Mejores prácticas operativas del CRS-1 y IOS XR

Contenido

Introducción

Este documento le ayuda a entenderlos:

- Proceso e hilos
- Tela del CRS-1
- Plano de Control
- Rommon y Monlib
- Módulo de interfaz de capa física (PLIM) y indicador luminoso LED amarillo de la placa muestra gravedad menor modular del servicio (MSC)
- Administración de la Configuración
- Security
- Fuera de la banda
- 'Protocolo de administración de red simple (SNMP)

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del ® XR del Cisco IOS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco IOS XR
- CRS-1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción del Cisco IOS XR

El Cisco IOS XR se diseña para escalar. El corazón es una arquitectura de Microkernel así que proporciona solamente los servicios esenciales tales como administración del proceso, previsión, señales, y temporizadores. Consideran a todos los otros servicios tales como sistemas de archivos, drivers, pilas del protocolo y aplicaciones como los administradores de recursos y funcionamiento en el espacio del usuario protegido de la memoria. Estos otros servicios pueden ser agregados o ser quitados en el tiempo de ejecución, que depende del diseño de programa. La huella de Microkernel es el kb solamente 12. El Microkernel y el sistema operativo subyacente es de los sistemas de software QNX, y se llama Neutrino. QNX se especializa en el diseño de sistema operativo en tiempo real. El Microkernel es con derecho preferente, y el planificador de trabajos es prioridad basada. Esto se asegura de que la transferencia de contexto entre los procesos sea muy rápida, y los hilos más prioritarios tienen siempre acceso al CPU cuando sea necesario. Éstos son algunas de las ventajas cuyo el Cisco IOS XR aprovecha. Pero, la ventaja

más grande es el diseño de la herencia de comunicaciones de proceso interes dentro de la base de los sistemas operativos.

El neutrino es un mensaje que pasa el sistema operativo, y los mensajes son los medios básicos de las comunicaciones entre procesos entre todos los hilos. Cuando un servidor determinado quiere proporcionar un servicio, crea un canal para los mensajes que intercambian. Los clientes asocian a los servidores el canal directamente asociando a la descripción del archivo relevante para utilizar el servicio. Todas las comunicaciones entre el cliente y servidor están al lado del mismo mecanismo. Esto es una ventaja enorme para un ordenador estupendo, que el CRS-1 es. Considere éstos cuando una operación de lectura local se realiza en un corazón estándar de UNIX:

- Interrupción de software en el corazón.
- Envíos del corazón en el sistema de archivos.
- Se reciben los datos.

Considere éstos en el caso remoto:

- Interrupción de software en el corazón.
- El corazón envía el NFS.
- El NFS llama al componente de interconexión de redes.
- El telecontrol envía al componente de interconexión de redes.
- Se llama el NFS.
- El corazón envía el sistema de archivos.

La semántica para el local leído y el telecontrol leído no son lo mismo. Los argumentos y los parámetros para bloquear de archivo y fijar los permisos son diferentes.

Considere el QNX caso local:

- Interrupción de software en el corazón.
- El corazón realiza el mensaje que pasa en el sistema de archivos.

Considere el caso no local:

- Interrupción de software en el corazón.
- El corazón entra QNET, que es el mecanismo de transporte de IPC.
- QNET entra el corazón.
- El corazón envía el sistema de archivos.

Toda la semántica que se refiere al argumento que pasa y los parámetros de sistema de archivos son idénticos. Todo se ha desemparejado en la interfaz de IPC que permite que segreguen al cliente y servidor totalmente. Esto significa que cualquier proceso puede ejecutarse dondequiera en cualquier momento. Si un procesador de la ruta determinado es peticiones de mantenimiento demasiado ocupadas, usted puede emigrar fácilmente esos servicios a un diverso CPU que se ejecute en un DRP. Un ordenador estupendo que dirige diversos servicios en diversos CPU se separó a través de los nodos múltiples que pueden comunicar fácilmente con cualquier otro nodo. La infraestructura existe para proporcionar la oportunidad de escalar. Cisco ha utilizado esta ventaja y ha escrito el software adicional que engancha en los principios de operación del mensaje que pasa el corazón que permite que CRS el router escale a los millares de Nodos, donde un nodo, en este caso un CPU, funciona con un caso del OS, si es un (RP) del proceso de la ruta, un Route Processor distribuido (DRP), un indicador luminoso LED amarillo de la placa muestra gravedad menor modular de los servicios (MSC), o un switch processor (SP).

Proceso e hilos

Dentro de los límites del Cisco IOS XR, un proceso es una área de memoria protegida que contiene uno o más hilos. De la perspectiva de los programadores, los hilos hacen el trabajo, y cada uno completa un trayecto de ejecución lógico para realizar una tarea específica. La memoria que los hilos requieren durante el flujo de ejecución pertenece al proceso actúan dentro, protegido contra cualquier otro hilo de los procesos. Un hilo es una unidad de ejecución, con un contexto de la ejecución que incluya un stack y se registre. Un proceso es un grupo de hilos que compartan un espacio de dirección virtual, aunque un proceso pueda contener un solo hilo pero contiene más a menudo más. Si otro hilo en un proceso diferente intenta escribir a la memoria en su proceso, se mata el proceso que ofende. Si hay más de un hilo que actúa dentro de su proceso, después ese hilo tiene acceso a la misma memoria dentro de su proceso, y como consecuencia es capaz sobregrabar los datos de otro hilo. Complete los pasos en un procedimiento para mantener la sincronización a los recursos para prevenir este hilo dentro del mismo proceso.

Un hilo utiliza un objeto llamado una exclusión mutua (MUTEX) para asegurar la exclusión mutua a los servicios. El hilo que tiene el MUTEX es el hilo que puede escribir a una área determinada de la memoria como un ejemplo. Otros hilos que no tienen el MUTEX no pueden. Hay también otros mecanismos para asegurar la sincronización a los recursos, y éstos son semáforos, variables condicionales o Condvars, las barreras, y Sleepons. Éstos no se discuten aquí, pero proporcionan los servicios de sincronización como parte de sus deberes. Si usted compara los principios discutidos aquí al Cisco IOS, después el Cisco IOS es un solo proceso que actúa muchos hilos, con todos los hilos que tengan acceso al mismo espacio de memoria. Pero, el Cisco IOS llama estos procesos de los hilos.

Estados del proceso y del hilo

Dentro del Cisco IOS XR hay los servidores que proporcionan los servicios y a los clientes que utilizan los servicios. Un proceso determinado puede tener varios hilos que proporcionen el mismo servicio. Otro proceso puede tener varios clientes que pudieron requerir un servicio determinado en cualquier momento. El acceso a los servidores no está siempre disponible, y si un acceso del pedido de cliente a un servicio que se sienta allí y que espera el servidor para estar libre. En este caso el cliente reputa bloqueado. Esto se llama un modelo de servidor de cliente de bloqueo. El cliente pudo ser bloqueado porque espera un recurso tal como un MUTEX, o debido al hecho de que el servidor todavía no ha contestado.

Publique un **comando ospf del proceso de la demostración** para marcar el estatus de los hilos en el proceso OSPF:

```
RP/0/RP1/CPU0:CWDCRS#show process ospf
                  Job Id: 250
                     PID: 110795
         Executable path: /disk0/hfr-rout-3.2.3/bin/ospf
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:10:06 2006
           Process state: Run
           Package state: Normal
       Started on config: cfg/gl/ipv4-ospf/proc/101/ord_a/routerid
```

```
                    core: TEXT SHAREDMEM MAINMEM
                Max. core: 0
                Placement: ON
             startup_path: /pkg/startup/ospf.startup
                   Ready: 1.591s
                Available: 5.595s
          Process cpu time: 89.051 user, 0.254 kernel, 89.305 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
250    1      40K  10 Receive       0:00:11:0509 ospf
250    2      40K  10 Receive       0:01:08:0937 ospf
250    3      40K  10 Receive       0:00:03:0380 ospf
250    4      40K  10 Condvar       0:00:00:0003 ospf
250    5      40K  10 Receive       0:00:05:0222 ospf
```

Observe que el proceso OSPF está dado un trabajo ID (JID), que es 250. Esto nunca cambia en un router corriente y generalmente en una versión determinada del Cisco IOS XR. Dentro del proceso OSPF hay cinco rosca cada uno con su propio hilo ID (TID). Mencionado es el espacio de pila para cada hilo, la prioridad de cada hilo y su estado.

Paso síncrono del mensaje

Se menciona anterior que QNX es un mensaje que pasa el sistema operativo. Es realmente un mensaje síncrono que pasa el sistema operativo. Muchos los problemas del sistema operativo se reflejan en la Mensajería síncrona. No se dice que el paso síncrono del mensaje causa cualquier problema, pero el síntoma del problema se refleja bastante en el paso síncrono del mensaje. Porque es síncrono, el ciclo vital o la información del estado es fácilmente accesible al operador del CRS-1, que ayuda en el proceso de Troubleshooting. El mensaje que pasa el ciclo vital es similar a esto:

- Un servidor crea un canal del mensaje.
- Un cliente conecta con el canal de un servidor (análogo al posix abierto).
- Un cliente envía un mensaje a un servidor (MsgSend) y las esperas para una contestación y los bloques.
- El servidor recibe (MsgReceive) un mensaje de un cliente, procesa el mensaje, y contesta al cliente.
- El cliente desbloquea y procesa la contestación del servidor.

Este client-server model de bloqueo es el paso síncrono del mensaje. Esto significa que el cliente envía un mensaje y los bloques. El servidor recibe el mensaje, lo procesa, contesta de nuevo al cliente y entonces el cliente desbloquea. Éstos son los detalles específicos:

- El servidor espera adentro RECIBE el estado.
- El cliente envía un mensaje al servidor y SE BLOQUEA.
- El servidor recibe el mensaje y lo desbloquea, si espera adentro reciba el estado.
- El cliente se traslada al estado de la CONTESTACIÓN.
- El servidor se mueve al estado de ejecución.
- Procesos del servidor el mensaje.
- El servidor contesta al cliente.
- El cliente desbloquea.

