RESUMEN PRIMER PARCIAL "AYGR"

La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y de los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable.

Realizar tareas de inicialización, monitoreo y control de una red de comunicaciones con el objetivo de que ésta cumpla los requisitos de los usuarios para los cuales fue diseñada y construida.

Funciones del NOC "Network Operation Center"

- Monitoreo y gestión de la red
- Monitoreo y gestión de las fallas.
- Información sobre la disponibilidad actual, histórica y planeada de los componentes y sistemas de la red.
- Estado de la red y estadísticas de operación.

MONITOREO + CONTROL = GESTIÓN

Monitoreo: observar y analizar el estado y el comportamiento de la configuración de red y sus componentes. Se dice que es una operación de lectura.

- Monitoreo Estático: características de un elemento/dispositivo de la red.
- Monitoreo Dinámico: relacionado con eventos en la red.
- Monitoreo Estadístico: resultado de la agregación de información dinámica.

Monitoreo de Prestaciones

- Indicadores Orientados al Servicio (calidad de servicio): Disponibilidad, tiempo de respuesta, fiabilidad.
- Indicadores Orientados a la Eficiencia (costo de esa calidad): Utilización, throughput, tiempo de respuesta, disponibilidad, fiabilidad.

Control, Alterar los parámetros de los componentes de la red. Se dice que es una operación de escritura.

Cinco categorías para organizar/ordenar la gestión de una red

- Gestión de la Performance: tiempos de respuestas, utilización, etc. Incluye dos categorías funcionales como ser el monitoreo (seguimiento de la actividad de la red) y control (que realiza ajustes para mejorar las prestaciones). Requiere el establecimiento de métricas adecuadas y determinar los valores relevantes a monitorear; recolectar datos de uso (baseline), capacity planning (para detectar tendencias), establecimiento de umbrales de notificación (alarmas), la construcción de una base de datos de dispositivos para el análisis offline, llevar a cabo simulaciones de la red para la optimización de performance y seguimiento de la latencia (entre query/respuesta). Consiste en medir y recolectar información para sacar conclusiones sobre la performance de la red
- Gestión de fallas: una falla se define como una acción que requiere algún tipo de procedimiento para ser corregida. Los errores, los cuales ocurren ocasionalmente, no siempre son considerados fallas. Cuando ocurre una falla se debe proceder de la siente forma: detectar y diagnosticar la localización de la falla, aislarla para evitar que se expanda por el resto de la red y resolverla de forma segura y rápida.
- Gestión de la Configuración: se ocupa de inicializar la red, mantener, añadir y actualizar el estado de los componentes u las relaciones ente ellos.
- Gestión de Seguridad: se debe contar con identificadores para cada hosts y la información sensible para cada uno de ellos. Además de generar reportes de fallas y de accesos no válidos, asignación de permisos y demás medidas de seguridad.
- Gestión de la Contabilidad: es necesario mantener información sobre el uso de los recursos de la red por usuario o tipos de usuarios. De esta manera, se podría determinar si hay algunos de ellos que estén haciendo un mal uso de la red y sus recursos. Además, dicha información es tenida en cuenta para planificar posibles extensiones de la red.

Protocolo SNMP

Es un protocolo de capa de aplicación que facilita el intercambio de información de gestión ente dispositivos de la red.

Puede utilizar SNMP para apagar una interfaz en el router o comprobar la velocidad a la que funciona su interfaz Ethernet. SNMP puede incluso controlar la temperatura de su interruptor y que le avise cuando ya es demasiado alta. SNMP por lo general se asocia con la gestión de los routers, pero es importante entender que se puede utilizar para manejar muchos tipos de dispositivos.

Permite crear herramientas de gestión que informen sobre el funcionamiento de la red o sub red, detecten fallas y funcionamientos incorrectos y permitan actuar sobre dispositivos de la red.

Se definen tres pilares fundamentales:

- MIB, colección de objetos identificados para la gestión, sus tipos y relaciones en una entidad gestionada. Un agente puede poner en práctica muchas MIB, pero todos los agentes implementan una MIB particular, llamado MIB-II. Es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas utilizando el protocolo de administración de red SNMP. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables. La MIB y los objetos contenidos en estas son situados en este árbol siguiendo las normas determinadas. Cada nivel, subnivel y objeto son representados con un nombre y un número dentro del árbol (OID).
  Se puede hacer referencia a un objeto empleando una secuencia de nombres o de números. Esta secuencia de nombres o números contiene la ruta que se sigue desde la "raíz" del árbol hasta la "hoja". La hoja hace referencia al objeto que es la última entidad posible.
- SMI, sintaxis usada para especificar una MIB. Define las reglas generales para nombrar objetos, definir sus tipos y codificar sus valores.
- SNMP:
  - SNMPv1, Idea: lograr una solución temporal hasta la llegada de protocolos de gestión mejores y más completos. Basado en el intercambio de información de red a través de mensajes (get y set) en texto plano.
  - SNMPv2, Incorpora mensajes get-bulk-request (multiples variables), mayor detalle en la definición de las variables y estructuras para facilitar el manejo de los datos.
  - SNMPv3, Énfasis en los mecanismos de seguridad,
    - Integridad del mensaje: asegura que el paquete no haya sido alterado durante la transmisión.
    - Autenticación: asegura la identidad del emisor del mensaje.
    - Cifrado

Componentes de SNMPv3

Un manager es un servidor que ejecuta algún tipo de sistema de software que puede manejar las tareas de gestión de una red. Los managers se refieren a menudo como estaciones de administración de red (NMS, Network Management Station). Un NMS es responsable de sondeo y la recepción de las traps de los agents en la red. Un pull, en el contexto de la gestión de la red, es el acto de realizar queries a un agent (router, switch, servidor Unix, etc.) por alguna información. Esta información puede ser utilizada después para determinar si se ha producido algún tipo de evento catastrófico.

