Pre-Delegation Testing

DNS Delegation Test Cases

Version K

File name: PDT_DNS_TC_Delegation.docx
Last saved: 2015-07-15

Document control

Document information and security

Made by	Responsible for fact	Responsible for document
Patrik Wallström	Patrik Wallström	Patrik Wallström

Security class	File name
External	PDT_DNS_TC_Delegation.docx

Revisions

Date	Version	Name	Description
2013-01-24	PA1	Patrik Wallström	Initial document
2013-04-08	B	Staffan Hagnell	Delivery D2 for production
2013-04-18	PC1	Patrik Wallström	Updated DNS04
2013-04-24	D	Patrik Wallström, Mats Dufberg	Updated wording in DNS04
2013-05-03	E	Mats Dufberg	Released
2013-06-04	F	Patrik Wallström, Mats Dufberg	Minor change in document structure
2013-07-01	G	Patrik Wallström, Mats Dufberg	Improved wording on fail criteria in the expected outcome sections. Changed from warning to fail in DNS04.
2013-07-08	H	Mats Dufberg	Changed the PASS criterion in DNS04. Released.
2013-07-25	I	Mats Dufberg, Mårten Frosth	Clearified DNS04 that the requirement is per network protocol type (IPv4 and IPv6). Minor updates of wording. Updated DNS04 with the test against the RIPE RIS database if the Cymru feed only reports one AS.
2013-09-19	J	Mats Dufberg, Mårten Frosth	Corrected text in DNS24.
2015-07-15	K	Mats Dufberg	DNS04 is updated to align with IANA requirements. Date of enforcement added in section 1.5.

LIST OF CONTENTS

1. Introduction

1.1 Scope

The Pre-Delegation Testing Provider will test the DNS service for the designated zone and verify the resulting answers. The test cases described in this document are all done using DNSCheck with the same set of input parameters.

1.2 References

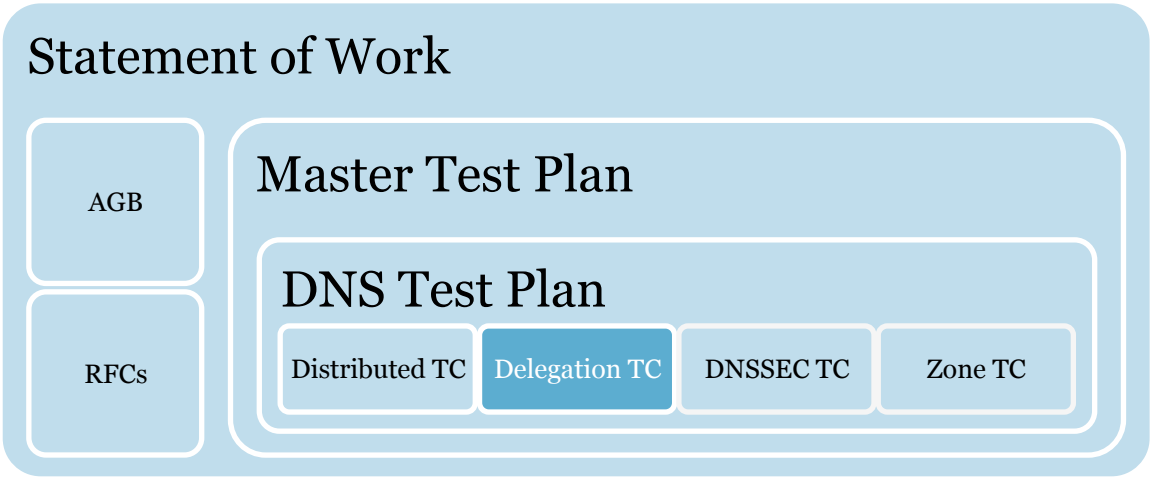
1.2.1 External

- IEEE 829-2008
- ICANN gTLD Applicant Guidebook, Version 2012-06-04
- IANA document "Technical requirements for authoritative name servers".[1]
- IANA document "Placing TLD delegation signer information in the root zone".[2]

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Pre-Delegation Testing, Master Test Plan
- Pre-Delegation Testing, DNS Test Plan

1.2.3 Document Hierarchy



1.3 Context

All tests are to be performed over IPv4 and IPv6 from at least five points on the Internet. At least one probe node should be located in every ICANN region.

