Lệnh Tracert là gì? Làm thế nào để áp dụng Tracert một cách hiệu quả?

Trên Windows thì các bạn đã có sẵn một số công cụ giúp chúng quản lý và kiểm tra mô hình mạng. Đó là 2 lệnh Ping và Tracert. Cụ thể, chúng giống nhau và khác nhau thế nào? Hãy cùng đọc hết bài viết dưới đây của Quản Trị Mạng.

Về mặt bản chất, chúng đều có thể được dùng khi ta muốn kiểm tra kết nối mạng từ máy đang dùng đến 1 máy chủ nào đó, có tín hiệu mạng hay không. Cụ thể hơn nữa thì:

- **LỆNH PING** : kiểm tra kết nối internet giữa 2 máy tính. Bằng cách gửi đi các gói tin, rồi nhận lại tín hiệu phản hồi từ phía bên kia.
- **Lệnh Tracert** thì có vẻ "cao siêu" hơn 1 chút, dùng để kiểm tra đường đi của các gói tin của lệnh Ping.

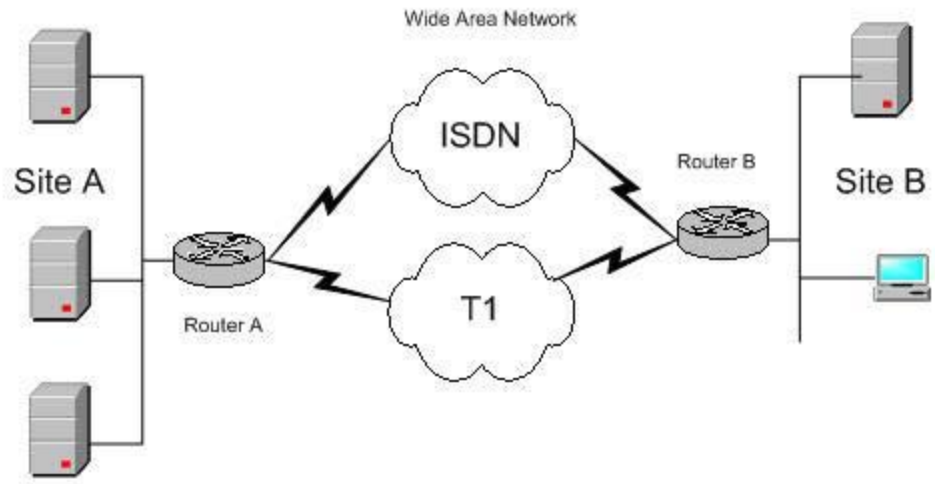
Tracert (hay Traceroute) là công cụ dựa trên nền tảng Windows cho phép bạn hỗ trợ chương trình kiểm tra cơ sở hạ tầng mạng. Trong bài này chúng tôi giới thiệu cách dùng Tracert để sửa chữa các vấn đề gặp trong thực tế. Điều này giúp tăng cường tính hữu ích của công cụ và chỉ cho bạn một số cách dùng khi làm việc với các mạng riêng của mình.

Tiện ích TCP/IP này cho phép bạn xác định các gói định hướng lưu chuyển trong toàn bộ mạng tới host cụ thể theo yêu cầu của bạn. Tracert hoạt động bằng cách tăng thêm giá trị "thời gian sống" (TTL) cho từng gói liên tiếp được gửi đi. Khi một gói đi qua một host, host này sẽ giảm TTL đi một giá trị và tiếp tục gửi nó sang host kế tiếp. Khi một gói có TTL đến được host cần tới, host sẽ loại bỏ gói và gửi thông báo thời gian ICMP quá hạn. Tracert nếu được dùng phù hợp và chính xác có thể giúp bạn tìm ra các điểm định tuyến không chính xác hoặc không tồn tại trong mạng của bạn.

