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 de Cisco Service Assurance Agent (SAA) et d'IPM (Internetwork Performance Monitor) pour mesurer la qualité de service (QoS) dans les réseaux VoIP (Voice over IP). Ces informations sont basées sur un projet de téléphonie IP réel. Ce document se concentre sur l'application des produits, et non sur les produits eux-mêmes. Vous devez déjà être familiarisé avec Cisco SAA et IPM et avoir accès à la documentation du produit requise. Voir Informations connexes pour les références à d'autres documents.

Remarque : La fonctionnalité SAA de Cisco dans le logiciel Cisco IOS® était anciennement appelée RTR (Response Time Reporter).

Lorsque vous gérez un réseau VoIP à grande échelle, vous devez disposer des outils nécessaires pour surveiller objectivement la qualité de la voix sur le réseau et établir des rapports à ce sujet. Il n'est pas possible de s'appuyer uniquement sur les commentaires des utilisateurs, car ils sont souvent subjectifs et incomplets. Les problèmes de qualité de la voix proviennent généralement de problèmes de qualité de service du réseau. Ainsi, lorsque vous identifiez des problèmes de qualité vocale, vous avez besoin d'un deuxième outil pour gérer et surveiller la qualité de service du réseau. L'exemple de ce document utilise Cisco SAA et IPM à cette fin.

Cisco Voice Manager (CVM) est utilisé avec Telemate.net pour gérer la qualité vocale. Il indique la qualité vocale des appels via le facteur d'affaiblissement de la planification/calcul (ICPIF) calculé par une passerelle Cisco IOS pour chaque appel. Cela permet au gestionnaire de réseau d'identifier les sites qui souffrent d'une mauvaise qualité vocale. Référez-vous à Gestion de la qualité vocale avec Cisco Voice Manager (CVM) et Telemate pour plus d'informations.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document ne se limite pas à des versions de logiciel ou de matériel spécifiques, mais les exemples de ce document utilisent ces versions de logiciel et de matériel :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problèmes de qualité de service dans un réseau VoIP

Plusieurs facteurs peuvent dégrader la qualité de la voix dans un réseau vocal packagé :

- La perte de paquets
- Délai excessif
- Une gigue excessive

Il est particulièrement important de surveiller ces chiffres de manière continue, si des services à commutation de paquets sont utilisés dans le WAN (par exemple, ATM, Frame Relay ou IP Virtual Private Network). Il existe de nombreux scénarios dans lesquels l'encombrement du réseau de l'opérateur, le formatage du trafic mal configuré sur les périphériques de périphérie ou la régulation mal configurée du côté de l'opérateur peuvent entraîner une perte de paquets ou une mise en mémoire tampon excessive. Lorsque le porteur abandonne 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, tel que Cisco SAA, qui peut injecter du trafic en entrée et valider son arrivée réussie en sortie.

Gestion de la qualité de service avec Cisco SAA et IPM

Il existe trois composants Cisco SAA et IPM :

- Sonde RTR
- Répondeur RTR
- console IPM

La sonde RTR envoie une rafale de paquets au répondeur RTR. Le répondeur RTR les retourne et les renvoie à la sonde. Cette opération simple permet à la sonde de mesurer la perte de paquets et le délai de transmission. Pour mesurer la gigue, la sonde envoie un paquet de contrôle au répondeur avant d'initier la rafale de paquet. Le paquet de contrôle informe le répondeur du nombre de millisecondes (ms) à attendre entre chaque paquet en rafale. Le répondeur mesure ensuite le délai entre les paquets pendant la rafale, et toute déviation par rapport à l'intervalle

prévu est enregistrée comme gigue.

La console IPM contrôle la surveillance QoS. Il programme les sondes RTR avec les informations pertinentes via le protocole SNMP (Simple Network Management Protocol). Il collecte également les résultats via SNMP. Aucune configuration Cisco IOS d'interface de ligne de commande n'est requise sur les sondes RTR.

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

Les sondes et les intervenants RTR doivent exécuter le logiciel Cisco IOS Version 12.0(5)T ou ultérieure. La dernière version de maintenance de 12.1 est recommandée. Les sondes RTR et les intervenants dans les exemples de ce document exécutent la version 12.1(4). La version IPM utilisée est IPM 2.5 pour Windows NT. Un correctif est disponible sur Cisco.com pour cette version. Ce correctif est important, car il corrige un problème dans lequel IPM configure les sondes RTR avec un paramètre de priorité IP incorrect.

