dig 활용방법 가이드

2004. 6.

IP 주 소 관 리 팀
한국인터넷정보센터

- 목 차 -

Dig (Domain Information Groper)

1. dig 개요

dig (Domain Information Groper)

BIND DNS 배포 패키지에 기본적으로 포함된 DNS 진단용 유틸리티
DNS lookup 유틸리티의 일종
널리 사용되어 왔던 nslookup을 대체할 예정 (nslookup은 향후 배포중단 예정)

dig은 어떤 경우에 사용하나?

DNS 네임서버 구성과 도메인 설정이 완료된 후, 인터넷 일반 사용자의 입장에서 설정한 도메인네임에 대한 DNS 질의응답이 정상적으로 이루어지는 지를 확인 점검하는 경우에 사용

이외에 ISP 네트워크 관리자가 ADSL/VDSL 가입자의 장애현상에 대한 원인파악을 위해 DNS 네임서버 문제여부를 진단하는 용도로 사용

왜 nslookup이 아니라 dig을 사용하나?

nslookup에 비해 dig이 DNS의 추가 표준사항을 충실히 반영한 진단도구로서 구현

dig은 BIND DNS 네임서버의 알고리듬을 사용 동작, 보다 정확한 진단동작 수행

BIND DNS의 배포처인 ISC(Internet Systems Consortium)은 nslookup은 향후 배포 패키지에서 제외할 예정이며, dig을 사용하기를 권고

dig은 어디서 얻을 수 있고 어떻게 설치하나?

dig은 현재 BIND DNS 패키지에 포함되어 배포되고 있음

Unix나 Linux 계열 OS에는 dig이 포함, OS 설치 시에 기본적 설치
Windows 계열 OS 경우, BIND DNS 설치패키지를 다운로드 후 설치 필요

dig의 설치관련 사항은 “4. dig 유틸리티 설치 및 환경 구성“ 참조

2. dig의 간단한 사용방법

도메인네임에 대한 질의

dig [@server] [name] [type]

server	DNS 질의를 할 대상 네임서버 네임서버의 도메인네임(domain name) 또는 IP 주소 지정 디폴트 동작: 지정하지 않은 경우 시스템 resolv.conf 파일의 네임서버 사용 시스템 resolv.conf에 네임서버 미지정 시, localhost 사용 **Note**: IP 주소 지정의 경우 IPv4 주소 또는 IPv6 주소 지정가능 IPv6 주소를 지정 가능한 시스템 : Unix, Linux 계열 OS 호스트
name	질의 대상 도메인 네임 DNS 패킷 Question Section의 QName에 지정될 질의 대상 도메인네임 디폴트 동작: 지정하지 않은 경우 루트 도메인(.)에 대해서 질의
type	질의 타입 DNS 패킷 Question Section의 QType에 지정되는 질의 대상 RR 타입 디폴트 동작: 지정하지 않은 경우 name이 지정되지 않은 경우: 루트 도메인(.)의 NS 타입 질의 name이 지정된 경우: 지정된 도메인네임의 A 타입 질의

일반적인 DNS 질의 예시

```
c:\>dig www.nic.or.kr A

; <<>> DiG 9.2.3 <<>> www.nic.or.kr A
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.nic.or.kr.                 IN      A

;; ANSWER SECTION:
www.nic.or.kr.          1772    IN      A       202.30.50.90

;; AUTHORITY SECTION:
nic.or.kr.              1798    IN      NS      ns2.nic.or.kr.
nic.or.kr.              1798    IN      NS      ns1.nic.or.kr.

;; ADDITIONAL SECTION:
ns1.nic.or.kr.          1791    IN      A       202.30.50.51
ns2.nic.or.kr.          1798    IN      A       220.73.220.113

;; Query time: 100 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Wed Jun 23 19:18:52 2004
;; MSG SIZE  rcvd: 115
```

IP 주소(IPv4, IPv6)에 대한 역변환 질의

dig [@server] -x ip_address

server	DNS 질의를 할 대상 네임서버 네임서버의 도메인네임(domain name) 또는 IP 주소 지정 디폴트 동작: 지정하지 않은 경우 시스템 resolv.conf 파일의 네임서버 사용 시스템 resolv.conf에 네임서버 미지정 시, localhost 사용 **Note**: IP 주소 지정의 경우 IPv4 주소 또는 IPv6 주소 지정가능 IPv6 주소를 지정 가능한 시스템 : Unix, Linux 계열 OS 호스트
-x ip_address	역변환 질의 대상 IP 주소 지정 IPv4의 경우: in-addr.arpa. 도메인네임으로 변환 후 질의 IPv6의 경우: ip6.arpa. 도메인네임으로 변환 후 질의 **Note**: IPv6 역변환 질의 가능한 dig 버전 BIND DNS 9.2.3 버전이상의 dig 유틸리티에서 가능 BIND DNS 8.3.2 버전이상의 dig 유틸리티에서 가능

IPv4 주소 역변환 질의 예시

```
C:\>dig -x 202.31.190.222

; <<>> DiG 9.2.3 <<>> -x 202.31.190.222
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;222.190.31.202.in-addr.arpa.   IN     PTR

;; ANSWER SECTION:
222.190.31.202.in-addr.arpa. 180 IN    PTR    rec.test.kr.

;; AUTHORITY SECTION:
190.31.202.in-addr.arpa. 180   IN     NS     ns2.test.kr.
190.31.202.in-addr.arpa. 180   IN     NS     ns1.test.kr.

;; ADDITIONAL SECTION:
ns1.test.kr.          180    IN     A      202.31.190.200
ns1.test.kr.          180    IN     AAAA   2001:dc5:a::200
ns2.test.kr.          180    IN     A      202.31.190.210
ns2.test.kr.          180    IN     AAAA   2001:dc5:a::210

;; Query time: 140 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 16:17:39 2004
;; MSG SIZE  rcvd: 194
```

