Windows Server 2019

Erweiterte Netzwerkadministration

Thomas Joos, Martin Dausch

1. Ausgabe, Mai 2019

ISBN 978-3-86249-852-9

W2019EN

HERDT

Impressum

Matchcode: W2019EN

Autoren: Thomas Joos, Martin Dausch

Produziert im HERDT-Digitaldruck

1. Ausgabe, Mai 2019

HERDT-Verlag für Bildungsmedien GmbH
Am Kümmerling 21–25
55294 Bodenheim
Internet: www.herdt.com
E-Mail: info@herdt.com

1

Informationen zu diesem Buch

1.1 Voraussetzungen und Ziele

Zielgruppe

- Systembetreuer und Administratoren, die ihre Kenntnisse von älteren Microsoft Serverversionen auf Windows Server 2019 upgraden möchten
- Netzwerkadministratoren, die ein Netzwerk unter Windows Server 2019 planen, einrichten und administrieren möchten
- Alle, die ihre Zertifizierungen auf Windows Server 2019 aktualisieren möchten

Empfohlene Vorkenntnisse

Bei den Kursteilnehmern werden Kenntnisse in den folgenden Bereichen vorausgesetzt:

- Netzwerkadministration mit Windows Server 2019
  (HERDT-Buch *Windows Server 2019 – Netzwerkadministration*)
- Netzwerkgrundkenntnisse (HERDT-Buch *Netzwerke – Grundlagen*)

Lernziele

Dieses Buch vermittelt Ihnen erweiterte Kenntnisse im Umgang mit Diensten und der Infrastruktur eines Windows-Server-2019-Netzwerks.

Hinweise zu Soft- und Hardware

Für den Aufbau der Testumgebung, die diesem Buch zugrunde liegt, benötigen Sie einen Computer mit folgender Hard- und Software:

Computer	Einen 64-Bit-Computer mit mindestens 8 GB Hauptspeicher und mindestens 200 GB freier Festplattenkapazität. Die Systeme sollten von DVD-ROM oder USB booten können. Für die Virtualisierung mit Hyper-V muss das System über die Virtualisierungsfunktion AMD-V bzw. Intels VT-x verfügen. Sowohl die CPU als auch das BIOS müssen diese Funktion beherrschen. Alle Computer müssen für Windows Server 2019 geeignet sein.
Software	Installationsdatenträger Windows Server 2019 (DVD, ISO-Abbild oder bootfähiger USB-Stick)

1.2 Netzwerk in der Testumgebung

Testumgebung mit einem Hostserver und bis zu fünf virtuellen Maschinen

Die Testumgebung sieht die Einrichtung eines Hostsystems unter Windows Server 2019 vor, auf dem dann über Hyper-V fünf virtuelle Maschinen aufgesetzt werden. Der Host ist dabei nicht Teil der virtuellen Firma und auch kein Domänenmitglied.

Es ist möglich, ein anderes Betriebssystem wie z. B. Linux oder macOS für den Host zu verwenden und Virtualisierungssoftware von anderen Herstellern (z. B. VMware oder VirtualBox von Oracle) einzusetzen. Diese Alternativen werden jedoch im Buch nicht beschrieben.

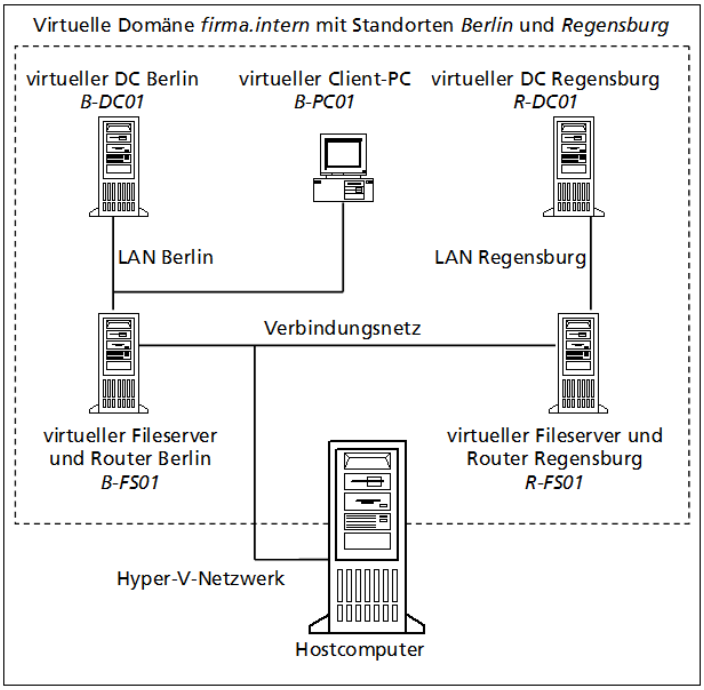
Dieses Buch baut zum Teil auf der Umgebung auf, die Sie beim Durcharbeiten des HERDT-Buches *Windows Server 2019 – Netzwerkadministration* erstellt haben. Neben dem Standort Berlin wird in diesem Buch ein zweiter Standort Regensburg eingerichtet. Jeder Standort verfügt über einen DC und einen Fileserver, der außerdem das Routing zwischen den Standorten übernimmt.

