

# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

Existen varias técnicas estructuradas de resolución de problemas, entre ellas:

- Descendente
- Ascendente
- Divide y vencerás



A continuación veremos en que consisten estos tres modelos para resolver problemas en una LAN, desde la perspectiva del modelo OSI.

# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

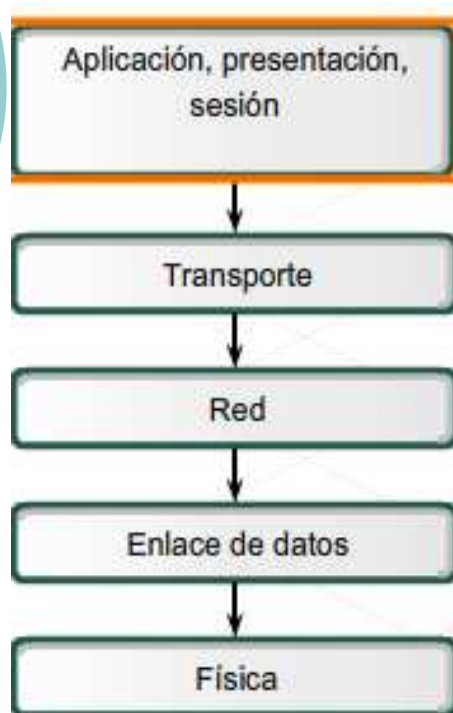
### Modelo descendente:

- Comienza con la capa de aplicación y sigue hacia abajo.
- Analiza el problema desde el punto de vista del usuario y de la aplicación.
- ¿Es sólo una aplicación la que no funciona, o son todas?. Por ejemplo: ¿el usuario puede acceder a diferentes páginas Web de Internet, pero no al correo electrónico?
- ¿Existen otras estaciones de trabajo con problemas similares?



# Resolución de incidencias en una LAN

## Enfoques en la resolución



| Enfoque de resolución de problemas | Cómo funciona   | Casos en los que es conveniente   | Ventajas/desventajas   |
|------------------------------------|---|---|--|
| Descendente                        | Siempre se comienza en la capa de aplicación y se sigue hacia abajo hasta descubrir la capa defectuosa. | Es conveniente para los problemas más simples o que puedan estar relacionados con la aplicación, el usuario o la capa superior. | Si finalmente el problema está relacionado con las capas inferiores, se gastará mucho tiempo y esfuerzo en las capas superiores o de aplicación. |

# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

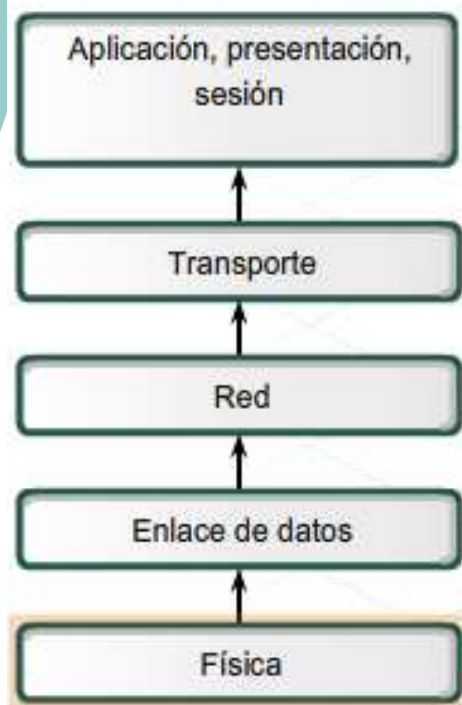
### Modelo ascendente:

- Comienza con la capa física y sigue hacia arriba.
- ¿Se extrajeron los cables de sus sockets?.
- Si el equipo tiene luces indicadoras, ¿están encendidas o apagadas?.



# Resolución de incidencias en una LAN

## Enfoques en la resolución



| Enfoque de resolución de problemas | Cómo funciona  | Casos en los que es conveniente   | Ventajas/desventajas  |
|------------------------------------|--|-----------------------------------|---|
| Ascendente                         | Siempre comienza en la capa física y va ascendiendo hasta que descubre la capa defectuosa. | Conveniente para casos complejos. | Es un enfoque lento pero sólido. Cuando el problema está relacionado con la aplicación (o la capa superior) este enfoque puede llevar mucho tiempo. |

# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

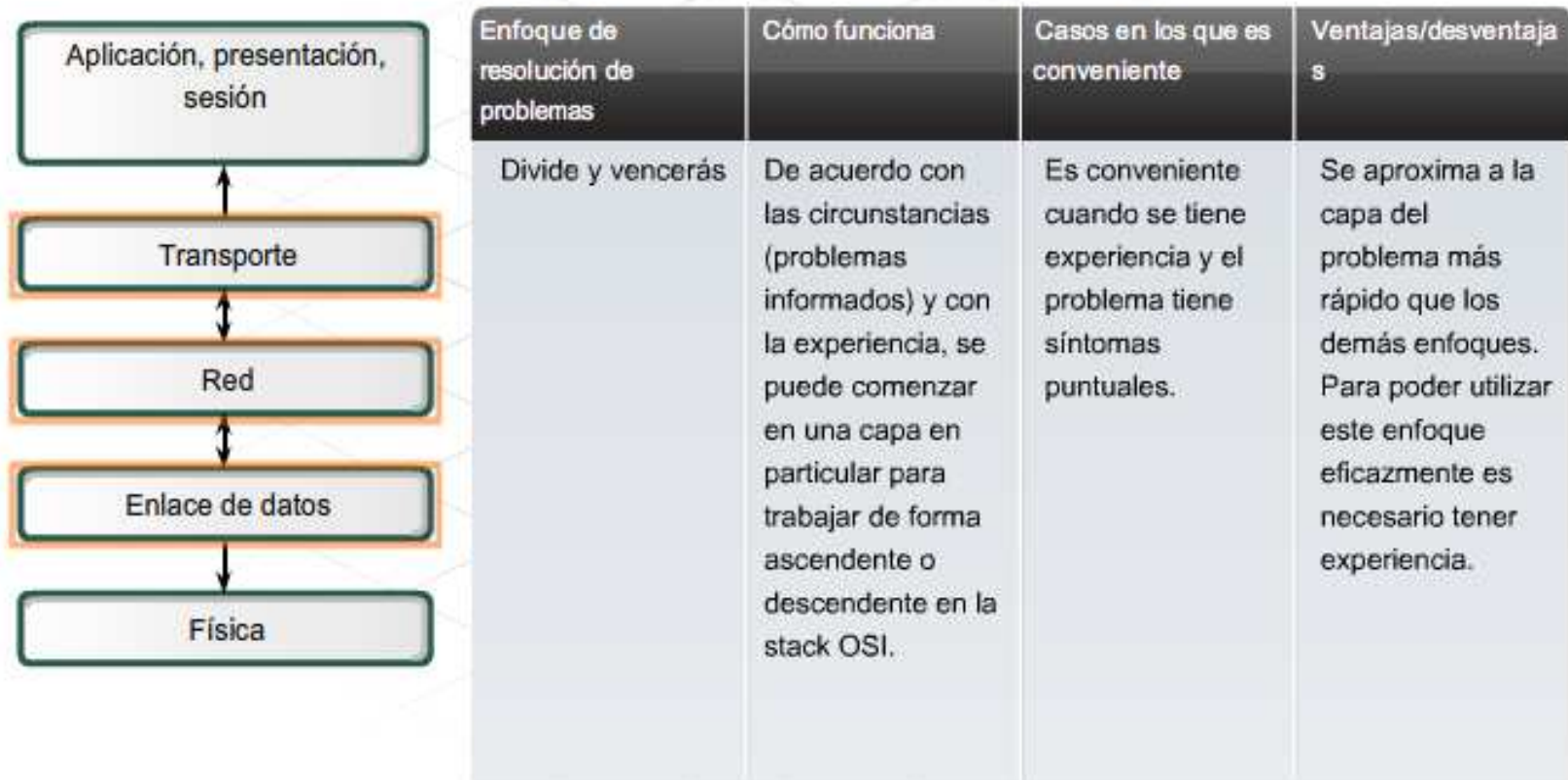
### Modelo divide y vencerás:

- Suele comenzar en una de las capas del medio para luego seguir hacia arriba o hacia abajo.
- Por ejemplo, el técnico en resolución de problemas puede comenzar en la capa de red verificando la información de configuración IP.



# Resolución de incidencias en una LAN

## Enfoques en la resolución





# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

La estructura de estos enfoques hace que sean ideales para aquellas personas que no tengan experiencia en resolver problemas.

Los individuos más experimentados suelen obviar los enfoques estructurados y seguir su instinto y su experiencia. Es posible que usen técnicas menos estructuradas, como:

- Ensayo y error
- Sustitución.





# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

### Modelo ensayo y error:

- Esta técnica se basa en el conocimiento individual para determinar la causa más probable del problema.
- El encargado de resolver problemas supone cuál puede ser la solución más probable.
- Tras implementar la solución, si no funciona, vuelve a intentarlo con otro supuesto.
- Este proceso se repite hasta aislar y solucionar el problema.



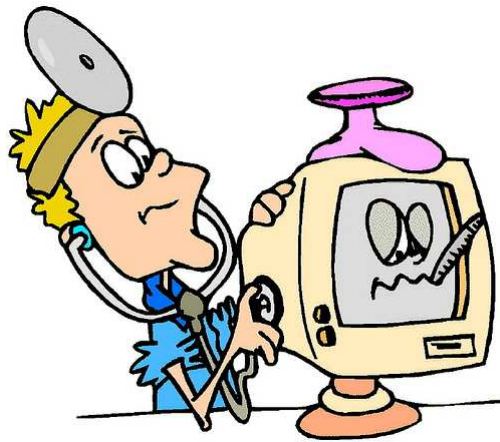
# Resolución de incidencias en una LAN

## Enfoques en la resolución

---

### Sustitución:

- Se supone que el problema es causado por un componente específico.
- La parte defectuosa se reemplaza por otra que se sabe que funciona.
- Es necesario disponer de repuestos para llevar a cabo esta técnica.





# Resolución de incidencias en una LAN

## Actividad

Identifique la técnica de resolución de problemas empleada.

|   | Divide y vencerás | Ascendente | Sustitución | Prueba y error |
|---|-------------------|------------|-------------|----------------|
| 1. Braseen está resolviendo un problema de conectividad de la red. Comienza su investigación en el medio físico verificando las conexiones de cables y lentamente va avanzando en su tarea a través del modelo de red por capas hasta llegar al software de aplicación que se ejecuta en los hosts.                                     |                   |            |             |                |
| 2. Medhat no logra conectarse a un sitio de Internet. Para comenzar a resolver el problema, primero prueba la conectividad de la red. Si falla, realizará su trabajo bajando por las capas hasta llegar al medio físico. De lo contrario, realizará su trabajo ascendiendo hacia la resolución de problemas del software de aplicación. |                   |            |             |                |
| 3. Patti está resolviendo un problema en la red. Sobre la base de su experiencia en casos similares, supone que el problema reside en una configuración errónea de IP y comienza el proceso de resolución de problemas a partir de allí.  |                   |            |             |                |

# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

---

Herramientas sw de consola:

- ipconfig: muestra información de la configuración IP.
- ping: prueba las conexiones con otros hosts IP.
- tracert: muestra la ruta exacta recorrida hacia el destino
- netstat: muestra las conexiones de red.
- nslookup: directamente solicita al servidor de nombre información sobre un dominio de destino.





# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

---

### Ipconfig (ifconfig en linux).

- Se utiliza para ver información sobre la configuración IP. dirección IP, máscara de subred y puerta de enlace.
- ipconfig /all muestra información adicional, que incluye la dirección MAC y los servidores DNS entre otras.
- ipconfig /release. Libera el interfaz de red de la dirección IP obtenida por un servidor DHCP.
- ipconfig /renew. Vuelve a solicitar la dirección IP a los servidores DHCP.



# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

Ping. Se utiliza para probar si se puede acceder a un host de destino. Utiliza el protocolo ICMP. Algunos ejemplos son:

- ping 192.168.7.5
- ping [www.cisco.com](http://www.cisco.com) . En este caso habrá de resolver el nombre a la IP utilizando los servidores DNS.
- Utiliza el protocolo ICMP.

```
C:\Users\Profesor>ping

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
        [-r cuenta] [-s cuenta] [[-j lista-host] ! [-k lista-host]]
        [-w tiempo_espera] [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
-t          Hacer ping al host especificado hasta que se detenga.
            Para ver estadísticas y continuar, presione Ctrl+Inter;
            para detener, presione Ctrl+C.
-a          Resolver direcciones en nombres de host.
-n cuenta  Número de solicitudes de eco para enviar.
-l tamaño  Enviar tamaño del búfer.
-f          Establecer marca No fragmentar en paquetes (sólo IPv4).
-i TTL     Tiempo de vida.
-v TOS     Tipo de servicio (sólo IPv4. Esta opción quedó obsoleta y
            no tiene ningún efecto sobre el campo de tipo de servicio
            del encabezado IP).
-r cuenta  Registrar la ruta de saltos de cuenta (sólo IPv4).
-s cuenta  Marca de tiempo de saltos de cuenta (sólo IPv4).
-j lista-host Ruta de origen no estricta para lista-host (sólo IPv4).
-k lista-host Ruta de origen estricta para lista-host (sólo IPv4).
-w tiempo_espera Tiempo de espera en milisegundos para cada respuesta.
-R          Usar encabezado de enrutamiento para probar también
            la ruta inversa (sólo IPv6).
-S srcaddr  Dirección de origen que se desea usar.
-4          Forzar el uso de IPv4.
-6          Forzar el uso de IPv6.
```



# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

---

### Tracert

- Proporciona información de conectividad de la ruta que un paquete recorre a fin de llegar a destino e información de conectividad de cada router (salto) que haya en el camino.
- Tracert puede ayudar a identificar dónde se perdió o se demoró un paquete debido a cuellos de botella o zonas más lentas de la red.
- La utilidad tracert básica sólo permite hasta 30 saltos entre un dispositivo de origen y uno de destino, antes de suponer que no se puede llegar al destino.
- El número de saltos se puede ajustar con el parámetro -h.



# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

---

### Tracert.

A continuación se muestra un ejemplo del comando Tracert. La opción -d indica que no se muestren los nombres de los dispositivos intermedios, sólo su dirección IP.

```
Traza a la dirección www.telefonica.net [213.4.130.95]  
sobre un máximo de 30 saltos:
```

```
  1      1 ms      <1 ms      <1 ms  192.168.1.1  
  2     63 ms     61 ms     63 ms  192.168.153.1  
  3     62 ms     62 ms     62 ms  80.58.120.177  
  4     63 ms     64 ms     63 ms  80.58.75.153  
  5      *        *        *      Tiempo de espera agotado para esta  
solicitud.  
  6      *        *        *      Tiempo de espera agotado para esta  
solicitud.  
  7      *        *
```

# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

### Netstat.

- Permite conocer los procesos activos en el PC. Indica el protocolo que se está usando, la dirección IP y el número de puerto local, la dirección IP y el número de puerto ajenos y el estado de la conexión.

```
C:\Users\Profesor>netstat -a -p TCP -n
```

Conexiones activas

| Proto | Dirección local    | Dirección remota   | Estado      |
|-------|--------------------|--------------------|-------------|
| TCP   | 0.0.0.0:135        | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:445        | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:912        | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:5357       | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49152      | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49153      | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49154      | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49155      | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49157      | 0.0.0.0:0          | LISTENING   |
| TCP   | 0.0.0.0:49165      | 0.0.0.0:0          | LISTENING   |
| TCP   | 127.0.0.1:49156    | 0.0.0.0:0          | LISTENING   |
| TCP   | 127.0.0.1:52156    | 127.0.0.1:52157    | ESTABLISHED |
| TCP   | 127.0.0.1:52157    | 127.0.0.1:52156    | ESTABLISHED |
| TCP   | 192.168.0.98:139   | 0.0.0.0:0          | LISTENING   |
| TCP   | 192.168.0.98:49165 | 192.168.0.84:49319 | ESTABLISHED |
| TCP   | 192.168.12.1:139   | 0.0.0.0:0          | LISTENING   |
| TCP   | 192.168.56.1:139   | 0.0.0.0:0          | LISTENING   |
| TCP   | 192.168.142.1:139  | 0.0.0.0:0          | LISTENING   |

# Resolución de incidencias en una LAN

## Herramientas sw para detectar problemas

### Nslookup.

- Permite que el usuario final busque información sobre un nombre DNS en particular en el servidor DNS.
- En el comando nslookup, la información recibida incluye la dirección IP del servidor DNS que se está utilizando y la dirección IP asociada al nombre DNS especificado.

```
C:\>nslookup cisco.netcad.net
Servidor: DNSTEST.svr.example.com
Dirección: 192.168.254.32

Respuesta no autoritativa:
Nombre: cisco.netcad.net
Dirección: 209.165.200.224
```

