Dan Beninson

Instituto de Tecnología Nuclear

INSTRUMENTACIÓN Y CONTROL DE REACTORES DE POTENCIA: ESTUDIO DE PROTOCOLOS DE REDES PARA LA OBTENCIÓN, TRATAMIENTO Y PRESENTACIÓN DE LA INFORMACIÓN

CARRERA: ESPECIALIZACIÓN EN REACTORES NUCLEARES Y SU CICLO DE COMBUSTIBLE

Alumno: Ing. Alfredo Dupont
Director: Ing. Juan Carlos Dezzutti
Co-director: Mgr. Ing. Luis María Pizarro

CNEA

UNSAM
UNIVERSIDAD NACIONAL DE SAN MARTÍN

Índice

Abreviaturas

ARP ..... Adress Resolution Protocol
BID ..... Bridge Identificator
CPU ..... Central Processing Unit
CSMA/CD ..... Carrier Sense Multiple Access / Collision Detection
IEEE ..... Institute of Electrical and Electronics Engineers
IP ..... Internet Protocol
ISO ..... International Organization for Standarization.
LLC ..... Logical Link Control
MAC ..... Media Access Control
NIC ..... Network Interface Card
OSI ..... Open System Interconnection
PLC ..... Programmable Logic Controler
PPP ..... Point to Point Protocol
RNRP ..... Redundant Network Routing Protocol
RSTP ..... Rapid Spanning Tree Protocol
STP ..... Spanning Tree Protocol
TCP ..... Transmission Control Protocol
TTL ..... Time To Live
UDP ..... User Datagram Protocol

Agradecimientos:

A mi director, Ing. Juan Carlos Dezzutti por su apoyo.
A mi co-director, Mgr. Ing. Luis María Pizarro por su acompañamiento constante en este trabajo.
Al Ing. Pablo Juárez del Valle por facilitarme su software y las muchas sugerencias y observaciones aportadas.
A mi familia por su paciencia.

Resumen

Se realizó la medición de tiempos de reconfiguración de dos protocolos de manejo de redundancia usados en redes de control y supervisión Ethernet de sistemas de control distribuidos, candidatos a ser utilizados en el control de plantas nucleares de potencia: RSTP (Rapid Spanning Tree Protocol) y RNRP (Redundant Network Routing Protocol). El primero es abierto y el segundo propietario de la firma ABB.

1 Introducción

1.1 Sistemas de control

Se puede considerar a un sistema de control como un conjunto de elementos que intervienen sobre un proceso para mantenerlo dentro de ciertos parámetros que se fijan como valores de consigna. El tratamiento de los sistemas dinámicos utilizando la disciplina llamada Teoría de Control se aplica tanto a procesos mecánicos y electrónicos, como también a biológicos y sociales.

Un sistema de control en el que la salida no tiene efecto sobre la acción de control se denomina **sistema de control de lazo abierto**. De esta forma, la salida no se compara con la entrada de referencia y por lo tanto a cada entrada de referencia corresponde una condición de operación fija. La precisión del sistema depende de la calibración y, si existen perturbaciones grandes, el sistema puede no cumplir con la función asignada *(fig. 1)*.

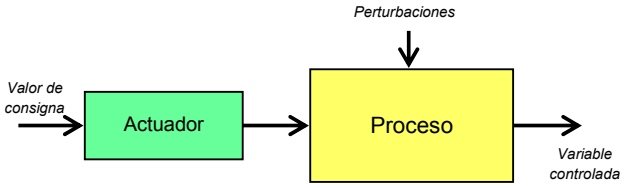


fig. 1 – Control de lazo abierto

Los **sistemas de control de lazo cerrado** son aquellos en los que la salida es realimentada a la entrada. Se realiza una comparación (diferencia) de la señal de salida con el valor de consigna y la señal resultante (señal de error) entra al controlador que realiza las acciones necesarias para reducir este error y llevar al sistema al valor deseado. Suele llamarse también a estos sistemas como *sistemas de control realimentado* o *sistemas de control automático (fig. 2)*. (1)

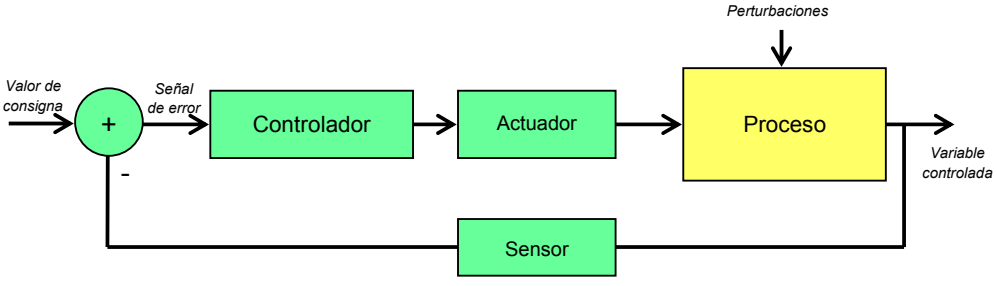


fig. 2 – Control de lazo cerrado

Si bien el sistema es *de control automático*, existe un lazo de realimentación entre salida y entrada que no está incluido en la *fig. 2*: es el constituido por el ***operador***. (2)

En la *fig. 3* las líneas de punto indican observación por parte del operador de planta y las líneas llenas posibilidad de actuación: por ejemplo, es el operador quien, en algunos casos, puede fijar el valor de

consigna (*setpoint*) y puede actuar manualmente sobre el actuador al observar que el proceso se aparta de los valores deseados.

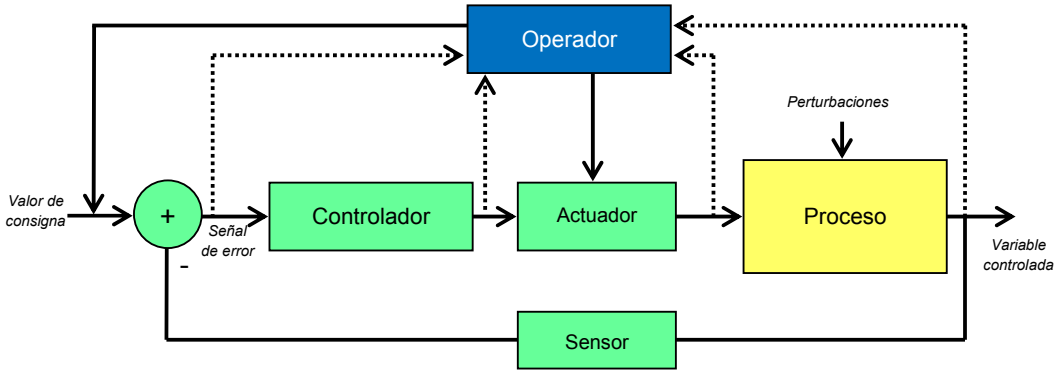


fig. 3 – Control de lazo cerrado incluyendo al aperador

En las figuras anteriores se ha mostrado un sistema con una entrada y una salida. En una planta compleja las entradas y salidas llegan a varios miles y corresponden a cientos de procesos diferentes.

Cabe aclarar que no todos los procesos en una planta tienen lazos de control realimentado automático, también existen lazos de control *a lazo abierto*. El operador puede determinar el estado de estos lazos abiertos a través de un sistema de supervisión de manera que, incluyendo al operador, estos lazos son también cerrados.

Hay dos maneras de manejar las miles de señales de una planta: de manera centralizada o distribuida.

El **control centralizado** se basa en la idea de que un solo controlador maneja todos los procesos de la planta. Un ejemplo de central nuclear que implementa control centralizado es el diseño Candu 6 de Embalse. En este caso es una computadora redundada la que realiza el control de toda la planta *(fig. 4)*.

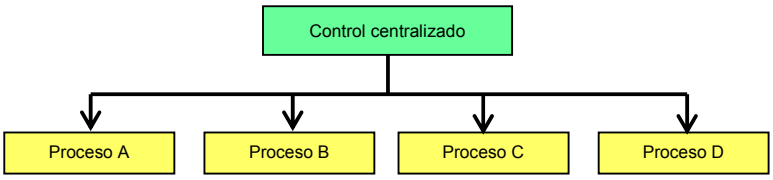


fig. 4 – Control Centralizado

El desarrollo de la tecnología en diversas áreas como el de las redes de datos, los microprocesadores, microcontroladores, PLCs más potentes, bases de datos y aplicaciones cliente servidor ha contribuido a la aparición de otra filosofía de control: el control distribuido.

La *fig. 5* muestra un esquema de **control distribuido** donde cada dispositivo de control toma las decisiones de control de uno o varios procesos. Los dispositivos de control tienen comunicación entre sí a través de redes de datos (lo que permite el intercambio de información y la sincronización), pero cada dispositivo es quien controla el o los procesos que se le han asignado, de manera que la falla de un controlador no imposibilita proseguir con los procesos controlados por los demás.

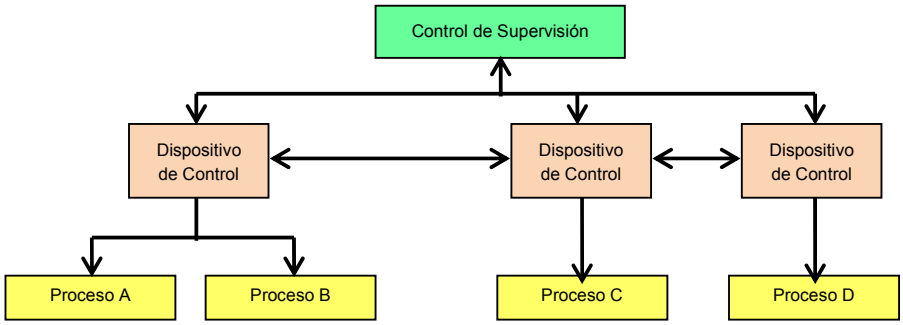


fig. 5 – Control distribuido

1.2 Las redes de comunicación de un sistema distribuido

El desarrollo del control distribuido en la industria va paralelo al de las comunicaciones digitales. Las líneas que interconectan los diferentes elementos de un sistema de control distribuido son redes de datos industriales. En éstas, por cada enlace circulan datos digitales en unidades denominadas paquetes conformados en base a diversas reglas denominadas protocolos.

La utilización de redes simplifica el cableado ya que muchas señales pueden multiplexarse en un único enlace, pero, como contrapartida, la falla de un único enlace puede producir la pérdida de muchas señales a la vez.

La *fig. 3* muestra de manera esquemática la acción del operador en un lazo de una variable de entrada y una de salida. En la *fig. 6* se muestra la acción del operador para el caso de una planta que utiliza control distribuido. Se observa que si bien el control automático de los procesos se lleva a cabo por los dispositivos de control, la supervisión (y por ende el control global) es ejercido por el operador. La información de planta que llega al nivel de supervisión como así también las acciones que el operador realiza sobre la planta constituyen datos que viajan por las redes digitales que conectan el *Control de supervisión* con los distintos *Dispositivos de control.*

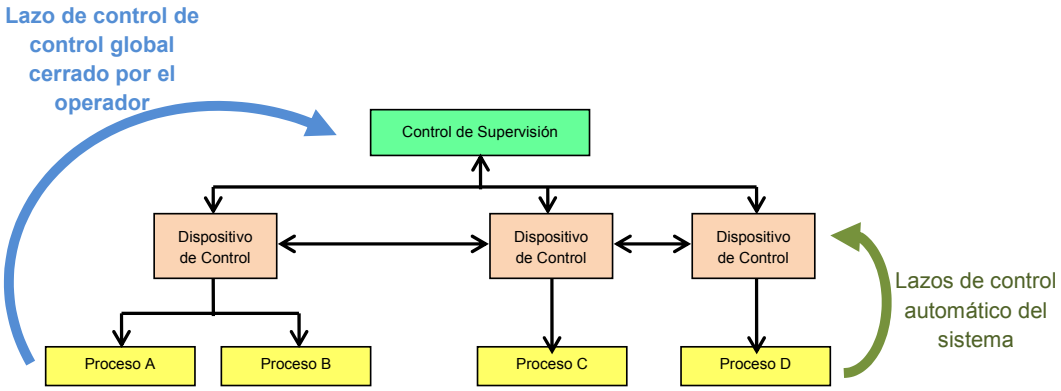


fig. 6 – El operador cierra el lazo de control global de la planta

Es por esto que se requiere que las redes de datos que constituyen el sistema de control distribuido a aplicar en una central nuclear reúnan condiciones de disponibilidad muy altas. Para alcanzar estas condiciones se redundan redes y dispositivos utilizando algunas de las configuraciones descriptas más adelante. (3) (4)

Así como ciertos protocolos rigen las comunicaciones en las redes de datos del sistema de control, otros manejan la redundancia, es decir, son conjuntos de reglas que determinan en qué condiciones se considerará en falla un enlace y realizan las acciones necesarias para que se utilice el enlace alternativo.