IPv6 주소 역변환 질의 예시

```
c:\>dig -x 2001:6b0:1:ea:a00:20ff:fe8f:708f

; <<>> DiG 9.2.3 <<>> -x 2001:6b0:1:ea:a00:20ff:fe8f:708f
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;f.8.0.7.f.8.e.f.f.f.0.2.0.0.a.0.a.e.0.0.1.0.0.0.0.b.6.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
f.8.0.7.f.8.e.f.f.f.0.2.0.0.a.0.a.e.0.0.1.0.0.0.0.b.6.0.1.0.0.2.ip6.arpa. 3600 IN PTR renskav.stacken.kth.se.

;; AUTHORITY SECTION:
a.e.0.0.1.0.0.0.0.b.6.0.1.0.0.2.ip6.arpa. 3600 IN NS ns.stacken.kth.se.

;; Query time: 1622 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Wed Jun 23 17:19:21 2004
;; MSG SIZE  rcvd: 143
```

dig 질의결과 출력내용 분석

아래는 dig을 사용한 DNS 질의 결과로써 디폴트 형식의 출력 내용이다.
이를 기준으로 각 출력내용에 대해 설명한다.

```
c:\>dig www.nic.or.kr A

; <<>> DiG 9.2.3 <<>> www.nic.or.kr A
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.nic.or.kr.                 IN      A

;; ANSWER SECTION:
www.nic.or.kr.          1772    IN      A       202.30.50.90

;; AUTHORITY SECTION:
nic.or.kr.              1798    IN      NS      ns2.nic.or.kr.
nic.or.kr.              1798    IN      NS      ns1.nic.or.kr.

;; ADDITIONAL SECTION:
ns1.nic.or.kr.          1791    IN      A       202.30.50.51
ns2.nic.or.kr.          1798    IN      A       220.73.220.113

;; Query time: 100 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Wed Jun 23 19:18:52 2004
;; MSG SIZE  rcvd: 115
```

dig 출력내용은 DNS 메시지의 Header, Question Section, Answer Section, Authority Section, Addition Section의 구조에 맞추어 출력된다.

이에 부가하여 끝 부분에 dig이 첨가하는 부가적인 정보로써 DNS 응답소요 시간, DNS 응답서버 정보, DNS 메시지 사이즈 정보 등을 출력한다.

```
; <<>> DiG 9.2.3 <<>> www.nic.or.kr A
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
```

>>DIG 9.2.3<<	dig의 버전정보 (dig이 포함된 BIND DNS 버전과 동일) 이 라인의 뒷부분은 dig에 입력된 문자열 출력
opcode:	DNS 응답 메시지의 operation code DNS 질의 유형을 표시 DNS 질의 유형: QUERY : Standard Query IQUERY : Inverse Query (현재는 사용 않음) STATUS : Server Status Request NOTIFY : DNS Notify Message UPDATE : DNS Dynamic Update Message

status:	DNS 응답메시지의 RCODE(Response Code) 표시 응답 메시지의 응답 코드 RCODE 종류: NOERROR : No Error [Standard Query] FORMERR : Format Error [Standard Query] SERVFAIL : Server Failure [Standard Query] NXDOMAIN : Non-Existent Domain [Standard Query] NOTIMP : Not Implemented [Standard Query] REFUSED : Query Refused [Standard Query] YXDOMAIN : Name Exists when it should not [DNS UPDATE] YXRRSET : RR Set Exists when it should not [DNS UPDATE] NXRRSET : RR Set that should exist does not [DNS UPDATE] NOTAUTH : Server Not Authoritative for zone [DNS UPDATE] NOTZONE : Name not contained in zone [DNS UPDATE] BADVERS : Bad OPT Version [EDNS0] ※ Standard Query RFC1035, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", 에서 정의된 기본적인 DNS 질의응답 메시지 ※ DNS UPDATE = DNS Dynamic Update RFC2136, "Dynamic Updates in the Domain Name System (DNS UPDATE)", 에서 정의된 DNS Dynamic Update 메시지 (원격에서 동적으로 도메인네임 및 RR 정보 변경 기능) ※ EDNS0 RFC2671, "Extension Mechanisms for DNS (EDNS0)" DNS 헤더 flag 및 기타 DNS 기능 확장 정의
id:	DNS transaction ID를 표시 DNS 프로토콜에서 DNS 질의 메시지와 DNS 응답 메시지 대응 관계 표시
flags:	DNS Header Section의 flag 필드 값 표시 flag 종류: qr : Query/Response bit (set = Response) rd : Recursion Desired (set = Recursion Desired) ra : Recursion Available (set = Recursion Available, Server) tc : Truncation (set = Message is truncated) aa : Authoritative Answer (set = Authoritative Answer) ad : 확장 flag, Authentic Data cd : 확장 flag, Checking Disabled ※ RFC1035, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", ‘4.1.1. Header section format’에서 기본 flag 정의됨 ※ RFC2535, "Domain Name System Security Extensions", '6.1. The AD and CD Header Bits'에서 확장 flag 정의
QUERY:	DNS Query Section의 RR 개수 (항상 1) DNS 메시지 Header Section의 QDCOUNT 필드에 해당
ANSWER:	DNS Answer Section의 RR 개수 DNS 메시지 Header Section의 ANCOUNT 필드에 해당
AUTHORITY:	DNS Authority Section의 RR 개수 DNS 메시지 Header Section의 NSCOUNT 필드에 해당
ADDITIONAL:	DNS Additional Section의 RR 개수 DNS 메시지 Header Section의 ARCOUNT 필드에 해당

```
;; QUESTION SECTION:
;www.nic.or.kr.                IN      A

;; ANSWER SECTION:
www.nic.or.kr.          1772    IN      A       202.30.50.90

;; AUTHORITY SECTION:
nic.or.kr.              1798    IN      NS      ns2.nic.or.kr.
nic.or.kr.              1798    IN      NS      ns1.nic.or.kr.

;; ADDITIONAL SECTION:
ns1.nic.or.kr.          1791    IN      A       202.30.50.51
ns2.nic.or.kr.          1798    IN      A       220.73.220.113
```

;; QUESTION SECTION:	DNS 질의 내용을 표시
;; ANSWER SECTION:	DNS 질의 사항에 대한 DNS 응답 RR을 표시
;; AUTHORITY SECTION:	DNS 응답 RR이 속한 도메인 존의 NS RR 정보 만일 nic.or.kr. 존(zone)에 www.nic.or.kr이 존재하지 않는 경우에는 nic.or.kr 도메인의 SOA RR 정보 포함
;; ADDITIONAL SECTION:	부가적인 RR 정보를 표시 주로 ANSWER SECTION이나 AUTHORITY SECTION의 RR에 관련된 부가적인 A RR, AAAA RR 정보 포함

```
;; Query time: 100 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Wed Jun 23 19:18:52 2004
;; MSG SIZE  rcvd: 115
```

;; Query time:	DNS 질의 메시지 발송시점에서 응답시점까지의 소요시간
;; SERVER:	DNS 응답 메시지를 보내온 질의응답 네임서버
;; WHEN	DNS 응답 메시지를 받은 시점의 date & time
;; MSG SIZE rcvd:	응답받은 DNS 메시지의 size 표시 (byte 단위) **Note**: IP 및 TCP/UDP 헤더는 제외된 size임

IPv6 DNS 점검 활용

AAAA RR에 대한 질의

아래와 같이 IPv6 주소에 대한 기본적인 질의는 AAAA RR에 대한 질의를 통해 이루어진다.

dig *domain_name* AAAA

```
C:\>dig www.krdnsv6.or.kr aaaa

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1800    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1800    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1800    IN      NS      ns1.nic.or.kr.

;; Query time: 130 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 15:46:45 2004
;; MSG SIZE  rcvd: 103
```

위의 경우, www.krdnsv6.or.kr 도메인네임의 IPv6 주소는 "2001:dc5:a::100"이다.

