

Comandos para visualizar e gerenciar informações TCP/IP

Conteúdos

- Descrição sumária de comandos e ferramentas
- Como obter informações de redes TCP/IP
- Ferramentas nslookup e dig para resolução de nomes/endereços usando DNS
- Informações básicas sobre máscaras de rede em IPv4 e comprimento de prefixo em IPv6

Por Gerson L Camillo Revisão: 11 setembro 2023

Visualizar, monitorar e configurar conectividade em redes TCP/IP

Existem duas formas de interagir com o sistema:

- GUI (*Graphical User Interface*): interface gráfica de usuário que fornece um conjunto de opções para interagir com o sistema para realizar as tarefas de visualização e configuração de rede.

- CLI (*Command Line Interface*): Interface de linha de comando na qual se insere os comandos e os respectivos parâmetros para testar e configurar uma rede.

Por exemplo, no Windows temos a GUI padrão e o terminal é executável cmd (prompt de comando). No Linux é o aplicativo de Terminal.

Os comandos no Windows iniciarão pelo sinal > e os do Linux pelo \$.

Descrição das opções dos comandos. A forma de especificar e os tipos podem variar de sistema para sistema. No Windows: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/command-line-syntax-key>.

Texto sem colchetes ([]) ou chaves ({}).	Itens que precisam ser especificados no comando
[]	Opcional
{ }	Parâmetros obrigatórios; escolher um
	Separador de opções; escolher um
<>	Opções que precisam ser substituídas (parâmetros)
...	Itens que podem ser repetidos

COMANDOS E FERRAMENTAS

IPCONFIG

Descrição sumária: comando do Windows para visualizar as interfaces de rede (nomes descritivos para as interfaces) e os respectivos endereços IP (IPv4 e/ou IPv6), máscara de sub-rede e configuração de *gateway* padrão.

Comando: **ipconfig**

Comando: **ipconfig /all** (para informações completas)

IFCONFIG

Descrição sumária: comando do Linux e do Mac OS para visualizar as interfaces de rede (nomes informativos, como eno1, enp1s0, wlp2s0, lo) e respectivos valores de:

- Status: UP, RUNNING;
- Estatísticas de pacotes e de dados;
- Configuração de interface: endereço IP (inet:IPv4 e/ou inet6:IPv6), endereço de MAC (endereço de hardware), endereço de *broadcast* e máscara de sub-rede.

Comando: **ifconfig**

Comando: **ifconfig -a** (para informações completas, inclusive com interfaces inativas)

Observação: informação de *gateway* padrão é obtida no Linux através do comando ROUTE.

PING (Packet InterNetwork Groper)

Descrição sumária: ferramenta de rede para testar conectividade IP.

Descrição completa: usa o protocolo ICMP (mensagem tipo 8) para enviar datagramas ECHO_REQUEST para o endereço IP de destino. Finalidades: verificar se a rede está funcionando; determinar se hosts remotos (fora de nossa rede) estão ativos/inativos; verificar a resolução de nome para endereço IP; e, também para obter informações de atraso de ida e volta (RTT – Round-Trip Time).

Comando: **ping -c 4 www.google.com**

Observações:

a) O comando **ping** sem opções apresenta ajuda para o mesmo.

b) O comando **ping** primeiro procura o endereço IP relativo ao nome www.google.com para então disparar pacotes ICMP.

c) Para usar endereços IPv6 (de 128 bits), usar o comando **ping6**.

d) Toda máquina com TCP/IP instalado e habilitado possui uma interface virtual, conhecida como localhost (ou lo). Pode-se testar se o protocolo IP está funcionando, através da execução do comando:

ping -c 4 localhost

Possíveis resultados:

ping 10.10.2.10 Pinging 10.10.2.10 with 32 bytes of data: Destination host unreachable. Destination host unreachable. Destination host unreachable. Destination host unreachable. Ping statistics for 10.10.2.10: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms	Destino não pode ser alcançado: endereço não existe ou não há rota para esse destino. Como é um endereço privado, deve estar dentro da mesma rede local.
ping videiro.ifc.edu.br Unreachable host videiro.ifc.edu.br ou ping: videiro.ifc.edu.br: Name or service not known	Host (videiro.ifc.edu.br) não existe: não foi possível encontrar um endereço IP para esse nome (<u>problemas na resolução de nomes DNS</u>).
ping 210.100.100.100 Pinging 210.100.100.100 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 210.100.100.100: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms	A máquina de endereço 210.100.100.100 existe mas está desligada ou não respondendo pacotes ICMP.
ping -c 4 www.google.com PING www.google.com (172.217.162.100) 56(84) bytes of data. 64 bytes from gru14s07-in-f4.1e100.net (172.217.162.100): icmp_seq=1 ttl=55 time=26.5 ms 64 bytes from gru14s07-in-f4.1e100.net (172.217.162.100): icmp_seq=2 ttl=55 time=27.4 ms 64 bytes from gru14s07-in-f4.1e100.net (172.217.162.100): icmp_seq=3 ttl=55 time=26.0 ms 64 bytes from gru14s07-in-f4.1e100.net (172.217.162.100): icmp_seq=4 ttl=55 time=28.1 ms --- www.google.com ping statistics --- 4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev = 26.082/27.069/28.149/0.811 ms	O host foi alcançado e respondeu. O nome www.google.com está associado ao endereço IP 172.217.162.100. A estatísticas indicam que não houve perda de pacotes e o tempo médio foi de 27,069 ms para: um pacote sair da máquina local até o destino; ser processado no destino; um pacote sair do destino para a máquina local. O valor de TTL foi de 55, considerando estar logo abaixo de 64 (ver a seguir), indica que devem haver nove roteadores no caminho.

