

2

Analyse und Entwicklung
von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.). Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=	100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte	
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

1. Aufgabe (28 Punkte)

aa) 4 Punkte, pro richtiger Zeile 1 Punkt

Netz-ID	Subnetzmaske (dezimal)	Next-Hop oder Interface
203.0.113.64	255.255.255.252	WAN
172.16.0.0	255.255.0.0	LAN
10.10.0.0	255.255.255.192	DMZ
0.0.0.0	0.0.0.0	WAN oder 203.0.113.66

ab) 3 Punkte

WAN: 203.0.113.67

LAN: 172.16.255.255

DMZ: 10.10.0.63

ac) 6 Punkte

Unicast stellt eine „1 zu 1“-Kommunikation dar, ein Sender sendet an einen Empfänger, z. B. Abruf einer Internetseite.

Multicast stellt eine „1 zu viele“-Kommunikation dar, ein Sender sendet an eine definierte Gruppe von Empfängern, z. B. senden eines Livestreams über IPTV.

Broadcast stellt eine „1 zu alle“-Kommunikation dar, ein Sender sendet an alle anderen Geräte im Netzwerk. Z. B. wird ein ARP-Request ins Netzwerk gesendet, um die MAC-Adresse zu einer IP zu ermitteln.

Andere Erklärungen und Beispiele sind möglich.

ad) 4 Punkte

Start-Adresse: 224.0.0.0

End-Adresse: 239.255.255.255

ba) 3 Punkte

Der Webserver wird über Portforwarding/Destination-NAT von außen erreicht. Der Router wandelt dazu Pakete, die auf der öffentlichen Adresse mit einem der definierten Ports ankommen so um, dass das Paket an die interne Adresse weitergeschickt wird.

bb) 4 Punkte

Version 4	IHL 5	ToS 0	Length 52	
Identification 58007			Flags 2	Fragment-Offset 0
TTL 127		Protocol 6	Header-Checksum 0	
Source-IP-Address 203.0.113.65				
Destination-IP-Address 51.38.104.145				

bc) 2 Punkte

Client 1 vergleicht seine Netz-ID mit der (vermuteten) Netz-ID des Ziel-Rechners. Da diese in verschiedenen IP-Netzen liegen, wird das Paket an das Default-Gateway gesendet.

bd) 2 Punkte

Der Client sendet einen ARP-Request als Broadcast ins lokale Netz. Darin fragt er nach der MAC-Adresse des Standard-Gateways. Dieses sendet seine MAC-Adresse.

2. Aufgabe (22 Punkte)

aa) 4 Punkte

Auf dem Client ist Netzwerkkonfiguration mittels DHCP eingestellt. Wenn kein DHCP-Server antwortet, erstellt der Rechner automatisch eine Adresse im Bereich 169.254.0.0/16 (APIPA).

Alternativ: Bei IPv4-Adresskonflikten kann ebenfalls diese Adresse zugeordnet werden.

Ähnliche Lösungen möglich!

ab) 4 Punkte

Der Anfang „FE80“ steht für „link local address“; also die Geräte, die am gleichen Netzwerklink/segment hängen. Der Bereich nach dem :: ist der Interface Identifier. Dieser wird aus der MAC-Adresse generiert oder zufällig erzeugt.

Ähnliche Lösungen sind möglich.

ac) 3 Punkte

Manuelle Konfiguration der Netzwerkparameter IP-Adresse, Netzmaske, Gateway und DNS-Serveradresse oder

Wenn DHCP-Server verfügbar ist, mittels „ipconfig /renew“ die Netzwerkeinstellungen per DHCP neu anfordern.

Weitere Lösungen sind möglich.

ba) 2 Punkte

Die Namensauflösung der IP des File-Servers schlägt fehl, da der eingetragene öffentliche DNS-Server die interne Adresse des File-Servers nicht kennt.

bb) 3 Punkte

Die IP-Adresse des Domain-Controllers 172.16.1.11 als DNS-Server eintragen.

Die IP-Adresse des Domain-Controllers zusätzlich als ersten Eintrag als DNS-Server eintragen.

In den Netzwerkeinstellungen (den fest eingetragenen DNS 8.8.8.8 löschen und) auf „DNS-Serveradresse automatisch beziehen“ einstellen.

Weitere Lösungen sind möglich.

ca) 1 Punkt

Einzustellendes Protokoll: IMAP

cb) 2 Punkte

Einzustellende Verbindungssicherheit: STARTTLS

cc) 3 Punkte

Einzustellende Authentifizierungsmethode: Passwort, normal

3. Aufgabe (24 Punkte)

aa) 2 Punkte

Die Anzahl der generierbaren IPv4-Adressen ist durch die Limitierung auf 32 Bit begrenzt und reicht nicht mehr aus, um den wachsenden Bedarf zu decken.

IPv6 bietet mit 128 Bit Adressraum genügend IP-Adressen.

ab) 6 Punkte

- Bietet eine höhere Skalierbarkeit und ermöglicht es, sehr viel mehr Geräte als bisher direkt mit dem Internet zu verbinden.
- Erhöht die Sicherheit bei der Datenübertragung durch die Einbindung von Verschlüsselungs- und Authentifizierungsfunktionen
- Eingebaute Sicherheit auf Netzwerkschicht (IPsec)
- Effizienteres Routing ohne Fragmentierung von Paketen
- Eingebaute Quality of Service (QoS), die verzögerungsempfindliche Pakete unterscheidet
- Eliminierung von NAT zur Erweiterung des Adressraums von 32 auf 128 Bit
- Zustandslose Adressen-Autokonfiguration für einfachere Netzwerkverwaltung
- Verbesserte Header-Struktur mit weniger Verarbeitungsaufwand

Andere Antworten sind möglich.

ba) 2 Punkte

- Netzwerkverwaltung vereinfachen
- Netzwerksicherheit erhöhen
- Datenverkehr aufteilen
- Zugriff auf Netzwerkressourcen steuern

bb) 8 Punkte (je 2 Punkte für richtige Zeile)

1. Subnetz 2001:DB8:CAFE::/50 (0000 → 0000 0000 0000 0000)
2. Subnetz 2001:DB8:CAFE:4000::/50 (4000 → 0100 0000 0000 0000)
3. Subnetz 2001:DB8:CAFE:8000::/50 (8000 → 1000 0000 0000 0000)
4. Subnetz 2001:DB8:CAFE:C000::/50 (C000 → 1100 0000 0000 0000)

Die binäre Darstellung dient nur als Hilfestellung für die Korrektur.

ca) 3 Punkte

IPv6-Clients können dadurch eine Grundkonfiguration erstellen, um an dem IPv6-Netzwerk teilnehmen zu können, in dem sie sich befinden. Dazu gehört eine link-local IPv6-Adresse, die selbst generiert wird. Über das Router-Advertisement bekommt dann jeder Host den globalen Präfix und die IPv6-Adresse des DNS-Servers. Die IPv6-Adresse des Standard-Gateway ist der Absender vom Router-Advertisement.

cb) 3 Punkte

Begründung für DHCPv6-Server

- Verwaltet Adresspools, vergibt daraus IP-Adressen an die Clients
- Protokolliert die Zuordnung der IP-Adressen an Clients
- Zuweisung Zeitserver
- Zuweisung Druckserver
- Zuweisung TFTP-Server
- Zuweisung DNS-Server
- Vergabe der Adressen für mehrere Subnetze

4. Aufgabe (26 Punkte)

aa) 3 Punkte

- PSK könnte an externe Personen weitergegeben werden.
- PSK ist anfällig für Brute-Force Angriffe.
- Wenn eine Person das Unternehmen verlässt, ist weiterhin ein Zugriff auf das WLAN möglich, solange der PSK nicht abgeändert wird.
- Wenn ein Endgerät entwendet wurde, kann dies für Angriffe über das WLAN-Netzwerk verwendet werden.
- Datenverkehr kann ausgespäht werden.

ab) 2 Punkte

- WPA2-Enterprise mit eindeutiger Identifizierung einer Person durch eindeutige Anmeldeinformationen
- WPA2-Enterprise mit Zertifikaten

Andere Lösungen (z. B. WPA 3 verwenden) sind auch möglich.

ba) 3 Punkte

- Kompromittierung des internen Netzwerkes durch nicht-verwaltete Endgeräte
- Priorisierung des Internetverkehrs für interne Anwendungen
- Zeitlich begrenzter Internetzugang für Gäste/Mitarbeiter
- Zugriff auf interne Anwendungen/Daten für persönliche und fremde Endgeräte unterbinden
- u. a.

bb) 2 Punkte

- Neue Accesspoints haben nur ein 5 GHz WLAN
- Fehlerhafte Konfiguration, sodass nur ein WLAN mit 5 GHz ausgestrahlt wird
- Falsche Kanalauswahl
- Funksignal kommt bei Kamera nicht mehr ausreichend an
- Interne Antennen statt externer Antennen

Andere Antworten sind möglich.

ca) 6 Punkte

SSID	Service Set Identifier – Name des WLAN
BSSID	Basic Service Set Identifier – Eindeutige Identifizierung des APs
CHANNEL	Verwendeter WLAN-Kanal
BW[MHz]	Kanalbreite des WLANs
SECURITY	Verwendete Verschlüsselungsmethode
SIGNAL	Empfangs-Signalstärke des WLANs

Die ausgeschriebene Abkürzung ist nicht zwingend erforderlich bzw. alleine nicht ausreichend als Erläuterung.

cb) 2 Punkte

Das Netzwerk „<hidden>“ und „MEDIA-AGENTUR“ verwenden beide den Kanal 1.

Andere technisch korrekte Lösungen sind möglich.

cc) 2 Punkte

Im Accesspoint ist das SSID-Broadcasting deaktiviert.

da) 3 Punkte

Die Gäste erhalten jeweils einen Bon (Ticket, Voucher) mit Zugangsdaten in schriftlicher Form, die für einen bestimmten Zeitraum gültig sind. Diese müssen sie auf einer Website eingeben, die nach Verbindung mit der angegebenen SSID erscheint.

db) 3 Punkte

- Durch das Zugangsportal (Captive Portal) kann vom Gast die Zustimmung zu den Nutzungsbedingungen eingeholt werden.
- Volumenabhängige Begrenzung
- Freigabe von Diensten abhängig vom jeweiligen Ticket
- Auf der Portalseite können dem Gast direkt Informationen angeboten werden, z. B. zu eigenen Produkten (Promotion, Umfrage etc.)
- u. a.