Utilisation de Cisco Service Assurance Agent et de Internetwork Performance Monitor pour gérer la qualité de service dans les réseaux Voix sur IP

Contenu

Introduction

Ce document décrit l'utilisation du Cisco Service Assurance Agent (SAA) et de l'Internetwork Performance Monitor (IPM) de mesurer le Qualité de service (QoS) dans des réseaux de la voix sur ip (VoIP). Ces informations sont basées sur un projet du monde réel de Téléphonie sur IP. Ce document se concentre sur l'application des Produits, pas sur les Produits eux-mêmes. Vous devriez déjà être familiarisé avec Cisco SAA et IPM et avoir accès à la documentation du produit priée. Voir les informations relatives pour des références à l'autre documentation.

Remarque: La fonctionnalité de Cisco SAA en logiciel de Cisco IOS® a été autrefois connue comme Fonction Response Time Reporter (RTR).

Quand vous gérez un réseau VoIP de grande puissance, vous devez avoir les outils nécessaires objectivement surveillez et rendez compte de la Qualité vocale dans le réseau. Il n'est pas faisable de compter sur seul le feedback des utilisateurs, parce qu'il est souvent subjectif et inachevé. Les problèmes de qualité voix proviennent typiquement des problèmes de QoS de réseau. Ainsi, quand vous identifiez des problèmes de qualité voix, vous avez besoin d'un deuxième outil pour gérer et surveiller le réseau QoS. L'exemple dans ce document utilise Cisco SAA et IPM à cet effet.

Cisco Voice Manager (CVM) est utilisé avec Telemate.net pour gérer la Qualité vocale. Il rend compte de la Qualité vocale des appels par l'intermédiaire du problème/du facteur de planification calculé de problème (ICPIF) qui est calculé par une passerelle de Cisco IOS pour chaque appel. Ceci permet au gestionnaire de réseau pour identifier les sites qui souffrent de la médiocre qualité de voix. Référez-vous à la gestion de la qualité vocale avec le pour en savoir plus de Cisco Voice Manager (CVM) et de Telemate.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité aux versions de matériel ou logiciel spécifiques, mais les exemples dans ce document utilisent ces le logiciel et les versions de matériel :

- Logiciel Cisco IOS version 12.1(4)
- IPM 2.5 pour Windows NT
- Commutateur de gamme Catalyst 4500

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.

Questions de QoS dans un réseau VoIP

Plusieurs facteurs peuvent dégrader la Qualité vocale dans un réseau de voix en paquets :

- Perte de paquets
- Retard excessif
- Instabilité excessive

Il est particulièrement important que vous surveilliez ces figures sur une base actuelle, si des services de commutation de paquets sont utilisés dans le WAN (par exemple, atmosphère, Relais de trames, ou réseau privé virtuel IP). Il y a de nombreux scénarios où l'encombrement dans le réseau d'opérateur, le trafic misconfigured formant sur les périphériques de périphérie, ou le maintien de l'ordre misconfigured du côté porteuse peut entraîner la perte de paquets ou la mise en mémoire tampon excessive. Quand le transporteur relâche des paquets, il n'y a aucune preuve évidente sur les périphériques de périphérie. Par conséquent, vous avez besoin d'un outil de bout en bout comme Cisco SAA qui peut injecter le trafic sur le d'entrée et validez son arrivée réussie au de sortie.

Gérer QoS avec Cisco SAA et IPM

Il y a trois Cisco SAA et des composants IPM :

- Sonde de RTR
- Rtr responder
- Console IPM

La sonde de RTR envoie une rafale des paquets au rtr responder. Le rtr responder les tourne autour et les envoie de nouveau à la sonde. Cette exécution simple permet à la sonde pour mesurer la perte de paquets et le délai d'aller-retour. Pour mesurer le jitter, la sonde envoie un paquet de contrôle au responder avant qu'elle initie la rafale de paquet. Le paquet de contrôle informe le responder combien de millisecondes (ms) à prévoir entre chaque paquet dans la rafale.

Le responder mesure alors le retard d'inter-paquet pendant la rafale, et n'importe quelle déviation de l'intervalle de prévoir est enregistrée en tant que jitter.

