

10 giải pháp khắc phục sự cố DNS Resolution

Khi DNS Resolution không hoạt động, bạn sử dụng máy tính để truy cập mạng Internet sẽ đều bị thất bại. DNS không phải là "tính năng tuyệt vời" trên hệ thống mạng, nhưng nó là "tính năng cần" phải có.

Nếu vai trò của bạn là **Network Admin**, chắc hẳn bạn đã từng được nghe rất nhiều người dùng thắc mắc về vấn đề hệ thống mạng của họ bị "sập", nguyên nhân thường là do các máy chủ DNS, có thể kèm cả lỗi DNS Server not responding, Không thể tìm thấy DNS Address máy chủ...

Vậy làm thế nào để khắc phục được hạ tầng cơ sở mạng khi máy tính người dùng và DNS không phân giải được tên miền? Mời các bạn cùng tham khảo bài viết dưới đây của Quản trị mạng.

1. Kiểm tra kết nối mạng

Trong rất nhiều trường hợp khi bạn mở trình duyệt Web và nhập một URL vào đó, nhưng URL thất bại không thể truy cập được trang Web. Trường hợp này nguyên nhân bạn nghĩ đến đầu tiên là do lỗi DNS. Tuy nhiên thực tế thì trong trường hợp này nguyên nhân có thể là do kết nối mạng của bạn.

Điều này càng đúng hơn nếu bạn sử dụng Laptop và kết nối mạng bằng Wifi. Với giao thức bảo mật không dây, key sẽ được "điều chỉnh" lại hoặc cường độ tín hiệu của sóng vô tuyến sẽ bị yếu dần, dẫn đến kết nối mạng bị mất.

Nguyên nhân mất kết nối mạng có thể xảy ra trên bất kỳ loại mạng nào.

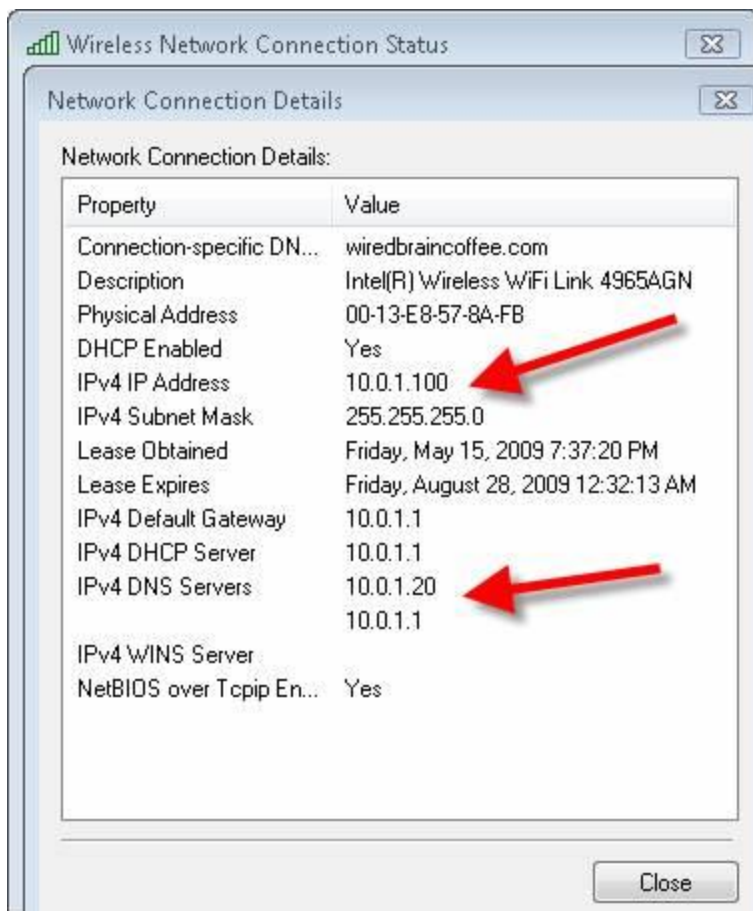
Nói cách khác, trước khi đổ lỗi cho DNS, hãy bắt đầu khắc phục sự cố bằng cách kiểm tra "**OSU Layer 1 - Physical**" đầu tiên sau đó kiểm tra kết nối mạng của bạn.