Un trap es una forma para decirle al agent que algo ha ocurrido. Los traps se envían de forma asincrónica, no en respuesta a las preguntas de los NMS.

El agente, es una pieza de software que se ejecuta en los dispositivos de red que están siendo administrando. Puede ser un programa independiente (un demonio, en lenguaje Unix), o puede ser incorporado en el sistema operativo. La NMS puede consultar el estado de cada interfaz y tomar las medidas apropiadas si alguno de ellos está caído. Cuando el agente se da cuenta de que algo ha ocurrido, se puede enviar una captura de los NMS. Este trap se origina en el agente y se envía a la NMS, donde se maneja apropiadamente. Algunos dispositivos envían una trap de "fuera de peligro" cuando hay una transición de un mal estado a un buen estado.

Las polls y los traps pueden ocurrir al mismo tiempo.

SNMP and UDP

SNMP utiliza el Protocolo de datagramas de usuario (UDP) como protocolo de transporte para el paso datos entre los gestores y agentes. UDP, fue elegido por el Protocolo de Control de Transmisión (TCP), ya que es sin conexión; es decir, hay un extremo a otro de conexión se hace entre el agente y el NMS cuando datagramas (paquetes) se envían de ida y vuelta. Este aspecto de la UDP hace que sea poco fiable ya que no hay reconocimiento de datagramas perdidos al nivel de protocolo. Todo depende de la aplicación SNMP para determinar si se pierden los datagramas y las retransmiten si así lo desea.

SNMP utiliza el puerto UDP 161 para el envío y la recepción de solicitudes y el puerto 162 para la recepción de las traps de los dispositivos gestionados.

SNMP Operations

- La operación Get: La petición GET es iniciada por el NMS, que envía la solicitud al agente. El agente recibe la solicitud y la procesa. Si el agente tiene éxito en la recopilación de la información solicitada, se envía un GetResponse al SMN. Uno de los elementos en la solicitud GET es una variable binding. Una variable de unión, o var-bind, es una lista de objetos MIB que permite a los destinatarios de una solicitud ver lo que el autor quiere saber.
- La Operación GetBulk: la operación GetBulk, permite a una aplicación de gestión para recuperar una gran parte de una tabla a la vez. La operación GetBulk, por otro lado, le dice al agente que envíe de vuelta como respuesta todo lo que puede. Esto significa que las respuestas incompletas son posibles.
- Set Operation: El comando set se utiliza para cambiar el valor de un objeto gestionado o para crear una nueva fila en una tabla. Los objetos que se definen en la MIB como lectura-escritura o de lectura, sólo puede ser modificado o creado con este comando. Es posible para un NMS configurar más de un objeto a la vez.

Acuerdo de Nivel de Servicios (SLAS)

Es un acuerdo entre el proveedor del servidor y el cliente (es soportado por QoS). Contrato por la prestación del servicio (transporte IP), los requerimientos son derivados de los requerimientos de las aplicaciones a las cuales desea dar soporte, saltan cuando se hizo el relevamiento.

Hay flujos de tráficos con diferentes requerimientos en cuanto a delay, pérdidas, jitter. Hay diferentes aplicaciones con diferentes requerimientos, o sus usuarios tienen diferentes requerimientos. De acuerdo a los requerimientos se va a clasificar el tráfico en clases y se les aplica prioridades. Si la red está congestionada, se descartan paquetes, hay que saber cuáles, cuántos, cuándo. Esta prioridad se da en las colas.

Métricas de medición

- Delay (Retardo): Se puede cuantificar, ya sea como en un solo sentido de demora o de ida y vuelta (RTT). En este caso, el RTT se puede determinar si el emisor indica su timestamp cuando envía en el paquete su timestamp y resta este valor cuando recibe la respuesta. La medición de delay en un sentido requiere que el emisor y el receptor tengan sincronizados los relojes locales de tal manera que el delay unidireccional pueda ser determinado en el receptor. Si el receptor también recibe el timestamp en el paquete de prueba la diferencia entre el timestamp del envío y el de recepción es el delay unidireccional. RTT es más fácil de implementar y mide el delay unidireccional. Para aplicaciones como la videoconferencia interactiva puede no importar en qué dirección el delay es experimentado. Si el exceso es experimentado en absoluto, entonces el servicio se verá afectado. Si se producen violaciones en el SLA por delay, el RTT oculta los detalles de la dirección en la que se produjo el problema. El delay puede proporcionar un número de indicadores importantes del rendimiento de la red.
    - Delay mínimo: El retardo de red mínimo es el retardo de "línea de base" de red que proporciona una indicación del retraso que experimentará el tráfico cuando la ruta del origen al destino está cargada ligeramente. Este se compone de retardo de propagación, retardo de conmutación, y el retardo de serialización. Los valores de retraso por encima del mínimo proporcionan una indicación de la congestión experimentada a lo largo del camino.

