Cisco IOS-Management für hochverfügbare Netzwerke: Whitepaper zu Best Practices

Inhalt

Einführung

Die Bereitstellung und Wartung der zuverlässigen Cisco IOS®-Software hat in der heutigen

geschäftskritischen Netzwerkumgebung höchste Priorität. Um eine unterbrechungsfreie Verfügbarkeit zu erreichen, müssen Cisco und die Kunden neue Impulse setzen. Cisco muss sich zwar auf sein Engagement für die Softwarequalität konzentrieren, Netzwerkdesign- und Supportgruppen müssen sich jedoch auch auf Best Practices für das Cisco IOS-Softwaremanagement konzentrieren. Ziel ist eine höhere Verfügbarkeit und eine effizientere Softwareverwaltung. Diese Methode ist eine kombinierte Partnerschaft für den Austausch, das Lernen und die Implementierung von Best Practices für das Softwaremanagement.

Dieses Dokument stellt ein effektives Framework von Cisco IOS-Managementverfahren für Enterprise- und Service Provider-Kunden bereit, das zu einer verbesserten Softwarezuverlässigkeit, einer reduzierten Netzwerkkomplexität und einer erhöhten Netzwerkverfügbarkeit beiträgt. Dieses Framework trägt auch zur Verbesserung der Effizienz des Softwaremanagements bei, indem es Verantwortungsbereiche und Überschneidungen bei Softwareverwaltungstests und Validierungen zwischen den Cisco Versionsprozessen und dem Kundenstamm von Cisco identifiziert.

Überblick über Cisco IOS Best Practices

Die folgende Tabelle bietet einen Überblick über die Best Practices von Cisco IOS. Diese Tabellen können als Managementübersicht über die definierten Best Practices, als Checkliste für Lückenanalysen zur Überprüfung der aktuellen Cisco IOS-Managementpraktiken oder als Framework zur Erstellung von Prozessen rund um das Cisco IOS-Management verwendet werden.

Die Tabellen definieren die vier Lebenszykluskomponenten des Cisco IOS-Managements. Jede Tabelle beginnt mit einer Strategie und einer Toolübersicht für den identifizierten Lebenszyklus-Bereich. Anhand der zusammengefassten Strategien und Tools werden spezifische Best Practices definiert, die nur für den definierten Lebenszyklus gelten.

Planung - Erstellung des Cisco IOS Management Framework - Die Planung ist die erste Phase des Cisco IOS-Managements, die erforderlich ist, um Unternehmen bei der Entscheidung zu unterstützen, wann ein Software-Upgrade durchgeführt werden soll, wo ein Upgrade durchgeführt werden muss und welche Prozesse zum Testen und Validieren potenzieller Images verwendet werden.

Best Practices	Details
Strategie und Tools für die Cisco IOS-Planung	Die Planung des Cisco IOS-Managements beginnt mit einer ehrlichen Bewertung der aktuellen Praktiken, der Entwicklung erreichbarer Ziele und der Projektplanung.
Definitionen der Softwareversionsverfolgung	Gibt an, wo die Softwarekonsistenz gewahrt werden kann. Ein Software-Programmzweig kann als eine einzigartige Softwareversionsgruppierung definiert werden, die sich von anderen Bereichen nach geografischem Gebiet, Plattformen, Modulen oder Funktionsanforderungen unterscheidet.
Aktualisierung	Aktualisierungszyklusdefinitionen können

szyklus und Definitionen	als grundlegende Qualitätsschritte in der Software definiert werden. Mithilfe des Änderungsmanagements wird festgelegt, wann ein Software-Upgrade-Zyklus eingeleitet werden soll.
Zertifizierungsprozess	Die Schritte des Zertifizierungsprozesses sollten die Identifikation von Gleisen, Definitionen von Aktualisierungszyklen, die Verwaltung potenzieller Kunden, Tests/Validierung und mindestens einige Produktionszwecke für Pilotprojekte umfassen.

Design - Auswahl und Validierung von IOS-Versionen - Ein klar definierter Prozess für die Auswahl und Validierung von Cisco IOS-Versionen hilft Unternehmen dabei, ungeplante Ausfallzeiten aufgrund erfolgloser Upgrade-Versuche und ungeplanter Software-Fehler zu reduzieren.

Best Practices	Details
Strategie und Tools für die Auswahl und Validierung von Cisco IOS	Definition von Prozessen für die Auswahl, das Testen und die Validierung neuer Cisco IOS-Versionen. Dazu gehört ein Netzwerk-Testlabor, das das Produktionsnetzwerk emuliert.
Kandidaten-Management	Unter "Kandidaten-Management" versteht man die Identifizierung von Softwareversionsanforderungen und potenziellen Risiken für die jeweilige Hardware und die aktivierten Funktionssätze.
Tests und Validierung	Das Testen und Validieren ist ein wichtiger Aspekt des Softwaremanagements und der Netzwerktechnik mit hoher Verfügbarkeit. Sachgerechtes Testen kann die Ausfallzeiten der Produktion erheblich reduzieren, die Schulung der Mitarbeiter des Netzwerk-Supports erleichtern und die Prozesse für die Netzwerkimplementierung optimieren.

Implementierung - Schnelle und erfolgreiche Cisco IOS-Bereitstellung - Gut definierte Implementierungsprozesse ermöglichen eine schnelle und erfolgreiche Bereitstellung neuer Cisco IOS-Versionen.

Best Practices	Details
Strategie und Tools	Die grundlegende Strategie für Cisco IOS-Bereitstellungen besteht in der Durchführung

für Cisco IOS-Bereitstellungen	der endgültigen Zertifizierung im Rahmen eines Pilotprozesses und der schnellen Bereitstellung mithilfe von Upgrade-Tools und einem klar definierten Implementierungsprozess.
Pilotprozess	Um die potenzielle Exposition zu minimieren und die verbleibenden Produktionsprobleme besser zu erfassen, wird ein Software-Pilotprogramm empfohlen. Im Rahmen des einzelnen Pilotplans sollten die Auswahl des Pilotprojekts, die Dauer des Pilotprojekts und die Messung berücksichtigt werden.
Implementierung	Nach Abschluss der Pilotphase sollte die Cisco IOS-Implementierungsphase beginnen. Die Implementierungsphase kann mehrere Schritte umfassen, um den Erfolg und die Effizienz von Software-Upgrades sicherzustellen. Dazu gehören der langsame Start, die abschließende Zertifizierung, die Vorbereitung von Upgrades, die Automatisierung von Upgrades und die abschließende Validierung.

Betrieb - Management der hochverfügbaren Cisco IOS-Implementierung - Zu den Best Practices für Cisco IOS-Prozesse zählen Softwareversionskontrolle, Cisco IOS Syslog-Management, Problemmanagement, Konfigurationsstandardisierung und Verfügbarkeitsmanagement.

Best Practices	Details
Strategien und Tools für Cisco IOS Operations	Die erste Strategie des Cisco IOS-Betriebs besteht darin, die Umgebung so einfach wie möglich zu gestalten und Abweichungen bei der Konfiguration und den Cisco IOS-Versionen zu vermeiden. Die zweite Strategie besteht darin, Netzwerkfehler zu erkennen und schnell zu beheben.
Software-Versionskontrolle	Die Softwareversionskontrolle umfasst die Implementierung nur standardisierter Softwareversionen und die Überwachung des Netzwerks, um Software aufgrund der Nichtversionskonformität zu validieren oder möglicherweise zu ändern.
Proaktive Syslog-Verwaltung	Die Syslog-Erfassung, -Überwachung und -Analyse sind Fehlermanagementprozesse, die zur Behebung von mehr Cisco IOS-spezifischen Netzwerkproblemen empfohlen werden, die auf andere Weise schwer oder nicht zu identifizieren sind.
Problemmana	Detaillierte Problemmanagement-

gement	Prozesse, die Problemerkennung, Informationserfassung und einen gut analysierten Lösungspfad definieren. Diese Daten können zur Bestimmung der Ursache verwendet werden.
Standardisierung der Konfiguration	Konfigurationsstandards stellen die gängige Praxis dar, globale Standardkonfigurationsparameter wie Geräte und Services zu erstellen und beizubehalten, was zu einer globalen Konsistenz der Unternehmenskonfiguration führt.
Verfügbarkeitsmanagement	Das Verfügbarkeitsmanagement ist der Prozess der Qualitätsverbesserung, bei dem die Netzwerkverfügbarkeit als Metrik zur Qualitätsverbesserung eingesetzt wird.

Software-Lebenszyklus-Management - Prozessübersicht

Das Lifecycle-Management der Cisco IOS-Software ist definiert als die Gesamtheit der Planungs-, Design-, Implementierungs- und Betriebsprozesse, die für zuverlässige Softwareimplementierungen und Netzwerke mit hoher Verfügbarkeit empfohlen werden. Dazu gehören Prozesse zur Auswahl, Validierung und Pflege von Cisco IOS-Versionen im Netzwerk.

Das Lifecycle-Management für Cisco IOS-Software zielt darauf ab, die Netzwerkverfügbarkeit zu verbessern, indem die Wahrscheinlichkeit von Softwarefehlern, die in der Produktion festgestellt wurden, oder von Software-bezogenen Änderungen/Upgrades verringert wird. Die in dieser Dokumentation definierten Best Practices tragen dazu bei, solche Defekte und Änderungsfehler zu reduzieren, da viele Kunden von Cisco und das Cisco Advanced Services-Team praktische Erfahrungen gesammelt haben. Das Lifecycle-Management von Software kann anfänglich zu höheren Ausgaben führen, niedrigere Gesamtbetriebskosten können jedoch durch weniger Ausfälle und optimierte Bereitstellungs- und Supportmechanismen realisiert werden.

Planung - Entwicklung des Cisco IOS Management Framework

Die Planung ist die erste Phase des Cisco IOS-Managements, die ein Unternehmen dabei unterstützen soll, zu bestimmen, wann die Software aktualisiert werden muss, wo ein Upgrade durchgeführt werden muss und welche Prozesse zum Testen und Validieren potenzieller Images verwendet werden.

Zu den Best Practices zählen Definitionen der Softwareversionsspuren, Aktualisierungszyklen und Definitionen sowie die Erstellung eines internen Software-Zertifizierungsprozesses.

Strategie und Tools für die Cisco IOS-Planung

Beginnen Sie die Cisco IOS-Managementplanung mit einer ehrlichen Bewertung der aktuellen Praktiken, der Entwicklung erreichbarer Ziele und der Projektplanung. Die Selbstbeurteilung sollte durch den Vergleich von Best Practices in diesem Dokument mit Prozessen innerhalb Ihres Unternehmens erfolgen. Grundlegende Fragen sollten Folgendes umfassen:

- Verfügt mein Unternehmen über einen Softwarezertifizierungsprozess, der Softwaretests/-validierungen umfasst?
- Verfügt mein Unternehmen über Cisco IOS-Softwarestandards mit einer begrenzten Anzahl von Cisco IOS-Versionen, die im Netzwerk ausgeführt werden?
- Hat mein Unternehmen Schwierigkeiten, festzustellen, wann ein Upgrade der Cisco IOS-Software durchgeführt werden soll?
- Hat mein Unternehmen Schwierigkeiten, neue Cisco IOS-Software effizient und effektiv bereitzustellen?
- Hat mein Unternehmen nach der Bereitstellung Probleme mit der Cisco IOS-Stabilität, die die Kosten für Ausfallzeiten erheblich beeinträchtigen?

Im Anschluss an die Analyse sollte Ihr Unternehmen mit der Definition von Zielen für das Cisco IOS-Softwaremanagement beginnen. Zunächst sollten Sie eine funktionsübergreifende Gruppe von Managern und/oder Leads zusammenfassen, die aus Architekturplanungsgruppen, Engineering, Implementierung und Betrieb Nutzen ziehen, um Cisco IOS-Ziele und Projekte zur Prozessoptimierung zu definieren. Ziel der ersten Meetings sollte es sein, allgemeine Ziele, Rollen und Verantwortlichkeiten zu bestimmen, Aktionspunkte zuzuweisen und erste Projektpläne festzulegen. Definieren Sie außerdem wichtige Erfolgsfaktoren und -kennzahlen, um die Vorteile des Softwaremanagements zu ermitteln. Mögliche Kennzahlen:

- Verfügbarkeit (aufgrund von Softwareproblemen)
- Kosten von Software-Upgrades
- für Upgrades benötigte Zeit
- Anzahl der in der Produktion ausgeführten Softwareversionen
- Erfolgsrate bei Software-Upgrades/Fehlerquoten

Neben der allgemeinen Planung des Cisco IOS-Management-Frameworks definieren einige Unternehmen auch laufende Softwareplanungs-Meetings, die monatlich oder vierteljährlich stattfinden. Ziel dieser Meetings ist es, die aktuelle Softwarebereitstellung zu überprüfen und mit der Planung neuer Softwareanforderungen zu beginnen. Die Planung umfasst u. a. die Überprüfung oder Änderung aktueller Softwareverwaltungsprozesse oder die einfache Definition von Rollen und Verantwortlichkeiten für die verschiedenen Softwareverwaltungsphasen.

Die Werkzeuge in der Planungsphase bestehen ausschließlich aus Software Inventar Management Tools. Der CiscoWorks 2000 Resource Manager Essentials (RME) Inventory Manager ist das primäre Tool für diesen Bereich. Der CiscoWorks2000 RME Inventory Manager vereinfacht die Versionsverwaltung von Cisco Routern und Switches mithilfe webbasierter Reporting-Tools, die Cisco IOS-Geräte anhand von Softwareversion, Geräteplattform, Speichergröße und Gerätenamen melden und sortieren.

Definitionen der Softwareversionsverfolgung

Die erste Best Practice für die Planung der Cisco IOS Software-Verwaltung legt fest, wo die Softwarekonsistenz erhalten bleiben kann. Ein Software-Programmzweig ist definiert als eine einzigartige Gruppierung von Softwareversionen, die sich von anderen Bereichen nach geografischer Region, Plattformen, Modulen oder Funktionsanforderungen unterscheidet. Optimal: In einem Netzwerk sollte nur eine Softwareversion ausgeführt werden. Dadurch werden die Kosten für das Softwaremanagement erheblich gesenkt und eine konsistente und leicht verwaltbare Umgebung bereitgestellt. Tatsächlich müssen die meisten Unternehmen jedoch aufgrund von Funktions-, Plattform-, Migrations- und Verfügbarkeitsproblemen in bestimmten Bereichen mehrere Versionen des Netzwerks ausführen. In vielen Fällen funktioniert dieselbe Version nicht auf heterogenen Plattformen. In anderen Fällen kann die Organisation nicht warten,

bis eine Version alle Anforderungen erfüllt. Ziel ist es, die kleinsten Software-Tracks für das Netzwerk zu identifizieren, die für Tests/Validierung, Zertifizierung und Upgrades infrage kommen. In vielen Fällen kann das Unternehmen insgesamt etwas mehr Möglichkeiten haben, um die Kosten für Tests/Validierung, Zertifizierung und Upgrades zu senken.

Der erste Unterschied besteht in der Plattformunterstützung. In der Regel verfügen LAN-Switches, WAN-Switches, Core-Router und Edge-Router jeweils über separate Software-Tracks. Möglicherweise sind weitere Software-Programmzweige für bestimmte Funktionen oder Services erforderlich, z. B. Data-Link Switching (DLSw), Quality of Service (QoS) oder IP-Telefonie, insbesondere wenn diese Anforderung im Netzwerk lokalisiert werden kann.

Ein weiteres Kriterium ist die Zuverlässigkeit. Viele Unternehmen versuchen, die zuverlässigste Software für den Netzwerkkern und das Rechenzentrum auszuführen und bieten gleichzeitig neuere erweiterte Funktionen bzw. Hardware-Support am Netzwerk-Edge an. Andererseits sind Skalierbarkeits- oder Bandbreitenfunktionen häufig in Core- oder Rechenzentrumsumgebungen gefragt. Für bestimmte Plattformen, z. B. größere Verteilungsstandorte mit einer anderen WAN-Router-Plattform, sind möglicherweise weitere Programmzweige erforderlich. In der folgenden Tabelle sehen Sie ein Beispiel für eine Software-Track-Definition für ein großes Unternehmen.

Verfolgung	Bereich	Hardware-Plattformen	Funktionen	Cisco IOS-Version	Zertifizierungsstatus
1	LAN Core-Switching	6500	QoS	12.1 E(A8)	Tests
2	LAN Access Switch	2924XL 2948XL	Unidirectional Link Detection Protocol (UDLD), Spanning Tree Protocol (STP)	12,0(5,2)XU	Zertifiziert 01.03.2001
3	LAN-Distribution/ Zugriff	5500 6509	Supervisor 3	5.4(4)	Zertifiziert 01.07.01
4	Distribution Switch Route Switch Module (RSM)	RSM	Open Shortest Path First (OSPF) - Routing	12.0(11)	Zertifiziert 04.03.2002

5	WAN-Headend-Verteilung	7505 7507 7204 7206	OSPF Frame Relay	12.0(11)	Zertifiziert 01.11.201
6	WAN-Zugang	2600	OSPF Frame Relay	12.1(8)	Zertifiziert 01.06.01
7	IBM-Konnektivität	3600	SDLC-Headend (Synchronous Data Link Control)	11,3(8)T1	Zertifiziert 11.1.00

Auch die Zuweisung von Programmzweigen kann sich im Laufe der Zeit ändern. In vielen Fällen können Funktionen oder Hardware-Support in weitere Hauptsoftwareversionen integriert werden, sodass verschiedene Programmzweige gemeinsam migrieren können. Nach der Definition der Ablaufverfolgungsdefinitionen kann die Organisation mithilfe anderer definierter Prozesse zu Konsistenz und Validierung neuer Versionen migrieren. Track-Definitionen sind ebenfalls ein fortlaufender Vorgang. Jedes Mal, wenn eine neue Funktion, ein neuer Service, eine neue Hardware oder ein neues Modul erkannt wird, sollte ein neuer Programmzweig in Betracht gezogen werden.

Unternehmen, die einen Track-Prozess einleiten möchten, sollten mit neu definierten Track-Anforderungen beginnen, oder in einigen Fällen mit Stabilisierungsprojekten für bestehende Netzwerke. Ein Unternehmen kann auch einige identifizierbare Gemeinsamkeiten mit vorhandenen Softwareversionen aufweisen, die die Definition der aktuellen Spur ermöglichen. In den meisten Fällen ist eine schnelle Migration zu identifizierten Versionen nicht erforderlich, wenn der Kunde über eine ausreichende Netzwerkstabilität verfügt. Die Netzwerkarchitektur oder die Engineering-Gruppe ist normalerweise Eigentümer des Prozesses der Spurdefinition. In einigen Fällen ist möglicherweise eine Person für die Definition der Gleise zuständig. In anderen Fällen sind Projektleiter für die Entwicklung von Software-Anforderungen und neuen Track-Definitionen auf Basis individueller Projekte verantwortlich. Es empfiehlt sich auch, die Definitionen der Programmzweige vierteljährlich zu überprüfen, um festzustellen, ob neue Programmzweige erforderlich sind oder ob alte Programmzweige konsolidiert oder aktualisiert werden müssen.

