محور الشبكات – المحاضرة (2)

# بروتوكولات الاتصال في الشبكات والإنترنت: التفصيل والتطبيق

***Network Communication Protocols: Detailed Study***

| | | | |
|---|---|---|---|
| **المرحلة** | الثانية – الدراسة الصباحية | **المادة** | الحاسوب |
| **الإعداد** | أ.م.د. حيدر حسن محمد | **المدة المقترحة** | ساعتان (نظري + نشاط) |

## أهداف المحاضرة (Learning Objectives)

بعد انتهاء المحاضرة يكون الطالب قادراً على أن:

1. يعرّف البروتوكول (Protocol) ويشرح عناصره ولماذا تُصمَّم الشبكات في طبقات (Layers).
2. يميّز بين نموذجي OSI وTCP/IP ويحدد موقع كل بروتوكول فيهما.
3. يشرح بالتفصيل بروتوكولات: TCP وUDP وIP وICMP وARP وHTTP وHTTPS وFTP وSMTP وPOP3 وIMAP وDNS وDHCP وEthernet.
4. يقارن بين TCP وUDP، وIPv4 وIPv6، وPOP3 وIMAP.
5. يتتبع ما يحدث عند كتابة عنوان موقع في المتصفح خطوة بخطوة.
6. يربط البروتوكولات بتطبيقاتها الرياضية ويستخدم أوامر تشخيص الشبكة.

## خارطة المحاضرة (Lecture Map)

| المحور | العنوان | الجانب التطبيقي |
|---|---|---|
| **1** | مفهوم البروتوكول وعناصره (Concept & Elements) | تشبيه ومقارنة |
| **2** | نموذجا OSI وTCP/IP والتغليف (Layering & Encapsulation) | جدول الطبقات |
| **3** | بروتوكولات النقل: TCP, UDP (Transport Protocols) | بطاقات + مصافحة ثلاثية |
| **4** | بروتوكولات الإنترنت: IP, ICMP, ARP (Internet Protocols) | بطاقات IPv4/IPv6 + |
| **5** | بروتوكولات التطبيقات: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP | بطاقات تفصيلية |
| **6** | بروتوكولات الشبكة المحلية: Ethernet, Wi-Fi (LAN Protocols) | مقارنة المعايير |
| **7** | جدول المنافذ، مثال شامل، تطبيقات رياضية، ونشاط عملي | تتبع طلب ويب |

## أولاً: مفهوم البروتوكول (Concept of Protocol)

**البروتوكول (Protocol)** هو مجموعة من القواعد والمعايير التي تحدد كيفية **تنسيق** البيانات وإرسالها واستقبالها ومعالجة الأخطاء بين الأجهزة في الشبكة، بحيث تفهم الأجهزة المختلفة (من صانعين مختلفين) بعضها.

**تشبيه (Analogy)**

البروتوكول كقواعد المرور: يتفق السائقون على الإشارات والأولويات فتنساب الحركة دون صدام، حتى لو اختلفت السيارات. وهو أيضاً كقواعد لعبة كرة القدم: لا تُلعب مباراة دولية دون قانون موحد.

### العناصر الثلاثة لأي بروتوكول (Elements of a Protocol)

| العنصر | المعنى | مثال |
|---|---|---|
| **البنية (Syntax)** | تنسيق البيانات وترتيب الحقول | ترتيب حقول العنوان والمحتوى في رسالة HTTP |
| **الدلالة (Semantics)** | معنى كل حقل وما يجب فعله | الرمز 404 يعني أن الصفحة غير موجودة |
| **التوقيت (Timing)** | سرعة الإرسال وترتيب الرد | الانتظار قبل إعادة إرسال حزمة لم يصل تأكيدها |

**من يضع البروتوكولات؟ (Standards Bodies):** IETF (وثائق RFC)، IEEE (Ethernet وWi-Fi)، ISO (نموذج OSI)، W3C (معايير الويب)، ITU (الاتصالات).

