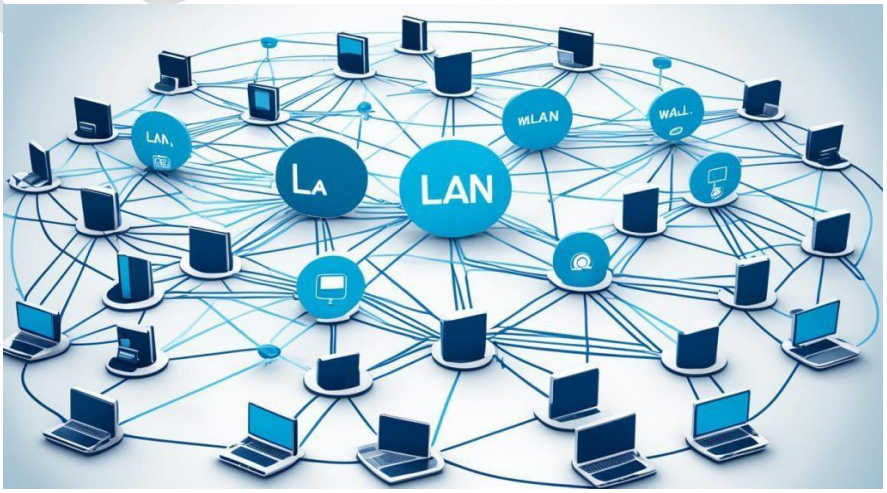
الأمنية والشبكات
Security and Networking

تُعَدّ الشبكات الحاسوبية من الركائز الأساسية في عالم التكنولوجيا الحديثة التي تدعم أنظمة المعلومات في العصر الرقمي، إذ أتاحت ربط الأجهزة والتواصل وتبادل البيانات والمعلومات والموارد بسرعة وكفاءة بين الأجهزة المختلفة، سواء كانت في إطار مؤسسة أو عبر الإنترنت ومن خلال الشبكات، أصبح بالإمكان مشاركة الملفات والطابعات والاتصال عبر الإنترنت وإدارة الأنظمة عن بُعد، مما أسهم في تسهيل العمل المؤسسي والتعليم والبحث العلمي والتجارة الإلكترونية.

ومع تزايد الاعتماد على التكنولوجيا في الحياة اليومية، يبرز أهمية الأمان الشبكي كعنصر حيوي في حماية المعلومات والموارد حيث يمثل الأمن في الشبكات مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الشبكات من التهديدات المحتملة مثل الهجمات السيبرانية، والبرامج الضارة، والاختراقات. فمع تزايد وتعقيد التهديدات، أصبح من الضروري فهم كيفية تأمين الشبكات لضمان سلامة البيانات وسرية المعلومات. يتطلب بناء شبكة آمنة استراتيجيات متعددة تشمل التشفير، التحكم في الوصول، واستخدام جدران الحماية، بالإضافة إلى التوعية والتدريب المستمر للمستخدمين. لذا، فإن فهم أساسيات شبكات الحاسوب وأمنها يعد خطوة أساسية نحو إنشاء بيئات عمل آمنة وموثوقة تساهم في تعزيز الإنتاجية وتحقيق الأهداف المؤسسية.

1- ماهي الشبكة؟ What is a network?

الشبكة هي مجموعة من الأجهزة المتصلة التي يمكنها التواصل مع بعضها البعض لمشاركة الموارد والمعلومات. تشمل هذه الأجهزة أجهزة الكمبيوتر، والخوادم، والمحولات، والموجهات، وغيرها من الأجهزة. يمكن أن تكون الشبكات سلكية أو لاسلكية، وتتفاوت في الحجم من الشبكات المحلية الصغيرة (LAN) إلى الشبكات العالمية مثل الإنترنت. تتكون شبكة الحاسوب من عدة مكونات رئيسية، تشمل مكونات مادية Hardware ومكونات برمجية Software.



2- أنواع الشبكات Types of networks

يمكن تصنيف الشبكات إلى عدة أنواع بناءً على نطاقها وحجمها وبنيتها:

1- الشبكة المحلية (LAN):

تُعَدّ الشبكة المحلية (Local Area Network – LAN) أحد أهم أنواع الشبكات وأكثرها استخدامًا في بيئات العمل التعليمية والمؤسسية، إذ تُعتبر البنية والاتصال الداخلي وتبادل البيانات بين الحواسيب والأجهزة داخل نطاق جغرافي محدود مثل مبنى، مختبر، أو حرم جامعي.

تُعَدّ الشبكة المحلية (LAN) أحد أهم أنواع الشبكات وأكثرها استخدامًا في بيئات العمل التعليمية والمؤسسية وهي مجموعة من أجهزة الكمبيوتر والأجهزة الأخرى المتصلة ببعضها البعض ضمن منطقة جغرافية محدودة، مثل منزل، مكتب، أو مبنى. أدت الشبكات المحلية إلى ثورة في طريقة إدارة الأنظمة وتبادل المعلومات، حيث سمحت بالوصول السريع إلى الموارد المشتركة (كالطابعات والخوادم وقواعد البيانات)، وسهّلت عمليات الإدارة المركزية، والنسخ الاحتياطي، وتأمين الاتصال الداخلي. تتميز الشبكات المحلية بالسرعات العالية في نقل البيانات وانخفاض تكلفة الاتصال، حيث تكون الأجهزة مترابطة من خلال كابلات أو عبر تقنية Wi-Fi. تتميز الشبكة المحلية بعدة خصائص، منها:

1- **نطاق محدود**: تعمل داخل مبنى واحد أو مجمّع مؤسسي.
2- **سرعة عالية**: عادةً ما توفر الشبكات المحلية سرعات نقل بيانات أعلى من الشبكات الواسعة (WAN) لأنها لا تتطلب مسافات طويلة لنقل البيانات قد تصل إلى 10 Gbps أو أكثر.
3- **ملكية خاصة**: تُدار وتُمتلك من قِبل الجهة نفسها.
4- **تكلفة منخفضة**: تكلفة إنشاء شبكة محلية أقل مقارنة بالشبكات الأوسع، وذلك بفضل المعدات المستخدمة وتوزيع الشبكة.
5- **الأمان**: تحكم وإدارة مركزية حيث يمكن إدارة الأمان بسهولة أكبر في الشبكات المحلية، حيث يمكن التحكم في الوصول إلى البيانات والموارد.
6- **المشاركة**: تتيح الشبكات المحلية مشاركة الموارد مثل الطابعات، الملفات، والاتصال بالإنترنت بين الأجهزة المتصلة.

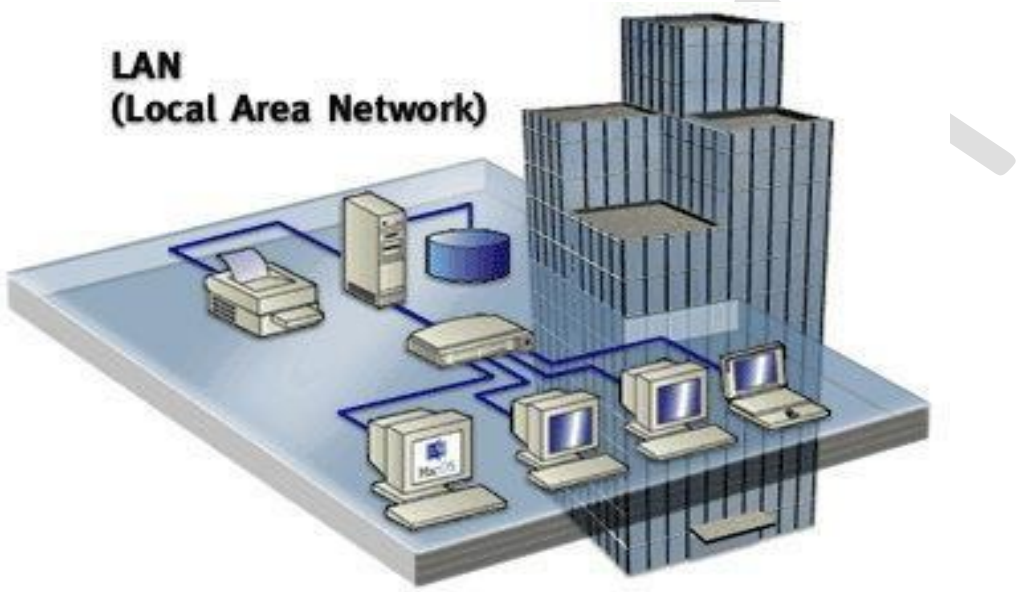
تستخدم الشبكات المحلية LAN في العديد من التطبيقات، مثل:

1. **الجامعات**: ربط المختبرات وقواعد البيانات.
2. **الشركات**: مشاركة الملفات والخدمات.
3. **المستشفيات**: إدارة سجلات المرضى.
4. **المدارس**: تشغيل أنظمة الامتحانات الإلكترونية.
5. **المنازل الذكية**: ربط الأجهزة والتحكم بها.

ESRA QUBA

للشبكة المحلية LAN عيوب عديدة منها:

1. ضعف الأمان وسهولة انتشار الفيروسات.
2. توقف الشبكة إذا تعطّل الخادم الرئيسي.
3. بطء الأداء عند زيادة المستخدمين.
4. تكاليف صيانة وتحديث مرتفعة.
5. محدودية النطاق الجغرافي.



