CONGESTIÓN EN LAS REDES DE DATOS

JOSE A. BARRETO GUERRA

JAVIER E. PATRÓN MORENO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS, D. T. Y C.

2008

CONGESTIÓN EN LAS REDES DE DATOS

JOSE A. BARRETO GUERRA

JAVIER E. PATRÓN MORENO

Monografía presentada para optar al
Titulo de ingeniero de sistemas

DIRECTOR
GONZALO GARZÓN

UNIVERSIDAD DE TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS, D. T. Y C.

2008

Nota de aceptación

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma de jurado

Cartagena, Agosto 1 de 2008

Cartagena, Agosto 1 de 2008

Señores:

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Apreciados señores

Por medio de la presente nos permitimos informarle que la monografía titulada "**CONGESTIÓN EN LAS REDES DE DATOS"** ha sido desarrollas de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que es satisfactorio y amerita ser presentado para su evaluación.

Atentamente:

JOSE A. BARRETO GUERRA	**JAVIER E. PATRÓN MORENO**
06227044	**06227047**

Cartagena, Agosto 1 de 2008

Señores:

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Apreciados señores

Por medio de la presente nos permitimos informarle que la monografía titulada "**CONGESTIÓN EN LAS REDES DE DATOS"** ha sido desarrollas de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que es satisfactorio y amerita ser presentado para su evaluación.

Atentamente:

GONZALO GARZÓN
Director

AUTORIZACIÓN

Cartagena de Indias, D. T Y C.

Agosto 1 de 2008

Yo JOSE A. BARRETO GUERRA identificado con la cedula de ciudadanía numero 73.207.194 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE en la biblioteca

_____

JOSE A. BARRETO GUERRA

AUTORIZACIÓN

Cartagena de Indias, D. T Y C.

Agosto 1 de 2008

Yo JAVIER E. PATRÓN MORENO identificado con la cedula de ciudadanía numero 73.008.981 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE en la biblioteca

_____

JAVIER E. PATRÓN MORENO

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grados aprobados y no pueden ser explotados comercialmente sin autorización

DEDICATORIA

Doy gracias a Dios por permitirme cumplir con éxitos todos estos años de estudio, A mis padres, por su apoyo incondicional y esfuerzos para brindarme mis estudios. A toda mi familia por estar conmigo, en los momentos buenos y malos dándome ánimos para seguir adelante.

Jose A. Barreto Guerra.

DEDICATORIA

Doy gracias a Dios, ya que me dio las fuerzas para no desfallecer, a mis padres que serán siempre el motor de mi vida, a mi familia que me motivó seguir adelante, a mis compañeros de trabajo por apoyarme siempre.

Javier E. Patrón Moreno

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A nuestro director, Ingeniero **GONZALO GARZÓN.** Por su constante colaboración y apoyo durante el desarrollo de nuestra monografía.

Al ingeniero**, Isaac Zúñiga** por su colaboración clave, en el enfoque del desarrollo de nuestra monografía.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE DIAGRAMAS

Pág.

RESUMEN

El control de congestión tiene una gran importancia para el mejoramiento de la congestión en la red. Lo que implica todo un conjunto de técnicas para detectar y corregir los problemas que surgen cuando no todo el tráfico ofrecido a una red puede ser cursado, con los requerimientos de retardo, u otros, necesarios desde el punto de vista de la calidad del servicio. Por tanto, es un concepto global, que involucra a toda la red, y no sólo a un remitente y un destinatario de información, como es el caso del control de flujo.

Sin embargo, se ha propuesto varios algoritmos para el control de congestión, los cuales como en el caso de los algoritmos de encaminamientos, se pueden clasificar de varias formas. La más lógica consiste en dividirlas en dos clases: en bucle abierto y en bucle cerrado.

Los algoritmos en bucle abierto evitan la concurrencia(es decir sistemas que permiten que múltiples procesos sean ejecutados al mismo tiempo), de la congestión, asegurando que el flujo de tráfico generado por el origen no degradara las prestaciones de la red mas allá de las QoS especificada. Si no se puede garantizar la QoS requerida, la red deberá rechazar el flujo de tráfico. La función a través del cual se toma la decisión de aceptar o rechazar el flujo de tráfico se llama control de admisión.

Por otro lado el algoritmo de bucle cerrado se hace llamar así, porque el estado de la red se conoce el punto donde se regula el tráfico, generalmente el origen. Además no suelen realizar reserva de recursos alguna.

Es importante hacer notar que los algoritmos de control de congestión constituyen una forma efectiva de reducir sobrecargas temporales en la red (generalmente, del orden de varios milisegundos). Si la sobrecarga dura mucho más de este tiempo (varios segundos o incluso minutos), el encaminamiento adaptable puede ayudar evitando los nodos y los enlaces congestionados. Si el periodo de sobrecarga es aun mayor debe actualizarse la red mediante, por ejemplo, la introducción de enlaces de mayor capacidad, conmutadores mas rápidos, en otros.

Por otra parte se tienen herramientas de monitorización que permiten detectar fallos o errores que generan congestión en la red, con sus respectivos dispositivos utilizados para controlar el funcionamiento de la red; a través de un software de gestión de red. Uno de los más utilizados es el **Network inspector,** el cual permite realizar un seguimiento y diagnostico de forma activa y rápida los problemas en entornos a TCP/IP. Así como también la herramienta Network Protocol Inspector, el cual radica la administración en elemento de gestión de red que permita monitorizar y controlar los procesos de congestión en la red.

INTRODUCCIÓN

Día a día se hace más notable el crecimiento de las redes. La cantidad de usuarios que se conectan en la red se ha incrementado mucho mas, por lo cual se requiere de mayor tratamiento con respecto a las aplicaciones que los usuarios manejen a la hora de satisfacer sus necesidades. Un factor muy importante es el de la congestión, el cual provoca mucho tráfico en la red.

Este trabajo de monografía se concentrará en los diferentes métodos formales de verificación de errores con fines de mejoramiento de la calidad de servicio (QoS), en la redes. Entre esos métodos se encuentran el control de congestión que opera de una forma efectiva en reducir sobrecargas temporales en la red. Como también la parte de monitoreo, el cual con sus respectivas herramientas se pueden utilizar para tener un mejor control del funcionamiento dentro la red, para diferentes usuarios para la satisfacción de sus necesidades.

1. CAPÌTULO

EL PROBLEMA DE LA INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

1.2. OBJETIVOS

1.3. JUSTIFICACIÓN

1.1. BREVE DESCRIPCIÓN DEL PROBLEMA

En la actualidad el auge de las redes de datos ha sido vital en el funcionamiento de cualquier empresa u organización. Donde se encuentra muchas ventajas pero de igual forma distintas maneras de cómo ese soporte puede afectar su rendimiento en una determinada red de datos, Así como también en las prestaciones de servicio (QoS). Por lo tanto es necesario saber como funcionan y como se ocasionan esos problemas, a través de distintos métodos de combatir la congestión los cuales puedan implementarse para llegar a tener mayor estabilidad y mejoría en la calidad del servicio.

1.2. OBJETIVOS

1.2.1. Objetivo General

Estudiar y documentar el problema de la congestión en redes como generador de inconvenientes que afectan la calidad de servicio (QoS), con el fin de facilitar la administración de una red.

1.2.2. Objetivos Específicos.

Definir el concepto de congestión y sus respectivas implicaciones adquiridas en la red.

Analizar los aspectos más relevantes en el diseño de una red con el fin de diagnosticar las posibles congestiones que se pueden presentar.

Describir el mecanismo de monitoreo que ofrecen herramientas que permiten detectar la congestión en la red, para lograr un mayor funcionamiento y calidad de servicio (QoS).

1.3. JUSTIFICACIÓN

Las redes de datos se han convertido en el soporte tecnológico, para cualquier organización por lo que la implementación de una red se hace cada día más indispensable para las empresas en su ámbito de automatización.

A pesar que este es un tema muy estudiado en los programas de Ingeniería de Redes se pretende en focalizar los aspectos más relevantes y en los esquemas que ayudaran a resolver cualquier problema que se presente y que altere el correcto funcionamiento de una Red de Datos.

Actualmente este problema de Congestión en las redes, es muy importante por que a pesar de que las tecnologías avanzan de igual manera estos problemas siempre saltan a la vista y se hace necesario tener técnicas y formas sencillas de poder evitar o solucionar en el momento en que se pueda presentar.

Con el avance que se tenga de este tema de la congestión, se va a hacer muy notorio como surgen estos problemas y como se implementan sistemas o software de gestión de una red, que en la actualidad es una herramienta utilizada por los administradores de red para poder realizar controles en las mismas.

2. CONGESTIÓN EN LA RED

2.1. LA CONGESTIÓN

2.2. CONTROL DE FLUJO

2.3. CONTROL DE CONGESTIÓN

2.4. GESTIÓN DE TRÁFICO

2.5. MECANISMOS DE CONTROL DE CONGESTIÓN

2.1 LA CONGESTIÓN

La congestión en una red es definida como una excesiva cantidad de paquetes almacenados en los buffers de varios nodos en espera de ser transmitidos. En donde la congestión es indeseable porque aumenta los tiempos de viaje de los paquetes y retrasa la comunicación entre usuarios.

Para entender este fenómeno de la congestión es necesario analizar el comportamiento de la subred de conmutación de paquete como una subred de colas. En cada nodo, asociado a cada canal de entrada o salida habrá una cola de entrada o salida respectivamente. Si la velocidad de llegada de los paquetes al nodo excede la velocidad con que estos pueden ser transmitidos, la cola asociada al canal de salida empieza a crecer y los paquetes irán experimentando un retardo creciente, que podría llegar a tender a infinito si la longitud de las colas lo permitiera. El retardo crece de forma alarmante cuando la tasa de ocupación de la línea, para la que los paquetes están encolados, sobrepasa el 80%.[1]

Cuando se alcanza el punto de saturación y el nodo no puede absorber más paquetes, tiene dos posibilidades: Rechazar los nuevos paquetes que van llegando. Ejercer un control de flujo sobre sus vecinos, impidiendo el envío de nuevos paquetes.

