SNMPv3

Simple Network Management Protocol

Network Management -II

LEC (2)

NAJLAA FARAH
JOLII8425@GMAIL.COM

Outline

- SNMPV3 key features
- SNMPV3 architecture
- Elements of an entity
- SNMPV3 applications
- Command generator
- Command responder
- Notification originator
- Notification receiver
- Proxy forwarder
- SNMPV3 management information base
- Security
- Security threats
- Security model
- Message format

key features OF SNMPv3

- SNMPv3 performs the Same functions of SNMPv1 & SNMPv2 :
  - Monitoring
  - Managing
- Basic update of SNMPv3 is:
  - Security.
  - Administration operations

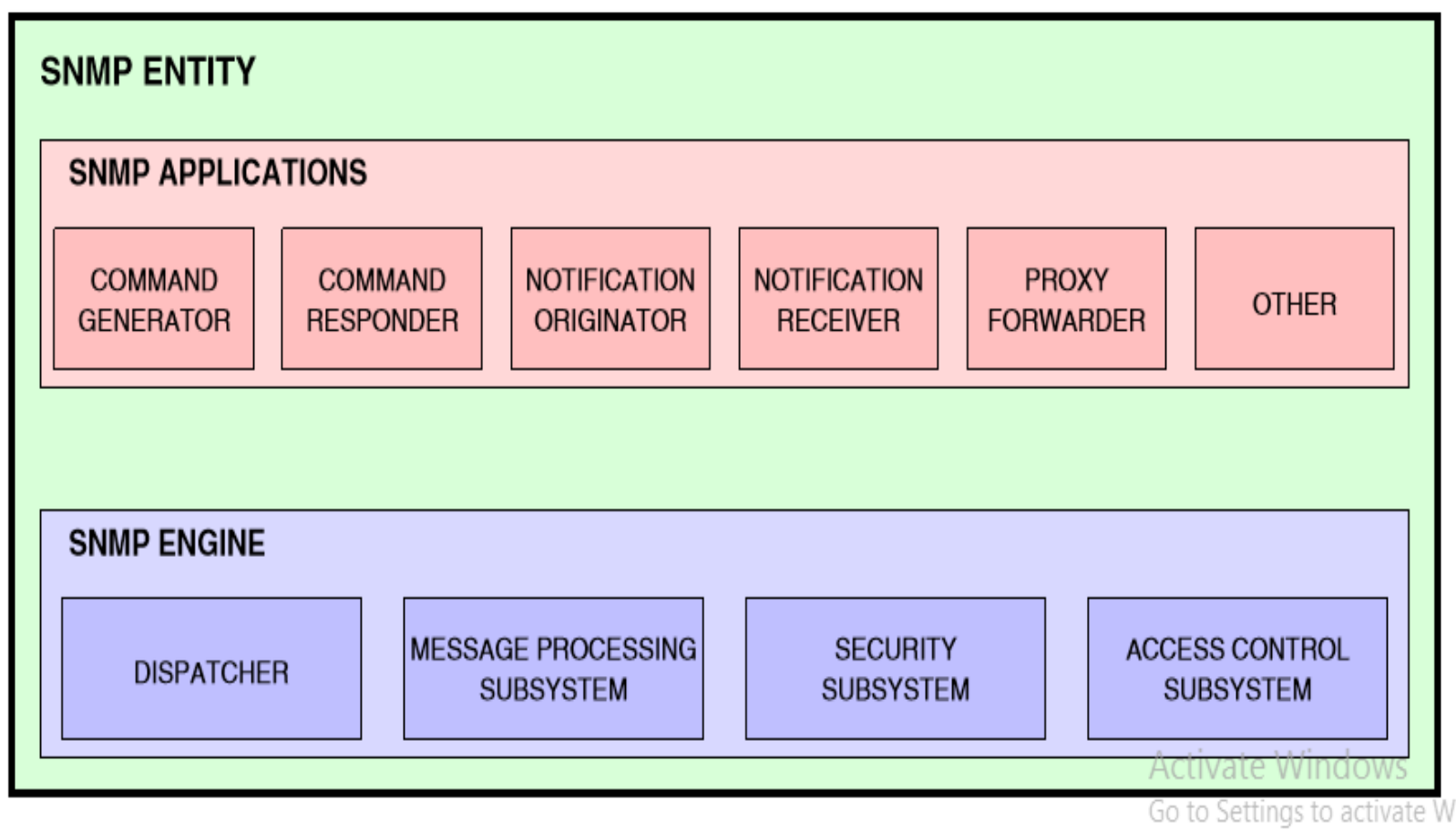
- وذلك بهدف بناء تصميم عام يتميز بنظام أمني مرن يجعل من الممكن إجراء عمليات التفاعل بين المدير وأجهزة الإدارة تحقق عمليات الأمن التي تطلبها المؤسسة.
- الهدف الآخر هو أن يتم تصميم نظام عمليات إدارة الأمن بسهولة.