Hình 1: Kết nối mạng không dây vẫn ở trạng thái tốt

Lưu ý về cách **Access** là **Local and Internet**. Nếu **Access** hiển thị là **Local**, đồng nghĩa với việc địa chỉ mạng của bạn không hợp lệ (trong trường hợp này, bạn chỉ có một APIPA riêng bắt đầu với địa chỉ 169.x.x.x).

Tiếp theo bạn cần đảm bảo rằng bạn có một địa chỉ IP hợp lệ trên hệ thống mạng. Bạn có thể kiểm tra địa chỉ IP của mình bằng cách vào **View Status** sau đó chọn **Details**, kiểm tra địa chỉ IP và xác nhận địa chỉ IP của DNS Server. Nếu địa chỉ IP của bạn là **169.x.x.x** đồng nghĩa với việc bạn không thể kết nối Internet được.



Hình 2: Thăm định địa chỉ IP của bạn và các địa chỉ IP của DNS Server

2. Xác nhận địa chỉ IP của DNS Server là "chuẩn" và đúng thứ tự

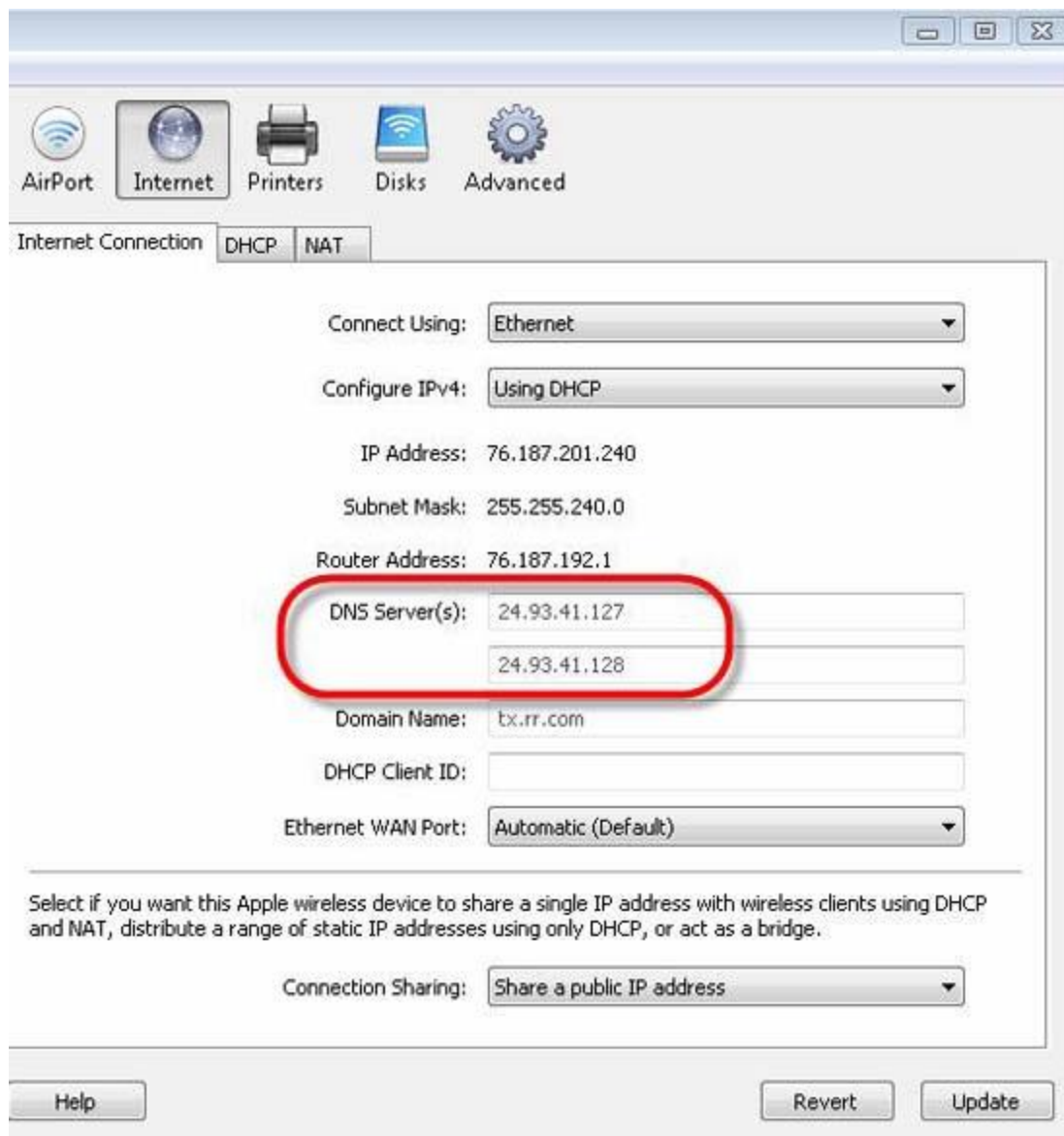
Sau khi bạn có địa chỉ IP hợp lệ và có thể kết nối được Internet, lúc này bạn có thể đi sâu vào các vấn đề bên trong DNS bằng cách xác nhận lại địa chỉ IP của DNS Server đã chuẩn và đúng thứ tự hay chưa.

