Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit en détail quels types de trafic sont appariés contre les class-map par défaut, qui font partie du Catalyst 6500 par défaut Sup2T/de la configuration CoPP du Catalyst 6880 (Réglementation du plan de commande) qui est automatiquement configurée sur le périphérique. Ceci est configuré afin de protéger sa CPU contre être surchargée.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

CoPP est activé par défaut sur le Catalyst 6500/SUP2T et Commutateurs du Catalyst 6880 et est basé sur un modèle préconfiguré. Quelques configuration de class-map n'ont pas des déclarations correspondantes de correspondance étant donné qu'ils capturent le trafic pas sur la liste de contrôle d'accès MAC/IP (ACL), mais plutôt sur les exceptions internes qui sont signalées par l'engine d'expédition quand le trafic est reçu par le commutateur et une décision d'expédition pris.

Si un class-map spécifique doit être ajouté/modifié/retiré de la stratégie en cours de CoPP, alors il doit être fait du mode de configuration dans le mode de policy-map. Voir le guide de configuration du logiciel de version 15.0SY de Catalyst 6500 - Réglementation du plan de commande (CoPP) pour la syntaxe exacte.

Les classes d'exception de par défaut de CoPP ont ces descriptions :

Cas	nom de class-map	Description
Panne de Maximum Transmission Unit (MTU)	classe-copp-mtu-échec	La longueur de paquet dépasse la taille sortante d'interface MTU. Si le bit de Don't Fragment n'est pas placé, la fragmentation est exigée. Si le bit de Don't Fragment est placé, le message d'inaccessibilité de destination de Protocole ICMP (Internet Control Message Protocol) indique que la « fragmentation a eu besoin et le DF placer » est censé être généré et renvoyé à la source. Référence : RFC-791, RFC-1191
Panne du Time to Live (TTL)	classe-copp-TTL-échec	Paquet TTL = 1 (pour l'ipv4), limite de saut = 0 ou 1 (pour l'IPv6) Le TTL = 0 (pour l'ipv4) peut être jeté dans le matériel immédiatement pendant que le saut précédent est censé détruire le paquet quand le TTL est décrémenté à 0. La limite de saut = 0 (pour l'IPv6) est différente de TTL = 0 parce qu'on lui énonce dans RFC-2460, la section 8.2 que « à la différence de l'ipv4, des Noeuds d'IPv6 ne sont pas exigé pour imposer la vie maximum de paquet. C'est la raison que le champ de Time to Live d'ipv4 a été renommé limite de saut dans IPv6". Ceci signifie que le paquet entrant d'IPv6 avec la limite de saut = 0 est encore valide, et le message ICMP devrait être renvoyé. Référence : RFC-791, RFC-2460
Options	classe-copp-options	Paquet avec des options (pour l'ipv4), en-tête d'extension de saut par saut (pour l'IPv6). Par exemple, routeur RFC-2113 vigilant, artère stricte de source, et ainsi de suite. Des en-têtes d'extension ne sont pas examinées ou sont traitées par tout noeud le long du chemin de la livraison d'un paquet, jusqu'à ce que le paquet atteigne le noeud (ou chacun de l'ensemble de Noeuds dans l'ofmulticast de cas) identifié dans le champ d'adresse de destination de l'en-tête theIPv6. La

		seule exception est l'en-tête d'options de saut par saut, qui diffuse les informations qui doivent être examinées et traitées par chaque noeud le long du chemin de la livraison d'un paquet, qui inclut les noeuds sources et de destination. Le matériel traitant sur des champs d'option n'est pas pris en charge, cela est traitement de logiciel/commutation est nécessaire. Référence : RFC-791/RFC-2460
Panne du Reverse Path Forwarding (RPF) (Unicast)	classe-copp-ucast-RPF-échec	Le contrôle manquant du paquet RPF est filtré. Cependant, en raison des ressources limitées dans le matériel, le contrôle RPF ne peut pas être fait dans le matériel dans certains cas (c'est-à-dire, plus de 16 interfaces RPF liées à un IP). Quand cela se produit, le paquet est envoyé au logiciel pour un contrôle complet RPF. Le premier RPF a manqué paquet de données (adressé à un groupe de multidiffusion) est envoyé au logiciel afin du Protocol Independent Multicast (PIM) - affirment le processus pour commencer. Une fois que le processus est fait, un routeur/expéditeur indiqués est élu. Si le paquet suivant (le même écoulement) ne provient pas le routeur indiqué, il déclenche une panne RPF, et le matériel peut la relâcher immédiatement (afin d'empêcher une attaque de Déni de service (DOS)).
Échec RPF (Multidiffusion)	classe-copp-mcast-RPF-échec	Le premier RPF a manqué paquet de données (adressé à un groupe de multidiffusion) est envoyé au logiciel pour que le processus de PIM-affirmation commence. Une fois que le processus est fait, un routeur/expéditeur indiqués est élu. Si le paquet suivant (le même écoulement) ne provient pas le routeur indiqué, il déclenche une panne RPF, et le matériel peut la relâcher immédiatement (afin d'empêcher une attaque DoS). Cependant, si la table de routage est mise à jour, un nouveau routeur indiqué pourrait devoir être choisi (par l'intermédiaire de PIM-affirmez), qui veut dire que le RPF a manqué paquet doit atteindre le logiciel (pour que PIM-affirmez reprenne). Afin de faire cela, une

