

Verificación de acuerdo con políticas de la organización

Breve descripción:

Este componente formativo aborda elementos generales y claves del proceso de verificación de dispositivos y servicios de red, según las políticas y criterios de la organización. Con su estudio responsable, el aprendiz podrá apropiarse de inspección física y lógica de la red, parámetros, comandos, monitoreos de rendimiento, protocolos de prueba y demás acciones propias del proceso.

Tabla de contenido

Introducción	1
1. Verificación de conectividad	3
1.1. Inspección física de la red	4
1.2. Inspección lógica de la red	5
2. Verificación de dispositivos de cómputo	16
3. Verificación de red	18
3.1. Monitoreo de rendimiento	19
3.2. Monitoreo de red	20
3.3. Protocolos de prueba	21
Síntesis	26
Material complementario	27
Glosario	28
Referencias bibliográficas	29
Créditos	30

Introducción

Reciba una gran bienvenida al estudio del componente formativo “**Verificación de acuerdo con políticas de la organización**”. Comience consultando el siguiente video, donde se ofrece un primer acercamiento y contextualización con los temas por desarrollar. ¡**Adelante!**

Video 1. Verificación de acuerdo con políticas de la organización



[Enlace de reproducción del video](#)

Síntesis del video: Verificación de acuerdo con políticas de la organización

Las acciones y procesos de prevención en cualquiera de las áreas y procesos de las organizaciones, es cada vez más habitual.

En términos financieros, es más barato invertir en prevención que gastar recursos y tiempo en reparaciones de cualquier índole.

Por esta razón, la monitorización de la infraestructura es un proceso que debe realizarse en tiempo real, de manera periódica, utilizando herramientas de observación, de análisis, de gestión, entre otras.

Al hablar de una infraestructura informática local, los conocimientos están más relacionados con el rendimiento que con los gastos habituales de gestión. En la actualidad, se tiene la posibilidad del despliegue de una infraestructura híbrida y en la nube.

Las grandes organizaciones, las cuales pueden tener cientos o miles de servidores o, incluso, las pymes con pocos servicios, propenden por la renta de una gestión más natural, donde la confiabilidad, disponibilidad, escalabilidad y buena relación costo / beneficio no se pueden descuidar.

Esta evolución ha llevado a que el “software” de gestión también vaya a la par. Los modelos híbridos giran en torno al seguimiento y administración de los recursos locales y externos, con igual facilidad y eficiencia.

Las arquitecturas en la nube tienen una gestión fácil de llevar, ya que estos “softwar” cumplen con GUI y UX de primera.

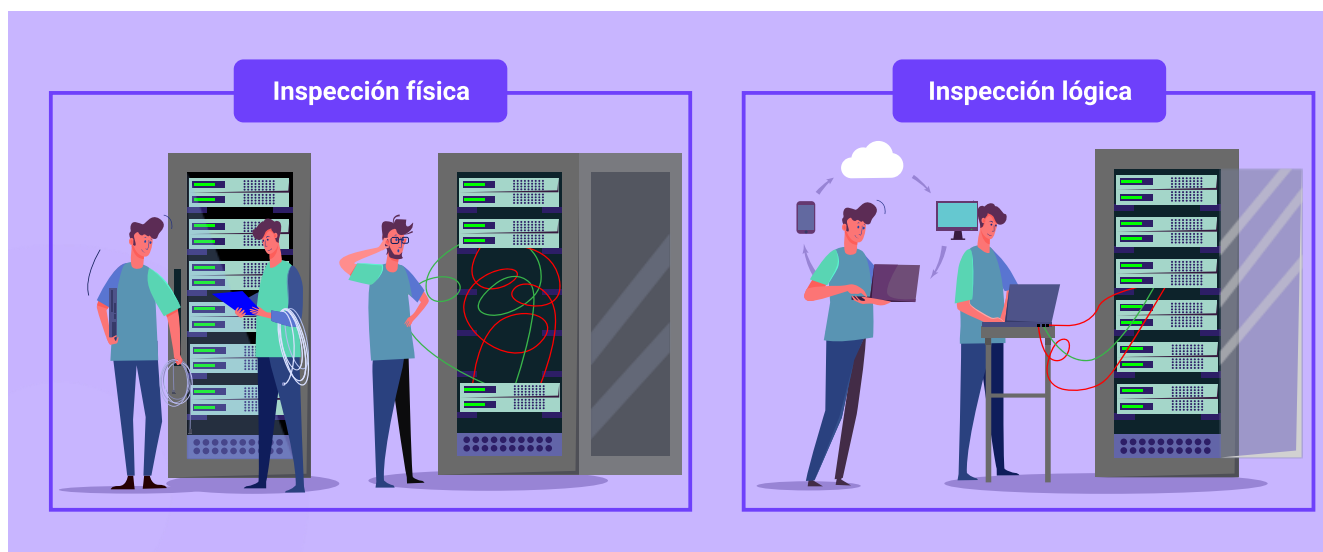
1. Verificación de conectividad

A partir del desarrollo de las infraestructuras tecnológicas, el personal encargado de la administración de la red realiza una verificación inicial antes del despliegue; esto para comprobar la instalación de los dispositivos periféricos y que su configuración cumpla con los requerimientos de la organización. Así mismo, se verifica la red de datos.

Para realizar esa actividad, los administradores cuentan con un conjunto de herramientas e instrumentos que pueden ser tanto físicos (cableado, dispositivos, conexiones, módems, etc.) como en “software” (configuraciones, comandos, etc.), dicha comprobación debe ser documentada a fin de realizar futuras revisiones.

La siguiente figura ilustra las características de cada tipo de inspección:

Figura 1. Inspección física e inspección lógica



1.1. Inspección física de la red

La primera comprobación consiste en la revisión física de la red mediante un recorrido donde se inspecciona el estado de los cables, los conectores, los paneles y los adaptadores de red.

Donde se requiera la inspección de la operatividad del cableado, se usan herramientas físicas para el testeo de la red; estos son:

- a. Comprobadores de continuidad.** También llamados “tester”, polímetro o multímetro, esta herramienta se usa para realizar mediciones de continuidad del cableado. Entre estos se encuentran dos tipos: multímetro y medidor de potencia de fibra óptica.
- b. Multímetro digital.** Mide magnitudes eléctricas (voltaje y corriente), algunos modelos miden también parámetros como temperatura ($^{\circ}\text{C}$, $^{\circ}\text{F}$), resistividad (Ω). Cuenta con dos cables de prueba usados para realizar la medición directa en el punto de conexión a verificar.
- c. Medidor de potencia de fibra óptica.** Sirven para verificar el cableado de fibra óptica, permite medir pérdidas y niveles de potencia e inspeccionar.
- d. Comprobadores de red.** Estas son herramientas que permiten comprobar el estado de conectividad física entre los dos extremos de los cables de red, la información que brinda esta prueba de continuidad, cruzamiento, terminales de conexión, entre otros.

