Entender os comandos ping estendido e traceroute estendido

Contents

Introdução

Este documento descreve como usar os traceroute comandos extendedpinge extended.

Pré-requisitos

Requisitos

Este documento requer conhecimento prévio dos comandospinge traceroute comandos.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS® Software
- Todos os Cisco Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Oing PCommand

O comandoping(Packet InterNet Groper) é um método muito comum para solucionar problemas de

acessibilidade de dispositivos. Ele usa duas mensagens de consulta ICMP, requisições de eco ICMP e respostas de eco IMCP para determinar se um host remoto está ativo. O ping comando também mede o tempo necessário para receber a resposta de eco.

O ping comando primeiro envia um pacote de solicitação de eco para um endereço e depois espera uma resposta. O ping será bem-sucedido somente se a ECHO REQUEST chegar ao destino e o destino for capaz de obter uma ECHO REPLY de volta à origem do ping dentro de um intervalo de tempo predefinido.

O comando ing PCestendido

Quando um ping comando normal é enviado de um roteador, o endereço origem do ping é o endereço IP da interface que o pacote usa para sair do roteador. Se um ping comando estendido for usado, o endereço IP de origem poderá ser alterado para qualquer endereço IP no roteador. A verificação estendida ping é usada para executar uma verificação mais avançada da acessibilidade do host e da conectividade de rede. O ping comando estendido funciona somente na linha de comando do EXEC privilegiado. O normal ping funciona no modo EXEC de usuário e no modo EXEC privilegiado. Para usar esse recurso, insira ping na linha de comando e pressione Return. Você receberá um prompt dos campos de acordo com a seção Descrições do campo de comando ping deste documento.

Descrições dos campos do ing PCommand

Esta tabela lista as descrições dos campos de ping comando. Esses campos podem ser modificados com o uso do ping comando extended.

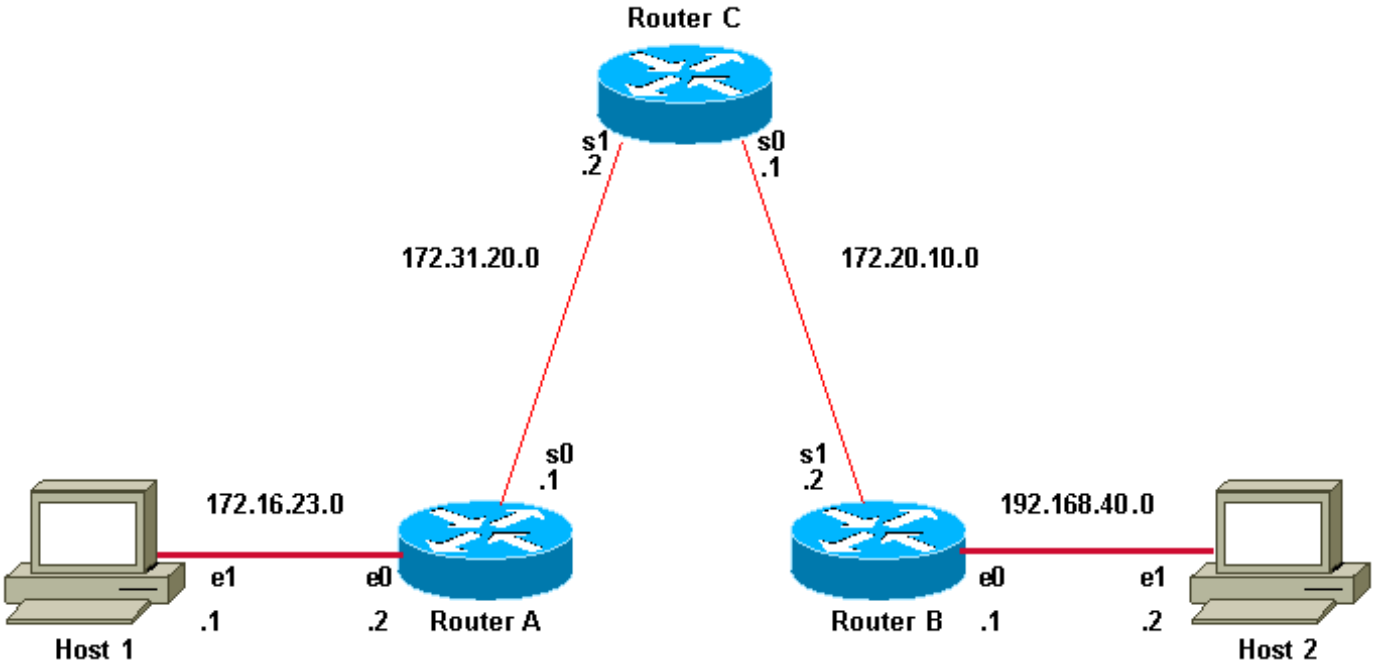
Campo	Descrição
Protocolo [ip]:	Solicita um protocolo suportado. Digite appletalk, clns, ip, novell, apollo, vines, decnet ou xns. O padrão é ip.
Endereço IP de destino:	Solicita o endereço IP ou nome do host do nó de destino em que planeja fazer o ping. Se você especificou um protocolo compatível diferente de IP, digite o endereço adequado para esse protocolo aqui. O padrão é nenhum.
Contagem de repetições [5]:	Número de pacotes de ping enviados para o endereço de destino. O padrão é 5.
Tamanho do datagrama [100]:	Tamanho do pacote de ping (em bytes). Padrão: 100 bytes.