Die Testumgebung wird Schritt für Schritt aufgebaut:

- Installation des Hosts und Hinzufügen der Serverrolle *Hyper-V*
- Installation des Berliner Domänencontrollers *B-DC01*
- Einrichtung der Domäne *firma.intern*
- Einrichtung der Standorte und Subnetze
- Installation des Berliner Routers und Fileservers *B-FS01*
- Installation des Regensburger Domänencontrollers *R-DC01*
- Installation des Regensburger Routers und Fileservers *R-FS01*
- Installation eines Windows-8.1-Clients

Sie können die Server *B-DC01* und *B-FS01* aus der Testumgebung des HERDT-Buchs *Windows Server 2019 – Netzwerkadministration* weiter verwenden. Bevor Sie dies tun, müssen Sie jedoch den zweiten Domänencontroller *B-DC02* ordnungsgemäß zurückstufen und dann aus dem Active Directory entfernen.

Eine sinnvolle Alternative ist die Verwendung von Snapshots, die angefertigt wurden, bevor die Server zum Mitglied einer Domäne oder zum DC gemacht wurden. Auf diese Weise sparen Sie sich die Neuinstallation und vermeiden Probleme mit dem AD und den DNS.



Testumgebung mit vier virtuellen Servern und einem Client

Namenskonventionen im Schulnetz

Falls Sie Ihre Testumgebung im Rahmen einer Schulung erstellen, richten Sie sich bei der Wahl von Standorten und IP-Adressen nach den Vorgaben Ihres Kursleiters.

Vorschläge für die Testumgebung

Die virtuellen Umgebungen ermöglichen es jedem Kursteilnehmer, eine identische Versuchsumgebung aufzubauen. Dabei gibt es Folgendes zu bedenken:

- Alle Teilnehmer sollten bei der Namensvergabe dasselbe Schema benutzen. Durch die konsequente Bezeichnung können alle Ressourcen stets eindeutig zugeordnet werden.
- Halten Sie den Aufbau der Testumgebung einfach. Eine komplizierte Umgebung schafft zusätzliche Fehlerquellen.
- Im Buch wird die Domäne *firma.intern* heißen. Jeder Teilnehmer sollte jedoch als Domänennamen seinen Firmennamen, Nachnamen oder einen anderen Namen verwenden, der im Schulungsnetzwerk einmalig ist. Befolgen Sie bei der Auswahl des Domänennamens die Vorgaben des Kursleiters.
- Achten Sie darauf, dass der Domänenname den Bestandteil *intern* enthält, z. B. *firma.intern*. Da die Domäne *intern* nicht im Internet-DNS registriert werden kann, handelt es sich automatisch um einen internen Domänennamen für das firmeneigene Netzwerk.
- Beachten Sie die Namenskonventionen. Ein Rechnername sollte maximal 15 Zeichen umfassen. Benennen Sie in Hyper-V die virtuellen Maschinen nach dem Schema *V-<Name des virtuellen Servers>*. So können Sie am Fenstertitel sofort erkennen, in welcher VM Sie sich gerade befinden.

1.3 Namensgebung in diesem Buch

In diesem Buch wird auf eine durchgehende Bezeichnungsweise geachtet. Alle Bezeichnungen sollen **aussagekräftige Namen** sein, aus denen die Funktion hervorgeht. Das mag zunächst aufwendig und kompliziert erscheinen. Wenn Sie jedoch einmal mit einem fremden Active Directory oder Skript arbeiten müssen, werden Sie für eindeutige Bezeichnungen sehr dankbar sein. Wenn Sie das nachfolgend beschriebene Schema anwenden, können Sie alleine durch die Bezeichnung erkennen, ob es sich um einen Rechnernamen, eine Gruppe oder eine Organisationseinheit handelt, egal in welchem Kontext Sie das Objekt vorfinden.