Ambas estrategias conducirán a la saturación de los nodos vecinos al que inicialmente tenía problemas, debido a que no podrán deshacerse de los paquetes

[1] http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/congest.html

que tenían para enviar. Así, la congestión en un punto de la subred se propaga rápidamente hacia las zonas vecinas.

Por ello, será deseable establecer algún tipo de control para evitar estas situaciones. Donde disminuirá las prestaciones de la subred respecto al caso ideal en una tasa aproximadamente igual a la sobrecarga de control generada; pero evitará que se produzcan situaciones catastróficas que podrían conducir al bloqueo total de la subred.

Actualmente las redes están experimentando un aumento en la transmisión de archivos de gráficos de gran tamaño, imágenes, vídeos con movimiento y aplicaciones multimedia, así como un aumento en la cantidad de usuarios de red. Todos estos factores representan una exigencia aún mayor para la capacidad de ancho de banda.

Cuando cada vez más personas utilizan la red para compartir grandes archivos, acceder a servidores de archivo y conectarse a Internet, se produce la congestión de red. Esto puede dar como resultado tiempos de respuesta más lentos, transferencias de archivos más largas y usuarios de red menos productivos debido a los retardos de red. Para aliviar la congestión de red, se necesita más ancho de banda o bien, el ancho de banda disponible debe usarse con mayor eficiencia.

El caudal depende del tipo de red y tiene un valor nominal máximo, que no podremos superar en ningún caso. Pero además, la red no ofrece el mismo caudal real si se le ofrece poco tráfico o si se le ofrece mucho[2]. Por ejemplo la siguiente figura:

[2] http://www.it.uc3m.es/~prometeo/rsc/apuntes/Conges/conges.html

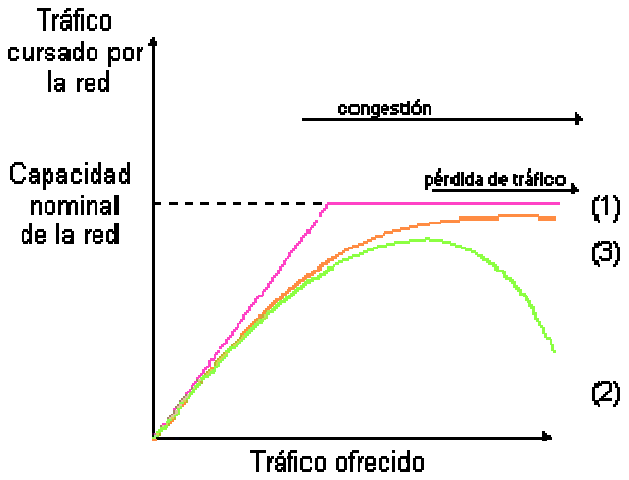


Figura 1. Caudal en función del tráfico ofrecido

http://www.it.uc3m.es/~prometeo/rsc/apuntes/Conges/conges.html

En esta figura la curva **(1)** representa el comportamiento ideal de la red. Hay linealidad hasta llegar a la capacidad nominal de la red, momento en el que el tráfico cursado se satura. La curva **(2)** representa el comportamiento real típico de una red. Como puede observarse, al llegar a la zona de saturación, cuanto más tráfico hay ofrecido, menos tráfico se cursa.
Esto es debido, por ejemplo, a que los paquetes tardarán mucho tiempo en llegar a su destino, y mientras tanto serán retransmitidos por la fuente, pensando que se han perdido por el camino.

Esto, a su vez, origina una explosión de tráfico, ya que cada paquete es retransmitido varias veces, hasta que consigue llegar a tiempo al destino. Para evitar esa degradación, se introduce el control de congestión que trata de aproximar el comportamiento de la red al dado por la curva **(3)**, evitando así entrar en una zona de degradación.

2.2. CONTROL DE FLUJO

Es una técnica que permite sincronizar el envío de información entre dos entidades que producen o procesan el envió a distintas velocidades. Por ejemplo, como se muestra en la siguiente figura 2.

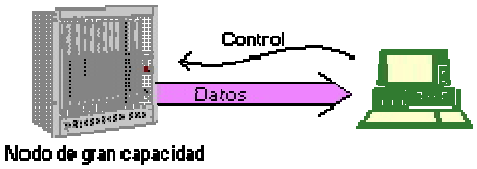


Figura 2. Conexión entre nodo de alta capacidad y PC

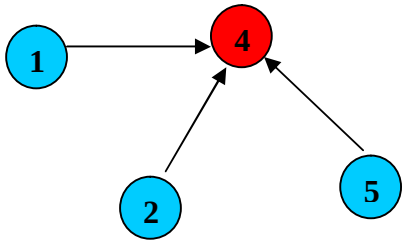
http://www.it.uc3m.es/~prometeo/rsc/apuntes/Conges/conges.html

En este caso, dada la gran velocidad a la que produce y envía información, el nodo desborda al PC, por lo que éste debe enviar información de control (control de flujo) para que el nodo reduzca su tasa de envío de datos. De esta forma, deteniendo a la fuente cada cierto tiempo, el PC puede procesar el tráfico que le envía el nodo.

2.3. CONTROL DE CONGESTIÓN

El problema de la congestión tiene lugar cuando existen demasiados paquetes que tratan de acceder a la misma memoria temporal en un conmutador. Un ejemplo, que describe como funciona la congestión en una red de

comunicaciones de la figura 3, donde los nodos 1,2 y 5 envían ráfagas de paquetes al nodo 4 de forma simultanea, y que la velocidad total de llegada de paquetes es mayor que la velocidad a la que estos pueden transmitirse.



En este caso, la memoria temporal del nodo 4 se comenzara a llenar. Si esta situación dura demasiado, empezará a rechazar paquetes. Cuando un destino detecta la pérdida de paquetes, puede requerir al emisor su retransmisión, la cual puede llevarse a cabo y empeorar aun más la situación de la congestión.

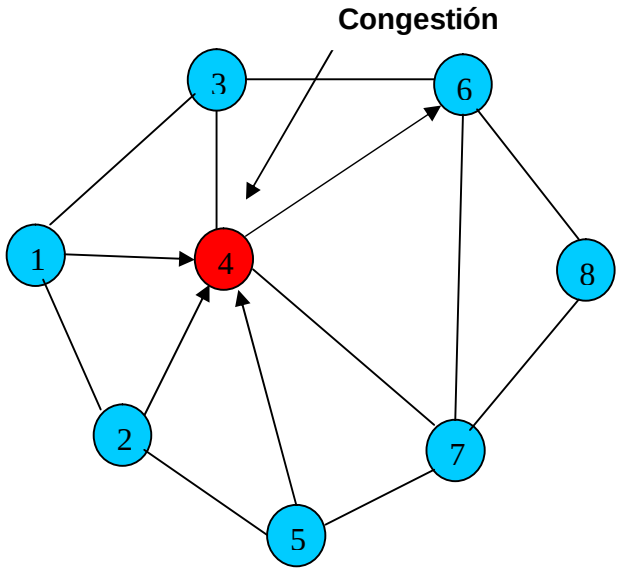


Figura 3. Congestión en un nodo

LEÓN, Alberto G. Redes de Comunicación

Esto provocara a su vez que el nodo 4 rechace más paquetes y solicite nuevas retransmisiones por parte del receptor. Aquí se tiene un concepto global, que involucra a toda la red, y no sólo a un remitente y un destinatario de información, como es el caso del control de flujo.

Por lo tanto el rendimiento será muy bajo en el destino (grafica de congestión no controlada). El objetivo del control de congestión es eliminar o reducir la congestión, lo cual, si se hace adecuadamente, mejorara las prestaciones (grafica de congestión controlada). [3]

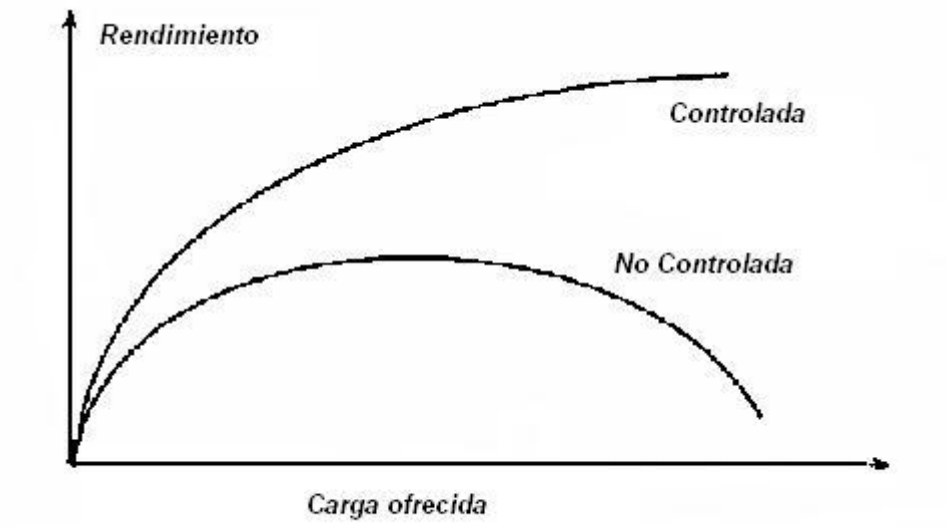


Figura 4. El rendimiento decae cuando se produce la congestión

[3] LEÓN, Alberto G. Redes de Comunicación

2.3.1. Técnicas de control de congestión

Estas son algunas técnicas de control de congestión usadas en redes de conmutación de paquetes, de retransmisión de tramas y ATM y en interconexiones basadas en IP.

