KAPITEL 4

Konfigurieren des Netzwerks

Um die Prüfung zu bestehen, müssen Sie sich mit den Grundlagen der Vernetzung auskennen. Bei vielen Aktionen unter Windows 10 wird vorausgesetzt, dass eine Verbindung zu einem Netzwerk besteht. Daher ist in vielen Bereichen der Prüfung ein Basiswissen über Netzwerke wichtig. Dieses Kapitel handelt von den wichtigsten Netzwerkkomponenten von Windows 10 und deren Konfiguration.

In diesem Kapitel abgedeckte Prüfungsziele:

- Prüfungsziel 4.1: Konfigurieren von IP-Einstellungen
- Prüfungsziel 4.2: Konfigurieren von Netzwerkeinstellungen
- Prüfungsziel 4.3: Konfigurieren und Verwalten der Netzwerksicherheit

Prüfungsziel 4.1: Konfigurieren von IP-Einstellungen

Die IP-Adresse ist die wichtigste Angabe über jeden Windows 10-Computer, der an ein Netzwerk angeschlossen ist. Eine IP-Adresse identifiziert einen Computer im lokalen Netzwerksegment eindeutig und ist eine unverzichtbare Information für viele Wege, auf denen ein Computer im Netzwerk kommuniziert, beispielsweise für die Namensauflösung oder für die Übertragung von Dateien.

Dieser Abschnitt deckt folgende Prüfungsziele ab:

- Herstellen einer Verbindung zu einem Netzwerk
- Konfigurieren der Namensauflösung
- Konfigurieren des Netzwerkstandorts

Herstellen einer Verbindung zu einem Netzwerk

Netzwerke sind Ansammlungen von Computern und anderen Geräten, die untereinander kommunizieren können. Jeder Computer, jeder Netzwerkdrucker, jeder Server und jedes andere ans Netzwerk angeschlossene Gerät muss über eine Adresse verfügen, die es im Netzwerk definiert. Die Adresse muss eindeutig sein. Es kann also keine zwei Geräte mit derselben Adresse geben. Daher ist die Vergabe der Adressen ein wichtiger Teil bei der Konfiguration der Geräte und bei der Verbindung mit Netzwerken.

IP-Adressen

Jedes Gerät im Netzwerk muss über eine eindeutige IP-Adresse (Internet Protocol) verfügen. Im Format IPv4 handelt es sich um eine 32-Bit-Zahl. Sie wird gewöhnlich als Gruppe von vier Dezimalzahlen dargestellt, die jeweils durch einen Punkt voneinander getrennt sind, wie zum Beispiel in 192.168.4.20. Außerdem wird jedem Gerät eine Subnetzmaske zugeordnet. Sie legt fest, welcher Teil der IP-Adresse das Netzwerk definiert und welcher Teil das Gerät definiert. Zusammen genommen definieren die IP-Adresse und die Subnetzmaske das Netzwerk, in dem ein Gerät kommunizieren kann.

Ist eine Kommunikation mit anderen Geräten außerhalb des lokalen Netzwerksegments erforderlich, muss ein Gateway angegeben werden. Gewöhnlich ist dies die Adresse eines Routers, der Verbindungen zu anderen Netzwerken und zum Internet herstellen kann. Zusammen definieren die IP-Adresse, die Subnetzmaske und das Standardgateway die IP-Verbindungsfähigkeit eines Computers im Netzwerk. Es gibt zwei Methoden, einen Computer mit einer IP-Adresse zu versorgen. Man kann sie manuell definieren oder von einem DHCP-Server (Dynamic Host Configuration Protocol) zuweisen lassen.

Wird auf keine der beiden Weisen eine IP-Adresse zugeordnet, weist Windows automatisch eine private IP-Adresse zu. Die Methode heißt APIPA (Automatic Private IP Addressing). APIPA-Adressen fallen in den Adressbereich 169.254.x.x.

PRÜFUNGSTIPP

Informieren Sie sich über die IP-Adressbereiche für die Klassen A, B und C, damit Sie eine Vorstellung davon haben, wie viele Netzwerke jede Klasse bietet und wie viele Geräte die Netzwerke aufnehmen können. Merken Sie sich außerdem die Adressbereiche für private lokale Netzwerke (192.x.x.x, 172.x.x.x, und 10.x.x.x für die Klassen C, B und A).

Netzwerkterminologie

Machen Sie sich mit folgenden Bezeichnungen vertraut:

- **APIP** Das ist eine verbindungslokale IP-Adresse, die von Windows automatisch zugewiesen wird, wenn keine anderen Wege für die Zuordnung einer IP-Adresse zur Verfügung stehen. Dadurch ist das Gerät in der Lage, im lokalen Netzwerksegment zu kommunizieren. Router leiten Datenpakete mit solchen Adressen nicht weiter.
- **Standardgateway** Damit ist ein Gerät gemeint, das eine Verbindung mit anderen Netzwerken ermöglicht. Häufig handelt es sich dabei um das Internet, aber das Ziel kann auch ein anderes Netzwerksegment aus einer Unternehmensdomäne sein.
- **DHCP** DHCP ist ein Netzwerkprotokoll, mit dem Geräte in einem Netzwerk automatisch mit IP-Adressen versorgt werden. Ein DHCP-Server weist diese Adressen zu. Die IP-Adressen gelten aber nur für einen bestimmten Zeitraum und müssen anschließend erneuert werden. Ist für bestimmte Computer eine statische Adresse erforderlich, lässt sich DHCP so konfigurieren, dass Adressen für diese Geräte reserviert werden können.
- **DHCP-Bereich** Ein DHCP-Bereich ist ein aufeinanderfolgender Bereich mit IP-Adressen, die den Geräten aus einem Subnetz zugeordnet werden können

- **DNS** DNS (Domain Name Service) ist ein Dienst, der es Benutzern ermöglicht, statt einer IP-Adresse den Namen des gewünschten Kommunikationspartners anzugeben. Ein DNS-Server liefert die zu einem Namen gehörige IP-Adresse. Der Vorgang wird *Namensauflösung* genannt.
- **IPv4** Diese IP-Adresse ist 32 Bit breit und wird dezimal in vier Gruppen zu jeweils 8 Bit dargestellt. Sie besteht aus zwei Teilen, nämlich aus der Netzwerk-ID und der Host-ID. Die Netzwerk-ID beschreibt das Netzwerk und die Host-ID das betreffende Gerät in diesem Netzwerk. Von IPv4-Adressen gibt es die Varianten *Unicast*, *Broadcast* oder *Multicast*.
- **Subnetzmaske** Die Subnetzmaske ist eine 32-Bit-Zahl, die in Dezimalform ebenfalls als Gruppe aus vier 8-Bit-Zahlen dargestellt wird, die jeweils durch einen Punkt voneinander getrennt sind. Schreibt man diese Zahl in Binärform auf, geben die Einsen am Anfang der Zahl den Bereich an, der die Netzwerk-ID festlegt, und die nachfolgenden Nullen den Bereich, in dem die Host-IDs liegen. Die Standardsubnetzmasken haben für Adressen der Klasse A die Form 255.0.0.0, für Adressen der Klasse B die Form 255.255.0.0 und für Adressen der Klasse C die Form 255.255.255.0. In binärer Form sieht 255.0.0.0 zum Beispiel folgendermaßen aus: 11111111 00000000 00000000 00000000.
- **IPv6** Die verfügbaren IPv4-Adressen reichen für die wachsende Zahl der Computer nicht aus. Man braucht eine bessere Lösung, die es deutlich mehr Computern ermöglicht, miteinander zu kommunizieren. IPv6 ist diese Lösung. Es handelt sich nicht mehr um einen 32-Bit-Adressraum, sondern um einen 128-Bit-Adressraum mit 16-Bit-Grenzen. Dadurch lassen sich viel mehr Adressen angeben. Eine typische IPv6-Adresse sieht zum Beispiel so aus: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

WEITERE INFORMATIONEN **IP-Adressierung**

Unter *https://technet.microsoft.com/en-us/library/cc958829.aspx* finden Sie weitere Informationen darüber, wie IP-Adressen definiert sind und wie sie funktionieren.

Konfigurieren der IP-Einstellungen

Auf einem Windows 10-Computer können Sie die IP-Einstellungen im Eigenschaftsdialogfeld einer Netzwerkkarte vornehmen. So öffnen Sie das Eigenschaftsdialogfeld:

1. Klicken Sie die Schaltfläche *Start* auf der Taskleiste mit der rechten Maustaste an und klicken Sie auf *Netzwerkverbindungen*.
2. Klicken Sie im Fenster *Netzwerkverbindungen* die entsprechende Netzwerkkarte mit der rechten Maustaste an und klicken Sie auf *Eigenschaften* (Abbildung 4.1).

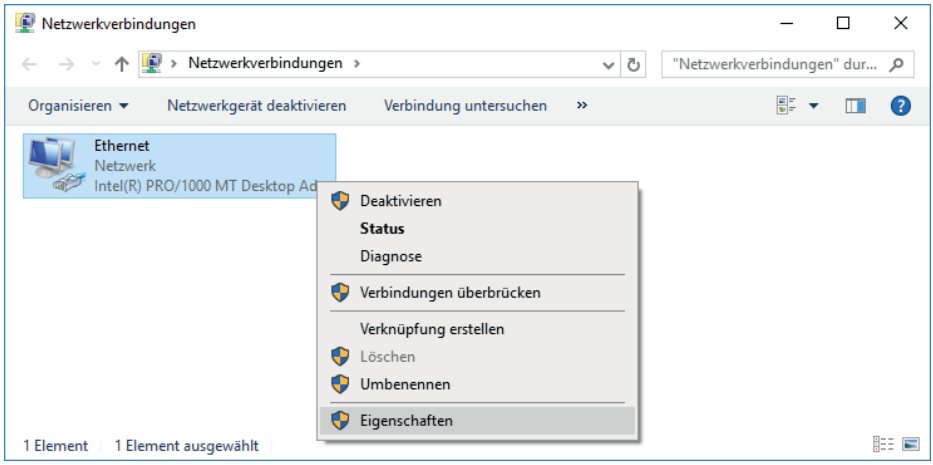

ABBILDUNG 4.1 Öffnen des Eigenschaftsdialogfelds einer Netzwerkkarte

3. Wählen Sie im *Eigenschaften*-Dialogfeld das *Internetprotokoll Version 4 (TCP/IPv4)* und klicken Sie auf *Eigenschaften* (Abbildung 4.2).

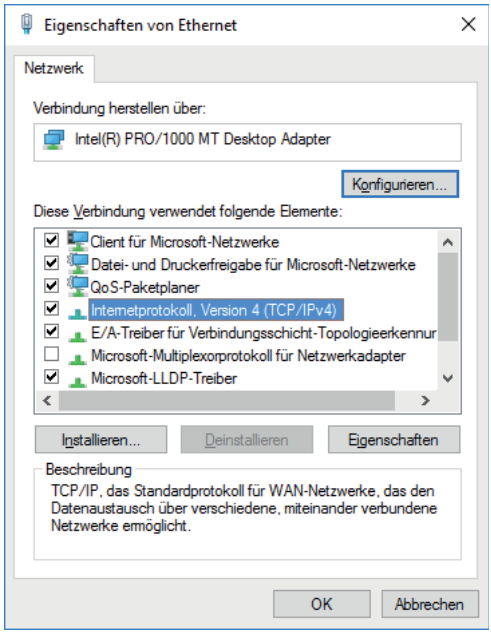

ABBILDUNG 4.2 Das Eigenschaftsdialogfeld einer Netzwerkkarte

4. Nehmen Sie im Dialogfeld *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)* die gewünschten Einstellungen vor und geben Sie bei Bedarf die erforderlichen Adressen ein (Abbildung 4.3). Sie haben die Wahl, die IP-Adresse und die Adressen der DNS-Server automatisch von einem DHCP-Server abzurufen, oder Sie können die Adressen manuell festlegen. In diesem Fall müssen Sie zumindest eine IP-Adresse und eine Subnetzmaske eingeben.