Por otro lado, al realizar la verificación física de los dispositivos de red como “switch”, “router”, servidores, entre otros, se suele realizar una inspección rápida de los indicadores luminosos, comúnmente conocidos como LED, que proporcionan una vista rápida del estado de conexión del equipo.

Algunos identificadores LED que se encuentran en estos dispositivos son:

Tabla 1. Indicadores LED

LED	FUNCIÓN
Sistema o “Power”.	Indica si el equipo está encendido y conectado a la red eléctrica.
Estado del enlace del puerto.	Se asocia a la conexión del dispositivo en la red.
Modo del puerto.	Indica el modo de operación del puerto.
Velocidad de transmisión.	Indica la velocidad de transmisión a la que opera el puerto.

Nota: tomado de Castaño (2013).

1.2. Inspección lógica de la red

Es aquella que se implementa mediante “software”; permite verificar la conectividad lógica de la red. Esta inspección del sistema consta de comprobar que los parámetros de los dispositivos de dicha red estén correctamente configurados. Así, se puede revisar la comunicación interna y externa de los equipos en red.

Dentro de las inspecciones lógicas de red se encuentran:

Parámetros de red

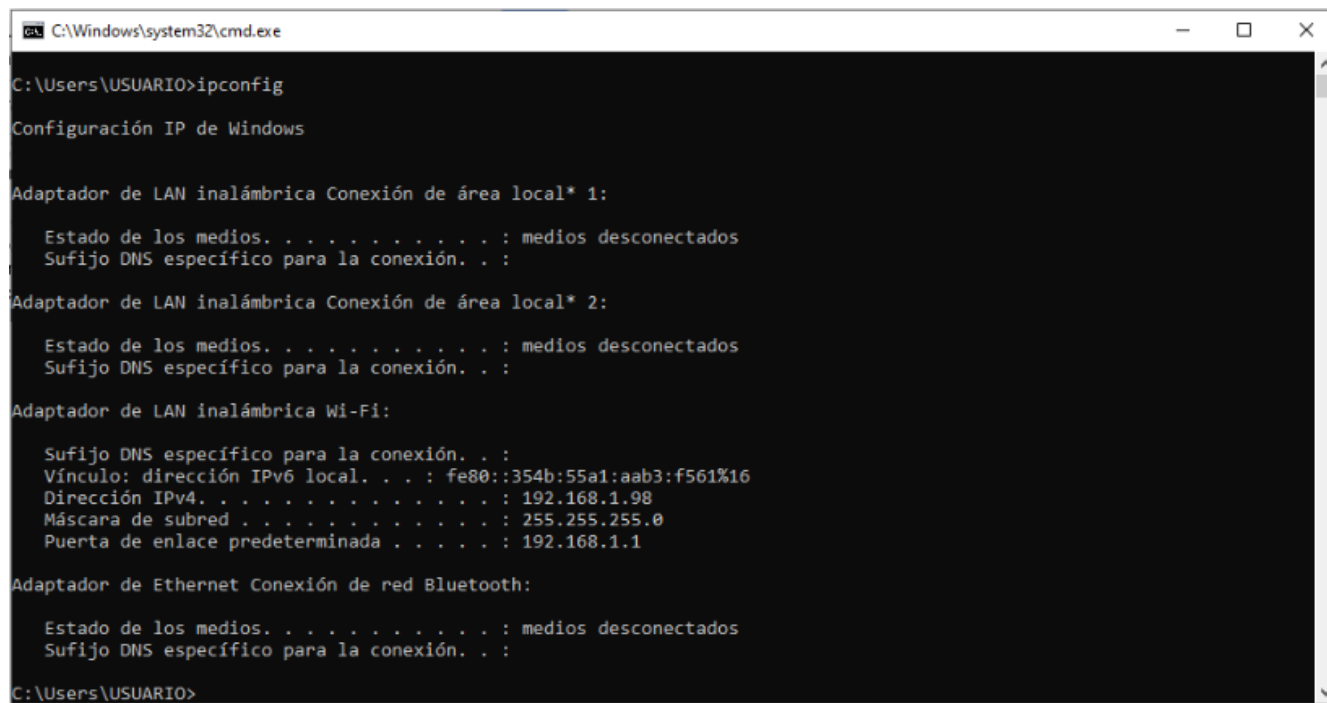
- Comando “ping”
- Comando “tracert” y “tracert”

- Comando ARP
- Comando “Route”
- Comando “Nslookup”

Parámetros de red

Para realizar dicha verificación se hace uso de los comandos del sistema “ipconfig” en sistemas operativos “Windows”, o “ifconfig” en sistemas operativos derivados de UNIX como Linux o MAC OS. Esta operación se realiza en el intérprete de comando conocido como **cmd.exe** o símbolo del sistema, su invocación muestra los parámetros básicos de la configuración TCP/IP de las interfaces de red habilitadas en los equipos de cómputo o estaciones de trabajo:

Figura 2. Comando “ipconfig”



```
C:\Windows\system32\cmd.exe

C:\Users\USUARIO>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

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

Adaptador de LAN inalámbrica Conexión de área local* 2:

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

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::354b:55a1:aab3:f561%16
    Dirección IPv4. . . . . : 192.168.1.98
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.1.1

Adaptador de Ethernet Conexión de red Bluetooth:

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

C:\Users\USUARIO>
```


Dentro de los parámetros de red a visualizar se tienen la dirección IP, la máscara de subred y la puerta de enlace predeterminada o “Gateway”.

Cuando se desee conocer mayor información de la configuración TCP/IP del equipo se puede recurrir a los siguientes comandos del sistema:

Tabla 2. Comandos del sistema

Windows	UNIX
“ipconfig/all” : muestra la información detallada de las interfaces del equipo.	“ifconfig-a” : muestra la información detallada de las interfaces del equipo.
“ipconfig/release” : permite borrar la configuración actual del adaptador de red.	“ifconfig interfaz address dirección_IP netmask” máscara : permite modificar los parámetros de acceso a la red de una interfaz según las especificaciones de dirección_IP y máscara configurados.
“Ipconfig/renew” : permite volver a cargar la configuración del adaptador de red.	“Ifconfig interfaz up” : habilita la interfaz indicada.

Nota: tomado de Castaño (2013).

Comando “ping”

“Ping” (“Packet Internet Groper”) está presente tanto en sistemas operativos Windows como en UNIX y en los sistemas operativos de red de algunos “routers”. El

comando “ping” emplea el protocolo ICMP (Protocolo de control y notificación de errores) que está implementado por el modelo TCP/IP.

Para verificar la conectividad de los dispositivos en red se especifica la dirección IP del dispositivo destino con el que se quiere establecer la conexión; si el comando “ping” no recibe respuesta, esto indica un problema de conectividad que se encuentra ubicado en algún elemento del nivel físico o de red, o en la misma configuración de red del equipo origen o destino.