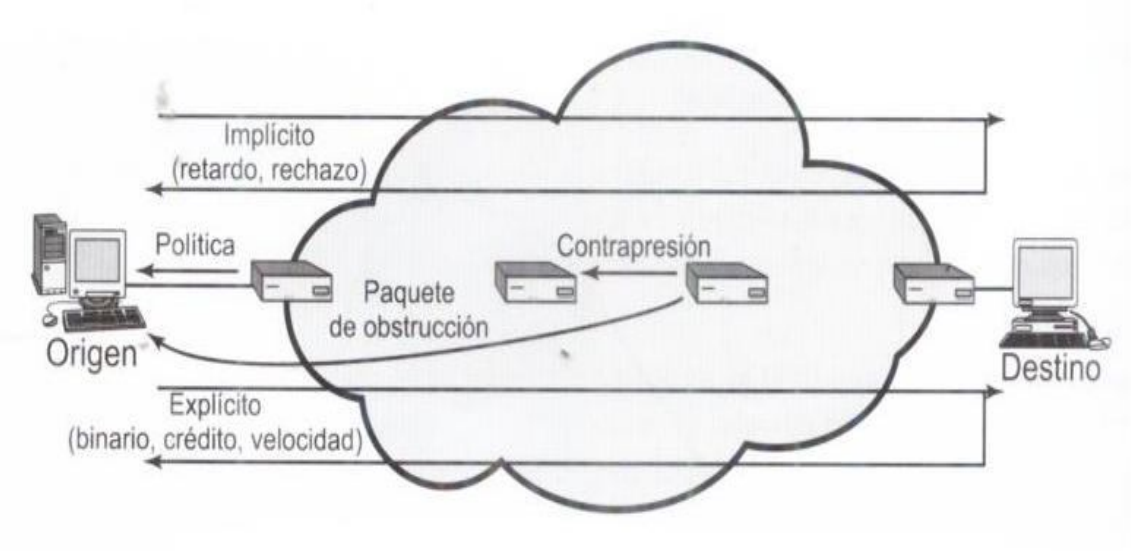


Figura 5. Mecanismo de control de congestion

STALLINGS, William, Comunicaciones y redes de computadores, Pág. 414-416

2.3.1.1 Contrapresión

Esta técnica produce un efecto similar a la contrapresión en fluidos que caen por un tubo. Cuando el extremo del tubo esta cerrado (u obstruido) el fluido realiza una presión hacia atrás en el tubo hasta el punto de origen, en donde el flujo es detenido o frenado.

La contrapresiona se puede realizar a nivel de enlaces o de conexiones lógicas por ejemplo en circuitos virtuales. Además se puede aplicar de forma selectiva a las conexiones lógicas, de manera que el flujo desde un nodo al siguiente solo s e reduzca o se pare para algunas conexiones, generalmente para aquellas con mayor tráfico. En este caso, la retracción se propagará hacia atrás los emisores a lo largo de las conexiones en cuestión.

2.3.1.2 Paquetes de obstrucción

Estos paquetes de obstrucción son paquetes de control generado por un nodo congestionado y transmitido hacia atrás hacia un nodo de origen a fin de reducir el filtro de tráfico. Un ejemplo de paquete de obstrucción es el paquete, ralentización del emisor (Source Quench) usado en el ICMP (Protocolo de mensajes de control de internet). Tanto un dispositivos de encaminamiento como un sistema final destino pueden llevar a cabo el envío de este mensaje hacia un sistema final de origen solicitando la reducción de la velocidad a la que este emite trafico hacia la internet de destino.

2.3.1.3 Señalización implícita de congestión

Cuando se produce la congestión en la red, pueden suceder dos cosas, como ya se ha mencionado: (1) El retardo de transmisión de un paquete dado desde un emisor hasta un destino aumenta hasta ser apreciable mayor que el término de retardo de propagación fijo, y (2) se rechazan paquetes. Si un emisor es capaz de detectar el incremento en los retardos y en el rechazo de paquetes, tiene una evidencia explicita de la congestion en la red.

Por lo tanto si todos los emisores pueden detectar la ocurrencia de congestion y, en respuesta a ella, reducir el flujo, de dicha congestion se podrá aliviar. Así pues, el control de congestion en base a la señalización implícita es responsabilidad de los sistemas finales y no precisa acción alguna por parte de los nodos de la red.

2.3.1.4 Señalización explícita de congestión

En terminas generales, para evitar explícitamente la congestion, la red alerta a los sistemas finales acerca del incremento de la congestion en la red y estos toman las medidas oportunas para reducir la carga de entrada en la red.

Las técnicas de señalización explícita de congestión se pueden dividir en tres categorías generales:[4]

- Binarias: se activan un bit en un paquete de datos transmitido por un nodo congestionado, de modo que un emisor puede reducir el flujo de trafico cunado recibe una indicación binaria de congestion sobre una conexión lógica.

- Basadas en crédito: estos esquemas son usuales para el control de flujo extremo a extremo, en el que un sistema destino hace uso de crédito para evitar que el emisor provoque el desbordamiento de las memorias temporales de recepción, así como el limite como para llevar a cabo el control de congestión.

- Basadas en velocidad: estos esquemas proporcionan un límite explicito de velocidad para el emisor sobre una conexión lógica, de forma que el origen solo puede transmitir datos por debajo de este límite. Para controlar la congestion,

[4] STALLINGS, William, Comunicaciones y redes de computadores, Pág. 414-416 ,

cualquier nodo a lo largo del camino de la conexión puede reducir el límite de la velocidad mediante el envío de un mensaje de control hacia el emisor.

2.4 GESTIÓN DE TRÁFICO

Existen numerosas cuestiones relacionadas con el control de congestión que podrían incluirse bajo el concepto de gestión de tráfico. Cuando un nodo se satura y debe rechazar paquetes se puede aplicar alguna regla sencilla como la consistente en el rechazo de los paquetes mas recientemente recibidos.

Sin embargo se pueden utilizar otras consideraciones para mejorar la aplicación de las técnicas de control de congestión y de la política de rechazo.

2.4.1 Imparcialidad

A medida que aumentan la congestión, los flujos de paquetes entre los emisores y los destinos sufrirán aumento en los retardos y, para la congestion, perdidas de paquetes. Un ejemplo de una técnica que podría se adecuada consiste en el mantenimiento por parte de los nodos de una cola separada para cada conexión lógica o para cada pareja origen-destino. Si todas las memorias temporales asociadas a las colas tienen el mismo tamaño, las colas con mayor tráfico sufrirán rechazos mas a menudo, permitiendo q las conexiones con bajo tráfico compartan la capacidad.

2.4.2 Calidad de servicio

Es especialmente importante que durante los periodos de congestion los flujos de trafico con distintos requisitos sean tratados de forma diferente y se les asigne una calidad de servicio (QoS) diferente. Un ejemplo, un nodo puede transmitir en la misma cola paquetes de alta prioridad con referencia sobre paquetes con prioridad menor; o un nodo puede mantener diferentes colas con distintos niveles QoS y dar prioridad a los niveles superiores. [5]

2.4.3 Reservas

Una forma de evitar la congestion y asegurar al mismo tiempo un servicio de una calidad dada para aplicaciones es el uso de un esquema de reserva. Donde un esquema de este tipo es una parte integral de las redes ATM. Cuando se establece la conexión lógica, la red y el usuario llevan a cabo un acuerdo de tráfico en el que especifica una velocidad de transmisión, además de otras características del flujo de tráfico.

Un aspecto importante del esquema de reservas es el que hace referencia ala política del tráfico (como en la figura). Un nodo de la red, generalmente el nodo al que se encuentra conectado el sistema final, supervisa el flujo de tráfico y lo compara con el acuerdo realizado, de forma que el exceso de tráfico se descarta o se marca para indicar que es susceptible de ser rechazado o de sufrir un retardo.

[5] STALLINGS, William, Comunicaciones y redes de computadores, Pág. 416- 417,

2.5. MECANISMOS DE CONTROL DE CONGESTIÓN

El problema del control de congestión puede enfocarse matemáticamente desde el punto de vista de la teoría de control de procesos, dependiendo en general de los requisitos de aplicación (por ejemplo , calidad de servicio).y según esto se han propuesto varios algoritmos para el control de congestión, los cuales se dividen soluciones de bucle abierto y bucle cerrado.

2.5.1. Solución en bucle abierto.

El control de congestión en bucle abierto no hace uso de información de realimentación para regular el flujo de trafico, sino que en esta técnica se asume que, una vez aceptado un origen, su flujo de trafico no sobrecargará la red.

Las soluciones de bucle abierto que también combaten la congestión de las redes mediante un adecuado diseño de las mismas. Existen múltiples variables con las que el diseñador puede jugar a la hora de diseñar la red. Estas variables influirán en el comportamiento de la red frente a la congestión.[6]