Am Anfang einer Bezeichnung muss das wichtigste Ordnungsmerkmal stehen, das in einer alphabetisch geordneten Liste dafür sorgt, dass zusammengehörige Einträge auch zusammen aufgeführt werden. Bei Computernamen ist dies der Standort, währen es bei Gruppen, Organisationseinheiten und Ressourcen sinnvoller ist, sie nach ihrer Funktion zu benennen. Sie können diese Kriterien selbst festlegen, wichtig ist vor allem, dass dabei eine sinnvolle Hierarchie entsteht, an die Sie sich stets halten.

Bindestriche als Trennzeichen

Alle Bezeichnungen werden aus mehreren Bestandteilen zusammengesetzt, die jeweils mit einem Bindestrich (bzw. einem Minuszeichen) voneinander getrennt werden. Verwenden Sie wenn möglich **innerhalb** eines Namensbestandteils keine Minuszeichen.

Keine Leerzeichen

Ersetzen Sie alle Leerzeichen in Bezeichnungen und Namensbestandteilen durch einen Unterstrich. Dadurch sehen Sie auf einen Blick, wo ein Element aufhört und das nächste anfängt, außerdem können Sie so in der Eingabeaufforderung oder der PowerShell und in Skripten auf Anführungszeichen verzichten.

Keine Umlaute

Verzichten Sie grundsätzlich auf die Verwendung von Umlauten und Sonderzeichen, denn so haben Sie auch in internationalen Umgebungen keine Probleme.

Benutzernamen

Die Anmeldenamen werden durch den Anfangsbuchstaben des Vornamens und den vollen Nachnamen gebildet. Dabei wird auf Umlaute und Sonderzeichen verzichtet.

Autokennzeichen als Standortkürzel

Für die Kennzeichnung des Standorts wird jeweils das Autokennzeichen der Stadt verwendet, also B für Berlin und R für Regensburg.

Rechnernamen

Alle Rechnernamen beginnen mit dem Standortkürzel. Danach kommt eine Abkürzung für die Hauptfunktion des Servers: **DC** für Domain Controller, **FS** für Fileserver und **RDS** für Remotedesktopservices, direkt gefolgt von einer zweistelligen laufenden Nummer. Dabei ergeben sich Bezeichnungen wie z. B. *B-DC02*, *R-FS01* oder *HB-DC01*. Clientcomputer werden z. B. als *B-**PC**01* benannt.

Durch das Voranstellen des Standortnamens werden alle Computer am Standort in einer alphabetisch geordneten Liste zusammenhängend angezeigt. Durch die fortlaufende Nummerierung werden automatisch alle Rechner mit der gleichen Hauptfunktion (DC, FS usw.) an einem Standort untereinander angezeigt.

Namen der virtuellen Maschinen

Die VMs tragen den Namen des virtuellen Computers mit vorangestelltem V für virtuell, z. B. *V-B-DC01 oder V-R-FS01*. Dadurch können die Hyper-V-VMs von den Servern in der Testumgebung unterschieden werden.

Organisationseinheiten

Alle Organisationseinheiten beginnen mit OU, damit man sofort erkennt, worum es sich handelt.

Gruppen

Bei allen Gruppen wird die Art der Gruppe vorangestellt:

- **LG** für lokale Gruppen
- **GG** für globale Gruppen
- **UG** für universale Gruppen
- **SG** für Sammelgruppen
- **VG** für Verteilergruppen
- **SGV** für Sammel-Verteilergruppen

Sonstige Abkürzungen

- Alle Freigaben und Abteilungslaufwerke beginnen mit *LW_* für Laufwerk.
- Lokale Gruppen für die Laufwerke tragen am Ende des Namens ein Kürzel für die Berechtigungen: **L** für Lesen, **AE** für „Ändern“, **VZ** für „Vollzugriff“ und **KZ** für „Kein Zugriff“.

Abteilungsnamen und Mitarbeitergruppen

Bezeichnungen im Active Directory können etwas länger sein, daher sollten Sie die Bezeichnung von Abteilungen und Personengruppen ausschreiben. Wenn Sie die vollständige Bezeichnung verwenden, müssen Sie sich auch keine Abkürzung merken. Schreiben Sie also *Buchhaltung* statt *BuchH*, *Verwaltung* statt *Verw* und *Abteilungsleiter* statt *AbtL* oder *AL* (*AL* könnte zum Beispiel auch *Abteilungslaufwerk* bedeuten).

