

أساسيات الشبكات الحاسوبية

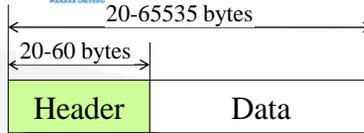
مدرس المقرر
أ.د. مثنى علي القبيلي

العام الدراسي 2023-2024

الفصل الدراسي الثاني

<https://manara.edu.sy/>

البروتوكول IPv4: شكل رزمة البيانات



VER 4 bits	HLEN 4 bits	Type of Service 8 bits	Total Length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation Offset 13 bits
Time To Live 8 bits		Protocol 8 bits	Header Checksum 16 bits	
Source IP address 32 bits				
Destination IP address 32 bits				
IP Option Var				

IP Header: Version, Length, ToS

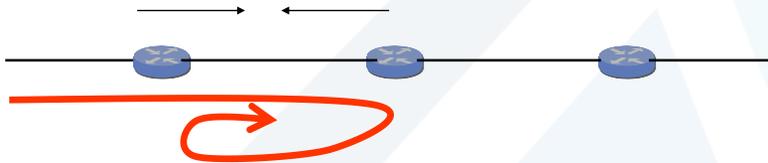
- Version number (4 bits)
 - Indicates the version of the IP protocol
 - Necessary to know what other fields to expect
 - Typically “4” (for IPv4), and sometimes “6” (for IPv6)
- Header length (4 bits)
 - Number of 32-bit words in the header
 - The smallest value is 5: $5 * 32 = 160 \text{ bits} = 20 \text{ bytes}$
 - Can be more when “IP options” are used (eg. The biggest value is 15: $15 * 32 = 480 \text{ bits} = 60 \text{ bytes}$ (max header))
- Type-of-Service (8 bits)
 - Allow packets to be treated differently based on needs
 - E.g., low delay for audio, high bandwidth for bulk transfer

IP Header: Length, Fragments, TTL

- Total length (16 bits)
 - Number of bytes in the packet
 - Maximum size is 65,535 bytes ($2^{16} - 1$)
 - ... though underlying links may impose harder limits
- Fragmentation information (32 bits)
 - Packet identifier, flags, and fragment offset
 - Supports dividing a large IP packet into fragments
 - ... in case a link cannot handle a large IP packet
- Time-To-Live (8 bits)
 - Used to identify packets stuck in forwarding loops
 - ... and eventually discard them from the network

IP Header: More on Time-to-Live (TTL)

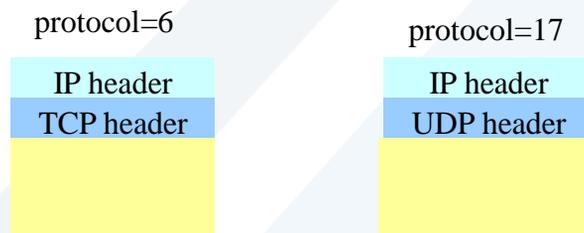
- Potential robustness problem
 - ✓ Forwarding loops can cause packets to cycle forever
 - ✓ Confusing if the packet arrives much later



- Time-to-live field in packet header
 - ✓ TTL field decremented by each router on the path
 - ✓ Packet is discarded when TTL field reaches 0...
 - ✓ ...and "time exceeded" message is sent to the source

IP Header Fields: Transport Protocol

- Protocol (8 bits)
 - Identifies the higher-level protocol
 - ✓ E.g., "6" for the Transmission Control Protocol (TCP)
 - ✓ E.g., "17" for the User Datagram Protocol (UDP)
 - Important for demultiplexing at receiving host
 - ✓ Indicates what kind of header to expect next



البروتوكول IPv4: Protocol



حيث يتم إخبار العقدة الهدف بالبروتوكول الذي سيتم استخدامه مثلًا TCP ➤

يوجد فقط 256 قيمة يمكن تحديدها هنا ➤

تم تحديد وحفظ قائمة البروتوكولات من قبل IANA والتي نمت إلى 135 بروتوكول الآن ➤

يبين الجدول التالي محددات بروتوكول لبعض البروتوكولات الشائعة ➤

Protocol Number	Protocol	RFC
1	Internet Control Message Protocol (ICMP)	RFC 792
2	Internet Group Message Protocol (IGMP)	RFC 1112
4	IP encapsulated within IP	RFC 2003
6	Transmission Control Protocol (TCP)	RFC 793
17	User Datagram Protocol (UDP)	RFC 768
46	ReSource reSerVation Protocol (RSVP)	RFC 2205
47	General Routing Encapsulation (GRE)	RFC 2784
89	Open Shortest Path First (OSPF)	RFC 2328
124	IS-IS Intradomain Routing Protocol (IS-IS)	RFC 1142
132	Stream Control Transmission Protocol (SCTP)	RFC 2960

