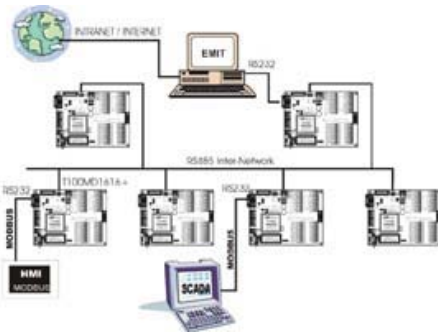


Khắc phục sự cố các vấn đề kết nối trong mạng (Phần 1)

Nguồn : quantrimang.com

Brien M. Posey



Quản trị mạng - Phần cứng và phần mềm mạng ngày nay ngày càng trở nên tin cậy hơn nhưng, tuy nhiên đôi khi vẫn có những thứ xảy ra không như mong muốn. Chính vì vậy trong loạt bài này, chúng tôi sẽ giới thiệu cho các bạn về một số kỹ thuật khắc phục sự cố để bạn sử dụng khi các máy tính trong mạng gặp các vấn đề khó khăn trong truyền thông. Vì mục đích nhằm giới thiệu cho những người vẫn ít kinh nghiệm trong làm

việc với giao thức TCP/IP, nên chúng tôi sẽ bắt đầu bằng những kiến thức cơ bản, sau đó sẽ làm việc với các kỹ thuật nâng cao hơn.

Thẩm định kết nối mạng

Khi một host có vấn đề nào đó trong truyền thông với host khác, thứ đầu tiên mà bạn cần phải thực hiện là thu thập các thông tin về vấn đề đó. Cụ thể hơn, bạn cần đọc các tài liệu về cấu hình của host, chỉ ra xem host có vấn đề truyền thông với các máy tính khác trên mạng hay không và xem vấn đề ảnh hưởng thế nào có ảnh hưởng tới các host khác hay không.

Cho ví dụ, cho rằng một máy trạm làm việc có một vấn đề truyền thông với một máy chủ nào đó. Tự bản thân nó không thực sự cho bạn nhiều thông tin. Mặc dù vậy, nếu bạn tìm hiểu thêm một chút sâu hơn và phát hiện máy trạm không thể truyền thông với tất cả các máy chủ khác trong mạng thì vấn đề có thể nằm ở cấp mạng, có được kết nối hay không, hay cổng của bộ chuyển mạch bị hỏng hoặc có thể là một vấn đề trong việc cấu hình mạng chẳng hạn.

Tương tự như vậy, nếu máy trạm có thể truyền thông với một số máy chủ trong mạng, nhưng không phải tất cả thì điều đó cũng cho bạn có được một sự gợi ý về vị trí nhằm tìm kiếm vấn đề. Trong kiểu tình huống đó, bạn có thể sẽ kiểm tra xem những máy chủ nào không thể liên lạc. Liệu tất cả chúng có nằm trên một subnet? Nếu vậy thì vấn đề định tuyến có thể gây ra lỗi này.

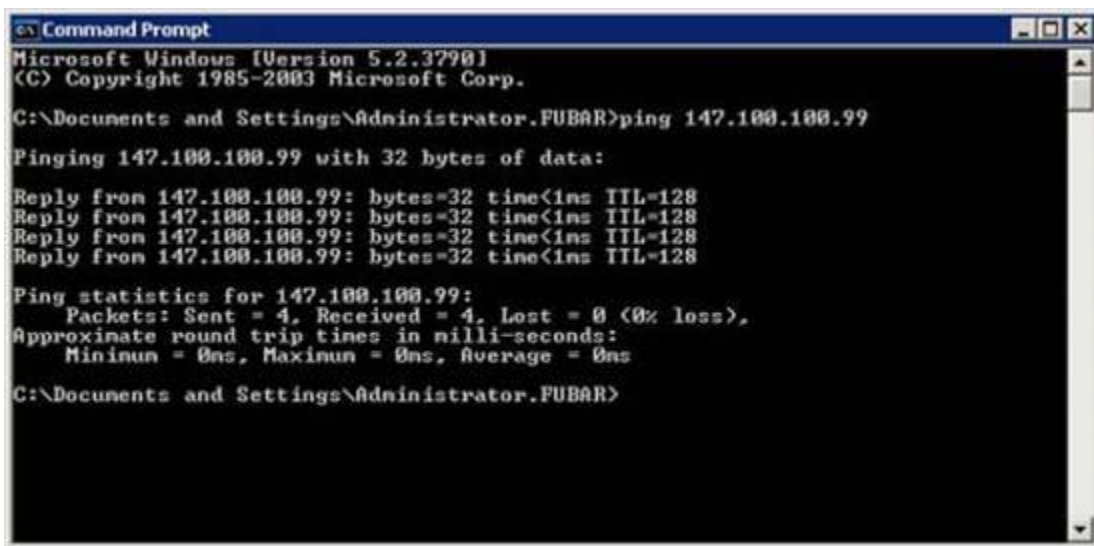
Nếu nhiều máy trạm làm việc có vấn đề truyền thông với một máy chủ cụ thể thì vấn đề có thể không nằm ở các máy trạm trừ khi các máy trạm này đã được cấu hình lại gần đây. Trong trường hợp này, vấn đề thiên về sự cố xảy ra ở máy chủ.

Chúng ta sẽ bắt đầu từ những bài test cơ bản. Những bài test mà chúng tôi sẽ giới thiệu cho các bạn sẽ không thể hiện nhiều nguyên nhân của vấn đề nhưng chúng sẽ giúp thu hẹp được nhiều thứ để bạn biết đâu quá trình khắc phục sự cố từ đâu.

PING

PING là một tiện ích chuẩn đoán TCP/IP đơn giản nhất đã được tạo ra, nhưng những thông tin mà nó có thể cung cấp cho bạn lại hoàn toàn vô giá. Đơn giản nhất, PING cho bạn biết được máy chủ của bạn có truyền thông được với các máy tính khác hay không.

Thứ đầu tiên mà chúng tôi khuyên bạn thực hiện là mở cửa sổ lệnh (Command Prompt), sau đó nhập vào đó lệnh PING, tiếp đến nhập vào địa chỉ IP của máy mà bạn đang có vấn đề truyền thông. Khi thực hiện ping, máy mà bạn đã chỉ định sẽ cho ra 4 phản hồi, xem thể hiện trong hình A.



```
Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.FUBAR>ping 147.100.100.99

Pinging 147.100.100.99 with 32 bytes of data:

Reply from 147.100.100.99: bytes=32 time<1ms TTL=128
Reply from 147.100.100.99: bytes=32 time<1ms TTL=128
Reply from 147.100.100.99: bytes=32 time<1ms TTL=128
Reply from 147.100.100.99: bytes=32 time<1ms TTL=128

Ping statistics for 147.100.100.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator.FUBAR>
```

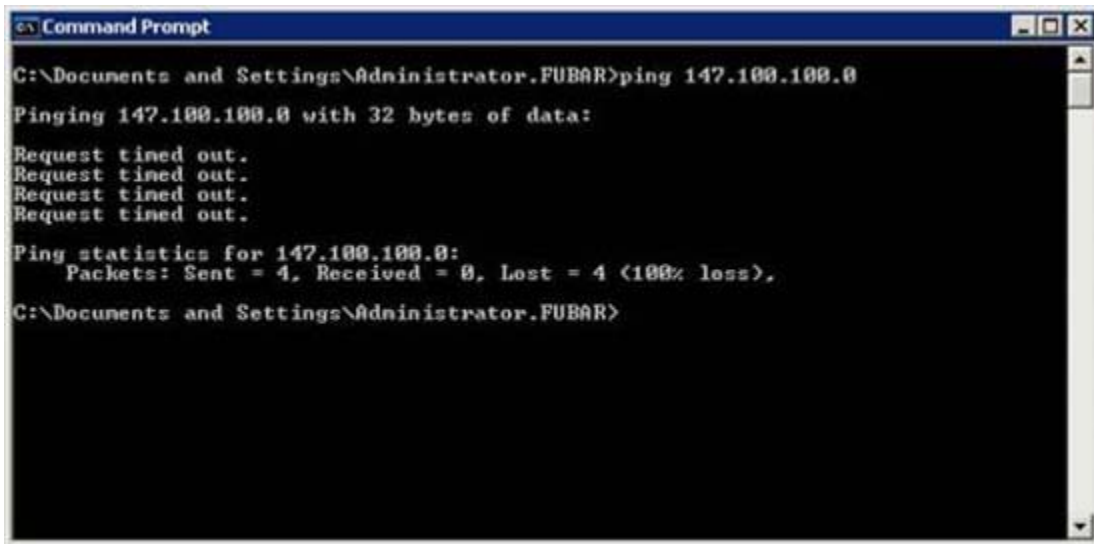
Hình A: Mỗi một máy sẽ tạo ra 4 phản hồi

Những phản hồi này về cơ bản sẽ cho bạn biết được khoảng thời gian máy tính được chỉ định đáp trả 32 byte dữ liệu là bao nhiêu. Cho ví dụ, trong hình A, một trong 4 đáp trả được nhận đều nhỏ hơn 4 ms.