Ping em redes IPv6

Endereços IPv6: são 128 bits expressos em 32 caracteres hexadecimais

Endereços Globais (roteáveis na Internet): prefixo **2800::/3**

- Exemplo de um endereço com prefixo: 2804:eeee:4444:deab:d056:a234:c345:3

- Normalmente endereços para documentação: 2001:db8::

- Endereço localhost IPv6

Comando: **ping6** ou **ping 6 ::1**

- Endereço público global IPv6

Comando: **ping6** ou **ping 6 2804:eeee:4444:deab:d056:a234:c345:3**

- Endereços com escopo local no link (link local scope): prefixo **fe80::/10**

a) Toda interface habilitada IPv6 recebe um endereço fe80:: e normalmente roteadores usam esse endereço para trocar informações entre os mesmos. Como ele tem um escopo local, só poderá ser acessível quando associado ao respectivo enlace (por isso, link scope). Então, os comandos devem especificar a interface ao qual o respectivo endereço está associado.

b) No Windows, esse endereço especifica a interface como um número apenas ao endereço e separado por um símbolo por cento: **fe80::1%14** **fe80::b295:75ff:fe67:f10b%5**

Então, os comandos devem especificar a interface. No caso do Linux:

ping6 -I wlan0 fe80::1ab2

ou

ping6 fe80::1ab2%wlan0

- Endereços multicast: prefixo **ff02::x** sendo: x=1 para todos os hosts x=2 todos os roteadores

a) O comando ping para endereços multicast também devem especificar a interface:

ping -I wlan0 ff02::1

ou

ping ff02::1%wlan0

O comando ping interpreta qual o tipo de endereço (IPv4 ou IPv6) e chama a função correta.

Todos os hosts locais (subrede) respondem.

ping ff02::2%wlan0

Todos os roteadores respondem (normalmente um só roteador por subrede local).

Para ver a tabela de associação endereço IP (neste caso IPv6) e o respectivo endereço MAC:

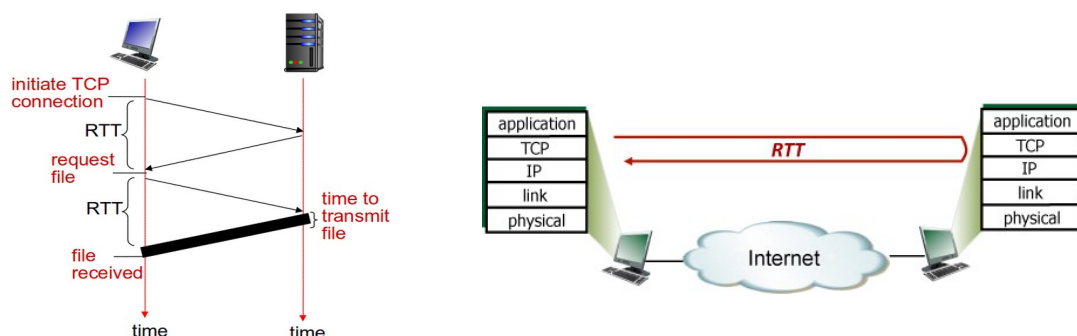
ip -6 neigh

O equivalente para endereços IPv4 é o comando **arp -a** (ou **ip -4 neigh**).

TTL¹ (*Time-To-Live*): tempo de vida de um datagrama na rede. É um valor (máximo 255) que o originador do datagrama inclui no cabeçalho do IP e cujo valor é decrementado (diminuído de 1) a cada passagem por roteador. Quando o valor chega a 0, o pacote é descartado. O valor inicial depende de qual tipo de sistema (sistema operacional) gerou o pacote. Alguns valores padrões de TTL iniciais:

Dispositivo/Sistema Operacional	Protocolo	TTL
Linux (kernel 2.4)	ICMP	255
Linux (kernel 3 e acima)	ICMP	64
Windows 7, Server, 10	ICMP/TCP/UDP	128

RTT (*Round-Trip Delay Time* (RTD) ou *Round-Trip Time* (RTT): tempo que um pequeno pacote leva para percorrer a ida e volta do cliente para um servidor. Exemplos:



NETSTAT

Descrição sumária: apresenta estatísticas de protocolo e conexões de rede TCP/IP.

Comando: **netstat**

Observação: esse comando possui várias opções e muitas estão relacionadas às conexões TCP/IP na máquina local.

O comando netstat também pode ser usado para informar estatísticas a nível de rede. Na seção sobre informações de rede, esse assunto será expandido.

Encontrado no Windows e Linux. Algumas opções e parâmetros são diferentes para os dois sistemas.

Comando (Windows): **netstat -a** [-n somente números IP e números de porta; -o mostra processos associados a determinada conexão; -p tcp udp define os protocolos; -e estatísticas Ethernet]

ARP

Descrição sumária: mostra e modifica a tabela de tradução de endereços IP em endereços MAC (endereços relativos ao protocolo de camada de enlace, o Ethernet). Os endereços MAC dessa tabela informam quais os dispositivos/computadores com os quais a presente máquina conectada fisicamente (por cabo ou sem fio).

Descrição adicional: essa tabela é conhecida também como cache ARP, pois os mapeamentos são geralmente temporárias (poucos minutos). Entradas permanentes podem ser inclusas através da criação manual dos mapeamentos. As flags indicam: **C**, para uma entrada completa no cache ARP; **M**, para entradas permanentes; e, **P**, para entradas publicadas.

Comando: **arp**

Sem opções, apresenta a tabela relacionando o endereço de MAC (HW ou hardware) com o endereço IP.

Comando: **arp -n** Usa números em vez dos nomes.

¹ No IPv6 o campo correspondente no cabeçalho é **Hop Limit**.

NSLOOKUP

Descrição sumária: comando padrão para tradução (resolução) de nomes de Internet em endereços IP.

Trabalha usando o **protocolo DNS**.

Comando: **nslookup www.planalto.gov.br**

Comando retorna o endereço IP para o nome www.planalto.gov.br consultando o servidor DNS configurado localmente (geralmente pelo provedor de serviço ISP).

Encontrado no Windows e Linux.