Unternehmen, die Software-Tracks mit strikter Versionskontrolle identifizieren und pflegen, haben mit einer abnehmenden Anzahl an Softwareversionen im Produktionsnetzwerk den größten Erfolg. Dies führt in der Regel zu einer verbesserten Softwarestabilität und allgemeinen Netzwerkzuverlässigkeit.

Aktualisierungszyklus und Definitionen

Aktualisierungszyklusdefinitionen werden als grundlegende Qualitätsschritte in der Software definiert und dienen zur Bestimmung, wann ein Software-Upgrade-Zyklus eingeleitet werden soll. Mithilfe von Definitionen für den Aktualisierungszyklus kann ein Unternehmen einen Software-Upgrade-Zyklus ordnungsgemäß planen und die erforderlichen Ressourcen zuweisen. Ohne Aktualisierungszyklusdefinitionen steigt die Zuverlässigkeit der Software in der Regel aufgrund von Funktionsanforderungen in den aktuellen stabilen Versionen. Ein weiteres Risiko könnte darin

bestehen, dass Unternehmen die Möglichkeit verpassen, eine neue Version ordnungsgemäß zu testen und zu validieren, bevor die Nutzung der Produktion erforderlich ist.

Ein wichtiger Aspekt dieses Verfahrens ist die Ermittlung, wann und in welchem Umfang Softwareplanungsprozesse eingeleitet werden sollten. Dies liegt daran, dass eine der Hauptgründe für Softwareprobleme darin besteht, eine Funktion, einen Service oder eine Hardware-Funktionalität in der Produktion ohne gebührende Sorgfalt einzustellen oder ein Upgrade auf eine neue Cisco IOS-Version ohne Berücksichtigung von Überlegungen zum Softwaremanagement durchzuführen. Ein weiteres Problem ist das nicht-Upgrade. Viele Kunden stehen vor der schwierigen Aufgabe, Software über verschiedene Hauptversionen zu aktualisieren, indem sie normale Softwarezyklen und -anforderungen ignorieren. Die Schwierigkeit liegt in den Bildgrößen, Änderungen am Standardverhalten, Änderungen am CLI (Command Level Interpreter) und Protokolländerungen.

Cisco empfiehlt einen klar definierten Upgrade-Zyklus, der auf den in diesem Whitepaper definierten Best Practices basiert und bei Bedarf mit neuen Hauptfunktionen, Services oder Hardware-Support initiiert wird. Der Grad der Zertifizierung und der Prüfung/Validierung sollte (anhand des Risikos) analysiert werden, um die genauen Test-/Validierungsanforderungen zu ermitteln. Die Risikoanalyse kann nach geografischem Standort, logischem Standort (Core-, Distribution- oder Access-Layer) oder der geschätzten Anzahl der betroffenen Personen/Kunden durchgeführt werden. Wenn die Hauptfunktion oder die Hardware-Funktion in der aktuellen Version enthalten ist, sollten auch einige rationalisierte Upgrade-Zyklusprozesse initiiert werden. Wenn die Funktion relativ gering ist, sollten Sie das Risiko berücksichtigen und dann entscheiden, welche Prozesse initiiert werden sollen. Darüber hinaus sollte ein Softwareupgrade in maximal zwei Jahre erfolgen, um sicherzustellen, dass Ihr Unternehmen relativ aktuell bleibt und der Upgrade-Prozess nicht zu aufwändig ist.

Kunden sollten auch berücksichtigen, dass keine Bugfixes an Softwarezügen vorgenommen werden, die den Status "End of Life" (EOL) überschritten haben. Auch die geschäftlichen Anforderungen sollten berücksichtigt werden, da in vielen Umgebungen zusätzliche Funktionen mit nur wenigen oder gar keinen Test-/Validierungsprozessen und damit einhergehenden Ausfallzeiten toleriert oder sogar akzeptiert werden können. Kunden sollten bei der Prüfung ihrer Testanforderungen auch die neueren Daten berücksichtigen, die im Rahmen von Cisco Release-Vorgängen gesammelt wurden. Eine Analyse von Fehlern und Ursachen zeigte, dass die überwiegende Mehrheit der Fehlerursachen das Ergebnis von Entwicklern war, die innerhalb des betroffenen Software-Bereichs programmiert haben. Dies bedeutet, dass ein Unternehmen, das in einer vorhandenen Version eine bestimmte Funktion oder ein bestimmtes Modul zu seinem Netzwerk hinzufügt, wahrscheinlich einen Fehler im Zusammenhang mit dieser Funktion oder diesem Modul feststellen wird, dass jedoch die Wahrscheinlichkeit, dass die neue Funktion, Hardware oder das neue Modul andere Bereiche beeinflusst, viel geringer ist. Diese Daten sollten es Organisationen ermöglichen, die Testanforderungen zu senken, wenn neue Funktionen oder Module hinzugefügt werden, die in vorhandenen Versionen unterstützt werden, indem nur der neue Service oder die neue Funktion in Verbindung mit anderen aktivierten Diensten getestet wird. Die Daten sollten auch bei der Aktualisierung von Software berücksichtigt werden, die auf einigen kritischen Fehlern im Netzwerk basiert.

Die folgende Tabelle zeigt die empfohlenen Upgrade-Anforderungen für eine große Hochverfügbarkeitsfirma:

Software-Management-Trigger	Software-Lebenszyklus-Anforderung
Neuer Netzwerkservice.	Vollständige Softwarelebenszyklusvalidierun

Beispielsweise ein neuer ATM-Backbone oder ein neuer VPN-Service.	g mit Tests neuer Funktionen (in Verbindung mit anderen aktivierten Services), reduzierten Topologietests, Was-wäre-wenn-Leistungsanalyse und Anwendungsprofiltests
Neue Netzwerkfunktionen werden in der aktuellen Softwareversion nicht unterstützt. Beispiele sind QoS und Multiprotocol Label Switching (MPLS).	Vollständige Softwarelebenszyklusvalidierung einschließlich neuer Funktionstests in Kombination mit anderen aktivierten Services, reduzierten Topologietests, Was-wäre-wenn-Leistungsanalyse und Anwendungsprofiltests
Neue wichtige Funktion oder Hardwaremodul, das in der aktuellen Version vorhanden ist. Fügen Sie z. B. ein neues GigE-Modul, Multicast-Unterstützung oder DLSW hinzu.	Verwaltung von Kandidaten. Mögliche umfassende Validierung auf Basis der Versionserfordernisse. Mögliche eingeschränkte Tests/Validierung, wenn das Kandidatenmanagement die aktuelle Version als potenziell akzeptabel ansieht.
Geringfügige Funktionserweiterung. Zum Beispiel ein TACACS-Gerät für die Zugriffskontrolle.	Berücksichtigen Sie das mögliche Management anhand des Risikos der Funktion. Testen oder testen Sie die neue Funktion basierend auf dem Risiko.
Software wird für zwei Jahre oder vierteljährlich zur Softwareüberprüfung produziert.	Management von Kandidaten und Geschäftsentscheidungen in Bezug auf das vollständige Lebenszyklusmanagement, um die aktuelle unterstützbare Version zu identifizieren.

Notfall-Upgrades

In einigen Fällen müssen Software-Upgrades aufgrund von schwerwiegenden Fehlern durchgeführt werden. Dies kann zu Problemen führen, wenn die Organisation nicht über eine Notfallaktualisierung verfügt. Die Probleme bei Software reichen von nicht verwalteten Software-Upgrades, bei denen Software ohne Lebenszyklus-Management aktualisiert wird, bis hin zu Situationen, in denen Netzwerkgeräte ständig abstürzen, das Unternehmen jedoch keine Upgrades vornimmt, da die Zertifizierung/Tests für die nächste mögliche Version noch nicht abgeschlossen ist. Cisco empfiehlt in diesen Situationen, in denen begrenzte Tests und Pilotprojekte in weniger geschäftskritischen Bereichen des Netzwerks durchgeführt werden, ein Verfahren zur Aktualisierung in Notfällen.

Wenn schwerwiegende Fehler ohne erkennbare Problemumgehung auftreten und das Problem mit Softwarefehlern zusammenhängt, empfiehlt Cisco, den Cisco Support vollständig zu

engagieren, um den Fehler zu isolieren und festzustellen, ob oder wann eine Lösung verfügbar ist. Wenn die Lösung verfügbar ist, empfiehlt Cisco einen Aktualisierungszyklus für Notfälle, um schnell festzustellen, ob das Problem mit begrenzter Ausfallzeit behoben werden kann. In den meisten Fällen führt ein Unternehmen eine unterstützte Version des Codes aus, und die Problembehebung ist in einer neueren Zwischenversion der Software verfügbar.

Organisationen können sich auch auf potenzielle Notfall-Upgrades vorbereiten. Die Vorbereitung umfasst die Migration zu unterstützten Cisco IOS-Versionen und die Identifizierung/Entwicklung von potenziellen Austauschversionen innerhalb desselben Cisco IOS-Zuges wie der zertifizierten Version. Unterstützte Software ist wichtig, da sie bedeutet, dass die Entwicklung von Cisco immer noch Bugfixes zum identifizierten Software-Train hinzufügt. Durch die Pflege der unterstützten Software im Netzwerk wird die Validierungszeit aufgrund der vertrauten und stabileren Codebasis reduziert. In der Regel handelt es sich bei einem möglichen Ersatz um ein neues Zwischensoftware-Image innerhalb desselben Cisco IOS-Zuges ohne zusätzliche Funktionen oder Hardware-Support. Eine Strategie für den Austausch von Software ist besonders wichtig, wenn sich das Unternehmen in der Anfangsphase der Einführung eines bestimmten Software-Zuges befindet.

Zertifizierungsprozess

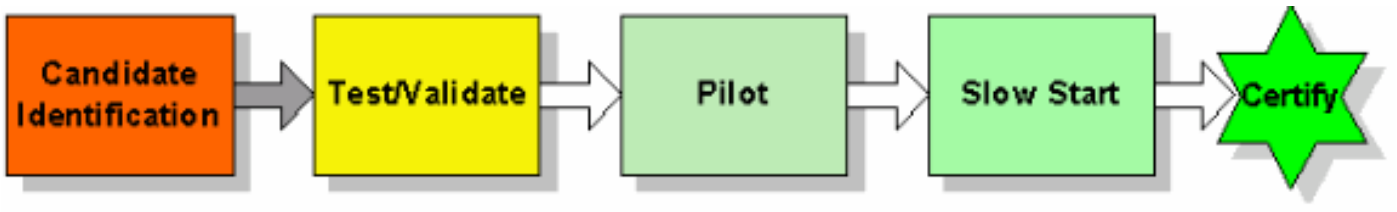
Durch einen Zertifizierungsprozess wird sichergestellt, dass validierte Software in der Produktionsumgebung des Unternehmens konsistent bereitgestellt wird. Die Schritte des Zertifizierungsprozesses sollten die Identifikation von Nachverfolgen, Definitionen von Aktualisierungszyklen, die Verwaltung potenzieller Kunden, Tests/Validierungen und eine gewisse Verwendung der Pilotproduktion umfassen. Ein einfacher Zertifizierungsprozess trägt jedoch weiterhin dazu bei, sicherzustellen, dass konsistente Softwareversionen innerhalb der identifizierten Programmzweige bereitgestellt werden.

Starten Sie einen Zertifizierungsprozess, indem Sie Personen aus Architektur, Technik/Bereitstellung und Betrieb identifizieren, die den Zertifizierungsprozess entwerfen und verwalten. Die Gruppe sollte zunächst Geschäftsziele und Ressourcenfunktionen berücksichtigen, um sicherzustellen, dass der Zertifizierungsprozess auch weiterhin erfolgreich verläuft. Weisen Sie anschließend Personen oder Gruppen die Gesamtverantwortung für die wichtigsten Schritte im Zertifizierungsprozess zu, einschließlich der Ablaufverfolgung, Lebenszyklus-Upgrade-Definitionen, Tests/Validierung und Pilotprojekte. Jeder dieser Bereiche sollte innerhalb der Organisation definiert, genehmigt und formell kommuniziert werden.

Enthalten sind auch Richtlinien für die Qualität oder Genehmigung in jeder Phase des Zertifizierungsprozesses. Dies wird manchmal auch als Qualitätsgatterprozess bezeichnet, da bestimmte Qualitätskriterien erfüllt werden müssen, bevor der Prozess zum nächsten Schritt übergehen kann. Dadurch wird sichergestellt, dass der Zertifizierungsprozess effektiv ist und die zugewiesenen Ressourcen wert ist. Im Allgemeinen, wenn Probleme mit der Qualität in einem Bereich gefunden werden, der Prozess treibt den Aufwand in einen Schritt zurück.

Softwarekandidaten erfüllen die festgelegten Zertifizierungskriterien aufgrund der Softwarequalität oder des unerwarteten Verhaltens möglicherweise nicht. Wenn Probleme mit Auswirkungen auf die Umwelt festgestellt werden, sollte das Unternehmen über ein optimiertes Verfahren verfügen, um eine spätere vorläufige Version zu zertifizieren. Dies trägt dazu bei, die Ressourcenanforderungen zu reduzieren, und ist im Allgemeinen wirksam, wenn das Unternehmen weiß, was geändert wurde und welche Fehler behoben wurden. Es ist nicht ungewöhnlich, dass ein Unternehmen ein Problem mit einem anfänglichen Kandidaten hat und eine spätere vorläufige Cisco IOS-Version zertifiziert. Organisationen können auch eine

Zertifizierung mit begrenztem Funktionsumfang anbieten oder Vorbehalte vorbringen, wenn Probleme bestehen, und ein Upgrade auf eine später vollständig zertifizierte Version durchführen, wenn eine neue Zwischenzeit validiert wurde. Das nachfolgende Flussdiagramm ist ein grundlegender Zertifizierungsprozess mit Qualitätsterminen (eine Überprüfung nach jedem Block):



Design - Auswahl und Validierung von Cisco IOS-Versionen

Durch eine klar definierte Methodik für die Auswahl und Validierung von Cisco IOS-Versionen können Unternehmen ungeplante Ausfallzeiten aufgrund erfolgloser Aktualisierungsversuche und ungeplanter Softwarefehler reduzieren.

Die Entwurfsphase umfasst die Verwaltung potenzieller Kandidaten sowie Tests und Validierungen. Das Kandidatenmanagement ist der Prozess, mit dem bestimmte Versionen für die definierten Software-Tracks identifiziert werden. Das Testen/Validieren ist Teil des Zertifizierungsprozesses und stellt sicher, dass die angegebene Softwareversion innerhalb des erforderlichen Programmzweigs erfolgreich ist. Das Testen/Validieren sollte in einer Laborumgebung mit reduzierter Topologie und Konfiguration erfolgen, die der Produktionsumgebung sehr ähnlich ist.

Strategie und Tools für die Auswahl und Validierung von Cisco IOS

Jedes Unternehmen sollte über einen Prozess für die Auswahl und Validierung von Cisco IOS-Standardversionen für das Netzwerk verfügen, beginnend mit einem Prozess für die Auswahl der Cisco IOS-Version. Ein funktionsübergreifendes Team aus Architektur, Technik und Betrieb sollte den möglichen Managementprozess definieren und dokumentieren. Nach der Genehmigung sollte der Prozess an die entsprechende Liefergruppe weitergeleitet werden. Es wird außerdem empfohlen, eine Standard-Managementvorlage zu erstellen, die mit den identifizierten Kandidateninformationen aktualisiert werden kann.

Nicht alle Unternehmen verfügen über eine hoch entwickelte Laborumgebung, die die Produktionsumgebung einfach nachahmen kann. Einige Unternehmen überspringen Labortests aufgrund der Kosten und der Möglichkeit, eine neue Version im Netzwerk ohne größere geschäftliche Auswirkungen als Pilotprojekt einzusetzen. Unternehmen, die sich für eine hohe Verfügbarkeit entscheiden, werden jedoch ermutigt, ein Labor zu erstellen, das das Produktionsnetzwerk nachahmt, und einen Test-/Validierungsprozess zu entwickeln, um eine hohe Testabdeckung für neue Cisco IOS-Versionen sicherzustellen. Die Einrichtung der Übung sollte etwa sechs Monate in Anspruch nehmen. Während dieser Zeit sollte die Organisation an der Erstellung spezifischer Testpläne und -prozesse arbeiten, um sicherzustellen, dass das Labor in vollem Umfang genutzt wird. Für Cisco IOS bedeutet dies die Erstellung spezifischer Cisco IOS-Testpläne für jeden erforderlichen Software-Programmzweig. Diese Prozesse sind in größeren Unternehmen von entscheidender Bedeutung, da viele Labs nicht für neue Produkte und Software-Einführungen verwendet werden.

In den folgenden Abschnitten werden die Tools für das Management und die Tests/Validierung von Kandidaten für die Auswahl und Validierung von Cisco IOS kurz beschrieben.

Tools für das Kandidaten-Management

Hinweis: Um die meisten der unten bereitgestellten Tools zu verwenden, müssen Sie ein registrierter Benutzer sein und angemeldet sein.

- Versionshinweise - Enthält Informationen zur Hardware-, Modul- und Funktionsunterstützung einer Version. Die Versionshinweise sollten während des Kandidatenmanagements überprüft werden, um sicherzustellen, dass der gesamte erforderliche Hardware- und Software-Support in der potenziellen Version vorhanden ist, und um mögliche Migrationsprobleme, einschließlich unterschiedlicher Standardverhalten oder Upgrade-Anforderungen, zu verstehen.

Test- und Validierungstools

Test- und Validierungstools werden zum Testen und Validieren von Netzwerklösungen einschließlich neuer Hardware, Software und Anwendungen verwendet.

