Gebruik van Cisco Service Assurance Agent en Internetwork Performance Monitor om Quality-of-Service in Voice-over-IP netwerken te beheren

Inhoud

Inleiding

Dit document beschrijft het gebruik van Cisco Service Assurance Agent (SAA) en Internetwork Performance Monitor (IPM) om de kwaliteit van de service (QoS) in Voice-over-IP-netwerken (VoIP) te meten. Deze informatie is gebaseerd op een project van IP-telefonie in de echte wereld. Dit document is gericht op de toepassing van de producten en niet op de producten zelf. U dient al bekend te zijn met Cisco ASA en IPM en toegang te hebben tot de vereiste productdocumentatie. Zie Verwante informatie voor verwijzingen naar andere documentatie.

Opmerking: De Cisco SAA-functionaliteit in Cisco IOS®-software werd voorheen bekend als Response Time Reporter (RTR).

Wanneer u een grootschalig VoIP-netwerk beheert, moet u de benodigde gereedschappen hebben om de spraakkwaliteit in het netwerk objectief te bewaken en te rapporteren. Het is niet mogelijk om alleen op feedback van gebruikers te vertrouwen, omdat deze vaak subjectief en onvolledig is. Spraakkwaliteitsproblemen zijn doorgaans het gevolg van QoS-problemen in het netwerk. Dus, wanneer je spraakkwaliteitsproblemen identificeert, heb je een tweede gereedschap nodig om het netwerk QoS te beheren en te bewaken. Het voorbeeld in dit document gebruikt Cisco SAA en IPM voor dit doel.

Cisco Voice Manager (CVM) wordt gebruikt met Telemate.net om spraakkwaliteit te beheren. Het rapporteert over de spraakkwaliteit van oproepen via de Impament/Calculated Planning Impament Factor (ICPIF) die door een Cisco IOS gateway voor elke vraag wordt berekend. Dit stelt de netwerkbeheerder in staat om plaatsen te identificeren die aan slechte stemkwaliteit lijden. Raadpleeg Spraakkwaliteit beheren met Cisco Voice Manager (CVM) en Telemate voor meer informatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- of hardwareversies, maar de voorbeelden in dit document maken gebruik van deze software- en hardwareversies:

- Cisco IOS-softwarerelease 12.1(4)E
- IPM 2.5 voor Windows NT
- Catalyst 4500 Series switch

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

QoS-problemen in een VoIP-netwerk

Verschillende factoren kunnen spraakkwaliteit in een gepacketiiseerd spraaknetwerk aantasten:

- Verlies van pakketten
- Overmatige vertraging
- buitensporig bezwaar

Het is in het bijzonder belangrijk dat u deze cijfers constant controleert, als de pakketgeschakelde services in WAN worden gebruikt (bijvoorbeeld ATM, Frame Relay of IP Virtual Private Network). Er zijn talloze scenario's waarbij stremming in het dragernetwerk, verkeerd geconfigureerd traffic shaping op de rand-apparaten of slecht ingesteld toezicht aan de kant van de drager pakketverlies of buitensporige buffers kan veroorzaken. Wanneer de vervoerder pakketten laat vallen is er geen duidelijk bewijs op de randapparaten. Daarom hebt u een end-to-end gereedschap nodig zoals de SAA van Cisco die verkeer op de ingang kan injecteren en zijn succesvolle aankomst bij stress valideren.

QoS beheren met Cisco ASA en IPM

Er zijn drie SAA- en IPM-onderdelen van Cisco:

- RTR-test
- RTR-responder
- IPM-console

De RTR-test stuurt een aantal pakketten naar de RTR-responder. De RTR-responder draait ze om en stuurt ze terug naar de sonde. Met deze eenvoudige handeling kan de sonde pakketverlies en retourvertraging meten. Om de jitter te meten, stuurt de sonde een controlepakket naar de responder voordat de pakketbreuk wordt gestart. Het controlepakket informeert de responder hoeveel milliseconden (ms) tussen elk pakket in de burst moeten verwachten. De responder meet vervolgens de interpakketvertraging tijdens de breuk en elke afwijking van het verwachte interval

wordt geregistreerd als jitter.