NOTE! : DNS에는 도메인네임의 IP 주소를 모두 질의하는 방법은 없음
www.krdnsv6.or.kr의 IPv4 주소를 파악하려면, 'dig www.krdnsv6.or.kr A'로
www.krdnsv6.or.kr의 IPv6 주소를 파악하려면, 'dig www.krdnsv6.or.kr AAAA'로 질의해야 함
결국, IPv4와 IPv6가 공존하는 환경에서 도메인네임의 IP 주소는 A 타입 질의와 AAAA 타입 질의를 모두 수행해 봐야 파악할 수 있음
IPv6 어플리케이션 역시 AAAA 타입 DNS 질의와 A 타입 DNS 질의를 각각 수행하여 도메인네임의 IP 주소리스트를 파악한 후 통신을 개시함

IPv6 주소를 사용하여 IPv6 패킷의 DNS 질의

IPv6 주소를 사용하여 구성된 DNS 네임서버에 대해서 IPv6 패킷기반의 DNS 서비스가 정상적인지 확인할 필요성이 발생할 수 있다.

이 경우, dig을 아래와 같이 사용하여 IPv6 패킷 기반의 DNS 점검을 할 수 있다.

dig @ipv6_address ***domain_name type*** **또는**
dig @name_server_domain_name ***domain_name type***

이때, **ipv6_address**는 IPv6 주소를 그대로 사용하는 경우이고,
name_server_domain_name은 IPv6 주소의 네임서버 도메인네임을 사용하는 경우이다.

```
$ dig @2001:dc5:a::222 www.krdnsv6.or.kr aaaa

; <<>> DiG 9.2.2 <<>> @2001:dc5:a::222 www.krdnsv6.or.kr aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14793
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1095    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1095    IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.          1095    IN      NS      ns2.nic.or.kr.

;; Query time: 79 msec
;; SERVER: 2001:dc5:a::222#53(2001:dc5:a::222)
;; WHEN: Thu Jun 24 15:57:05 2004
;; MSG SIZE  rcvd: 103
```

```
$ dig @rec.test.kr. www.krdnsv6.or.kr aaaa

; <<>> DiG 9.2.2 <<>> @rec.test.kr. www.krdnsv6.or.kr aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49779
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      888     IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          888     IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          888     IN      NS      ns1.nic.or.kr.

;; Query time: 16 msec
;; SERVER: 2001:dc5:a::222#53(rec.test.kr.)
;; WHEN: Thu Jun 24 16:00:32 2004
;; MSG SIZE  rcvd: 103
```

NOTE! : IPv6 DNS 패킷 질의는 Unix, Linux 계열 IPv6 지원 시스템에서 가능
Windows용 BIND DNS의 dig 유틸리티는 아직 Windows OS의 IPv6 스택을 지원하지 못하고 있음
따라서 일반 PC에서는 IPv6 패킷의 DNS 질의 점검에 dig을 사용할 수 없음

NOTE : KRDNSv6 웹 사이트(www.krdnsv6.or.kr)에서는 웹 기반 dig 제공
PC에서 IPv6 패킷 기반의 DNS 질의점검이 곤란하므로, 어디에서나 IPv6 패킷의 DNS 질의점검이 가능하도록 웹 기반 dig 점검 기능을 제공하고 있음

3. dig 고급 활용

dig 출력 양식의 조정

dig의 출력양식과 관련된 옵션을 각 옵션별로 정리한다.

+[no]cmd	command line을 출력할 것인지 아닌지를 지정 디폴트: +cmd (명령 라인의 내용을 출력함)

예시 : "+cmd", "+nocmd" 옵션 지정, 결과 비교

```
c:\>dig +cmd www.krdnsv6.or.kr. a

; <<>> DiG 9.2.3 <<>> +cmd www.krdnsv6.or.kr. a
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      A

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1789    IN      A       202.31.190.100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1789    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1789    IN      NS      ns1.nic.or.kr.

;; Query time: 90 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:13:09 2004
;; MSG SIZE  rcvd: 91
```

```
c:\>dig +nocmd www.krdnsv6.or.kr. a
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      A

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1773    IN      A       202.31.190.100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1773    IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.          1773    IN      NS      ns2.nic.or.kr.

;; Query time: 70 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:13:26 2004
;; MSG SIZE  rcvd: 91
```

+[no]comments	comment line들을 출력할 것인지 아닌지를 지정 comment line은 ";; ANSWER SECTION:"과 같은 라인 디폴트: +comments

예시 : "+comments", "+nocomments" 옵션 지정, 결과 비교

Note : "+nocomments" 사용시 DNS 메시지 Header 정보가 출력되지 않게 됨

```
c:\>dig +comments www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> +comments www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1800    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1800    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1800    IN      NS      ns1.nic.or.kr.

;; Query time: 120 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:20:45 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig +nocomments www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> +nocomments www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;www.krdnsv6.or.kr.            IN      AAAA
www.krdnsv6.or.kr.      1794    IN      AAAA    2001:dc5:a::100
krdnsv6.or.kr.          1794    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1794    IN      NS      ns1.nic.or.kr.
;; Query time: 40 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:20:51 2004
;; MSG SIZE  rcvd: 103
```

+[no]question +[no]answer +[no]authority +[no]additional	DNS 메시지 Question, Answer, Authority, Additional Section 내용의 출력여부 각각 지정 디폴트: +question +answer +authority +additional

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.           IN     AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.     1368    IN     AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1368    IN     NS     ns2.nic.or.kr.
krdnsv6.or.kr.         1368    IN     NS     ns1.nic.or.kr.

;; Query time: 120 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:27:57 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +noquestion

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +noquestion
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; ANSWER SECTION:
www.krdnsv6.or.kr.     1333    IN     AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1333    IN     NS     ns1.nic.or.kr.
krdnsv6.or.kr.         1333    IN     NS     ns2.nic.or.kr.