- **Traffic Generators** (Datenverkehrsgeneratoren): Generieren von Datenverkehrsströmen mit mehreren Protokollen und Paketraten, mit denen die Übertragungsrate für eine bestimmte Verbindung anhand bestimmter Protokolle modelliert wird. Benutzer können die Quell-, Ziel-MAC- und Socketnummern angeben. Diese Werte können in festgelegten Schritten erhöht oder als statische/feste oder in zufälligen Schritten konfiguriert werden. Datenverkehrsgeneratoren können Pakete für die folgenden Protokolle generieren:IPInternetwork Packet Exchange (IPX)DECnetAppleXerox Network Systems (XNS)Internet Control Message Protocol (ICMP)Internet Group Management Protocol (IGMP)Connectionless Network Service (CLNS)User Datagram Protocol (UDP)Virtual Integrated Network Service (VINES)DatenverbindungspaketeTools sind über Agilent und Spirent Communications verfügbar.
- **Packet Counter/Capture/Decoder (Sniffer)** - Ermöglicht dem Kunden, Pakete auf allen Paket- und Datenverbindungsebenen selektiv zu erfassen und zu decodieren. Das Tool kann es dem Benutzer ermöglichen, die Filter anzugeben, sodass nur die angegebenen Protokolldaten erfasst werden können. Mithilfe von Filtern kann der Benutzer außerdem festlegen, dass die Pakete einer bestimmten IP-Adresse, Portnummer oder MAC-Adresse zugeordnet werden. Tools sind von Sniffer Technologies erhältlich.
- **Network Simulator/Emulator** - Ermöglicht dem Kunden, die Routing-Tabellen bestimmter Router auf Basis der Anforderungen des Produktionsnetzwerks zu füllen. Unterstützt die Generierung von Routern wie IP Routing Information Protocol (RIP), OSPF, Intermediate System-to-Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) und Border Gateway Protocol (BGP). Tools sind über PacketStorm Communications und Spirent Communications verfügbar.
- **Session Emulators** (**Sitzungsemulatoren**): Generieren von Multiprotokoll-Datenverkehrsströmen in einem Gleitfenster und können Datenverkehrsströme mit mehreren Protokollen über das Testnetzwerk an das empfangende Gerät senden. Das empfangende Gerät sendet die Pakete zurück an die Quelle. Das Quellgerät überprüft die Anzahl der gesendeten, empfangenen, nicht sequenzierten Pakete und Fehlerpakete. Das Tool bietet außerdem die Flexibilität, die Fensterparameter im Transmission Control Protocol (TCP) zu definieren, wodurch die Client/Server-Datenverkehrssitzungen im Labornetzwerk eng nachahmt werden. Die Tools sind über Empirix verfügbar.
- **Network Emulators** für **große Umgebungen** - Unterstützen Sie das Testen der Skalierbarkeit

größerer Umgebungen. Diese Tools können Kontrolltypen-Datenverkehr in eine Labortopologie erstellen und leicht in diese injizieren, um eine Produktionsumgebung genauer nachzuahmen. Zu den Funktionen gehören Route Injectors, Protokoll-Nachbarn und Layer-2-Protokoll-Nachbarn. Tools sind über Agilent und Spirent Communications verfügbar.
- **WAN-Simulatoren** - Ideal für das Testen von Anwendungsdatenverkehr in Unternehmen, bei dem Bandbreite und Verzögerungen potenziell ein Problem darstellen. Diese Tools ermöglichen es Unternehmen, eine Anwendung lokal mit der geschätzten Verzögerung und Bandbreite zu testen, um zu sehen, wie die Anwendung über das WAN funktioniert. Diese Tools werden häufig für die Anwendungsentwicklung und die Erstellung von Anwendungsprofilen in Unternehmen eingesetzt. Adtech, ein Geschäftsbereich von Spirent Communications und Shunra , stellt WAN-Simulationstools bereit.

Kandidaten-Management

Unter "Kandidaten-Management" versteht man den Prozess zur Ermittlung der Softwareversionsanforderungen und der potenziellen Risiken für die jeweilige Hardware und die aktivierten Funktionssätze. Es wird empfohlen, dass ein Unternehmen vier bis acht Stunden damit verbringt, Softwareanforderungen, Versionshinweise, Softwarefehler und potenzielle Risiken gründlich zu prüfen, bevor es eine Veröffentlichung testet. Im Folgenden wird die Grundlage für die Bewerberverwaltung beschrieben:

- Identifizieren Sie Softwarekandidaten mithilfe der Cisco Connection Online (CCO)-Tools.
- Reifegrad der Risikoanalyse-Software, neue Funktionen oder Code-Support
- Identifizieren und Nachverfolgen bekannter Softwarefehler, Probleme und Anforderungen während des gesamten Lebenszyklus
- Ermitteln Sie das Standardkonfigurationsverhalten des ausgewählten Bildes.
- Beibehaltung von Kandidaten für die Aus- und Weiterleitung bei potenziellen Änderungen.
- Bug-Scrubs.
- Cisco Advanced Services-Support.

Mit der zunehmenden Anzahl von Cisco Produktionen und Softwareschulungen wurde die Identifizierung von Softwarekandidaten immer komplexer. CCO verfügt jetzt über mehrere Tools, darunter den Cisco IOS-Upgrade-Planer, das Tool zur Suche von Software, die Matrix zur Kompatibilität von Software und Hardware sowie das Tool zur Produktaktualisierung, mit dem Unternehmen potenzielle Veröffentlichungskandidaten identifizieren können. Diese Tools finden Sie unter http://www.cisco.com/cisco/software/navigator.html.

Analysieren Sie anschließend das Risiko potenzieller Softwarekandidaten. Hierbei wird ermittelt, wo sich die Software derzeit in der Laufzeitkurve befindet. Anschließend werden die Anforderungen für die Bereitstellung mit dem potenziellen Risiko des Veröffentlichungskandidaten abgewogen. Wenn ein Unternehmen beispielsweise Software für die frühzeitige Bereitstellung in einer kritischen Hochverfügbarkeitsumgebung bereitstellen möchte, sollten die damit verbundenen Risiken und Ressourcenanforderungen für eine erfolgreiche Zertifizierung in Betracht gezogen werden. Ein Unternehmen sollte mindestens Software-Management-Ressourcen für Situationen mit höherem Risiko hinzufügen, um Erfolg zu gewährleisten. Wenn jedoch eine Version für die allgemeine Bereitstellung (GD) verfügbar ist, die die Anforderungen eines Unternehmens erfüllt, werden weniger Ressourcen für das Software-Management benötigt.

Wenn potenzielle Releases und Risiken identifiziert werden, führen Sie einen Bug Scrub durch, um festzustellen, ob identifizierte schwerwiegende Fehler vorliegen, die möglicherweise die Zertifizierung verhindern würden. Die Cisco Bug Watcher-, Bug Navigator- und Bug Watcher-

Agenten können dabei helfen, potenzielle Probleme zu identifizieren. Sie sollten während des gesamten Softwarelebenszyklus zur Identifizierung potenzieller Sicherheits- oder Defektprobleme verwendet werden.

Ein neuer Softwarekandidat sollte ebenfalls auf mögliche Standardkonfigurationsverhalten überprüft werden. Dies kann durch Überprüfen der Versionshinweise für das neue Software-Image und durch Überprüfen der Konfigurationsunterschiede mit dem potenziellen Image auf den festgelegten Plattformen erreicht werden. Das Management von Kandidaten kann auch die Identifizierung von Back-Out- oder Go-To-Versionen beinhalten, wenn die ausgewählte Version zu einem bestimmten Zeitpunkt des Prozesses die Zertifizierungskriterien nicht erfüllt. Durch die Überwachung von Fehlern im Zusammenhang mit Funktionen für eine bestimmte Spur kann eine Organisation potenzielle Kandidaten für Zertifizierungen verwalten.

Cisco Advanced Services ist außerdem ein hervorragendes Tool für das Management potenzieller Kunden. Diese Gruppe bietet weitere Einblicke in den Entwicklungsprozess und die Zusammenarbeit zwischen einer großen Anzahl von Branchenexperten in vielen unterschiedlichen Branchen-Umgebungen. Im Cisco Support gibt es in der Regel die besten Bug Scrubs- oder Kandidat-Management-Funktionen, da die Softwareversionen anderer Unternehmen über umfangreiches Know-how und Transparenz verfügen.

Tests und Validierung

Tests und Validierungen sind ein wichtiger Aspekt von Best Practices für das Management und der Netzwerke mit hoher Verfügbarkeit insgesamt. Sachgerechtes Testen kann die Ausfallzeiten der Produktion erheblich reduzieren, die Schulung der Mitarbeiter des Netzwerk-Supports erleichtern und die Netzwerkimplementierungsprozesse optimieren. Um jedoch wirksam zu sein, muss die Organisation die erforderlichen Ressourcen für den Aufbau und die Wartung der geeigneten Laborumgebung bereitstellen, die erforderlichen Ressourcen für die Durchführung der richtigen Tests einsetzen und eine empfohlene Testmethodik verwenden, die auch die Erfassung von Messwerten umfasst. Ohne einen dieser Bereiche entspricht ein Test- und Validierungsprozess möglicherweise nicht den Erwartungen eines Unternehmens.

Die meisten Unternehmen verfügen nicht über die empfohlene Testumgebung. Aus diesem Grund haben viele Unternehmen Lösungen nicht korrekt bereitgestellt, Netzwerkänderungen nicht durchgeführt oder Softwareprobleme festgestellt, die in einer Laborumgebung isoliert worden sein könnten. In einigen Umgebungen ist dies akzeptabel, da die Kosten von Ausfallzeiten die Kosten einer anspruchsvollen Laborumgebung nicht ausgleichen. In vielen Unternehmen können Ausfallzeiten jedoch nicht toleriert werden. Diese Organisationen werden dringend aufgefordert, die empfohlenen Testlabore, Testtypen und Testmethoden zu entwickeln, um die Qualität des Produktionsnetzwerks zu verbessern.

Testlabor und -umgebung

Das Labor sollte ein abgelegener Bereich sein, in dem genügend Platz für Schreibtische, Workbenches, Testgeräte sowie Geräte-Schränke oder -Racks vorhanden ist. Die meisten großen Unternehmen benötigen zwischen vier und zehn Racks, um die Produktionsumgebung nachzuahmen. Es wird empfohlen, eine Testumgebung aufrechtzuerhalten, während Tests ausgeführt werden. Dadurch wird verhindert, dass Labortests aufgrund anderer Lab-Prioritäten, wie z. B. Hardwarefreigabe, Schulungen oder Implementierungsbeispiele, unterbrochen werden. Die logische Sicherheit wird ebenfalls empfohlen, um zu verhindern, dass betrügerische Routen in das Produktionsnetzwerk eindringen oder unerwünschter Datenverkehr das Labor verlassen kann. Dies kann mithilfe von Routing-Filtern und erweiterten Zugriffslisten auf einem Gateway-Router im

Labor erfolgen. Die Anbindung an das Produktionsnetzwerk ist für Software-Downloads und den Zugriff von der Produktionsumgebung auf das Labornetzwerk hilfreich.

Die Labortopologie sollte in der Lage sein, die Produktionsumgebung für bestimmte Testpläne nachzuahmen. Es wird empfohlen, Hardware-, Netzwerktopologie- und Funktionskonfigurationen zu reproduzieren. Natürlich ist eine Reproduktion der eigentlichen Topologie nahezu unmöglich, aber man kann die Netzwerkhierarchie und die Interaktion zwischen den Produktionsgeräten reproduzieren. Dies ist wichtig für die Protokoll- oder Funktionsinteraktion zwischen mehreren Geräten. Einige Testtopologien sind je nach Software-Testanforderungen unterschiedlich. So sollten beispielsweise für Cisco IOS-Tests am WAN-Edge keine Geräte oder Tests vom LAN-Typ erforderlich sein, sondern nur WAN-Edge-Router und WAN-Distribution-Router. Der Schlüssel liegt darin, die Softwarefunktionalität nachzuahmen, ohne die Produktion zu duplizieren. In einigen Fällen können Tools sogar verwendet werden, um groß angelegtes Verhalten nachzuahmen, z. B. die Anzahl der Protokollnachbarn und die Anzahl der Routing-Tabellen.

Außerdem werden Tools benötigt, um bei einigen Testtypen zu helfen, indem die Nachahmung der Produktionsumgebung und die Erfassung von Testdaten verbessert werden. Zu den Tools, die die Nachahmung der Produktion unterstützen, gehören Traffic Collectors, Traffic Generators und WAN-Simulationsgeräte. Smartbits ist ein gutes Beispiel für ein Gerät, das Netzwerkverkehr erfassen und wiedergeben oder große Datenmengen generieren kann. Ein Unternehmen kann auch von Geräten profitieren, die beim Sammeln von Daten helfen, z. B. Protokollanalysatoren.

Die Übung erfordert auch eine gewisse Verwaltung. Viele größere Unternehmen verfügen über einen Vollzeit-Labormanager, der für die Verwaltung des Labornetzwerks verantwortlich ist. Andere Unternehmen nutzen vorhandene Architektur- und Technikerteams für die Laborvalidierung. Zu den Aufgaben des Labormanagements gehören die Bestellung von Laborgeräten und die Bestandsverfolgung, die Verkabelung, das physische Platzmanagement, die Definition von Laborregeln und -richtungen, die Planung von Übungen, die Erstellung von Labortopologien, das Schreiben von Testplänen, die Durchführung von Labortests und das Management potenzieller identifizierter Probleme.

Testtypen

Insgesamt gibt es viele verschiedene Arten von Tests, die durchgeführt werden können. Bevor ein vollständiges Testlabor und ein Testplan erstellt werden, der alles in einer Vielzahl von Konfigurationen testen kann, sollte ein Unternehmen die verschiedenen Testtypen, den Zweck des Tests und die Frage verstehen, ob Cisco Engineering, technisches Marketing oder Kundenbetreuung für einige der verschiedenen Tests verantwortlich sein sollte oder sein könnte. Kundentestpläne decken im Allgemeinen die exponierteren Testtypen ab. Die folgende Tabelle hilft, die verschiedenen Testtypen zu verstehen, wann die Tests durchgeführt werden sollten, und verantwortliche Parteien.

Von den unten beschriebenen Tests ist das ordnungsgemäße Testen der spezifischen Funktionen, der Topologie und des Anwendungs-Mixes eines Unternehmens normalerweise der wertvollste. Es ist wichtig zu wissen, dass Cisco alle Funktionen und Regressionstests durchführt. Cisco ist jedoch nicht in der Lage, das Anwendungsprofil Ihres Unternehmens mit Ihrer spezifischen Kombination aus Topologie, Hardware und konfigurierten Funktionen zu testen. Tatsächlich ist es nicht möglich, die gesamte Bandbreite an Funktionen, Hardware, Modulen und Topologiepermutationen zu testen. Darüber hinaus kann Cisco die Interoperabilität mit Geräten von Drittanbietern nicht testen. Cisco empfiehlt, die genaue Kombination aus Hardware, Modulen, Funktionen und Topologie in der Umgebung zu testen. Diese Tests sollten in einem Labor mit einer zusammengefassten Topologie durchgeführt werden, die die Produktionsumgebung Ihres Unternehmens zusammen mit anderen unterstützenden Testtypen wie Leistung, Interoperabilität,

Ausfall und Einbrennen darstellt.

Test	Testübersicht	Prüfverantwortung
Merkmale und Funktionen	Bestimmt, ob grundlegende Cisco IOS-Funktionen und Cisco Hardwaremodule wie angekündigt funktionieren. Funktionen oder Module sowie Konfigurationsoptionen für Funktionen sollten getestet werden. Das Entfernen und Hinzufügen von Konfigurationen sollte getestet werden. Grundlegende Ausfalltests und Einbrennungstests sind enthalten.	Cisco Gerätetests
Regression	Bestimmt, ob die Funktion oder das Modul in Verbindung mit anderen Modulen und Funktionen funktioniert und ob die Cisco IOS-Version in Verbindung mit anderen Cisco IOS-Versionen in Bezug auf die definierten Funktionen funktioniert. Beinhaltet einige Tests zum Einbrennen und Ausfällen.	Regressionstests von Cisco
Grundlegende Geräteleistung	Bestimmt die grundlegende Leistung der Funktion oder des Moduls, um	Cisco Gerätetests

	festzustellen, ob die Cisco IOS-Funktion oder die Hardwaremodule die Mindestanforderungen bei der Auslastung erfüllen.	
Topologie/Funktion/Hardwarekombination	Bestimmt, ob Funktionen und Module in einer bestimmten Topologie und Modul-/Feature-/Hardwarekombination wie erwartet funktionieren. Diese Tests sollten die Protokollüberprüfung, die Funktionsüberprüfung, die Befehlsüberprüfung **anzeigen**, Einbrenntests und Ausfalltests umfassen.	Cisco testet standardmäßige, angekündigte Topologien in Laboren wie Enterprise Solutions Engineering (ESE) und Network Solutions Integration Test Engineering (NSITE). Kunden mit hoher Verfügbarkeit sollten nach Bedarf Kombinationen von Funktionen, Modulen und Topologien testen, insbesondere mit Early-Adopter-Software und nicht standardmäßigen Topologien.
Ausfall (Was-falls)	Beinhaltet häufige Ausfallarten oder Verhaltensweisen, die in einer bestimmten Funktions-/Modul-/Topologieumgebung auftreten können, sowie potenzielle Auswirkungen auf die Funktionalität. Ausfalltests	Cisco ist für grundlegende Ausfalltests verantwortlich. Kunden sind letztendlich für Leistungsprobleme bei Ausfällen im Zusammenhang mit der Skalierbarkeit ihrer individuellen Umgebung verantwortlich. Ausfalltests sollten möglichst

	umfassen den Austausch von Karten, Verbindungs-Flaps, Gerätefehler, Verbindungsausfälle und Kartenausfälle.	im Kundenlabor durchgeführt werden.
Netzwerkleistung (Was-wenn)	Untersucht die Gerätelast in Bezug auf eine bestimmte Kombination aus Funktion, Hardware und Topologie. Der Schwerpunkt liegt auf der Geräteleistung und -leistung wie CPU, Arbeitsspeicher, Puffernutzung und Verbindungsauslastung im Verhältnis zu einem festgelegten Datenverkehrstyp und Ressourcenanforderungen für Protokolle, Nachbarn, Anzahl der Routen und andere Funktionen. Der Test trägt zur Skalierbarkeit in größeren Umgebungen bei.	Letztendlich sind die Kunden für die Last und Skalierbarkeit der Geräte verantwortlich. Bedenken hinsichtlich der Auslastung und Skalierbarkeit werden häufig von Cisco Sales oder Advanced Services angesprochen und häufig in Cisco Labs wie den Customer Proof-of-Concept Labs (CPOC) getestet.
Fehlerbehebung	Stellt sicher, dass Fehlerbehebungen den identifizierten Fehler beheben.	Cisco testet Bugfixes, um sicherzustellen, dass der Fehler behoben wird. Kunden sollten auch testen, um

		sicherzustellen, dass der Fehler behoben ist und der Fehler keinen anderen Aspekt des Moduls oder der Funktion beschädigt. Maintenance Releases sind Regressionstests, Zwischenveröffentlichungen sind es in der Regel jedoch nicht.
Netzwerkmanagement	Gegenstand: SNMP-Verwaltungsfunktionen (Simple Network Management Protocol), SNMP MIB-Variablengenauigkeit, Trap-Unterstützung und Syslog-Unterstützung	Cisco testet die grundlegenden SNMP-Funktionen und die Genauigkeit der MIB-Variablen. Kunden sollten die Ergebnisse des Netzwerkmanagements validieren und sind letztendlich für die Managementstrategie und -methodik für die Bereitstellung neuer Technologien verantwortlich.
Netzwerkemulation im großen Stil	Bei der groß angelegten Netzwerkemulation werden Tools wie der Router-Simulator von Agilent und die Testtools-Suite von Spirent verwendet, um größere Umgebungen zu simulieren. Dazu gehören Protokollnachbarn, Anzahl der Frame-Relay Permanent	Cisco Kunden sind in der Regel für die Aspekte der Netzwerksimulationstests verantwortlich, die ihre Netzwerkumgebung reproduzieren. Dazu gehören u. a. die Anzahl der Routing-Protokoll-Nachbarn/-Adjacencies und die zugehörigen Routing-Tabellengrößen

	Virtual Circuits (PVC), Größe der Routing-Tabellen, Cache-Einträge und andere Ressourcen, die normalerweise in der Produktion benötigt werden und nicht standardmäßig im Labor vorhanden sind.	und andere Ressourcen, die in der Produktion sind.
Interoperabilität	Testt alle Aspekte der Verbindung mit Netzwerkgeräten von Drittanbietern, insbesondere wenn Protokoll- oder Signalisierungsinteroperabilität erforderlich ist.	Cisco Kunden sind in der Regel für alle Aspekte der Interoperabilitätstests verantwortlich.
Einbrennen	Gegenstand: Router-Ressourcen im Laufe der Zeit Bei Einbrennungstests muss ein Gerät in der Regel mit einer gewissen Auslastung ausgestattet werden, um die Ressourcenauslastung einschließlich Arbeitsspeicher, CPU und Puffer im Laufe der Zeit zu untersuchen.	Cisco führt einfache Einbrennungstests durch. Kundentests werden in Bezug auf eindeutige Topologie-, Geräte- und Funktionskombinationen empfohlen.

