



Herramientas y tecnologías

Gestión de Redes

Tipos de herramientas

Pruebas de
capa física

Alcanzabilidad
y conectividad

Análisis de
paquetes

Descubrimiento

Interrogación
de dispositivos

Monitorización
de eventos

Monitorización
de rendimiento

Análisis de flujo

Ingeniería de
encaminamiento
y tráfico

Configuración

Aplicación de
Seguridad

Planificación de
red

Pruebas de capa física

- Puede haber fallos en la red por problemas físicos.
 - ▣ Cables en mal estado, fibras ópticas mal soldadas....
 - ▣ Interferencias entre señales, ruidos, diafonías
- Herramientas de diagnosis (dispositivos):
 - ▣ **Tester cableado**
 - **Carrier sensor**: verifica la señal en las líneas de un cable (led).
 - **Reflectómetros**: pueden saber a qué distancia se ha cortado un cable.
 - **Certificador de cableado**: verifica que los parámetros de transmisión (diafonía, nivel de señal...) cumplen con la norma.
 - ▣ **Tester wifi**: verifica que la señal wifi es adecuada y que no tiene interferencias



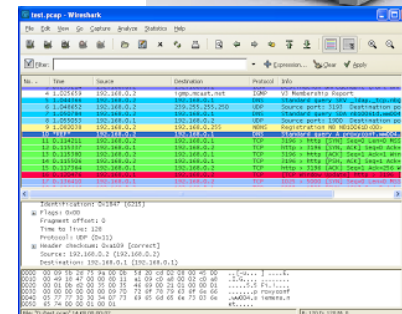
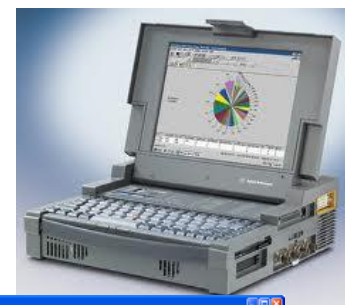
Alcanzabilidad y conectividad

- Conocer si hay conexión entre dos puntos de la red.
- Normalmente se comprueba en capa de red:
 - ▣ **Ping** es la herramienta más usada.
 - Basada en ICMP, ampliamente desplegada en dispositivos TCP/IP
 - Ofrece información de retardo
 - Ampliamente desplegada en los sistemas y fácil de usar
 - Permite automatizar procesos complejos de descubrimiento mediante scripts.
 - Opciones avanzadas:
 - **Selección de tamaño del paquete** permite verificar si hay problemas con paquetes grandes.
 - Enviar un flujo constante de peticiones (1 req/seg).
 - Definir tiempo de la prueba y obtener estadísticas sobre resultados.



Análisis de paquetes

- Analizador de protocolos puede ser:
 - ▣ Hardware
 - ▣ Software: **Wireshark** <http://www.wireshark.org>
- Diagnóstico de problemas:
 - ▣ Análisis de protocolos.
 - ▣ Captura de paquetes para post-procesamiento
 - ▣ Definir filtros de paquetes o flujos en la captura o el análisis.
- Contabilidad, análisis de rendimiento
 - ▣ Informes de interconexión: ¿quién habla con quién?
 - ▣ Estadísticas de tráfico: por host, por tipo de protocolo...



Descubrimiento de rutas

- Usado para saber detalles sobre el punto en el que falla una conexión.
- Ampliamente usada la aplicación **Traceroute / Tracert**
 - ▣ Proporciona información sobre los routers intermedios (saltos) por los que se pasas para llegar a un destino y el retardo de cada salto.

```
tracert www.google.com
```

```
tracert: Warning: www.google.com has multiple addresses; using 173.194.34.211
```

```
tracert to www.google.com (173.194.34.211), 64 hops max, 52 byte packets
```

```
 1 192.168.67.254 (192.168.67.254) 0.936 ms 0.569 ms 0.561 ms
```

```
 2 172.29.0.254 (172.29.0.254) 0.713 ms 0.662 ms 0.597 ms
```

```
 3 193.145.14.126 (193.145.14.126) 2.177 ms 1.715 ms 1.639 ms
```

```
 4 redimadrid.xe0-0-5-51.ciemat.rt1.mad.red.rediris.es (130.206.212.9) 2.240 ms 2.198 ms 2.040 ms
```

```
 5 193.149.1.94 (193.149.1.94) 6.440 ms 3.299 ms 3.157 ms
```

```
 6 216.239.49.196 (216.239.49.196) 3.325 ms 3.296 ms 3.175 ms
```

```
 7 72.14.237.124 (72.14.237.124) 3.437 ms 3.579 ms 3.440 ms
```

