إدارة الشبكة

مقدمة

- أصبحت الشبكات العامة "الاتصالات" والحاسوبية وأنظمة المعالجة الموزعة جزءاً أساسياً ومهماً في حياتنا اليومية وأصبحت أكثر تعقيداً بسبب نموها المتزايد والذي فرض على المختصين في مجال الشبكات ومنهم العاملون في مجال إدارة الشبكات إيجاد المزيد من التطبيقات الشبكية القادرة على مساعدة مدراء الشبكات في إدارتها والتحكم بها لكي تدعم المزيد من المستخدمين، وبشكل عام للحفاظ على الأداء الجيد للعمل في ظل وجود شبكة أو شبكات كبيرة، فإنه لابد من استخدام الأدوات الإدارية لإدارة هذه الشبكات ولاسيما الشبكات التي تتضمن أجهزة بأنواع وماركات متنوعة، علاوةً على ذلك فإن هذه الأدوات تساعدنا في زيادة اللامركزية لخدمات الشبكة وأهمية محطات العمل التي تعتمد على نظام العميل/الخادم أو ما يعرف بـ: Client/Server.

- إن إدارة الشبكات تتطلب نظام إدارة شبكي يتضمن مجموعة شاملة من أدوات التحكم التي تتكامل مع البرمجيات وأجهزة شبكة الاتصال لجمع البيانات حول عمل الشبكة والتحكم بها، وعندما يتم تحديد كيفية استخدام الجهاز فيمكن للإدارة إعداده واختيار البرنامج المناسب ومجموعة من الصفات والقيم لهذا الجهاز.

- تتكون شبكات البيانات وشبكات الاتصالات الحديثة من مكونات فردية ونظم منطقية والتي يمكننا تهيئتها لأداء العديد من التطبيقات بكل تنوعاتها، فمثلاً الجهاز نفسه يمكن إعداده للعمل كموجه اتصالات Router، أو كعقدة طرفية Node أو كلاهما، وعندما يتم تحديد كيفية استخدام الجهاز فيمكن للإدارة إعداده واختيار البرنامج المناسب ومجموعة من الصفات والقيم لهذا الجهاز (مثلاً طبقة النقل لإعادة الإرسال المؤقت).

- مع أن التصميم الجيد للشبكة واستخدام التقانات والأجهزة المناسبة هما من الخطوات المطلوبة للشبكة غير أنها غير كافية إذ تحتاج أيضاً إلى إدارة الشبكة بشكل سليم.

- سنعمل على توصيف التتابعات أو التطورات التي تسمح لنا بفهم وإدراك بيئة إدارة الشبكة والتي يمكن أن تجيب على ضروريات وفرضيات التنظيم.

- في المرحلة التمهيدية سنتعرف على الخواص الأساسية للشبكة التي يراد إدارتها.

- أهم البروتوكولات المستخدمة في إدارة الشبكة ولاسيما SNMP بكافة نسخه المتتابعة.

- بعدها سنركز على وظائف الإدارة التي تسمح لنا بتحديد حاجاتنا لكي نستطيع إدارة الشبكة وما هي الحلول الأساسية لإدارة الشبكات.

المشاكل العامة التي تواجه الشبكة

- ضياع التوصيل (وصلة، العقدة، الوسط الملائم).
- مضاعفة عنوان IP.
- مشاكل القطع.
- تهيئة الشبكة.
- مشاكل الأداء.

الصعوبات أو التحديات
التي تواجه مدراء تكنولوجيا المعلومات

- الوثوقية.
- مشاكل الزمن الحقيقي.
- التطور التكنولوجي المتسارع.
- بيئة إدارة المخدم/ الزيون.
- المعيارية.
- المشاكل غير المتوقعة.
- الإدارة المركزية.
- ... إلخ.

إدارة الشبكة

- **تعريف:**
  - **إدارة الشبكة والخدمات.**
  - **إدارة، تشغيل، مراقبة، صيانة، ... إلخ.**
- **الهدف:**
  - **التأكد من أن المستخدمين للشبكة يحصلون على جودة خدمات تكنولوجيا المعلومات المتوقعة.**

نظام إدارة الشبكة

- هو عباره عن مجموعه من الأدوات التي تقوم بعملية المراقبه والتحكم بالشبكة.
- يحتاج مدير الشبكة للتعرف على أوضاع الأجهزة العاملة في الشبكة وأوضاع الوصلات، ومدى الحمل عليها والعديد من القراءات اللازمة لتتبع حالات الشبكات.

- تعالج إدارة الشبكة الفعاليات أو النشاطات التي تضمن عمل الشبكة والوصول للخدمات التي يمكن أن تقدمها الشبكة وهذه الفعاليات يمكن أن تكون مجمعة وفق وظائفها أو مهمتها. إن تحليل أو تجزئة العمل يرتب بواسطة OSI لخمس مجالات من الإدارة وهي:
  - إدارة التهيئة Configuration. – إدارة الأخطاء Faults.
  - إدارة تقدير الخصائص Performances. – إدارة السعر.
  - إدارة الأمن والسرية. سيتم دراسة كل واحدة منها بشكل مفصل لاحقاً.

- والسؤال البديهي هو ما الذي نريد إدارته؟

- يتوجب على العديد من مستويات الإدارة أن تكون مبينة ومعينة وذلك لتؤمن المنفعة والفائدة المرجوة، فالصفة المميزة يمكن أن تكون مطبقة انطلاقاً من العناصر المكونة للشبكة مثل تجهيزات الشبكة (مكونات مادية وبرمجية ومستخدمين)، فعلى سبيل المثال:

– إدارة البنية التحتية للشبكة: وهذا يخص إدارة كلاً من عناصر الشبكة (كل التجهيزات التي تكون موصولة بالشبكة وكذلك البرامج التي تكون موجودة فيها) والبرامج التي تؤلف أو تبني مختلف شبكات المؤسسات أو الشركات.

– إدارة Desktop: وهذا يعني نسبياً كل النواحي لإدارة نقاط منافذ الشبكة، وهذا يعني بالعموم إدارة محطات الطرفيات وكل البرامج التي تكون محملة بهذه الطرفيات، فعلى سبيل المثال لا الحصر نذكر: نظام استثمار الشبكة، تطبيقات وخدمات الاتصال الموضوعة بالخدمة، ... إلخ.

أهداف إدارة الشبكة

آ- الأهداف العامة، وتتمثل بـ:

- فهم واستيعاب ما هي الشبكة والتصورات الأساسية لإيصال المعلومات أو البيانات العابرة للشبكة.
- فهم الرهانات الاستراتيجية للشبكة.
- تآلف وانسجام الوظائف الأساسية لإدارة الشبكة.
- الإلمام والإطلاع على مختلف الهندسيات المعمارية للشبكة.
- المعرفة الجيدة للحدود الحالية لإدارة الشبكة.

ب- الأهداف النوعية، وتتمثل بـ:

- معرفة مميزات وخواص وظائف الشبكة ومعرفة مختلف بيانات الشبكة.
- تمييز الشبكة المعلوماتية عن شبكة الاتصالات.
- تحديد الوظائف الأساسية لإدارة الشبكة.
- معرفة وتمييز اختلافات الهندسيات المعمارية لبروتوكولات الاتصال.
- إشراك أو ربط معماريات إدارة الشبكات بمختلف نماذج الشبكات.
- المقارنة بين SNMP, OSI, ...etc.
- تحديد وتوصيف الوظائف الخمس الأساسية لإدارة الشبكة من أجل البحث عن الحل الأمثل.

بيئات إدارة الشبكة

- بيئة الإدارة: هي مجموعة التجهيزات مع بعضها البعض والمرتكزة على نفس التكنولوجيا والتي تسمح بوضع أغراض إدارة الشبكة بالخدمة، ويوجد صنفان لهذه البيئات وهما:

  - بيئة قياسية (عامة): وتكون مرتكزة على هندسة معمارية مفتوحة وبروتوكولات تسمح بإدارة التجهيزات التي تضع بالخدمة وظائف الإدارة العامة.

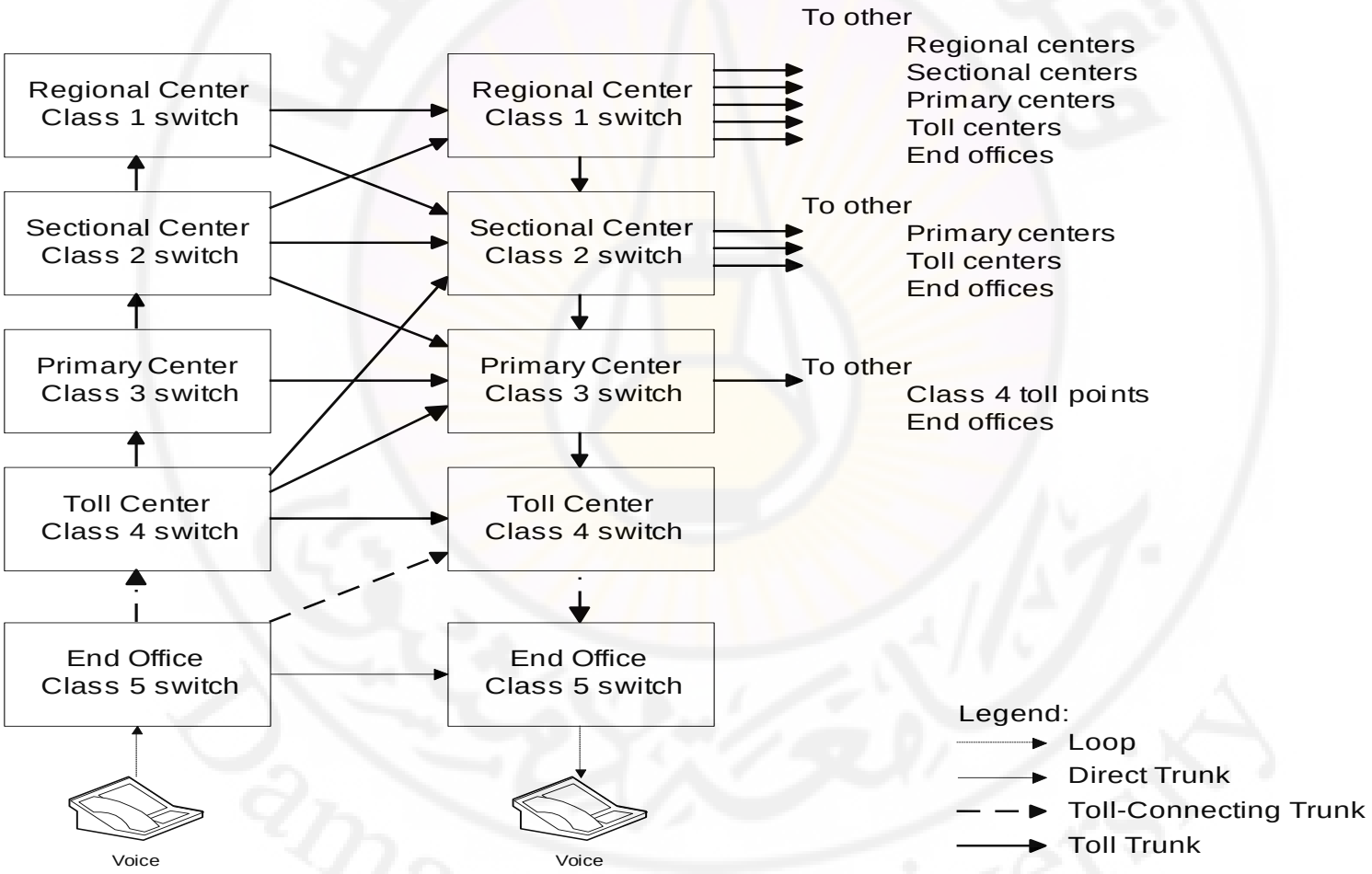
  - بيئة خاصة (مملوكة): وتكون مرتكزة على بروتوكولات الاتصالات غير العامة والتي لا تسمح بشكل عام إلا بإدارة التجهيزات الخاصة.

شبكة الهاتف

- مميزاتها:
  - وثوقية: تنفذ ما هو متوقع منها.
  - يمكن الاعتماد عليها عندما يرغب ويحتاجها الشخص.
  - جودة جيدة بالتوصيل وسماع الأطراف لبعضهم البعض بشكل حسن.

- الأسباب:
  - تخطيط جيد، تصميم وتحسين مستمر بالخدمات.
  - تشغيل جيد وإدارة للشبكة.

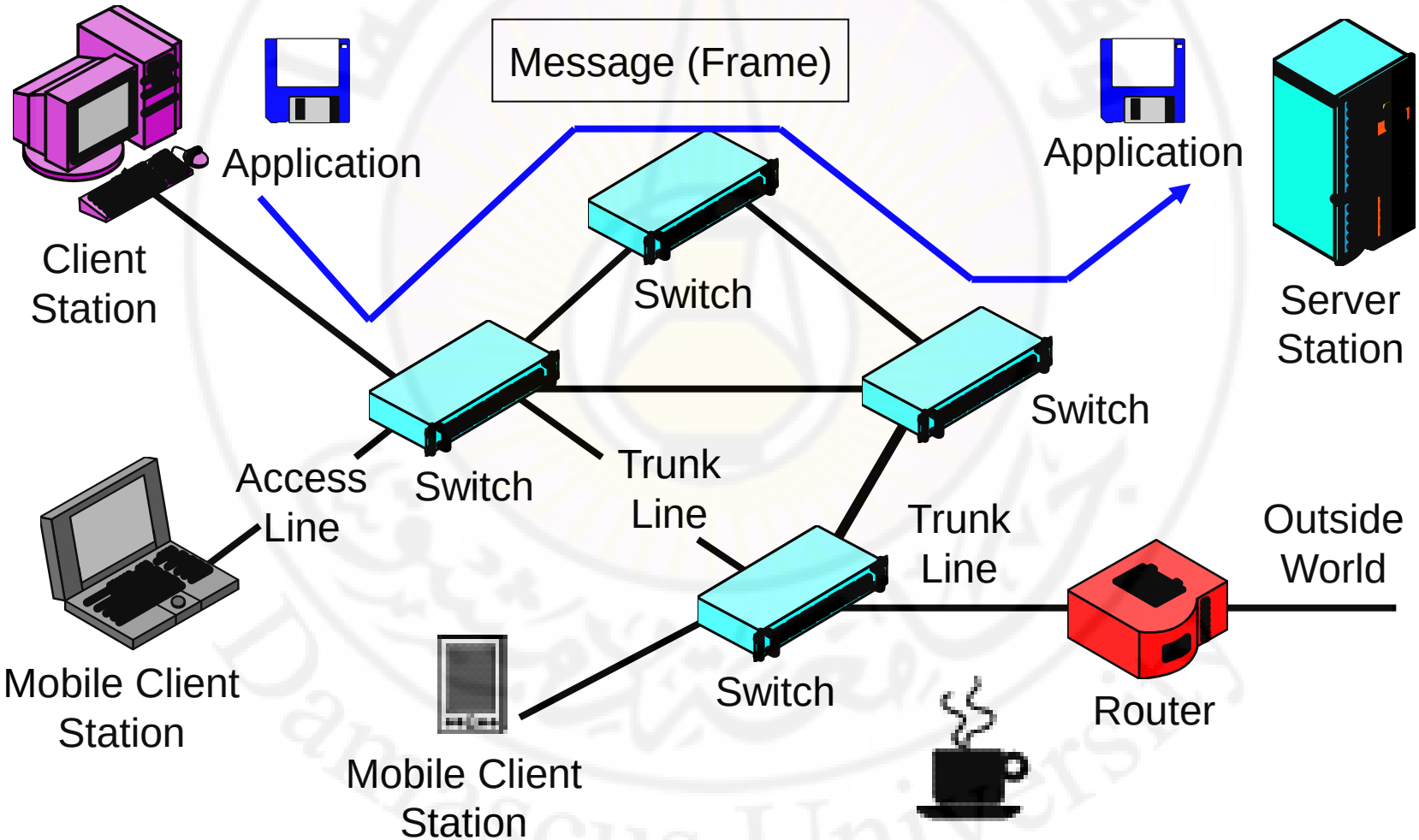
نموذج (موديل)شبكة الهاتف



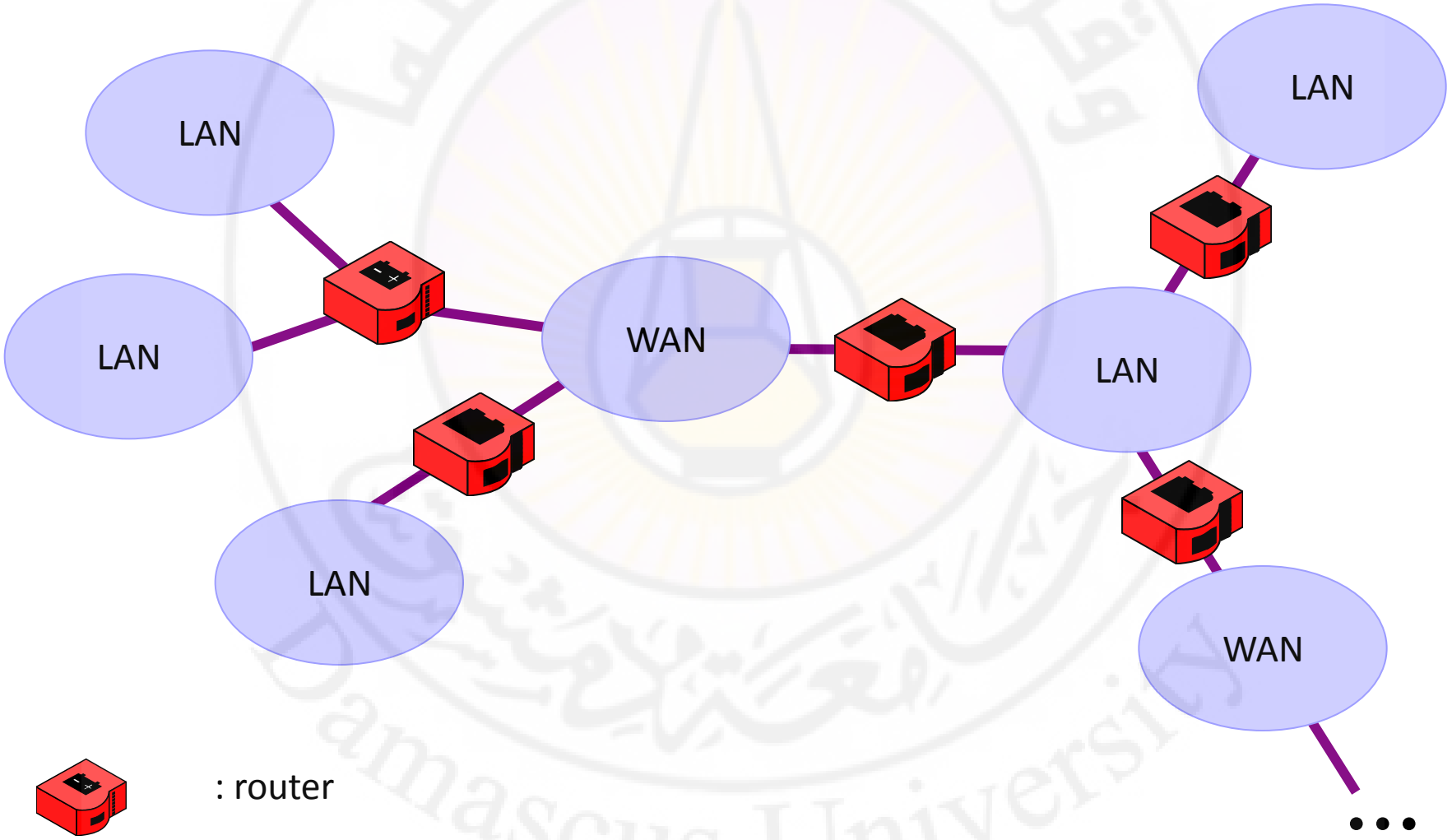
مركز تشغيل الشبكة
NOC : Network Operation Center

- مراقبة بارمترات الشبكة مثل: معدل إرشال الإشارة، ضياع الإرسال، انقطاع الاتصال، ... إلخ.
- إدارة خلال الزمن الحقيقي للشبكة.
- أنظمة صيانة التي تقيس ضياع الإشارة، وجودة الخدمة، ... إلخ.
- أنظمة قياس حركة المكالمات.
- أنظمة التشغيل تكون موزعة على المقاسم.
- إدارة الشبكة تنفذ بشكل مركزي هذه الأمور التي ينفذها مركز تشغيل الشبكة.

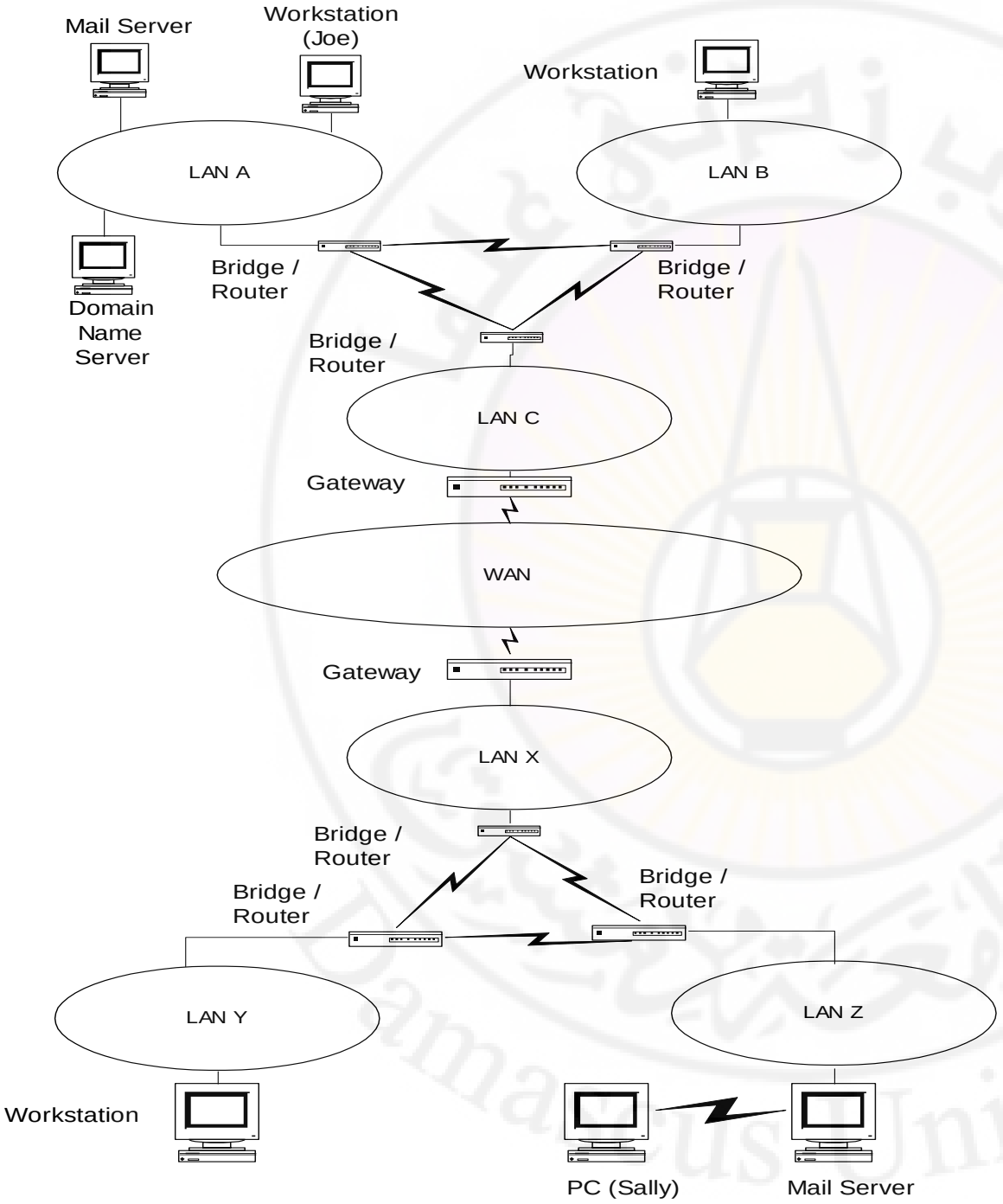
شبكة اتصال المعطيات



شبكة الإنترنت



يوضح الشكل التالي تهيئة شبكة الإنترنت:



الشبكات المعتمدة على TCP / IP

- TCP/IP: هو حقيبة (مجموعة) من البروتوكولات.
- شبكة الإنترنت تعتمد عليه في عملها.
- IP: هو بروتوكول انترنت عند طبقة الشبكة.
- TCP: هو بروتوكول نقل موجه التوصيل ويتأكد من توصيلات النهاية – النهاية.
- UDP : هو بروتوكول نقل بدون إقامة اتصال ويؤمن خدمات المعطيات.
- E-mail, WWW, FTP, Telnet: TCP/IP
- Network mgmt. (SNMP): UDP/IP
- ICMP: part of TCP/IP suite

يوضح الجدول التالي مقارنة بين الشبكة الهاتفية وشبكة الإنترنت المعتمدة على TCP / IP:

Telephone Network	TCP/IP, Internet
Terminal telephone	Terminal PDAs, PC, Workstations, …
Application (Content) Voice	Application (Content) Data: File, Message Voice, Image, Video.
Bandwidth Requirement Static (64 kbps)	Bandwidth Requirement Dynamic (kbps ~ Mbps)
Transmission Loop: UTP Trunk: Optical Fiber	Transmission Access: UTP, Coaxial Cable, … Trunk: Coaxial Cable, Optical Fiber
Network Elements (NEs) CPE, Switch, Mux, Cross connect	Network Elements (NEs) Hub, Switch, Bridge, Router

Telephone Network	TCP/IP, Internet
Addressing **telephone number** **Intelligent Networks**	**Addressing** **MAC, IP, Port, Domain Name, URL**
Network Configuration **fixed, or** **seldom changed**	**Network Configuration** **Changed frequently**
Growth **Stable, not changed**	**Growth** **grow in dog years, new applications**
Network Management **Well planned** **NOCs** **Nes**	**Network Management** **?** **Network Management Tools/Systems** **Less support in NEs**

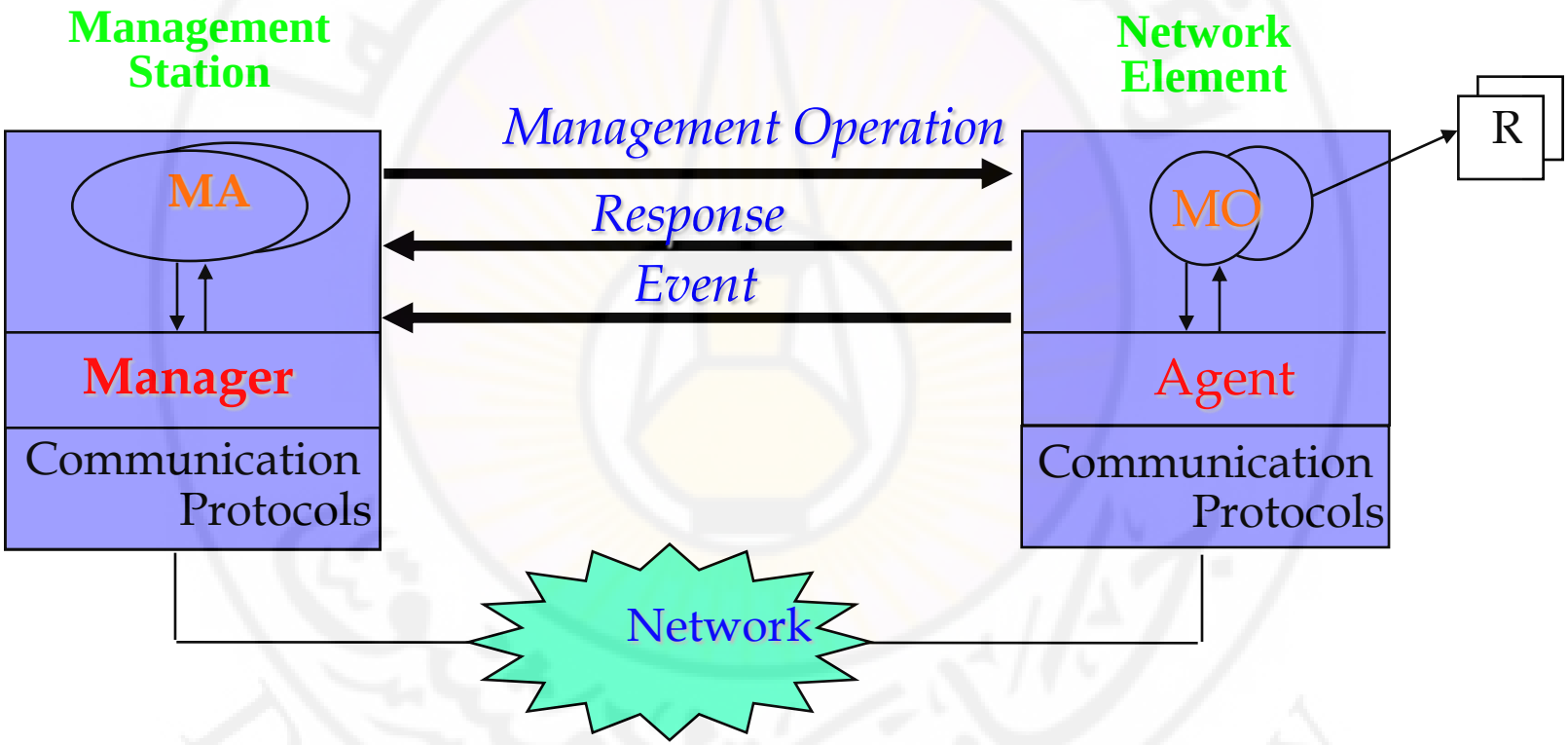
المحاضرة الثانية

بنية إدارة الشبكة

مقدمة

- يزداد استخدام الشبكات الحاسوبية في مجالات الحياة يوماً بعد يوم وتتضخم هذه الشبكات مع التطور المستمر للتقنيات الشبكية.
- تتكون الشبكات بشكل عام من مجموعة من المكونات المادية والبرمجية المتفاعلة مع بعضها البعض وذلك لأداء الخدمة المطلوبة منها وهي تبادل البيانات ومشاركة الموارد بسهولة ويسر.
- وكغيرها من الأنظمة الأخرى تحتاج الشبكة للمراقبة كغيرها من الأنظمة بهدف ضمان استمرارها واكتشاف الأعطال وغيرها..
- تهدف إدارة الشبكة بشكل عام لضمان تحقيق الشبكة وتكاملها وتأمين التفاعل بين المكونات البرمجية والمادية، بالإضافة لتوفير القدرة للمستخدم على مراقبة الشبكة بهدف اختبارها، إعدادها، تصدير إعداداتها، تحليلها، اختبارها والتحكم بموارد الشبكة لتقديم خدمة ذات أداء سريع وجودة عالية بكلفة مقبولة.
- تتضمن إدارة الشبكة الانتشار الجيد وتنسيق المكونات المادية، وتكامل المكونات البرمجية والعنصر البشري لمراقبة واختبار واقتراع وتهيئة وتحليل وتقييم والتحكم بالشبكة وعناصرها لتلبي متطلبات الزمن الحقيقي والأداء وجودة الخدمة عند كلفة معقولة.

