OSI Testfragen

Testfragen Netzwerktechnik bis Firewall

1. Was ist der Hauptzweck eines Netzwerks?

Antwort anzeigen

Ein Netzwerk verbindet mehrere Geräte miteinander, damit sie Daten austauschen und gemeinsame Ressourcen nutzen können, zum Beispiel Drucker, Server, Internetzugang oder zentrale Datenspeicher.

---

2. Nenne drei Vorteile von Netzwerken.

Antwort anzeigen

Drei Vorteile sind:

- schneller Datenaustausch
- gemeinsame Nutzung von Ressourcen, zum Beispiel Drucker oder Server
- zentrale Datenspeicherung und einfachere Datensicherung

---

3. Nenne drei Nachteile oder Risiken von Netzwerken.

Antwort anzeigen

Drei Nachteile oder Risiken sind:

- Schadsoftware kann sich schneller verbreiten
- Angriffe oder Spionage von innen und außen sind möglich
- Aufbau, Wartung und Administration verursachen Kosten

---

4. Was bedeutet LAN?

Antwort anzeigen

LAN bedeutet Local Area Network. Es beschreibt ein lokales Netzwerk, zum Beispiel in einer Wohnung, Schule, Firma oder einem Büro.

---

5. Was ist der Unterschied zwischen LAN, MAN und WAN?

Antwort anzeigen

LAN ist ein lokales Netzwerk in einem begrenzten Bereich.

MAN verbindet Netzwerke innerhalb einer Stadt oder Region.

WAN verbindet Netzwerke über große Entfernungen, zum Beispiel über Länder oder Kontinente hinweg. Das Internet ist ein Beispiel für ein WAN.

---

6. Welche Topologie wird heute in LANs meistens verwendet?

Antwort anzeigen

Meistens wird die Sterntopologie verwendet. Dabei sind die Endgeräte zentral mit einem Switch verbunden.

---

7. Was bedeutet Vollduplex?

Antwort anzeigen

Vollduplex bedeutet, dass Daten gleichzeitig in beide Richtungen übertragen werden können.

Beispiel: Ein PC kann gleichzeitig Daten senden und empfangen.

---

8. Was bedeutet Halbduplex?

Antwort anzeigen

Halbduplex bedeutet, dass Daten in beide Richtungen übertragen werden können, aber nicht gleichzeitig.

Beispiel: Erst sendet Gerät A, danach Gerät B.

---

9. Wozu dient das OSI-Schichtenmodell?

Antwort anzeigen

Das OSI-Schichtenmodell teilt Netzwerkkommunikation in einzelne Schichten auf. Dadurch kann man besser verstehen, welche Aufgabe auf welcher Ebene passiert, und Fehler systematisch eingrenzen.

---

10. Wie heißen die 7 OSI-Schichten von oben nach unten?

Antwort anzeigen

Von oben nach unten:

7. Anwendung
8. Darstellung
9. Sitzung
10. Transport
11. Vermittlung
12. Sicherung
13. Bitübertragung

---

11. Auf welcher OSI-Schicht arbeitet die MAC-Adresse?

Antwort anzeigen

Die MAC-Adresse arbeitet auf Schicht 2, der Sicherungsschicht.

---

12. Auf welcher OSI-Schicht arbeitet die IP-Adresse?

Antwort anzeigen

Die IP-Adresse arbeitet auf Schicht 3, der Vermittlungsschicht.

---

13. Auf welcher OSI-Schicht arbeiten TCP und UDP?

Antwort anzeigen

TCP und UDP arbeiten auf Schicht 4, der Transportschicht.

---

14. Was ist der Unterschied zwischen OSI-Modell und TCP/IP-Modell?

Antwort anzeigen

Das OSI-Modell hat 7 Schichten und ist eher ein theoretisches Referenzmodell.

Das TCP/IP-Modell ist praxisnäher und wird im echten Netzwerkbetrieb häufiger verwendet. Es fasst mehrere OSI-Schichten zusammen.

---

15. Was bedeutet Datenkapselung?

Antwort anzeigen

Datenkapselung bedeutet, dass jede Netzwerkschicht eigene Steuerinformationen zu den Daten hinzufügt.

Beispiel:

Anwendungsdaten werden in TCP verpackt, TCP wird in IP verpackt, IP wird in Ethernet verpackt.

---

16. Was gehört zur Schicht 0 im Unterrichtskontext?

Antwort anzeigen

Zur Schicht 0 gehören die eigentlichen Übertragungsmedien, zum Beispiel:

- Kupferkabel
- Glasfaser
- Funk bei WLAN

Schicht 0 gehört nicht offiziell zum OSI-Modell, wird aber oft zur Erklärung genutzt.