Giới thiệu về Tracert

Tracert là công cụ dòng lệnh nền tảng Windows dùng để xác định đường đi từ nguồn tới đích của một gói Giao thức mạng Internet (IP - Internet Protocol). **Tracert** tìm đường tới đích bằng cách gửi các thông báo Echo Request (yêu cầu báo hiệu lại) Internet Control Message Protocol (ICMP) tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL), tức thời gian cần để gửi đi sẽ được tăng lên cho tới khi gặp đúng đích cần đến. Đường đi được xác định từ quá trình này.

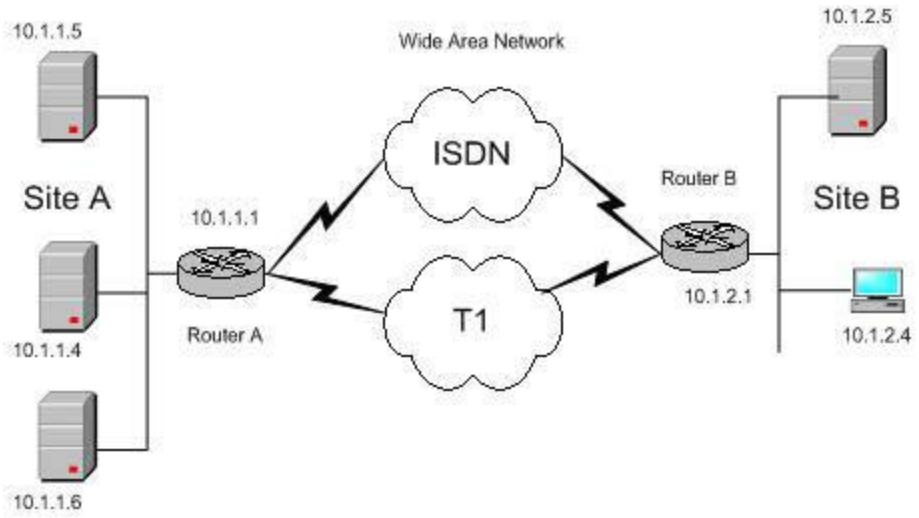
Nhìn vào hình minh hoạ sau bạn có thể hình dung ra được cách thức Tracert hoạt động trong một mạng sản xuất.



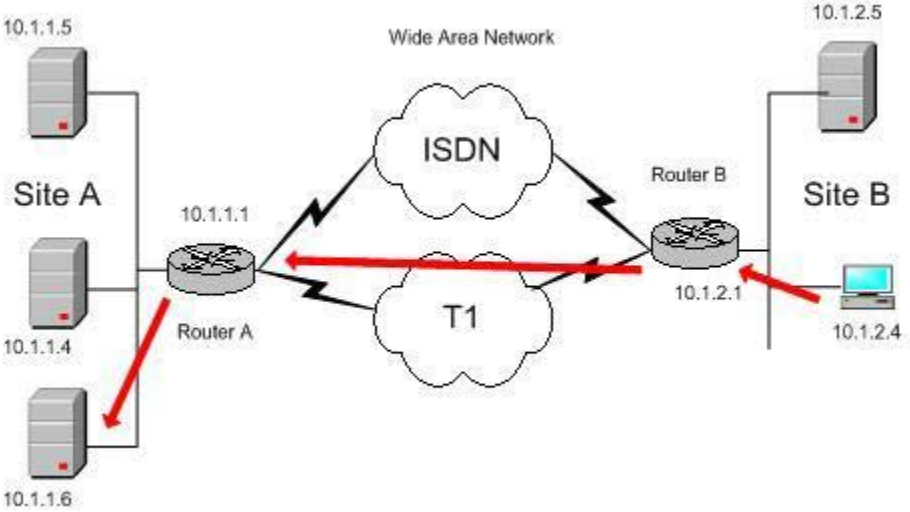
Sử dụng Tracert như thế nào

Như bạn thấy ở hình minh hoạ, chúng ta sẽ gửi lưu lượng từ trạm kiểm tra bên B (Site B) tới một server ở bên A (Site A). Các gói tin sẽ truyền đi trong mạng diện rộng WAN phân tách thành hai phía nối với nhau qua liên kết T1 và một liên kết dự phòng ISDN (Integrated Services Digital Network). Để dùng tiện ích **Tracert**, đơn giản bạn chỉ cần biết địa chỉ IP của máy đích muốn gửi đến, cách sử dụng Tracert chính xác và bạn cần tìm cái gì trong kết quả.