    - Umbral superado: puede ser útil para contar el número de paquetes de prueba, de un total que experimentó un retraso de más de un umbral definido, establecido para indicar cuando un paquete llegó demasiado tarde para ser útil.
    - Delay promedio: El retardo promedio puede ser interesante para propósitos de tendencia, pero para fines de comparación deben registrarse junto con la desviación estándar de la muestra. Las mayores desviaciones estándar de la norma pueden ser indicativos de problemas falsos más que de una tendencia.
    - Delay-Jitter: Se considera generalmente que es la variación del retardo de ida para dos paquetes consecutivos. Afortunadamente, para el cálculo del jitter no hay necesidad de conocer los retrasos individuales de un solo sentido. En su lugar, esto se puede calcular a partir de la diferencia entre timestamps tomadas en los dispositivos individuales.
- Pérdida de paquetes: Con el fin de determinar la pérdida de paquetes, es necesario que haya una manera de distinguir entre un paquete perdido y un paquete con un retardo grande pero finito:
    1. Período de pérdida: Define la frecuencia y la longitud (pérdida de ráfaga) de la pérdida una vez que comienza.
    2. Distancia pérdida: define la separación entre los periodos de pérdida.
- Ancho de banda y Throughput: La aplicación de throughput depende de muchos factores, que pueden variar ampliamente dependiendo de implementaciones de sistema de extremo y los perfiles de tráfico.
- Disponibilidad: La disponibilidad de servicios IP se define en general como disponibilidad de la red o como la disponibilidad del servicio.
    - Disponibilidad de la red: disponibilidad de la red bidireccional o conectividad entre dos dispositivos de monitorización activos se pueden determinar usando pruebas de envío desde un emisor a un receptor y luego de vuelta al emisor. Por cada respuesta recibida con éxito, la red se considera disponible.
    - Disponibilidad del servicio: Es un indicador definido cuando un servicio está disponible entre un punto de entrada especificado y un punto de salida especificada dentro de los límites de las métricas de SLA comprometidos para el servicio.
- Calidad de Experiencia: Proporciona una medida numérica subjetiva por parte de los usuarios de la red.

La sincronización de reloj

La forma más precisa para sincronizar los relojes de los dispositivos de red consiste en sincronizar cada dispositivo con una fuente de reloj externa precisa como un reloj GPS o radio reloj lo cual no sería viables para ubicaciones muy distantes. Un enfoque alternativo es la de distribuir el tiempo usando un protocolo, tal como el protocolo de tiempo de red (NTP). NTP sincroniza los relojes entre dispositivos de red mediante el intercambio de mensajes con timestamp entre un servidor y sus clientes. NTP busca precisión a largo plazo a expensas de la exactitud de corto plazo.

Debido a las limitaciones y los costos de entre dispositivos de sincronización de reloj, un modelo de implementación común es la de distribuir el tiempo a partir de una fuente de reloj a todos los dispositivos dentro de un punto de presencia (POP). La sincronización de los routers de acceso a través de NTP en general no es lo suficientemente precisa y el uso de fuentes de reloj en estos lugares generalmente no es viable, por lo tanto, los informes de SLA de los enlaces de acceso de POP de acceso del router es comúnmente reportado como RTT en lugar de un solo sentido demora.

Calidad de Servicio (QoS)

Consideramos que un servicio es una descripción del tratamiento global del tráfico de un cliente a través de un dominio particular.

Podemos definir la calidad de servicio en términos de los requisitos fundamentales para una aplicación, la cual se puede definir en términos de las métricas de SLA para el desempeño del servicio IP.

Calidad de servicio, implica algo más que asegurar que un servicio de red sea capaz de soportar los requisitos de SLA de las aplicaciones.

Son mecanismos que nos van a ayudar a lograr los acuerdos (SLAS). Como por ejemplo priorizar tráfico, manejarlo de alguna manera para cumplir los SLAS.

No se asegura calidad de servicio a internet porque nadie puede asegurar que se tenga una determinada tasa de transferencia con todos los sitios de todas las redes de todo el mundo, porque va a depender de la carga del servidor al que se conecta. Pero si hay calidad de servicio dentro de la nube provista porque es administrada por alguien.

Maximizar la satisfacción del usuario requiere que las aplicaciones de usuario final trabajar con eficacia.

FUNCIONES DE UN ROUTER: validar header, decrementar TTL, recalcular checksum, buscar ruta, fragmentar si es necesario (MTU de enlace salida < tamaño de paquete), procesar opciones si es necesario, descartar paquetes ante congestión, clasificar paquetes, filtrar paquetes, marcar paquetes (al clasificarlos puede ser que se necesite marcar), NAT, priorizar tráfico, verificar conformidad de tráfico.

