

Die Journey zum Cloud- Netzwerkmanagement

Inhalte

Die Weiterentwicklung des Netzwerkmanagements	3
Die Trends für das Netzwerk	3
Automatisierung und Analytik	3
As-a-Service-Nutzung	4
Internet of Things (IoT)	4
Sicherheit	4
Kundenreferenz zur hybriden Arbeit	5
Was ist Cloud-Netzwerkmanagement?	6
Was ist Cloud-Monitoring?	7
Was ist Cloud-Management?	7
Das Cisco IT-Betriebsmodell für das gesamte Spektrum	8
Ein (virtuelles) On-Premises-Betriebsmodell	8
Der Weg zur Cloud-First-IT-Transformation	9
Fazit	9
Ressourcen	9



Die Weiterentwicklung des Netzwerkmanagements

Das Netzwerkmanagement verändert sich derzeit grundlegend. Durch Innovationen wie hybride Arbeit, Augmented Reality (AR), Virtual Reality (VR) und Robotik befinden sich immer mehr unterschiedliche Geräte im Netzwerk. Dies fordert niedrigere Latenzzeiten und einen neuen Sicherheitsansatz. Darüber hinaus stellen sich Unternehmen zunehmend dezentraler auf und unterstützen immer mehr verschiedene Standorte. Zusammengenommen belasten diese beiden Veränderungen das Netzwerk und die dafür zuständigen Teams massiv und bedrohen die Grundlage für zukünftige Technologie- und Geschäftsinnovationen.

IT-Teams müssen sicherstellen, dass das Netzwerk bereits heute für diese Herausforderungen gerüstet ist, und darüber hinaus auch die Herausforderungen von morgen im Blick behalten. Netzwerkbetriebsteams gehen dieses Thema direkt an und folgen neuen Trends, um eine mobilere, vielfältigere und datenhungrigere Benutzer- und Gerätebasis zu unterstützen.

Diese Verschiebungen lassen sich in Automatisierung und Analytik, As-a-Service-Nutzung von Technologie, IoT und Sicherheit kategorisieren. Jeder dieser Bereiche spielt mit den anderen zusammen. Gemeinsam zeigen sie die gestiegenen Anforderungen an Einfachheit, Ausfallsicherheit und Agilität im Netzwerk.

Dieses Whitepaper skizziert diese Trends und stellt ein skalierbares IT-Betriebsmodell als Weg vor, die IT beim Umgang mit diesen Trends zu unterstützen.

Die Trends für das Netzwerk

Cisco sieht mehrere Faktoren, die IT-Abteilungen bei der Ausrichtung des Netzwerkes auf die Zukunft beachten müssen. Dabei zeigt sich, dass IT-Abteilungen anders arbeiten, um Anwendungen schneller bereitzustellen und neue Geräte zu unterstützen, ohne die Sicherheit zu gefährden.

Automatisierung und Analytik

Das Netzwerk wird zunehmend komplexer und umfasst eine Vielzahl von Geräten, Verbindungsmöglichkeiten und Standorten, von denen aus eine Verbindung hergestellt werden kann. Es geht nicht mehr nur um Laptops und Handys – alles ist vernetzt, von Beleuchtung und intelligenten Kameras bis hin zu Thermostaten. Aus diesem Grund verlassen sich Netzwerkbetriebsteams auf Automatisierung, künstliche Intelligenz (KI) und Machine Learning (ML), um den Netzwerkbetrieb zu vereinfachen.

Ein Beispiel ist die zunehmende Anzahl von Menschen, die von unterwegs arbeiten. Cisco meldete 2021 einen Anstieg mobiler Meetings um 300 %.¹ Dies führt zu Richtlinien- und Identitätsherausforderungen. Ohne einen gewissen Grad an Automatisierung können Netzwerkbetriebsteams Identität und Richtlinien nur auf sehr grundlegender Ebene managen. Diese Teams nutzen jetzt die Netzwerktelemetrie und automatisieren das Identitäts- und Richtlinienmanagement mithilfe von KI- und ML-Modellen, um schneller zu verstehen, ob BenutzerInnen die sind, die sie zu sein vorgeben, und ob sie über ein sicheres Netzwerk teilnehmen. Um dies effektiv zu erreichen, muss das Netzwerk agil, flexibel und allgegenwärtig sein.