2- الشبكة الواسعة (WAN):

تُعد الشبكة الواسعة (Wide Area Network – WAN) من أهم أنواع الشبكات التي أحدثت نقلة نوعية في عالم الاتصالات الحديثة، إذ سمحت بربط المدن، الدول، بل والقارات ببعضها البعض، لتشكّل العمود الفقري لشبكة الإنترنت العالمية. WAN هي شبكة اتصالات تعمل على ربط عدة شبكات محلية عبر مسافات بعيدة من خلال أجهزة موجهات (Routers) وبروتوكولات خاصة، لتتيح للمستخدمين في مواقع مختلفة الاتصال وكأنهم ضمن شبكة واحدة.

الشبكة الواسعة (WAN) هي شبكة تمتد عبر نطاق جغرافي كبير (مدن، دول، أو حتى قارات)، وتُستخدم لربط شبكات محلية (LANs) أو شبكات مدنية (MANs) ببعضها البعض باستخدام وسائط اتصال عامة أو خاصة مثل خطوط الهاتف، الألياف الضوئية، الأقمار الصناعية، أو شبكات الاتصالات اللاسلكية.

يُستخدم هذا النوع من الشبكات بشكلٍ رئيسي في المؤسسات الكبرى، الهيئات الحكومية، الجامعات متعددة الفروع، وشركات الاتصالات، حيث يُمكّن من مشاركة الموارد والخدمات والمعلومات على نطاق جغرافي واسع جدًا. تتميز الشبكة الواسعة بعدة خصائص، منها:

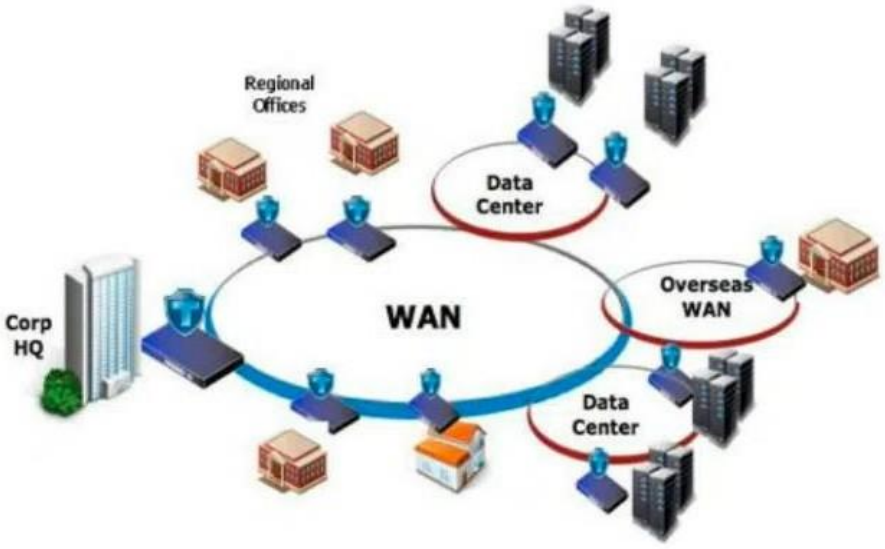
1. نطاق جغرافي واسع جدًا.
2. سرعة اتصال متفاوتة حسب نوع الوسائط.
3. ملكية مشتركة بين جهات متعددة.
4. تكلفة تشغيلية مرتفعة وتتطلب أجهزة توجيه متقدمة.
5. تعتمد على وسائط اتصال عامة وخاصة.
6. تحتاج الى برامج امان متقدمة وجدران حماية وتشفير للبيانات.

تستخدم الشبكات الواسعة WAN في العديد من التطبيقات، مثل:

1. ربط فروع الجامعات في محافظات مختلفة.
2. شبكات البنوك والمصارف المركزية.
3. الحكومة الإلكترونية بين الوزارات.
4. الشركات العالمية مثل Google وMicrosoft والشركات متعددة الجنسيات.
5. شبكات شركات الاتصالات ومقدمي الإنترنت.

للشبكة الواسعة WAN عيوب عديدة منها:

1. تكلفة مرتفعة في الإنشاء والصيانة.
2. بطء نسبي مقارنة بالشبكات المحلية.
3. تعقيد إداري وأمني.
4. الاعتماد على مزودي الخدمة.



FSRA QUBA

3- الشبكة الحضرية (MAN):

تُعد الشبكة الحضرية (Metropolitan Area Network – MAN) من أنواع الشبكات المهمة التي تقع في المنتصف بين الشبكة المحلية (LAN) والشبكة الواسعة (WAN)، إذ تربط عدداً من الشبكات المحلية المنتشرة داخل مدينة واحدة أو منطقة حضرية باستخدام تقنيات عالية السرعة.

فالشبكة الحضرية (MAN) هي شبكة تربط عدة شبكات محلية (LANs) ضمن نطاق جغرافي متوسط، مثل مدينة أو مجمع صناعي أو منطقة جامعية. تُعد حلقة وصل بين الشبكات المحلية الصغيرة والشبكات الواسعة الكبيرة، حيث تُستخدم لتبادل المعلومات بسرعة عالية بين المواقع المختلفة داخل المدينة. تُستخدم MAN عادة لربط الجامعات أو الفروع الحكومية أو المؤسسات التي تقع ضمن حدود مدينة واحدة لتبادل البيانات والخدمات. ومن خصائص الشبكة الحضرية:

1. تغطي نطاقًا جغرافيًا يتراوح بين 10 إلى 50 كيلومترًا.
2. تستخدم وسائط اتصال عالية السرعة مثل الألياف الضوئية.
3. تربط شبكات متعددة تابعة لمؤسسة واحدة أو عدة مؤسسات داخل المدينة.
4. تُدار غالبًا من قبل مزود خدمة الاتصالات المحلي أو الجهة المالكة.
5. توفر سرعات نقل بيانات عالية (قد تصل إلى 1000 Mbps أو أكثر).
6. تُستخدم كمرحلة وسيطة بين LAN وWAN.

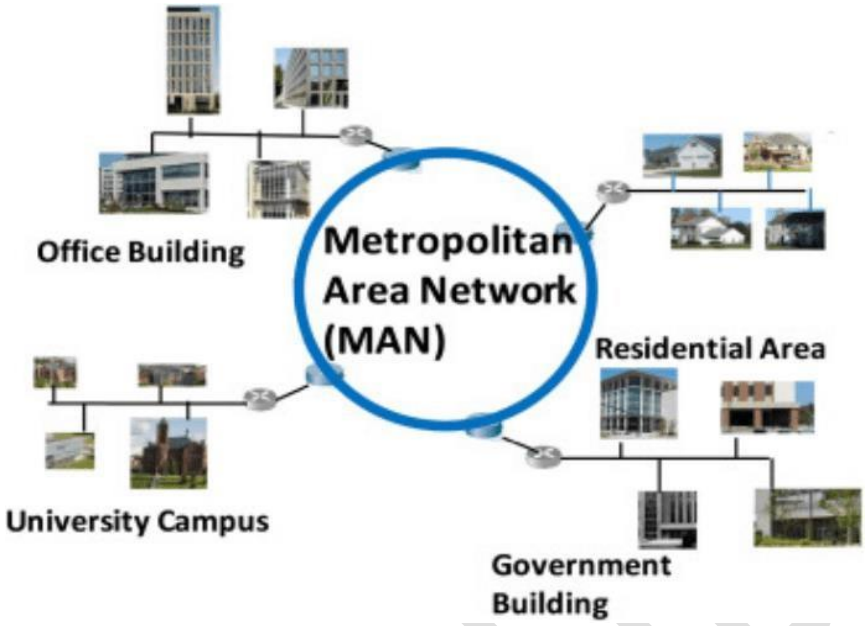
تستخدم الشبكات الحضرية MAN في العديد من التطبيقات، مثل:

1. ربط فروع الجامعات والمؤسسات التعليمية داخل مدينة واحدة.
2. ربط المستشفيات والمراكز الصحية بشبكة بيانات موحدة.
3. شبكات الحكومة المحلية أو البلدية.
4. ربط الشركات والمصارف في مركز المدينة.
5. تشغيل كاميرات المراقبة والأنظمة الأمنية في المدن الذكية.

للشبكة الحضرية MAN عيوب عديدة منها:

1. تكلفة إنشاء مرتفعة بسبب استخدام الألياف الضوئية.
2. إدارة وصيانة أعقد من الشبكات المحلية.
3. تأثر الأداء في حالة زيادة الحمل على الشبكة.

ESRA OUDA



4- الشبكة الشخصية (PAN):

تُعتبر الشبكة الشخصية (Personal Area Network – PAN) من أصغر أنواع الشبكات من حيث النطاق الجغرافي وعدد الأجهزة المتصلة. تُستخدم PAN لربط الأجهزة الإلكترونية القريبة من المستخدم مثل الحاسوب والهاتف الذكي والسماعات اللاسلكية والأجهزة القابلة للارتداء (Wearables). تُعد هذه الشبكات الأساس في الاتصالات الشخصية والأنظمة الذكية الحديثة، حيث تُستخدم على نطاق واسع في المنازل والمكاتب الصغيرة.

الشبكة الشخصية (PAN) هي شبكة صغيرة جدًا تُستخدم لربط الأجهزة الإلكترونية الشخصية ضمن نطاق محدود لا يتجاوز عادة 10 أمتار. تعمل PAN عبر وسائط سلكية مثل USB أو لاسلكية مثل Bluetooth و Infrared (الأشعة تحت الحمراء) وWi-Fi Direct. من خصائص الشبكة الشخصية:

1. نطاق جغرافي صغير جدًا (عادة من 1 إلى 10 أمتار).
2. عدد محدود من الأجهزة (2 إلى 8 أجهزة عادة).
3. سرعة نقل بيانات متوسطة حسب نوع التقنية.
4. منخفضة التكلفة وسهلة الإعداد.
5. تُستخدم غالبًا في التطبيقات الشخصية والمنزلية.
6. لا تحتاج إلى إدارة مركزية معقدة.