Dentro de la nube se van a tener los ruteadores de borde y los de core. Ambos con diferentes funcionalidades. Los routers de borde se relacionan con el equipamiento del usuario. Tienen diferentes funcionalidades para que no todos los routers clasifiquen el mismo tráfico todas las veces. Si se tiene que limitar al usuario a 3mb, esta limitación la hace el router de borde, el marcado de paquetes también. Descarte, dropeo, y remarcado, adentro.

Se separa al router en dos:

- Data plane: los paquetes son procesador, se busca en la tabla para saber por qué interface se tienen que mandar, y también a veces la clasificación y el filtrado, acondicionamiento del tráfico (policing). Se aplican en los nodos de la red y pueden afectar directamente el comportamiento de reenvío de paquetes. Estos mecanismos se pueden clasificar en función de las características de comportamiento primitivas que se imparten al tráfico.
- Control plane: es la parte donde están ejecutándose los procesos que hablan los diferentes protocolos de ruteo. Se generan tablas (información de fordwardeo) que usa el Data Plane. Mecanismos que normalmente se ocupan del control de admisión y reserva de recursos, se implementan típicamente como procesos de software, tales como los protocolos de enrutamiento.

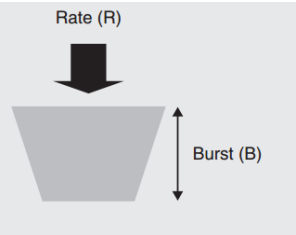
Policing

No deja pasar más de lo que no tiene que pasar. Controla la tasa máxima de envío, marcando (o descartando) paquetes. Policing es un mecanismo que puede ser usado para asegurar que un flujo de tráfico no exceda una velocidad máxima definida.

Implementaciones de Policing

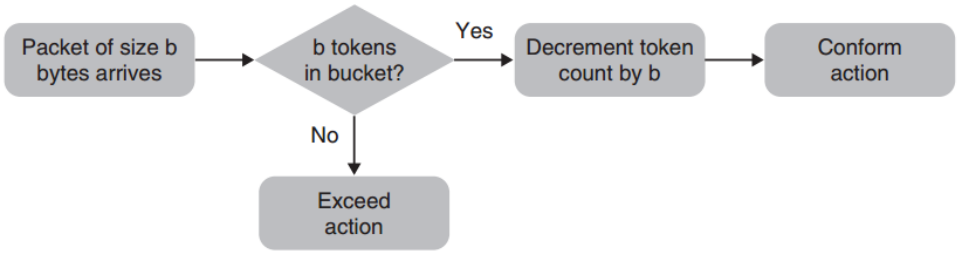
- Single Token-Bucket: Cuando un paquete de llega, el tamaño de paquete b se compara con el número de fichas que hay actualmente en el balde. Si las fichas son suficientes, es decir dentro del balde hay una cantidad de fichas que es mayor o igual a la cantidad de bytes del paquete; entonces el paquete ha sido "conforme". Si no hay fichas suficientes en el balde, entonces el paquete ha "excedido". Si el paquete se ajusta a continuación, entonces se decrementa de la cubeta la misma cantidad de fichas que el tamaño del paquete.

Las acciones más sencillas son transmitir el paquete si se ajusta y descartar el paquete si es superior. Aplicado de esta forma, la política de token bucket aplicaría una tasa máxima de R y B de ráfagas en el flujo de tráfico.

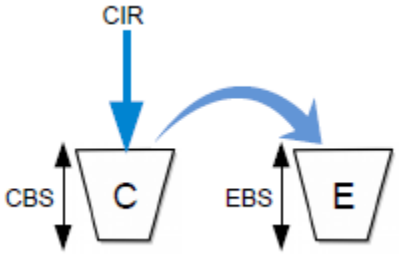


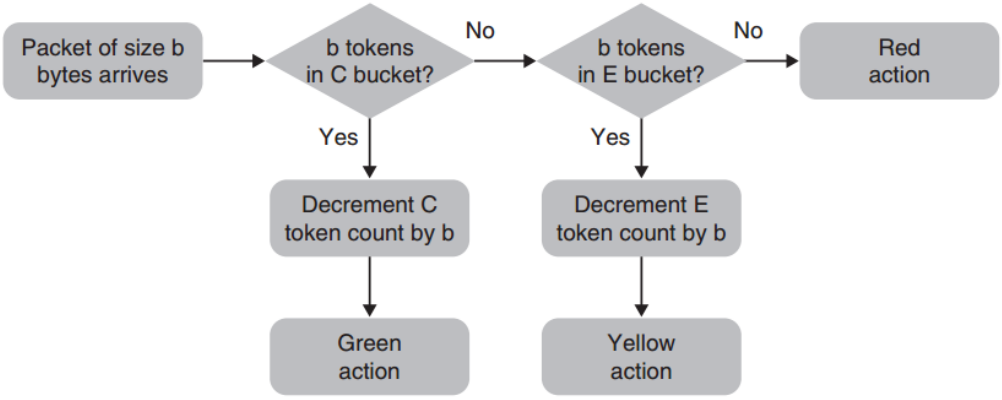
Es importante señalar que un token bucket policer nunca retrasa el tráfico, mientras que si lo hace un shaper. Es decir, no hay paquetes almacenados en el balde. Sólo hay fichas en el balde. Por lo tanto, como un token bucket no retrasa el tráfico, no puede volver a ordenar o priorizar el tráfico como un planificador.