Falls Sie Abkürzungen verwenden, müssen die Abkürzungen eindeutig und unverwechselbar sein.

In diesem Buch werden Abkürzungen zum Beispiel für Städtenamen, Gruppen, Abteilungslaufwerke und Zugriffsberechtigungen verwendet.

Betrachten Sie zum besseren Verständnis die folgenden Beispiele für den Standort *Berlin*:

V-B-DC01	Bezeichnung für die Hyper-V-VM, außerdem Bezeichnung für die virtuelle Festplattendatei
B-DC01	Computername des virtuellen Computers, hier der erste Domänencontroller
OU-Berlin	Dies ist die Organisationseinheit für den Standort *Berlin*. Darin befinden sich alle weiteren Unter-OUs.
OU-B-Verwaltung	Organisationseinheit für die Verwaltungsabteilung in Berlin; diese ist eine Unter-OU von *OU-Berlin*.
GG-B-Verwaltung-Abteilungsleiter	Globale Gruppe (GG) für den Standort Berlin (B), für die Abteilungsleitung von Verwaltung
LG-B-LW_Verwaltung-L	Lokale Gruppe (LG) in Berlin (B) für das Abteilungslaufwerk (LW_) der Verwaltung mit Lese-Berechtigungen (L)
B-LW_Verwaltung	Name des Freigabeordners auf dem Dateiserver für das Abteilungslaufwerk
SG-B-Abteilungsleiter	Sammelgruppe für alle Abteilungsleiter am Standort *Berlin*
SGV-B-Buchhaltung	Sammel-Verteilergruppe (z. B. für E-Mails) mit allen Mitarbeitern der Buchhaltung

1.4 Aufbau und Konventionen

Inhaltliche Gliederung

Das vorliegende Buch baut auf dem HERDT-Buch *Windows Server 2019 – Netzwerkadministration* auf. Vermittelt werden weiterführende Strategien und Arbeitsabläufe für ausgewählte Verwaltungsaufgaben, die die Infrastruktur eines Windows-Server-2019-Netzwerks betreffen. Zu diesem Zweck wird eine virtuelle Testumgebung mit zwei Standorten mit jeweils zwei Servern erstellt. Im weiteren Verlauf kommt noch ein Windows-8-Client hinzu.

Dazu widmet sich jeweils ein Theoriekapitel dem nächsten Schritt für die Implementierung spezieller Dienste und stellt die grundlegenden Konzepte dar. Daran schließt sich dann jeweils ein Übungskapitel an, das detaillierte Arbeitsanleitungen zum Ausführen der vorher behandelten Konfigurationsmaßnahmen enthält. Die Arbeitsbeschreibungen beziehen sich dabei auf die Zielsetzung, ein Netzwerk mit Windows Server 2019 in einer Testumgebung zu implementieren, zu verwalten und zu optimieren.

Typografische Konventionen

Im Text erkennen Sie bestimmte Programmelemente an der Formatierung:

Kursivschrift	kennzeichnet Programmelemente wie Register oder Schaltflächen.
`Courier`	wird für Benutzereingaben und Systembefehle verwendet.
Spitze Klammern `<>`	kennzeichnen Platzhalter.

2

IP-Adressen und Subnetze

2.1 Adressen unter IPv4

Kommunikation in Netzen

Erfolgreiche Kommunikation in einem Netzwerk setzt voraus, dass Informationen vom Sender über ein geeignetes Medium an den Empfänger geleitet werden. Dies gilt z. B. für Menschen, die über ein Telefonnetz den richtigen Anschluss der Gegenseite anwählen. Ebenso gilt dies für Computer, die die Gegenseite über das LAN-Äquivalent einer Telefonnummer – die IP-Adresse – identifizieren.

Daneben müssen noch eine Reihe weiterer Bedingungen erfüllt werden. Da diese Protokolle ein eigenes Thema darstellen und der praktischen Ausrichtung des vorliegenden Buches widersprechen, wird an dieser Stelle nur auf die Grundlagen von TCP/IP eingegangen. Das Thema Netzwerkkommunikation und Protokolle im Allgemeinen finden Sie ausführlich in den HERDT-Büchern *Netzwerke – Protokolle und Dienste* sowie *Netzwerke – Netzwerktechnik*.