Characteristics of SNMPv3

- SNMPv3 has number of Characteristics:

1. Message Authentication (Valid manager).
2. Privacy.
3. Authorization (View Based Access Control).
4. Remote Configuration.

SNMPV3 Architecture: Elements of an Entity



SNMPv3 Engine

SNMPv3 **Engine** defines four components of They are:

1. Dispatcher.
2. Message Processing Subsystem
3. Security Subsystem
4. Access Control System

Dispatcher

1. Send & receive messages.
2. Determine and **processing** type of message version (SNMPv1, SNMPv2, SNMPv3) (receiver mes).
3. Delivery of the message to message processing Subsystem also, to other entities (managers/agents in SNMP entity).

Message Processing Subsystem

- Do processing to outgoing message (SNMPv1, SNMPv2, SNMPv3) and other protocols.

Security Subsystem

Do Security processing uses:

User Based Security Model (USM) –SNMPv3

Community Based Security Model- SNMPv1, SNMPv2.

Access Control System

Do
allow/deny to MIB

SNMPv3 Applications

SNMPv3 formally defines five types of applications

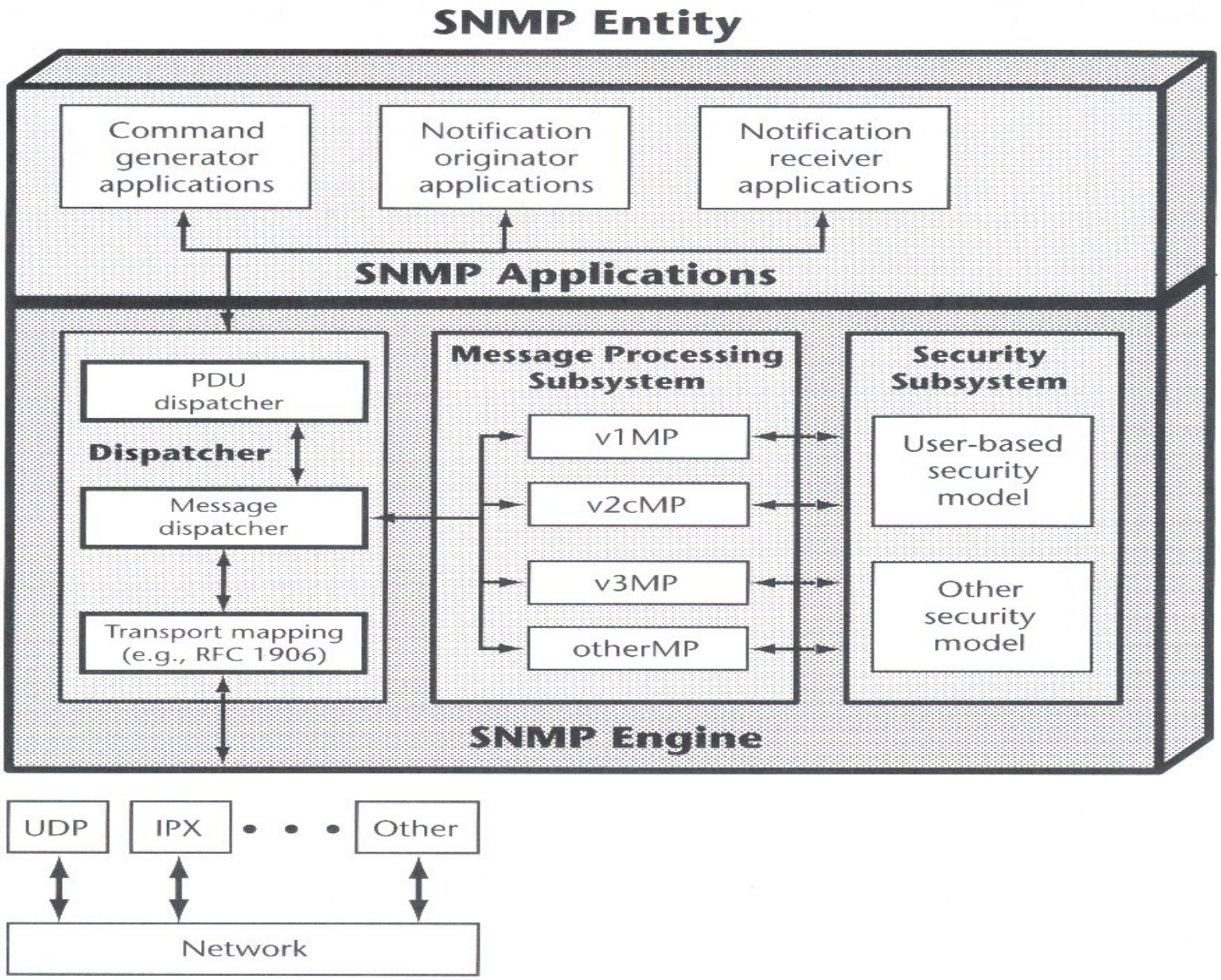
They are:

1.Command Generator -function (Generate different types to SNMPv3 messages)

2.Command Responder -function (reply to SNMPv3 messages)

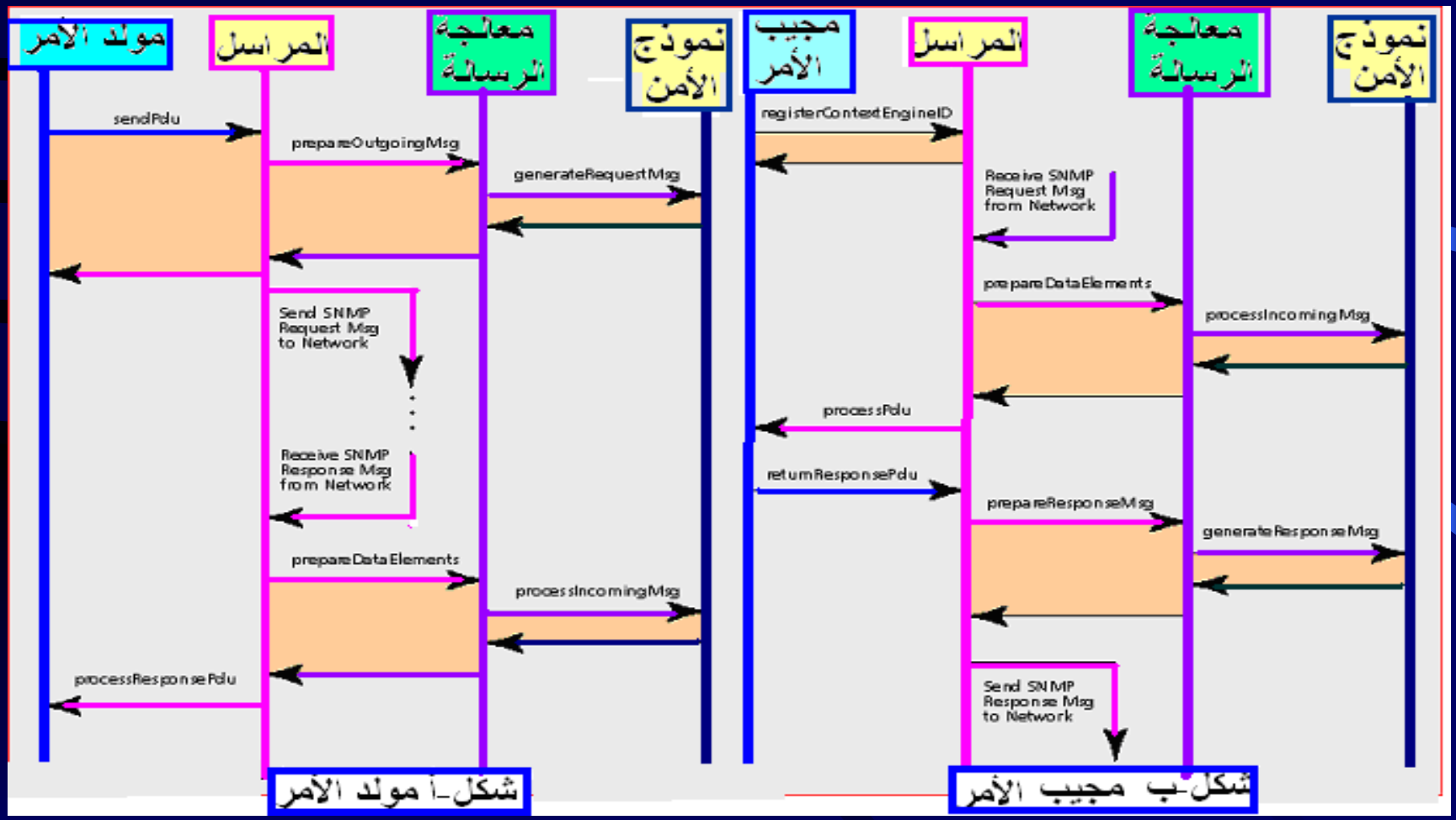
Con..

