario 1 test.

It was verified that there were changes in communication due to TCP/UDP/fragment, etc.

(Although the possibility for delay was verified, the delayed network environment could not be established.)

Scenario 4

(i) DNSKEY record error

<A-27> Test result => No issues

<A-28> Test result => No issues

<A-58> Test result => No issues

<A-61> Test result => The test was not conducted because a zone could be signed without a KSK signature.

<A-79> Test result => No issues

(ii) RRSIG record error

<A-27, 28> Covered by the test results of Scenario 4-1.

<A-76> Test result => No issues (Conducted at the same time with <A-79>.)

<A-95> Test result => No issues

<A-115> Test result => No issues

(iii) NSEC record error

Test result => No issues

(iv) DS record error

<A-47> Test result => No issues

<A-76> Conducted by the Scenario 4-2.

<A-78> Test result => No issues

<A-79> Conducted by the Scenario 4-1.

<A-81> The test was not conducted because changes in TTL could not be generated.

(vi) NSEC3PARAM record error

The test was not conducted because NSEC3 was not in use. => Separate test

(vii) NSEC3 record error

The test was not conducted because NSEC3 was not in use. => Separate test

Scenario 5

(i) Network issues of the testing device

Test result => No issues

(ii) Network issues between the testing device and the full-service resolver

Test result => No issues

(iii) Network issues between the full-service resolver and the authoritative server

Test result => No issues

(iii) Queries between the full-service resolver and the authoritative server

Test result => No issues

(iv) Setting issues of the full-service resolver

<F-85> Test result => No issues

<F-86> Test result => No issues

<F-87> Test result => No issues

<F-130> Test result => No issues

<F-147> Test result => No issues (However, the test was not conducted in the v6 environment.)

Scenario 6

(i) The same queries result in success or failure.

Covered by the Scenario 5 test.

(ii) Success/failure depends on the content of queries.

<F-85> Test result => No issues

Scenario 7

(i) Queries from the full-service resolver to the authoritative server get delayed.

The test was not conducted because the preparation of the delayed network environment was not ready.

(ii) Network issues between the testing device and the full-service resolver

The test was not conducted because the preparation of the delayed network environment was not ready.

(iii) Full-service resolver Setting issues

Covered by the Scenario 5 test.

Scenario 8

(i) DNSSEC of the full-service resolver is invalid.

<F-130> Test result => No issues

(ii) There are issues with trust anchors of the full-service resolver.

<F-154> Test result => No issues

<F-201> The test was not conducted.

(iii) Time setting issues of the full-service resolver

Covered by the Scenario 8-5 test.

(iii) Linkage issues between the DS record and the DNSKEY record

<A-47> Test result => No issues

<A-76> Test result => No issues

<A-78> Test result => No issues

<A-79> Test result => No issues

<A-81> Test result => No issues

<A-115> Test result => No issues

(iv) Issues with the DNSSEC signatures

<A-27> Test result => No issues

<A-28> Test result => No issues

<A-58> Test result => No issues

<A-115> Test result => No issues

Scenario 9

(i) The results are out of the scope of assumptions.

Covered by the authoritative server test.

(ii) The results via the authoritative server are correct, but the results via the full-service resolver are incorrect.

Test result => No issues

■ Case Study 4: Obtained Findings

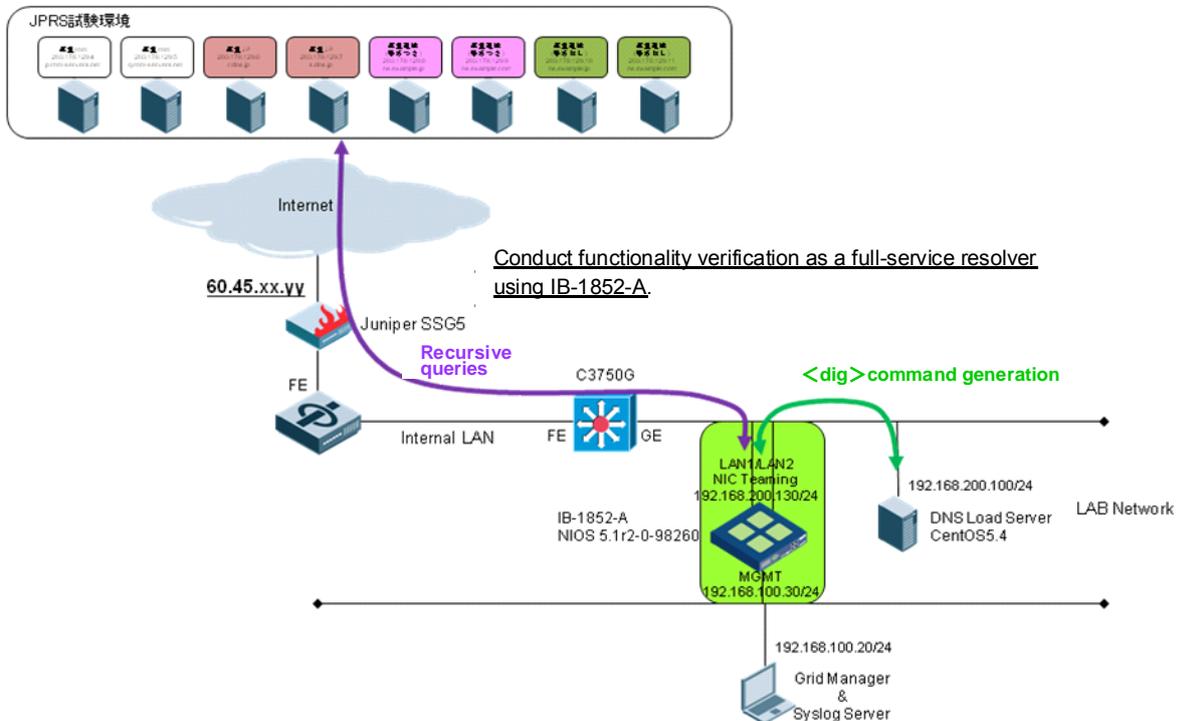
With regard to the failure of queries in the full-service resolver (validation failure), it is difficult to identify a specific issue as “SERVFAIL” is indicated uniformly on the full-service resolver side in the case of a problem with the authoritative server on the parent side, authoritative server, DS, DNSKEY, etc.

Furthermore, even if an issue is identified, it is possible that the issue which causes SERVFAIL cannot be identified without a validation on the authoritative server side.

=> It is necessary to establish an operational flow and investigation procedures including verification of cache information, manual validation of obtained signature information and a verification method of queries to the authoritative server.

Verification of Functionality: Case Study 5

■ Case Study 5: Experimental Environment



DNS APPLIANCE DEVICE: Infoblox 1852-A Network Service Appliance

Software version: NIOS 5.1r2-0-98260

* NIOS = Name of the internal OS of the Infoblox appliance

■ Case Study 5: Summary of Experimental Results

The tests were conducted for the verification items listed under “IV. Verification items, 2. Verification items on the full-service resolver side” in the “DNSSEC Verification of Functionality: Procedure Manual (Ver. 1.2).”

▼ Verification item <F-2>: Verification of AD bits using a full-service resolver (DNSSEC-compliant)

- Result: Successful

▼ Verification item <F-27>: Signature expiration field in the RRSIG record should indicate a time later than the current time.

- Result: Successful

▼ Verification item <F-28>: Signature inception field in the RRSIG record should indicate a time prior to the current time.

- Result: Successful

▼ Verification item <F-47>: Algorithm of the DS record should match that of the corresponding

DNSKEY record.

- Result: Successful

▼ Verification item <F-49>: Digest of the DS record should be hash of the key of the corresponding DNSKEY record.

- Result: Successful

▼ Verification item <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.

- Result: Successful

▼ Verification item <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.

- Result: Successful

▼ Verification item <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.

- Result: Successful

▼ Verification item <F-130>: DO bits should be set for full-service resolver (security-compliant) in recursive search irrespective of DO bits of original queries.

- Result: Successful

▼ Verification item <F-147>: IP layer of full-service resolver (security-compliant) should be able to process fragmented UDP packets properly whether it is IPv4 or v6.

- Result: Successful

▼ Verification item <F-154>: Full-service resolver (security-compliant) should have a function to incorporate at least one reliable public key or DS in its setting.

- Result: Successful

▼ Verification item <F-194>: Self-signed DNSKEY with the REVOKE bit should be revoked.

- Result: The test was not conducted in this technology experiment.

▼ Verification item <F-196>: Revoked DNSKEY should not be used as a trust anchor.

- Result: The test was not conducted in this technology experiment.

▼ Verification item <F-201>: New keys should be added to the trust anchor when the time limit has passed.

- Result: The test was not conducted in this technology experiment.

▼ Verification item <F-202>: New keys should not be added to the trust anchor before the time limit has passed.

- Result: The test was not conducted in this technology experiment.

* Note: RE: Verification items: <F-194>, <F-196>, <F-201> and <F-202>

“NIO 5.1r2-0-98260” does not support “RFC5011 Automated Updates of DNS Security (DNSSEC) Trust Anchors,” which will be supported by NIO to be released in the future.

▼ Verification item <F-229>: The NSEC3PARAM record should exist at the top of the zone.

- Result: Successful

■ Case Study 5: Detailed Experimental Results

Detailed Experimental Results

▼ Verification item <F-2>: Verification of AD bits using a full-service resolver (DNSSEC-compliant)

```
[root@centos ~]# dig +dnssec @192.168.200.130 www.jp.rs.jp a
```

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 www.jp.rs.jp a
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14593
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.jp.rs.jp.                IN      A

;; ANSWER SECTION:
www.jp.rs.jp.                900     IN      A      192.0.2.1
www.jp.rs.jp.                900     IN      RRSIG  A 8 3 900 20101225232004 20091225222004
14883 jp.rs.jp. VizFF1EuRocTXsrACbU52G5YQi8CQEhxzwFrSoHgv8+PqXeXD3jhXsqe
KXtZQIzUEYKVMghjs/CkOLeLG7w0V4z2oKhkQ70TVTVc/Qqq8fnpQh5Z
B3TytXng3ZkO25UcbH6ujw4clYSCTKGexn3ia4tm1XCuGb2xDUOhPsc+ Sy0=

;; Query time: 151 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 15:43:51 2010
;; MSG SIZE  rcvd: 223
```

▼ Verification item <F-27>: Signature expiration field in the RRSIG record should indicate a time later than the current time.

▼ Verification item <F-28>: Signature inception field in the RRSIG record should indicate a time prior to the current time.

```
[root@centos ~]# dig +dnssec @192.168.200.130 jp.rs.jp SOA
```

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 jp.rs.jp SOA
; (1 server found)
```

```

;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50086
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
jprs.jp.                IN      SOA

;; ANSWER SECTION:
jprs.jp.                900    IN      SOA      ns.jprs.jp. root.jprs.jp. 1 3600 900 604800 900
jprs.jp.                900    IN      RRSIG   SOA 8 2 900 20101225232004
20091225222004 14883 jprs.jp.
EDXMyT8SJMbnepEHLRNMO37GzpV0NWFjkTVWJVbEW2SOPzMFNaeyERD2
WnrIRaDq11xYYDSotg1lsmSFSTICJmS1g2iFS3KTDU2MSTQH/qjZjlyd
wNC/oWYnXLtoIIhJRD+Afg4BgEwQ9Yif9KCwf/VrpRj4r0poKTS+IIsx NzI=
;; Query time: 19 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 16:03:19 2010
;; MSG SIZE  rcvd: 247

```

▼ Verification item <F-47>: Algorithm of the DS record should match that of the corresponding DNSKEY record.