Grundlagen von Netzwerkkommunikation

In einem LAN mit Ethernet kommunizieren alle Systeme über gemeinsame Medien (shared media). Vergleichbar ist dies mit einem Raum, in dem mehrere Personen gleichzeitig Gespräche führen (in diesem wäre das gemeinsame Medium die Luft, die die Schallwellen an alle überträgt).

Um nun gezielte Kommunikation zwischen bestimmten Systemen zu ermöglichen, muss eine Möglichkeit gefunden werden, die Kommunikationen voneinander zu trennen. Dies kann bei Personen dadurch erreicht werden, dass sich diejenigen, die miteinander sprechen wollen, nebeneinanderstellen. Sie bauen sozusagen eine eigene Verbindung innerhalb des gemeinsamen Mediums auf.

Computer dagegen können nicht ihren Standort wechseln, sondern müssen auf Protokollebene eine geeignete Verbindung aufbauen, die den Verkehr von der restlichen Kommunikation trennt.

Damit nun Nachrichten gezielt zwischen den richtigen Computern (Hosts) ausgetauscht werden können, müssen diese eindeutig identifizierbar sein. Im Computernetzwerk wird hierzu die IP-Adresse verwendet.

Aufbau von IPv4-Adressen

Adressen unter IPv4 lassen sich mit Telefonnummern vergleichen. Sie bestehen aus einem Anteil, der das Netzwerk identifiziert, und einem Bestandteil, der den Anschluss innerhalb des Netzwerkes identifiziert. Im Telefonnetz entspräche dies der Vorwahl und der Anschlusskennung.

Formal betrachtet verwendet IPv4 dabei stets Adressen von 32 Bit Länge:

11000000101010001001101100010001

Für Benutzer ist eine Darstellung der IP-Adresse im Dezimalsystem jedoch einprägsamer und leichter verständlich als die Binärdarstellung. IP-Adressen werden deshalb in vier Blöcke oder **Oktette** zu je einem Byte (entsprechend 8 Bit) zerlegt. Jeder dieser Blöcke repräsentiert für sich $2^8 = 256$ mögliche Kombinationen der 8 Binärstellen, entsprechend einem Dezimalwert von 0...255. Die vier Oktette werden hintereinander notiert und durch Punkte getrennt (dotted decimal notation):

1100 0000 . 1010 1000 . 1001 1011 . 0001 0001 = 192.168.155.17

Es gelten die üblichen Regeln der Umwandlung von Binärzahlen in Dezimalzahlen. Ein einfaches Verfahren funktioniert folgendermaßen:

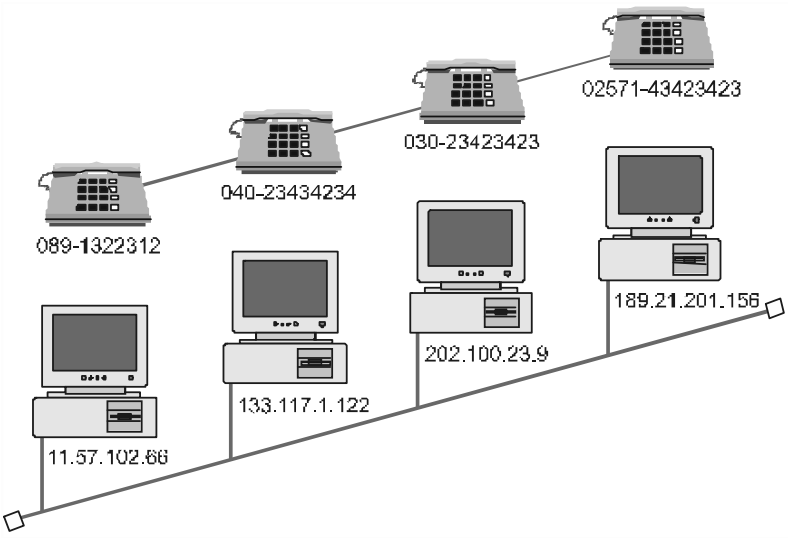
- Notieren Sie für jede Binärstelle eines Oktetts den entsprechenden Dezimalwert.

Binärstelle	1	0	1	0	1	0	0	0
Dezimalwert	128	64	32	16	8	4	2	1
	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)

- Bilden Sie die Summe aller Dezimalwerte, deren Binärstelle 1 ist. Das Ergebnis ist der zugehörige Dezimalwert des Oktetts.

