www.prozhe.com

بسم الله الرحمن الرحيم

www.prozhe.com

www.prozhe.com

دانشگاه آزاد اسلامی واحد هرسین

عنوان :

شبکه خصوصی مجازی VPN

استاد راهنما :

سرکار خانم مهندس سارا خسروی

تهیه کننده :

حسن صفری مفرد

شماره دانشجویی :

۸۹۱۰۲۱۸۱

بهار ۹۱

www.prozhe.com

www.prozhe.com

تقدیر و تشکر :

« من علمنی حرفاً فقد صرنی عبداً »

هر کس یک حرف به من بیاموزد مرا بنده خود ساخته است.

امام علی (ع)

با سلام و درود به مشعل داران علم و آگاهی و نجات دهنده انسانها از گمراهی و ضلالت و راهنمای طالبان علم و حقیقت به سوی دستیابی و کسب معرفت.

در این مقاله از زحمات استاد گرانقدرم «سرکار خانم مهندس سارا خسروی» که اینجانب را در انجام این تکلیف یاری و راهنمایی نموده اند خالصانه تقدیر و تشکر می نمایم و همچنین از زحمات کلیه کسانیکه مرا در انجام این پروژه همراهی نموده اند کمال تشکر و قدردانی را دارم.

www.prozhe.com

www.prozhe.com

تقدیم به:

استاد ارجمند سرکار خانم مهندس سارا خسروی

به پاس آفرینش و راهبری اندیشه های زیبا ، در پهنه آسمان علم و شکیبایی

و به پاس هر آنچه که خالصانه و صبورانه به من آموختید

تا بیاموزم که در راه شناخت علم ، چگونه رهرو باشم .

www.prozhe.com

www.prozhe.com

فهرست مطالب

چکیده	۱
فصل اول	۲
۱-شبکه های خصوصی مجازی	۳
۱-۱ عناصر تشکیل دهنده یک VPN	۴
۱-۳ شبکه های LAN جزایر اطلاعاتی	۵
۱-۴ امنیت VPN	۷
۱-۵ تکنولوژی های VPN	۹
فصل دوم	۱۳
۲-مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش نخست)	۱۴
چکیده	۱۴
۲-۱ . مقدمه	۱۵
۲-۲ . IPVPN چیست؟	۱۶
۲-۳ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش دوم)	۱۸
۲-۳-۱ نیازمندیهای مدیریتی IPVPN – از دیدگاه service provider	۱۸
۲-۳-۲ مدیریت پیکربندی برای VPNهای مبتنی بر شبکه(طرف provider)	۱۹
۲-۳-۳ مدیریت پیکربندی برای VPN های بر مبنای CE	۲۰
۲-۴ مانیتور کردن کارایی	۲۱

www.prozhe.com

www.prozhe.com

۲-۵ Qos در IPVPN ها ۲۲

۲-۵-۱ IntServ ۲۲

۲-۵-۲ DiffServ ۲۳

۲-۶ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش سوم) ۲۵

۲-۶-۱ MPLS ۲۵

۲-۶-۲ .سرویسهای مجتمع در حوزههای MPLS با استفاده از سیگنالینگ CR-LDP ۲۵

۲-۶-۳ .MPLS و DiffServ ۲۶

۲-۶-۴ .QoS در MPLS VPNها ۲۶

۲-۷ مدیریت IPVPN ها ۲۷

۲-۸ نیازمندیهای مدیریت QoS ۲۸

۲-۹- قابلیتهای عمومی مدیریت QoS برای تدارک IPVPN ۲۹

۲-۱۰ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش چهارم) ۲۹

۲-۱۰-۱ مدیریت QoS برای توافقات سطح سرویس (SLA) ۲۹

۲-۱۱ خصوصیات مدیریت QoS برای پیاده سازی ۳۰

۲-۱۲ مفاهیم مدیریتی کاربردی و مدل های پیشنهادی ۳۲

بر طبق استاندارد IETF سه گزینه برای گسترش سیستمهای مدیریت VPN و سیستمهای پشتیبانی QoS برای تحویل سرویس VPN وجود دارد ۳۳

www.prozhe.com

www.prozhe.com

مدیریت بر مبنای سیاست با استفاده از یک معماری عملیاتی لایهای ۳۳

۲-۱۳ SLA مجتمع شده ومدیریت اطلاعات QoS ۳۴

۲-۱۴ جداسازی مدیریت در شبکه سرویسهای VPN و شبکه انتقال VPN ۳۵

۲-۱۵ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش پنجم) ۳۵

به طور کلی روشهای اندازه گیری و مانیتور کردن پارامترهای کارایی شبکه به دو دسته تقسیم میشوند ۳۶

فصل سوم ۳۸

۳-مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) ۳۹

۳-۱ مانیتورکردن برمبنای سیاست ۳۹

۳-۲ بسته های OAM نهفته ۴۰

۳-۳ نیازمندیهای شبکههای بدون اتصال ۴۱

۳-۴ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش هفتم و پایانی) ۴۲

۳-۴-۱ مانیتور کردن ترافیک در شبکه های خصوصی مجازی ۴۲

۳-۵ عملیات گره های مانیتورینگ ۴۲

۳-۵-۱ نتیجه گیری روش مانیتورینگ نهفته ۴۳

نتایج ۴۵

منابع و ماخذ ۴۳

www.prozhe.com

www.prozhe.com

بسمه تعالی

نظر داوران

این پروژه با عنوان شبکه خصوصی مجازی VPN در تاریخ ۱۳۹۱/۰۳/۲۵ توسط آقای حسن صفری مفرد

به شماره دانشجویی ۸۹۱۰۲۱۸۱ دفاع و به عنوان پروژه پایانی در مقطع کاردانی پذیرفته شده است .

استاد راهنما : سرکار خانم مهندس سارا خسروی

تاریخ و امضاء

www.prozhe.com

www.prozhe.com

چکیده :

یک VPN ، شبکه ای اختصاصی بوده که از یک شبکه عمومی (عموما" اینترنت) ، بـرای ارتبـاط بـا سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض اسـتفاده از خطوط واقعی نظیر : خطوط Leased ، از یک ارتبـاط مجـازی بکمـک اینترنـت بـرای شـبکه اختصاصـی بمنظور ارتباط به سایت ها استفاده می کند.

همزمان با عمومیت یافتن اینترنت ، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خـود را بدرستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدنـد.ایـن نـوع شـبکه بصـورت کـاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبـور تعریـف شـده ، قـادر بـه ورود بـه شـبکه و استفاده از منابع موجود می باشند. اخیرا" ، تعداد زیادی از موسسات و سازمانها بـا توجـه بـه مطـرح شـدن خواسته های جدید (کارمنـدان از راه دور ، ادارات از راه دور)، اقـدام بـه ایجـاد شـبکه هـای اختصاصـی مجازی Virtual Private Network(VPN) نموده اند.

با توجه به موارد گفته شده ، چه ضرورتی بمنظور استفاده از VPN وجود داشته و VPN تامین کننده، کدامیک از اهداف و خواسته های مورد نظر است؟ با توجه به مقایسه انجام شده در مثال فرضی، مـی تـوان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می شود. زیردریائی فوق دارای خصایص متفاوت نظیر :

- دارای سرعت بالا است .
- هدایت آن ساده است .
- قادر به استتار(مخفی نمودن) شما از سایر زیردریا ئیها و کشتی ها است .
- قابل اعتماد است .
- پس از تامین اولین زیردریائی ، افزودن امکانات جانبی و حتی یـک زیردریـائی دیگرمقـرون بـه صـرفه خواهد بود

www.prozhe.com

www.prozhe.com

فصل اول

www.prozhe.com

www.prozhe.com

۱- شبکه های خصوصی مجازی

در طی ده سال گذشته دنیا دستخوش تحولات فراوانی در عرصه ارتباطات بوده است . اغلب سازمانها و موسسات ارائه دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه ای مسائل را دنبال و در صدد ارائه راهکارهای مربوطه بودند ، امروزه بیش از گذشته نیازمند تفکر در محدوده جهانی برای ارائه خدمات و کالای تولیده شده را دارند. به عبارت دیگر تفکرات منطقه ای و محلی حاکم بر فعالیت های تجاری جای خود را به تفکرات جهانی و سراسری داده اند. امروزه با سازمانهای زیادی برخورد می نمائیم که در سطح یک کشور دارای دفاتر فعال و حتی در سطح دنیا دارای دفاتر متفاوتی می باشند . تمام سازمانهای فوق قبل از هر چیز بدنبال یک اصل بسیار مهم می باشند : یک روش سریع ، ایمن و قابل اعتماد بمنظور برقراری ارتباط با دفاتر و نمایندگی در اقصی نقاط یک کشور و یا در سطح دنیا اکثر سازمانها و موسسات بمنظور ایجاد یک شبکه WAN از خطوط اختصاصی (Leased Line) استفاده می نمایند.خطوط فوق دارای انواع متفاوتی می باشند. ISDN (با سرعت ۱۲۸ کیلوبیت در ثانیه)، (OC3 Optical Carrier-3) (با سرعت ۱۵۵ مگابیت در ثانیه) دامنه وسیع خطوط اختصاصی را نشان می دهد. یک شبکه WAN دارای مزایای عمده ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت وکارآئی است . پشتیانی و نگهداری یک شبکه WAN در عمل و زمانیکه از خطوط اختصاصی استفاده می گردد ، مستلزم صرف هزینه بالائی است.

همزمان با عمومیت یافتن اینترنت ، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خود را بدرستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدند.این نوع شبکه بصورت کاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده ، قادر به ورود به شبکه و استفاده از منابع موجود می باشند. اخیرا" ، تعداد زیادی از موسسات و سازمانها با توجه به مطرح شدن خواسته های جدید (کارمندان از راه دور ، ادارات از راه دور)، اقدام به ایجاد شبکه های اختصاصی مجازی Virtual Private Network(VPN) نموده اند.

www.prozhe.com

www.prozhe.com

یک VPN ، شبکه ای اختصاصی بوده که از یک شبکه عمومی (عموما" اینترنت) ، بـرای ارتبـاط بـا سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض اسـتفاده از خطوط واقعی نظیر : خطوط Leased ، از یک ارتبـاط مجـازی بکمـک اینترنـت بـرای شـبکه اختصاصـی بمنظور ارتباط به سایت ها استفاده می کند.

۱-۱ عناصر تشکیل دهنده یک VPN

دو نوع عمده شبکه های VPN وجود دارد :

o دستیابی از راه دور (Remote-Access) . به این نوع از شـبکه هـا VPDN)Virtual private dial-up network)، نیز گفته می شود.در شبکه های فـوق از مـدل ارتبـاطی User-To-Lan (ارتبـاط کاربر به یک شبکه محلی) استفاده می گردد. سازمانهائی که از مدل فوق استفاده می نماینـد ، بـدنبال ایجـاد تسهیلات لازم برای ارتباط پرسنل (عموما" کاربران از راه دور و در هر مکـانی مـی تواننـد حضـور داشـته باشند) به شبکه سازمان می باشند. سازمانهائی که تمایل به برپاسازی یک شبکه بزرگ " دستیابی از راه دور " می باشند ، می بایست از امکانات یک مرکز ارائه دهنـده خـدمات اینترنـت جهـانی ESP)Enterprise service provider) استفاده نمایند. سـرویس دهنـده ESP ، بمنظـور نصـب و پیکربنـدی VPN ، یـک NAS)Network access server) را پیکربندی و نرم افزاری را در اختیـار کـاربران از راه دور بمنظـور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی بـه NAS و اسـتفاده از نرم افزار مربوطه بمنظور دستیابی به شبکه سازمان خود خواهند بود.