De IPM-console controleert de QoS-bewaking. Het programmeert de RTR-tests met de relevante informatie via Simple Network Management Protocol (SNMP). De resultaten worden ook via SNMP verzameld. Op de RTR-problemen is geen interface-Cisco IOS-configuratie vereist.

Geef de opdracht **rtr** mondiale configuratie uit om de RTR-responders handmatig te configureren.

Bij de RTR-problemen en -responders moet Cisco IOS-softwarerelease 12.0(5)T of hoger worden uitgevoerd. De meest recente onderhoudsrelease van 12.1 mainstream wordt aanbevolen. De RTR-sondes en de respondenten in de voorbeelden in dit document hebben release 12.1(4) uitgevoerd. De IPM-versie in gebruik is IPM 2.5 voor Windows NT. Er is een pleister beschikbaar op Cisco.com voor deze versie. Dit lapje is belangrijk, omdat het een probleem vastlegt waar IPM de RTR spelden met een incorrecte instelling voor de IP voorrang vormt.

Ontwerpen

Voordat u een Cisco SAA- en IPM-oplossing implementeert, moet u één of ander ontwerpwerk met deze overwegingen in gedachten uitvoeren:

- Plaatsing van RTR-sondes en -responders
- Verkeerstype dat van sonde naar responder wordt verzonden

Er zijn een aantal zaken die in aanmerking moeten worden genomen wanneer je besluit over de plaatsing van sondes en responders. In de eerste plaats wil je dat de QoS-meting op elke site van toepassing is, en niet alleen op probleemsites. Dit komt doordat de vertragings- en jitternummers die IPM-rapporten voor een bepaalde site indienen, het meest bruikbaar zijn in vergelijking met andere sites in hetzelfde netwerk. Dus wilt u sites meten met goede QoS *en* slechte QoS. Een goed presterende site kan morgen ook een slecht presterende site worden, als gevolg van veranderingen in verkeerspatronen of netwerkwijzigingen. U wilt dit detecteren voordat de spraakkwaliteit wordt beïnvloed en het wordt door de gebruikers gerapporteerd.