Figura 3. Comando “ping” a dirección IP



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19042.631]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\USUARIO>tracert www.google.com.co

Traza a la dirección www.google.com.co [142.250.78.131]
sobre un máximo de 30 saltos:

 1    6 ms    3 ms    6 ms  192.168.1.1
 2     *      *      *      Tiempo de espera agotado para esta solicitud.
 3   17 ms   16 ms   16 ms  72.14.222.115
 4   53 ms   54 ms   55 ms  72.14.222.114
 5  133 ms   59 ms   61 ms  108.170.253.209
 6   59 ms   64 ms   59 ms  142.250.210.141
 7   59 ms   56 ms   55 ms  bog02s18-in-f3.1e100.net [142.250.78.131]

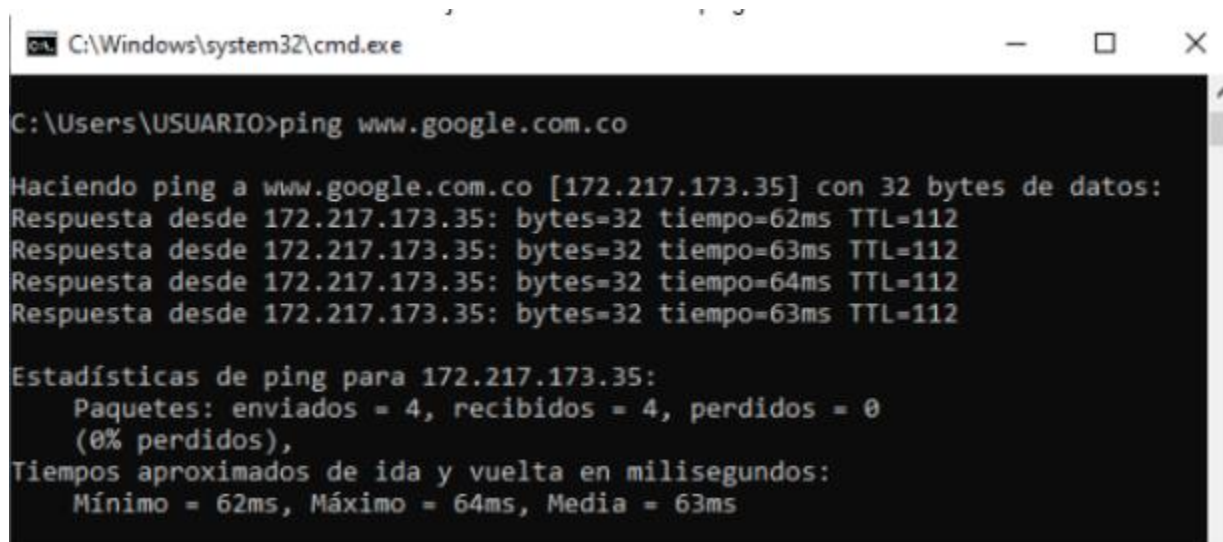
Traza completa.

C:\Users\USUARIO>

```

Para ejecutar la prueba “ping” se usa la ventana del símbolo del sistema digitando la siguiente línea: **“ping” dirección_IP_host_destino.**

Figura 4. Ejecución del comando ping a URL



```

C:\Windows\system32\cmd.exe

C:\Users\USUARIO>ping www.google.com.co

Haciendo ping a www.google.com.co [172.217.173.35] con 32 bytes de datos:
Respuesta desde 172.217.173.35: bytes=32 tiempo=62ms TTL=112
Respuesta desde 172.217.173.35: bytes=32 tiempo=63ms TTL=112
Respuesta desde 172.217.173.35: bytes=32 tiempo=64ms TTL=112
Respuesta desde 172.217.173.35: bytes=32 tiempo=63ms TTL=112

Estadísticas de ping para 172.217.173.35:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 62ms, Máximo = 64ms, Media = 63ms
  
```

La dirección IP 8.8.8.8 esta asignada a los servidores de Google. También se puede realizar ping a un sitio web en internet con el que se desea establecer conexión, usando la siguiente línea: **“ping” URL_pagina_web**.

Al usar el comando “ping”, este envía un mensaje ICMP con una solicitud de **echo** al equipo destino. Los resultados emitidos están conformados por el número de paquetes que se envían de origen a destino, los paquetes recibidos y los paquetes perdidos, incluyendo el tiempo de ida y vuelta de los paquetes, medido en milisegundos. Si la conexión a internet es la correcta se obtiene una respuesta donde los paquetes perdidos representan el 0 %.

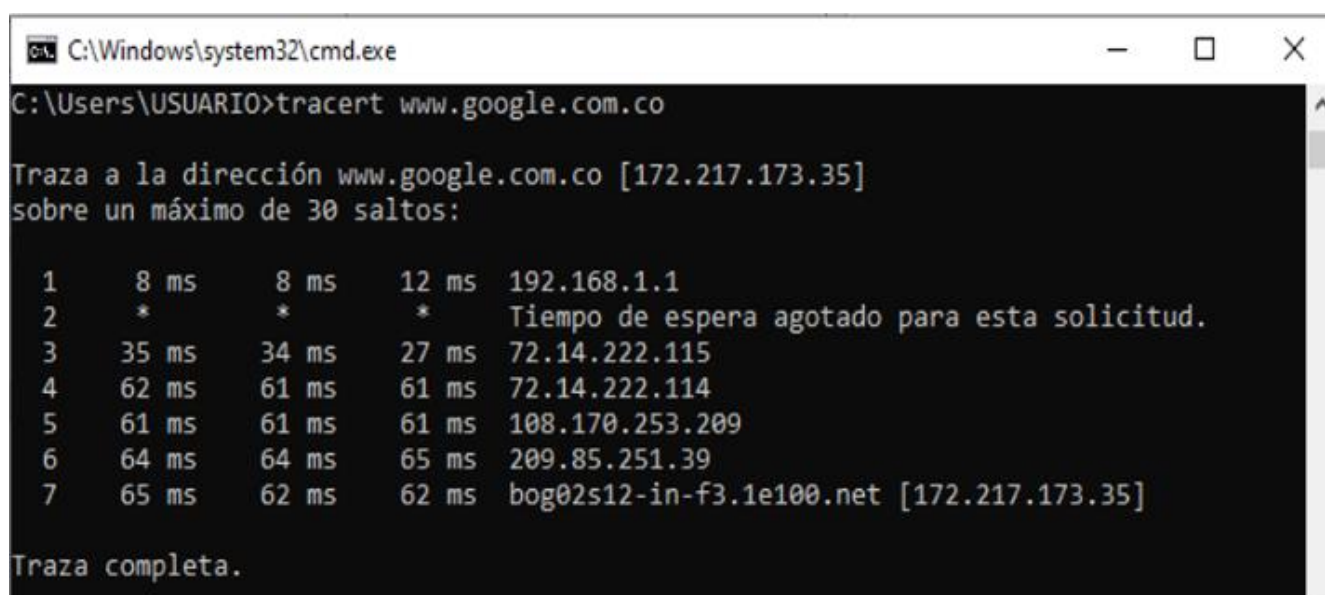
Comando “tracert” y “traceroute”

El comando “tracert” para sistemas operativos Windows y “traceroute” para sistemas operativos UNIX como MAC OS o Linux y para sistemas operativos de red de algunos “routers”, es una herramienta de diagnóstico que permite rastrear el recorrido de los paquetes y los tiempos de retardo que se producen. Al aplicar el comando, este

muestra los datos de los dispositivos de red y los nodos por los que pasa y el tiempo que toma cada salto hasta conseguir llegar al destino.

En sistemas Windows, para ejecutar este comando, se abre una ventana del sistema **cmd.exe** o símbolo del sistema. Allí, digitar la siguiente línea: **“tracert”**
URL_pagina_web.

Figura 5. Comando “tracert”