نموذج إدارة الشبكة



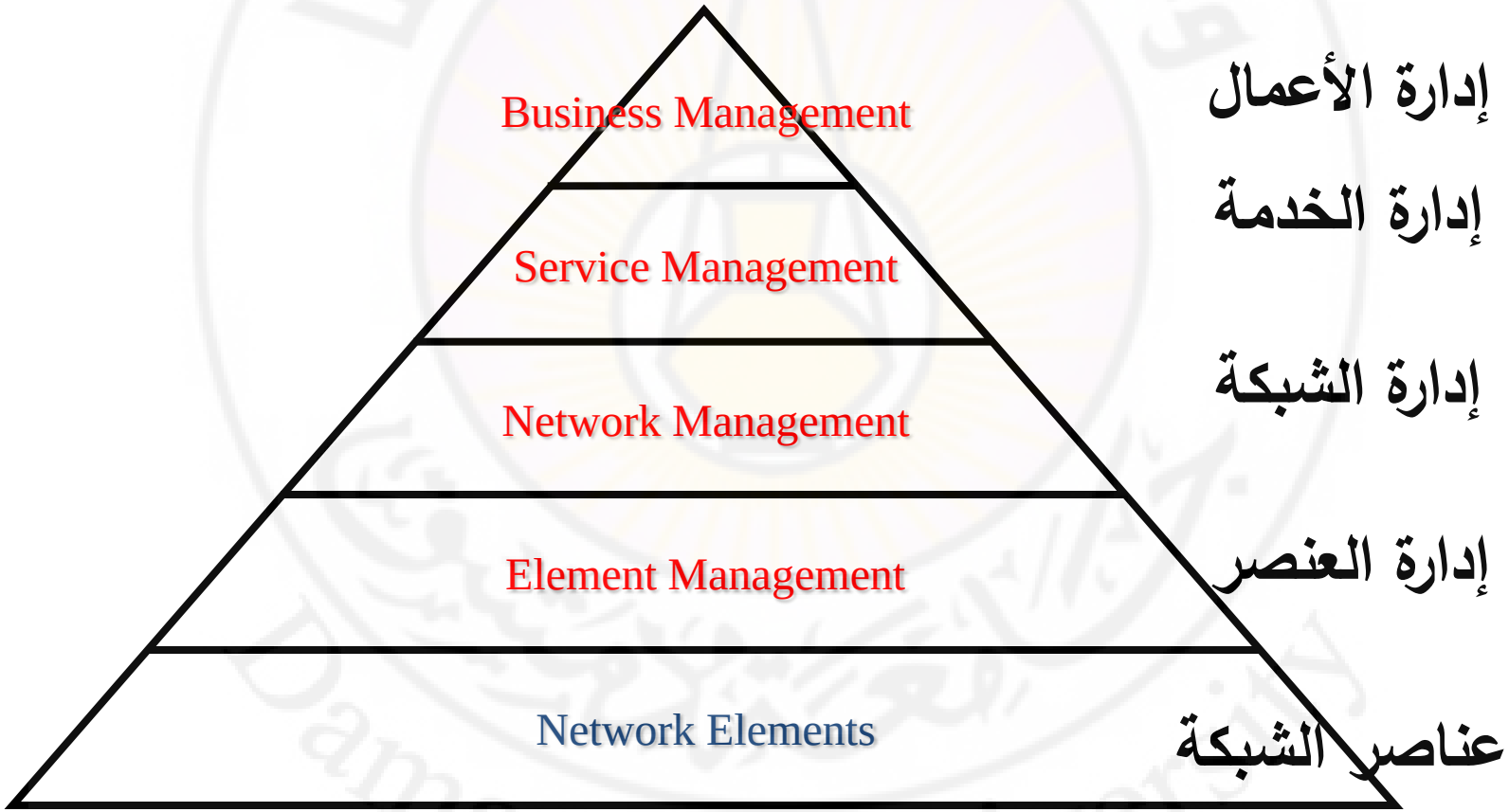
Legend :

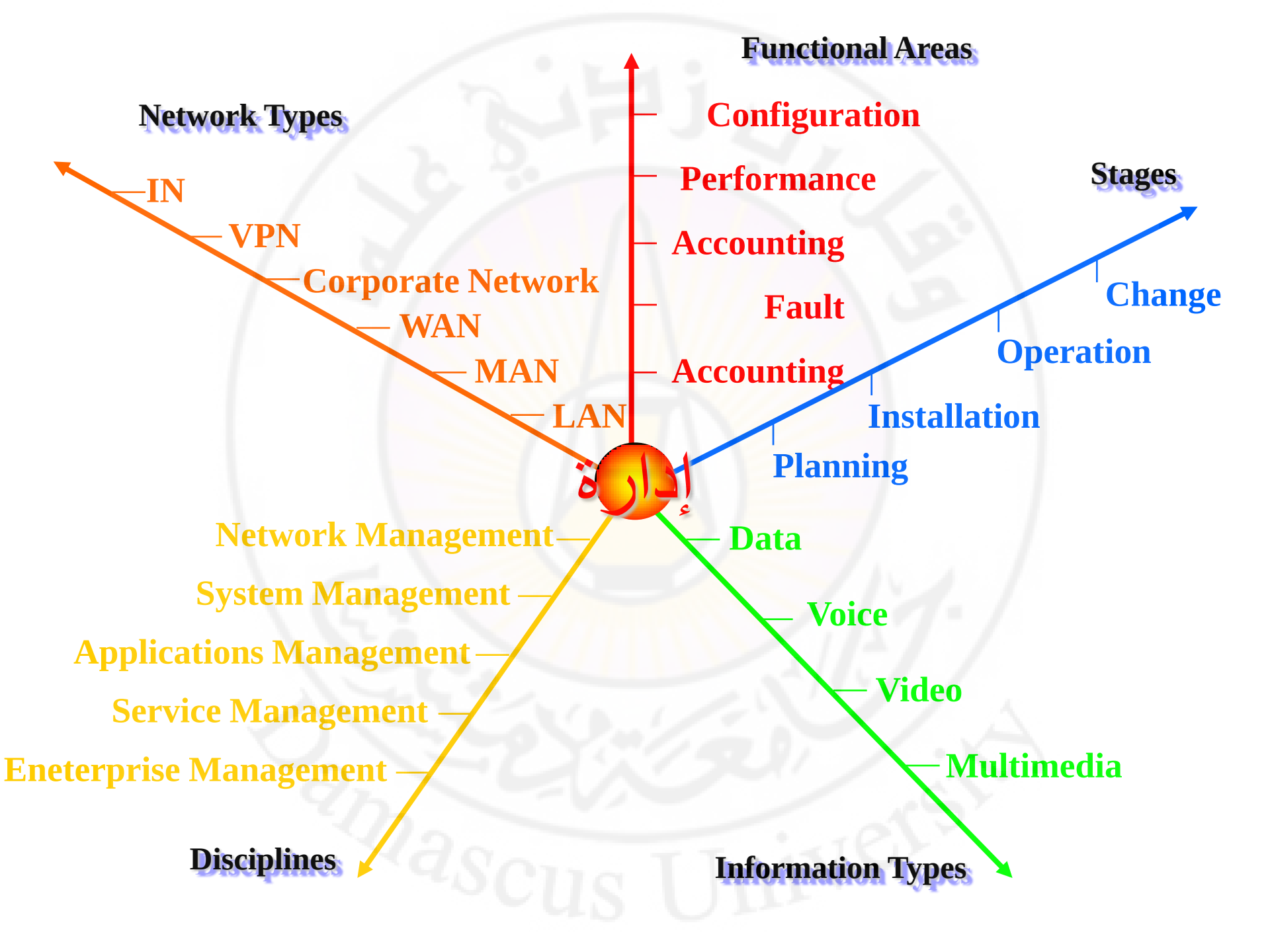
MA: Manager Applications

MO: Managed Objects

R: Real Resource

هرم الإدارة

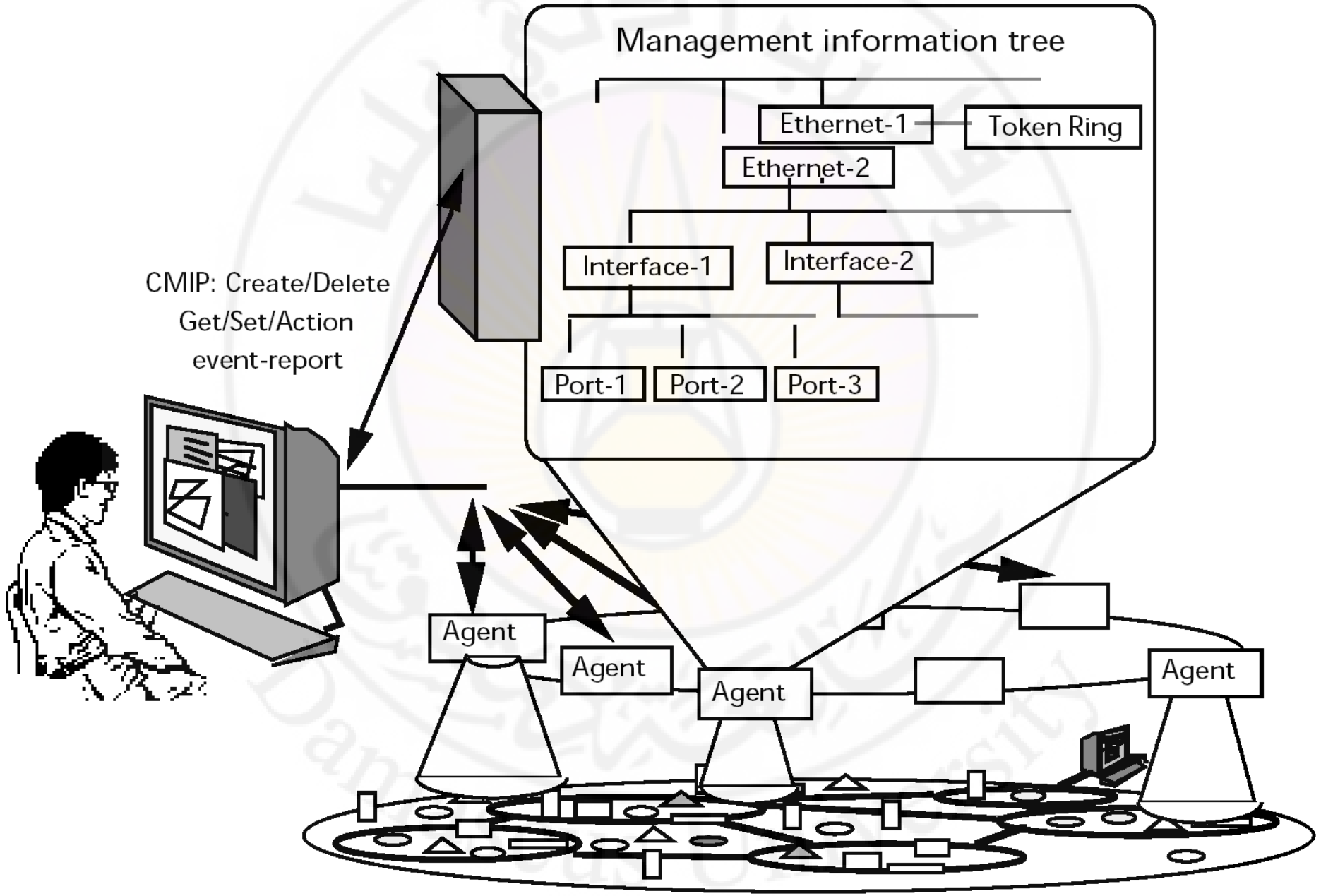

Business Management
Service Management
Network Management
Element Management
Network Elements
إدارة الأعمال
إدارة الخدمة
إدارة الشبكة
إدارة العنصر
عناصر الشبكة


Functional Areas
Configuration
Performance
Accounting
Fault
Accounting
Network Types
IN
VPN
Corporate Network
WAN
MAN
LAN
Stages
Change
Operation
Installation
Planning
إدارة
Network Management
System Management
Applications Management
Service Management
Eneterprise Management
Disciplines
Data
Voice
Video
Multimedia
Information Types

مكونات أو عناصر إدارة الشبكات

- المدير:
  - يرسل الطلبات إلى الوكلاء.
  - مراقبة الإنذارات.
  - تطبيقات منزلية.
  - يؤمن واجهة مناسبة للمستخدم.
- الوكيل:
  - جمع المعلومات من الأهداف.
  - تهيئة بارمترات الأهداف.
  - الاستجابة لطلبات المدراء.
  - توليد الإنذارات وإرسالها إلى المدراء.
- الأغراض المدارة:
  - عنصر الشبكة المراد إدارته.
  - وكيل إدارة المنازل.
  - كل الأغراض غير المدارة/ القابلة للإدارة.
- بروتوكول إدارة الشبكة.
- معلومات إدارة الشبكة.

يوضح الشكل التالي عناصر إدارة الشبكة:



بنية إدارة الشبكة

- تتكون الشبكة بشكل عام من مجموعة من الأجهزة (المبدلات، الموجهات، المخدمات وأجهزة الحاسب الشخصية وغيرها...)، وتعمل هذه الأجهزة على تخزين بيانات تخص إعداداتها، ويمكن لجهاز المدير أن يقوم بالاستعلام عنها من خلال رسائل متبادلة بين هذه الأجهزة والمدير.
- يصف هذا النموذج مكونات إدارة الشبكات وعلاقاتها مع بعضها البعض.
- مكونات إدارة الشبكات:
  - المدير.
  - الوكيل.
  - الأغراض المدارة.
- بشكل عام يقوم المدير، ويعرف بـ (Manager) بإرسال رسالة طلب (request) للحصول على بيانات الإدارة من ما يعرف بالوكيل (agent)، والذي يحتفظ ببيانات الإدارة والتي يمكن نمذجتها من خلال MIB، أو YANG، ويقوم بإرسال رسالة رد للمدير بناءاً على البيانات المطلوبة.

- المعطيات المدارة تكون مخزنة على كل جهاز باستخدام الأغراض.
- لذلك معطياتنا المدارة يمكن اعتبارها كأغراض مدارة.
- المعطيات يمكن نمذجتها باستخدام:

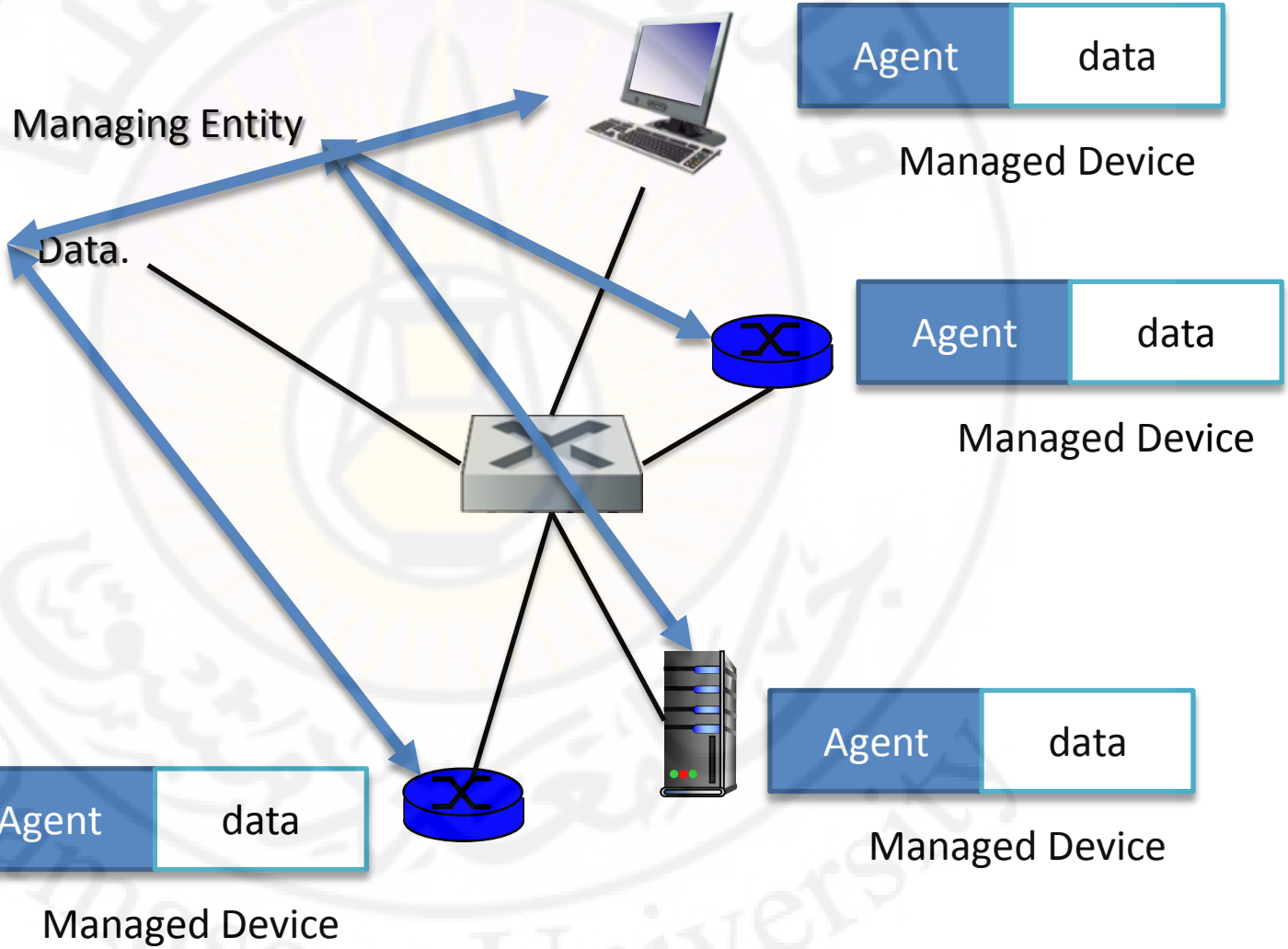
– قاعدة معلومات الإدارة MIB.

– توليد تالي آخر أيضاً YANG (Yet Another Next Generation).

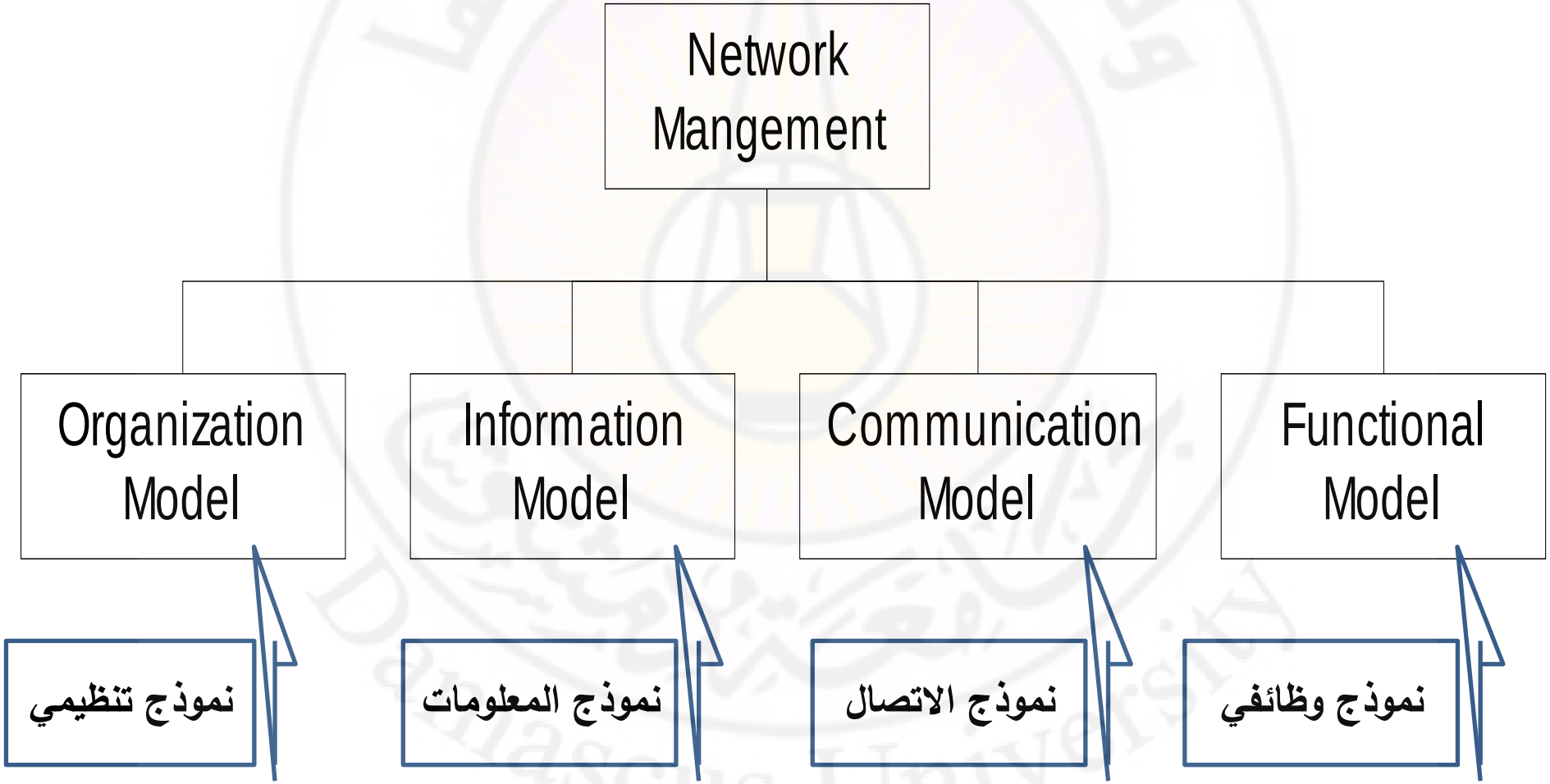
- المعطيات يمكن جمعها عن طريق رسائل الطلب/سؤال والاستجابة.

يوضح الشكل التالي بنية إدارة الشبكة:





نموذج إدارة الشبكة OSI

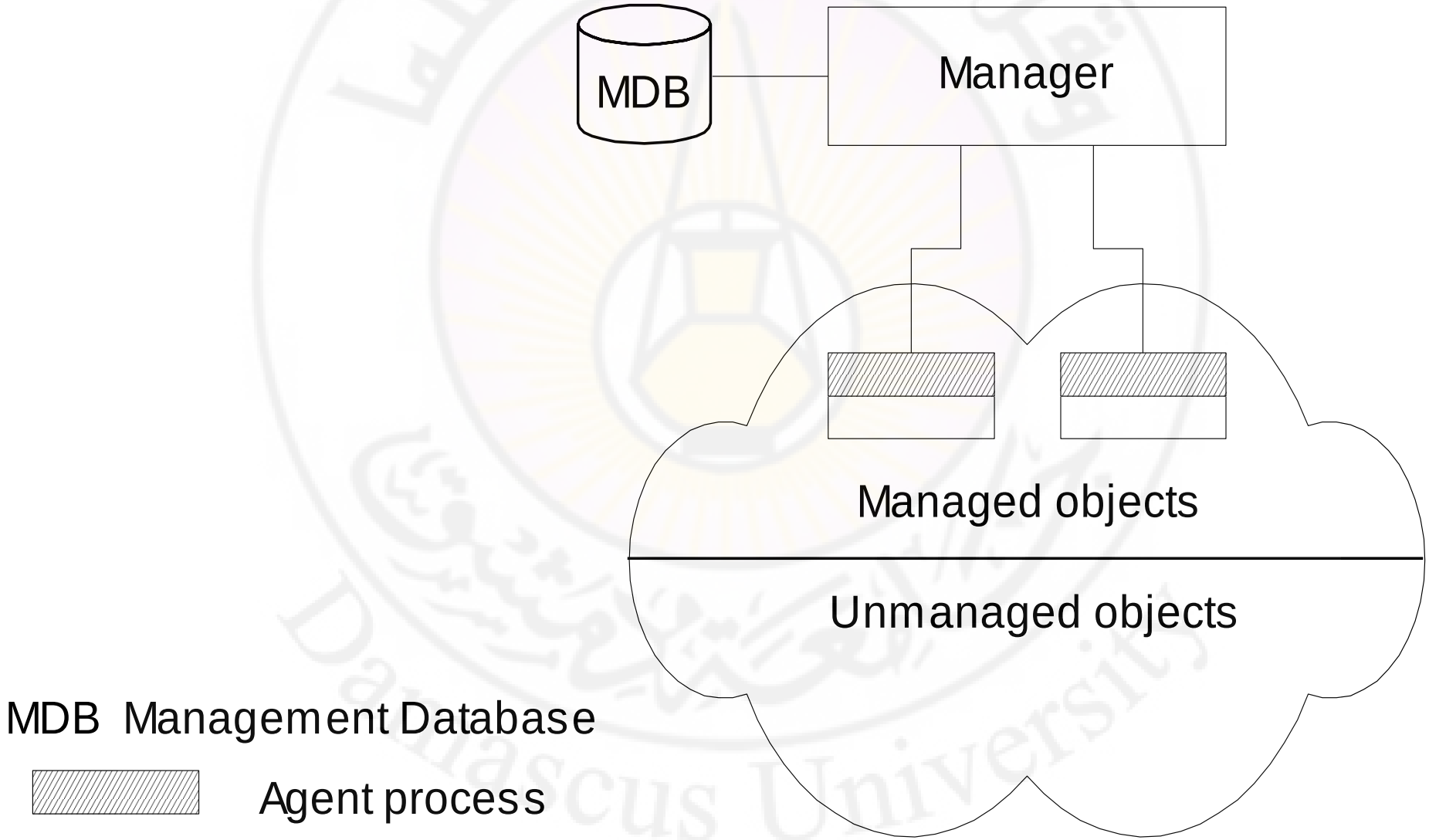


- النموذج التنظيمي:
  - مكونات إدارة الشبكة.
  - وظائف المكونات.
  - العلاقات.
- نموذج المعلومات:
  - بنية إدارة المعلومات (SMI) .
    - التركيب والأدلة.
  - قاعدة معلومات الإدارة (MIB) .
    - تنظيم معلومات الإدارة.
  - أهداف محددة.

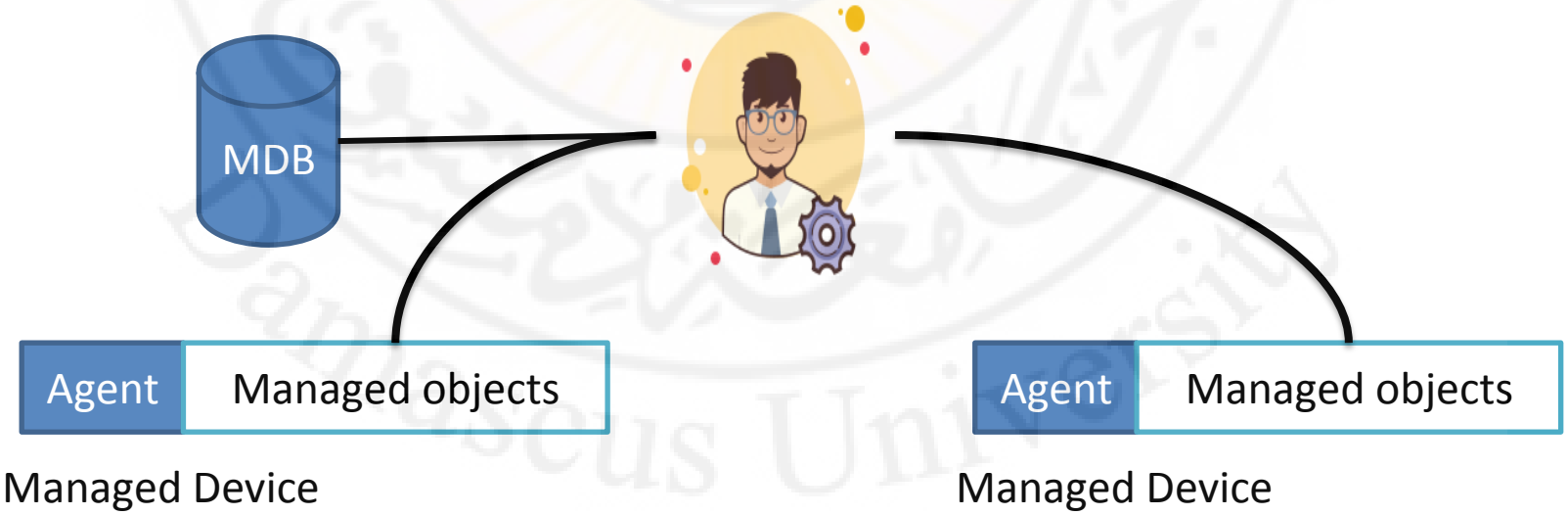
- نموذج الاتصال:
  - تحويل التركيب برسائل ثنائية الاتجاه.
  - بنية تحويل(PDU) .
- نموذج وظائفي:
  - وظائف التطبيق.
    - مكونات التهيئة.
    - مكونات المراقبة.
    - قياس الأداء.
    - معلومات آمنة.
    - تعريف الحسابات.

النموذج التنظيمي

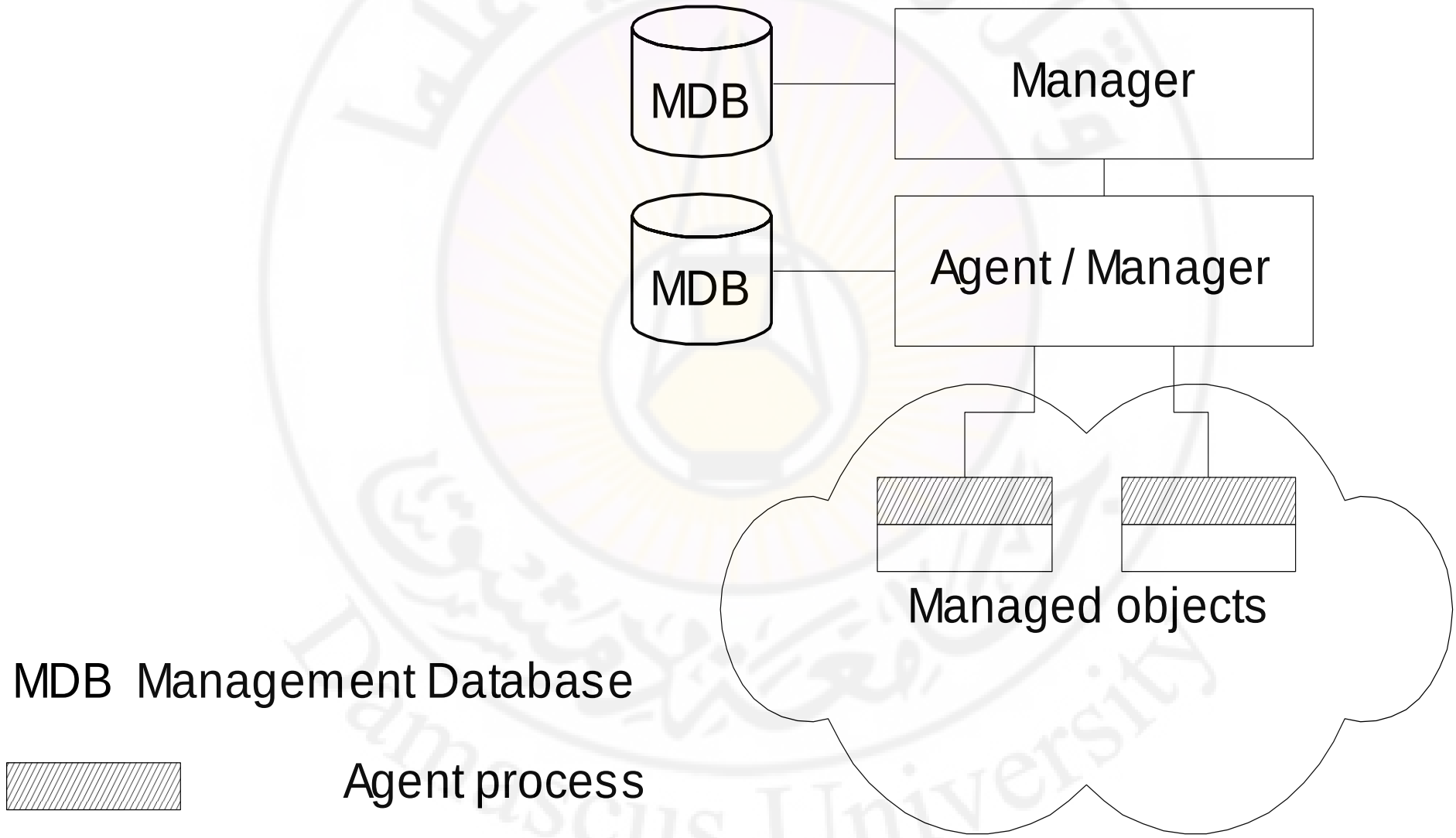
يوضح الشكل التالي نموذجاً تنظيمياً لإدارة الشبكة ثنائية الطبقة:



- العلاقة بين المدير والوكلاء يمكن أن تكون بطرق مختلفة.
- العلاقة تكون بين المدير والعديد من الوكلاء. ندعوها نموذج ثنائي الطبقة.
- المعطيات المجمعة من الوكلاء يمكن تخزينها لافي أي أنظمة MDB.
- يتم تخزين البيانات التي يبشكل عام يكون التفاعل بين المدير والأغراض المُدارة عن طريق إرسال طلبات من المدير واستقبال ردود عن بيانات هذه الأغراض وذلك عن طريق الوكيل (agent). النموذج تم تجميعها لدى المدير ضمن أي نظام تخزين ممكن. وبهذا يمكننا استخدامها للمعالجة لاحقاً.
- يوضح الشكل التالي نموذج إدارة من طبقتين المدير والأجهزة المُدارة:



يوضح الشكل التالي نموذجاً تنظيمياً لإدارة الشبكة ثلاثية الطبقة:



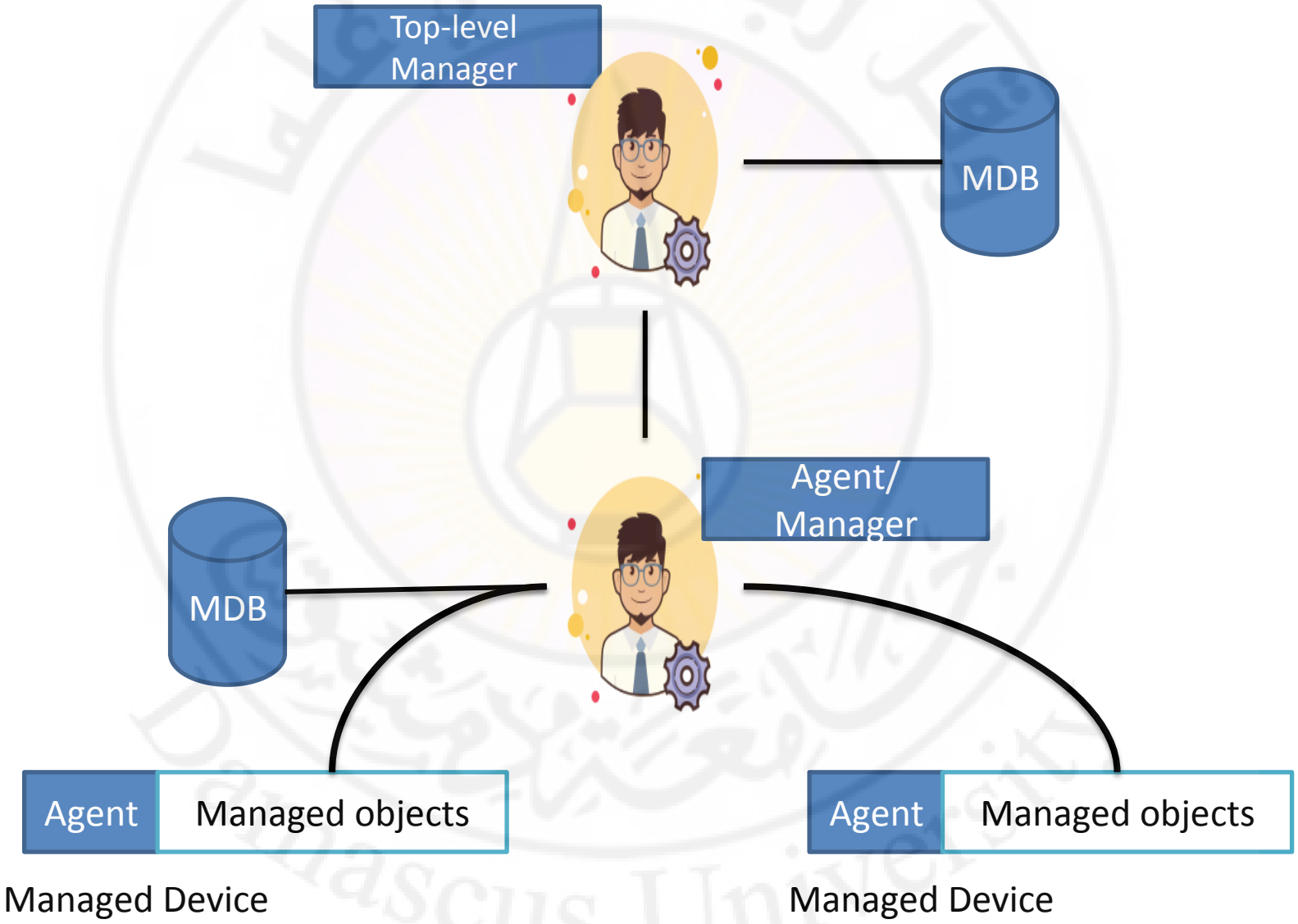
– الطبقة الواقعة بالوسط تتصرف كوكيل ومدير.