3. **Notification Originator -**function (send Trap and Inform messages).
4. **Notification Receiver –**function (Receive and process Trap and Inform messages)
5. **Proxy Forwarder -**function (Delivery of messages between SNMP Entity components)

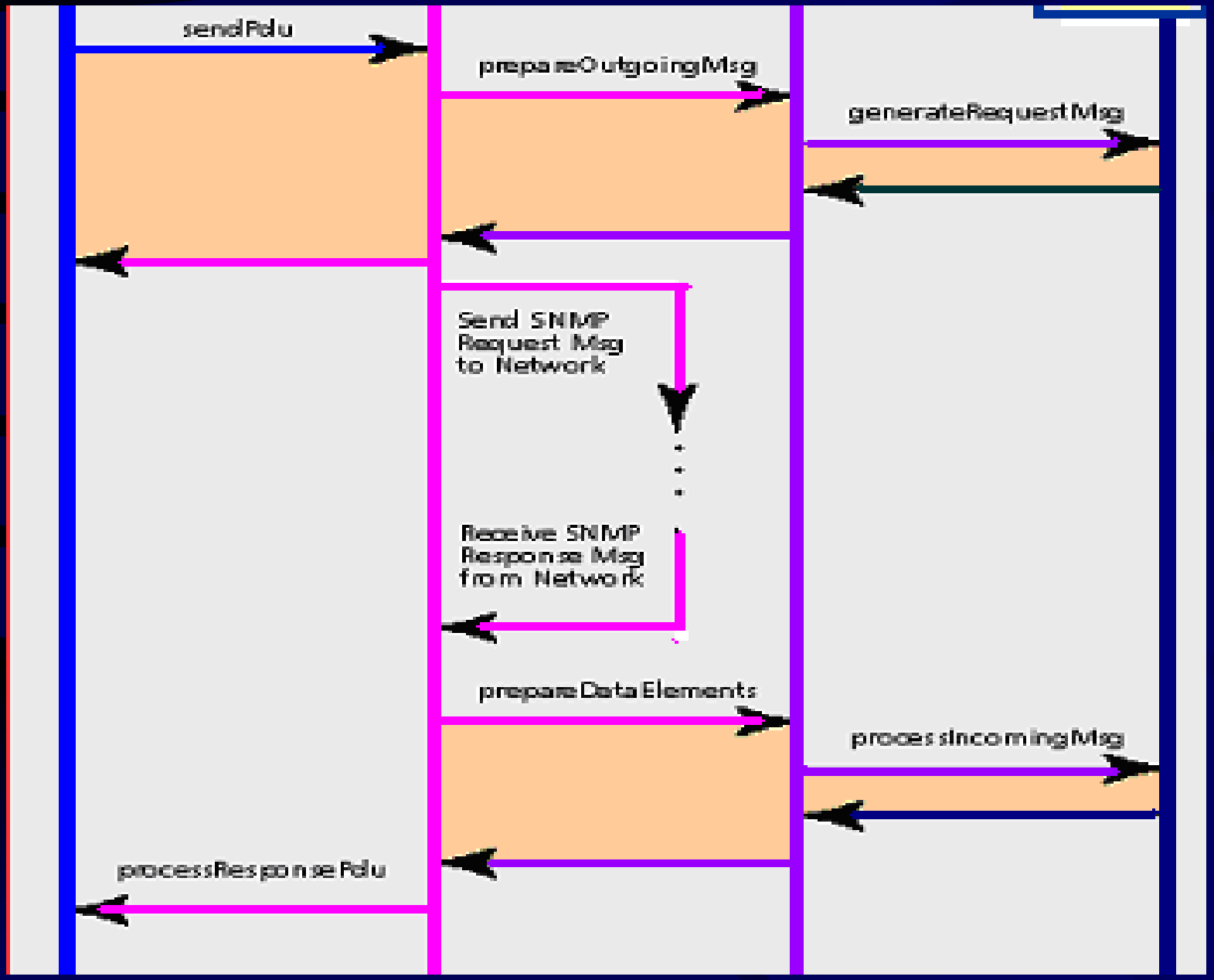


Entity of SNMPv3 manager and application

Operations of SNMPv3 Engine and application



- يتم إجراء الخدمات Services بين وحدات برامج التشغيل Modules في محطة التشغيل Entity في بروتوكول "سنمب-ف3" بواسطة
- معاملات Parameters
- ودوال أولية functions .
- تستخدم المعاملات لتمرير بيانات ومعلومات التحكم، بينما تستخدم الدوال لتحديد الوظائف المطلوب تحقيقها.


sendPdu
prepareOutgoingMsg
generateRequestMsg
Send SNMP
Request Msg
to Network
Receive SNMP
Response Msg
from Network
prepareDataElements
processIncomingMsg
processResponsePdu

