معهد رسل الحضارة الدولي
للعلوم التقنية والفنية

معهد رسل الحضارة

قسم الحاسب الالي – الفصل الثاني

اساسيات الشبكات

CCNA-1

د. محمد عبدالرحمن

فصل الربيع 2025

المحاضرة الأولى

مقدمة عن شبكات الإنترنت

تُعد **شبكات الإنترنت (Internet Networks)** من أهم الإنجازات التقنية في العصر الحديث، حيث غيّرت بشكل جذري أسلوب تواصل البشر وتبادلهم للمعلومات. الإنترنت هي بنية تحتية عالمية تعتمد على **شبكات مترابطة** من الحواسيب والأجهزة الرقمية، تتيح للمستخدمين الوصول إلى مصادر معلوماتية وخدمية ضخمة، وتوفير وسائل تواصل تفاعلية في الزمن الحقيقي.

نشأت فكرة الإنترنت من مشروع **ARPANET** الذي أطلقته وزارة الدفاع الأمريكية في أواخر الستينيات بهدف إنشاء شبكة اتصال بين مراكز البحث العلمي، وقد تطورت لاحقًا لتشمل مختلف أنحاء العالم تحت ما يُعرف اليوم بـ **شبكة الإنترنت العالمية.(World Wide Web)**

مفهوم شبكة الإنترنت

يمكن تعريف الإنترنت بأنها:

"شبكة عالمية من الشبكات (A network of networks) تستخدم **بروتوكولات قياسية** لتبادل البيانات والمعلومات بين الأجهزة المرتبطة بها، أبرزها بروتوكولTCP/IP ".

تمثل الإنترنت البيئة الحاضنة للعديد من الخدمات مثل :**البريد الإلكتروني، تصفح الويب، خدمات السحابة، تطبيقات الوسائط المتعددة، التجارة الإلكترونية، والتعلم الإلكتروني.**

أهمية شبكات الإنترنت

- **الوصول إلى المعلومات** :تُعد مصدرًا مفتوحًا للمعلومات والمعرفة في مختلف المجالات.
- **التواصل الفوري** :تمكّن من التواصل بين الأفراد عبر البريد الإلكتروني، الرسائل الفورية، ومكالمات الفيديو.
- **التعليم والتدريب** :توفر بيئة تعليمية مفتوحة من خلال أنظمة التعليم الإلكتروني.(E-learning)
- **التجارة والخدمات** :تُستخدم في التسوق الإلكتروني، المعاملات المالية، والخدمات الحكومية الرقمية.
- **البحث العلمي** :تُسهم في نشر وتبادل الأبحاث العلمية والبيانات بين المؤسسات الأكاديمية حول العالم.

أنواع شبكات الإنترنت

يمكن تصنيف شبكات الإنترنت إلى أنواع متعددة حسب **النطاق الجغرافي، البنية التحتية، والغرض من الاستخدام** .ويُعد هذا التصنيف ضروريًا لفهم كيفية بناء الشبكات وتوزيع الموارد.

1-الشبكة المحلية(LAN - Local Area Network)

التعريف

هي شبكة تربط مجموعة من الأجهزة داخل **نطاق جغرافي محدود،** مثل مبنى أو مؤسسة.

الخصائص

- سرعة نقل بيانات عالية.
- تكلفة منخفضة نسبيًا.
- صيانة وإدارة مركزية.

الاستخدامات

- شبكات المكاتب والمختبرات الجامعية.

2-الشبكة الواسعة(WAN - Wide Area Network)

التعريف

شبكة تغطي **نطاقًا جغرافيًا كبيرًا** كمدينة أو دولة أو حتى عدة قارات، وتربط شبكات محلية متعددة.

الخصائص

- تعتمد غالبًا على مزودي خدمة الإنترنت.(ISPs)
- تكلفة تشغيل أعلى.
- سرعة أقل من LAN في العادة.

مثال بارز

الإنترنت نفسه يُعد أكبر شبكة.WAN

3-الشبكة المدنية(MAN - Metropolitan Area Network)

التعريف

شبكة تغطي منطقة جغرافية متوسطة مثل **مدينة أو حرم جامعي،** وتوفر اتصالًا أسرع من.WAN

الاستخدامات

- شبكات المؤسسات الكبيرة والجامعات.
- شبكات المدن الذكية.(Smart Cities)

4-الشبكات اللاسلكية(Wireless Networks)

الأنواع الفرعية

- **WLAN**مثل :Wi-Fi داخل المنازل والمكاتب.
- **WWAN**مثل شبكات الجيل الرابع والخامس G/5G4 :على مستوى المناطق والمدن.
- **WPAN**مثل :Bluetooth لمسافات قصيرة بين الأجهزة.

الخصائص

- مرونة وسهولة في التثبيت.
- مناسبة للأجهزة المحمولة.

5-الشبكة الشخصية(PAN - Personal Area Network)

التعريف

شبكة صغيرة جدًا تربط أجهزة شخصية مثل الهاتف الذكي، الحاسوب المحمول، وسماعات الرأس.

المسافة

عادة لا تتجاوز 10 أمتار.

6-شبكات الحوسبة السحابية(Cloud Networks)

التعريف

شبكات تعتمد على البنية التحتية الافتراضية للوصول إلى موارد الحوسبة عبر الإنترنت.

المزايا

- مرونة في الوصول.
- توسع سهل.

استخدامات شبكات الإنترنت

أحدثت شبكات الإنترنت ثورة في مجالات متعددة من الحياة اليومية والعملية، إذ أصبحت تمثل العمود الفقري للتواصل، التعليم، الأعمال، والترفيه. ويمكن تصنيف استخدامات الإنترنت في عدة مجالات رئيسية كما يلي:

1- الاتصالات(Communication)

يُعد التواصل من أبرز استخدامات الإنترنت، حيث تُمكِّن الأفراد من التواصل الفوري عبر:

- البريد الإلكتروني(Email)

- المحادثات النصية والصوتية(Chats & VoIP)
- المؤتمرات المرئية(Video Conferencing)
- شبكات التواصل الاجتماعي(Social Media)

مثلZoom :، WhatsApp، Microsoft Teams، Gmail، Facebook.

2- التعليم والتعلم الإلكتروني(E-Learning)

ساهم الإنترنت في تطوير منظومات التعليم من خلال:

- التعليم عن بعد عبر منصات مثلCoursera :، Udemy، Moodle.
- المكتبات الرقمية والكتب الإلكترونية.
- الصفوف الافتراضية وتبادل المحتوى الأكاديمي بين الجامعات.
- الاختبارات والتقييمات الإلكترونية.

3-الخدمات المصرفية والمالية(E-Banking & E-Commerce)

يُمكّن الإنترنت من:

- الوصول إلى الحسابات البنكية وتنفيذ المعاملات المالية.
- التسوق الإلكتروني ودفع الفواتير.
- التداول عبر الإنترنت.(Online Trading)

مثلPayPal :، Amazon، تطبيقات البنوك.

4- الوصول إلى المعلومات والمعرفة(Information Access)

يوفر الإنترنت قاعدة بيانات ضخمة تشمل:

- الأخبار والمقالات والأبحاث العلمية.
- المنتديات العلمية والمدونات المتخصصة.
- الموسوعات مثلWikipedia.

5- إدارة الأعمال والعمل عن بُعد(Business & Remote Work)

- منصات التعاون بين فرق العمل مثلTrello ، Slack.
- الوصول إلى الأنظمة المؤسسية من أي مكان.
- خدمات الحوسبة السحابية (Cloud Services) مثل Google Workspace وMicrosoft Azure.

6-الترفيه والإعلام(Entertainment & Media)

- بث الفيديو والصوت (Streaming) مثل Netflix وSpotify.
- الألعاب الإلكترونية الجماعية.
- مشاهدة الأخبار والبرامج التلفزيونية.
- التدوين والبودكاست.

7- الصحة الرقمية(E-Health & Telemedicine)

- حجز المواعيد الطبية إلكترونيًا.
- الاستشارات الطبية عبر الإنترنت.
- الوصول إلى السجلات الطبية الرقمية.

8-الخدمات الحكومية الإلكترونية(E-Government)

- تقديم الخدمات للمواطنين عبر بوابات إلكترونية.
- التقديم للوثائق الرسمية ودفع الرسوم الحكومية.
- التصويت الإلكتروني في بعض الدول.

التحديات التي تواجه شبكات الإنترنت

على الرغم من التطور الكبير في تقنيات الإنترنت، فإن هناك العديد من التحديات التي تؤثر على كفاءتها وأدائها. تتنوع هذه التحديات بين قضايا فنية، وأمنية، وتنظيمية. في ما يلي أبرز التحديات التي تواجه شبكات الإنترنت:

1- أمن البيانات والخصوصية(Data Security and Privacy)

- **التهديدات الأمنية** :تتعرض شبكات الإنترنت للعديد من الهجمات مثل الفيروسات، والبرمجيات الخبيثة، والهجمات الإلكترونية مثل **DDoS**.
- **الخصوصية** :مع زيادة مشاركة البيانات الشخصية على الإنترنت، تُصبح حماية المعلومات الشخصية تحديًا رئيسيًا، خاصة مع تزايد قضايا سرقة الهوية.

مثال :اختراق بيانات المستخدمين على منصات التواصل الاجتماعي أو التسوق الإلكتروني.

2- توافر الشبكة وسرعة الاتصال(Network Availability and Speed)

- **التأخير وزمن الاستجابة :**قد تواجه بعض الشبكات تحديات في الحفاظ على زمن استجابة منخفض في الخدمات مثل البث المباشر أو التطبيقات التي تعتمد على الاتصال الفوري.
- **الازدحام الشبكي(Network Congestion)** :يحدث عندما تتجاوز حركة البيانات القدرة الاستيعابية للشبكة، مما يؤدي إلى انخفاض الأداء وزيادة التأخير.

3- التنظيم الحكومي والسياسات(Regulation and Policy)

- **الرقابة على الإنترنت** :تواجه بعض الدول تحديات تنظيمية تتعلق بالرقابة على المحتوى الذي يتم تداوله عبر الإنترنت، مما يحد من حرية الوصول إلى المعلومات.
- **الاختلافات في التشريعات** :تختلف سياسات تنظيم الإنترنت من دولة إلى أخرى، مما يخلق تحديات في التعاون بين الدول في معالجة المشاكل العابرة للحدود مثل الجرائم الإلكترونية

.

4- الهجمات الإلكترونية(Cyber Attacks)

- **هجمات :(DDoS (Distributed Denial of Service** تُعد من أبرز التهديدات التي تُعرقل عمل الإنترنت عن طريق إغراق المواقع الإلكترونية بحركة مرور ضارة.
- **الهجمات على البنية التحتية الحيوية** :مثل الهجمات التي تستهدف أنظمة الطاقة أو شبكات النقل المرتبطة بالإنترنت.

5- فجوة الوصول إلى الإنترنت(Digital Divide)

- **التفاوت في الوصول** :على الرغم من التقدم الكبير، إلا أن هناك تفاوتًا كبيرًا في **الوصول إلى الإنترنت** بين الدول المتقدمة والدول النامية.
- **البنية التحتية المحدودة** :بعض المناطق تفتقر إلى البنية التحتية اللازمة لتوفير خدمة الإنترنت بشكل مستدام.

مثال :في بعض المناطق الريفية أو النائية، تكون سرعة الاتصال بالإنترنت ضعيفة أو غير متوفرة.

6-استدامة الطاقة(Energy Sustainability)

- **استهلاك الطاقة** :تُعتبر شبكات الإنترنت، وخاصة مراكز البيانات، من أكبر مستهلكي الطاقة. وبحث كيفية تقليل هذا الاستهلاك أصبح تحديًا بيئيًا.
- **الاعتماد على مصادر الطاقة المتجددة** :يتزايد الضغط على الشركات لتحويل مراكز البيانات إلى مصادر طاقة نظيفة.

7- التطور التكنولوجي السريع(Rapid Technological Evolution)

- **التكيف مع التقنيات الحديثة** :يفرض تطور تقنيات الإنترنت مثل **5G**و**الذكاء الاصطناعي** تحديات على شبكات الإنترنت في كيفية التكيف والتطوير بشكل مستمر لتلبية متطلبات الأجيال الجديدة من التطبيقات.

الاسئلة الاسترشادية

1- اذكر ثلاثة من أنواع شبكات الانترنت
2- اذكر ثلاثة من استخدامات شبكات الانترنت
3- اذكر ثلاثة من التحديات التي تواجه شبكات الانترنت
4- اذكر خصائص الشبكات المحلية LAN
5- اذكر خصائص الشبكات الواسعة WAN
6- اذكر مزايا شبكات الحوسبة السحابية

المحاضرة الثانية

أساس فكرة الاتصال بالشبكة وتعريف كل من البروتوكولات في الشبكة

أساس فكرة الاتصال بالإنترنت عبر الشبكة

تُعد شبكة الإنترنت من أعظم الابتكارات التقنية في القرن العشرين، وقد أسهمت في إحداث ثورة في مجالات التواصل، المعلومات، والتعليم، وغيرها. وتقوم فكرة الاتصال بالإنترنت على بنية معقدة من الشبكات المرتبطة ببعضها البعض، وهي تعمل وفق مجموعة من البروتوكولات والمعايير التقنية التي تنظم كيفية إرسال واستقبال البيانات.

1- المفهوم العام للشبكة

الشبكة في السياق التقني تشير إلى مجموعة من الأجهزة المتصلة ببعضها لتبادل البيانات. ويمكن أن تكون هذه الشبكات محلية (LAN)تغطي مساحة صغيرة مثل مبنى، أو واسعة (WAN) مثل الإنترنت التي تربط العالم أجمع. والإنترنت هي شبكة شبكات، أي أنها تتكون من عدد ضخم من الشبكات المتصلة ببعضها، والتي تتواصل فيما بينها باستخدام بروتوكولات موحدة.

2-البروتوكولات كأساس للاتصال

يعتمد الاتصال بالإنترنت على حزمة بروتوكولات تُعرف باسم **TCP/IP** (Transmission Control Protocol/Internet Protocol). هذه الحزمة تتيح تقسيم البيانات إلى حزم صغيرة، ثم إرسالها عبر الشبكة وإعادة تجميعها عند الوصول. يعمل بروتوكول الإنترنت (IP) على تحديد العناوين التي توجه الحزم إلى وجهتها الصحيحة، بينما يضمن بروتوكول التحكم في الإرسال (TCP) أن تصل البيانات بشكل كامل ودقيق.

3-مزودو خدمة الإنترنت والبنية التحتية

الاتصال بالإنترنت لا يتم مباشرة بين المستخدم وبقية العالم، بل يمر عبر ما يُعرف بـ "مزودي خدمة الإنترنت (ISPs)." يقوم هؤلاء المزودون بتوفير نقطة الدخول إلى الإنترنت عبر البنية التحتية كالكابلات الضوئية أو الأقمار الصناعية أو شبكات الهاتف المحمول. ويتصل المستخدم بالمزود من خلال جهاز المودم، الذي يحول الإشارة الرقمية إلى إشارات يمكن نقلها عبر وسائل الاتصال المختلفة.

4-نظام أسماء النطاقات(DNS)

نظرًا لأن عناوين الإنترنت عبارة عن أرقام(IP Addresses) ، فقد تم تطوير **نظام أسماء النطاقات (DNS)** ليسهل على المستخدمين الوصول إلى المواقع باستخدام أسماء سهلة التذكر مثل www.example.com. يقوم DNS بترجمة هذه الأسماء إلى عناوين IP التي يمكن للحواسيب فهمها.

5-تطور البنية التحتية للاتصال

تطورت تقنيات الاتصال بالإنترنت من الاتصال عبر الهاتف (Dial-up) إلى النطاق العريض(Broadband) ، ثم إلى الألياف البصرية، وأخيرًا إلى الشبكات اللاسلكية وتقنية الجيل الخامس (5G). وقد ساهم هذا التطور في زيادة سرعة وكفاءة الاتصال، مما مكّن من تقديم خدمات جديدة كالبث المباشر، والحوسبة السحابية، والتفاعل الآني.

الاتصال بالإنترنت عبر الشبكة يعتمد على بنية تقنية متكاملة تضم الشبكات، والبروتوكولات، والبنية التحتية، وأنظمة التوجيه. وتكمن عظمة الإنترنت في مرونتها وقدرتها على النمو والتطور، مما يجعلها عنصرًا محوريًا في العالم المعاصر.

بروتوكولات الإنترنت

تلعب البروتوكولات دورًا أساسيًا في عمل الإنترنت، فهي بمثابة "لغة التواصل" التي تتيح للأجهزة المختلفة حول العالم تبادل البيانات والتفاهم بطريقة منظمة وآمنة. من دون البروتوكولات، لا يمكن أن يتم أي نوع من الاتصال أو نقل البيانات عبر الشبكات، سواء كانت محلية أو عالمية مثل الإنترنت.

مفهوم البروتوكول

البروتوكول هو مجموعة من القواعد والتعليمات التي تُحدد كيفية تبادل البيانات بين طرفين. في عالم الشبكات، تُنظم البروتوكولات عمليات الاتصال، بدءًا من إرسال حزم البيانات، مرورًا بتوجيهها، وانتهاءً بتجميعها وفهمها عند الطرف المستقبل.

بروتوكول الإنترنت(IP)

عد بروتوكول الإنترنت (IP) حجر الزاوية في بنية الإنترنت الحديثة، وهو أحد المكونات الأساسية لحزمة بروتوكولات TCP/IP، التي تُشكل الأساس لجميع الاتصالات الشبكية. تم تصميم IP ليُمكّن من توجيه ونقل البيانات عبر شبكات مترابطة ومتعددة، مما يسمح للأجهزة المختلفة بالتواصل باستخدام عناوين فريدة.

تعريف بروتوكول الإنترنت

بروتوكول الإنترنت هو **بروتوكول تشغيلي من الطبقة الثالثة (طبقة الشبكة)** في نموذجOSI ، ووظيفته الأساسية هي **تحديد وتوجيه الحزم (Packets) من المصدر إلى الوجهة** باستخدام عنوان .IP يعمل IP بطريقة لا تتطلب اتصالًا دائمًا بين الطرفين(Connectionless) ، أي أن كل حزمة تُنقل بشكل مستقل عن غيرها، وقد تسلك طرقًا مختلفة قبل أن تصل إلى نفس الوجهة.

وظائف بروتوكولIP

1. **العنونة(Addressing) :**
يُوفر IP آلية لتمييز كل جهاز على الشبكة عبر عنوان IP فريد.
2. **تجزئة الحزم(Fragmentation) :**
عندما تكون الحزمة أكبر من الحد الأقصى لنقل البيانات في شبكة معينة، يقوم IP بتقسيمها إلى أجزاء أصغر.
3. **التوجيه(Routing) :**
يضمن IP أن تصل الحزم إلى وجهتها النهائية، حتى عبر شبكات متعددة باستخدام أجهزة التوجيه.(Routers)
4. **عدم الاعتماد على الاتصال(Connectionless) :**
لا يُنشئ IP قناة اتصال ثابتة بين المصدر والوجهة؛ بل تُرسل الحزم دون التأكد من تسليمها، وتُترك مسؤولية التأكد لبروتوكولات النقل مثل.TCP

إصدارات بروتوكولIP

الإصدار الرابع IPv4

- أُطلق في الثمانينات، ويستخدم عناوين بطول 32 بت.
- يمكن أن يُولّد ما يقارب **4.3مليار عنوان فريد.**
- يُكتب بصيغة **أربعة أرقام مفصولة بنقاط**)مثل: 192.168.1.1.(

- بسبب النمو السريع في عدد الأجهزة المتصلة، بدأت تظهر **مشكلة نفاد العناوين**.

الإصدار السادس IPv6

- تم تطويره لمعالجة قيودIPv4 ، ويستخدم عناوين بطول **128بت**.
- يمكنه توفير عدد غير محدود تقريبًا من العناوين.(2^128)
- يُكتب بصيغة **ثماني مجموعات من الأرقام الست عشرية**)مثل: db8:85a3:0000:0000:8a2e:0370:7334).2001:0
- يتضمن مزايا متقدمة مثل:
  - دعم أفضل للجودة والخدمات.(QoS)
  - تحسينات في الأمان من خلال.IPSec
  - تقليل الحاجة إلى الترجمة بين الشبكات.(NAT)

أهمية IP في بيئة الإنترنت

كل تواصل يتم عبر الإنترنت، من تصفح الويب إلى إرسال بريد إلكتروني، يعتمد على عناوين IP لتحديد هوية الأجهزة. تعمل أجهزة التوجيه في الشبكات العالمية على استخدام عناوين IP لتحديد المسارات المناسبة التي تسلكها الحزم حتى تصل إلى وجهتها، بغض النظر عن بعدها أو تعقيد الطريق.

تحديات بروتوكولIP

- في حالة **IPv4**، لا تزال شبكات كثيرة تعتمد على أساليب مثل **NAT**(ترجمة عناوين الشبكة) لتجاوز محدودية العناوين.
- تحتاج **الترقية إلى IPv6** إلى تحديثات في البنية التحتية، وهو ما يجعل عملية الانتقال بطيئة رغم أهميتها.

بروتوكول الإنترنت (IP) ليس مجرد آلية لنقل البيانات، بل هو البنية الأساسية التي تقوم عليها الإنترنت الحديثة. وبينما ما يزال IPv4 هو المسيطر في الاستخدام، فإن IPv6 يمثل المستقبل الذي سيُمكّن من توسيع الإنترنت بما يتناسب مع النمو المتسارع في عدد الأجهزة الذكية والخدمات السحابية.

بروتوكول التحكم في الإرسال(TCP)

يُعد **بروتوكول التحكم في الإرسال (TCP)** أحد البروتوكولات الأساسية في حزمة بروتوكولات الإنترنت(TCP/IP) ، وهو المسؤول عن ضمان نقل البيانات **بشكل موثوق ومنظم** بين الأجهزة عبر الشبكة. وعلى عكس بروتوكول الإنترنت (IP) الذي لا يضمن تسليم البيانات، يقوم TCP بتوفير اتصال موثوق من الطرف إلى الطرف (End-to-End) من خلال آليات متقدمة للتحقق من الاستلام وتصحيح الأخطاء.

تعريف بروتوكولTCP

TCPهو **بروتوكول من طبقة النقل** (Transport Layer)في نموذج الشبكات، وهو يعمل مباشرة فوق بروتوكول الإنترنت (IP).يتمثل دوره الرئيسي في **إدارة الاتصال بين التطبيقات** على طرفي الاتصال وضمان تسليم البيانات بشكل صحيح، بدون تكرار أو فقد.

أهم وظائفTCP

1. **إقامة الاتصال(Connection Establishment) :**
يستخدم TCP عملية تعرف بـ "المصافحة الثلاثية (Three-Way Handshake) "لبدء الاتصال بين الطرفين:
   - الجهاز الأول يرسل طلب الاتصال.(SYN)
   - الجهاز الثاني يرد بموافقة.(SYN-ACK)
   - الجهاز الأول يؤكد.(ACK)
2. **تقسيم البيانات وإعادة تجميعها(Segmentation and Reassembly) :**
يُجزئ TCP البيانات إلى مقاطع (Segments) ويُرقمها، بحيث يتمكن الطرف المستقبل من إعادة تجميعها بالترتيب الصحيح.
3. **التحكم في التدفق(Flow Control) :**
يُحدد TCP كمية البيانات التي يمكن للطرف المستقبل التعامل معها، من خلال ما يُعرف بـ "نافذة الاستقبال " (Receive Window).
4. **التحكم في الازدحام(Congestion Control) :**
يتحكم TCP في كمية البيانات المرسلة لتقليل فقدان الحزم عند ازدحام الشبكة، باستخدام خوارزميات مثل **Slow Start**و**Congestion Avoidance**.
5. **التحقق من صحة البيانات(Error Checking) :**
يُضمّن TCP في كل مقطع بيانات رمز تحقق (Checksum) لرصد الأخطاء، ويُعيد إرسال الحزم التالفة أو المفقودة.

مزايا بروتوكولTCP

- **موثوقية عالية** في نقل البيانات.
- يضمن **الترتيب الصحيح** للحزم.
- يقدم **إرسالًا مؤكدًا** مع إمكانية إعادة الإرسال.
- يدعم تطبيقات تحتاج إلى اتصال مستقر مثل:
  - **تصفح الويب(HTTP/HTTPS)**
  - **نقل الملفات(FTP)**
  - **البريد الإلكتروني(SMTP, IMAP)**

مقارنة بين TCP وUDP

المعيار	TCP	UDP
نوع الاتصال	موثوق (اتصال مُنشأ)	غير موثوق (بدون اتصال)
الترتيب	يضمن الترتيب	لا يضمن الترتيب
إعادة الإرسال	نعم	لا
السرعة	أبطأ بسبب الإجراءات الأمنية	أسرع
الاستخدام	تطبيقات تحتاج دقة	تطبيقات تحتاج سرعة

تحدياتTCP

- **زمن الاستجابة الطويل** في بعض الحالات، خاصة مع الشبكات ذات الكمون العالي.
- **الاستهلاك الزائد للموارد** مقارنة بـUDP ، بسبب التحقق المستمر من تسليم البيانات.
- لا يُناسب **التطبيقات التي تتحمل فقدان بعض البيانات،** مثل الفيديو المباشر أو الألعاب.

يمثل بروتوكول TCP أحد العناصر الجوهرية في بنية الإنترنت، حيث يوفر وسيلة مضمونة وفعالة لنقل البيانات بين الأجهزة. ورغم وجود بروتوكولات أسرع مثلUDP ، إلا أن TCP يظل الخيار الأفضل عندما تكون **الموثوقية وسلامة البيانات** هما الأولوية.

بروتوكولات أخرى مهمة

1. **UDP (User Datagram Protocol)**
بروتوكول سريع ولكن غير موثوق، لا يتحقق من تسليم الحزم. يُستخدم في تطبيقات تتطلب السرعة مثل البث الحي والألعاب.

ما هو بروتوكولUDP ؟

- يُعرف بـUser Datagram Protocol
- أحد بروتوكولات طبقة النقل في نموذجTCP/IP
- يُستخدم لنقل البيانات بسرعة دون الحاجة إلى إنشاء اتصال مسبق

خصائصUDP

- بروتوكول غير موثوق(No reliability)
- لا يُعيد إرسال الحزم المفقودة
- لا يضمن ترتيب وصول الحزم
- لا يعتمد على المصافحة الثلاثية(Three-Way Handshake)

مكونات رأس حزمةUDP

- رقم منفذ المصدر
- رقم منفذ الوجهة
- طول الحزمة
- رمز التحقق(Checksum)

مميزاتUDP

- سرعة عالية في نقل البيانات
- تقليل زمن التأخير(Low Latency)
- خفيف الوزن من حيث الحمل على الشبكة
- مناسب لتطبيقات الوقت الحقيقي

عيوبUDP

- لا يضمن تسليم البيانات
- عرضة لفقدان أو تكرار الحزم
- لا يحتوي على آليات للتحكم في التدفق أو الازدحام

استخداماتUDP

- بث الفيديو والصوت المباشر) مثل VoIP و(IPTV
- الألعاب عبر الإنترنت
- استعلامات نظام أسماء النطاقات(DNS)
- بروتوكولات بث الوقت مثلNTP

مقارنة سريعة معTCP

الخاصية	UDP	TCP
موثوقية البيانات	غير مضمونة	مضمونة
الترتيب	غير مضمون	مضمون
السرعة	عالية	أبطأ نسبياً
الاستخدامات	بث مباشر، ألعاب	تصفح، بريد، تحميل ملفات

2. **HTTP/HTTPS (HyperText Transfer Protocol / Secure)**
تُستخدم لنقل صفحات الويب HTTPS .هو النسخة المؤمنة منHTTP ، ويستخدم بروتوكولات التشفير لحماية البيانات.

ما هوHTTP/HTTPS ؟

- **HTTP** :بروتوكول نقل النصوص التشعبية
- **HTTPS** :نسخة آمنة من(HTTP (HyperText Transfer Protocol Secure
- يُستخدمان لنقل البيانات عبر الإنترنت بين المتصفح والخادم(server)
- يعملان في طبقة التطبيق (Application Layer) في نموذجTCP/IP

خصائصHTTP

- يعتمد على الاتصال غير المشفر(Unencrypted)
- لا يضمن أمان البيانات أثناء النقل
- يعمل عبر المنفذ 80 في الشبكة
- يتم استخدامه في معظم مواقع الإنترنت غير الحساسة

خصائصHTTPS

- يعتمد على الاتصال المشفر باستخدامSSL/TLS
- يضمن أمان البيانات وحمايتها أثناء النقل

- يعمل عبر المنفذ 443 في الشبكة
- يُستخدم في المواقع التي تتطلب أمانًا عاليًا مثل البنوك والمتاجر الإلكترونية

مميزاتHTTP

- بسيط وسريع في نقل البيانات
- سهل الاستخدام في المواقع التي لا تتطلب أمانًا عاليًا
- لا يتطلب موارد إضافية للتشفير
- يستخدم على نطاق واسع في الإنترنت

مميزاتHTTPS

- تشفير البيانات لضمان سرية المعلومات أثناء النقل
- مصادقة الخادم لضمان أنه الموقع الصحيح
- حماية ضد الهجمات مثل"Man-in-the-Middle"
- يُستخدم في المواقع التي تتطلب تأكيد هوية المستخدم مثل المواقع البنكية والتجارة الإلكترونية

الفرق بين HTTP وHTTPS

الخاصية	HTTP	HTTPS
الأمان	غير مشفر	مشفر باستخدامSSL/TLS
المنفذ	80	443
الاستخدام	مواقع غير حساسة	مواقع حساسة مثل الإنترنت المصرفي
حماية البيانات	لا يوجد	مشفر

استخداماتHTTP/HTTPS

- **HTTP** :مواقع الإنترنت العامة، المدونات، المقالات
- **HTTPS** :الدفع الإلكتروني، تسجيل الدخول، البيانات الحساسة

3. **FTP (File Transfer Protocol)**
يُستخدم لنقل الملفات بين الأجهزة عبر الإنترنت.

ما هوFTP ؟

- بروتوكول نقل الملفات(File Transfer Protocol)
- يُستخدم لنقل الملفات بين الحواسيب عبر شبكة الإنترنت
- يعمل في طبقة التطبيق (Application Layer) في نموذجTCP/IP
- يعتمد على بروتوكول TCP لضمان موثوقية الاتصال
- يستخدم منفذي الاتصال: 21 للأوامر و20 لنقل البيانات

خصائصFTP

- يستخدم نموذج "العميل – الخادم(Client-Server Model) "

- يسمح برفع الملفات إلى الخادم أو تحميلها منه
- يدعم أوامر متعددة مثل: تحميل، حذف، إعادة تسمية، إنشاء مجلدات
- يتطلب عادةً اسم مستخدم وكلمة مرور للاتصال بالخادم

مميزاتFTP

- إمكانية نقل ملفات كبيرة بسهولة
- يدعم استئناف عمليات التحميل/الرفع إذا توقفت
- متوافق مع أنظمة تشغيل متعددة
- يدعم نقل ملفات متعددة في جلسة واحدة

عيوبFTP

- لا يُوفر التشفير بشكل افتراضي (الاتصال غير آمن)
- بيانات الدخول وكلمات المرور تُرسل كنصوص صريحة
- عرضة لهجمات التنصت والاختراق) مثل "Sniffing" و("Brute Force"
- يحتاج إلى فتح منافذ متعددة في جدران الحماية

استخداماتFTP

- إدارة ملفات المواقع الإلكترونية (رفع ملفات إلى الخادم)
- مشاركة الملفات بين المؤسسات
- نسخ الملفات احتياطيًا بين أجهزة خوادم
- تبادل الملفات في شبكات داخلية أو بين مراكز بيانات

4. **DNS (Domain Name System)**
يُحول أسماء النطاقات) مثل (google.com إلى عناوين IP يمكن للأجهزة فهمها.

ما هوDNS ؟

- نظام أسماء النطاقات(Domain Name System)
- يُحوّل أسماء النطاقات القابلة للقراءة) مثل (google.com إلى عناوين IP رقمية (مثل 142.250.190.14)
- يعمل في طبقة التطبيق ضمن نموذجTCP/IP
- يُعد "دفتر الهاتف" للإنترنت

كيف يعملDNS ؟

1. يُدخل المستخدم اسم الموقع في المتصفح
2. يرسل المتصفح طلبًا إلى خادم DNS للاستعلام عن عنوانIP
3. يُعيد خادم DNS العنوان الرقمي المرتبط بالنطاق
4. يتم الاتصال بالخادم المستهدف باستخدام عنوانIP

مكونات نظامDNS

- **المُستخدم(Client)** :عادةً متصفح الويب
- **المُحلل المحلي(DNS Resolver)** :يطلب البيانات نيابةً عن العميل

- **خوادم الجذر(Root Servers)**: تُوجّه إلى خوادم المستوى الأعلى
- **خوادم المستوى الأعلى(TLD Servers)**: مثل .com و.org
- **خوادم الأسماء الموثوقة(Authoritative Servers)**: تُعطي العنوان النهائي للنطاق المطلوب

مميزاتDNS

- يُبسط استخدام الإنترنت بتوفير أسماء سهلة التذكّر
- يسرّع الاتصال عبر التخزين المؤقت
- يُمكن تحديث السجلات بسهولة دون تغيير إعدادات المستخدم
- يُستخدم على نطاق عالمي ويُدار بطريقة موزعة لضمان التوافر

عيوبDNS

- عرضة لهجمات مثل "DNS Spoofing" أو"Cache Poisoning"
- تأخير في التحديث بسبب التخزين المؤقت
- الحاجة إلى حماية الخوادم لضمان الموثوقية
- بدون تشفير افتراضي) إلا عند استخدام DNS over HTTPS أو(TLS

استخداماتDNS

- تصفح الإنترنت بسهولة عبر الأسماء
- توجيه البريد الإلكتروني
- استخدامات في الحوسبة السحابية وخدماتCDN
- البنية الأساسية لتطبيقات الإنترنت

5. **SMTP, POP, IMAP**

بروتوكولات تُستخدم في إرسال واستقبال البريد الإلكتروني.

ما هي بروتوكولات البريد الإلكتروني؟

بروتوكولات البريد الإلكتروني هي مجموعة من القواعد التي تُستخدم لإرسال واستقبال رسائل البريد عبر الإنترنت، وأهمها:

- **SMTP (Simple Mail Transfer Protocol)**: لإرسال الرسائل
- **POP (Post Office Protocol)**: لتنزيل الرسائل من الخادم إلى الجهاز
- **IMAP (Internet Message Access Protocol)**: **للوصول إلى الرسائل وإدارتها عن بُعد**

مقارنة بين SMTP و POPوIMAP

البروتوكول	الاستخدام الأساسي	الحذف من الخادم	مزامنة بين الأجهزة	المنفذ الافتراضي
SMTP	إرسال الرسائل فقط	لا ينطبق	لا ينطبق	25أو 587
POP3	استلام الرسائل (تحميلها)	نعم	لا	110أو 995
IMAP	استلام البريد (عن بُعد)	لا (إلا عند الحذف)	نعم	143أو 993

استخدامات شائعة

- **SMTP** :عند إرسال رسالة جديدة
- **POP** :للاستخدام الشخصي على جهاز واحد
- **IMAP** :للشركات أو الأفراد الذين يستخدمون عدة أجهزة (هاتف، كمبيوتر، تابلت)

طبقات النموذج المرجعي(TCP/IP Model)

تُقسم البروتوكولات حسب وظائفها ضمن نموذج TCP/IP إلى أربع طبقات رئيسية:

1. **طبقة الوصول إلى الشبكة(Network Access Layer)**
   تتعامل مع الوسائط الفيزيائية والاتصال المحلي.
2. **طبقة الإنترنت(Internet Layer)**
   تضم بروتوكول IP وتتحكم بتوجيه الحزم بين الشبكات.
3. **طبقة النقل(Transport Layer)**
   تشمل TCP وUDP، وتتحكم في تدفق البيانات بين التطبيقات.
4. **طبقة التطبيقات(Application Layer)**
   تضم البروتوكولات التي تتعامل مباشرة مع المستخدم مثل HTTP و FTPوDNS.

تمثل بروتوكولات الإنترنت العمود الفقري للاتصال الرقمي الحديث، فهي تُحدد كيفية تبادل البيانات بشكل موثوق وآمن. من خلال تنظيم الأدوار المختلفة عبر الطبقات المتعددة، تُمكّن هذه البروتوكولات من تحقيق تواصل فعال بين المليارات من الأجهزة على مستوى العالم.

