# ANHANG C

# Antworten zu den Fragen zur Einschätzung des Wissensstands

## Kapitel 1

1. D und F. Zu den anderen Antworten: Ethernet definiert Protokolle sowohl des Physical als auch des Data Link Layer. PPP ist ein Data-Link-Protokoll, IP ein Network-Layer-Protokoll und SMTP und HTTP Application-Layer-Protokolle.
2. A und G. Zu den anderen Antworten: IP ist ein Network-Layer-Protokoll, TCP und UDP sind Transport-Layer-Protokolle und SMTP und HTTP sind Application-Layer-Protokolle.
3. B. Die Interaktion benachbarter Layer geschieht auf einem Computer, wobei in diesem Modell zwei Layer benachbart sind. Der übergeordnete Layer fordert beim nächstniedrigeren Layer Dienste an und der untergeordnete Layer bietet seine Dienste dem nächsthöheren Layer an.
4. B. Die Interaktion gleichrangiger Layer geschieht auf verschiedenen Computern. Die von diesem Layer definierten Funktionen müssen üblicherweise von mehreren Computern vollzogen werden, z. B. indem ein Absender für ein Segment eine Sequenznummer angibt und der Empfänger den Erhalt dieses Segments bestätigt. Dieser Prozess wird auf nur einem Layer definiert, aber dieser muss auf verschiedenen Geräten implementiert sein, damit die Funktion ausgeführt werden kann.
5. A. Eine Kapselung ist als Prozess definiert, bei dem Daten ein Header aus einem übergeordneten Layer vorangestellt wird (möglicherweise wird auch ein Trailer angehängt).
6. D. Der Konvention nach bezieht sich der Begriff *Frame* auf den Teil einer Netzwerknachricht, in dem der Data-Link-Header sowie -Trailer und die gekapselten Daten enthalten sind. Beim Begriff *Paket* werden die Data-Link-Header und -Trailer weggelassen und es bleibt nur der Header des Network Layer mit seinen gekapselten Daten. Der Begriff *Segment* lässt den Header des Network Layer weg und es bleibt nur der Header des Transport Layer mit seinen gekapselten Daten.
7. C. Der Network Layer beschäftigt sich mit der Übermittlung von Daten über den vollständigen Ende-zu-Ende-Pfad. Dafür ist es erforderlich, dass man jedes Gerät anhand von Adressen identifizieren kann. Dabei muss es sich um logische Adressen handeln, die nicht mit den physischen Details des Netzwerks verknüpft sind.
8. A. Zum Physical Layer im OSI-Modell gehören alle Standards, die die Form von Steckverbindern, die Leitungsführung in den Verbindungskabeln, elektrische Details und die Kodierung festlegen, mit denen die elektrischen Signale für den Versand über ein Kabel in Bits kodiert werden.

## Kapitel 2

1. A. Das IEEE definiert die Ethernet-LAN-Standards, wobei die Namen standardmäßig mit 802.3 beginnen und bei allen Kabeln verwendet werden. Das IEEE definiert ferner die WLAN-Standards, deren Namen normalerweise mit 802.11 beginnen und die einen von Ethernet separaten Standard darstellen.
2. C. Die Zahl vor dem Wort *BASE* definiert die Datenrate in Megabit pro Sekunde (Mbit/s). 1000 Mbit/s entsprechen 1 Gigabit pro Sekunde (1 Gbit/s). Das *T* im Suffix verweist auf eine Twisted-Pair- oder UTP-Verkabelung und somit ist 1000BASE-T der auf UTP basierende Standardname für Gigabit Ethernet.
3. B. Bei Crossover-Kabeln kreuzen sich die Adernpaare für eine Richtung an einer Stelle, wobei ein Adernpaar für die Senderichtung und eines für die Empfangsrichtung verwendet wird. Bei 10-Mbit/s- und 100-Mbit/s-Ethernet verbindet das spezielle Crossover-Kabel das Adernpaar für die Pins 1 bzw. 2 an den beiden Kabelenden mit den Pins 3 bzw. 6 am anderen Ende des Kabels.
4. B, D und E. Router, Ethernet-Ports an Wireless Access Points und PC-NICs senden alle über die Pins 1 und 2, während Hubs und LAN-Switches die Daten über die Pins 3 und 6 übermitteln. Straight-Through-Kabel verbinden Geräte zum Senden über jeweils gegenüberliegende Kontaktpaare, weil das Kabel die Anschlussbelegung nicht kreuzen muss.
5. B. NICs und Switch-Ports verwenden den CSMA/CD-Algorithmus (Carrier Sense Multiple Access with Collision Detection) zur Implementierung der Halbduplexlogik. Zwar versucht CSMA/CD, Kollisionen zu vermeiden, kann deren Vorkommen aber erkennen und regelt, wann die Ethernet-Knoten das Senden unterbrechen sollen, um zu warten und es später erneut zu versuchen.
6. C. Durch das FCS-Feld im Ethernet-Trailer mit 4 Byte kann der empfangende Knoten sehen, was der sendende Knoten mit einer mathematischen Formel berechnet hat. Dies ist ein zentraler Bestandteil für die Fehlererkennung. Beachten Sie, dass Ethernet einen Prozess für die Fehlererkennung, nicht aber für die Fehlerkorrektur definiert.
7. B, C und E. Bei der vorab zugewiesenen universellen MAC-Adresse, die jeder Ethernet-Port bei der Herstellung erhält, wird die Adresse in zwei Hälften mit jeweils 3 Byte aufgeteilt. Die erste Hälfte bezeichnet man als OUI (Organizationally Unique Identifier), den das IEEE als eindeutige Hexadezimalzahl dem Unternehmen zuweist, die das Produkt herstellt. Dieser OUI wird nur von diesem Unternehmen verwendet.
8. C und D. Ethernet unterstützt Unicast-Adressen, die einen Ethernet-Knoten identifizieren, und Gruppenadressen, über die man einen Frame an mehrere Ethernet-Knoten versenden kann. Bei den Gruppenadressen gibt es die Typen *Broadcast-Adresse* und *Multicast-Adresse*.

## Kapitel 3

1. B. Das vieradrige Kabel des Telekommunikationsanbieters wird mit dem Gerät verbunden, das als CSU/DSU dient. Dabei kann die CSU/DSU ein externes Gerät sein oder in eine serielle Interfacekarte des Routers integriert werden. LAN-Switches haben keine seriellen Interfaces und serielle Router-Interfaces haben keine Transceiver.

2. C. Standleitungen können mit verschiedenen voreingestellten Datenraten betrieben werden. Dazu gehören Vielfache von 64 Kbit/s bis hin zum 24-Fachen von 64 Kbit/s. Die Datenraten können auch Vielfache von T1-Datenraten sein, also 1,544 Mbit/s bis hin zum 28-Fachen dieser Datenrate.
3. B. Im HDLC-Standard-Header gibt es kein Type-Feld, über das die Art des Pakets identifiziert werden kann, das im HDLC-Frame gekapselt ist.
4. B und D. Die physische Installation arbeitet nach einem Modell, bei dem jeder Router über eine physische Ethernet-Verbindung mit einem SP-Gerät über ein SP-Feature namens Point of Presence (PoP) verbunden ist. Der Ethernet-Link reicht nicht vom einen Endverbrauchergerät zum anderen. Aus Sicht des Data Link Layer arbeiten beide Router mit dem gleichen Ethernet-Standard-Header und -Trailer, wie sie in LANs verwendet werden; bei diesen Ethernet-WAN-Links ist HDLC nicht relevant.
5. B und C. Standleitungen übermitteln Daten mit der gleichen Datenrate in beide Richtungen und somit ist dieser Dienst symmetrisch. DSL und Kabelinternet bieten asymmetrische Datenraten, wobei die Datenrate im Downstream höher ist. BGP ist ein Routing-Protokoll und keine Technologie für den Internetzugang.
6. C. Bei DSL sind keine Änderungen bei der Telefonverkabelung nötig. Das Telefon kann mit jeder funktionierenden Telefonsteckdose verbunden werden, so als gäbe es weder DSL-Modem noch -Router.

## Kapitel 4

1. A und C. Der Network Layer definiert die logische Adressierung (als Gegenstück zur physischen Adressierung). Mit der logischen Adressstruktur kann man Adressen leicht gruppieren und macht somit das Routing effizienter. Die Pfadauswahl bezieht sich auf das Vorhaben, die besten Routen in einem Netzwerk zu finden. Die physische Adressierung und Aushandlung der Verbindungsparameter sind typische Funktionen des Data Link Layer und die Fehlerkorrektur ist normalerweise eine Funktion des Transport Layer.
2. B. 224.1.1.1 ist eine Klasse-D-Adresse.
3. D. Das erste Oktett von Klasse-A-Adressen reicht von 1 bis 126 inklusive, bei Klasse B von 128 bis 191 inklusive und bei Klasse C von 192 bis 223 inklusive. 127 befindet sich technisch im Bereich von Klasse A, wird aber zur Verwendung als Loopback-Adresse reserviert.
4. D und F. Wird kein Subnetting eingesetzt, müssen sich alle Adressen im gleichen Netzwerk wie 10.1.1.1 (alle Adressen im Klasse-A-Netzwerk 10.0.0.0) im gleichen LAN befinden. Adressen, die von diesem Netzwerk über einen Router getrennt sind, können sich nicht im Netzwerk 10.0.0.0 befinden. Also sind nur die beiden Antworten korrekt, bei denen eine gültige Unicast-IP-Adresse aufgeführt wird, die sich nicht im Netzwerk 10.0.0.0 befindet.
5. A. PC1 wird ein Ethernet-Frame an Router 1 senden und dabei als Absenderadresse die MAC-Adresse von PC1 sowie als Empfängeradresse die MAC-Adresse von Router 1 angeben. Router 1 entkapselt das IP-Paket aus diesem Ethernet-Frame, indem er Ethernet-Header und -Trailer entfernt. Router 1 wird das IP-Paket weiterleiten und es dafür zuerst in ein HDLC-Frame kapseln – der vorherige Ethernet-Frame wird *nicht* im HDLC-Frame gekapselt. Router 2 wird das IP-Paket aus dem HDLC-Frame entkapseln und es an das Ethernet-LAN weiterleiten, wobei ein neuer Ethernet-Header und -Trailer eingefügt wird, der aber anders aussieht als zuvor. Der Header wird die MAC-Adresse von Router 2 als Absenderadresse und die MAC-Adresse von PC2 als Empfängeradresse angeben.

6. C. Router vergleichen die Empfänger-IP-Adresse des Pakets mit ihrer IP-Routing-Tabelle und verwenden die Anweisungen der jeweils passenden Route, um das IP-Paket weiterzuleiten.
7. B und C. IPv4-Hosts nutzen generell eine Logik mit zwei Hauptzweigen. Um ein IP-Paket an einen anderen Host im gleichen IP-Netzwerk oder ein Subnetz im gleichen LAN weiterzuleiten, schickt der Absender das IP-Paket direkt an diesen Host. Anderenfalls versendet er das Paket an seinen Default-Router (auch als Default-Gateway bezeichnet).
8. A und C. Router führen zwar alle in den vier Antworten angegebenen Aktionen aus, doch das Routing-Protokoll ist nur für die in den beiden angegebenen Antworten benannten Funktionen zuständig. Unabhängig vom Routing-Protokoll erlernt ein Router die Routen für IP-Subnetze und IP-Netzwerke, die direkt mit seinen Interfaces verbunden sind. Router leiten außerdem IP-Pakete weiter, aber dieser Prozess nennt sich IP-Routing oder IP-Forwarding und ist von den Abläufen des Routing-Protokolls unabhängig.
9. C. Über das Address Resolution Protocol (ARP) kann PC1 Informationen lernen, doch diese Infos werden nicht auf einem Server gespeichert. Via **ping** kann der Anwender von PC1 erfahren, ob Pakete im Netzwerk fließen können, aber auch bei diesem Befehl wird kein Server benutzt. Beim Domain Name System (DNS) agiert PC1 als DNS-Client und kontaktiert einen DNS-Server, der mit Informationen über die IP-Adressen antwortet, die zu einem bestimmten Hostnamen gehören.

## Kapitel 5

1. D und E. Viele Header enthalten ein Feld, das den in der Nachricht nachfolgenden Header identifiziert. Ethernet verwendet das Ethernet-Type-Feld und der IP-Header arbeitet mit dem Protocol-Feld. Die TCP- und UDP-Header benennen die Anwendung, die die auf den Header folgenden Daten empfangen sollen, mithilfe des im jeweiligen Header enthaltenen Port-Felds.
2. A, B, C und F. IP definiert das Routing – nicht TCP. Viele andere Protokolle definieren eine Verschlüsselung, nicht aber TCP. Die korrekten Antworten listen einfach verschiedene TCP-Features auf.
3. C. TCP führt Windowing, Fehlerkorrektur und eine geordnete Datenübertragung aus, UDP hingegen nicht. Keines von beiden sorgt für Routing oder Verschlüsselung.
4. C und F. Die Bezeichnungen *Paket* und *L3PDU* beziehen sich auf den Header zuzüglich der durch Layer 3 gekapselten Daten. *Frame* und *L2PDU* beziehen sich auf den Header (und Trailer) zuzüglich der durch Layer 2 gekapselten Daten. *Segment* und *L4PDU* beziehen sich auf Header und Daten, die vom Transport-Layer-Protokoll gekapselt werden.
5. B. Beachten Sie, dass der gesamte Text zwischen // und / den Hostnamen darstellt. Der Text vor // identifiziert das Application-Layer-Protokoll und der Teil nach dem / repräsentiert den Namen der Webseite.
6. C und D. Web-Traffic verwendet TCP als Transportprotokoll und HTTP als Anwendungsprotokoll. Infolgedessen verwendet der Webserver in der Regel den TCP-Port 80, bei dem es sich um den Well-Known-Port für HTTP-Traffic handelt. Nachrichten, die an den Webserver übertragen werden, würden den TCP-Empfängerport 80 aufweisen, vom Server versendete Nachrichten hätten den Absenderport 80.

