Fragen zur Prüfungsvorbereitung Teil 2

Aufgabe 21: (1 Punkt)

Ein TCP-Paket überholt ein vor ihm abgeschicktes Paket. Wie kann der Empfänger diesen Fehler korrigieren? *(F128*)

Antwort: Der Empfänger speichert es entsprechende seiner Sequenznumber in dem Puffer mit der Größe des Window ab. Somit liegt er an *seinem* Speicherplatz

Aufgabe 22: (2 Punkte)

Eine öffentliche IPv6-Adresse ist definiert als 2000::/3. Wieviel Adressen gibt es dafür ? In der 2-Potenzschreibweise, sowie den ungefähren Wert als Zehnerpotenz. *(F11)*
Antwort: $2^{125} = 2^5 * 2^{120} \approx 32 * 10^{36}$

Aufgabe 23: (6 Punkte)

Nennen Sie die 3 direkt aufeinander aufbauenden Ebenen des ISO/OSI-Modells, die in ihren Headern Adressen und ähnliches enthalten. Benennen sie diese Adressen und geben Sie ihre Reichweite an. *(F5)*

Antwort:
Layer 2, Sicherungsschicht/Data Link Layer, MAC-Adressen, gelten lokal bis zum Router/Gateway
Layer 3, Vermittlungsschicht/Network Layer, IP-Adressen, gelten system- bzw. Weltweit
Layer 4, Transportschicht/Transport Layer, Ports (Port-Adressen?!), gelten auf 1 Computersystem

Aufgabe 24: (1 Punkte)

Welchen Nachteil hat die symmetrische Verschlüsselung gegenüber der asymmetrischen Verschlüsselung. *(F144-147)*

Antwort: Die Verteilung des Schlüssels ist unsicher. Darf eigentlich nicht auf dem gleichen Medium verteilt werden. Ist der Schlüssel abhandengekommen, kann der Angreifer alles machen.
Vorteil der symmetrischen Verschlüsselung ist seine Geschwindigkeit bei kleinerer Schlüssellänge! Kann ähnlich oder sicherer sein als asymmetrischer Verschlüsselung mit langem Schlüssel.

Aufgabe 25 (3 Punkte)

Beim symmetrischen Verschlüsseln wird ein Schlüssel verwendet. Wieviel sind es bei der asymmetrischen Verschlüsselung? Benennen Sie diese. *(F145-147)*

Antwort: 4(Vier): Den privaten und den öffentlichen Schlüssel jeweils des Partners und den Eigenen. Den öffentlichen des anderen wird zum Verschlüsseln (alle dürfen verschlüsseln, für den Besitzer des privaten Schlüssels) und der mit Kennwort geschützte private Schlüssels zum Entschlüsseln. Beim Signieren ist es genau andersherum

Aufgabe 26 (5 Punkte)

Was enthält ein Zertifikat? Wie ist es vor einer Manipulation geschützt? *(F148-150)*
Antwort: den öffentlichen Schlüssel, manchmal auch den private, Seriennummer, Inhaber (X.500), Verwendungszweck, Seriennummer, CRL-Pfad, Gültigkeitszeitraum, Hashwert,…
Er besitzt ein Fingerabdruck, den man überprüfen kann und er ist vom Trustcenter unterschrieben, was man prüfen kann. CRL.

Aufgabe 27 (5 Punkte)

Unter welchen Umständen kann ein Switch sich zu einem Hub degradieren? Welche Funktionen kann er dann nicht mehr? Wovon hängen diese Funktionen ab? (F48-53)
Antwort: Schleife gesteckt; MAC-Adressspeicher läuft über; alle Funktionen, die mit MAC-Adressen zusammenstehen, hängendavon ab, also schalten der Verbindung, VLAN, u.ä.; Bessere können statt Degrieren zu Hub→Portabschaltung

Aufgabe 28: (2 Punkte)

Ein TCP-Paket geht unterwegs verloren. Wer initiiert das wiederholte Versenden des Paketes und was ist der auslösende Impuls? *(F121, 127-129)*

Antwort: der Absender, beim Warten auf des ACK-Paket gibt es ein TimeOut.(Der Empfänger hat es ja nicht empfangen und kann es also nicht mit ACK bestätigen)

Aufgabe 29: (2 Punkte)

Twisted Pair ist gegenüber Störungen recht resistent. Was führt dazu und was passiert, wenn es nicht greift! *(F22)*

Antwort: Das enge Aneinanderliegen der beiden Leitungen (Twisted Pair) und die differentielle Spannung. In den Adern wird durch elektromagnetische Einflüsse die gleiche Spannung/Stromrichtung initiiert, was die Differentialspannungsabstand nicht verändert. Ansonsten würden Pakete verändert und damit verloren gehen. (Der FCS sollte Fehler zeigen).