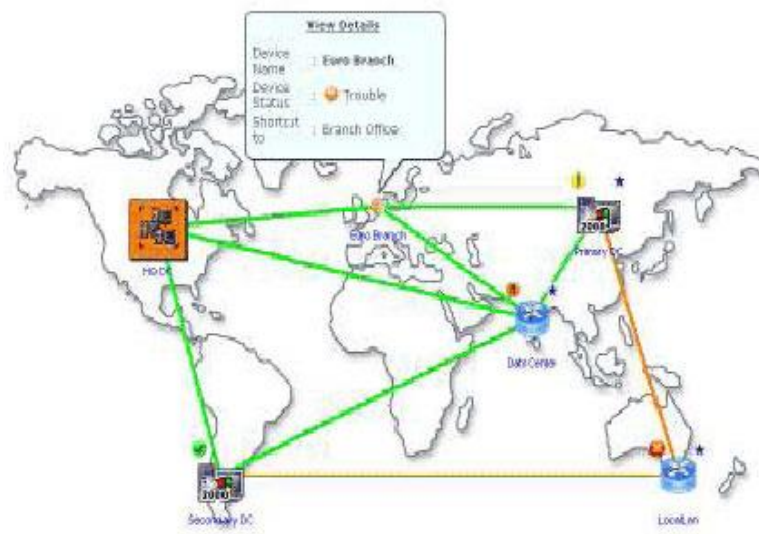
```
 8 mad01s08-in-f19.1e100.net (173.194.34.211) 3.132 ms 3.153 ms 3.148 ms
```

Descubrimiento de topología

- El inventario de una red incluye la topología y es interesante de mantener para la Herramientas y Tecnologías.
- Internet es fácilmente extensible: tecnología de switches es cero configuración.
- Esto puede originar el cambio de topología indocumentada en grandes redes de empresas.
- El objetivo del descubrimiento de topología es mantener actualizada la información.

Descubrimiento de topología

- Herramientas gráficas que descubren los interfaces con dirección IP y los dibujan separados por subredes.
- Protocolos: LLDP (Link-Layer Discovery Protocol), CDP, etc.
- Disponible en las plataformas de gestión: ej. **OPManager**
 - ▣ Visualiza Topología jerárquica: zoom en subredes.
 - ▣ Mapa de localización.



Interrogación de dispositivos

□ Lectura del estado de los dispositivos

▣ Interfaz en línea de comandos (CLI)

- Muchos elementos de red soportan CLI
- Preguntar sobre estado de interfaces (up/down) y configuración
- Consola y pregunta mediante comandos
- Consulta directa del administrador/gestor. No programable.

▣ Interfaces Web (GUI, REST, etc.)

- Interfaz gráfico para ver el estado y configuración de los dispositivos.
- Consulta directa del administrador/gestor. No programable.

▣ Interfaces programados

- Útil para consultar un dispositivo mediante un programa.
- El usuario puede usar una aplicación que utiliza este método.
- Ejemplos: [SNMP](#), CMIP/XML

Interrogación de dispositivos: Ejemplo ONOS (CLI y REST)

```
Welcome to Open Network Operating System (ONOS)!
```



```
Documentation: wiki.onosproject.org
Tutorials:    tutorials.onosproject.org
Mailing lists: lists.onosproject.org
```

```
Come help out! Find out how at: contribute.onosproject.org
```

```
Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown ONOS.
```

```
onos> devices
```

```
id=of:0000000000000001, available=true, role=MASTER, type=SWITCH, mfr=Nicira, Inc., hw=Open vSwitch, sw=2.0.2, serial=None, driver=ovs, channelId=127.0.0.1:33489, managementAddress=127.0.0.1, protocol=OF_10
id=of:0000000000000002, available=true, role=MASTER, type=SWITCH, mfr=Nicira, Inc., hw=Open vSwitch, sw=2.0.2, serial=None, driver=ovs, channelId=127.0.0.1:33488, managementAddress=127.0.0.1, protocol=OF_10
id=of:0000000000000003, available=true, role=MASTER, type=SWITCH, mfr=Nicira, Inc., hw=Open vSwitch, sw=2.0.2, serial=None, driver=ovs, channelId=127.0.0.1:33487, managementAddress=127.0.0.1, protocol=OF_10
```

```
GET http://127.0.0.1:8181/onos/v1/devices
```

```
Enter username for karaf at 127.0.0.1:8181: onos
```

```
Password:
```

```
{"devices":[{"id":"of:0000000000000003","type":"SWITCH","available":true,"role":"MASTER","mfr":"Nicira, Inc.,"hw":"Open vSwitch","sw":"2.0.2","serial":"None","chassisId":"3","annotations":{"managementAddress":"127.0.0.1","protocol":"OF_10","channelId":"127.0.0.1:33487"}},{ "id":"of:0000000000000001","type":"SWITCH","available":true,"role":"MASTER","mfr":"Nicira, Inc.,"hw":"Open vSwitch","sw":"2.0.2","serial":"None","chassisId":"1","annotations":{"managementAddress":"127.0.0.1","protocol":"OF_10","channelId":"127.0.0.1:33489"}},{ "id":"of:0000000000000002","type":"SWITCH","available":true,"role":"MASTER","mfr":"Nicira, Inc.,"hw":"Open vSwitch","sw":"2.0.2","serial":"None","chassisId":"2","annotations":{"managementAddress":"127.0.0.1","protocol":"OF_10","channelId":"127.0.0.1:33488"}}]}
```

Interrogación de dispositivos: Ejemplo ONOS (GUI)

The screenshot displays the ONOS (Open Network Operating System) GUI. At the top, the header includes the ONOS logo and the text "Open Network Operating System". On the right side of the header, there is a help icon and the text "onos".

The main area of the GUI shows a network topology with three blue square nodes connected in a V-shape. On the left side, there is a panel for the IP address "127.0.0.1", which includes a checkmark and the text "Devices: 3".

On the right side, there is a panel titled "ONOS Summary" with the following data:

ONOS Summary	
Version :	1.8.2
Devices :	3
Links :	4
Hosts :	0
Topology SCCs :	1
Intents :	0
Tunnels :	0
Flows :	15

At the bottom left, there is a toolbar with various icons for network management, including a monitor, a list, a gear, a network diagram, a link, a globe, a cloud, a refresh, a search, a zoom in, a zoom out, a reset, and a help icon.

Monitorización de eventos

- Un evento indica un problema, o incidencia anormal.
 - ▣ Nivel de tráfico por encima de un umbral, número excesivo de procesos, caída de un enlace...
- Iteración entre herramienta de monitorización de eventos y elementos gestionados.
 - ▣ Sondeo (polling). [SNMP](#)
 - ▣ Notificación asíncrona. [SNMP Trap](#)
- Cuando ocurre un evento importante la herramienta de monitorización notifica al gestor.



Monitorización de eventos: parámetros

- **Nivel de disparo** (trigger level) para notificar al gestor.
- **Nivel de gravedad:** colores asociados para visualización
 - ▣ Emergency (Red)
 - ▣ Problem (Yellow)
 - ▣ Warning (Orange)
 - ▣ Notification (Green)
- Soportado por las plataformas de gestión como **OPManager**.

Monitorización de eventos: visualización

- Visualiza estados discretos: link up/down
- Aplicable a gestión de fallos
- Se puede **limitar** la visualización a un determinado nivel de gravedad: sólo eventos de emergencias y problemas
- ¿La limitación tienen influencia en el trafico de gestión?
 - ▣ En notificaciones
 - ▣ En sondeo
- Baja **granularidad**: normalmente las limitaciones no se pueden definir a nivel de eventos en un elemento, son genéricas.

Monitorización de rendimiento

- Igual que monitorización de eventos: sondeo o notificación.
- Diferente visualización: evolución de valores con el tiempo.
 - ▣ Utilización de un enlace
 - ▣ Velocidad de transmisión o datos: pkts/seg o bps
 - ▣ Velocidad de conexiones: conexiones/seg
- Formatos de visualización:
 - ▣ **Progresión temporal**: evolución con el tiempo del rendimiento en un elemento
 - ▣ **Histograma**: comparativa de medidas de rendimiento en diferentes elementos en un instante de tiempo dado. Por ejemplo: comparativa de diferentes enlaces.

Análisis de flujo

- Analiza flujos de tráfico (paquetes correspondientes a una comunicación end-to-end).
- Dos fases:
 - ▣ Captura de paquetes.
 - ▣ Análisis de paquetes capturados.
- Beneficios:
 - ▣ Puede ayudar a conocer la naturaleza del tráfico analizado:
Por ejemplo predominan pocas conexiones largas o muchas conexiones cortas.
 - ▣ Puede ayudar a aislar la fuente de un problema
 - Por ejemplo determinar que un determinado flujo es responsable de la sobrecarga del enlace.
- Herramienta: **NetFlow, IPFIX**

Encaminamiento e ingeniería de tráfico

- Encaminamiento es muy automatizado, pero existen....
- **Herramientas de encaminamiento e ingeniería de tráfico**
 - ▣ Define la ruta que debe seguir determinados flujos
 - ▣ Control de los recursos dedicados a un flujo (QoS)
 - ▣ Definir ruta de backup por si falla la principal

Configuración

- Ver estado y modificar los parámetros de configuración del dispositivo.
- Gran variedad de herramientas: genéricas y propietarias.
- Pueden usar diferentes interfaces:
 - ▣ CLI, NETCONF
 - ▣ Interfaz programático (SNMP)
 - ▣ HTML (screen scraping). El gestor usa un web browser.

Ejemplo de configuración de un router con CLI

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# interface fastethernet 5/4
```

```
Router(config-if)# ip address 172.20.52.106 255.255.255.248
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)# end
```

```
Router#
```

Aplicación de seguridad

- Herramientas específicas de seguridad:
 - ▣ Firewall, IDS, VPN....
- En ocasiones las soluciones de seguridad van integradas en otras herramientas o en el elemento gestionado.
- Ejemplo: router con soporte de VPN (configurar túnel cifrado).

Planificación de red

- Herramientas que usan los administradores para planificar y configurar redes.
- Soportan planificación de futuras capacidades, arquitectura de seguridad o estrategia de recuperación ante fallos.
- Ejemplo: **GNS3**