الاسئلة الاسترشادية

1- اذكر ثلاثة من وظائف بروتوكول IP
2- اذكر ثلاثة من وظائف بروتوكول TCP
3- اذكر ثلاثة من مزايا بروتوكول TCP
4- اذكر ثلاثة من تحديات بروتوكول TCP
5- اذكر ثلاثة من خصائص بروتوكول UDP
6- اذكر ثلاثة من مزايا بروتوكول UDP
7- اذكر ثلاثة من عيوب بروتوكول UDP
8- اذكر ثلاثة من استخدامات بروتوكول UDP
9- اذكر ثلاثة من البروتوكولات التي تستخدم في البريد الالكتروني

المحاضرة الثالثة

نماذج الطبقية والعنونة في الشبكات

أولًا: مفهوم النماذج الطبقية في الشبكات

- تُستخدم النماذج الطبقية لتقسيم مهام الشبكة إلى طبقات منظمة، تُسهل التصميم، التطوير، والصيانة.
- كل طبقة تؤدي وظائف محددة وتتواصل مع الطبقات المجاورة لها فقط.

تحديات النماذج الطبقية في الشبكات

النماذج الطبقية، مثل **نموذج OSI (Open Systems Interconnection) ونموذجTCP/IP** ، تُستخدم لتنظيم عمل الشبكات وتقسيمها إلى طبقات وظيفية. هذه النماذج توفر فوائد كبيرة، مثل تبسيط التصميم، تعزيز التوافقية بين الأنظمة، ودعم الابتكار، لكنها تواجه مجموعة من التحديات عند التطبيق العملي.

أبرز التحديات المرتبطة بالنماذج الطبقية:

1. **الفجوة بين النظرية والتطبيق:**
   - نموذج OSI مثالي من الناحية النظرية، لكنه لا يُستخدم عمليًا كما هو.
   - نموذج TCP/IP هو المستخدم فعليًا، لكنه لا يتبع حدودًا واضحة لكل طبقة مثل نموذج.OSI
2. **عدم التوافق التام بين النماذج:**
   - الطبقات في نموذج OSI لا تتطابق دائمًا مع نظيرتها في نموذج.TCP/IP
   - على سبيل المثال: طبقتا "الجلسة" و"العرض" في OSI ليس لهما تمثيل واضح في.TCP/IP
3. **التعقيد في تنفيذ التفاعل بين الطبقات:**
   - رغم أن الطبقات مستقلة نظريًا، إلا أن بعض البروتوكولات تحتاج إلى معلومات من طبقات أخرى، مما يسبب "تداخلًا" يخلّ بمفهوم الفصل الطبقي.
4. **ضعف الأداء بسبب تعدد الطبقات:**
   - تمرير البيانات عبر عدة طبقات قد يزيد من زمن التأخير أو استهلاك الموارد، خاصة في الشبكات ذات الأداء الحرج.
5. **صعوبة التتبع والتحليل عند حدوث مشاكل:**
   - عند حدوث خلل في الشبكة، من الصعب أحيانًا تحديد الطبقة المسؤولة عن الخطأ بدقة بسبب التداخل والتعقيد.
6. **قيود الابتكار في بعض البروتوكولات:**
   - بعض الابتكارات تتطلب تجاوز حدود الطبقات(Cross-layer Design) ، وهو ما يتعارض مع التصميم الطبقي التقليدي.
7. **التكامل مع التقنيات الحديثة:**
   - مثل الحوسبة السحابية، إنترنت الأشياء، والشبكات المعرفة بالبرمجيات(SDN) ، التي قد تحتاج إلى تجاوز النماذج التقليدية أو تخصيصها.
8. **نقص الدعم الكامل لبعض البروتوكولات:**
   - ليست كل البروتوكولات تحقق الفصل المثالي بين الوظائف، مثل بروتوكول HTTP الذي يتعامل أحيانًا مع الجوانب الأمنية (TLS) أو التحكم في الجلسة.

ملخص التحديات حسب طبيعتها:

الوصف	نوع التحدي
عدم تطابق النماذج – تداخل الطبقات – تعقيد التفاعل	تنظيمي / هيكلي
ضعف الأداء – صعوبة التتبع – زيادة التعقيد في التطبيق	تقني
صعوبة إدخال تحسينات أو تصميمات جديدة تتجاوز الحدود التقليدية	ابتكاري
صعوبة التوافق بين أنظمة تستخدم نماذج أو بروتوكولات مختلفة	توافقية

ميزات وعيوب النماذج الطبقية في الشبكات

النماذج الطبقية، مثل نموذج **OSI**ونموذج **TCP/IP**، تُعد من الركائز الأساسية لفهم وتصميم شبكات الحاسوب. تعتمد هذه النماذج على تقسيم وظائف الشبكة إلى **طبقات مستقلة**، بحيث تؤدي كل طبقة وظيفة محددة وتتفاعل مع الطبقات الأخرى من خلال واجهات معيارية.

أولاً :ميزات النماذج الطبقية

1. **تبسيط التصميم والتطوير**
   - تقسيم الشبكة إلى طبقات يسهل عملية الفهم، والتصميم، والتطوير، حيث يمكن التركيز على كل طبقة بشكل مستقل.
2. **قابلية إعادة الاستخدام والتطوير**
   - يمكن تعديل أو ترقية طبقة معينة دون التأثير الكبير على باقي الطبقات (طالما تم الحفاظ على الواجهة).
3. **سهولة التعليم والتدريب**
   - النماذج الطبقية تُستخدم كأساس في المناهج الأكاديمية لتعليم الشبكات بطريقة منظمة ومترابطة.
4. **تعزيز التوافقية(Interoperability)**
   - يسهل التوافق بين معدات وبرمجيات مختلفة من مصنعين متعدّدين بفضل وجود معايير واضحة لكل طبقة.
5. **مرونة في الاختبار وحل المشكلات**
   - يسمح النموذج بعزل المشكلة في طبقة محددة لتبسيط عملية التشخيص والمعالجة.
6. **دعم الابتكار**
   - كل طبقة تُعتبر مساحة مستقلة للتطوير، مما يسمح بتطوير بروتوكولات وتقنيات جديدة دون التأثير على البنية العامة.

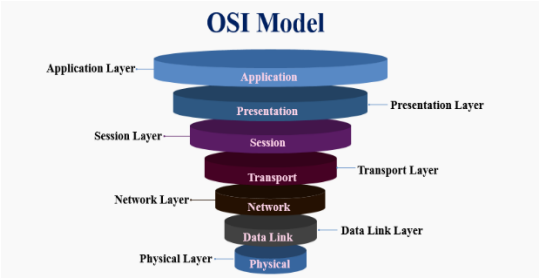
ثانيًا :عيوب النماذج الطبقية

1. **فصل غير واقعي بين الطبقات**
   - في التطبيق العملي، يحدث تداخل بين وظائف الطبقات، وقد تتبادل معلومات بشكل غير مباشر، مما يتعارض مع الفرضية النظرية للفصل التام.
2. **انخفاض الأداء أحيانًا**
   - بسبب مرور البيانات عبر عدة طبقات، يمكن أن تزداد التأخيرات أو يُستهلك قدر أكبر من الموارد (CPU, Memory).
3. **زيادة التعقيد**
   - التطبيق الصارم للنموذج الطبقي قد يؤدي إلى نظام أكثر تعقيدًا، خاصة عند محاولة تنفيذ طبقات لا تُستخدم فعليًا.
4. **ضعف المرونة في بعض السيناريوهات**
   - لا تتلاءم بعض التطبيقات الحديثة) مثل إنترنت الأشياء أو الشبكات المعرفة بالبرمجيات (SDN مع النموذج الطبقي التقليدي بسهولة.

5. **عدم تطابق بين النماذج النظرية والتطبيقات الفعلية**
   - نموذج OSI مثالي أكاديميًا، لكنه لم يُعتمد بالكامل عمليًا، بينما نموذج TCP/IP هو الأكثر استخدامًا، رغم أن بنيته غير مطابقة تمامًا للنموذج الطبقي.
6. **تقييد حرية التصميم**
   - الالتزام الصارم بالطبقات قد يمنع بعض الابتكارات، مثل استخدام معلومات من أكثر من طبقة لتحسين الأداء.(Cross-Layer Optimization)

أشهر النماذج الطبقية

1- نموذج(OSI (Open Systems Interconnection



- مكون من 7 طبقات:
  1. الطبقة الفيزيائية(Physical Layer)
  2. طبقة ربط البيانات(Data Link Layer)
  3. طبقة الشبكة(Network Layer)
  4. طبقة النقل(Transport Layer)
  5. طبقة الجلسة(Session Layer)
  6. طبقة العرض(Presentation Layer)
  7. طبقة التطبيق(Application Layer)
- يُستخدم كمرجع أكاديمي لفهم كيفية عمل الشبكات

2- نموذجTCP/IP

- يتكون من 4 طبقات أساسية:
  1. طبقة الوصول إلى الشبكة(Network Access Layer)
  2. طبقة الإنترنت(Internet Layer)
  3. طبقة النقل(Transport Layer)
  4. طبقة التطبيق(Application Layer)
- يُستخدم فعليًا في الإنترنت والشبكات الحديثة

مقارنة بين OSI وTCP/IP

نموذجTCP/IP	نموذجOSI	الطبقات
Application	Application	التطبيق
مدمجة مع التطبيق	Presentation + Session	العرض والجلسة
Transport	Transport	النقل
Internet	Network	الشبكة
Network Access	Data Link + Physical	ربط البيانات والفيزيائية

ثانيًا: نظام العنونة في الشبكات

- الهدف من العنونة هو تحديد الأجهزة داخل الشبكة وتمكين الاتصال بينها
- يتم استخدام أنواع مختلفة من العناوين في كل طبقة من طبقات الشبكة

أنواع العناوين في الشبكات

1. **العنوان الفيزيائي(MAC Address)**
   - يُستخدم في طبقة ربط البيانات
   - عنوان ثابت مرتبط ببطاقة الشبكة
   - يُكتب بصيغة00:1A:2B:3C:4D:5E :
2. **عنوان(IP (IP Address**
   - يُستخدم في طبقة الشبكة
   - نوعان IPv4 :(مثل 192.168.1.1) و) IPv6مثل 2001(1::db8:
   - يُستخدم لتوجيه الحزم عبر الإنترنت
3. **رقم المنفذ(Port Number)**
   - يُستخدم في طبقة النقل
   - يُحدد التطبيق أو الخدمة داخل الجهاز) مثل: 80 لـHTTP ، 443 لـ(HTTPS
4. **أسماء النطاقات(Domain Names)**
   - تُستخدم في طبقة التطبيق
   - أسماء سهلة التذكّر بدلاً من عناوين) IP مثل(google.com

علاقة العناوين بالطبقات

الوظيفة	الطبقة المستخدمة فيه	نوع العنوان
التوجيه داخل الشبكة المحلية	ربط البيانات(Data Link)	MAC Address
التوجيه بين الشبكات	الشبكة(Network)	IP Address
تحديد التطبيق المستقبل	النقل(Transport)	Port Number
تسمية سهل للموارد	التطبيق(Application)	Domain Name

الاسئلة الاسترشادية

1- اذكر ثلاثة من التحديات المرتبطة بالنماذج الطبقية
2- اذكر ثلاثة من مزايا النماذج الطبقية
3- اذكر ثلاثة من مزايا النماذج الطبقية
4- اذكر ثلاثة من طبقات نموذج OSI
5- اذكر ثلاثة من طبقات نموذج TCP\IP
6- اذكر ثلاثة من أنواع العناوين في الشبكات

المحاضرة الرابعة

نموذج(OSI (Open Systems Interconnection

نموذج **OSI**هو **نموذج مرجعي** يحدد كيف يتم إرسال البيانات عبر الشبكة من جهاز إلى جهاز آخر باستخدام سبع طبقات. تم تصميمه من قبل **المنظمة الدولية للتوحيد القياسي (ISO)** لتوفير إطار عمل يمكن من خلاله فهم وتنظيم عمليات الاتصال بين الأنظمة.

الطبقات التي يتكون منها نموذج OSI

1-الطبقة الفيزيائية(Physical Layer)

- **التعريف:**
  الطبقة الفيزيائية هي الطبقة الأولى في نموذجOSI ، وتُعنى بنقل البيانات على شكل إشارات كهربائية أو ضوئية أو موجات لاسلكية عبر الوسائط المادية.

المهام الرئيسية

- تحويل البيانات الرقمية إلى إشارات قابلة للإرسال عبر الوسيط المادي
- تحديد الخصائص الفيزيائية للوسيط (نوع الكابل، التردد، الطول الموجي)
- إدارة التوصيلات الفعلية بين الأجهزة (الموصلات، الفتحات، المقابس)
- تحديد معدل نقل البيانات (Data Rate) أو ما يُعرف بالـ"Bandwidth"
- التحكم في التزامن الزمني للإرسال والاستقبال(Synchronization)
- معالجة ترميز البيانات (Encoding) وتحويلها إلى شكل يمكن نقله

وسائط الإرسال(Transmission Media)

- **وسائط سلكية:**
  - كابلات نحاسية(Twisted Pair, Coaxial)
  - كابلات ألياف بصرية(Fiber Optic)
- **وسائط لاسلكية:**
  - موجات الراديو(Wi-Fi)
  - الأشعة تحت الحمراء
  - البلوتوث

الأجهزة المرتبطة بالطبقة الفيزيائية

- كابلات الشبكة
- محولات الإشارة(Modems)
- المكررات(Repeaters)
- محولات الألياف(Media Converters)
- بطاقات الشبكة (NICs) من جهة الواجهة الفيزيائية

خصائص الطبقة الفيزيائية

- لا تتعامل مع معنى البيانات أو محتواها

- لا تُجري أي نوع من التحقق أو التصحيح
- تُعد الأساس لجميع الطبقات العليا، إذ توفر وسيلة الاتصال المادي

2- طبقة ربط البيانات(Data Link Layer)

- **التعريف:**
الطبقة الثانية في نموذجOSI ، مسؤولة عن **نقل البيانات بشكل موثوق** عبر الوصلة الفيزيائية بين جهازين متصلين مباشرة.

المهام الرئيسية

- **تأطير البيانات(Framing) :**
تقسيم البيانات إلى إطارات (Frames) قابلة للإرسال
- **الكشف عن الأخطاء وتصحيحها:**
باستخدام تقنيات مثل - CRC) التحقق الدوري (لضمان سلامة البيانات
- **التحكم في التدفق(Flow Control) :**
تنظيم سرعة الإرسال لتجنب ازدحام المستقبل
- **التحكم في الوصول للوسط(MAC - Media Access Control) :**
إدارة كيفية وصول الأجهزة إلى الوسط المشترك في الشبكات المحلية

أنواع العناوين المستخدمة

- **عنوان(MAC (MAC Address :**
  - عنوان فيزيائي ثابت مكوّن من 48 بت
  - يُستخدم لتحديد الأجهزة داخل الشبكة المحلية
  - مكتوب بصيغة مثل00:1A:2B:3C:4D:5E :

التقسيم الفرعي للطبقة

- **التحكم في الوصول إلى الوسيط(MAC) :**
مسؤول عن تنظيم الوصول إلى الوسيط في شبكات مثل الإيثرنت والواي فاي
- **التحكم في المنطق الرابط(LLC - Logical Link Control) :**
مسؤول عن تأطير البيانات والتفاعل مع طبقة الشبكة

البروتوكولات والأمثلة

- Ethernet
- Wi-Fi (IEEE 802.11)
- PPP (Point-to-Point Protocol)
- HDLC (High-Level Data Link Control)

الأجهزة المرتبطة

- **المبدلات:(Switches)**
تعمل في طبقة ربط البيانات وتستخدم عنوان MAC لتوجيه الإطارات

خصائص الطبقة

- تنقل الإطارات داخل نفس الشبكة المحلية(LAN)
- لا تهتم بالتوجيه عبر شبكات مختلفة (هذه مهمة طبقة الشبكة)
- تعتبر "الوسيط" بين الطبقة الفيزيائية وطبقة الشبكة

3-طبقة الشبكة(Network Layer)

- **التعريف:**
الطبقة الثالثة في نموذجOSI ، مسؤولة عن **توجيه البيانات (Routing)** وتحديد المسار الأنسب لنقلها بين الشبكات المختلفة.

المهام الرئيسية

- **التوجيه:(Routing)**
اختيار أفضل مسار لإرسال الحزم من المصدر إلى الوجهة عبر شبكة الإنترنت
- **عنونة الأجهزة:(Logical Addressing)**
استخدام عناوين منطقية (IP addresses) لتحديد كل جهاز على الشبكة
- **تجزئة الحزم:(Packet Fragmentation)**
تقسيم الحزم الكبيرة لتتناسب مع قدرة الوسائط الناقلة
- **التغليف:(Encapsulation)**
تغليف البيانات داخل "حزم (Packets) "تحتوي على عنوان المرسل والمستقبل

العناوين المستخدمة

- **عنوان:(IP (IP Address**
  - يُستخدم لتحديد موقع الجهاز عبر الإنترنت
  - نوعان:
    - IPv4: مثل 192.168.1.1
    - IPv6: مثل db8::12001:
  - يتغير حسب موقع الجهاز في الشبكة، بخلاف عنوان MAC الثابت

البروتوكولات الأساسية

- **IP (Internet Protocol):**
  - أهم بروتوكول في هذه الطبقة، يُستخدم لتوجيه الحزم
  - نوعان IPv4 :وIPv6
- **ICMP (Internet Control Message Protocol):**
  - يُستخدم لإرسال رسائل التحكم مثل"Ping"
- **ARP (Address Resolution Protocol):**
  - يُستخدم لتحويل عنوان IP إلى عنوانMAC

الأجهزة المرتبطة

- **الموجهات:(Routers)**
  - تعمل في طبقة الشبكة

- تقوم بتحديد المسارات بين الشبكات المختلفة باستخدام جداول التوجيه

الفرق بين الطبقة الثانية والثالثة

طبقة الشبكة	طبقة ربط البيانات	المعيار
IPمنطقي	MACفيزيائي	نوع العنوان
بين شبكات مختلفة(WAN)	شبكة محلية(LAN)	مجال العمل
Router	Switch	الجهاز المسؤول

4- طبقة النقل(Transport Layer)

- **التعريف:**
الطبقة الرابعة في نموذجOSI ، مسؤولة عن **نقل البيانات بين التطبيقات على الأجهزة المختلفة** بشكل موثوق أو غير موثوق، حسب نوع البروتوكول.

المهام الرئيسية

- **التحكم في تدفق البيانات:(Flow Control)**
تنظيم معدل إرسال البيانات لضمان عدم فقدانها
- **التحكم في الأخطاء:(Error Control)**
التحقق من سلامة البيانات وإعادة الإرسال في حالة وجود أخطاء
- **التجزئة وإعادة التجميع:(Segmentation & Reassembly)**
تقسيم البيانات الكبيرة إلى أجزاء صغيرة ثم تجميعها عند المستقبل
- **إدارة الاتصالات:(Connection Management)**
إنشاء وإنهاء الاتصال بين التطبيقات (في البروتوكولات القائمة على الاتصال)

البروتوكولات الرئيسية

- **TCP (Transmission Control Protocol):**
  - بروتوكول موثوق
  - يعتمد على الاتصال(Connection-oriented)
  - يضمن تسليم البيانات بالترتيب وبدون فقدان
- **UDP (User Datagram Protocol):**
  - بروتوكول غير موثوق
  - بدون اتصال(Connectionless)
  - أسرع لكنه لا يضمن وصول البيانات أو ترتيبها

أرقام المنافذ(Port Numbers)

- تُستخدم لتحديد التطبيق أو الخدمة داخل الجهاز
- أمثلة:
  - Port 80: HTTP
  - Port 443: HTTPS
  - Port 25: SMTP

- Port 53: DNS
- Port 21: FTP

الأجهزة المرتبطة

- على الرغم من أن طبقة النقل تعمل على **البرمجيات(Software)** ، إلا أنها جزء أساسي في عملية الاتصال بين التطبيقات عبر الشبكة

الفرق بين TCP وUDP

المعيار	TCP	UDP
الاتصال	قائم على الاتصال	غير قائم على الاتصال
الموثوقية	موثوق، يضمن وصول البيانات	غير موثوق، لا يضمن الوصول
السرعة	أبطأ نسبيًا	أسرع
الاستخدام	تصفح الويب، البريد الإلكتروني	البث المباشر، الألعاب

5- طبقة الجلسة(Session Layer)

- **التعريف:**
الطبقة الخامسة في نموذجOSI ، مسؤولة عن **إدارة وتنظيم الجلسات (Sessions)** بين التطبيقات على الأجهزة المختلفة أثناء عملية الاتصال.

المهام الرئيسية

- **إنشاء الجلسة:(Session Establishment)**
بدء جلسة اتصال بين تطبيقين على أجهزة مختلفة
- **إدارة الجلسة:(Session Management)**
تنظيم عملية تبادل البيانات أثناء الجلسة وتحديد من يرسل ومتى
- **إنهاء الجلسة:(Session Termination)**
إنهاء الاتصال بطريقة سليمة بعد الانتهاء من تبادل البيانات
- **التزامن:(Synchronization)**
إضافة نقاط مرجعية (Checkpoints) في الاتصال الطويل لاستئناف النقل من آخر نقطة عند الانقطاع

الاستخدامات الشائعة

- تطبيقات بث الفيديو أو الصوت حيث يجب الحفاظ على تزامن البيانات
- خدمات قواعد البيانات التي تتطلب تتبع جلسات المستخدم
- مؤتمرات الفيديو والاتصال الهاتفي عبر الإنترنت(VoIP)

أمثلة على البروتوكولات

- NetBIOS (Network Basic Input Output System)
- RPC (Remote Procedure Call)
- SIP (Session Initiation Protocol) – يُستخدم لإنشاء الجلسات في تطبيقات VoIP

الفرق بين طبقة الجلسة والطبقات الأخرى

- **أعلى من طبقة النقل :** لا تهتم بنقل البيانات بل بتنظيمها
- **أقل من طبقة العرض :** لا تهتم بشكل البيانات بل بإدارة الجلسات فقط

الأجهزة المرتبطة

- هذه الطبقة تُدار بالكامل على مستوى البرمجيات (Software) ضمن أنظمة التشغيل أو التطبيقات

6- طبقة العرض(Presentation Layer)

- **التعريف:**
الطبقة السادسة في نموذج OSI ، مسؤولة عن **تهيئة وتنسيق البيانات** لتكون قابلة للفهم من قبل التطبيقات، سواء عند الإرسال أو الاستقبال.

المهام الرئيسية

- **تنسيق البيانات(Data Formatting) :**
تحويل البيانات إلى صيغة مشتركة بين المرسل والمستقبل (مثل تحويل الأرقام، النصوص، الصور)
- **الترميز وفك الترميز(Encoding/Decoding) :**
تحويل البيانات من شكل إلى آخر عند الإرسال، والعكس عند الاستقبال) مثل ASCII ، (Unicode
- **الضغط وفك الضغط(Compression/Decompression) :**
تقليل حجم البيانات لتسريع النقل واستعادتها لحجمها الأصلي عند الوصول
- **التشفير وفك التشفير(Encryption/Decryption) :**
حماية البيانات من خلال تشفيرها قبل النقل، وفك تشفيرها عند الاستلام

الاستخدامات الشائعة

- التعامل مع أنواع متعددة من تنسيقات الملفات) مثل .docx ، .pdf، .jpg، (.mp3
- تبادل البيانات بين أنظمة ذات صيغ مختلفة
- توفير الأمان في الاتصالات المشفرة مثل HTTPS

أمثلة على البروتوكولات والتقنيات

- SSL/TLS (Secure Sockets Layer / Transport Layer Security)
- MIME (Multipurpose Internet Mail Extensions)
- JPEG، MP3، GIF، MPEG كمثال على تنسيقات تحتاج معالجة على هذه الطبقة

الفرق بينها وبين الطبقات الأخرى

- **ليست مسؤولة عن إرسال أو استقبال البيانات فعليًا**
- تعمل كـ"مترجم" بين التطبيق والشبكة
- تسهّل التواصل بين أنظمة مختلفة من حيث البنية أو اللغة أو التنسيق

الأجهزة المرتبطة

- تُدار بالكامل من خلال **البرمجيات أو التطبيقات** مثل متصفحات الإنترنت، برامج التشفير، برامج الوسائط

7- طبقة التطبيقات(Application Layer)

- **التعريف:**
الطبقة السابعة والأخيرة في نموذجOSI ، وهي الطبقة التي يتفاعل فيها المستخدم مباشرة مع **التطبيقات** والشبكة، وتُسهم في توفير الخدمات الضرورية للتواصل عبر الشبكة.

المهام الرئيسية

- **توفير الخدمات للتطبيقات:**
تسهم في تمكين التطبيقات من استخدام الشبكة من خلال توفير البروتوكولات التي تُسهل الاتصال والتفاعل بين الأجهزة.
- **إدارة البيانات بين التطبيقات:**
مسؤولة عن إرسال واستقبال البيانات من التطبيقات إلى الطبقات السفلية في نموذج.OSI
- **التفاعل مع المستخدم النهائي:**
تُمثل الوسيلة التي يتفاعل من خلالها المستخدمون مع الشبكة عبر التطبيقات (مثل المتصفحات، البريد الإلكتروني، وغيرها).

البروتوكولات الأساسية

- **HTTP/HTTPS (HyperText Transfer Protocol / Secure):**
بروتوكولات تُستخدم لتصفح الإنترنت وتحميل صفحات الويب.
- **FTP (File Transfer Protocol):**
بروتوكول لنقل الملفات بين جهازين عبر الشبكة.
- **SMTP (Simple Mail Transfer Protocol):**
بروتوكول يُستخدم لإرسال البريد الإلكتروني.
- **IMAPو:POP3 (Internet Message Access Protocol & Post Office Protocol)**
بروتوكولات لقراءة البريد الإلكتروني واسترجاعه من الخوادم.
- **DNS (Domain Name System):**
بروتوكول لتحويل أسماء النطاقات (مثل www.example.com) إلى عناوين IP.

الاستخدامات الشائعة

- **تصفح الإنترنت:**
من خلال متصفحات الإنترنت باستخدام بروتوكولاتHTTP/HTTPS

- **إرسال واستقبال البريد الإلكتروني:**
عبر بروتوكولاتSMTP ، POP3، IMAP
- **نقل الملفات:**
باستخدام بروتوكول FTP لنقل البيانات بين الخوادم والأجهزة
- **التفاعل مع التطبيقات عبر الشبكة:**
مثل تطبيقات المحادثات عبر الإنترنت، الألعاب متعددة اللاعبين

الفرق بينها وبين الطبقات الأخرى

- **تتعامل مع التطبيقات مباشرة:**
فهي الطبقة الوحيدة التي تتفاعل مع المستخدمين أو التطبيقات نفسها
- **تستفيد من جميع الطبقات السفلية:**
تعتمد على الطبقات الأخرى مثل طبقة النقل والشبكة لتمكين الاتصال

الأجهزة المرتبطة

- **الخوادم:(Servers)**
توفر خدمات مختلفة مثل البريد الإلكتروني، استضافة المواقع، نقل الملفات، وما إلى ذلك
- **الأجهزة العميلة:(Clients)**
مثل أجهزة الكمبيوتر أو الهواتف الذكية التي تستخدم التطبيقات عبر الشبكة

ميزات وعيوب نموذجOSI

نموذج (Open Systems Interconnection) **OSI**هو نموذج مرجعي يُستخدم لفهم كيفية تفاعل أجهزة الكمبيوتر عبر الشبكات. كما هو الحال مع أي نموذج تقني، لنموذج OSI بعض **الميزات** و**العيوب** التي تؤثر على مدى فعاليته في التطبيقات العملية.

الميزات:

1. **التقسيم المنهجي:**
نموذج OSI يقسم عملية الاتصال بين الأجهزة إلى سبع طبقات، مما يجعل من السهل فهم وتنظيم عمليات الاتصال الشبكي. هذا **التقسيم** يعزز من **المرونة** و **التوسع** في تصميم الشبكات.
2. **تحقيق التوافق بين الأنظمة المختلفة:**
يساعد نموذج OSI في جعل الأجهزة والبرمجيات المختلفة من شركات مختلفة تتواصل مع بعضها، لأنه يوفر معايير واضحة للتفاعل بين الطبقات. هذا **يُسهل التفاعل بين الأنظمة** المتنوعة والمتعددة.
3. **المرونة في التعديل والتحديث:**
يمكن تعديل وتحسين الطبقات الفردية دون التأثير على الطبقات الأخرى. إذا تم تحسين إحدى الطبقات، لن يكون لذلك تأثير كبير على باقي النظام. هذه المرونة تسهل **التطوير المستمر** للشبكات.
4. **التفاعل بين الطبقات:**
كل طبقة في نموذج OSI تقدم خدمة للطبقة العليا منها، مما يجعل العملية سلسة ويضمن **التنظيم** و **الفعالية** في نقل البيانات بين الأجهزة.
5. **التوجيه والتخزين السهل للمعلومات:**
يوفر نموذج OSI **التوجيه** بين الطبقات ويتيح للمطورين فهماً أسهل لكيفية بناء أنظمة شبكية من خلال **المعمارية الهرمية** التي يعتمد عليها.

6. **دعم البرمجيات المتعددة:**
بفضل تقسيمه إلى طبقات، يمكن أن يعمل نموذج OSI مع مجموعة متنوعة من **البروتوكولات** التي تُستخدم في كل طبقة من الطبقات، مما يساهم في **التنوع** و **التوسعة**.

العيوب:

1. **التطبيقات العملية المحدودة:**
رغم أن نموذج OSI هو نموذج مرجعي ممتاز من حيث الفهم والتنظيم، إلا أنه في الواقع لا يُستخدم بشكل مباشر في كثير من الشبكات الحديثة. غالبًا ما يُستخدم **نموذج TCP/IP** بدلاً منه في تطبيقات الشبكات الحقيقية، خاصة في الإنترنت.
2. **تعقيد غير ضروري:**
نموذج OSI يحتوي على **سبع طبقات**، مما قد يكون **معقدًا** في بعض الحالات مقارنةً بنماذج أبسط مثل نموذج TCP/IPالذي يحتوي على **أربع طبقات** فقط. بعض الطبقات في OSI قد لا تكون ضرورية في بعض التطبيقات العملية.
3. **المواصفات الغامضة في بعض الطبقات:**
على الرغم من أن نموذج OSI يوفر تقسيمًا منطقيًا للطبقات، فإن بعض الطبقات (مثل طبقة الجلسة أو طبقة العرض) قد تكون **غامضة** في تطبيقها في بيئات شبكية حقيقية. بعض الطبقات قد تتداخل في عملها مع طبقات أخرى، مما يسبب **الارتباك** في التطبيق.
4. **التأخير في التصميم والتنفيذ:**
تطبيق نموذج OSI في **تصميم الشبكات** قد يتطلب الكثير من الوقت والجهد لتطوير كل طبقة بالشكل المثالي. كما أن تخصيص الموارد لكل طبقة قد يؤدي إلى **بطء** في الأداء أو **زيادة في التكلفة**.
5. **عدم وجود معايير عالمية محددة:**
رغم أن نموذج OSI يوفر **إطارًا مرجعيًا جيدًا**، إلا أنه لا يُحدد **بشكل دقيق** كيفية تنفيذ كل طبقة. هذا يترك المجال لبعض الاختلافات في التنفيذ بين الأنظمة المختلفة.
6. **قد لا يتناسب مع تطبيقات الشبكات الحديثة:**
بما أن النموذج تم تطويره في **السبعينيات**، قد لا يكون ملائمًا بشكل كامل للتقنيات والشبكات الحديثة التي تركز على **المرونة العالية** وكفاءة **الأداء** .يتطلب تطبيقه في العصر الحالي تعديلًا كبيرًا في بعض الحالات.

الخلاصة:

- **الميزات :**يوفر نموذج OSI **مرونة**، و **تنظيمًا** جيدًا، و **التوافق بين الأنظمة** .كما يسهل فهم عملية الاتصال عبر الشبكات.
- **العيوب :**يواجه تحديات في **التطبيق العملي**، **التعقيد الزائد**، وعدم التكيف الكامل مع **التقنيات الحديثة**.

الاسئلة الاسترشادية

1- اذكر ثلاثة من مهام الطبقة الفيزيائية في نموذجOSI
2- اذكر ثلاثة من الأجهزة المرتبطة بالطبقة الفيزيائية في نموذجOSI
3- اذكر ثلاثة من خصائص الطبقة الفيزيائية في نموذجOSI
4- اذكر ثلاثة من مهام طبقة ربط البيانات في نموذجOSI
5- اذكر ثلاثة من بروتوكولات طبقة ربط البيانات في نموذجOSI
6- اذكر ثلاثة من مهام طبقة الشبكة في نموذجOSI
7- اذكر ثلاثة من مهام طبقة النقل في نموذجOSI
8- اذكر ثلاثة من مهام طبقة العرض في نموذجOSI

9- اذكر ثلاثة من بروتوكولات طبقة العرض في نموذجOSI
10- اذكر ثلاثة من مزايا وعيوب نموذجOSI

المحاضرة الخامسة

أسس الطبقات وعلاقتها ببعضها في نماذج الشبكات

تعتمد النماذج الطبقية في الشبكات، مثل **نموذج OSI** و**نموذجTCP/IP** ، على مبدأ أساسي يُسمى **التقسيم الطبقي (Layering)**، والذي يهدف إلى تبسيط التصميم، والتطوير، والتشغيل، والصيانة في نظم الاتصالات.

أولاً :مفهوم الطبقات في الشبكات

- **الطبقة(Layer) :**
  وحدة وظيفية مستقلة تؤدي مجموعة محددة من المهام المرتبطة بالاتصال، وتتفاعل فقط مع الطبقتين المجاورتين لها (التي تعلوها والتي تقع أسفلها).
- **نموذج الشبكة الطبقي** يُقسم النظام إلى مجموعة من الطبقات، بحيث:
  - كل طبقة تقدم **خدمات** إلى الطبقة التي تعلوها.
  - وتعتمد على **خدمات** الطبقة التي تقع أسفلها.

ثانياً :العلاقات بين الطبقات

1. **علاقة رأسية (بين الطبقات):**

العلاقة الرئيسية بين الطبقات في النماذج الطبقية مثل نموذج OSI أو TCP/IP تُبنى على **مبدأ الخدمة والتجريد** .هذه العلاقة تُعرف بـ **العلاقة الرأسية(Vertical Relationship)** ، وهي التي تحدد كيف تتفاعل كل طبقة مع الطبقات المجاورة لها في نفس الجهاز.

مفهوم العلاقة الرأسية بين الطبقات:

1. **كل طبقة تقدم "خدمات" للطبقة التي تعلوها**
   - دون أن تكشف لها تفاصيل كيفية أداء هذه الخدمات.
   - مثال: طبقة الشبكة تقدّم خدمة "توصيل الحزم" لطبقة النقل، دون أن تُشركها في تفاصيل التوجيه.
2. **كل طبقة تستخدم "خدمات" الطبقة التي أسفلها**
   - وتفترض أن هذه الخدمات متوفرة وتؤدي عملها بشكل موثوق، دون التدخل في كيفية تنفيذها.
   - مثال: طبقة التطبيق تستخدم خدمات طبقة النقل لإرسال البيانات، ولا تحتاج لمعرفة تفاصيل البروتوكول المستخدم مثل TCP أوUDP .
3. **التفاعل يتم عبر "واجهات "(Interfaces) محددة**
   - كل طبقة تتواصل مع الطبقة الأخرى عبر واجهة تُحدد مجموعة من الوظائف أو التعليمات التي تسمح لها باستخدام خدماتها.

الواجهات (Interfaces) في الطبقات الشبكية

الواجهة (Interface) في النماذج الطبقية للشبكات تشير إلى **النقطة التي تتفاعل من خلالها طبقتان متجاورتان** داخل نفس الجهاز. أي أنها تمثل الطريقة التي تستخدم بها طبقة معينة **خدمات الطبقة التي أسفلها.**

المفهوم العام للواجهة:

- كل طبقة في النموذج الطبقي لا تتعامل مع الطبقات الأخرى بشكل مباشر.
- بل تستخدم "واجهة" تمكّنها من الوصول إلى خدمات الطبقة الأدنى منها بطريقة محددة.

- هذه الواجهة تُعرّف **كيف** يمكن للطبقة العليا أن تطلب الخدمات، وليس **كيف** تُنفذ تلك الخدمات.