Khi bạn thực hiện một lệnh PING, một trong 4 tình huống sẽ xảy ra, mỗi một tình huống trong đó đều có ý nghĩa của riêng nó.

Tình huống đầu tiên có thể xảy ra là máy được chỉ định sẽ tạo ra 4 phản hồi. Điều đó chỉ thị rằng máy trạm hoàn toàn có thể truyền thông với host được chỉ định ở mức TCP/IP.

Tình huống thứ hai có thể xuất hiện là tất cả 4 yêu cầu time out, như thể hiện trong hình B. Nếu bạn quan sát trình hình A, bạn sẽ thấy rằng mỗi đáp trả đều kết thúc bằng TTL=128. TTL là viết tắt của Time To Live. Nó có nghĩa rằng mỗi một trong 4 truy vấn và đáp trả phải được hoàn thiện trong khoảng thời gian 128 ms. TTL cũng được giảm mỗi lần khi bước nhảy trên đường trở về. Bước nhảy xuất hiện khi một gói dữ liệu chuyển từ một mạng này sang một mạng khác. Chúng tôi sẽ nói thêm về các bước nhảy trong phần sau của loại bài này.



```
Command Prompt
C:\Documents and Settings\Administrator.FUBAR>ping 147.100.100.0
Pinging 147.100.100.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 147.100.100.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator.FUBAR>
```

Hình B: Nếu tất cả các yêu cầu đều bị time out thì điều đó nói lên rằng truyền thông giữa hai địa chỉ này bị thất bại

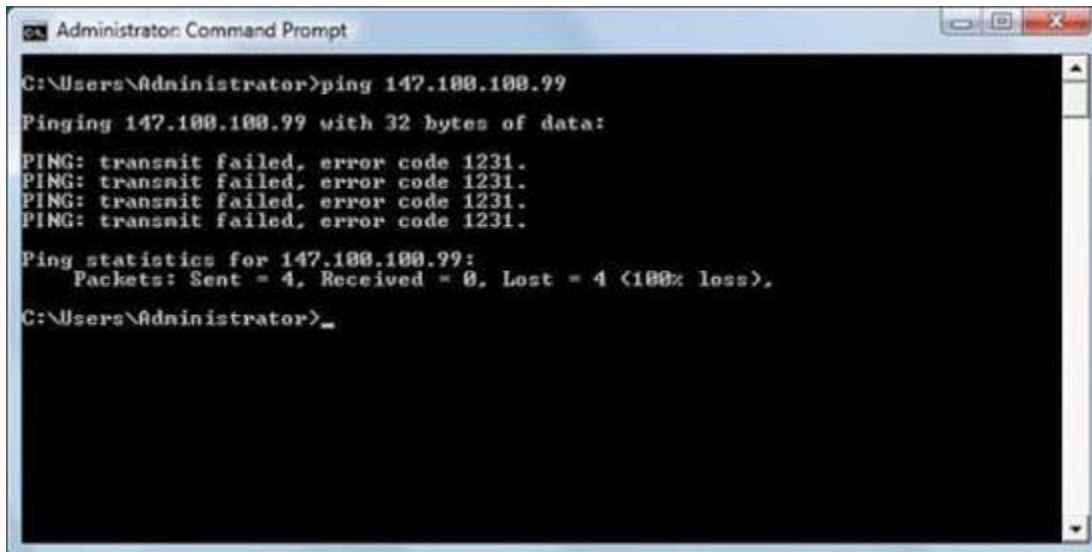
Bất cứ tốc độ nào, nếu tất cả 4 yêu cầu đều bị time out, thì điều đó có nghĩa rằng TTL bị hết hiệu lực trước khi phản hồi được nhận. Điều này có nghĩa một trong ba ý sau:

- Các vấn đề của truyền thông sẽ cản trở các gói truyền tải giữa hai máy. Điều này có thể do hiện tượng đứt cáp hoặc bảng định tuyến bị tỗi, hoặc một số lý do khác.
- Truyền thông xuất hiện, nhưng quá chậm đối trong phức đáp. Điều này có thể bị gây ra bởi sự tắc nghẽn trong mạng, bởi phần cứng hay vấn đề chạy dây của mạng bị lỗi.
- Truyền thông vẫn hoạt động nhưng tường lửa lại khóa lưu lượng ICMP. PING sẽ không làm việc trừ khi tường lửa của máy đích (và bất kỳ tường lửa nào giữa hai máy) cho phép ICMP echo.

Tình huống thứ ba có thể xảy ra khi bạn nhập vào lệnh PING là vẫn nhận được một số phản hồi nhưng một số khác time out. Điều này có thể là do cáp mạng tỗi, phần cứng lỗi hoặc hiện tượng tắc nghẽn trong mạng.

Tình huống thứ tư có thể xuất hiện khi ping là một thông báo lỗi giống như

những gì thể hiện trên hình C.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following text:

```
C:\Users\Administrator>ping 147.100.100.99
Pinging 147.100.100.99 with 32 bytes of data:
PING: transmit failed, error code 1231.
PING: transmit failed, error code 1231.
PING: transmit failed, error code 1231.
PING: transmit failed, error code 1231.

Ping statistics for 147.100.100.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>_
```

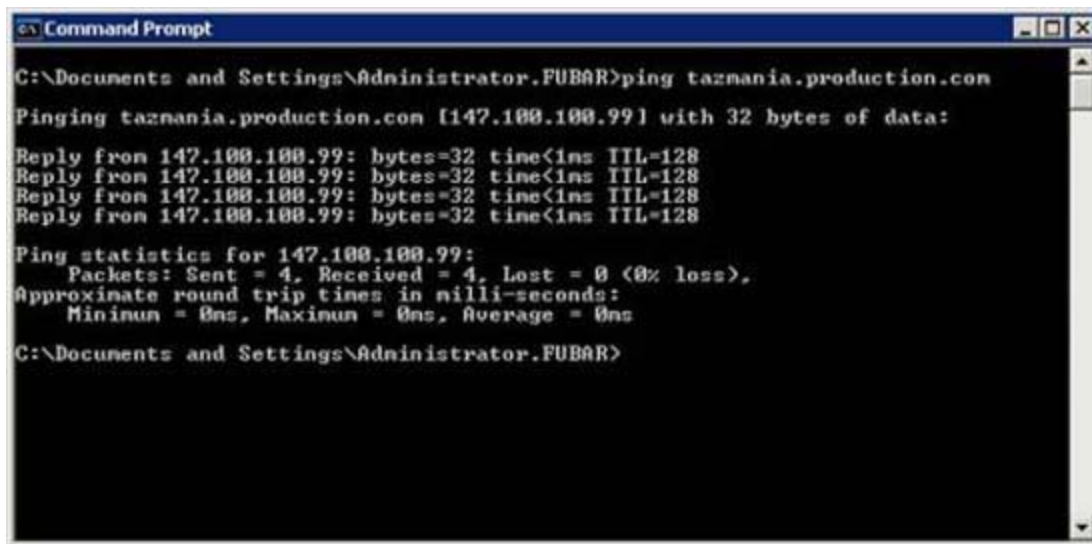
Hình C: Lỗi chỉ thị rằng TCP/IP không được cấu hình đúng

Lỗi “PING: Transmit Failed” chỉ thị rằng TCP/IP không được cấu hình đúng trên máy tính bạn đang nhập vào lệnh PING. Lỗi này xuất hiện trong Windows Vista. Các phiên bản Windows cũ hơn cũng sinh ra một lỗi khi TCP/IP bị cấu hình sai, nhưng thông báo lỗi được hiển thị là “Destination Host Unreachable”.

PING thành công sẽ như thế nào?

Tin tưởng hay không, một ping thành công không phải là một hiện tượng lạ, thậm chí nếu hai máy có vấn đề truyền thông với nhau. Nếu xảy ra điều này, thì có nghĩa rằng cơ sở hạ tầng mạng bên dưới vẫn tốt và các máy tính vẫn có thể truyền thông với nhau ở mức TCP/IP. Thường thì đây vẫn là một dấu hiệu tốt vì vấn đề đang xuất hiện không quá nghiêm trọng.

Nếu truyền thông giữa hai máy bị thất bại nhưng hai máy có thể PING với nhau thành công (khi thực hiện lệnh PING từ hai máy), thì có một vấn đề khác bạn có thể thử ở đây. Thay cho việc ping đến một host bởi địa chỉ IP, bạn hãy thay thế địa chỉ IP bằng tên miền hoàn chỉnh của nó, xem thể hiện trong hình D.



```
C:\Documents and Settings\Administrator\FUBAR>ping tazmania.production.com
Pinging tazmania.production.com [147.188.188.99] with 32 bytes of data:
Reply from 147.188.188.99: bytes=32 time<1ms TTL=128
Reply from 147.188.188.99: bytes=32 time<1ms TTL=128
Reply from 147.188.188.99: bytes=32 time<1ms TTL=128
Reply from 147.188.188.99: bytes=32 time<1ms TTL=128

Ping statistics for 147.188.188.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator\FUBAR>
```

Hình D: Thử ping host của mạng bằng tên miền hoàn chỉnh

Nếu bạn có thể ping bằng địa chỉ IP, nhưng không ping được bằng tên miền hoàn chỉnh thì vấn đề có thể là ở DNS. Máy trạm có thể được cấu hình sử dụng máy chủ DNS sai, hoặc máy chủ DNS có thể gồm một host record cho máy mà bạn đang muốn ping đến.