## ثانياً: النماذج الطبقية والتغليف (Layered Models & Encapsulation)

تُقسَّم عملية الاتصال إلى **طبقات (Layers)** تؤدي كل منها وظيفة محددة وتخدم التي فوقها. فائدة ذلك: تبسيط التصميم، وإمكانية تغيير بروتوكول طبقة دون المساس بالأخرى (كتغيير Wi-Fi إلى كابل دون تغيير المتصفح).

| رقم OSI | طبقة OSI (OSI Layer) | طبقة TCP/IP | أمثلة بروتوكولات / وحدة البيانات |
|---|---|---|---|
| **7** | التطبيق (Application) | التطبيق (Application) | HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP — وحدة: بيانات (Data) |
| **6** | العرض (Presentation) | التطبيق | التشفير والترميز: TLS, JPEG |
| **5** | الجلسة (Session) | التطبيق | إدارة الجلسات |
| **4** | النقل (Transport) | النقل (Transport) | TCP, UDP — وحدة: مقطع (Segment) / Datagram |
| **3** | الشبكة (Network) | الإنترنت (Internet) | IP, ICMP — وحدة: حزمة (Packet) |
| **2** | ربط البيانات (Data Link) | الوصول للشبكة (Network Access) | Ethernet, Wi-Fi, ARP — وحدة: إطار (Frame) |
| **1** | الفيزيائية (Physical) | الوصول للشبكة | الكابلات والإشارات — وحدة: بتات (Bits) |

### التغليف (Encapsulation)

عند إرسال بيانات، تُضيف كل طبقة **ترويسة (Header)** خاصة بها، وكأنك تضع الرسالة في ظرف ثم الظرف في صندوق ثم الصندوق في شاحنة. وعند الاستقبال تُنزع الترويسات بالترتيب المعاكس.

**1. بيانات التطبيق** *Data* ◄ **2. مقطع TCP/UDP** *Segment* ◄ **3. حزمة IP** *Packet*

**4. إطار Ethernet/Wi-Fi** *Frame* ◄ **5. إشارات** *Bits*

**للحفظ**
ترتيب طبقات TCP/IP الأربع من الأعلى: Application → Transport → Internet → Network Access.

## ثالثاً: بروتوكولات النقل (Transport Protocols)

تعمل طبقة النقل بين التطبيقات على الأجهزة المختلفة، وتستخدم **أرقام المنافذ (Ports)** لتحديد أي تطبيق يستلم البيانات: IP يوصل الحزمة إلى الجهاز، والمنفذ يوصلها إلى التطبيق المناسب.

| بروتوكول التحكم بالنقل<br>*TCP – Transmission Control Protocol* | |
|---|---|
| **الوظيفة** | نقل موثوق ومرتب للبيانات بين تطبيقين. |
| **الطبقة** | النقل (Transport). |
| **الخصائص** | موجّه بالاتصال (Connection-oriented)؛ ترقيم المقاطع؛ تأكيد الاستلام (ACK)؛ إعادة إرسال المفقود؛ التحكم بالتدفق (Flow Control) والازدحام (Congestion Control). |
| **آلية العمل** | يبني اتصالاً بمصافحة ثلاثية (3-Way Handshake)، ثم ينقل البيانات المرقمة، ثم يُنهي الاتصال. |
| **يُستخدم في** | الويب (HTTP/HTTPS)، البريد (SMTP, IMAP)، نقل الملفات (FTP). |
| **الأمان** | عرضة لهجمات SYN Flood التي تستغل المصافحة الثلاثية (تُشرح في محاضرة التهديدات). |

