Aufgabe 1: Allgemeine Grundlagen (4 + 4 + 2 + 6 + 4 = 20 Punkte)

a) Was versteht man unter *vertikaler* und *horizontaler* Kommunikation? Geben Sie für die beiden Kommunikationsformen jeweils ein Beispiel und erklären Sie es kurz.

b) *Skizzieren* Sie das Internet-Referenzmodell und benennen Sie die einzelnen Schichten.

c) Was ist der wesentliche Unterschied zwischen der Sicherungsschicht und der Vermittlungsschicht?

d) Schicht 2 des OSI-Referenzmodells ist in zwei Teilschichten aufgeteilt, die Logical Link Control (LLC) und die Medium Access Control (MAC). *Warum* macht man diese Aufteilung, und *welche Aufgaben* haben die beiden Teilschichten jeweils?

e) Sie empfangen ein HTTP-Paket über Ethernet. *Skizzieren* Sie den Aufbau des Pakets mit Headern aller Schichten. *Hinweis*: die Angabe der Headergrößen in Bytes ist *nicht* notwendig.

Aufgabe 2: Lokale Netze
(1 + 4 + 7 + 7 + 8 = 27 Punkte)

a) Worin unterscheiden sich *Hubs* und *Switches* bei der Kopplung von Netzen?

b) Für den Aufbau lokaler Netze gibt es unterschiedliche Topologien. Skizzieren Sie die *Ring*- und die *Sterntopologie*. Welche *Vor- und Nachteile* haben die Topologien?

c) Ethernet beruht auf dem Zugriffsverfahren *CSMA/CD*. Betrachten Sie folgenden konkreten Fall: An einem Ethernet-Bus sind drei Stationen A, B und C angeschlossen. A möchte Daten an C versenden und lauscht, ob die Leitung frei ist. Dies ist der Fall, und A beginnt zu senden. Gleichzeitig hat B ebenfalls gelauscht und beginnt nun auch, Daten an C zu senden.

- Woran liegt es, dass es in diesem Fall trotz CSMA/CD zu einer Kollision kommt?

- Woran erkennen A, B und C jeweils, dass es zu einer Kollision gekommen ist?

- Wie wird die Kollisionssituation aufgelöst, und welche CSMA-Strategien kennen Sie dafür?

d) Berechnen Sie für die Bitfolge „111110101“ die *CRC-Prüfsumme* mit dem Generatorpolynom $G(x) = x^4 + x + 1$. Wie sieht die zu übertragende Bitfolge aus? Wie erkennt der Empfänger, dass die Bitfolge korrekt empfangen wurde?

e) Sie nutzen ein Sliding-Window-Verfahren für die Flusskontrolle. Die Fenstergröße betrage W=8, der Modulus M=12. Zum betrachteten Zeitpunkt hat der Sender die Rahmen mit den Sequenznummern N(S)=2,3,4,5,6,7 gesendet, ohne bisher eine Bestätigung erhalten zu haben.

- Welche Rahmen darf der Sender noch senden, bis er auf Bestätigungen warten muss?

- Wie ändert sich die Situation, wenn der Sender folgende Bestätigungen erhält?
  - N(R) = 8
  - N(R) = 3
  - N(R) = 2

Aufgabe 3: Das Internet-Protokoll (3 + 3 + 8 + 3 + 4 = 21 Punkte)

a) Früher wurden die IP-Adressbereiche in *Netzklassen* eingeteilt. Was *bedeutet* der Begriff Netzklasse? Worin *unterscheiden* sich die einzelnen Netzklassen?

b) In den 90er Jahren ist man zu *classless routing* übergegangen. Aus welchem *Grund* geschah dies? Welche *Vorteile* bietet CIDR gegenüber dem alten (classful) Ansatz?

c) Wie viele *Bits für Subnetze* werden durch die Subnetz-Maske 255.255.252.0 in einem Netz mit dem Adressraum 137.226.0.0/16 bereitgestellt? Wieviele *Rechner* stehen pro Subnetz zur Verfügung? Geben Sie die *vollständigen Adressräume* für das niedrigstwertige und höchstwertige Subnetze an.

d) Erläutern Sie den Begriff Multicast. *Wozu* wird Multicast verwendet, und *warum*?

e) *Skizzieren* sie grob, wie in IPv4-Netzen Multicast umgesetzt wird. *Welches Protokoll* wird dafür verwendet?