Al llegar un paquete se compara con su tamaño en bytes con los token-bytes que hay en el bucket. Si hay suficientes se decrementan tantos token-bytes como bytes del paquete (paquete en conformidad). Sino el paquete no está "en conformidad".

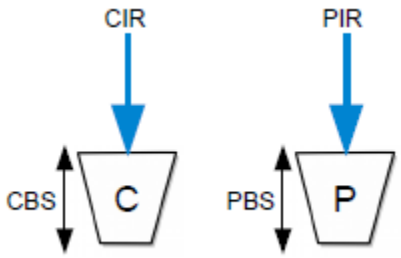


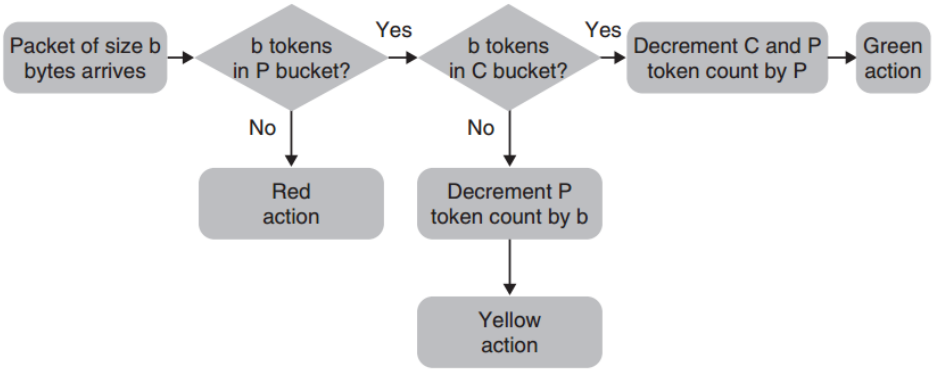
- Single Rate Three Color Marker: Los "tres colores" se refieren a los tres estados. SR-TCM utiliza dos baldes de fichas. Los baldes se definen como C y E (para conforme y en exceso, o conforme y excedente) con el tamaño máximo de ráfaga CBS y EBS, respectivamente. Ambos baldes están llenos de fichas. Cuando un paquete de esa corriente llega:



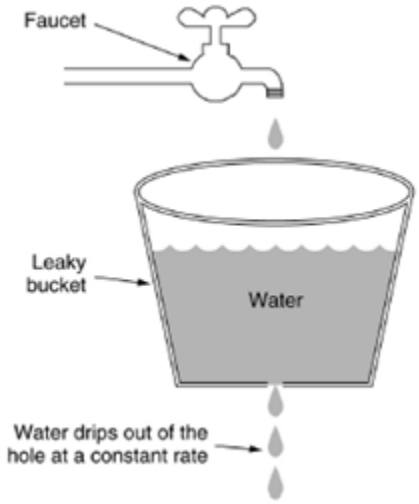


  - El tamaño del paquete B se compara con el número de fichas actualmente en el cubo C. Si las fichas existentes son mayores o iguales al tamaño del paquete, entonces sólo se disminuye el balde C en tantas fichas como bytes del paquete. Color verde.
  - Sino, si las fichas en el balde C no son suficientes, entonces el paquete ha superado el balde C. Ahora se compara con el balde E. Si las fichas del balde E son mayores o iguales al tamaño del paquete en bytes, entonces el balde de E solamente se disminuye en esa cantidad. Color amarillo claro.
  - Si no hubiera ni tantas fichas en el balde C o E como bytes en el paquete, entonces color rojo y no se disminuye ningún balde.
- Two Rate Three Color Marker: TR-TCM utiliza dos baldes de fichas. Sin embargo, una diferencia notable con respecto al caso anterior, es que los baldes se llenan a diferentes velocidades. C se llena a la tasa de información comprometida (CIR), mientras que P se llena al tipo de información pico (PIR). Cuando un paquete llega:
    - Si B > tokens en P. Acción roja, sino
    - Si B > tokens en C, disminuir B fichas de P, acción amarilla, sino
    - Sino B tokens de C y P, acción verde.





Shaping



Shaping, como policing, es un mecanismo que puede ser usado para asegurar que un flujo de tráfico no exceda una velocidad máxima definida. También al igual que policing, un shaping puede ser visualizado como un mecanismo de token bucket con una profundidad máxima definida conocida como la ráfaga B, y una tasa R definida en la que el balde está lleno de fichas de tamaño byte. El número mínimo de fichas en el cubo es cero. La diferencia entre un shaper y un policer se hace evidente cuando se considera lo que sucede cuando un shaper se aplica a una corriente de tráfico. Cuando un paquete llega, el tamaño de paquete b se compara con el número de fichas que hay actualmente en el balde. Si hay al menos tantas fichas de bytes en el balde como hay bytes en el paquete, entonces el paquete se transmite sin demora. Si hay menos fichas en el balde que bytes en el paquete, entonces el paquete se retrasa hasta que haya suficientes fichas en el balde. Cuando hay suficientes fichas en el balde, el paquete se envía y el cubo se disminuye en un número de fichas igual al número de bytes en el paquete. El shaper es significativamente diferente al policer, ya que actúa para eliminar o marcar el tráfico no conforme en lugar de retrasar. Un policer puede considerarse como un caso especial de un shaper con una cola con una longitud máxima de cero paquetes.