- سایت به سایت (Site-to-Site) . در مدل فوق یک سازمان با توجه به سیاست های موجـود ، قـادر بـه اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیـر اینترنـت اسـت . شـبکه هـای VPN کـه از روش فوق استفاده می نمایند ، دارای گونه های خاصی در این زمینه می باشند:

www.prozhe.com

www.prozhe.com

- مبتنی بر اینترانت . در صورتیکه سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آنها در یک شبکه اختصاصی باشد ، می توان یک اینترانت VPN را بمنظور برقرای ارتباط هر یک از شبکه های محلی با یکدیگر ایجاد نمود.
- مبتنی بر اکسترانت . در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد ، می توان یک اکسترانت VPN را بمنظور ارتباط شبکه های محلی هر یک از سازمانها ایجاد کرد. در چنین حالتی سازمانهای متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

استفاده از VPN برای یک سازمان دارای مزایای متعددی نظیر : گسترش محدوه جغرافیائی ارتباطی ، بهبود وضعیت امنیت ، کاهش هزینه های عملیاتی در مقایسه با روش های سنتی WAN ، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور ، بهبود بهره وری ، توپولوژی آسان ،... است . در یکه شبکه VPN به عوامل متفاوتی نظیر : امنیت ، اعتمادپذیری ، مدیریت شبکه و سیاست ها نیاز خواهد بود.

۱-۳ شبکه های LAN جزایر اطلاعاتی

فرض نمائید در جزیره ای در اقیانوسی بزرگ ، زندگی می کنید. هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر نزدیک و برخی دیگر دارای مسافت طولانی با جزیره شما می باشند. متداولترین روش بمنظور مسافرت به جزیره دیگر ، استفاده از یک کشتی مسافربری است. مسافرت با کشتی مسافربری ، بمنزله عدم وجود امنیت است. در این راستا هر کاری را که شما انجام دهید، توسط سایر مسافرین قابل مشاهده خواهد بود. فرض کنید هر یک از جزایر مورد نظر به مشابه یک شبکه محلی (LAN) و اقیانوس مانند اینترنت باشند. مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب و یا سایر دستگاههای موجود در اینترنت است . شما دارای هیچگونه کنترلی بر روی کابل ها و روترهای موجود در اینترنت نمی باشید. (مشابه عدم کنترل شما بعنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی) .در صورتیکه تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد ، اولین مسئله ای که با چالش های جدی برخورد خواهد کرد ، امنیت خواهد بود.

www.prozhe.com

www.prozhe.com

فرض کنید، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد .مسیر ایجاد شده یک روش ایمن، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می آورد. همانطور که حدس زده اید، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه های بالائی خواهد بود.(حتی اگر جزایر در مجاورت یکدیگر باشند). با توجه به ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن ، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده است. در صورتیکه جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است، هزینه های مربوط بمراتب بیشتر خواهد بود. وضعیت فوق ، نظیر استفاده از یک اختصاصی Leased است. ماهیت پل های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکن قادر به ارتباط جزایر(شبکه های LAN) خواهند بود. سازمانها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می نمایند. مهمترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمانهای مورد نظر با یکدیگر است . در صورتیکه مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد ، هزینه مربوط به برقرای ارتباط نیز افزایش خواهد یافت .

با توجه به موارد گفته شده ، چه ضرورتی بمنظور استفاده از VPN وجود داشته و VPN تامین کننده، کدامیک از اهداف و خواسته های مورد نظر است؟ با توجه به مقایسه انجام شده در مثال فرضی، می توان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می شود. زیردریائی فوق دارای خصایص متفاوت نظیر :

- دارای سرعت بالا است .
- هدایت آن ساده است .
- قادر به استتار(مخفی نمودن) شما از سایر زیردریا ئیها و کشتی ها است .
- قابل اعتماد است .
- پس از تامین اولین زیردریائی ، افزودن امکانات جانبی و حتی یک زیردریائی دیگرمقرون به صرفه خواهد بود

www.prozhe.com

www.prozhe.com

در مدل فوق ، با وجود ترافیک در اقیانوس ، هر یک از ساکنین دو جزیره قادر به تردد در طـول مسـیر در زمان دلخواه خود با رعایت مسایل ایمنی می باشند. مثال فوق دقیقا" بیانگر تحوه عملکرد VPN اسـت . هر یک از کاربران از راه دور شبکه قادربه برقراری ارتباطی امن و مطمئن بـا اسـتفاده از یـک محـیط انتقـال عمومی (نظیر اینترنت) با شبکه محلی (LAN) موجود در سازمان خود خواهنـد بـود. توسـعه یـک VPN (افزایش تعداد کاربران از راه دور و یا افزایش مکان های مورد نظر) بمراتب آسانتر از شبکه هائی است کـه از خطوط اختصاصی استفاده می نمایند. قابلیت توسعه فراگیر از مهمتزین ویژگی های یک VPN نسبت بـه خطوط اختصاصی است .

۱-٤ امنیت VPN

شبکه های VPN بمنظور تامین امنیت (داده ها و ارتباطات) از روش های متعددی استفاده می نمایند :

- فایروال . فایروال یک دیواره مجازی بین شبکه اختصای یـک سـازمان و اینترنـت ایجـاد مـی نمایـد. بـا استفاده از فایروال می توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یـک سـازمان انجـام داد. ایجاد محدودیت در تعداد پورت ها فعال ، ایجاد محدودیت در رابطه به پروتکل های خاص ، ایجاد محدودیت در نوع بسته های اطلاعاتی و ... نمونه هائی از عملیاتی است که می توان بـا اسـتفاده از یـک فایروال انجام داد.
- رمزنگاری . فرآیندی است که با استفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را بـرای کـامپیوتر دیگـر ارسال می نماید. سایر کامپیوترها ی مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیـب پس از ارسال اطلاعات توسط فرستنده ، دریافت کنندگان، قبل از استفاده از اطلاعات می بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم مـی گردد :
  - رمزنگاری کلید متقارن
  - رمزنگاری کلید عمومی

www.prozhe.com

www.prozhe.com

در رمز نگاری " کلید متقارن " هر یک از کامپیوترها دارای یک کلید Secret (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می باشند. در روش فوق می بایست در ابتدا نسبت به کامپیوترهائی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند ، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می بایست دارای کلید رمز مشابه بمنظور رمزگشائی اطلاعات باشند. بمنظور رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد. فرض کنید قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را داشته باشید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می شود .در الگوریتم فوق هر حرف به دوحرف بعد از خود تبدیل می گردد.(حرف A به حرف C ، حرف B به حرف D) .پس از رمزنمودن پیام و ارسال آن، می بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام لرسال شده، هر حرف به دو حرق قبل از خود می باطست تبدیل گردد. در چنین حالتی می باطست به دوست امین خود، واقعیت فوق (کلید رمز) گفته شود. در صورتیکه پیام فوق توسط افراد دیگری دریافت گردد ، بدلیل عدم آگاهی از کلید ، آنان قادر به رمزگشائی و استفاده از پیام ارسال شده نخواهند بود.

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" برای کامپیوتر شما (ارسال کننده) قابل شناسائی و استفاده است . کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند ، گذاشته می شود. بمنظور رمزگشائی یک پیام رمز شده ، یک کامپیوتر می بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال کننده) ، کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید . یکی از متداولترین ابزار "رمزنگاری کلید عمومی" ، روشی با نام Pretty Good Privacy(PGP) است . با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

- IPSec . پروتکل Internet protocol security protocol(IPsec) ، یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می باشد . قابلیت روش فوق در مقایسه با الگوریتم های رمزنگاری بمراتب بیشتر است . پروتکل فوق دارای دو روش رمزنگاری است : Tunnel، Transport

www.prozhe.com

www.prozhe.com

در روش tunel ، هدر و Payload رمز شده درحالیکـه در روش transport صـرفا" payload رمـز می گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت است :

- روتر به روتر
- فایروال به روتر
- کامپیوتر به روتر
- کامپیوتر به سرویس دهنده

? سـرویس‌دهنـده AAA . سـرویس‌دهنـدگان (AAA : Authentication ,Authorization, Accounting) بمنظور ایجاد امنیت بالا در محیط های VPN از نـوع "دسـتیابی از راه دور" اسـتفاده مـی گردند. زمانیکه کاربران با استفاده از خـط تلفـن بـه سیسـتم متصـل مـی گردنـد ، سـرویس دهنـده AAA درخواست آنها را اخذ و عمایات زیر را انجام خواهد داد :

- شما چه کسی هستید؟ (تایید، Authentication)
- شما مجاز به انجام چه کاری هستید؟ (مجوز، Authorization)
- چه کارهائی را انجام داده‌اید؟ (حسابداری، Accounting)

۱-۵ تکنولوژی های VPN

با توجه به نوع VPN (" دستیابی از راه دور" و یا " سایت به سایت")، بمنظور ایجاد شبکه از عناصر خاصی استفاده می‌گردد:

- نرم افزارهای مربوط به کاربران از راه دور
- سخت افزارهای اختصاصی نظیر یک " کانکتور VPN" و یا یک فایروال PIX
- سرویس دهنده اختصاصی VPN بمنظور سرویُس های Dial-up
- سرویس دهنده NAS که توسط مرکز ارائه خدمات اینترنت بمنظور دستیابی به VPN از نوع "دسـتیابی از را دور" استفاده می شود.

www.prozhe.com

www.prozhe.com

- شبکه VPN و مرکز مدیریت سیاست ها

با توجه به اینکه تاکنون یک استاندارد قابل قبول و عمومی بمنظور ایجاد شVPN ایجاد نشده است، شرکت های متعدد هر یک اقدام به تولید محصولات اختصاصی خود نموده اند.

- کانکتور VPN . سخت افزار فوق توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل های متفاوت و قابلیت های گوناگون عرضه شده است . در برخی از نمونه های دستگاه فوق امکان فعالیت همزمان ۱۰۰ کاربر از راه دور و در برخی نمونه های دیگر تا ۱۰.۰۰۰ کاربر از راه دور قادر به اتصال به شبکه خواهند بود.
- روتر مختص VPN . روتر فوق توسط شرکت سیسکو ارائه شده است . این روتر دارای قابلیت های متعدد بمنظور استفاده در محیط های گوناگون است . در طراحی روتر فوق شبکه های VPN نیز مورد توجه قرار گرفته و امکانات مربوط در آن بگونه ای بهینه سازی شده اند.
- فایروال PIX . فایروال PIX(Private Internet eXchange) قابلیت هائی نظیر NAT ، سرویس دهنده Proxy ، فیلتر نمودن بسته ای اطلاعاتی ، فایروال و VPN را در یک سخت افزار فراهم نموده است . Tunneling) تونل سازی (اکثر شبکه های VPN بمنظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان " Tunneling " استفاده می نمایند. در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو نقطه (ورود و خروج بسته اطلاعاتی) قابل فهم می باشد. دو نقطه فوق را "اینترفیس های تونل" می گویند. روش فوق مستلزم استفاده از سه پروتکل است :

- پروتکل حمل کننده . از پروتکل فوق شبکه حامل اطلاعات استفاده می نماید.
- پروتکل کپسوله سازی . از پروتکل هائی نظیر: IPSec,L2F,PPTP,L2TP,GRE استفاده می گردد.
- پروتکل مسافر. از پروتکل‌هائی نظیر IPX,IP,NetBeui بمنظور انتقال داده های اولیه استفاده می‌شود.

با استفاده از روش Tunneling می توان عملیات جالبی را انجام داد. مثلا" می توان از بسته ای اطلاعاتی که پروتکل اینترنت را حمایت نمی کند (نظیر NetBeui) درون یک بسته اطلاعاتی IP استفاده

www.prozhe.com

www.prozhe.com

و آن را از طریق اینترنت ارسال نمود و یا می توان یک بسته اطلاعـاتی را کـه از یـک آدرس IP غیـر قابـل روت (اختصاصی) استفاده می نماید ، درون یک بسته اطلاعاتی که از آدرس‌های معتبر IP استفاده می‌کنـد، مستقر و از طریق اینترنت ارسال نمود.

در شبکه های VPN از نوع " سـایت بـه سـایت " ، generic routing encapsulation(GRE) بعنوان پروتکل کپسوله سازی استفاده می‌گردد. فرآیند فوق نحوه استقرار و بسته بندی " پروتکل مسـافر" از طریق پروتکل "حمل کننده" برای انتقال را تبین می نماید. (پروتکل حمـل کننـده ، عمومـا" IP اسـت) . فرآیند فوق شامل اطلاعاتی در رابطه با نوع بست های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنـده و سـرویس دهنـده اسـت . در برخـی مـوارد از پروتکـل IPSec (در حالـت tunnel) برای کپسوله سازی استفاده می گردد.پروتکل IPSec ، قابل اسـتفاده در دو نـوع شـبکه VPN (سایت به یایت و دستیابی از راه دور) است . اینترفیش های Tunnel می بایست دارای امکانات حمایتی از IPSec باشند.

