

Fragensammlung Netzwerktechnologien Layer 5 und höher

DHCP

Was bedeutet DHCP? (1 P.)

- Dynamic Host Configuration Protocol

welche Probleme löst DHCP? (2 P.)

- Manuelle Vergabe und Wartung von IP Adressen ist zeitaufwändig und fehlerbehaftet
- Doppelte Vergabe von IP Adressen

Welche Informationen teilt ein DHCP Server dem Client mit? maximal erreichbar (5 P.)

- IP Adresse
- Netzmaske
- Nameserver
- Dauer der Lease
- Zeitserver

DNS

Was bedeutet das Kürzel DNS?

- Domain Name Service

Was heißt DNS und was wird dadurch möglich? (2 P.)

- Domain Name Service
- Auflösung von Name zu IP Adresse
- Auflösung von IP Adresse zu einem Hostnamen

Was ist der Unterschied zwischen einem "autoritativen" und einem "rekursiven" DNS-Server?

- rekursiv: kommuniziert mit anderen (authoritativen) DNS Servern
- rekursiv: Aufgabe ist, für Endgeräte Antworten zu finden
- rekursive hat keine eigenen Daten ausser den DNS ROOT Server IP Adressen
- autoritativ: Hat eigene Zonen (=Domain) Informationen

Beim Verbinden Ihres Handys mit einem WLAN kriegt es u.A. die IP-Adresse eines DNS-Servers. Ist dieser *rekursiv* oder *autoritativ*?

- rekursiv

Was versteht man unter einem DNS-Root-Server?

- autoritativ für alle NS-Einträge aller Top-Level-Domains, es gibt eine fixe Liste mit Root-Servern, 13 Stück

Ist ein DNS-Root-Server *rekursiv* oder *autoritativ*?

- autoritativ

Erklären Sie, warum man DNS als eine *hierarchische Datenbank* bezeichnet!

- Weil es eine Baumstruktur ist
- Weil delegiert, also weitergeleitet wird

Was bedeutet das Kürzel TLD?

- Top Level Domain

Was verstehen Sie unter dem Begriff "Delegation" im Zusammenhang mit DNS?

- Die Information über NS-Einträge von einer Domain wird mitgeteilt.

Auf welchem Standard-Port ist das DNS-Service erreichbar?

- 53 UDP

Whois

Welche Informationen können mittels "whois" abgefragt werden? (4 P.)

- Daten zu einer Person einer Domain
- Eigentümer
- Standort
- Nameserver
- Registrar
- IP Adressen

Was bedeutet das Kürzel "AS" und was bedeutet es? (2 P.)

- Autonomes System
- Eine Ansammlung von mehreren Netzen unter Verwaltung einer administrativen Instanz

Organisationen

Welche Organisation verwaltet die Vergabe von IP-Ranges (Subnets) in Europa? (1 P.)

- RIPE

Ein Land beschließt, keine Sommerzeit mehr zu machen. Welche Organisation muß die Verwaltung dieses Landes informieren? (1 P.)

- IANA

Welche Organisation verwaltet Standard-Portnummern?

- IANA

Was bedeutet das Kürzel IANA?

- Internet Assigned Numbers Authority

Welche Organisation betreut die Internet RFC's?

- IETF Internet Engineering Task Force

Was sind Internet RFC's?

- technische Spezifikationen für Internet Technologien
- "Request for Comments"

NTP

Wofür steht NTP?

- Network Time Protocol

Wofür steht UTC?

- Universal Time Coordinated

Welche Ports werden von NTP verwendet

- TCP + UDP 123

Was bedeutet "Stratum" im Zusammenhang mit NTP?

- "Abstand" .. wieviele Hops zur Atomuhr / ultimativen Zeitquelle

Ist ein niedriger oder ein hoher Stratum-Wert Anzeichen einer sehr guten Zeitquelle?

- niedrig

Was ist eine Zeitquelle und welche kennen Sie?

- GPS, Atomuhr (stratum 1)
- Jeder NTP Server

NTP ermöglicht eine Genauigkeit von welcher Größenordnung typischerweise für Endgeräte? (Minuten, Sekunden, ms (Millisekunden), μ s (Mikrosekunden) ns (Nanosekunden))

- Millisekunden

Wie viele Millisekunden hat eine Sekunde?

- 1000

Wie viele Millisekunden hat eine Minute?

- 60_000

Wie viele Mikrosekunden hat eine Sekunde?

- 1_000_000

Wie viele Nanosekunden hat eine Millisekunde?

- 1000

Wie wird die Umstellung von Winterzeit auf Sommerzeit in NTP durchgeführt?

- gar nicht!

Gibt es in der NTP-Zeit Sommerzeit, Winterzeit, und Schaltjahre?

- nein!