Testmethodik

Sobald eine Organisation weiß, was sie testet, sollte eine Methodik für den Testprozess entwickelt werden. Der Zweck einer Best Practice-Testmethodik besteht darin, sicherzustellen, dass die vereinbarten Tests umfassend, gut dokumentiert, leicht reproduzierbar und wertvoll sind, um potenzielle Produktionsprobleme zu identifizieren. Die Dokumentation und das Reproduzieren von

Laborszenarien ist besonders wichtig, um spätere Versionen zu testen oder um Bugfixes in der Laborumgebung zu testen. Die Schritte einer Testmethodik sind im Folgenden dargestellt. Einige Testschritte können auch gleichzeitig ausgeführt werden.

1. Erstellen Sie eine Testtopologie, die die zu testende Produktionsumgebung simuliert. Eine WAN-Edge-Testumgebung kann nur einige Core-Router und einen Edge-Router umfassen, während ein LAN-Test mehr Geräte umfassen kann, die die Umgebung am besten repräsentieren können.
2. Konfigurieren Sie Features, die die Produktionsumgebung simulieren. Die Konfiguration der Übungsgeräte sollte eng mit der erwarteten Hardware- und Softwarekonfiguration der Produktionsgeräte übereinstimmen.
3. Erstellen Sie einen Testplan, definieren Sie Tests und Ziele, dokumentieren Sie die Topologie und definieren Sie Funktionstests. Zu den Tests gehören die grundlegende Protokollvalidierung, die Befehlsvalidierung, Ausfalltests und Einbrennen-in-Tests. Ein Beispiel für einen bestimmten Test in einem Testplan finden Sie in der folgenden Tabelle.
4. Validieren der Routing- und Protokollfunktionen Dokumentieren oder Baseline-erwartete Befehlsergebnisse **zeigen**. Die Protokolle sollten sowohl Layer-2-Protokolle wie ATM, Frame-Relay, Cisco Discovery Protocol (CDP), Ethernet und Spanning-Tree als auch Layer-3-Protokolle wie IP, IPX und Multicast umfassen.
5. Überprüfen der Funktionsfunktionalität Dokumentieren oder Baseline-erwartete Befehlsergebnisse **zeigen**. Zu den Funktionen gehören globale Konfigurationsbefehle und alle wichtigen Funktionen wie Authentifizierung, Autorisierung und Abrechnung (AAA).
6. Simulieren Sie die Last, die in der Produktionsumgebung erwartet wird. Die Lastsimulation kann mit Traffic Collectors/Generatoren durchgeführt werden. Validieren Sie erwartete Nutzungsvariablen von Netzwerkgeräten wie CPU, Arbeitsspeicher, Puffer-Auslastung und Schnittstellenstatistiken, um Paketverluste zu untersuchen. Dokumentieren oder Baseline-erwartete Befehlsergebnisse **zeigen**.
7. Führen Sie Ausfalltests durch, bei denen erwartet wird, dass das Gerät und die Software mit dem Problem oder der Verhinderung einer zu hohen Belastung umgehen. Beispiel: Entfernen von Karten, Flapping von Verbindungen, Flapping von Routen und Broadcast-Stürme. Stellen Sie sicher, dass die richtigen SNMP-Traps basierend auf den im Netzwerk genutzten Funktionen erstellt werden.
8. Die Testergebnisse und die Messwerte der Geräte sollten während der Tests reproduzierbar sein.

Testname	**Hot Standby Router Protocol (HSRP)-Failover**
Testkonfigurationsanforderungen	Wenden Sie die Last auf die primäre Gateway-Schnittstelle an. Der Datenverkehr sollte aus Sicht der Benutzerkonsole zu etwa 20 % zum Gateway und aus Sicht der Benutzerkonsole zu etwa 60 % zum Gateway hin reichen. Erhöhen Sie außerdem den Datenverkehr auf eine höhere Auslastung.
Testschritte	Überwachen von STP und HSRP über **show**-Befehle Fail the primary gateway interface connection and then restore the connection after the

	information is collection
Erwartete Messwerte	CPU während Failover Anzeigen der Schnittstelle vor, während und nach dem primären und sekundären Gateway. HSRP vor, während und nach dem Angriff anzeigen
Erwartete Ergebnisse	Das primäre Gateway wird innerhalb von zwei Sekunden auf das andere Router-Gateway umgeleitet. Befehle **anzeigen**, die die Änderung korrekt wiedergeben. Ein Failover auf das primäre Gateway erfolgt, wenn die Verbindung wiederhergestellt wird.
Tatsächliche Ergebnisse	
Erfolgreich oder fehlerhaft	
Zum Erzielen des Erfolgs erforderliche Änderungen	

Gerätemessungen

Führen Sie während der Testphase die folgenden Messungen durch, und dokumentieren Sie sie, um sicherzustellen, dass das Gerät ordnungsgemäß funktioniert:

- Arbeitsspeichernutzung
- CPU-Last
- Puffernutzung
- Schnittstellenstatistiken
- Routentabellen
- Spezifisches Debuggen

Die Informationen für Messungen variieren je nach implementiertem Test. Je nach den zu lösenden spezifischen Fragen können zusätzliche Messdaten bereitgestellt werden.

Messen Sie für jede getestete Anwendung die Parameter, um sicherzustellen, dass sich die Leistung der jeweiligen Anwendung nicht negativ auswirkt. Hierzu wird eine Leistungsbasis verwendet, die zum Vergleich der Leistung vor und nach der Bereitstellung verwendet werden kann. Beispiele für Anwendungsmesstests:

- Die durchschnittliche Zeit, die für die Anmeldung bei einem Netzwerk erforderlich ist.
- Die durchschnittliche Zeit, die zum Kopieren einer Gruppe von Dateien im Network File System (NFS) benötigt wird.
- Die durchschnittliche Zeit, die erforderlich ist, um eine Anwendung zu starten und zum ersten Bildschirm aufgefordert zu werden.
- Andere anwendungsspezifische Parameter.

Implementierung - Schnelle und erfolgreiche Cisco IOS-

Bereitstellung

Ein klar definierter Implementierungsprozess ermöglicht die effiziente Bereitstellung neuer Cisco IOS-Versionen.

Die Implementierungsphase umfasst den Pilotprozess und den Implementierungsprozess. Durch den Pilotprozess wird sichergestellt, dass die Cisco IOS-Version in der Umgebung erfolgreich ist und der Implementierungsprozess schnelle und erfolgreiche groß angelegte Cisco IOS-Bereitstellungen ermöglicht.

Strategie und Tools für Cisco IOS-Bereitstellungen

Die Strategie für Cisco IOS-Bereitstellungen besteht darin, mithilfe von Upgrade-Tools und einem klar definierten Implementierungsprozess eine abschließende Zertifizierung im Rahmen eines Pilotprozesses und eine schnelle Bereitstellung durchzuführen.

Bevor ein Pilotprozess für das Netzwerk gestartet wird, entwickeln viele Organisationen allgemeine Richtlinien für Pilotprojekte. Die Pilotleitfäden sollten Erwartungen an alle Piloten umfassen, z. B. Erfolgskriterien, zulässige Pilotenstandorte, Pilotendokumentation, Erwartungen der Piloten, Anforderungen an die Benutzerbenachrichtigung und erwartete Dauer der Pilotphase. Ein funktionsübergreifendes Team aus Technik, Implementierung und Betrieb ist in der Regel an der Erstellung von allgemeinen Richtlinien für Pilotprojekte und einem Pilotprozess beteiligt. Nach der Erstellung des Pilotprozesses können einzelne Implementierungsgruppen in der Regel erfolgreiche Pilotprojekte mithilfe der festgelegten Best Practice-Methoden durchführen.

Sobald eine neue Softwareversion für die Bereitstellung und die endgültige Zertifizierung genehmigt wurde, muss das Unternehmen mit der Planung des Cisco IOS-Upgrades beginnen. Die Planung beginnt mit der Identifizierung neuer Image-Anforderungen, einschließlich Plattform, Speicher, Flash und Konfiguration. Die Architektur- und Technikergruppen definieren in der Regel neue Anforderungen an Software-Images in der Phase, in der sich die Verwaltung des Cisco IOS-Management-Lebenszyklus anbahnt. Nachdem die Anforderungen identifiziert wurden, muss jedes Gerät von der Implementierungsgruppe validiert und ggf. aktualisiert werden. Das CiscoWorks2000 Software Image Manager (SWIM)-Modul kann die Cisco IOS-Anforderungen auch anhand des Gerätebestands validieren. Wenn alle Geräte validiert oder auf die richtigen neuen Image-Standards aktualisiert wurden, kann die Implementierungsgruppe mit der Implementierung des CiscoWorks2000 SWIM-Moduls als Tool für die Softwarebereitstellung beginnen.

Sobald das neue Image mehrfach erfolgreich implementiert wurde, kann mithilfe von CiscoWorks SWIM eine schnelle Bereitstellung eingeleitet werden.

Cisco IOS-Bestandsverwaltung

Der CiscoWorks200 Resource Manager Essentials (RME) Inventory Manager vereinfacht die Versionsverwaltung von Cisco Routern und Switches mithilfe webbasierter Reporting-Tools, die Cisco IOS-Geräte anhand von Softwareversion, Geräteplattform und Gerätenamen melden und sortieren.

Cisco IOS SWIM

CiscoWorks2000 SWIM kann dabei helfen, die fehleranfällige Komplexität des Upgrade-Prozesses zu reduzieren. Integrierte Links zu CCO korrelieren die Online-Informationen von Cisco

über Software-Patches mit der im Netzwerk bereitgestellten Cisco IOS- und Catalyst-Software, wobei die entsprechenden technischen Hinweise hervorgehoben werden. Neue Planungstools finden Systemanforderungen und senden Benachrichtigungen, wenn Hardware-Upgrades (Boot ROM, Flash RAM) erforderlich sind, um die vorgeschlagenen Software-Image-Updates zu unterstützen.

Bevor eine Aktualisierung initiiert wird, werden die Voraussetzungen für ein neues Image anhand der Bestandsdaten des Zielswitches oder Routers validiert, um ein erfolgreiches Upgrade sicherzustellen. Wenn mehrere Geräte aktualisiert werden, synchronisiert SWIM die Download-Aufgaben und ermöglicht dem Benutzer, den Fortschritt des Auftrags zu überwachen. Geplante Aufträge werden über einen Snoff-Prozess gesteuert, der es Managern ermöglicht, die Aktivitäten eines Technikers zu autorisieren, bevor sie die einzelnen Upgrade-Aufgaben starten. RME 3.3 bietet die Möglichkeit, Software-Upgrades für Cisco IGX-, BPX- und MGX-Plattformen zu analysieren, wodurch die Ermittlung der Auswirkungen eines Software-Upgrades erheblich vereinfacht und beschleunigt wird.

Pilotprozess

Um die potenzielle Exposition zu minimieren und die verbleibenden Produktionsprobleme besser zu erfassen, wird ein Software-Pilotprogramm empfohlen. Pilotprojekte sind in der Regel wichtiger für neue Technologiebereitstellungen, aber viele neue Softwarebereitstellungen werden mit neuen Services, Funktionen oder Hardware verknüpft, wo ein Pilotprojekt wichtiger ist. Im Rahmen des einzelnen Pilotplans sollten die Auswahl des Pilotprojekts, die Dauer des Pilotprojekts und die Messung berücksichtigt werden. Bei der Auswahl des Pilotprojekts wird ermittelt, wann und wo ein Pilotprojekt durchgeführt werden sollte. Pilotemessung ist der Prozess der Erfassung der erforderlichen Daten, um Erfolg und Fehler oder potenzielle Probleme zu identifizieren.

Bei der Auswahl des Pilotprogramms wird angegeben, wo und wie ein Pilotprojekt durchgeführt wird. Ein Pilot kann mit einem Gerät in einem Bereich mit geringen Auswirkungen beginnen und sich auf mehrere Geräte in einem Bereich mit höherer Wirkung erstrecken. Bei der Pilotauswahl, bei der die Auswirkungen verringert werden können, sind folgende Überlegungen zu berücksichtigen:

- In einem Netzwerkbereich installiert, der aufgrund der Redundanz für die Auswirkungen eines einzelnen Geräts ausfallsicher ist.
- In einem Netzwerkbereich mit einer minimalen Anzahl von Benutzern hinter dem ausgewählten Gerät, die mögliche Auswirkungen auf die Produktion bewältigen können.
- Erwägen Sie, das Pilotprojekt entlang von Architekturlinien zu trennen. So können Sie beispielsweise ein Pilotprojekt im Access-, Distribution- und/oder Core-Layer des Netzwerks durchführen.

Die Dauer dieses Pilotprojekts sollte auf der Zeit basieren, die erforderlich ist, um alle Gerätefunktionen ausreichend zu testen und zu bewerten. Dies sollte sowohl Einbrennen als auch Netzwerk bei normalen Datenverkehrslasten umfassen. Die Dauer hängt auch vom Schritt eines Code-Upgrades und dem Netzwerkbereich ab, in dem das Cisco IOS ausgeführt wird. Wenn es sich bei dem Cisco IOS um eine neue Hauptversion handelt, wird eine längere Pilotphase empfohlen. Wenn es sich bei der Aktualisierung um eine Maintenance-Version mit minimalen neuen Funktionen handelt, reicht eine kürzere Pilotphase aus.

Während der Pilotphase ist es wichtig, die Ergebnisse auf ähnliche Weise zu überwachen und zu dokumentieren wie bei den ersten Tests. Dazu gehören Benutzerumfragen, Erfassung von Pilotendaten, Problemerfassung und Kriterien für Erfolg/Misserfolg. Einzelpersonen sollten direkt

für die Nachverfolgung und Überwachung der Fortschritte bei Pilotprojekten verantwortlich sein, um sicherzustellen, dass alle Probleme identifiziert werden und die am Pilotprojekt beteiligten Nutzer und Dienste mit den Ergebnissen des Pilotprojekts zufrieden sind. Die meisten Organisationen werden eine Version zertifizieren, wenn sie in einer Pilot- oder Produktionsumgebung erfolgreich ist. Dieser Schritt ist in einigen Umgebungen ein kritischer Fehler, da er als erfolgreich wahrgenommen wird, wenn keine Mess- oder Erfolgskriterien identifiziert oder dokumentiert werden.

Implementierung

Nach Abschluss der Pilotphase im Produktionsnetzwerk beginnt die Cisco IOS-Implementierungsphase. Die Implementierungsphase umfasst mehrere Schritte, um den Erfolg von Software-Upgrades und die Effizienz der Implementierung sicherzustellen. Dazu gehören der langsame Start der Implementierung, die abschließende Zertifizierung, die Vorbereitung von Upgrades, die Automatisierung von Upgrades und die abschließende Validierung.

Der langsame Start der Implementierung ist der Prozess der langsamen Implementierung einer neu getesteten Version, um sicherzustellen, dass das Bild vollständig der Produktionsumgebung ausgesetzt ist, bevor die endgültige Zertifizierung und vollständige Konvertierung erfolgen. Einige Unternehmen beginnen möglicherweise mit einem Gerät und einem Tag der Gefährdung, bevor sie am folgenden Tag auf zwei Geräte-Upgrades umsteigen, und am nächsten Tag vielleicht noch ein paar mehr. Wenn etwa zehn Geräte in Betrieb genommen wurden, kann die Organisation bis zu ein bis zwei Wochen vor der endgültigen Zertifizierung der jeweiligen Cisco IOS-Version warten. Nach der endgültigen Zertifizierung kann die Organisation die identifizierte Version schneller und mit deutlich höherem Vertrauensniveau bereitstellen.

Nach dem langsamen Start-Prozess sollten alle Geräte, die für ein Upgrade identifiziert wurden, mithilfe des Gerätebestands und einer Matrix der Cisco IOS-Mindeststandards für Bootstrap, DRAM und Flash überprüft und validiert werden, um sicherzustellen, dass die Anforderungen erfüllt werden. Die Daten können über interne Tools, SNMP-Tools von Drittanbietern oder mithilfe des CiscoWorks2000 RME erfasst werden. CiscoWorks2000 SWIM überprüft oder überprüft diese Variablen vor der Implementierung. Es ist jedoch immer gut zu wissen, was bei Implementierungsversuchen zu erwarten ist.