– كمدير: فإنه يجمع المعطيات من عناصر الشبكة، ويعالجها، ويخزن النتائج في قواعد المعطيات.

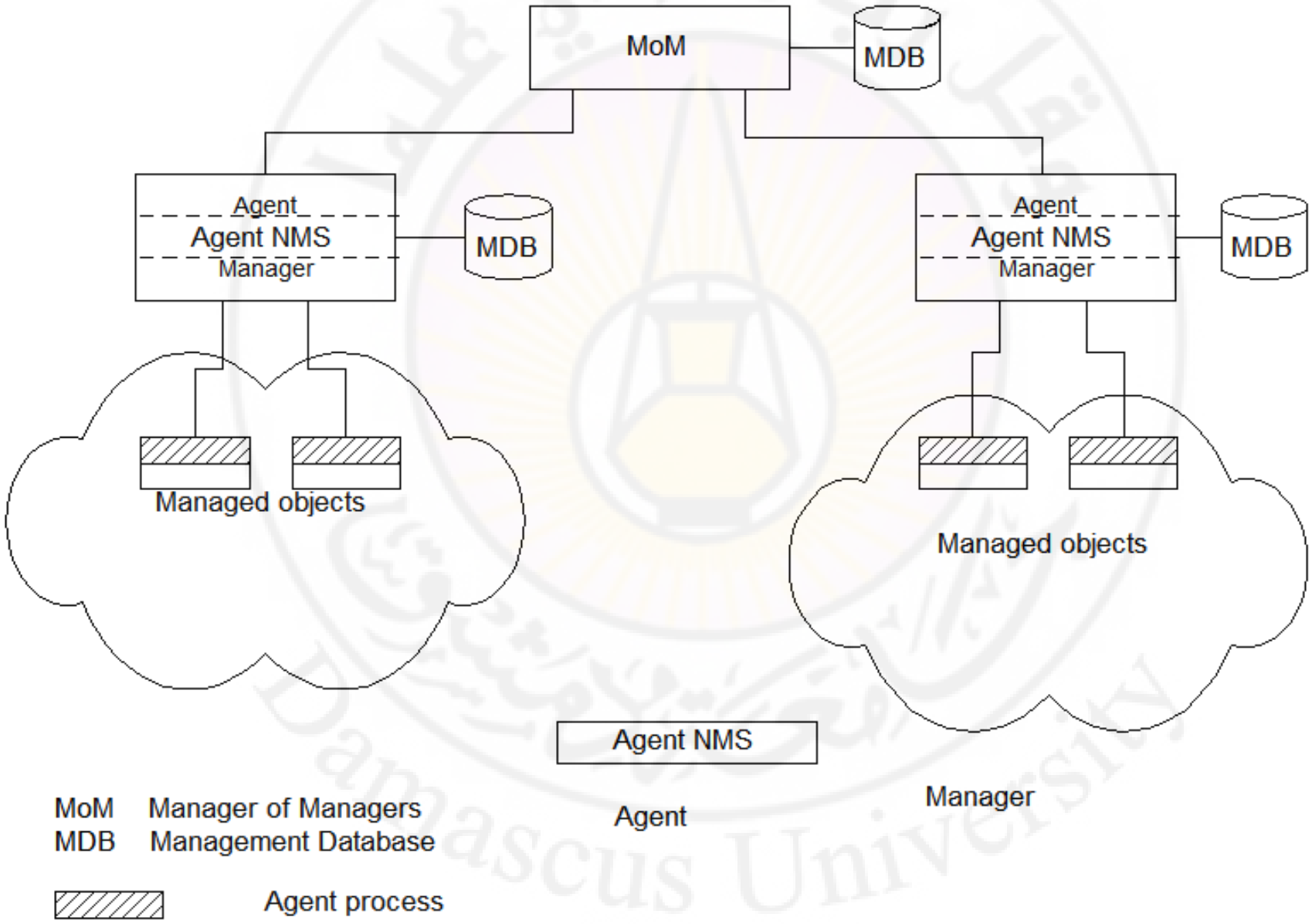
– إنه يرسل المعلومات إلى المدير بالمستوى القمة.

– فعلى سبيل المثال، العقدة التي تقع في الوسط تكون مستخدمة لصنع بعض القياسات الاحصائية في المعطيات المجمعة من الوكلاء وبعدئذ تمر النتائج إلى المدير بالمستوى القمة.

يوضح الشكل التالي نموذج ثلاثي الطبقات:

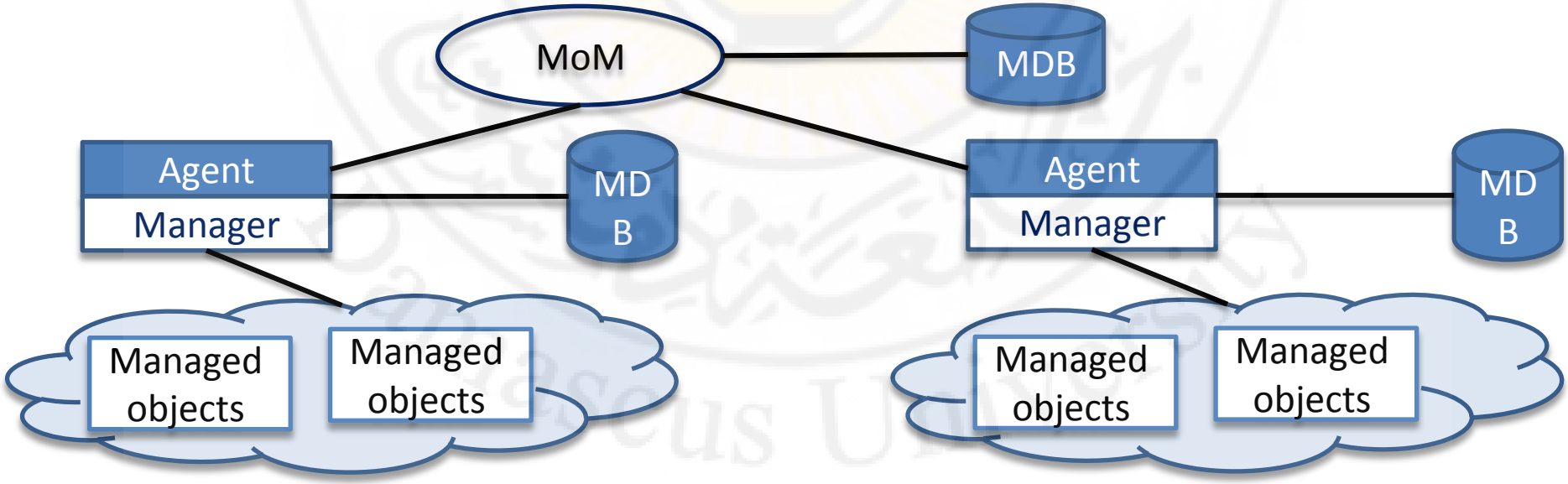


يوضح الشكل التالي نموذجاً تنظيمياً لإدارة شبكة مدير إلى مدراء:

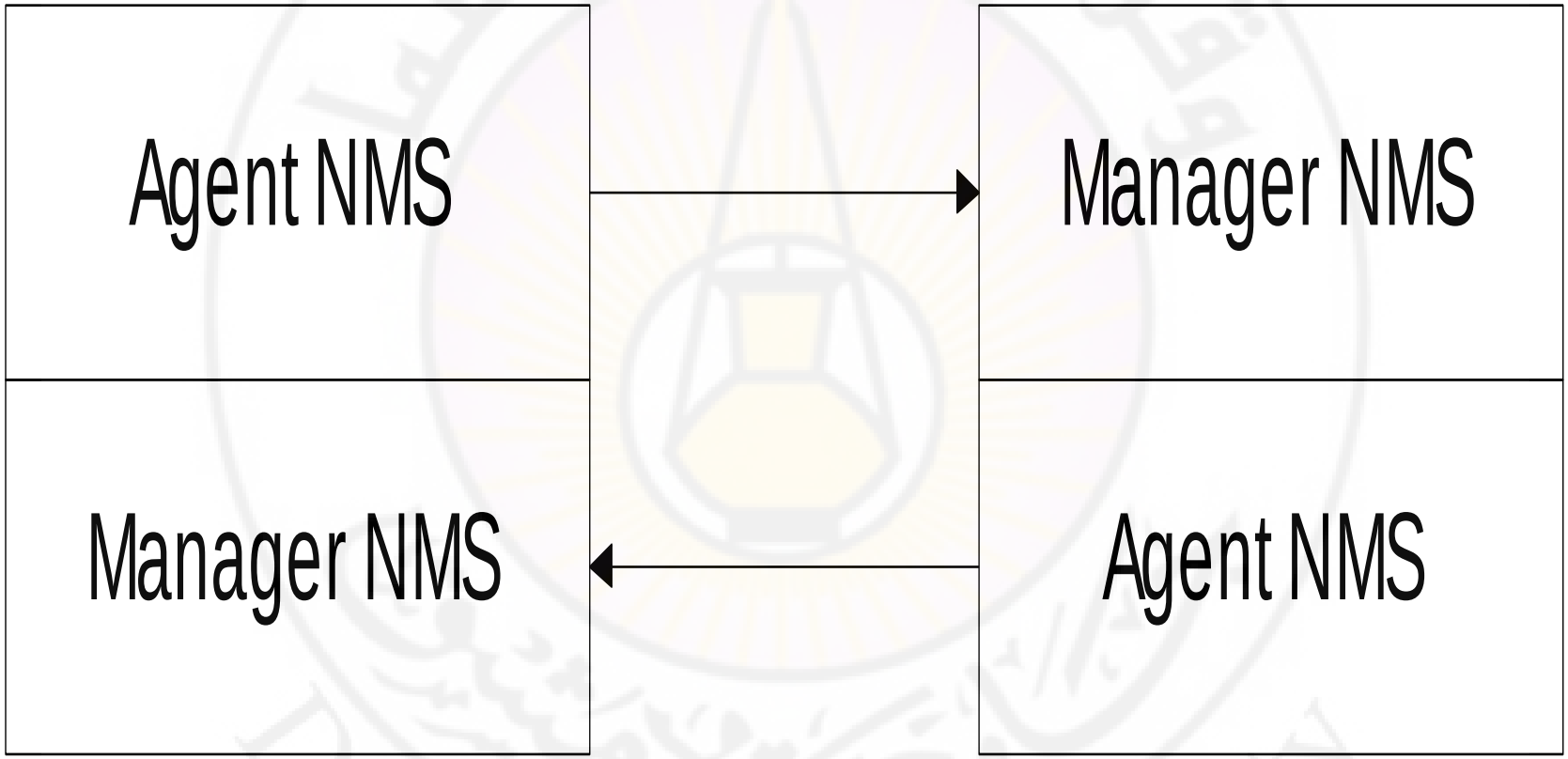


- مجالات الشبكة من الممكن إدارتها بشكل محلي وبرؤية عامة للشبكات يمكن مراقبتها من قبل مدير من المدراء.

- نستطيع إعادة رؤية العلاقة بين المدير والوكلاء كطريقة مخدم–زبون، حيث المدير يخدم كمعطيات طلبات الزبون من الوكلاء والذي يتصرف كمخدم والذي يعمل للاستجابة للطلبات القادمة.



يوضح الشكل التالي نظام إدارة الشبكة الند:



دور ثنائي لعملية الإدارة

- يصف النموذج التنظيمي مكونات الشبكة المدارة وعلاقاتها مع بعضها البعض (مبدلة، موجه، ... إلخ).
- الكينونة المدارة تملك عملية إدارة وتدعى الوكيل.
- المدير (محطة إدارة الشبكة) يدير الكينونات المدارة عبر السؤال أو الاستفهام عن بعض المعلومات من الوكلاء.
- يهتم النموذج التنظيمي بمكونات إدارة الشبكة بالإضافة للعلاقة بين هذه المكونات.
- وهنا يمكننا التميز بين مكونين رئيسين:

١- الأجهزة المُدارة: هي الأجهزة التي تحوي عملية وكيل إدارة تعمل عليها وتعرف بالوكيل (Agent)، حيث يتم الاستفادة من ما يعرف بالأغراض المُدارة للحصول على معلومات هذه الأجهزة.

٢- المدير: وهو المسؤول عن القيام بعملية إرسال الطلبات والحصول على الردود من الوكلاء. وبناءً على نتيجة الرد يمكننا تحديد آلية التعامل مع الوضع الحالي للجهاز المُدار أو الشبكة ككل.

- قد لا تحوي بعض الأجهزة إمكانية الإدارة أو تدعم بروتوكولات خاصة فهنا يمكننا استخدام ما يعرف بـ proxy للترجمة بين البروتوكولات المختلفة.

نموذج المعلومات

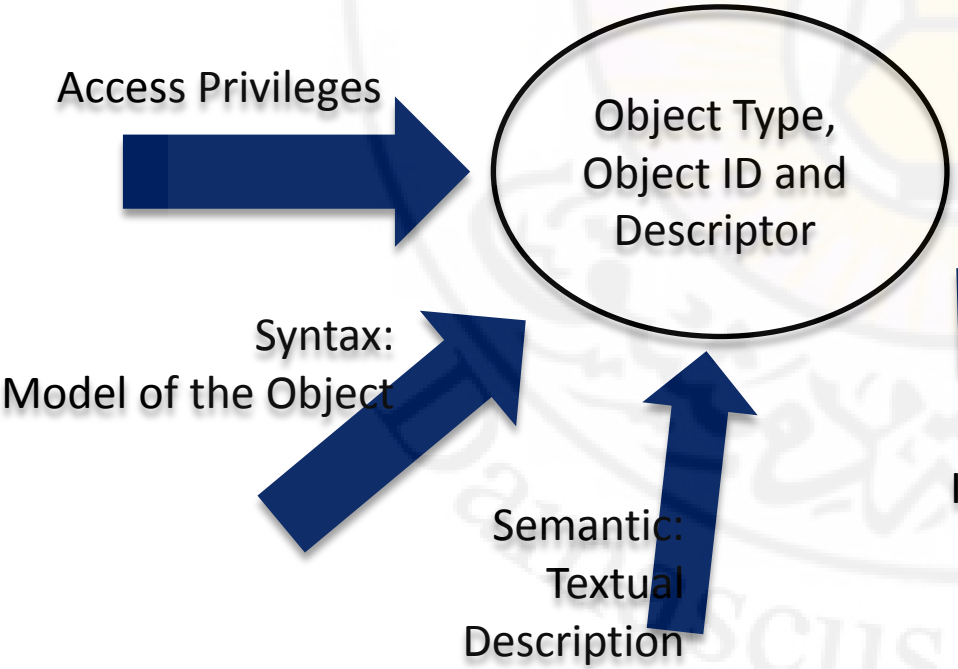
- نموذج المعلومات يكون مهتماً ببنية ومخزن المعلومات.
- بنية معلومات الإدارة SMI تعرف شكل أو قالب المعلومات ومعنى المعلومات.
- قاعدة معلومات الإدارة MIB تكون مستخدمة من قبل كلاً المدير والوكيل لتخزين وتغير المعلومات.
  - قاعدة معلومات الإدارة MIB المرتبطة بالوكيل تدعى agentMIB.
  - قاعدة معلومات الإدارة MIB المرتبطة بالمدير تتألف من كل المعلومات وكل مكونات الشبكة التي يجب إداراتها.

تمثيل البيانات يتم بشكل فريد مشابه لتمثيل الكتب الإلكترونية حيث لكل كتاب معرف فريد ISBN (International Standard Book Number) وهو عبارة عن رقم من ١٠ منازل يمثل كتاباً فريداً.
بنفس الطريقة يمكننا النظر لتمثيل الأغراض المُدارة ضمن الشبكة.

نموذج المعلومات

- تمثيل الغرض:

Characteristics	Example
Object Type	pktCounter
Syntax	Counter
Access	Read only
Status	Mandatory
Description	Counts number of packets.



نموذج المعلومات

- الغرض المدار يمتلك العديد من الخصائص.
  – واجهة الموجه ربما تمتلك (رقم، عنوان IP، ... إلخ).

- يوجد العديد من العمليات التي يمكن تشكيلها على الأغراض المستخدم (المدير)، ويمكن رؤيته وتشكيله فقط بعمليات محددة.
- على الغرض عن طريق إحداث وكيل الإدارة.

- رؤية سمات الغرض بأن مشاهدات الوكيل تكون برؤية MIB.

- العمليات التي يمكن للمستخدم أن ينفذها تكون بالدخول على MIB.

نموذج المعلومات

- بنية ومخزن معلومات الإدارة **SMI**: والتي تحدد التركيب وقواعد إدارة المعلومات، إضافةً إلى معلومات أخرى كالحالة.

- يوضح التالي مثالاً عن **SMI**:

- Example

```
sysDescr: { system 1 }
  Syntax:      OCTET STRING
  Definition:  "A textual description of
                the entity. "
  Access:      read-only
  Status:      mandatory
```

قاعدة معلومات الإدارة MIB

- قاعدة معلومات الإدارة MIB: مخزن مؤلف من مفاهيم إدارة المعلومات.
- تحتوي قاعدة المعلومات على المعلومات حول الأغراض.
- تنظيمها عن طريق الأغراض ذات العلاقة.
- تعرف العلاقة بين الأغراض.
- هي ليست قاعدة معطيات فيزيائية، وإنما هي قاعدة معطيات افتراضية، والتي تصنف أو تجمع في وحدة الإدارة.

رؤية MIB

- حتى نفهم هذه الرؤية سنقارنها بفهرس الكتب الموجودة في أفرع المكتبة المنتشرة في مقاطعة على سبيل المثال.
- كل فرع يملك مجموعة من الكتب.
- الكتب في كل فرع تكون مجموعة مختلفة.
- قاعدة المعلومات للمقاطعة تملك رؤية أو فهرس لكل الكتب.
- قاعدة المعلومات لكل فرع تملك فهرس الكتب التي تنتمي إلى ذلك الفرع، وهذا يعني أن كل فرع يمتلك فهرس خاص به من قاعدة المعطيات.
- دعنا نطبق ذلك على رؤية MIB.

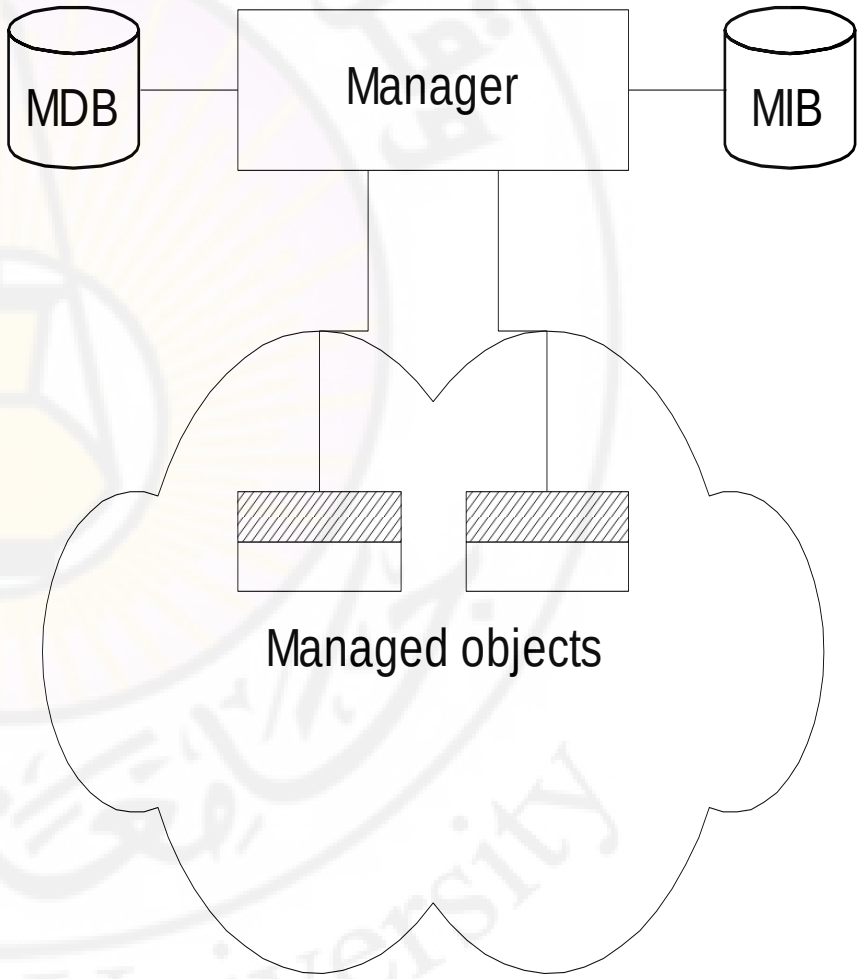
Damascus University

رؤية MIB و دخول الغرض

- الغرض المدار يمتلك العديد من السمات أو المزايا والتي تكون قاعدته المعلومات.
- يوجد العديد من العمليات التي يمكن تنفيذها على الأغراض.
- المستخدم (المدير) يستطيع رؤية وتشكيل عمليات محددة فقط على الغرض عن طريق إحداث وكيل الإدارة.
- رؤية سمات الغرض بأن صفات الوكيل تكون رؤية MIB.
- العملية التي يقوم بها "ينفذها" المستخدم (المدير) تكون الدخول على MIB.

مقارنة قاعدة معطيات الإدارة وقاعدة معلومات الإدارة

- MDB
  - Management Data Base –
  - physical database –
- MIB
  - Management Information Base –
  - virtual database –



الأغراض المدارة في MIB

- الأغراض المدارة يمكن أن تكون:
  - عناصر الشبكة (مكونات مادية، نظام).
    - مجمعات، جسور، موجهات، تسهيلات الارسال.
  - البرمجيات.
    - برامج، خوارزميات.
  - معلومات تنفيذية.
    - اتصال الشخص، اسم مجموعة الأغراض (مجموعة IP).

Damascus University

شجرة معلومات الإدارة

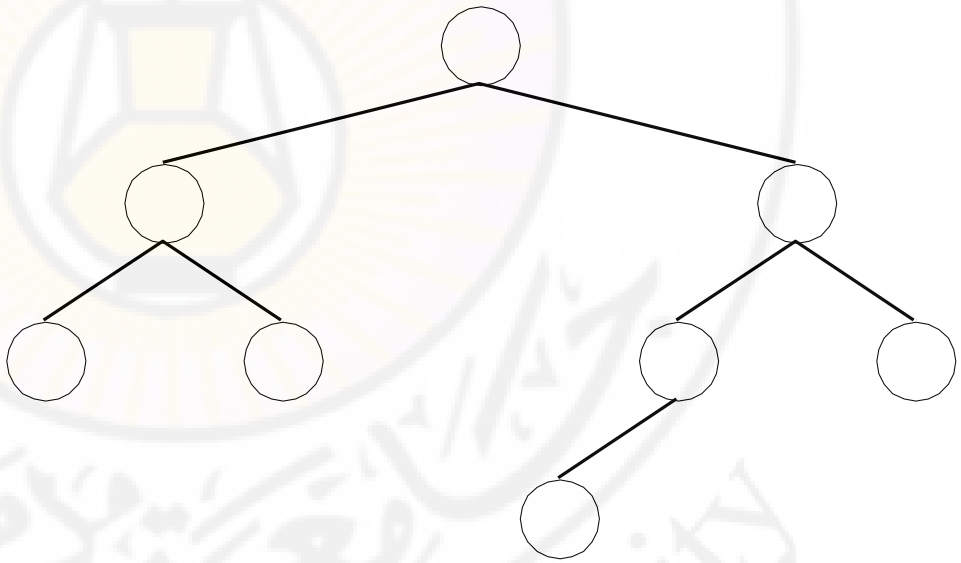
- MO تكون معرفة ببنية الشجرة والمحددة من قبل النموذج OSI.

Root

Level 1

Level 2

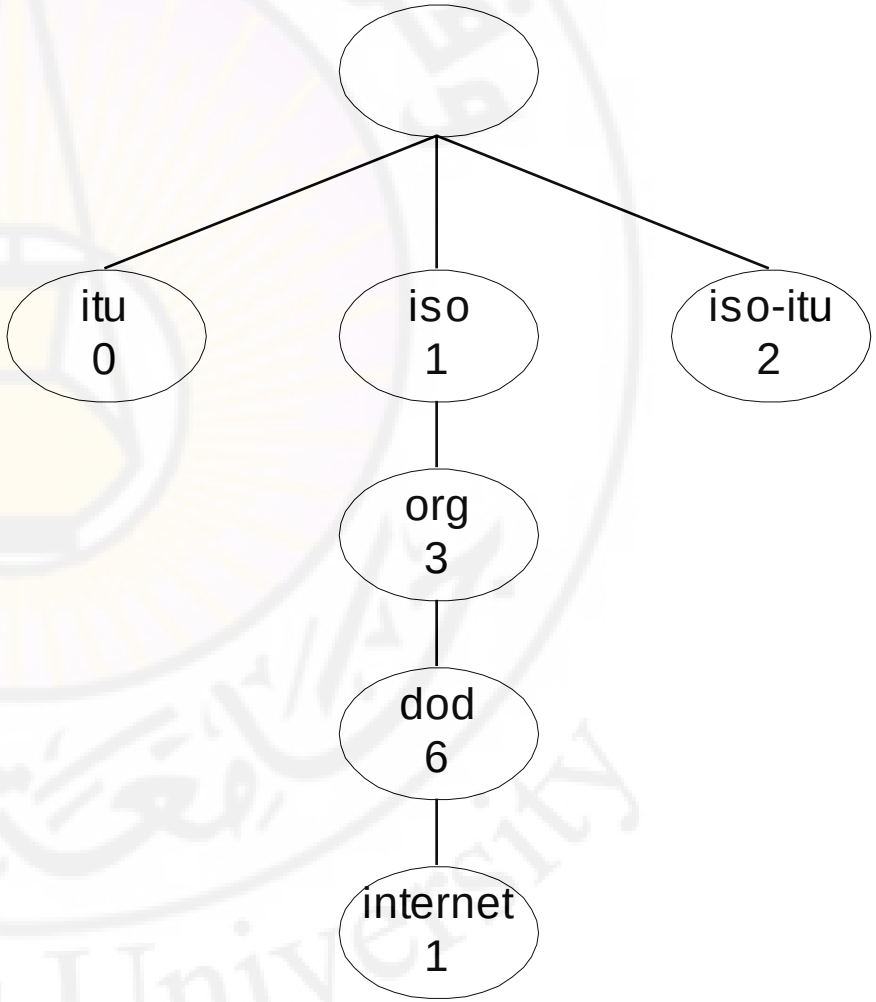
Level 3



Damascus University

شجرة معلومات إدارة OSI

Designation:•	
1 iso•	
org•	1.3
dod•	1.3.6
internet•	1.3.6.1



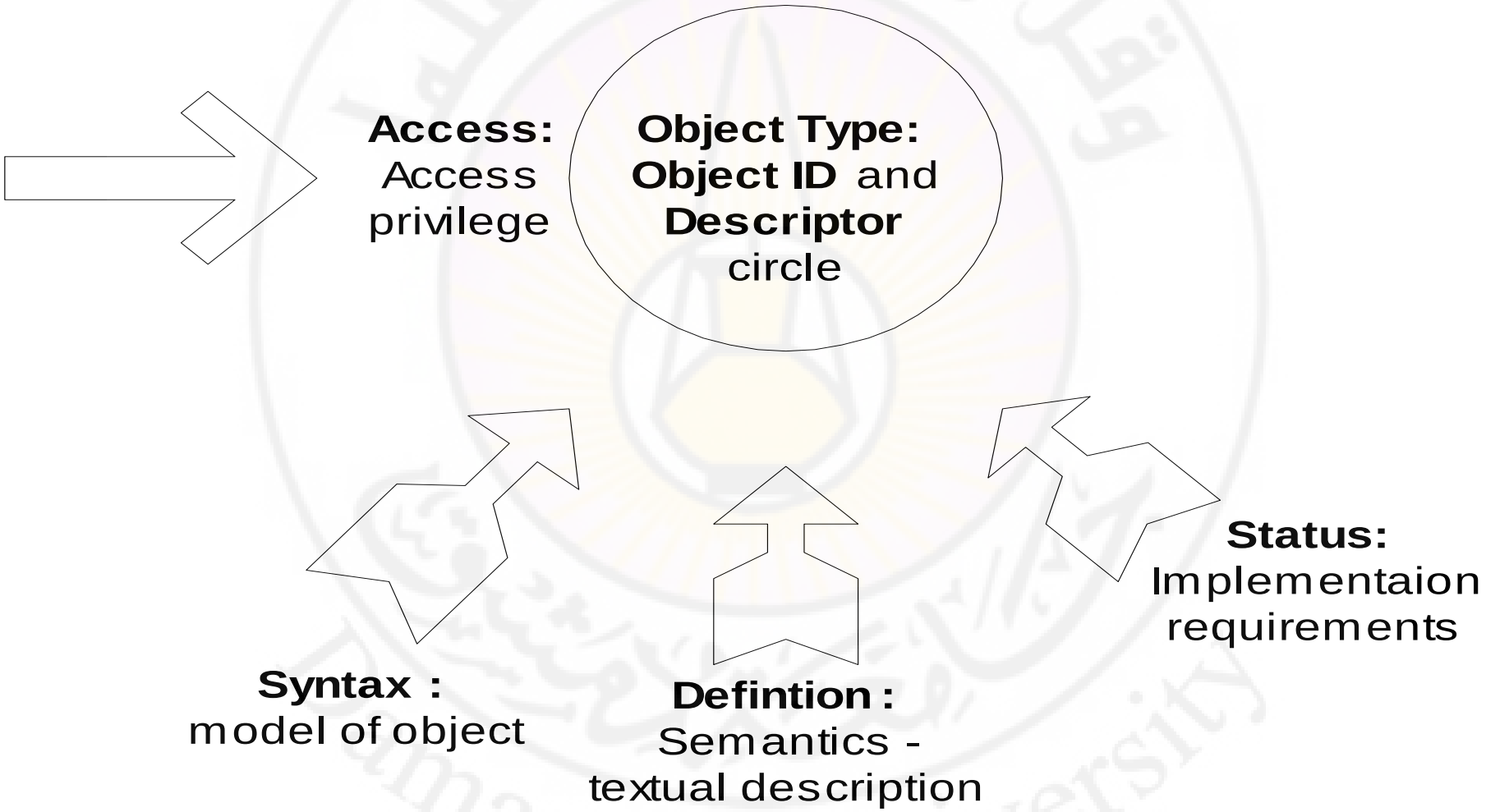
نموذج الغرض والمثال

- كل شكل غرض يملك مميز فريد (هوية التعريف) والاسم وفيمايل توضيح ذلك:
- ***Object Type***
  - **Name**
  - **Syntax**
  - **Definition**
  - **Status**
  - **Access**

```
sysName
Octet String
"The name of a system"
Mandatory
Read-Only
```

- مقترح الغرض.
- كل شكل غرض يملك مقرح أو عدة مقترحات.