Conception

Avant de déployer une solution Cisco SAA et IPM, vous devez effectuer des travaux de conception en tenant compte des considérations suivantes :

- Placement des sondes et des répondeurs RTR
- Type de trafic envoyé de la sonde au répondeur

Il y a un certain nombre de choses à prendre en considération lorsque vous décidez du placement des sondes et des intervenants. Tout d'abord, vous voulez que la mesure QoS couvre chaque site, et pas seulement les sites problématiques. Ceci est dû au fait que les numéros de délai et de gigue signalés par IPM pour un site donné sont plus utiles que les autres sites du même réseau. Ainsi, vous voulez mesurer les sites avec une bonne qualité de service *et une* mauvaise qualité de service. En outre, un site performant peut devenir un site peu performant demain, en raison de changements dans les modèles de trafic ou de changements de réseau. Vous devez le détecter avant qu'il n'affecte la qualité de la voix et soit signalé par les utilisateurs.

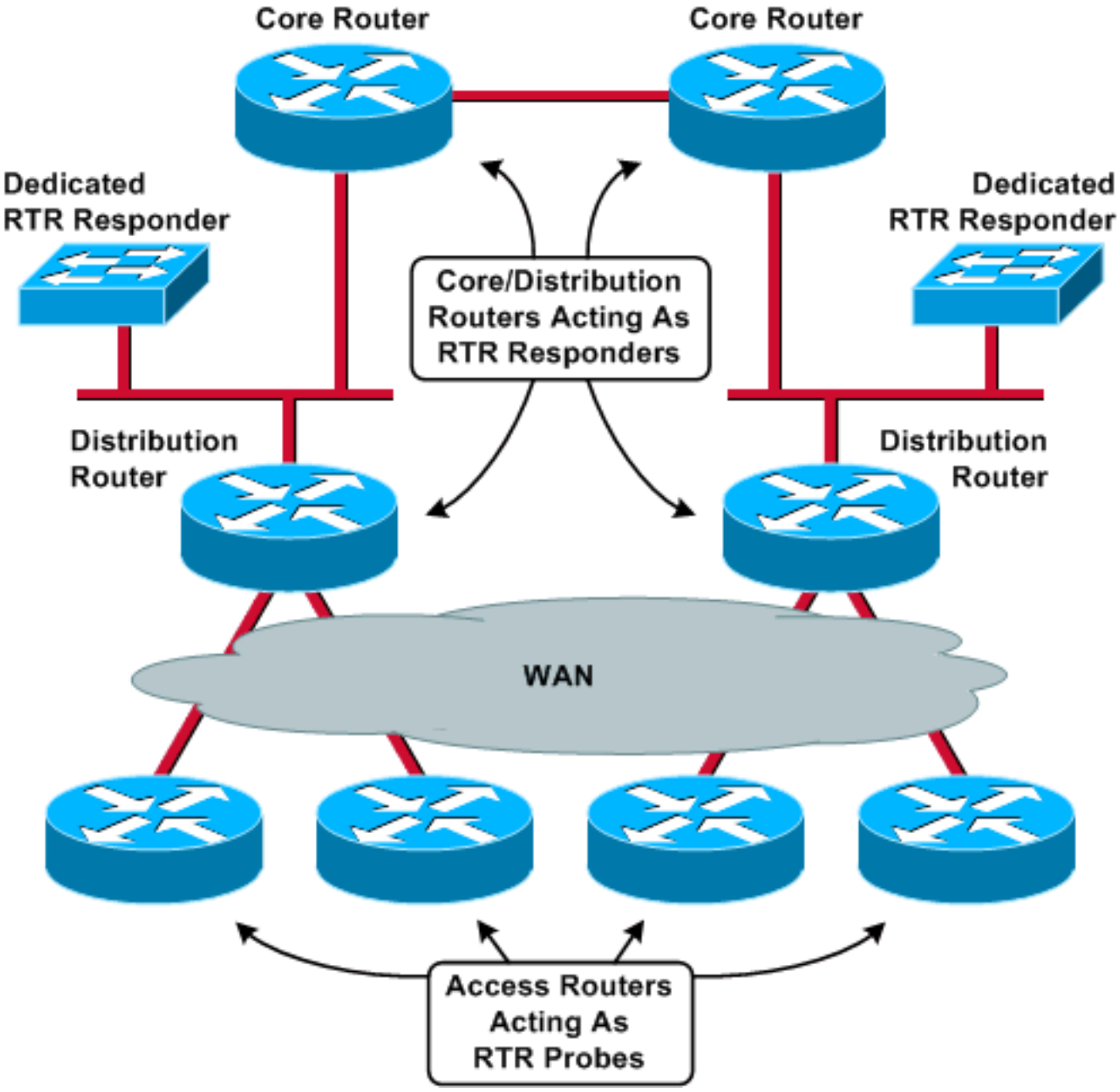
Deuxièmement, l'utilisation du processeur est importante. Un routeur déjà occupé peut ne pas être en mesure de traiter le composant RTR en temps opportun, ce qui peut fausser les résultats. En outre, si vous placez trop d'instances de sonde sur un seul routeur, vous risquez de créer des problèmes d'utilisation élevée du CPU, même s'il n'en existait aucun auparavant. L'approche choisie pour l'exemple de réseau dans ce document (et cela devrait fonctionner dans la plupart des réseaux) consiste à placer les sondes RTR sur les routeurs distants/de filiale. Ces routeurs connectent généralement un seul LAN à un service WAN relativement lent. Par conséquent, les routeurs des filiales ont souvent une utilisation très faible du CPU et peuvent facilement faire face à RTR. L'autre avantage de cette conception est que vous répartissez la charge sur le plus grand nombre possible de routeurs. Gardez à l'esprit qu'il est plus pratique d'être une sonde que d'être un répondeur, car les sondes nécessitent une certaine quantité d'interrogation SNMP.

