Regulamentação QoS e marcação com os Engine do supervisor baseado em IOS do catalizador 4000/4500

Índice

Introdução

A função de vigilância determina se o nivel do tráfego está no perfil especificado (contrato). A função Vigilância permite a sair do tráfego de perfil ou reduzir o tráfego para um valor diferente de DSCP (Ponto de Código de Serviços Diferencial) para aplicar o nível de serviço contratado. DSCP é uma medida do nível de QoS (Qualidade de Serviço) do pacote. Junto com o DSCP, a precedência do IP e a classe de serviço (CoS) também são usadas para transmitir o nível de QoS do pacote de informação.

Policiar não deve ser confundido com o modelagem de tráfego, embora ambos se assegurem de que o tráfego fique dentro do perfil (contrato). A vigilância não faz ligação do tráfego; portanto, o retardo de transmissão não é afetado. Em vez de fazer buffering de pacotes fora do perfil, a vigilância irá descartá-los ou marcá-los com um nível diferente de QoS (marcação DSCP). O modelagem de tráfego protege o tráfego fora de perfil e alisa intermitências de tráfego, mas afeta o atraso e a variação de retardo. Dar forma pode somente ser aplicado em uma interface enviada, quando policiar puder ser aplicado em ambas as interfaces recebidas e enviadas.

O catalizador 4000/4500 com Supervisor Engine 3, 4 e 2+ (SE3, SE4, SE2+ a partir de agora neste documento) apoia o policiamento em entrante e em direções de saída. O modelagem de tráfego é apoiado igualmente, porém este documento tratará somente a vigilância e marcação. Marcação é um processo de alteração do nível de QoS do pacote, de acordo com uma política.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Vigilância de QoS e parâmetros de marcação

A vigilância é configurada através da definição dos mapas de política de QoS e da aplicação deles a portas (QoS baseadas em portas) ou a VLANs (QoS baseada em VLAN). O vigilante é definido pelos parâmetros de taxa e de burst, bem como pelas ações para um tráfego dentro perfil e fora do perfil.

Existem dois tipos de vigilantes suportados: agregado e por interface. Cada policer pode ser aplicado a várias portas ou VLANs.

O vigilante agregado age no tráfego em todas as portas/VLANs aplicadas. Por exemplo, nós aplicamos o policer agregado para limitar o tráfego do Trivial File Transfer Protocol (TFTP) ao 1 Mbps em VLAN 1 e 3. Tal vigilante permitirá o 1 Mbps do tráfego TFTP em VLAN 1 e 3 junto. Se aplicarmos um vigilante por interface, limitaremos o tráfego TFTP a 1 Mbps em cada VLAN de 1 a 3.

Nota: Se ambas as vigilâncias de ingresso e egresso forem aplicadas a um pacote, a decisão mais severa será tomada. Isto é, se o vigilante de ingresso especifica para deixar cair o pacote e a vigilância de saída especifica para marcar para baixo o pacote, o pacote será deixado cair. A Tabela 1 resume a ação de QoS no pacote quando ele é tratado por ambas as políticas, de ingresso e de saída.