Managed Object: Internet Perspective

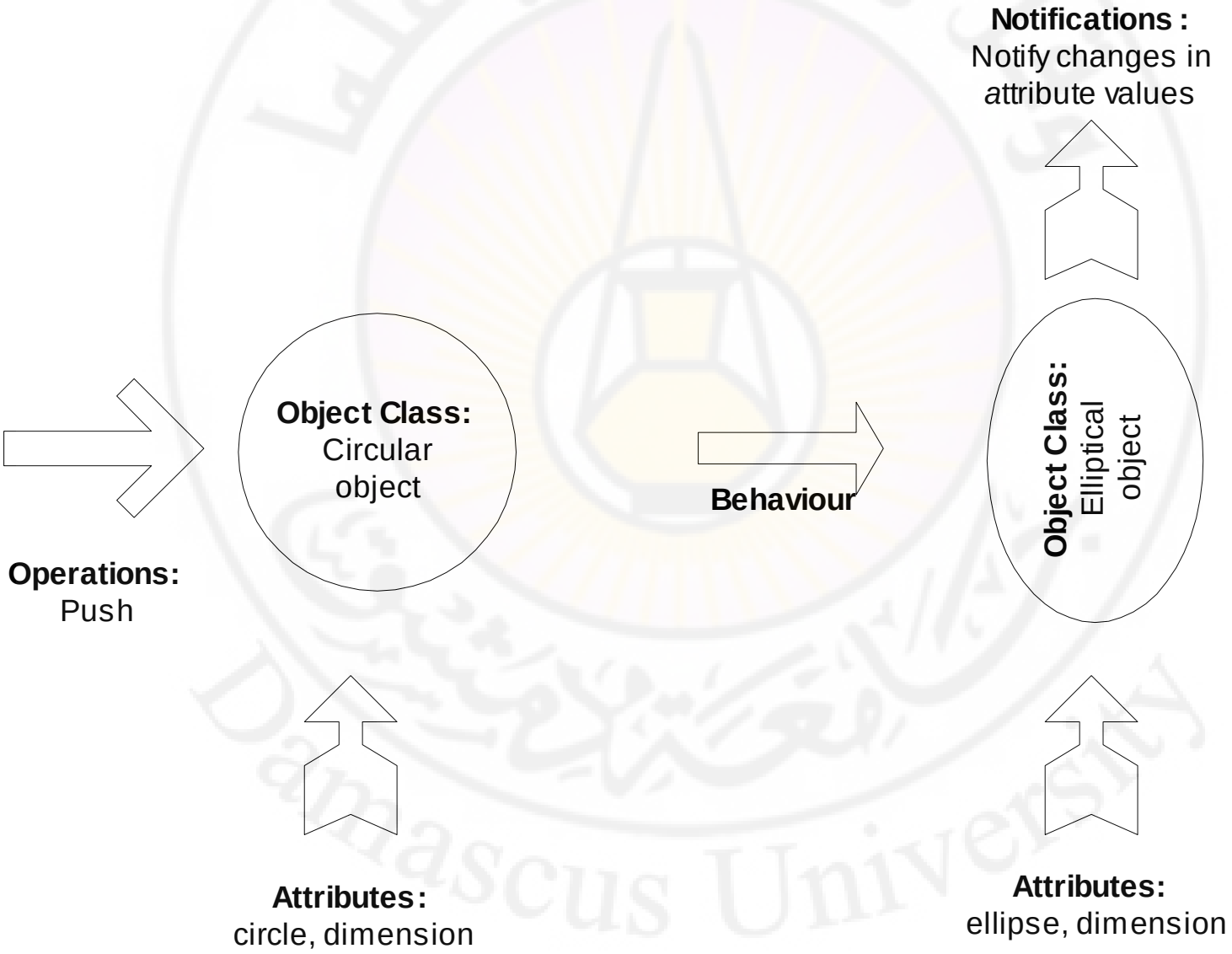


Managed Object: Internet Perspective

object ID	unique ID (OID)
and ***descriptor***	and name for the object
syntax	used to model the object
access	access privilege to a managed object
status	implementation requirements
definition	textual description of the semantics of object type

References: RFC 1155, RFC 1212

Managed Object: OSI Perspective



فيمايلي مثال على عداد الحزم من وجهة نظر OSI والانترنت

Characteristics	Example
Object type	PktCounter
Syntax	Counter
Access	Read-only
Status	Mandatory
Description	Counts number of packets

Figure 3.10(a) Internet Perspective

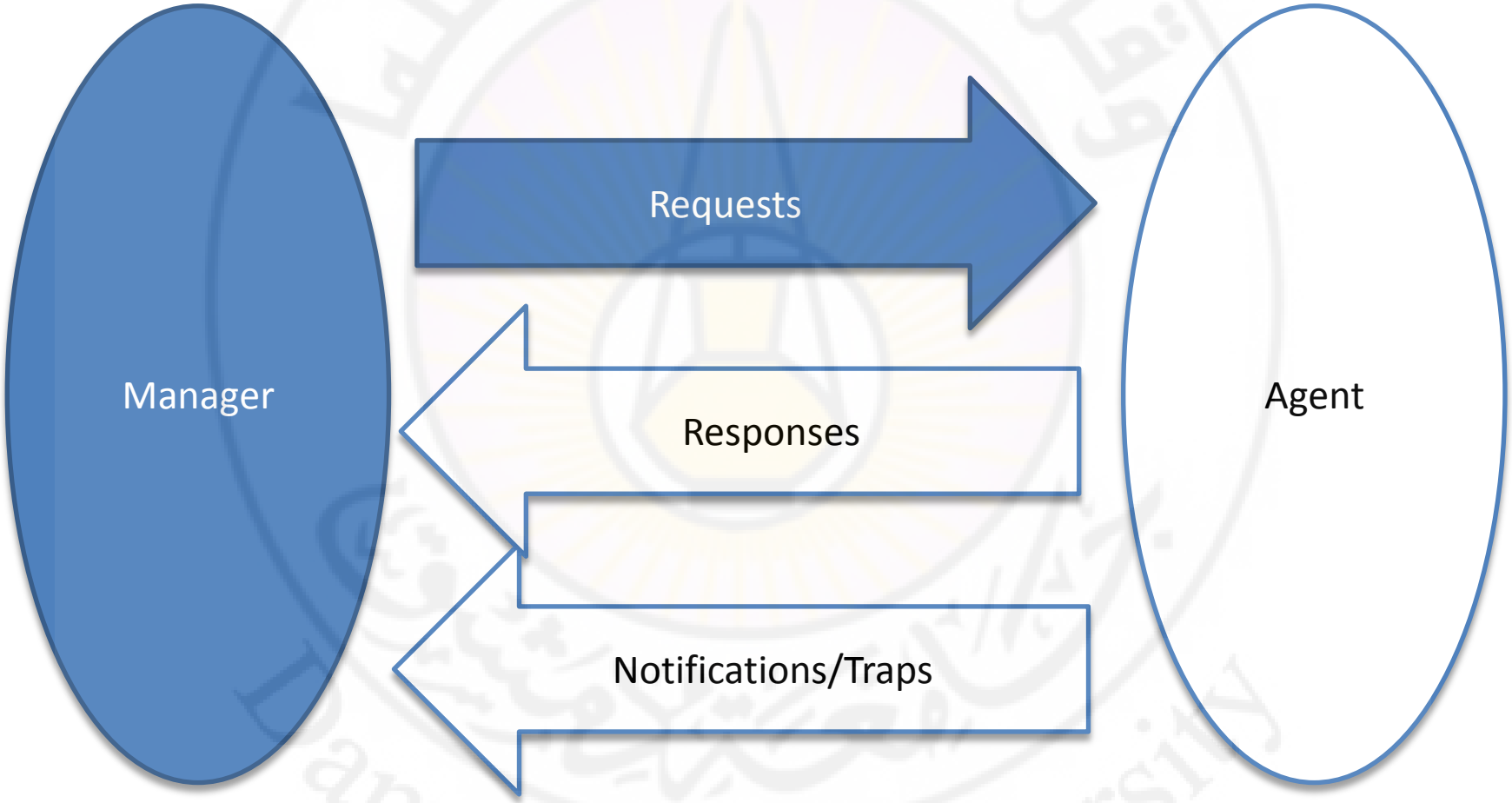
Characteristics	Example
Object class	Packet Counter
Attributes	Single-valued
Operations	get, set
Behavior	Retrieves or resets values
Notifications	Generates notifications on new value

Figure 3.10 (b) OSI Perspective

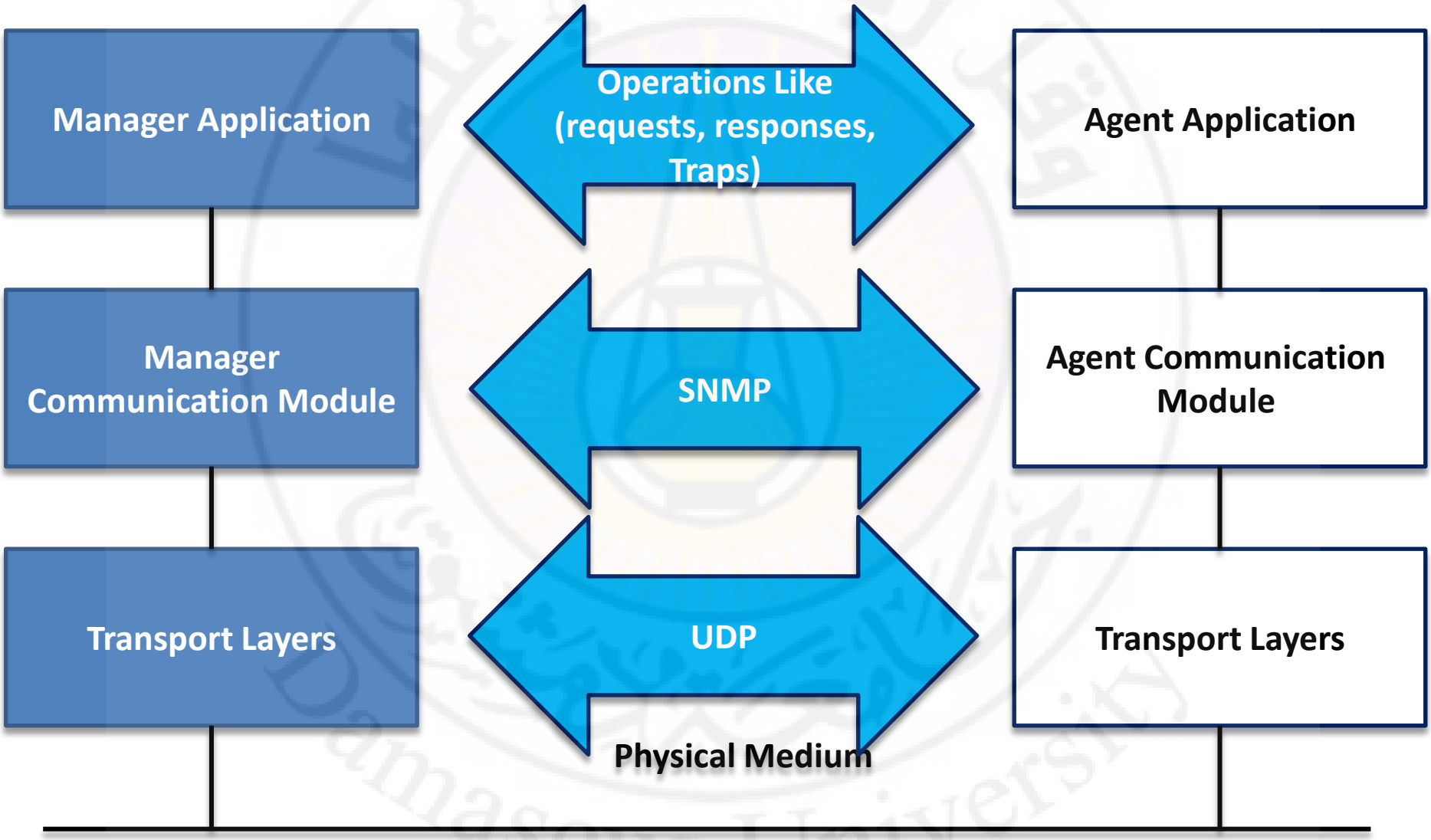
نموذج الاتصال

- نموذج الاتصال يكون مهتماً بتبادل المعلومات بين الأنظمة.
- ثلاثة أوجه نحتاجها للعنونة في اتصال المعلومات بين كينونتين وهي:
  - بروتوكول النقل.
  - بروتوكول التطبيق (قالب رسالة الاتصال).
  - الرسالة الحقيقية أو الفعلية (أوامر واستجابات).

يوضح الشكل التالي ذلك:

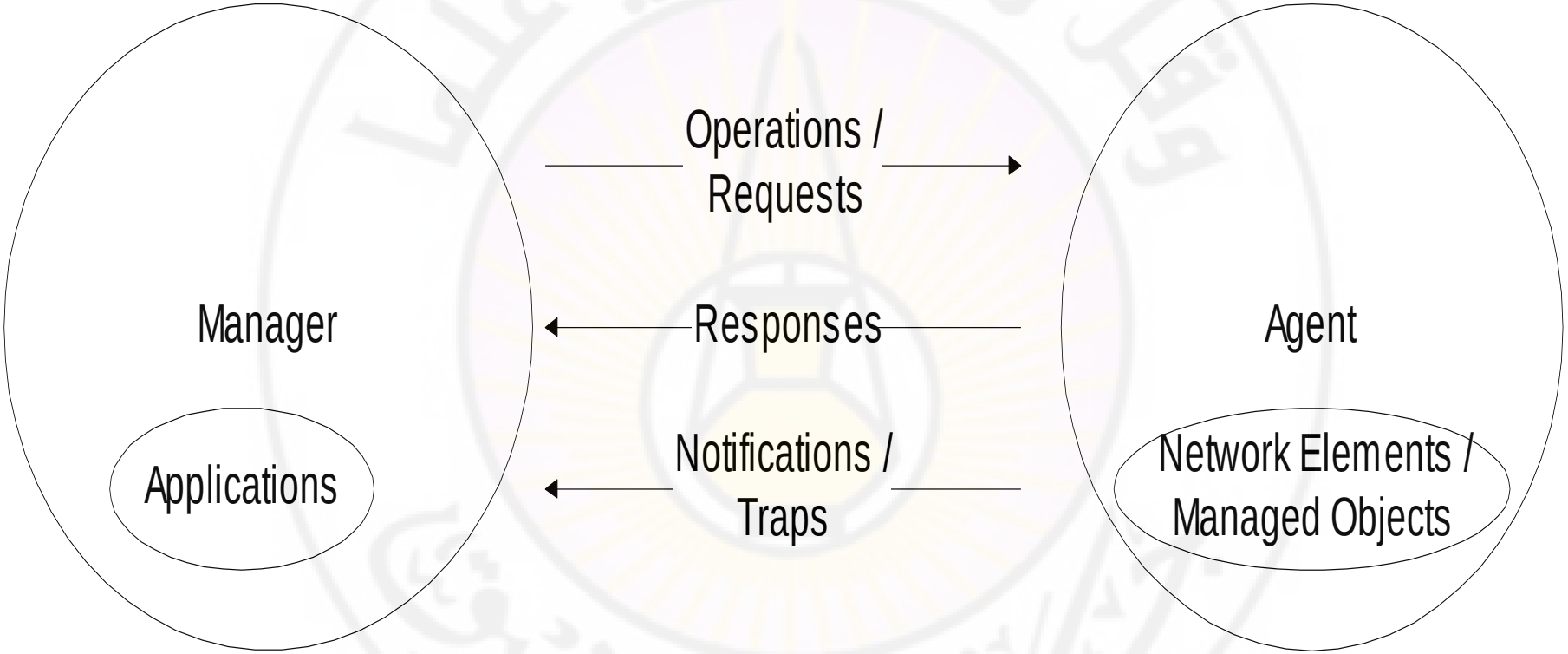


نموذج الاتصال



يوضح لنا الشكل الموجود هرمية الاتصال التي تتم بين المدير والوكيل، حيث يقوم المدير بتحديد طلب معين كالحصول على بيانات ما معينة من الوكيل (request)، ولإرسال الطلب مع معرف الغرض المُدار الذي يريده المدير يستخدم أحد بروتوكولات الإدارة، وفي مثالنا هنا نستخدم SNMP، ويجب علينا تحديد بروتوكول طبقة النقل وهنا تم تحديده كـ UDP، كما يقوم الوكيل بمعالجة الطلب القادم من المدير ويرسل الرد (response) مروراً بالمراحل السابقة ذاتها.

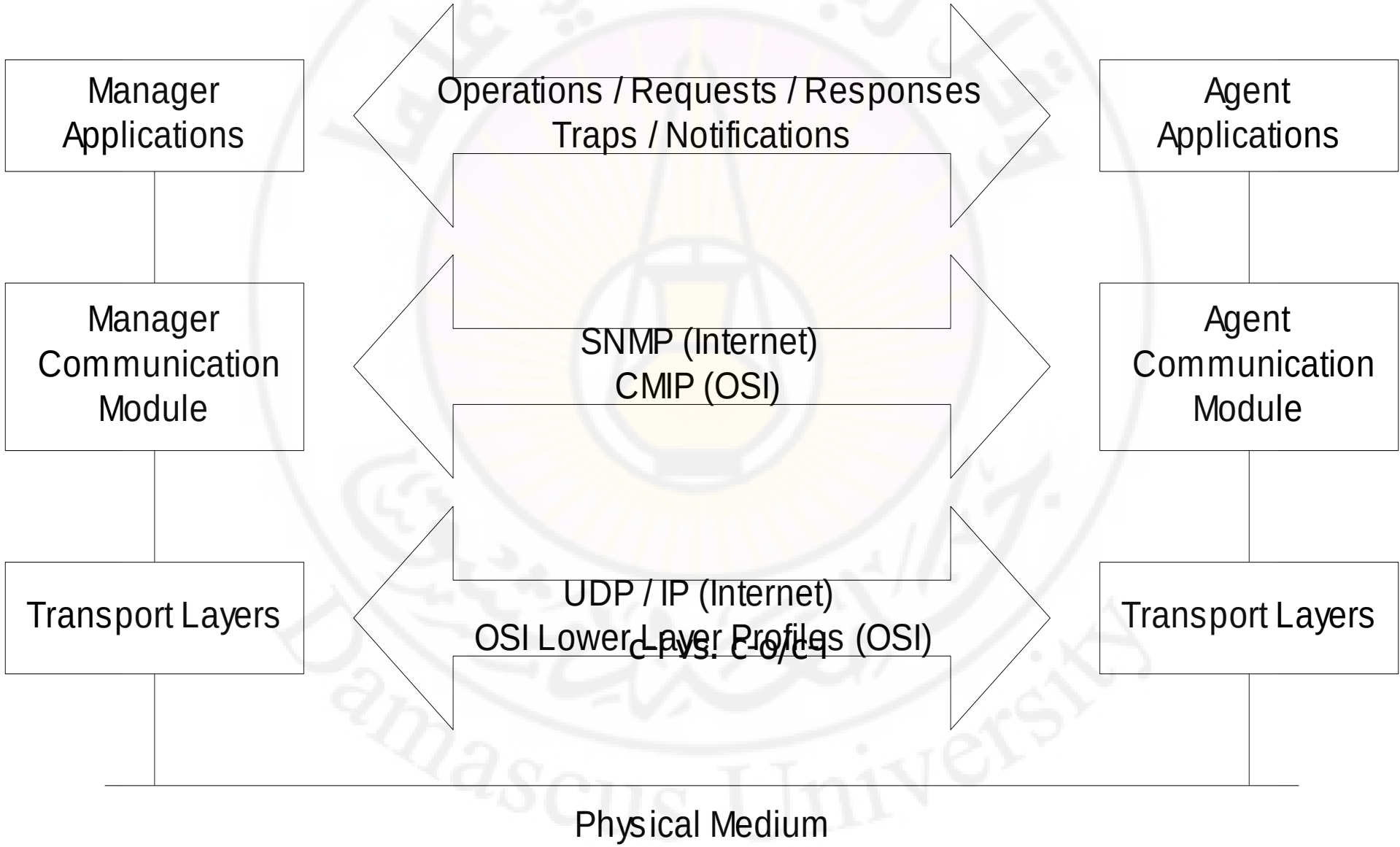
نموذج الاتصال



Internet: Request/Response ↔ OSI: Operations

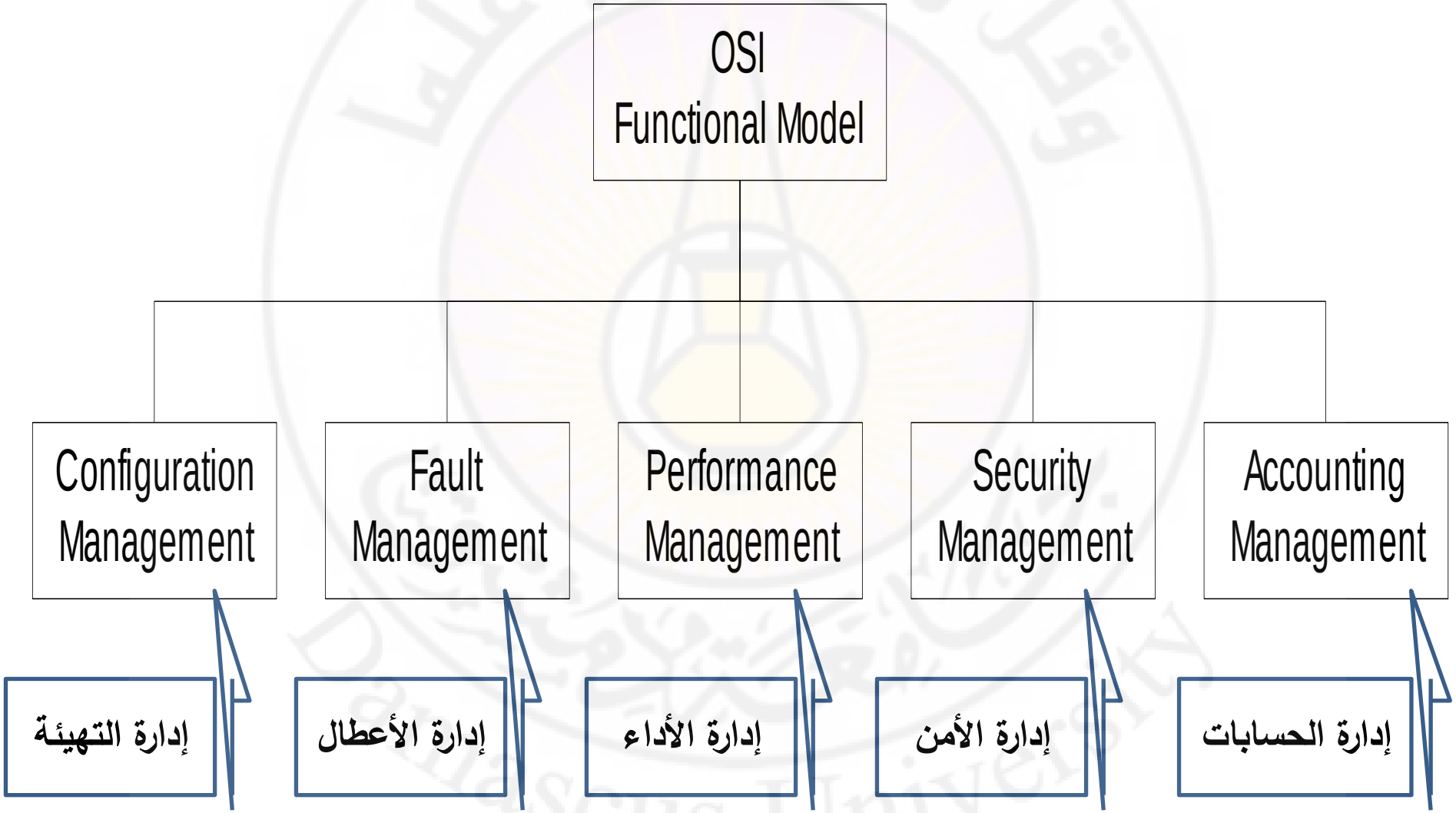
Internet: Traps/Notifications ↔ OSI: Notifications

بروتوكولات التحويل أو الانتقال



C++ vs. C-o/c-1

النموذج الوظائفي لإدارة الشبكة وفقاً لـ OSI



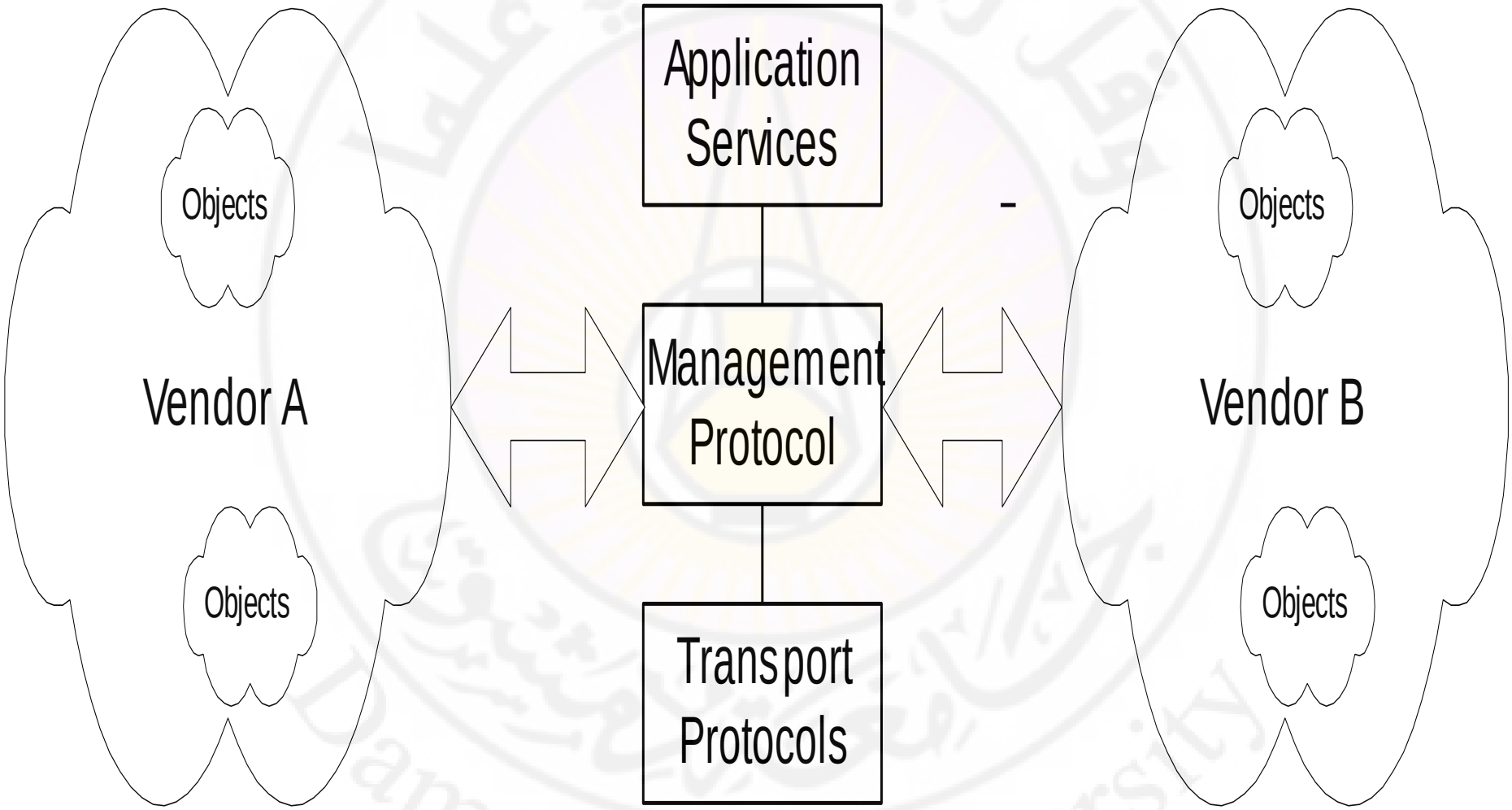
- إدارة التهيئة:
  - وضع وتغيير تهيئة الشبكة وبارامترات المكون.
  - تنفذ الإنذارات.
- إدارة العطل أو الخطأ:
  - اكتشاف وعزل الفشل في الشبكة.
- إدارة الأداء أو الخصائص.
- إدارة الأمن أو السرية:
  - الدخول أو الولوج إلى مصادر الشبكة.
  - التحقق، الشرعنة، والتشفير.
- إدارة الحسابات:
  - حسابات الشبكة.
  - كلفة الشبكة.

- ركزنا في ما سبق على جلب قيم الأغراض المُدارة من الوكيل لكن لابد لأي بروتوكول إدارة أن يوفر لنا إمكانية تغيير إعدادات أي جهاز مُدار ضمن الشبكة لتحقيق هدف معين كتحسين الأداء أو تفعيل خدمة معينة. بالإضافة لضبط بعض العتبات التي تسمح للوكيل بإرسال تقرير للمدير بتجاوز هذه العتبة على سبيل المثال (تحديد حجم الاستهلاك في الانترنت) عند تجاوز الاستهلاك على منفذ معين مقدار حجم معين بالبايت يمكن إرسال رسالة تنبيه للمدير تفيد بذلك.

- يمكن للوكيل إرسال إشعارات دون طلب من المدير ويمكن أن تحوي هذه الإشعارات على معلومات مثلاً حدوث خلل في جهاز ما أو خدمة معينة.

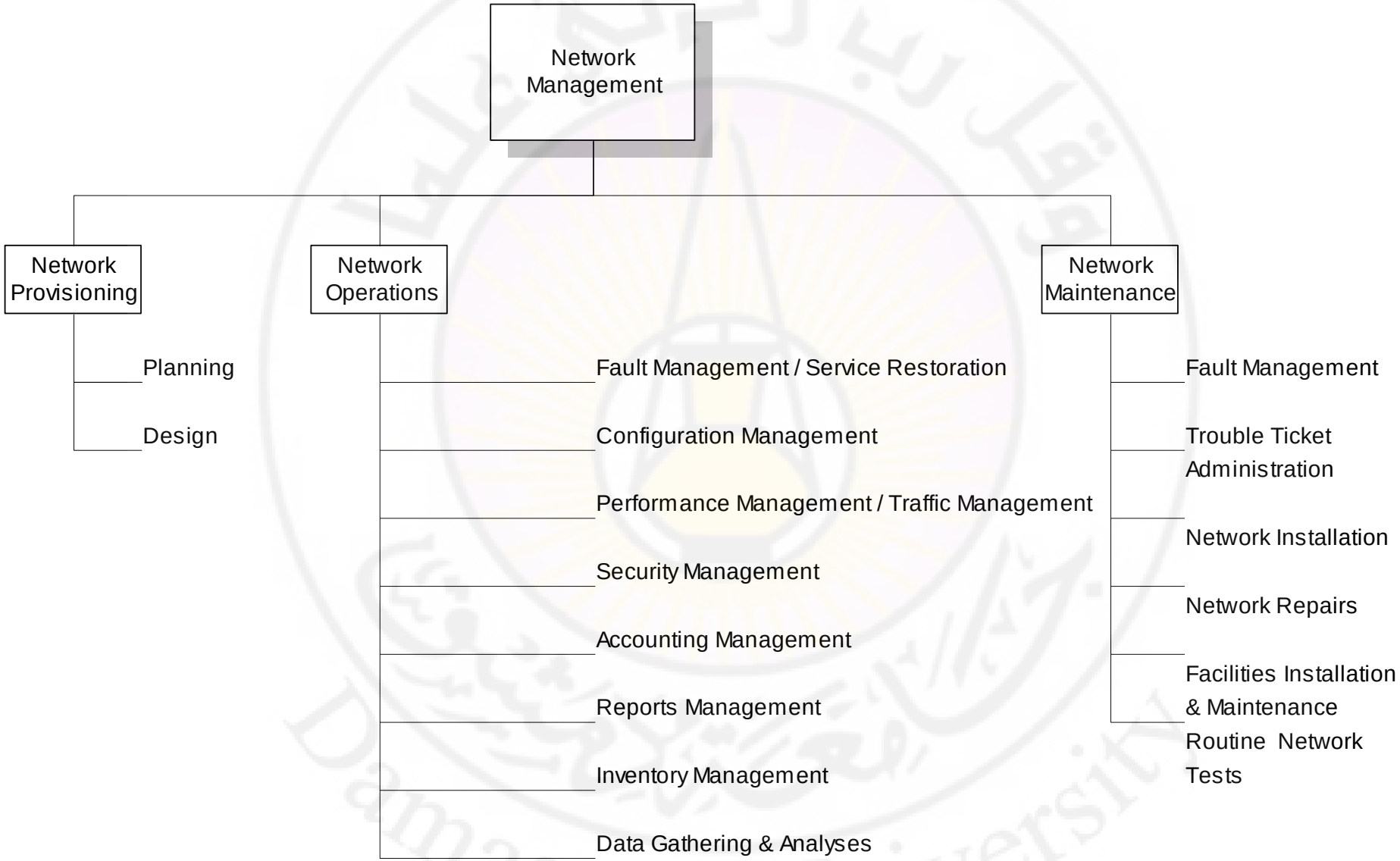
- يجب أن يكون البروتوكول يراعي عامل الأداء الجيد دون التأثير على الشبكة.
- كما ويجب مراعاة آليات الحماية (كتشفير الرسائل وحمايتها، تحديد الأشخاص المخول لهم الوصول لبيانات الإدارة وكيفية التوثق من هوياتهم).
- أخيراً لابد من تحديد كم الاستهلاك وكلفة تشغيل هذه الخدمة ضمن الشبكة.