;; Query time: 100 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:28:32 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +noquestion +noanswer +noauthority +noadditional

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +noquestion +noanswer +noauthority +noadditional
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; Query time: 60 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:29:36 2004
;; MSG SIZE  rcvd: 103
```

+[no]stats	DNS 메시지 끝부분의 DNS 응답소요 시간 등 출력여부 지정 디폴트: +stats

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1177    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1177    IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.          1177    IN      NS      ns2.nic.or.kr.

;; Query time: 140 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:31:09 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +nostats

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +nostats
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1170    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1170    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1170    IN      NS      ns1.nic.or.kr.
```

+[no]short	DNS 응답결과를 가장 간단한 내용만 출력함 디폴트: +noshort

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1046    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1046    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1046    IN      NS      ns1.nic.or.kr.

;; Query time: 110 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:33:20 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +short
2001:dc5:a::100
```

+short +identity	DNS의 간단한 응답결과 출력시 네임서버 정보 추가출력 지정 디폴트: +short +noidentity

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig www.krdnsv6.or.kr. aaaa +short
2001:dc5:a::100
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +short +identity
2001:dc5:a::100 from server 202.31.190.222 in 10 ms.
```

+[no]qr	DNS 질의 메시지의 Question Section 출력 포함 여부 지정 디폴트: +noqr

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig www.krdnsv6.or.kr. aaaa

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      887     IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          887     IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          887     IN      NS      ns1.nic.or.kr.

;; Query time: 90 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:35:59 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +qr

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +qr
;; global options:  printcmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      884     IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          884     IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.          884     IN      NS      ns2.nic.or.kr.

;; Query time: 80 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:36:02 2004
;; MSG SIZE  rcvd: 103
```

+[no]multiline	DNS 리소스레코드(Resource Record) 출력시 확장된 형식으로 출력 지정 디폴트: +nomultiline

예시 : 각 옵션 지정, 결과 비교
Note : 특히 SOA RR과 같은 리소스레코드 출력에 적용

```
c:\>dig krdnsv6.or.kr. soa

; <<>> DiG 9.2.3 <<>> krdnsv6.or.kr. soa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;krdnsv6.or.kr.              IN      SOA

;; ANSWER SECTION:
krdnsv6.or.kr.         1800    IN      SOA     ns1.krnic.net. root.ns1.nic.or.kr. 2004052518 3600 300 3600000 1800

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1800    IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.         1800    IN      NS      ns2.nic.or.kr.

;; Query time: 170 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:46:05 2004
;; MSG SIZE  rcvd: 125
```

```
c:\>dig krdnsv6.or.kr. soa +multiline

; <<>> DiG 9.2.3 <<>> krdnsv6.or.kr. soa +multiline
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;krdnsv6.or.kr.         IN SOA

;; ANSWER SECTION:
krdnsv6.or.kr.         1796 IN SOA ns1.krnic.net. root.ns1.nic.or.kr. (
                            2004052518 ; serial
                            3600       ; refresh (1 hour)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            1800       ; minimum (30 minutes)
                            )

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1796 IN NS ns1.nic.or.kr.
krdnsv6.or.kr.         1796 IN NS ns2.nic.or.kr.

;; Query time: 150 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:46:09 2004
;; MSG SIZE  rcvd: 125
```

dig의 DNS TCP/UDP 질의

DNS 네임서버는 반드시 TCP 53, UDP 53 포트 모두에 대해서 DNS 서비스를 제공해야 한다.

DNS 질의는 UDP 53을 사용하는 것이 대부분이다.
그럼에도 TCP 53 포트에 대해서 반드시 DNS 서비스를 제공해야 하는 것은 UDP DNS 응답 메시지가 512 바이트를 초과하는 경우에 TCP 53 포트의 서비스가 가능해야 하기 때문이다.

이외에 TCP 53 포트를 사용하는 DNS 동작이 있다.
존 전송(zone transfer)의 경우, 항상 TCP 53번 포트를 사용하여 요청과 데이터 전송이 이루어진다.

따라서 DNS 네임서버의 서비스 정상여부 점검의 경우, UDP 53 포트만이 아니라 TCP 53 포트에 대해서도 DNS 질의응답 점검을 하는 것이 바람직하다.

+[no]vc +[no]tcp	DNS 질의를 TCP를 사용하여 수행 지정 '+[no]vc'와 '+[no]tcp'는 동일한 기능으로 명칭만 다름 디폴트: +novc, +notcp

예시 : 각 옵션 지정, 결과 비교
Note : TCP 기반 질의여부는 패킷 캡쳐 프로그램을 사용하여 확인

```
c:\>dig www.krdnsv6.or.kr. aaaa +vc

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +vc
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1800    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1800    IN      NS      ns1.nic.or.kr.
krdnsv6.or.kr.          1800    IN      NS      ns2.nic.or.kr.

;; Query time: 130 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:54:33 2004
;; MSG SIZE  rcvd: 103
```

```
c:\>dig www.krdnsv6.or.kr. aaaa +tcp

; <<>> DiG 9.2.3 <<>> www.krdnsv6.or.kr. aaaa +tcp
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.            IN      AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.      1778    IN      AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.          1778    IN      NS      ns2.nic.or.kr.
krdnsv6.or.kr.          1778    IN      NS      ns1.nic.or.kr.

;; Query time: 120 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Thu Jun 24 11:54:54 2004
;; MSG SIZE  rcvd: 103
```

dig의 DNS 질의 소스 IP 주소 지정

CASE 1 : DNS 질의의 IPv6 소스 IP 지정

IPv6 도입에 따라 호스트 들은 IPv4 주소와 IPv6 주소를 모두 갖는 IPv4/IPv6 듀얼스택 호스트가 주종을 이룰 것으로 예상된다.

이때, Global Unicast IPv6 주소는 하나의 인터페이스에 다수가 설정될 수 있다. DNS 질의 점검은 어느 IPv6 주소를 소스 IP 주소로 지정하여 사용할 것인지를 점검할 상황이 발생할 수 있다. IPv6 주소에 따라 방화벽 등에서 차단되는 경우가 있을 수 있고, 네임서버에서 특정한 IPv6 주소에 대해 DNS 서비스를 제한 설정한 경우도 있을 수 있기 때문이다.

dig은 이러한 다수 IP 주소를 지닌 multi-homed 호스트 환경에서 발송 DNS 패킷의 소스 IP 주소를 지정할 수 있는 옵션을 제공한다.

CASE 2 : 존 전송(zone transfer) 소스 IP 지정

슬레이브 네임서버를 구성하는 경우, 슬레이브 네임서버 시스템이 2개 이상의 IP 주소를 가진 환경에서는 존 전송(zone transfer) 요청을 매스터 네임서버로 송출할 때, 어느 IP 주소를 소스 IP 주소로 하여 패킷이 발송될 것인지 예측하기가 어렵니다.

특히, 매스터 네임서버에서 해당 존에 대해 allow-transfer 옵션을 사용하여 접근 가능한 호스트를 IP 주소 기준으로 제한하고 있을 때, 슬레이브 네임서버에서 발생하는 존 전송(zone transfer) 요청 DNS 패킷의 소스 IP 주소는 지정된 IP 주소를 사용해야 할 필요가 있다.

이러한 환경에서 슬레이브 네임서버를 구성하고 이에 대한 진단을 해야 할 경우, dig을 사용하여 어느 소스 IP 주소가 존 전송(zone transfer) 요청이 가능하도록 허용되어 있는지 확인할 수 있다.

-b ip_address	발송 DNS 패킷의 소스 IP 주소를 지정 주의 : ip_address는 시스템에 설정된 IP 주소에 한정됨 디폴트: +novc, +notcp
예시 : 각 옵션 지정, 결과 비교 Note : 패킷의 소스 IP 주소는 패킷 캡쳐 프로그램으로 확인 가능	