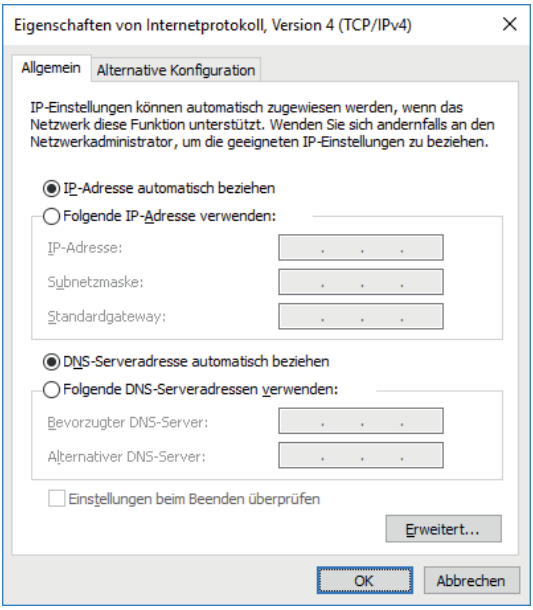

ABBILDUNG 4.3 Das Dialogfeld für die IPv4-Konfiguration

PRÜFUNGSTIPP

Vielleicht werden Sie in der Prüfung gefragt, wie man auf der Befehlszeile IPv4- oder IPv6-Adressen konfiguriert. Dann brauchen Sie den Befehl *Netsh*. Sehen Sie sich die entsprechenden Optionen des Befehls an. Vielleicht werden Sie aufgefordert, den Befehl für die Einrichtung einer statischen Adresse für einen Computer auszuwählen. Dieser Befehl hat folgende Form: *netsh interface ipv4 set address „<Name der Ethernet-Verbindung>" static 192.168.5.12 255.255.255.0 192.168.1.10*. Soll die Adresse von einem DHCP-Server geliefert werden, sieht der Befehl so aus: *netsh interface ipv4 set address name="<Name der Ethernet-Verbindung>" source=dhcp*.

Verbinden mit einem Netzwerk

Beim ersten Versuch, eine Verbindung mit einem lokalen Netzwerk herzustellen, werden Sie aufgefordert, folgende Frage zu beantworten: »Möchten Sie zulassen, dass Ihr PC von anderen PCs und Geräten in diesem Netzwerk gefunden werden kann?«

- **Nein** Diese Option ist für öffentliche Netzwerke und Hotspots vorgesehen (Bibliotheken, Coffee-Shops). Der Computer des Benutzers ist für andere nicht sichtbar und nicht zugänglich. Auch der Benutzer kann keine anderen Computer sehen, die mit dem Netzwerk verbunden sind.
- **Ja** Diese Option ist für private, vertrauenswürdige Netzwerke vorgesehen (zu Hause oder am Arbeitsplatz), und für Heimnetzgruppen. Die Computer werden von einem Router geschützt und stellen keine direkte Verbindung zum Internet her.

Diese beiden Optionen erscheinen nicht, wenn Sie eine Verbindung zu einer Active Directory-Domäne herstellen. Wenn Sie erscheinen und Sie eine Option auswählen, werden einige Einstellungen automatisch vorgenommen, nämlich für die Netzwerkerkennung, die Datei- und Druckerfreigabe, die Firewall, für Apps, die eingehende Verbindungen annehmen dürfen, und einige andere Dinge. Befindet sich der Computer in einem privaten oder einem Domänennetzwerk, wird die Netzwerkerkennung aktiviert, in einem öffentlichen Netzwerk dagegen nicht.

Beheben von Verbindungsproblemen

Wenn ein Computer keine Verbindung zum Netzwerk herstellen kann, muss das Verbindungsproblem behoben werden. Die Ursache kann auf den betreffenden Computer beschränkt sein, weil zum Beispiel das Ethernet-Kabel abgezogen wurde oder weil die Drahtlos-Funktionen des Computers deaktiviert wurden. Vielleicht gibt es einen IP-Adressenkonflikt im Netzwerk und die IP-Adresse des Computers muss erneuert werden. Häufig finden bereits die Problembehandlungstools des *Netzwerk- und Freigabecenters* die Ursache und können eine Lösung anbieten. Lässt sich die Ursache nicht erkennen, haben Sie ein ernsthafteres Problem. Vielleicht ist ein Netzwerkserver, ein Gateway oder eine andere wichtige Ressource ausgefallen oder ein Netzwerksegment oder ein wichtiges übergeordnetes Netzwerk ist beschädigt. Vielleicht liegt das Problem auch beim Internet-Dienstanbieter, in einem Cloud-Dienst oder bei anderen Diensten, die Sie nicht beeinflussen können.

> ***HINWEIS*** **Anzeigen des Verbindungsstatus**
>
> **Wenn Sie den Status einer Verbindung überprüfen möchten, öffnen Sie das *Netzwerk- und Freigabecenter* und klicken auf *Adaptereinstellungen ändern*. Klicken Sie dann doppelt auf das Symbol der betreffenden Verbindung und klicken Sie auf *Details*. Dann erscheint ein Dialogfeld, in dem Sie die *Physische Adresse*, die Aktivierung von DHCP und die IP-Adressen ablesen können. Zu den Angaben gehören die IP-Adressen des DNS-Servers, des Standardgateways und des DHCP-Servers, sowie das Ausstellungsdatum und das Ablaufdatum der DHCP-Lease. Mit dem Befehl *ipconfig /all* können Sie diese Daten auch auf einer Befehlszeile abrufen.**

NETZWERK- UND FREIGABECENTER

Das *Netzwerk- und Freigabecenter* ermöglicht eine Überprüfung der Zustände der aktiven Netzwerke. Gibt es ein Problem, können Sie auf *Probleme beheben* klicken und abwarten, ob das *Netzwerk- und Freigabecenter* es beheben kann. Manche Probleme lassen sich beheben, indem man die IP-Adresse abgibt und neu anfordert oder den Netzwerkadapter zurücksetzt. Manchmal ist es auch so einfach wie das Einstöpseln eines abgezogenen Ethernet-Kabels.

Lässt sich ein Problem nicht automatisch beheben, haben Sie die Auswahl aus einer Liste von Problembehandlungsoptionen. Dazu gehören Optionen zur Behebung von Problemen mit der Verbindung zu Websites, für den Zugriff auf freigegebene Ordner, die Suche nach Computern und Dateien in einer Heimnetzgruppe, die Suche und Behebung von Problemen mit drahtlosen Netzwerkverbindungen und die Behebung von Problemen mit eingehenden

Verbindungen. Wenn Sie eine Option wählen und das entsprechende Modul zur Problembehebung starten, findet es gewöhnlich das Problem und führt eine Reparatur durch, oder es fordert Sie auf, die Reparatur zu genehmigen. Vielleicht fordert es Sie auch auf, zuvor etwas zu tun und beispielsweise das Ethernet-Kabel wieder an den Computer anzuschließen.

BEFEHLSZEILENTOOLS

Wenn weder das *Netzwerk- und Freigabecenter* noch das *Info-Center* bei der Lösung von Verbindungsproblemen helfen können, ist die Lösung wohl etwas komplizierter. Vielleicht ist ein Router ausgefallen oder das Gateway der Domäne oder des Netzwerksegments ist nicht in Betrieb. Vielleicht ist der DNS-Server nicht zugänglich oder wurde auf dem Computer falsch konfiguriert. Oder die eindeutige firmeninterne IP-Adresse des Computers wurde in eine APIPA-Adresse geändert, weil es ein nicht gelöstes Problem mit dem Netzwerk gibt.

In solchen Fällen stehen eine Reihe von Befehlszeilentools zur Verfügung, mit denen Sie dem Problem auf die Spur kommen können:

- **Ping** Dieses Tool überprüft die Verbindungen zu anderen TCP/IP-Computern auf IP-Ebene. Dazu sendet es ICMP-Echoanforderungen an den Empfänger (ICMP steht für Internet Control Message Protocol). Der Empfänger der Nachrichten wird zusammen mit den Antwortzeiten angezeigt, sofern die Verbindung funktioniert. Ping ist der wichtigste Befehl zur Überprüfung von Verbindungen, Erreichbarkeit und Namensauflösung.
- **Ipconfig und Ipconfig /all** Dieser Befehl zeigt alle Werte der TCP/IP-Netzwerkkonfiguration an. Außerdem kann er DHCP- und DNS-Einstellungen aktualisieren. Ohne den Parameter */all* zeigt Ipconfig die IPv4- und IPv6-Adressen, die Subnetzmasken und die Standardgateways für alle Netzwerkadapter an, die im Computer installiert sind. Gebräuchliche Parameter sind */release*, */renew* und */flushdns*.
- **Tracert** Dieses Tool ermittelt den Verbindungspfad zu einem bestimmten Ziel und zeigt Informationen über jeden Verbindungsabschnitt des Übertragungswegs an. Solch ein Abschnitt beginnt und endet jeweils mit einem Durchgang durch einen Router. Aus diesen Informationen können Sie ablesen, ob die Übertragungen im normalen Rahmen erfolgen oder ob vielleicht Probleme vorliegen.
- **Netstat** Dieser Befehl zeigt eine Liste der aktiven TCP-Verbindungen und die Ports an, an denen der Computer auf eingehende Daten wartet. Außerdem zeigt der Befehl statistische Daten über die Ethernet-Verbindungen, die IP-Routingtabelle sowie Daten zu IPv4 und IPv6 an.
- **Netsh** Dieser Befehl ermöglicht Ihnen, die Netzwerkkonfiguration des Computers auf der Befehlszeile zu ändern
- **Nslookup** Dieses Tool zeigt Informationen an, die Sie zur Diagnose von DNS-Problemen verwenden können

Konfigurieren der Namensauflösung

Computer werden durch eine eindeutige IP-Adresse repräsentiert, die man zur Kommunikation mit den Computern verwenden kann. Die Kommunikation mit einer bestimmten IP-Adresse kann auf der Befehlszeile erfolgen. Sie können zum Beispiel so etwas wie **ping 192.168.4.5** eingeben, um Verbindungsprobleme mit einem anderen Computer im lokalen Netzwerksegment zu erkennen und zu beheben. Allerdings ist die Kommunikation auf dieser Ebene sehr mühsam.

DNS ermöglicht Benutzern die Verwendung von Namen statt Nummern. Ein DNS-Server liefert zu einem Namen die passende IP-Adresse. Der Vorgang wird *Namensauflösung* genannt. DNS-Server speichern Informationen über die Namen und Adressen von Internet-Computern. Die Listen, die sie dabei aufstellen, werden an Tausende von DNS-Servern weitergeleitet, die im Internet verfügbar und über die ganze Welt verteilt sind. Die Anforderung zur Namensauflösung wird an einen dieser Server gesendet. Kann der Server den Namen nicht auflösen, leitet er die Anforderung an einen anderen Server weiter, der sie gegebenenfalls an einen weiteren Server sendet, und so weiter, bis der Name aufgelöst ist.

Gewöhnlich liefert Ihr DHCP-Server auch die Adressen der DNS-Server, die von den Computern in Ihrem Netzwerk für die Namensauflösung verwendet werden sollen. Das geschieht, wenn die Option *DNS-Serveradresse automatisch beziehen* gewählt ist. Im Eigenschaftsdialogfeld der Verbindung können Sie die gewünschten DNS-Server auch manuell eintragen (Abbildung 4.3). Das ist zum Beispiel erforderlich, wenn ein Computer in einer Domäne einen bestimmten DNS-Server verwenden soll. Es kann auch in einem virtuellen privaten Netzwerk oder in einem virtuellen Computer erforderlich werden.

Je nach Konfiguration löst Windows 10 Hostnahmen durch folgende Aktionen auf:

1. Überprüfen, ob der Hostname mit dem lokalen Hostnamen übereinstimmt
2. Überprüfen des DNS-Auflösungscaches. Er enthält Informationen aus der lokalen Datei *Hosts*.
3. Senden einer DNS-Anfrage an die konfigurierten DNS-Server

Beheben von Problemen mit der Namensauflösung

Die wichtigsten Hilfsmittel zur Behebung von Problemen mit der Namensauflösung sind *IPConfig* und *NSLookup*, sowie die Windows PowerShell-Cmdlets `Get-NetIPAddress`, `Get-NetIPv4Protocol` und `Resolve-DnsName`.

