ホスト サービスとアプリケーションの実装

ホスト サービスとアプリケーションの実装

ルータ上の Cisco IOS XR ソフトウェア ホスト サービスおよびアプリケーション機能は主に、ネットワークの接続性とパケットが宛先に達するまでのルートをチェックし、ホスト名を IP アドレスに（または IP アドレスをホスト名に）マッピングして、ルータと UNIX ワークステーション間でファイルを転送するために使用します。

ネットワーク接続性ツール

ネットワーク接続性ツールを使用すると、ネットワーク上のデバイスに対して traceroute や ping を実行して、デバイスの接続をチェックできます。

ping

ping コマンドは、デバイスのアクセシビリティのトラブルシューティングに広く使用されている方法です。これは、2 つのインターネット制御メッセージプロトコル（ICMP）クエリーメッセージ、ICMP エコー要求、および ICMP エコー応答を使用して、リモート ホストがアクティ

ブであるかどうかを判断します。pingコマンドは、エコー応答を受信するまでにかかる時間も測定します。

ping コマンドは、最初に 1 つのアドレスにエコー要求パケットを送信して応答を待ちます。ping が正常に完了するのは、エコー要求が宛先に届き、定義済みの時間内に宛先が ping の送信元にエコー応答（ホスト名が存続している）を返すことができる場合だけです。

bulkオプションが導入されたため、複数の宛先の到達可能性をチェックできるようになりました。宛先は、CLIから直接入力します。このオプションは、ipv4の宛先でのみサポートされます。

ネットワーク接続の確認

基本的なネットワーク接続性の診断を支援する手段として、多くのネットワーク プロトコルがエコープロトコルをサポートしています。プロトコルでは、宛先ホストに特殊なデータグラムを送信し、そのホストからの応答データグラムを待ちます。このエコープロトコルからの結果は、ホストに至るパスの信頼性、パスの遅延、およびホストに到達できるのか、ホストが機能しているのかを評価するのに役立ちます。

ネットワーク接続を確認するための設定

次の設定は、ルータ A の インターフェイスとルータ B の インターフェイスから送信される拡張 ping コマンドを示しています。この ping が成功する場合、ルーティング上の問題がないことを示します。ルータ Aはルータ Bのインターフェイスに到達する方法を認識していて、ルータ B はルータ A の インターフェイスに到達する方法を認識しています。また、両方のホストには適切に設定されたデフォルト ゲートウェイがあります。

ルータ A からの拡張 **ping** コマンドが失敗する場合、ルーティング上の問題があることを意味します。3 つのルータのいずれでもルーティングの問題が発生する可能性があります。ルータ A では、ルータ B のインターフェイスのサブネットへのルートや、ルータ C とルータ B 間のサブネットへのルートが不明になる可能性があります。ルータ B では、ルータ A のサブネットへのルートや、ルータ C とルータ A 間のサブネットへのルートが不明になる可能性があります。ルータ C では、ルータ A またはルータ B のイーサネット セグメントのサブネットへのルートが不明になる可能性があります。ルーティングに関する問題を修正してから、ホスト 1 からホスト 2 への ping を実行する必要があります。ホスト 1 からホスト 2 への ping を実行できない場合は、両方のホストのデフォルト ゲートウェイを確認してください。ルータ A の インターフェイスとルータ B の インターフェイスとの接続は、拡張 ping コマンドを使用してチェックします。

ルータ A からルータ B の インターフェイスへの通常の ping では、ping パケットの送信元アドレスは発信インターフェイスのアドレス、つまり インターフェイスのアドレス（10.0.0.2）になります。ルータ B が ping パケットに応答するとき、送信元アドレス（つまり、10.0.0.2）に応答します。このように、ルータ A の インターフェイス（10.0.0.2）とルータ B の TenGigE インターフェイス（10.0.0.1）間の接続だけがテストされます。

ルータ A の インターフェイス（10.0.0.2）とルータ B の インターフェイス（10.0.0.1）との接続をテストするには、拡張 ping コマンドを使用します。拡張 **ping** コマンドには、**ping** パケットの送信元アドレスを指定するオプションがあります。

設定例

この使用例では、拡張 ping コマンドを使用して、2 つの IP アドレス（ルータ A（10.0.0.2）とルータ B（10.0.0.1））間の IP 接続を検証します。

```
Router# ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
Router#!!!!!

*/If you do not enter a hostname or an IP address on the same line as the ping command,

the system prompts you to specify the target IP address and several other command
parameters.
After specifying the target IP address, you can specify alternate values for the
remaining parameters or accept the displayed default for each parameter /*

Router# ping
Protocol [ipv4]:
Target IP address: 10.0.0.1
Repeat count [5]: 5
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 1
Extended commands? [no]: no
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 10.0.0.1, timeout is 1 seconds:
!!!!!
Success rate is 100 percent (5/5)
Router#!!!!!
```

関連コマンド

複数の宛先に対するネットワーク接続性のチェック

bulk オプションを使用すると、複数の宛先への到達可能性をチェックできます。宛先は、CLI から直接入力します。このオプションは、ipv4 の宛先でのみサポートされます。

設定例

次の IP アドレスを持つ IP ネットワーク上の複数のホストへの到達可能性とネットワーク接続を確認します。

- 1: 1.1.1.1
- 2: 2.2.2.2
- 3: 3.3.3.3

```
Router# ping bulk ipv4 input cli batch
*/You must hit the Enter button and then specify one destination address per line*/
Please enter input via CLI with one destination per line and when done Ctrl-D/(exit) to
 initiate pings:
1: 1.1.1.1
2: 2.2.2.2
3: 3.3.3.3
4:
```

```
Starting pings...
Target IP address: 1.1.1.1
Repeat count [5]: 5
Datagram size [100]: 1
% A decimal number between 36 and 18024.
Datagram size [100]: 1
% A decimal number between 36 and 18024.
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 10
Extended commands? [no]: no
Sweep range of sizes? [no]: q
% Please answer 'yes' or 'no'.
Sweep range of sizes? [no]: q
% Please answer 'yes' or 'no'.
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 1 seconds:
!!!!!
Success rate is 100 percent (5/5),
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]: q
% A decimal number between 36 and 18024.
Datagram size [100]:
Timeout in seconds [2]:
Interval in milliseconds [10]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Sending 5, 100-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
Target IP address:  3.3.3.3
Repeat count [5]: 4
Datagram size [100]: 100
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 10
Extended commands? [no]: no
Sweep range of sizes? [no]: no
Sending 4, 100-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 1 seconds:
!!!!!
Success rate is 100 percent (4/5),
```

関連コマンド

traceroute

ping コマンドを使用してデバイス間の接続性を検証できる場合は、**traceroute** コマンドを使用してパケットがリモート接続先までにたどるパスおよびルーティングに障害がある場所を検出できます。

traceroute コマンドは、各 ICMP "time-exceeded" メッセージの送信元を記録して、パケットが宛先に達するまでにたどったパスを示すことができます。IP **traceroute** コマンドを使用すると、パケットがネットワーク経由でたどるパスをホップバイホップで特定できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

traceroute コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータとサーバで特定のリターン メッセージが生成されるようにします。traceroute コマンドは、TTL フィールドが 1 に設定されている宛先ホストに、ユーザ データグラム プロトコル（UDP）データグラムを送信します。ルータは 1 または 0 の TTL 値を検出すると、データグラムをドロップし、送信元に ICMP の time-exceeded メッセージを戻します。traceroute 機能は、ICMP time-exceeded メッセージの送信元アドレス フィールドを調べ、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute コマンドは TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 の UDP パケットを受け取り、データグラムを廃棄して、送信元に time-exceeded メッセージを戻します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを判断するために、traceroute コマンドは、宛先ホストが使用しないと予測される非常に大きな値をデータグラムの UDP 宛先ポートに設定します。ホストは、この未知のポート番号を持つデータグラムを受信すると、送信元に ICMP port unreachable error メッセージを戻します。このメッセージにより、宛先に到達したことを traceroute 機能に伝えます。

パケット ルートのチェック

traceroute コマンドを使用すると、パケットが宛先に到達するまでに実際にたどるルートをトレースできます。

設定例

10.0.0.2 から 20.1.1.1 へのルートをトレースします。

```
Router# traceroute 20.1.1.1
Type escape sequence to abort.
Tracing the route to 20.1.1.1
 1  10.0.0.1 39 msec  *  3 msec

*/If you do not enter a hostname or an IP address on the same line as the traceroute
command, the system prompts you to specify the target IP address and several other
command parameters. After specifying the target IP address, you can specify alternate
values for the remaining parameters or accept the displayed default for each
parameter/*

Router #traceroute
Protocol [ipv4]:
Target IP address: 20.1.1.1
Source address: 10.0.0.2
Numeric display? [no]:
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 20.1.1.1
 1  10.0.0.1 3 msec  *  3 msec
```

関連コマンド

ドメイン サービス

Cisco IOS XR ソフトウェア ドメイン サービスは、Berkeley Standard Distribution（BSD）ドメイン リゾルバとして機能します。ドメイン サービスは、アプリケーション（Telnet など）やコマンド（**ping**、**traceroute** など）で使用される、ホスト名対アドレスのマッピングのローカル キャッシュを保持します。ローカルキャッシュにより、ホスト名からアドレスへの変換の速度が向上します。ローカルキャッシュには、2つのタイプのエントリが存在します。スタティックとダイナミックです。domain ipv4 host または domain ipv6 host コマンドを使用して設定されたエントリはスタティック エントリとして追加され、ネーム サーバから受信したエントリはダイナミック エントリとして追加されます。

ネーム サーバは、World Wide Web（WWW）でネットワーク ノードの名前をアドレスに変換するために使用されます。ネーム サーバは、DNS サーバから DNS プロトコルを使用して、ホスト名を IP アドレスにマッピングする分散データベースを維持します。domain name-server コマンドを使用して、1 つ以上のネーム サーバを指定できます。

アプリケーションでホストの IP アドレスまたは IP アドレスのホスト名が必要になると、ドメイン サービスに対してリモート プロシージャ コール（RPC）が実行されます。ドメイン サービスは、キャッシュ内で IP アドレスまたはホスト名を探し、エントリが見つからない場合にはネーム サーバに DNS クエリーを送信します。

ドメイン名要求を完了するために Cisco IOS XR ソフトウェアで使用されるデフォルト ドメイン名を指定できます。単一のドメインまたはドメイン名のリストを指定することもできます。IP ホスト名にドメイン名が含まれていない場合には、ホスト テーブルに追加される前に指定のドメイン名が付加されます。1 つまたは複数のドメイン名を指定するには、domain name コマンドまたは domain list コマンドを使用します。

ドメイン サービスの設定

デフォルトでは、DNS によるホスト名からアドレスへの変換がイネーブルになっています。**domain lookup disable** コマンドによってホスト名からアドレスへの変換がディセーブルになっている場合は、 **no domain lookup disable** コマンドを使用して変換を再びイネーブルにします。

設定例

スタティック ホスト名とアドレスのマッピングを定義します。IPv4 アドレスを 2 つのホスト（192.168.7.18 と 10.2.0.2 192.168.7.33）に関連付けます（またはマッピングします）。ホスト名は host1 と host2 です。

```
Defining the Domain Host
==================================
Router# configure
Router(config)#domain ipv4 host host1 192.168.7.18
```

```
Router(config)#domain ipv4 host host2 10.2.0.2 192.168.7.33
Router(config)#commit

Defining the Domain Name
=========================
*/Define cisco.com as the default domain name/*
Router#configure
Router(config)#domain name cisco.com
Router(config)#commit

Specifying the Addresses of the Name Servers
=============================================
*/Specify host 192.168.1.111 as the primary name server
and host 192.168.1.2 as the secondary server/*
Router#configure
Router(config)#domain name-server 192.168.1.111
Router(config)#domain name-server 192.168.1.2
Router(config)#commit
```

確認

```
Router#show hosts
Default domain is cisco.com
Name/address lookup uses domain service
Name servers: 192.168.1.111, 192.168.1.2

Host                      Flags     Age(hr) Type Address(es)
host2                   (perm, OK)    0      IP  10.2.0.2
                                                 192.168.7.33
host1                   (perm, OK)    0      IP  192.168.7.18
```

関連コマンド

TFTP サーバ

サーバとしてだけ機能するマシンをネットワークの各セグメントに配置するのは、コストがかかり、非効率的です。しかし、すべてのセグメントにサーバがあるのではない場合、ネットワーク セグメントを超えたネットワークの操作によって相当の遅延が引き起こされることがあります。ルータを TFTP サーバとして機能するように設定すると、ルータの通常の機能を使用しながらコストと遅延時間を削減できます。

一般に、TFTP サーバとして設定されたルータは、フラッシュ メモリから他のルータにシステム イメージまたはルータ コンフィギュレーション ファイルを提供します。他のタイプのサービス要求に応答するようにルータを設定することもできます。

TFTP サーバとしてのルータの設定

TFTP 機能の実装前に、サーバとクライアント ルータは互いに到達可能である必要があります。ping コマンドを使用してサーバとクライアント ルータ間の接続を（いずれかの方向で）テストして、この接続を検証します。

