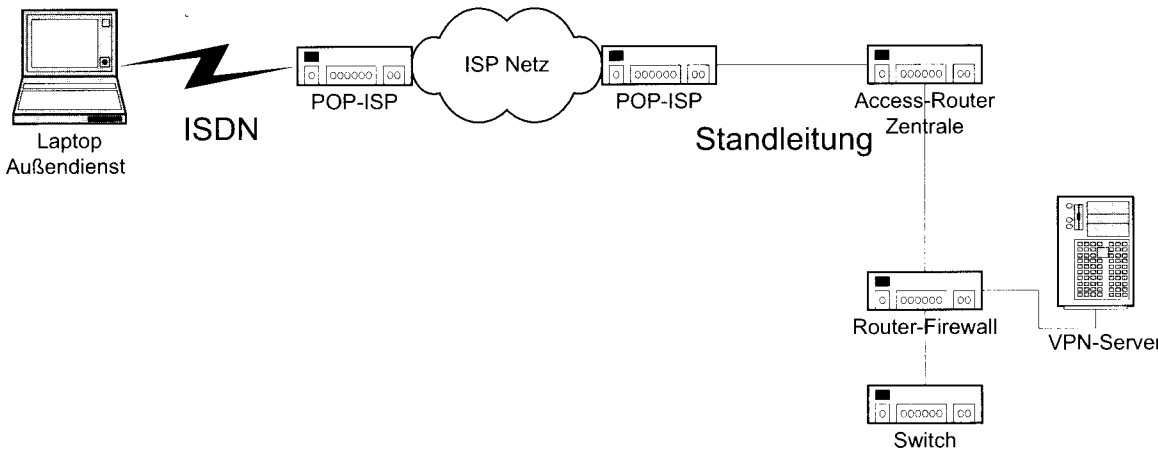
## 1. Handlungsschritt (20 Punkte)

a) Lösungsbeispiel




Andere Netzwerke sind möglich. (8 P.)

ba) Integrität: Schutz der Daten vor Datenverlust. Übertragung einer verschlüsselten Prüfsumme, die erkennen lässt, ob Daten verändert wurden. (2 P.)

bb) Authentizität: Sicherstellung / Gewährleistung der Echtheit von Daten. Die Echtheit der empfangenen Daten wird durch Bedingungen sichergestellt, die auch für den Absender der Daten bindend sind. Damit wird sichergestellt, dass die Daten tatsächlich vom ausgewiesenen Absender stammen. (2 P.)

bc) Vertraulichkeit: Die Daten werden mittels kryptographischer Verfahren vor unbefugten Dritten während einer Übertragung verschlüsselt. Die Daten liegen auf dem Quell- und auf dem Zielrechner unverschlüsselt vor. (2 P.)

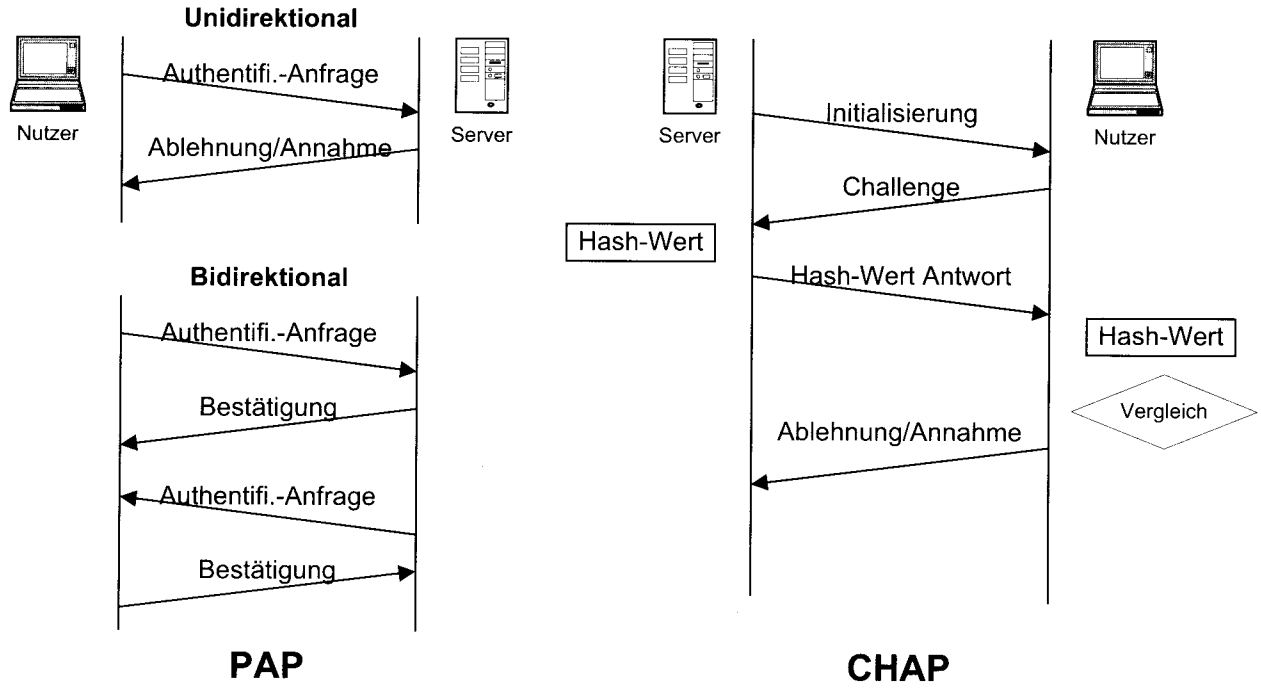
c) Frame Relay FR
- Schnelles paket- und verbindungsorientiertes Verfahren
- Geringe Durchlaufverzögerung
- Paketlänge 261 – 8192 Byte
- *Übertragungsraten 64 kBit/s bis 2,048 Mbit/s*
- Arbeitet auf OSI Schichten 1 und 2 (3 P.)

