Gestión de Cisco IOS para redes de alta disponibilidad: Informe oficial de Mejores Prácticas

Contenido

Introducción

La implementación y el mantenimiento de software fiable de Cisco IOS® es una prioridad en el entorno de red empresarial crítico de hoy en día que requiere un enfoque renovado de Cisco y del cliente para lograr una disponibilidad ininterrumpida. Mientras que Cisco debe concentrarse en su compromiso por la calidad del software, los grupos de diseño y soporte de red también deben concentrarse en las mejores prácticas para la administración de software del IOS de Cisco. El objetivo es una mayor disponibilidad y eficacia en la gestión del software. Este método es una sociedad combinada para compartir, aprender e implementar las mejores prácticas de administración de software.

Este documento proporciona un marco operativo efectivo de las prácticas de administración de Cisco IOS para clientes de empresas y proveedores de servicios que ayudan a promover una mayor fiabilidad del software, una menor complejidad de la red y una mayor disponibilidad de la red. Este marco también ayuda a mejorar la eficacia de la administración de software al identificar áreas de responsabilidad y superposiciones en las pruebas de la administración del software y la validación entre las operaciones de lanzamiento de Cisco y la base de clientes de Cisco.

Resumen de las mejores prácticas IOS de Cisco

Las siguientes tablas proporcionan una descripción general de las mejores prácticas de Cisco IOS. Se pueden utilizar estas tablas como una descripción general de la administración de las mejores prácticas definidas como una lista de control del análisis de problemas para revisar las prácticas de administración actuales del IOS de Cisco, o como un marco para crear procesos alrededor de la administración del IOS de Cisco.

Las tablas definen los cuatro componentes del ciclo de vida de la administración de Cisco IOS. Cada tabla comienza con una estrategia y un resumen de herramientas para el área de ciclo de vida identificado. A continuación, se muestra el resumen de la estrategia y las herramientas, que se aplican únicamente al área de ciclo de vida definida.

Planificación - Creación del marco de administración de Cisco IOS: la planificación es la fase inicial de la administración de Cisco IOS necesaria para ayudar a una organización a determinar cuándo actualizar el software, dónde actualizar y qué proceso se utilizará para probar y validar las imágenes potenciales.

Práctica recomendada	Detalle
Estrategia y herramientas para la planificación del IOS de Cisco	Empezar con la planificación de la administración de Cisco IOS comienza con una evaluación honesta de las prácticas actuales, el desarrollo de objetivos alcanzables y la planificación de proyectos.
Definiciones de seguimiento de versiones	Identifica dónde se puede mantener la consistencia del software. Una opción de software se puede definir como un grupo de versiones de software único, diferenciado de otras áreas por una ubicación geográfica

de software	única, plataformas, módulos o requisitos de funciones.
Ciclo de actualización y definiciones	Las definiciones del ciclo de actualización pueden ser establecidas como pasos de calidad básicos en la administración de software y modificaciones, usados para determinar en qué momento debe iniciarse un ciclo de actualización del software.
Proceso de certificación	Los pasos del proceso de certificación deben incluir la identificación de la pista, las definiciones del ciclo de actualización, la gestión de candidatos, las pruebas/validación y, al menos, algún uso de producción piloto.

Diseño - Selección y validación de versiones de IOS: tener un proceso bien definido para seleccionar y validar versiones de Cisco IOS ayuda a una organización a reducir el tiempo de inactividad no planificado debido a intentos fallidos de actualización y defectos de software no planificados.

Práctica recomendada	Detalle
Estrategia y herramientas para la selección y validación de IOS de Cisco	Defina los procesos para seleccionar, probar y validar las nuevas versiones de Cisco IOS. Esto incluye un laboratorio de prueba de la red que emula la red de producción.
Gestión de candidatos	La gestión de candidatos es la identificación de los requisitos de versión de software y los riesgos potenciales para el hardware en particular y los conjuntos de funciones habilitados.
Prueba y validación	Prueba y validación son aspectos críticos para la administración de software y la red de gran disponibilidad. Las pruebas de laboratorio adecuadas pueden reducir significativamente el tiempo de inactividad de la producción, ayudar a formar al personal de soporte de red y ayudar a simplificar los procesos de implementación de la red.

Implementación - Implementación rápida y exitosa de Cisco IOS: los procesos de implementación bien definidos permiten a una organización implementar rápida y exitosamente nuevas versiones de Cisco IOS.

Práctica	Detalle

recomendada	
Estrategia y herramientas para la instalación del IOS de Cisco	La estrategia básica para las implementaciones del IOS de Cisco es realizar una certificación final vía un proceso piloto y una implementación rápida por medio de herramientas de actualización y un proceso de implementación bien definido.
Proceso piloto	Para minimizar la exposición potencial y capturar con mayor seguridad cualquier problema de producción restante, se recomienda un programa piloto. El plan piloto individual debería considerar la selección piloto, la duración piloto y la medición.
Instrumentación	Una vez finalizada la fase piloto, debe comenzar la fase de implementación de Cisco IOS. La fase de implementación puede incluir diversos pasos para asegurar el éxito de la actualización del software y la eficacia de la implementación, incluyendo inicio lento, certificación final, preparación de la actualización, automatización de la actualización y validación final.

Operaciones - Administración de la Implementación de Cisco IOS de Alta Disponibilidad: Entre las mejores prácticas para las operaciones de Cisco IOS se incluyen el control de versiones de software, la administración de Syslog de Cisco IOS, la administración de problemas, la estandarización de la configuración y la administración de disponibilidad.

Práctica recomendada	Detalle
Estrategias y herramientas para el funcionamiento del IOS de Cisco	La primera estrategia de las operaciones de Cisco IOS es mantener el entorno lo más sencillo posible, evitando la variación en la configuración y en las versiones de Cisco IOS. La segunda estrategia es la capacidad de identificar y resolver rápidamente los fallos de la red.
'Control de versión de software'	El control de versión de software es el proceso de implementación de sólo versiones de software estandarizadas y de supervisión de la red, con el fin de validar o, posiblemente, cambiar software debido a que la versión no es la adecuada.
Administración	La recolección, el monitoreo y el análisis de Syslog son los procesos de administración

proactiva de Syslog	de fallas recomendados para resolver más problemas de redes específicos de Cisco IOS que son difíciles o imposibles de identificar por otros medios.
Administración de problemas	Procesos de administración de problemas detallados que definen la identificación de problemas, la recopilación de información y una ruta de solución bien analizada. Estos datos pueden utilizarse para determinar la causa raíz.
Estandarización de la configuración	Los estándares de configuración representan la práctica de crear y mantener parámetros de configuración globales estándar en dispositivos y servicios similares, lo que se traduce en uniformidad de la configuración global en toda la empresa.
Gestión de disponibilidad	La gestión de la disponibilidad es el proceso de mejora de la calidad utilizando la disponibilidad de la red como métrica de mejora de la calidad.

Información general sobre el proceso de administración de la vida útil del software

La gestión del ciclo de vida del software Cisco IOS se define como el conjunto de procesos de planificación, diseño, implementación y funcionamiento recomendados para implementaciones de software fiables y redes de alta disponibilidad. Esto incluye procesos para seleccionar, validar o mantener las versiones del IOS de Cisco en la red.

El objetivo de la administración del ciclo de vida del software Cisco IOS es mejorar la disponibilidad de la red reduciendo la probabilidad de defectos de software identificados en la producción o fallas de cambio/actualización relacionadas con el software. Las mejoras prácticas que se definen en esta documentación han sido presentadas para reducir tales defectos y revertir las fallas en base a la experiencia en la práctica de muchos clientes de Cisco y del equipo de Servicios avanzados de Cisco. Es posible que la administración de la vida útil del software inicialmente aumente los gastos, sin embargo, pueden lograrse costos generales de propiedad debido a las interrupciones y los mecanismos de soporte y despliegue más racionalizados.

Programación – Elaboración del régimen de administración IOS de Cisco

La planificación es la fase inicial de la administración del IOS de Cisco que tiene por objeto ayudar a una organización a determinar cuándo actualizar el software, dónde actualizarlo y qué proceso se usará para probar y validar las posibles imágenes.

Entre las mejores prácticas se incluyen definiciones de seguimiento de versiones de software, ciclo de actualización y definiciones, y la creación de un proceso interno de certificación de software.

Estrategia y herramientas para la planificación del IOS de Cisco

Comience la planificación de la administración de Cisco IOS con una evaluación honesta de las prácticas actuales, el desarrollo de objetivos alcanzables y la planificación de proyectos. La evaluación propia debería hacerse mediante la comparación de las mejores prácticas que se describen en este documento y los procesos que se aplican en su empresa. Las preguntas básicas deben incluir lo siguiente:

- ¿Cuenta mi organización con un proceso de certificación de software que incluya pruebas/validación de software?
- ¿Cuenta mi organización con estándares de software de Cisco IOS con una cantidad limitada de versiones de Cisco IOS que se ejecutan en la red?
- ¿Tiene mi organización dificultades para determinar cuándo actualizar el software Cisco IOS?
- ¿Tiene mi organización dificultades para implementar el nuevo software Cisco IOS de forma eficiente y eficaz?
- ¿Tiene mi organización problemas de estabilidad de Cisco IOS después de la implementación que afectan seriamente al coste del tiempo de inactividad?

Después de la evaluación, su organización debe comenzar a definir objetivos para la administración del software Cisco IOS. Comience haciendo posible un grupo de funcionalidad recíproca de administradores o terminales desde los grupos de planificación de arquitectura, ingeniería, implementación y operaciones para ayudar a definir los objetivos del IOS de Cisco y los proyectos de mejoras de proceso. El propósito de las reuniones iniciales debería ser la determinación de los objetivos, los roles y las responsabilidades generales, la asignación de ítems de acción y la definición de la programación inicial del proyecto. Además, defina indicadores y factores de éxito fundamentales para determinar las ventajas de la gestión del software. Las métricas potenciales incluyen:

- disponibilidad (debido a problemas de software)
- costo de mejoras del software
- tiempo requerido para las actualizaciones
- número de versiones de software actuales en producción
- tasas de éxito/fallo de cambio de actualización de software

Además de la planificación general del marco de administración de Cisco IOS, algunas organizaciones también definen las reuniones de planificación de software en curso que se celebrarán mensualmente o trimestralmente. El objetivo de estas reuniones es revisar la implementación de software actual y comenzar a planificar cualquier nuevo requisito de software. La planificación puede incluir volver a analizar o modificar procesos de administración de software actuales, o sencillamente definir papeles y responsabilidades para las diferentes fases de la administración de software.

Las herramientas de la fase de planificación constan únicamente de herramientas de software para administración de inventario. El administrador de inventario de CiscoWorks 2000 Resource Manager Essentials (RME) es la herramienta principal utilizada en esta área. CiscoWorks2000 RME Inventory Manager simplifica en gran medida la administración de versiones de los routers y switches de Cisco a través de herramientas de informes basadas en la Web que informan y ordenan los dispositivos Cisco IOS en función de la versión de software, la plataforma de dispositivos, el tamaño de la memoria y el nombre del dispositivo.

Definiciones de seguimiento de versiones de software

La primera práctica recomendada de planificación de administración del software del IOS de Cisco identifica dónde se puede mantener la consistencia del software. Una opción de software se define como un grupo de versiones de software único, diferenciado de otras áreas por una ubicación geográfica, plataformas, módulos o requisitos de funciones únicos. Lo óptimo es que una red deba ejecutar una sola versión de software. Esto reduce considerablemente los costes relacionados con la gestión del software y proporciona un entorno coherente y fácil de gestionar. Sin embargo, la realidad es que la mayoría de las organizaciones deben ejecutar varias versiones en la red debido a problemas de funciones, plataformas, migración y disponibilidad dentro de áreas específicas. En muchos casos, la misma versión no funciona en plataformas heterogéneas. En otros casos, la organización no puede esperar a que una versión admita todos sus requisitos. El objetivo es identificar la menor cantidad de seguimientos de software para la red considerando los requisitos de prueba/validación, certificación y actualización. En muchos casos, es posible que la organización disponga de un número ligeramente mayor de opciones para reducir los costes generales de pruebas/validación, certificación y actualización.

El primer hecho diferenciador es el soporte de plataforma. En general, cada uno de los switches LAN, switches WAN, routers de núcleo y routers de borde tienen ramas de software individuales. Pueden necesitarse otros seguimientos de software para funciones o servicios específicos, como Data-Link Switching (DLSw), Calidad de Servicio (QoS) o IP Telephony, especialmente si este requisito puede localizarse dentro de la red.

Otro criterio es la fiabilidad. Muchas organizaciones intentan ejecutar el software más fiable hacia el núcleo de la red y el Data Center, al tiempo que ofrecen funciones avanzadas más recientes o soporte de hardware, hacia el perímetro. Por otra parte, las funciones de escalabilidad o ancho de banda suelen ser más necesarias en entornos de Data Center o de núcleo. SE pueden necesitar otras pistas para plataformas específicas, tales como sitios de distribución que tengan una plataforma de router WAN diferente. La siguiente tabla es un ejemplo de definición de seguimiento de software para una organización empresarial grande.

Seguimiento	Área	Plataformas de hardware	Funciones	Versión de Cisco IOS	Estado de la certificación
1	Switching de núcleo LAN	6500	QoS	12.1E(A8)	Prueba
2	switch de acceso LAN	2924XL 2948XL	Protocolo de detección de link unidireccional (UDLD), Protocolo de árbol transversal (STP).	12.0(5.2)XU	Certified 3/1/01
3	Acceso/distribución de LAN	5500 6509	Supervisor 3	5.4(4)	Certified 7/1/01

4	Módulo de switch de ruta de distribución (RSM)	RSM	Ruteo Abrir el trayecto más corto primero (OSPF)	12.0(11)	Certificado 3/4/02
5	distribución de cabecera WAN	7505 7507 7204 7206	Frame Relay OSPF	12.0(11)	Certificación 11/1/01
6	acceso WAN	2600	Frame Relay OSPF	12.1(8)	Certified 6/1/01
7	conectividad de IBM	3600	Terminal de control de enlace de datos síncrono (SDLC)	11.3(8)T1	Certificación 11/1/00

Las asignaciones de seguimiento también pueden modificarse con el transcurso del tiempo. En muchos casos, las funciones o el soporte de hardware se pueden integrar en versiones de software de línea principal, lo que permite que las distintas pistas puedan migrar finalmente juntas. Una vez establecidas las definiciones de rastreo, la organización puede usar otros procesos definidos para lograr la consistencia y validación de nuevas versiones. Las definiciones de seguimiento son también un esfuerzo en curso. Cada vez que se identifique un nuevo requisito de función, servicio, hardware o módulo, se debe considerar una nueva opción.

Las organizaciones que deseen iniciar un proceso de seguimiento deben comenzar con los requisitos de seguimiento recientemente definidos o, en algunos casos, con proyectos de estabilización para las redes existentes. Una organización también puede tener algunos elementos comunes identificables con las versiones de software existentes que pueden hacer posible la definición de la pista actual. En la mayoría de los casos, no se requiere una migración rápida a las versiones identificadas si el cliente dispone de suficiente estabilidad en la red. La arquitectura de red, o grupo de ingeniería, normalmente posee el proceso de definición de la pista. En algunos casos, una persona puede ser responsable de las definiciones de seguimiento. En otros casos, los directores de proyectos se encargan de desarrollar los requisitos de los programas informáticos y las nuevas definiciones de las pistas basadas en proyectos individuales. También es una buena idea revisar las definiciones de seguimiento trimestralmente para determinar si se necesitan nuevas pistas o si las antiguas requieren consolidación o actualización.