<http://www.iana.org/assignments/protocol-numbers>

7

<https://manara.edu.sy/>



IP Header: Checksum on the Header

- Checksum (16 bits)
 - Sum of all 16-bit words in the IP packet header
 - If any bits of the header are corrupted in transit
 - ... the checksum won't match at receiving host
 - Receiving host discards corrupted packets
 - ✓ Sending host will retransmit the packet, if needed

$$\begin{array}{r}
 134 \\
 + 212 \\
 \hline
 = 346
 \end{array}
 \quad \longrightarrow \quad
 \begin{array}{r}
 134 \\
 + 216 \\
 \hline
 = 350 \\
 \text{Mismatch!}
 \end{array}$$

8

<https://manara.edu.sy/>

IP Header: To and From Addresses

- Two IP addresses
 - ✓ Source IP address (32 bits)
 - ✓ Destination IP address (32 bits)
- Destination address
 - ✓ Unique identifier for the receiving host
 - ✓ Allows each node to make forwarding decisions
- Source address
 - ✓ Unique identifier for the sending host
 - ✓ Recipient can decide whether to accept packet
 - ✓ Enables recipient to send a reply back to source

البروتوكول IPv4: IP Options

- وهو متغير بين 0 و 40 بايت وتشمل: فحص الشبكة **network testing**، الأمن **security**، تشخيص الأخطاء **debugging** ويحدد قائمة الموجبات التي ستزورها رزمة البيانات إضافة إلى خصائص أخرى
- يسمح IP بإدخال بعض حقول الخصائص بين حقلي ترويسة IP (20 بايت) والمعطيات المحملة. هذه الحقول هي جزء من ترويسة IP وتصف مجموعة من المميزات التي يجب تطبيقها على رزمة البيانات
- من الضروري أن تلتزم عقدة ما تستقبل رزمة بيانات تحتوي على خصائص معينة أن تؤدي عملها مع أخذ هذه البارامترات بالحسبان
- يتم ترميز الميزة/الخاصية ككتلة TLV: Type-Length-Variable، بحيث تبدأ كل خاصية بمحدد النموذج والذي يحدد أي خاصية موجودة الآن. ثم يتبعها طول الحقل والذي يبين عدد البايتات التي تتطلبها الخاصية (التي تشملها مع حقلي الطول والنموذج). وأخيراً يأتي حقل المتغير وهي المعطيات الخاصة بهذه الخاصية



البروتوكول IPv4 : IP Options

- **Options:**
 - Security restrictions
 - Record Route: each router that processes the packet adds its IP address to the header.
 - Timestamp: each router that processes the packet adds its IP address and time to the header.
 - (loose) Source Routing: specifies a list of routers that must be traversed.
 - (strict) Source Routing: specifies a list of the only routers that can be traversed.



