وزارة التعليم العالي والبحث العلمي
جامعة ديالى
كلية القانون والعلوم السياسية
قسم القانون

الأمن والشبكات

Security and Networking

م. عادل عبد الجبار محمد

Introduction

مقدمـــــة

تُعدّ **الشبكات** الرقمية العمود الفقري لعصر المعلومات، إذ تمكّن الأفراد والمؤسسات من تبادل البيانات والخدمات بشكل سريع وفعال عبر بيئات محلية وعالمية مثل الإنترنت. ومع تزايد حجم البيانات المنقولة وتعقيد البنى التحتية الشبكية، أصبحت مسألة تأمين هذه الشبكات قضية محورية للحفاظ على سرية المعلومات وسلامتها وضمان توافرها.

يُعرف **أمن الشبكات** بأنه مجموعة من السياسات والتقنيات المصممة لحماية موارد الشبكة من التهديدات الداخلية والخارجية، بما في ذلك الوصول غير المصرّح به، التعديل أو الإتلاف المتعمد للبيانات، أو تعطيل الخدمات. ويشمل ذلك استخدام التشفير، الجدران النارية، أنظمة كشف ومنع التسلل، إدارة الهوية والتحكم بالوصول، إضافةً إلى وضع خطط الاستجابة للحوادث الأمنية.

What is a network?

ما هي الشبكــة؟

الشبكة هي ببساطة **مجموعة من جهازين أو أكثر متصلة معاً** بهدف تبادل البيانات أو الموارد أو الخدمات. هذه الأجهزة قد تكون حواسيب، هواتف، طابعات، خوادم، أو حتى أجهزة إنترنت الأشياء.

وظيفتها الأساسية:

- نقل البيانات بين الأجهزة.
- مشاركة الموارد (مثل الإنترنت أو الطابعات أو الملفات).
- تسهيل الاتصال والتعاون بين المستخدمين أو الأنظمة.

انواع الشبكات

الشبكة الشخصية
(PAN)

شبكة التخزين
(SAN)

الشبكة الحضرية
(MAN)

الشبكة الموسعة
(WAN)

الشبكة المحلية
(LAN)

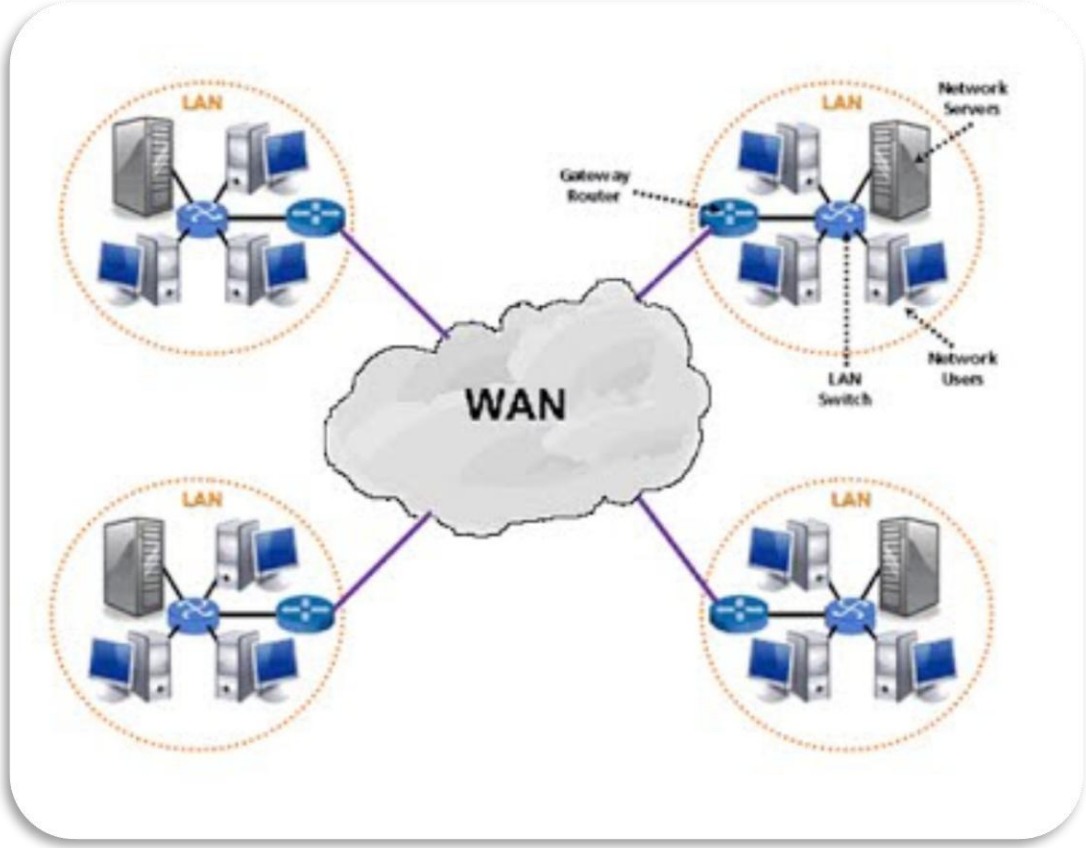
الشبكـــة المحليـــة (LAN – Local Area Network)