تستخدم الشبكات الشخصية PAN في العديد من التطبيقات، مثل:

1. ربط الهاتف الذكي مع الحاسوب لمزامنة البيانات.
2. تشغيل السماعات اللاسلكية عبر Bluetooth.
3. نقل الملفات بين الأجهزة المحمولة.
4. ربط الساعة الذكية أو أجهزة تتبع اللياقة البدنية بالهاتف لتتبع الحالة الصحية.
5. التحكم في الأجهزة المنزلية الذكية (مثل الإضاءة أو المكيفات).
6. الألعاب متعددة اللاعبين أي أنّ اللاعبين يتصلون فيما بينهم مباشرةً عبر شبكة قصيرة المدى (مثل Bluetooth أو Wi-Fi Direct) من دون الحاجة إلى الإنترنت.

للشبكة الشخصية PAN عيوب عديدة منها:

1. نطاق تغطية محدود.
2. بطء في نقل البيانات مقارنة بـ LAN أو WAN.
3. ضعف الأمان في بعض التقنيات مثل Bluetooth.
4. محدودية عدد الأجهزة المتصلة.



5- شبكة التخزين (SAN):

تعتبر شبكة تخزين البيانات (Storage Area Network – SAN) من أهم التقنيات المستخدمة في مراكز البيانات الحديثة. تهدف هذه الشبكات إلى توفير بيئة اتصال عالية السرعة بين الخوادم وأجهزة التخزين، مما يتيح نقل وإدارة البيانات بكفاءة وأمان. تُستخدم SAN في المؤسسات الكبيرة التي تتعامل مع كميات ضخمة من البيانات، مثل البنوك، المستشفيات، الجامعات، وشركات الاستضافة السحابية.

شبكة التخزين (SAN) هي شبكة متخصصة عالية الأداء تُستخدم لربط الخوادم (Servers) بأجهزة التخزين (Storage Devices) عبر شبكة مستقلة مخصّصة لتخزين البيانات. تتيح SAN مشاركة وحدات التخزين على مستوى الكتلة (Block Level) وليس على مستوى الملفات فقط، مما يجعلها أكثر سرعة ومرونة من الشبكات التقليدية. تُعتبر SAN مثالية للبيئات التي تتطلب معالجة كميات كبيرة من البيانات، مثل مراكز البيانات والتطبيقات المؤسسية. ومن خصائصها:

1. سرعة عالية جدًا في نقل البيانات (حتى 32 Gbps أو أكثر).
2. تفصل بين شبكة البيانات التشغيلية وشبكة التخزين لتحسين الأداء.
3. إمكانية توسيع السعة التخزينية بسهولة دون إيقاف النظام.
4. دعم عمليات النسخ الاحتياطي والاستعادة الفورية.
5. موثوقية عالية وتقليل فترات التوقف (High Availability).
6. إمكانية إدارة التخزين بشكل مركزي من خلال برمجيات إدارة متخصصة.

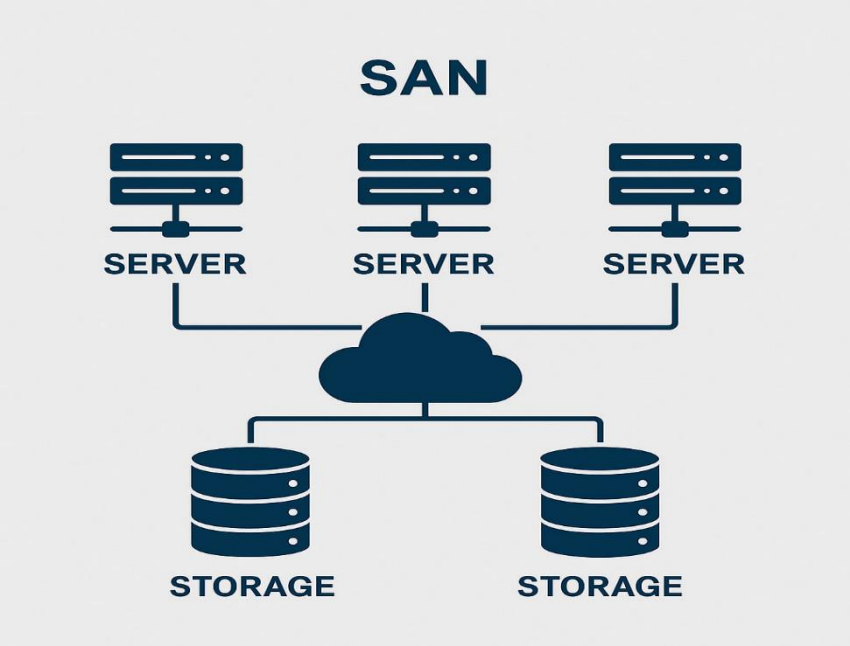
تستخدم شبكات التخزين SAN في العديد من التطبيقات، مثل:

1. مراكز البيانات (Data Centers) لتخزين وإدارة البيانات الضخمة.
2. أنظمة البنوك والمعاملات المالية.
3. أنظمة المستشفيات التي تعتمد على قواعد بيانات كبيرة.
4. بيئات الحوسبة السحابية وخوادم التطبيقات.
5. أنظمة النسخ الاحتياطي واستعادة البيانات.

لشبكة التخزين SAN عيوب عديدة منها:

1. تكلفة عالية لإنشاء وصيانة البنية التحتية.
2. تحتاج إلى خبرات فنية متقدمة في الإدارة.
3. صعبة التوسعة بدون تخطيط دقيق.
4. تأثر الأعطال المركزية بكل الشبكة.

ESRA OUBA



فيما يلي جدول مقارنة بين أنواع الشبكات الخمسة:

النوع	الاسم الكامل	النطاق الجغرافي	عدد الأجهزة	السرعة	الاستخدام الرئيسي	المزايا	العيوب
LAN	Local Area Network	داخل مبنى أو مؤسسة (حتى 1 كم)	من عشرات إلى مئات	عالية جدًا (حتى 1 جيجابت/ثانية أو أكثر)	ربط أجهزة الشركة أو الجامعة	سرعة عالية، أمان محلي	محدود النطاق، يحتاج صيانة
WAN	Wide Area Network	دول ومدن وقارات	غير محدد (هائل)	متوسطة	ربط شبكات متعددة عبر الإنترنت	تغطية عالمية	بطء نسبي، تكاليف كبيرة
MAN	Metropolitan Area Network	على مستوى مدينة أو جامعة	مئات إلى آلاف	متوسطة إلى عالية	ربط شبكات LAN داخل مدينة	تغطي نطاق أوسع من LAN	تكلفتها أعلى، إدارتها أصعب
PAN	Personal Area Network	بضعة أمتار (≈10م)	قليل جدًا (2–5 أجهزة)	منخفضة إلى متوسطة	ربط الأجهزة الشخصية مثل الهاتف والسماعة	سهولة الاتصال، لا تحتاج إنترنت	نطاق قصير وسرعة محدودة
SAN	Storage Area Network	داخل مركز بيانات (حتى مئات الأمتار)	خوادم وأجهزة تخزين	عالية جدًا	تخزين ونقل البيانات بين الخوادم	أداء عالٍ وموثوقية كبيرة	مكلفة ومعقدة التركيب

3- مكونات الشبكة الأساسية Basic network components

تُعتبر الشبكات أحد الأعمدة الأساسية في عالم التكنولوجيا الحديثة، حيث تسهم في تسهيل الاتصال وتبادل المعلومات بين الأجهزة. لفهم كيفية عمل الشبكات بفعالية، من الضروري التعرف على المكونات الأساسية التي تشكل هذه الشبكات. تشمل هذه المكونات الأجهزة، البرمجيات، البروتوكولات، الخطوط، والأجهزة الطرفية، وكل عنصر يلعب دورًا مهمًا في تحسين الأداء وضمان الاتصال السلس.

تتفاعل المكونات المختلفة مع بعضها البعض لتكوين نظام متكامل يسمح بنقل البيانات بسلاسة وأمان. من الموجهات والمحولات التي تدير حركة البيانات، إلى البرمجيات التي تدعم التشغيل والإدارة، تساهم كل هذه العناصر في تعزيز فعالية الشبكة وكفاءتها. مع تزايد الاعتماد على الشبكات في مختلف المجالات، يصبح فهم هذه المكونات أكثر أهمية لضمان بناء شبكات موثوقة وقابلة للتوسع.

تُعد مكونات الشبكة الأساسية (Network Components) الركيزة التي تقوم عليها أي بنية شبكية، سواء كانت شبكة محلية (LAN) أو حضرية (MAN) أو واسعة (WAN). حيث تتكوّن الشبكة من مجموعة من العناصر المادية (Hardware) والبرمجية (Software) التي تتكامل لتشكّل بيئة اتصال متكاملة تسمح بتبادل البيانات بين المستخدمين والأجهزة والتطبيقات بشكل آمن وفعّال.

فيما يلي شرح مبسّط لأهم المكونات الأساسية:

أولاً: المكونات المادية (Hardware Components)

وتقسم الى:

1. أجهزة الحاسوب (Computers)

ويقصد بها الحواسيب، السيرفرات، والطابعات التي تشكّل نقاط النهاية (End Devices) في الشبكة.

2. بطاقة واجهة الشبكة (Network Interface Card - NIC)

بطاقة واجهة الشبكة هي أحد المكونات الأساسية في أي شبكة حاسوب، وتُعد الوسيط الذي يربط الجهاز بالشبكة سواء كانت سلكية أو لاسلكية. وهي قطعة من العتاد (Hardware) تُركّب داخل الحاسوب أو تُدمج في اللوحة الأم، وتقوم بتمكين الجهاز من إرسال واستقبال البيانات عبر الشبكة.