در شبکه های VPN از نوع " دستیابی از راه دور " ، Tunneling با استفاده از PPP انجام می گیرد. PPP بعنوان حمل کننده سایر پروتکل های IP در زمان برقراری ارتبـاط بـین یـک سیسـتم میزبـان و یـک سیستم ازه دور ، مورد استفاده قرار می گیرد.

هر یک از پروتکل های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه های VPN از نوع " دستیابی از راه دور " استفاده می گردند:

- Layer 2 Forwarding(L2F) . پروتکل فوق توسط سیسکو ایجاد شده اسـت . در پروتکـل فـوق از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده اند ، استفاده شد ه است .

(Point-to-Point Tunneling Protocol(PPTP) . پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است . این پروتکل امکان رمزنگاری ٤٠ بیتی و ١٢٨ بیتـی را دارا بـوده و از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده اند ، استفاده می نماید.

www.prozhe.com

www.prozhe.com

- Layer 2 Tunneling Protocol(L2TP). پروتکل فوق با همکاری چندین شرکت ایجاد شده است. پروتکل فوق از ویژگی های PPTP و L2F استفاده کرده است . پروتکل L2TP بصورت کامل IPSec را حمایت می کند. از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می گردد :

- سرویس گیرنده و روتر
- NAS و روتر
- روتر و روتر

عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (ایترفیس ورودی تونل) برای متقاضی ارسال می دارد. کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی ، تا به منزل شما (اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می نمائید.

www.prozhe.com

www.prozhe.com

فصل دوم

www.prozhe.com

www.prozhe.com

۲- مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش نخست)

چکیده

این مقاله در ابتدا به تعریف شبکه‌های خصوصی مجازی به طور عام و سپس VPNهای مبتنی بر IP می‌پردازد و انواع مختلف این شبکه را معرفی می کند. در ادامه نیازمندی‌های مدیریتی آن را از دید نواحی کارکردی FCAPS شرح داده می‌شود. بخش بعدی این مقاله مدل‌های مختلف کیفیت سرویس در این شبکه‌ها را ارایه می دهد. سپس نحوه‌ی مدیریت IPVPNها برای برآورده ساختن نیازمندی‌های کارایی و کیفیت سرویس و در انتها یک روش برای مانیتور کردن نهفته پارامترهای کیفیت سرویس IPVPN ها آورده می‌شود. معماری پیشنهادی در این بخش دو مشخصه‌ی اصلی دارد، نخست این‌که از یک روش in-serveice استفاده می‌کند که در آن پارامترهای ترافیک واقعی کاربر به وسیله بسته‌های مخصوص مانیتورینگ اندازه گیری می‌شوند و دیگر این‌که توابع مانیتورینگ، یک بخش مجتمع از عناصر عادی شبکه را تشکیل می‌دهند.

www.prozhe.com

www.prozhe.com

۲-۱ . مقدمه

امروزه شبکه‌های خصوصی مجازی (Virtual Private Network)ها که از طریق تسهیلات backbone های IP اجرا می شوند، بسیار مورد اقبال قرار گرفته‌اند. VPN های مبتنی بر IP به عنوان یکی از نوید بخش‌ترین سرویس‌ها برای تهیه‌کنندگان شبکه نمایان شده‌اند. گسترش دامنه‌دار IPVPN ها به دلیل نبود پیاده‌سازی‌های عملی و سردرگمی در بین تعداد بالای راه‌حل‌هایی که به وسیله ترکیب IPVPN تشریح می‌شوند، به تعویق افتاده است. به علاوه پرسش‌ها و تردیدهایی در باره-ی امنیت (security)، کیفیت سرویس یا قابلیت گسترش پیاده‌سازی VPN مبتنی بر IP وجود دارند.

www.prozhe.com

www.prozhe.com

۲-۲ . IPVPN چیست؟

سازمان‌ها از شبکه‌های خصوصی برای ارتباط با سایت‌های دور و نیز ارتباط با سازمان‌های دیگر استفاده می‌کنند. با گسترش اینترنت، بسیاری از سازمانها به سمت شبکه‌های خصوصی مجازی حرکت کرده اند که بسیاری از مزایای شبکه‌های خصوصی را با هزینه‌ای کمتر ارایه می‌دهند. اگرچه VPNها دارای خطرهایی را هم دربردارند، با معماری و پیاده‌سازی درست می‌توانند برای یک سازمان به حد کافی مفید باشند.

مفهوم شبکه‌ی خصوصی مجازی یک مفهوم جدید نیست. فناوری‌هایی مانند ISDN، FrameRelay یا ATM در دهه‌های گذشته به عنوان مبنایی برای پیاده‌سازی این مفهوم استفاده شده‌اند. بدون توجه به هر قالب یا فناوری که پشت سر آن باشد، یک VPN سرویسی را تهیه می‌کند که از لحاظ عملکرد معادل یک شبکه‌ی خصوصی با منابع عمومی است.

VPN می‌تواند به عنوان سرویسی تعریف شود که اتصال دهندگی مشتری در میان چندین سایت روی یک زیربنای تسهیم شده با همان سیاست‌های دسترسی یا امنیت یک شبکه‌ی خصوصی گسترش می‌یابد.

یک VPN باید در کارایی، اطمینان، امنیت، مدیریت و کیفیت سرویس قابل مقایسه با یک شبکه‌ی خصوصی باشد. مشتریهای سرویس‌های VPN تسهیلات و تجهیزات تسهیم شده‌ای را که به وسیله یک اپراتور شبکه‌ی عمومی، مدیریت، مهندسی و راه اندازی می‌شود، استفاده می‌کنند.

یک شبکه‌ی خصوصی مجازی IP می‌تواند به عنوان یک پیاده‌سازی VPN تعریف شود که از منابع تسهیم شده یا عمومی شبکه‌ی IPبرای پیروی از مشخصات یک شبکه خصوصی مبتنی بر IP استفاده می کند. در مقایسه با مدل‌های VPN اتصال‌گرای کلاسیک که مبتنی بر فناوری‌هایی هم‌چون ATM یا Frame Relayهستند، پیاده‌سازی VPNهای مبتنی بر IP با چالش‌های زیر روبه‌رو هستند:

- چگونه یک شبکه IP تسهیم شده را برای استفاده شرکت خصوصی، ایمن کنیم.
- چگونه تضمین کنیم که کیفیت و ظرفیت شبکه که مورد نیاز محدوده‌ی وسیعی از کاربران و کاربردهاست، به طور کامل پوشش داده می‌شوند.

www.prozhe.com

www.prozhe.com

دو نوع اصلی از VPN ها به طور مشخص شناخته شده اند:

۱- VPNهای مبتنی بر تجهیزات مربوط به مشتری یا CPE (Customer Premise Equipment)

۲- VPN های مبتنی بر شبکه.

در یک VPN مبتنی بر CPE دانش و اطلاعات مربوط به شبکه ی مشتری محدود به تجهیزات شخصی مشتری است. تدارک و مدیریت VPN به مدیریت شبکه‌ی مشتری وابسته است که به وسیله پیکربندی دستی تونل‌های بین CPEها انجام می‌شود، هرچند به طور معمول تامین‌کنندگان خدمات، مسوولیت مدیریت و تدارک تجهیزات کاربر را، برای کاهش نیازمندی‌های مدیریتی مشتری بر عهده دارند.

در VPNهای مبتنی بر شبکه، عملیات و کنترل به وسیله تجهیزات شبکه‌ی تامین‌کننده‌ی خدمات ایجاد می‌شود. شبکه‌ی مشتری به وسیله‌ی تونل‌ها که بین جفت روترهای کناری کار گذاشته می‌شوند، پشتیبانی می‌شود. تونلها ممکن است از کپسوله کردن‌های مختلف برای فرستادن ترافیک از طریق تامین‌کننده‌ی خدمات استفاده کنند. دو نوع اصلی از VPNهای مبتنی بر شبکه، VPNهای مبتنی بر لایه‌ی۲ و VPNهای مبتنی بر لایه‌ی ۳ هستند. شکل ۲ مدل یک VPN مبتنی بر شبکه را نشان می‌دهد که می‌توان آن را با مدل قبلی مقایسه کرد.

یک دسته‌بندی رایج از VPNها بر این مبناست که آیا CPE مشتری و تامین‌کننده‌ی خدمات اطلاعات مسیریابی را در سطح لایه‌ی ۳ تبادل می‌کنند یا خیر. دو مدل پیاده¬سازی از VPNها می‌توانند بر مبنای ضوابط زیر تعریف شود:

- مدل روی هم قرار گرفته (overlay): مدلی است که سرویس VPN از لحاظ عملکرد، معادل خطوط leased، شبیه‌سازی شده است و تامین‌کننده خدمات و مشتری اطلاعات مسیریابی لایه‌ی ۳ را تبادل نمی کنند. این مدل مسوولیت‌های مشتری و provider را به روشنی از یکدیگر جدا می‌کند.

www.prozhe.com

www.prozhe.com

- مدل peer-to-peer : وقتی تهیه‌کننده‌ی خدمات و مشتری اطلاعات مسیریابی لایه‌ی ۳ را رد و بدل می کنند، این مدل پیادهسازی مسیریابی مشتری را آسان می‌کند و تدارک آسان‌تری برای ارایه‌ی خدمات VPN به وجود می‌آورد.

مدل overlay: در مدل VPN روی هم قرار گرفته، تضمین کیفیت سرویس به طور معمول مبتنی بر پهنای باند تضمین شده بر روی یک VC مشخص و بیشینه‌ی پهنای باند در دسترس، بر روی یک VC خاص بیان می‌شود.

مدل peer-to-peer : در حقیقت مدل peer-to-peer VPN به منظور از میان بردن مشکلات موجود در مدل overlay VPNمعرفی شده است. در مدل peer-to-peer، روتر های کناری provider به طور مستقیم اطلاعات مسیریابی را با روتر CPE تبادل می‌کنند.

۲-۳ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش دوم)

۲-۳-۱ نیازمندیهای مدیریتی IPVPN – از دیدگاه service provider

۱. مدیریت خرابی (fault management): جنبه‌های پشتیبانی و کارکردهای مورد نیاز برای مدیریت خرابی شامل موارد زیر است:

- مشخص کردن مشتری‌هایی که از خرابی متاثر شده‌اند.
- کشف خطا (گزارش‌های حوادث، alarmها، مشخص کردن خطاها)
- تعیین محل خرابی
- ثبت حوادث
- عملیات اصلاحی (ترافیک، مسیریابی، تخصیص منابع).

VPNهای مبتنی بر شبکه بر یک زیرساخت شبکه‌ای واحد تکیه دارند، بنابراین سیستم مدیریت شبکه باید ابزاری برای اطلاع دادن به provider مربوط به VPNی که تحت تاثیر یک خرابی قرار گرفته است، تدارک ببیند. باید ابزاری برای مانیتور کردن وضعیت عنصر شبکه و ثبت رخداد مربوط به قطع سرویس به

www.prozhe.com

www.prozhe.com

صورت جزیی یا کلی وجود داشته باشد. در این راستا برای VPNهای مبتنی بر شبکه‌های به هم متصل، نه تنها برچسب زدن troubleها که ارسال علایمی که نشانه‌های alarm را در بردارد نیز - به ویژه در محیطی که دارای چندین تدارک سرویس است- مورد نیاز است.

خرابی‌هایی که به وسیله‌ی انواع مختلف خطاهای پیکربندی ایجاد شده‌اند و سرویس‌هایی که به دلیل پایین آمدن‌جدی کارایی، از رده خارج شده‌اند، باید به دقت شناخته شوند، اما تشخیص این‌گونه خطاها و پاک کردن خرابی‌ها در مواقعی که مساله شامل حوزه‌های provider ی به هم متصل فراوان و گره‌های زیاد است، ممکن است دشوار باشد. مدیریت خرابی باید به وسیله مانیتور کردن وضعیت و رخداد با استفاده از پروتکل های کنترلی موجود، وجود دسترسی‌های خاص مشتری و قیدهای مسیریابی و استفاده از تنظیم‌های مناسب پارامتر پیکربندی را بررسی کند. به عنوان حداقل ملزومات، باید توانایی تشخیص برقراری اتصال لایه ۲ (L2) یا مسیرهای قابل رسیدن لایه ۳ (L3)در داخل یک VPN به وجود آید.