Las organizaciones que identifican y mantienen el seguimiento de software con control estricto de versión han demostrado tener el éxito más alto con un número decreciente de versiones de software en la red de producción. Esto generalmente se traduce en una mayor estabilidad del software y en la confiabilidad general de la red.

Ciclo de actualización y definiciones

Las definiciones del ciclo de actualización se definen como pasos de calidad básicos en la

administración del software y de las modificaciones, usados para determinar en qué momento debe iniciarse un ciclo de actualización del software. Las definiciones del ciclo de actualización permiten a una organización planificar correctamente un ciclo de actualización de software y asignar los recursos necesarios. Debido a los requisitos de la función en las versiones actuales estables, sin las definiciones de ciclos de actualización, una organización experimenta normalmente un aumento de problemas de confiabilidad del software. Otra exposición podría ser que la organización no tuviera la oportunidad de probar y validar correctamente una nueva versión antes de que se requiera el uso de producción.

Un aspecto importante de esta práctica es determinar cuándo y en qué medida deben iniciarse los procesos de planificación de software. Esto se debe al hecho de que una de las principales causas de problemas de software es activar una función, servicio o capacidad de hardware en producción sin la debida diligencia, o actualizar a una nueva versión de Cisco IOS sin consideraciones de administración de software. Otro problema no es la actualización. Al ignorar los ciclos y requisitos de software normales, muchos clientes se enfrentan a la difícil tarea de actualizar el software a través de varias versiones principales diferentes. La dificultad se debe al tamaño de las imágenes, cambios de comportamiento predeterminado, cambios en el Interpretador del nivel de comando (CLI) y cambios de protocolo.

Cisco recomienda que se inicie un ciclo de actualización bien definido, basado en las prácticas recomendadas tal y como se definen en este documento, siempre que se requiera una nueva función principal, servicio o soporte de hardware. El grado de certificación y comprobación/validación debe analizarse (en función del riesgo), para determinar los requisitos precisos de comprobación/validación. El análisis de riesgos pueden realizarse por la ubicación geográfica, la ubicación lógica (capas de acceso, núcleo y distribución) o la cantidad aproximada de gente/clientes afectados. Si la función principal o la capacidad de hardware están contenidas en la versión actual, también deberían iniciarse algunos procesos de ciclo de actualización simplificados. Si la función es relativamente menor, considere el riesgo y luego decida qué procesos deben iniciarse. Además, el software debe actualizarse en dos años o menos para garantizar que su organización se mantenga relativamente al día y que el proceso de actualización no sea demasiado complicado.

Los clientes también deben considerar el hecho de que no se corregirán los errores en los trenes de software que hayan superado el estado End Of Life (EOL). También deberían tenerse en cuenta los requisitos de la empresa, ya que muchos entornos pueden tolerar, o incluso aceptar, más adiciones de características con muy pocos procesos de prueba/validación, o sin necesidad de ellos, y un tiempo de inactividad reducido. Los clientes también deben tener en cuenta los datos más recientes recopilados en las operaciones de la versión de Cisco al considerar sus requisitos de prueba. Un análisis de los errores y las causas principales mostró que la gran mayoría de las causas de la raíz de los errores fueron el resultado de la codificación de los desarrolladores dentro del área de software afectada. Esto significa que si una organización agrega una función o módulo particular a su red en una versión existente, existe la probabilidad de que se produzca un error relacionado con esa función o módulo, pero una probabilidad mucho menor de que la nueva característica, hardware o módulo afecte a otras áreas. Estos datos deben permitir que las organizaciones reduzcan los requisitos de comprobación cuando se agregan características o módulos nuevos compatibles con las versiones existentes, al comprobar sólo el nuevo servicio o característica junto con los servicios habilitados. Los datos también se deben considerar al realizar la actualización del software basada en unos pocos errores críticos encontrados en la red.

La siguiente tabla muestra los requisitos de actualización recomendados para una organización empresarial de alta disponibilidad:

Desencadenador de administración de software	Requisitos de Ciclo vital del software
Nuevo servicio de red. Por ejemplo, una nueva estructura básica ATM o un nuevo servicio VPN.	Validación completa del ciclo de vida del software, incluidas las nuevas pruebas de funciones (junto con otros servicios habilitados), las pruebas de topología colapsadas, el análisis de rendimiento de hipótesis y las pruebas de perfiles de aplicaciones.
La nueva capacidad de red no se admite en la versión de software actual. Algunos ejemplos son QoS y switching de etiquetas multiprotocolo (MPLS).	Validación completa del ciclo de vida del software, incluidas nuevas pruebas de funciones, junto con otros servicios habilitados, pruebas de topología colapsadas, análisis de rendimiento de hipótesis y pruebas de perfiles de aplicaciones.
Nuevo módulo de hardware o función principal que existe en la versión actual. Por ejemplo, agregar un nuevo módulo GigE, soporte de multidifusión o DLSW.	Proceso de gestión de candidatos. Validación completa posible basada en los requisitos de la versión. Posibilidad de validación o prueba limitada si la administración de candidatos identifica a la versión actual como potencialmente aceptable.
Incorporación de funciones secundarias. Por ejemplo, un dispositivo TACACS para el control de acceso.	Considere la gestión de candidatos en función del riesgo de la función. Considere la posibilidad de probar o probar la nueva función en función del riesgo.
Software en producción durante dos años o una revisión trimestral del software.	Gestión de candidatos y decisiones empresariales con respecto a la gestión completa del ciclo de vida para identificar la versión soportable actual.

Actualizaciones de emergencia

En algunos casos, las organizaciones se enfrentan a la necesidad de actualizar el software debido a errores catastróficos. Esto puede provocar problemas si la organización no posee una metodología de actualización de emergencia. Los problemas con el software pueden variar desde actualizaciones de software no administradas, donde el software se actualiza sin administración de la vida útil del software, hasta situaciones donde los dispositivos de red fallan continuamente, pero la organización no se actualiza ya que no se ha completado la certificación/prueba sobre la

siguiente versión candidata. Cisco recomienda un proceso de actualización de emergencia para estas situaciones en las que se realizan pruebas y pruebas piloto limitadas en áreas menos críticas para el negocio de la red.

Si se producen errores catastróficos sin una solución alternativa aparente y el problema está relacionado con los defectos de software, Cisco recomienda que el soporte de Cisco se comprometa completamente a aislar el defecto y determinar si hay una solución disponible o cuándo. Cuando la solución se encuentra disponible, Cisco recomienda realizar un ciclo de actualización de emergencia para determinar rápidamente si el problema puede separarse con un tiempo de inactividad limitado. En la mayoría de los casos, una organización está ejecutando una versión compatible del código y la solución del problema está disponible en una versión provisional del software más reciente.

Las organizaciones también pueden prepararse para potenciales actualizaciones de emergencia. La preparación incluye la migración para soportar versiones de IOS de Cisco y la identificación/desarrollo de versiones de reemplazo de candidato dentro del mismo tren de IOS de Cisco como la versión certificada. El software compatible es importante, ya que significa que el desarrollo de Cisco está aún agregando arreglos de errores a la secuencia de software identificada. Al mantener el software compatible en la red, la organización reduce el tiempo de validación debido a la base de código más familiar y estable. Generalmente, un candidato para reemplazo es una nueva imagen de software interina/temporal dentro del mismo tren del IOS de Cisco sin agregados de soporte de funciones o hardware. Una estrategia de sustitución de candidatos es especialmente importante si la organización se encuentra en la fase inicial de adopción de un determinado programa informático.

Proceso de certificación

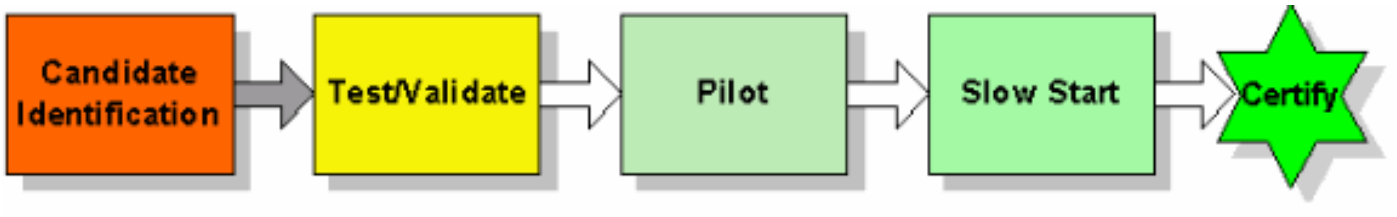
Un proceso de certificación ayuda a garantizar que el software validado se implemente de forma uniforme en el entorno de producción de la organización. Los pasos del proceso de certificación deben incluir la identificación de la pista, las definiciones del ciclo de actualización, la gestión de candidatos, las pruebas/validación y algunos usos de producción piloto. Sin embargo, un proceso de certificación simple sigue ayudando a garantizar que las versiones de software coherentes se implementen dentro de las opciones identificadas.

Inicie un proceso de certificación identificando a las personas de la arquitectura, ingeniería/implementación y operaciones que elaborarán y administrarán el proceso de certificación. En primer lugar, el grupo debería considerar los objetivos empresariales y las capacidades de recursos para garantizar que el proceso de certificación siga teniendo éxito. A continuación, asigne a las personas o los grupos la responsabilidad general de los pasos clave del proceso de certificación, incluida la gestión del seguimiento, las definiciones de actualización del ciclo de vida, las pruebas/validación y los programas piloto. Cada una de estas áreas debe ser definida, aprobada y comunicada formalmente dentro de la organización.

Incluya también directrices de calidad o aprobación en cada fase del proceso de certificación. Esto a veces se denomina proceso de puerta de acceso de calidad porque se deben cumplir ciertos criterios de calidad antes de que el proceso pueda pasar al siguiente paso. Esto ayuda a garantizar que el proceso de certificación sea eficaz y que merezca los recursos asignados. En general, cuando se detectan problemas de calidad en un área, el proceso retrocede un paso.

Es posible que los candidatos a software no cumplan los criterios de certificación definidos debido a la calidad del software o a un comportamiento inesperado. Cuando existen problemas que afectan el entorno, la empresa debe aplicar un proceso más efectivo a fin de certificar una

próxima versión provisoria. Esto ayuda a reducir los requisitos de recursos y, en general, es eficaz si la organización puede entender qué cambió y qué defectos se resolvieron. No es raro que una organización experimente un problema con un candidato inicial y certifique una versión provisional posterior de Cisco IOS. Las organizaciones también pueden realizar una certificación limitada o proporcionar advertencias si existen algunos problemas y pueden actualizar a una versión posterior totalmente certificada cuando se haya validado un nuevo interín. El siguiente organigrama a continuación es un proceso de certificación básica e incluye gates de calidad (una revisión siguiendo cada bloque):



Diseño - Selección y Validación de Versiones de Cisco IOS

Disponer de una metodología bien definida para seleccionar y validar las versiones de Cisco IOS ayuda a una organización a reducir el tiempo de inactividad no planificado debido a intentos de actualización fallidos y defectos de software no planificados.

La fase de diseño incluye la gestión de candidatos y las pruebas/validación. La gestión de candidatos es el proceso utilizado para identificar versiones específicas para las pistas de software definidas. La prueba/validación forma parte del proceso de certificación y garantiza que la versión de software identificada tenga éxito dentro de la opción requerida. La prueba/validación debe realizarse en un entorno de laboratorio con una topología colapsada y una configuración muy similar a la del entorno de producción.

Estrategia y herramientas para la selección y validación de IOS de Cisco

Cada organización debe tener un proceso para seleccionar y validar las versiones estándar de Cisco IOS para la red comenzando con un proceso para seleccionar la versión de Cisco IOS. Un equipo interfuncional de arquitectura, ingeniería y operaciones debe definir y documentar el proceso de gestión del candidato. Una vez aprobado, el proceso debe entregarse al grupo de entrega adecuado. También se recomienda crear una plantilla de gestión de candidatos estándar que se pueda actualizar con la información de los candidatos a medida que se identifique.

No todas las organizaciones tienen un entorno de laboratorio sofisticado que pueda imitar fácilmente el entorno de producción. Algunas organizaciones se saltan las pruebas de laboratorio debido a los gastos y a la capacidad de probar una nueva versión en la red sin que ello afecte a la empresa. Sin embargo, se recomienda a las organizaciones de alta disponibilidad que creen un laboratorio que imite la red de producción y que desarrollen un proceso de prueba/validación para garantizar una alta cobertura de prueba para las nuevas versiones de Cisco IOS. Una organización debe permitir unos seis meses para construir el laboratorio. Durante este tiempo, la organización debe trabajar para crear procesos y planes de prueba específicos para garantizar que el laboratorio se utilice en su totalidad. Para Cisco IOS, esto significa la creación de planes de prueba específicos de Cisco IOS para cada opción de software requerida. Estos procesos son fundamentales en organizaciones más grandes porque muchos laboratorios dejan de utilizarse para introducir nuevos productos y software.

Las siguientes secciones describen brevemente las herramientas de administración y

prueba/validación que se deben utilizar para la selección y validación de Cisco.

Herramientas de gestión de candidatos

Nota: Para utilizar la mayoría de las herramientas proporcionadas a continuación, debe ser un usuario registrado y debe haber iniciado sesión.

- Release Notes: proporciona información sobre el soporte de hardware, módulo y función de una versión. Las notas de la versión deben revisarse durante la administración de candidato para asegurarse de que haya toda la compatibilidad de software y hardware requerida en la versión potencial, y para comprender cualquier problema de migración incluyendo diferentes comportamientos predeterminados o requisitos de actualización.

Herramientas de prueba y validación

Las herramientas de prueba y validación se utilizan para probar y validar las soluciones de red, incluido el nuevo hardware, el nuevo software y las nuevas aplicaciones.

- **Generadores de tráfico**: genera flujos de tráfico multiprotocolo y tasas de paquetes sin procesar utilizados para modelar la velocidad a través de cualquier link en particular utilizando protocolos específicos. Los usuarios pueden identificar los números de zócalo, MAC de destino y origen. Estos valores pueden incrementarse en pasos específicos o pueden configurarse como estáticos/fijos o en incrementos aleatorios. Los generadores de tráfico pueden generan paquetes para los siguientes protocolos:IPIntercambio de paquetes entre redes (IPX)DECnetAppleSistemas de red Xerox (XNS)Internet Control Message Protocol (ICMP)Protocolo de administración de grupos de Internet (IGMP)Servicio de red sin conexión (CLNS)User Datagram Protocol (UDP)Servicio de red integrada virtual (VINES)Paquetes de link de datosLas herramientas están disponibles en Agilent and Spirent Communications .
- **Contador/Captura/Decodificador de Paquetes (Sniffer)**: permite al cliente capturar y descodificar selectivamente paquetes en todas las capas de paquetes y enlaces de datos. La herramienta tiene la capacidad de permitirle al usuario especificar los filtros, lo que permite capturar sólo datos de protocolo específicos. Los filtros permiten además al usuario especificar la captura de los paquetes que coinciden con una dirección IP, número de puerto o dirección MAC en particular. Las herramientas están disponibles en Sniffer Technologies.
- **Simulador/emulador de red**: permite al cliente llenar las tablas de ruteo de routers específicos, según los requisitos de la red de producción. Soporta la generación de routers de IP Routing Information Protocol (RIP), OSPF, Intermediate System-to-Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) y Border Gateway Protocol (BGP). Las herramientas están disponibles en PacketStorm Communications y Spirent Communications.
- **Emuladores de sesión**: generan flujos de tráfico de múltiples protocolos de ventanas deslizantes y son capaces de enviar flujos de tráfico multiprotocolo a través de la red de prueba hacia el dispositivo receptor. El dispositivo receptor devuelve los paquetes con la función de eco hacia la fuente. El dispositivo de origen comprueba el número de paquetes enviados y recibidos, los paquetes sin secuencia y los paquetes con error. La herramienta también otorga flexibilidad para definir los parámetros de ventana en el Protocolo de control de transmisión (TCP), imitando de este modo las sesiones de tráfico cliente/servidor en la red de laboratorio. Las herramientas están disponibles desde Empirix.
- **Emuladores de red a gran escala**: ayudan a probar la escalabilidad de entornos más grandes. Estas herramientas pueden crear e inyectar tráfico del tipo control en una topología de

laboratorio con facilidad, con el objetivo de reproducir con mayor detalle, un entorno de producción. Las capacidades incluyen inyectores de ruta, vecinos de protocolo y vecinos de protocolo de Capa 2. Las herramientas están disponibles en Agilent and Spirent Communications .