Timeout em segundos [2]:	Intervalo. Padrão: 2 (segundos). O ping é declarado bem-sucedido somente se o pacote RESPOSTA EM ECO é recebido antes deste intervalo de tempo.
Comandos Extended [n]:	Especifica se uma série de comandos adicionais aparece ou não. O padrão é não.
Ingress ping [n]:	O ping de entrada simula os pacotes recebidos na interface de entrada especificada para o destino. O padrão é não. (A disponibilidade dessa opção é diferente da versão do software usada.)
Interface ou endereço de origem:	A interface ou o endereço IP do roteador para ser usado como endereço de origem para as sondas. O roteador normalmente captura o endereço IP da interface externa a ser usada. A interface também pode ser mencionada, mas com a sintaxe correta conforme mostrado aqui: Source address or interface: ethernet 0 Esta é uma saída parcial do`ping`comando estendido. A interface não pode ser escrita como e0.
DSCP Value [0]:	Especifica o Ponto de Código de Serviços Diferenciados (DSCP). O valor de DSCP apresentado é colocado em cada sondagem. O padrão é 0. (A disponibilidade dessa opção é diferente da versão do software usada.)
Tipo de serviço [0]:	Especifica o Tipo de serviço (ToS). O ToS solicitado é colocado em cada probe, mas não há nenhuma garantia de que todos os roteadores processem o ToS. É a seleção de qualidade de serviço de Internet. O padrão é 0.
Definir o bit DF em um cabeçalho de IP? [não]:	Especifica se o bit deve Don't Fragment (DF) ser definido no pacote ping. Se “sim” for especificado, a opção DF não permite que este

	pacote seja fragmentado quando ele tiver que passar por um segmento com uma unidade máxima de transmissão (MTU) menor, e você receberá uma mensagem de erro do dispositivo que queria fragmentar o pacote. Essa opção é útil para determinar a menor MTU no caminho para um destino. O padrão é não.
Validar dados de resposta? [não]:	Especifica se os dados da resposta devem ou não ser validados. O padrão é não.
Padrão de dados [0xABCD]	Especifica o padrão de dados. Diferentes padrões de dados são usados para solucionar framing erros e problemas clocking em linhas seriais. O padrão é [0xABCD].
Loose (Livre), Strict (Estrito), Record (Registro), Timestamp (Estampa de tempo), Verbose (Detalhado), [none] (nenhum):	Opções de cabeçalho IP. Esse prompt oferece mais de uma opção a ser selecionada. São elas: • Verbose é automaticamente selecionado, junto com qualquer outra opção. • Registro é uma opção muito útil, pois exibe o(s) endereço(s) dos saltos (até nove) atravessados pelo pacote. • Loose permite que você influencie o caminho ao especificar os endereços dos saltos que você deseja que o pacote atravesse. • Restrito é usado para especificar o(s) salto(s) que você quer que o pacote atravesse, mas nenhum outro salto pode ser visitado, • Carimbo de hora é usado para medir o tempo de ida e volta de determinados hosts. A diferença entre a opção Record desse comando e o comando traceroute é que a opção Record não apenas informa os saltos que a solicitação de eco (ping) atravessou para chegar ao destino, mas também informa os saltos visitados no caminho de retorno. Com o comando traceroute, você não obtém

