What is a Network Management System?

As many businesses start to realize the importance of delivering reliable, secure wireless access, they also quickly find out that it's a lot more complex than simply throwing up some access points and handing out your password.As we know from the Wi-Fi engineering process, you're wireless network is never done, rather a constant work in progress.

However, managing your Wi-Fi network isn't easy to do, especially if you lack the experience and certifications required to know what you're doing. Whether you're upgrading an existing wireless system that's outdated or you're deploying wireless for the first time, there are two important components that have to be factored into your new WLAN design to maintain performance and proper security:

- Network management system
- Network access control

A network management system integrates with both your wireless and wired infrastructure, providing real-time visibility of your entire network.

With an NMS deployed you'll be able to proactively monitor things like:

- Access points
- Switches
- End-users and their devices
- Even what your end-users are doing while on the network, from streaming video to surfing the internet.

A network management system or platform (as it's sometimes called) allows you or a managed service provider to do this by monitoring how your system and the end-users/devices it's required to support are actually performing.

In addition to monitoring your network an NMS solution can also help you decrease the time it takes to troubleshoot wifi problems as well as avoid them all together.

Some network management systems have features that allow you to simulate what your end-users are experiencing on your current wireless system. This can allow you to stay ahead of potential problems and even test new additions to your network before they go live.

Benefits for your wired infrastructure

Switching plays a critical role in your ability to deliver reliable wifi access to your guests, customers and employees.

With the right network management system you'll be able to monitor things such as:

- Your switches up and down
- How many devices are connected to your switches
- Information about the type of device, IP addresses
- Troubleshooting- being able to see a specific AP is connected to X switch port
- Traffic information

Information you just won't have access to without this type of application or integration.

A Network management is all about monitoring your network to manage and maintain wifi performance on your very much alive, wireless system.

What is Network Access Control?

Network access control or NAC, is exactly what it sounds like-it controls access to your network. Network access control, or NAC, solutions support network visibility and access management through policy enforcement on devices and users of corporate networks.

Why is it important to have a NAC solution?

With organizations now having to account for exponential growth of mobile devices accessing their networks and the security risks they bring, it is critical to have the tools that provide the visibility, access control, and compliance capabilities that are required to strengthen your network security infrastructure.

A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.

Simple network management protocol (SNMP)

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) –

SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor network, detect network faults and sometimes even used to configure remote devices.

SNMP components –

There are 3 components of SNMP:

1. SNMP Manager –
   It is a centralised system used to monitor network. It is also known as Network Management Station (NMS)
2. SNMP agent –
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. Management Information Base –
   MIB consists of information of resources that are to be managed. This information is organised hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –

Different variables are:

1. GetRequest –
   SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
2. GetNextRequest –
   This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
3. GetBulkRequest –
   This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
4. SetRequest –
   It is used by SNMP manager to set the value of an object instance on the SNMP agent.
5. Response –
   It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
6. Trap –
   These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
7. InformRequest –
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