Publique el **comando show process** para ver en qué estados es el cliente y servidor.

```
RP/0/RP1/CPU0:CWDCRS#show processes
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
1      1       0K  0  Ready       320:04:04:0649 procnto-600-smp-cisco-instr
```

```
1      3        0K  10 Nanosleep     0:00:00:0043 procnto-600-smp-cisco-instr
1      5        0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      7        0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      8        0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      11       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      12       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      13       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      14       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      15       0K  19 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      16       0K  10 Receive       0:02:01:0207 procnto-600-smp-cisco-instr
1      17       0K  10 Receive       0:00:00:0015 procnto-600-smp-cisco-instr
1      21       0K  10 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      23       0K  10 Running       0:07:34:0799 procnto-600-smp-cisco-instr
1      26       0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      31       0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      33       0K  10 Receive       0:00:00:0000 procnto-600-smp-cisco-instr
1      39       0K  10 Receive       0:13:36:0166 procnto-600-smp-cisco-instr
1      46       0K  10 Receive       0:06:32:0015 procnto-600-smp-cisco-instr
1      47       0K  56 Receive       0:00:00:0029 procnto-600-smp-cisco-instr
1      48       0K  10 Receive       0:00:00:0001 procnto-600-smp-cisco-instr
1      72       0K  10 Receive       0:00:00:0691 procnto-600-smp-cisco-instr
1      73       0K  10 Receive       0:00:00:0016 procnto-600-smp-cisco-instr
1      78       0K  10 Receive       0:09:18:0334 procnto-600-smp-cisco-instr
1      91       0K  10 Receive       0:09:42:0972 procnto-600-smp-cisco-instr
1      95       0K  10 Receive       0:00:00:0011 procnto-600-smp-cisco-instr
1      103      0K  10 Receive       0:00:00:0008 procnto-600-smp-cisco-instr
74     1        8K  63 Nanosleep     0:00:00:0001 wd-mbi
53     1       28K  10 Receive       0:00:08:0904 dllmgr
53     2       28K  10 Nanosleep     0:00:00:0155 dllmgr
53     3       28K  10 Receive       0:00:03:0026 dllmgr
53     4       28K  10 Receive       0:00:09:0066 dllmgr
53     5       28K  10 Receive       0:00:01:0199 dllmgr
270    1       36K  10 Receive       0:00:36:0091 qsm
270    2       36K  10 Receive       0:00:13:0533 qsm
270    5       36K  10 Receive       0:01:01:0619 qsm
270    7       36K  10 Nanosleep     0:00:22:0439 qsm
270    8       36K  10 Receive       0:00:32:0577 qsm
67     1       52K  19 Receive       0:00:35:0047 pkgfs
67     2       52K  10 Sigwaitinfo   0:00:00:0000 pkgfs
67     3       52K  19 Receive       0:00:30:0526 pkgfs
67     4       52K  10 Receive       0:00:30:0161 pkgfs
67     5       52K  10 Receive       0:00:25:0976 pkgfs
68     1        8K  10 Receive       0:00:00:0003 devc-pty
52     1       40K  16 Receive       0:00:00:0844 devc-conaux
52     2       40K  16 Sigwaitinfo   0:00:00:0000 devc-conaux
52     3       40K  16 Receive       0:00:02:0981 devc-conaux
52     4       40K  16 Sigwaitinfo   0:00:00:0000 devc-conaux
52     5       40K  21 Receive       0:00:03:0159 devc-conaux
65545  2       24K  10 Receive       0:00:00:0487 pkgfs
65546  1       12K  16 Reply         0:00:00:0008 ksh
66     1        8K  10 Sigwaitinfo   0:00:00:0005 pipe
66     3        8K  10 Receive       0:00:00:0000 pipe
66     4        8K  16 Receive       0:00:00:0059 pipe
66     5        8K  10 Receive       0:00:00:0149 pipe
66     6        8K  10 Receive       0:00:00:0136 pipe
71     1       16K  10 Receive       0:00:09:0250 shmwin_svr
71     2       16K  10 Receive       0:00:09:0940 shmwin_svr
61     1        8K  10 Receive       0:00:00:0006 mqueue
```

Proceso bloqueado y estados del proceso

Publique el comando **bloqueado proceso de la demostración** para ver qué proceso está en el estado bloqueado.

```
RP/0/RP1/CPU0:CWDCRS#show processes blocked
  Jid       Pid Tid                 Name State  Blocked-on
65546      4106   1                  ksh Reply    4104  devc-conaux
  105     61495   2              attachd Reply   24597  eth_server
  105     61495   3              attachd Reply    8205  mqueue
  316     65606   1           tftp_server Reply    8205  mqueue
  233     90269   2               lpts_fm Reply   90223  lpts_pa
  325    110790   1             udp_snmpd Reply   90257  udp
  253    110797   4                ospfv3 Reply   90254  raw_ip
  337    245977   2                fdiagd Reply   24597  eth_server
  337    245977   3                fdiagd Reply    8205  mqueue
65762   5996770   1                  exec Reply       1  kernel
65774   6029550   1                  more Reply    8203  pipe
65778   6029554   1       show_processes Reply       1  kernel
RP/0/RP1/CPU0:CWDCRS#
```

El paso sincronizado del mensaje le permite para seguir fácilmente el ciclo vital del Inter-Process Communication entre los subprocesos diferentes. En cualquier momento, un hilo puede estar en un estado específico. Un estado bloqueado puede ser un síntoma de un problema. Esto no significa que si un hilo está en el estado bloqueado entonces hay un problema, así que no publica el comando **bloqueado proceso de la demostración** y abre un caso con el Soporte técnico de Cisco. Los hilos bloqueados son también muy normales.

Observe la salida anterior. Si usted mira el primer hilo en la lista, obsérvela es el ksh, y su contestación se bloquea en el devc-conaux. El cliente, el ksh en este caso, envió un mensaje al proceso del devc-conaux, el servidor, que es devc-conaux, contestación ksh de los controles bloqueada hasta que conteste. El Ksh es el shell de UNIX que alguien utiliza en la consola o el puerto auxiliar. El Ksh espera la entrada de la consola, y si no hay ninguno porque el operador no está tecleando, después sigue bloqueado hasta tal hora que procesa una cierta entrada. Después de procesar, el ksh vuelve a la contestación bloqueada en el devc-conaux.

Esto es normal y no ilustra un problema. La punta es que los hilos bloqueados son normales, y depende de qué versión XR, tiene el tipo de sistema usted, de lo que usted ha configurado y quién hace lo que altera ése la salida del comando **bloqueado proceso de la demostración**. El uso del comando **bloqueado proceso de la demostración** es una buena manera de comenzar a resolver problemas los problemas del tipo OS. Si hay un problema, por ejemplo el CPU es alto, después utiliza el comando anterior para ver si cualquier cosa mira fuera de normal.

Entienda cuál es normal para su router de funcionamiento. Esto proporciona una línea de fondo para que usted utilice como comparación cuando usted resuelve problemas los ciclos vitales de proceso.

En cualquier momento, un hilo puede estar en un estado particular. Esta tabla proporciona una lista de los estados:

Si es el estado:	El hilo es:
MUERTO	Muerto. El corazón está esperando para liberar los recursos de los hilos.
EJECUTÁNDOSE	Activamente ejecutándose en un CPU
LISTO	El no ejecutarse en un CPU pero está listo para ejecutarse
PARADO	Suspendido (señal SIGSTOP)
ENVÍE	Esperar un servidor para recibir un

	mensaje
‘RECIBIR’	Esperar a un cliente para enviar un mensaje
CONTESTACIÓN	Esperar un servidor para contestar a un mensaje
STACK	Esperando más stack para ser afecte un aparato
WAITPAGE	Esperar al administrador de proceso para resolver un incidente de página
SIGSUSPEND	Esperar una señal
SIGWAITINFO	Esperar una señal
NANOSLEEP	El dormir por un período de tiempo
MUTEX	El esperar para adquirir un MUTEX
CONDVAR	Esperando una variable condicional que se señalará
INCORPORARSE	Esperar la realización de otro hilo
INTR	Esperar una interrupción
SEM	El esperar para adquirir un semáforo

Procesos importantes y sus funciones

El Cisco IOS XR tiene muchos procesos. Éstos son algunos importantes con sus funciones explicadas aquí.

Monitor de sistema de vigilancia (WDSysmon)

Esto es un servicio proporcionado para la detección de proceso cuelga y las condiciones de memoria baja. Memoria baja puede ocurrir como resultado de una fuga de memoria o de una cierta otra circunstancia extraña. Una caída puede ser el resultado de varias condiciones tales como interbloqueos de proceso, Loop infinito, cárceles del corazón o errores de previsión. En cualquier entorno con hilos múltiples el sistema puede conseguir en un estado conocido como una condición del interbloqueo, o apenas simplemente interbloqueo. Un interbloqueo puede ocurrir cuando uno o más hilos no pueden continuar debido a la contención de recurso. Por ejemplo, rosque A puede enviar un mensaje para roscar B mientras que el hilo B envía simultáneamente un mensaje para roscar el A. Ambos hilos esperan en uno a y pueden estar adentro envían el estado bloqueado, y ambos hilos esperan para siempre. Éste es un caso simple que implica dos hilos, pero si un servidor es responsable de un recurso que sea utilizado por muchos hilos se bloquea en otro hilo, después los muchos hilos que piden acceso a ese recurso puede ser envían esperar bloqueado en el servidor.