- **Simuladores de WAN**: ideales para probar el tráfico de aplicaciones empresariales en las que el ancho de banda y el retraso son potencialmente un problema. Estas herramientas permiten a las organizaciones probar localmente una aplicación con el retraso estimado y el ancho de banda para ver cómo funciona la aplicación en la WAN. A menudo se utilizan estas herramientas para el desarrollo de aplicaciones y para los tipos de pruebas para perfiles de aplicaciones dentro de las organizaciones empresariales. Adtech, una división de Spirent Communications y Shunra proporcionan herramientas de simulación WAN.

Gestión de candidatos

La gestión de candidatos es el proceso de identificar los requisitos de versión de software y los riesgos potenciales para el hardware en particular y los conjuntos de funciones habilitados. Se recomienda que una organización pase de cuatro a ocho horas investigando correctamente los requisitos de software, las notas de la versión, los defectos de software y los riesgos potenciales antes de probar una versión. A continuación se describe la base de la gestión de candidatos:

- Identifique candidatos de software a través de las herramientas de Cisco Connection Online (CCO).
- Madurez del software de análisis de riesgos, nueva función o soporte de código.
- Identifique y realice un seguimiento de los errores, problemas y requisitos de software conocidos durante todo el ciclo de vida.
- Identifique el comportamiento de configuración predeterminado de la imagen seleccionada.
- Mantener el respaldo y reenviar candidatos para los posibles cambios de candidatos.
- Limpieza de errores.
- Soporte de servicios avanzados de Cisco.

La identificación de candidatos a software se hizo más compleja con el creciente número de producciones y trenes de software de Cisco. CCO ahora cuenta con varias herramientas, entre las que se incluyen el planificador de actualizaciones de Cisco IOS, la herramienta de búsqueda de software, la matriz de compatibilidad de hardware de software y la herramienta de actualización de productos, que pueden ayudar a las organizaciones a identificar posibles candidatos a la versión. Estas herramientas se pueden encontrar en http://www.cisco.com/cisco/software/navigator.html.

A continuación, analice el riesgo del software candidato potencial. Este es el proceso de entender dónde reside actualmente el software en la curva de madurez y, a continuación, sopesar los requisitos para la implementación con el riesgo potencial del candidato a la versión. Por ejemplo, si una organización desea poner el software de implementación temprana (ED) en un entorno crítico de alta disponibilidad, se debe considerar el riesgo asociado y el requisito de recursos para una certificación exitosa. Una organización debe, como mínimo, añadir recursos de gestión de software para situaciones de mayor riesgo a fin de garantizar el éxito. Por otra parte, si se dispone de una versión de implementación general (GD) que satisfaga las necesidades de una organización, se necesitan menos recursos de gestión de software.

Cuando se identifican posibles entregas y riesgos, realice una limpieza de errores para determinar si existe algún error catastrófico ya identificado que potencialmente pudiera impedir la certificación. Los agentes Bug Watcher, Bug Navigator y Bug Watcher de Cisco pueden ayudar a

identificar posibles problemas y se deben utilizar durante todo el ciclo de vida del software para identificar posibles problemas de seguridad o defectos.

También se debe revisar un nuevo candidato de software para detectar posibles comportamientos de configuración predeterminados. Esto puede lograrse mediante una revisión de las notas de actualización de la nueva imagen de software y de las diferencias de configuración con la imagen potencial cargada en las plataformas designadas. La gestión de candidatos también puede incluir la identificación de versiones de respaldo o versiones de destino si la versión elegida no cumple los criterios de certificación en algún momento del proceso. Al observar los errores de funcionamiento relacionados con las funciones para una pista específica, una organización puede mantener a posibles candidatos para la certificación.

Los servicios avanzados de Cisco también son una excelente herramienta para la gestión de candidatos. Este grupo puede proporcionar una perspectiva más detallada del proceso de desarrollo y la colaboración entre un gran número de expertos del sector en muchos entornos de mercado vertical diferentes. Generalmente, los mejores eliminadores de errores o las capacidades de administración de candidatos están contemplados por el soporte de Cisco debido al nivel de experiencia y visibilidad en las versiones de software de producción ejecutadas en otras organizaciones.

Prueba y validación

Las pruebas y la validación son un aspecto fundamental de las mejores prácticas de gestión y de las redes de alta disponibilidad en general. Las pruebas en laboratorio correctas pueden reducir significativamente el tiempo de inactividad de la producción, ayudan a capacitar al personal del soporte técnico de redes y hacen que los procesos de instrumentación de red sean más eficientes. Sin embargo, para ser eficaz, la organización debe asignar los recursos necesarios para crear y mantener el entorno de laboratorio adecuado, aplicar los recursos necesarios a fin de realizar las pruebas correctas y utilizar una metodología de prueba recomendada que incluya la recopilación de mediciones. Sin ninguna de estas áreas, un proceso de prueba y validación puede no cumplir las expectativas de una organización.

La mayoría de las organizaciones empresariales no cuentan con el entorno de laboratorio de pruebas recomendado. Por esta razón, muchas organizaciones han implementado soluciones de forma incorrecta, han experimentado fallos en los cambios de red o han experimentado problemas de software que podrían haberse aislado en un entorno de laboratorio. En algunos entornos, esto es aceptable, ya que el coste del tiempo de inactividad no compensa el coste de un entorno de laboratorio sofisticado. Sin embargo, en muchas organizaciones no se puede tolerar el tiempo de inactividad. Se insta a estas organizaciones para que desarrollen los laboratorios recomendados, tipos y metodologías de pruebas para mejorar la calidad de la red de producción.

Laboratorio y entorno de prueba

El laboratorio debe ser una zona aislada con suficiente espacio para escritorios, bancos de trabajo, engranajes de prueba y gabinetes o bastidores de equipos. La mayoría de las grandes organizaciones necesitarán entre cuatro y diez racks de equipos para imitar el entorno de producción. Se recomienda algún tipo de seguridad física para ayudar a mantener un entorno de prueba mientras las pruebas se están realizando. Esto ayuda a evitar que se interrumpa una prueba de laboratorio debido a otras prioridades de laboratorio, como préstamos de hardware, formación o ensayos de implementación. También se recomienda la seguridad lógica para evitar que las rutas falsas entren en la red de producción o que el tráfico no deseado salga del

laboratorio. Esto se puede llevar a cabo con la ayuda de filtros de ruteo y listas de acceso ampliado en un router de gateway de laboratorio. La conectividad a la red de producción es útil para las descargas de software y el acceso a la red de laboratorio desde el entorno de producción.

La topología de laboratorio debe ser capaz de duplicar el entorno de producción para los planes de prueba específicos. Se recomienda reproducir las configuraciones de hardware, topología de red y funciones. Por supuesto, reproducir la topología real es casi imposible, pero lo que se puede hacer es reproducir la jerarquía de red y la interacción entre los dispositivos de producción. Esto es importante para la interacción del protocolo o de la función entre varios dispositivos. Algunas topologías de prueba serán diferentes según los requisitos de prueba del software. Las pruebas de Cisco IOS de extremo de la WAN, por ejemplo, no deben requerir dispositivos de tipo LAN ni pruebas y solo pueden requerir routers de extremo de la WAN y routers de distribución WAN. La clave es imitar la funcionalidad de software sin duplicar la producción. En algunos casos, las herramientas incluso se pueden utilizar para imitar el comportamiento a gran escala, como los conteos de vecinos de protocolo y las tablas de ruteo.

También se necesitan herramientas para ayudar con algunos tipos de pruebas mediante la mejora de la capacidad para duplicar el entorno de producción y para reunir datos de pruebas. Las herramientas que ayudan a la producción mímica incluyen colectores de tráfico, generadores de tráfico y dispositivos de simulación WAN. Smartbits es un buen ejemplo de un dispositivo que puede recolectar y repetir el tráfico de red o generar volúmenes de tráfico grandes. Una organización también puede beneficiarse de dispositivos que pueden ayudar a recopilar datos, como analizadores de protocolos.

El laboratorio también requiere cierta gestión. Muchas organizaciones de mayor tamaño cuentan con un administrador de laboratorio a tiempo completo que se encarga de gestionar la red de laboratorio. Otras organizaciones utilizan la arquitectura existente y los equipos de ingeniería para validación de lab. Las responsabilidades de gestión de laboratorio incluyen el pedido de seguimiento de activos y equipos de laboratorio, cableado, gestión del espacio físico, la definición de reglas y dirección de laboratorio, programación de laboratorios, documentación de laboratorio, configuración de topologías de laboratorio, redacción de planes de pruebas, realización de pruebas de laboratorio y gestión de posibles problemas identificados.

Tipos de pruebas

En general, hay muchos tipos de pruebas diferentes que pueden realizarse. Antes de crear un laboratorio de pruebas completo y un plan de pruebas que pueda probarlo todo en una multitud de configuraciones, una organización debe comprender los diferentes tipos de pruebas, el propósito de las pruebas y si la ingeniería, el marketing técnico o la defensa de clientes de Cisco deben o no ser responsables de algunas de las distintas pruebas. Los planes de prueba para clientes suelen abarcar los tipos de prueba más expuestos. La siguiente tabla ayuda a entender los diferentes tipos de prueba, cuándo deben realizarse las pruebas y las partes responsables.

De las pruebas que se indican a continuación, las pruebas adecuadas del conjunto de funciones, la topología y la combinación de aplicaciones específicas de una organización suelen ser las más valiosas. Es importante saber que Cisco realiza pruebas completas de funciones y regresión, pero Cisco no puede probar el perfil de aplicaciones de su organización con su combinación específica de topología, hardware y funciones configuradas. De hecho, no es factible probar toda la gama de funciones, hardware, módulos y permutaciones de topología. Además, Cisco no puede probar la interoperabilidad con equipos de terceros. Cisco recomienda que las organizaciones prueben la combinación precisa de hardware, módulos, características y topología que se encuentran en su entorno. Estas pruebas se deben llevar a cabo en un laboratorio, con una topología colapsada

que representa el entorno de producción de su organización con otros tipos de pruebas compatibles, como rendimiento, interoperabilidad, interrupción y grabación.

Prueba	Información general sobre pruebas	Responsabilidad de prueba
Función y funcionalidad	Determina si las funciones básicas de Cisco IOS y los módulos de hardware de Cisco funcionan como se anuncia. Se debe probar la funcionalidad de la función o del módulo, así como las opciones de configuración de la función. Se deben probar la eliminación y la adición de la configuración. Se incluyen pruebas básicas de interrupción y pruebas de grabación.	Prueba de dispositivos de Cisco
Regresión	Determina si la función o el módulo funciona junto con otros módulos y funciones, y si la versión de Cisco IOS funciona conjuntamente con otras versiones de Cisco IOS en relación con las funciones definidas. Incluye algunas pruebas de quemaduras y interrupciones.	Prueba de regresión de Cisco
Rendimiento básico de los	Determina el rendimiento	Prueba de dispositivos de

dispositivos	básico de la función o módulo para determinar si la función o los módulos de hardware de Cisco IOS cumplen los requisitos mínimos de carga.	Cisco
Topología/Función/Combinación de hardware	Determina si las funciones y los módulos funcionan como se espera en una combinación específica de topología y módulo/función/hardware. Esta prueba debería incluir la verificación de protocolos, funciones y de los comandos show, las pruebas programadas en fábrica y las pruebas de interrupción.	Cisco prueba topologías anunciadas estándar en laboratorios como la ingeniería de soluciones empresariales (ESE) y la ingeniería de pruebas de integración de soluciones en red (NSITE). Los clientes de alta disponibilidad deben probar las combinaciones de características/módulos/topologías según sea necesario, especialmente con el software de adopción temprana y las topologías no estándar.
Interrupción (Qué pasa si)	Incluye tipos o comportamientos de interrupción comunes que pueden ocurrir en un entorno específico de característica/módulo/topología y posible impacto en la funcionalidad. Las pruebas de interrupción	Cisco es responsable de las pruebas de interrupción básicas. En última instancia, los clientes son los responsables de las interrupciones en el rendimiento relacionadas con la escalabilidad de su entorno individual. Las pruebas de

	incluyen el intercambio de tarjeta, oscilación de link, fallas de link y fallas de tarjeta.	interrupción se deben realizar, si es posible, en el entorno de laboratorio del cliente.
Rendimiento de la red (qué sucede)	Investiga la carga del dispositivo en relación con una combinación específica de característica/hardware/topología. El centro de atención es el desempeño y la capacidad del dispositivo como por ejemplo la utilización de la CPU, la memoria y el búfer y el uso del link con relación al tipo de tráfico y a los requerimientos de los recursos en cuanto a protocolos, vecinos, número de rutas y otras características del conjunto. Esta prueba ayuda a asegurar la escalabilidad en entornos más grandes.	En última instancia, los clientes son los responsables de la carga y la escalabilidad de los dispositivos. Las preocupaciones de carga y escalabilidad suelen surgir a través de los servicios avanzados o de ventas de Cisco y a menudo se prueban con laboratorios de Cisco, como los Laboratorios de prueba de concepto (CPOC) del cliente.
Corrección de errores	Garantiza que las correcciones de errores reparen el defecto identificado.	Cisco prueba las correcciones de errores para asegurarse de que se corrige el error. Los clientes también deben probar para asegurarse de que el error que han experimentado se corrija y que el error no interrumpa ningún otro aspecto

		del módulo o la función. Las versiones de mantenimiento se prueban de regresión, pero las versiones provisionales no suelen.
Administración de la red	Investiga las capacidades de gestión del protocolo simple de administración de red (SNMP), la precisión de variables MIB SNMP, el soporte de trampa y la compatibilidad con Syslog.	Cisco es responsable de probar las funciones básicas de SNMP, la funcionalidad y la precisión de las variables MIB. Los clientes deben validar los resultados de la gestión de la red y, en última instancia, son responsables de la estrategia y la metodología de gestión para las nuevas implementaciones de tecnología.
Emulación de red a gran escala	La emulación de red a gran escala utiliza herramientas como el simulador de router de Agilent y el conjunto de herramientas de prueba de Spirent para simular entornos más grandes. Esto podría incluir los vecinos protocolos, los conteos de circuito virtual permanente de retransmisión de tramas (PVC), los tamaños de las tablas de	Los clientes de Cisco son generalmente responsables de los aspectos de las pruebas de simulación de red que reproducen su entorno de red, que puede incluir el número de vecinos/adyacencias del protocolo de ruteo y los tamaños de tabla de ruteo asociados y otros recursos que están en producción.

	ruteo, las entradas de memoria caché y otros recursos normalmente necesarios en la producción que no están disponibles en laboratorio de forma predeterminada.	
Interoperabilidad	Pone a prueba todos los aspectos relacionados con la conectividad a equipos de red de terceros, especialmente si se requiere interoperabilidad de protocolo o señalización.	En general, los clientes de Cisco son responsables de todos los aspectos de las pruebas de interoperabilidad.
Grabación	Investiga los recursos del router con el tiempo. Las pruebas de activación suelen requerir que un dispositivo esté cargado de alguna manera con la investigación del uso de los recursos, incluida la memoria, la CPU y las memorias intermedias a lo largo del tiempo.	Cisco realiza pruebas básicas de grabación. Se recomienda realizar pruebas con clientes en relación con combinaciones únicas de topología, dispositivo y función.