Tracert hoạt động dựa vào thao tác với trường Time to Live (TTL). Bằng cách tăng TTL và sau mỗi lần gặp router, giá trị của nó lại giảm đi một, gói tin được gửi tới router tiếp theo. Mỗi lần gói tin được gửi từ router này đến router khác, người ta gọi là nó đã thực hiện một bước nhảy (hop). Khi trường TTL có giá trị trở về 0, router sẽ gửi thông báo "Time Exceeded" ICMP (hết thời gian) tới máy nguồn. Bạn có thể xem ví dụ với mạng mẫu sau của chúng tôi trong phần minh hoạ bên dưới. Với địa chỉ IP nguồn và đích,… chúng ta sẽ dùng trạm làm việc ở Site B và server bên Site A để thực hiện bài kiểm tra.



Từ minh hoạ này bạn có thể thấy IP nguồn là 10.1.2.4 và IP đích (ví dụ) có thể là 10.1.1.6. Việc định tuyến thông thường diễn ra từ Site B sang Site A, qua liên kết có dung lượng cao hơn là T1 (1.544 Mbqs). Liên kết ISDN có dung lượng 128 Kbqs chỉ được dùng dự phòng trong trường hợp liên kết chính gặp lỗi. **Tracert** sẽ chỉ cho bạn thấy các gói tin được gửi từ Site B, tại máy có địa chỉ 10.1.2.4, qua liên kết T1 tới máy có địa chỉ 10.1.1.1. như thế nào. Bạn còn có thể biết được cách gửi các gói tin tới mạng LAN cục bộ (10.1.1.0) và cuối cùng là 10.1.1.6 như thế nào. Khi các gói tin đã được gửi đi, **Tracert** sẽ dùng giao diện đầu tiên trên router nó nhìn thấy để thông báo lại các bước nhảy router. Vì thế, hãy xem xét toàn bộ đường đi hoàn chỉnh của chúng ta trước khi gửi các gói tin đi.