[6] LEÓN, Alberto G. Redes de Comunicación

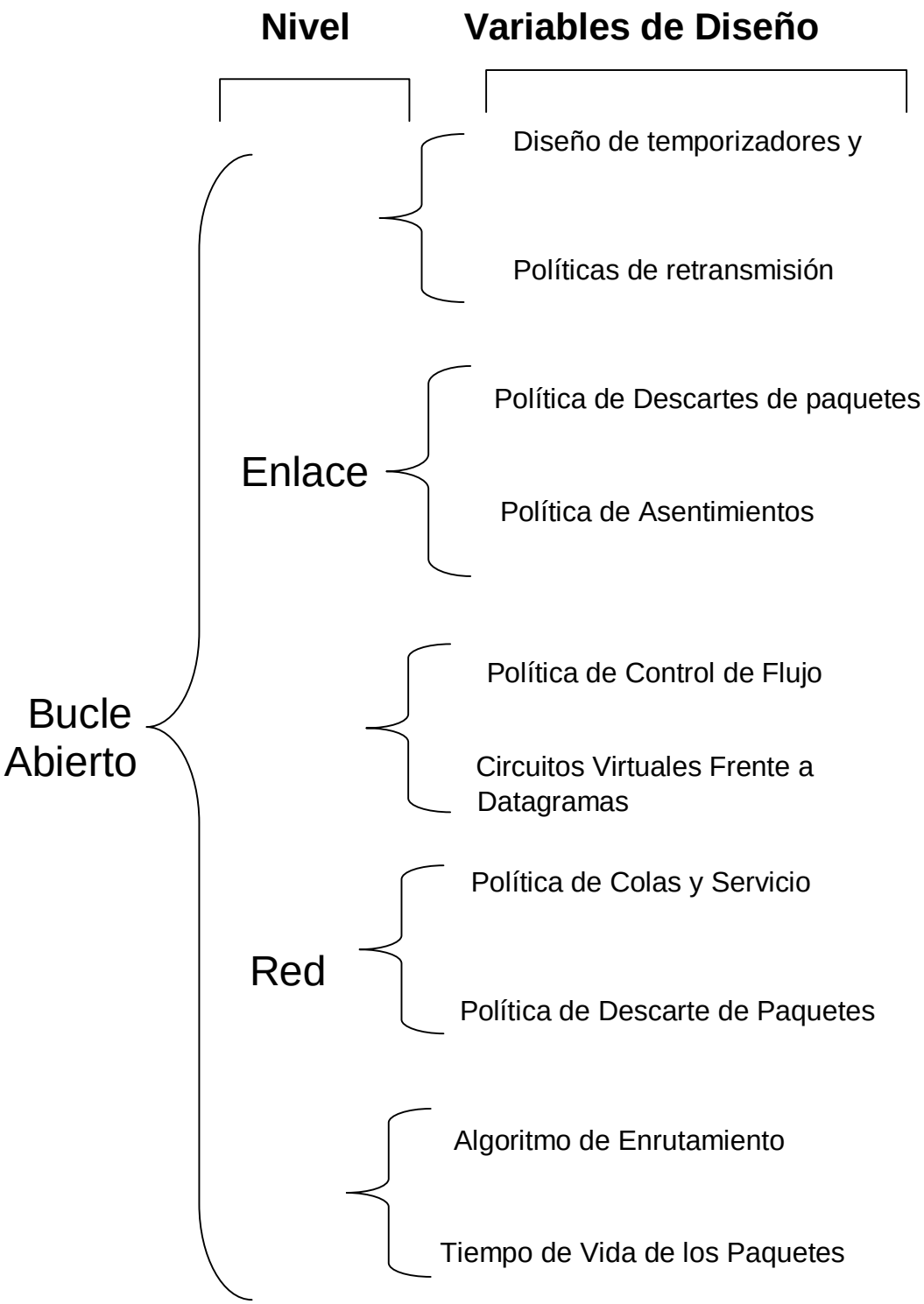

Nivel
Variables de Diseño
Diseño de temporizadores y
Políticas de retransmisión
Enlace
Política de Descartes de paquetes
Política de Asentimientos
Bucle Abierto
Política de Control de Flujo
Circuitos Virtuales Frente a Datagramas
Red
Política de Colas y Servicio
Política de Descarte de Paquetes
Algoritmo de Enrutamiento
Tiempo de Vida de los Paquetes

Diagrama 1.

2.5.1.1. Control de Admisión

Esta es una técnica de control de congestión en bucle abierto preventiva. Fue originalmente propuesta para redes de conmutación de paquetes mediante circuitos virtuales tales como a.m., aunque también para el uso en redes de datagramas. El control de Admisión trabaja generalmente de modo conexión, peor puede ser también de modo de ráfagas.

La idea principal de a.C. (*Connection Admisión Control),* es muy simple: cuando un origen solicita un establecimiento de conexión, CAC decide aceptar o rechazar la conexión. Si se puede satisfacer la QoS de todos los orígenes que comparten el mismo camino, la conexión se aceptará. La QoS se puede expresar en términos de retardo máximo, probabilidad de perdidas, varianza de retardo y otros parámetros de prestaciones.

Para que CAC pueda determinar si se cumple la QoS debe conocer el flujo del tráfico de cada origen. Así, cada uno de ellos debe especificar su flujo de tráfico, mediante un conjunto de parámetros de tráfico, llamado descriptor de tráfico, durante el establecimiento de la conexión. Un descriptor de tráfico pude contener la velocidad de pico, la velocidad media, el tamaño máximo de ráfaga, y se supone que describe de forma compacta y adecuada el flujo de tráfico.[7]

[7] LEÓN, Alberto G. Redes de Comunicación

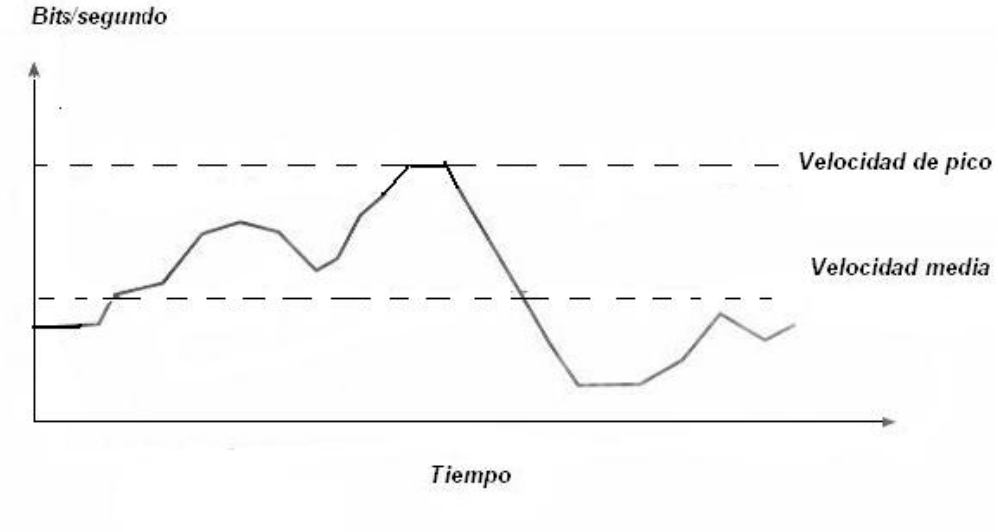


Figura 6. Ejemplo Flujo de tráfico

En esta figura se muestra un flujo de tráfico generado por un origen, inclinándose la velocidad de pico y media. El tamaño máximo de ráfaga hace referencia generalmente al tiempo máximo durante el que se genera el tráfico a la velocidad de pico. [8]

Por lo tanto CAC debe calcular la cantidad de ancho de banda que debería reservarse para el origen formando como base las características del flujo de tráfico, cantidad que suele estar comprendida entre la velocidad media y la de pico y que se conoce como ancho de banda efectivo del origen.

[8] LEÓN, Alberto G. Redes de Comunicación

2.5.1.2. Supervisión

Una vez que ha aceptado una conexión a través de CAC, la QoS se satisfacerá si el origen respeta el descriptor de trafico especificado durante el establecimiento de la llamada. Por el contrario, si el flujo de tráfico viola en contrato inicial, puede que la red no sea capaz de mantener un nivel de prestaciones aceptable. Para evitar que el origen incumpla su contrato, la red puede monitorizar el flujo de tráfico durante la duración de la conexión.

El proceso de monitorización y hacer cumplir el contrato del flujo de trafico se conoce como *supervisión de trafico.* Cuando se viola el contrato acordado, la red puede elegir entre el rechazo o el etiquetado del trafico que lo incumple. El tráfico etiquetado se transmitirá por la red, pero con baja prioridad, y en caso de congestión será el primero que se pierda.

2.5.1.3. Algoritmo del cubo con escape

La mayoría de las implementaciones de la función de supervisión de tráfico hacen uso de este algoritmo. Su funcionalidad es como tener el flujo de trafico para el dispositivo de superviso o control como el agua vertida en un cubo con un agujero en su fondo.

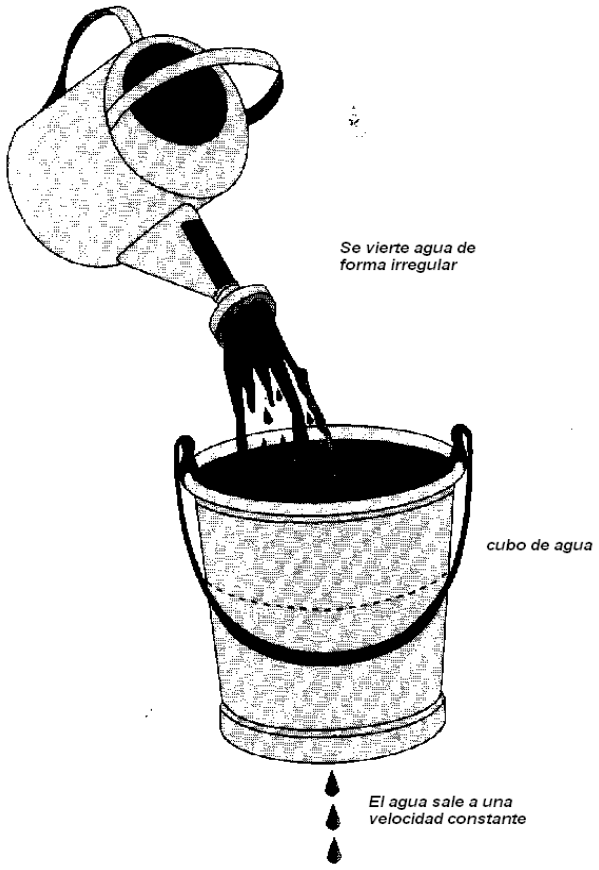


Figura 7. Cubo de escape
LEÓN, Alberto G. Redes de Comunicación

El cubo tiene una cierta profundidad con una velocidad constante cuando no esta vació. Un contenedor (es decir, un paquete) de agua se declara conforme si el cubo no rebosa cuando se vierte en el. El rebosamiento se producirá si el paquete es demasiado grande o si el cubo estaba casi lleno debido al vertido de paquetes anteriores.