Metodología de prueba

Una vez que una organización sabe lo que está probando, se debe desarrollar una metodología para el proceso de prueba. El objetivo de una mejor práctica es probar la metodología para ayudar a comprobar que lo acordado sobre las pruebas es completo, bien documentado, fácil de reproducir y valioso en términos de encontrar los problemas potenciales de producción. La documentación y la recreación de escenarios de laboratorio es especialmente importante para probar versiones posteriores o para probar las correcciones de errores encontradas en el entorno

de laboratorio. A continuación se muestran los pasos de una metodología de prueba. También pueden realizarse algunos pasos de prueba simultáneamente.

1. Cree una topología de prueba que simule el entorno de producción sometido a prueba. Un entorno de prueba de extremo de la WAN puede incluir unos pocos routers de núcleo y un solo router de borde, mientras que una prueba de LAN puede incluir más dispositivos que puedan representar mejor el entorno.
2. Configure las funciones que simulan el entorno de producción. La configuración de los dispositivos de laboratorio debe coincidir estrechamente con las configuraciones esperadas de hardware y software de los dispositivos de producción.
3. Escriba un plan de prueba, defina las pruebas y los objetivos, documente la topología y defina las pruebas funcionales. Las pruebas incluyen la validación básica del protocolo, la validación del comando show, interrupción de la prueba y prueba de impresión a fuego. En la tabla siguiente se muestra un ejemplo de una prueba específica dentro de un plan de pruebas.
4. Valide la funcionalidad de ruteo y protocolo. Documentar o basar los resultados **esperados del comando show**. Los protocolos deberían incluir tanto protocolos de Capa 2 (por ejemplo ATM, Frame Relay, Protocolo de detección de Cisco (CDP), Ethernet y Árbol de expansión) como protocolos de Capa 3 (por ejemplo IP, IPX y multidifusión).
5. Valide la funcionalidad de la función. Documentar o basar los resultados **esperados del comando show**. Las funciones pueden incluir comandos de configuración globales y cualquier función crítica como la autenticación, autorización y contabilidad (AAA).
6. Simule carga, que es lo esperado en el entorno de producción. La simulación de carga se puede realizar con los recopiladores/generadores de tráfico. Validar las variables de uso del dispositivo de redes esperadas incluidas la CPU, memoria, uso del búfer y estadísticas de interfaz con una investigación de pérdida de paquetes. Documentar o basar los resultados **esperados del comando show**.
7. Realice pruebas de interrupción en las que se espera que el dispositivo y el software gestionen o eviten la sobrecarga. Por ejemplo, la eliminación de tarjetas, la inestabilidad de enlaces, la inestabilidad de rutas y las tormentas de difusión. Asegúrese de que se generen las trampas SNMP correctas en función de las funciones que se utilizan dentro de la red.
8. Documentar los resultados de las pruebas y las mediciones de los dispositivos a medida que las pruebas deben ser repetibles.

Nombre de la prueba	**Conmutación por fallo del protocolo de router en espera en caliente (HSRP)**
Requisitos de configuración de prueba	Aplique la carga a la interfaz de gateway principal. El tráfico debe ser aproximadamente 20% hacia la gateway desde la perspectiva de la estación del usuario y 60% entrante hacia la perspectiva de la estación del usuario. Además, aumente el tráfico a una carga mayor.
Pasos de prueba	Monitoree STP y HSRP a través de los comandos **show**. Error en la conexión de interfaz de gateway principal y, a continuación, recupere la conexión después de recopilar la información.
Mediciones	CPU durante la conmutación por fallas. Muestra la interfaz antes, durante y después del gateway

esperadas	principal y secundaria. Mostrar la interfaz HSRP antes, durante, y después.
'Resultados esperados'	La gateway primaria conmuta por error hacia la otra gateway del router en dos segundos. **los** comandos **show** reflejan correctamente el cambio. La conmutación por fallas al gateway principal ocurre cuando se restaura la conectividad.
Resultados reales	
Éxito o error	
Modificaciones necesarias para lograr el éxito	

Mediciones de dispositivos

Durante la fase de prueba, realice y documente las siguientes mediciones para asegurarse de que el dispositivo funciona correctamente:

- Uso de la memoria
- Cargas de CPU
- Uso del búfer
- Estadísticas de interfaz
- Tablas de rutas
- Depuración específica

La información para las mediciones varía de acuerdo a la prueba implementada. Puede haber información adicional para la medición. Esto depende de los problemas específicos que se están tratando.

Para cada aplicación que se está probando, mida parámetros para asegurarse de que no hay un impacto negativo en el rendimiento de la aplicación dada. Esto se completa utilizando una base de referencia de rendimiento que se puede utilizar para comparar el rendimiento antes y después de la implementación. Algunos ejemplos de pruebas de medición de aplicaciones son:

- El tiempo promedio que lleva registrarse en una red.
- El tiempo promedio que requiere el Sistema de archivos de red (NFS) para copiar un grupo de archivos.
- Tiempo promedio que se tarda en iniciar una aplicación y recibir el mensaje con la primera pantalla.
- Otros parámetros específicos de la aplicación.

Implementación - Implementación rápida y exitosa de Cisco IOS

Un proceso de implementación bien definido permite a una organización implementar de manera eficiente nuevas versiones de Cisco IOS.

La fase de aplicación incluye el proceso experimental y el proceso de aplicación. El proceso piloto garantiza que la versión de Cisco IOS tendrá éxito en el entorno y el proceso de implementación permite implementaciones rápidas y exitosas de Cisco IOS a mayor escala.

Estrategia y herramientas para la instalación del IOS de Cisco

La estrategia para las implementaciones del Cisco IOS es realizar una certificación final vía un proceso piloto y una implementación rápida por medio de herramientas de actualización y un proceso de implementación bien definido.

Antes de iniciar un proceso piloto de red, muchas organizaciones crean directrices piloto generales. Las pautas piloto deberían incluir las expectativas de todos los pilotos, como criterios, ubicaciones aceptables de pilotos, documentación piloto, expectativas de propietarios de pilotos, requisitos de notificación de usuarios y tiempos piloto previstos. Un equipo interfuncional de ingeniería, implementación y operaciones suele participar en la creación de directrices piloto generales y un proceso piloto. Una vez creado el proceso piloto, los grupos individuales de implementación pueden llevar a cabo pilotos exitosos mediante los mejores métodos de práctica conocidos.

Una vez que se haya aprobado una nueva versión de software para la implementación y la certificación final, la organización necesita iniciar la planeación de la actualización de IOS de Cisco. La planificación comienza con la identificación de los requerimientos de una nueva imagen, que incluyen la plataforma, la memoria, flash y la configuración. Los grupos de arquitectura e ingeniería normalmente definen nuevos requisitos de imagen de software en la fase de administración candidata del ciclo de vida de administración de Cisco IOS. Una vez que se identificaron los requerimientos, el grupo de implementación debe validar cada dispositivo y, si es posible, actualizarlo. El módulo CiscoWorks2000 Software Image Manager (SWIM) también puede ejecutar el paso de validación mediante la validación de los requerimientos de Cisco IOS en relación con el inventario de dispositivos. Cuando todos los dispositivos fueron validados y/o actualizados con los nuevos estándares de imagen correctos, el grupo de implementación puede iniciar un proceso de implementación de comienzo lento que utiliza el módulo SWIM de CiscoWorks2000 como herramienta de despliegue de software.

Una vez que la nueva imagen se ha implementado exitosamente varias veces, la organización puede comenzar a ponerse en funcionamiento al usar SWIM CiscoWorks.

Administración del inventario de Cisco IOS

El administrador de inventario CiscoWorks2000 Resource Manager Essentials (RME) simplifica mucho la administración de versiones de los routers y switches de Cisco a través de herramientas de informes basados en la Web que informan y ordenan los dispositivos Cisco IOS según la versión del software, la plataforma del dispositivo y el nombre de éste.

SWIM de Cisco IOS

CiscoWorks2000 SWIM puede ayudar a reducir las complejidades propensas a errores del proceso de actualización. Los enlaces integrados a CCO relacionan la información en línea de Cisco sobre los parches de software con el software Cisco IOS y Catalyst implementado en la red, destacando las notas técnicas relacionadas. Las nuevas herramientas de planificación encuentran

los requisitos del sistema y envían notificaciones cuando se necesitan actualizaciones de hardware (ROM de inicio, memoria RAM Flash) para admitir las actualizaciones de imágenes de software propuestas.

Antes de iniciar una actualización, los requisitos previos de una nueva imagen se validan con el switch de destino o los datos de inventario del router para ayudar a garantizar una actualización exitosa. Cuando se actualizan múltiples sistemas, SWIM sincroniza las tareas de descarga y permite al usuario monitorear el progreso del trabajo. Los trabajos programados son controlados a través de un proceso de cierre de datos, permitiendo que los gerentes autoricen las actividades de un técnico antes de iniciar cada actividad de actualización. RME 3.3 incluye la capacidad para analizar las actualizaciones del software para Cisco IGX, BPX, y las plataformas de MGX, que en gran medida simplifican y reducen el tiempo requerido para determinar el impacto de una actualización de software.

Proceso piloto

Para minimizar la exposición potencial y capturar con mayor seguridad cualquier problema de producción restante, se recomienda un programa piloto. En general, los pilotos son más importantes para los nuevos despliegues tecnológicos, sin embargo, muchos despliegues nuevos de software serán enlazados con los servicios, las funciones o hardware nuevos, donde un piloto es más crítico. El plan piloto individual debe tener en cuenta la selección piloto, la duración piloto y la medición. La selección de piloto es el proceso para identificar cuándo y dónde debe realizarse un piloto. La medición piloto es el proceso de recopilación de los datos necesarios para identificar el éxito y el fracaso o los problemas potenciales.

La selección piloto identifica dónde y cómo se completará un piloto. Un piloto puede comenzar con un dispositivo en un área de bajo impacto y extenderse a varios dispositivos en un área de mayor impacto. Algunas consideraciones para la selección piloto donde se puede reducir el impacto son las siguientes:

- Instalado en un área de la red resistente a un único impacto del dispositivo debido a la redundancia.
- En un área de la red con un número mínimo de usuarios detrás del dispositivo seleccionado que pueden hacer frente a un posible impacto en la producción.
- Considere la posibilidad de separar el piloto según las líneas de arquitectura. Por ejemplo, puede probarlo en las capas de acceso, distribución y/o núcleo de la red.

La duración de este piloto deberá basarse en el tiempo que requiere para probar y evaluar suficientemente todas las funciones de los dispositivos. Esto debería incluir tanto la grabación como la red bajo cargas de tráfico normales. La duración también depende del paso en la actualización de código y del área de la red donde el Cisco IOS se está ejecutando. Si Cisco IOS es una nueva versión principal, se prefiere un período piloto más largo. Mientras que si la actualización es una versión de mantenimiento con funciones nuevas mínimas, un período piloto más corto será suficiente.

Durante la fase piloto es importante supervisar y documentar los resultados de manera similar a la prueba inicial. Puede incluir encuestas, recolección de datos piloto, recolección de problemas y criterios de falla/éxito. Las personas deben ser directamente responsables del seguimiento y la supervisión de los progresos realizados en la fase piloto para asegurarse de que se detecten todos los problemas y de que los usuarios y servicios que participan en la fase piloto estén satisfechos con los resultados de la prueba piloto. La mayoría de las organizaciones certificarán una versión si tiene éxito en un entorno piloto o de producción. En algunos entornos, este paso es un fracaso crítico debido a un éxito percibido cuando no se identifican o documentan criterios de

medición o éxito.

Instrumentación

Una vez que la fase piloto se haya completado dentro de la red de producción, comience la fase de implementación de Cisco IOS. La fase de implementación incluye diversos pasos para asegurar el éxito de la actualización del software y la eficacia de la implementación, incluyendo inicio lento de la implementación, certificación final, preparación de la actualización, automatización de la actualización y validación final.

El inicio lento de la implementación es el proceso de implementación lenta de una versión recientemente probada para asegurarse de que la imagen esté completamente expuesta al entorno de producción antes de la certificación final y la conversión a escala completa. Algunas organizaciones pueden comenzar con un dispositivo y un día de exposición antes de pasar a las actualizaciones de dos dispositivos al día siguiente y quizás algunos más al otro día. Cuando se han puesto en producción aproximadamente diez dispositivos, la organización puede esperar hasta una o dos semanas antes de la certificación final de la versión específica del IOS de Cisco. En la certificación final, la organización puede desplegar más rápidamente la versión identificada con un nivel de confianza mucho más alto.

Después del proceso de inicio lento, todos los dispositivos identificados para la actualización deben revisarse y validarse usando el inventario de dispositivos y una matriz de los estándares mínimos de Cisco IOS para bootstrap, DRAM y flash para asegurarse de que se cumplen los requisitos. Los datos pueden adquirirse a través de herramientas internas, herramientas SNMP de terceros o a través del uso de CiscoWorks2000 RME. El CiscoWorks2000 SWIM no revisa o inspecciona estas variables antes de instrumentarlas. Sin embargo, siempre es una buena idea saber qué esperar durante los intentos de implementación.

Si se programan más de cien dispositivos similares para las actualizaciones, se recomienda encarecidamente utilizar un método automatizado. Se ha demostrado que la automatización mejora la eficacia de las actualizaciones y el porcentaje de éxitos en las actualizaciones de dispositivos durante implementaciones de gran tamaño, basándose en una actualización interna de 1000 dispositivos con y sin SWIM. Cisco recomienda que CiscoWorks 2000 SWIM se utilice para implementaciones de gran tamaño debido al grado de verificación que se realiza durante la actualización. SWIM incluso saldrá de una versión de Cisco IOS si se detecta un problema. SWIM funciona mediante la creación y programación de trabajos de actualización, donde se configura un trabajo con los dispositivos, imágenes de actualización deseadas y tiempo de ejecución del trabajo. Cada trabajo debe contener doce o menos actualizaciones de dispositivos y hasta doce trabajos pueden ejecutarse simultáneamente. SWIM también verifica que la versión de actualización de Cisco IOS programada se ejecute satisfactoriamente luego de la actualización. Se recomienda permitir aproximadamente veinte minutos para cada actualización del dispositivo (incluida la verificación). Con esta fórmula, una organización puede actualizar treinta y seis dispositivos por hora. Cisco también recomienda actualizar un máximo de cien dispositivos por noche para reducir la exposición a posibles problemas.

Después de una actualización automatizada, se debe realizar alguna validación para garantizar el éxito. La herramienta SWIM de CiscoWorks2000 puede ejecutar secuencias de comandos personalizadas luego de la actualización a fin de realizar más comprobaciones de éxito. La verificación incluye la validación de que el router tiene el número de rutas apropiado, la garantía de que las interfaces físicas/lógicas están funcionando y activas o la validación de que el dispositivo es accesible. La siguiente lista de verificación de ejemplo puede validar completamente el éxito de una implementación de Cisco IOS:

- ¿El dispositivo se recargó correctamente?
- ¿Es posible realizar ping y alcanzar el dispositivo a través de las plataformas del sistema de administración de red (NMS)?
- ¿Están activas y activas las interfaces esperadas en el dispositivo?
- ¿El dispositivo tiene las adyacencias de protocolo de ruteo correctas?
- ¿Se ha llenado la tabla de ruteo?
- ¿El dispositivo pasa el tráfico correctamente?

