SNMP

د. فادي تركاوي

- في ظل الأنفتاح الكبير على الانترنت وعلى الشبكات وزيادة نسبة الأجهزة التى تقوم بعملية أدارة الشبكات مثل الروترات والسويتشات وزيادة فعاليتها يوم بعد يوم وحتى يستطيع مهندسي الشبكات مراقبة أجهزتهم وطريقة أدائها فكان لا بد لهم من إيجاد بروتوكول خاص للمراقبة عن بعد يعطيهم بيانات دائمة لكفاءة عمل الأجهزة على الشبكة وبما فيها كفاءة عمل المعالج والرامات وكمية نقل البيانات ضمن الشبكة والكثير من خصائص المراقبة الهامة

Functional Areas of Network Management

Configuration Management ادارة الاعدادات - inventory, configuration, provisioning

Fault Management ادارة الأخطاء – reactive and proactive network fault management

Performance Management إدارة الأداء - # of packets dropped, timeouts, collisions, CRC errors

Security Management إدارة الأمان - SNMP doesn't provide much here

Accounting Management إدارة الحسابات - cost management and chargeback assessment

Asset Management أدارة الاحصائيات - statistics of equipment, facility, and administration personnel

Planning Management إدارة التخطيط - analysis of trends to help justify a network upgrade or bandwidth increase

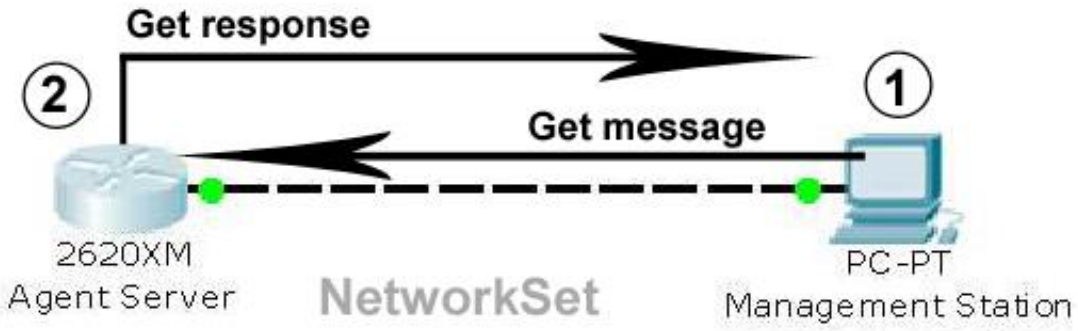
مقدمه

- تم البدأ في تطوير بروتوكول الـ SNMPعام ١٩٨٨ ليقوم بعملية المراقبة وهو بروتوكول مطور من بروتوكول آخر تم تطويره عام ١٩٨٧ أسمه SGMPأو Simple Gateway Management Protocolوجاء بعده بروتوكول آخر ظن الجميع انه سوف يحل مكان SNMPوهو CMIP secure Common Management Information Protocolلكن الأخير لم يدوم كثيرا كون الـ SNMP أثبت فعاليته بشكل أقوى على الساحة كونه يعمل على نظاقات واسعة وقابل للعمل مع جميع أنواع مكونات الشبكة(Network componentوفي الحقيقة بروتوكول الـ SNMPيقسم الى قسمين القسم الأول ويدعى Agentاو السيرفر وهو هنا الجهاز المراد مراقبته مثل الروتر، السويتش، الطابعة الخ أما القسم الثاني NMS(Network Management Stationأو العميل وهو لجهاز الذي سوف يستلم البيانات من الـAgent

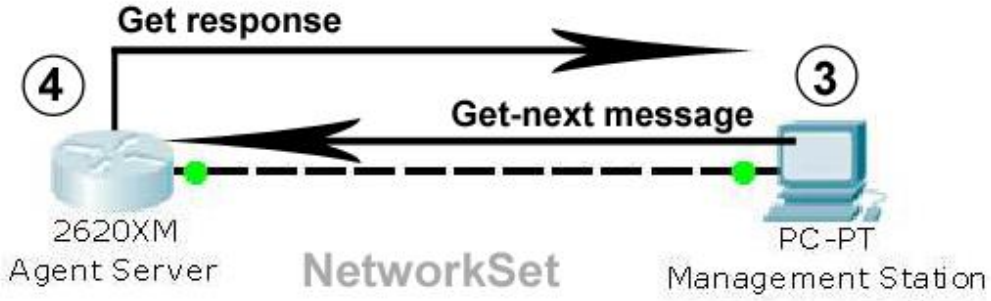
كيف يعمل الـ SNMP؟

- لنتفق أولا على الأشياء الاساسية التى يجب ان نعرفها وهي أن هذا البروتوكول هو أحد بروتوكولات الطبقة السابعة Application Layer ويستخدم الـ UDP/IP للأرسال ومن خلال البورت ١٦١ & ١٦٢ وهو ستخدم خمس أنواع من الرسائل للتواصل بين السرفر والعميل وهي GET, GET-NEXT, GET-RESPONSE, SET, and TRAP

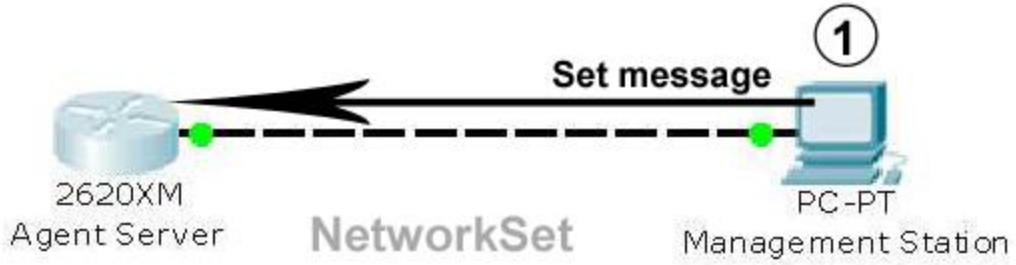
- فعندما يريد المدير ان يبدأ المراقبة يقوم بأرسال Get message الى الـ Agent وهو بدوره يرسل المطلوب على شكل Get-Response وكما نرى من الصورة القادمة



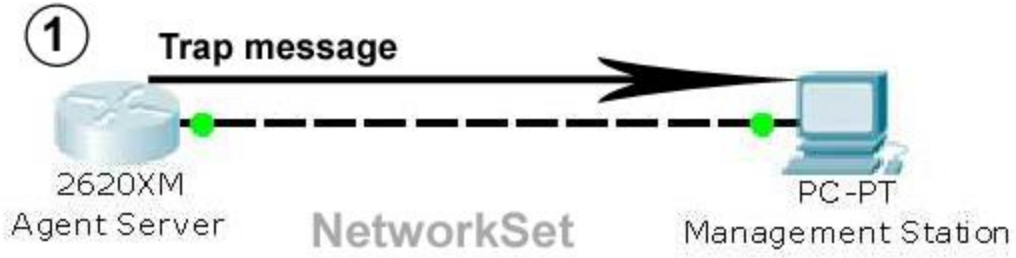
- أما بالنسبة للرسالة Get-Nextفهي عندما يريد أن يتابع عملية المراقبة ويرغب ي الحصول على المزيد من المتغييرات



- رسالة الـ Setترسل من قبل المدير لكي يطلب من الـ Agent لشيء يتم تحديده لتغير قيمة ما



- رسالة ال Trapترسل من قبل الـ Agentفي حال حدوث شيء ما في لجهاز المراقب مثلا توقف بورت عن العمل (Link Down/Upوهو في هذه الحالة يرسلها على البورت ١٦٢ بينما باقي الرسائل ترسل على البورت ١٦١



The Three Parts of SNMP

SNMP network management is based on three parts:

- SNMP Protocol
  - Defines format of messages exchanged by management systems and agents.
  - Specifies the Get, GetNext, Set, and Trap operations
- Structure of Management Information (SMI)
  - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
- Management Information Base (MIB)
  - A map of the hierarchical order of all managed objects and how they are accessed

إصدارات البروتوكول

- SNMPv1 -وهو يُعدّ قديماً نسبيّاً.
- SNMPv2cهناك أكثر من نسخة من SNMPv2أكثرها استخداماً SNMPv2cوالتي تمّ إضافة تعديلات وتطويرات فيها عن النّسخة الأولى السّابقة.
- SNMPv3وهو الأحدث من بين النّسخ. وأهمّ ما فيه هو إمكانيّة إضافة authenticationوكذلك encryptionللـ Packets.

SMIStructure of Management Information
بنية معلومات الإدارة

- يمكننا اعتبار SMIعلى أنها لغة لتعريف المتحولات والمعطيات المستخدمة والمخزنة في قاعدة المعطيات MIB، والهدف الأساسي من ذلك هو تبسيط قاعدة المعطيات بحيث إنه يمكن لها تخزين نمطين من المتحولات وهما النمط السلمي Scalarوالنمط المصفوفاتي ببعدين ٢ Dimentional arrayof scalars،قاعدة معطيات الإدارة ومعرف الغرض Management InformationBase & Object ID:
- إن MIBهي قاعدة المعطيات التي تحوي الأغراض وقيم المتحولات المرتبطة بها، والنسخة المستخدمة حالياً من قاعدة المعطيات هي النسخة الثاني MIB 2والتي تحتوي علي مجموعة من الأغراض.
وتجدر الملاحظة إلى ضرورة توفر حد أدنى من المعلومات في الـ MIB، وذلك لكي يستطيع المدير أن يتعامل معها، كما يمكن لكل مدير أن يضيف أغراض أخرى لقاعدة المعطيات لأهداف أخرى.
وتشكل قاعدة المعطيات شجرة تدعي MIB treeبحيث توضع الأغراض فيها بشكل هرمي بحيث يكون لكل غرض اسم وقيمة وعنوان . OID