Comando: **nslookup www.ifc.edu.br 8.8.8.8**

Comando retorna o endereço IP para o nome www.ifc.edu.br consultando o servidor DNS do Google (8.8.8.8).

Em um documento separado, serão apresentadas informações e exemplos detalhados.

Obs.: informações mais detalhadas e exemplos ao final deste documento.

ROUTE

Descrição sumária: apresenta a tabela de roteamento local (uma definição melhor seria tabela de encaminhamento local). Além disso, permite manipular a mesma, incluindo, alterando ou apagando rotas.

Comando - Linux: **route [-n]**

Comando - Windows: **route print**

Sem opções apresenta a tabela e com a opção -n somente o endereços.

TRACERT ou TRACEROUTE

Descrição sumária: comando que permite visualizar a rota e os roteadores pelos quais passaram os pacotes até chegar ao destino. Apresenta também o tempo para alcançar cada roteador.

Comando no Windows: **tracert www.google.com**

Comando no Linux: **traceroute www.google.com** ou **tracepath www.google.com**

NBTSTAT

Descrição sumária: apresenta informações de nome de computadores e dispositivos em redes Windows.

Computadores executando Windows em redes Microsoft recebem um nome ue é mapeado para endereços IP. Esses mapeamentos podem ser visualizados pelo Nbtstat. Além disso, pode-se visualizar compartilhamentos de rede (pastas e impressoras).

Comando: **nbtstat**

Exclusivo do Windows.

INFORMAÇÕES DE REDES TCP/IP

Como visualizar as informações de conectividade TCP/IP num computador. Há duas formas, uma delas via GUI e outra via CLI. Os exemplos serão executados em linha de comando (CLI) tanto no Linux quanto no Windows. Observação: os comandos serão executados no modo de usuário (não de administrador ou root), de forma que algumas opções de comandos não estarão disponíveis.

Linux: aplicativo Terminal. Windows: aplicativo prompt de comando (pesquisar por **cmd**).

Listar as interfaces de rede e as respectivas configurações e status:

Windows	Linux
<p>> ipconfig Exibe a configuração TCP/IP da máquina. Sem parâmetros, apresenta: endereço IP da interface, máscara de sub-rede e endereço de gateway padrão.</p> <p>> ipconfig /all (mostra todas as informações) Exibe informações completas. Além das indicadas acima, também: servidores DNS, servidor DHCP e outras informações relativas à interface.</p> <p>> netsh interface ipv4 ipv6 show addresses</p>	<p>\$ ifconfig Exibe a configuração TCP/IP do computador. Lista as interfaces ativas, com o acréscimo de informações de estatísticas de pacotes (bytes) enviados e recebidos. A primeira linha indica também um conjunto de flags ao lado do nome da interface. Exemplo: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> UP: a interface está ativa RUNNING: a interface está com TCP/IP configurado e trocando dados.</p> <p>Exemplo: wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fe80::88c2:36c6:a454:b5ac prefixlen 64 scopeid 0x20<link> ether ec:0e:c4:60:ab:f5 txqueuelen 1000 (Ethernet) RX packets 6771169 bytes 9062781127 (8.4 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 3082122 bytes 412276291 (393.1 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</p> <p>\$ ifconfig -a Inclui todas as interfaces, inclusive as inativas.</p>

Observações:

a) O Windows lista as interfaces através de sua descrição, a qual pode conter a velocidade (largura de banda) do dispositivo e do protocolo suportado. Por exemplo, uma interface pode ser descrita como Ethernet 1Gbps, a qual informa que essa interface suporta o protocolo Gigabit Ethernet (GbE or 1 GigE) a uma velocidade de um bilhão de bits por segundo.

b) Os endereços IP podem ser públicos ou privados. Endereços IPv4 privados não podem constar nos pacotes IP que são enviados pela Internet. Os roteadores descartam qualquer pacote contendo endereço de origem e/ou destino que contenha um IP privado. As seguintes faixas são endereços **IP privados**:

10.0.0.0 - 10.255.255.255

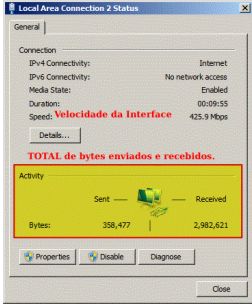
172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Eles são usados nas redes internas e nas redes domésticas para conectar computadores e dispositivos ao roteador caseiro.

O restante do conjunto de endereços são considerados públicos, ou seja, são roteáveis na Internet. Os roteadores que conectam redes locais com a Internet fazem (normalmente) a conversão de endereços privados para endereços públicos, através de um mecanismo chamado NAT (*Network Address Translation*).

Estatísticas de pacotes (ou bytes) recebidos e transmitidos. Pode ser por interface e/ou protocolo:

Windows	Linux
<p>As estatísticas podem ser obtidas de duas formas:</p> <p>a) Via GUI, através do Centro de Redes e Compartilhamento e Adaptadores. Ao abrir o adaptador atualmente ativo (com conexão com a Internet) é possível visualizar a velocidade da interface e o total de bytes enviados e recebidos. Ou através: “Painel de Controle” > “Conexões de Rede”: clicar botão direito sobre a conexão e “Status”.</p>	<p>\$ ifconfig ou ip -a</p> <p>Para cada interface, informa as estatísticas de pacotes (bytes) enviados e recebidos. Obs: somente para interfaces com flag RUNNING (flags=4163<UP,BROADCAST,RUNNING,MULTICAST>).</p> <p>Exemplo:</p> <pre>wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fe80::88c2:36c6:a454:b5ac prefixlen 64 scopeid 0x20<link> ether ec:0e:c4:60:ab:f5 txqueuelen 1000 (Ethernet) RX packets 6771169 bytes 9062781127 (8.4 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 3082122 bytes 412276291 (393.1 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre> <p>Também se pode visualizar erros e colisões (em se tratando da camada de enlace usando o Ethernet).</p>
	<p>\$ netstat -s</p> <p>Apresenta uma visualização completa de estatísticas por protocolo: IP, ICMP, UDP e TCP.</p> <p>Exemplo:</p> <p>\$ netstat -s</p> <p>Ip:</p> <pre>... 6996307 total packets received ... 6984728 incoming packets delivered ...</pre> <p>Icmp:</p> <pre>52519 ICMP messages received ... 52558 ICMP messages sent ...</pre> <p>Tcp:</p> <pre>... 6844820 segments received 3050544 segments sent out</pre> <p>Estatísticas por interface de rede</p> <p>\$ ip -s address</p> <p>Estatísticas e configuração TCP</p> <p># ss -tni</p>
<p>b) Pelo terminal de comando:</p> <p>Estatísticas por protocolo:</p> <p>> netstat -s</p> <p>ou, estatísticas por interface (camada de enlace).</p> <p>> netstat -e</p>	

