Práticas principais da Cisco: operações de gerenciamento do Cisco IOS

Contents

Resumo

As práticas principais da Cisco são um conjunto de documentos codificados que fornecem orientação relevante e confiável sobre operações de rede para produtos e soluções da Cisco. As práticas principais são desenvolvidas e apoiadas pelos premiados engenheiros do Cisco TAC e Advanced Services, que você pode usar para ajudar a criar seu próprio conjunto de práticas principais para emular. Os clientes da Cisco aplicaram essas práticas recomendadas em seu ambiente de rede para obter desempenho e disponibilidade de rede.

É altamente recomendável complementar essas práticas principais com serviços da Cisco e de seus parceiros. Para obter mais informações sobre como otimizar o desempenho e a disponibilidade de sua rede, entre em contato com seu representante de vendas de serviços sobre o site Cisco Advanced Services e obtenha mais informações sobre o Network Otimization

Support - Focused Engineering Support, Network Availability Improvement Support (NAIS), Software Management Process Assessment (SMPA) e a implementação NAIS-SMPA.

Introdução

Overview

Os processos operacionais relacionados ao gerenciamento de software podem ajudar a reduzir a complexidade da rede, diminuir os problemas de suporte reativo e melhorar o tempo de resolução de problemas. Este documento fornece uma estratégia, recomendações de ferramentas e melhores práticas para o gerenciamento geral do software Cisco IOS® (Cisco IOS).

As seções Criando uma Estratégia de Operações de Gerenciamento do Cisco IOS e Seguindo uma Prática Recomendada do Processo de Operações de Gerenciamento do Cisco IOS neste documento discutem a metodologia recomendada para começar e listam as melhores ferramentas a serem usadas para a fase de operações. A fase de operações inclui os processos de práticas recomendadas para o seguinte:

Processo	Descrição
Controle de versão de software	Rastreamento, validação e melhoria da consistência de software dentro dos "controles" de software identificados.
Gerenciamento de falhas	Monitorar proativamente e agir sobre mensagens SNMP e Syslog de maior prioridade geradas pelo Cisco IOS.
Gerenciamento de problemas	Coleta rápida e eficiente de informações sobre problemas críticos relacionados a software para ajudar a evitar futuras ocorrências.
Padronização da configuração	"Padronização" de configurações para reduzir a possibilidade de código não testado ser utilizado na produção e para padronizar o comportamento de recursos e protocolos de rede.
Gerenciamento de disponibilidade	Melhorar a disponibilidade com base em métricas, metas de melhoria e projetos de melhoria

Este documento pressupõe que você tenha implementado os seguintes processos de melhores práticas para o planejamento, o projeto e a implementação do Cisco IOS:

- Áreas de software gerenciáveis identificadas (rastreamentos de software) em seu ambiente com base nos requisitos de plataforma, módulo, recurso, protocolo e topologia.

- Versões selecionadas, certificadas e comunicadas do Cisco IOS por controles de software.
- Implementou consistentemente as versões padrão do Cisco IOS em cada um dos controles de software.

Objetivos

Esta seção o ajuda a gerenciar e manter versões padronizadas do Cisco IOS dentro de faixas definidas. Você aprenderá a:

- Desenvolva um processo de controle de versão de software para garantir a consistência da versão do software nos controles de software identificados.
- Monitore, notifique e resolva processos baseados em mensagens e alertas de gerenciamento de falhas de dispositivos (SNMP/Syslog) para ajudar a resolver proativamente possíveis problemas de software e falhas.
- Coleta eficiente de informações de problemas críticos para o software para ajudar a reduzir o tempo de resolução de problemas relacionados ao software.
- Padronize as configurações do dispositivo para ajudar a garantir a consistência de protocolo, recurso, acesso e segurança para o ambiente.

Público-alvo

Este documento é apropriado para indivíduos e gerentes com orientação técnica que são responsáveis pela operação diária da rede. O documento descreve como estabelecer processos operacionais para ajudá-lo a reduzir a complexidade da rede, diminuir problemas de suporte reativo e melhorar o tempo de resolução de problemas criando consistência de rede e melhorando os recursos para gerenciamento pró-ativo de falhas.

Pré-requisitos

Os envolvidos nas operações de gerenciamento do Cisco IOS devem ter um sólido conhecimento de projeto e administração de infraestrutura de rede, particularmente com equipamentos da Cisco, e devem ter acesso a detalhes da topologia da rede de destino, configuração de dispositivo, perfil de atividade, uso de aplicativo e política de utilização de recursos. O acesso e a experiência com as ferramentas de informação disponíveis no Cisco Connection Online (CCO) também são necessários. Se você ainda não se registrou no CCO, sugerimos que o faça para acessar as ferramentas descritas neste documento.

Criando uma estratégia de operações de gerenciamento do Cisco IOS

Existem muitas estratégias e ferramentas de qualidade para ajudar a gerenciar os ambientes Cisco IOS. Este capítulo concentra-se em três estratégias principais para gerenciar operações do Cisco IOS em ambientes de maior disponibilidade e inclui uma matriz de ferramentas

operacionais importantes que são especificamente úteis para gerenciar problemas do Cisco IOS e do Cisco IOS.

A primeira estratégia importante é manter o ambiente o mais simples possível, evitando ao máximo variações na configuração e nas versões do Cisco IOS. A certificação Cisco IOS já foi discutida, no entanto, a consistência da configuração é outra área importante. O grupo de arquitetura e engenharia deve ser responsável pela criação dos padrões de configuração. O grupo de implementação e operações tem a responsabilidade de configurar os padrões e mantê-los através do controle de versão do Cisco IOS e dos padrões/controles de configuração do Cisco IOS.