Los interbloqueos pueden ocurrir entre algunos hilos, pero pueden afectar otros hilos como consecuencia. Los interbloqueos son evitados por el buen diseño de programa, pero con independencia de cómo un programa se diseña y se escribe magnífico. Una Secuencia de eventos determinada que son dependiente de los datos con las sincronizaciones específicas puede causar a veces un interbloqueo. Los interbloqueos no son siempre deterministas y son generalmente muy difíciles de reproducirse. WDSysmon tiene muchos hilos con uno que se ejecute en la prioridad más alta que el neutrino soporta, 63. El ejecutarse en la prioridad 63 la asegura que el hilo consigue hora de la CPU en un entorno de previsión con derecho preferente

basado prioridad. WDSysmon trabaja con la capacidad y los vigilar del perro guardián del hardware los procesos del software que buscan las condiciones de la caída. Cuando se detectan tales condiciones, WDSysmon recoge la Más información alrededor de la condición, puede coredump el proceso o el corazón, poner en escrito a los Syslog, funciona con los scripts, y mata a los procesos bloqueados. Dependiente sobre cómo es drástico es el problema, puede iniciar un Switch del Route Processor encima para mantener la operación del sistema.

```
RP/0/RP1/CPU0:CWDCRS#show processes wdsysmon
                  Job Id: 331
                     PID: 36908
         Executable path: /disk0/hfr-base-3.2.3/sbin/wdsysmon
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:07:36 2006
           Process state: Run
           Package state: Normal
                    core: SPARSE
                Max. core: 0
                   Level: 40
              Mandatory: ON
             startup_path: /pkg/startup/wdsysmon.startup
             memory limit: 10240
                   Ready: 0.705s
        Process cpu time: 4988.295 user, 991.503 kernel, 5979.798 total

JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
331    1      84K  19 Receive       0:00:00:0029 wdsysmon
331    2      84K  10 Receive       0:17:34:0212 wdsysmon
331    3      84K  10 Receive       0:00:00:0110 wdsysmon
331    4      84K  10 Receive       1:05:26:0803 wdsysmon
331    5      84K  19 Receive       0:00:06:0722 wdsysmon
331    6      84K  10 Receive       0:00:00:0110 wdsysmon
331    7      84K  63 Receive       0:00:00:0002 wdsysmon
331    8      84K  11 Receive       0:00:00:0305 wdsysmon
331    9      84K  20 Sem           0:00:00:0000 wdsysmon
```

El WDSysmon de proceso tiene nueve hilos. Cuatro funcionados con en la prioridad 10, los otros cuatro están en 11, 19, 20 y 63. Cuando se diseña un proceso, el programador considera cuidadosamente la prioridad que cada hilo dentro del proceso debe ser dado. Según lo discutido previamente, el planificador de trabajos es la prioridad basada, que significa que un hilo más prioritario se apropia siempre de uno de la prioridad baja. La prioridad 63 es la prioridad más alta que un hilo puede ejecutarse en, que es el hilo 7 en este caso. El hilo 7 es el hilo del vigilante, el hilo ese los cerdos de las pistas CPU. Debe ejecutarse en una prioridad más alta que los otros hilos que los mira de otra manera no pudieron conseguir la ocasión de ejecutarse en absoluto, que la previene de los pasos que fue diseñada para realizar.

Netio

En el Cisco IOS, hay el concepto de transferencia y de process switching rápidos. La transferencia rápida utiliza el código CEF y ocurre en el tiempo de interrupción. El process switching utiliza el ip_input, que es el código del Switching IP, y es un proceso planificado. En Plataformas más de gama alta el CEF Switching se hace en hardware, y el ip_input se programa en el CPU. El equivalente del ip_input en el Cisco IOS XR es Netio.

```
P/0/RP1/CPU0:CWDCRS#show processes netio
                  Job Id: 241
                     PID: 65602
         Executable path: /disk0/hfr-base-3.2.3/sbin/netio
              Instance #: 1
                    Args: d
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:07:53 2006
           Process state: Run
           Package state: Normal
                    core: DUMPFALLBACK COPY SPARSE
                Max. core: 0
                   Level: 56
              Mandatory: ON
             startup_path: /pkg/startup/netio.startup
                   Ready: 17.094s
        Process cpu time: 188.659 user, 5.436 kernel, 194.095 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
241    1     152K  10 Receive       0:00:13:0757 netio
241    2     152K  10 Receive       0:00:10:0756 netio
241    3     152K  10 Condvar       0:00:08:0094 netio
241    4     152K  10 Receive       0:00:22:0016 netio
241    5     152K  10 Receive       0:00:00:0001 netio
241    6     152K  10 Receive       0:00:04:0920 netio
241    7     152K  10 Receive       0:00:03:0507 netio
241    8     152K  10 Receive       0:00:02:0139 netio
241    9     152K  10 Receive       0:01:44:0654 netio
241    10    152K  10 Receive       0:00:00:0310 netio
241    11    152K  10 Receive       0:00:13:0241 netio
241    12    152K  10 Receive       0:00:05:0258 netio
```

El grupo mantiene el proceso (el GSP)

Hay una necesidad de la comunicación en cualquier superordenador con varios miles de Nodos ese que cada uno funciona con su propio caso del corazón. En Internet, uno a muchos comunicación se hace eficientemente vía los protocolos de la multidistribución. El GSP es el protocolo interno de la multidistribución que se utiliza para IPC dentro del CRS-1. El GSP proporciona uno a muchos la comunicación confiable del grupo que está sin conexión con la semántica asíncrona. Esto permite que el GSP escale al mil de los Nodos.

```
RP/0/RP1/CPU0:CWDCRS#show processes gsp
                  Job Id: 171
                     PID: 65604
         Executable path: /disk0/hfr-base-3.2.3/bin/gsp
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:07:53 2006
           Process state: Run
           Package state: Normal
                    core: TEXT SHAREDMEM MAINMEM
                Max. core: 0
                   Level: 80
              Mandatory: ON
             startup_path: /pkg/startup/gsp-rp.startup
                   Ready: 5.259s
```

```
               Available: 16.613s
        Process cpu time: 988.265 user, 0.792 kernel, 989.057 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
171    1     152K  30 Receive       0:00:51:0815 gsp
171    3     152K  10 Condvar       0:00:00:0025 gsp
171    4     152K  10 Receive       0:00:08:0594 gsp
171    5     152K  10 Condvar       0:01:33:0274 gsp
171    6     152K  10 Condvar       0:00:55:0051 gsp
171    7     152K  10 Receive       0:02:24:0894 gsp
171    8     152K  10 Receive       0:00:09:0561 gsp
171    9     152K  10 Condvar       0:02:33:0815 gsp
171    10    152K  10 Condvar       0:02:20:0794 gsp
171    11    152K  10 Condvar       0:02:27:0880 gsp
171    12    152K  30 Receive       0:00:46:0276 gsp
171    13    152K  30 Receive       0:00:45:0727 gsp
171    14    152K  30 Receive       0:00:49:0596 gsp
171    15    152K  30 Receive       0:00:38:0276 gsp
171    16    152K  10 Receive       0:00:02:0774 gsp
```

Descargador del contenido del bulto BCDL

BCDL es para confiablemente datos de multidifusión usados a los diversos Nodos tales como RP y MSC. Utiliza el GSP como el transporte subyacente. Garantías BCDL **en la** salida de la **orden de los** mensajes. Dentro de BCDL hay un agente, un productor y un consumidor. El agente es el proceso que comunica con el productor para extraer y mitigar los datos antes de sus Multicast a los consumidores. El productor es el proceso que presenta los datos que todo el mundo quiere, y el consumidor es el proceso interesado recibir los datos proporcionados por el productor. BCDL se utiliza durante las actualizaciones del Software Cisco IOS XR.

Mensajería ligera (LWM)

El LWM es una forma creada por Cisco de Mensajería que fue diseñada para crear una capa de abstracción entre las aplicaciones que el proceso inter comunica con uno a y el neutrino, con la meta como independencia del sistema operativo y de la capa de transporte. Si Cisco desea de cambiar al vendedor OS de QNX algún otro, una capa de abstracción entre las funciones rudimentarias de las ayudas del sistema operativo subyacente quita la dependencia en el sistema operativo y las ayudas en virar hacia el lado de babor a otro sistema operativo. El LWM proporciona la entrega de mensajes garantizada síncrona, que les gusta el mensaje nativo del neutrino que pasa, hace al remitente bloquear hasta que el receptor conteste.

El LWM también proporciona la salida del mensaje asíncrono vía 40 pulsos del bit. Los mensajes asíncronos son asynchronously enviado, que significa que el mensaje está hecho cola y el remitente no bloquea, sino no es recibido por el asynchronously del servidor, pero cuando el servidor sondea para el mensaje disponible siguiente. El LWM se estructura como el cliente/servidor. El servidor crea un canal que le dé un **oído** para escuchar adentro los mensajes y siente en un tiempo el loop haga un mensaje reciba escuchar en el canal, que acaba de crear. Cuando llega un mensaje desbloquea y consigue un Identificador de cliente, que es con eficacia la misma cosa que la recepción ID del mensaje recibió. El servidor entonces realiza alguno que procesa y posterior hace una contestación del mensaje al Identificador de cliente.

En el lado del cliente hace un mensaje conecta. Consigue pasado un identificador al cual conecte y después haga un mensaje envíe y se bloquea. Cuando el servidor acaba de procesar, contesta y el cliente se desbloquea. Éste es virtualmente lo mismo que el mensaje nativo de los neutrinos que pasa, así que la capa de abstracción está muy ligeramente.

El LWM se diseña con un número mínimo de llamadas del sistema y de Switches del contexto

para el rendimiento alto, y es el método preferido de IPC en el entorno del Cisco IOS XR.

Envmon

A lo sumo el fundamental llano, el sistema de monitor de entorno es responsable del advertir cuando los parámetros físicos, por ejemplo temperatura, voltaje, velocidad de la fan y así sucesivamente, caída fuera de los rangos operativos, y de apagar el hardware que se acerca a los niveles críticos donde el hardware pudo ser dañado. Monitorea cada sensor disponible del hardware, compara el Valor medido contra los umbrales indicador luminoso LED amarillo de la placa muestra gravedad menor-específicos, y aumenta periódicamente las alarmas cuanto sea necesario para lograr esta tarea. Un proceso persistente, comenzado en la inicialización del sistema, que sondea periódicamente todos los sensores del hardware, por ejemplo voltaje, temperatura, y velocidad de la fan, en el chasis y proporciona estos datos a los clientes externos de la Administración. Además, el proceso periódico compara las lecturas del sensor con los umbrales de la alarma y publica las alertas ambientales a la base de datos del sistema para la acción subsiguiente del administrador del incidente. Si las lecturas del sensor están peligroso fuera de rango, el proceso del monitoreo de entorno pudo hacer el indicador luminoso LED amarillo de la placa muestra gravedad menor ser apaga.