وظيفتها:

1. تحويل البيانات من صيغة رقمية يفهمها الحاسوب إلى إشارات يمكن نقلها عبر الكابل أو الموجات اللاسلكية.
2. التعرّف على الأجهزة الأخرى في الشبكة من خلال عنوان فريد يُسمى عنوان MAC (Media Access Control Address).
3. إدارة الاتصال بين الجهاز وباقي الشبكة لضمان عدم تضارب الإشارات أو فقدان البيانات.

أنواع بطاقات واجهة الشبكة:

1. **بطاقة سلكية (Ethernet NIC):**

تُستخدم الكيبلات وتُعرف بسرعتها العالية واستقرارها.

2. **بطاقة لاسلكية (Wireless NIC):**

تتصل بالشبكة عبر الواي فاي (Wi-Fi) وتُستخدم عادة في الهواتف، الحواسيب المحمولة، والأجهزة الذكية.

3. **بطاقة مدمجة (Integrated NIC):**

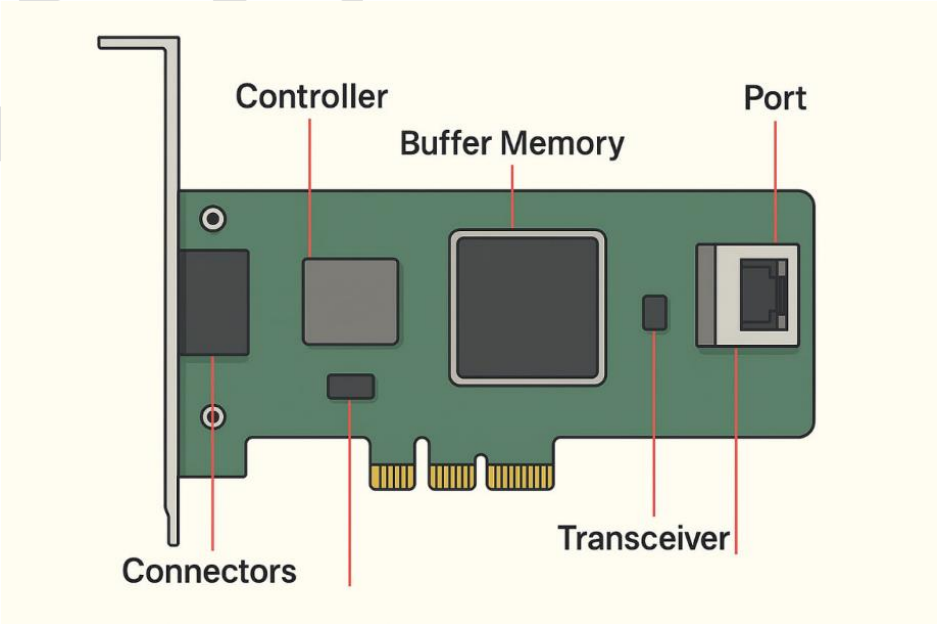
تأتي مدمجة في اللوحة الأم لمعظم الأجهزة الحديثة.

4. **بطاقة خارجية (External NIC):**

تُوصل عبر منفذ USB ، وتُستخدم عندما لا تكون البطاقة المدمجة متوفرة أو لا تعمل.

أهميتها:

1. تُمكّن الحواسيب من التواصل وتبادل الملفات والإنترنت.
2. تعتبر أساس عمل الشبكات المحلية (LAN).
3. بدونها لا يمكن للجهاز الانضمام إلى أي شبكة.



4. الكابلات (Cables)

الكابلات هي وسائط مادية تُستخدم لنقل البيانات أو الإشارات بين الأجهزة داخل الشبكات أو الأنظمة الإلكترونية.

من أنواعها:

1. كابل الأزواج المجدولة (Twisted Pair)

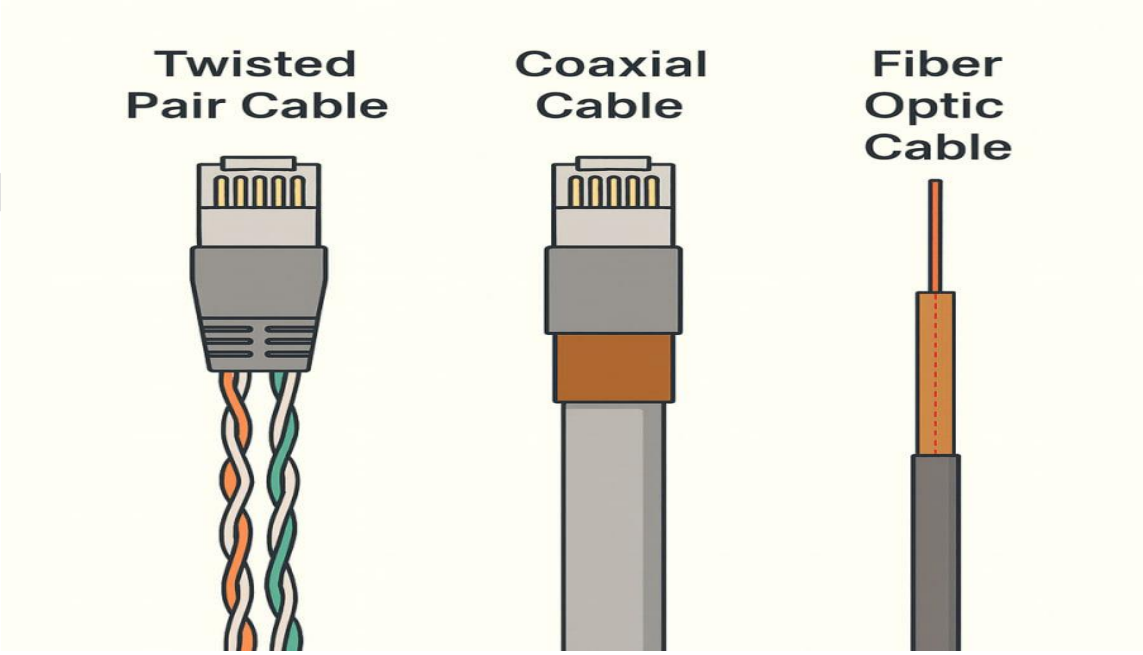
هو كابل يحتوي على أسلاك نحاسية مزدوجة ملتفة معًا لتقليل التشويش أثناء نقل البيانات، ويُستخدم عادةً في الشبكات المحلية (LAN) لربط الحواسيب بالمبدلات أو الموجهات.

2. كابل الألياف الضوئية (Fiber Optic)

هو نوع من الكابلات يستخدم خيوطًا زجاجية أو بلاستيكية رفيعة لنقل البيانات على شكل نبضات ضوئية بدلًا من الإشارات الكهربائية، ويتميز بسرعات عالية جدًا ومدى طويل مع مقاومة قوية للتشويش والتداخل.

3. الكابل المحوري (Coaxial)

هو كابل يستخدم سلكًا نحاسيًا مركزيًا محاطًا بطبقة عازلة وغلاف معدني خارجي لحمايته من التشويش. يُستخدم لنقل إشارات الإنترنت والتلفاز والاتصالات، ويتميز بثبات الإشارة ومتانته، لكنه أقل سرعة من الألياف الضوئية وأثقل من كابل الأزواج المجدولة.



4. الموزع (Hub)

الموزّع (Hub) هو أحد المكونات الأساسية في الشبكات المحلية (LAN)، ويُستخدم لربط مجموعة من الأجهزة (مثل الحواسيب والطابعات) ببعضها في شبكة واحدة. يُعتبر من أبسط أجهزة الشبكات، وغالبًا ما يُستخدم في الشبكات الصغيرة أو التعليمية. فهو جهاز يقوم بتجميع الإشارات القادمة من أجهزة متعددة وإعادة إرسالها إلى جميع الأجهزة المتصلة به، بحيث تصل البيانات إلى كل المنافذ في نفس الوقت. الربط الأساسي للموزع يكون سلكي فقط.

وظيفة الموزّع:

عندما يُرسل أحد الأجهزة بيانات عبر الشبكة:

1. يستقبل الموزّع هذه البيانات.
2. ثم ينقلها إلى جميع الأجهزة المتصلة به دون تمييز.
3. الجهاز الذي يكون عنوانه مطابقًا فقط هو من يستقبل البيانات ويعالجها، أما البقية فتتجاهلها.

أنواع الموزعات:

1. **موزّع نشط (Active Hub):**

يقوم بتضخيم الإشارة قبل إرسالها لباقي الأجهزة. يحتاج إلى مصدر طاقة كهربائية.

2. **موزّع غير نشط (Passive Hub):**

يمرر الإشارة كما هي دون تقوية أو معالجة. لا يحتاج إلى طاقة كهربائية.

3. **موزّع ذكي (Intelligent Hub):**

يحتوي على قدرات إدارة ومراقبة حركة البيانات في الشبكة.

