

HERRAMIENTAS DEL SISTEMA EN WIMDOWS NT

Algunas de las herramientas del sistema para la red en Windows NT son:

1. ipconfig: Esta herramienta muestra la dirección IP, la máscara de subred y otros detalles de configuración de la red de la computadora.
2. ping: Esta herramienta se utiliza para verificar la conectividad de la red entre dos dispositivos. Envía un paquete de datos a una dirección IP específica y espera una respuesta.
3. tracert: Esta herramienta rastrea la ruta que toma un paquete de datos para llegar a su destino. Muestra cada salto que realiza el paquete a través de diferentes routers y servidores en su camino hacia su destino.
4. netstat: Esta herramienta muestra una lista de todas las conexiones de red activas en la computadora, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.
5. nslookup: Esta herramienta se utiliza para buscar la dirección IP correspondiente a un nombre de dominio o para buscar el nombre de dominio correspondiente a una dirección IP.
6. route: Esta herramienta se utiliza para configurar y ver la tabla de enrutamiento de la computadora, que se utiliza para determinar cómo se deben enrutar los paquetes de datos a través de la red.

Estas son solo algunas de las herramientas del sistema para la red en Windows NT. Hay muchas otras herramientas y utilidades disponibles para ayudar a configurar y solucionar problemas de redes en este sistema operativo.

HERRAMIENTAS DEL SISTEMA PARA RED EN LINUX

Algunas de las herramientas del sistema para la red en Linux son:

1. ifconfig: Esta herramienta muestra la dirección IP, la máscara de subred y otros detalles de configuración de red de la interfaz de red activa.

2. ping: Esta herramienta se utiliza para verificar la conectividad de la red entre dos dispositivos. Envía un paquete de datos a una dirección IP específica y espera una respuesta.

3. traceroute: Esta herramienta rastrea la ruta que toma un paquete de datos para llegar a su destino. Muestra cada salto que realiza el paquete a través de diferentes routers y servidores en su camino hacia su destino.

4. netstat: Esta herramienta muestra una lista de todas las conexiones de red activas en la computadora, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.

5. nmap: Esta herramienta se utiliza para escanear una red y encontrar los dispositivos que están activos y los puertos que están abiertos en ellos.

6. ip: Esta herramienta es una herramienta más avanzada para la configuración de la red en Linux. Permite configurar direcciones IP, rutas, interfaces de red y otros detalles de la red.

Estas son solo algunas de las herramientas del sistema para la red en Linux.

HERRAMIENTAS DEL SISTEMA PARA RED DE WINDOWS PROFECCIONAL

Algunas de las herramientas del sistema para la red en Windows Professional son:

1. ipconfig: Esta herramienta muestra la dirección IP, la máscara de subred y otros detalles de configuración de la red de la computadora.
2. ping: Esta herramienta se utiliza para verificar la conectividad de la red entre dos dispositivos. Envía un paquete de datos a una dirección IP específica y espera una respuesta.
3. tracert: Esta herramienta rastrea la ruta que toma un paquete de datos para llegar a su destino. Muestra cada salto que realiza el paquete a través de diferentes routers y servidores en su camino hacia su destino.
4. netstat: Esta herramienta muestra una lista de todas las conexiones de red activas en la computadora, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.
5. nslookup: Esta herramienta se utiliza para buscar la dirección IP correspondiente a un nombre de dominio o para buscar el nombre de dominio correspondiente a una dirección IP.
6. Remote Desktop Connection: Esta herramienta permite conectarse a un equipo remoto a través de la red y controlarlo como si estuviera sentado frente a él.
7. Shared Folders: Esta herramienta permite compartir carpetas y archivos con otros usuarios de la red.

Estas son solo algunas de las herramientas del sistema para la red en Windows Professional.