Aufgabe 30: (8 Punkte)

LWL gibt es in verschiedenen Dicken und Typen. Nennen Sie die beiden Typen und ordnen Sie ihnen Dicke und Reichweite und Maximalgeschwindigkeit zu *(F28-30)*

Antwort: 9 µm; Monomode/Singlemode, dutzende von km, >100Gbit/s

50..62,5 µm/100..200 µm, Multimode, hunderte Meter, bis 10 Gbit/s

Aufgabe 31: (3 Punkt)

Nennen Sie 3 Probleme, die bei der Verlegung von LWL auftreten können. *(F30)*

Antwort: Glasbruch, Glassplitter, schiefe Kanten beim Trennen, ungenaue Justierung, falscher Strahlwinkel, Staubansammlung

Aufgabe 32: (4 Punkte)

Welche Teile enthält eine IPv6-Adresse wie fd00:adi:cafe:1:affe:edda::1 und woran erkennt man sie? *(F68-71)*

Antwort: Präfixanteil: Kennzeichen für privates Netz (fd::/8, eigentlich fc::/7), Präfix/Netzsegment/ProviderID (00:adi:cafe:1), der letzte Teil kann als Subnetz vergeben werden (z.B.: 1), Netzwerkkarte, Kundenanteil (affe:edda::1) auch hier könnte ein Subnetz eingerichtet sein. Schlecht zu erkennen an der Adresse allein, i.A. /64, kann auch /56 sein oder andere Einteilung sein.

Aufgabe 33: (3 Punkte)

Woran erkennt man das Standardgateway und wie funktioniert es? Kann es mehrere Standardgateways geben und wenn ja, wie arbeiten sie dann zusammen? *(F92)*

Antwort: 0.0.0.0/0 oder ::/0, Bei der Maskierung und dem Vergleich trifft es immer zu, das Standardgateway wird also immer ausgeführt. Es kann mehrere Gateways geben, es wird aber immer nur das erste aktive genommen (Gibt es Störungen, wird es deaktiviert und das nächste ist dran)

Aufgabe 34: (3 Punkte)

Anfragen über mehrere Router kommen an, aber deren Antworten kreisen im Netz und bringen dann ein TTL von 0. Woran kann es liegen? *(F98, 87ff)*

Antwort: Wahrscheinlich ist das Paket über ein Standardgateway von einem oder mehreren Routern ans Ziel gekommen, die Route für den Rückweg ist aber nicht gesetzt. Ob die Meldung TTL=0 zurückkommt ist fragwürdig, da ohne das Eingreifen der Firewall die Routingregeln für alle Pakete also auch Rückkehren) wirken. Theoretisch ist auch ein in einer Richtung geschlossener Port eines Routers/Host denkbar, aber dann wird die Antwort normalerweise geblockt (oder reject)

Aufgabe 35: (4 Punkte)

Wie ist ein DNS-Name aufgebaut? Worüber kann man DNS-Namen auflösen? *(F156-159)*

Antwort: Ein DNS-Name besteht aus mehreren Domänen getrennt durch den Punkt, die von rechts nach links durchnummeriert sind (first level, Second level Third level name,..). Ganz rechts kann ein Punkt für die Root-Server stehen, ganz links steht ein Hostname. Man kann die DNS-Namen über die hosts-Datei und dem verteilten DNS-Servern auflösen (Seltener auch über WINS). Die Auflösung erfolgt von rechts (dem Root-Servern) nach links (den zu suchenden Host, besser gesagt seiner IP)

Aufgabe 36: (3 Punkte)

Man sagt, dass es 13 DNS-Root-Server gibt. Stimmt es, oder sind es mehr? Reicht deren Leistung? *(F158)*

Antwort: Lange Zeit waren es „nur“ 13 Höchstleistungsserver, die vor allem in den USA standen. Mittlerweile wird die Leistung durch Anycast auf mehr als 100 Server aufgeteilt. Die Anzahl wird wohl noch steigen. Mit der steigenden Anzahl steigt die Angst und die Gefahr, das die DNS-Auflösung im Internet geteilt und damit (von hoher Stelle) manipuliert/zensiert wird.

Aufgabe 37: (2 Punkte)

Wie kann man den Google-Server 8.8.8.8 einerseits mit einer Adresse und andererseits interaktiv anfragen? *(F159)*

Antwort: nslookup www.web.de 8.8.8.8

nslookup – 8.8.8.8 durch den Strich geht er in den interaktiven Modus

Aufgabe 38: (4 Punkte)

Was ist eine statefull und was eine stateless IP-Konfiguration? Welche Arten gehören dazu? *(F160)*

Antwort: Statefull ist eine zentral Protokollierbare, da vollständig vergeben Adr., stateless ist nur die Vergabe des Präfixes, den Netzwerkanteil wählt sich die Schnittstelle selbst, somit auch nicht zentral protokollierbar (da zentral ja nur der Präfix bekannt ist!) DHCP ist statefull, Router Advertisement ist stateless. DHCP ist für IPv4, seltener für IPv6 (dort auch verpönt!), RA ist nur für IPv6.

Aufgabe 39: (6 Punkte)

Nennen Sie die Portnummern zu folgende Diensten: *(F118, 120)*

POP3: 110	HTTPS: 443	FTPS: 989, 990	SMB3: 445
RDP: 3389	HTTP: 80	FTP: 21, 20	DNS: 53
OpenVPN: 1194	POP3S: 995	SSH: 22	SMTP: 25

Aufgabe 40: (4 Punkte)

Wie lang sind MAC-Adressen? Welche beiden Teile enthält sie? Was ist sie für eine, wenn sie mit 52 beginnt? *(F46-47)*

Antwort: 48 bit bzw. 6 Byte, damit gibt es 2^{48} bzw 256 * 10^{12} also etwa 3 * 10^{14} Adressen. Sie sind eingeteilt in Herstelleranteil (24 bit bzw. 3 Byte) und dem Schnittstellenanteil (24 bit bzw. 3 Byte). Damit können 16 Mio. Hersteller jeweils 16 Mio. Netzwerkkarten bestücken (Hersteller haben öfters mehrere Nummern/Bereiche), Bit 1 des ersten Bytes hat die Bedeutung Individual (0) oder local (1). $X2_H$ ist also local, eine selbst zuweisbare (z.B. zu einer VM gehörenden) MAC.

Aufgabe 41: (5 Punkte)

Schreiben Sie die Regeln für CSMA/CD auf? Schauen Sie sich dann die Unterschiede zu CSMA/CA an! *(F39-40)*
Antwort: 1) Horchen ob Medium frei, wenn nicht weiter warten (**C**arrier **S**ense), 2) Paket senden, 3) Kollision erkennen durch mithorchen (**C**ollision **D**etection), 4) Bei Kollision Stop, zufällige Zeit warten und weiter mit 1, 5) Nach max. Anzahl von versuchen abbrechen und Timeout nach oben melden. CSMA/CD ist ein Verfahren für dem mehrfachen Zugriff (**M**ultiple **A**ccess) auf ein Medium, wenn ein Erkennen von Kollisionen (z.B. durch Spannungsmessung) möglich ist. CA kann kein CD, die Pakete müssen deshalb bestätigt (ACK) werden. Kein ACK → nochmal senden (Mit Wartezeit)

Aufgabe 42: (4 Punkte)

VLAN-aktivierte Switches haben 2 einstellbare Porttypen. Nennen Sie sie und beschreiben Sie den Unterschied. *(F57-59)*
Antwort: Tagged Port – Das VLAN-Tag wird nicht entfernt, alle Pakete werden zur weiteren Auswertung außerhalb des Switches an diesem Anschluss ausgeliefert
Untagged Port – Nur Pakete mit der eingestellten VLAN-Nummer werden ausgeliefert, das VLAN-Tag wird aus dem Ethernetheader entfernt.

Aufgabe 43: (1 Punkt)

Um was handelt es sich bei RIPv2, BGP, OSPF und IS-IS? (Nicht prüfungsrelevant) *(F101)*

Antwort: Es sind Routingprotokolle, die die Routingtabelle optimieren und anpassen oder selbst Pakete ausliefern. Dabei unterhalten sich diese Dienste mit denselben Diensten auf anderen Routern.

Aufgabe 44: (2 Punkte)

In einer MS-Domäne sorgt Kerberos für eine SSO-Anmeldung. Was bedeutet das und wie realisiert Kerberos es? *(F139)*

Antwort: SSO – Single Sign On. Einmal mit Benutzer und Passwort anmelden, das gilt dann für alle Dienste. Kerberos stellt dann nach der Anmeldungsprüfung ein Benutzerticket und bei Bedarf für die Nutzung jedes weitere Dienstes ein Ticket auf Basis seines Benutzertickets aus. Die Daten für die Prüfung des Benutzers und die der Dienste stehen in einer Datenbank, bei MS-Domänen das Active Directory (AD) mit seiner LDAP-Datenbank.