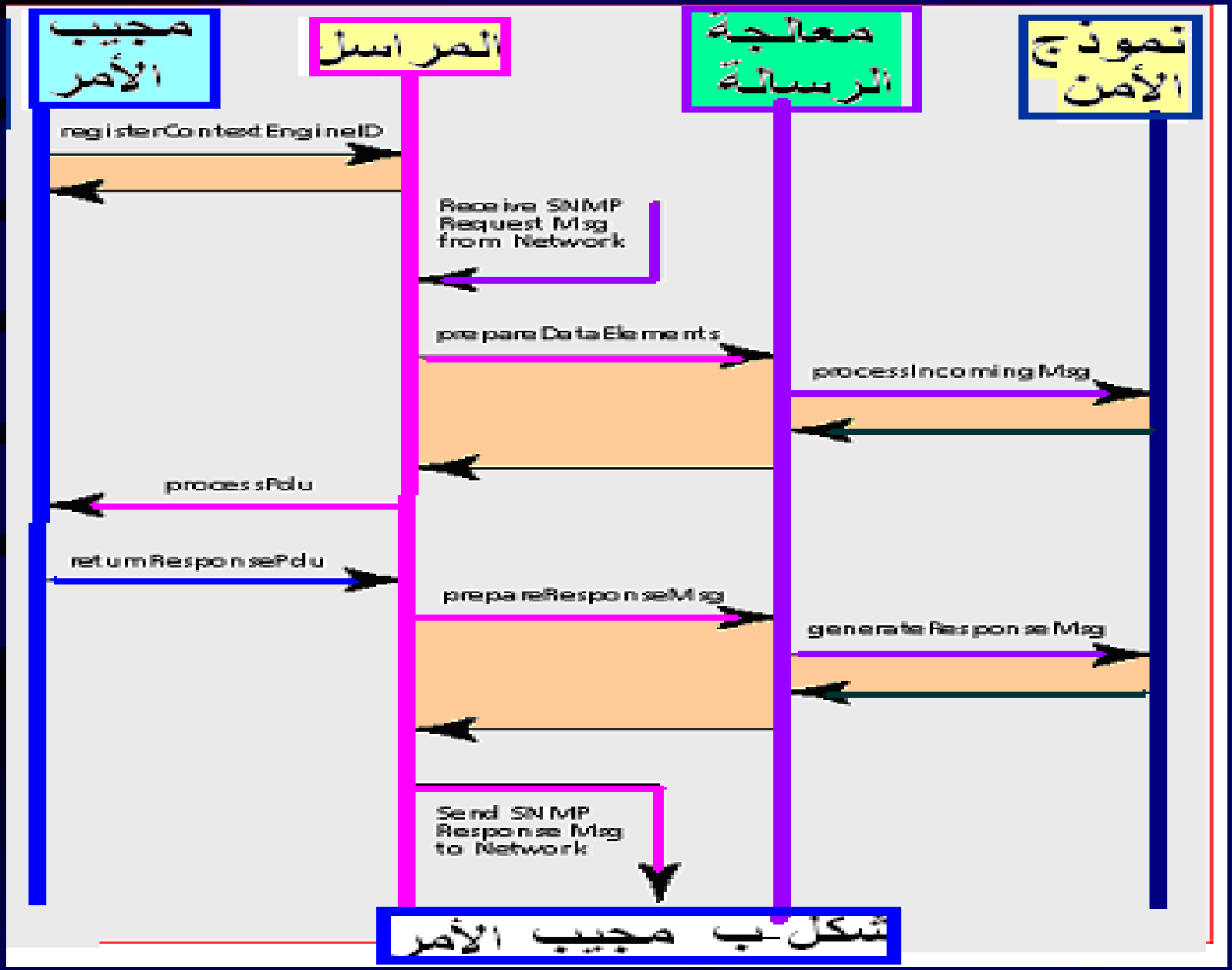
Command Generator Application

- Uses sendPDU and Generate processResponsePDU from dispatcher function.
- Provides **SendPDU** Call function the dispatcher with information (Destination, parameters security, PDU *sending)
- Do dispatcher *invoke to Message Processing Subsystem ⟶ Security Subsystem –message

- يقوم المنجز بعد ذلك بتسليم الرسالة المجهزة إلى مستوى النقل Transport Layer (مثلا UDP) للإرسال.
- إذا فشلت عملية تجهيز الرسالة، يظهر المنجز بيان وقوع خطأ، وذلك في قيمة دالة نداء العودة sendPDU .
- عندما تنجح عملية تجهيز الرسالة، يخصص مراسل محدد sendPDUHandle إلى وحدة PDU، و يتم ترجيع هذه القيمة إلى مولد الأمر.
- يخزن مولد الأمر القيمة sendPDUHandle لكي يستطيع توفيق الاستجابة المتتابعة من وحدة PDU مع الطلب الأصلي originalRequest.
- يرسل المنجز كل استجابة من وحدة PDU إلى تطبيق مولد الأمر الصحيح بواسطة استخدام الدالة processResponsePDU.