Introducción de la tela del CRS-1

- Tela gradual — topología de Benes de 3 etapas
- Dynamic Routing dentro de la tela para minimizar la congestión
- Célula basada: 136 células byte, carga útil de datos de 120 bytes
- Control de flujo para mejorar el aislamiento de tráfico y para minimizar mitigar los requisitos en la tela
- Etapa para efectuar la entrega del Speedup
- Dos moldes de tráfico soportados (unicast y Multicast)
- Dos prioridades del tráfico soportadas por el molde (cielo y tierra)
- Soporte para los grupos de multidifusión de la tela del 1M (FGIDs)
- Tolerancia de fallas rentable: Redundancia N+1 o N+k usando los aviones de la tela en comparación con 1+1 en el coste grandemente creciente

Cuando usted se ejecuta en el modo del chasis único, el s1, el s2 y el asics S3 están situados en las mismas placas de fábrica. Este indicador luminoso LED amarillo de la placa muestra gravedad menor también se refiere comúnmente como **indicador luminoso LED amarillo de la placa muestra gravedad menor S123**. En una configuración del Multi-chasis, se separa el s2 y está en el chasis de placa de fábrica (FCC). Esta configuración requiere dos placas de fábrica formar un avión, un indicador luminoso LED amarillo de la placa muestra gravedad menor del s2, y un indicador luminoso LED amarillo de la placa muestra gravedad menor S13. Cada MSC conecta con ocho aviones de la tela para proporcionar la Redundancia de modo que si usted suelta uno o más aviones, su tela todavía pase el tráfico aunque el tráfico total, que puede pasar a través de la tela, sea más bajo. CRS puede todavía actuar en el linerate para la mayoría de los tamaños de paquetes con solamente siete aviones. El backpressure se envía sobre la tela sobre un impar e incluso plano. No se recomienda para ejecutar un con menos del sistema dos aviones, en un impar e incluso plano. Cualquier cosa menos de dos aviones no es una configuración admitida.

El avión de la tela

El diagrama anterior representa un avión. Usted tiene que multiplicar ese diagrama por ocho. Eso significa que el rociador (ingressq) asic de un LC conecta con 8 S1s (1 s1 por el avión). El s1 en

cada avión de la tela conecta con 8 rociadores:

- los 8 LC superiores del chasis
- los 8 LC inferiores

Hay 16 S1s por 16 chasis del slot LC: 8 para el top LC (1 por el avión) + 8 para la parte inferior LC.

En los solo 16 chasis del slot, una placa de fábrica S123 tiene 2 S1s, 2 s2 y 4 S3. Ésa es parte del cómputo del speedup de la tela. Hay dos veces mÌas tráfico, que puede salir la tela como el tráfico puede ingresar. Hay también actualmente dos esponjas (fabricq) por el LC comparado a 1 rociador. Esto permite mitigar en la salida LC cuando más de un ingreso LC sobrecarga una salida LC. La salida LC puede absorber ese ancho de banda adicional de la tela.

Supervisión de la tela

Disponibilidad y Conectividad planas:

```
RP/0/RP1/CPU0:CWDCRS#show processes gsp
                  Job Id: 171
                     PID: 65604
          Executable path: /disk0/hfr-base-3.2.3/bin/gsp
               Instance #: 1
               Version ID: 00.00.0000
                  Respawn: ON
            Respawn count: 1
  Max. spawns per minute: 12
             Last started: Tue Jul 18 13:07:53 2006
            Process state: Run
            Package state: Normal
                     core: TEXT SHAREDMEM MAINMEM
                Max. core: 0
                    Level: 80
                Mandatory: ON
             startup_path: /pkg/startup/gsp-rp.startup
                    Ready: 5.259s
                Available: 16.613s
         Process cpu time: 988.265 user, 0.792 kernel, 989.057 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
171    1     152K  30 Receive       0:00:51:0815 gsp
171    3     152K  10 Condvar       0:00:00:0025 gsp
171    4     152K  10 Receive       0:00:08:0594 gsp
171    5     152K  10 Condvar       0:01:33:0274 gsp
171    6     152K  10 Condvar       0:00:55:0051 gsp
171    7     152K  10 Receive       0:02:24:0894 gsp
171    8     152K  10 Receive       0:00:09:0561 gsp
171    9     152K  10 Condvar       0:02:33:0815 gsp
171    10    152K  10 Condvar       0:02:20:0794 gsp
171    11    152K  10 Condvar       0:02:27:0880 gsp
171    12    152K  30 Receive       0:00:46:0276 gsp
171    13    152K  30 Receive       0:00:45:0727 gsp
171    14    152K  30 Receive       0:00:49:0596 gsp
171    15    152K  30 Receive       0:00:38:0276 gsp
171    16    152K  10 Receive       0:00:02:0774 gsp
```

Marque si aviones están recibiendo/que transmiten células y algunos errores están incrementando:

```
RP/0/RP1/CPU0:CWDCRS#show processes gsp
                  Job Id: 171
                     PID: 65604
         Executable path: /disk0/hfr-base-3.2.3/bin/gsp
              Instance #: 1
              Version ID: 00.00.0000
                 Respawn: ON
           Respawn count: 1
  Max. spawns per minute: 12
            Last started: Tue Jul 18 13:07:53 2006
           Process state: Run
           Package state: Normal
                    core: TEXT SHAREDMEM MAINMEM
                Max. core: 0
                   Level: 80
              Mandatory: ON
             startup_path: /pkg/startup/gsp-rp.startup
                   Ready: 5.259s
               Available: 16.613s
        Process cpu time: 988.265 user, 0.792 kernel, 989.057 total
JID    TID  Stack pri state        HR:MM:SS:MSEC NAME
171    1     152K  30 Receive       0:00:51:0815 gsp
171    3     152K  10 Condvar       0:00:00:0025 gsp
171    4     152K  10 Receive       0:00:08:0594 gsp
171    5     152K  10 Condvar       0:01:33:0274 gsp
171    6     152K  10 Condvar       0:00:55:0051 gsp
171    7     152K  10 Receive       0:02:24:0894 gsp
171    8     152K  10 Receive       0:00:09:0561 gsp
171    9     152K  10 Condvar       0:02:33:0815 gsp
171    10    152K  10 Condvar       0:02:20:0794 gsp
171    11    152K  10 Condvar       0:02:27:0880 gsp
171    12    152K  30 Receive       0:00:46:0276 gsp
171    13    152K  30 Receive       0:00:45:0727 gsp
171    14    152K  30 Receive       0:00:49:0596 gsp
171    15    152K  30 Receive       0:00:38:0276 gsp
171    16    152K  10 Receive       0:00:02:0774 gsp
```

Las siglas en el comando anterior:

- CE — Error corregible
- Ecu — Error incorregible
- PE — Error de paridad

No se preocupe si notan algunos errores, pues ésta puede suceder en el bootup. Los campos no deben incrementar en el tiempo de ejecución. Si son, puede ser una indicación de un problema en la tela. Publique este comando para conseguir una ruptura de los errores por el avión de la tela:

```
admin show controllers fabric plane <0-7> statistics detail
```

Controle la descripción plana

La Conectividad del avión del control entre el chasis del linecard y el chasis de la tela está actualmente vía los puertos Gigabit Ethernet en los RP (LCC) y SCGE (FCC). La interconexión entre los puertos se proporciona vía un par de Catalyst 6500 Switch, que se pueden conectar vía dos o más puertos Gigabit Ethernet.

Configuración del Catalyst 6500

Ésta es configuración recomendada para los switches de Catalyst usados para el avión del control del multi-chasis:

- Un solo VLA N se utiliza en todos los puertos.
- Todos los puertos ejecutados en el modo de acceso (ningún enlace).
- El Spanning-tree 802.1w/s se utiliza para la prevención del loop.
- Dos o más links se utilizan para cruz-conectar el dos Switches y el STP se utiliza para loop-previene. La canalización no se recomienda.
- Puertos que conectan con modo PRE-estándar del uso del CRS-1 RP y SCGE puesto que IOS-XR no soporta el 802.1s basado los estándares.
- El UDLD se debe habilitar en los puertos que conectan entre el Switches y entre el Switches y el RP/SCGE.
- El UDLD se habilita por abandono en el CRS-1.

Refiera a sacar a colación el Software Cisco IOS XR en un sistema de Multishelf para más información sobre cómo configurar un Catalyst 6500 en un sistema de Multishelf.

Administración del avión del control del Multi-chasis

El chasis del Catalyst 6504-E, que proporciona la Conectividad del avión del control para el sistema del multi-chasis, se configura para estos servicios de administración:

- Administración en la banda vía el Gigabit de puerto el 1/2, que conecta con un switch LAN en cada estallido. El acceso se permite solamente para un pequeño rango de subred y los protocolos.
- El NTP se utiliza para fijar el Tiempo del sistema.
- El syslogging se realiza a los host estándar.
- La Consulta SNMP y los desvíos se pueden habilitar para las funciones críticas.

Note: Ningunos cambios se deben realizar al Catalyst en funcionamiento. La prueba anterior se debe hacer en cualquier cambio planificado y se recomienda altamente que esto está hecha durante una ventana de mantenimiento.

