Comandos básicos de troubleshooting

Visualización de la configuración

Para visualizar la "running configuration", simplemente teclear:

```
show
```

Nota: este comando solo muestra la configuración que NO esta por defecto. Para ver toda la configuración (incluida la de por defecto), teclear:

```
show  full-configuration
```

Para encontrar un comando CLI dentro de la configuración, se puede utilizar el signo pipe "|" con "grep", por ejemplo:

```
show | grep -f ipv6
show full-configuration | grep -f ipv6
```

Información general

```
get system interface physical          #Verificar estado de las interfaces hardware
get hardware nic <nic-name>            #detalle de una interface en concreto
fnsysctl ifconfig <nic-name>           #Comando oculto para ver todos los detalles de una interface
get system status                      #Ver estado general
get system performance status          #Uso de CPU y red
diagnose sys top                       #Verficar los top services del sistema
diagnose sys top-summary               #Más sencilla que el anterior de forma agrupada
diagnose ip arp list                   #Conocer la tabla arp del equipo
diagnose autoupdate versions           #Conocer las actualizaciones instaladas
diagnose log test                      #Generar todas las entradas de log posibles
diagnose test application dnsproxy 6   #Ver todos los objetos FQDN del sistema
diagnose debug crashlog read           #Ver el crashlog
```

Troubleshooting general de red

```
execute ping-options ?
execute ping-options source <ip-address-de-la-interface>
execute ping <hostname|ip>
execute ping6-options ?
execute ping6 <hostname|ip>
execute traceroute <hostname|ip>
execute tracert6 <hostname|ip>
```

Routing

```
get router info routing-table all       #Tabla de rutas
diagnose ip route list                  # información detallada de la tabla de rutas
get router info routing-table details x.x.x.x # Detalle para la IP x.x.x.
get router info kernel                  #Tabla de rutas/forwarding completa
get router <routing-protocol>           #Información por protocolo de routing
diagnose firewall proute list           #Información del PBR
diagnose ip rtcache list                #Información route cache = sesiones activas con la información de routing
diagnose ip rtcache clear       # limpiar la cache de rutas
```

High Availability

```
diagnose sys ha status                  #Conocer el estado del cluster
execute ha manage  ?                    #Conocer el id de los nodos del cluster
execute ha manage <device-index>        #Cambiar al CLI de otro nodo desde el master
diagnose sys ha showcsum                #Verificar si el checksum coincide para saber si estan sincronizados
```

Tabla de Sesiones

```
get system session list                 #Verificar las sesiones activas
diagnose sys session filter clear       #Borrar cualquier filtro de visualización
diagnose sys session filter ?           #Posibles filtros
diagnose sys session filter dst   8.8.8.8
diagnose sys session filter dport   53
```

Sniffer

El sistema permite hacer sniffer del trafico como si fuera un tcpdump. La sintaxis es esta:

```
diagnose sniffer packet <interface|any>  '<tcpdump-filter>' <verbose>
<count> <time-format>
```

En detalle:

```
verbose :
1: print header of packets
2: print header and data from ip of packets
3: print header and data from ethernet of packets (if available)
4: print header of packets with interface name
5: print header and data from ip of packets with interface name
6: print header and data from ethernet of packets (if available)
with intf name
count : number of packets
time-format : a: UTC time; l: local time
```

Ejemplos:

```
diagnose sniffer packet any 'host 8.8.8.8' 4 4 l
diagnose sniffer packet any 'host 8.8.8.8 and dst port 53' 4 10 a
diagnose sniffer packet wan1 'dst port (80 or 443)' 2 50 l
```

Flujos de tráfico

Para conocer en detalle la información de una conexión.

```
diagnose debug reset
diagnose debug flow filter ?
diagnose debug flow filter saddr 192.168.1.1
diagnose debug flow filter daddr 8.8.8.8
diagnose debug flow show console enable
diagnose debug enable
diagnose debug flow trace start 10
diagnose debug disable
```

VPN

Para hacer debug de las conexiones IKE/IPSEC:

```
get vpn ike gateway <nombre>
get vpn ipsec tunnel name <nombre>
get vpn ipsec tunnel details
diagnose vpn tunnel list
diagnose vpn ipsec status
get router info routing-table all
```

Para hacer debug de las sesiones IKE/IPSEC:

```
diagnose debug reset
diagnose vpn ike log-filter clear
diagnose vpn ike log-filter ?
diagnose vpn ike log-filter dst-addr4 8.8.8.8
diagnose debug app ike 255
diagnose debug enable
diagnose debug disable
```

Logs

Para visualizar los log's de forma similar al GUI pero haciendo desde el CLI:

```
execute log filter reset
execute log filter category event
execute log filter field (enter)
execute log filter field dstport 8001
execute log filter view-lines 1000
execute log filter start-line 1
execute log display
```

Comando "total"

Un comando no siempre conocido pero muy útil porque saca toda la información del sistema en un solo comando:

```
execute tac report
```