وظائف الواجهات في النماذج الطبقية:

1. **توفير وسيلة للتفاعل بين الطبقات:**
   - مثلًا: طبقة التطبيق ترسل البيانات إلى طبقة النقل عبر واجهة محددة تتضمن تنسيقات وتوجيهات.
2. **إخفاء تفاصيل التنفيذ الداخلي:**
   - الطبقة العليا لا تحتاج لمعرفة طريقة تنفيذ الطبقة السفلى لوظائفها، بل تركز فقط على **ماذا يمكن أن تفعل؟** وليس **كيف؟**
3. **التقليل من الاعتماد المتبادل:**
   - من خلال الواجهة، يمكن تغيير بروتوكولات الطبقة السفلى دون التأثير على الطبقة العليا طالما أن الواجهة لم تتغير.
4. **تحديد الخدمات المتاحة:**
   - الواجهة توضح بالضبط ما هي الوظائف التي تقدمها الطبقة السفلى للطبقة التي تعلوها (مثل إرسال، استلام، إنشاء اتصال...).

مثال على واجهة في نموذجOSI :

- **طبقة النقل ← واجهتها ← طبقة التطبيق**
  - طبقة التطبيق تستخدم أوامر مثل:
    send(data)أو connect(host, port)
  - لكنها لا تعرف كيف تُقسَّم البيانات أو كيف يتم التحكم في التدفق؛ كل ذلك تديره طبقة النقل من خلال بروتوكول مثل.TCP

خصائص واجهات الطبقات:

الخاصية	التوضيح
التجريد	تخفي التفاصيل الداخلية للطبقة السفلى
التوحيد	تقدم نفس الوظائف دائمًا بغض النظر عن البروتوكول
الاستقلالية	تغيير بروتوكول داخلي لا يؤثر على الطبقة العليا
التحديد الدقيق	تحدد بدقة ما يمكن وما لا يمكن تنفيذه عبرها

الفرق بين "الواجهة" و"البروتوكول:"

المفهوم	داخل نفس الجهاز	بين جهازين متصلين
الواجهة	تربط طبقتين متجاورتين	لا علاقة لها بالجهاز الآخر
البروتوكول	لا يُستخدم داخليًا	ينظّم التواصل بين طبقات متماثلة في جهازين

تبسيط العلاقة الرأسية بمثال:

لنأخذ سيناريو إرسال رسالة بريد إلكتروني:

العلاقة الرأسية	الوظيفة	الطبقة
تستخدم طبقة النقل لإرسال البيانات	إنشاء رسالة البريد الإلكتروني	التطبيق
تستخدم طبقة الشبكة لتوجيه القطع	تقسيم الرسالة إلى قطع(segments)	النقل
تستخدم طبقة ربط البيانات لتوصيل الحزم عبر الوسيط	اختيار المسار المناسب	الشبكة
تستخدم الطبقة الفيزيائية لإرسال الإشارات	تحويل الحزم إلى إطارات	ربط البيانات
لا تعتمد على طبقة أدنى، بل تنقل البيانات فعليًا	إرسال الإشارات عبر الأسلاك أو الهواء	الفيزيائية

خلاصة العلاقة الرأسية:

- **تدرج وظيفي من الأدنى إلى الأعلى** :البيانات تنتقل من طبقة إلى طبقة أخرى حتى تصل إلى التطبيق.
- **استقلالية معتمدة** :كل طبقة مستقلة وظيفيًا، لكنها تعتمد على خدمات الطبقة أسفلها.
- **التجريد** :لا تحتاج الطبقة العليا لمعرفة تفاصيل تنفيذ الخدمات، بل تركز على وظيفتها فقط.

2. **علاقة أفقية (بين نظائر الطبقات):**

في النماذج الطبقية للشبكات مثل **OSI**و**TCP/IP**، العلاقة الأفقية هي العلاقة التي **تربط بين نظيرين من نفس الطبقة** ولكن على **جهازين مختلفين**.
بمعنى آخر، كل طبقة تتواصل مع **نظيرتها في الطرف الآخر من الاتصال**، باستخدام بروتوكول معيّن، وكأنها تتفاعل "أفقيًا" عبر الشبكة.

المفهوم الرئيسي:

- **كل طبقة لا تتواصل مباشرة مع نظيرتها في الطرف الآخر، بل ترسل البيانات إلى الطبقة التي أسفلها.**
- لكن من **وجهة نظر منطقية**، يبدو وكأن طبقة معينة تتحدث إلى نظيرتها مباشرة، باستخدام **بروتوكول موحّد**.

توضيح:

مثلاً:

- طبقة **النقل (Transport Layer)** في جهاز A تستخدم بروتوكول **TCP** .
- ترسل البيانات إلى طبقة الشبكة، وتصل في النهاية إلى طبقة **النقل** في جهازB .
- في هذا السياق، **طبقة النقل في" A تتحدث" إلى طبقة النقل في B باستخدامTCP** .

العلاقة الأفقية تتم من خلال:

1. **بروتوكولات الطبقة**
   - مثلHTTP ، TCP، IP، إلخ.
   - هذه البروتوكولات تُحدد كيفية تبادل البيانات بين نظائر الطبقات.
2. **رؤوس البروتوكولات(Protocol Headers)**
   - كل طبقة تضيف رأسًا (Header) يحتوي على معلومات تُستخدم بواسطة نظيرتها في الجهاز الآخر.

الفرق بين العلاقة الرأسية والأفقية:

ما يتم تبادله	بين ماذا؟	نوع العلاقة
خدمات وتعليمات	طبقات مختلفة في نفس الجهاز	**رأسية**
بروتوكولات ورسائل	طبقات متماثلة في أجهزة مختلفة	**أفقية**

3. **التجريد(Abstraction) :**

التجريد هو أحد المبادئ الأساسية التي تقوم عليها النماذج الطبقية في تصميم الشبكات، مثل نموذج **OSI**و **TCP/IP.**يهدف إلى **إخفاء التفاصيل المعقدة** لكل طبقة عن الطبقات الأخرى، بحيث يمكن التركيز فقط على الوظائف الأساسية التي تقدمها الطبقة دون معرفة كيف تنفذها داخليًا.

مفهوم التجريد

- التجريد يعني أن **كل طبقة تعرض "واجهة" بسيطة** تُستخدم من قِبل الطبقة التي تعلوها.
- لا تحتاج الطبقة العليا إلى فهم كيفية تنفيذ الطبقة السفلية لوظائفها؛ كل ما تحتاجه هو معرفة **ما الخدمة التي تقدمها**.

كيف يعمل التجريد؟

- **كل طبقة تؤدي مجموعة من المهام المحددة، وتعتمد على الطبقة التي أسفلها لأداء مهام أخرى.**
- الطبقة العلوية ترى فقط نتائج ما تقدمه الطبقة التي أسفلها، دون أن "ترى" أو تتفاعل مع تفاصيل التنفيذ.

مثال:

طبقة **النقل (Transport Layer)** تقدم خدمة "إرسال بيانات موثوقة" إلى طبقة التطبيق، لكنها تستند في عملها على طبقة الشبكة لإيصال البيانات، دون أن تهتم كيف يتم التوجيه أو التحويل عبر الشبكة.

فوائد التجريد:

1. **تسهيل الفهم**
   - المطوّر أو المهندس يمكنه فهم أو العمل على طبقة معينة دون الحاجة لفهم التفاصيل الدقيقة لباقي الطبقات.
2. **سهولة التطوير والتعديل**
   - يمكن تغيير أو تحسين بروتوكول في طبقة معينة دون التأثير على باقي الطبقات طالما بقيت الواجهة نفسها.
3. **إعادة الاستخدام**
   - البروتوكولات التي تنفذ وظائف معينة يمكن استخدامها في أنظمة متعددة طالما أنها تحافظ على نفس التجريد.
4. **الفصل بين المهام**
   - كل طبقة تركز على مهمة واحدة، ما يجعل النظام أكثر تنظيماً وكفاءة.

أمثلة على التجريد في الطبقات:

التجريد الذي توفره	الطبقة
توفير واجهات الاستخدام للمستخدم) مثلHTTP ، (FTP	التطبيق
إرسال واستلام البيانات بشكل موثوق أو غير موثوق(TCP/UDP)	النقل
تحديد مسار البيانات عبر الشبكة(IP)	الشبكة
ضمان تسليم الإطارات عبر الوسيط المحلي	ربط البيانات

ثالثاً :أسس تصميم الطبقات

1. **الوظائف المتقاربة تُدمج في طبقة واحدة**
   - تُجمع المهام ذات الطبيعة المتشابهة أو التي تعتمد على بعضها في طبقة واحدة لتقليل التداخل.
2. **الفصل بين المهام المختلفة**
   - تُفصل المهام التي تختلف في طبيعتها، مثل التوجيه Routing (طبقة الشبكة) عن التحكم بالجلسة Session Controlطبقة الجلسة.
3. **الاتساق في مستوى التجريد**
   - يجب أن تقدم كل طبقة مستوى تجريديًا موحدًا للطبقة التي تعلوها، بحيث لا تتطلب معرفة التفاصيل الدقيقة للطبقات الأخرى.
4. **تقليل الاعتمادية المتبادلة**
   - تسهيل التطوير والتحديث عن طريق الحد من التداخل والاعتمادية الزائدة بين الطبقات.

رابعاً :مثال على العلاقة بين الطبقات في نموذجOSI

تتعامل مع	وظيفتها الرئيسية	الطبقة
طبقة العرض	واجهة المستخدم والخدمات النهائية	التطبيق
طبقة الجلسة	تنسيق البيانات والتشفير والترميز	العرض
طبقة النقل	إدارة جلسات الاتصال	الجلسة
طبقة الشبكة	توصيل موثوق أو غير موثوق	النقل
طبقة ربط البيانات	التوجيه وتحديد المسار	الشبكة
الطبقة الفيزيائية	التحكم في الوصول للوسيط وضمان الإطارات	ربط البيانات
لا تتعامل مع طبقة أدنى منها	إرسال واستقبال الإشارات عبر الوسيط	الفيزيائية

خامساً :فائدة العلاقات بين الطبقات

- **التدرج الوظيفي :**كل طبقة تؤدي مهمة محددة مما يسهل استبدالها أو تحديثها.
- **التخصص :**يمكن تحسين كل طبقة على حدة لتقديم أداء أفضل.
- **قابلية التوسع :**من الممكن تطوير بروتوكولات جديدة داخل طبقة دون التأثير على باقي الطبقات.
- **سهولة التصحيح والتشخيص :**تحديد المشاكل حسب موقعها في النموذج الطبقي.

التوجيه(Routing)

التوجيه (Routing) هو العملية التي تُحدد بها أجهزة الشبكة، وخاصة **أجهزة التوجيه(Routers)** ، المسار الأمثل الذي يجب أن تسلكه حزمة البيانات (Packet) من المصدر إلى الوجهة عبر الشبكة، خصوصًا في الشبكات واسعة النطاق مثل الإنترنت.

أهداف التوجيه:

1. **الوصول إلى الوجهة بأقل تكلفة ممكنة** من حيث الزمن، عدد القفزات، عرض النطاق الترددي، وغيرها.
2. **تحقيق التوازن في الحمل بين المسارات.**
3. **التعامل مع الأعطال وإيجاد طرق بديلة تلقائيًا.**
4. **تحقيق الكفاءة والاعتمادية في نقل البيانات عبر الشبكات المتعددة.**

مكونات عملية التوجيه:

1. **جداول التوجيه(Routing Tables) :**
تحتوي على معلومات حول الشبكات الأخرى، وأفضل المسارات للوصول إليها.
2. **خوارزميات التوجيه(Routing Algorithms) :**
تُستخدم لتحديد الطريق الأمثل. وتنقسم إلى:
   - **ثابتة(Static) :**يتم إعدادها يدويًا.
   - **ديناميكية(Dynamic) :**يتم تحديثها تلقائيًا باستخدام بروتوكولات التوجيه.
3. **بروتوكولات التوجيه(Routing Protocols) :**
تُستخدم لتبادل معلومات التوجيه بين أجهزة التوجيه، ومنها:
   - **RIP (Routing Information Protocol)**
   - **OSPF (Open Shortest Path First)**
   - **EIGRP (Enhanced Interior Gateway Routing Protocol)**
   - **BGP (Border Gateway Protocol)**

أنواع التوجيه:

التوضيح	النوع
يُضبط يدويًا، مناسب للشبكات الصغيرة والمستقرة	**توجيه ثابت(Static Routing)**
يعتمد على بروتوكولات تتبادل معلومات الشبكة باستمرار	**توجيه ديناميكي (Dynamic Routing)**
يستخدم عند عدم وجود مسار محدد في جدول التوجيه، غالبًا يُرسل إلى راوتر خارجي	**توجيه افتراضي(Default Routing)**

كيفية عمل التوجيه (ببساطة):

1. عند إرسال حزمة بيانات، يبحث الجهاز في جدول التوجيه لمعرفة المسار الأنسب.
2. تُرسل الحزمة إلى جهاز التوجيه (Router) التالي في الطريق.
3. يُكرّر كل راوتر نفس العملية حتى تصل الحزمة إلى وجهتها.

مثال:

- جهاز A يريد إرسال بيانات إلى جهاز B على شبكة بعيدة.
- جهاز التوجيه الأقرب إلى A يبحث في جدول التوجيه ويُحدد أفضل مسار.
- تُمرر البيانات من راوتر إلى آخر حسب المسارات المحددة حتى تصل إلى.B

الفرق بين التوجيه والتبديل(Switching) :

التبديل(Switching)	التوجيه(Routing)	الميزة
يعمل في طبقة ربط البيانات(Data Link Layer)	يعمل في طبقة الشبكة(Network Layer)	الطبقة
Switches	Routers	الأجهزة
داخل نفس الشبكة المحلية(LAN)	بين الشبكات	نطاق العمل

التحديات التي تواجه العلاقة بين الطبقات في الشبكات

العلاقة بين الطبقات في الشبكات – كما في **نموذج OSI** أو **نموذج – TCP/IP** تمثل حجر الأساس في تصميم الأنظمة الشبكية الحديثة. ورغم أن هذه النماذج مبنية على مبدأ **التجريد والتنظيم الهرمي**، إلا أن هناك عدة تحديات تؤثر على كفاءة وأمان وتكامل الاتصال بين الطبقات.

فيما يلي أهم **التحديات الأكاديمية والتقنية** المرتبطة بالعلاقة بين الطبقات في الشبكات:

1-التجريد المفرط(Over-Abstraction)

- **الوصف :**قد تؤدي التجريدات بين الطبقات إلى حجب التفاصيل المهمة، مما يصعّب تحسين الأداء على مستوى أدنى أو أعلى.
- **الأثر :**يقلل من مرونة التفاعل بين التطبيقات والبنية التحتية.

2-الكفاءة في التواصل بين الطبقات

- **الوصف :**عند إرسال البيانات بين الطبقات، تُضاف رؤوس بيانات (Headers) في كل طبقة، مما يزيد من حجم البيانات الإجمالي.
- **الأثر :**يؤدي إلى **زيادة الحمل الشبكي (Overhead)** وانخفاض الكفاءة، خاصة في الشبكات ذات النطاق المحدود.

3- عدم التناسق بين النماذج النظرية والتطبيق العملي

- **الوصف :**نموذج OSI مثالي لكنه غير مطبق حرفيًا، على عكس نموذج TCP/IP الأكثر شيوعًا.
- **الأثر :**يؤدي إلى اختلاف في التفسيرات والوظائف بين الأنظمة، مما يؤثر على التوافقية.\

4- تداخل المهام بين الطبقات

- **الوصف :**في بعض الأحيان تقوم طبقة معينة بمهام ليست من اختصاصها الأصلي.
- **مثال :**الطبقة الرابعة (النقل) قد تتعامل مع قضايا أمنية تعود إلى الطبقة السابعة (التطبيق).
- **الأثر :**يسبب **تضاربًا في المسؤوليات** ويُصعّب عمليات الصيانة والتوسعة.

5- قضايا الأمان(Security Challenges)

- **الوصف :**طبقات معينة قد تُصبح نقاط ضعف، مثل:
  - ضعف المصادقة في طبقة التطبيق.
  - هجمات حجب الخدمة (DoS) تستهدف طبقة النقل.
- **الأثر :**عدم معالجة الأمان على كل طبقة قد يسبب **اختراقات عابرة للطبقات**.

6- تأثير التحديث في طبقة على الطبقات الأخرى

- **الوصف :**إجراء تعديل على بروتوكول في طبقة معينة قد يتطلب تعديلات في طبقات أخرى.
- **الأثر :**يقلل من الاستقلال الحقيقي للطبقات، ويزيد من تعقيد التطوير.

7- أداء البروتوكولات بين الطبقات

- **الوصف :**بعض البروتوكولات ليست مصممة للعمل بكفاءة مع بروتوكولات من طبقات أخرى.
- **الأثر :**يؤدي إلى عنق زجاجة (Bottleneck) في الأداء أو ضعف في نقل البيانات.

8- صعوبة تتبع الأخطاء

- **الوصف :**بسبب توزيع المسؤوليات عبر عدة طبقات، يصعب أحيانًا تحديد مصدر الخطأ بدقة.
- **الأثر :**يُعقّد عمليات التشخيص والصيانة.

9- ضعف الدعم للابتكارات الحديثة

- **الوصف :**بعض التطبيقات أو التقنيات الناشئة) مثل SDN أو 5 (Gتحتاج إلى تجاوز النموذج الطبقي التقليدي.
- **الأثر :**النموذج الطبقي قد يقيد الابتكار ما لم يُعد تصميمه أو يُدمج بمرونة.

العلاقة بين الطبقات في الشبكات تقوم على مبدأ التنظيم والاعتماد التدريجي، لكنها ليست خالية من التحديات. التغلب على هذه التحديات يتطلب موازنة بين **الهيكلة الأكاديمية** و**مرونة التصميم العملي**.

الاسئلة الاسترشادية

1- اذكر ثلاثة من وظائف الواجهات في النماذج الطبقية
2- اذكر ثلاثة من خصائص الواجهات في النماذج الطبقية
3- اذكر ثلاثة من فوائد التجريد
4- اذكر ثلاثة من أسس تصميم الطبقات
5- اذكر ثلاثة من فوائد العلاقات بين الطبقات
6- اذكر ثلاثة من اهداف التوجيه
7- اذكر ثلاثة من مكونات عملية التوجيه
8- اذكر ثلاثة من أنواع التوجيه

المحاضرة السادسة

طبقة التطبيق وعلاقتها بباقي الطبقات

في نموذج الشبكات مثل نموذج **OSI**أو **TCP/IP**، تُعد **طبقة التطبيق (Application Layer)** الطبقة العليا، وهي المسؤولة عن **التفاعل المباشر مع المستخدم** وتوفير واجهات للوصول إلى خدمات الشبكة. لفهم علاقتها بباقي الطبقات، من المهم توضيح وظائفها أولاً، ثم كيف تعتمد على الطبقات الأخرى لتحقيق الاتصال الكامل.

أولًا: تعريف طبقة التطبيق

- **وظيفتها :**تُمثل نقطة التفاعل بين المستخدم وبرامج الشبكة.
- **توفر بروتوكولات** مثل:
  - HTTPلتصفح الويب
  - SMTPلإرسال البريد
  - FTPلنقل الملفات
  - DNSلتحويل أسماء النطاقات
- **لا تتعامل مباشرة مع تفاصيل الشبكة** (كالإرسال الفعلي للبيانات)، بل تعتمد على الطبقات السفلى لذلك.

ثانيًا: علاقة طبقة التطبيق بالطبقات الأخرى

1-طبقة النقل(Transport Layer)

- **العلاقة :**طبقة التطبيق تعتمد على طبقة النقل لضمان **نقل موثوق للبيانات**.
- **أمثلة:**
  - تستخدم بروتوكول **TCP**عندما تحتاج إلى ضمان الاستلام الكامل مثلHTTP ، SMTP .
  - تستخدم **UDP**عندما لا يكون التسليم الموثوق ضروريًا مثلDNS ، بث الفيديو.

2- طبقة الشبكة(Network Layer)

- **العلاقة غير مباشرة.**
- تقوم طبقة النقل بتجزئة البيانات، ثم تمريرها إلى طبقة الشبكة التي تقوم بتحديد **المسار الأفضل للبيانات عبر الشبكة**.
- الطبقة التطبيقية لا ترى تفاصيل مثل عناوين IP أو التوجيه.

3- طبقة ربط البيانات (Data Link Layer) والطبقة الفيزيائية

- **العلاقة غير مرئية تمامًا لطبقة التطبيق،** لكنها ضرورية لنقل البيانات فعليًا عبر الوسط المادي.
- تنقل الإشارات عبر الكابلات أو الهواء (في الشبكات اللاسلكية)، وهي المسؤولة عن التحكم في الوصول إلى الوسيط.

ثالثًا: من أعلى إلى أسفل (التسلسل عند الإرسال)

1. المستخدم يرسل طلبًا عبر تطبيق (مثل متصفح).
2. طبقة التطبيق تنشئ البيانات باستخدام بروتوكول) مثل.(HTTP
3. طبقة النقل تضيف رأس (Header) خاص بها لتوفير التحكم بالتدفق وضمان التوصيل.
4. طبقة الشبكة تضيف عنوان IP لتحديد الوجهة.
5. طبقة ربط البيانات تضيف عنوان MAC لنقل البيانات عبر الشبكة المحلية.
6. البيانات تُرسل فعليًا عبر الوسيط في الطبقة الفيزيائية.

ماهو الرأس (Header)

في سياق الشبكات، وخاصة عند الحديث عن **طبقة التطبيق** وبروتوكول مثل **HTTP**، يُقصد بـ **الرأس (Header)** مجموعة من **الحقول الوصفية** التي تُضاف إلى الرسائل أو الطلبات لتوفير معلومات إضافية تُوجّه كيفية معالجة هذه الرسائل من قبل المستقبل (مثل الخادم أو المتصفح).

أولًا: ما هو الـHeader ؟

الرأس هو **جزء من الطلب أو الاستجابة** يُرسل قبل المحتوى الأساسي(Body) ، ويتكون من **أزواج "اسم: قيمة "**توضح خصائص الرسالة أو معلومات عن المرسل والمحتوى.

مثال عام على رأس:HTTP

GET /index.html HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0
Accept: text/html

الشرح

السطر الأول**GET /index.html HTTP/1.1 :**

هذا هو سطر الطلب الأساسي ويتكون من 3 أجزاء:

1. **GET**
   - نوع الطلب :(Method) يعني أن العميل (مثلاً متصفحك) يطلب **الحصول على مورد**)صفحة، صورة، ملف.(...
   - لا يُرسل بيانات في الجسم(body) ، بل يطلب فقط عرضها.
2. **/index.html**
   - هو **المسار** (Path)إلى المورد على الخادم.
   - في هذه الحالة، يطلب الملف index.htmlالموجود على الجذر.
3. **HTTP/1.1**
   - يشير إلى **إصدار بروتوكول HTTP** المستخدم في هذا الطلب.
   - HTTP/1.1يتيح استخدام ميزات مثل الاتصال المستمر (Keep-Alive) وضغط البيانات.

السطر الثاني Host: www.example.com :

- هذا الرأس (Header) يُخبر الخادم عن **اسم المضيف (Domain)** المطلوب.
- مهم جدًا خاصة في الخوادم التي تستضيف عدة مواقع.(virtual hosting)
- بدون هذا الرأس، قد لا يعرف الخادم أي موقع تقصده.

السطر الثالث User-Agent: Mozilla/5.0 :

- يصف **العميل (Client)** الذي يرسل الطلب.
- يُستخدم من قبل الخوادم لتحديد نوع الجهاز أو المتصفح لتقديم محتوى مناسب.
- مثال: قد يرسل الخادم نسخة خفيفة من الموقع إذا عرف أن المتصفح على هاتف.

السطر الرابع Accept: text/html :

- يُخبر الخادم عن **نوع المحتوى الذي يمكن للعميل قبوله**.
- هنا، العميل يُفضّل الحصول على محتوى بصيغةHTML .
- يمكن أن يتضمن أنواع متعددة مفصولة بفواصل مثل : text/html, application/json.

ثانيًا: أنواع رؤوسHTTP (Headers)

يمكن تصنيف رؤوس HTTP إلى عدة أنواع:

1- عامة General Headers

- تُستخدم في الطلب والاستجابة معًا.
- مثال:
  - Date: تاريخ إرسال الرسالة.
  - Connection: التحكم في اتصال TCP مثلkeep-alive .

2- في الطلبRequest Headers

- ترسل معلومات من العميل إلى الخادم.
- أمثلة:
  - Host: اسم الخادم المطلوب.
  - User-Agent: نوع المتصفح أو التطبيق.
  - Accept: نوع البيانات المقبولة(HTML, JSON, etc) .
  - Authorization: معلومات التوثيق إذا كان الوصول محمياً.

3-في الاستجابة Response Headers

- ترسل معلومات من الخادم إلى العميل.
- أمثلة:
  - Server: نوع خادم الويب.
  - Set-Cookie: إنشاء ملفات تعريف الارتباط.

- Content-Type: نوع البيانات المسترجعة.

4-خاصة بالمحتوى Entity Headers

- تتعلق بخصائص البيانات الفعلية في الجسم(Body) .
- أمثلة:
  - Content-Length: طول البيانات.
  - Content-Encoding: نوع الضغط(gzip, deflate) .
  - Content-Language: اللغة المستخدمة.

ثالثًا: أهمية الرؤوس

- **تحديد نوع البيانات :**كي يعرف المتصفح كيف يعالج الاستجابة.
- **تحديد اللغة أو التشفير :**لتقديم نسخة مناسبة للمستخدم.
- **توثيق المستخدم :**عبر رأس Authorization.
- **إدارة الجلسات :**عبر Cookieو Set-Cookie.
- **أمان وتحكم :**مثل X-Frame-Optionsو Strict-Transport-Security.

مثال تطبيقي كامل لطلب:HTTP

GET /home HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0
Accept: text/html
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

هذا الطلب يطلب الصفحة home/من خادم www.example.com، ويخبره أن العميل يستخدم متصفح معين ويقبل ملفات HTML، ويتضمن بيانات توثيق.

الرأس (Header) هو آلية وصفية تُمكن طرفي الاتصال من **تبادل معلومات ما وراء البيانات**، مثل طريقة التشفير، نوع المحتوى، الهوية، التفاوض على اللغة، وغيرها. الرؤوس ضرورية لتحقيق التكامل، التوافق، والأمان بين التطبيقات.

نموذج مرئي لرأس (Header) طلبHTTP

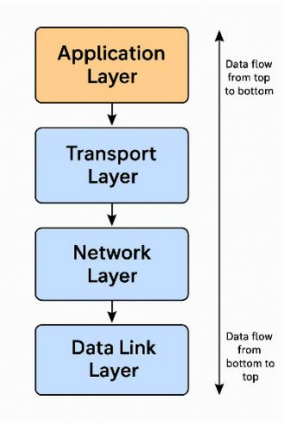
```
┌──────────────────────────────────────────────────────┐
│ طلب GET                                              │
├──────────────────────────────────────────────────────┤
│ GET /index.html HTTP/1.1          ← الطلب سطر        │
├──────────────────────────────────────────────────────┤
│ Host: www.example.com             ← المطلوب الخادم عنوان
│ User-Agent: Mozilla/5.0           ← العميل أو المتصفح نوع
│ Accept: text/html                 ← المقبول المحتوى نوع
│ Accept-Language: en-US            ← المفضلة اللغة
│ Connection: keep-alive            ← الاتصال إدارة
│ Authorization: Basic ...          ← (اختياري) المستخدم توثيق
└──────────────────────────────────────────────────────┘
```

ملاحظات على النموذج:

- **السطر الأول(Request Line) :**
  - يحتوي على نوع الطلب (GET) والمسار (/index.html) وإصدار البروتوكول.(HTTP/1.1)
- **الأسطر التالية(Headers) :**
  - كل سطر هو رأس (Header) مكون من اسم وقيمة.
  - تساعد الخادم في فهم كيفية التعامل مع الطلب والمحتوى.
- **لا يوجد محتوى (Body) هنا** لأن طلب GETلا يرسل بيانات.

من أسفل إلى أعلى (عند الاستقبال)

1. البيانات تُستقبل من الوسيط الفيزيائي.
2. يتم التحقق منها في طبقة ربط البيانات، ثم تمريرها للأعلى.
3. طبقة الشبكة تُحدد التوجيه.
4. طبقة النقل تفكّ تجزئة البيانات وتُعيد ترتيبها.
5. طبقة التطبيق تُفسّر البيانات وتُرسلها للتطبيق (مثلاً: عرض صفحة ويب).



طبقة التطبيق هي "البوابة" التي يدخل منها المستخدم إلى عالم الشبكة، لكن **عملها لا يكتمل دون الاعتماد على الطبقات الأخرى** .هي مسؤولة عن المحتوى والمعنى، بينما تتكفل الطبقات السفلى بعملية النقل، التوجيه، والتحكم في البيانات. هذه العلاقة المبنية على **مبدأ الفصل الوظيفي** تجعل الشبكات أكثر تنظيمًا ومرونة في التطوير والصيانة.

مزايا طبقة التطبيق

1-واجهة مباشرة مع المستخدم

- توفر للمستخدمين برامج وتطبيقات مثل المتصفحات والبريد الإلكتروني وخدمات الدردشة.
- تسهل التفاعل مع الشبكة دون الحاجة لفهم تعقيداتها.

2-دعم مجموعة واسعة من البروتوكولات

- مثلHTTP ، FTP، SMTP، DNS، وغيرها.
- تتيح تنوعًا في الوظائف (التصفح، التحميل، الإرسال...).

2-قابلية التوسع والتطوير

- من الممكن تحديث التطبيقات والبروتوكولات دون تعديل على الطبقات السفلى.
- تدعم إنشاء تطبيقات شبكية حديثة (مثل تطبيقات الويب والسحابة والهواتف الذكية).

4- إمكانية تخصيص الخدمة

- يمكن برمجة الطبقة لتتناسب مع احتياجات محددة لمؤسسة أو نظام.
- مثل تخصيص إعدادات البريد أو التحكم في الوصول إلى قواعد البيانات.

5-معالجة البيانات بالتكامل مع التطبيقات

- تقوم الطبقة بتهيئة البيانات كي تتناسب مع المعالجة في التطبيقات المختلفة.
- مثال: تحويل اسم النطاق (DNS) إلى عنوان IP قبل إرسال الطلب إلى الخادم.

ثانيًا :عيوب طبقة التطبيق

1- ضعف التحكم في الأمان

- تقع مسؤولية الأمان غالبًا على التطبيقات نفسها، مما يجعلها عرضة للاختراق إذا لم تُبرمج بشكل صحيح.
- يمكن استغلالها عبر هجمات مثل:
  - XSSحقن نصوص
  - SQL Injection
  - CSRFتزوير الطلبات

2-الاعتماد الكامل على البروتوكولات السفلية

- طبقة التطبيق لا تستطيع نقل البيانات بمفردها، بل تعتمد على طبقة النقل وما دونها.
- أي خلل في الطبقات الأخرى يؤدي إلى فشل خدماتها.

3- قد تكون ثقيلة الأداء

- بعض بروتوكولات طبقة التطبيق تستهلك موارد كثيرة من النظامCPU) ، .(RAM
- مثل تشفير البيانات أو تحميل ملفات كبيرة FTP) أو.(HTTPS

4-صعوبة التوافقية بين الأنظمة المختلفة

- ليس كل نظام يدعم نفس بروتوكولات التطبيق، مما يُحدث مشكلات في التوافق.
- مثال: بعض أنظمة البريد لا تدعم ترميزات معينة أو امتدادات ملفات.

5-العبء على المصمم والمطور

- يتطلب تصميم هذه الطبقة معرفة قوية بتقنيات الشبكات والبرمجة والتشفير.
- وأي خطأ في الكود قد يؤثر على أمان وموثوقية النظام ككل.

طبقة التطبيق تمثل واجهة الاستخدام العليا في نموذج الشبكة، وتُعتبر من أهم الطبقات في تقديم خدمات ملموسة للمستخدم. ورغم فوائدها في التفاعل، التنوع، والتوسع، إلا أنها أيضًا تُعد نقطة ضعف رئيسية من حيث الأمان والكفاءة، وتتطلب تصميمًا دقيقًا لضمان الأداء السليم.

بروتوكول HTTP (Hypertext Transfer Protocol)

أولًا :مزايا بروتوكولHTTP

1-بساطة التصميم وسهولة الاستخدام

- البروتوكول يعتمد على نصوصASCII ، ويمكن للمطورين اختباره بسهولة عبر المتصفح أو أدوات مثل PostmanوcURL .
  - ASCIIهو اختصار لـ **American Standard Code for Information Interchange**، وهو معيار ترميز يُستخدم لتمثيل الأحرف النصية في الحواسيب. يتكون من **7بتات** (128 رمزًا) تشمل الحروف الإنجليزية (الكبيرة والصغيرة)، الأرقام، وبعض الرموز وعلامات التحكم. ظهر لأول مرة في الستينيات لتمكين التفاهم بين الأجهزة المختلفة. تُستخدم ASCII بشكل واسع في بروتوكولات الشبكات مثل HTTP و .SMTPرغم محدوديته، لا يزال أساسًا للعديد من أنظمة الترميز الحديثة مثل.UTF-8
  - Postmanهو **أداة برمجية مجانية** تُستخدم لاختبار وتوثيق واجهات برمجة التطبيقات .(APIs) تتيح للمطورين إرسال طلبات HTTP ومراقبة الاستجابات بسهولة. تدعم أوامر مثل GET و POSTو PUT وDELETE، وتسمح بإضافة رؤوس وجسم (Body) مخصص للطلب. توفر بيئة مرئية تسهّل اختبار واجهات RESTful بدون الحاجة إلى كتابة كود. تُستخدم على نطاق واسع في تطوير واختبار التطبيقات الحديثة.
  - cURLهو **أداة سطر أوامر** تُستخدم لإرسال واستقبال البيانات عبر بروتوكولات الإنترنت مثل HTTP و .FTPيُستخدم بشكل أساسي لاختبار واجهات برمجة التطبيقات (APIs) أو لتنزيل الملفات من الإنترنت. يدعم العديد من طرق الطلب مثل GET و POSTويتيح إضافة رؤوس أو بيانات. يُستخدم في الأنظمة التشغيلية المختلفة ويُعد من الأدوات المهمة للمطورين. يتميز ببساطته وسرعته ومرونته في التعامل مع الطلبات الشبكية.

2- العمل بدون حالة(Stateless)

- كل طلب مستقل عن الآخر، مما يقلل من استهلاك الموارد في الخوادم.
- يسهل التوسع الأفقي (مثل تحميل الطلبات على أكثر من خادم).

العمل بدون حالة (Stateless) هو مبدأ أساسي في تصميم الأنظمة، وخاصة في **بروتوكولات الشبكات مثلHTTP** ، ويعني أن **كل طلب يتم التعامل معه بشكل مستقل** دون أن يحتفظ الخادم بأي معلومات عن الطلبات السابقة.

شرح مبسط:

- في النظام **Stateless**، لا يخزن الخادم معلومات عن المستخدم أو الجلسة بعد تنفيذ الطلب.
- كل مرة يُرسل فيها العميل طلبًا، يجب أن يحتوي الطلب على **جميع البيانات اللازمة** لمعالجته.
- لا يتم الاعتماد على "الذاكرة" بين الطلبات، مما يجعل الخادم أكثر بساطة وقابلية للتوسع.

مثال:

عندما تزور صفحة ويب، فإن الخادم يعالج الطلب ويرسل الصفحة، ثم "ينسى" كل شيء عنك بعد ذلك.

مزايا:

- سهولة التوسع.
- تقليل استهلاك الذاكرة على الخادم.
- تحسين الأداء في بعض الحالات.

عيب رئيسي:

- إذا احتاج النظام إلى تتبع الجلسات (مثل تسجيل الدخول)، فلابد من حلول إضافية مثل ملفات **الكوكيز (Cookies)** أو **رموز التوثيق.(Tokens)**

3- دعم واسع وانتشار عالمي

- مدعوم في جميع متصفحات الإنترنت وأجهزة الحاسوب والهواتف الذكية.
- يُعد معيارًا أساسيًا في تطبيقات الويب.