Command Responder Application

- **Uses four function of dispatcher are:**
- registerContextEngineID,
- unregisterContextEngineID,
- processPDU,
- returnResponsePDU.
- بالإضافة إلى دالة واحدة للتعامل مع نظام تحكم الوصول هي isAccessAllowed.



شكل ب مجيب الأمر

- **يقوم مستجيب الأمر بعد ذلك بتنفيذ الخطوات الآتية:**
- – يفحص محتويات طلب وحدة PDU. ينبغي أن يتوافق نوع العملية مع الأنواع المسجلة سابقا بواسطة هذا التطبيق.
- – يحدد إذا كان دخول هذه العملية الإدارية المطلوبة لوحدة PDU مسموحة أم لا. ولهذا الغرض يتم استدعاء الدالة accessAllowed .
- يبين معامل نموذج الأمن securityModelParameters عملية الاستجابة على هذه الدالة، وذلك بواسطة تحديد نموذج الأمن الذي ينبغي استخدامه، بواسطة نظام تحكم الوصول Access Control Subsystem. يتحقق نظام تحكم الدخول من سماحية الطلب الرئيسي requesting Principal (بواسطة فحص الاسم الأمني security-Name)، عند هذا المستوى الأمني (securityLevel) من طلب عملية إدارية (view-Type) لعنصر إداري (variableName)، في هذا السياق (contextName).

- – إذا تمت سماحية الدخول، يقوم مستجيب الأمر بتنفيذ العملية الإدارية، وتجهيز الاستجابة (الرد) على وحدة PDU. إذا أخفقت سماحية الدخول، يقوم مستجيب الأمر بتجهيز استجابة ملائمة لوحدة PDU لتبيان هذا الإخفاق.
- – يقوم مسجل الأمر بمخاطبة المنجز، بواسطة الدالة returnResponsePDU لإرسال استجابة لوحدة PDU.

Notification Originator Application

- يتبع نفس الخطوات المستخدمة في تطبيق مولد الأمر. عندما يطلب إرسال طلب إعلام لوحدة PDU، فإنه يستخدم دالة sendPDU، ودالة processResponsePDU بنفس الطريقة المتبعة في تطبيق مولد الأمر. عندما يطلب إرسال رسالة PDU trap يتم فقط استخدام الدالة sendPDU.

Notification Receiver Application

- **تطبيق مستقبل الإشعار:**
- يتَّبِعُ جزءاً من الخطوات التي يقوم بها تطبيق مستجيب الأمر. ينبغي على مستقبل الإشعار أن يقوم بالتسجيل أولا، لكي يستقبل الإشعار Inform أو المصيدة Trapمن وحدات PDU. يتم استقبال أنواع وحدات بيانات البروتوكول PDUs بواسطة الدالة processPDU. يتم الاستجابة على رسالة الإشعار Inform PDU بواسطة استخدام رسالة الاستجابة returnResponsePDU.

Proxy Forwarder Application

- **تطبيق الوكيل المعاون:**
- يستخدم دوال المنجز لكي يرسل رسائل "سنمب–ف3". يقوم الوكيل المعاون بمعالجة أربعة أنواع من الرسائل هي:
- أ – رسائل تحتوي على أنواع وحدات PDU من تطبيق مولد الأمر. ويحدد آلة "سنمب–ف3" الهدف أو الآلة الأقرب للهدف ويرسل الطلب requestPDU المناسب.
- .

- ب – رسائل تحتوي على أنواع وحدات PDU من تطبيق منشئ الإشعار، ويحدد آلة "سنمب–ف3" التي ينبغي أن تستقبل الإشعار، ويرسل الإشعار المناسب لوحدات PDUs.
- ج – رسائل تحتوي على نوع استجابة response PDU. ويحدد الطلب المرسل سابقا أو الإشعار. عندما يتوافق مع هذه الاستجابة، يرسل استجابة مناسبة لوحدة PDU.
- د – رسائل تحتوي على مبين تقرير report indicator . إن وحدات مبين التقرير تحقق الاتصالات بين آلات بروتوكول "سنمب–ف3". يحدد الوكيل المعاون الطلب المرسل سابقا أو الإشعار، عندما يحدث توافق مع مبين التقرير، يقوم بإرجاع مبين التقرير إلى مرسل initiator الطلب أو الإشعار

User-based Security Model (USM)