Nếu nhìn vào hình D, bạn có thể thấy rằng địa chỉ IP của máy được liệt kê bên phải tên miền hoàn chỉnh. Điều này chứng tỏ rằng máy tính có thể chuyển sang một tên miền hoàn chỉnh. Bảo đảm rằng địa chỉ IP mà tên được chuyển sang là chính xác. Nếu bạn thấy một địa chỉ IP khác so với địa chỉ mong đợi thì có thể host record của DNS bị lỗi.

Kết luận

Bài này đã giới thiệu cho các bạn một số bước cơ bản để test kết nối cơ bản giữa hai máy tính. Trong phần tiếp theo, chúng tôi sẽ giới thiệu một số kỹ thuật để các bạn sử dụng trong quá trình khắc phục sự cố.

Khắc phục sự cố các vấn đề kết nối trong mạng (Phần 2)

Nguồn : quantrimang.com

Brien M. Posey

Quản Trị Mạng - Trong phần thứ nhất, chúng tôi đã giới thiệu cho các bạn cách sử dụng lệnh PING để thực hiện những bài test cơ bản cho kết nối, bên cạnh đó là giới thiệu về cách làm sáng tỏ các kết quả. Trong phần hai, chúng tôi sẽ tiếp tục giới thiệu cho các bạn một số bài test đơn giản hơn để bạn có thể sử dụng nhằm chuẩn đoán trạng thái của kết nối hiện hành.

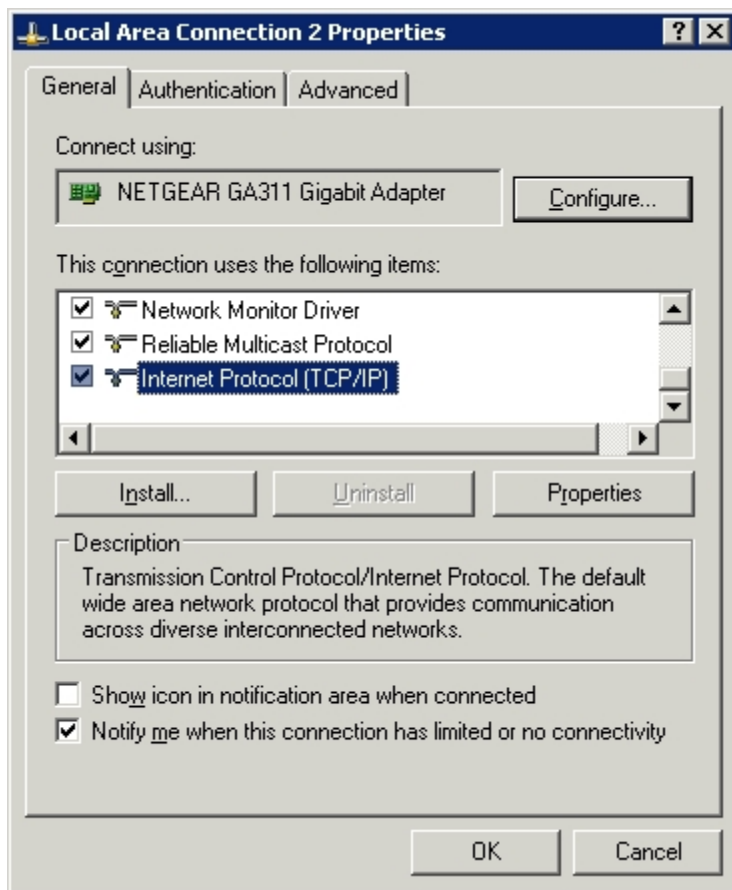
Trước khi bắt đầu

Như đã giải thích trong phần thứ nhất của loạt bài này, mục đích của loạt bài này là tạo một hướng dẫn khắc phục sự cố cho những người mới có các kỹ năng cơ bản. Chính vì vậy chúng tôi sẽ bắt đầu bằng các kỹ thuật khắc phục sự cố cơ bản và dần dần sẽ chuyển sang các kỹ thuật cao hơn.

Xác nhận kết nối

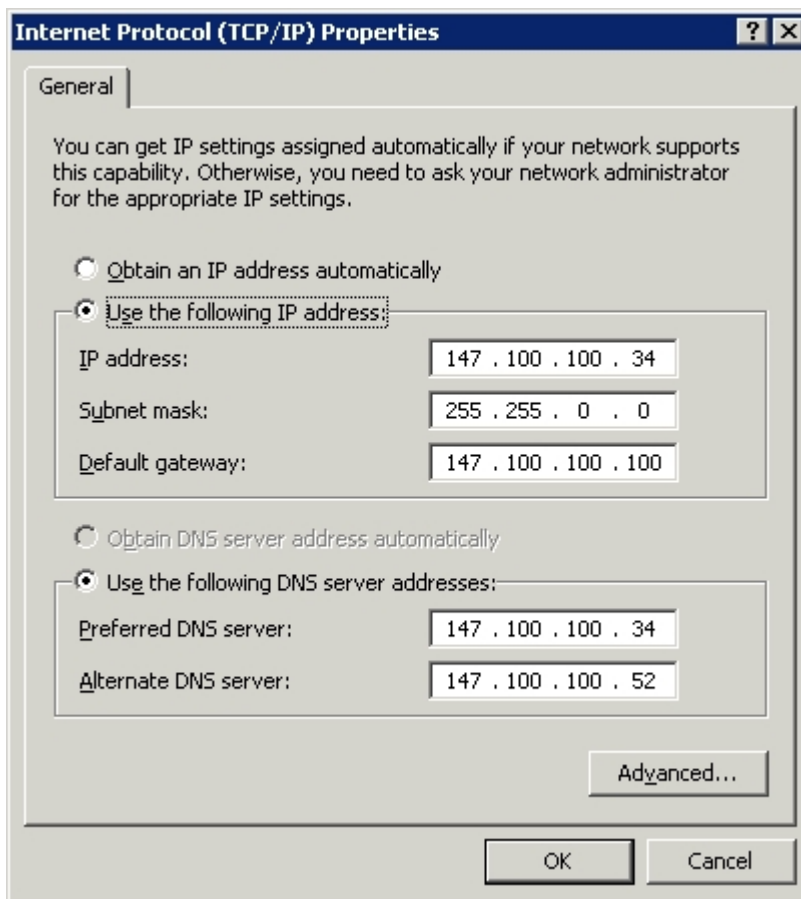
Trong phần trước, chúng tôi đã giới thiệu một số vấn đề cơ bản trong sử dụng lệnh PING để test kết nối mạng. Mặc dù vậy, nếu bạn gặp phải vấn đề truyền thông với các host khác trong mạng, hoặc các host trong mạng từ xa thì vẫn còn đó một số kiểu PING khác để bạn có thể phát hiện được những gì đang xảy ra với mạng của mình.

Trước khi giới thiệu những kỹ thuật này, các bạn cần phải hiểu về cách cấu hình của các host đang gặp phải vấn đề về truyền thông như thế nào. Thủ tục test ở đây khác nhau đối với các phiên bản Windows khác nhau, chính vì vậy chúng tôi sẽ giới thiệu cách kiểm tra cấu hình mạng trên một máy tính đang chạy hệ điều hành Windows Server 2003. Thứ đầu tiên mà bạn phải thực hiện là phải xác định xem máy tính hiện đang chạy một cấu hình địa chỉ IP tĩnh hay động. Để thực hiện điều đó, bạn hãy mở Control Panel, sau đó chọn tùy chọn Network Connections. Kích chuột phải vào kết nối mà bạn muốn chuẩn đoán, chọn lệnh Properties. Bằng cách thực hiện các thao tác đó, bạn sẽ thấy một trang thuộc tính của kết nối xuất hiện như thể hiện trong hình A.



Hình A: Trang thuộc tính của kết nối mạng

Lúc này, hãy cuộn thanh danh sách các mục mà kết nối sử dụng cho tới khi tìm được mục TCP/IP protocol (đã được chọn trong hình A). Chọn giao thức này, sau đó kích nút Properties để xuất hiện trang thuộc tính Internet Protocol (TCP/IP) Properties, xem thể hiện trong hình B.



Hình B: Trang Internet Protocol (TCP/IP) Properties được sử dụng để cấu hình giao thức TCP/IP

Khi bạn gặp màn hình này, hãy để ý đến cấu hình địa chỉ IP của máy tính. Đặc biệt bạn cần phải lưu ý đến một số mục sau:

- Máy tính sử dụng cấu hình động hay tĩnh?
- Nếu cấu hình tĩnh đang được sử dụng thì địa chỉ IP, subnet mask, và default gateway là gì?
- Máy tính có nhận địa chỉ máy chủ DNS tự động hay không?
- Nếu địa chỉ máy chủ DNS đang được chỉ định bằng một địa chỉ cụ thể thì địa chỉ đang được sử dụng là gì?