۲. مدیریت پیکربندی(configuration management)- نیازهای مرتبط: IETF به تازگی جزییات نیازمندی‌ها را به طور جداگانه‌برای پیکربندی‌های مبتنی بر CE و مبتنی بر PE به صورت زیر تعریف کرده است:

۲-۳-۲ مدیریت پیکربندی برای VPNهای مبتنی بر شبکه(طرف provider):

نیازمندی‌های مدیریت پیکربندی که تنها برای یک VPN طرف provider است، به شرح زیر است:

- سیستم مدیریت شبکه(NMS) باید دست کم پیکربندی جنبه‌های زیر را برای روتر های PE لایه‌ی ۳ پشتیبانی کند: عضویت اینترانت و اکسترانت و پروتکل مسیریابی CE برای هر اتصال قابل دسترسی، اندازه‌گیری‌های مسیر، تونل‌ها و غیره.
- NMS باید شناسه‌هایی را برای SPها، PPVPNها، PEها و CEها به کار برد و از "تونل‌های سلسله مراتبی" پشتیبانی کند.

www.prozhe.com

www.prozhe.com

- تونل‌ها باید بین دستگاه‌های P و PE پیکربندی شوند. که این پیکربندی نیازمند هماهنگی و مشارکت شناسه‌های تونل‌ها، تونل‌های سلسله مراتبی، VPNها و هر اطلاعات سرویس وابسته به آن‌ها، برای مثال یک سرویس QoS/SLA است.
- پروتکل‌های مسیریابی که بین روتر های PE و دستگاه‌های CE اجرا می‌شوند باید برای هر VPN پیکربندی شوند.
- برای سرویس چندپخشی، پروتکل های مسیریابی چندبخشی نیز باید قابل پیکربندی باشند.
- پروتکل‌های مسیریابی که بین روتر های PE اجرا می‌شوند و آن‌هایی که بین روتر های P و PE اجرا می‌شوند نیز باید پیکربندی شوند.
- پیکربندی یک PPVPN بر مبنای PE باید متناسب با پیکربندی زیرساخت پایه‌ی آن شامل اجزای متصل شده‌ی شبکه‌های لایه ۲ و لایه ۱ یک PPVPN باشد.

۲-۳-۳ مدیریت پیکربندی برای VPN های بر مبنای CE

نیازمندی‌های مدیریتی خاص برای VPNهای بر مبنای CE، شامل موارد زیر است:

- تونل‌ها باید بین دستگاه‌های CE پیکربندی شوند. برای این پیکربندی باید:
- هماهنگی شناسه‌های تونل‌ها، VPNها و هر نوع اطلاعات سرویس وابسته به آن‌ها؛ برای مثال، یک سرویس QoS/SLA.
- پروتکل‌های مسیریابی که بین روتر های PE اجرا می‌شوند و دستگاه‌های CE، باید پیکربندی شوند. همچنین برای سرویس چندپخشی، باید پروتکل های مسیریابی چندپخشی قابل پیکربندی باشند.

۳. مدیریت حسابداری(Accounting management)-بسیاری از تهیه کنندگان سرویس هزینه شارژ را بر مبنای میزان مصرف ارایه می‌کنند، بنابراین اندازه‌گیری‌هایی که میزان مصرف منابع را نشان می‌دهد باید (با استفاده از سیستم‌های پشتیبانی و پروتکل ها) کامل باشد، تا بتوان به حساب مشتریان رسیدگی کرد. همچنین ممکن است NMS به نگه‌داری همبستگی میان اطلاعات حسابداری با اطلاعات مدیریت

www.prozhe.com

www.prozhe.com

خرابی و کارآیی نیاز داشته باشد. همه‌ی راه‌حل‌های گسترش PPVPN باید چه‌گونگی انجام توابع مدیریت حسابداری زیر را تشریح کنند:

- اندازه‌گیری میزان استفاده از منابع
- جمع‌آوری اطلاعات حسابداری
- ذخیره‌سازی و مدیریت اندازه‌گیری‌ها

بسیاری از تهیه‌کنندگان سرویس ممکن است به اطلاعات اندازه‌گیری نزدیک به زمان واقعی نیاز داشته باشند و ممکن است این نیازمندی را به عنوان بخشی از یک سرویس مدیریت شبکه مشتری ارایه دهند.

٤. مدیریت کارایی (Performance Management)- مدیریت کارایی شامل مجموعه توابعی است که درگیر مانیتور کردن و جمع‌آوری داده‌های مربوط به کارایی دستگاه‌های مربوط، تسهیلات و خدمات و هم‌چنین محاسبه‌ی میزان توافق با مشخصات سطح سرویس (SLS) مانند QoS و اندازه‌گیری‌های قابل دسترسی بودن هستند. مدیریت کارایی هم‌چنین باید تحلیل جنبه‌های مهم یک PPVPN، مانند میزان استفاده از پهنای باند، زمان پاسخ، در دست‌رس بودن، آمارگیری‌های QoS، و برنامه‌ریزی‌های آینده بر مبنای داده‌های جمع آوری شده را پشتیبانی کند.

٤-٢ مانیتور کردن کارایی

NMS باید رفتار دستگاه را از لحاظ توانایی در ارزیابی اندازه‌گیری‌های کارایی مربوط به یک توافق سطح سرویس مشخص، مانیتور کند. NMS هم‌چنین باید جنبه هایی از یک VPN را که به طورمستقیم به یکSLA وابسته نیستند، مانند سطوح مصرف و تغییرات کارایی در وضعیت‌های پرباری، مانیتور کند.

سیستم مدیریت شبکه باید SLAهای بین SP و مشتری‌های گوناگون رابر طبق SLS (Service Level Specification)های مرتبط پشتیبانی کند.

www.prozhe.com

www.prozhe.com

۵. مدیریت امنیت- تابع مدیریت امنیت کارکردی NMS، باید شامل جنبه‌هایی از مدیریت برای تضمین امنیت دستگاه‌ها، اتصالات قابل دسترس و پروتکل های داخل شبکه PPVPN و هم‌چنین امنیت داده‌ها و کنترل‌های مشتریان باشد. .

۲-۵ Qos در IPVPN ها

کیفیت سرویس به طور کلی به معنای اطمینان از داشتن کم‌ترین تاخیر یا گم شدن کم‌ترین میران بسته هاست. که برای انواع مشخصی از کاربردها یا ترافیک تعریف شود. شبکه‌های سنتی شرکت‌ها می‌توانستند سطوح ثابتی را برای در دسترس بودن منابع در همه‌ی وضعیت‌ها تضمین کنند که این تضمین با استفاده از مدارهای اجاره‌ای اختصاصی صورت می‌گرفت. VPNهای لایه‌ی ۲ می‌توانند کارایی قابل قبول و قابل مقایسه با راه‌حل‌های خطوط اختصاصی، ایجاد کنند. هم‌چنین انتظار می‌رود که تهیه کنندگان سرویس IPVPN نیز ز QoS به همان نوع پشتیبانی کنند.

به وسیله IETF دو چارچوب به عنوان معماری‌های QoS در شبکه‌های بر مبنای IP به وجود آمده است: سرویس‌های مجتمع (IntServ) و سرویس‌های متمایز (DiffServ). هم‌چنین MPLS همراه با مدیریت ترافیک و مسیریابی مبتنی بر محدودیت نیز ابزارهای جدیدی را برای مدیریت و کنترل QoS تهیه می‌کنند. که این روش‌ها قابل کاربرد به VPNهای مبتنی بر IP نیز هستند.

۲-۵-۱ IntServ:

در مدل سرویس‌های مجتمع، applicationها مشخصات ترافیکی خود را می دانند و به گره‌های میانی شبکه علامت می‌دهند تا منابع مشخصی را برای‌شان ذخیره کنند تا بتوانند مشخصات ترافیکی آن‌ها را برآورده سازند. بر حسب در دست‌رس بودن منابع، گره‌های میانی شبکه، منابع را رزرو می‌کند و یک پیغام acknowledgement مثبت یا منفی برمی‌گرداند. این بخش از استاندارد، کنترل ورود

www.prozhe.com

www.prozhe.com

(admissioncontrol) نامیده می‌شود. پروتکل سیگنالینگی که در این بخش بیش‌تر استفاده می‌شود RSVP یا Resource reSerVation Protocol نامیده می‌شود.

RSVP دو نوع کلاس سرویس را وابسته به نوع کاربرد و میزان حساسیت آن به تاخیر، گم شدن بسته ها و ... تحویل می‌دهد:

۱.سرویس تضمین شدهGuaranteed service: این سرویس پهنای باند را برای ترافیک application مورد نظر و بیشینه‌ی معینی را برای تاخیر تضمین می‌کند.

۲. سرویس با بار کنترل شدهControl-load service: در این سرویس تاخیر متوسط تضمین می‌شود، اما تاخیر انتها به انتهایی، که به وسیله یک بسته‌ی دلخواه ایجاد می‌شود، به طور دقیق نمی‌تواند محاسبه شود.

عمده‌ترین مشکل روش‌های سرویس مجتمع، در استفاده از RSVP است. RSVP به تک تک جریان های هر ترافیک یک QoS نسبت می‌دهد. بنابراین ترافیک سیگنالینگ سنگینی باید بین عناصر شبکه که وابسته به یک ناحیه مرکزی از شبکه هستند، مبادله شود. به علاوه، بعد از این‌که یک رزرو صورت گرفت و ارتباط برقرار شد، هر عنصر شبکه باید برای هر بسته IP رسیده، کلاسی مشخص کند تا متعلق بودن آن به یک جریان QoS مشخص شود و اگر بسته IP رسیده متعلق به جریان QoS مورد نظر بود، منابع لازم را به جریان نسبت دهد. بنابراین در استفاده از RSVP مسایلی هم‌چون قابلیت گسترش در حوزه‌ی سیگنالینگ، کلاس‌بندی و مکانیزم‌های زمان‌بندی وجود دارد.

۲-۵-۲ DiffServ:

تدارک سرویس متمایز برای تهیه‌ی QoS در یک شبکه از طریق مکانیزم‌هایی است که می‌توانند برای به دست آوردن یک سرویس برای مشتری انتهایی استفاده شوند. یکی از این مکانیزم‌ها رفتار در هر(HOP)یا (PHB) است. DiffServ تعدادی از رفتارهای داده‌ها را که به عنوان یک PHB شناخته می شوند، تعریف می‌کند. این رفتارها می‌توانند به بسته‌های هر گره اعمال شوند (همه‌ی بسته‌هایی که از یک

www.prozhe.com

www.prozhe.com

لینک عبور می‌کنند و به رفتار مشابهی نیاز دارند یک Behavior Aggregate (BA) را تشکیل می‌دهند). PHB برای مشخص کردن رفتار نسبت داده شده به هر بسته در گره به کار می‌رود. این رفتار شامل انتخاب صف و تنظیم زمان‌بندی و آستانه‌ی ازدحام است. بسته‌ها برای تشخیص رفتاری که نیاز دارند، با استفاده از بایت DS علامت‌گذاری می‌شوند. بایت DS در قسمت بایتTOS که در هِدِر IP وجود دارد، قرار می گیرد. PHBهای تعریف شده عبارت‌اند از:

- Expedited Forwarding(EF)

EF PHB در هر گره loss پایین، jitter پایین و تاخیر پایین را عرضه می‌دارد.

- Assured Forwarding(AF)

گروه AF PHB، N کلاس فورواردینگ غیر وابسته را تعریف می‌کند (در حال حاضر ٤ کلاس فورواردینگ غیر وابسته تعریف شده است) که به صورت AF1 تا AFn هستند. در داخل هر یک از این کلاس‌های فورواردینگ، برای احتمال تحویل بسته، M زیر کلاس وجود دارد (در حال حاضر ۳ زیرکلاس تعریف شده است). هر کلاس فورواردینگ در داخل این گروه به طور مستقل برای منابعی مانند فضای بافر و حداقل ظرفیت خروجی که باید به وسیله‌ی مکانیزم زمان‌بندی تضمین شود، پیکربندی می‌شود.