1.3 Objetivos del presente trabajo

El propósito de este trabajo es analizar dos protocolos de gestión de redundancia teniendo como objetivo verificar su aptitud para ser usados en una planta nuclear de generación eléctrica. Se consideran mediciones en los tiempos de reconfiguración de un protocolo abierto (RSTP) y otro propietario (RNRP). Ambos trabajan sobre la tecnología Ethernet que es utilizada por varios fabricantes de sistemas de control para las redes de supervisión y control.

Antes de la presentación de los resultados de laboratorio y las conclusiones a las que se ha arribado, y sobre todo para el entendimiento de las mismas, se introduce brevemente el modelo de referencia OSI, la arquitectura de las redes de un sistema de control distribuido típico de una planta nuclear moderna, los tipos de redundancia y una descripción de Ethernet y de los protocolos redundantes estudiados.

2 El modelo de referencia OSI

El modelo OSI (Open System Interconnection) es un modelo descriptivo creado en 1984 por ISO. Proporciona a los fabricantes un conjunto de estándares que aseguran una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI.

Consta de siete capas numeradas, cada una de las cuales ilustra una función de red específica. La *fig. 7* muestra cada una de estas capas con su relación en redes de control. (4) (5)

	Capa OSI	Tareas típicas asignadas	Dispositivo de red utilizado en esa capa
7	Aplicación	Suministra servicios de red a los procesos de aplicaciones	
6	Presentación	Representación de datos. Compresión de datos. Conversión.	
5	Sesión	Sincronización. Estructura de diálogo.	
4	Transporte	Conexiones de extremo a extremo. Transferencia de datos fiable.	
3	Red	Direcciones lógicas. Empaquetado y determinación de la mejor ruta	Router
2	Enlace de datos	Mecanismo de acceso al medio. Estructuración en tramas. Prioridad.	Switch
1	Física	Definición de la interfase física (cables, conectores, voltajes, velocidades de transmisión de datos	Hub

fig. 7 – Capas del modelo OSI

La división en capas permite obtener las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

3 Arquitectura de control distribuido de una central nuclear moderna

La *fig. 8* muestra una posible arquitectura de control de una central nuclear moderna. Se observa en la figura la estratificación de las redes de toda la planta: red de campo, de control y de supervisión. Puede existir o no una conexión de la red de supervisión con la red empresarial de la planta. (6)

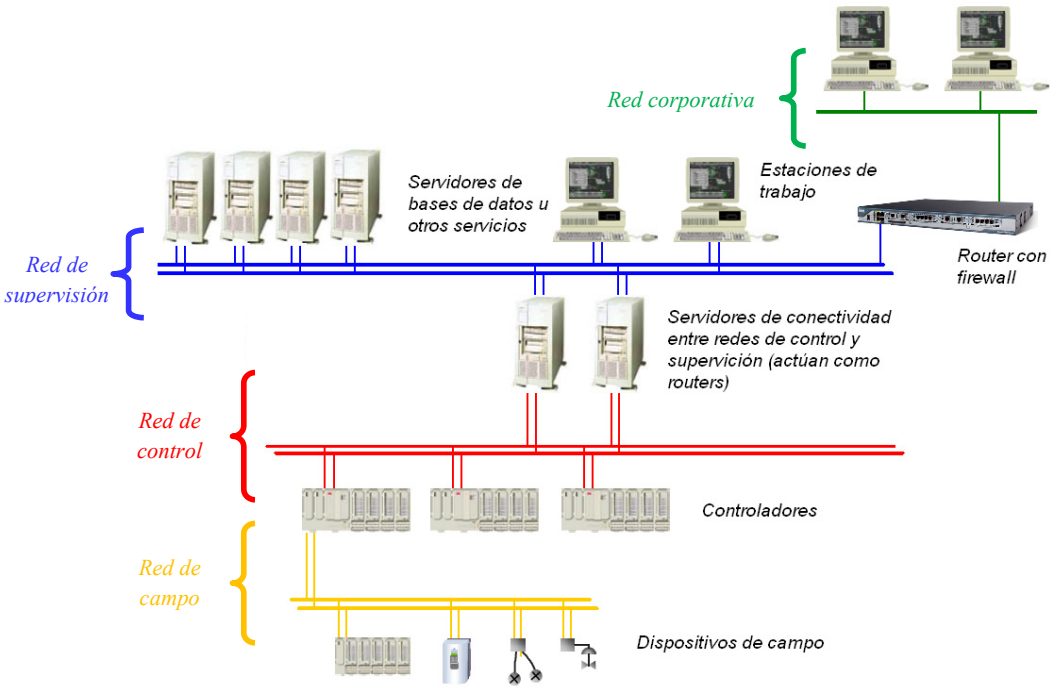


fig. 8 - Arquitectura del sistema de control distribuido de una central nuclear moderna

3.1 Red de campo

Típicamente es una red digital, bidireccional, multipunto, montada sobre un bus serie que conecta dispositivos de campo como sensores y actuadores con los dispositivos de control. En muchos casos estos buses sustituyen los tradicionales enlaces punto a punto de 4-20 mA. Los elementos de campo compatibles con algunos de los buses más utilizados permiten funciones como autodiagnóstico y configuración remota centralizada.

Debido a que en muchos casos se requiere comunicación en tiempo real, estas redes implementan generalmente un esquema de tres capas del modelo OSI: física, enlace de datos y aplicación.

El control automático de la planta es realizado por los dispositivos de control, tomando datos de los sensores e interviniendo, a través de los actuadores, sobre los procesos de la planta. Ya que la red de campo interconecta estos dispositivos, debe tener una alta disponibilidad.

En algunas circunstancias los bucles de corriente de 4-20 mA se mantienen hasta dispositivos concentradores llamados cabezales o "periferia descentralizada" que multiplexan un gran número de señales hacia un bus de campo.

Ejemplos de buses de campo son: Profibus DP y Fieldbus Foundation.

El presente trabajo no se focaliza en este nivel de redes.

3.2 Red de control

Esta red interconecta las distintas unidades que realizan el control de la planta y los servidores de datos que en algunos casos sirven de nexo con la red de supervisión.

Si bien esta red no tiene exigencias tan elevadas en cuanto a disponibilidad como la red de campo puesto que el control de los procesos se realiza por debajo de ella, es también una red de alta disponibilidad. Las soluciones de diversos fabricantes tienden a utilizar la tecnología Ethernet estándar en este nivel, lo que permite emplear, en la mayoría de los casos, dispositivos estándar (llamados en la jerga "of the shelf") y un cableado muy semejante al de las redes de IT (las redes locales de computadoras).

Ya que las redes de control son redes de alta disponibilidad, se recurre en este nivel a la redundancia y es aquí donde se aplican los protocolos estudiados en este trabajo.

3.3 Red de supervisión

La red de supervisión interconecta los diferentes servidores de la planta (servidores de conexión con la red de control, servidores históricos –bases de datos- y otros que requiera el sistema) y las estaciones de operación e ingeniería. Generalmente esta red está diseñada sobre tecnología Ethernet.

Las estaciones de operación son aquellas computadoras en las que los operadores pueden supervisar los parámetros de la planta y tomar acciones sobre la misma. Las estaciones de ingeniería están pensadas para la configuración y monitoreo del sistema de control, incluyendo sus redes de comunicaciones.

La separación de las redes de control y supervisión obedece a varias razones:

- La naturaleza de los tráficos en ambas redes es diferente: la red de control maneja mensajes pequeños y generalmente igualmente espaciados, la red de supervisión soporta, además, paquetes de mayor tamaño y por ráfagas. Es por ello que la red de control está preparada para el tráfico que se espera en ella por el uso de protocolos específicos.
- Aislación de fallas: cualquier inconveniente que lleve a un aumento desmedido del tráfico en la red de supervisión y que pudiera afectar o incluso inutilizar el medio de comunicación de supervisión no afectará a la red de control ya que entre ambas se encuentran dispositivos que funcionan como routers, filtrando estos tráficos. De esta manera, ante este tipo de anomalías en la red de supervisión, la red de control seguirá operando.
- Si existe segregación de las redes de control y de supervisión, no es necesario mantener tablas de enrutamiento tan grandes, ya que el número de dispositivos se encuentra dividido y así se utilizan menos recursos en los nodos.

3.4 Red corporativa

La conexión de la red de supervisión con esta red puede no existir en una instalación particular. Bajo el nombre *red de empresa* se han colocado las redes que tengan relación con la coordinación de planta y planificación.

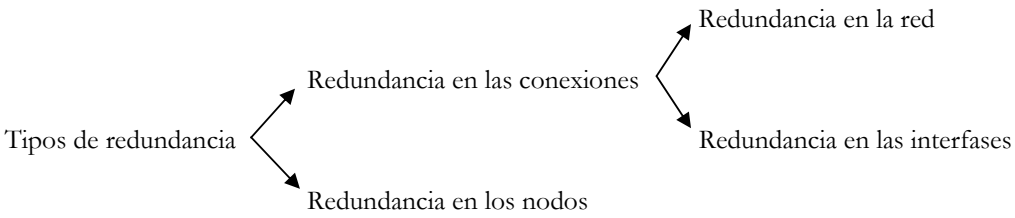
En el caso de ser implementada, algunos parámetros de la base de datos de históricos de la red de supervisión podrían estar disponibles en este nivel. Esta implementación implica un acceso de sólo lectura a los valores y una estricta política de seguridad.

La tecnología utilizada en este nivel es siempre Ethernet.

4 Redundancia

4.1 Tipos de redundancia en un sistema de control

Las exigencias de disponibilidad en la redes de datos digitales de un sistema de control llevan a considerar formas que aumentan la disponibilidad de tal sistema. Una forma de aumentarla es contar con sistemas redundantes, es decir, tener dispositivos o líneas de comunicación secundarios con los cuales se pueda cumplir la función de comunicación en caso de falla de los primarios. Los diferentes tipos de redundancia que se consideran son: (7) (8)



4.1.1 Redundancia en las conexiones

En este tipo de redundancia, se duplica la conexión del dispositivo final que realiza la tarea dentro del sistema de control. Una parte o todo el camino que recorren los datos tiene un camino alternativo, o bien la conexión con ese camino está redundada; pero el dispositivo es único y constituye en sí mismo un único punto de falla. La redundancia en las conexiones puede realizarse con una o ambas de las siguientes alternativas: redundancia en la red y/o redundancia en las interfases.

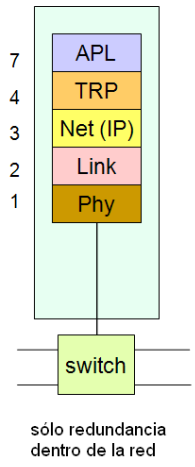


fig. 9 – Redundancia en la red

La **redundancia en la red** brinda caminos alternativos cuando ocurre la falla de un enlace o dispositivo activo de red, pero los nodos finales están conectados a la red mediante un solo camino. Un ejemplo típico es una red anillo con un único enlace de unión a la red por cada dispositivo. La *fig. 9* muestra un nodo simple con interfase simple conectado a una red redundada. En este caso los dispositivos que implementan el algoritmo que permite la reconfiguración ante fallas de la red son los propios dispositivos activos de la misma (en el caso de Ethernet, como veremos más adelante, estos dispositivos se denominan switches).