Identificar os endereços do roteador (gateway) padrão para acesso a redes externas e/ou a Internet.

O roteador (também referenciado como gateway) é um equipamento de rede (ou um computador configurado para tal) que interliga duas redes diferentes: uma é a rede doméstica ou da empresa enquanto a outra é a rede externa, especificamente a grande rede da Internet.

O roteador possui ao menos duas interfaces: uma para a rede interna e outra para a rede externa. Cada qual com um endereço de Internet (IPv4 ou IPv6) específico:

Windows	Linux
<p>> ipconfig</p> <p>Exibe a configuração TCP/IP da máquina. Sem parâmetros, apresenta: endereço IP da interface, máscara de sub-rede e endereço de gateway padrão.</p> <p>> ipconfig /all (mostra todas as informações)</p> <p>Exibe informações completas. Além das indicadas acima, também: servidores DNS, servidor DHCP e outras informações relativas à interface.</p> <p>O PowerShell é uma combinação de terminal, linguagem de scripting e programa.</p> <p>> netsh interface ipv4 ipv6 show route</p>	<p>\$ ifconfig</p> <p>Exibe a configuração TCP/IP do computador. Lista as interfaces ativas, com o acréscimo de informações de estatísticas de pacotes (bytes) enviados e recebidos.</p> <p>A primeira linha indica também um conjunto de flags ao lado do nome da interface. Exemplo:</p> <pre>flags=4163<UP,BROADCAST,RUNNING,MULTICAST> UP: a interface está ativa RUNNING: a interface está com TCP/IP configurado e trocando dados.</pre> <p>Exemplo:</p> <pre>wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fe80::88c2:36c6:a454:b5ac prefixlen 64 scopeid 0x20<link> ether ec:0e:c4:60:ab:f5 txqueuelen 1000 (Ethernet) RX packets 6771169 bytes 9062781127 (8.4 GiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 3082122 bytes 412276291 (393.1 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre> <p>\$ ifconfig -a</p> <p>Inclui todas as interfaces, inclusive as inativas.</p>

Obs.: em Linux, existe instalado por padrão nas distribuições atuais o pacote **iproute2** que torna legados os comandos `ifconfig` e `route`, dentre alguns. O principal comando disponível é o **ip** que tem as funções do `ifconfig` e incorpora diversas outras.

Informações de DNS. Há comandos que permitem visualizar os servidores DNS habilitados no sistema operacional e comandos com determinadas opções para obter e apagar o cache local (tabela com as últimas resoluções de nomes para endereços IP).

Windows

```
> ipconfig /displaydns  
> ipconfig /flushdns
```

Linux

Por padrão, armazena informações de servidores DNS no arquivo `/etc/resolv.conf`. Mas em versões mais atuais, um serviço de sistema (`systemd-resolve`) está encarregado de gerenciar o serviço de resolução de nomes (incluindo suporte ao DNSSEC).

```
$ resolvectl status
```

```
$ systemd-resolve --statistics  Não disponível no Debian/Ubuntu  
$ systemd-resolve --status      Não disponível no Debian/Ubuntu  
$ sudo systemd-resolve --flush-caches  Não disponível no Debian/Ubuntu
```

Também há um programa para interagir com o serviço `systemd-resolve`:

```
$ resolvectl flush-caches
```

MacOS

```
~ scutil --dns
```

Tabela de Rotas. O SO mantém uma tabela de rotas para fins de encaminhamento dos datagramas IP que são criados pela pilha TCP/IP. Ela é gerada de forma dinâmica quando o sistema define as configurações de IP através do protocolo DHCP ou a tabela pode ser manipulada estaticamente através de comandos.

Para impressão da tabela:

Windows

```
> route print  
> netstat -r
```

Linux

```
$ route [-n somente informação numérica]  
$ ip neigh
```

As informações de rede em dispositivos celulares podem ser obtidas nas opções e sistema.

- Android: System → About phone → Network ou Nas configurações e Wi-Fi → Advanced Wi-Fi

Mas, no caso do Android (e, em alguns casos, no iOS), há aplicações na loja que permitem obter informações mais detalhadas. A questão é que são muitas alternativas e a instalação deve ser cuidadosa para evitar o mínimo de “intrusão” e de coleta de dados pessoais. Como sugestão, seguem:

- WiFi Analyzer (desenv. Zoltan Pallagi): fornece informações sobre redes sem fio disponíveis, incluindo canal (frequência central) e largura de canal, de forma visual, além de outros dados correlatos; também fornece dados da rede celular conectada.

- Network Cell Info: essa ferramenta mostra diversas informações sobre a rede celular. Inclui informações básicas sobre rede sem fio conectada atualmente.

- HE.NET tools: ferramenta que imita parte das ferramentas de rede disponíveis no sítio. A HE.networks é uma provedora global de infraestrutura de internet (Tier-1).

Obs.: na pesquisa nas lojas, os nomes podem mudar conforme a versão e linguagem do sistema.