Wenn Sie keine Verbindung zu einem Remotehost herstellen können und ein Problem in der Namensauflösung vermuten, können Sie die Namensauflösung folgendermaßen überprüfen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und löschen Sie mit folgendem Befehl den DNS-Auflösungscache:

   ```
   IPConfig /flushdns
   ```

   Als Alternative bietet sich das Windows PowerShell-Cmdlet `Clear-DnsClientCache` an.
2. Überprüfen Sie die Erreichbarkeit eines Remotehosts mit dessen IP-Adresse. Dazu können Sie den Befehl `Ping` oder das Windows PowerShell-Cmdlet `Test-Connection` verwenden. Anschließend überprüfen Sie die Namensauflösung. Ist der Ping-Befehl mit

der IP-Adresse erfolgreich, aber nicht mit dem Hostnamen, liegt das Problem in der Namensauflösung.

3. Überprüfen Sie die Verbindung zum Host mit seinem vollqualifizierten Domänennamen. Geben Sie zum Beispiel in einem PowerShell-Fenster folgenden Befehl ein:

   ```
   Test-connection LON-cl1.adatum.com
   ```

   Sie können auch den Befehl `Ping` verwenden.

4. Ist der Test erfolgreich, hat das Verbindungsproblem wahrscheinlich nichts mit der Namensauflösung zu tun.

5. Ist der Test nicht erfolgreich, bearbeiten Sie die Textdatei *C:\Windows\System32\Drivers\Etc\hosts*. Fügen Sie den entsprechenden Eintrag am Ende der Datei ein. Fügen Sie zum Beispiel folgende Zeile ein und speichern Sie die Datei:

   ```
   172.16.0.51         LON-cl1.adatum.com
   ```

6. Führen Sie den Test erneut mit dem Hostnamen durch. Nun sollte die Namensauflösung funktionieren.

7. Überprüfen Sie den DNS-Auflösungscache und achten Sie darauf, ob die Namen korrekt aufgelöst werden. Um den DNS-Auflösungscache anzuzeigen, geben Sie in einer Eingabeaufforderung folgenden Befehl ein:

   ```
   IPConfig /displaydns
   ```

   Sie können auch das Windows PowerShell-Cmdlet `Get-DnsClientCache` verwenden.

8. Entfernen Sie den Eintrag, den Sie zur Datei *Hosts* hinzugefügt haben, und löschen Sie den DNS-Auflösungscache. Geben Sie in einer Eingabeaufforderung folgenden Befehl ein und überprüfen Sie den Inhalt der Datei *Dateiname.txt*, um die Stufe in der Namensauflösung zu finden, in der sich der Fehler zeigt:

   ```
   NSLookup.exe –d2 LON-cl1.adatum.com > Dateiname.txt
   ```

   Der entsprechende Windows PowerShell-Befehl lautet:

   ```
   Resolve-DnsName lon-cl1.adatum.com > Dateiname.txt
   ```

Konfigurieren des Netzwerkstandorts

Bei der ersten Verbindung eines Computers mit einem Netzwerk müssen Sie entscheiden, ob Sie dem Netzwerk vertrauen. Dadurch werden die entsprechenden Firewall- und Sicherheitseinstellungen automatisch festgelegt. Wenn Sie an verschiedenen Standorten Verbindungen zu Netzwerken herstellen, können Sie dafür sorgen, dass Ihr Computer jederzeit auf eine passende Sicherheitsstufe eingestellt ist, indem Sie den entsprechenden Netzwerkstandort wählen.

Windows 10 verwendet seine NLA-Fähigkeiten (Network Location Awareness), um die Netzwerke eindeutig zu identifizieren, mit denen ein Computer verbunden ist. Beim Erkennen der Standortkategorie werden Informationen über die Netzwerke angefordert, beispielsweise IP-Adressen und MAC-Adressdaten von wichtigen Netzwerkkomponenten wie Router und Gateways (MAC steht für Media Access Control).

Es gibt drei Netzwerkstandorttypen:

- **Domänennetzwerke** Solche Netzwerke sind in Unternehmen üblich, in denen viele Computer vorhanden sind. Verwenden Sie diese Option, wenn im Netzwerk die Kommunikation mit einem Domänencontroller möglich ist. Die Netzwerkerkennung ist standardmäßig aktiviert und der Computer kann kein Mitglied einer Heimnetzgruppe werden. Heimnetzgruppen lassen sich nicht erstellen.
- **Private Netzwerke** Das sind Netzwerke in Privatwohnungen oder am Arbeitsplatz, bei denen man die Geräte und die Leute kennt, die im Netzwerk arbeiten, und ihnen vertraut. In einem privaten Netzwerk ist die Netzwerkerkennung eingeschaltet. In einem Heimnetzwerk können Computer einer Heimnetzgruppe angehören.
- **Gast oder öffentliche Netzwerke** Damit sind Netzwerke an öffentlichen Plätzen gemeint. Diese Einstellung verhindert, dass der Computer für andere Computer sichtbar ist. Heimnetzgruppen sind nicht verfügbar und die Netzwerkerkennung ist ausgeschaltet.

Der Netzwerkstandort *Gast oder öffentliche Netzwerke* verhindert, dass bestimmte Programme und Dienste ausgeführt werden. Dadurch ist ein Computer besser vor nicht autorisierten Zugriffen geschützt. Wenn Sie eine Verbindung mit einem öffentlichen Netzwerk hergestellt haben und Windows-Firewall aktiviert ist, fragen einige Programme oder Dienste vielleicht, ob sie durch die Firewall kommunizieren dürfen, damit sie ordnungsgemäß arbeiten können.

Mit der Heimnetzgruppen-Problembehandlung können Sie den Netzwerkstandort in einer Heimnetzgruppe ändern. Vielleicht ist dies nie erforderlich, aber man sollte sich merken, dass dies zumindest eine Option ist. Im lokalen Netzwerk einer Arbeitsgruppe können Sie die gewünschten Änderungen in der App *Einstellungen* vornehmen:

1. Klicken Sie in der App *Einstellungen* auf *Netzwerk und Internet*.

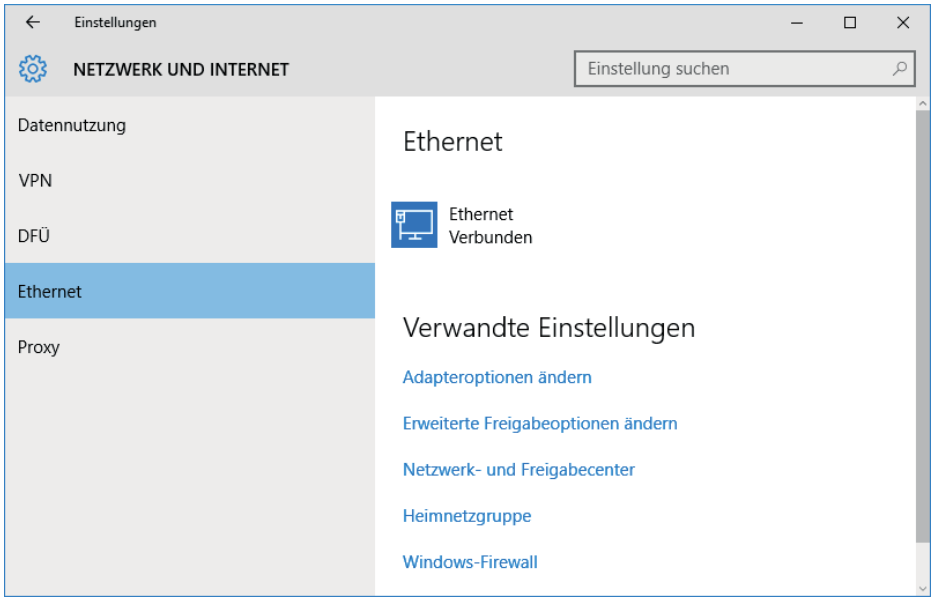

ABBILDUNG 4.4 Die Seite *Netzwerk und Internet* der App *Einstellungen*

2. Klicken Sie auf der Seite *Netzwerk und Internet* auf *Ethernet* und dann auf den Adapter, für den Sie die Netzwerkadresse konfigurieren möchten. In Abbildung 4.4 ist dies *Ethernet*.
3. Bringen Sie auf der Konfigurationsseite den Schalter unter *Dieser PC soll gefunden werden* nach Bedarf in die Stellung *Aus*, wenn Sie in einem öffentlichen Netzwerk arbeiten und der PC nicht sichtbar sein soll, oder in die Stellung *Ein*, wenn Sie in einem privaten Netzwerk arbeiten.

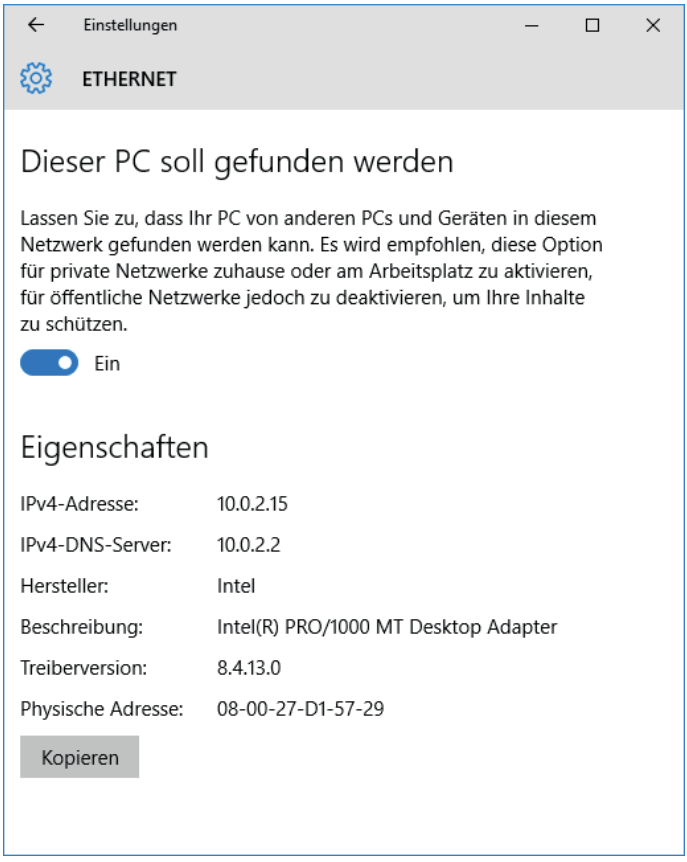

ABBILDUNG 4.5 *Dieser PC soll gefunden werden*

Gedankenexperiment

Beheben von Verbindungsproblemen bei Mobilgeräten

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sie untersuchen die Verbindungsprobleme eines neuen Laptops, der zu einem kleinen, lokalen Firmennetzwerk hinzugefügt wurde, in dem es bereits acht andere Computer gibt. Drei dieser acht Computer sind ebenfalls Laptops, die bisher ohne Probleme Verbindungen herstellen konnten. Der neue Laptop kann eine Verbindung herstellen, wenn er mit einem Ethernet-Kabel an den Router angeschlossen wird, aber nicht drahtlos.

Beantworten Sie folgende Fragen:

1. **Worin vermuten Sie die Ursache des Problems?**
2. **Kann die Problembehandlung im *Netzwerk- und Freigabecenter* Ihrer Meinung nach das Problem lösen?**
3. **Was würden Sie tun, falls die Problembehandlung für Internetverbindungen das Problem zwar erkennt, aber nicht beheben kann, und warum?**

Zusammenfassung der Lektion

- Bei der Verbindung mit einem Netzwerk erhält Ihr Computer eine IP-Adresse, die im aktuellen Netzwerksegment eindeutig ist
- Jeder Computer, der mit einem Netzwerk verbunden ist, braucht eine IP-Adresse. Bei Bedarf stehen eine Reihe von Problembehandlungstools zur Verfügung, mit denen Sie Verbindungsprobleme untersuchen können.
- Die Namensauflösung ermöglicht die Verwendung von verständlichen Namen für die anderen Geräte im Netzwerk, statt einer IP-Adresse
- Der Standorttyp eines Netzwerks (Network Location) bestimmt, welche Art von Netzwerkdatenverkehr über eine Netzwerkkarte möglich ist

Lernzielkontrolle

Beantworten Sie folgende Fragen, um Ihr Wissen über den Stoff dieses Abschnitts zu überprüfen. Antworten auf diese Fragen und Erklärungen, warum die jeweilige Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Was ist die Aufgabe von DNS (Domain Name System)?
   - **A.** Den Computern im lokalen Netzwerk oder Netzwerksegment automatisch IP-Adressen zuzuweisen
   - **B.** IPv6-Datenverkehr über ein IPv4-Netzwerk zu übertragen

C. Hostnamen in IP-Adressen aufzulösen

D. APIPA-Adressen zuzuweisen, wenn keine IP-Adresse von einem DHCP-Server zur Verfügung steht

2. Wie können Sie einem Gerät in einem Netzwerk eine statische IP-Adresse zuweisen, beispielsweise einem Computer oder einem Netzwerkdrucker? (Wählen Sie alle zutreffenden Antworten.)

