# DNS mit BIND

## Ausgangslage

Um unsere geplante Web-Umgebung erfolgreich zu betreiben, benötigen wir einen Namenserver (DNS). Als erstes werden wir uns als Kurzrepetition etwas die Theorie auffrischen. DNS wurde schon im Modul 300 (resp. 123 / 127 im ÜK) behandelt.

## Aufgaben

Lösen Sie mit Hilfe des ausgeteilten Dokumentes art239-alle Artikel im Kapitel Domain Name System auf den Seiten **7-12** die folgenden Aufgaben:

Skizzieren Sie den DNS-Hierarchiebaum für folgender Domäne:   
*www.bbzbl.ch* und mit der IP *94.126.16.60*?

Öffnen Sie die Webseite von Switch (<https://www.nic.ch/de/whois>)

* Suchen Sie den Halter der Domäne *bbzbl.ch*

Notieren Sie stichwortartig Ihre Erkenntnisse:

Öffnen Sie die Webseite <https://www.whois.com/whois/>

* Kontrollieren Sie, wo sich der Root-Server 198.41.0.4 befindet?
* Versuchen Sie den Standort des Servers 193.0.14.129 zu ermitteln?

Starten Sie den Router vmLF1 und den PC vmWP2. Öffnen Sie auf dem vmWP2 die Webseite [www.bbzbl.ch](http://www.bbzbl.ch). Wird die Anfrage vom vmWP2 aus nun rekursiv oder iterativ durchgeführt? Wie können Sie es herausfinden?

Bereiten Sie den vmWP2 auf die Untersuchung einer DNS-Anfrage vor:

* Öffnen Sie mit Start -> Ausführen -> cmd eine Eingabeaufforderung
* Löschen Sie mit dem Befehl ipconfig /flushdns den lokalen DNS-Cache
* Öffnen Sie das Programm Wireshark und wählen Sie die Aufzeichnung auf dem Adapter VMWare Ethernet Adapter
* Erzeugen Sie mit dem Befehl ping www.bbzbl.ch eine DNS-Abfrage
* Wechseln Sie in den wireshark und untersuchen Sie  
  die **Forward** **DNS-Abfrage (Standard query)**:

| * Mit welchem Protokoll wird die DNS-Abfrage durchgeführt? |  |
| --- | --- |
| * Was steht im QR-Feld und was bedeutet dieser? |  |
| * Welche Bedeutung hat der Wert im RD-Feld? |  |
| * Wie viele DNS-Anfragen stehen im Question-Feld? |  |
| * Wie viele RR stehen im Answer-Feld? |  |
| * Flags: 0x0100 (Standard query) bedeutet? |  |

* Untersuchen Sie als nächstes **die** **DNS-Antwort (Standard query response)**:

| * Wie viele RR stehen im Answer-Feld? |  |
| --- | --- |
| * Welche RR-Typen stehen im Answer-Feld? |  |

Untersuchen Sie nun **die** **Reverse-DNS Auflösung**:

* Löschen Sie erneut mit dem Befehl ipconfig /flushdns den lokalen DNS-Cache
* Starten Sie mit dem Wireshark eine neue Aufzeichnung auf dem Adapter Ethernet0
* Erzeugen Sie mit dem Befehl nslookup 94.126.16.60 eine Reverse-DNS-Abfrage
* Untersuchen Sie als nächstes **die** **DNS-Antwort (Standard query response)**:

| * Wie viele DNS-Abfragen werden gemacht? |  |
| --- | --- |
| * Wie viele RR stehen im Answer-Feld? |  |
| * Welche RR-Typen stehen im Answer-Feld? |  |

**Zeit: 30 Min.**