## Kapitel 6

1. A und B. Der fragliche Befehl ist ein EXEC-Befehl, der nur User-Modus-Zugriff benötigt. Als solchen können Sie diesen Befehl sowohl im User- als auch im Enable-Modus verwenden. Weil es ein EXEC-Befehl ist, können Sie diesen (entsprechend der Fragestellung) nicht im Konfigurationsmodus verwenden.

   Beachten Sie jedoch, dass Sie im Konfigurationsmodus das Wort **do** vor den EXEC-Befehl setzen können (z. B. **do show mac address-table**); so lässt sich der Befehl aus jedem beliebigen Konfigurationsmodus absetzen.

2. B. Der Befehl, auf den in der Frage angespielt wird (also **reload**), ist ein EXEC-Befehl, der den Enable-Modus benötigt. Dieser Befehl ist im User-Modus nicht verfügbar.

   Beachten Sie jedoch, dass Sie im Konfigurationsmodus das Wort **do** vor den EXEC-Befehl setzen können (z. B. **do reload**); so lässt sich der Befehl aus jedem beliebigen Konfigurationsmodus absetzen.

3. B. SSH bietet die Option für eine sichere Remote-Anmeldung, bei der alle Datenübermittlungen verschlüsselt werden – so etwa der Austausch von Passwörtern. Bei Telnet werden alle Daten einschließlich Passwörter unverschlüsselt übertragen.

4. A. Switches (wie auch Router) legen die aktuell verwendete Konfiguration im RAM ab. Dabei nutzen Sie das NVRAM zum Speichern der Konfigurationsdatei, die beim nächsten Laden des IOS durch das Gerät geladen werden soll.

5. F. Die Datei *startup-config* befindet sich im NVRAM und die Datei *running-config* im RAM.

6. B und C. Durch den Befehl **exit** gelangt der Benutzer von einem untergeordneten Konfigurationsmodus zurück in den globalen Konfigurationsmodus bzw. – falls er sich bereits im globalen Konfigurationsmodus befindet– zurück in den Enable-Modus. Aus dem Konsolenmodus versetzt er den Benutzer zurück in den globalen Konfigurationsmodus. Sowohl der Befehl **end** als auch die Tastenfolge CTRL+Z versetzen den Benutzer unabhängig vom aktuellen Konfigurationsmodus stets zurück in den Enable-Modus.

## Kapitel 7

1. A. Ein Switch vergleicht die Empfänger-MAC-Adresse mit der MAC-Adresstabelle. Wird ein passender Eintrag gefunden, dann leitet der Switch den Frame über das entsprechende Interface weiter. Wird keine Übereinstimmung gefunden, flutet der Switch den Frame.

2. C. Ein Switch flutet Broadcast-Frames, Multicast-Frames (falls keine Multicast-Optimierungen aktiviert sind) sowie Unicast-Frames mit unbekanntem Empfänger (also Frames, deren Empfänger-MAC-Adresse sich nicht in der MAC-Adresstabelle befindet).

3. A. Ein Switch flutet Broadcast-Frames, Multicast-Frames (falls keine Multicast-Optimierungen aktiviert sind) sowie Unicast-Frames mit unbekanntem Empfänger (also Frames, deren Empfänger-MAC-Adresse sich nicht in der MAC-Adresstabelle befindet).

4. B. Switches müssen die Position aller MAC-Adressen kennen, die im LAN relativ zu diesem lokalen Switch verwendet werden. Wenn ein Switch einen Frame empfängt, identifiziert die Absender-MAC-Adresse den Absender. Das Interface, an dem der Frame eintrifft, ermittelt das lokale Switch-Interface, das in der LAN-Topologie am dichtesten bei diesem Knoten liegt.

5. C. Der Befehl **show interfaces status** gibt pro Interface eine Zeile aus. Cisco Catalyst-Switches geben den Interfacetyp entsprechend der höchsten Datenrate des Interface an. Folglich fallen 10/100-Interfaces in die Kategorie Fast Ethernet. Bei einer funktionierenden Verbindung würde für die Ports FastEthernet 0/1 bis 0/10 der Status *connected* angegeben, während die übrigen Interfaces den Status *notconnected* aufwiesen.

6. D. Richtige Antwort: Jeder Eintrag gibt die erlernte MAC-Adresse an. Definitionsgemäß werden dynamisch erlernte MAC-Adressen durch Prüfung der Absender-MAC-Adresse eingehender Frames erlernt. (Durch diese Tatsache wird auch eine der falschen Antworten ausgeschlossen.)

   Mit dem Befehl **show mac address-table dynamic** wird die aktuelle Liste der MAC-Tabelleneinträge aufgelistet. Diese enthielt zum Zeitpunkt der Erstellung der Ausgabe drei bekannte Einträge. Der Zähler in der letzten Ausgabezeile gibt die Anzahl der aktuellen Einträge an, nicht die Gesamtzahl der erlernten MAC-Adressen seit dem letzten Neustart. So hätte der Switch etwa auch andere MAC-Adressen erlernen können, deren Einträge bereits zu einem früheren Zeitpunkt abgelaufen und deswegen aus der MAC-Adresstabelle entfernt worden wären.

   Die Antwort schließlich, die angibt, dass Port Gi0/2 direkt mit einem Gerät mit einer bestimmten MAC-Adresse verbunden ist, kann stimmen, muss es aber nicht. Dieser Port könnte genauso gut mit einem anderen Switch verbunden sein, der wiederum mit einem weiteren Switch verbunden ist usw., und an einen dieser Switches wäre dann das Gerät angeschlossen, das die angegebene MAC-Adresse verwendet.

## Kapitel 8

1. B. Wenn beide Befehle konfiguriert sind, akzeptiert das IOS nur das Passwort, wie es im Befehl **enable secret** konfiguriert wurde.

2. A. Zur Beantwortung dieser Frage ist es wahrscheinlich am besten, sich zunächst die Gesamtkonfiguration vor Augen zu führen und dann alle Antworten zu ermitteln, die dieser Konfiguration entsprechen. Die Befehle im VTY-Line-Konfigurationsmodus wären **password** *passwort* und **login**. Nur eine Antwort gibt einen VTY-Subbefehl an, der einer dieser beiden Befehle ist.

   Zu den falschen Antworten:

   Eine Antwort erwähnt Konsolensubbefehle. Die Konsole definiert nicht, was passiert, wenn Remote-Benutzer sich anmelden; diese Details sind Bestandteil der VTY-Line-Konfiguration.

   Eine Antwort nennt den Befehl **login local**; dieser Befehl bedeutet, dass der Root-Switch die lokale Liste konfigurierter Benutzernamen und Passwörter verwendet. Die Frage gab an, dass der Techniker nur Passwörter, aber keine Benutzernamen verwenden wollte.

   Eine Antwort nennt den Befehl **transport input ssh**, der – weil das Schlüsselwort **telnet** fehlt – Telnet deaktiviert. Zwar kann dieser Befehl nützlich sein, aber SSH funktioniert nicht, wenn nur Passwörter verwendet werden: Das Protokoll erfordert neben dem Passwort zwingend einen Benutzernamen. Folglich würde durch die Deaktivierung von Telnet (und das alleinige Zulassen von SSH) erfolgreich verhindert, dass sich überhaupt jemand remote am Switch anmeldet.

3. B und C. Für SSH ist neben dem Einsatz von Benutzernamen auch ein Passwort erforderlich. Man kann z. B. über den globalen Befehl **username** Benutzernamen (und entsprechende Passwörter) so definieren, dass sie SSH unterstützen. Die VTY-Lines müssten auch so konfiguriert werden, dass sie den Einsatz von Benutzernamen vorschreiben; das geht z. B. über den VTY-Subbefehl **login local**. Der Befehl **transport input ssh** könnte zu einer sinnvollen Konfiguration gehören, ist aber kein globaler Konfigurationsbefehl (wie in einer der falschen Antworten behauptet). Ähnlich bezeichnet eine Antwort **username** als Befehl im VTY-Konfigurationsmodus, was ebenfalls der falsche Modus ist.
4. A, D und F. Um einen Telnet-Zugriff zu erlauben, muss beim Switch die Passwortsicherheit aktiviert sein, mindestens anhand des Konfigurationssubbefehls **password** für die VTY-Lines. Zusätzlich benötigt der Switch eine IP-Adresse (die per VLAN-Interface konfiguriert wird) und ein Default-Gateway, sofern er mit Hosts in einem anderen Subnetz kommunizieren soll.
5. B und C. Für den SSH-und Telnet-Zugriff braucht ein Switch immer eine korrekte IP-Konfiguration. Dies schließt die Konfiguration einer korrekten IP-Adresse und Maske auf einem VLAN-Interface ein. Dieses VLAN-Interface benötigt dann einen Pfad aus dem Switch heraus über Ports, die dem betreffenden VLAN zugewiesen sind. Im vorliegenden Fall, in dem alle Ports VLAN 2 zugewiesen sind, muss der Switch das Interface VLAN 2 (und zu diesem Zweck den Konfigurationsbefehl **interface vlan 2**) verwenden.

   Um die Anforderung zu erfüllen, Anmeldungen auch von Hosts außerhalb des lokalen Subnetzes zu gestatten, muss auf dem Switch mit dem globalen Befehl **ip default-gateway 172.16.2.254** ein korrektes Default-Gateway konfiguriert werden.
6. A. Der Line-Subbefehl **logging synchronous** synchronisiert die Anzeige von Logmeldungen mit anderen Befehlsausgaben, damit die Logmeldung die Ausgabe eines **show**-Befehls nicht unterbricht. Der Befehl **no ip domain-lookup** ist kein Line-Subbefehl. Die anderen beiden falschen Antworten sind zwar Line-Subbefehle, haben aber mit der Konfiguration der in der Frage genannten Funktion nichts zu tun.

## Kapitel 9

1. F. Cisco-Switches haben keinen Befehl, um das Autonegotiating von Datenrate und Duplexmodus zu deaktivieren. Stattdessen deaktiviert ein Switch-Port, bei dem sowohl **speed** als auch **duplex** konfiguriert sind, das Autonegotiating.
2. E. Bei Cisco-Switches kann man im Interfacekonfigurationsmodus die Datenrate (mit dem Befehl **speed**) und den Duplexmodus (mit dem Befehl **duplex**) konfigurieren.
3. A und D. Die Regeln für das IEEE-Autonegotiating sehen vor, dass ein Gerät, welches das Autonegotiating nutzen möchte, aber vergeblich auf eine Reaktion der Gegenstelle wartet, die niedrigste unterstützte Datenrate verwendet. Cisco-Switches setzen diese Regel allerdings außer Kraft: Sie nehmen eine Stichprobe des elektrischen Signals, um die Datenrate des angeschlossenen Geräts zu ermitteln. Deswegen verwendet der Switch zur Übertragung eine Datenrate von 1000 Mbit/s. Der Switch nutzt die IEEE-Default-Einstellung für den Duplexbetrieb basierend auf der Datenrate, und der IEEE-Default für Duplexübertragungen bei 1000 Mbit/s ist der Vollduplexbetrieb. In diesem Fall entsprechen die Switch-Einstellungen also sowohl der Datenrate als auch der Duplexeinstellung des PC.

4. B. Die Einstellung für die maximale Zahl von MAC-Adressen steht standardmäßig auf 1 und somit muss der Befehl **switchport port-security maximum** nicht konfiguriert werden. Mit Sticky-Learning braucht man auch die konkreten MAC-Adressen nicht vorzudefinieren. Allerdings muss man die Port Security aktivieren und das erfordert den Interfacesubbefehl **switchport port-security**.

5. B und C. Zunächst zu den zwei falschen Antworten: Im *restrict*-Modus bewirkt der Empfang eines Frames, der gegen die Port-Security-Richtlinie verstößt, noch nicht, dass der Switch das Interface in den Status *err-disabled* versetzt. Zwar werden alle Frames verworfen, die gegen die Anforderungen verstoßen, aber das Interface bleibt aktiv und legitime Frames (z. B. der zweite) werden nach wie vor weitergeleitet.

   Was die beiden richtigen Antworten angeht, so sorgt ein Port im *restrict*-Modus dafür, dass der Switch Logmeldungen für unzulässige Frames ausgibt, bei konfiguriertem SNMP Traps zu diesem Vorfall versendet und den Zähler für unzulässige Frames hochsetzt.

6. B und D. Was den Sticky-Parameter angeht, bewirkt der Befehl, dass der Switch die Absender-MAC-Adresse erlernt und damit einen Interfacesubbefehl **switchport port-security mac-address** *adresse* absetzt. Die Port Security fügt den Befehl jedoch zur *running-config* hinzu; deswegen muss der Netzwerktechniker auch den EXEC-Befehl **copy running-config startup-config** absetzen, um die Konfiguration zu speichern.

   Zur zweiten richtigen Antwort: Benutzer können einen Switch an das Kabelende anschließen, auch wenn mehrere Geräte mit diesem Switch verbunden sind. Nichts anderes geschieht in echten Netzwerken, wenn Benutzer feststellen, dass sie zusätzliche Ports auf ihrem Schreibtisch benötigen. Allerdings sorgt die Default-Einstellung **switchport port-security maximum 1** dafür, dass ein Frame von der zweiten eindeutigen Absender-MAC-Adresse einen Verstoß darstellt, und aufgrund der Default-Einstellung wird der Port dann in den Status *err-disabled* versetzt.