128 + 32 + 8 = 168

IP-Adressen sind ihrer Funktion nach vergleichbar mit Telefonnummern: Auch Telefonanschlüsse verfügen über eine weltweit eindeutige Nummer, über die sie gezielt erreicht werden können.



Vergleich von IP-Adressen und Telefonnummern

Die Bestandteile einer IPv4-Adresse

IP-Adressen werden, ebenso wie Telefonnummern mit Vorwahl und Rufnummer, in zwei Teile untergliedert, die verschiedene Aufgaben erfüllen. So ist es möglich, jeden Host auch in einem globalen IP-Netzwerk wie dem Internet genau zu lokalisieren. Rechtliche, verwaltungs- und übertragungstechnische Gründe erfordern außerdem die Aufteilung des globalen IP-Netzwerks in einzelne voneinander weitgehend unabhängige **Segmente** oder **IP-Subnetze**. Entsprechend dieser Aufteilung verfügt jede IP-Adresse über zwei Bestandteile:

- eine **Netzwerkadresse**, die das jeweilige Netzwerksegment angibt, in dem sich ein Host befindet,
- eine **Hostadresse**, die den einzelnen Host in einem Segment angibt.

Die Netzwerkadresse kann ihrerseits in eine im gesamten Internet bekannte **Netzwerkkennung** und eine nur innerhalb eines Segments bekannte **Subnetzkennung** aufgeteilt werden. Diese Subnetzkennung kann dazu verwendet werden, große Subnetze weiter aufzuteilen.

Definitionsgemäß beginnt eine IP-Adresse mit der Netzwerkadresse und endet mit der Hostadresse. An einer beliebigen Stelle findet also ein Wechsel von der Netzwerkadresse zur Hostadresse statt. In der klassischen Definition von IP wird diese Stelle mithilfe einer **Adressklasse** festgelegt.

Ferner sind im Bereich der Hostadressen noch zwei Sonderfälle zu berücksichtigen:

- Eine Hostadresse, die nur aus Stellen mit einer binären 0 besteht, beispielsweise 192.168.1.**0**, ist die Netzwerkadresse selbst und darf daher nicht für einen einzelnen Host verwendet werden.
- Bestehen die Stellen der Hostadresse jedoch alle aus einer binären 1, beispielsweise 192.168.1.**255**, handelt es sich um die **Broadcastadresse** des betreffenden Netzwerks. Unter dieser Adresse werden alle Hosts eines Netzwerks gemeinsam angesprochen. Sie darf deshalb ebenfalls nicht für einzelne Hosts verwendet werden.

Die Zahl der nutzbaren Hostadressen eines Bereichs muss stets um zwei (die Netzwerkadresse und die Broadcastadresse) vermindert werden.

Arten von IP-Adressen

IP-Adressen können einzelne Hosts, bestimmte Gruppen von Hosts, alle Hosts eines Teilnetzes oder alle erreichbaren Hosts adressieren.

Ziel-Adressat	Übertragungsart und Beschreibung	Beispiel
Einzelner Host	Unicast, eine einzelne Adresse einer bestimmten Netzwerkschnittstelle	192.168.155.*17*
Gruppe von Hosts	Multicast, z. B. alle Hosts, auf denen das Protokoll OSPF (Open Shortest Path First) installiert ist	224.0.0.5
Alle Hosts eines Teilnetzes	Ein Directed Broadcast spricht alle Hosts eines Subnetzes oder Netzes an, z. B. zur Suche nach einem NetBIOS-Namen im eigenen Subnetz.	192.168.155.*255*

Ziel-Adressat	Übertragungsart und Beschreibung	Beispiel
Alle Hosts	Ein Limited Broadcast adressiert alle Hosts, die physikalisch im gleichen Segment erreicht werden können. Er dient z. B. zur Suche nach einem DHCP-Server (Dynamic Host Configuration Protocol).	255.255.255.255

Eine IP-Adresse enthält einen Anteil von Informationen, die Zielsysteme identifizieren, und einen Anteil von Informationen für die Netzwerkidentifikation.

Adressklassen

Wegen der Verschwendung von IP-Adressen werden die im Folgenden beschriebenen Adressklassen im Internet nicht mehr verwendet und sind durch das effizientere klassenlose Inter-Domänen-Routing (Classless Inter-Domain Routing, CIDR) abgelöst worden. Die ehemaligen Netze der Klassen A bis E gibt es nicht mehr, aus historischen Gründen ist es dennoch zum Verständnis der IP-Adressierung sinnvoll, sie zu kennen, außerdem werden Begriffe wie „Klasse-C-Netz“ immer noch verwendet, um die Größe eines Subnetzes zu beschreiben.