COMANDOS IMPORTANTES BASADO EN REDES EN WINDOWS NT

Aquí hay algunos comandos importantes basados en redes en Windows NT:

1. ipconfig: Esta herramienta se utiliza para obtener información sobre la configuración de red, como la dirección IP, la máscara de subred y la puerta de enlace predeterminada.
2. ping: Este comando se utiliza para verificar la conectividad de la red entre dos dispositivos. Envía un paquete de datos a una dirección IP específica y espera una respuesta.
3. tracert: Este comando se utiliza para rastrear la ruta que toma un paquete de datos para llegar a su destino. Muestra cada salto que realiza el paquete a través de diferentes routers y servidores en su camino hacia su destino.
4. netstat: Este comando se utiliza para mostrar una lista de todas las conexiones de red activas en la computadora, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.
5. nslookup: Este comando se utiliza para buscar la dirección IP correspondiente a un nombre de dominio o para buscar el nombre de dominio correspondiente a una dirección IP.
6. nbtstat: Este comando se utiliza para obtener información sobre los recursos compartidos y los nombres NetBIOS en la red.
7. route: Este comando se utiliza para mostrar y modificar la tabla de enrutamiento de la red.
8. arp: Este comando se utiliza para mostrar y modificar la tabla ARP de la red.
9. net: Este comando se utiliza para administrar usuarios, grupos, recursos compartidos y servicios de red.
10. telnet: Este comando se utiliza para conectarse a un servidor remoto a través de la red y administrarlo.

COMANDOS IMPORTANTES BASADO EN REDES EN LINUX

Aquí hay algunos comandos importantes basados en redes en Linux:

1. ifconfig: Este comando se utiliza para obtener información sobre la configuración de red, como la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```
root@virt225:~# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1892 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1892 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:885311 (864.5 KB)  TX bytes:885311 (864.5 KB)

venet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:127.0.0.1  P-t-P:127.0.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:5377 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4595 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1255667 (1.1 MB)  TX bytes:502559 (490.7 KB)

venet0:0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:84.246.215.14  P-t-P:84.246.215.14  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1

venet0:1  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.100.58  P-t-P:192.168.100.58  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
```

2. ping: Este comando se utiliza para verificar la conectividad de la red entre dos dispositivos. Envía un paquete de datos a una dirección IP específica y espera una respuesta.

```
soloetic@soloetic:~$ ping www.soloetic.com
PING www.soloetic.com (46.105.203.22) 56(84) bytes of data:
64 bytes from 46.105.203.22: icmp_seq=1 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=2 ttl=51 time=132 ms
64 bytes from 46.105.203.22: icmp_seq=3 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=4 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=5 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=6 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=7 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=8 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=9 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=10 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=11 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=12 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=13 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=14 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=15 ttl=51 time=131 ms
64 bytes from 46.105.203.22: icmp_seq=16 ttl=51 time=136 ms
64 bytes from 46.105.203.22: icmp_seq=17 ttl=51 time=131 ms
^C
--- www.soloetic.com ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16183ms
rtt min/avg/max/mdev = 131.234/131.946/136.795/1.333 ms
soloetic@soloetic:~$
```

3. traceroute: Este comando se utiliza para rastrear la ruta que toma un paquete de datos para llegar a su destino. Muestra cada salto que realiza el paquete a través de diferentes routers y servidores en su camino hacia su destino.

```
prabhakar@inspiron-3542:~$ traceroute google.com
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets
 1 192.168.43.45 (192.168.43.45)  2.014 ms  2.313 ms  2.588 ms
 2 * * *
 3 10.45.1.230 (10.45.1.230)  75.449 ms  115.244 ms  115.224 ms
 4 10.45.8.178 (10.45.8.178)  93.856 ms  115.138 ms  93.822 ms
 5 10.45.8.187 (10.45.8.187)  115.116 ms  115.106 ms  115.070 ms
 6 * * *
 7 218.248.235.141 (218.248.235.141)  120.589 ms  108.033 ms  106.962 ms
 8 218.248.235.142 (218.248.235.142)  114.489 ms  * *
 9 72.14.211.114 (72.14.211.114)  98.076 ms  93.232 ms  93.781 ms
10 108.170.253.113 (108.170.253.113)  98.688 ms  91.388 ms  108.170.253.97 (108.170.253.97)  107.241 ms
11 74.125.253.69 (74.125.253.69)  95.120 ms  72.14.237.165 (72.14.237.165)  102.594 ms  103.137 ms
12 maa03s23-ln-f14.1e100.net (172.217.26.206)  101.794 ms  97.987 ms  97.165 ms
prabhakar@inspiron-3542:~$
```

4. netstat: Este comando se utiliza para mostrar una lista de todas las conexiones de red activas en la computadora, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.

```

[isolvetic@localhost ~]$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:netbios-ssn     0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:http            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:localhost:domain  0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ipp             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:smtp            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:microsoft-ds      0.0.0.0:*               LISTEN
tcp6       0      0 :::netbios-ssn         ::::*                   LISTEN
tcp6       0      0 :::sunrpc              ::::*                   LISTEN
tcp6       0      0 :::http                ::::*                   LISTEN
tcp6       0      0 :::ssh                 ::::*                   LISTEN
tcp6       0      0 localhost:ipp          ::::*                   LISTEN
tcp6       0      0 localhost:smtp         ::::*                   LISTEN
tcp6       0      0 :::microsoft-ds        ::::*                   LISTEN
[isolvetic@localhost ~]$ _

```

5. nslookup: Este comando se utiliza para buscar la dirección IP correspondiente a un nombre de dominio o para buscar el nombre de dominio correspondiente a una dirección IP.

```

1 root@tecmin-arch ~ # pacman -Sy dnsutils
:: Synchronizing package databases...
core is up to date
extra is up to date
community
warning: bind-tools-9.14.7-1 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Packages (1) bind-tools-9.14.7-1

Total Download Size: 1.62 MiB
Total Installed Size: 5.88 MiB
Net Upgrade Size: 0.00 MiB

:: Proceed with installation? [Y/n] _

```

6. dig: Este comando se utiliza para buscar información detallada sobre un nombre de dominio.

```

susel:~ # dig linux-bible.com

; <<>> DiG 9.6-ESV-R7-P4 <<>> linux-bible.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59095
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;linux-bible.com.      IN      A

;; ANSWER SECTION:
linux-bible.com.      5      IN      A      198.57.241.163

;; Query time: 25 msec
;; SERVER: 192.168.198.2#53(192.168.198.2)
;; WHEN: Tue Sep 2 21:05:20 2014
;; MSG SIZE rcvd: 49

```

7. route: Este comando se utiliza para mostrar y modificar la tabla de enrutamiento de la red.

8. arp: Este comando se utiliza para mostrar y modificar la tabla ARP de la red.

9. ip: Este comando se utiliza para administrar direcciones IP, puertos y rutas de red.

10. ssh: Este comando se utiliza para conectarse a un servidor remoto de forma segura y administrarlo.

Estos son solo algunos de los comandos importantes basados en redes en Linux.

COMANDOS IMPORTANTES PARA RED EN WINDOWS PROFESSIONAL

Aquí hay algunos comandos importantes para redes en Windows Professional:

1. ipconfig: Este comando se utiliza para mostrar la configuración de red actual, incluyendo la dirección IP, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS.

```
C:\Users\HOSHIL>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
```

2. ping: Este comando se utiliza para comprobar la conectividad entre dos dispositivos enviando paquetes de datos a una dirección IP específica y esperando una respuesta.

```
C:\Users\HOSHIL>ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
        [-4] [-6] nombre_destino

Opciones:
  -t          Hacer ping al host especificado hasta que se detenga.
               Para ver estadísticas y continuar, presione
               Ctrl-Interrumpir; para detener, presione Ctrl+C.
  -a          Resolver direcciones en nombres de host.
  -n count    Número de solicitudes de eco para enviar.
  -l size     Enviar tamaño de búfer.
  -f          Establecer marca No fragmentar en paquetes (solo IPv4).
  -i TTL      Período de vida.
  -v TOS      Tipo de servicio (solo IPv4. Esta opción está desusada y
               no tiene ningún efecto sobre el campo de tipo de servicio
               del encabezado IP).
```

3. **tracert**: Este comando se utiliza para mostrar la ruta que un paquete de datos toma para llegar a su destino, mostrando cada salto que hace el paquete a través de diferentes routers y servidores.

```
C:\Users\HOSHIL>tracert

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
        [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
  -d          No convierte direcciones en nombres de hosts.
  -h saltos_máximos Máxima cantidad de saltos en la búsqueda del objetivo.
  -j lista-host  Enrutamiento relajado de origen a lo largo de la
                 lista de hosts (solo IPv4).
  -w tiempo_espera Tiempo de espera en milisegundos para esperar cada
                 respuesta.
  -R          Seguir la ruta de retorno (solo IPv6).
  -S srcaddr   Dirección de origen para utilizar (solo IPv6).
  -4          Forzar usando IPv4.
  -6          Forzar usando IPv6.
```

4. **netstat**: Este comando se utiliza para mostrar una lista de todas las conexiones de red activas en el equipo, junto con información sobre el protocolo utilizado, los puertos locales y remotos, y el estado de la conexión.

```
C:\Users\HOSHIL>netstat

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    127.0.0.1:49803       INCURCIO-117:49807    ESTABLISHED
TCP    127.0.0.1:49807       INCURCIO-117:49803    ESTABLISHED
TCP    192.168.0.124:49276   52.188.179.207:https  CLOSE_WAIT
TCP    192.168.0.124:49343   52.109.13.63:https    TIME_WAIT
TCP    192.168.0.124:49346   dsl-189-247-93-13-dyn:https FIN_WAIT_1
TCP    192.168.0.124:49349   qro01s23-in-f10:https ESTABLISHED
TCP    192.168.0.124:49350   ext-189-247-164-33:http TIME_WAIT
TCP    192.168.0.124:49351   20.69.137.228:https   ESTABLISHED
TCP    192.168.0.124:49352   192.229.211.108:http  ESTABLISHED
TCP    192.168.0.124:49353   https-208-111-157-0:http ESTABLISHED
TCP    192.168.0.124:49355   a23-49-40-171:http    ESTABLISHED
TCP    192.168.0.124:49356   qro01s27-in-f3:http   ESTABLISHED
```


5. nslookup: Este comando se utiliza para buscar la dirección IP correspondiente a un nombre de dominio o para buscar el nombre de dominio correspondiente a una dirección IP.

```
C:\Users\HOSHIL>nslookup
DNS request timed out.
    timeout was 2 seconds.
Servidor predeterminado: UnKnown
Address: 192.168.0.1
```

6. nbtstat: Este comando se utiliza para mostrar información sobre los recursos compartidos y los nombres NetBIOS en la red.

```
C:\Users\HOSHIL>nbtstat

Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP
usando NBT (NetBIOS sobre TCP/IP).

NBTSTAT [ [-a Nombreremoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [intervalo] ]
```

7. route: Este comando se utiliza para mostrar y modificar la tabla de enrutamiento de la red.

```
C:\Users\HOSHIL> route

Manipula tablas de enrutamiento de red.

ROUTE [-f] [-p] [-4|-6] comando [destino] [MASK máscara_red] [puerta_enlace]
[METRIC métrica] [IF interfaz]

    -f                Borra las tablas de enrutamiento de todas las entradas
                        de puerta de enlace. Si se usa junto con uno de los
                        comandos, se borrarán las tablas antes de ejecutarse el
                        comando.
```

8. arp: Este comando se utiliza para mostrar y modificar la tabla ARP de la red.

```
C:\Users\HOSHIL>arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones
físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
```

9. net: Este comando se utiliza para administrar usuarios, grupos, recursos compartidos y servicios de red.

```
C:\Users\HOSHIL>net
La sintaxis de este comando es:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

10. telnet: Este comando se utiliza para conectarse a un servidor remoto a través de la red y administrarlo.

CUADRO COMPARATIVO

Comando	Windows nt	linux	Windows Professional
ifconfig	No disponible	Muestra la configuración de red	No disponible
ipconfig	Muestra la configuración de red	No disponible	Muestra la configuración de red
ping	Comprueba la conectividad entre dispositivos	Comprueba la conectividad entre dispositivos	Comprueba la conectividad entre dispositivos
tracert/traceroute	Muestra la ruta de un paquete a su destino	Muestra la ruta de un paquete a su destino	Muestra la ruta de un paquete a su destino
Netstat	Muestra las conexiones de red activas	Muestra las conexiones de red activas	Muestra las conexiones de red activas

Nslookup	Realiza consultas DNS para buscar información	Realiza consultas DNS para buscar información	Realiza consultas DNS para buscar información
ssh	No disponible	Permite conectarse a un servidor remoto de forma segura	No disponible
dig	No disponible	Realiza consultas DNS avanzadas	No disponible