Plantillas de Configuración Básica de Gestión para Equipamiento Cisco

# 1. INTRODUCCION

## 1.1. Objetivo

Este documento presenta las plantillas de configuración básica de gestión comunes a todos los routers y switches de Cisco Networks homologados para su utilización como EDCs en los servicios de GGEE, en sus diferentes modalidades.

En este documento se han incluido plantillas de configuración para los equipos que se indican a continuación:

Cisco 892FSP, versión 15.4(3)M3

Familia ISR1100, versión 16.9.4

Familia ISR4000, versión 16.9.4

Cisco ASR1001-X, versión 16.9.4

Cisco ASR1009-X, versión 16.9.6

Cisco ASR920. Versión 16.9.4

Cisco ASR903, versión 16.12.3

Cisco C9200L, versión 16.12.4

Cisco C9300L, versión 16.12.4

Cisco C1000, versión 15.2(7)E3k

Aquellas configuraciones de gestión que no sean genéricas se podrán consultar en las plantillas del servicio correspondiente.

Toda la parte de QoS referente a la clase de Gestión se mantiene en las plantillas estándar para conservar la homogeneidad y el orden en la configuración de las clases. Lo mismo ocurre con la configuración de routing.

## 1.2. Documentación de referencia

Como documentación de referencia se ofrecen los siguientes manuales de plantillas:

• DTSRPV-2003 MacroLAN\_plantillas\_Cisco\_Switch\_vX.X

• DTSRPV-2005 MacroLAN\_Plantillas\_Cisco\_Router\_vX.X

• Plantillas de Configuracion del Servicio VPN IP para Equipos de Cliente Cisco (vX.XX.XX)

• Plantillas Ibercom IP Puntos Centrales Generico Switches Cisco vX.XX.XX

• Plantillas\_Datainternet\_BA\_vX.X

• Plantillas\_SILAN\_ConWiFi\_Switches\_Cisco\_vX.XX

## 1.3. Unidad responsable

D. Desarrollo de Servicios y Sistemas

D. Desarrollo de Servicios Empresas

• G. Certificación Equipamiento de Cliente

o J. Equipamiento de Soluciones de Datos

# 2. PLANTILLAS DE CONFIGURACION

## 2.1. Configuración común a todos los servicios

### 2.1.1. Definición del banner

Desde el modo de configuración del equipo, se especifica el banner que se mostrará antes de que el usuario introduzca sus credenciales de acceso:

banner login @ {{Texto\_Banner\_Pre\_Autenticacion}} @

{{Texto\_Banner\_Pre\_Autenticacion}} Texto que sale antes de autenticarse

A continuación, se introduce el banner que se mostrará una vez que el usuario haya sido autenticado correctamente:

banner exec @ {{Texto\_Banner\_Post\_Autenticacion}} @

{{Texto\_Banner\_Post\_Autenticacion}} Texto que sale despues de autenticarse

NOTA: La escritura de los <Texto\_Banner> debe comenzar y terminar con un <Caracter\_Delimitador> (%, &, $, @, …) para funcionar correctamente. Además, este carácter no se puede utilizar dentro de <Texto\_Banner>. Durante la introducción del texto es posible utilizar la tecla Enter para producir saltos de línea. Cada línea admite un máximo de 255 caracteres.

### 2.1.2. Configuración de fecha y zona horaria

Desde el modo enable, se ajusta la fecha y hora locales del equipo.

clock set {{hora\_minuto\_segundo}} {{dia}} {{mes}} {{ano}}

{{hora\_minuto\_segundo}} formato <hh(0-23):mm(0-59):ss(0-59)>

{{dia}} formato <día(1-31)>

{{mes}} formato <mes(January..December)>

{{ano}} formato numero

Desde el modo de configuración, se configura la zona horaria y los parámetros del cambio de horario de verano.

{% if localizacion\_canarias == false %}

clock timezone MET 1

{% endif %}

clock summer-time METDST recurring last Sun Mar 2:00 last Sun oct 3:00

### 2.1.3. Nombre del equipo

Asignación del mnemónico del EDC. Desde el modo de configuración:

hostname {{Mnemonico\_EDC}}

{{Mnemonico\_EDC}}

### 2.1.4. Desactivacion de servicios no necesarios

Por motivos de seguridad, se desactivarán una serie de protocolos y servicios que no van a ser utilizados en el EDC. Desde el modo de configuración:

no cdp run

no service tcp-small-servers

no service udp-small-servers

no service finger

no service dhcp

{% if modelo\_equipo != "Cisco C1000" %}

no ip source-route

{% endif %}

no ip domain-lookup

no service config

no ip bootp server !!! \*

no ip name-server

\* Determinados modelos no admiten este comando al no disponer de la funcionalidad, por lo que no es problemático si al introducirlo da error.