Avec cette conception, les répondeurs RTR doivent être placés dans le coeur. Les intervenants seront plus occupés que les sondes, car ils répondront à de nombreuses sondes. Ainsi, une conception robuste déploie des routeurs dédiés qui agissent uniquement en tant que répondeurs. La plupart des entreprises ont des routeurs retirés sur le module qui peuvent exécuter cette fonction. Tout routeur doté d'une interface Ethernet suffit. Les routeurs coeur/distribution peuvent également doubler en tant que répondeurs. Le schéma de réseau de cette section décrit les deux scénarios.

Étalez la charge sur le plus grand nombre possible de routeurs et surveillez l'utilisation du processeur RTR à l'aide de 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
```



Lorsque vous comparez des sondes avec des intervenants, il est recommandé de maintenir une topologie cohérente entre la sonde et le répondeur. Par exemple, toutes les sondes et tous les répondeurs doivent être séparés par le même nombre de routeurs, de commutateurs et de liaisons WAN. Ce n'est qu'à cette condition que les résultats IPM peuvent être comparés directement entre les sites.

Dans cet exemple, il existe 200 sites distants et quatre sites principaux/de distribution. Un Catalyst 4500 sur chaque site de distribution agit en tant que répondeur RTR dédié. Chacun des 200 routeurs distants agit comme une sonde RTR. Chaque sonde cible le répondeur situé sur le site de distribution directement connecté.

Les rafales de trafic envoyées par les sondes aux intervenants doivent se voir attribuer les mêmes niveaux de QoS par le réseau que ceux donnés à la voix. Cela peut signifier que vous devez ajuster les configurations de priorité LLQ (Low Latency Queueing) ou RTP (Routing Table Protocol) sur le routeur, de sorte que le trafic des sondes RTR soit soumis à une file d'attente de priorité stricte. Lorsque vous configurez la sonde pour les paquets RTP, seul le port UDP (User Datagram Protocol) de destination peut être contrôlé et non le port source. Une configuration de routeur LLQ type dans cet exemple de réseau comporte des listes d'accès qui classent spécifiquement les paquets RTR dans la même file d'attente que la voix :