1.4 Notation for description

Each test case for the DNS service is described in their own section. The test procedures are described directly in the test case.

[1] http://www.iana.org/procedures/nameserver-requirements.html per 2012-12-18
[2] http://www.iana.org/procedures/root-dnssec-records.html per 2012-12-18

1.5 Enforcement

This version of this document (version K) is enforced at 2015-08-31. Prior to that date, see previous version of this document.

2. Minimum number of name servers

2.1 Test case identifier

DNS01 Minimum number of name servers

2.2 Objective

There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

This test case fulfills the requirement 2.1.1 in the "Technical requirements for authoritative name servers" document.

2.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
TLD	The ASCII compatible name of the TLD	String
DnsNameServer-[1..n]	FQDN of authoritative name server	String
DnsGlueRecord-[1..n]	All IPv4 or IPv6 addresses for auth NS	String

The above input is also considered to be the exact same information that is sent to IANA for inclusion in the root zone. IANA will only publish the subordinate host glue records in the root zone.

2.4 Outcome(s)

There must be at least two name servers in the input delegation data. If there are less than two distinct IPv4 addresses for the delegated name servers, the message DELEGATION:TOO_FEW_NS_IPV4 is generated and this test case fails.

There must be at least two distinct IPv6 addresses for the delegated name servers. If there are less than two distinct IPv6 addresses, the message DELEGATION:TOO_FEW_NS_IPV6 is generated and this test case fails.

There must be at least two NS records for the delegation. If there are less than two NS records, the message DELEGATION:TOO_FEW_NS is generated and this test case fails.

2.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

2.6 Special procedural requirements

This test has no procedural requirements.

2.7 Intercase dependencies

This test has no intercase dependencies.

2.8 Ordered description of steps to be taken to execute the test case

An NS query is made to all listed name servers for the designated zone. The NS records in the answer are compared with the parent zone (from the input data). If the total number of common NS records between parent and zone is less than two the DELEGATION:TOO_FEW_NS message is generated.

The IP addresses of all NS records are collected. If the total count of distinct IPv4 addresses is below 2 the message TOO_FEW_NS_IPV4 is generated. If the total count of distinct IPv6 addresses is below 2 the message TOO_FEW_NS_IPV6 is generated. If the total of common NS records in the delegation from both the parent and the child zone is below 2, the message DELEGATION:TOO_FEW_NS is also generated.

3. Name server reachability

3.1 Test case identifier

DNS02 Name server reachability

3.2 Objective

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53.

This test case fulfills the requirements 2.3.1 in the "Technical requirements for authoritative name servers" document, and the requirements on TCP and UDP of section 5.2 in the Applicant Guidebook.

3.3 Inputs

See section 2.3 in this document.

3.4 Outcome(s)

If any query is failing to get an answer, the error message NAMESERVER:NO_UDP and NAMESERVER:NO_TCP is generated and this test case fails.

3.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 must be authoritative for the designated zone.

3.6 Special procedural requirements

This test has no procedural requirements.

3.7 Intercase dependencies

This test has no intercase dependencies.

3.8 Ordered description of steps to be taken to execute the test case

A SOA query is sent over UDP and TCP to all the listed nameservers. If any query fails to give an answer, either the message NAMESERVER:NO_UDP or NAMESERVER:NO_TCP is generated.

4. Answer authoritatively

4.1 Test case identifier

DNS03 Answer authoritatively

4.2 Objective

The name servers must answer authoritatively for the designated zone. Responses to queries to the name servers for the designated zone must have the “AA”-bit set.

This test case fulfills the requirements 2.4.1 and 2.4.2 in the “Technical requirements for authoritative name servers” document.

4.3 Inputs

See section 2.3 in this document.

4.4 Outcome(s)

If any name server answers without the AA-bit, the error message NAMESERVER:NOT_AUTH is generated and this test case fails.

4.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

4.6 Special procedural requirements

This test has no procedural requirements.

4.7 Intercase dependencies

This test has no intercase dependencies.