Nếu quan sát trong hình thứ 2 ở trên bạn có thể nhìn thấy địa chỉ IP của IPv4 DNS Server. Lưu ý rằng địa chỉ IP của IPv4 DNS Server IP bao gồm cả Local LAN / Subnet để bạn có thể truy cập, thậm chí trong trường hợp nếu cổng mặc định bị hỏng.

Đây là cách nó làm việc trên hầu hết các mạng doanh nghiệp. Mặc dù vậy, các máy chủ DNS của bạn không phải lúc nào cũng nằm trên subnet. Trong thực tế, với hầu hết các ISP, các IP của DNS Server thậm chí còn không nằm trên cùng subnet với cổng mặc định (default gateway).

Trong hầu hết các cấu hình router của gia đình hay các doanh nghiệp vừa và nhỏ (home/SMB) không có các máy chủ DNS riêng và các SMB router sẽ proxy (ủy nhiệm) DNS đến các máy chủ DNS thực. Trong trường hợp đó, địa chỉ IP của DNS Server có thể cùng với địa chỉ IP Router của bạn.

Cuối cùng, bảo đảm rằng DNS Server của bạn nằm đúng thứ tự. Trong trường hợp thể hiện trong hình 2, DNS Server nội bộ là 10.0.1.20. Nó được cấu hình để “forward” tất cả các tên miền mà nó không thể phân giải đến 10.0.1.1, địa chỉ router nội bộ. Router đó sẽ proxy DNS đến DNS Server của ISP. Chúng ta thể tra cứu các DNS Server đó trên router của mình, xem thể hiện trong hình 3.



Hình 3: Các DNS Server đã nhận từ ISP thông qua DHCP

Đầu tiên, cần đảm bảo rằng DNS Server của bạn nằm ở đúng thứ tự. Nếu trường hợp bạn có một local DNS Server, giống như trên và đang tra cứu tên miền nội bộ (local DNS name), muốn PC client tra cứu local DNS name đó trong local DNS Server đầu tiên, trước Internet DNS Server. Khi đó, local DNS server của bạn phải nằm đầu tiên trong các thiết lập DNS.