```
class-map VoiceRTP
  match access-group name IP-RTP

policy-map 192Kbps_site
  class VoiceRTP
    priority 110

ip access-list extended IP-RTP
  deny   ip any any fragments
  permit udp 10.0.16.0 0.255.239.255
              range 16384 32768 10.0.16.0 0.255.239.255
              range 16384 32768 precedence critical
  permit udp any any eq 20000 precedence critical
  permit udp any eq 20000 any precedence critical
```

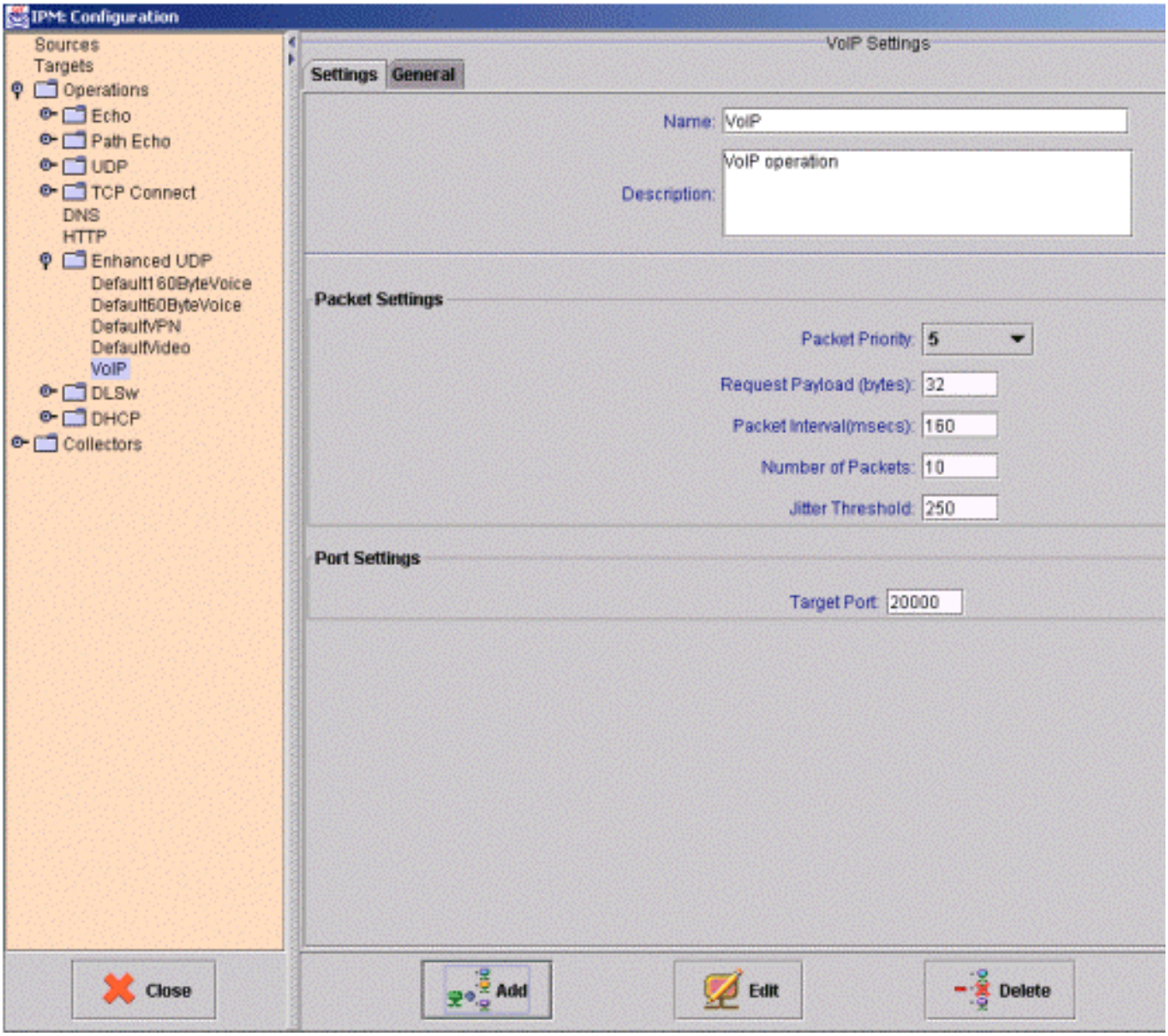
La liste d'accès IP-RTP comporte les lignes de classification suivantes :

- `deny ip any fragments`Refuser tout fragment IP, car une liste d'accès de couche 4 les autorise implicitement.
- `permit udp 10.0.16.0 0,255.239.255 plage 16384 32768 10.0.16.0 0,255.239.255 plage 16384 3276 Priorité critique 8`Autoriser les paquets RTP des sous-réseaux vocaux dont la priorité IP est définie sur 5.
- `permit udp any eq 20000 priority Critical`Autoriser les paquets RTP de la sonde RTR à accéder au répondeur RTR.
- `permit udp any eq 2000 any priority Critical`Autoriser les paquets RTP du répondeur RTR à revenir à la sonde RTR.

Veillez à ce que l'ajout du trafic RTR ne provoque pas la sursouscription des files d'attente LLQ et entraîne l'abandon des paquets voix réels. L'opération IPM **Default60ByteVoice** standard envoie des rafales de paquets RTP avec les paramètres suivants :

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

Cela signifie que, lors d'une rafale, RTR consomme 35,2 Kb de bande passante LLQ. S'il n'y a pas suffisamment de bande passante pour LLQ, créez une nouvelle opération IPM et augmentez l'intervalle de paquets. Avec les paramètres affichés dans cette fenêtre de configuration IPM, une rafale consomme seulement 1 Kbits/s de bande passante :



Résultats

Le tableau de cette section est un exemple de rapport IPM. Ce rapport contient trois instances de sonde RTR. N'oubliez pas qu'une seule sonde physique peut être configurée avec plusieurs instances de sonde RTR qui ciblent différents intervenants 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%

Voici la signification de chacune des colonnes :

Moyenne :

IPM calcule une moyenne pour chaque heure d'échantillonnage. Ces moyennes horaires sont ensuite moyennes sur une période plus longue pour obtenir les moyennes quotidiennes, hebdomadaires ou mensuelles. En d'autres termes, pour le rapport quotidien, IPM calcule la moyenne pour chaque heure des 24 dernières heures. Il calcule ensuite la moyenne quotidienne comme la moyenne de ces 24 moyennes.

Max. moy. :

Cette valeur est la moyenne de tous les maximums horaires pour chaque jour, semaine et mois du graphique. En d'autres termes, pour le rapport quotidien, l'IPM prend le plus grand échantillon signalé au cours de chacune des 24 dernières heures. Il calcule ensuite la moyenne maximale quotidienne comme la moyenne de ces 24 échantillons.

Plus de % :

Pourcentage d'échantillons dépassant le seuil configuré pour le collecteur.

Erreur % :