4-مرونة في استخدام الطرق(Methods)

- يدعم طرقًا متنوعة مثل:
  - GETطلب بيانات

GETهو نوع من أنواع طلبات HTTP يُستخدم لطلب **جلب البيانات** من الخادم دون تعديلها. يتم إرسال البيانات المطلوبة من خلال عنوان URL فقط، ولا يحتوي الطلب على جسم .(Body) يُعد هذا النوع من الطلبات **آمنًا** لأنه لا يُحدث تغييرات على الخادم. يتم استخدامه بشكل واسع في تصفح الصفحات، مثل عرض المقالات أو نتائج البحث. لا يجب استخدام GETلإرسال معلومات حساسة لأنه يُعرض في شريط العنوان ويمكن تخزينه في سجل المتصفح.

- POSTإرسال بيانات

POSTهو نوع من طلبات HTTP يُستخدم لإرسال **بيانات من العميل إلى الخادم** بهدف معالجتها أو تخزينها. تُرسل البيانات في جسم الطلب(Body) ، وليس في العنوان، مما يجعله أكثر أمانًا من GETفي بعض الحالات. يُستخدم عادةً في نماذج التسجيل، تسجيل الدخول، أو إرسال تعليقات. يتيح إنشاء موارد جديدة على الخادم أو تنفيذ عمليات تؤثر في قاعدة البيانات. بخلاف GET، يعتبر POSTطلبًا غير آمن بمعنى أنه يُحدث تغييرًا في حالة النظام.

- PUTو DELETEللتحديث والحذف فيREST APIs

- PUTهو نوع من طلبات HTTP يُستخدم لتحديث مورد موجود أو إنشاء مورد جديد إذا لم يكن موجودًا، حيث يتم إرسال البيانات الجديدة في جسم الطلب .(Body) يُعد " PUTإدخالًا كاملًا" لأنه يستبدل المورد بالكامل بالمحتوى المُرسل.
- أما DELETE، فهو يُستخدم لحذف مورد معين من الخادم. يُرسل الطلب عادةً مع معرّف المورد في عنوانURL ، ولا يتطلب جسمًا. كلا الطلَبين PUT) و (DELETEيمكن أن يُحدثا تغييرات دائمة في قاعدة البيانات، ولهذا يُعتبران من الطلَبات "غير الآمنة" (أي تُغير حالة النظام.(

- يمكّن من تصميم أنظمة RESTful بمرونة عالية.

أنظمة **RESTful**هي أنظمة أو خدمات ويب تُبنى على معماريةREST (Representational State Transfer) ، وهي أسلوب تصميم يُستخدم لتطوير واجهات برمجة التطبيقات (APIs) التي تعمل عبر بروتوكول .HTTP تعتمد RESTful على مجموعة من المبادئ التي تجعل الاتصال بين العميل والخادم بسيطًا وفعالًا.

الخصائص الرئيسية لأنظمة:RESTful

1. **بدون حالة(Stateless) :**لا يحتفظ الخادم بأي معلومات عن الجلسة بين الطلبات.
2. **استخدامHTTP :**تعتمد على أوامر HTTP القياسية مثل GET، POST، PUT، وDELETE.
3. **الوصول إلى الموارد :**تُعرَّف الموارد باستخدام) URI مثل (users/1/، ويتم تمثيلها غالبًا بصيغة JSON أوXML .
4. **فصل العميل عن الخادم :**يمكن لكل من العميل والخادم أن يتطور بشكل مستقل.
5. **إمكانية التخزين(Cachability) :**يمكن الاستفادة من التخزين المؤقت لتحسين الأداء.

أمثلة على أنظمةRESTful :

- واجهات برمجة التطبيقات الخاصة بـGitHub ، Twitter، Google Maps.
- الخدمات الخلفية في تطبيقات الويب أو الهواتف الذكية.

5-دعم الإضافات(Headers & Extensions)

- يمكن تضمين رؤوس مخصصة لنقل معلومات إضافية مثل التوثيق (Authentication) أو اللغة أو نوع المحتوى (MIME types).

Authenticationفي الشبكات هو عملية **التحقق من هوية المستخدم أو الجهاز** قبل السماح له بالوصول إلى شبكة أو نظام. الهدف الرئيسي من المصادقة هو التأكد من أن الشخص أو الكيان الذي يحاول الوصول هو فعلاً من يدّعي أنه هو.

مكونات أساسية للمصادقة:

1. **المعرف :(Username)** يُمثل هوية المستخدم.
2. **الوسيلة السرية (مثل كلمة المرور) :**تُستخدم لإثبات هذه الهوية.

أنواع طرق المصادقة:

- **شيء تعرفه** :مثل كلمة المرور أو رمز.PIN
- **شيء تملكه** :مثل بطاقة ذكية أو هاتف.
- **شيء أنت عليه** :مثل بصمة الإصبع أو التعرف على الوجه.

أمثلة في الشبكات:

- إدخال كلمة المرور للاتصال بشبكة.Wi-Fi
- تسجيل الدخول إلى حساب بريد إلكتروني عبر متصفح.
- استخدام رموز تحقق ثنائية (2FA) عند الدخول إلى نظام حساس.

6-التكامل مع الطبقات الأخرى

- يعمل بسهولة فوق بروتوكولات مثلTCP ، ويُستخدم بكفاءة في HTTPS (HTTP over TLS/SSL) لتأمين البيانات.

ثانيًا :عيوب بروتوكولHTTP

1- عدم الأمان في الإصدار التقليدي HTTP بدونSSL

- البيانات تنتقل بنص عادي(Plain Text) ، مما يجعلها عرضة لاعتراضها من طرف ثالث.
- يستخدم اليوم غالبًا مع بروتوكول HTTPS لتجاوز هذه المشكلة.

SSL (Secure Sockets Layer)هو **بروتوكول أمني** يُستخدم لتأمين الاتصال بين العميل والخادم عبر الإنترنت. يقوم بتشفير البيانات المتبادلة لحمايتها من التجسس أو التلاعب أثناء النقل. يُستخدم بشكل واسع في المواقع الإلكترونية لتأمين المعاملات، خاصة تلك التي تتطلب معلومات حساسة مثل كلمات المرور أو بيانات الدفع. يتم التعرف على الاتصال المؤمَّن باستخدام SSL من خلال ظهور "https://" في عنوان الموقع. على الرغم من أن SSLتم استبداله الآن بـTLS ، إلا أن المصطلح لا يزال يُستخدم بشكل شائع.

2-ضعف في إدارة الجلسات(Session Management)

- كونه عديم الحالة(Stateless) ، يجب إنشاء تقنيات خارجية مثل الـ Cookies أو الـ Session Tokens لإدارة تواصل المستخدمين مع التطبيقات.

3- زيادة في استهلاك البيانات

- مع كل طلب يتم إرسال رؤوس (Headers) قد تكون كبيرة، حتى لو كان المحتوى المطلوب صغيرًا.
- لا يوجد ضغط افتراضي للبيانات في HTTP/1.1 تحسنت الحالة في HTTP/2 و3.

4- عرضة لهجمات شهيرة

- مثل:
  - **Man-in-the-Middle (MITM)**: إذا لم يُستخدم HTTPS.
  - **Cross-site scripting (XSS)**
  - **HTTP Header Injection**

5- قلة التحكم في التدفق والزمن

- ليس مصممًا لنقل البيانات بشكل متدفق أو زمني دقيق (مثل الفيديو الحي)، لذلك يُستخدم بروتوكولات أخرى كـ RTSP لهذا الغرض.

الاسئلة الاسترشادية

1- اذكر ثلاثة من بروتوكولات طبقة التطبيق
2- اذكر ثلاثة من أنواع رؤوس HTTP (Headers)
3- اذكر ثلاثة من وظائف رؤوس HTTP (Headers)
4- اذكر ثلاثة من مزايا طبقة التطبيق
5- اذكر ثلاثة من عيوب طبقة التطبيق
6- اذكر ثلاثة من مزايا بروتوكول HTTP (Hypertext Transfer Protocol)
7- اذكر ثلاثة من أنواع طرق المصادقة
8- اذكر ثلاثة من عيوب بروتوكول HTTP (Hypertext Transfer Protocol)

المحاضرة السابعة

أشهر البروتوكولات المستخدمة في طبقة التطبيق

في طبقة التطبيق (Application Layer) من نموذج الشبكات OSI وTCP/IP، توجد العديد من البروتوكولات الشائعة التي تُستخدم لتوفير خدمات متنوعة للمستخدمين والتطبيقات. من أشهر هذه البروتوكولات:

1 -HTTP (HyperText Transfer Protocol)

HTTP (HyperText Transfer Protocol)هو بروتوكول طبقة التطبيق يُستخدم أساسًا لنقل صفحات الويب والبيانات بين **المتصفح (العميل)** و**الخادم (السيرفر)** عبر الإنترنت. يُعتبر HTTP أساس الاتصال في شبكة الويب العالمية.(WWW)

خصائصHTTP :

1. **بروتوكول بدون حالة(Stateless) :**
لا يحتفظ بأي معلومات عن الطلبات السابقة، مما يعني أن كل طلب يتم معالجته بشكل مستقل.
2. **يستخدم طريقة الطلب (Request) والاستجابة(Response) :**
حيث يرسل العميل طلبًا، ويستجيب الخادم بالمحتوى المطلوب (صفحةHTML ، صورة، ...JSONإلخ.)
3. **يعتمد على بروتوكول TCP في النقل:**
لضمان وصول البيانات بشكل موثوق.
4. **يدعم عدة أنواع من الطلبات:**
مثل GETجلب بيانات، POSTإرسال بيانات، PUT، .DELETE
5. **غير مشفر بطبيعته:**
مما يعني أن البيانات تنتقل بشكل واضح، ويمكن اعتراضها، ولهذا يُفضّل استخدام HTTPS للأمان.

عيوب HTTP

بروتوكول (Hypertext Transfer Protocol) HTTP هو البروتوكول الأساسي المستخدم لنقل البيانات عبر الإنترنت. على الرغم من أنه مهم جدًا في الاتصال بين الخوادم والعملاء، إلا أن له بعض العيوب:

1. **عدم الأمان:**
   - **HTTP**لا يوفر تشفيرًا للبيانات المتبادلة بين العميل (مثل المتصفح) والخادم. لذلك، فإن البيانات مثل كلمات المرور أو المعلومات الشخصية يمكن أن تُسرق إذا كانت تُرسل عبر شبكات غير آمنة.
   - لتجاوز هذه المشكلة، يُستخدم (HTTP Secure) **HTTPS**الذي يعتمد على بروتوكولات الأمان مثل SSL/TLSلتشفير البيانات.
2. **لا يضمن استمرارية الاتصال:**
   - فيHTTP ، كل طلب يتم معالجته بشكل مستقل دون حفظ حالة الاتصال بين العميل والخادم. هذا يعني أن كل طلب يتطلب إعادة الاتصال وتبادل البيانات من البداية، مما يستهلك وقتًا وموارد.
3. **عدم وجود آلية لإدارة الجلسات:**
   - HTTPهو بروتوكول غير موجه للحفاظ على الحالة بين الطلبات. وهذا يعني أنه لا يستطيع تتبع تفاعلات المستخدم عبر عدة طلبات دون أن يستخدم تقنيات إضافية مثل **الكوكيز** أو **الجلسات** لتخزين هذه المعلومات.
4. **قيد حجم البيانات:**
   - قد يكون هناك قيود على حجم البيانات التي يمكن إرسالها في طلب .HTTP على سبيل المثال، يحدد بعض الخوادم أو المتصفحات حدودًا لحجم رأس HTTP أو حجم البيانات المرفقة بالطلب.
5. **الاعتماد على الخوادم:**
   - لأن HTTP يعتمد على خوادم معينة لمعالجة الطلبات، فإن أداء النظام قد يتأثر إذا كانت الخوادم غير متوفرة أو في حالة ضغط على الشبكة.

6. **القابلية للتعرض للهجمات:**
   - البروتوكول قد يكون عرضة لعدة أنواع من الهجمات مثل هجوم **Man-in-the-Middle**أو هجوم **SQL Injection**إذا كانت تطبيقات الويب لا تُصمم بشكل صحيح.

2- HTTPS (HTTP Secure) :

HTTPS (Hypertext Transfer Protocol Secure)هو بروتوكول يستخدم لتأمين الاتصال بين العميل (مثل متصفح الويب) والخادم عبر الإنترنت. يعتمد HTTPS على **بروتوكولات الأمان** مثل **SSL (Secure Sockets Layer)** و **TLS (Transport Layer Security)**لتشفير البيانات وضمان أمانها خلال النقل، ويستخدم في المقام الأول لضمان الأمان وحماية المعلومات الحساسة مثل كلمات المرور، البيانات المالية، والمعلومات الشخصية.

مزايا:HTTPS

1. **التشفير:(Encryption)**
   - **HTTPS**يقوم بتشفير البيانات التي يتم إرسالها بين العميل والخادم باستخدام **SSL/TLS.**هذا التشفير يضمن أن البيانات التي يتم نقلها عبر الشبكة لا يمكن قراءتها أو التلاعب بها من قبل أطراف ثالثة (مثل القراصنة أو المتسللين).
   - يشمل هذا التشفير **المحتوى** (مثل النصوص والصور)، وكذلك **المعلومات الحساسة** مثل كلمات المرور أو بيانات الدفع.
2. **التحقق من الهوية:(Authentication)**
   - يستخدم HTTPS **شهادات SSL/TLS** للتحقق من هوية الخادم. عند الاتصال بموقع يستخدمHTTPS ، يقوم الخادم بتقديم شهادة تُصدرها هيئة معترف بها (مثل **Let's Encrypt**أو **Comodo**).
   - هذه الشهادة تضمن للعميل أن الاتصال يتم مع الخادم الصحيح وليس مع مهاجم يحاول التظاهر بأنه الخادم الشرعي (هجوم **Man-in-the-Middle**).
3. **تكامل البيانات:(Data Integrity)**
   - HTTPSيضمن **تكامل البيانات**، مما يعني أن البيانات التي يتم إرسالها بين العميل والخادم لا يمكن تعديلها أو تلفها أثناء النقل.
   - يتم استخدام **التوقيع الرقمي** في إطار بروتوكول SSL/TLS لضمان أن المحتوى المرسل هو نفسه المحتوى الذي استلمه الطرف الآخر.
4. **تحسين تصنيف محركات البحث:(SEO)**
   - محركات البحث مثل **جوجل** تعطي أفضلية للمواقع التي تستخدم HTTPS في تصنيفاتها. هذا يعني أن المواقع التي تستخدم HTTPS يمكن أن تظهر بشكل أعلى في نتائج البحث مقارنةً بالمواقع التي تستخدم HTTPفقط.
   - لذلك، يعد استخدام HTTPS مفيدًا لتحسين أداء الموقع وزيادة زيارته من خلال محركات البحث.
5. **أمان في التعامل مع البيانات الحساسة:**
   - يعتبر HTTPS ضروريًا عندما تتعامل المواقع مع بيانات حساسة مثل المعلومات الشخصية، تفاصيل الدفع، أو أي نوع من البيانات الخاصة. من دونHTTPS ، يكون من الممكن سرقة هذه البيانات بسهولة بواسطة المهاجمين.
6. **الامتثال للمعايير الأمنية:**
   - من خلال استخدامHTTPS ، تلتزم المواقع بمعايير أمان البيانات مثل **GDPR**(اللائحة العامة لحماية البيانات) أو **PCI-DSS**(معيار أمان البيانات في صناعة بطاقات الدفع)، التي تشترط استخدام أمان أقوى عند التعامل مع بيانات المستخدمين الحساسة.

عيوب:HTTPS

1. **زيادة التكلفة:**
   - بعض **شهادات SSL/TLS** تتطلب دفع رسوم سنوية أو لمرة واحدة، وقد تكون هذه التكلفة عبئًا على بعض الشركات الصغيرة أو المواقع.
   - رغم وجود بعض الشهادات المجانية مثل **Let's Encrypt**، إلا أن بعض الشهادات المدفوعة توفر ميزات إضافية مثل التوثيق الموسع (EV) وزيادة الثقة في الموقع.
2. **زيادة تحميل المعالج(Overhead) :**
   - استخدام HTTPS يتطلب عملية **التشفير وفك التشفير** التي تستغرق وقتًا وموارد أكبر من عملية HTTP العادية.
   - عند إرسال طلبات عبرHTTPS ، يجب على الخادم والعميل إتمام **مفاوضات SSL/TLS** التي يمكن أن تضيف بعض التأخير في الاتصال وتستهلك موارد أكثر من.HTTP
3. **التعقيد في الإعداد:**
   - إعداد HTTPS يمكن أن يكون معقدًا، خاصة بالنسبة للأشخاص الذين ليس لديهم خبرة تقنية. يتطلب الأمر شراء شهادة SSL/TLS وتثبيتها بشكل صحيح على الخادم.
   - علاوة على ذلك، يتطلب التأكد من صحة الشهادة وتحديثها بشكل دوري لمنع انتهاء صلاحيتها.
4. **المشاكل مع الشهادات المنتهية:**
   - إذا كانت **شهادة SSL/TLS** قد انتهت أو كانت غير صالحة، سيظهر تحذير أمني للمستخدمين عند محاولة الوصول إلى الموقع، مما يقلل من الثقة ويؤثر سلبًا على سمعة الموقع.
   - في حال كان هناك خطأ في تكوين الشهادة، مثل استخدامها على نطاق غير صحيح، يمكن أن يتسبب ذلك في مشاكل في الاتصال وأخطاء في الأمان.
5. **التحديات في التبديل من HTTP إلى:HTTPS**
   - عند التبديل من **HTTPإلىHTTPS** ، يجب تحديث جميع الروابط داخل الموقع) مثل روابط الصور، الجافا سكريبت، وأوراق الأنماط (CSS للتأكد من أنها تشير إلى .**HTTPS**
   - عدم القيام بذلك يمكن أن يؤدي إلى **محتوى مختلط** (Mixed Content)، حيث يتم تحميل بعض الموارد عبر HTTP بينما يتم تحميل بقية الصفحة عبرHTTPS ، مما يسبب مخاطر أمنية ويؤدي إلى تحذيرات من المتصفح.
6. **تأثير بسيط على أداء الشبكة:**
   - بشكل عام، فإن البروتوكولات الأمنية مثل SSL/TLS تستهلك جزءًا من سرعة الاتصال بسبب عمليات التشفير وفك التشفير، خاصةً في المواقع التي تتعامل مع عدد كبير من الزوار أو البيانات.

3-FTP (File Transfer Protocol) :

FTP (File Transfer Protocol)هو بروتوكول يُستخدم لنقل الملفات بين الخوادم والعملاء عبر شبكة الإنترنت أو الشبكات المحلية. يتيح FTP للمستخدمين تحميل الملفات من أو رفعها إلى الخادم، ويعتبر أحد أقدم وأشهر البروتوكولات في مجال تبادل الملفات عبر الإنترنت.

مزايا:FTP

1. **نقل ملفات كبيرة:**
   - **FTP**يدعم نقل الملفات ذات الحجم الكبير، مما يجعله خيارًا مثاليًا لتبادل البيانات والملفات الكبيرة عبر الإنترنت أو الشبكات الداخلية.
   - يمكن نقل ملفات متعددة في وقت واحد أو إجراء عمليات نقل متوازية، مما يعزز من كفاءة وسرعة نقل الملفات.
2. **إمكانية الوصول السهل:**
   - يمكن للمستخدمين الوصول إلى ملفاتهم عن طريق تطبيقات FTP أو عبر **المتصفحات** التي تدعم بروتوكولFTP ، مثل **FileZilla**أو .**WinSCP**

- يُمكن أيضًا استخدام سطر الأوامر للوصول إلى الخوادم من خلالFTP ، مما يوفر مرونة أكبر في التعامل مع الملفات.

3. **إدارة الملفات:**
   - يدعم FTP إدارة الملفات بسهولة مثل **إنشاء المجلدات، حذف الملفات، تعديل الأذونات، وتنظيم الملفات** على الخوادم البعيدة.
   - يمكن للمستخدمين رفع، تنزيل، وتعديل الملفات مباشرة على الخادم، مما يجعله مثاليًا للمواقع أو الخوادم التي تتطلب تحديثًا مستمرًا للمحتوى.
4. **تبادل الملفات عبر الشبكات المحلية:**
   - يمكن استخدام FTP لتبادل الملفات بين أجهزة الكمبيوتر عبر **الشبكات المحلية** (LAN)وليس فقط عبر الإنترنت، مما يسهل مشاركة الملفات بين المستخدمين في نفس الشبكة.
5. **دعم للعملية التلقائية:(Automation)**
   - يمكن تكامل FTP مع **برمجيات السكربتات** أو **الأنظمة الآلية** لإجراء نقل الملفات تلقائيًا في أوقات معينة أو بشكل دوري. هذه الميزة مفيدة جدًا في البيئات التي تتطلب نقل ملفات مجدول.
6. **دعم لجلسات متعددة:(Multi-session)**
   - يدعم FTP فتح عدة جلسات متوازية، مما يتيح إمكانية نقل عدة ملفات في وقت واحد، وبالتالي تسريع عملية النقل.

عيوب:FTP

1. **عدم الأمان:(Security Issues)**
   - **FTP**يرسل البيانات بما في ذلك أسماء المستخدمين وكلمات المرور بشكل **غير مشفر**، مما يجعلها عرضة للهجمات مثل **هجوم** .(MITM) **Man-in-the-Middle** يمكن للمهاجمين أن يلتقطوا البيانات المرسلة بين العميل والخادم.
   - لحل هذه المشكلة، تم تطوير **FTPS**و) **SFTP**التي تعتمد على (**SSH**كبدائل آمنة لـFTP ، حيث توفر تشفيرًا قويًا لحماية البيانات.
2. **لا يوجد تكامل مع الحوسبة السحابية:**
   - على الرغم من أنه يمكن تكامل FTP مع بعض الأنظمة، إلا أن الاستخدام السائد لتخزين الملفات في **السحابة** مثل Google Drive أو Dropbox قد يقلل من أهميةFTP ، حيث أن هذه الخدمات توفر ميزات أكثر أمانًا وسهولة في الاستخدام.
3. **تحديات في التكوين والإعداد:**
   - إعداد خوادم FTP يتطلب مهارات فنية، حيث يجب على مسؤولي النظام تكوين الأذونات، وتحديد الوصول للمستخدمين، وضبط الإعدادات المناسبة لضمان الأمان.
   - قد يواجه المستخدمون مشاكل في الوصول إلى الخوادم إذا تم تكوين الجدار الناري بشكل غير صحيح أو لم يتم إعداد الخدمة بالشكل السليم.
4. **محدودية نقل البيانات بين الشبكات المختلفة:**
   - بينما يعمل FTP بشكل جيد عبر الشبكات المحلية، قد يواجه مشاكل في بعض البيئات الشبكية مثل الشبكات **المعزولة خلف جدران نارية أوNAT** ، حيث قد يتعذر الوصول إلى الخوادم بدون تكوين صحيح للبوابات أو المنافذ.
5. **عدم دعم التوثيق المتقدم:**
   - بروتوكول FTP التقليدي لا يدعم تقنيات التوثيق المتقدمة مثل **التوثيق متعدد العوامل** (MFA)، مما قد يجعل الوصول إلى الخوادم أقل أمانًا.
6. **مشاكل في نقل الملفات عبر الجدران النارية:**
   - **FTP**يمكن أن يواجه مشاكل في البيئات التي تحتوي على جدران نارية أو بروكسيات تحظر بعض أنواع الاتصال أو تمنع الوصول إلى المنافذ المستخدمة من قبل البروتوكول (مثل المنفذ 21).

4-SMTP (Simple Mail Transfer Protocol) :

SMTP (Simple Mail Transfer Protocol)هو بروتوكول يُستخدم لإرسال رسائل البريد الإلكتروني بين الخوادم عبر الإنترنت. يتم استخدامه لنقل البريد الإلكتروني من جهاز العميل إلى خوادم البريد الإلكتروني) مثلGmail ، Yahoo، Outlook)أو بين خوادم البريد الإلكتروني نفسها.

مزايا:SMTP

1. **إرسال البريد الإلكتروني عبر الإنترنت:**
   - **SMTP**هو البروتوكول الأساسي المسؤول عن إرسال رسائل البريد الإلكتروني من المرسل إلى الخادم، ومن ثم إلى المتلقي.
   - يعمل بشكل موثوق في نقل الرسائل عبر الشبكات المختلفة باستخدام **خوادم البريد الإلكتروني**.
2. **دعم لعدة أنواع من البيانات:**
   - SMTPيمكنه إرسال **النصوص**، و **الصور**، و **المرفقات** مثل الملفات الصوتية، الفيديو، والصور، وذلك عندما يُدمج مع بروتوكولات أخرى مثل .(Multipurpose Internet Mail Extensions) **MIME**
   - يعمل SMTP مع العديد من الأنواع المختلفة للبيانات لتنسيق الرسائل البريدية بالشكل المطلوب.
3. **دعم الرسائل الجماعية:**
   - يُمكن للبروتوكول إرسال البريد الإلكتروني إلى عدة مستلمين في وقت واحد، مما يُسهل **إرسال رسائل جماعية** أو حملات تسويقية عبر البريد الإلكتروني.
4. **دعم التحقق من الهوية(Authentication) :**
   - بروتوكولات **SMTP Auth**تُمكن المستخدمين من التحقق من هويتهم عند إرسال الرسائل. هذا يساهم في منع استخدام الخوادم لإرسال البريد العشوائي (Spam) أو الهجمات الإلكترونية.
5. **البساطة في التنفيذ:**
   - **SMTP**هو بروتوكول بسيط يعتمد على نصوص أوامر لتنظيم وإرسال الرسائل عبر الخوادم. بفضل هذه البساطة، من السهل تنفيذه وصيانته في مختلف أنواع بيئات البريد الإلكتروني.
6. **التكامل مع أنظمة البريد الإلكتروني الأخرى:**
   - يعمل SMTP جنبًا إلى جنب مع بروتوكولات أخرى مثل **IMAP** (Internet Message Access Protocol)و **POP3** (Post Office Protocol)لتمكين استلام الرسائل من الخوادم وعرضها على العميل. في حين أن SMTP يختص بالإرسال، فإن **IMAP**و **POP3**يعالجان استلام الرسائل.

عيوب:SMTP

1. **لا يدعم استقبال الرسائل:**
   - **SMTP**مخصص فقط لإرسال البريد الإلكتروني ولا يمكنه استلام الرسائل. يتم استخدام بروتوكولات أخرى مثل **IMAP**و **POP3**لاستلام البريد الإلكتروني وعرضه للمستخدم.
   - لذا، على الرغم من أن SMTP مفيد للإرسال، إلا أنه لا يوفر وظيفة كاملة للبريد الإلكتروني بدون البروتوكولات المساندة الأخرى.
2. **عرضة للبريد العشوائي(Spam) :**
   - نظرًا لأن SMTP لا يحتوي على آليات قوية للتحقق من المرسل، فإنه يمكن أن يُستخدم لإرسال البريد العشوائي. العديد من الخوادم لا تتحقق من هوية المرسل بشكل كافٍ، مما يجعل من السهل استخدام SMTPفي الهجمات.
   - لكن يمكن تقليل هذه المشكلة عبر تقنيات أخرى مثل **SPF** (Sender Policy Framework)و **DKIM** (DomainKeys Identified Mail)و **DMARC**.
3. **عدم وجود تشفير قوي (في بعض الحالات):**
   - في النسخة التقليدية منSMTP ، لا يتم تشفير الرسائل بشكل آمن، مما يجعل من الممكن أن يتم اعتراض الرسائل في الطريق بين العميل والخادم.

- لحل هذه المشكلة، يمكن استخدام **SMTPS** (SMTP Secure) الذي يوفر تشفير الاتصال باستخدام **SSL/TLS**، ولكن ليس كل الخوادم تدعمه بشكل افتراضي.

4. **حجم المرفقات:**
   - في بعض الأحيان، تكون هناك قيود على حجم المرفقات التي يمكن إرسالها عبر **SMTP**، حيث قد تكون بعض الخوادم أو خدمات البريد الإلكتروني تحد من حجم المرفقات لأسباب تتعلق بالأداء أو الأمان.
   - يجب استخدام تقنيات مثل **MIME** لتقسيم الرسائل الكبيرة أو ضغط الملفات قبل إرسالها.
5. **مشاكل في التعامل مع الرسائل المجمعة:**
   - على الرغم من أن SMTP يدعم إرسال رسائل إلى عدة مستلمين، إلا أنه قد يواجه صعوبة في التعامل مع الرسائل المجمعة أو الرسائل التي تحتوي على العديد من المرفقات أو التنسيقات المعقدة. قد تحتاج هذه الحالات إلى تقنيات إضافية لتحسين الأداء والتوافق.
6. **الإعداد المعقد للبعض:**
   - في بعض الأحيان، قد يكون إعداد خوادم **SMTP** معقدًا، خاصة عندما يتعلق الأمر بتوفير مستويات أمان عالية أو عندما يتم استخدامه في بيئات معقدة. قد يتطلب الأمر معرفة تقنية في تكوين الخوادم ومنع الرسائل المزعجة أو الهجمات.

IMAP (Internet Message Access Protocol)-5

IMAP (Internet Message Access Protocol) هو بروتوكول يُستخدم للوصول إلى رسائل البريد الإلكتروني على الخوادم. يتيح **IMAP** للمستخدمين عرض وتنظيم وإدارة رسائل البريد الإلكتروني المخزنة على الخادم من خلال عملاء البريد الإلكتروني مثل **Outlook** أو **Thunderbird** أو **Gmail**.

يختلف **IMAP** عن بروتوكولات أخرى مثل **POP3** (Post Office Protocol) في أنه يسمح بالوصول المتعدد والمتزامن إلى البريد الإلكتروني من أجهزة مختلفة، حيث تبقى الرسائل مخزنة على الخادم بدلاً من أن يتم تنزيلها وتخزينها محليًا.

مزايا:IMAP

1. **الوصول المتعدد:(Multiple Access)**
   - يُمكن للمستخدمين الوصول إلى بريدهم الإلكتروني من عدة أجهزة في وقت واحد (مثل الهاتف المحمول، الكمبيوتر الشخصي، أو الجهاز اللوحي). حيث تظل الرسائل على الخادم، ولا يحتاج المستخدمون إلى تنزيلها على جهاز واحد فقط.
   - هذا مفيد للغاية للمستخدمين الذين يحتاجون إلى الوصول إلى بريدهم من أماكن أو أجهزة مختلفة.
2. **مزامنة الرسائل:**
   - يعمل **IMAP** على **مزامنة جميع الرسائل والإجراءات** بين العميل والخادم. على سبيل المثال، إذا قمت بقراءة رسالة، أو حذف رسالة، أو نقلتها إلى مجلد آخر على جهاز واحد، ستنعكس هذه التغييرات على جميع الأجهزة المتصلة بنفس الحساب.
   - هذه المزامنة التلقائية تجعل **IMAP** الخيار المثالي لأولئك الذين يريدون الوصول إلى بريدهم الإلكتروني بمرونة من أكثر من جهاز.
3. **تنظيم الرسائل على الخادم:**
   - يمكن للمستخدمين تنظيم رسائل البريد الإلكتروني إلى مجلدات على الخادم دون الحاجة إلى تنزيلها إلى جهازهم. يمكن إنشاء مجلدات وتنظيم الرسائل بناءً على الفئات أو الأهمية.
   - هذا يساعد في **إدارة البريد الإلكتروني** بشكل أكثر فعالية ومرونة.
4. **الوصول إلى الرسائل دون الحاجة لتنزيلها بالكامل:**
   - مع **IMAP**، يمكن للمستخدمين معاينة **رؤوس الرسائل** أو **الجزء الأول من الرسالة** دون الحاجة إلى تنزيلها بالكامل.
   - يسمح هذا للمستخدمين بمعرفة محتوى الرسائل بسرعة قبل اتخاذ القرار بتحميل الرسالة بالكامل.
5. **التخزين على الخادم:**

- بما أن الرسائل تبقى على الخادم بدلاً من جهاز العميل، يمكن الوصول إليها في أي وقت من أي جهاز. هذا يُعد مثاليًا للمستخدمين الذين يحتاجون إلى تخزين رسائلهم بشكل دائم، خاصة إذا كان لديهم كمية كبيرة من البريد الإلكتروني.

6. **الدعم لعدد كبير من الرسائل والمجلدات:**
   - يدعم **IMAP** العمل مع **عدد كبير من الرسائل** والمجلدات المختلفة على الخادم. بفضل المزامنة مع الخادم، يتم إدارة الرسائل والمجلدات بكفاءة دون التأثير على المساحة التخزينية المحلية.

عيوب:IMAP

1. **الاعتماد على اتصال الإنترنت:**
   - يتطلب **IMAP** اتصالًا مستمرًا بالإنترنت للوصول إلى البريد الإلكتروني. إذا كان الاتصال بالإنترنت ضعيفًا أو غير متاح، لا يمكن للمستخدم الوصول إلى رسائله.
   - هذا يختلف عن **POP3**، الذي يسمح بتنزيل الرسائل على الجهاز المحلي، بحيث يمكن الوصول إليها لاحقًا بدون الحاجة إلى الاتصال بالإنترنت.
2. **استهلاك مساحة الخادم:**
   - بما أن الرسائل يتم تخزينها على الخادم وليس على جهاز العميل، فإن ذلك يمكن أن يؤدي إلى استهلاك **مساحة الخادم** بسرعة، خاصة إذا كان الحساب يحتوي على كمية كبيرة من الرسائل.
   - في بعض الحالات، قد تفرض **خوادم البريد الإلكتروني** قيودًا على سعة التخزين الخاصة بالحساب، مما يستدعي حذف الرسائل القديمة أو ترحيلها إلى مجلدات أرشيفية.
3. **مقارنة بالـPOP3 :**
   - في **POP3**، يتم تنزيل الرسائل إلى الجهاز المحلي، مما يعني أن المستخدمين لا يحتاجون إلى الاتصال المستمر بالإنترنت للوصول إلى بريدهم الإلكتروني. أما في **IMAP**، فإن المستخدم يجب أن يكون متصلًا بالإنترنت باستمرار للوصول إلى رسائلهم.
   - لذلك، قد يُفضل بعض المستخدمين **POP3** إذا كانوا لا يحتاجون إلى الوصول إلى رسائلهم إلا على جهاز واحد أو إذا كانوا يفضلون تخزين البريد الإلكتروني محليًا.
4. **أداء منخفض في بعض الحالات:**
   - في حال كان هناك **عدد كبير من الرسائل** في الحساب، قد يواجه المستخدم بعض التأخير في التصفح أو تحميل الرسائل على الأجهزة المتصلة. قد يحتاج الخادم إلى وقت أطول لمزامنة البيانات بين الأجهزة المختلفة.
5. **الحد من الوصول إلى بعض الميزات في بعض الخدمات:**
   - في بعض الأحيان قد تحد **خدمات البريد الإلكتروني** من بعض الميزات الخاصة بـ **IMAP**، مثل التقارير التفصيلية أو تخصيص المجلدات، بناءً على نوع الحساب أو الخادم المستخدم.

POP3 (Post Office Protocol version 3)- 6

POP3 (Post Office Protocol version 3) هو بروتوكول يُستخدم لاستلام رسائل البريد الإلكتروني من الخوادم إلى العميل (الجهاز المحلي). يعمل **POP3** بشكل أساسي على تنزيل رسائل البريد الإلكتروني من الخادم إلى جهاز المستخدم (مثل الكمبيوتر أو الهاتف المحمول)، بحيث يمكن للمستخدم قراءتها أو معالجتها دون الحاجة إلى الاتصال المستمر بالإنترنت.

مزايا:POP3

1. **الوصول إلى البريد الإلكتروني دون الحاجة للإنترنت:**
   - بعد تنزيل الرسائل عبر **POP3**، يتم تخزينها محليًا على جهاز المستخدم. هذا يعني أنه يمكن الوصول إلى البريد الإلكتروني وقراءته دون الحاجة إلى الاتصال بالإنترنت.
   - هذه الميزة مفيدة بشكل خاص في البيئات التي يكون فيها الاتصال بالإنترنت غير مستمر أو محدود.
2. **استهلاك أقل للموارد على الخادم:**

- بعد تنزيل الرسائل من الخادم، يتم حذفها عادةً من الخادم (حسب الإعدادات). هذا يقلل من الضغط على الخادم ويمنع تراكم الرسائل، مما يساعد في الحفاظ على مساحة الخادم.
- يكون هذا مثاليًا للأشخاص الذين لا يحتاجون إلى تخزين رسائلهم على الخادم لفترات طويلة.