يوضح الشكل التالي التشاركية ما بين المشتركين:

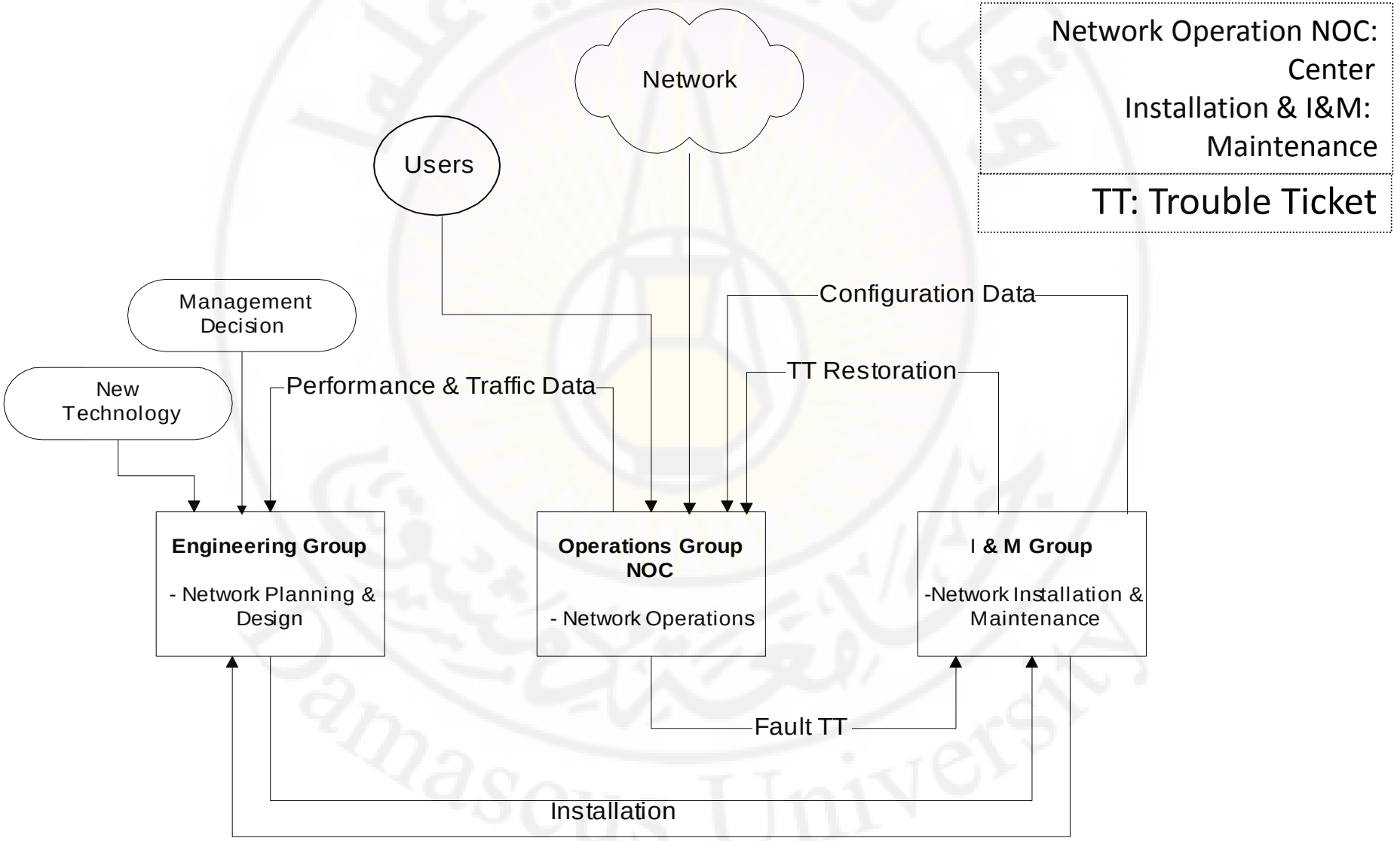


وظائف إدارة الشبكة

وظائف إدارة الشبكة



المخطط الوظائفي لإدارة الشبكة



وظائف إدارة الشبكة

- إدارة التهيئة: تعلمك عن أين where كل شيء في الشبكة.
- إدارة الأعطال: تعلمك ماذا what تعمل الشبكة.
- إدارة الأداء: تعلمك كيف how الشبكة تعمل.
- إدارة الحسابات: تعلمك متى when تستخدم الشبكة.
- إدارة الأمن أو السرية: تعلمك بكيفية how استخدام الشبكة.

- من أجل كل واحدة من هذه الوظائف، فإن المدير سينفذ مايلي:
  - عملية تجميع البيانات للإدارة.
  - تفسيرها.
  - التحكم بعناصر الشبكة.
- وهذه الفعاليات تكون منفذة عن بعد على عناصر الشبكة، ولكن قبل أن نشرح هذه الأفكار بشكل مفصل، فمن الضروري أن نتعرف على آلية مراقبة الشبكة عن بعد وهذا ما سنعرفه فيمايلي.

إدارة التهيئة
CM: Configuration Management

- هي عملية لإيجاد وتركيب أجهزة الشبكة.
- إدارة التهيئة تحدد، وتحل، وتتحكم، تجمع المعطيات، تزود المعطيات للنظام الشبكي.
- الشبكة يمكن أن تكون مميزة وفقاً لمعايير مختلفة ومن أهمها كما نعرف: الامتداد، الطبولوجيا، تكنولوجيا الهندسة المعمارية، التجهيزات، ولكن قبل كل شيء لابد من تحديد مفهوم الشبكة.

Damascus University

- نحتاج إضافةً إلى تأمين الأجهزة الشبكية إلى اتباع مبادئ أساسية في إدارة تصميم الشبكة لضمان أمن الشبكة، ويستخدم هنا مايلي:

  - وضع البارامترات التي تتحكم بالعمل الروتيني للنظام الشبكي.
  - ربط الأسماء مع الأغراض أو الأهداف المراد إداراتها.
  - تأسيس وإغلاق الأغراض المراد إدارتها.
  - جمع المعلومات لما هو مقبول حول الشروط الحالية للنظام الشبكي.
  - الحصول على بلاغات للتغيرات المقبولة على النظام الشبكي.
  - تغيير تهيئة النظام الشبكي.

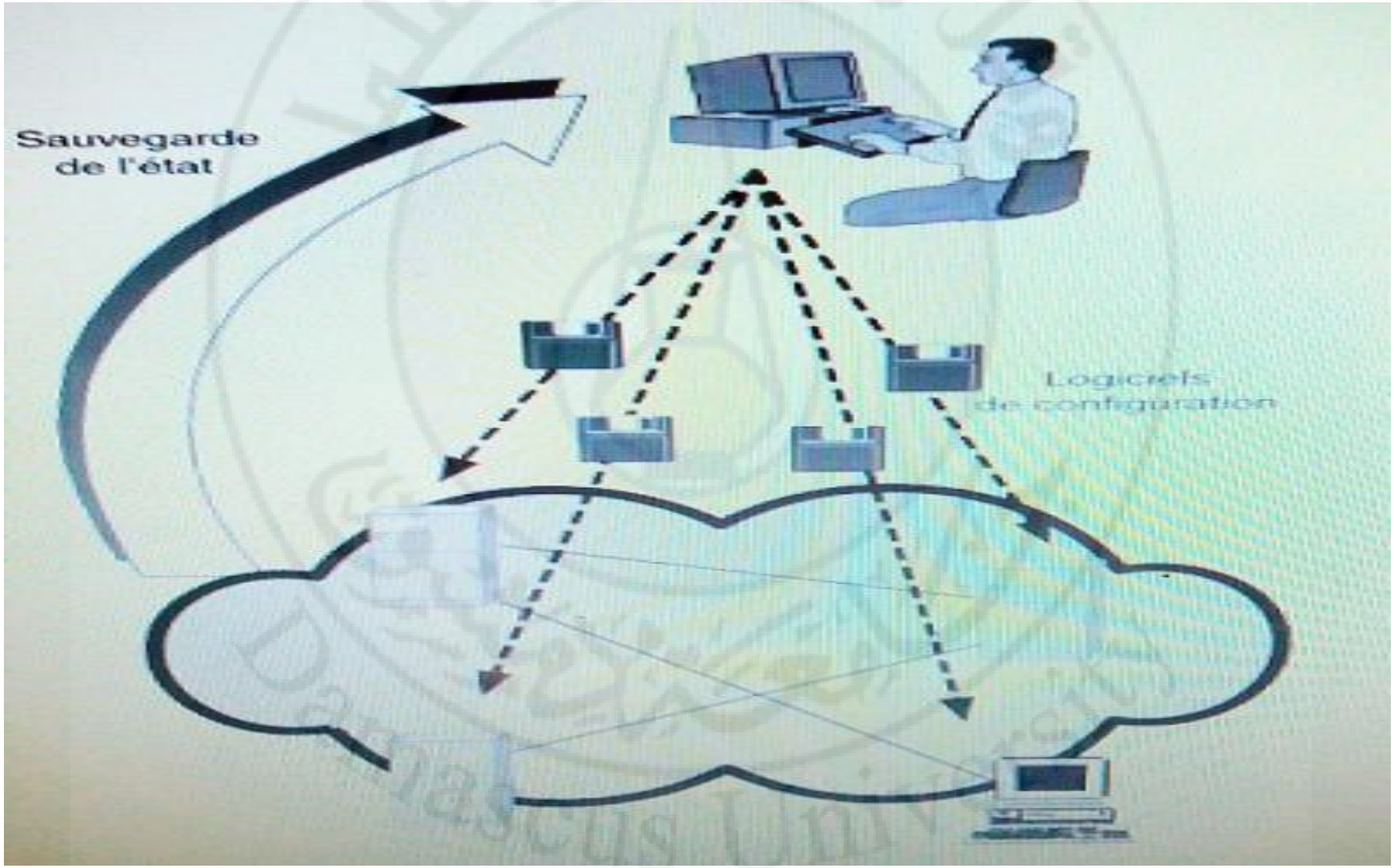
- هذه الإدارة تسمح بتعيين وتحديد قيم البارامترات المختلفة والمراحل المطلوبة واللازمة لإدارة عملية التهيئة وتكمن بـ:

  - تجميع البيانات.

  - التحكم بحالة النظام الشبكي.

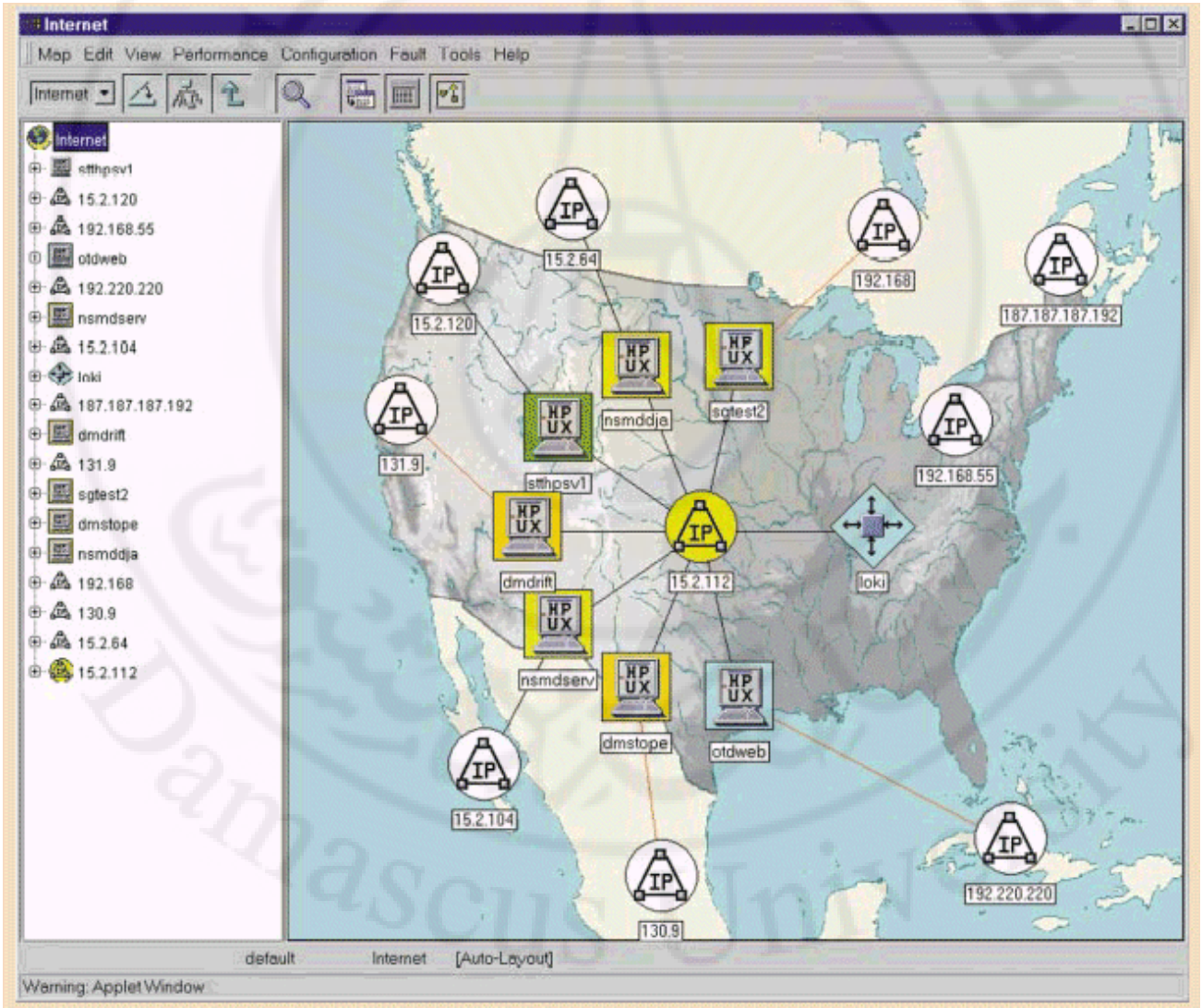
  - حفظ الحالة.

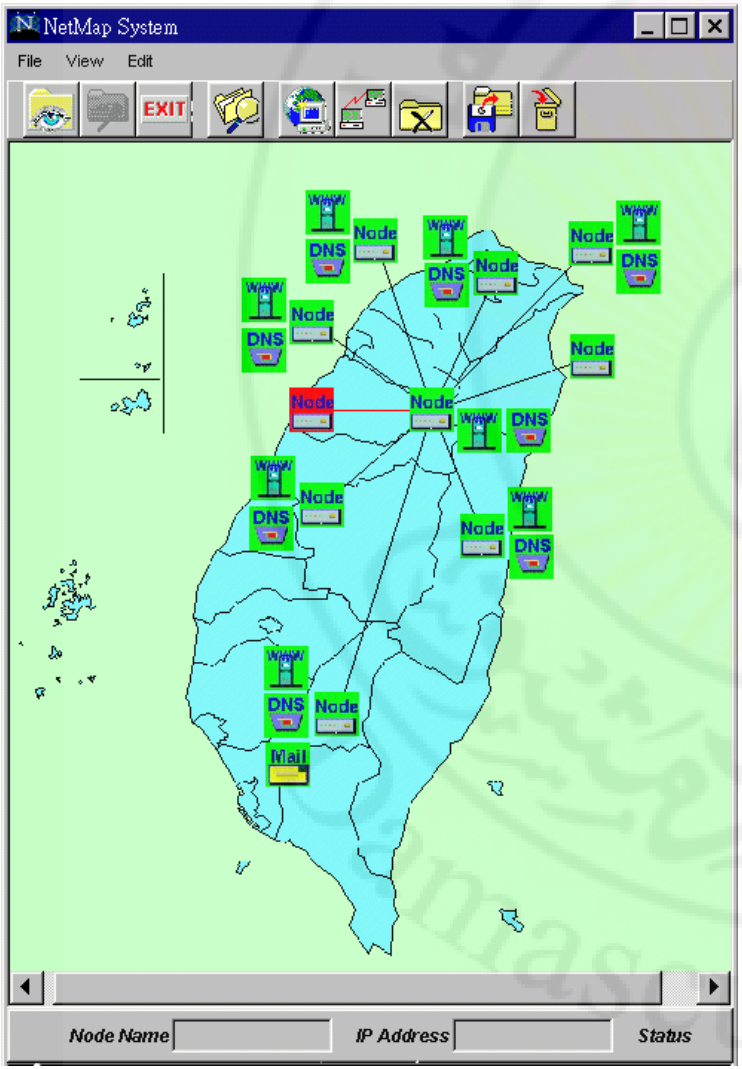
- يوضح الشكل التالي ذلك:


Sauvegarde
de l'état
Logiciels
de configuration

- هذه الإدارة يمكن أن تغطي الوظائف أو المهام التالية:
  - الاقلاع أو تلقين التجهيزات.
  - عملية تموضع البارامترات.
  - جمع معلومات الحالة والتدخل في البارامترات.
  - تعديل هيئة النظام.
  - ترابط الأسماء بالهدف المراد إدارته.
  - تغيير عنوان IP للتجهيزة.
  - تغيير عنوان IP للموجه.
  - تغيير جدول التوجيه.

إدارة التهيئة: اكتشاف آلي




NetMap System
File
View
Edit
EXIT
Node
DNS
Mail
Node Name
IP Address
Status


節點狀態顯示
新增節點
刪除節點
檢視/修改內容
尋找節點
重新整理
CHT-DNS&Mail
0%:25ms
CHT-FireW
100%:0ms
品質監控
介面資訊
刪除節點
檢視/修改內容
ODAS主機
0%:24ms
北分-FireWall
0%:22ms
北分-WWW
0%:21ms
北分-Mail
100%:0ms
北分-DNS
0%:22ms
中分-DNS
0%:29ms
中分-Mail
100%:0ms
中分-WWW
0%:30ms
總公司WAN Port
0%:25ms
數據分公司WAN Port
0%:33ms
訓練所WAN Port
0%:28ms
研究所WAN Port
0%:3ms
國際分公司WAN Port
0%:26ms
告警訊息：
清除告警
HiView
Unsigned Java Applet Window

إدارة الأعطال
(FM: Fault Management)

- إدارة الأعطال تكتشف المشكلة وتعمل على معالجتها وتصحيها والعودة للعمل الطبيعي.

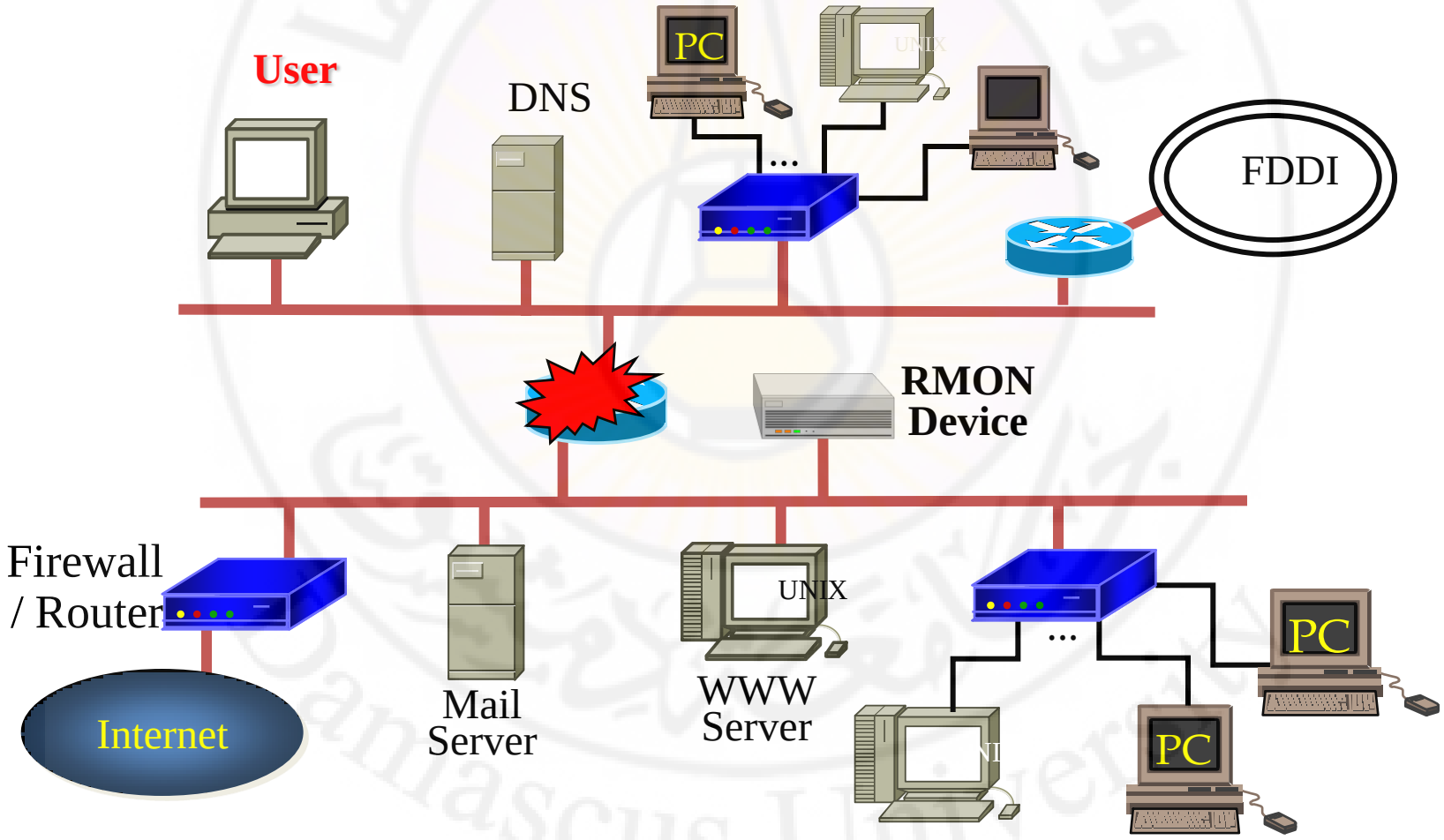
- تتضمن إدارة الأعطال الخطوات التالية:
  - اكتشاف المشكلة.
  - Isolate المشكلة.
  - تثبيت المشكلة إذا كان ممكناً ذلك وعدم تفاقمها.

- تستخدم نظام بطاقة المشكلة.

Damascus University

- صيانة وفحص الأخطاء.
- قبول ملاحظات اكتشاف الأخطاء والتصرف لتلافيها.
- متابعة وتحديد الأعطال.
- الاحتفاظ بتعقبات اختبارات التشخيص.
- تصحيح الأعطال.

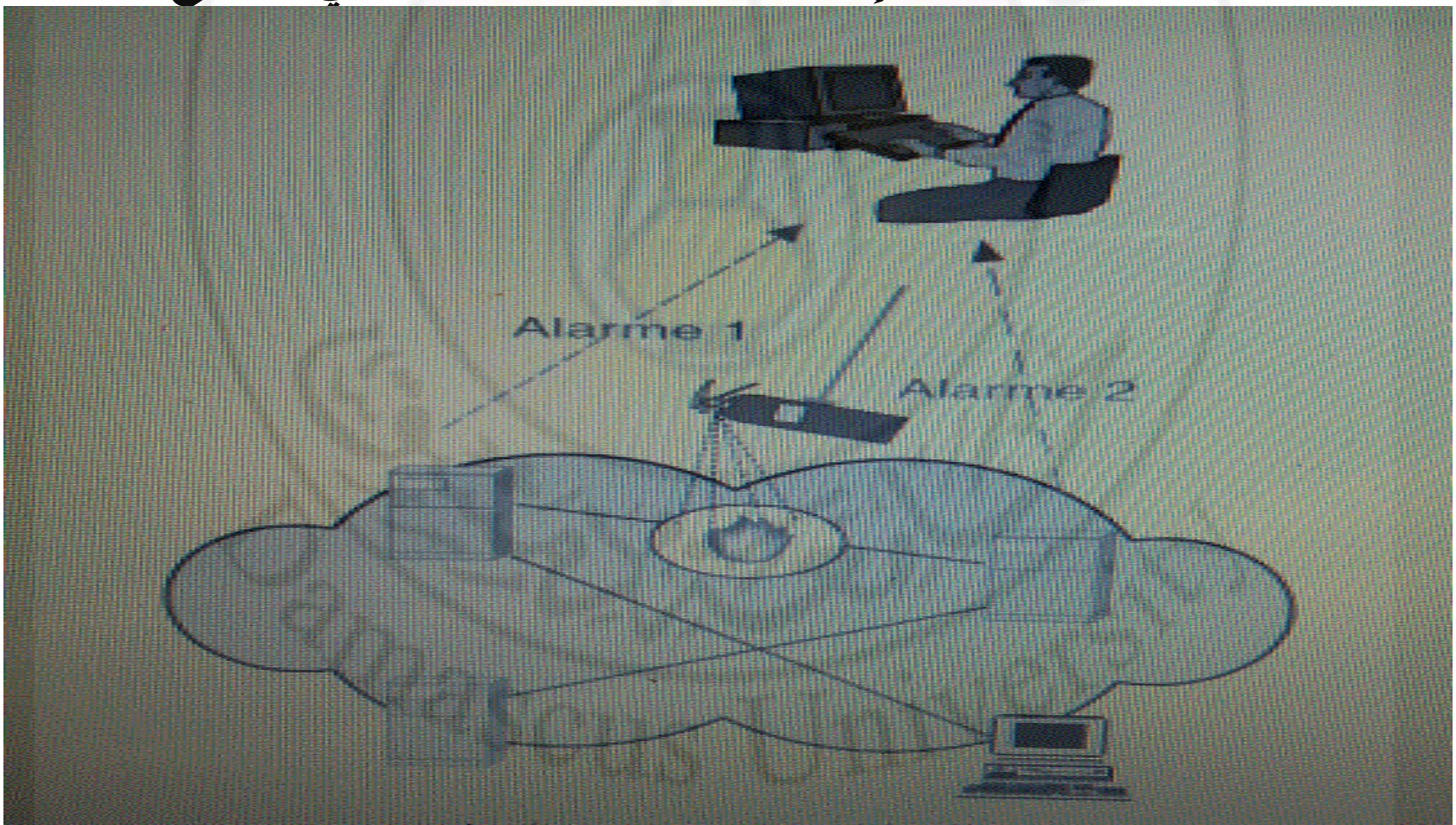
مثال على إدارة العطل



FM例子：障礙存錄


障礙存錄系統
檢視問題票
操作問題票
問題節點
168.95.64.127:T1
Record 1 of 271
問題票序號 嚴重性 狀態 開啓時間 問題節點 主題
229 39657 2 關閉 1998/07/17 10:30 168.95.95.218:T1- T1 網管資訊障礙
230 39655 1 關閉 1998/07/17 10:30 168.95.64.128:T1- 接取伺服器T1 障礙
231 39654 1 關閉 1998/07/17 10:30 168.95.64.127:T1- 接取伺服器T1 障礙
232 39653 1 關閉 1998/07/17 10:30 168.95.64.127:T1- 接取伺服器T1 障礙
233 39645 2 關閉 1998/07/02 12:24 10.1.27.6 一般伺服器 Round Trip Tim
234 39644 1 關閉 1998/07/02 11:54 10.144.18.207 一般伺服器網路介面障礙
235 39643 2 關閉 1998/07/02 11:24 10.1.27.6 一般伺服器 Round Trip Tim
236 39642 2 關閉 1998/07/02 10:39 10.1.27.6 一般伺服器 Round Trip Tim
237 39641 1 關閉 1998/07/02 10:09 10.144.73.127 一般伺服器網路介面障礙
238 39640 2 關閉 1998/07/02 08:39 10.1.27.6 一般伺服器 Round Trip Tim
239 39639 2 關閉 1998/07/02 08:24 10.79.2.254 一般伺服器 Round Trip Tim
目前顯示為已關閉之問題票：開啓年月(1998/7)
Unsigned Java Applet Window

- إن إدارة الأخطاء تسمح بكشف وتحديد الموضع الذي حدث فيه الخطأ وصيانة الأعطال والإعادة للخدمة والشكل التالي يوضح ذلك:



- هذه الإدارة يمكن أن تغطي الوظائف والمهام التالية:

– كشف الأخطاء، وتتضمن:

- تهيئة التقارير لحوادث العمل.
- إدارة العدادات أو حافات الإنذار.
- فلترة البيانات أو المعلومات.
- إعلان عدم العمل.

- تحديد الأخطاء، ويتم ذلك عن طريق:
  - تقارير الخطر.
  - القياسات.
  - الفحوصات.

– الصيانة، وتكون بـ:

- أخذ القياسات المصححة.

- إعادة التوجيه.

- الحد من الحركية أو التدفق عن طريق الفلترة أو إعادة جدولة الخدمة أو إعادة جدولة الخدمة كفحوصات الوظائف وإدارة أنظمة المنابع، ... إلخ.

- تسجيل أزمنة الحوادث والاحصائيات: إن إدارة الأخطاء هي ضرورية ولكن غير كافية لتقديم الخدمة المنتظرة لذلك هي تشمل:

  - تسجيل زمن الأخطاء وتسجيل الاحصائيات التي يمكن أن تبين احتمال وقوع الأعطال ومدة بقاء العطل وزمن الصيانة.