Asynchronous Transfer Mode ATM
- Multimediafähig
- Übertragungsraten bis 622 Mbit/s
- Zellen mit je 53 Byte (5 Header, 48 Daten)
- Nutz- und Steuerkanäle
- Verbindungsorientierte Multiplex- und Vermittlungstechnik (3 P.)

## 2. Handlungsschritt (20 Punkte)

a) PAP: Password Authentification Protocol
CHAP: Challenge Handshake Protocol

Lösungsvorschlag:




(10 P.)

b)

| | PAP | CHAP |
|---|---|---|
| Vorteil | - Einfache Handhabung und Implementierung<br>- Auch für große Unternehmen geeignet | - Passwörter werden nicht im Klartext übertragen.<br>- Authentifizierung ist auch während einer Verbindung möglich. |
| Nachteil | - Ungeschützt, da Passwörter im Klartext übertragen werden<br>- Keine Vergabe von unterschiedlichen Netzwerkrechten möglich | - Schlecht skalierbar<br>- Keine Vergabe von unterschiedlichen Netzwerkrechten möglich |

(4 P.)

c)

- Datenpakete einschließlich Header werden verschlüsselt mit einem zusätzlich erzeugten Protokollkopf über ein öffentliches (unsicheres) Transitnetz sicher weitergeleitet.
- Ein L2TP-Tunnel kann von einem Endgerät (Dial-in) oder von einem Netzwerk-Server (Dial-out) initiiert werden.
- Ein L2TP-Tunnel ist für den Nutzer des Endgerätes transparent und erfordert keine zusätzlichen Installationen außer der Einwahlmöglichkeit zum POP.
- Über einen L2TP-Tunnel können mehrere logische PPP-Verbindungen aufgebaut werden.
- Zur Authentifizierung kann auf PAP und CHAP zurückgegriffen werden.
- L2TP hat keine eigenen Sicherheitsmechanismen.
- L2TP kann protokollunabhängig eingesetzt werden (IP, IPX, NetBUI, SNA)

(6 P.)

## 3. Handlungsschritt (20 Punkte)

a)
- Telefonnummer
- Benutzerkennung
- Passwort
- ggf. IP- Adresse
- DNS-Server
- u. a.

(3 P.)

ba)
Punkt-zu-Punkt-Protokoll über eine ISDN-Verbindung . . . (1 P.)
- wurde für die Verkapselung von Datagrammen über serielle Leitungen konzipiert.
- unterstützt die Übertragung von LAN-Protokollen über Weitverkehrsnetze.
- soll die Einschränkungen der Interoperabilität aufheben.
- unterstützt herstellerübergreifend Router und Brücken bei WAN-Verbindungen.
- ermöglicht die Übermittlung von Daten über synchrone und asynchrone Wähl- und Standleitungen. (6 P., 3 x 2 P.)

bb) NetBEUI und IPX/SPX (2 P.)

ca) Zuordnung von Domänennamen zu den zugeordneten IP Adressen (4 P.)

cb) hosts (2 P.)

cc) 127.0.0.1 localhost
192.168.0.1 internet proxy.http (2 P.)