▼ Verification item <F-49>: Digest of the DS record should be hash of the key of the corresponding DNSKEY record.

```
[root@centos ~]# dig +dnssec @192.168.200.130 secure.crisp.jp DNSKEY
```

```
; <<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 secure.crisp.jp
DNSKEY
```

```
;(1 server found)
```

```
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29418
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

```

```
;; OPT PSEUDOSECTION:
```

; EDNS: version: 0, flags: do; udp: 4096

:: QUESTION SECTION:

;secure.crisp.jp. IN DNSKEY

:: ANSWER SECTION:

secure.crisp.jp. 3600 IN DNSKEY 256 3 8

AwEAAfGAwdnb94WE8rST4J23LOqirOgOekeITguDf+XuAeJG/IXT33k7
lsHeUREhlc98snoTjeOkWLYALaR1f+P5XfSUEkX8+hqNACVb+9s/2ZHD
QzYTHoBd9GSOViEJCSagD1DqF3/XsfHqQ8Qu2w3uEpIK1SDz2Vt3m3HD
mGk1goOSQzTq5xFW3xnlebvRzGIBELQnrLww89bv0YGdtycdTcQ/25NI
6d8C76BBbVJHw4CohxPlxkDgR5BCgIBkWtx2O8LI8tdBAsFPNp7KuaAr
csm/E5I6plQbi1PKLCuFp1ntOnZMprnPwo3feO6ixNzovjogVfTMt5GM 9DpKAenW1Hk=

secure.crisp.jp. 3600 IN DNSKEY 257 3 8

AwEAAbbVykYDNiGzdhCaUYN74unIJUMoa6T8dj1IvaCUGXc88SHJqYno
jp7BU+GSjFvC1/GOAZ8tQ/jiT2zbz5uUEg320dC/SsX2gmzC4IqTLTOZ
44fQo/Ap3vSr9EDIPxES4o5G1TO42SPheBZwY7nb7lQSRINSflotsOpM
7rgS4SOI8c/HfRc/VGgBq4DJ6GmcP+H73GD8baR95CmwVAxUAvPEtiB9
jkKxE0hxRxUXziAXfA2ft005m6AAW/yqtyu1qvmSgnvDKswu2aFbEFVh
864zjE6yEqj3Si8xhlfYJft/+qdvDZ5XPLR4FqbBO4HsXiPqp4hTYpKs kBt+21VqUxM=

secure.crisp.jp. 3600 IN DNSKEY 257 3 8

AwEAAAd1byrZ98iVpSts+jsCmw2oUCazrjml3N8mDuf7r2QyhX8FeDTIC
O47gCxY4vgM37wPU772wuKuINP0zAAU3HPbbIYpaHYqkAavjNv6balij
kZbgaGocIXmQnDWuwLoZW8EBpkDcURx6zItaMoJdrD6w+VJ0gCRkJ35
Zhbyat2hxysnHUiHjrAOgXv2tq8FgemZP7weI68YmHe9l96OuSGjS6Yy
K9zLolTcJ8F3DV1HzgjLsfThRnqv/DoiGRJKGQ5pvG1SzzgCcsOTmZV
V0fuVSzKAc/moiH3vJkpKH3ZbqZEQ/sup9heVYwII87TQfBqnS0bYoZ8 bW+teSV46p0=

secure.crisp.jp. 3600 IN RRSIG DNSKEY 8 3 3600 20100913170201

20100816170201 41014 secure.crisp.jp.

bJNzsVuMERTq6DyOLZeoji5SQDjiKC57sOEU0b6SKkTZiAfssznkFoKU
0TEg/QbW5DgOA0NgzBRPdLftRdTkL5OzJW3C5ahgZKKRxaG3fycfPNdN
nHvz69AJWQxOICS/pAbgrg7SUKlanvxAQah5UXFaGR2CTeY8PH+n0jd2
pFZlubIutFY9sdxsPDRU4fEQ5LsfUhpCPn9PL1bETVzcSE5wP006UB0
QRZ/z58T5vtOi9h5djfLtnWVHTXSUasSuR6yrU/9dvq+qEUbWJE+szFv
T4H4m3aEaA9jXBhl8Vp1aty8AqMdWgTpqHyFllYupdCWLH7V+TfzyMvI LS63HQ==

secure.crisp.jp. 3600 IN RRSIG DNSKEY 8 3 3600 20100913170201

20100816170201 52567 secure.crisp.jp.

ysdQABVvLHU8jtX+HR8Jnw/r0PFFKMoJWqe3DwA3vMlvFqCpVJrS4xFps

```
klS6G56hX0IfPSJL17bw3T8gQukYQKO6dJuL5XI7LkmndDWMZp0C5Qgq
JKkJc4mBrOhvsNmgMssHRgs+FInSkHV9ztLquUSP9IkD5zNtFzu8Ppml
Uc2t3jUVwUfTgUTruAU3o2zHKdtB3gIcwD47hfbmEg3C5k88+bPePAY4
jBz/ki3k2clDfXHMOPbzReBQOOi0B2lluA91GtfXwTv7J4bFN7QSVBLS
ev1bSM7Fpz3RZ7lRojLvmWifnTzqptSHBTL7ahKo8PkXU3m6tqXmRMGw l8BshQ==
secure.crisp.jp.          3600      IN          RRSIG      DNSKEY 8 3 3600 20100913170201
20100816170201 55533 secure.crisp.jp.
LgGz9nPuf4cZaf/bsBnHrOfXGoXYor79flBxUqCkEwK2gxA8lco2KvdR
dkixWqJR6uq3WDXQq1281sEznbfgXzzkL9AugIbCI9aPPxG9tnKccEf6
VVSLF4XZ54icOHZs0te4c5AJREb4QMktCZ5cdT9BynGIlixzSL5nDTGe
0CbGHUdCGLK6A6IMaSO5c9sj36z6rYO3bUJc10BeLQsy7n91Zkb0jHrq
PcXCFviJ8s/drSq7SdJ8zzMHblns3O8pql2NhznVTZf36N0Bf5daI6/f
2DU7javf8FqgWo2IBvK/EGpuURed97BoDsXGm5gwQN4pM4r7TqZhcJRJ NCq88g==
```

```
:: Query time: 23 msec
:: SERVER: 192.168.200.130#53(192.168.200.130)
:: WHEN: Tue Aug 17 16:29:21 2010
:: MSG SIZE   rcvd: 1781
```

▼ Verification item <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.

▼ Verification item <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.

▼ Verification item <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.

```
[root@centos ~]# dig +dnssec @192.168.200.130 crisp.jp DNSKEY
```

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 crisp.jp DNSKEY
(1 server found)
;; global options:  printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 15040
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;crisp.jp.                IN          DNSKEY
```

The message “;; Truncated, retrying in TCP mode.” is not shown.

:: ANSWER SECTION:

crisp.jp. 120 IN DNSKEY 256 3 8

AwEAAarS/K6aW3SzFgYFbXYSIoSfYC4CKP1dEW6/p1SlcwZvsUfiBrzV
i4FGgoI1mBnCgy71h5teGNn9MAIqMpXG2f0cGFdSsq05DRsfPeu1f9Vr
0/YZ21jE/ORZ0vrH/iSmp1WhZN9w9rlJcPbNFDtkqMW9DbR4ZVQKiHyD C5uineLt

crisp.jp. 120 IN DNSKEY 256 3 8

AwEAAadCB3Q0Z5tVMLjZOIXzh7E2ymjNf5uUUqXXm0kBJN3+J2IIGUI18
QoncJxDP4ytGjFsLcmqimfq+PhIppUyI3YAZnllm+bRFt8fieF/gt3uk
g9H7nA+kb44PuyJmp/iFhzOrA8uq9LkKCD/5VLnrnK+awNs3k8HnPmCr 4EIFSKI3

crisp.jp. 120 IN DNSKEY 257 3 8

AwEAAAbQJK+no7FHAm9eeWIF2DAIQBSimcuK8h0Dj3BDMZS5s4Svv2mxo
e5P5zUtoel3Ewhv2dRfBOznZMUvC6H9gG7IF5h9VDdKmH4O71TL/yycp
2COJ7UOr+xxvqJLfMkx2odPRBS4xlK+5xk7XMRcfwXx34eQTgPUa8+ye
FvRNclzHgOgVA9/N/iZ94wUMSxW1y4YyEONmVtHbVyssU8DAP7yzYc/F
5BEHtXdvxmapQ4LR9V4Z8p7V8rmkIL40JRRB7O8AxWrxM7y4RNHr/6V0
nMRCXT6G1Ee7SqBFAw183juDvIw0DjtHPOjOqdoQWpPSe7cNDd16xLAd TIAT3RML2PE=

crisp.jp. 120 IN DNSKEY 257 3 8

AwEAAadtNcWMzNhB6frxTiy/sNltsplfch0NoqUNDx3uP33sslxGgdKs
3W2hSpweK6PwMW/hFiyYwbnfrHK3pmZIP6PylH1femxtLyU2ozvAYUD5
U4g5eo71Ytey0xNaBIFAuMUXGm2KZjUeuN/2IS2iZjQEYYa/ew1st4sd
ZRztjB/euTz1IsffMap5CqijQyS6Awc84LwafYzFzTs93MnuoNoqp9IM
G/wM6BvEqMvkC5HOAgsL+vxM/BuxcFdX0lug29weV92uK02cZUwtct81
+z1Ld/E7kQhtnVZ0ZRFrq4CDuYsB.JPwm1rec8E4WX91UkPWaMOqHDmOW doe+0QMWqbc=

crisp.jp. 120 IN RRSIG DNSKEY 8 2 120 20100901104857

20100802104857 10770 crisp.jp.

jnhD5yy42Qew3Vd/Ee4fQuQNx6pLrJcknpRREtoqG0fwY8xZf3+WtqUy
RwkOe53i4+1Etml+4LeL4dscf159vlEWMwwMAXn9bdL/no2yBapeqfoK
rfbMrSNCHTgPtHX63CGj1riEqx/MltDPxZiG6yvG/RKehztySj8cNW8V 9Jg=

crisp.jp. 120 IN RRSIG DNSKEY 8 2 120 20100901104857

20100802104857 42817 crisp.jp.

CLg1CCTII5U5rXMxYc7YECDwR0uaGsHw/zlnojz19rVsZlUxes7s6QIR
ToZ2Jvhur7NiyXcwFs8uCWWhVB4oSKVgPwnWE2bUhol7vRfmJdsKSy3Jv
m56xYxiTu/8QN9YsxXjg+bDgTKrxAJozJX1nQHh0UmLK0Wa+M9vgPezZ
jZOflVMvElen0ArzaVmVh2wv4OqCci/HAivrDpWmkNBNrFlsegusMOzd
/tawQhI5N42q+GrYU1giKQq3NH8bpLSFLqWrVWK+5q2Ti1J/pmX39W0e
oyzq60u/KSwGKaK3ebTO+hyyd3HQ8ZkZqoIZXEWfYsVcgSlcpGXL2lux 88x+Gg==

```
crisp.jp.          120    IN      RRSIG   DNSKEY 8 2 120 20100901104857
20100802104857 46627 crisp.jp.
ZZTAtUp0UJ4CflkYZm/4IcC6b6bnR6L+cSaR1fTrh8y5PvC+jbGVZU1P
kYZhdfKO/uiIIsboULvDI26eA0Shy3Di55e8PQIsbA1qLUzbS+KvbpSy
3QaQcdyJ2ZhFfLt2heHSTIIYuE/wNMODzEILZG4oGELchNq5clwBnAg2
pj034HwK41//JMAEFZRg7fueItL7xAes1QEnMFOR7tRQv/WiG5D825WV
elUd16uPqngoOWIiWR/JEVCMfaxpq87rP8kgSu7HDILAzMT7W6DqO9Pj
GP+Y9lyFYwL7wxWMvHeG6zOjBzTDzDnDIRa/LJmIvoq4UMuBCJC/R3Ze Rz28/Q==
```

```
:: Query time: 22 msec
:: SERVER: 192.168.200.130#53(192.168.200.130)
:: WHEN: Tue Aug 17 16:44:01 2010
:: MSG SIZE   rcvd: 1645
```

▼ Verification item<F-130>: DO bits should be set for full-service resolver (security-compliant) in recursive search irrespective of DO bits of original queries.