```

C:\Windows\system32\cmd.exe
C:\Users\USUARIO>tracert www.google.com.co

Traza a la dirección www.google.com.co [172.217.173.35]
sobre un máximo de 30 saltos:

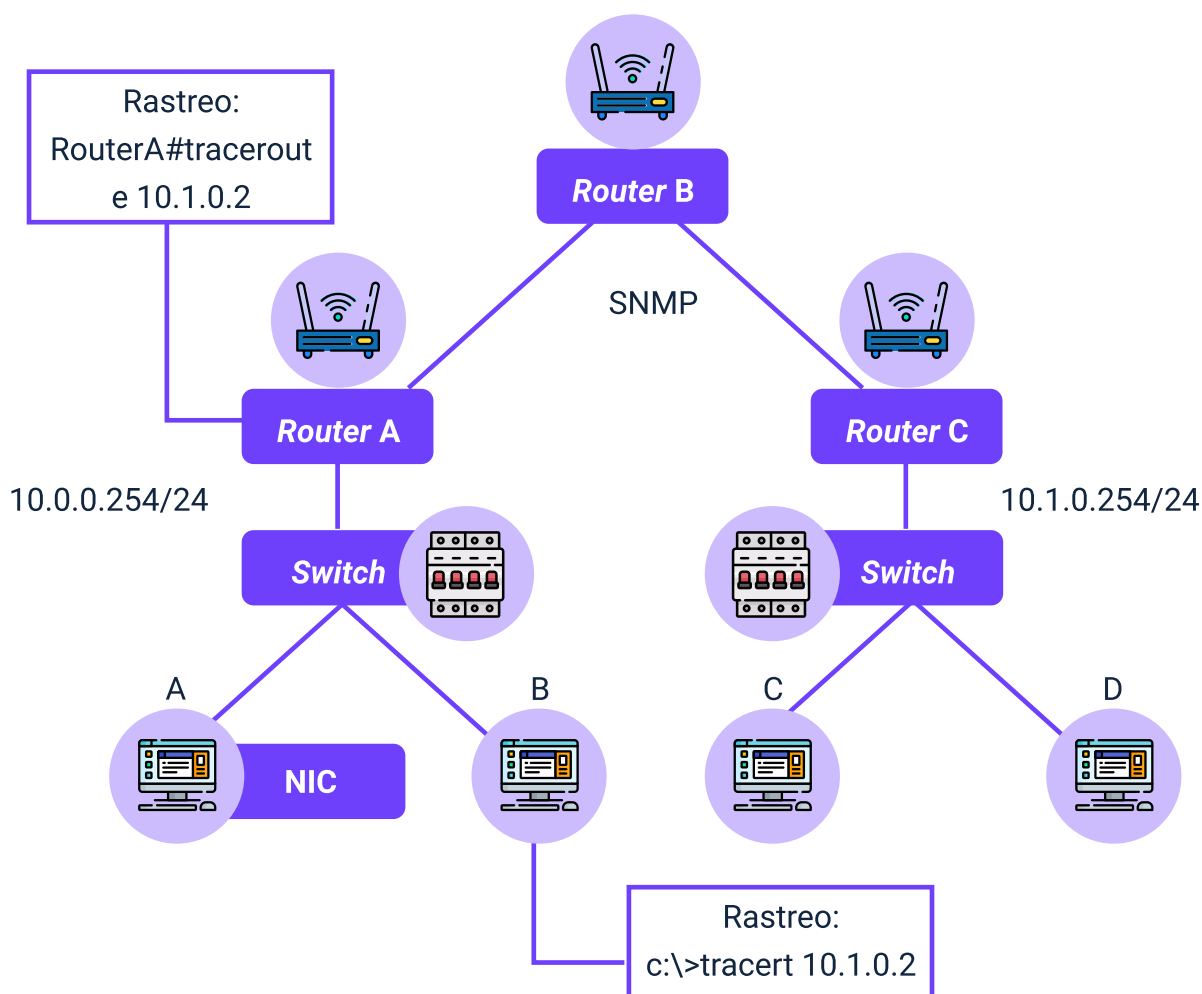
 1    8 ms    8 ms    12 ms    192.168.1.1
 2     *      *      *      Tiempo de espera agotado para esta solicitud.
 3   35 ms   34 ms   27 ms    72.14.222.115
 4   62 ms   61 ms   61 ms    72.14.222.114
 5   61 ms   61 ms   61 ms   108.170.253.209
 6   64 ms   64 ms   65 ms   209.85.251.39
 7   65 ms   62 ms   62 ms   bog02s12-in-f3.1e100.net [172.217.173.35]

