SNMP چیست؟ آشنایی با پروتکل مدیریت شبکه SNMP (نسخه PDF)

اگر تـا به حـال اسم نرم افزارهـای مانیتورینگ شـبکه به گوشـتان خورده است شایـد از خودتان پرسـیده باشـید که این نرم افزارها چگونه میتواننـد اطلاعات کلاینت ها و ابزارهای شـبکه را دریافت کننـد؟چطور میتواننـد وضـعیت کلاینت ها را در شـبکه بدانند؟ چطوری میشود فهمیـد یـک کلاینتی در شـبکه دچار مشـکل شـده است؟ خب جواب تمام این سوال ها، پروتکل پرکاربردی است به نام SNMP که مخفف Simple Network Management Protocol می باشـد. در این مطلب قصـد داریم که موارد زیر را در باره این پروتکل بسـیار پرکاربرد توضـیح دهیم:

- SNMP چیست؟
- اجزا این SNMP چه چیزهایی هستند و کاربرد هر کدام از این اجزا چه چیزی است؟
- آشنایی با دستورات اولیه SNMP
- ورژن های SNMP

SNMP چیست؟

اگر دارین این مقاله رو میخونین حتما با لایه های شـبکه آشنا هستین! SNMP یک پروتکل لایه هفتم شبکه و یا Application است که برای مـدیریت و مـانیتور کردن و یـا جمع آوری اطلاعات از Device هـای شـبکه و عملکرد آن ها مورد اسـتفاده قرار میگیرد. Device هایی مثل روترها، سوییچ ها، پرینترها، اسـکنرها و حتی Device های اینترنت اشـیا. حتی علاوه بر سـخت افزارها که با SNMP می توان مانیتور کرد، میتوان برای مانیتور کردن سرویس هایی مثل DHCP نیز از آن استفاده کنیم.

SNMP میتواند Function های زیادی را اجرا کند. میتواند تنها وضـعیت Device را ببینیم و یـا حتی تنظیماتی را و یا تغییراتی را بر روی آن انجام دهیم. مثل Reset کردن یک پسورد و یا تغییر تنظیمات کانفیگ یک سوییچ. میتوان گزارشـی از مصرف پهنای باند، cpu و حافظه ی در حال اسـتفاده را تهیه کند. حتی بعضـی از SNMP Manager هـا میتواننـد به صورت اتوماتیـک ایمیل ها و یا پیام های متنی را مبنی بر استفاده بیش از حد از منابع برای مدیران شبکه ارسال نمایند.در ادامه نحوه دریافت این اطلاعات را توسط اجزا SNMP بیان خواهیم کرد.

اجزا پروتکل SNMP

همانطور که SNMP می تواند در شـبکه های با انواع اندازه ها اسـتفاده شود ، بیشتر مزیت استفاده از آن در شبکه های بسیار بزرگ است. فرض کنیـد برای رفع اشـکال در شـبکه ای با صـدها نود بخواهید به هر سیسـتم به صورت Manually وارد شوید و وضـعیت آن را بررسـی نمایید! که این کار به شدت زمانبر و هزینه بر است. اما با اسـتفاده ازSNMP ، یک مدیر شـبکه قادر خواهد بود تا تمام آن نودهای شبکه را تنها از طریق یک Interface مدیریت و مانیتور کند! خب حالا بریم سراغ اینکه ببینیم SNMP از چه اجزایی تشکیل شده است:

۱- SNMP Agent :

این یـک برنامه است که بر روی Device و یا سرویسـی که در حال مانیتور شـدن است نصب میشود (یا وجود دارد و تنها باید آن را فعال کنیم) و کارش جمع آوری اطلاعات در مورد پارامترهای مختلف است مثل مقدار اسـتفاده از پهنای باند و یا فضای ذخیره سازی و ... .زمانی که توسط SNMP Manger) SNMP Manger چیه؟ در پایین توضـیح داده شـده) به Device یـا سـرویس مورد نظر کوئری زده میشود، این Agent ای که در اونجـا مـا آن را فعال کردیم، اطلاعات جمع آوری کرده را به SNMP Mangager ارسال می کند. وظیفه دیگر یک Agent این است که میتواند NMS را در صورت بروز خطا نیز با خبر کند.یادتان باشد همانطور که گفتیم بیشتر Device ها با یک SNMP Agent از پیش نصب شده تولید میشوند و تنها نیاز است که آن را فعال و کانفیگ کنیم.

پس عملکردهای یک Agent را میتوان به صورت زیر نوشت:

۱. • جمع آوری Management Information ها درباره محیط اطراف خود
۲. • ذخیره Management Information ها و یا بازیابی این اطلاعات در MIB (توضیح MIB در پایین)
۳. • اطلاع دادن یک رویداد به NMS

۴. • رفتار کردن به مانند پراکسی برای بعضی از نودهای شبکه که قابلیت SNMP Management را ندارند.

۲- NMS (SNMP Manager)

خب حالا- بریم سراغ جز دیگر این پروتکل که درواقع نقش مدیر را در این پروتکل بازی میکند. SNMP Manager که به آن NMS نیز میگویند، یک پلتفرم نرم افزاری است که مسئولیت ایجاد ارتباط با Agent های تعبیه شده در Device های شبکه را برعهده دارد و اطلاعات جمع آوری شده توسطAgent ها را دریافت می کند.این NMS از Agent نیز میخواهد که در فواصل معینی، آپدیت هایی را از طریق SNMP ارسال نماید. اینکه یک NMS چه کاری با این اطلاعاتی که از Agent دریافت می کند می تواند انجام دهد، بستگی به توانایی ها و ویژگی های NMS دارد. NMS های مختلفی وجود دارند که دارای قابلیتهای مختلف و توانایی ساپورت کردن تعداد نودهای مختلفی را دارند.

پس عملکردهای یک NMS را میتوان به صورت زیر بیان کرد:

۱. • کوئری زدن به Agent ها
۲. • دریافت پاسخ ها (Response ها) از طرف Agent ها
۳. • Set کردن (تنظیم کردن) متغیرها در Agent ها
۴. • تایید ناهمزمان رویدادها از طرف Agent ها

۳- Managed Devices

Managed Device ها و یا عناصر شبکه (Network Elements) در واقع همان قسمت هایی از شبکه هستند که Agent برروی آنها قرار دارد. مثل روترها، سوییچ ها، سرورها، Workstation ها، پرینترها، UPS ها و ... .

۴- MIB (Management INFORMation Base)

هر Agent ای یک دیتابیسی از اطلاعات را که توضیح دهنده پارامترهای Managed Device ها هستند بدست می آورد که به این دیتابیس MIB و یا Management INFORMation Base می گویند. MIB یک دیتابیس است، دیتابیسی است که SNMP از آن استفاده می کند تا به Agent کوئری بزند و از Agent اطلاعات خاصی را درخواست کند . این دیتابیس باید در NMS بارگذاری (Load) شود و ازین طریق است که NMS میتواند وضعیت این Device ها را مانیتور کند.

درواقع می توان گفت که این MIB شامل مقادیر آماری و کنترلی تعریف شده برای نودهای روی شبکه است. و به صورت خلاصه اینکه فایل های MIB مجموعه ای از سوالاتی هستند که یک SNMP Manager میتواند از یک Agent ای بپرسد. Agent این داده ها را به صورت Local جمع آوری و ذخیره میکند. بنابراین SNMP Manager از این سوالات استاندارد و یا حتی خصوصی که مربوط به هر Agent خاصی میتوانند باشند اطلاع دارد.

دستورات اولیه SNMP

سادگی در تبادل اطلاعات، پروتکل SNMP را به یک پروتکل بسیار مورد قبول تبدیل کرده است. در این قسمت با دستورات کوتاه SNMP آشنا خواهد شد:

GET

دستور GET یک درخواست است که توسط Manager به سمت Managed Device ارسال میشود. اجرای این دستور منجر به دریافت یک یا تعدادی Value از Managed Device خواهد شد.

GETNEXT

این دستور نیز مشابه دستور GET است. تفاوت مهمی که با GET دارد این است که اجرای این دستور منجر به گرفتن مقدار OID (به هر آیتم در MIB یک Object ID اختصاص داده میشود) بعدی در درخت MIB) MIB tree) خواهد شد.

GETBULK

این دستور برای دریافت داده های حجیم از MIB Table استفاده خواهد شد.

SET

این عملیات توسط Manager برای تغییر و یا تخصیص دادن یک مقدار از Managed Device استفاده میشود.

TRAPS

عکس دستورات بالا که ابتدا از SNMP Manager صادر می شدند، TRAPS ابتدا توسط Agent ها صادر میشوند. درواقع سیگنالی هستند که توسط Agent به SNMP Manager هنگام وقوع یک رویداد ارسال میشوند.

INFORM

این دستور همانند دستور TRAP ابتدا توسط Agent ارسـال میشود با این تفاوت که INFORM شامل تاییـدیه ای از طرف SNMP Manager برای دریافت پیام میباشد.

RESPONSE

این دستور توسط Agent به سمت SNMP Manager در پاسـخ به یک درخواست GET ارسال میشود. که محتوای آن مقـدار Variable هایی است که در GET درخواست شده است.

ورژن های SNMP

SNMP از زمان پیدایشـش آپـدیت هایی را به خود دیده است. اما ورژن های ۱ و ۲ آن بیشترین ورژن های مورد اسـتفاده بوده اند. ورژن سوم SNMP ورژن ایمن تری نسبت به ورژن های ۱ و ۲ است.

ورژن ۱

این اولین ورژن از SNMP است که در RFC ۱۱۵۵ و RFC ۱۱۵۷ تعریف شده است.

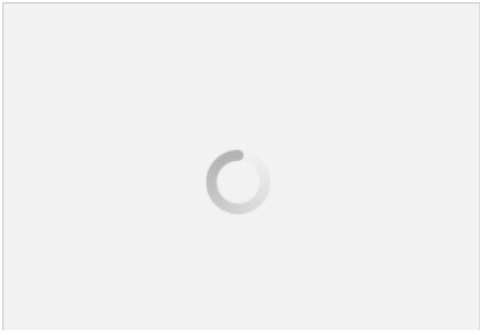
ورژن ۲C

این پروتکل تجدیـد نظر شـده ای است که شامل بهبودهایی بر ورژن ۱ می باشد. که در RFC ۱۹۰۶ ، RFC ۱۹۰۵ ، RFC ۱۹۰۱ و RFC ۲۵۷۸ تعریف شده است.

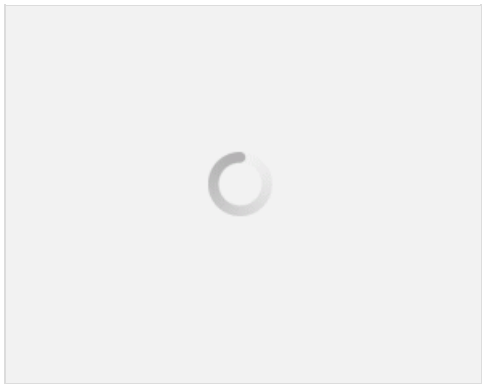
ورژن ۳

ورژن سوم ورژن امنی را برای SNMP تعریف می کند و ویژگی های امنیتی را در بردارد مثل رمزنگاری پیام های رد و بدل شونده. و در RFC ۳۴۱۴ ، RFC ۳۴۱۲ ، RFC ۳۴۱۱ ، RFC ۱۹۰۶ ، ۱۹۰۵ و RFC ۳۴۱۵ تعریف شـده است.خب در آخر این مقاله هم تصاویری از نحوه کار کردن پروتکل SNMP را با دستوراتی که در بالا گفتیم مشاهده می کنید:

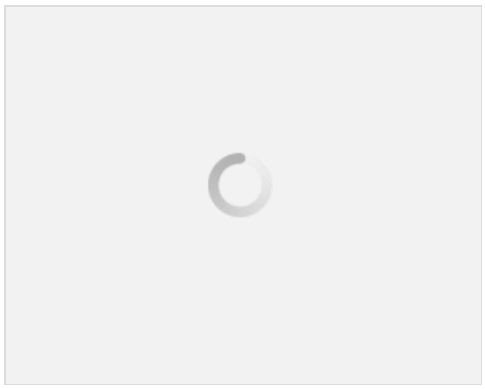
GET GETNEXT GETBULK / SET



TRAP



INFORM



علی آزادی

@حمید

منظورتون از اینکه UDP همگانیه چیه؟

UDP پکتیه که نیاز به تایید از طرف مقصد نداره و سبک تره بر خلاف TCP

حمید

مگر udp پروتکلی نیست که به صورت همگانی اطلاعات ارسال میکنه پس چرا در تصاویر که نمایش داده شده از این پروتکل اسـتفاده شده با توجه به امنیتی بودن نسخه ۳

ممنون میشم اگر روشنم کنید.

مطلب اصلی