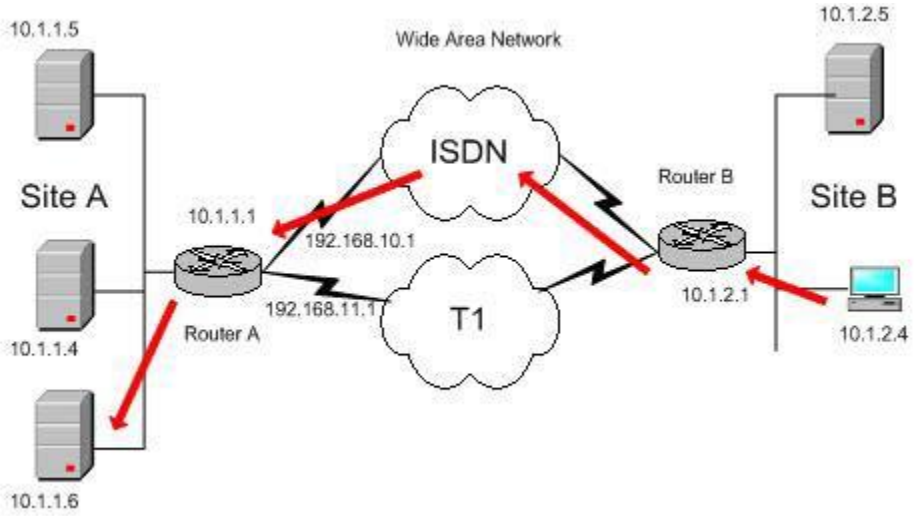


Đường đi (được tô màu đỏ trên hình) là danh sách các router nằm giữa host nguồn và host đích. Một điểm rất quan trọng cần nhớ là các giao diện ở phía bên trái sẽ được dùng khi mô tả. Giao diện bên trái là giao diện của router gần nhất với host gửi tin trong đường đi. Trong ví dụ này bạn có thể thấy đường đi qua T1, từ phía B

(Site B) sang phía A (Site A). Bây giờ chúng ta hãy cùng xem tại sao điều này lại quan trọng.

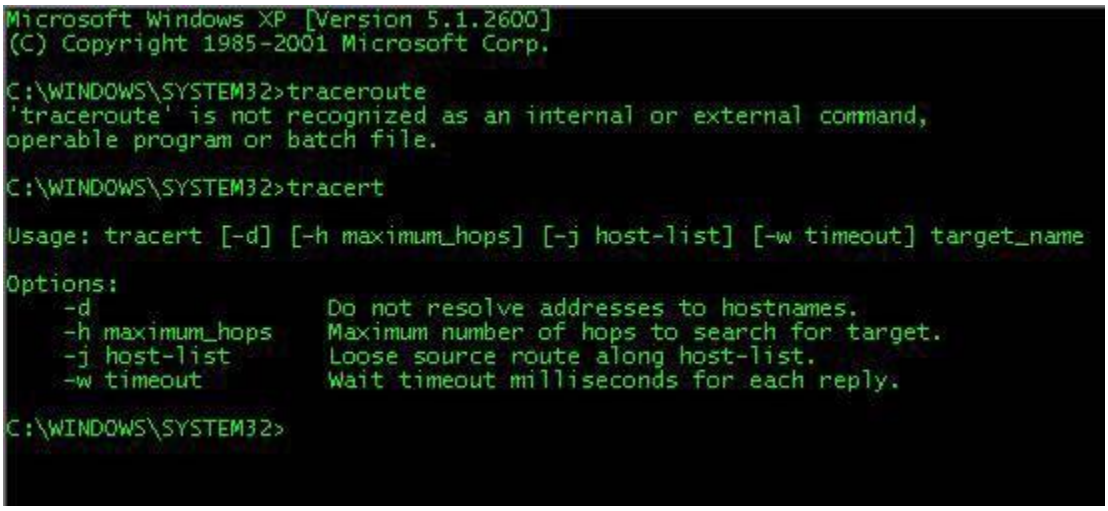
Vậy các cách làm việc của tracert là gì? Khi khởi chạy và sử dụng, tracert sẽ báo cáo (in ra) danh sách đã được sắp xếp các địa chỉ của từng host mà nó đã đi qua trên đường đến đích. Điều này thực sự hay vì bạn có thể biết được nhiều hơn về đường đi này. Nếu bạn thu được phần gần mặt phân cách, bạn sẽ thấy một thiết lập mới của địa chỉ IP trong hình minh họa tiếp theo (192.168.10.1 và 192.168.11.1) 10.1 được sử dụng cho liên kết ISDN và 11.1 sử dụng cho liên kết T1. Vậy tại sao điều này lại quan trọng?