```
% dig @2001:dc5:a::222 -b 2001:dc5:a:0:203:baff:fe67:f795 www.krdnsv6.or.kr aaaa

; <<>> DiG 9.2.2 <<>> @2001:dc5:a::222 -b 2001:dc5:a:0:203:baff:fe67:f795 www.krdnsv6.or.kr aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17001
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.           IN     AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.     1800    IN     AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1800    IN     NS     ns2.nic.or.kr.
krdnsv6.or.kr.         1800    IN     NS     ns1.nic.or.kr.

;; Query time: 23 msec
;; SERVER: 2001:dc5:a::222#53(2001:dc5:a::222)
;; WHEN: Thu Jun 24 12:27:31 2004
;; MSG SIZE  rcvd: 103
```

```
% dig @2001:dc5:a::222 -b 2001:dc5:a::200 www.krdnsv6.or.kr aaaa

; <<>> DiG 9.2.2 <<>> @2001:dc5:a::222 -b 2001:dc5:a::200 www.krdnsv6.or.kr aaaa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65004
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.krdnsv6.or.kr.           IN     AAAA

;; ANSWER SECTION:
www.krdnsv6.or.kr.     1788    IN     AAAA    2001:dc5:a::100

;; AUTHORITY SECTION:
krdnsv6.or.kr.         1788    IN     NS     ns2.nic.or.kr.
krdnsv6.or.kr.         1788    IN     NS     ns1.nic.or.kr.

;; Query time: 2 msec
;; SERVER: 2001:dc5:a::222#53(2001:dc5:a::222)
;; WHEN: Thu Jun 24 12:27:43 2004
;; MSG SIZE  rcvd: 103
```

IXFR(Incremental Zone Transfer) 점검

DNS의 기본적인 존 전송(zone transfer)의 데이터 전송 메커니즘은 AXFR (transfer of an entire zone)이다.

그러나 AXFR을 기반한 존 전송(zone transfer) 메커니즘은 도메인 존의 모든 내용을 전송하기 때문에 이에 대한 개선이 필요하게 되었다.

IXFR(Incremental Zone Transfer)는 변경된 도메인 존 내용만을 전송하는 기능을 제공한다. 이로써 도메인 존 전송에 있어 효율적인 데이터 전송이 가능하게 되었다.

DNS 점검 및 문제 분석 중에 IXFR을 사용한 도메인 존 전송에 대한 점검이 필요할 수 있다.
또한, Dynamic Update를 사용한 도메인 존의 데이터 변경 상황을 조회할 필요성도 발생할 수 있다.

이 경우에 QType(DNS 질의 타입)을 IXFR로 하여 dig을 사용한 점검이 가능하다.

관련 RFC: RFC1995, "Incremental Zone Transfer in DNS"

NOTE! : IXFR은 dynamic update 적용 시에 변경된 데이터만 전송
수작업으로 도메인 존 파일을 수정하고 BIND DNS에 반영하는 경우, IXFR로 존 전송(zone transfer) 요청시 AXFR과 동일하게 전체 도메인 존 데이터를 전송함.

ixfr=*serial_number*	QType IXFR을 사용하여 *serial_number* 이후에 변경된 사항을 조회 이는 type 옵션의 IXFR 타입 지정의 경우임

예시 : 각 옵션 지정, 결과 비교

```
c:\>dig @202.31.190.200 dns.test.kr. axfr

; <<>> DiG 9.2.3 <<>> @202.31.190.200 dns.test.kr. axfr
;; global options:  printcmd
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052419 180 180 604800 180
dns.test.kr.          180    IN     NS     ns1.dns.test.kr.
dns.test.kr.          180    IN     NS     ns2.dns.test.kr.
justin01.dns.test.kr.  180    IN     A      203.255.208.31
justin01.dns.test.kr.  180    IN     AAAA   2002:abcd:3456::abcd:3456
www.ngix.dns.test.kr.  60     IN     A      203.254.33.19
www.ngix.dns.test.kr.  60     IN     AAAA   2001:2b8:1::19
ns1.dns.test.kr.       180    IN     A      202.31.190.200
ns1.dns.test.kr.       180    IN     AAAA   2001:dc5:a::200
ns2.dns.test.kr.       180    IN     A      202.31.190.210
ns2.dns.test.kr.       180    IN     AAAA   2001:dc5:a::210
test001.dns.test.kr.   180    IN     A      211.202.78.8
www.vsix.dns.test.kr.  60     IN     CNAME  www2.vsix.dns.test.kr.
www2.vsix.dns.test.kr. 60     IN     A      203.254.33.100
www2.vsix.dns.test.kr. 60     IN     AAAA   2001:2b8:1::100
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052419 180 180 604800 180
;; Query time: 100 msec
;; SERVER: 202.31.190.200#53(202.31.190.200)
;; WHEN: Thu Jun 24 13:01:17 2004
;; XFR size: 16 records
```