As-a-Service-Nutzung

Traditionell konzentrierte sich die IT auf die Installation und das Management von Infrastruktur als Reaktion auf geschäftliche Anforderungen, wobei der Schwerpunkt auf dem Management von Infrastrukturkosten lag. Mit dem Anstieg der As-a-Service-Nutzung sehen IT-Abteilungen eine Möglichkeit, diese Dynamik zu ändern.

Die Kostenstruktur der As-a-Service-Technologie und die Möglichkeit, Services basierend auf Ergebnissen zu skalieren und neue Funktionen einfacher hinzuzufügen, tragen dazu bei, den Fokus von IT-Teams weg von Kostensenkungen hin zu gewinnbringenden Aktivitäten zu verlagern.

Internet of Things (IoT)

Die Verbreitung von Geräten, Ressourcen und Sensoren mit Remote-Zugriff in Innen- und Außenbereichen nimmt zu. Die Cisco Studie zeigt, dass bis 2023 IoT-Geräte die Hälfte aller vernetzten Geräte ausmachen werden (2018 war es noch ein Drittel).² Unternehmen betrachten das IoT als Lösung für eine Vielzahl von Problemen, darunter beispielsweise die Verbesserung der Arbeitssicherheit durch Monitoring der Luftqualität in Büroumgebungen und die Effizienznachverfolgung im Lager durch das Monitoring der Bewegung von Ressourcen und Geräten.

Ein solcher Zustrom von Geräten im Netzwerk wird zu weiteren Konvergenzen zwischen IT- und OT-Teams führen. Da die OT stark auf das Netzwerk angewiesen ist, müssen IT- und OT-Teams zusammenarbeiten und Informationen über Netzwerk- und Geräteintegrität, Frequenzbandnutzung, Sicherheit, Richtlinien und Wartungsaufwand austauschen. Die IT benötigt ein stärker datengesteuertes und mobiles Netzwerk, um dies effektiv umzusetzen.

Sicherheit

Aufgrund der komplexen Mobilität, einer heterogenen Gerätebasis und des IoT denkt die IT anders über Sicherheit. IT-Teams haben erkannt, dass Sicherheit nicht aus einem geschützten Perimeter rund um das Netzwerk bestehen kann, sondern über das gesamte Netzwerk hinweg erfolgen muss. Vom Büro bis zum Café, vom Laptop bis zur vernetzten Überwachungskamera: Sicherheit muss alles im Netzwerk durchdringen.

Der Netzwerkzugriff ist weltweit rund um die Uhr verfügbar. Netzwerkbetriebsteams müssen in der Lage sein, jederzeit und überall auf Sicherheitsbedrohungen zu reagieren. Sofortiger Zugriff auf das Netzwerk, unabhängig davon, ob AdministratorInnen vor Ort oder zu Hause sind, ist unerlässlich.

Jeder dieser Bereiche spielt mit den anderen zusammen. Gemeinsam zeigen sie die gestiegenen Anforderungen an Einfachheit, Ausfallsicherheit und Agilität beim Netzwerkmanagement.

¹ [Cisco Hybrid Work Index, 2021.](#)

² [IoT and the Network: What Is the Future? Cisco, 2020.](#)

Dies treibt die IT letztendlich in Richtung Cloud-Management für das Netzwerk. Diese Umstellung ist bereits im Gange: Drei von fünf Unternehmen berichten, dass sie eine Art Cloud-basierte Plattform für das Management der Netzwerkinfrastruktur nutzen.³

Kundenreferenz zur hybriden Arbeit

Ein Anwendungsfall, der das Zusammenspiel dieser Trends und den daraus resultierenden Bedarf an Cloud-Netzwerkmanagement verdeutlicht, ist die Zunahme hybrider Arbeit.

Die Pandemie hat zu einem erheblichen Cloud-Boom auf Anwendungsebene geführt: 70 % der Unternehmen gaben an, dass sie die Migration von Anwendungen in die Cloud beschleunigt haben.⁴ Dies war eine Frage des geschäftlichen Überlebens, da die MitarbeiterInnen zu Remote-Arbeit wechselten und Zugriff auf Collaboration- und Produktivitätstools benötigten. Allerdings hat die Nutzung der Cloud auf der Anwendungsebene nicht nachgelassen. Laut einem aktuellen Gartner-Bericht werden bis 2025 95 % der digitalen Workloads auf Cloud-nativen Plattformen bereitgestellt werden.⁵

Damit diese Cloud-Anwendungen unabhängig vom Standort oder Gerät effektiv funktionieren können, muss das Netzwerk mobiler, flexibler und für den Remote-Zugriff optimiert sein.