```
[root@centos ~]# dig @192.168.200.130 www.jp A
```

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.el5_4.2 <<>> @192.168.200.130 www.jp A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1864
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
:: QUESTION SECTION:
```

```
;www.jp A      IN      A
```

```
:: ANSWER SECTION:
```

```
www.jp A      900    IN      A      192.0.2.1
```

```
:: Query time: 868 msec
:: SERVER: 192.168.200.130#53(192.168.200.130)
:: WHEN: Tue Aug 17 17:02:34 2010
:: MSG SIZE   rcvd: 45
```

Verification of the content of cache

```
Infoblox > set dns flush all
```

```

Infoblox > show dns cache
;
; Start view default
;
;
; Cache dump of view 'default' (cache _default)
;
$DATE 20100817080328
; secure
.                86345   IN NS    p.root-servers.net.
                86345   IN NS    q.root-servers.net.
; secure
                86345   RRSIG   NS 8 0 86400 20110712091518 (
                20100712081518 40509 .
                U5lmzncDTyS3Up+rdFZnlV+gPw1KAhtv5Fb
                CtR7VyAvYWP529nf08+pKC6tBqZUIWSLEINE
                66o7LfBnovzobYNpuqaCUQcXWndFW1VZ0M+i
                oGpUazpJowpcScJ15Xtbm5h9DN5+9Wa2YQnM
                Fyzz8fPPVgpDkyUAM0PQbMk/0e8= )
*snip*
; glue
ns.jp.r.s.jp.    86345   A       203.178.129.8
; pending-additional
                845     RRSIG   A 8 3 900 20101225232004 (
                20091225222004 14883 jp.r.s.jp.
                vLk2grQhX9z29iZQE6+xkbZy4JSdDbe5e2Zz
                WOn3HKVhOYvwspKodWctgRTvLBuy9Mdl/eBB
                rv521NiosZnuX0/cuq/tDbjKxuxj7sdMMVr+
                cXdoQzHuhSA4lTuiC+Vn96Eu9wXyw5yjP2Ap
                R8am3j71+v9/SiKh4WH9KPwFot0= )
; glue
                86345   AAAA    2001:200:132:3::8
; pending-additional
                845     RRSIG   AAAA 8 3 900 20101225232004 (
                20091225222004 14883 jp.r.s.jp.
                hVnPup5vUG0lJIMlJgJbIQLTZidfc1r1215n
                c04PHFeX73NtMRqnxzV39JEJBarN2pAwjTto

```

```
9KBZ/ETvp2/5QCMfSa8sHIex1Reew9sRtqBC
iDr/D8rVn7WeDgUF9xY7Mrb616bMrcqMLyBY
j7xsJTqTHNrRnGWxefcR0uBO510= )
```

```
; secure
www.jp.rs.jp.      846      A      192.0.2.1
; secure
                  846      RRSIG   A 8 3 900 20101225232004 (
                  20091225222004 14883 jp.rs.jp.
```

```
VizFF1EuRocTXsrACbU52G5YQi8CQEhxzwFr
SoHgv8+PqXeXD3jhXsqeKXtZQIzUEYKVMghj
s/CkOLeLG7w0V4z2oKhkQ70TVTVc/Qqq8fnp
Qh5ZB3TytXng3ZkO25UcbH6ujw4clYSCTKGe
xn3ia4tm1XCuGb2xDUOhPsc+Sy0= )
```

snip

; Bad cache

;

; Dump complete

▼ Verification item <F-147>: IP layer of full-service resolver (security-compliant) should be able to process fragmented UDP packets properly whether it is IPv4 or v6.

Infoblox > ping 203.178.129.26 packetsize 1472

pinging 203.178.129.26

PING 203.178.129.26 (203.178.129.26) 1472(1500) bytes of data.

1480 bytes from 203.178.129.26: icmp_seq=1 ttl=51 time=12.9 ms

1480 bytes from 203.178.129.26: icmp_seq=2 ttl=51 time=12.2 ms

1480 bytes from 203.178.129.26: icmp_seq=3 ttl=51 time=12.9 ms

1480 bytes from 203.178.129.26: icmp_seq=4 ttl=51 time=12.6 ms

1480 bytes from 203.178.129.26: icmp_seq=5 ttl=51 time=12.6 ms

--- 203.178.129.26 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4019ms

rtt min/avg/max/mdev = 12.282/12.695/12.968/0.250 ms

[root@centos ~]# dig +dnssec @192.168.200.130 crisp.jp DNSKEY

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 crisp.jp DNSKEY
```

```
;(1 server found)
```

```

;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15054
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;crisp.jp.                IN      DNSKEY

;; ANSWER SECTION:
crisp.jp.                8      IN      DNSKEY  256 3 8
AwEAAarS/K6aW3SzFgYFbXYSIoSfYC4CKP1dEW6/p1SlwZvsUfiBrzV
i4FGgoI1mBnBcgy71h5teGNn9MAIqMpXG2f0cGFdSsq05DRsfPeu1f9Vr
0/YZ21jE/ORZ0vrH/iSmp1WhZN9w9rlJcPbNFDtkqMW9DbR4ZVQKiHyD C5uineLt
crisp.jp.                8      IN      DNSKEY  256 3 8
AwEAAAdCB3Q0Z5tVMLjZOIXzh7E2ymjNf5uUUqXXm0kBJN3+J2IIGUI18
QoncJxDP4ytGjFsLcmqimfq+PhIppUyI3YAZnIIm+bRFt8fieF/gt3uk
g9H7nA+kb44PuyJmp/iFhzOrA8uq9LkKCD/5VLnrnK+awNs3k8HnPmCr 4EIFSKI3
crisp.jp.                8      IN      DNSKEY  257 3 8
AwEAAAbQJK+no7FHAm9eeWIF2DAIQBSimcuK8h0Dj3BDMZS5s4Svv2mxo
e5P5zUtoel3Ewhv2dRfBOznZMUvC6H9gG7IF5h9VDdKmH4O71TL/yycp
2COJ7UOr+XvqJLfMkx2odPRBS4xIK+5xk7XMRcfwXx34eQTgPUa8+ye
FvRNclzHgOgVA9/N/iZ94wUMSxW1y4YyEONmVtHbVyssU8DAP7yzYc/F
5BEHtXdvxmapQ4LR9V4Z8p7V8rmkIL40JRRB7O8AxWrxM7y4RNHr/6V0
nMRCXT6G1Ee7SqBFAw183juDvIw0DjtHPOjOqdoQWpPSe7cNDd16xLAd TIAT3RML2PE=
crisp.jp.                8      IN      DNSKEY  257 3 8
AwEAAAdtNcWMzNhB6frxTiy/sNItspZlfch0NoqUNDx3uP33sslxGgdKs
3W2hSpweK6PwMW/hFiyYwbnfrHK3pmZIP6PylIH1femxtLyU2ozvAYUD5
U4g5eo71Ytey0xNaBIFAuMUXGm2KZjUeuN/2IS2iZjQEYYa/ew1st4sd
ZRztjB/euTz1IsffMap5CqiJQyS6Awc84LwafYzFXTs93MnuoNoqp9IM
G/wM6BvEqMvkC5HOAgsL+vxM/BuxcFdX0lug29weV92uK02cZUwtct81
+z1Ld/E7kQhtnVZ0ZRFrq4CDuYsB.JPwm1rec8E4WX91UkPWaMOqHDmOW doe+0QMwqbc=
crisp.jp.                8      IN      RRSIG   DNSKEY  8 2 120 20100901104857
20100802104857 10770 crisp.jp.
jnhD5yy42Qew3Vd/Ee4fQuQNx6pLrJcknpRREtoqG0fwY8xZf3+WtqUy
RwkOe53i4+1Etml+4LeL4dscf159vIEWMwwMAXn9bdL/no2yBapeqfoK

```

rfbMrSNCHTgPtHX63CGj1riEqx/MltDPxZiG6yvG/RKehztySj8cNW8V 9Jg=
crisp.jp. 8 IN RRSIG DNSKEY 8 2 120 20100901104857
20100802104857 42817 crisp.jp.

CLg1CCTII5U5rXMxYc7YECDwR0uaGsHw/zlnojz19rVsZIUxes7s6QIR
ToZ2Jvhur7NiyXcwFs8uCWWhVB4oSKVgPwnWE2bUhOL7vRfmJdsKSy3Jv
m56xYxiTu/8QN9YsxXjg+bDgTKrxAJozJX1nQHh0UmLK0Wa+M9vgPezZ
jZOflVMvElen0ArzaVmVh2wv4OqCci/HAivrDpWmkNBNrFlscgusMOzd
/tawQhI5N42q+GrYU1giKQq3NH8bpLSFLqWrVWK+5q2Ti1J/pmX39W0e
oyzq60u/KSwGKaK3ebTO+hyyd3HQ8ZkZqoIZXEWfYsVcgSIcpGXL2lux 88x+Gg==
crisp.jp. 8 IN RRSIG DNSKEY 8 2 120 20100901104857
20100802104857 46627 crisp.jp.

ZZTAtUp0UJ4CflkYZm/4IcC6b6bnR6L+cSaR1fTrh8y5PvC+jbGVZU1P
kYZhdfKO/uiIIsboULvDI26eA0Shy3Di55e8PQIsbA1qLUzbS+KvbpSy
3QaQcdyJ2ZhFfLt2heHSTIIYuE/wNMODzEILZG4oGELchNq5clwBnAg2
pj034HwK41//JMAEFZRg7fueItL7xAes1QEnMFOR7tRQv/WiG5D825WV
eIUd16uPqngoOWIiWR/JEVCMfaxpq87rP8kgSu7HDILAzMT7W6DqO9Pj
GP+Y9lyFYwL7wxWMvHeG6zOjBzTDzDnDIRa/LJmIvoq4UMuBCJC/R3Ze Rz28/Q==

:: Query time: 0 msec
:: SERVER: 192.168.200.130#53(192.168.200.130)
:: WHEN: Tue Aug 17 17:29:18 2010
:: MSG SIZE rcvd: 1645

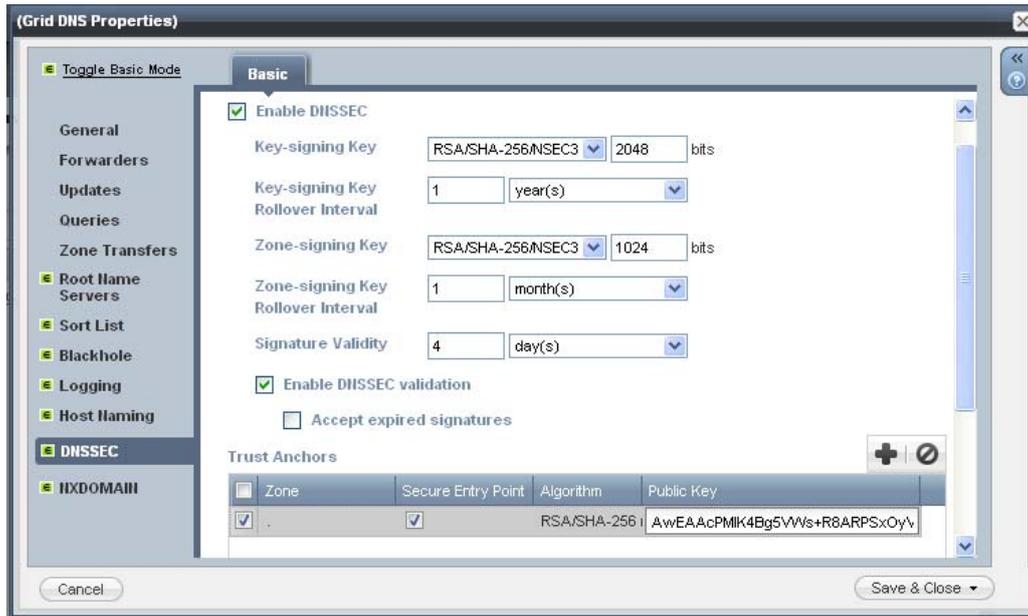
▼ Verification item <F-154>: Full-service resolver (security-compliant) should have a function to incorporate at least one reliable public key or DS in its setting.

Root key of the pseudo tree

trusted-keys {

"." 257 3 8 "AwEAAcPMIK4Bg5VWs+R8ARPSxOyV+crdg/kawfraPfIT+rCTRdi43MYX
3kG+XJtkVIC5/FE08yUpjy9dAtSorqOcYXSd66H1UxCq/vwmBEOlpAB
50DZ/xMgGyp/EOZHvpOgObNo2ITKcggGmU2KvPYfoXzqH+oyE4ApaE1
2/GZj1A0QQ4nidD23c4FBzpszZXteeiEA8DWkaicfWLKYyjQ75hm4zbu
FvQRq9O6isY+2SVqLiITmzmwWvsf6/onftwO0qToiiUQWvUdMwN6QsjF
/qRamFa7ToPPw37ydSfPWstxiPXj3b1WhKOr0Zgdr6tEwWtulhD4OWEr Wdqf/bAGZD0=";
};

Set up of the trust anchors on NIOS GUI



- ▼ Verification item <F-194>: Self-signed DNSKEY with the REVOKE bit should be revoked.
- ▼ Verification item <F-196>: Revoked DNSKEY should not be used as a trust anchor.
- ▼ Verification item <F-201>: New keys should be added to the trust anchor when the time limit has passed.
- ▼ Verification item <F-202>: New keys should not be added to the trust anchor before the time limit has passed.

The test was not conducted in this technology experiment for verification items: <F-194>, <F-196>, <F-201> and <F-202>.

- ▼ Verification item <F-229>: The NSEC3PARAM record should exist at the apex of the zone.