## 4. Handlungsschritt (20 Punkte)

a) Eine Firewall überwacht die Kommunikation zwischen zwei Netzen. Sie wird zum Schutz gegen Angriffe aus einem Netz mit geringerem Schutzbedarf eingesetzt. (4 P.)

ba)
- Wenige Möglichkeiten zur Protokollierung
- Missbrauch von Protokollen nicht erkennbar
- Keine Content-Filterung

(2 P.)

bb)
In Abhängigkeit von konfigurierten Filterregeln werden die Pakete
- durchgelassen (allow)

oder
- verworfen (deny)

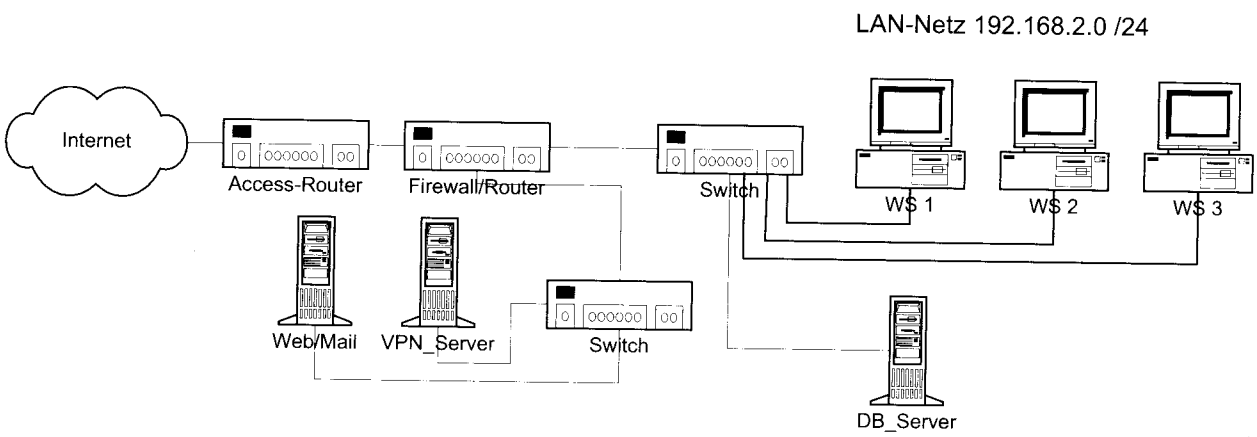
(2 P.)

bc) Mailverkehr ist möglich, da Port 25 (SMTP) nicht gesperrt ist. (3 P.)

ca) Eine DMZ ist ein separates Netzwerk zwischen dem internen LAN und dem Internet. Dabei gilt die DMZ zwar als vertrauenswürdiger als das Internet, die DMZ-Rechner erhalten aber nicht die gleichen Rechte wie die Rechner des LAN. So wird beispielsweise der Traffic von der DMZ zum LAN kontrolliert. Die DMZ ist der Platz für alle Dienste, die direkt mit dem Internet Kontakt aufnehmen müssen. Wenn nun Web- oder Mail-Server attackiert werden, hat dies keinen Einfluss auf die Sicherheit des LAN. (4 P.)

cb) 192.168.x.0/24 für x = 1 bis 254 ohne 2 (internes LAN) (1 P.)

cc) Lösungsvorschlag. Eine Lösung mit zwei Firewalls/Router (intern-extern) ist auch als richtige Lösung zu bewerten.




(4 Punkte)

