تنفيذ جودة الخدمة

المحتويات

المقدمة
ما هي التطبيقات التي تحتاج إلى جودة الخدمة؟
فهم خصائص التطبيقات
معرفة مخطط الشبكة
ربط أحجام رأس طبقة
إنشاء فئات بناء على المعايير
إنشاء نهج لوضع علامة على كل فئة
العمل من الحافة إلى اللب
إنشاء سياسة لمعالجة حركة المرور
تطبيق السياسة
إستخدام مدير سياسة جودة الخدمة (QPM) لمراقبة تأثيرات السياسة
توصيات جودة الخدمة (QoS) للأغراض العامة
معلومات ذات صلة

المقدمة

يقدم هذا المستند بعض الإرشادات عالية المستوى لتنفيذ جودة الخدمة (QoS) في شبكة تعمل كنقل للتطبيقات المتعددة، بما في ذلك التطبيقات الحساسة للتأخير والتي تتطلب عرض نطاق ترددي كبير. قد تعزز هذه التطبيقات العمليات التجارية، ولكنها تعمل على زيادة موارد الشبكة. يمكن أن توفر جودة الخدمة خدمات آمنة ويمكن التنبؤ بها وقابلة للقياس ومضمونة لهذه التطبيقات من خلال إدارة التأخير وتباين التأخير (التشوه) وعرض النطاق الترددي وفقد الحزمة في الشبكة.

ما هي التطبيقات التي تحتاج إلى جودة الخدمة؟

أولا، حدد التطبيقات التي تعتبر حيوية للأعمال والتي تتطلب الحماية. قد يتعين عليك مراجعة جميع التطبيقات المتنافسة على موارد الشبكة. إذا كان هذا هو الحال، فاستخدم محاسبة NetFlow، أو التعرف على التطبيق المستند إلى الشبكة (NBAR)، أو مدير أجهزة جودة الخدمة (QDM) لتحليل أنماط حركة مرور البيانات في الشبكة.

توفر محاسبة NetFlow تفاصيل حول حركة مرور الشبكة ويمكن إستخدامها لالتقاط تصنيف حركة المرور أو أسبقية الحركة مرور البيانات المقترنة بكل تدفق.

NBAR هو أداة تصنيف يمكن أن تعرف حركة المرور حتى طبقة التطبيق. وهو يوفر إحصائيات لكل واجهة وكل بروتوكول وثنائية الإتجاه لكل تدفق حركة مرور يمر عبر واجهة. كما تقوم NBAR بتصنيف المنفذ الفرعي؛ والبحث والتعريف خارج منافذ التطبيق.

QDM هو تطبيق إدارة شبكة قائم على الويب يوفر واجهة مستخدم رسومية سهلة الاستخدام لتكوين وظائف جودة الخدمة المتقدمة المستندة إلى IP ومراقبتها في الموجهات.

فهم خصائص التطبيقات

من المهم فهم خصائص التطبيقات التي تحتاج إلى الحماية. تميل بعض التطبيقات إلى أن تكون حساسة لزمن الوصول أو فقدان الحزمة، في حين تعتبر تطبيقات أخرى "عدوانية" لأنها ثقيلة أو تستهلك الكثير من عرض النطاق. إذا كان التطبيق مدفوعا، حدد ما إذا كان هناك انفجار مستمر أو انفجار صغير. هل حجم الحزمة للتطبيق كبير أو صغير؟ هل التطبيق يستند إلى TCP أو UDP؟

ميزة	توجيهية
تطبيق حساس للتأخير أو الفقد. (الصوت والفيديو في الوقت الحقيقي)	لا تستخدم الكشف المبكر العشوائي المرجح (WRED)، أو تنظيم حركة المرور، أو التجزئة (FRF-12)، أو وضع السياسات. بالنسبة لهذا النوع من حركة المرور، يجب تنفيذ قوائم انتظار تقليل التأخير (LLQ) واستخدام قائمة انتظار الأولوية لحركة المرور الحساسة للتأخير.
التطبيق الذي يتم تحميله باستمرار أو يعد خللا في عرض النطاق الترددي. (FTP و HTTP)	أستخدم WRED أو تنظيم حركة مرور البيانات أو قوائم الانتظار العادلة والمقدرة المعتمدة على الفئة (CBWFQ) لضمان النطاق الترددي.
تطبيق يستند إلى TCP.	أستخدم WRED نظرا لأن الحزم المفقودة تتسبب في تراجع TCP ثم قم

	بالتجميع مرة أخرى باستخدام خوارزمية البدء البطيء. إذا كانت حركة المرور تستند إلى UDP ولا تغير سلوكها عند إسقاط الحزم، فلا تستخدم WRED. أستخدم التنظيم إذا كنت بحاجة إلى تحديد المعدل للتطبيق، وإلا فقط أترك الحزم تقع من بعد.