Se hace notar que no todos los shaper necesitan ser implementados con un mecanismo de token-bucket. Otro

> La diferencia entre el Shaper y el Policer es que el Shaper demora la transmisión de un paquete si no hay fichas en el balde. En caso contrario, el policer transmite sin demora.

mecanismo que se utiliza para el shaper es el leaky bucket. Con un algoritmo de leaky bucket, se puede visualizar que los paquetes se almacenan en el balde. Los paquetes que llegan son colocados en el balde que tiene un agujero en la parte inferior. La profundidad del balde con goteo, determina el número máximo de paquetes que pueden ser encolados en el balde. Si un paquete llega cuando este ya está lleno, el paquete se descarta.

Encolado y Prioridad

Manejar los paquetes recibidos y planificar su envío en una interfaz de salida.

Paquetes que llegan van a parar a algún buffer (región de memoria) donde hay apuntadores a los paquetes dentro de ese buffer. Esos paquetes se tienen que enviar por alguna interfaz de salida. Para hacer esto, dentro de un router hay un queue manager. Tiene que organizar los paquetes, darle prioridad a un paquete sobre otros, pero en un tiempo acotado. Los buffers son de tamaño finito, a veces se necesita descartar paquetes.

Técnicas de Encolado

- FIFO: primero en llegar primero en ser servido. Sabiendo Tamaño buffer / capacidad del enlace se sabe el retardo máximo (delay máximo). No provee QoS (no diferencia trafico). Solución es la planificación con prioridades
- STRICT PRIORITY QUEUEING: Asegura que el tráfico importante sea procesado primero. Hay ciertos procesos que tienen prioridad. El problema es que las colas con más prioridad causan que las demás nunca sean atendidas. Se puede aplicar policing para que los paquetes de menor prioridad puedan ser atendidos. Pre-emptive: packet level o quantum level (tiempo asignado, se interrumpe el que está siendo servido).
- WEIGHTED BANDWIDTH SCHEDULING:
  - WEIGHTED ROUND ROBIN: Considere un planificador que tiene tres colas con pesos, A, B y C con los pesos de 1, 2 y 4, respectivamente. En una ronda, el planificador visita cada cola y da servicios a una cantidad de tráfico desde esa cola según los pesos de las mismas. En el ejemplo anterior, la ponderación de servicio entre las colas se define en términos de paquetes. Si todos los paquetes en las diferentes colas son del mismo tamaño, la asignación del ancho de banda disponible de enlace también se pondera entre las colas en la misma proporción. En un planificador WRR si algunas colas están inactivas, a continuación, el planificador pasa a la siguiente cola y por lo tanto el ancho de banda no utilizado para las colas inactivas se redistribuye entre aquellas que, si lo están en proporción a sus pesos relativos, para cumplir con las garantías mínimas del servicio. Si el tamaño promedio de paquetes en las diferentes colas son los mismos, entonces WRR será justo en promedio. Si los tamaños promedio de paquetes de las distintas colas no son los mismos, entonces el planificador potencialmente podría normalizar los pesos de las colas de acuerdo con el tamaño medio de paquete de cada cola.

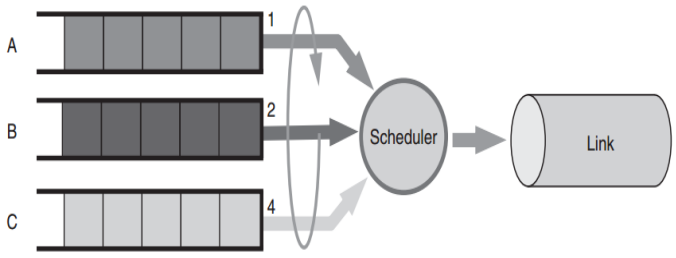


Figure 2.14 WRR scheduling example

  - WEIGHTED FAIR QUEING: Cuando un paquete llega a una cola previamente inactivas, su tiempo de servicio se calcula tomando el tiempo de ida actual y añadir el tamaño del paquete multiplicado por el peso de la cola. En consecuencia, con WFQ la proporción de ancho de banda de una cola es inversamente proporcional al peso de dicha cola. Trata de emular un scheduler ideal que pudiera servir a cada cola. Por cada paquete que arriba, calcula cual es el tiempo de envío.
  - DEFICIT ROUND ROBIN: Es una modificación WRR tal que puede ser justo sin conocer los tamaños promedio de paquetes. Esto se logra mediante el seguimiento de un contador de déficit para cada cola. Cuando es el turno de una cola para ser atendida, el planificador intentará servir por todo un quantum completo. En la práctica, es poco probable que el quantum sea exactamente igual al tamaño del siguiente paquete, o los próximos paquetes en la parte delantera de la cola. En este caso, tantos paquetes enteros serán atendidos desde la parte delantera de la cola como pueden ser acomodados por el quantum. Si el primer paquete es mayor que el quantum disponible, entonces no se dará servicio a los paquetes en esa ronda. Si hay más paquetes en la cola que pueden ser acomodados por la quanto, el planificador los transferirá a la siguiente ronda. De esta manera, las colas que no reciben su parte justa en una ronda reciben una recompensa en la próxima ronda.