Traza completa.
  
```

Para realizar la prueba de la ruta hacia un “host” remoto, se ejecuta desde un equipo Windows en la línea de comandos “tracert” seguido de la dirección IP destino; si se realiza desde un “router” se usa la línea “tracert” seguido de la dirección IP destino.

La figura siguiente, detalla más y mejor la ejecución del comando “tracert” y “tracert”:

Figura 6. Comando “tracert” y “traceroute”



La figura inmediatamente anterior da cuenta de las herramientas de diagnóstico de red que señalan la ruta que los datos siguen desde un dispositivo hasta su destino, revelando los nodos intermedios y los tiempos de respuesta en cada salto. Estas herramientas son cruciales para identificar posibles cuellos de botella y mejorar la eficiencia de la comunicación en la red.

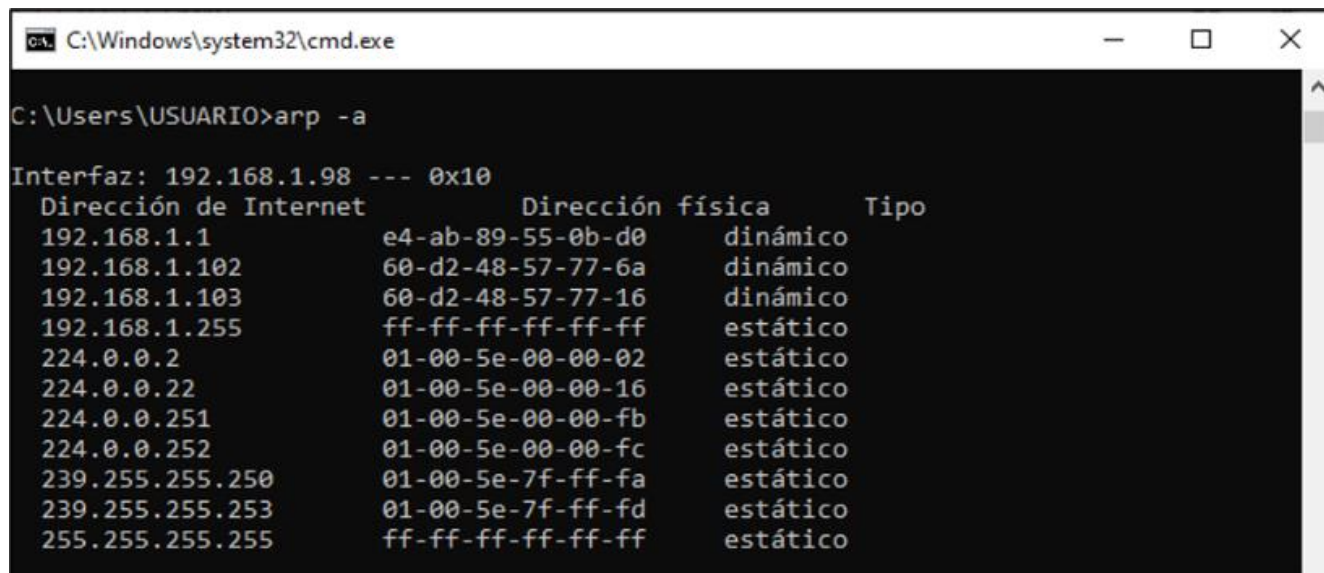
Las columnas con la información que se muestra en la pantalla después de la ejecución del comando “Tracert” indica, respectivamente: primera columna el número

de salto, las siguientes tres columnas el tiempo de respuesta de los paquetes que son enviados, donde el símbolo del asterisco (*) indica que no se obtuvo respuesta, y la última columna indica la dirección IP del nodo por el que pasa el paquete.

Comando ARP

El comando ARP, (Protocolo de resolución de direcciones) permite obtener la información de la tabla ARP del dispositivo en red.

Figura 7. Comando ARP



```

C:\Windows\system32\cmd.exe

C:\Users\USUARIO>arp -a

Interfaz: 192.168.1.98 --- 0x10
Dirección de Internet      Dirección física      Tipo
192.168.1.1                e4-ab-89-55-0b-d0    dinámico
192.168.1.102              60-d2-48-57-77-6a    dinámico
192.168.1.103              60-d2-48-57-77-16    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
239.255.255.253            01-00-5e-7f-ff-fd    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
  
```

Como sugiere la imagen del comando ARP, la tabla contiene una asociación de dirección IPv4 con su correspondiente dirección MAC o dirección física, incluido el tipo de direccionamiento IP (estático o dinámico). Para la ejecución del comando ARP se usa la ventana **cmd.exe** digitando la siguiente línea: **arp -a**.

Comando “Route”

Este comando es una herramienta del sistema que permite la consulta de las tablas de enrutamiento del equipo en red.

Figura 8. Comando “Route print”

```
C:\Windows\system32\cmd.exe
C:\Users\USUARIO>route print

=====
Lista de interfaces
17...2a 39 26 38 47 2b .....Microsoft Wi-Fi Direct Virtual Adapter
9...aa 39 26 38 47 2b .....Microsoft Wi-Fi Direct Virtual Adapter #2
16...28 39 26 38 47 2b .....Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
12...28 39 26 38 47 2c .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.1.1         192.168.1.98    45
127.0.0.0           255.0.0.0           En vínculo          127.0.0.1       331
127.0.0.1           255.255.255.255     En vínculo          127.0.0.1       331
127.255.255.255     255.255.255.255     En vínculo          127.0.0.1       331
192.168.1.0         255.255.255.0       En vínculo          192.168.1.98    301
192.168.1.98        255.255.255.255     En vínculo          192.168.1.98    301
192.168.1.255       255.255.255.255     En vínculo          192.168.1.98    301
224.0.0.0           240.0.0.0           En vínculo          127.0.0.1       331
224.0.0.0           240.0.0.0           En vínculo          192.168.1.98    301
255.255.255.255     255.255.255.255     En vínculo          127.0.0.1       331
255.255.255.255     255.255.255.255     En vínculo          192.168.1.98    301
=====
Rutas persistentes:
Ninguno

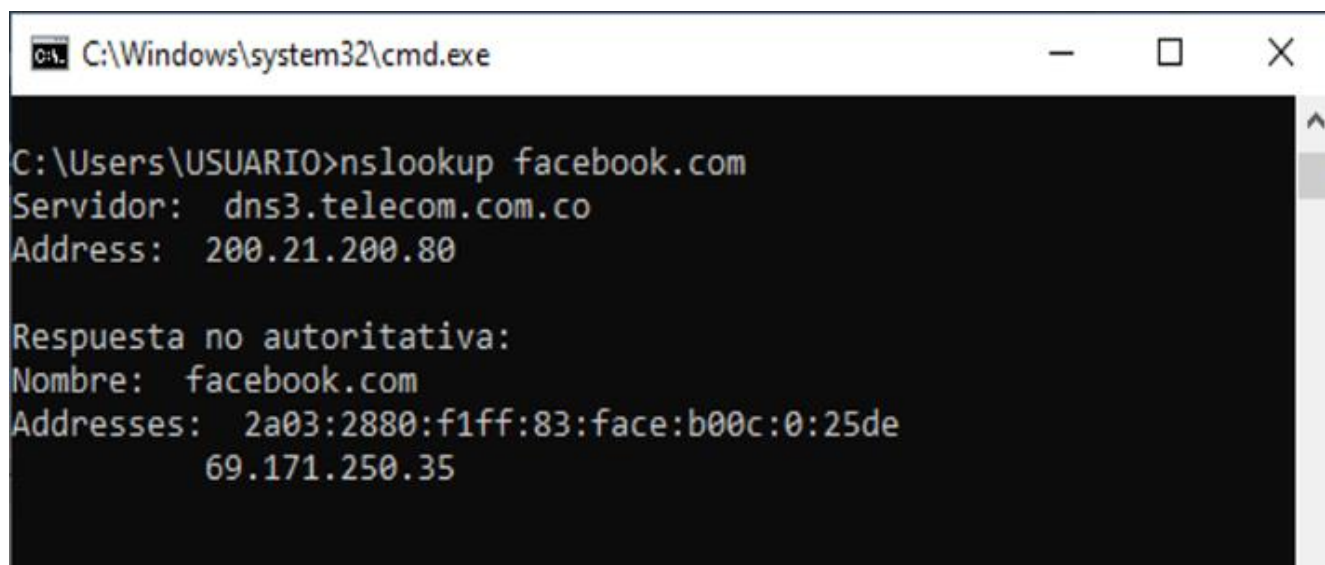
IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica    Puerta de enlace
1 331 ::1/128                      En vínculo
16 301 fe80::/64                  En vínculo
16 301 fe80::354b:55a1:aab3:f561/128
En vínculo
1 331 ff00::/8                    En vínculo
16 301 ff00::/8                    En vínculo
=====
Rutas persistentes:
Ninguno
```

Para consultar la información en sistemas operativos Windows en la ventana **cmd.exe** digitar la siguiente línea: **“route print”**, para sistemas derivados de UNIX digitar la línea: **“route -n**.

Comando “Nslookup”

Este comando es una herramienta del sistema que permite la comprobación del correcto funcionamiento del servidor DNS. La información asocia el nombre de dominio consultado a su respectiva dirección IPv4 o IPv6 según sea el caso.

Figura 9. Comando “nslookup”