Untersuchungen von Enterprise Management Associates zeigen, dass 85 % der Unternehmen einen dauerhaften Anstieg der Anzahl der MitarbeiterInnen zu verzeichnen haben, die zumindest teilweise im Homeoffice arbeiten.⁶ Darüber hinaus arbeiten die Beschäftigten nicht mehr nur von ihrem Laptop aus. Cisco Daten zufolge ist die Anzahl der Meetings, die über Mobilgeräte aufgerufen werden, um 200 % gestiegen.⁷

Wenn Menschen in Rahmen von hybriden Arbeitsmodellen ins Büro zurückkehren, müssen Arbeitgeber darüber nachdenken, wie sie ihrer Belegschaft dabei helfen können, sich sicher zu fühlen, und wie sich die Kosten eines teilweise leer stehenden Gebäudes im Zaum halten lassen. Gleichzeitig implementiert die IT Änderungen, um Anwendungen schnell bereitzustellen, das Richtlinienmanagement zu automatisieren und MitarbeiterInnen zu schützen, wo immer sie sich befinden. Da Netzwerkbetriebsteams größtenteils selbst hybrid arbeiten, müssen IT-Abteilungen eine Reihe komplizierter Überlegungen anstellen, welche dann wiederum die oben beschriebenen Trends vorantreiben.

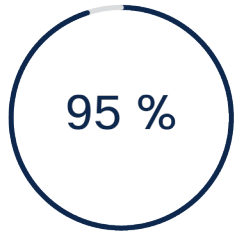
³ [Cisco Global Networking Trends Report, 2022](#).

⁴ Enterprise Management Associates, [Hybrid Work Requires Network Transformation](#), 2022.

⁵ Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, [Gartner, 2021](#).

⁶ Enterprise Management Associates, [Hybrid Work Requires Network Transformation](#), 2022.

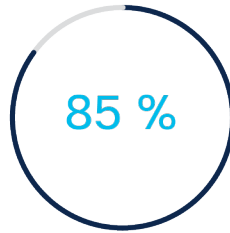
⁷ [Cisco Hybrid Work Index, Daten von Februar 2020 bis Januar 2022](#).



95 %

Bis 2025 werden 95 % aller neuen digitalen Workloads auf Cloud-nativen Plattformen bereitgestellt werden.

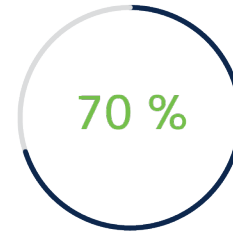
Quelle: Gartner



85 %

85 % der Unternehmen verzeichnen einen dauerhaften Anstieg der Anzahl der MitarbeiterInnen, die zumindest teilweise im Homeoffice arbeiten.

Quelle: Enterprise Management Associates



70 %

70 % der Unternehmen geben an, dass die Pandemie die Migration von Anwendungen zur Cloud beschleunigt hat.

Quelle: Enterprise Management Associates

Abbildung 1.

Trends, welche die Migration in die Cloud vorantreiben

Hier kommt die Cloud ins Spiel. IT-Abteilungen benötigen die richtige Mischung aus Netzwerktechnologie, einfachem Management und betrieblicher Flexibilität, um hybrides Arbeiten in großem Maßstab zu ermöglichen. Netzwerkteams implementieren Cloud-Netzwerkmanagement für folgende Zwecke:

- Ermöglichung von Remote-Monitoring und/oder -Management
- Unterstützung von netzwerkübergreifender Automatisierung für Echtzeitdiagnosen, automatisiertes Onboarding und Richtlinienmanagement
- Erfassung der Daten von Benutzergeräten und IoT-Sensoren im gesamten Netzwerk, um die Entscheidungsfindung zu beschleunigen

Alles in allem erfordern Netzwerke ein hohes Maß an Anpassbarkeit und Einfachheit sowie die Möglichkeit, BenutzerInnen unabhängig von ihrem Standort sicher zu verbinden und zu unterstützen. Damit schließt sich der Kreis zu den oben genannten Trends und der Bedarf, Cloud-Netzwerke schon heute aufzubauen, verdeutlicht sich.