Les contrôles de console IPM la surveillance de QoS. Il programme les sondes de RTR avec les informations pertinentes par l'intermédiaire du Protocole SNMP (Simple Network Management Protocol). Il collecte également les résultats par l'intermédiaire du SNMP. Aucune configuration Cisco IOS d'interface de ligne de commande n'est exigée sur les sondes de RTR.

Émettez la commande de configuration globale de **rtr responder**, de configurer manuellement les rtr responder.

Les sondes et les responders de RTR doivent exécuter le Logiciel Cisco IOS version 12.0(5)T ou plus tard. La dernière release de maintenance du courant principal 12.1 est recommandée. Les sondes et les responders de RTR dans les exemples dans ce document exécutent la version 12.1(4). La version IPM est en service IPM 2.5 pour Windows NT. Un correctif est disponible sur Cisco.com pour cette version. Ce correctif est important, car il répare un problème où l'IPM configure les sondes de RTR avec un établissement incorrect de Priorité IP.

Conception

Avant que vous déployiez Cisco SAA et la solution IPM, vous devez effectuer un certain travail de conception avec ces considérations à l'esprit :

- Placement des sondes et des responders de RTR
- Type de trafic qui est envoyé de la sonde au responder

Il y a un certain nombre de choses à prendre en compte quand vous décidez au sujet du placement des sondes et des responders. D'abord, vous voulez que la mesure de QoS couvre chaque site, pas simplement des sites à problème. C'est parce que les nombres de retard et instabilité que l'IPM signale pour un site donné sont les plus utiles une fois comparés à d'autres sites dans le même réseau. Ainsi, vous voulez mesurer des sites avec bon QoS *et* QoS pauvre. En outre, un site performant peut devenir un site pauvre-exécutant demain, dû aux changements des structures de trafic ou des modifications de réseau. Vous voudrez détecter ceci avant qu'il affecte la Qualité vocale et soit signalé par les utilisateurs.

En second lieu, l'utilisation du processeur est importante. Déjà un routeur saturé peut ne pas pouvoir entretenir le composant de RTR en temps utile, et ceci peut biaiser les résultats. En outre, si vous placez trop d'exemples de sonde sur n'importe quel routeur unique, vous pourriez créer des problèmes d'utilisation du CPU élevé quoiqu'aucun n'ait existé avant. L'approche choisie pour le réseau d'exemple dans ce document (et ceci devrait fonctionner dans la plupart des réseaux) est de placer les sondes de RTR sur le distant/Routeurs secondaires. Ces Routeurs connectent typiquement un LAN unique à un service WAN relativement lent. Par conséquent, les Routeurs secondaires souvent ont l'utilisation du processeur très basse et peuvent facilement faire face au RTR. L'autre avantage de cette conception est que vous distribuez le chargement à travers autant de Routeurs comme possibles. Maintenez dans l'esprit que c'est plus de travail à être une sonde que pour être un responder, car les sondes prennent une interrogation SNMP.