### المصافحة الثلاثية في TCP (Three-Way Handshake)

**1. العميل يرسل SYN** *طلب اتصال* ◄ **2. الخادم يردّ SYN-ACK** *موافقة وتأكيد* ◄ **3. العميل يرسل ACK** *تأكيد* ◄ **4. بدء نقل البيانات** *Data Transfer*

| بروتوكول مخطط بيانات المستخدم<br>*UDP – User Datagram Protocol* | |
|---|---|
| **الوظيفة** | نقل سريع وخفيف دون ضمان وصول أو ترتيب. |
| **الخصائص** | غير موجّه بالاتصال (Connectionless)؛ ترويسة صغيرة (8 بايت)؛ لا تأكيد ولا إعادة إرسال؛ زمن تأخير أقل. |
| **يُستخدم في** | البث المباشر، المكالمات الصوتية والمرئية (VoIP)، الألعاب الإلكترونية، استعلامات DNS. |
| **ملاحظة** | بروتوكول QUIC الحديث (أساس HTTP/3) مبني فوق UDP ويضيف الموثوقية والتشفير. |

### مقارنة TCP وUDP

| وجه المقارنة | TCP | UDP |
|---|---|---|
| **الاتصال** | موجّه بالاتصال (مصافحة) | بلا اتصال |
| **الموثوقية** | عالية: تأكيد وإعادة إرسال | غير مضمونة |
| **الترتيب** | يضمن الترتيب | لا يضمنه |
| **السرعة** | أبطأ نسبياً | أسرع وأخف |
| **الاستخدام** | ملفات، صفحات ويب، بريد | بث مباشر، صوت، ألعاب |
| **مثال رياضي** | رفع تقرير أداء أو فيديو للتحليل | بث مباراة مباشرة أو مكالمة مدرب عن بُعد |

## رابعاً: بروتوكولات الإنترنت (Internet Layer Protocols)

| بروتوكول الإنترنت<br>*IP – Internet Protocol* | |
|---|---|
| **الوظيفة** | العنونة (Addressing) وتوجيه الحزم (Routing) من المصدر إلى الوجهة عبر شبكات مختلفة. |
| **الطبقة** | الإنترنت / الشبكة (Network). |
| **الخصائص** | بلا اتصال، وبأفضل جهد (Best Effort): لا يضمن الوصول؛ يعتمد على TCP لتحقيق الموثوقية. |
| **النسختان** | IPv4 (عنوان 32 بت) وIPv6 (عنوان 128 بت). |
| **المكونات** | عنوان المصدر والوجهة، TTL (عدد القفزات المسموحة)، رقم البروتوكول المحمول. |

### مقارنة IPv4 وIPv6

| وجه المقارنة | IPv4 | IPv6 |
|---|---|---|
| **طول العنوان** | 32 بت (نحو 4.3 مليار عنوان) | 128 بت (عدد هائل عملياً) |
| **الشكل** | أربع خانات عشرية: 192.168.1.10 | ثماني مجموعات سداسية عشرية: db8::1:2001 |
| **المشكلة** | نفاد العناوين العامة وحاجة إلى NAT | حل مشكلة النفاد ودعم أفضل للأجهزة المتصلة |
| **الأمان** | IPsec اختياري | تصميمه يتكامل مع IPsec أصلاً (دون أن يكون إلزامياً) |

**عناوين خاصة وعامة (Private vs Public IP)**
العناوين الخاصة (Private) مثل 192.168.x.x و10.x.x.x و172.16.x.x–31 تُستخدم داخل الشبكات المحلية ولا تُوجَّه عبر الإنترنت. أما العنوان العام (Public) فيمنحه مزود الخدمة، وتقوم خاصية **NAT** في الراوتر بترجمة العناوين الخاصة إلى عنوان عام واحد.

