شرکت دانش بنیان ارگ

آرام رمز گستران

SNMP

معرفی محصول

SNMP پروتکل لایه Application است که امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می کند و در واقع قسمتی از پروتکل TCP/IP می باشد. این پروتکل توانایی مدیریت و پیدا کردن مشکلات و حل آنها را در شبکه برای مدیران مهیا می کند. سه نسخه از این پروتکل موجود است که عبارتند از:

- SNMP V1
- SNMP V2
- SNMP V3

هر سه ورژن، دارای یک سری مشخصات مشترک هستند. البته باید افزود نسخه شماره سه بسیار ایمن تر از نسخه های دیگر است.

یك شبكه مدیریت مبتنی بر SNMPشامل سه عنصر كلیدی است:

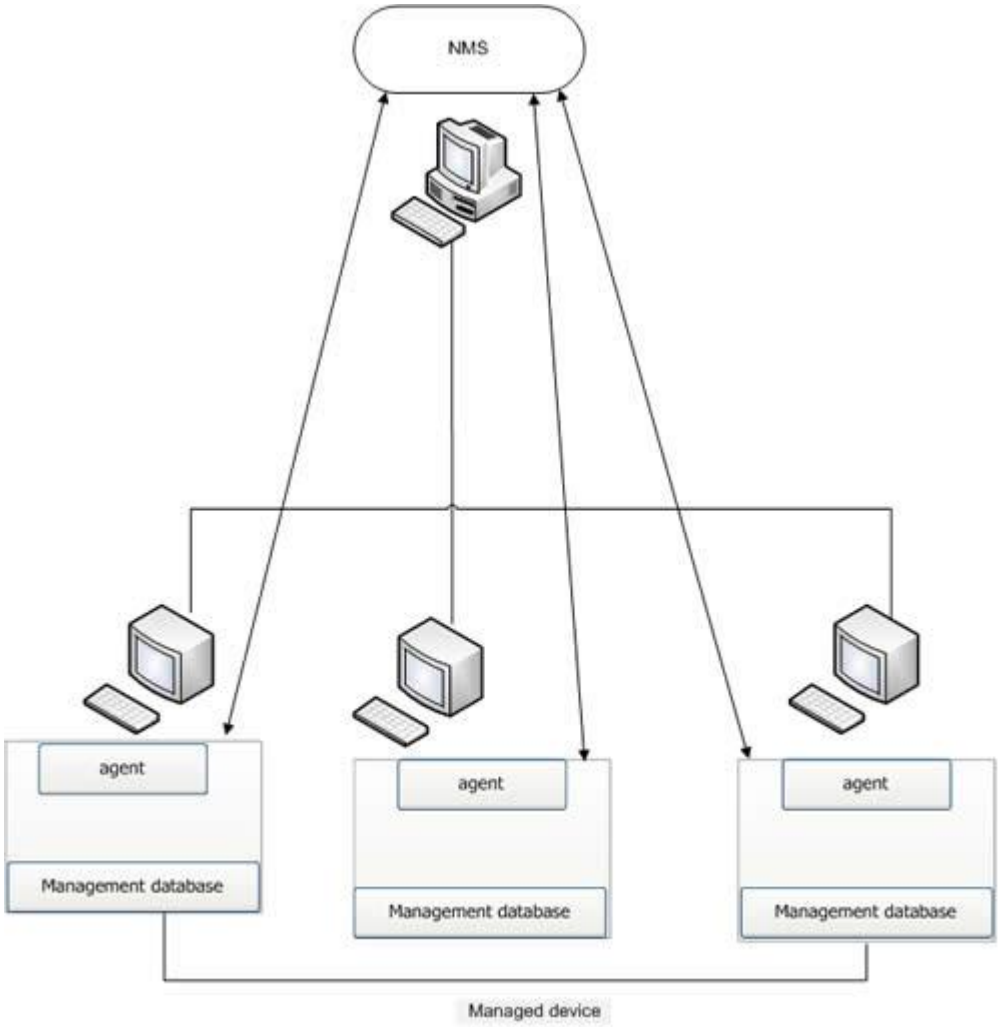
- **عناصر اصلی درSNMP**

- سیستم مدیریت شبکه (Network Management System NMS)
- کارگزاران (Agent)
- تجهیزات مدیریت شده (Managed devices)