4.8 Ordered description of steps to be taken to execute the test case

All listed name servers are queried for the SOA record over UDP and TCP. If any of the name servers fail to give an authoritative answer (“AA-bit” is set in the answer), the message NAMESERVER:NOT_AUTH is generated.

5. Network diversity

5.1 Test case identifier

DNS04 Network diversity

5.2 Objective

The name servers must be in at least two topologically separate networks for IPv4 and IPv6, respectively.

This test case fulfills the requirements 2.5.2 in the "Technical requirements for authoritative name servers" document.

5.3 Inputs

See section 2.3 in this document. In addition to this we use the IP to ASN mapping in the RIPE RIS database[3].

5.4 Outcome(s)

There must be at least two different origin ASs from the process described in section 5.8. The RIPE RIS database is used to determine if at least two origin ASs are used. If it does not report at least two origin ASs for IPv4 and IPv6, respectively, this test case fails. The two origin ASs must also have some independence as described in the steps below.

5.5 Environmental needs

The RIPE RIS database must be available online.

5.6 Special procedural requirements

This test has no procedural requirements.

5.7 Intercase dependencies

This test has no intercase dependencies.

5.8 Ordered description of steps to be taken to execute the test case

1. All NS records and their IP addresses are looked up for the designated zone.
2. The following steps are done independently for the IPv4 and IPv6 addresses, respectively, and both protocols must pass.
    a. For all IP addresses do a lookup of origin ASNs using one of the following commands[4]:

[3] http://www.ripe.net/data-tools/stats/ris/routing-information-service
[4] The exact command can vary depending on OS on which the command is executed. The example here is from a computer with Ubuntu Linux. Also see http://www.ripe.net/ris/riswhois.html

whois -h riswhois.ripe.net -- "-F -M **<IPaddr>**"
whois -h riswhois.ripe.net -- "-M **<IPaddr>**"

b. Each lookup will result in a set of origin ASNs (one or more ASNs). Save that set to a list of sets.
c. When comparing two sets in the list, the sets are considered to be equal if they have the same ASNs as elements. The order between ASNs in a set shall be ignored.
d. Compare the sets in the list. If there are two sets in the lists thar are NOT equal, then the tested protocol (IPv4 or IPv6) will pass, or else it will fail.

3. If both IPv4 and IPv6 pass the steps above, this Test Cass ends with PASS, else it ends with FAIL.

5.9 Examples of passing and failing configurations

In our examples the nameservers have three IP addresses, x_1, x_2 and x_3. The lookup of origin gives the result as below.

Example 1. This configuration is a PASS. Two addresses have different origin ASs:

x_1: 65536
x_2: 65536, 65550
x_3: 65550

Example 2. This configuration is also a PASS. One address has a different configuration of origin ASs than the other:

x_1: 65536
x_2: 65536, 65550
x_3: 65536, 65550

Example 3. This configuration is a FAIL. All addresses have the same configuration of origin ASs:

x_1: 65536, 65550
x_2: 65536, 65550
x_3: 65536, 65550

Example 3. This configuration is also a FAIL. The addresses have only one and the same origin AS:

x_1: 65536
x_2: 65536
x_3: 65536

Note that the tests of origin ASs are done independently on IPv4 and IPv6, and that both must meet the requirments to give a PASS on this test case.

6. Consistency between glue and authoritative data

6.1 Test case identifier

DNS05 Consistency between glue and authoritative data

6.2 Objective

For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.

This test case fulfills the requirements 2.6.1 in the "Technical requirements for authoritative name servers" document.

6.3 Inputs

See section 2.3 in this document.

6.4 Outcome(s)

If there is an inconsistency between the IP-addresses for any host on any authoritative name server, the error message DELEGATION:INCONSISTENT_GLUE is generated and this test case fails.

6.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

6.6 Special procedural requirements

This test has no procedural requirements.

6.7 Intercase dependencies

This test has no intercase dependencies.

6.8 Ordered description of steps to be taken to execute the test case

The name server data on the input parameters side is compared to the content of the answers for all the name servers. If there is an inconsistency between the sets of IP-addresses the message DELEGATION:INCONSISTENT_GLUE is generated.