	informações sobre o caminho da resposta em eco. O comando traceroute emite prompts para os campos necessários. O comando traceroute coloca as opções solicitadas em cada sondagem. No entanto, não há garantias de que todos os roteadores (ou nós de extremidade) processem as opções. O padrão é nenhum.
Intervalo de varredura dos tamanhos [n]:	Permite que você varie os tamanhos dos pacotes de eco enviados. Isso é utilizado para determinar os tamanhos mínimos das MTUs configuradas nos nós ao longo do caminho para o endereço de destino. Assim, os problemas de desempenho causados por fragmentação de pacotes são reduzidos. O padrão é não.
!!!!!	Cada ponto de exclamação (!) indica o recebimento de uma resposta. Um ponto final (.) indica que o servidor de rede atingiu o tempo limite enquanto aguardava uma resposta. Consulte os caracteres de ping para obter uma descrição dos outros caracteres.
A taxa de sucesso é 100%	A porcentagem de pacotes ecoados de volta para o roteador com sucesso. Em geral, qualquer porcentagem menor que 80 é considerada problemática.
round-trip min/avg/max = 1/2/4 ms	Intervalos do tempo de ida e volta dos pacotes de eco do protocolo com mínimo/médio/máximo (em milissegundos).

Neste diagrama, Host 1 e Host 2 não conseguem fazer o ping entre si. Você pode solucionar esse problema nos roteadores para determinar se há um problema de roteamento ou se um dos dois hosts não tem seu gateway padrão definido corretamente.



O Host 1 e o Host 2 não conseguem fazer ping

Para que a pingtransição do Host 1 para o Host 2 seja bem-sucedida, cada host precisa apontar seu gateway padrão para o roteador em seu respectivo segmento de LAN, ou o host precisa trocar informações de rede com os roteadores que usam um protocolo de roteamento. Se o gateway padrão do host não está configurado corretamente ou se o host não tem as rotas corretas na tabela de roteamento, ele não consegue enviar os pacotes para os destinos que não estão presentes no cache do Address Resolution Protocol (ARP). Também é possível que os hosts não consigam fazer o ping entre si, porque um dos roteadores não tem uma rota para a sub-rede na qual o host envia seus pacotes de ping.

Exemplo

Este é um exemplo do comando ping estendido originado da interface do Roteador A Ethernet 0 e destinado para a interface do Roteador B Ethernet. Se este ping for bem-sucedido, é uma indicação que não há problema de roteamento. O Roteador A sabe como chegar à Ethernet do Roteador B, e o Roteador B sabe como chegar à Ethernet do Roteador A. Além disso, ambos os hosts têm seus gateways padrão configurados corretamente.

Se o pingcomando estendido do Roteador A falhar, significa que há um problema de roteamento. Pode haver um problema de roteamento em qualquer um dos três roteadores. O Roteador A poderia ter perdido uma rota para a sub-rede do Roteador B Ethernet, ou para a sub-rede entre o Roteador C e o Roteador B. O Roteador B poderia ter perdido uma rota para a sub-rede do Roteador A, ou para a sub-rede entre o Roteador C e o Roteador A; e o Roteador C poderia ter perdido uma rota para a sub-rede dos segmentos Ethernet do Roteador A ou do Roteador B. Você deve corrigir todos os problemas de roteamento e, em seguida, o Host 1 deve tentar fazer ping no Host 2. Se o Host 1 ainda não conseguir fazer ping no Host 2, você precisará verificar os dois gateways padrão. A conectividade entre a Ethernet do Roteador A e a Ethernet do Roteador B é verificada com o comando ping estendido.

Com um ping normal do Roteador A para a interface de Ethernet do Roteador B, o endereço de

origem do pacote ping seria o endereço da interface de saída, ou seja, o endereço da interface serial 0 (172.31.20.1). Quando o Roteador B responde ao pacote de ping, ele responde para o endereço de origem (ou seja, 172.31.20.1). Desta forma, somente a conectividade entre a interface serial 0 do Roteador A (172.31.20.1) e a interface Ethernet do roteador B (192.168.40.1) é testada.