```
[root@centos bin]# ./dig +dnssec @192.168.200.130 jp NSEC3PARAM
```

```
; <<>> DiG 9.6.2-P2 <<>> +dnssec @192.168.200.130 jp NSEC3PARAM
```

```
;(1 server found)
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34689
```

```
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags: do; udp: 4096
```

```
;; QUESTION SECTION:
```

```
;jp. IN NSEC3PARAM
```

:: ANSWER SECTION:

jp. 0 IN NSEC3PARAM 1 0 10 CAFE
jp. 0 IN RRSIG NSEC3PARAM 8 1 0 20100916030235

20100817030235 54813 jp.

kEmt4tYBDaH4pUVNI/M++G3q/QTZQLTwk8QEdVieCYTTKAdfA8gxMpvw

tMpcxng2swE65XP5PRNwWRi133Ku4RbCfu1CcgC+7pkC7T6y/SkPNqHf

9NxjAFkGpXGNdigyKaet+JrOV9ItCUmUVL/bs+G8ei50gGSclJ/HAnel

oxRufg6afqs6ohLzGfeqWK+A7BTCJvbR+mpNr3yeazpBqmg6aX89fb3w

/3sLqUPrOJCKif4+Z1GFiTiv+8vpUiHqZ3uHaj23gCythrd5r1SBL2Z

QjBvXkLWRUnjN1oVJNs+34L3ZUDoMM3gPtqzqpBMm0uK2hiun5jrYNMA c5p9ng==

:: Query time: 13 msec

:: SERVER: 192.168.200.130#53(192.168.200.130)

:: WHEN: Tue Aug 17 20:37:34 2010

:: MSG SIZE rcvd: 340

■ Case Study 5: Obtained Findings

▼ Infoblox NIOS compatibility with the RSA/SHA-2 signature algorithm

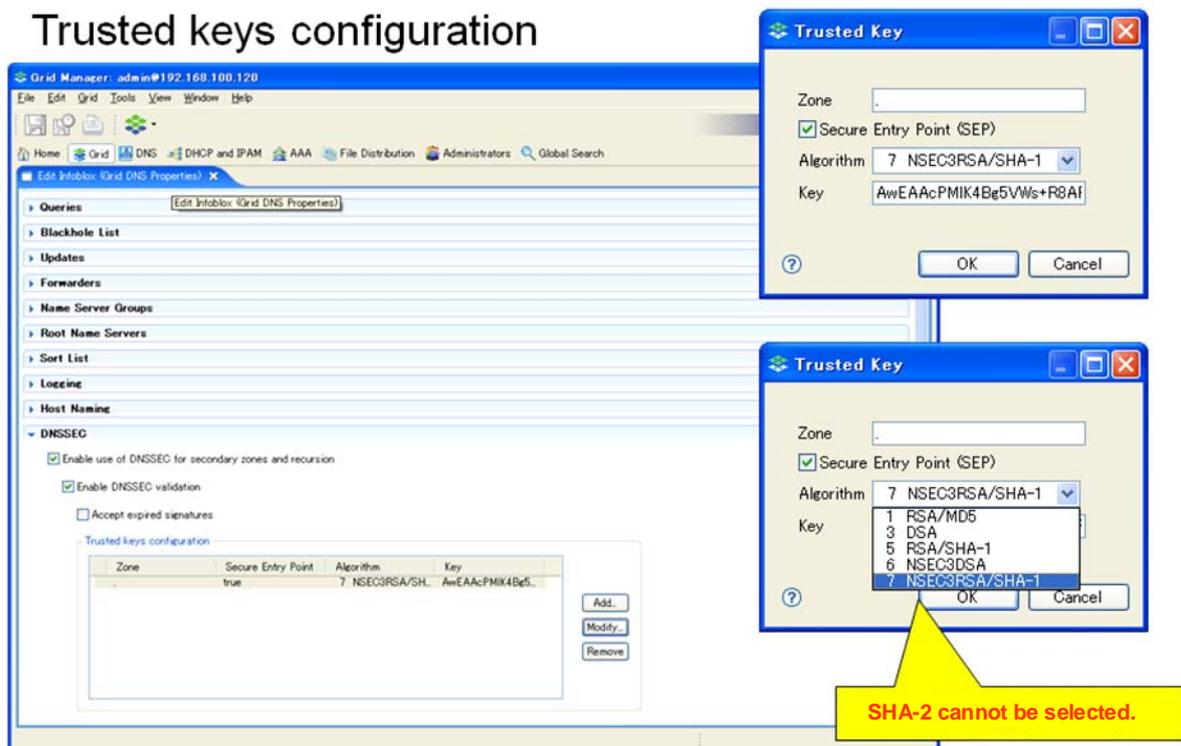
Infoblox NIOS (4.3r3 and above) supports the secondary name server for the DNSSEC zone and the import of trust anchors for the cache (full-service resolver) name server, and NIOS (5.0r1 and above) supports the key management of the primary name server for the DNSSEC zone and a signature function. However, only NIOS (5.1r2 and above) supports the RSA/SHA-2(SHA-256/SHA-512) signature algorithm which is used in root zone.

In the case of implementing the DNSSEC-compliant cache name server using the Infoblox appliance in the future, it is recommended to deploy NIOS (5.1r2 and above) which supports the RSA/SHA-2 signature algorithm.

▼ Example of a validation failure in the cache server due to inconsistency in the signature algorithm

Test result for NIOS (4.3r6)

The RSA/SHA-2 signature algorithm is used for the pseudo root server.



When the DNSSEC validation of a cache server is enabled, the test fails as follows.

```
C:\dig>dig @192.168.200.120 jprs.jp a +dnssec
; <<>> DIG 9.3.2 <<>> @192.168.200.120 jprs.jp a +dnssec
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 1797
;; flags: qr rd ra, QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do, udp: 4096
;; QUESTION SECTION:
;jprs.jp.                IN      A

;; Query time: 187 msec
;; SERVER: 192.168.200.120#53(192.168.200.120)
;; WHEN: Fri May 21 14:07:18 2010
;; MSG SIZE rcvd: 36
```

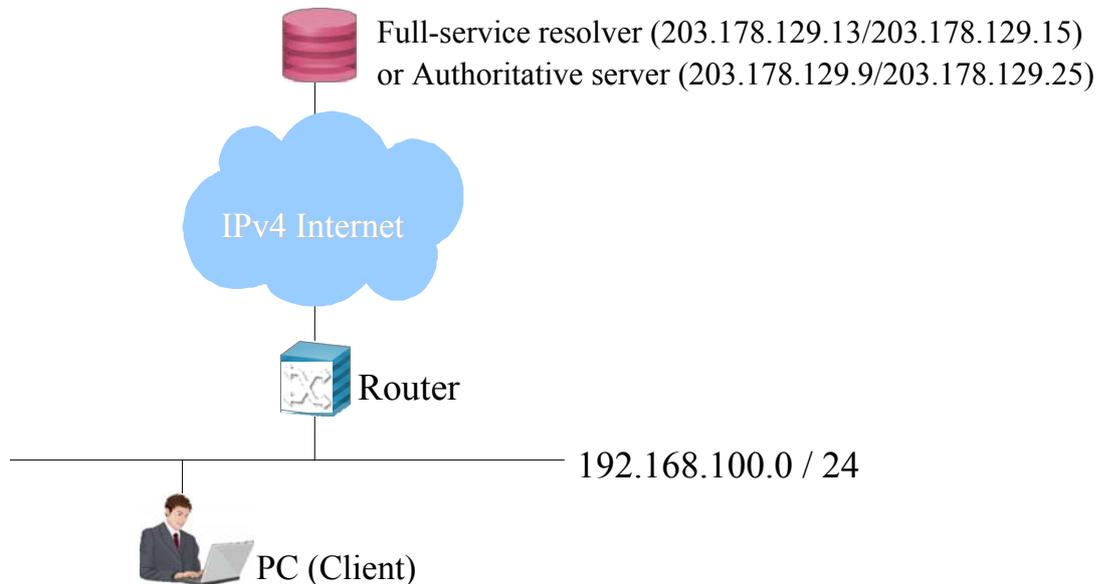
SERVFAIL is returned.

Validation fails due to inconsistency in the signature algorithm.