La **redundancia en las interfases** requiere que cada dispositivo final tenga dos conexiones a la red. Según la arquitectura de la misma, ambas conexiones pueden pertenecer a redes completamente independientes o formar parte de una sola red que tiene enlaces múltiples. Como se observa en la *fig. 10* pueden existir diferentes implementaciones de la redundancia en las interfases, dependiendo de cuántas capas del modelo OSI serán duplicadas y, por ende, qué direcciones se utilizarán para referenciar a cada una de las interfases del nodo.

4.1.2 Redundancia en los nodos

En este caso, el dispositivo final que realiza la tarea dentro del sistema de control está redundado, es decir, existe otro dispositivo idéntico que puede realizar la función asignada al primero en caso de falla de éste.

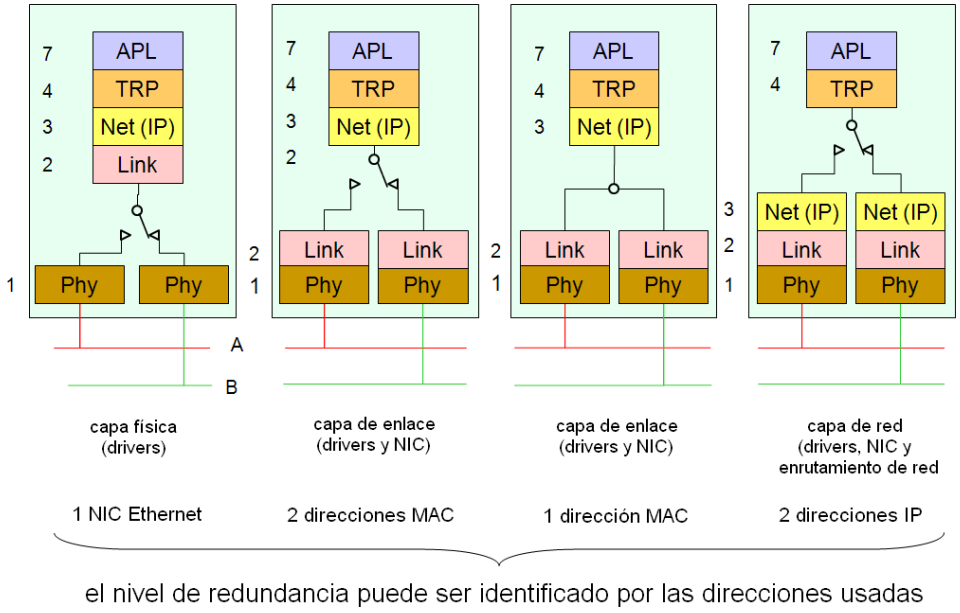


fig. 10 – Redundancia en las conexiones

Dependiendo del grado de disponibilidad que se desee alcanzar, y de consideraciones de costo/beneficio, se implementarán uno o varios de los tipos de redundancia indicados anteriormente, como se muestra a continuación:

Sin redundancia: Los nodos son simples y están interconectados por una única red. Cualquier falla simple dejará al dispositivo involucrado fuera de servicio.

fig. 11 – Sin redundancia

Redundancia en la red: Soporta fallas en los enlaces de los dispositivos activos de la red. No soporta fallas de los propios dispositivos activos de red, ya que los enlaces de los nodos son simples y al entrar en falla el elemento al que está conectado, se perderá la conexión a la red al no tener un camino alternativo. En el ejemplo mostrado en la *fig. 12* la red tiene una topología de anillo.

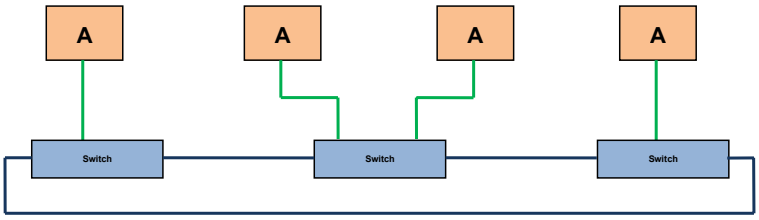


fig. 12 – Redundancia en la red

Redundancia en las interfases y en la red: Puede soportar fallas en una interfase de un nodo, en uno de los enlaces del nodo a la red o de un dispositivo activo de red. En la *fig. 13* se ha generalizado dos redes independientes y no se muestran dispositivos activos.

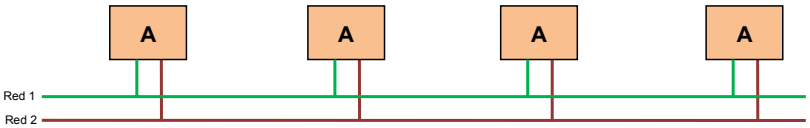


fig. 13 – Redundancia en las interfases y en la red

Redundancia en los nodos, redundancia en la red, interfases simples: Puede soportar fallas de nodo **o** de red. Existe un elemento conmutador que pasa a activo al dispositivo B en caso de falla del A. *(fig. 14)*

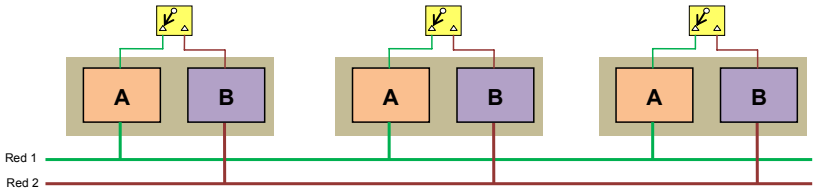


fig. 14 – Redundancia en los nodos y en la red, interfases simples

Redundancia en los nodos y redundancia en la red, interfases redundadas: Se tiene redundancia completa (en los nodos y las conexiones). Puede soportar fallas de nodo **y** de red.

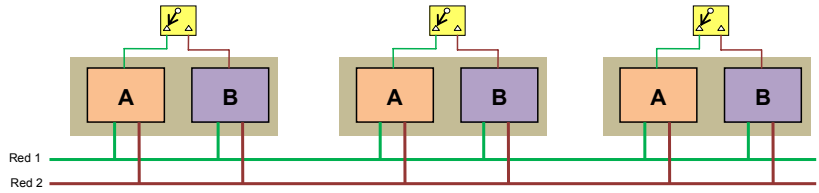


fig. 15 – Redundancia en los nodos y en las conexiones

Generalmente, en los casos de redundancia de nodo *(fig. 15 y fig. 16)*, los conmutadores toman la decisión de cambiar a B basándose en una señal que los dispositivos intercambian por una línea auxiliar o por la misma red indicando su estado de funcionamiento. Esta señal es llamada *Señal de Heartbeat* ya que le permite al nodo saber en cada momento si su contraparte se encuentra "viva".

Sólo uno de los nodos redundados A o B pueden tener el control. Si A lo tiene, B igualmente se encuentra en un estado activo, sensando entradas, realizando cálculos y comparando las salidas calculadas con los datos que A coloca en sus salidas. Se dice, entonces, que B se encuentra en *hot standby*.

4.2 Métodos de redundancia

4.2.1 Redundancia Dinámica

También llamada redundancia *standby*. Los dispositivos redundados permanecen inactivos o realizan otras actividades mientras su contraparte activa se encarga de realizar la función. Al entrar en falla un componente, el elemento correspondiente inactivo pasa a actividad *luego de un tiempo de reconfiguración*. Este tiempo es el que insume detectar la falla y activar el elemento redundante.

El nombre de redundancia dinámica indica que se deben realizar acciones para lograr que se restablezca la función luego de una falla.

4.2.2 Redundancia Estática

Ambas redundancias participan en la función. La planta puede utilizar cualquiera de los dispositivos redundados en cualquier momento, dependiendo de alguna política, como podría ser enviar por ambas redes redundadas todos los datos a transferir.

En la redundancia estática no existe *tiempo de reconfiguración*, pero el sistema resulta más complejo y requiere el manejo de políticas de sincronización: en el ejemplo anterior, los nodos receptores deben poder manejar la duplicación y secuenciación de los paquetes que se envían duplicados por ambas redes. [7]

5 Redes Ethernet

Ethernet es una familia de tecnologías para networking que actualmente permite transmisiones de datos sobre cable de cobre de par trenzado o fibra óptica a velocidades de 10, 100, 1000 y 10000 Mbps. [5]

El estándar que describe Ethernet es el IEEE 802.3. Las capacidades añadidas en cuanto a velocidades y medios se denotan mediante una o dos letras agregadas (Ej. 802.3u, 802.3ab).

Ethernet opera en la subcapa inferior de la capa 2 del modelo OSI, llamada subcapa MAC (Media Access Control) y en la capa física (capa 1) *(fig. 16)*.

El direccionamiento de cada uno de los dispositivos en Ethernet se realiza mediante una dirección MAC (también llamada dirección física) la cual es un número único de 48 bits, cuyos primeros 24 bits denotan al fabricante (identificador exclusivo de organización) y los 24 siguientes identifican unívocamente al dispositivo.

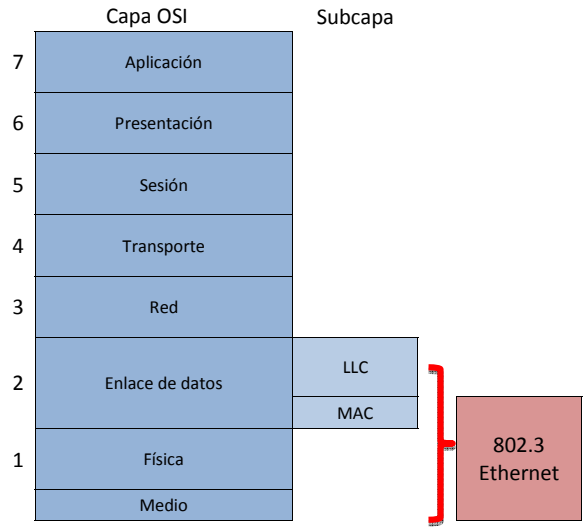


fig. 16 – Ubicación de Ethernet en el modelo OSI

5.1 Control de acceso al medio

El control de acceso al medio en una red indica la manera en que los dispositivos utilizarán el canal de transmisión para hacer un uso eficiente de él. El método de acceso al medio utilizado por Ethernet se denomina CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

CSMA /CD funciona de la siguiente manera: cuando un dispositivo tiene datos para transmitir, escucha en el canal compartido. Si el canal está ocupado, espera un tiempo aleatorio antes de volver a intentar. Si no hay transmisiones en el canal, envía la trama y, simultáneamente, escucha. Existe la posibilidad de que otro dispositivo intente transmitir al mismo tiempo, lo que provoca una colisión y ambas tramas transmitidas se corrompen. En tal caso, se sigue transmitiendo un tiempo más para que todos los dispositivos del canal identifiquen la colisión. Inmediatamente cada uno de los dos dispositivos involucrados invocan un algoritmo de postergación. Al vencer el tiempo de postergación cada dispositivo intentará nuevamente.

Un segmento físico de una red Ethernet donde las tramas pueden colisionar, es decir interferir unas con otras, se llama *dominio de colisión*.

En Ethernet ningún dispositivo tiene prioridad de transmisión; además pueden ocurrir varias postergaciones antes de realizar un envío de trama exitoso, por lo tanto no puede determinarse exactamente cuándo se podrá transmitir. Esto implica que Ethernet es una tecnología de redes no determinística.

Un nodo puede direccionar información hacia otros nodos de 3 maneras:

- Unicast: Envío de información desde un emisor a un único receptor.
- Multicast: Envío de información desde un emisor a un grupo de receptores.
- Broadcast: Envío de información desde un emisor a todos los receptores dentro de la red.

5.2 Dispositivos de red

5.2.1 Hubs

Un hub es un dispositivo repetidor de múltiples puertos que, al recibir una trama en uno de sus puertos, lo replica -luego de realizar amplificaciones de señal y tareas de sincronización- por todos los puertos, excepto por el que ingresó al dispositivo. Los hubs trabajan en la capa física del modelo OSI y no toman decisiones de red. Estos dispositivos no dividen dominios de colisión, es decir, todos sus puertos forman parte del mismo dominio.