Testando conectividade a um serviço de rede: servidor Web: normalmente se usa um navegador web (Firefox, Chrome, etc) para acessar uma URL com o fim de testar servidores Web (Apache, Nginx, etc). Alternativamente, podem ser usados programas de linha de comando para testar/debugar o acesso. Obs.: o comando curl normalmente não disponível, logo, devendo ser instalado.

```
telnet www.wikipedia.org 80<ENTER><ENTER>
```

```
curl -I https://www.wikipedia.org
```

 Obtendo somente os cabeçalhos de um servidor HTTP
-vIl

```
curl --trace-ascii trace-wikipedia.txt https://www.wikipedia.org
```

Obtendo o endereço IP (IPv4 ou IPv6) público: esse endereço é aquele usado para conexão entre hosts e deve ser único em toda internet. Endereços especializados em informar endereços IP públicos:

<https://www.whatismyip.com>

<https://ipinfo.io/>

<https://icanhazip.com/>

Comando curl usado para obter também essa informação:

```
curl -4 icanhazip.com
```

Obtendo o número de AS (*Autonomous System*) ou ASN que identifica uma rede grande que possui uma única política de roteamento. Elas se caracterizam por: organizações que fornecem serviços de conectividade na Internet; a rede ou conjunto de redes administradas por uma única organização; e, essas organizações controlam de forma única um determinado espaço de endereços de IP.

O número de ASN do provedor ao qual se conecta à Internet pode ser obtido por acesso aos seguintes sítios:

<https://bgp.he.net> e <https://ipinfo.io>

Com o número de ASN se pode pesquisar mais informações no serviço Whois do Registro:

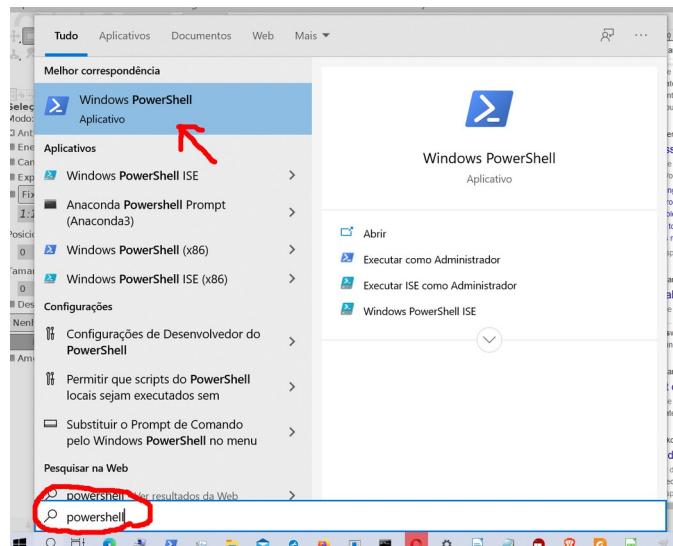
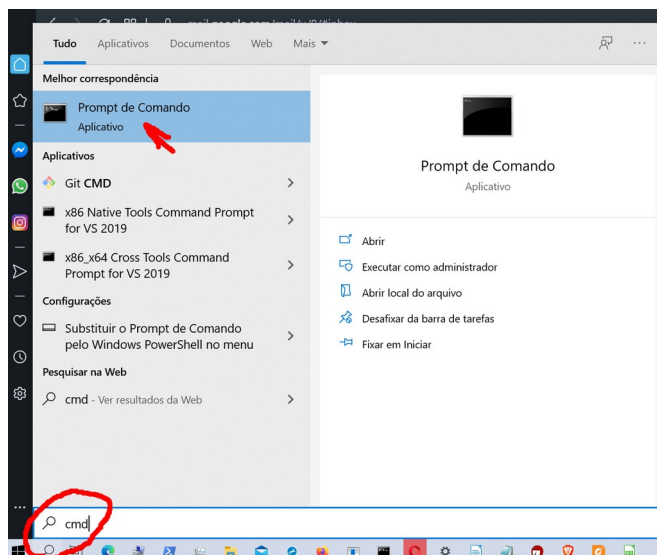
<https://registro.br/tecnologia/ferramentas/whois/>

Como visualizar informações de rede no Windows usando terminais de comando

- Prompt de Comando (padrão em todas as versões)
- Windows PowerShell (disponível a partir de versões mais recentes): possui maiores capacidades

Obs.: independente de qual for usar, em termos de comandos para visualizar informações de rede, qualquer dos dois terminais serve. Aqui os comandos serão mostrados usando o Windows PowerShell.

Nestas duas imagens, como invocar cada terminal:



Na próxima figura, o comando ipconfig sendo executado num terminal PowerShell

> ipconfig

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Experimente a nova plataforma cruzada PowerShell https://aka.ms/pscore6

PS C:\Users\ > ipconfig

Configuração de IP de Windows...

Adaptador Ethernet VirtualBox Host-Only Network:

    Sufixo DNS específico de conexão. . . . . : fe80::fcd0:9525:1ca4:7686%8
    Endereço IPv6 de link local . . . . . : 192.168.56.1
    Endereço IPv4. . . . . : 255.255.255.0
    Máscara de Sub-rede . . . . . : 
    Gateway Padrão. . . . . : 

Adaptador de Rede sem Fio Conexão Local* 1:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . : 

Adaptador de Rede sem Fio Conexão Local* 2:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . : 

Adaptador Ethernet Ethernet 2:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . : 

Adaptador de Rede sem Fio Wi-Fi:

    Sufixo DNS específico de conexão. . . . . : fe80::c95a:99fb:1a17:be98%7
    Endereço IPv6 de link local . . . . . : 192.168.7.12
    Endereço IPv4. . . . . : 255.255.255.128
    Máscara de Sub-rede . . . . . : 192.168.7.1
    Gateway Padrão. . . . . : 
```

Como resultado são vistas diversas interfaces de rede presentes no sistema.

- A primeira é um adaptador Ethernet VirtualBox Host-Only Network. A informação de adaptador Ethernet informa que a interface executa o protocolo de enlace Ethernet, que determina endereçamento (endereços MAC) e mecanismos de transporte entre o computador e o dispositivo diretamente conectado (um outro computador ou o roteador sem fio da rede). Esta é uma interface virtual, pois foi criada pelo programa VirtualBox² para executar outros sistemas operacionais

- Há outras interfaces, mas estão desconectadas.

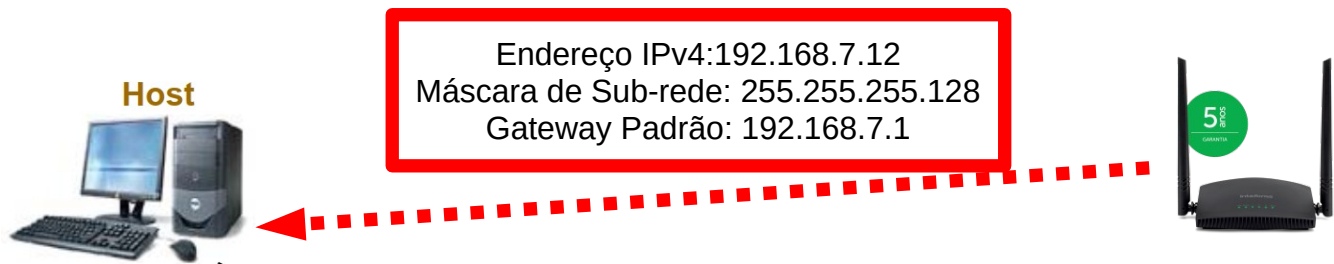
- Mas, a mais importante é apresentada como: Adaptador de Rede sem Fio Wi-Fi. É a interface que no momento está conectada à rede sem fio e, portanto, possui endereço IP, fornecido pelo servidor DHCP que está rodando no roteador Wi-Fi. Também executa o

protocolo de enlace Ethernet, que trata da conexão entre o adaptador e o roteador Wi-Fi, exclusivamente. O protocolo IP e seu endereço IPv4 tratam da conexão com hosts/computadores remotos (especificamente,

2 Sítio do VirtualBox: <https://www.virtualbox.org/>. Existem versões para Windows, Linux e Mac e com ele instalado é possível criar uma máquina virtual e instalar nela qualquer outro sistema operacional. Por exemplo: aqui no Windows ela executa uma máquina virtual do Linux Ubuntu Server.

com as interfaces dos mesmos).

Quais informações fornecidas pelo ipconfig para a interface de rede **Adaptador de Rede sem Fio Wi-Fi:**



Esses três elementos permitem que um computador possa estabelecer conectividade em rede e poder acessar uma rede externa (no caso a Internet). O endereço pode ser tanto o IPv4 ou o IPv6 ou ambos podem ser alocados à mesma interface. O endereço denominado de **link local** é alocado pelo sistema operacional (no caso o Windows) e **somente é para conectividade local entre computadores diretamente conectados**.

Para visualizar as informações mais completas, então há necessidade de executar o comando com a opção de mostrar tudo:

```
> ipconfig /all
```

E, um resultado parcial, ou seja, só da interface ativa na rede, segue mostrado na figura a seguir:

```
Adaptador de Rede sem Fio Wi-Fi:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Intel(R) Wireless-AC 9462
Endereço Físico . . . . . : 5C-CD-5B-4D-4A-81
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::c95a:99fb:1a17:be98%7(Preferencial)
Endereço IPv4. . . . . : 192.168.7.12(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.128
Concessão Obtida. . . . . : segunda-feira, 6 de julho de 2020 10:12:40
Concessão Expira. . . . . : segunda-feira, 6 de julho de 2020 13:43:51
Gateway Padrão. . . . . : 192.168.7.1
Servidor DHCP . . . . . : 192.168.7.1
IAID de DHCPv6. . . . . : 89967963
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-26-75-DF-21-5C-CD-5B-4D-4A-81
Servidores DNS. . . . . : 1.1.1.1
                          181.213.132.2
                          181.213.132.3
```

Agora, um conjunto completo de informações relacionadas ao funcionamento da pilha TCP/IP referentes à interface de rede **Adaptador de Rede sem Fio Wi-Fi:**

- **Descrição:** Intel® Wireless-AC 9462 [É o modelo da interface de rede sem fio presente no computador. Importante para questões de problemas de compatibilidade e de drivers.]
- **Endereço Físico:** 5C-CD-5B-4D-4A-81 [É o **endereço MAC**³ (*media access control address*) e identifica unicamente uma interface entre todas as outras interfaces Ethernet no mundo, independente se são placas para cabeamento RJ-45, placas de rede sem fio, interfaces de roteadores, etc]
- **DHCP Habilitado:** indica se o servidor está fornecendo endereço IP para este computador. No caso, o servidor DHCP está sendo executado no roteador Wi-Fi.
- **Endereço IPv6 de link local:** como informado anteriormente, se o DHCP não fornecer um endereço IP, então o sistema aloca um endereço chamado de link local (**com ele somente é possível fazer conexões na rede local**).
- **Endereço IPv4:** 192.168.7.12
- **Máscara de Sub-rede:** 255.255.255.128
- **Gateway Padrão:** 192.168.7.1

3 Informações: https://pt.wikipedia.org/wiki/Endere%C3%A7o_MAC

- **Servidores DNS:** 1.1.1.1, 181.212.132.2, 181.213.132.3

Aqui são três endereços IPv4 de servidores DNS. Eles não são requisitos para conectar à Internet, mas sem eles configurados não conseguiríamos acessar sítios pelos nomes, apenas por endereços IP. Por exemplo, se quiséssemos acessar o registro.br e os endereços DNS não estivessem funcionais, somente seria possível o acesso digitando o respectivo endereço IP: 200.160.2.3 O DNS é um protocolo core da rede, pois permite o uso de nomes em vez de endereços IP, mas não é requisito para conectividade Internet.

Observações:

a) Um endereço MAC é um identificador único de uma placa de rede (ou interface de rede) que é definida pelo fabricante da mesma. Então, diferente do endereço IP, que é definido pela rede em que se está no momento, o endereço MAC será sempre o mesmo, independente da rede, pois está gravado⁴ no chipset do mesmo. Como está vinculado ao fabricante, pode-se descobrir um fabricante pelo três primeiros bytes (ou seis primeiros caracteres hexadecimais) e fazendo consulta em determinados sítios. Por exemplo: os caracteres **5C-CD-58** foram alocados para a Intel, conforme pode pesquisar em:

<https://www.wireshark.org/tools/oui-lookup.html>

<https://standards.ieee.org/products-services/regauth/oui36/index.html>

b) Ainda sobre MAC, uma questão de notação: também é padrão usar dois pontos como separador de bytes: 5C:CD:58:4D:4A:81 (fora do mundo Microsoft, é o mais usado)

⁴ Apesar de não ser possível mudar um endereço MAC, há programas que conseguem alterá-lo: não é algo desejável na prática de redes.

DNS: exemplos dos comandos nslookup e dig

Resolução RECURSIVA (padrão) para o nome **www.google.br** usando **nslookup** e **dig**

\$ nslookup www.google.com 1.1.1.1

Server: 1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:

Name: www.google.com
Address: 142.250.219.132
Name: www.google.com
Address: 2800:3f0:4001:808::2004

Servidores DNS recursivos abertos e públicos:
<https://1.1.1.1/dns/>
<https://developers.cloudflare.com/1.1.1.1/setup>
<https://developers.google.com/speed/public-dns/>
<https://dns.google/>

Programa dig disponível em Linux:

\$ nome_a_resolver soa|ns|all|a|aaaa +recurse|+norecurse|+trace|+tcp|+dnssec @dns_server

\$ dig www.climate.gov aaaa @8.8.8.8