| بروتوكول رسائل التحكم بالإنترنت<br>*ICMP – Internet Control Message Protocol* | |
|---|---|
| **الوظيفة** | الإبلاغ عن الأخطاء واختبار الاتصال بين الأجهزة. |
| **الطبقة** | الإنترنت (Network). |
| **أمثلة** | أمر **ping** يرسل Echo Request ويستلم Echo Reply، وأمر **tracert/traceroute** يكشف المسار بتغيير TTL. |
| **الأمان** | قد يُستغل في الاستطلاع أو الإغراق، لذلك تقيّده بعض الجدران النارية. |

| بروتوكول تحليل العناوين<br>*ARP – Address Resolution Protocol* | |
|---|---|
| **الوظيفة** | تحويل عنوان IP إلى عنوان MAC (العنوان الفيزيائي لبطاقة الشبكة) داخل الشبكة المحلية. |
| **آلية العمل** | يبث الجهاز سؤالاً: «من يملك العنوان 192.168.1.1؟» فيرد صاحب العنوان بعنوان MAC الخاص به. |
| **الأمان** | لا يتحقق من هوية المجيب، فهو عرضة لانتحال ARP Spoofing الذي يُستخدم في هجمات الرجل في الوسط. |

## خامساً: بروتوكولات التطبيقات (Application Layer Protocols)

| بروتوكول نقل النص التشعبي *HTTP – HyperText Transfer Protocol* | |
|---|---|
| **الوظيفة** | نقل صفحات الويب والموارد بين الخادم والمتصفح. |
| **النموذج** | طلب واستجابة (Request / Response) فوق TCP، المنفذ الافتراضي 80. |
| **الطرائق (Methods)** | GET لطلب مورد، POST لإرسال بيانات، PUT للتحديث، DELETE للحذف. |
| **الإصدارات** | HTTP/1.1، ثم HTTP/2، ثم HTTP/3 فوق QUIC/UDP. |
| **الأمان** | ينقل البيانات بنص واضح (غير مشفر)، فيمكن اعتراضها. |

| رمز الحالة (Status Code) | الفئة | المعنى |
|---|---|---|
| **200** | نجاح (Success) | تم الطلب بنجاح |
| **302 / 301** | إعادة توجيه (Redirect) | المورد انتقل إلى عنوان آخر |
| **403** | خطأ عميل (Client Error) | ممنوع الوصول |
| **404** | خطأ عميل | الصفحة غير موجودة |
| **500** | خطأ خادم (Server Error) | عطل داخلي في الخادم |

| HTTP الآمن *HTTPS – HTTP over TLS* | |
|---|---|
| **الوظيفة** | نقل صفحات الويب مع تشفير وتوثيق الخادم وحماية سلامة البيانات. |
| **آلية العمل** | HTTP فوق طبقة التشفير TLS، المنفذ 443. تعتمد على **شهادة رقمية (Digital Certificate)** يصدرها مرجع موثوق (CA). |
| **الخطوات** | المتصفح يطلب الاتصال ← الخادم يرسل شهادته ← تحقق المتصفح منها ← الاتفاق على مفاتيح تشفير الجلسة ← نقل البيانات مشفّرة. |
| **الحماية** | السرية (Confidentiality) + السلامة (Integrity) + توثيق الخادم (Authentication). |
| **تنبيه** | القفل يعني أن الاتصال مشفّر فقط، ولا يعني أن الموقع نفسه أمين أو غير احتيالي. |
| **ملاحظة** | SSL هو الاسم القديم وتم التخلي عنه؛ الإصدار الحديث هو TLS 1.2 وTLS 1.3. |

| بروتوكول نقل الملفات *FTP – File Transfer Protocol* | |
|---|---|
| **الوظيفة** | نقل الملفات بين حاسوبين عبر الشبكة (رفع Upload وتنزيل Download). |
| **الخصائص** | فوق TCP؛ المنفذ 21 للأوامر والمنفذ 20 للبيانات في الوضع النشط؛ يتطلب اسم مستخدم وكلمة مرور. |
| **الأمان** | ينقل بيانات الدخول والملفات دون تشفير؛ يُستعاض عنه بـ **SFTP** (عبر SSH، المنفذ 22) أو **FTPS** (FTP فوق TLS). |
| **مثال** | رفع مصمم الموقع ملفات الصفحات إلى خادم الاستضافة. |