Tabela 1: Ação de QoS dependendo da política de ingresso e saída

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

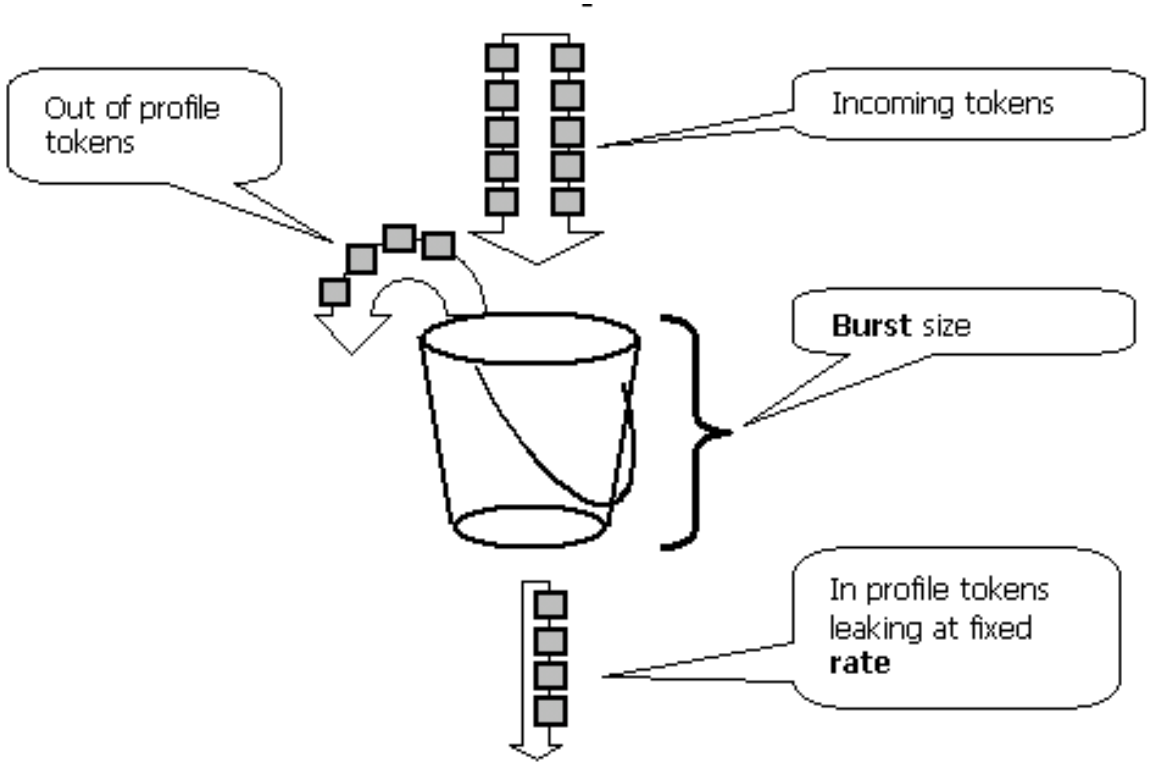
O catalizador 4000 SE3, SE4, QoS Hardware SE2+ é executado de tal maneira que a marcação real do pacote ocorre após a vigilância de saída. Isso significa que mesmo se a política de ingresso fizer uma marcação no pacote (por marcação do vigilante ou uma marcação normal), a política de egresso ainda verá pacotes marcados com o nível de QoS original. A política de egresso verá o pacote caso não tenha sido marcado pela política de ingresso. Isto significa o seguinte:

- A marcação de saída substituí a marcação de entrada.
- A política de saída não pode corresponder aos novos níveis de QoS alterados pela marcação de ingresso.

Outras implicações importantes são as seguintes:

- Não é possível fazer a marcação e marcar a mesma classe de tráfego na mesma política.
- Os policeres agregados são por-sentido. Isto é, se um policer agregado é aplicado ao ingresso e à saída, haverá dois policeres agregados, um na entrada e um na saída.
- Quando um policer agregado é aplicado dentro da política aos VLAN e à interface física, eficazmente haverá dois policeres agregados - um para as interfaces de VLAN e outro para interfaces física. Atualmente, não é possível vigiar as interfaces de VLAN e física juntamente no vigilante agregado.

Policiando no catalizador 4000 SE3, o SE4, SE2+ segue com o conceito de leaky bucket, porque o modelo abaixo ilustra. Tokens correspondentes a pacotes de tráfego de entrada são colocados em um bucket (nº de tokens = tamanho do pacote). Em intervalos regulares, um número definido de tokens (derivados da taxa configurada) é removido do bucket. Se não houver lugar no bucket para acomodar um pacote recebido, o pacote é considerado fora de perfil e descartado ou marcado, de acordo com a ação de vigilância configurada.



Observe que, embora o modelo acima possa passar essa impressão, o tráfego não é colocado em buffer no bucket. O tráfego real não está fluindo através do bucket. A cubeta é usada somente para decidir se o pacote é em perfil ou fora de perfil.

Note que implementação de hardware exata do policiamento poderia ser diferente, funcionalmente segue ao modelo acima.

Os seguintes parâmetros controlam a operação de vigilância:

- A taxa define quantos tokens são removidos em cada intervalo. Isso define efetivamente a taxa de vigilância. Todo o tráfego abaixo da taxa é considerado em perfil.
- O intervalo define com que freqüência os tokens são removidos do bucket. O intervalo está fixado em 16 nanossegundos (16 s *10-9). O intervalo não pode ser alterado.
- A intermitência define a quantidade máxima de tokens que o bucket pode conter em determinado momento.

Refira a vigilância e marcação de comparação na seção dos Engine do supervisor baseado em IOS do catalizador 6000 e do catalizador 4000/4500 na extremidade deste documento para diferenças na explosão entre o catalizador 6000 e o catalizador 4000 SE3, SE4, SE2+.

O vigilante garante que, se você examinar qualquer período de tempo (de zero a infinito), ele nunca permitirá mais que

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

de tráfego através do vigilante durante esse período.

O catalizador 4000 SE3, SE4, QoS Hardware SE2+ tem determinada granularidade para o policiamento. Dependendo da taxa configurada, o desvio máximo da taxa é de 1,5% da taxa.

