



**Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:**

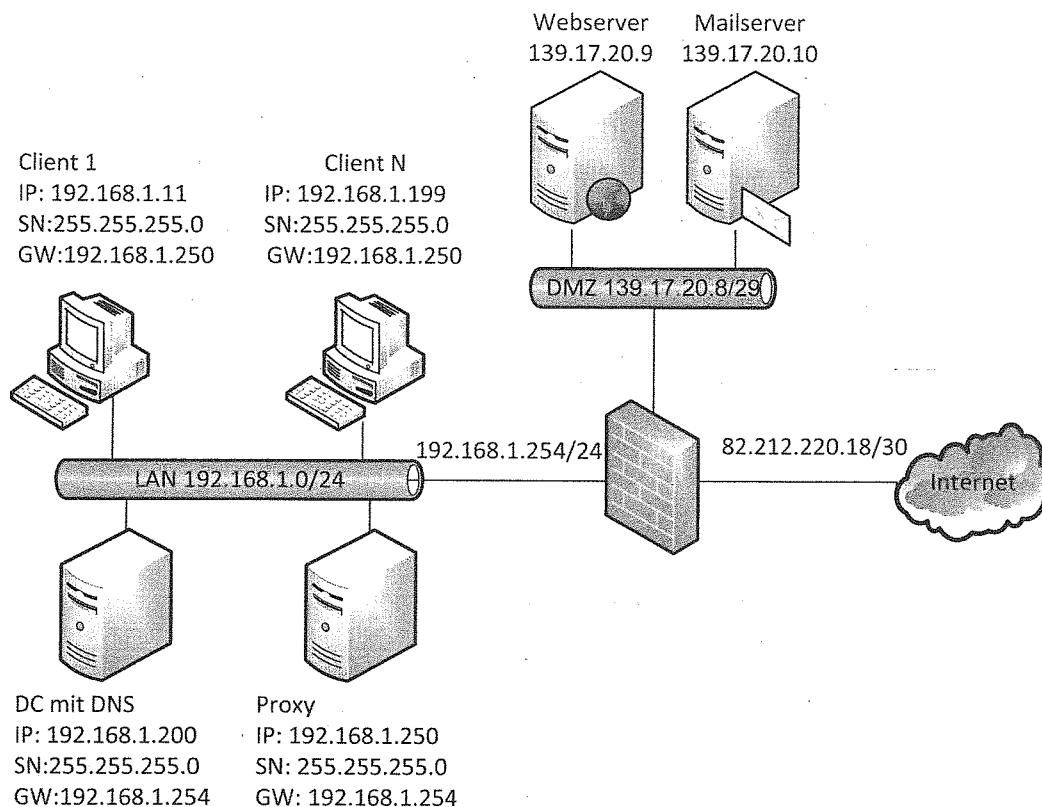
Sie sind Mitarbeiterin/Mitarbeiter der OHAGE GmbH, Hameln. Sie arbeiten in der IT-Abteilung. Im Rahmen eines Projekts soll Mitarbeitern und Kunden ein flexibler Zugang zum Firmennetzwerk unter Berücksichtigung aktueller Sicherheitsstandards eingerichtet werden.

Im Rahmen dieses Projekts sollen Sie vier der folgenden fünf Aufgaben bearbeiten:

1. Das Netzwerk auf Fehler analysieren und Fehler beseitigen, IPv6 einführen
2. WLAN-Komponenten beschaffen
3. VLANs einrichten, Firewallregeln erklären und ergänzen
4. Einen RADIUS-Server bereitstellen
5. Einen Passwortgenerator entwickeln

**1. Handlungsschritt (25 Punkte)**

Die OHAGE GmbH verfügt über die abgebildete Netzwerkstruktur:



a) Sie sollen die IP-Konfiguration von Client 1 prüfen. Mit `ipconfig` erhalten Sie die folgende Ausgabe:

Ethernet-Adapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: ohage.de

Verbindungslokale IPv6-Adresse . . : fe80::5226:90ff:fea9:1758%12

IPv4-Adresse . . . . . : 192.168.1.11

Subnetzmaske . . . . . : 255.255.255.0

Standardgateway . . . . . : 192.168.1.250


Ermitteln und korrigieren Sie den Fehler in der IP-Konfiguration.

4 Punkte

b) Beim Verbindungsaufbau zu einem Server wurde das folgende IP-Paket mitgeschnitten:

```
0000 45 00 00 34 37 16 40 00 7f 06 e3 8e c0 a8 01 11
0010 8b 11 14 0a f0 60 00 19 c6 5d 76 0f 00 00 00 00
0020 80 02 20 00 5c d6 00 00 02 04 05 b4 01 03 03 08
```

Aufbau des TCP/IP-Headers

0	4	8	15	16	24	31
Version		HLEN	Service Type		Total Length	
Identification				Flags	Fragment Offset	
Time-To-Life			Protocol		Header Checksum	
Source IP-Address						
Destination IP-Address						
Source Port				Destination Port		
Sequence Number						
Acknowledgement Number						
Header Length		Reserved	Code Bits		Window Size	
Checksum				Urgent Pointer		

IP-Header	
TCP-Header	

ba) Bestimmen Sie die Quell- und Ziel-IP-Adresse in hexadezimaler und in dezimaler Schreibweise.

4 Punkte

bb) Ermitteln Sie die maximale Anzahl an Routern, die dieses IP-Paket noch passieren kann.

2 Punkte

bc) Erläutern Sie, warum die Header Checksum an jedem Hop neu berechnet werden muss.

2 Punkte

bd) Erläutern Sie, wie der Client den Quell-Port erzeugt hat.

2 Punkte

be) Bestimmen Sie den Ziel-Port in dezimaler Schreibweise und den Namen der Anwendung, die der Client auf dem Server anspricht.

2 Punkte

Fortsetzung 1. Handlungsschritt →

c). Die Administratoren der OHAGE GmbH überlegen, IPv6 einzuführen.

ca) Erläutern Sie, warum sich der Client die IPv6-Adresse

fe80::5226:90ff:fea9:1758

generiert hat.

3 Punkte

cb) Zu Testzwecken soll der Adressraum des IPv6-Netzes

2001:db8:AAAA:BB00::/56

in vier gleich große Teilnetze aufgeteilt werden.

Ergänzen Sie jeweils die Netzadresse der Subnetze 2 – 4:

6 Punkte

Netz	Netz-Adresse
1	2001:db8:AAAA:BB00::
2	2001:db8:AAAA:BB_____
3	2001:db8:AAAA:BB_____
4	2001:db8:AAAA:BB_____

## 2. Handlungsschritt (25 Punkte)

Korrekturrand

Die OHAGE GmbH möchte für ihre Mitarbeiter und Kunden in ihren Konferenzräumen einen Internetzugang in Form eines WLAN-Netzwerkes einrichten.

- aa) Der WLAN-Access-Point wird im Infrastruktur-Modus betrieben.

Erläutern Sie den Begriff „Infrastruktur-Modus“.

3 Punkte

---

---

---

---

---

- ab) Der WLAN-Access-Point unterstützt den Standard IEEE802.11n mit einer Datentransferrate von 300 Mbit/s. Bei einem Test mit einem Notebook wurde nur eine maximale Transferrate von 48 Mbit/s erzielt.

Erläutern Sie drei mögliche Gründe, warum die Transferrate nicht dem angegebenen Wert von 300 Mbit/s entspricht. 6 Punkte

---

---

---

---

---

---

---

---

---

---

- b) Für die Anmeldung an das WLAN soll ein RADIUS-Dienst (Remote Authentication Dial-In User Service) genutzt werden.

- ba) Bei der Nutzung von RADIUS wird von einem AAA-System gesprochen.

Nennen Sie die drei AAA Begriffe.

3 Punkte

---

---

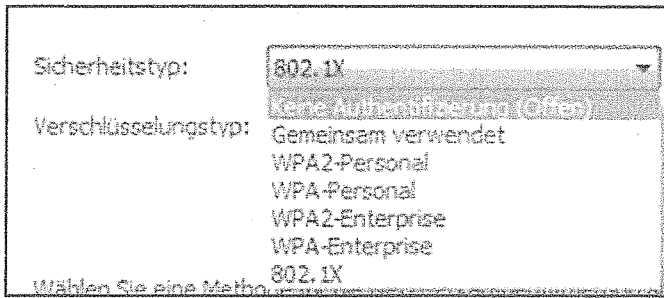
---

---

---

Fortsetzung 2. Handlungsschritt →

bb) Für die Nutzung des WLANs müssen die Notebooks der Mitarbeiter konfiguriert werden.



Nennen Sie die richtige Einstellung für den Sicherheitstyp (siehe Abbildung) bei Nutzung eines RADIUS-Dienstes. 3 Punkte

c) Um den Montageaufwand für den WLAN-Accesspoint möglichst gering halten zu können, wird der Einsatz von PoE (Power over Ethernet) vorgeschlagen. Ein PoE-fähiger Switch ist vorhanden.

Auszug aus dem Handbuch:

This Switch supports the IEEE802.3af-2003 standards in two modes.

Mode A: Power is carried on the same pins as data, by applying a common-mode voltage to each pair. The common-mode voltage is easily extracted from data signal. On pins 1 and 2 devices receive data and phantom-power transmitted positive voltage. Transmit data and negative voltage uses pins 3 and 6.

Mode B: Only two of the four pairs in the cable are needed to use a 100 Mbit/s network. The power is transmitted on the unused conductors of a CAT5 network cable. The power source applies positive voltage to pins 4 and 5. negative voltage is applied to pins 7 and 8.

Source voltage range is specified from 44 to 57 V (typical 48 V). The maximum current is 350 mA per port. Approximately 2.5 W of power is lost on a CAT5 cable of 100 m length. 12.9 W is available at the powerd device.

ca) Erklären Sie mithilfe des Textes die Funktionsweise von PoE in dem Modus, der eine gemeinsame Nutzung von Daten und Stromversorgung auf den Aderpaaren vorsieht. 4 Punkte

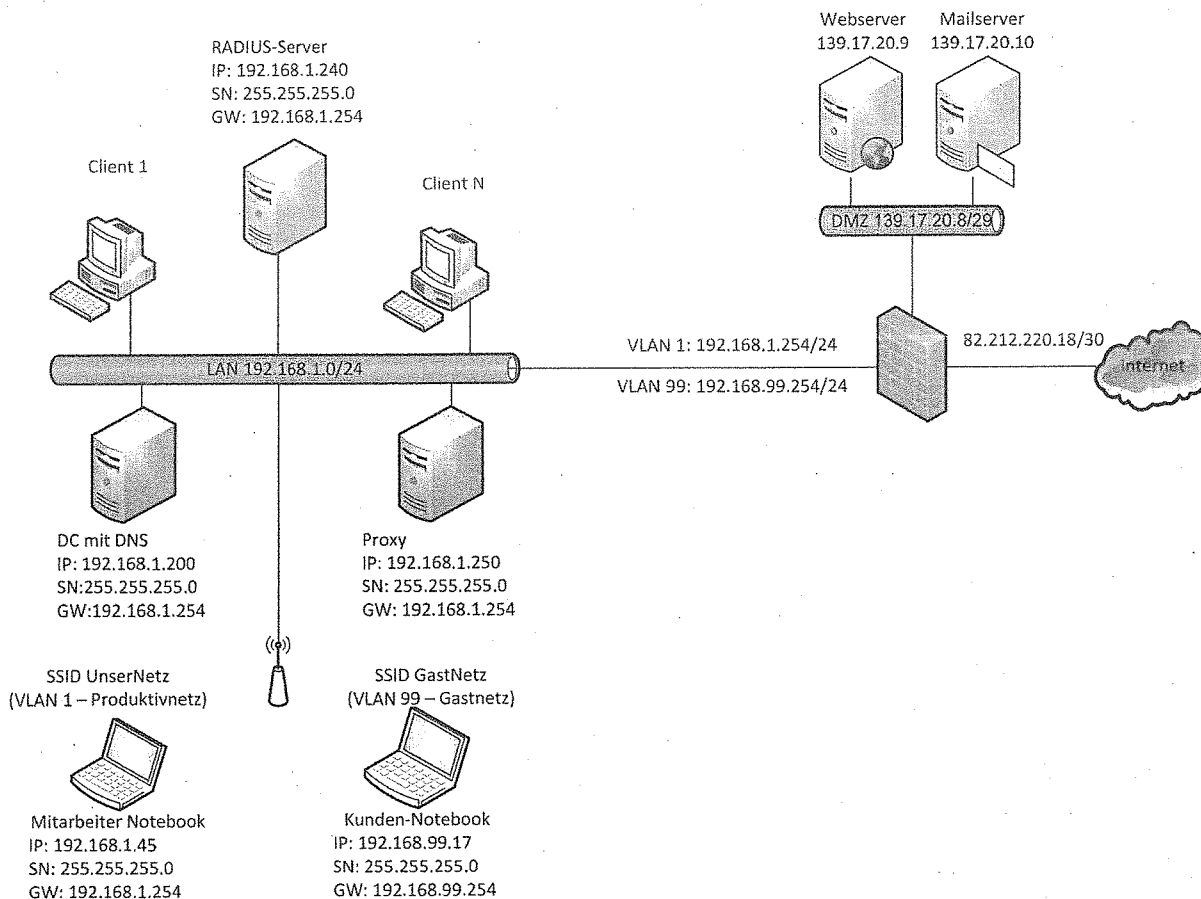
cb) Geben Sie die maximale Leistungsabgabe eines Switch-Ports an. 3 Punkte

cc) Nennen Sie drei weitere Geräte, für die sich ein sinnvoller Einsatz an einem PoE-fähigen Switch anbietet. 3 Punkte

### 3. Handlungsschritt (25 Punkte)

Korrekturrand

Nach der Erweiterung um die WLAN-Komponenten verfügt das Netzwerk der OHAGE GmbH über den folgenden Aufbau:



a) Das WLAN soll für Mitarbeiter und Kunden in zwei VLANs getrennt werden. Der Access-Point unterstützt Multi-SSID.

Erläutern Sie in diesem Zusammenhang zwei wichtige Aufgaben von Multi-SSID.

4 Punkte

b) VLANs können dynamisch oder statisch eingerichtet werden.

Erläutern Sie den prinzipiellen Unterschied zwischen den beiden Einrichtungsarten.

4 Punkte

Fortsetzung 3. Handlungsschritt →

- c) Der WLAN-Access-Point wird an einen getaggten Port (VLAN 1 und VLAN 99) am Switch angeschlossen.

Erläutern Sie, warum ein VLAN-Tag bei der Übertragung nötig ist.

4 Punkte

- d) Auf der Firewall (Stateful Packet Inspection) wurden für die VLANs zwei Interfaces eingerichtet: VLAN1 für das Netz 192.168.1.0/24, VLAN99 für das Gastnetz 192.168.99.0/24.

Um den Datenverkehr absichern zu können, wurden unter anderem folgende Regeln aufgestellt:

Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Interface	Richtung
1	Permit	IP	192.168.1.200/32	Any	-	-	VLAN1	IN
2	Permit	TCP	192.168.1.250/32	Any	Any	80	VLAN1	IN
3	Permit	TCP	192.168.1.250/32	Any	Any	443	VLAN1	IN
4	Permit	TCP	192.168.1.0/24	139.17.20.10/32	Any	25	VLAN1	IN
5	Permit	TCP	192.168.1.0/24	139.17.20.10/32	Any	110	VLAN1	IN
6	Deny	IP	Any	Any	-	-	ANY	IN

- da) Erläutern Sie die Firewallregeln 1 – 6.

9 Punkte

Nr.	Erläuterung
1	
2	
3	
4	
5	
6	

- db) Ergänzen Sie die nötigen Regeln, um dem Gastnetz (VLAN99) einen Zugriff auf das Internet zu ermöglichen.

Für die Namensauflösung im Gastnetz sorgt die Firewall.

4 Punkte

Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Interface	Richtung
1	Permit	IP	192.168.1.200/32	Any	-	-	VLAN1	IN
2	Permit	TCP	192.168.1.250/32	Any	Any	80	VLAN1	IN
3	Permit	TCP	192.168.1.250/32	Any	Any	443	VLAN1	IN
4	Permit	TCP	192.168.1.0/24	139.17.20.10/32	Any	25	VLAN1	IN
5	Permit	TCP	192.168.1.0/24	139.17.20.10/32	Any	110	VLAN1	IN
6								
7								
8	Deny	IP	Any	Any	-	-	ANY	IN



#### 4. Handlungsschritt (25 Punkte)

Sie sollen im Rahmen des Projekts einen Server für den RADIUS-Dienst bereitstellen.

- a) Vor der Softwareinstallation soll noch der Arbeitsspeicher des Servers vergrößert werden. Dazu werden 4 GiByte DDR3-1333 (PC3-10600, 512 MiBit x 72) Module mit ECC-Support verwendet.

Erläutern Sie, welche Art von Speicherfehlern mithilfe dieser ECC-Speichermodule erkannt und/oder korrigiert werden können.

4 Punkte

- b) Beim Formatieren der Systemfestplatte kann die Größe der Zuordnungseinheit auf folgende Werte festgelegt werden:

512 Byte, 1.024 Byte, 2.048 Byte, 4.096 Byte, 8.192 Byte, 16.384 Byte, 32.768 Byte und 65.536 Byte

Erläutern Sie den Zweck dieser Auswahlmöglichkeit.

4 Punkte

- c) Da die Performance des Servers nicht Ihren Erwartungen entspricht, führen Sie einen Benchmark-Test durch. Dabei wird für die Systemfestplatte (Serial ATA 6.0 Gbit/s) eine durchschnittliche Datenübertragungsrate von 220 MByte/s festgestellt.

Geben Sie die Formel zur Berechnung der Datenübertragungsrate in MByte/s für die SATA III Schnittstelle an.

3 Punkte

[illegible]

- d) Nach der Installation des Betriebssystems bleibt der RADIUS-Server zunächst in einem eigenständigen Netzwerk ohne DNS-Server mit zwei Test-Clients.

- da) Bei jedem Boot-Vorgang des Servers erscheint für einige Sekunden die Meldung:

Intel® Boot Agent PXE Base Code (PXE-2.1 build 091)

Initializing and establishing link ...

Erläutern Sie, ob dieser Teil des Boot-Vorgangs für die Funktion des RADIUS-Servers notwendig ist.

3 Punkte

4 Punkte

[illegible]

4 Punkte

[illegible]

3 Punkte

---

---

---

---

---

---

Anlage zum 5. Handlungsschritt

ASCII-Tabelle

ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen
0	NUL	32	SP	64	@	96	`
1	SOH	33	!	65	A	97	a
2	STX	34	"	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	\$	68	D	100	d
5	ENQ	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	'	71	G	103	g
8	BS	40	(	72	H	104	h
9	TAB	41	)	73	I	105	i
10	LF	42	*	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DC1	49	1	81	Q	113	q
18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	ETB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	Esc	59	;	91	[	123	{
28	FS	60	<	92	\	124	
29	GS	61	=	93	]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	DEL

### 5. Handlungsschritt (25 Punkte)

Für die Benutzerverwaltung sollen Passwörter nach folgendem Prinzip erstellt werden. Das Passwort besteht aus zehn zufällig gewählten Zeichen, die Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen sein können.

Beispiel: X5\_b } 4R? aG

Hinweis:

- Zur Unterstützung steht Ihnen die ASCII-Tabelle (siehe perforierte Anlage) zur Verfügung.
- Ein zufälliger Integerwert aus dem Bereich 0 bis 127 kann mit der Funktion `rand(127)` erzeugt werden.
- Die Funktion `char(zahl)` wandelt eine Zahl in das ASCII-Zeichen um.
- Das Passwort soll zur Überprüfung auf dem Bildschirm angezeigt werden.

a) Erstellen Sie mit einem Struktogramm, einem Programmablaufplan oder Pseudocode (Anlehnung an eine gängige Programmiersprache) eine Lösung für die Passwortgenerierung. 15 Punkte

This image shows a full page of blank graph paper. The grid consists of small, equal-sized squares formed by thin black lines. There are no margins, text, or other markings on the page.

b) Für die Speicherung von Passwörtern werden häufig Hash-Algorithmen, wie zum Beispiel MD5 oder SHA1, verwendet.

Erläutern Sie die Funktionsweise eines Hash-Algorithmus.

4 Punkte

---

---

---

---

c) Neben Benutzername und Passwort werden digitale Zertifikate zur Authentifizierung verwendet.

Erläutern Sie, wie der Server die Echtheit des Clientzertifikats prüfen kann.

6 Punkte

---

---

---

---

---

---

---

---

---

---

**PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!**

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

- ☐ 1 Sie hätte kürzer sein können.    ☐ 2 Sie war angemessen.    ☐ 3 Sie hätte länger sein müssen.

☐