```
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> www.climate.gov @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62267
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.climate.gov.          IN      A
```

```
;; ANSWER SECTION:
www.climate.gov.          300     IN      CNAME   d20wafhwsciww2.cloudfront.net.
d20wafhwsciww2.cloudfront.net. 60 IN      A       18.67.136.74
d20wafhwsciww2.cloudfront.net. 60 IN      A       18.67.136.48
d20wafhwsciww2.cloudfront.net. 60 IN      A       18.67.136.61
d20wafhwsciww2.cloudfront.net. 60 IN      A       18.67.136.46
```

```
;; Query time: 332 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed May 31 16:20:52 UTC 2023
;; MSG SIZE rcvd: 151
```

\$ nslookup -type=ns .Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:

```
.      nameserver = m.root-servers.net.
.      nameserver = l.root-servers.net.
.      nameserver = k.root-servers.net.
.      nameserver = j.root-servers.net.
.      nameserver = i.root-servers.net.
.      nameserver = h.root-servers.net.
.      nameserver = g.root-servers.net.
.      nameserver = f.root-servers.net.
.      nameserver = e.root-servers.net.
.      nameserver = d.root-servers.net.
.      nameserver = c.root-servers.net.
.      nameserver = b.root-servers.net.
.      nameserver = a.root-servers.net.
```

\$ nslookup -type=a m.root-servers.net.**\$ nslookup -norec -type=a ufsc.br 150.162.1.84**Server: 150.162.1.84
Address: 150.162.1.84#53Name: ufsc.br
Address: 150.162.2.10Modo interativo do Nslookup (os comandos são inseridos diretamente no modo “comando”):**\$ nslookup**

```
> set rec
> set type=ns
> .
> set type=a
> m.root-servers.net.
```

```
> server 202.12.27.33
> set norec
> set type=ns
> br.
```

```
> server 200.219.159.10
> set norec          Obs.: dispensável, somente para reforçar o que estamos fazendo
> set type=ns
> ufsc.br.
```

Retornaram dados de servidores de nomes:

```
ufsc.br      nameserver = slave2.ufsc.br.
ufsc.br      nameserver = slave1.ufsc.br.
slave2.ufsc.br  internet address = 150.162.1.84
slave1.ufsc.br  internet address = 150.162.242.74
slave2.ufsc.br  has AAAA address 2801:84:0:1001:150:162:1:84
slave1.ufsc.br  has AAAA address 2801:84:0:1242:150:162:242:74
```

```
> server 150.162.1.84
> set type=a
> ufsc.br.
Server:      150.162.1.84
Address:     150.162.1.84#53
```

Name: ufsc.br
Address: 150.162.2.10

Resposta: endereço IP 150.162.2.10 referente ao nome ufsc.br e foi respondido por um servidor autoritativo para a respectiva zona (resposta autoritativa).

Uma resposta **Não Autoritativa**

\$ nslookup -type=a ufsc.br.

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: ufsc.br

Address: 150.162.2.10


```
$ dig ns .
```

```
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 27817
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;
;                IN      NS
;; ANSWER SECTION:
.                3793    IN      NS      m.root-servers.net.
.                3793    IN      NS      l.root-servers.net.
```

```
$ dig a l.root-servers.net.
```

```
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22114
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; QUESTION SECTION:
;l.root-servers.net.
;
;                IN      A
;; ANSWER SECTION:
l.root-servers.net. 3582139 IN      A      199.7.83.42
```

```
$ dig +nored ns @199.7.83.42 ufsc.br.
```

```
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41823
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; QUESTION SECTION:
;ufsc.br.
;
;                IN      A
;; AUTHORITY SECTION:
br.                172800 IN      NS      a.dns.br.
...
;; ADDITIONAL SECTION:
a.dns.br.          172800 IN      A      200.219.148.10
...
a.dns.br.          172800 IN      AAAA   2001:12f8:6::10
...
```