Ao configurar a taxa de intermitência, você precisa de levar em consideração que alguns protocolos (tais como o TCP) executam os mecanismos de controle de fluxo que reagem na perda de pacotes. Por exemplo, o TCP reduz o indicador pela metade para cada pacote perdido. Quando policiada a uma determinada taxa, a utilização de link eficaz será mais baixa do que a taxa configurada. Um pode aumentar a explosão a fim conseguir a melhor utilização. Um bom começo para tal tráfego seria ajustar duas vezes a explosão para ser igual à quantidade de tráfego enviada com taxa desejada durante o Round-Trip Time (RTT). Pela mesma razão, não é recomendado avaliar a operação de vigilância pelo tráfego orientado de conexão, porque mostrará geralmente o desempenho mais baixo do que permitido pelo vigilante.

Nota: O tráfego sem conexão também pode reagir à vigilância de maneira diferente. Por exemplo, o Network File System (NFS) utiliza blocos, que podem consistir em mais de um pacote de Protocolo de datagrama de usuário (UDP). Um pacote deixado cair pôde provocar muitos pacotes (bloco inteiro) a ser retransmitidos.

Por exemplo, o seguinte é um cálculo da explosão para uma sessão de TCP, com uma taxa de vigilância de 64 kbps e um TCP RTT de 0.05 segundos:

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

Nota: o <burst> é para uma sessão de TCP, assim que deve ser escalado para calcular a média do número esperado de sessões que vão através do vigilante. Este é apenas um exemplo, portanto, é necessário avaliar, em cada caso, os requisitos de tráfego/aplicativos e o comportamento versus recursos disponíveis para escolher os parâmetros de vigilância.

A ação de vigilância serve para derrubar o pacote (queda) ou alterar o DSCP do pacote (marcação para baixo). Para que o pacote seja marcado com valor inferior, é necessário modificar o mapa de DSCP vigiado. O DSCP policiado padrão observa o pacote ao mesmo DSCP, isto é, nenhuma marca ocorre para baixo.

Nota: É possível que os pacotes sejam enviados fora de ordem quando um pacote fora de perfil for marcado com um valor inferior a um DSCP para uma fila de saída diferente do DSCP original. Por este motivo, se pedir dos pacotes é importante, recomenda-se marcar abaixo dos pacotes de fora de perfil ao DSCP traçado à mesma fila de saída que pacotes em perfil.

As características da vigilância e marcação apoiaram pelos Engine do supervisor baseado em IOS do catalizador 4000/4500

O ingresso (interface de entrada) e a saída (interface enviada) que policia são apoiados no catalizador 4000 SE3, SE4, SE2+. O interruptor apoia 1024 ingressos e 1024 vigilâncias de saída.

Dois ingressos e duas vigilâncias de saída são usados pelo sistema para o comportamento depoliciamento do padrão.

Note que quando o policer agregado é aplicado dentro da política a um VLAN e a uma interface física, uma entrada de policer de hardware adicional é usado. Atualmente, não é possível vigiar as interfaces de VLAN e física juntamente no vigilante agregado. Isso pode ser alterado em versões de software futuras.

Todas as versões de software incluem o apoio para policiar. O catalizador 4000 apoia a declaração de compatibilidade válida até 8 pela classe, e até 8 classes são apoiadas pelo mapa de política. As declarações de compatibilidade válida são como segue:

- match access-group
- match ip dscp
- precedência compatível de ip
- combine alguns

Nota: Para pacotes V4 não-IP, a instrução match ip dscp é a única maneira de classificar, já que os pacotes estão entrando em portas de entroncamento confiando em CoS. Não se deixe confundir pela palavra-chave ip no comando match ip dscp, porque o DSCP interno tem correspondente, isso se aplica a todos os pacotes, não somente ao IP. Quando uma porta está configurada como CoS configurável, a última mencionada é extraída do quadro L2 (rotulado como 802.1Q ou ISL) e convertida como o DSCP interno que utiliza um mapa de QoS CoS para DSCP. Esse valor DSCP interno pode ser correspondido na política com o comando match ip dscp.

As ações de política válida são como segue:

- polícia
- set ip dscp
- set ip precedence
- trust dscp
- trust cos

A marcação permite a alteração do nível de QoS do pacote com base na classificação ou vigilância. A classificação racha o tráfego em classes diferentes para o processamento de QoS baseado em critérios definidos. A fim combinar a Precedência IP ou o DSCP, a interface de entrada correspondente deve ser ajustada ao modo confiado. O interruptor apoia a confiança de CoS, confiando o DSCP, e as interfaces não confiável. Trust (Confiança) especifica o campo a partir do qual o nível de QoS do pacote será derivado.

Ao confiar no CoS, o nível de QoS será derivado do cabeçalho L2 do ISL ou do pacote encapsulado 802.1Q. Ao confiar o DSCP, o interruptor derivará o QoS em nível do campo DSCP do pacote. Confiar no CoS só é importante nas interfaces de truncamento e confiar no DSCP é válido apenas para pacotes IP V4.

Quando uma interface não é confiável (este é o estado padrão quando QoS está habilitado), o DSCP interno será derivado do CoS ou DSCP configurável padrão para a interface correspondente. Se nenhum padrão CoS ou DSCP é configurado, o valor padrão será zero (0). Uma vez determinado o nível de QoS original do pacote, ele é mapeado no DSCP interno. O DSCP interno pode ser retido ou alterado por marcação ou vigilância.

Após a passagem do pacote pelo processamento do QoS, os campos de nível do QoS (no campo IP DSCP para o IP e no cabeçalho ISL/802.1Q, se houver) serão atualizados no DSCP interno.

Existem mapas especiais usados para converter a métrica QoS de confiança do pacote em DSCP interno e vice-versa. Estes mapas são como segue:

- DSCP DSCP policiado; usado para derivar DSCP sob vigilância ao registrar o pacote.
- DSCP para CoS: usado para derivar o nível de CoS a partir do DSCP interno para atualizar o cabeçalho do pacote de saída ISL/802.1Q.
- CoS para DSCP: usado para derivar o DSCP interno do CoS recebido (cabeçalho ISL/802.1Q) quando a interface está no modo Cos de confiança.

Observe que, quando uma interface está em modo CoS confiável, o CoS de saída sempre será o mesmo CoS de entrada. Isto é específico à implementação de QoS no catalizador 4000 SE3, SE4, SE2+.

Configurando e monitorando a vigilância

Configurar o policiamento nos IO envolve as seguintes etapas:

1. Definição de um vigilante.
2. Definindo critérios para selecionar tráfego para vigilância.
3. Definindo a serviço-política usando a classe e a aplicação de um vigilante a uma classe especificada.
4. Aplicação de uma política de serviço a uma porta ou VLAN.

Considere o seguinte exemplo. Há um gerador de tráfego anexado à porta 5/14 ~17 de emissão Mbps do tráfego UDP com um destino da porta 111. Queremos que o tráfego seja submetido à política de 1 Mbps e que o tráfego em excesso seja cancelado.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Note que quando uma porta reagir do modo QoS baseado em VLAN, mas nenhuma política de serviços é aplicada ao VLAN correspondente, o interruptor seguirá a política de serviços (eventualmente) aplicada em uma porta física. Isto permite uma flexibilidade adicional ao combinar QoS baseado em porta e em VLAN.

Existem dois tipos de vigilantes suportados: agregado nomeado e por interface. Um vigilante agregado nomeado vigiará o tráfego combinado de todas as interfaces às quais ele é aplicado. O exemplo acima utilizou um vigilante nomeado. Um vigilante por interface, diferentemente de um vigilante nomeado, irá vigiar o tráfego de forma separada em cada interface em que é aplicado. Um vigilante por interface é definido na configuração de mapa de política. Considere o exemplo a seguir com um vigilante agregado por interface:

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

O comando seguinte é usado monitorar a operação de vigilância:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

O contador próximo do mapa de classe está contando o número de pacotes que correspondem à classe correspondente.

Esteja ciente das considerações específicas da seguinte aplicação:

- O contador de pacote por classe não é por interface. Isto é, ele conta todos os pacotes correspondentes à classe, entre todas as interfaces em que essa classe é aplicada na política de serviços.

- Os vigilantes não mantêm contadores de pacote de informação, simplesmente os contadores de bytes são apoiados.
- Não há um comando específico para verificar a taxa de tráfego oferecida ou de saída por vigilante.
- Os contadores são atualizados em uma base periódica. Se o comando acima estiver sendo executando repetidamente em rápida sucessão, contadores ainda poderão aparecer em algumas ocasiões.

Configurando e monitorando a marcação

A configuração das marcas envolve os seguintes passos:

1. Defina os critérios para classificação do tráfego: lista de acesso, DSCP, precedência de IP etc.
2. Defina as classes de tráfego a ser classificadas usando os critérios definidos previamente.
3. Crie um mapa de políticas conectando ações de marcação e/ou ações de vigilância às classes definidas.
4. Configuração do modo confiável nas interfaces correspondentes.
5. Aplique o mapa de política a uma interface.

Considere o exemplo seguinte onde nós queremos o tráfego de entrada com Precedência IP 3 hospedar a porta 777 de 192.168.196.3 UDP traçada à Precedência IP 6. Todos os outros tráfegos de precedência 3 IP são vigiados a 1 Mbps e tráfego em excesso deve ser marcado com precedência 2 IP.

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

O comando do **sh policy interface** é usado monitorar a marcação. As implicações e a saída de amostra são documentadas na configuração de vigilância acima.

Comparando a vigilância e marcação nos Engine do supervisor baseado em IOS do catalizador 6000 e do catalizador 4000/4500

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

Informações Relacionadas

- Entendendo e configurando QoS
- Suporte Técnico - Cisco Systems