La profundidad del cubo se emplea para absorber las irregularidades en el flujo de agua, de modo que si se prevé que este sea suave, el cubo puede ser poco profundo, mientras que si es a ráfagas, el cubo deberá tener una mayor

profundidad. La velocidad de salida o drenado se corresponde a la velocidad de trafico que se desea(es decir el control).[9]

2.5.2. Solución bucle cerrado

El control de congestión en bucle cerrado se basa en el empleo de información de realimentación para regular la velocidad del origen. Este algoritmo de bucle cerrado reacciona ante la congestión cuando está ya produciendo, o cuando se va a producir, generalmente regulando el tráfico de acuerdo al estado de la red.

Esta información puede ser implícita o explicita. En la implícita, el origen puede considerar un valor de tiempo máximo para decidir si ha producido congestión en la red. En cambio, en la realimentación explicita se envía el origen de un mensaje explicito para indicarle el estado de congestión de la red.

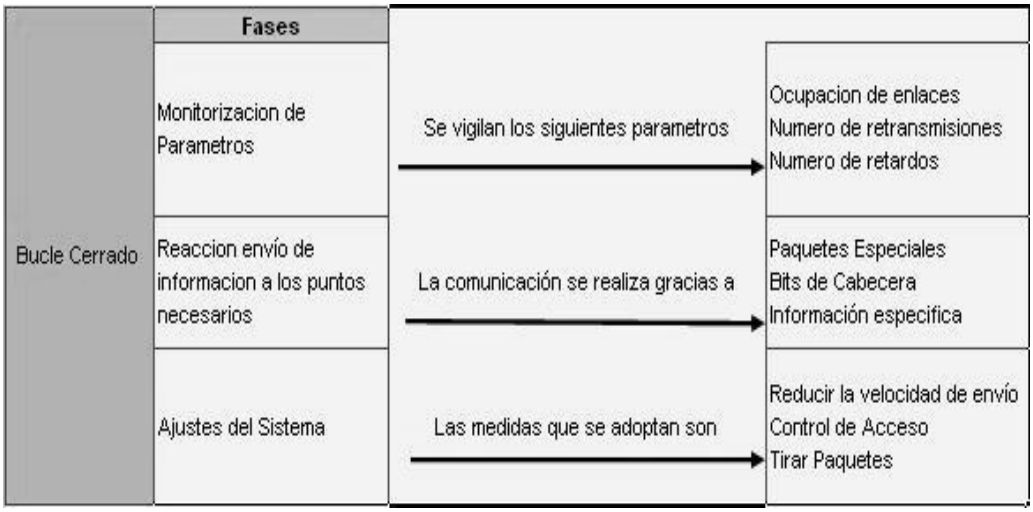


Diagrama 2.

[9] LEÓN, Alberto G. Redes de Comunicación

2.5.2.1. Monitorización de parámetros.

La monitorización, es poder observar el crecimiento de la red, para poder planificar su ampliación y la adaptación de servicios nuevos antes de que la red se colapse por el tráfico. Por esto se vigilan los siguientes parámetros:

- Ocupación de los enlaces y de los buffers (colas de espera en los nodos)
- Porcentaje de descartes
- Número de retransmisiones

Los Retardos y "jitters". Los cuales son oscilaciones de la separación temporal entre paquetes. En aplicaciones que requieren sincronización (videoconferencia, sincronizar audio con video),[10] es muy importante que esas oscilaciones sean pequeñas. Como también es importante la reacción, en el envió de información de los puntos necesarios. Donde la comunicación se realiza gracias a:

Paquetes especiales: Los cuales no están sometidos a control de congestión y se saltan las colas de espera en los nodos. Enviando el nodo que, gracias a la monitorización, ha detectado la congestión.

Bits de cabecera: En los paquetes enviados, indico en la cabecera que empieza a haber congestión. (Ejemplo Frame Relay).

Información específica: Si se recibe una alerta de congestión (mediante bits de cabecera de paquetes que circulan por la red), se solicita más información.

[10] http://www.it.uc3m.es/~prometeo/rsc/apuntes/Conges/conges.html

3. CAPÍTULO

HERRAMIENTAS DE MONITORIZACIÓN PARA LA CONGESTIÓN EN LA RED.

3.1. LA MONITORIZACIÓN DE LA CONGESTIÓN EN LA RED

3.2. SOFTWARE DE GESTIÓN NETWORK INSPECTOR

3. HERRAMIENTAS DE MONITORIZACIÓN DE CONGESTIÓN EN LA RED

3.1 MONITORIZACIÓN DE LA CONGESTIÓN EN LA RED

Monitorizar una red es un proceso complejo. Muchos factores intervienen en el rendimiento de una red. Un servidor de bases de datos nuevos, que envía una base de datos completa a los usuarios que solo necesita un breve informe, puede incrementar de repente la carga en la red.

Una aplicación cliente servidor que este mal diseñada puede ir cargando la red de forma gradual, a medida que los usuarios se vayan fijando en ella y la vayan utilizando. Un servidor de red que no este ajustado pude formar embotellamiento a medida que los usuarios se vayan poniendo de la cola para acceder a ese servidor. Un servidor de impresora nuevo puede trasmitir con tanta frecuencia el incremente de traficote la red.

La clave para solucionar este tipo de problemas es en disponer de herramientas para la monitorización de la red y llegar a ser un experto en su manejo.

3.1.1 Tráfico en La Red

La mejor manera de llegar a conocer una red es utilizar las herramientas de monitorización para estudiar las características que tiene el tráfico de red y realizar pruebas comparativas del rendimiento de la red. Las pruebas comparativas proporcionan una base para poder realizar una comparación de los datos

recopilados durante situaciones problemáticas con los datos obtenidos en situaciones en las que el tráfico de la red es normal. Siendo así, una forma de diagnosticar los problemas.[11]

Puntos de Referencias para el diagnostico del problema.

- Generando estadísticas de la CPU, del disco, de la memoria y de la entrada/salida sin que haya usuarios en el sistema, establecer una referencia para poder comparar con los periodos en los que haya usuarios.

- Utilizando el monitoreado del rendimiento para establecer los periodos de máxima, media y mínima actividad.

- Recopilando estadísticas de rendimiento de los periodos de máxima, media y mínima actividad para cada aplicación de software nueva que se instala.

- Haciendo seguimiento de la utilización de los servidores, por ejemplo el incremento de usuarios, de software y en la cantidad de tiempo, por término medio, que los usuarios que están conectados al sistema.

3.1.3 Protocolo simple de gestión de red (SNMP)

Este protocolo SNMP (Simple Network Management Protocol) es muy utilizado, que permite a los administradores de la red monitorizar la actividad de la red constantemente. SNMP se desarrollo como una alternativa al estándar OSI para la

[11] PALMER Michael J. Redes Informáticas

administración de la red: el protocolo de información de gestión común (CMIP Common Management Interfaces Protocol).CMIP ha tardado en aparecer y provoca una sobrecarga en el sistema. Muchos fabricantes han escogido SNMP en el lugar de CMIP por su sencillez.

Una ventaja del protocolo de SNMP es que puede funcionar de forma independiente de la red, lo que significa que no depende de una conexión bidireccional a nivel de protocolo con otras entidades de red. Esta cualidad permite que este protocolo analizar la actividad de la red, por ejemplo poder detectar paquetes incompletos y observar la actividad de transmisión sin depender de la posible falta de información de un nodo que este fallando.[12]

Como también tiene la ventaja de que las funciones de administración se realizan en una de las estaciones de trabajo de la red (NMS). CMIP, sin embargo, realiza la gestión de la red en los propios nodos de la red que están siendo gestionados.

3.1.4 Dispositivos para monitorizar la red

Estos dispositivos abarcan desde simples medidores de tensión hasta complicados analizadores de protocolos. Los dispositivos que tienen mas funciones de monitorización de red también tienen un precio superior.

Si se dispone de una red pequeña, compuesta por 10 o 20 estaciones de trabajo, probablemente se necesite un equipo sencillo, por ejemplo voltímetros o polímetros. Si se administrando una red empresarial con cientos de nodos, se necesitaran varios equipos, como un analizador de protocolos.

[12] PALMER Michael J. Redes Informáticas

Algunos ejemplos de dispositivos para monitorear y medir parámetros de red.

- Voltímetros, polímetros y medidores de potencia óptica.
- Escáner de cable
- Medidor de transceptores
- Analizador Mau
- Reflectometro de domino temporal
- Analizador de protocolos

3.2. SOFTWARE DE GESTION NETWORK INSPECTOR

La herramienta Network Inspector es una solución exclusiva que realiza un seguimiento y diagnostica de forma activa y rápida los problemas en entornos TCP/IP, IPX y NetBIOS.

Network Inspector, cuyo diseño es utilizado para redes Ethernet LAN, identifica rápidamente si los problemas encontrados se ubican en un servidor, cliente, conmutador, enrutador o impresora gracias a la veloz detección y la clara visualización de la red.

Es tan práctico ya que, con tan sólo pulsar un botón, puede conseguir un informe de inventario de sus dispositivos IP, IPX, o NetBIOS ubicados en la red, así como de los servicios que éstos ofrecen.

Network Inspector está diseñado con un agente de seguimiento y una arquitectura de consola de visualización. Los agentes pueden distribuirse en la red, de forma

que cada uno realice un seguimiento de un dominio de difusión y que una o varias consolas tengan acceso remoto a los datos recopilados por dichos agentes.[13]

3.2.1. Características

La principal características de la herramienta es la detección exhaustiva de dispositivos Network Inspector detecta rápidamente los dispositivos del dominio de difusión. Con esta detección de dispositivos se obtiene la visibilidad de:

- Tipo/Nombres: Nombres de equipos DNS, IPX® Login y NetBIOS®
- Direcciones: todas las direcciones Inasociadas al nodo y a la dirección MAC
- Servicios disponibles: conmutación, enrutamiento, correo electrónico, Web e impresión
- Interfaces: velocidad y tipo
- Protocolos: IP, IPX y NetBIOS
- Configuración de la interfaz del dispositivo incluyendo velocidad, tipo, MTU, ranura y el conmutador más empleado y los puertos de enrutamiento, así como los dispositivos de cada puerto de conmutación.