Para testar a conectividade entre a Ethernet 0 (172.16.23.2) do Roteador A e a Ethernet 0 (192.168.40.1) do Roteador B, use o `ping` comando extended. Com o extended `ping`, você tem a opção de especificar o endereço de origem do `ping`pacote, como mostrado aqui:

<#root>

```
RouterA>
enable

RouterA#
ping

Protocol [ip]:
Target IP address: 192.168.40.1

!--- The address to ping.

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.23.2

!---Ping packets are sourced from this address.

Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

!--- Ping is successful.

RouterA#
This is an example with extended commands and sweep details:
```

```
RouterA>
enable

RouterA#
ping


Protocol [ip]:

!--- The protocol name.



Target IP address: 192.168.40.1

!--- The address to ping.



Repeat count [5]: 10

!--- The number of ping packets that are sent to the destination address.



Datagram size [100]:

!--- The size of the ping packet in size. The default is 100 bytes.



Timeout in seconds [2]:

!--- The timeout interval. The ping is declared successful only if the
!--- ECHO REPLY packet is received before this interval.



Extended commands [n]: y

!--- You choose yes if you want extended command options
!--- (Loose Source Routing, Strict Source Routing, Record route and Timestamp).



Source address or interface: 172.16.23.2

!--- Ping packets are sourced from this address and must be the IP address
!--- or full interface name (for example, Serial0/1 or 172.16.23.2).
```

```
Type of service [0]:

!--- Specifies Type of Service (ToS).



Set DF bit in IP header? [no]:

!--- Specifies whether or not the Don't Fragment (DF) bit is to be
!--- set on the ping packet.



Validate reply data? [no]:

!--- Specifies whether or not to validate reply data.



Data pattern [0xABCD]:

!--- Specifies the data pattern in the ping payload. Some physical links
!--- might exhibit data pattern dependent problems. For example, serial links
!--- with misconfigured line coding. Some useful data patterns to test
!--- include all 1s (0Xffff), all 0s (0x0000) and alternating
!--- ones and zeros (0Xaaaa).



Loose, Strict, Record, Timestamp, Verbose[none]:

!--- IP header options.



Sweep range of sizes [n]: y

!--- Choose yes if you want to vary the sizes on echo packets that are sent.



Sweep min size [36]:
Sweep max size [18024]:
Sweep interval [1]:

Sending 179890, [36..18024]-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:



!--- The count 179890 depends on the values of min sweep,
!--- max sweep, sweep interval and repeat count. Calculations are based on:
```

```
!--- 18024(high end of range) - 36(low end of range) = 17988(bytes in range)
!--- 17988(bytes in range) / 1(sweep interval) = 17988 (steps in range)
!--- 17988(bytes in range) + 1 (first value) = 17989(values to be tested)
!--- 17989(values to be tested) * 10(repeat count) = 179890 (pings to be sent)
!--- In order to decrease the value, increase the sweep interval or decrease
!--- the repeat count, or you can even decrease the difference between
!--- Minimum and Maximum sweep size. Based on the previous example, the
!--- number 17890 is an expected value and tries to ping 17890 times.


Packet sent with a source address of 172.16.23.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms


!--- Ping is successful.


RouterA#
```

O comando Traceroute

Onde o ping pode ser usado para verificar a conectividade entre dispositivos, o traceroute comando pode ser usado para descobrir os caminhos que os pacotes percorrem para um destino remoto, bem como onde o roteamento é interrompido.

A finalidade por trás do traceroute comando é registrar a origem de cada mensagem de tempo excedido ICMP para fornecer um rastreamento do caminho que o pacote percorreu para alcançar o destino.

O dispositivo que executa o traceroute comando envia uma sequência de datagramas UDP (User Datagram Protocol), cada um com incrementos de valor TTL (Time-To-Live), para um endereço de porta inválido (Default 33434) no host remoto.

Primeiro, três datagramas são enviados, cada um com um valor de campo TTL definido como 1. O valor TTL de 1 faz com que o datagrama exceda o tempo limite assim que atingir o primeiro roteador no caminho. Esse roteador então responde com uma mensagem de tempo excedido de ICMP, indicando que o datagrama expirou.

Em seguida, mais três mensagens UDP são enviadas, cada uma com o valor TTL definido como 2. Isso faz com que o segundo roteador no caminho para o destino retorne mensagens de tempo excedido ICMP.

Esse processo continua até que os pacotes alcancem o destino e até que o sistema que origina o traceroute recebimento das mensagens de tempo excedido ICMP de cada roteador no caminho para o destino. Como esses datagramas tentam acessar uma porta inválida (padrão 33434) no host de destino, o host responde com mensagens de porta inacessível de ICMP que indicam uma porta inacessível. Este evento sinaliza que o programa traceroute deve encerrar.

