اليوم الثلاثون: TCP و UDP

مقدمة عن بروتوكولات طبقة النقل

في نموذج OSI، طبقة النقل (Transport Layer) هي الطبقة الرابعة. في نموذج TCP/IP، هذه هي الطبقة الثالثة. المهمة الرئيسية لطبقة النقل هي توفير اتصال من طرف إلى طرف (End-to-End Communication) بين التطبيقات على أجهزة مختلفة. البروتوكولان الرئيسيان في هذه الطبقة هما TCP (Transmission Control Protocol) و UDP (User Datagram Protocol).

لفهم الفرق بينهما، تخيل أنك تريد إرسال رسالة إلى صديق. TCP يشبه إرسال رسالة مسجلة (Registered Mail) حيث تحصل على إيصال يؤكد وصول الرسالة، وإذا لم تصل يعيد النظام إرسالها، وتصل الرسائل بالترتيب الصحيح. UDP يشبه إرسال بطاقة بريدية (Postcard) - ترسلها ولا تعرف إن وصلت أم لا، وهي أسرع وأبسط. في الشبكات، نختار TCP عندما تكون الموثوقية مهمة (مثل تحميل ملف أو تصفح ويب)، ونختار UDP عندما تكون السرعة أهم من الموثوقية (مثل بث فيديو مباشر أو VoIP).

TCP - بروتوكول التحكم بالإرسال

TCP هو بروتوكول موجه للاتصال (Connection-Oriented). هذا يعني أنه قبل إرسال أي بيانات، يجب إنشاء اتصال (Connection) بين المرسل والمستقبل. TCP يضمن وصول البيانات بشكل موثوق (Reliable) وبالترتيب الصحيح (In-Order).

مميزات TCP:

1. موثوقية (Reliability): يستخدم أرقام تسلسل (Sequence Numbers) وتأكيدات (Acknowledgments) لضمان وصول كل حزمة. إذا لم يستقبل المرسل تأكيداً لحزمة خلال وقت معين، يعيد إرسالها.

2. التحكم بالتدفق (Flow Control): يستخدم TCP آلية النافذة المنزلقة (Sliding Window) لمنع المرسل من إغراق المستقبل بكمية بيانات أكبر مما يستطيع معالجته.

3. التحكم بالازدحام (Congestion Control): يكتشف TCP ازدحام الشبكة ويبطئ الإرسال تلقائياً لتجنب تفاقم الازدحام.

4. ترتيب البيانات (Ordering): كل حزمة TCP لها رقم تسلسل (Sequence Number). المستقبل يعيد ترتيب الحزم إذا وصلت بترتيب مختلف.

5. فحص الأخطاء (Error Checking): TCP يحتوي على حقل 16 بت (Checksum) للتحقق من سلامة البيانات.

Three-Way Handshake (المصافحة الثلاثية)

قبل أن يبدأ جهازان بتبادل البيانات عبر TCP، يجب إنشاء اتصال. هذا يتم عبر عملية تسمى Three-Way Handshake

(المصافحة الثلاثية). تتكون من ثلاث خطوات:

الخطوة الأولى: يرسل العميل (Client) حزمة TCP مع علم SYN (Synchronize) مضبوط إلى 1. يختار العميل رقم تسلسل أولي (Initial Sequence Number - ISN) عشوائياً. هذه الحزمة تقول: "أريد إنشاء اتصال. هذا هو رقمي التسلسلي الأول."

الخطوة الثانية: يستقبل الخادم (Server) حزمة SYN. إذا كان الخادم مستعداً لاستقبال الاتصال، يرد بحزمة تحتوي على علمي SYN و ACK مضبوطين. يضع الخادم رقم التأكيد (ACK Number = ISN) الخاص بالعميل + 1. ويختار رقم تسلسل خاص به (Server ISN). هذه الحزمة تقول: "تم استقبال طلبك. أنا موافق. هذا رقمي التسلسلي."

الخطوة الثالثة: يرسل العميل حزمة مع علم ACK فقط مضبوط. يضع رقم التأكيد = Server ISN + 1. الآن تم إنشاء الاتصال ويمكن بدء تبادل البيانات. هذه الحزمة تقول: "تم استقبال ردك. الآن يمكننا البدء في إرسال البيانات."

هذه العملية تضمن أن كلا الطرفين جاهزان ومتزامنان قبل بدء إرسال البيانات الفعلية. بعد انتهاء الاتصال، يتم استخدام عملية مشابهة مكونة من 4 خطوات (Four-Way Handshake) لإغلاق الاتصال باستخدام FIN (Finish).