```
May 21 14:11:55 (none) named[23718]: client 192.168.1.23#3712: query: jprs.jp IN A +ED
May 21 14:11:55 (none) named[23718]: validating @0x85a2258: jprs.jp A: no valid signature found
May 21 14:11:55 (none) named[23718]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23718]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.5#53
May 21 14:11:55 (none) named[23717]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23717]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.4#53
May 21 14:11:55 (none) named[23717]: no valid DS resolving 'jprs.jp/A/IN': 203.178.129.9#53
May 21 14:11:55 (none) named[23717]: validating @0x85ae2b8: jprs.jp A: no valid signature found
May 21 14:11:55 (none) named[23717]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23717]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.4#53
May 21 14:11:55 (none) named[23718]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23718]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.5#53
May 21 14:11:55 (none) named[23718]: no valid DS resolving 'jprs.jp/A/IN': 203.178.129.8#53
```

Verification of Functionality: Case Study 6

■ Case Study 6: Experimental Environment



* CentOS5.4 is used for PC (Client).

BIND-9.7.0rc1 is installed.

■ Case Study 6: Summary of Experimental Results

By testing the following verification items on a full-service resolver and an authoritative server for both cases with and without a signature, it has been verified that the router's behaviours do not interfere with the DNSSEC communication during the transparent transmission using a router with a standard filter which sufficiently meets DNS requirements from a client.

- <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.
- <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.
- <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.
- <A-85>: Authoritative server (security-compliant) should have a UDP communication capability via EDNS0.
- <A-86>: Authoritative server (security-compliant) should support UDP messages of 1220 bytes.
- <A-87>: Authoritative server (security-compliant) should support UDP messages of 4000 bytes.

■ Case Study 6: Detailed Experimental Results

▼ Make queries to the full-service resolver (with a signature).

○ Verification item <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.

1. Make queries whose response results will exceed 512 bytes to the full-service resolver.

- Make queries by adding a <+dnssec> option to the dig command.
- Add the full-service resolver's address after @.
- Specify a zone name for the signature zone.
- Specify <DNSKEY> for a record type. Verify the following.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are included in the response.
- Verify that the data volume of the response results (MSG SIZE rcvd:) exceeds 512 bytes.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.
- Verify that the udp of the OPT PSEUDOSECTION section of the response results shows 4096.

2. Perform queries by adding the <+bufsize=512> option.

Verified the following item:

- Verify that <; Truncated, retrying in TCP mode> is shown just below the results of the dig command. This is because the data volume of the server's response to the query exceeded the maximum size of the UDP specified by the PC.

○ Verification item <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.

Make queries whose response results will exceed 1220 bytes to the full-service resolver.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are included in the response.
- Verify that the data volume of MSG SIZE rcvd: exceeds 1220 bytes.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.

○ Verification item <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.

By setting another full-service resolver (Fedora10, BIND-9.7.0rc1) locally, ensure that the MSG SIZE will exceed 4000 bytes.

Verified the following item:

- Verify that normal response could be obtained for queries whose response results may exceed 4000 bytes.

▼ Make queries to the full-service resolver (without a signature).

○ Verification item <F-85>: Full-service resolver (security-compliant) should have a UDP communication capability via EDNS0.

1. Make queries whose response results will exceed 512 bytes to the full-service resolver.

- Make queries by adding a <+dnssec> option to the dig command.
- Add the full-service resolver's address after @.
- Specify a zone name without a signature.
- Specify <DNSKEY> for a record type. Verify the following.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are not included in the response.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.
- Verify that the udp of the OPT PSEUDOSECTION section of the response results shows 4096.

○ Verification item <F-86>: Full-service resolver (security-compliant) should support UDP messages of 1220 bytes.

Could not verify this because there was no signature and it was not possible to make the MSG SIZE larger.

○ Verification item <F-87>: Full-service resolver (security-compliant) should support UDP messages of 4000 bytes.

Could not verify this because there was no signature and it was not possible to make the MSG SIZE larger.

▼ Make queries to the authoritative server (with a signature).

- ○ Verification item <A-85>: Authoritative server (security-compliant) should have a UDP communication capability via EDNS0.

1. Make queries whose response results will exceed 512 bytes to the authoritative server.

- Make queries by adding a <+dnssec> option to the dig command.
- Add the authoritative server's address after @.
- Specify a zone name for the signature zone.
- Specify < DNSKEY> for a record type.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are included in the response.
- Verify that the data volume of the response results (MSG SIZE rcvd:) exceeds 512 bytes.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.
- Verify that the udp of the OPT PSEUDOSECTION section of the response results shows 4096.

2. Perform queries by adding the <+bufsize=512> option.

Verified the following item:

- Verify that <; Truncated, retrying in TCP mode> is shown just below the results of the dig command. This is because the data volume of the server's response to the query exceeded the maximum size of the UDP specified by the PC.

- Verification item <A-86>: Authoritative server (security-compliant) should support UDP messages of 1220 bytes.

Make queries whose response results will exceed 1220 bytes to the authoritative server.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are included in the response.
- Verify that the data volume of MSG SIZE rcvd: exceeds 1220 bytes.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.

- Verification item <A-87>: Authoritative server (security-compliant) should support UDP messages of 4000 bytes.

Could not verify this because the test was not possible without setting up another authoritative server locally.