		fuite périodique au mécanisme logiciel (par écoulement) pour le paquet RPF-échoué est disponible dans le matériel. La note cependant, s'il y a une énorme quantité d'écoulements puis une fuite périodique peut être trop pour que le logiciel manipule. Le matériel CoPP est encore exigé pour la Multidiffusion RPF a manqué paquet. Référence : RFC-3704, RFC-2362
Réécriture des paquets de matériel non prise en charge	classe-copp-unsupp-réécriture	Tandis que le matériel peut réécrire des paquets dans divers cas, quelques cas juste ne peuvent pas être faits dans la conception matérielle en cours. Et pour ceux, le matériel envoie le paquet au logiciel.
NO--artère d'ICMP Acl-baisse d'ICMP L'ICMP réorientent	classe-copp-ICMP-réorienter-inaccessible	Les paquets ont envoyé au logiciel pour la génération des messages ICMP. Comme l'ICMP réorientez, destination ICMP inaccessible (par exemple. inaccessible d'hôte ou administrativement interdit). Référence : RFC-792/RFC-2463
Le Technologie Cisco Express Forwarding (CEF) reçoivent (l'IP de destination est l'IP du routeur)	classe-copp-recevez	Si l'IP de la destination du paquet est l'une des adresses IP du routeur (frappera le CEF reçoivent la contiguïté), alors le logiciel est censé traiter le contenu.
Le CEF glanent (l'IP de destination appartient à un du réseau du routeur)	classe-copp-glanez	Si l'IP de la destination du paquet appartient à un du réseau du routeur, mais il n'est pas résolu (c'est-à-dire, aucun hit dans la table de Forwarding Information Base (FIB)), il frappera le CEF glanent la contiguïté, étant envoyé au logiciel où la procédure de résolution obtiendra commencé. Pour l'ipv4, le même écoulement continue à frapper le CEF glanent jusqu'à ce que l'adresse soit résolue. Pour l'IPv6, une entrée provisoire de FIB qui s'assortit l'IP de destination (et les points pour relâcher la contiguïté à la place) obtient installé pendant la résolution. S'il ne peut pas être résolu dans la durée spécifiée, l'entrée de FIB est retirée (c'est-à-dire, les mêmes débuts d'écoulement pour frapper le CEF glanent de nouveau).
Paquet destiné au	classe-copp-mcast-IP-control	Le paquet de contrôle doit être traité par le logiciel.

multicast IP 224.0.0.0/4 Paquet destiné au multicast IP FF::/8	class-copp-mcast-ipv6-control	Le paquet de contrôle doit être traité par le logiciel.
Paquet de multidiffusion qui doit être copié sur le logiciel	classe-copp-mcast-copie	Dans certains cas, le paquet de multidiffusion doit être copié sur le logiciel pour une mise à jour d'état (le paquet est toujours matériel pont sur le même VLAN). Par exemple, (*, G/m) frappé pour l'entrée dense de mode, basculement double-RPF SPT.
Paquet de multidiffusion obtenant un coup manqué dans la table FIB	classe-copp-mcast-coup de volée	L'IP de destination (multicast IP) est un coup manqué dans la table FIB. Le paquet est donné un coup de volée au logiciel.
Source directement connectée (ipv4)	classe-copp-IP-connecté	Le trafic de multidiffusion des sources directement connectées sont envoyés au logiciel où un état de Multidiffusion peut être créé (et installé dans le matériel).
Source directement connectée (IPv6)	class-copp-ipv6-connected	Le trafic de multidiffusion des sources directement connectées sont envoyés au logiciel où un état de Multidiffusion peut être créé (et installé dans le matériel).
Paquet d'émission	classe-copp-émission	Des paquets d'émission (par exemple, IP/Non-IP avec émission DMAC et unicast sur IP avec Multidiffusion DMAC) sont coulés au logiciel.
Inconnu de Protocol à (c'est-à-dire, non vérifié par) en termes de commutation de matériel	classe-copp-UNKNOWN-Protocol	Le protocole Non-IP, tel que l'Internetwork Packet Exchange (IPX) et ainsi de suite, ne sera pas matériel commuté. Ils sont envoyés au logiciel et obtiennent expédié là.
Le trafic de données multicast étant livré dedans par l'intermédiaire du port conduit où PIM est désactivé	class-copp-mcast-v4-data-on-routedPort	Le trafic de données multicast qui entre par un port conduit (où PIM est désactivé) est coulé au logiciel. Cependant, il n'est pas nécessaire de les envoyer au logiciel ainsi ils sont lâchés.
Le trafic de données multicast étant livré dedans	class-copp-mcast-v6-data-on-routedPort	Le trafic de données multicast qui entre par un port conduit (où PIM est désactivé) est coulé au logiciel. Cependant, il n'est pas nécessaire de les