Esto es una muestra de configuración de la administración:

```
#In-band management connectivity
interface GigabitEthernet2/1
 description *CRS Multi-chassis Management Ethernet - DO NOT TOUCH*
 ip address [ip address] [netmask]
 ip access-group control_only in
!
!
ip access-list extended control_only
 permit udp [ip address] [netmask] any eq snmp
 permit udp [ip address] [netmask] eq ntp any
 permit tcp [ip address] [netmask] any eq telnet

#NTP

ntp update-calendar
ntp server [ip address]

#Syslog
logging source-interface Loopback0
logging [ip address]
```

```
logging buffered 4096000 debugging
no logging console

#RADIUS
aaa new-model
aaa authentication login default radius enable
enable password {password}
radius-server host [ip address] auth-port 1645 acct-port 1646
radius-server key {key}

#Telnet and console access
!
access-list 3 permit [ip address]
!
line con 0
 exec-timeout 30 0
 password {password}
line vty 0 4
 access-class 3 in
 exec-timeout 0 0
password {password}
```

ROMMON y Monlib

El monlib de Cisco es un programa ejecutable que se salva en el dispositivo y se carga en el RAM para la ejecución por el ROMMON. El ROMMON utiliza el monlib para acceder los archivos en el dispositivo. Las versiones ROMmones se pueden actualizar y se deben hacer tan bajo recomendación del Soporte técnico de Cisco. La última versión ROMmon es 1.40.

Instrucciones para la actualización

Complete estos pasos:

1. Descargue el binaries ROMMON del CRS-1 ROMMON (clientes registrados solamente) de Cisco.
2. Desempaquete el archivo TAR y copie los 6 archivo bin en CRS el directorio raíz del disk0.

```
#In-band management connectivity
interface GigabitEthernet2/1
 description *CRS Multi-chassis Management Ethernet - DO NOT TOUCH*
 ip address [ip address] [netmask]
 ip access-group control_only in
!
!
ip access-list extended control_only
 permit udp [ip address] [netmask] any eq snmp
 permit udp [ip address] [netmask] eq ntp any
 permit tcp [ip address] [netmask] any eq telnet

#NTP

ntp update-calendar
ntp server [ip address]

#Syslog
logging source-interface Loopback0
logging [ip address]
logging buffered 4096000 debugging
no logging console

#RADIUS
```

```
aaa new-model
aaa authentication login default radius enable
enable password {password}
radius-server host [ip address] auth-port 1645 acct-port 1646
radius-server key {key}

#Telnet and console access
!
access-list 3 permit [ip address]
!
line con 0
 exec-timeout 30 0
 password {password}
line vty 0 4
 access-class 3 in
 exec-timeout 0 0
password {password}
```

3. Utilice el **diag de la demostración | ROM inc. |NODO|**Comando **PLIM** para ver la versión ROMmon actual.

```
RP/0/RP0/CPU0:ROUTER(admin)#show diag | inc ROM|NODE|PLIM
NODE 0/0/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/0/CPU0 : 4OC192-POS/DPT
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/2/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/2/CPU0 : 8-10GbE
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/4/SP : Unknown Card Type
NODE 0/6/SP : MSC(SP)
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
PLIM 0/6/CPU0 : 16OC48-POS/DPT
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/RP0/CPU0 : RP
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/RP1/CPU0 : RP
  ROMMON: Version 1.19b(20050216:033559) [CRS-1 ROMMON]
NODE 0/SM0/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM1/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM2/SP : FC/S
  ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
NODE 0/SM3/SP : FC/S
ROMMON: Version 1.19b(20050216:033352) [CRS-1 ROMMON]
```

4. Entra el modo ADMIN y utiliza el **rommon de la actualización todo el** comando del **disk0** para actualizar el ROMMON.

```
RP/0/RP0/CPU0:ROUTER#admin
RP/0/RP0/CPU0:ROUTER(admin)#upgrade rommon a all disk0
Please do not power cycle, reload the router or reset any nodes until
 all upgrades are completed.
Please check the syslog to make sure that all nodes are upgraded successfully.
If you need to perform multiple upgrades, please wait for current upgrade
 to be completed before proceeding to another upgrade.
Failure to do so may render the cards under upgrade to be unusable.
```

5. Dé salida al modo ADMIN y ingrese el **registro de la demostración | el inc. "ACEPTABLE, el ROMMON A"** y se aseeguran todos los Nodos actualizados con éxito. Si los Nodos uces de los fallan, vuelva al paso 4 y reprograme.

```
RP/0/RP0/CPU0:ROUTER#show logging | inc "OK, ROMMON A"
RP/0/RP0/CPU0:Oct 28 14:40:57.223 PST8: upgrade_daemon[380][360]: OK, ROMMON A is
programmed successfully. SP/0/0/SP:Oct 28 14:40:58.249 PST8: upgrade_daemon[125][121]: OK,
```

```
ROMMON A is programmed successfully. SP/0/2/SP:Oct 28 14:40:58.251 PST8:
upgrade_daemon[125][121]: OK, ROMMON A is programmed successfully. LC/0/6/CPU0:Oct 28
14:40:58.336 PST8: upgrade_daemon[244][233]: OK, ROMMON A is programmed successfully.
LC/0/2/CPU0:Oct 28 14:40:58.365 PST8: upgrade_daemon[244][233]: OK, ROMMON A is programmed
successfully. SP/0/SM0/SP:Oct 28 14:40:58.439 PST8: upgrade_daemon[125][121]: OK, ROMMON A
is programmed successfully. SP/0/SM1/SP:Oct 28 14:40:58.524 PST8: upgrade_daemon[125][121]:
OK, ROMMON A is programmed successfully. LC/0/0/CPU0:Oct 28 14:40:58.530 PST8:
upgrade_daemon[244][233]: OK, ROMMON A is programmed successfully. RP/0/RP1/CPU0:Oct 28
14:40:58.593 PST8: upgrade_daemon[380][360]: OK, ROMMON A is programmed successfully.
SP/0/6/SP:Oct 28 14:40:58.822 PST8: upgrade_daemon[125][121]: OK, ROMMON A is programmed
successfully. SP/0/SM2/SP:Oct 28 14:40:58.890 PST8: upgrade_daemon[125][121]: OK, ROMMON A
is programmed successfully. SP/0/SM3/SP:Oct 28 14:40:59.519 PST8: upgrade_daemon[125][121]:
OK, ROMMON A is programmed successfully.
```

6. Entra el modo ADMIN y utiliza el **rommon b de la actualización todo el** comando del **disk0** para actualizar el ROMMON.

```
RP/0/RP0/CPU0:ROUTER#admin
RP/0/RP0/CPU0:ROUTER(admin)#upgrade rommon b all disk0
Please do not power cycle, reload the router or reset any nodes until
 all upgrades are completed.
Please check the syslog to make sure that all nodes are upgraded successfully.
If you need to perform multiple upgrades, please wait for current upgrade
 to be completed before proceeding to another upgrade.
Failure to do so may render the cards under upgrade to be unusable.
```

7. Dé salida al modo ADMIN y ingrese el **registro de la demostración | el inc. "ACEPTABLE, el ROMMON B"** y se aseeguran todos los Nodos actualizados con éxito. Si los Nodos uces de los fallan, vuelva al paso 4 y reprograme.

```
RP/0/RP0/CPU0:Router#show logging | inc "OK, ROMMON B"
RP/0/RP0/CPU0:Oct 28 13:27:00.783 PST8: upgrade_daemon[380][360]: OK,
ROMMON B is programmed successfully.
LC/0/6/CPU0:Oct 28 13:27:01.720 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/2/SP:Oct 28 13:27:01.755 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
LC/0/2/CPU0:Oct 28 13:27:01.775 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/0/SP:Oct 28 13:27:01.792 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM0/SP:Oct 28 13:27:01.955 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
LC/0/0/CPU0:Oct 28 13:27:01.975 PST8: upgrade_daemon[244][233]: OK,
ROMMON B is programmed successfully.
SP/0/6/SP:Oct 28 13:27:01.989 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM1/SP:Oct 28 13:27:02.087 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
RP/0/RP1/CPU0:Oct 28 13:27:02.106 PST8: upgrade_daemon[380][360]: OK,
ROMMON B is programmed successfully.
SP/0/SM3/SP:Oct 28 13:27:02.695 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
SP/0/SM2/SP:Oct 28 13:27:02.821 PST8: upgrade_daemon[125][121]: OK,
ROMMON B is programmed successfully.
```

8. **El comando upgrade** apenas quema una sección reservada especial del bootflash con el nuevo ROMMON. Pero el nuevo ROMMON sigue siendo inactivo hasta que se recargue el indicador luminoso LED amarillo de la placa muestra gravedad menor. Tan cuando usted la recarga el indicador luminoso LED amarillo de la placa muestra gravedad menor, el nuevo ROMMON es activo. Reajuste cada nodo uno a la vez o apenas reajuste al router entero para hacer esto.

```
Reload Router:
RP/0/RP0/CPU0:ROUTER#hw-module node 0/RP0/CPU0 or 0/RP1/CPU0 reload (depends on which on is
in Standby Mode.
```

```
RP/0/RP0/CPU0:ROUTER#reload
!--- Issue right after the first command. Updating Commit Database. Please wait...[OK]
Proceed with reload? [confirm] !--- Reload each Node. For Fan Controllers (FCx), !--- Alarm
Modules (AMx), Fabric Cards (SMx), and RPs (RPx), !--- you must wait until the reloaded
node is fully reloaded !--- before you reset the next node of the pair. But non-pairs !---
can be reloaded without waiting. RP/0/RP0/CPU0:ROUTER#hw-module node 0/RP0/CPU0 or
0/RP1/CPU0 reload
!--- This depends on which on is in Standby Mode. RP/0/RP0/CPU0:ROUTER#hw-module node
0/FC0/SP
RP/0/RP0/CPU0:ROUTER#hw-module node 0/AM0/SP
RP/0/RP0/CPU0:ROUTER#hw-module node 0/SM0/SP
!--- Do not reset the MSC and Fabric Cards at the same time. RP/0/RP0/CPU0:ROUTER#hw-module
node 0/0/CPU
```

9. Utilice el **diag de la demostración | ROM inc. |NODO|**Comando **PLIM** para marcar la versión de la ROMmon actuales.

```
RP/0/RP1/CPU0:CRS-B(admin)#show diag | inc ROM|NODE|PLIM
NODE 0/0/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/0/CPU0 : 4OC192-POS/DPT
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/2/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/2/CPU0 : 8-10GbE
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/6/SP : MSC(SP)
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
PLIM 0/6/CPU0 : 16OC48-POS/DPT
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/RP0/CPU0 : RP
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]
NODE 0/RP1/CPU0 : RP
  ROMMON: Version 1.32(20050525:193559)  [CRS-1 ROMMON]]
NODE 0/SM0/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM1/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM2/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
NODE 0/SM3/SP : FC/S
  ROMMON: Version 1.32(20050525:193402)  [CRS-1 ROMMON]
```

Note: En CRS-8 y el chasis de la tela, el ROMMON también fija las velocidades de la fan a la velocidad predeterminada de 4000 RPM.