Trước khi đi tiếp, chúng tôi muốn đề cập đến một vấn đề đó là, nếu một máy tính có nhiều adapter mạng được cài đặt, khi đó sẽ có nhiều kết nối mạng được liệt kê trong Control Panel. Chính vì vậy bạn cần biết được kết nối nào tương ứng với adapter mạng nào.

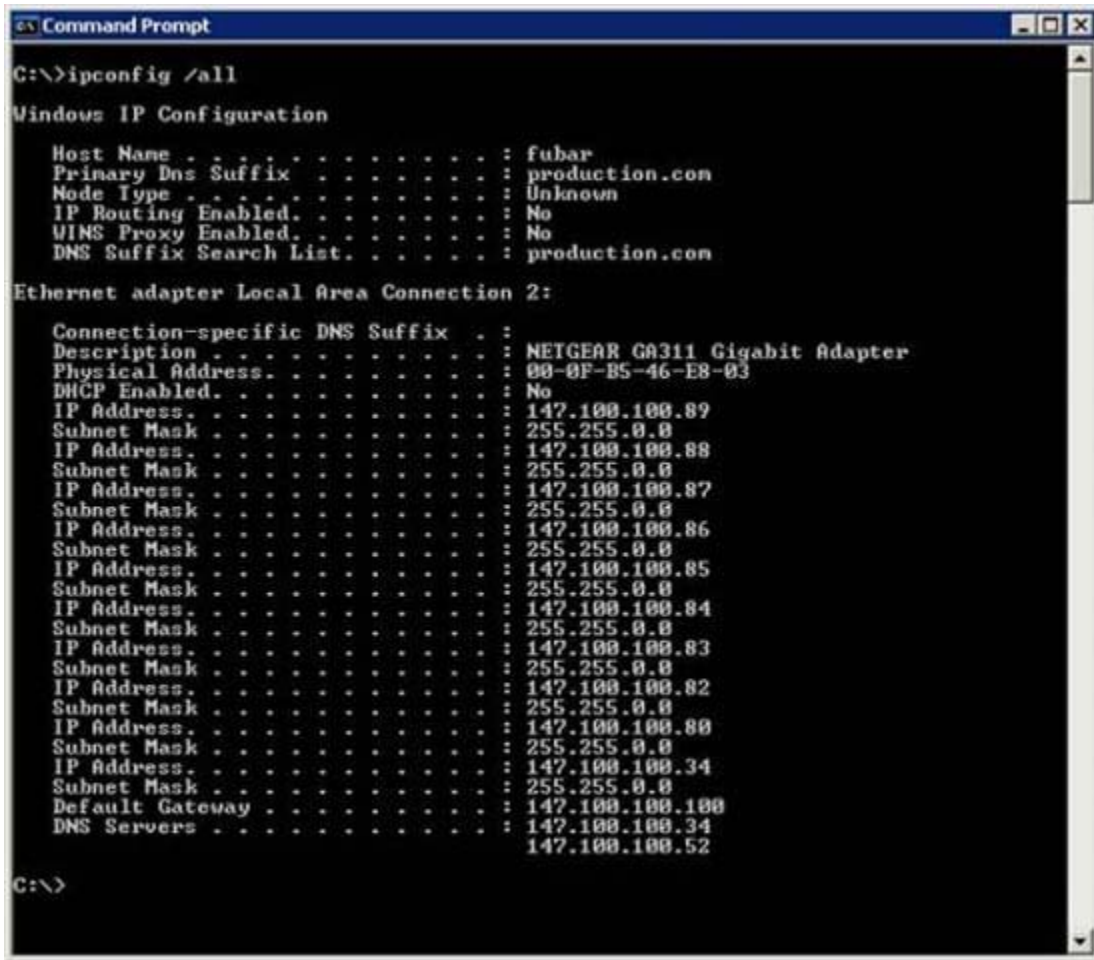
Nếu bạn nghi ngờ về sự tương ứng giữa một kết nối nào đó với adapter mạng, hãy kiểm tra kiểu của adapter đó. Nếu quan sát trong hình A, bạn sẽ thấy kiểu adapter mạng được liệt kê ở phần đỉnh của màn hình. Nếu cần, bạn có thể mở

case của máy tính để xem adapter mạng nào mà cáp mạng của bạn được kết nối đến, làm như vậy bạn có thể chắc chắn về kết nối mạng đúng của mình.

Khi bạn đã biết được cách TCP/IP được cấu hình như thế nào cho adapter mạng, chúng ta phải xác định xem Windows có nhận biết về cấu hình đó hay không. Để thực hiện điều này, hãy mở cửa sổ lệnh và nhập vào lệnh dưới đây:

IPCONFIG /ALL

IPCONFIG thực sự có thể cho bạn biết được rất nhiều những gì đang diễn ra. Cho ví dụ, hãy để ý màn hình thể hiện trong hình C. Khi bạn nhập vào lệnh *IPCONFIG /ALL*, thứ đầu tiên mà bạn phải thực hiện là tìm đến đúng adapter mạng. Trong trường hợp này, việc tìm đến đúng adapter là một điều hoàn toàn dễ dàng vì chỉ có một adapter được liệt kê trong danh sách. Lưu ý rằng *IPCONFIG* cũng có thể cung cấp cho bạn số kết nối (trường hợp này là kết nối số 2 - Ethernet adapter Local Area Connection 2). Nếu để ý trong hình A, bạn sẽ thấy tiêu đề của trang thuộc tính thể hiện trong hình cũng có cùng tên. Kèm với mô tả của adapter mạng vật lý sẽ cho bạn biết chính xác bạn đang xem xét kết nối mạng nào.



Hình C: Lệnh IPCONFIG /ALL hiển thị cho bạn cấu hình IP của máy tính

Rõ ràng thứ đầu tiên mà bạn có thể thấy trong hình C là có rất nhiều địa chỉ IP khác nhau của kết nối. Lý do cho điều này là chúng tôi đã tạo một screenshot trên một Web server. Web server cấu hình nhiều website, mỗi một website lại có địa chỉ IP của riêng nó. Chúng tôi muốn sử dụng máy chủ này để minh chứng một điểm rằng, cấu hình địa chỉ IP mà bạn thấy khi bạn mới quan sát trên trang thuộc tính của TCP/IP không phải luôn là địa chỉ mà Windows đang sử dụng. Trong trường hợp này, thông tin cấu hình của IP được thể hiện trong hình B vẫn hợp lệ. Nó đóng vai trò như một địa chỉ IP chính của máy tính. Tuy nhiên, vẫn có nhiều địa chỉ IP khác cũng vẫn có thể sử dụng.

Bước tiếp theo trong quá trình khắc phục sự cố có nhiều thay đổi và phụ thuộc vào máy tính hiện có đang sử dụng cấu hình địa chỉ động hay tĩnh. Nếu nó sử dụng cấu hình tĩnh thì lúc này bạn hãy kiểm tra để bảo đảm rằng địa chỉ IP, subnet mask, default gateway, và địa chỉ DNS server đều được liệt kê phù hợp với những gì được nhập vào trong trang thuộc tính TCP/IP.

Trong trường hợp sử dụng địa chỉ IP động mà bạn muốn xem địa chỉ IP và xem

xem nó có nằm trong dải địa chỉ mong đợi hay không. Nếu phải khắc phục sự cố cho vấn đề trên một mạng không thân thuộc, trường hợp này bạn có thể sẽ không biết được dải địa chỉ của nó là gì. Nếu rơi vào tình huống này, có một số giá trị có ý nghĩa mà bạn có thể tìm kiếm ở đây.

Manh mối rõ ràng nhất một vấn đề nào đó sai lạc là một địa chỉ IP có giá trị 0.0.0.0. Sự hiện hữu của địa chỉ IP này thường chỉ thị một trong ba vấn đề sau:

Adapter mạng không được kết nối với mạng (có thể vì cáp mạng hoặc tiếp xúc ở cổng).

Địa chỉ IP bị phóng thích.

Xuất hiện hiện tượng xung đột địa chỉ IP.

Nếu bạn nhận được địa chỉ này, hãy thử nhập vào ba lệnh dưới đây:

```
IPCONFIG /RELEASE  
IPCONFIG /RENEW  
IPCONFIG /ALL
```

Các lệnh này cơ bản sẽ thông báo cho máy tính bỏ địa chỉ hiện hành của nó, và tìm lại một địa chỉ IP mới, sau đó sẽ hiện cho bạn các thông tin cấu hình mới. Đôi khi quá trình này cũng khắc phục được vấn đề, nhưng đôi khi cũng không khắc phục được. Tuy nhiên dấu sao nó cũng mang lại những manh mối gây ra vấn đề kết nối mạng của bạn.