Note: Certifique-se de não ter desabilitado o comando ip unreachable com o comando no ip unreachables em qualquer VLAN. Esse comando faz com que o pacote seja descartado sem mensagens de erro de ICMP. Nesse caso, o traceroute não funciona.

O comando traceroute estendido

O traceroute comando estendido é uma variação do traceroute comando. Um comando trackers estendido pode ser usado para ver o caminho que os pacotes percorrem para chegar a um destino. O comando também pode ser usado para verificar o roteamento ao mesmo tempo. Isso é útil quando você soluciona problemas de loops de roteamento ou quando determina onde os pacotes são perdidos (se uma rota for perdida ou se os pacotes forem bloqueados por uma lista de controle de acesso ou firewall). Você pode usar o comando ping estendido para determinar o tipo de problema de conectividade e, em seguida, o comando traceroute estendido para identificar onde o problema ocorre.

Uma mensagem de erro de tempo excedido indica que um servidor de comunicação intermediário viu e descartou o pacote. Uma mensagem de erro de destino inacessível indica que o nó de destino recebeu a sondagem e a descartou porque não conseguiria entregar o pacote. Caso a temporização termine antes de receber a resposta, o trace imprime um asterisco (*).

O comando termina quando qualquer um desses eventos acontece:

- O destino responde.
- o TTL máximo é excedido.
- O usuário interrompe o rastreamento com a seqüência de escape.

Note: Você pode chamar essa sequência de escape ao pressionar simultaneamente Ctrl+Shift e 6.

Descrições de campo do comando traceroute

Esta tabela lista as descrições de campo do comando traceroute.

Campo	Descrição

Protocolo [ip]:	Solicita um protocolo suportado. Digite appletalk, clns, ip, novell, apollo, vines, decnet ou xns. O padrão é ip.
Endereço IP de destino	Você precisa inserir um nome do host ou um endereço IP. Não há padrão.
Endereço origem:	A interface ou o endereço IP do roteador para ser usado como endereço de origem para as sondas. O roteador normalmente captura o endereço IP da interface externa a ser usada.
Exibição numérica [n]:	O padrão é ter uma exibição simbólica e numérica; no entanto, você pode suprimir a exibição simbólica.
Tempo limite em segundos [3]:	O número de segundos a esperar por uma resposta a um pacote de prova. O padrão é 3 segundos.
Contagem da prova [3]:	O número de provas a serem enviadas em cada nível de TTL. A contagem padrão é 3.
Minimum Time to Live [1]:	O valor TTL das primeiras provas. O padrão é 1, mas pode ser definido com um valor mais alto para eliminar a exibição de saltos desconhecidos.
Tempo Máximo de Vida [30]:	O maior valor de TTL que pode ser usado. O padrão é 30. O traceroute comando termina quando o destino é alcançado ou quando esse valor é alcançado.
Número de Porta [33434]:	A porta de destino usada pelas mensagens de teste UDP. O padrão é 33434.
Loose (Livre), Strict (Estrito), Record (Registro), Timestamp (Estampa de tempo), Verbose (Detalhado), [none] (nenhum):	Opções de cabeçalho IP. Você pode especificar qualquer combinação. O traceroute comando emite prompts para os campos obrigatórios. O traceroute comando coloca as opções solicitadas

	em cada sonda; no entanto, não há garantias de que todos os roteadores (ou nós de extremidade) processem as opções.

Exemplo

<#root>

```
RouterA>

enable


RouterA#

traceroute


Protocol [ip]:
Target IP address: 192.168.40.2


!--- The address to which the path is traced.



Source address: 172.16.23.2
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.40.2

1 172.31.20.2 16 msec 16 msec 16 msec
2 172.20.10.2 28 msec 28 msec 32 msec
3 192.168.40.2 32 msec 28 msec *


!--- The traceroute is successful.



RouterA#
```

Note: O traceroute comando estendido pode ser executado somente no modo EXEC privilegiado, enquanto o traceroute comando normal funciona nos modos EXEC privilegiado e de usuário.

Informações Relacionadas

- Página de tecnologia de protocolos roteados TCP/IP
- Página de Suporte do IP Routing
- Entender os comandos Ping e Traceroute
- Usar o comando traceroute nos sistemas operacionais
- Suporte técnico e downloads 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.