معرفة مخطط الشبكة

قد تحتاج بعض الأجهزة إلى ترقية IOS للاستفادة من ميزات جودة الخدمة التي تريد تنفيذها. تساعدك مخططات مخطط الشبكة وتكوينات الموجه وإصدار البرامج على كل جهاز على تقدير عدد الأجهزة التي تتطلب ترقية IOS. ارجع إلى مكتبة الأيقونات من Cisco للحصول على الأيقونات التي يمكن أن تساعدك على إنشاء مخططات الشبكة.

- قم بتقييم إستخدام وحدة المعالجة المركزية (CPU) على كل موجه أثناء فترات الانشغال للمساعدة في تحديد كيفية توزيع ميزات جودة الخدمة بين الأجهزة لمشاركة الحمل.
- تصنيف أنواع حركة مرور بيانات الأعمال الحرجة والواجهات التي ستعبر بها حركة المرور هذه. حدد المجموعات أو الفئات ذات الأولوية التي سيتم إنشاؤها لتحقيق أهداف جودة الخدمة لشبكتك.
- حدد الحد الأقصى للتأخير الذي يمكن للتطبيقات الهامة أن تتعامل معه وتضبط معلمات الاندفاع داخل مكيفات حركة المرور (مظلات حركة المرور أو المنظومات) لاستيعاب هذا التأخير.
- تعرف على المعدلات المعتمدة على كل واجهة: الكمبيوترات المتعددة (PVCs) أو الواجهات الفرعية وقم بتكوين النطاق الترددي ليتطابق.
- حدد الارتباطات البطيئة للمساعدة في تحديد مكان الاختناقات في الشبكة وحدد كيفية تطبيق آليات كفاءة الارتباط على الواجهات المناسبة.
- قم بحساب التكاليف الإضافية من الطبقة 2 والطبقة 3 لكل نوع من أنواع الوسائط التي ستقوم بنقل حركة مرور البيانات الحيوية للشركات. سيساعد ذلك في حساب المقدار الصحيح من عرض النطاق الترددي المطلوب لكل فئة.
- وثمة معلومة رئيسية أخرى هي ما إذا كنت تريد حماية حركة المرور استنادا إلى التطبيق أو مصدر IP أو الوجهة أو كليهما.

ربط أحجام رأس طبقة

نوع الوسائط	ربط رأس طبقة
Ethernet	14 بايت

PPP	6 بايت
ترحيل الإطارات Frame Relay	4 بايت
ATM	5 بايت/خلية

إنشاء فئات بناء على المعايير

بمجرد تحديد التطبيقات التي تحتاج إلى جودة الخدمة ومعايير التصنيف لاستخدامها (استنادا إلى خصائص التطبيقات)، تكون مستعدا لإنشاء فئات استنادا إلى هذه المعلومات.

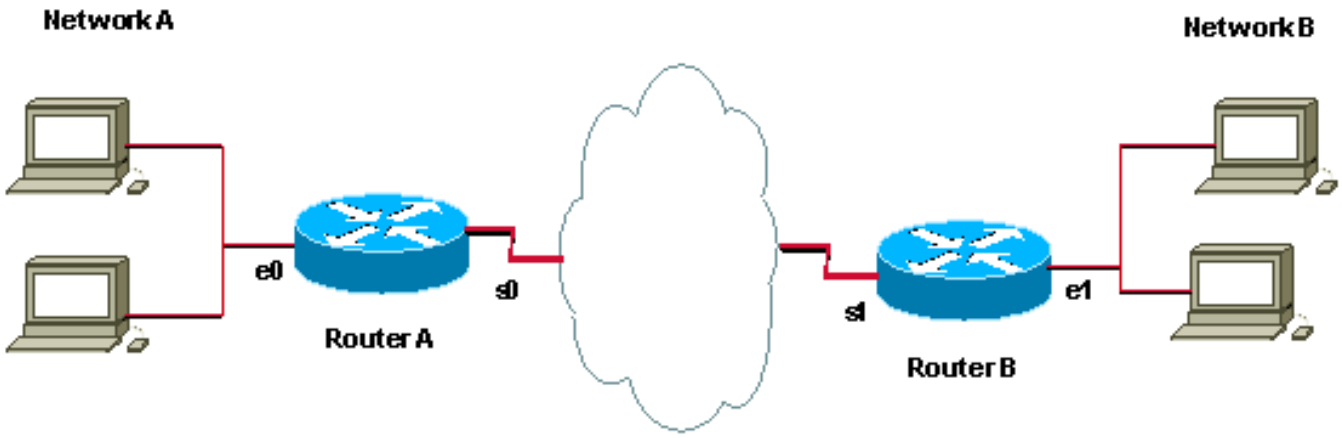
إنشاء نهج لوضع علامة على كل فئة

قم بإنشاء سياسة لوضع علامة على كل فئة من فئات حركة المرور بقيم الأولوية المناسبة (أستخدم نقطة تحكم الخدمات المميزة (DSCP) أو أسبقية IP). سيتم وضع علامة على حركة المرور عند دخولها إلى الموجه على واجهة الدخول. سيتم إستخدام العلامات لمعالجة حركة المرور حيث إنها تترك الموجه على واجهة الخروج.