التحكم بالتدفق (Flow Control) والنافذة المنزلقة (Sliding Window)

التحكم بالتدفق يضمن أن المرسل لا يرسل بيانات أسرع مما يستطيع المستقبل معالجته. كيف يعمل؟ المستقبل يعلن عن حجم نافذته (Window Size) في كل حزمة TCP. النافذة هي عدد البايتات التي يمكن للمستقبل استقبالها حالياً. المرسل يرسل فقط ضمن حدود هذه النافذة.

إذا كان المستقبل مشغولاً أو لديه ذاكرة مؤقتة ممتلئة (Buffer Full)، يخفض حجم النافذة. إذا أصبحت النافذة 0، يتوقف المرسل عن الإرسال تماماً حتى يستقبل إعلاناً بنافذة جديدة غير صفرية. هذه الآلية تسمى Sliding Window لأن النافذة "تنزلق" للأمام مع استقبال البيانات والتأكيد عليها.

مثال مبسط: إذا أعلن المستقبل عن نافذة بحجم 1000 بايت، يمكن للمرسل إرسال 1000 بايت دون انتظار تأكيد. عندما يستقبل تأكيداً لأول 500 بايت، "تنزلق" النافذة إلى الأمام 500 بايت، ويمكن للمرسل إرسال 500 بايت إضافية. هذا يحسن الكفاءة لأن المرسل لا ينتظر تأكيد كل حزمة على حدة.

أعلام TCP (TCP Flags)

رأس TCP (TCP Header) يحتوي على حقل أعلام (Flags) بحجم 6 بتات (في الأجهزة الحديثة 9 بتات). كل بت يمثل علماً (Flag) يمكن ضبطه إلى 1 أو 0. الأعلام الستة الأساسية:

1. SYN (Synchronize): يستخدم في بداية الاتصال للمزامنة بين الأرقام التسلسلية. حزم SYN عادة أول حزمة في أي اتصال TCP.

2. ACK (Acknowledgment): يشير إلى أن حقل رقم التأكيد (ACK Number) صالح. جميع الحزم بعد المصافحة الثلاثية لديها ACK = 1 (ماعدا SYN الأولى).

3. FIN (Finish): يستخدم لإنهاء الاتصال. عندما يريد أحد الطرفين إنهاء الاتصال، يرسل حزمة مع FIN = 1.

4. RST (Reset): يستخدم لإعادة ضبط الاتصال فجأة. يرسل RST عند حدوث خطأ غير متوقع أو عندما يحاول جهاز إنشاء

اتصال بمنفذ غير موجود.

5. PSH (Push): يطلب من طبقة TCP تسليم البيانات فوراً إلى التطبيق دون انتظار ملء المخزن المؤقت. مفيد للتطبيقات التفاعلية مثل Telnet و SSH.

6. URG (Urgent): يشير إلى أن بعض البيانات في الحزمة عاجلة ويجب معالجتها فوراً. يستخدم مع حقل Urgent Pointer لتحديد نهاية البيانات العاجلة.

هذه الأعلام تساعد TCP في إدارة الاتصال بشكل دقيق. على سبيل المثال، معرفة حزمة SYN تسمح ببناء المصافحة الثلاثية. معرفة حزمة FIN تسمح بإنهاء الاتصال بشكل مهذب.

رأس TCP (TCP Header)

رأس TCP له حجم 20 بايت (بدون خيارات) ويمكن أن يصل إلى 60 بايت مع الخيارات. الحقول الرئيسية:

1. Source Port (16 بت): منفذ المصدر (0-65535).
2. Destination Port (16 بت): منفذ الوجهة (0-65535).
3. Sequence Number (32 بت): الرقم التسلسلي للحزمة. يستخدم لترتيب الحزم والتحكم بالتدفق.
4. Acknowledgment Number (32 بت): تأكيد استقبال البيانات. يحتوي على رقم التسلسل التالي المتوقع استقباله.
5. Data Offset (4 بت): حجم رأس TCP (بالكلمات 32 بت). يحدد أين تبدأ البيانات.
6. Reserved (3 بت): محجوز للاستخدام المستقبلي.
7. Flags (9 بت): الأعلام المختلفة (SYN, ACK, FIN, RST, PSH, URG).
8. Window Size (16 بت): حجم النافذة (كم بايت يمكن استقبالها).
9. Checksum (16 بت): فحص أخطاء لكل من رأس TCP والبيانات.
10. Urgent Pointer (16 بت): يشير إلى نهاية البيانات العاجلة (يستخدم مع URG flag).
11. Options (متغير): خيارات إضافية مثل MSS و Window Scaling.