---

17. Was ist ein Twisted-Pair-Kabel?

Antwort anzeigen

Ein Twisted-Pair-Kabel ist ein Netzwerkkabel mit verdrillten Adernpaaren. Die Verdrillung reduziert Störungen. Es wird häufig mit RJ45-Steckern im LAN verwendet.

---

18. Wie weit darf ein normales Twisted-Pair-Ethernet-Kabel ungefähr sein?

Antwort anzeigen

In der Praxis gilt meistens eine maximale Länge von ungefähr 100 Metern.

---

19. Was ist der Unterschied zwischen Multimode- und Singlemode-LWL?

Antwort anzeigen

Multimode-LWL wird eher für kürzere bis mittlere Strecken verwendet.

Singlemode-LWL wird für lange Strecken verwendet und hat einen kleineren Faserkern.

---

20. Warum darf man nicht direkt in eine Glasfaser schauen?

Antwort anzeigen

Weil dort unsichtbares Laserlicht austreten kann. Dieses Licht kann die Augen schädigen, auch wenn man es nicht sieht.

---

21. Welche WLAN-Verschlüsselung sollte mindestens verwendet werden?

Antwort anzeigen

Mindestens WPA2 sollte verwendet werden. Besser ist WPA3, wenn alle Geräte es unterstützen.

---

22. Warum ist ein Gäste-WLAN sinnvoll?

Antwort anzeigen

Ein Gäste-WLAN trennt fremde oder private Geräte vom internen Netzwerk. Gäste sollen zum Beispiel ins Internet kommen, aber nicht auf interne Server, Drucker oder NAS-Systeme zugreifen können.

---

23. Was ist ein Ethernet-Frame?

Antwort anzeigen

Ein Ethernet-Frame ist die Datenübertragungseinheit auf Schicht 2. Er enthält unter anderem Ziel-MAC-Adresse, Quell-MAC-Adresse, Nutzdaten und eine Prüfsumme.

---

24. Was ist die Aufgabe der FCS oder CRC im Ethernet-Frame?

Antwort anzeigen

FCS beziehungsweise CRC dient zur Fehlererkennung. Damit kann erkannt werden, ob ein Ethernet-Frame beschädigt wurde.

Fehlerhafte Frames werden verworfen.

---

25. Was ist eine MAC-Adresse?

Antwort anzeigen

Eine MAC-Adresse ist die Hardwareadresse einer Netzwerkschnittstelle. Sie ist normalerweise 48 Bit lang und wird hexadezimal dargestellt.

Beispiel:

```
00:1A:2B:3C:4D:5E
```

---

26. Was macht ein Switch?

Antwort anzeigen

Ein Switch verbindet Geräte in einem LAN und leitet Ethernet-Frames anhand der MAC-Adresse gezielt an den richtigen Port weiter.

---

27. Was ist der Unterschied zwischen einem Hub und einem Switch?

Antwort anzeigen

Ein Hub sendet empfangene Daten an alle Ports weiter.

Ein Switch lernt MAC-Adressen und sendet Frames gezielt nur an den passenden Port.

Ein Switch ist dadurch effizienter und sicherer als ein Hub.

---

28. Was ist eine SAT-Tabelle oder MAC Address Table?

Antwort anzeigen

Das ist die Tabelle eines Switches, in der gespeichert wird, welche MAC-Adresse an welchem Port erreichbar ist.

Dadurch kann der Switch Frames gezielt weiterleiten.

---

29. Was macht ARP?

Antwort anzeigen

ARP bedeutet Address Resolution Protocol.

ARP ermittelt zu einer IPv4-Adresse die passende MAC-Adresse im lokalen Netzwerk.

---

30. Was ist ein ARP-Request?

Antwort anzeigen

Ein ARP-Request ist eine Anfrage im lokalen Netzwerk:

„Wer hat diese IP-Adresse? Bitte sende mir deine MAC-Adresse.“

Diese Anfrage wird als Broadcast gesendet.

---

31. Was ist ein ARP-Reply?

Antwort anzeigen

Ein ARP-Reply ist die Antwort auf einen ARP-Request.

Das Zielgerät antwortet mit seiner MAC-Adresse.

---

32. Was ist ein Managed Switch?

Antwort anzeigen

Ein Managed Switch ist ein konfigurierbarer Switch. Man kann zum Beispiel VLANs, Port-Mirroring, Spanning Tree, Link Aggregation oder Port-Sicherheit einrichten.