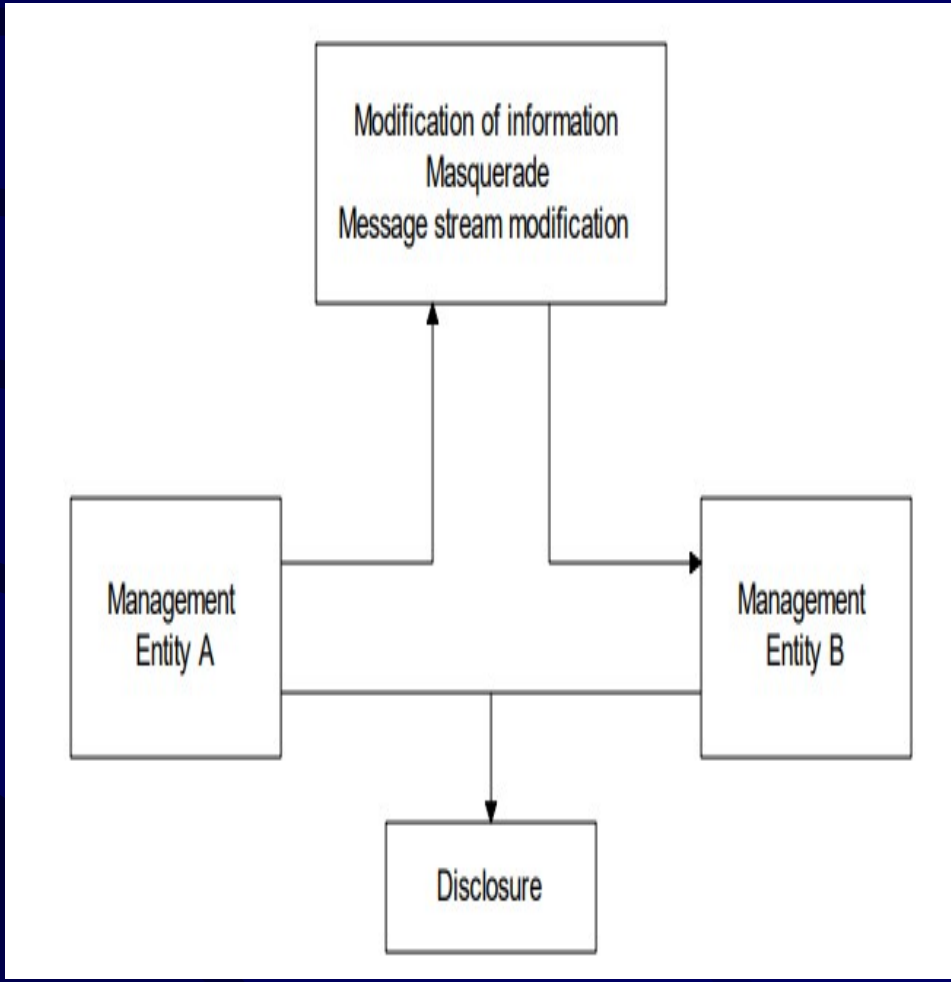
- The User-based Security Model (USM) is used by SNMPv3.
- USM is used for the following reasons:
- Authentication and Privacy.

Security Threats

USM designed to security from four basic Threat:.

1. Modification of information
2. Masquerade
3. Message stream modification
4. Disclosure

- As shown in following figure:



تهديدات أخرى

- يوجد بعض التهديدات الأخرى التي لم يتم تصميم نموذج USM لإجراء عمليات الحماية منها وهي:

➢ – **إنكار الخدمة Denial of Service:**

- المقصود بهذا التهديد هو أن يقوم المهاجم بمحاولة منع المستخدم الشرعي من استخدام الشبكة. حيث يقوم المهاجم هنا بمحاولة منع المبادلات التي تتم بين المدير والوكيل. ويحتاج هذا النوع من التهديدات وجود وسائل أمنية أخرى، خلاف الموجودة في بروتوكول إدارة الشبكة.

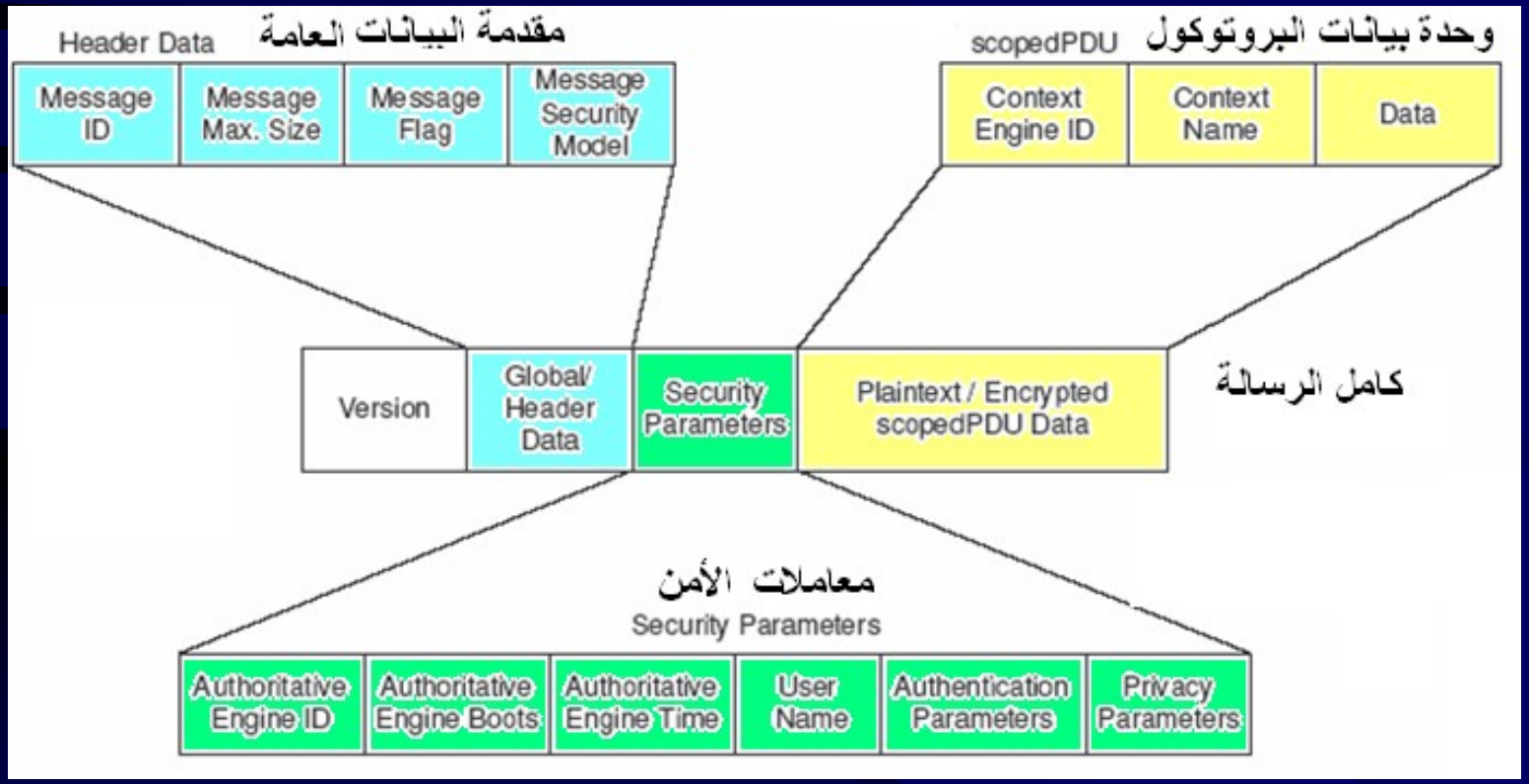
- **تحليل الحركة Traffic Analysis:**

- قد يتمكن المهاجم من مراقبة النموذج العام لحركة مرور الرسائل بين المديرين والوكلاء. إن نماذج تحليل حركة مرور الرسائل يمكن معرفته بواسطة بروتوكول إدارة الشبكة، باستخدام أوامر " SNMPV3 " على فترات منتظمة. ولذلك لا يوجد ميزة هامة للحماية ضد ملاحظة المهاجم نماذج حركة مرور الرسائل.

وسائل الحماية:

- للحماية من التهديدات السابقة فإن نموذج أمن المستخدم USM في بروتوكول "SNMPV3" يستخدم بروتوكولين مختلفين للتوثيق هما بروتوكول HMAC-MD5-96 وبروتوكول HMAC-SHA-96.
- ويستخدم نموذج USM مفتاحين، أحدهما خاص لتحقيق الخصوصية هو privKey، والمفتاح الآخر لتحقيق التوثيق وهو authKey. ويستخدم هذان المفتاحان للمستخدمين المحليين Local Users ، والمستخدمين عن بعد Remote Users. وأن هذين المفتاحين لا يتم تخزينهما في قاعدة المعلومات الإدارية MIB في الشبكة. ولذلك من غير الممكن الوصول إليهما مباشرة من خلال رسائل SNMPV3 get,set

Message format FOR SNMPV3



READ

- جدول2.3 تابع عناصر الأشكال المكونة لرسالة بروتوكول "SNMPV3

Thanks