```

C:\Windows\system32\cmd.exe

C:\Users\USUARIO>nslookup facebook.com
Servidor:  dns3.telecom.com.co
Address:  200.21.200.80

Respuesta no autoritativa:
Nombre:  facebook.com
Addresses:  2a03:2880:f1ff:83:face:b00c:0:25de
           69.171.250.35
  
```

La ejecución del comando se puede realizar de dos formas: una interactiva, donde en sistemas operativos Windows en la consola **cmd.exe** se digita: “nslookup”, al presionar la tecla “enter” se realizará una conexión con el servidor DNS y aquí se puede realizar la consulta digitando la URL. De otra forma no interactiva se digita el comando directamente en la consola **cmd.exe**, por ejemplo: “**nslookup**” **facebook.com**.

En el siguiente video se explican algunos de los comandos de red en Windows que pueden ser usados para verificar la conectividad de la red:

Video 2. Comandos de red en Windows



[Enlace de reproducción del video](#)

Síntesis del video: Comandos de red en Windows

Este es un video tutorial donde la instructora SENA ofrece los pasos y acciones por seguir en la revisión de los comandos de red de Windows, lo cual permite obtener toda la información sobre los equipos conectados en red.

2. Verificación de dispositivos de cómputo

Dentro de los sistemas informáticos, el uso de sistemas computacionales es constante. De tal modo, realizar una verificación de estos dispositivos dentro de una red es muy importante.

Dentro de las actividades de comprobación se encuentran:

- a. Rendimiento del sistema (“benchmark”).** Mide el rendimiento de cualquier componente del sistema desde la CPU hasta la tarjeta gráfica; el resultado de la prueba ejecutada mediante un programa, ya sea “online” o instalado en la máquina; devuelve información detallada de las características y evalúa si el equipo se encuentra funcionando de forma correcta o si presenta alguna falla. Algunos programas gratuitos para dicha verificación son: CPU-Z, HWMonitor, Speccy, entre otros.
- b. Simulación de cargas.** Una carga representa la cantidad de procesamiento que se le asigna a un dispositivo de cómputo; la carga de prueba es una similitud de la carga habitual de la máquina. Con esta verificación, lo que se busca es comprobar si dicho dispositivo es pertinente para la ejecución de una aplicación concreta.
- c. Consumo de recursos.** La ejecución del proceso genera un consumo de recursos que el administrador del sistema debe gestionar y controlar de forma adecuada. Los sistemas operativos tienen incorporado un administrador de tareas. Esta herramienta proporciona información sobre el o los procesos que se están ejecutando, entre otras características del sistema.
- d. Aplicaciones de monitorización.** Permiten verificar el estado de los parámetros del sistema. Dentro de las placas bases de los dispositivos de

cómputo actuales, la **BIOS** ofrece dichas funciones que contienen el monitoreo de componentes como el microprocesador, memoria, voltaje, entre otros.

3. Verificación de red

Para abordar la gestión de redes en sí, hay que considerar primero algunos escenarios a manera de ejemplo, en el cual componentes complejos del sistema interactúan y son inspeccionados, gestionados y monitoreados por un supervisor.

- El primer escenario a estudiar es el caso del panel de control de un avión, el cual le permite al piloto monitorear las variables operativas y analizar los datos para asegurar que los dispositivos estén operando dentro de los límites.
- Como segundo escenario, se tiene una planta de generación de energía eléctrica, esta tiene una sala de control donde los diales, medidores y luces monitorean el estado de las variables a verificar (presión, flujo, temperatura, entre otros) en las tuberías, válvulas, contenedores y otros componentes del sistema. Estos dispositivos de monitoreo le permiten al operador tomar acciones en caso de presentarse problemas inminentes.
- En una forma similar, el administrador de la red supervisará, gestionará y controlará prontamente el sistema que se le confía. La verificación de la red incluye un monitoreo de red; en un sentido más amplio indica la forma de supervisar de manera constante la funcionalidad de la red a fin de garantizar que los parámetros cumplen con las especificaciones del diseño de la organización.

Cuando un administrador encuentra un problema de red, puede ejecutar algunas verificaciones del sistema realizando inspección física o lógica, a fin de localizar el origen del problema y ajustar la configuración del sistema. Se puede optar por un reinicio del “hardware” o “software” o acceder de forma remota.