Wenn für Upgrades mehr als hundert ähnliche Geräte geplant sind, wird dringend empfohlen, eine automatisierte Methode einzusetzen. Die Automatisierung verbessert nachweislich die Effizienz von Upgrades und erhöht den Prozentsatz der erfolgreichen Geräteupgrades bei großen Bereitstellungen, die auf einem internen Upgrade von 1.000 Geräten mit und ohne SWIM basieren. Cisco empfiehlt die Verwendung von CiscoWorks 2000 SWIM für große Bereitstellungen, da während des Upgrades der Grad der Überprüfung ermittelt wurde. SWIM wird sogar dann wieder aus einer Cisco IOS-Version entfernt, wenn ein Problem erkannt wird. SWIM-Funktionen durch Erstellen und Planen von Upgrade-Jobs, bei denen ein Job mit den Geräten konfiguriert wird, gewünschte Upgrade-Images und Laufzeit des Jobs. Jeder Job sollte zwölf oder weniger Geräte-Upgrades enthalten, und bis zu zwölf Jobs können gleichzeitig ausgeführt werden. SWIM überprüft außerdem, ob die geplante Cisco IOS-Upgrade-Version nach dem Upgrade erfolgreich ausgeführt wird. Es wird empfohlen, ca. 20 Minuten pro Geräte-Upgrade (einschließlich Verifizierung) einzuplanen. Mit dieser Formel kann ein Unternehmen 36 Geräte pro Stunde aufrüsten. Cisco empfiehlt außerdem ein Upgrade von bis zu 100 Geräten pro Abend, um potenzielle Probleme zu vermeiden.

Nach einem automatisierten Upgrade sollten einige Validierungen durchgeführt werden, um den Erfolg sicherzustellen. Das CiscoWorks2000 SWIM-Tool kann nach dem Upgrade

benutzerdefinierte Skripts ausführen, um eine weitere Erfolgsüberprüfung durchzuführen. Die Überprüfung umfasst die Überprüfung, ob der Router über die entsprechende Anzahl an Routen verfügt, die Sicherstellung, dass logische/physische Schnittstellen aktiv und aktiv sind, oder die Überprüfung, dass auf das Gerät zugegriffen werden kann. Die folgende Beispielkontrollliste kann den Erfolg einer Cisco IOS-Bereitstellung vollständig überprüfen:

- Wurde das Gerät ordnungsgemäß neu geladen?
- Ist das Gerät Pingable und über die Netzwerkmanagement-System-Plattformen (NMS) erreichbar?
- Sind die erwarteten Schnittstellen auf dem Gerät aktiv und aktiv?
- Verfügt das Gerät über die richtigen Adjacencies für das Routing-Protokoll?
- Wird die Routing-Tabelle ausgefüllt?
- Lässt das Gerät den Datenverkehr ordnungsgemäß weiterleiten?

Betrieb - Management der hochverfügbaren Cisco IOS-Implementierung

Best Practices für die hohe Verfügbarkeit der Cisco IOS-Umgebung tragen dazu bei, die Netzwerkkomplexität zu reduzieren, die Problembehebungszeit zu verkürzen und die Netzwerkverfügbarkeit zu verbessern. Der Betriebsbereich des Cisco IOS-Managements umfasst Strategien, Tools und Best Practice-Methoden, die für die Verwaltung von Cisco IOS empfohlen werden.

Zu den Best Practices für Cisco IOS-Prozesse gehören die Softwareversionskontrolle, das Cisco IOS Syslog-Management, das Problem-Management, die Standardisierung der Konfiguration und das Verfügbarkeitsmanagement. Die Softwareversionskontrolle umfasst die Verfolgung, Validierung und Verbesserung der Softwarekonsistenz innerhalb der identifizierten Software-Programmzweige. Die Cisco IOS Syslog-Verwaltung ist der Prozess der proaktiven Überwachung und Reaktion auf Syslog-Meldungen höherer Priorität, die von Cisco IOS generiert werden. Problemmanagement ist die Praxis, kritische Probleminformationen schnell und effizient für softwarebezogene Probleme zu sammeln, um zukünftige Ereignisse zu verhindern. Die Standardisierung von Konfigurationen ist der Prozess der Standardisierung von Konfigurationen, um das Potenzial für ungetesteten Code in der Produktion zu verringern und das Verhalten von Netzwerkprotokollen und -funktionen zu standardisieren. Das Verfügbarkeitsmanagement ist der Prozess zur Verbesserung der Verfügbarkeit anhand von Kennzahlen, Verbesserungszielen und Verbesserungsprojekten.

Strategien und Tools für Cisco IOS Operations

Zur Verwaltung von Cisco IOS-Umgebungen stehen zahlreiche Qualitätsstrategien und -tools zur Verfügung. Die erste wichtige Strategie für den Cisco IOS-Betrieb besteht darin, die Umgebung so einfach wie möglich zu gestalten und so weit wie möglich Abweichungen bei der Konfiguration und den Cisco IOS-Versionen zu vermeiden. Die Cisco IOS-Zertifizierung wurde bereits diskutiert, aber die Konsistenz der Konfiguration ist ein weiterer wichtiger Bereich. Die Architektur-/Engineering-Gruppe sollte für die Erstellung von Konfigurationsstandards zuständig sein. Die Implementierungs- und Betriebsgruppe ist dann für die Konfiguration und Wartung der Standards über die Cisco IOS-Versionskontrolle und -Konfigurationsstandards/-kontrolle verantwortlich.

Die zweite Strategie für den Cisco IOS-Betrieb ist die Fähigkeit, Netzwerkfehler zu erkennen und schnell zu beheben. Netzwerkprobleme sollten in der Regel von der Betriebsgruppe identifiziert

werden, bevor Benutzer sie anrufen. Auch Probleme sollten so schnell wie möglich ohne weitere Auswirkungen oder Veränderungen auf die Umwelt gelöst werden. Einige der wichtigsten Best Practices in diesem Bereich sind das Problem-Management und das Cisco IOS Syslog-Management. Cisco Output Interpreter ist ein Tool zur schnellen Diagnose von Abstürzen der Cisco IOS-Software.

Die dritte Strategie ist eine konsequente Verbesserung. Der primäre Prozess ist die Verbesserung eines qualitätsbasierten Programms zur Verbesserung der Verfügbarkeit. Durch die Durchführung von Ursachenanalysen für alle Probleme, einschließlich der Probleme im Zusammenhang mit Cisco IOS, kann ein Unternehmen die Testabdeckung verbessern, die Problembehebungszeiten verkürzen und Prozesse optimieren, die die Auswirkungen von Ausfällen beseitigen oder reduzieren. Darüber hinaus können allgemeine Probleme analysiert und Prozesse entwickelt werden, um diese Probleme schneller zu beheben.

Zu den Tools für den Cisco IOS-Betrieb gehören die Bestandsverwaltung für die Softwareversionskontrolle (CiscoWorks2000 RME), die Syslog-Verwaltung zur Verwaltung von Syslog-Meldungen sowie Geräte-Konfigurationsmanager zur Verwaltung der Konsistenz der Gerätekonfiguration.

Syslog-Verwaltung

Syslog-Meldungen sind Meldungen, die vom Gerät an einen Sammlungsserver gesendet werden. Diese Meldungen können Fehler sein (z. B. ein ausgefallener Link), oder sie können informativ sein, z. B. wenn jemand gerade ein Terminal auf einem Gerät konfiguriert hat.

Syslog-Verwaltungstools protokollieren und verfolgen Syslog-Meldungen, die von Routern und Switches empfangen wurden. Einige Tools verfügen über Filter, mit denen unerwünschte Nachrichten entfernt werden können, die wichtige Nachrichten beeinträchtigen können. Syslog-Tools sollten auch das Erstellen von Berichten basierend auf den erhaltenen Nachrichten ermöglichen. Die Berichte können nach Zeitraum, Gerät, Meldungstyp oder Meldungspriorität angezeigt werden.

Das beliebteste Syslog-Tool für die Cisco IOS-Verwaltung ist der CiscoWorks2000 RME Syslog Manager. Weitere Tools sind verfügbar, darunter SL4NT, ein Shareware-Programm von Netal und Private I von OpenSystems.

CiscoWorks Device Configuration Manager

Der CiscoWorks200 Device Configuration Manager verwaltet ein aktives Archiv und bietet eine einfache Möglichkeit, Konfigurationsänderungen für mehrere Cisco Router und Switches zu aktualisieren. Der Konfigurationsmanager überwacht das Netzwerk auf Konfigurationsänderungen, aktualisiert das Archiv, wenn eine Änderung erkannt wird, und protokolliert die Änderungsinformationen an den Änderungsüberwachungsdienst. Über eine webbasierte Benutzeroberfläche können Sie das Archiv nach bestimmten Konfigurationsattributen durchsuchen und den Inhalt zweier Konfigurationsdateien vergleichen, um Unterschiede zu erkennen.

Cisco Output Interpreter

Der Cisco Output Interpreter ist ein Tool zur Diagnose von Software-erzwungenen Abstürzen. Das Tool kann dabei helfen, Softwarefehler zu identifizieren, ohne das Cisco Technical Assistance Center (TAC) anzurufen, oder es kann nach einem Software-erzwungenen Absturz als primäre Information an das TAC verwendet werden. Diese Informationen helfen im Allgemeinen, eine

Lösung für das Problem zu beschleunigen, zumindest hinsichtlich der erforderlichen Informationserfassung.

Software-Versionskontrolle

Die Softwareversionskontrolle umfasst die Implementierung nur standardisierter Softwareversionen und die Überwachung des Netzwerks, um Software aufgrund der Nichtversionskonformität zu validieren oder möglicherweise zu ändern. Im Allgemeinen erfolgt die Softwareversionskontrolle mithilfe eines Zertifizierungsprozesses und der Standardkontrolle. Viele Unternehmen veröffentlichen Versionsstandards auf einem zentralen Webserver. Darüber hinaus ist das Implementierungspersonal darauf geschult, die aktuelle Version zu überprüfen und die Version zu aktualisieren, wenn sie nicht den Standards entspricht. Einige Unternehmen verfügen über einen Prozess, bei dem eine sekundäre Validierung durch Audits durchgeführt wird, um sicherzustellen, dass der Standard bei der Implementierung eingehalten wird.

Im laufenden Betrieb sind nicht standardmäßige Netzwerkversionen zu beobachten, insbesondere wenn Netzwerk- und Betriebspersonal groß sind. Dies kann auf ungeschulte, neuere Mitarbeiter, falsch konfigurierte Boot-Befehle oder nicht geprüfte Implementierungen zurückzuführen sein. Es empfiehlt sich, in regelmäßigen Abständen Softwareversionsstandards mithilfe von Tools wie CiscoWorks 2000 RME zu validieren, mit denen alle Geräte nach der Cisco IOS-Version sortiert werden können. Wenn nicht standardmäßige Bedingungen identifiziert werden, sollten diese sofort markiert und ein Trouble Ticket oder ein Change Ticket initiiert werden, um die Version auf den festgelegten Standard zu bringen.

Proaktive Syslog-Verwaltung

Die Syslog-Erfassung, -Überwachung und -Analyse sind Fehlermanagementprozesse, die zur Behebung von mehr Cisco IOS-spezifischen Netzwerkproblemen empfohlen werden, die auf andere Weise schwer oder nicht zu identifizieren sind. Die Syslog-Erfassung, -Überwachung und -Analyse tragen dazu bei, die Problembehebungszeit zu verkürzen, indem viele Fehler proaktiv identifiziert und behoben werden, bevor schwerwiegendere Netzwerkprobleme auftreten oder von Benutzern gemeldet werden. Syslog bietet im Vergleich zum konsistenten SNMP Polling für eine große Anzahl von MIB-Variablen auch eine effizientere Methode zum Erfassen einer Vielzahl von Problemen. Die Syslog-Erfassung, -Überwachung und -Analyse wird mithilfe der richtigen Cisco IOS-Konfiguration, der Syslog-Korrelationstools wie CiscoWorks2000 RME und/oder der Syslog-Ereignisverwaltung durchgeführt. Die Syslog-Ereignisverwaltung erfolgt durch Analyse der gesammelten Syslog-Daten für identifizierte kritische Meldungen und anschließende Weiterleitung einer Warnmeldung oder eines Traps an einen Ereignismanager zur Benachrichtigung und Behebung in Echtzeit.

Die Syslog-Überwachung erfordert Unterstützung für das NMS-Tool oder Skripts, die bei der Analyse und Meldung von Syslog-Daten helfen. Dazu gehört die Möglichkeit, Syslog-Meldungen nach Datum oder Uhrzeit, Gerät, Syslog-Meldungstyp oder Häufigkeit der Meldungen zu sortieren. In größeren Netzwerken können Tools oder Skripts implementiert werden, um Syslog-Daten zu analysieren und Alarme oder Benachrichtigungen an Ereignismanagementsysteme oder Betriebspersonal zu senden. Wenn Warnungen für eine Vielzahl von Syslog-Daten nicht verwendet werden, sollte die Organisation Syslog-Daten mit höherer Priorität mindestens täglich überprüfen und Support-Tickets für potenzielle Probleme erstellen. Zur proaktiven Erkennung von Netzwerkproblemen, die bei der normalen Überwachung möglicherweise nicht sichtbar sind, sollten regelmäßige Überprüfungen und Analysen der historischen Syslog-Daten durchgeführt werden, um Situationen zu erkennen, die möglicherweise kein unmittelbares Problem darstellen, aber ein Anzeichen für ein Problem darstellen, bevor sich daraus Servicebeeinträchtigungen

ergeben.

Problemmanagement

Viele Kunden verzeichnen zusätzliche Ausfallzeiten aufgrund fehlender Prozesse im Problem Management. Weitere Ausfallzeiten können auftreten, wenn Netzwerkadministratoren versuchen, das Problem schnell mithilfe einer Kombination aus servicerelevanten Befehlen oder Konfigurationsänderungen zu beheben, anstatt Zeit für die Problemerkennung, die Erfassung von Informationen und einen gut analysierten Lösungspfad zu verbringen. Das beobachtete Verhalten in diesem Bereich umfasst das Neuladen von Geräten oder das Löschen von IP-Routing-Tabellen, bevor ein Problem und dessen Ursache untersucht werden. In einigen Fällen liegt dies an der Problemlösung auf erster Support-Ebene. Das Ziel bei allen softwarebezogenen Problemen sollte es sein, schnell die erforderlichen Informationen für die Ursachenanalyse zu sammeln, bevor die Verbindung oder der Service wiederhergestellt wird.

In größeren Umgebungen wird ein Problem Management Prozess empfohlen. Dieser Prozess sollte ein gewisses Maß an Standard-Problembeschreibungen und angemessene **show-**Befehlsauflistungen enthalten, bevor die Eskalation auf eine zweite Ebene erfolgt. Der First-Tier-Support darf niemals das Löschen von Routen oder Neuladen von Geräten sein. Optimal: Die erste Ebene sollte schnell Informationen sammeln und auf eine zweite Ebene eskalieren. Wenn man zunächst nur wenige Minuten für die Problemermittlung oder die Problembeschreibung aufwendet, ist eine Ursachenerkennung viel wahrscheinlicher, was eine Problemumgehung, die Laborerkennung und die Berichterstellung ermöglicht. Der Support auf zweiter Ebene sollte gut mit den Informationen vertraut sein, die Cisco benötigt, um ein Problem zu diagnostizieren oder einen Fehlerbericht zu erstellen. Dazu gehören Speicherabbilder, die Ausgabe von Routing-Informationen und die Ausgabe von **Geräteanzeigebefehlen**.

Standardisierung der Konfiguration

Globale Gerätekonfigurationsstandards gewährleisten die Beibehaltung globaler Standardkonfigurationsparameter für Geräte und Services, was zu einer globalen Konsistenz der Konfiguration im gesamten Unternehmen führt. Globale Konfigurationsbefehle sind Befehle, die auf das gesamte Gerät und nicht auf einzelne Ports, Protokolle oder Schnittstellen angewendet werden. Globale Konfigurationsbefehle wirken sich im Allgemeinen auf den Gerätezugriff, das allgemeine Geräteverhalten und die Gerätesicherheit aus. In Cisco IOS umfasst dies Dienstbefehle, IP-Befehle, VTY-Befehle, Konsolenport-Befehle, Protokollierungsbefehle, AAA/TACACS+-Befehle, SNMP-Befehle und Banner-Befehle. Wichtig bei globalen Gerätekonfigurationsstandards ist auch eine geeignete Namenskonvention für Geräte, die es Administratoren ermöglicht, das Gerät, den Gerätetyp und den Gerätestandort anhand des DNS-Namens (Domain Name System) des Geräts zu identifizieren. Die globale Konsistenz der Konfiguration ist für die allgemeine Unterstützung und Zuverlässigkeit einer Netzwerkumgebung wichtig, da sie dazu beiträgt, die Netzwerkkomplexität zu reduzieren und die Netzwerkunterstützung zu verbessern. Probleme bei der Unterstützung treten häufig ohne Standardisierung der Konfiguration auf, da das Geräteverhalten inkorrekt oder inkonsistent ist, der SNMP-Zugriff nicht funktioniert und die allgemeine Gerätesicherheit nicht gewährleistet ist.

Die Einhaltung globaler Gerätekonfigurationsstandards wird in der Regel von einer internen Engineering- oder Betriebsgruppe durchgeführt, die globale Konfigurationsparameter für ähnliche Netzwerkgeräte erstellt und verwaltet. Es empfiehlt sich auch, eine Kopie der globalen Konfigurationsdatei in TFTP-Verzeichnissen bereitzustellen, damit diese zunächst auf alle neu bereitgestellten Geräte heruntergeladen werden können. Außerdem ist eine für das Internet zugängliche Datei hilfreich, die die Standardkonfigurationsdatei mit einer Erläuterung der

einzelnen Konfigurationsparameter bereitstellt. Einige Unternehmen konfigurieren sogar regelmäßig weltweit ähnliche Geräte, um eine globale Konsistenz der Konfiguration zu gewährleisten, oder überprüfen Geräte regelmäßig auf die korrekten globalen Konfigurationsstandards. Protokoll- und Schnittstellenkonfigurationsstandards stellen die Aufrechterhaltung von Standards für die Schnittstellen- und Protokollkonfiguration dar.

Die Konsistenz der Protokoll- und Schnittstellenkonfiguration verbessert die Netzwerkverfügbarkeit, indem sie die Netzwerkkomplexität verringert, das erwartete Geräte- und Protokollverhalten sicherstellt und die Netzwerkunterstützung verbessert. Inkonsistente Protokoll- oder Schnittstellenkonfigurationen können zu unerwartetem Geräteverhalten, Problemen bei der Datenverkehrsweiterleitung, erhöhten Konnektivitätsproblemen und einer erhöhten Reaktionszeit des Supports führen. Schnittstellenkonfigurationsstandards sollten CDP-Schnittstellendeskriptoren, Caching-Konfiguration und andere protokollspezifische Standards umfassen. Protokollspezifische Konfigurationsstandards können Folgendes umfassen:

- IP-Routing-Konfiguration
- DLSW-Konfiguration
- Konfiguration der Zugriffslisten
- ATM-Konfiguration
- Konfiguration von Frame-Relay
- Spanning-Tree-Konfiguration
- VLAN-Zuweisung und -Konfiguration
- Virtual Trunking Protocol (VTP)
- HSRP

Hinweis: Je nach Konfiguration im Netzwerk können andere protokollspezifische Konfigurationsstandards verwendet werden.