Một vấn đề khác có thể làm lỗi hệ thống của bạn là địa chỉ IP nằm trong dải 169.254.x.x nhưng lại có subnet mask là 255.255.0.0. Một số phiên bản Windows sẽ tự động sử dụng địa chỉ này nếu địa chỉ IP không thể tìm thấy từ máy chủ DHCP.

Kết luận

Trong phần này, chúng tôi đã giới thiệu cho các bạn cách kiểm tra cấu hình địa chỉ IP của một máy tính để tìm ra những manh mối gây ra vấn đề. Trong phần tiếp theo của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn cách sử dụng các thông tin cấu hình để test kết nối mạng.

Khắc phục sự cố các vấn đề kết nối trong mạng (Phần 3)

Nguồn : quantrimang.com

Brien M. Posey

Quản trị mạng - Trong phần trước của loạt bài này, chúng tôi đã giới thiệu cho các bạn cách phân biệt địa chỉ IP nào hệ thống của bạn đang sử dụng với tư cách là địa chỉ chính. Bước tiếp theo trong quá trình là thẩm định cấu hình địa chỉ IP có làm việc chính xác và không xuất hiện vấn đề nào đối với ngăn xếp giao thức TCP/IP hay không.

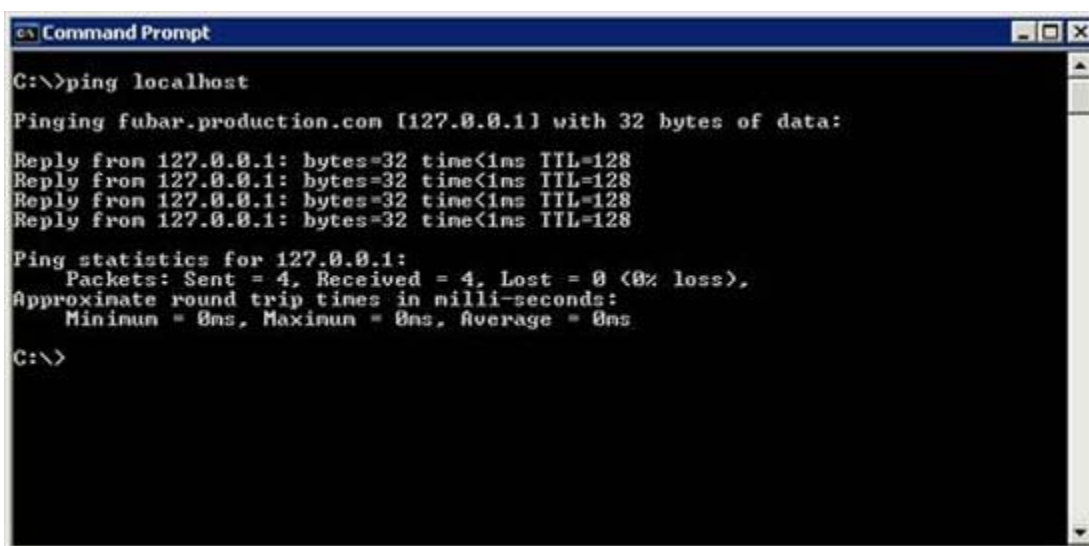
Bài test đầu tiên mà bạn cần thực hiện là ping một địa chỉ host nội bộ. Ở đây có một số cách khác nhau để có thể thực hiện nhiệm vụ này. Cách thứ nhất là nhập lệnh dưới đây:

PING LOCALHOST

Khi nhập vào lệnh này, Windows sẽ ping đến địa chỉ 127.0.0.1. Không quan tâm đến địa chỉ IP của máy bạn, Windows luôn sử dụng địa chỉ 127.0.0.1 như một địa chỉ host nội bộ. Chính vì vậy, giải pháp khác thay thế cho lệnh trên là nhập vào lệnh dưới đây:

Ping 127.0.0.1

Sau khi nhập vào lệnh này, bạn sẽ thấy một quá trình ping thành công giống như các lệnh ping khác. Hãy xem ví dụ thể hiện trong hình A.



```
C:\>ping localhost

Pinging fubar.production.com [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Hình A: Bạn sẽ nhận được một ping thành công khi thực hiện ping địa chỉ host

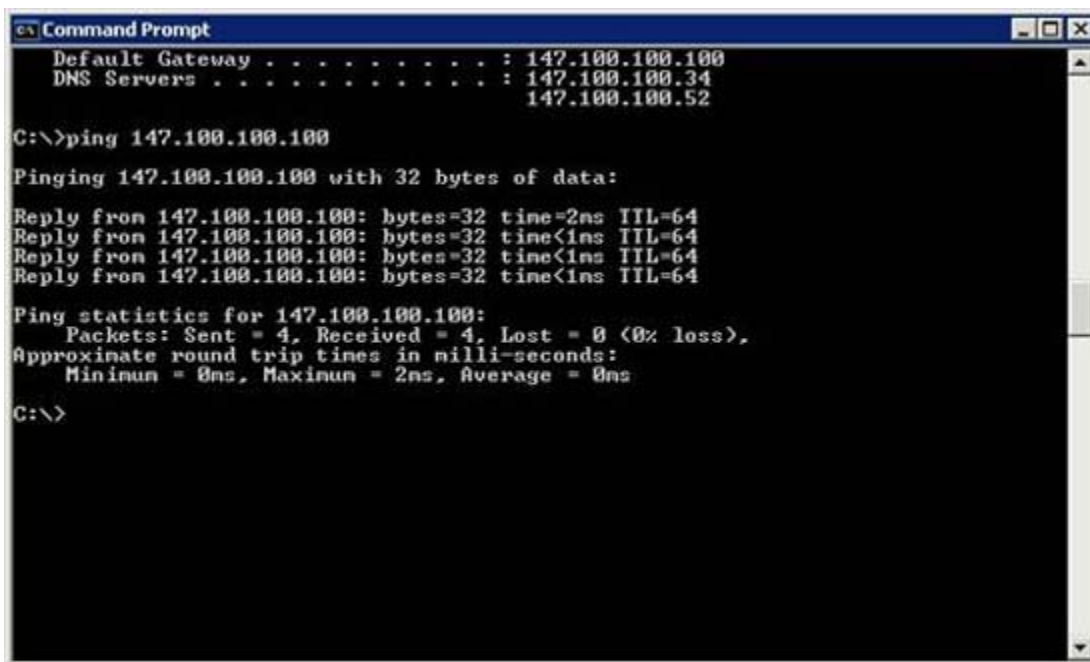
nội bộ

Việc ping địa chỉ host nội bộ không có tác dụng gì trong việc chuẩn đoán các vấn đề truyền thông với host ở xa. Mặc dù vậy nó lại cho phép bạn xác nhận rằng ngăn xếp TCP/IP nội bộ của bạn đang thực hiện đúng chức năng. Nếu bạn ping địa chỉ host nội bộ và nhận được một thông báo lỗi cho biết không xác nhận được đích thì trường hợp này TCP/IP đã bị cấu hình sai hoặc một phần nào đó của ngăn xếp TCP/IP nội bộ bị hỏng.

Ping Gateway mặc định

Trong phần trước của loạt bài này, chúng tôi đã đề cập rằng, có một số khía cạnh khác nhau đối với việc cấu hình TCP/IP và trang bị một chút kiến thức khắc phục sự cố. Bên cạnh đó là một số thông tin hoặc địa chỉ IP của Gateway mặc định và của máy chủ DNS chính.

Giả dụ rằng các host mà bạn muốn truyền thông nằm trên một mạng từ xa, hoặc trên một đoạn mạng khác của công ty bạn thì điều tiếp theo mà bạn cần thực hiện là ping Gateway mặc định. Bạn có thể thực hiện thao tác này bằng cách gắn thêm địa chỉ IP của cổng mặc định vào lệnh ping. Cho ví dụ, quan sát trong hình B bạn sẽ thấy rằng cấu hình TCP/IP liệt kê địa chỉ Gateway mặc định là 147.100.100.100. Chúng tôi đã ping đến địa chỉ này. Thao tác này đã thẩm định rằng máy nội bộ có thể truyền thông với Gateway mặc định. Nó cũng cho bạn biết rằng sự truyền thông trên mạng nội bộ hiện đang làm việc như dự định, chỉ ít cũng ở mức địa chỉ IP.