```
c:\>dig @202.31.190.200 dns.test.kr. ixfr=2004052415

; <<>> DiG 9.2.3 <<>> @202.31.190.200 dns.test.kr. ixfr=2004052415
;; global options:  printcmd
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052419 180 180 604800 180
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052415 180 180 604800 180
justin01.dns.test.kr.  180    IN     AAAA   2002:abcd:3456::abcd:3456
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052416 180 180 604800 180
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052416 180 180 604800 180
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052417 180 180 604800 180
justin01.dns.test.kr.  180    IN     AAAA   2002:abcd:3456::abcd:3456
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052417 180 180 604800 180
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052418 180 180 604800 180
justin002.dns.test.kr. 60     IN     A      10.0.0.1
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052418 180 180 604800 180
justin002.dns.test.kr. 60     IN     A      10.0.0.1
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052419 180 180 604800 180
dns.test.kr.          180    IN     SOA    ns1.dns.test.kr. admin.dns.test.kr. 2004052419 180 180 604800 180
;; Query time: 120 msec
;; SERVER: 202.31.190.200#53(202.31.190.200)
;; WHEN: Thu Jun 24 13:11:32 2004
;; XFR size: 14 records
```

위의 사례에서는, serial number 2004052415에서 현재의 serial number에 이르기까지의 각 도메인 존의 serial number 버전에 따라 추가/삭제된 리소스레코드 정보가 표시되고 있음을 확인할 수 있다.

AXFR을 사용한 도메인 존 파일 생성 및 수정

AXFR(transfer of an entire zone)을 이용하면 특정 도메인 존(zone)에 속하는 모든 리소스레코드를 조회할 수 있다.

DNS 네임서버를 매스터 네임서버와 슬레이브 네임서버로 구성한 경우, 디폴트로 동작하는 존 전송(zone transfer) 메커니즘에서도 AXFR 타입의 DNS 질의응답을 사용한다.

AXFR은 RFC1035 "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION"에서 정의된 기본적인 DNS 질의 타입 중 하나이다.

AXFR은 TCP 53을 사용하여 네임서버로부터 도메인 존 내의 모든 RR을 전송받는다.

아래의 명령을 수행하면 dig을 사용하여 지정한 도메인 존(zone)의 내용을 호스트에서 확인할 수 있다.

dig @server *domain_zone_name* AXFR

server	이 경우에는 ***domain_zone_name***의 네임서버 중 하나를 지정 이때, 해당 네임서버가 zone transfer를 허용하는 경우, 응답 가능 리커시브 네임서버에 대하여 위 명령을 수행할 수 없음
domain_zone_name	도메인 존(zone)의 네임 SOA RR을 가지는 도메인네임을 의미함
AXFR	transfer of an entire zone

도메인을 다른 네임서버로 이전해야 하는 경우가 있다.
도메인 존 파일을 쉽게 얻을 수 있는 상황이면, 도메인 존 파일을 새로운 네임서버에 바로 적용하는 방법으로 작업할 수 있다.

그러나 급히 이전하거나, 이전 네임서버의 도메인 존 파일을 얻을 수 없는 경우, dig을 사용하여 도메인 존 파일을 쉽게 작성할 수 있다.
단, 이 경우에 이전 네임서버가 존 전송(zone transfer)을 허용하는 상태에서 가능하다.

먼저 원하는 도메인 존(zone)의 네임서버 정보를 파악한다.

SOA 타입 질의를 아래 예시와 같이 수행한다.

예시 : 도메인 존의 SOA RR 및 NS RR 확인
출력 내용에서 매스터 네임서버 및 슬레이브 네임서버 확인

```
c:\>dig dns.test.kr. soa +multiline

; <<>> DiG 9.2.3 <<>> dns.test.kr. soa +multiline
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;dns.test.kr.          IN SOA

;; ANSWER SECTION:
dns.test.kr.          180 IN SOA ns1.dns.test.kr. admin.dns.test.kr. (
                          2004052419 ; serial
                          180        ; refresh (3 minutes)
                          180        ; retry (3 minutes)
                          604800     ; expire (1 week)
                          180        ; minimum (3 minutes)
                          )

;; AUTHORITY SECTION:
dns.test.kr.          180 IN NS ns2.dns.test.kr.
dns.test.kr.          180 IN NS ns1.dns.test.kr.

;; ADDITIONAL SECTION:
ns1.dns.test.kr.       180 IN A 202.31.190.200
ns1.dns.test.kr.       180 IN AAAA 2001:dc5:a::200
ns2.dns.test.kr.       180 IN A 202.31.190.210
ns2.dns.test.kr.       180 IN AAAA 2001:dc5:a::210

;; Query time: 140 msec
;; SERVER: 202.31.190.222#53(202.31.190.222)
;; WHEN: Fri Jun 25 12:10:21 2004
;; MSG SIZE  rcvd: 195
```

위 예시를 기준할 때, DNS.TEST.KR. 도메인 존의 매스터 네임서버는 SOA RR의 MNAME 필드의 값인 "ns1.dns.test.kr."이다.

그리고 DNS.TEST.KR.에 대한 NS RR로 지정된 "ns1.dns.test.kr."과 "ns2.dns.test.kr."이 DNS.TEST.KR. 도메인의 존(zone)이 설정된 네임서버이다.

SOA RR의 MNAME 필드와 동일한 도메인 네임을 가진 "ns1.dns.test.kr."이 매스터 네임서버이다. 그리고 나머지 "ns2.dns.test.kr."이 슬레이브 네임서버이다.

매스터 네임서버 혹은 슬레이브 네임서버를 **server**로 지정하여 dig을 사용한 AXFR 질의를 아래 사례와 같이 수행한다.

예시 : 도메인 존(zone) 내부의 모든 RR 정보를 출력
이 경우, +multiline 옵션 사용