5.2.2 Switches

Un switch es un dispositivo de networking que funciona en la capa 2 del modelo OSI. El switch aprende la dirección MAC de cada dispositivo conectado a sus puertos de conexión tomando la dirección de origen de las tramas recibidas por cada puerto y la agrega a una tabla. Se relaciona de esta manera la dirección MAC de cada dispositivo conectado al puerto físico del switch. Considerando la tabla de direcciones MAC, el switch puede decidir el envío de próximas tramas a un puerto, siempre que la dirección MAC de destino figure en la tabla. Este modo de operación se denomina segmentación, lo cual implica la división de la red en tantos segmentos como puertos tenga el switch (dominios de colisión). El resultado final es que, luego del aprendizaje de las direcciones MAC, cada dispositivo conectado al switch tiene con él un enlace punto a punto, full dúplex y libre de colisiones.

5.2.3 Routers

Un router es un dispositivo de networking que funciona en la capa 3 del modelo OSI. Al igual que los switches mantiene una tabla mediante la cual decide el envío de paquetes por determinado enlace, pero las direcciones utilizadas corresponden a la capa 3 del modelo OSI. Básicamente un router es un dispositivo que une dos o más redes. Una diferencia fundamental con respecto a los switches (además de la capa en la que operan) es que los routers pueden manejar direcciones de manera jerárquica. Así, pueden identificarse un gran número de nodos o redes por medio de una parte de su dirección (o subred). Todos esos nodos tendrán sólo una referencia en la tablas de enrutamiento, con lo que se reduce el tamaño de ésta. [5]

Los dispositivos de hardware llamados routers son computadoras dedicadas a funciones de red. La función de enrutamiento puede ser realizada también por computadoras que cumplan otras funciones dentro del sistema de control, como se observa en el modelo de la *fig. 8*.

6 Protocolos para el manejo de la redundancia

6.1 Definición

Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí. Los protocolos de comunicaciones determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos.

Estos protocolos pueden ser abiertos, en el caso de que estén normados por organizaciones o comités como el IEEE. Los protocolos abiertos pueden ser implementados por cualquier fabricante en sus productos. Por otro lado distintos fabricantes han desarrollado protocolos propios de los cuales, si bien se describe su funcionamiento, no se brindan todos los detalles ya que pertenecen a la empresa fabricante.

En el caso de las redes que implementan redundancia, existen protocolos que manejan la reconfiguración de las mismas en caso de falla de un enlace o dispositivo activo. Estos protocolos pueden trabajar en distintos dispositivos y en distintas capas del modelo OSI.

Se describirán a continuación dos protocolos para el manejo de la redundancia: Rapid Spanning Tree Protocol (RSTP), un protocolo abierto que se implementa en los dispositivos activos de una red (switches) y que trabaja en la capa 2 del modelo OSI (capa de enlace de datos); y Redundant Network Routing Protocol (RNRP), un protocolo propietario de la firma ABB que se implementa en los dispositivos finales de la red y que trabaja en la capa 3 del modelo OSI (capa de red)

6.2 Rapid Spanning Tree Protocol (RSTP)

6.2.1 Generalidades del protocolo

RSTP está descripto en IEEE 802.1w. Las normas de STP y RSTP se han unificado en IEEE802.1D-2004.

RSTP es un protocolo de enlaces redundantes implementado en la capa 2 del modelo OSI. Los nodos finales (si sólo se trabaja con RSTP) tienen una única conexión a la red por lo que implementa el tipo de redundancia indicado en la *fig. 9*. Los enlaces redundantes se dan entre distintos dispositivos activos (switches).

Cuando se implementan enlaces redundantes en la capa 2 del modelo OSI se generan topologíaas físicas con bucles. Considerando la topología de la *fig. 17*, si el switch SW1 debe transmitir un broadcast lo hará por todos sus puertos (a través de las líneas 1 y 2). El switch SW2 recibirá la trama broadcast la retransmitirá por la línea 3 y el switch SW3 la retransmitirá por la línea 2. SW1 la recibirá y la retransmitirá por la línea 1 (SW3 también transmitirá tramas en el sentido contrario). Al cabo de poco tiempo la red estará completamente ocupada enviando tramas broadcast a tal punto que puede degradar su desempeño o incluso inutilizarla para el envío de tráfico. Esto se conoce como *"tormenta de broadcast"*.

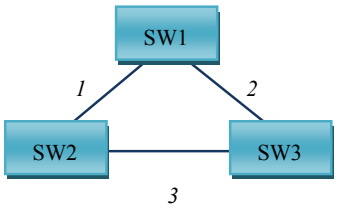


fig. 17 – Topología con bucle

Para solucionar el problema de las tormentas de broadcast y otros relacionados con la duplicación e inconsistencia de tramas se desarrolló el protocolo Spanning Tree (IEEE 802.1D).

El protocolo spanning tree creaba un árbol lógico sin bucles sobre una topología física con bucles. Para realizarlo, bloqueaba ciertos puertos de algunos switches. La operación del protocolo era transparente para los dispositivos finales. El problema con STP era su tiempo de convergencia (de 30 a 60 segundos) que lo hacían inadecuado para ser utilizado en una red de control o supervisión.

El protocolo Rapid Spanning Tree es la evolución del STP (Spanning Tree Protocol). RSTP mejora drásticamente los tiempos de convergencia del antiguo protocolo a valores que oscilan entre medio segundo y algunos segundos. Soporta 4096 puertos interconectados y es compatible con STP.

RSTP también crea un árbol lógico sin bucles sobre una topología física que tiene bucles. Su funcionamiento es el siguiente: todos los switchs involucrados intercambian tramas de control llamadas

BPDUs (Bridge Protocol Data Unit). Mediante el intercambio de las BPDUs uno de los switches es promovido a raíz del spanning tree. Esta elección se realiza teniendo en cuenta un valor llamado BID (Bridge ID), que se conforma de la siguiente manera:

fig. 18 – Bridge ID

La prioridad es un valor configurable comprendido entre 0 y 65535 y que normalmente tiene el valor predeterminado de 32767. El switch con BID menor será promovido a raíz del árbol.

Las BPDUs se envían de manera predeterminada cada 2 segundos (hello time) y contienen información acerca del switch emisor, su prioridad, MAC, prioridad del puerto y costo del puerto. El costo depende únicamente de la velocidad del enlace. El hello time puede configurarse en un mínimo de 1 segundo.

Las BPDUs son un indicador de que el enlace permanece vivo. Si se pierden 3 BPDUs seguidas en un enlace, el switch considera que ha perdido conectividad con su vecino. Si la falla es de link a nivel físico, se detectará mucho más rápidamente. Ya que las BPDUs son generadas por cada switch, el cambio de topología es informado inmediatamente hacia arriba y hacia abajo del switch que la detecta.

6.2.2 Los puertos en RSTP

Estado de los puertos

Al iniciarse el sistema, el algoritmo STA (Spanning Tree Algorithm) elige el switch raíz. Basándose en las BPDUs enviadas por el switch raíz, el resto de los switches seleccionan como **puerto raíz** el más cercano a aquel (en términos de costos).

Un puerto es **designado** si es el que envía BPDUs con el menor valor BID.

En un segmento dado, el puerto designado es el único camino hacia el switch raíz. Si hubiera más de un camino, se está en presencia de un bucle. Todos los puertos del switch raíz son designados. El switch raíz es el único de la topología que no tiene puerto raíz.

Un puerto de un switch que se encuentra en un segmento en el que el puerto de otro switch envía BPDUs con menor BID que las que él envía, se coloca en estado "descartando" y constituye un **puerto alternativo**.

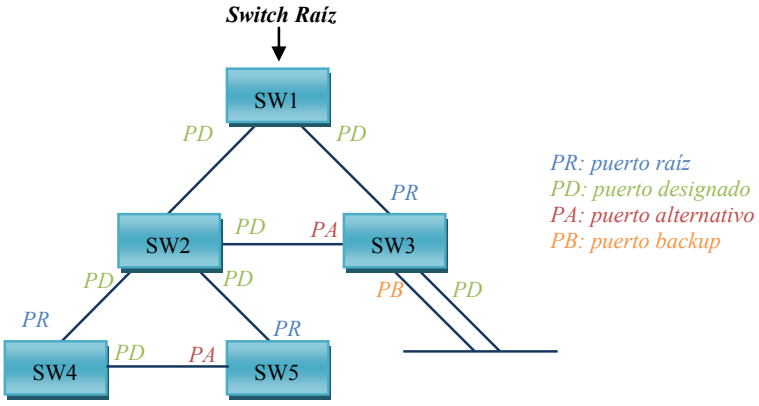


fig. 19 – Puertos de switches aplicando RSTP en una topología con bucles

Cuando en un switch un puerto recibe una BPDU con BID menor que la proveniente de otro puerto propio, pasa al estado descartando y constituye un **puerto de reserva** o **puerto backup**. En este caso, dos puertos del switch están conectados al mismo segmento de red.

Puertos de borde

Si un switch tendrá puertos conectados a dispositivos finales, es posible configurar esos puertos para que no intercambien BPDUs. En estas condiciones, el puerto no genera cambios de topología y mejora el tiempo de convergencia.

Si el puerto recibe una BPDU, inmediatamente pierde su estado y se transforma en un puerto spanning tree normal. [9] [10]

6.2.3 Tiempos de convergencia

La rápida transición es una de las características más importantes en el estándar 802.1w. RSTP no se basa en timers (como su antecesor STP), sino en un mecanismo de avisos para poner en modo de envío un puerto de manera segura, sin generar topologías lógicas con bucles que llevarían a la producción de tormentas de broadcast.

Para lograr una rápida convergencia es necesario la configuración de puertos de borde y contar con enlaces punto a punto entre los switches. La existencia de enlaces punto a punto se deriva automáticamente del modo dúplex del puerto: se asume que un puerto que opera en full dúplex está conectado a un enlace punto a punto, mientras que un puerto que trabaja en half dúplex es un puerto compartido. Es posible colocar una configuración explícita en el puerto.

Se analizan a continuación dos casos de falla y la forma conceptual en que RSTP convergirá.

Caso 1: Pérdida de conexión. Si en la *fig. 20*, existe una falla en la línea que conecta SW1 con SW2:

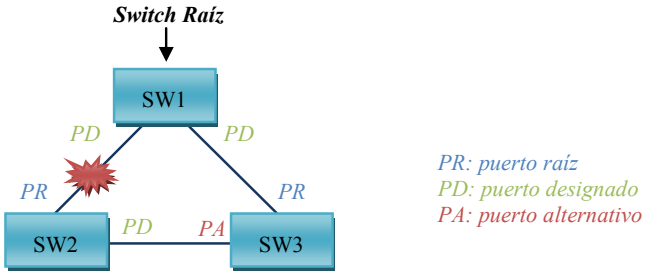


fig. 20- Pérdida de conexión en RSTP

La pérdida del link con el switch raíz hace que SW2 envíe una BPDU inferior que la del switch raíz, pero intentando ser la raíz del spanning. SW3 que conoce que el switch raíz está operativo pues mantiene aún su conexión con él, responde con otra BPDU que contiene información acerca de SW1. Como consecuencia, SW2 coloca el puerto que conecta a SW3 como puerto raíz y el puerto de SW3 pasa a ser el puerto designado en el segmento *(fig. 21)*.

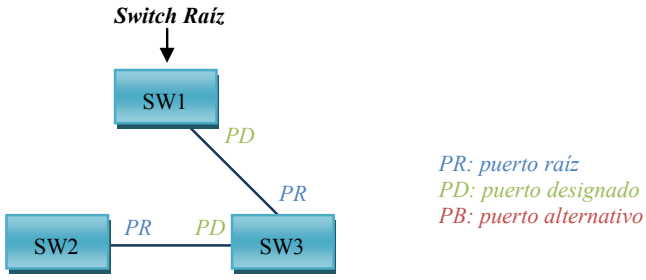


fig. 21 – Reconfiguración luego de la pérdida de conexión

Caso 2: En la fig. 22, el puerto p2 del switch SW2 es el puerto raíz, p3 y p4 son puertos de borde y p5 es un puerto alternativo (bloqueado). Si el puerto p1 del switch SW2 se conecta al switch raíz SW1 (puerto p0), inmediatamente los puertos de ambos switches se colocan como puertos designados y en estado descartando (bloqueado). Ambos switches intercambian BPDUs. Ya que SW1 posee una mejor BPDU, SW2 coloca en sync cada uno de sus restantes puertos. Esto significa que:

a) El puerto está en modo de bloqueo (descartando), ó
b) El puerto es un puerto de borde.