```
Command Prompt
Default Gateway . . . . . : 147.100.100.100
DNS Servers . . . . . : 147.100.100.34
                       147.100.100.52

C:\>ping 147.100.100.100

Pinging 147.100.100.100 with 32 bytes of data:

Reply from 147.100.100.100: bytes=32 time=2ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64

Ping statistics for 147.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

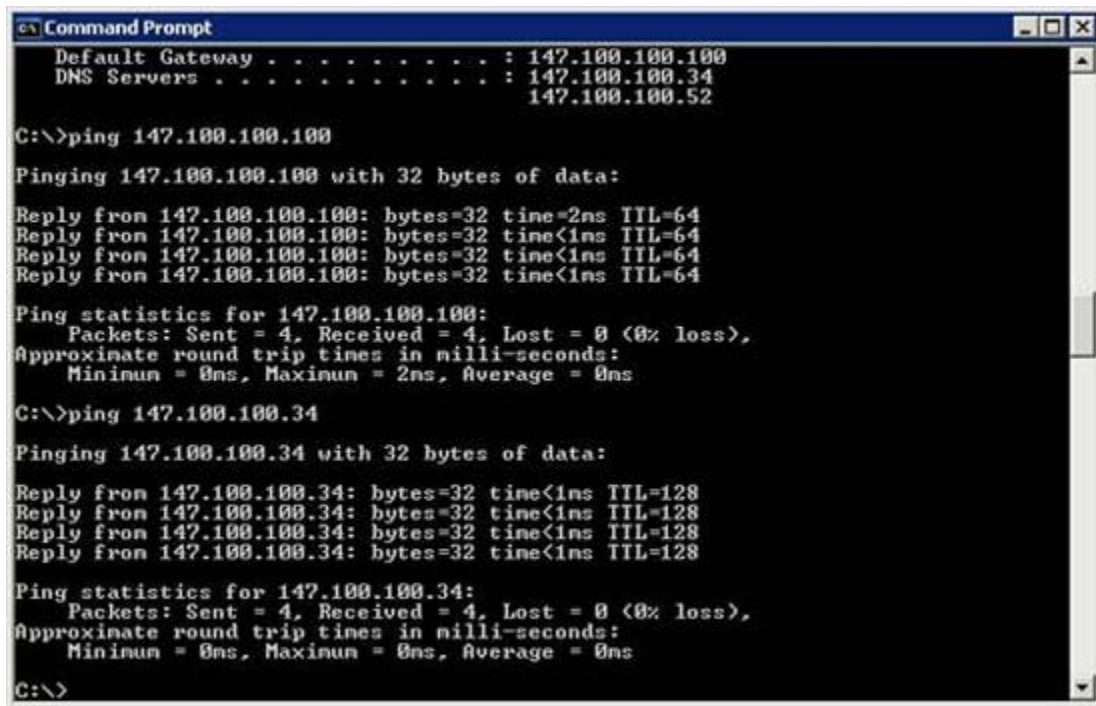
Hình B: Ping gateway mặc định đã thẩm định được rằng các gói IP có thể đến

được
cổng mặc định của mạng.

Ping DNS Server

Cho đến đây, chúng ta đã xác minh được rằng truyền thông ở mức địa chỉ IP hiện đang làm việc giữa máy tính nội bộ và Gateway mặc định. Mặc dù vậy điều này vẫn không bảo đảm rằng các hostname hiện đang thể hiện các địa chỉ IP. Trong phần thứ nhất của loạt bài này, chúng tôi đã giới thiệu cho các bạn về cách sử dụng tên miền đầy đủ của host đích kết hợp với lệnh ping để thẩm định rằng máy chủ DNS hiện đang thực hiện công việc của nó. Tuy nhiên ở đây còn có một số cách khác để dàng test DNS.

Một thứ bạn có thể thực hiện ở đây là ping đến địa chỉ IP của máy chủ DNS, xem thể hiện trong hình C. Tuy thao tác này không bảo đảm DNS hiện có làm việc đúng cách hay không nhưng nó cũng thẩm định được rằng máy tính nội bộ có thể truyền thông với máy chủ DNS.



```
Command Prompt
Default Gateway . . . . . : 147.100.100.100
DNS Servers . . . . . : 147.100.100.34
                       147.100.100.52

C:\>ping 147.100.100.100

Pinging 147.100.100.100 with 32 bytes of data:

Reply from 147.100.100.100: bytes=32 time=2ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64
Reply from 147.100.100.100: bytes=32 time<1ms TTL=64

Ping statistics for 147.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 147.100.100.34

Pinging 147.100.100.34 with 32 bytes of data:

Reply from 147.100.100.34: bytes=32 time<1ms TTL=128
Reply from 147.100.100.34: bytes=32 time<1ms TTL=128
Reply from 147.100.100.34: bytes=32 time<1ms TTL=128
Reply from 147.100.100.34: bytes=32 time<1ms TTL=128

Ping statistics for 147.100.100.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Hình C: Bạn cần thẩm định rằng host có thể truyền thông với máy chủ DNS

Một vấn đề khác nữa bạn có thể thực hiện là sử dụng lệnh Nslookup để thẩm định rằng DNS đang làm việc đúng cách. Để thực hiện theo thao tác này, bạn chỉ cần nhập vào lệnh Nslookup, sau đó là tên miền đầy đủ của host từ xa. Lệnh Nslookup có thể phân tích tên miền hoàn chỉnh thành địa chỉ IP, xem thể hiện trong hình D.



```
C:\>nslookup brienposey.com
*** Can't find server name for address 147.100.100.34: Non-existent domain
Server: Unknown
Address: 147.100.100.34

Non-authoritative answer:
Name: brienposey.com
Address: 24.235.10.4

C:\>
```

Hình D: Lệnh Nslookup thông báo cho bạn biết DNS server có thể phân giải hostname hay không.

Hình trên có thể khiến bạn một chút bối rối lúc đầu nếu bạn không quen làm việc với Nslookup. Ban đầu, màn hình này sẽ xuất hiện một báo cáo lỗi. Nếu quan sát kỹ hơn bạn sẽ thấy phần thông đầu tiên được trả về nói đến máy chủ DNS nội bộ. Điều này là vì địa chỉ IP được tham chiếu tương xứng với địa chỉ IP của máy chủ DNS. Mặc dù vậy, phần bên dưới các thông tin trả về lại cung cấp cho bạn địa chỉ IP của host mà bạn yêu cầu. Miễn là địa chỉ IP này được liệt kê thì truy vấn DNS của bạn đã thành công.

Nếu quá trình phân giải tên miền thất bại, khi đó có một vấn đề về DNS. Vấn đề thực có thể là một trong số các vấn đề đối với máy chủ DNS. Cho ví dụ, các máy chủ DNS đang chuyển tiếp địa chỉ có thể sai, hoặc máy chủ DNS có thể không truy cập được Internet (mức truy cập cần liên lạc với máy chủ DNS mức cao hơn). Cũng có thể dịch vụ DNS của máy chủ DNS có thể bị ngưng. Các kiểu vấn đề này cũng có thể ảnh hưởng đến các máy khách khác vì nhiều máy khách thường phụ thuộc vào một máy chủ DNS nào đó.

Nếu sự phân giải tên miền DNS thành công thì bạn cần phải thẩm định địa chỉ IP được trả về trong suốt quá trình phân tích. Bạn có thể thực hiện điều này bằng cách so sánh địa chỉ IP được trả về với địa chỉ IP thực mà host từ xa đang sử dụng. Các địa chỉ IP này cần phải tương xứng với nhau, tuy nhiên có một số điều kiện có thể gây ra sự sai lệch, khi đó kết quả truyền thông sẽ bị thất bại.

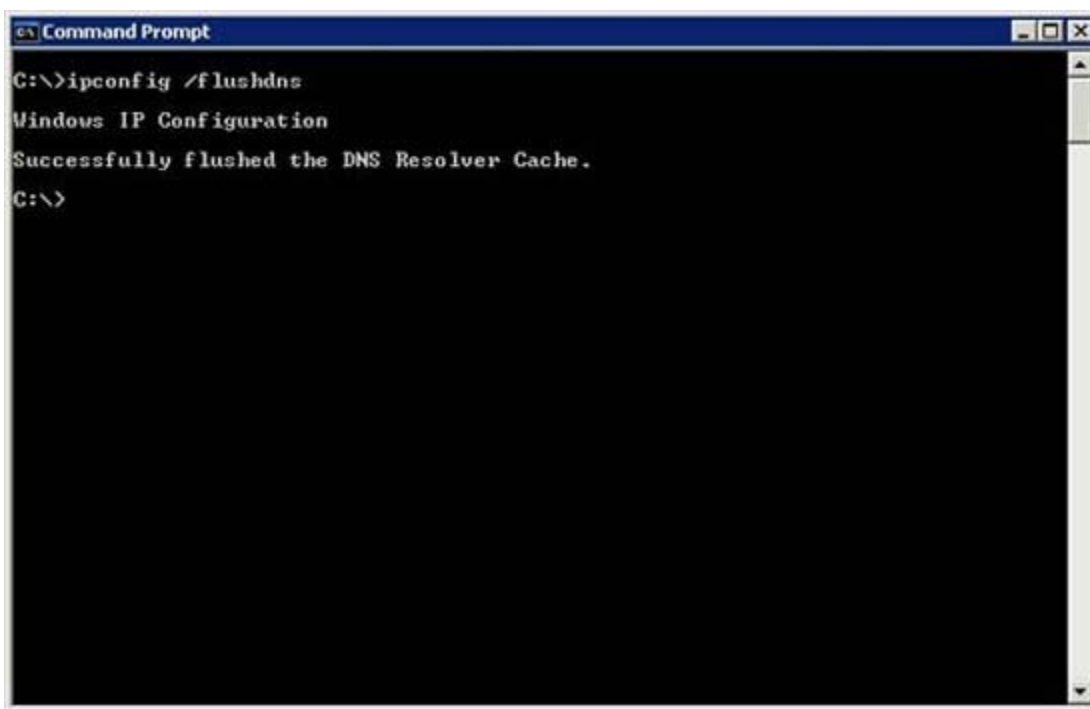
Nếu bạn bắt gặp một sự sai lệch về địa chỉ IP thì điều đó có thể là kết quả của tình trạng bị malware xâm nhập vào máy khách, hoặc có thể là kết quả của sự nhiễm độc của DNS. Sự nhiễm độc DNS là một quá trình trong đó DNS cache sẽ được phổ biến các địa chỉ IP sai hoặc không hợp lệ.

Nếu bạn bắt gặp vấn đề như vậy, chúng tôi khuyên bạn nên quét malware trên máy khách. Bên cạnh đó bạn cũng có thể quét luôn cả spyware và virus vì chúng cũng có thể gây ra vấn đề kiểu như vậy. Khi máy khách hoàn toàn sạch sẽ, hãy làm sạch DNS cache. Bạn có thể làm sạch DNS cache bằng cách nhập vào lệnh dưới đây:

IPCONFIG /FLUSHDNS

Bạn có thể xem ví dụ về lệnh này trong hình E.

Có một lưu ý quan trọng các bạn cần lưu ý ở đây là DNS cache có thể chứa các địa chỉ IP không đúng nhưng nó không có nghĩa rằng DNS bị nhiễm độc. Đôi khi các host được gán các địa chỉ IP mới, điều này làm cho DNS cache đôi khi chưa biết về những thay đổi đó.