Thứ hai, bạn có thể ping địa chỉ IP của DNS Server của ISP. Theo cách này, chỉ cần các DNS server được liệt kê nằm ở trên router của mình, bạn có thể

thẩm định rằng mình có thể ping chúng thậm chí từ máy tính nội bộ của mình:

Lưu ý về thời gian đáp trả khi ping đến DNS Server của ISP. Quá trình này có thể làm chậm các tra cứu DNS hoặc thậm chí còn có thể làm thất bại nếu nó mất quá lâu thời gian để DNS server đáp trả.

```
ca. Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\david>ping 24.93.41.127

Pinging 24.93.41.127 with 32 bytes of data:
Reply from 24.93.41.127: bytes=32 time=769ms TTL=248
Reply from 24.93.41.127: bytes=32 time=788ms TTL=248
Reply from 24.93.41.127: bytes=32 time=812ms TTL=248
Reply from 24.93.41.127: bytes=32 time=865ms TTL=248

Ping statistics for 24.93.41.127:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 769ms, Maximum = 865ms, Average = 808ms

C:\Users\david>
```

Hình 4: Ping DNS Server của ISP

Lưu ý về thời gian đáp trả từ hành động ping của bạn đến DNS Server của ISP. Điều này có thể làm chậm các tra cứu DNS hoặc thậm chí còn có thể làm thất bại nếu nó mất quá lâu thời gian để DNS server đáp trả.

3. Ping địa chỉ IP của host mà bạn muốn (trường hợp nếu bạn biết)

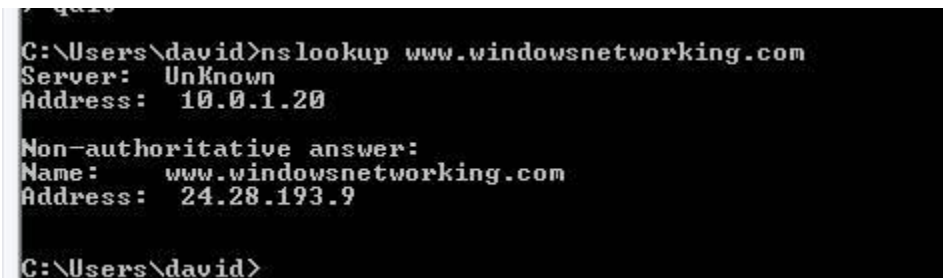
Cách nhanh chóng để chứng minh lỗi là do DNS chứ không phải do sự cố kết nối mạng đó là ping địa chỉ IP của Host mà bạn muốn truy cập đến. Nếu kết nối đến tên miền thất bại nhưng kết nối đến địa chỉ IP thành công đồng nghĩa với việc vấn đề của bạn nằm ở DNS.

Tuy nhiên nếu DNS Server của bạn không hoạt động thì rất khó có thể chỉ ra địa chỉ IP mà bạn đang kết nối đến là gì. Để thực hiện test này, bạn phải có một sơ đồ (diagram) mạng hoặc giống như nhiều Admin vẫn thực hiện, chỉ cần nhớ địa chỉ IP của host.

Nếu làm việc, chờ cho tới khi DNS server khả dụng lần nữa, bạn có thể đặt một entry trong file hosts của mình để map IP đến hostname.

4. Tìm DNS server đang được sử dụng bằng nslookup

Bạn có thể sử dụng lệnh nslookup để tìm kiếm các thông tin về DNS resolution của mình. Một trong những cách đơn giản là bạn có thể sử dụng lệnh này để xem DNS server nào đang cung cấp cho bạn câu trả lời và DNS server nào không.



```
C:\Users\dauid>nslookup www.windowsnetworking.com
Server: UnKnown
Address: 10.0.1.20

Non-authoritative answer:
Name: www.windowsnetworking.com
Address: 24.28.193.9

C:\Users\dauid>
```

Hình 5: Đầu ra của lệnh nslookup

Lưu ý trong hình 5, DNS server của ISP đã cung cấp cho chúng ta thông tin “non-authoritative answer”, có nghĩa rằng nó không cấu hình miền nhưng vẫn có thể cung cấp hồi đáp.