- Default Behavior(DE)

DE PHB ترافیک موجود best effort را مشخص و رفتاری تعریف می‌کند که گره، هر تعدادی از این بسته‌ها را که امکان داشته باشد در کوتاه‌ترین زمان ممکن تحویل دهد.

www.prozhe.com

www.prozhe.com

۲-٦ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش سوم)

۲-٦-۱ MPLS

برای سرویس های QoS در یک شبکه IP، می‌توان از معماری سرویس‌های مجتمع و سرویس‌های متمایز استفاده کرد. اما به دلیل استفاده از برچسب‌ها درMPLS، برای کار کردن بر روی یک معماری MPLS، به ایجاد تغییراتی نیاز است. برای ایجاد این تغییرات سه روش به IETF پیشنهاد شده است:

۲-٦-۲ .سرویس‌های مجتمع در حوزه‌های MPLS با استفاده از سیگنالینگ CR-LDP

یکی از پی‌آمدهای مهم مسایل قابلیت گسترش در IntServ این است که QoS در سطح IntServ فقط می‌تواند در بین نواحی جانبی شبکه ایجاد شود. این وضعیت باعث جلوگیری از توسعه‌ی آن به داخل نواحی مرکزی و پیاده سازی QoS انتها به انتها می‌شود. استفاده از پروتکل MPLS در شبکه‌ی مرکزی بعضی از مسایل مربوط به scalability را حذف می‌کند و باپروتکل CD-LDP مسیرهایی به نام LSP یا Lable Switched Path تعریف می‌شوند که دارای محدودیت های QoS هستند و کلاس‌بندی QoS را با استفاده از حوزه های MPLS و نواحیIntServ ایجاد می‌کنند. بدین منظور، LSR ورودی MPLS مانند یک gateway دارای کیفیت سرویس MPLS/IntServ عمل می‌کند. بعد از پذیرش یک پیغام RSVP که منابع را رزرو می‌کند،LSR ورودی، یک LSR مسیریابی شده به طرف LSRهای خروجی برقرار می‌کند. مقادیر پارامترهای ترافیکی (مانند پارامترهای QoS) از پیغام‌های resv مربوط استخراج می شود. ترافیک فرستنده RSVP حوزه‌ی MPLS با استفاده از این مسیر CR-LSP عبور می‌کند. LSRهایی که در کناره‌ی حوزه‌های MPLS نیستند، تنها پیغام‌های CR-LDP را پردازش می‌کنند. اگرچه این روش می¬تواند تا حدی مشکل scalability را حل کند، برای همکاری بهتر روش سرویس متمایز با MPLS به نظر می¬رسد که تغییرات بیش¬تری در شبکه¬ی هسته موردنیاز است.

www.prozhe.com

www.prozhe.com

۲-٦-۳. MPLS و DiffServ

ممکن است لازم باشد یک LSP به دلیل ارتباط با خواص کیفیت یک سرویس خاص، بـه وسـیله¬ی مکانیزم¬های QoS در داخل LSRها از طریق ابزاری غیر از MPLS اجرا شود. نیازمندی اصـلیMPLS برای پشتیبانی از DiffServ این است که تضمین کند بسته‌ها رفتار QoS مناسـب خـود را بـه وسـیله هـر LSR داخل شبکه دریافت می‌کنند.

۲-٦-٤. QoS در MPLS VPNها

VPNهای سنتی که بر مبنای فنـاوری‌هـای لایـه ۲ یـا خطـوط اجـاره‌ای (leased line) هسـتند، بـه صورت تضمین شده، پایین‌ترین سطح کیفیت سرویسی را که به وسـیله پارامترهـایی ماننـدCIR (در مـورد Frame Relay)، CBR و SCR (در موردATM) یا پهنای باند مدار (در مورد خطـوط اجـاره‌ای) بیـان می شوند، عرضه می کنند. البته در مورد VPNهای MPLS نیز کاربران باید تضـمین‌هـای مشـابهی بـرای QoS داشته باشند.

دو مسیر اصلی کنترل QoS در VPNهای MPLS وجود دارد- مدل pipe و مدل hose:

مدل hose بر مبنای دو پارامترICR (Ingress Committed Rate) و ECR (Egress Committed Reate) است که برای هر رابط CE/PE تعریف می‌شوند. این دو پـارامتر، ترافیکی را که هر روتر CE (طرف مشتری) می‌تواند به سایت‌های VPN دیگر انتقال دهد یا از سایت‌هـای VPN دیگر دریافت کند، مشخص می‌کنند.

شکل ٤ مثالی را از مدل hose نشان می‌دهد.که در این مورد روتر CE که به سایت ۱ متصل است مـی تواند تا ۵۱۲ kbit/s را از سایت‌های دیگر همان VPN دریافت کند و تا ۲۵٦ kbit/s را انتقال دهـد. بایـد توجه شود که این مقادیر وابسته به توزیع ترافیک در بین سایت‌های remote هستند. برای مثال به سایت ۱ اجازه داده می‌شود که اگر در همان زمان در حال ارسال هیچ ترافیکی به سـایت ۳ نباشـد، ۲۵٦kbit/s را در یک فاصله زمانی مشخص به سایت ۲ بفرستد.

www.prozhe.com

www.prozhe.com

کنترل QoS در هسته MPLS ممکن است به وسیله‌ی DiffServ صورت گیرد. در این مورد مدل مبنای hose می‌تواند به طور جداگانه برای هر کلاس سرویسی به کار برده شود. از دیدگاه مشتری یکی از فواید مدل hose این است که نیاز به دانستن جزییات توزیع ترافیک بین سایت‌های VPN ندارد. این ویژگی پیاده‌سازی این روش را آسان می‌کند.

مدل دیگر، مدل pipeاست که شامل تدارک برای تضمین QoS، برای مثال کمینه‌ی پهنای باند، بین هر جفت از روتر های CE است. LSPهای دارای پهنای باند تضمین شده بین PEها که درMPLS مورد استفاده قرار می‌گیرند، می‌توانند برای پشتیبانی از مدل pipe استفاده شوند.

مدل pipe روش QoS پایه‌ای را که در VPNهای ATM یا Frame Relay سنتی استفاده می شود، در خود دارد. (جدا از این واقعیت که مدل pipe یک طرفه است در حالی که در ATM یا Frame Relay ارتباط در حالت عادی دو طرفه تعریف می شود.)

در مثالی که در شکل ۵ نشان داده شده است، دو ارتباط سایت‌های "۳ و"۱ و سایت‌های "۳ و ۲" به ترتیب دارای پهنای باند ۵ Mbit/s و ۷ Mbit/s هستند.

مدل pipe می‌تواند به تعدادی از کلاس‌های سرویس اعمال شود.

از آن‌جا که یک راه‌حل واحد که دربرگیرنده و برطرف‌کننده‌ی همه‌ی نیازها باشد، وجود ندارد، در عمل پیاده‌سازی‌هایی که به صورت ترکیبی از دو مدل هستند، می‌توانند مناسب‌ترین راه‌حل باشند.

۲-۷ مدیریت IPVPN ها

در این بخش ابتدا بر مبنای آخرین نسخه‌ی سندIETF، توان‌مندی‌های کارکردی که به علاوه جزیی از سرویس‌های پشتیبانی مدیریتی برای تدارک IPVPN به شمار می‌آیند، تشریح می‌شود و سپس مطابق مفهوم TMNمروری بر جنبه‌های مدیریتی مربوط به آن، خواهد شد. در انتها بر مبنای ویرایش‌های تازه توسعه یافته‌ی مدل مدیریتی و QoS، چارچوب در بر گیرنده‌ی IP و معماری مدیریتی مخصوص VPN نشان داده می‌شود.

www.prozhe.com

www.prozhe.com

۲-۸ نیازمندیهای مدیریت QoS

از آن‌جایی که VPNها به طور معمول اتصالات شبکه‌ی خصوصی امنی هستند که در روی یک زیرساخت قابل دسترس عمومی مانند اینترنت یا شبکه‌ی تلفن عمومی ایجاد می‌شوند، به طور ایده آل یک VPN باید شبیه یک شبکه‌ی خصوصی رفتار کند؛ یعنی امن باشد، در دست‌رس باشد و نیز کارایی قابل پیش بینی داشته باشد. به طور معمول بر طبق مدل TMN، رفتار جداگانه‌ای برای جنبه‌های مدیریتی شبکه و جنبه‌های کنترلی آن در نظر گرفته می‌شود.

توابع مدیریتی اغلب به صورت یک لایه‌ی پوششی که عملیات مخصوص FCAPS را انجام می‌دهند، پیاده‌سازی می‌شوند. امروزه این جداسازی واضح بین سطح کنترلی و سطح مدیریتی چندان آشکار نیست. انواع مخصوصی از مدیریت شبکه تا کنون در پروتکل ها (لایه بالا) به صورت نهفته قرار گرفته‌اند و روند و خط سیر به سمت سرمایه‌گذاری بسیار بیش‌تری در مدیریت خدمات و توسعه‌ی مکانیزم‌های مدیریتی سطح بالا برای خودکار کردن زیربرنامه‌های خاص مدیریتی و کاهش زمان تحویل تا حد امکان در حرکت است.

یکی از موضوعات کلیدی برای موفقیت یک راه‌حل VPN، مساله کیفیت سرویس– QoS است. ترکیب VPN همراه QoS منجر به محصولاتی با قابلیت رقابتی بالا می‌شود. بنابراین هم VPN و هم QoS باید با یک روش مجتمع مدیریت شوند. بدون توجه به اینکه چه معماریی برای VPN انتخاب می شود یا چه فناوری، QoS را پشتیبانی می‌کند. سرویس‌های IPVPN فرصت خوبی را برای تهیه‌کنندگان خدمات فراهم می‌کنند تا منافع جدید و بیش‌تری را دریافت کنند. تامین کتندگانی که بتوانند سرویس‌های IPVPN قابل مدیریت و به سرعت قابل گسترشی را عرضه کنند، سود رقابتی را به دست می‌آورند. کلید موفقیت و سودبخشی نهایی خدمات IPVPN را می‌توان به طور ساده در فناوری فراهم شده جست‌وجو کرد. مدیریت‌پذیری سرویس و مدیریت کل دوره‌ی زمانی؛ یعنی برنامه‌ریزی (planning)، تدارک (provisioning)، مانیتورینگ، عملیات (operation) و صورت‌حساب (billing)؛ هر دو مهم هستند.

مدیریت سرویس به مدیریت زیر ساخت شبکه ای که در زیر آن قرار گرفته و تدارک و تهیه رابط‌هایی برای داده‌ها و مکانیزم‌هایی که فرایند کلی تجاری provider را پیش ببرند بستگی دارد. تهیه‌کنندگان

www.prozhe.com

www.prozhe.com

سرویس، دیگر، روی قیمت با یکدیگر رقابت نمی‌کنند بلکه بر روی زمان تحویل سرویس رقابت می‌کنند. بنابراین کلید گسترش سودآور سرویس VPN، مدیریت است.

۲-۹- قابلیتهای عمومی مدیریت QoS برای تدارک IPVPN

۱. پشتیبانی از نیازمندی‌های گوناگون ترافیک (QoS) کاربر آن گونه که کاربر تعریف می‌کند.

۲. ارائه، پشتیبانی و نگه‌داری سطوح توافق شده‌ی سرویس (برای مثال پیکربندی، خرابی، کارایی، امنیت و...)

۳. هر FCAPS ی باید با SLA مقایسه شود و هر تخطی از QoS و SLA باید به طور خودکار کشف شود . تدارک و تهیه‌ی اطلاعات کارایی، آمارها و غیره ؛ یعنی فعال کردن مکانیزم‌های مانیتورینگ و اندازه گیری‌های مناسب نیازمندی‌های QoS و SLA؛ تحلیل اطلاعات (برای مثال پهنای باند، زمان پاسخ، فراهم بودن، تلفات بسته و غیره)، پیش بینی روند آینده، حتا مسایل و یا توصیه‌هایی در ارتباط با SLA های جاری، الگوی ترافیکی، QoS و غیره.