```
C:\>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\>
```

Hình E: Nếu bạn nghi ngờ DNS cache chứa các thông tin sai, hãy thực hiện các biện pháp quét và làm sạch Internet

Kết luận

Trong phần này, chúng tôi đã giới thiệu cho các bạn cách thẩm định ngăn xếp

giao thức TCP/IP nội bộ có làm việc đúng hay không. Tiếp đó là giải thích về cách test khả năng của host nội bộ về khả năng liên lạc với máy chủ DNS và máy chủ gateway mặc định và cách test Hostname. Trong phần tiếp theo của loạt này, chúng tôi sẽ giới thiệu cho các bạn về một số vấn đề hay gặp trong sử dụng lệnh Ping, cụ thể là sẽ thảo luận về các vấn đề định tuyến.

Khắc phục sự cố các vấn đề kết nối trong mạng - Phần 4

Nguồn : quantrimang.com

Brien M. Posey

Quản trị mạng - Cho tới đây trong loạt bài này, chúng tôi đã giới thiệu cho các kiểu thao tác để bạn có thể thực hiện đối với lệnh ping để chuẩn đoán các vấn đề kết nối mạng. Trong phần này, chúng tôi sẽ tiếp tục giới thiệu bằng một số biến thể khác của kỹ thuật này.

Mất gói dữ liệu

Khi chúng ta đã sử dụng lệnh ping, cho dù lệnh có có được thực hiện thành công hoặc bị thất bại thì điều đó thực sự vẫn không đáng kể gì. Bạn có thể nhớ lại lệnh ping được thiết kế để trả về bốn đáp trả khác nhau. Đôi khi một hoặc nhiều trong số các đáp trả đó có thể thất bại, còn một số khác có thể thành công. Điều này xảy ra có nghĩa rằng hệ thống đang có hiện tượng bị mất gói dữ liệu.

Trong trường hợp như vậy, host nội bộ và host từ xa hoặc cả hai đều hoạt động tốt, nhưng có thể xuất hiện một số điều kiện khác gây ra hiện tượng mất mát các gói tin trong khi truyền tải. Tuy giao thức TCP/IP được thiết kế để nó có thể thử lại (retry) một gói dữ liệu đã bị mất trong quá trình truyền tải này, tuy nhiên việc mất gói dữ liệu sẽ làm giảm hiệu suất của hệ thống. Một kết nối chậm lúc này sẽ hiệu quả hơn đối với một kết nối tốc độ cao xuất hiện hiện tượng mất gói dữ liệu.

Một thứ khó khăn đối với vấn đề mất gói dữ liệu là việc tìm lần lại được dấu vết của nó. Bạn có thể biết hiện tượng mất gói dữ liệu xảy ra nếu một số đáp trả cho lệnh ping thất bại, nhưng các gói ICMP đã được sử dụng bởi lệnh ping này là quá nhỏ để có thể trả về điều kiện mạng đang tồn tại gây ra hiện tượng mất mát trong các tình huống thực tế.

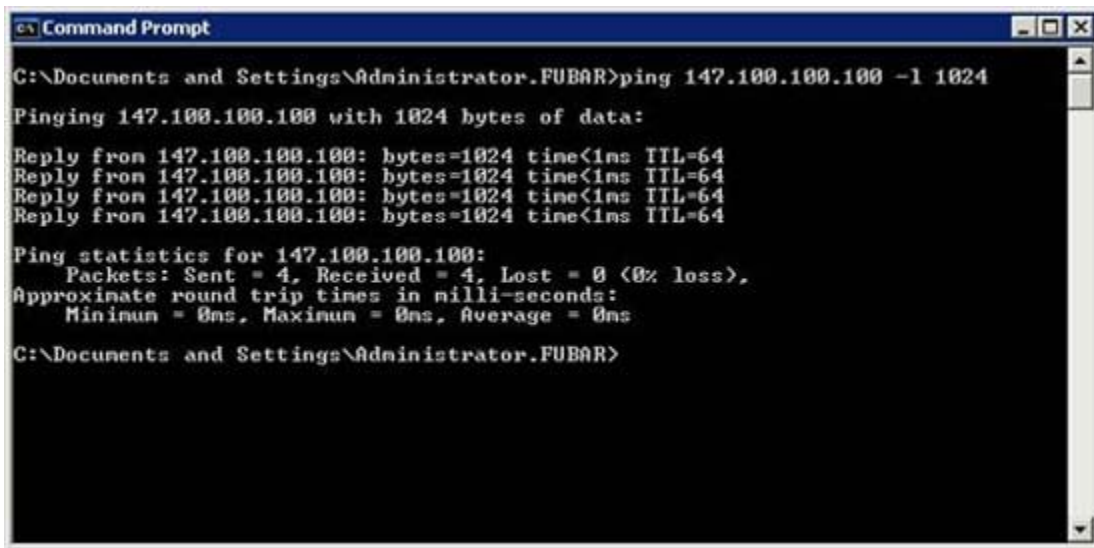
Nếu bạn nghi ngờ hiện tượng mất gói dữ liệu có thể xảy ra nhưng khi ping lại không trả về bất cứ một lỗi nào, khi đó bạn có thể tăng kích thước của các gói ICMP lên. Các gói lớn hơn thường dễ dẫn đến hiện tượng thất bại nếu mạng có vấn đề nào đó đang tồn tại. Bạn có thể đặt kích thước gói lớn hơn trong lệnh ping bằng các sử dụng tiếp lệnh -L.

Việc sử dụng tiếp lệnh này khá đơn giản. Tất cả những gì chúng ta cần phải thực hiện là nhập vào lệnh ping và theo sau là địa chỉ mà bạn muốn ping tới, tiếp đó là tiếp lệnh -L và số byte mà bạn muốn gửi. Cho ví dụ, giả dụ rằng mạng của bạn đang có hiệu suất cực kỳ kém khi kết nối đến một host nào đó. Bạn có thể nghi ngờ lúc này hiện tượng mất gói dữ liệu có thể xảy ra, nhưng khi ping lại cho

các kết quả thành công mỹ mãn. Hãy thực hiện lệnh ping với kích thước của gói dữ liệu là 1024 byte như dưới đây:

Ping 192.168.1.1 -L 1024

Bạn có thể thấy được ví dụ thực về cách làm việc của lệnh này trong hình A.