Khi nhận được kết quả từ **Tracert**, một số người không thạo làm việc với công cụ này sẽ thấy lúng túng. Router cổng vào 10.1.1.1 mặc định của Site A được thay thế bằng địa chỉ WAN. Chỉ là một router nhưng giao diện khác. Điều này mang tính chất bắt buộc khi muốn kiểm tra với **Tracert** bởi vì nếu bạn nhầm, bạn sẽ không biết được mình đang đọc gì.
Ví dụ, đường đi bạn thấy ở hình minh hoạ trên là từ 10.1.2.4 tới 10.1.2.1 (cổng vào mặc định của mạng LAN). Sau đó nó sẽ qua mạng WAN tới 10.1.1.1. Chỉ có một vấn đề xuất hiện ở đây là bạn sẽ không thấy địa chỉ xuất hiện. Sau khi T1 có giao diện trên router (11.1) của phía A (Site A) và thực hiện liên kết ISDN (10.1) thì hai địa chỉ IP này là quan trọng nhất trong kết quả trả ra của **Tracert**. Đó là do trong ví dục này T1 có thể bị lỗi và đường đi bây giờ là qua ISDN. Điều này hoạt động "như được công khai hoá". Nhưng chuyện gì sẽ xảy ra nếu bạn để T1 online trở lại (trừ trường hợp bạn cảm thấy tốc độ mạng của mình tại T1 tụt từ 1.544 Mbqs xuống còn 128 Kbqs), bạn không nên dùng liên kết ISDN thêm phút nào nữa. Đó là điều chúng ta sẽ kiểm tra.



Kiểm tra Tracert

Bây giờ, để dùng Tracert, đơn giản bạn chỉ cần mở màn hình lệnh Command Prompt. Để thực hiện điều này, bạn vào ***Start*** -> ***Run*** -> ***cmd*** -> ***tracert*** (*Chú ý*: bạn phải gõ "**tracert**" vì bạn có thể thấy **Traceroute** chỉ hoạt động trên UNIX/Linux và các hệ thống khác như Cisco, v.v…).



Trong ví dụ sau, sau khi gõ lệnh "**tracert**" và xem phần thông tin hiển thị ra bạn có thể thấy các gói di chuyển qua hai router (như ở phần minh họa trên) rồi mới tới host đích 10.1.1.6. Ở đây, cổng vào mặc định từ Site B là 10.1.2.1 và địa chỉ IP của router trên mạng WAN qua các liên kết T1 và ISDN (lần lượt) là 192.168.11.1 và 192.168.10.1.

Đầu tiên chúng ta hãy xem mọi việc diễn ra như thế nào khi dùng T1.

```
C:\>tracert 10.1.1.6
 Tracing route to 10.1.1.6 over a maximum of 30 hops (Xác định đường đi tới địa chỉ 10.1.1.6 qua tối đa 30 bước nhảy)
----------------------------------------------------
1 2 ms 3 ms 2 ms 10.1.2.1
2 25 ms 83 ms 88 ms 192.168.11.1
3 25 ms 79 ms 93 ms 10.1.1.6
Trace complete. ( Quá trình xác định hoàn tất)
```

Bây giờ, nếu T1 bị lỗi và chuyển sang dùng ISDN, bạn sẽ thấy có một 'đường đi' khác và nó 'dài hơn' so với đường đi ban đầu.

```
C:\>tracert 10.1.1.6
Tracing route to 10.1.1.6 over a maximum of 30 hops
----------------------------------------------------
1 2 ms 3 ms 2 ms 10.1.2.1
2 75 ms 83 ms 88 ms 192.168.10.1
```

3 75 ms 79 ms 93 ms 10.1.1.6
Trace complete.

Như bạn thấy, sử dụng **tracert** sẽ giúp bạn xác định rõ được đường dẫn mạng như nó hướng ra ngoài thông qua mạng và quan trọng nhất là làm thế nào để dữ liệu đi qua đường dẫn đó.

Sử dụng các tuỳ chọn Tracert

Dùng **Tracert**, các bạn nên biết một số tuỳ chọn sau. Hữu ích nhất là tuỳ chọn đầu tiên "-d". Nó được dùng khi bạn muốn loại bỏ giải pháp DNS. Các server name (tên máy chủ) cũng rất hữu ích, nhưng nếu nó không được thiết lập hoặc thiết lập sai, hay đơn giản là bạn chỉ muốn có địa chỉ IP của host, bạn nên dùng tuỳ chọn "-d".