A segunda estratégia principal é a capacidade de identificar e resolver rapidamente falhas de rede. O grupo de operações geralmente deve identificar problemas de rede antes que os usuários os informem, e os problemas devem ser resolvidos o mais rápido possível sem causar impacto adicional ou alterar o ambiente. Duas práticas recomendadas importantes nessa área são o gerenciamento de problemas e o gerenciamento de falhas (ambos serão discutidos mais adiante neste documento).

Observação: a ferramenta de decodificador de pilha do Cisco IOS pode ser usada para ajudar a diagnosticar rapidamente falhas do software Cisco IOS.

A terceira estratégia principal é "melhorar consistentemente". O principal processo é melhorar um programa de melhoria de disponibilidade baseado em qualidade. Executando a análise de causa básica em todos os problemas, inclusive problemas relacionados ao Cisco IOS, uma organização pode melhorar a cobertura de testes, melhorar os tempos de resolução de problemas e melhorar processos que eliminarão ou reduzirão o impacto da paralisação. A organização também pode verificar problemas comuns e construir processos para resolvê-los com mais rapidez.

Identificando Produtos Finais

Os resultados do processo de operação do Cisco IOS Software Management incluem:

- Processos e ferramentas de controle de versão de software
- Monitoramento e processos de gerenciamento de falhas
- Processos de gerenciamento de problemas
- Padrões de configuração de dispositivos e processos de auditoria
- Metodologia de disponibilidade de rede, relatórios e processos de revisão

Identificação das principais medidas do dispositivo

As métricas devem ser definidas como parte do plano de operações e usadas para determinar se as ferramentas e os processos estão produzindo os resultados desejados. A seguir estão alguns exemplos de métricas úteis de gerenciamento do software Cisco IOS:

- Disponibilidade da rede (devido a problemas de software)

- % de conformidade da versão do Cisco IOS com o padrão (em uma base por trilha)
- % de consistência de configuração do dispositivo (com base em padrões)
- Métricas de gerenciamento de problemas (MTTR, número de tíquetes, códigos de encerramento)

Definindo Funções e Responsabilidades

Identifique, qualifique e monte um grupo multifuncional de gerentes e/ou leads dos grupos de arquitetura de rede, engenharia de rede e implementação/operações para ajudar a garantir o sucesso das fases de planejamento, projeto, implementação e operações de seus projetos de atualização do IOS.

Identificação das áreas de especialização necessárias

Montar um grupo multifuncional de gerentes e/ou leads dos grupos de gerenciamento, engenharia e implementação de rede e operações para ajudar na fase de operações do seu projeto de gerenciamento do Cisco IOS.

Identificando os principais contribuidores

- Gerente(s) de rede:

  Nome do(s) gerente(s), departamento, informações de contato

  Nome do backup principal, departamento, informações de contato

  Nome, departamento e informações de contato do backup secundário, se necessário
- Arquiteto(s) de rede:

  Nome do(s) arquiteto(s), departamento, informações de contato

  Nome do backup principal, departamento, informações de contato

  Nome, departamento e informações de contato do backup secundário, se necessário
- Engenheiro(s) de rede:

  Nome, departamento e informações de contato do(s) engenheiro(s)

  Nome do backup principal, departamento, informações de contato

  Nome, departamento e informações de contato do backup secundário, se necessário
- Engenheiro(s) de operações de rede (NOC):

  Nome, departamento e informações de contato do(s) engenheiro(s)

Nome do backup principal, departamento, informações de contato

Nome, departamento e informações de contato do backup secundário, se necessário

Identificação de responsabilidades

- Os gerentes de rede são responsáveis por:
    - Mantendo o plano do projeto
    - Atribuindo/reatribuindo recursos
    - Gerenciamento do controle de alterações
    - Gerenciando o progresso
    - Gerenciando relatórios orçamentários
- Os arquitetos de rede são responsáveis por:
    - Analisando padrões de rede e avisos de versão
    - Manutenção da matriz de atualização de software
    - Manutenção da Matriz de Gerenciamento de Candidatos
    - Manutenção da matriz de requisitos de memória
- Os engenheiros de rede (NOC) são responsáveis por:
    - Implementar e garantir a conformidade com os padrões de rede
    - Identificação de problemas de software e causas básicas
    - Recomendando ações corretivas
    - Monitorando a rede

Recursos de Orçamento

Os requisitos de recursos devem ser determinados na etapa de operações para oferecer suporte à estratégia de gerenciamento de software da organização. Isso incluirá o tempo de pessoal necessário e as despesas de capital necessárias para oferecer suporte à estratégia de software.

Em muitos casos, um retorno sobre o investimento (ROI) ou um plano orçamentário para práticas de gerenciamento de software pode ser gerado com base no custo do tempo de inatividade e nos requisitos de disponibilidade. Se a organização puder determinar o tempo de inatividade devido a problemas de software, a maior parte desse custo poderá ser compensada por meio das práticas recomendadas de gerenciamento de software identificadas. Se o custo não puder ser totalmente compensado, a organização deve considerar uma estratégia de gerenciamento de software mais

básica que ajude a melhorar a produtividade, evitando retrabalhos adicionais como resultado de problemas de software.

Seguindo uma prática recomendada do processo de operações de gerenciamento do Cisco IOS

As melhores práticas para seguir um processo de operações de gerenciamento do Cisco IOS incluem:

Prática recomendada	Detalhe
Controle de versão de software	Implementar apenas versões de software padronizadas e monitorar a rede para validar ou possivelmente alterar o software devido à conformidade com versões diferentes.
Gerenciamento de falhas	A coleta, o monitoramento e a análise de mensagens SNMP e Syslog são processos de gerenciamento de falhas recomendados para resolver mais problemas específicos da rede do Cisco IOS que sejam difíceis ou impossíveis de identificar de outra forma.
Gerenciamento de problemas	Processos detalhados de gerenciamento de problemas que definem a identificação de problemas, a coleta de informações e um caminho de solução bem analisado. Esses dados são usados para determinar a causa raiz.
Padronização da configuração	Os padrões de configuração representam a prática de criar e manter parâmetros de configuração "global" padrão em dispositivos e serviços semelhantes, resultando em consistência de configuração global em toda a empresa.
Gerenciamento de disponibilidade	Melhoria de qualidade usando a disponibilidade da rede como métrica de melhoria de qualidade.