هر یک از تجهیزات شبکه که می‌بایست مدیریت شوند (Managed Devices)، در واقع یک نود از شبکه هستند که دارای یک(Agent) درون خود می باشند. این تجهیزات اقدام به جمع آوری و ذخیره سازی اطلا عات می‌کنند و سپس این اطلاعات را در اختیار NMS قرار میدهند. این تجهیزات گاهی اوقات عناصر شبکه نیز نامیده می شوند که می توانند تجهیزاتی از قبیل روترها،سوئیچها، Bridge ها، Hubها، کامپیوتر ها و پرینتر ها باشند.

به عبارت دیگر می توان گفت هر یک از اجزاء شبکه که از پروتکل SNMP پشتیبانی کرده و می توان از آنها با استفاده از NMS ها به واسطه پروتکل SNMP اطلاعات دریافت نمود، یک Managed Device خوانده می‌شود.

فرامین پایه در SNMP



تجهیزات مدیریت شده، توسط چهار فرمان اصلی کنترل می شوند که این چهار فرمان عبارتند از:

تجهیزات مدیریت شده، توسط چهار فرمان اصلی کنترل می شوند که این چهار فرمان عبارتند از:

Read: با این فرمان NMS تجهیزات مدیریت شده را مانیتور می‌کند و متغییرهای گوناگونی را که توسط تجهیزات مدیریت شده نگهداری می‌شوند را امتحان یا بازرسی می‌کند.

Write: با این فرمان NMS تجهیزات مدیریت شده را کنترل می کند و مقادیر متغییرهای ذخیره شده در تجهیزات مدیریت شده را تغییر می دهد.

Trap: با این فرمان تجهیزات مدیریت شده به صورت غیر هم زمان رخدادها را برای NMS گزارش می کنند. در واقع وقتی واقعه ای رخ می دهد؛ به ازای هر رخداد، یك Trap از طرف تجهیزات کنترل شده به سمت NMS ارسال می شود.

Operation Traversal: با این فرامین پیمایشی، NMS تصمیم می گیرد که کدام یك از متغییرهای یك تجهیز مدیریت شده، پشتیبانی شود و به صورت متوالی اطلاعات را در داخل جداول متغییرها جمع آوری می کند. (مانند جدول مسیریابی Table Routing)

پایگاه اطلاعات مدیریتی در SNMP (MIB)

MIB در واقع مجموعه ای از اطلاعات است که به صورت سلسله مراتبی سازماندهی شده است و از پروتکل های مدیریتی از قبیل SNMP استفاده می کند. MIBها شامل موضوعات مدیریت شده (Objects) هستند که توسط شناسه های Object Identifier مشخص می‌شوند. یك موضوع مدیریت شده که گاهی اوقات MIB نامیده می شود، در واقع یکی از مشخصه های تجهیزات مدیریت شده است. دو نوع موضوع مدیریت شده وجود دارد:

- Scalar Object
- Tabular Object

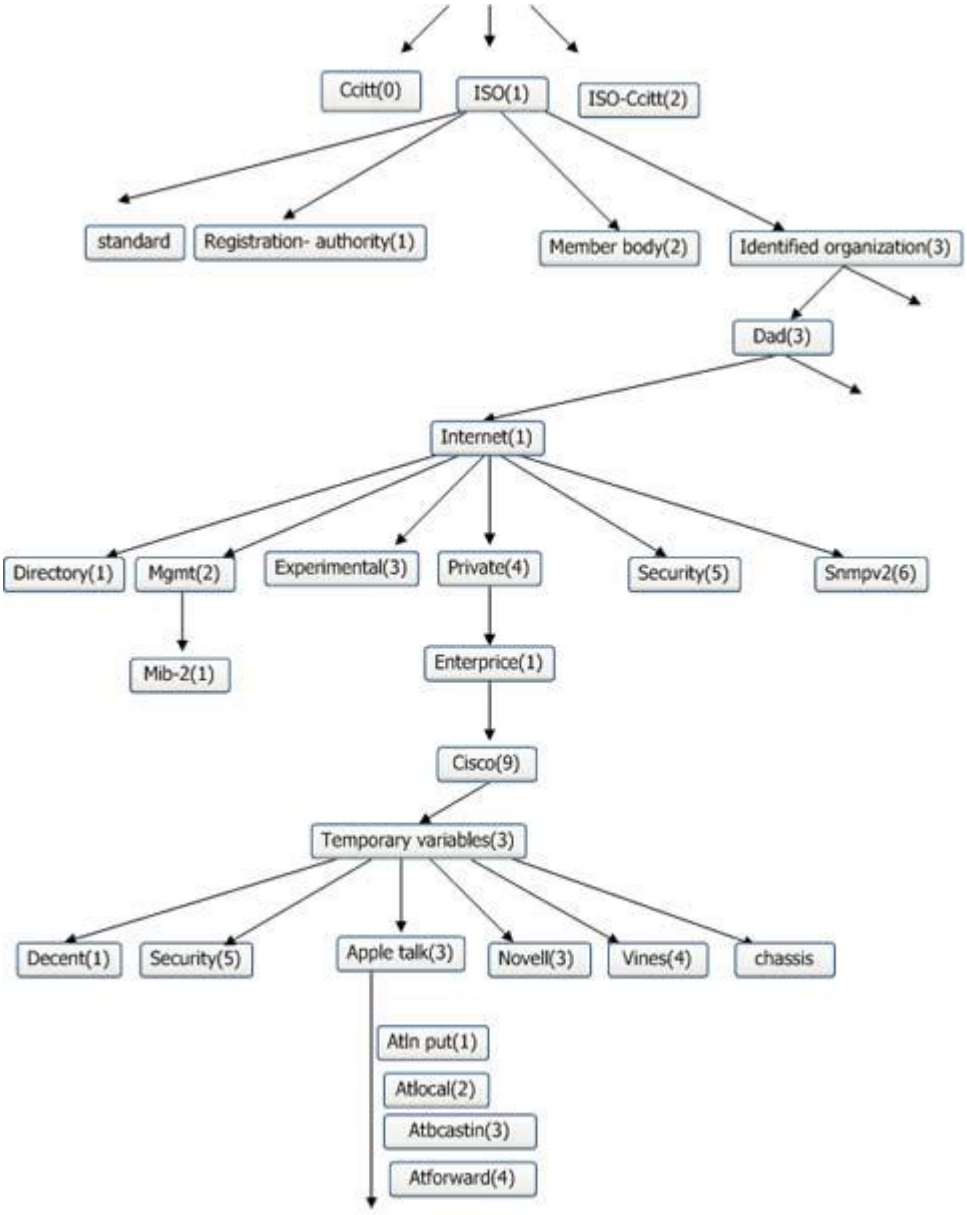
موضوعات Scalar یك نمونه موضوع واحد را تعریف می‌کنند، ولی موضوعاتTabular چندین موضوع به هم پیوسته و مرتبط که به صورت گروهی در جداول MIB قرار دارند را تعریف می‌کنند. برای مثال تعداد پکتهای ورودی Apple Talk به یك اینترفیس از یك روتر با معین می‌شود که یك موضوعScalar است و یك نمونه موضوع واحد را نشان می‌دهد. در سلسه مراتب MIB، هر موضوع برای شناسایی دارای یك شناسه Object ID است. سلسه مراتب MIB بصورت یك درخت (Nameless route) شرح داده می شود. شکل زیر سطوح واگذار شده توسط سازمانهای مختلف را در درخت MIB نشان می‌دهد.