Was ist Cloud-Netzwerkmanagement?

Um diese Herausforderungen zu bewältigen und sich an die Anforderungen einer stärker verteilten Belegschaft anzupassen, stellen Unternehmen schnell auf Netzwerkmanagement-Plattformen in der Cloud um. Das Cloud-Netzwerkmanagement macht nicht nur ein physisches Netzwerkmanagementgerät vor Ort überflüssig, sondern unterstützt IT-Abteilungen auch bei der Weiterentwicklung ihrer Betriebsabläufe, um diese neuen Anforderungen direkt zu erfüllen.

Mit Cloud-Management können IT-Abteilungen komplexe Netzwerke von überall aus überwachen und managen. Um mehr darüber zu erfahren, wie sich diese Funktion auf die Trends im Netzwerkbereich auswirkt, lohnt es sich, einen genaueren Blick auf Cloud-Monitoring und -Management zu werfen.

Was ist Cloud-Monitoring?

Cloud-Monitoring bietet mehr als nur einen Überblick über die Netzwerkumgebung in einem zentralen Dashboard. Netzwerkbetriebsteams können Cloud-Monitoring nutzen, um Netzwerkstatistiken (z. B. Datenverkehrsinformationen) und Konfigurationen (z. B. verbundene Ports) zu überprüfen und grundlegende Fehlerbehebungen durchzuführen – und das aus einer Entfernung von 10 m oder mehr als 150 km.

Einer der ersten Vorteile, der sich BenutzerInnen von Cloud-Monitoring offenbart, ist der skalierbare Zugriff auf Netzwerkdaten. Cloud-Monitoring von Netzwerken verbindet die Switching- und Zugriffsinfrastruktur mit einem zentralen Dashboard, über das Daten geleitet werden. So können IT-Abteilungen schneller Entscheidungen treffen und die Infrastruktur kann als Backbone für Automatisierungsmaßnahmen dienen.

Dieser Zugriff auf Daten beschleunigt auch die Problembhebung. NetzwerkadministratorInnen können Probleme mit Switch-Verbindungen identifizieren und die Auswirkungen von überall auf der Welt abmildern. Dies wird immer wichtiger, da immer mehr Switches bereitgestellt werden, um Trends wie IoT mit PoE-gesteuerter Beleuchtung (Power over Ethernet) zu unterstützen und Daten von IoT-Hubs in ein zentrales Dashboard zu übertragen.

Cloud-Monitoring ist oft ein erster Schritt in Richtung eines vollständigen Cloud-Managements, da Netzwerkbetriebsteams die Vorteile der Cloud nutzen können, ohne ihr vorhandenes On-Premises-Managementssystem ersetzen zu müssen.

Was ist Cloud-Management?

Cloud-Management umfasst Cloud-Monitoring und bietet Netzwerkbetriebsteams ein hohes Maß an Flexibilität und Agilität. Mit dem zentralen Dashboard lassen sich Onboarding, Identität, Port-Konfiguration für Switches, Analysen und Sicherheit remote managen – ganz ohne die Kosten und Komplexität von On-Premises-Wireless-Controllern und Overlay-Management-Systemen. Die aus dem Netzwerk gesammelten Daten lassen sich außerdem verwenden, um diese Prozesse mit automatisierten Sicherheitswarnungen und Zero-Touch-Bereitstellung von Geräten vollständig zu automatisieren.

Durch die Möglichkeit, große Netzwerke mit Zehntausenden Endpunkten von einem zentralen Hub aus zu managen, können IT-Teams die zuvor beschriebenen Netzwerkrends voll ausnutzen. Tatsächlich managen fast 700.000 Cisco Kunden ihr Netzwerk zumindest teilweise über die Cloud.

Bei der Nutzung der Cloud ist die Flexibilität ein weiterer Vorteil. Cloud-Netzwerkmanagement (einschließlich Monitoring) ist ein As-a-Service-Angebot. IT-Abteilungen können das Cloud-Netzwerkmanagement ohne die Vorabkosten einer On-Premises-Lösung nutzen. Darüber hinaus lässt es sich einfach auf die Anforderungen des Unternehmens skalieren und ist mit den neuesten Funktionen und Sicherheitsupdates immer auf dem aktuellen Stand.