Las redes privadas y públicas han crecido de pequeñas redes a una gran infraestructura global, la necesidad de administrar la gran cantidad de componentes de “hardware” y “software” dentro de estas redes, de manera más sistemática, también se ha vuelto una tarea más importante. Además, en los sistemas informáticos se pueden configurar a fin de monitorear la red con avisos y alarmas que se envíen de forma automática al administrador de la red.

3.1. Monitoreo de rendimiento

Los monitoreos de rendimiento permiten analizar el rendimiento de la red. Son útiles a la hora de verificar las funciones de los dispositivos que se monitoreen.

Dentro de los parámetros de rendimiento de la red, usualmente monitoreados, se encuentran:

- a. **Estado de la CPU.** De acuerdo a las funcionalidades de la red, los dispositivos continuamente están transmitiendo paquetes de datos o tramas; debido a esto, el sistema puede sobrecargarse por la cantidad de servicios que se prestan como DHCP, DNS, cortafuegos, entre otros. El monitoreo permite verificar el rendimiento del procesador. Llegado el caso de presentarse una bajada en el rendimiento, el administrador tomará las acciones con el fin de solucionar.
- b. **Uso de la memoria.** La información de la red, como tablas de enrutamiento, se almacena en la memoria de los dispositivos de la capa de red. Esta gran cantidad de información puede ocasionar que se colapse el almacenamiento interno; por tal motivo, el rendimiento de la red se verá afectado ocasionando pérdida de paquetes en la transmisión de datos o caída de los servicios de red.

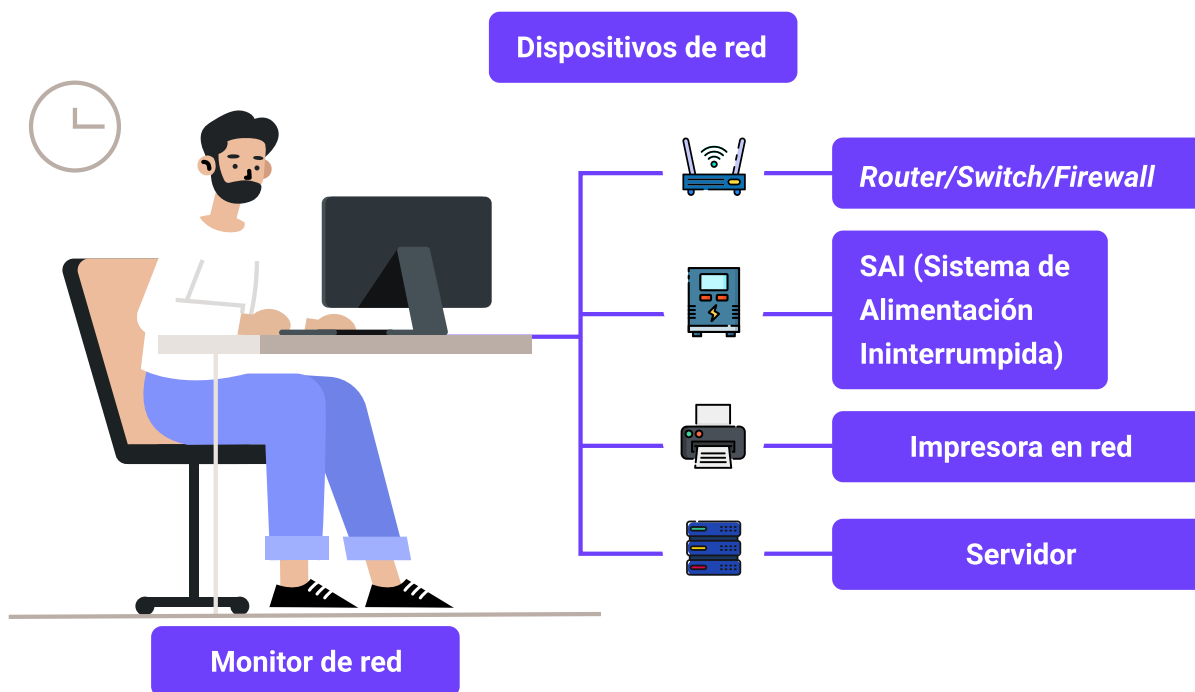
- c. **Tipo de tráfico.** El monitoreo del tráfico de la red resulta útil para detectar posibles congestiones o un exceso de solicitudes de servicios como HTTP o DHCP.

3.2. Monitoreo de red

Dentro de las fases más largas de la ejecución y puesta en marcha de sistemas informáticos, está la monitorización de la red, la cual permite la supervisión a fin de detectar posibles fallas en la red y verificar su correcto funcionamiento.

El monitoreo de red no es exclusivo para organizaciones con infraestructuras de red extensas; también es necesario y conveniente realizar una supervisión en redes con pocos dispositivos a fin de detectar problemas que afecten los servicios prestados por la empresa.

Figura 10. Elementos a monitorear en red



Nota: adaptado de Castaño (2013).

La figura inmediatamente anterior sugiere, como elementos de monitoreo en una red, los siguientes:

- “Router” / “Switch” / “Firewall”.
- SAI (Sistema de Alimentación Ininterrumpida).
- Impresora en red.
- Servidor.

Entre las herramientas de monitorización de la red se puede mencionar:

- **Analizadores de protocolos.** También conocidos como “sniffers”. Estos analizan el tráfico de la red y proporcionan datos como cantidad y tipo de tráfico. Lo principal, al examinar las tramas de red, es detectar los tipos de protocolos que se están usando, para prevenir posibles ataques del exterior de la red.
- **Algunos ejemplos de analizadores.** **Tcpdump** para sistemas UNIX, pertenece a “software” libre. **Wireshark**, esta herramienta está disponible para sistemas UNIX y Windows. **Ntop** herramienta de “software” libre.
- **Monitorización remota.** Son herramientas en las que un dispositivo de red recopila y analiza los datos resultantes del monitoreo de los dispositivos de red y los centraliza en un único dispositivo que facilita la consulta por parte del administrador de red.

3.3. Protocolos de prueba

Se trata de protocolos incorporados al modelo TCP/IP que permiten una administración y gestión de la red. Dichos protocolos conforman un conjunto de

lineamientos que son reglas e instrucciones que permiten a los dispositivos compartir información en la red; los sistemas de monitoreo de red aplican estos protocolos para identificar fallas y notificar al administrador de la red.

Según Valdivia (2020) hay dos protocolos importantes, que son usados para testear redes de datos:

- “Internet Control Message Protocol” (ICMP): es el Protocolo de mensajes de control de Internet.
- “Simple Network Management Protocol” (SNMP): es el Protocolo simple de administración de redes.

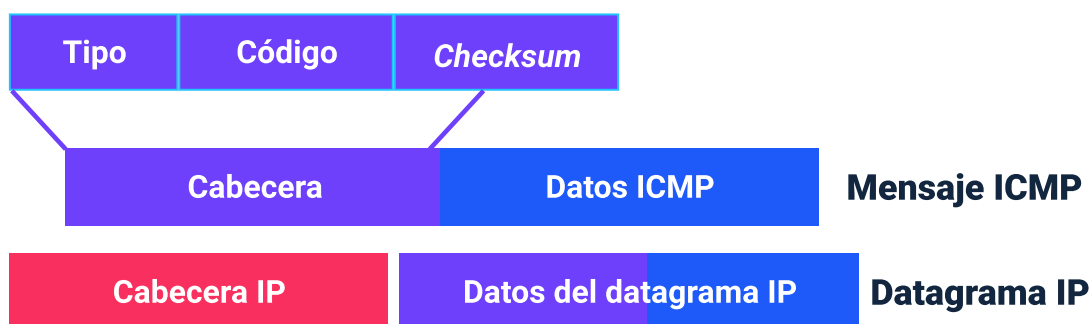
Protocolo ICMP

Es un protocolo ubicado en la capa de red del modelo TCP/IP. Los dispositivos que trabajan en esta capa como los “routers” y servidores, usan este protocolo para enviar información sobre incidencias en la red. Este protocolo permite el envío de mensajes ICMP que se transmiten como datagramas IP, a través de la red.

Dentro de las funcionalidades de los mensajes ICMP, está la de confirmar si un destino se encuentra activo y es alcanzable; también, informar problemas de parámetros en una cabecera de datagrama, la sincronización de reloj y las estimaciones de tiempo de tránsito; además, obtiene direcciones de Internet y máscaras de subred.