1

- تغطي مساحة صغيرة مثل منزل أو مكتب أو مبنى.
- توفر اتصالًا سريعًا بين الأجهزة، عادة باستخدام كابلات إيثرنت أو Wi-Fi .
- مثال: شبكة داخل مكتب تسمح بمشاركة الملفات والطابعات بين الموظفين.

الشبكــة الموسعــة (WAN – Wide Area Network)

2



- تغطي مساحة جغرافية كبيرة، مثل مدينة، دولة، أو حتى العالم.
- تربط شبكات LAN متعددة عبر الإنترنت أو خطوط خاصة.
- مثال: الإنترنت نفسه يُعد أكبر شبكة WAN .

MAN – Metropolitan Area Network الشبكة الحضريــة

3

- أكبر من LAN وأصغر من WAN، تغطي مدينة أو منطقة حضرية.
- غالبًا تُستخدم لتوصيل فروع شركات أو الجامعات داخل المدينة.

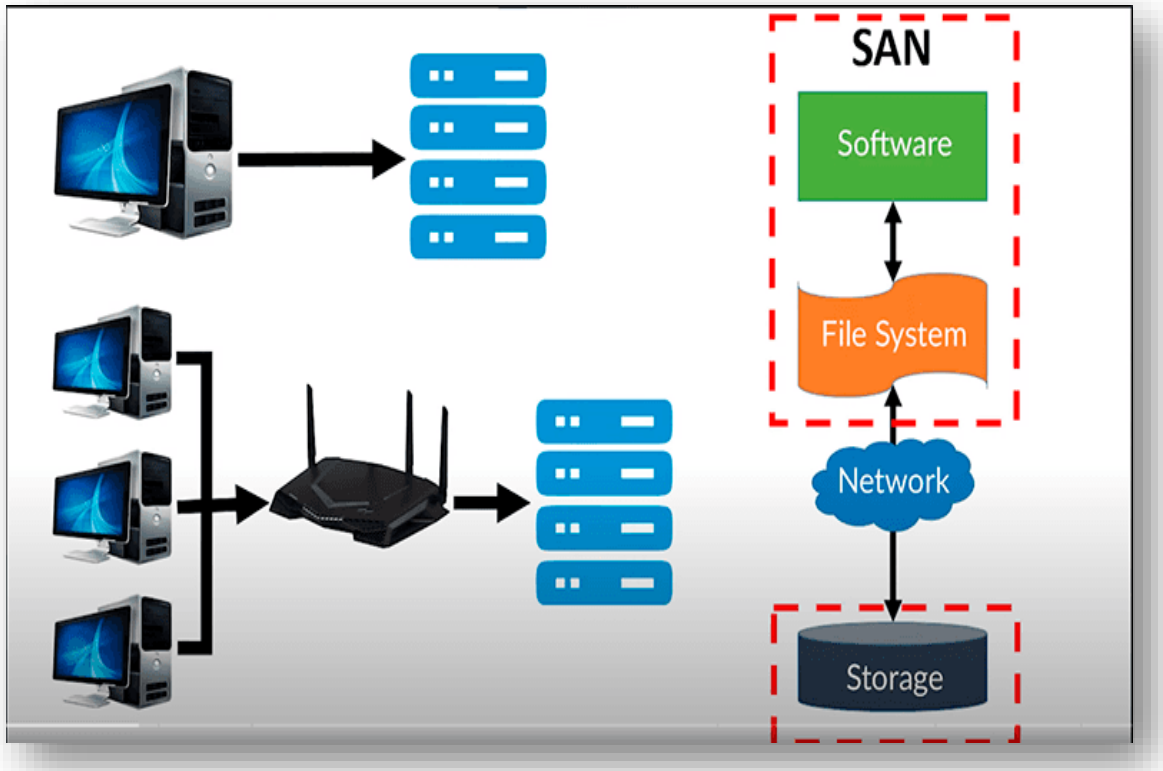
الشبكة الشخصية (PAN – Personal Area Network)