Adressklassen werden auch als Netzklassen oder Netzwerkklassen (englisch: Classful Networks) bezeichnet. Sie wurden 1981 durch den Entwurf RFC 791 als Adressierungsmethode vorgeschlagen und wenig später für das Internet eingeführt. Durch die Adressklassen werden IPv4-Adressen in Netzwerk- und Hostadressen aufgeteilt, indem die Anzahl der Binärstellen (= Bits) für die Netzwerkadresse festgelegt wird. Es wurden fünf Adressklassen definiert, die sich an einer bestimmten Abfolge der ersten vier Bits einer beliebigen IP-Adresse erkennen lassen:

Adressklasse	Bits der Netzwerkadresse	Abfolge der ersten vier Bits	Anzahl der Hostadressen je Netz	Adressbereich
Klasse A	8 (ein Byte)	0XXX	16. 777 214	0.0.0.0 bis 127.255.255.255
Klasse B	16 (zwei Byte)	10XX	65.534	128.0.0.0 bis 191.255.255.255
Klasse C	24 (drei Byte)	110X	254	192.0.0.0 bis 223.255.255.255
Klasse D	– (Multicastgruppen)	1110	nicht verfügbar	224.0.0.0 bis 239.255.255.255
Klasse E	– (Experimentell)	1111	nicht verfügbar	240.0.0.0 bis 255.255.255.255

Für die normale Verwendung waren die Adressen der Klassen A bis C verfügbar. Dies sind die sogenannten **Unicast**-Adressen im Bereich zwischen 0.0.0.0 und 223.255.255.255, die bis heute für eine 1:1-Kommunikation zwischen Systemen benutzt werden.

Die starre Aufteilung der IP-Adressen mittels Adressklassen führte infolge der rasanten Zunahme der Anzahl von Hosts im Internet zu einer raschen Verknappung der verfügbaren IP-Adressen. Wenn für ein bestimmtes Subnetz eine Anzahl von Hostadressen benötigt wurde, die – vielleicht nur geringfügig – über den 254 Adressen in einem Klasse-C-Netz lag, war sofort die Vergabe eines vollständigen Klasse-B-Netzes erforderlich.

Nicht genutzte Adressen aus diesem Klasse-B-Netz konnten dann jedoch nicht mehr an andere Interessenten vergeben werden, weil jede Netzwerkadresse nur ein einziges Netz kennzeichnen darf. Andernfalls wäre die Eindeutigkeit der Netzwerkadressen im Internet nicht mehr gewährleistet. Alle nicht benötigten Hostadressen gingen somit verloren, teilweise einige Zehntausend Adressen in einem einzelnen Netz der Klasse B.

Die klassenbasierte Verwaltung der IP-Adressen wurde später um **private Adressbereiche** ergänzt. Die damals festgelegten drei privaten Adressbereiche liegen jeweils in einer der historischen Netzklassen. Diese Aufteilung hat auch heute noch Bestand.

Private Adressen

Private IP-Adressen stehen für Netzwerke zur Verfügung, die nicht oder nur über spezielle Router mit dem Internet verbunden sind. Folgende private IPv4-Adressen werden im Internet nicht weitergeleitet und dürfen von jedem Betreiber eines privaten IP-Netzwerks verwendet werden:

Private Klasse-A-Adressen	10.0.0.0 bis 10.255.255.255	10.0.8 bzw. 10/8	entspricht einem Klasse-A-Netz mit 16.777.214 Hostadressen
Private Klasse-B-Adressen	172.16.0.0 bis 172.31.255.255	172.16.0.0/12 bzw. 172.16/12	entsprechen 16 Klasse-B-Netzen mit jeweils 65.534 Hostadressen
Private Klasse-C-Adressen	192.168.0.0 bis 192.168.255.255	192.168.0.0/16 bzw. 192.168/16	entsprechen 256 Klasse-C-Netzen mit jeweils 254 Hostadressen

2.2 Subnetzmasken und Subnetze

Die Subnetzmaske

Bei der Auswertung von IP-Adressen mittels Adressklassen genügt die Angabe einer IP-Adresse, um daraus mithilfe der Klassendefinition die Netzwerkadresse und die Hostadresse zu ermitteln. Die Subnetzmaske (Subnet Mask) stellt den Nachfolger der Adressklassen dar. Ihr Hauptvorteil ist die Möglichkeit, die Länge der Netzwerkadresse nicht nur in Schritten ganzer Oktette zu verschieben, wie dies bei den Adressklassen A bis C der Fall war. Mithilfe der Angabe einer Subnetzmaske gemeinsam mit der erteilten IP-Adresse kann die Netzwerkadresse vielmehr an jeder beliebigen Stelle der IP-Adresse enden.

