TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze
Prof. Anja Feldmann, Marco Canini, Petr Kuznetsov, Stefan Schmid
Arne Ludwig, Oliver Hohlfeld, Juhoon Kim, Thomas Krenc, Enric Pujol, Felix Poloczek

2nd Assignment: Network Protocols and Architectures, WS 12/13

Question 1: $(10 + 10 + 10 + 10 = 40$ points) *Domain Name System*

(a) Use one of the tools `nslookup` or `dig` to send DNS queries to three DNS servers: Your local DNS server (default DNS server) and the two DNS servers you found using a whois database[1] for some domains. Issue a query for each of the different kinds of record types: `A`, `NS`, and `MX` to each of the three DNS servers. This should lead to nine queries. Summarize your findings.

(b) Use any of the tools to find a Web server that has multiple IP addresses. Does the `www.net.t-labs.tu-berlin.de` have multiple IP addresses?

(c) If a hostname has multiple IP addresses which of the IPs is used? How and for which purpose can this be leveraged?

(d) DNS is using UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

Question 2: $(30 + 10 = 40$ points) *Content Distribution Networks*

(a) A Content Distribution Network (CDN) replicates the same content in many locations throughout the world. A CDN typically directs clients to the appropriate replica by returning customized answers to DNS queries (e. g., by controlling the response to a request for the IP address of `www.tagesschau.de`).

Use a DNS lookup utility like *dig* to find two sites other than `www.tagesschau.de` that use a CDN. (Hint: Examine popular web sites.) You will find the usage of CDNs by examining the DNS records provided in the *Answer Section* of the dig output. Which CDN is used (guess from the names in the DNS records)? Which observations can you make regarding the DNS records used to provide the CDN functionality? (try to explain your observations) Try to locate the IP of the used CDN cache servers using a whois database (e. g., ripe.net): In which network/ISP is the server located?

You *can* try to query the same site from different locations (e. g., university vs. home, or two different ISPs) and compare the results.

Describe your observations.

(b) Compare the DNS Time-to-Live (TTL) for different DNS records (e. g., A vs. CNAME). Do they differ? If so, which one is smaller? Why do you think this is the case? Provide two negative implications of having a small TTL value.

Please turn!

[1] See `http://www.ripe.net/whois`, `http://whois.arin.net/ui` or `http://www.denic.de/de/whois/index.jsp`.

Question 3: (20 points) *Application Layer Protocols*

Choose *one* of the application layer protocols listed below:
SMTP, POP3, IMAP, IRC, Jabber/XMPP, NTP, NNTP, SIP, RTP, Gopher, DHCP, SSH.
If you think an interesting protocol is missing, you can also propose one. (We will not accept suggestions like HTTP and DNS that were extensively discussed.)

Start some research on the chosen protocol and try to briefly discuss it along the following lines:

(a) Briefly (!) summarize its purpose and basic functionality.

(b) Which transport layer protocol does it use?

(c) Is the protocol standardized? Can you find the standard? (Hint: `http://www.ietf.org/rfc.html`)

Question 4: (10 points) *Worksheet 1 - question 4b)*

Reminder: If you did not already submitted the answer to question 4b) (first worksheet), you can do it here.

Due Date: Thursday, November, 8th 2012 only until 13:55 h s. t.

- **As PDF files (no MS Office or OpenOffice files):** Uploaded via ISIS (`https://www.isis.tu-berlin.de/course/view.php?id=7028`)
- **On paper:** Postbox in the Telefunkenhochhaus (basement, behind the doorman right)
- Put your name, StudentID number (Matrikelnummer) **and** the name of your tutor on your solution.