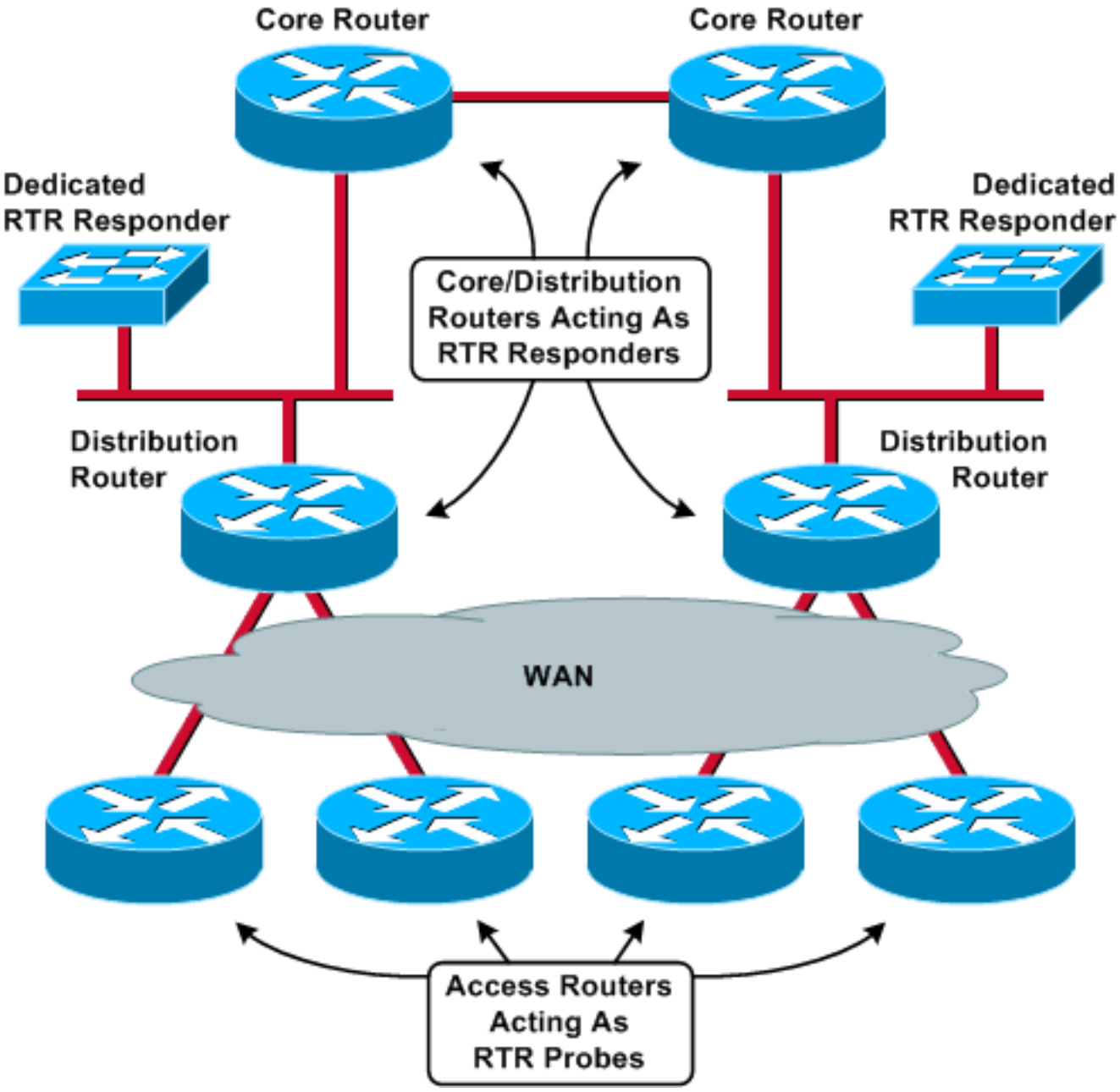
Avec cette conception, les rtr responder doivent être placés au centre. Les responders seront plus occupés que les sondes, parce qu'ils répondront à beaucoup de sondes. Ainsi, une conception robuste déploie les Routeurs dédiés qui agissent seulement comme des responders. La plupart des organismes ont retiré des Routeurs sur le module qui peut remplir cette fonction. N'importe quel routeur avec une interface Ethernet suffira. Alternativement, le noyau/routeurs de distribution peut doubler comme responders. Le schéma de réseau dans cette section dépeint les deux

scénarios.

Propagez-vous le chargement à travers autant de Routeurs comme possibles, et surveillez l'utilisation du CPU de RTR avec cette commande :

```
Router# show processes cpu | i Rtt|PID

PID  Runtime(ms)   Invoked  uSecs  5Sec   1Min   5Min    TTY Process
67           0         7      0   0.00%  0.00%  0.00%   0 Rtt Responder
```



Quand vous appariez des sondes avec des responders, il est recommandé que vous mettez à jour une topologie cohérente entre la sonde et le responder. Par exemple, tous les sondes et responders devraient être séparés par le même nombre de Routeurs, de Commutateurs, et de liens WAN. Seulement alors peuvent des résultats IPM être directement comparés parmi des sites.

Dans cet exemple, il y a 200 sites distants et quatre sites de noyau/distribution. Un Catalyst 4500 à chaque site de distribution agit en tant que rtr responder dédié. Chacun des 200 Routeurs distants agit en tant que sonde de RTR. Chaque sonde vise le responder qui se trouve au site directement connecté de distribution.