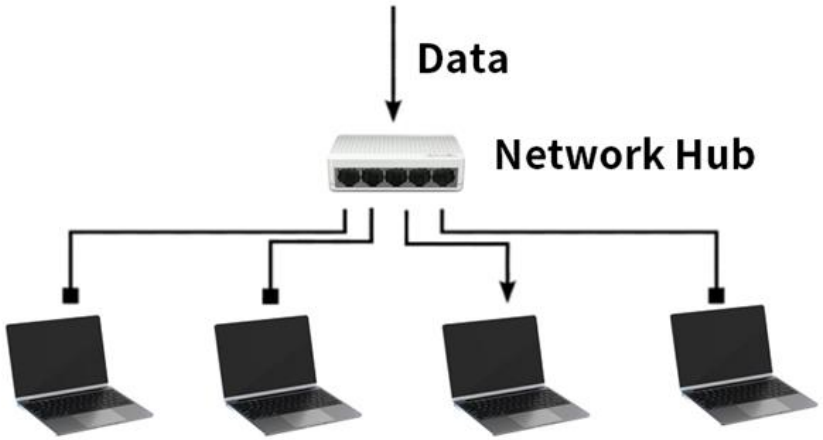
مميزات الموزع:

- ✅ سهل التركيب والاستخدام.
- ✅ رخيص الثمن مقارنة بالمبدلات (Switches).
- ✅ مناسب للشبكات الصغيرة والبسيطة.

ESRA QUBA

عيوب الموزع:

- ✗ يرسل البيانات إلى جميع الأجهزة، مما يُسبب ازدحامًا في الشبكة.
- ✗ لا يستطيع تمييز الأجهزة أو توجيه البيانات بذكاء.
- ✗ أبطأ وأقل كفاءة من المبدّل (Switch).
- ✗ يفتقر إلى خصائص الأمان والتحكم.



5. المبدّل (Switch)

المبدّل (Switch) هو أحد أهم أجهزة الشبكات، ويُعتبر تطورًا متقدّمًا عن الموزّع (Hub)، لأنه أكثر ذكاءً وسرعة وكفاءة في إدارة حركة البيانات داخل الشبكة المحلية (LAN). وهو جهاز يربط عدة أجهزة حاسوب داخل شبكة محلية، ويقوم بتوجيه البيانات بدقة إلى الجهاز المقصود فقط، وليس إلى جميع الأجهزة كما يفعل الموزّع.

وظيفة المبدّل:

عند إرسال جهاز ما بيانات إلى جهاز آخر في الشبكة:

1. يستقبل المبدّل البيانات.
2. يقرأ عنوان الـMAC الخاص بالجهاز المستقبل. حيث يحتفظ المبدّل بجدول يُسمى MAC Address Table. هذا الجدول يربط كل منفذ بعنوان الجهاز المتصل به. عندما تمر البيانات لأول مرة، يتعلم المبدّل العناوين تلقائيًا ويخزنها في هذا الجدول.
3. يرسل البيانات فقط إلى المنفذ الذي يتصل به الجهاز المقصود.

وبهذا يقلل المبدّل من الازدحام ويحسن أداء الشبكة بشكل كبير.

أنواع المبدل:

هناك عدة أنواع من المبدلات منها:

1. مبدّل مُدار (Managed Switch):

يسمح بالإدارة والمراقبة والتحكم في حركة البيانات. يُستخدم في الشبكات الكبيرة (مثل الجامعات أو الشركات).

2. مبدّل غير مُدار (Unmanaged Switch):

سهل الاستخدام، يُستخدم في المنازل أو الشبكات الصغيرة. لا يمكن التحكم في إعداداته.

3. المبدل الذكي (Smart Switch)

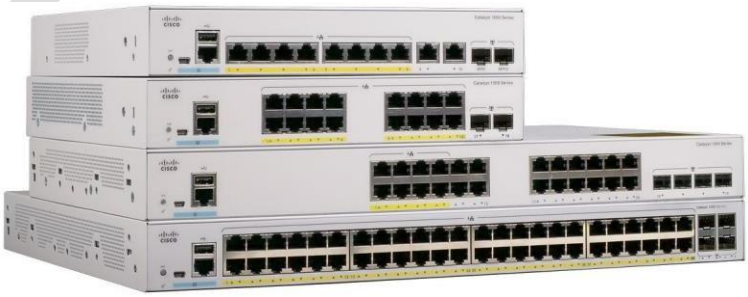
خليط بين النوعين السابقين. يحتوي على إعدادات أساسية ولكن أبسط من المبدل المُدار الكامل.

مميزات المبدل:

- ✅ يوجّه البيانات للجهاز الصحيح فقط.
- ✅ يقلل من ازدحام الشبكة.
- ✅ أسرع من الموزع (Hub).
- ✅ أكثر أمانًا وكفاءة.
- ✅ يدعم نقل البيانات في الاتجاهين (Full Duplex).

عيوبه:

- ❌ أغلى من الموزّع.
- ❌ يحتاج إعدادًا وإدارة في الأنواع المتقدمة.
- ❌ لا يربط بين شبكات مختلفة (مثل الراوتر).



ESRA QUBA

6. الراوتر (الموجه Router)

هو أحد أهم أجهزة الشبكات الحديثة، ويُعتبر العقل الذي يربط بين الشبكات المختلفة، مثل ربط شبكة المنزل أو المكتب بشبكة الإنترنت. وظيفته الأساسية هي توجيه البيانات من شبكة إلى أخرى بأفضل مسار ممكن.

الراوتر هو جهاز شبكة ذكي يقوم بتحديد المسار الأفضل للبيانات بين شبكات متعددة ويُستخدم في المنازل، الشركات، والمؤسسات لربط الشبكات المحلية (LAN) بالإنترنت (WAN).

وبشكل مبسط هو مثل **المرور** الذي يوجّه السيارات (البيانات) إلى الطريق الصحيح بين الشبكات.

وظيفة الراوتر:

عندما ترسل جهازك طلبًا للوصول إلى موقع على الإنترنت:

1. يقوم الراوتر باستلام الطلب من شبكتك المحلية.
2. يحلل عنوان الوجهة (IP Address) للموقع المطلوب. حيث كل جهاز في الشبكة له عنوان IP. الراوتر يستخدم جداول تُسمى Routing Tables لتحديد المسار الأنسب لكل حزمة بيانات.
3. يختار أفضل مسار لتوصيل البيانات إلى وجهتها عبر الشبكات الأخرى.
4. يستقبل الرد من الإنترنت ويعيد توجيهه إلى الجهاز الذي أرسل الطلب.
5. يمكنه أيضًا توزيع الإنترنت على عدة أجهزة في نفس الوقت.

أنواع الراوتر (الموجه):

هناك العديد من أنواع الموجهات منها:

1. الراوتر السلكي (Wired Router)

- يُستخدم الكابلات (Ethernet) لربط الأجهزة.
- مناسب للشبكات المكتبية الثابتة.
- يتميز بالثبات والأمان العالي.

2. الراوتر اللاسلكي (Wireless Router – Wi-Fi)

- يوفّر اتصالًا لاسلكيًا عبر موجات Wi-Fi.
- الأكثر انتشارًا في المنازل والمكاتب.
- يربط الأجهزة بالإنترنت دون أسلاك.

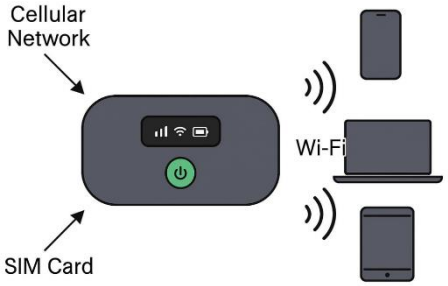
ESRA QUBA

3. راوتر VPN (VPN Router)

- يوفّر اتصالًا مشفّرًا وآمنًا عبر الإنترنت.
- يُستخدم في الشركات لحماية البيانات أثناء التنقل بين الفروع.

4. الراوتر المحمول (Portable Router أو Mobile Router)

هو راوتر يعمل بشريحة SIM مثل الهاتف، ويحوّل إشارة الإنترنت من شبكة الموبايل إلى واي فاي (Wi-Fi) يمكن للأجهزة الأخرى الاتصال بها هو جهاز صغير يُستخدم لتوفير الإنترنت أثناء التنقل يتميز بـ :



Portable Router

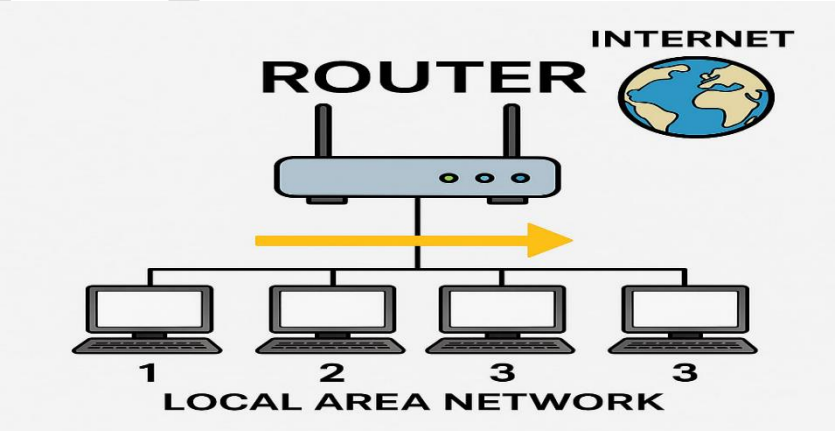
- صغير الحجم وسهل الحمل.
- يعمل بالبطارية، ويمكن استخدامه في أي مكان.
- يمكن توصيل عدة أجهزة في نفس الوقت (هاتف، لابتوب، تابلت...).
- لا يحتاج إلى كابلات.

مميزات الراوتر:

✅ يربط الشبكات المحلية بالإنترنت.
✅ يختار المسار الأفضل للبيانات.
✅ يحتوي على جدار حماية مدمج للحماية من الهجمات.
✅ يدعم الاتصال السلكي واللاسلكي.
✅ يمكنه توزيع عناوين IP تلقائيًا.

عيوب الراوتر:

❌ أغلى من الموزّع والمبدّل.
❌ يحتاج إلى إعدادات أكثر تعقيدًا.
❌ إذا تم ضبطه بشكل غير صحيح، قد يُضعف أمان الشبكة.