Funciones: gestionar la implementación de Cisco IOS de alta disponibilidad

Las operaciones de prácticas recomendadas de alta disponibilidad del entorno de Cisco IOS ayudan a reducir la complejidad de la red, mejorar el tiempo de resolución de problemas y mejorar la disponibilidad de la red. La sección de operaciones de la administración de Cisco IOS incluye estrategia, herramientas y metodologías de mejores prácticas recomendadas para administrar Cisco IOS.

Entre las prácticas recomendadas para las operaciones de Cisco IOS se incluyen el control de versiones de software, la administración de Syslog de Cisco IOS, la administración de problemas, la estandarización de la configuración y la administración de disponibilidad. El control de versiones de software es el proceso de seguimiento, validación y mejora de la consistencia del software dentro de las opciones identificadas. La administración de Syslog del IOS de Cisco es el proceso de monitorear proactivamente y actuar en los mensajes Syslog de mayor prioridad generados por el IOS de Cisco. La administración de problemas es la práctica de recolectar información sobre problemas críticos de manera rápida y eficiente para cuestiones de software, con el fin de prevenir que se repitan en el futuro. La estandarización de la configuración es el proceso de estandarización de las configuraciones para reducir el potencial de que el código no probado se ejerza en producción y para estandarizar el comportamiento de los protocolos y las funciones de red. La gestión de la disponibilidad es el proceso para mejorar la disponibilidad en función de las métricas, los objetivos de mejora y los proyectos de mejora.

Estrategias y herramientas para el funcionamiento del IOS de Cisco

Existen muchas herramientas y estrategias de calidad para ayudar a administrar los entornos de Cisco IOS. La primera estrategia clave para las operaciones de Cisco IOS es mantener el entorno sencillo, al evitar la variación en la configuración y en las versiones de Cisco IOS tanto como sea posible. La certificación del IOS de Cisco ya se ha discutido, sin embargo la consistencia de la configuración es otro área clave. El grupo arquitectura/ingeniería debe encargarse de la creación de los estándares de configuración. El grupo de implementación y de operaciones tenía a su cargo la configuración y el mantenimiento de los estándares por medio del control y los estándares de configuración y control de la versión ISO de Cisco.

La segunda estrategia para las operaciones de Cisco IOS es la capacidad de identificar y resolver rápidamente los fallos de red. Los problemas de red generalmente deben ser identificados por el grupo de operaciones antes de que los usuarios los llamen. Deberían resolverse los problemas tan pronto como sea posible antes de que afecten aún más el entorno o provoquen cambios mayores en él. Algunas prácticas recomendadas clave en esta área son la administración de problemas y la administración de Syslog de Cisco IOS. Una herramienta para ayudar a diagnosticar rápidamente caídas del software del IOS de Cisco es el Output Interpreter de Cisco.

La tercera estrategia es una mejora constante. El proceso principal consiste en mejorar un programa de mejora de la disponibilidad basado en la calidad. Mediante el análisis de las causas principales de todos los problemas, incluidos los relacionados con Cisco IOS, una organización puede mejorar la cobertura de las pruebas, mejorar los tiempos de resolución de problemas y mejorar los procesos que eliminan o reducen el impacto de las interrupciones. La organización también puede analizar los problemas comunes y crear procesos para resolverlos más rápidamente.

Las herramientas para operaciones de IOS de Cisco incluyen administración del inventario para el control de la versión de software (CiscoWorks2000 RME), administración de Syslog para mensajes Syslog y administradores de configuración de dispositivos para administrar la uniformidad en la configuración de dispositivos.

Administración de Syslog

Los mensajes syslog son mensajes enviados por el dispositivo a un servidor de recolección. Estos mensajes pueden ser errores (por ejemplo, un link bajando), o pueden ser informativos, tales como cuando alguien ha ingresado a configurar una terminal en un dispositivo.

Las herramientas de administración de Syslog registran y siguen los mensajes de Syslog recibidos por routers y switches. Algunas herramientas poseen filtros para permitir la eliminación de mensajes no deseados que pueden opacar a otros verdaderamente importantes. Las herramientas de Syslog también permiten la creación de informes basados en los mensajes recibidos. Los informes pueden ordenarse por período de tiempo, dispositivo, tipo de mensaje o prioridad de mensaje.

La herramienta Syslog más popular para la administración de Cisco IOS es CiscoWorks2000 RME Syslog Manager. Hay otras herramientas disponibles, como SL4NT, un programa shareware de Netal y Private I de OpenSystems.

Administrador de configuración de dispositivos CiscoWorks

El Administrador de configuración de dispositivos CiscoWorks2000 mantiene un archivo activo y proporciona una forma sencilla de actualizar los cambios de configuración en varios routers y switches de Cisco. El administrador de configuración monitorea la red para ver los cambios de configuración, actualiza el archivo cuando se detecta un cambio y registra la información de cambio en el servicio de auditoría de cambios. Una interfaz de usuario basada en Web permite buscar en el archivo atributos de configuración específicos y comparar el contenido de dos archivos de configuración para facilitar la identificación de diferencias.

Intérprete de resultados de Cisco

El Cisco Output Interpreter es una herramienta utilizada para diagnosticar caídas del sistema forzadas por software. La herramienta puede ayudar a identificar defectos de software sin llamar al Centro de asistencia técnica de Cisco (TAC), o puede ser usada como información primaria para el TAC luego de producirse una caída del sistema forzada por software. En general, esta información ayudará a acelerar la solución del problema, al menos en términos de la recopilación de información necesaria.

'Control de versión de software'

El control de versión de software es el proceso de implementación de sólo versiones de software

estandarizadas y de supervisión de la red, con el fin de validar o, posiblemente, cambiar software debido a que la versión no es la adecuada. En general, el control de versiones de software se realiza mediante un proceso de certificación y control de estándares. Muchas organizaciones publican estándares de versión en un servidor web central. Además, se capacita al personal de implementación para que revise qué versión se está ejecutando y actualice la versión si no cumple con las normas. Algunas organizaciones tienen un proceso de puerta de acceso de calidad en el que se completa la validación secundaria mediante auditorías para asegurarse de que se sigue el estándar durante la implementación.

Durante el funcionamiento, es frecuente ver versiones no estándar en la red, especialmente si el personal de red y operaciones es grande. Esto podría deberse al personal más reciente sin entrenamiento, a los comandos de inicio mal configurados o a las implementaciones sin verificar. Siempre es una buena idea validar periódicamente los estándares de versión de software utilizando herramientas como CiscoWorks 2000 RME que pueden ordenar todos los dispositivos por versión de Cisco IOS. Cuando se identifican versiones de software no estándar, deben marcarse inmediatamente y debe iniciarse un ticket de problema o uno de cambio para hacer que la versión corresponda al estándar identificado.

Administración proactiva de Syslog

La recolección, el monitoreo y el análisis de Syslog son los procesos de administración de fallas recomendados para resolver más problemas de redes específicos de Cisco IOS que son difíciles o imposibles de identificar por otros medios. La recopilación, supervisión y análisis de Syslog ayudan a mejorar el tiempo de resolución de problemas mediante la identificación y resolución de muchos fallos de forma proactiva antes de que los usuarios experimenten o informen de problemas de red más graves. Syslog también proporciona un método más eficiente de recolectar una amplia variedad de problemas cuando se compara con el sondeo SNMP consistente para un gran número de variables MIB. La recopilación, supervisión y análisis de Syslog se realiza mediante la configuración de Cisco IOS correcta, las herramientas de correlación de Syslog, como CiscoWorks2000 RME, y/o la administración de eventos de Syslog. La administración de eventos de Syslog se realiza analizando los datos de Syslog recopilados para los mensajes críticos identificados y reenviando después una alerta o trampa a un administrador de eventos para la notificación y resolución en tiempo real.

La supervisión del sistema de registro requiere de la ayuda de la herramienta NMS o de secuencias para el análisis y la generación de informes en los datos del sistema de registro. Incluye la capacidad para ordenar los mensajes de Syslog por período de tiempo y fecha, dispositivo, tipo de mensaje o frecuencia de mensaje. En redes más grandes, se pueden implementar herramientas o scripts para analizar los datos de Syslog y enviar alertas o notificaciones a sistemas de administración de eventos o al personal de operaciones e ingeniería. Si no se utilizan alertas para una amplia variedad de datos de Syslog, la organización debe revisar los datos de Syslog de mayor prioridad al menos diariamente y crear listas de problemas para posibles problemas. Para detectar proactivamente los problemas de red que pueden no verse a través de la supervisión normal, se deben realizar revisiones y análisis periódicos de los datos históricos de Syslog para detectar situaciones que pueden no indicar un problema inmediato, pero que pueden proporcionar una indicación de un problema antes de que se convierta en un servicio que impacta.

Administración de problemas

Muchos clientes experimentan tiempo de inactividad adicional debido a la falta de procesos en la gestión de problemas. El tiempo de inactividad adicional puede producirse cuando los

administradores de red intentan resolver el problema rápidamente mediante una combinación de comandos que afectan al servicio o cambios de configuración en lugar de dedicar tiempo a la identificación de problemas, la recopilación de información y una ruta de solución bien analizada. El comportamiento observado en esta área incluye la recarga de dispositivos o el borrado de tablas de IP Routing antes de investigar un problema y su causa raíz. En algunos casos, esto ocurre debido a los objetivos de resolución de problemas de soporte de primer nivel. El objetivo de todas las cuestiones relacionadas con software debería ser recolectar rápidamente la información necesaria para el análisis de las causas raíz antes de restaurar la conectividad o el servicio.

Se recomienda un proceso de administración de problemas en entornos más grandes. Este proceso debe incluir una cierta cantidad de descripciones de problemas predeterminados y de grupos de comandos show adecuados antes de subir al segundo nivel. La asistencia de primer nivel nunca debe estar despejando rutas ni recargando dispositivos. Óptimamente, la organización de primer nivel debe recolectar información rápidamente y ascender a un segundo nivel. Al dedicar al principio unos pocos minutos más a la identificación de problemas o la descripción de problemas, es mucho más probable que se detecte la causa raíz, lo que permite una solución temporal, identificación de laboratorio e informes de errores. El soporte de segundo nivel debe estar bien versado en los tipos de información que Cisco puede necesitar para diagnosticar un problema o presentar un informe de bug. Esto incluye vaciados de memoria, resultado de información de ruteo y resultado del comando show del dispositivo.

Estandarización de la configuración

Los estándares de configuración de dispositivos globales representan la práctica de mantener parámetros de configuración globales estándar en dispositivos y servicios similares, lo que se traduce en uniformidad de la configuración global para toda la empresa. Los comandos de configuración global son comandos que se aplican a todo el dispositivo y no a puertos, protocolos o interfaces individuales. Los comandos de configuración globales generalmente afectan al acceso del dispositivo, el comportamiento general del dispositivo y la seguridad del dispositivo. En Cisco IOS, esto incluye comandos de servicio, comandos IP, comandos vty, comandos de puerto de consola, comandos de registro, comandos AAA/TACACS+, comandos SNMP y comandos de banner. También es importante en los estándares de configuración de dispositivos globales una convención de nombres de dispositivos apropiada que permita a los administradores identificar el dispositivo, el tipo de dispositivo y la ubicación del dispositivo en función del nombre del sistema de nombres de dominio (DNS) del dispositivo. La coherencia de la configuración global es importante para la compatibilidad y fiabilidad generales de un entorno de red, ya que ayuda a reducir la complejidad de la red y a mejorar la compatibilidad de la misma. Muchas veces se experimenta una dificultad de soporte sin la estandarización de configuración debido a un comportamiento incorrecto o incoherente del dispositivo, al acceso SNMP y a la seguridad general del dispositivo.

El mantenimiento de los estándares de configuración de dispositivos globales se realiza normalmente mediante un grupo de operaciones o ingeniería interno que crea y mantiene parámetros de configuración globales para dispositivos de red similares. También es una buena práctica proporcionar una copia del archivo de configuración global en los directorios TFTP para que puedan descargarse inicialmente en todos los dispositivos que se aprovisionan recientemente. También es útil un archivo accesible a través de la Web que proporcione al archivo de configuración estándar una explicación de cada parámetro de configuración. Incluso, algunas organizaciones configuran periódicamente dispositivos similares de manera global para garantizar la coherencia de tal configuración o para revisar los dispositivos con regularidad en función de las normas de configuración global adecuadas. Los estándares de configuración de

interfaz y protocolo representan la práctica de estándares de mantenimiento para la configuración de interfaz y protocolo.

La consistencia entre la configuración del protocolo y la de la interfaz aumenta la disponibilidad de la red al reducir la complejidad de ésta, brindar el funcionamiento esperado del dispositivo y el protocolo e incrementar la capacidad de soporte de la red. La irregularidad en la configuración de un protocolo o de una interfaz puede resultar en un comportamiento inesperado del dispositivo, problemas de ruteo de tráfico, crecientes problemas de conectividad y creciente tiempo de soporte reactivo. Los estándares de configuración de interfaz deben incluir descriptores de interfaz CDP, configuración de almacenamiento en caché y otros estándares específicos de protocolo. Los estándares de configuración específicos del protocolo pueden incluir:

- configuración de IP Routing
- configuración de DLSW
- Configuración de la lista de acceso
- configuración ATM
- configuración de Frame Relay
- Configuración del árbol de expansión
- Asignación y configuración de VLAN
- Protocolo de enlace troncal virtual (VTP)
- HSRP

Nota: Es posible tener otros estándares de configuración específicos de protocolo dependiendo de lo que esté configurado dentro de la red.

Un ejemplo de los estándares IP puede incluir:

- Tamaño de subred
- Espacio de dirección IP utilizado
- Protocolo de ruteo utilizado
- Configuración de protocolo de ruteo

El mantenimiento de los estándares de configuración de protocolos e interfaces es normalmente responsabilidad de los grupos de implementación e ingeniería de redes. El personal de ingeniería debe encargarse de identificar, probar, validar y documentar los estándares. A continuación, el grupo de implementación se encarga de utilizar los documentos de ingeniería o las plantillas de configuración para aprovisionar nuevos servicios. El grupo de ingeniería debería crear documentación sobre todos los aspectos de estándares requeridos para asegurar consistencia. También se deben crear plantillas de configuración para ayudar a aplicar los estándares de configuración. Los grupos de operaciones deberían capacitarse con respecto a las normas y deben ser capaces de identificar problemas de configuración no estándar. La coherencia de la configuración es de gran ayuda en la fase de prueba, validación y certificación. De hecho, sin las plantillas de configuración estandarizadas, es casi imposible probar, validar o certificar adecuadamente una versión del IOS de Cisco para una red de tamaño moderado.

Gestión de disponibilidad

La gestión de la disponibilidad es el proceso de mejora de la calidad utilizando la disponibilidad de la red como métrica de mejora de la calidad. Muchas organizaciones están midiendo ahora la disponibilidad y el tipo de interrupción. Los tipos de interrupción incluyen hardware, software, link/portadora, energía/entorno, diseño o error de usuario/proceso. Al identificar las interrupciones y realizar análisis de la causa principal inmediatamente después de la recuperación, la organización puede identificar métodos para mejorar la disponibilidad. Casi todas las redes que

han logrado una alta disponibilidad tienen algún proceso de mejora de la calidad.