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

-d	Ngăn Tracert xử lý địa chỉ IP của các router ở giữa với tên của chúng. Điều này có thể giúp nâng cao tốc độ hiển thị kết của của Tracert.
-h	Số lượng lớn nhất các hop (bước nhảy) trong đường đi đến host đích. Giá trị mặc định là 30 hop
-j	Bạn có thể dùng tuỳ chọn này với một danh sách host (HostList). Các thông báo Echo Request (yêu cầu báo hiệu lại) dùng tuỳ chọn Loose Source Route trong phần header của địa chỉ IP với tập hợp các đích trung gian được mô tả trong HostList. Việc sử dụng tuỳ chọn Loose Source Route giúp các đích trung gian lần lượt được tách riêng bởi môt hoặc nhiều router. Số lượng lớn nhất địa chỉ hay tên trong danh sách host list là 9. HostList là một loạt địa chỉ IP (là các số thập phân liền nhau với các dấu chấm đan xen) cách nhau bởi một khoảng trắng.
-w	Khoảng thời gian (tính theo mili giây) chờ thông báo ICMP Time Exceeded hoặc Echo Reply đáp lại tương ứng với thông báo Echo Request. Nếu vượt quá khoảng thời gian quy định mà không có thông báo gì, dấu hoa thị (*) sẽ được hiển thị. Thời gian mặc định là 4000 (tức 4 giây)
-?	Phần trợ giúp ở màn hình lệnh.

Sử dụng Tracert để gỡ rối như thế nào

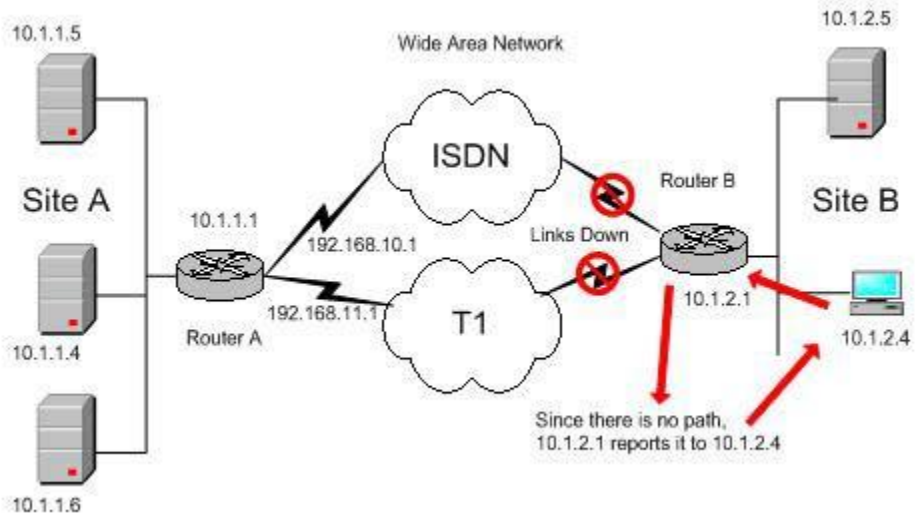
Có thể đôi khi phần thông tin hiển thị ra ngoài không rõ ràng khiến bạn không hiểu. Chẳng hạn như khi xuất hiện các dấu hoạ thị bạn sẽ làm gì? Như đã đề cập đến ở phần trên, dấu hoa thị có thể hiển thị sai, vì gói ICMP có thể đã được chuyển đến nơi nhưng có cái gì đó đã cản trở quá trình thông báo lại, thường là một

nguyên tắc nào đó trong tường lửa hoặc danh sách điều khiển truy cập (Access Control List).