このタスクを実行すると、ルータを TFTP サーバとして設定できます。これにより、TFTP クライアントとして機能する他のデバイスは、slot0: や /tmp などの特定のディレクトリ（TFTP ホーム ディレクトリ）の下にあるファイルをルータに対して読み書きできます。

（注） セキュリティを確保するため、ファイルがすでに存在していないと、TFTP サーバでは書き込み要求を正常に完了できません。

TFTP 機能の実装前に、サーバとクライアント ルータは互いに到達可能である必要があります。ping コマンドを使用してサーバとクライアント ルータ間の接続を（いずれかの方向で）テストして、この接続を検証します。

設定例

TFTP サーバとしてルータを設定します（ホーム ディレクトリの disk0:）。

```
Router#configure
Router(config)#tftp ipv4 server homedir disk0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config tftp ipv4 server homedir disk0:
tftp vrf default ipv4 server homedir disk0:
```

確認

```
Router#show cinetd services
Vrf Name Family Service     Proto Port ACL  max_cnt  curr_cnt wait  Program Client Option

default  v4     tftp     udp   69      unlimited 0       wait   tftpd   sysdb disk0:

default  v4       telnet      tcp   23      10        0       nowait telnetd sysdb
```

関連コマンド

ファイル転送サービス

ファイル転送プロトコル（FTP）、簡易ファイル転送プロトコル（TFTP）、リモート コピー プロトコル（RCP）の各クライアント、およびセキュア コピープロトコル（SCP）はファイル システムまたはリソース マネージャとして実装されます。たとえば、tftp:// で始まるパス名は TFTP リソース マネージャによって処理されます。

ファイル システム インターフェイスは、URL を使用して、ファイルの場所を指定します。URL は、WWW でファイルまたは場所を指定するのに広く使用されています。ただし、Cisco ルータの URL には、ルータまたはリモート ファイル サーバ上のファイルの場所も指定されます。

ルータがクラッシュしたときは、ルータのメモリ内容全体のコピーを取得するのが便利です（これをコア ダンプと言います）。テクニカル サポート担当者が、クラッシュの原因を特定

するのに使用します。SCP、FTP、TFTP、RCP を使用すると、コア ダンプをリモート サーバに保存できます。

FTP

ファイル転送プロトコル（FTP）は、TCP/IP プロトコル スタックの一部であり、ネットワーク ノード間でファイルを転送するのに使用します。FTP は、RFC 959 で定義されています。

FTP 接続使用時のルータ設定

FTP 接続を使用してネットワーク上のシステム間でファイルを転送するようにルータを設定できます。次の FTP の特性を設定できます。

- パッシブ モード FTP
- パスワード
- IP アドレス

設定例

ルータによる FTP 接続の使用をイネーブルにします。パッシブ FTP 接続を使用するようにソフトウェアを設定し、匿名ユーザのパスワードを設定して、FTP 接続の送信元 IP アドレスも指定します。

```
Router#configure
Router(config)#ftp client passive
(Optional) Router(config)#ftp client vrf vrfa
Router(config)#ftp client anonymous-password xxxx
Router(config)#ftp client source-interface HundredGigE 0/9/0/0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config ftp client passive
ftp client passive
ftp client vrf vrfa
Router#show running-config ftp client anonymous-password xxxx
ftp client anonymous-password xxxx
Router#show running-config ftp client source-interface HundredGigE 0/9/0/0
ftp client source-interface HundredGigE 0/9/0/0
```

関連コマンド

- ftp client passive
- ftp client anonymous-password
- ftp client source-interface

TFTP

Trivial File Transfer Protocol（TFTP）は FTP の簡易版で、ネットワークを介して 1 つのコンピュータから別のコンピュータにファイルを転送できます。通常は、クライアント認証（ユーザ名とパスワードなど）を使用しません。

TFTP 接続使用時のルータ設定

設定例

TFTP 接続を使用するようにルータを設定し、TFTP 接続の送信元アドレスとして HundredGigE 0/9/0/0 の IP アドレスを設定します。

```
Router#configure
Router(config)#tftp client source-interface HundredGigE 0/9/0/0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config tftp client source-interface HundredGigE 0/9/0/0
tftp client source-interface HundredGigE 0/9/0/0
```

確認

```
Router#show cinetd services
Vrf Name Family  Service  Proto Port ACL max_cnt  curr_cnt  wait   Program Client Option

default  v4    tftp udp    69      unlimited  0       wait   tftpd    sysdb disk0:

default  v4      telnet   tcp    23      10         0       nowait telnetd  sysdb
```