Eine Subnetzmaske wird wie die IP-Adresse als 32 Bit langes Datenwort vom Host verarbeitet. Sie besteht jedoch nicht aus einer beliebigen Abfolge von Binärzahlen, sondern beginnt mit einer binären 1 und enthält maximal einen Wechsel zur binären 0, beispielsweise:

11111111 00000000 00000000 00000000 oder 255.0.0.0

Per Definition zeigen die Stellen der Subnetzmaske, deren Binärwert 1 ist, die Netzwerkadresse an. Alle Stellen mit einer 0 in der Subnetzmaske gehören dagegen zur Hostadresse. In der Binärdarstellung wird dies sofort deutlich:

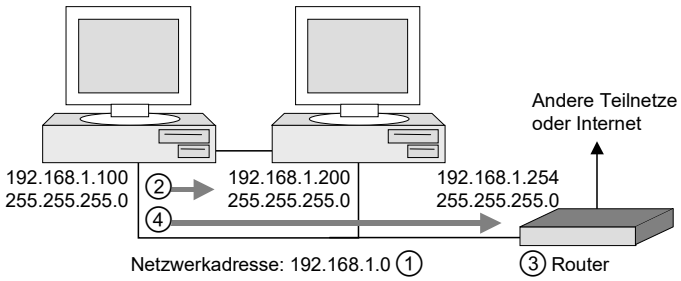
IP-Adresse	192.168.132.0	1100 0000	1010 1000	1000 0100	0000 0000
Subnetzmaske	255.255.255.0	1111 1111	1111 1111	1111 1111	0000 0000
		Netzwerkadresse			**Hostadresse**

Neben der Dezimalschreibweise gibt es für Subnetzmasken auch eine vereinfachte Schreibweise, die nur noch die Zahl der Stellen der Netzwerkadresse hinter einer IP-Adresse angibt. Die IP-Adresse 192.168.1.100 mit der 24-stellig gesetzten Subnetzmaske 255.255.255.0 kann dementsprechend auch geschrieben werden als 192.168.1.100**/24**. Diese Schreibweise wird als CIDR-Notation bezeichnet und ist wegen ihrer Übersichtlichkeit weit verbreitet.

Funktion der Subnetzmaske

Die Subnetzmaske legt fest, zu welchem Teilnetz eine gegebene IP-Adresse gehört. Die Angabe einer Subnetzmaske, zusätzlich zur IP-Adresse, ist deshalb zwingend erforderlich. Mit der Subnetzmaske wird die Netzwerkadresse dieser IP-Adresse genau definiert, eine Änderung der Subnetzmaske bedeutet eine Änderung der Teilnetzzugehörigkeit.

Ein Host verwendet die Subnetzmaske, um zu bestimmen, welcher Teil seiner IP-Adresse die Netzwerkadresse ① ist. Anschließend ermittelt er die Netzwerkadresse seines Kommunikationspartners. Wenn beide Netzwerkadressen identisch sind, werden die Daten an das eigene Teilnetz gesendet ②. Befindet sich das Netzwerkziel jedoch außerhalb des eigenen Subnetzes, wird anhand der Routentabelle ein geeigneter Router ③ ermittelt, der den Weitertransport der Daten übernimmt ④.



Kommunikation innerhalb und außerhalb eines IP-Teilnetzes

Gerade und ungerade Subnetzmasken

Anstelle der Definitionen der Klassen A, B und C können folgende entsprechende Subnetzmasken eingesetzt werden:

- 11111111 00000000 00000000 00000000 = 255.0.0.0 — für vormalige Klasse-A-Netzwerke
- 11111111 11111111 00000000 00000000 = 255.255.0.0 — für vormalige Klasse-B-Netzwerke
- 11111111 11111111 11111111 00000000 = 255.255.255.0 — für vormalige Klasse-C-Netzwerke

Diese Subnetzmasken werden als **gerade Subnetzmasken**, **natürliche Subnetzmasken** oder **Standard-Subnetzmasken bezeichnet** und bieten dieselbe Funktionalität wie die bestehenden Klassendefinitionen.