| بروتوكول نقل البريد البسيط *SMTP – Simple Mail Transfer Protocol* | |
|---|---|
| **الوظيفة** | **إرسال** البريد الإلكتروني من العميل إلى الخادم ومن خادم إلى آخر. |
| **المنفذ** | 25 بين الخوادم، و587 لإرسال العميل (مع التشفير)، و465 (SMTPS). |
| **الخصائص** | بروتوكول نصي بأوامر مثل MAIL FROM وRCPT TO وDATA. |
| **الأمان** | صُمم دون توثيق قوي للمرسل، فسهّل انتحال العناوين (Spoofing) وهجمات التصيد، ولذلك أُضيفت آليات مثل SPF وDKIM وDMARC. |

| بروتوكولا استقبال البريد *POP3 & IMAP* | |
|---|---|
| **POP3 (Post Office Protocol v3** | **يحمّل** الرسائل إلى جهازك وغالباً يحذفها من الخادم؛ المنفذ 110 (أو 995 مشفّر). مناسب لجهاز واحد وللعمل دون اتصال. |
| **IMAP (Internet Message Access Protocol** | **يزامن** الرسائل مع الخادم فتبقى عليه وتظهر على جميع أجهزتك؛ المنفذ 143 (أو 993 مشفّر). مناسب لأكثر من جهاز. |
| **الأمان** | يجب استخدام النسخ المشفّرة (بمنافذ 995 و993) لمنع كشف كلمة المرور. |

**1. المرسل** *Mail Client* ◄ **2. SMTP: خادم المرسل** ◄ **3. SMTP: خادم المستلم**

**4. POP3 / IMAP** ◄ **5. المستلم** *Mail Client*

| نظام أسماء النطاقات *DNS – Domain Name System* | |
|---|---|
| **الوظيفة** | تحويل أسماء النطاقات (www.uomustansiriyah.edu.iq) إلى عناوين IP؛ فهو «دليل هاتف الإنترنت». |
| **الطبقة والمنفذ** | طبقة التطبيق؛ المنفذ 53 (UDP غالباً، وTCP للاستجابات الكبيرة). |
| **الهرمية** | الخادم الجذر (Root) ← خوادم النطاقات العليا (TLD: .com, .edu, .iq) ← الخادم المخوّل (Authoritative). |
| **خطوات الاستعلام** | الجهاز يسأل المحلل المتكرر (Recursive Resolver) ← يسأل الجذر ثم TLD ثم الخادم المخوّل ← يعود بالعنوان ويُخزَّن مؤقتاً (Cache). |
| **الأمان** | عرضة لانتحال DNS (DNS Spoofing/Cache Poisoning)، ويُعزَّز بـ DNSSEC وDNS over HTTPS. |

| بروتوكول التهيئة الديناميكية للمضيف *DHCP – Dynamic Host Configuration Protocol* | |
|---|---|
| **الوظيفة** | منح الأجهزة عنوان IP وقناع الشبكة والبوابة وDNS تلقائياً عند الاتصال. |
| **الخطوات DORA** | Discover (اكتشاف) ← Offer (عرض) ← Request (طلب) ← Acknowledge (تأكيد). |

| | |
|---|---|
| **المنفذ** | UDP 67 (الخادم) و68 (العميل). |
| **الأمان** | قد يُنتحل بخادم DHCP مزيف (Rogue DHCP) يوزع بوابة خبيثة. |