العمل من الحافة إلى اللب

العمل من الموجه الأقرب لحركة المرور تجاه المركز. قم بتطبيق علامتك على واجهة الدخول للموجه. في المخطط أدناه، يكون الموجه A هو المكان الواضح لوضع علامة على حركة المرور وتطبيق السياسة للبيانات المستمدة من الشبكة A والموجهة للموجه B. سيتم وضع علامة على حركة المرور عند دخولها إلى واجهة Ethernet0 للموجه A، وسيتم تطبيق سياسة جودة الخدمة على واجهة Serial0 للموجه A عند خروجها من الموجه. إذا كان يجب تطبيق السياسة نفسها في كلا الاتجاهين (بحيث تتلقى حركة المرور التي يتم الحصول عليها من الشبكة B والموجهة للشبكة A نفس المعالجة)، فيجب وضع علامة على حركة المرور الواردة من الشبكة B عند دخولها إلى واجهة إيثرنت الخاصة بالموجه B1 ومعالجتها كما تقوم بترك الموجه على الواجهة Serial1.

بمجرد تمييز حركة المرور على واجهة الدخول على موجه واحد، فإنها تحافظ على نفس العلامات كما هي تجتاز نقلات متعددة (ما لم يتم إعادة تمييزها). عادة، يجب وضع علامة على حركة المرور مرة واحدة فقط. يمكن تطبيق سياسات جودة الخدمة على نقلات إضافية استنادا إلى هذه العلامات. يجب عليك فقط إعادة وضع علامة في حالة وصول حركة المرور من مجال غير موثوق به.



إنشاء سياسة لمعالجة حركة المرور

الآن بعد أن قمت بتمييز حركة المرور، يمكنك إستخدام العلامات لإنشاء سياسة والقيام بتصنيف حركة المرور على بقية أجزاء الشبكة. نوصي بإبقاء السياسة بسيطة باستخدام ما لا يزيد عن أربعة فئات.

إن أمكن، قم بتطبيق جودة الخدمة واختباره في بيئة معملية. قم بنشرها في الشبكة المباشرة بعد أن تكون راضيا عن النتائج.

تطبيق السياسة

تطبيق النهج في الإتجاه المناسب. قرر ما إذا كان يجب تطبيق السياسة في إتجاه واحد أو في كلا الاتجاهين. قم دائما بوضع علامة على حركة مرور البيانات ومعالجتها بالقرب من المصدر قدر الإمكان، كما هو موضح في إنشاء سياسة لوضع علامة على كل قسم فئة في هذا المستند.

نوصي بتطبيق السياسة نفسها في كلا الاتجاهين لتصفية حركة المرور الواردة من كل من جانبي الموقع والموجهة إليه. هذا يعني أنه يجب عليك تطبيق نفس النهج الصادر على الواجهة التسلسلية للموجه A والواجهة التسلسلية للموجه B.

إستخدام مدير سياسة جودة الخدمة (QPM) لمراقبة تأثيرات السياسة

أستخدم QPM كنظام كامل للتحكم المركزي في السياسات ونشر السياسات المؤتمتة والموثوقة.

توصيات جودة الخدمة (QoS) للأغراض العامة

فيما يلي قائمة بفئات جودة الخدمة وبعض ميزات جودة الخدمة الأكثر إستخداما المرتبطة بكل فئة.

الفئة	**مميزات جودة الخدمة المرتبطة**
نموذج خدمة جودة الخدمة	جودة الخدمة (DiffServ) المزودة عند الإمكان أو المشار إليها (RSVP) عند الضرورة.
التصنيف/الوسم	نقاط رمز DiffServ أو معرف مجموعة جودة الخدمة.
إدارة الازدحام	LLQ أو CBWFQ.
تجنب الازدحام	WRED متوافق مع DiffServ.
كفاءة الارتباط	MLPPP و LFI و FRF.11 و FRF.12 و CRTP
إرسال الإشارات	RSVP، QPPB

مكيفات حركة المرور/وضع السياسات	واضع السياسات المستند إلى الفئة وتنظيم حركة البيانات العامة (GTS) أو تنظيم حركة بيانات ترحيل الإطارات (FRTS).
التكوين/المراقبة	واجهة سطر الأوامر (CLI) لجودة الخدمة (QPM)، QDM المعيارية

معلومات ذات صلة

- صفحة دعم جودة الخدمة
- صفحة دعم بروتوكولات IP المُوجّهة
- صفحة دعم توجيه IP
- صفحة دعم IS-IS
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).