▼ Make queries to the authoritative server (without a signature).

○ Verification item <A-85>: Authoritative server (security-compliant) should have a UDP communication capability via EDNS0.

1. Make queries whose response results will exceed 512 bytes to the authoritative server.

- Make queries by adding a <+dnssec> option to the dig command.
- Add the authoritative server's address after @.
- Specify a zone name for the authoritative zone.
- Specify < DNSKEY> for a record type.

Verified the following items:

- Verify that DNSKEY records and RRSIG records for the zone are included in the response.
- Verify that <; Truncated, retrying in TCP mode> is not shown just below the results of the dig command.
- Verify that the udp of the OPT PSEUDOSECTION section of the response results shows 4096.

2. Perform queries by adding the <+bufsize=512> option.

Verified the following item:

- Verify that <; Truncated, retrying in TCP mode> is shown just below the results of the dig command. This is because the data volume of the server's response to the query exceeded the maximum size of the UDP specified by the PC.

○ Verification item <A-86>: Authoritative server (security-compliant) should support UDP messages of 1220 bytes.

Could not verify this because there was no signature and it was not possible to make the MSG SIZE larger.

○ Verification item <A-87>: Authoritative server (security-compliant) should support UDP messages of 4000 bytes.

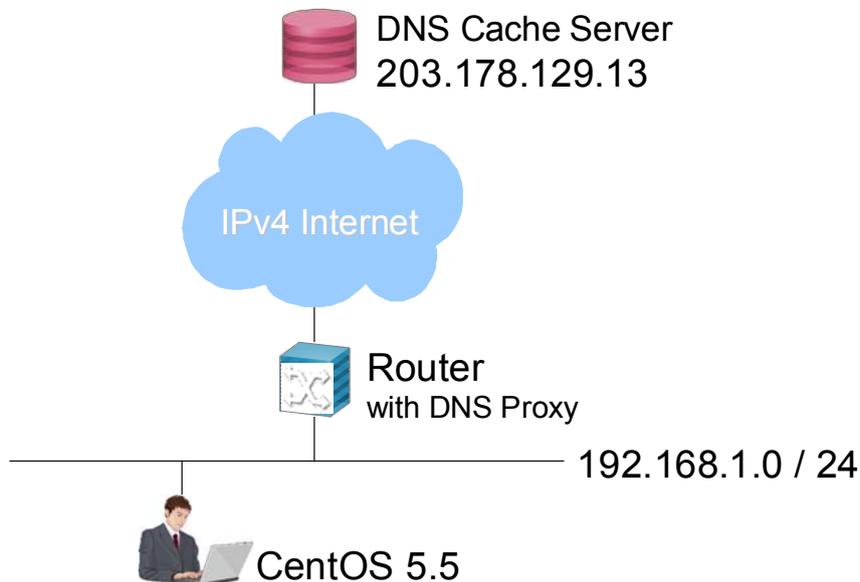
Could not verify this because there was no signature and it was not possible to make the MSG SIZE larger.

■ Case Study 6: Obtained Findings

Although some verification items could not be tested, our findings generally suggest that the router's filter and transfer functions do not interfere with the DNSSEC communication for a full-service resolver and an authoritative server with or without a signature.

Verification of Functionality: Case Study 7

■ Case Study 7: Experimental Environment



■ Case Study 7: Summary of Experimental Results

Verification of the DNS Proxy function for in-house broadband routers (for corporate and private use) was conducted in reference to <F-85>, <F-86> and <F-87> of the “DNSSEC Verification of Functionality: Procedure Manual” and the [RFC5625] DNS Proxy Implementation Guidelines.

■ Case Study 7: Detailed Experimental Results

(1) Verification was conducted to see whether the devices could process OPT RR and various flags transparently.

=> It was verified that all devices were normal.

(2) Verification was conducted to see whether the devices were EDNS0-compliant and could process packets of 1,220 bytes properly.

=> It was verified that some devices could not process properly.

(3) Verification was conducted to see whether the devices were EDNS0-compliant and could process packets of 4,000 bytes properly.

=> It was verified that some devices could not process properly.

(4) Verification was conducted to see whether the TCP Fallback was functioning properly.

=> It was verified that the TCP Fallback was not functioning properly for some devices.

(5) Verification was conducted to see the impact of the DNS cache on the devices.

=> It was verified that the DNS cache impacted on some devices negatively.

■ Case Study 7: Obtained Findings

It was verified that packets exceeding 512 bytes could not be processed by some devices and that there were some conditions in which the DNSSEC validation could not be conducted in the case of a cache implementation only for specific RRs.

Although it is desirable to implement a cache function not only for specific RRs but also for all kinds of RRs, we think that it is realistic not to implement a cache function itself as there are too many things to consider.

(1) Issue of not being able to process packets exceeding 512 bytes

Although the packet size is cut down to 512 bytes for the transfer when response packets exceeding 512 bytes are received, the stub resolver cannot fallback to TCP as packets are transferred using “TC=0.”

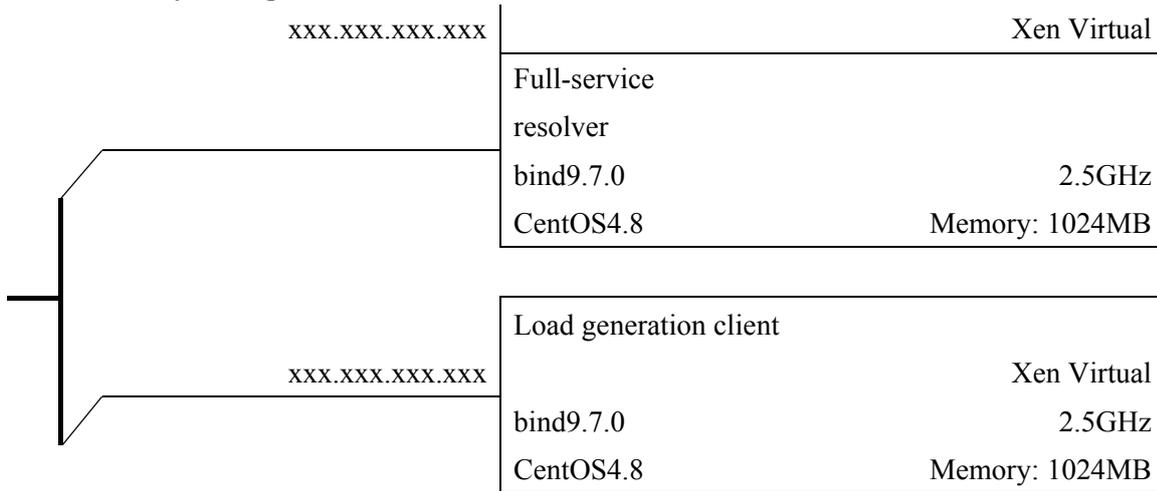
(2) Issue of the cache implementation for specific RRs only

In the cache implementation for specific RRs only, the RRSIG RRs cannot be cached. In this condition, the DNSSEC validation cannot be conducted until the cache entries expire (TTL expiry) because only cached RRs are returned as a response when queries are sent from other devices.

Results of Performance Verification

Performance Verification: Case Study 1

■ Case Study 1: Experimental Environment

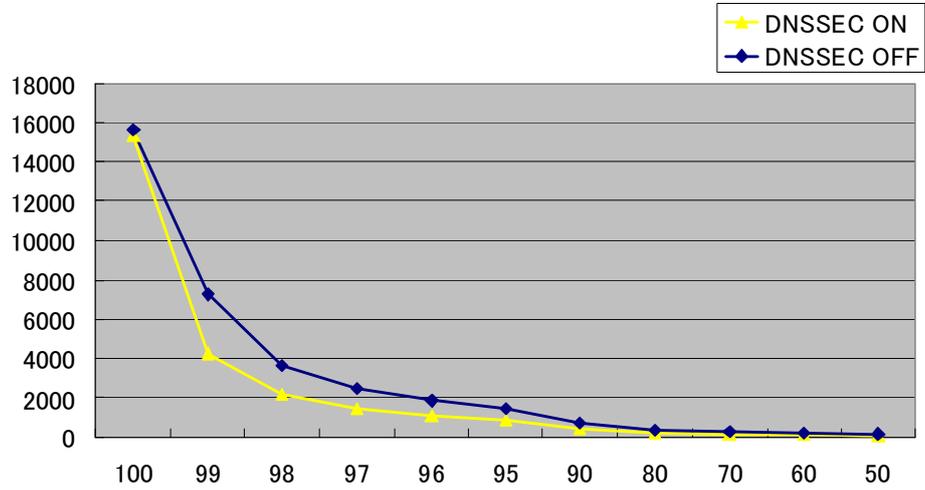


■ Case Study 1: Summary of Experimental Results

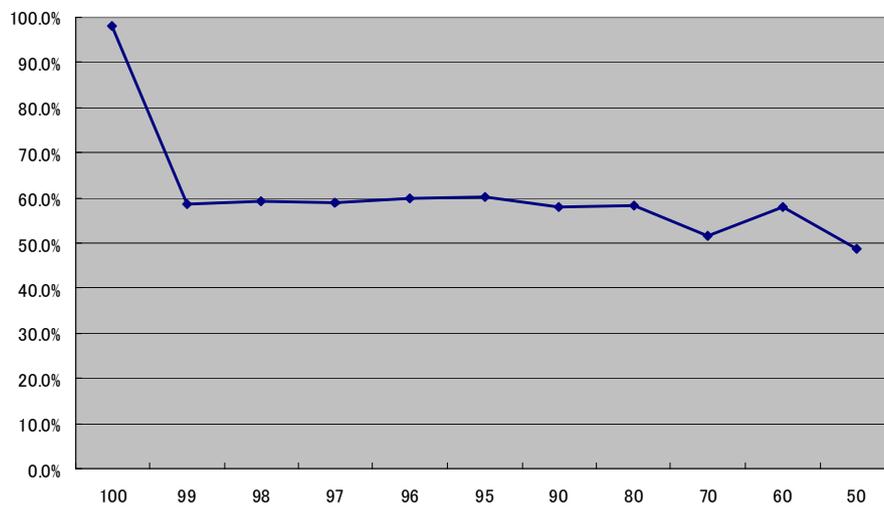
It was verified that the full-service resolver's CPU usage rate and memory usage increased and the query processing capability decreased by enabling DNSSEC.

■ Case Study 1: Detailed Experimental Results(1)

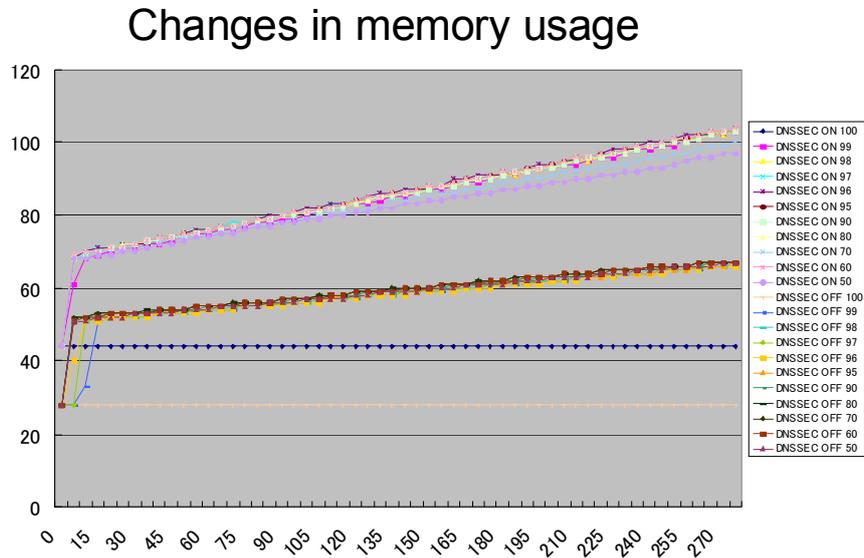
qps per cache hit rate



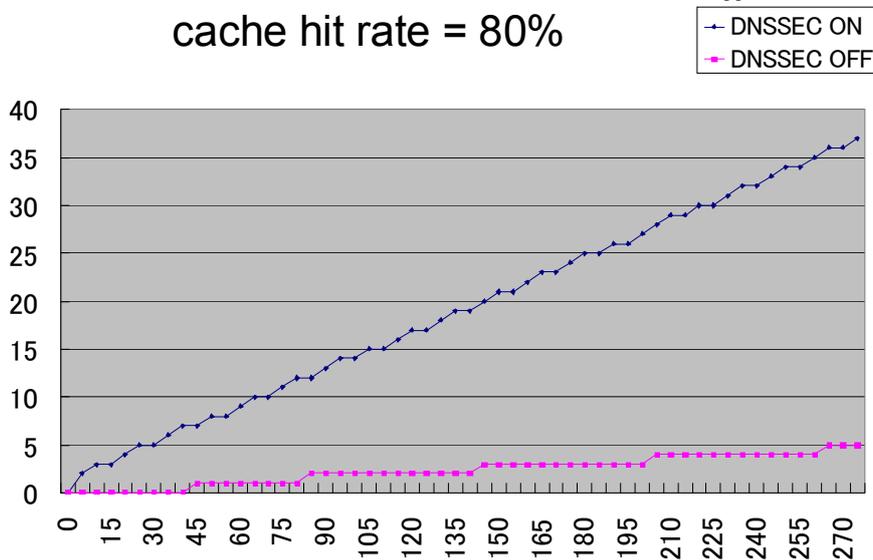
qps rate: DNSSEC ON/OFF



■ Case Study 1: Detailed Experimental Results(2)



Change in memory increase: 100 qps,
cache hit rate = 80%



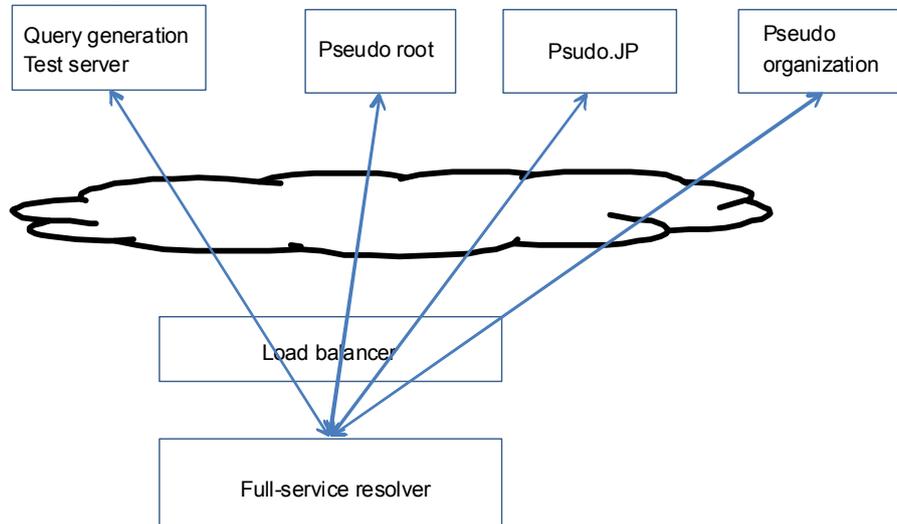
■ Case Study 1: Obtained Findings

The memory usage increased by eight times when NSEC3 was used and the query results were mostly “NXDOMAIN.”

The query processing capability decreased to 60% when DNSSEC was ON.

Performance Verification: Case Study 2

■ Case Study 2: Experimental Environment



Functionality	HW	Application	Note
Full-service resolver	SUN X2100 Solaris10	bind-9.7.0	IPv4 only
Load balancer	A10networks AX2500		IPv4 only
Query generation	SUN NetraT1	queryperf (modified version)	IPv4 only

■ Case Study 2: Summary of Experimental Results

The following tests were conducted using a cache server based on the “5. Measurement Procedures” in the “DNSSEC Performance Verification: Procedure Manual (Ver. 1.1)” by JPRS.

5. Measurement Procedures

5.1. Measurement of Behavioral Changes for Various Patterns of the Validator

a) DNS name resolution by a <dig> command and verification of the DNSSEC validation

1. The following configurational changes should be made depending on the pattern.

- Changes to the network configuration of the validator server (MTU, TCP, fragment)
- Changes to the configuration file of the validator server (DO=0/1, TA configuration)
- Changes to the zone data which will be configured in the authoritative server (ZSK=1024/2048, without a signature)

2. After the above configurational changes are made, verifications should be conducted on the validator server by using the following <dig> commands when both the validator and

authoritative servers are in operation. It should be verified whether the name resolution and the validation are successful or not by looking at the output results of the <dig> command.

Without a signature:

