### Grundlagen der Datenübertragung (z.B. Übertragungsmedien)

##### Vorteile:

* Schnellerer Zugriff auf gemeinsame Daten(-banken)
* Gemeinsame Nutzung von Hardwareprodukten (z.B. Drucker)
* Gemeinsame Nutzung von verfügbaren Ressourcen (Rechenleistung, Speicherkapazität, Software, Internetzugang)
* Allgemeiner Informationsaustausch untereinander (vergleichsweise schnell)

###### Risiken:

* Fremdzugriff bzw. allgemeiner Missbrauch (zusätzliche Angriffsmöglichkeit)
* Je nach Art des Netzwerkes, sind die Geräte voneinander abhängig
* Viren können sich leichter verbreiten
* Datenverlust bei unzureichender Sicherung

### IPv4 und IPv4-Adressen (Internet Protocol Version 4)

* 4 Byte – 32 Bit
* Weltweit gibt es 2^32 = 4,3 Mrd. verschiedene IPv4 Adressen
* Kleinste Adresse 🡪 Netzwerkadresse
* Größte Adresse 🡪 Broadcastadresse
* Damit zwei Rechner kommunizieren können müssen sie im Gleichen Subnetz sein

### MAC-Adressen

* MAC steht für „Media Access Control”
* **Eindeutige Identifikation** eines Gerätes im Subnetz (unveränderlich)
* Länge von 48 Bit, eingeteilt in Sechs 2er-Blöcke

Arbeitet auf **Sicherungsschicht**

Anzahl verfügbarer MAC-Adressen: 248 = 1612 = (24)12 = 24\*12 = 281 Billionen

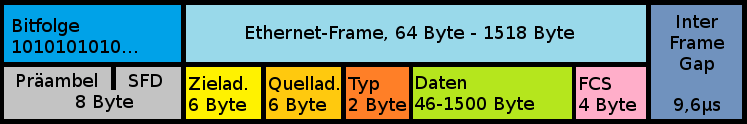
FF:FF:FF:FF:FF:FF ist die Broadcast-MAC und spricht alle Geräte gleichzeitig an

Werden nur zu Kommunikation im Subnetz verwenden, daher kann es mehrmals die gleiche geben

### ARP-Protokoll - Adresse Resolution Protokoll

* Protokoll, dass zu einer IP-Adresse die zugehörige physikalische Adresse (MAC) ermittelt

### Ethernet

* Arbeitet auf **Sicherungsschicht**
* Für Kommunikation von Nachbar zu Nachbar (im Subnetz) läuft über MAC Adresse

### OSI-Modell (Open system Interconnection)

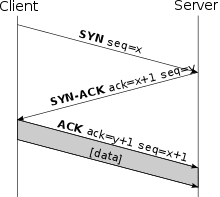
Referenzmodell, mit dem sich die Kommunikation zwischen verschiedenen technischen Systemen beschreiben und definieren lässt

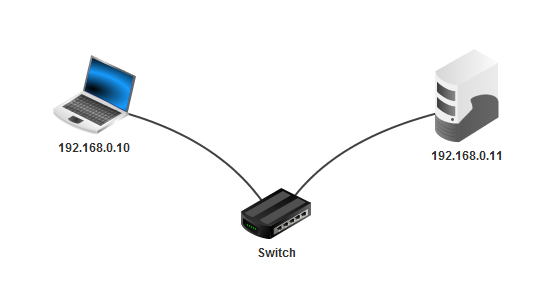
|  |  |  |
| --- | --- | --- |
| 1 | Bitübertragungsschicht | physikalische Anpassung der Bits auf das Übertragungsmedium |
| 2 | Sicherungsschicht | Segmentierung der Daten und Sicherung mit Prüfsummen |
| 3 | Vermittlungsschicht | Vermittlung der Pakete zum nächsten Netzwerkknoten |
| 4 | Transportschicht | Zuteilung von Daten zur Anwendung |
| 5 | Sitzungsschicht | Steuerung und Kontrolle der Verbindung |
| 6 | Darstellungsschicht | Wandlung der Daten in unabhängige Format |
| 7 | Anwendungsschicht | Bereitstellung von Funktionen der Anwendung wie die Daten ein- und -ausgabe |