[13] FLUKE Network, Network Inspector, Software de seguimiento en la red,

La detección de dispositivos de Network Inspector también ofrece:

- Registro continuo de errores y cambios de los dispositivos de la red para aislar rápidamente los problemas
- Soluciones para los problemas de la red
- Notificación de sucesos por correo electrónico o buscapersonas
- Informes de inventario impresos en formato HTML, incluyendo IP, IPX y NetBIOS

3.2.2 Utilidades

Las utilidades de este software son convenientes y funcionales para la correcta y amplia cobertura de la red. Una de las utilidades es el Potente diagnóstico del conmutador, El análisis gráfico del puerto de conmutación de Network Inspector puede realizarse mediante los puertos más utilizados y editarse en papel o en la Web. Los informes se actualizan cada dos minutos.

Para realizar esta función networks inspector introduce una nueva herramienta se denomina Trace SwitchRoute, esta función le permite ver la ruta exacta mediante los conmutadores que dos dispositivos utilizan para comunicarse, incluyendo la velocidad de los enlaces. Al hacer doble clic en los dispositivos de la ruta se abre una ventana con la relación de sus propiedades, lo que facilita el análisis de los problemas de tráfico.

Otra función es el registro continuo de errores y cambios en los dispositivos de red, Network Inspector busca de forma automática los dispositivos mal configurados, tales como las direcciones IP duplicadas y las máscaras de subred incorrectas. El seguimiento continuo de Network Inspector permite a una aplicación detectar los problemas y obstáculos del dominio de difusión tales como servidores que ya no responden y cambios de dirección IP.[14]

La notificación de acontecimientos es otra funcionalidad de Network Inspector, puede configurarse de forma sencilla para crear una página o un mensaje de correo electrónico cuando se detectan errores en los dispositivos y se sobrepasan los umbrales.

Por ultimo una documentación rápida, todos los resultados de detección de Network Inspector puede editarse tanto en formato estándar como html. Network Inspector ofrece una documentación sencilla con los informes de inventario IP, IPX y NetBios en los que se muestran nombres, direcciones y servicios.

Veamos en unos ejemplos sencillos de algunos pantallazos del software de gestión network inspector, que explicaran que se debe para monitorear una red.

[14] FLUKE Network, Network Inspector, Software de seguimiento en la red,

Funcionamiento del software network inspector

En esta ventana, en el icono **inspector** se muestran todos los dispositivos que contiene la red, y en cada uno de ellos aparece su nombre, su Netbios name, su IP Address y su dirección MAC. Si no tiene nombre aparece por defecto su IP Address.

Refresh: Actualiza la información que viaja en la red.

Sort: Organiza los dispositivos en el panel.

Trace SR: Ejecuta el comando trace al comando seleccionado.

Tools: Muestra varias herramientas de ejecución como ping, telnet, Web etc. Esta opción aparece también en las propiedades de cada dispositivo.

Reports: Genera los reportes.

Net Map: Muestra en forma grafica como estan conectados los swiches, router, servidores y otros dispositivos.

Haciendo clic en el botón del Agente. para que pueda empezarse.

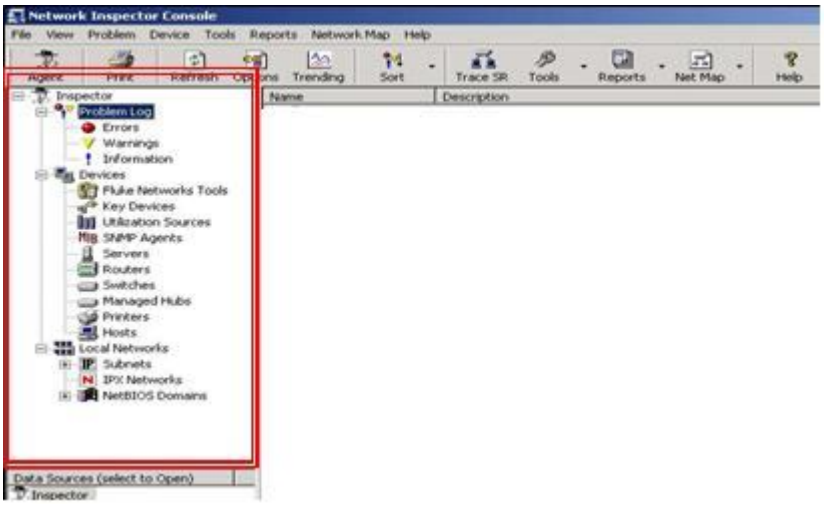
El software de Network Inspector se diseña discretamente, pasivamente y activamente, colecciona o reúne los datos de la red. Como tal, toma tiempo para que los dispositivos aparezcan. La red que se estudia debe descubrirse en un minuto o dos. La colección activa de datos estadísticos se tarda durante los primeros 10 minutos. Una red de la producción real podría tomar 30 minutos o antes de la mayoría de los datos que se revelan.

Menú inspector

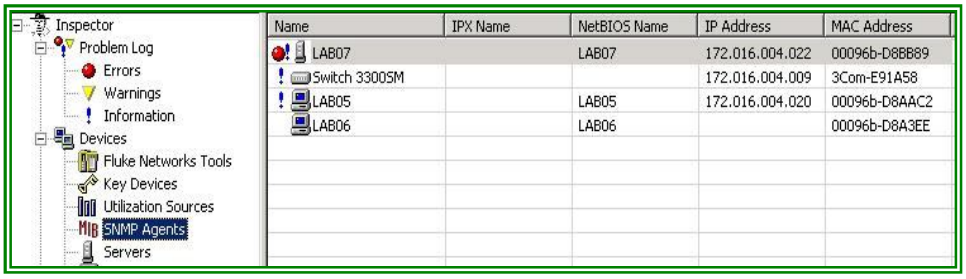
Problem Log: Muestra todos los tipos de errores de cada dispositivo con la descripción del error, advertencia e información de cada dispositivo. Además cuando fue detectado y la última vez que ocurrió.[15]
Existen tres tipos:

- Errors (Errores)
- Warnings (Advertencia)
- Information (Información)

[15] ZUÑIGA, Isaac, S, NETWORK INSPECTOR, UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**,**

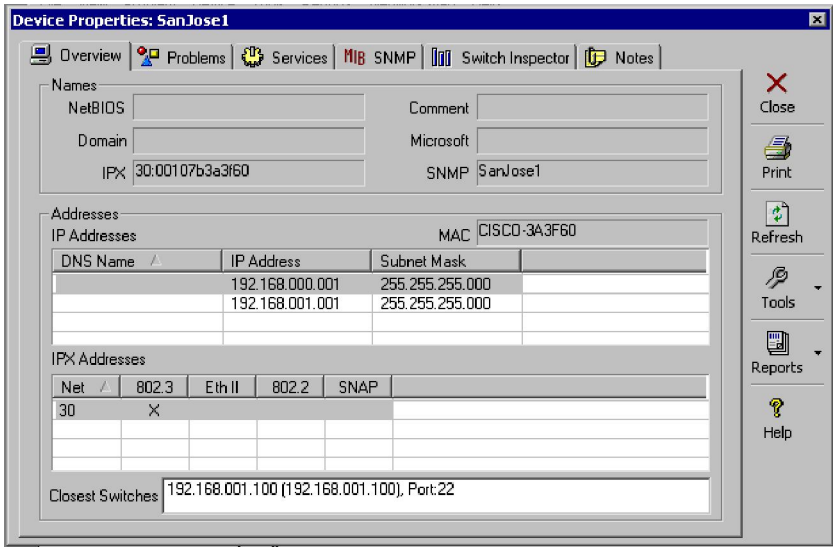


SNMP Agents: Muestra Todos los dispositivos que tienen el servicio SNMP.



Para los iconos Server, Routers Switches Manager Hubs, Printers y Host muestra los dispositivos equivalentes existentes en la red.

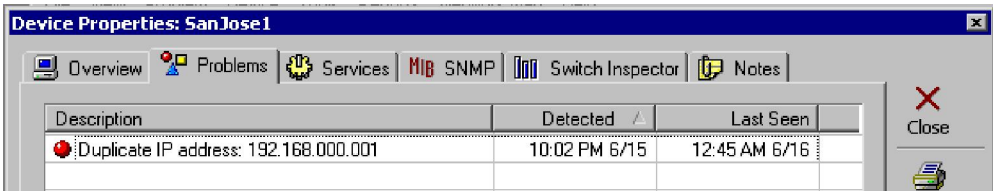
Cuando se hace doble click en el nombre del router y examina las propiedades de los dispositivo disponibles. eso resulta y depende de los dispositivos incluidos en las subredes de la LAN.



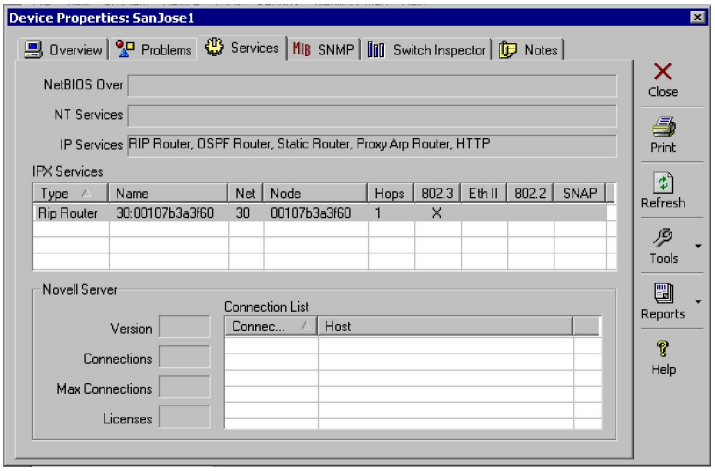
La grafica muestra las propiedades del dispositivo seleccionado, la MAC del fabricante de ese dispositivo y las direcciones IP ligadas a ese dispositivo.