   A. Im Eigenschaftsdialogfeld des Netzwerkadapters des Geräts

   B. Im Info-Center, in den Sicherheitsoptionen

   C. In einer Eingabeaufforderung mit dem Befehl `Netsh`

   D. In den erweiterten Freigabeeinstellungen des *Netzwerk- und Freigabecenters*

3. Sie brauchen Informationen über eine bestimmte Netzwerkkarte, wie die physische Adresse, die DHCP-Konfiguration, die IPv4- und IPv6-Adressen, die Subnetzmaske und die Adressen, die für den DNS-Server, den DHCP-Server und das Standardgateway konfiguriert sind. Außerdem möchten Sie wissen, wann die DHCP-Lease erneuert werden muss. Was würden Sie verwenden?

   A. `Ipconfig`

   B. `Ipconfig /all`

   C. `Ping`

   D. `Tracert`

4. Wie würden Sie einen konfigurierten Netzwerkstandort in Windows 10 ändern?

   A. Im Eigenschaftsdialogfeld des Netzwerkadapters des Computers

   B. Mit den Wartungsoptionen des Info-Centers

   C. Sie klicken in der App *Einstellungen* mit der rechten Maustaste auf das Netzwerk, klicken auf *Dieses Netzwerk nicht mehr nutzen* und stellen dann erneut eine Verbindung her.

   D. In der App *Einstellungen* unter *Netzwerk und Internet*

Prüfungsziel 4.2: Konfigurieren von Netzwerkeinstellungen

Es gibt eine ganze Reihe Einstellungen für Netzwerke, die Sie vornehmen können. Sie können Verbindungen zu Drahtlosnetzwerken und zu Breitbandnetzwerken herstellen und die Liste der Drahtlosnetzwerke verwalten, zu denen Sie eine Verbindung hergestellt haben. Außerdem können Sie den aufenthaltsortabhängigen Druck konfigurieren, damit Benutzer automatisch auf dem gewünschten lokalen Drucker drucken können. Und Sie können die Einstellungen der Netzwerkkarten anpassen, um gegebenenfalls die Standardeinstellungen zu ändern und die Übertragungsleistung zu verbessern.

Dieser Abschnitt deckt folgende Prüfungsziele ab:

- Verbinden mit einem Drahtlosnetzwerk
- Verwalten bevorzugter Drahtlosnetzwerke
- Konfigurieren von Netzwerkkarten
- Konfigurieren des aufenthaltsortabhängigen Druckens

Verbinden mit einem Drahtlosnetzwerk

Eine wachsende Zahl von Geräten verwendet Drahtlosnetzwerke als Hauptmethode für die Verbindung mit firmeneigenen Intranets und dem Internet. Außerdem erwarten viele Benutzer an ihrem Arbeitsplatz eine Infrastruktur für Drahtlosnetzwerke. Daher ist eine gewisse Praxiserfahrung mit Drahtlosnetzwerken heutzutage eine wichtige Forderung. In Windows 10 können Sie mit dem Netzwerksymbol auf der Taskleiste eine Verbindung mit einem Drahtlosnetzwerk herstellen:

1. Klicken Sie auf der Taskleiste des Desktops auf das Netzwerksymbol (Abbildung 4.6).

ABBILDUNG 4.6 Eine Liste der verfügbaren Drahtlosnetzwerke

2. Klicken Sie das gewünschte Netzwerk in der Liste an.
3. Wählen Sie bei Bedarf das Kontrollkästchen *Automatisch verbinden*. Dann wird der Netzwerksicherheitsschlüssel gespeichert, damit Sie ihn nicht bei jeder Verbindung mit dem Netzwerk erneut eingeben müssen.
4. Klicken Sie auf *Verbinden*. Wenn das Netzwerk gesichert ist, werden Sie aufgefordert, den Netzwerksicherheitsschlüssel einzugeben.

Verwalten bevorzugter Drahtlosnetzwerke

Windows 10 führt Buch über alle Netzwerke, mit denen Sie eine Verbindung herstellen, und ermittelt automatisch Prioritätswerte. Wenn Sie mehrere verschiedene Verbindungen verwenden, versucht Windows 10 in dieser Reihenfolge, Verbindungen herzustellen: Ethernet, WLAN und dann mobiles Breitband. Stehen auf einem Windows 10-Computer alle drei Netzwerktypen zur Verfügung, wird zuerst das Ethernet verwendet. Führt dies nicht zum Erfolg, wird WLAN verwendet. Ist beides nicht verfügbar, wird das mobile Breitband verwendet. Sie können den Computer auch so konfigurieren, dass er automatisch das mobile Breitband verwendet. Haben Sie bereits zu mehreren Drahtlosnetzwerken eine Verbindung hergestellt und sind mehrere dieser Netzwerke verfügbar, stellt Windows 10 eine Verbindung zu dem Netzwerk her, mit dem Sie zuletzt verbunden waren.

Falls Sie automatisch mit einem Netzwerk verbunden wurden, aber ein anderes auswählen möchten, klicken Sie in der Netzwerkliste auf das Netzwerk. Die Liste können Sie mit einem Klick auf das Netzwerksymbol öffnen, das Sie rechts auf der Taskleiste finden.

In Windows 10 können Sie bevorzugte Netzwerke auf zwei verschiedene Weisen verwalten. Erstens können Sie die Seite *WiFi* unter *Netzwerk und Internet* der App *Einstellungen* verwenden.

1. Öffnen Sie die App *Einstellungen*.
2. Klicken Sie auf *Netzwerk und Internet* und dann auf *WLAN*.
3. Klicken Sie auf der Seite *WiFi* auf *WLAN-Einstellungen verwalten*.
4. Klicken Sie im unteren Teil der Seite unter *Bekannte Netzwerke verwalten* auf das Netzwerk, das Sie verwalten möchten.
5. Klicken Sie auf *Nicht speichern*, um das Netzwerkprofil zu löschen.

Sie können Drahtlosnetzwerke auch mit Netsh verwalten. So löschen Sie Netzwerkprofile mit Netsh:

1. Geben Sie auf einer Befehlszeile folgenden Befehl ein:

   ```
   Netsh wlan show profiles
   ```

2. Suchen Sie das Profil heraus, das Sie entfernen möchten, und verwenden Sie folgenden Befehl:

   ```
   Netsh wlan delete profile name=<Profilname>
   ```

Konfigurieren von Netzwerkkarten

Wenn Sie im Fenster *Netzwerkverbindungen* eine Netzwerkkarte mit der rechten Maustaste anklicken, können Sie verschiedene Arbeiten durchführen:

- Aktivieren oder Deaktivieren des Adapters. Das kann bei der Behebung von Problemen hilfreich sein. Außerdem suchen deaktivierte Drahtlosadapter nicht mehr ständig nach Netzwerken, wenn Sie die Verbindungen nicht brauchen.
- Herstellen oder Trennen einer Verbindung

- Anzeigen des Adapter- oder Verbindungsstatus. Sie können dies zur Anzeige der übertragenen Datenmenge verwenden, zur Diagnose von Verbindungsproblemen, zur Überprüfung der Signalqualität und der Übertragungsgeschwindigkeit oder zur Ermittlung der Netzwerkkennung (Service Set Identifier, SSID).
- Ermitteln der Ursache von Verbindungsproblemen. Sie können mit einem Klick auf die Schaltfläche *Diagnose* automatische Tools starten, die Ihnen bei der Problembehebung helfen.
- Überbrücken von zwei oder mehr Verbindungen. Sie müssen zwei LAN-Verbindungen oder Hochgeschwindigkeits-Internetverbindungen auswählen, die nicht für die gemeinsame Nutzung von Internetverbindungen (Internet Connection Sharing) verwendet werden. Eine Netzwerkbrücke ist ein Gerät, das Verbindungen zu mehreren Netzwerksegmenten herstellen kann.
- Erstellen einer Verknüpfung zum Adapter, damit er leichter zugänglich wird
- Löschen des Eintrags, sofern die Option verfügbar ist
- Umbenennen des Adapters
- Anzeigen der Adaptereigenschaften. Sie sehen das Eigenschaftsdialogfeld, das in diesem Kapitel bereits beschrieben wurde. Darin sehen Sie, welche Verbindung der Adapter benutzt. Sie können Protokolle, den erweiterbaren virtuellen Switch von Hyper-V, den Microsoft-LLDP-Treiber und andere Dinge installieren oder entfernen. Für die gewählten und installierten Optionen können Sie auch weitere Eigenschaften anzeigen.

Untersuchen Sie die Optionen, die für die Adapter verfügbar sind, auf die Sie Zugriff haben. Klicken Sie in jedem *WiFi*-Eigenschaftsdialogfeld auf *Konfigurieren*, um die erweiterten Optionen zu sehen. Sie können den Computer auf der Registerkarte *Energieverwaltung* so einstellen, dass er das Gerät abstellt, um Strom zu sparen, oder dass er von dem Gerät aktiviert wird. Außerdem können Sie auf der Registerkarte *Ereignisse* die aufgetretenen Ereignisse durchsehen, auf den Registerkarten *Details*, *Treiber* und *Allgemein* Informationen über den Adapter und die Treiber nachlesen und auf der Registerkarte *Erweitert* im Detail Konfigurationsoptionen überprüfen.

Konfigurieren des aufenthaltsortabhängigen Druckens

Benutzer werden immer mobiler. Das bedeutet, dass sie wahrscheinlich von verschiedenen Standorten aus Zugriff auf Netzwerke und Geräte brauchen. Drucker können in jeder Art von Netzwerk verfügbar sein, sei es in der Privatwohnung, im Büro oder in einem Kiosk-Computer der Firma. Allerdings ist es sehr umständlich, bei jeder Verbindung mit einem anderen Netzwerk einen Drucker auswählen zu müssen. Daher gibt es das aufenthaltsortabhängige Drucken. Dabei kann ein Benutzer für jeden Ort, an dem er sich aufhält, einen Standarddrucker festlegen (genauer gesagt, für jedes Netzwerk, mit dem er Verbindung aufnimmt). Dadurch wird auch verhindert, dass ein Benutzer versehentlich den falschen Drucker verwendet. Das kann wichtig werden, wenn die ausgedruckten Informationen vertraulich sind.

PRÜFUNGSTIPP

Für den aufenthaltsortabhängigen Druck müssen die Dienste *NlaSvc* (Network Location Awareness, NLA) und *Netprofm* (Netzwerklistendienst) ausgeführt werden. Ersterer sammelt und verwaltet Informationen über die Netzwerkverbindungen, Letzterer identifiziert das Netzwerk, mit dem der Computer verbunden ist. Überprüfen Sie, ob beide Dienste ausgeführt werden, falls das aufenthaltsortabhängige Drucken nicht funktioniert.

So konfigurieren Sie das aufenthaltsortabhängige Drucken:

1. Klicken Sie in der App *Einstellungen* auf *Geräte*, *Drucker & Scanner* und im unteren Teil der Seite auf *Geräte und Drucker*.
2. Klicken Sie auf einen Drucker und dann in der Menüleiste auf *Standarddrucker verwalten*.
3. Wählen Sie *Beim Ändern des Netzwerks den Standarddrucker ändern*.
4. Wählen Sie in der Liste *Netzwerk auswählen* das zu konfigurierende Netzwerk aus.
5. Wählen Sie in der Liste *Drucker auswählen* den Drucker aus, der bei einer Verbindung mit dem in Schritt 4 ausgewählten Netzwerk als Standarddrucker verwendet werden soll.
6. Klicken Sie auf *Hinzufügen*.

   Ihr neuer Eintrag erscheint als neue Konfiguration für den aufenthaltsortabhängigen Druck (Abbildung 4.7).