3. **أداء أسرع عند تحميل الرسائل:**
- نظرًا لأن **POP3** يقوم بتنزيل الرسائل إلى الجهاز المحلي، فإن قراءة الرسائل في المستقبل ستكون أسرع، حيث أن المحتوى موجود على الجهاز المحلي ولن يتطلب الاتصال بالخادم.
- لا يتطلب تحميل الرسائل في كل مرة يقوم المستخدم بفتحها، مما يؤدي إلى تجربة أكثر سلاسة.

4. **التحكم الكامل في البريد الإلكتروني على الجهاز المحلي:**
- يتيح **POP3** للمستخدمين إدارة رسائلهم البريدية تمامًا على جهازهم المحلي، مثل تنظيم الرسائل في مجلدات، وحذف الرسائل، وتصنيفها.
- كل هذه العمليات تتم دون التأثير على الخادم أو الأجهزة الأخرى.

5. **سهولة الإعداد:**
- إعداد **POP3** يكون عادة بسيطًا، ويمكن تكوينه بسهولة على العديد من برامج البريد الإلكتروني) مثل Outlook، Thunderbird، وغيرها.(
- لا يتطلب الإعدادات المعقدة كما في بروتوكولات أخرى مثل **IMAP**.

عيوب:POP3

1. **فقدان الرسائل عند حذفها من الخادم:**
- في حالة تكوين **POP3** بحيث تُحذف الرسائل من الخادم بعد تنزيلها (وهو الخيار الافتراضي في العديد من الحالات)، فإن الرسائل ستكون متاحة فقط على الجهاز المحلي.
- إذا فقدت الجهاز أو حدث خطأ ما فيه، فقد تفقد الوصول إلى هذه الرسائل إلى الأبد.

2. **عدم التزامن بين الأجهزة:**
- **POP3** لا يدعم المزامنة بين الأجهزة المختلفة. بمجرد تنزيل الرسالة إلى جهاز معين، لا تكون الرسالة مرئية على أجهزة أخرى.
- بمعنى آخر، إذا قرأت رسالة أو حذفتها على جهاز واحد، فلن يتم تحديث ذلك على الأجهزة الأخرى التي تتصل بنفس الحساب.
- هذا يعد عيبًا كبيرًا للمستخدمين الذين يحتاجون إلى الوصول إلى البريد الإلكتروني من عدة أجهزة.

3. **لا يتيح تنظيم البريد الإلكتروني عبر الخوادم:**
- في **POP3**، يتم تنزيل الرسائل على الجهاز المحلي، ولا يمكن تنظيمها على الخادم بشكل فعال مثل **IMAP**. لذا، إذا كانت لديك الكثير من الرسائل أو كنت بحاجة إلى تنظيم البريد الإلكتروني باستخدام مجلدات على الخادم، فلن يكون **POP3** مناسبًا.

4. **إدارة البريد الإلكتروني المدمج فقط:**
- **POP3** لا يتيح إدارة الرسائل عبر الخوادم بشكل مرن كما في **IMAP**. في **POP3**، يمكن فقط تنزيل البريد الإلكتروني، وحينما تتم هذه العملية، يتم غالبًا حذف الرسائل من الخادم (إذا لم يتم تكوين الإعدادات لحفظ الرسائل على الخادم).

5. **محدودية التخزين على الخادم:**
- نظرًا لأن الرسائل عادةً ما يتم تنزيلها وحذفها من الخادم بعد التنزيل، فإن هذا قد يكون مناسبًا للمستخدمين الذين لا يحتاجون إلى الوصول إلى رسائلهم القديمة من أماكن متعددة. ولكن في حالة حاجة المستخدمين إلى حفظ الرسائل على الخادم لفترات طويلة، سيكون **POP3** غير ملائم.

DNS (Domain Name System)-7

DNS (Domain Name System) هو نظام يُستخدم لتحويل أسماء النطاقات (مثل www.example.com) إلى عناوين **IP** (مثل 192.168.1.1) التي يستخدمها الإنترنت لتحديد الخوادم والمواقع. ببساطة، هو "دليل الهاتف" للإنترنت، حيث يترجم أسماء النطاقات القابلة للقراءة البشرية إلى عناوين قابلة للفهم من قبل أجهزة الكمبيوتر.

مزايا:DNS

1. **سهولة الوصول إلى المواقع باستخدام أسماء نطاقات:**
   - **DNS**يسمح للمستخدمين باستخدام **أسماء نطاقات** مثل "google.com" بدلاً من الحاجة إلى تذكر عناوين **IP**الرقمية المعقدة لكل موقع على الإنترنت.
   - هذا يسهل التصفح بشكل كبير ويوفر تجربة استخدام مرنة للمستخدمين.
2. **التوزيع اللامركزي للبيانات:**
   - **DNS**يعمل بشكل **لامركزي**، حيث يتم توزيع قواعد البيانات عبر شبكة من **خوادم DNS** حول العالم. هذا يزيد من الكفاءة ويمنح النظام مرونة وموثوقية أكبر في نقل البيانات.
   - يمكن للمستخدمين الوصول إلى الخوادم الأقرب لهم مما يسرع من عملية الاستعلام.
3. **سرعة الوصول إلى المواقع:**
   - نظرًا لأن DNS يعتمد على **ذاكرة التخزين المؤقت** (Cache)في العديد من الخوادم، يمكن تخزين نتائج الاستعلامات مؤقتًا، مما يجعل عملية الوصول إلى المواقع أسرع في المرات التالية.
   - هذا يقلل من الحاجة إلى إجراء استعلامات DNS جديدة لكل طلب.
4. **إدارة وتحويل النطاقات بسهولة:**
   - باستخدام **DNS**، يمكن للمؤسسات إدارة أسمائها النطاقية وتحويلها بسهولة. يمكن إعداد سجلات (**A**لربط النطاق مع عنوان(IP ،) **MX**لتوجيه البريد الإلكتروني(، **CNAME**(لتوجيه النطاقات إلى نطاقات أخرى)، وغيرها من السجلات.
   - هذه السجلات تجعل من السهل تغيير الموقع أو الخادم دون الحاجة لتعديل الإعدادات في كل جهاز عميل.
5. **دعم الأمان(DNSSEC) :**
   - يمكن استخدام **DNSSEC (DNS Security Extensions)**لتحسين الأمان في **DNS**، حيث يضيف طبقات تحقق لضمان أن البيانات التي يتم استرجاعها من DNS هي حقيقية وغير معدلة.
   - هذا يساعد في حماية النظام من الهجمات مثل **التلاعب بالاستعلامات** أو **الهجمات من نوع-Man-in-the-Middle**.
6. **توزيع الأحمال(Load Balancing) :**
   - باستخدام **DNS**، يمكن للمواقع الكبيرة أو الخدمات استخدام **تقنيات توزيع الأحمال** بحيث يتم توجيه المستخدمين إلى خوادم مختلفة بناءً على الموقع الجغرافي أو حالة الخادم.
   - يساعد ذلك في تحسين الأداء وزيادة موثوقية الموقع.

عيوب:DNS

1. **قابلية الهجوم(DNS Attacks) :**
   - **DNS**عرضة لعدة أنواع من الهجمات، مثل:
     - **DNS Spoofing**أو :**Cache Poisoning**حيث يمكن للمهاجمين إدخال بيانات مزيفة في ذاكرة التخزين المؤقت لـ DNS لإعادة توجيه المستخدمين إلى مواقع ضارة.
     - **DDoS (Distributed Denial of Service)**: يمكن مهاجمة خوادم **DNS**عبر هجمات DDoSلإيقاف الخدمات.
   - لكن يمكن تقليل هذه المخاطر باستخدام تقنيات مثل **DNSSEC**لتأمين النظام.
2. **التأخير في الاستعلامات:**
   - **DNS**قد يتسبب في تأخير طفيف في الاتصال بالموقع، حيث أن النظام يقوم بالبحث عن العنوان الصحيح في سلسلة من الخوادم قبل أن يتم الوصول إلى الموقع المطلوب.
   - هذا التأخير عادة ما يكون ضئيلًا، لكن يمكن أن يؤثر على سرعة تحميل الموقع في بعض الحالات.
3. **إدارة معقدة لبعض السجلات:**
   - **إدارة سجلات DNS** قد تكون معقدة في بعض الأحيان، خاصة إذا كانت هناك العديد من السجلات الخاصة بأسماء النطاقات المختلفة.

- قد يحتاج المسؤولون إلى فحص دوري للبيانات والتأكد من دقتها وتحديثها للحفاظ على أداء النظام بشكل جيد.

4. **التخزين المؤقت غير محدث:**
   - **ذاكرة التخزين المؤقت لـ** (DNS Cache) **DNS** يمكن أن تكون قديمة في بعض الأحيان. إذا تم تغيير عنوان IP الخاص بموقع ويب، قد يستمر النظام في توجيه الطلبات إلى العنوان القديم حتى يتم تحديث السجلات عبر الإنترنت.
   - هذا يمكن أن يؤدي إلى بعض المشكلات المؤقتة في الوصول إلى المواقع بعد إجراء تغييرات على الخوادم.
5. **اعتماد على خوادمDNS :**
   - عندما لا يكون لدى المستخدمين خوادم DNS موثوقة أو إذا كانت الخوادم نفسها غير متوفرة، قد لا يتمكنون من الوصول إلى الإنترنت أو إلى المواقع. قد يواجهون مشاكل في الاتصال بالإنترنت في حالة وجود مشاكل في خوادم **DNS**التي يعتمدون عليها.

DHCP (Dynamic Host Configuration Protocol)-8

DHCP (Dynamic Host Configuration Protocol)هو بروتوكول يستخدم لتوزيع إعدادات الشبكة بشكل تلقائي على الأجهزة المتصلة بشبكة معينة. يتضمن ذلك تخصيص **عناوينIP** ، **قناع الشبكة الفرعية، البوابة الافتراضية، خوادم DNS**، وغيرها من الإعدادات التي يحتاجها جهاز الكمبيوتر أو أي جهاز آخر للاتصال بالشبكة.

مزايا:DHCP

1. **التخصيص التلقائي لعناوين:IP**
   - يقوم **DHCP**بتخصيص **عنوان IP** بشكل تلقائي للجهاز عند الاتصال بالشبكة، مما يسهل العملية ويمنع الحاجة لتخصيص العناوين يدويًا.
   - هذا يقلل من الأخطاء البشرية الناتجة عن التخصيص اليدوي ويزيد من كفاءة إدارة الشبكة.
2. **إدارة المركزية لإعدادات الشبكة:**
   - يُمكن للمسؤولين عن الشبكة إدارة إعدادات الشبكة مثل **عناوين IP** و **خوادم DNS** بشكل مركزي عبر خادمDHCP ، مما يسهل تحديث هذه الإعدادات لجميع الأجهزة في الشبكة في وقت واحد.
   - عند إجراء تغييرات في إعدادات الشبكة، يمكن تطبيقها فورًا على جميع الأجهزة بدون الحاجة إلى تعديل يدوي لكل جهاز.
3. **توفير العناوين بشكل ديناميكي:**
   - يسمح **DHCP**بتوزيع العناوين بشكل ديناميكي، حيث يمكن تخصيص عنوان IP جديد للجهاز عند كل اتصال أو بعد فترة معينة.
   - يساعد ذلك في تقليل استهلاك عناوين **IP**الثابتة، مما يجعل من السهل تخصيص العناوين حسب الحاجة.
4. **سهولة إضافة أجهزة جديدة إلى الشبكة:**
   - عندما يتم توصيل جهاز جديد بالشبكة، يقوم **DHCP**بتخصيص عنوان IP جديد للجهاز بشكل تلقائي، مما يجعل عملية إضافة أجهزة جديدة إلى الشبكة أكثر سهولة وأسرع.
   - لا يحتاج المستخدم أو المسؤول إلى إجراء أي إعدادات يدويًا لجهاز جديد للاتصال بالشبكة.
5. **تقليل التعارضات في عناوين:IP**
   - بما أن **DHCP**يقوم بتوزيع العناوين تلقائيًا وفقًا لقواعد محددة ويشمل آلية **إدارة العناوين المحجوزة**، فإن ذلك يقلل من احتمالية حدوث **تعارضات في عناوينIP** ، حيث يتم تجنب تخصيص نفس العنوان لجهازين في نفس الوقت.
6. **إمكانية تخصيص عناوين IP مخصصة للأجهزة المحددة:**
   - يمكن لـ **DHCP**تخصيص عناوين IP ثابتة لأجهزة معينة باستخدام **عناوين MAC** الخاصة بها، ما يسمح بتخصيص عنوان IP دائم لجهاز معين (مثل الخوادم والطابعات).

عيوب:DHCP

1. **التعطيل في حالة تعطل الخادم:**
   - إذا كان خادم **DHCP** لا يعمل أو يعاني من مشكلة، فإن الأجهزة التي تحتاج إلى عنوان IP جديد لن تتمكن من الحصول عليه، مما قد يؤدي إلى انقطاع الاتصال بالشبكة.
   - يمكن أن يكون هذا عائقًا إذا كان الخادم المركزي غير متاح لفترة طويلة أو في حال حدوث خطأ في الشبكة.
2. **القابلية للاختراق والهجمات:**
   - نظراً لأن **DHCP** يعتمد على بروتوكول شبكة غير آمن، فإن النظام قد يكون عرضة لبعض الهجمات مثل **هجوم DHCP Spoofing** ، حيث يمكن لمهاجم أن يحاكي خادم **DHCP** ويوجه الأجهزة إلى خوادم ضارة أو غير موثوقة.
   - يمكن للمهاجمين استغلال هذا النوع من الهجمات لسرقة المعلومات أو تعطيل الشبكة.
3. **إدارة IPs محدودة في الشبكات الكبيرة:**
   - في الشبكات الكبيرة التي تحتوي على العديد من الأجهزة، قد يعاني خادم **DHCP** من تحميل عالي أو يحتاج إلى تكوين معقد لمجموعة واسعة من العناوين.
   - قد تتطلب الشبكات الكبيرة بنية تحتية معقدة وخوادم DHCP متعددة لضمان توزيع العناوين بشكل موثوق.
4. **إمكانية حدوث مشاكل في الاتصال عند انتهاء مدة صلاحية العنوان:**
   - مع **DHCP**، يتم تخصيص **عناوين IP** لفترة زمنية محددة. إذا لم يتم تجديد العنوان قبل انتهائه، قد يحدث انقطاع مؤقت في الاتصال.
   - إذا كانت الشبكة لا تدير عملية التجديد بشكل صحيح، فقد تحدث مشاكل في الوصول إلى الإنترنت أو الخدمات الأخرى.
5. **صعوبة في تتبع الأجهزة:**
   - بما أن **DHCP** يخصص عناوين **IP** بشكل ديناميكي، يصبح من الصعب تتبع الأجهزة استنادًا إلى عنوان IP ثابت. قد تحتاج إلى استخدام وسائل أخرى مثل **عناوين MAC** لتحديد الأجهزة بشكل دقيق.

Telnet-9

Telnet هو بروتوكول قديم يُستخدم للوصول إلى الأجهزة البعيدة عبر شبكة الإنترنت أو الشبكات المحلية. يعمل على توفير واجهة سطر الأوامر للتحكم عن بعد في الأجهزة مثل الخوادم، أجهزة الكمبيوتر، والموجهات (routers) عبر الشبكة. تم تطوير **Telnet** في السبعينات وكان أحد الأدوات الأساسية لإدارة الشبكات قبل ظهور بروتوكولات أكثر أمانًا مثل **SSH**.

مزايا Telnet :

1. **سهولة الاستخدام والإعداد:**
   - يعتبر **Telnet** بسيطًا للغاية في الاستخدام والإعداد. يمكن للمستخدم الاتصال بسهولة بالأجهزة عن بعد باستخدام **اسم المستخدم** و **كلمة المرور** عبر سطر الأوامر، مما يجعله أداة مباشرة وسهلة.
2. **الوصول البعيد:**
   - يوفر **Telnet** وسيلة للوصول إلى الخوادم والأجهزة البعيدة لتنفيذ الأوامر وتشغيل البرامج بدون الحاجة إلى التواجد الفعلي بالقرب منها.
3. **دعم منصات متعددة:**
   - يعمل **Telnet** عبر العديد من أنظمة التشغيل مثل **Windows** و **Linux** و **macOS**، وهو مدعوم بشكل افتراضي في العديد من الأجهزة والخوادم.
4. **أداة مجانية ومفتوحة المصدر:**
   - **Telnet** هو بروتوكول مفتوح المصدر، مما يعني أنه يمكن استخدامه مجانًا على العديد من الأجهزة والأنظمة.
5. **قابلية التخصيص:**
   - يدعم **Telnet** العديد من الأوامر البرمجية التي يمكن تخصيصها لتناسب احتياجات معينة، مما يسمح بإجراء مهام معقدة أو مؤتمتة على الأجهزة البعيدة.

عيوب Telnet :

1. **أمان ضعيف:**
   - أكبر عيب في **Telnet**هو **عدم تشفير الاتصال** .يتم إرسال البيانات (مثل اسم المستخدم وكلمة المرور) بشكل نصي عادي عبر الشبكة، مما يجعله عرضة للسرقة عبر **الهجمات من نوع-Man-in-the Middle** .
   - هذا يعني أنه في حال كانت الشبكة غير مؤمنة، يمكن للمهاجمين التقاط البيانات الحساسة بسهولة باستخدام أدوات مثل **Packet Sniffers**.
2. **عدم وجود طبقات أمان إضافية:**
   - لا يوفر **Telnet**أي نوع من المصادقة المتقدمة أو آليات الأمان الأخرى مثل التحقق الثنائي (2FA) أو التشفير، مما يجعله غير مناسب للاستخدام في البيئات التي تتطلب أمانًا عاليًا.
3. **استخدام محدود في الشبكات الحديثة:**
   - في ظل الوعي المتزايد حول الأمان في الشبكات، **Telnet**قد تم استبداله في العديد من الحالات بـ **SSH (Secure Shell)**الذي يوفر اتصالات مشفرة وآمنة.
   - وبسبب عيوب الأمان، فإن **Telnet**نادرًا ما يُستخدم في الشبكات الحديثة.
4. **نقص في وظائف الرسومات:**
   - **Telnet**هو **بروتوكول نصي فقط** ولا يدعم واجهات رسومية أو بيئات عمل رسومية، مما يعني أنه محدود بالنسبة للمهام التي تتطلب واجهات رسومية أو تطبيقات متقدمة.
5. **تسبب مشاكل في التكوين على الشبكات المعقدة:**
   - قد لا يتوافق **Telnet**بشكل جيد مع شبكات الجدران النارية الحديثة أو الأنظمة التي تحتاج إلى تكوينات معقدة، مما قد يؤدي إلى صعوبة الوصول إلى الأجهزة عبر **Telnet**في بعض الحالات.

10-SSH (Secure Shell)

SSH (Secure Shell)هو بروتوكول يستخدم للوصول إلى أجهزة الكمبيوتر والخوادم عن بعد بشكل آمن. يتيح **SSH** للمستخدمين الاتصال بأجهزة أخرى عبر الشبكة، وتنفيذ الأوامر، وإدارة الملفات، وتصفح النظام، وكل ذلك مع **تشفير** كامل للبيانات لضمان أمان الاتصال. يعد **SSH**بديلاً آمنًا لبروتوكولات غير آمنة مثل **Telnet**و **rlogin**.

مزاياSSH :

1. **أمان عالي (تشفير البيانات):**
   - **SSH**يوفر **تشفيرًا قويًا** لجميع البيانات المرسلة بين العميل والخادم. هذا يعني أن أي معلومات يتم تبادلها، مثل **اسم المستخدم، كلمة المرور**، أو الأوامر، يتم تشفيرها، مما يجعل من الصعب على المهاجمين اعتراضها أو الوصول إليها.
   - يستخدم **SSH**تقنيات تشفير متقدمة مثل **AES**و **RSA**، مما يضمن مستوى أمان عاليًا.
2. **المصادقة المتقدمة:**
   - يدعم **SSH**المصادقة **باستخدام المفاتيح العامة والخاصة**، مما يعزز الأمان أكثر من المصادقة التقليدية باستخدام كلمات المرور فقط.
   - في المصادقة بواسطة **المفاتيح العامة**، يتم توليد زوج من المفاتيح (عامة وخاصة)، ويتم تخزين المفتاح العام على الخادم والمفتاح الخاص على العميل. لا يحتاج المستخدم إلى إدخال كلمة مرور لتسجيل الدخول، فقط استخدام المفتاح الخاص.
3. **الاتصال الآمن عن بعد:**
   - باستخدام **SSH**، يمكن للمستخدمين الوصول إلى الخوادم أو الأجهزة البعيدة وتوفير واجهة سطر أوامر للعمل عليها بشكل آمن.
   - يمكن تنفيذ أوامر النظام، إدارة الملفات، وتشغيل التطبيقات عن بعد بكل أمان، مما يساعد في إدارة الأنظمة بشكل مرن.
4. **دعم التوجيه عبر الأنفاق(Tunneling) :**
   - يدعم **SSH**تقنية **الأنفاق الآمنة(SSH tunneling)** ، التي تسمح بتوجيه البيانات بشكل آمن عبر اتصال غير آمن.

- يمكن استخدام هذه التقنية لتشفير الاتصال بتطبيقات معينة أو نقل البيانات بين الشبكات الخاصة العامة (مثل تصفح الإنترنت أو نقل البيانات عبر الأنفاق).

5. **التحكم في الوصول إلى الأجهزة:**
   - يتيح **SSH**للمسؤولين تكوين **التحكم في الوصول** بدقة باستخدام **المفاتيح العامة** والمصادقة المتقدمة. يمكن تكوين صلاحيات المستخدمين بشكل مرن، مما يجعل من السهل فرض سياسات الأمان.
   - بالإضافة إلى ذلك، يتيح **SSH**إعدادات لتحديد من يمكنه الاتصال بالخوادم وأي الأوامر مسموح بها.
6. **إمكانية نقل الملفات بشكل آمن:**
   - **SSH**يسمح بنقل الملفات بشكل آمن باستخدام أدوات مثل **SCP (Secure Copy Protocol)**و **SFTP (SSH File Transfer Protocol)**.
   - يمكن نقل الملفات بين الخوادم أو الأجهزة بشكل محمي ضد التنصت أو التلاعب.
7. **دعم تعدد الأنظمة:**
   - يعمل **SSH**على العديد من أنظمة التشغيل مثل **Linux**و **Windows**و **macOS**، مما يجعله أداة شائعة جدًا في بيئات متنوعة.

عيوبSSH :

1. **تعقيد الإعداد:**
   - على الرغم من أن **SSH**يوفر أمانًا قويًا، إلا أن تكوينه بشكل صحيح قد يكون معقدًا، خاصة بالنسبة للمستخدمين المبتدئين. يجب تكوين المفاتيح العامة والخاصة بشكل صحيح، وإعداد التوثيق، وضبط إعدادات الشبكة.
   - إعداد خوادم **SSH**قد يتطلب بعض الخبرة لضمان تكامل الأمان بشكل صحيح.
2. **استهلاك الموارد:**
   - **SSH**قد يستهلك موارد أكثر مقارنة ببعض البروتوكولات الأخرى مثل **Telnet**، وذلك بسبب الحاجة إلى تشفير البيانات وتبادل المفاتيح.
   - يمكن أن يؤثر ذلك على أداء النظام أو الخوادم في البيئات التي تحتوي على العديد من الجلسات أو الاتصال المستمر.
3. **مخاطر إدارة المفاتيح:**
   - إدارة المفاتيح العامة والخاصة قد تكون عرضة لأخطاء بشرية إذا لم تتم بشكل دقيق. إذا تم تسريب مفتاح خاص أو إذا كان المفتاح الخاص غير آمن، فإن ذلك يشكل خطرًا أمنيًا.
   - من المهم أن يتم تخزين المفاتيح الخاصة بشكل آمن على الأجهزة، وتجنب نقلها عبر وسائل غير آمنة.
4. **الإعداد المتقدم لتوزيع المفاتيح:**
   - إذا كان لديك عدد كبير من الأجهزة أو الخوادم، فإن توزيع المفاتيح العامة قد يكون معقدًا. يتطلب الأمر عمل الكثير من التكوينات اليدوية على العديد من الأنظمة، مما قد يكون مرهقًا.
5. **حاجة إلى الجدران النارية المفتوحة:**
   - يتطلب **SSH**عادة فتح المنفذ 22) المنفذ الافتراضي لـ (SSH في **الجدار الناري**، مما قد يثير بعض المخاوف الأمنية في حالة تعرض المنفذ للهجمات.

الاسئلة الاسترشادية

1- اذكر ثلاثة من مزايا HTTPS (HTTP Secure)
2- اذكر ثلاثة من عيوب HTTPS (HTTP Secure)
3- اذكر ثلاثة من مزايا FTP (File Transfer Protocol)
4- اذكر ثلاثة من عيوب FTP (File Transfer Protocol)
5- اذكر ثلاثة من مزايا SMTP (Simple Mail Transfer Protocol)

6- اذكر ثلاثة من عيوب SMTP (Simple Mail Transfer Protocol)
7- اذكر ثلاثة من مزايا IMAP (Internet Message Access Protocol)
8- اذكر ثلاثة من عيوب IMAP (Internet Message Access Protocol)

المحاضرة الثامنة

طبقة النقل ومفهوم المنافذ

طبقة النقل (Transport Layer) هي الطبقة الرابعة في نموذجOSI ، وتقابلها طبقة النقل في نموذج .TCP/IP تُعد هذه الطبقة مسؤولة عن **توصيل البيانات بين التطبيقات** التي تعمل على أجهزة مختلفة عبر الشبكة، وتحرص على أن تصل البيانات **بشكل موثوق ومنظم**.

المهام الأساسية لطبقة النقل:
1- التحكم في التدفق (Flow Control)

التحكم في التدفق هو إحدى وظائف طبقة النقل في الشبكات، ويهدف إلى **تنظيم معدل إرسال البيانات** بين المرسل والمستقبل حتى لا يتم إرهاق الطرف المستقبل ببيانات لا يستطيع معالجتها بسرعة كافية.

شرح مبسط:

- تخيّل أن المرسل جهاز قوي قادر على إرسال كمية كبيرة من البيانات بسرعة، بينما المستقبل أبطأ ويحتاج وقتًا لمعالجة هذه البيانات.
- **دون التحكم في التدفق**، قد يتم فقدان البيانات إذا لم يستطع المستقبل استيعاب كل شيء في الوقت المناسب.

آلية العمل:

1. **المستقبل يُبلغ المرسل بحجمه الأقصى للبيانات الممكن استقبالها** في كل مرة يعرف ذلك في TCP بمصطلح "Window Size" .
2. **المرسل ينتظر إشارة (Acknowledgment)** من المستقبل قبل إرسال المزيد.
3. في حال امتلاء الذاكرة المؤقتة للمستقبل(Buffer) ، يُوقف المرسل مؤقتًا.

بروتوكولات داعمة:

- في **TCP**، يتم تنفيذ التحكم في التدفق من خلال **Sliding Window Protocol** .
- **UDP**لا يحتوي على ميزة التحكم في التدفق، لذا هو أسرع لكنه غير موثوق.

2-التأكد من التوصيل(Reliability) :
التأكد من التوصيل هو إحدى المهام الأساسية في **طبقة النقل**، ويقصد به ضمان أن البيانات المُرسلة من جهاز ما **تصل كاملة، صحيحة، ومرتّبة** إلى الجهاز الآخر عبر الشبكة.

أهداف التأكد من التوصيل:

1. **عدم فقدان البيانات أثناء النقل.**
2. **اكتشاف الأخطاء وتصحيحها** في حال حدوث تلف في البيانات.
3. **إعادة إرسال الأجزاء المفقودة أو التالفة.**
4. **الحفاظ على ترتيب البيانات** كما أُرسلت.

كيف يتحقق ذلك مثال منTCP :

- **ترقيم الحزم(Sequence Numbers) :**
كل جزء من البيانات يُعطى رقمًا تسلسليًا لضمان ترتيبها.
- **الإقرار(Acknowledgment) :**
المستقبل يُرسل إشعارًا للمرسل بأنه استلم البيانات بنجاح.
- **إعادة الإرسال التلقائي(Retransmission) :**
إذا لم يتلقَّ المرسل إقرارًا خلال وقت معين، يُعيد إرسال البيانات.

3- تقسيم البيانات إلى مقاطع(Segmentation) :
تقسيم البيانات إلى مقاطع هو عملية تقوم بها طبقة النقل لتجزئة الرسائل أو البيانات الكبيرة القادمة من الطبقات العليا (مثل طبقة التطبيق) إلى **أجزاء أصغر** تُسمى **Segments**، لتسهيل إرسالها عبر الشبكة.

لماذا نحتاج إلى التقسيم؟

1. **الشبكات لا تنقل كميات ضخمة دفعة واحدة،** بل تعتمد على إرسال وحدات صغيرة الحجم وفقًا للحد الأقصى لوحدة الإرسالMTU .
2. **تقليل فرص الخطأ،** حيث يسهل اكتشاف وإعادة إرسال مقطع صغير بدلاً من رسالة كبيرة.
3. **تحقيق الكفاءة،** لأن نقل البيانات على شكل مقاطع متتابعة يسهل إدارتها وتتبعها.

ماذا يحدث في التقسيم؟

- يتم إعطاء كل مقطع **رقم تسلسلي**.
- يتم إرسال المقاطع عبر الشبكة.
- عند الوصول، تُجمَّع هذه المقاطع في الطرف المستقبل **لإعادة تشكيل الرسالة الأصلية**.

مثال توضيحي:

لو أردنا إرسال ملف حجمه 10 ميجابايت، فقد تقوم طبقة النقل بتقسيمه إلى:

- 1000مقطع كل منها 10 كيلوبايت.
- كل مقطع يحتوي على جزء من البيانات، بالإضافة إلى رأس (Header) يحدد رقمه التسلسلي ومعلومات التوصيل.

4-التحكم في الأخطاء(Error Control) :
التحكم في الأخطاء هو إحدى وظائف طبقة النقل، ويهدف إلى **اكتشاف وتصحيح الأخطاء** التي قد تحدث أثناء نقل البيانات عبر الشبكة، سواء كانت بسبب ضوضاء، تلف في الحزم، أو فقدان أجزاء من البيانات.

آلية التحكم في الأخطاء تتضمن:

1. **التحقق من صحة البيانات باستخدامChecksum :**
كل مقطع بيانات يُرفق به كود تحقق (Checksum) يتم حسابه عند الإرسال، ويُعاد التحقق منه عند الاستقبال للتأكد من عدم تلف البيانات.
2. **الإقرار(Acknowledgment) :**
المستقبل يُرسل إشعارًا للمرسل بأنه استلم البيانات بدون أخطاء.

3. **إعادة الإرسال(Retransmission) :**
إذا لم يستلم المرسل الإقرار خلال وقت معين، يُفترض أن البيانات ضاعت أو تلفت، فيُعاد إرسالها.
4. **اكتشاف التكرار أو الترتيب الخاطئ:**
يتم استخدام الأرقام التسلسلية (Sequence Numbers) لمنع تكرار البيانات أو إعادة ترتيبها.

الفرق بين TCP و UDP في هذا السياق:

- **TCP** :يحتوي على آليات مدمجة للتحكم في الأخطاء، لذا يُعد بروتوكولًا موثوقًا.
- **UDP** :لا يتضمن هذه الآليات، ويُستخدم في التطبيقات التي تتحمل بعض الفقدان (مثل البث المباشر).

5- تعدد الإرسال(Multiplexing) :
تعدد الإرسال في طبقة النقل هو عملية تُتيح **إرسال بيانات من تطبيقات متعددة في وقت واحد عبر نفس الاتصال الشبكي**، مع ضمان وصول كل جزء من البيانات إلى التطبيق الصحيح عند المستقبل.

كيف يعمل تعدد الإرسال؟

1. كل تطبيق (مثل متصفح، بريد إلكتروني، دردشة...) يُخصص له **رقم منفذ(Port Number) 66.**
2. عندما ترسل البيانات من التطبيقات، تقوم طبقة النقل بإضافة **رأس (Header)** يحتوي على رقم المنفذ المصدر والمنفذ الوجهة.
3. عند الاستقبال، تستخدم طبقة النقل هذه الأرقام لتوجيه البيانات إلى التطبيق المناسب.

مثال:

- المتصفح يستخدم المنفذ 80 عند الاتصال بخادم.HTTP
- تطبيق البريد يستخدم المنفذ 25 أو 587 عند إرسال بريد إلكتروني.
- كل هذه البيانات تمر في نفس الوقت من الجهاز نفسه، ولكن تُفصل وتُوجه بشكل صحيح باستخدام التعدد.

الفرق بين Multiplexing وDemultiplexing :

- **Multiplexingفي المرسل :**تجميع تدفقات بيانات متعددة في قناة واحدة.
- **Demultiplexingفي المستقبل :**تفكيك البيانات المجمعة وتوجيهها للتطبيقات المناسبة.

أشهر البروتوكولات في طبقة النقل:

1-TCP (Transmission Control Protocol) :
بروتوكول **TCP (Transmission Control Protocol)**هو أحد أهم بروتوكولات طبقة النقل في نموذج الإنترنت، ويُستخدم لضمان **نقل البيانات بشكل موثوق، منظم، وخالٍ من الأخطاء** بين الأجهزة المتصلة بالشبكة.

مثال على استخدامه:

- متصفح الإنترنت عند تحميل صفحة يستخدم TCP للتواصل مع الخادم.
- نقل الملفات عبرFTP .

- إرسال البريد الإلكتروني باستخدامSMTP .

2-UDP (User Datagram Protocol) :

بروتوكول UDP بروتوكول بيانات المستخدم (هو بروتوكول اتصال يُستخدم عبر الإنترنت لنقل البيانات. وهو جزء من مجموعة بروتوكولات الإنترنت(IP) ، ويعمل في طبقة النقل بجانب بروتوكول TCP (بروتوكول التحكم في النقل). فيما يلي بعض النقاط الرئيسية حول بروتوكول:UDP

1. **بروتوكول غير متصل** :يعتبر UDP بروتوكولًا غير متصل، مما يعني أنه لا يحتاج إلى إقامة اتصال قبل إرسال البيانات، وهو عكس بروتوكول TCP الذي يتطلب مصافحة (Handshake) لإنشاء اتصال قبل نقل البيانات.
2. **غير موثوق** :لا يضمن UDP تسليم البيانات بشكل موثوق. يمكن أن تُفقد الحزم أو تُسلم بشكل غير مرتب أو تُكرر. لا توجد آليات للاعتراف أو إعادة الإرسال فيUDP ، مما يجعله أسرع ولكنه أقل موثوقية من.TCP
3. **السرعة** :بفضل طبيعته غير المتصلة والخفيفة، يُعتبر UDP أسرع من .TCP لديه تقليل في التحميل الزائد، ولهذا السبب يُستخدم في التطبيقات التي تكون فيها السرعة أكثر أهمية من الموثوقية.
4. **هيكل الحزمة** :تتكون حزم UDP من رأس وبيانات. يحتوي الرأس على معلومات مثل منافذ المصدر والوجهة، وطول الحزمة، وتحقق من صحة البيانات.(Checksum)
5. **حالات الاستخدام** :يُستخدم UDP عادة في التطبيقات التي تحتاج إلى أداء حقيقي في الوقت الفعلي، مثل:
   - **البث المباشر** :تطبيقات الفيديو والصوت و VoIP(الصوت عبر الإنترنت) غالبًا ما تستخدم UDP لأن فقدان البيانات الطفيف يُفضل على التأخير أو التخزين المؤقت.
   - **DNSنظام أسماء النطاقات** :عادة ما تُرسل استفسارات DNS عبر UDP للحصول على استجابات أسرع.
   - **الألعاب عبر الإنترنت** :تستخدم الألعاب متعددة اللاعبين غالبًا UDP للتواصل السريع بين اللاعبين، حيث يكون تأخير الوقت (Latency) أمرًا بالغ الأهمية، ويمكن تحمل فقدان بعض البيانات.
6. **عدم وجود تحكم في التدفق** :لا يحتوي UDP على آليات مدمجة للتحكم في التدفق (مثل تعديل سرعة نقل البيانات بناءً على قدرة المستقبل على معالجتها) أو التحكم في الازدحام، على عكس.TCP

باختصار، يُعتبر UDP الأنسب للتطبيقات التي تحتاج إلى السرعة ويمكنها تحمل بعض فقدان البيانات، بينما يُفضل TCP عندما تكون موثوقية البيانات وتكاملها أمرًا بالغ الأهمية.

مفهوم المنافذ

المنافذ (Ports) في الشبكات هي **نقاط افتراضية** تُستخدم لتحديد التطبيقات أو الخدمات التي تعمل على جهاز معيّن، وتُعد جزءًا من آلية الربط بين طبقة النقل مثل TCP أو UDP والتطبيقات المختلفة.

المفهوم ببساطة:

عند إرسال أو استقبال البيانات عبر الإنترنت، لا يكفي معرفة عنوان الـ IP فقط، بل نحتاج أيضًا إلى تحديد **أي تطبيق** أو خدمة على هذا الجهاز يجب أن تُرسل إليه هذه البيانات. هنا يأتي دور المنافذ.

خصائص المنافذ:

1. **تمثَّل بأرقام تتراوح من 0 إلى 65535.**
2. **كل تطبيق أو خدمة تعمل على الجهاز تستمع على رقم منفذ معين.**
3. **يُستخدم المنفذ مع عنوان IP لتكوين ما يسمى "socket" مثل 192.168.1.1:80.**

أنواع المنافذ:

1-المنافذ المعروفة(Well-known ports) :
المنافذ المعروفة هي مجموعة من المنافذ التي تم تخصيصها لخدمات أو تطبيقات معينة على الإنترنت. هذه المنافذ تقع في نطاق الأرقام من **0إلى 1023**، وقد تم تخصيصها من قبل **IANA(الهيئة المعينة لأرقام الإنترنت (**لضمان أن كل تطبيق أو خدمة تستخدم منفذًا محددًا ومعروفًا.

إليك بعض النقاط الرئيسية حول المنافذ المعروفة:

1. **التخصيص المحدد** :كل منفذ معروف يتم تخصيصه لخدمة معينة. على سبيل المثال:
   - **المنفذ 80** :يستخدم عادة لخدمة **HTTP** (HyperText Transfer Protocol)التي تدير تصفح المواقع على الويب.
   - **المنفذ 443** :مخصص لخدمة **HTTPS** (HyperText Transfer Protocol Secure)، الذي يُستخدم للتصفح الآمن للمواقع عبر تشفير البيانات.
   - **المنفذ 21** :مخصص لبروتوكول **FTP** (File Transfer Protocol)لنقل الملفات بين الأنظمة.
   - **المنفذ 25** :يُستخدم لبروتوكول **SMTP** (Simple Mail Transfer Protocol)لإرسال البريد الإلكتروني.
2. **الاستخدام العام** :هذه المنافذ تُستخدم من قبل العديد من التطبيقات والخدمات التي تتطلب الاتصال عبر الإنترنت، مثل:
   - **خوادم الويب.**
   - **البريد الإلكتروني.**
   - **خوادم الألعاب.**
   - **خوادم قواعد البيانات.**
3. **التقيد بالمواصفات** :التطبيقات التي تستخدم المنافذ المعروفة يجب أن تلتزم بتخصيصات هذه المنافذ لتجنب حدوث تعارض بين التطبيقات المختلفة. على سبيل المثال، لا يمكن لتطبيقات غير HTTP أن تستخدم المنفذ 80، إلا إذا كان مصممًا للاستخدام مع هذه الخدمة.
4. **المنافذ المعروفة مقابل المنافذ غير المعروفة** :بجانب المنافذ المعروفة، توجد أيضًا **المنافذ المسجلة** (من 1024 إلى 49151) و**المنافذ الخاصة** أو **العشوائية** (من 49152 إلى 65535). المنافذ المسجلة هي تلك التي يتم تخصيصها لتطبيقات معينة من قبلIANA ، بينما المنافذ العشوائية تُستخدم من قبل التطبيقات لأغراض مؤقتة.
5. **الأمان** :نظرًا لأن المنافذ المعروفة ترتبط بخدمات شائعة، فإنها يمكن أن تكون أهدافًا للهجمات الإلكترونية إذا لم يتم تأمينها بشكل صحيح. على سبيل المثال، يمكن أن تكون خدمات مثل **FTP**و **SMTP**عرضة للهجوم إذا كانت غير محمية.

2-المنافذ المسجلة(Registered ports) :
المنافذ المسجلة هي مجموعة من المنافذ التي تقع ضمن النطاق **من 1024 إلى 49151** .تم تخصيص هذه المنافذ من قبل **IANAالهيئة المعينة لأرقام الإنترنت** لخدمات وتطبيقات معينة لا تتطلب الاستخدام الحصري كما هو الحال مع **المنافذ المعروفة(Well-known ports)** ، ولكنها لا تزال تستخدم بشكل شائع لتطبيقات خاصة أو برامج معينة.

النقاط الرئيسية حول المنافذ المسجلة:

1. **التخصيص:**
   - على عكس المنافذ المعروفة التي يتم تخصيصها بشكل صارم للخدمات الأساسية مثل HTTP أوFTP ، يمكن للمنافذ المسجلة أن تُستخدم لتطبيقات وخدمات متعددة غير محصورة في نوع واحد.
   - يمكن أن تُستخدم هذه المنافذ من قبل الشركات أو التطبيقات لتقديم خدمات معينة، وتتم عملية التسجيل لدى IANAلضمان أن هذه المنافذ تُستخدم بطريقة منظمة وتجنب التعارض مع تطبيقات أخرى.
2. **النطاق:**
   - **النطاق** من 1024 إلى 49151.

- هذه المنافذ غير محجوزة لخدمات أو بروتوكولات معينة، ولكنها تتطلب التسجيل لدى IANA ليتم تخصيصها لتطبيق معين.

3. **الأمثلة** :بعض المنافذ المسجلة الشهيرة تشمل:
   - **المنفذ 3306** :يستخدمه **MySQL**نظام إدارة قواعد البيانات.
   - **المنفذ 5432** :يستخدمه **PostgreSQL**نظام إدارة قواعد البيانات.
   - **المنفذ 8080** :يُستخدم في بعض الأحيان بديلًا عن المنفذ 80 في خدمات **HTTP**، خصوصًا عند تشغيل خوادم ويب محلية أو في بيئات تطوير.
4. **الاستخدام:**
   - تُستخدم المنافذ المسجلة لتطبيقات مثل خوادم البريد الإلكتروني) باستثناء SMTP الذي يستخدم المنفذ 25(، خوادم قواعد البيانات، بعض بروتوكولات الألعاب، تطبيقات المراسلة، أو التطبيقات التي تحتاج إلى منفذ ثابت للاتصال.
   - على سبيل المثال، تُستخدم المنافذ المسجلة أيضًا لبرامج مثل **SQL**، **HTTP**البديل**(8080)** ، وبرامج **FTP**الخاصة.
5. **الاختلاف عن المنافذ المعروفة:**
   - لا تتطلب المنافذ المسجلة التخصيص الحصري، لذا يمكن استخدامها من قبل العديد من التطبيقات المختلفة.
   - عكس المنافذ المعروفة التي تُستخدم لخدمات الإنترنت الأساسية، المنافذ المسجلة تُستخدم بشكل رئيسي من قبل تطبيقات أو خدمات غير قياسية، وقد تكون مملوكة لمطورين أو شركات معينة.
6. **التسجيل لدى:IANA**
   - للحصول على منفذ في هذا النطاق، يجب على المطورين أو الشركات التسجيل مع .IANA هذه الخطوة تمنع التعارض بين التطبيقات وتتيح تخصيص المنافذ وفقًا للاحتياجات الخاصة.
   - عملية التسجيل ليست معقدة ولكنها تتطلب تقديم معلومات حول التطبيق والخدمة التي ستستخدم المنفذ.
7. **الأمان:**
   - نظرًا لأن هذه المنافذ تُستخدم لتطبيقات متنوعة، فإن تأمينها يعد أمرًا بالغ الأهمية. يجب مراقبتها وحمايتها من الهجمات المحتملة، خاصة إذا كانت تستخدم لتطبيقات تتعامل مع بيانات حساسة.

3- المنافذ الديناميكية Dynamic أوPrivate :

المنافذ الديناميكية أو المنافذ الخاصة (Private Ports) هي مجموعة من المنافذ التي تقع في النطاق **من 49152 إلى 65535** .يتم تخصيص هذه المنافذ لاستخدامات مؤقتة وعشوائية من قبل التطبيقات والخدمات عندما تحتاج إلى إجراء اتصال عبر الشبكة. وهي تختلف عن المنافذ المعروفة والمسجلة في أنها لا تُخصص لخدمات ثابتة أو محددة مسبقًا.

النقاط الرئيسية حول المنافذ الديناميكية:

1. **التخصيص العشوائي:**
   - تُستخدم المنافذ الديناميكية بشكل أساسي من قبل التطبيقات لاختيار منفذ عشوائي عند الحاجة لإجراء اتصال عبر الشبكة.
   - يتم اختيار هذه المنافذ تلقائيًا بواسطة النظام أو التطبيق عند فتح اتصال جديد، ولا يُشترط أن تكون مرتبطة بخدمة معينة أو ثابتة.
2. **النطاق:**
   - **النطاق** :من 49152 إلى 65535.
   - نظرًا لكونها "ديناميكية" أو "عشوائية"، يُمكن استخدامها بشكل موقت من قبل التطبيقات لإجراء اتصالات مؤقتة.
3. **الاستخدام:**
   - تُستخدم هذه المنافذ من قبل الأنظمة والتطبيقات لإنشاء **اتصالات قصيرة الأمد** أو **مؤقتة**.
   - **الاتصالات الصادرة** :عندما يقوم جهاز ما (مثل الكمبيوتر أو الهاتف المحمول) بالاتصال بخادم، فإنه عادةً ما يستخدم منفذًا ديناميكيًا لا يُحدّد مسبقًا من قبل التطبيق.

- **البروتوكولات مثل HTTP** أو **SMTP**قد تستخدم المنافذ المعروفة (مثل 80 أو 25)، بينما تستخدم الأنظمة هذه المنافذ الديناميكية للاتصال بالخوادم وتلقي الاستجابة عبر الإنترنت.
- **البروتوكولات مثل DHCP** (بروتوكول التكوين التلقائي للمضيفات) قد تستخدم المنافذ الديناميكية لإنشاء جلسات مؤقتة.

4. **لا حاجة للتسجيل:**
   - لا يتطلب استخدام المنافذ الديناميكية تسجيلًا لدى **IANA**(الهيئة المعينة لأرقام الإنترنت)، حيث يمكن للتطبيقات استخدام أي منفذ ضمن هذا النطاق بشكل عشوائي.
5. **الاستخدامات الشائعة:**
   - **الاتصالات عبر الشبكة المحلية أو الإنترنت** :على سبيل المثال، عند اتصال جهاز كمبيوتر بخادم أو جهاز آخر عبر الإنترنت، يتم عادة تخصيص منفذ ديناميكي مؤقت (عشوائي) من هذا النطاق.
   - **البروتوكولات مثل :(NAT (Network Address Translation** تقوم هذه البروتوكولات باستخدام المنافذ الديناميكية لتوجيه الاتصال عبر الشبكة.
6. **الأمان:**
   - **تعرض أقل للهجمات** :نظرًا لأن هذه المنافذ يتم تخصيصها عشوائيًا، فإنها عادةً ما تكون أقل عرضة للهجمات مقارنةً بالمنافذ المعروفة أو المسجلة، والتي تُستخدم لخدمات ثابتة قد تكون هدفًا للهجمات.
   - مع ذلك، يجب مراقبتها وحمايتها بشكل جيد لأن بعض البرامج الخبيثة قد تحاول استخدام هذه المنافذ لتحقيق الاتصال بالخوادم البعيدة.

المنافذ الديناميكية تُستخدم بشكل رئيسي للاتصالات المؤقتة والعشوائية من قبل التطبيقات، ولا يتم تخصيصها لخدمات ثابتة. توفر هذه المنافذ المرونة في تخصيص الاتصال عبر الشبكة، مما يساعد على تجنب حدوث تعارضات بين التطبيقات والخدمات المختلفة.

مثال توضيحي:

- عند تصفح موقع ويب، يُرسل المتصفح طلبًا إلى خادم الموقع على **المنفذ 80**)إذا كان (HTTP أو) **443**إذا كان HTTPS).
- في الوقت نفسه، يُنشئ المتصفح منفذًا عشوائيًا على جهازك لاستقبال الرد.

أمثلة عملية باستخدام أوامر شهيرة لفحص المنافذ.

1- باستخدام أمر netstat لفحص المنافذ المفتوحة محليًا

على Windows أو:Linux

netstat -an

- يعرض كل المنافذ المفتوحة والاتصالات النشطة.
- الخيار a-يعرض كل الاتصالات والمنافذ المستمعة.
- الخيار n-يعرض الأرقام بدون ترجمتها لأسماء.

لإظهار التطبيقات المرتبطة بالمنافذ:

bash
CopyEdit
netstat -anb

ستحتاج إلى تشغيل الأمر كـ **مسؤول.(Administrator)**

2- باستخدام telnetلاختبار منفذ على جهاز بعيد

telnet www.example.com 80

- يحاول الاتصال بموقع معين عبر المنفذ 80.(HTTP)
- إذا ظهر لك شاشة فارغة أو رسالة نجاح، فالاتصال نجح.
- إذا ظهرت "Connection refused" أو"Could not open connection" ، فالمنفذ مغلق أو الخدمة غير فعالة.

في ,+Windows 10 قد تحتاج إلى تفعيل telnet عبر:

- لوحة التحكم <البرامج <تشغيل ميزات ويندوز <وضع علامة على."Telnet Client"

3- باستخدام PowerShell لفحص منفذ معيّن:

Test-NetConnection -ComputerName www.google.com -Port 443

- يتحقق من إمكانية الوصول إلى **منفذ 443 (HTTPS)** على موقع.Google
- يعطي نتيجة مفصلة عن الحالة (نجح / فشل).

الاسئلة الاسترشادية

1- اذكر ثلاثة من مهام طبقة النقل
2- اذكر ثلاثة من بروتوكولات طبقة النقل
3- اذكر ثلاثة خصائص المنافذ
4- اذكر ثلاثة من أنواع المنافذ
5- اذكر ثلاثة من استخدامات المنافذ المعروفة
6- اذكر ثلاثة من استخدامات المنافذ الديناميكية

المحاضرة التاسعة

بروتوكول(UDP (User Datagram Protocol

مقدمة:

بروتوكول UDP هو أحد البروتوكولات المستخدمة في طبقة النقل في نموذج **OSI**و **TCP/IP**. يتميز بأنه بروتوكول غير موثوق وغير متصل، مما يعني أنه يرسل البيانات بشكل مباشر دون التحقق من وصولها أو تنظيمها. وقد تم تصميمه لتوفير نقل سريع للبيانات في التطبيقات التي لا تتطلب تحققًا صارمًا من تسليم الحزم. يتميز ببساطته وكفاءته في العديد من السيناريوهات مثل تدفق الفيديو والصوت (VoIP) والألعاب عبر الإنترنت.

خصائص:UDP

- **غير متصل(Connectionless)** :لا يقوم UDP بإنشاء اتصال بين المرسل والمستقبل قبل إرسال البيانات، مما يجعل عملية النقل أسرع وأبسط.
- **غير موثوق(Unreliable)** :لا يضمن UDP تسليم البيانات، فقد تفقد بعض الحزم أو يتم تسليمها بترتيب غير صحيح.
- **السرعة** :نظرًا لأنه لا يتطلب إجراء مصافحة اتصال بين الأطراف، فإن عملية النقل تتم بسرعة أكبر مقارنة ببروتوكولات مثل **TCP**.
- **بروتوكول بسيط** :يحتوي UDP على رأس بسيط يتكون من 8 بايت فقط. في المقابل، يحتوي بروتوكول TCP على رأس أكبر يحتوي على مزيد من المعلومات.
- **التحقق من الأخطاء** :يوفر UDP التحقق من الأخطاء من خلال الـ **checksum** للتحقق من تكامل البيانات التي يتم إرسالها.

المصافحة (Handshake)

هي عملية تفاعل بين جهازين أو طرفين في شبكة، تُستخدم لتأسيس اتصال موثوق بينهما، حيث يتفق الطرفان على كيفية إرسال واستقبال البيانات بطريقة صحيحة وموثوقة. تُعتبر المصافحة جزءًا أساسيًا في العديد من البروتوكولات، مثل **TCP (Transmission Control Protocol)**، لضمان أن الاتصال بين الأجهزة يتم بشكل صحيح وأن البيانات يمكن أن تُنقل بشكل موثوق.

أنواع المصافحة:

1. **المصافحة الثلاثية(Three-Way Handshake)** :هذه هي المصافحة التي يتم استخدامها في **بروتوكولTCP** ، وهي عملية مكونة من ثلاث خطوات لبدء الاتصال بين جهازين. الهدف من هذه المصافحة هو ضمان أن كلا الجهازين جاهزان لتبادل البيانات بشكل آمن وموثوق.

الخطوات:

- **الخطوة 1(SYN (Synchronize** : :
  - عندما يريد جهاز (العميل) الاتصال بجهاز آخر (الخادم)، يبدأ العميل عملية المصافحة بإرسال رسالة SYN إلى الخادم. تتضمن هذه الرسالة رقم تسلسل (Sequence Number) يتم استخدامه في الاتصال. تشير هذه الرسالة إلى أن العميل يرغب في فتح اتصال.
- **الخطوة 2(SYN-ACK (Synchronize-Acknowledge** : :

- في هذه الخطوة، يقوم الخادم برد على رسالة العميل بإرسال رسالة تحتوي على **SYN**لتأكيد رغبته في الاتصال، بالإضافة إلى **ACK** (Acknowledgment)التي تشير إلى أنه استقبل رسالة العميل بنجاح. الرسالة تتضمن رقم تسلسل جديد تم تحديده من قبل الخادم.

- **الخطوة 3(ACK (Acknowledge** : :
  - بعد أن يتلقى العميل رسالة الخادم، يقوم بالرد برسالة **ACK**، التي تؤكد أن العميل استلم الرسالة وتؤكد إعداد الاتصال بين الطرفين. بعد هذه الخطوة، يصبح الاتصال جاهزًا لنقل البيانات.

المثال:

- **العميل(Client)** :إرسال.SYN
- **الخادم(Server)** :استقبال SYN ثم إرسال.SYN-ACK
- **العميل(Client)** :استقبال SYN-ACK ثم إرسال.ACK

بعد هذه الخطوات الثلاث، يصبح الاتصال بين العميل والخادم مفتوحًا، ويمكن للطرفين بدء نقل البيانات بأمان.

2. **المصافحة في بروتوكولات أخرى:**
   - في **بروتوكولات مثل(UDP (User Datagram Protocol** ، لا يوجد مفهوم المصافحة UDP .هو بروتوكول **غير متصل**، لذا لا يحتاج إلى مصافحة للاتصال بين العميل والخادم.
   - بروتوكولات أخرى مثل(**SSL/TLS**)المستخدمة في (HTTPS)تتطلب أيضًا مصافحة لتأمين الاتصال بين العميل والخادم، وهي تشمل تبادل مفاتيح تشفير ومعلومات التحقق للتأكد من سلامة الاتصال.

أهمية المصافحة:

- **ضمان الاتصال** :المصافحة تضمن أن الاتصال قد تم إنشاؤه بنجاح بين الطرفين وأن كلا الجهازين جاهزان لتبادل البيانات.
- **التأكد من الإعدادات** :أثناء المصافحة، يتفق الطرفان على إعدادات الاتصال مثل رقم التسلسل، حجم النافذة (Window Size)،والتوقيتات المختلفة.
- **الأمان** :في بعض البروتوكولات مثلSSL/TLS ، يتم استخدام المصافحة لتأمين الاتصال من خلال التحقق من هوية الطرفين وتبادل المفاتيح الخاصة بالتشفير.

مزايا المصافحة:

1. **التحقق من الجهوزية** :تضمن المصافحة أن كلا الطرفين جاهزان لتبادل البيانات.
2. **إعداد اتصال موثوق** :تجعل المصافحة الاتصال أكثر موثوقية من خلال التحقق من رقم التسلسل وسلامة البيانات.
3. **تحسين الأمان** :في بعض البروتوكولات، تساهم المصافحة في حماية البيانات عبر التحقق من الهوية وتبادل المفاتيح السرية.

عيوب المصافحة:

1. **زيادة الوقت** :المصافحة تتطلب تبادل عدة رسائل بين الطرفين قبل بدء نقل البيانات، مما قد يؤدي إلى زيادة وقت التأخير (Latency) في بعض الحالات.
2. **التعقيد** :في بعض الحالات، قد تكون المصافحة معقدة وتتطلب تنسيقًا دقيقًا بين الطرفين، مما يزيد من تعقيد تصميم البروتوكولات.

المصافحة هي خطوة أساسية في بناء اتصال موثوق وآمن بين الأطراف المتصلة عبر الشبكة. بينما توفر بروتوكولات مثل TCPمصافحة ثلاثية لفتح الاتصال بشكل موثوق، فإن بروتوكولات أخرى قد تستخدم طرقًا مختلفة لضمان الأمان والجودة في تبادل البيانات.

هيكل الحزمة فيUDP :

يتكون الهيكل الأساسي للحزمة في UDP من أربع مكونات رئيسية:

1. **رقم المنفذ المصدر** 16بت
2. **رقم المنفذ الوجهة** 16بت
3. **الطول** (16 بت): يحدد طول بيانات UDP مع رأس الحزمة.
4. **التلخيص(Checksum)** :يتم استخدامه للتحقق من تكامل البيانات.

التلخيص (Checksum) هو آلية تستخدم للتحقق من صحة البيانات أثناء إرسالها عبر الشبكة أو تخزينها. يُستخدم التلخيص للكشف عن الأخطاء التي قد تحدث أثناء عملية النقل أو التخزين، مثل الأخطاء الناتجة عن التشويش في الإشارة أو المشاكل في الأجهزة.

مفهوم التلخيص:

التلخيص هو قيمة عددية يتم حسابها بناءً على البيانات التي سيتم إرسالها أو تخزينها. يتم حساب هذه القيمة عبر خوارزميات رياضية معينة، ثم تُرسل أو تُخزن هذه القيمة مع البيانات. عند وصول البيانات إلى الطرف المستلم، يتم حساب التلخيص مرة أخرى باستخدام نفس الخوارزمية على البيانات المستلمة. إذا كانت القيمتان متطابقتين، فهذا يعني أن البيانات لم تتعرض لأي تغيير أثناء النقل أو التخزين. إذا اختلفت القيمتان، فهذا يشير إلى وجود خطأ في البيانات.

كيفية عمل التلخيص:(Checksum)

1. **حساب التلخيص:**
   - في البداية، يتم تقسيم البيانات إلى وحدات صغيرة (مثل البايتات).
   - ثم تُجمع هذه الوحدات بطريقة معينة باستخدام خوارزمية رياضية.
   - النتيجة النهائية لهذه العملية هي قيمة التلخيص، التي يتم إرسالها مع البيانات أو تخزينها بجانبها.
2. **التحقق من التلخيص:**
   - عند وصول البيانات إلى الطرف المستلم، يتم حساب التلخيص على نفس البيانات.
   - إذا كانت قيمة التلخيص التي تم حسابها متطابقة مع التلخيص المرسل، فهذا يعني أن البيانات لم تتعرض للتلف.
   - إذا كانت القيم غير متطابقة، فهذا يعني أن البيانات قد تعرضت للتلف أثناء النقل أو التخزين، وبالتالي يجب على الطرف المستلم اتخاذ الإجراءات المناسبة.

أنواع التلخيص:(Checksum)

1. **تلخيص بسيط:**
   - يقوم بجمع قيم البايتات في البيانات وتطبيق بعض العمليات الرياضية البسيطة عليها. يُستخدم هذا النوع في حالات بسيطة حيث لا تكون الأخطاء المحتملة كبيرة.
2. **تلخيص متقدم) مثل:(CRC**

- يستخدم **فحص التكرار الدوري(Cyclic Redundancy Check)** ، وهو من أنواع التلخيص الأكثر تطورًا، ويعتمد على تطبيق العمليات الرياضية الأكثر تعقيدًا للكشف عن الأخطاء. يُستخدم **CRC**في العديد من التطبيقات مثل شبكات الاتصال، الأقراص الصلبة، وأجهزة النقل.

3. **تلخيص في بروتوكولات الشبكة:**
   - يتم استخدام التلخيص في العديد من بروتوكولات الشبكة مثل **UDP**و **TCP**للتحقق من صحة البيانات أثناء إرسالها عبر الشبكة. في حالة بروتوكولUDP ، يتم تضمين التلخيص في رأس الحزمة للتحقق من البيانات.

دور التلخيص في بروتوكولات الشبكة:

1. **UDP (User Datagram Protocol):**
   - في **UDP**، يتم تضمين التلخيص في كل حزمة بيانات مرسلة للتحقق من تكامل البيانات. إذا كانت الحزمة تحتوي على أخطاء أثناء النقل، يتم تجاهلها ولا يتم تسليمها إلى التطبيق.
2. **TCP (Transmission Control Protocol):**
   - في **TCP**، يُستخدم التلخيص أيضًا للتحقق من البيانات أثناء عملية النقل. يُضاف التلخيص إلى كل حزمة بيانات مرسلة، ويتم التحقق منه عند وصول الحزمة إلى الطرف المستقبل.
   - TCPيتعامل مع الأخطاء بشكل مختلف عنUDP ، حيث يضمن إعادة إرسال الحزم التي تحتوي على أخطاء (عبر آلية **إعادة الإرسال**.(

أهمية التلخيص:

1. **اكتشاف الأخطاء:**
   - التلخيص يُستخدم لاكتشاف الأخطاء التي قد تحدث أثناء النقل، مثل الأخطاء الناتجة عن تداخل الإشارة أو الفشل في الأجهزة. إذا تم اكتشاف أن البيانات تحتوي على أخطاء، يتم طلب إعادة الإرسال في بعض البروتوكولات مثل.TCP
2. **تحقيق التكامُل:**
   - التلخيص يضمن أن البيانات التي يتم نقلها أو تخزينها لم تتعرض لتغييرات غير متوقعة، مما يزيد من موثوقية النظام.
3. **تحسين الأمان:**
   - على الرغم من أن التلخيص لا يضمن أمانًا كاملاً ضد الهجمات مثل التلاعب بالبيانات (أو **الاختراقات**(، فإنه يساعد في تقليل الأخطاء الناتجة عن الفشل في الأجهزة أو الشبكات.

التحديات والعيوب:

1. **القدرة المحدودة على الكشف عن الأخطاء:**
   - على الرغم من أن التلخيص يمكنه اكتشاف العديد من الأخطاء، إلا أنه قد يفشل في اكتشاف بعض الأنواع من الأخطاء المعقدة. في بعض الأحيان، قد تتسبب الأخطاء في تغييرات في البيانات لا تؤثر بشكل كافٍ على التلخيص وبالتالي يتم قبول البيانات غير الصحيحة.
2. **الكفاءة:**
   - الحسابات المتعلقة بالتلخيص قد تؤدي إلى زيادة الضغط على النظام في بعض الحالات، خاصة إذا كانت البيانات كبيرة جدًا أو إذا كان النظام يستخدم خوارزميات معقدة مثل .**CRC**
3. **التحقق الجزئي فقط:**
   - التلخيص لا يضمن بالضرورة اكتشاف كل الأخطاء، حيث إنه يقوم فقط بالتحقق من صحة البيانات عبر حساب التلخيص الخاص بها. قد تحدث بعض الأخطاء التي لا تؤثر على قيمة التلخيص، وبالتالي لا يتم اكتشافها.

التلخيص في العالم الحقيقي:

- في **البروتوكولات** مثل **TCP**و **UDP**، يساهم التلخيص في ضمان أن البيانات تُنقل بشكل صحيح وآمن بين الأجهزة.
- في **أجهزة التخزين** مثل الأقراص الصلبة أو الأقراص المدمجة، يُستخدم التلخيص لضمان أن البيانات التي تُقرأ من الجهاز أو تُكتب عليه سليمة وصحيحة.
- في **تطبيقات البث المباشر**، مثل الفيديو عبر الإنترنت أو الصوت عبر الإنترنت(VoIP) ، يُستخدم التلخيص للتحقق من سلامة البيانات المرسلة عبر الشبكة.

التلخيص هو أداة أساسية لضمان تكامل البيانات أثناء النقل أو التخزين. على الرغم من أن التلخيص قد لا يكون قادرًا على اكتشاف جميع أنواع الأخطاء، فإنه يعد أداة قوية وفعالة للكشف عن الأخطاء البسيطة ويحسن موثوقية النظام. في الشبكات، يعتبر التلخيص مكونًا حيويًا في البروتوكولات مثل **UDP**و **TCP**لتحقق من صحة البيانات وسلامتها.

تعتبر هذه الهيكلية بسيطة جدًا مقارنةً بـTCP ، ما يجعل UDP أكثر كفاءة في الاستخدام في التطبيقات التي تحتاج إلى السرعة ولا تهتم بالموثوقية التامة.

مميزاتUDP :

- **السرعة والكفاءة** :بما أنه لا يتطلب مصافحة أو إدارة لحالة الاتصال، فإن UDP يرسل البيانات بسرعة كبيرة.
- **البساطة** :هيكل رأس UDP بسيط ويحتاج إلى قدر ضئيل جدًا من المعالجة على مستوى الشبكة.
- **التوافق مع تطبيقات الزمن الحقيقي** UDP :مثالي للتطبيقات التي تحتاج إلى التأخير المنخفض مثل الصوت والفيديو عبر الإنترنت، حيث أن تأخير المعالجة قد يكون أكثر ضررًا من فقدان بعض الحزم.
- **مرونة الاستخدام** :يمكن للتطبيقات استخدام UDP لنقل البيانات بين الأجهزة بسهولة دون الحاجة إلى تعقيدات الإعدادات التي يتطلبها بروتوكول.TCP

عيوبUDP :

- **عدم ضمان التسليم** :أحد أكبر العيوب هو أنه لا يتم ضمان تسليم البيانات أو ترتيبها بشكل صحيح. إذا فقدت حزمة بيانات أثناء النقل، فلن يتم إعادة إرسالها.
- **عدم وجود آلية لتدفق البيانات** :لا يوفر UDP آلية للتحكم في تدفق البيانات، مما يعني أنه قد يتم إرسال كميات ضخمة من البيانات بسرعة كبيرة دون أن يكون هناك أي اعتبار لقدرة المستقبل على التعامل معها.
- **عدم وجود حماية ضد الازدحام** :بروتوكول UDP لا يتضمن آليات لحماية الشبكة من الازدحام، مما قد يتسبب في اختناقات شبكية في بعض الحالات.
- **عدم وجود آلية للتحقق من التسليم** :لا توجد آلية في UDP لمعرفة ما إذا كانت البيانات قد وصلت بنجاح إلى المستقبل. في حالة فقدان الحزمة، لا توجد آلية لتعويض هذا الفقد.

تحديات استخدامUDP :

- **فقدان الحزم** :بما أن UDP لا يضمن التسليم، فإنه من الممكن أن تُفقد بعض الحزم أثناء النقل. هذا يشكل تحديًا في التطبيقات التي تتطلب تسليمًا دقيقًا وموثوقًا.
- **ترتيب الحزم** :في بعض الأحيان قد تصل الحزم في ترتيب غير صحيح. وهذا يمكن أن يكون مشكلة في تطبيقات مثل نقل الملفات أو في الاتصالات التي تتطلب ترتيبًا معينًا للبيانات.
- **التحقق من التكامل** :بينما يتيح UDP التحقق من الأخطاء باستخدام **الـchecksum** ، فإنه لا يوفر أي نوع من التصحيح التلقائي. إذا اكتشف المستقبل أن الحزمة تحتوي على أخطاء، يتم التخلص منها دون إعادة إرسال.
- **الأمان** :بما أن UDP لا يحتوي على آليات أمان مدمجة، فقد يتم استغلاله في بعض الهجمات مثل **الهجمات DDoS**)الهجمات الموزعة لحجب الخدمة.(

حالات الاستخدام المثالية لبروتوكولUDP :

- **تطبيقات الصوت والفيديو** :مثل **VoIP**أو خدمات البث المباشر التي تتطلب إرسال البيانات بسرعة وبدون تأخير، حيث يمكن تحمل فقدان بعض الحزم بدلاً من حدوث تأخير.
- **الألعاب عبر الإنترنت** :الألعاب التي تحتاج إلى التفاعل السريع بين اللاعبين تستفيد من UDP لأنه يتيح نقل البيانات بسرعة دون الحاجة إلى انتظارات إضافية.
- **البروتوكولات مثلDNS** :يُستخدم **DNS**(نظام أسماء النطاقات) بشكل شائع مع UDP بسبب متطلبات السرعة وقلة الحاجة إلى ضمان التسليم.
- **البث الأحادي(Unicast)** :استخدام UDP في تطبيقات البث الأحادي يُمكن أن يكون أكثر كفاءة من TCP في بعض السيناريوهات.

مقارنة بين UDP وTCP :

- **الاتصال** :بينما يتطلب TCP الاتصال قبل إرسال البيانات، فإن UDP لا يحتاج إلى اتصال مسبق.
- **الموثوقية** :يوفر TCP ضمانات بتسليم البيانات بشكل موثوق، بينما لا يوفر UDP هذه الضمانات.
- **التحكم في التدفق** :يحتوي TCP على آليات للتحكم في تدفق البيانات ومنع الازدحام، بينما لا يحتوي UDP على هذه الآليات.
- **التسليم المتسلسل** :يضمن TCP التسليم المرتب للبيانات، بينما قد يصل البيانات في UDP بترتيب غير صحيح.
- **الأداء** :يعد UDP أسرع وأكثر كفاءة في التطبيقات التي تحتاج إلى السرعة على حساب الموثوقية.

تطبيقات بروتوكول UDP في الشبكات:

- **البث المتعدد(Multicasting)** :يمكن لبروتوكول UDP أن يكون مفيدًا في تطبيقات البث المتعدد حيث يتم إرسال نفس البيانات إلى عدة مستلمين في وقت واحد.
- **بروتوكولات الوقت الحقيقي** :مثل **RTP**(بروتوكول نقل الوقت الحقيقي) الذي يستخدم في البث الحي للصوت والفيديو.
- **بروتوكولات نقل الملفات** :في بعض الحالات يمكن استخدام UDP في تطبيقات نقل الملفات عندما تكون السرعة أكثر أهمية من الموثوقية التامة.

تطور UDP في الشبكات الحديثة:

- **UDP-Lite** :هو نوع من UDP الذي يستخدم للتحقق من تكامل جزء من البيانات بدلاً من التحقق من كل الحزمة. يُستخدم في بعض التطبيقات مثل الصوت عبر الإنترنت حيث قد تكون بعض الأخطاء مقبولة.
- **QUIC** :هو بروتوكول جديد تم تطويره بواسطة **Google**يعتمد على UDP ويهدف إلى تحسين سرعة الإنترنت وتقليل تأخيرات الاتصال.

بروتوكول UDP يعد من البروتوكولات الهامة في عالم الشبكات، ويُستخدم في العديد من التطبيقات التي تحتاج إلى سرعة وأداء عاليين. ومع ذلك، فإنه يحمل بعض القيود مثل عدم ضمان تسليم البيانات وعدم وجود آليات للتحقق من الأخطاء أو التحكم في التدفق. هذه العيوب قد تجعل استخدامه غير مناسب لبعض التطبيقات التي تتطلب موثوقية عالية. ومع ذلك، يظل UDP خيارًا مثاليًا في حالات معينة، مثل الصوت والفيديو في الوقت الحقيقي، والألعاب عبر الإنترنت، والتطبيقات التي لا تحتاج إلى ضمانات التسليم.

الاسئلة الاسترشادية

1- اذكر ثلاثة من خصائص بروتوكول(UDP (User Datagram Protocol
2- اذكر استخدامات المصافحة
3- اذكر مزايا المصافحة
4- اذكر عيوب المصافحة
5- اذكر ثلاثة من تطبيقات بروتوكول(UDP (User Datagram Protocol

المحاضرة العاشرة

بروتوكول TCP (بروتوكول التحكم في النقل - Transmission Control Protocol) هو أحد البروتوكولات الأساسية في مجموعة بروتوكولات TCP/IP، ويُستخدم لضمان نقل البيانات بشكل موثوق ومنظم بين الأجهزة على الشبكة.

خصائص بروتوكول TCP:

1. موثوقية (Reliable):

- يضمن وصول البيانات كاملة دون أخطاء أو فقدان.

- يستخدم آلية التأكيدات (ACKs) لتأكيد استلام الحزم.

- يعيد إرسال الحزم المفقودة أو التالفة.

2. اتصالي (Connection-Oriented):

- ينشئ اتصالاً (Session) بين المرسل والمستقبل عبر مصافحة ثلاثية (Three-Way Handshake):

1. SYN: يرسل العميل طلب اتصال.
2. SYN-ACK: يستجيب الخادم بالموافقة.
3. ACK: يؤكد العميل الاتصال.

مُزامَنة SYN

هو أحد **أعلام التحكم (Flags)** في رأس حزمة **بروتوكولTCP** ، ويُستخدم لبدء إنشاء اتصال بين جهازين عبر **المصافحة الثلاثية.(Three-Way Handshake)**

وظيفة حزمة:SYN

1. **بدء الاتصال:**
   - عندما يريد العميل (Client) الاتصال بالخادم(Server) ، يرسل حزمة تحتوي على علم **SYN=1**مع رقم تسلسل عشوائي.(**Sequence Number**)
   - مثال:

1. Copy
2. Download

```
Client → Server: SYN=1, Seq=X
```

2. **استجابة الخادم:(SYN-ACK)**
   - يرد الخادم بحزمة تحتوي على:

- **SYN=1** لبدء اتصاله الخاص.
- **ACK=1** لتأكيد استلام SYN الأول.
- **Acknowledgment Number = X+1** رقم التأكيد.
- **Sequence Number = Y** رقم تسلسل جديد من الخادم.

- مثال:

1. Copy
2. Download

```
Server → Client: SYN=1, ACK=1, Seq=Y, Ack=X+1
```

3. **تأكيد العميل:(ACK)**

- يرسل العميل حزمة تأكيد نهائية تحتوي على:
  - **ACK=1** مع **Acknowledgment Number = Y+1.**
- مثال:

1. Copy
2. Download

```
Client → Server: ACK=1, Ack=Y+1
```

- بعد هذه الخطوة، يصبح الاتصال **مُنشئًا (Established)** وجاهزًا لنقل البيانات.

أهمية SYN :

- **ضمان الموثوقية** :تُجنب المصافحة الثلاثية فقدان الحزم أو إنشاء اتصالات غير مرغوب فيها.
- **مزامنة الأرقام التسلسلية** :يتم تبادل أرقام **Seq** و **Ack** لترتيب الحزم وتجنب التضارب.

هجمات تستغل SYN :

- **هجوم SYN Flood** :
  - يقوم المهاجم بإرسال عدد هائل من حزم **SYN** دون إكمال المصافحة (بدون إرسال **ACK** النهائي)، مما يُرهق موارد الخادم ويؤدي إلى **رفض الخدمة(DoS)** .
  - **الوقاية** :استخدام **SYN Cookies** أو جدران الحماية.(Firewalls)

تأكيد الاستلام ACK Acknowledgment في بروتوكولTCP

ACKهو أحد **أعلام التحكم (Flags)** في رأس حزمة **TCP**، ويُستخدم لتأكيد استلام البيانات بشكل موثوق بين المرسل والمستقبل. يعتمد عليه **TCP**لضمان عدم فقدان الحزم وتصحيح الأخطاء تلقائيًا.

وظيفة حزمةACK

- **تأكيد استلام البيانات:**
  عندما يستقبل جهاز ما حزمة بيانات(Segment) ، يرسل حزمة **ACK**تحتوي على رقم التأكيد (**Acknowledgment Number**)الذي يُشير إلى أن جميع البيانات حتى هذا الرقم قد تم استلامها بنجاح.
- **المساعدة في التحكم في التدفق:(Flow Control)**
  يُستخدم **ACK**لتحديد سرعة إرسال البيانات بناءً على حجم النافذة (**Window Size**) المعلن من المستقبل.

كيف يعملACK ؟

أ) في المصافحة الثلاثية(Three-Way Handshake)

1. **العميل** → **الخادم**SYN=1, Seq=X :
2. **الخادم** → **العميل** ← SYN=1, ACK=1, Seq=Y, Ack=X+1 :هنا يُرسل الخادم **ACK**لتأكيد استلام **SYN**الأول.
3. **العميل** → **الخادم** ← ACK=1, Ack=Y+1 :يُرسل العميل **ACK**لتأكيد اكتمال الاتصال.

ب) أثناء نقل البيانات

- إذا أرسل **الخادم** بيانات إلى العميل:

1. Copy
2. Download

```
Server → Client: [Data], Seq=100, Len=50
Client → Server: ACK=1, Ack=150 (150 = 50 + 100 لأن)
```

  - الرقم **150**يعني: "لقد استلمت كل البيانات حتى الرقم 149، أرسل لي البيانات بدءًا من 150."

أنواع آلية التأكيد(ACK Mechanisms)

الوصف	النوع
يُرسل ACK لكل حزمة بيانات (غير فعال في الشبكات السريعة).	**التأكيد الفردي(Simple ACK)**
يُرسل ACK واحد لتأكيد استلام مجموعة من الحزم) مثل.(TCP	**التأكيد التجميعي(Cumulative ACK)**
يُحدد الحزم المفقودة بدقة (يُستخدم في الشبكات ذات الأداء العالي).	**التأكيد الانتقائي(Selective ACK - SACK)**

هجمات تستغلACK

- **هجوم:ACK Flood**
  - يقوم المهاجم بإغراق الخادم بحزم **ACK**زائفة لاستنزاف موارده.
  - **الوقاية** :استخدام جدران الحماية (Firewalls) وكشف الأنماط غير الطبيعية.
- **استغلال ACK في هجمات انتحال الهوية:(Spoofing)**
  - قد يُستخدم **ACK**لتأكيد اتصالات مزيفة في هجمات **Man-in-the-Middle**.

3. تحكم في التدفق (Flow Control):

- يتحكم في معدل إرسال البيانات لمنع ازدحام الشبكة.

- يستخدم آلية نافذة التدفق (Sliding Window).

نافذة التزحلق (Sliding Window) في بروتوكول TCP

نافذة التزحلق (Sliding Window) هي آلية ذكية يستخدمها بروتوكول TCP لتحسين كفاءة نقل البيانات عبر الشبكة، حيث تسمح بإرسال عدة حزم بدون انتظار تأكيد (ACK) لكل حزمة على حدة، مما يزيد من سرعة نقل البيانات ويقلل التأخير.

1. كيف تعمل نافذة التزحلق؟

تقسّم آلية Sliding Window البيانات إلى حزم مرقمة، وتتحكم في عدد الحزم التي يمكن إرسالها قبل الحاجة إلى انتظار تأكيد الاستلام (ACK).

المكونات الأساسية:

- نافذة الإرسال (Send Window) عدد الحزم التي يمكن إرسالها دون انتظار تأكيد.
- نافذة الاستقبال (Receive Window) المساحة المتاحة في ذاكرة المستقبل لتخزين البيانات الواردة.
- حد النافذة (Window Size) يُعلن عنه المستقبل لتجنب إغراقه بالبيانات (Flow Control).

آلية العمل:

1. المرسل (Sender) يرسل مجموعة من الحزم ضمن نطاق النافذة المسموح به.

2. المستقبل (Receiver) يستقبل الحزم ويُرسل ACK مع رقم التأكيد (Acknowledgment Number) وحجم النافذة الجديد.

3. عند استلام ACK، تنزلق النافذة للأمام (Slides Forward) لتحرير مساحة لإرسال حزم جديدة.

2. مثال توضيحي لنافذة التزحلق

لنفترض أن:

- حجم النافذة (Window Size) = 5 حزم (يمكن إرسال 5 حزم قبل انتظار ACK).

- أرقام التسلسل (Sequence Numbers) تبدأ من 1.

الخطوة	الإجراء	النافذة (الحزم المرسلة)	حالة ACK
1	إرسال الحزم 1، 2، 3، 4، 5	[1، 2، 3، 4، 5]	في الانتظار
2	استلام ACK=3 (تم استقبال حتى الحزمة 2)	تنزلق النافذة → [3، 4، 5، 6، 7]	يُرسل 6,7
3	استلام ACK=6 (تم استقبال حتى الحزمة 5)	تنزلق → [6، 7، 8، 9، 10]	يُرسل 8,9,10

3. فوائد نافذة التزحلق

1. زيادة الإنتاجية: إرسال عدة حزم دون انتظار تأكيد لكل واحدة.
2. التحكم في التدفق (Flow Control): يتكيف مع سعة الشبكة والجهاز المستقبِل.
3. التحكم في الازدحام (Congestion Control): يقلل حجم النافذة عند اكتشاف ازدحام.

4. مشاكل محتملة وحلولها

أ) فقدان حزمة ACK

- الحل: إعادة الإرسال بعد انتهاء المهلة (Timeout).

ب) نافذة استقبال صغيرة (Zero Window)

- إذا كان حجم نافذة المستقبل = 0، يتوقف المرسل حتى يُرسل المستقبل Window Update.

ج) ازدحام الشبكة (Congestion)

- يُقلل TCP حجم النافذة تدريجياً باستخدام خوارزميات مثل:

- Slow Start → Congestion Avoidance → Fast Retransmit.

5. نافذة التزحلق في Wireshark

عند تحليل حزم TCP في Wireshark، يمكن رؤية:

- Window Size في رأس TCP.

- تغيير حجم النافذة بناءً على ظروف الشبكة

6. الفرق بين Sliding Window و Stop-and-Wait

المعيار	نافذة التزحلق (Sliding Window)	انتظر ثم أرسل (Stop-and-Wait)
الكفاءة	عالية (إرسال متعدد بدون انتظار)	منخفضة (انتظار ACK بعد كل حزمة)
الاستخدام	TCP (الاتصالات الحديثة)	نادرًا (في أنظمة بسيطة)

7. الخلاصة

- Sliding Window آلية أساسية في TCP لتحسين الأداء.

- تمنع إغراق المستقبل بالبيانات (Flow Control).

- تتكيف مع ظروف الشبكة (Congestion Control).

- تُستخدم في كل الاتصالات الحديثة مثل التصفح والبث.

4. تحكم في الازدحام (Congestion Control):

- يقلل من معدل الإرسال عند اكتشاف ازدحام في الشبكة.

5. ترتيب الحزم (Sequencing):

- يرقم الحزم لضمان تجميعها بالترتيب الصحيح عند المستقبل.

بنوة رأس TCP (TCP Header):

يحتوي رأس TCP على معلومات مهمة مثل:

- أرقام المنافذ (Port Numbers) (مصدر/وجهة).

- أرقام التسلسل (Sequence & Acknowledgment Numbers).

- أعلام التحكم (Flags) مثل SYN, ACK, FIN, RST.

- حجم نافذة التدفق (Window Size).

استخدامات TCP:

- التصفح عبر HTTP/HTTPS.

- إرسال البريد الإلكتروني عبر SMTP.

- نقل الملفات عبر FTP.

- الاتصالات الآمنة مثل SSH.

عيوب TCP:

- حمل زائد (Overhead) بسبب آلية التحكم والموثوقية.

- غير مناسب للتطبيقات في الوقت الحقيقي (مثل الألعاب أو VoIP) حيث السرعة أهم من الموثوقية.

خاتمة:

يُعد TCP العمود الفقري للإنترنت نظرًا لموثوقيته، لكنه ليس الخيار الأمثل لكل التطبيقات، خاصة تلك التي تحتاج إلى سرعة عالية مع احتمالية فقدان بعض البيانات.

الاسئلة الاسترشادية

1- اذكر أنواع آلية التأكيد(ACK Mechanisms)
2- اذكر مكونات نافذة التزحلق
3- اذكر فوائد نافذة التزحلق
4- اذكر المشاكل المحتمل حدوثها في نافذة التزحلق
5- اذكر أنواع آلية التأكيد(ACK Mechanisms)

المحاضرة الحادية عشر

العنونة في IPv4

IPv4 (الإصدار الرابع من بروتوكول الإنترنت) هو النظام الأساسي لتحديد الأجهزة على الشبكة باستخدام عناوين فريدة. إليك شرح مفصل لعنونة IPv4:

1. هيكل عنوان IPv4

- الطول: 32 بت (4 بايت)، مُقسَّمة إلى 4 أجزاء (أوكتيتات) تفصل بينها نقاط.

- مثال: `192.168.1.1`.

- التنسيق الثنائي: كل أوكتيت يمثل 8 بت (مثال: `192` → `11000000`).

2. فئات عناوين IPv4

تنقسم عناوين IPv4 إلى 5 فئات رئيسية:

الفئة	النطاق	الاستخدام	الشبكة/المضيف
A	1.0.0.0 – 126.255.255.255	شبكات كبيرة (الحكومات)	8 بت مضيف / 24 بت شبكة
B	128.0.0.0 – 191.255.255.255	شبكات متوسطة (الجامعات)	16 بت مضيف / 16 بت شبكة
C	192.0.0.0 – 223.255.255.255	شبكات صغيرة (الشركات)	24 بت مضيف / 8 بت شبكة
D	224.0.0.0 – 239.255.255.255	البث المتعدد (Multicast)	مُخصصة للبث الجماعي
E	240.0.0.0 – 255.255.255.255	أغراض بحثية واحتياطية	غير مستخدمة عمليًا

3. عنوان الشبكة وعنوان المضيف

عنوان الشبكة (Network Address):

هو العنوان الذي يُعرِّف شبكة كاملة ضمن نطاق عناوين IPv4. يُستخدم لتمييز الشبكة عن غيرها وتوجيه البيانات بشكل صحيح.

كيفية تحديد عنوان الشبكة

1. عنوان IP: مثل `192.168.1.10`.

2. قناع الشبكة الفرعية (Subnet Mask): مثل `255.255.255.0` (أو `/24` بتنسيق CIDR).

3. عملية AND بين البتات:

- تُطبق عملية AND منطقية بين كل بت في عنوان IP وبتات القناع.

- النتيجة هي عنوان الشبكة.

عنوان الشبكة: `192.168.1.0` (بالترميز العشري).

خصائص عنوان الشبكة

- الجزء الثابت: يُحدد بواسطة القناع (الجزء الذي تكون فيه بتات القناع = `1`).

- الجزء المتغير: يُحدد بواسطة البتات المتبقية (الجزء الذي تكون فيه بتات القناع = `0`)، ويُستخدم لعناوين المضيفين.

- لا يُمكن تعيينه لأي جهاز: لأنه يمثل الشبكة ككل.

أهمية عنوان الشبكة

1. توجيه البيانات (Routing): تساعد أجهزة الراوتر على تحديد الشبكة الهدف.

2. تقسيم الشبكات (Subnetting): فصل الشبكات الفرعية لمنع الازدحام.

3. إدارة العناوين: تحديد نطاق العناوين المتاحة للمضيفين.

مثال آخر

- عنوان IP: `10.20.30.40`

- القناع: `255.255.0.0` (أو `/16`).

- عنوان الشبكة: `10.20.0.0`.

الاستخدام في التطبيقات

- عند إعداد شبكة محلية (LAN)، يتم تعيين عنوان الشبكة في إعدادات الراوتر.

- مثال: إذا كان الراوتر يستخدم عنوان الشبكة `192.168.1.0/24`، فسيوزع عناوين المضيفين من `192.168.1.1` إلى `192.168.1.254`.

ملاحظة

- عنوان البث (Broadcast Address): هو آخر عنوان في الشبكة (مثال: `192.168.1.255`) ويُستخدم لإرسال بيانات لجميع الأجهزة في الشبكة.- عنوان البث (Broadcast Address):

- يُستخدم لإرسال بيانات لجميع الأجهزة في الشبكة (مثال: `192.168.1.255`).

العناوين الصالحة للمضيفين (Valid Host Addresses)

هي العناوين التي يمكن تعيينها للأجهزة (مثل الحواسيب، الطابعات، الخوادم) داخل شبكة فرعية (Subnet). تُستثنى منها عنوان الشبكة (Network Address) وعنوان البث (Broadcast Address).

كيفية حساب العناوين الصالحة

1. حدد عنوان الشبكة:

- يتم الحصول عليه عن طريق تطبيق عملية AND بين عنوان IP وقناع الشبكة.

2. حدد عنوان البث:

- هو آخر عنوان في نطاق الشبكة الفرعية.

3. العناوين الصالحة:

- جميع العناوين بين عنوان الشبكة + 1 و عنوان البث - 1.

مثال 1: شبكة /24 (Subnet Mask: 255.255.255.0)

- عنوان الشبكة: `192.168.1.0`

- عنوان البث: `192.168.1.255`

- العناوين الصالحة: `192.168.1.1` إلى `192.168.1.254` (254 عنوان).

مثال 2: شبكة /25 (Subnet Mask: 255.255.255.128)

- عنوان الشبكة: `192.168.1.128`

- عنوان البث: `192.168.1.255`

- العناوين الصالحة: `192.168.1.129` إلى `192.168.1.254` (126 عنوان).

مثال 3: شبكة /30 (Subnet Mask: 255.255.255.252)

- عنوان الشبكة: `192.168.1.0`

- عنوان البث: `192.168.1.3`

- العناوين الصالحة: `192.168.1.1` و `192.168.1.2` (2 عناوين).

جدول يوضح عدد العناوين الصالحة بناءً على قناع الشبكة

مثال	عدد العناوين الصالحة	قناع الشبكة (CIDR)
192.168.1.1 - 192.168.1.254	254	/24 (255.255.255.0)
192.168.1.129 - 192.168.1.254	126	/25 (255.255.255.128)
192.168.1.1 - 192.168.1.62	62	/26 (255.255.255.192)
192.168.1.1 - 192.168.1.2	2	/30 (255.255.255.252)

ملاحظات مهمة

1. العناوين المحجوزة:

- عنوان الشبكة: لا يُمكن تعيينه لأي جهاز (مثال: `192.168.1.0`).

- عنوان البث: يُستخدم لإرسال بيانات لجميع الأجهزة (مثال: `192.168.1.255`).

2. الشبكات الصغيرة جدًا (/31 و/32):

- /31: تُستخدم لشبكات نقطة-إلى-نقطة (Point-to-Point) حيث يُمكن استخدام جميع العناوين.

- /32: يحتوي على عنوان واحد فقط (يُستخدم أحيانًا للتوجيه).

3. الاستثناءات:

- في بعض الأنظمة (مثل Cisco IOS)، قد تسمح شبكات /31 باستخدام العناوين كاملة.

خطوات تحديد العناوين الصالحة

1. اختر عنوان IP وقناع الشبكة.

2. احسب عنوان الشبكة باستخدام عملية AND.

3. احسب عنوان البث عن طريق تعيين جميع بتات المضيف في عنوان الشبكة إلى `1`.

4. استبعد عنوان الشبكة وعنوان البث، والباقي هي العناوين الصالحة.

مثال تطبيقي

- الشبكة: `10.0.0.0/8` (`Subnet Mask: `255.0.0.0`).

- عنوان الشبكة: `10.0.0.0`.

- عنوان البث: `10.255.255.255`.

- العناوين الصالحة: `10.0.0.1` إلى `10.255.255.254` (16,777,214 عنوان).

الخلاصة

العناوين الصالحة للمضيفين هي الأساس لإدارة الأجهزة على الشبكة. فهمها يُساعد في تجنب التعارضات وتحسين استخدام العناوين المتاحة.

4. قناع الشبكة الفرعية (Subnet Mask)

- الغرض: تحديد الجزء المُخصص للشبكة والجزء المُخصص للمضيف في العنوان.

- أمثلة:

- قناع الفئة الافتراضي لـ C: `255.255.255.0` (يُكتب `/24` في تنسيق CIDR).

- قناع مخصص: `255.255.255.128` (يُكتب `/25`).

5. التقسيم الفرعي (Subnetting)

هو عملية تقسيم شبكة كبيرة إلى شبكات فرعية أصغر (Subnets) لتحسين كفاءة إدارة العناوين، تقليل الازدحام، وتعزيز الأمان. يُستخدم في شبكات IPv4 وIPv6، ويُعد أساسيًا في تصميم الشبكات الحديثة.

أهداف التقسيم الفرعي

1. تحسين استخدام العناوين: تجنب هدر العناوين في الشبكات الكبيرة.

2. تقليل الازدحام (Traffic): عزل حركة البيانات داخل الشبكات الفرعية.

3. تعزيز الأمان: فصل الأقسام الحساسة (مثل الخوادم) عن بقية الشبكة.

4. سهولة الإدارة: تقسيم الشبكة إلى وحدات منطقية صغيرة.

مكونات التقسيم الفرعي

1. عنوان الشبكة الأصلي (Parent Network): مثل `192.168.1.0/24`.

2. قناع الشبكة الفرعية (Subnet Mask): يُحدد عدد البتات المخصصة للشبكة الفرعية.

3. عدد البتات المُقترضة (Borrowed Bits): بتات تُؤخذ من جزء المضيف لإنشاء شبكات فرعية.

خطوات التقسيم الفرعي

1. تحديد احتياجات الشبكة

- عدد الشبكات الفرعية المطلوبة.

- عدد العناوين الصالحة للمضيفين في كل شبكة فرعية.

2. حساب عدد البتات المُفترضة

- استخدم المعادلة:

$$\text{عدد الشبكات الفرعية} = n^2$$

حيث (n) = عدد البتات المُفترضة من جزء المضيف.

3. تحديث قناع الشبكة

- أضف البتات المُفترضة إلى قناع الشبكة الأصلي.

- مثال:

- قناع أصلي: `/24` → `255.255.255.0`.

- إذا افترضنا 3 بتات: القناع الجديد → `/27` → `255.255.255.224`.

4. حساب عدد العناوين لكل شبكة فرعية

5. تحديد نطاقات الشبكات الفرعية

- ابدأ من عنوان الشبكة الأصلي وأضف "حجم الكتلة (Block Size)" لكل شبكة فرعية.

4. نطاقات الشبكات الفرعية:

الشبكة الفرعية	نطاق العناوين	عنوان الشبكة	عنوان البث
Subnet 1	192.168.1.1 - 192.168.1.62	192.168.1.0	192.168.1.63
Subnet 2	192.168.1.65 - 192.168.1.126	192.168.1.64	192.168.1.127
Subnet 3	192.168.1.129 - 192.168.1.190	192.168.1.128	192.168.1.191
Subnet 4	192.168.1.193 - 192.168.1.254	192.168.1.192	192.168.1.255

فوائد التقسيم الفرعي

- تحسين الأداء: تقليل نطاق البث (Broadcast Domain).

- إدارة مرنة: تخصيص موارد لكل قسم حسب الحاجة.

- تعزيز الأمان: عزل الشبكات الفرعية عن بعضها (مثل فصل قسم المحاسبة عن الضيوف).

تحديات التقسيم الفرعي

- التعقيد: يحتاج إلى حسابات دقيقة لتجنب الأخطاء.

- التخطيط المسبق: يجب التنبؤ بعدد الشبكات والمضيفين المطلوبين مسبقًا.

التقسيم الفرعي المتغير (VLSM)

تقنية متقدمة تسمح بتقسيم الشبكة إلى شبكات فرعية بأحجام مختلفة حسب الحاجة.

- مثال:

  - شبكة فرعية كبيرة لـ 100 جهاز.

  - شبكة فرعية صغيرة لـ 10 أجهزة (مثل الخوادم).

الخلاصة

التقسيم الفرعي مهارة أساسية في إدارة الشبكات، تُحسّن الكفاءة والأمان. كلما مارستها أكثر، أصبحت الحسابات أكثر سهولة!

6. العناوين الخاصة (Private IPs)

هي عناوين IP مُخصصة للاستخدام داخل الشبكات المحلية (مثل المنزلية أو المؤسسية) ولا يمكن توجيهها عبر الإنترنت العام. تُستخدم لتوفير عناوين فريدة للأجهزة داخل الشبكة دون استهلاك العناوين العامة المحدودة في IPv4.

النطاقات المُخصصة للعناوين الخاصة

في IPv4، تم تخصيص 3 نطاقات رئيسية للعناوين الخاصة:

1. الفئة A:

- النطاق: 10.0.0.0 – 10.255.255.255
- قناع الشبكة الافتراضي: 255.0.0.0 (أو `/8` بتنسيق CIDR).
- السعة: ~16 مليون عنوان.
- الاستخدام: شبكات كبيرة (كالحكومات أو الشركات الكبرى).

2. الفئة B:

- النطاق: 172.16.0.0 – 172.31.255.255
- قناع الشبكة الافتراضي: 255.240.0.0 (أو `/12`).
- السعة: ~1 مليون عنوان.
- الاستخدام: شبكات متوسطة (كالفروع المؤسسية).

3. الفئة C:

- النطاق: 192.168.0.0 – 192.168.255.255
- قناع الشبكة الافتراضي: 255.255.0.0 (أو `/16`).
- السعة: ~65 ألف عنوان.
- الاستخدام: شبكات صغيرة (كالمنازل أو المكاتب الصغيرة).

لماذا تُستخدم العناوين الخاصة؟

1. توفير عناوين IPv4:

- بسبب ندرة العناوين العامة (IPv4 محدود بـ ≈4.3 مليار عنوان).

2. عزل الشبكات الداخلية:

- حماية الأجهزة من الوصول المباشر عبر الإنترنت.

3. إعادة استخدام العناوين:

- يمكن لشبكات مختلفة استخدام نفس النطاقات الخاصة دون تعارض.

كيف تتصل الأجهزة ذات العناوين الخاصة بالإنترنت؟

تُستخدم تقنية NAT (ترجمة عناوين الشبكة) لتحويل العناوين الخاصة إلى عنوان عام واحد (أو مجموعة عناوين) عند الاتصال بالإنترنت.

- مثال:

- جهازك المنزلي (IP: `192.168.1.5`) → يُترجم عبر الراوتر (IP العام: `203.0.113.10`) للوصول إلى الإنترنت.

أمثلة على استخدام العناوين الخاصة

- الراوتر المنزلي:

- يُوزع عناوين مثل `192.168.1.1` إلى `192.168.1.254`.

- شبكة الشركة:

- قد تستخدم نطاق `10.0.0.0/8` لإدارة فروع متعددة.

- الأجهزة الذكية:

- الطابعات، الكاميرات، والأجهزة الذكية داخل الشبكة المحلية.

مقارنة بين العناوين الخاصة والعامة

المعيار	العناوين الخاصة	العناوين العامة
النطاق	10.0.0.0 - 10.255.255.255	أي عنوان خارج النطاقات الخاصة
	172.16.0.0 - 172.31.255.255	
	192.168.0.0 - 192.168.255.255	
التوجيه على الإنترنت	غير ممكن	ممكن
الاستخدام	داخل الشبكات المحلية	على الإنترنت العام

ملاحظات مهمة

- IPv6: لا تحتوي على عناوين خاصة بالمعنى التقليدي، لكنها تستخدم نطاق Unique Local Addresses (ULA) (`fd00::/8`) لأغراض مشابهة.

- التكرار: يمكن استخدام نفس العنوان الخاص في شبكات مختلفة (مثال: شبكتان منفصلتان تستخدمان `192.168.1.1`).

- الأمان: العناوين الخاصة لا تحمي الشبكة من الهجمات وحدها؛ يجب دعمها بجدران نارية (Firewalls).

الخلاصة

العناوين الخاصة هي حجر الأساس لإدارة الشبكات الداخلية بكفاءة، وتُجنب نضوب عناوين IPv4. مع ذلك، يعتمد اتصالها بالإنترنت على تقنيات مثل NAT لربط العالمين الخاص والعام.

7. العناوين العامة (Public IPs)

- تُعيّن بواسطة مزودي الخدمة (ISPs) وتكون فريدة عالميًا.

- مثال: `203.0.113.5`.

8. عناوين خاصة أخرى

- البث العام (Broadcast): `255.255.255.255`.

- العنوان المحلي (Loopback): `127.0.0.1` (لاختبار الاتصال بالجهاز نفسه).

- APIPA: `169.254.x.x` (عند فشل الحصول على IP من خادم DHCP).

9. مشكلة نضوب عناوين IPv4

- السبب: العدد المحدود (≈4.3 مليار عنوان) لا يكفي لجميع الأجهزة.

- الحلول:

  - NAT (ترجمة عناوين الشبكة): مشاركة عنوان عام واحد بين عدة أجهزة.

  - الانتقال إلى IPv6: الذي يحتوي على 128 بت (≈340 تريليون تريليون عنوان).

10. مثال عملي

- العنوان: `192.168.1.10` مع قناع `/24` (`255.255.255.0`).

  - عنوان الشبكة: `192.168.1.0`.

  - عنوان البث: `192.168.1.255`.

  - العناوين المتاحة للمضيفين: `192.168.1.1` إلى `192.168.1.254`.

الخلاصة

IPv4 هو نظام عنونة أساسي للإنترنت، لكنه يعاني من محدودية العناوين. يُستخدم مع تقنيات مثل NAT وSubnetting لتحسين الاستفادة من العناوين المتاحة، بينما يُعد IPv6 الحل طويل المدى.

المحاضرة الثاني عشر

الكابلات المستخدمة في الشبكات

تُستخدم عدة أنواع من الكابلات في الشبكات الحاسوبية، ويختلف اختيار النوع بناءً على السرعة المطلوبة، المسافة، التكلفة، ومقاومة التداخل. إليك أشهر الأنواع:

1. الكابلات الملتوية (Twisted Pair)

هي نوع من الكابلات المستخدمة في نقل البيانات عبر الشبكات الحاسوبية والاتصالات، وتُعتبر الأكثر شيوعًا في الشبكات المحلية (LAN) بسبب تكلفتها المنخفضة وسهولة تركيبها. تعتمد فكرتها على التواء زوج من الأسلاك النحاسية لتقليل التداخل الكهرومغناطيسي (EMI) وتحسين جودة الإشارة.

أنواع الكابلات الملتوية

تنقسم إلى نوعين رئيسيين بناءً على وجود غلاف حماية

1. كابل UTP (Unshielded Twisted Pair)

- الوصف:

- لا يحتوي على غلاف معدني واقٍ.

- يتكون من 4 أزواج ملتوية من الأسلاك النحاسية المغطاة بطبقة عازلة.

- المميزات:

- خفيف الوزن ورخيص الثمن.

- سهل التركيب والصيانة.

- العيوب:

- أقل مقاومة للتداخل الكهرومغناطيسي مقارنةً بـ STP.

- الاستخدامات الشائعة:

- الشبكات المنزلية والمكاتب الصغيرة.

- كابلات الهاتف.

2. كابل STP (Shielded Twisted Pair)

- الوصف:

- يحتوي على غلاف معدني (شيلد) يحيط بكل زوج من الأسلاك أو الكابل بأكمله.

- المميزات:

- مقاومة عالية للتداخل الكهرومغناطيسي والضوضاء.

- مناسب للبيئات الصناعية ذات التشويش العالي.

- العيوب:

- أثقل وزنًا وأعلى تكلفة من UTP.

- صعوبة في التركيب بسبب الشيلد.

- الاستخدامات الشائعة:

- الشبكات الصناعية.

- المناطق ذات الكثافة الكهرومغناطيسية العالية (قرب المحركات أو الكابلات الكهربائية).

فئات كابلات UTP

يتم تصنيف كابلات UTP حسب الأداء والسرعة إلى عدة فئات:

الفئة	السرعة القصوى	التردد	الاستخدام
Cat5	100 Mbps	100 MHz	شبكات Ethernet القديمة
Cat5e	1 Gbps	100 MHz	الشبكات المنزلية والمكاتب
Cat6	10 Gbps	250 MHz	شبكات الشركات المتوسطة
Cat6a	10 Gbps	500 MHz	شبكات البيانات عالية السرعة
Cat7	10 Gbps	600 MHz	التطبيقات الصناعية والسرعات الفائقة

الفئة	السرعة القصوى	التردد	الاستخدام
Cat8	40 Gbps	2000 MHz	مراكز البيانات والشبكات المتطورة

مكونات الكابلات الملتوية

1. الأسلاك النحاسية: 4 أزواج ملتوية (8 أسلاك).
2. العازل (Insulator): مادة بلاستيكية تحيط بكل سلك.
3. الغلاف الخارجي (Jacket): طبقة واقية من البلاستيك أو المطاط.
4. الشيلد (في STP): طبقة معدنية (ألومنيوم أو نحاس) للحماية.

الموصلات (Connectors)

- موصل RJ45: الأكثر استخدامًا لتوصيل الكابلات الملتوية بالأجهزة (مثل أجهزة الكمبيوتر، السويتشات، الراوترات).
- موصل RJ11: يُستخدم في كابلات الهاتف.

مزايا الكابلات الملتوية

1. التكلفة المنخفضة مقارنةً بكابلات الألياف الضوئية.
2. المرونة: سهلة الثني والتركيب في المساحات الضيقة.
3. التوافق: تدعم معظم أجهزة الشبكات الحديثة.
4. تقليل التداخل: بفضل التواء الأسلاك.

عيوب الكابلات الملتوية

1. مسافة محدودة: أقصى مسافة فعالة هي 100 متر دون تضخيم الإشارة.
2. حساسية للتداخل (خاصة UTP).
3. سرعة محدودة مقارنةً بالألياف الضوئية.

تطبيقات عملية

1. شبكات Ethernet: مثل توصيل أجهزة الكمبيوتر بالراوتر.

2. أنظمة الهاتف: لنقل الإشارات الصوتية.

3. أنظمة المراقبة: كاميرات IP.

نصائح للاستخدام الأمثل

- تجنب وضع الكابلات بالقرب من مصادر التداخل (مثل الكابلات الكهربائية).

- استخدام كابلات Cat6 أو أعلى للسرعات فوق 1 Gbps.

- التأكد من أن الموصلات (RJ45) مُحكمة التركيب لتجنب فقدان الإشارة.

الخلاصة

الكابلات الملتوية هي العمود الفقري للشبكات المحلية بسبب توازنها بين التكلفة والأداء. اختيار الفئة المناسبة يعتمد على السرعة المطلوبة والبيئة المحيطة.

2. الكابلات المحورية (Coaxial)

هي نوع من الكابلات تُستخدم لنقل الإشارات عالية التردد (مثل إشارات التلفزيون، الإنترنت، والاتصالات) بفقدان منخفض للطاقة. تتميز بتركيبها الطبقي الذي يوفر حماية من التداخل الكهرومغناطيسي، مما يجعلها مناسبة للمسافات المتوسطة والبيئات ذات الضوضاء العالية.

مكونات الكابل المحوري

1. الموصل الداخلي (Core):

- سلك نحاسي صلب أو مجدول في المركز، ينقل الإشارة الكهربائية.

2. العازل (Dielectric Insulator):

- طبقة بلاستيكية أو هوائية تحيط بالموصل الداخلي لمنع التلامس مع الطبقات الخارجية.

3. الغلاف المعدني (Shield):

- شبكة من الأسلاك النحاسية أو رقاقة معدنية تحمي الإشارة من التداخل الكهرومغناطيسي.

4. الغلاف الخارجي (Jacket):

- طبقة عازلة من البلاستيك (مثل PVC) تحمي الكابل من العوامل الخارجية (الرطوبة، الحرارة، إلخ).

أنواع الكابلات المحورية

النوع	الوصف	الاستخدام
Thinnet (10BASE2)	- قطر رفيع (≈6 مم). - مسافة قصوى: **185 مترًا**. - سرعة: **10 Mbps**.	شبكات Ethernet القديمة (مثل LAN).
Thicknet (10BASE5)	- قطر سميك (≈10 مم). - مسافة قصوى: **500 متر**. - سرعة: **10 Mbps**.	شبكات المسافات الطويلة.
RG-6	- تصميم حديث. - يدعم الترددات العالية (حتى **3 GHz**).	التلفزيون الكبلي (Cable TV)، الإنترنت (DOCSIS).
RG-59	- أرق من RG-6. - ترددات أقل (حتى **1 GHz**).	كاميرات المراقبة، أنظمة الفيديو.

مميزات الكابلات المحورية

1. مقاومة عالية للتداخل: بفضل الغلاف المعدني.

2. نقل إشارات عالية التردد: مثل إشارات الفيديو والإنترنت.

3. مسافات أطول: مقارنةً بالكابلات الملتوية (حتى 500 متر بدون تضخيم).

4. متانة: تحمل الظروف البيئية القاسية.

عيوب الكابلات المحورية

1. التكلفة العالية: مقارنةً بالكابلات الملتوية (UTP).

2. المرونة المحدودة: صعوبة الثني بسبب السماكة.

3. التوصيلات المعقدة: تتطلب موصلات دقيقة (مثل BNC أو F-type).

4. السرعة المحدودة: لا تنافس الألياف الضوئية في السرعات العالية.

الاستخدامات الشائعة

1. شبكات التلفزيون الكبلي (Cable TV): مثل توصيل جهاز التلفزيون بالشبكة.

2. الاتصالات عبر الأقمار الصناعية: نقل إشارات البث المباشر.

3. كاميرات المراقبة (CCTV): توصيل الكاميرات بأجهزة التسجيل.

4. الاتصال بالإنترنت (DOCSIS): عبر مزودي الخدمة مثل الكابل المودم.

5. الشبكات اللاسلكية: توصيل الهوائيات (Antennas) بالراوترات.

الموصلات (Connectors)

1. BNC (Bayonet Neill–Concelman):

- يُستخدم في الشبكات القديمة وكاميرات المراقبة.

- يتم تثبيته عبر تدويره بشكل نصف دائري.

2. F-type:

- الأكثر شيوعًا في التلفزيون الكبلي والإنترنت (المودم).

- يتم ربطه عبر لفّه يدويًا.

3. N-type:

- للاستخدامات الصناعية عالية التردد.

مقارنة مع الكابلات الملتوية (Twisted Pair)

المعيار	الكابلات المحورية	الكابلات الملتوية (UTP)
التداخل	مقاومة عالية	مقاومة متوسطة
السرعة	(في الأنواع الحديثة) Gbps حتى 10	Gbps (Cat6a) حتى 10
التكلفة	أعلى	أقل
المرونة	محدودة	عالية

نصائح للاستخدام الأمثل

- تجنب الثني الحاد: لتجنب تلف الموصل الداخلي.

- استخدام موصلات عالية الجودة: لمنع فقدان الإشارة.

- الابتعاد عن مصادر التداخل: مثل الكابلات الكهربائية.

الخلاصة

الكابلات المحورية لا تزال خيارًا مهمًا في تطبيقات نقل الإشارات عالية التردد، خاصة في البث التلفزيوني والمراقبة. رغم تطور تقنيات مثل الألياف الضوئية، إلا أنها تحافظ على مكانتها في بيئات محددة بفضل موثوقيتها ومقاومتها للتداخل.

3. الألياف الضوئية (Fiber Optic)

هي كابلات متطورة تنقل البيانات عبر الضوء بدلًا من الإشارات الكهربائية، مما يوفر سرعات فائقة ومسافات نقل طويلة مع مقاومة عالية للتداخل. تُستخدم في البنية التحتية للإنترنت عالي السرعة، شبكات الاتصالات، والتطبيقات الصناعية.

مكونات الكابل الضوئي

1. اللب (Core):

- أنبوب زجاجي أو بلاستيكي رفيع (قطره ≈ 9-62.5 ميكرون) ينقل الضوء.

2. الغلاف (Cladding):

- طبقة تحيط باللب، مصنوعة من مادة معامل انكسارها أقل لتعكس الضوء داخليًا.

3. الغلاف الواقي (Buffer Coating):

- طبقة بلاستيكية تحمي الألياف من الرطوبة والضرر الميكانيكي.

أنواع الألياف الضوئية

النوع	الوصف	الاستخدام
أحادي النمط (Single-Mode)	- قطر لب صغير (≈9 ميكرون). - شعاع ضوئي واحد. - مسافات طويلة (حتى **100 كم**).	شبكات الاتصالات بعيدة المدى، خطوط الإنترنت الدولية.
متعدد الأنماط (Multi-Mode)	- قطر لب أكبر (≈50-62.5 ميكرون). - أشعة ضوئية متعددة. - مسافات قصيرة (حتى **2 كم**).	الشبكات المحلية (LAN)، مراكز البيانات، أنظمة CCTV.

مميزات الألياف الضوئية

1. سرعة فائقة: تصل إلى Terabits في الثانية (أسرع بكثير من النحاس).

2. مسافات طويلة: نقل البيانات دون تضخيم لمسافات تصل إلى 100 كم.

3. مقاومة التداخل: لا تتأثر بالمجالات الكهرومغناطيسية أو الإشعاعات.

4. أمان عالي: صعوبة التنصت على الإشارات الضوئية.

5. عرض نطاق ترددي كبير: مناسب للفيديو عالي الدقة والبيانات الضخمة.

عيوب الألياف الضوئية

1. التكلفة العالية: مقارنةً بكابلات النحاس.

2. تركيب معقد: يتطلب معدات وأدوات خاصة (مثل أدوات لحام الألياف).

3. هشاشة: الألياف الزجاجية قد تنكسر إذا ثُنيت بقوة.

الاستخدامات الشائعة

- شبكات الإنترنت عالية السرعة (FTTH): توصيل المنازل بالإنترنت عبر الألياف.

- مراكز البيانات: الربط بين الخوادم بسرعات فائقة.

- الاتصالات البحرية: كابلات تحت البحر تربط بين القارات.

- التطبيقات الطبية: المناظير الضوئية وأدوات الجراحة الدقيقة.

- الأنظمة العسكرية: اتصالات آمنة وسريعة.

مقارنة مع كابلات النحاس

المعيار	الألياف الضوئية	كابلات النحاس (مثل UTP)
السرعة	حتى **100+ Tbps**	حتى **10 Gbps**
المسافة	حتى **100 كم**	حتى **100 متر**
التداخل	مقاومة كاملة	عرضة للتداخل الكهرومغناطيسي
التكلفة	عالية	منخفضة

كابلات Ethernet القياسية

هي الكابلات الأكثر استخدامًا لتوصيل الأجهزة في الشبكات المحلية (LAN) عبر بروتوكول Ethernet. تعتمد على تقنية الكابلات الملتوية (Twisted Pair) مع موصلات RJ45، وتُصنف حسب سرعتها وعرض النطاق الترددي إلى عدة فئات. إليك التفاصيل:

1. أنواع كابلات Ethernet حسب الفئة (Category)

الفئة	السرعة القصوى	التردد	الاستخدام
Cat5	100 Mbps	100 MHz	شبكات قديمة (نادرة الاستخدام اليوم).
Cat5e	1 Gbps	100 MHz	الشبكات المنزلية والمكاتب الصغيرة.
Cat6	10 Gbps	250 MHz	شبكات الشركات (لمسافات حتى 55 مترًا).
Cat6a	10 Gbps	500 MHz	مسافات أطول (حتى 100 متر).
Cat7	10 Gbps	600 MHz	بيئات ذات تداخل عالي (مخَصَّصة).
Cat8	40 Gbps	2000 MHz	مراكز البيانات والشبكات المتطورة.

2. مكونات كابلات Ethernet

1. الأسلاك الملتوية (Twisted Pairs):

- 4 أزواج من الأسلاك النحاسية الملتوية لتقليل التداخل.

2. الغلاف (Shielding):

- UTP (Unshielded Twisted Pair): بدون غلاف حماية (الأكثر شيوعًا).
- STP (Shielded Twisted Pair): مع غلاف معدني للحماية من التداخل.

3. الموصلات (RJ45):

- موصلات بلاستيكية قياسية لتوصيل الكابل بالأجهزة (مثل الراوترات أو الحواسيب).

3. استخدامات كابلات Ethernet

- الشبكات المنزلية: توصيل أجهزة الكمبيوتر، التلفزيونات الذكية، والطابعات.

- المكاتب: ربط أجهزة الشبكة (سويتشات، راوترات، خوادم).

- مراكز البيانات: نقل البيانات بسرعات عالية بين الخوادم.

- أنظمة PoE (Power over Ethernet): توصيل أجهزة مثل كاميرات المراقبة مع نقل الطاقة عبر الكابل.

4. مقارنة بين UTP وSTP

المعيار	UTP	STP
التداخل	أقل مقاومة	مقاومة عالية بفضل الغلاف المعدني
التكلفة	منخفضة	أعلى
المرونة	خفيفة وسهلة التركيب	أثقل وأقل مرونة
الاستخدام	المنازل والمكاتب	البيئات الصناعية أو ذات الضوضاء

5. نصائح لاختيار الكابل المناسب

1. السرعة المطلوبة:

- للاستخدام اليومي (تصفح الإنترنت، بث الفيديو): Cat5e أو Cat6.

- للألعاب أو نقل الملفات الكبيرة: Cat6a أو Cat7.

2. المسافة:

- تجاوز 55 مترًا لسرعات 10 Gbps؟ اختر Cat6a.

3. التداخل:

- في بيئات صناعية؟ اختر STP أو Cat7.

4. التوافق:

- تأكد أن الأجهزة تدعم سرعة الكابل (مثال: سويتش 1 Gbps مع Cat6).

6. أشهر التطبيقات العملية

- توصيل الراوتر بالكمبيوتر: كابل Cat5e أو Cat6.

- شبكات الألعاب (Gaming): كابل Cat6a لتقليل زمن التأخير (Latency).

- كاميرات IP: كابل Cat5e مع دعم PoE.

الخلاصة

كابلات Ethernet القياسية هي العمود الفقري للشبكات السلكية. اختيار الفئة المناسبة يعتمد على السرعة، المسافة، والبيئة المحيطة. إذا كنت تريد سرعة فائقة وموثوقية، استثمر في كابلات Cat6 أو أعلى! 🚀 ---

5. مقارنة بين أنواع الكابلات

المعيار	Twisted Pair	Coaxial	Fiber Optic
السرعة	حتى 10 Gbps	حتى 10 Gbps	حتى 100 +Tbps
المسافة	حتى 100 متر	حتى 500 متر	حتى 100 كم
التكلفة	منخفضة	متوسطة	عالية
مقاومة التداخل	متوسطة (UTP) / عالية (STP)	عالية	عالية جدًا

الاسئلة الاسترشادية

1- اذكر ثلاثة من أنواع الكابلات المستخدمة في الشبكات
2- اذكر ثلاثة من مكونات الكابلات الملتوية
3- اذكر ثلاثة من مزايا الكابلات الملتوية
4- اذكر عيوب الكابلات الملتوية
5- اذكر ثلاثة من تطبيقات الكابلات الملتوية
6- اذكر ثلاثة من مكونات الكابلات المحورية
7- اذكر ثلاثة من مزايا الكابلات المحورية
8- اذكر ثلاثة من عيوب الكابلات المحورية
9- اذكر ثلاثة من استخدامات الكابلات المحورية
10- اذكر ثلاثة من مزايا الالياف الضوئية

المحاضرة الرابعة عشر

تواصل الكوابل المختلفة (مثل كوابل الإيثرنت، الألياف البصرية، الكوابل المحورية، إلخ) يمكن محاكاته باستخدام أدوات وبرمجيات متخصصة لفهم كيفية نقل الإشارات والبيانات عبر هذه الوسائط. فيما يلي طرق شائعة لمحاكاة تواصل الكوابل:

1. محاكاة باستخدام برمجيات الشبكات

تُستخدم برامج مثل Cisco Packet Tracer، GNS3، أو OMNeT++ لمحاكاة سلوك الكوابل في شبكات الحاسوب، بما في ذلك:

- كابلات الإيثرنت (Ethernet):

- محاكاة سرعات نقل البيانات (مثل 10/100/1000 Mbps).

- تحليل تأثير الطول على الإشارة (مثل الحد الأقصى لطول كابل CAT6: 100 متر).

- نمذجة التداخل الكهرومغناطيسي (EMI) والتوهين (Attenuation).

- الألياف البصرية (Fiber Optic):

- محاكاة فقدان الإشارة عبر المسافات الطويلة.

- تحليل تأثيرات التشتت (Dispersion) وانعكاس الإشارة.

مثال: في Cisco Packet Tracer، يمكنك توصيل أجهزة افتراضية بكابلات مختلفة ومراقبة جودة الإشارة.

2. محاكاة باستخدام MATLAB/Simulink

تُستخدم لنمذجة الإشارات التناظرية والرقمية عبر الكوابل، مثل:

- الكوابل المحورية (Coaxial):

- نمذجة نقل إشارات التردد الراديوي (RF).

- حساب الفقدان في الكابل (Cable Loss)

.

- كابلات الزوج الملتوي (Twisted Pair):

- تحليل تأثير التداخل (Crosstalk) بين الأسلاك.

- نمذجة تأثيرات Capacitance و Inductance.

مثال:

```matlab
% نموذج بسيط لإشارة تمر عبر كابل
t = 0:0.001:1؛
signal = sin(2pi5t) 5 إشارة جيبية بتردد % ؛Hz
attenuated_signal = signal  exp(-0.1length(t))محاكاة التوهين % ؛
plot(t, attenuated_signal)؛
```

3. محاكاة باستخدام أدوات RF مثل ANSYS HFSS أو CST Studio

تُستخدم لمحاكاة الخصائص الكهرومغناطيسية للكوابل عالية التردد، مثل:

- كابلات HDMI أو USB:

- تحليل سلامة الإشارة (Signal Integrity).

- نمذجة العاكسية (Return Loss) والتشويه (Distortion).

- كابلات الألياف البصرية:

- محاكاة انتشار الضوء عبر الألياف.

- حساب تأثيرات Nonlinear Effects مثل تشتت رامان (Raman Scattering).

4. محاكاة باستخدام بروتوكولات برمجية (مثل NS-3)

تُستخدم لمحاكاة طبقات البروتوكولات (مثل TCP/IP) عبر وسائط كابلات مختلفة:

- كابلات الإيثرنت:

- محاكاة تأثير زمن الوصول (Latency) وفقدان الحزم (Packet Loss).

- كابلات الألياف البصرية:

- نمذجة سرعات نقل البيانات العالية (مثل 100 Gbps).

5. محاكاة باستخدام Arduino أو Raspberry Pi

يمكن بناء دائرة فعلية لمحاكاة نقل الإشارات عبر كوابل:

- الكابلات التناظرية (Analog):

- إرسال إشارة جيبية عبر كابل ومقارنة الإشارة المُرسَلة بالمستقبَلة.

- الكابلات الرقمية (Digital):

- استخدام بروتوكولات مثل UART أو SPI عبر كابلات مختلفة وقياس معدل الأخطاء (BER).

6. محاكاة باستخدام Python (مكتبات مثل NumPy و Matplotlib)

```python
import numpy as np
import matplotlib.pyplot as plt
محاكاة توهين الإشارة في كابل
length = np.arange طول الكابل بالمتر  (0، 100، 0.1)
attenuation = 0.2  np.sqrt(length) نموذج توهين
```

```
plt.plot(length, attenuation)

plt.xlabel('Length (m)')

plt.ylabel('Attenuation (dB)')

plt.title('Signal Attenuation in Cable')

plt.show()
```

جدول مقارنة بين أدوات المحاكاة:

الأداة	الاستخدام الرئيسي	مثال على الكوابل المدعومة
Cisco Packet Tracer	شبكات الحاسوب	Ethernet, Fiber
MATLAB/Simulink	نمذجة الإشارات التناظرية والرقمية	Coaxial, Twisted Pair
ANSYS HFSS	محاكاة كهرومغناطيسية عالية الدقة	HDMI, USB, RF Cables
NS-3	بروتوكولات الشبكات	Ethernet, Fiber
Python	نماذج رياضية بسيطة	أي نوع (حسب المعادلات المُدخلة)

خطوات عامة لمحاكاة تواصل الكوابل:

1. تحديد الهدف: ما الذي تريد تحليله؟ (مثال: التوهين، التداخل، سرعة النقل).
2. اختيار الأداة: بناءً على نوع الكابل وطبقة النموذج (فيزيائية، بروتوكولات، إلخ).
3. إدخال المعلمات: مثل طول الكابل، التردد، معامل التوهين.
4. تشغيل المحاكاة: وتحليل النتائج (مخططات، جداول، إحصائيات).
5. التحسين: تعديل المعلمات لتحسين الأداء (مثال: تقليل الطول لتحسين السرعة).

تحديات شائعة في المحاكاة:

- التعقيد الحسابي: خاصة في المحاكاة الكهرومغناطيسية عالية التردد.

- دقة النموذج: قد لا تعكس النماذج الرياضية السلوك الحقيقي بدقة 100%.

- تكاليف البرمجيات: بعض الأدوات مثل ANSYS HFSS مكلفة.

باختيار الأداة المناسبة وإدخال المعلمات بدقة، يمكنك محاكاة سلوك أي كابل وتحسين تصميم الشبكات أو أنظمة الاتصالات.

ميزات وعيوب استخدام أسلوب المحاكاة في توصيل الكوابل

الميزات (الإيجابيات):

1. توفير التكاليف:

- لا حاجة لشراء كوابل أو معدات فعلية باهظة الثمن للاختبار.

- تقليل تكاليف الأخطاء (مثل تلف الكوابل في الاختبارات الفعلية).

2. المرونة في الاختبار:

- إمكانية محاكاة سيناريوهات متطرفة أو نادرة (مثل درجات حرارة عالية، ترددات غير عادية).

- تعديل معلمات الكابل (الطول، المادة، التوصيلية) بسرعة ودون جهد.

3. السلامة:

- تجنب مخاطر الاختبارات الفعلية (مثل التيارات العالية أو الإشعاع الكهرومغناطيسي).

4. تحليل مفصَّل:

- دراسة تأثيرات دقيقة مثل:

- التوهين (Attenuation).

- التداخل الكهرومغناطيسي (EMI).

- تشوه الإشارة (Signal Distortion).

- تصور النتائج عبر رسوم بيانية أو جداول (مثل استخدام MATLAB أو Python).

5. التجارب المتكررة:

- إمكانية إعادة المحاكاة بنفس المعلمات أو مع تغييرات طفيفة لتحسين النتائج.

6. القابلية للتوسع:

- محاكاة شبكات كاملة مع أنواع كوابل مختلفة (مثل Ethernet، Fiber) دون بناء بنية تحتية فعلية.

العيوب (السلبيات):

1. عدم الدقة الكاملة:

- النماذج الرياضية قد لا تعكس الواقع بدقة 100%، خاصة في الظواهر غير الخطية (مثل التشويش العشوائي).

- إهمال عوامل بيئية مثل الرطوبة أو الاهتزازات في بعض النماذج.

2. الاعتماد على موارد حاسوبية:

- المحاكاة الدقيقة (مثل محاكاة كهرومغناطيسية عالية التردد) تتطلب أجهزة قوية ووقتًا طويلًا.

- بعض البرمجيات (مثل ANSYS HFSS) مكلفة وتحتاج إلى تراخيص خاصة.

3. صعوبة نمذجة التفاعلات المعقدة:

- قد تفشل المحاكاة في نمذجة تفاعلات غير متوقعة بين الكوابل والأجهزة المجاورة.

- صعوبة محاكاة الأعطال الميكانيكية (مثل انكسار الكابل أو التآكل).

4. المنحنى التعليمي:

- تحتاج إلى خبرة في استخدام أدوات المحاكاة (مثل GNS3 أو NS-3) وفهم الخوارزميات المستخدمة.

5. النتائج النظرية ≠ التطبيق العملي:

- قد تعطي المحاكاة نتائج مثالية، لكن التطبيق الفعلي يعاني من مشكلات غير مُتوقعة (مثل تداخل من مصدر خارجي).

6. الوقت المستغرق:

- إعداد نموذج محاكاة دقيق قد يستغرق وقتًا أطول من الاختبار الفعلي في بعض الحالات.

مقارنة سريعة بين المحاكاة والاختبار الفعلي:

المعيار	المحاكاة	الاختبار الفعلي
التكلفة	منخفضة (برمجيًا)	عالية (معدات، كوابل، صيانة)
الوقت	يعتمد على تعقيد النموذج	مباشر لكن قد يتطلب إعدادًا طويلًا
الدقة	محدودة بالنموذج الرياضي	عالية (تعكس الواقع مباشرةً)
المرونة	عالية (تعديل المعلمات بسهولة)	محدودة (تتطلب تغييرات مادية)
السلامة	آمنة تمامًا	قد تنطوي على مخاطر

متى تُستخدم المحاكاة؟

- في المراحل الأولية: لاختبار الأفكار وتصميم النماذج.

- عند صعوبة التطبيق الفعلي: مثل اختبار كابلات تحت الماء أو في الفضاء.

- لتحليل الظواهر غير المرئية: مثل انتشار الإشارات الكهرومغناطيسية.

الخلاصة:

المحاكاة أداة قوية لفهم سلوك الكوابل وتصميم الأنظمة بكفاءة، لكن يجب دمج نتائجها مع الاختبارات الفعلية لضمان الدقة.

مثال عملي:

- استخدام MATLAB لمحاكاة فقدان الإشارة في كابل Ethernet، ثم التأكد عبر قياسات فعلية باستخدام Oscilloscope.

الاسئلة الاسترشادية

1- اذكر ثلاثة من أنواع المحاكاة المستخدمة في اختبار الكابلات
2- اذكر ثلاثة من تحديات المحاكاة المستخدمة في اختبار الكابلات
3- اذكر ثلاثة من ميزات المحاكاة المستخدمة في اختبار الكابلات

4- اذكر ثلاثة من عيوب المحاكاة المستخدمة في اختبار الكابلات

المحاضرة الخامسة عشر

ربط الأجهزة عبر الشبكات

في الحياة العملية، تُستخدم عدة طرق وتقنيات لربط أجهزة الشبكات معًا، سواء في الشبكات المحلية (LAN) أو الواسعة (WAN). إليك أشهر طرق الاتصال بين الأجهزة مع أمثلة واقعية:

1. الاتصال السلكي (Wired Connections):

أ. كابلات Ethernet (Twisted Pair):

- الاستخدام: الأكثر شيوعًا في المكاتب والمنازل.

- الأنواع:

- CAT5e/CAT6: لدعم سرعات 1 Gbps إلى 10 Gbps (حتى 100 متر).

- CAT7/CAT8: لسرعات أعلى (حتى 40 Gbps) ومواجهة أفضل للتداخل.

- أمثلة عملية:

- توصيل أجهزة الكمبيوتر بالـ Switch في مكتب.

- ربط الراوتر بالمودم عبر كابل Ethernet.

ب. الألياف البصرية (Fiber Optic):

- الاستخدام: للاتصالات عالية السرعة والمسافات الطويلة.

- Single-Mode: مسافات تصل إلى 100 كم (مثلاً: بين مدن في شبكات ISP).

- Multi-Mode: مسافات أقصر (حتى 2 كم) داخل مراكز البيانات.

- أمثلة عملية:

- ربط مراكز البيانات التابعة لشركة ما عبر مدن مختلفة.

- توصيل أبراج الاتصالات بالشبكة الأساسية.

ج. الكابلات المحورية (Coaxial):

- الاستخدام: أقل شيوعًا اليوم، لكنها تُستخدم في:

- توصيل أجهزة المودم الكبلي (Cable Modem) بشبكة الإنترنت.

- أنظمة CCTV (الكاميرات الأمنية).

2. الاتصال اللاسلكي (Wireless Connections):

أ. Wi-Fi (IEEE 802.11):

- الاستخدام: في المنازل، المكاتب، والأماكن العامة.

- المعايير الشائعة:

- Wi-Fi 6 (802.11ax): سرعات تصل إلى 9.6 Gbps.

- Wi-Fi 5 (802.11ac): سرعات حتى 3.5 Gbps.

- أمثلة عملية:

- توصيل الهواتف الذكية والأجهزة اللوحية بالشبكة في المقهى.

- إنشاء شبكة لاسلكية بين مبنى وآخر عبر Point-to-Point Wireless Bridge.

ب. البلوتوث (Bluetooth):

- الاستخدام: للأجهزة القريبة (حتى 10 أمتار).

- أمثلة عملية:

- توصيل الطابعات اللاسلكية أو السماعات بالحاسوب.

- نقل البيانات بين الهاتف والسيارة (مثلاً: Android Auto).

ج. اتصالات الخلايا (G/5G4):

- الاستخدام: للاتصال بالإنترنت في الأماكن النائية أو أثناء التنقل.

- أمثلة عملية:

- استخدام الراوترات المتنقلة (Mobile Hotspot) لتوفير الإنترنت في السفر.

- أنظمة IoT (مثل العدادات الذكية) التي تستخدم شريحة اتصال G4.

3. تقنيات خاصة للشبكات الواسعة (WAN):

أ. MPLS (Multiprotocol Label Switching):

- الاستخدام: لربط فروع الشركات عبر مدن أو دول.

- مثال: شركة لها فرع في القاهرة وآخر في دبي تستخدم MPLS لربط شبكتيها.

ب. VPN (Virtual Private Network):

- الاستخدام: لتأمين الاتصال بين أجهزة بعيدة عبر الإنترنت.

- مثال: موظف يعمل من المنزل يتصل بشبكة الشركة عبر VPN.

ج. Leased Lines (خطوط مؤجرة):

- الاستخدام: اتصال مخصص عالي السرعة بين موقعين (مثال: E1/T1 Lines).

- مثال: بنك يربط فروعه بخطوط مؤجرة لضمان أمان وسرعة الاتصال.

4. تقنيات مبتكرة وحديثة:

أ. Power over Ethernet (PoE):

- الاستخدام: تزويد الأجهزة بالطاقة والبيانات عبر كابل Ethernet واحد.

- مثال: توصيل كاميرات IP أو نقاط الوصول اللاسلكية (Access Points) بدون حاجة لمصدر طاقة منفصل.

ب. الشبكات المعرفة بالبرمجيات (SDN):

- الاستخدام: لإدارة الشبكات بشكل مركزي وديناميكي.

- مثال: شركة تستخدم SDN لتحسين تدفق البيانات بين مكاتبها حول العالم.

ج. تقنية Li-Fi (الاتصال عبر الضوء):

- الاستخدام: نقل البيانات عبر موجات الضوء المرئي (VLC).

- مثال: مختبرات عسكرية أو مستشفيات حيث يُمنع استخدام الإشارات اللاسلكية.

5. أمثلة عملية لتركيبات شبكية شائعة:

أ. شبكة منزلية نموذجية:

- المودم → راوتر → سويچ (Switch) → أجهزة الكمبيوتر عبر Ethernet.

- راوتر → نقاط وصول لاسلكية (Wi-Fi Access Points) → الهواتف والأجهزة الذكية.

ب. شبكة شركة متوسطة:

- راوتر رئيسي → سويچ أساسي (Core Switch) → سويچات فرعية (Access Switches) → أجهزة الموظفين.

- خوادم (Servers) متصلة مباشرة بالسويچ الأساسي لضمان سرعة الوصول.

ج. شبكة بين مبانٍ متباعدة:

- استخدام الألياف البصرية أو الوايرلس مايكرويف (Wireless Microwave) لربط مبنى المقر الرئيسي بفروع الشركة.

6. عوامل اختيار طريقة الاتصال المناسبة:

1. المسافة:

- أقل من 100 متر: Ethernet.

- أكثر من 1 كم: Fiber أو Wireless Microwave.

2. السرعة المطلوبة:

- نقل بيانات عالي السرعة (مثل مراكز البيانات): Fiber.

- استخدام عادي (مثل التصفح): Wi-Fi أو Ethernet.

3. التكلفة:

- الكابلات النحاسية (Ethernet) أرخص من الألياف البصرية.

4. المرونة:

- الاتصال اللاسلكي مناسب للأجهزة المتنقلة.

5. الأمان:

- الاتصالات السلكية أكثر أمانًا من اللاسلكية (إذا لم تُدار بشكل صحيح).

الخلاصة:

اختيار طريقة الاتصال يعتمد على الاحتياجات العملية والميزانية والبيئة. غالبًا ما تُدمج تقنيات متعددة (مثل Ethernet + Wi-Fi + MPLS) لتحقيق التوازن بين السرعة، التغطية، والتكلفة.

التحديات التي تواجه الاتصال بين الأجهزة في الشبكات

فيما يلي التحديات الرئيسية التي تواجه الاتصال بين أجهزة الشبكات المختلفة في البيئات العملية، مع أمثلة توضيحية:

1. التوافقية والاختلاف في المعايير

- الوصف: اختلاف بروتوكولات الاتصال (مثل TCP/IP مقابل NetBEUI) أو تقنيات الشبكات (مثل Ethernet مقابل Token Ring).

- مثال: جهاز قديم يعتمد على IPv4 قد لا يتواصل مع شبكة حديثة تستخدم IPv6 دون تكوين تحويل البروتوكولات (NAT64).

2. مشكلات الأمان

- الوصف: التهديدات مثل الاختراق، هجمات DDoS، أو تسرب البيانات.

- مثال: هجوم إلكتروني على كاميرا IP غير مؤمنة في شبكة شركة، مما يؤدي إلى اختراق الشبكة بأكملها.

3. اختلاف سرعات النقل وعرض النطاق (Bandwidth)

- الوصف: عدم توازن السرعات بين الأجهزة (مثال: جهاز يدعم 1 Gbps وآخر 100 Mbps).

- مثال: بطء نقل الملفات بين خادم سريع وجهاز كمبيوتر قديم في شبكة مكتبية.

4. التداخل الكهرومغناطيسي (EMI)

- الوصف: تداخل الإشارات بسبب الأجهزة الكهربائية القريبة أو الكابلات غير المحمية.

- مثال: تشويش إشارة Wi-Fi في مصنع بسبب الآلات الصناعية.

5. تعقيد الإدارة والتهيئة

- الوصف: صعوبة تكوين إعدادات الأجهزة يدويًا (مثل VLANs، QoS، أو جداول التوجيه).

- مثال: خطأ في تكوين راوتر يؤدي إلى انقطاع الإنترنت عن قسم كامل في الشركة.

6. التوسع والنمو غير المخطط له

- الوصف: عدم قدرة البنية التحتية الحالية على استيعاب أجهزة جديدة أو احتياجات متزايدة.

- مثال: إضافة عشرات الأجهزة الذكية (IoT) إلى شبكة منزلية دون ترقية السويچ (Switch)، مما يؤدي إلى تباطؤ الشبكة.

7. مشكلات الطبقة المادية (Physical Layer)

- الوصف: تلف الكابلات، أو حدود المسافة (مثل انخفاض جودة إشارة Ethernet بعد 100 متر).

- مثال: انقطاع إشارة الألياف البصرية بسبب انحناء الكابل بشكل حاد.

8. التقنيات القديمة (Legacy Systems)

- الوصف: صعوبة دمج أجهزة قديمة مع تقنيات حديثة.

- مثال: طابعة قديمة تعتمد على منفذ Parallel تحتاج إلى محول خاص للاتصال بشبكة Ethernet.

9. الأخطاء البشرية

- الوصف: إعدادات خاطئة أو توصيلات غير صحيحة.

- مثال: توصيل كابل Ethernet في منفذ خاطئ على السويچ، مما يعطل جزءًا من الشبكة.

10. التحديات اللوجستية والبيئية

- الوصف: تأثير العوامل الخارجية مثل الحرارة، الرطوبة، أو الاهتزازات.

- مثال: تلف كابلات الألياف البصرية في مناطق صحراوية بسبب درجات الحرارة العالية.

11. التكاليف المادية

- الوصف: ارتفاع تكلفة الكابلات عالية الجودة (مثل الألياف البصرية) أو الأجهزة المتطورة.

- مثال: شركة ناشئة تختار كابلات CAT5e بدلاً من CAT8 لتقليل التكاليف، مما يحد من سرعة الشبكة المستقبلية.

12. اختلاف أنظمة التشغيل والبرمجيات

- الوصف: تعارض بين أنظمة إدارة الأجهزة (مثال: تعذر تواصل جهاز يعمل بنظام Linux مع آخر يعمل بـ Windows بسبب إعدادات SMB).

- مثال: فشل مشاركة ملفات بين حاسوب يعمل بـ macOS وآخر بـ Windows دون تكوين صحيح.

13. التحديات في الشبكات اللاسلكية

- الوصف:

  - محدودية التغطية وضعف الإشارة.

  - تداخل الترددات مع شبكات مجاورة.

- مثال: انخفاض جودة مكالمات VoIP في طابق علوي بسبب ضعف إشارة Wi-Fi.

14. الامتثال للأنظمة واللوائح

- الوصف: ضرورة الالتزام بمعايير أمان وحماية البيانات (مثل GDPR أو HIPAA).

- مثال: شركة صحية تُغرم بسبب استخدامها شبكة غير مشفرة تنقل بيانات المرضى.

15. إدارة الطاقة

- الوصف: انقطاع التيار الكهربائي أو عدم كفاية أنظمة UPS.

- مثال: توقف خوادم شركة خلال عاصفة بسبب انقطاع الكهرباء دون وجود مصدر طاقة احتياطي.

16. التحديات في الشبكات الهجينة (Hybrid Networks)

- الوصف: صعوبة دمج البنية التحتية المحلية (On-Premises) مع السحابة (Cloud).

- مثال: بطء الوصول إلى البيانات المخزنة على AWS من فرع الشركة بسبب مشكلات في اتصال WAN.

17. الاعتمادية المفرطة على مورد واحد

- الوصف: انهيار الشبكة بالكامل عند فشل جهاز مركزي (مثل راوتر رئيسي).

- مثال: توقف جميع عمليات البنك بسبب عطل في السويچ الأساسي.

18. التعامل مع الأجهزة الذكية (IoT)

- الوصف:

  - اختلاف بروتوكولات الاتصال (مثل Zigbee مقابل Wi-Fi).

  - زيادة نقاط الضعف الأمنية.

- مثال: ثلاجة ذكية مصابة ببرنامج ضار تُهاجم شبكة المنزل بأكملها.

19. مشكلات التوجيه (Routing)

- الوصف: تعقيد جداول التوجيه أو فشل في تحميل التوازن (Load Balancing).

- مثال: ازدحام حركة البيانات على مسار واحد بينما المسار الآخر غير مُستغل.

20. التعافي من الكوارث (Disaster Recovery)

- الوصف: عدم وجود خطة احتياطية لاستعادة الشبكة بعد انهيارها.

- مثال: حريق في مركز البيانات يدمر جميع الأجهزة دون وجود نسخ احتياطية خارج الموقع.

ملخص التحديات والحلول المقترحة:

التحدي	الحل المقترح
التوافقية	استخدام بوابات أو محولات (Gateways) لتحويل البروتوكولات.
الأمان	تشفير البيانات وتحديث أنظمة الحماية بانتظام.
الإدارة	استخدام أدوات إدارة مركزية مثل Cisco DNA Center.
التكاليف	التخطيط المسبق واختيار حلول قابلة للتوسع.
الأخطاء البشرية	تدريب الفريق واعتماد أتمتة المهام (Automation).

الخلاصة:

مواجهة هذه التحديات يتطلب فهمًا عميقًا لاحتياجات الشبكة، وتخطيطًا استراتيجيًا، واستثمارًا في التقنيات والأدوات المناسبة، مثل:

- الشبكات المعرّفة بالبرمجيات (SDN) لتبسيط الإدارة.

- الحلول السحابية الهجينة لتحسين المرونة.

- أنظمة المراقبة الذكية (مثل Nagios أو SolarWinds) لاكتشاف الأعطال مبكرًا.

الاسئلة الاسترشادية

1- اذكر ثلاثة من أنواع ربط الأجهزة عبر الشبكات
2- اذكر ثلاثة من عوامل اختيار طريقة الاتصال المناسبة
3- اذكر ثلاثة من التحديات التي تواجه ربط الأجهزة عبر الشبكات

المراجع

1- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
2- Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
3- Forouzan, B. A. (2012). *Data Communications and Networking* (5th ed.). McGraw-Hill.
4- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.
5- Forouzan, B. A. (2017). *Data Communications and Networking*. McGraw-Hill Education.
6- Stallings, W. (2013). *Data and Computer Communications*. Pearson.
7- Comer, D. E. (2018). *Internetworking with TCP/IP Volume One* (6th ed.). Pearson.
8- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
9- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Pearson.
10- Internet Society. (2023). *Internet Protocols and Standards*. Retrieved from https://www.internetsociety.org
11- Comer, D. E. (2018). *Internetworking with TCP/IP Volume One* (6th ed.). Pearson.
12- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
13- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
14- CERT Coordination Center. (2020). *Cybersecurity and Internet Challenges*. https://www.us-cert.cisa.gov/
15- OECD. (2020). *The Digital Divide and Global Connectivity*. https://www.oecd.org/digital/
16- Trossen, D., et al. (2019). *The Future of Networking and Communications*. Springer.
17- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
18- Comer, D. E. (2018). *The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works* (5th ed.). Pearson.
19- Leiner, B. M., et al. (2009). *A Brief History of the Internet*. ACM SIGCOMM Computer Communication Review, 39(5), 22–31. https://www.internetsociety.org/internet/history-internet/brief-history-internet/
20- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
21- Comer, D. E. (2018). *The Internet Book: Everything You Need to Know About Computer Networking*. Pearson.
22- Cisco Networking Academy. (2023). *Introduction to Networks v7*. https://www.netacad.com/