Les rafales de trafic envoyées par les sondes aux responders doivent être données les mêmes niveaux de QoS par le réseau qu'est donné pour exprimer. Ceci peut signifier que vous devez ajuster la basse latence faisant la queue (LLQ) ou conduisant des configurations prioritaires de protocole de tables (RTP) sur le routeur, de sorte que le trafic des sondes de RTR soit sujet à la file d'attente à priorité déterminée stricte. Quand vous configurez la sonde pour des paquets de RTP, seulement le port de Protocole UDP (User Datagram Protocol) de destination peut être commandé et pas le port de source. Une configuration de routeur typique LLQ dans ce réseau d'exemple a les Listes d'accès qui classifient spécifiquement les paquets de RTR dans la même file d'attente que la Voix :

```
Router# show processes cpu | i Rtt|PID

PID  Runtime(ms)  Invoked  uSecs  5Sec   1Min   5Min    TTY Process
67           0         7      0   0.00%  0.00%  0.00%   0 Rtt Responder
```

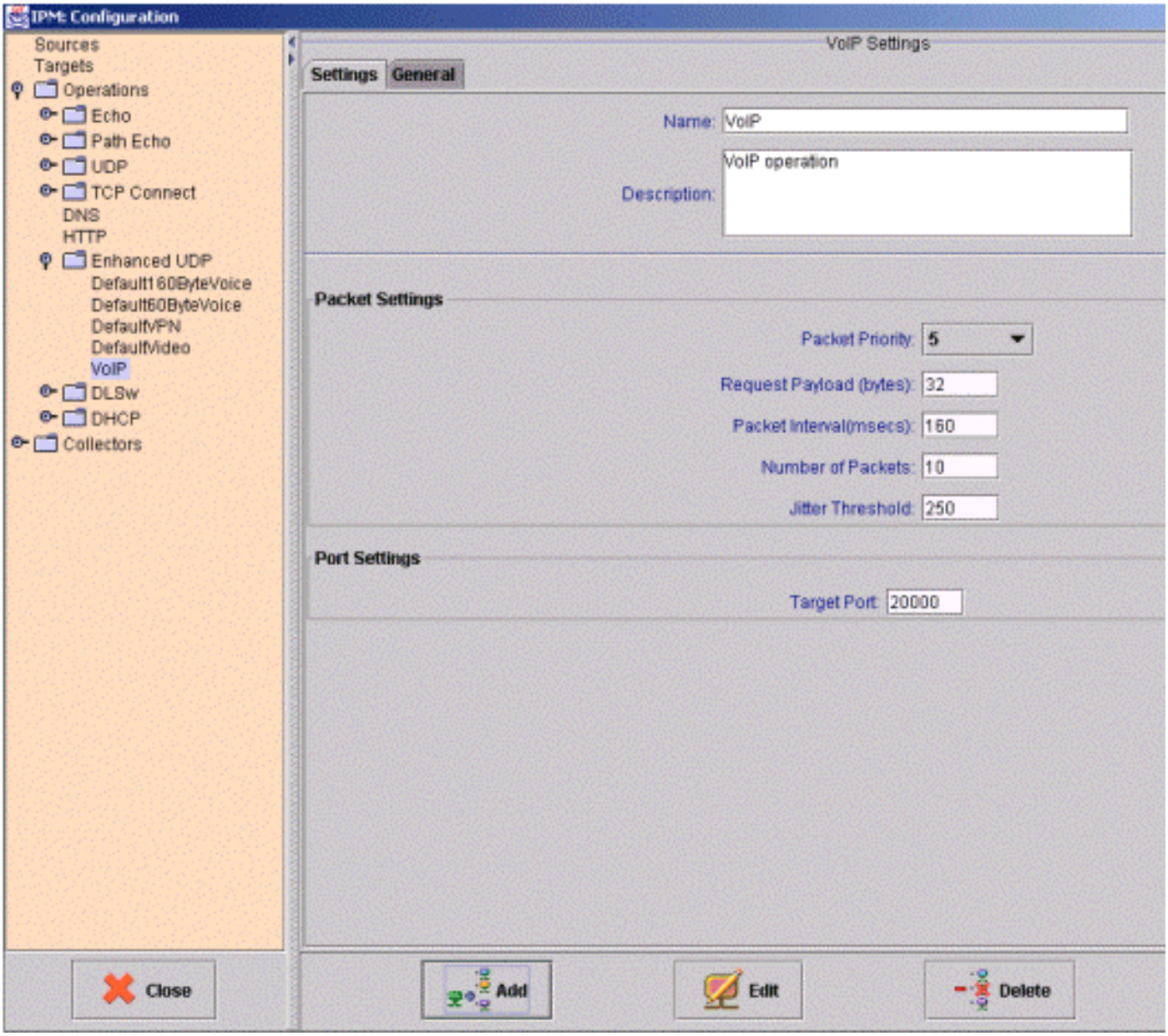
La liste d'accès IP-RTP a ces lignes de classification :