Descripción PLIM y MSC

Esto representa el flujo de paquetes en el router del CRS-1, y estos términos se utilizan alternativamente:

IngressQ ASIC también se llama el rociador ASIC.

FabricQ ASIC también se llama la esponja ASIC.

EgressQ ASIC también se llama el Sharq ASIC.

Los SPP también se llaman el PSE (motor) del Packet Switch ASIC.

Rx PLIM > rx SPP > ingreso Q > tela > tela Q > tx SPP > salida Q > tx PLIM (rociador) (esponja)

(Sharq)

Los paquetes se reciben en el módulo de interfaz de capa física (PLIM).

El PLIM contiene las interfaces físicas para el MSC con el cual se acopla. El PLIM y el MSC son indicadores luminosos LED amarillo de la placa muestra gravedad menor separados conectados vía el backplane del chasis. Como consecuencia al tipo del PLIM definen a los tipos de interfaz para un MSC específico con el cual se acopló. El dependiente sobre el tipo de PLIM, el indicador luminoso LED amarillo de la placa muestra gravedad menor contiene un diverso número de Asics que proporciona los medios físicos y enmarcar para las interfaces. El propósito del PLIM Asics es proporcionar la interfaz entre el MSC y las conexiones físicas. Termina la fibra, hace la luz a la conversión eléctrica, termina los media que enmarcan siendo SDH/Sonet/Ethernet/HDLC/PPP, marca el CRC, agrega una cierta información de control llamada el encabezado de memoria intermedia y adelante los bits que permanece sobre el MSC. El PLIM no hace fuente/fregadero el HDLC o las señales de mantenimiento de PPP. Éstos son dirigidos por el CPU en el MSC.

El PLIM también proporciona estas funciones:

- MAC que filtra para 1/10 Gigabit Ethernet
- Ingreso/salida MAC que explica 1/10 Gigabit Ethernet
- VLA N que filtra para 1/10 Gigabit Ethernet
- VLA N que explica 1/10 Gigabit Ethernet
- El mitigar y notificación de congestión del ingreso

Oversubscription PLIM

10GE PLIM

Los 8 X10G PLIM ofrece la capacidad para terminar aproximadamente el 80 Gbps del tráfico mientras que la capacidad de reenvío del MSC es un máximo del 40 Gbps. Si todos los puertos disponibles en el PLIM se pueblan, después el oversubscription ocurre y el modelado de QoS llega a ser extremadamente importante asegurarse de que el tráfico de primera clase no está caído inadvertidamente. Para alguno, el oversubscription no es una opción y debe ser evitado. Solamente cuatro de los ocho puertos se deben utilizar para hacer esto. Además, el cuidado se debe tomar para asegurarse de que el ancho de banda óptimo dentro del MSC y del PLIM está disponible para cada uno de los cuatro puertos.

Note: Los cambios de la correlación de puertos de la versión 3.2.2 hacia adelante. Vea estos diagramas.

Correlación de puertos hasta la versión 3.2.1 Correlación de puertos de la versión 3.2.2 hacia adelante

Como se mencionó anteriormente, los puertos físicos son mantenidos por uno de los dos FabricQ Asics. La asignación de los puertos a ASIC se define y no puede estáticamente ser alterada. Además, los 8 X10G PLIM tiene dos PLA Asics. El primer PLA mantiene los puertos 0 a 3, los segundos servicios 4 a 7. La capacidad de ancho de banda de un solo PLA en los 8 X10G PLIM es aproximadamente 24 Gbps. El Switching Capacity de un solo FabricQ ASIC es aproximadamente 62 Mpps.

Si usted puebla el puerto 0 a 3 o puertos 4 a 7, la capacidad de ancho de banda del PLA (24 Gbps) se comparte entre los cuatro de los puertos que restringen el rendimiento de

procesamiento general. Si usted puebla los puertos 0,2,4 y 6 (hasta 3.2.1) o 0,1,4 y 5 (3.2.2 hacia adelante) como todos estos puertos es mantenido por el un FabricQ ASIC, cuyo Switching Capacity es 62 Mpps, otra vez, que restringe la capacidad de producción.

Es el mejor utilizar los puertos de una forma que obtiene la mayor eficiencia de los PLAs y del FabricQ Asics para alcanzar el rendimiento óptimo.

SIP-800/SPA

El SIP-800 PLIM ofrece la capacidad de actuar con los indicadores luminosos LED amarillo de la placa muestra gravedad menor de interfaz modular conocidos como adaptadores de puerto del servicio (SPA). El SIP-800 proporciona 6 bahías SPA con una capacidad teórica de la interfaz del 60 Gbps. La capacidad de reenvío del MSC es un máximo del 40 Gbps. Si se poblaran todas las bahías en el SIP-800, después, dependiente sobre el tipo SPA, es posible que ocurre el oversubscription y modelado de QoS llega a ser extremadamente importante para asegurarse de que el tráfico de primera clase no está caído inadvertidamente.

Note: El oversubscription no se soporta con las interfaces POS. Pero, la colocación de los 10 GB POS SPA debe ser apropiada para asegurarse que la capacidad de producción correcta está proporcionada. El Ethernet SPA 10 GB se soporta solamente en IOS-XR la versión 3.4. Este SPA ofrece las capacidades del oversubscription.

Para alguno, el oversubscription no es una opción y debe ser evitado. Solamente cuatro de los sixbays se deben utilizar para hacer esto. Además, el cuidado debe ser orden admitida para asegurarse de que el ancho de banda óptimo dentro del MSC y del PLIM está disponible para cada uno de los cuatro puertos.

Asignación de la bahía SPA

Como se menciona en previamente, los puertos físicos son mantenidos por uno de los dos FabricQ Asics. La asignación de los puertos a ASIC se define y no puede estáticamente ser alterada. Además, el SIP-800 PLIM tiene dos PLA Asics. El primer PLA mantiene los puertos 0,1 y 3, los segundos servicios 2, 4 y 5.

La capacidad de ancho de banda de un solo PLA en el SIP-800 PLIM es aproximadamente 24 Gbps. El Switching Capacity de un solo FabricQ ASIC es aproximadamente 62 Mpps.

Si usted puebla el puerto 0,1 y 3 o puertos 2, 4 y 5, la capacidad de ancho de banda del PLA (24 Gbps) se comparte entre los tres de los puertos que restringen el rendimiento de procesamiento general. Puesto que un solo FabricQ cada los servicios esos grupos de puertos, el índice del PAQUETE MÁXIMO del grupo de puertos es 62 Mpps. Es el mejor utilizar los puertos de una forma que obtiene la mayor eficiencia de los PLAs para alcanzar el ancho de banda óptimo.

Colocación sugerida:

	Bay# SPA	Bay# SPA	Bay# SPA	Bay# SPA
Opción 1	0	1	4	5
Opción 2	1	2	3	4

Si usted quiere poblar el indicador luminoso LED amarillo de la placa muestra gravedad menor con más de cuatro SPA, la recomendación es completar una de las opciones enumeradas previamente, que separan las interfaces entre los grupos cuadripolos (0,1 y 3 y 2,4 y 5). Usted debe entonces colocar los módulos siguientes SPA en uno de los puertos abiertos en cualquiera los 0,1 y 3 y 2,4 y 5 grupos de puertos.

DWDM XENPACKs

De la versión 3.2.2 hacia adelante, el DWDM XENPACKs puede ser instalado y proporcionar los módulos **armoniosos de la** óptica. Los requisitos de enfriamiento de tales módulos XENPACK requieren que haya un slot en blanco entre los módulos instalados. Además, si un solo módulo DWDM XENPACK está instalado, un máximo de cuatro puertos puede ser utilizado, incluso si el módulos XENPACK no son dispositivos DWDM. Esto por lo tanto tiene un impacto directo en el FabricQ al PLA a la correlación de puertos. La atención necesita ser prestada a este requisito y se considera en esta tabla.

Colocación sugerida:

	Port- de la óptica	**Port- de la óptica**	**Port- de la óptica**	**Port- de la óptica**
Opción 1 o DWDM XENPACK	0	2	5	7
Opción 2	1	3	4	6

Para 3.2.2 o más adelante o 3.3 instalación, evite el cambio de la asignación de FabricQ. Un modelo más simple de la colocación se puede por lo tanto utilizar para el asiduo y los módulos DWDM XENPACK.

	Port- de la óptica	**Port- de la óptica**	**Port- de la óptica**	**Port- de la óptica**
Opción 1	0	2	4	6
Opción 2	1	3	5	7

Si usted quiere poblar el indicador luminoso LED amarillo de la placa muestra gravedad menor con más de cuatro puertos NON-DWDM XENPACK, la recomendación es completar una de las opciones enumeradas, que separa los módulos de interfaz óptica entre los grupos cuadripolos (0-3 y 4-7). Usted necesita entonces colocar los módulos de interfaz óptica siguientes en uno de los puertos abiertos en los 0-3 o 4-7 grupos de puertos. Si usted utiliza el grupo de puertos 0-3 para el módulo de interfaz óptica #5, los módulos de interfaz óptica #6 se deben colocar en el grupo de puertos 4-7.

Refiera a los módulos DWDM XENPAK para más detalles.

Administración de la Configuración

La configuración adentro IOS-XR se hace con una configuración de dos fases, la configuración es

ingresada por el usuario en la primera etapa. Ésta es la etapa donde solamente la sintaxis de configuración es marcada por el CLI. La configuración ingresada en esta etapa se sabe solamente al proceso del agente de la configuración, por ejemplo, CLI/XML. La configuración no se verifica puesto que no se escribe al servidor del sysdb. La aplicación backend no se notifica y no puede acceder o tener ningún conocimiento de la configuración en esta etapa.

En la segunda etapa, la configuración es confiada explícitamente por el usuario. En esta etapa la configuración se escribe al servidor del sysdb, las aplicaciones backend verifican las configuraciones y las notificaciones son generadas por el sysdb. Usted puede abortar una sesión de la configuración antes de que usted confíe la configuración ingresada en la primera etapa. Así pues, no es seguro asumir que toda la configuración ingresada en la etapa una está confiada siempre en la etapa dos.

Además, la operación y/o la configuración del funcionamiento del router se pueden modificar por los usuarios múltiples durante la etapa una y la etapa dos. Así pues, ninguna prueba del router que funciona con la configuración y/o al estado operacional en la etapa una no pudo ser válida en la etapa dos donde la configuración está confiada realmente.

Sistemas del archivo de configuración

El sistema del archivo de configuración (CF) es un conjunto de los archivos y directorios usados para salvar la configuración del router. Los CF se salvan bajo directorio disk0:/config/, que es el media predeterminado usado en el RP. Los archivos y los directorios en los CF son internos al router y se deben nunca modificar o quitar por el usuario. Esto puede dar lugar a la pérdida o a la corrupción de la configuración y afecta al servicio.

Los CF son checkpointed al espera-RP después de cada cometer. Esto ayuda al coto el archivo de configuración del router después de un fall encima.

Durante el bootup del router, la configuración activa más reciente es aplicada de la base de datos del cometer de la configuración salvada en los CF. No es necesario que el usuario salve manualmente la configuración activa después de cada cometer de la configuración, puesto que esto es hecha automáticamente por el router.

No es recomendable realizar los cambios de configuración mientras que la configuración está siendo aplicada durante el bootup. Si la aplicación de la configuración no es completa, usted ve este mensaje cuando usted abre una sesión al router:

Proceso de la configuración del sistema

La configuración de inicio para este dispositivo está cargando actualmente. Esto puede tardar algunos minutos. Le notifican sobre la realización. No intente por favor configurar de nuevo el dispositivo hasta que este proceso sea completo. En algunos casos pocos probables, puede ser que sea deseable restablecer la configuración del router de un usuario proporcionó al archivo de configuración ASCII en vez de restablecer la configuración activa más reciente de los CF.

Usted puede forzar la aplicación de un archivo de configuración por:

```
using the "-a" option with the boot command. This option forces
    the use of the specified file only for this boot.
```

```
rommon>boot <image> -a <config-file-path>

setting the value of "IOX_CONFIG_FILE" boot variable to the
path of configuration file. This forces the use of the specified file
for all boots while this variable is set.

rommon>IOX_CONFIG_FILE=<config-file-path>
rommon>boot <image>
```

Mientras que usted restablece la configuración del router, una o más el elemento de configuración pudo no poder tomar el efecto. Toda la configuración fallada se guarda en los CF y se mantiene hasta la recarga siguiente.

Usted puede hojear la configuración fallada, dirigir los errores y reaplicar la configuración.

Éstas son algunas extremidades para dirigir la configuración fallada durante el lanzamiento del router.

En IOX, la configuración se puede clasificar como configuración fallada por tres razones:

1. Errores de sintaxis — El analizador de sintaxis genera los errores de sintaxis, que indican generalmente que hay una incompatibilidad con los comandos CLI. Usted debe corregir los errores de sintaxis y reaplicar la configuración.
2. Errores semánticos — Los errores semánticos son generados por los componentes backend cuando el administrador de configuración restablece la configuración durante el lanzamiento del router. Es importante observar que el cfgmgr no es responsable de asegurar la configuración está validado como parte de la configuración corriente. Cfgmgr es simplemente un intermediario y señala solamente cualquier error semántico que los componentes backend generen. Está hasta cada propietario componente backend para analizar la razón del incidente y para determinar la razón del incidente. Los usuarios pueden ejecutar el commands> de la descripción <CLI del modo de configuración para encontrar fácilmente al propietario del verificador componente backend. Por ejemplo, si el BGP 217 del router aparece como configuración fallada, el comando de la descripción muestra que el verificador componente es el componente ipv4-bgp.

```
RP/0/0/CPU0:router#configure terminal
RP/0/0/CPU0:router(config)#describe router bgp 217
The command is defined in bgpv4_cmds.parser

Node 0/0/CPU0 has file bgpv4_cmds.parser for boot package /gsr-os-mbi-3.3.87/mbi12000-rp.vm
from gsr-rout
Package:
    gsr-rout
        gsr-rout V3.3.87[Default]  Routing Package
        Vendor : Cisco Systems
        Desc   : Routing Package
        Build  : Built on Mon Apr  3 16:17:28 UTC 2006
        Source : By ena-view3 in /vws/vpr/mletchwo/cfgmgr_33_bugfix for c2.95.3-p8
        Card(s): RP, DRP, DRPSC
        Restart information:
          Default:
            parallel impacted processes restart
Component:
    ipv4-bgp V[fwd-33/66]  IPv4 Border Gateway Protocol (BGP)

File: bgpv4_cmds.parser


User needs ALL of the following taskids:
```

```
        bgp (READ WRITE)

It will take the following actions:
  Create/Set the configuration item:
         Path: gl/ip-bgp/0xd9/gbl/edm/ord_a/running
        Value: 0x1
Enter the submode:
        bgp
RP/0/0/CPU0:router(config)#
```

3. Aplique los errores — La configuración se ha verificado y se ha validado con éxito como parte de la configuración corriente pero el componente backend no puede poner al día a su estado operacional por alguna razón. La configuración muestra en ambos la configuración que se ejecuta, puesto que fue verificada correctamente, y como configuración fallada debido al error operativo backend. El comando de la **descripción** se puede funcionar con otra vez en el CLI que no pudo ser aplicado para encontrar el componente para aplicar al propietario.Complete estos pasos para hojear y reaplicar la configuración fallada durante los operadores de lanzamiento:Para los operadores R3.2 puede utilizar este procedimiento para reaplicar la configuración fallada:Los operadores pueden utilizar el comando del **inicio fallado de la configuración de la demostración** para hojear la configuración fallada guardada durante el inicio del router.Los operadores deben ejecutar el **noerror del inicio fallado de la configuración de la demostración | clasifíe el comando myfailed.cfg** para salvar la configuración fallada de lanzamiento a un archivo.Los operadores deben ir al **modo de configuración** y a la **carga del** uso**/a los comandos commit** para reaplicar esto configuración fallada:

   ```
   RP/0/0/CPU0:router(config)#load myfailed.cfg
   Loading.
   197 bytes parsed in 1 sec (191)bytes/sec
   RP/0/0/CPU0:router(config)#commit
   ```

   Para los operadores de las imágenes R3.3 puede utilizar este procedimiento actualizado:Los operadores deben utilizar el comando del **inicio fallado de la configuración de la demostración** y el comando del **inicio fallado de la configuración de carga** para hojear y reaplicar cualquier configuración fallada.

```
RP/0/0/CPU0:router#show configuration failed startup
!! CONFIGURATION FAILED DUE TO SYNTAX/AUTHORIZATION ERRORS
telnet vrf default ipv4
server max-servers 5 interface POS0/7/0/3 router static
address-family ipv4 unicast
 0.0.0.0/0 172.18.189.1

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
router bgp 217 !!%
Process did not respond to sysmgr !
RP/0/0/CPU0:router#

RP/0/0/CPU0:router(config)#load configuration failed startup noerror
Loading.
263 bytes parsed in 1 sec (259)bytes/sec
RP/0/0/CPU0:mike3(config-bgp)#show configuration
Building configuration...
telnet vrf default ipv4 server max-servers 5 router static
address-family ipv4 unicast
  0.0.0.0/0 172.18.189.1
 !
!
router bgp 217
```

```
!
end

RP/0/0/CPU0:router(config-bgp)#commit
```

Descargador del corazón

Por abandono IOS-XR escribe un vaciado de memoria al disco duro si una caída de proceso, pero no si el corazón sí mismo causa un crash. Observe que para un sistema del multi-chasis estas funciones están soportadas actualmente solamente para el chasis 0 del linecard. El otro chasis se soporta en una futura versión del software.

Se sugiere que el corazón vacia para los RP y los MSC esté habilitado con el uso de estos configuración en las configuraciones estándar y admin-MODE:

```
RP/0/0/CPU0:router#show configuration failed startup
!! CONFIGURATION FAILED DUE TO SYNTAX/AUTHORIZATION ERRORS
telnet vrf default ipv4
server max-servers 5 interface POS0/7/0/3 router static
address-family ipv4 unicast
 0.0.0.0/0 172.18.189.1

!! CONFIGURATION FAILED DUE TO SEMANTIC ERRORS
router bgp 217 !!%
Process did not respond to sysmgr !
RP/0/0/CPU0:router#

RP/0/0/CPU0:router(config)#load configuration failed startup noerror
Loading.
263 bytes parsed in 1 sec (259)bytes/sec
RP/0/0/CPU0:mike3(config-bgp)#show configuration
Building configuration...
telnet vrf default ipv4 server max-servers 5 router static
address-family ipv4 unicast
  0.0.0.0/0 172.18.189.1
 !
!
router bgp 217
!
end

RP/0/0/CPU0:router(config-bgp)#commit
```

Configuración del volcado del corazón

Esto da lugar a este acontecimiento para una caída del corazón:

1. Un RP causa un crash y un volcado se escribe al disco duro en ese RP en el directorio raíz del disco.
2. Si un MSC causa un crash, un volcado se escribe al disco duro de RP0 en el directorio raíz del disco.

Esto no tiene ningún impacto el los tiempos de la Conmutación por falla RP puesto que la expedición directa (NSF) se configura para los Routing Protocol. Puede tardar algunos minutos adicionales para que el RP causado un crash o el linecard esté disponible otra vez después de que siga una caída mientras que escribe la base.

Un ejemplo de la adición de esta configuración al estándar y a la configuración de modo admin se muestra aquí. Observe que la configuración de modo admin requiere los DRP ser utilizada.

Esta salida muestra un ejemplo de configuración del volcado del corazón:

```
RP/0/RP0/CPU0:crs1#configure
RP/0/RP0/CPU0:crs1(config)#exception kernel memory kernel filepat$
RP/0/RP0/CPU0:crs1(config)#exception dump-tftp-route port 0 host-$
RP/0/RP0/CPU0:crs1(config)#commit
RP/0/RP0/CPU0:crs1(config)#
RP/0/RP0/CPU0:crs1#admin
RP/0/RP0/CPU0:crs1(admin)#configure
Session                   Line        User      Date                      Lock
00000201-000bb0db-00000000  snmp        hfr-owne  Wed Apr  5 10:14:44 2006
RP/0/RP0/CPU0:crs1(admin-config)#exception kernel memory kernel f$
RP/0/RP0/CPU0:crs1(admin-config)#exception dump-tftp-route port 0$
RP/0/RP0/CPU0:crs1(admin-config)#commit
RP/0/RP0/CPU0:crs1(admin-config)#
RP/0/RP0/CPU0:crs1(admin)#
```

Security

LPTS

Del paquete local de transporte de los servicios (LPTS) de las manijas paquetes destinados localmente. LPTS se hace de diversos diversos componentes.

1. El principal se llama el proceso del árbitro del puerto. Escucha las peticiones del socket de diversos procesos de protocolo, por ejemplo, BGP, IS-IS y no pierde de vista toda la información obligatoria para esos procesos. Por ejemplo, si un proceso BGP escucha en el número de socket 179, el PA obtiene esa información de los procesos BGP, y después asigna un atascamiento a ese proceso en un IFIB.
2. El IFIB, es otro componente del proceso LPTS. Ayuda a guardar un directorio de donde está un proceso que está escuchando un atascamiento específico del puerto. El IFIB es generado por el proceso del árbitro del puerto y guardado con el árbitro del puerto. Entonces genera los subconjuntos múltiples de esta información.El primer subconjunto es una rebanada del IFIB. Esta rebanada se puede asociar al protocolo del IPv4 y así sucesivamente. Las rebanadas entonces se envían para apropiarse de los administradores del flujo, que entonces utilizan la rebanada IFIB para remitir el paquete al proceso apropiado.El segundo subconjunto es un PRE-IFIB, permite que el LC remita el paquete al proceso apropiado si solamente un proceso existe o a un administrador apropiado del flujo.
3. Los administradores del flujo ayudan más lejos a distribuir los paquetes si la mirada para arriba es no trivial, por ejemplo, los procesos múltiples para el BGP. Cada administrador del flujo tiene una rebanada o las rebanadas múltiples del IFIB y correctamente adelante de los paquetes a los procesos apropiados asociados a la rebanada del IFIB.
4. Si una entrada no se define para el puerto destino entonces puede ser caída o ser remitida al administrador del flujo. Un paquete se remite sin el puerto asociado si hay una directiva asociada para el puerto. Las ayudas del administrador del flujo entonces generan una nueva entrada de la sesión.

¿Cómo se remite un paquete interno?

Hay dos tipos de flujos, los flujos de la capa 2 (HDLC, PPP) y acoda 4 flujos ICMP/PING y la encaminamiento fluye.

1. Capa 2 HDLC/PPP — Estos paquetes son identificados por el Protocol Identifier y enviados directamente a las colas de administración del tráfico CPU en el rociador. Los paquetes del protocolo de la capa 2 consiguen prioritarios y después son cogidos por el CPU (vía Squid) y procesados. Por lo tanto el Keepalives para la capa 2 se responde directamente vía al LC vía el CPU. Esto evita la necesidad de entrar al RP para las respuestas y los juegos con el tema de la administración de la interfaz distribuida.
2. ICMP (paquetes de la capa 4) se recibe en el LC y se envían vía las operaciones de búsqueda con el IFBI en las colas de administración del tráfico CPU en el rociador. Estos paquetes después se envían al CPU (vía Squid) y se procesan. La respuesta entonces se envía a través de las colas de administración del tráfico de la salida del rociador para ser remitida a través de la tela. Esto es en caso de que otra aplicación también necesite la información (replicada a través de la tela). Una vez a través de la tela el paquete se destina a la salida apropiada LC y a través de la cola apropiada de la esponja y del control.
3. Ruteando los flujos se miran para arriba en el IFIB y entonces enviado a las colas de modelado de salida (8000 colas de administración del tráfico) uno de los cuales es reservado para los paquetes de control. Esto es no una cola modelada y se mantiene simplemente cada vez que es lleno. – prioritario. El paquete entonces es enviado con la tela en las colas de alta prioridad en un conjunto de las colas de administración del tráfico CPU en la esponja (similar a Squid hace cola en el rociador), y entonces los procesos por el proceso apropiado, el administrador del flujo o el proceso real. Una respuesta se devuelve con la esponja del linecard de la salida y entonces hacia fuera el linecard. La esponja de la salida LC tiene una cola especial puesta a un lado para manejar los paquetes de control. Las colas de administración del tráfico en la esponja están partidas en prioritario, control y los paquetes de prioridad baja, por la base del puerto de egreso.
4. El PSE tiene un conjunto de policers que se configura para la tarifa que limita la capa 4, la capa 2 y los paquetes de ruteo. Éstos se preestablecen y cambian para ser usuario configurable más adelante.

Uno del problema más común con LPTS es los paquetes se caen que, cuando usted intenta hacer ping al router. El policers LPTS es generalmente tarifa que limita estos paquetes. Éste es el caso para confirmar:

```
RP/0/RP0/CPU0:ss01-crs-1_P1#ping 192.168.3.14 size 8000 count 100
Type escape sequence to abort.
Sending 100, 8000-byte ICMP Echos to 192.168.3.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!
!!!!!!!!!!!!!!!.!!!!!!!!!!!!!
Success rate is 97 percent (97/100), round-trip min/avg/max = 1/2/5 ms
RP/0/RP0/CPU0:ss01-crs-1_P1#show lpts pifib hardware entry statistics location 0/5/CPU0 | excl
0/0

* - Vital; L4 - Layer4 Protocol; Intf - Interface;
DestAddr - Destination Fabric Address;
na - Not Applicable or Not Available

Local, Remote Address.Port          L4    Intf         DestAddr     Pkts/Drops
---------------------------------- ----- ------------ ------------ --- any
any   any          Punt       100/3
224.0.0.5 any                       any   PO0/5/1/0    0x3e         4/0
224.0.0.5 any                       any   PO0/5/1/1    0x3e         4/0
```

```
<further output elided>
```

IPSec

Los paquetes del IP son intrínsecamente inseguros. El IPSec es un método usado para proteger los paquetes del IP. El IPSec del CRS-1 se implementa en el trayecto de reenvío del software, por lo tanto sesión IPSec se termina en el RP/DRP. Un número total de 500 sesiones del IPSec por el CRS-1 se soporta. El número depende de la velocidad CPU y de los recursos afectados un aparato. No hay limitación del software a esto, sólo el tráfico local-originado y local-terminado en el RP es elegible para la dirección del IPSec. El modo de transporte de IPSec o el modo túnel puede ser utilizado para el tipo de tráfico, aunque el anterior es preferido debido a menos gastos indirectos en el Procesamiento IPSec.

R3.3.0 soporta el cifrado del BGP y de OSPFv3 sobre el IPSec.

Refiera a la guía de configuración de la seguridad del sistema del Cisco IOS XR para más información sobre cómo implementar el IPSec.

Note: El IPSec requiere la empanada crypto, por ejemplo, hfr-k9sec-p.pie-3.3.1.

Fuera de la banda

Consola y acceso AUX

El CRS-1 RP/SCs tiene una consola y puerto auxiliar disponible para fuera de los fines de administración de la banda, así como un puerto de Ethernet de administración para fuera de banda vía el IP.

La consola y puerto auxiliar de cada RP/SCGE, dos por los chasis, se puede conectar con un servidor de la consola. Esto significa que el sistema del chasis único requiere cuatro puertos de la consola, y los sistemas del multi-chasis requieran 12 puertos más dos puertos más para los motores del supervisor en el Catalyst 6504-E.

La conexión del puerto auxiliar es importante puesto que proporciona el acceso IOS-XR al corazón y puede permitir la recuperación del sistema cuando esto no es posible vía el puerto de la consola. El acceso vía el puerto auxiliar está solamente disponible para los usuarios localmente definido en el sistema, y solamente cuando el usuario tiene acceso del raíz-sistema o del nivel del Cisco-soporte. Además el usuario debe hacer una **contraseña secreta** definir.

Acceso de Terminal virtual

Telnet y el Secure Shell (SSH) se pueden utilizar para alcanzar el CRS-1 vía los puertos VTY. Por abandono ambos se inhabilitan, y el usuario necesita habilitarlos explícitamente.

Note: El IPSec requiere la empanada crypto, por ejemplo, hfr-k9sec-p.pie-3.3.1.

Primero genere las claves RSA y DSA tal y como se muestra en de este ejemplo para habilitar SSH:

```
RP/0/RP1/CPU0:Crs-1#crypto key zeroize dsa
% Found no keys in configuration.
```

```
RP/0/RP1/CPU0:Crs-1#crypto key zeroize rsa
% Found no keys in configuration.

RP/0/RP1/CPU0:Crs-1#crypto key generate rsa general-keys
The name for the keys will be: the_default
  Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keypair.
  Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [1024]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

RP/0/RP1/CPU0:Crs-1#crypto key generate dsa
The name for the keys will be: the_default
  Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits. Choosing
a key modulus
How many bits in the modulus [1024]:
Generating DSA keys ...
Done w/ crypto generate keypair
[OK]

!--- VTY access via SSH & telnet can be configured as shown here. vty-pool default 0 4 ssh
server ! line default secret cisco users group root-system users group cisco-support exec-
timeout 30 0 transport input telnet ssh ! ! telnet ipv4 server
```

Información Relacionada

- Soporte del Routers
- Soporte Técnico y Documentación - Cisco Systems