Controle de versão de software

O controle da versão do software é o processo de implementação apenas das versões de software padronizadas e de monitoramento da rede para validar ou possivelmente alterar o software devido à compatibilidade de não versão. Em geral, o controle de versão de software é realizado por meio de um processo de certificação e controle de padrões. Muitas organizações publicam padrões de versão em um servidor Web central. Além disso, uma equipe de implementação é treinada para revisar qual versão está sendo executada e para atualizar a versão se ela não estiver em conformidade com os padrões. Algumas organizações têm um processo de portal de qualidade, em que a validação secundária é concluída por meio de auditorias para garantir que o padrão seja seguido durante a implementação.

Durante a operação da rede, também é comum ver versões de software não padrão na rede, especialmente se a rede é grande com uma grande equipe de operações. Isso pode ocorrer devido a um dos seguintes motivos:

- Equipe mais nova e sem treinamento
- Comandos de inicialização configurados incorretamente
- Implementações não verificadas

Recomenda-se validar periodicamente os padrões de versão de software usando ferramentas como o CiscoWorks2000 Resource Manager Essentials (RME) que pode classificar todos os dispositivos pela versão do Cisco IOS. Quando uma versão não padrão é identificada, ela deve ser imediatamente sinalizada e um ticket de problema ou ticket de alteração deve ser iniciado para trazer a versão ao padrão identificado.

Ferramentas disponíveis

O gerenciador de inventário do CiscoWorks2000 RME simplifica muito o gerenciamento da versão do Cisco IOS de roteadores e switches da Cisco através de ferramentas de relatório baseadas na Web que relatam e classificam dispositivos com base na versão do software, plataforma do dispositivo e nome do dispositivo.

Gerenciamento de falhas

O gerenciamento de falhas é o processo de coleta, monitoramento e análise de mensagens SNMP e Syslog para resolver mais problemas de rede específicos do Cisco IOS que sejam difíceis ou impossíveis de identificar de outra forma.

Coleção de interceptações SNMP

A coleta e a notificação de interceptação (trapping) SNMP é um processo básico no gerenciamento de falhas usado para identificar eventos de software ou hardware e/ou travamentos sem sobrecarga ou atraso de polling SNMP incorrido a partir de intervalos de polling. As mensagens de interceptação são geradas diretamente do dispositivo de rede para um sistema de gerenciamento de rede que fornece serviços de notificação. A coleta e a notificação dessas armadilhas são essenciais para a rápida resolução de muitos eventos de rede, incluindo eventos que não causam impacto no usuário, como a perda de dispositivos primários ou links em um

ambiente redundante.

Para coletar e monitorar essas armadilhas, as armadilhas devem ser configuradas corretamente no dispositivo, bem como nos sistemas de gerenciamento de rede. Os sistemas de gerenciamento de rede devem alertar o grupo de operações de rede quando uma interceptação (trap) for recebida. A notificação pode ocorrer na forma de paging, e-mail ou telas de eventos em um ambiente NOC.

Independentemente de como os dados são apresentados, essas instâncias de falha, ou exceções, devem ser analisadas e revisadas regularmente (de preferência diariamente) pelas operações de rede e/ou pela equipe de suporte da rede. As causas de todas as exceções encontradas devem ser investigadas. Algumas exceções registradas podem não ser críticas o suficiente para acionar imediatamente um alarme no Centro de Operações de Rede. A análise proativa, a investigação e a resolução de exceções menores podem ajudar os grupos de suporte a reduzir ou evitar interrupções da rede.

Coleção de Mensagens de Syslog

As mensagens de syslog são enviadas pelo dispositivo a um servidor de coleta. Essas mensagens podem ser erros de hardware ou software ou podem ser informativas (como quando alguém está em um terminal de configuração em um dispositivo).

O monitoramento de syslog requer suporte à ferramenta Network Management System (NMS) ou scripts para ajudar a analisar e relatar dados de Syslog. Isso inclui a capacidade de classificar mensagens de Syslog por data ou período, dispositivo, tipo de mensagem de Syslog ou frequência de mensagem. Em redes maiores, ferramentas ou scripts podem ser implementados para analisar dados de Syslog e enviar alertas ou notificações para sistemas de gerenciamento de eventos ou pessoal de operações e engenharia. Se os alertas para uma grande variedade de dados Syslog não forem usados, a organização deve revisar os dados Syslog de maior prioridade pelo menos diariamente e criar tickets de problemas para possíveis problemas. Para detectar proativamente problemas de rede que podem não ser vistos através do monitoramento normal, a revisão periódica e a análise de dados históricos de Syslog devem ser executadas para detectar situações que podem não indicar um problema imediato, mas podem fornecer uma indicação de um problema antes que ele se torne um impacto no serviço.

Ferramentas disponíveis

Algumas das ferramentas mais populares do receptor de interceptação SNMP incluem o seguinte:

- HP OpenView Network Node Manager da Hewlett Packard em openview.hp.com
- Integridade do espectro da Aprisma em www.aprisma.com
- NetView da IBM Tivoli em www.tivoli.com

A ferramenta de Syslog mais popular para o gerenciamento do Cisco IOS é o gerenciador de Syslog CiscoWorks2000 RME. Outras ferramentas disponíveis incluem SL4NT, um programa shareware de www.netal.com deixando cisco.com e Private I da OpenSystems em www.opensystems.com

Gerenciamento de problemas

O gerenciamento de problemas, um aspecto do gerenciamento de falhas, é a disciplina de gerenciar problemas desde o momento da ocorrência, através de identificação, solução de problemas, resolução e fechamento.