```
dig @localhost example.jp. A
```

With a signature:

```
dig @localhost +dnssec example.jp. A
```

- b) The validator load and the queries to the authoritative server should be measured for the pattern with the name resolution.
1. As in a), the network and server configurations should be changed depending on the pattern.
 2. The load measurement tool (*) should be activated on the validator server and the CPU usage rate and the memory usage should be measured.
* Scripts to measure the CPU usage rate, memory usage, load average, etc. should be prepared.
 3. DSC (DSC Collector) should be activated on the validator and authoritative servers.
 4. Load tests by queryperf (modified version) should be conducted on the query generator.
Commands should be changed by DO bits.

Transmission intervals should be specified on the millisecond time scale for the <-i> option. In the following example, the transmission interval was “10,000 qps” as “0.1ms” was specified.

```
DO=0
```

```
queryperf -d query.txt -s 192.0.2.1 -l 300 -i 0.1
```

```
DO=1
```

```
queryperf -d query.txt -s 192.0.2.1 -D -l 300 -i 0.1
```

5. After the load tests are finished, the load measurement tool/DSC should be turned off on the validator and authoritative servers.

In the above procedures, switching of patterns during the validation and measurements should be conducted as follows.

■ Case Study 2: Detailed Experimental Results

RE: “5.1. a)-1.” of the Measurement Procedures

- The network configurational changes (MTU, TCP, fragment, etc.) were not conducted because the experimental environment coexisted with the production environment and the changes could not be made.
- With regard to the configuration file change of the validator, behavioral changes were monitored with and without the TA configuration.
- The tests were not conducted for the authoritative server because it was not set up.

RE: “5.1. b)” of the Measurement Procedures

A test query by queryperf which would not cause a cache hit for five consecutive minutes could not be prepared. Therefore the load to the server due to the DNSSEC validation decreased to the level which was lower than expected after a while, which was believed to be due to the cache hit. Consequently, a prominent difference in the load to the server could not be identified with or without the DNSSEC validation.

However, it was verified that the cache size was more than doubled when accessed a pseudo tree with a signature compared to when accessed a pseudo tree without a signature.

■ Case Study 2: Obtained Findings

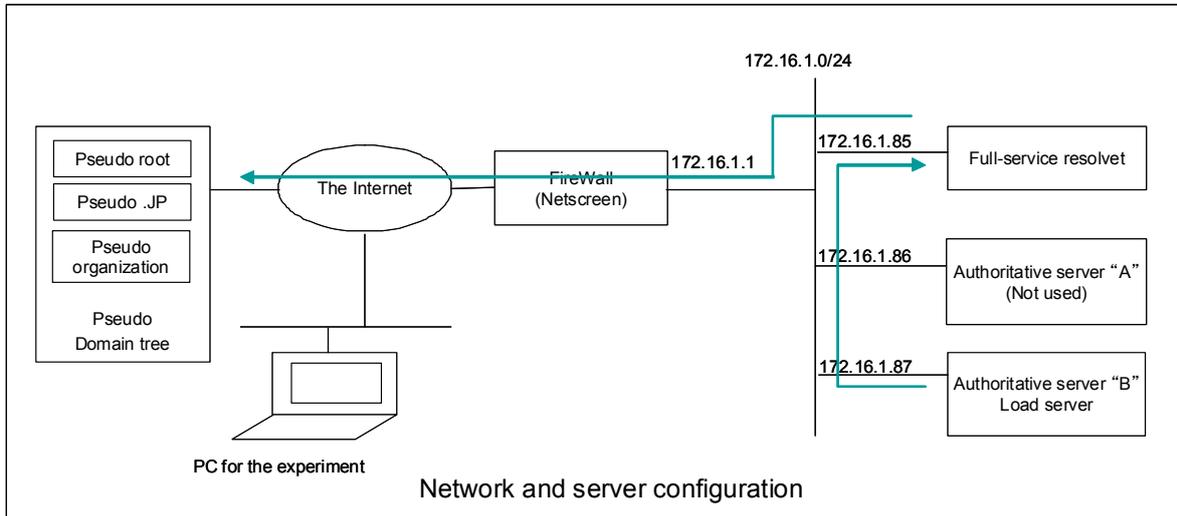
A prominent difference in the server load could not be identified with or without the DNSSEC validation.

However, as the cache size is expected to be more than double when DNSSEC is on, we think that it is necessary to replace servers, as appropriate, in light of the server load and the processing capability of servers in the service environment.

Performance Verification: Case Study 3

■ Case Study 3: Experimental Environment

• Experimental Environment Configuration



- Software configuration:
OS:Solaris10 BIND:9.7.0-P1
- Load tool:
queryperf dnssperf

■ Case Study 3: Summary of Experimental Results

<Experiment Procedures>

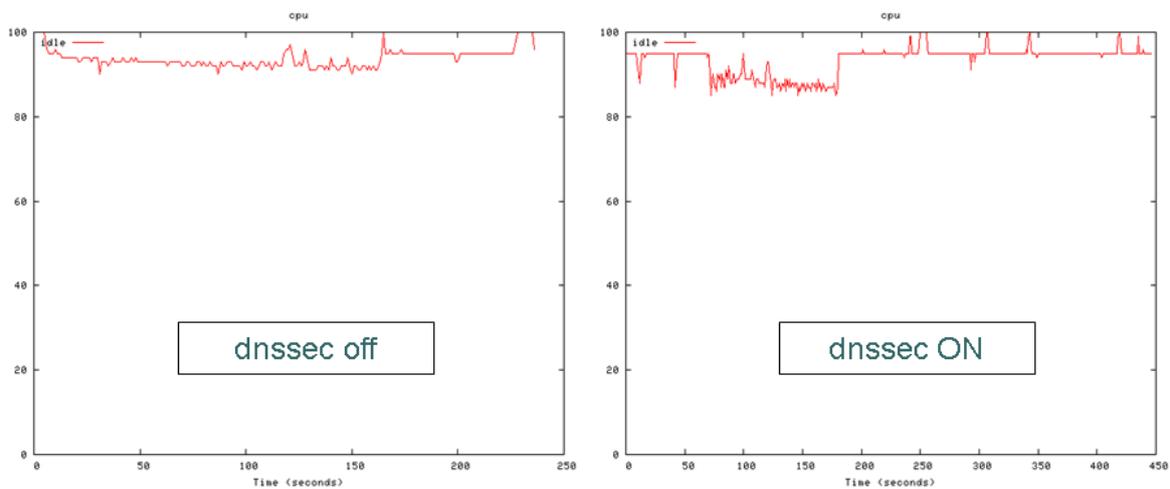
- Processing status is monitored by deploying “dnssperf/queryperf” in the testing device and loading the full-service resolver.
- The DNS query information is obtained as a sample and processed into a data format suitable for the test.
- 100,000 records are used as a data for the test. (Not all of the records are uniq.)
- “vmstat” and “top” are used to measure the performance.

<Result>

- The load to the full-service resolver and the memory usage increased due to the processing of the DNS request for DNSSEC.

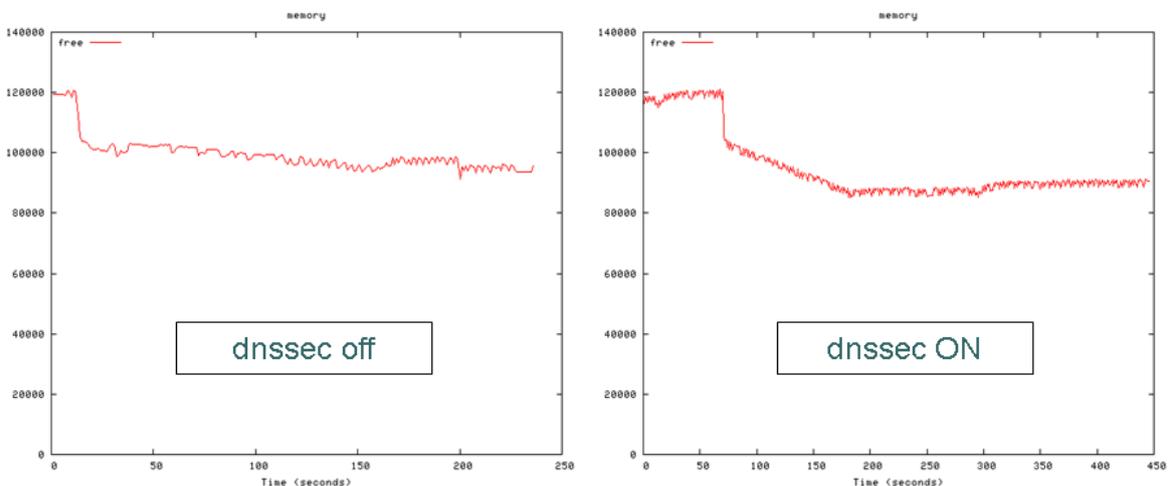
■ Case Study 3: Detailed Experimental Results

- Comparison on the CPU value: dnssec On/Off



It was verified that the CPU load increased when DNSSEC was on compared to when DNSSEC was off. (Due to the band width restrictions of the upper network, the processing number of DNS decreased and the full CPU capability could not be utilized.)

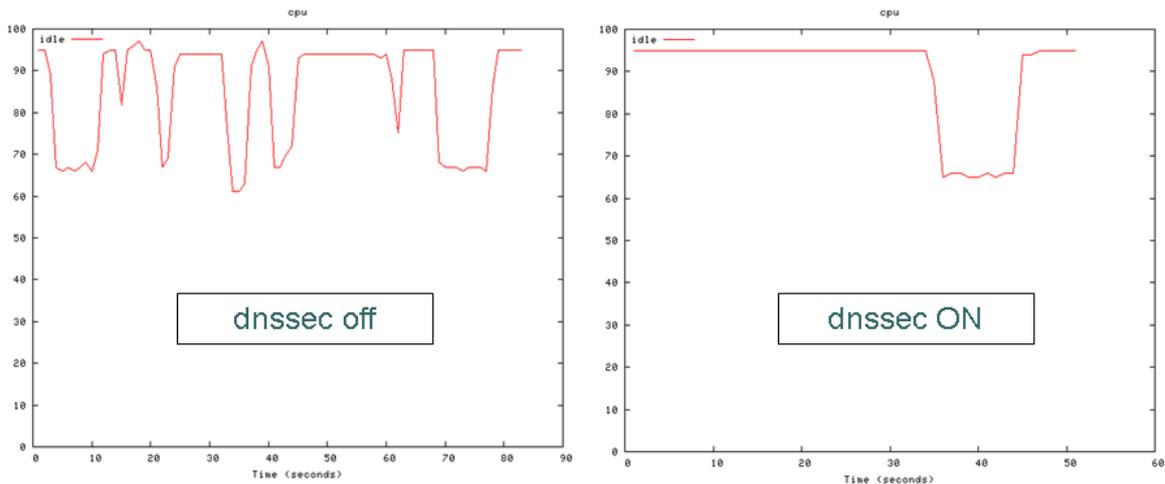
- Comparison of the memory value: dnssec On/Off



A prominent difference in memory consumption was not observed when DNSSEC was on compared to when DNSSEC was off.

(There is a possibility that the difference in data was not observed because the number of <uniq> queries used for the test was too few.)

- Comparison of CPU: full cache



The CPU load with the cache hit rate of 100% showed the same value when DNSSEC was on and when DNSSEC was off.

It seemed that there is only little (or no) impact of the DNSSEC validation on cached information.

■ Case Study 3: Obtained Findings

No significant differences due to the testing environment or restrictions of network configurations were observed as a result of the performance comparison in the testing environment.

However, it was verified that the load increased marginally when DNSSEC was on as a result of this experiment.

Since the load to the full-service resolver changes depending on the DNSSEC usage rate, we think that it is necessary to monitor the following for the full-service resolver to be used for service on an ongoing basis and reinforce and expand the system.

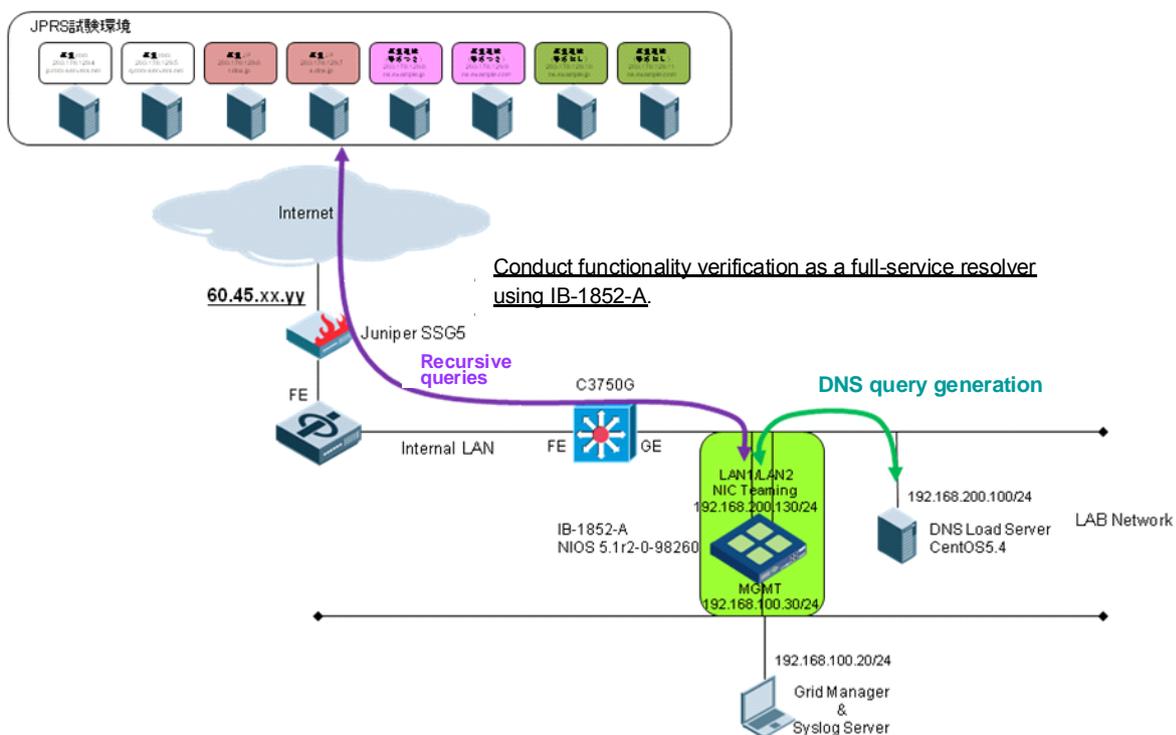
- Memory usage
- Cache hit rate
- Server CPU usage
- Network band width usage
- Number of connections

Furthermore, a prominent difference in performance was observed due to the cache hit rate when DNSSEC was on compared to when DNSSEC was off.

It seemed that it is necessary to consider avoiding busy hours when stopping/starting the server (or clearing cache). It is also necessary to establish a method for warming up.

Performance Verification: Case Study 4

■ Case Study 4: Experimental Environment



DNS APPLIANCE DEVICE: Infoblox 1852-A Network Service Appliance

Software version: NIOS 5.1r2-0-98260 * NIOS = Name of the internal OS of the Infoblox appliance

■ Case Study 4: Summary of Experimental Results

▼ The impact on appliance load was verified with the cache hit rate of 100% with and without the DNSSEC validation. The test was conducted by sending a test query (www.xxx.co.jp A) of 100 unique domains from a Linux load generation server to the IB-1852-A DNS cache server by using “queryperf.”

The test was conducted only for the IPv4 address by using the RSA 2024 bit-type testing environment of a pseudo tree under the DNS technology experimental environment.

* Verification items in accordance with the “DNSSEC Performance Verification: Procedure Manual (Ver. 1.2) were not conducted.

▼ Experimental result:

With regard to the degree of impact on performance of a cache server, it was verified that the performance was down by approximately 13% when the DNSSEC validation was on compared to when the DNSSEC validation was off.

It was also verified that the performance was impacted by the additional message size of the RRSIG record for the DNS query response.

■ Case Study 4: Detailed Experimental Results

▼ IB-1852-A, without the DNSSEC validation, 100% cache hit rate

Queryperf, without the <-D> option

1st time: 141238.4 qps Appliance CPU load average: 81%
2nd time: 142645.4 qps Appliance CPU load average: 84%
3rd time: 142131.4 qps Appliance CPU load average: 83%
4th time: 141813.0 qps Appliance CPU load average: 82%
5th time: 141439.3 qps Appliance CPU load average: 82%

Without the DNSSEC validation, example of a <dig> response

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.e15_4.2 <<>> @192.168.200.130 www.xxxxx.co.jp A
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10029
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.xxxxx.co.jp.          IN      A

;; ANSWER SECTION:
www.xxxxx.co.jp.          861     IN      A       192.0.2.1

;; Query time: 0 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 24 20:44:34 2010
;; MSG SIZE  rcvd: 49
```

▼IB-1852-A, with the DNSSEC validation, 100% cache hit rate

queryperf, with the <-D> option

1st time: 123276.8 qps Appliance CPU load average: 83%
2nd time: 123065.5 qps Appliance CPU load average: 82%
3rd time: 123418.6 qps Appliance CPU load average: 84%
4th time: 122981.4 qps Appliance CPU load average: 81%
5th time: 123616.6 qps Appliance CPU load average: 84%

Without the DNSSEC validation, example of the <dig> response

```
<<>> DiG 9.3. 6-P1-RedHat-9.3. 6-4.P1.e15_4.2 <<>> +dnssec @192.168.200.130 www.xxxxx.co.jp A
; (1 server found)
;; global options: printcmd
```

```

;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 25119
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.xxxxx.co.jp.          IN      A

;; ANSWER SECTION:
www.xxxxx.co.jp.          666     IN      A      192.0.2.1
www.xxxxx.co.jp.          666     IN      RRSIG   A 8 4 900 20101225225717 20091225215717
24018 xxxxx.co.jp. GPTQObu3iCAksBwl5qAo+epHdEulfnA8dYW6MWGWLptfwMpZ/nJaYnur
GKc2MQh6zD5Q8RFFpdZrXWOWrqW9W8ffry5mmrdaEQxhSibmsoshw3GA
ymaM/J9F1UAFnQFPKLLHCGJUtdMbMxD5LtxaSBwRI07rZFyGKPYeXgs2 HHs=

;; Query time: 0 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 24 20:41:58 2010
;; MSG SIZE rcvd: 231

```

(*Reference: shell scripts used for the test)

```

#!/bin/sh
SECS=300
INPUT=cached_test.data
SERVER=192.168.200.130
NUM=60
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out1 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out2 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out3 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out4 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out5 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out6 2>&1 &
wait
grep 'Queries per' out? | awk 'BEGIN { sum=0; } { sum += $5; } END { printf("Total:
%.1f qps\n", sum); }'

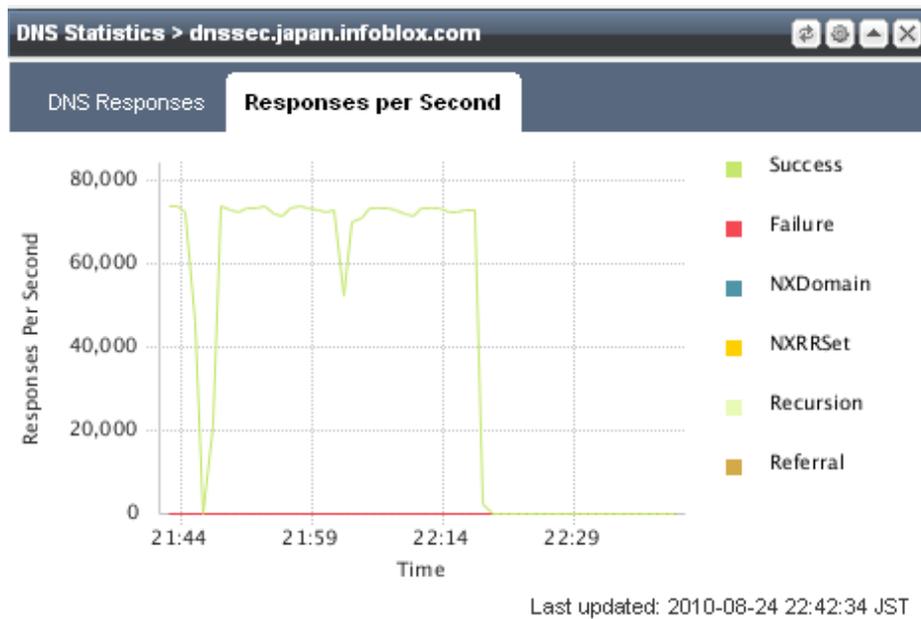
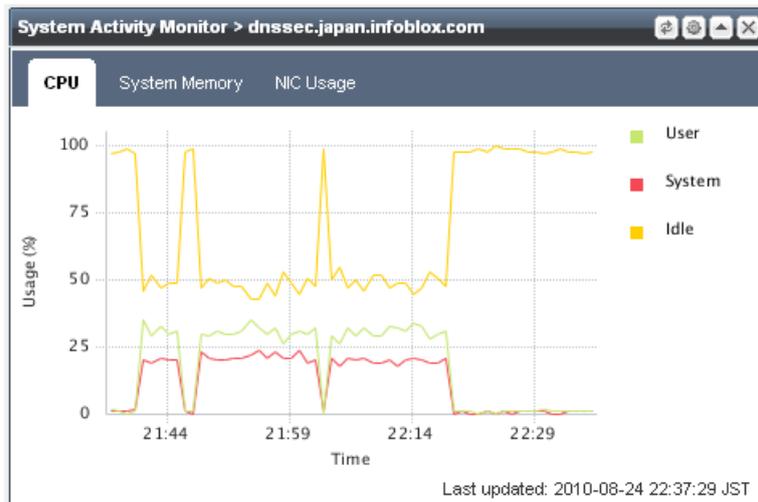
```

■ Case Study 4: Obtained Findings

This experiment was conducted with the cache hit rate of 100% and with and without the DNSSEC validation. When deploying DNSSEC into the production environment, it was necessary to examine the impact on performance of the cache server in consideration of the rate of incursive queries, average size of responses when the DNSSEC validation is on, etc.

(Reference)

NOIS (5.1r2 and above) has an expanded function and users can check the CPU/Memory/NIC usage rate and DNS query response statistics in a graph on the Infoblox Grid Administration page.



Performance Verification: Case Study 5

Changes in the load to the authoritative DNS server with the DNSSEC validation

■ Case Study 5: Experimental Environment

Two types of hardware were prepared for the DNS server. One server was relatively new and the other was relatively old.

	CPU	OS
Server “A”	Xeon E5540 (2.53GHz) × 2	CentOS 5.5
Server “B”	Pentium-III 1.26GHz	FreeBSD 8.0

Changes in response performance were measured with and without DNSSEC by activating BIND 9.7.x (“named”) in these servers and measuring the response performance with the load by <dnperf> from another server connected to the LAN. Furthermore, the NSEC method and the NSEC3 method were compared when DNSSEC was on.

Changes in the load to the authoritative DNS server with the DNSSEC validation

Data used for the measurement:

- Zone data to be measured
The zone data of a small-scale domain name in actual operation (total number of resource records = 244) was used almost as is.
- Query data used for <dnperf>
The data which was generated from the query log to the DNS server in the aforementioned zone
 - Although actual queries were used, DNSKEY queries, were also included because the DLV environment was used for the DNSSEC validation.
- DNSSEC parameters
 - Encrypted algorithm: RSASHA256
 - KSK key length: 2048 bits
 - ZSK key length: 1024 bits

■ Case Study 5: Experimental Results

Result 1: Comparison of response performance in each method (Unit: number of queries per second)

	Method	Server "B" (Pentium-III)		Server "A" (E5540)	
		Existence	Denial of existence	Existence	Denial of existence
Without DNSSEC	N/A	9345	8855	58423	58248
With DNSSEC	NSEC	8352	7433	57279	56642
	NSEC3	7309	3364	57122	41437

Existence: Existing domain names were extracted from the query logs.

Denial of existence: Authenticated denial of existence records generated from existence

Iterations of NSEC3: 5

The CPU usage rate of Server "A" was around 30 to 45%. Although the server in which <queryperf> was activated had the same specs with Server "A," there is a possibility that sufficient amount of the load could not be generated because <dnperf> is a single thread. Therefore, it can be assumed that maximum capabilities of Server "A" were higher. The CPU usage rate for Server "B" was 100% for every test and it was verified that the amount of the load was sufficient.

Result 2: Average DNS response size for each method

	Method	Normal	Existence	Denial of existence
Without DNSSEC	N/A	115	115	112
With DNSSEC	NSEC	602	598	648
	NSEC3	637	604	884

Normal: The query logs were applied as is. (Denial of existence rate: approximately 8%)

Existence: Existing domain names were extracted from the query logs. (including DNSKEY)

Denial of existence: Authenticated denial of existence records generated from existence

As a reference, the DNS query size was 45 bytes on average.

■ Case Study 5: Obtained Findings

The response performance of the authoritative DNS server decreased to a certain degree when DNSSEC

was on. The rate of decrease was around 10 to 20% for the response of existing names. The denial of existence response of NSEC3, in particular, could cause more than 50% of drop in processing capability.

The number of DNS response packets from the authoritative DNS server increased by five to eight times as a result of the DNSSEC validation.

Performance Verification: Case Study 6

Changes in response performance of the NSEC3 method in accordance with the number of iterations

It is known that when the NSEC3 method is used for the DNSSEC validation, the load to the server increased in response to the number of iterations. The test was conducted to measure such changes. The measurement environment was as described in the previous section. The number of iterations was increased from 0 to 100 in sequence when generating zone data , <named> was set, and the response performance by the <queryperf> command was measured repeatedly.

■ Case Study 6: Experimental Environment

The experimental environment was the same as that of the “Performance Verification: Case Study 5.”

■ Case Study 6: Experimental Results

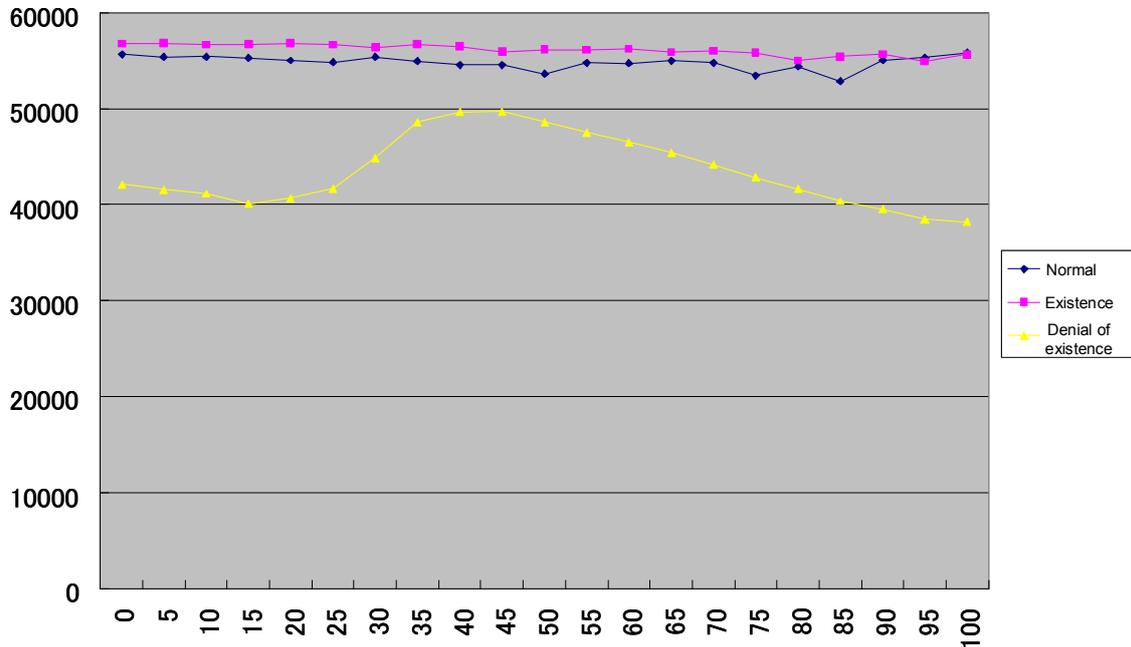
“Normal,” “Existence,” and “Denial of existence” in the following graphs refer to the following.

Normal: The query logs were applied as is. (Denial of existence rate: approximately 8%)

Existence: Existing domain names from the query logs were used. (including DNSKEY)

Denial of existence: Queries of the authenticated denial of existence records generated from existence

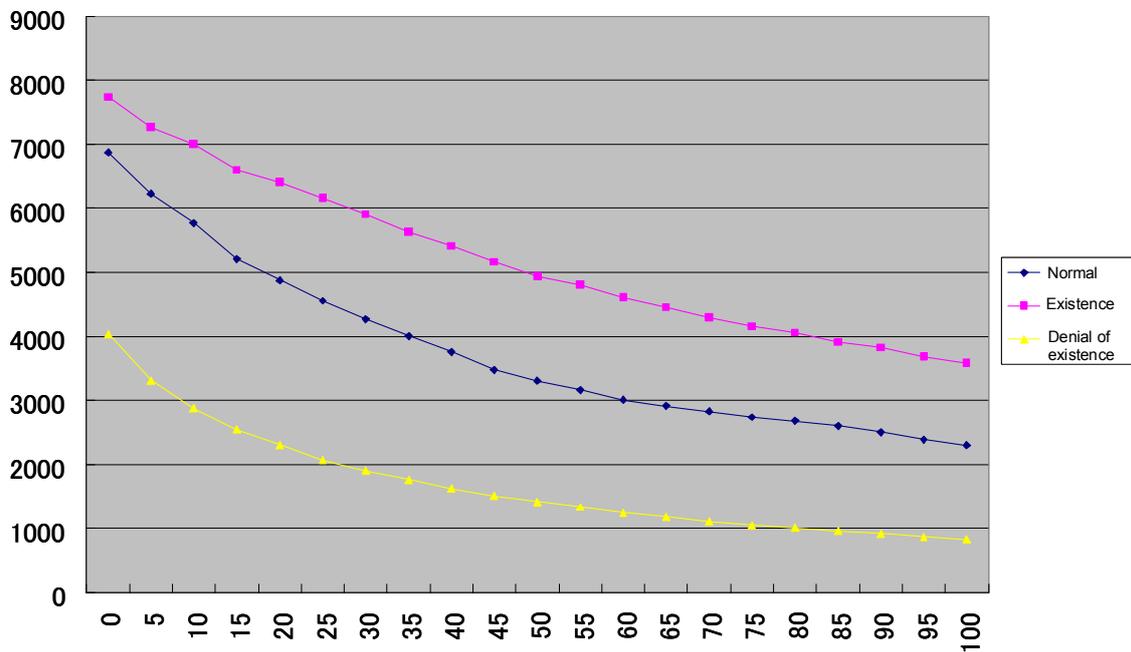
Iterations and changes in response performance for Server “A”



X-axis: Iterations; Y-axis: Response performance (qps)

During the measurement, the maximum CPU occupancy rate of <named> of Server “A” reached approximately 90% (for a response of denial of existence for 100 iterations.) Furthermore, changes in response performance of denial of existence in accordance with the changes in the number of iterations showed similar results. Although it was unnatural, we assume that it was caused by some kind of impact such as CPU characteristics.

Changes in iterations and response performance for Server “B”



X-axis: Iterations; Y-axis: Response performance (qps)

It was verified that the existence response performance of Server “B” deteriorated in accordance with the increase in the number of iterations. We assume that it was impacted by the fact that NSEC3 needs to calculate hash even for the existence responses.

■ Case Study 6: Obtained Findings

It is not desirable to make the number of iterations for the NSEC3 method extremely large because it could negatively impact the response performance. We think that “10” should cause no material impact.

This report was jointly authored by the following companies and all rights including copyright are reserved by each of these companies.

Infoblox Inc.

NEC AccessTechnica, Ltd.

NEC BIGLOBE, Ltd.

NTT Communications Corporation

KDDI CORPORATION

So-net Entertainment Corporation

Japan Registry Services Co., Ltd.

Yamaha Corporation