## سادساً: بروتوكولات الشبكة المحلية (LAN Protocols)

| **إيثرنت** *Ethernet – IEEE 802.3* | |
|---|---|
| **الوظيفة** | تحديد كيفية إرسال الإطارات (Frames) عبر الكابلات في الشبكة المحلية. |
| **التاريخ** | طوّره Robert Metcalfe وزملاؤه في Xerox PARC في السبعينيات، وتبنّاه IEEE كمعيار 802.3. |
| **عنوان MAC** | عنوان فيزيائي من 48 بت (مثل 00:1A:2B:3C:4D:5E) يميز بطاقة الشبكة. |
| **السرعات** | من 10 ميغابت/ث إلى 100 وغيغابت وما فوق في الأنظمة الحديثة. |
| **آلية الوصول** | اعتمد قديماً CSMA/CD للتعامل مع التصادمات، وحلّت المبدلات (Switches) محله فاختفت التصادمات عملياً. |

| **الواي فاي** *Wi-Fi – IEEE 802.11* | |
|---|---|
| **الوظيفة** | ربط الأجهزة لاسلكياً بالشبكة المحلية عبر نقطة وصول (Access Point). |
| **الأجيال** | 802.11be/802.11n (Wi-Fi 4) ← 802.11ac (Wi-Fi 5) ← 802.11ax (Wi-Fi 6 ← 6E) (Wi-Fi 7). |
| **النطاقات** | 2.4 غيغاهرتز (مدى أبعد وسرعة أقل) و5 و6 غيغاهرتز (سرعة أعلى ومدى أقصر). |
| **الأمان** | WEP (ضعيف ومهجور) ← WPA ← WPA2 ← WPA3 (الأحدث والموصى به). |

**بروتوكولات رياضية قريبة (Sports Wearables)**
تتصل الساعات وأحزمة النبض بالهاتف غالباً عبر **Bluetooth Low Energy (BLE)** أو **ANT+**، وهما بروتوكولان لاسلكيان قصيرا المدى ومنخفضا الاستهلاك للطاقة، ثم يزامن الهاتف البيانات عبر HTTPS إلى الخوادم السحابية.

## سابعاً: جدول المنافذ الشائعة (Well-Known Ports)

| البروتوكول | المنفذ | النقل | ملاحظة أمنية |
|---|---|---|---|
| **HTTP** | 80 | TCP | غير مشفر |
| **HTTPS** | 443 | TCP | مشفّر بـ TLS |
| **FTP** | 21 (و20) | TCP | غير مشفر؛ استخدم SFTP/FTPS |
| **SSH / SFTP** | 22 | TCP | مشفّر؛ بديل آمن لـ Telnet |
| **Telnet** | 23 | TCP | غير مشفر؛ يُمنع |
| **SMTP** | 25 / 587 / 465 | TCP | فعّل التشفير والتوثيق |
| **DNS** | 53 | UDP/TCP | عرضة للانتحال |

| البروتوكول | المنفذ | النقل | ملاحظة أمنية |
|---|---|---|---|
| **DHCP** | 68 / 67 | UDP | احذر الخوادم المزيفة |
| **POP3** | 110 (995) | TCP | استخدم 995 المشفّر |
| **IMAP** | 143 (993) | TCP | استخدم 993 المشفّر |

## ثامناً: مثال شامل: ماذا يحدث عند كتابة عنوان موقع؟ (What Happens When You Type a URL)

افترض أنك كتبت في المتصفح عنوان موقع اتحاد رياضي https://example-federation.org:

**1. DNS:** ترجمة الاسم إلى عنوان IP ◄ **2. ARP/DHCP:** معرفة البوابة والعنوان المحلي ◄ **3. TCP:** مصافحة ثلاثية مع الخادم ◄ **4. TLS:** التحقق من الشهادة وتبادل المفاتيح

**5. HTTP:** إرسال طلب GET ◄ **6.** الخادم يرسل الاستجابة 200 + الصفحة ◄ **7.** المتصفح يعرض الصفحة *HTML*

لاحظ أن عدة بروتوكولات تعمل معاً في ثوانٍ: **DHCP** منحك عنوانك أصلاً، و**ARP** ربط العنوان بالجهاز المحلي، و**DNS** ترجم الاسم، و**TCP** أنشأ القناة الموثوقة، و**TLS** حماها، و**HTTP** طلب الصفحة، و**IP** وجّه الحزم عبر الإنترنت، و**Ethernet/Wi-Fi** نقل الإطارات.

## تاسعاً: البروتوكولات في التطبيقات الرياضية (Protocols in Sports Applications)

| السيناريو | البروتوكولات | السبب |
|---|---|---|
| **بث مباراة مباشرة** | HTTP / UDP (مع مقاطع صغيرة) / QUIC | سرعة وتأخير أقل مع تحمّل فقدان بسيط |
| **رفع تقرير أداء أو فيديو للتحليل** | SFTP أو TCP + HTTPS | ضمان وصول الملف كاملاً مع التشفير |
| **إرسال برنامج تدريبي للاعب بالبريد** | SMTP + IMAP (مشفّرة) | إرسال واستقبال مع مزامنة الأجهزة |
| **حجز بطولة أو شراء تذكرة** | HTTPS | حماية بيانات الدفع والهوية |
| **ساعة رياضية تزامن البيانات** | BLE/ANT+ ثم HTTPS | اتصال موفّر للطاقة ثم نقل آمن للسحابة |
| **شبكة قاعة رياضية** | DHCP + Wi-Fi 802.11 + DNS | منح العناوين تلقائياً وتوصيل المستخدمين |

## عاشراً: نشاط عملي: تتبّع البروتوكولات (Hands-on Activity)

| الأمر | البروتوكول الذي تتتبعه | المطلوب |
|---|---|---|
| **ipconfig /all** | DHCP + IP + MAC | سجّل عنوان IP والبوابة وخادم DHCP وDNS وعنوان MAC |
| **ping 8.8.8.8** | ICMP | سجّل متوسط زمن الاستجابة وعدد الحزم المفقودة |
| **nslookup uomustansiriyah.edu.iq** | DNS | سجّل عنوان IP الذي يظهر |
| **tracert 8.8.8.8** | ICMP + TTL | عدد القفزات |

| الأمر | البروتوكول الذي تتتبعه | المطلوب |
|---|---|---|
| **arp -a** | ARP | اذكر جهازين وعنوانَي MAC المقابلين |

**ملحوظة:** نفّذ هذه الأوامر على شبكتك الشخصية أو شبكة المختبر الجامعي فقط وبإذن المشرف.

## حادي عشر: مسرد المصطلحات (Glossary)

| المصطلح (Term) | المعنى |
|---|---|
| **Protocol** | بروتوكول: قواعد الاتصال |
| **Layer** | طبقة |
| **Encapsulation** | التغليف: إضافة ترويسة في كل طبقة |
| **Port** | منفذ: يحدد التطبيق على الجهاز |
| **Handshake** | مصافحة: تبادل لإنشاء الاتصال |
| **ACK** | رسالة تأكيد الاستلام |
| **Header** | ترويسة تحمل معلومات التحكم |
| **MAC Address** | العنوان الفيزيائي لبطاقة الشبكة |
| **IP Address** | عنوان الجهاز في الشبكة |
| **NAT** | ترجمة العناوين الخاصة إلى عامة |
| **TTL** | الوقت/القفزات المسموحة للحزمة |
| **Certificate** | شهادة رقمية لتوثيق الموقع |
| **Resolver** | محلّل DNS |
| **Lease** | مدة تأجير عنوان IP من DHCP |
| **Latency** | زمن الاستجابة |

## ثاني عشر: أسئلة تدريبية (Practice Questions)

### أولاً: اختيار من متعدد (Multiple Choice)

**1) البروتوكول المناسب لبث مباراة مباشرة يحتمل فقدان بعض الحزم هو:**

أ) TCP
ب) UDP
ج) FTP
د) POP3

**2) منفذ HTTPS الافتراضي:**

أ) 80
ب) 21
ج) 443
د) 25

**3) وظيفة DNS:**

أ) تشفير الرسائل
ب) تحويل أسماء النطاقات إلى عناوين IP
ج) منح العنوان تلقائياً
د) نقل الملفات