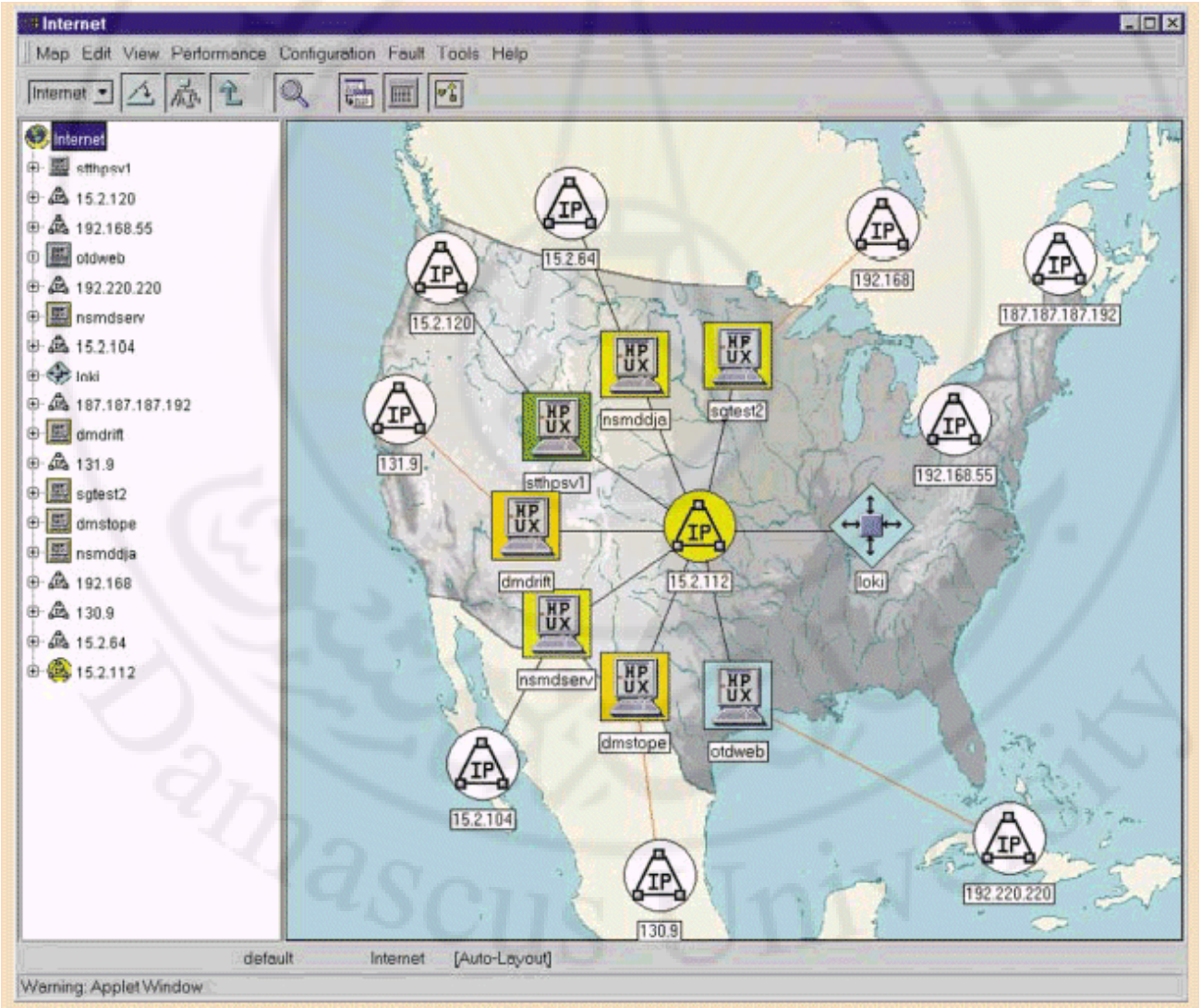
  - دور المستخدمين الذي يشتمل على إعلامهم بمشاكل الشبكة، وكذلك إمكانية التنبيه بنفسهم عن الحوادث مثل:

    * انقطاع الكابل.
    * التهيئة السيئة لإحدى التجهيزات.
    * إعادة إقلاع الحادثة والتجهيزات.

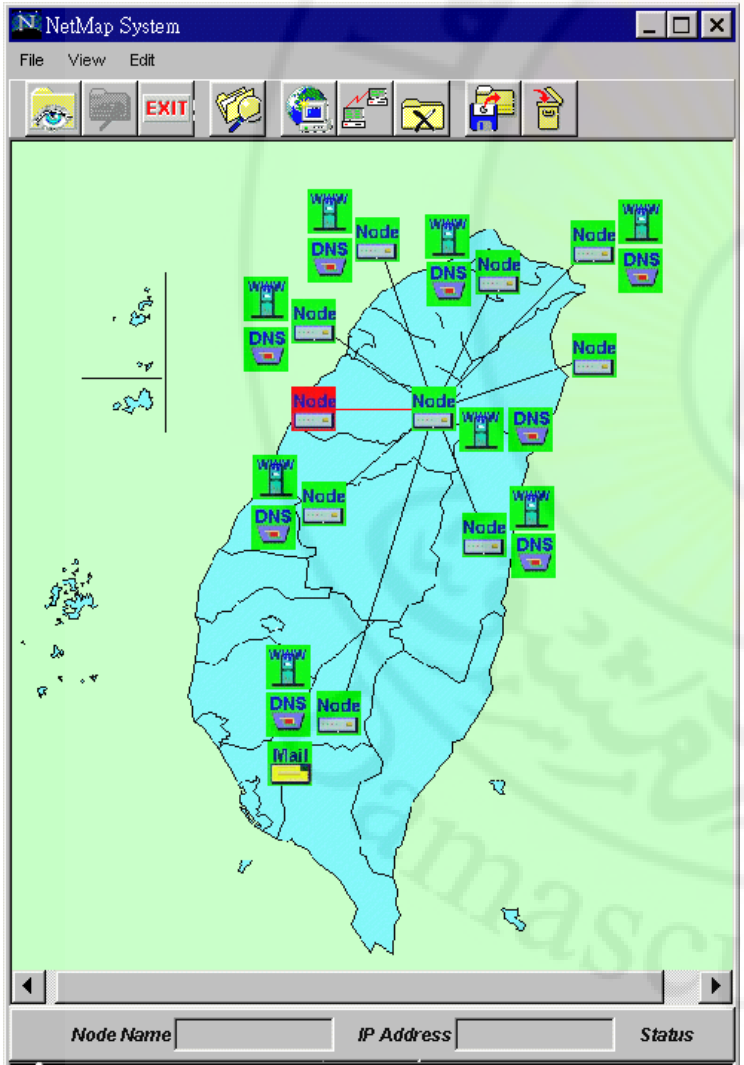
إدارة الأداء أو تقدير الخصائص
(PM: Performance Management)

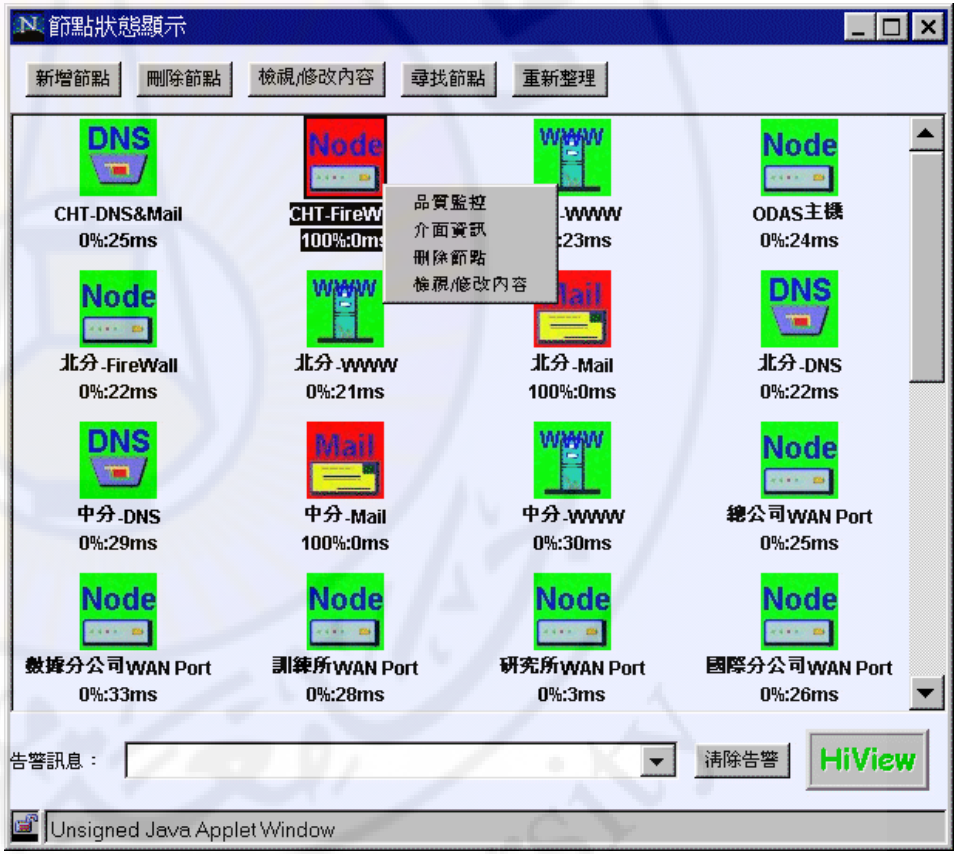
- الهدف منها قياس أداء المكونات المادية والبرمجية ووسط الاتصال للشبكة.
- البارامترات التي تقيسها:
  - Overall throughput
  - النسبة المئوية للاستخدام.
  - معدل الخطأ.
  - زمن الاستجابة.

CM: Auto Discovery



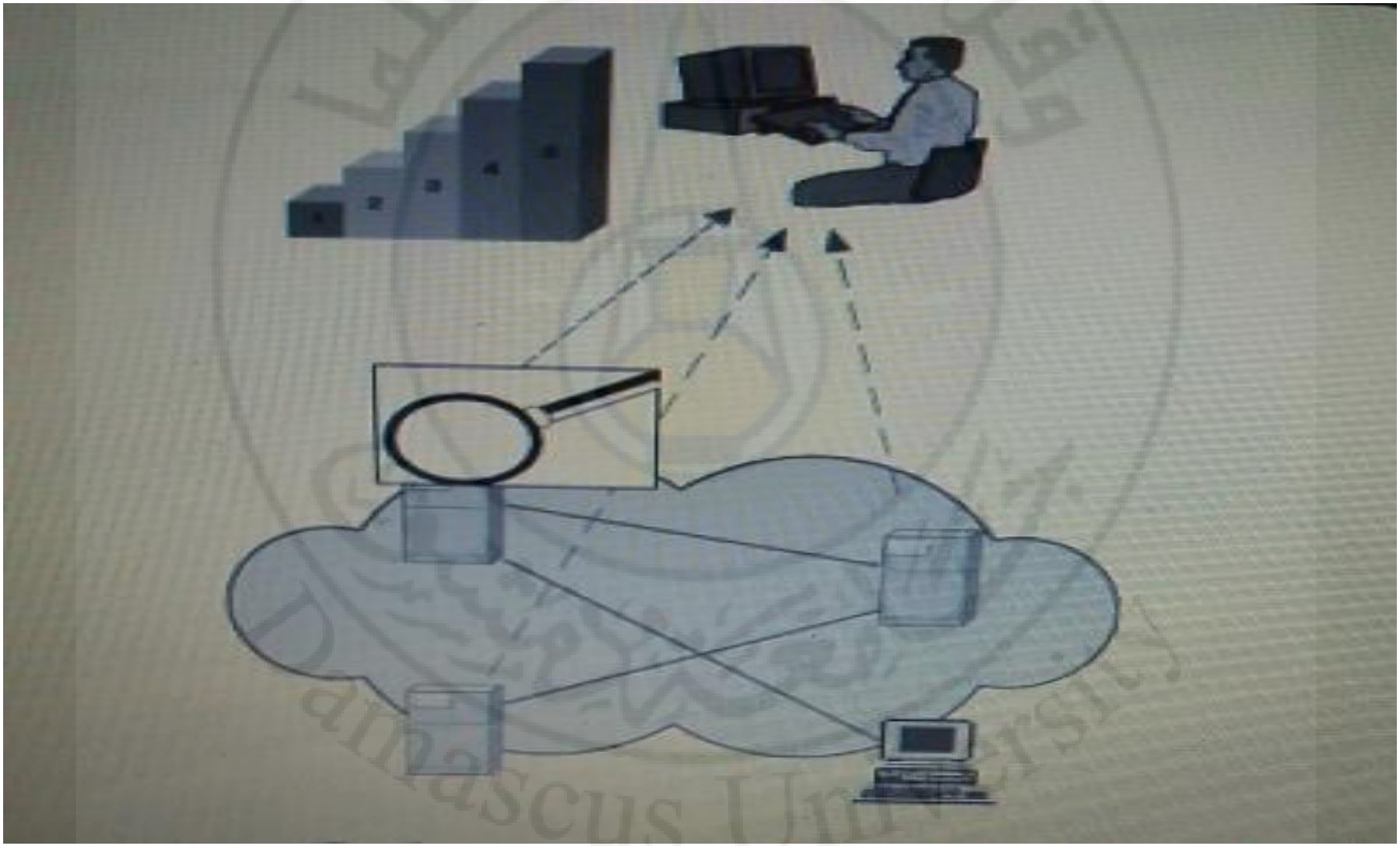
(CHTNet):CM


NetMap System
File View Edit
EXIT
Node Name
IP Address
Status

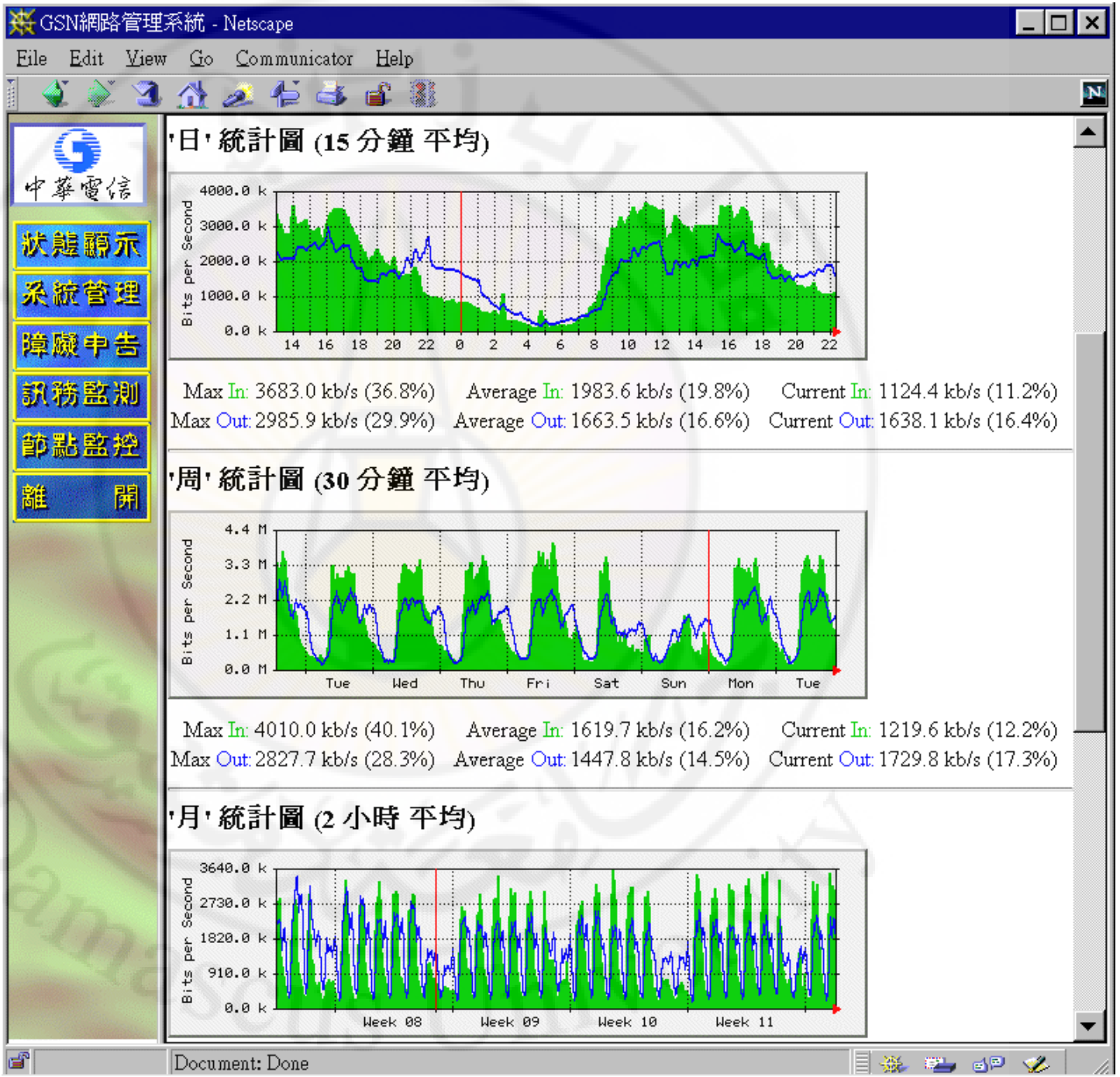

節點狀態顯示
新增節點
刪除節點
檢視/修改內容
尋找節點
重新整理
CHT-DNS&Mail
0%:25ms
CHT-FireW
100%:0ms
品質監控
介面資訊
刪除節點
檢視/修改內容
ODAS主機
0%:24ms
北分-FireWall
0%:22ms
北分-WWW
0%:21ms
北分-Mail
100%:0ms
北分-DNS
0%:22ms
中分-DNS
0%:29ms
中分-Mail
100%:0ms
中分-WWW
0%:30ms
總公司WAN Port
0%:25ms
數據分公司WAN Port
0%:33ms
訓練所WAN Port
0%:28ms
研究所WAN Port
0%:3ms
國際分公司WAN Port
0%:26ms
告警訊息：
清除告警
HiView
Unsigned Java Applet Window

مهام إدارة الأداء

- جمع معلومات إحصائية.
- فحص وصيانة ملفات الدخول وتواريخ حالة النظام.
- تحديد أداء النظام عند الشروط الطبيعية والاصطناعية.
- تغيير حالات عمل النظام الشبكي من أجل الحصول على أداء عالي منه.
- التحليل الستاتيكي قبل انتاج لوحة الجداول.
- يبين الشكل التالي ذلك:



PM demo


GSN網路管理系統 - Netscape
File Edit View Go Communicator Help
中華電信
狀態顯示
系統管理
障礙申告
訊務監測
節點監控
離 開
'日' 統計圖 (15 分鐘 平均)
Bits per Second
4000.0 k
3000.0 k
2000.0 k
1000.0 k
0.0 k
14 16 18 20 22 0 2 4 6 8 10 12 14 16 18 20 22
Max In: 3683.0 kb/s (36.8%) Average In: 1983.6 kb/s (19.8%) Current In: 1124.4 kb/s (11.2%)
Max Out: 2985.9 kb/s (29.9%) Average Out: 1663.5 kb/s (16.6%) Current Out: 1638.1 kb/s (16.4%)
'周' 統計圖 (30 分鐘 平均)
Bits per Second
4.4 M
3.3 M
2.2 M
1.1 M
0.0 M
Tue Wed Thu Fri Sat Sun Mon Tue
Max In: 4010.0 kb/s (40.1%) Average In: 1619.7 kb/s (16.2%) Current In: 1219.6 kb/s (12.2%)
Max Out: 2827.7 kb/s (28.3%) Average Out: 1447.8 kb/s (14.5%) Current Out: 1729.8 kb/s (17.3%)
'月' 統計圖 (2 小時 平均)
Bits per Second
3640.0 k
2730.0 k
1820.0 k
910.0 k
0.0 k
Week 08 Week 09 Week 10 Week 11
Document: Done

- تقدم هذه الإدارة الوظائف التي تسمح بالوصول للنهاية وفق التخطيط الكامل لموارد الشبكة ومنها نذكر:

  – تجميع البيانات: معدل الأخطاء، أزمنة العبور، سرعة النقل، ... إلخ.

  – حفظ وتحليل النشرات لحالة النظام.

- إن هذا القسم من الإدارة يقسم لقسمين هما:

  – إدارة تقدير الخصائص بالزمن الحقيقي.

  – إدارة تقدير الخصائص بالزمن المؤخر أو المغاير.

- من أجل تقدير الخصائص بالزمن الحقيقي فإنه يتوجب على الوظائف التالية أن تكون مهيأة:

– تسجيلات قياسات تقدير الخصائص وهذه تكون بـ:
  – التهيئة والوضع بالخدمة ضمن الشروط الدقيقة للقياس.
  – إدارة جمع المعلومات.
  – الفلترة.
  – تجميع الاحصائيات.
  – ملائمة القياسات حسب الطلب أو حسب إدارة الملفات المجمعة.
– مراقبة فعالية الشبكة بواسطة:
  – إظهار استخدام الموارد.
  – الإعلام عن تجاوز الحدود.
  – التحليل لتقدير الخصائص.

- هذا يفرض:

–إظهار وظيفة الشبكة (تقاسم الحمل، اختلاف سرعة النقل، زمن الاستجابة، الجاهزية، ... إلخ).

–تحليل الأسباب الممكنة التي تسبب تجاوز الحدود المسموحة. ".

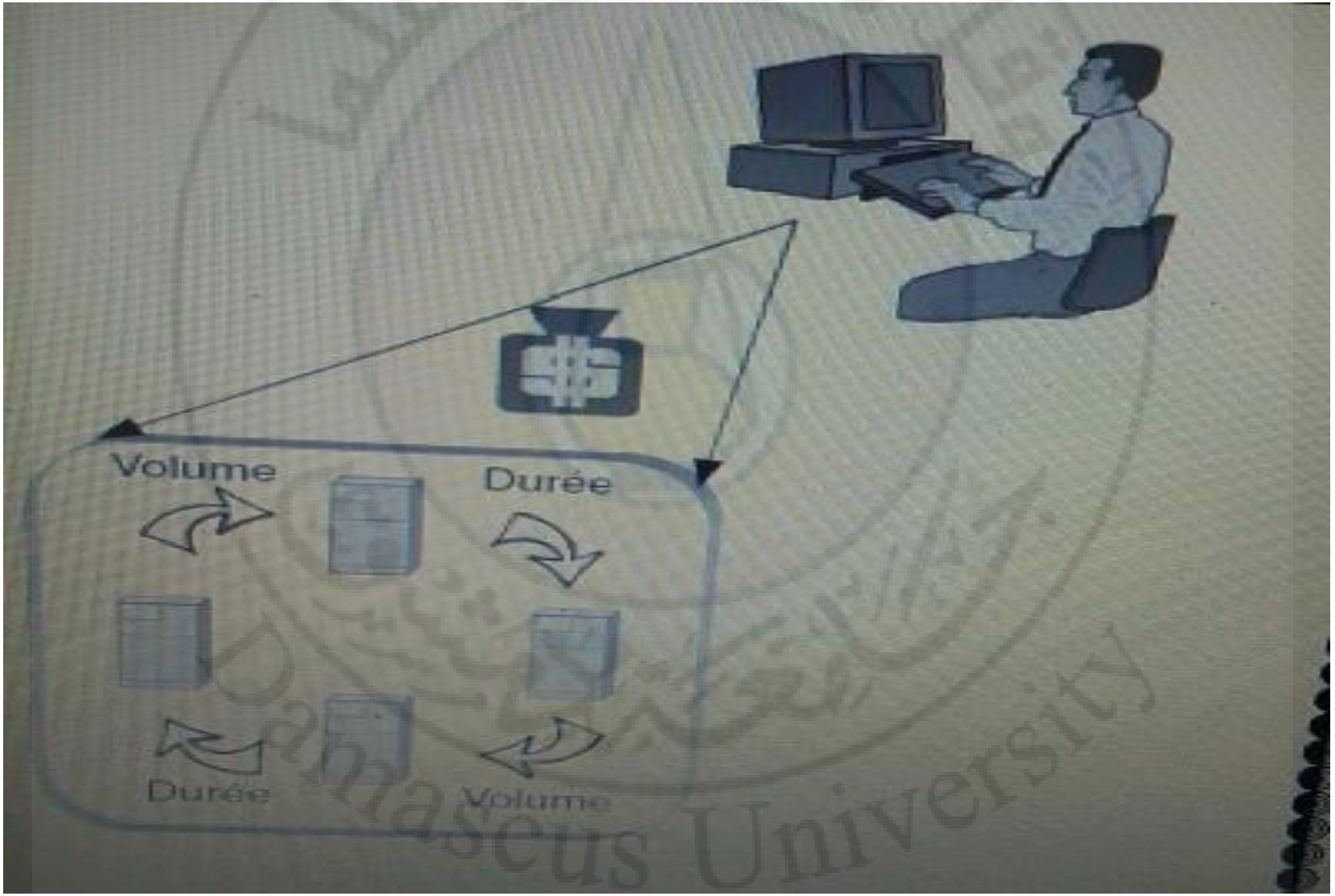
- تغيير التهيئة لأخذ القياسات المصححة والوقائية، فإدارة القياسات المصححة تركز على كشف مشكلة تقدير الخصائص بإعادة تخصيص الموارد وذلك بواسطة تعديل بارامترات التهيئة أو بواسطة إعادة نشر الحركية للشبكة، أما إدارة القياسات الوقائية فتركز على أخذ القياسات الأولية التي تسمح بتجنب الوصول للمرحلة الحرجة وهذه الحالة تنفذ بزمن مختلف وتشمل:
  - تحليل المعلومات بواسطة التجميع الإحصائي.
  - نشر لوحة جداول التقارير والتي يمكن أن تكون دورية أو تصنع بناءاً على الطلب.
  - بعض أشكال التحاليل المتوقعة تكون بواسطة مصفوفات الحركة، اكتشاف مخاطر حالات الإشباع، نمذجات سيناريوية، تخطيط حجم الشبكة "أبعاد".

إدارة الحسابات أو المحاسبة
(AM: Accounting Management)

- تتابع إدارة الحسابات كل استخدام شخصي أو لمجموعة من الأشخاص لمصادر أو موارد الشبكة بهدف التأكد من أن المستخدمون يمتلكون موارد مقبولة وكافية.

- تمكن إدارة الحسابات charges ليكون مؤسساً من أجل موارد الشبكة وتحديد الكلفة لاستخدام هذه الموارد الخاصة بالشبكة.

- تسمح هذه الإدارة بمعرفة مهام الأشياء المراد إدارتها وكلفة الاتصالات وهذه التقديرات تكون منظمة كتابع لحجم وزمن النقل والشكل التالي يوضح ذلك:


Volume
Durée
Durée
Volume

مهام إدارة الحسابات

- إعلام المستخدمين عن كلفة استخدام موارد الشبكة.
- تمكين حدود الحسابات التي توضع وتنظيم هيكلتها لاستخدام موارد الشبكة.
- تحديد الكلف عند وجود مشاركة للعديد من الموارد لاختيار هدف اتصال المعطى.
- القياسات على استخدامات الموارد وتسجيلاتها للحصول على التوصيف الزمني.
- التحكم بالحصص النسبية عن طريق المستخدم الذي يوضع بالخدمة والاستهلاك الدائم لموارد الشبكة والتحقق من سماحية الاستهلاك.

- **المراقبة والتحكم بالاستهلاك أو الصرفيات عن طريق:**

  - **التخزين ووضع تعرفة للمشغلات.**

  - **إدارة قسم الضرائب.**

  - **تقدير الزمن الحقيقي للاستهلاك الدائم.**

  - **التحقق من الفواتير.**

  - **تحديد كلفة الاستثمار.**

- الإدارة المالية: بشكل بديهي نجد في إدارة الحسابات قسم مالي والذي يرتكز على:
  - مراوحة الأسعار (الخدمة، المستخدم، التطبيق).
  - التحليل والتنبؤ بالاستهلاك.
  - دراسة احتمال تخفيض الأسعار.

❑ الفوترة: إن فعالية إدارة المحاسبة تصل في النهاية للفوترة الداخلية وهذا يفرض:

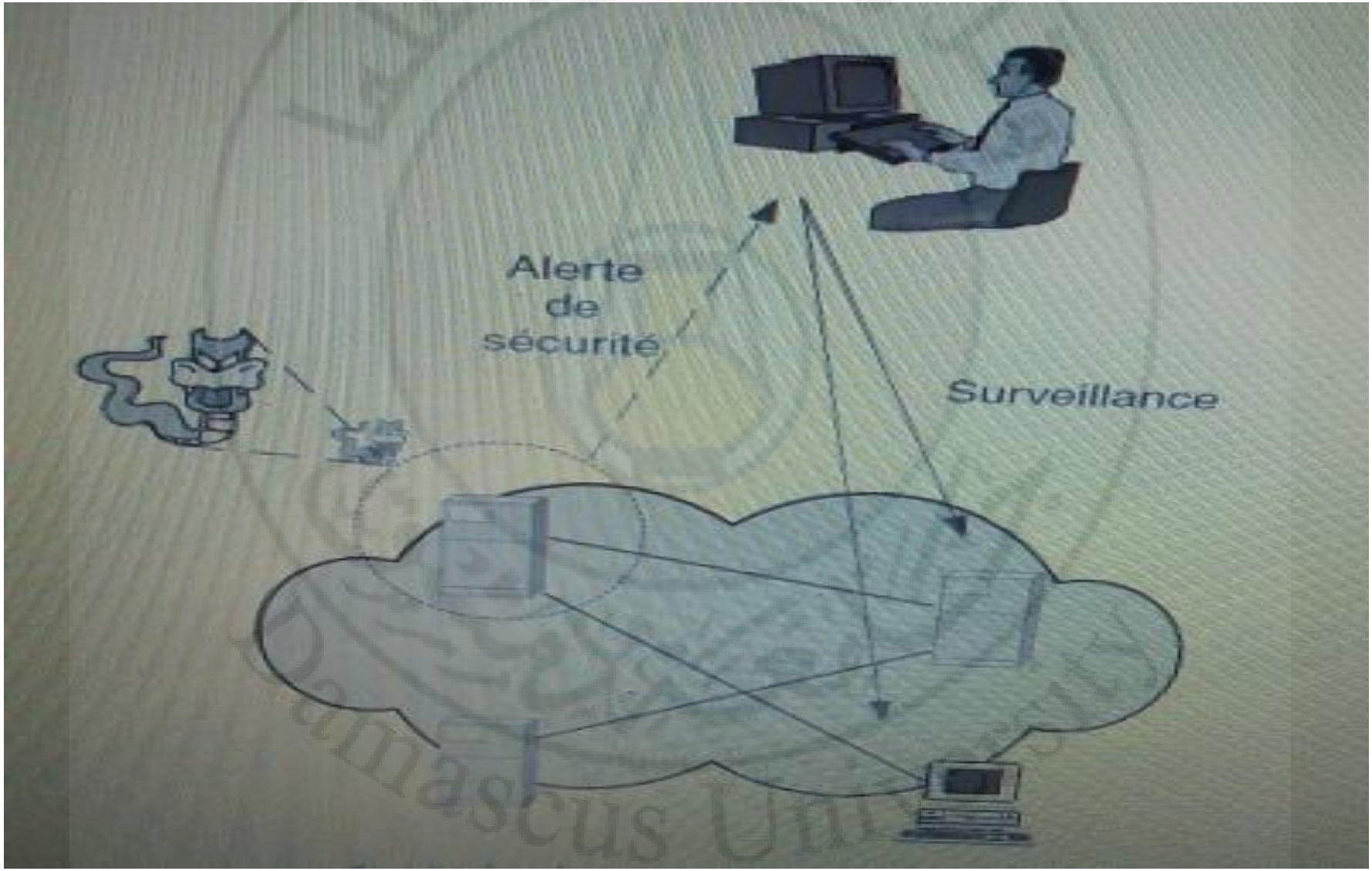
- إدارة الزبائن.
- إصدار الفواتير.
- التخزين الزمني

إدارة السرية أو الأمن
(SM: Security Management)

- إدارة السرية: هي العمل الذي يشتمل على مراقبة توزع وجريان المعلومات المستخدمة لضمان أمنها وسريتها وهي تشتمل بشكل عام على التشفير ولائحة سماحيات الوصول أو عملية التحكم بدخول المعلومات إلى النظام الشبكي.

- يوضح الشكل التالي ذلك:

Damascus University


Alerte
de
sécurité
Surveillance

- مهام إدارة الأمن:
  - إنشاء، حذف، تحكم بخدمات الأمن وآلياتها.
  - توزيع معلومات الأمن ذات الصلة.
  - إصدار تقارير عن الأحداث الأمنية ذات الصلة.
  - دعم التوثيق.
  - المراقبة وتثبيت السماحيات.
  - المراقبة وتثبيت طلبات المنافذ.
  - إدارة المفاتيح.
  - صيانة وتثبيت وفحص ملفات الأمن.

- لدعم سياسات الشبكة، فإن إدارة الشبكة تشتمل على جمع المعلومات لإدارة الشبكة وتفسيرها وفيمايلي الأعمال المتوجب وضعها لتنفيذ ذلك:

  - ضمان الأمن النسبي لإدارة الشبكة هي بذاتها وهذا يعني:

    - إدارة حقوق النفاذ لمواقع العمل.
    - إدارة الحقوق المرتبطة بالمشغلات.
    - السماحيات بالوصول إلى معلومات الإدارة.

- ضمان أمن وسرية منافذ الشبكة الخاصة بالإدارة، ومن أجل ذلك يجب وضع الآليات التي تفرض أعمالاً والتي يتم بواسطتها مايلي:

- تحديد شروط الاستخدام.

- تعديل البارامترات.

- إدارة لوائح السماحيات.

- تنفيذ المراقبة للمنافذ (هويات، توقيت، زمن التوصيل، اتجاه التوزيع، ... إلخ).

- كشف محاولات الدخول الاحتيالي والدخول غير الشرعي.

- تزيد إدارة الشبكات الآمنة من صعوبة إدارة الشبكات، لذلك من الأهمية بمكان عند إدارة الشبكات الآمنة اتباع مقاربة إدارية معتمدة على القواعد الإجرائية والتقنية، ويمكن تعريف هذه القواعد على أنها التوجيهات الرسمية والإلزامية للسلوك. إن القواعد الإجرائية هي التي تفرض القواعد التقنية كإعداد جدار نار أو مخدم وكيل للتوافق مع التوجيهات الإجرائية، حيث يقع على مسؤولية مدير الشبكة اتباع القواعد الإدارية المفروضة ويشمل هذا عادةً على القواعد التقنية المرتبطة بالأجهزة الأمنية وتصميم الشبكة وحماية البوابات، وسنفصل فيمايلي شرح كل واحدة على حده.