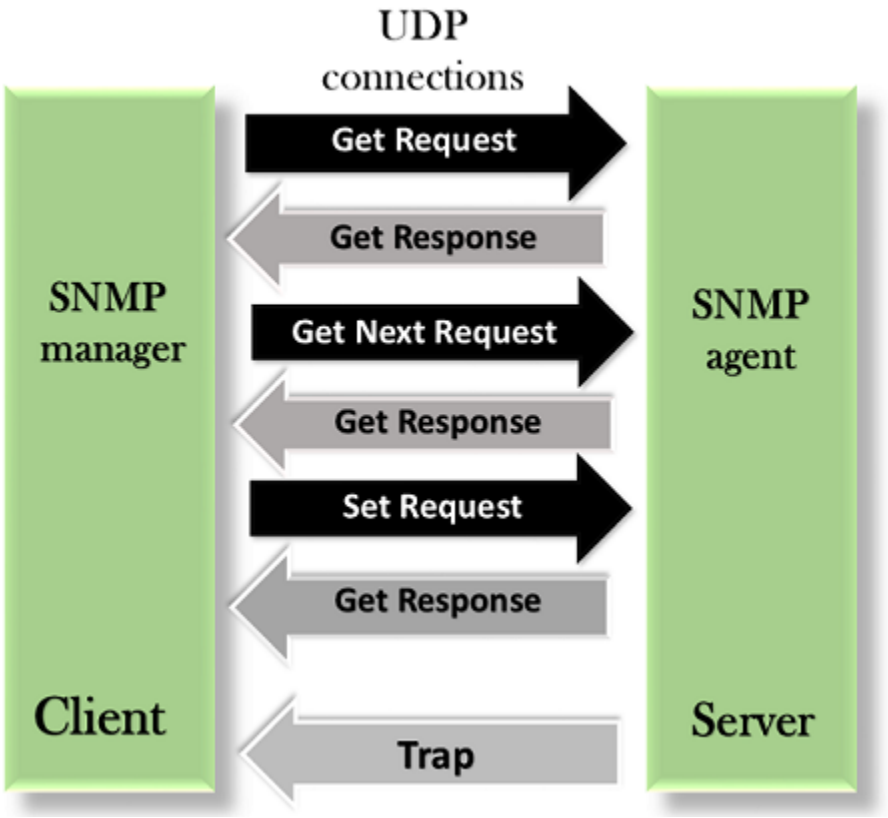
SNMP security levels –

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. noAuthNoPriv –
   This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
2. authNopriv – This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. authPriv – This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

SNMP versions –
There are 3 versions of SNMP:

1. SNMPv1 –
   It uses community strings for authentication and use UDP only.
2. SNMPv2c –
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. SNMPv3 –
   It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.



SNMP uses UDP

At the transport layer, the protocol used for SNMP message transportation is UDP. This is because UDP outperforms TCP in lossy networks where congestion is usually very high. One thing to remember is to fine tune the time-outs of UDP to fetch the best performance in lossy networks.

Also, the implementation of SNMP is kept simple. Simple as in simple network management protocol. Using TCP makes things far more complex and should be avoided in network management until and unless absolutely required.

****

The definition of SNMP MIB can be a bit cryptic to newbies. So lets, understand the concept of SNMP MIBs through a small example here.

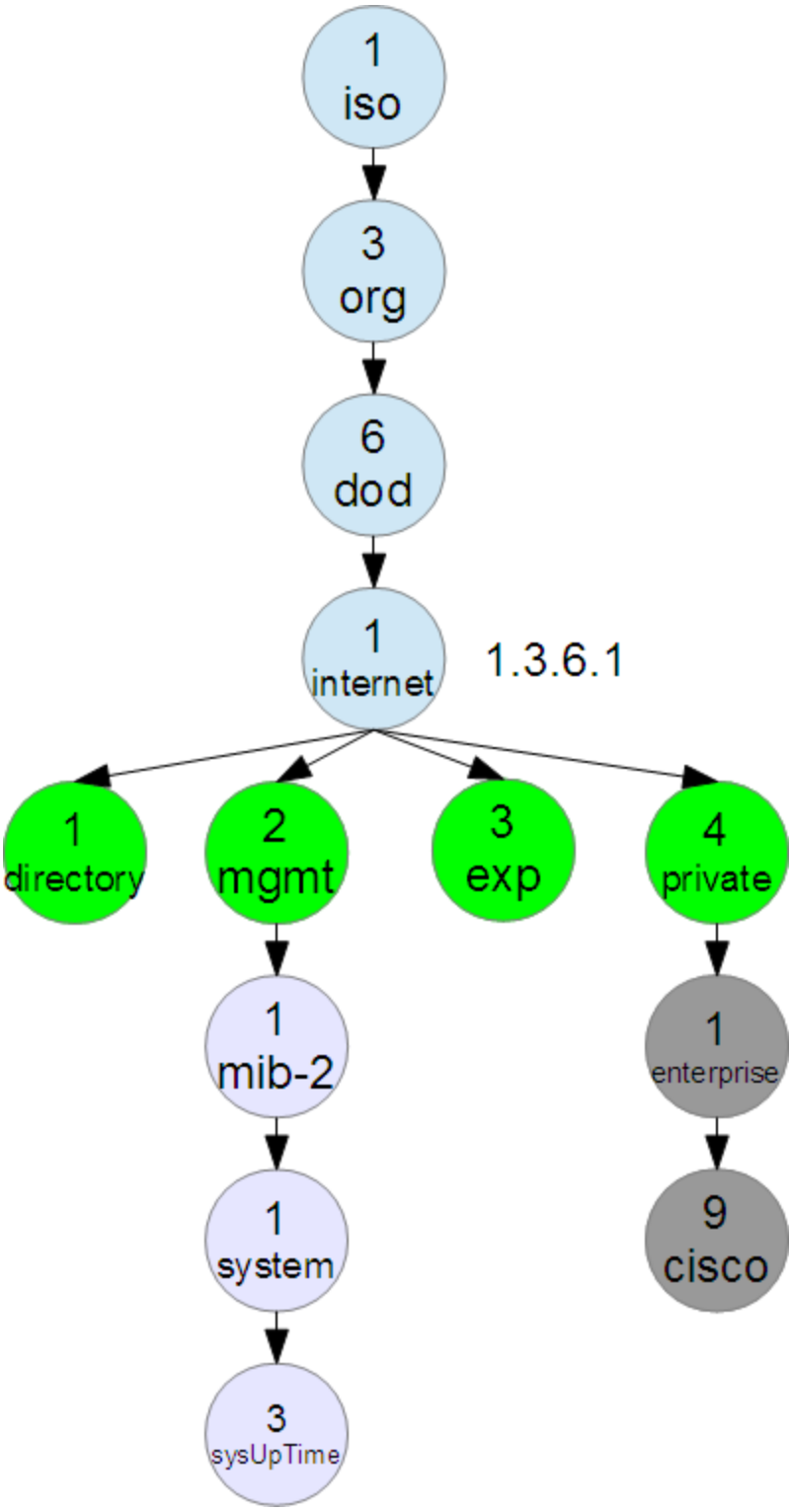
Suppose a mobile company server sends a poll question to all the company's subscribers through SMS. Being that company's subscriber, you get that message on your phone and you reply to it. Simple enough. Now, assume a situation where in a next poll the same company sends MMS this time. But, this time your phone is not able to comprehend that SMS due to some of its technology limitations (or any other problem). So, in this case you won't be able to receive and hence reply to the MMS.