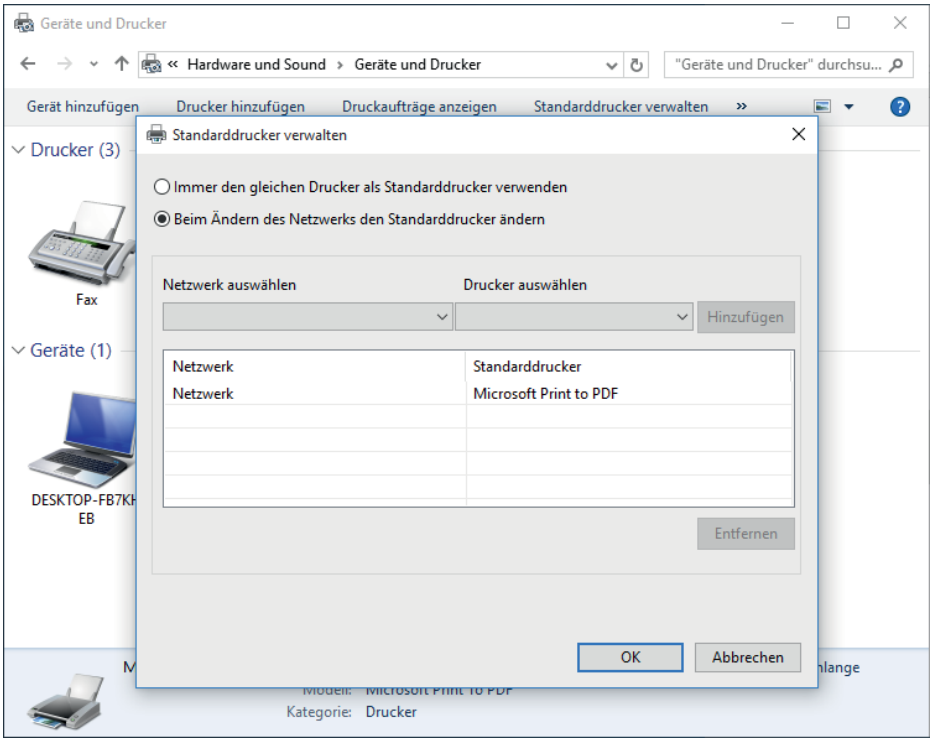

ABBILDUNG 4.7 Das Dialogfeld *Standarddrucker verwalten*

Gedankenexperiment

Aktivieren des Drucks in Drahtlosnetzwerken

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sie unterstützen einige mobile Computerbenutzer, für die es zum Arbeitsalltag gehört, in jedem Monat Verbindungen zu einem Dutzend verschiedener Drahtlosnetzwerke herzustellen und auf den dort verfügbaren Druckern etwas auszudrucken. Einige Benutzer haben sich darüber beschwert, dass sie die Drucker manuell auswählen müssen und dabei gelegentlich den falschen Drucker wählen. Das ist nicht nur ärgerlich, sondern auch ein Sicherheitsrisiko für Ihre Firma, weil die Dokumente vertraulich sind.

Außerdem stellen die Laptops der Benutzer automatisch Verbindungen zu Netzwerken her, die nicht mehr für die Arbeit erforderlich sind. Die Liste der Netzwerke ist ziemlich lang und Sie möchten die Einträge für die nicht mehr benötigten Netzwerke löschen. Manche Netzwerke sind deswegen nicht mehr erwünscht, weil sie eine schlechte Leistung aufweisen, beispielsweise Netzwerke von manchen Hotels oder bestimmten Konferenzräumen. Wo die Netzwerke keine gute Leistung bieten, sollen die Laptops auf mobiles Breitband ausweichen.

Beantworten Sie folgende Fragen:

1. **Welche Funktion aktivieren Sie auf den Windows 10-Laptops der Benutzer, um die Drucker festzulegen, die in den einzelnen Netzwerken als Standarddrucker verwendet werden sollen, und von welchen Diensten hängt diese Funktion ab?**
2. **Eine der Mitarbeiterinnen hat in einem bestimmen Hotel eine Verbindung zum kostenlosen WLAN-Netz des Hotels hergestellt. Was müssen Sie tun, um das Verbindungsprofil zu löschen, damit die Mitarbeiterin beim nächsten Aufenthalt in diesem Hotel mit dem mobilen Breitbandnetz arbeiten kann?**

Zusammenfassung der Lektion

- Es gibt verschiedene Methoden, eine Verbindung zu einem Drahtlosnetzwerk herzustellen, beispielsweise die Verwendung der Systemsteuerung. Der übliche Weg führt über das Netzwerksymbol rechts auf der Taskleiste.
- Es gibt eine Standardpriorität für die Netzwerke, mit denen ein Benutzer bisher Verbindungen hergestellt hat: Ethernet, WLAN und mobiles Breitband. Wenn zwei oder mehr Drahtlosverbindungen verfügbar sind, wählt Windows standardmäßig die Verbindung aus, die zuletzt verwendet wurde. Sie können Netzwerkverbindungen in der App *Einstellungen* oder mit dem Befehl `Netsh` verwalten.

- Für jede Netzwerkkarte stehen einige Konfigurationsoptionen zur Verfügung. Klicken Sie die Netzwerkkarte in *Netzwerkverbindungen* mit der rechten Maustaste an und wählen Sie aus dem Kontextmenü die gewünschte Option.
- Für den aufenthaltsortabhängigen Druck können Benutzer für jedes Netzwerk, mit dem sie eine Verbindung herstellen, einen Standarddrucker wählen

Lernzielkontrolle

Beantworten Sie folgende Fragen, um Ihr Wissen über den Stoff dieses Abschnitts zu überprüfen. Antworten auf diese Fragen und Erklärungen, warum die jeweilige Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Ein Benutzer hat folgende Verbindungen zur Verfügung: eine Ethernet-Verbindung, drei WLAN-Verbindungen und eine mobile Breitbandverbindung. Welche Verbindung wählt Windows 10 aus?
   - **A.** Ethernet
   - **B.** Die letzte Drahtlosverbindung, mit der eine Verbindung hergestellt wurde
   - **C.** Breitband
   - **D.** Der Benutzer wird zur Auswahl aufgefordert.
2. Sie müssen die erweiterten Eigenschaften eines Drahtlosadapters bearbeiten und die Einstellungen für die Optionen *AdHoc 11n* und *Empfangspuffer* ändern. Wo tun Sie dies? (Wählen Sie zwei Antworten aus. Jede gültige Antwort ist die Hälfte der Lösung.)
   - **A.** Sie klicken den Adapter im Fenster *Netzwerkverbindungen* mit der rechten Maustaste an und klicken auf *Eigenschaften*. Dann klicken Sie auf *Konfigurieren*.
   - **B.** Sie klicken den *WLAN*-Adapter im Fenster *Netzwerkverbindungen* mit der rechten Maustaste an und klicken auf *Eigenschaften*. Dann klicken Sie auf *Installieren*.
   - **C.** Sie klicken den *WLAN*-Adapter im Fenster *Netzwerkverbindungen* mit der rechten Maustaste an und klicken auf *Status*. Dann klicken Sie auf *Drahtloseigenschaften*.
   - **D.** Sie führen die Änderungen im Eigenschaftsdialogfeld des *WLAN*-Adapters auf der Registerkarte *Erweitert* durch.
3. Sie wollen mit dem Befehl `Netsh` ein Netzwerkprofil löschen. Welche der folgenden Aussagen über den Befehl `Netsh` ist korrekt? (Wählen Sie alle zutreffenden Antworten.)
   - **A.** Er muss in einer Windows PowerShell-Sitzung mit erhöhten Rechten eingegeben werden.
   - **B.** Er muss in einer Eingabeaufforderung eingegeben werden.
   - **C.** Er muss in einer Eingabeaufforderung mit erhöhten Rechten eingegeben werden.
   - **D.** Sie müssen die Parameter *wlan delete profile name=<Profilname>* verwenden.
   - **E.** Sie müssen die Parameter *wlan remove profile=<Profilname>* verwenden.

4. Ein Client muss eine Verbindung zu einem Drahtlosnetzwerk herstellen, dass seine SSID nicht aussendet. Wie können Sie eine Verbindung herstellen?
   - **A.** Sie verwenden den Befehl *netsh wlan add profile=<Profilname>*, um eine Verbindung zum Netzwerk herzustellen.
   - **B.** Sie verwenden im *Netzwerk- und Freigabecenter* die Option *Neue Verbindung oder neues Netzwerk einrichten*.
   - **C.** Sie klicken in der Taskleiste auf das Netzwerksymbol. Dann klicken Sie auf das Netzwerk, mit dem eine Verbindung hergestellt werden soll.
   - **D.** Sie öffnen das *Netzwerk- und Freigabecenter* und klicken auf *Probleme beheben*. Dann beheben Sie die Probleme mit der Netzwerkkarte und stellen eine Verbindung her, wenn Sie dazu aufgefordert werden.

Prüfungsziel 4.3: Konfigurieren und Verwalten der Netzwerksicherheit

Ein Windows 10-Computer ist durch Angriffe aus dem Netz vermutlich wesentlich stärker gefährdet als durch Angriffe, die von anderen Orten ausgehen. Angriffe aus dem Netzwerk können viele Computer zum Ziel haben und die Angreifer können sich irgendwo auf dieser Welt aufhalten, während andere Angriffsformen den physischen Zugang zum Computer voraussetzen. In diesem Abschnitt erfahren Sie etwas über Sicherheitsrisiken im Netzwerk und über die Maßnahmen, die man dagegen ergreifen kann.

Dieser Abschnitt deckt folgende Prüfungsziele ab:

- Konfigurieren von *Windows-Firewall*
- Konfigurieren von *Windows-Firewall mit erweiterter Sicherheit*
- Konfigurieren von Verbindungssicherheitsregeln mit IPsec
- Konfigurieren von Authentifizierungsausnahmen
- Konfigurieren der Netzwerkerkennung

Konfigurieren von Windows-Firewall

Windows-Firewall ist eine Softwarelösung, die in Windows 10 verfügbar ist und eine virtuelle Barriere zwischen dem lokalen Computer und dem Netzwerk errichtet, mit dem der Computer verbunden ist. Sinn dieser Barriere ist es, den lokalen Computer vor unerwünschtem eingehenden Datenverkehr zu schützen. Außerdem soll die Barriere das Netzwerk vor unerwünschtem Datenverkehr schützen, der vom lokalen Computer ausgeht. Die Firewall lässt es zu, dass bestimmte Daten im Computer eintreffen oder ihn verlassen, während andere Datenübertragungen blockiert werden. Es werden standardmäßig bestimmte Einstellungen vorgegeben, die sich aber ändern lassen. Diese Art von Schutz wird *Filterung* genannt. Bezugspunkte dieser Filter sind IP-Adressen, Anschlüsse (Ports) und Protokolle.

- IP-Adressen werden jedem Computer und jeder anderen Netzwerkressource zugewiesen, die direkt mit dem Netzwerk verbunden ist. Die Firewall kann Datenverkehr auf der Basis der IP-Adresse einer Ressource oder eines Adressenbereichs zulassen oder sperren.
- Portnummern sind bestimmten Anwendungen zugeordnet, die auf dem Computer ausgeführt werden, und identifizieren daher diese Anwendung. Port 21 ist zum Beispiel mit FTP (File Transfer Protocol) verknüpft, Port 25 mit SMTP (Simple Mail Transfer Protocol), Port 53 mit DNS, Port 80 mit HTTP (Hypertext Transfer Protocol) und Port 443 mit HTTPS (HTTP Secure).
- Protokolle legen die Art der Datenpakete fest, die gesendet und empfangen werden. Zu den gebräuchlichen Protokollen gehören TCP, Telnet, FTP, HTTP, POP3 (Post Office Protocol 3), IMAP (Internet Message Access Protocol), HTTPS und UDP (User Datagram Protocol). Sie sollten die gebräuchlichen Protokolle kennen, wenn Sie sich zur Prüfung anmelden.

Für die Firewall werden standardmäßig zwar eine ganze Reihe von Regeln definiert, aber Sie können Ihre eigenen Regeln für eingehenden und ausgehenden Datenverkehr definieren, um die Firewall an die Erfordernisse anzupassen. Im Verlauf dieses Kapitels erfahren Sie mehr darüber.