### TCP - Transmission Control Protocol: (4te Layer)

* Nötig für den zuverlässigen und verbindungsorientierten[[1]](#footnote-1) Datentransport in Computernetzwerken
* Verbindungsart, die es ermöglicht Daten völlig unabhängig voneinander und in beide Richtungen zu übertragen
* Soll einen Paketverlust während der Kommunikation verhindern

# Filius (alles, was wir im Unterricht behandelt haben)

Kommunikation eines einfachen Clients mit einem Echo-Server:



Portnummern:

* Mehrstellige Ziffer, die die einzelnen Dienste eines Rechners kennzeichnet
* Portnummern sind „Unter-Adressen“, die angeben an welche Anwendung ein Datenpaket adressiert wird
* Anhand der Portnummer wird das Datenpaket im Zielrechner an die Zielanwendung weitergegeben
* Portnummern werden durch einen Doppelpunkt getrennt an die IP-Adresse angehängt (siehe oben)
* Gängige Portnummern:

|  |  |  |
| --- | --- | --- |
| **Portnummer** | **Bezeichnung** | **Zweck** |
| 80 | http | Webseiten, unverschlüsselt veraltet |
| 25 | Smtp | E-Mail-Kommunikation |
| 20/21 | FTP | Dateienübertragung |
| 443 | https | Webseiten, verschlüsselt |

Datenpaketerstellung beim durchlaufen der OSI-Schichten:

7 Anwendung

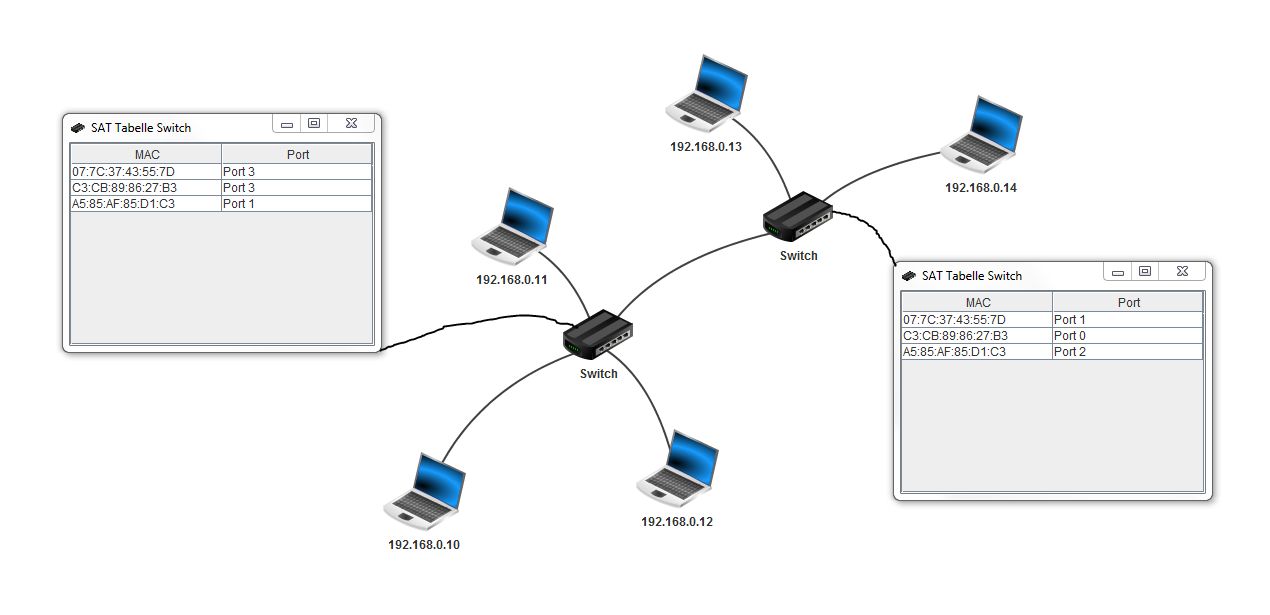
6 Anwendung

5 Anwendung

4 [TCP-Header] [Daten] 🡪 sichere Datenübertragung

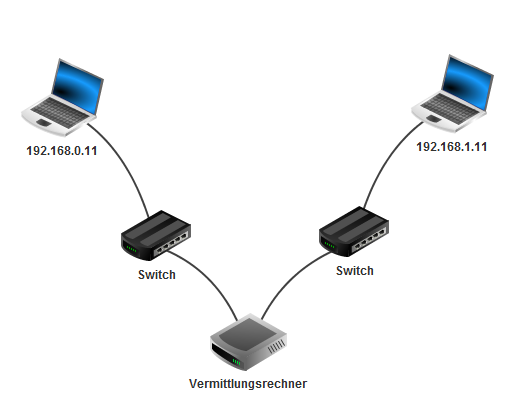
3 [IP-Header] [TCP-Header] [Daten] 🡪 Adressierung

2 [] [Ziel-MAC] [Quell-MAC] [] [IP-Header] [TCP-Header] [Daten] [FCS[[2]](#footnote-2)] 🡪 Adressierung

Switches:

* Dient primär zur Kommunikation innerhalb des Netzwerkes
* Zentraler Knotenpunk in einem Netzwerk mit mehr als zwei Computern
* Die Verbindung über Switches ist nur Offline in einem Subnetz möglich
* Nach der ersten Netzwerkanfrage speichert der Switch in der SAT-Tabelle (siehe Grafik oben) die MAC-Adressen und den zugehörigen Port um Netzwerksignale entsprechend weiterleiten zu können
* Vermittler zwischen Empfänger und Sender (Abbildung 3)
* Kann gleichzeitig Daten senden und empfangen
* Arbeitet auf Layer 2 (OSI-Schichtenmodell)
* Cut-Through => direkte Weiterleitung (Bis zur Quell-MAC wird es ebenfalls zwischengespeichert Vorteil: schneller
* Store and Forward => Daten werden zwischengespeichert Vorteil: Pakete können überprüft werden
* Qualitätsmerkmale: max. Größe der SAT-Tabelle und verfügbare Bandbreite

Vermittlungsrechner (Router):

* Kann mehrere IP bzw. MAC-Adressen haben
* Verbindet zwei unterschiedliche Subnetzwerke (Internet gilt hier ebenfalls als Subnetz) mit einander
* Der Vermittlungsrechner braucht mindestens zwei IP bzw. MAC-Adressen
* Speichert meistverwendete Seiten (Domains) zwischen um den DNS-Server zu entlasten
* Sitzt zwischen Local Area Networks (LANs) und Wide Area Networks

Einfache Installation eines Vermittlungsrechners:

1. Sicherstellen, dass die angeschlossenen Rechner in unterschiedlichen Subnetzen liegen (vgl. Netzwerkteil der IP-Adresse)
2. Jeder Port des Routers erhält eine IP-Adresse aus dem entsprechend „angeschlossenem“ Subnetz (z.B. die Kleinste)
3. An allen Rechner wird als Gateway-Adresse[[3]](#footnote-3) *die* IP-Adresse des Routers eingestellt, welche für das entsprechende Subnetz eingestellt wurde

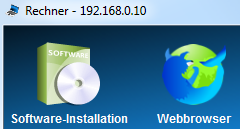
Schematischer Darstellung der Einstellungen für das Netzwerk oben:

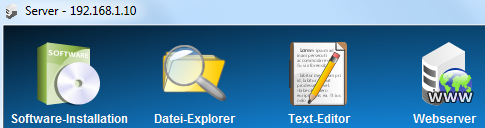
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rechner 1** | | **Switch** | **Vermittlungsrechner** | | **Switch** | **Rechner 2** | |
| IP-Adresse | Gateway | ⬌ |  |  | ⬌ | Gateway | IP-Adresse |
| 192.168.0.11 | 192.168.0.1 | 192.168.0.1 | 192.168.1.1 | 192.168.1.1 | 192.168.1.11 |

Zugriff auf einen Webserver:

Um mit einem Rechner auf eine Website (die auf einem im Aufbau platzierten Webserver liegt) zugreifen zu können, müssen Rechner und Server gemäß dem oben beschriebenen Aufbau über einen Vermittlungsrechner verbunden werden.