۲-۱۰ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش چهارم)

۲-۱۰-۱ مدیریت QoS برای توافقات سطح سرویس (SLA)

برخی از قابلیت‌های مدیریتی باید در SLAها قرار گیرند و برای هر VPN، هر سایت VPN و یا هر مسیر VPN فرمول‌بندی شوند. مدیریت SLA باید بر مبنای موارد زیر باشد:

- اهداف سطح خدمات که از بعضی یا همه موارد مقابل تشکیل می شود:قابلیت انتقال IP، پارامترهای QoS، در دست‌رس بودن، مطمئن بودن، تثبیت و تایید تحویل، پشتیبانی پویا و قابلیت حمل ونقل، امنیت، پهنای باند، اولویت ها، تشخیص هویت، پروتکل های پشتیبانی شده، گسترش انعطاف‌پذیری و متصل بودن و مدت زمان SLA.

www.prozhe.com

www.prozhe.com

- اهداف مانیتورینگ سرویس: مانیتورینگ QoS با در نظر گرفتن اهداف، ردیابی جریان، تهیه و ارایه گزارش‌های موردنیاز، اهداف سود و زیان مالی، گزینش صورت‌حساب، جریمه‌ها، قیمت‌گذاری و هزینه های خاتمه‌ی زود هنگام سرویس.

مدیریت QoS کمک می‌کند تا ترافیک بحرانی، کارایی قابل قبولی داشته باشد.

۲-۱۱ خصوصیات مدیریت QoS برای پیاده سازی

کاربران به طور عادی توجهی به مکان‌شناسی شبکه یا سطح بالای امنیت و یا حتا فناوری خاص یا پروتکل ی که VPN مورد استفاده‌ی آن‌ها را پشتیبانی می‌کند، ندارند. آن‌ها به طور معمول درباره‌ی زمان پاسخ مورد قبول در دست‌رسی به یک سایت راه دور و کیفیت مورد نظر در زمانی که از سرویس‌ها استفاده می‌کنند، توجه دارند.

تهیه‌کنندگان سرویس باید بتوانند SLAهای انتها به انتها و QoS تضمین شده تحویل دهند. تهیه کنندگان سرویس ممکن است مایل باشند سرویس‌های پردازش را که به وسیله SLAها تعریف شده‌اند، به عنوان بخشی از VPNهای‌خود، ارایه دهند. QoS در شبکه‌های IP به دستگاه‌ها این هوشمندی را می‌دهد که در ابتدا به ترافیکی رسیدگی کنند که با سیاست شبکه مطابقت دارد.

ویژگی‌های مورد نیاز مدیریتی بر طبق جداسازی سطح سرویس و سطح شبکه، به دو گروه تقسیم می شوند:

در سطح سرویس، applicationهای مدیریت QoS، باید حداقل کارکردهای زیر را فراهم کنند (روش‌های مدیریت QoS):

- تدارک خودکار سرویسVPN: بر طبق تقاضای مشتریان، درخواست‌های اتصال باید به سرعت و به طور کامل برآورده وQoS باید تضمین شود. ابزارهای مدیریت QoS باید دارای راه‌حل‌هایی باشند که اجازه دهند VPNها ایجاد شوند، دارای پشتیبانی از انتخاب‌های مختلف برای کلاس‌های سرویس (COS) باشند، SLA خاص VPN را تدارک ببینند، دارای گزارش‌های کارایی باشند و...

www.prozhe.com

www.prozhe.com

- مانیتورینگ کارایی: گرفتن اطلاعات ترافیکی از شبکه‌و جمع‌آوری آن از جهات گوناگون و در فواصل زمانی مختلف و تعریف چگونگی نگاشت اندازه‌گیری‌های QoS به پارامترهای کارایی سطح سرویس به طوری که بتواند برای مشتری ارایه شود، باید امکان‌پذیر باشد. ویژگی‌های SLA، مانند تاخیر، در دست‌رس بودن، بازدهی و jitter باید در سطوح مختلف مانیتور و جمع‌آوری شود.
- مدیریت سرویس مشتری: مشتری‌ها باید با خدمات مدیریتی مانند: تدارک و فراهم‌آوری خودکار، سرویس‌های پیکربندی QoS، گزارش‌های زمان‌بندی شده از پیروی SLA و غیره آشنا شوند.

در سطح شبکه روش‌های مدیریت QoS زیر باید مورد توجه قرار گیرند:

- کلاس‌بندی بسته‌ها- به گروه‌بندی بسته‌ها بر طبق ضوابط از پیش تعریف شده کمک می‌کند، به طوری که گروه‌های به دست آمده از بسته‌ها می‌توانند، برای داشتن رفتارهای مشخص با بسته های هر گروه به کار روند. ضوابط کلاس بندی ترافیک قبل و بعد از وارد شدن به VPN می‌تواند آدرس‌های IP، URL، آدرس‌های MAC، شماره‌ی پورت TCP/UDP، حق تقدم IP یا نوبت‌دهی در زمان باشد.
- علامت‌گذاری رنگ‌بندی بسته- بعد از کلاس‌بندی، بسته‌ها باید با یک Id یکسان (با استفاده از فیلد TOS در IP، DSCP و غیره)، علامت‌گذاری شوند تا اطمینان حاصل شود که کلاس‌بندی به صورت انتها به انتها در نظر گرفته شده است.
- مدیریت پهنای باند- بعد از کلاس‌بندی ترافیک، باید دریافت رفتار صحیح به وسیله آن از جهت زمان بندی و صف‌بندی در روتر ها تضمین شود.
- Traffic Shaping- این روش برای صاف کردن و مرتب کردن جریان‌های ترافیک استفاده می‌شود. Tocken Bucket Shaper می‌تواند برای جلوگیری از ترافیک burst و نیز جلوگیری ازpeakهای ترافیکی به جای استفاده از مشخصات روتر های PE، استفاده شود، هم‌چنین دستگاه‌های shaper ممکن است به ازای هر سایت بین CE و PE به وسیله مشتریان پیاده‌سازی شوند.

www.prozhe.com

www.prozhe.com

- جلوگیری از ازدحام- shaping در هر مورد ممکن است باعث ایجاد صف‌های طولانی در روتر های کناری شود، بنابراین جلوگیری از ورود یا drop کردن بسته‌ها از جریان‌های تولید شده به وسیله‌ی کاربردهای غیرحساس می‌تواند از ازدحام زیاد در شرایط بارهای زیاد جلوگیری کند.

۲-۱۲ مفاهیم مدیریتی کاربردی و مدل های پیش‌نهادی

در اثبات تحویل مناسب و مدیریت شده‌ی خدمات VPN، موضوعات اساسی مورد توجه اپراتورهای شبکه و تولیدکنندگان خدمات به شرح زیر است:

I. برای پیاده‌سازی ابزارهای اندازه‌گیری مقدار مصرف؛ اندازه گیری‌های کارایی مصرف منابع و اندازه گیری انواع نقاط دست‌رسی قابل اندازه‌گیری، رابط‌هایی که به دست آوردن داده‌های مربوط را از نتایج اندازه‌گیری امکان‌پذیر می‌کنند.

II. برای انتخاب و پیاده‌سازی در گرفتن داده‌ها؛ مدیریت، مستندسازی، ابزارهای رسیدگی به داده‌ها، قوانین و راه‌حل‌ها، منابع مورد نیاز و جنبه‌هایی که رسیدگی به داده‌ها و قابلیت‌های ذخیره‌سازی و هم‌چنین تبدیلات داده‌ها و ابزارهای پردازش داده‌ها را می‌پوشانند، باید یک MIB استاندارد به کار برده شود و سیستم‌های پایگاه داده‌ی پشتیبان عملیات و مدیریت باید به صورت مجتمع وجود داشته باشد.

III. برای عرضه مدیریت خرابی که وابسته به عنصر شبکه است، برای پیاده سازی ثبت رخدادها و قابلیت‌های مانیتور کردن وضعیت، علاوه بر سطوح alarm قابل انتخاب برای سیگنال زدن نشانه‌ی alarm، مجتمع‌سازی گزارش‌دهی خرابی و فرآیندها و سیستم‌های trouble ticket پیش‌نهاد می‌شود.

IV. برای پشتیبانی از اتوماسیون در مدیریت پیکربندی، مدل تحویل سرویس IPVPN بر مبنای مفهوم تهیه‌کننده‌ی اصلی پیش‌نهاد می‌شود. عملیات زیر می‌تواند بر مبنای این مدل انجام شود:

- مذاکرات در مورد مکان‌شناسی سایت و پیش‌بینی ترافیک مربوط (ظرفیت و نوع payloadی که قرار است انتقال یابد) و تغییرات بر حسب تقاضا در رزرو منابع.

www.prozhe.com

www.prozhe.com

- توجه به مشتری و در نظر گرفتن رابط‌هایی برای رسیدگی به دستورات سیستم پشتیبانی از زمان تحویل سرویس، به صورت مجتمع.

V.برای به کار بردن مناسب ابزارهای انتخاب شده مانیتورینگ کارایی، راه‌حل‌های استاندارد اندازه گیری، و طرح‌های ارزیابی‌کننده در مدیریت کارایی. پارامترها، ضوابط اندازه‌گیری و اهداف باید از SLAهای محصولات معمول و مورد توافق گروههای کاربری مربوط انتخاب شوند. افزون بر این ارزیابی آماری نیز مورد نیاز است.

VI. برای پیاده‌سازی سیستم‌های پشتیبانی استاندارد، که برای اهداف تشخیص هویت، حدود و اختیارات و مدیریت حساب‌رسی به کار برده می‌شوند. برای به کاربردن معماری بر مبنای امنیت، برای پیاده سازی قابلیت‌های ایجاد بازرسی‌های امنیتی.

بر طبق استاندارد IETF سه گزینه برای گسترش سیستم‌های مدیریت VPN و سیستم‌های پشتیبانی QoS برای تحویل سرویس VPN وجود دارد:

- استفاده از یک مدل call-centre برای کنترل مشتری
- گسترش سیستم‌های مدیریتی سفارشی و اغلب اختصاصی و کنترل سیستم‌ها، مانیتور کردن راه‌حل‌های پیاده‌سازی برای مدیریت backbone شبکه‌ی IPVPN و تحویل سرویس VPN.
- برای پیاده سازی استاندارد و نیز راه‌حل‌های مدیریت VPN بر مبنای سیاست.

مدیریت بر مبنای سیاست با استفاده از یک معماری عملیاتی لایه‌ای

مدل معماری QoS بر مبنای سیاست در استاندارد IETF شامل چهار گزینه‌ی کارکردی است: پیکربندی، عنصر شبکه، موتور سیاست و حساب‌رسی. با این روش، فرآیندهای مدیریتی انعطاف‌پذیر و توسعه‌پذیر پیاده‌سازی می‌شوند که با یکدیگر می توانند از هزینه‌ی QoS و هزینه‌های مبتنی بر میزان استفاده، پشتیبانی کنند.

www.prozhe.com

www.prozhe.com

این معماری یک ارایه عملی را در زمان واقعی از دیدگاه‌های مختلف، عرضه می دارد. این دیدگاه‌ها می‌تواند مبتنی بر مشتریان، فیلتر کردن داده‌های مدیریتی به ازای هر VPN و یا حساب‌رسی نیازمندی‌های مورد نیاز امنیتی باشد.

در این معماری نقاط اعمال سیاست (Policy Enforcement Points-PEP) مسوول عرضه‌ی کنترل بر مبنای سیاست به وسیله پیاده‌سازی سیاست و فرآیند اندازه‌گیری در لایه‌ی NE و سپس اعمال کنترل به مدیریت عنصر (Element Management-EM) است، در حالی که سیاست به وسیله لایه‌ی مدیریت شبکه انتخاب و پیاده‌سازی می‌شود.

بر مبنای سیاست کیفیت خدمات NMS/OSS، قابلیت‌های مدیریت SLA و هزینه‌ی QoS نیز ممکن است پیاده سازی شوند (در این شکل لایه‌ی مدیریت سرویس/تجاری که در بالای لایه مدیریت شبکه قرار دارد، نشان داده نشده است).

وقتی که یک provider اصلی وجود دارد که دارای سیستم‌ها و راه‌حل‌های مختلف دست‌رسی برای تهیه و تدارک شبکه و هم‌چنین یک شبکه‌ی مرکزی و یک backboneIP است، به طور خاص می‌توان از این مدل استفاده کرد.

۲-۱۳ SLA مجتمع شده ومدیریت اطلاعات QoS

برای این‌که بتوانیم به طور واقعی مدیریت مجتمع SLA را انجام دهیم، لازم است در همه‌ی سرویس های وابسته و اطلاعات مشتریان، یک مدیریت موثر داشته باشیم. توابع مدیریت SLAباید گستره‌ی وسیعی از منابع داده را ترکیب کنند، وابستگی آن‌ها را پیدا و در نهایت ارزیابی و مدیریت کنند تا بتوانند به گونه‌ای موثر برآورده شدن SLAها را مدیریت و ضمانت کنند.

www.prozhe.com

www.prozhe.com

۲-۱٤ جداسازی مدیریت در شبکه سرویس‌های VPN و شبکه انتقال VPN

تا کنون لایه‌های جداسازی شده شبکه‌ی سرویس‌ها و شبکه‌ی انتقال به وسیله‌ی ITU-T که سرویس های IP و چارچوب پشتیبانی از IPVPN را گسترش دادند، معرفی شده‌اند. این مفهوم لایه‌ای به عنوان یک روش بنیادین برای مدل مدیریت شبکه و QoS شناخته می‌شود.

با این مفهوم مدیریت شبکه (و QoS)، اندازه‌گیری‌های کارایی، توابع تولید آلارم و مانیتور کردن، می توانند بر مبنای اهداف پارامتری دارای انتخاب، اندازه‌گیری‌های استاندارد موجود و ابزارهای مدیریتی موجود باشند. نقاط مرجع که رابط‌های مدیریتی پیاده‌سازی شده برای توابع گوناگون هستند، باید برای مانیتور کردن و اندازه‌گیری‌های QoS، تبادل اطلاعات QoS و فعل وانفعالات اجزای مختلف به کار برده شوند. سیستم‌های مدیریت QoS و نقاط مرجع قرار است به طور خاص برای انواع مختلف ترافیک انتها به انتها و برای ویژگی‌های ارتباطی VPNها طراحی شوند.

۲-۱۵ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش پنجم)

ایجاد چارچوبی برای مانیتورکردن نهفته‌ی پارامترهای کیفیت خدمات در شبکه‌های خصوصی مجازی مبتنی بر پروتکل اینترنت در این بخش به طور مختصر یک چار چوب برای مانیتور کردن نهفته‌ی کارایی پارامترهای QoS در شبکه‌های IP و به طور خاص در شبکه‌های خصوصی مجازی ارایه می‌شود.

فعالیت‌های اندازه‌گیری باید تابع سیاست‌های اپراتور و اهداف مدیریت کارایی باشند، که آن‌ها نیز به توافقات سطح سرویس (SLA) و نیازهای عملیاتی وابسته هستند و دلیلی برای انجام مانیتورینگ گسترده‌ی کارایی به خودی خود، وجود ندارد.

معماری پیش‌نهاد شده مبتنی بر یک روش in-service است که در بخش‌های بعدی مفهوم آن توضیح داده خواهد شد. در این روش پارامترهای ترافیکی کاربر به وسیله مانیتورینگ اختصاصی اندازه گیری می شوند. توابع مانیتورینگ، یک بخش مجتمع از عناصر عادی شبکه را تشکیل می‌دهند. شبیه‌سازی‌هایی که

www.prozhe.com

www.prozhe.com

مبتنی بر ثبت مسیر ترافیک تست با استفاده از ردیابی هستند، نتایج امکان‌پذیر را در استفاده از این مدل نشان می‌دهند. در انتهای این بخش بعضی از نتایج پیاده‌سازی توصیف خواهد شد.

اپراتورهای مخابرات تمایل دارند که خدماتی از مخابرات در شبکه‌های IP ایجاد کنند، که نیازمندی های کیفیت خدمات را به طور جدی برآورده سازند. در نتیجه یک اپراتور باید به ابزار کارآمدی برای مانیتورینگ و کنترل پارامترهای کارایی مربوط دست‌رسی داشته باشد. به علاوه داشتن دانش کافی درباره رفتار شبکه برای اهداف عملیاتی، بازبینی و تحقیق درباره برآورده شدن توافقات سطح خدمات، بسیار حیاتی و مهم است. تا کنون در شبکه‌های تلفنی سنتی از روش ایجاد دامنه‌های خصوصی منطقی استفاده شده است. اما از آن‌جایی کهپروتکل اینترنت امروزه در همه جا، از جمله مخابات عمومی، حاضر است، شبکه‌های خصوصی مجازی مبتنی بر IP به عنوان یک روش مهم برای تهیه‌ی خدمات مخابراتی معتبر و ایمن مورد ملاحظه قرار گرفته‌اند.

به طور کلی روش‌های اندازه گیری و مانیتور کردن پارامترهای کارایی شبکه به دو دسته تقسیم می شوند:

۱- روش‌های پسیو مانندsnifferهای متداول و وسایل اندازه‌گیری ترافیک

۲- روش‌های اکتیو که درآن بسته‌های مخصوص کنترل یا تست تولید می‌شوند. (مانند(ping در روش‌های پسیو، به منظور ذخیره‌سازی و جمع آوری اطلاعات، بسته‌ها به ترتیب از فیلدهای مختلف هدر بسته، دریافت می‌شوند. snifferهای متداول، تحلیل‌گرهای پروتکل و وسایل اندازه‌گیری ترافیک همگی بر این اصل بنا شده‌اند (مانند RMON Probes,NetFlow,NetraMet,ntop,tcpdump). بر خلاف روش‌های اکتیو، مانیتورهای پسیو بار ترافیکی اضافی به شبکه تحمیل نمی‌کنند. گذشته از این ویژگی non-intrusive بودن، روش‌های پسیو را قادر به جمع‌آوری اطلاعات جزیی فراوان می‌کند. افزون بر این ثبت و نوشتن تاریخچه از ردپای بسته‌ها در شبکه‌های با سرعت بالا بیش‌تر به مقدمات مخصوصی برای جمع‌آوری، ذخیره و پردازش حجم زیادی از داده‌ها نیاز دارد. در عوض روش‌های اکتیو بر مبنای

www.prozhe.com

www.prozhe.com

تزریق بسته‌های probe با استفاده از ICMP عمل می‌کنند.مثال‌هایی از ابزارهـای مبتنـی بـر روش‌هـای اکتیو عبارت‌اند از: PingER، Active Measurement Project(AMP)، National Internet Measurement Infrastructure، surveyor و RIPE's test traffic project.

یک روش گسترش یافته که در طبقه}بندی قبلی نمی گنجد استفاده از پروتکل مدیریتی SNMP برای بازیابی اطلاعات از MIBهای عناصر شـبکه اسـت. بسـیاری از ابزارهـا ماننـد MultiRouter Traffic Grapher بر مبنای رای‌گیری (polling) از شمارنده‌های ترافیک در MIBهای روتر هاست.RMON که گامی به سوی مانیتورینگ توزیع شده به شمار می‌آید، به صورت یکMIB سازمان‌دهی شده است. بنابراین یک مدیر می‌تواند با استفاده از SNMP، اطلاعات ترافیکی را از Probeها به دست آورد.

روش‌های مانیتورینگ کارایی همچنین به دو گروه in-service یا out-of-service تقسیم‌بندی مـی شوند. روش‌های out-of-service فقط به ترافیک تستی که به طور خاص تولید شـده اسـت، اعمـال مـی شوند، درحالی که هدف از روش‌های in-service مانیتور کردن ترافیک واقعی کاربر است: مانیتورینگ in-service ممکن است با استفاده از روش‌های مختلف اکتیو یا روش‌های پسیو غیرمداخلانه انجـام شـود. در دنباله‌ی این مقاله تمرکز اصلی بر روی مانیتورینگ in-service خواهد بود و مدلی برای مانیتور کردن بسته هایی که به منظور برآورد پارامترهای کارایی به ترافیک کاربر اضافه شده اند، پیش‌نهاد می‌شود. این بسته‌های مانیتورینگ اختصاصی که حامـل اطلاعـات OAM(Operation,Administration, Maintenance) هستند. ممکن است به عنوان یک روش in-service اکتیو مورد توجه قرار گیرند.

ITU-T سلول‌های OAM را برای مانیتورینگ کارایی و خرابی در شبکه‌های ATM، استاندارد کرده است. اما بر خلاف ATM، IP یک پروتکل بدون اتصال با طول بسته متغیر است که به احتمـال زیـاد مهـم ترین دلیل برای ناچیز بودن پروتکل های مشابه در دنیای IP است.

www.prozhe.com

www.prozhe.com

فصل سوم

www.prozhe.com

www.prozhe.com

۳- مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP)

معماری ایده‌ی اصلی، توسعه‌ی یک ساختار مناسب برای مانیتور کردن پارامترهای کارایی شبکه در شبکه‌های IP است. بعضی معتقدند که اندازه‌گیری‌ها و توابع مانیتورینگ باید مطابق با سیاست اپراتور و اهداف مدیریت کارایی محاسبه و با نوع سرویس عر ضه شده، تنظیم شود. یک اپراتور شبکه افزون بر آگاهی از رفتار شبکه، باید به مانیتور کردن توافقات سطح سرویس (SLA)ها و کیفیت سرویس اشراف کامل داشته باشد. این مهارتها به وسیله‌ی سیستمهای مدیریت شبکه‌ی مبتنی بر مشتری پشتیبانی می‌شود. به علاوه، یک سیستم مانیتورینگ قدرتمند که بتواند کارایی وا قعی شبکه را منعکس کند، باید قادر به ایجاد توابع تخصیص ظرفیت پویا باشد.

در این مقاله IPVPNها را به عنوان مبنای مطالعه انتخاب شده‌اند. همان‌طور که در شکل ۷ دیده می شود، در مکان‌شناسی فرض شده، یک شبکه‌ی هسته، به وسیله‌ی گره‌های کناریprovider و گره‌های کناری مشتری احاطه شده است. شبکه‌های خصوصی مجازی می‌توانند به روش‌های مختلف پیاده‌سازی شوند. شبکه‌های مبتنی بر روتر که "تونل" نامیده می‌شوند، به وسیله اتصالات نقطه به نقطه‌ی روی هم قرار گرفته، ایجاد می‌شوند. با استفاده از کپسوله کردن مسیر کلی یا IPSec، MPLS وعده می‌دهد که چارچوب انعطاف‌پذیرتر و توسعه‌پذیرتری را برای VPNهای مبتنی بر سوییچ‌های سلولی، یا محیطی ترکیب شده از روتر ها و سوییچ¬ها ایجاد کند.

۳-۱ مانیتورکردن برمبنای سیاست

در روش نهفته که در ادامه با جزییات بیشتری تشریح خواهد شد، گرههای مانیتورینگ باید بتوانند به طور دینامیک و خودکار، مطابق سیاستها و کمکهای اپراتور پیکربندی شوند. شبکه‌هایی که دارای راهنمای سرویس هستند، یک معماری توافقی و عملی برای پیاده‌سازی مانیتورینگ کارایی بر مبنای سیاست دارند. یک اپراتور باید بتواند درباره‌ی زمان، چگونگی و محل قرارگیری توابع مانیتورینگ در شبکه، تصمیم‌گیری کند. از آنجا که چندین شبکه‌ی منطقی، کلاس¬های سرویس مختلف، پارامترهای گوناگون و مقادیر زیادی

www.prozhe.com

www.prozhe.com

از عناصر شبکه در این تصمیم‌گیری قرار می‌گیرند، رابط مدیریتی در این محیط پیچیده، باید بر حسب سیاست‌های مختلف مانیتورینگ بیان شود، این در حالی است که جزییات سطح پایین، پوشیده هستند.