7. Consistency between delegation and zone

7.1 Test case identifier

DNS06 Consistency between delegation and zone

7.2 Objective

The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.

This test case fulfills the requirements 2.7.1 in the "Technical requirements for authoritative name servers" document.

7.3 Inputs

See section 2.3 in this document.

7.4 Outcome(s)

The NS sets between the parent and the child zone must be consistent. If the NS sets are not consistent the error message DELEGATION:EXTRA_NS_PARENT or DELEGATION:EXTRA_NS_CHILD is generated and this test case fails.

7.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

7.6 Special procedural requirements

This test has no procedural requirements.

7.7 Intercase dependencies

This test has no intercase dependencies.

7.8 Ordered description of steps to be taken to execute the test case

All authoritative name servers are queried for the NS set. The name server data on the input parameters side is compared to the content of the answers for all the name servers. If there is an inconsistency between the NS record sets, the message DELEGATION:EXTRA_NS_PARENT or DELEGATION:EXTRA_NS_CHILD is generated.

8. SOA record consistency between authoritative name servers

8.1 Test case identifier

DNS07 SOA record consistency between authoritative name servers

8.2 Objective

The data served by the authoritative name servers for the designated zone must be consistent. All authoritative name servers must serve the same SOA record for the designated zone.

This test case fulfills the requirements 2.8.1 and 2.8.3 in the "Technical requirements for authoritative name servers" document.

8.3 Inputs

See section 2.3 in this document.

8.4 Outcome(s)

All authoritative name servers must have consistent SOA digests and SOA serial values. If there is any inconsistency, the error messages CONSISTENCY:SOA_SERIAL_DIFFERENT or CONSISTENCY:SOA_DIGEST_DIFFERENT is generated, and this test case fails in this first step.

If there are occurrences of the error CONSISTENCY:SOA_SERIAL_DIFFERENT, there is a manual inspection of the SOA Serial numbers in the logs. See the requirement in 2.8.3.1 in the "Technical requirements for authoritative name servers" document. If the difference of the SOA Serial is considered minor, the error is discarded, and the test case is passed. If the difference is considered major, this test case fails.

8.5 Environmental needs

All name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

8.6 Special procedural requirements

If for operational reasons the zone content fluctuates rapidly, the serial numbers need only be loosely coherent. Manual inspection of the logs in case of the occurrence of CONSISTENCY:SOA_SERIAL_DIFFERENT.

There are several different methods to set the SOA Serial number. The most popular are "unix time" where the Serial is a second counter based on unix time, "date" where the Serial is a date and a serial number counter at the end, and "counter" where the Serial value is just any type of counter. The most common use is probably "unix time". In both "date" and "unix time" it should be easy to note that the authoritative name servers do not differ any more than a few serial number updates. A manual inspection of the SOA serial should be enough to determine if the zone updates work properly or not, and if the serial values are within a reasonable range, the test is ok.

8.7 Intercase dependencies

This test has no intercase dependencies.

8.8 Ordered description of steps to be taken to execute the test case

The SOA record is queried from all the name servers found in the input parameters, and also in the zone itself. If the SOA serial number is not all the same for all the answers, the message CONSISTENCY:SOA_SERIAL_DIFFERENT is generated. A digest is calculated from the SOA records as well, and if the digest is not all the same for all the answers the message CONSISTENCY:SOA_DIGEST_DIFFERENT is generated.

9. NS record consistency between authoritative name servers

9.1 Test case identifier

DNS08 NS record consistency between authoritative name servers

9.2 Objective

The data served by the authoritative name servers for the designated zone must be consistent. All authoritative name servers must serve the same NS record set for the zone domain.

This test case fulfills the requirements 2.8.1 and 2.8.2 in the "Technical requirements for authoritative name servers" document.

9.3 Inputs

See section 2.3 in this document.

9.4 Outcome(s)

All authoritative name servers must have consistent NS sets in the answer. If there is any inconsistency in the answers, the message CONSISTENCY:MULTIPLE_NS_SETS is generated and this test case fails.

9.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

9.6 Special procedural requirements

This test has no procedural requirements.

9.7 Intercase dependencies

This test has no intercase dependencies.