Ngoài ra bạn cũng có thể sử dụng lệnh này để so sánh các hồi đáp từ các DNS server khác nhau bằng cách cung cấp DNS server nào sử dụng.

5. Kiểm tra hậu tố DNS

Nếu bạn đang tra cứu host nội bộ trên một DNS server mà máy tính của bạn là một thành viên nằm trong đó, khi đó bạn có thể kết nối đến một host, không cần sử dụng FQDN (fully qualified DNS name) và hy vọng vào hậu tố của DNS có thể giúp bạn tìm ra vấn đề.

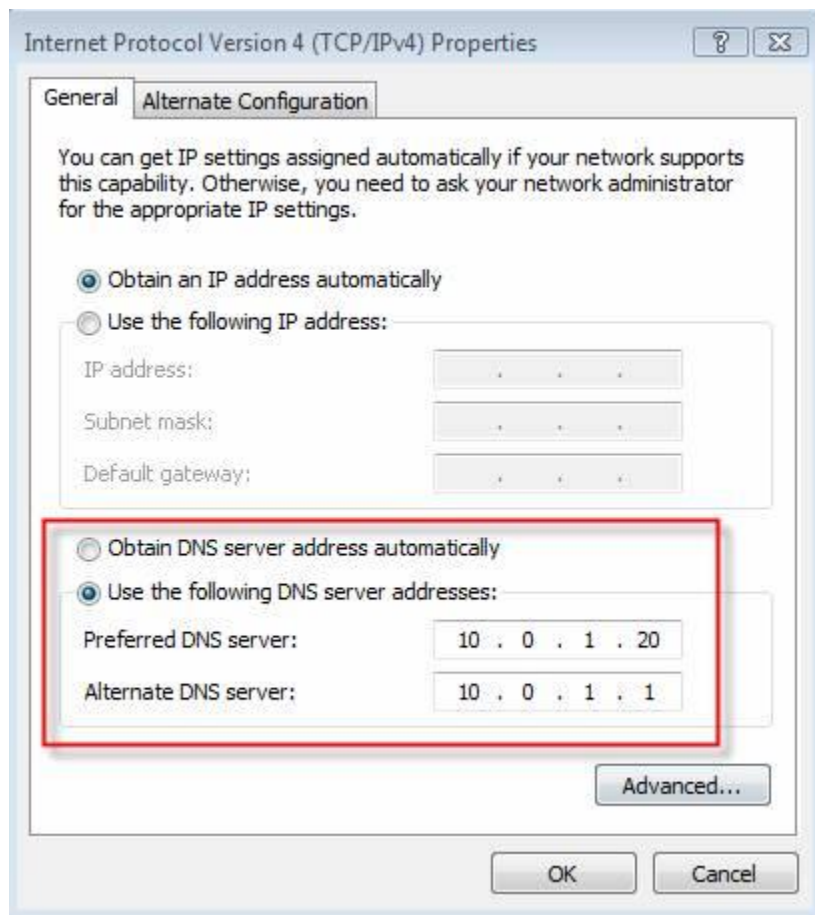
Cho ví dụ, nếu chúng ta kết nối đến “server1”, DNS server có thể có nhiều entry cho tên miền đó. Khi đó Network Adaptor của bạn sẽ được cấu hình với hậu tố DNS kết nối.

Chẳng hạn như ví dụ trong hình 2, DNS là wiredbraincoffee.com. Do đó bất cứ khi nào bạn nhập vào một tên miền như server1, hậu tố DNS sẽ được bổ sung vào phần cuối của nó để tạo thành server1.wiredbraincoffee.com.