So we see that the problem above happened because of lack of some MMS capabilities on your phone. So, in a nutshell your phone was not able to comprehend the incoming message successfully.

One could assume that same is the case with SNMP manager and an SNMP agent. The network protocol used between them is of-course SNMP but there has to be a protocol for composing and comprehending the information being queried. The information being queried could be anything like the disk usage of the network node that has agent running on it. So the crux is that there should be a standard structure in which the the query should be formed by the SNMP manager and the query should be understood by the SNMP agent.

The very basic component of the structure used in case of SNMP is an object. Every information that can be queried through SNMP is looked in terms of an object. For example, the a system's up time is an object known as 'sysUpTime'. Every object is has an associated ID known as Object ID or OID which is unique for every object. A group of objects form a MIB.

For example, if you take a look at the following image:



You will see that the whole information system in SNMP is in a form of tree where individual information nodes are objects having unique OIDs. For example the unique OID for the object sysUpTime is .1.3.6.1.2.1.1.3.0 . Looking at the figure above, you can easily deduce this OID. The '0' at the last of OID signifies that this object is a scalar and not a table.

There is also a textual description of the numeric OID. For example, the textual description of sysUpTime OID (presented above) is iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.

Computer Network | VIRTUAL TERMINAL

A network virtual terminal is a communications concept describing a variety of data terminal equipment (DTE), with different data rates, protocols, codes and formats, accommodated in the same network. This is done as a result of network processing where each device's data is converted into a network standard format, then converted into the format of the receiving device at the destination end.

In computing, a virtual terminal (VT) is a program that emulates the functionality of a classic terminal used during the early days of computing for accessing a server or a corporate mainframe.

In e-commerce, a virtual terminal is a Web-based solution that allows merchants to process credit card transactions. It is an alternative to a swipe machine.

A virtual terminal is also known as a terminal emulator.

A virtual terminal allows a PC to connect to a remote server, usually to perform a file transfer or run an application. In the past, this functionality used to be performed by a physical terminal, but is now emulated in software. The PC and the server may be running different operating systems, but can communicate using well-known network protocols such as Telnet, SSH, FTP, etc. A virtual terminal normally has a command-line interface, which requires typing cryptic commands to communicate with a server.

In open systems, a virtual terminal (VT) is an application service that:

1. Allows host terminals on a multi-user network to interact with other hosts regardless of terminal type and characteristics,
2. Allows remote log-on by local area network managers for the purpose of management,
3. Allows users to access information from another host processor for transaction processing,
4. Serves as a backup facility.

PuTTY is an example of a virtual terminal.

ITU-T defines a virtual terminal protocol based on the OSI application layer protocols. However, the virtual terminal protocol is not widely used on the Internet.