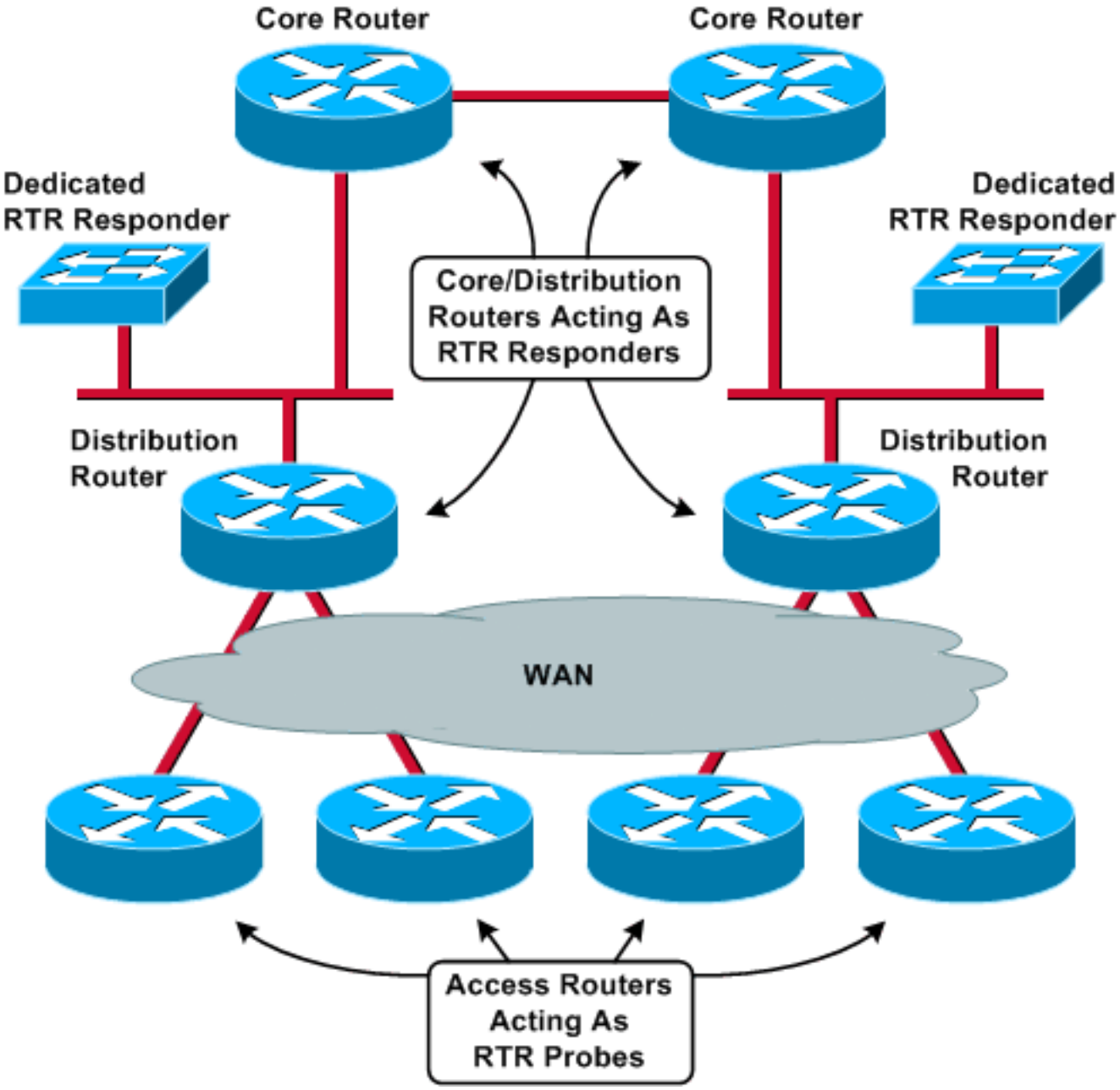
Ten tweede is het gebruik van CPU's belangrijk. Een reeds drukke router kan de component RTR niet tijdig kunnen onderhouden en dit kan de resultaten scheeftrekken. Als u ook te veel peilingen op één enkele router plaatst, kunt u problemen met een hoog CPU-gebruik creëren, ook al bestonden er voordien geen. De benadering die voor het voorbeeldnetwerk in dit document is gekozen (en dit zou in de meeste netwerken moeten werken) is om de RTRsondes op de ver/tak routers te plaatsen. Deze routers verbinden doorgaans één LAN met een relatief trage WAN-service. Daarom hebben filiaalrouters vaak een zeer laag CPU-gebruik en kunnen zij eenvoudig met RTR omgaan. Het andere voordeel van dit ontwerp is dat je de lading over zoveel mogelijk routers distribueert. Houd in gedachten dat het meer werk is om een sonde te zijn dan om een responder te zijn, omdat sondes een bepaalde hoeveelheid SNMP-stemmen kosten.

Bij dit ontwerp moeten de RTR-responders in de kern worden geplaatst. De responders zullen sterker zijn dan de sondes, omdat ze op veel problemen zullen reageren. Hierdoor implementeert een robuust ontwerp speciale routers die alleen fungeren als responders. De meeste organisaties hebben gepensioneerde routers op de plank die deze functie kunnen uitvoeren. Elke router met een Ethernet-interface is voldoende. In plaats hiervan kunnen de kern-/distributirouters ook verdubbelen als responders. In het netwerkdiagram in deze sectie worden beide scenario's weergegeven.