التجزئة في البروتوكول IPv4 : Fragmentation in IPv4

البروتوكول IPv4 : Fragmentation

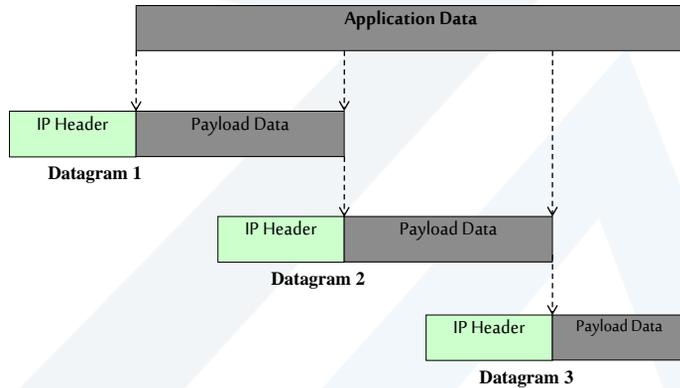


- ▶ تملك كل تقنية شبكة خصائص مختلفة تؤثر على طريقة IP المستخدمة
مثلاً: لكل تقنية حجم أعظمي لوحدة معطيات البروتوكول PDU: Protocol Data Unit وهو الحجم الأعظمي لرزمة البيانات التي يمكن إرسالها باستخدام تقنية الشبكة:
X.25: 576 بايت
Ethernet: 1500 بايت
FDDI: 4352 بايت
16 Mbps Token Ring: 17756 بايت
ويسمح IP نفسه بنقل رزمة بيانات تصل حتى 65535 بايت
- ▶ تدعم بعض تقنيات الشبكات تقسيم رزمة البيانات إلى أجزاء أصغر وإعادة تجميعها عند الهدف
مثلاً: تسمح شبكات ATM بنقل رزم ذات 48 بايت فقط وبالتالي عند استخدام IP، سيسمح برزم بيانات ذات 28 بايت من المعلومات فقط (+20 بايت ترويسة) في كل رزمة.
- ▶ هناك بعض التقنيات التي لا تدعم التجزئة وإعادة التجميع ولذلك نحن بحاجة إلى IP لتحديد/تقييد حجم رزم البيانات في الشبكة

البروتوكول IPv4 : Fragmentation



- ▶ يبين الشكل معطيات منقولة في IP بحيث تم تقسيمها إلى سلسلة من رزم IP. لكل رزمة محدد رزمة وحيد Unique Datagram Identifier يتوضع في الترويسة. يتم استخدام هذا الحقل للسماح بإعادة ترتيب رزم البيانات أو لاكتشاف ضياع بعض الرزم ، لذلك من المقنع وضع قيم متزايدة بقيمة 1 لكل رزمة بيانات

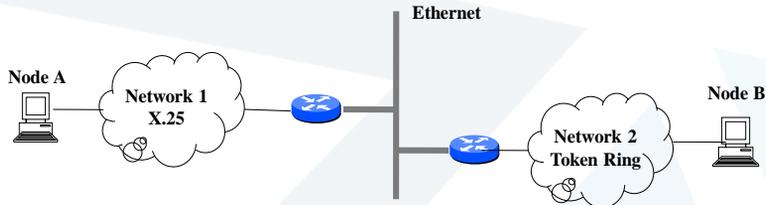


البروتوكول IPv4 : Fragmentation

➤ لا تسمح بعض التطبيقات بتقسيم معطياتها إلى عدة رزم منفصلة والتي يمكن أن تسبب لهم مشكلة إذا أرادوا أن ينتظروا وصول كل رزم البيانات قبل أن يبدأوا معالجة أول رزمة. وهي عملية تتعلق بروتوكولات التحكم أكثر منه بالمعلومات نفسها، حيث أنه يجب معالجة رسالة التحكم للرسالة الكاملة بينما يتم كتابة المعطيات على خرج الأجهزة كما تصل. تحتاج التطبيقات التي لا تسمح بالتجزئة للتوافق مع طبقة IP: ماهو الحجم الأعظمي لـ PDU للشبكة التي يتم التعامل معها، ويجب تقديم المعلومات في كتل تكون أصغر بشكل كاف لنقلها باستخدام رزمة IP واحدة (يجب الأخذ بعين الاعتبار البايتات التي تحتاجها الترويسة)