Gibt es in der NTP-Zeit *Sprünge*? Und falls ja, welche?

- Ja, Schaltsekunde, alle 2-5 Jahre nötig

Die NTP-Zeit ist ja im ganzen Internet überall die gleiche. Wodurch ist es trotzdem möglich, daß unsere Rechner und Handys die europäische Zeit haben, obwohl sie ja mit NTP synchronisiert sind?

- Zeitzonen Dateien

IP / UDP / TCP

Was versteht man unter einem Socket? Wofür braucht man das?

- Kombination IP:Portnummer

Wie viele Sockets werden für eine Netzwerkverbindung benötigt?

- 2

Was versteht man unter einem *socketpair*? Begründen Sie Ihre Antwort!

- Wenn sich 2 Sockets verbinden

Was verstehen Sie beim Thema IP unter einem *Port*? Erläutern Sie!

- Adresse eines Dienstes

Wodurch unterscheiden sich UDP und TCP im Wesentlichen?

- TCP ist sicherer und gibt Garantien, UDP ist schneller
- Wenn es Übertragungsfehler gibt, bekommt die Anwendung eine Fehlermeldung bei TCP, bei UDP nicht immer

Wie lautet die größtmögliche IP-Port-Nummer?

- $256^2 - 1$ oder 0xFFFF oder 65535

Was kann man mit dem Programm *wireshark* machen?

- Netzwerktraffic analysieren

Fragen zu VPN

Nennen Sie zwei typische Problemstellungen, für welche VPN eine Lösung ist.

- Dem Internet Provider nicht verraten was man surft.
- Zugriff auf Intranet wird von außen möglich.
- Zugriffe aus einem anderen Land simulieren, zB für Streaming Angebote

Was wird in RFC 1918 festgelegt?

- Welche Netze nicht im Internet erreichbar sind.
- Adressen für privates Netzwerk

Fragen zu NAT

Wofür steht das Kürzel NAT?

- Network Address Translation

Erklären Sie in einigen Sätzen die Funktionsweise von NAT

- NAT Router "versteckt" die privaten (RFC1819) Adressen hinter seiner eigenen offiziellen IP (tauscht aus)

Was versteht man unter "reverse NAT"? Erklären Sie in eigenen Worten!

- Wenn "hinter" einer offiziellen IP mehrere Server antworten sollen.

Sicherheit

Was bedeutet Authentisierung?

- System weiß, wer man ist, wer Du bist

Was ist die so genannte Two-Factor Authentisierung?

- zweifache Authentisierung, z.B. Email mit Link drinnen oder SMS mit Code.

Was bedeutet Autorisierung?

- System erlaubt oder verbietet bestimmte Aktionen abhängig davon wer ich bin im System
- Zuweisung von Rollen

Wodurch unterscheidet sich symmetrische von asymmetrischer Kryptographie?

- symmetrisch: Gleicher Schlüssel zum Ver- und Entschlüsseln
- asymmetrisch: Unterschiedliche Schlüssel zum Ver- und Entschlüsseln

Welches Problem löst das Diffie-Helman Verfahren?

- Dass beim Vereinbaren eines Schlüssel andere mithören.

Ist das Diffie-Helman Verfahren der symmetrischen oder asymmetrischen Kryptographie zuzuordnen?

- asymmetrisch, und ermittelt einen symmetrischen Schlüssel

Welche Informationen sind in Digitalen Zertifikaten enthalten?

- Wer ist Ersteller
- Wer ist Eigentümer
- Gültigkeitszeitraum

Welche besondere Eigenschaft hat ein Root-Zertifikat? (Stammzertifikat)

- Subject und Issuer sind gleich

Kann ein Zertifikat abgelaufen sein (also nicht mehr gültig)?

- Ja

Unter welchen Umständen ist ein nicht abgelaufenes Zertifikat ungültig?

- wenn es von der CA revoked wurde

Was ist eine Certificate Chain?

- Zwischen-CA's sind beteiligt

Was ist ein Hash-Algorithmus?

- Erzeugung von Prüfsummen

Was versteht man unter einer CA?

- Erzeugung von Zertifikaten

Welche Aufgaben hat eine CA?

- Erzeugung von Zertifikaten
- Zuordnung zu Personen für Missbrauchsfälle

Woher kann man ein digitales Zertifikat bekommen?

- Vom Provider / einer CA

Wie heißt das wichtigste Opensource-Werkzeug rund um das Thema Kryptographie?

- openssl

Könnte man theoretisch mit openssl eine Certificate Authority selber bauen?

- ja

Was versteht man unter dem Terminus "security by obscurity"?

- Sicherheit durch Geheimhaltung der Algorithmen

Was besagt das Kerckhoff'sche Prinzip?

- Nur die Geheimnisse sollen sicher sein, die Algorithmen öffentlich