Überprüfen der Einstellungen für Windows-Firewall

Sie können den Zustand der Windows-Firewall in der Systemsteuerung überprüfen. Auf der Seite *Windows-Firewall* sehen Sie schnell, ob die Firewall aktiv ist oder nicht, welche eingehenden Verbindungen standardmäßig blockiert werden, welches das aktive Netzwerk ist und bei welchen Ereignissen Sie informiert werden. Um Änderungen vorzunehmen, klicken Sie im linken Bereich der Seite auf *Windows-Firewall ein- oder ausschalten*. Dort können Sie Einstellungen für private und öffentliche Netzwerke ändern. Für beide Netzwerktypen gibt es zwei Optionen:

- *Windows-Firewall aktivieren* (diese Einstellung ist standardmäßig vorgewählt)
  - *Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Apps*
  - *Benachrichtigen, wenn eine neue App von der Windows-Firewall blockiert wird* (diese Einstellung ist standardmäßig vorgewählt)
- *Windows-Firewall deaktivieren (nicht empfohlen)*

Als Netzwerkadministrator sind für Sie die Optionen im linken Bereich der Seite *Windows-Firewall* am interessantesten, insbesondere die Optionen *Eine App oder ein Feature durch die Windows-Firewall zulassen* und *Erweiterte Einstellungen*. Über *Erweiterte Einstellungen* erfahren Sie im nächsten Abschnitt mehr. Hier geht es nun darum, wie man den Datenverkehr für eine App zulässt, die standardmäßig von der Firewall blockiert wird.

Zulassen des Datenverkehrs einer App durch Windows-Firewall

Der Datenverkehr von bestimmten Apps durch Windows-Firewall wird bereits zugelassen. Um welche Apps es sich handelt, können Sie überprüfen, wenn Sie auf der Seite *Windows-Firewall* der Systemsteuerung auf *Eine App oder ein Feature durch die Windows-Firewall zulassen* klicken. In der Liste stehen viele Apps, die Sie vermutlich kennen, wie *Datei- und Druckerfreigabe*, *Microsoft Solitaire Collection*, *Windows-Karten*, *Groove-Musik* und *Windows Media Player* (Abbildung 4.8). Nachdem Sie auf *Einstellungen ändern* geklickt und ihre Genehmigung als Administrator gegeben haben, ist die Schaltfläche *Einstellungen ändern* nicht mehr zugänglich und Sie können die Optionen in der Liste ändern. Sie werden feststellen, dass viele Apps nicht standardmäßig zugelassen werden, wie der *Windows Media Player-Netzwerkfreigabedienst (Internet)*, die *Windows-Remoteverwaltung*, *Remoteherunterfahren* und so weiter.

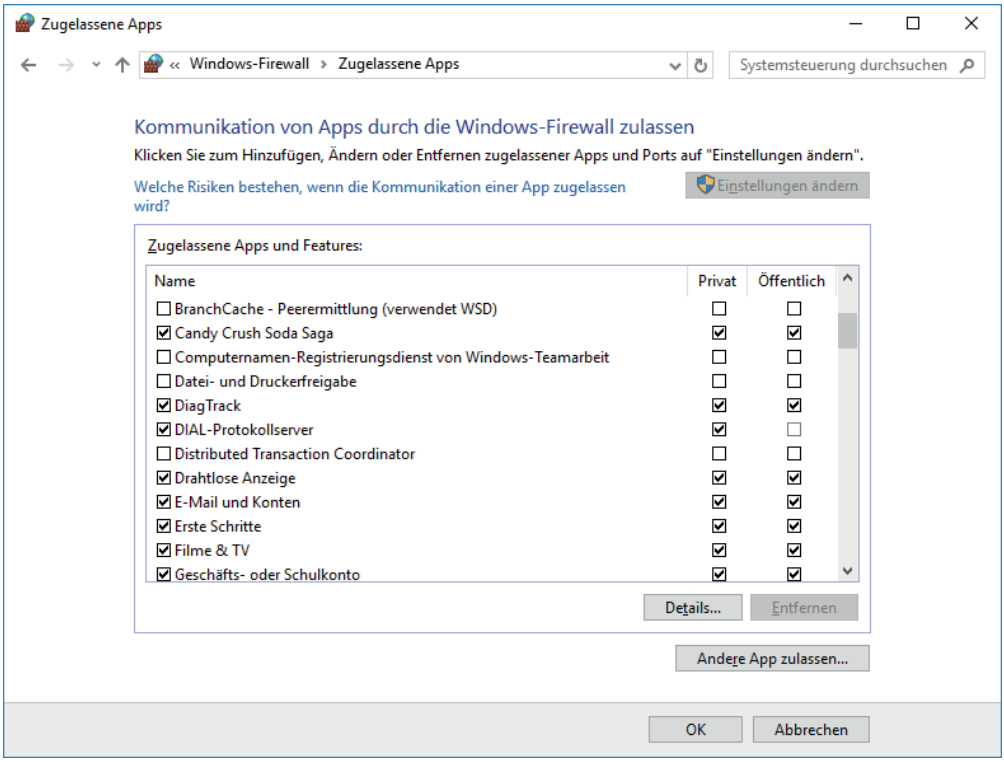

ABBILDUNG 4.8 Zugelassene Apps

Um den Datenverkehr einer App durch die Firewall zuzulassen oder zu blockieren, wählen Sie das entsprechende Kontrollkästchen unter dem Netzwerkprofil aus, für das die Einstellung vorgenommen werden soll. Wie Abbildung 4.8 zeigt, gibt es für jede App zwei Profile: *Privat* und *Öffentlich*. Wenn Sie die App nicht finden, für die Sie eine Einstellung vornehmen möchten, klicken Sie auf *Andere App zulassen*. Dann können Sie die gewünschte App im Dialogfeld *App hinzufügen* aussuchen.

Konfigurieren von Windows-Firewall mit erweiterter Sicherheit

Im Hauptfenster *Windows-Firewall* können Sie zwar einige Einstellungen vornehmen, aber die meisten Konfigurationsarbeiten erfolgen in *Windows-Firewall mit erweiterter Sicherheit*. Um dieses Fenster zu öffnen, klicken Sie im Fenster *Windows-Firewall* auf *Erweiterte Einstellungen* (Abbildung 4.9).

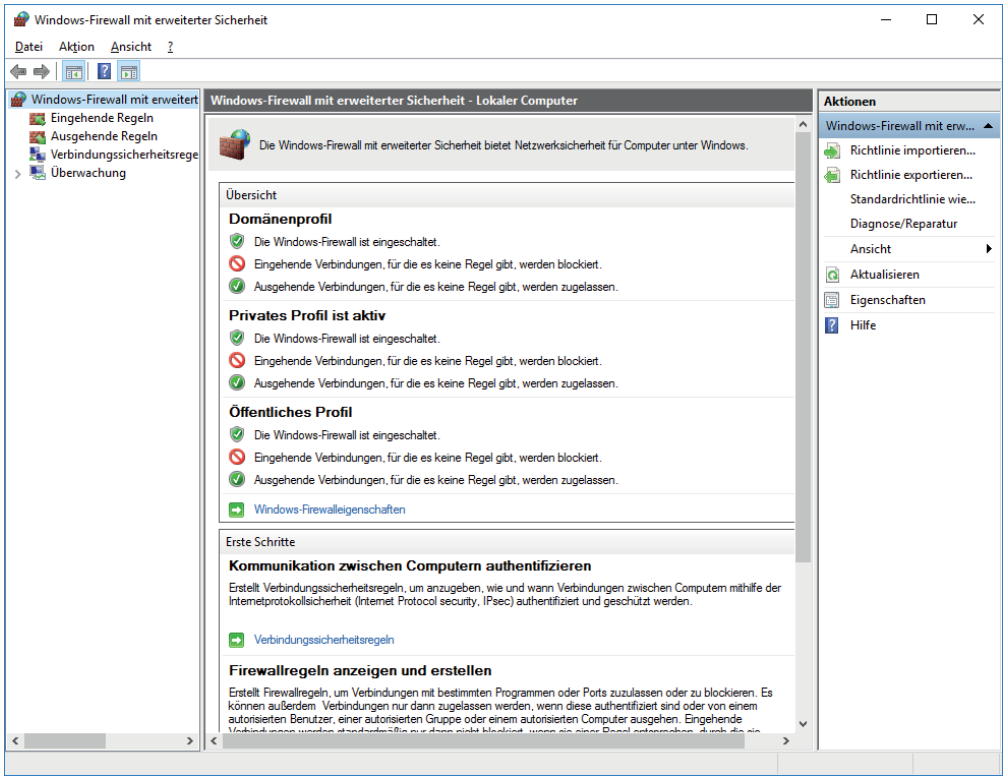

ABBILDUNG 4.9 Das Fenster *Windows-Firewall mit erweiterter Sicherheit*

Anschließend stehen mehrere Optionen zur Verfügung. Machen Sie sich mit den Begriffen vertraut, die auf dieser Seite verwendet werden.

- In der Konsolenstruktur im linken Bereich wählen Sie aus, was im mittleren Bereich und im Aktionsbereich angezeigt wird
  - **Eingehende Regeln** Listet alle konfigurierten eingehenden Regeln auf. Sie können diese Regeln in der Liste doppelt anklicken und nach Bedarf ändern. Manche Regeln sind vordefiniert und können zwar nicht geändert, aber deaktiviert werden. Wenn Sie die Zeit dafür haben, sollten Sie auch die anderen Knoten anklicken und untersuchen. Sie können auch im linken Bereich mit der rechten Maustaste auf *Eingehende Regeln* klicken und Ihre eigene Regel erstellen. Die verfügbaren Regeltypen sind *Programm*, *Port*, *Vordefiniert* und *Benutzerdefiniert*. Die Typen werden weiter hinten in diesem Abschnitt beschrieben.

- **Ausgehende Regeln** Hier stehen dieselben Optionen wie bei den eingehenden Regeln zur Verfügung, aber sie gelten für ausgehende Daten. Auch in diesem Fall können Sie *Ausgehende Regeln* im linken Bereich mit der rechten Maustaste anklicken und Ihre eigenen Regeln definieren.
- **Verbindungssicherheitsregeln** Verbindungssicherheitsregeln legen fest, wie sich Computer authentifizieren müssen, bevor Daten übertragen werden können. IPsec-Standards (Internet Protocol Security) legen fest, wie Daten bei ihrer Übertragung über ein TCP/IP-Netzwerk geschützt werden. Sie können einen entsprechenden Authentifizierungstyp für die Verbindung festlegen. Dann muss eine Authentifizierung erfolgen, bevor Daten übermittelt werden können. Über Verbindungssicherheitsregeln erfahren Sie im nächsten Abschnitt mehr.
- **Überwachung** Zeigt Informationen über das aktive Profil, den Firewallstatus und allgemeine Einstellungen für das private und öffentliche Profil

- Im rechten Bereich, dem Aktionsbereich, sehen Sie die Optionen, die für Ihre Auswahl im linken Bereich zur Verfügung stehen
  - **Richtlinie importieren oder exportieren, Standardrichtlinie wiederherstellen, Diagnose, Reparatur** Diese Aktionen ermöglichen Ihnen die Verwaltung der Einstellungen, die Sie für Ihre Firewall konfiguriert haben. Für Richtlinien wird die Dateinamenserweiterung *.wfw* verwendet.
  - **Neue Regel** Startet den entsprechenden Assistenten und ermöglicht Ihnen die Erstellung einer neuen Regel. Sie können den Assistenten auch im Menü *Aktion* starten.
  - **Filtern** Ermöglicht die Filterung der Regeln nach Domänenprofil, privatem oder öffentlichem Profil. Außerdem können Sie die Anzeige nach Status filtern (*Aktiviert*, *Deaktiviert*) und nach Gruppe. Verwenden Sie eine passende Filterung, um nur die Regeln anzuzeigen, die Sie sehen möchten.
  - **Ansicht** Ermöglicht die Anpassung der Konsole und der Spalten, die im mittleren Bereich der Konsole *Windows-Firewall mit erweiterter Sicherheit* angezeigt werden

Wenn Sie eine neue eingehende oder ausgehende Regel erstellen, haben Sie die Wahl unter vier Regeltypen. Ein Assistent unterstützt Sie bei der Erstellung. Der genaue Ablauf hängt vom Typ der Regel ab. Folgende Regeltypen stehen zur Wahl:

- **Programm** Eine Programmregel legt das Verhalten der Firewall für ein bestimmtes Programm fest, das Sie auswählen, oder für alle Programme, die die festgelegten Bedingungen erfüllen. Sie können zwar keine Apps kontrollieren, aber herkömmliche EXE-Dateien konfigurieren. Nach der Auswahl des Programms können Sie die Verbindung zulassen oder blockieren, oder Sie legen fest, dass eine Verbindung nur zugelassen wird, wenn die Verbindung sicher ist und eine Authentifizierung mit IPsec erfolgt. Sie können auch die Profile auswählen, für die die Regel gelten soll (*Domäne*, *Privat* oder *Öffentlich*), und der Regel einen Namen geben (Abbildung 4.10).
- **Port** Eine Portregel legt das Verhalten für TCP- und UDP-Ports fest und gibt an, welche Ports zugelassen oder gesperrt sind. Eine Regel kann für alle Ports gelten oder sich auf ausgewählte Ports beschränken. Wie bei anderen Regeln können Sie eine Verbin-

dung zulassen oder blockieren oder Sie legen fest, dass eine Verbindung nur zugelassen wird, wenn die Verbindung mit IPsec geschützt ist. Sie können auch die Profile auswählen, für die die Regel gelten soll (*Domäne*, *Privat* oder *Öffentlich*), und der Regel einen Namen geben.