Los interruptores más íntimos sólo aparecerán si a Inspector de la Red se ha proporcionado un SNMP válido para ellos.

La etiqueta Problems, indica que se produce un problema con una dirección IP dentro de la red. Esto ocurre si el administrador configurado duplico una dirección IP, el icono rojo indica ese problema.



La etiqueta de Services revela el IP e IPX Services que corren en las routers.

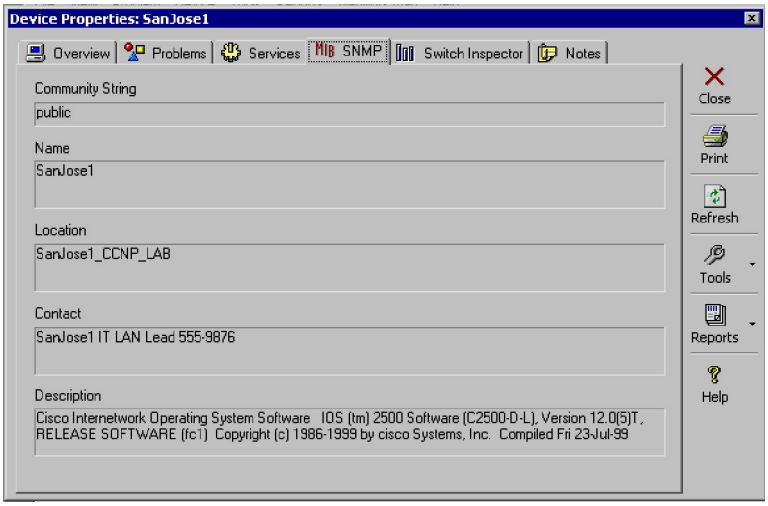


El IP Services en el gráfico revela que la IP tiene servicio de http, esto significa que el router puede accederse vía un navegador de Web.

El IPX Services muestra la ID de la Red de IPX (30), la dirección del Nodo (MAC), y el tipo del marco,

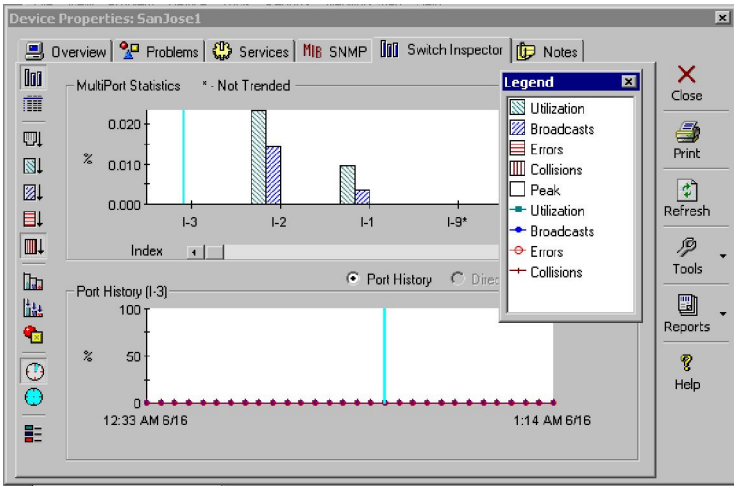
En el fondo de la ventana muestra a la información que se habría revelado si el dispositivo hubiera sido un Servidor de Novell. Un multi-homed servidor que es uno con más de un NIC (la conexión) en las redes separadas, está trabajando como un router o puente.

El MIB la etiqueta de SNMP revela la información de SNMP así como la del router.



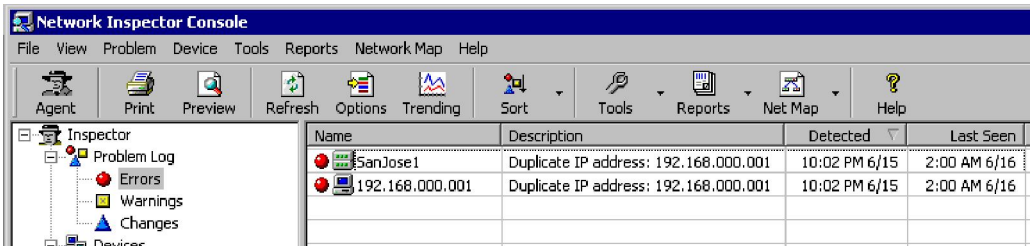
La etiqueta de switch inspector crea una variedad de mapas de los datos de interfaz del switch por el dispositivo seleccionado. Estos datos son reunidos durante el período inicial. La prueba switch inspector mantiene los gráficos de utilización básicos que cualquier SNMP habilitó el dispositivo. El nivel de información ofrecido por esta prueba depende en que MIBs son apoyados por el dispositivo seleccionado. Por ejemplo, desde que Sanjose1 es un router, el programador no puede desplegar directamente la dirección de cualquiera, conectó los dispositivos para un puerto resaltado.

Los botones en el lado izquierdo del cambio de la ventana son para el formato del mapa.

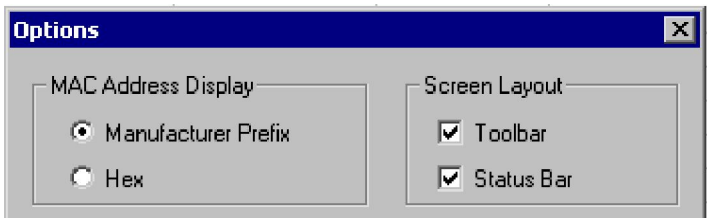


Mientras en el switch inspector, los Informes se abrochan en el lado correcto de la pantalla extenderá para mostrar dos opciones. Seleccione la opción de Actuación de Interruptor y un informe del multi-página con los varios mapas aparecerá en la pantalla. Se examina los resultados y la opción de detalle de Interruptor sólo trabaja con un interruptor.

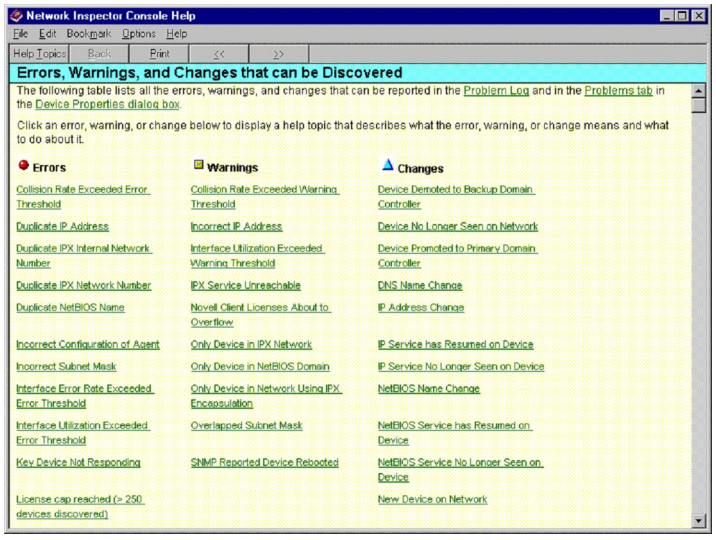
En el ejemplo siguiente, se muestran los Problemas o errores anotando y seleccionando las muestras de los Errores de los dispositivos en el costado derecho. Esto lo hace fácil de descubrir el IP doble y valla al dispositivo.



Haga clic en el botón de las Opciones en el toolbar y note que puede escoger entre el Prefijo del Fabricante y Hechizo. Seleccione el que no es escogido, examine las otras opciones, y entonces haga clic en OK. Note el resultado.



Otra parte de la consola es la opción de ayuda, solo presione F1 y se desplegara toda la ayuda e información que se necesite saber.



3.2.3 Herramientas de Administración de redes.

Aquí se encuentran unas herramientas muy eficaces para la administración de redes, como son los comando: ping y traceroute

Ping: es una de las herramientas más utilizadas y sencilla en la detección de fallas en redes que incluye dos mensajes: solicitud de eco (echo request) y respuesta de eco (echo reply). Ambos son mensajes ICMP (Internet Control Message Protocol) que es un protocolo parte de toda implementación de IP2, y realizan esas simples tareas: "interrogan" a un equipo ubicado según su dirección IP mediante la solicitud de eco, y el equipo interrogado al recibir este mensaje responde con una respuesta de eco. Con este simple mecanismo puede determinarse si un destino es accesible ó nó y si responde. Como puede determinarse en tiempo que se tardó en responder esa información puede suministrarse al usuario, también pueden enviarse múltiples mensajes ICMP de solicitud de eco y proporcionar estadísticas sobre tiempo de respuesta y pérdida de paquetes.

Un ejemplo: problema en la conexión.

Si no puede acceder a una página Web o a un servidor de correo electrónico, y el problema no se soluciona presionando el botón de “actualizar”, Esta herramienta puede ayudar a determinar dónde se encuentra exactamente un problema de la conexión.

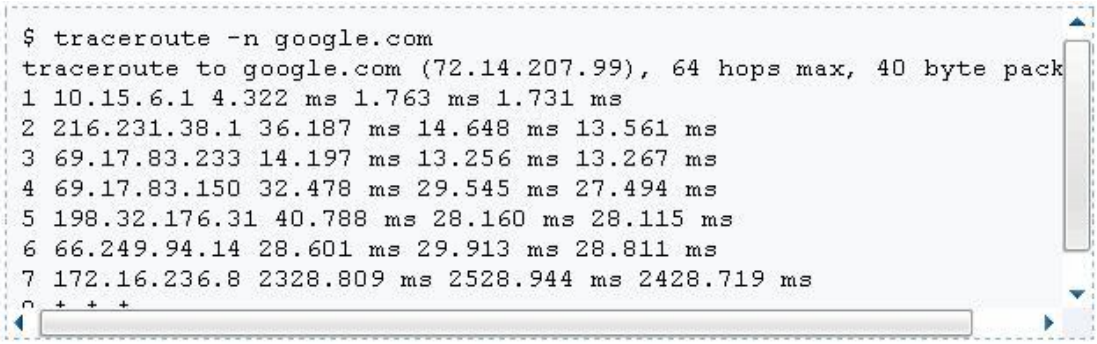
Ping. Casi todos los sistemas operativos (incluyendo Windows, Mac OS X, y por supuesto Linux y BSD) incluyen una versión de la utilidad ping. Utiliza paquetes ICMP para intentar contactar un servidor específico y le informa a usted cuánto tiempo lleva obtener una respuesta.