```
$ dig +nored ns @200.219.148.10 ufsc.br.
```

```
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 61391
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; QUESTION SECTION:
;ufsc.br.
;
;                IN      NS
;; AUTHORITY SECTION:
ufsc.br.          3600    IN      NS      slave1.ufsc.br.
ufsc.br.          3600    IN      NS      slave2.ufsc.br.
;; ADDITIONAL SECTION:
slave1.ufsc.br.   3600    IN      A      150.162.242.74
slave2.ufsc.br.   3600    IN      A      150.162.1.84
slave1.ufsc.br.   3600    IN      AAAA   2801:84:0:1242:150:162:242:74
slave2.ufsc.br.   3600    IN      AAAA   2801:84:0:1001:150:162:1:84
```

```
$ dig +nored a @150.162.242.74 ufsc.br.
```

```
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22264
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 2800
;; QUESTION SECTION:
;ufsc.br.
;
;                IN      A
;; ANSWER SECTION:
ufsc.br.          600     IN      A      150.162.2.10
```

Resposta: endereço IP 150.162.2.10 referente ao nome ufsc.br

NTP e tempo

Windows

Comando a seguir informa o status do relógio (tempo do sistema): ou configurado via relógio CMOS ou obtido por protocolo NTP

```
> w32tm /query /status
```

Para habilitar o NTP no Windows:

Painel de Controle > Relógio e Região > Data e Hora > Horário na Internet (aba)

Servidores de tempo:

- Serviço NTP.br (pertencente ao NIC.br): a.ntp.br, b.ntp.br e c.ntp.br
- Serviço time.nist.gov e time.windows.com

Linux

Comando básico disponível em distribuições Debian e Ubuntu:

```
$ timedatectl
```

Local time: Thu 2023-07-06 16:59:36 UTC

Universal time: Thu 2023-07-06 16:59:36 UTC

RTC time: Thu 2023-07-06 16:59:37

Time zone: Etc/UTC (UTC, +0000)

System clock synchronized: no

NTP service: inactive

RTC in local TZ: no

timedatectl - Control the system time and date

status

Show current settings of the system clock and RTC, including whether network time synchronization is active. If no command is specified, this is the implied default.

show

Show the same information as status, but in machine readable form.

Commands:

status	Show current time settings
show	Show properties of systemd-timedated
set-time TIME	Set system time
set-timezone ZONE	Set system time zone
list-timezones	Show known time zones
set-local-rtc BOOL	Control whether RTC is in local time
set-ntp BOOL	Enable or disable network time synchronization

systemd-timesyncd Commands:

timesync-status	Show status of systemd-timesyncd
show-timesync	Show properties of systemd-timesyncd

Cálculo em Sub-redes e endereços de Rede e de Broadcast (redes IPv4)

Basicamente é pegar a máscara de sub-rede e verificar quais bits são da sub-rede (ou seja, tudo zero). Por exemplo, para a máscara que aparece no resultado do ipconfig /all: 255.255.255.128

Máscara: 255. 255. 255. 128
Equivalente em binário: 11111111.11111111.11111111.10000000

Este bit de número 25 (por isso o endereço por vezes é escrito como 192.168.7.12/25) indica que ele pode assumir o valor zero ou um, logo poderia ter duas sub-redes. Foi escolhida a sub-rede 0, das duas possíveis (pode ser visto pelo sítio: <https://www.calculator.net/ip-subnet-calculator.html>):

Endereço de Rede (bits da parte de sub-rede igual a zero)	Faixa de endereços usáveis pelos dispositivos.	Endereço de Broadcast (bits da parte de sub-rede igual a um)
192.168.7.0	192.168.7.1 – 192.168.7.126	192.168.7.127
192.168.7.128	192.168.7.129 - 192.168.7.254	192.168.7.255

O endereço IP da interface é: 192.168.7.12, logo o equivalente em binário:

Endereço IP: 192. 168. 7. 12
Equivalente em binário: 11000000.10101000.00000111.00001100

Então, para endereço de broadcast, todos os bits da sub-rede (ou seja), os últimos que são zero na máscara, devem ser setados para 1, o que fica assim:

equivalente em binário: 11111111.11111111.11111111.01111111

Pois o bit de número 25 é zero no endereço IP.

Então em binário, voltando do endereço IP e setando todos os bits como um:

End broadcast em binário: 11000000.10101000.00000111.01111111

Equivalente: 192. 168. 7. 127

Este é o **endereço de broadcast**: 192.168.7.127 que os computadores usam numa rede local para descobrir outros computadores.

No sítio <https://www.calculator.net/ip-subnet-calculator.html> pode-se escolher a máscara que apareceu no resultado do ipconfig /all e incluir ela no campo

Subnet: 255.255.255.128/25 (no exemplo acima)

e no campo a seguir, o endereço IP da interface:

IP Address: 192.168.7.12

Calcular máscaras de rede e de sub-rede

Um sítio que permite cálculo de faixas de endereço IP dado o CIDR, é o seguinte. Há outros, além de ferramentas (programas) que podem ser instalados no Linux (e talvez no Windows também).

<http://jodies.de/ipcalc>

Segue um exemplo da tela:

Address (Host or Network)	Netmask (i.e. 24)	Netmask for sub/supernet (optional)
192.168.1.1	/ 24	move to: 26
<input type="button" value="Calculate"/>	<input type="button" value="Help"/>	

Por exemplo, tem-se um endereço IPv4 192.168.1.1/24 com máscara de sub-rede 255.255.255.0 (em binário, vinte e quatro bits ligados: 11111111.11111111.11111111.00000000) originalmente especificados para a rede e sub-rede. Então quer-se dividir essa sub-rede em sub-redes menores, de forma

que que serão usados mais alguns bits de host (aqueles que são zeros: haviam sobrado 8 bits zero, logo poderiam ser criados 256 hosts totais). Tirando um bit, a sub-rede fica:

11111111.11111111.11111111.10000000

Este bit pode tomar dois valores, logo posso criar duas sub-redes. Se tirasse dois bits, dividiria em quatro:

11111111.11111111.11111111.11000000

Mas, neste último caso, sobram menos bits para hosts. O sítio acima e vários outros irão fornecer quais seriam os endereços iniciais e finais de cada bloco criado.