> ***WEITERE INFORMATIONEN*** **Verbindungen und Sicherheit**
>
> **Wenn Sie eingehende und ausgehende Regeln erstellen und dabei festlegen, dass eine Verbindung nur zugelassen wird, wenn sie sicher ist und eine Authentifizierung mit IPsec erfolgt, wird die Verbindung entsprechend den IPsec-Einstellungen und den anwendbaren Regeln im Knoten *Verbindungssicherheitsregeln* geschützt. Die Erstellung von Verbindungssicherheitsregeln wird im nächsten Abschnitt beschrieben.**

- **Vordefiniert** Legt das Verhalten der Firewall für ein Programm oder einen Dienst fest, den Sie aus einer Liste mit Regeln auswählen, die für Windows vordefiniert wurden
- **Benutzerdefiniert** Eine Regel, die Sie von Grund auf neu definieren, wobei Sie jeden Aspekt der Regel festlegen. Verwenden Sie diesen Regeltyp, wenn die ersten drei Regeltypen nicht zum gewünschten Ergebnis führen.

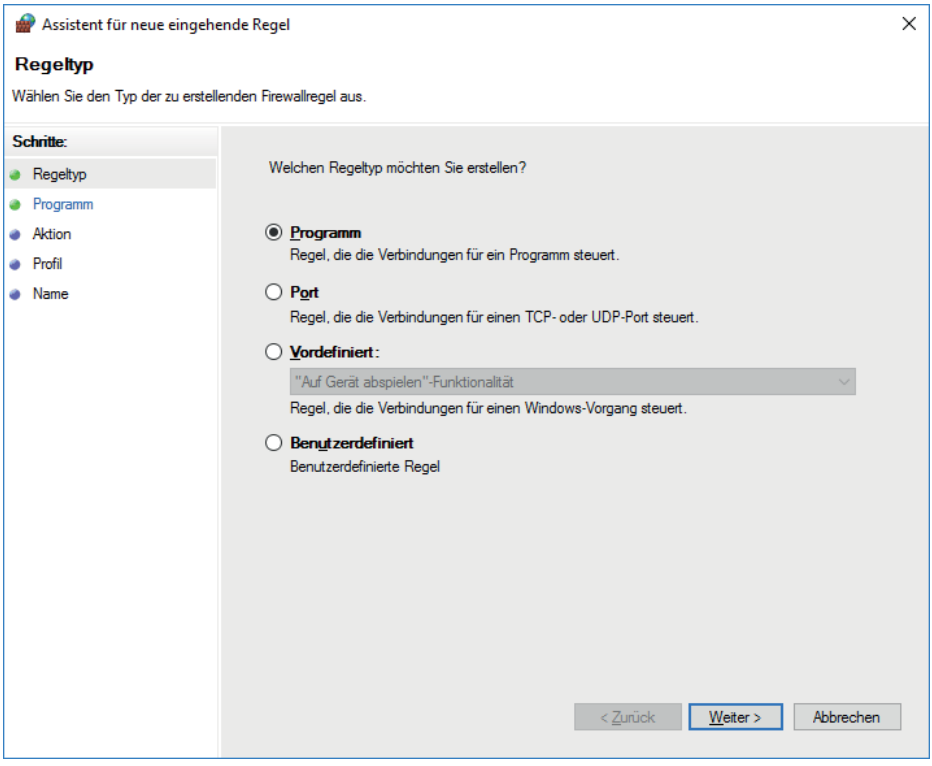

ABBILDUNG 4.10 Der *Assistent für neue eingehende Regeln*

PRÜFUNGSTIPP

In der Prüfung wird vielleicht nach der Erstellung von Regeln gefragt. Daher sollten Sie sich die Zeit nehmen und mit dem Assistenten einige Regeln erstellen, damit Sie mit dem Vorgang vertraut werden.

Wählen Sie im linken Bereich den Knoten *Windows-Firewall mit erweiterter Sicherheit* und klicken Sie im mittleren Bereich am unteren Ende des Abschnitts *Übersicht* auf *Windows-Firewalleigenschaften*. Dann öffnet sich das Eigenschaftsdialogfeld der Firewall (Abbildung 4.11). Dort können Sie Einstellungen an der Firewall und den Profilen vornehmen, selbst wenn Ihr Computer nicht mit dem Netzwerktyp verbunden ist, den Sie konfigurieren möchten.

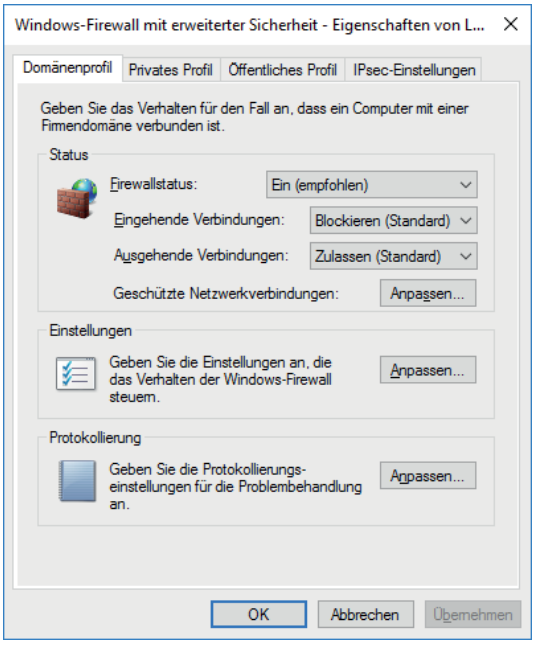

ABBILDUNG 4.11 Das Eigenschaftsdialogfeld von *Windows-Firewall mit erweiterter Sicherheit*

In Abbildung 4.11 ist die Registerkarte *Domänenprofil* gewählt. Wenn Sie möchten, können Sie die Firewall so konfigurieren, dass sie bei der Verbindung mit einem Domänennetzwerk ausgeschaltet ist. Außerdem können Sie die Einstellungen für das öffentliche Profil verschärfen und die Einstellungen für das private Profil anpassen. Schließlich können Sie auf der Registerkarte *IPsec-Einstellungen* die *IPsec-Standardeinstellungen*, *IPsec-Ausnahmen* und *IPsec-Tunnelautorisierung* anpassen. Sehen Sie sich alle Bereiche dieses Dialogfelds genauer an und machen Sie sich mit allen Begriffen vertraut, die Sie noch nicht kennen.

Konfigurieren von Verbindungssicherheitsregeln mit IPsec

Sie können mit IPsec die Geheimhaltung und Integrität der Daten beim Transport über ungesicherte Kanäle schützen und zudem eine Authentifizierung verlangen. Ursprünglich hatte IPsec den Zweck, den Datenverkehr über öffentliche Netzwerke zu schützen, aber viele Organisationen verwenden IPsec auch, um Schwächen in ihren privaten Netzwerken zu begegnen, die sonst ausgenutzt werden können.

Wenn Sie IPsec entsprechend implementieren, bietet es einen privaten Übertragungskanal für sensible oder vertrauliche Daten, sei es für E-Mails, FTP-Übertragungen, Nachrichtenfeeds, Übertragungen zu Partnern und Lieferanten, medizinische Akten oder beliebige andere Datenarten, die sich mit TCP/IP übertragen lassen. IPsec hat folgende Vorteile:

- Es bietet eine gegenseitige Authentifizierung vor und während der Kommunikation
- Es zwingt beide Kommunikationspartner, sich bei der Kommunikation gegenseitig zu identifizieren
- Es bietet durch die Verschlüsselung des IP-Datenverkehrs eine hohe Sicherheit

Grundlagen der Verbindungssicherheitsregeln

Eine Verbindungssicherheitsregel fordert eine Authentifizierung der beiden Kommunikationspartner, bevor eine Verbindung hergestellt und Daten übertragen werden können. *Windows-Firewall mit erweiterter Sicherheit* verwendet IPsec, um folgende Regeltypen anzubieten:

- **Isolation** Eine Isolationsregel isoliert Computer durch die Beschränkung von Verbindungen auf der Basis von Anmeldeinformationen wie Domänenmitgliedschaft oder Integritätsstatus. Isolationsregeln ermöglichen die Umsetzung einer Isolierungsstrategie für Server oder Domänen.
- **Authentifizierungsausnahme** Sie können eine Authentifizierungsausnahme verwenden, um Verbindungen zu kennzeichnen, die keine Authentifizierung erfordern. Die entsprechenden Computer geben Sie durch eine IP-Adresse an, durch einen IP-Adressbereich, durch ein Subnetz oder durch einen vordefinierten Computersatz, beispielsweise *Standardgateway*.
- **Server-zu-Server** Dieser Regeltyp schützt gewöhnlich Verbindungen zwischen Servern. Bei der Erstellung der Regel geben Sie die Endpunkte im Netzwerk an, zwischen denen die Kommunikation geschützt werden soll. Anschließend legen Sie die Authentifizierungsanforderungen und die Authentifizierungsmethode fest, die verwendet werden soll.
- **Tunnel** Diese Regel ermöglicht den Schutz von Verbindungen zwischen Gatewaycomputern. Sie wird gewöhnlich zum Schutz von Internet-Verbindungen zwischen zwei Sicherheitsgateways verwendet.
- **Benutzerdefiniert** Es können sich Situationen ergeben, in denen sich die erforderlichen Authentifizierungsregeln nicht mit den Regeln konfigurieren lassen, die im *Assistenten für neue Verbindungssicherheitsregeln* verfügbar sind. Dann können Sie eine benutzerdefinierte Regel für die Authentifizierung der Verbindung zwischen zwei Endpunkten erstellen.

Firewallregeln und Verbindungssicherheitsregeln

Firewallregeln ermöglichen den Datenverkehr durch eine Firewall, aber sie schützen nicht den Datenverkehr. Um den Datenverkehr mit IPsec zu schützen, können Sie Verbindungssicherheitsregeln erstellen. Allerdings ermöglicht eine Verbindungssicherheitsregel keinen Datenverkehr durch eine Firewall. Dazu müssen Sie eine entsprechende Firewallregel erstellen, wenn die Firewall den Datenverkehr nicht zulässt. Verbindungssicherheitsregeln gelten nicht für Programme und Dienste. Sie gelten nur zwischen den beiden Computern an den Enden der Verbindung.

PRÜFUNGSTIPP

Verbindungssicherheitsregeln legen fest, wann und wie eine Authentifizierung erfolgt, aber sie ermöglichen noch keine Kommunikation durch die Firewall. Um die Verbindung zuzulassen, müssen Sie eine entsprechende eingehende oder ausgehende Regel erstellen. Bei der Erstellung der eingehenden oder ausgehenden Regel geben Sie die Bedingungen für die Verbindung an, beispielsweise eine Authentifizierung mit IPsec. Wenn Sie dies tun, werden die Verbindungen entsprechend der IPsec-Einstellungen und Regeln im Knoten *Verbindungssicherheit* geschützt.