Muitos clientes passam por períodos de inatividade adicionais devido à falta de processos no gerenciamento de problemas. Um tempo de inatividade adicional pode ocorrer quando os administradores de rede tentam resolver o problema rapidamente usando uma combinação de comandos com impacto no serviço ou alterações de configuração, em vez de gastar tempo na identificação de problemas, coleta de informações e um caminho de solução bem analisado. O comportamento observado nessa área inclui a recarga de dispositivos ou a limpeza de tabelas de roteamento IP antes de investigar um problema e sua causa raiz. Em alguns casos, isso ocorre devido a metas de solução de problemas de suporte de primeiro nível. A meta, em todos os problemas relacionados a software, deve ser coletar rapidamente as informações necessárias para a análise da causa principal antes de restaurar a conectividade ou o serviço.

Recomenda-se um processo de gerenciamento de problemas que deve incluir um certo grau de descrições padrão dos problemas e coletas de comandos "show" apropriadas antes de encaminhar o problema para um segundo nível de suporte. O suporte de primeiro nível nunca deve incluir a limpeza de rotas ou o recarregamento de dispositivos. O ideal é que a organização de suporte de primeiro nível colete informações rapidamente e depois transfira o problema para o suporte de segundo nível. Gastando um pouco mais de tempo identificando e descrevendo o problema no suporte de nível um, uma descoberta da causa básica é muito mais provável, permitindo assim uma solução alternativa, identificação de laboratório e relatórios de erros. O suporte de segundo nível deve ser bem versado nos tipos de informações que a Cisco pode precisar para diagnosticar um problema ou arquivar um relatório de erros, incluindo:

- Despejos de memória
- Saída de informações de roteamento
- Saída do comando show do dispositivo

Padronização da configuração

Os padrões de configuração de dispositivos globais representam a prática de manter parâmetros de configuração "globais" padrão em dispositivos e serviços semelhantes, resultando em consistência de configuração global em toda a empresa. Os comandos de configuração global são comandos que se aplicam a todo o dispositivo e não a portas, protocolos ou interfaces individuais, e geralmente afetam o acesso ao dispositivo, o comportamento geral do dispositivo e a segurança do dispositivo. No Cisco IOS, isso inclui os seguintes comandos:

- Serviço
- IP
- VTY

- Porta de Console
- Registro
- AAA/TACACS+
- SNMP
- Banner

Também importante nos padrões de configuração de dispositivos globais é uma convenção de nomenclatura de dispositivos apropriada que permite que os administradores identifiquem o dispositivo, o tipo de dispositivo e a localização do dispositivo com base no nome DNS do dispositivo. A consistência da configuração global é importante para a capacidade de suporte e confiabilidade geral de um ambiente de rede porque ajuda a reduzir a complexidade da rede e a melhorar a capacidade de suporte da rede. Geralmente, o usuário passa por problemas no suporte sem padronização de configuração, seja devido a um comportamento incorreto ou indevido do dispositivo, ao acesso SNMP ou, ainda, devido à segurança geral do dispositivo.

A manutenção dos padrões de configuração de dispositivos globais é normalmente realizada por um grupo interno de engenharia ou operações que cria e mantém parâmetros de configuração global para dispositivos de rede semelhantes. Também é uma boa prática fornecer uma cópia do arquivo de configuração global em diretórios TFTP para que eles possam ser inicialmente baixados para todos os dispositivos recentemente provisionados. Também é útil um arquivo acessível pela Web que fornece o arquivo de configuração padrão com uma explicação de cada parâmetro de configuração. Algumas organizações configuram todos os dispositivos semelhantes periodicamente para ajudar a garantir a consistência da configuração global ou revisam periodicamente os dispositivos para obter os padrões de configuração global corretos.

Os padrões de configuração de interface ou protocolo representam a prática de manter padrões para a configuração de interface e protocolo, o que melhora a disponibilidade da rede, reduzindo a complexidade da rede, fornecendo o comportamento esperado de dispositivo e protocolo e melhorando a capacidade de suporte da rede. A inconsistência na configuração da interface ou do protocolo pode resultar em comportamento inesperado do dispositivo, problemas de roteamento de tráfego, aumento dos problemas de conectividade e aumento do tempo de suporte reativo.

Os padrões de configuração de interface podem incluir:

- CDP (protocolo de descoberta da Cisco)
- Descritores de interface
- Configuração de cache
- Outros padrões específicos de protocolo

Os padrões de configuração específicos do protocolo podem incluir:

- Configuração de roteamento IP
- configuração de DLSW
- Configuração da lista de acesso
- configuração de ATM
- Configuração do Frame Relay
- Configuração do Spanning Tree
- Atribuição e configuração de VLAN
- VTP (Virtual Trunking Protocol, protocolo de entroncamento virtual)
- HSRP (Hot Standby Routing Protocol, Protocolo de roteamento de hot standby)
- Outros, dependendo do que está configurado na rede

Um exemplo de padrões IP pode incluir o tamanho da sub-rede, o espaço de endereço IP usado, o protocolo de roteamento usado e a configuração do protocolo de roteamento.

Manter os padrões de configuração de protocolo e interface é normalmente responsabilidade dos grupos de implementação e engenharia de rede. O grupo de engenharia deve ser responsável por identificar, testar, validar e documentar os padrões. O grupo de implementação é responsável por usar os documentos de engenharia ou modelos de configuração para provisionar novos serviços. O grupo de engenharia deve criar documentação sobre todos os aspectos dos padrões exigidos para garantir consistência. Os modelos de configuração também devem ser criados para ajudar a aplicar os padrões de configuração. Os grupos de operação também devem receber treinamento sobre os padrões e devem ser capazes de identificar problemas de configurações que não sejam padrão. A consistência da configuração é de grande ajuda na fase de teste, validação e certificação. Sem modelos de configuração padronizados, é quase impossível testar, validar ou certificar adequadamente uma versão do Cisco IOS para uma rede moderadamente grande.