```
C:\Documents and Settings\Administrator.FUBAR>ping 147.100.100.100 -l 1024
Pinging 147.100.100.100 with 1024 bytes of data:
Reply from 147.100.100.100: bytes=1024 time<1ms TTL=64
Reply from 147.100.100.100: bytes=1024 time<1ms TTL=64
Reply from 147.100.100.100: bytes=1024 time<1ms TTL=64
Reply from 147.100.100.100: bytes=1024 time<1ms TTL=64
Ping statistics for 147.100.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator.FUBAR>
```

Hình A: Gắn lệnh -L vào lệnh ping sẽ cho phép bạn tăng kích thước của gói ICMP

Thời gian sống

Khái niệm tiếp theo mà chúng tôi muốn giới thiệu cho các bạn cũng liên quan đến lệnh ping là thời gian sống (Time To Live, được viết tắt là TTL). Nếu quan sát vào hình A, bạn sẽ thấy ở cuối mỗi một reply trong hình có TTL=64.

Có thể bạn đã biết, Internet gồm có một số lượng lớn các tuyến được kết nối với nhau. Mỗi tuyến được kết nối ít nhất với hai tuyến khác. Ý tưởng ẩn đằng sau kiến trúc này là nếu liên kết có bị "fail" thì vẫn còn ít nhất một đường dẫn khác dẫn đến đích. Vấn đề với kiểu kiến trúc này là khi cứ liên kết nào thất bại thì hiện tượng các gói dữ liệu truyền tải theo các đường vòng vô tận sẽ xuất hiện, và các đường vòng này sẽ vẫn tồn tại trong mạng mà không đến được đích cuối cùng của nó.

Đây chính là vấn đề mà các chuyên gia thiết kế đã đưa vào giá trị TTL. Bạn có thể cho là giá trị TTL như một cơ chế hủy các gói tin. Giá trị này được thiết lập ban đầu khá cao, mặc dù vậy số này có thể thay đổi phụ thuộc vào hệ điều hành mà bạn đang sử dụng. Mỗi lần gói dữ liệu truyền tải qua một router, gói sẽ được nhắc nhở phải thực hiện một bước nhảy. Mỗi khi bước nhảy xuất hiện, giá trị TTL được giảm đi một. Nếu giá trị TTL bằng không thì gói khi đó sẽ bị hủy hoàn

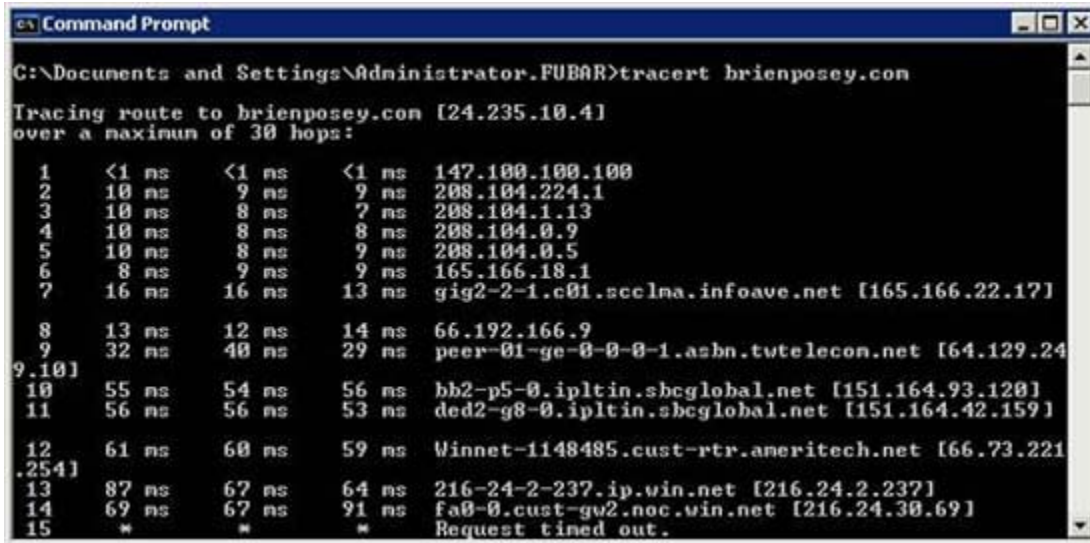
toàn. Điều này giúp tránh được hiện tượng gói dữ liệu không đi đến đích mà cứ luẩn quẩn lưu mãi trên mạng.

Kiểm tra tuyến

Một lý do khác tại sao giá trị TTL lại hữu dụng đến vậy là vì công cụ khắc phục sự cố có tên tracert hoạt động dựa trên nó. Việc sử dụng lệnh ping khá tốt cho việc khắc phục sự cố các mạng nhỏ trong đó có các host từ xa gần các host đang gửi dữ liệu, tuy nhiên khi nói đến Internet hoặc đến mạng diện rộng thì host từ xa có thể là cách đến hàng nghìn dặm. Thêm vào đó các gói ICMP được tạo bởi lệnh ping có thể truyền tải qua rất nhiều router để tới được host từ xa. Chính vì vậy đôi khi bạn sẽ gặp tình huống trong đó host nội bộ và host từ xa hoặc cả hai đều tốt nhưng một trong các router ở đâu đó lại có vấn đề. Để khắc phục vấn đề đó bạn có thể sử dụng lệnh tracert để chuẩn đoán vấn đề của bạn là gì.

Lệnh tracert hoạt động dựa trên lệnh ping. Ý tưởng cơ bản đằng sau lệnh này là gửi đi một gói ICMP đến host từ xa, nhưng với giá trị TTL đã được thiết lập bằng một số nào đó. Điều này làm cho router đầu tiên mà nó gặp phải sẽ gửi trở lại một TTL đã hết hạn trong thông báo truyền tải. Thông báo này gồm có các thông tin như nhận dạng router sinh ra thông báo. Xác minh router được minh chứng, sau đó gói ICMP được gửi lại lần nữa nhưng lúc này với một giá trị TTL khác. Lúc này, gói ICMP đến được router thứ hai trước khi giá trị TTL hết hạn. Quá trình này được lặp đi lặp lại, việc tăng giá trị TTL được thực hiện như vậy cho tới khi đến được host đích. Điều này cho phép bạn có thể biết được các thông tin về các router giữa host nội bộ và host từ xa. Đôi khi bạn còn có thể sử dụng thông tin này để lần các vấn đề của router có ảnh hưởng đến luồng lưu lượng.

Việc sử dụng lệnh tracert cũng giống như sử dụng lệnh ping. Để thực hiện điều đó, bạn chỉ cần nhập vào lệnh tracert, sau đó là địa chỉ IP hoặc tên miền hoàn chỉnh của host từ xa. Hình B thể hiện một trường hợp sử dụng lệnh tracert.



```
C:\Documents and Settings\Administrator.FUBAR>tracert brienposey.com
Tracing route to brienposey.com [24.235.10.4]
over a maximum of 30 hops:
  0  <1 ns    <1 ns    <1 ns    147.100.100.100
  1  10 ns     9 ns     9 ns     208.104.224.1
  2  10 ns     8 ns     7 ns     208.104.1.13
  3  10 ns     8 ns     8 ns     208.104.0.9
  4  10 ns     8 ns     9 ns     208.104.0.5
  5  8 ns      9 ns     9 ns     165.166.18.1
  6  16 ns    16 ns    13 ns    gig2-2-1.c01.scclna.infoave.net [165.166.22.17]
  7
  8  13 ns    12 ns    14 ns    66.192.166.9
  9  32 ns    40 ns    29 ns    peer-01-ge-0-0-1.asbn.tutelecon.net [64.129.24
9.10]
 10  55 ns    54 ns    56 ns    bb2-p5-0.ipltin.sbcglobal.net [151.164.93.120]
 11  56 ns    56 ns    53 ns    ded2-g8-0.ipltin.sbcglobal.net [151.164.42.159]
 12
 13  61 ns    60 ns    59 ns    Winnet-1148485.cust-rtr.ameritech.net [66.73.221
.254]
 14  87 ns    67 ns    64 ns    216-24-2-237.ip.win.net [216.24.2.237]
 15  69 ns    67 ns    91 ns    fa0-0.cust-gw2.noc.win.net [216.24.30.69]
 16  *        *        *        Request timed out.
```

Hình B: Lệnh tracert có thể được sử dụng để giải quyết các vấn đề về luồng lưu lượng

Có hai vấn đề bạn cần lưu ý ở đây trong khi sử dụng lệnh tracert này là: trước tiên là một số host có thể sử dụng tường lửa để khóa các gói ICMP. Vào trường hợp này, bạn sẽ thấy một loạt các dấu hoa thị chỉ thị rằng việc lần tuyến là không thể thực hiện với host vì không thể lấy được thông tin từ host đó.

Một vấn đề khác nằm ở bản thân các host, mỗi router đều được gán một địa chỉ IP. Không quan tâm đến chúng được sử dụng cho các host hay cho router hay không, các địa chỉ IP được cấu trúc theo cách để cho phép chúng phản ánh được vị trí địa lý. Trong thực tế, đôi khi các thông tin về địa lý này hoặc thậm chí các chỉ dẫn về tuyến lại được cung cấp bên trong tracert. Nếu bạn muốn có thêm nhiều thông tin, hãy thử dùng các công cụ của các hãng phần mềm thứ ba, các công cụ có thể theo dõi bằng kiểu đồ thị lệnh tracert dựa trên các thông tin địa lý. Bạn có thể xem ví dụ về một công cụ như vậy trong hình C.



Hình C: Bạn có thể thực hiện một traceroute ảo để xác định vị trí địa lý của host

Kết luận

Trong phần này, chúng tôi đã giới thiệu cho các bạn về cách tăng số lượng byte trong khi sử dụng lệnh ping nhằm làm rõ dấu vết của hiện tượng mất gói dữ liệu. Tiếp đó là giới thiệu về lệnh traceroute. Trong phần tiếp theo của loạt bài này, chúng tôi sẽ tiếp tục thảo luận bằng cách giới thiệu cách thông dịch các kết quả được cho bởi lệnh traceroute.