Für das Hosten einer Website müssen folgende Anwendungen installiert werden:





**Webbrowser**: Aufrufen der Zielwebsite durch Eingabe der Server-IP

**Datei-Explorer:** Organisation der Websitedateien (Bilddateien, HTML-Dokumente, etc.)

**Texteditor:** Bearbeiten der HTML-Dokumente mit dem Code für die Websites

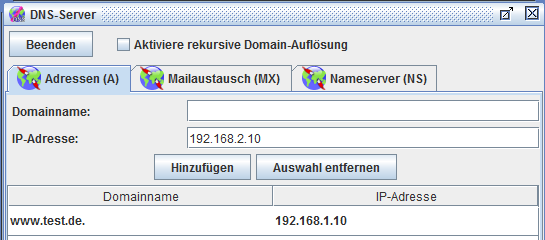
**Webserver:** Nötig zum Verbindungsaufbau zwischen Server und Rechner

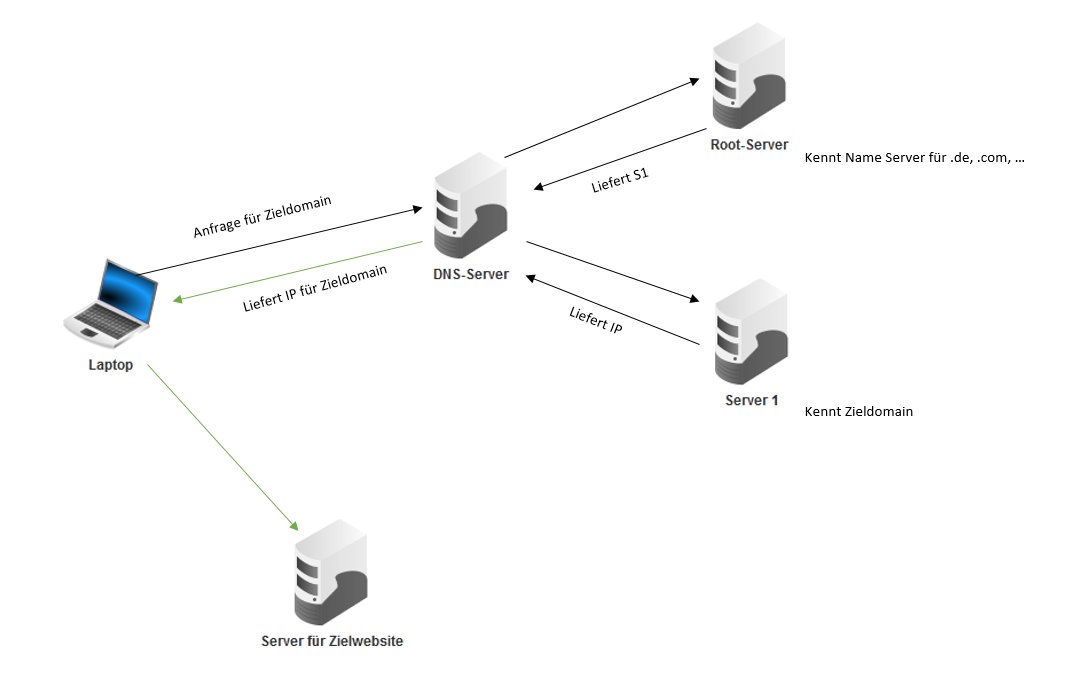
Beim Aufrufen einer Webseite wird zuerst die ***index.html*** Datei gesucht, eine solche muss daher existieren.

Heutzutage werden statt HTML-Dateien (Darstellung statischer Webseiten) PHP-Dateien für attraktivere Webseiten verwendet.

* **Server stellen Dienste bereit, ihr Clints stellen entsprechende Anfragen**

Einsatz von Domains:

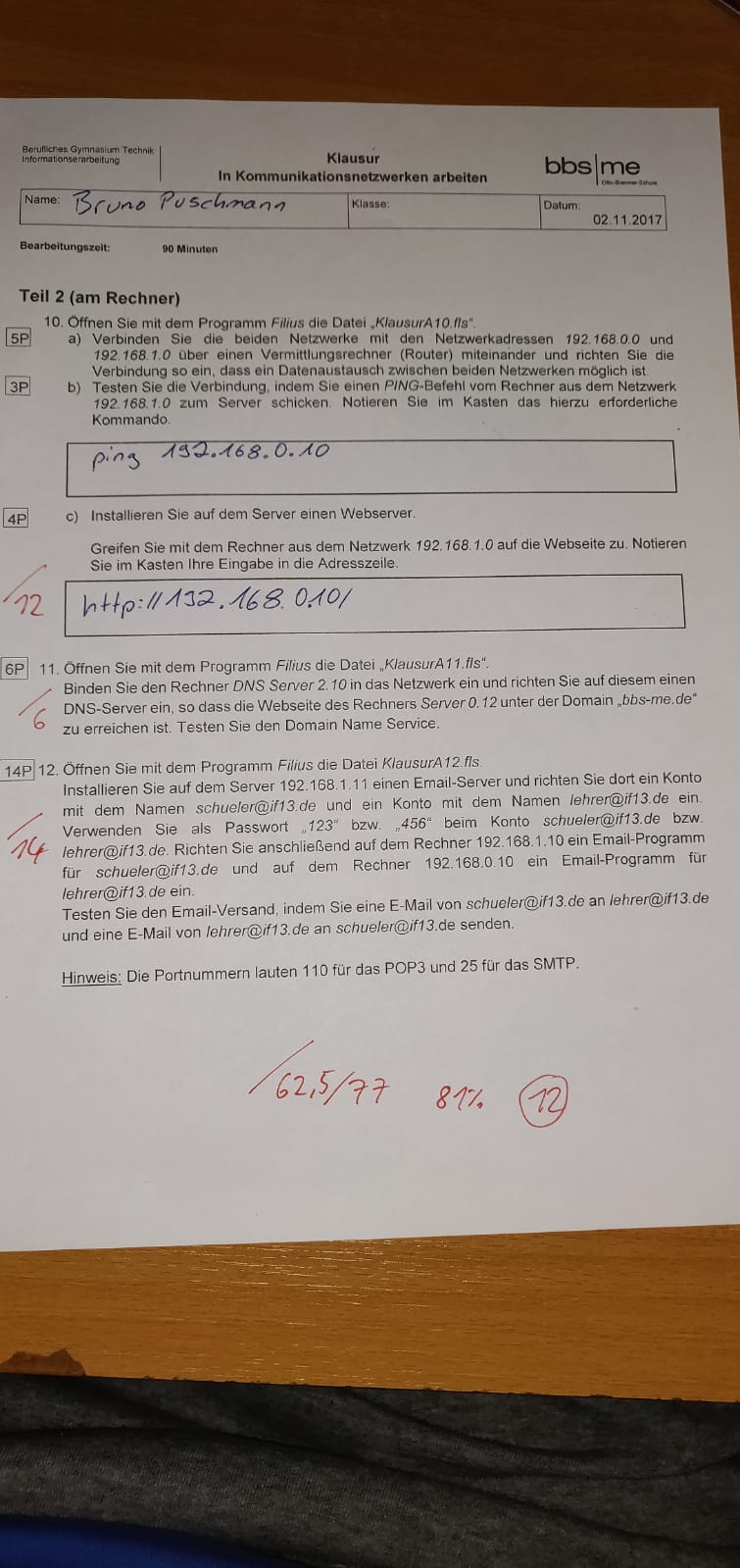
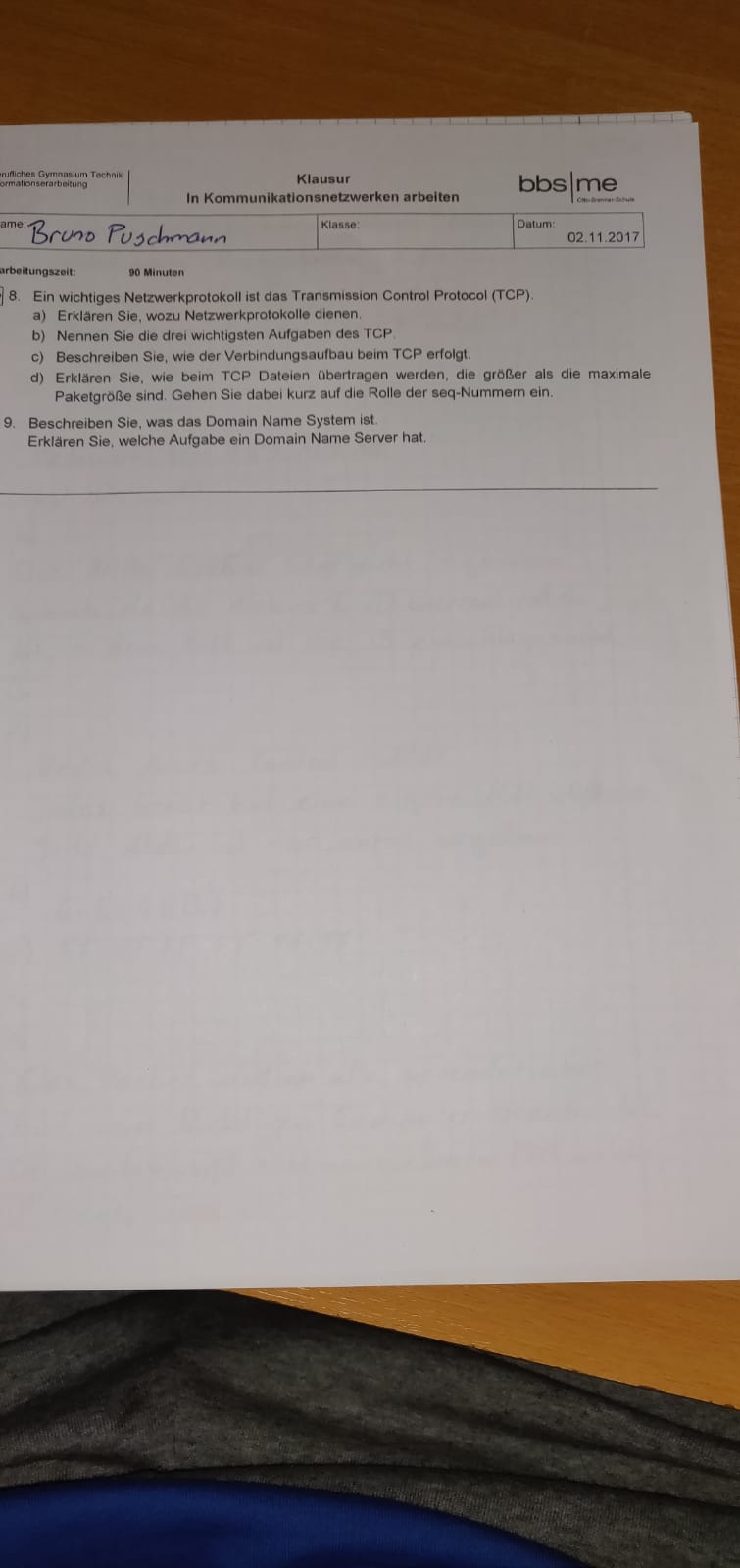
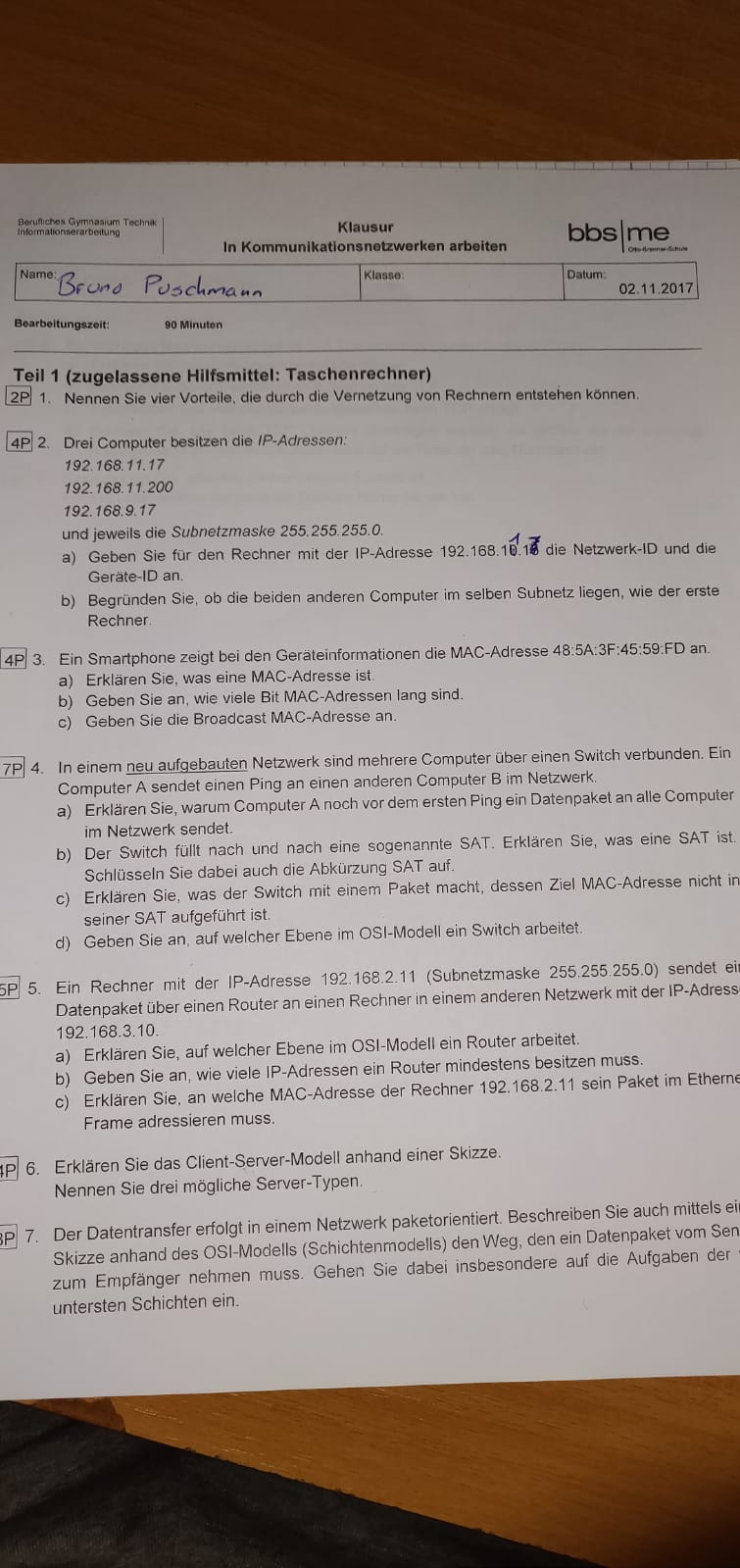
* In Filius können Webseiten durch Eingabe der Server-IP erreicht werden
* Um Domains („Internetadressen“) verwenden zu können, wird ein DNS-Server („Domain Name Service Server“) benötig
* Der DNS-Server enthält die Verknüpfungen zwischen Domainnamen (Verlinkungen zu den entsprechenden Webservern) und den zugehörigen IP-Adressen
* Der DNS-Server wird in einem eigenen Subnetz installiert und über eine Gateway-Adresse mit dem Vermittlungsrechner verbunden