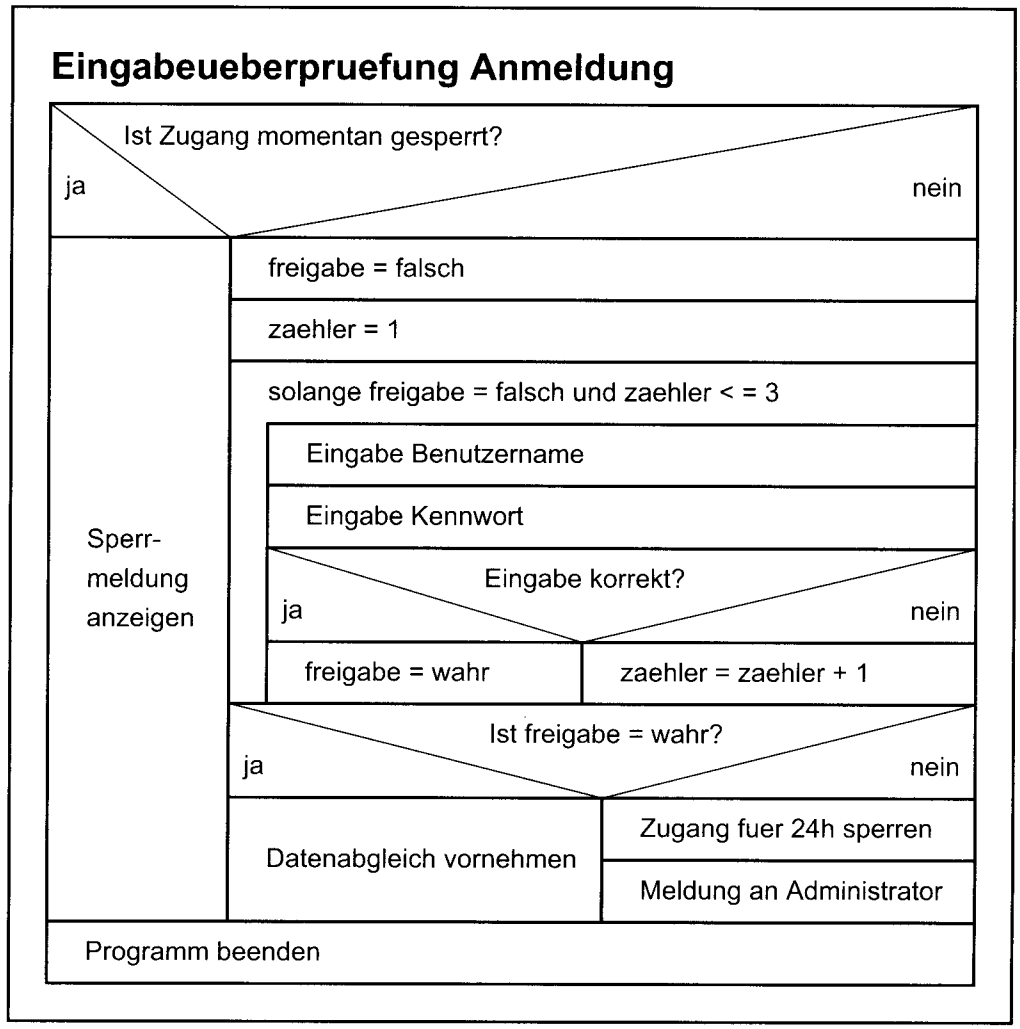
## 5. Handlungsschritt (20 Punkte)

aa) MySQL ist ein Programm, das die Anfragen annimmt, die in SQL geschrieben werden und Antworten zurückliefert.
ab) Mehrere 100.000 oder Millionen Datensätze oder mehrere Gigabyte
ac) Mehrere 100 Nutzer können gleichzeitig auf die Daten zugreifen.
ad) MySQL ist unabhängig vom Betriebssystem und der Programmiersprache.
ae) C, C++, Java, PHP, Perl, TCL and Python u. a. (10 P., 5 x 2 P.)

b)
- Oracle
- DB2
- Informix
- Sybase
- MS-SQL
- u. a. (2 P.)

c)
- Sichere und einheitliche Verwaltung von Daten
- Bereitstellung von Daten für Anwendungsprogramme
- Verhinderung unkontrollierter Zugriffe auf Daten
- Effiziente Zugriffsmöglichkeit auf die in der Regel sehr großen Datenbestände
- Einheitliche Basis für Anwendungen
- Flexible Datenauswertung
- Zentrale Überprüfung der Korrektheit von Daten (8 P.)

**6. Handlungsschritt (20 Punkte)**




Hinweise:
- freigabe: Variable für das Setzen des Wertes auf wahr oder falsch für eine korrekte bzw. inkorrekte Eingabe von Benutzername und Kennwort
- zaehler: Variable für das Zählen der Eingabeversuche
- Die logische Abfrage nach Durchlaufen der Schleife kann für dieses STG auch lauten:
  'Ist zaehler > 3'?
- Die Schleife kann auch fußgesteuert sein.