Das Cisco IT-Betriebsmodell für das gesamte Spektrum

Ihr IT-Betriebsmodell, Ihre Entscheidung

Flexibilität, Auswahl und Einfachheit

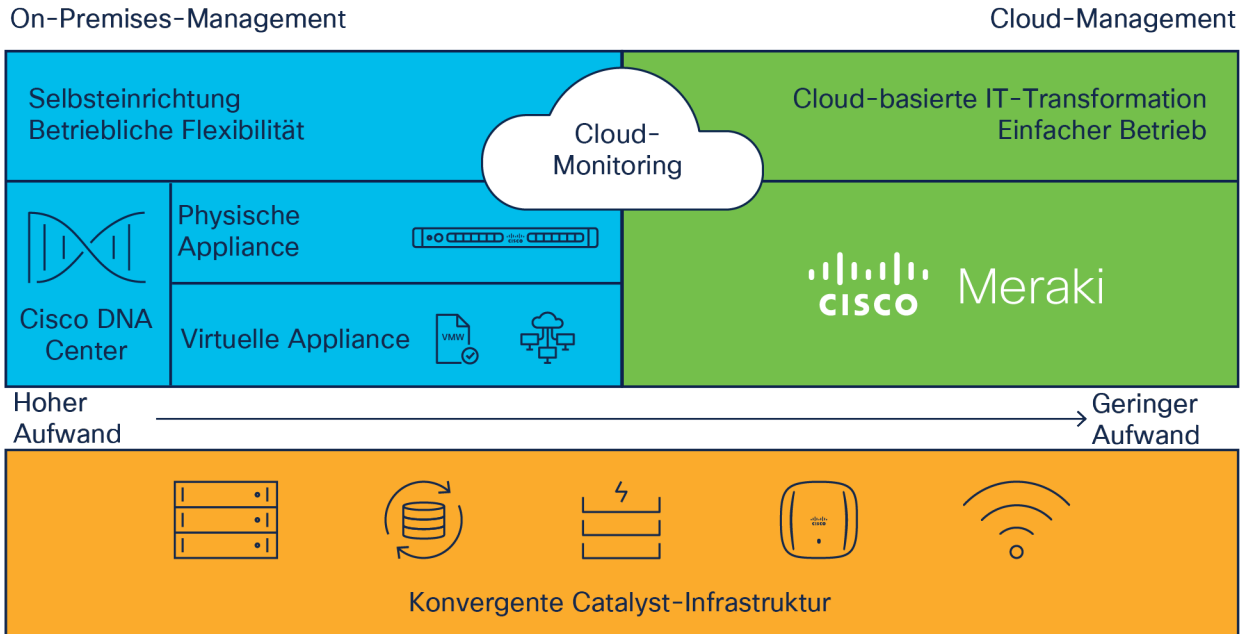


Abbildung 2.

Das Cisco Betriebsmodell für das gesamte Spektrum

Cisco bietet einen einheitlichen Ansatz für das Cloud-Netzwerkmanagement, der alles von On-Premises-Netzwerkmanagement bis hin zu vollständig in der Cloud gemanagten Netzwerken unterstützt. Ziel ist es, die Netzwerkbetriebsteams dort abzuholen, wo sich die Cloud gerade befindet.

Dieser Ansatz eröffnet IT-Abteilungen eine Fülle von Möglichkeiten basierend auf vertrauenswürdigen, bekannten Cisco Plattformen, die unabhängig vom Anwendungsfall ein konsistentes Erlebnis bieten.

Cisco investiert in On-Premises- und Cloud-Management, um die Herausforderungen von heute effektiv bewältigen zu können, und hat dabei gleichzeitig die zukünftigen Anforderungen der Kunden im Blick.

Ein (virtuelles) On-Premises-Betriebsmodell

Die Cloud ermöglicht zwar neue Anwendungsfälle und vereinfacht Abläufe, doch es lassen sich noch nicht alle Netzwerke in der Cloud hosten.

Cisco versteht diese Anforderungen und investiert daher weiterhin in seine On-Premises-Netzwerkmanagementplattform Cisco DNA Center. Die neueste Innovation von Cisco für das On-Premises-Netzwerkmanagement ist die virtuelle Cisco DNA Center-Appliance.