- `refusez à IP tous les n'importe quels fragments`Refusez tout fragment IP, comme une liste d'accès de la couche 4 permet implicitement ces derniers.
- `plage 16384 de 10.0.16.0 0.255.239.255 d'UDP d'autorisation 32768 priorité de la plage 16384 de 10.0.16.0 0.255.239.255 32768 essentielle`Paquets de RTP d'autorisation des sous-réseaux de Voix avec la Priorité IP réglée à 5.
- `permettez à UDP n'importe quelle n'importe quelle priorité de l'eq 20000 essentielle`Les paquets de RTP d'autorisation du RTR sondent aller au rtr responder.
- `permettez à UDP tout eq 20000 n'importe quelle priorité essentielle`Paquets de RTP d'autorisation du rtr responder allant de retour à la sonde de RTR.

Faites attention que l'ajout du trafic de RTR ne fait pas sur-être abonné et causer les files d'attente LLQ de vrais paquets vocaux d'être abandonnées. L'exécution standard **Default60ByteVoice** IPM envoie des rafales des paquets de RTP avec ces paramètres :

- Charge utile de demande : 60 octets**Remarque:** C'est l'en-tête et la Voix de RTP. Ajoutez 28 octets (IP/UDP) pour obtenir la taille du datagramme L3.
- Intervalle : 20 ms
- Nombre de paquets : 10

Ceci signifie que, pendant une rafale, le RTR consomme 35.2 KBS de la bande passante LLQ. S'il n'y a pas bande passante suffisante pour LLQ, alors créez une nouvelle exécution IPM et augmentez le packet interval. Les paramètres étant affiché dans cette fenêtre de configuration IPM, une rafale consomme le Kbps seulement 1 de la bande passante :



Résultats

La table dans cette section est un exemple d'un état IPM. Cet état contient trois exemples de sonde de RTR. Maintenez dans l'esprit qu'une sonde physique peut être configurée avec les plusieurs exemples de sonde de RTR qui visent différents responders ou utilisent différentes charges utiles.

Daily Jitter Summary Report 11/15/2000										
Collector Info		Round Trip Latency		Src Dest Jitter		Dest Src Jitter		Completions		
Collector	Operation	Avg	Avg Max	Avg	Avg Max	Avg	Avg Max	Trys	Over %	Error %
haw-WN	VoIP	72.71	102.79	1.74	7.65	2.62	25.88	1440	0%	0%
	Last Week	75.65	105.41	1.73	4.16	4.97	24.18	10113	0%	1%
	Last Month	74.89	103.01	1.70	3.77	6.74	24.98	7822	0%	1%
wat-WN	VoIP	72.27	121.88	2.17	12.50	3.19	39.13	1447	0%	1%
	Last Week	75.45	112.96	1.99	5.18	5.40	31.21	10127	0%	1%
	Last Month	74.00	110.51	1.83	4.91	6.44	29.76	7826	0%	1%
sfd-WN	VoIP	70.43	114.13	1.80	8.08	2.68	32.08	1440	0%	0%
	Last Week	73.92	112.17	1.75	4.68	4.94	30.19	10098	0%	1%
	Last Month	72.90	104.13	1.79	4.82	6.41	27.30	7831	0%	1%

Ce sont les significations de chacune des colonnes :

Moyenne :

L'IPM calcule une moyenne pour chaque heure de l'échantillonnage. Ces moyennes horaires sont alors ramenées à une moyenne à travers une plus longue période pour obtenir le quotidien, l'hebdomadaire, ou les moyennes mensuelles. En d'autres termes, pour l'état quotidien, l'IPM calcule la moyenne pour chaque heure pour les dernières 24 heures. Il calcule alors la moyenne quotidienne comme moyenne de ces 24 moyennes.