UDP - بروتوكول بيانات المستخدم

UDP هو بروتوكول بسيط بدون اتصال (Connectionless). على عكس TCP، لا يوجد مصافحة ثلاثية، لا يوجد ترتيب للبيانات، لا يوجد إعادة إرسال. UDP يرسل البيانات مباشرة دون أي تحضير. هذا يجعله أسرع بكثير من TCP ولكن أقل موثوقية.

مميزات UDP: سرعة عالية لأنه لا يوجد overhead للمصافحة والتأكيد. تأخير منخفض (Low Latency) مما يجعله مثالياً للتطبيقات الحية. بث (Broadcast) ممكن لأن UDP لا يتطلب اتصالاً. مفيد عندما يمكن تحمل فقدان بعض البيانات (Loss Tolerant).

عيوب UDP: لا ضمان لوصول البيانات (Best Effort). لا إعادة إرسال للحزم المفقودة. لا ترتيب للحزم (قد تصل بترتيب مختلف). لا تحكم بالتدفق أو الازدحام.

رأس UDP صغير جداً: 8 بايت فقط (مقارنة بـ 20 بايت لـ TCP). يحتوي على 4 حقول فقط: Source Port (16 بت)، Destination Port (16 بت)، Length (16 بت - طول الرأس + البيانات)، Checksum (16 بت - اختياري في IPv4).

أرقام المنافذ (Port Numbers)

يستخدم كل من TCP و UDP أرقام المنافذ لتحديد التطبيق أو الخدمة التي تتصل بها. المنافذ مقسمة إلى ثلاث نطاقات:

النطاق الأول: 0-1023 (Well-Known Ports). هذه منافذ محجوزة للخدمات المعروفة. يجب أن تعمل بصلاحية مسؤول (Root/Administrator) لتشغيل خدمة على منفذ أقل من 1024. أمثلة: FTP (20, 21)، HTTPS (443)، HTTP (80)، DHCP (67, 68)، DNS (53)، Telnet (23)، SSH (22).

النطاق الثاني: 1024-49151 (Registered Ports). هذه منافذ مسجلة يمكن للشركات استخدامها لتطبيقاتها. أمثلة: Microsoft RDP (3389)، RADIUS (1812, 1813)، SQL Server (1433).

النطاق الثالث: 49152-65535 (Dynamic / Private Ports). هذه منافذ عشوائية (Ephemeral Ports) تستخدمها التطبيقات مؤقتاً عند الاتصال بخادم. على سبيل المثال، عندما تتصفح موقع ويب، يستخدم متصفحك منفذاً عشوائياً في هذا النطاق للاتصال بالخادم على المنفذ 80.

المنافذ الشائعة التي يجب حفظها لـ CCNA

هذه المنافذ تحتاج حفظها لامتحان CCNA:

- FTP (File Transfer Protocol): 20 (بيانات) و 21 (تحكم) - TCP
- SSH (Secure Shell): 22 - TCP
- Telnet: 23 - TCP
- SMTP (Simple Mail Transfer Protocol): 25 - TCP
- DNS (Domain Name System): 53 - UDP (و TCP للمناطق)
- DHCP (Dynamic Host Configuration Protocol): 67 (خادم) و 68 (عميل) - UDP
- TFTP (Trivial File Transfer Protocol): 69 - UDP
- HTTP (Hypertext Transfer Protocol): 80 - TCP
- POP3 (Post Office Protocol v3): 110 - TCP
- NTP (Network Time Protocol): 123 - UDP

SNMP (Simple Network Management Protocol): 161 - UDP -

HTTPS (HTTP Secure): 443 - TCP -

```
! عرض اتصالات TCP الحالية على موجه Cisco
Router# show tcp brief
TCB        Local Address           Foreign Address         (state)
0x123456   192.168.1.1.23          192.168.1.100.49152     ESTAB
0x789ABC   192.168.1.1.443         10.0.0.2.51000          ESTAB

! عرض إحصائيات UDP
Router# show udp
! (المفتوحة UDP هذا الأمر يظهر تفاصيل عن مآخذ)
```

ملاحظة مهمة: الفرق الأساسي بين TCP و UDP يجب أن يكون واضحاً تماماً لامتحان CCNA. TCP = موثوق، موجّه للاتصال، بطيء نسبياً. UDP = غير موثوق، بدون اتصال، سريع. اختر TCP للتطبيقات التي تحتاج إلى تكامل البيانات (مثل البريد الإلكتروني وتصفح الويب). اختر UDP للتطبيقات الحساسة للوقت (مثل VoIP والبث المباشر والألعاب عبر الإنترنت).