**4) الخطوات الأربع لـ DHCP بالترتيب:**

أ) Discover, Offer, Request, Acknowledge
ب) Request, Offer, Discover, Acknowledge
ج) Offer, Discover, Acknowledge, Request
د) Acknowledge, Request, Offer, Discover

**5) البروتوكول الذي يزامن البريد على عدة أجهزة هو:**

أ) POP3
ب) SMTP
ج) IMAP
د) FTP

## ثانياً: صح أم خطأ (True / False)

1. TCP يضمن وصول البيانات مرتبة عبر التأكيد وإعادة الإرسال. ( )
2. FTP ينقل الملفات وكلمة المرور مشفّرة افتراضياً. ( )
3. عنوان IPv6 طوله 128 بتاً. ( )
4. ARP يحوّل عنوان IP إلى عنوان MAC. ( )

## ثالثاً: أسئلة قصيرة (Short Answer)

1. عدّد عناصر البروتوكول الثلاثة مع مثال لكل منها.
2. اشرح المصافحة الثلاثية في TCP.
3. قارن بين POP3 وIMAP.

## رابعاً: أسئلة تطبيقية (Applied)

1. تتبّع بالتسلسل البروتوكولات المستخدمة عند فتح موقع الجامعة من هاتفك عبر Wi-Fi.
2. اختر بروتوكولات مناسبة لثلاثة تطبيقات في نادٍ رياضي وبرّر اختيارك.

## الإجابات النموذجية (Answer Key)

| القسم | الإجابة |
|---|---|
| **اختيار من متعدد** | 1-ب ، 2-ج ، 3-ب ، 4-أ ، 5-ج |
| **صح / خطأ** | 1-صح ، 2-خطأ ، 3-صح ، 4-صح |

## ملخص المحاضرة (Summary)

- البروتوكول قواعد مشتركة تضمن تفاهم الأجهزة، وتُنظَّم البروتوكولات في طبقات تتعاون عبر التغليف.
- TCP للموثوقية وUDP للسرعة، وIP للعنونة والتوجيه، وDNS للأسماء، وDHCP للعناوين التلقائية، وHTTP/HTTPS للويب.
- كثير من البروتوكولات القديمة (HTTP, FTP, Telnet, POP3) غير مشفرة، ولذلك يجب استبدالها أو تأمينها؛ وهذا موضوع المحاضرة القادمة.

## المصادر والمراجع (References)

1. Kurose JF, Ross KW. Computer Networking: A Top-Down Approach. Pearson (latest edition).
2. Tanenbaum AS, Wetherall DJ. Computer Networks. 5th ed. Pearson; 2011.
3. Stallings W. Data and Computer Communications. Pearson (latest edition).
4. Postel J. RFC 793: Transmission Control Protocol. IETF; 1981. | RFC 768: User Datagram Protocol. 1980. | RFC 791: Internet Protocol. 1981.
5. Mockapetris P. RFC 1034/1035: Domain Names – Concepts and Facilities / Implementation and Specification. IETF; 1987.
6. Fielding R, et al. RFC 9110: HTTP Semantics. IETF; 2022. | Rescorla E. RFC 8446: TLS Protocol Version 1.3. IETF; 2018.
7. Klensin J. RFC 5321: Simple Mail Transfer Protocol. IETF; 2008. | Crispin M. RFC 3501: IMAP Version 4rev1. 2003.
8. Droms R. RFC 2131: Dynamic Host Configuration Protocol. IETF; 1997. | Deering S, Hinden R. RFC 8200: IPv6 Specification. 2017.
9. IEEE Std 802.3 (Ethernet) and IEEE Std 802.11 (Wireless LAN).

إعداد: **أ.م.د. حيدر حسن محمد**

**مدرس المادة**