La figura siguiente muestra el formato del mensaje ICMP:

Figura 11. Formato del mensaje ICMP



Nota: adaptado de Valdivia (2020).

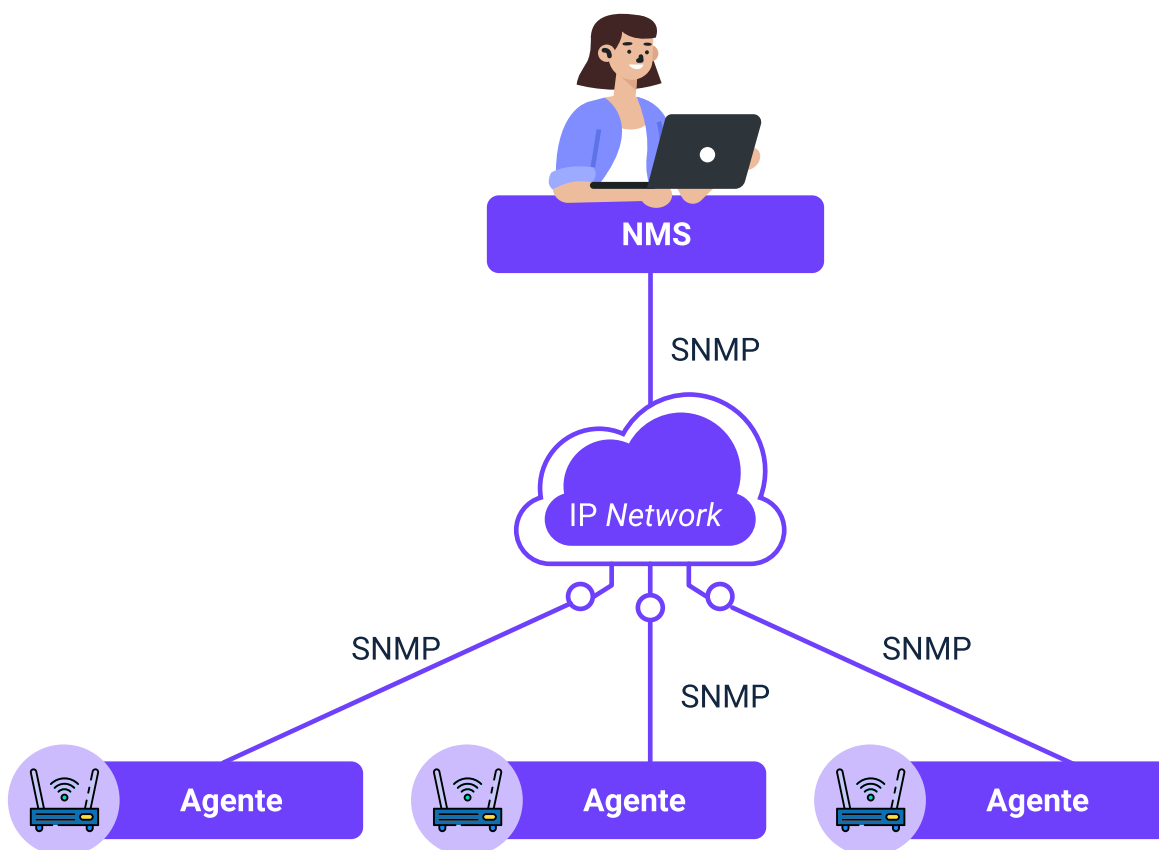
El desglose del formato del mensaje ICMP se detalla así:

- Tipo, código, “Checksum”
- Cabecera y datos ICMP
- Cabecera IP y datos del datagrama IP

Protocolo SNMP

Este protocolo se ubica en la capa de aplicación del modelo TCP/IP. Fue desarrollado para administrar servidores, estaciones de trabajo, “Switches”, “Routers”, “Access points”, entre otros. En una red de datos, el protocolo SNMP facilita el intercambio de información mediante el modelo cliente/servidor, proporcionando funciones de monitoreo de red que permita la supervisión de dispositivos de red.

Figura 12. Esquema SNMP



Los elementos claves a la hora de monitorizar una red basados en el protocolo SNMP son:

- a. **Agente de gestión.** Representa el “software” que se encuentra instalado en los equipos que se desean gestionar/monitorear. Estos mismos proporcionan la información que solicite el NMS, además este protocolo permite la gestión de forma remota.
- b. **NMS (“Network Management Station”).** Representa la estación de gestión de la red, requiere la instalación de “software” específico, que permita gestionar/monitorizar la red. Dentro del “software” de gestión de

SNMP se encuentra la “suite” **Net-SNMP** que integra diversas aplicaciones de gestión de red, basadas en el protocolo SNMP.

El funcionamiento de los elementos del protocolo SNMP se basa en la estructura de datos normalizada, denominada MIB (“Management information base”).

Simplemente, es una base de información con los datos que se reciben de los dispositivos gestionados, llamados agentes. El intercambio de información entre el NMS y el agente de gestión se realiza a través del protocolo UDP en el nivel de transporte.

Son tres las versiones del protocolo SNMP: **SNMPv1**, **SNMPv2**, y **SNMPv3**. Las versiones 1 y 2 no poseen mecanismo de cifrado de los mensajes SNMP. Si se desea proteger la información que se intercambia a fin de evitar posibles ataques, se debe usar la versión 3.

Síntesis

Ha llegado al final de los contenidos de este componente formativo. En este punto, haga un análisis del mapa que se muestra enseguida y realice su propia síntesis de los temas, conceptos y elementos desarrollados. ¡Adelante!



Este esquema de contenidos, muestra cómo la verificación de dispositivos y redes, orienta hacia la apropiación de conceptos y habilidades para la inspección física y lógica de la red, parámetros, comandos, monitoreos de rendimiento, protocolos de prueba y demás acciones conexas al proceso.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
3.3. Protocolos de prueba	Network Direction (2020). How SNMP Works Network Fundamentals Part 24.	Video	https://www.youtube.com/watch?v=vWZefoGNk5g

Glosario

“Checksum”: detecta cambios inesperados en una cadena de datos, verificando su integridad.

CPU: siglas que indican Unidad de Procesamiento Central, aquí se encuentran los componentes que permiten a los equipos electrónicos realizar el procesamiento de datos.

SAI: sistema de alimentación ininterrumpida o también conocido como UPS son dispositivos que sirven para proporcionar una protección eléctrica.

UDP: es el protocolo de datagramas de usuario, permite la transmisión de datagramas en red.

UNIX: sistema operativo multitarea y multiusuario. Los posteriores desarrollos de este sistema son Linux, MAC OS X, Android, iOS, entre otros.

URL: localizador de recursos uniforme, es un identificador que se le asigna a los recursos disponibles en internet como páginas WEB, textos, fotos, videos, entre otros. La URL tiene su correspondencia con una dirección IP.

Referencias bibliográficas

Ariganello, E. (2020). Redes cisco - Guía de estudio para la certificación CCNA 200-301. alphaeditorialcloud. <https://aprenderedes.com/wp-content/uploads/2020/04/CCNA-200-301-indice.pdf>

Castaño Ribes, R. J. (2013). Redes locales. Macmillan Iberia S.A. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/43257?page=298>

Valdivia, C. (2020). Sistemas informáticos y redes locales. Ediciones Paraninfo S.A.

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Mauricio Tovar Artunduaga	Experto Temático	Centro de Servicios y Gestión Empresarial. Regional Antioquia.
Jorge Eliécer Loaiza Muñoz	Experto Temático	Centro de Diseño e innovación tecnológica industrial. Regional Antioquia.
Cinthia Rocío Trejos Chacón	Experta Temática	Centro de la Industria, la empresa y los servicios. Regional Norte de Santander.
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Regional Santander – Centro Industrial del Diseño y la Manufactura
Blanca Flor Tinoco Torres	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander