Política e marcação de QOS com os mecanismos de supervisor baseados em IOS Catalyst 4000/4500

Contents

Introduction

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. O DSCP é uma medida do nível de Qualidade de Serviço (QoS) 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.

A vigilância não deve ser confundida com a modelagem de tráfego, embora ambas assegurem que o tráfego permaneça no 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). A modelagem de tráfego armazena o tráfego fora de perfil e suaviza as rajadas de tráfego, mas afeta a variação de retardo e retardo. A modelagem só pode ser aplicada em uma interface de saída, enquanto a vigilância pode ser aplicada em interfaces de entrada e saída.

O Catalyst 4000/4500 com Supervisor Engine 3, 4 e 2+ (SE3, SE4, SE2+ a partir de agora neste documento) suporta policiamento em direções de entrada e saída. A modelagem de tráfego também é suportada, no entanto, este documento tratará apenas de policiamento e marcação. Marcação é um processo de alteração do nível de QoS do pacote, de acordo com uma política.

Prerequisites

Requirements

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, aplicamos o vigilante agregado para limitar o tráfego do Trivial File Transfer Protocol (TFTP) a 1 Mbps nas VLANs 1 e 3. Esse vigilante permitirá 1 Mbps de tráfego TFTP nas VLANs 1 e 3 juntas. Se aplicarmos um vigilante por interface, limitaremos o tráfego TFTP a 1 Mbps em cada VLAN de 1 a 3.

Observação: se a política de entrada e saída for aplicada a um pacote, a decisão mais grave será tomada. Ou seja, se o vigilante de ingresso especificar que o pacote seja descartado e o vigilante de saída especificar que ele será marcado como inativo, o pacote será descartado. 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	$Mark_e$	$Mark_e$

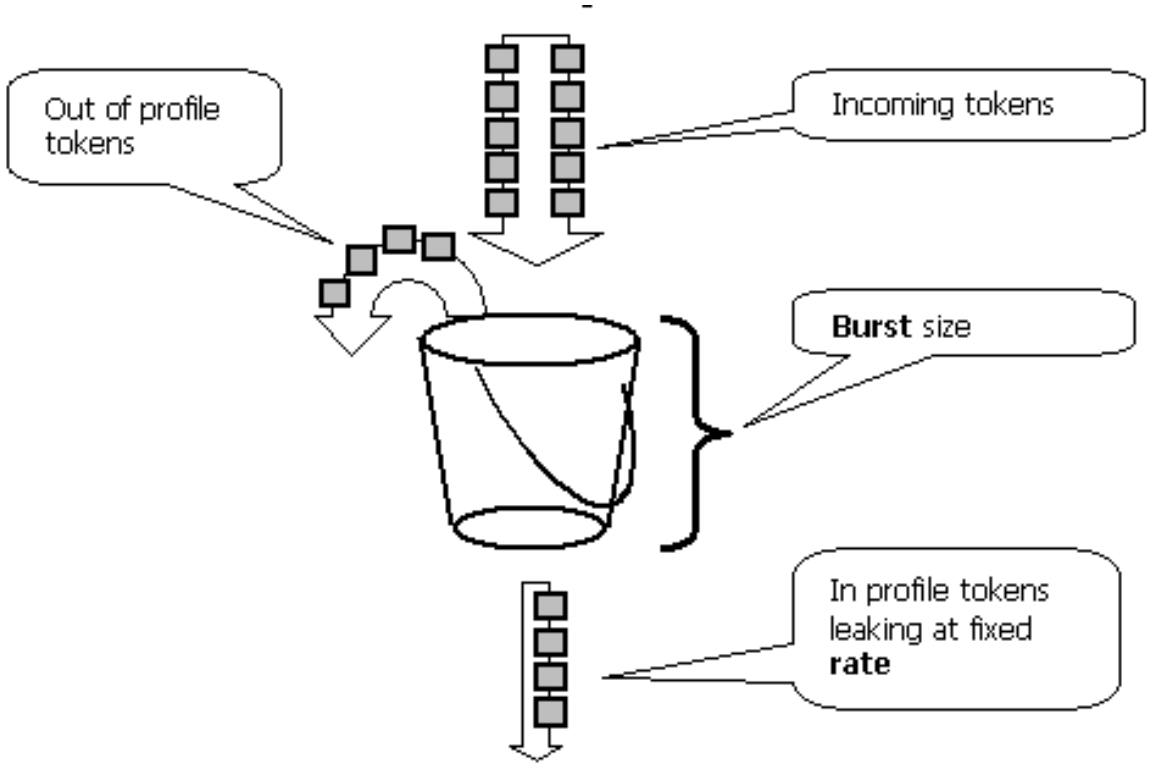
O hardware de QoS do Catalyst 4000 SE3, SE4, SE2+ é implementado de tal forma que a marcação real do pacote ocorre após o vigilante de saída. Isso significa que mesmo se a política de ingresso fizer uma marcação no pacote (por marcação do vigilante ou uma marcação normal), a política de egresso ainda 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. Isso 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 vigilantes agregados são por direção. Ou seja, se um vigilante agregado for aplicado tanto à entrada quanto à saída, haverá dois vigilantes agregados, um na entrada e um na saída.
- Quando um vigilante agregado é aplicado dentro da política às VLANs e à interface física, haverá efetivamente dois vigilantes agregados - um para as interfaces VLAN e outro para as interfaces físicas. Atualmente, não é possível vigiar as interfaces de VLAN e física juntamente no vigilante agregado.

O policiamento no Catalyst 4000 SE3, SE4, SE2+ está em conformidade com o conceito de vazamento de bucket, como ilustra o modelo abaixo. 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. O bucket é usado somente para decidir se o pacote está no perfil ou fora do perfil.

Observe que a implementação exata do hardware de policiamento pode ser diferente, funcionalmente, ela está em conformidade com o 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.

Consulte a seção Comparando Políticas e Marcação em Catalyst 6000 e Catalyst 4000/4500 IOS Based Supervisor Engines no final deste documento para obter diferenças na intermitência entre Catalyst 6000 e Catalyst 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 hardware de QoS do Catalyst 4000 SE3, SE4, SE2+ tem certa granularidade para a vigilância. Dependendo da taxa configurada, o desvio máximo da taxa é de 1,5% da taxa.

Ao configurar a taxa de burst, você precisa levar em conta que alguns protocolos (como o TCP) implementam mecanismos de controle de fluxo que reagem à perda de pacotes. Por exemplo, o TCP reduz a janela pela metade para cada pacote perdido. Quando policiada para uma determinada taxa, a utilização efetiva do link será inferior à taxa configurada. É possível aumentar a intermitência para obter melhor utilização. Um bom começo para esse tráfego seria definir a intermitência como igual ao dobro do tráfego enviado com a taxa desejada durante o tempo de ida e volta (RTT). Pelo mesmo motivo, não é recomendável fazer o benchmark da operação do vigilante por tráfego orientado a conexão, pois geralmente mostrará um desempenho menor do que o permitido pelo vigilante.

Observação: o tráfego sem conexão também pode reagir à vigilância de forma 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 descartado pode disparar muitos pacotes (bloco inteiro) para serem retransmitidos.

Por exemplo, o seguinte é um cálculo da intermitência para uma sessão 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]
```

Observação: <burst> é para uma sessão TCP, então ela deve ser dimensionada para a média do número esperado de sessões 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 comenta o pacote para o mesmo DSCP, ou seja, nenhuma marca baixa ocorre.

Observação: os pacotes podem ser enviados fora de ordem quando um pacote fora de perfil é marcado para um DSCP em uma fila de saída diferente do DSCP original. Por esse motivo, se a ordenação de pacotes for importante, é recomendável marcar pacotes fora de perfil para DSCP mapeados para a mesma fila de saída dos pacotes no perfil.

Recursos de policiamento e marcação suportados pelos Catalyst 4000/4500 IOS-Based Supervisor Engines

As políticas de entrada (interface de entrada) e saída (interface de saída) são suportadas no Catalyst 4000 SE3, SE4, SE2+. O switch suporta 1024 vigilantes de entrada e 1024 de saída. Dois vigilantes de entrada e dois de saída são usados pelo sistema para o comportamento padrão sem vigilância.

Observe que quando o vigilante agregado é aplicado dentro da política a uma VLAN e a uma interface física, uma entrada adicional de vigilante de hardware é usada. 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 suporte para vigilância. O Catalyst 4000 suporta até 8 instruções de correspondência válidas por classe e até 8 classes são suportadas por mapa de política. As instruções de correspondência válidas são as seguintes:

- match access-group
- match ip dscp
- precedência compatível de ip
- match any

Observação: para pacotes V4 não IP, a instrução **match ip dscp** é a única forma de classificação, desde que os pacotes estejam 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 válidas são as seguintes:

- 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 divide o tráfego em diferentes classes para o processamento de QoS com base em critérios definidos. Para corresponder a precedência de IP ou DSCP, a interface de entrada correspondente deve ser definida no modo confiável. O switch oferece suporte a CoS confiável, DSCP confiável e interfaces não confiáveis. 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 no DSCP, o switch derivará o nível de QoS 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 CoS ou DSCP padrão estiver 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 os seguintes:

- DSCP para 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. Isso é específico para a implementação de QoS no Catalyst 4000 SE3, SE4, SE2+.

Configurando e monitorando a vigilância

A configuração da vigilância no IOS envolve as seguintes etapas:

1. Definição de um vigilante.
2. Definindo critérios para selecionar tráfego para vigilância.
3. Definir política de serviço usando a classe e aplicando 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 conectado à porta 5/14 enviando ~17 Mbps de 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
!
```

Observe que, quando uma porta está no modo QoS baseado em VLAN, mas nenhuma política de servidor é aplicada à VLAN correspondente, o Switch seguirá a política de servidor (se houver)

aplicada a 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 seguinte comando é usado para 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 seguintes considerações específicas de implementação:

- 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 pacotes; somente contadores de bytes são suportados.
- Não há um comando específico para verificar a taxa de tráfego oferecida ou de saída por vigilante.
- Os contadores são atualizados periodicamente. 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 serem classificadas usando critérios previamente definidos.
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 a seguir onde queremos que o tráfego de entrada com precedência de IP 3 seja o host 192.168.196.3, porta UDP 777 mapeada para precedência de 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.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
```

```
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

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

Comparando políticas e marcações em mecanismos de supervisor baseados em IOS Catalyst 6000 e Catalyst 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