Saber qué contactar es tan importante como saber cómo hacerlo. Si no se puede conectar a un servicio en su navegador Web (por ejemplo, **http://yahoo.com/),** puede intentar contactarlo:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Si no puede contactar al enrutador por omisión, entonces lo más probable es que tampoco se pueda acceder a Internet. Si tampoco puede contactar otras direcciones IP en su LAN local, es tiempo de verificar su conexión. Si está utilizando cable Ethernet, Si está utilizando una conexión inalámbrica. El diagnóstico de problemas de la red con ping es casi un arte, pero es muy útil. Ya que probablemente se va a encontrar ping en casi cualquier computadora con la que se trabaje, es una buena idea aprender cómo usarlo apropiadamente.

Traceroute: es otra herramienta que hace envía una serie de mensajes UDP a una dirección IP y espera, si recibe respuesta ICMP puede trazar la ruta completa entre los dos puntos extremos (el que envió los mensajes y el destinatario cuya dirección IP se dio).



La opción -n le dice a traceroute que no se preocupe por resolver los nombres en el DNS, y hace que el programa corra más rápido. Usted puede ver que en el salto siete, el tiempo de recorrido de ida y vuelta se dispara a más de dos segundos, mientras que los paquetes parece que se desechan en el salto ocho. Esto puede indicar un problema en ese punto de la red. Si esta parte de la red está bajo su control, vale la pena comenzar sus esfuerzos para resolver el problema por allí.

Otro caso de estudio es el del tiempo lento de respuesta después de implementar las aplicaciones. (Archivo de grafico de gran tamaño, imágenes, multimedia).

Pues los usuarios se quejan del rendimiento. Por lo tanto se analiza el **rendimiento de los enlaces LAN**. También el ancho de banda de la LAN para determinar si la red soporta más suscripciones de las debidas y se comparan los resultados de referencia.

Así mismo se analizan las estadísticas de **switches multipuerto.** Especialmente los de la ruta entre el servidor y los clientes para determinar las existencias de puertos con errores o excesivas suscripciones.

CONCLUSIONES

Se puede concluir que la congestión en las redes de datos, ha sido un factor de gran importancia para el buen desempeño en la red. De igual forma está siendo combatida por mecanismos y sistemas predeterminados que analizan y monitorean la red en busca de un mayor mejoramiento en la QoS.

De igual forma se puede deducir que hay técnicas como las del bucle abierto que se le denomina soluciones pasivas y explica que una forma de evitar congestiones en la red de datos es necesario tener en cuenta unas varíales de diseño que son importantes al momento de delinear la red por ende minimizaran los problemas de congestión.

Las principales técnicas de monitorización, prevención y detección de errores en una red, están siendo utilizadas por los administradores de red para advertir la congestión y éstas viven más consolidadas y accesibles. Los software de gestión de red son de gran apoyo para realizar las funciones de monitoreo ya que cuentan con herramientas especificas que establecen en tiempo real donde se esta presentando un inconveniente y a quien esta afectando.

Fue complejo interconectar todos los procesos y conceptos de la congestión, es un tema que aun tiene mucho mas ámbito para seguir estudiándolo y cada día se hace mas efectivo el uso de herramientas para poder gestionar una red. La metodología fue determinante ya que se contó con los textos apropiados e información pertinente para la realización de ésta investigación.

RECOMENDACIONES

Es conveniente saber que el progreso de las comunicaciones seguirá siendo un proceso permanente, como también los diferentes tipos de fallos al momento de tener una transmisión de datos, como es el tema de la congestión, el cual se ha convertido en una situación muy común en el entorno de las redes de datos.

En el transcurso del desarrollo de esta monografía se encontró mucha información, precisa y se definieron muchos términos e ideas, acerca de los aspectos de la congestión en la red, que es muy impredecible cuando puede llevarse acabo. Lo que permite hoy un desafío, pronto una mejora, el cual se recomienda adquirir la información necesaria expuesta en este trabajo de grado, como un gran aporte para crear nuevos lineamientos para el mejoramiento en la administración de una red. Entre ellos se tiene en cuenta los diferentes herramientas de monitorizaron en las red, en este caso el software de gestión Network Inspector. Para el fácil entendimiento de los próximos estudiantes de esta temática.

BIBLIOGRAFÍA

LEÓN, Alberto G. Redes de Comunicación, 2 ed. Interamericana de España, S.A.U editorial McGRAW-HILL, 2002

PALMER Michael J. Redes Informáticas, Guía practica, 2000 Internacional Thomson Editores Spain Paraninfo, S.A.

STALLINGS, William, Comunicaciones y redes de computadores, 7 ed**.** Madrid: Pearson Educación, 2004

CISCO Systems, Networking Academy programa CCNA 1, Networking Basics v 3.1 Lab 7.1.9a, Copyright 2003, Cisco Systems, Inc.

ZUÑIGA, Isaac, S, NETWORK INSPECTOR, UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR, Cartagena de Indias, Junio 2007

Herramienta Web, para la enseñanza de protocolos de comunicación, control de la congestión [En línea]. [Citado 2008]. Disponible en Internet: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/congest.html

Zamorano M, Millán P. Control de Congestión y Enrutamiento en Redes ATM, Revista Facultad de Ingeniería. Vol. 6, 1999 [En línea]. [Citado 2008]. Disponible en Internet: http://redalyc.uaemex.mx/redalyc/pdf/114/11400603.pdf

TANENBAUM, Andrew S., Computer Networks, Prentice-Hall, Apuntes, Tema Control de Congestión. 1996 [En línea]. [Citado 2008]. Disponible en Internet: http://www.it.uc3m.es/~prometeo/rsc/apuntes/Conges/conges.html

FLUKE Network, Network Inspector, Software de seguimiento en la red, cisco/docs/ni5.pdf. [Citado 2008], Disponible en internet:: http://www.ufps.edu.co/cisco/docs/ni5.pdf

GLOSARIO

TÉRMINOS

AGENTE DE RED: es un dispositivo de red, por ejemplo una estaciona de trabajo o un enrutador, que esta equipado para reunir la información del rendimiento de la red y enviarla al NMS.

ANALIZADOR DE PROTOCOLOS. Es un dispositivo que se utiliza para comprobar los protocolos que se transmiten por la red. Trabaja de modo promiscuo, ya que captura todo el tráfico que circula por la red.

ATM: Asyncronous Transfer Mode. Modo de Transferencia Asíncrona. Tecnología de orientación de conmutación de celdas y con tecnologías multiplexaje. Usa paquetes fijos para llevar diferentes tipos de tráficos.

BUCLE ABIERTO: evitan la concurrencia de congestión asegurando que el flujo de tráfico generado por el origen no degradara las prestaciones de la red más allá de la QoS especificada.

BUCLE CERRADO: Reacciona ante la congestión cuando ésta ya se esta produciendo o cuando va a producirse (origen), generalmente regulando el trafico de acuerdo al estado de la red.

CAC: (Connection Admisión Control), control de admisión. Técnica de control de congestión en bucle abierto preventiva. Trabaja a modo de conexión.

ESCÁNER DE CABLE: Mide la longitud de un segmento de cable y también comprueba los posibles circuitos abiertos y cortocircuitos.

FRAME RELAY: Intercambio de tramas. Es una técnica de transmisión exactamente eficiente, usada para mandar información digital como voz, datos tráfico de redes de área local (LAN) y de gran área (WAN) a muchos puntos desde un solo puerto de una manera muy rápida.

ICMP: Protocolo de información de gestión común. Hace parte del estándar OSI para que el administrador de la red pueda reunir los datos sobre el rendimiento de la red.

IP:(Internet protocol), protocolo de Internet. Uno de los más importantes de los protocolos, el cual se puede basar el Internet.

LAN: Local Área Network. Red de Área Local. Red limitada en el espacio. Con comunicación de datos de alta velocidad.

NMS: Estación de gestión de red. Estación de trabajo dedicada a recopilar y almacenar los datos de rendimiento de la red, que se obtienen desde los nodos que están ejecutando el software de agente. Puede ejecutar el software de gestión de red que le permite recopilar toda la información y realizar las funciones de administración de red.

OHMETRO. Es un dispositivo que mide la resistencia y la continuidad en un circuito eléctrico.

POLÍMETRO: Es un dispositivo que mide una combinación de características eléctricas, por ejemplo voltios, ohmios y amperios.

PRUEBA COMPARATIVA: Estándar de hardware y software que se utiliza para medir el rendimiento ante las variaciones de carga o de las circunstancias.

QoS: Quality of Service. Calidad de Servicio. Es la idea de mejorar la tasa de transmisión, tasa de error y en muchos casos garantizar el servicio. QoS es de preocupaciones para las transmisiones continuas de ancho de banda para videos y transmisiones de multimedia.

REFLECTOMETRO DE DOMINIO TEMPORAL (TDR): Es un dispositivo que mide las características del cable de la red, por ejemplo la distancia, la impudencia, posniveles de interferencias de radiofrecuencia y la presencia de circuitos abiertos.

SNMP: Protocolo Sencillo de gestión de red. Permite a los ordenadores ya equipos de la red poder reunir datos según el formato entandar sobre el rendimiento de la red. Este protocolo forma parte del conjunto de protocolos TCP/IP.

Supervisión de Tráfico: es el proceso de monitorización y hacer cumplir el contrato del flujo de tráfico.

TCP/IP: Protocolo de Transmisión de control, Protocolo de Internet.