Drop

En este punto, antes de considerar el descarte de paquetes, es de destacar la diferencia entre los buffers y las colas. Los buffers son las ubicaciones físicas de la memoria, donde los paquetes se almacenan temporalmente mientras esperan a ser transmitidos. Las colas, por otro lado, no contienen paquetes a pesar de que es el lenguaje común para referirse a "paquetes en una cola"; más bien, una cola consiste en un conjunto ordenado de punteros a las ubicaciones en la memoria buffer donde en realidad se almacenan los paquetes en dicha cola.

Si la tasa de arribo supera continuamente el ancho de banda del enlace disponible, entonces el número de paquetes por lo menos en una de las colas debe aumentar continuamente. El buffer utilizado para encolar los paquetes que arriban es

de tamaño finito y en algún momento dicha memoria quedará excedida de forma inevitable. Por eso, los paquetes se deben eliminar.

Las principales razones para limitar o controlar el tamaño de la cola son, ya sea para limitar el retardo experimentado por los paquetes en la cola, o en un intento de optimizar el rendimiento alcanzado por el tráfico en la cola.

Técnicas de Descarte de Paquetes

- Tail Drop: Este mecanismo se utiliza para establecer un límite máximo en el número de paquetes que se pueden mantener en una cola. Antes de que un paquete sea encolado, el tamaño de la cola es chequeado; si el tamaño del paquete cola supera el límite máximo para la cola, entonces el paquete será descartado. Fijando el límite máximo de paquetes en una cola se puede hacer cumplir un retraso máximo. Con algunas aplicaciones como VoIP, si un paquete se retrasa demasiado, será de ninguna utilidad y es mejor descartarlo en lugar de consumir ancho de banda de la red y descartarlo en el destino. La pérdida de paquetes puede ser considerado como el caso más extremo de demora; es decir, un paquete que se retrasa infinitamente nunca llega, y para todos los efectos, puede considerarse perdido.
- Head Drop: Descarte por la cabeza de la cola (Head Drop) es una alternativa posible a Tail Drop. En este caso, el

Si se tiene la cola llena y llega un paquete que no se puede colocar entonces se dropea.

descarte de paquetes se realiza desde el comienzo de la cola en vez de por el final cuando el tamaño de la misma queda excedido. Head Drop mejora el rendimiento de TCP al permitir que la señal de congestión alcance más rápidamente el remitente que a esperar a que se completa la transmisión del primer paquete. Head Drop no es soportado por las implementaciones de proveedores router.

Igual que el anterior, pero dropea desde el inicio de la cola, o sea el primero que se iba a servir.

- WEGHTED TAIL DROP: Algunas implementaciones de colas soportan más de un límite en una cola. El tráfico que va a ser preferentemente desechados pueden ser clasificados por un marcado del resto del tráfico diferente; el tráfico puede haber sido marcado como diferencialmente dentro y fuera de la contratación a través de un controlador de políticas.

Usa las marcas (rojo, amarillo, verde) para ponerles un peso y dropear.

- RANDOM EARLY DETECTION: (RED) es un mecanismo de gestión de cola activa. Dicho mecanismo detecta la congestión antes de colas de desbordamiento, y brindan información de esta congestión a los sistemas finales con el fin de evitar el exceso de pérdida de paquetes debido a la congestión y el mantenimiento de un alto rendimiento de la red reduciendo al mínimo los retrasos en cola. Hay paquetes con una determinada probabilidad antes de que la cola se llene (al azar).

INTSERV (RFC 1633)

Redefinir el mismo byte en una arquitectura integrada de servicios. La idea es que haya una reserva de recursos de extremo a extremo. Desde el origen hasta el destino se arme un camino en el cual todos los nodos intermedios se reserven los recursos necesarios para asegurar el delay, el throughput del tráfico de cada flujo.

- Por eso es una clasificación por flujo.
- Administración de colas basadas en flujos.
- Hay un control de admisión, o sea que antes de poder empezar a cruzar tráfico, debe señalizarse ese camino, esto se hace con el protocolo RSVP.
- Esto no es escalable.
- Cada quíntupla es un flujo distinto que hay que clasificar, para los router es imposible.

DIFFERENTIATED SERVICES (DIFFSERV) RFC 2474

- Hay clasificación del tráfico y acondicionamiento (policing)
- El marcado con DSCP (Differentiated Services Code Point). Son los números que se va a poner al byte para identificar conjuntos o clases de tráficos (ya que no son flujos individuales) y se les da un comportamiento.
- Se definen los comportamientos por salto.