Moyenne maximum :

Cette valeur est la moyenne de tous les maximum horaires pour chaque jour, semaine, et mois dans le tableau. En d'autres termes, pour l'état quotidien, l'IPM prélève le plus grand échantillon signalé dans chacune des dernières 24 heures. Il calcule alors la moyenne maximum quotidienne comme moyenne de ces 24 échantillons.

Au-dessus de % :

C'est le pourcentage des échantillons qui étaient au-dessus du seuil configuré pour le collecteur.

Erreur % :

C'est le pourcentage des paquets qui ont rencontré une erreur. Une sonde de jitter signale plusieurs types d'erreurs :

- Perte de paquets écart-type — Paquets perdus entre la source et la destination
- Perte de paquets DS — Paquets perdus entre la destination et la source
- Busies — Le nombre d'occasions quand une exécution de Round-Trip Time (DURÉE DE TRANSMISSION) ne pourrait pas être initiée parce qu'une exécution précédente de DURÉE DE TRANSMISSION n'avait pas été terminée
- Ordre — Le nombre de fins d'exécution de DURÉE DE TRANSMISSION reçues avec un

identifiant inattendu d'ordre. Ce sont quelques possibles raison pourquoi ceci pourrait se produire :Un paquet dupliqué a été reçu.Une réponse a été reçue après qu'elle ait eu synchronisé-.Un paquet corrompu a été reçu et n'a pas été détecté.
- Baisses — Le nombre d'occasions quand l'un ou l'autre de ces derniers s'est produite :Une exécution de DURÉE DE TRANSMISSION ne pourrait pas être initiée parce qu'une certaine ressource interne nécessaire n'était pas disponible (par exemple, mémoire ou le sous-système de Systems Network Architecture [SNA])La fin d'exécution n'a pas pu être identifiée.
- MIA (porté disparu) — Le nombre de paquets qui sont perdus pour lequel aucune direction ne peut être déterminée.
- Tard — Le nombre de paquets qui sont arrivés après le délai d'attente.

Est la question qui résulte de ces informations ce qui le retard, le jitter, et les valeurs d'erreur sont acceptables dans un réseau VoIP. Malheureusement, il n'y a aucune réponse simple à cette question. Les valeurs acceptables dépendent du type de codecs, de la taille de mémoire tampon de jitter, et d'autres facteurs. En outre, il y a des interdépendances entre ces variables. Une perte de paquets plus élevée peut signifier que moins de jitter peut être toléré.

La meilleure manière d'obtenir les chiffres réalisables de retard et instabilité est de comparer des sites similaires dans le même réseau. Si chacun des 192 Kbps-reliait des sites mais des valeurs d'un jitter d'état autour de 50 ms, et le jitter restant de ms des états 100 de site, alors il y a un problème, indépendamment des valeurs nominales. L'IPM peut fournir la mesure actuelle du retard et instabilité 24x7 pour le tout le réseau, et il peut fournir une spécification de base pour l'utiliser comme benchmark pour des comparaisons de retard et instabilité.

Les erreurs sont des différentes, cependant. En principe, n'importe quel pourcentage d'erreur autre que zéro est une alerte. Les paquets de RTR sont donnés le même traitement de QoS que des paquets vocaux. Si le réseau QoS et le contrôle d'admission d'appel est robuste, aucun niveau d'encombrement ne devrait entraîner la perte de paquets ou le retard excessif pour la Voix ou les paquets de RTR. Par conséquent, vous pouvez s'attendre à ce que les comptes d'erreur IPM soient zéro. Les seules erreurs qui pourraient être considérées « normale » sont des erreurs de contrôle de redondance cyclique (CRC), mais ceux-ci devraient être rares dans une infrastructure de qualité. S'ils sont fréquents, ils constitue un risque à la Qualité vocale.

Informations connexes

- **Lecture recommandée :** Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems