اول: RMON چیست؟

همون‌طور که توی درس دیدیم به کمک SNMP می‌تونیم در شبکه بین مدیر و ایجینت‌ها پیغام رد و بدل کنیم و اگر بخوایم مانیتورینگ داشته باشیم باید تمامی داده‌هایی که در شبکه رد و بدل میشه رو به نوعی منتقل و آنالیز کنیم. ما می‌خواهیم کامپوننت جدیدی به اسم RMON رو معرفی کنیم که میخواد بیاد و کارهای مرتبط با مانیتورینگ رو جداگانه انجام بده و این بار رو از دوش مدیر شبکه برداره. RMON می‌تونه به صورت یه دستگاه stand-alone باشه یا میتونه به عنوان یه probe روی خود دستگاه‌های موجود توی شبکه مثل روترها، سوییچ‌ها و چیزهای شبیه به این‌ها باشه.

این کار مزایایی ایجاد میکنه:

- Offline operation: این اجازه به مدیر داده میشه که همیشه و به طور پیوسته نیازی نباشه که با آبجکت‌ها در ارتباط باشه. این میتونه هم به خاطر کم کردن هزینه‌های ارتباطی باشه یا حتی به خاطر خطاهایی که در ارتباط مدیر با اجزای شبکه پیش میاد. به این خاطر RMON به طور پیوسته با اجزا در ارتباطه و اطلاعات رو جمع آوری می‌کنه و به صورت بهینه‌تری در صورت نیاز با مدیر شبکه در ارتباط خواهد بود و به آن گزارش خواهد داد.
- مانیتورینگ فعال (Proactive): با وجود RMON ما یک جز شبکه را فقط به کارهای مانیتورینگ اختصاص می‌دهیم که همیشه فعال است و اطلاعات را جمع‌آوری می‌کند و وقتی که خطایی را به مدیر اطلاع می‌دهد، تاریخچه‌ی اتفاقاتی که در سیستم افتاده است را نیز نگه داشته است تا مدیر بتواند علت اتفاقات را هم تشخیص دهد.
- تشخیص مشکلات و گزارش‌دهی: این واحد مانیتورینگ قابل پیکره‌بندی است به صورتی که ما می‌توانیم آن را به گونه‌ای تنظیم کنیم که شرایطی که خطاهای خاصی پیش می‌آید را نیز بررسی کند و به طور پیوسته به آن‌ها توجه کند و در صورتی که یکی از آن‌ها رخ داد به مدیر گزارش دهد. قابلیتی شبیه به تنظیم یک سری rule که بر اساس آن‌ها آلرت ارسال شود.
- کامل‌کردن داده‌ها: با توجه به اینکه یک واحد اختصاصی برای مانیتورینگ داریم و این واحد به طور مستقیم با اجزای شبکه در ارتباط است، می‌تواند اطلاعات مهم‌تر را از داده‌ها در بیاورد و حتی آن‌ها را با توجه به شرایط شبکه تکمیل‌تر هم بکند تا برخی از خطاها راحت‌تر حل شوند.
- داشتن چندین مدیر: بسیاری از شبکه‌ها چندین مدیر دارند، RMON قابلیت اینکه گزارش‌های خود را به همه‌ی آن‌ها ارسال کند را نیز دارد که این ویژگی باعث می‌شود از منابع بهتر استفاده کنیم و همه‌ی مدیران شبکه از یک RMON به طور همزمان استفاده کنند.

دوم: RMON و MIB

خب حالا می‌تونیم بریم سراغ قرارگیری اجزای RMON در MIB و همچنین درخت اطلاعات مدیریتی (MIT). خب RMON هم مثل اکثر مفاهیم و تکنولوژی‌ها طی زمان کامل‌تر شده و نسخه‌های جدیدتری از اون رونمایی شدن. ما هم توی این ارائه به RMON 1 , 2 می‌پردازیم. هر کدوم از این نسخه‌ها توی چندین گروه طراحی شدن و اگر یک دستگاه مانیتورینگ میخواد که از ویژگی‌های هر کدوم از این گروه‌ها استفاده کنه باید تمامی آبجکت‌هایی که توی اون گروه هست رو پیاده‌سازی کنه.

توی شکل زیر می‌بینیم که در نهایت گروه RMON که یکی از زیرمجموعه‌های MIB-2 هست دارای چندین گروه است که برخی از اون‌ها توی RMON 1 و برخی دیگر توی RMON 2 معرفی شدن.

اگر بریم در قالب مدل پشته‌ای osi، در RMON 1 مانیتورینگ ما بیشتر در سطح ۲ لایه‌ی اول شبکه بوده. در RMON ۲ اما بیشتر به سمت لایه‌های ۳ تا ۷ شبکه برای مانیتورینگ رفته‌ایم.

سوم: RMON 1

این نسخه اولین نسخه ی RMON بود که RFC آن در سال 1995 ثبت شد. در کل مواردی که در این نسخه بررسی می شدند شامل موارد زیر هستند:

1. گروه Ethernet statistics: گروه آمار اترنت شامل آمار اندازه گیری شده توسط پروب برای هر رابط اترنت نظارت شده در این دستگاه است. این گروه از etherStatsTable تشکیل شده است. اطلاعاتی که در این جدول استفاده می شوند عبارتند از:
    1. تعداد کل رویدادهایی که بسته ها در آنها drop شدند
    2. تعداد کل بسته های عبوری از interface
    3. تعداد کل بسته های broadcast عبوری از interface
    4. تعداد کل بسته های multicat عبوری از inteface
    5. تعداد بسته های دریافتی که سایز آن ها بین 256 تا 511 octet باشد.

    و ...

    هر کدام از این etherstatsentry شامل اطلاعات آماری تنها برای یک ethernet interface است در واقع probe باید برای هر interface یک etherStats جدید ایجاد کند.
2. گروه Historty control: این گروه نمونه گیری آماری دوره ای از داده ها را از انواع مختلف شبکه ها کنترل می کند. کنترل نمونه گیری آماری از داده های شبکه های مختلف:
    - فاصله ی زمانی داده های نمونه برداری شده

- تعداد فواصل نمونه برداری گسسته
- سرریز نشدن bucketها

3. گروه Ethernet histroy: نمونه های آماری دوره ای را از یک شبکه اترنت ثبت می کند و آنها را برای بازیابی بعدی ذخیره می کند. این گروه از etherHistoryTable تشکیل شده است و هر رکوردی که در این جدول ثبت می شود متناظر یکی از نمونه ها است. این جدول شامل اطلاعاتی همانند گروه اول می شود. تفاوت این گروه با گروه اول در این است که گروه اول اطلاعات real time و در لحظه را شامل می شود. اما این گروه اطلاعات گذشته را ثبت می کند.
4. گروه Alarm: گروه هشدار به صورت دوره ای نمونه های آماری را از متغیرهای موجود در probe گرفته و آنها را با آستانه های پیکربندی شده قبلی مقایسه می کند. اگر متغیر نظارت شده از یک آستانه عبور کند، یک رویداد ایجاد می شود. این گروه شامل جدول alarmTable می شود که در این جدول آستانه های متغیر مورد بررسی، index رویدادی که قرار است در صورت عبور متغیر از آستانه رخ دهد (این index از جدول eventTable که بعدا توضیح داده می شود برداشته می شود). به جهت اینکه تعداد آلارم ها نیز زیاد نشود از مکانیزم hystersis استفاده می کنیم به این معنا که اطلاعات گذشته را نیز در تصمیم گیری برای ثبت هشدار دخیل می کنیم.
5. گروه Host: شامل آمار مربوط به هر host کشف شده در شبکه است. این گروه با نگه داشتن لیستی از آدرس های MAC مبدا و مقصد که در بسته ها که به طور بی رویه از شبکه دریافت می شوند، host ها را در شبکه کشف می کنند.
6. گروه HostTopN: برای تهیه گزارش‌هایی استفاده می‌شود که میزبان‌هایی را توصیف می‌کند که فهرستی را که بر اساس یکی از آمارهایشان مرتب شده است، در صدر قرار می‌دهند. آمارهای موجود نمونه هایی از یکی از آمارهای پایه آنها در بازه زمانی مشخص شده توسط ایستگاه مدیریت است. بنابراین، این آمار بر اساس نرخ است. ایستگاه مدیریت همچنین انتخاب می کند که چه تعداد از این میزبان ها گزارش شده است.
7. گروه matrix: آماری را برای مکالمات بین مجموعه ای از دو آدرس ذخیره می کند. به عنوان مثال تعداد بسته ها یا تعداد octetها و یا تعداد بسته های با خطا
8. گروه Filter: اجازه می دهد تا بسته ها با یک معادله فیلتر مطابقت داده شوند. این بسته های منطبق یک جریان داده را تشکیل می دهند که ممکن است ضبط شود یا ممکن است رویدادهایی ایجاد کند.
9. گروه Packet capture: اجازه می دهد تا بسته ها پس از عبور از یک کانال بر اساس یک فیلتر، ضبط شوند.
10. گروه Event: تولید و اعلان رویدادها را از این دستگاه کنترل می کند. این گروه شامل جدول eventTable می شود که از EventEntry تشکیل شده و بخش هایی مانند:
    - توصیف ورودی رویداد
    - نوع رویداد تولیدی

- آخرین زمان ارسال رویداد

را شامل می شود.

چهارم: RMON 2

محدودیت های RMON 1

اگرچه RMON1 بسیار موفقیت آمیز بود اما در پیاده سازی ها به وضوح مشخص شد که monitor کردن لایه ی 2 هنگام monitor کردن ترافیک شبکه گسترده WAN محدود است.

لازم به ذکر است که RMON 2 به عنوان جایگزین RMON 1 معرفی نشده است و تنها یک توسعه بر روی این نسخه ی اولیه است، بنابراین برای استفاده از تمام قابلیت های RMON می بایست از هر دو نسخه استفاده کرد.

ورژن RMON 2

یک توسعه روی ورژن اول آن بود که در سال 1997 در RFC 2021 به ثبت رسید. این ورژن از SMI v2 استفاده کرده است. توسعه ی این ورژن نسبت به ورژن قبلی در افزودن قابلیت های متعدد بوده است. به عبارتی در این نسخه آنالیزهای RMON بر خلاف RMONv1 که تنها در سطح لایه ی MAC بود تا سطح لایه ی اپلیکیشن بالا آمده است. در واقع قابلتی اندازه گیری ترافیک لایه 3 و اطلاعات آماری لایه ی اپلیکیشن را داراست.

گروه های موجود در RMON2:

1. گروه Protocol Directory: این گروه شامل لیست پروتکل هایی است که یک probe میتواند monitor کند.
2. گروه Protocol Distribution: اطلاعات آماری ترافیک هر پروتکل
3. گروه Address Mp: نگاشت آدرس های لایه ی network به لایه ی MAC
4. گروه Network layer host: اطلاعات آماری ترافیک لایه ی 3 به ازای هر host
5. گروه Network layer matrix: اطلاعات آماری ترافیک لایه ی 3 به ازای هر زوج مبدا و مقصد host
6. گروه Application layer host: اطلاعات آماری ترافیک توسط پروتکل لایه ی اپلیکیشن به ازای هر host
7. گروه Application layer matrix: اطلاعات آماری ترافیک توسط پروتکل لایه ی اپلیکیشن به ازای هر زوج مبدا و مقصد host
8. گروه User history: تریکیبی از دو گروه History و Alarm است تا مجموعه‌ای از تاریخچه مشخص‌شده توسط کاربر را ارائه دهد و همچنین نمونه های دوره ای از متغیرهای مشخص شده توسط کاربر را نشان دهد
9. گروه Probe configuration: یک روش استاندارد برای پیکربندی از راه دور پارامترهای کاوشگر، مانند trap destination و out-of-band management ارائه می‌کند.