Ein Beispiel für IP-Standards kann sein:

- Subnetzgröße
- Verwendeter IP-Adressraum
- Verwendetes Routing-Protokoll
- Konfiguration des Routing-Protokolls

Die Einhaltung von Protokoll- und Schnittstellenkonfigurationsstandards liegt normalerweise in der Verantwortung der Netzwerktechniker- und Implementierungsgruppen. Die Techniker müssen die Standards identifizieren, testen, validieren und dokumentieren. Die Implementierungsgruppe ist dann für die Bereitstellung neuer Dienste mithilfe der Engineering-Dokumente oder Konfigurationsvorlagen verantwortlich. Die Techniker sollten Dokumentation zu allen Aspekten der geforderten Standards erstellen, um die Konsistenz sicherzustellen. Außerdem sollten Konfigurationsvorlagen erstellt werden, um die Durchsetzung der Konfigurationsstandards zu erleichtern. Die Betriebsgruppen sollten auch für die Standards geschult werden und in der Lage sein, nicht standardmäßige Konfigurationsprobleme zu identifizieren. Die Konsistenz der Konfiguration ist in der Test-, Validierungs- und Zertifizierungsphase von großer Bedeutung. Tatsächlich ist es ohne standardisierte Konfigurationsvorlagen nahezu unmöglich, eine Clisco IOS-Version für ein mäßig großes Netzwerk angemessen zu testen, zu validieren oder zu zertifizieren.

Verfügbarkeitsmanagement

Das Verfügbarkeitsmanagement ist der Prozess der Qualitätsverbesserung, bei dem die Netzwerkverfügbarkeit als Metrik zur Qualitätsverbesserung eingesetzt wird. Viele Unternehmen

messen mittlerweile Verfügbarkeit und Ausfallart. Ausfallarten können Hardware, Software, Verbindung/Carrier, Stromversorgung/Umgebung, Design oder Benutzerfehler/Prozesse umfassen. Indem das Unternehmen Ausfälle identifiziert und unmittelbar nach der Wiederherstellung Ursachenanalysen durchführt, kann es Methoden zur Verbesserung der Verfügbarkeit identifizieren. Fast alle Netzwerke, die eine hohe Verfügbarkeit erreicht haben, weisen einen gewissen Qualitätsverbesserungsprozess auf.

Anhang A - Übersicht über Cisco IOS-Versionen

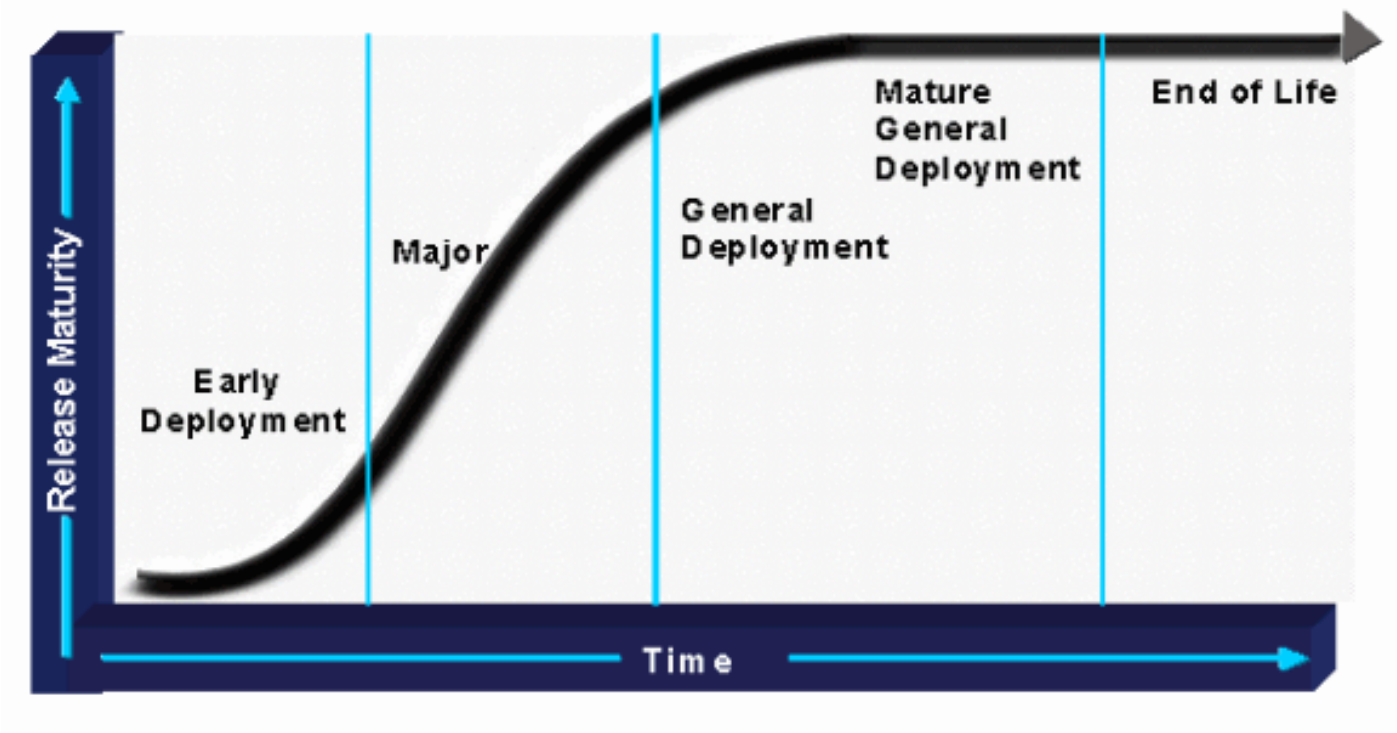
Die Cisco IOS Software-Release-Strategie basiert auf einer fundierten Softwareentwicklung, Qualitätssicherung und einer schnellen Markteinführung, die für den Erfolg der Netzwerke unserer Kunden von grundlegender Bedeutung sind.

Der Prozess ist in vier Kategorien von Releases definiert, die im Folgenden erläutert werden:

- Early Deployment Release (ED)
- Hauptversion
- Eingeschränkte Bereitstellung (LD)
- Allgemeine Bereitstellungsversion (GD)

Cisco erstellt und verwaltet eine IOS-Roadmap mit Informationen zu einzelnen Versionen, Zielmärkten, Migrationspfaden, neuen Funktionsbeschreibungen usw.

Die folgende Abbildung zeigt den Lebenszyklus der Cisco IOS-Softwareversion:



ED-Versionen

Cisco IOS ED-Versionen sind Fahrzeuge, die neue Entwicklungen auf den Markt bringen. Jede Wartungsrevision einer ED-Version beinhaltet nicht nur Fehlerbehebungen, sondern auch eine Reihe neuer Funktionen, neue Plattformunterstützung und allgemeine Verbesserungen der Protokolle und der Cisco IOS-Infrastruktur. Alle ein bis zwei Jahre werden die Funktionen und Plattformen der ED-Versionen auf die nächste Cisco IOS-Hauptversion portiert.

Es gibt vier Arten von ED-Veröffentlichungen, von denen jeder ein etwas anderes Release-Modell und Lifecycle-Meilensteine aufweist. Die ED-Releases können wie folgt klassifiziert werden:

- **Consolidated Technology Early Deployment (CTED) Releases** - Das neue Cisco IOS Release-Modell verwendet den konsolidierten ED Release Train, auch bekannt als "T" Train, um neue Funktionen, neue Hardwareplattformen und andere Verbesserungen für Cisco IOS einzuführen. Sie werden als konsolidierte Technologie bezeichnet, da sie über die Definition der internen Geschäftsbereiche (BU) und Geschäftsbereiche (LOB) hinausgehen. Beispiele für konsolidierte Technologieversionen sind Cisco IOS 11.3T, 12.0T und 12.1T.
- **Spezifische Technologie-Frühbereitstellung (STED)-Versionen** - STED-Versionen haben ähnliche Merkmale bei der Bereitstellung von Funktionen wie CTED-Versionen, mit der Ausnahme, dass sie auf eine bestimmte Technologie oder ein bestimmtes Marktsegment ausgerichtet sind. Sie werden immer auf bestimmten Plattformen veröffentlicht und unterliegen ausschließlich der Aufsicht einer Cisco BU. STED-Versionen werden mit zwei Buchstaben identifiziert, die an die Hauptversion angehängt sind. Beispiele für STED-Versionen sind Cisco IOS 11.3NA, 11.3MA, 11.3WA und 12.0DA.
- **SMED-Versionen (Specific Market Early Deployment**) - Die Cisco IOS SMEDs unterscheiden sich von STEDs dadurch, dass sie ein bestimmtes vertikales Marktsegment (ISPs, Unternehmen, Finanzinstitute, Telcom-Unternehmen usw.) ansprechen. SMEDs enthalten spezielle Anforderungen an technische Funktionen nur für bestimmte Plattformen, die für den beabsichtigten vertikalen Markt relevant sind. Sie können sich von CTEDs dadurch unterscheiden, dass sie nur für bestimmte Plattformen entwickelt werden, die für den vertikalen Markt relevant sind, während CTEDs für mehr Plattformen entwickelt werden, die auf einer breiteren Technologieanforderung basieren. Cisco IOS SMED-Versionen sind durch ein alphabetisches Zeichen gekennzeichnet, das an die Hauptversion angehängt wird (genau wie das CTED). Beispiele für SMEDs sind Cisco IOS 12.0S und 12.1E.
- **Kurzfristige Versionen für die frühzeitige Bereitstellung, auch als X Releases (XED)** bekannt - Cisco IOS XED-Versionen bringen neue Hardware und Technologien auf den Markt. Sie stellen weder Software-Wartungsversionen bereit noch stellen sie regelmäßige temporäre Software-Interimsrevisionen bereit. Wenn in der XED-Datei vor der Konvergenz mit dem CTED ein Fehler gefunden wird, wird eine Softwarewiederherstellung initiiert und dem Namen eine Nummer angefügt. Beispielsweise sind die Cisco IOS-Versionen 12.0(2)XB1 und 12.0(2)XB2 Beispiele für Neubauten von 12.0(2)XB.

Hauptversionen

Hauptversionen sind die primären Bereitstellungsmethoden für Cisco IOS-Softwareprodukte. Sie werden von der Cisco IOS Technology Division verwaltet und konsolidieren Funktionen, Plattformen, Funktionen, Technologien und die Verbreitung von Hosts aus früheren ED-Versionen. Cisco IOS-Hauptversionen streben nach höherer Stabilität und Qualität. Aus diesem Grund akzeptieren Hauptversionen nicht, dass Funktionen oder Plattformen hinzugefügt werden. Jede Wartungsversion enthält nur Fehlerbehebungen. Beispielsweise sind die Cisco IOS Software Releases 12.1 und 12.2 Hauptversionen.

Hauptversionen enthalten geplante Wartungsaktualisierungen, so genannte Wartungsversionen, die vollständig rezisionsgetestet sind, die aktuellsten Bugfixes enthalten und keine neuen Plattformen oder Funktionen unterstützen. Die Versionsnummer einer Hauptversion identifiziert die Hauptversion und deren Wartung. In der Cisco IOS Software-Version 12.0(7) ist 12.0 die Nummer der Hauptversion und 7 die zugehörige Wartungsstufe. Die vollständige Versionsnummer lautet 12.0(7). Ebenso ist 12.1 eine Hauptversion und 12.1(3) die dritte Wartungsversion der

Hauptversion der Cisco IOS Software, Version 12.1.

Begrenzte Bereitstellungsversionen

LD ist die Phase der Cisco IOS-Ausgereiftheit zwischen FCS und der allgemeinen Bereitstellung für die Hauptversionen. Die Cisco IOS ED-Versionen laufen nur in der eingeschränkten Bereitstellungsphase, da sie niemals eine GD-Zertifizierung erhalten.

Versionen für allgemeine Bereitstellung (GD)

Cisco erklärt zu einem bestimmten Zeitpunkt während des Lebenszyklus der Version, dass eine Hauptversion bereit für die GD-Zertifizierung ist. Nur eine größere Version kann den GD-Status erreichen. Sie erfüllt den GD-Zertifizierungsmeilenstein, wenn Cisco davon überzeugt ist, dass die Version

- Bewährt durch ein hohes Marktaufkommen in verschiedenen Netzwerken.
- Qualifiziert durch Kennzahlen, die auf Stabilitäts- und Bug-Trends analysiert werden.
- Qualifiziert durch Umfragen zur Kundenzufriedenheit.
- Eine Verringerung des normalisierten Trends bei Kunden fand Mängel in der Version gegenüber den vorherigen vier Wartungsversionen.

Ein funktionsübergreifendes Team für die GD-Zertifizierung, bestehend aus TAC-Technikern, Advanced Engineering Services (AES)-Technikern, System Test Engineering und Cisco IOS Engineering, wird gebildet, um jeden ausstehenden Fehler der Version zu bewerten. Dieses Team erteilt die endgültige Zulassung für die GD-Zertifizierung. Sobald eine Version den GD-Status erreicht hat, ist jede nachfolgende Version der Version auch GD. Folglich, sobald eine Freisetzung für GD erklärt wird; es tritt automatisch in die Phase der eingeschränkten Wartung ein. Während dieser Phase ist die technische Änderung des Codes, einschließlich Fehlerbehebungen bei der Überarbeitung des Hauptcodes, streng begrenzt und wird von einem Programm-Manager kontrolliert. Dadurch wird sichergestellt, dass keine unerwünschten Fehler an einer Version der Cisco IOS-Software mit GD-Zertifizierung auftreten. Die GD wird durch eine bestimmte Wartungsversion erreicht. Nachfolgende Wartungs-Updates für diese Version sind ebenfalls GD-Releases. Die Cisco IOS Software Version 12.0 erhielt beispielsweise die GD-Zertifizierung mit der Nummer 12.0(8). Die Cisco IOS Software Releases 12.0(9), 12.0(10) usw. sind GD-Releases.

Versuchs- oder Diagnosebilder

Experimentell- oder Diagnosebilder werden manchmal auch als technische Fachgebiete bezeichnet und nur dann erstellt, wenn kritische Softwareprobleme identifiziert wurden. Diese Images sind nicht Teil des normalen Veröffentlichungsprozesses. Bilder in dieser Kategorie sind kundenspezifische Builds, die dazu dienen, ein Problem zu diagnostizieren, eine Fehlerbehebung zu testen oder eine sofortige Lösung bereitzustellen. Eine sofortige Behebung ist möglich, wenn es nicht möglich ist, auf die nächste Zwischen- oder Wartungsversion zu warten. Test- oder Diagnosebilder können auf jeder unterstützten Software-Basis erstellt werden, einschließlich Wartungs- oder Zwischenversionen aller Releasetypen. Es gibt keine offiziellen Namenskonventionen, aber in vielen Fällen fügt der Entwickler dem Basisbildnamen Initialen, Exp (für experimentelle) oder zusätzliche Ziffern hinzu. Diese Images werden nur vorübergehend in Verbindung mit der Entwicklung von Cisco unterstützt, da das Cisco TAC und die Cisco IOS-Versionen keine unterstützende Dokumentation wie Symboltabellen oder den Verlauf der Basis-Images enthalten. Diese Images werden nicht von Cisco intern getestet.

Lebenszyklusende von Versionen - Meilensteine

Irgendwann werden GD-Versionen durch neuere Versionen mit den neuesten Netzwerktechnologien ersetzt. Aus diesem Grund wurde ein Prozess zur Einstellung der Freisetzung mit den folgenden drei wichtigen Meilensteinen eingerichtet:

- **End of Sales (EOS)** - Bei wichtigen Versionen ist das EOS-Datum drei Jahre nach dem Datum der ersten kommerziellen Lieferung (First Commercial Shipment, FCS). Damit wird ein Enddatum festgelegt, für das die Version für neue Systeme erworben werden kann. Die EOS-Version kann weiterhin von Cisco Connection Online (CCO) heruntergeladen werden, um Wartungsaktualisierungen durchzuführen.
- **End of Engineering (EOE)** - Die EOE-Version ist die letzte Maintenance-Version für die GD-Version und folgt in der Regel etwa drei Monate nach der EOS-Version. Kunden können weiterhin technischen Support vom Cisco TAC erhalten und die EOE-Version von CCO herunterladen. Das Produktbulletin mit den EOS- und EOE-Versionen und -Daten wird ein Jahr vor dem geplanten EOS-Datum veröffentlicht. Zu diesem Zeitpunkt sollten Kunden anfangen, ein Upgrade ihrer Cisco IOS-Software in Erwägung zu ziehen, um die neuesten Netzwerktechnologien nutzen zu können.
- **End of Life (EOL)** - Am Ende des Lebenszyklus der Produktversion wird der gesamte Support für die Cisco IOS-Softwareversion eingestellt und zum EOL-Datum nicht mehr zum Download verfügbar. Im Allgemeinen ist das EOL-Datum fünf Jahre nach dem EOE-Datum. Ein EOL-Produktbulletin wird etwa ein Jahr vor dem eigentlichen EOL-Datum veröffentlicht.