* Damit der DNS-Server korrekt arbeiten kann muss jedem Client im Netzwerk die IP-Adresse des Domain-Name-Server bekannt sein (Einstellungen)
* Ruft ein Client eine Domain auf, verbindet er sich mit dem DNS-Server um an die IP-Adresse zu gelangen (Verwendung des UDP-Protokolls)
* Webseiten im Internet lassen auch trotzdem noch über die IP-Adresse aufrufen (ist diese nicht bekannt kann sie mithilfe eines ping zur Domain über das CMD-Feld herausgefunden werden.
* Der DNS-Server verwaltet nur, die eigentliche Vergabe folgt über eine Organisation



UDP-Protokoll:

* Verwendung bei der DNS-Server-Kommunikation und z.B. Livestreams
* Es findet keine Kontrolle statt, ob die Pakete korrekt ausgetauscht wurden
* DNS-Server sollen nicht überlastet werden, Datenaustausch auf ein Minimum reduziert
* Sollte keine Antwort beim Client ankommen kann die Anfrage einfach nochmal gestellt werden

Klausur



1. [↑](#footnote-ref-1)
2. Frame-Check-Sequenz, Kontrollsumme – Nur Paketkontrolle, [↑](#footnote-ref-2)
3. Gateway = Eingangstor/ Ausgangstor: Adresse für Datenpakete die das Subnetz verlassen [↑](#footnote-ref-3)