4

- شبكة صغيرة جدًا حول شخص واحد، عادة لمسافة قصيرة.
- تربط أجهزة مثل الهاتف، الحاسوب، السماعات، والطابعات عبر البلوتوث أو USB .

شبكة التخزين (SAN – Storage Area Network)

5



- مصممة لنقل كميات كبيرة من البيانات بسرعة كبيرة غالبًا تستخدم ألياف ضوئية (Fiber Channel) .
- تسمح للخوادم بالوصول إلى وحدات التخزين كما لو كانت جزءًا من محرك الأقراص المحلي.
- يمكن توسيع التخزين وإدارته بسهولة دون التأثير على الشبكة العامة للمؤسسة.

مكونات الشبكة الأساسية

Basic network components

الأجهزة الطرفية (End Devices)

1

- هي الأجهزة التي يستخدمها المستخدمون للوصول إلى الشبكة.
- أمثلة: الحواسيب، الهواتف، الطابعات، الخوادم.
- وظيفتها: إرسال واستقبال البيانات عبر الشبكة.

أجهزة التوجيه (Routers)

2

- تربط شبكات مختلفة مع بعضها (مثل LAN بالإنترنت).
- وظيفتها: توجيه البيانات إلى الشبكة الصحيحة باستخدام عناوين IP .

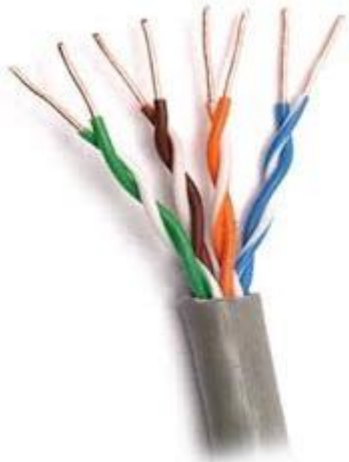
أجهزة التحويل (Switches)

3

- تربط أجهزة داخل نفس الشبكة المحلية (LAN) .
- وظيفتها: تمرير البيانات إلى الجهاز المستهدف فقط، مما يقلل الازدحام ويحسن الأداء.

الوسائط الناقلة (Transmission Media)

4



- هي الطريقة التي تنتقل بها البيانات بين الأجهزة.
  - ✓ أنواعها:
    - ✓ كابلات نحاسية (Ethernet) .
    - ✓ ألياف ضوئية (Fiber Optics) .
    - ✓ اتصالات لاسلكية (Wi-Fi، بلوتوث).

البروتوكولات (Protocols)

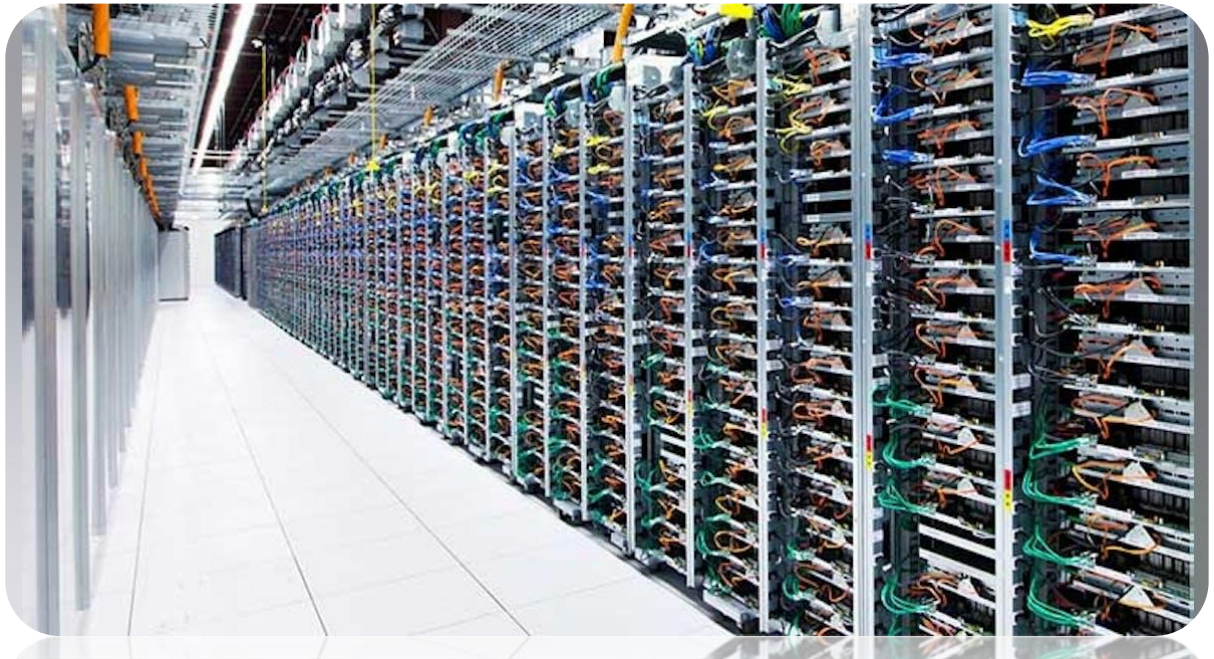
5

- مجموعة قواعد تحدد كيفية تبادل البيانات بين الأجهزة.
- أمثلة: TCP/IP، HTTP، DNS، FTP.
- وظيفتها: ضمان وصول البيانات بشكل صحيح ومنظم بين الأجهزة المختلفة.

الخـوادم (Servers)

6

- أجهزة قوية توفر خدمات معينة للمستخدمين أو الأجهزة الأخرى في الشبكة.
- وظائفها: استضافة المواقع، البريد الإلكتروني، قواعد البيانات، تخزين الملفات.



أساسيات أمان الشبكة

Network Security Basics

أمان الشبكة هو جزء أساسي من إدارة أي نظام شبكي، ويهدف إلى حماية البيانات والمعلومات من التهديدات الداخلية والخارجية وضمان عمل الشبكة بكفاءة. يقوم أمن الشبكة على مجموعة من المبادئ الأساسية، أهمها السرية لمنع الوصول غير المصرح به إلى المعلومات، سلامة البيانات لضمان عدم تعديلها أو التلاعب بها، والتوافر لضمان استمرار الخدمات والوصول إلى الموارد عند الحاجة. بالإضافة إلى ذلك، يعتمد الأمن على المصادقة والتحكم بالوصول، واستخدام الجدران النارية وأنظمة كشف التسلل، وصيانة التحديثات لحماية الشبكة من الهجمات والثغرات. فهم هذه الأساسيات يُعد الخطوة الأولى لبناء شبكة آمنة وموثوقة.

أساسيات أمان الشبكة Network Security Basics

١. **السرية (Confidentiality)**

- حماية المعلومات من الوصول غير المصرّح به.
- أمثلة: التشفير ((Encryption مثل (TLS - VPN

٢. **سلامة البيانات (Integrity)**

- ضمان عدم تعديل البيانات أثناء النقل أو التخزين.
- أمثلة: استخدام الـ Hash، HMAC، وأنظمة كشف التلاعب.

Network Security Basicsأساسيات أمان الشبكة

٣. **التوافر (Availability)**

- ضمان أن الشبكة والخدمات متاحة للمستخدمين عند الحاجة.
- أمثلة: النسخ الاحتياطي، خوادم احتياطية، حماية ضد هجمات الحرمان من الخدمة (DoS/DDoS)

٤. **المصادقة (Authentication)**

- التأكد من هوية المستخدم أو الجهاز قبل السماح له بالوصول.
- أمثلة: كلمات المرور، بطاقات ذكية، التحقق الثنائي.

Network Security Basicsأساسيات أمان الشبكة

٥. **التحكم بالوصول (Access Control)**

- تحديد من يمكنه الوصول إلى الموارد وما يمكنه فعله.
- أمثلة: قوائم التحكم (ACL)، صلاحيات المستخدمين.

٦. **الجدران النارية وأنظمة كشف التسلل (Firewall & IDS/IPS)**

- مراقبة حركة المرور وحماية الشبكة من الهجمات والبرمجيات الضارة.

٧. **التحديثات والصيانة (Updates & Patching)**

- المحافظة على الأجهزة والبرمجيات محدثة لسد الثغرات الأمنية.

فهم تهديدات الشبكة

Understanding network threats

مع تزايد اعتماد الأفراد والمؤسسات على الشبكات الرقمية لنقل البيانات وتوفير الخدمات، أصبحت **تهديدات الشبكة** واحدة من أهم التحديات التي تواجه أمن المعلومات. هذه التهديدات تشمل كل ما يمكن أن يضر بالسرية، سلامة البيانات، أو توافر الشبكة، سواء من قبل هجمات خارجية أو أخطاء داخلية. فهم هذه التهديدات هو الخطوة الأساسية لتصميم استراتيجيات حماية فعّالة والحفاظ على أمن الشبكة واستمرارية الخدمات.

الهجمات الضارة (Malicious Attacks)

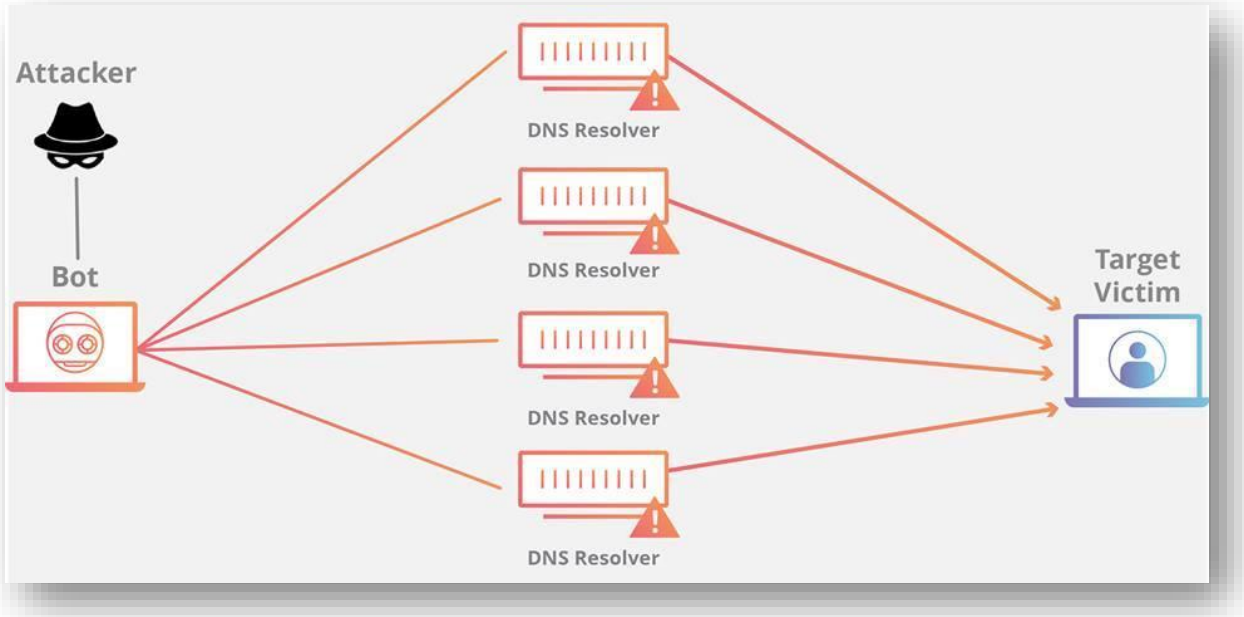
1

- تشمل البرمجيات الخبيثة مثل الفيروسات، الديدان (Worms)، وبرامج التجسس (Spyware).
- تهدف إلى سرقة البيانات، تعطيل الأنظمة، أو السيطرة على الأجهزة.

هجمات الحرمان من الخدمة (DoS / DDoS)

2

- محاولة جعل الشبكة أو الخدمات غير متاحة للمستخدمين الشرعيين.
- غالبًا عن طريق إرسال كمية ضخمة من الطلبات لتجاوز قدرة الخادم.



التصيد الاحتيالي (Phishing) والهندسة الاجتماعية

3

- محاولات لخداع المستخدمين لكشف معلومات حساسة مثل كلمات المرور أو أرقام الحسابات.

٤. **الهجمات الداخلية (Insider Threats)**

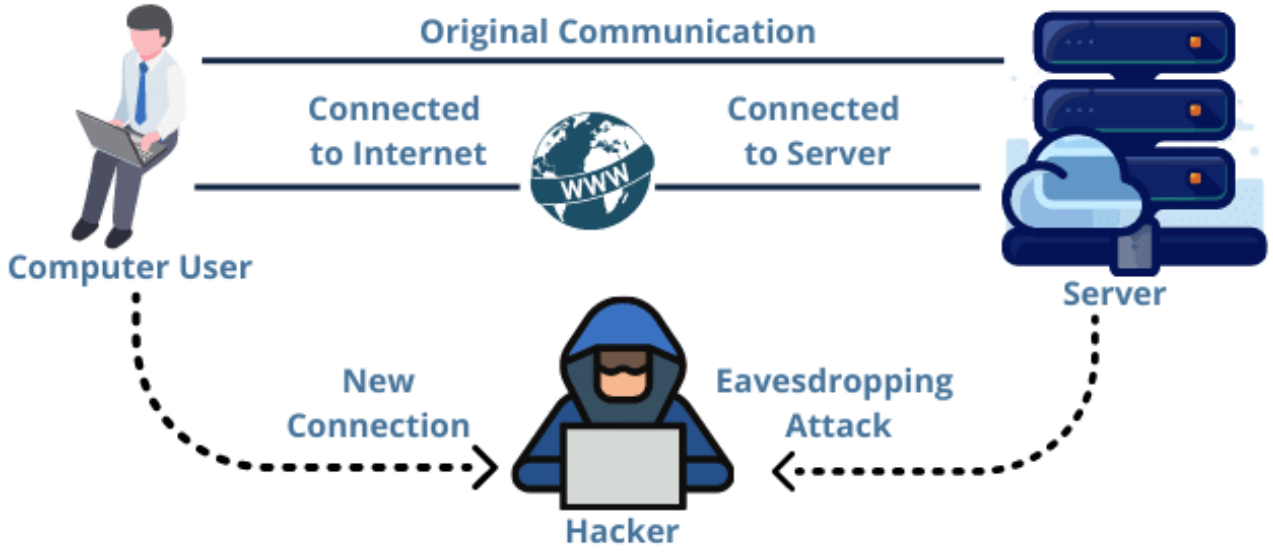
- تهديدات تأتي من داخل المؤسسة، مثل موظف يسيء استخدام صلاحياته للوصول إلى البيانات.

٥. **استغلال الثغرات والاختراق (Exploitation / Hacking)**

- مهاجمون يستفيدون من ضعف البرامج أو تكوين الشبكة للوصول غير المصرح به.

٦. التنصت على الشبكة (Eavesdropping / Sniffing)

- اعتراض البيانات أثناء نقلها عبر الشبكة، خاصة إذا لم يتم تشفيرها.



٧. التهديدات المتقدمة المستمرة (APT – Advanced Persistent Threats)

- هجمات طويلة الأمد ومخططة بدقة تستهدف سرقة معلومات حساسة أو السيطرة على الأنظمة بشكل خفي.

استكشاف أخطاء الشبكة

(Network Troubleshooting)

- هي عملية منهجية لتحديد أسباب المشكلات الشبكية (قطاع الاتصال، بطء، فقدان حزم، مشاكل DNS وإصلاحها).
- الهدف: استعادة الاتصال أو الأداء الطبيعي بأسرع وقت ممكن وبأقل تأثير على المستخدمين، مع توثيق الأسباب والحلول لمنع تكرارها.

استكشاف أخطاء الشبكة (Network Troubleshooting)

١. **تحديد نطاق المشكلة (حدد ماذا ومن متأثر)**

- اسأل: هل المشكلة تؤثر على جهاز واحد أم مجموعة أم الشبكة كلها؟
- هل المشكلة متواصلة أم متقطعة؟ متى بدأت؟ هل حدثت تغييرات حديثة (تحديث سويتش/راوتر، تغيير كابل، سياسات جدار ناري)؟
- سجِّل الوقت، المستخدمين المتأثرين، والخدمات المتأثرة (مثلاً: الإنترنت، خدمة داخلية DB، بريد).

٢. **جمع المعلومات الأساسية**

- أسماء الأجهزة/عناوين IP المتأثرة، أسماء المضيفين (hostnames).
- نتائج الفحص الأولي (رسائل الخطأ الظاهرة للمستخدم).
- أي سجلات (logs) من الأجهزة المتأثرة أو من عناصر البنية التحتية (firewall, router, server).

استكشاف أخطاء الشبكة (Network Troubleshooting)

٣. **التحقق من الطبقة الفيزيائية**

- افحص وصلات الكابل، وصلات الألياف، وصلات الطاقة على الأجهزة.
- تحقق من أضواء المنفذ على الراوتر.
- جرّب تغيير كابل أو المنفذ على الراوتر.
- في الشبكات اللاسلكية: تحقق من قوة الإشارة والتداخل والقناة.

٤. **التحقق من التوصيف المحلي**

- تأكد أن الجهاز حصل على عنوان IP صحيح .
- افحص إعدادات Speed لمنع التصادم .

استكشاف أخطاء الشبكة (Network Troubleshooting)

٥. **التحقق من الأجهزة والخدمات**

- هل الخدمة تعمل محليًا على الخادم؟
- أعد تشغيل الخدمة إذا لزم الأمر وراقب السجلات.

٦. **التوثيق والمتابعة**

- سجِّل كل خطواتك، النتائج، والتغييرات التي أجريتها.
- إذا تم الحلّ، وثّق السبب والإجراءات المتخذة لتجنُّبه مستقبلاً.