Namenskonvention für Cisco IOS-Versionen

Die Namenskonvention für Cisco IOS-Images stellt ein vollständiges Profil aller veröffentlichten Images bereit. Der Name enthält immer den Hauptversionsbezeichner und den Wartungsfreigabebezeichner. Der Name kann auch einen Zugbezeichner, einen Umbaubezeichner (für die Wartungsversion), spezielle Funktionsbezeichner für die Geschäftseinheit (BU) und BU-spezifische Kennzeichen für die Neuerstellung von Funktionen enthalten. Das Format kann wie folgt untergliedert werden:

Abschnitt "Namenskonvention"	Erläuterung
x,y	Eine Kombination aus zwei separaten (ein oder zwei) Ziffern, die durch ein " getrennt sind. die den Wert der Hauptversion angibt. Dieser Wert wird vom Cisco IOS-Marketing bestimmt. Beispiel: 12.1
z	Ein bis drei Ziffern, die die Wartungsversion von x.y kennzeichnen. Dies geschieht alle acht Wochen. Die Werte für die erste Wartungsversion sind 0 in der Beta-Version, 1 bei Erstauslieferung und 2. Beispiel: 12.1(2)
p	Ein alphanumerisches Zeichen, das eine Neuerstellung von x.y(z) identifiziert. Der Wert beginnt mit einem Kleinbuchstaben "a"

	für die erste Wiederherstellung, dann "b" usw. Beispiel: 12.1(2a)
A	Ein bis drei Buchstaben sind die Bezeichnung des Release Trains und sind für CTED-, STED- und X-Versionen obligatorisch. Es identifiziert auch eine Produktfamilie oder Plattform. Technology ED-Versionen verwenden zwei Buchstaben. Der erste Buchstabe stellt die Technologie dar, der zweite Buchstabe wird zur Differenzierung verwendet. Beispiele: A = Access Server/Dial technology (example:11.3AA) B = Broadband (example:12.2B) D = xDSL technology (example:12.2DA) E = Enterprise feature set (example:12.1E) H = SDH/SONET technology (example:11.3HA) N = Voice, Multimedia, Conference (example:11.3NA) M = Mobile (example:12.2MB) S = Service Provider (example:12.0S) T = Consolidated Technology (example:12.0T) W = ATM/LAN Switching/Layer 3 (example:12.0W5) Ein "X" in der ersten Position des Freigabenamens identifiziert eine einmalige Version basierend auf dem CTED-Zug "T". Zum Beispiel XA, XB, XC usw. Ein "X" oder "Y" in der zweiten Position des Releasenamens kennzeichnet eine kurzlebige ED-Version, die auf einer STED-Version basiert oder mit dieser verknüpft ist. Beispiel: 11.3NX (basierend auf 11.3NA), 11.3WX (basierend auf 11.3WA) usw.
o	Optionaler numerischer Bezeichner mit einer oder zwei Ziffern, der eine Neuerstellung eines bestimmten Freigabewerts identifiziert. Lassen Sie das Feld leer, wenn es keine Neuerstellung darstellt. Beginnt mit 1, dann 2 usw. Beispiel: 12.1(2)T1, 12.1(2)XE2
u	Ein oder zwei numerische Kennzeichnungen, die die Funktionalität der BU-spezifischen Version kennzeichnen. Der Wert wird vom BU-Marketingteam bestimmt. Beispiel: 11.3(6)WA4, 12.0(1)W5
V	Ein- bis zweistelliger numerischer Kennzeichner, der die Wartungsversion des BU-spezifischen Codes identifiziert. Die Werte sind 0 in der Beta-Version, 1 bei Erstauslieferung und 2 als erste Wartungsversion. Beispiel: 11.3(6)WA4(9), 12.0(1)W5(6)
p	Ein alphanumerischer Kennzeichner, der eine Neuerstellung einer bestimmten

	Technologieversion identifiziert. Der Wert beginnt mit einem Kleinbuchstaben "a" für die erste Wiederherstellung, dann "b" usw. Beispiel: 11.3(6)WA4(9a) wäre eine Wiederherstellung von 11.3(6)WA4(9).

Die folgende Grafik kennzeichnet die verschiedenen Abschnitte der Cisco IOS-Namenskonvention:

Anhang B: Zuverlässigkeit von Cisco IOS

Die Zuverlässigkeit von Cisco IOS ist ein Bereich, in dem Cisco kontinuierlich seine Anstrengungen zur Verbesserung der Infrastruktur unternimmt. Bevor kundenorientierte Best Practices besprochen werden, ist ein gewisses Verständnis der internen IOS-Qualität und -Zuverlässigkeit von Cisco erforderlich. Diese Abschnitte sollen in erster Linie einen Überblick über die jüngsten Bemühungen von Cisco im Bereich der Cisco IOS-Softwarequalität geben und die Annahmen des Kunden hinsichtlich der Softwarezuverlässigkeit enthalten.

Cisco IOS Quality-Programm

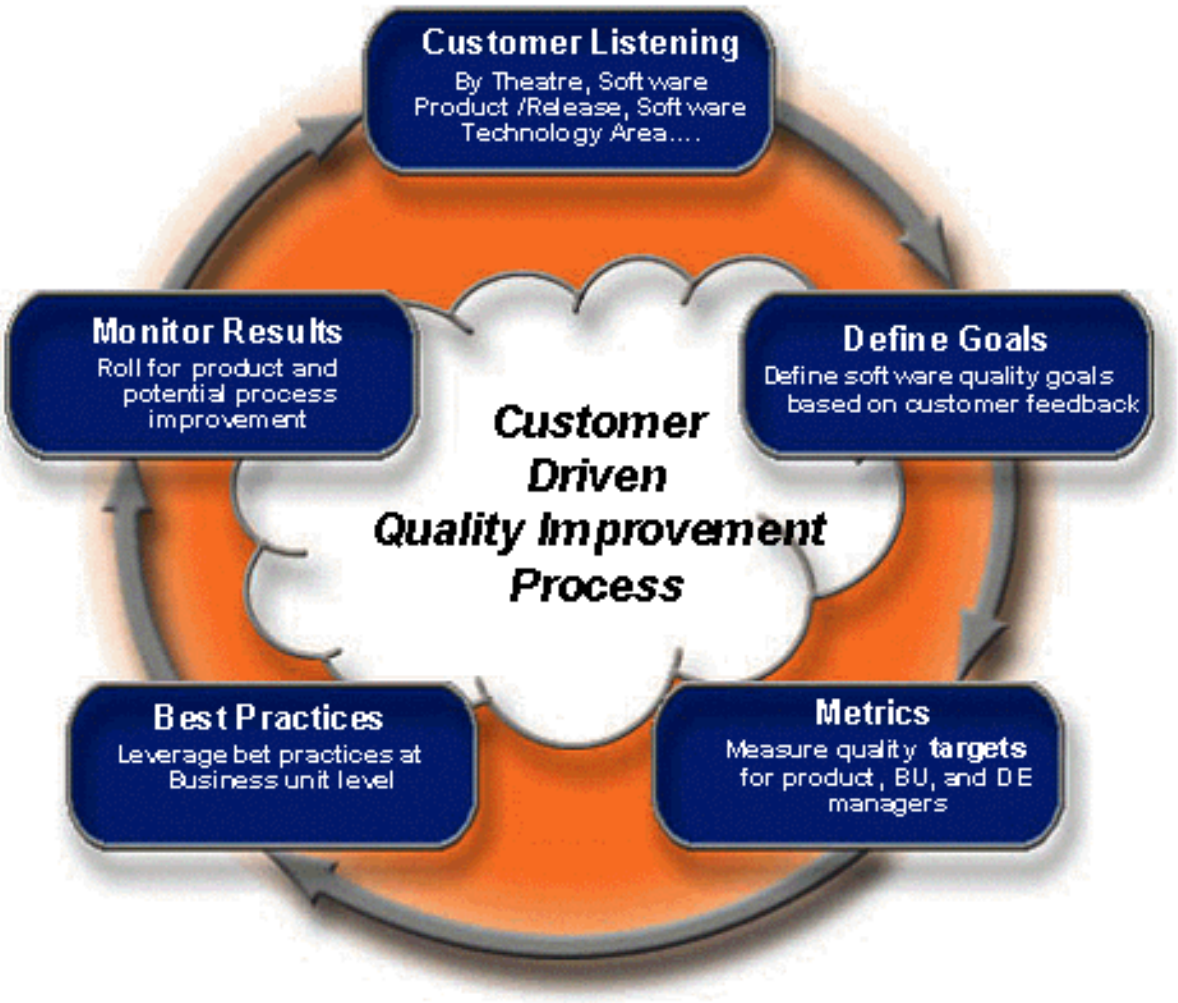
Cisco hat einen klar definierten IOS-Entwicklungsprozess namens GEM Great Engineering Methodology (GEM) entwickelt. Dieser Prozess hat einen dreiphasigen Lebenszyklus:

- Strategie und Planung
- Ausführung
- Bereitstellung

Zu den allgemeinen Bereichen innerhalb des Lebenszyklus gehören die Priorisierung der Einführung von Funktionen, die Entwicklung, der Testprozess, die Softwareeinführungsphase, die Lieferung an den ersten Kunden (FCS), GD und die Wartung von Engineering. Cisco befolgt außerdem eine Reihe von Best Practices für die Softwarequalität von Organisationen wie International Standards Organization (ISO), Telcordia (ehemals Bellcore), IEEE und dem Carnegie Mellon Software Engineering Institute. Diese Richtlinien sind in die GEM-Prozesse von Cisco integriert. Die Softwareentwicklungsprozesse von Cisco sind nach ISO 9001 (1994) zertifiziert.

Der primäre Prozess zur Qualitätsverbesserung von Cisco IOS-Software ist ein kundenorientierter Prozess, bei dem Cisco Kunden anhört, Ziele und Kennzahlen definiert, Best Practices implementiert und die Ergebnisse überwacht. Ein organisationsübergreifendes Team, das sich für

die Verbesserung der Softwarequalität einsetzt, unterstützt diesen Prozess. Nachfolgend ist ein Diagramm des Prozesses zur Verbesserung der Cisco IOS-Qualität dargestellt:



Der Qualitätsverbesserungsprozess hat für das Geschäftsjahr 2002 und darüber hinaus deutliche messbare Ziele. Das Hauptaugenmerk dieser Ziele liegt auf der Reduzierung von Fehlern, indem Softwareprobleme zu einem früheren Zeitpunkt des Testzyklus identifiziert, der Rückstand bei Fehlern reduziert, die Konsistenz der Funktionen und die Klarheit der Softwareversionen verbessert und konsistente, vorhersehbare Veröffentlichungspläne und Softwarequalität bereitgestellt werden. Zu den Initiativen in diesen Bereichen gehören neue Tools für die Testabdeckung (Identifizierung von Bereichen mit schwächerer Testabdeckung), Verbesserungen bei den Korrekturmaßnahmen im Testprozess und Verbesserungen bei den Regressionstests für das Cisco IOS-System. Zur Behebung dieser Probleme wurden zusätzliche Ressourcen bereitgestellt, und alle primären Cisco IOS-Softwareversionen unterliegen einem geschäftsführenden und funktionsübergreifenden Engagement.

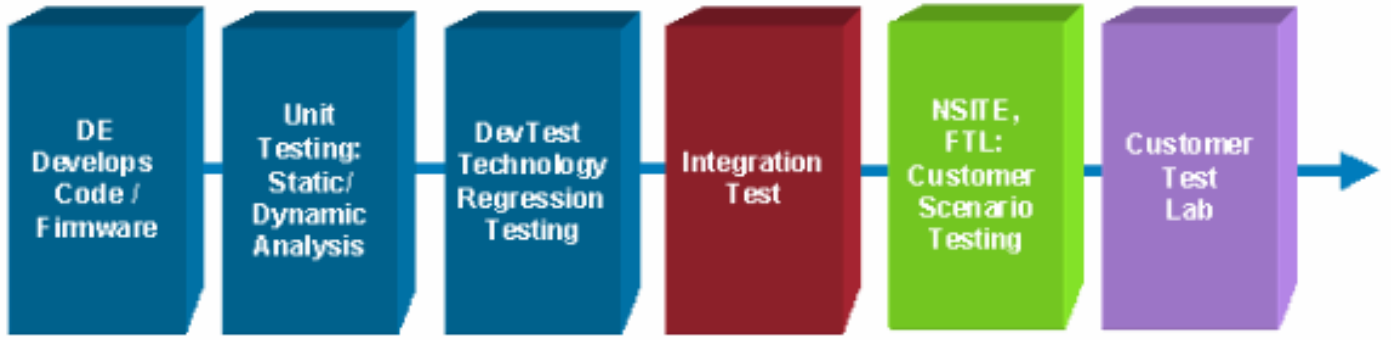
Cisco IOS-Versionstests

Ein integraler Bestandteil der Qualitätssicherung von Software ist die Qualität, der Umfang und die Abdeckung von Tests. Insgesamt verfolgt Cisco die folgenden IOS-Qualitätsziele:

- Reduzieren Sie gefundene interne Regressionsfehler von Cisco. Dies beinhaltet eine höhere Qualität bei der Entwicklung und die Identifizierung von mehr Problemen in der statischen/dynamischen Analyse.
- Weniger vom Kunden gefundene Fehler

- Reduzierung der ausstehenden Gesamtfehler
- Übersichtlichere Softwareversionen und konsistentere Funktionen
- Bereitstellung von Funktionen und Wartungsversionen mit Zeitplänen und hoher Qualität

Interne Tests von Cisco können als Prozess angesehen werden, bei dem in verschiedenen Testphasen verschiedene Fehler identifiziert werden. Das allgemeine Ziel ist es, die richtigen Arten von Fehlern im richtigen Labor zu finden. Dies ist aus mehreren Gründen wichtig. Die erste und wichtigste ist, dass in späteren Testphasen möglicherweise keine angemessene Testabdeckung vorhanden ist. Die Testkosten steigen zudem von einer Phase zur anderen erheblich, da sie in früheren Phasen automatisiert werden können und die Komplexität und das Fachwissen, die zu einem späteren Zeitpunkt erforderlich werden, zunehmen. Das folgende Diagramm zeigt das Testspektrum für Cisco IOS.



Die erste Stufe ist die Softwareentwicklung. Cisco bemüht sich in diesem Bereich um eine Verbesserung der anfänglichen Softwarequalität. Entwicklungsgruppen führen auch Codeüberprüfungen oder sogar mehrere Codeüberprüfungen durch, um sicherzustellen, dass andere Entwickler Softwareänderungen oder neuen Funktionscode genehmigen.

Der nächste Schritt ist der Komponententest. Bei Komponententests werden Tools verwendet, mit denen Softwareinteraktionen ohne die Verwendung eines Labors überprüft werden können. DevTest sind Labortests, die Funktionstests und Regressionstests umfassen. Mithilfe von Funktionstests wird die Funktionalität einer bestimmten Funktion überprüft. Dies umfasst die Konfiguration, die Dekonfiguration und das Testen aller Funktionsverbesserungen, die in der Funktionsspezifikation definiert sind. Regressionstests werden in einer automatisierten Testeinrichtung durchgeführt, um Funktionen und Verhalten laufend zu überprüfen. Der Schwerpunkt der Tests liegt in erster Linie auf Routing-, Switching- und Funktionsfunktionen in einer Reihe verschiedener Netzwerktopologien mit Pings und begrenzter Generierung von Datenverkehr. Regressionstests werden nur auf einer begrenzten Kombination von Funktionen, Plattformen, Softwareversionen und Topologien durchgeführt, da sehr viele mögliche Permutationen vorliegen. Heute werden jedoch über 4.000 Regressionstestskripte eingesetzt. Die Integrationstests wurden entwickelt, um die Labortests für ein umfassenderes Produkt- und Interoperabilitätspaket zu erweitern. Integrationstests erhöhen auch die Codeabdeckung von Tests, indem sie Tests erweitern, um Interoperabilitätstests, Stress- und Leistungstests, Systemtests und negative Tests (Testen unerwarteter Ereignisse) einzuschließen.

In der nächsten Laborphase werden End-to-End-Tests für gängige Kundenumgebungen durchgeführt. Diese werden im obigen Diagramm als Financial Test Lab (FTL) und NSITE, Customer Scenario Testing, angezeigt. FTL wurde entwickelt, um Testing für die geschäftskritische Finanzgemeinschaft bereitzustellen. NSITE ist eine Gruppe, die eingehendere Tests für verschiedene Cisco IOS-Technologien bereitstellt. Die NSITE- und FTL-Labs konzentrieren sich auf Bereiche wie Skalierbarkeits- und Leistungstests, Upgrades, Verfügbarkeit und Ausfallsicherheit, Interoperabilität und Betriebsfähigkeit. Die Benutzerfreundlichkeit konzentriert sich auf Massenbereitstellungsprobleme, Ereignismanagement/Korrelation und

Fehlerbehebung unter Last. In Cisco gibt es weitere Labs für verschiedene vertikale Märkte, um diese Bereiche zu testen.

Die letzte Übung, die im obigen Diagramm gezeigt wird, ist das Kundenlabor. Kundentests sind eine Erweiterung des Qualitätsaufwands und werden für Hochverfügbarkeitsumgebungen empfohlen, um sicherzustellen, dass die exakte Kombination aus Funktionen, Konfiguration, Plattformen, Modulen und Topologie vollständig getestet wurde. Die Testabdeckung sollte Netzwerkskalierbarkeit und -leistung in der identifizierten Topologie, spezifische Anwendungstests, negative Tests in der identifizierten Konfiguration, Interoperabilitätstests für Geräte von Drittanbietern und Einbrennungstests umfassen.

Software-MTBF

Eine der gängigsten Kennzahlen für die allgemeine Zuverlässigkeit ist die mittlere Betriebsdauer zwischen Ausfällen (MTBF). MTBF für die Softwarezuverlässigkeit ist nützlich, da die Analysefunktionen für die Hardwarezuverlässigkeit mithilfe von MTBF entwickelt wurden. Die Zuverlässigkeit der Hardware kann mithilfe einiger bestehender Standards genauer bestimmt werden. Cisco verwendet die Methode zur Teilezählung, die auf standardmäßigen MTBF-Daten von Telcordia Technologies basiert. Die MTBF-Software verfügt jedoch über keine entsprechenden Analysemethoden und muss für die MTBF-Analyse auf Feldmessungen basieren.

Cisco hat in den letzten drei Jahren Feldmessungen zur Sicherstellung der Softwarezuverlässigkeit für das interne IT-Netzwerk von Cisco durchgeführt. Diese Arbeit wird in Cisco dokumentiert. Die Arbeit basiert auf Software-erzwungenen Abstürzen für Cisco IOS-Geräte, die mithilfe von SNMP-Trap-Informationen zur Netzwerkverwaltung und Betriebszeiten gemessen werden können. Die Studie ermittelt die Softwarezuverlässigkeit mithilfe eines statistischen lokalen Verteilungsmodells für die identifizierten Softwareversionen. Die mittlere Reparaturzeit (MTTR) bei Softwareausfällen basiert auf den durchschnittlichen Neustart- und Wiederherstellungszeiten des Routers. In Unternehmensumgebungen wird eine Wiederherstellungszeit von sechs Minuten benötigt, bei größeren Internet Service Providern (ISPs) eine Wiederherstellungszeit von fünfzehn Minuten. Diese laufende Studie hat ergeben, dass die Software bei Veröffentlichung oder nach einigen Wartungsversionen im Allgemeinen die Verfügbarkeit von 99,999 % erreicht und im Laufe der Zeit sogar noch höher ist, da Software-erzwungene Abstürze als einzige Ausfallquelle ermittelt hat. Die Studie ermittelte potenzielle MTBF-Werte als Bereich zwischen 5.000 Stunden bei Software für die vorzeitige Bereitstellung und 50.000 Stunden bei Software für die allgemeine Bereitstellung.