Bạn nên xác nhận hậu tố DNS của mình là đúng.

6. Đảm bảo rằng các thiết lập DNS của bạn được cấu hình để “kéo” IP của DNS từ máy chủ DHCP

Cũng giống như khi bạn muốn Network Adaptor của mình “thu” được các địa chỉ IP của DNS Server từ DHCP Server. Nếu quan sát vào hình trên, bạn có thể nhìn thấy adaptor này đã được ghi rõ các địa chỉ IP của DNS Server.



Hình 6: Thăm định các thiết lập của DNS Server

Bạn phải thay đổi “**Obtain DNS server address automatically**” theo thứ tự để có được IP mới của DNS server. Để thực hiện điều đó, bạn chỉ cần mở thẻ **Properties** của Network Adaptor, sau đó click vào **Internet Protocol Version 4 (TCP/IPv4)**.

7. Giải phóng và “làm mới” địa chỉ IP của DHCP Server (và cả thông tin DNS)

Dù Adaptor của bạn đã được thiết lập để kéo các thông tin DNS từ DHCP, nhưng trong một số trường hợp nó có thể xảy ra hiện tượng xung đột địa chỉ IP hoặc nhận phải các thông tin DNS server cũ. Chính vì vậy sau khi đã lựa chọn “thu nhận” địa chỉ IP và DNS tự động, bạn nên “giải phóng” địa chỉ IP của mình và “renew – làm mới” nó.

Bạn có thể thực hiện điều này với Windows Diagnosis trong cấu hình Network của mình. Tuy nhiên cách nhanh nhất là sử dụng Command prompt. Nếu bạn đã kích hoạt UAC, chạy lệnh cmd của Windows dưới quyền Admin:

IPCONFIG /RELEASE

IPCONFIG /RENEW

Sau đó, thực hiện với lệnh **IPCONFIG /ALL** để xem những thông tin IP và DNS mới như thế nào.

8. Kiểm tra DNS Server và restart các dịch vụ hoặc reboot nếu cần thiết

Rõ ràng, nếu DNS server bị treo hoặc bị hỏng, hoặc bị cấu hình sai, bạn sẽ không thể khắc phục điều đó tại Client side. Tuy nhiên bạn có thể bypass máy chủ bị lỗi đó chứ không thể khắc phục được lỗi.

Theo cách đó, Admin – người chịu trách nhiệm cho DNS server sẽ phải kiểm tra trạng thái và cấu hình của DNS server để khắc phục vấn đề DNS.

9. Khởi động lại Router DNS văn phòng nhỏ hay gia đình

Như đã đề cập ở trên trong cách thứ 2 và được hiển thị trong hình minh họa thứ 3, trên các router của gia đình và các văn phòng nhỏ, thiết lập DNS server thường được thực hiện thông qua DHCP với DNS server thiết lập một địa chỉ IP của router và router sẽ proxy DNS đến DNS server của ISP.

Tuy vậy, máy tính nội bộ của bạn có thể có các thông tin mạng (gồm có các địa chỉ IP của DNS server), nhưng cũng có trường hợp router của bạn có

thông tin sai. Để bảo đảm rằng router của bạn có các thông tin DNS server mới nhất, bạn có thể thực hiện “giải phóng” một DHCP và “renew – làm mới” giao diện WAN của router với ISP. Hoặc cách dễ dàng hơn có thể là reboot router để nó nhận được các thông tin mới nhất.

10. Liên hệ với ISP

Tất cả chúng ta đều biết rằng việc liên lạc với một ISP để khắc phục một vấn đề về mạng sẽ mệt mỏi như thế nào. Tuy nhiên nếu máy tính của bạn vẫn gặp vấn đề về DNS resolution từ các máy chủ DNS của ISP thì bạn cần phải liên lạc với họ, và đó cũng chính là cách giải quyết cuối cùng.