Cisco DNA Center wird traditionell auf einer physischen Appliance ausgeführt. Die virtuelle Cisco DNA Center-Appliance macht diese Hardware überflüssig und stellt Cisco DNA Center in einem Public-Cloud-Service wie AWS oder in einer virtuellen VMware ESXi-Umgebung bereit. Sie kann sich vor Ort oder in einer Co-Location-Einrichtung befinden und bietet Funktionsparität mit der physischen Appliance.

Der Weg zur Cloud-First-IT-Transformation

Wie bereits erwähnt, ist die Transformation der in der Cloud gemanagten Netzwerke bereits im Gange. IT-Abteilungen müssen sich mit aktuellen Netzwerktrends auseinandersetzen, und dazu ist die vorhandene Netzwerkinfrastruktur nicht immer ausreichend. Cisco ist sich darüber im Klaren und arbeitet schon heute an der Zukunft des Netzwerks, indem es die Cisco Meraki Cloud-Plattform mit Cisco Catalyst-Hardware vereint. Diese skalierbare Plattform wird IT-Teams auf dem Weg von der On-Premises-Infrastruktur zur Cloud unterstützen.

Immer mehr IT-Abteilungen werden mit dieser Transformation beginnen, da die Gründe, warum sich Unternehmen für ein On-Premises-Netzwerk entscheiden, zunehmend an Bedeutung verlieren. Die Transformation hat bereits begonnen. Dies zeigt sich durch steigende Zuversicht rund um die Cloud in einigen Branchen, die Einführung von in der Meraki Cloud-Management-Plattform verfügbaren Cisco Catalyst Access Points mit hoher Dichte und Innovationen bei in der Cloud gemanagten Netzwerken, die mehr Anpassungsoptionen für Cloud-Netzwerke bieten.

Basierend auf diesem Wandel kann die IT sich auf skalierbare Weise an den zu Beginn dieses Whitepapers beschriebenen Trends orientieren. Heute können IT-Abteilungen mit minimaler Unterbrechung Cloud-Monitoring von Cisco Meraki für die Switches der Cisco Catalyst 9000-Familie bereitstellen, um Zugriff auf Netzwerkdaten in Echtzeit zu erhalten und die Remote-Fehlerbehebung von Netzwerkproblemen zu ermöglichen.

Die IT kann auf diesem Weg noch einen Schritt weitergehen, indem sie das Cloud-Management für die Access Points der Cisco Catalyst 9162-, 9164- und 9166-Serie mit der Cisco Meraki Cloud Management-Plattform ermöglicht.

Mit dieser Lösung wird die Catalyst-Hardware von Cisco DNA Center auf die Meraki Cloud-Management-Plattform migriert, wodurch kein On-Premises-Netzwerkmanagementsystem zur Unterstützung des Netzwerks mehr erforderlich ist.

Das IT-Betriebsmodell von Cisco ist vom On-Premises- bis hin zum Cloud-Netzwerkmanagement skalierbar und bietet konvergente Hardware, die unabhängig von der Managementplattform funktioniert. IT-Teams können in die Cloud wechseln, wenn sie dazu bereit sind, und ihre Technologieinvestitionen schützen, da sie Hardware nicht vollständig austauschen müssen.

Fazit

Das Netzwerk verändert sich schnell, und das Cisco IT-Betriebsmodell wurde entwickelt, um IT-Teams dabei zu helfen, bei der Implementierung eines Cloud-Netzwerkmanagements ein skalierbares, konsistentes Benutzererlebnis zu bieten. Mit dem Monitoring und dem Management von Cloud-Netzwerken von Cisco können IT-Abteilungen flexibler und reaktionsfähiger werden, müssen sich weniger Gedanken über das Management des Netzwerks machen und haben mehr Zeit, sich auf erfolgsfördernde Projekte zu konzentrieren.

Ressourcen

[Testen Sie unsere Meraki Instant-Demo](#)

[Sehen Sie sich eine Demo von Catalyst und Meraki im Zusammenspiel an](#)

[Weitere Informationen finden Sie im Meraki-Dashboard](#)

[Weitere Informationen über Zugriffsnetzwerke](#)

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter <https://www.cisco.com/go/offices>.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter folgender URL: <https://www.cisco.com/go/trademarks>. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)