---

33. Was ist Port-Mirroring?

Antwort anzeigen

Beim Port-Mirroring wird der Datenverkehr eines Ports auf einen anderen Port gespiegelt. Dadurch kann man den Verkehr zum Beispiel mit Wireshark analysieren.

---

34. Was ist Link Aggregation?

Antwort anzeigen

Link Aggregation fasst mehrere physische Netzwerkverbindungen zu einer logischen Verbindung zusammen.

Vorteile:

- höhere Gesamtbandbreite

- bessere Ausfallsicherheit
- Lastverteilung

---

35. Was ist Power over Ethernet?

Antwort anzeigen

Power over Ethernet, kurz PoE, bedeutet, dass Strom und Daten über dasselbe Netzwerkkabel übertragen werden.

Typische Geräte sind Access Points, IP-Telefone und Überwachungskameras.

---

36. Wozu dient das Spanning Tree Protocol?

Antwort anzeigen

Das Spanning Tree Protocol verhindert Netzwerkschleifen zwischen Switches.

Es blockiert bestimmte redundante Verbindungen logisch und kann sie bei Ausfall einer anderen Verbindung wieder aktivieren.

---

37. Was ist ein VLAN?

Antwort anzeigen

Ein VLAN ist ein Virtual Local Area Network.

Damit kann ein physisches Netzwerk in mehrere logisch getrennte Netzwerke aufgeteilt werden.

---

38. Warum setzt man VLANs ein?

Antwort anzeigen

VLANs werden eingesetzt, um Netzbereiche logisch zu trennen.

Vorteile:

- mehr Sicherheit
- bessere Struktur
- weniger Broadcast-Verkehr
- Trennung von Abteilungen, Gästen oder Servern

---

39. Was ist ein Tagged Port?

Antwort anzeigen

Ein Tagged Port überträgt VLAN-Informationen im Ethernet-Frame mit.

Er wird häufig für Verbindungen zwischen Switches oder zwischen Switch und Router/Firewall verwendet.

---

40. Was ist ein Untagged Port?

Antwort anzeigen

Ein Untagged Port gehört fest zu einem VLAN. Endgeräte wie PCs oder Drucker werden meistens an untagged Ports angeschlossen.

---

41. Was ist eine IPv4-Adresse?

Antwort anzeigen

Eine IPv4-Adresse ist eine 32-Bit-Adresse zur logischen Adressierung von Geräten in einem Netzwerk.

Beispiel:

```
192.168.1.10
```

---

42. Was macht die Subnetzmaske?

Antwort anzeigen

Die Subnetzmaske trennt eine IP-Adresse in Netzanteil und Hostanteil.

Beispiel:

`192.168.1.10/24`

Hier gehören die ersten 24 Bit zum Netzanteil.

---

43. Was ist die Netzadresse bei 192.168.1.10/24?

Antwort anzeigen

Die Netzadresse ist:

`192.168.1.0`

Bei `/24` gehören die ersten drei Oktette zum Netz. Das letzte Oktett ist der Hostanteil.

---

44. Was ist die Broadcast-Adresse bei 192.168.1.10/24?

Antwort anzeigen

Die Broadcast-Adresse ist:

`192.168.1.255`

Sie ist die letzte Adresse im Netz `192.168.1.0/24`.

---

45. Wie viele nutzbare Hosts gibt es in einem /24-Netz?

Antwort anzeigen

Ein `/24`-Netz hat 256 Adressen.

Davon sind 2 nicht nutzbar:

- Netzadresse

- Broadcast-Adresse

Also gibt es 254 nutzbare Hostadressen.

---

46. Welche privaten IPv4-Adressbereiche gibt es?

Antwort anzeigen

Private IPv4-Adressbereiche sind:

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`

Diese Adressen werden in privaten Netzwerken verwendet und nicht direkt im Internet geroutet.

---

47. Was bedeutet APIPA?

Antwort anzeigen

APIPA ist ein automatischer IPv4-Adressbereich, den ein Gerät verwenden kann, wenn kein DHCP-Server erreichbar ist.

Der Bereich lautet:

`169.254.0.0/16`

---

48. Was ist DHCP?

Antwort anzeigen

DHCP bedeutet Dynamic Host Configuration Protocol.

DHCP vergibt automatisch Netzwerkkonfigurationen an Clients, zum Beispiel:

- IP-Adresse
- Subnetzmaske
- Standardgateway

- DNS-Server

---

49. Wie lautet der DHCP-Ablauf?

Antwort anzeigen

Der DHCP-Ablauf lautet DORA:

1. Discover
2. Offer
3. Request
4. Acknowledge

Der Client sucht einen DHCP-Server, bekommt ein Angebot, fordert die Adresse an und erhält eine Bestätigung.

---

50. Was macht DNS?

Antwort anzeigen

DNS bedeutet Domain Name System.

DNS übersetzt Namen in IP-Adressen.

Beispiel:

`www.example.com`

wird in eine passende IP-Adresse aufgelöst.

---

51. Was ist Routing?

Antwort anzeigen

Routing bedeutet, Datenpakete zwischen verschiedenen Netzwerken weiterzuleiten.

Ein Router verbindet zum Beispiel zwei unterschiedliche IP-Netze miteinander.

---

52. Was ist ein Standardgateway?

Antwort anzeigen

Das Standardgateway ist der Router, an den ein Gerät Pakete sendet, wenn das Ziel nicht im eigenen lokalen Netzwerk liegt.

---

53. Was ist der Unterschied zwischen statischem und dynamischem Routing?

Antwort anzeigen

Beim statischen Routing werden Routen manuell eingetragen.

Beim dynamischen Routing tauschen Router Informationen automatisch über Routing-Protokolle aus.

---

54. Was ist ein Layer-3-Switch?

Antwort anzeigen

Ein Layer-3-Switch kann nicht nur auf Schicht 2 switchen, sondern auch auf Schicht 3 routen.

Er wird häufig eingesetzt, um VLANs im LAN miteinander zu verbinden.

---

55. Was ist ein Port in der Netzwerktechnik?

Antwort anzeigen

Ein Port ist eine Nummer auf Schicht 4, mit der Anwendungen oder Dienste auf einem Gerät unterschieden werden.

Beispiel:

- HTTP: Port 80
- HTTPS: Port 443
- SSH: Port 22

---

56. Was ist der Unterschied zwischen IP-Adresse und Port?

Antwort anzeigen

Die IP-Adresse sagt, welches Gerät gemeint ist.

Der Port sagt, welcher Dienst oder welche Anwendung auf diesem Gerät gemeint ist.

Beispiel:

`192.168.1.10:443`

Gerät: `192.168.1.10`
Dienst: Port `443`

---

57. Was ist TCP?

Antwort anzeigen

TCP ist ein verbindungsorientiertes Transportprotokoll.

Es sorgt für zuverlässige Datenübertragung, richtige Reihenfolge und erneute Übertragung bei Verlust.

---

58. Was ist UDP?

Antwort anzeigen

UDP ist ein verbindungsloses Transportprotokoll.

Es ist schneller und schlanker als TCP, garantiert aber keine Zustellung und keine richtige Reihenfolge.

---

59. Was ist der TCP-Three-Way-Handshake?

Antwort anzeigen

Der TCP-Three-Way-Handshake baut eine TCP-Verbindung auf.

Ablauf:

1. Client sendet SYN
2. Server antwortet mit SYN/ACK
3. Client bestätigt mit ACK

Danach ist die Verbindung aufgebaut.

---

60. Nenne je zwei typische Dienste für TCP und UDP.

Antwort anzeigen

Typische TCP-Dienste:

- HTTPS
- SSH

Typische UDP-Dienste:

- DNS
- DHCP

---

61. Was ist NAT?

Antwort anzeigen

NAT bedeutet Network Address Translation.

Dabei werden IP-Adressen übersetzt, zum Beispiel private interne IP-Adressen in eine öffentliche IP-Adresse für den Internetzugang.

---

62. Was ist PAT?

Antwort anzeigen

PAT bedeutet Port Address Translation.

Dabei werden zusätzlich Ports verwendet, damit mehrere interne Geräte gleichzeitig über eine öffentliche IP-Adresse ins Internet kommunizieren können.

---

63. Was ist Portforwarding?

Antwort anzeigen

Portforwarding leitet Anfragen von außen an ein internes Gerät weiter.

Beispiel:

Eine Anfrage an die öffentliche IP auf Port 443 wird an einen internen Webserver weitergeleitet.

---

64. Warum kann Portforwarding ein Sicherheitsrisiko sein?

Antwort anzeigen

Portforwarding macht interne Dienste von außen erreichbar.

Wenn der Dienst schlecht abgesichert, veraltet oder falsch konfiguriert ist, kann er angegriffen werden.

---

65. Was ist eine Allowlist?

Antwort anzeigen

Eine Allowlist erlaubt nur ausdrücklich freigegebene Verbindungen, Programme, Geräte oder Benutzer.

Alles andere wird blockiert.

---

66. Was ist eine Blocklist?

Antwort anzeigen

Eine Blocklist blockiert ausdrücklich verbotene Verbindungen, Programme, Geräte oder Benutzer.

Alles, was nicht auf der Blocklist steht, kann erlaubt sein.

---

67. Was ist sicherer: Allowlist oder Blocklist?

Antwort anzeigen

Eine Allowlist ist meistens sicherer, weil nur ausdrücklich erlaubte Dinge zugelassen werden.

Das Prinzip lautet:

Alles ist verboten, außer es wurde erlaubt.

---

68. Was macht eine Firewall?

Antwort anzeigen

Eine Firewall kontrolliert Netzwerkverkehr anhand von Regeln.

Sie entscheidet, welche Verbindungen erlaubt oder blockiert werden.

---

69. Welche Kriterien kann eine Firewall prüfen?

Antwort anzeigen

Eine Firewall kann zum Beispiel prüfen:

- Quell-IP-Adresse
- Ziel-IP-Adresse
- Protokoll
- Port
- Richtung
- Verbindungszustand
- teilweise auch Anwendung oder Inhalt

---

70. Was bedeutet Default Deny?

Antwort anzeigen

Default Deny bedeutet:

Alles ist standardmäßig verboten. Nur ausdrücklich erlaubte Verbindungen werden zugelassen.

Das ist ein sicheres Grundprinzip für Firewall-Regeln.

---

71. Was ist eine Paketfilter-Firewall?

Antwort anzeigen

Eine Paketfilter-Firewall prüft einzelne Pakete anhand von Informationen wie Quell-IP, Ziel-IP, Protokoll und Port.

Sie betrachtet normalerweise nicht den vollständigen Verbindungszustand.

---

72. Was ist eine SPI-Firewall?

Antwort anzeigen

SPI bedeutet Stateful Packet Inspection.

Eine SPI-Firewall merkt sich bestehende Verbindungen und kann Antworten automatisch einer erlaubten Verbindung zuordnen.

---

73. Was ist der Unterschied zwischen Paketfilter und SPI-Firewall?

Antwort anzeigen

Ein Paketfilter prüft einzelne Pakete anhand fester Regeln.

Eine SPI-Firewall prüft zusätzlich den Zustand der Verbindung. Dadurch kann sie erkennen, ob ein Paket zu einer bereits erlaubten Verbindung gehört.

---

74. Was ist eine DMZ?

Antwort anzeigen

DMZ bedeutet Demilitarisierte Zone.

Eine DMZ ist ein separates Netzwerk für Server, die von außen erreichbar sein müssen, zum Beispiel Webserver oder Reverse Proxy.

---

75. Warum verwendet man eine DMZ?

Antwort anzeigen

Eine DMZ schützt das interne LAN.

Wenn ein öffentlich erreichbarer Server in der DMZ angegriffen oder kompromittiert wird, soll der Angreifer nicht direkt Zugriff auf das interne Netzwerk bekommen.

---

76. Was ist der Unterschied zwischen einstufiger und zweistufiger DMZ?

Antwort anzeigen

Bei einer einstufigen DMZ trennt eine Firewall Internet, DMZ und LAN.

Bei einer zweistufigen DMZ gibt es zwei Firewalls: eine zwischen Internet und DMZ und eine zwischen DMZ und LAN.

Die zweistufige DMZ ist sicherer, aber aufwendiger.

---

77. Was ist die INPUT-Chain bei einer Linux-Firewall?

Antwort anzeigen

INPUT betrifft Datenverkehr, der direkt an die Firewall selbst gerichtet ist.

Beispiel:

Ein Administrator verbindet sich per SSH mit der Firewall.

---

78. Was ist die OUTPUT-Chain bei einer Linux-Firewall?

Antwort anzeigen

OUTPUT betrifft Datenverkehr, der von der Firewall selbst ausgeht.

Beispiel:

Die Firewall stellt selbst eine DNS-Anfrage oder lädt Updates herunter.

---

79. Was ist die FORWARD-Chain bei einer Linux-Firewall?

Antwort anzeigen

FORWARD betrifft Datenverkehr, der durch die Firewall hindurchgeleitet wird.

Beispiel:

Ein Client aus dem LAN geht über die Firewall ins Internet.

---

80. Warum ist eine Firewall allein kein vollständiger Schutz?

Antwort anzeigen

Eine Firewall schützt nur nach ihren Regeln und an der Stelle, an der sie eingesetzt wird.

Zusätzlich braucht man:

- Updates
- sichere Passwörter
- Benutzerrechte
- Backups
- Monitoring
- Virenschutz
- sichere Konfiguration
- Schulung der Benutzer

Revision #1
Created 21 May 2026 02:33:35 by Admin
Updated 3 June 2026 06:18:12 by Admin