Aufgabe 4: Routing (3 + 4 + 6 + 3 = 16 Punkte)

a) Woran kann ein Sender erkennen, dass die Ziel-IP-Adresse eines IP-Paketes sich *nicht in seinem eigenen* IP-Subnetz befindet? Geben Sie ein einfaches Beispiel.

b) Auf welchen Netzwerkschichten sind Ihnen *Broadcastadressen* bekannt? Wie behandeln *Switches* und *Router* solche Pakete?

c) Network Address (Port) Translation – NA(P)T ist eine Möglichkeit, mit der Knappheit von IP-Adressen umzugehen. Diese Technik wird von den meisten DSL-Routern verwendet. Beschreiben Sie das *Prinzip von NA(P)T*. Können durch dieses Prinzip irgendwelche *Probleme* bei der Kommunikation zwischen Ihren eigenen Rechnern bzw. bei der Kommunikation Ihrer Rechner mit externen Rechnern entstehen?

d) Erläutern Sie kurz den Zweck des *ICMP-Protokolls* und geben Sie zwei Beispiele, wann das Protokoll zum Einsatz kommt.

Aufgabe 5: Transportschicht (6 + 4 + 2 + 6 = 18 Punkte)

a) *Welche Dienste* werden von der *Transportschicht* innerhalb eines Kommunikationssystems zur Verfügung gestellt? Worin unterscheiden sich insbesondere *verbindungslose* und *–orientierte* Dienste? Ist die *Bestätigung* von gesendeten Daten ein notwendiger Bestandteil der Transportschicht? *Begründen* Sie ihre Antwort.

b) In Vorlesung und Übung haben sie das *PUSH-Flag* von TCP kennengelernt. *Was bewirkt* das Flag auf der Empfängerseite? In *welchen Situationen* ist die Verwendung sinnvoll? Nennen Sie ein *Beispiel*.

c) Welche Rolle haben *Ports* bei TCP?

d) Erläutern Sie die *Gemeinsamkeiten* und *Unterschiede* von Fluss- und Staukontrolle bei TCP: Welche *Probleme* versuchen *beide* zu beheben? *An welchen Stellen* tritt das Problem jeweils auf? Wie erfährt der Sender, dass er aufgrund von Flusskontrolle seine Sendegeschwindigkeit reduzieren muss? Wie verhält es sich im Fall von Staukontrolle?

Aufgabe 6: Sicherheit (1 + 2 + 2 + 5 + 8 = 18 Punkte)

a) Um eine sichere Kommunikation mit Internet-Protokollen zu erreichen, gibt es z.B. IPsec. Worin besteht der Unterschied zwischen *Tunnel- und Transportmodus* bei IPsec?

b) Worin besteht der *Vorteil von Blockchiffren* gegenüber monoalphabethischen Chiffren?

c) DES führt eine Verschlüsselung in 16 identischen Runden durch. Worin besteht der *Sinn dieser Mehrfachausführung*?

d) Im Regelfall ist eine zu verschlüsselnde Nachricht zu lang, um sie mit DES zu verschlüsseln, so dass man sie vor der Verschlüsselung erst in Blöcke passender Länge segmentieren muss. In diesem Fall kommt z.B. *Cipher Block Chaining (CBC)* zum Einsatz. Wie funktioniert dieses Verfahren und warum wird es eingesetzt?

e) Wie kann man unter Verwendung von RSA einen *Authentifizierungsalgorithmus* erstellen? Gegeben sei **e=7** und **n=33**. Bestimmen Sie den privaten Schlüssel d, und authentifizieren Sie die Nachricht **m=4**. Erläutern Sie, wie der Empfänger die Authentizität der Nachricht überprüfen kann (Hier reicht eine Angabe des Rechenwegs, Sie brauchen für diesen letzten Schritt das Ergebnis nicht zu berechnen).

Bonusaufgaben
(6 + 4 = 10 Punkte)

Um die Klausur zu bestehen, müssen Sie genügend Punkte in den vorherigen Aufgaben erreichen. Mit diesen zusätzlichen Bonusaufgaben können Sie Ihre Note verbessern.

Bonusaufgabe 1: IP-Topologie

Gegeben sei ein Netz mit dem Adressraum und Subnetzmaske 134.130.28.0/22. Dieses möchten sie *unter kompletter Ausnutzung* des zur Verfügung stehenden Adressraums in 6 Subnetze zerlegen, wobei 2 der Subnetze jeweils doppelt so groß sein sollen wie jedes der 4 anderen. Geben Sie die entstehenden Netze und ihre Subnetzmasken an.

Bonusaufgabe 2: Kanaleffizienz

Eine Client-Server Anwendung zwischen Erde und Mond nutzt zur Kommunikation ein Sliding-Window-Protokoll. Die Übertragungsverzögerung beträgt in *jeder Richtung 1s*. Wie groß muss das *Übertragungsfenster* gewählt werden, damit bei entsprechender Bandbreite der Verbindung die Anwendung eine Datenübertragungsrate von 100Mbit/s überhaupt erreichen kann? Was passiert, wenn Sie die gleiche Anwendung in Ihrem lokalen Netz mit einer Übertragungsverzögerung in *jeder Richtung von 1ms* austesten? *Diskutieren* Sie die Auswirkungen in Bezug auf Netzwerke mit hoher Bandbreite und Latenz (long fat networks) wie im Fall der Erde-Mond-Kommunikation.