   Was die zweite falsche Antwort betrifft, so verhindert die Konfiguration nicht, dass unbekannte MAC-Adressen auf den Port zugreifen können, denn in der Konfiguration ist keine MAC-Adresse vordefiniert.

## Kapitel 10

1. A. Eine Kollisionsdomäne enthält alle Geräte, deren Frames mit jenen kollidieren könnten, die von den anderen Geräten der Domäne gesendet wurden. Bridges, Switches und Router separieren oder segmentieren ein LAN in mehrere Kollisionsdomänen, was Hubs und Repeater wiederum nicht machen.

2. A, B und C. Eine Broadcast-Domäne enthält alle Geräte, deren gesendete Broadcast-Frames an alle anderen Geräte in der Domäne übertragen werden sollen. Hubs, Repeater, Bridges und Switches separieren bzw. segmentieren das LAN nicht in mehrere Broadcast-Domänen, Router hingegen schon.

3. B und D. Die Access-Layer-Switches binden Endpunkte an – egal, ob Server oder Endbenutzergeräte. Weiter ist jeder Access-Layer-Switch in der Regel mit zwei Distribution-Layer-Switches verbunden, während es zwischen den Access-Layer-Switches keinerlei direkte Verbindungen gibt. Hierdurch entsteht eine Partial-Mesh-Struktur. Ein 2-Ebenen-Modell – auch Collapsed Core genannt – umfasst überhaupt keine Core-Switches.

4. A und C. Nicht die Distribution-Layer-Switches, sondern die Access-Layer-Switches binden Endpunkte an – egal, ob Server oder Endbenutzergeräte. Weiter ist jeder Access-Layer-Switch in der Regel mit zwei Distribution-Layer-Switches verbunden, während es zwischen den Access-Layer-Switches keinerlei direkte Verbindungen gibt. Hierdurch entsteht eine Partial-Mesh-Struktur. Ein 3-Ebenen-Modell – auch Core-Design genannt – verwendet Core-Switches und nutzt ein Partial-Mesh mit Links zwischen Distribution- und Core-Switches. Im Wesentlichen ist jeder Distribution-Switch mit mehreren Core-Switches, normalerweise aber nicht mit anderen Distribution-Switches verbunden.
5. D. Der Access-Layer umfasst Access-Layer-Switches, die mit Endpunkten verbunden sind. Ein einzelner Access-Layer-Switch mit Endpunkten sieht wie eine Sterntopologie aus. Der Distribution-Layer bildet ein Partial-Mesh mit Links zwischen Distribution- und Access-Layer-Switches, ist also weder ein Full-Mesh noch ein Hybrid.
6. B und D. Die IEEE-Ethernet-Standards unterstützen Kabelstrecken mit einer Länge bis 100 Meter, sofern eine UTP-Verkabelung eingesetzt wird. Die meisten Standards, die mit Glasfaserkabeln arbeiten (wie die in den beiden korrekten Antworten), verwenden Kabel, die länger als 100 Meter sind.

## Kapitel 11

1. B. Ein VLAN ist eine Gerätegruppe in der gleichen Layer-2-Broadcast-Domäne. Ein Subnetz enthält oft genau die gleiche Gerätegruppe, ist aber ein Konzept von Layer 3. Eine Kollisionsdomäne bezieht sich auf eine Gruppe Ethernet-Geräte, hat aber andere Regeln als VLANs, nach denen bestimmt wird, welche Geräte sich in der gleichen Kollisionsdomäne befinden.
2. D. Zwar sind ein Subnetz und ein VLAN keine gleichwertigen Konzepte, doch befinden sich Geräte, die zum selben VLAN gehören, meist im selben Subnetz und umgekehrt.
3. B. 802.1Q definiert einen Header mit 4 Bytes, der nach den Feldern für die Empfänger- und Absender-MAC-Adresse des ursprünglichen Frames eingefügt wird. Durch Einfügen dieses Headers werden weder Absender- noch Empfängeradresse des ursprünglichen Frames geändert. Der Header selbst enthält ein 12-Bit-VLAN-ID-Feld, das das mit dem Frame verknüpfte VLAN identifiziert.
4. A und C. Die Einstellung **dynamic auto** bedeutet, dass der Switch das Trunking verhandeln kann. Er kann aber nur auf Verhandlungsnachrichten reagieren und den Verhandlungsprozess nicht selber einleiten. Insofern muss der andere Switch für das Trunking oder aber so konfiguriert sein, dass er den Verhandlungsprozess einleitet (dies konfiguriert man mit der Option **dynamic desirable**).
5. Die konfigurierte VTP-Einstellung des transparenten VTP-Modus gibt an, dass der Switch VLANs konfigurieren kann, d. h., das VLAN ist konfiguriert. Zusätzlich erscheinen die VLAN-Konfigurationsdetails wie z. B. der VLAN-Name als Teil der Datei *running-config*.
6. B und C. Der Befehl **show interfaces switchport** listet den administrativen und auch den operativen Status eines jeden Ports auf. Wenn ein Switch das Trunking bei einem Port erkennt, gibt dieser Befehl für den Trunk-Status *trunk* aus. Der Befehl **show interfaces trunk** listet eine Gruppe von Interfaces auf, die aktuell als Trunks operieren. Also identifizieren diese beiden Befehle Interfaces, bei denen es sich um operative Trunks handelt.

## Kapitel 12

1. C und D. Diese Frage dreht sich um ein Thema, das seinem Wesen nach subjektiv ist. Cisco schreibt keine bestimmte Troubleshooting-Methodik vor. Allerdings gibt es eine Reihe von Best Practices, die sich als sinnvoll erwiesen haben und in realen Netzwerken auch funktionieren. Die falschen Antworten zu dieser Frage wurden bewusst auffällig ausgewählt. Damit sollte veranschaulicht werden, was Cisco zu den Troubleshooting-Methoden in den Prüfungsthemen sagt. Diese Frage verknüpft diese Themen nämlich mit Aufgaben für den gesunden Menschenverstand, wie es auch bei den Prüfungsthemen der Fall ist.

   Eine falsche Antwort besagt, dass man nicht unnötig Zeit mit der Dokumentation verlieren soll. Dies steht im Gegensatz zu einem der Prüfungsthemen und widerspricht allen guten Troubleshooting-Praktiken. Grenzen Sie Probleme ein und notieren Sie Ihre Erkenntnisse.

   Zwei Antworten benennen den empfohlenen letzten Schritt beim Troubleshooting-Prozess, weswegen (mindestens) eine davon falsch sein muss. Die Behebung des Problems ist nicht der letzte Schritt: Wenn nämlich das Problem behoben ist, sollte sich die damit befasste Person vergewissern, dass dies tatsächlich der Fall ist, und möglicherweise den Zustand für eine gewisse Zeit überwachen, bevor das Problem endgültig als behoben betrachtet wird.

   Die Antwort, die den Eskalationsvorgang erwähnt, definiert im Wesentlichen einen guten Prozess: Wenn der Techniker das Problem nicht lösen kann, sollte er wissen, wie er es an einen anderen Techniker oder Manager eskaliert, und dabei die Vorgehensweise befolgen.

2. A, B und D. Der Status *disabled* im Befehl **show interfaces status** ist der gleiche wie der Status *administratively down/down*, der im Befehl **show interfaces** gezeigt wird. Das Interface muss mit dem Befehl **show interfaces status** aktiviert worden sein, damit der Switch Frames darüber versenden kann.

3. A und D. Bei SW2 ist das IEEE-Standard-Autonegotiating durch die Konfiguration von Datenraten- und Duplexeinstellungen grundsätzlich deaktiviert worden. Allerdings können Cisco-Switches die vom anderen Gerät verwendete Datenrate erkennen, auch wenn Autonegotiating ausgeschaltet ist. Außerdem besagt bei 1 Gbit/s der IEEE-Autonegotiating-Standard, dass der Vollduplexmodus zum Einsatz kommen soll, wenn die Duplexeinstellungen nicht verhandelt werden können. Also arbeiten beide Seiten mit 1 Gbit/s im Vollduplexmodus.

4. B und D. Der Befehl **show interfaces** listet die aktuellen Einstellungen für Datenrate und Duplexmodus auf, sagt aber nichts darüber aus, wie die Einstellungen konfiguriert oder ausgehandelt wurden. Der Befehl **show interfaces status** listet vor den Einstellungen für Datenrate und Duplexmodus das Präfix **a-** auf, um anzuzeigen, dass diese Einstellung per Autonegotiating erfolgt ist. Fehlt dieses Präfix, wurde diese Einstellung konfiguriert.

5. B und C. Das IOS fügt MAC-Adressen, die per Port Security konfiguriert wurden, als statische MAC-Adressen ein. Somit erscheinen sie nicht in der Ausgabe des Befehls **show mac address-table dynamic**. **show mac address-table port-security** ist kein gültiger Befehl.

6. A und C. Der Befehl **show mac address-table** listet alle Einträge in der MAC-Adresstabelle des Switchs auf, einschließlich der dynamisch erlernten und statisch definierten Adressen. Von links nach rechts gelesen werden in der Ausgabe die VLAN-ID, die MAC-Adresse, der Typ (statisch oder dynamisch) und die verknüpften Ports (über die die Frames, die an die angegebene Adresse gesendet wurden, von diesem Switch weitergeleitet werden) aufgeführt.

**7.** B. Die Frage besagt, dass der Port-Security-Status *secure-shutdown* ist. Dieser Status wird nur vom Port-Security-Modus *shutdown* verwendet und in diesem Fall wird das Interface auch in den Status *err-disabled* versetzt. Diese Tatsachen erklären, warum die betreffende Antwort korrekt ist – und zwei der anderen Antwortoptionen eben nicht.

Die Antwort, die den Violation-Zähler erwähnt, ist falsch, weil im *shutdown*-Modus der Zähler nicht mehr weiterzählt, sobald sich das Interface im *secure-shutdown*-Modus befindet. Er wird auf 0 zurückgesetzt, wenn das Interface mit den nacheinander abgesetzten Befehlen **shutdown** und **no shutdown** zurückgesetzt wird.

**8.** D. Der Befehl **show interface switchport** listet für einen Switch den konfigurierten Wert des Befehls **switchport mode** im administrativen Modus auf und teilt uns hier mit, dass SW1 den Konfigurationsbefehl **switchport mode trunk** verwendet. Der operative Status zeigt den aktuellen Funktionsstatus (*trunk*). Bei den vier Antworten wird in einer fälschlicherweise behauptet, dass der operative Status von SW2 ebenfalls *trunk* lauten muss, aber es ist möglich, dass der eine Switch Trunking einsetzt und ein anderer nicht. In einer anderen Antwort wird behauptet, der administrative Modus müsse *trunk* sein, was im Grunde bedeutet, dass der Befehl **switchport mode trunk** verwendet werden muss. Jedoch gibt es bei SW2 ein paar andere Konfigurationsoptionen, die funktionieren würden, z. B. die Befehle **switchport mode dynamic desirable** und **switchport mode dynamic auto**. Die richtige Antwort nennt auch einen der beiden Befehle (nämlich **switchport mode dynamic auto**).

## Kapitel 13

**1.** B und D. Um zu bestimmen, ob sich die Interfaces von zwei Geräten im gleichen Subnetz befinden sollten, lautet die allgemeine Regel, ob die beiden Interfaces durch einen Router voneinander getrennt sind. Damit Hosts in einem VLAN Daten an Hosts in anderen VLANs senden können, muss ein lokaler Router über sein LAN-Interface mit dem gleichen VLAN wie die Hosts verbunden sein und über eine Adresse im gleichen Subnetz wie die Hosts verfügen. Alle Hosts im gleichen VLAN auf dem gleichen Switch sind dann nicht durch einen Router voneinander getrennt, also befinden sich diese Hosts ebenfalls im gleichen Subnetz. Doch bei einem anderen PC, der mit dem gleichen Switch verbunden ist, sich aber in einem anderen VLAN befindet, müssen die Pakete den Router passieren, damit sie Host A erreichen. Also muss die IP-Adresse von Host A verglichen mit diesem neuen Host in einem anderen Subnetz sein.

**2.** D. Der Definition zufolge dürfen in allen IPv4-Subnetzen zwei bestimmte Adressen nie als IPv4-Hostadressen verwendet werden: der erste (niedrigste) numerische Wert im Subnetz für die Subnetz-ID sowie der letzte (höchste) numerische Wert im Subnetz für die Subnetz-Broadcast-Adresse.

**3.** B und C. Es werden mindestens sieben Subnetzbits benötigt, weil $2^6 = 64$. Also kann man mit sechs Subnetzbits keine 100 verschiedenen Subnetze nummerieren. Mit sieben Subnetzbits geht das, da $2^7 = 128 \geq 100$. Entsprechend reichen sechs Hostbits nicht, weil $2^6 - 2 = 62$, aber sieben Hostbits sind genug, da $2^7 - 2 = 126 \geq 100$.

Die Netzwerk-, Subnetz- und Hostbits müssen zusammen 32 Bits ergeben, also ist eine der Antworten verkehrt. Die Antwort mit den acht Netzwerkbits kann nicht korrekt sein, weil in der Frage von einem Klasse-B-Netzwerk die Rede ist. Also müssen immer insgesamt

16 Netzwerkbits vorhanden sein. Die beiden korrekten Antworten haben 16 Netzwerkbits (die sind auch erforderlich, denn in der Frage wird ja ein Klasse-B-Netzwerk vorausgesetzt) und jeweils mindestens sieben Subnetz- und sieben Hostbits.

4. A und C. Die privaten IPv4-Netzwerke, die in RFC 1918 definiert werden, sind das Klasse-A-Netzwerk 10.0.0.0, die 16 Klasse-B-Netzwerke von 172.16.0.0 bis 172.31.0.0 und die 256 Klasse-C-Netzwerke, die mit 192.168 beginnen.
5. A, D und E. Die privaten IPv4-Netzwerke, die in RFC 1918 definiert werden, sind das Klasse-A-Netzwerk 10.0.0.0, die 16 Klasse-B-Netzwerke von 172.16.0.0 bis 172.31.0.0 und die 256 Klasse-C-Netzwerke, die mit 192.168 beginnen. Die drei korrekten Antworten stammen aus dem Bereich der öffentlichen IP-Netzwerke und von denen ist kein Wert reserviert.
6. A und C. Ein nicht in Subnetze unterteiltes Klasse-A-, -B- oder -C-Netzwerk besteht aus zwei Teilen: dem Netzwerk- und dem Hostanteil.
7. B. Ein nicht in Subnetze unterteiltes Klasse-A-, -B- oder -C-Netzwerk besteht aus zwei Teilen: dem Netzwerk- und dem Hostanteil. Für das Subnetting erstellt der Techniker einen neuen Subnetzanteil, indem er sich bei den Hostbits bedient und somit deren Zahl verringert. Der Subnetzanteil der Adressstruktur existiert erst, wenn der Techniker eine nicht standardkonforme Maske wählt. Der Netzwerkanteil verbleibt in einer konstanten Größe.

## Kapitel 14

1. B und C. Bei Klasse-A-Netzwerken ist das erste Oktett im Bereich 1 bis 126 inklusive und deren Netzwerk-IDs haben eine 0 in den letzten drei Oktetten. 130.0.0.0 ist eigentlich ein Klasse-B-Netzwerk (mit dem ersten Oktett aus dem Bereich 128 bis 191 inklusive). Alle mit 127 beginnenden Adressen sind reserviert und somit ist 127.0.0.0 kein Klasse-A-Netzwerk.
2. E. Klasse-B-Netzwerke beginnen in den ersten Oktetten immer mit Werten zwischen 128 und 191 inklusive. Die Netzwerk-ID hat einen beliebigen Wert aus dem Bereich 128 bis 191 im ersten Oktett sowie einen beliebigen Wert zwischen 0 und 255 inklusive im zweiten Oktett. In den beiden letzten Oktetten stehen dezimale Nullen. Bei zwei Antworten steht im zweiten Oktett 255, was akzeptabel ist. Bei zwei Antworten steht im zweiten Oktett 0 und auch das ist akzeptabel.
3. B und D. Das erste Oktett (172) befindet sich im Bereich der Werte für Klasse-B-Adressen (128 – 191). Infolgedessen kann die Netzwerk-ID durch Kopieren der ersten beiden Oktette (172.16) geformt werden und dann werden für die beiden letzten Oktette Nullen geschrieben (172.16.0.0). Die Standardmaske für alle Klasse-B-Netzwerke lautet 255.255.0.0 und die Zahl der Hostbits in allen nicht in Subnetze aufgeteilten Klasse-B-Netzwerken beträgt 16.
4. A und C. Das erste Oktett (192) befindet sich im Bereich der Werte für Klasse-C-Adressen (192 – 223). Infolgedessen kann die Netzwerk-ID durch Kopieren der ersten drei Oktette (192.168.6) geformt werden und dann wird für das letzte Oktett eine Null geschrieben (192.168.6.0). Die Standardmaske für alle Klasse-C-Netzwerke lautet 255.255.255.0 und die Zahl der Hostbits in allen nicht in Subnetze aufgeteilten Klasse-C-Netzwerken beträgt 8.
5. D. Um die Netzwerk-Broadcast-Adresse zu finden, bestimmen Sie zuerst die Klasse und dann die Zahl der Hostoktette. Dann konvertieren Sie die Hostoktette in 255, um die Broadcast-Adresse des Netzwerks zu erstellen. In diesem Fall befindet sich 10.1.255.255 in einem Klasse-A-Netzwerk und die letzten drei Oktette sind die Hostoktette, was die Netzwerk-Broadcast-Adresse 10.255.255.255 ergibt. Bei 192.168.255.1 handelt es sich um

eine Klasse-C-Adresse, das letzte Oktett ist der Hostanteil, was zur Netzwerk-Broadcast-Adresse 192.168.255.255 führt. Die Adresse 224.1.1.255 ist eine Klasse-D-Adresse und befindet sich somit in keinem Unicast-IP-Netzwerk. Also trifft die Frage hierauf nicht zu. Bei 172.30.255.255 haben wir eine Klasse-B-Adresse, die letzten beiden Oktette sind die Hostoktette und wir bekommen die Netzwerk-Broadcast-Adresse 172.30.255.255.

## Kapitel 15

1. C. Wenn man an die Konvertierung von jeweils einem Oktett denkt, dann werden die ersten beiden Oktette jeweils in acht binäre Einsen konvertiert. 254 wird in die 8-Bit-Binärzahl 11111110 konvertiert und die dezimale 0 in die 8-Bit-Binärzahl 00000000. Also ergibt die Gesamtzahl der binären Einsen (die die Präfixlänge definieren) 8 + 8 + 7 + 0 = /23.
2. B. Wenn man an die Konvertierung von jeweils einem Oktett denkt, dann werden die ersten drei Oktette jeweils in acht binäre Einsen konvertiert. 240 wird in die 8-Bit-Binärzahl 11110000 konvertiert. Also ergibt die Gesamtzahl der binären Einsen (die die Präfixlänge definieren) 8 + 8 + 8 + 4 = /28.
3. B. /30 ist das Äquivalent der Maske, die 30 binäre Einsen aufweist. Um den Wert ins DDN-Format zu konvertieren, schreiben Sie alle binären Einsen (in diesem Fall 30) und dann die binären Nullen für den Rest der 32-Bit-Maske auf. Dann nehmen Sie jeweils acht Bits auf einmal und konvertieren sie von binär in dezimal (oder merken sich die neun möglichen Werte im DDN-Format für die Maskenoktette und deren binäre Entsprechung). Mit /30 für die Maske in dieser Frage führt das zur binären Maske 11111111 11111111 11111111 11111100. Alle drei ersten Oktette bestehen aus binären Einsen und werden somit alle in 255 konvertiert. Das letzte Oktett 11111100 wird in 252 konvertiert, alles zusammen ergibt die DDN-Maske 255.255.255.252. Eine Umwandlungstabelle finden Sie in Anhang A, »Numerische Referenztabellen«.
4. C. Der Netzwerkanteil ist je nachdem, ob sich die Adresse in einem Klasse-A-, -B- oder -C-Netzwerk befindet, immer entweder 8, 16 oder 24 Bits groß. Als Klasse-A-Adresse ist N = 8. Die Maske 255.255.255.0 ist – ins Präfixformat konvertiert – /24. Die Zahl der Subnetzbits ist die Differenz zwischen der Präfixlänge (24) und N, also in diesem Fall S = 16. Die Länge des Hostanteils ist jene Zahl, durch die Sie mit Addieren zur Präfixlänge (24) auf 32 kommen, also in diesem Fall H = 8.
5. A. Der Netzwerkanteil ist je nachdem, ob sich die Adresse in einem Klasse-A-, -B- oder -C-Netzwerk befindet, immer entweder 8, 16 oder 24 Bits groß. Bei Klasse-C-Adressen gilt: N = 24. Die Zahl der Subnetzbits ist die Differenz zwischen der Präfixlänge (27) und N, also in diesem Fall S = 3. Die Länge des Hostanteils ist jene Zahl, durch die Sie mit Addieren zur Präfixlänge (27) auf 32 kommen, also in diesem Fall H = 5.
6. D. Die Regeln für eine klassenlose Adressierung definieren eine zweiteilige Struktur für die IP-Adresse: den Präfix- und den Hostanteil. Diese Logik ignoriert die Klasse-A-, -B- und -C-Regeln und kann aus jeder beliebigen Adressklasse auf die 32 Bit langen IPv4-Adressen angewendet werden. Durch das Ignorieren der Klasse-A-, -B- und -C-Regeln ignoriert die klassenlose Adressierung jede vordefinierte Unterscheidung beim Netzwerkanteil einer IPv4-Adresse.
7. A und B. Die Masken in binärer Form definieren eine Zahl mit binären Einsen und die Zahl der binären Einsen definiert die Länge des Präfixteils (Netzwerkanteil plus Subnetzanteil). Bei einem Klasse-B-Netzwerk hat der Netzwerkanteil 16 Bits. Um 100 Subnetze zu unter-

stützen, muss der Subnetzanteil mindestens sieben Bit lang sein. Sechs Subnetzbits ergäben nur $2^6$ = 64 Subnetze, während sieben Subnetzbits zu $2^7$ = 128 Subnetzen führen. Die /24-Antwort liefert acht Subnetzbits und die 255.255.255.252-Antwort 14 Subnetzbits.

## Kapitel 16

1. D. Wenn man nach Konzepten der klassenbezogenen IP-Adressierung arbeitet, wie sie in Kapitel 15, »Subnetzmasken analysieren«, beschrieben werden, bestehen Adressen aus drei Teilen: dem Netzwerk-, dem Subnetz- und dem Hostanteil. Für Adressen in einem klassenbezogenen Netzwerk muss der Netzwerkanteil für die Nummern, die im gleichen Netzwerk sind, identisch sein. Für Adressen im gleichen Subnetz muss der Wert für Netzwerk- und Subnetzanteil identisch sein. Der Hostanteil unterscheidet sich, wenn man verschiedene Adressen im gleichen Subnetz vergleicht.
2. B und D. In jedem Subnetz ist die Subnetz-ID die kleinste Zahl aus dem Bereich und die Broadcast-Adresse des Subnetzes die größte und dazwischen befinden sich die verwendbaren IP-Adressen. Alle Nummern in einem Subnetz haben identische binäre Werte im Präfixteil (klassenlose Sichtweise) sowie im Netzwerk- plus Subnetzanteil (klassenbezogene Sichtweise). Damit die Subnetz-ID die niedrigste Zahl ist, muss sie den kleinsten möglichen binären Wert im Hostanteil aufweisen (nur Nullen). Damit die Broadcast-Adresse die größte Zahl ist, muss sie den größtmöglichen binären Wert im Hostanteil aufweisen (nur binäre Einsen). Zu den verwendbaren Adressen gehören weder Subnetz-ID noch Broadcast-Adresse des Subnetzes. Also bestehen die Adressen im Bereich der verwendbaren IP-Adressen im Hostanteil nie nur aus Nullen oder nur aus Einsen.
3. C. Die Maske wird in 255.255.255.0 konvertiert. Um die Subnetz-ID für jedes Oktett der Maske, das 255 lautet, zu finden, können Sie die korrespondierenden Werte der IP-Adresse kopieren. Für Maskenoktette mit dem Dezimalwert 0 können Sie eine 0 in diesem Oktett der Subnetz-ID schreiben. Von daher kopieren Sie die 10.7.99 und schreiben für das vierte Oktett eine 0, was die Subnetz-ID 10.7.99.0 ergibt.
4. C. Erstens muss das zugehörige Subnetz (also die ID des Subnetzes, in dem die Adresse sich befindet) numerisch kleiner sein als die IP-Adresse, wodurch eine der Antworten bereits entfällt. Die Maske wird in 255.255.255.252 konvertiert. Von daher können Sie die ersten drei Oktette der IP-Adresse wegen ihres Werts 255 kopieren. Beim vierten Oktett muss der Wert der Subnetz-ID ein Vielfaches von 4 sein, weil 256 – 252 (Maske) = 4. Zu diesen Vielfachen gehören auch 96 und 100 und die richtige Wahl ist das Vielfache, das am dichtesten am Wert der IP-Adresse in diesem Oktett (97) liegt, ohne ihn zu überschreiten. Also lautet die korrekte Subnetz-ID 192.168.44.96.
5. C. Die ID des zugehörigen Subnetzes ist in diesem Fall 172.31.77.192. Sie finden, basierend auf Subnetz-ID und Maske, anhand verschiedener Methoden die Broadcast-Adresse des Subnetzes. Wenn Sie dem dezimalen Prozess des Buchs folgen, wird die Maske in 255.255.255.224 konvertiert, wodurch Oktett 4 zum interessanten Oktett wird und die Magic Number 256 – 224 = 32 lautet. Für die drei Oktette mit der Maske 255 kopieren Sie die Subnetz-ID (172.31.77). Addieren Sie beim interessanten Oktett den Wert der Subnetz-ID (192) zur Magic Number (32) hinzu und ziehen Sie 1 ab, was 223 ergibt. Wir erhalten als Subnetz-Broadcast-Adresse also 172.31.77.223.
6. C. Zur Beantwortung dieser Frage müssen Sie den Adressbereich des Subnetzes herausfinden, was üblicherweise bedeutet, die Subnetz-ID und die Broadcast-Adresse des Sub-

netzes zu berechnen. Bei einer Subnetz-ID und Maske von 10.1.4.0/23 wird die Maske in 255.255.254.0 konvertiert. Um die Broadcast-Adresse des Subnetzes zu finden (dem in diesem Kapitel beschriebenen dezimalen Prozess zufolge), können Sie die ersten beiden Oktette der Subnetz-ID kopieren, weil der Wert der Maske in jedem Oktett 255 lautet. Sie schreiben 255 ins vierte Oktett, weil die Maske eine 0 im vierten Oktett aufweist. Im (interessanten) Oktett 3 addieren Sie die Magic Number (2) zum Wert der Subnetz-ID (4) und subtrahieren 1, was 2 + 4 – 1 = 5 ergibt. (Die Magic Number in diesem Fall wird mit 256 – 254 = 2 berechnet.) So ermitteln Sie 10.1.5.255 als Broadcast-Adresse. Die letzte verwendbare Adresse ist um 1 kleiner: 10.1.5.254. Der Bereich, der die letzten 100 Adressen enthält, lautet 10.1.5.155 bis 10.1.5.254.

## Kapitel 17

1. B und E. Cisco-Router verfügen über einen Ein-/Aus-Schalter, aber Cisco-Switches generell nicht.
2. A. Sowohl Switches als auch Router konfigurieren IP-Adressen, also kann man die Befehle **ip address** *adressmaske* und **ip address dhcp** für Router und Switches verwenden. Der Befehl **interface vlan 1** kann nur auf Switches angewendet werden.
3. B und D. Um Pakete weiterzuleiten, muss ein Router-Interface eine IP-Adresse zugewiesen bekommen haben und sich im Interfacestatus *up/up* befinden. Um eine serielle Verbindung in einem Lab zu erstellen, ohne CSU/DSUs einzusetzen, muss ein Router mit dem Befehl **clock rate** auf die Datenrate der Verbindung konfiguriert werden. Die Befehle **bandwidth** und **description** sind nicht erforderlich, um eine Verbindung funktionsfähig zu machen.
4. C. Wenn der erste der beiden Statuscodes *down* lautet, bedeutet das typischerweise, dass es ein Problem auf Layer 1 gibt (z. B. ist das physische Kabel möglicherweise nicht mit dem Interface verbunden).
5. C und E. Der Befehl **show ip interface brief** listet alle IPv4-Interfaceadressen auf, aber keine der Masken. Der Befehl **show version** listet weder IP-Adressen noch Masken auf. Die anderen drei Befehle führen sowohl Adresse als auch Maske auf.
6. B. Ein Router hat eine IPv4-Adresse für jedes verwendete Interface, wogegen ein LAN-Switch nur eine IPv4-Adresse aufweist, die lediglich für den Zugriff auf diesen Switch verwendet wird. Die restlichen Antworten listen Konfigurationseinstellungen auf, die die gleichen Konventionen für Router und Switches verwenden.

## Kapitel 18

1. B. PCs arbeiten nach einer Logik mit zwei Optionen: Sende lokale Pakete (die für Hosts im gleichen Subnetz bestimmt sind) direkt und sende Remote-Pakete (die für Hosts in anderen Subnetzen gedacht sind) an das Default-Gateway. In diesem Fall lautet die eigene IP-Adresse des PCs 192.168.4.77 mit der Maske 255.255.255.224, also befindet sie sich in Subnetz 192.168.4.64/27. Dieses Subnetz hat einen Adressbereich von 192.168.4.64 bis 192.168.4.95, einschließlich der Subnetz- und der Broadcast-Adresse. Infolgedessen sendet der PC das Paket an sein Default-Gateway. Was die anderen falschen Antworten angeht: Wenn beim Befehl **ping** ein Hostname verwendet worden wäre, hätte zuerst ein DNS-Server den Namen auflösen müssen. Außerdem hat der PC bereits eine IP-Adresse und deswegen wäre DHCP gar nicht nötig.

2. A und C. Die Route definiert die Gruppe der Adressen, die durch die Route anhand von Subnetz-ID und Maske repräsentiert wird. Der Router kann diese Zahlen verwenden, um den Adressbereich zu ermitteln, der zu dieser Route passt. Die anderen beiden Antworten zeigen Fakten, die hilfreich sind, wenn man Pakete weiterleiten will, die zur Route passen.
3. A und F. Von allen aufgeführten Befehlen handelt es sich nur bei den beiden richtigen Antworten um syntaktisch korrekte Befehle für die Router-Konfiguration. Der Befehl zum Aktivieren des 802.1Q-Trunkings lautet **encapsulation dot1q** *vlan-id*.
4. C. Die Konfiguration des Routing-Features des Layer-3-Switches verwendet VLAN-Interfaces, wobei die Interfacenummer zur VLAN-ID passt. Die passenden direkt angeschlossenen Routen werden dann – wie alle direkt angeschlossenen IP-Routen – die Interfaces auflisten, aber keine Next-Hop-IP-Adresse. Die drei direkt angeschlossenen Routen werden die VLAN-Interfaces 1, 2 bzw. 3 auflisten.
5. C. Der Befehl **ip route** kann wahlweise direkt die IP-Adresse des Next-Hop-Routers oder aber das Interface des lokalen Routers angeben. Er gibt zudem die Subnetz-ID und die passende Subnetzmaske an und definiert den zur Route passenden Adressbereich.
6. Die korrekte Syntax gibt eine Subnetzadresse und dann eine Subnetzmaske im punktgetrennten Dezimalformat an. Darauf folgt entweder ein ausgehendes Interface oder die IP-Adresse des nächsten Hops.
7. B. Der Befehl **ip route** kann ein ausgehendes Interface oder eine Next-Hop-Adresse angeben, wodurch eine Antwort bereits ausgeschlossen werden kann. Der Befehl verwendet auch die korrekte Syntax, weswegen eine weitere Antwort entfällt. Es besteht im Zusammenhang mit der Konfiguration des Befehls **ip route** keine Notwendigkeit für einen Router, bestimmte Interface-IP-Adressen zu verwenden, und damit kommt auch eine weitere Antwortoption nicht mehr infrage.

   Bei der Analyse eines neuen **ip route**-Befehls überprüft das IOS beispielsweise, ob das ausgehende Interface den Status *up/up* hat, die Next-Hop-Adresse erreichbar ist und, wenn es eine konkurrierende Route aus einer anderen Quelle gibt, diese eine bessere administrative Distanz aufweist.

## Kapitel 19

1. A und D. RIPv2 bietet viele interne Merkmale, z. B. die Anzahl der Hops als Metrik und Split-Horizon als Möglichkeit zur Vermeidung von Routing-Loops. RIPv2 sendet seine Updates an die Multicast-IP-Adresse 224.0.0.9. Ferner sendet das Protokoll regelmäßig vollständige Routing-Updates – und zwar auch bei stabilem Netzwerk.
2. B. Bei der von RIP verwendeten Metrik werden Router als »Hops« bezeichnet. Damit fallen bereits drei Antworten weg. Aus Sicht eines Routers mit einer RIP-Route umfasst die Anzahl der Hops alle Router zwischen ihm und dem Zielsubnetz, nicht aber den lokalen Router selbst. Nehmen wir beispielsweise an, eine Route auf R1 führe in ein bestimmtes Subnetz und diese Route hat die Metrik 2. Dies wäre der Fall, wenn der Ende-zu-Ende-Pfad von R1 in das Subnetz bei R1 beginnt und dann über R2 und R3 bis zur direkten Anbindung in das Subnetz verläuft.
3. A, C und E. Der RIPv2-Befehl **network** gibt das klassenbezogene Netzwerk (also das Klasse-A-, -B- oder -C-Netzwerk), in dem eine Interfaceadresse vorhanden ist, statt der Subnetznummer oder der Interfaceadresse an. Insofern sind die beiden **network**-Befehle, die die Klasse-A-Netzwerke 10.0.0.0 und 11.0.0.0 benennen, korrekt. Außerdem verwendet

RIP den globalen Befehl **router rip** ohne weiteren Parameter, um den Benutzer in den RIP-Konfigurationsmodus zu versetzen, damit er dort **network**-Befehle konfigurieren kann.

4. A. Der RIPv2-Befehl **network** gibt das klassenbezogene Netzwerk (also das Klasse-A-, -B- oder -C-Netzwerk), in dem eine Interfaceadresse vorhanden ist, statt der Subnetznummer oder der Interfaceadresse an. Der Befehl **network 10.0.0.0** aktiviert RIP auf allen Interfaces auf dem lokalen Router, die Adressen im Netzwerk 10.0.0.0 haben.

5. B und C. Die Antworten geben verschiedene Zahlen an, die in der Ausgabezeile aufgeführt sind. Die beiden Zahlen in Klammern – 120 und 1 – benennen die administrative Distanz bzw. die Metrik. Die Angabe von 13 Sekunden (im Zähler *00:00:13*) bezieht sich auf den Zähler, der angibt, wann der Router zuletzt von einem benachbarten RIP-Router Informationen zu dieser Route erhalten hat. Allerdings kann die Route durchaus schon vor deutlich längerer Zeit hinzugefügt worden sein: Der Timer bezeichnet die seit dem letzten Update und nicht die seit dem Hinzufügen der Route zur Routing-Tabelle des lokalen Routers verstrichene Zeit.

6. C und D. Die Ausgabe zeigt uns die folgende Konfiguration: **router rip**, **maximum-paths 5**, **passive-interface gigabitethernet0/1**, **network 192.168.1.0**, **network 192.168.5.0** und **no auto-summary**.

7. A. Von den vier Antwortoptionen ist diejenige die falsche, bei der die Routing-Informationen nur in einer Richtung ausgetauscht werden. In diesem Fall gibt R2 als passiver Router keine Routen gegenüber R1 bekannt, d. h., R1 erlernt keine Routen. R2 hingegen erlernt weiter Routen.

   Zwei falsche Antworten erwähnen Probleme, die dazu führen würden, dass beide Router keine Routen mehr voneinander erlernen. Die Antwort mit den IP-Adressen in den unterschiedlichen Subnetzen führt dazu, dass beide Router die RIP-Updates des jeweils anderen ignorieren würden. Die Antwort zum fehlenden **network**-Befehl auf R1 bedeutet, dass R1 weder Updates senden noch über sein Interface G0/0 eingehende Updates verarbeiten würde, weswegen R1 und R2 hier nichts voneinander lernen könnten. Bei der Antwort schließlich, die den Befehl **no auto-summary** nennt, würde das Erlernen von Routen durch einen Router nicht unterbunden, sondern lediglich Auswirkungen darauf haben, welche Routen ein Router bekanntgeben würde.

## Kapitel 20

1. B und D. Der Client sendet eine Discover-Nachricht und der Server antwortet mit einer Offer-Nachricht. Dann sendet der Client einen Request und der Server schickt in der Acknowledgment-Nachricht die IP-Adresse zurück.

2. E. Bei den Antworten werden drei syntaktisch korrekte Befehle aufgelistet, aber eine ist verkehrt: **ip dhcp-server 10.1.10.1**. Die Antwort mit diesem Befehl ist falsch. Der Befehl **ip helper-address 10.1.10.1** wird tatsächlich als Interfacesubbefehl gebraucht, aber nur bei Remote-Routern wie dem Boston-Router. Dieser Befehl ist für den DNS-Server nicht erforderlich. Zwar wird der Befehl **ip helper-address 10.1.10.2** akzeptiert, er ist aber für die Arbeit mit DNS oder DHCP nicht hilfreich. Der Befehl **ip name-server 10.1.10.2** schließlich funktioniert beim Atlanta-Router, aber damit können Benutzer des CLI des Atlanta-Routers nur den DNS-Server nutzen, er wirkt sich nicht auf den DNS-Traffic der Benutzer aus.

   Der Boston-Router würde den Befehl **ip helper-address 10.1.10.1** brauchen, um DHCP-Anforderungen an den DHCP-Server in Atlanta zu senden.

3. B. Die Konfiguration legt die auf Clients bezogenen Einstellungen in einem DHCP-Pool ab: Client-IP-Adresse, Maske, Default-Router und die IP-Adressen der DNS-Server. Im Pool wird auch die Lease-Dauer der Adresse für den Client aufgelistet. Nur die Exclude-Liste (**ip dhcp exclude-address**) befindet sich außerhalb des DHCP-Pools.

4. B. Ist einem Host keine IPv4-Adresse zugewiesen, dann sollte der erste Schritt darin bestehen, eine solche Adresse per DHCP anzufordern. Am Anfang der Frage könnte man den Eindruck gewinnen, als wäre dieser Vorgang bereits abgeschlossen und sonst wäre noch nichts im Netzwerk passiert. Diese Aussage soll eigentlich bedeuten, dass keine ARPs und keine DNS-Nachrichten übertragen wurden – und Benutzernachrichten schon gar nicht!

   Wenn der Benutzer **www.ciscopress.com** in seinem Browserfenster eingibt, muss PC1 den Namen zunächst einmal in die zugehörige IPv4-Adresse auflösen. Allerdings befindet sich der DNS-Server (10.9.9.9) in einem ganz anderen Subnetz. PC1 erlernt während des DHCP-Prozesses keinen ARP-Eintrag für den Default-Router. (Zur Erinnerung: Alle von diesem DHCP-Client versendeten DHCP-Nachrichten werden nicht an die MAC-Adresse des Routers versendet.) Folglich gilt: Auch wenn der nächste wichtige Schritt für PC1 darin besteht, den Namen *www.ciscopress.com* aufzulösen und die zugehörige IP-Adresse zu erlernen, ist die tatsächlich nächste von ihm versendete Nachricht ein ARP-Request. So erlernt PC1 die MAC-Adresse von R1 und kann den DNS-Request dann an R1 weiterleiten.

   Was die falschen Antworten angeht, versendet PC1 nach dem ARP-Request zur Ermittlung der MAC-Adresse des Default-Routers einen DNS-Request und schließlich ein IP-Paket an die IP-Adresse des Servers. Und wenn der Server sich tatsächlich im selben Subnetz wie PC1 befinden sollte, würde PC1 zum Ermitteln der IP-Adresse des Servers ebenfalls ARP nutzen.

5. C. Definitionsgemäß wird ein Subnetz-Broadcast (also ein an die Subnetz-Broadcast-Adresse gesendetes Paket) – auch Directed-Broadcast genannt – wie jedes andere Paket geroutet, bis es bei einem Router eintrifft, der mit dem betreffenden Subnetz verbunden ist. Für den letzten Weiterleitungsschritt kapselt der Router das IP-Paket in einen Ethernet-Broadcast-Frame mit der Empfänger-MAC-Adresse FFFF.FFFF.FFFF, damit alle Hosts im Zielsubnetz eine Kopie des Pakets erhalten.

   Ein Unicast-Paket würde im letzten Schritt nicht als Data-Link-Broadcast weitergeleitet werden.

   Ein Netzwerk-Broadcast würde von verschiedenen Routern nach Bedarf repliziert werden, um dann in alle Subnetze im klassenbezogenen Netzwerk übermittelt zu werden.

   Ein Multicast-Paket schließlich würde an einen Teil der Subnetze abhängig davon zugestellt, welche Subnetze Hosts enthalten, die zuvor den Empfang von Paketen angefordert haben, die an die betreffende Multicast-Adresse gesendet werden.

6. D. Definitionsgemäß wird ein Multicast-IP-Paket (also ein an eine Klasse-D-IP-Multicast-Adresse gesendetes Paket) nach Bedarf von Routern kopiert werden, um dann in Kopie nach Bedarf an mehrere, aber nicht alle Router weitergeleitet zu werden. Die Logik steht im Zusammenhang mit dem vorherigen Wissen eines Hostregistrierungsprozesses, bei dem Hosts ihr Interesse äußern, Pakete zu erhalten, die an eine bestimmte Multicast-IP-Adresse gesendet werden. Router tauschen diese Informationen aus, damit sie beim Eintreffen eines neuen Multicast-Pakets wissen, wohin Kopien dieses Multicast-Pakets gesendet werden müssen – und wohin nicht (weil sich keine Hosts in diesem Teil des Netzwerks für den Empfang einer Kopie registriert haben).

Ein Unicast-Paket würde im letzten Schritt nicht als Data-Link-Broadcast weitergeleitet werden.

Ein Netzwerk-Broadcast würde von verschiedenen Routern nach Bedarf repliziert werden, um dann in alle Subnetze im klassenbezogenen Netzwerk übermittelt zu werden.

Ein Subnetz-Broadcast würde als einzelnes Paket an den letzten Router im Pfad übermittelt. Dieser Router würde das betreffende IP-Paket dann als LAN-Broadcast weiterleiten, damit alle Hosts in diesem Subnetz eine Kopie erhalten.

## Kapitel 21

**1.** A. Bei einem 50-prozentigen Wachstum muss die Maske genug Subnetzbits definieren, um 150 Subnetze zu erstellen. Infolgedessen braucht die Maske mindestens acht Subnetzbits (sieben Subnetzbits ergeben $2^7$ oder 128 Subnetze und acht Subnetzbits ergeben $2^8$ oder 256 Subnetze). Entsprechend bedeutet der Bedarf für ein 50-prozentiges Wachstum bei der Größe des größten Subnetzes, dass der Hostanteil genug Bits benötigt, um 750 Hosts pro Subnetz bereitstellen zu können. Neun Hostbits reichen nicht ($2^9 - 2 = 510$), aber zehn Hostbits ergeben 1022 Hosts pro Subnetz ($2^{10} - 2 = 1022$). Weil wegen der Wahl eines Klasse-B-Netzwerks 16 Netzwerkbits existieren, benötigt das Design (mindestens) 34 Bits insgesamt in der Maske (16 Netzwerk-, acht Subnetz- und zehn Hostbits), aber es existieren nur 32 Bits – und somit erfüllt keine Maske die Anforderungen.

**2.** B. Bei einem Wachstum von 20 Prozent muss das Design 240 Subnetze unterstützen. Sieben Subnetzbits erfüllen diesen Bedarf nicht ($2^7 = 128$), aber bei acht Subnetzbits ist das der Fall ($2^8 = 256$). Entsprechend wäre die kleinste Zahl für Hostbits dann acht, weil es nach einem 20-prozentigen Wachstum 144 Hosts pro Subnetz gäbe. Diese Zahl erfordert acht Hostbits ($2^8 - 2 = 254$). Diese Zahlen sind das Minimum für die Subnetz- und Hostbits.

Die richtige Antwort lautet 10.0.0.0/22 und hat acht Netzwerkbits, weil es sich bei der Netzwerkklasse um ein Klasse-A-Netzwerk handelt, 14 Subnetzbits (/22 – 8 = 14) und zehn Hostbits (32 – 22 = 10). Diese Maske sorgt für mindestens acht Subnetz- und acht Hostbits. Die Masken in den anderen Antworten unterstützen entweder nicht mindestens acht Hostbits oder mindestens acht Subnetzbits.

**3.** B. Um 1000 Subnetze zu unterstützen, werden zehn Subnetzbits ($2^{10} = 1024$) benötigt. Das Design verwendet ein Klasse-B-Netzwerk, was bedeutet, dass auch 16 Netzwerkbits vorhanden sind. Also ist 255.255.255.192 oder /26 die kürzeste Maske, die die Anforderungen erfüllt, und sie setzt sich aus 16 Netzwerk- plus zehn Subnetzbits zusammen. Die Antwort mit /28 liefert ebenfalls anforderungsgerecht ausreichend Subnetze, aber verglichen mit /26 bietet /28 weniger Hostbits und somit weniger Hosts pro Subnetz.

**4.** C und D. Die Maske wird in 255.255.252.0 konvertiert und somit ist die Differenz zwischen den Subnetz-IDs (in diesem Kapitel als Magic Number bezeichnet) 256 – 252 = 4. Die Subnetz-IDs starten also bei 172.30.0.0, dann 172.30.4.0 und dann 172.30.8.0 usw. (im dritten Oktett um 4 hochgezählt). Die Maske impliziert in Verwendung mit einem Klasse-B-Netzwerk sechs Subnetzbits und ergibt insgesamt 64 Subnetz-IDs. Die letzte davon, 172.30.252.0, kann leicht erkannt werden, weil das dritte Oktett, in dem sich die Subnetzbits befinden, den gleichen Wert hat wie die Maske in diesem dritten Oktett.

**5.** A. Die erste (numerisch kleinste) Subnetz-ID ist die gleiche Adresse wie die des klassenbezogenen Netzwerks, also 192.168.9.0. Die verbleibenden Subnetz-IDs sind jeweils um 8

größer als die vorangegangene Subnetz-ID in der Sequenz, also 192.168.9.8, 192.168.9.16, 192.168.9.24, 192.168.9.32 usw. bis hin zu 192.168.9.248.

6. D. Bei Verwendung der Maske /24 (255.255.255.0) werden die Subnetz-IDs im dritten Oktett um 1 inkrementiert. Das liegt daran, dass in einem Klasse-B-Netzwerk 16 Netzwerkbits existieren, und mit der Maske /24 sind die nächsten acht Bits Subnetzbits. Also enthält das gesamte dritte Oktett Subnetzbits. Alle Subnetz-IDs werden im letzten Oktett eine 0 haben, weil das gesamte vierte Oktett aus Hostbits besteht. Beachten Sie, dass 172.19.0.0 (das Nullsubnetz) und 172.19.255.0 (das Broadcast-Subnetz) vielleicht etwas komisch aussehen, aber gültige Subnetz-IDs sind.

## Kapitel 22

1. B, C und D. Klassenlose Routing-Protokolle unterstützen per Definition VLSM, weil sie die Subnetzmaske in ihren Routing-Updates übermitteln. Von den aufgeführten Antworten ist nur RIPv1 (RIP Version 1) kein klassenloses Routing-Protokoll.

2. A. Beachten Sie, dass VLSM manchmal auch für Variable-Length Subnet Masking steht; dieser Begriff bezeichnet den Prozess der Verwendung verschiedener Masken im selben klassenbezogenen Netzwerk, während Variable-Length Subnet Mask die Subnetzmaske selbst benennt.

3. A. Das Subnetz 10.5.0.0 255.255.240.0 impliziert den Bereich 10.5.0.0 bis 10.5.15.255, in dem keine Überschneidung auftritt. 10.4.0.0 255.254.0.0 impliziert den Bereich 10.4.0.0 bis 10.5.255.255, in dem eine Überschneidung vorhanden ist. 10.5.32.0 255.255.224.0 impliziert den Bereich 10.5.32.0 bis 10.5.63.255, in dem eine Überschneidung vorhanden ist. 10.5.0.0 255.255.128.0 impliziert den Bereich 10.5.0.0 bis 10.5.127.255, in dem eine Überschneidung vorhanden ist.

4. D. Die vier Antworten implizieren die folgenden Bereiche: 172.16.0.0/21: 172.16.0.0 – 172.16.7.255. 172.16.6.0/23: 172.16.6.0 – 172.16.7.255. 172.16.16.0/20: 172.16.16.0 – 172.16.31.255. 172.16.11.0/25: 172.16.11.0 – 172.16.11.127. Das Subnetz 172.16.8.0/22 aus der Frage impliziert einen Bereich von 172.16.8.0 bis 172.16.11.127, in dem der Nummernbereich in Subnetz 172.16.11.0/25 enthalten ist.

5. C. Die Frage listet drei vorhandene Subnetze auf, die zusammen Teile des Klasse-C-Netzwerks 192.168.1.0 bilden. Wenn man nur die letzten Oktettwerte auflistet, belegen diese Subnetze 0 bis 63, 128 bis 131 sowie 160 bis 167. Das neue Subnetz mit der Maske /28 braucht 16 fortlaufende Adressen und die Subnetznummern müssen im letzten Oktett alle Vielfache von 16 sein (0, 16, 32 usw.). Schaut man sich die verbrauchten Nummern erneut an, beginnt der erste freie Bereich bei 64 und verläuft bis 127. Also gibt es mehr als genug Kapazität für 16 Adressen. Folglich ist die numerisch kleinste Subnetznummer 192.168.1.64/28 und reicht von 192.168.1.64 bis 192.168.1.79.

## Kapitel 25

1. A und C. Standard-ACLs überprüfen die Absender-IP-Adresse. Der Adressbereich 10.1.1.1 bis 10.1.1.4 kann mit einer ACL verglichen werden, erfordert aber mehrere **access-list**-Befehle. Der Vergleich aller Hosts in Barneys Subnetz lässt mit dem Befehl **access-list 1 permit 10.1.1.0 0.0.0.255** durchführen.

2. A und D. Der Bereich gültiger ACL-Nummern für nummerierte Standard-IP-ACLs lautet 1 bis 99 und 1300 bis 1999 inklusive.
3. D. 0.0.0.255 entspricht allen Paketen, bei denen die ersten drei Oktette identisch sind. Dies ist nützlich, wenn Sie ein Subnetz vergleichen wollen, in dem der Subnetzanteil die ersten drei Oktette umfasst (wie es hier auch der Fall ist).
4. E. 0.0.15.255 entspricht allen Paketen, bei denen die ersten 20 Bits identisch sind. Dies ist nützlich, wenn Sie ein Subnetz vergleichen wollen, in dem der Subnetzanteil die ersten 20 Bits umfasst (wie es hier auch der Fall ist).
5. A. Der Router durchsucht die ACL-Anweisungen immer der Reihe nach und stoppt, sobald eine passende ACL-Anweisung gefunden wurde. Anders gesagt, er arbeitet nach der Logik der ersten Übereinstimmung. Ein Paket mit der Absender-IP-Adresse 1.1.1.1 würde zu allen drei in dieser Frage beschriebenen explizit konfigurierten Befehlen passen. Dementsprechend wird die erste Anweisung angewandt.
6. B. Eine falsche Antwort (die mit der Wildcard-Maske 0.0.255.0) passt zu allen Paketen, die mit 172.16 beginnen und eine 5 im letzten Oktett haben. Eine verkehrte Antwort passt nur zur spezifischen IP-Adresse 172.16.5.0. Eine unkorrekte Antwort verwendet die Wildcard-Maske 0.0.0.128, bei der es nur ein Wildcard-Bit (binär) gibt, und passt nur zu den Adressen 172.16.5.0 und 172.16.5.128. Die korrekte Antwort passt zum Adressbereich von 172.16.4.0 bis 172.16.5.255.

## Kapitel 26

1. E und F. Erweiterte ACLs können die Header von Layer 3 (IP) und Layer 4 (TCP, UDP) sowie einige andere überprüfen, nicht jedoch Informationen des Application Layer (Layer 5–7). Erweiterte ACLs mit Namen können dieselben Felder überprüfen wie nummerierte erweiterte ACLs.
2. A und E. Der korrekte Bereich der ACL-Nummern bei erweiterten IP-ACLs liegt zwischen 100 und 199 sowie zwischen 2000 und 2699. Die Antworten, die den Parameter **eq www** nach 10.1.1.1 angeben, entsprechen der Absenderportnummer und die Pakete fließen in Richtung des Webservers und nicht von ihm weg.
3. E. Weil das Paket in Richtung beliebiger Webclients übertragen wird, müssen Sie die Portnummer des Webservers als Absenderport überprüfen. Der Client-IP-Adressbereich ist in der Frage nicht angegeben, wohl aber die Server, d. h., die Absenderadresse, die mit 172.16.5 beginnt, ist die richtige Antwort.
4. A und C. Vor IOS 12.3 mussten, um eine Zeile aus einer ACL zu entfernen, nummerierte ACLs entfernt und dann neu konfiguriert werden. Seit IOS 12.3 können Sie auch den ACL-Konfigurationsmodus und Sequenznummern einsetzen, um jeweils eine ACL-Zeile zu löschen.
5. B und C. Ein Router umgeht die ACL-Logik für die eigenen ausgehenden ACLs bei Paketen, die von ihm selbst erstellt wurden. Bei eingehenden Paketen machen Router keine derartige Ausnahme. Folglich ist ACL B riskanter als ACL A, weil B als eingehende ACL aktiv ist.

   Der Befehl **ping 1.1.1.1** in zwei Antworten richtet sich an ein eigenes Ethernet-Interface des Routers. Deswegen würde der Router ausgehende ACL-Logik für dieses Interface ignorieren, eingehende ACL-Logik aber verarbeiten. Das bedeutet, dass Router R1 die Logik von ACL A umginge, weil diese als ausgehende ACL für das Interface G0/1 von R1 aktiv ist.

6. C und D. Die Befehle **show ip access-lists** und **show access-lists** zeigen beide die Konfiguration der IPv4-ACLs einschließlich der Zeilennummern an. Weder **show running-config** noch **show startup-config** listen diese ACL-Zeilennummern auf. Im vorliegenden Fall enthielte die *startup-config* überhaupt keine ACL-Konfiguration.

## Kapitel 27

1. D. Der ursprüngliche Zweck von CIDR bestand darin, die Routenzusammenfassung mehrerer Klasse-A-, -B- und -C-Netzwerke zu ermöglichen und so die Routing-Tabellen im Internet klein zu halten. Von den vorgeschlagenen Antworten fasst nur 200.1.0.0 255.255.0.0 mehrere Netzwerke zusammen.
2. B und E. RFC 1918 nennt die privaten Netzwerkadressen. Hierzu gehören das Klasse-A-Netzwerk 10.0.0.0, die Klasse-B-Netzwerke 172.16.0.0 bis 172.31.0.0 und die Klasse-C-Netzwerke 192.168.0.0 bis 192.168.255.0.
3. C. Bei statischer NAT werden die Einträge statisch konfiguriert. Da die Frage die Übersetzung für Inside-Adressen erwähnt, wird im Befehl das Schlüsselwort **inside** benötigt.
4. A. Bei dynamischer NAT werden die Einträge als Ergebnis des ersten Paketflusses aus dem Inside-Netzwerk erstellt.
5. A. Der Parameter **list 1** referenziert eine IP-ACL, die Pakete vergleicht und die Inside-Local-Adressen ermittelt.
6. A und C. In der Konfiguration fehlt das Schlüsselwort **overload** im Befehl **ip nat inside source** und im Interfacesubbefehl **ip nat outside** auf dem seriellen Interface.
7. B. Die letzte Zeile erwähnt, dass der Pool sieben Adressen enthält, die alle reserviert sind, und der Fehlschlagszähler steht kurz vor 1000, d. h., es wurden aufgrund fehlender Kapazität im NAT-Pool knapp tausend neue Datenströme abgewiesen.

## Kapitel 28

1. C. NAT war eine kurzfristige Abhilfe gegen die Verknappung der IPv4-Adressen. Die gilt vor allem für das PAT-Feature, mit dem viele Hosts private IPv4-Adressen nutzen können und dabei nur eine öffentliche IPv4-Adresse benötigen. IP Version 5 existierte kurz als experimentelles Protokoll und hatte nichts mit der Verknappung der IPv4-Adressen zu tun. IPv6 geht dieses Verknappungsproblem direkt an, ist aber eine langfristige Lösung. ARP hat keinerlei Einfluss auf die Zahl der verwendeten IPv4-Adressen.
2. A. Router verwenden die gleichen Prozessschritte wie bei IPv4-Paketen, wenn sie IPv6-Pakete weiterleiten. Router leiten IPv6-Pakete basierend auf den IPv6-Adressen weiter, die im IPv6-Header der IPv6-Pakete aufgeführt sind, indem sie die Empfänger-IPv6-Adresse mit der IPv6-Routing-Tabelle des Routers vergleichen. Als Folge davon verwirft der Router die im eingehenden Frame vorhandenen Data-Link-Header und -Trailer und übrig bleibt das IPv6-Paket. Der Router vergleicht die Empfänger-IPv6-Adresse (nicht die Absenderadresse) im Header mit seiner IPv6-Routing-Tabelle und leitet das Paket dann basierend auf der passenden Route weiter.
3. D. Folgt man den Schritten im Buch, entfernt der erste Schritt bis zu drei führende Nullen in jedem Quartett und übrig bleibt FE80:0:0:100:0:0:0:123. Dies hinterlässt zwei Strings mit aufeinanderfolgenden Quartetten nur mit Nullen; indem der längste String von allen in :: geändert wird, lautet die Adresse FE80:0:0:100::123.

4. B. Die Adresse in dieser Frage enthält viele Quartette, bei denen man leicht in eine übliche Falle tappen könnte: in einem Quartett aus Hexadezimalzahlen die Nullen am Ende zu entfernen. Um IPv6-Adressen zu verkürzen, sollte man nur führende Nullen in einem Quartett entfernen. Viele der Quartette haben Nullen am Ende (also Nullen auf der rechten Seite des Quartetts). Achten Sie also darauf, nicht diese Nullen zu entfernen.
5. A. Die unverkürzte Version einer IPv6-Adresse muss 32 Stellen haben und nur eine Antwort erfüllt dies. In diesem Fall zeigt die ursprüngliche Zahl vier Quartette und ein ::. Also wurde das :: durch vier Quartette mit 0000 ersetzt, wodurch die Zahl acht Quartette bekommt. Dann wurden bei jedem Quartett mit weniger als vier Stellen Nullen vorangestellt, sodass jedes Quartett vier Hexadezimalzahlen hat.
6. C. Die Präfixlänge /64 bedeutet, dass die letzten 64 Bits bzw. die letzten 16 Stellen der Adresse alle in Nullen geändert werden sollen. Durch diesen Prozess bekommt man das unverkürzte Präfix 2000:0000:0000:0005:0000:0000:0000:0000. Die letzten vier Quartette bestehen nur aus Nullen und diese sind somit der beste und längste String aus Nullen, den man mit :: ersetzen kann. Nach Entfernen der führenden Nullen in anderen Quartetten lautet die Antwort 2000:0:0:5::/64.

## Kapitel 29

1. C. Unique-Local-Adressen weisen an den ersten beiden Stellen FD auf.
2. A. Global-Unicast-Adressen können mit vielen verschiedenen Anfangswerten beginnen, aber üblicherweise meist entweder mit der Hexadezimalzahl 2 oder 3.
3. D. Das globale Routing-Präfix ist der Adressblock, den eine Organisation von einer Vergabestelle zugewiesen bekommen hat, und wird durch Präfixwert und Präfixlänge dargestellt. Alle IPv6-Adressen in einem Unternehmen haben in diesen ersten Bits ihrer IPv6-Adressen den gleichen Wert. Wenn ein Unternehmen einen öffentlichen IPv4-Adressblock verwendet, haben entsprechend alle Adressen den gleichen Wert im Netzwerkanteil.
4. B. Durch das Subnetting eines Blocks mit Global-Unicast-Adressen, bei dem alle Subnetze die gleiche Präfixlänge bekommen, werden die Adressen in drei Teile aufgeteilt. Das sind das globale Routing-Präfix, das Subnetz und die Interface-ID.
5. D. Unique-Local-Adressen beginnen mit dem zweistelligen Hexadezimalpräfix FD, gefolgt von der zehnstelligen globalen ID als Hexadezimalzahl.

## Kapitel 30

1. A. Diese korrekte Antwort führt genau die gleiche IPv6-Adresse auf, die in der Frage aufgelistet ist, und hat in der Syntax der Antwort die Präfixlänge /64 sowie keine Leerzeichen. Eine andere Antwort ist identisch, außer dass zwischen Adresse und Präfixlänge ein Leerzeichen steht, was einen Syntaxfehler darstellt. Die beiden Antworten mit dem Parameter **eui-64** enthalten nur eine Adresse, aber kein Präfix. Um korrekt zu sein, hätten sie ein Präfix aufführen müssen, obwohl keine von beiden zu der in der Frage erwähnten IPv6-Adresse führt.
2. B. Anhand des Parameters **eui-64** wird der Router den Interface-ID-Teil der IPv6-Adresse berechnen und dafür dessen MAC-Adresse berücksichtigen. Beginnend mit 5055.4444.3333, fügt der Router in der Mitte FF FE ein (5055.44FF.FE44.3333). Dann invertiert der Router das siebte Bit im ersten Byte. Übersetzt heißt das: Hier wird 50 als Hexadezimalzahl in das

binäre 01010000 konvertiert und das siebte Bit invertiert. Also lautet der String 01010010, der dann zurück in die Hexadezimalzahl 52 konvertiert wird. Der Wert für die Interface-ID lautet schließlich 5255:44FF:FE44:3333. Die verkehrten Antworten listen einfach einen falschen Wert auf.

3. A und C. Von den vier Antworten zeigen die beiden korrekten Antworten die minimal erforderliche Konfiguration, um IPv6 auf einem Cisco-Router zu unterstützen (**ipv6 unicast-routing**) und IPv6 auf jedem Interface zu aktivieren, üblicherweise durch Einfügen einer Unicast-Adresse bei jedem Interface (**ipv6 address …**). Die beiden verkehrten Antworten enthalten nicht existierende Befehle.
4. A. Mit dem Befehl **ipv6 address**, der für eine globale Unicast-Adresse konfiguriert wurde (ohne dass jedoch mit dem Befehl **ipv6 address** eine Link-Local-Adresse konfiguriert wurde), berechnet der Router seine Link-Local-Adresse für das Interface basierend auf seiner MAC-Adresse und den EUI-64-Regeln. Die erste Hälfte der Link-Local-Adresse beginnt mit FE80:0000:0000:0000. Der Router berechnet dann die zweite Hälfte des Werts für die Link-Local-Adresse, indem er in der MAC-Adresse (0200.0001.000A) in der Mitte FF FE einfügt (0200.00FF.FE01.000A) und das siebte Bit umkehrt (0000.00FF.FE01.000A).
5. B. FF02::1 wird von allen IPv6-Hosts in der Verbindung verwendet, FF02::5 von allen OSPFv3-Routern und FF02::A von allen EIGRPv6-Routern. FF02::2 wird verwendet, um Pakete an alle IPv6-Router auf einem Link zu senden.

## Kapitel 31

1. B. PC1 muss die MAC-Adresse von PC2 feststellen. Anders als bei IPv4 wird bei IPv6 nicht ARP verwendet, sondern NDP. Genauer gesagt nutzt PC1 die NS-Nachricht (Neighbor Solicitation) von NDP, um PC2 aufzufordern, ein NDP Neighbor Advertisement (NA) zurückzusenden. SLAAC bezieht sich auf die Adresszuweisung und hat nichts mit der Erkennung der MAC-Adressen von Nachbarn zu tun.
2. D. Hosts können alle Router anhand einer NDP RS-Nachricht (Router Solicitation) auffordern, sich zu identifizieren. Dazu senden die Router eine NDP RA-Nachricht (Router Advertisement) zurück. Die NDP NS-Nachricht kann auch von PC1 verwendet werden, aber nicht zu dem Zweck, die IPv6-Adresse seines Default-Routers zu lernen. DAD ist eine Funktion, bei der tatsächlich NDP NS- und NA-Nachrichten verwendet werden, aber zu dieser Funktion gehört nicht die Erkennung von Default-Router-Adressen. EUI-64 schließlich definiert weder ein Protokoll noch eine Nachricht.
3. A und C. Die NDP RA-Nachricht listet die IPv6-Adresse des Routers, die in der Verbindung bekannten IPv6-Präfixe und die entsprechenden Präfixlängen auf. Bei der Verwendung von DHCPv6 erlernt der Host die IPv6-Adressen des DNS-Servers durch DHCPv6-Nachrichten. Für MAC-Adressen der Nachbarn in der Verbindung verwenden Hosts die NDP NS- und NA-Nachrichten.
4. D. Mit SLAAC hat der Host ein Mittel, um seine Unicast-Adresse zu wählen. Über NDP lernt er außerdem seine Präfixlänge plus die Adresse/n von Default-Routern. Dann verwendet er Stateless-DCHP, um die Adressen des/der DNS-Server/s zu lernen.
5. B und D. Über SLAAC erlernt der Host mittels NDP RS/RA-Nachrichten das Präfix von einem Router und erstellt dann die restliche Adresse (die Interface-ID). Um den Wert für die Interface-ID zufällig zu generieren, kann der Host nach EUI-64-Regeln vorgehen oder einen

definierten Prozess verwenden. Der Host erlernt die Interface-ID nicht von einem anderen Gerät, was dazu beiträgt, dass der Prozess zustandslos wird, weil kein anderes Gerät dem Host seine vollständige Adresse zuweisen muss.

6. A. Der Befehl **show ipv6 neighbors** listet alle IPv6-Adressen der Nachbarn (Router und auch Hosts) sowie deren entsprechende MAC-Adressen auf. Dabei wird aber nicht vermerkt, welche davon Router sind – für diese Information sorgt der Befehl **show ipv6 routers**.

## Kapitel 32

1. A und C. Hat das aktive Interface eine IPv6-Adresse, fügt der Router eine direkt angeschlossene Route für das Präfix (Subnetz) hinzu, das durch den Befehl **ipv6 address** impliziert wird. Außerdem wird basierend auf der Unicast-Adresse eine lokale Hostroute (mit der Präfixlänge /28) eingefügt. Der Router fügt basierend auf der Link-Local-Adresse keine Route hinzu.

2. A und C. Die beiden richtigen Antworten zeigen die korrekte Subnetz-ID (Präfix) und die Präfixlänge für die beiden angeschlossenen Subnetze 3111:1:1:1::/64 und 3222:2:2:2::/64. Die Antwort mit der Präfixlänge /128 erscheint in einer lokalen Route, aber solche Routen werden vom Befehl **show ipv6 route connected** gar nicht angezeigt. Die andere falsche Antwort gibt die gesamte IPv6-Adresse mit der Präfixlänge /64 aus; bei Verwendung des Präfixes /64 würde die gesamte Adresse aber gar nicht angezeigt.

3. A. Alle vier Antworten zeigen beispielhaft Befehle, die ein ausgehendes Interface verwenden. Die beiden mit **ip route** beginnenden Befehle definieren nur IPv4-Routen; aufgrund der in den Befehlen aufgeführten IPv6-Präfixe würden diese Befehle abgewiesen werden. Die beiden Befehle, die mit **ipv6 route** beginnen, sind syntaktisch korrekt, aber der Befehl sollte das Interface des lokalen Routers aufführen (ein Interface auf dem Router, auf dem der Befehl konfiguriert wird). R5 muss sein lokales Interface S0/1/1 als ausgehendes Interface verwenden.

4. B. Alle vier Antworten zeigen beispielhaft Befehle, die die IPv6-Adresse eines Next-Hop-Routers verwenden. Zwei der Antworten listen die eigene IPv6-Adresse von R5 auf (Unicast oder Link-Local), was verkehrt ist. Bei der Adresse sollte es sich um eine Adresse auf dem benachbarten Router handeln, in diesem Fall R6. Bei den beiden Antworten, die Adressen auf dem Router R6 aufführen, ist jene korrekt, die die globale Unicast-Adresse von R6 auflistet. Diejenige, bei der die Link-Local-Adresse von R6 aufgelistet ist, würde ebenfalls das ausgehende Interface von R5 erfordern. Also würde die Antwort, in der FE80::FF:FE00:6 steht, ebenfalls abgewiesen.

5. C. Das IOS fügt eine neue statische Route zur IPv6-Routing-Tabelle hinzu, wenn bei Verwendung einer Global-Unicast-Adresse für den nächsten Hop der Router über eine funktionierende Route zum Erreichen dieser Next-Hop-Adresse verfügt und es keine bessere Route (d. h. keine Route mit niedrigerer administrativer Distanz) in genau dieses Subnetz gibt. Insofern gibt die richtige Antwort einen Grund dafür an, warum diese Route nicht aufgeführt wird. Der in einer Antwortoption erwähnte Umstand, dass eine bessere Route mit der administrativen Distanz 110 vorhanden sei, wäre zwar ein gültiges Argument dafür, dass die statische Route nicht aufgelistet wird, aber aus der Frage geht eindeutig hervor, dass keine Route in das Subnetz in der Routing-Tabelle aufgeführt wird, weswegen diese konkurrierende Route schlicht und einfach nicht existiert.

Die beiden anderen Antworten sind im **ipv6 route**-Befehl fehlerhaft. Dieser Befehl kann eine Link-Local-Adresse als nächsten Hop angeben, muss es aber nicht. Außerdem benötigt der Befehl bei Verwendung einer Global-Unicast-Adresse als nächstem Hop kein ausgehendes Interface als Parameter.

6. A und B. Die Ausgabe zeigt zwei statische Routen, wie wir dem Code *S* ganz links in der Ausgabe entnehmen können. Beide wurden aufgrund der **ipv6 route**-Befehle zur IPv6-Routing-Tabelle hinzugefügt. In beiden Fällen beträgt die administrative Distanz 1. Der Wert ist als erste Zahl in Klammern angegeben.

   Beachten Sie bei den beiden falschen Antworten, dass der Interfacesubbefehl **ipv6 address** das Hinzufügen verbundener IPv6-Routen zur Routing-Tabelle bewirkt. Zwar könnte das Attribut *directly connected* der einen Route andeuten, dass es sich um eine direkt angeschlossene Route handelt, aber das *S* ganz links zeigt auch hier die Herkunft der Route an. Ähnlich ist auch die Antwortoption falsch, in der ein IPv6-Routing-Protokoll genannt ist, denn beide Routen weisen den Code *S* (»Static«) auf.

## Kapitel 33

1. D. Standardmäßig werden alle Meldungsebenen auf der Konsole eines Cisco-Gerätes geloggt. Zu diesem Zweck verwendet das IOS die Logebene 7 (Debugging). Hiermit werden Meldungen der Schweregrade 7 und darunter an die Konsole übermittelt. Alle falschen Antworten geben Ebenen an, die unter 7 liegen.
2. C. Der Befehl **logging trap 4** beschränkt Nachrichten, die (nach Konfiguration des Befehls **logging host** *ip-adresse*) an einen Syslog-Server gesendet werden, auf die Ebenen 0 bis 4.
3. A. NTP verwendet Protokollnachrichten zwischen Clients und Servern, damit die Clients ihre Systemuhr an den Server anpassen können. NTP hat überhaupt nichts mit der Taktung über eine serielle Leitung zu tun. Auch zählt es keine CPU-Zyklen, sondern verlässt sich auf Nachrichten vom NTP-Server. Außerdem definiert der Client die IP-Adressen des Servers und muss sich nicht im gleichen Subnetz befinden.
4. B und C. Ein Router im Client/Server-Modus agiert sowohl als Client, indem er seine Zeit zu der eines anderen Servers synchronisiert, als auch als Server, der seine Zeitinformationen anderen NTP-Clients zur Verfügung stellt. Mit dem Befehl **ntp server** wird die Clientfunktion aktiviert, wobei ein anderer Server anzugeben ist, wäre mit dem Befehl **ntp master** die NTP-Serverfunktion auf dem betreffenden lokalen Router aktiviert.
5. E und F. CDP stellt Informationen über Nachbarn fest. Mit **show cdp** bekommen Sie mehrere Optionen, die abhängig von den verwendeten Parametern mehr oder weniger Informationen ausgeben.
6. E und F. Der Befehl **show cdp neighbors** gibt pro Nachbar eine Zeile aus. Auf jeden Fall werden aber Informationen über die Plattform des Nachbarn aufgeführt, zu denen üblicherweise die Hardwaremodellnummer gehört. Der Befehl **show cdp entry Hannah** listet verschiedene Angaben über den benachbarten Router auf, z. B. weitere Details über das Hardwaremodell und die IOS-Version.

## Kapitel 34

1. B. Wenn beide Befehle konfiguriert sind, akzeptiert das IOS nur das Passwort, wie es im Befehl **enable secret** konfiguriert wurde.
2. A. Der Befehl **service password-encryption** verschlüsselt Passwörter auf einen Router oder Switch, die andernfalls als Klartext angezeigt würden. Zwar handelt es sich um ein hervorragendes Konzept, doch lässt sich der Algorithmus mithilfe von Informationen, die auf verschiedenen Websites im Internet zu finden sind, problemlos aushebeln. Cisco stellt bereits seit langer Zeit Ersatz für Befehle bereit, die Passwörter unverschlüsselt speichern, und nutzt stattdessen Hashes. Dies ist etwa bei Befehlen wie **enable secret** und **username secret** der Fall. Diese Befehle werden auch deswegen bevorzugt, weil Probleme mit unverschlüsselten oder leicht zu entschlüsselnden Passwörtern hierbei nicht auftreten.
3. B. Der Befehl **enable secret** speichert einen MD5-Hash. Der Befehl **service password-encryption** ist hierbei irrelevant. Der Router wandelt den Hash-Wert nicht wieder in ein unverschlüsseltes Passwort um. Vielmehr erstellt er nach Eingabe des unverschlüsselten Passworts durch den Benutzer selbst einen Hash und vergleicht dessen Wert mit dem in der Konfiguration angegebenen.
4. B. Nach der Zeichenfolge **banner login** wird das erste Zeichen, das kein Leerzeichen ist, als erstes Trennzeichen interpretiert. In diesem Fall handelt es sich um den Buchstaben *t*. Also wird das zweite *t* – der erste Buchstabe im Wort »the« – als Endtrennzeichen interpretiert. Das daraus resultierende Login-Banner ist der Text zwischen diesen beiden *t* – nämlich »his is«.
5. A. Der Befehl **ip access-class 1 in** aktiviert die Verarbeitung von am Router eingehenden Telnet- und SSH-Verbindungen durch ACL 1 basierend auf der Absender-IP-Adresse dieser eingehenden Pakete. Er hat aber keine Auswirkungen auf Versuche, auf dem Router per Telnet oder SSH einen anderen Host zu kontaktieren. Ebenso wenig beeinflusst er das Erreichen des Enable-Modus durch einen Benutzer. Auch mit der Filterung von Paketen, die anderenfalls über diesen Router geroutet würden, hat er nichts zu tun. Beachten Sie, dass die ACL alle Pakete mit einer Absender-IP-Adresse im Subnetz 172.16.4.0/23 prüft. Dies betrifft dann auch den Bereich der Adressen zwischen 172.16.4.0 und 172.16.5.255.

## Kapitel 35

1. A. Der **copy**-Befehl gibt zunächst den als Quelle und erst dann den als Kopierziel verwendeten Speicherort an. Damit ist **copy flash tftp** falsch, weil die Frage ja besagt, dass die Datei in den Flash-Speicher des Routers kopiert werden soll. Beim Kopieren von Dateien per SCP wird der **copy**-Befehl nicht verwendet. Der Befehl **ios restore** ist kein IOS-Befehl. Mit dem Befehl **copy ftp flash** schließlich kann eine Datei von einem FTP-Server in den Flash-Speicher eines Routers kopiert werden.
2. B. Der erste Schritt bei der Suche nach einem IOS-Image besteht in der Abfrage des Boot Field im Konfigurationsregister. Aus dem dort abgelegten Wert geht hervor, ob das ROMMON-Image oder das IOS geladen werden soll und wie ggf. auf der Suche nach dem IOS vorzugehen ist. Mit diesem ersten Schritt (also dem Boot Field) wird der Router normalerweise angewiesen, die Imagedatei im Flash-Speicher zu verwenden.

3. D. Der Befehl **show version** stellt eine einfache Möglichkeit dar, Speicherort und Name der Imagedatei des Betriebssystems zu überprüfen, unter dem Ihr Cisco-Router läuft. Bei den anderen Antworten ist nur **show running-config** ein gültiger Befehl.
4. D. Die letzte Hexadezimalziffer im Konfigurationsregister ist das sogenannte Boot Field. Es legt fest, wie der Bootvorgang des Routers abläuft. Beispielsweise kann dieses Zeichen auf dem Router festgelegt werden, um das Booten im ROMMON-Modus zu erzwingen.
5. A. Im Zuge der Passwortwiederherstellung müssen Sie das Konfigurationsregister zurücksetzen, damit der Router die vorhandene Startkonfigurationsdatei ignoriert. Hierzu können Sie in den ROMMON-Modus booten.
6. A. Das IOS speichert Arbeitselemente wie die Datei *running-config* und den Arbeitsspeicher für das IOS im RAM. Das ROM wird als Permanentspeicher für den POST- und Bootstrap-Code verwendet, der Flash-Speicher für das IOS und andere Dateien, und das NVRAM ist für die *startup-config* gedacht.
7. D. Der Befehl **copy ftp running-config** kopiert eine Datei in die *running-config,* ersetzt diese aber nicht, weswegen die *running-config* nach Ausführung dieses Befehls nicht mehr unbedingt der Quelldatei entsprechen muss. Der Befehl **copy ftp startup-config** hat keine Auswirkungen auf die *running-config*. Einen Befehl namens **archive restore ftp** gibt es nicht. Mit **config replace** wird eine Datei aus dem Archiv in die *running-config* kopiert und der dort vorhandene Inhalt ersetzt, ohne den Router neu zu laden.

## Kapitel 36

1. D. Beim traditionellen Cisco IOS-Imagemodell wurde jeweils spezifisch für eine bestimmte Kombination aus Router-Modell, Version/Release und Feature-Set eine eigene IOS-Datei erstellt. In diesem Fall gäbe es für eine einzelne Version des Modells *X* je eine IOS-Imagedatei für die Package-Kombinationen Base, Base + Voice, Base + Security usw. – und weitere Images für alle anderen Kombinationen etwa von Base mit mehreren jeweils unterschiedlichen zusätzlichen Feature-Sets.
2. A. Die neue Cisco IOS-Imagedatei, die Zugriff auf alle wesentlichen IOS-Funktionen bietet, ist das Universal-Image.
3. B. Der UDI besteht aus zwei Hauptkomponenten: der Produkt-ID (PID) und der Seriennummer (SN).
4. D. Zum Aktivieren einer erworbenen Lizenz erhält der Kunde einen PAK. An einer bestimmten Stelle im Prozess lädt der Kunde die Lizenzschlüsseldatei herunter und speichert sie an einer Stelle, von der aus der Router sie mit dem EXEC-Befehl **license install** *url* kopieren kann.
5. A. Zum Aktivieren einer Nutzungsrechtelizenz benötigt der Kunde keinen PAK. Stattdessen benennt der Kunde die betreffende Lizenz namentlich mit dem Befehl **license boot**. Von den beiden Antworten, die diesen Befehl enthalten, gibt nur eine die korrekte Syntax an. Nach dem Hinzufügen und Speichern der Konfiguration wird die Lizenz ab dem nachfolgenden Neustart verwendet.