Pourcentage de paquets ayant rencontré une erreur. Une sonde de gigue signale plusieurs types d'erreurs :

- SD Packet Loss : paquets perdus entre la source et la destination
- Perte de paquets DS : paquets perdus entre la destination et la source
- Busies : nombre d'occasions où une opération RTT n'a pas pu être lancée parce qu'une opération RTT précédente n'avait pas été effectuée
- Séquence : nombre de terminaisons de l'opération RTT reçues avec un identificateur de séquence inattendu. Voici quelques raisons possibles de cette situation :Un paquet dupliqué a

été reçu.Une réponse a été reçue après le délai d'attente.Un paquet endommagé a été reçu et n'a pas été détecté.
- Drops : nombre d'occurrences de l'un ou l'autre de ces événements :Une opération RTT n'a pas pu être lancée car certaines ressources internes nécessaires n'étaient pas disponibles (par exemple, mémoire ou sous-système SNA)Impossible de reconnaître l'achèvement de l'opération.
- MIA (Missing in Action) : nombre de paquets perdus pour lesquels aucune direction ne peut être déterminée.
- Late : nombre de paquets arrivés après le délai d'attente.

La question qui se pose à partir de ces informations est de savoir quelles valeurs de délai, de gigue et d'erreur sont acceptables dans un réseau VoIP. Malheureusement, il n'y a pas de réponse simple à cette question. Les valeurs acceptables dépendent du type de codec, de la taille du tampon d'instabilité et d'autres facteurs. En outre, il existe des interdépendances entre ces variables. Une perte de paquets plus élevée peut signifier que moins de gigue peut être tolérée.

Le meilleur moyen d'obtenir des données de délai et de gigue réalisables est de comparer des sites similaires sur le même réseau. Si tous les sites rattachés à 192 Kbits/s, mais qu'un seul indique des valeurs de gigue d'environ 50 ms, et que le site restant signale une gigue de 100 ms, alors il y a un problème, indépendamment des valeurs nominales. L'IPM peut fournir une mesure continue du délai et de la gigue 24 h/24 et 7 j/7 pour l'ensemble du réseau, et il peut fournir une ligne de base à utiliser comme référence pour les comparaisons de délai et de gigue.

Les erreurs sont cependant différentes. En principe, tout pourcentage d'erreur autre que zéro est un indicateur rouge. Les paquets RTR reçoivent le même traitement QoS que les paquets voix. Si la QoS du réseau et le contrôle d'admission des appels sont robustes, aucun niveau de congestion ne doit entraîner de perte de paquets ou de retard excessif pour les paquets voix ou RTR. Par conséquent, vous pouvez vous attendre à ce que le nombre d'erreurs IPM soit égal à zéro. Les seules erreurs pouvant être considérées “ ” normales sont les erreurs CRC (Cycles Redundancy Check), mais elles doivent être rares dans une infrastructure de qualité. S'ils sont fréquents, ils constituent un risque pour la qualité de la voix.

Informations connexes

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