Gerenciamento de disponibilidade

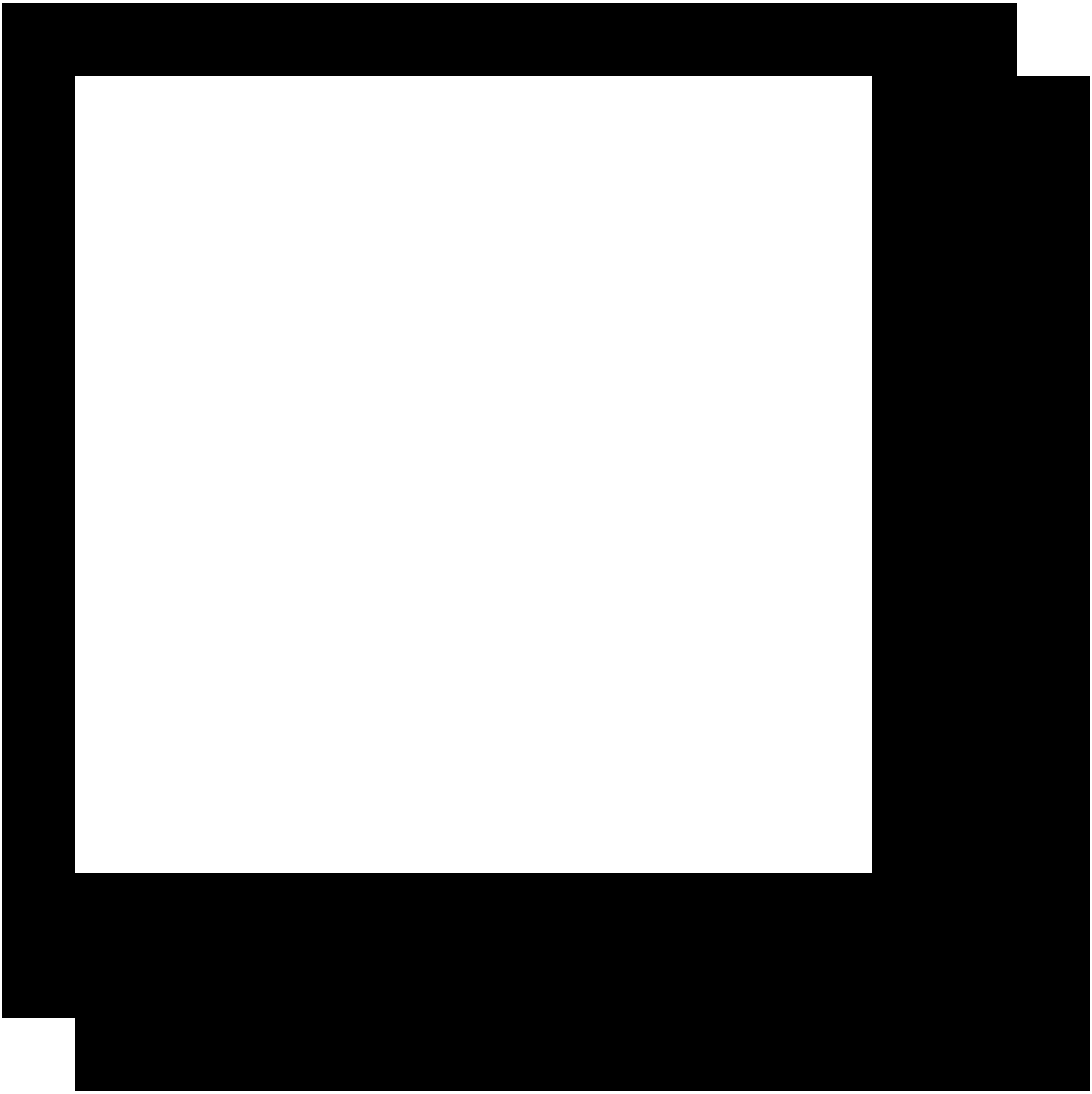
O gerenciamento de disponibilidade é o processo de melhoria de qualidade usando a disponibilidade da rede como métrica de melhoria de qualidade. Muitas empresas estão medindo a disponibilidade e o tipo de paralisação. Os tipos de interrupção podem incluir o seguinte:

- Hardware
- Software
- Link/operadora
- Energia/ambiente

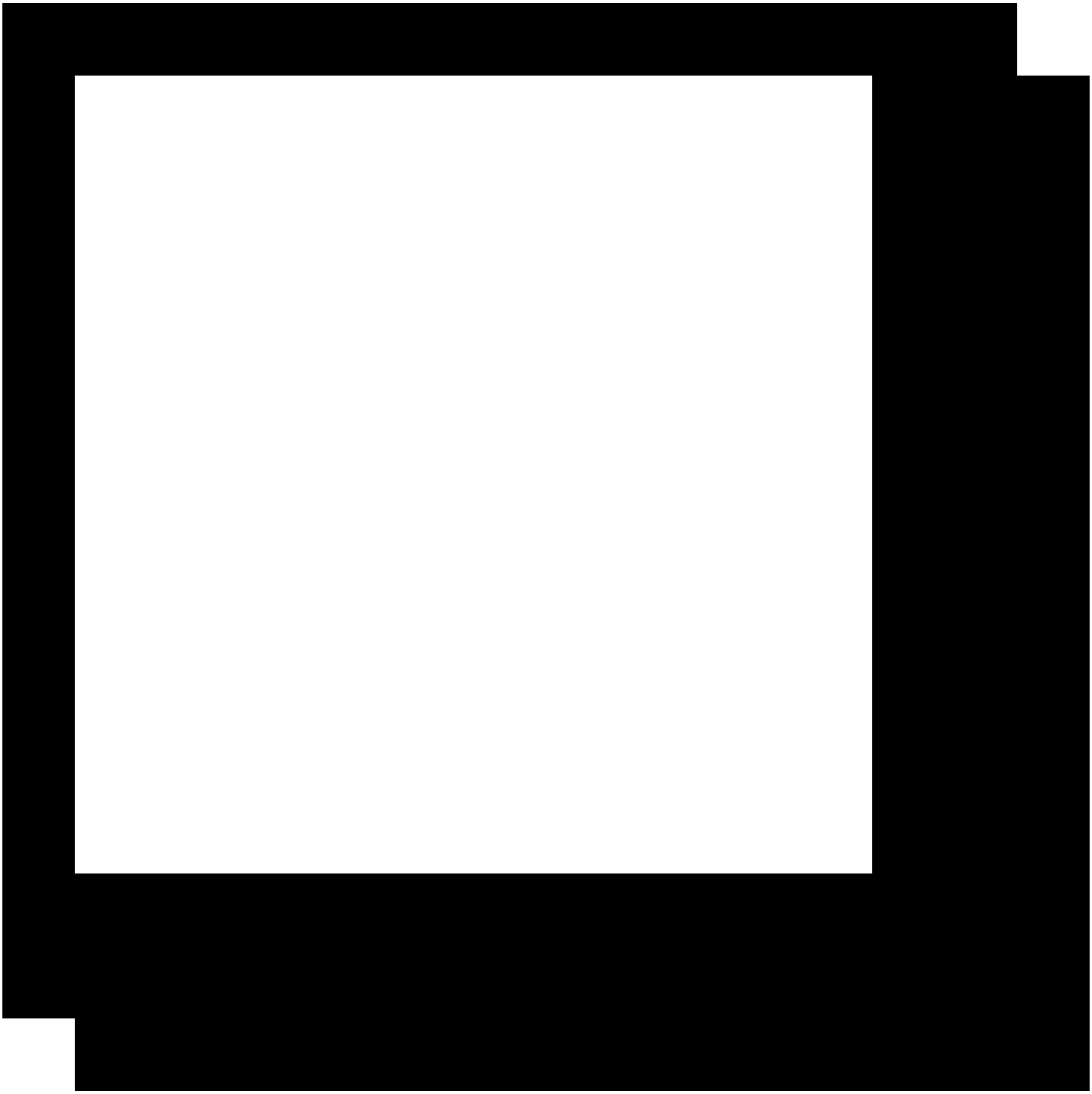
- Projeto
- Erro de usuário/processo

Ao identificar paralisações e executar a análise de causa básica imediatamente após a recuperação, a organização pode identificar métodos para melhorar a disponibilidade. Quase todas as redes que alcançaram alta disponibilidade têm algum tipo de processo de melhoria de qualidade em vigor.

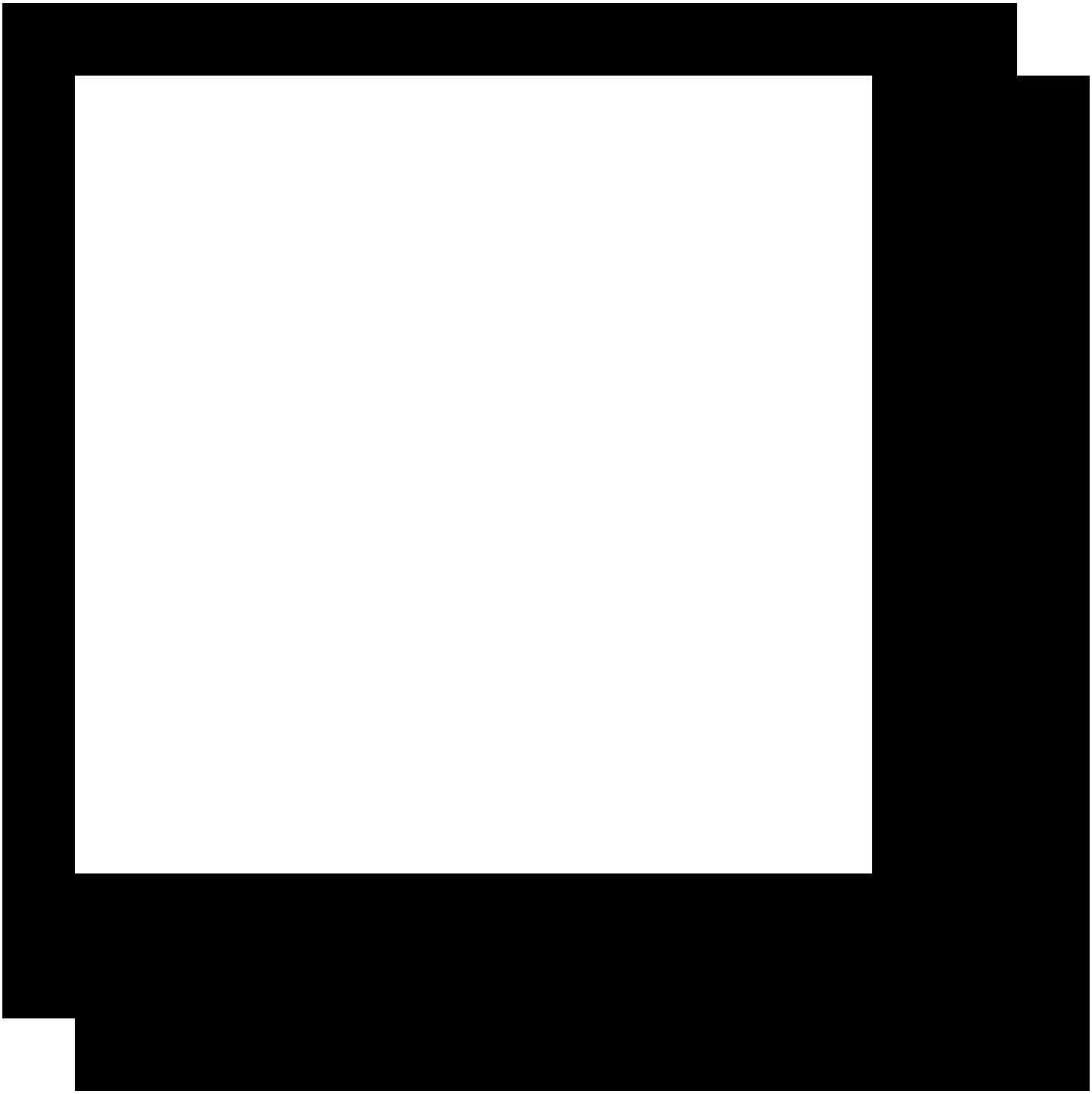
Lista de verificação de operações de gerenciamento do Cisco IOS



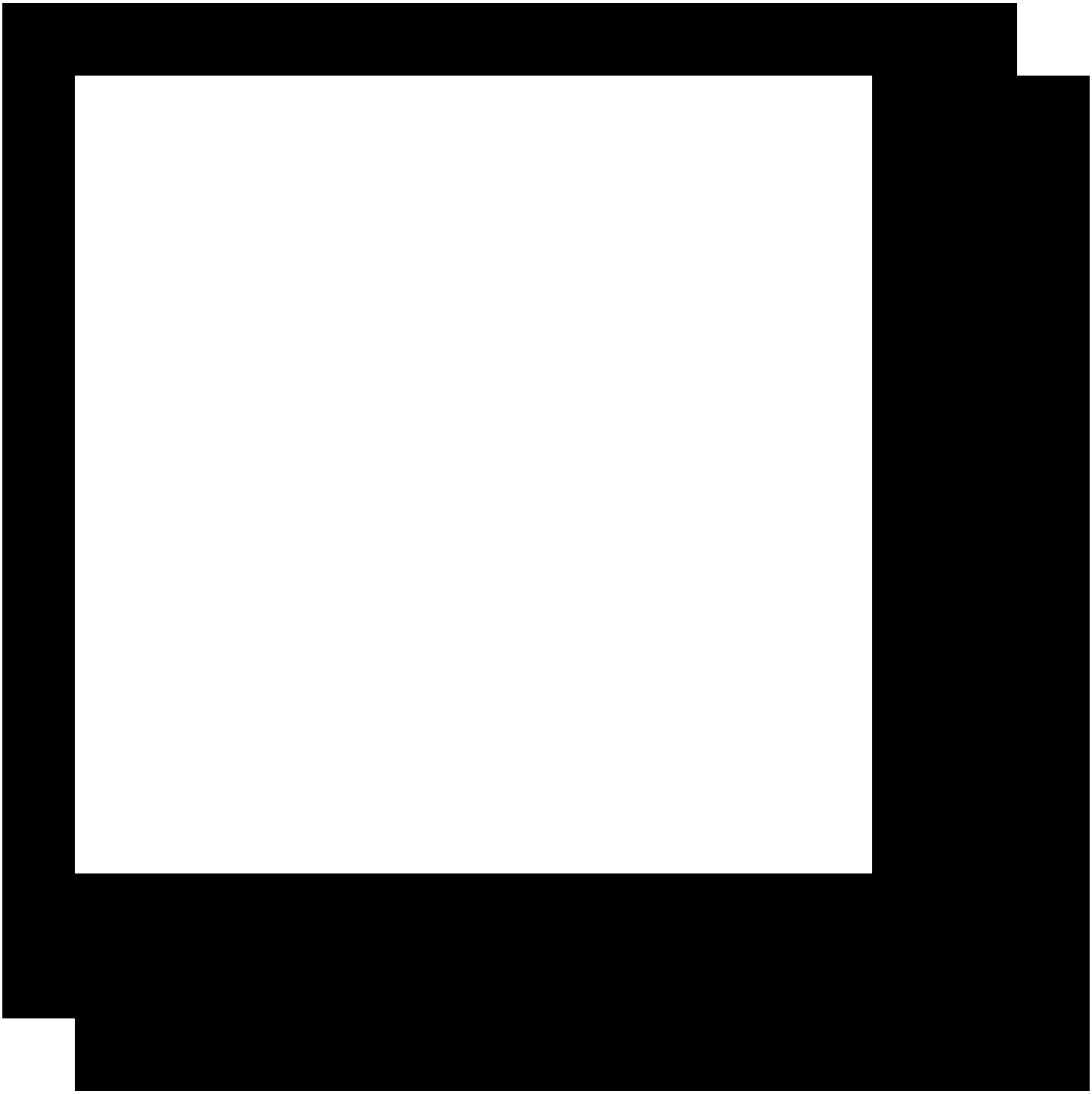
Passo 1: Definir objetivos e requisitos comerciais (somente clientes registrados)



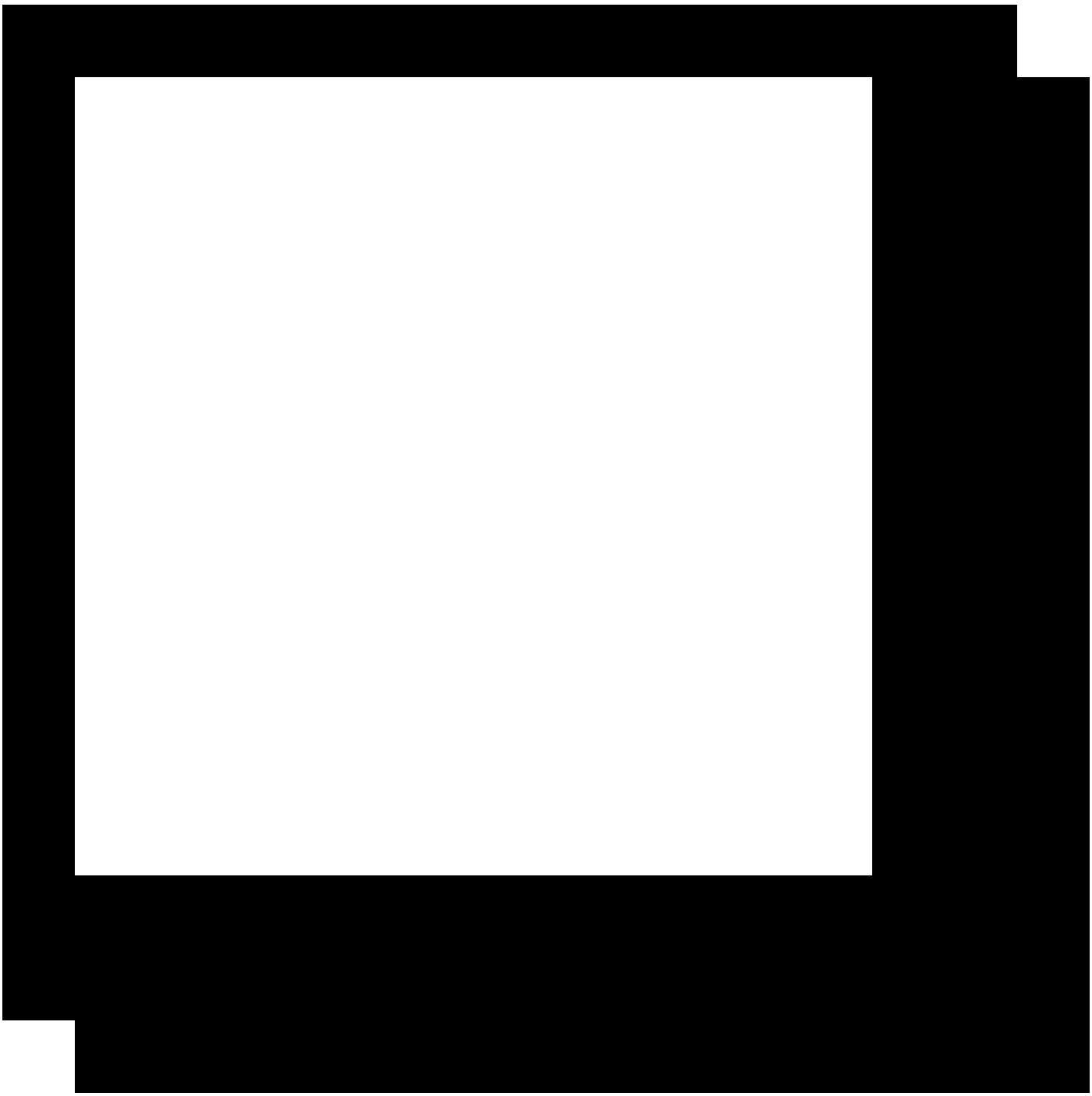
Passo 2: Avaliar o status atual das práticas de gerenciamento do software Cisco IOS (somente clientes registrados)



Passo 3: Definir funções e responsabilidades (somente clientes registrados)



Etapa 4: Desenvolver um plano de projeto de gerenciamento de software (somente clientes registrados)



Etapa 5: Desenvolver uma Matriz de Requisitos de Software (somente clientes registrados)

Informações Relacionadas

Um apêndice foi criado para ajudar o cliente a obter outras informações valiosas relacionadas ao Cisco IOS, como: fundamentos do Cisco IOS, processos internos do Cisco IOS Software, análise de confiabilidade do software, programa de qualidade interna da Cisco, metodologias de teste interno da Cisco e uma análise de campo que mostra as práticas atuais do setor e as experiências gerais do cliente com o software Cisco IOS

- Cisco IOS Management: informações adicionais sobre o gerenciamento do Cisco IOS e as

práticas recomendadas podem ser encontradas no white paper "Cisco IOS Management for High Availability Networking" no seguinte site: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml

- Para obter informações específicas sobre como executar testadores de rede, que comandos CLI usar, como analisar e interpretar dados de tráfego de rede e como estabelecer políticas de uso de aplicativos, visite http://www.cisco.com. Este site oferece uma ampla variedade de soluções de suporte, treinamento, referência técnica e consultoria.
- O Cisco IOS tem convenções de nomenclatura específicas definidas aqui: http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.s
- As informações sobre a disponibilidade da versão do Cisco IOS são fornecidas aqui: http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- As versões do Cisco IOS são removidas do CCO e não podem mais ser solicitadas. Certifique-se de definir as expectativas do cliente de acordo.
- Os boletins do produto Cisco IOS são usados para anunciar as versões do Cisco IOS aos clientes. Eles contêm informações breves sobre o conteúdo da versão. Verifique aqui a disponibilidade de novas versões do Cisco IOS http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- A equipe de resposta a incidentes de segurança do produto lida com a segurança dos produtos da Cisco. Quaisquer problemas relacionados à segurança do Cisco IOS devem ser encaminhados a este grupo. A Cisco publica publicamente suas vulnerabilidades de segurança. http://tools.cisco.com/security/center/publicationListing
- Defeitos do Cisco IOS: Defeitos graves do Cisco IOS devem ser recomendados para adiamento. Qualquer funcionário da Cisco pode fazer a recomendação.
- Os problemas de campo no Cisco IOS são comunicados aos clientes através de avisos do Cisco IOS. http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Recursos do Cisco IOS: a ferramenta Feature Navigator permite que os clientes encontrem versões que suportem recursos específicos e vice-versa. http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
- O Cisco Software Advisor permite que os clientes encontrem suporte de software para recursos ou suporte de software para hardware. http://tools.cisco.com/Support/Fusion/FusionHome.do (somente clientes registrados)

Serviços e suporte da Cisco

- Serviços de suporte técnico
- Serviços específicos para tecnologias e soluções de rede da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.