Bạn có thể dùng **Tracert** để tìm ra chỗ gói tin bị ngừng lại trên mạng. Trong ví dụ sau, cổng mặc định đã tìm ra rằng không có đường đi nào hợp lệ ở bất kỳ host nào. Điều này có nghĩa là cả hai liên kết (T1 và ISDN) đều đã "sập" và không có đích nào có thể đến.

```
C:\>tracert 10.1.1.6
Tracing route to 22.110.0.1 over a maximum of 30 hops
----------------------------------------------------
1 10.1.2.1 reports: Destination net unreachable.
Trace complete.
```

Từ ví dụ này bạn có thể thấy, khi bạn gửi yêu cầu kiểm tra **Tracert** tới địa chỉ 10.1.1.6, cổng LAN mặc định báo lại rằng nó không thể tìm thấy đường đi. Nhìn vào sơ đồ cụ thể sau có thể giúp bạn hiểu vấn đề rõ ràng hơn.



Bạn có thể thấy, không có đường đi nào cho gói tin. Router gần nguồn nhất thông báo rằng từ nguồn không có đường đi nào để tới các host khác.

Chú ý quan trọng về Tracert

Dưới đây là một số chú ý quan trọng giúp bạn hiểu sâu hơn về **Tracert**.

- Không phải lúc nào **Tracert** cũng giúp bạn tìm kiếm 'latency' (độ trễ). Để xác định đường đi và cung cấp độ trễ cũng như các gói tin thất lạc cho từng router và liên kết trong đường đi, sủ dụng lệnh "**pathping**". Bạn có thể tham khảo bài về pathping đã được Quantrimang.com giới thiệu trước đây.
- **Tracert** chỉ có thể dùng được nếu giao thức Internet Protocol (TCP/IP) đã được cài đặt như là thành phần trong các thuộc tính của một bộ điều hợp mạng

(network adapter) ở Network Connections. Đây là một tiện ích TCP/IP sử dụng ICMP, một giao thức nằm trong bộ giao thức TCP/IP.

- Trong phiên bản Linux hiện đại, tiện ích **tracerouter** (không phải là **tracert** mặc dù một số hệ thống Linux cũng cho phép bạn sử dụng **tracert**) dùng UDP datagram với mã số cổng là 33434. Windows dùng yêu cầu báo hiệu lại ICMP (kiểu 8) được biết đến nhiều hơn với các gói ping.

Tóm tắt:

Trong bài này chúng tôi đã chuyển tới bạn khái niệm cơ bản về **Tracert**. **Tracert** (hay còn được biết đến là **traceroute**) là một công cụ dựa trên nền tảng Windows, cho phép bạn hỗ trợ kiểm tra cơ sở hạ tầng mạng. Cụ thể trong bài chúng tôi hướng dẫn bạn cách dùng tracert để gỡ lỗi các vấn đề xảy ra trong thực tế như đa đường đi hay các link không hoạt động. Điều này giúp tăng cường tính hữu ích của công cụ và chỉ cho bạn cách sử dụng khi làm việc với mạng riêng của mình. Tiện ích TCP/IP này cũng cho phép bạn xác định đường đi của các gói tin truyền qua mạng tới host cụ thể bạn chỉ định. Khi một gói tin đi qua một host, host sẽ giảm giá trị TTL của gói tin đi một giá trị và gửi tới host tiếp theo. Khi quá thời gian mà chưa đến đúng địa chỉ cần tìm, host nhận được gói tin sẽ loại bỏ và gửi lại thông báo thời gian quá hạn ICMP. **Tracert** nếu được dùng hợp lý có thể giúp bạn tìm ra các điểm trong mạng được định tuyến không chính xác hoặc không tồn tại. **Tracert**(hay **traceroute**) là công cụ bạn phải kiểm soát được nếu có kế hoạch làm việc trên mạng. Nó (và **ping**, **pathping**) có thể được dùng để giúp bạn ánh xạ và gỡ lỗi mạng dễ dàng. Các bạn nên tìm hiểu về các công cụ này kỹ hơn từ các bài tham khảo.