Konfigurieren von Authentifizierungsausnahmen

Wenn Sie eine Regel konfigurieren, die Datenverkehr zwischen den beteiligten Computer nur zulässt, wenn die Verbindung mit IPsec geschützt ist, erstellen Sie eine Authentifizierungsausnahme. Sie konfigurieren diese Option auf der Seite *Aktion* des Assistenten für die neue Regel, wenn Sie eine eingehende oder ausgehende Regel erstellen. Wenn Sie auf der Seite *Aktion* die Option *Verbindung zulassen, wenn sie sicher ist* wählen, legen Sie fest, dass die Verbindung mit den IPsec-Einstellungen und Regeln im Knoten *Verbindungssicherheitsregel* zugelassen wird.

So erstellen Sie zum Beispiel eine eingehende Regel, die für einen einzelnen TCP-Port gilt (Telnet, Port 23), und erstellen eine Authentifizierungsausnahme dafür:

1. Wählen Sie in *Windows-Firewall mit erweiterter Sicherheit* den Knoten *Eingehende Regeln* und klicken Sie den Knoten mit der rechten Maustaste an.
2. Klicken Sie auf *Neue Regel*.
3. Wählen Sie als Regeltyp *Port* und klicken Sie auf *Weiter*.
4. Lassen Sie auf der Seite *Protokolle und Ports* die Option *TCP* gewählt und geben Sie im Eingabefeld *Bestimmte lokale Ports* die Zahl **23** ein. Klicken Sie auf *Weiter*.
5. Wählen Sie die auszuführende Aktion *Verbindung zulassen, wenn sie sicher ist*, und klicken Sie auf *Weiter*.
6. Um autorisierte Benutzer oder Ausnahmen zu konfigurieren, wählen Sie das entsprechende Kontrollkästchen, klicken auf *Hinzufügen* und wählen die gewünschten Einträge im Dialogfeld *Benutzer oder Gruppen auswählen* aus. Klicken Sie auf *Weiter*.
7. Legen Sie die gewünschten autorisierten Computer und Ausnahmen fest. Dabei gehen Sie ähnlich wie im vorigen Schritt vor. Klicken Sie auf *Weiter*.

8. Wählen Sie die Profile aus, in denen die Regel gelten soll. Klicken Sie auf *Weiter*. Geben Sie der Regel einen Namen. Klicken Sie auf *Fertig stellen*.

> ***WICHTIG*** **Vorbereitung auf die Prüfung**
>
> **Dieses Buch behandelt die Prüfungsziele, die für diese Prüfung festgelegt wurden. Auf der entsprechenden Seite von Microsoft für diese Prüfung heißt es: »Bitte beachten Sie, dass sich die Prüfungsfragen auf die Themen in den nachfolgenden Aufzählungen beziehen, jedoch nicht darauf beschränkt sind«.**
>
> **Das bedeutet, dass auch Fragen zu Themen gestellt werden können, die wir nicht behandeln, und wir können uns beim besten Willen nicht vorstellen, worum es sich handeln könnte. Ein kleines Beispiel: Vielleicht werden Sie über die verschiedenen Arten der Authentifizierung im WLAN gefragt, wie TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption System) und die verschiedenen WPA-Methoden (Wi-Fi Protected Access). Vielleicht tauchen auch Fragen auf, zu deren Beantwortung Sie bestimmte Dateinamenserweiterungen kennen müssen, beispielsweise WFW. Das ist der Dateityp, der beim Export einer Windows-Firewall-Richtlinie verwendet wird. Vielleicht wird auch noch erwartet, dass Sie etwas über BranchCache oder DirectAccess wissen.**

Konfigurieren der Netzwerkerkennung

Standardmäßig ist die Netzwerkerkennung für private Netzwerke und Domänennetzwerke aktiviert und für öffentliche Netzwerke deaktiviert. Sie ermöglicht es einem Computer, andere Computer in einem Netzwerk zu finden. Außerdem wird der Computer für andere Computer im Netzwerk sichtbar. Das ist völlig in Ordnung, wenn das Netzwerk vertrauenswürdig ist, aber es ist keine gute Idee, wenn man dem Netzwerk nicht trauen kann. Da diese und andere Einstellungen für die verschiedenen Netzwerktypen automatisch konfiguriert werden, wie auch die entsprechenden Einstellungen für Ports und Protokolle, braucht der Netzwerkadministrator nicht jeden Aspekt einer Verbindung manuell zu konfigurieren.
Es gibt eine Besonderheit. Selbst wenn die Netzwerkerkennung deaktiviert ist, kann ein Windows 10-Computer trotzdem eine Verbindung zu Netzwerkressourcen herstellen, wenn der Benutzer die Namen und Pfade dieser Ressourcen kennt (er muss sie kennen, weil sie im Datei-Explorer nicht zu finden sind).

Es ist möglich, die Konfiguration der Netzwerkerkennung im *Netzwerk- und Freigabecenter* zu ändern:

1. Öffnen Sie das *Netzwerk- und Freigabecenter*.
2. Klicken Sie im linken Bereich auf *Erweiterte Freigabeeinstellungen ändern*.
3. Klicken Sie auf den nach unten gerichteten Pfeil neben dem Netzwerktyp, in dem Sie die Einstellung ändern möchten: *Privat* oder *Gast oder Öffentlich*.
4. Nehmen Sie die gewünschte Einstellung für die Netzwerkerkennung vor. Beachten Sie die anderen Optionen (Abbildung 4.12).
5. Klicken Sie auf *Änderungen speichern*.

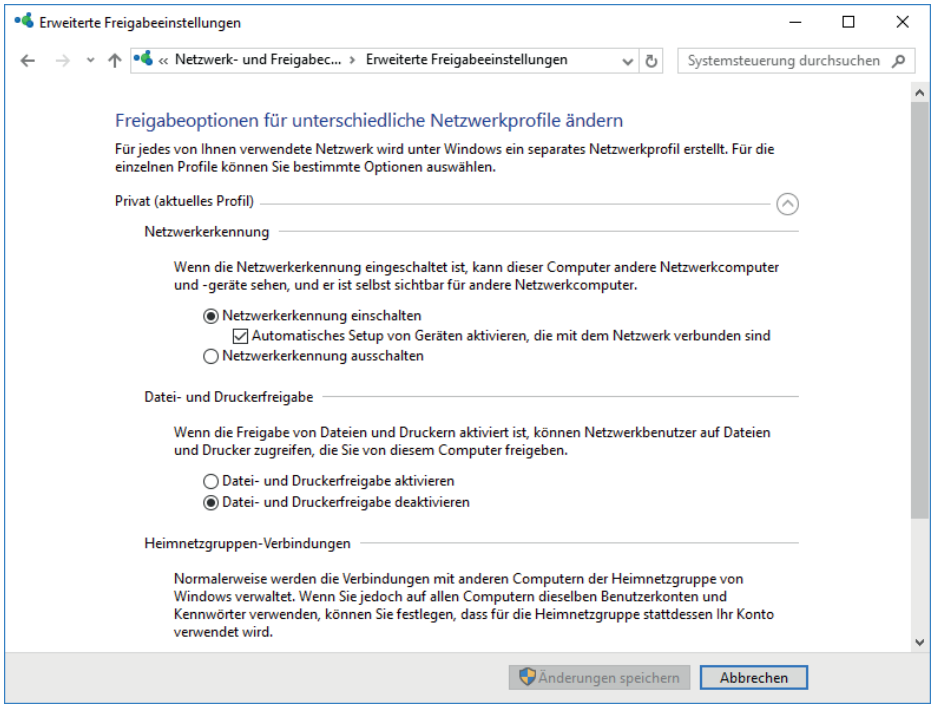

ABBILDUNG 4.12 *Erweiterte Freigabeeinstellungen*

Gedankenexperiment

Konfigurieren der Firewall auf Mobilgeräten

Im folgenden Gedankenexperiment wenden Sie an, was Sie über dieses Prüfungsziel wissen. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ein Kunde hat eine große Medienbibliothek mit Tausenden von Musikdateien angesammelt. Er möchte über das Internet auf diese Dateien zugreifen können, damit er die Musik in seinem Büro auf einem Computer abspielen kann. Er hat auf beiden Computern die entsprechenden Optionen im Media Player aktiviert. Allerdings funktioniert die Übertragung nicht.

1. Was müssen Sie in der Firewall tun, damit der Media Player Musikdateien über das Internet übertragen kann?
2. Führen Sie die erforderlichen Arbeiten in *Windows-Firewall* oder in *Windows-Firewall mit erweiterter Sicherheit* durch?
3. Müssen Sie dafür als Administrator angemeldet sein?

Zusammenfassung der Lektion

- In *Windows-Firewall* können Sie die Einstellungen für private und öffentliche Netzwerke überprüfen und einige Grundeinstellungen vornehmen. Außerdem können Sie die Firewall dort deaktivieren.
- In *Windows-Firewall* wird der Datenverkehr von Anwendungen entweder zugelassen oder blockiert. Sie können Ausnahmen erstellen, damit der Datenverkehr von bestimmten Anwendungen die Firewall durchlaufen kann.
- *Windows-Firewall mit erweiterter Sicherheit* bietet Administratoren wesentlich mehr Optionen. Sie können ihre eigenen eingehenden und ausgehenden Regeln sowie Verbindungssicherheitsregeln konfigurieren, Authentifizierungsausnahmen einrichten und die Einstellungen der Firewall ändern.
- Auf der Seite *Erweiterte Freigabeeinstellungen* der Systemsteuerung können Sie die Konfiguration der Netzwerkerkennung für die verfügbaren öffentlichen und privaten Profile ändern.

Lernzielkontrolle

Beantworten Sie folgende Fragen, um Ihr Wissen über den Stoff dieses Abschnitts zu überprüfen. Antworten auf diese Fragen und Erklärungen, warum die jeweilige Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche Art von Authentifizierung muss durchgeführt werden, damit Daten übertragen werden können, wenn Sie in *Windows-Firewall mit erweiterter Sicherheit* eine eingehende oder ausgehende Regel erstellen und auf der Seite *Aktion* des Assistenten für neue Regeln die Option *Verbindung zulassen, wenn sie sicher ist* wählen?
   - **A.** Verbindungen müssen mit IPsec authentifiziert werden und Nullkapselung verwenden.
   - **B.** Verbindungen können mit IPsec geschützt werden, müssen es aber nicht.
   - **C.** Die Verbindungen sind vertraulich und müssen daher verschlüsselt werden.
   - **D.** Verbindungen werden entsprechend der Einstellungen in den IPsec-Eigenschaften und Regeln im Knoten *Verbindungssicherheitsregel* geschützt.
2. Wofür können Sie eine Isolationsregel verwenden, wenn Sie in *Windows-Firewall mit erweiterter Sicherheit* eine Verbindungssicherheitsregel erstellen? (Wählen Sie alle zutreffenden Antworten.)
   - **A.** Sie können Verbindungen auf der Basis von Domänenmitgliedschaften einschränken.
   - **B.** Sie können Verbindungen auf der Basis des Integritätsstatus des Computers einschränken.
   - **C.** Sie können verlangen, dass ein Tunnel eingerichtet wird.
   - **D.** Sie können die Regel verwenden, um ein Subnetz auf der Basis der IP-Adressen zu isolieren.

3. Wo deaktivieren Sie die Netzwerkerkennung für das private Netzwerkprofil?
   - **A.** Im *Netzwerk- und Freigabecenter* unter *Adaptereinstellungen*
   - **B.** In *Windows-Firewall* unter *Erweiterte Einstellungen*
   - **C.** Im *Netzwerk- und Freigabecenter* unter *Erweiterte Freigabeeinstellungen*
   - **D.** Im Eigenschaftsdialogfeld, das sich mit einem Klick auf *Windows-Firewalleigenschaften* in *Windows-Firewall mit erweiterter Sicherheit* öffnen lässt
4. Wo können Sie sich eine Liste der aktiven Firewallregeln ansehen?
   - **A.** Im *Netzwerk- und Freigabecenter* unter *Adaptereinstellungen*
   - **B.** In *Windows-Firewall* unter *Erweiterte Einstellungen*
   - **C.** Im *Netzwerk- und Freigabecenter* unter *Erweiterte Einstellungen*
   - **D.** In *Windows-Firewall mit erweiterter Sicherheit* unter der Option *Überwachung*