Apéndice A: Descripción general de las versiones de Cisco IOS

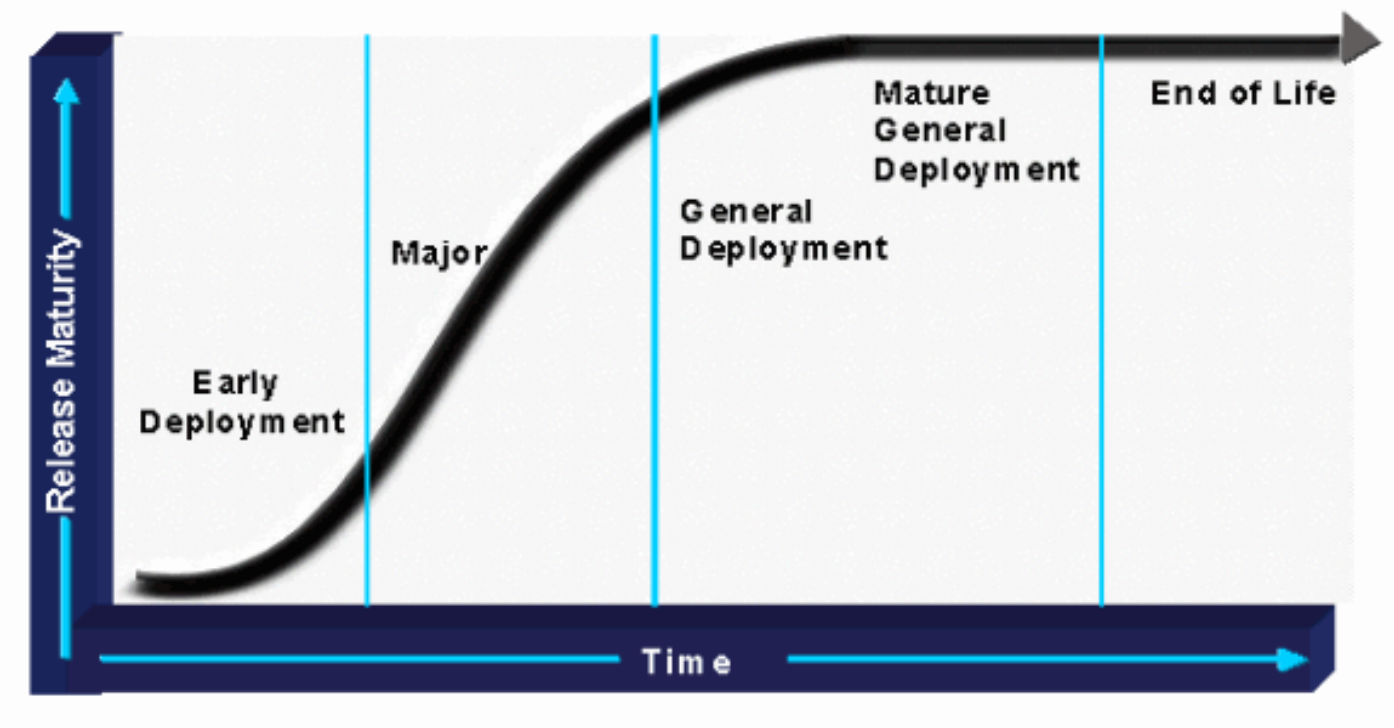
La estrategia de publicación del software del IOS de Cisco se construye alrededor del desarrollo de software seguro, control de calidad y tiempos rápidos de comercialización, factores fundamentales para el éxito de las redes de los clientes de Cisco.

El proceso se define alrededor de cuatro categorías de versiones que se explican a continuación:

- Versión de implementación temprana (ED)
- Versión principal
- Versión de implementación limitada (LD)
- Versión de implementación general (GD)

Cisco crea y mantiene una hoja de ruta de IOS que contiene información sobre versiones individuales, mercados de destino, rutas de migración, descripciones de nuevas funciones, etc.

La figura siguiente ilustra el ciclo de vida de la versión de software del IOS de Cisco:



Versiones ED

Las versiones ED de Cisco IOS son vehículos que aportan un nuevo desarrollo al mercado. Cada revisión de mantenimiento de una versión ED incluye no sólo correcciones de errores, sino también un conjunto de nuevas funciones, soporte de nueva plataforma y mejoras generales a los protocolos y a la infraestructura de Cisco IOS. Cada uno o dos años, las características y plataformas de las versiones ED se trasladan a la próxima versión principal de Cisco IOS.

Existen cuatro tipos de versiones de ED, cada una con características de modelo de versión y ciclo de vida ligeramente distintas. Las versiones ED se pueden clasificar como:

- **Versiones consolidadas de implementación anticipada de tecnología (CTED)**: el nuevo

modelo de versión de Cisco IOS utiliza el tren de versión ED consolidado, también conocido como el tren "T", para introducir nuevas funciones, nuevas plataformas de hardware y otras mejoras en Cisco IOS. Se denominan tecnologías consolidadas porque trascienden las definiciones internas de unidades empresariales (BU) y líneas de negocio (LOB). Ejemplos de versiones de tecnología consolidada son Cisco IOS 11.3T, 12.0T y 12.1T.

- **Versiones específicas de implementación anticipada de tecnología (STED)**: las versiones STED tienen características de compromiso de funciones similares a las de las versiones CTED, excepto que se dirigen a una tecnología específica o mercado. Siempre se presentan en plataformas específicas y están solamente bajo la supervisión de una Cisco BU. Las versiones STED se identifican agregando dos letras a la versión principal. Ejemplos de versiones STED son Cisco IOS 11.3NA, 11.3MA, 11.3WA y 12.0DA.
- **Versiones específicas de implementación temprana en el mercado (SMED)**: las SMED de Cisco IOS se diferencian de las STED por el hecho de que se dirigen a un segmento de mercado vertical específico (ISP, empresas, instituciones financieras, compañías de Telcom, etc.). Las PYMES incluyen requisitos específicos de funciones tecnológicas sólo para plataformas específicas de importancia utilizadas por el mercado vertical previsto. Se pueden diferenciar de las CTED por el hecho de que sólo se construyen para plataformas específicas de importancia para el mercado vertical, mientras que las CTED se crearían para más plataformas basadas en un requisito tecnológico más amplio. Las versiones SMED de Cisco IOS se identifican mediante un carácter alfabético agregado a la versión de la versión principal (al igual que CTED). Ejemplos de SMED son Cisco IOS 12.0S y 12.1E.
- **Versiones de implementación temprana de corta duración, también conocidas como X Releases (XED)**: las versiones XED de Cisco IOS introducen en el mercado nuevos hardware y tecnologías. No proporcionan revisiones de mantenimiento de software ni proporcionan revisiones interinas de software normal. Si se encuentra un defecto en el XED antes de su convergencia con el CTED, se inicia una reconstrucción de software y se agrega un número al nombre. Por ejemplo, las versiones 12.0(2)XB1 y 12.0(2)XB2 del IOS de Cisco son ejemplos de reconstrucciones 12.0(2)XB.

Versiones principales

Las versiones principales son los principales vehículos de implementación para los productos de software del IOS de Cisco. Son administrados por la División Tecnología del IOS de Cisco y consolida las funciones, plataformas, funcionalidad, tecnología y la proliferación del host de versiones ED anteriores. Las versiones principales de Cisco IOS buscan una mayor estabilidad y calidad. Por esa razón, las versiones principales no aceptan la adición de funciones o plataformas. Cada revisión de mantenimiento proporciona solamente correcciones de errores. Por ejemplo, las versiones 12.1 y 12.2 del software del IOS de Cisco son versiones principales.

Las versiones principales tienen actualizaciones de mantenimiento programadas denominadas versiones de mantenimiento que se han probado completamente con regresión, incorporan las correcciones de errores más recientes y no admiten nuevas plataformas o funciones. El número de versión de una versión importante identifica la importancia de la versión y el nivel de mantenimiento. En Cisco IOS Software Release 12.0(7), 12.0 es el número de la versión principal y 7 es su nivel de mantenimiento. El número de versión completo es 12.0(7). De modo similar, 12.1 es una versión principal y 12.1(3) es la tercera versión de mantenimiento de la versión principal 12.1 del IOS de Cisco.

Versiones de implementación limitada (LD)

LD es la fase de madurez de Cisco IOS entre FCS y la implementación general para las versiones

principales. Las versiones ED de Cisco IOS solo se encuentran en la fase de implementación limitada porque nunca alcanzan la certificación GD.

Versiones de implementación general (GD)

En algún momento durante el ciclo de vida de la versión, Cisco declarará una versión principal lista para la certificación GD. Sólo una versión principal puede alcanzar el estado GD. Cumple con el objetivo de la certificación GD cuando Cisco se satisface de que la versión ha sido:

- Probada a través de exposición prolongada en el mercado en diversas redes.
- Calificado según mediciones analizadas en función de tendencias de estabilidad y errores.
- Calificado mediante las encuestas de satisfacción de los clientes.
- Una reducción en la tendencia normalizada del cliente encontró defectos en la versión con respecto a las cuatro versiones de mantenimiento anteriores.

Se ha formado un equipo interfuncional de certificación GD de defensa del cliente compuesto por ingenieros del TAC, ingenieros de servicios de ingeniería avanzada (AES), ingeniería de pruebas del sistema e ingeniería del IOS de Cisco para evaluar todos los defectos pendientes de la versión. Este equipo otorga la aprobación final para la certificación GD. Cuando una versión alcance el estado GD, todas las revisiones subsecuentes de la versión también serán GD. Por consiguiente, una vez declarada la liberación, ingresa automáticamente a la fase de mantenimiento restringido. Mientras está en esta fase, la modificación de ingeniería del código, incluidas las correcciones de errores con rediseño del código principal, está estrictamente limitada y controlada por un administrador de programas. Esto asegura que no se introduzcan errores adversos en una versión de software del IOS de Cisco con certificación GD. GD se logra por medio de una versión de mantenimiento particular. Las actualizaciones de mantenimiento posteriores para esa versión también son versiones de GD. Por ejemplo, Cisco IOS Software Release 12.0 obtuvo la certificación GD en 12.0(8). Por lo tanto, las versiones 12.0(9), 12.0(10) y así sucesivamente son versiones GD.

Imágenes experimentales o diagnósticas

Las imágenes experimentales o de diagnóstico a veces se denominan especiales de ingeniería y sólo se crean cuando se han identificado problemas críticos de software. Estas imágenes no forman parte del proceso normal de lanzamiento. Las imágenes de esta categoría son generaciones específicas para el cliente diseñadas para ayudar a diagnosticar un problema, probar una corrección de errores o proporcionar una solución inmediata. Se puede proporcionar una solución inmediata cuando no es posible esperar a la siguiente versión provisional o de mantenimiento. Las imágenes experimentales o de diagnóstico pueden construirse sobre cualquier base de software soportada, incluidas las versiones provisionales o de mantenimiento de cualquier tipo de versión. No existen convenciones oficiales de nomenclatura, pero en muchos casos el desarrollador agregará iniciales, exp (para experimentación) o dígitos adicionales al nombre de la imagen base. Estas imágenes son soportadas solamente de manera temporal junto con el desarrollo de Cisco debido a que las operaciones de Cisco TAC y de la versión Cisco IOS no conservan documentación complementaria como tablas de símbolos o historia de imagen base. Estas imágenes no se someten a pruebas internas de Cisco.

Puntos destacados de la vida útil de la versión

En algún momento, las versiones de GD se sustituyen por nuevas versiones con las últimas tecnologías de red. Por lo tanto, un proceso de eliminación de versión fue establecido con los siguientes tres ejes principales:

- **Fin de ventas (EOS)**: para las versiones principales, la fecha de EOS es tres años después de la fecha del primer envío comercial (FCS). Esto establece una fecha final para la compra de la versión para nuevos sistemas. La versión de EOS aún puede descargarse desde Conexión en línea de Cisco (CCO) para realizar actualizaciones de mantenimiento.
- **Fin de ingeniería (EOE)**: la versión de EOE es la última versión de mantenimiento para la versión de GD y suele seguir aproximadamente tres meses después de la versión de EOS. Los clientes pueden seguir recibiendo soporte técnico del TAC de Cisco, así como descargar la versión de EOE de CCO. Se publica el boletín del producto que anuncia las fechas y versiones de EOS y EOE un año antes de la fecha estipulada de EOS. En este momento, los clientes deben empezar a investigar la actualización de su software Cisco IOS para aprovechar las últimas tecnologías de red.
- **Fin de vida útil (EOL)**: al final del ciclo de vida de la versión, se termina toda la compatibilidad con la versión de software del IOS de Cisco y ya no está disponible para la descarga en la fecha de fin de vida útil. En general, la fecha EOL es cinco años después de la fecha EOE. Un boletín del producto EOL se publica aproximadamente un año antes de la fecha EOL real.

Convención de nombres de versión de Cisco IOS

La convención para nombres de imágenes del IOS de Cisco proporciona un perfil completo de todas las imágenes lanzadas. El nombre siempre incluye el identificador de versión principal y el identificador de versión de mantenimiento. El nombre también podría incluir un designador de tren, un designador de reconstrucción (para la versión de mantenimiento), designadores de características específicas de una unidad de negocios (BU) e identificadores de reconstrucción de designador de característica específica de una BU. El formato se puede desglosar de la siguiente manera:

Sección Convención de denominación	Explicación
x.y	Una combinación de dos identificadores de dígitos separados (uno o dos) separados por un '.' que identifica el valor de versión principal. Este valor lo determina el marketing de Cisco IOS. Ejemplo: 12,1
z	Uno a tres dígitos que identifican la versión de mantenimiento de x.y. Esto ocurre cada ocho semanas. Los valores son 0 en beta, 1 en FCS y 2 para la primera versión de mantenimiento. Ejemplo: 12.1(2)
p	Un carácter alfa que identifica una reconstrucción de x.y(z). El valor comienza con una "a" minúscula para la primer reconstrucción,

	sigue con una "b" y así sucesivamente. Ejemplo: 12.1(2a)
R	Una a tres letras alfa son el designador del tren de liberación y son obligatorias para las versiones CTED, STED y X. También identifica una familia de productos o plataformas. Las versiones ED de tecnología utilizan dos letras. La primera letra representa la tecnología y la segunda letra se utiliza para diferenciación. Por ejemplo: 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) Una "X" en la primera posición del nombre de la versión identifica una versión única basada en el tren CTED "T". Por ejemplo, XA, XB, XC, etc. Una "X" o "Y" en la segunda posición del nombre de la versión identifica una versión ED de corta duración basada en una versión STED o afiliada a ella. Por ejemplo, 11.3NX (basado en 11.3NA), 11.3WX (basado en 11.3WA), etc.
o	Designador numérico opcional de uno o dos dígitos que identifica una reconstrucción de un valor de versión en particular. Deje en blanco si no representa una reconstrucción. Comienza con 1, luego 2, y así sucesivamente. Ejemplo: 12.1(2)T1, 12.1(2)XE2
u	Designador numérico de uno o dos dígitos que identifica la funcionalidad de la versión específica de la BU. El valor está determinado por el equipo de marketing de BU. Ejemplo: 11.3(6)WA4, 12.0(1)W5
v	Designador numérico de uno a dos dígitos que identifica la versión de mantenimiento del código específico de la BU. Los valores son 0 en beta, 1 en FCS y 2 para la primera versión de mantenimiento. Ejemplo: 11.3(6)WA4(9), 12.0(1)W5(6)
p	Un indicador de carácter alfa que identifica una nueva compilación de una versión tecnológica específica. El valor comienza con una "a" minúscula para la primera recopilación; luego, "b" y así sucesivamente. Ejemplo: 11.3(6)WA4(9a) sería una recopilación de 11.3(6)WA4(9).