١- أمن الأجهزة: نذكر من الوظائف التي يمكن أن تتضمنها إدارة الأجهزة الإعداد الأمن للمسيرات وتحقيق حارس الإغراق وتحليل سجلات الأجهزة، وفيمايلي شرح هذه الأمور بشيء من التفصيل:

آ- الإعداد الآمن للمسيرات: يعتبر المسير من المكونات الرئيسة في الشبكات حيث يعمل على مستوى الطبقة الثالثة (طبقة الشبكة)، وهو مسؤول عن توجيه الطرود عبر مجموعة من الشبكات. بما أن الطرود تمر عبر المسير، فيمكن أن يؤدي بعض المهام الأمنية مثل تلك المتعلقة بتصفية الطرود على المستوى الثالث ومن هنا تأتي أهمية إعداد المسير بعناية لتأمين الحماية اللازمة للشبكات الموصولة إليه.

ب- حارس الإغراق Flood Guard: تعتبر هجمات حجب الخدمة DOS و DDOS من أخطر الأنواع للهجمات، حيث يستخدم حارس الإغراق كأحد وسائل الدفاع ضد هذا النوع من الهجوم، وهي ميزة تتحكم بمقدار تحمل جهاز ما لطلبات خدمة لم يتم الرد عليها وتساعد في تجنب هجمات حجب الخدمة. يستطيع مدير الشبكة تحديد العتبة العليا للعدد الأعظمي لطلبات تأسيس الاتصال التي يستطيع الجهاز تحملها. عند الوصول إلى العتبة العليا يجري اعتراض أي طرد جديد موجه إلى أحد المخدمات وإسقاطه ويمكن العثور على حارس الإغراق في تجهيزات مثل جدران النار وأجهزة كشف و/أو تجنب التسلل IDS/IPS.

ت- تحليل السجلات **Log Analysis**: تحوي السجلات الأحداث التي تقع وتعتبر هامة جداً إذا كانت متعلقة بأمن الحواسيب، ويمكن أن تكون عملية مراقبة هذه السجلات مفيدة لمعرفة طريقة حدوث الهجوم ولمعرفة إذا تمت مقاومته بنجاح. يمكن تصنيف السجلات المتعلقة بأمن النظام ضمن الحواسيب ضمن صنفين هما:

- سجلات نظام تشغيل.
- سجلات التطبيق الأمن.

أما أجهزة الشبكة العتادية فهي تولد سجلات تعكس حالة كامل الشبكة. في حال كان الجهاز الذي يولد السجلات هو جهاز متخصص بالأمن كجدار النار فمن الممكن العثور على معلومات أمنية محددة ضمن هذه السجلات، ونذكر من أنواع سجلات الأجهزة الأمنية مايلي:

- الأنظمة الشبكية لكشف التسلل NIDS، والأنظمة الشبكية لتجنب التسلل NIPS: حيث يسجل هذا النوع من الأنظمة معلومات أمنية تفصيلية متعلقة بالتصرفات المشبوهة وبالأفعال التي قام بتنفيذها جهاز NIPS لتعطيل هذه الهجمات.

- أنظمة أسماء النطاقات DNS: حيث يخزن مخدم الأسماء سجلات متعلقة بجميع الطلبات التي تم استلامها بما فيها الطلبات الخاطئة أو رسائل التنبيه.
- المخدمات الوكيلية Proxy Servers: حيث تخزن هذه المخدمات جميع عناوين URL التي تم النفاذ إليها من خلالها.
- جدران النار Fire Walls: يمكن أن تفيد هذه السجلات في إيجاد عناوين IP جديدة تحاول استكشاف الشبكة وبناءاً على ما سبق تحديد ضرورة وضع قواعد أمنية أشد لمنع المهاجم. تعتبر سجلات جدران النار التي تزود معلومات أساسية فقط محدودة الفائدة.

أما بالنسبة لنوع المعلومات الواجب فحصها ضمن سجلات جدران النار فهي:

١- عناوين الانترنت التي تم رفضها وإسقاط طرودها: حيث تفيد هذه المعلومات في معرفة المؤسسة أو الموقع التي قدمت منها الطرود المرفوضة الأمر الذي يسهل على مدير جدار النار عملية الاتصال بمالك هذه المؤسسة لتوضيح سبب قيام أشخاص ينتمون لها في توليد طرود استكشاف أو طرود مرفوضة على الشبكة.

٢- استكشاف البوابات التي لا يوجد خدمات تطبيقية مرتبطة بها: عادةً قبل أن يحاول مهاجم ما تنصيب برنامج طروادي على حاسب ما بغية خلق باب خلفي، فإنه يقوم باستكشاف كون البوابة التي يعمل عليها هذا الطروادي مخصصة لتطبيق أخر على الحاسب الضحية، لذلك يمكن أن تفيد سجلات جدار النار في مقارنة البوابات المفتوحة غير المعروف هدفها مع البوابات التي يستخدمها برامج الأبواب الخلفية الشائعة.

٣- الطرود المسيرة من المصدر: أي طرد يحمل عنوان مصدر داخلي لكن جرى توليده من خارج الشبكة يمكن أن يدل على محاولة مهاجم غش (تزييف) عنوان داخلي في سبيل النفاذ إلى الموارد الداخلية.

٤- اتصالات خارجة مشبوهة: كشف اتصال خارجي لمخدم ويب عام يمكن أن يدل على أن مهاجم ما استطاع شن هجمات على مواقع أخرى من خلال المخدم.

٥- الدخول الفاشل: عند اكتشاف عدة محاولات دخول فاشلة من نطاق ما، فيجب خلق قاعدة جديدة تمنع أي اتصال من هذا النطاق.

- نحتاج إضافةً إلى تأمين الأجهزة الشبكية إلى اتباع مبادئ أساسية في إدارة تصميم الشبكة لضمان أمن الشبكة، ويستخدم هنا مايلي:

آ- فصل الشبكات: ويقصد بها منع أجزاء تنتمي إلى شبكة محمية من الاتصال بالشبكات الخارجية أو غير المحمية لتجنب تجسير الشبكات كمنع الشبكة الخاصة بالطلاب مثلاً من الدخول إلى الشبكة المخصصة لشؤون الطلاب، ويمكن تحقيق فصل الشبكات فيزيائياً عن طريق وصل حواسيب الطلاب إلى مبدلات ومسيرات مختلفة.

ب- الحماية من الحلقات: يبين الشكل التالي مثالاً عن تشكيل حلقة مكونة من ٣ وصلات بين ٣ مبدلات، ففي حالة عدم استخدام بروتوكول شجرة التغطية STP عند هذه المبدلات فإن ظاهرة عاصفة البث يمكن أن تحدث إذا أرسل المضيف Z رسالة إلى المضيف X وكانت المبدلات الثلاثة لا تعرف البوابة الموصولة إلى المضيف X. يمكن لهذه الظاهرة أن تعرف الشبكة في ثوان معدودة وتجعلها غير مستقرة بسبب دوران الإطار في الشبكة إلى اللانهاية.

ت- إدارة الشبكات المحلية الافتراضية: إن استخدام الشبكات المحلية الافتراضية يسمح بتجزئة الشبكة الكلية إلة عدة مجموعات مناطقية تربط كل شبكة جزئية افتراضية مستخدمين متباعدين جغرافياً ومتناثرين حول الشبكة الكلية (كل مستخدم موصول على مبدلة مختلفة) الأمر الذي يقلل حركات المرور ويزيد الأمن.
يوجد عدة مبادئ عامة لإدارة مثل هذه الشبكات وهي:

- يجب أن لا تتواصل هذه الشبكات مع أخرى إلا عن طريق مسير.
- إعداد بوابات المبدلات الحرة على أنها تتبع الشبكات الافتراضية الخاصة غير المستخدمة.
- يجب تغيير أسماء الشبكات الافتراضية الخاصة المحلية.
- إعداد بوابات المبدلات التي تمرر طرود الشبكات الافتراضية الخاصة المحلية الموسومة بشكل يسمح بتوجيه سمات محددة.
- يجب عدم وضع الأجهزة العامة مثل مخدمات تطبيقات الوب ضمن شبكة افتراضية محلية خاصة.

أمن البوابات
(SG: Security Gate)

- يعتبر تأمين البوابات خطوة مهمة وهامة في إدارة الشبكات، حيث يمكن تأمين البوابات عن طريق مايلي:

- تعطيل البوابات غير المستخدمة: يمكن هنا مثلاً تعطيل البوابات غير المستخدمة على المبدلة. تسمح أي مبدلة لا تستخدم بروتوكول أمن البوابات لأي مهاجم استطاع أن يرتبط ببوابة غير مستخدمة من تحقيق هجمات على الشبكة ويجب على مدير الشبكة النفاذ على جميع المبدلات وتعطيل البوابات غير المستخدمة فيها.

- تقييد عناوين MAC: Media Access Control وتصفيتها: تصفي هذه العملية عناوين MAC القادمة إلى مبدلة ما وتحدد العدد الأعظمي لها ويمكن تعريف بوابة مبدلة للسماح بعنوان MAC وحيد ومحدد مسبقاً يستطيع الاتصال بهذه البوابة الأمر الذي يسمح لمضيف واحد فقط بالاتصال بالمبدلة عن طريق هذه البوابة.

- استخدام البروتوكول IEEE802.1X: يقدم هذا البروتوكول أعلى درجات حماية بوابات المبدلات ويتم هنا تحقيق الاستيقان حسب البوابة، ويمنع هذا البروتوكول مرور أي طرد عبر أي بوابة حتى يتم التحقق من هوية الزبون المتصل إلى البوابة عن طريق معلومات اعتماده المخزنة على مخدم استيقان. هذا يمنع أي جهاز غير مصادق عليه من استقبال أي طرد قبل إتمام عملية التحقق من الهوية كما أنه يحد النفاذ إلى مخدم الاستيقان لمنع تعرض هذا المخدم إلى أي نوع من الهجمات.


DNS

مقدمة

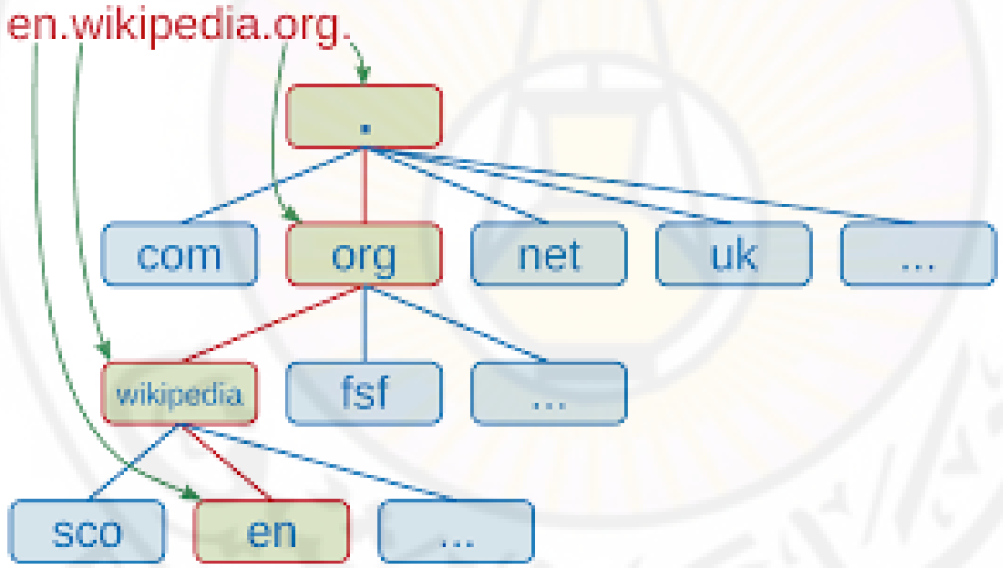
* كانت أنظمة التشغيل لشركة ميكروسوفت قبل نظام تشغيل ويندوز ٢٠٠٠ تستخدم أنظمة التشغيل ويندوز نت والتي تعتمد على خدمة WINS: Windows Internet Name Service، والتي كانت تعتمد على البروتوكول NetBIOS والذي كان يخص أنظمة تشغيل شركة ميكروسوفت ولا تعمل على أي أنظمة تشغيل أخرى.

* ولعلا الفرق ما بين خدمة DNS وخدمة WINS تكمن بمايلي:
نعلم أن لكل جهاز عنوان IP محدداً في الشبكة وأن مهمة DNS هي ترجمة أسماء المواقع مثل WWW.Microsoft.Com إلى عنوان IP للجهاز الذي يشغل خدمة الويب، ومعلوم للجميع أنه في الشبكة المحلية يكون لكل جهاز اسم وليكن مثلاً pc1 ويطلق على هذا النوع من الأسماء NetBIOS Names وأن المسؤول عن ترجمة هذه العناوين هو الخدمة WINS وحدها ولا تعمل إلا على أنظمة تشغيل ويندوز.
* تتوافق الخدمة DNS مع أغلب أنظمة التشغيل لهذا قررت شركة ميكروسوفت ابتداءً من نظام تشغيل ويندوز ٢٠٠٠ وما يليه استخدام الخدمة DNS بدلاً من WINS.

* أي أن خدمة الـ DNS تقوم بترجمة أسماء ومضيفي IP إلى عناوين IP، بينما تقوم خدمة الـ WINS بترجمة الأسماء NetBIOS إلى عناوين IP.

ما هو DNS (Domain name sysem)

- هي قاعدة معطيات موزعة تستعمل في الشبكات التي تستخدم TCP/IP لترجمة أسماء الحواسيب الى عناوين IP
- بنية DNS هي بنية هرمية حيث قاعدة المعطيات مفهرسة بالاسم و بالتالي اسم مجال الطفل يلحق باسم مجال الأب
- الشبكات الخاصة تستعمل DNS لايجاد الحواسيب ضمن شبكاتها المحلية و الانترنت
- Windows NT من Microsoft كانت تستخدم خدمة WINS التي كانت تعتمد على البروتوكول NetBIOS في إيجاد IP لأسماء الحواسيب .
- تظهر أهمية DNS في Active Directory في عثور أجهزة العملاء على متحكمات المجال من أجل النفاذ الى الشبكة , و عثور متحكمات المجال على بعضها لكي تتشارك فيما بينها بمعلومات المستخدمين و المجموعات و غير ذلك .


en.wikipedia.org.
.
com
org
net
uk
...
wikipedia
fsf
...
sco
en
...

مخزن أسماء المجالات

- المجال الجذري Root Domain : إن المجال الجذري هو في أعلى الهرمية و يتم تمثيله كنقطة . و تدير المجال الجذري للإنترنت عدة مؤسسات .
- المجالات ذات المستوى الأعلى (Top-Level Domain) : تكون المجالات ذات المستوى الأعلى شيفرات للأسماء مؤلفة من حرفين أو ثلاثة حروف . و تكون المجالات ذات المستوى الأعلى مصنفة حسب نوع المؤسسة أو المكان الجغرافي .
- المجالات ذات المستوى الثاني (Domain Second Level): يقوم مركز المعلومات القومي NIC بتعين و تسجيل المجالات في المستوى الثاني للأفراد و المؤسسات و الانترنت. و يمكن أن يحتوي المجال ذو المستوى الثاني على مضيفين و مجالات فرعية .
- أسماء المضيفين (Host Names): تشير أسماء المضيفين الى حواسيب معينة على الانترنت أو في شبكة خاصة . و اسم المضيف هو الجزء في أقصى يسار اسم مجال واحد بالكامل أو FQDN و تستعمل الخدمة DNS الاسم الكامل الخاص بالمضيف لترجمة اسم الى عنوان IP .

* من المجالات ذات المستوى الأعلى نذكر على سبيل المثال التالي:
  - gov: مؤسسة حكومية.
  - com: مؤسسة تجارية.
  - edu: مؤسسة تربوية.
  - org: مؤسسة غير تجارية.
  - sy: الجمهورية العربية السورية.

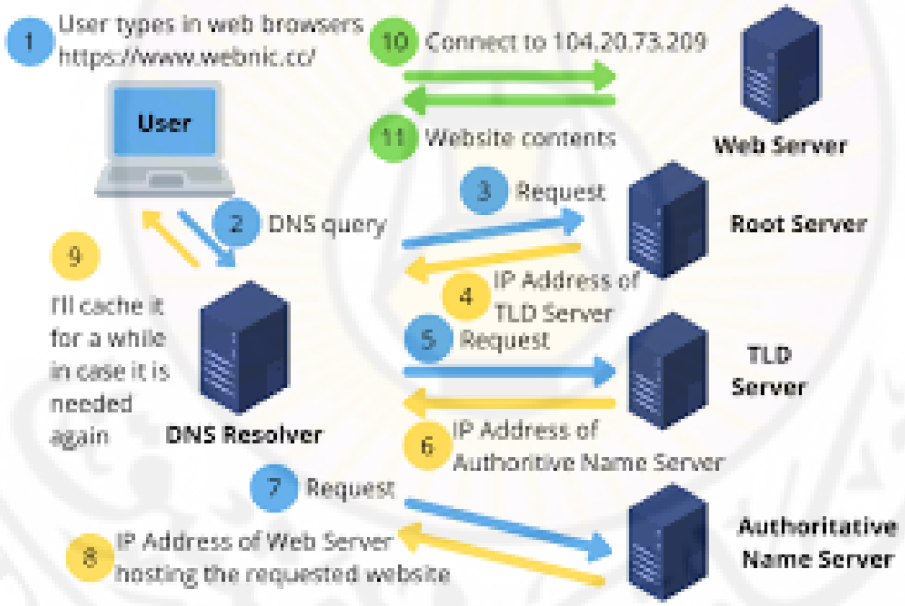
* من قواعد تسمية المجالات نذكر مايلي:
  - الحد من عدد مستويات المجالات بحيث لا يتجاوز خمسة مستويات.
  - استعمال أسماء فريدة للمجالات.
  - استعمال أسماء بسيطة بحيث يسهل تذكرها بالنسبة للمستخدمين.
  - تجنب أسماء المجالات الطويلة.

* المنطقة: هي الوحدة الإدارية الأساسية في نظام خدمة الـ DNS وتمثل جزءاً من قاعدة معطيات الخدمة DNS، وتحتوي المنطقة على معلومات حول جزء من المجال.

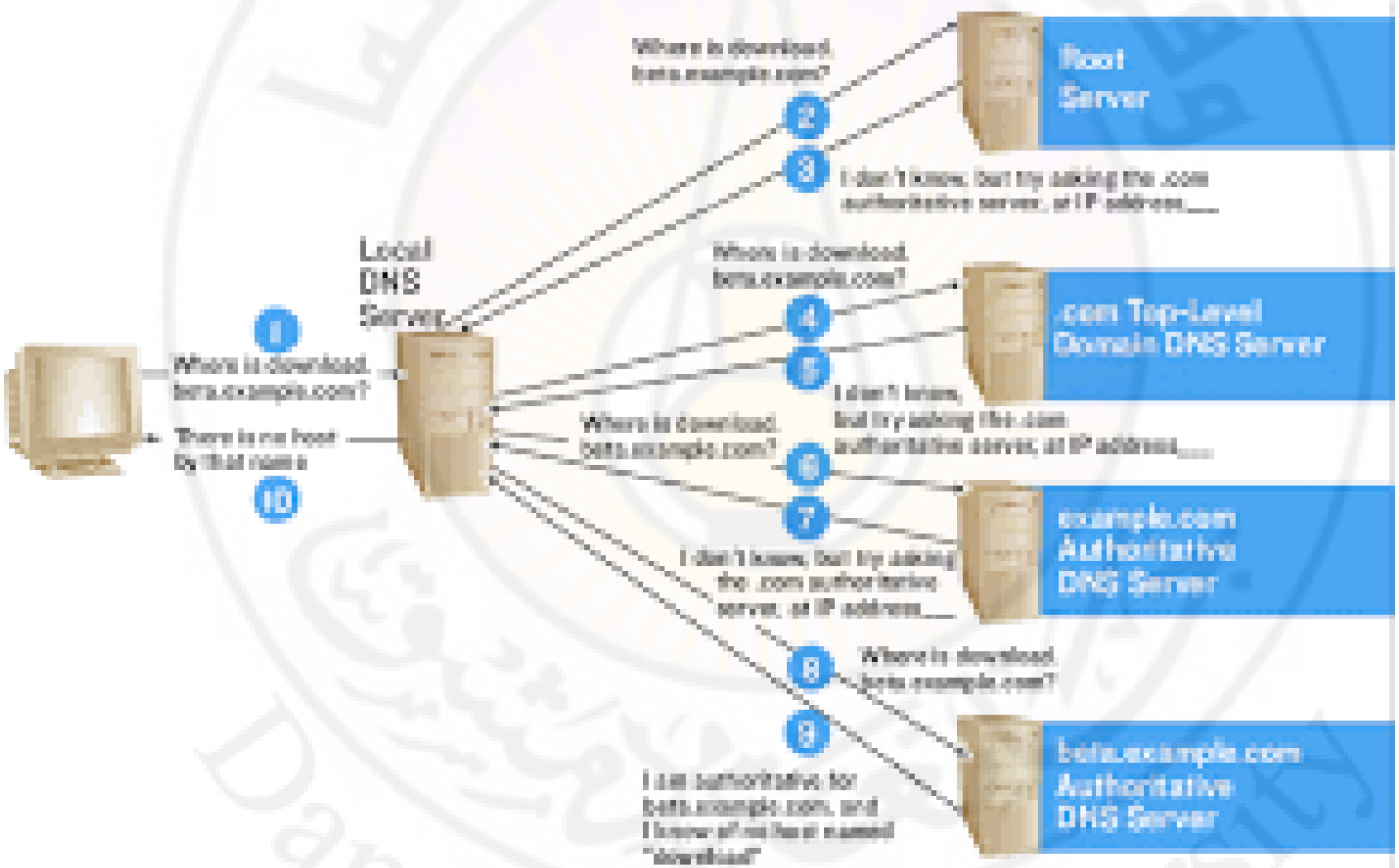
* إن وجود المناطق يؤدي إلى توزيع الإدارة وتسهيل الحصول على المعلومات والتعامل معها وزيادة كفاءة وفعالية نخدمات الخدمات DNS في سرعة تنفيذ الخدمات وتحمل الأخطاء.

أنواع المناطق في الخدمة DNS

- Active Directory Integrated منطقة متكاملة مع خدمة الدليل الفعال : و يمثل هذا النوع النسخة الرئيسية لأي منطقة جديدة . و تستعمل المنطقة خدمات الدليل الفعال لتخزين و استنساخ ملفات المناطق و هذا الخيار يزودنا بتحديثات امنة و تخزين مندمج .
- Standard Primary المناطق القياسية الأولية : تعد هذه المنطقة النسخة الرئيسية لمنطقة جديدة و مخزنة في ملف نصي قياسي . قم بإدارة و صيانة منطقة رئيسية على الكمبيوتر الذي تنشئ المنطقة فيه . و يدار هذا النوع من المناطق و يحفظ على الحاسوب الذي تم إنشاء المنطقة الجديدة Zone عليه . و يسهل هذا الخيار تبادل معطيات DNS مع مخدمات DNS الأخرى التي تستعمل طرق التخزين النصي .
- Standard Secondary المناطق القياسية الثانوية : يمثل هذا النوع نسخة مطابقة عن منطقة موجودة مسبقا , و هو للقراءة فقط غير قابل للتعديل و مخزنة في ملفات نصية قياسية . و يجب أن يكون عند إنشاء منطقة قياسية أولية مضبوط تكوينها لانشاء منطقة قياسية ثانوية , أي أنه يجب تحقيق التلازم بين المناطق القياسية الأولية و الثانوية . و تتجلى الفائدة منها قي إنشاء مصدر احتياطي للمعلومات في حال توقف مخدم DNS الرئيسي .


1 User types in web browsers https://www.webnic.cc/
User
2 DNS query
9 I'll cache it for a while in case it is needed again
DNS Resolver
10 Connect to 104.20.73.209
11 Website contents
Web Server
3 Request
Root Server
4 IP Address of TLD Server
5 Request
TLD Server
6 IP Address of Authoritive Name Server
7 Request
8 IP Address of Web Server hosting the requested website
Authoritative Name Server

HOW DNS WORKS



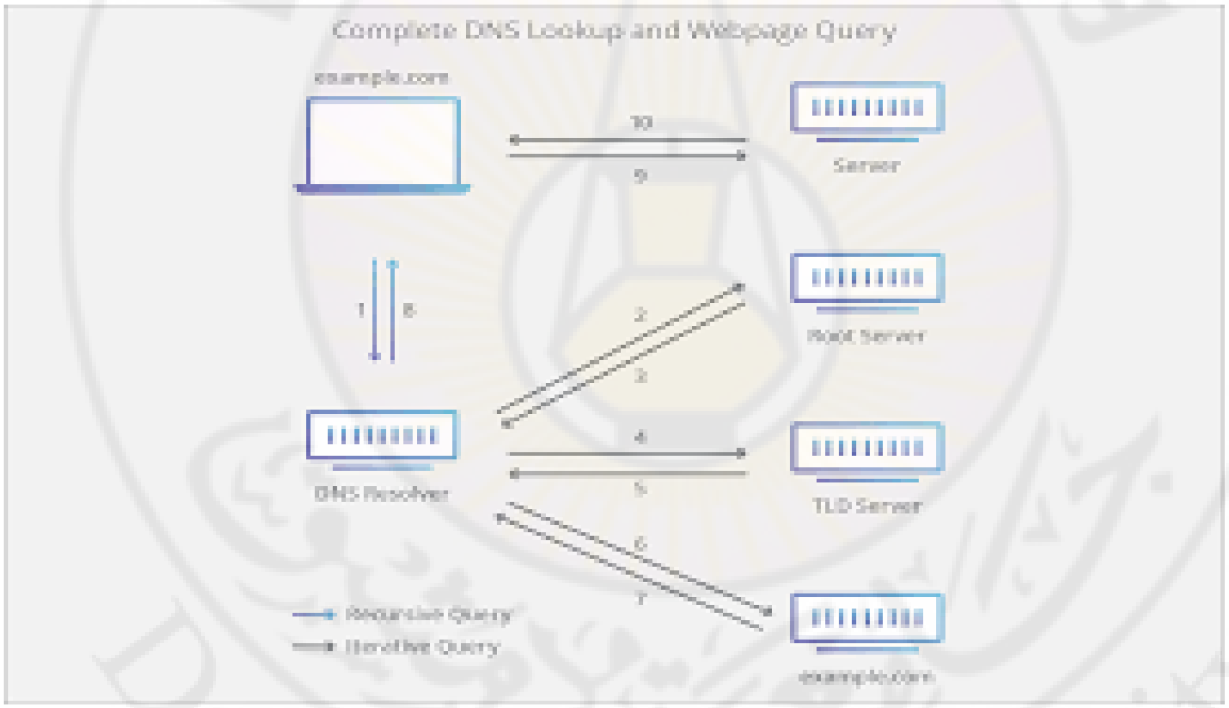
*** إن عملية ترجمة الأسماء هي تحويل هذه الأسماء إلى عناوين IP وعملية الترجمة تشبه التفتيش عن اسم في دليل الهاتف، حيث يقترن كل اسم برقم هاتف.**

- استعلام التفتيش الأمامي Forward Lookup
- يترجم استعلام التفتيش الأمامي Forward Lookup الاسم الى عنوان IP المطابق له.
- بينما استعلام التفتيش العكسي يترجم العنوان IP الى الاسم المطابق له.
- تستعمل الخدمة DNS منهجية المخدم/العميل لترجمة الأسماء
- لترجمة استعلام تفتيش أمامي , يمرر العميل استعلاما الى مخدم أسماء محلي . و يقوم مخدم الاستعلام المحلي إما بترجمة الاستعلام أو يستعلم مخدم أسماء اخر لكي يترجمه.

مثال : عندما يريد عميل ما أن يستعلم مخدم الأسماء عن العنوان IP لاسم الموقع www.Microsoft.com تتم عملية التفتيش الأمامي وفق الخطوات التالية :

- يقوم العميل بتمرير طلب استعلام التفتيش الأمامي المخدم الأسماء المحلي.
- يقوم مخدم الأسماء المحلي بفحص ملف قاعدة معطيات منطقته لتحديد ما إذا كان يحتوي على استعلام العميل أم لا.
- اذا كان مخدم الأسماء المحلي لا يحتوي على استعلام العميل فإنه يرسل الاستعلام الى أحد مخدمات DNS الجذرية طالبا منه ترجمة اسم المضيف.
- يعيد مخدم الأسماء الجذري إرسال مرجع الى مخدمات الأسماء com.
- يرسل مخدم الأسماء المحلي طلبا الى مخدم أسماء com. الذي يرد بمرجع الى مخدم الأسماء Microsoft
- يرسل مخدم الأسماء المحلي طلبا الى مخدم الأسماء Microsoft
- يعيد مخدم الأسماء Microsoft العنوان IP للاسم www.Microsoft.com الى مخدم الأسماء المحلي (و ذلك لأنه ترخيصا لذلك من مخزن أسماء المجالات)
- يرسل مخدم الأسماء المحلي العنوان IP للاسم www.Microsoft.com الى العميل

- يخبئ مخدم الأسماء نتيجة الاستعلام لفترة محدودة من الوقت تسمى عمر . و تحدد المنطقة التي زودت نتائج الاستعلام العمر (يضبط بقيمة افتراضية .60 min).
- بعد أن يخبئ مخدم الأسماء نتيجة الاستعلام يبدأ العمر بالتناقص.
- عندما تنتهي صلاحية العمر يحذف DNS نتيجة الاستعلام من مخبئه.
- تمكن عملية التخبئة مخدم الأسماء من ترجمة الاستعلامات الأخرى الى الجزء نفسه بسرعة.

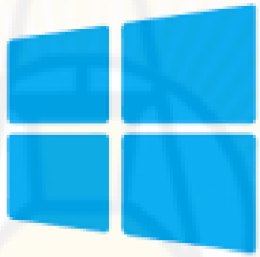

Complete DNS Lookup and Webpage Query
example.com
10
9
Server
1
8
2
7
Root Server
3
4
5
DNS Resolver
TLD Server
6
Recursive Query
Iterative Query
example.com


DNS Lookup
IP address for Google.com?
74.125.142.147
USER
DNS SERVER
Reverse DNS Lookup
Who is 74.125.142.147?
Google.com
USER
DNS SERVER

استعلام التفتيش العكس

- تستخدم استعلامات التفتيش العكسي أدوات لإيجاد المشاكل كأداة سطر الأوامر NSLOOKUP .
- تستعمل استعلامات التفتيش العكسي لاعطاء تقريرا عن أسماء المضيفين.
- تطبق بعض البرامج الأمان و ذلك بالقدرة على الاتصال بأسماء أفضل من الاتصال بعناوين IP
- بما أن قاعدة المعطيات DNS الموزعة مفهرسة بالاسم و ليس بالعنوان IP فإن عملية استعلام التفتيش العكسي هي عملية بحث معقدة عن كل اسم مجال. و لحل هذه المشكلة تم إنشاء مجال ذي مستوى ثاني خاص يدعى in-addr-arpa
- يتبع المجال in-addr-arpa نظام التسمية الهرمية كبقية مخزن أسماء المجال و لكنه يستند على العناوين IP و ليس على أسماء المجالات باستعمال القواعد التالية :

1. تسمى المجالات الفرعية بالأرقام في التمثيل العشري المنقط للعناوين IP
2. يتم ترتيب البايتات في العنوان IP يبتدئ بحقل رقم الشبكة
3. تدبر الشركات المجالات الفرعية للمجال in-addr-arpa بناءا على العناوين IP المعينة لها و قناع الشبكة الفرعية.



Microsoft
Active Directory

الدليل الفعال Active Directory

هي عملية ترتيب المعلومات عن جميع العناصر في الشبكة على شكل بنية هرمية بحيث تسهل عملية الوصول لها و كذلك التحكم في هذه العناصر, و المقصود بهذه العناصر المستخدمين و الموارد المشتركة مثل الأقراص و الطابعات و الملفات و جميع وسائط التخزين و كذلك الأجهزة .

- تحتوي خدمة الدليل الفعال على الدليل و هو عبارة عن قاعدة معطيات تحتوي على معلومات على موارد الشبكة و يقصد بموارد الشبكة (المستخدمين, الأجهزة, المجموعات, الطابعات, الملفات, التطبيقات, معلومات الأمان.....الخ)و هذه الموارد تسمى بكائنات الشبكة Objects.
- تزود خدمة الدليل الفعال بالوسائل اللازمة للوصول الى موارد الشبكة طبعا إذا كان المستخدمون يمتلكون الأذونات الملائمة.
- تستعمل خدمة الدليل الفعال نظام التسمية نفسه لأسماء الميادين DNS المتخدمة في الانترنت.
- تستعمل خدمة الدليل الفعال البروتوكول LDAP (Light Weight Directory Access Protocol)عند تبادل المعلومات بين خدمة الدليل الفعال مع أي برنامج أو دليل .

- تمكننا خدمة الدليل الفعال من التحكم في عناصر المجال المعين الذي يتحكم به نظام التشغيل وتحتوي على العديد من الآليات لتنفيذ عملية التحكم هذه.

- تمكننا خدمة الدليل الفعال من عمل الكثير من الأنشطة التي تساعد على التحكم وإدارة الشبكة كإضافة مستخدمين أو إضافة أجهزة ؟إلى الشبكة ومجموعةً من الأنشطة الأخرى.

- تتكامل خدمة الدليل الفعال مع السياسة الأمنية الموضوعة على النظام الشبكي حيث يتم الوصول إلى أي عنصر من عناصر الدليل الفعال وفقاً لسياسة الأذونات الموجودة في النظام، فمثلاً إذا كان هناك مستخدم وليس لديه إذن بالوصول إلى ملف معين فإن خدمة الدليل الفعال لن تكون متوفرة لذلك المستخدم بالنسبة لهذا الملف.

مميزات خدمة الدليل الفعال Features of Active Directory

- **تنظيم المعلومات Organize Information** : يتم ذلك في أقسام تسمح بتخزين عدد كبير جداً من العناصر (الكائنات) و بالتالي يمكن للدليل الفعال أن يتوسع كلما توسعت الشبكة.
- **توفر خدمة الدليل الفعال مستودع مركزي Provides a central repository** و الذي يقوم بتجميع و توزيع المعلومات عن العناصر في الشبكة بما تحتوي و يسهل الوصول اليها من قبل المستخدم.
- **تزود خدمة الدليل الفعال بالأمن Security** و ذلك من خلال التأكد من الدخول الى الشبكة و التحكم بالوصول الى الكائنات و تشغيلها في الدليل.

فوائد خدمة الدليل الفعال Benefits of Active Directory

1. **تخفيض التكلفة الكلية (TCO(Reduced Total Cost of Ownerships:** تشمل التكلفة الكلية TCO تكلفة كل من الصيانة و التدريب و الدعم الفني و تحديث الأجهزة و البرمجيات. لذلك تساعد خدمة الدليل الفعال على تخفيض هذه التكلفة عن طريق تطبيق السياسات Policies التي تسمح بإعداد نظام الشبكة و تحميل البرامج, و إعداد الأجهزة, و تحميل التطبيقات من مكان مركزي , و هذا يخفض زمن الإعداد و تحميل البرامج على كل جهاز .
2. **مرونة الإدارة Flexible Administration :** تسمح الوحدات التنظيمية Organization Unit في المجال بإمكانية تخصيص صلاحية الإدارة للمستخدمين على الشبكة.
3. **قابلية التوسع Scalability :** تتميز خدمة الدليل الفعال بخاصية قابلية التوسع للعمل مهما كان حجم الشبكة.
4. **تبسيط الإدارة Simplified Administration :** تزود خدمة الدليل الفعال بقائمة الأدوات الإدارية Administrative Tools و التي تبسط الإدارة و تجعل إدارة موارد الشبكة أسهل.

المجال Domain : هو مجموعة من الحواسيب المتصلة ببعضها في الشبكة و تتشارك في منطقة التخزين و تأمين المعلومات و يوفر المجال مركزية الإدارة على مصادر الشبكة و عليه فإن أي مستخدم يستطيع تشغيل المصادر المشتركة على جهاز حاسوب في المجال من خلال ما لديه من أذونات خاصة.

- يخزن المجال معلومات عن كائنات الشبكة التي يحتوي عليها في قاعدة معطيات تسمى الدليل.
- يوجد الدليل على الحواسيب المضبوطة كمتحكمات مجال.
- يتضمن كل مجال على متحكم مجال أو أكثر.
- إن **متحكم المجال Domain Controller :**هو مخدم يخزن نسخة من دليل المجال و يجعل الإدارة مركزية و يشرف على معلومات الأمان عن طريق التحقق من صحة المستخدم و الأذونات التي يملكها .
- يشبه المجال Domain مفهوم مجموعة العمل Workgroup و لكنه يوفر عدد من المزايا المفيدة.

• مميزات المجال Features of a Domain

يتميز المجال بعدد من المميزات هي:

1. **تسجيل دخول فردي Single Logon :** يزود المجال عملية تسجيل دخول واحدة للوصول الى موارد الشبكة طبعا إذا كان يمتلك الأذونات الملائمة , و بذلك فإن جميع حسابات المستخدمين يتم تخزينها في مكان مركزي.
2. **حساب وحيد للمستخدم Single User Account :** يحتاج المستخدم في المجال الى حساب وحيد للوصول الى كل موارد الشبكة على الحواسيب المختلفة طبعا إذا كان يمتلك الأذونات الملائمة.
3. **الإدارة المركزية Centralized Management :** تتميز إدارة المجال بالإدارة المركزية , لأن كل موارد الشبكة مخزنة في مكان مركزي.
4. **قابلية التوسع Scalability :** يمكن توسيع حجم المجال لكي نستطيع بناء شبكات كبيرة لأن الدليل الفعال يتوسع كلما كبرت الشبكة.

Damascus University

فوائد المجال Benefits of a domain

يقدم المجال عدة فوائد أهمها

1. **تنظيم الكائنات Organized Objects :** يمكن تنظيم الكائنات في المجال في وحدات تنظيمية Organizational Units و هذه الكائنات يمكن أن تشترك مع واحد أو أكثر من المجالات مثل المستخدمين و حسابات و برامج و خدمات و ملفات. بالتالي يستطيع مدير الشبكة إدارة هذه الوحدات التنظيمية بدلا من إدارة الكائنات بشكل فردي.
2. **سهولة تحديد مواقع المعلومات Easy Location of Information :** يوفر المجال سهولة تحديد مواقع المعلومات العائدة للكائنات الشبكية و ذلك من خلال قائمة كائنات المجال List of Domain Objects فإذا كان الكائن موجودا داخل هذه القائمة يمكن للمستخدمين تعيين و استخدام هذا الكائن . كما يوجد قوائم التحكم بالوصول (ACL (Access Control Lists و هي حدود أمنية تتحكم بالوصول إلى كائنات المجال.
3. **تنسيق التشغيل Streamlined Access :** هو تطبيق سياسة في المجال حيث يمكن التوضيح للمستخدمين عن كيفية تشغيل و استخدام كائنات المجال من خلال تطبيق سياسة Policy المجال و لا يمكن تطبيق هذه السياسة في المجالات الأخرى.
4. **تفويض الترخيص Delegated Authority :** تمكن المجالات من تخصيص تراخيص الى مدير الشبكة لإدارة الكائنات في المجال أو لإدارة الكائنات في واحدة أو أكثر من الوحدات التنظيمية Organization Unit في المجال ما يحد من عدد المديرين

يمكن أن يحتوي المجال على الحواسيب التالية :

1. **متحكمات المجال Domain Controller :** هي حواسيب تشغل أحد أنظمة التشغيل للمخدمات , و كل متحكم مجال يخزن نسخة من الدليل و إذا حصل أي تحديث على الدليل يُنسخ هذا التحديث الى كل متحكمات المجال الأخرى الياً .
2. **مخدمات أعضاء Membership Servers :** هي حواسب تشغل أحد أنظمة التشغيل للمخدمات , و لكن لا يخزن نسخة عن الدليل و لا يتحقق من صحة دخول المستخدمين ووظيفته تزويد الموارد المشتركة.
3. **الحواسيب العميلة :** هي حواسيب تشغل أنظمة التشغيل .O.S وظيفتها تأمين واجهة للمستخم تتيح له الوصول إلى الكائنات الشبكية في المجال ليس غير ذلك.

هناك بعض التسميات الهامة نذكر منها :

- **الكائنات الشبكية Objects :** يطلق على موارد الشبكة اسم الكائنات و يمكن تنظيم الكائنات في فئات Classes تسمى هذه الفئات بالوحدات التنظيمية (Organization Unit) OU.
- **الكائنات الحاوية Container Objects :** هي كائنات تحتوي على كائنات أخرى مثل المجال.
- **الوحدات التنظيمية OU :** هي فئة من الكائنات تستخدم لتنظيم الكائنات ضمن المجال.

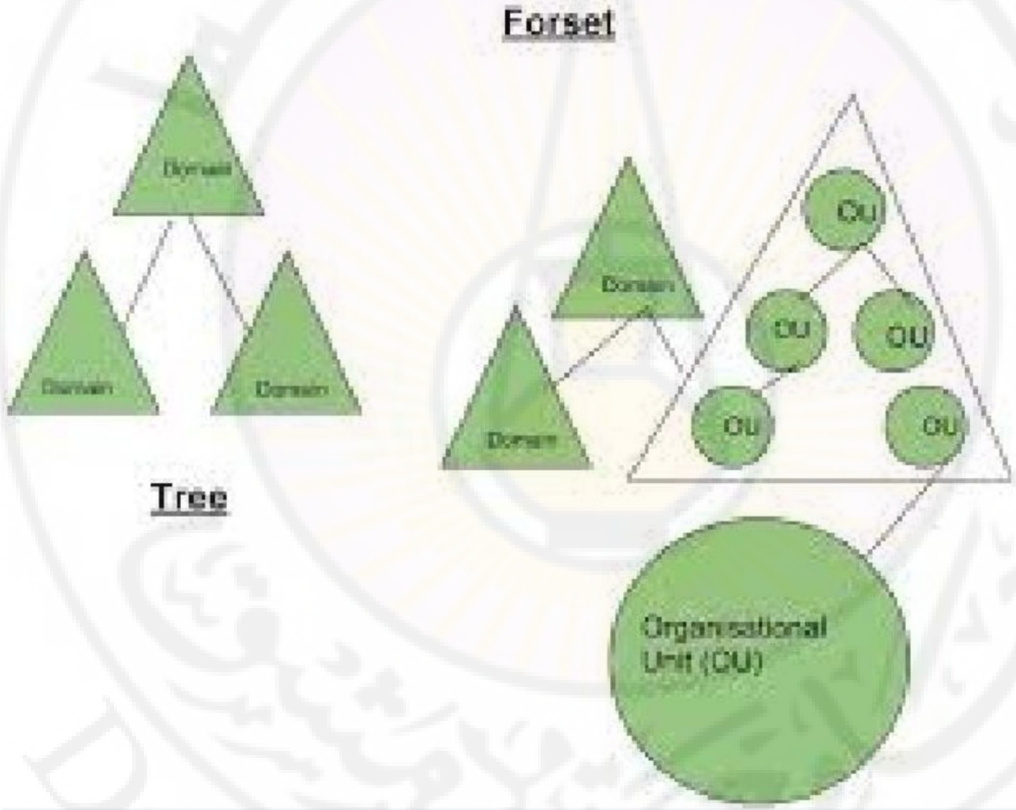
الأشجار Trees

الغابات Forests

Damascus University

ما الفرق في الوحدات التنظيمية OU (الأشجار Trees و الغابات Forests) في خدمة الدليل الفعال ؟

الأشجار Trees	الغابات Forests
تتكون من مجال أو أكثر على شكل بنية تسمية هرمية.	تتكون من شجرة أو أكثر على شكل بنية تسمية هرمية.
تحتوي على دليل واحد و لكن كل مجال يحتوي على جزء من الدليل.	تحتوي على دليل واحد و لكن كل شجرة تحتوي على جزء من الدليل.
المستخدم الذي يسجل الدخول الى مجال يمكنه أن يستخدم الموارد في مجال آخر طبعا إذا كان يملك الأذونات المناسبة.	المستخدم الذي يسجل الدخول الى مجال في شجرة يمكنه أن يستخدم الموارد في الغابة طبعا إذا كان يملك الأذونات المناسبة لكن يجب أن يسجل اسم المجال بالكامل.
كل المجالات في الشجرة تعمل كوحدة واحدة.	كل الأشجار في الغابة تعمل كوحدة واحدة.
	العلاقة بين الأشجار داخل الغابة علاقة ثقة متعدية.


Forset
Domain
Domain
Domain
Tree
Domain
Domain
OU
OU
OU
OU
OU
Organisational
Unit (OU)

صيغ المجالات :

تنقسم صيغ المجالات الى نوعين :

1. **الصيغة المختلطة Mixed Mode :** و هي الصيغة التي تسمح لمتحكم المجال بأن يتعامل مع متحكمات مجال ذات مستوى أقدم.
2. **الصيغة الفطرية Native Mode :** و هي الصيغة التي لا تسمح لمتحكم المجال بأن يتعامل مع متحكمات مجال ذات مستوى أقدم .

يمكن التغيير من الصيغة المختلطة الى الصيغة الفطرية لكن لا يمكن التغيير من الصيغة الفطرية الى الصيغة المختلطة .

DHCP
Dynamic host configuration protocol

What is DHCP?



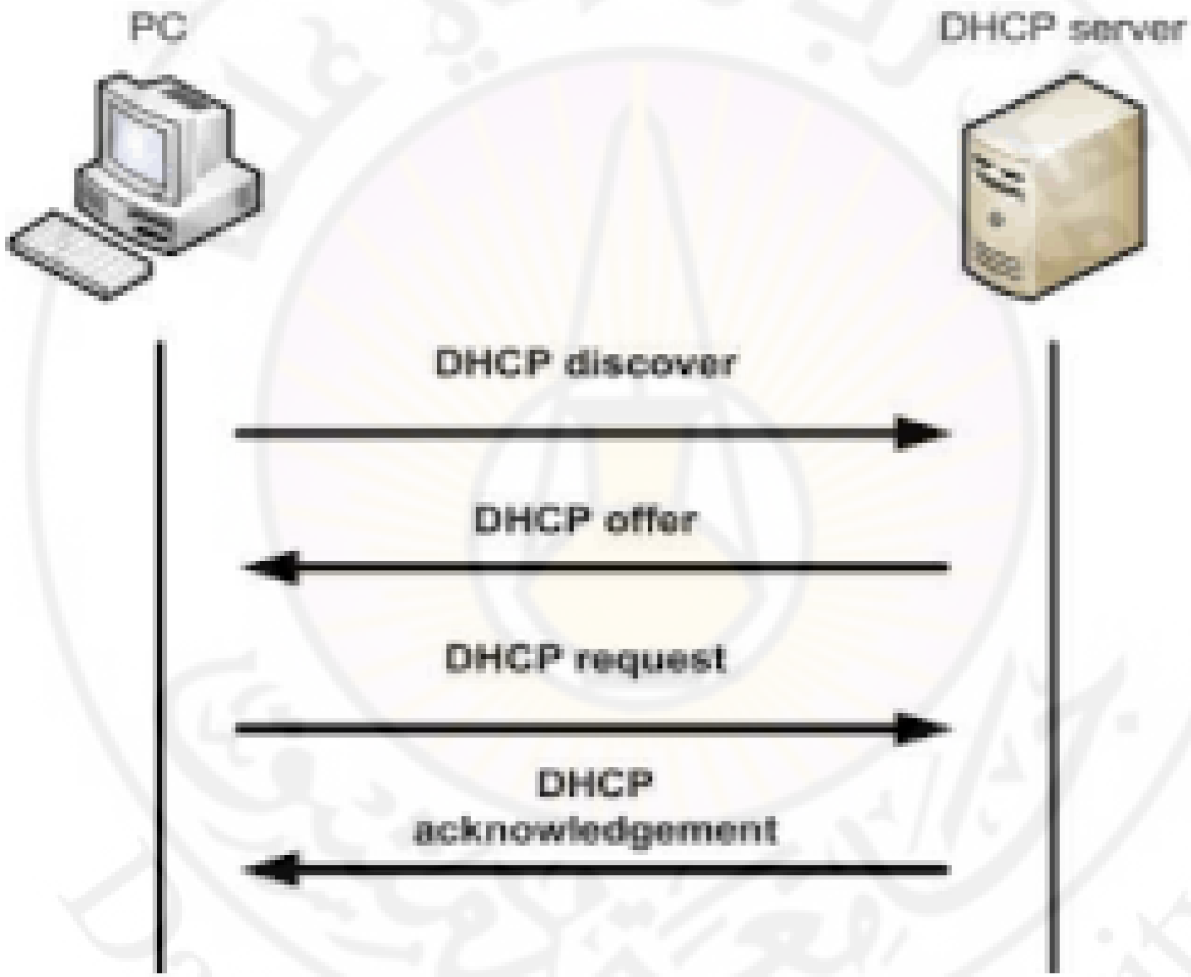
Damascus University

- تسمح الخدمة DHCP بإعدادت المكدس TCP/IP بشكل الي على حواسيب العملاء و بالتالي نضمن عدم وجود حاسبين على الشبكة نفسها لهما عنوان IP نفسه و بسبب العدد الهائل للحواسيب التي تدخل على شبكة الانترنت جاءت الخدمة DHCP لتقوم بإدخال إعدادات TCP/IP اليا .



مبدأ عمل DHCP

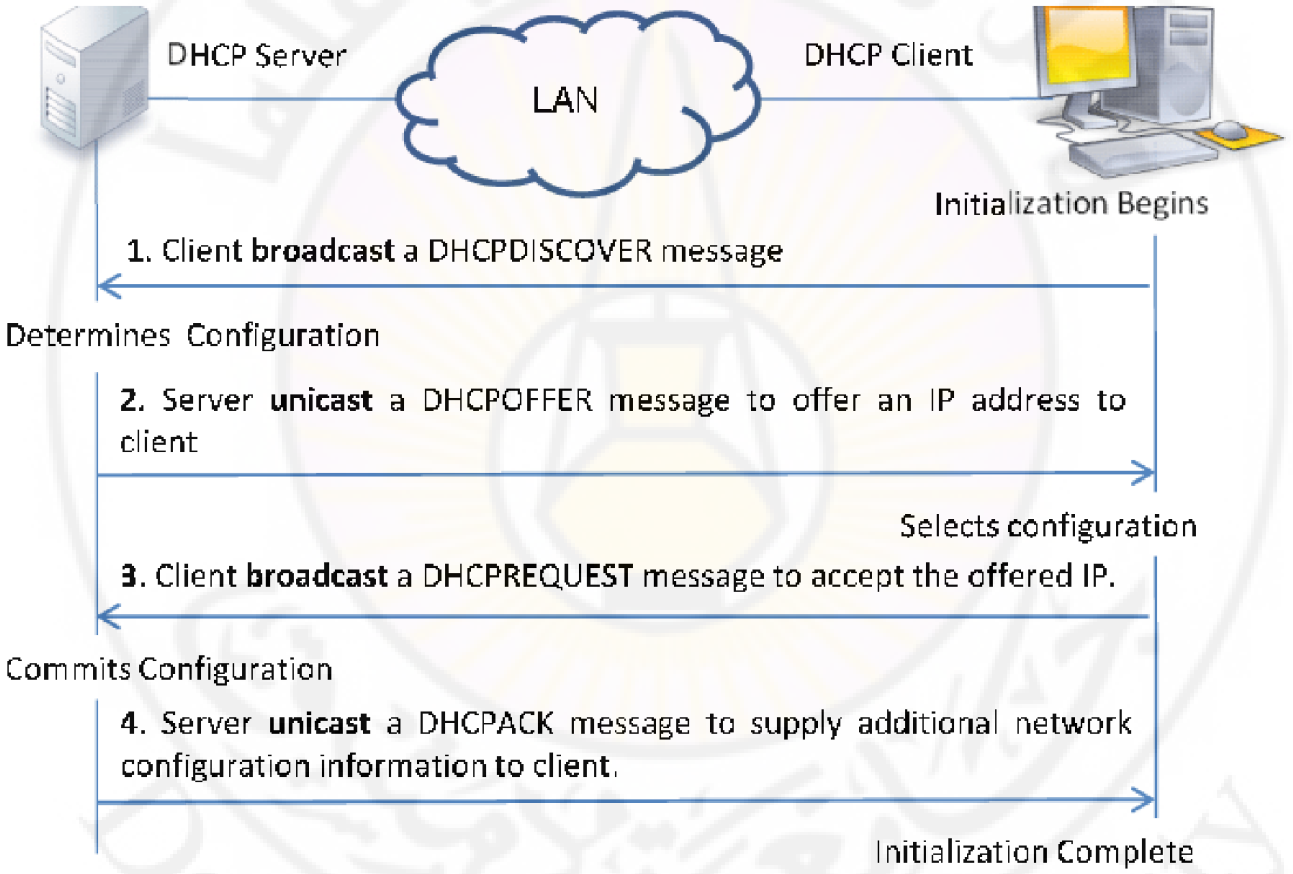
- كلما دخل الحاسوب على الشبكة يطلب العنوان IP من مخدم DHCP وعندما يستقبل مخدم DHCP طلب تأخير عنوان IP يختار عنوان IP من مدى العناوين الموجودة في قاعدة معطيات DHCP ويقوم بعرض هذا العنوان على عميل الخدمة DHCP.
- إذا وافق العميل على العرض المقدم له يقوم مخدم DHCP بحجز هذا العنوان للحاسوب العميل لمدة محددة.
- هذه المدة الزمنية تحدد بشكل افتراضي بثمانية أيام ويمكن ضبطها حسب الحاجة.
- يعطي مخدم DHCP لكل حاسوب عميل المعلومات التالية:
  - عنوان IP.
  - قناع الشبكة الفرعية.
  - قيم إضافية أخرى مثل: عنوان البوابة الافتراضية، عنوان مخدم DNS، عنوان مخدم WINS.



Damascus University

عمليات استئجار DHCP

- طلب استئجار عنوان IP
- عرض تأجير عنوان IP
- اختيار عنوان IP
- تأكيد تأجير عنوان IP


DHCP Server
LAN
DHCP Client
Initialization Begins
1. Client broadcast a DHCPDISCOVER message
Determines Configuration
2. Server unicast a DHCPOFFER message to offer an IP address to client
Selects configuration
3. Client broadcast a DHCPREQUEST message to accept the offered IP.
Commits Configuration
4. Server unicast a DHCPACK message to supply additional network configuration information to client.
Initialization Complete

IP Lease Request

- تبدأ عملية استئجار DHCP عندما يبث العميل رسالة DHCPDiscover التي تطلب معلومات عنونة IP .
- بما أن العميل لا يعرف عنوان IP للمخدم فإنه يستخدم العنوان (0.0.0.0)كعنوان مصدر و العنوان (255.255.255.255) كعنوان الوجهة
- تحتوي الرسالة DHCPDiscover على العنوان الفيزيائي MAC Address لحاسوب العميل , كما تحتوي هذه الرسالة على اسم الحاسوب للعميل لكي تستطيع مخدمات DHCP تحديد العميل الذي أرسل الطلب .

IP Lease Offer

- كل مخدمات DHCP التي تلقت طلب استئجار عنوان IP تبث الرسالة DHCP Offer التي تحتوي على المعلومات التالية :

  العنوان الفيزيائي Mac Address للعميل

  عنوان IP المعروض

  قناع الشبكة الفرعية Subnet Mask

  مدة الايجار

  معرف المخدم (عنوان IP لمخدم DHCP الذي قدم العرض)

- كل مخدمات DHCP التي بثت رسالة عرض تأجير عنوان IP تحجز هذه العناوين لكي لا يتم عرضها على عملاء آخرين .
- يمكن أن يستلم العميل عدة عروض اذا كان هناك عدة مخدمات DHCP و في أغلب الأحيان يختار العميل أول عرض يتلقاه .
- ينتظر عميل DHCP لمدة ثانية واحدة لتلقي عرض تأجير عنوان IP إذا لم يستقبل أي عرض يعيد بث الطلب أربع مرات في الفترات الزمنية 2,4,8,18 sec
- إذا لم يستقبل العميل عرض تأجير عنوان IP بعد الطلبات الأربعة ، عندئذ يستخدم عنوان IP في المدى المحجوز من العنوان (169.254.0.1) الى العنوان (169.254.255.254) و في هذه الحالة يتم استخدام العنونة الالية الخاصة APIPA بحيث يمكنه الاتصال بالحواسيب الأخرى على الشبكة الفرعية التي تقع ضمن هذا المدى المحجوز و يستمر العميل بالبحث عن مخدم DHCP كل خمس دقائق .

IP Lease Selection

- يختار العميل عنوان IP من العرض الأول الذي تلقاه و من ثم يبث الرسالة DHCP Request الى كل مخدمات DHCP التي أرسلت عروض ليدل بأنه قد قبل عرضا .
- تحتوي هذه الرسالة DHCP Request على عنوان IP للمخدم DHCP الذي قبل عرضه.
- كل مخدمات DHCP الأخرى تسحب عروضها لتأجيرها الى عملاء اخرين .

Damascus University

IP Lease Acknowlwdgment

- يقوم مخدم DHCP الذي قدم العرض المقبول ببث الرسالة DHCPACK كدليل على تأكيد تأجير عنوان IP بنجاح .
- تحتوي هذه الرسالة DHCPACK على عنوان IP المحجوز و معلومات أخرى .
- عندما يستقبل عميل DHCP رسالة تأكيد تأجير عنوان IP (DHCPACK) تكون قد تمت إعدادات المكدس TCP/IP بشكل ناجح و يعد العميل هو عميل للخدمة DHCP بحيث يستطيع الاتصال على الشبكة.

- ملاحظة مهمة : تتم كل الاتصالات بين مخدم DHCP و عميل DHCP باستخدام البروتوكول UDP من خلال البوابات ذات الأرقام 67 68

ملاحظة مهمة : إذا كان الحاسوب يمتلك أكثر من بطاقة شبكة فإن الخدمة DHCP تعين عنوان IP لكل بطاقة شبكة.


DHCP Client
IP:
0.0.0.0:68
Eth:
A:B:C:D:E:F
Discover sent to
255.255.255.255:67/FF:FF:FF:FF:FF
Reply sent to
255.255.255.255:68/A:B:C:D:E:F
Request sent to
10.1.1.1:67/F:A:B:C:D:E
Ack sent to
255.255.255.255:68/A:B:C:D:E:F
DHCP Server
IP:
10.1.1.1:67
Eth:
F:A:B:C:D:E

تجديد استئجار الخدمة DHCP بشكل الي

- يحاول عميل DHCP تجديد الاستئجار بعد انقضاء 50% من مدة الايجار و ذلك بإرسال الرسالة DHCP Request مباشرة الى مخدم DHCP الذي حصل منه على الايجار.
- تحتوي رسالة طلب تجديد الاستئجارDHCPRequest على المعلومات التالية :
  - عنوان IP Address Source للعميل .
  - عنوان IP Address Destination لمخدم DHCP.
  - عنوان IP Address الذي تم عرضه.
  - عنوان MAC Address للعميل
- إذا كان مخدم DHCP متوفر فإنه سيجدد الاستئجار و يرسل الرسالة DHCPACK التي تبين على مدة الايجار الجديدة أو أية بارامترات حديثة.
- يقوم العميل بتحديث الاعدادات عندما يستقبل الرسالة DHCPACK .
- إذا لم يستطع عميل DHCP تجديد إيجاره بعد انقضاء 50% من مدة الايجار يستمر باستعمال المعلومات الحالية.
- ثم يقوم ببث الرسالة DHCP Discover للكشف عن مخدم DHCP و ذلك لتغيير عنوانه بعد انقضاء 87.5% من مدة الايجار الحالية
- في هذه الحالة يوافق عميل DHCP على الحصول على إيجار لعنوان IP من أي مخدم اخر و بالتالي ضبط إعدادات TCP/IP و عندما يستجيب أي مخدم DHCP بإرسال الرسالة DHCP Offer الى العميل لتحديث إيجاره , يستطيع العميل تغيير إيجاره (يستطيع العميل تغيير ايجاره استنادا على رسالة العرض المقدمة من المخدم)
- إذا انتهت فترة الايجار يجب على العميل إيقاف استخدام عنوان IP الحالي, و بعد ذلك يبدأ عميل DHCP بإجراء عمليات استئجار DHCP لاستئجار عنوان IP الجديد.

- ملاحظة مهمة : إذا كانت طلبات تجديد استئجار عنوان IP للعميل DHCP Request غير ناجحة أو كان هناك عناوين مكررة على الشبكة أو أن العنوان IP المطلوب غير متوفر عندها يرسل مخدم DHCP الرسالة DHCPNACK رسالة عدم تأكيد تأجير عنوان IP عندها يجب على العميل التخلي عن ايجار عنوان IP و محاولة الحصول على عنوان IP جديد و ذلك بدءا بطلب جديد DHCP Discover.

تجديد استئجار DHCP يدوياً

- C:/> ipconfig/renew

يقوم هذا الأمر بإرسال الرسالة DHCP Request الى المخدم DHCP لتحديث معلومات الإعدادات و كذلك مدة الايجار

- C:/> ipconfig/release

و ذلك لتخلي العميل عن استئجار العنوان IP حيث يقوم هذا الأمر بإرسال الرسالة DHCP Release الى المخدم DHCP لتخلي العميل عن إيجاره .

- يمكن أن يتخلى العميل عن إيجاره عندما ينتقل إلى شبكة أخرى .

- المدى Scope هو مجموعة عناوين IP يمكن تأجيرها لعملاء DHCP
- خيارات المدى Scope Options يمكن ضبط المدى بخيارات تؤهل مخدم DHCP لإعطاء معلومات إضافية مع عنوان IP المؤجر فعلى سبيل المثال يمكن ضبط المدى ليقوم بإعطاء عنوان البوابة الافتراضية Default gateway الى الحواسيب العميلة و هذا المتغير يسمى خيار المدى .
- بارامترات المدى Scope Parameters :هناك عدة بارامترات يجب تحديدها عند إنشاء مدى جديد باستخدام معالج إنشاء مدى جديد New Scope Wizard و هذه البارامترات هي:

1- اسم المدى Name

2- الوصف Description و هو اختياري يصف المدى و الغرض من إنشائه

3- عنوان البداية و النهاية للمدى Start IP address and end IP address و يقوم مخدم DHCP بتوزيع العناوين ضمن هذا المدى و هذا يساعد على التقليل من مشاكل الحصول على عنوان مكرر أو استخدام العنوان نفسه في أكثر من مدى

4- عنوان قناع الشبكة الفرعية Subnet Mask لتخصيصه الى حواسيب عملاء DHCP

5- مدى العناوين المستثناة Exclusion Address Range يمكن استثناء عنوان IP أو أكثر من المدى و العناوين المستثناة لا تعطى الى عملاء DHCP و لتجنب مشكلة الحصول على عنوان مكرر يستثنى أي عنوان IP ساكن يدوي على الشبكة

6- مدة الايجار Lease Duration طول المدة الزمنية لتأجير عنوان IP يمكن تحديدها في الأيام و الساعات و الدقائق و المدة الزمنية الافتراضية لتأجير عنوان IP هو ثمانية أيام و يمكن وضع مدة غير محددة عن طريق ضبط المدى بعد إنشائه. و يزود معالج إنشاء مدى جديد بخيار ضبط المدى غير المحدد.

خيارات عامة للمدى Common Scope Options :

يسمح معالج إنشاء في مخدم DHCP بضبط الخيارات العامة للمدى لتوفير عناوين IP إضافية و هذه العناوين هي :

- عنوان البوابة الافتراضية للمدى Router Default Gateway
- اسم المجال Domain Name توفر الخيارات العامة للمدى اسم المجال حسب تسمية DNS الذي تنتمي إليه حواسيب العملاء
- مخدمات DNS,WINS توفر عناوين كل من مخدمات DNS WINS للعملاء لاستخدامها في اتصالات الشبكة .

تخصيص استخدام خيارات المدى Customizing the use of scope options :

يمكن ضبط خيارات المدى على كل عملاء DHCP على مجموعة من الحواسيب أو على حاسوب واحد , يمكن ضبط خيارات المدى على أربعة مستويات هي :

1. **مستوى المخدم Server Level** :

- يتم تطبيق هذا المستوى على كل عملاء DHCP الذين يريدون استئجار عنوان IP من مخدم DHCP
- يتم تطبيق هذا المستوى إذا كان كل حواسيب العملاء على كل الشبكات الفرعية يريدون معلومات الإعداد نفسها.
- على سبيل المثال يمكن ضبط كل الحواسيب لاستخدام مخدم DNS نفسه

2. **مستوى المدى Scope Level :**

- يسمح هذا الخيار فقط لحواسيب العملاء باستئجار عناوين IP في ذلك المدى.
- كل شبكة فرعية تتطلب إلى مدى مختلف و يمكن تحديد عنوان بوابة افتراضية لكل مدى
- هذه الخيارات التي تم ضبطها في مستوى المدى تأخذ الأولوية على الخيارات التي تم ضبطها في مستوى المخدم.

3. مستوى الفئة Class Level :

- الخيارات التي تم ضبطها في هذا المستوى تطبق فقط على العملاء التي تعرف نفسها لخادم DHCP على إنها تنتمي الى فئة Class معينة
- الخيارات التي تم ضبطها في المستوى Class Level تأخذ الأولوية على الخيارات التي تم ضبطها في المستوى Scope Level

4. مستوى حجز العميل Reserved Client Level :

- هذه الخيارات لهذا المستوى يتم تطبيقها على حواسيب محددة على سبيل المثال جزء من حواسيب عملاء DHCP تستخدم Router للنفاذ على الموارد خارج الشبكة الفرعية.
- هذه الخيارات التي تم ضبطها في مستوى حجز العميل تأخذ الأولوية على الخيارات التي تم ضبطها في أي مستوى آخر .