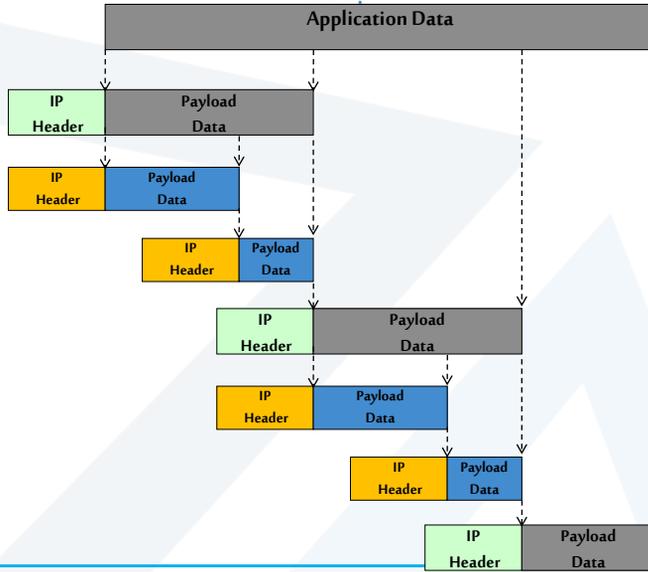
لنأخذ مثلاً شبكة كما في الشكل، حيث ترتبط العقدة A مع شبكة X.25 حيث $\text{max PDU}=576 \text{ bytes}$. عندما تريد العقدة A إرسال رزم بيانات إلى العقدة B فإنها ستكون متأكدة أنه لا يوجد أي رزمة بيانات أكبر من 576 بايت. عندما تتقدم الرزمة فإنها تتجاوز الشبكة X.25 وتقابل شبكة Ethernet. باعتبار أن max PDU لشبكة الـ Ethernet هو 1500 بايت، فإنه سيتم نقل رزمة بيانات IP بكل بساطة بدون أي حاجة لإعادة تقسيمها. عندما يصل الانتقال إلى Token Ring والتي لها $\text{max PDU}=17756 \text{ bytes}$ فيمكن للرمز أن تواصل انتقالها إلى الهدف

البروتوكول IPv4 : Fragmentation



➤ لكن إذا فرضنا أن العقدة B تريد إرسال إجابة إلى العقدة A وعلى اعتبار أن العقدة B متصلة بشبكة Token Ring، فإنها ستحضر رزمة بيانات تصل لطول 17756 بايت. سيتم نقلها باتجاه العقدة A حتى تصل للشبكة Ethernet حيث تكون كبيرة جداً. لذلك وحتى يتم نقل رزمة البيانات فيجب تجزئتها إلى أجزاء أصغر ليست أكبر من 1500 بايت. أيضاً لكي تصل الأجزاء إلى الشبكة X.25 فيجب تجزئتها من جديد حتى يتم نقلها عبر هذه الشبكة. تتوضح عملية التجزئة كما في الشكل

البروتوكول IPv4 : Fragmentation



<https://manara.edu.sy/>

17



البروتوكول IPv4 : Fragmentation

- لذلك: عندما تصل رزمة البيانات إلى شبكة حيث max PDU لها أصغر من حجم رزمة البيانات، فسوف يتم تجزئتها إلى رزم أصغر. يتم نسخ ترويسة IP لكل جزء من أجزاء الرزمة الأصلية، مثل: TTL، عنوانا المصدر والهدف هي نفسها. محدد الرزمة لكل جزء هو نفسه لذلك فإن كل أجزاء الرزمة الأصلية يمكن تحديدها بسهولة
- من الممكن أن لاتصل الأجزاء بالترتيب بسبب المسارات المختلفة التي يمكن أن تسلكها هذه الأجزاء عبر الشبكة
- نحن بحاجة لمعرفة توضع كل جزء ضمن الرزمة الأصلية، ويتم تحقيق ذلك من خلال حقل Fragment Offset في ترويسة IP. يتكون هذا الحقل من 13 بت، وعندما تصل الأجزاء إلى الهدف فسيتم ترتيبها ومن ثم تجميعها
- تشغل عملية التنفيذ عداداً Timer عندما يصل الجزء الأول من السلسلة، ولذلك فعندما لا يكتمل هذا التعاقب بسبب ضياع رزمة مثلاً في الشبكة فلن يتم تخزين الأجزاء المتبقية للأبد
- يعتمد التقريب المنطقي على استخدام قياس TTL المتبقي بالثانية لتحديد زمن حياة الأجزاء التي يُنتظر تجميعها، بإعطاء زمن حياة أعظمي حتى 405 دقيقة، لكن بعض التطبيقات لاتستخدم ذلك وتشغل عداداً بحدود 15 ثانية

18

<https://manara.edu.sy/>

البروتوكول IPv4 : Fragmentation



- تتم عملية التجميع دوماً عند العقدة الهدف ولا تتم نهائياً عند عقدة وسطية في الشبكة حتى إذا انتقلت الرزمة من شبكة ذات PDU صغير إلى أخرى يمكن أن تدعم PDU كبيراً
- تحاول بعض التطبيقات تجنب عملية التجزئة ضمن الشبكة. وهذا مفيد في بعض الأحيان إذا علمت أن العقدة الهدف لا تملك القدرة أو الموارد لتجميع الأجزاء، ويتم ذلك من خلال تثبيت البت الثاني من حقل Flag في ترويسة IP:

- ✓ البت الأول محجوز ويأخذ قيمة 0
- ✓ البت الثالث هو Must Fragment (MF)
- ✓ البت الثاني هو Don't Fragment (DF) والذي يتم تثبيته تلقائياً إلى 0 ليبدل على السماح بالتجزئة و 1 لتجنب التجزئة.
- أي عقدة وسطية تستقبل الرزمة مع $DF=1$ ، يجب أن لا تجزئ رزمة البيانات، وتحاول اختيار طريق لا يتطلب تجزئة رزمة البيانات أو يجب في حالات أخرى إهمال أي رزمة لا تستطيع نقلها بسبب حجمها

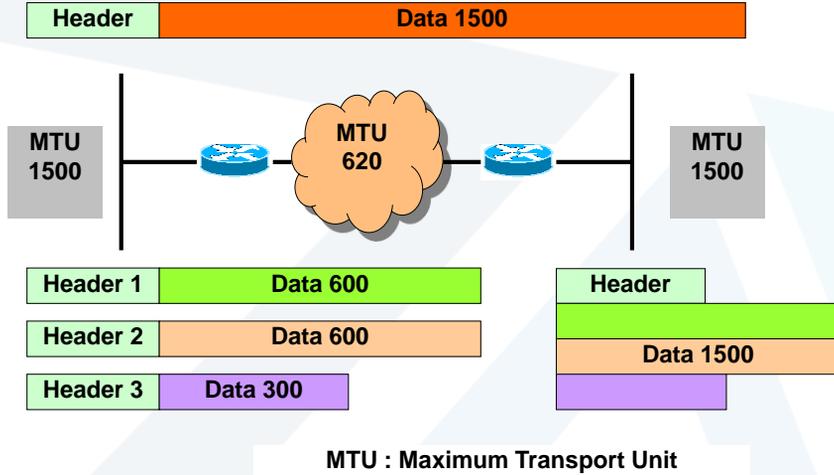
البروتوكول IPv4 : Fragmentation



- يمكن تجنب عملية التجزئة من خلال اكتشاف وحدة النقل الأعظمية Maximum Transmission Unit (MTU) بين المصدر والهدف. وهي أصغر PDU أعظمية lowest maximum PDU على كل الوصلات بين المنبع والهدف
- تحاول بعض البروتوكولات في الطبقات العليا اكتشاف هذه القيمة من خلال المعلومات المتبادلة بين العقد على طول الطريق. ثم تستخدم عندها هذه المعلومات لاختيار الطرق الخاصة أو لتقديم المعطيات إلى IP بأصغر تخزين ممكن والتي لا يمكن أبداً أن تحتاج لتجزئتها

- **Maximum size of IP datagram is 65535, but the data link layer protocol generally imposes a limit that is much smaller**
- **Example:**
 - Ethernet frames have a maximum payload of 1500 bytes
 - IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes
- **The limit on the maximum IP datagram size, imposed by the data link protocol is called **maximum transmission unit (MTU)****

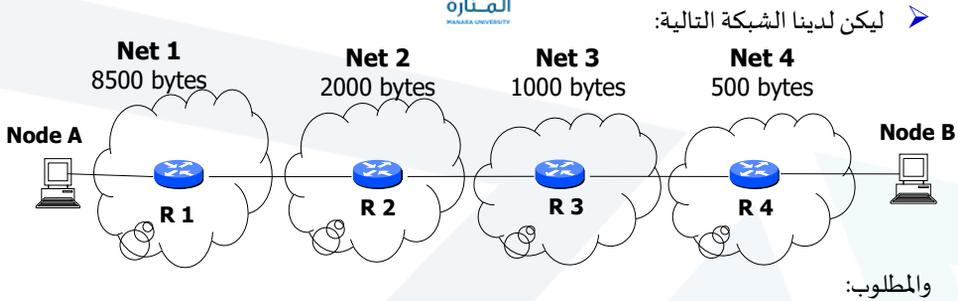
البروتوكول IPv4 : Fragmentation



21

<https://manara.edu.sy/>

تمرين 1



إذا أرادت العقدة A إرسال رسالة إلى العقدة B، بين ما هو عدد الرسائل التي ستصل إلى R3 إذا كانت المعطيات الكلية المراد إرسالها هي (10000 بايت) مع العلم بأنه تم استخدام خصائص لـ IP بمقدار 10 بايت؟ يمكن الإجابة سواء بالحل أو بالرسم.

22

<https://manara.edu.sy/>

تمرين 1



حالة الانتقال من A إلى R1:

باعتبار أن R1 يتعامل مع Net1، أي بمعدل نقل 8500 bytes وبما أن ترويسة IP تأخذ 20 bytes ولدينا خصائص بمقدار 10 bytes فسيكون حجم الترويسة هو 30 bytes لذا سيكون لدينا رسالتين: واحدة 8470 bytes والثانية 1530 bytes

$$\text{Number of messages at R1} = 1 * 8500 + 1 * 1560 = 2 \text{ messages}$$

تمرين 1



عند الانتقال من R1 إلى R2:

باعتبار أن R2 يعمل مع Net 2، أي بمعدل نقل 2000 bytes وبما أن ترويسة IP تأخذ 30 bytes، فستنقسم رسالة 8470 bytes إلى 5 رسائل:

4 رسائل كل منها تنقل 1970 bytes وبيانات الرسالة الرابعة تنقل 590 bytes

وتمر رسالة 1530 bytes دون تقسيم.

$$\text{Number of messages at R2} = 4 * 2000 + 1 * 620 + 1 * 1560 = 6 \text{ messages}$$

تمرين 1

عند الانتقال من R2 إلى R3:

كل رسالة 1970 bytes سيتم تقسيمها إلى 3 رسائل: $1970/970=2$ وتبقى رسالة تحوي 30 بايت.

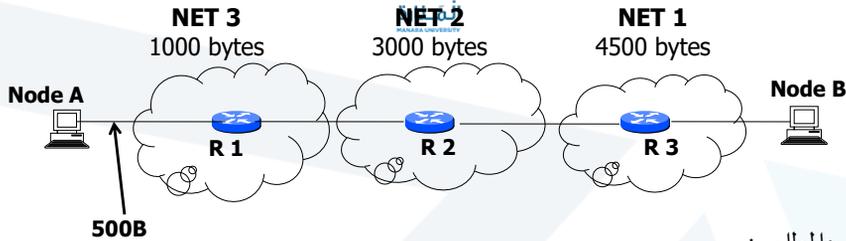
ورسالة 1530 bytes سيتم تقسيمها إلى 2 رسائل: $1530/970=1$ وتبقى رسالة تحوي 560 بايت.

لذا يكون عدد الرسائل التي ستصل إلى R3 هو:

$$\begin{aligned} \text{Number of messages at R3} &= 4*(2*1000+1*60)+1*620+1*(1+1000+1*590) \\ &= 8*1000+4*60+1*620+1*1000+1*590 \\ &= 9*1000+1*620+1*590+4*60= 15\text{messages} \end{aligned}$$

تمرين 2

ليكن لدينا الشبكة التالية: ➤



والمطلوب: ➤

1. في حال أردنا إرسال رسالة من NET2 إلى NET3 واستقبلت عقدة وسطية/ موجه هذه الرسالة وكانت بحجم 2000 بايت وكان علم عدم التجزئة مرفوعاً، فما هو الحل الذي ستقوم به هذه العقدة؟
2. في حال أردنا إرسال رسالة من NET1 إلى NET3 (من R3 إلى R1) فما هو حجم الرسالة الأعظمي الذي يمكننا إرساله بدون تجزئة؟
3. بين ما هو عدد الرسائل التي ستصل إلى A في حال إرسال معطيات من العقدة B قدرها (4500 بايت)، أي كيف سيكون عدد الرسائل من R3 إلى R2 ومن ثم من R2 إلى R1؟
4. في حال لدينا خصائص بمقدار 10 بايت، فهل سيتغير عدد الرسائل وأحجامها؟ فسر ذلك بالحل؟



Thanks

<https://manara.edu.sy/>