Configuración de otros parámetros generales. Desde el modo de configuración:

service nagle

service tcp-keepalives-in

ip subnet-zero

service timestamps debug datetime localtime msec show-timezone

service timestamps log datetime localtime msec show-timezone

### 2.1.5. Gestión por loopback

Se crea la interfaz loopback de gestión.

interface loopback 600

description Direccion IP de gestion EDC

ip address {{IPGestion}} 255.255.255.255

no ip directed-broadcast

no ip proxy-arp

no shutdown

exit

ip tftp source-interface Loopback 600

ip ftp source-interface Loopback 600

ip tacacs source-interface Loopback 600

logging source-interface Loopback 600

snmp-server trap-source Loopback 600

ntp source Loopback 600

{{IPGestion}}: Es la dirección IP utilizada para la gestión del EDC. Por tanto, debe ser única en todo el ámbito del servicio.

### 2.1.6. Control de acceso al EDC

#### 2.1.6.1. Escenarios con EDC Simple

Activacion del servicio de encriptado de passwords

service password-encryption

Configuración de la contraseña de acceso al modo enable (también se usará para autenticar los accesos a este modo cuando el servidor TACACS+ esté inaccesible):

enable secret {{Password\_Enable}}

{{Password\_Enable}}

Se crea un usuario local que permitirá el acceso al equipo vía consola y remoto mientras no se configuren las funcionalidades de AAA o cuando el servidor TACACS+ esté innacesible.

username {{Usuario}} secret {{Password\_Usuario}}

{{Usuario}}

{{Password\_Usuario}}

Habilita el acceso SSH al equipo

{% if modelo\_equipo =="Cisco ASR903" or modelo\_equipo =="Cisco ASR920" or modelo\_equipo =="Cisco ASR1000" or modelo\_equipo =="Familia ISR4000" or modelo\_equipo =="Familia ISR1100" or modelo\_equipo =="Cisco ASR1009-X" %}

ip domain name {{Mnemonico\_EDC}}

{% else %}

ip domain-name {{Mnemonico\_EDC}}

{% endif %}

crypto key generate rsa

1024

ip ssh version 2

{{Mnemonico\_EDC}}

Se crea un filtro para controlar los accesos remotos al equipo, que sufrirá algunas modificaciones en función del servicio que se esté configurando.

Servicios MacroLAN, VPNIP y DataInternet

{% if servicio == "MacroLAN" or servicio == "VPNIP" or servicio == "DataInternet" %}

access-list 52 remark Accesos Remotos

{% for CentroGestion in CentrosGestion\_MACROLAN\_VPNIP\_DATAINTERNET %}

access-list 52 permit {{CentroGestion.IP\_CentroGestion}} {{CentroGestion.MascaraInversa}}

{% endfor %}

access-list 52 permit host {{IP\_PE\_1}}

access-list 52 permit host {{IP\_PE\_2}}

{% if VLAN\_Servicio\_respaldo %}

access-list 52 permit host {{IP\_PE\_3}}

access-list 52 permit host {{IP\_PE\_4}}

{% endif %}

access-list 52 deny any

{% endif %}

{{CentroGestion.IP\_CentroGestion}} Es una red IP del Centro de Gestión desde la que se quiere acceder vía remota al equipo.

{{CentroGestion.MascaraInversa}}

{{IP\_PE\_1}} Son cada una de las direcciones IP de los PEs sobre la VLAN de Servicio.

{{IP\_PE\_2}} Son cada una de las direcciones IP de los PEs sobre la VLAN de Servicio.-#}

{{IP\_PE\_3}} En el servicio MacroLAN, son las direcciones IP de los PEs sobre la VLAN de Servicio de respaldo en escenarios de EDC único con redundancia de acceso y Caudales Exclusivos.-#}

{{IP\_PE\_4}} En el servicio MacroLAN, son las direcciones IP de los PEs sobre la VLAN de Servicio de respaldo en escenarios de EDC único con redundancia de acceso y Caudales Exclusivos.-#}

Servicios SiLAN e Ibercom Punto Central

{% if servicio == "SILAN" or servicio == "Ibercom Punto Central" or servicio == "DataInternet" %}

access-list 52 remark Accesos Remotos

{% for CentroGestion in CentrosGestion\_SILAN\_IBERCOM %}

access-list 52 permit {{CentroGestion.IP\_CentroGestion}} {{CentroGestion.MascaraInversa}}

{% endfor %}

access-list 52 permit {{Red\_VLAN\_Gestion}} {{MascaraInversa\_VLAN\_Gestion}}

access-list 52 deny any

{% endif %}

{{CentroGestion.IP\_CentroGestion}}

{{CentroGestion.MascaraInversa}}

{{Red\_VLAN\_Gestion}} Se incluye la red configurada en la VLAN 30 que permitirá el acceso remoto desde los EDCs Principal y Backup y el salto entre switches.-#}

{{MascaraInversa\_VLAN\_Gestion}}-#}

Se limita el número máximo de sesiones simultáneas a 5. También se configuran los tiempos de desconexión por inactividad. La línea "login local" hay que configurarla antes de introducir el comando "aaa new-model" del apartado 2.1.7, ya que en caso contrario el equipo no lo aceptará.

Se aplica la lista de acceso a los interfaces VTY y al puerto auxiliar (en caso de que exista):

line con 0

login local

exec-timeout {{Timeout}}

exit

{% if tiene\_puerto\_auxiliar %}

{% if modelo\_equipo != "Cisco ASR920" and modelo\_equipo != "Cisco ASR903" and modelo\_equipo != "Familia ISR4000" and modelo\_equipo != "Familia ISR1100" %}

line aux 0

login local

exec-timeout {{Timeout}}

transport input telnet ssh

transport output telnet ssh

access-class 52 in

exit

{% endif %}

{% endif %}

line vty 0 4

login local

exec-timeout {{Timeout}}

transport input telnet ssh

transport output telnet ssh

access-class 52 in

exit

line vty 5 15

transport input none

transport output none

exit

{% if modelo\_equipo == "Familia ISR1100" or modelo\_equipo == "Familia ISR4000" %}

line 2

transport input none

exit

{% endif %}

{{Timeout}} Es el tiempo de inactividad en minutos que provocará la desconexión de la sesión.-#}

Desactivacion de los servidores HTTP/HTTPS

no ip http server

no ip http secure-server

#### 2.1.6.2. Escenarios con dos o más EDCs

Además de configurar todo lo indicado en el apartado 2.1.6.1, se incluyen los siguientes comandos.

Se permitirá en todos los EDCs el acceso remoto desde el resto de EDCs de la sede. Es imprescindible que dentro de la ACL 52 la nueva regla se situe por encima del "deny any", que siempre debe ser la última expresión de la lista.

{% if servicio == "VARIOS EDC" %}

no access-list 52

access-list 52 remark Accesos Remotos

{% for CentroGestion in CentrosGestion\_MACROLAN\_VPNIP\_DATAINTERNET %}

access-list 52 permit {{CentroGestion.IP\_CentroGestion}} {{CentroGestion.MascaraInversa}}

{% endfor %}

access-list 52 permit host {{IP\_PE\_1}}

access-list 52 permit host {{IP\_PE\_2}}

{% if VLAN\_Servicio\_respaldo %}

access-list 52 permit host {{IP\_PE\_3}}

access-list 52 permit host {{IP\_PE\_4}}

{% endif %}

{% for IP\_LAN\_EDC in IPs\_LAN\_EDC %}

access-list 52 permit host {{IP\_LAN\_EDC.IP}}

{% endfor %}

access-list 52 deny any

{% endif %}

{{CentroGestion.IP\_CentroGestion}}

{{CentroGestion.MascaraInversa}}

{{IP\_PE\_1}}

{{IP\_PE\_2}}

{{IP\_PE\_3}}

{{IP\_PE\_4}}

{{IP\_LAN\_EDC.IP}} Es la IP dentro de la LAN, puede cambiar en función de los servicios contratados por el cliente:

• Si existe el servicio SiLAN, será la IP asignada al resto de EDCs en la VLAN de Gestión.

• En cualquier otro caso, será la IP asignada al resto de EDCs en la LAN de cliente.-#}

Para ello, se debe eliminar la ACL de manera completa.

no access-list 52

Y a continuación volver a crearla con todos los términos, tal y como se indica arriba.

Una vez realizadas las modificaciones, es recomendable comprobar que sobre las lines vty 0 4 sigue aplicado el comando "access-class 52 in".

### 2.1.7. Configuración TACACS+

Antes de continuar, es necesario haber creado el usuario local y seguido todos los pasos indicados en el apartado 2.1.6 para evitar posibles pérdidas de conectividad con el EDC.

Creación de un nuevo modelo de AAA.

aaa new-model

no tacacs-server directed-request

Configuracion de los servidores TACACS+

{% for servidor\_TACACS in servidores\_TACACS %}

tacacs server TACACS+\_{{loop.index}}

address ipv4 {{servidor\_TACACS.IP\_Servidor}}

key {{servidor\_TACACS.CLAVE\_Servidor}}

exit

{% endfor %}

aaa group server tacacs+ TACACS+CG

{% for servidor\_TACACS in servidores\_TACACS %}

server name TACACS+\_{{loop.index}}

{% endfor %}

exit

{{loop.index}}

{{servidor\_TACACS.IP\_Servidor}}

{{servidor\_TACACS.CLAVE\_Servidor}}

Para equipos con versiones anteriores a las indicadas, que no admitan los nuevos comandos, se utilizará el antiguo modelo de configuración.

{% for servidor\_TACACS in servidores\_TACACS %}

tacacs-server host {{servidor\_TACACS.IP\_Servidor}} key {{servidor\_TACACS.CLAVE\_Servidor}}

{% endfor %}

aaa group server tacacs+ TACACS+CG

{% for servidor\_TACACS in servidores\_TACACS %}

server {{servidor\_TACACS.IP\_Servidor}}

{% endfor %}

exit

{{servidor\_TACACS.IP\_Servidor}} Es la dirección IP de cada uno de los servidores TACACS+.

{{servidor\_TACACS.CLAVE\_Servidor}} Es la clave de autenticación entre el EDC y el TACACS+.

En futuras versiones de IOS este último modelo será eliminado, por lo que es conveniente que se comience a utilizar el nuevo en el mayor número de plataformas posibles.

Configuración de los parámetros de autenticación por TACACS+.

aaa authentication login default group TACACS+CG local

aaa authentication enable default group TACACS+CG enable

Configuración del accounting de comandos por TACACS+.

aaa accounting exec default start-stop group TACACS+CG

aaa accounting commands 0 default start-stop group TACACS+CG

aaa accounting commands 1 default start-stop group TACACS+CG

aaa accounting commands 15 default start-stop group TACACS+CG

¡¡¡ En este momento es necesario finalizar la sesión y entrar de nuevo en el equipo con los nuevos credenciales para continuar con la configuración, de otra forma se perderá la conectividad !!!

Configuración de la autorización de comandos por TACACS+.

aaa authorization exec default group TACACS+CG if-authenticated

aaa authorization commands 0 default group TACACS+CG local

aaa authorization commands 1 default group TACACS+CG local

aaa authorization commands 15 default group TACACS+CG local

### 2.1.8. Configuración de NTP

Se configuran los servidores NTP que el EDC utilizará para sincronizar temporalmente. También se define una ACL para limitar las IPs desde las que se admiten paquetes NTP.

{% for servidor\_NTP in servidores\_NTP %}

{% if loop.first %}

ntp server {{servidor\_NTP.IPServidor}} prefer

{% else %}

ntp server {{servidor\_NTP.IPServidor}}

{% endif %}

{% endfor %}

access-list 53 remark Gestion NTP

{% for servidor\_NTP in servidores\_NTP %}

access-list 53 permit host {{servidor\_NTP.IPServidor}}

{% endfor %}

access-list 53 deny any

ntp access-group peer 53

{{servidor\_NTP.IPServidor}} Es la dirección IP de cada uno de los servidores NTP.-#}

### 2.1.9. Configuración SNMP

Se crea un filtro para controlar los accesos de lectura SNMP.

access-list 50 remark Gestion SNMP lectura

{% for servidor\_SNMP in servidores\_SNMP %}

access-list 50 permit host {{servidor\_SNMP.CentroGestion}} {{servidor\_SNMP.MascaraInversa}}

{% endfor %}

access-list 50 deny any

{{servidor\_SNMP.CentroGestion}} Es un rango de direcciones IP desde el que se permiten accesos de lectura SNMP.

{{servidor\_SNMP.MascaraInversa}}

Se crea otro filtro para controlar los accesos de lectura/escritura SNMP.

access-list 51 remark Gestion SNMP escritura

{% for servidor\_SNMP in servidores\_SNMP %}

access-list 51 permit {{servidor\_SNMP.CentroGestion}} {{servidor\_SNMP.MascaraInversa}}

{% endfor %}

access-list 51 deny any

{{servidor\_SNMP.CentroGestion}} Es un rango de direcciones IP desde el que se permiten accesos de lectura/escritura SNMP.

{{servidor\_SNMP.MascaraInversa}}

Datos administrativos:

snmp-server location {{Localizacion\_EDC}}

snmp-server chassis-id {{Mnemonico\_EDC}}

snmp-server contact {{Persona\_de\_Contacto}}

{{Localizacion\_EDC}}

{{Mnemonico\_EDC}}

{{Persona\_de\_Contacto}}

Comunidades de lectura y lectura/escritura.

snmp-server community {{Comunidad\_SNMP\_Lectura}} RO 50

snmp-server community {{Comunidad\_SNMP\_Escritura}} RW 51

{{Comunidad\_SNMP\_Lectura}}

{{Comunidad\_SNMP\_Escritura}}

Control de accesos TFTP.

{% if modelo\_equipo == "Cisco C9200L" or modelo\_equipo == "Cisco C9300L" %}

snmp-server file-transfer access-group 51 protocol tftp

{% endif %}

snmp-server tftp-server-list 51

Se añade persistencia a los índices de los interfaces del equipo.

snmp-server ifindex persist

### 2.1.10. Activación de traps SNMP

Cada servicio requerirá la activación de unas traps SNMP determinadas.

#### 2.1.10.1. MacroLAN

{% if servicio == "MacroLAN" %}

snmp-server enable traps

no snmp-server enable traps snmp authentication

no snmp-server enable traps syslog

{% if Ejecutar\_Comando %}

no snmp-server enable traps isdn

snmp-server enable traps isdn call-information

{% endif %}

{% endif %}

#### 2.1.10.2. VPNIP

{% if servicio == "VPNIP" %}

{% if modelo\_equipo != "Cisco C1000" and modelo\_equipo != "Cisco C9200L" and modelo\_equipo != "Cisco C9300L" %}

snmp-server enable traps isdn call-information

{% endif %}

snmp-server enable traps config

snmp-server enable traps entity

{% if modelo\_equipo != "Cisco ASR1001-X" and modelo\_equipo != "Cisco ASR1009-X" and modelo\_equipo != "Cisco ASR920" and modelo\_equipo != "Cisco ASR903" and modelo\_equipo != "Familia ISR4000" and modelo\_equipo != "Familia ISR1100" %}

snmp-server enable traps envmon

{% endif %}

{% if modelo\_equipo != "Cisco C1000" and modelo\_equipo != "Cisco C9200L" and modelo\_equipo != "Cisco C9300L" %}

snmp-server enable traps bgp

snmp-server enable traps frame-relay

snmp-server enable traps rtr

{% endif %}

{% if Ejecutar\_Comando %}

snmp-server enable traps isdn

{% endif %}

snmp-server enable traps snmp linkup linkdown coldstart warmstart

{% if modelo\_equipo != "Cisco C1000" and modelo\_equipo != "Cisco C9200L" and modelo\_equipo != "Cisco C9300L" %}

snmp-server enable traps atm pvc

{% endif %}

{% endif %}

#### 2.1.10.3. DataInternet

{% if servicio == "DataInternet" %}

snmp-server enable traps config

{% if modelo\_equipo != "Cisco ASR1001-X" and modelo\_equipo != "Cisco ASR1009-X" and modelo\_equipo != "Cisco ASR920" and modelo\_equipo != "Cisco ASR903" and modelo\_equipo != "Familia ISR4000" and modelo\_equipo != "Familia ISR1100" %}

snmp-server enable traps envmon

{% endif %}

{% if modelo\_equipo != "Cisco C1000" and modelo\_equipo != "Cisco C9200L" and modelo\_equipo != "Cisco C9300L" %}

snmp-server enable traps bgp

snmp-server enable traps rtr

{% endif %}

snmp-server enable traps snmp linkup linkdown coldstart warmstart

{% if modelo\_equipo != "Cisco C1000" and modelo\_equipo != "Cisco C9200L" and modelo\_equipo != "Cisco C9300L" %}

snmp-server enable traps atm pvc

{% endif %}

{% endif %}

#### 2.1.10.4. SiLAN e Ibercom IP Punto Central

{% if servicio == "SILAN" or servicio == "Ibercom Punto Central" %}

snmp-server enable traps

{% endif %}

#### 2.1.10.5. Destino de los traps

Atención: La IP de la colectora no debe configurarse de forma manual, los sistemas realizarán una configuración automática con la IP asignada. La configuración manual de esta IP puede provocar un mal funcionamiento de los sistemas colectores de alarmas, por lo que debe evitarse.

En caso de que sea necesaria la configuración manual por alguna necesidad que lo justifique se utilizará la configuración que se detalla a continuanción.

### 2.1.11. Configuración de RMON

#### 2.1.11.1. Servicios MacroLAN, VPNIP y DataInternet

{% if servicio == "MacroLAN" or servicio == "VPNIP" or servicio == "DataInternet" %}

Definición de EVENTOS y ALARMAS RMON para variables MIB de una única instancia

rmon event 100 log trap {{Comunidad\_Lectura\_1}} description NUM\_INTERFACES\_HA\_CAMBIADo owner config

rmon event 200 log trap {{Comunidad\_Lectura\_1}} description MEMoRIA\_LIBRE\_SUPERIoR\_A\_500K owner config

rmon event 201 log trap {{Comunidad\_Lectura\_1}} description MEMoRIA\_LIBRE\_INFERIoR\_A\_500K owner config

rmon event 300 log trap {{Comunidad\_Lectura\_1}} description SUPERADo\_UMBRAL\_DE\_USo\_DE\_CPU owner config

rmon event 301 log trap {{Comunidad\_Lectura\_1}} description USo\_DE\_CPU\_ACEPTABLE owner config

rmon alarm 100 interfaces.1.0 900 delta rising-threshold 1 100 falling-threshold -1 100 owner config

rmon alarm 200 lsystem.8.0 3600 absolute rising-threshold 500000 200 falling-threshold 500000 201 owner config

rmon alarm 300 lsystem.58.0 900 absolute rising-threshold 70 300 falling-threshold 55 301 owner config

{{Comunidad\_Lectura\_1}}

En esta plantilla se definen las siguientes ALARMAS y EVENTOS RMON:

• Alarma 100:

o Se encarga de la monitorización de la variable MIB ifNumber (.1.3.6.1.2.1.2.1.0) cuyo valor indica el número de interfaces de red presentes en el equipo, independientemente del estado en el que se encuentran.

o Esta variable MIB se monitoriza cada 900 segundos (15 minutos).

o Esta asociada a un único EVENTO > 100. De manera que se generará el Trap SNMP asociado a la superación de la alarma RMON 100 cada vez que el número de interfaces cambie al aumentar en 1 o al decrecer en 1.

• Alarma 200:

o Se encarga de la monitorización de la variable MIB freeMem (.1.3.6.1.4.1.9.2.1.8.0) cuyo valor indica la cantidad de memoria libre en bytes.

o Esta variable MIB se monitoriza cada 3600 segundos (1 hora)).

o Evento de SUBIDA = 200 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 200 cuando el valor de la variable MIB freeMem sea superior a 500000 bytes.

o Evento de BAJADA = 201 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 200 cuando el valor de la variable MIB freeMem sea inferior a 500000 bytes.

• Alarma 300:

o Se encarga de la monitorización de la variable MIB avgBusy5 (.1.3.6.1.4.1.9.2.1.58.0) cuyo valor indica el porcentaje de consumo de CPU en los últimos 5 minutos.

o Evento de SUBIDA = 300 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 300 cuando el valor de la variable MIB avgBusy5 sea superior al 70%.

o Evento de BAJADA = 301 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 300 cuando el valor de la variable MIB avgBusy5 sea inferior al 55%.

Definición de EVENTOS y ALARMAS RMON para variables MIB de varias instancias

rmon event 52 log trap {{Comunidad\_Lectura\_2}} description DESCARTES\_DE\_ENTRADA\_MAL owner config

rmon event 53 log trap {{Comunidad\_Lectura\_2}} description DESCARTES\_DE\_ENTRADA\_BIEN owner config

rmon event 54 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_DE\_ENTRADA\_MAL owner config

rmon event 55 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_DE\_ENTRADA\_BIEN owner config

rmon event 56 log trap {{Comunidad\_Lectura\_2}} description DESCARTES\_DE\_SALIDA\_MAL owner config

rmon event 57 log trap {{Comunidad\_Lectura\_2}} description DESCARTES\_DE\_SALIDA\_BIEN owner config

rmon event 58 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_DE\_SALIDA\_MAL owner config

rmon event 59 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_DE\_SALIDA\_BIEN owner config

rmon event 62 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_COLISIONES owner config

rmon event 63 log trap {{Comunidad\_Lectura\_2}} description ERRORES\_COLISIONES\_RECUPERADAS owner config

{% for alarma in monitorizacion\_variables\_MIB %}

rmon alarm {{alarma.codigo\_alarma}} {{alarma.OID}} {{alarma.instancia}} {{alarma.Y}} delta rising-threshold {{alarma.Z}} {{alarma.Evento\_SUBIDA}} falling-threshold {{alarma.Z1}} {{alarma.Evento\_BAJADA}} owner config

{% endfor %}

{% endif %}

{{Comunidad\_Lectura\_2}}

{{alarma.codigo\_alarma}}

{{alarma.OID}}

{{alarma.instancia}} valor númerico entero que define la instancia de la variable MIB asociada al interfaz que cuya variable MIB asociada deseamos monitorizar.

{{alarma.Y}} tiempo definido en segundos que indica el periodo de tiempo cada cuanto deseamos monitorizar el valor de la variable MIB definida en la alarma.

{{alarma.Z}} Valor del umbral de SUBIDA. Este valor deberá estar expresado en las mismas unidades que utilice la variable MIB que está siendo monitorizada.

{{alarma.Evento\_SUBIDA}}

{{alarma.Z1}} Valor del umbral de BAJADA. Este valor deberá estar expresado en las mismas unidades que utilice la variable MIB que está siendo monitorizada.

{{alarma.Evento\_BAJADA}}

Donde:

• Se configurará un CÓDIGO de Alarma distinto para cada instancia que deseemos monitorizar de una determinada Variable MIB.

• El código de la Alarma será un número de 5 dígitos, donde los dos primeros dígitos corresponden con el primer código de EVENTO PAR (Evento asociado a la superación del Umbral de Subida). Los tres últimos dígitos se numerará consecutivamente, uno para cada instancia, desde el valor "000" hasta el valor "999" (1000 posibles valores)

Por ejemplo: se podrán configurar 999 alarmas con los códigos 62000 hasta 62999 para poder monitorizar hasta 999 instancias de la variable MIB locIfInCollisions.

• <instancia> > valor númerico entero que define la instancia de la variable MIB asociada al interfaz que cuya variable MIB asociada deseamos monitorizar.

• <Y> > tiempo definido en segundos que indica el periodo de tiempo cada cuanto deseamos monitorizar el valor de la variable MIB definida en la alarma.

• <Z> > Valor del umbral de SUBIDA. Este valor deberá estar expresado en las mismas unidades que utilice la variable MIB que está siendo monitorizada.

• <Z1> > Valor del umbral de BAJADA. Este valor deberá estar expresado en las mismas unidades que utilice la variable MIB que está siendo monitorizada.

En esta plantilla se definen las siguientes ALARMAS y EVENTOS RMON:

• Alarma 52XXX:

o Se encarga de la monitorización de la variable MIB ifInDiscards (.1.3.6.1.2.1.2.2.1.13.<instancia>) cuyo valor indica el número de paquetes entrantes que han sido elegidos para ser descartados incluso aunque no se hayan detectado errores en ellos.

o Esta variable MIB se monitoriza cada <Y> segundos.

o Evento de SUBIDA = 52 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 52XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea superior a <Z>.

o Evento de BAJADA = 53 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 52XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea inferior a <Z1>.

• Alarma 54XXX:

o Se encarga de la monitorización de la variable MIB ifInErrors (.1.3.6.1.2.1.2.2.1.14.<instancia>) cuyo valor indica el número de paquetes entrantes que contenían errores de manera que no han podido ser entregados a protocolos de capas superiores para su procesado.

o Esta variable MIB se monitoriza cada <Y> segundos.

o Evento de SUBIDA = 54 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 54XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea superior a <Z>.

o Evento de BAJADA = 55 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 54XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea inferior a <Z1>.

• Alarma 56XXX:

o Se encarga de la monitorización de la variable MIB ifOutDiscards (.1.3.6.1.2.1.2.2.1.19.<instancia>) cuyo valor indica el número de paquetes salientes que han sido elegidos para ser descartados incluso aunque no se hayan detectado errores en ellos para evitar que sean trasmitidos.

o Esta variable MIB se monitoriza cada <Y> segundos.

o Evento de SUBIDA = 56 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 56XXX cuando el valor de la variable MIB ifOutDiscards.<instancia> sea superior a <Z>.

o Evento de BAJADA = 57 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 56XXX cuando el valor de la variable MIB ifOutDiscards.<instancia> sea inferior a <Z1>.

• Alarma 58XXX:

o Se encarga de la monitorización de la variable MIB ifOutErrors (.1.3.6.1.2.1.2.2.1.20.<instancia>) cuyo valor indica el número de paquetes salientes que contenían errores de manera que no han podido ser transmitidos.

o Esta variable MIB se monitoriza cada <Y> segundos.

o Evento de SUBIDA = 58 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 58XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea superior a <Z>.

o Evento de BAJADA = 59 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 58XXX cuando el valor de la variable MIB ifInDiscards.<instancia> sea inferior a <Z1>.

• Alarma 62XXX:

o Se encarga de la monitorización de la variable MIB locIfCollisions (.1.3.6.1.4.1.9.2.2.1.1.25.<instancia>) cuyo valor indica el número de colisiones en salida detectadas en el interfaz al que hace referencia la <instancia>.

o Esta variable MIB se monitoriza cada <Y> segundos.

o Evento de SUBIDA = 62 > Se generará un Trap SNMP de RMON por superación del Umbral de Subida asociado a la Alarma 62XXX cuando el valor de la variable MIB locIfCollisions.<instancia> sea superior a <Z>.

o Evento de BAJADA = 63 > Se generará un Trap SNMP de RMON por superación del Umbral de Bajada asociada a la Alarma 62XXX cuando el valor de la variable MIB locIfCollisions.<instancia> sea inferior a <Z1>.

#### 2.1.11.2. SILAN

{% if servicio == "SILAN" %}

rmon event 46 log trap {{Comunidad\_Lectura\_3}} description ERRORES\_CoLISIoNES owner config

rmon event 47 log trap {{Comunidad\_Lectura\_3}} description ERRORES\_CoLISIoNES\_RECUPERADAS owner config

rmon event 100 log trap {{Comunidad\_Lectura\_3}} description NUM\_INTERFACES\_HA\_CAMBIADO owner config

rmon event 200 log trap {{Comunidad\_Lectura\_3}} description MEMORIA\_LIBRE\_SUPERIOR\_A\_500K owner config

rmon event 201 log trap {{Comunidad\_Lectura\_3}} description MEMORIA\_LIBRE\_INFERIOR\_A\_500K owner config

rmon event 300 log trap {{Comunidad\_Lectura\_3}} description SUPERADO\_UMBRAL\_DE\_USO\_DE\_CPU owner config

rmon event 301 log trap {{Comunidad\_Lectura\_3}} description USO\_DE\_CPU\_ACEPTABLE owner config

rmon alarm 100 ifNumber.0 900 delta rising-threshold 1 100 falling-threshold -1 100 owner config

rmon alarm 200 lsystem.8.0 3600 absolute rising-threshold 500000 200 falling-threshold 500000 201 owner config

rmon alarm 300 lsystem.58.0 900 absolute rising-threshold 70 300 falling-threshold 55 301 owner config

rmon alarm 46001 lifEntry.25.10001 900 delta rising-threshold 100 46 falling-threshold 100 47 owner config

{% endif %}

{{Comunidad\_Lectura\_3}}

#### 2.1.11.3. Ibercom Punto Central

{% if servicio == "Ibercom Punto Central" %}

rmon event 46 log trap {{Comunidad\_Lectura\_4}} description ERRORES\_COLISIoNES owner config

rmon event 47 log trap {{Comunidad\_Lectura\_4}} description ERRORES\_COLISIoNES\_RECUPERADAS owner config

rmon event 100 log trap {{Comunidad\_Lectura\_4}} description NUM\_INTERFACES\_HA\_CAMBIADO owner config

rmon event 200 log trap {{Comunidad\_Lectura\_4}} description MEMORIA\_LIBRE\_SUPERIOR\_A\_500K owner config

rmon event 201 log trap {{Comunidad\_Lectura\_4}} description MEMORIA\_LIBRE\_INFERIOR\_A\_500K owner config

rmon event 300 log trap {{Comunidad\_Lectura\_4}} description SUPERADO\_UMBRAL\_DE\_USO\_DE\_CPU owner config

rmon event 301 log trap {{Comunidad\_Lectura\_4}} description USO\_DE\_CPU\_ACEPTABLE owner config

rmon alarm 100 interfaces.1.0 900 delta rising-threshold 1 100 falling-threshold -1 100 owner config

rmon alarm 200 lsystem.8.0 3600 absolute rising-threshold 500000 200 falling-threshold 500000 201 owner config

rmon alarm 300 lsystem.58.0 900 absolute rising-threshold 70 300 falling-threshold 55 301 owner config

rmon alarm 46001 1.3.6.1.4.1.9.2.2.1.1.25. {{X}} 900 delta rising-threshold 100 46 falling-threshold 100 47 owner config

{% endif %}

{{Comunidad\_Lectura\_4}}

{{X}} Corresponde a la instancia SNMP del interfaz LAN cuyas colisiones deseamos monitorizar.

NOTA: Para este servicio sólo tiene sentido en la interfaz LAN de cliente. El valor de <X>, del tipo de alarma 46001, dependerá de cada equipo, ya que hace referencia al número que le asigna el router al arrancar, por lo que es obligación del centro que quiera implementar esta parte del RMON buscar cuál es el que hace referencia a la interfaz que queremos chequear. Para saber cuál es, se puede realizar la siguiente acción.

### 2.1.12. Configuración de Syslog

logging buffered {{Tamano\_Buffer}} debugging

no logging console

logging facility {{Local\_x}}

logging {{IPServidorSyslog}}

logging trap informational

logging rate-limit console 10 except errors

{{Tamano\_Buffer}} Es el tamaño máximo, en bytes, del buffer utilizado para almacenar los mensajes de "log". Se recomienda un valor de 100000, equivalente aproximadamente a 100KB.

{{Local\_x}} Se particularizará al valor que se defina en el servidor Syslog del Centro de Gestión.

{{IPServidorSyslog}} Es la dirección IP del servidor Syslog en el Centro de Gestión.

Donde:

<Tamaño\_Buffer> Es el tamaño máximo, en bytes, del buffer utilizado para almacenar los mensajes de "log". Se recomienda un valor de 100000, equivalente aproximadamente a 100KB.

<Local\_x> Se particularizará al valor que se defina en el servidor Syslog del Centro de Gestión.

<IPServidorSyslog> Es la dirección IP del servidor Syslog en el Centro de Gestión.

Donde:

Donde:

Donde:

Donde:

<X> Corresponde a la instancia SNMP del interfaz LAN cuyas colisiones deseamos monitorizar.

NOTA: Para este servicio sólo tiene sentido en la interfaz LAN de cliente. El valor de <X>, del tipo de alarma 46001, dependerá de cada equipo, ya que hace referencia al número que le asigna el router al arrancar, por lo que es obligación del centro que quiera implementar esta parte del RMON buscar cuál es el que hace referencia a la interfaz que queremos chequear. Para saber cuál es, se puede realizar la siguiente acción.