FSRA OUBA

7. نقطة الوصول اللاسلكية (Access Point)

نقطة الوصول اللاسلكية (Access Point) هي جهاز يتيح للأجهزة مثل الهواتف واللابتوبات الاتصال بالشبكة المحلية (LAN)عن طريق الواي فاي (Wi-Fi) بدلًا من الكابلات وكذلك توسيع نطاق الشبكة اللاسلكية (Wi-Fi). يستقبل البيانات من السويتش/الراوتر عبر كابل إيثرنت، ويُحوّلها إلى موجات لاسلكية والعكس.

وظيفتها:

1. تعمل كجسر (Bridge) بين الشبكة السلكية (المتصلة بالمبدل أو الراوتر) وبين الأجهزة اللاسلكية مثل الهواتف واللابتوبات.
2. تقوم ببث إشارة الواي فاي ليستطيع المستخدمون الاتصال بالشبكة أو بالإنترنت دون الحاجة إلى أسلاك.

أنواع نقاط الوصول:

هناك العديد من أنواع نقاط الوصول منها:

1. نقطة وصول مستقلة (Standalone Access Point)

- تعمل بشكل منفصل دون الحاجة إلى وحدة تحكم مركزية.
- تُستخدم عادةً في البيوت أو المكاتب الصغيرة.
- إعدادها بسيط لكنها لا تناسب الشبكات الكبيرة.

2. نقطة وصول بإدارة مركزية (Controller-Based Access Point)

- تُدار من خلال وحدة تحكم مركزية .
- مثالية للمؤسسات والشركات الكبيرة حيث يمكن التحكم بعدة نقاط وصول من مكان واحد.
- تُسهل الإدارة وتضمن استقرار الشبكة، لكنها أغلى سعرًا.

3. موسع نطاق الإشارة (Range Extender / Repeater)

- لا تُنشئ شبكة جديدة، بل تُعيد بث إشارة الراوتر لزيادة التغطية.
- تُستخدم في المنازل أو الأماكن التي فيها ضعف في الإشارة.
- سهلة الإعداد لكنها قد تُخفض السرعة قليلاً.

مميزات نقطة الوصول:

- ✅ توسّع نطاق الشبكة.
- ✅ تدعم عددًا كبيرًا من الأجهزة.
- ✅ يمكن إدارتها مركزيًا.
- ✅ سهلة التوسعة والإضافة.
- ✅ تحسّن جودة الإشارة.

ESRA OUDA

عيوب نقطة الوصول:

- ✗ مرتفعة التكلفة.
- ✗ إعدادها معقد.
- ✗ قد يحدث تداخل بالإشارات.
- ✗ تعتمد على الاتصال السلكي.
- ✗ ضعف الأداء عند سوء التوزيع.



8. المودم Modem

وهو جهاز يقوم بتحويل الإشارات الرقمية من الحاسوب إلى إشارات تناظرية (Analog) يمكن إرسالها عبر خطوط الهاتف أو الكابل، ثم يعيد تحويلها مرة أخرى إلى رقمية عند الاستقبال.

وظيفته:

الوظيفية الأساسية للمودم هي ربط شبكتك المحلية (LAN) أو جهازك بالإنترنت. وكذلك هو الوسيط بين مزوّد الخدمة (ISP) وبين شبكتك المنزلية أو المؤسسية.

أنواع المودم:

هناك العديد من أنواع المودمات منها:

1. **مودم الطلب الهاتفي Dial-up Modem**

   قديم جدًا، يستخدم خطوط الهاتف التقليدية.

2. **مودم الكابل Cable Modem**

   يستخدم كابل التلفاز لتوفير إنترنت أسرع.

3. **مودم الألياف الضوئية Fiber Modem**

   خاص بخدمة الألياف الضوئية .

4. **المودم اللاسلكي Wireless Modem (4G / 5G Modem)**

   يعمل بشرائح الهاتف المحمول .

معلومة مهمة:

في أغلب الأجهزة الحديثة، يكون المودم مدمجًا مع الراوتر في جهاز واحد يسمى Modem Router، بحيث يقوم المودم بالاتصال بمزود الإنترنت، والراوتر يوزّع الإنترنت لاسلكيًا على الأجهزة.

مميزات المودم:

- ✅ يوفّر الاتصال بالإنترنت من خلال مزوّد الخدمة.
- ✅ يحوّل الإشارات بين الرقمية والتناظرية بدقة.
- ✅ سهل التركيب والاستخدام.
- ✅ يمكن دمجه مع الراوتر لتوزيع الإنترنت.
- ✅ تتنوع أنواعه لتناسب جميع تقنيات الاتصال (DSL، Fiber، G4، إلخ).

عيوب المودم:

- ❌ لا يوزّع الإنترنت على الأجهزة (إلا إذا كان مدمجًا مع راوتر).
- ❌ يعتمد على نوع الخدمة المقدّمة من مزوّد الإنترنت.
- ❌ قد يكون بطيئًا في الأنواع القديمة مثل Dial-up وDSL.
- ❌ يحتاج إلى إعداد وصيانة عند تغيّر الخدمة أو الشبكة.
- ❌ قد يتأثر بالأعطال في الخطوط أو الكابلات الخارجية.



فيما يلي جدول مقارنة لأجهزة الشبكة:

الجهاز	التعريف	الوظيفة الأساسية	يبث الإنترنت؟	ذكي في التوجيه؟	عدد المنافذ عادةً
Hub (الموزّع)	جهاز بسيط يربط عدة أجهزة في شبكة محلية	يرسل البيانات إلى جميع الأجهزة دون تمييز	✗ لا	✗ لا	4 – 12
Switch (المبدّل)	يربط الأجهزة في نفس الشبكة لكن بذكاء	يرسل البيانات للجهاز المعني فقط عبر MAC Address	✗ لا	☑ جزئيًا	8 – 48
Router (الراوتر)	يربط بين شبكات مختلفة (مثل LAN و Internet)	يوجّه البيانات بين الشبكات باستخدام IP	☑ نعم	☑ نعم جدًا	2 – 8
Access Point (نقطة الوصول)	يربط الأجهزة اللاسلكية بالشبكة السلكية	توفّر اتصال Wi-Fi ضمن الشبكة المحلية	✗ لا (تحتاج راوتر)	✗ لا	1 – 2
Modem (المودم)	يحوّل الإشارات بين رقمية وتناظرية للاتصال بالإنترنت	يربط الشبكة المحلية بمزوّد الإنترنت	☑ نعم	✗ لا	1 – 2

ثانياً: المكونات البرمجية (Software Components)

تمثل الجزء غير المادي الذي يُدير حركة البيانات ويتيح التواصل بين الأجهزة. وتشمل هذه المكونات أنظمة التشغيل والبروتوكولات وآليات الإدارة التي تُمكّن الشبكة من العمل بكفاءة حيث تقسم الى:

1. أنظمة التشغيل الشبكية (Network Operating System NOS)

وهي المسؤولة عن إدارة موارد الشبكة، المستخدمين، الأذونات، والأمان.

مثل: Windows Server، Linux، Unix.

2. برامج الشبكة (Network Software)

تُستخدم لمراقبة أداء الشبكة واكتشاف الأعطال وإصلاحها. حيث تسمح بإدارة الشبكة وتحليل الأداء.

مثل: SolarWinds، Wireshark، PRTG Network Monitor،.

3. البروتوكولات (Protocols)

مجموعة من القواعد والمعايير التي تحدد كيفية تبادل البيانات وتنظّم عملية الاتصال بين الأجهزة.

ومن أشهرها: IP / TCP (نقل البيانات عبر الإنترنت)

HTTP / HTTPS (تصفح الويب)

4- اساسيات أمان الشبكة Network Security Basics

مع تطور الاتصالات الرقمية وتزايد اعتماد المؤسسات على الإنترنت، أصبح أمن الشبكات من أهم الركائز في عالم الحوسبة. حيث يُعتبر أمان الشبكة عنصرًا حيويًا في عالم التكنولوجيا الحديثة، حيث تتزايد التهديدات السيبرانية بشكل مستمر. ومع الاعتماد المتزايد على الشبكات في الأعمال التجارية، والتعليم، والخدمات الحكومية، يصبح تأمين هذه الشبكات أمرًا ضروريًا لحماية المعلومات الحساسة والبيانات الشخصية. تتضمن أساسيات أمان الشبكة مجموعة من السياسات والتقنيات التي تهدف إلى حماية الشبكات من الهجمات والاختراقات حيث يهدف هذا المجال إلى حماية البنية التحتية للشبكات، والمعلومات، والأنظمة من الوصول غير المصرّح به أو التعديل أو التدمير. فأمن الشبكة لا يقتصر على منع الاختراقات فحسب، بل يشمل أيضًا ضمان سرية البيانات وسلامتها وتوافرها من خلال تنفيذ استراتيجيات فعالة مثل استخدام جدران الحماية، وتشفير البيانات، وإدارة الهوية، يمكن للمؤسسات تقليل المخاطر وتعزيز مستوى الأمان. علاوة على ذلك، يعتبر التوعية والتدريب جزءًا أساسيًا من أمان الشبكة، حيث يُساعد الموظفون على التعرف على التهديدات المحتملة والتصرف بشكل مناسب.

اذاً أمن الشبكة (Network Security) هو مجموعة من السياسات والإجراءات والتقنيات التي تُستخدم لحماية البيانات والأجهزة والشبكات من الهجمات أو الأعطال أو التهديدات الإلكترونية. يشمل ذلك التحكم في الوصول، التشفير، مراقبة النشاط، الكشف عن التسلل، والتعافي من الحوادث. بمعنى آخر، هو نظام شامل من الأدوات والإجراءات يهدف إلى منع الاستخدام غير المصرح به وضمان اتصال آمن ومستقر بين المستخدمين داخل الشبكة.

في ظل التحديات الكبيرة التي تواجهها الشبكات اليوم، فإن فهم أساسيات أمان الشبكة يُعد خطوة أساسية نحو بناء بيئة آمنة وموثوقة للتواصل وتبادل المعلومات. وهنا نذكر بعض الأساسيات المهمة في هذا المجال:

1. التحديث المستمر:

يجب تحديث أنظمة التشغيل والبرامج بصورة منتظمة لسد الثغرات الأمنية التي قد يستغلها المهاجمون حيث تعتبر هذه الخطوة أساسية لتأمين الأجهزة المستخدمة في الشبكة.

2. كلمات المرور القوية:

استخدام كلمات مرور معقدة يصعب تخمينها، وتغييرها بشكل دوري لحماية الحسابات من الاختراق.

3. التشفير (Encryption):

يُستخدم لتأمين البيانات أثناء نقلها عبر الشبكة، بحيث لا يتمكن أي طرف غير مصرح له من قراءتها ويستخدم بروتوكولات خاصة للتشفير مثل HTTPS لتأمين البيانات اثناء النقل.

4. جدران الحماية (Firewalls):

تعمل كحاجز بين الشبكة الداخلية والعالم الخارجي، وتقوم بفلترة حركة البيانات غير المرغوب فيها. وتعتبر خطوة ضرورية لتأمين الشبكة نفسها.

5. نُظم كشف ومنع التسلل (IDS/IPS):

تُراقب الأنشطة داخل الشبكة وتكتشف محاولات الاختراق أو الهجمات المشبوهة. تستخدم لرصد حركة المرور، وتحليل السجلات الأمنية لتحديد أي نشاط غير طبيعي. هذه الإجراءات تساهم في تعزيز الأمان العام للشبكة.

6. المصادقة (Authentication):

يقصد بالمصادقة التأكد من هوية المستخدمين الذين يحاولون الدخول إلى النظام حيث تعتبر عملية التحقق من الهوية ضرورية لضمان أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى الشبكة حيث ان إدارة الهوية بشكل فعال يساعد في تقليل احتمالات الاختراق.

7. النسخ الاحتياطي (Backup):

أخذ نسخ احتياطية منتظمة من البيانات الهامة لتفادي فقدانها في حال وقوع هجمات أو أعطال أو التعرض لهجمات سيبرانية حيث ان إجراء النسخ الاحتياطي المنتظم للبيانات يُعتبر جزءًا مهمًا من الاستراتيجية الأمنية.

8. التدريب والتوعية الأمنية:

يعتبر التوعية والتدريب عنصرًا أساسيًا في تعزيز أمان الشبكة ويقصد به رفع مستوى الوعي لدى المستخدمين حول مخاطر الإنترنت وأهمية اتباع الممارسات الأمنية السليمة فان تثقيف الموظفين حول السياسات والإجراءات الأمنية يُساعد في تقليل المخاطر.

الخلاصة

أمان الشبكة لا يعتمد على جهاز واحد أو برنامج واحد، بل على منظومة متكاملة من السياسات والإجراءات التقنية والبشرية. تبدأ من التحليل والتخطيط، مرورًا بالتحكم والمراقبة، وتنتهي بالتدريب والاستجابة الذكية.
إن بناء بيئة شبكية آمنة يتطلب تعاونًا بين إدارة تكنولوجيا المعلومات، والإدارة العليا، والمستخدمين أنفسهم لضمان حماية البيانات واستمرارية الخدمات في وجه أي تهديد.

ESRA OUBA

5- فهم تهديدات الشبكة Understanding network threats

في بيئة رقمية مترابطة مثل شبكات المؤسسات والجامعات، تُعدّ تهديدات الشبكة من أخطر التحديات الأمنية التي قد تتسبب في تعطيل الخدمات أو سرقة البيانات أو إتلاف الأنظمة. ولفهم كيفية الحماية، يجب أولًا فهم طبيعة التهديدات وأنواعها ومصادرها لأنها الأساس في تصميم استراتيجيات أمان فعّالة.

تُعتبر تهديدات الشبكة مجموعة من المخاطر التي يمكن أن تؤثر سلبًا على سلامة البيانات وأمن الأنظمة. فهي أي خطر محتمل يمكن أن يستغل ثغرة أمنية داخل النظام أو الأجهزة أو التطبيقات، مما يؤدي إلى اختراق أو تلاعب أو تعطيل للشبكة أو بياناتها. يمكن أن تأتي التهديدات من مصادر خارجية مثل القراصنة، أو من مصادر داخلية مثل المستخدمين أو الإهمال البشري.

في عصر التكنولوجيا الحديثة، تتزايد هذه التهديدات بشكل مستمر، مما يتطلب فهمًا عميقًا لها لضمان حماية الشبكات. إليك تفصيلًا لأبرز تهديدات الشبكة:

1- الفيروسات والبرمجيات الخبيثة Viruses & Malware

تُعتبر الفيروسات (Viruses) والبرمجيات الخبيثة (Malware) من أخطر التهديدات التي تواجه الشبكات. هذه البرامج الضارة يمكن أن تتسلل إلى الأجهزة من خلال تحميلات غير موثوقة أو مرفقات بريد إلكتروني. بمجرد دخولها، يمكن أن تؤدي إلى:

- **تلف البيانات:** قد تقوم بتشفير البيانات أو حذفها، مما يؤدي إلى فقدان المعلومات القيمة.
- **جمع المعلومات:** يمكن أن تُستخدم لتجميع معلومات حساسة، مثل كلمات المرور أو البيانات المالية.
- **التحكم عن بُعد:** بعض البرمجيات الخبيثة تمنح المهاجمين القدرة على التحكم في الجهاز المصاب.

من **امثلتها**: فيروس, تروجان, برامج تجسس (Spyware).

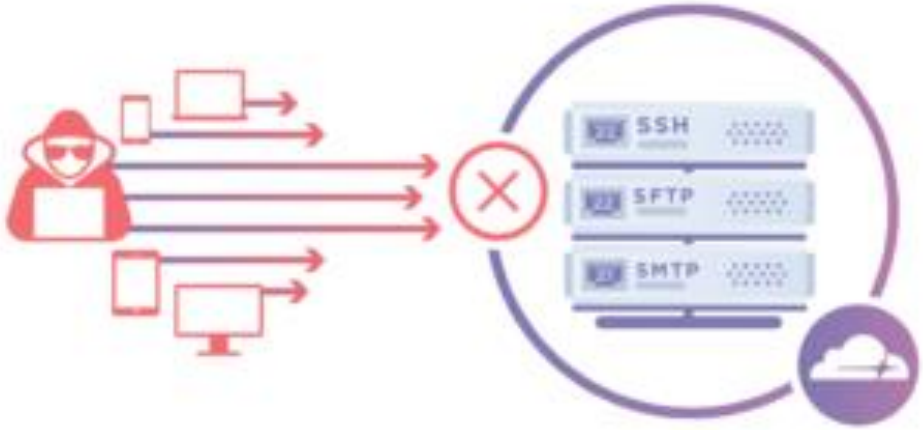


2- هجمات الحرمان من الخدمة الموزعة DDoS Attacks

تعتبر هجمات الحرمان من الخدمة الموزعة (DDoS) من أبرز التهديدات التي تستهدف الشبكات. في هذا النوع من الهجمات، يقوم المهاجمون بزيادة عدد الطلبات الواردة إلى خادم معين بحيث تمنعه من تقديم الخدمة للمستخدمين بهدف تعطيل المواقع والشبكات والخدمات الإلكترونية مما يؤدي إلى:

- **إيقاف الخدمة:** يتسبب ذلك في توقف الخادم عن الاستجابة للمستخدمين الشرعيين.
- **إبطاء الأداء:** قد يؤدي إلى بطء استجابة الشبكة بشكل عام، مما يؤثر على تجربة المستخدم.

من امثلتها: هجوم على البنك الوطني الدنماركي عام 2023 حيث تم إغراق الخوادم بطلبات HTTP مزيفة مما أدى الى توقف موقع البنك وخدماته الإلكترونية مؤقتًا.



3- الاختراقات Hacking

الاختراق هو عملية الدخول غير المصرح به إلى الأنظمة أو الشبكات عبر ثغرات برمجية أو كلمات مرور ضعيفة بهدف سرقة البيانات أو إلحاق الضرر. من هذه الاختراقات ما يلي:

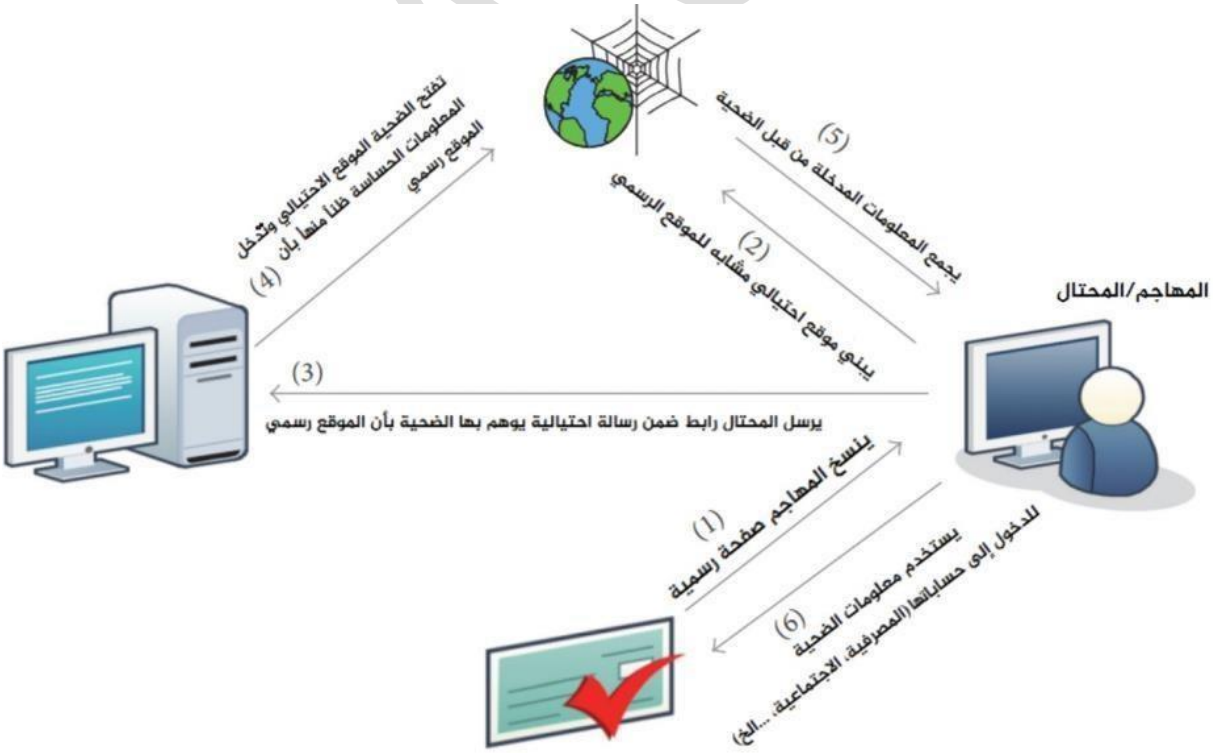
- الاختراقات عبر الشبكات أي استخدام الثغرات الأمنية في الشبكات للوصول إلى المعلومات الحساسة, سرقة بيانات, تخريب الأنظمة, تثبيت برامج تجسس.
- تسريب بيانات المستخدمين.
- زرع أبواب خلفية (Backdoors) تسمح بالدخول لاحقًا.



4- التصيد الاحتيالي Phishing

يُعتبر التصيد الاحتيالي نوعًا من الهجمات التي تهدف إلى خداع المستخدمين للكشف عن بياناتهم الحساسة. يُعتبر من أكثر الهجمات انتشاراً ويستخدم المهاجمون رسائل بريد إلكتروني مزيفة أو مواقع ويب تبدو شرعية لجذب الضحايا وخداع المستخدمين وإدخال معلوماتهم الخاصة. يمكن أن تشمل المخاطر:

- **سرقة الهوية:** قد يؤدي إلى سرقة معلومات الهوية الشخصية مثل أرقام الضمان الاجتماعي أو معلومات الحسابات المصرفية.
- **إلحاق الضرر بالسمعة:** ان تسرب بيانات العملاء أو تعرض أنظمتهم للاختراق يؤدي إلى تآكل الثقة بالمؤسسة، وقد ينعكس ذلك على الانخفاض في ولاء العملاء وتراجع العقود التجارية وفرص التعاون.



5- التهديدات الداخلية Insider Threats

لا تقتصر التهديدات على المهاجمين الخارجيين فقط؛ بل يمكن أن تأتي أيضًا من داخل الشركة او المؤسسة نفسها. من التهديدات الداخلية:

- **الموظفون غير المصرح لهم:** قد يقوم بعض الموظفين بالوصول إلى معلومات حساسة بدون إذن. بهدف الانتقام او تسريب البيانات عمداً.
- **سوء الاستخدام العرضي:** يمكن أن يتسبب الموظفون في أضرار من خلال تصرفات غير مسؤولة، مثل تحميل برامج غير آمنة او إهمال أو جهل يؤدي لتسريب معلومات.



الخلاصة

فهم تهديدات الشبكة يعتبر خطوة أساسية في تطوير استراتيجيات أمان فعالة حيث من خلال التعرف على الأنواع المختلفة من التهديدات، يمكن للمؤسسات اتخاذ الإجراءات اللازمة لحماية شبكاتها وبياناتها. ويشمل ذلك تنفيذ تدابير الأمان المناسبة، وتوعية المستخدمين، وإجراء تقييمات دورية للمخاطر.

6- استكشاف أخطاء الشبكة Network troubleshooting

تُعد عملية استكشاف أخطاء الشبكة وإصلاحها من أهم المهارات في إدارة الأنظمة والبنى التحتية التقنية. فالشبكات — مهما كانت متطورة — قد تواجه مشكلات تؤثر على الاتصال أو الأداء أو الأمان، مما يتطلب قدرة على تحديد المشكلة، تحليلها، ثم إصلاحها دون التأثير على استمرارية الخدمة.

اذاً استكشاف أخطاء الشبكة هي عملية تحليل وتحديد المشكلات التي تؤثر على أداء الشبكة أو تعيق الاتصال بين الأجهزة. تعتبر هذه العملية ضرورية للحفاظ على استمرارية العمل وتحسين أداء الشبكة. إليك بعض الخطوات الرئيسية لاستكشاف أخطاء الشبكة:

1. تحديد المشكلة (Identify the Problem)

قبل البدء في الإصلاح، يجب تحديد طبيعة المشكلة بدقة أي ابدأ بتجميع معلومات دقيقة مثل هل المشكلة في جهاز واحد أم أكثر؟ هل الاتصال الداخلي (LAN) يعمل لكن الإنترنت لا؟ هل نوع الاتصال سلكي أم لاسلكي؟ متى بدأت المشكلة؟ هل حدث تغيير قبلها (تحديث، إعداد جديد، كابل جديد)؟ حيث يمكن أن تتضمن المشاكل ما يلي:

- **انقطاع الاتصال**: عدم القدرة على الوصول إلى الإنترنت أو إلى أجهزة معينة.
- **بطء الأداء:** تأخر في تحميل الصفحات أو تنزيل الملفات.
- **مشكلات في الاتصال اللاسلكي:** ضعف الإشارة أو انقطاع الاتصال.

2. التحقق من الاجهزة

بعد تحديد المشكلة، يجب فحص الأجهزة المتصلة بالشبكة بهدف التأكد أنه لا يوجد عطل مادي أو انقطاع فيزيائي. تشمل هذه الخطوة:

- **إعادة تشغيل الأجهزة**: قد تحل إعادة تشغيل الأجهزة مثل الموجهات، والمحولات، والأجهزة الطرفية العديد من المشكلات.
- **فحص الكابلات**: تأكد من أن جميع الكابلات متصلة بشكل صحيح وليست تالفة.
- **لو الاتصال لاسلكي:** تأكد من قوة الإشارة ومن أنك متصل بالشبكة الصحيحة.

3. اختبار الاتصال (Ping Test)

ابدأ من الأقرب إلى الأبعد:

- فحص كرت الشبكة المحلي.
- فحص إعدادات الـ IP.
- فحص الاتصال بالراوتر.
- فحص الاتصال بالإنترنت.
- فحص (Domain Name System DNS) نظام أسماء النطاقات.
- تتبع المسار Traceroute إذا توقف المسار داخل الشبكة هذا يعني ان المشكلة داخلية. اما إذا توقف بعد الخروج من الشبكة فهذا يعني ان المشكلة من مزود خدمة الإنترنت (ISP).

ESRA QUBA

4. فحص جدار الحماية (Firewall) وسياسات الأمان

- تأكد أن الجدار الناري لا يمنع الوصول إلى الإنترنت.
- عطِّل جدار الحماية مؤقتًا لاختبار الاتصال.
- تحقق من اعدادات سياسات الوصول.
- افحص برامج الحماية (Antivirus) التي قد تعزل الشبكة.

5. جرّب الحلول السريعة

تهدف هذه الخطوات الى حل الأعطال البسيطة بسرعة قبل الدخول في فحوصات متقدمة (مثل traceroute أو تحليل الحزم) مثل:

- **إعادة تشغيل** الأجهزة أو تبديل الكابل.
- **تجديد عنوان** الـ IP (Renew IP).
- **مسح ذاكرة الـ DNS:** أحيانًا الجهاز يحتفظ بعنوان قديم لموقع، فيسبب خطأ في الاتصال.
- **تغيير كابل أو منفذ الشبكة** : أحيانًا العطل في الكابل نفسه أو في المنفذ (Port).
- **تعطيل وإعادة تفعيل كرت الشبكة**: تصلح أخطاء التهيئة البسيطة أو تعارض التعريفات.

6. توثيق النتائج (Documentation & Prevention)

بعد حل المشكلة، يجب توثيق العملية. يجب أن تشمل الوثائق:

- **وصف المشكلة**: ما هي المشكلة وكيف تم اكتشافها.
- **الخطوات المتبعة:** الخطوات التي تم اتخاذها لاستكشاف الأخطاء وإصلاحها.
- **ضع توصيات** لمنع تكرارها (تحديثات، صيانة دورية، مراقبة).

الخلاصة

استكشاف أخطاء الشبكة هو عملية منهجية تهدف إلى تحديد وحل المشكلات التي تؤثر على أداء الشبكة، من خلال اتباع خطوات محددة، مثل تحديد المشكلة، والتحقق من الأجهزة، واختبار الاتصال، يمكن تحسين كفاءة الشبكة وضمان استمرارية العمل. تعتبر هذه العملية ضرورية للحفاظ على أداء الشبكة بشكل مثالي، وتقليل فترات التوقف.

ESRA QUBA