Verspreid de lading over zoveel mogelijk routers en controleer het gebruik van RTR CPU met deze opdracht:

```
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
```



Wanneer u sondes met responders vergelijkt, wordt het aanbevolen om een consistente topologie tussen sonde en responder te handhaven. Bijvoorbeeld, alle speldenprikken en hulpverleners zouden door het zelfde aantal routers, switches, en WAN links moeten worden gescheiden. Alleen dan kunnen de IPM-resultaten rechtstreeks tussen de sites worden vergeleken.

In dit voorbeeld zijn er 200 afgelegen locaties en vier kern-/distributielocaties. Een Catalyst 4500 op elke distributieplaats fungeert als een speciale RTR-responder. Elk van de 200 externe routers werkt als een RTR-test. Elke sonde richt zich op de responder die zich op de direct aangesloten distributieplaats bevindt.

De uitbarstingen van verkeer die door de sondes naar de responders worden gestuurd moeten door het netwerk dezelfde QoS-niveaus krijgen als de stem wordt gegeven. Dit kan betekenen dat u de lage wachtrijen (LLQ) of de prioriteitsconfiguraties van het Routing Table Protocol (RTP) aan de router moet aanpassen, zodat het verkeer vanaf de RTR-problemen onderworpen is aan strikte

prioriteitswachtrij. Wanneer u de sonde voor RTP-pakketten configureren kan alleen de doelpoort met User Datagram Protocol (UDP) worden bestuurd en niet de bronpoort. Een typische LLQ-routerconfiguratie in dit voorbeeldnetwerk heeft toegangslijsten die specifiek de RTR-pakketten in dezelfde wachtrij als spraak classificeren:

```
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
```

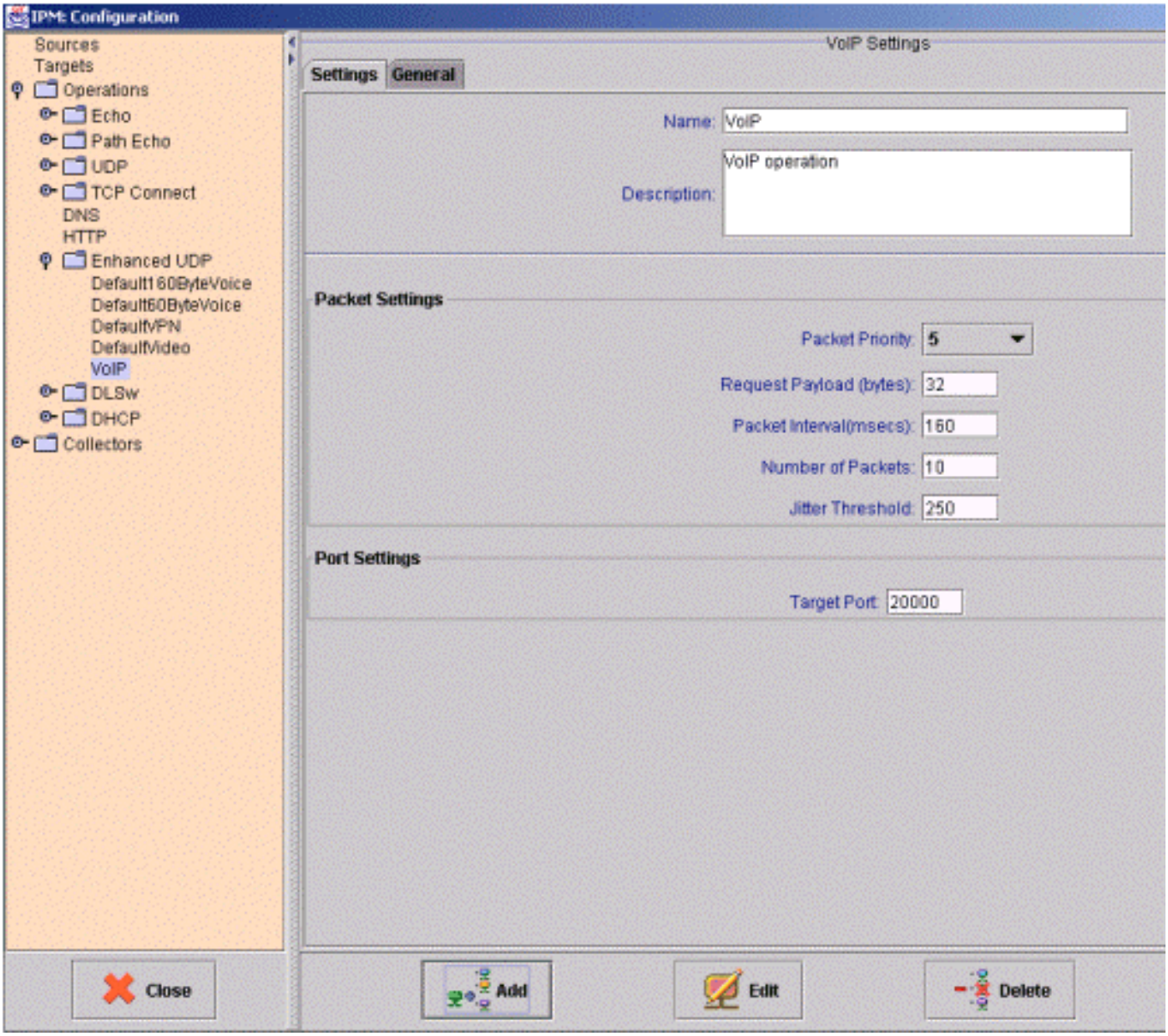
De IP-RTP toegangslijst heeft deze classificerende lijnen:

- `eventuele fragmenten te ontkennen`Ontken een IP-fragment, omdat een Layer 4-toegangslijst dit impliciet toestaat.
- `toegelaten udp 10.0.16.0 0.255.239.255 bereik 16384 32768 10.0.16.0 0.255.239.255 bereik 16384 327 prioriteit`Toon RTP pakketten van stemsubnetten met IP voorrang aan 5.
- `het udp toestaan om alle belangrijke gebeurtenissen van 2000 te toetsen`Geef RTP-pakketten van RTR-test op naar RTR-responder.
- `in 2000 elk nieuw prioriteitsgebied`Geef RTP-pakketten van RTR-responder toestemming om terug te gaan naar RTR-test.

Let op dat het toevoegen van RTR-verkeer er niet voor zorgt dat de LLQ-wachtrijen te vol geabonneerd zijn en dat er echte spraakpakketten worden gedropt. De standaard Default**60ByteVoice** IPM-handeling verstopt fragmenten van RTP-pakketten met deze parameters:

- payload-aanvraag: 60 bytes**Opmerking:** Dit is de RTP-header en -stem. Voeg 28 bytes (IP/UDP) toe om de L3 datagramgrootte te krijgen.
- Intervaal: 20 ms
- Aantal pakketten: 10

Dit betekent dat, tijdens een breuk, RTR 35,2 Kb van de bandbreedte van LLQ verbruikt. Als er niet voldoende bandbreedte voor LLQ is, kunt u een nieuwe IPM-handeling maken en het pakketinterval verhogen. Met de parameters die in dit IPM configuratievenster worden getoond, neemt een burst slechts 1 Kbps van bandbreedte in beslag:



Resultaten

De tabel in deze paragraaf is een voorbeeld van een IPM-rapport. Dit rapport bevat drie RTR-proefinstellingen. Houd in gedachten dat één fysieke test kan worden geconfigureerd met meerdere RTR-tests die op verschillende responders zijn gericht of die verschillende payload-combinaties gebruiken.

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%

Dit zijn de betekenissen van elk van de kolommen:

Avg:

De IPM berekent een gemiddelde voor elk uur van bemonstering. Deze uurgemiddelden worden vervolgens over een langere periode gemiddeld om de dagelijkse, week- of maandgemiddelden te verkrijgen. Met andere woorden, voor het dagelijkse rapport berekent IPM het gemiddelde voor elk uur van de afgelopen 24 uur. Vervolgens berekent het het daggemiddelde als het gemiddelde van deze 24 gemiddelden.