۳-۲ بسته های OAM نهفته

هدف از مانیتورینگ نهفته، اندازه‌گیری پارامترهای کارایی شبکه بر مبنای ترافیک واقعی کاربر است. این بسته‌های مانیتورینگ اختصاص داده شده یا همان بسته‌های OAM، بین بلاک‌های بسته‌ی داده‌های معمولی جای داده می‌شوند. گره فرستنده بسته‌های مانیتورینگی تولید می کند که اطلاعات مانیتورینگ را بین هر N بسته‌ی کاربر، به طور متوسط، حمل می‌کند. گره گیرنده بسته‌های مانیتورینگ را کشف و اطلاعات را اضافه می کند. سپس آن‌ها را به گره مبدا برمی‌گرداند. پردازش، ذخیره‌سازی و تحلیل ممکن است به وسیله‌ی سرورهای اختصاصی برای کل شبکه صورت گیرد. هم‌زمان‌سازی کلاک‌ها در گره‌های مانیتورینگ، برای اندازه‌گیری تاخیر یک طرفه، برای مثال می‌تواند به وسیله‌ی سیستم موقعیت‌یابGPS و پروتکل زمانی شبکه (NTP) صورت گیرد. با استفاده از این روش می‌توان نتایج زیر را به دست آورد:

- تعداد بسته‌های گم شده بین گره‌های گیرنده و فرستنده و نرخ گم شدن بسته‌ها در طول دوره‌ی اندازه گیری
- طول پریودهای بدون loss و پریودهای loss که بر حسب تعداد بلاک‌های OAM پشت سرهم – شامل بسته های گم شده و تعداد بلاک های OAM که بدون loss – بیان شده است.
- نمونه‌هایی از تاخیر انتقال و تغییرات تاخیر، بین گره‌های فرستنده و گیرنده.
- برآوردی از ظرفیت استفاده شده (throughput) بین هر جفت از گره‌های کناری فرستنده –گیرنده. برای این کار باید طول متوسط بسته را به دست آورد.

یک قالب از بسته‌های OAM پیش‌نهادی در شکل ۸ نشان داده شده است. هِدِر IP معمولی بسته‌های OAM شامل نشانی مقصد گره گیرنده (خروجی) و نشانی مبدا گره فرستنده (ورودی) است. یک شماره، ترتیب بسته‌های OAM گم شده را کشف می‌کند. گره ورودی تعداد کلی بسته‌های فرستاده شده (به طور

www.prozhe.com

www.prozhe.com

تجمعی) و زمان جاری را در مکان‌های مربوط می‌نویسد. گره خروجی تعداد کلی بسته‌های دریافتی (به طور تجمعی) و زمان جاری را در مکان‌های هدر مربوط قرار می‌دهد.

An OAM block consisting of N packets

۳-۳ نیازمندی‌های شبکه‌های بدون اتصال

مانیتورینگ کارایی در شبکه‌های مبتنی بر پروتکل های بدون اتصال مانند IP اهمیت زیادی دارد. در پروتکل های اتصال‌گرا مانند ATM، هر بسته یا سلول وابسته به یک اتصال منطقی در یک مسیر از پیش تعیین شده قرار می‌گیرد. یک دیتاگرام IP فقط آدرس‌های شبکه‌ی مبدا و مقصد را حمل می‌کند و هیچ تضمینی وجود ندارد که هر دیتاگرام در یک session همان مسیر را از فرستنده به گیرنده طی کند و به همان ترتیب اولیه برسد. در مقایسه با ATM یک تفاوت دیگر این است که IP اجازه می‌دهد بسته‌ها طول متغیر داشته باشند. به همین دلیل باید هنگام برآورد، نرخ‌های انتقال و نرخ گم شدن بسته‌ها مورد توجه قرار گیرد.

در نتیجه در به کاربردن بسته‌های OAM برای نظارت بر پارامترهای کارایی در شبکه‌های IP یک گره ورودی (فرستنده) باید بتواند گره‌های خروجی (گیرنده) را که بسته باید از طریق آن‌ها عبور کند، پیدا کند. این کار به طور خاص با استفاده از آدرس‌های IP مقصد در هدر بسته صورت می‌گیرد. به طور مشابه یک گره گیرنده باید تعیین کند که یک بسته‌رسیده با توجه به آدرس مبدا IP، از کدام گره فرستنده، ارسال شده است. به علاوه، گره گیرنده باید بتواند اندازه‌ی متوسط بسته برای بلوک‌های OAM را محاسبه کند تا در برآورد بهره‌وری و مصرف از این اطلاعات استفاده شود. گرچه ممکن است حالت عمومی پیچیده باشد، این روش در شبکه‌های خصوصی مجازی که مکان‌شناسی، به طور کامل شناخته و مسیریابی محدود شده است، عملی است.

www.prozhe.com

www.prozhe.com

۳-٤ مدیریت شبکه های خصوصی مجازی بر مبنای پروتکل اینترنت (IP) (بخش هفتم و پایانی)

۳-٤-۱ مانیتور کردن ترافیک در شبکه های خصوصی مجازی

هدف از مانیتور کردن ترافیک، اندازه گیری و تخمین lossها، تاخیرها و بهره‌وری برای ترافیک IP در شبکه‌های خصوصی مجازی و بین گره‌های کناری provider یا گره‌های کناری مشتری بر مبنای یک مکان شناسی عمومی که در شکل ۱۰ نشان داده شده، است.

همان‌طور که پیش از این بیان شد، طبیعت connection-less بودن IP مساله‌ای اساسی در طراحی سیستم‌های مانیتورینگ است. برای استفاده از بسته‌های OAM در شبکه‌های IP به توابع جست‌وجو (look-up)، لازم است که گره‌های مانیتورینگ خروجی (و ورودی) را تعیین کنند. اگرچه در شبکه‌های خصوصی مجازی، که به وسیله‌ی تونل‌های نقطه به نقطه پیاده سازی شده است، آدرس گره خروجی در یک هدر IP اضافی حمل می‌شود. برای این کار، آدرس، به گره مانیتورینگ خروجی صحیح با آدرس مقصد IP در هدر بسته منطبق می‌شود. در موارد عمومی‌تر یک رویه‌ی مشابه ممکن است به توابع جست‌وجوی پیچیده‌تری نیاز داشته باشد.

۳-۵ عملیات گره های مانیتورینگ

توابع مانیتورینگ وقتی فعال می‌شوند که مجموعه‌ای از وضعیت‌های خاص که سیاست مانیتورینگ اپراتور را به طور کامل بیان می‌کنند، پوشانده شوند. برای کلاس‌های یک سرویس مشخص باید در طی پریودهای زمانی مشخصی مانیتور شوند. یک روتر وقتی به عنوان یک گره مانیتورینگ ورودی عمل می‌کند، باید عملیات مانیتورینگ را برای هر VPN انجام دهد (و به طور مشابه به عنوان یک گره مانیتورینگ خروجی). روتر باید شمارنده‌های جداگانه‌ای را برای هر گره خروجی مانیتورینگ به دست آورد تا بتواند توالی تعداد بسته‌هایی را که به هر یک از گره‌های گیرنده فرستاده شده‌اند، نگه‌داری کند. بسته‌های OAM به وسیله‌ی گره ورودی، تولید می‌شوند و به طور متوالی در داخل ترافیک کاربر بین بلوک‌های بسته‌های کاربر قرار می‌گیرند، به طوری که آدرس مقصد به گره مانیتورینگ خروجی اشاره کند. آدرس مبدا با آدرس

www.prozhe.com

www.prozhe.com

گره مانیتورینگ ورودی هماهنگ می‌شود. شکل ۹payload بسته OAM را نشان می‌دهد. یک روتر که به عنوان گره مانیتورینگ خروجی عمل می‌کند، باید تعیین کند که بسته‌های رسیده کاربر از کدام گره ورودی رسیده‌اند، با توجه به آدرس مبدا در هدر بسته. هر گره گیرنده باید یک شمارنده برای هر گره ورودی نگه دارد و عملیات زیر را انجام دهد:

- بسته‌های OAM را از طریق شماره پروتکل منحصر به فرد در هدر بسته پیدا می‌کند.
- یک مهر زمانی در بسته‌های OAM قرار دهد که نشان دهنده‌ی زمان جاری در گره خروجی باشد.
- مقدار جاری شمارنده را در بسته وارد کند تا ردپای شماره بسته‌های دریافت شده از گره خروجی را نشان داده شود.
- بسته OAM را به گره ورودی فرستنده برگرداند.

۳-۵-۱ نتیجه گیری روش مانیتورینگ نهفته

داده‌های اندازه گیری شده که به وسیله‌ی بسته‌های OAM حمل می‌شوند یا در گره‌های مربوط ذخیره می‌شوند، ممکن است به وسیله‌ی گره ورودی آغازین یا یک سرور تنها، پردازش شوند. اختلاف بین تعداد بسته‌های فرستاده شده (Number Of Sent Packets) در بسته nام OAM و بسته‌ی n-1ام OAM تعداد بسته‌های فرستاده شده در یک بلوک OAM را مشخص می‌کند. این محاسبات در مورد تعداد بسته های دریافت شده (Number Of Received Packets) نیز صادق است (شکل ۹). بنابراین اختلاف این دو نشان‌گر تعداد بسته‌های گم شده در بلوک OAM است. یک نمونه از تاخیر انتقال بین یک گره فرستنده و یک گره گیرنده به وسیله اختلاف بین TimeAtReceiver و TimeAtSenderدر یک بسته OAM داده می‌شود.بسته‌های مانیتورینگ گم شده از طریق شماره‌های ترتیب گم شده کشف می‌شوند.

هیچ تضمینی وجود ندارد که همه بسته‌ها در یک رشته بین دو گره یک مسیر را در کل دوره‌ی زمانی دنبال کنند. یک راه برای تشخیص تغییرات در مسیر این است که از ابزاری استفاده کنیم که به طور متناوب مسیر بین دو گره کناری را ثبت کند. اگر بسته‌ها به ترتیبی غیر از ترتیب فرستاده شدن دریافت شدند،

www.prozhe.com

www.prozhe.com

اختلاف در ترتیب می‌تواند باعث شود که بلوک‌های OAMشامل بسته‌های بیش‌تر یا کم‌تری ازتعداد N بسته پیش‌بینی شده باشند. بنابراین یک بسته که متعلق به بلوکی در فرستنده است، ممکن است به دلیل تغییراتی در مسیر، در یکی از بلوک‌های مجاور در گره گیرنده دیده شود. اگر در همان زمان بسته‌ها در این بلوک‌ها گم شوند تعیین این‌که در کدام بلوک loss اتفاق افتاده، همیشه امکان‌پذیر نیست. اگرچه از آن‌جایی که مقادیر شمارنده در بسته‌های OAM تجمعی هستند، تلفیق تعدادی از بلوک‌های پشت سر هم در واحدهای بزرگ‌تر امکان‌پذیر است.

www.prozhe.com

www.prozhe.com

نتایج

شبکه‌های خصوصی مجازی با داشتن معماری مدیریتی مناسب و پیاده‌سازی صحیح، می‌توانند برای سازمان‌ها مفید باشند، به طوری که دیگر به داشتن یک شبکه خصوصی کامل که منابع زیادی را برای پیاده سازی استفاده می‌کند، نیازی نباشد. از طرفی وقتی یک شبکه‌ی خصوصی مجازی برای داشتن ارتباط با دنیای اینترنت بر روی backbone اینترنت سوار می‌شود و بسته‌های آن آدرس IP می‌گیرند، مساله اشتراک منابع پیش می‌آید و ممکن است، در اختیار قرار دادن منابع برای درخواست‌ها در همه‌ی زمان‌ها امکان‌پذیر نباشد. بنابراین باید توابعی را برای تضمین کیفیت سرویس در این شبکه‌ها به کار ببریم. بنابراین ضرورت مدیریت این شبکه‌ها در مقایسه با شبکه‌هایی که برای کیفیت سرویس تضمین پایین‌تری دارند، بسیار محسوس است.

www.prozhe.com

www.prozhe.com

منابع و ماخذ :

۱- شبکه‌های خصوصی مجازی VPNs- پدیدآورنده: داریوش زاهدمنش، مهران طریحی- ناشر: نص-۱۳۸۹

۲- راه‌کارهای مجازی‌سازی در شبکه-پدیدآورنده: محمدرضا نیکوکلام مظفر-ناشر: پندار پارس، مانلی، پارشمن- اسفند ۱۳۹۰

۳- شبکه های علمی مجازی-پدیدآورنده: سعیدرضا عاملی، کورش گوهریان (ویراستار)-ناشر: پژوهشکده مطالعات فرهنگی و اجتماعی-۱۳۸۸

www.prozhe.com