```
c:\>dig @ns1.dns.test.kr. dns.test.kr. axfr +multiline

; <<>> DiG 9.2.3 <<>> @ns1.dns.test.kr. dns.test.kr. axfr +multiline
;; global options:  printcmd
dns.test.kr.          180 IN SOA ns1.dns.test.kr. admin.dns.test.kr. (
                          2004052419 ; serial
                          180       ; refresh (3 minutes)
                          180       ; retry (3 minutes)
                          604800     ; expire (1 week)
                          180       ; minimum (3 minutes)
                          )
dns.test.kr.          180 IN NS ns1.dns.test.kr.
dns.test.kr.          180 IN NS ns2.dns.test.kr.
justin01.dns.test.kr.   180 IN A 203.255.208.31
justin01.dns.test.kr.   180 IN AAAA 2002:abcd:3456::abcd:3456
www.ngix.dns.test.kr.   60 IN A 203.254.33.19
www.ngix.dns.test.kr.   60 IN AAAA 2001:2b8:1::19
ns1.dns.test.kr.       180 IN A 202.31.190.200
ns1.dns.test.kr.       180 IN AAAA 2001:dc5:a::200
ns2.dns.test.kr.       180 IN A 202.31.190.210
ns2.dns.test.kr.       180 IN AAAA 2001:dc5:a::210
test001.dns.test.kr.    180 IN A 211.202.78.8
www.vsix.dns.test.kr.   60 IN CNAME www2.vsix.dns.test.kr.
www2.vsix.dns.test.kr.  60 IN A 203.254.33.100
www2.vsix.dns.test.kr.  60 IN AAAA 2001:2b8:1::100
dns.test.kr.          180 IN SOA ns1.dns.test.kr. admin.dns.test.kr. (
                          2004052419 ; serial
                          180       ; refresh (3 minutes)
                          180       ; retry (3 minutes)
                          604800     ; expire (1 week)
                          180       ; minimum (3 minutes)
                          )
;; Query time: 160 msec
;; SERVER: 202.31.190.200#53(ns1.dns.test.kr.)
;; WHEN: Fri Jun 25 12:10:39 2004
;; XFR size: 16 records
```

위의 사례에서 출력된 내용을 파일로 저장하여 약간의 편집을 한다.

수정 편집할 사항은 대략적으로 아래와 같다.

도메인의 네임서버	DNS.TEST.KR.의 NS RR에 지정된 도메인 네임의 주소를 새로운 매스터 네임서버 및 슬레이브 네임서버 IP 주소로 수정 위 경우, ns1.dns.test.kr. 및 ns2.dns.test.kr.의 A RR 및 AAAA RR 수정
SOA RR	DNS.TEST.KR 네임서버의 도메인네임을 변경하는 경우, SOA RR의 NMAE 필드 값을 새로운 매스터 네임서버 도메인네임으로 변경수정 Serial number를 현재 일자로 수정
중복 SOA RR 삭제	AXFR 결과출력 내용에는 항상 SOA RR이 앞뒤로 중복 포함됨 DNS 응답 프로토콜에서 도메인 존(zone) 내용을 전송 시, 모든 RR의 앞뒤로 도메인 존(zone)의 영역을 구분하는 SOA RR을 표시 따라서 도메인 존 파일로 편집시 맨 끝의 중복 SOA RR을 삭제

이외의 dig이 출력한 사항은 모두 도메인 존(zone) 파일의 comment 표기(;)에

의한 comment이므로 도메인 존 파일로 사용 시 영향을 미치지 않는다.

이로써 간단하게 이전 네임서버에서 도메인 존 정보를 얻어 새로운 도메인 존 파일을 생성하여 새로운 네임서버에 적용할 수 있다.

이와 유사하게 루트 네임서버에 대한 root.cache 또는 root.hint 파일을 생성하여 사용할 수도 있다.

이 경우에는 아래의 명령을 수행한다.

dig @a.root-servers.net. . NS > root.cache

이 결과로 출력된 내용은 아래 예시와 같다.

dig은 도메인 존 파일의 문법에 따라 데이터를 출력한다.
따라서 아래 예시와 같이 dig 자체가 생성하는 내용은 모두 comment 표기(;)로 처리되어 있어, 네임서버에 이 출력결과를 파일로 저장하여 적용하여도 동작에 문제가 발생하지 않는다.

다음은 루트 네임서버의 네임서버 정보를 간편하게 얻는 방법의 예시이다.

```
c:\>dig @a.root-servers.net. . NS > root.cache

c:\>more root.cache

; <<>> DiG 9.2.3 <<>> @a.root-servers.net. . NS
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                          IN     NS

;; ANSWER SECTION:
.                    518400  IN     NS     A.ROOT-SERVERS.NET.
.                    518400  IN     NS     H.ROOT-SERVERS.NET.
.                    518400  IN     NS     C.ROOT-SERVERS.NET.
.                    518400  IN     NS     G.ROOT-SERVERS.NET.
.                    518400  IN     NS     F.ROOT-SERVERS.NET.
.                    518400  IN     NS     B.ROOT-SERVERS.NET.
.                    518400  IN     NS     J.ROOT-SERVERS.NET.
.                    518400  IN     NS     K.ROOT-SERVERS.NET.
.                    518400  IN     NS     L.ROOT-SERVERS.NET.
.                    518400  IN     NS     M.ROOT-SERVERS.NET.
.                    518400  IN     NS     I.ROOT-SERVERS.NET.
.                    518400  IN     NS     E.ROOT-SERVERS.NET.
.                    518400  IN     NS     D.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN     A      198.41.0.4
H.ROOT-SERVERS.NET.     3600000 IN     A      128.63.2.53
C.ROOT-SERVERS.NET.     3600000 IN     A      192.33.4.12
G.ROOT-SERVERS.NET.     3600000 IN     A      192.112.36.4
F.ROOT-SERVERS.NET.     3600000 IN     A      192.5.5.241
B.ROOT-SERVERS.NET.     3600000 IN     A      192.228.79.201
J.ROOT-SERVERS.NET.     3600000 IN     A      192.58.128.30
K.ROOT-SERVERS.NET.     3600000 IN     A      193.0.14.129
L.ROOT-SERVERS.NET.     3600000 IN     A      198.32.64.12
M.ROOT-SERVERS.NET.     3600000 IN     A      202.12.27.33
I.ROOT-SERVERS.NET.     3600000 IN     A      192.36.148.17
E.ROOT-SERVERS.NET.     3600000 IN     A      192.203.230.10
D.ROOT-SERVERS.NET.     3600000 IN     A      128.8.10.90