Avg Max:

Deze waarde is het gemiddelde van alle uurmaximum voor elke dag, week en maand in de grafiek. Met andere woorden, voor het dagverslag neemt IPM de grootste steekproef die in elk van de afgelopen 24 uur is gerapporteerd. Vervolgens wordt het dagelijkse maximale gemiddelde berekend als het gemiddelde van deze 24 monsters.

Meer dan 1 %:

Dit is het percentage monsters dat boven de ingestelde drempel voor de verzamelaar lag.

Fout %:

Dit is het percentage pakketten dat een fout tegenkwam. Een jitter-toets rapporteert verschillende soorten fouten:

- SD Packet Loss—Packet dat tussen bron en bestemming verloren is
- DS Packet Loss-Packet dat tussen bestemming en bron is verloren
- Buis—het aantal keren dat een RTT-operatie (round-trip time) niet kon worden gestart omdat een eerdere RTT-operatie niet was voltooid
- Volgorde—het aantal RTT - transacties dat wordt ontvangen met een onverwachte sequentidentificatiecode. Dit zijn een paar mogelijke redenen waarom dit zou kunnen

gebeuren:Er is een dubbele verpakking ontvangen.Er werd een antwoord ontvangen nadat de termijn was verstreken.Een beschadigd pakje is ontvangen en is niet gedetecteerd.
- Drops - het aantal keren dat een van deze gevallen zich voordeed:Een RTT-werking kon niet worden gestart omdat een aantal benodigde interne middelen niet beschikbaar was (bijvoorbeeld geheugen of het subsysteem Systems Network Architecture [SNA])Voltooiing van bewerking kon niet worden herkend.
- MIA (Ontbrekend in Actie) - het aantal pakketten dat verloren wordt waarvoor geen richting kan worden bepaald.
- Te laat-het aantal pakketten dat na de time-out is aangekomen.

De vraag die uit deze informatie voortvloeit is welke vertraging, jitter en foutwaarden aanvaardbaar zijn in een VoIP-netwerk. Helaas is er geen eenvoudig antwoord op deze vraag. Aanvaardbare waarden hangen af van het codepatype, de grootte van de jitter-buffer en andere factoren. Daarnaast zijn er onderlinge afhankelijkheden tussen deze variabelen. Een hoger pakketverlies kan betekenen dat minder jitter wordt getolereerd.

De beste manier om werkbare vertraging en Jitter figures te verkrijgen is gelijksoortige plaatsen in hetzelfde netwerk te vergelijken. Als alle 192 Kbps aangesloten sites maar één rapport ongeveer 50 ms hoger zijn en de resterende site 100 ms jitter meldt, is er een probleem, ongeacht de nominale waarden. IPM kan een doorlopende 24x7-vertraging en jittermeting voor het gehele netwerk bieden, en kan een basislijn bieden om te gebruiken als benchmark voor vertraging en jittervergelijkingen.

Er zijn echter andere fouten. In principe is elk foutenpercentage anders dan nul een rode vlag. De RTR-pakketten krijgen dezelfde QoS-behandeling als spraakpakketten. Als het netwerk QoS en de Call Admission Control robuust is, zou geen congestieniveau pakketverlies of buitensporige vertraging voor spraak- of RTR-pakketten kunnen veroorzaken. Daarom kunt u verwachten dat de IPM fouttellingen nul zijn. De enige fouten die als "normaal" kunnen worden beschouwd, zijn CRC-fouten (Cyclic Redundancy Control), maar deze fouten moeten zeldzaam zijn in een kwaliteitsinfrastructuur. Als ze frequent zijn, vormen ze een risico voor de spraakkwaliteit.

Gerelateerde informatie

- **Aanbevolen lezen:** Probleemoplossing voor Cisco IP-telefonie
- Technische ondersteuning en documentatie – Cisco Systems