El siguiente gráfico rotula las distintas secciones de la convención de nombres de IOS de Cisco:

Apéndice B: fiabilidad de Cisco IOS

La fiabilidad de Cisco IOS es un área en la que Cisco se esfuerza continuamente por mejorar. Antes de hablar de las mejores prácticas orientadas al cliente, es necesario comprender mejor los esfuerzos de fiabilidad y calidad del IOS interno de Cisco. Estas secciones principalmente tienen el propósito de proporcionar una descripción general de los esfuerzos más recientes de Cisco en la calidad del software del IOS de Cisco y qué suposiciones de los clientes deberían realizarse teniendo en cuenta la confiabilidad del software.

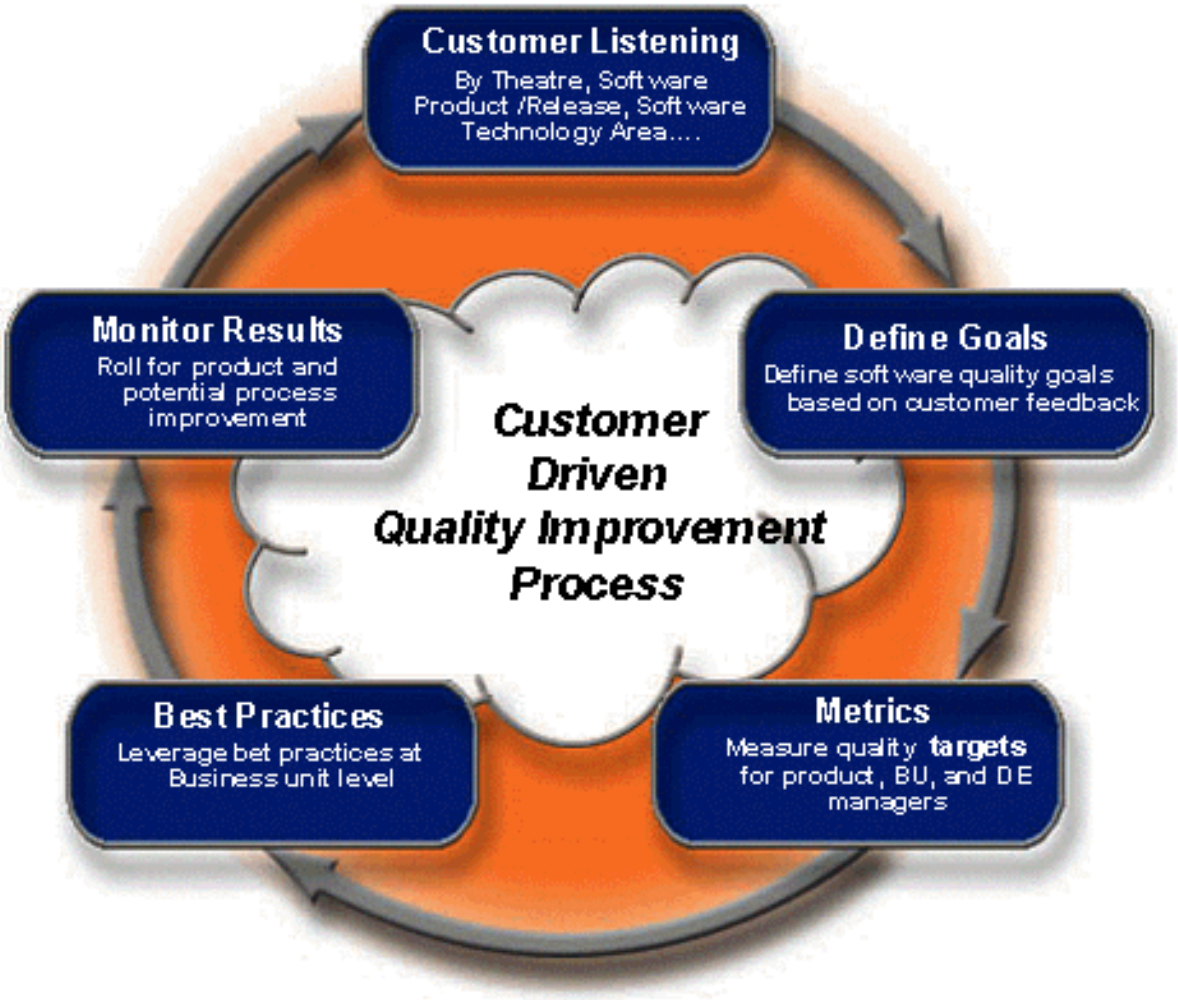
Programa de calidad de Cisco IOS

Cisco cuenta con un proceso de desarrollo de IOS bien definido llamado GEM Great Engineering Methodology (GEM). Este proceso tiene un ciclo de vida de tres fases:

- Estrategia y planificación
- Ejecución
- Implementación

Entre las áreas generales del ciclo de vida se incluyen la priorización de la introducción de características, el desarrollo, el proceso de prueba, las fases de introducción del software, el envío del primer cliente (FCS), GD y la ingeniería de mantenimiento. Cisco también sigue una serie de directrices de mejores prácticas de calidad de software de organizaciones como International Standards Organization (ISO), Telcordia (anteriormente Bellcore), IEEE y el Carnegie Mellon Software Engineering Institute. Estas directrices se incorporan a los procesos GEM de Cisco. Los procesos de desarrollo de software de Cisco cuentan con la certificación ISO 9001 (1994).

El proceso principal para el mejoramiento de la calidad del software IOS de Cisco es un proceso orientado al cliente mediante el cual Cisco escucha al cliente, define las metas y las métricas, implementa las mejores prácticas y monitorea los resultados. Un equipo interorganizacional comprometido con la mejora de la calidad del software impulsa este proceso. A continuación se muestra un diagrama del proceso de mejora de la calidad de Cisco IOS:



El proceso de mejora de la calidad tiene objetivos claramente medibles para el ejercicio 2002 y años posteriores. El enfoque principal de estos objetivos es el de reducir los defectos al identificar los problemas de software en una etapa temprana del ciclo de prueba, reducir el registro de defectos, mejorar la consistencia de características y la claridad de la versiones de software, y brindar programas de versiones predecibles y calidad de software de manera constante. Entre las iniciativas para abordar estas áreas se incluyen nuevas herramientas de cobertura de pruebas (que identifican áreas de menor cobertura de pruebas), mejoras en el proceso de acción correctiva de prueba y mejoras en las pruebas de regresión del sistema de Cisco IOS. Se han aplicado recursos adicionales para abordar estos problemas y existe un compromiso ejecutivo y multifuncional para todas las versiones principales del software Cisco IOS.

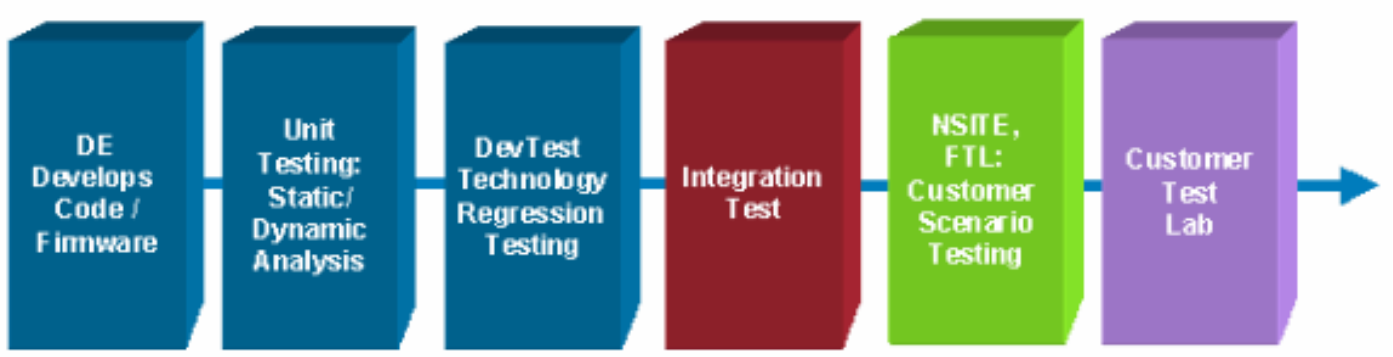
Prueba de la versión de Cisco IOS

Una parte integral del esfuerzo de calidad de la confiabilidad del software dentro de Cisco es la calidad, el alcance y la cobertura de las pruebas. En general, Cisco tiene los siguientes objetivos de calidad de IOS:

- Reducir los defectos de regresión interna de Cisco encontrados. Esto incluye una mayor calidad en el desarrollo y la identificación de más problemas en el análisis estático/dinámico.
- Reduzca los defectos detectados por el cliente
- Reducción de los defectos extraordinarios totales.
- Aumentar la claridad de las versiones de software y la uniformidad de las funciones
- Proporcionar versiones de funciones y mantenimiento con programaciones y calidad

Las pruebas internas de Cisco pueden considerarse un proceso en el que se identifican diferentes

defectos en diferentes etapas de las pruebas. El objetivo general es encontrar los tipos correctos de defectos en el laboratorio adecuado. Esto es importante por varios motivos. La primera y más importante es que posiblemente no exista una cobertura de prueba adecuada en las etapas de prueba posteriores. Los costos de las pruebas también aumentan significativamente de etapa a etapa debido a la posibilidad de automatizar en etapas anteriores y a la creciente complejidad y experiencia requeridas posteriormente. El siguiente diagrama describe el espectro de prueba de Cisco IOS.



El primer paso es el desarrollo del software. Cisco se esfuerza por mejorar la calidad inicial del software en este ámbito. Los grupos de desarrollo también realizan revisiones de código o incluso varias revisiones de código para asegurarse de que otros desarrolladores aprueban cambios de software o nuevo código de característica.

La próxima etapa es la prueba de unidad. Las pruebas unitarias utilizan herramientas que examinan la interacción del software sin el uso de un laboratorio. DevTest son pruebas de laboratorio que incluyen pruebas de función/funcionalidad y pruebas de regresión. Las pruebas de funciones/funcionalidades están diseñadas para examinar la funcionalidad de una función determinada. Esto incluye la configuración, la desconfiguración y la prueba de todas las combinaciones de características, tal como está definido en la especificación de las características. La prueba de regresión se realiza en un recurso para pruebas automatizado diseñado para validar la funcionalidad y el comportamiento de funciones de manera continua. Las pruebas se centran principalmente en el ruteo, la conmutación y la funcionalidad de las características en diferentes topologías de red mediante el uso de pings y la generación limitada de tráfico. Las pruebas de regresión sólo se realizan en una combinación limitada de funciones, plataformas, versiones de software y topologías debido al gran número de posibles permutaciones, sin embargo, en la actualidad se utilizan más de 4000 scripts de prueba de regresión. Las pruebas de integración se han diseñado para ampliar las capacidades de prueba de laboratorio a fin de ofrecer un conjunto más completo de productos e interoperabilidad. Las pruebas de integración también aumentan la cobertura del código de prueba al ampliar las pruebas para incluir pruebas de interoperabilidad, pruebas de resistencia y rendimiento, pruebas del sistema y pruebas negativas (pruebas de eventos inesperados).

La próxima fase de laboratorio ofrece una prueba de extremo a extremo para los entornos comunes de cliente. Estos se muestran en el diagrama anterior como Laboratorio de pruebas financieras (FTL) y NSITE, Prueba de escenarios de clientes. FTL se creó para proporcionar pruebas a la comunidad financiera crítica. NSITE es un grupo que proporciona pruebas más exhaustivas para diferentes tecnologías de Cisco IOS. Los laboratorios NSITE y FTL se concentran en áreas como la comprobación de escalabilidad y rendimiento, capacidad de actualización, disponibilidad y resiliencia, interoperabilidad y capacidad de servicio. La facilidad de mantenimiento se centra en los problemas de aprovisionamiento masivo, la gestión/correlación de eventos y la resolución de problemas bajo carga. Existen otros laboratorios dentro de Cisco para diferentes mercados verticales que ayudan a probar estas áreas.

El último laboratorio que se muestra en el diagrama de arriba está identificado como el laboratorio del cliente. Las pruebas realizadas por los clientes son una extensión del esfuerzo de calidad y se recomiendan para los entornos de alta disponibilidad a fin de garantizar que la combinación exacta de características, configuración, plataformas, módulos y topología se haya probado completamente. Una cobertura de evaluación adecuada debería incluir el rendimiento y la escalabilidad de la red en la topología identificada, pruebas de aplicaciones específicas, pruebas negativa en la configuración identificada, pruebas de interoperabilidad para dispositivos que no son de Cisco y pruebas automatizadas, completas y continuas.

Software MTBF

Una de las métricas más comunes de fiabilidad general es el tiempo medio entre fallos (MTBF). MTBF para la confiabilidad del software es útil debido a las capacidades de análisis que se han desarrollado para la confiabilidad del hardware usando MTBF. La fiabilidad del hardware se puede determinar con mayor precisión utilizando algunos estándares existentes. Cisco utiliza el método de recuento de piezas basado en los datos estándar de MTBF de Telcordia Technologies. Sin embargo, el software del MTBF no cuenta con metodologías de análisis correspondientes y debe basarse en la medición sobre el terreno para el análisis del MTBF.

Durante los últimos tres años, Cisco ha realizado mediciones de campo de confiabilidad de software para la red de TI interna de Cisco y este trabajo se documenta en Cisco. El trabajo se basa en las caídas del sistema forzadas por software en los dispositivos con IOS de Cisco, que pueden ser medidas utilizando la información de trampas de SNMP de administración de red y la información de tiempo de actividad. El estudio identifica la confiabilidad del software utilizando un modelo de distribución normal estadística para las versiones de software identificadas. El tiempo medio de reparación (MTTR) de fallos de software se basa en los tiempos medios de reinicio y recuperación del router. Se utiliza un tiempo de recuperación de seis minutos para entornos empresariales y de quince minutos para proveedores de servicios de Internet (ISP) de mayor tamaño. El resultado de este estudio en curso es que el software generalmente cumple con la disponibilidad de líneas finas cuando se lanza o después de unas pocas versiones de mantenimiento, y es aún más alto con el tiempo, como se mide utilizando caídas forzadas por software como la única fuente de tiempo de inactividad. El estudio identificó los valores MTBF potenciales como un intervalo entre 5,000 horas para el software de liberación temprana y 50,000 horas para el software de liberación general.

La refutación más común de este trabajo es que las caídas forzadas por el software no incluyen todas las instancias de interrupciones que tienen lugar debido a problemas de confiabilidad del software. Si esta métrica se utiliza en esfuerzos de mejora de la calidad, puede ayudar a mejorar la tasa de caídas forzadas por software pero puede ignorar otras áreas críticas de confiabilidad de software. Este comentario permanece sin respuesta debido a la dificultad de predecir con exactitud la confiabilidad del software utilizando una metodología de estadística. Los estadísticos de calidad del software de Cisco han concluido que se necesitaría un conjunto más amplio de datos precisos para predecir de forma fiable el MTBF del software utilizando una gama más amplia de tipos de interrupciones. Además, el análisis estadístico teórico sería difícil debido a variables como la complejidad de la red, la experiencia del personal para resolver problemas relacionados con el software, el diseño de la red, las funciones habilitadas y los procesos de administración de software.

En este momento, no se ha completado ningún trabajo del sector para predecir con mayor precisión la fiabilidad del software con mediciones sobre el terreno debido a la dificultad de recopilar con precisión este tipo de datos confidenciales. Además, la mayoría de los clientes no desean que Cisco recopile información de disponibilidad directamente desde su red debido a la

naturaleza propietaria de los datos de disponibilidad. Sin embargo, algunas organizaciones recopilan datos sobre la fiabilidad del software y Cisco anima a las organizaciones a recopilar métricas sobre la disponibilidad debido a las interrupciones del software y a realizar análisis de las causas principales de dichas interrupciones. Algunas organizaciones con mayor confiabilidad de software han usado esta actitud proactiva para mejorar la confiabilidad del software mediante una cantidad de prácticas que pueden controlar.