Como los puertos p3 y p4 son puertos de borde y p5 está bloqueado, ya cumplen con la condición sync, por lo tanto el único puerto que debe bloquearse es el p2.

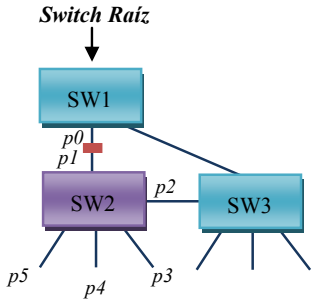


fig. 22 – Conexión de un puerto formando una topología con bucles en RSTP

Una vez hecho esto, SW2 desbloquea su puerto p1 y lo coloca como puerto raíz e informa explícitamente a SW1 que puede desbloquear su puerto p0.

De esta manera, los cambios en la topología se informan entre switches inmediatamente ocurren; y se bloquean los puertos necesarios. Esto se desencadena cuando el evento ocurre.

En RSTP el número máximo de switches por los cuales puede pasar la señal en la topología desde origen hasta destino es de siete. [9]

6.3 Redundant Network Routing Protocol (RNRP)

6.3.1 Generalidades del protocolo

RNRP es un protocolo de enrutamiento de paquetes IP (capa 3) desarrollado por la firma ABB. Está diseñado para ser usado en redes de automatización de alta disponibilidad. [11] [12] [13]

El protocolo soporta redundancia completa (nodos y redes). Los dispositivos finales tienen dos interfaces de red (NICs) con dos direcciones IP diferentes. La implementación de la redundancia de esta forma puede ser observada en la *fig. 10*, en el esquema capa de red.

Al ser un protocolo de enrutamiento, cada dispositivo mantiene una tabla que le permite conocer por qué camino debe enviar los paquetes para alcanzar cada destino.

Periódicamente cada nodo intercambia información de enrutamiento con los demás utilizando direccionamiento multicast. La información se envía por todas las interfases como un vector de enrutamiento que indica qué otros nodos de la red puede ver el nodo que envía. Cada nodo de la red utiliza estos vectores para construir la tabla de enrutamiento. El intervalo de tiempo entre cada envío de los paquetes con información del protocolo se denomina *"send period"*. Este valor puede ser ajustado entre 1 y 60 segundos (de manera predeterminada send period = 1 segundo).

El protocolo permite el manejo de múltiples áreas de red. Un área es una estructura de red sin routers constituida por dos redes IP independientes y con iguales capacidades. Cada red individual dentro de un área tiene asignada un *path number* para identificarla. La red primaria tiene el path number = 0 y la secundaria el path number = 1 *(fig. 23)*.

Un nodo se identifica en RNRP por:

- El número de área de red (0-31)
- El número de nodo (1-500)

El path number es un parámetro en cada interface de red. Cada camino en un área de red corresponde a una subred IP. El número de subred IP es el mismo para todas las interfaces en el mismo path. El protocolo trabaja de tal manera que la existencia de las interfaces y redes redundadas en las capas inferiores es transparente para las aplicaciones. Las aplicaciones se comunican utilizando siempre las direcciones de la red primaria. En caso de indisponibilidad de esta red, el protocolo hace las conversiones de direcciones necesarias para transmitir por la red secundaria. El nodo destino vuelve a hacer la conversión de manera que toda la transmisión, desde el punto de vista de la aplicación, fue realizada por el primer camino.

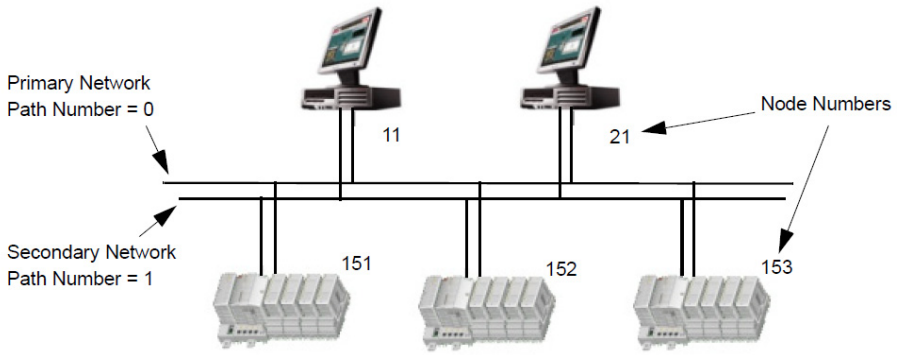


fig. 23 – Red constituida por un área

RNRP puede configurarse en un dispositivo para que actúe como router entre dos áreas de red. En este caso el dispositivo poseerá dos interfaces de red en cada área. Esto suele hacerse con servidores de datos que ofician de routers entre las redes de control y supervisión como se muestra en la *fig. 24*.

La redundancia implementada por RNRP funciona con dispositivos estándares de redes Ethernet, aunque no se limita a esta tecnología (puede integrar enlaces PPP). (11)

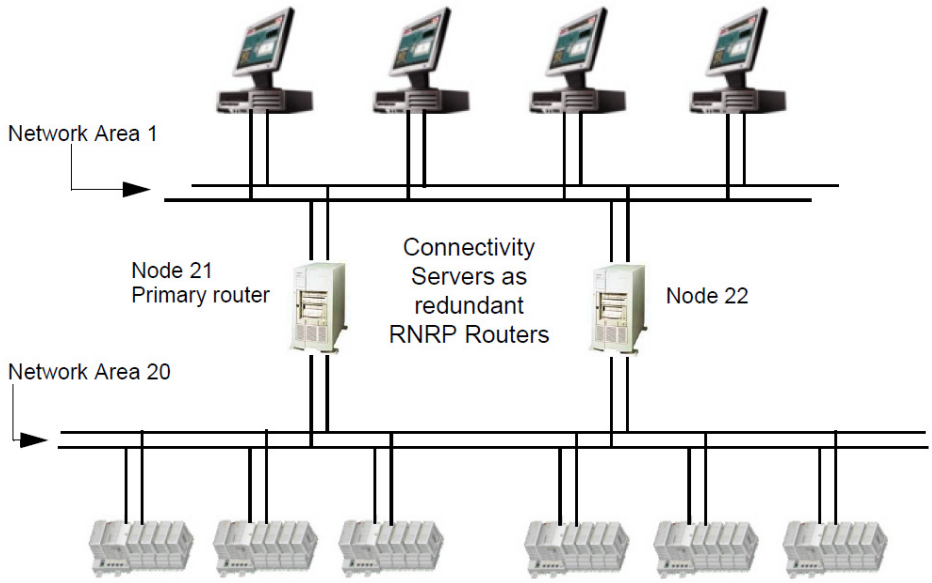


fig. 24 – Dos áreas de red con dos servidores de conectividad actuando como routers redundados

6.3.2 Manejo de fallas dentro de un área

Dentro de un área de red RNRP puede manejar puntos de falla simples en todas las conexiones nodo a nodo.

Al ocurrir una falla en una parte de la red o en un enlace de un nodo, el tiempo para actualizar la tabla de enrutamiento de todos los nodos a la vez con la nueva información es igual al "*send period*".

Cuando se detecta una falla, se rutea por la red secundaria sólo la información del nodo afectado. Los demás nodos siguen comunicándose entre sí a través de la red primaria. Esto se ejemplifica en la *fig. 25* donde el nodo A ha sufrido una falla en su conexión a la red primaria y el nodo B a la red secundaria.

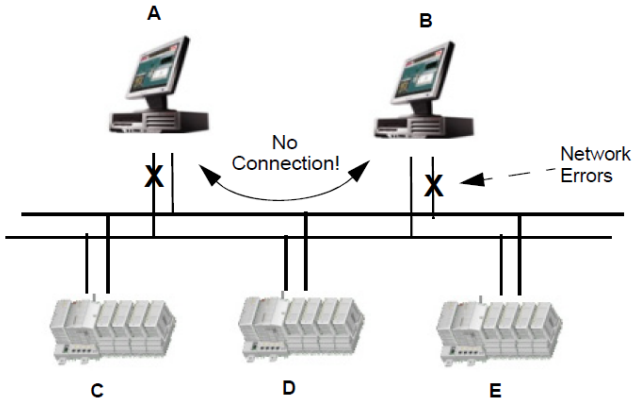


fig. 25 – Manejo de fallas en un área de red

En este ejemplo las comunicaciones entre el nodo A y el nodo B no son posibles, pero todas las demás comunicaciones entre pares permanecen funcionando:

- El nodo A puede comunicarse a través de la red secundaria con los nodos C, D y E.
- El nodo B puede comunicarse a través de la red primaria con los nodos C, D y E.
- Los nodos C, D y E mantienen sus comunicaciones redundantes

6.3.3 Notificación de caída de nodo

RNRP puede detectar la caída de un nodo o red remota. Se considera caído cuando no es posible alcanzar el nodo por ninguna de las redes. Las aplicaciones que se suscriben al estado de RNRP pueden utilizar esta información, de manera que se puede, por ejemplo, realizar el cambio de un servidor activo al redundante cuando se de por caído al principal. RNRP genera un evento de "nodo caído" (node down event) teniendo en cuenta el parámetro de configuración MaxLostMessages. El tiempo hasta que se genere el evento es:

*Tiempo hasta evento de nodo caído = (MaxLostMessages + 1) * SendPeriod*

Con los valores predeterminados: [10]

*Tiempo hasta evento de nodo caído = (3 + 1) * 1 =* **4 segundos**

6.3.4 Configuración de direcciones IP en las interfaces

En una red basada en el protocolo IP, las direcciones de la capa de Red (capa 3) constan de 32 bits. Una parte de este conjunto de bits (los más significativos) corresponden a la identificación de la subred y la restante (menos significativos) corresponden a la identificación del host dentro de la subred.

Al utilizar RNRP existen restricciones en cuanto a la asignación de direcciones IP a las interfases de cada uno de los nodos. La dirección IP en RNRP está conformada bit a bit de la siguiente manera:

XXXXXXXX.XXXXXXPP.LAAAAANN.NNNNNNNN

Donde

- Los primeros 14 bits (**X**) corresponden a la subred, por lo que la máscara de red deberá ser siempre 255.255.252.0
- **PP** es el path number. (0 ó 1 indicando la red primaria o la secundaria)
- **L** es la bandera *Local Flag* (indica si se transmitirán o no paquetes fuera del área en que se encuentra el nodo)
- **AAAAA** es el número de área.
- **NN.NNNNNNNN** es el número de nodo.

Existe una configuración por defecto que ABB llama *configuración implícita* de las direcciones. Si se utiliza esta configuración no es necesario ningún cambio en los parámetros del protocolo RNRP para que éste funcione correctamente. Esta configuración implícita exige que todos los nodos conectados al path 0 están en la subred 172.16.0.0/14 y los conectado al path 1 en la red 172.17.0.0/14.

Es posible utilizar otras subredes para los paths 0 y 1. En este caso se está en la *configuración explícita*. En esta configuración, las direcciones IP deben cumplir con la estructura mostrada más arriba. [10]

En las pruebas de laboratorio del presente trabajo, por simplicidad, los nodos fueron configurados utilizando la configuración implícita.

7 Pruebas de laboratorio

Se realizaron mediciones de los tiempos de restablecimiento de comunicaciones ante fallas de enlace y de puerto en distintos escenarios, utilizando el protocolo RSTP primero y luego RNRP.

En todos los casos se utilizó una aplicación cliente/servidor (no propia) programada en Visual Basic 6.0 para que desde una computadora (PC1) se enviaran paquetes UDP a otra (PC2). Este envío se realizaba cíclicamente mediante un objeto Timer propio de VB6.0. En la PC2 se visualizaba la secuencia de los paquetes recibidos de la PC1. Los paquetes llevaban información de la secuencia de generación. Las PCs corrían Windows XP Professional Service Pack 2.

Se planteó realizar los experimentos cortando diferentes líneas de conexión y contando los paquetes perdidos hasta el restablecimiento de la comunicación. Lo mismo se haría para medir los tiempos de reconexión.

UDP es un protocolo de la capa de transporte no orientado a la conexión. La pérdida de un paquete UDP no implica la retransmisión del mismo por parte de la capa transporte emisora. Esta es la razón por la que se lo utilizó UDP en lugar de TCP (usando TCP, al restablecerse la comunicación de red, la máquina emisora hubiera retransmitido los paquetes no recibidos por el receptor, impidiendo la medición ya que la misma se basaba en la pérdida de paquetes).

Se ajustó el tiempo de envío de los paquetes UDP en 15 ms. El error máximo cometido no sería mayor que dos veces ese intervalo, es decir 30 ms. Esto arroja un error no mayor que 3% considerando el segundo como tiempo esperado de convergencia en ambos protocolos.

7.1 Medición de tiempos de convergencia en RSTP

7.1.1 Planteo del escenario de pruebas

Se utilizaron dos switches no industriales "of the shelf": Baseline Switch 2226 Plus de 3Com con versión de firmware 1.0.1.16. Estos switches tienen 24 puertos de 100Mbps y dos puertos uplink de 1Gbps. Se configuraron los puertos de uplink de cada switch con un costo de 5000 para el puerto 25 y 10000 para el 26 de manera que el protocolo RSTP bloqueara el puerto 26 por tener costo superior. Las pruebas consistieron en desconectar el puerto 25 y medir la cantidad de paquetes perdidos hasta que se restableciera la conexión a través del puerto 26. [14]

7.1.2 Falla de enlace

Se utilizó para las pruebas la topología que aparece en la *fig. 26*. La pérdida de link es detectada rápidamente por los switches. Esta pérdida provoca el envío de BPDUs indicando "topology change" y desencandenando el recálculo del árbol de extensión.

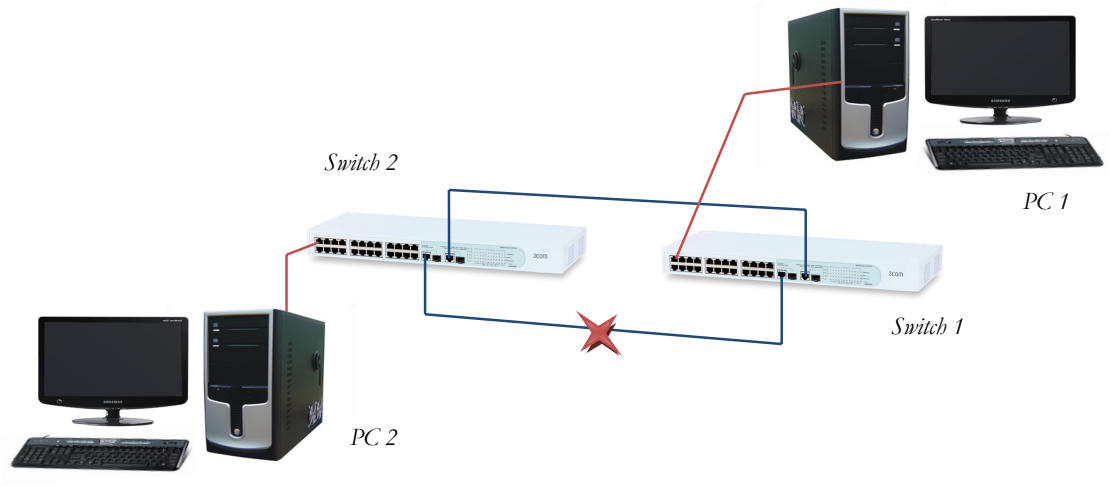


fig. 26 – Topología utilizada para medición de tiempos de reconfiguración luego de fallas de link en RSTP

Se consideraron dos casos:

a) Con los 24 puertos de 100 Mbps del switch interviniendo en el cálculo del árbol de extensión (es decir que no estuvieron configurados como "puertos de borde". Los resultados fueron los siguientes:

Topología	fig. 26
Tipo de falla estudiada	Pérdida de link
Hello time	2 s
Uplink	1Gbps
Puertos de 100 Mbps	No puertos de borde

Tiempo de convergencia [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	938	1766	984	1234	1781	1297	735	1078	1328	1172	735	1781	1231
Conexión	30030	29422	29453	29844	29438	29641	29235	29235	29672	29453	29235	30030	29542

b) Sin intervención de los 24 puertos de 100 Mbps en el cálculo del árbol de extensión (es decir configurados como "puertos de borde"):

Topología	fig. 26
Tipo de falla estudiada	Pérdida de link
Hello time	2 s
Uplink	1Gbps
Puertos de 100 Mbps	Puertos de borde

Tiempo de convergencia [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	1390	1484	531	1641	1547	391	1359	844	1281	1360	391	1641	1182
Conexión	282	265	282	282	468	266	484	265	265	281	265	484	314

7.1.3 Falla de puerto

Para evaluar el tiempo de convergencia en el caso de falla de un puerto de un dispositivo, pero que aún tenga link, se utilizó la topología mostrada en la *fig. 27*, donde los switches ubicados en el uplink de los puertos 25 (sw1 y sw2) no reconocen el protocolo RSTP, por lo tanto simularían la falla propuesta.

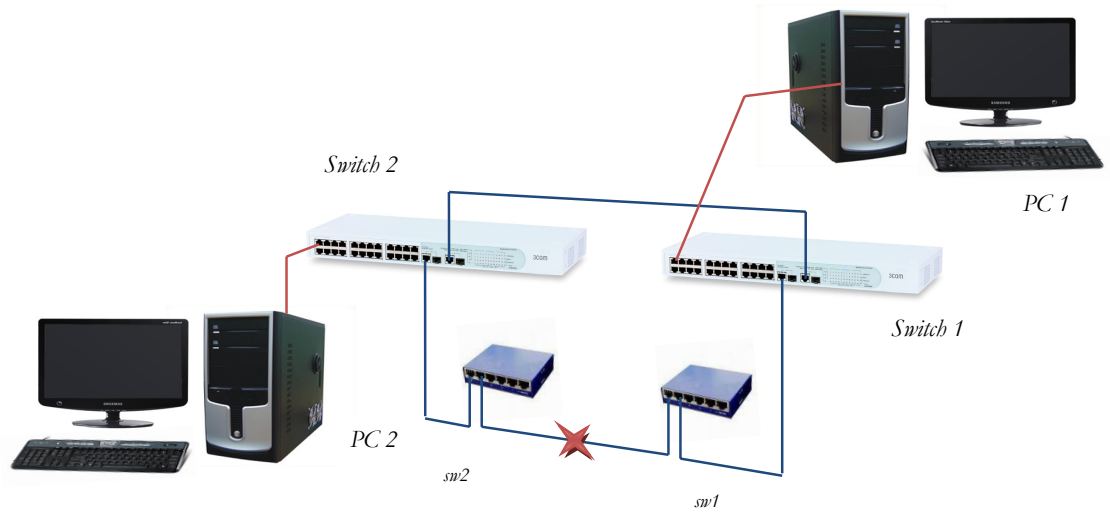


fig. 27 – Topología utilizada para medición de tiempos de reconfiguración luego de fallas de puerto en RSTP

Ya que no se contaba con switches con puertos de 1 Gbps, se utilizaron dos switches con puertos de 100 Mbps. El cambio de velocidad de uplink no debía afectar los resultados de la medición con respecto a una prueba utilizando uplinks de 1 Gb, puesto que no había carga en el enlace y los paquetes intercambiados eran pequeños, resultando así un tráfico despreciable a 100 Mbps.

De nuevo se consideraron dos casos. En ambos se configuraron los puertos de 100 Mbps de Switch 1 y Switch 2 como puertos de borde:

a) El tiempo entre transmisiones de BPDUs (Hello Time) se mantuvo en el valor predeterminado de 2 segundos:

Topología	fig. 27
Tipo de falla estudiada	Falla de puerto
Hello time	2 s
Uplink	100 Mbps
Puertos de 100 Mbps	Puertos de borde

Tiempo de convergencia [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	4937	4390	4485	4204	4969	4719	4437	4109	5797	4000	4000	5797	4604
Conexión	187	313	359	328	328	140	344	328	344	344	140	359	301

b) El hello time se llevó al valor mínimo (1 segundo):

Topología	fig. 27
Tipo de falla estudiada	Falla de puerto
Hello time	1 s
Uplink	100 Mbps
Puertos de 100 Mbps	Puertos de borde

Tiempo de convergencia [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	2172	2578	2609	2016	2250	2032	2734	2906	2594	2797	2016	2906	2468
Conexión	734	734	734	735	735	734	734	47	734	1328	47	1328	724

7.2 Medición de tiempos de reconexión en RNRP

7.2.1 Planteo del escenario de pruebas y registro de mediciones

Para la medición de los tiempos de reconexión del protocolo RNRP se utilizó el mismo equipamiento. Se agregó una segunda NIC a cada computadora y se instaló el protocolo RNRP en ambas. En todas las pruebas se realizó la desconexión de enlaces de la red primaria, ya que es la que RNRP utiliza por defecto y sólo cambia a la secundaria en caso de falla de la primera.

Luego de un análisis de los parámetros ajustables de RNRP y teniendo en cuenta que el experimento se realizaría en una única área de red, se mantuvo la configuración por defecto del protocolo RNRP ya que ésta daría los mejores tiempos de reconexión.

Las direcciones IP asignadas a las NICs de las computadoras se eligieron teniendo en cuenta las recomendaciones de ABB (configuración implícita).

En la bibliografía no se aclara si el protocolo puede detectar pérdidas de enlace y de esa manera reconectar más rápidamente tal como lo hacen los switches con sus enlaces en RSTP. Se decidió comprobarlo haciendo tres rondas de mediciones: dos provocando fallas en los enlaces con las PCs (que son quienes envían los paquetes de protocolo) y una en la red, manteniendo intactos los enlaces. Por comparación de los resultados se podría inferir si el protocolo censa el estado de las NICs.

La primera ronda de mediciones se realizó con la topología indicada en la *fig. 28*. En la segunda se provocó la falla indicada en la *fig. 29*. En la tercera se agregó un switch auxiliar a la red primaria y se desconectó el enlace entre switches de manera que las estaciones no perdieran link y se simulara un error en la red *(fig. 30)*.

En todos los switches se desactivó el protocolo RSTP.

Los resultados fueron los siguientes:

a) Desconexión del enlace emisor:

Topología	fig. 28
Tipo de falla estudiada	Pérdida de link envío
Send Period	1 s

Tiempo de reconfiguración [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	328	1313	1438	844	1266	734	1125	1422	1141	859	328	1438	1047
Conexión	0	0	0	0	0	0	0	0	0	0	0	0	0

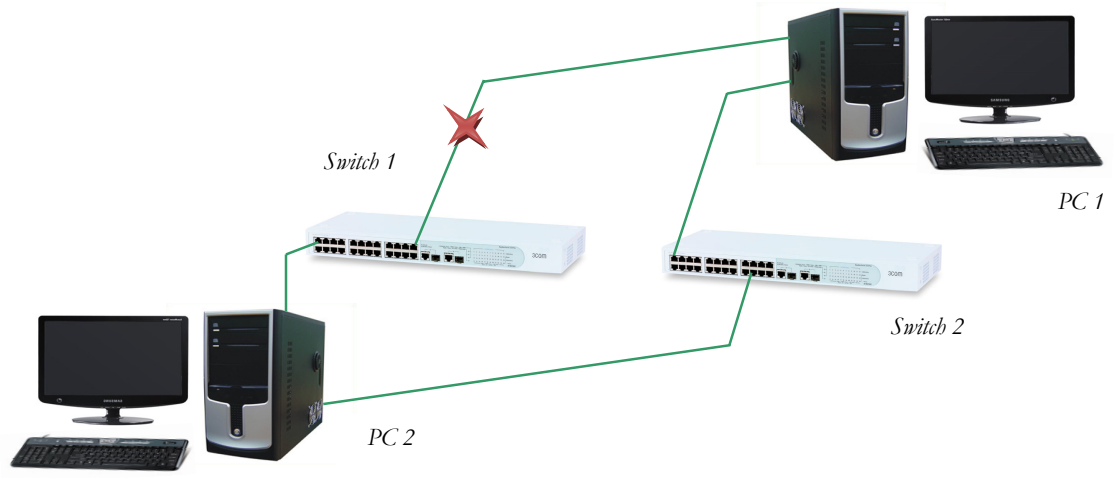


fig. 28- Topología utilizada para medición de tiempos de reconexión luego de fallas de enlace emisor en RNRP

b) Desconexión del enlace receptor:

Topología	fig. 29
Tipo de falla estudiada	Pérdida de link recepción
Send Period	1 s

Tiempo de reconfiguración [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	782	1407	1453	1516	922	1157	1250	1094	1047	735	735	1516	1136
Conexión	0	0	0	0	0	0	0	0	0	0	0	0	0

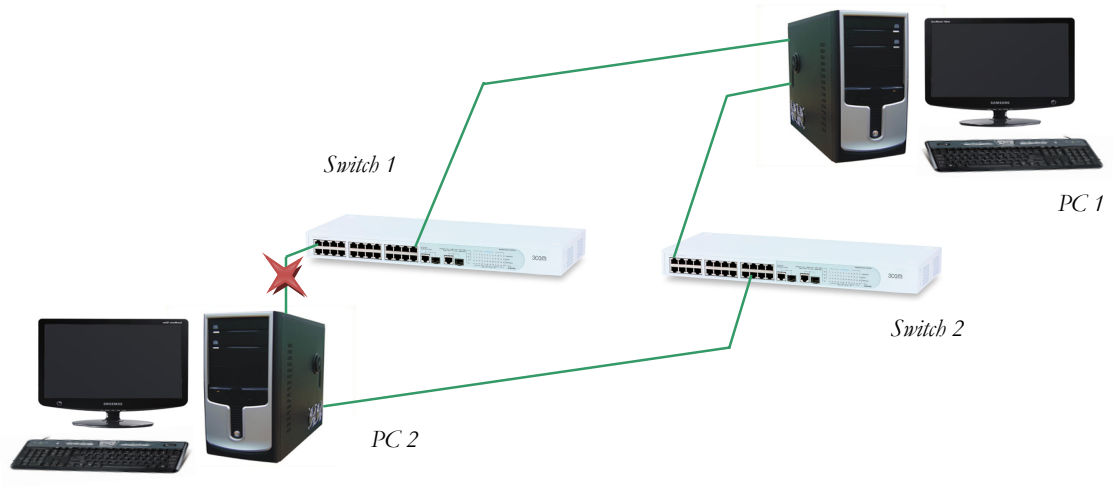


fig. 29 – Medición de tiempos de reconexión luego de fallas de enlace receptor en RNRP

c) Desconexión del enlace entre switches:

Topología	fig. 30
Tipo de falla estudiada	Falla de red
Send Period	1 s

Tiempo de reconfiguración [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	1219	828	953	1328	1078	1485	891	1328	1047	938	828	1485	1109
Conexión	0	0	0	0	0	0	0	0	0	0	0	0	0

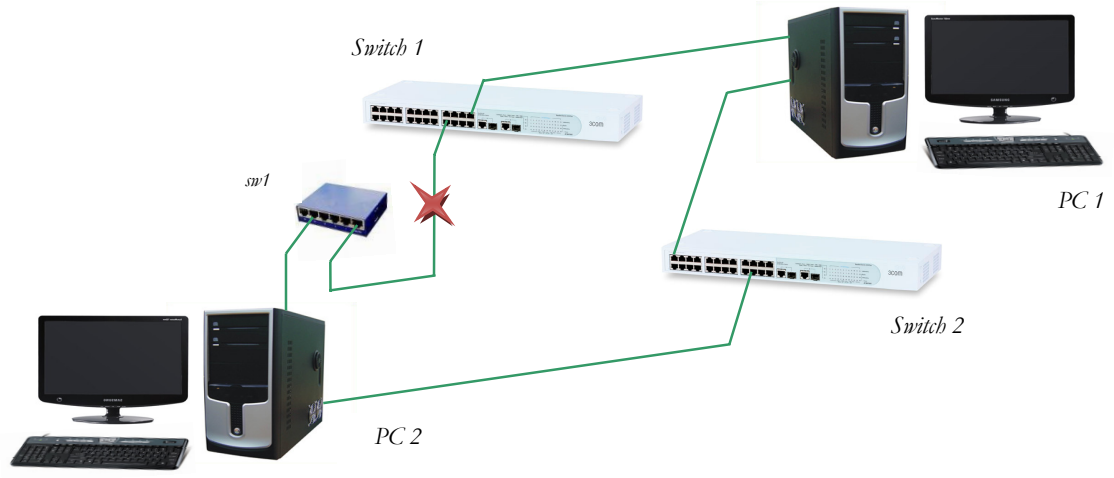


fig. 30 – Topología utilizada para medición de tiempos de reconexión luego de fallas de la red primaria en RNRP

En las tres configuraciones se pudo observar, mediante la utilización de un analizador de protocolo (Programa WireShark) que en la reconexión no se duplican datos, es decir, el primer paquete de datos enviado por la red reconectada (la 0) tiene el número de secuencia siguiente al del último paquete enviado por la red de secundaria.

7.2.2 Mediciones adicionales

Al observarse que el tiempo máximo de reconfiguración supera el segundo, se realizaron dos pruebas más. En la primera se suprimieron los switches y se interconectaron las computadoras con dos cables directamente. Es posible realizar esto porque en la configuración planteada se tienen sólo dos dispositivos. Los resultados fueron similares, con lo que se descartó que los valores por encima del segundo se debieran a alguna característica de los switches empleados.

Seguidamente se incrementó el valor "*send period"* a 10 segundos y se repitieron las pruebas en las tres topologías. En la tabla siguiente se muestran los resultados para la topología de la fig. 30, ya que con las demás los valores fueron comparables a ésta.

Topología	fig. 30
Tipo de falla estudiada	Falla de red
Send Period	10 s

Tiempo de reconfiguración [ms]													
	1	2	3	4	5	6	7	8	9	10	mín.	máx.	prom.
Desconexión	15031	14422	16078	18234	13594	13125	16797	17515	18750	12343	12343	18750	15589
Conexión	0	0	0	0	0	0	0	0	0	0	0	0	0

Se observa que los tiempos máximos de reconfiguración para *"send period"* de 1 segundo y de 10 segundos están en el orden de 1.5 veces este valor, con lo que se descartó que los tiempos superiores a los esperados se debieran a retardos en la red o a demoras en el procesamiento de las computadoras: el tiempo por encima del valor de *"send period"* se debería al mecanismo de detección de fallas del protocolo.

Para comprobar esto se analizó el proceso de reconfiguración paquete a paquete.

7.2.3 Análisis de la reconfiguración con analizador de protocolos de red

Como se destacó en la descripción del funcionamiento de RNRP, cada nodo envía un vector de enrutamiento indicando qué nodos puede ver en la red. Esta información se envía por ambas redes a intervalos de tiempos fijados por el valor *"send period"* y cada nodo receptor actualiza su tabla de enrutamiento **basándose en esta información**. La forma en que un nodo identifica un problema en el camino hacia otro es la pérdida de paquetes de protocolo provenientes de ese nodo, pero esto **sólo modifica su tabla de enrutamiento**, no se generan paquetes para indicar el cambio antes de que venza el tiempo *"send period"* (no existen envíos de paquetes de protocolo tipo "topology change".

Considerando que el envío de paquetes de protocolo no está sincronizado en los diferentes nodos y que los paquetes de protocolo sólo se envían cada *"send period"* segundos, es esperable variaciones en los tiempos de reconfiguración y que estos tiempos puedan superar el valor *"send period"*.

Se decidió observar el protocolo paso a paso en una reconfiguración utilizando el analizador de protocolos *Wireshark 1.2.8* en el nodo receptor (PC2) de la *fig. 29*. La captura de pantalla de la *fig. 31* muestra los paquetes enviados y recibidos por ambos adaptadores de red de la computadora receptora.

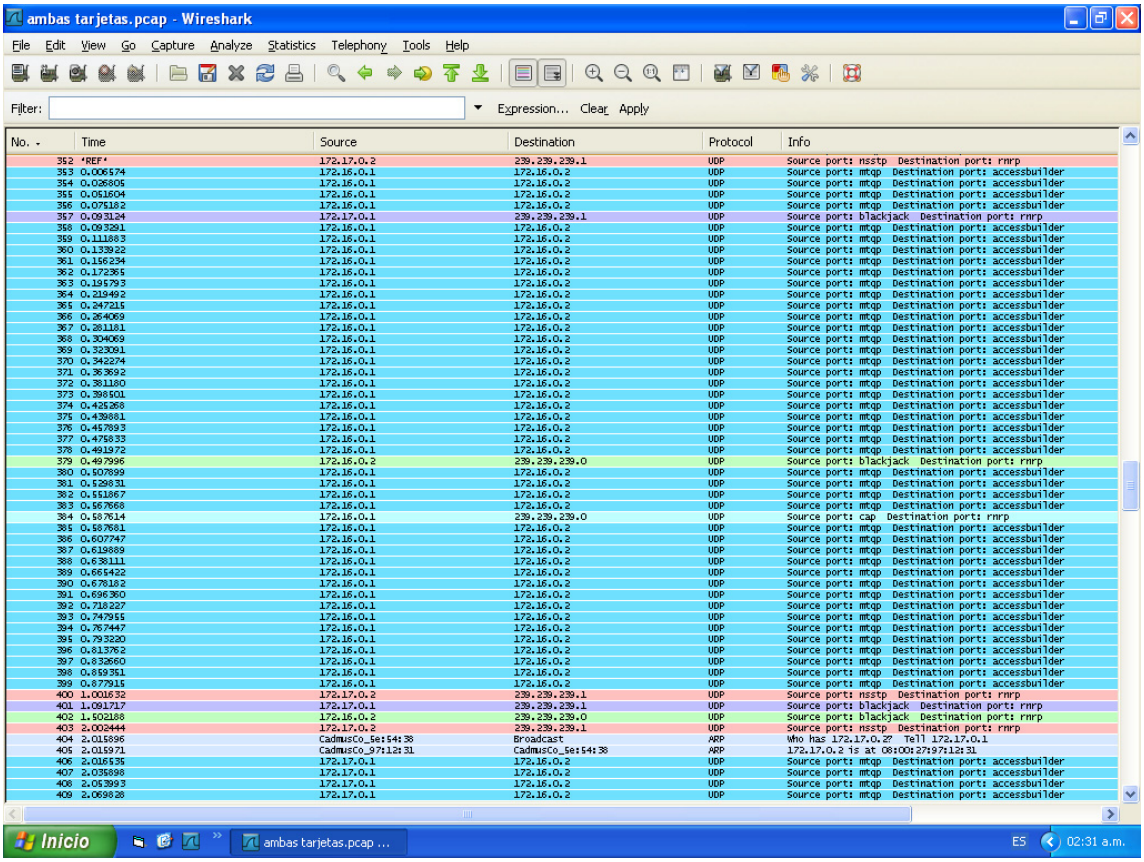


fig. 31 – Proceso de reconexión capturado en el nodo receptor por el analizador de protocolo

Los paquetes de protocolo enviados por cada una de las cuatro NICs están mostrados según los colores: [1]

Nodo	Path	Dirección IP	Color
PC1 (emisor)	0	172.16.0.1	Verde claro
	1	172.17.0.1	Azul
PC2 (receptor)	0	172.16.0.2	Verde vivo
	1	172.17.0.2	Rosado

Los paquetes de datos (provenientes de la aplicación generadora de tráfico en la máquina emisora) aparecen en color celeste.

Se observa que existe desconexión desde el tiempo 0.877915 hasta el 2.016535, o sea por 1.139 segundos. La aplicación midió en esta misma desconexión 1.142 segundos.

En un mismo path, los nodos transmisor y receptor muestran desfasajes de aproximadamente 90 milisegundos (considerando despreciable la latencia) y un mismo nodo envía paquetes por cada una de sus tarjetas con un desfasaje de aproximadamente medio *"send period"*, lo que representa en este caso unos 500 milisegundos.

[1] Tanto en la fig. 31 como en la fig. 32 se ha utilizado la codificación de colores mostrada en la tabla para indicar los envíos desde cada una de las 4 NICs involucradas

El esquema de la *fig. 32* ilustra mejor la forma en que se realiza la reconfiguración en el caso mostrado. Sólo se muestran los envíos y recepciones **de paquetes de protocolo**. Mientras tanto, los datos se están enviando por el path 0.

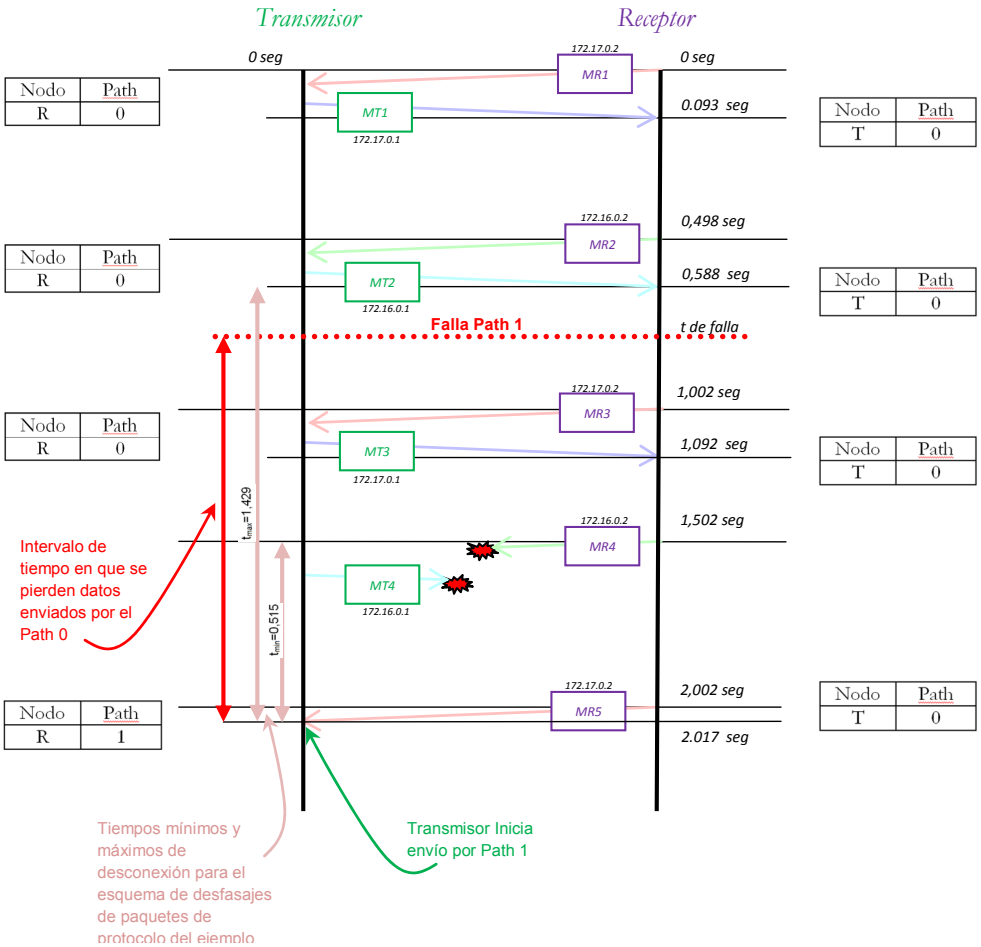


fig. 32 – Esquema del proceso de reconexión

Mensaje enviado	Tiempo (desde el punto de vista del receptor)	Dirección IP de origen	Path	Información en el mensaje
MR1	0 ms	172.17.0.2	1	T alcanzable por path 0 T alcanzable por path 1
MT1	93 ms	172.17.0.1	1	R alcanzable por path 0 R alcanzable por path 1
MR2	498 ms	172.16.0.2	0	T alcanzable por path 0 T alcanzable por path 1
MT2	588 ms	172.16.0.1	0	R alcanzable por path 0 R alcanzable por path 1
MR3	1,002 ms	172.17.0.2	1	T alcanzable por path 0 T alcanzable por path 1
MT3	1,092 ms	172.17.0.1	1	R alcanzable por path 0 R alcanzable por path 1
MR4	1,502 ms	172.16.0.2	0	T alcanzable por path 0 T alcanzable por path 1
MT5	----- ms	172.16.0.1	0	R alcanzable por path 0 R alcanzable por path 1
MR5	2,002	172.17.0.2	1	***T NO ALCANZABLE por path 0*** T alcanzable por path 1

Referencias:

- T: Transmisor
- R: Receptor
- Caracteres en rojo: paquetes perdidos por rotura del enlace.
- Fondo violeta: paquetes transmitidos por el receptor.
- Fondo verde: paquetes transmitidos por el emisor.

Al inicio de la secuencia ambas redes están funcionando normalmente. En t=0 el nodo receptor envía su vector de enrutamiento por la red 1 (path 1) y poco milisegundos después el nodo transmisor envía por la misma red su propio vector. Así, las tablas de enrutamiento de cada nodo indican que es posible alcanzar el nodo contrario por la red 0 (path 0).

Con un desfasaje de alrededor de 500 ms ocurre el envío de paquetes de protocolo desde el receptor al emisor y viceversa por la red 0. No hay cambios en la información contenida en las tablas de enrutamiento de cada nodo.

Luego de estos eventos ocurre la falla de la red 0. A partir de este momento dejan de recibirse paquetes de datos, puesto que es el emisor quien debe cambiar a la red 1 y aún no tiene información de que haya ocurrido una falla en el path 0 (su tabla de enrutamiento indica que el nodo receptor puede alcanzarse a través de la red 0).

Cuando, alrededor de un segundo después del inicio de la secuencia, emisor y receptor vuelvan a intercambiar paquetes por la red 1, no tendrán aún información de la falla del path 0, por lo que las tablas de enrutamiento seguirán sin cambios y continuarán perdiéndose paquetes por la red 0.

En el tiempo 1,502 segundos los nodos transmitirán paquetes por la red 0 (MR4 y MT4). Estos paquetes se perderán e indicarán a cada nodo que no es posible ver el nodo contrario por esa red. Esta información se enviará recién en el próximo envío (en t=2,002) donde se observa que la tabla de enrutamiento enviada por el receptor indica que puede ver al transmisor sólo por el path 1.

Apenas el transmisor recibe este paquete con el vector de enrutamiento del receptor, cambia su tabla de enrutamiento y, a partir de este momento, envía por la red 1, restableciéndose la recepción.

Un hecho importante a observar es que efectivamente el protocolo detecta fallas por pérdida de *un* paquete de protocolo, pero sólo puede cambiar la tabla de enrutamiento de un emisor cuando explícitamente el receptor le indique que ha detectado la falla del path 0 y que está funcionando el path 1. Esto explica por qué en el tiempo t=2,017 aún no ha cambiado la tabla de enrutamiento del nodo receptor.

En el caso de falla mostrado el tiempo de desconexión fue de 1,139 segundos. Por observación de la *fig. 32 l*os valores máximos y mínimos de tiempo de desconexión podrían haber sido *para el caso mostrado*:

- t_{min}=0,515 segundos
- t_{max}=1,429 segundos

Si existen desfasajes diferentes entre los paquetes de protocolo, estos valores cambiarán.

8 Conclusiones

Del análisis de los protocolos estudiados y de los resultados obtenidos en las mediciones se puede arribar a la siguiente tabla comparativa entre RSTP y RNRP

RSTP (Rapid Spanning Tree Protocol)	RNRP (Redundant Network Routing Protocol)
Abierto – IEEE 802.1w	Propietario de la firma ABB
Redundancia en la red	Redundancia en los nodos y en la red
Funciona en la capa 2 del modelo OSI	Funciona en la capa 3 del modelo OSI
Protocolo de reconfiguración de enlaces	Protocolo de enrutamiento
Implementado en los switches	Implementado en los nodos
Los enlaces nodo-switch, si están redundados, deben ser tratados por otro protocolo	Los enlaces redundantes de los nodos son tratados por el protocolo
Puede detectar pérdida de link en un puerto con lo que mejora su tiempo de reconfiguración	No detecta pérdidas de link. Reconfigura por la pérdida de paquetes del protocolo
Tiempo de reconfiguración no nulo en la reconexión y con cortes en los enlaces no configurados como puertos de borde	Tiempo de reconfiguración nulo en la reconexión
No puede detectar la caída de un dispositivo final pues opera con los dispositivos activos de la red	Puede detectar la caída de un dispositivo final (la pérdida de conectividad por ambas redes redundantes o la caída del nodo)
En una topología con dos nodos y dos switches converge dentro de los 3 segundos ante la falla/restitución de un enlace en el peor caso.	En una topología con dos nodos reconfigura dentro del segundo y medio ante la falla de un enlace/dispositivo activo en el peor caso.

Con la metodología desarrollada y aplicada en el presente trabajo para el análisis de protocolos de reconfiguración de redes de supervisión y control basadas en tecnología Ethernet, se puede afirmar que:

Es posible utilizar RSTP como protocolo de reconfiguración de enlaces redundantes en las redes de supervisión y control de una central nuclear de potencia siempre que el sistema de control de esa instalación permita tiempos de desconexión de hasta 3 segundos. En el caso de utilizar redundancia de nodos debe resolverse esta redundancia mediante otro protocolo.

Es posible aplicar RNRP como protocolo de reconfiguración de redes redundantes en una central nuclear de potencia siempre que el tiempo máximo admitido de desconexión en caso de falla no sea superior a los 1.5 segundos en las redes de control y supervisión separadamente.

Si el sistema que corre sobre la red Ethernet se basa en el protocolo de transporte TCP (capa 4 del modelo OSI), independientemente del protocolo de reconfiguración, los datos perdidos durante la desconexión se retransmitirán luego de la reconexión, por lo que los valores históricos se mostrarán a partir de este momento. Durante el tiempo de la desconexión no se actualizarán los valores en las consolas de operador.

9 Referencias

1. **Katsuhiko Ogata**. Ingeniería de Control Moderna, 2da edición. Prentice Hall. 1993.
2. **Nancy Leveson – Mats Heimdahl – Jon Reese**. Designing Specification Languages for Process Control Systems: Lessons Learned and Steps to the Future.
3. **IAEA. Safety Standards Series**. Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety Guide No. NS-G-1.3. 2002.
4. **G. G. Preckshot – NUREG/CR-6082 UCRL-ID-114567**. Data Communications. 1993.
5. **Cisco**. Cisco Networking Academy Program v3.1.
6. **IAEA. Technical Reports Series**. Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook. 1999.
7. **Kai Hansen**. Redundancy Ethernet in Industrial Automation. IEEE. 2005.
8. **Hubert Kirrmann – Dacfey Dzung**. Selecting a Standard Redundancy Method for Highly Available Industrial Networks. IEEE. 2006
9. **IEEE Std 802.1D- 2004** (Revision of IEEE Std 802.1D-1998). IEEE Standard for Local and metropolitan area networks. Media Access Control (MAC) Bridges. IEEE. 2004.
10. **Alfredo Dupont – Pablo Juárez del Valle**. Análisis del protocolo RSTP para redes de Supervisión y Control. IN-CAREM25I-2-A8661 Rev. 0. 2008
11. **ABB**. System 800xA. Automation System Network Design and Configuration (800xA System Version 5.0 SP2). Document number: 3BSE034463R5021. June 2008.
12. **ABB**. System 800xA. System Guide Functional Description. Document number: 3BSE038018R5021. July 2008.
13. **ABB**. System 800xA. Basic Configuration. Course T314. Document number: 3BDS013442 / Rev C. January 2008.
14. **Alfredo Dupont – Pablo Juárez del Valle**. Medición de los tiempos de convergencia en una red con protocolo RSTP (802.1W). IN-CAREM25I-3-A8661 Rev. 0. 2008