Der häufigste Grund für diese Arbeit ist, dass Software-erzwungene Abstürze nicht alle Ausfallzeiten einschließen, die aufgrund von Problemen mit der Softwarezuverlässigkeit entstehen. Wenn diese Kennzahl bei der Qualitätsverbesserung verwendet wird, kann sie die Geschwindigkeit von Software-erzwungenen Abstürzen erhöhen, andere kritische Bereiche der Softwarezuverlässigkeit jedoch ignorieren. Dieser Kommentar bleibt weitgehend unbeantwortet, da es schwierig ist, die Zuverlässigkeit der Software mithilfe einer statistischen Methodik präzise vorherzusagen. Statistiker von Cisco zur Softwarequalität kamen zu dem Schluss, dass eine größere Stichprobe genauer Daten erforderlich ist, um Software-MTBF zuverlässig mit einer breiteren Palette von Ausfallarten vorhersagen zu können. Darüber hinaus wäre die theoretische statistische Analyse aufgrund von Variablen wie Netzwerkkomplexität, Erfahrung der Mitarbeiter bei der Behebung von softwarebezogenen Problemen, Netzwerkdesign, aktivierten Funktionen und Softwareverwaltungsprozessen schwierig.

Zurzeit wurde in der Branche keine Arbeit geleistet, um die Softwarezuverlässigkeit mit Feldmessungen genauer vorherzusagen, da es schwierig ist, diese Art sensibler Daten präzise zu

erfassen. Die meisten Kunden möchten aufgrund der proprietären Verfügbarkeitsdaten zudem nicht, dass Cisco Verfügbarkeitsinformationen direkt über ihr Netzwerk sammelt. Einige Unternehmen sammeln jedoch Daten zur Zuverlässigkeit von Software, und Cisco empfiehlt Unternehmen, Kennzahlen zur Verfügbarkeit aufgrund von Softwareausfällen zu erfassen und eine Ursachenanalyse für diese Ausfälle durchzuführen. Unternehmen mit höherer Softwarezuverlässigkeit haben diese proaktive Haltung genutzt, um die Zuverlässigkeit von Software durch eine Reihe von Methoden zu verbessern, die sie kontrollieren können.

Annahmen zur Softwarezuverlässigkeit

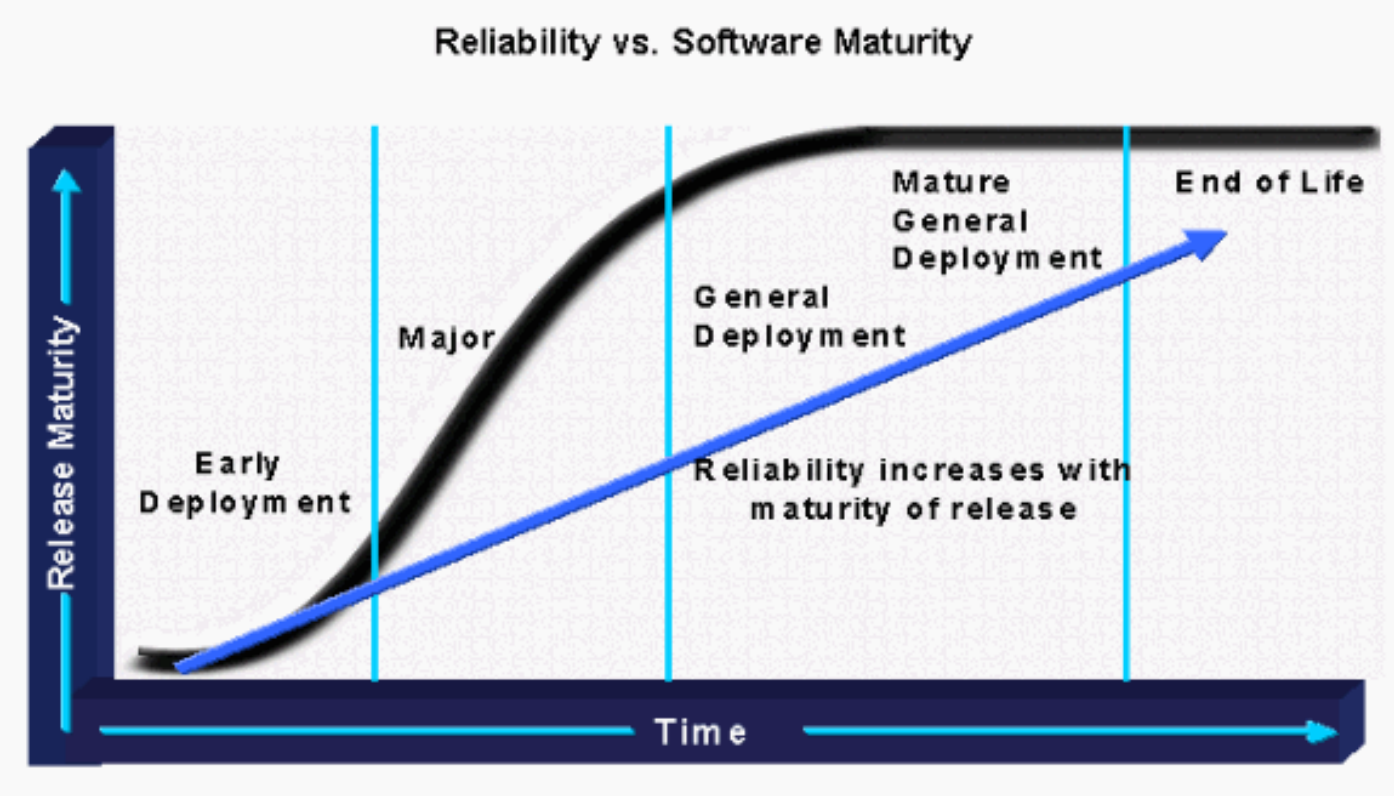
Als Ergebnis von Kundenfeedback, proaktiven Studien der Cisco IOS Technologies Group und Ursachenanalysen durch das Cisco Advanced Services Team wurden einige neuere Annahmen und Best Practices entwickelt, die zur Verbesserung der Zuverlässigkeit von Software beitragen. Diese Annahmen beziehen sich auf die Prüfungsaufgaben, die Ausgereiftheit oder das Alter der Software, die aktivierten Funktionen und die Anzahl der bereitgestellten Softwareversionen.

Testverantwortlichkeit

Die erste neue Annahme befasst sich mit der Testverantwortlichkeit. Cisco ist stets für das Testen/Validieren neuer Funktionen und Funktionen verantwortlich, um sicherzustellen, dass diese in neuen Produkten verwendet werden. Cisco ist auch für Regressionstests verantwortlich, um sicherzustellen, dass neue Softwareversionen abwärtskompatibel sind. Cisco kann jedoch nicht alle Funktionen, Topologien und Plattformen gegen alle potenziellen Probleme validieren, die eine Kundenumgebung mit sich bringen kann (Design-Eigenheiten, Load-Profile und Datenverkehrsprofile). Zu den Best Practices für Kunden im Bereich hohe Verfügbarkeit gehören Tests in einer reduzierten Labortopologie, die das Produktionsnetzwerk anhand von benutzerdefinierten Funktionen, Design, Services und Anwendungsdatenverkehr nachahmt.

Zuverlässigkeit im Vergleich zu ausgereiften Software-Lösungen

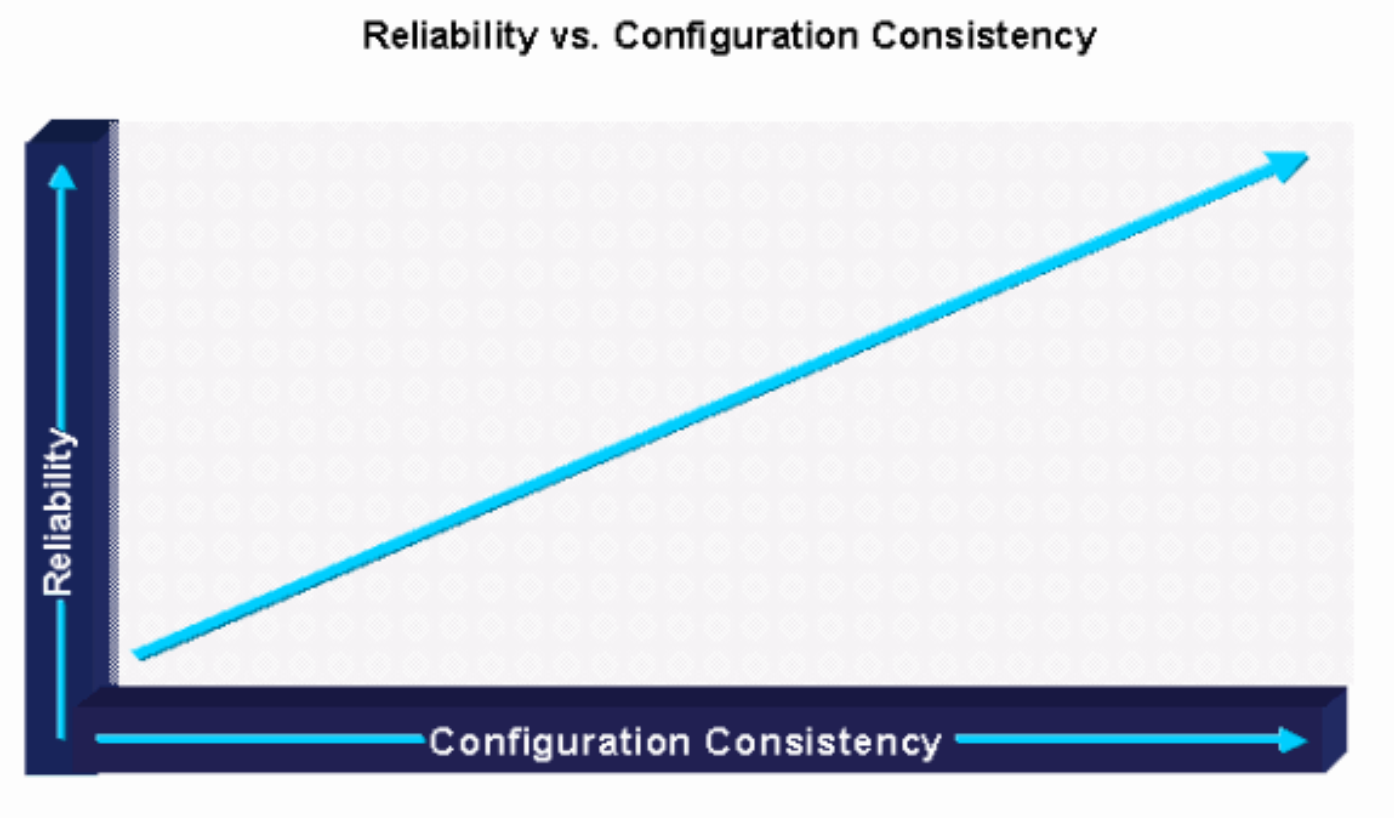
Die Zuverlässigkeit der Software ist in erster Linie ein Faktor für die Ausgereiftheit der Software. Die Software ist ausgereift, sobald sie verfügbar ist (Nutzung) und identifizierte Fehler behoben werden. Der Betrieb von Cisco hat eine Release-Architektur implementiert, um sicherzustellen, dass die Software ausgereift ist, ohne dass neue Funktionen hinzugefügt werden müssen. Kunden, die eine hohe Verfügbarkeit benötigen, benötigen ausgereiftere Software mit den Funktionen, die sie jetzt benötigen. Zwischen der Ausgereiftheit der Software, den Verfügbarkeitsanforderungen und den geschäftlichen Faktoren für neue Funktionen oder Funktionen besteht dann ein Kompromiss. Viele Unternehmen verfügen über Standards oder Richtlinien für eine akzeptable Ausgereiftheit. Einige akzeptieren nur die fünfte Zwischenfreigabe eines bestimmten Zuges. Für andere kann es die neunte oder GD Zertifizierung sein. Letztlich muss das Unternehmen sein akzeptables Risiko hinsichtlich der Softwarereife festlegen.



Zuverlässigkeit im Vergleich zur Anzahl der Funktionen und Standards

Die Zuverlässigkeit der Software ist auch ein Faktor dafür, wie viel Code in einer Produktionsumgebung getestet und ausgeführt wird. Je mehr Hardware-Plattformen und -Module zur Verfügung stehen, desto größer ist auch der auszuführende Code, was das Risiko von Softwarefehlern erhöht. Das Gleiche gilt für die Anzahl der konfigurierten Protokolle, die Vielzahl der Konfigurationen und sogar für die Vielzahl der implementierten Topologien oder Designs. Design-, Konfigurations-, Protokolle- und Hardwaremodulfaktoren können zu der ausgeübten Codemenge und dem erhöhten Risiko bzw. der erhöhten Exposition gegenüber Softwarefehlern beitragen.

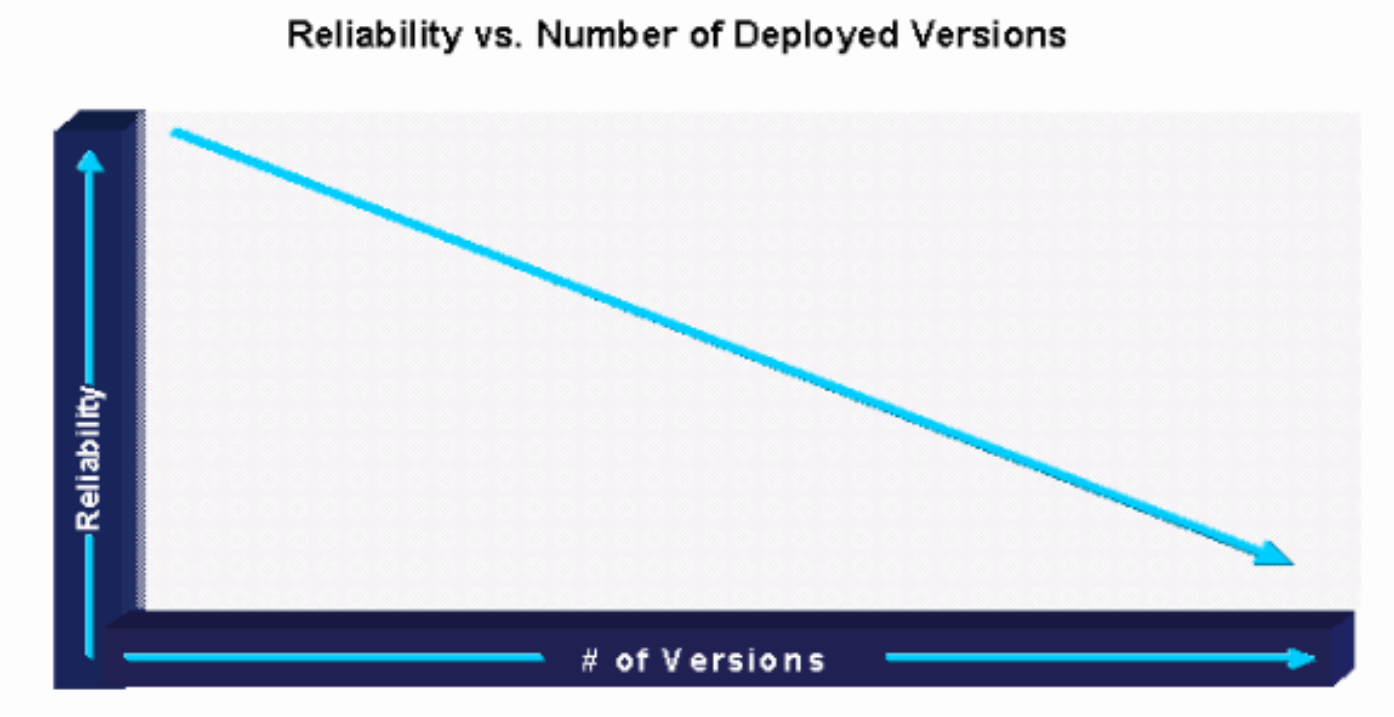
Softwareversionsvorgänge verfügen jetzt über spezielle Software, die den in einem bestimmten Bereich verfügbaren Code in der Regel beschränkt. Geschäftsbereiche haben empfohlene Designs und Konfigurationen, die bei Cisco gründlicher getestet wurden und häufiger von Kunden verwendet werden. Darüber hinaus haben Kunden damit begonnen, Best Practices für standardisierte modulare Topologien und Standardkonfigurationen zu implementieren, um die Anzahl der nicht getesteten Codezugriffe zu reduzieren und die Zuverlässigkeit der Software insgesamt zu verbessern. Einige Hochverfügbarkeitsnetzwerke verfügen über strenge Standard-Konfigurationsrichtlinien, modulare Topologiestandards und Softwareversionskontrolle, um das Risiko einer ungeprüften Codeexposition zu reduzieren.



Zuverlässigkeit im Vergleich zur Anzahl der bereitgestellten Versionen

Ein weiterer Faktor für die Softwarezuverlässigkeit ist die Interoperabilität zwischen Versionen und die schiere Codemenge, die mit mehreren Versionen ausgeführt wird. Mit zunehmender Anzahl an Softwareversionen steigt auch die Anzahl der durchgeführten Codeprozesse, wodurch das Risiko von Softwarefehlern erhöht wird. Das Risiko für die Zuverlässigkeit steigt aufgrund des zusätzlichen Codes, der mit mehreren Versionen ausgeführt wird, beinahe exponentiell an. Es wird inzwischen anerkannt, dass Unternehmen mindestens eine Handvoll Versionen im Netzwerk ausführen müssen, um bestimmte Funktionen und Plattformanforderungen zu erfüllen. Die Ausführung von mehr als 50 Versionen in einer größtenteils homogenen Netzwerkumgebung ist jedoch in der Regel ein Hinweis auf Softwareprobleme, da diese vielen Versionen nicht ordnungsgemäß analysiert oder validiert werden können.

Um die Zuverlässigkeit der Software zu verbessern, führt Cisco Development Regressionstests durch, um sicherzustellen, dass verschiedene Softwareversionen kompatibel sind. Darüber hinaus ist der Softwarecode modularer, und die Wahrscheinlichkeit, dass sich Core-Module im Laufe der Zeit zwischen den Versionen wesentlich ändern, ist geringer. Durch die Cisco Versionsprozesse wurde auch die Softwaremenge für Kunden geändert, da Versionen mit bekannten Defekten oder Interoperabilitätsproblemen schnell von den CCO entfernt werden, wenn Fehler gefunden werden.



Zugehörige Informationen

- Cisco Internetworking Operating Systems (IOS)
- Technischer Support und Dokumentation für Cisco Systeme