Suposiciones acerca de la confiabilidad del software

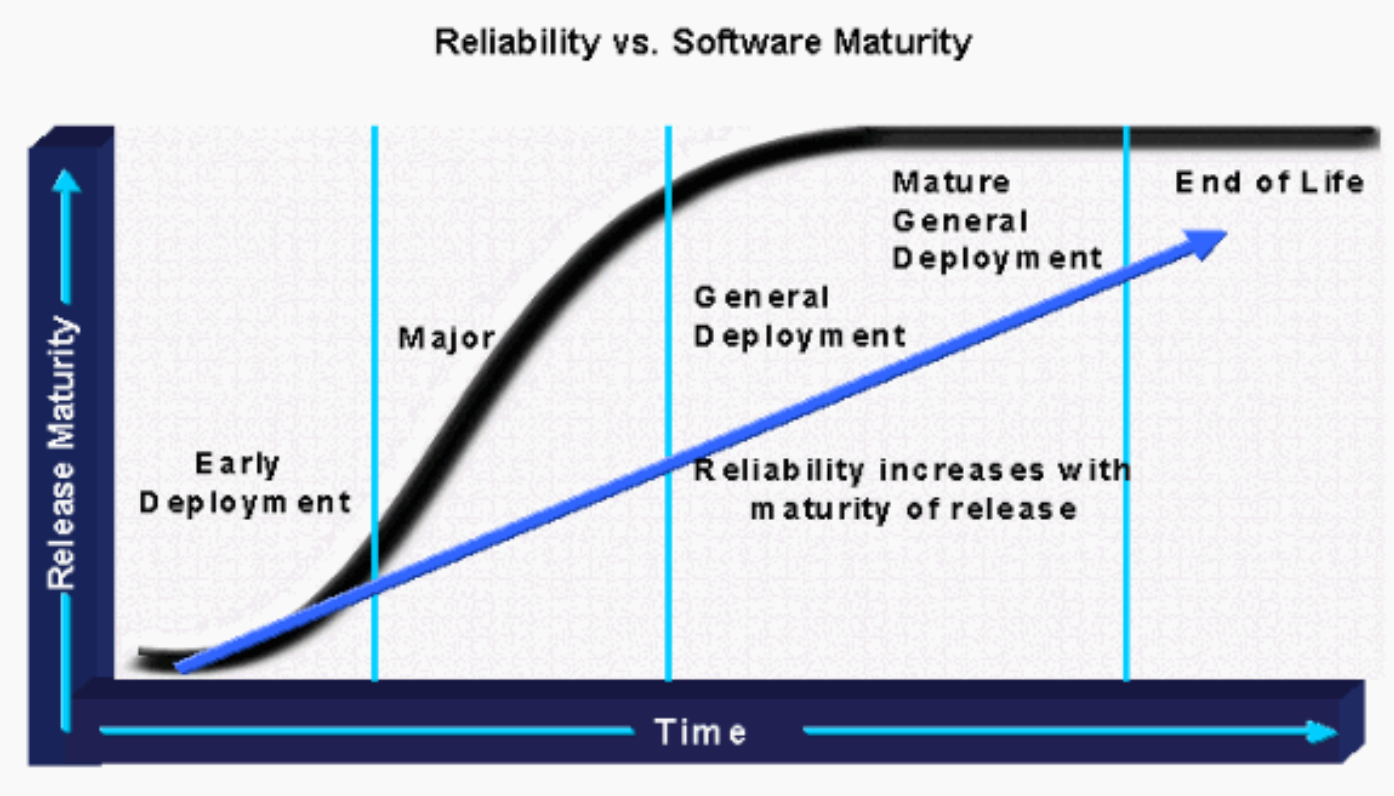
Como resultado de los comentarios de los clientes, los estudios proactivos realizados por el grupo Cisco IOS Technologies y el análisis de las causas principales realizado por el equipo de Cisco Advanced Services, se han formado algunas suposiciones y prácticas recomendadas nuevas que ayudan a mejorar la fiabilidad del software. Estas suposiciones se centran en las responsabilidades de prueba, la madurez o edad del software, las características habilitadas, y la cantidad de versiones del software desplegadas.

Responsabilidad de las pruebas

La primera nueva suposición se refiere a la responsabilidad de pruebas. Cisco es siempre responsable de probar/validar nuevas funciones y funcionalidades para asegurarse de que funcionan en nuevos productos. Cisco también se encarga de las pruebas de regresión para garantizar que las nuevas versiones de software sean compatibles con versiones anteriores. Sin embargo, Cisco no puede validar todas las funciones, la topología y la plataforma con cada advertencia potencial que un entorno de cliente pueda aplicar (idiosincrasias de diseño, cargas y perfiles de tráfico). Entre las prácticas recomendadas de alta disponibilidad para los clientes se incluyen las pruebas en una topología de laboratorio colapsada que imita la red de producción mediante funciones definidas por el cliente, diseño, servicios y tráfico de aplicaciones.

Confiabilidad vs. Madurez del software

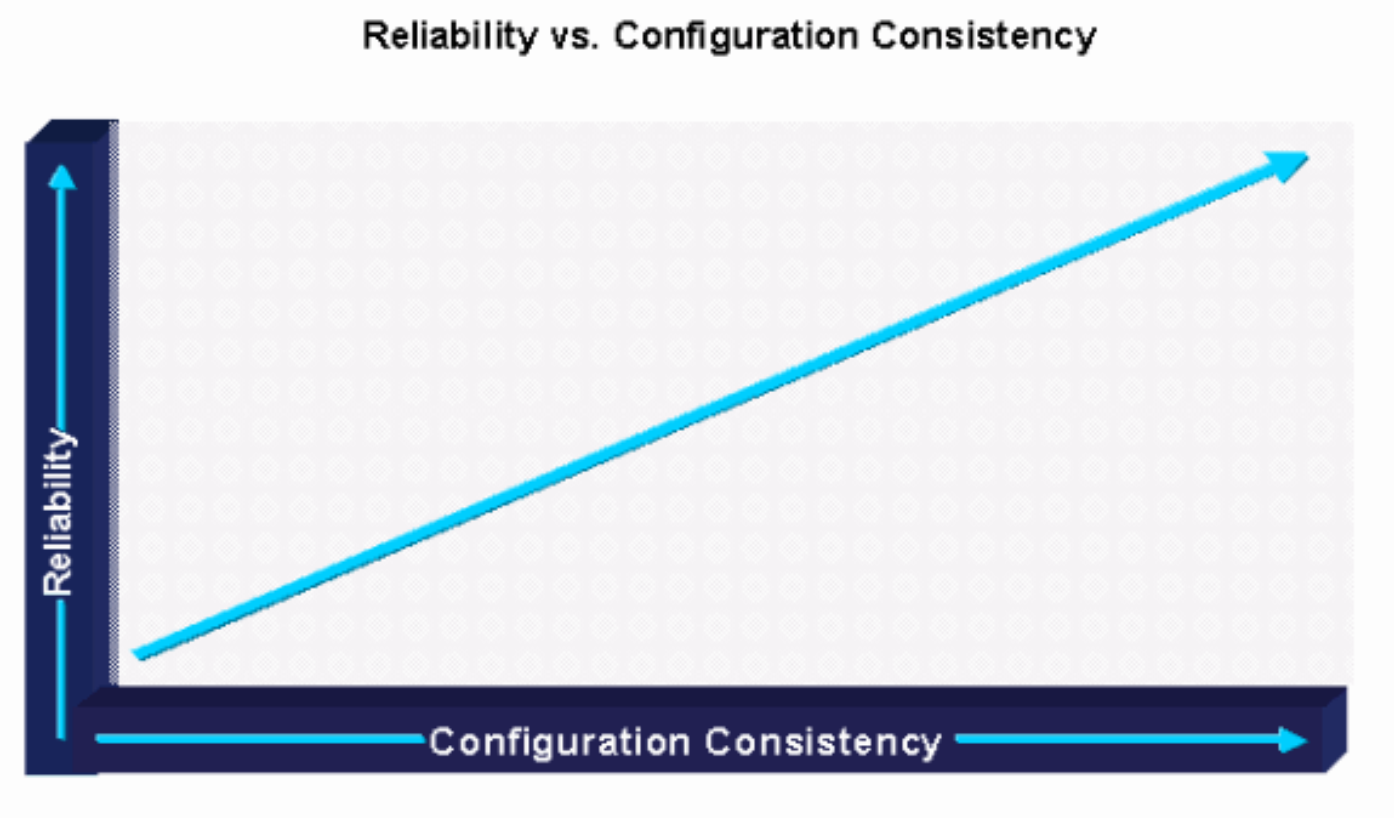
La confiabilidad del software es principalmente un factor de la madurez del software. El software madura a medida que se expone (con el uso) y se corrigen los errores de funcionamiento identificados. Las operaciones de lanzamiento de Cisco han pasado a una arquitectura de lanzamiento de tren para garantizar que el software madura sin que se añadan nuevas funciones. Los clientes que requieren una alta disponibilidad buscan un software más maduro con las funciones que necesitan ahora. A continuación, existe una compensación entre la madurez del software, los requisitos de disponibilidad y los impulsores empresariales de las nuevas funciones o funcionalidades. Muchas organizaciones cuentan con normas o directrices para lograr una madurez aceptable. Algunas sólo aceptan la quinta versión provisoria de un tren determinado. Para otros, puede ser la novena certificación o la certificación GD. En última instancia, la organización debe decidir sus niveles aceptables de riesgo en términos de madurez de software.



Confiabilidad vs. cantidad de características y estándares

La confiabilidad del software también es un factor de la cantidad de código que se prueba y se ejerce en un entorno de producción. A medida que aumenta la cantidad de diferentes plataformas y módulos de hardware, también aumenta la cantidad de código ejercida, lo que generalmente aumenta la exposición a defectos de software. Se puede decir lo mismo sobre la cantidad de protocolos configurados, la variedad de configuraciones e incluso la variedad de topologías o diseños implementados. Los factores de diseño, configuración, protocolos y módulos de hardware pueden contribuir a la cantidad de código que se ejerce y al aumento del riesgo o exposición a defectos de software.

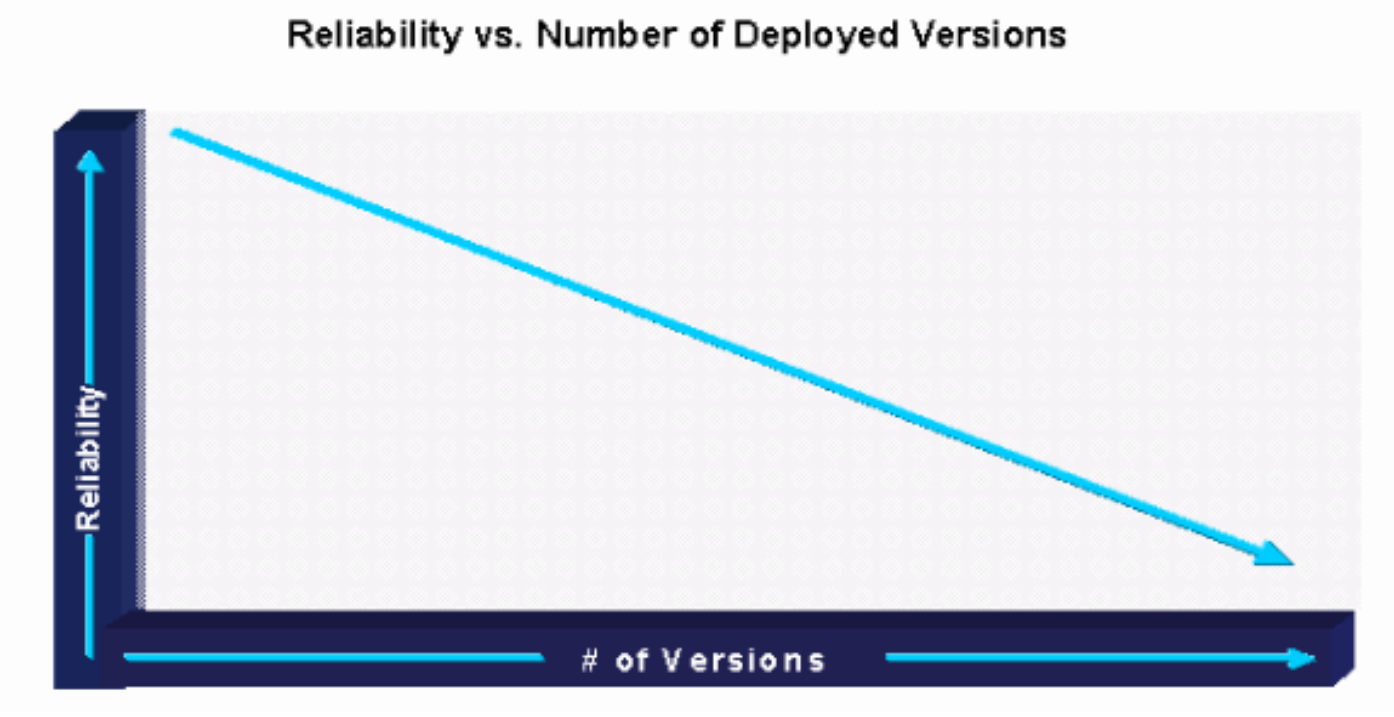
Las operaciones de versión de software ahora tienen un software específico que generalmente limita el código disponible en un área en particular. Las unidades empresariales han recomendado diseños y configuraciones que se han probado más a fondo en Cisco y que los clientes utilizan más ampliamente. Los clientes también han comenzado a adoptar las mejores prácticas para topologías modulares estandarizadas y configuraciones estándar para reducir la cantidad de exposición a código no probado y mejorar la fiabilidad general del software. Algunas redes de disponibilidad alta tienen pautas de configuración estándar estrictas, estándares de topología modular y control de versión de software que ayudan a reducir el riesgo de exposición al código no probado.



Confiabilidad vs. Cantidad de versiones desplegadas

Otro factor de confiabilidad del software es la interoperabilidad entre las versiones y la mera cantidad de código que se ejerce con múltiples versiones. A medida que aumenta la cantidad de versiones de software, también aumenta la cantidad de código ejercida, lo que aumenta la exposición a defectos de software. El riesgo para la confiabilidad se incrementa casi exponencialmente debido al código adicional que se utiliza con versiones múltiples. Ahora se reconoce que las organizaciones necesitan ejecutar al menos un puñado de versiones en la red para cubrir los requisitos específicos de la plataforma y las funciones. Sin embargo, la ejecución de alrededor de cincuenta versiones en un ambiente de red mayormente homogéneo, es normalmente una indicación de que existen problemas de software debido a la incapacidad de analizar o validar correctamente tantas versiones.

Para mejorar la fiabilidad del software, el desarrollo de Cisco realiza pruebas de regresión de software para asegurarse de que las diferentes versiones de software sean compatibles. Además, el código de software es más modular y los módulos principales tienen menos probabilidades de cambiar significativamente entre las versiones con el tiempo. Las operaciones de la versión de Cisco también han cambiado la cantidad de software disponible para los clientes, ya que las versiones con defectos conocidos o problemas de interoperabilidad se eliminan rápidamente de CCO a medida que se detectan defectos.



Información Relacionada

- Sistemas operativos de interconexión de redes (IOS) de Cisco
- Soporte Técnico y Documentación - Cisco Systems