;; Query time: 220 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net.)
;; WHEN: Fri Jun 25 12:35:15 2004
;; MSG SIZE  rcvd: 436
```

EDNS0 기능을 사용한 점검

EDNS0는 DNS의 한계를 극복하기 위해 확장된 옵션 RR이다.

하나의 예로서, DNS는 UDP 메시지로 질의 응답할 때, DNS 메시지 크기가 512 바이트를 초과할 수 없다는 한계를 지니고 있다.

만일 네임서버에서 DNS 응답을 할 때, 512 바이트를 초과하는 DNS 메시지가 생성되었다면, 네임서버는 DNS Header flag 중 TC(Truncation) 플래그를 1로 세팅하여 응답한다. 이는 512 바이트 크기를 초과하여 응답 메시지의 정보내용이 충분한 정보가 아니라는 것을 의미한다.

TC 플래그가 세팅된 DNS 응답메시지를 받은 호스트는 이 응답메시지를 폐기하고 동일한 내용의 DNS 질의를 TCP 53을 사용하여 재 질의한다.

이 동작은 512 바이트라는 UDP 상의 DNS 메시지 최대 크기제한에서 비롯한다.

EDNS0의 각 필드 중 buffer size를 지정하는 필드가 있다.
buufer size를 512 바이트 이상의 값, 즉 1024 byte, 2048 byte 등으로 지정하는 경우, 512 바이트 이상의 DNS 응답 메시지를 UDP로 응답받을 수 있다.

dig은 아래와 같이 이를 지정하여 점검에 사용할 수 있다.

dig @*server* *domain_name* *type* +bufsize=*size*

예:

dig @202.31.190.222 www.dns.test.kr AAAA +bufsize=2048

NOTE : EDNS0는 아직 본격적으로 활용되지 않고 있음
ENDS0는 다양한 확장기능을 제공하고 있지만, 모든 네임서버 및 리졸버가 지원해야 그 기능을 충분히 활용가능
아직은 EDNS0 지원 네임서버 및 리졸버가 많지 않은 상황
그러나 특수한 경우에 DNS 질의응답의 효율성을 위해 부분적으로 적용가능하며 이 경우, dig을 사용한 점검에 EDNS0 옵션을 적용할 수 있음
EDNS0는 IPv6 지원 DNS 체계 및 한글도메인, DNSSEC과 같은 DNS 보안적용의 경우에 관련하여 본격적으로 필요하게 될 기능임

4. dig 유틸리티 설치 및 환경 구성

BIND DNS 패키지에 포함된 dig 유틸리티

dig은 BIND DNS 패키지에 포함된 유틸리티이다.

BIND DNS는 ISC(Internet System Consortium) 사이트에서 배포하고 있다.

구분		사이트 주소
ISC 웹 사이트		http://www.isc.org
ISC FTP 사이트	BIND DNS 8 버전 소스 패키지	ftp://ftp.isc.org/isc/bind/
	BIND DNS 9 버전 소스 패키지	ftp://ftp.isc.org/isc/bind9/
	Windows용 BIND DNS 바이너리 설치 패키지	ftp://ftp.isc.org/isc/bind/contrib/

Unix 및 Linux 계열 호스트에서는 BIND DNS 소스 패키지를 컴파일하고 설치하는 과정에서 dig이 함께 컴파일 되어 설치가 된다.
dig이 디폴트로 설치되는 위치는 '/usr/local/bin'이다.

Windows 계열 OS 호스트에서는 BIND DNS의 바이너리 설치 패키지를 다운로드 받아 압축을 풀면 dig 실행 유틸리티를 얻을 수 있다.

Unix 계열 호스트에서의 dig 사용 환경

dig은 DNS 진단 '어플리케이션'이다.

dig은 다른 어플리케이션과 마찬가지로 시스템 호스트 환경설정 값을 이용하여 동작한다.

/etc/resolv.conf 파일

dig은 옵션 중 '@server'가 지정되지 않은 경우, /etc/resolv.conf 파일의 nameserver에 설정된 IP 주소를 DNS 질의를 할 디폴트 네임서버로 사용한다.

/etc/hosts 파일

dig 실행시에 '@server'가 IP 주소가 아닌 네임으로 지정된 경우, dig은 이 'server' 네임을 시스템 OS 함수를 호출하여 IP 주소를 파악한다.

곧, dig은 '@server'에 지정된 도메인 네임 또는 니모닉만큼은 스스로 DNS 절차를 수행하지 않고 시스템 환경에서 그 IP 주소 정보를 파악한다.

따라서 /etc/hosts에 아래와 같이 니모닉이 설정되어 있는 경우,
'dig @krdns www.krdnsv6.or.kr.'을 수행하면, dig은 'krdns'의 IP 주소를 '202.31.190.222'로 리턴받고 이 주소에 대하여 DNS 질의를 수행한다.

```
$ cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
192.0.2.100             test-pc.krdnsv6.or.kr.

202.31.190.222          krdns
```

Linux 호스트의 경우에는 아래와 같이 /etc/hosts 파일에 IPv6 주소를 사용하여 니모닉 네임 v6dns를 지정하면, 'dig @v6dns www.krdnsv6.or.kr'은 질의대상 네임서버에 대해 "2001:dc5:a::222" 주소를 사용하여 DNS 질의를 수행한다.

```
$ cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
192.0.2.100             test-pc.krdnsv6.or.kr.

2001:dc5:a::222         v6dns
```

Linux에서 위와 같은 IPv6 주소에 대한 니모닉 설정 및 사용이 가능한 것은 Linux OS의 시스템 함수가 /etc/hosts 파일의 IPv6 주소 표현 문자열을 해석할 수 있기 때문이다.

Windows 계열 호스트의 dig 설치 및 관련 환경 설정

ISC의 Windows용 설치 바이너리 패키지를 다운로드 받는다.

특정 디렉토리를 정하여 압축파일을 풀어내면 BIND DNS의 Windows용 실행파일들이 해당 디렉토리에 존재하게 된다.

이 중에서 BIND DNS 서버 설치용 실행파일은 “BINDInstall.exe”이다.
Windows 호스트에 BIND DNS 서버를 설치하는 경우에는 이 설치 실행 파일을 실행한다.

단지 dig 등의 BIND DNS 유틸리티만 사용하려는 경우에는 아래의 절차를 수

행하여 dig 및 기타 유틸리티 사용을 위한 시스템 환경 설정을 한다.

BIND DNS 실행파일을 저장한 디렉토리를 "C:\bind"라고 가정한다면, PC에서 "내 컴퓨터" -> "속성" 또는 "등록정보" -> "고급" -> "환경변수"를 선택한다.
"환경변수" 창에서 "시스템 변수"의 변수 중 "Path"를 선택하여 "편집" 기능으로 "Path" 변수 값의 문자열 끝에 ";C:\bind"를 추가한다.

"C:\WINNT\SYSTEM32\DRIVERS\ETC" 디렉토리에 resolv.conf 파일을 작성, 저장한다.
resolv.conf 파일에는 아래와 같은 형식으로 디폴트 네임서버 IP 주소를 저장한다.

```
namserver 192.0.2.222
```

NOTE : Windows 시스템의 hosts 파일, resolv.conf 파일, services 파일
Windows NT, Windows 2000, Windows XP, Windows 2003 등의 Windows OS가 설치된 호스트에서는 Unix 및 Linux의 /etc 디렉토리에 있는 hosts, resolv.conf, services, networks, protocols 파일에 해당하는 시스템 환경구성 파일들은 "C:\WINNT\SYSTEM32\DRIVERS\ETC"에 위치한다.
시스템 OS에 따라서 디렉토리는 "C:\WINDOWS\SYSTEM32\DRIVERS\ETC"가 될 수도 있다.

이로써 시스템 상에서 BIND DNS에 포함된 유틸리티들을 실행할 수 있는 설정을 완료한다.

NOTE! : BIND DNS의 Windows OS 시스템 IPv6 스택 미지원
Windows XP, Windows 2003 서버는 IPv6를 지원하는 OS
Windows 2000의 경우, "Microsoft IPv6 Technology Preview for Windows 2000"를 설치하여 IPv6 지원환경 구성 가능
그러나 BIND DNS는 아직 Windows 계열 OS의 IPv6 스택을 지원하지 않음
BIND DNS의 dig을 포함한 유틸리티들도 IPv6 패킷기반 DNS 통신은 불가능
따라서 Windows 호스트에서 아래의 명령은 실행시 에러발생
"dig @2001:dc5:a::222 www.krdnsv6.or.kr AAAA"