9.8 Ordered description of steps to be taken to execute the test case

An NS record query for the TLD is made for all the name servers found in the input parameters. If any of the NS records in an authoritative answer is not consistent with any of the other answers, the message CONSISTENCY:MULTIPLE_NS_SETS is generated.

10. No truncation of referrals

10.1 Test case identifier

DNS09 No truncation of referrals

10.2 Objective

Referrals from the parent zone's name servers must fit into a non-EDNS0 UDP DNS packet and therefore the DNS payload must not exceed 512 octets.

This test case fulfills the requirements 2.9.1 and 2.9.2 in the “Technical requirements for authoritative name servers” document.

10.3 Inputs

See section 2.3 in this document.

10.4 Outcome(s)

The created DNS referral packet must not be more than 512 octets. If the DNS packet is larger than 512 bytes, the message DELEGATION:MIN_REFERRAL_SIZE_TOO_BIG is generated and this test case fails.

10.5 Environmental needs

This test has no environmental requirements.

10.6 Special procedural requirements

This test has no procedural requirements.

10.7 Intercase dependencies

This test has no intercase dependencies.

10.8 Ordered description of steps to be taken to execute the test case

An empty DNS answer packet is generated. All NS records from the input, and all the in-bailiwick glue is added to the packet. If the size of the packet is more than 512 octets the message DELEGATION:MIN_REFERRAL_SIZE_TOO_BIG is generated.

11. Prohibited networks

11.1 Test case identifier

DNS10 Prohibited networks

11.2 Objective

The authoritative name server IP addresses must not be in specially designated networks that are either not globally routable, or are otherwise unsuited for authoritative name service.

This test case fulfills the requirements in 2.10 of the "Technical requirements for authoritative name servers" document.

11.3 Inputs

See section 2.3 in this document.

11.4 Outcome(s)

All IP addresses used by the name servers in the delegation for the designated zone must be globally routable. If any of the IP addresses used is reserved, private or otherwise unsuitable (see the table in 11.8), any of the error messages ADDRESS:RESERVED_IPV4, ADDRESS:RESERVED_IPV6, ADDRESS:UNSUITABLE_IPV4, ADDRESS:UNSUITABLE_IPV6, ADDRESS:INVALID or ADDRESS:PRIVATE_IPV4 is generated and this test case fails.

11.5 Environmental needs

This test has no environmental requirements.

11.6 Special procedural requirements

This test has no procedural requirements.

11.7 Intercase dependencies

This test has no intercase dependencies.

11.8 Ordered description of steps to be taken to execute the test case

All name servers found in the input parameters are queried for their IP addresses in the zone. Along with IP addresses from the input data, all addresses are is compared to a list containing blocks of reserved IPv4 addresses not suitable for global routing, blocks of reserved IPv6 addresses not suitable for global routing, and Teredo and 6to4 IPv6 tunnel addresses. This is a table of the message and the message generated if the IP address is within the disallowed address range:

Address blocks	Description	DNSCheck message
127/8, 169.254/16, 192.0.0.0/24, 23.255.255.0/24, 224.0.0.0/4, 240.0.0.0/4	Reserved IPv4 address blocks from RFC 3330. RFC 5735 and RFC 5771 (Multicast)	ADDRESS:RESERVED_IPV4
::1/128, ::/128, ::FFFF:0:0/96, fe80::/10, fc00::/7, 2001:db8::/32, 2002::/16, 2001::/32, 5f00::/8, 3ffe::/16, 2001:10::/28, ::/0, ff00::/8	Special use IPv6 address blocks from RFC 5156	ADDRESS:RESERVED_IPV6
192.88.99.0/24	6to4 IPv4 anycast address	ADDRESS:UNSUITABLE_IPV4
2001::/32, 2002::/16	Teredo and 6to4	ADDRESS:UNSUITABLE_IPV6
::<ipv4-address>/96, Syntactically incorrect IP-address	IPv4 mapped IPv6 address and syntactically incorrect addresses	ADDRESS:INVALID
10/8, 172.16/12, 192.168/16, 100.64/10	Private or Shared IPv4 addresses from RFC1918 and RFC 6598	ADDRESS:PRIVATE_IPV4

12. No open recursive name service

12.1 Test case identifier

DNS11 No open recursive name service

12.2 Objective

The authoritative name servers must not provide recursive name service.

This test case fulfills the requirements 2.11.1 in the “Technical requirements for authoritative name servers” document.

12.3 Inputs

See section 2.3 in this document.

12.4 Outcome(s)

No name server must respond with a possible referral packet. If the response is a referral, the message NAMESERVER:RECURSIVE is generated and this test case fails.

12.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

12.6 Special procedural requirements

This test has no procedural requirements.

12.7 Intercase dependencies

This test has no intercase dependencies.

12.8 Ordered description of steps to be taken to execute the test case

A SOA query for an almost certainly nonexistent name sent to the list of name servers, with the recursion request and DNSSEC flags set, resulting in a response with the recursion available flag set, an RCODE other than SERVFAIL or REFUSED and not referring to other servers. If the response is a possible referral, the message NAMESERVER:RECURSIVE is generated.

13. Same source address

13.1 Test case identifier

DNS12 Same source address

13.2 Objective

Responses from the authoritative name servers must contain the same source IP address as the destination IP address of the initial query.

This test case fulfills the requirements 2.12.1 in the "Technical requirements for authoritative name servers" document.

13.3 Inputs

See section 2.3 in this document.

13.4 Outcome(s)

The DNS answer must come from the same source IP address as the destination of the query. If there is a mismatch, the message NAMESERVER:NOT_SAME_SOURCE is generated and this test case fails.

13.5 Environmental needs

All authoritative name servers listed in the inputs section 2.3 should be authoritative for the designated zone.

13.6 Special procedural requirements

This test has no procedural requirements.

13.7 Intercase dependencies

This test has no intercase dependencies.

13.8 Ordered description of steps to be taken to execute the test case

One query per authoritative name server IP address is made, and the answer is verified to come from the same IP address. If there is a mismatch between these IP addresses, the message NAMESERVER:NOT_SAME_SOURCE is generated.

14. Check invalid syntax for SOA RNAME

14.1 Test case identifier

DNS23 Syntax for SOA RNAME

14.2 Objective

The SOA RNAME field must be valid in accordance with section 3.3.13 in RFC 1035 and section 3.4 in RFC 2822.

This test case is an addition to the Statement of Work; see section 2.1.2 in the DNS Test Plan document.

14.3 Inputs

See section 2.3 in this document.

14.4 Outcome(s)

The SOA field RNAME must comply with RFC 2822 “Address Specification”. If the validation of RNAME fails, the message MAIL:ADDRESS_SYNTAX is generated and this test case fails.

14.5 Environmental needs

This test has no environmental requirements.

14.6 Special procedural requirements

This test has no procedural requirements.

14.7 Intercase dependencies

This test has no intercase dependencies.

14.8 Ordered description of steps to be taken to execute the test case

A SOA query is made to all authoritative name servers. The SOA field RNAME is validated against the rules described in RFC 2822, “Address Specification”. If the RNAME field does not validate, the message MAIL:ADDRESS_SYNTAX is generated.

15. Check SOA Minimum value

15.1 Test case identifier

DNS24 SOA Minimum

15.2 Objective

The SOA Minimum field must be set to 300 seconds or more.

This test case is an addition to the Statement of Work; see section 2.1.2 in the DNS Test Plan document.

15.3 Inputs

See section 2.3 in this document.

15.4 Outcome(s)

The SOA Minimum value must not be less than 300. If the value is less than 300, the message SOA:MINIMUM_SMALL is returned and this test case emits a warning.

15.5 Environmental needs

This test has no environmental requirements.

15.6 Special procedural requirements

This test has no procedural requirements.

15.7 Intercase dependencies

This test has no intercase dependencies.

15.8 Ordered description of steps to be taken to execute the test case

The value from the SOA Minimum field is retrieved. If the value is less than 300 the message SOA:MINIMUM_SMALL is generated.

16. Global

16.1 Glossary

The glossary is available in the Master Test Plan.

16.2 Document change procedures

Document change procedures are documented in the Master Test Plan.