関連コマンド

- tftp client source-interface type
- show cinetd services

SCP

セキュア コピー プロトコル（SCP）は、ファイルを転送するための認証されたセキュアな方式を提供するファイル転送プロトコルです。SCP は SSHv2 に依存して、リモート ロケーションからローカル ロケーションに、またはローカル ロケーションからリモート ロケーションにファイルを転送します。

Cisco IOS XR ソフトウェアは SCP サーバ操作とクライアント操作をサポートしています。デバイスが SCP 要求を受信すると、SSH サーバ プロセスはクライアントとやり取りする SCP サーバ プロセスを生成します。各着信 SCP サブシステム要求に対して新しい SCP サーバ インスタンスが生成されます。デバイスが宛先デバイスにファイル転送要求を送信する場合、そのデバイスはクライアントとして機能します。

デバイスがファイル転送のためにリモート ホストとの SSH 接続を開始すると、リモート デバイスはソース モードまたはシンク モードで要求に応答することができます。ソース モードで

は、デバイスはファイル ソースになります。デバイスはそのローカル ディレクトリからファイルを読み取り、目的の宛先に転送します。シンク モードでは、デバイスは転送するファイルの宛先になります。

SCP を使用して、ローカル デバイスから宛先デバイスに、または宛先デバイスからローカル デバイスにファイルをコピーできます。

SCP では、個々のファイルの転送のみを実行できます。宛先デバイスから別の宛先デバイスにファイルを転送することはできません。

SCP によるファイル転送

セキュア コピー プロトコル（SCP）を使用すると、送信元デバイスと宛先デバイス間でファイルを転送できます。一度に 1 つのファイルを転送できます。宛先がサーバの場合は、SSH サーバ プロセスが実行されている必要があります。

設定例

ファイル「test123.txt」をローカル ディレクトリからリモート ディレクトリに転送します。

```
Router#scp /harddisk:/test123.txt xyz@1.75.55.1:/auto/remote/test123.txt
Connecting to 1.75.55.1...
Password:
Router#commit
```

確認

テキスト「test123.txt」ファイルがコピーされたことを確認します。

```
xyz-lnx-v1:/auto/remote> ls -altr test123.txt
-rw-r--r-- 1 xyz eng 0 Nov 23 09:46 test123.txt
```

関連コマンド

- scp

Cisco inetd

Cisco インターネット サービス プロセス デーモン（Cinetd）は、システムのブート後にシステム マネージャによって開始されるマルチスレッド サーバ プロセスです。Cinetd は、Telnet サービスや TFTP サービスなどのインターネット サービスをリッスンします。Cinetd が特定のサービスをリッスンするかどうかは、ルータ コンフィギュレーションによって異なります。たとえば、 **tftp server** コマンドを入力すると、Cinetd は TFTP サービスのリッスンを開始します。要求が届くと、Cinetd はサービスに関連付けられたサーバ プログラムを実行します。

Telnet

Telnet をイネーブルにすると、ネットワーキング デバイスで着信 Telnet 接続が許可されます。

設定例

Telnet をイネーブルにして、ルータに同時にアクセスできるユーザの数を 10 人に制限します。

```
Router# configure
Router(config)# telnet ipv4 server max-servers 10
Router(config)# commit
```

確認

```
Router# show cinetd services
Vrf Name  Family    Service   Proto Port ACL max_cnt  curr_cnt  wait   Program Client
Option
default   v4         tftp      udp  69       unlimited  0        wait   tftpd   sysdb
disk0:
default   v4      telnet  tcp  23        10  0        nowait telnetd sysdb
```

関連コマンド

Syslog の送信元インターフェイス

ロギング送信元インターフェイスを設定すると、特定のルータから VRF で発信される syslog トラフィックを、単一のデバイスからの着信として識別できます。

設定例

リモート Syslog サーバの送信元インターフェイスをイネーブルにします。デフォルトの vrf のロギング送信元インターフェイスとして loopback 2 を設定します。

```
Router#configure
Router(config)#logging source-interface Loopback2
Router(config)#logging source-interface Loopback3 vrf vrfa
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config logging
/*Logging configuration after changing the source into loopback2 interface.
logging console debugging
logging monitor debugging
logging facility local4
logging 123.100.100.189 vrf default severity info port default
logging source-interface Loopback2
logging source-interface Loopback3 vrf vrfa
```

関連コマンド

- logging source-interface
- show running-configuration logging