Object IDهای بالاترین سطح، به سازمان های استاندارد سازی مختلف متعلق اند و Object IDهای سطوح پایینتر به سازمانهای وابسته آن اختصاص می یابند. فروشندگان می توانند شعبات و یا شاخه هایی را تعریف کنند که شامل موضوعات مدیریت شده برای تولیدات خودشان است و MIBهایی که استاندارد نشده اند، در شاخه های آزمایشی قرار می گیرند. برای مثال موضوعات مدیریت شده atln put می تواند بوسیله نام موضوعی ISO مشخص شود. ضمناً یك نمایشگر عددی برای رهگیری و رسیدن به موضوع مورد نظر نیز وجود

دارد. مثلا برای atln put مقدار این نمایشگر عددی معادل 1.3.6.1.4.1.9.3.3.1 خواهد بود.

SNMP V1

اولین نسخه از SNMP می باشد که به همراه ساختار اطلاعات مدیریتی مربوطه (SMI) و به ترتیب در RFC 1155 و RFC 1157 مورد بررسی قرار گرفته است.



(SMI: structure of management information)

(RFC: request for comments)

SNMP V1روی پروتکل هایی نظیر موارد زیر استفاده می شود:

UDP: user datagram protocol

IP: internet protocol

IPX: novel internet packet exchange

DDP: apple talk datagram protocol

CLNS: OSI connectionless network service

این پروتکل به صورت گسترده و به عنوان يك پروتکل مدیریتی در ارتباطات اینترنتی مورد استفاده قرار می گیردSMI .نیز با استفاد ه از ASN.1 قوانینی را جهت بررسی اطلاعات مدیریتی ارائه میدهد.

ASN.1: abstract syntax notation . One

SMIدارای سه مشخصه کلیدی است:

انواع داده با نماد سازمانی ASN.1 data types (ASN.1)

سه نوع از انواع داده عبارتند از:

- نام(Name) که به صورت Object ID استفاده می شود.
- ترکیب (Syntax) که نوع داده موضوع را معین می کند، مانندInteger/string
- رمزگذاری (encoding) تشریح می‌کند که چگونه اطلاعات مربوط به يك موضوع مدیریت شونده، به صورت يك سری از آیتم های data شکل دهی شده و برای انتقال روی شبکه مورد استفاده قرار می‌گیرد.
- انواع داده ویژه (SMI- specific data types)

به دو دسته تقسیم می شوند:

- انواع داده ساده (simple data types)که سه نوع داده ساده داریم و همگی دارای مقادیر واحدند:
- نوع داده integrate در رنجی از -2,147,483,648 تا +2,1447,483,647
- نوع داده octet stringدر رنجی از 0~65,535
- نوع داده object ID که مجموعه هایی از تمام ID هایی هستند که براساس قوانین موجود در ASN.1 در نظر گرفته شده اند.
- انواع داده با کاربر وسیع (Application- wide data types) که هفت نوع داده با کاربر وسیع داریم:
- نوع دادهnetwork address که برای نمایش یک آدرس از یک پروتکل خاص استفاده می شود. البته باید توجه داشت که در SNMP V1 تنها آدرس های 32 بیتی پشتیبانی می شوند.
- نوع دادهCounter که به صورت اعداد صحیح مثبت اند و شماره آنها افزایش می یابد تا به مقدار ماکزیمم خود برسد و سپس به صفر بر می گردد و باید توجه داشت که در SNMP V1، سایز کانتر ها 32 بیتی است.
- نوع داده gauges که اعداد صحیح مثبت هستند و مقدار آنها افزایش یا کاهش پیدا می کنند، ولی همیشه مقدار ماکزیمم خود را حفظ می کنند.
- نوع داده time ticks که برای نمایش برخی رخدادها تا یک صدم ثانیه استفاده می شوند .
- نوع داده opaque(مبهم) که برای نمایش یک رشته اطلاعات رمز نگاری قضاوتی شده (arbitrary encoding) که با نوع داده های SMIمطابقت ندارد، استفاده می شود.
- نوع داده Integrate برای نمایش اطلاعاتی که دارای مقادیر صحیح اند.
- نوع داده unsigned integrateبرای نمایش اطلاعاتی که دارای مقادیر غیر صحیح اند.
- جدول SNMP MIB table (MIB)

در این جدول می توان با فرامین SET ، GET NEXT،GETبه یک سطر مورد نظر دسترسی پیدا کرد.

فرمان های پروتکل SNMP V1

SNMP یک پروتکل ساده پرسش/ پاسخ سیستم مدیریت شبکه NMS یک درخواست می فرستند و تجهیزات مدیریت شده پاسخ مربوطه را بر می گردانند. این رفتار توسط چهار فرمان GET, GET NEXT, SET, TRAP اجرا می‌شود:

فرمانGET توسط NMS برای بازیابی مقدار object instanceهای یک agent استفاده می شود. در واقع کارگزار (agent) در پاسخ به فرمان GET مقادیر مربوط به instance Object ها را در یک لیست تهیه می‌کند.

فرمان GET NEXT توسط NMS برای بازیابی مقدار Object instance های بعدی در یک جدول و یا لیست استفاده می‌شود.

فرمانSET توسط NMS برای ست کردن یا قرار دادن مقادیر Object instance در جدول یا لیست یک کارگزار استفاده می‌شود

فرمان Trap توسط کارگزار برای آگاهی دادن به NMS از وقوع یک رخداد مهم و معنی دار بطور غیر هم زمان استفاده می‌شود.

SNMP V2

SNMP V2 در واقع توسعه تدریجی SNMP V1 است که براساس استانداردهای اینترنت در سال 1993 تهیه شده است و به لحاظ تئوری یک سریOperation های اضافی را ارائه می کند.

SNMP V2و ساختار اطلاعات مدیریتی(SMI)

SMI برای بررسی اطلاعات مدیریتی مورد استفاده در ANS.1 تعریف شده است و در RFC 1902 بررسی شده است در این ساختار نوع جدیدی از داده ها از قبیل Bit string، network counter،address اضافه شده است:

Bit stringفقط در ورژن دو تعریف شده است و شامل چندین Named bit است که یک مقدار را مشخص می کند

Network address نمایش دهنده یک آدرس از یک پروتکل خاص می‌باشد و باید توجه داشت که در ورژن یک، تنها آدرس های 32 بیتی و در ورژن دو، سایر انواع آدرس‌ها نیز پشتیبانی می شوند.

Counter مقادیر صحیح غیر صفرند که از یک مقدار شروع به افزایش می‌کنند تا به سطح ماکزیمم خود برسند و سپس به صفر بر می‌گردند و باید توجه کرد در ورژن یک،Counter ها 32 بیتی و در ورژن دو، هم 32 بیتی و هم 64 بیتی تعریف می‌شوند.

ماجولهای اطلاعات SMI

این ماجولها سه نوع هستند و برای مشخص کردن یک گروه از تعاریف مربوط به هم استفاده می شوند:

- ماجول MIB modules شامل تعاریفی از موضوعات مدیریت شده مرتبط می‌باشد.
- ماجول Compliance statement راه حلی اصولی برای بررسی یک گروه از موضوعات مدیریت شده (که از یک استاندارد یکسان پیروی می کنند) را ارائه می‌دهد.
- ماجول Capability statement که سطح دقیق پشتیبانی مورد مطالبه توسط یک کارگزار Agent را نشان می‌دهد.

فرمان های پروتکلSNMP V2

فرامین get، get next،set که در SNMP V1 وجود داشت در ورژن دو نیز وجود دارد با این تفاوت که برخی از آنها بهبود یافته اند و تعدادی فرمانTrap که تمام عملکردهای گذشته را پشتیبانی می‌کند ولی با این فرمت پیام متفاوت و جدیدی ارائه شده است. همچنین فرامین جدید Get bulk, Inform نیز اضافه شده اند:

- Get Bulk: این فرمان توسط NMS برای بازیابی بلاکهای بزرگ دیتا از قبیل سطرهای چندگانه یک جدول استفاده می‌شود. درصورتیکه با این فرمان نتوان تمام اطلاعات را بازیابی کرد قسمتی از آن (Partially results) دریافت می شود در حالیکه در ورژن یک چیزی دریافت نمی‌شد.
- Inform: توسط این فرمان NMS، اطلاعات Trap را به سایر NMS ها ارسال می کند و سپس پاسخ آنها را دریافت می‌کند.

مدیریت درSNMP

SNMP یک پروتکل مدیریتی توزیع شده است. لذا یک سیستم در این پروتکل می‌تواند بطور انحصاری به صورت یک NMS یا یک Agent یا هر دوی آنها عمل کند. در رابطه با موارد اخیر (تواما)، NMS نیاز خواهد داشت که یک سیستم سوالی و جوابی (System query) تجهیزات را مدیریت کند و اقدام به تهیه گزارشات محلی و ذخیره اطلاعات مدیریتی کند.

مدیریت درSNMP

SNMP فاقد هرگونه توانائی در شناسایی و تصدیق Authentication می‌باشد که این امر باعث آسیب پذیری در انواع سطوح امنیتی که عبارتند از:

Masquerading (تغییر شکل رخدادها): شامل یک اقدام غیر مجاز برای اجراء کارمندهای مدیریتی بوسیله فردی که یک عنصر مدیریتی مجاز را شناسایی کرده است.

modification Information (تغییر در اطلاعات): شامل یک اقدام غیر مجاز برای تغییر یک پیام تولید شده توسط یک عنصر مجاز است. این اقدام می تواند در مورد فرامین مربوط به مدیریت مالی و یا پیکربندی صورت گیرد.

message sequence modification & Timing (تغییر در توالی و زمانبندی): این حالت وقتی رخ می‌دهد که یک عنصر غیر مجاز اقدام به ثبت، ضبط، کپی ویا تاخیر انداختن یک پیام تولید شده توسط یک عنصر مجاز کرده و بعدا به آن پاسخ می‌دهد.

Results Disclosure (فاش سازی نتایج): این حالت وقتی رخ می دهد که یک عنصر غیر مجاز مقادیر ذخیره شده در موضوعات مدیریت شده را استخراج می‌کند و یا اینکه رخدادهای قابل توجه در حال تبادل بین Agent ها و Manager را می خواند و یاد می‌گیرد.

SNMP Interoperability

همانطور که گفته شده در حال حاضر SNMP V2 و SNMP V1 در دو محدوده کلیدی متفاوت و دارای عدم سازگاری اند، این محدوده ها عبارتند از:

- فرمتها
- فرامین پروتکل

پیام ها در ورژن دو، از فرمت های متفاوتی برای (protocol data unit) PDU ها و هدرها استفاده می‌کنند. در RFC1908، دو استراتژی همزیستی برای SNMP V1 و SNMP V2 تعریف شده است که عبارتند از:

Proxy agent:

یک agent در SNMP V2 می تواند به صورت Proxy روی تجهیزاتی که توسط snmpv1 مدیریت شده اند عمل کند. در واقع proxy agent، پیام های trapرا از SNMPV1 به پیام های Trap در SNMPV2 نگاشت می کند و سپس آنها را به NMS فوروارد می‌کند و بالعکس. نحوه عمل به صورت زیر است:

NMS(SNMPV2) یک فرمان را به یک Agent(SNMP V1) صادر میکند.

NMS پیام SNMP را به Proxy agent(SNMPV2) می فرستد.

Proxy agent پیام های set, get, get next را برای agent(snmpv1) بدون تغییر و تبدیل آنها فوروارد می کند.

پیام های get bulk توسط proxy agent به پیام های get next تبدیل شده و سپس به agent(snmpv1) فوروارد می‌شوند.

:Bilingual network management system

این سیستم مدیریت شبکه دو زبانه، از هر دو پروتکل (SNMPV1& 2) پشتیبانی می‌کند. برای پشتیبانی از این دو محیط مدیریتی مجزا، می بایست یک درخواست مدیریتی در NMS دو زبانه به یک Agent مرتبط شود و سپس NMS، اطلاعات ذخیره شده در یک دیتا بیس، محلی را برای نمایش اینکه Agent از SNMPV1 و یا از SNMPV2 پشتیبانی می‌کند را آزمایش می کند و براساس اطلاعات موجود در دیتابیس، NMS با Agent ی که از ورژن مناسبSNMP استفاده می‌کند، ارتباط برقرار می‌کند.

فرمت پیام درSNMPV1

پیام های SNMP V1 شامل دو قسمت هستند:

Header

Protocol data unit(PDU)

که در شکل زیر نشان داده شده است:

Headerشامل دو قسمت است:

1. شماره ورژن (Version. No) که ورژن پروتکل SNMP مورد استفاده را نشان می دهد.
2. انجمن (Community name) که یک محیط دسترسی برای گروهی از NMSها را تعریف می کند. در واقع نام انجمن یک فرم ضعیف از شناسائی Authentication است. زیرا تجهیزاتی که نام انجمن را نمی‌شناسد، نمی‌توانند از فرامین SNMP استفاده کنند.

SNMP V1- PDU protocol data unit

این قسمت شامل فرامین مشخص (get، set،.....) و عملوندهائی که نشان دهنده موضوع مربوط به این داد و ستد اطلاعاتی(Transaction) است، می‌باشد. فیلدهای PDU دارای طول متغییراند(که توسط ASN.1 تجویز شده است) و در شکل زیر نمایش داده شده است:

در سطرهای زیر تشریح فیلدهای مختلف شکل قبل آمد است

PDU Type: نوع PDU انتقال داده را مشخص می کند.

Request ID: درخواست های SNMP را با پاسخ ها مربوط می کند.

status Error: نشان دهنده یکی از شماره های خطا یا نوع خطا می باشد. توجه کنید که در این فیلد، تنها عملکرد پاسخ ست می شود و سایر عملکردها با مقدار صفر ست می شوند.

index Error: یک خطا را به یک نمونه موضوع ویژه مربوط می کند. توجه کنید که در این فیلد تنها عملکرد پاسخ ست می شود و سایر عملکردها با مقدار صفر ست می شوند.

bindings Variable: هر variable binding یک نمونه موضوع ویژه را به مقدار جاری خودش مرتبط می کند (بجز درخواست های get, get next، زیرا مقادیر آنهاIgnored است.

فرمت:Trap- PDU

- Enterprise:

نوع موضوع مدیریت شده ایی را که مولد Trap است، نشان می دهد.

- Agent address:

آدرس موضوع مدیریت شده ایی را که مولد Trap است را ارائه می کند.

- Generic trap type:

معین کننده یکی از شماره های ویژه کدهای Trap است.

- Time stamp:

مدت زمانی را که بین آخرین Network Reinitialization و تولید کننده یک Trap سپری شده است را ارائه می کند.

- Variable binding:

هر variable binding یک نمونه موضوع ویژه را با مقدار جاری خودش مرتبط می کند.

فرمت پیامSNMP V2

در این ورژن هم شمای کلی پیام به صورت شکل زیر شامل یک قسمت هدر و یک قسمت PDU است:

هدرهای پیام در SNMP V2 شامل دو فیلد هستند:

- Version number:ورژن SNMP ئی که استفاده شده است را معین می کند.
- Community name : نام انجمن به عنوان یک رمز عبور جهت دسترسی NMS ها به اطلاعات Managed device مورد استفاده قرار می‌گیرد. لازم به ذکر است دسترسی به اطلاعات SNMP بدون ارئه نام انجمن صحیح، امکان پذیر نمی‌باشد.

واحد داده در پروتکل(SNMP V2 (SNMP V2 PDU

فرمتهای واحد داده با عملکردهای پروتکل SNMP مرتبط است و همانطور که توسط abstract (ASN.1 no.1 syntax notation) تجویز شده است، فیلدهای آن دارای طول متغییراند.

در شکل زیر فرمت فیلدهای آن نشان داده شده است:

- PDU type:

نوع واحد داده انتقال داده شده را نشان می دهد (trap, set, response, inform, get next, get).

- Request ID:

درخواستهای SNMP را با پاسخ های مربوطه مرتبط می کند.

- Error status:

یکی از شماره های خطا را نشان می دهد.

- Error index:

یک خطا را با یک نمونه موضوع ویژه مرتبط می کند.

- Variable binding:

هر کدام ازVariable bindings ، یک نمونه موضوع ویژه را به مقدار جاری اش مرتبط می کند، بجز درخواست های get, get next که مقدار آنها Ignored است

Get Bulk PDU Format

شکل زیر فرمت آن را نشان می دهد:

- PDU Type:

عملکرد get bulk را مشخص می کند.

- Request ID:

درخواستهای SNMP را به پاسخ ها مرتبط می کند.

- Non repeaters :

وقتی که برخی از نمونه موضوعات فقط با یک متغییر قابل سنجش باشند و یا تنها با یک بار درخواست قابل بازیافت باشند، از این مقدار استفاده می شود.

- Max repetition :

نشان دهنده حداکثر دفعاتی است که تغییرات توسط فیلد Non repeaters نشان داده شده اند.

- Variable binding

مقدار جاری یک نمونه موضوع را مشخص می کند (بجز get ,get next که مقدارشان ignored است)

سیستم فونیکس ورژن 7

امکان ارسال و دریافت اطلاعات از انواع پروتکل های صنعتی از جمله ModBus، BacNet، LonWork ، SNMP را دارد .

برای راه اندازی سیستم SNMP کافی است داده های زیر را در اختیار کارشناسان شرکت ارگ قرار دهید:

1-لیست MIB دستگاه که از طریق این لیست بتوان کد OID برای نمایش اطلاعات را استخراج کرد .
2- IP دستگاه
3- کلمه ی رمز Community
این اطلاعات در فرم زیر وارد می شود :

SNMP AGENT

این قابلیت به کاربر این امکان را می دهد تا از طریق نرم افزار های کنترل شبکه بتواند مقادیر حسگرهای تابلوی ارگ را بخواند.

به این صورت که هر enid را ما تبدیل به oid میکنیم تا برای نرم افزارهای تحت شبکه قابل خواندن بشود.

به عنوان مثال:

1.3.6.1.4.1.39850.2 ابتدای همه oid ها است وثابت می باشد. اما ادامه oid نسبت به نوع حسگر متفاوت می شود.

1.3.6.1.4.1.39850.2.1001.0.9.1.1.11

به ترتیب از چپ و از 1.3.6.1.4.1.39850.2 به بعد:

1001: سریال فونیکس

0: شماره ABM

9: category مربوط به حسگر

1: خروجی / ورودی:0، خروجی:1

1: آنالوگ / دیجیتال:0 ، آنالوگ:1

11: شماره پورت