par l'intermédiaire du port conduit où PIM est désactivé		envoyer au logiciel ainsi ils sont lâchés.
Passerelle de redirect to d'ACL d'entrée le paquet	classe-copp-ucast-d'entrée-acl-jeté un pont sur	Le matériel a 8 exceptions liées à l'acl réglées par le logiciel par l'intermédiaire d'un ACL pour réorienter. Celui-ci associe dans des paquets monodiffusions pont l'à la CPU par l'ACL pour la mémoire associative ternaire (TCAM) a associé des raisons.
Passerelle de redirect to d'ACL de sortie le paquet	classe-copp-ucast-de sortie-acl-jeté un pont sur	Le matériel a 8 exceptions liées à l'acl réglées par le logiciel par l'intermédiaire d'un ACL pour réorienter. Celui-ci associe dans des paquets monodiffusions pont l'à la CPU par l'ACL pour la mémoire associative ternaire (TCAM) a associé des raisons.
Paquets de passerelle de redirect to d'ACL de Mcast à la CPU	classe-copp-mcast-acl-jeté un pont sur	Le matériel a 8 exceptions liées à l'acl réglées par le logiciel par l'intermédiaire d'un ACL pour réorienter. Celui-ci associe au traitement de Multidiffusion.
Passerelle d'ACL à la CPU pour le procédé d'équilibrage de charge du serveur	classe-copp-slb	Le matériel a 8 exceptions liées à l'acl réglées par le logiciel par l'intermédiaire d'un ACL pour réorienter. Celui-ci associe à un matériel réorientent pour une décision d'Équilibrage de charge de serveur (SLB).
Le log de l'ACL VACL réorientent	classe-copp-vacl-log	Le matériel a 8 exceptions liées à l'acl réglées par le logiciel par l'intermédiaire d'un ACL pour réorienter. Celui-ci associe à la redirection de paquet par ACL de la liste de contrôle d'accès VLAN (VACL) à la CPU pour le Cisco IOS se connecter des buts.
Surveillance DHCP	classe-copp-DHCP-piller	Le DHCP a pillé des paquets sont réorientés à la CPU pour le traitement DHCP
La stratégie de MAC a basé l'expédition	classe-copp-MAC-pbf	L'expédition basé par stratégie doit être fait dans la CPU puisque le matériel n'est pas capable pour expédier des paquets dans ce cas.
Contrôle d'admission au réseau d'ip admission	classe-copp-IP-admission	Afin de fournir l'accès au réseau basé sur les qualifications de l'antivirus de l'hôte, il y a validation de posture par l'intermédiaire d'une des ces options : (1) l'interface L2 utilisera IP de port LAN (LPIP), où des paquets de Protocole ARP

		(Address Resolution Protocol) sont réorientés qu'à la CPU, (2) l'interface L3 utilise l'adresse IP de passerelle (GWIP). Après la validation, il y a l'authentification (*). Pour une interface L2 c'est WebAuth, qui exécute l'interception de paquet de HTTP et pourrait également exécuter la redirection URL (*). Pour l'interface L3, c'est AuthProxy.
Inspection dynamique d'ARP	classe-copp-ARP-piller	Afin d'empêcher l'attaque (homme-dans-le-moyenne) d'empoisonnement d'ARP, inspection dynamique d'ARP (également connue sous le nom d'inspection dynamique d'ARP (DAI)) valide les demandes/réponses d'ARP par quand il les intercepte et puis traite dans la CPU contre une de ceux-ci : (1) ARP utilisateur-configuré ACLs (pour les hôtes statiquement configurés), (2) adresse MAC aux attaches d'adresse IP enregistrées dans la base de données de confiance (c'est-à-dire, liaisons DHCP). Seulement des paquets valides d'ARP sont utilisés pour mettre à jour le cache local d'ARP ou expédiés. Le processus de validation exige l'implication CPU de paquets d'ARP, qui signifie que le matériel CoPP est nécessaire afin d'empêcher une attaque DoS.
CPU de redirect to d'ACL pour le WCCP	classe-copp-wccp	Utilisé au cas où le paquet/écoulement devrait être réorienté à la CPU pour la décision d'expédition du Web Cache Communication Protocol (WCCP).
CPU de redirect to d'ACL pour l'architecture de mise en place de service (SIA)	classe-copp-service-mise en place	Utilisé au cas où le paquet/écoulement devrait être réorienté à la CPU pour la décision SIA.
Détection de réseau d'IPv6	classe-copp-ND	Afin de réorienter le paquet de détection de réseau d'IPv6 à la CPU pour traiter plus loin. Référence : RFC4861

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier s'il y avait du trafic observé dans les class-map configurés l'uns des de CoPP,

sélectionnez la commande de **show policy-map control-plane**.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Commutateurs de la gamme Cisco Catalyst 6500 protecteur utilisant la Réglementation du plan de commande, la limitation de débit de matériel, et les listes de contrôle d'accès
- Guide de configuration du logiciel de version 15.0SY de Catalyst 6500 - Réglementation du plan de commande (CoPP)
- Support et documentation techniques - Cisco Systems