Dentro de un dominio administrado por una entidad:

-Hay paquetes que llegan, son clasificados: policing, se marcan con DSCP, luego los ruteadores intermedios lo que hacen es mirar lo que dice DSCP así saben cómo clasificar ese tráfico y en qué cola ponerlo. Cuando sale del dominio se rutea de manera normal.

MPLS – MULTIPROTOCOL LABEL SWITCHING

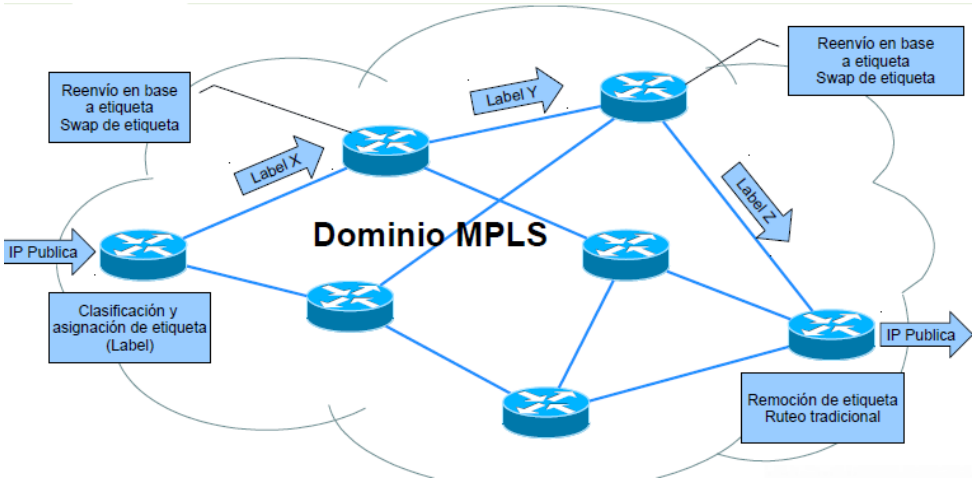
MPLS añade una etiqueta en frente de un paquete, como otro de cabeza de modo que los routers saben cómo actuar sobre la base de esta etiqueta. Para ello deben ser routers de etiqueta conmutada (LSRs), y cada LSR deben mantener una asignación válida para las etiquetas de entrada y de salida. Esto, a su vez, significa que LSRs mantienen estados en términos de etiquetas de entrada / salida asociados con un camino en particular, a que se refiere como una etiqueta de ruta (LSP), que puede ser designada para una clase particular de los flujos de tráfico conmutado. Tenga en cuenta que un LSP debe ser establecido de ante mano entre dos routers para que los paquetes pueden seguir este camino. Para establecer una trayectoria, se utiliza un protocolo de distribución de etiquetas.

Una etiqueta en MPLS es de 20 bits de largo y es parte de una cabecera MPLS shim 32 bits. Un paquete con una cabecera shim MPLS se conoce como un paquete de MPLS. Si un paquete de MPLS lleva un paquete IP, entonces podemos pensar en MPLS puede ser de capa 2.5 según el modelo OSI. Tenga en cuenta que aún requiere la ayuda de la capa 2 para la entrega de paquetes entre dos LSRs adyacentes. La principal diferencia de MPLS de ser de capa 2 es que proporciona una forma de ruteo a través de las etiquetas con múltiples saltos.

La cabecera de cuña de 32 bits también incluye 3 bits experimentales, un bit ("S" bits) para indicar que esta etiqueta es la última etiqueta (parte inferior de la pila) para el caso de las etiquetas apiladas, y 8 bits para el tiempo de vida (TTL). Los bits experimentales tienen el propósito de describir los servicios que requieren diferentes prioridades. La etiqueta de valores de 0 a 15 están reservados.

Hay otra terminología, túnel, estrechamente relacionada con un LSP. Un túnel ofrece un servicio de transporte entre dos routers para que los paquetes de una corriente específica pueden fluir sin ser ruteado hacia ruteadores intermedios que no pertenecen al túnel.

Cuando un paquete MPLS llega a un LSR, la etiqueta de entrada se intercambia con una etiqueta de salida; esto supone que un LSP ya está definido y tablas de búsqueda en LSRs tienen entradas apropiadas. Antes de enviar un paquete MPLS recibido, el valor TTL se reduce en uno. Si el valor TTL se convierte en cero, entonces el paquete de MPLS se descarta.



MPLS permite que se apilen etiquetas. Esto significa que una cabecera shim de MPLS puede aparecer más de una vez y cada una de ellas está relacionada con LSP en particular en ciertos puntos.

Una red MPLS debe tener routers de frontera, que son el punto de que un paquete IP original se antepone con una etiqueta MPLS. Estos routers son conocidos como routers de borde etiqueta (LER).

- El primer dispositivo realiza un routing lookup (como antes), pero:
- En vez de encontrar el next-hop, encuentra el router final.
- Y encuentra un camino predeterminado hacia éste.
- El router aplica una etiqueta basado en esta info.
- Los routers siguientes usan esta etiqueta para rutear (como en CV)
- El último router remueve la etiqueta
- Continua el ruteo IP tradicional.