

11:16 AM



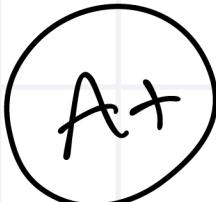
Kasit Note ▼



لـ شرپناز الحاج
بلدر

A hand-drawn illustration on graph paper. At the top, a large black arrow points to the left. Below it is a stylized orange robot head with a single small square eye and a simple black line for a mouth. To the right of the head is a speech bubble containing the letters 'woi'. A thick black line extends from the bottom of the speech bubble, curves down and to the left, then turns back up towards the right, ending near the bottom edge of the page.

Java Networks



لیان الطیطی

Chapter 01: Introduction

الهدف الأسمى من وجود الشبكات ← Data Communication

شو ہی ال Data Communication

The exchange of data between two devices via some form of transmission media.

تبادل للبيانات بين جهازين عن طريق إحدى وسائل النقل.

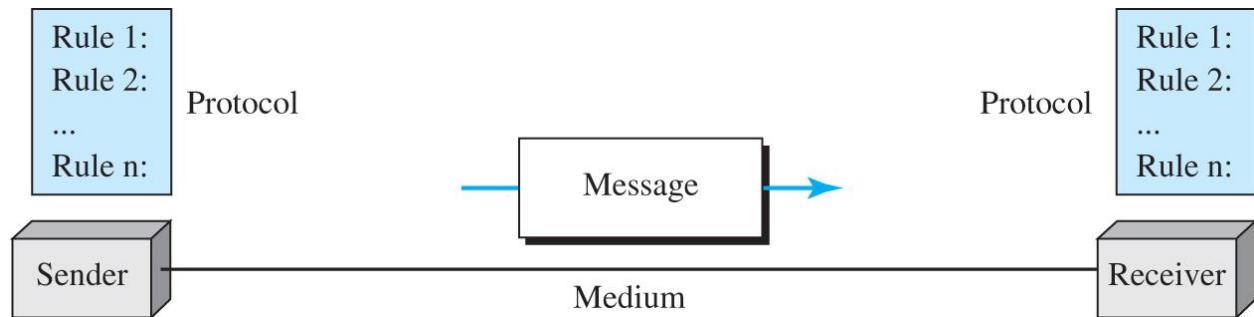
It depends on four characteristics:

كفاءة الـ Data Communication يتعمد على 4 خصائص:

- 1- Delivery → حتى تتأكد إذا ال Data وصلت أو لا
 - 2- Accuracy → ال Data مش بس لازم توصل. لازم توصل بسلامة
 - 3- Timeliness → انه ال Data توصل بسرعة (مثلاً متى يعتبر حالي متأخرة، أو لمتى معاي....)
 - 4- Jitter → هل المسافة الزمنية بين كل رسالتين هي نفسها؟ مثلاً هل كل 10 ثواني رح توصلي رسالة؟

متى بصير في jitter؟ لما المسافة ما تكون متساوية (حتى لو كان الاختلاف صغير)

Components of Data Communication:



- 1- Sender
 - 2- Receiver
 - 3- Transmission Medium : Wireless , Wire وسیطة الانتقال ممكن تكون
 - 4- Protocols: مثلًا متى بصللي أبعثت ، متى أشيك ، شو أتصرف إذا صار مشكلة ،
 - 5- Message: video, audio, images, numbers ممكن تكون



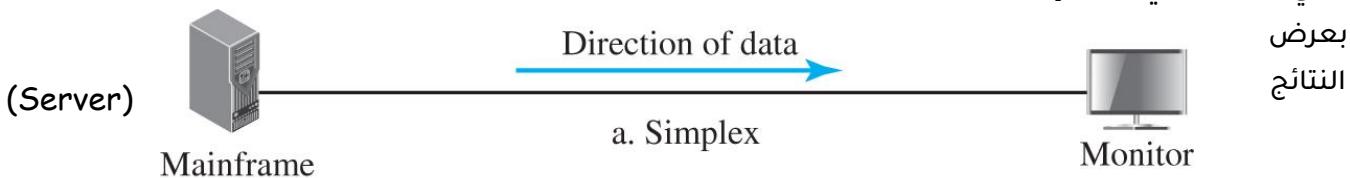
- i- Text → Represented as a bit pattern using Unicode.
- ii- Numbers → represented in binary.
- iii- Images → represented as bit patterns using either RGB or YCM.
- iv- Audio → Refers to the recording or broadcasting of sound or music, represented as analog or digital signals.
- v- Video → Can be a continuous images or a combination of images.

Data Flow

Communication between two devices can be simplex, half-duplex, and duplex.

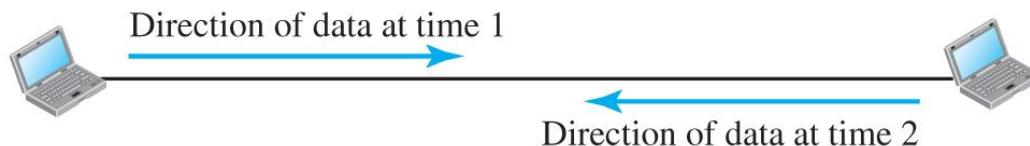
- 1- Simplex: The communication is in one direction. Only one of the two connected devices can send or receive.

زي بالمحاضرة لما الدكتورة تضل تحكي والطلاب بسمعوا ، أو مثل الشارع الي باتجاه واحد.
يعني من a إلى b بس.



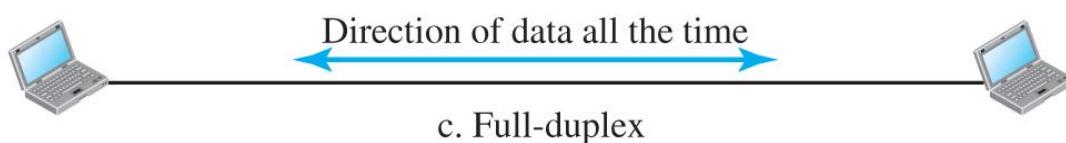
- 2- Half-Duplex: Each station can send or receive, but not at the same time.

زي بالمحاضرة لما الدكتورة تكون بتسأل وبدها الجواب من الطلبة ممكن الدكتورة تحكي أو الطلبة يحكوا بس مش بنفس الوقت.



- 3- Full-Duplex: Both stations can send or receive at the same time.

زي الشارع الي بمسارين دائمًا في داتا بتمشي من a إلى b أو العكس بنفس الوقت (زي مساجات الواتس).



What is the Network?

- The interconnection of a set of devices capable of communication.
التوصيل لمجموعة من الأجهزة التي عندها القدرة على الاتصال.
- A device can be:
 - Host → Such as a large computer, desktop, laptop, workstation, cellular phone, or security system.
 - Connecting device → Such as a router a switch, a modem that changes the form of data.

Network Criteria

المعايير التي لازم الشبكة تكون قادرة على تلبيتها

1- Performance → Can be measured:

- Transit time: The amount of time required for a message to travel from one device to another.
- Response time: the elapsed time between an inquiry and a response.

بنقدر نقيس كفاءة الشبكة عن طريق:

- وقت العبور: الوقت اللازم لانتقال الرسالة من جهاز لآخر.
 - وقت الاستجابة: الوقت الذي يمضي بين السؤال والرد.
- باختصار بنقدر نحي انه بنقيسه عن طريق مصطلح اسمه Throughput (قدیه بتنتقل الداتا بوحدة الزمن ، عدد المسجات بالزمن ، كلما كانت أعلى كان أحسن).

2- Reliability → The accuracy of delivery → Can measured by:

- The frequency of failure.
- The time it takes a link to recover from a failure.
- Network's robustness in a catastrophe.

احنا ما بدنا بنس انه الداتا توصل بسرعة على حساب سلامتها

ف ال Reliability بتخليي الداتا توصل (صحيحة ، كاملة ، مرتبة)(complete, correct, inorder)



3- Security →

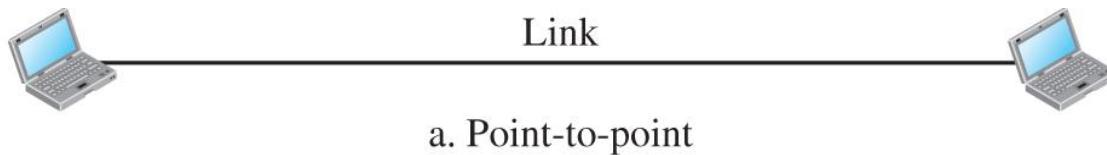
- i. Protecting data from unauthorized access.
- ii. Protecting data from damage and development.
- iii. Implementing policies and procedures for recovery from breaches and data losses.

Physical Structures

- Network: Two or more devices connected through links.
- Link: A communications pathway that transfers data from one device to another. مسار اتصالات بنقل البيانات من جهاز لآخر.

Types of Connection:

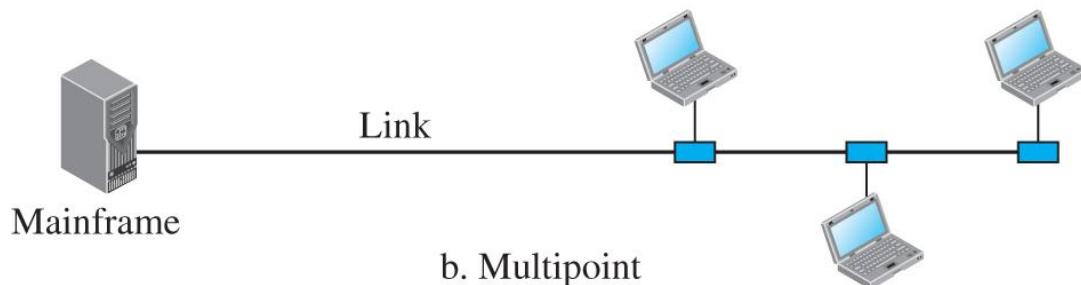
1- Point to point: بربط بين نقطتين وما في حدا بالنص link



2- Multipoint: مجموعة من ال points شابكين بنفس ال communication link ، يعني إذا كان الكيبيل عليه أكثر من حدا تكون موجود مثثان يخدم أكثر من نقطتين.

كيف بنعرف انه الرسالة لازم توصل لهاد المكان؟

كل نود بالشبكة عنده كرت شبكة فيه عنوان شريحة . لما تتبعت الرسالة يتم مقارنة عنوان الشريحة للجهاز المستقبل والمرسل ، إذا نفس العنوان فالرسالة بتتبعت ، وإذا لا بعهملها.

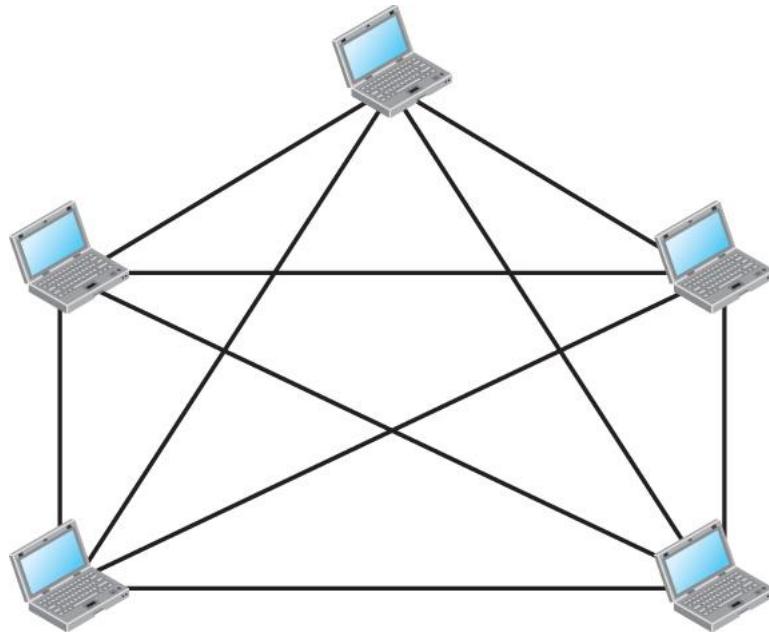


Physical Topology

- The term physical topology refers to the way in which a network is laid out physically.
- يعني لو أنا بنيت شبكة وحطيت communication devices وشبكتهم بكيل وصورتهم من فوق هاد هو مفهوم ال Topology .
- Two or more devices connect to a link; two or more links form a topology.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Basic Topologies:

- 1- **Mesh Topology:** كل node شابكة على عدد كبير من ال nodes الموجودة (مو شرط كلهم).
 - عدد ال communication links عالي.
 - ال message path سريعة؛ لأنه تقريباً كل node مربوطة مع الثانية * إيجابية.
 - ال mesh بيأخذ وقت وجهد وفلوس (بده بنية تحتية كبيرة وهاد كله بده مصارى ، وأمور الصيانة) ** سلبية.



هون عدد الأجهزة = 5 ، عدد ال links الي رح يكونوا (بأحسن الأحوال) = 10
وهاي بنسميهها fully connected mesh topology



2- Star Topology:

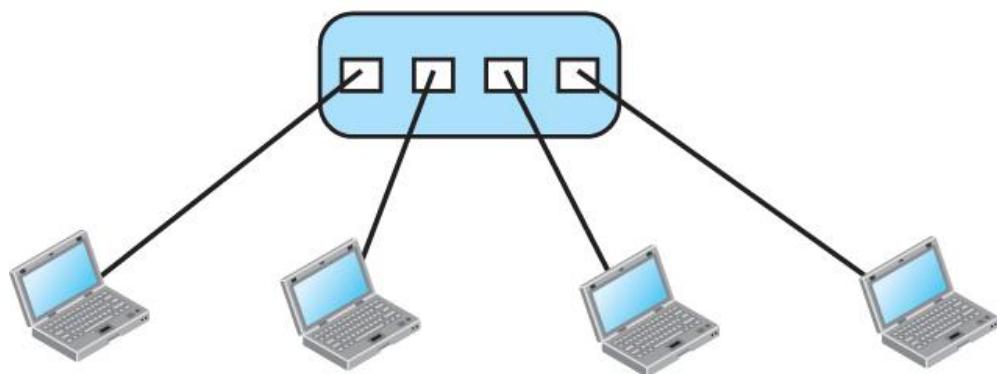
الصندوق المغلق الي يكون على باب المختبر بنسميه switch (ممكن يكون hub - رح نشرح لقادم الفرق بينهم -).

مش مُتاح أني أحكي مباشرة مع أي جهاز، لازم بالأول مع ال switch .
ال switch بعمل عمليات فلترة و forwarding (يعني بعملي على flow of control على traffic) *^{إيجابية}.

إذا ال switch خرب كل الشبكة بتوقع بنسمى هاي العملية ← failure ** سلبية.

ممكن يصير عندي bottleneck (اختناق)، لأنه كل ال traffic لازم تدخل على ال switch ونطلع منه، بنقدر نتجنبها عن طريق اختيار switch مساحته تغطي الي عنا وأكثـر شوي.

Switch or Hub

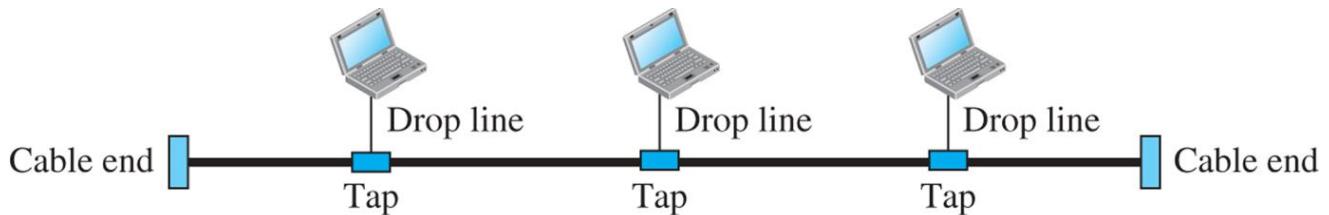


3- Bus topology:

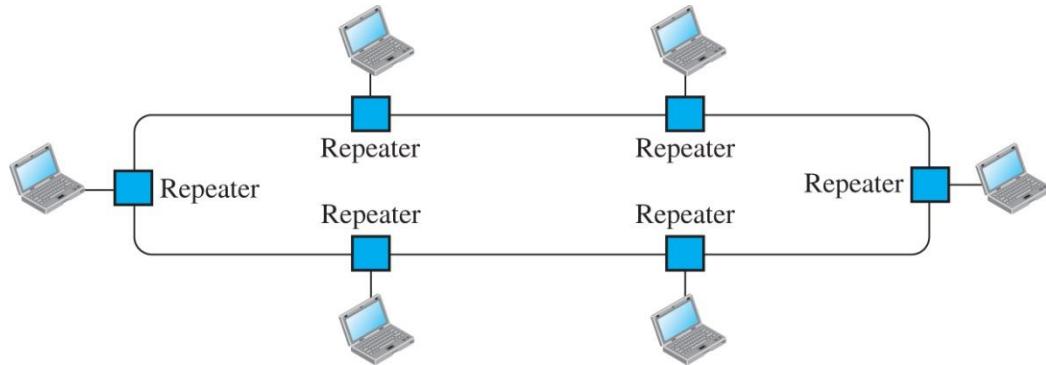
بتشبيه الـ multipoint , بسيط , الكيبل الهـ ends 2 , كل حدا بشبك على الـ bus عن طريق المدخل.

من أكبر عيوبه أنه بأزم (زي الشارع لما يكون أزمة وما حدا قادر يتحرك) ، صعب نطور الشبكة تبعته .

إذا الشبكة الي عندي صغيرة وعدد ال PCs قليلة ، هو خيار جيد ومثمن مُكلف لأنه ما يحتاج ل router أو hub أو بنية تحتية.



4- Ring topology: يشبه ال bus topology ، زى كأني بشبك ال 2 ends bus مع بعض، هون ال PCs بتواصل مع الي بعده لحد ما يوصل للي بده اياه. يعني يا بتواصل مع الي قبله أو الي بعده بس.



Network Types: (أنواع الشبكات حسب المساحة الجغرافية)

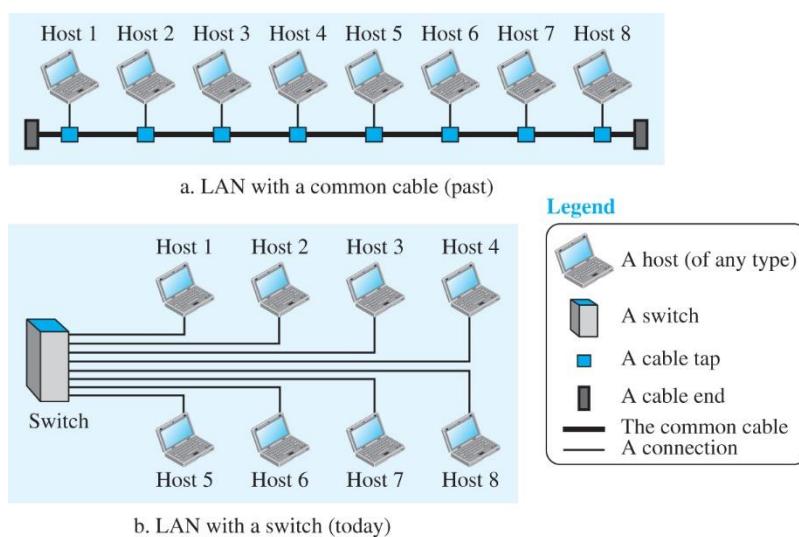
1- LAN (Local Area Network): Usually privately owned and connects some hosts in a single office, building, or campus.

ال LAN ما بتجاوز حدود بنية مثل كلية ال it (كل مختبر بمثيل LAN ، وكل طابق LAN ، بعدين كل المبني بشبكة مع بعض).

2- WAN (Wide Area Network): A connection of devices capable of communication. a WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

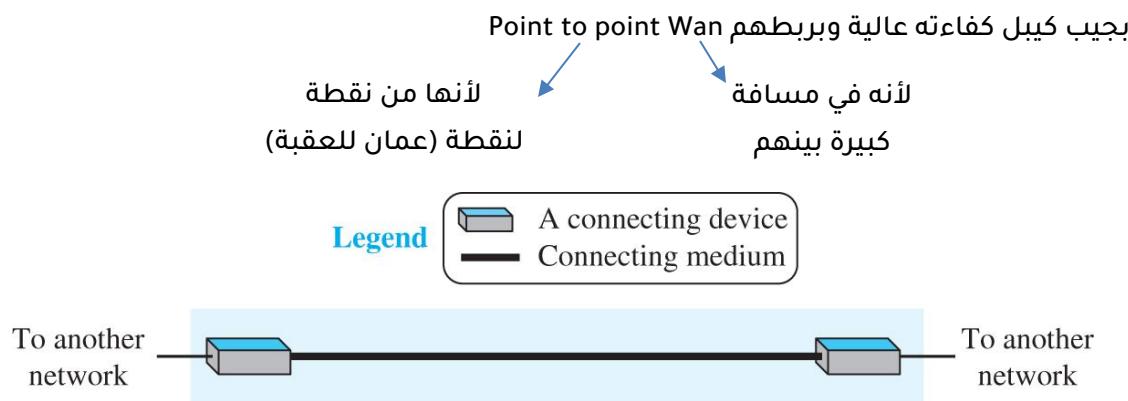
ال WAN لمسافة شاسعة بتربط ال PCs على مستوى البلد.

زمان كانت ال LAN ترتبط ك Bus والشبكة كانت كثير بطئنة. أما هلا ك Star



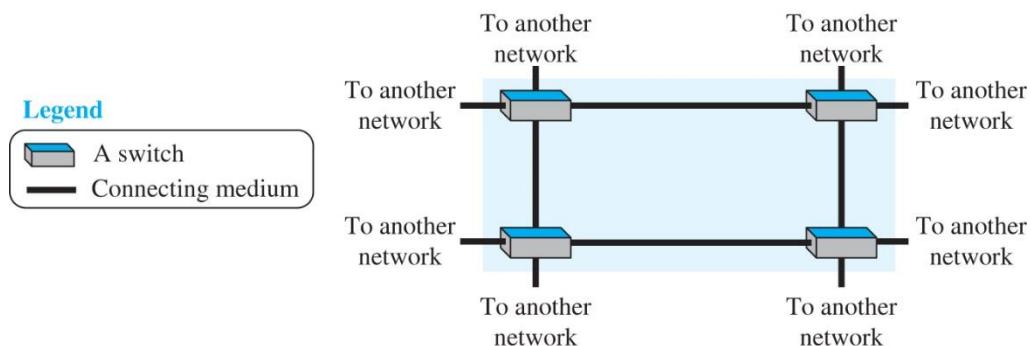
Point-to-Point WAN: A network that connects two communicating devices through a transmission media (cable or air).

- مثلاً أنا عندي بنك الله فرع بعمان وبالعقبة وفي عند كل فرع Router ، كيف يربط الاثنين بعض؟



Switched WAN: A network with more than two ends, used in the backbone of global communication.

- مثلاً بنك الله فرع رئيسي بعمان وأفرع ثانية بالمحافظات، كل فرع الله Router يستخدم switch . عددهم يكون من 4 - 10 بالكثير. مشان يشبكهم ك mesh topology



- يعني ال Switch إذا كان عندي 2 رئيسيات ، إذا أكثر يستخدم ال point to point

internet (lowercase i): Two or more networks that can communicate with each other.

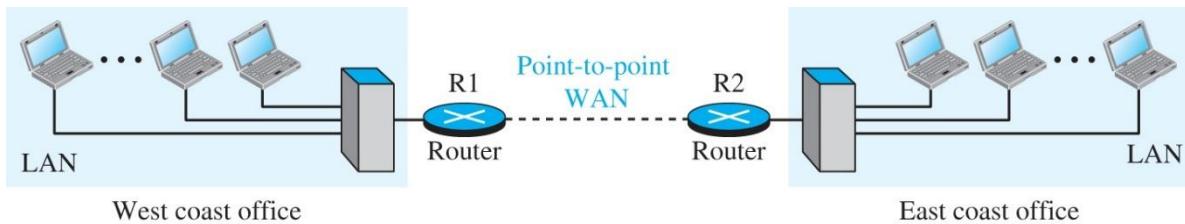
Internet (uppercase I): Composed of millions of interconnected networks.



الفرق بين Intranet, internet, Internet

Intranet → لما تكون جوا الجامعة وبشبكة الناس بعضهم (داخلي) Within the organization
 internet → لما بدأ شبكت الجامعة الأردنية بسمية Between different organization
 Internet → لما شبكتنا العالم مع بعض

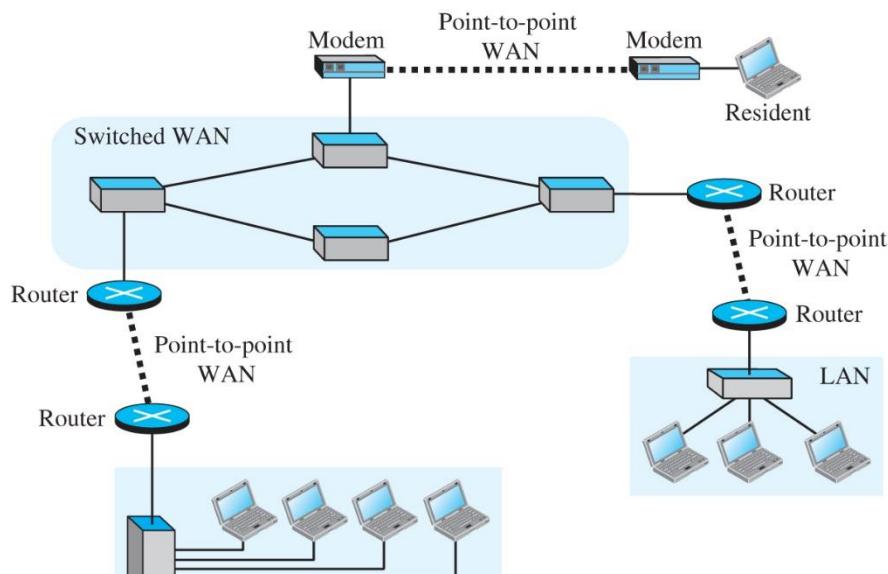
- داخل مؤسسة وحدة Intranet ←
- بين مؤسستين internet ←
- بين العالم كله Internet ←

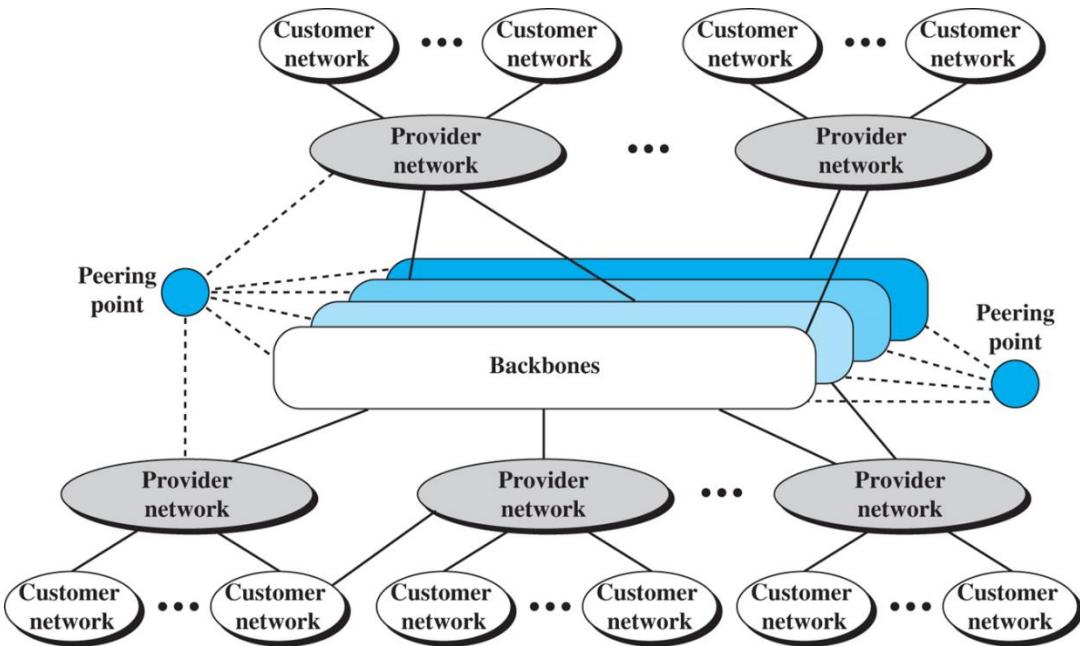


بنك الله فرع بمدينة وفرع بمدينة ثانية بشبكيهم بعض عن طريق point to point WAN هاي .internet

شبكت LAN مع LAN ثانية بواسطة 2 Routers وحطيت بينهم Point to point WAN هاي .internet

حتى لو كان عندي أكثر من فرع وشبكتهم عن طريق الـ Switch WAN كمان اسمها .internet





عنا أكثر من **customer network** موزعين حسب المنطقة الجغرافية، وبكل منطقة حسب طبيعة الـ **customers** هل هم أفراد أو شركات صغيرة أو كبيرة أو متوسطة ، بعد هيك احنا بنتطلع على الانترنت عن طريق مزود الخدمة (أورانج، زين، أمنية....) ، حتى مزودي الخدمة هدول باخذوا الانترنت من مزودي الخدمة الي أكبر منهم.

في شركة مسؤولة عن الانترنت بالعالم موجودة بأمريكا ، هي المسؤولة عن انه كل الناس يشبّوا على الانترنت، الشركة مقسمة الكرة الأرضية لمناطق حسب القارات (**مثلًا** احنا اسمينا الشرق الأوسط وشمال أفريقيا) كل منطقة فيها ISP رئيسيات اسمهم **National ISP** ، حتى زين وأمنية بياخذوا النت من **Regional ISP** والـ **ISPs القاربيات** والقاريبات تكونوا مربوطين **بأمريكا**.

لما نشبّك على الانترنت يكون عنا **Router** اي كفاءتهم عالية مربوطين مع بعض ب شبكات هائلة الإمكانية ، تكونوا مجموعة مش بس **Backbone** وحدة لي؟

مشان إذا **Router** فيهن طفا الانترنت ما يطفي على العالم + مشان ما تصير نقطة اختناق **(Bottleneck)**

Accessing the Internet

- The Internet today is an internetwork that allows any user to become part of it.
- The user, however, needs to be physically connected to an ISP.
- The physical connection is normally done through a point-to-point WAN.

مشان ما يكون في بطء بالوصول للانترنت



- Using Telephone Networks: Today most residences and small businesses have telephone service, which means they are connected to a telephone network. Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN.
- Using Cable Networks: More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service.
- Using Wireless Networks: Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

- زمان في ناس استخدموا البنية التحتية للتلفونات مشان يشبکوا على الانترنت، وفي ناس استخدموا البنية التحتية للتلفزيونات مشان يشبکوا على الانترنت.
- كانت التمديادات والاتصالات هي تبعت التلفونات الأرضية ولما يدهم يشبکوا على الانترنت كانوا يجيّبوا Modem ويشبکوه بخط التلفون، فلما بدهم يشغلوا الانترنت يشغلوا خط التلفون وهيك بتبطل تجيهم اتصالات(يعني الانترنت وخط التلفون على نفس الـ *(frequency)*).
- الناس الي بأمريكا كانوا يستخدموا البنية التحتية للتلفزيونات.
- الـ *Wireless* مفید للأماكن النائية كثیر، لأنهم ما عندهم بنية تحتية (تلفزيونات أو خطوط أرضية).



Direct Connection to the Internet

A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet. (نفس الـ ISP نفسه) بالرسمة فوق

Protocol Layering

The rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate directly.

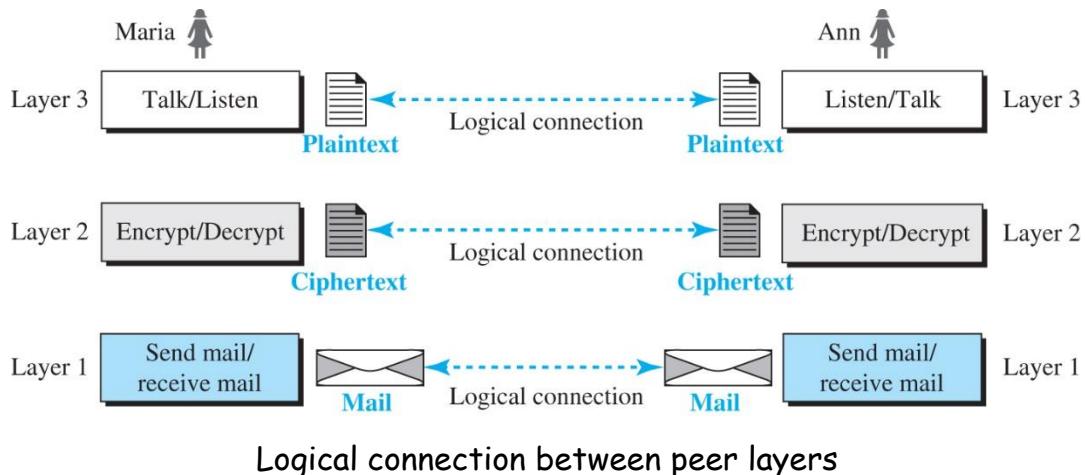
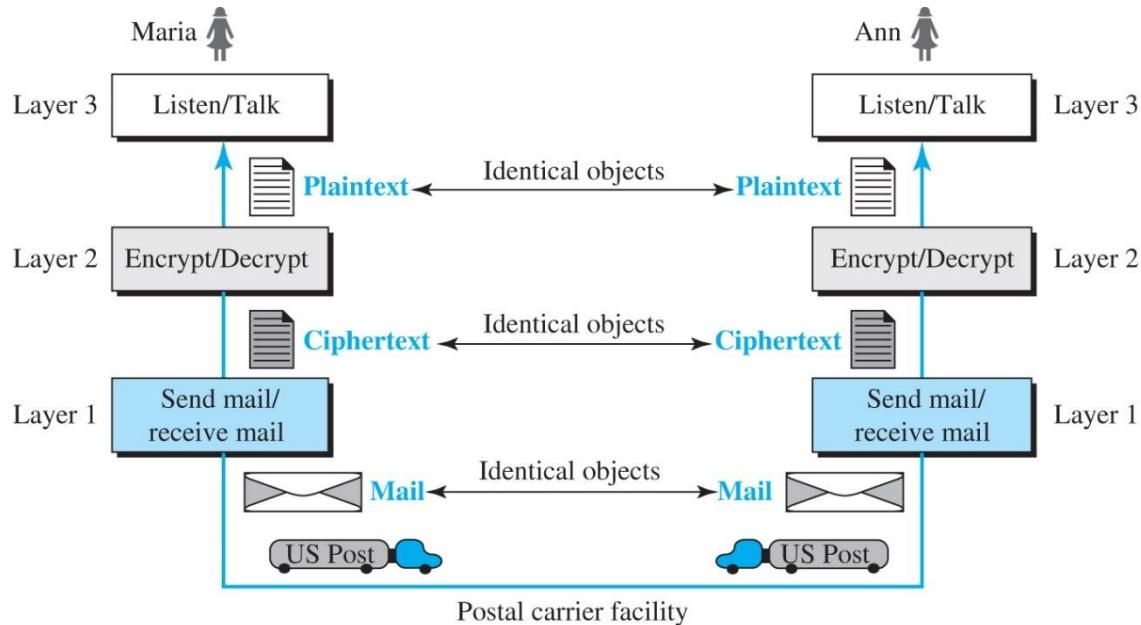
حكينا من قبل شو يعني protocols انه مجموعة من القوانين الي بتضبط التواصل ما بين 2 end points

**خلينا نشوف هدول المثالين (مش كثير مهمين)

- A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP.



- In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria. They decide to continue their conversion using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted. They use an encryption/decryption technique.



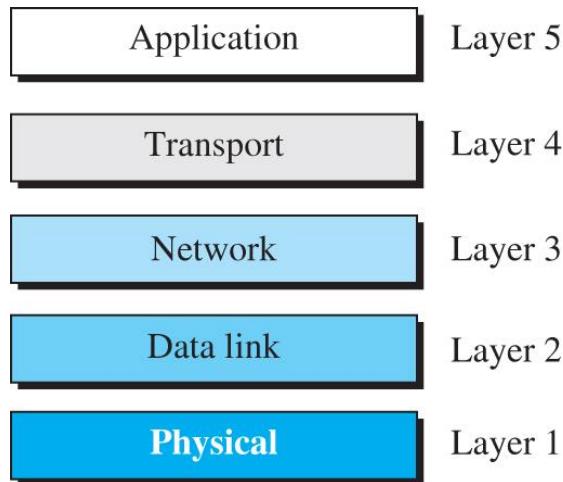
يعني باختصار السيناريو الثاني أسهل لأنه مثلاً لو بدأ غير protocol معين بال layer 1 هو مضطربة
أبنليس بكل ال layers بس بروح على الـ بدأ ايـه وبغيـره (فتـطوير الـ system وتحـسيـنه بـكون
بسـرعة عـالـيـة).
فـكرة اـنـي أـقـسـمـ الـ Design لـ layers أـفـضـلـ منـ أـنـه يـكـونـ بـ layer وـحدـةـ.



TCP/IP Protocol Suite

(Transmission Control Protocol / Internet Protocol). This is the protocol suite used in the Internet today.

Layers in the TCP/IP protocol suite



- Layer 1 → Physical Layer:

- Responsible for carrying individual bits in a frame across the link.
- The lowest level in the TCP/IP protocol suite.
- The communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.

○ معنية بتحويل 0 و 1 لموجات رح نحي عنه أكثر بتشابط .2

- Layer 2 → Data Link Layer:

- We have seen that an internet is made up of several links (LANs and WANs) connected by routers.
- When the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link.

○ بشووف كل مجموعة من 0 و 1 مع بعض ، تكون معتمدة اعرف الاداٽا وين بتبدأ ووين

بتنتهي / بتحكم بالدور مثلاً a بدها تحكي مع b و c مع d ممكن يخبطوا الرسائل

بعض في حاجة أكبر لموضوع ال control على ordering of communication

. ورح نحي عنه بتشابط .3 معنية بال physical addressing .



- Layer 3 → Network Layer:
 - Responsible for creating a connection between the source computer and the destination computer.
 - The communication at the network layer is host-to-host.
 - There can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.

بكون عندها اطلاع على الشبكة كاملة وبنقدر تعطيني ال shortest path بين ال source و destination . ورح نحكي عنها بتشابتر 4 .

- ال physical address مثل رقمك الوطني ما بتغير.
- ال logical address مثل رقم تلفونك أو ايميلك ممكن يتغيروا (عنواين لالك بس ممكن تتغير).

- Layer 4 → Transport Layer:

- The logical connection at the transport layer is also end-to-end.
- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet.
- The transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.
- Transmits user datagrams without first creating a logical connection.

دورها انها تطلع على موضوع ال reliability (الي حكينا عنه من قبل انه الداتا توصل صحيحة ومرتبة ...) وتشوف إذا رح تعالجه جزئياً أو كلياً أو لا، ورح نحكي عنه بتشابتر 9 .

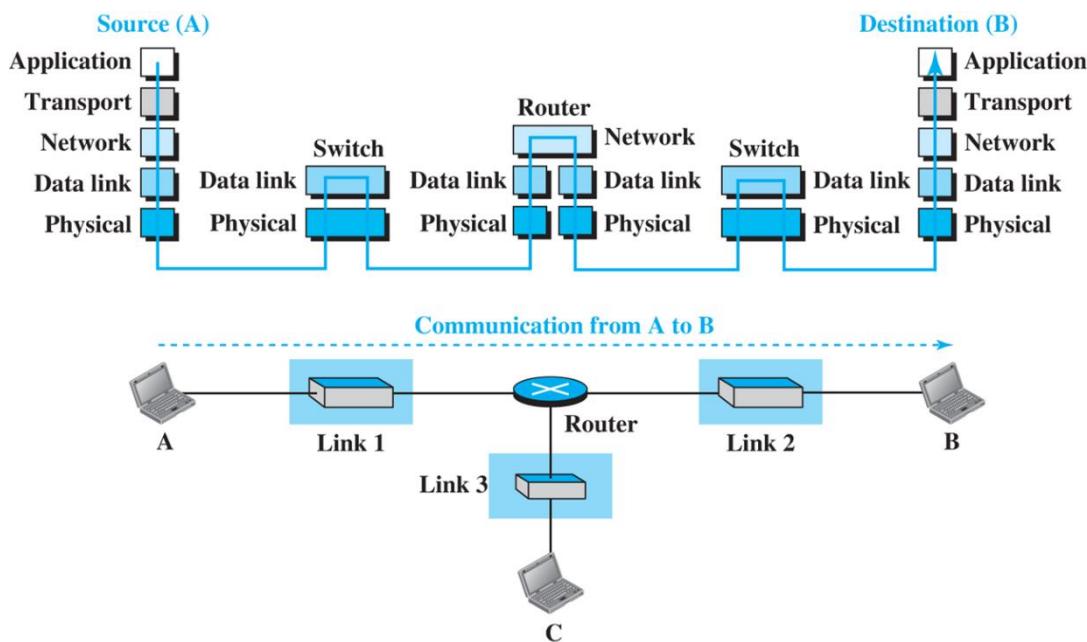
- Layer 5 → Application Layer:

- The logical connection between the two application layers is end-to-end.
- The two application layers exchange messages between each other as though there were a bridge between the two layers.
- The communication is done through all the layers.
- Communication at the application layer is between two processes (two programs running at this layer).



- A process sends a request to the other process and receives a response.
- Process-to-process communication is the duty of the application layer.
- شو بده ال User؟ بنحاول نخبي عن ال user قدر الامكان تفاصيل الشبكة لأنه كل ما عرف ال user أقل كلما كان أحسن ،

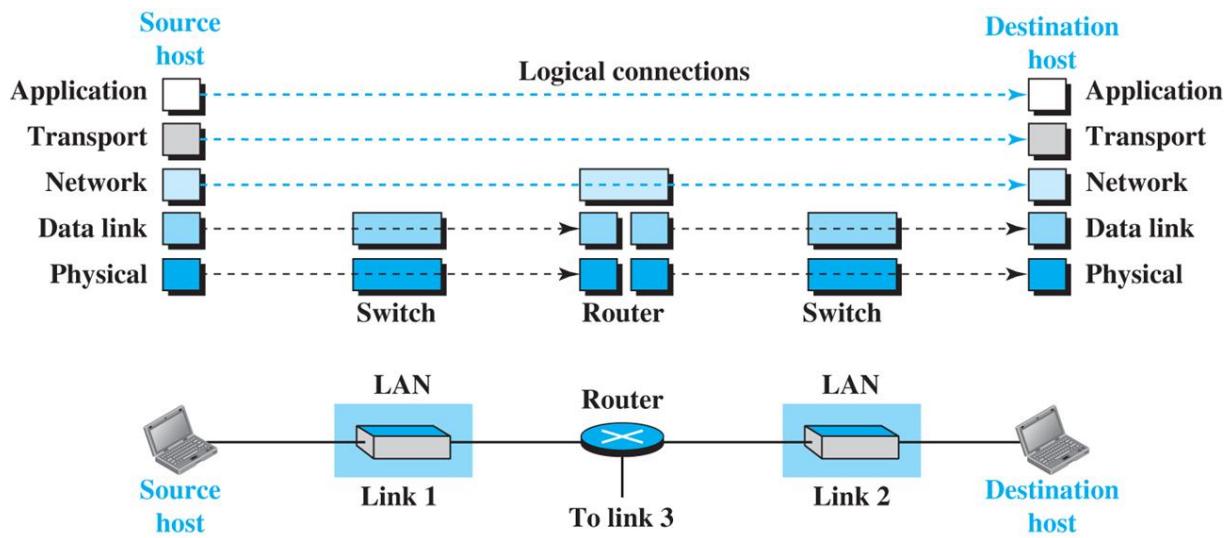
مثلاً ال user أكيد الله العلاقة بال reliability للبيانات فمو غريب انه قريبة على هاد ال layer . بس ال user مو معني بأقصر طريق بينه وبين ال destination أو بال physical address فالمفروض يكون باتصال مع ال layer اي بتخدمه فقط . رح نحكي عنه بتشابتر 10 أكثر .



- مثلاً هون جهاز A هو تبع الدكتورة وال switch المسئول عنها ، والجهاز الي بدها تحكي معه وال switch المسئول عنه وفي بينهم بالنص . Router .
- كيف ال communication يتم؟ كومبيوتر A بحكي مع B ، من خلال انه الرسالة بتطلع من A لل switch المسئول عنه وبوديها لل Router ، الراوتر بختار الرسالة رايحة لمين ل B أو C بناءً على ال IP Address . بستلمها ال switch الثاني وبوصلها ل B .
- الجهازين A و B بحتاجوا ال protocol stack كامل .
- أما ال switch وظيفته بس انا ياخذ المسج من A ويوصله للراوتر ، طب لي ماذد بس أول physical, datalink 2layers
- الراوتر عنده ال physical, datalink, network layers ، لي عند ال physical + datalink layers قاسمهن لنصين؟ عشان يكون الله فائدة لازم على الأقل ينزل عليه كرتين نتورك layers

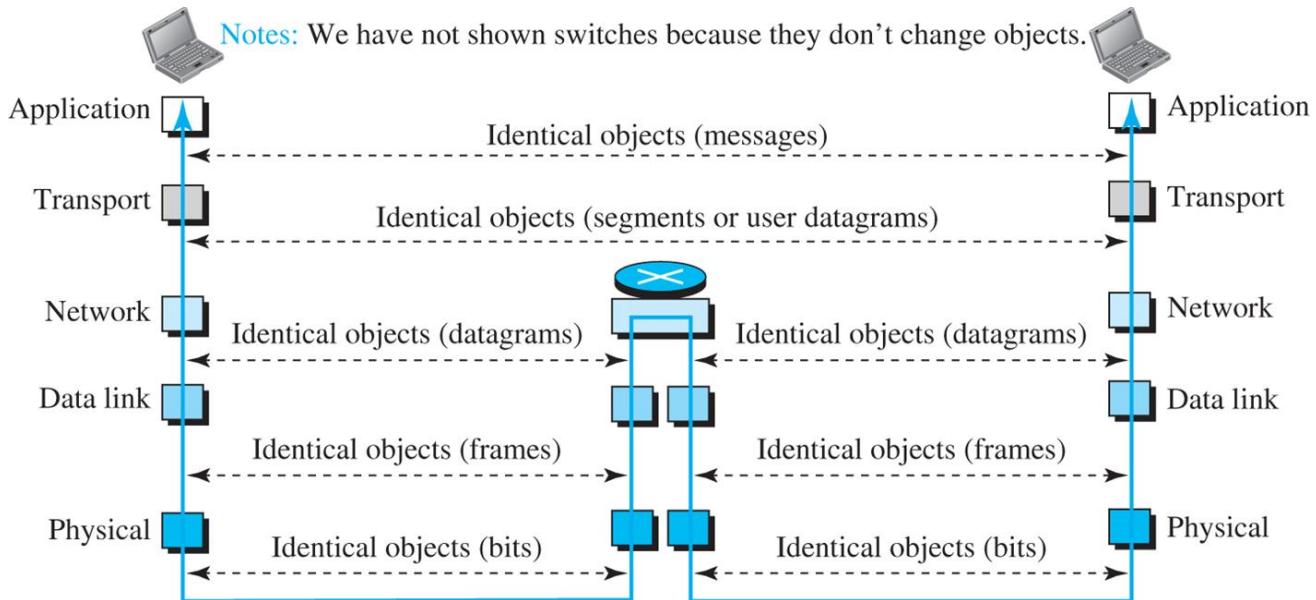


كل وجه من IP Address وشایفة الشبكة ، يعني كل وجه من وجوه الراوتر شایف عالم مختلف.



- ال Network layer للراوتر بتكون شایفة كل الشبكة وشایفة a, b, c وبتاخذ قرار انه هاي الرسالة عشان توصل b لازم تطلع من مخرج معين.
- في مصطلح اسمه protocol يحكوا مع بعض لازم ال peer layering لما 2 nodes ← يكروا مع نفسه بالضبط تتبع الشانية يعني ال physical layer بيحكي مع ال stack تتبع الأولى يكون نفسه بالضبط تتبع الثانية network layer وال physical layer
- ال physical layer وال datalink layer هدفهم دائمًا الخطوة الجاي انهم بوصلوا الرسالة الي بين ايديهم للي بعدهم وهاد المصطلح اسمه hope to hope.
- ال Network Layer هي الي كاشفة كل الشبكة ، بتنشوف ال path كله من ال source الى destination ، عارفة كل المخارج والمداخل ومين موجود ومين لاً فبهمها توصل الرسالة من ال source الى destination هيك هي الي بتحكي لل physical + datalink عشان next hope layer مين ال abstraction تكون في زي source ما بنشوف خط واحد بين ال source وال destination ما بنشوف فيه التفاصيل.





المسج الها اسم بكل layer -
 بال physical layer مافي رسالة في 1,0 بس (bits) -
 ال datalink layer بشوف كل رزمة متالية من ال 0 , 1 وبسميها Frame (لما نصير بشوف
 كلمة frame لازم نعرف انه قصدنا عن ال datalink layer .
 ال network layer هو مسمى المساجات فيها datagrams الأصلح انه تكون packet (packet)
 فاحنا رح نستخدم مصطلح ال packet -
 ال transport layer تسمية المسج بتعتمد مين ال protocol الي عم يتفرج عليه ، بـ
 TCP + (User Datagram Protocol) UDP ← 3 protocols عنا TCP/IP Stack
 (network layer IP + (Transmission Control Protocol)
 بتعامل مع ال user datagrams .
 أما ال TCP بشوف الداتا بشكل مختلف وبسميتها segments .
 آخر اشي لما نوصل عند ال user بنسميهم message -

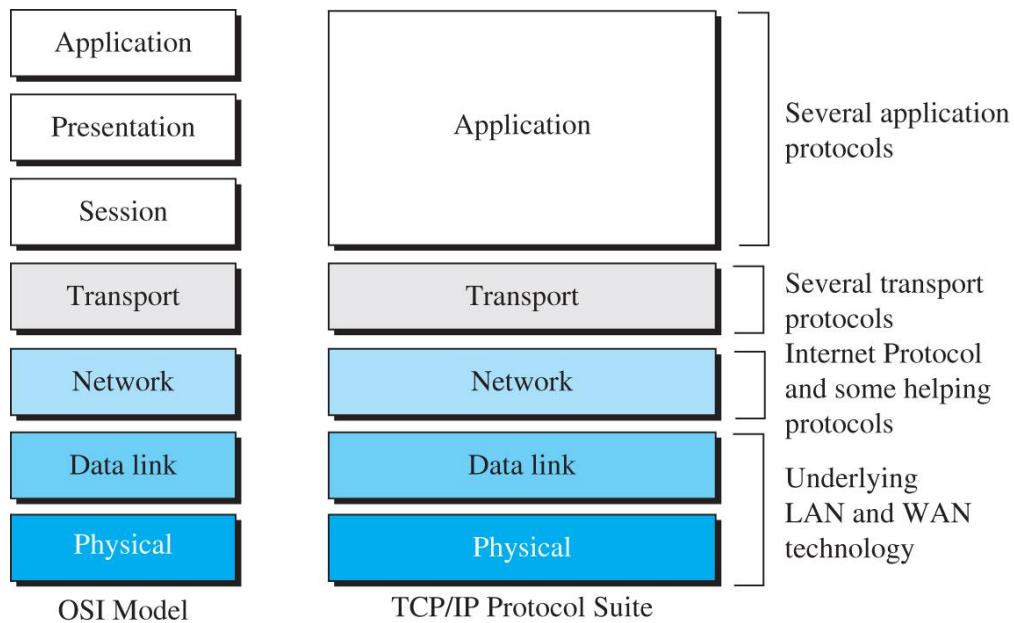
OSI Model

- When speaking of the Internet, everyone talks about the TCP/IP protocol suite, this suite is not the only suite of protocols defined.
- Established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- Almost three-fourths of the countries in the world are represented in the ISO.

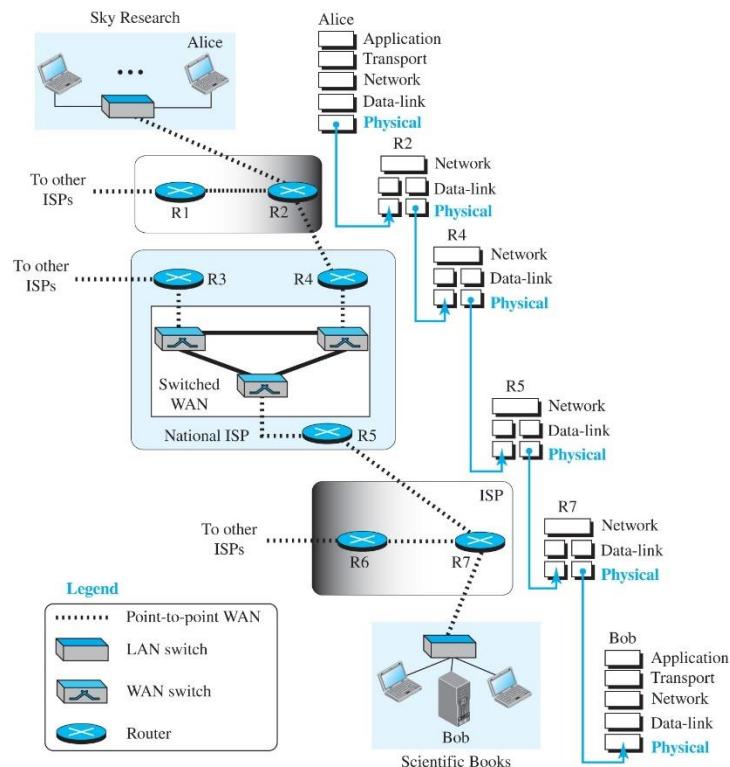


- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

دائمًا المتنافسين ال TCP وال OSI ، فعليًا بليشت الشغالة من ال OSI ، مؤسسة ال ISO عملت protocol stack عشان موضوع الشبكات ما يفلت ، لأنه إذا كل واحد بنى ال protocol stack لحاله الناس رح يبتلوا يقدروا يحكوا مع بعض ، فعمل اشي موحد ، الي هو



Chapter 02: Physical Layer



Alice بتشتغل على الكمبيوتر وبدها تبعث رسالة ل Bob بدها توصل من حاسوبها لحاسوبه، وكل واحد بيلد، فاستخدمت ال ISPs لحد ما وصل الراوتر بعدين ال موجود بجهاز Bob.

لو جابتلنا بهاي الرسمة هل هاد ? Switch أو Router لأنه في أول connection device (physical, datalink, network) 3 Layers عطول بحط .Router

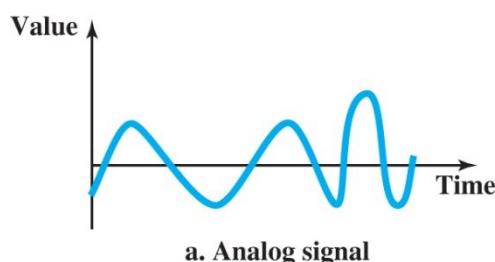
ولاحظوا انه ال physical layer بحكي مع ال physical layer (الي حكينا عنه من قبل وسميناه peer layering).

كلنا بنعرف انه بالحواسيب الداتا هي رقمية ، لكن الموجات الي بتنقل عن طريق ال wireless media هي كهرومغناطيسية ، فبدنا نلاقي طريقة تحمل هاي الموجات.

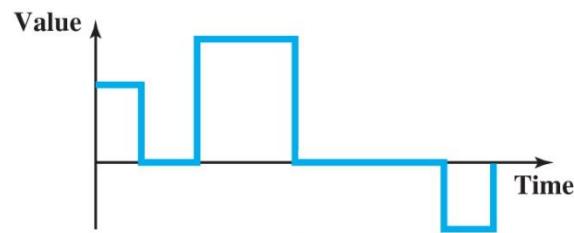


Signals

في عنا نوعين من الموجات (Analog Signals, Digital Signals) -



a. Analog signal



b. Digital signal

ال Analog signals موجودة كبنية تحياء للاتصالات من قبل الشبكات
لما نقارن بين رسمة الموجتين رح نلاحظ انه ال Analog smooth رسمتها أما الموجة
الرقمية درجية ، سبب الدرجية هو انه الموجة عم تحاول تشفير ال 0,1 ، لما تكون 0 الخط
بكون على ال x-axis ، لما تكون 1 بطلع حسب القيمة الي بتشفير ال 1 ، بعددين بصير الاقتران
درجى.

Analog Signals

معظم البنية التحتية الموجودة بتدعم ال Analog Signals -

- An analog signal can take one of the two forms: periodic or aperiodic.

أهم تصنيف لل Analog Signals هو الي بشوف هل الموجة periodic (دورية) أو aperiodic (not a).
معناها انه بعد فترة زمنية معينة بترجع الموجة بتكرر حالها.

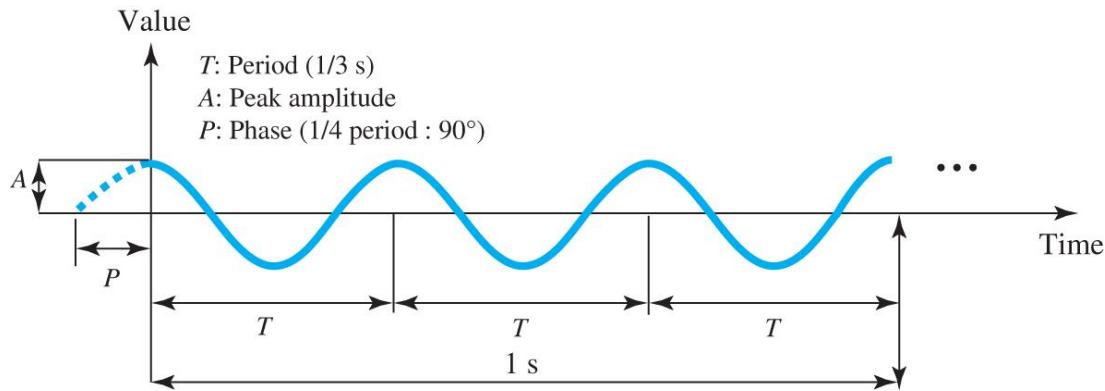
← Periodic ← النمط عشوائي.
مشان هيك بالموجة الدورية أنا بقدر أتنبأ بشكلها أما الثانية لأن.

تصنيف الموجات حسب مدى تعقيدتها: موجات بسيط (simple) + موجات مركبة
(composite).

- A simple periodic signal, a sine wave, cannot be decomposed into simpler signals.



Sine Wave



موجة الجيب هي أبسط شكل للموجة ال periodic . ما بقدر أحلاها لمركبات ، كل 360 درجة
بترسم حالها ، وقمنها بين ال 1- .

- **Phase:** The position of the waveform relative to time 0. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift.
الموجة هون بالرسمة بنلاحظ انه معمول لها shifting (إزاحة أفقية) (زي لما تحضر مسلسل وهو مبلش قبل ما انت تيجي) هاد اسمه ال phase انه متى الموجة بلشت بالنسبة ل (0,0) . إذا كانت مسبقة أو متاخرة بدننا نشوف تأخرت أو سبقت بكم ،
تقاس ال phase بال degrees ، مثلاً هون بالرسمة سبقت ب ربع دورة وربع ال $360 = 90$ فهون الزاوية 90 ، (لي حكينا 360 ؟ لأنه موجة الجيب بتكرر حالها كل 360 درجة).
- **Peak Amplitude:** The absolute value of its highest intensity.
ال amplitude هو القراءة العامودية (على ال y-axis) ، أعلى قراءة بتوصلها (بغض النظر عن الإشارة) اسمها peak amplitude .
- **Period(T):** Refers to the amount of time, in seconds, that a signal needs to complete one cycle.
المدة الزمنية الي الموجة بتحتاجها مشان ترسم حالها مرة ، تقاس بالثانية ، مثلاً بالشكل الي فوق بتحتاج ثلث ثانية مشان تكرر حالها مرة .
- **Frequency (f):** Refers to the number of periods in one second, measured in Hertz (Hz).
كم مرة بعيد حال بالثانية الوحدة ، مثلاً بالمثال الي فوق 3 مرات.



- Period and frequency are inverse of each other, in other words

$$(f = 1/T).$$

ال $1/\text{sec} = \text{Hz}$ عكس ال Hz هي frequency مثان هيك وحدة ال period .
 الموجة بوصفها يا إما باستخدام ال (frequency, peak, phase) أو (peak, period, phase).
 لأنه ال frequency وال period يعتمدوا بعض.

Wavelength

- The distance a simple signal can travel in one period.
- Wavelength binds the period or the frequency of a simple sine wave to the propagation speed in the medium.
- If we represent wavelength by λ , propagation speed by c , and frequency by f , and period by T , we get:

$$\lambda = c/f = c \cdot T$$

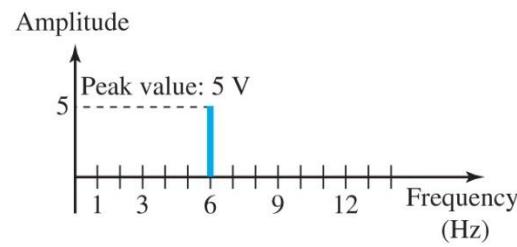
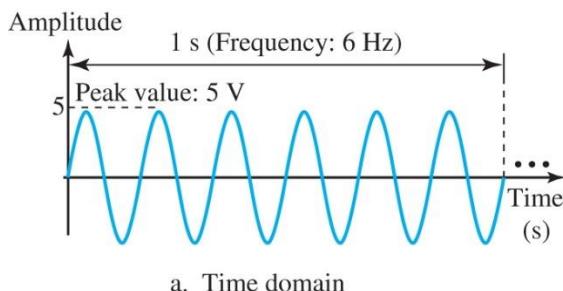
المسافة = السرعة . الزمن
 (لما λ الطول الموجي)

الطول الموجي بحكي عن المسافة المترية الي بتقطعها الموجة وبعتمد الموضوع على سرعة انتقال المادة بالوسيل (c)
 سرعة انتقال المادة بالوسط الفيزيائي اسمها .propagation speed (wired, wireless)
 ال propagation speed بعمنا نوعين منه (wired, wireless)
 ال 3أنواع : wiredTwisted pair, fiber, Coaxial cable
 يعني c مش رقم عشوائي هي سرعة انتقال الضوء أو سرعة انتقال المادة بأسلاك النحاس.

Time and Frequency Domain

A sine waves is comprehensively defined by its amplitude, frequency, and phase.
 This can be done in both time and frequency domain.

الي بعمنا عملياً هي ال composite signals بس عشان نفهم من وين اجت لازم نفهم ال simple signals



مرات بكون بدي أركب أكثر من موجة مع بعض فبرسمهم قدامي عشان اشوف شورح -
أعمل فيهم .

برسمة (a) موجة عادية ال sine waves تبعتها 0 ، ال phase = 5 = peak amplitude ، عشان -
ترسم حالها مرة وحدة بتحتاج سدس ثانية ، ال frequency تبعها = 6 (يعني بالثانية الواحدة
بترسم حالها 6 مرات) .

تخيلوا بدي أرسم كمان موجتين معها رح تكون الرسمة معجقة فمشان يكون ال -
frequency domain visualization أسهل قرروا انهم يستخدمو ال period بدلاًلة ال frequency period
يعني بعتمدوا عبعض بدل ما ارسم الموجة بدلاًلة ال frequency ، يعني بدل ما يكون ال time لي ما يكون ال frequency ، محور الصادات نفسه ، بس الموجة بترسمها خط عمودي واحد بس .

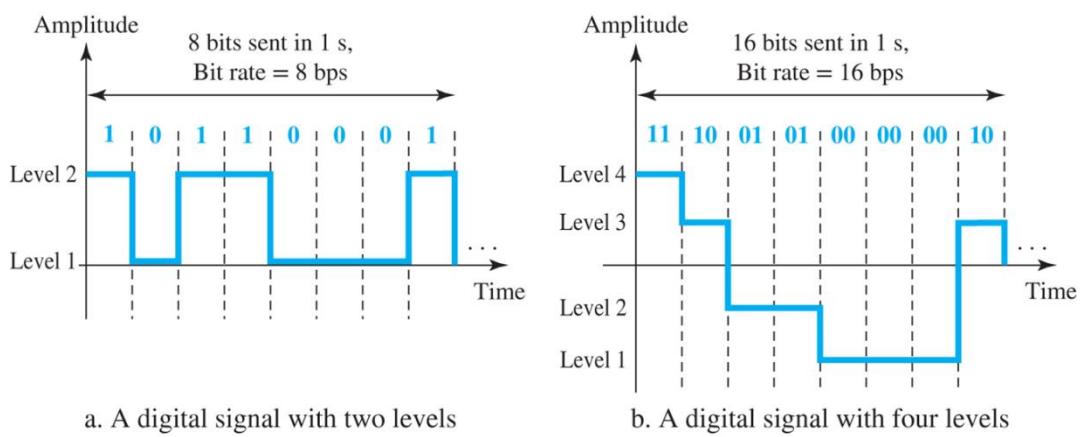
Composite Signal

A composite signal is made of many simple sine waves.

عشان ال composite signal تكونوا مركباتها ال simple different كل وحدة -
، لما نركبهم عبعض وبطلع composite signal بهمني مصطلح ال frequency bandwidth .

- Bandwidth: The difference between the lowest and highest frequencies in the signal.
 - . الفرق بين أقل تردد وأعلى تردد بال composite signal -
 - . مشارن أعرف ال bandwidth لازم تكون ال composite signal -
 - . وحدة قياسه Hz -

Digital Signals



برسمة a

عطول بنعرف انها digital signals لأنها درجية . -

1 Level بعّبر عن ال 0 و 2 Level بعّبر عن ال 1 ، فمثلاً لما تكون الفولتية 0 لهاي الموجة معناهه بشقّر ال 0 ، لما تكون الفولتية 5 يكون قصدي ال 1 . -

برسمها بناءً على ال binary strings ، زي ما حكينا لما يكون عندي 0 برسم خط عن 1 level ولما يكون عندي 1 برسم خط عند 2 level . -
قدرينا نمرق 8 bits بكل ثانية . -

برسمة b

الدرجة الوحيدة واقف عليها 2 bits واستخدمنا 4 Levels بدل 2 (ثنين سالبات وثنين موجبات) ، إذا كانت ال string الي عندي 11 برسم الخط ع level 4 ، 10 برسمه ع level 3 ، 01 level 2 . -

هون قدرينا نقل 16 bits كل ثانية (ضعف الداتا) ، وال throughput هون أعلى .
انه تكون ال digital signals دورية (periodic) احتمال كثير بعيد . -

(ملاحظة سريعة فكرة انه ال 11 هي level 4 هي افتراض فقط يعني ممكن تتغير)

طيب لي ما نزيد كمان levels؟

- نظريًا (بالورقة والقلم) فعليًا هاد الاشي أحسن لأنه كلما زدنا كلما حيزيد ال throughput
- أما فيزيائيًا ، هاي موجة وبالأخير رح تمشي بكيل فيه مقاومة ، وعندها طاقة . لما تمشي بالكيل شو رح يصير بطاقتها؟ رح تبليش تص محل ، ولما تبليش تص محل level 3 + 4 رح يسيحوا والرسالة رح تتفسر خطأ .

بما انه ال digital signals مش periodic فما بنفع أوصفها بال frequency وال period . Bit Rate

Bit Rate: The number of bits sent in 1 second.

بالثانية الوحدة كم bit بتقدر تمرق . -



Example

Assume we have downloaded text documentation at the rate of 100 pages per second. A page is an average of 24 lines with 80 characters per line. If we assume that one character requires 8 bits, the bit rate is:

هو معطيني 100 صفحة بالثانية ، فأنا بدي أحوّل الـ 100 صفحة هدول لـ bits .

بحكيلي افترض انه الصفحة فيها 24 سطر، والسطر فيه 80 characters .

الـ 8 bits = 1 byte ، والـ 1 byte هو character .

بضرب $100 * 24$ = عدد الأسطر per sec سا مش كافي

بضرب $80 * 24 * 100$ = عدد الـ bytes per sec characters (بس أنا ما بدي bytes per sec characters)

فبضرب بـ 8

$$100 * 24 * 80 * 8 = 1,536,000 \text{ bps}$$

وآخر اشي لو بدننا نحولها لـ Mega bps بضرب بـ 10^{-6}

$$= 1.536 \text{ Mbps.}$$

- كمان شغلة كنا نحكيها بالـ analog signals ومتش مُلائم انه نحكيها هون لأنها aperiodic

- الي هو الـ wavelength ، لقينا معيار بديل عنه واي هو الـ Bit Length

Bit Length: The distance one bit occupy on the transmission medium.

- يعبر عن المسافة الزمنية الي بيأخذها bit واحد في الـ transmission medium

$$\text{Bit Length} = 1 / \text{bit rate}$$

The length of the bit in the last Example:

$$1 / 1,536,000 = 0.651 \text{ microseconds}$$

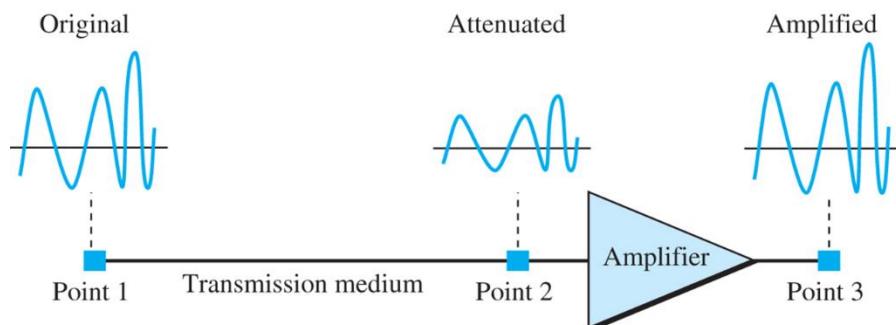


Transmission of Digital Signal

- جماعة الرياضيات بحبوا التعريفات ، فمشان يقبلوا بال digital signal عرفوها بدلاًلة ال analog signal
- Digital Signal: A composite analog signal with frequency between zero and infinity.
- هاد الاشي بتترتب عليه انه كان في طريقتين لإرسال ال digital الداتا: الطريقة القديمة ال baseband ، والأحدث ال broadband
- Broadband: Changing the digital signal to analog signal and send the analog signal.
- يعني بتبلش ال digital data بتحولها ل digital signal بعدين بتحولها ل analog signal . يعني بتبعتها بالبنية التحتية لل analog .
- Baseband: Sending the digital signal without changing it to analog signal.
- هون هو بده البنية التحتية تدعم ال digital data + signal بدون ما أحول ل analog signal . فبأخذ ال digital data بحملها ف digital signals وبيعتها زي ما هي .
- يفضل انه نبعث الداتا عن طريق ال Baseband لي ؟
- أسرع ، لأنني بختصر مراحل (عملية التحويل بتاخذ وقت خصوصاً انه ما بصير مرة وحدة بصير بكل risk) ، وأسلم (ما فيها hope) .

Signal Impairment الاعتلالات الموجية

1) Attenuation and Amplification اضمحلال الموجة



هي مشكلة فيزيائية ماحدا الله دخل فيها ، طبيعة الموجة انها تحمل طاقة ، ولما بتمر عبر وسط بتخسر جزء من طاقتها بسبب المقاومة . الخاصية الي بتتأثر هي ال amplitude . بالمثال فوق في موجة عنا بعد ما قطعت مسافة معينة من نقطة 1 إلى 2 بإحدى ال transmission medium ووصلت لنقطة 2 مضغوطه عامودياً (عم فقد طاقة) .



الحل اني استخدم مقوّيات (Amplifier) ، بتصرير عمليات معايرة مشان يعرفوا وين المكان الصحيح الي رح ينحط فيه المقوّي (مشان كمان لو نحط قبل ممكّن تزيد القيم كثير).

- Attenuation: A loss of energy.
- When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
- To compensate for this loss, we need amplification.

- في عنا قانون بنقيس فيه الموجة في حال تم تقويتها أو في حال ضعفت شو مقدار القوة أو الضعف

$$10 \log_{10} P_2 / P_1$$

↓ ↓
الطاقة الجديدة الطاقة القديمة

Example

Suppose a signal travels through a transmission medium and its power is reduced to one half. This means that $P_2 = 0.5 P_1$. In this case, the attenuation (loss of power) can be calculated as:

$$10 \log_{10}(0.5P_1) / P_1 = 10 \log_{10} 0.5 = 10 \times (-0.3) = -3\text{dB}$$

A loss of 3 dB (-3 dB) is equivalent to losing one-half the power.

لأنها طلعت سالبة رح تكون (loss of power) الموجة ضعفت

لو كانت موجة بتكون (gain of power)

2) Distortion التشوّيه

- The signal changes its form or shape.
- Occur in a composite signal made up of different frequencies.
- تشوه في شكل الموجة.



- احنا بالعادة بنبعث مجموعة من ال composite signals مع بعض ك signals ، فمثلاً لو كان عننا 3 موجات وغيرها ال phase 0 (للسهولة) وبندمجهم ، على الطريق ممكن وحدة تسبّب ال phase ووحدة تأخر ، يعني ما يمشوا كلهم عنفس السرعة هون الشكل الخارجي للموجات بختلف.
- هل في حل للموضوع؟ ممكن نستخدم فلتر بس كثير مرات الموضوع ما يكون مُجدي.

3) Noise التشویش

- تكون عندي موجة أصلية فيها مركبات فالى بصير انه بتيجي موجة دخيلة وبتدخل على المركبة وبتعمل موجة جديدة، هون عنجد الفلتر بتفيينا (زي السماعات الي بتعمل cancellation cancellation بين المستويات different frequencies بتستخدم هاد النوع من الفلتر، مدي الصوت معروف ال noise تاعتنه فأي اشي خارج مدي ال frequency تبع الصوت بعتبره إزعاج وبشيشه ، وممكن إذا كانت ال noise خبيثة عادي بتتدخل).

Signal-to-Noise Ratio (SNR) = (average signal power) / (average noise power)

الوضع الطبيعي انه الكسر يكون أكبر من 1 لأن المفترض انه موجتي تكون أقوى من ال noise . أما إذا كانت قوة ال noise أقوى من قوة الموجة وقتها الكسر يكون أقل من 1 ، والأخطر انها تكون 0 .

Data Rate Limits: How fast we can send data, in bits per second.

Depends on three factors:

1) The bandwidth available

كلما زاد ال Data rate (أي انتشار البيانات) زاد ال bandwidth (أي عدد مقاعد الموجة) وكلما كان عدد مقاعد الموجة أكبر بمتكون فرصتي أنني أركب فيه أكثر

2) The level of the signals we use

زي الرسمة الي حطينا فيها levels 4 شفنا انه ال bitrate زاد (كلما قدرت أجز أكثر بنفس وحدة الزمن)

3) The quality of the channel (the level of noise)

كلما كانت ال noise أكثر كلما كانت ال bitrate أقل لأنه بخفف فعاليته

في عنا صيغتين يستخدموا مشان نقرر شو ال bitrate اي رح يستخدم أكثر بنسميمهم formulas مش equation لأنه ما تم اشتقاقةهم بحساب رياضي.

- Nyquist for a noiseless channel, and Shannon for a noisy channel.



لـي شـتـيـنـ؟ لأنـهـ وـلـاـ وـحدـةـ فـيـهـمـ بـتـطـلـعـ Nyquistـ -
 عـلـىـ الـأـلـ مـشـانـ هـيـكـ اـسـمـهـاـ levelsـ وـ b~andwidthـ مـشـانـ هـيـكـ اـسـمـهـاـ for a noiseless channelـ -
 أـمـاـ بـتـطـلـعـ عـلـىـ الـأـلـ noiseـ وـlـاـlـ Mـشـانـ هـيـكـ اـسـمـهـاـ for a noisy bandwidthـ -
 channelـ

Noiseless Channel: Nyquist Bit Rate

$$\text{Bit Rate} = 2 \cdot B \cdot \log_2 L$$

$B = \text{bandwidth}$

Example

We need to send 265 kbps over a noiseless (ideal) channel with a bandwidth of 20 kHz. How many signal levels do we need? We can use the Nyquist formula as shown:

$$265,000 = 2 \times 20,000 \times \log_2 L \rightarrow \log_2 L = 6.625 \quad L = 2^{6.625} = 98.7 \text{ levels}$$

- Since this result is not a power of 2, we need to either increase the number of levels or reduce the bit rate. If we have 128 levels, the bit rate is 280 kbps. If we have 64 levels, the bit rate is 240 kbps.

Noisy Channel: Shannon Capacity

$$C = B \cdot \log_2(1 + \text{SNR})$$

Example

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as shown below.

$$C = B \log_2(1 + \text{SNR}) = B \log_2(1 + 0) = B \log_2 1 = B \times 0 = 0$$

- The data is so corrupted in this channel that it is useless when received.
 يعني فعليًّا كل البنية التحتية ما بتسمى اشي إذا ال noise كثير قوي.



Example

We can calculate the theoretical highest bit rate of a regular telephone line. A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communications. The signal-to-noise ratio is usually 3162. For this channel the capacity is calculated as shown below.

$$C = B \log_2(1 + SNR) = 3000 \log_2(1 + 3162) = 34,881 \text{ bps}$$

This means that the highest bit rate for a telephone line is 34.881 kbps. If we want to send data faster than this, we can either **increase the bandwidth** of the line or **improve the signal-to noise ratio**.

Using Both Limits

Example

We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level? (ما بجيروا زي هيک بالامتحان)

First, we use the Shannon formula to find the upper limit

$$C = B \log_2(1 + SNR) = 10^6 \log_2(1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}$$

The Shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps, for example. Then we use the Nyquist formula to find the number of signal levels.

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L \rightarrow \log_2 L = 2 \rightarrow L = 4$$



كيف بنقيس أداء الشبكة؟

1- Bandwidth

كلما بلشت بشبكة ال bandwidth تبعها أكبر ، كان عندك فرصة افضل انه تعطي bitrate أعلى وبالتالي كفاءة أفضل

Example

The bandwidth of a subscriber line is 4 kHz for voice or data. The bit rate of this line for data transmission can be up to 56 kbps, using a sophisticated modem to change the digital signal to analog. If the telephone company improves the quality of the line and increases the bandwidth to 8 kHz, we can send 112 kbps.

2- Throughput: The measure of how fast we can actually send data through a network.

هو فعلياً ال bitrate بس بصيغة أخرى ، وأكدت كلما كان التزوبوت أفضل كانت الشبكة أسرع.

3- Latency (Delay)

How long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

بدى الرسالة كاملة وبدوركم المدة الزمنية الي رح تستغرقها على شرط توصل لل destination . من اللحظة الي أول bit فيها انعمله transmission

Types of delay:

1- Propagation Delay

عبارة عن فيزياء ، الزمن اللازム لانتقال bit واحد عبر الوسط الفيزيائي ، عادةً تكون صغيراً . ويعتمد على سرعة انتقال الموجة بالوسط الفيزيائي.

2- Transmission delay

يعتمد على الزمن اللازيم عشان ال packet تتحمل على الشبكة وهاد الاشي يعتمد على عاملين رئيسيات : طول الرسالة / bitrate . كلما كان ال bitrate تاعي أفضل كلما كان ال transmission أقل ، كلما كان طول الرسالة أقل كلما كان ال transmission أقل.



3- Queuing delay

عندى path من ال source الى destination . اى path تكون من مجموعة من الراوترز وال switches حسب شو النتورك الي بدي ايها ، بالوضع الطبيعي بتنتقل الرسالة مني لـ switch المسئول عنى للراوتر للراوتر الي بعده لحد ما توصل للراوتر المسؤول عن ال destination . كل واحد من هدول الراوترز لما توصله الى packet تبعتي لازم تصفع على الدور لبين ما يفضى يشتغل فيها (زي الكاشير) ، إذا الى queue كان مفلل بنعمللها dropping وهاد الاشي سيء.

فهي معناها قديه بدي استنى عالدور عشان الراوتر يتفرج على ال packet ويقرر من أي مخرج لازم تطلع.

4- Processing delay

أقل اشي تأثيراً ، لنه CPU time مشكلتك معه بس انه يجييك الدور ، وأول ما يجييك الدور كثير سريع ، بس بتتفقد الى destination IP address وبتقرر من أي مخرج تطلع.

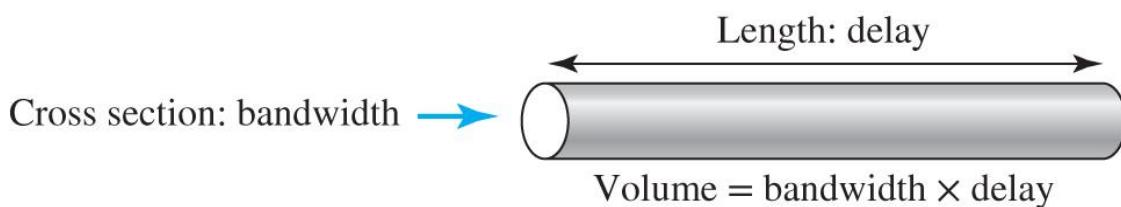
الي بنخاف منهم هم الى transmission delay + queuing delay -

- Bandwidth and delay are two performance metric of a link. However, what is very important in data communications is the product of the two, the bandwidth-delay product.

delay * bandwidth -

- We can think about the link between two points as a pipe. We can say that the volume of the pipe defines the bandwidth-delay product.

كلما كانت الى اكبر كلما كانت حجم الماسورة أوسع بالتالي -
كفاءتها أعلى



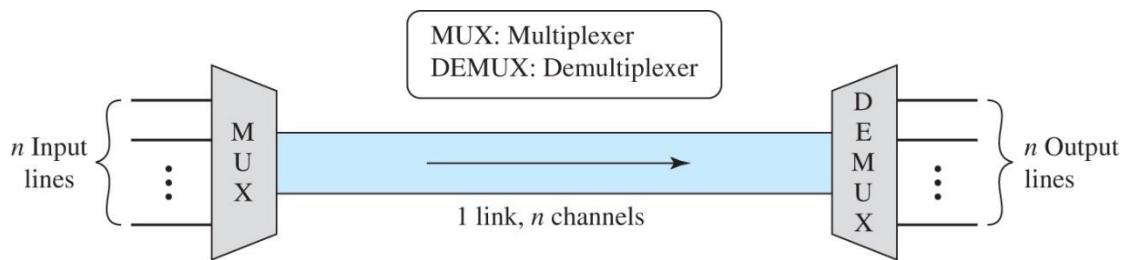
Jitter

- حكينا عنه من قبل انه التباعد الزمني بين كل رسالتين متغير ، أنا بدي يكون قيمة ثابتة
- A problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

Multiplexing

- عندي كابل بسع bandwidth كبيرة بس الداتا تبعـت اليوزر ما تحتاج كل هاد المكان يحتاج مساحة بسيطة ، بس أنا ما بدي أخدم يوزر واحد بدي أخدم 5 4 10 ، فكل يوزر يكون ماذ bandwidth بسيط ، فكيف بدي أستفيد من ال capacity الي عندي؟ بعمل ال multiplexing ، باخذ اليوزر الصغار وبركب كل واحد على frequency مختلفة وهيك باخذ الحيز كامل.

- We have links with limited bandwidths.
- Sometimes we need to combine several low-bandwidth channels to make use of one channel with a larger bandwidth.
- Sometimes we need to expand the bandwidth of a channel to achieve goals such as privacy and anti-jamming.

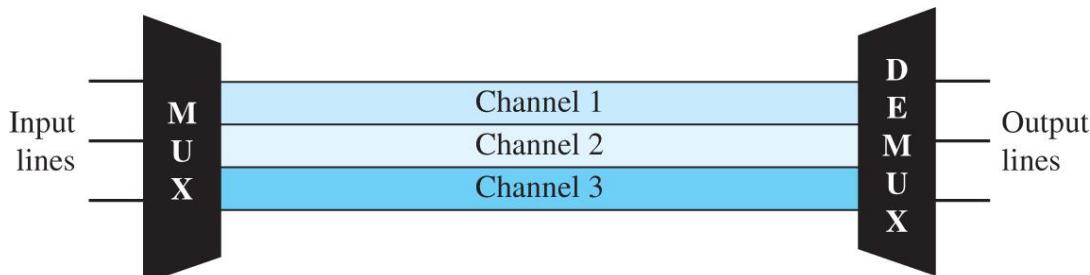


- عندي مجموعة من اليوزر كل واحد فيه input line خاص به (رسالته ، بياناته) بفوتوا كل الرسائل المختلفة من اليوزر المختلفين على ال MUX (بنية تحتية عبارة عن مجموعة من الأجهزة بعملا على دمج المسجات الي من اليوزر المختلفين) بمساحة كبيرة ، من برا بتبيـن انها اشي كثير كبير بس فعليا هي كلها مسارب كل مسرب بخدم مجموعة معينة من الناس ، والداتا بالأخير بتنقل عبر ال hopes بموجة وحدة كبيرة ولما بتوصل على ال



- بصير في destination ، بتاخذ الموجة الكبيرة وبتفكفكها وبتطلع منها كل رسالة وبتعطيها للشخص الي بستناها.
- فبدل ما أطلع كل رسالة لحال واخليهم يصفوا على الدور بطلع كل الرسائل مرة وحده.
- في عندي نمطين من ال multiplexing بعتمدوا على البنية التحتية هل بتدعم ال baseband أو broadband
- إذا كانت بتدعم ال analog signals لازم الجا لاشي اسمه Frequency-Division Multiplexing

Frequency-Division Multiplexing



- عندي link كبير فيه bandwidth كبير معناته أنا عندي مجموعة كبيرة من frequencies بدعمها هاد اللينك فكيف بدبي أخدم اليوزر من خلله؟
- بمسك اليوزرز الي عندي (مثلًا بالصورة في 3) كل يوزر عنده binary data ، اليوزر اخر همه هاي الداتا كيف بتنقل همه بس انها توصل لل destination . فأنا باخذ من اليوزر الأول ال binary data تاعته وبتحولها ل analog signals وبعدين بختار الموجة التناظرية على محدد وبلزم الداتا تاعتت اليوزر انها تتبعت بهداء ال frequency
- مثلًا بتثبت frequency معينة ليوزر محدد بتصير كل رسائله بتتحمل على frequency ، مثلًا بتثبت frequency ما حدا ثاني بشاركه بهداء ال frequency analog signal بس بهداء ال frequency ما حدا ثالث بشاركه بهداء ال second digital signal ومنها ل analog signal وبلزمته ب ال frequency range واليوزر الثالث نفس الاشي....
- بتطلع الداتا من hope ل hope لحد ما توصل ال destination تكون في demultiplexer
- فلاتر كل فلتر بسحب frequency معينة وبفكفها وبتحولها ل analog signals ل signal data ، وهيك اليوزر يستلم الرسالة من اليوزر المقابل لاله.
- Frequency-division multiplexing(FDM): an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted together.

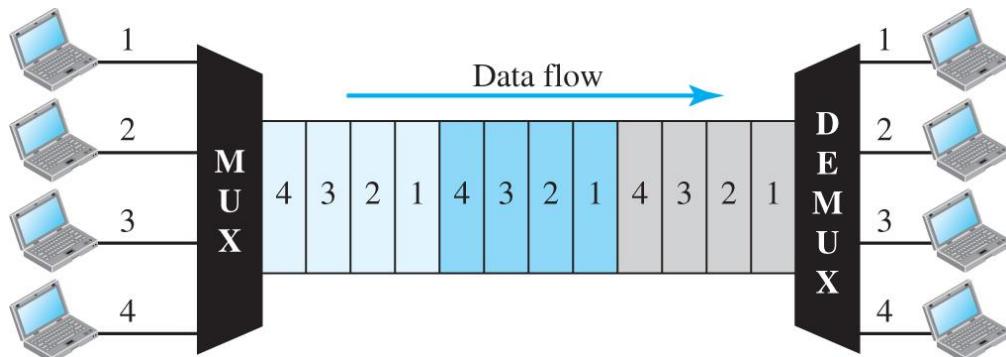


هون ال privacy ← مثلاً في حرب ، وبدنا نبث رسالة من قاعدة عسكرية لقاعدة عسكرية -
 ثانية ، وعارف انه العدو بتنصت عليك وبدك تصعب عليه مهمة انه يعرف شو الرسالة.
 فشوا ممكن نعمل؟ ممكن نستغل فكرة ال bandwidth الكبيرة ونقسم الرسالة لأجزاء .
 وكل جزء نبيه على frequency مختلفة ، فالي بتنصت ما بعرف ال substring الي رح تيجي
 رح تبئها على أي frequency وهاي العملية بنسميها frequency hopping -
 لو البنية التحتية جديدة وما فيها analog transmission فيها digital transmission ما بقدر
 أطبق ال Frequency-Division Multiplexing ، ف رح أستخدم النوع الثاني من ال
 Time-Division Multiplexing وهو multiplexing

Time-Division Multiplexing

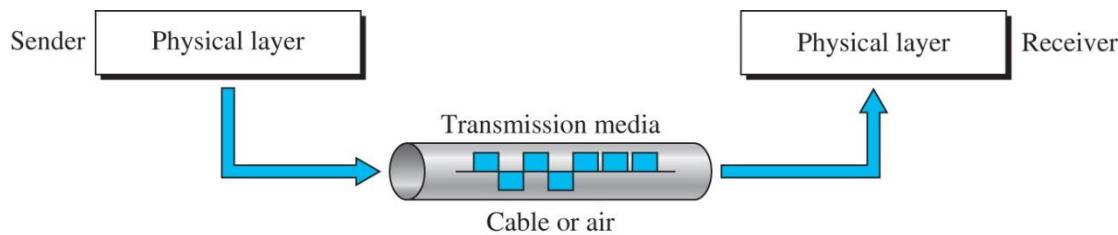
مثلاً لو عندي 4 users ، بخصوص ال bandwidth كامل ليوزر واحد لمدة زمنية محددة ، وإذا -
 خلصت المدة خلص بروح دورك بأول cycle . بعدين بعد ما يخلص دور الكل برجع الدور على
 الأول

- Time-division multiplexing (TDM): A digital technique that allows several connections to share the high bandwidth of a link.



Transmission Media

- Transmission media are located below the physical layer and are directly controlled by the physical layer

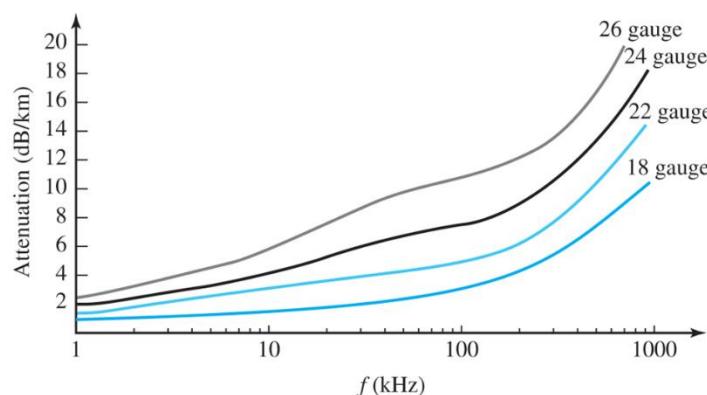
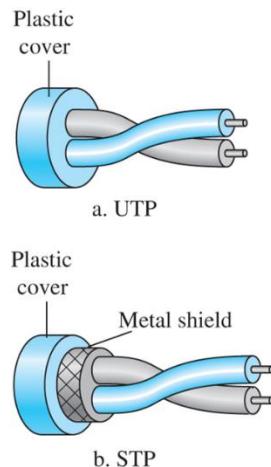


رح نحكي هلا ال transmission media شو أنواع الكيبل والي تكون عبر الفراغ أو الهواء شو أنواعها كمان.

- Guided Media: Which are those that provide a conduit from one device to another.
 - . guided media بتسخدم الكوايل بنسميها physical layer او communication media أي اشي wireless يعني عبر الهواء اسمه unguided .
 - . أي اشي Guided انواع ال

1) Twisted-pair cable

- Consists of two conductors, each with its own plastic insulation



ال 2 twisted cables ملفوقين على بعض وبكونوا نحاس وفي عليهم من برا بلاستيك (ما في طبقة عازلة) فاسمها unshielded (الي برسمه a)، ما بخدم مسافات طويلة ، بس تركيبه وفكه سهل ، (الي برسمه b) الي بفرق عن a انه بين الجذلة والبلاستيك في طبقة من المعدن (زي الشبك بتكون) فائدتها انها بتقلل من تداخل

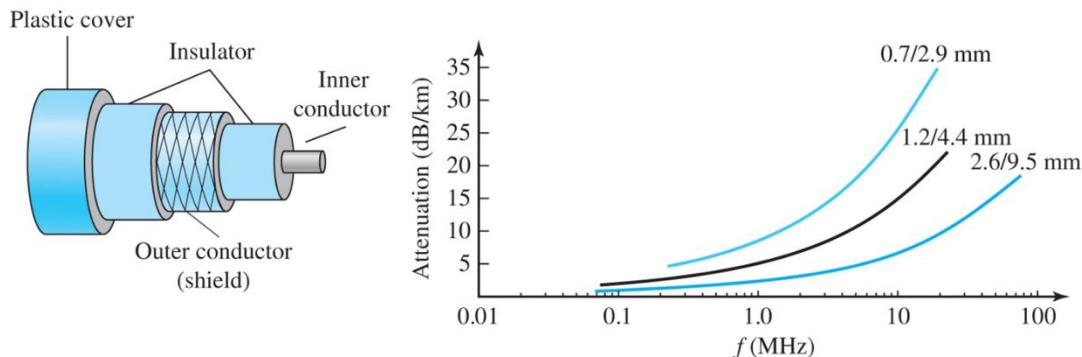


الموجات الكهرومغناطيسية ، فبتعزل الكيبل بطريقة أفضل عن التشویش الى ممکن يكون حوالیه ، وبدعم bandwidth أعلى.

- الأرقام الي موجودة على يمين الرسمة (18 gauge, 22 gauge,...) بتدل على السماكة ، الرقم الأقل معناه انه السماكة أكبر . والرقم الأكبر معناه انه السماكة أقل . فهوون أسمك اشي ال 18 gauge .
- مين الي عنده قدرة أكبر على مقاومة ال attenuation؟ السلك الأسمك (يعني 18).

2) Coaxial Cable

- Carries signals of higher frequency ranges more than those in twisted-pair cable.

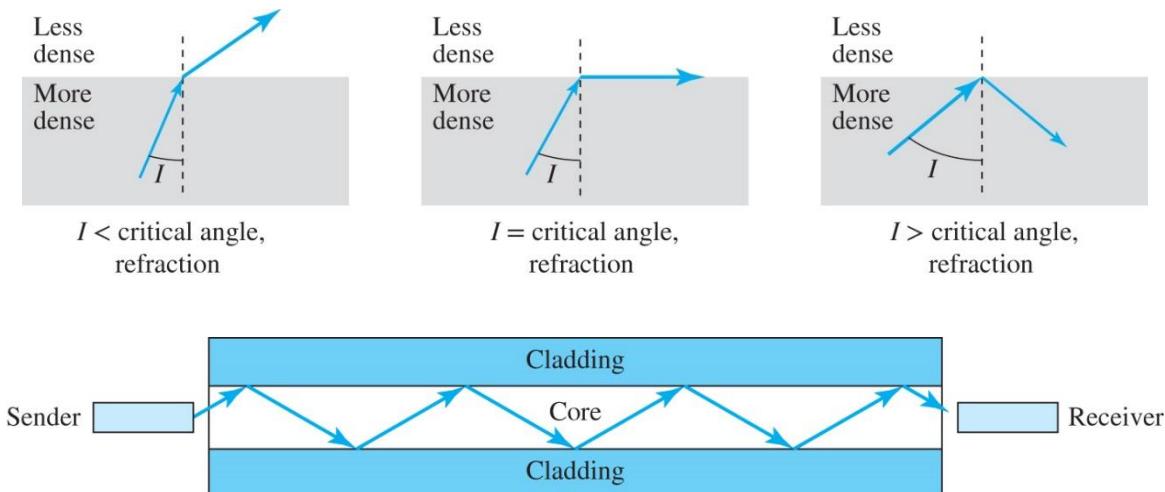


- الكوابل المحورية تكون كيبل جوا كيبل ، بالأول كيبل نحيف كثير (Inner conductor) . بعدين مادة عازلة (Insulator) ، وبعدين كمان كيبل (Outer conductor) وكمان مادة عازلة (plastic cover) . وأخر اشي (Insulator) .
- فعليًا هو محمي من التشویش بطريقه أفضل من ال twisted pair . وبقدر يغطي مسافات متريه أكبر .
- بالرسمة على اليمين في قطر الكيبل الداخلي وقطر الكيبل الخارجي ، يقاسوا بل mm . كل ما كان القطر أكبر كلما كان الكيبل أثخن .
- بتدعم frequency و bandwidth أكبر من twisted pair . كلما كانت السماكة أكبر ، كلما كان تعرشك لل attenuation أقل . التعامل معها بده متخصصين .



3) Fiber-Optic Cable

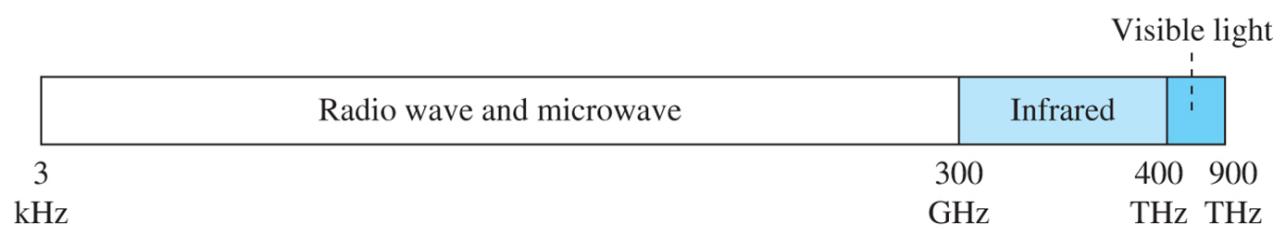
- Made of glass or plastic and transmits signal in the form of light.



- مافي مجال أي حدا يلمسه أو يعمله صيانة (بده حدا مختص).
- بنите التحتية مكلفة ، وبينمدة لمسافات بعيدة.
- من جوا تكون شعيرة أو أكثر من الزجاج أو بلاستيك.
- بشتغل بمبدأ انعكاس الضوء ، الضو لما بسقط من مكان أكثر سماكة لمكان أقل سماكة بنكسر بس لما الزاوية تبلش تزيد الضو بتعكس، ففكرت الفايبر انه الدات بحولها لومضات ضوئية والومضات بحشرها جوا الكيبل، بحشرها عن طريق أنه بسقطها.
- هون ال bandwidth جدًا عالي بس مُكلف جدًا.

Unguided Media: Wireless

- Transport electromagnetic waves without using a physical conductor.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.



- الطيف الكهرومغناطيسي ببلش من 3kHz ل 900 THz ، الي بعد ال 400 THz ما بهمنا لأنه الضوء المرئي ، الي بدننا اياه من 3 kHz ل 400 THz .
- ال Infrared يستخدم بس مش كثير لأنه ما بغطي مسافات كبيرة (زي الريموت تبع التفزيون).
- موجات الراديو بتغطي مسافات أكبر من موجات الميكرويف.
- موجات الراديو بنسميتها omnidirectional يعني أي حدا بلقط الموجة .
- أما موجات الميكرويف unidirectional من راس لراس ، فإذا ما كنت واقف بالاتجاه الصحيح ممكن ما تلقط الموجة
- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called **radio waves**.
- Waves ranging in frequencies between 1 and 300 GHz are called **microwaves**.
- Radio waves, for the most part, are omnidirectional.
- Microwaves are unidirectional.
- When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.
- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm) can be used for short-range communication.
- Infrared waves, having high frequencies, cannot penetrate walls.
- This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.



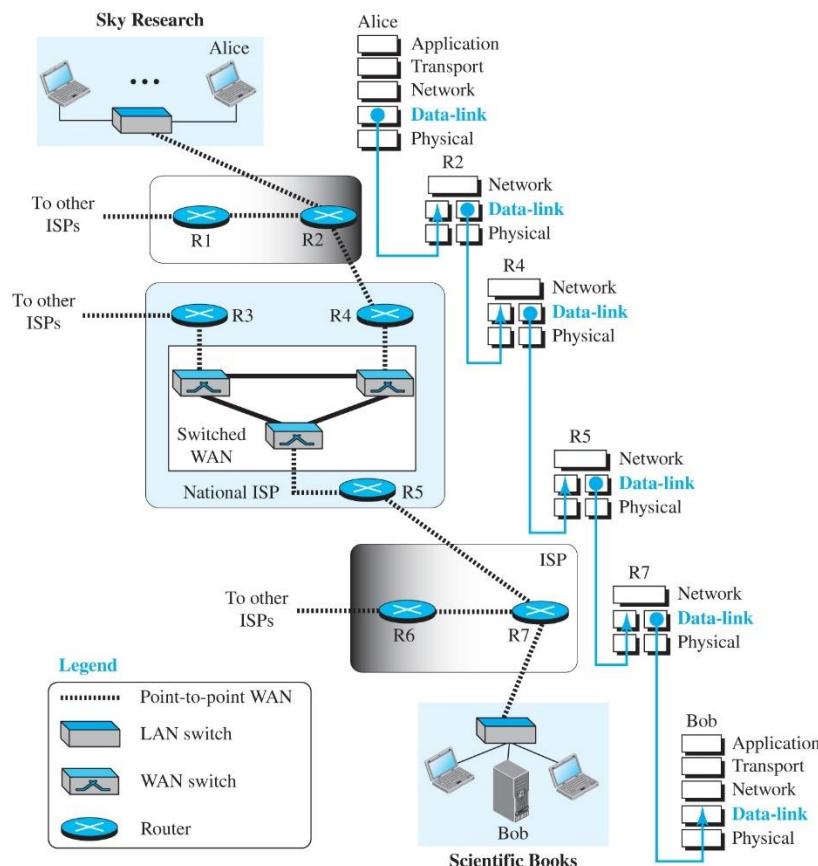
Chapter 03: Data-Link Layer

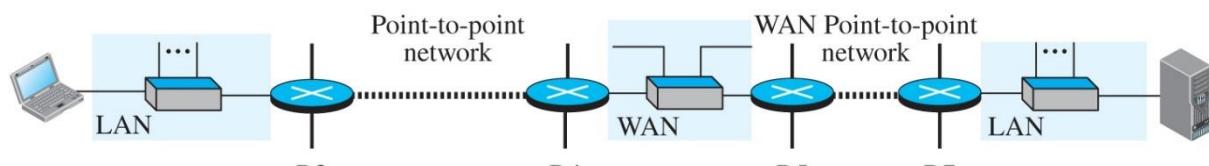
شو سبب التوأمة ما بين ال data link layer و ال physical layer

في كثير physical layer بال data link layer مشان تشتغل بتحتاج ل protocols معينة .
مشان هيك في مصنعين بعملوهم ك (data link و physical layer) package وحدة -
يعني مش أي data link layer protocol الخاصة فيه) - يعني مش أي layer protocols physical layer

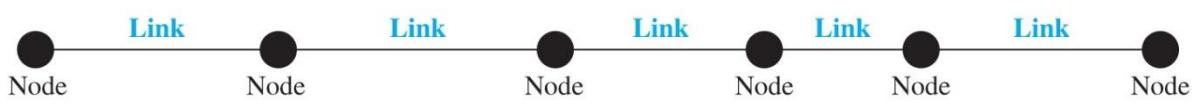
الاثنين مهمهم انهم يوصلوا الرسالة لل next physical layer و ال data link layer -
ما بال physical layer كان همها انه ال 0 و 1 ينطلقوا لل next hope . hope
النظر شو هم ، كمان ال data link layer هدفها انه ال frame يوصل لل next hope .
الها علاقة وين ال destination أو شو المسافة بينه، بس بدها توصل لل next hope

- The Internet is a combination of networks glued together by connecting devices (routers or switches).
- If a packet is to travel from a host to another host, it needs to pass through these networks.





a. A small part of the Internet



b. Nodes and links

بالرسمة بيبني انه بين أي node و node على الطريق في link لما بدننا ننتقل من ال source destination، سواءً كانت هاي ال node هي switch أو router ، فال فكرة من الرسمة يذكرني انه بال data link layer احنا بس بنتطلع على ال next hop ما بهمني ال path كاماً ..

قبل ما نتفرج على ال data link layer شو طبيعة ال protocols الي فيها وشو المشاكل الي بتحلها لازم نميز هاد ال link هو بس ل 2 points ومافي حدا ثانى مشاركون فيه إذاً اه ال data link layer هون بس بتركز على موضوع ال framing (بتشيك انه سليم، بنتقل media access control بسلامة، شو محتوياته...) ومافي داعي تهكّل هم اشي اسمه ال point to point (يعنى مين بشاركني بهذا ال link) وهای الحالة هي ال



- الحالة الثانية هي ال broadcast link هون معناها بال broadcast انه هاد ال link مشترك وفي أكثر من sender غيري ممكن يكونوا هلاً عم يستخدموا معي (زي شارع وفيه مسارب ومنش انت لحالك بتسوق فيه فما بتقدر تتجاوز ...) فهون إذا كانت هيك الحالة هاد ال link ما بقتصر علي بس في nodes ثانية عم تحاول تعمل sending هاد اسمه ال broadcast link . media access control (MAC) اي هي ال framing . يعني باختصار ال data link layer بتهتم بمسألتين، الأولى ال framing وهذا دائمًا لازم تتعالج،

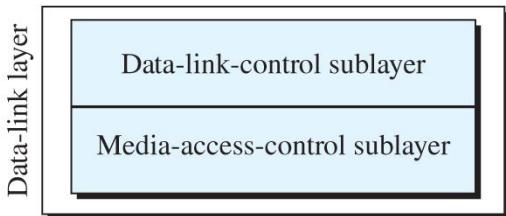
والثانية ال media access control هي ممكن نحتاجها، إذا كان اللينك broadcast وفي ناس غيري يستخدموا اللينك معي بنفس الوقت، هاد الموضوع تكون أقل خطورة إذا كانت ال links wired . وبتزيد خطورته إذا كانت ال communication unguided بصير صعب أعرف إذا في حدا ثاني عم بدخل على ال communication media وبستخدمها معي أو لا، أما إذا اللينك point to point ما بستخدمها لأنني لحالي وما حدا بزاحمي.

- Two nodes are physically connected by a transmission medium such as cable or air.
- We need to remember that the data-link layer controls how the medium is used.
- We can have a data-link layer that uses the whole capacity of the medium; we can also have a data-link layer that uses only part of the capacity of the link.
- In other words, we can have a point-to-point link or a broadcast link.
- We can divide the data-link layer into two sublayers: data link control (DLC) and media access control (MAC).
- This is not unusual because, as we will see in later chapters, LAN protocols actually use the same strategy.

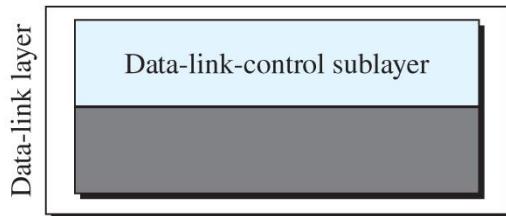
- ال DLC هي المنطقه الي بتعالج كل الشغلات المتعلقة بال framing (من وين بلش، وين خلص، كم bit فيه، شو طوله، عم بوصل بسرعة كبيرة أو ببطء، هل هي سليمة أو لا) ولازم أساويها دائمًا.

أما لو كانت broadcast link بصير عندي غير ال framing كمان frame (مين عم بشاركتي باللينك، هل مسموح لي أبعث، جهزت ال frame، بصير أبعث أو لا)، بال point to point ما بتكون فعالة لأنه مافي حدا بشاركتي باللينك.





a. Data-link layer of a broadcast link



b. Data-link layer of a point-to-point link

الي رح ناخذه هلاً بهاد التشابتر رح يكون نفس تشاپتر 4 و 6. بس الفرق انه هون رح نشرح بشكل عام، ما رح نسمى أي data link layer باسمه، بتشاپتر 4 و 6 رح نخصص ف رح يكون تطبيق على 3.

Data Link Control (DLC)

- (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast.
- Data link control functions include framing and flow and error control.
error control و flow control و framing
- بال DLC بدن اال

Framing

نفترض في node وبدى packet وبيجي اال network layer من ال sender machine .
أجهزها ك frame عشان تنزل على الشبكة. بدی أشوف هل هاد ال packet كبير أو صغير،
إذا كبير رح أقسمه ، وإذا صغير وحجمه مناسب بدی أرتبه وأضيفله header (فيه البيانات
الأساسية تبعتي مثل ال physical address و ال MAC Address) وال node تبعي وتبع ال physical address
بعدى) و trailer (فيه كود بالعادة الهدف تبعه ال error control).
بعض بروتوكولات ال data link layer بتفترض انه اال frame حجمه ثابت، مثلًا 16 بايت،
فكل فريم تكون االله 16 بايت يعني اال next node لما بتستلم اال 0 و 1 من ال physical
ما عندها مشكلة تعرف هي وين لأنه عند كل 16 بايت بفصل، فحدود الفريم بتكون
معروفة وسهل تحديها.

المشكلة بال data link layer الثانية الي بتسمح بتفاوت حجم الفريم، هون عشان نعرف
بداية الفريم أو نهايته قرروا انهم يحطوا علامة عن طريق sequence معينة من اال 0 و 1
بقرروا انه يعتبروا البداية مثلًا وبسموها flag، ونفس الاشي بعملوا للنهاية.
مش كل مسج موجود بالشبكة هو user data، مرات تكونوا الرواتر بتواصلوا بين بعض،
فممكן يكون الفريم الي بالشبكة هو control frame ومتش data frame.

في عنا مشكلة بالحالة الثانية، نفترض انه اال user بده بيعدت user data frame . ممكن اال
الي افترضناه للنهاية هو user data بس كان نفس اال binary string pattern الي بمثل

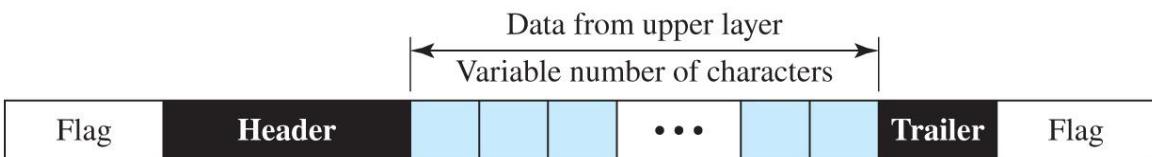


نهاية ال frame. الحل هو انه قبل ما نبعث الفريم نشيّك على الحالات. بنأخذ ال user data وبنتفقدها، إذا فيها pattern حساس بالنسبة لل data link layer بنعملي اشي بحيث انه كل ما يشوفوه تعرف انه هاد user data مش command وما تاخذها، هاي الحركة اسمها stuffing، أي مكان عند ال user data حساس بضيف عنده بایت معين (حشوة) ودائماً بنضيفها قبل الداتا وبعد ما أخلص بضيف ال header و trailer، بحط علامة البداية والنهاية، وبعدها بروح وبوصل ال next hop، وبحوال ال physical layer flag trailer و header وال flag و بتفرج عالداتا، بدبي أرجع لفريم، لما يطلعلي الفريم بشيل ال network layer ممكن يكون معمول الداتا لأصلها، فقبل ما أمسك الداتا وأرفعها لل network layer (إذا لقيت بشيله stuffing).

- The data-link layer needs to pack bits into frames, so that each frame is distinguishable from another.
- Our postal system practices a type of framing.
- The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.
- Frames can be fixed or variable size. In the first, there is no need to define the boundary of the frame; in the second, we need to do so.

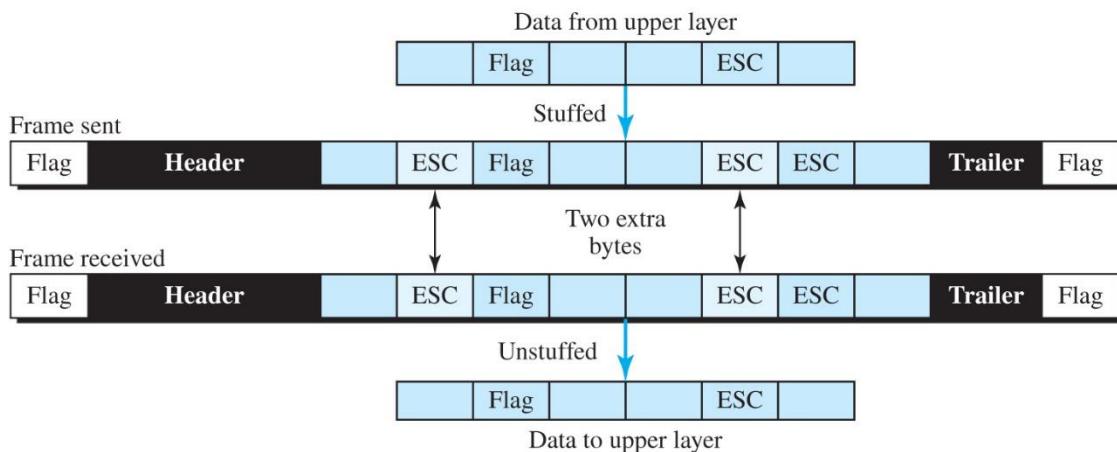
Character-Oriented Framing

- In this type of framing, data to be carried are 8-bit characters.
- In this type of framing, we need to do byte-stuffing to prevent a special character to be interpreted as beginning or end of the message.



بعض بروتوكولات ال data link layer بتحب تشوّف الفريم bytes وبسموها ال character oriented framing، وفي بروتوكولات بتحب تشوّفها bit by bit وبسموها bit oriented framing، الشنتين بعملوا stuffing، بس ال character oriented framing بعملوا stuffing، أما ال bit oriented bytes ← stuffing ال بعملوا bit oriented bytes.





الـ **data link layer protocols** (زي الكلمة المحفوظة بلغات البرمجة)، والـ **byte** هو معين يستخدمه الـ **data link layer** كإشارة على بداية الفريم أو نهايته.

أول اشي بتطلع على الـ **user data** هل فيها اشي حساس؟ هون عنا 2 حساسة، الأولى الـ **Flag**. بس هو بالنسبة اله عبارة عن **user data** طبيعية، مش بداية أو نهاية فريم، وفي كمان **ESC**.

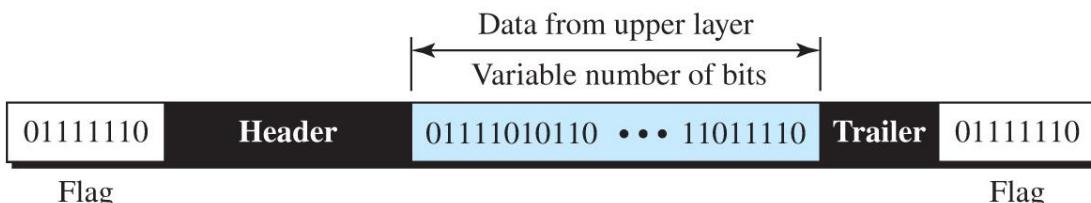
يُجَيِّبُ الـ *data link layer* قبل الـ *flag* بـ *ESC* (دائماً الحشوة قبل)، وعند الـ *ESC* الثانية بعمل نفس الحركة، الـ *ESC* إلى عم بدخلها مختلفة عن الـ *ESC* الموجودة الأولى (إلى بالأزرق الفاتح) حشو أما الثانية (إلى بالأزرق الغامق) *user data*، وبعدها بـ *header* و *flag* البداية والنهاية وبنزل الرسالة على الشبكة، بتوصيل الـ *next* و *trailer* *header* *destination* *hope* *next* *unstuffing* *unstuffing*، بعد ما تشيل الـ *ESC* الأولى (إذا في *flag* أو لا *ESC* بعدها أو *stuff*) إذا في *ESC* (إذا في *Flag*). *ESC* بعدها الأولى.

- ولاحظوا انه ال user data كان حجمها 6 byte بعدها 6 byte stuffing صار ما عملنا .8 byte

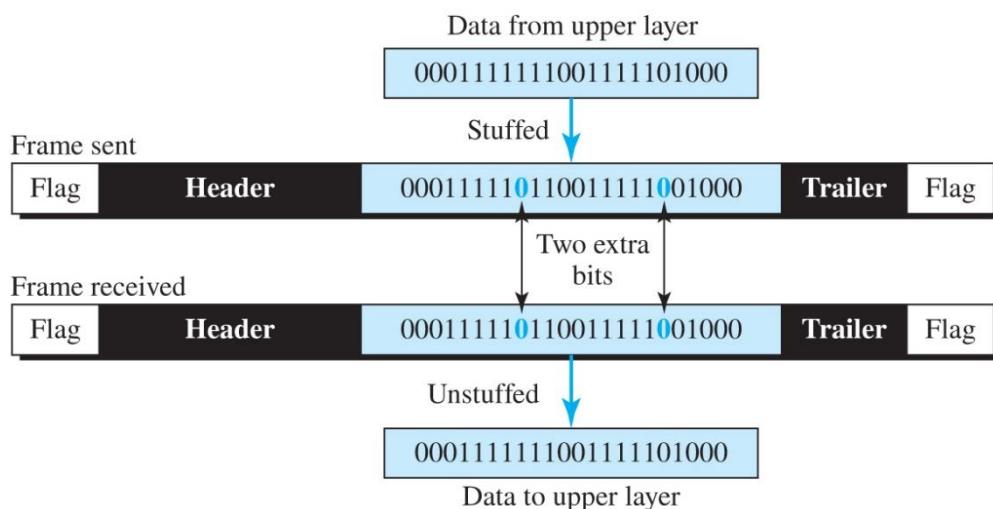


Bit-Oriented Framing

- In bit-oriented framing data is a sequence of bits.
- To separate one frame from another, we normally use an 8-bit flag (01111110).
- To prevent that a byte to be interpreted as a flag, we do bit stuffing.



بال **bit oriented** في نفس المشكلة بس بحلوها باستخدام ال **bit**.
 هون بتتشفوف الفريم 0 و 1 . **flag** البداية والنهاية 01111110 ones (6). هاد ال pattern ممكن يظهر ضمن بيانات اليوزر.



قبل ما نضيف ال **header, trailer, flags** . بنشوف هل عندي 5 ones . إذا لقيت بضيف 0 (وهون الإضافة بتكون بعد) ، وبعدها بحط ال **header, trailer, flags** . لما توصل ال **destination** بده يشيك هل معمول stuff أو لا مشان تشيله، بدوّر على 5 وحدات وال **bit** السادس رح يكون 0 وبتشيله.



Error Control

- Error detection and error correction.
- It allows the receiver to inform the sender of any frames lost or damage in transition and coordinates the retransmission of frames by the sender.

كثير مهم انه كل hope على الطريق قبل ما نوصل لل destination تشيّك على الفريم من ناحية ال error تاعه، تتأكد هل ال frame سليم أو مضروب، يعني ما بدننا ننقل فريم على مستوى الشبكة كلها وأغلب فيه كل الراوترز ويأخذ دور و resources مشان اكتشف بالأخير انه كان corrupted، من البداية أول ما بيبي انه هاد الفريم تالف إذا ما بقدر أصلحه بعهمله، عادي لو أهملناه لأنه تالف ولأنه ال layers الثانية بتعالج موضوعه.

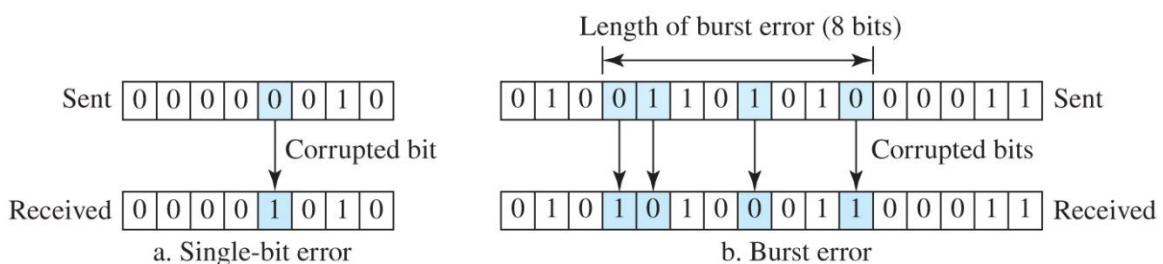
المهم أكثر من ال error correction هو ال error detection اي اكتشف وين الخطأ لأنه مش دايماً بقدر أعرف انه في خطأ ، يعني لما ال error detection algorithm يحكيلي انه هاد الفريم سليم ، مش بالضرورة يكون صح لأنه الفحص الي بيعمله غير قادر على اكتشاف كل أنواع الأخطاء، تكون مصمم على اكتشاف حالات معينة، بس لما يحكيلي انها خطأ فهي أكيد خطأ.

Types of Error

- Single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.
- Burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

لو كنت بتطلع على الداتا كل byte الحال وكان عندي bit واحد فيه خلل تكون عندي single bit error، وهون تكون تصليح الخطأ سهل لأنه رح يكون ال bit يا 0 أو 1 فإذا احنا عارفين الخطأ بس بقلبه وبنحلل الموضوع.

أما ال burst error المتشكلة بتكون ب 2bits أو أكثر إذا ما بنعرف شو الداتا الي رح نستلمها رح نفوت بالتحذير (مثلاً كان الخطأ ب 00، كيف بدبي أصححه هل هو 01 أو 10 أو 11) فهو أسهل اي أعمله drop.



- بالحالة a في عندي 1 byte وبنلاحظ انه كل الداتا سليمة ما عدا الي بالأزرق هو الوحيدة التالفة، هون احنا عارفين ال sent و received داتا فقادرين حكم إذا هاد ال bit مزبوط أو لا، وبنلاحظ انه علاجه سهل.

- أما الحالة b بنلاحظ هون انه الرسالة أطول، ولو قارنا كل bit رح نشوف انه عنا 4 bits فيهم أخطاء معناته هي burst error، هون احنا عارفين ال sent, received data فقادرين حكم.

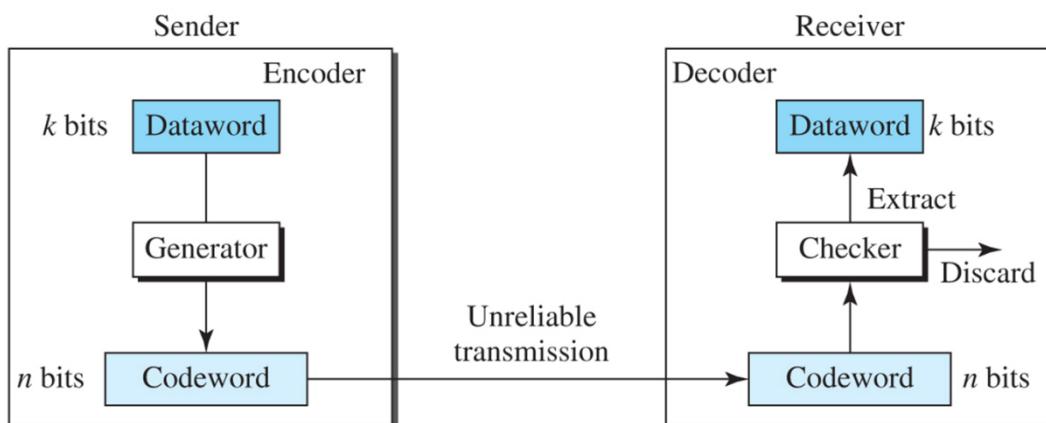
- في مصطلح مهم بال اسمه burst error، كيف بنحسب؟ عدد ال bits بين أول مكان ظهر فيه خلل وآخر مكان ظهر فيه خلل (المسافة بين أول خطأ وآخر واحد)، مثلًا بمثابة فوق ال 8 bits = length of the burst error معناته انه أنا عندي 8 أخطاء.

Block Coding

- We divide our message into blocks, each of k bits, called data-words.
- We add r redundant bits to each block to make the length $n = k + r$.
- The resulting n -bit blocks are called codewords.

- فكرته انه نستخدم مبدأ ال redundancy (أحط اشي extra) مشاناكتشف الأخطاء.
- بجيب ال binary string الي بدي أبعتها وبقسمها لوحدات متساوية بالطول رح نسمى الطول K . بعدين بنأخذ كل وحدة منهم وبنعمل append بنزلق معها extra bit، ولازم تكون مقررين كم عددهم، فالرسالة الجديدة بصير طولها n -bit. ال block الأصلي بنسميه .codewords أما الجديد data words

- ال destination يوصله ال codewords، وظيفة ال destination انه يقرر هل هاي ال data سليمة أو لا، إذا كانت سليمة بنتخلص من ال r bits وبنتخلص ال codewords منها، وبسلمهما لبقيه ال word processing.



بالرسمة الـ *encoder* تكون عنده k اي طولها k bit، وبجيب الـ *generator* وبفصللها عدد من الـ r bits وبلزقهم فيها وبطلع منها *checker* وبتوصيل الـ *next hope* زي ما هي (كوحدة وحدة) على *codeword* عكس الـ *generator* وظيفته يشيك عليها ويشفوف هل رح تمر أو لا، إذا حكى رح تمر بنعمل *extraction* بنزيل الـ r bits وبكملي، إذا حكى انها خطأ بعمللها *discard*.

Example

Let us assume that $k = 2$ and $n = 3$.

<i>Datawords</i>	<i>Codewords</i>	<i>Datawords</i>	<i>Codewords</i>
00	000	10	101
01	011	11	110

- 2 ومadam $n = 3$ معناته $r = 1$ ، يعني رح أقسم الرسالة كل 2 bits مع بعض والـ *generator* رح يزيد bit واحد.
- مادام رح أقسام الداتا تبعتي ل 2 معناته رح يكون عندي 4 *datawords* (00 أو 01 أو 10 أو 11) فالـ *generator* بضيف bit واحد - هو بقرر شو 0 أو 1 - الـ bit الإضافي دائمًا يكون أقصى اليمين، الي رح ينطلق عبر الشبكة هو الـ *codewords* وطولها هون 3.
- فأنا عندي *binary string* طوله 3، ففعليًا عنا 8 احتمالات الله (من 000 إلى 111)، 4 منهم بس الـ *checker* رح يعتبرهم مقبولين وبقدر يرجعهم *dataword* ، الـ 4 الآقيين بما انه ما الهم مكان بالجدول رح يكونوا *corrupted*.
- يعني بنقدر نحكى انه تكون عنا 3 احتمالات:
 - انه أستلم *codewords* صحيحة وهي فعلًا صحيحة وأفهمها وأطلع الـ *datawords* منها.
 - أستلم *codewords* مش موجودة بالـ *dictionary* فبتكون أكيد غلط وبنهملها.
 - أستلم *codewords* صحيحة وأقبلها بس هي فعلًا غلط (هي تحولت من شكل صحيح لشكل ثاني صحيح) فالـ *error detector* ما بقدر يشفوف هاد الخطأ.

Example

The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it. (الحالة الأولى)



The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded. (الحالة الثانية)

The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable. (الحالة الثالثة)

Hamming Distance

- The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits.
- The Hamming distance can easily be found if we apply the XOR operation (\oplus) on the two words and count the number of 1s in the result.
- Note that the Hamming distance is a value greater than or equal to zero.
فكرته انه بنجيف يكونوا بنفس الطول، إذا ما كانوا بنفس الطول ال hamming distance يكون
- مشان نقيسه بتحط ال 2 binary strings تحت بعض، وبعد كل bit مع ال bit الي مقابله هل متساوين أو مختلفين، إذا كانوا متساوين تكون ال distance بهاد ال bit = 0، إذا كانوا مختلفين ال distance بتزيد 1 (زي أنه counter).

Example

Let us find the Hamming distance between two pairs of words.

- The Hamming distance $d(000, 011)$ is 2 because $(000 \oplus 011)$ is 011 (two 1s).
- The Hamming distance $d(10101, 11110)$ is 3 because $(10101 \oplus 11110)$ is 01011 (three 1s).

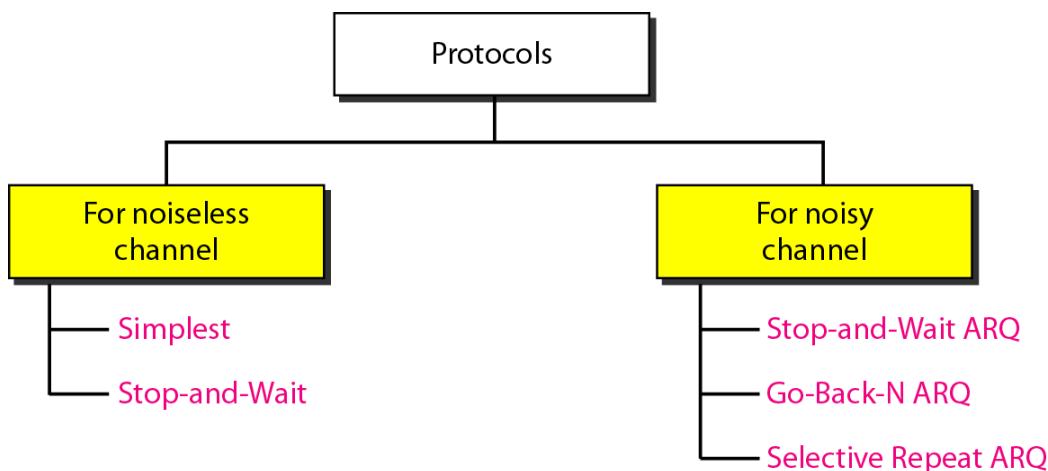
*للذكير ال XOR في حال كانوا مختلفين بتعطيني 1 وإذا متشابهين 0.

After finishing all issues related to DLC sublayer, we discuss two DCL protocols that actually implement these concepts: **HDLC** and Point-to-Point.

HDLC (High-level Data Link Control): A bit-oriented protocol for communication over point-to-point and multipoint links. It implements the stop-and-wait protocol.



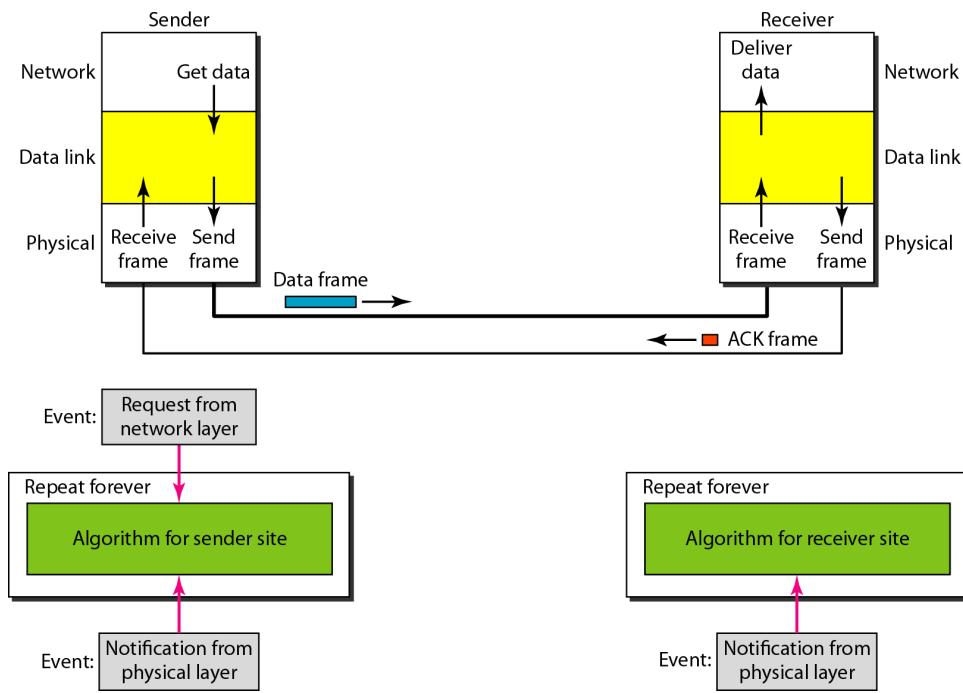
- حكينا من قبل انه ال data link control sublayer فيها 3 شغلات framing, error control, flow control . حكينا عن ال framing و ال error control ضل علينا المصطلح الثالث واي هو flow control ، الي بدنى نعرفه بس بهاد التشابتر عنه ، انه ال data link next hope layer بتعمل flow control ، شو الهدف منه؟ احنا بنتطلع على ال hope و ال next hope مثلًا ال sender و ال switch الي وراه، ال sender بضملي انه ال next hope وال sender سرعتهم متقاربة، يعني ما يكون ال sender عم ببعثت وال next hope مو مستوعبة الداتا، والاشي الثاني ال **ACK acknowledgement** أنا لما ببعثت لـ **frame** (Ack) ممكن أعملها **discard** (الي حكينا عنه فوق) كيف ال sender رح يعرف الي عملت **flow control protocols**؟ ال **discard** هي الي بتبلغه.



ال **flow controls protocols** تم تقسيمها لتصنيفين (مشان يسهلوا الدراسة)، اشي لـ **noisy channel** واشي لـ **noiseless channel**

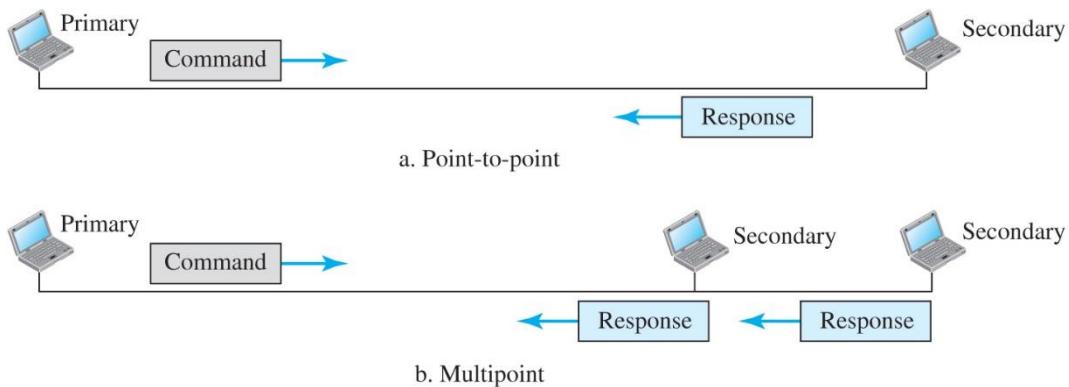
فعليًا مافي اشي بالحياة اسمه **noiseless channel** (كل ال channels noise) بس عشان يفهمونا ال **protocols** فكفروا الأفكار تبعته، فاعتبروا انه مافي noise وانه الداتا بتوصل دائمًا وبس بدنى نضبط السرعة انه ما يكون ال **sender receiver** أسرع من ال **sender receiver**. وعملوا **protocols** ال **simplest + stop and wait** هي بروتوكول غير قابل للتطبيق بالحياة الواقعية لأنه بتفترض انه الداتا ما بتضيع وانه ال **sender + receiver** سرعتهم متناسقة وما عنا مشاكل، وال **stop and wait** كمان لا يطبق بالواقع بس فكرته انه ال **sender** ببعثت فريم لـ **next hope** وبستناها تعمله **check**. فال **sender** بشغل عداد وبضل يستناها إذا طفى العداد وما اجت ال **acknowledgement** بعتبرها ضاعت أو وصلت مضروبة (يعني ببعثت وبستن)، تخيلوا مسجات الواتس وبدنا نبعث رسالة وما بزبط نبعث الثانية غير لما ينرد على الرسالة تبعتنا، فهو فعليًا اشي مش عملي أبدًا.





- بالـ stop and wait البدائي بفترضوا انه دائمًا اـ ACK رح تيجي حتى لو طولت ومستحيل تضيع(فبضل يستنناها لحد ما تيجي).
- لاحظوا بالرسمة مافي كلمة timer لأنـه بدائي.
- بالـ ARQ زي ما حكينا بشغللها عداد وفي حال ما اجـت بضـيعـها.
- بالـ selective repeat ARQ و go back N ARQ لـ 10 لـ بينـ ما تـيجـي اـ ACK، وإذا بـعـتـ اـ 10 ولـساـ ما اـ جـاـ رـحـ يـعـمـلـ retransmission والـ فـرقـ بينـهمـ بهـايـ النـقطـةـ، وـرحـ نـحـكيـ عـنـهـ لـ قـدـامـ.

Normal response mode



- لما يكون الليـنـكـ point to point وأـبـعـتـ com~mandـ علىـ الـ other pointـ لأنـهـ فيـ بـسـ sender + receiverـ واحدـ.
- بالـ multipointـ فيـ عنـديـ أـكـثـرـ منـ حـدـاـ فـ رـحـ يـجـيـنـيـ res~ponseـ مـنـهـمـ، مـمـكـنـ يـكـونـ مـنـهـمـ كـلـهـمـ أوـ مـنـ جـزـءـ مـنـهـمـ (صـبـ أـنـاـ شـوـ بـدـيـ).



Asynchronous balanced mode



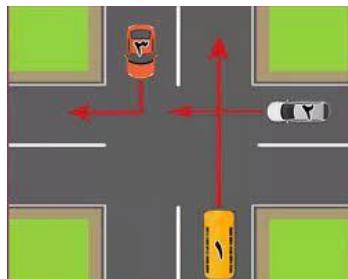
- هون في اشي اسمه ال piggybacking، أنا بدي أبعث رسالتين بدل ما أبعثت 2 frames واحد فيهم يكون response لاشي سابق وواحد command لاشي لاحق بدمجهم مع بعض بفريم واحد وبس بلعب بال flags الي فيه، فهيك بخلي الفريم يخدم غرضين ، وهيك ما بضطر لكل فريم أستنى ال ACK.

Media Access Control (MAC)

- بال بكون في Sender بده يبعث داتا وفي node بدها تستقبله ، وبنفس الوقت في sender ثانى قرر يبعث داتا، في حال كنا محظوظين الأول بكون مأخذ قناة خاصة فيه والثانى قناة ثانية ، ولما يبعثوا ال frames كل واحد يبعثها على موجته الخاصة وما بكون في مشاكل، بس لو كنت باستخدام wireless transmission أو ما كان في noise بهاي الحالة ممكن لما الاثنين يبعثوا ال frames يتداخلوا الموجات ويصير عندي هون بصير في تصادم .

مشان نقرب الفكرة أكثر خلينا نشوف هاد المثال

- في اشي اسمه التقاطع المتكافئ (زي الي بالصورة)، مافي عليه أولويات ف كل السيارات بتكون متكافئة، بالسواقة في دور معين الناس بتلتزم فيها



مشان يمرقوا بعض (protocol)، إذا الناس التزمت بالدور كل السيارات رح تمثي بدون تصادمات، وإذا لأ رح تصير الحوادث، يعني الناس بتكون متربوكة لاحترامها للقانون، بس في مرات بكون في شرطي سير على التقاطعات الحساسة هو الي بتحكم فيها (بس مش دائمًا بكون في)، الي بعمله الشرطي انه بسّكّر مسرّب وبفتح مسرّب، فلما يكون موجود رح تخف التصادمات.

Random Access: No station is superior to another station and none is assigned the control over another.

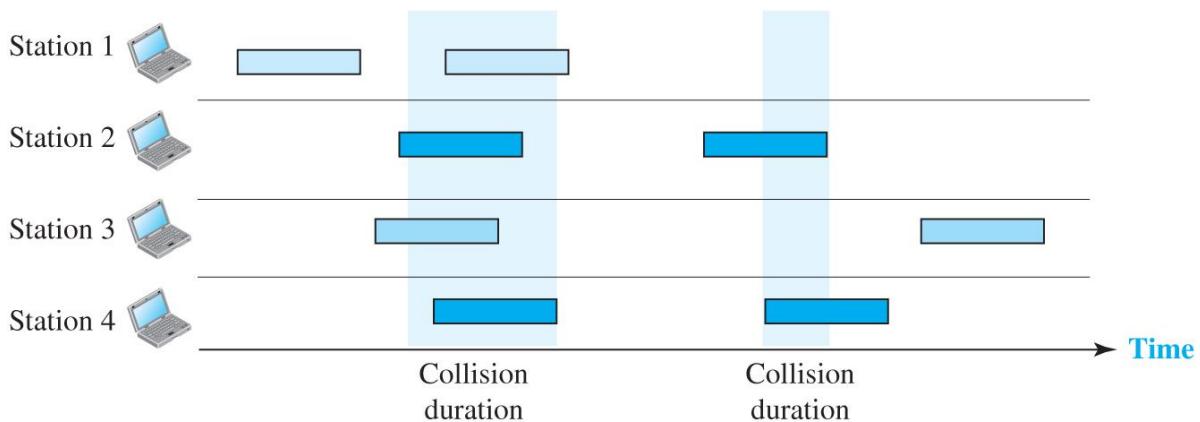
- ال random access نفس فكرة المثال الي فوق بدون شرطي، أما ال control access هي مع شرطي.



Aloha

- The earliest random access method, was developed at the University of Hawaii in early 1970.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

ال Aloha نوعين أول واحد ال pure، هي "سبهلهة" بتنزل الفريم بال shared media يا بجيبي ACK ووقتها بتكون الفريم تبعتي وصلت وببعت الفريم الي بعده، يا إما ما بجيبي وبدنا نعيدي ال transmission فبنستنى شوي وبنرجع نبعته ويابوصل أو ما بوصل، بكون معي عدد محاولات معين، وبضل أعيدي لحد ما تزبطة، وإذا استنفذت عدد المحاولات بشوف ال network layer إذا ممكن تلاقيلي path ثانية، أو ممكن تنحل بأكثر من طريقة.

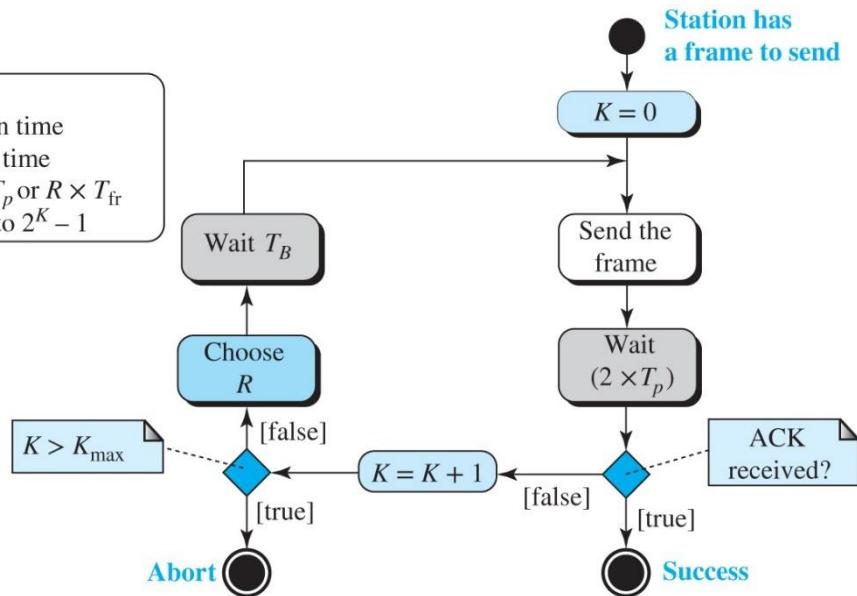


هون مثال على Frames in a pure ALOHA . عندي ناس بشتغلوا على 4 stations ، الأول رمت ال frames وال الثلث الثانيين كانوا نايمين فبمسنوا الفريم عادي، ال station الثانية كلهم صحبو مش كلهم بلشوا مع بعض - بس تقاطعوا - المستطيل الأزرق الي متقاطعين عنده هاد ال transmission delay الي حكينا عنه من قبل (بحمل الفريم عالشبكة وفي حدا ثاني عم بحمل معي)، هون بصير في تصادم، هون ال 4 frames رح يصيروا noise وما رح يوصلوا ، شو الحل؟ ال Aloha بتحكي إذا صار في تصادم وفشل انه بيعت الفريم استنى شوي (الانتظار هاد يكون بعشوائية لأنه إذا كلهم استنو بنفس المدة الزمنية رح يصير نفس السيناريyo)، حسب الرسمة station الثالثة خلص مرقت، بس 2 و 4 رجع صار في بينهم تصادم فبرجعوا يستنو كمان مرة ..



Legend

K : Number of attempts
 T_p : Maximum propagation time
 T_{fr} : Average transmission time
 T_B : (Backoff time): $R \times T_p$ or $R \times T_{fr}$
 R : (Random number): 0 to $2^K - 1$



أول اشي في عندي counter اسمه k رح يعدلني عدد محاولاتي (K_{max}) هي أقصى عدد للمحاولات، يتم قياسها حسب تجارب)، ببعت الفريم (بتستهلك مدة زمنية مقدارها ال $* transmission delay$ لحد ما ينزل كل الفريم عالشبكة، بعدين بستنى ال ACK (بستنى 2 $\times propagation delay = T_p$ (T_p \times K \times $frame_length / bit_rate$)).
 الضعف؟ الموجة رح تقطع مسافة متيرية عبر الوسط (وقت للفريم يوصل على $next hope$ ، وقت للرد لحتن ترجع عندي) ، في حال وصل بتكون أمرورنا تمام برجع مرة ثانية بصفر العداد وببعت الفريم الي بعده ، وفي حال بعد الفترة الزمنية هاي ما وصلت بكون فشل ورح نحاول مرة ثانية بس بنزيد على العداد k واحد وبتشيك هل تجاوزت ال $max range$ أو لا، في حال تجاوزت بكون استنفذت محاولاتي وبرفعه لل $layer$ الي فوق، إذا ما تجوزنا ال $max range$ (عبارة عن عدد صحيح بمثيل رقم عشوائي بكون محصور ضمن ال $range$ (back off time) T_B) وهي عباره عن ضرب ال R ب ال T_p أو T_{fr} .
 كلما زادت K كلما كان احتمال انه الاثنين يختاروا نفس ال R أقل (يعني تصدامات أقل).

للذكر*

$$\text{transmission time} = \frac{\text{frame_length}}{\text{bit_rate}}$$

$$\text{Propagation delay} = \frac{\text{distance}}{\text{medium_speed}}$$



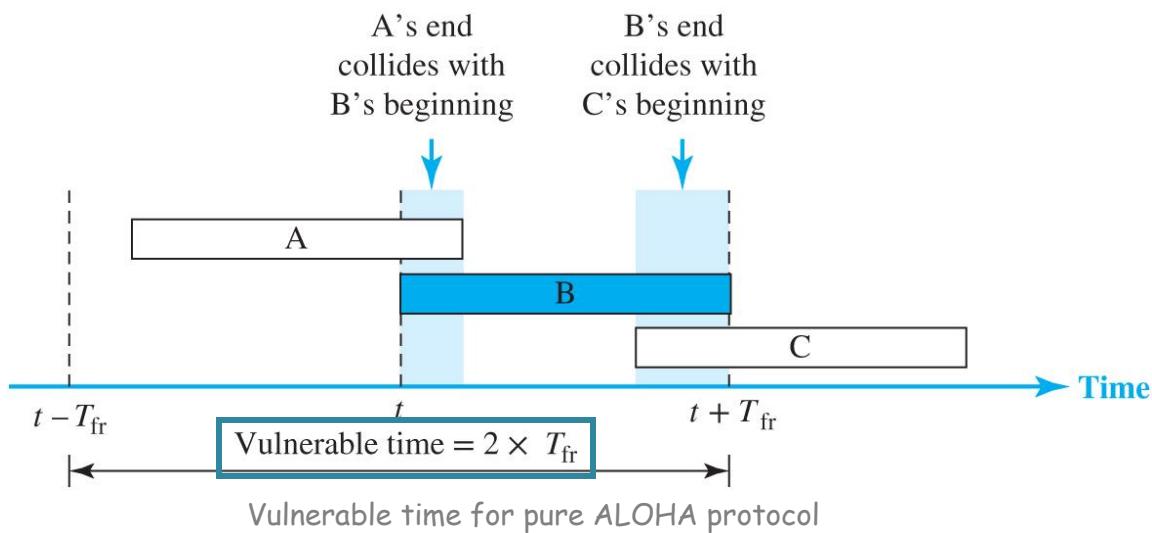
Example

The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s, find T_p .

$$T_p = (600 \times 10^3) / (3 \times 10^8) = 2 \text{ ms.}$$

For $K = 2$, the range of R is $\{0, 1, 2, 3\}$. This means that T_B can be 0, 2, 4, or 6 ms, based on the outcome of the random variable R .

- . أعطاني أقصى مسافة متيرية = 600 ، ومadam مسافة متيرية يعني propagation delay .
فالافتراض يعطيني سرعة انتقال الموجة بالوسط، ولو ما أعطاني اياه فهي فحتكون سرعة الضوء .
- . حسبناها عن طريق قانونها 2^k - R



- . ال vulnerability معنها المدة الزمنية الي لازم يمتنعوا الآخرين فيها عن عمل ال transmission عشان الفريم تمشي .
- . بال pure ALOHA الفريم تبعي مهدد من ال sender الي قرر يبعث الفريم تاعه وما كان مخلص لما أنا قررت أبعثت (هو بليس يبعث قبلي وما خلص وأنا بديت) فهوون رح نتصادم مع بعض، وفي كمان خطر من الي قرر يبدأ بعد ما أنا بديت، فهون أنا بدتي 2 transmission delay ميشان أضمن أنه الي قبلني والي بعدي ما يؤثروا علي، المدة الزمنية هي طول هاي المدة ما حدا رح يبعث عشان هيكل ال pure ALOHA مش كفؤة.



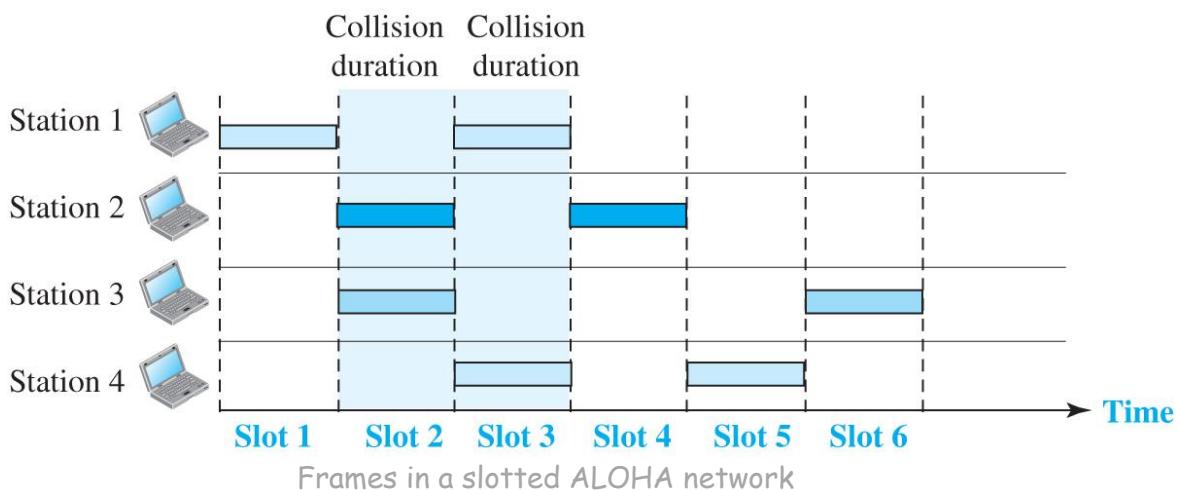
Example

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

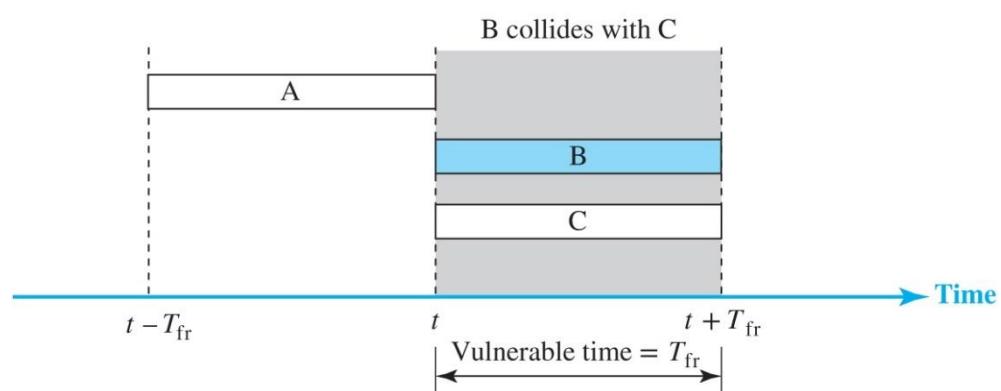
Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms.

The vulnerable time is $2 \times 1 \text{ ms} = 2 \text{ ms}$. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the period (1 ms) that this station is sending.

• transmission delay = 200 bit معناه هو بفکر بال - طول الفريم



النوع الثاني من ال ALOHA هو ال Slotted ALOHA ، فعليًا هي pure ALOHA مع تعديل، الوقت يقسم إلى slots ، كل slot طوله = 1 transmission delay = 1 node . وبحكي لـ لـ ALOHA وتبعي الفريم لازم تستني لبداية ال slot ، ممنوع تبعي بنص أو آخر ال slot . طيب وين الخطأ؟ لما حدا يقرر يبعث معه بنفس ال slot ، هون delay كامل راح، لأنه عمل معه تصادم.

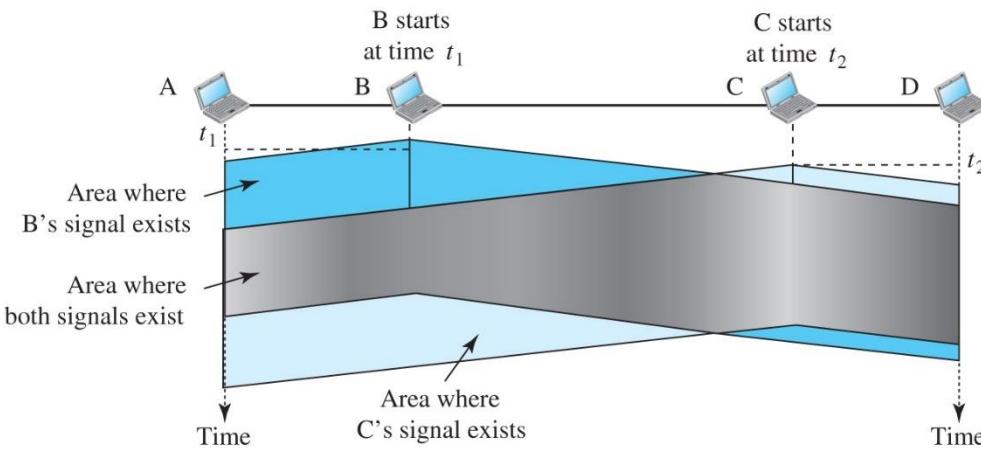


- بالشكل فوق، الـ T_{fr} vulnerable time = T_{fr} لأنه بطل في مشكلة من إلى قبل أو إلى بعد المشكلة بس مع إلى بيعت معه بنفس الـ Slot.

Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

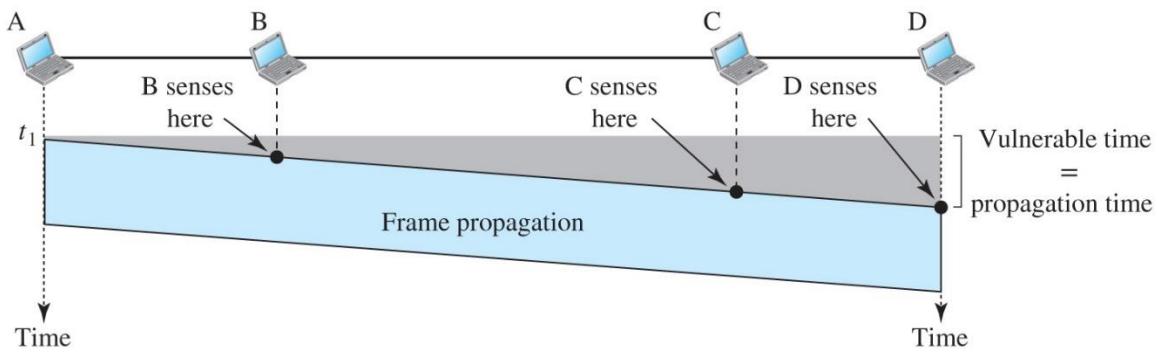
- مجموعة من البروتوكولز المحسنة عن الـ ALOHA، اختصار فكرته هي "sense before transmit" or "listen before talk". انه أنا قبل ما أبعث ما أبعث الفريم لازم أحاول أعمل sensing على الميديا وأشوف هل في موجة موجودة بغض النظر إذا طبيعية أو موجة noise، إذا في موجة شغالة معناته في حدا عم بعمل transmission وأنا بمتتنع عنه، إذا مافي حدا بعمل transmission عطول بيعت.



- لو اجتنا هاي الرسمة بالامتحان عطول لازم نعرف انها CSMA لأنه بستنى بعدين بعمل ما بعمله عطول، مثلاً node B ما بتبلش مباشرة frame على هيئة signal فالموجة تاعته بتنطلق على كامل الكيبيل، ما بتاخذ نفس الوقت عشان توصل لـ A or C or D لأنه بدخل الـ propagation delay، أنا ما بعيت إلا لما تأكدى انه الميديا فاضية، بس بعد ما أعمل ما بعيت ما بعمل transmission موجتي لازم تاخذ propagation delay منشان توصل لكل الناس الي عالكيبيل.
 كل مجموعة bits بتركب موجة والموجة بتنطلق، سواءً كانت analog or digital.
 بالنسبة لـ C كمان كان بده بيعت، فلما عمل sensing بالأول تأخر شوي ما عمل مباشره بالمقابل
 لأنه عارف انه B عم بيعت، فهو بالنسبة الله لما كان عم بعمل transmission



المفروض، الميديا تكون فاضية ، فتجنبت اني أتصادم مع حدا بسبب ال transmission فصار في propagation delay ، الموجة تاعت B رح تحتاج مدة زمنية أكبر من 0 عشان ترحل عبر shared media ، بعد نقطة معينة رح تصطدم بموجة ثانية لأنه كمان الموجة هاي عم تعمل propagation فهو صار في تصادم . يعني بال CSMA التصادم بصير بسبب ال propagation delay مش بسبب ال transmission delay .



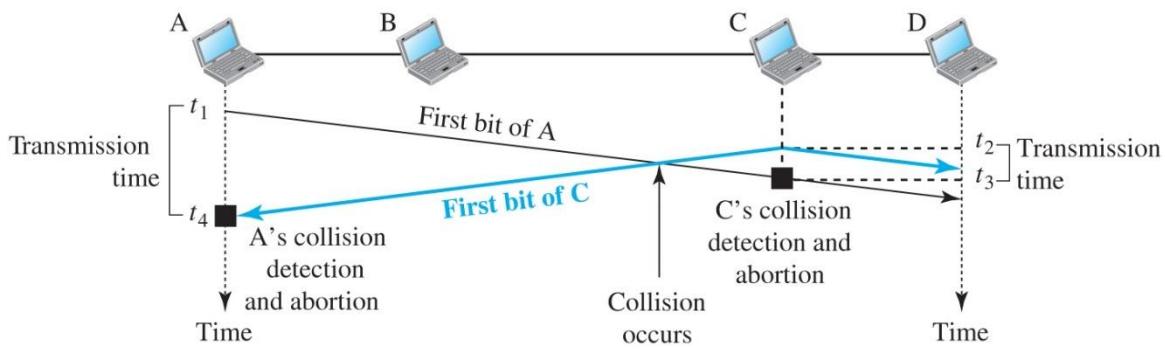
ال propagation delay بيأخذ وقت، لاحظوا بالصورة وفلنفترض انه A الي عم بيعت، t_1 من أول ما بلشت الموجة بلش ال propagation ماشي وما بيوصل عند D على خط أفقى بينزل الخط لي؟ لأنه لازم يمر وقت عشان الفريم يوصل، ال propagation delay قيمة لا تساوي صفر حتى لو كانت صغيرة، فطالما الفريم تبعي عم بعمل vulnerable time = propagation time هو محدد انه يصير عليه collision عشان هيكل ال propagation time تاعده ما فعشان أضمن انه الفريم تبعي يصل لازم أضمن انه خلال ال propagation time تاعده ما يكون في موجة ثانية عم تعمل propagation وإلا رح يصير في تصادم و noise signals . المشكلة بال CSMA انه ما بحكيلي شو أعمل لو صار collision . بس بقلي إذا في حدا عم بعمل transmission لا ت عمل transmission استنى ، ولما يخلص بنعمل، ولو صار collision؟ عشان يجاوبوا عالسؤال صمموا عائلتين:

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

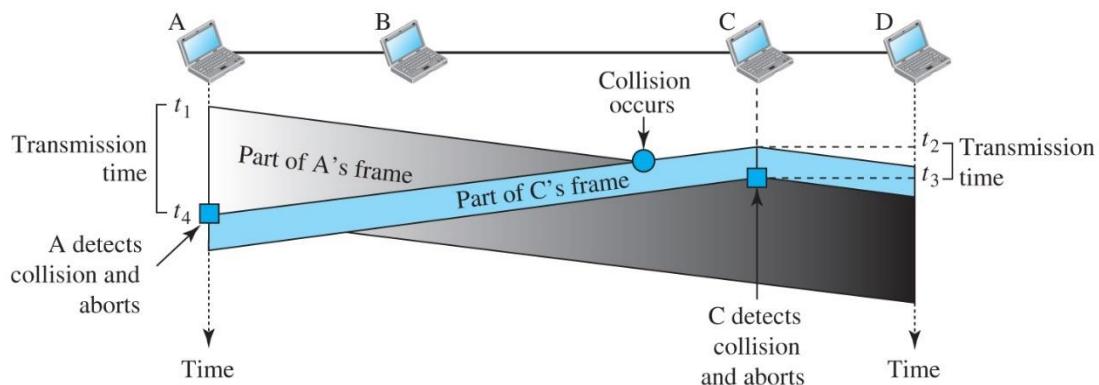
- The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

بتنظر ال collision يحدث وبتصرف .
بال wired LANs زي الي يستخدموا ال twisted pair ما بتكون المسافات كبيرة، ال .Collision Detection مش كثير بتحدث فبيستخدموا ال collision



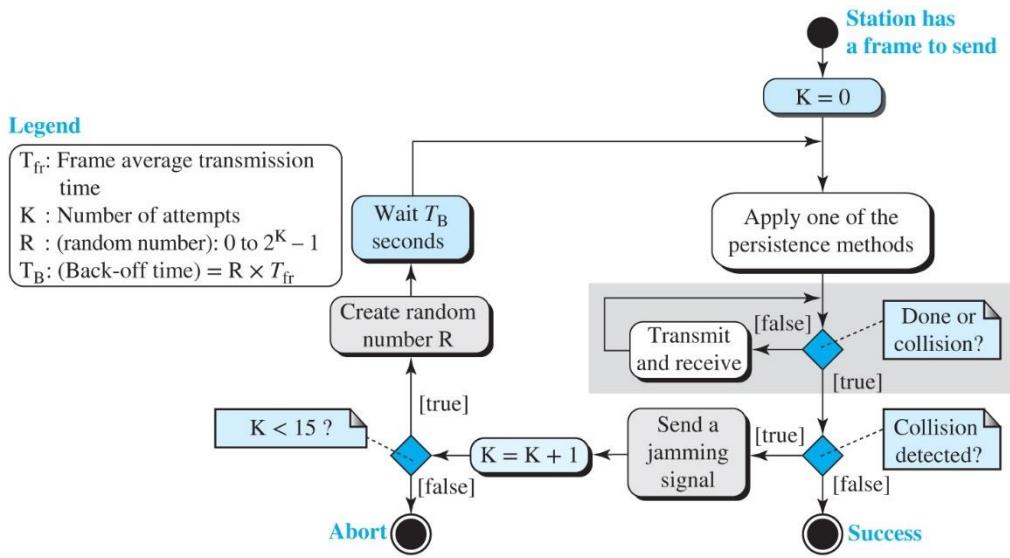


- بده يحكيلى انه أول bit من رسالتك إذا اصطدم خلص كل الباقي بروح.
 - بهاي الرسمة + A + C عم يبعتوا وفي تصادم بينهم ، A التزمت بالبروتوكول استنت لبين ما
 صار ما في حدا بعمل transmission وعملت، وموجتها من أول ما عملت
 عملت propagation فهي أمرها تمام، C استنتها لخلصت transmission ونزلت موجتها،
 وحصل اصطدام ، ال C عند detection وعملية إرسالة الفريم فشلت لما
 كان 3 time ، أما A عرف عن ال collision لما كان الزمن 4 ، عشان أعرف انه صار
 لازم الموجة الي نتجت عنه تعمل propagation لعندى (زي لما يصير حادث سير السيارات
 بتعرف انه في من التصادم وانه الطريق مسکر، السيارات البعيدة ما تكونوا شايفينه بس
 بتوقعوا انه فيه)، فهوون نقطه C كانت قريبة على نقطة التصادم فعرفت بسرعة لأنه ال
 عملت noise signal على أنها أسرع (بتعتمد على المسافة المتيرية وسرعة
 الضوء) لأنها أقرب، أما A تأخرت لعرفت لأنه الموجة قطعت مسافة متيرية أكبر، يعني
 بالنهاية كلهم بعرفوا بس مش بنفس اللحظة الزمنية.



- هاي الرسمة انعكاس للي قبلها، بس بدل ما تكون على مستوى bit واحد على مستوى جزء
 من الفريم، نفس الاشي والنتيجة وحدة.





. $15 = k_{max}$ -

الي بصير من البداية اشي اسمه apply one of the persistence methods يعني you listen before you transmit . لو عملت listen ولقيت انه هاي الميديا مشغولة شو

بعمل؟ الحل هو persistence methods ، في ناس بضلهم يزتووا ، وفي ناس باخذوا sleeping time بعدين برجع بشيك، إذا كانت النود شابكة على كهرباء عادية ما عندها مشكلة تضل تشيك، بس إذا كانت wireless وبطاريتها limited مش منيح تضل تشيك لأنه بسحب من البطارية فباخذوا sleeping time بعدين برجعوا بحربوا حظهم بعد شوي وهاد هو ال persistence methods ، الي بهمنا انه رح نستنى لحد ما الميديا تصير free. شو بعمل لبين ما تصير free مش مهم ، بعد ما أعدّي من هون معناها انه الميديا صارت free، ال transmission تكون عن loop ، لأنه واحدنا بنعمل transmission نسمع هل ال signal الموجودة على هاد ال channel هي نفسها الي عم بيعتها أو لـ ، إذا سمعت غير الي عم تطلع منك معناهه صار collision وبنكون نسمع noise و signal غريبة ، فهوون الموضوع ما بعتمد على ال ACK . رح أستنى مدة زمنية كافية انه أعمل transmission والموجة تاعتي تعمل next hope لل propagation

إذا قطعت هاي المسافة بسلام بفترض انه الفريم تاعيوصل. إذا خلل ال transmission سمعت اشي مش طبيعي رح أعرف اني فشلت بإرسال الموجة تاعتي وبفترض اني لازم أعمل retransmission مرة ثانية، بعدها كسرنا ال loop وطلعنـا معناها يا إما خلصنا وما سمعنا أي noise فخلص تكون success ، أو كسرنا ال loop وطلعنـا لأنه سمعنا موجة غير موجتنا، بالحالة هاي بنكون فتنا بال collision ورح نفترض انه الفريم تبعنا ضاع وبدى أعمله retransmission قبل ما أعمها لازم أخبر الي حوالي أنه الطريق مش سالك فببعت اشي اسمه jamming signal مشان المناطق البعيدة يوصلها انه اللينك هاد في عليه collision ومأزم، بعدين بضيف على ال K واحد وبشوف إذا لسا معـي محاولات أو لـ، إذا تجاوزـت ال 15 معناها ما معـي محاولات وخلص، إذا لـسا معـي محاولات بكمـل نفس الألـ고ـرـيـثـم تبعـت ال ALOHA . بعمل random number generation وبـضرـبه بـسـ بالـ T_{fr} .

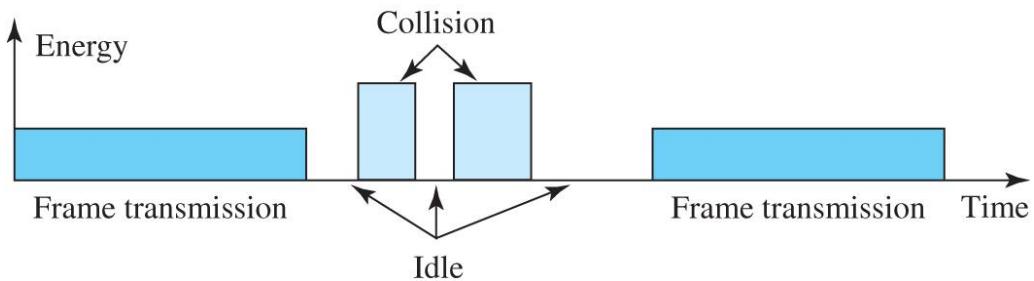


الـ CSMA عادة يطبق بالـ LANs يعني مسافة قصيرة والسرعة سرعة ضوء معناته الـ propagation delay رح يكون صغير كثير وقريب للصفر مشان هيك ما بنضرب الـ T_p بـ R .
 بستنى الـ back of time وبعد ما ينقضي ما برجع بيعت، بعيد من أول بتشوف هل الميديا available وإذا كانت مشغولة كمان بدي أستنى لبين ما تصير فاضية وبعدين برجع بيعت.
 الحد الأدنى لطول الفريم عشان أسمح لحالياً أعرف انه صار collision . خلينا ناخذ **أسوأ الاحتمالات** . لنفترض بدي أبعت لأبعد نقطة، عشان أسمع الـ noise تبعثر noise، لازم الفريم تاعي يعمل propagation لك كل المسافة من عندي لأبعد نقطة عنني ويصطدم هناك والـ noise يرجع كل المسافة عندي، فأنا خطر علي اختيار حجم صغير بخليني أبعت وأطلع من الـ loop وأنا فاهمة أنه ما صار collision وما رح يصير لأنني ما عم بستنى كفاية لحتى أسمع صوت الضربة الي صار، فلازم يكون عندي آلية بتضمن اني استنى كفاية أسمع الموجة تاعت الـ noise وهي راجعة، فلازم يكون الفريم طويل بما فيه الكفاية الي يسمح لأول bit على الأقل يطلع لآخر نقطة بالشبكة ويختلط وتتراجع موجة الـ noise لعندي.

Example

A network using CSMA/CD has a bitrate of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs , what is the minimum size of the frame?

The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2 \mu\text{s}$. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is $10 \text{ Mbps} \times 51.2 \mu\text{s} = 512 \text{ bits}$ or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet, as we will see later in the chapter.



وحدة من الأساليب الي ما بتحبذ انه الـ collision غير انه في إضاعة للجهد لأنه الموجة ضاع عليها فريم ورح نعمل retransmission ، الموجة المخصصة للتصادم بتتميز عن الموجة الطبيعية انه الـ attributes مختلفه ، فهوون الـ node بتصرف طاقة أكبر عشان تعمللها transmission وبستنزف البطارية.



Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)

- Invented for wireless networks.

- بنحاول انه ال collision ما يصير.

- بال wireless احتمال حدوث ال collision أكبر فبنستخدم ال Collision Avoidance . رج

ناخذه أكثر بتشابتر 4

Controlled Access

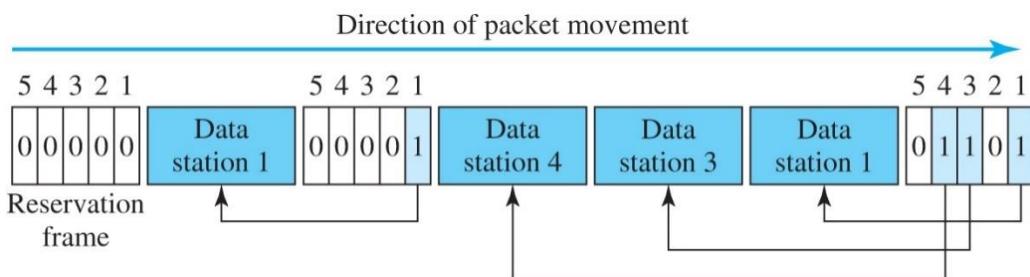
- In controlled access, the stations consult one another to find which station has the right to send.
 - A station cannot send unless it has been authorized by other stations.

هدفهم يمنعوا الـ **collision** من الحدوث من الأساس. كل البروتوكولز الموجدة ضمنهم مبدأ عملها الدورية، في دورية واضحة بين الـ **nodes** وكل نود لما ييجي دورها بتبعه، فلما يكون في دورية وكل نود عارف من رح يبعث ما حدا بتعدا على حدا وبنمنع حدوث التصادم من الأساس (زي لما حكينا عن مثل الشرطي السير لما يكون واقف هو الي بتحكم بالشارع فكل سيارة بتكون عارفة متى رح تمشي)، مش كل الـ **access protocol** تكون **control access** بتكون بحاجة لشرطي، مثل الـ **Reservation** ما بتحتاج بس بتعتمد مبدأ الدورية والكل تكون متفقة عليها.

Reservation

- A station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

مبدأ عملها الزمن مقسم دائماً لمرحلتين أساسيات وبعيدوا نفسهم، المرحلة الأولى الـ reservation frame عادة تكون أقصر بكون فيها اسمه reservation frame محظوظ فيه لكل نود بهاي الـ Boolean flag or bit - shared media . بس يجيها الفريم إذا بتحب تبعن بتحط محل الـ bit تاعها 1 وإذا ما بتحب بتحط محله 0 ، هاد الفريم بلف على الكل والكل بكتب إذا بده يبعث أو لا المرة الجاي وهيك بتخلص فترة reservation وبيتلش المرحلة الثانية الي هي transmission ، الكل عارف مين حيبعث ومين لا وكل نود بعرف متى رح يجي دورها ولما يجي الوقت بيعت الفريم تاعه، فهيك بنمنع حدوث collision ، لأنه ما حدا بيتعت بغير دوره.



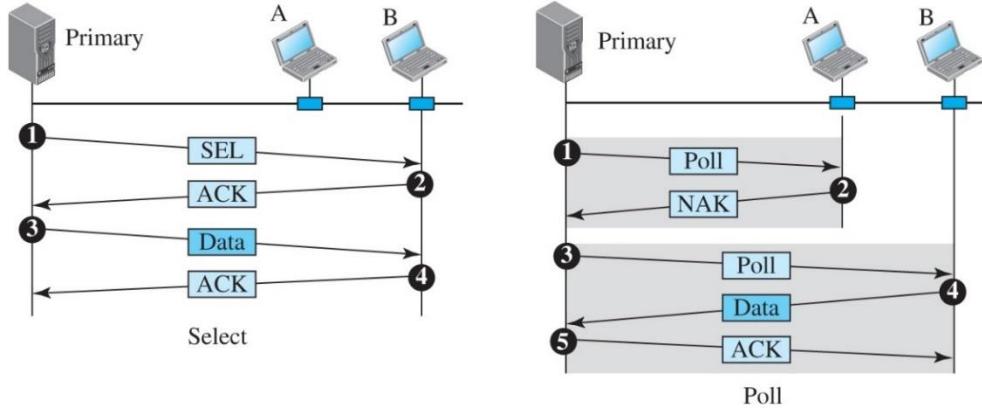
- بالفترة الأولى كان الـ reservation كله أصفار (يعني ما حدا بده يبيعت)، بالفترة الثانية بس واحد بده يبيعت الـ 4 stations ما بدهم، بالفترة الي بعدها 1 و 3 و 4 صاروا بدهم بيعتوا ، بالأول بطلع الفريم تبع station 1 بعدين الفريم تبع station 3 بعدين تبع station 4 (مهم الترتيب مشان الدور). - هون مافي شرطي بس الكل بلزم بدوره-

Polling

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.
- The primary device controls the link; the secondary devices follow its instructions.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.

- هون بنسأل النود بدها تبعت ولا لأ، عشان الـ polling protocols تشتفل لازم يكون في شرطي ينسميه الـ primary (نود خصائصه بتكون أعلى من النود العادي) ، والنود الباقيه تكونوا طبيعين secondary .

- الـ primary مهمته بس تنظيم السير



- الـ polling protocols بصير فيها عمليتين الـ selection + polling protocols ، بعدي الـ select بكون الـ primary مافي حدا ببيعت لحدا الداتا مباشرة ، كل الداتا لازم تمر عبر الـ primary. يعني إذا نود A بدها تبعت فريم لنود B لازم تبعت للـ primary الي بعمل forward لنود B ، وإذا نود B بدها ترد على A رح تمر بنفس الآلية.

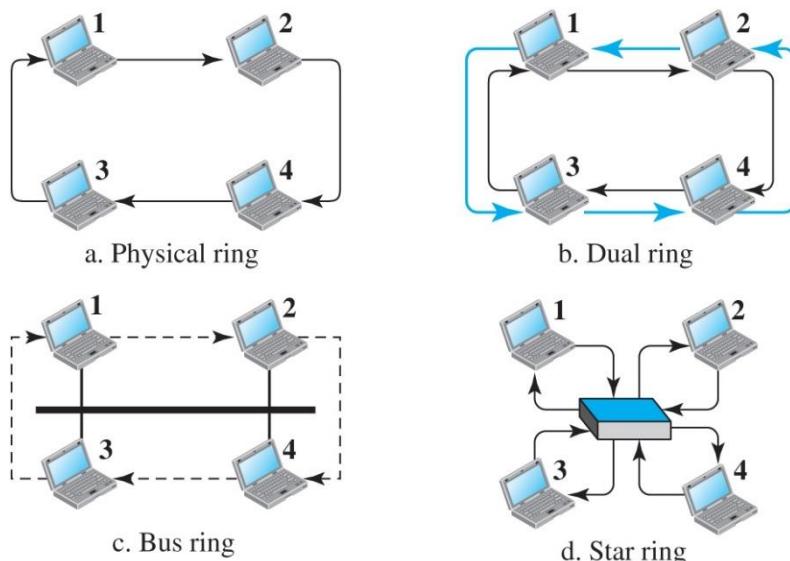
- مرحلة الـ select بكون الـ primary عينه رسالة بده يوصلها لـ B ، فبعمل لـ B (SEL B) يعني بتحكيلها primary بعرف انه عنده داتا رساله بده يوصلها لـ B ، يا بتحكيلي انها جاهزة ACK أو لأ ، إذا جاهزة بضخلها البيانات و B بتحكيله انه البيانات وصلت (دائماً الي بستلم الداتا لازم يعطي ok انه الداتا تمام).



- مرحلة ال poll، ال primary بشفوف كل نود إذا بدها تبعت أو لا ، بالرسمة سأل أول اشي A إذا بدها تبعت (poll)، لازم ترد وتحكيله او لا، هون A حكتله لا (NAK). بروح على الي بعدها بعلتها poll مثـان يشوف إذا بدها تبعت بعدين بتعمـت مباشرة الداتـا (نفس فـكرة ال B piggybacking انه الفـريم يكون نفسـه منه داتـا و ACK) لحد ما B يضـخلـه كل البيانات الي بـده إـيـاهـا . لما ال primary يتسلـم كل البيانات بـيـعـتـ لـ ACK B انه وصلـته ...

Token Passing

- In the token-passing method, the stations in a network are organized in a logical ring.
 - In other words, for each station, there is a predecessor and a successor. The predecessor is the station that is logically before the station in the ring; the successor is the station that is after the station in the ring.
- على فـكرة ال topology controlled access عـنـا ال token passing بـتـعـتمـدـ ال token هو special frame فـاليـ معـهـ ما بـتـسـفـيدـ منهـ ، الـ tokenـ بـقـدرـ يـبـعـتـ والـيـ ماـ معـهـ ماـ يـقـدرـ وهـيـكـ بـضـمـنـ أنهـ وـاحـدـ بـسـ الـيـ رـحـ يـبـعـتـ الدـاتـاـ .



بالرسمـةـ بـدـهـ يـورـجـيـنيـ انهـ مـوـضـوعـ الـ tokenـ مـمـكـنـ نـرـفـعـهـ مـثـشـ بـسـ لـلـ ring topologiesـ الـ physical ringـ بـرـسـمـةـ aـ هـايـ طـبـيـعـيـةـ ringـ وـكـلـ نـوـدـ شـايـفـةـ بـسـ اليـ بـعـدـهاـ وـأـوـلـ ماـ أـحـصـلـ عـلـيـ الـ tokenـ بـيـعـتـ فـرـيمـ وـبـيـعـتـ بـسـ لـلـيـ بـعـدـيـ . الـ Dual ringـ بـرـسـمـةـ bـ نـفـسـ فـكـرـةـ الـ duplexـ اـنـهـ دـاتـاـ بـتـنـدـقـ بـاـتـجـاهـيـنـ يـعـنـيـ أـنـاـ بـاـيـدـيـ tokenـ يـاـ بـيـعـتـ لـلـيـ بـعـدـيـ أـوـ الـيـ قـبـلـيـ وـفـيـ حـالـ كـانـ عـنـديـ tokenـ بـيـعـتـ فـيـ حـالـ مـاـ كـانـ مـاـ بـيـعـتـ .

الـ bus ringـ بـرـسـمـةـ cـ هـونـ الـ topologyـ مـوـ busـ هيـ ringـ . فيـ اـشـيـ رـحـ نـاخـذـهـ بـتـشـابـتـرـ 6ـ اـسـمـهـ الـ Bus LANsـ عـبـارـةـ عـنـ سـوـفـتـوـيرـ بـنـزـلـهـ عـلـيـ مـسـتـوـيـ الـ بـنـيـةـ التـحـتـيـةـ لـلـشـبـكـةـ بـتـخـلـيـ .



النود يتعاملوا مع بعض على انهم topology غير ال topology التي هي بالحقيقة مشبوكين فيها، فال physical wiring تكون bus أما السوفتوير بيحكي انهم ring وبصیر معرف ring . على bus previous, next ال ring star هي برسمة d مثل على ال hybrid topology. أنا عندي logical - وكل نود بينه وبين ال switch عامل ring ونفس المبدأ الي معاه ال token هو الي بيعت.

Channelization

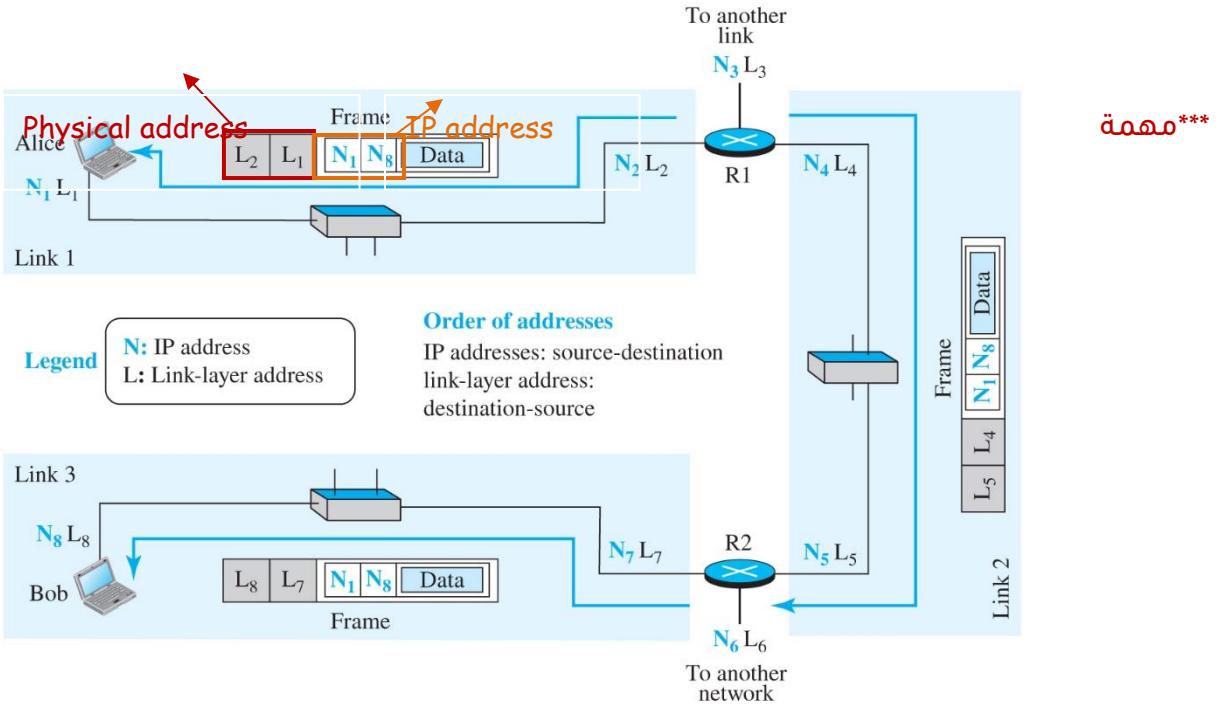
- Channel partition is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.
- Since this method is normally used in wireless LAN, we postpone this discussion until Chapter 4.

غير ال channelization عنا ال random control - نفس فكرة ال frequency division multiplexing و time division multiplexing . بس مش انه عندي bandwidth كبير وبدني أوزعه، تكون عندي ال bandwidth على القد بس بدبي أحدد لكل يوزر مساحة خاصة يلتزم فيها وهيك أنا بضمون ما يصير في تصادم لي؟ لأنهم ما رح يكونوا موجودين على نفس الزمن والمكان، يا إما بشتغل على التردد وبقسم ال bandwidth لأجزاء وبعطيه ل sender معين وهيك بيعت الفريم زي ما بده بدون تصادم لأنه كل واحد بشتغل عتردد - زي الراديوا - ، أما بال time division برفع لفكرة الوقت انه بعطيه ال bandwidth كاملة لاله مدة زمنية معينة وبالزمن الواحد شخص واحد بقدر بيعت.

Link-Layer Addressing

- In an internetwork such as the Internet we cannot make a datagram reach its destination using only IP addresses. The source and destination IP addresses define the two ends but cannot define which links the packet should pass through.





عم بحكي عن العلاقة بين ال physical address and logical address ولی أنا بحتاجهم الاثنين وما بكفي بس واحد؟

لازم نفهم شغلة، عشان تقدر تبعث فريم لنود انت بتشتغل على مستوى ال physical address يعني لازم تكون معك ال physical address لالها، فإذا بدهن تعطي الفريم لل next hope وهو معك بنفس الشبكة ال physical address تبع الاثنين معروفين وبتسلم فالموضوع بسيط.

لما بدهن تبعث رسالة لحدا برا الشبكة ال physical address قيمة بتضمحل لأنه في هاي الحالة ال next hope هي الراوتر وهون بصير ضروري يكون عندي ال logical address عشان أعرف أجياب عنوان الشخص الي بدبي أحكي معه.

بالرسمة Alice بدها تبعث رسالة ل Bob و LAN موجود ب Bob . Alice . LAN وبـ second address وبيناتهم مجموعة من الراوترز، مافي قيمة إذا Alice كانت بس بتعرف ال physical address ، الي بفیدها انها تعرف ال logical address (MAC address) address network layer (address) تبعه وهون الراوترز بساعدوها، الي بتعمله رسالتها من ال network layer بتنزل فيها داتا من ال layers العليا، وبال header تبع ال packet يرمي بـ IP address = N₁ L₈ الى زلت من logical address في layer Alice and Bob على الترتيب.

Alice لازم تكون عارفة ال IP address لجهازها وجهاز Bob عشان توصلله. هاد ال packet بده ينزل على data link layer ويتحول لفريم وينحطله بال MAC address في ال header تبعي وتبع ال MAC address next hope ، ال MAC address لا يكون حدا معن بنفس الشبكة، إذا متنش بنفس LAN ال MAC address next hope فطبعي تكون هي ال source ، مافي next hope destination في قيمة له، حاسوب Alice . الراوتر الي عندها هو ال hope MAC address traffic ، الراوتر الي المسئول عن الشبكة، Alice فيها هو الي بقدر يطلع ال traffic إذا Alice بدها تحكي مع حدا برا الشبكة، الراوتر R1 المسئول عن شبكة Alice عنده 3 أوجه، وجه network interface card شایفة



نفس ال LAN الى Alice فيها وال IP address تبعها و physical address (على الترتيب)، ووجه شايف نتوورك بعيدة N₃L₃ ، ووجه شايف النتوورك N₄L₄ ، فالراوتر من حكمه على ال IP Address تبع Bob عرف انه لازم يبعث هاد الفريم ل N₄L₄ ، فبتتحول ال physical address من N₁L₁ ل N₂L₂ (من hope ل hope من physical address ما بتغير)، بعد هيكل بعمل forward من N₄L₅ هيكل وصلت logical address الرسالة عند R2 - من قراءته لل destination address بيعرف انه في عنده LAN هو responsible عندها بتحتوي على هاد الشخص الي هي على ال N₇L₇ interface ، بيمسك الفريم ويغير ال Source وال next hope ل N₈L₇ وبسلم الرسالة ل Bob وتسلیم الرسالة لازم يتم من حدا معك بنفس LAN .

- ال physical address بخليني أمرق الرسالة من hope أما ال logical address
- (IP address) هو الي بختار المسار عشان بالنهاية أتحرك من ال source لل destination
- بال IP address بحط ال Physical address source . أما بال IP address العكس.
- لو كانوا Bob و Alice موجودين بنفس LAN ما بعمل كل هاد الاشي وبس بحتاج ل physical address ومنش حاجة لراوتر أبداً.

Types of Addresses

1. Unicast Address: Each host or interface is assigned a unicast address.
The link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A2:34:45:11:92:F1

ببعث لجهاز محدد (من راس لراس)
ال physical address يتكون من 48 bits يعني binary 6 بال bytes صعب أكتب ال 48 hexadecimal bits فبكتبهم عن طريق (باخذ كل 4 bits وبكتب بدهاem ال المقابل له) وعشان أفصل بایت عن بایت بحط :

2. Multicast Address: One-to-many communication.
The link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A2:34:45:11:92:F1

معظم ال MAC address هي network interface card يعطي لكرت الشبكة ، في بعض MAC address محفوظة لخدمات خاصة، ما بصير المصنعين يطبعوها على كروت الشبكة منها ال multicast address يتم منحه لمجموعة من الأجهزة ب LAN بحيث إذا ببعث فريم وال destination MAC address هو هاد ال multicast address كل



الناس الي بالمجموعة بعتبروا انه الفريم موجّه لاله، كمثال بذنا نعمل امتحان بمختبر فيه 40 حاسوب والدكتورة بدها تفصل ال 40 لـ 20 ، 20 طالب بـ form 1 و 20 بـ form 2 .
بدها تعمل set up على مستوى ال data link layer للأجهزة الي بفورم 1، مختلف عن ال set up الي بفورم 2 ، مثل رح تعمل 40 فريم لكل جهاز لحال وتحكيله يعمل up .
بتعمل جروب وبحط فيها الأجهزة تبع فورم 1 وبتحدد address وبتخليلهم أعضاء بالجروب ونفس الاشي للجروب الثاني، كل جهاز بدها بس تحكيله هو لأنّي مجموعة بنتمي، هيك بصير عنا 2 multicast (معناه بعثنا لجزء من الشبكة مو كلها).

3. Broadcast Address: Means one-to-all address.

A broadcast address is made of 48 bits of 1's.

FF:FF:FF:FF:FF:FF

- ببعث لكل الناس الي معنّي بنفس LAN .
- زي لما الدكتور تبعث عتيمز إعلان لكل الشعب .
- لو بس لشعبة معينة تكون multicast .
- ولو بس لطلاب محدد تكون unicast .
- هون ال physical address بكون كله 1 فبتم ترجمته كله ل F .
- لما تكون انت على LAN ممكن يوصلك كثير frames مو شرط تكون لالك بس لأنك موجود على نفس الكيبل رح تسمعها ، بس إذا ال MAC address يعنيك بتستلمها ، إذا لأنّي بتهملها .

Address Resolution Protocol (ARP)

- Any time a node has a packet to send to another node, it has the IP address (network-layer address of the next node); it needs the link-layer address of the next node.
- This is done by a protocol called ARP located in the network layer.
الهدف الأساسي منه أترجم أو أحول أو أعرف ال IP address الشو ال MAC address اللي شو ال IP address .
مهم عشان أقدر أسلم الرسالة باليد (تذكروا الرسمة الي فوق).
ال ARP ببعث رسالة لكل الناس الي بال LAN وبتحكيلهم هاد ال IP address موجود بهاي الشبكة شو ال MAC address المقابل لاله، الشخص المعنى بعطيه ال MAC address .

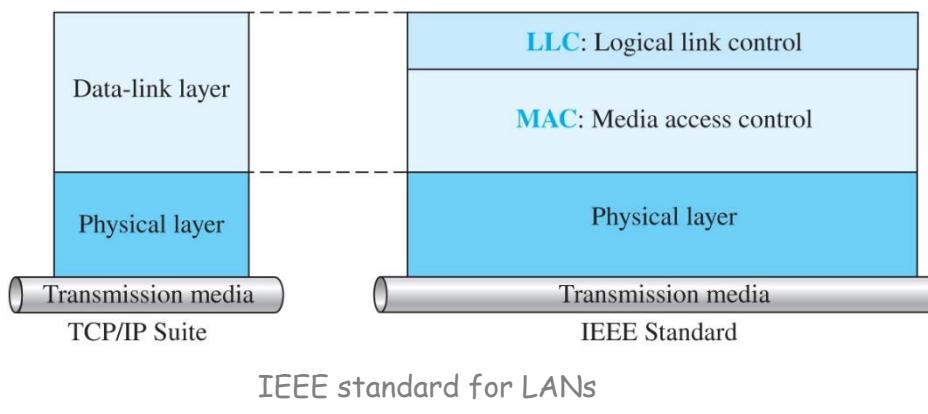


Chapter 04: Local Area Network (LANs)

Ethernet

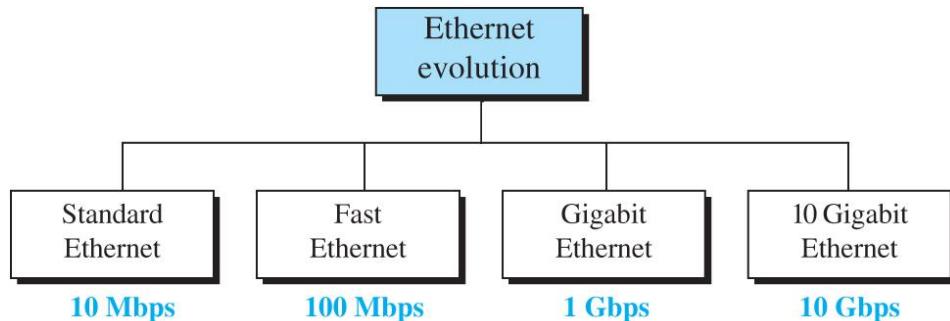
- In Chapter 1, we learned that a local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus.
- In the 1980s and 1990s several different types of wired LANs were used. The IEEE has subdivided the data-link layer into two sub-layers: logical link control (LLC) and media access control (MAC).

ال Ethernet هو أكثر ال data link layer protocols شيوعاً .
هو عبارة عن ال data link layer protocols المخصص لل wired LANs .
مؤسسة IEEE صنعت ال standards لـ wired LANs (مشان مش كل مصنع يصمم
و بروتوكولات حاله) ، الهدف من ال standards أنه لما المصنعين كلهم
يتلزموا فيها ال devices بحسب انه ال رح تقدر تحكي مع بعض
كمثال بالجامعة يتم تجهيز المختبرات عن طريق عطاءات، مجمع القاعات العلمية أخذ
عطاء من شركة معينة، وكلية الهندسة أخذت عطاء من شركة ثانية، بلآخر الأجهزة الي
بالعلمية والهندسة رح يضطروا يتواصلوا مع بعض، فما بزبط ما يكونوا قادرین على
التواصل، وهو منطق نشتري كل أجهزة الجامعة من نفس مزود الخدمة، فال IEEE لما
عملت هدول ال standards أي شركة عم تبني بنية تحتية لـ physical layer + data link
layer عم تمشي على ال protocol، هاد الاشي بخلي كل الأجهزة interoperable +
هيك حتى لو كان المصنوع مختلف كل الأجهزة رح
يفهموا ويحكوا مع بعض .



بالصورة بنشوف منظور ال IEEE لـ physical layer + data link layer .
بال physical layer TCP/IP suite عنا ال transmission media مبني عليها مباشرة ال .+ data link layer
أما ال IEEE بحطوا ال transmission media + physical layer بس ال LLC + MAC ← 2 sublayers .
بدهم يقسموها ل





Ethernet evolution through four generations

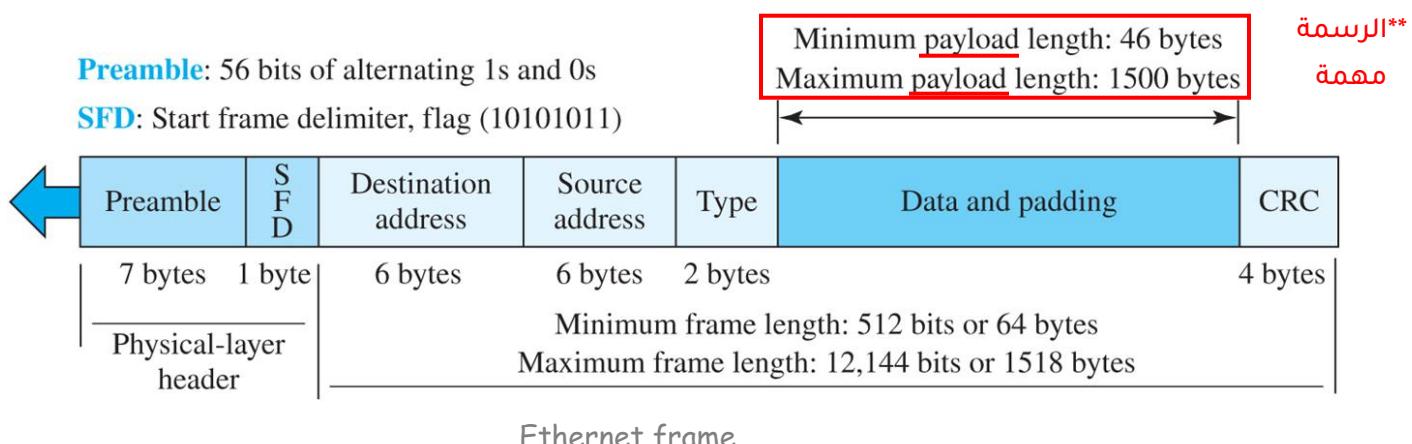
الـ bit rate تطور عبر السنوات، أول ما بليش كان standard Ethernet والـ 100 Mbps بـ Fast Ethernet، بعدين طبع الـ 10 Mbps = الـ 10 Gbps

Standard Ethernet

- We refer to the original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet.
 - Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution.
- كثير شغلات كانت موجودة بال standard Ethernet ضللت بال generations المتقدمة.
- بس كمان كثير شغلات ثانية تم تغييرها عيشان يقدروا يواكبوا الـ bit rate العالية.

Connectionless and Unreliable Service

- Ethernet provide a connectionless service, which means that the frames are sent independent of each other.
- الـ connectionless and unreliable service عبارة عن Ethernet يعني إذا عندي مجموعة من الـ frames وعم ينطلقوا من الـ source كل واحد عم بمشي على الـ next hop مو شرط كلهم يتبعوا نفس المسار (يعني كل واحد على كيفه).



ال (SFD) مع بعض ← اسمهم ال 8 bytes = preamble + start frame delimiter
 -
 Ethernet physical layer header (زي ال flag الي تكون بداية الفريم ← لأنه ال physical layer header)
 بدعم أنه الفريم يكون حجمه مثل ثابت فلازم يكون في flag بداية (protocol)
 .56 bits of alternating 1s and 0s = preamble
 ال SFD pattern تبعته 1 byte = .10101011
 ال header تبع الفريم تكون من 14 bytes وال 4 bytes = trailer ←
 يعني ال 18 bytes = header + trailer
 ال physical header بيلش بال 48 bytes يعني هو ال destination address
 current physical address هو ال source address.(next hope address
 . 12 bytes = source + destination لـ MAC address hope
 ال type ، بتتشابه 3 كان يمرق علينا frame ينكتب عليه ACK أو select أو poll، مثل كل
 الفريم الي بنشووفها data frames في كثير control frames بحوكوا فيها ال nodes مع
 بعض بعيداً عن بيانات اليوزر، فال 2 bytes هدول بحددوا شو نوع الفريم الي بتعامل
 معاه سواءً كان OR control frame user frame
 ال packet (هي ال النازلة من ال network layer) بتراوح طولها ما
 بين 46 bytes (الحد الأدنى المسموح فيه) والحد الأقصى = 1500 bytes
 عن طريقها بنقدر نعرف ال min and max frame length .
 ال 4 bytes cyclic redundancy check ← CRC بتم إضافتهم بالنهاية لضمان الداتا
 انها سليمة.
 ال Ethernet protocol بطبق خوارزمية فيها عمليات حسابية على الداتا الموجودة
 وبخصوصها ب 4 bytes next hope ، ال الفريم بتتمسك عليه نفس الخوارزمية إذا
 طلع معها ال 4 bytes الي قبل بتفترض انه الفريم أمن وسلام، أما إذا كان ال
 غير بتفترض انه الفريم corrupted وبتهمله .

Frame Length

- Ethernet has imposed restriction on maximum and minimum length to provide correct operation of CSMA/CD.
- An Ethernet frame has minimum length of 64 bytes.
- The maximum length limit is 1518 bytes (without preamble and SFD). This means that maximum payload is 1500 bytes.

Min frame length = header and trailer (18 bytes) + min payload length (46 bytes)

Max frame length = header and trailer (18 bytes) + max payload length (1500 bytes).

في حال كان ال packet الي نزل حجمه أقل من 46 bytes بنعمل padding بنزلق فيها
 عشان توصل لل 46 bytes (الي هو الحد الأدنى).



لو كان حجمه أكبر من 1500 بتصير عملية ال fragmentation، بتقسم لفريمز أصغر.

Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

نفس الـ حكيناه بتتشابتر 3.

Transmission of Address Bits

- The way addresses are sent online is different from the way they are written in hexadecimal notation: Transmission is left to right, byte by byte; however, for each byte, the least significant bit that defines the address type is sent first.

كيف بنبعثت الـ MAC address بالشبكة؟
بالـ MAC address دائمًا بتتبعت البيانات left to right byte by byte .بس البايت الواحد right to left المثال:

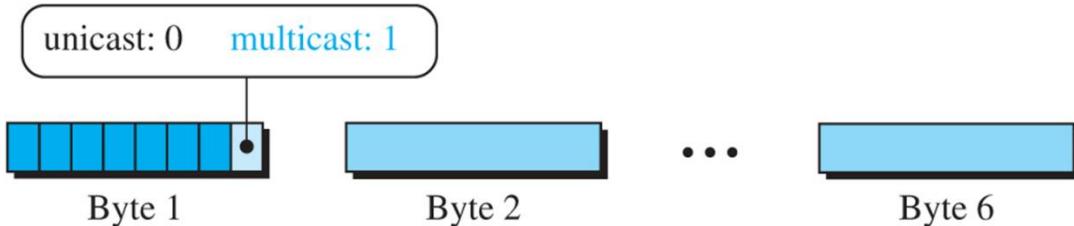
- The example shows how the address 47:20:1B:2E:08:EE is sent out online.
- The address is sent left to right, byte by byte
- For each byte, it is sent right to left, bit by bit, as shown below:

Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

لفترض انه عنا هاد ال MAC address ← 47:20:1B:2E:08:EE كيف بنبعثت؟
روح ينبعط أول بايت ال 47 بعدين 20 بعدين 1B بعدها 2E بعدها 08 بعدها EE (right)

ال 47 لما نخليها binary بتصير 01000111 . هلا هاد لما نبعته بنبلش من اليمين
11100010 ، وبكميل للباقي نفس الاشي.





Unicast and multicast addresses

- حكينا من قبل .broadcast or multicast or unicast هو 3 أنواع MAC address انه ال الوحيد الي بدرج ضمن نطاق ال broadcast هو الي بتكون من 1s : FF : FF : FF : FF : FF
- ال unicast ببعثت ل node معينة (يعني حتى لو وقع بأكثر من stations بس وحدة الي بتستلمه) ال multicast (زي جروب الوايـس) كيف بنميز ما بين ال unicast و ال multicast ؟
- بنتطلع على ال byte الموجودة أقصى اليسار، ال bit الموجودة على اليمين بهاد البايت، إذا كانت 0 معناهه unicast، وإذا كانت 1 معناهه multicast يعني باختصار ال byte الموجود على الشمال عبارة عن 2 hexadecimal numbers يعني باختصار ال byte الموجود على الشمال عبارة عن 2 hexadecimal numbers . multicast unicast فإذا كان زوجي معناهه وإذا كان فردي إلى عاليـمـين ، إذا كان زوجي معناهه unicast وإذا كان فردي .

Example

Define the type of the following destination addresses:

a. 4A : 30 : 10 : 21 : 10 : 1A

This is a unicast address because A in binary is 1010 (even).

b. 47 : 20 : 1B : 2E : 08 : EE

This is a multicast address because 7 in binary is 0111 (odd).

c. FF : FF : FF : FF : FF : FF

This is a broadcast address because all digits are Fs in hexadecimal.

في حال ما كنتوا متذكرين كيف بنحول من binary ل hexadecimal شوفوا هاد الفيديو .



Summary of Standard Ethernet implementations

	<i>Implementation</i>	<i>Medium</i>	<i>Medium Length(m)</i>	<i>Encoding</i>
Twisted pair	10Base5	Thick coax	500 m	Manchester
	10Base2	Thin coax	185 m	Manchester
Twisted pair	10Base-T	2 UTP	100 m	Manchester
Fiber	10Base-F	2 Fiber	2000	Manchester

هاد الجدول رح يمر علينا بكل generation رح نحكى عنه . -

عامود ال encoding مو مطلوب . -

عامود ال implementation . -

10Mbps 10Base5

Baseband

ال 5 و 2 هم coaxial والرقم
الأكبر يعني أسمك فالمسافة
الي بخطيها أكبر

Fast Ethernet (100 Mbps)

- In the 1990s, Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet.
- The designers of the Fast Ethernet needed to make it compatible with the Standard Ethernet. The MAC sublayer was left unchanged. But the features of the Standard Ethernet that depend on the transmission rate, had to be changed.

تم تطوير ال fast ethernet وعملوا ال ضاعفوا ال standard ethernet -
أضعاف، حاولوا قدر الإمكان انهم يحافظوا على ملائم ال standard ethernet ، حسّنوا
كفاءة ال physical layer فاستخدمو أنواع أفضل من الكوابل ، أما ال MAC layer حاولوا
ما يغيروا فيها .

Access Method

- We remember that the proper operation of the CSMA/CD depends on the transmission rate, the minimum size of the frame, and the maximum network length.
- If we want to keep the minimum size of the frame, the maximum length of the network should be changed.



- In other words, if the minimum frame size is still 512 bits, and it is transmitted 10 times faster, the collision needs to be detected 10 times sooner, which means the maximum length of the network should be 10 times shorter (the propagation speed does not change).

المفروض بما أنه تم زيادة ال bit rate . لما يزيدوا ، لما بلشوا يطبقوا الموضوع لاحظوا أنه الأداء نزل والداتا عم توصل corrupte لي؟ لأنه لما عم بنزيد ال 10 bitrate أضعف ما عم بنغير حجم الفريم . وحسب معادلة ال transmission delay

$$\text{transmission time} = \text{frame_length}/\text{bit_rate}$$

ال frame length عم بضل ثابت وال bitrate بالمقام عم نظرية ب 10 ، معناه ال propagation delay رح يقل للغشier ، بهاي الحالة هل احنا فعلياً عم بنطبق قاعدة ال ضعف CSMA يزبط ؟ احتمال كبير لا ، من هون لما نسيو هاد الاشي وكانت الداتا توصل ب bitrate عاليه بس توصل كلها corrupted . شو الحل طيب ؟

قرروا انهم ما بدhem يغيروا ال frame length ومعناه ال propagation رح يضل نازل للغشier . فالحل انه ال propagation ينزل كمان للغشier . شو معادلة ال propagation delay = distance/medium_speed

ثابتة ما حد بقدر يلعب فيها (سرعة الضوء) . فما في حل إلا نلعب بال distance . بدننا نصغر قطر الشبكة كمان للغشier .

Auto-negotiation

- A new feature added to Fast Ethernet is auto-negotiation. It allows two station to negotiate the mode or data rate of transmission.
- للسبي الي حكيناه فوق طلع اشي اسمه auto negotiation . انه النود الي بتحكي مع بتتفقوا هل هم بدhem يحكوا next hope simplex or half duplex or duplex . أو بدhem يعتمدوا ال bitrate كله ولا لسا المسافة ما نزلت فالبتالي ما رح ياخذوا ال 100Mbps كلها ...

فهيكم عم بعطونا سماحية في حال ما قدرنا نقلل من قطر الشبكة الي عنا ، بنختار انه ما نستخدم ال 100Mbps .

Physical Layer

- To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer.
- Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
- The two-wire implementation can be either shielded twisted pair (STP), which is called 100Base-TX, or fiber-optic cable, which is called 100Base-FX.



- The four-wire implementation is designed only for unshielded twisted pair (UTP), which is called 100Base-T4.

Summary of **Fast Ethernet** implementations

<i>Implementation</i>	<i>Medium</i>	<i>Medium Length</i>	<i>Wires</i>	<i>Encoding</i>
100Base-TX	STP	100 m	2	4B/5B + MLT-3
100Base-FX	Fiber	185 m	2	4B/5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

نفس الـ **Implementation** قبل الـ **Medium** ما رح نطلع عليه .
 الـ **Implementation** 100Mbps رح نعرف انها **fast ethernet** .
 الـ **Implementation** هي **fiber** والـ **Implementation** هي **twisted pair** .
 الـ **Implementation** هي **TX** والـ **Implementation** هي **shielded** .
 أما الـ **Implementation** هي **T4** وهو **unshielded cables** مع بعض .
 هاد الاشي بخليله يقاوم الـ **interference** وعرضة أقل للـ **attenuation** (أقل احتياج للـ **amplifiers**) .
 بنلاحظ انه المسافات فيها مثل كثير كبيرة بس مع هيك الفايبر أطول اشي .

Gigabit Ethernet (1000 Mbps)

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps).
- The IEEE committee calls it the Standard 802.3z.
- The goals of the Gigabit Ethernet were to upgrade the data rate to 1 Gbps, but keep the address length, the frame format, and the maximum and minimum frame length the same.

تم تسمية هاد المشروع بـ **802.3z** .

كمان هون ضاعفوا الـ **bitrate** بس ما بدهم يغيروا الـ **frame size** .

MAC Sublayer

- A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched.
- However, to achieve a data rate of 1 Gbps, this was no longer possible. Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.
- Almost all implementations of Gigabit Ethernet follow the full-duplex approach, so we mostly ignore the half-duplex mode.



اختاروا انهم ما يعدلوا على ال MAC layer ، انه التعديل يتم على data link layer . قرروا -
 انهم يشتغلوا half duplex and duplex .simplex بدون -
 استبدلوا ال switch controlled access بنوع من ال random access ، يعني جيب -
 وأشبك ال PCs عليه م Shan ما يكون في سيناريو لل collision. هيك كل جهاز تكون له
 كيبل عل switch فلو بعث أي فريم رح يوصل مباشرة ، فبس رححتاج انه ال switch يكون
 كبير م Shan يتتحمل كل ال traffic .

- In the **full duplex mode**, there is a central switch connected to all computers. There is no collision in this mode.
- In the **half duplex mode**, a switch can be replaced by a hub.

Summary of **Gigabit Ethernet** implementations

<i>Implementation</i>	<i>Medium</i>	<i>Medium Length(m)</i>	<i>Wires</i>	<i>Encoding</i>
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

.1 Giga ل 1000 نسبة -
 .baseband ل Base -
 short = S -
 long = L
 shielded twisted pair = C
 unshielded twisted pair = T4
 كالعادة ال fiber بجيب مسافات أكثر من twisted pair -

10-Gigabit Ethernet

- In recent years, there has been another look into the Ethernet for use in metropolitan areas.
- The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used as LAN and MAN (metropolitan area network).
- The IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae.

هون حكوا انهم بدئم يطلعوا كمان لـ wireless MAN (زي مثلاً أجزاء من العاصمة-أقل من ال -WAN).
 ال 802.3ae بسموه IEEE -
 لازم يشتغل ك full duplex بس.



- 10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet.
- Four implementations are the most common: 10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4.

Summary of 10-Gigabit Ethernet implementations

Implementation	Medium	Medium Length	Number of wires	Encoding
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 km	2	8B10B

لاحظوا انه هون كلهم Fiber -

ترتيبهم تذكروهم زي كانهم

Short

Long

(XL) Extended

وأكبر اشي EW

الـ number of wires ما تدققوا عليه كثير الدكتوراة حكت.

WIFI, IEEE 802.11 PROJECT

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- It is sometimes called wireless Ethernet. In some countries, including the United States, the public uses the term WiFi (short for wireless fidelity) as a synonym for wireless LAN.
- WiFi, however, is a wireless LAN that is certified by the WiFi Alliance.

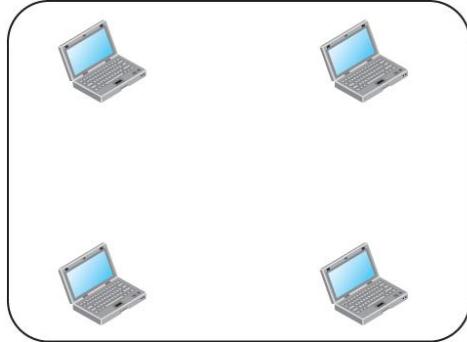
Architecture

- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

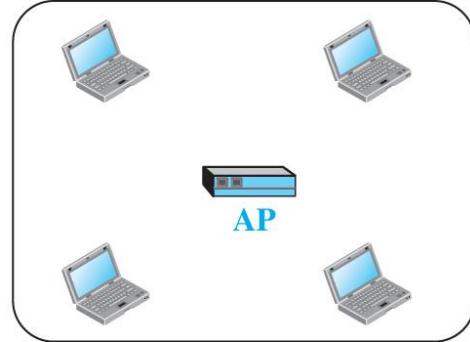
Basic Service Set (BSS)

- IEEE defines the basic service set as the building block of a wireless LAN. It also defines an optional base station known as the access point (AP).





Ad hoc BSS

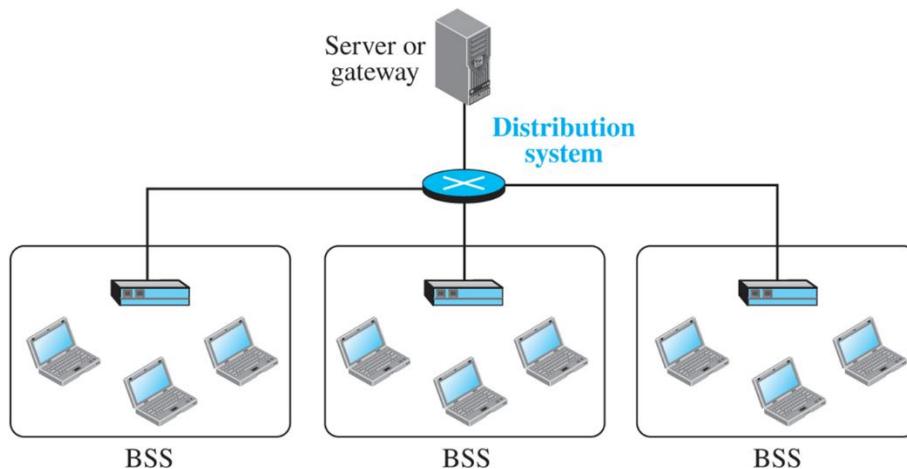


Infrastructure BSS

- الـ BSS زي مختبر صغير، فهي عبارة عن LAN معزولة عن الآخرين.
- الـ Ad hoc OR Infrastructure شكلين كلهم نفس النوع ومافي حدا فيهم مميز عن الـ Ad hoc مجموعة من الـ wireless nodes كلهم نفس النوع ومافي حدا فيهم مميز عن الثاني (زي لما حكينا عن الـ controlled access بس بدون شرطي).
- الـ Infrastructure فيه شرطي.
- الـ AP (Access Point) بالعادة بتكون مميزة عن باقي الـ stations هي بمثابة شرطي بنظم الـ traffic.
- في شبكات بتكون pure Ad hoc وفي شبكات pure infrastructure وفي شبكات بتكون hybrid يعني كبنية تحتية هي Infrastructure فيها AP بس هاي الـ Infrastructure دائمًا بتشتغل، إذا بتطفي بتتحول لـ Ad hoc وإذا بتشتغل بتكون Infrastructure.

Extended Service Set (ESS)

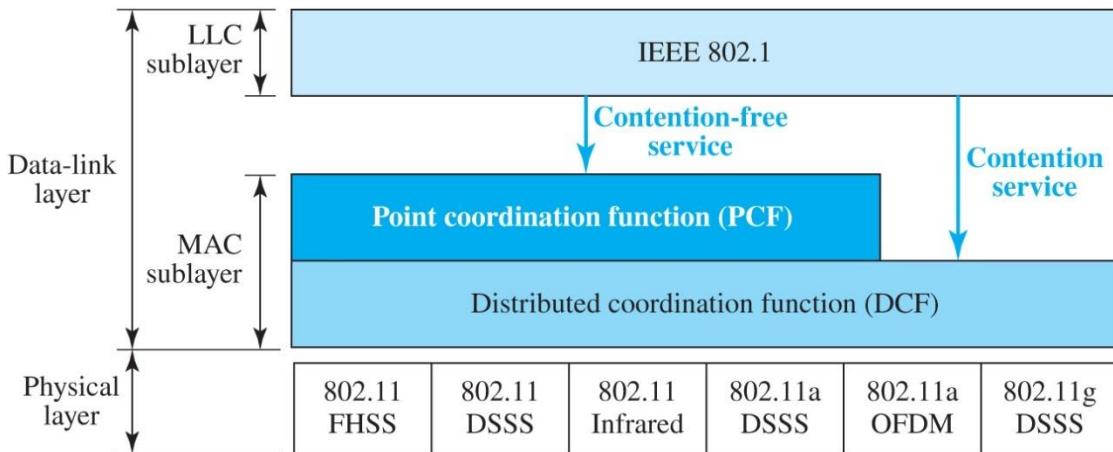
- An extended service set is made of two or more BSS with Aps that are connected together using a distribution system.
- هون كل BSS في switch بشبكتها بالشبكة ما تكون جزء منها وظيفته بس يطلعها على الشبكة يعني لكل BSS في switch مربوط بـ distribution system (زي الراوتر بس أكبر) اللي بشبكتهم بالـ gateway اللي بتطلعهم على الانترنت.



- IEEE defines three types of stations: no transition, BSS transition, and ESS transition.

MAC Sublayer

- IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

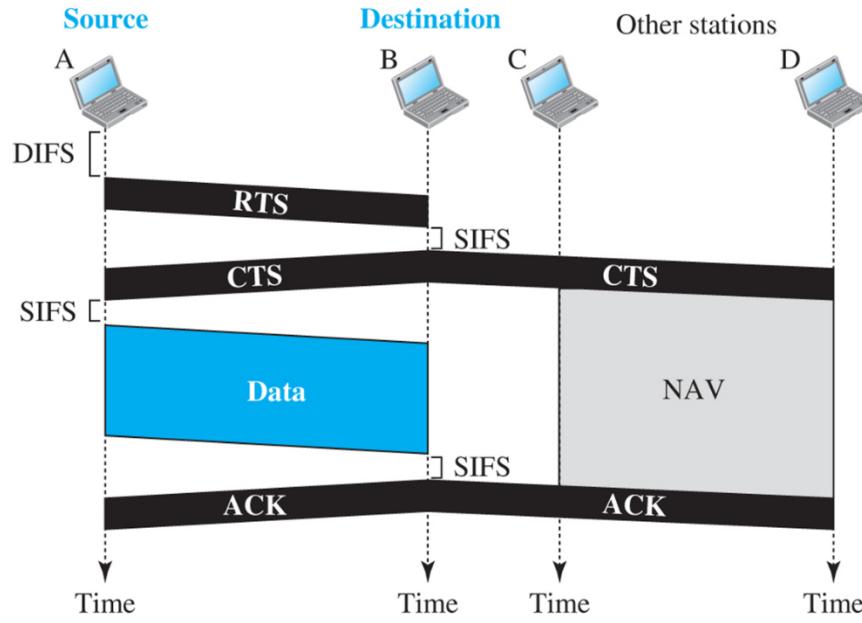


حكينا بتشابتر 3 عن ال random access الي كانت بتسمح لل حدوث انه يحدث وبتعامل معه ، وال controlled access الي كانت تمنع حدوثه بشكل كامل. ال IEEE عملوا نفس الاشي بس بسميات مختلفة حافظوا على فكرة انه ال data link layer مقسمة لجزئين، الأول اسمه framing, flow control, (Data link control) (LLC) Control (DCF) (Distributed coordination function) والثانية coordination function (PCF). ال PCF فكرتها الأساسية انه يكون في شرطي سير يعمل يضمن الدورية ويمنع حدوث collision (زي ال polling). ال DCF هومحاكاة لل random access وتحديداً ال CSMA/CA، حكينا من قبل فكرة ال CSMA/CA انه بحاول ياخذ خطوات قبل ما يصير ال CSMA/CA يعني ما يستناه يصير. بنلاحظ بالرسمة انه ال physical layer مقسمة لأكثر من صنف . هم عبارة عن أنواع مختلفة من ال IEEE wireless technologies الي ال standard (802.11).
بنلاحظ كمان انه في اشي اسمه contention service واسمها contention free service يعني بصير في تزاحم وممكن يصير collision = Contention ف بال DCF هي contention service يعني بصير في تزاحم وممكن يصير أما بال PCF في AP بوزع الدورية وبالتالي مافي تزاحم فما في collision. بنلاحظ كمان انه المستطيل تبع ال PCF أقصر من ال DCF وهاد معناه انه مش ضروري كل الموجودين بال physical layer أطبق عليهم ال PCF بس لازم أطبق ال DCF.



Distribution Coordination Function (DCF)

- One of the two protocol defined by IEEE at the MAC sublayer is called distribution coordination function (DCF), which uses CSMA/CA.



CSMA/CA and NAV

حكينا بال CSMA النود شو بتعمل قبل ما تبعت؟ بتصلها تسمع لحد ما تصير ل channel فاضية بعدين بتبعت.

هون بالرسمة الي بصير هو أنه نود A بدها تبعت داتا لنود B. بتستنى مدة زمنية اسمها carrier (distributed inter frame spacing) DIFS (distributed inter frame spacing) هاي المدة عم تعمل فيها ال sensing، لو في حدا عم بعمل transmission أو فات ب...collision والمفروض بعد ما تمرف هاي المدة يكون ال carrier sensing اشتغل تمام وال channel available . بعدها بتكتب شو هو ال MAC address (request to send) RTS هو بتبعن RTS بعدها ومين النود الي بدها تحكي معها وبتبعد، النود المعنية B إذا وصلها ال SIFS معناها انه ال channel متاحة، وإذا هي قبليت وبدها تستلم داتا بتستنى مدة زمنية SIFS (Short Interframe Space) هاي المدة بتستناها عشان ال RTS تسمع كل النود انه احنا رح نشغل الميديا، والمدة بتكون قصيرة لأنه مدام الرسالة وصلتني بنجاح معناته الميديا فاضية فنستعجل قبل ما حدا ثاني يشغل ال channel (يعني لازم نستنى بس مدة طويلة) ومبشرة بعدها بتبعن RTS (Clear to Send) كمان هي special control frame بكتب فيها لمين بنعطي الإذن (لأنه ممكن يكون وصلني 2 RTS) والرسالة هاي بسمع فيها كل النودز، لي بسمع الكل؟ عشان الحدا الثاني الي بده يبعث داتا يسنتى، لي؟ غالباً هاي النود بتكون عبطاريات يعني معرضة انها تخسر طاقتها، إذا كل شوي عملنا carrier sensing هاد بستهلك البطارية، بهون لما النود الثانية بوصلها ال CTS بتطفي وبتحط حالها ب ال NAV (network allocation vector) هو عبارة عن field

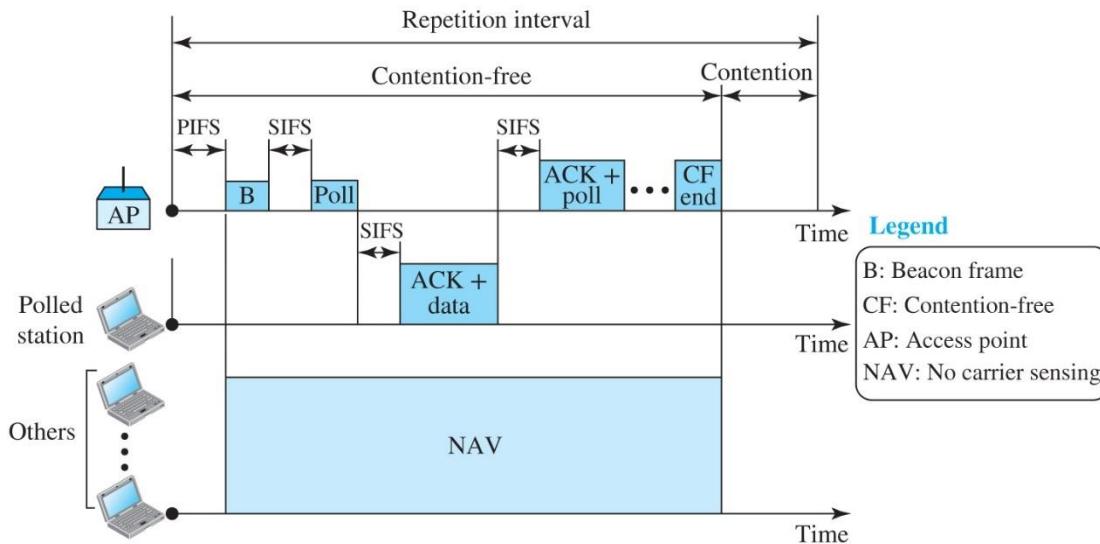


بال header تبع الغريم مخزن فيه قديه المدة الزمنية الى متوقع نحتاجها ليخلص ال transmission بين A و B (النود الي بتكون بعالي الحالية بتكون طافية وممنوع تعمل CTS (carrier sensing). لما النود A تسمع ال NAV state وبعدها عطول بتبلش بضم البيانات، وقت SIFS مشان الباقى يفوتوا بال SIFS عشان نتأكد انه الداتا وصلت بنجاح بعدها بس تخلص الداتا الي بدها تبعتها بستنى SIFS عشان تأكد انه الداتا وصلت بنجاح بعدها نود B بتبعتها ACK للجميع عشان A تعرف انه الداتا وصلت بنجاح عشان ما ترجع تعمل وعشان النودز الباقيه تصحي (لأنه ممكن تكون خلصت أسرع من ال NAV).

Point Coordination Function (PCF)

- This is an optional access that can be implemented in an infrastructure network. PCF has priority over DCF.
- However, to allow DCF frame to get access to the network repetition interval has been added to the network.

هاد البديل في حال ما كنا بدننا نشتغل DCF ، بشبه كثير فكرة ال polling الي حكينا عنها - بتشابتر 3.



لازم تكون الشبكة Infrastructure في AP ، ال PCF بتعين بتكون شغاله وبتسنی PIFS بعدين بتبعتها control frame اسمها B هي علامة معناها انه احنا راح نبلش PCF. بنسنی SIFS مشان كل النودز توصلها ال B وبعدين بتبلش يعمل polling بتسأل وحدة واحدة هل بدك تبعتي؟ يا إما بتوافق وبتعطيها ACK + Data أو ما بتوافق، في حال station وافتقت الباقى بنحطو بمرحلة ال NAV ، بعد ما يخلص بستنى شوي وبعمل ACK + polling اللي بعدها لحد ما يعمل الدور عكل النودز، بضل يلف يلف لحد ما يخلص المدة السموحة الـ PCF لأنه الـ AP فعلياً مش مسموح يضل الـ PCF شغال 24 ساعة، الزمن مقسم لفترات والفترة الواحدة بتدعم الشكلين ، هون مثلًا الـ PCF 90% من الوقت و 10% DCF ، فلازم يكون في علامة نبعتها لما نبلش بالـ PCF وكمان علامة لما بدنـ



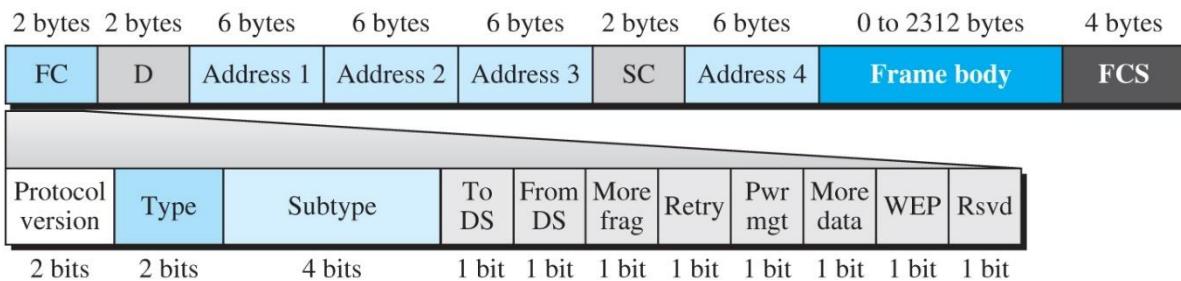
نخلصه الي هو ال Beacon end CF بس هدفه العكس انه طفووا ال PCF واشتغلوا .DCF

Fragmentation

- The wireless environment is very noisy, so frames are often corrupted.
- A corrupted frame cannot be resubmitted.
- The protocol recommend fragmentation. The division of frame into smaller ones.

فكربته انه في حال كان حجم الفريم قريب من الحد الأعلى بقسمه frames أصغر وأبعث كل واحد لحال، لأنه في حال bit واحد تعرض ل collision الفريم كله بضيع ولازم نعمله retransmission ، فبنقسمها مشان في حال صار بنعمل لجزئية بسيطة بس.

Frame Format



هاد معقد أكثر من ال frame ethernet فيه header + body + trailer . حجم ال body كبيره (0 to 2312 bytes) . ال FCS الي بالأسود نفسه ال CRC الي بال ethernet بس هون يستخدمو خوارزمية أكبر شوي.

ال header بيلش بال FC (frame control) فيه معلومات مهمة عن الفريم بعدها 6 bytes إذا بدبي أحط نود ب NAV state تكون هون ، بعدين عنا 4 Addresses وكلهم physical address إما type، subtype أو protocol version . ال subtype إما management or data لإدارة شؤون الشبكة (النود الي طفا أو ضوا ...) ، ال control (هاد الفريم ACK أو B) مش دائمًا ال 4 بشتغلوا .

ال to DS and from DS addresses هل ال 4 مفغلات وإذا لا مين مفغل ومين لا.

ال More frag bit هو ي تكون on or off إذا كان on معناهه هاي عباره عن fragment بس مش الوحيدة (ممكن الأولى وممكن الوسطى) بس لو كان 0 معناهه يا إما انه هاي هي الأخيرة يا إما أصلًا مافي fragmentation.



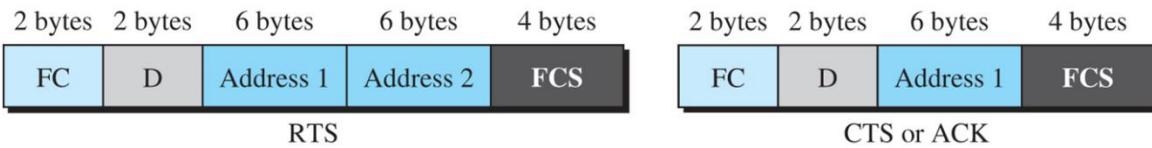
ال مشان أعرف إذا هاد الفريم **retransmitted** أو **genuine** . إذا كان **on** تكون
 ال **retransmitted**
 ال **power saving** إذا عم نشتغل على أو لأن **power management**
 ال **more frames** غير عن **more data** . هاي معناها **more fragments** بغض النظر عن
 ال **fragmentation** ، هل في فريم بعد هاد ولا هاد آخر واحد
 ال **Web** هو اشي لـ **encryption**

Field	Explanation
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 4.6)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

هاد الجدول نفس الي حكيناه فوق بس نتبه على ال **type** ، إذا كان **00** -
management . إذا كان **01** - **control**

- A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.

Control frames



بال **RTS** ال **FC** نفس الي قبل ، مافي **4 addresses** بس **2** عنواني وعنوان الشخص
 الي بدبي أبعته .

بال **CTS, ACK** نفس الهيئة، باخذوا **address 1 , FC,D** هو مين المعني بالرد بس .
 ال **CTS, ACK** نفس الشكل بس لما نطلع على ال **header** وال **subtype** بنقدر نحدد شو
 هي .

ال **ACK** معناها انه استلمت الداتا بنجاح فالي بعث الداتا يروح اللي بعده .
 ال **CTS** لسا ما استلمت اشي .



Values of subfields in control frames

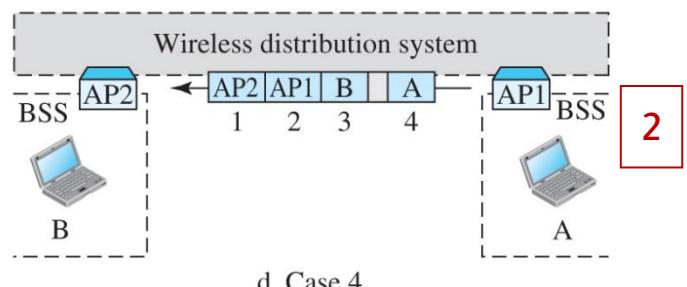
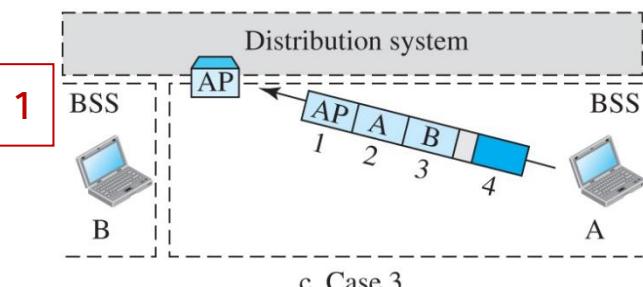
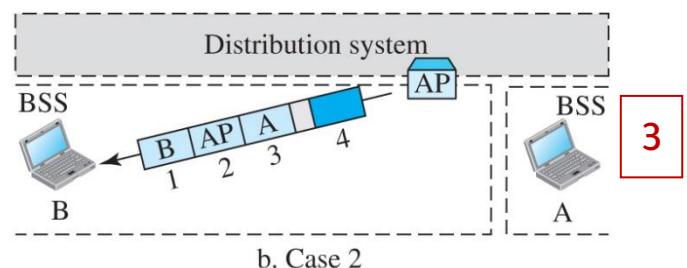
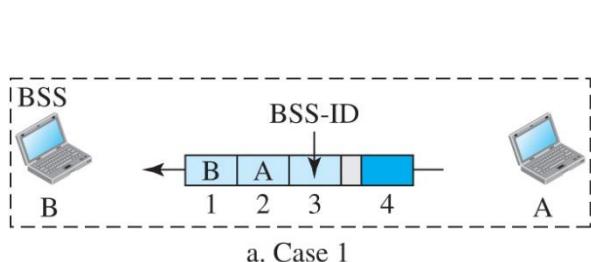
Subtype	Meaning
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

b6s

Addressing Mechanism

- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS.
- Each flag can be either 0 or 1, resulting in four different situations.
- The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
3	0	Destination	Source	BSS ID	N/A
	0	Destination	Sending AP	Source	N/A
	1	Receiving AP	Source	Destination	N/A
	1	Receiving AP	Sending AP	Destination	Source



ال case الرئيسية الأولى أنه ال source وال destination موجودين بنفس ال service set . بالحالة هاي ال next hope هو ال destination . بھاي الحاله ال AP ما بتدخلوا . لأنه بما انه موجودين بنفس ال service set فمعناته رح يكونوا يعرفوا ال MAC address وما رح يحتاجوا غيره . بھاي الحاله ال $TO = From + 0$.

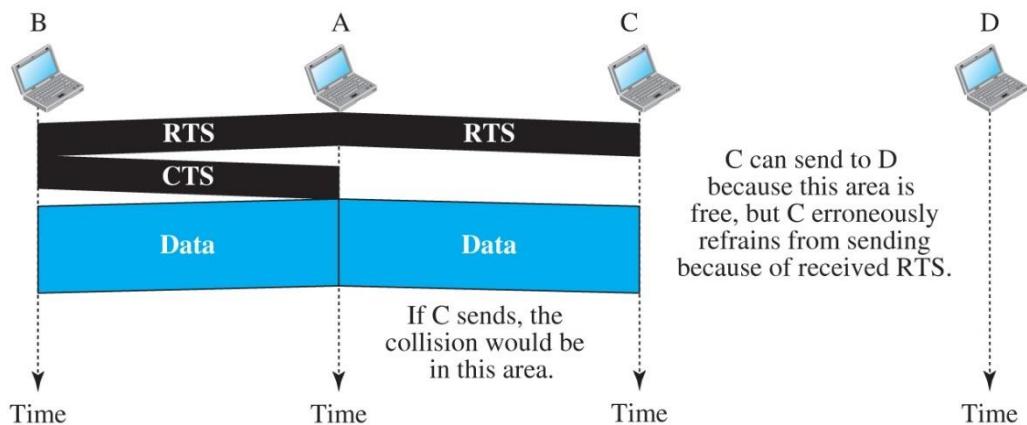
الحالة الرئيسية الثانية ال extended service set بنفس ال source and destination بس مش بنفس ال basic service set (زي لما جهاز بمختبر بده يحيى مع جهاز بمختبر ثاني بس بنفس الطابق)، بعدي الحالة أنا ما بقدر أحكي مباشرة مع الشخص المعنى، ف A بدها تحكي مع B ، بتبعث لل AP المسؤولة عنه، بس بستخدم ال to + from بطريقة معينة مشان أفهم ال AP مين أنا و مع مين بدبي أحكي، الرسمة الي فوق تمثل ال 3 خطوات الي بمر فيها السيناريو الثاني (أني احكي مع حدا مش معاي بنفس ال basic service set). (ورح نمشي حسب الترتيب الأحمر).

آخر خطوة (case 2) ضل آخر اشي انه ال AP تبعث B تتسلمه الرسالة لـ B .
source وهما الحالات الوحيدة الي تستفيد من الأربعه.
B، ف بالعنوان الأول رح يكون ال AP تبعث B وبعدين لـ A وبعدين ال destination و forwarding للفرئيم لل AP المسؤولة عن الخطوة الثانية الـ AP

للحفاظ على ملائمة المنهجية، نكتفي بذكر الحالات التي ينطوي عليها الترميم، وهي الحالات التالية:

Exposed Station Problem

- A similar problem to the hidden station problem is exposed station problem.
 - In this problem, refrains using a channel when the channel is available.



- نود A بده يبعث لنود B . فطبعي أي حدا بده يشتغل على الـ collision avoidance بده يعمل RTS لكل الي بال communication range من ضمنهم بالرسمة النود C . ما دخلها بالحوار ما بين A و B ، (لما تمر جنب ناس بتعرفهم ويكونوا بحكوا عن حدا وتفكير انهم بحكوا عنك) C بصير فيها زي هيك ، سمعت الـ RTS من A لـ B فكرت انه ممنوع تبعث (فعلياً هي ممنوع تبعث لـ A . بس لو بدها تحكي مع D الموجة تبعتها ما راح تتصادم مع A وبعيدة عنها فعادي لو حكت) فهو C بالغت بالاحتياط .

<i>IEEE</i>	<i>Technique</i>	<i>Band</i>	<i>Modulation</i>	<i>Rate (Mbps)</i>
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

- All implementations, except the infrared, operate in the industrial, scientific, and medical (ISM) band, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400-4.835 GHz, and 5.725-5.850 GHz.

- الـ IEEE 802.11 protocols صمموا الـ protocols تبعـت 802.11 كلها تستفيد من جـءـ من الطـيف الكـهـرـوـمـغـنـاطـيـسيـ اسمـهـ unlicensed bands وـاقـعـ بـرـينـجـ الرـادـيوـ والمـاـيـكـروـوـيفـ، مـعـظـمـ هـايـ التـرـدـدـاتـ تـمـلـكـهاـ الـحـكـومـاتـ وـشـرـكـاتـ اـتـصـالـاتـ عـشـانـ تعـطـيـكـ cellular service عـلـيـهـ بـتـدـفـعـكـ اـشـتـراكـاتـ، النـاسـ المـسـؤـولـينـ عـنـ الطـيفـ الـكـهـرـوـمـغـنـاطـيـسيـ وـتـوزـيـعـهـ عـالـعـالـمـ

تركـواـ جـءـ منـ الرـادـيوـ والمـاـيـكـروـوـيفـ ماـ بـيـعـوهـ الـحـكـومـاتـ لـنـاسـ، وـمـاـ بـحـقـ لـشـرـكـاتـ الـاـتـصـالـاتـ تـدـفـعـكـ مـصـارـيـ مـشـانـهـمـ وـسـمـوـهـ industrial scientific medical band .

- الجـدولـ موـ حـفـظـ بـسـ بـدـنـاـ نـفـهـمـ مـنـهـ كلـ وـحدـةـ مـنـهـمـ بـتـشـتـغلـ عـلـىـ band وـبـنـلـاحـظـ اـنـهـ النـطـاقـاتـ ضـيـقةـ، وـفـيـ وـاحـدـ مـنـهـ infrared (معـ اـنـهـ بـرـاـ المـاـيـكـروـوـيفـ بـسـ مـدـعـومـ وـبـقـدـرـ أـسـتـخـدـمـهـ مـجـانـيـاـ باـسـتـخـدـامـ الـ ISM band) .

ولـاحـظـواـ اـنـهـ كـلـ مـاـ زـادـ الـ bandwidth عمـ بـزـيدـ الـ bitrate وـلـاحـظـواـ اـنـهـ كلـ ماـ زـادـ الـ bandwidth عمـ بـزـيدـ الـ bitrate عمـ بـزـيدـ الـ bandwidth .

لوـ بـدـنـاـ نـقـارـنـ الـ wirelessـ مـعـ الـ wiredـ لـلـ ethernetـ رـجـلـاـقـيـ انهـ higherـ اـعـلـىـ بـكـثـيرـ .



BLUETOOTH

- A wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other.
 - A Bluetooth LAN is an ad- hoc network.
 - The devices, sometimes called gadgets, find each other and make a network called a piconet.

شركة Ericsson صممت protocol stack مختلف، وهاد السبب انه ما بتقدر ال wifi نوع ثانی من ال wireless LANs .

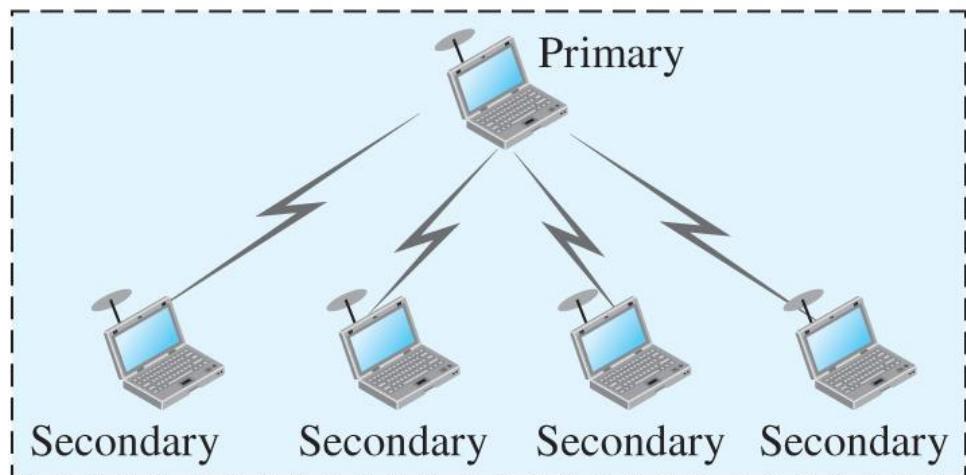
٦. Bluetooth device تحكي مع device LAN فيها کش صبغة -

- ال LAN فيها كثير صغيرة.

- ال LAN Bluetooth Ad hoc يعني ما في أجهزة معينة مختلفة عن الثانيات بمواصفات أعلى بتحكمهم أو بتحكم فيهم، كلهم زي بعض، بس هاد الاشي ما بمنع انه وحدة منهم تكون primary وتضبط الشبكة.

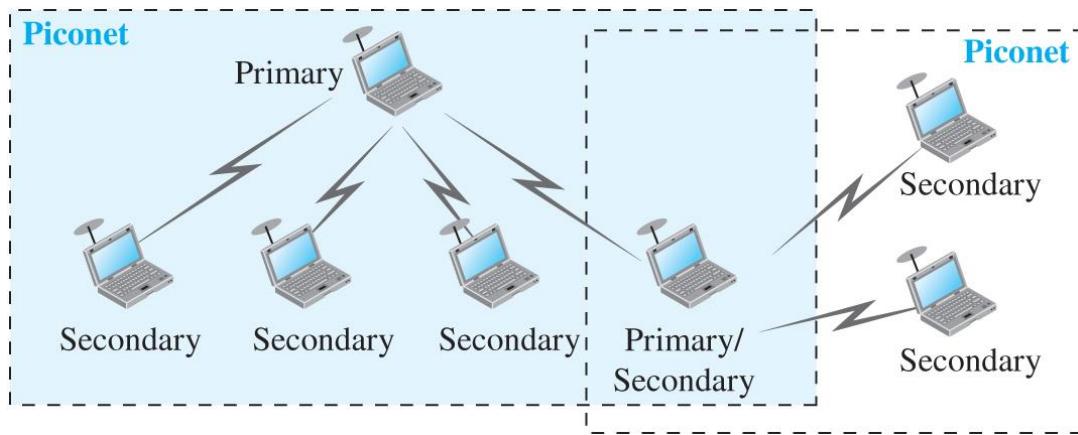
- Bluetooth defines two types of networks: piconet and scatternet .piconet or scatternet هي star topology . فعلياً الـ Bluetooth يجي بشكليين
 - Piconet (a small net): It can have up to 8 stations, one of which is called the primary; the other are called the secondaries. هي محاكاة لـ basic service set . مسافتها صغيرة (زي غرفة بالبيت).
 - كل الأجهزة الي فيها زي بعض حتى لو اسمه primary (كشكل هو infrastructure) . فعلياً هو (ad hoc).

Piconet

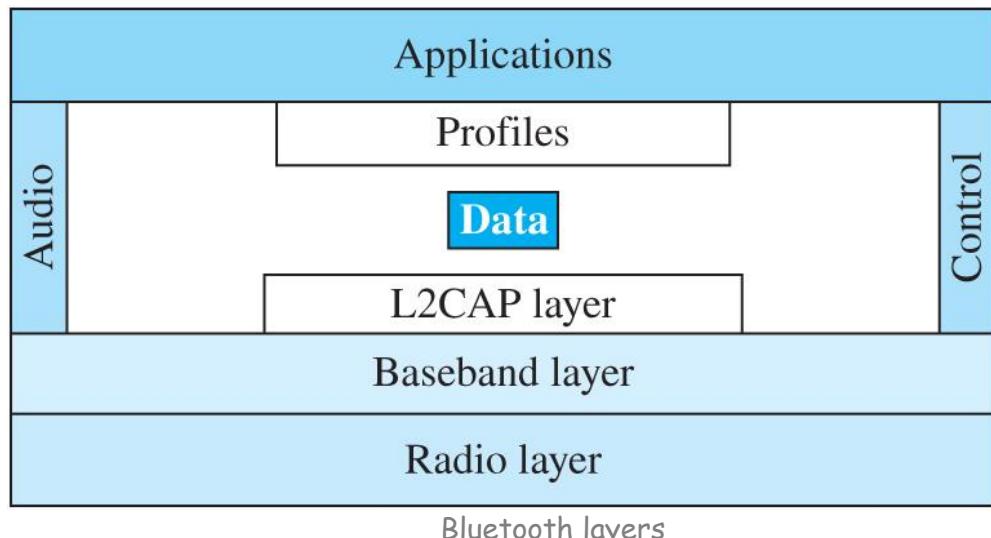


Scatternet: Piconets can be combined to create a scatternet. A secondary station in one piconet can be a primary in another one.

- هي محاكاة لـ extended service set ، عبارة عن مجموعة من الـ piconets فيةم تداخل . يعني ممكن الي يكون primary بـ piconet يكون secondary بـ another one.



- A Bluetooth device has a built-in short-range radio transmitter. The current rate is 1 Mbps with a 2.4-GHz bandwidth.



الرسمة بتعبير عن البلوتوث protocol stack مختلف عن الـ TCP or OSI . بالأول عند الـ MAC وهو محاكاة لـ baseband layer . الـ physical layer هي محاكاة لـ radio layer data link sublayer . الـ L2CAP بتشبه الـ LLC sublayer .

L2CAP: The Logical Link Control and Adaption Protocol is roughly equivalent to the LLC sublayer in LANs.

Baseband Layer: The Baseband layer is roughly equivalent to MAC sublayer in LANs.



Radio Layer: The radio layer is roughly equivalent to the physical layer of the Internet model.

Bluetooth devices are low-power and have a range of 10 m.



L2CAP data packet format

- هاد الفريم بالبلوتوث،

ال channel ID هي الـ ي تحدد مين بحكي مع مين

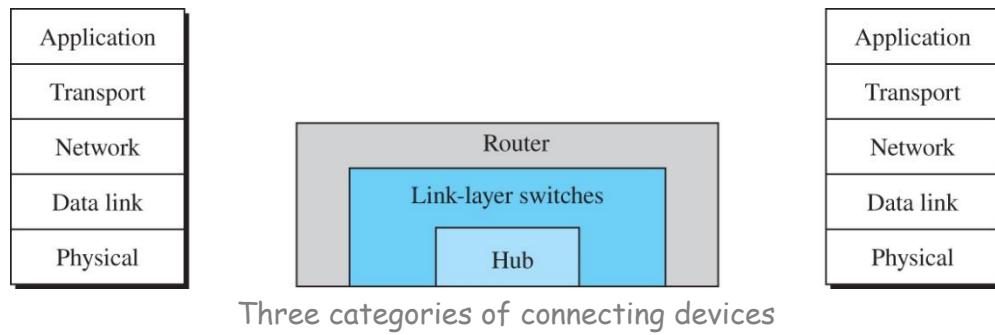
. 2 bytes = length الـ



Chapter 06: Connecting Devices And Virtual LANs

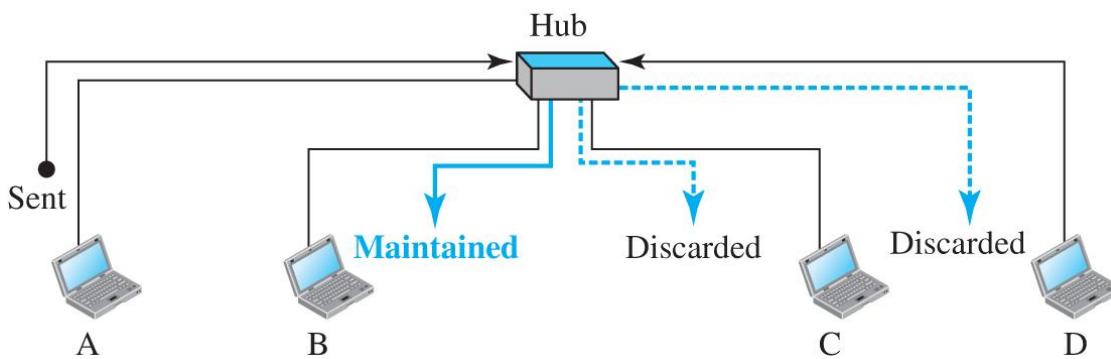
Connecting Devices

- Hosts and networks do not normally operate in isolation.
- We use connecting devices to connect hosts together to make a network or to connect networks together to make an internet.
- Connecting devices can operate in different layers of the Internet model.
- We discuss three kinds of connecting devices: hubs, link-layer switches, and routers.



Hubs

- A device that operates only in the physical layer.
- Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern.



حكينا ببداية المادة عن ال repeater الي بعيد بناء الموجة عشان إذا بلش يصير لها physical layer انه نلحقها قبل ما تضمحل تماماً، شغل ال repeater بال physical layer .
ال repeater جواته hup لما تدخل علىه الفريم تكون شايفها سلسلة من 0s and 1s على شكل موجات لأنه ما بفهم غير physical layer .



بحص إذا كان بدها amplifications بعملها تقوية بعدين بعمل إعادة إرسال لهاي الفريم على جميع المخارج الي شابكة عليه بدون تميز .
 بالرسمة A بدها تبعت لـ B ، فبعثت بالأول للـ hub بشوف إذا بدها تقوية أو لا . بعدين بكرر الرسالة على جميع المخارج ، باقي المخارج (C + D) لازم يميزوا انهم مو الـ next hope .
 وبهملوها ، وبستملها .

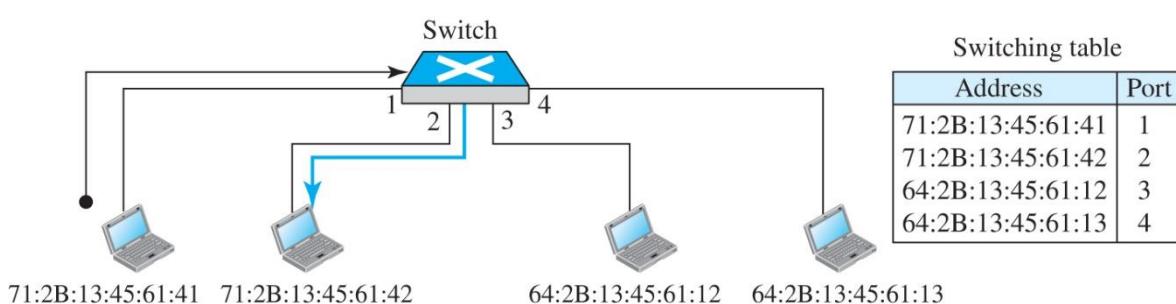
Link-Layer Switches

- A link-layer switch (or switch) operates in both the physical and the data-link layers.
- As a physical-layer device, it regenerates the signal it receives.
- As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

Filtering

- One may ask what is the difference in functionality between a link-layer switch and a hub.
- A link-layer switch has filtering capability.
- It can check the destination link-layer address of a frame and can decide from which outgoing port the frame should be sent.
- A link-layer switch has several advantages over a hub: **collision elimination** and **connecting heterogenous routers**.

الـ switch مفطي الـ repeater فهو يقوم بأعمال الـ physical + data link layer . بس هو أذكي من الـ hub انه عنده القدرة انه يعمل filtering . لأنه شايف الـ data link layer والـ MAC address وبميزة الـ next and current hopes .
 على أي مخرج لازم تنزل (منش زي الـ hub بتنزل على الكل) .
 الجدول بالرسمة يكون مكتوب فيه الـ MAC address للأجهزة الشابكين عليها .

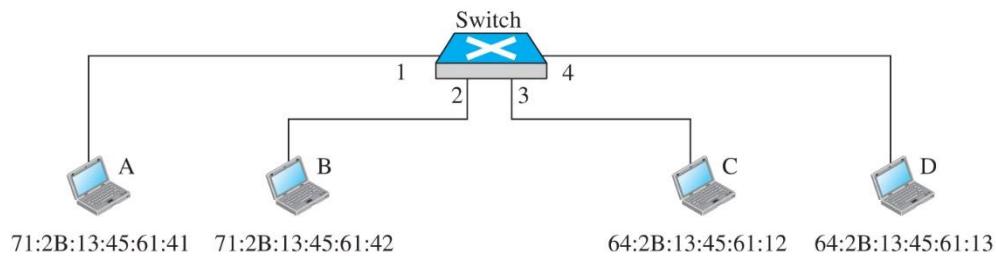


Transparent Switches

- A transparent switch is a switch in which the stations are completely unaware of the switch's existence.
- If a switch is added or deleted from the system, reconfiguration of the stations is unnecessary.

Gradual building of table

Address	Port	Address	Port
		71:2B:13:45:61:41	1
a. Original		b. After A sends a frame to D	
71:2B:13:45:61:41	1		
64:2B:13:45:61:13	4		
c. After D sends a frame to B		71:2B:13:45:61:41	1
71:2B:13:45:61:42	2	64:2B:13:45:61:13	4
d. After B sends a frame to A		71:2B:13:45:61:42	2
64:2B:13:45:61:12	3	e. After C sends a frame to D	



Learning switch

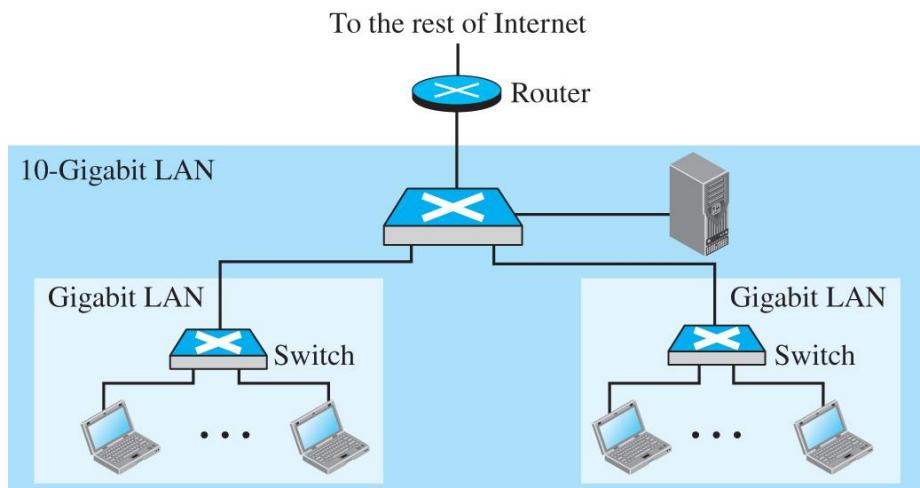
هون بشرحلي كيف الجدول بتم بناعه .
ال switch أول ما يتربك بالشبكة يكون فاضي،
بعدين بوصله أول مرة أنه A بعثت ل D فريم، فبعرف انه A شابكة ب port 1 . وبما أنه لسا
مو عارف وين port D ف رح يبعث الرسالة للكل أول مرة،
وبعدين لما يبعث D رسالة بعرف ال port تبعها ، وبكميل على هاي الناحية

Routers

- A router is a three-layer device; it operates in the physical, data-link, and network layers.

إذا بدبي أطلع ل LAN ثانية لازم استخدم الراوتر لأنه بشوف ال network layer . فهي قادرة
على تمييز ال Source + destination IP address . وظيفة الراوتر انه يتفرج على الشبكة
. source to the destination packet من ال



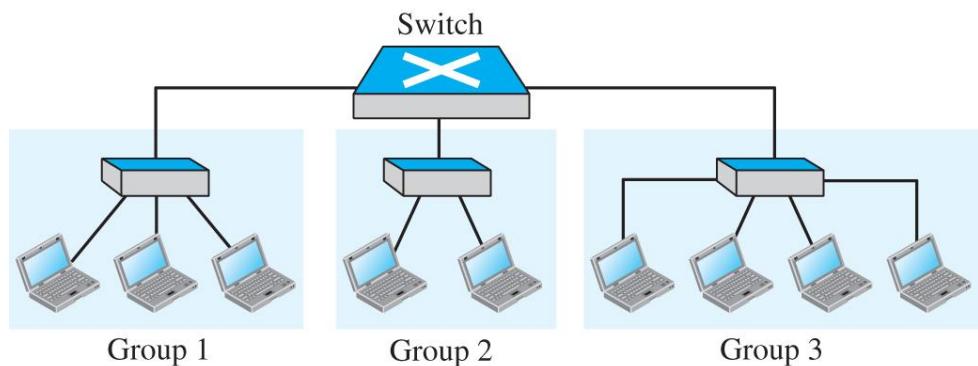


بالرسمة بنشوف ميزة بالراوتر انه في حال كنت بجي أشبك على الانترنت أو على شبكة الـ **switch** تبعها عالي ، فالراوتر عنده قدرة أكثر من الـ **bandwidth**

Virtual LANS

- A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic.
- What happens if we need a virtual connection between two stations belonging to two different physical LANs? We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

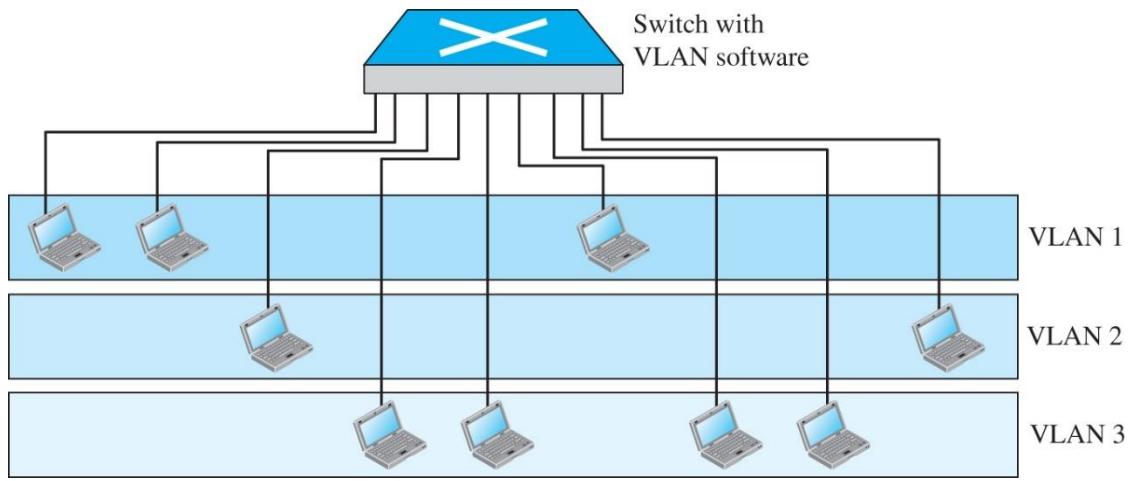
صار طبيعي مع أي **switch** ينزل معاه **virtual LANs** لل **software** انه يرجع يركب الأجهزة ب شبكات مختلفة بدون بتسمح لل **network administrator** تفكيك أي كابل أو تحريك الأجهزة، وكمانقدر يعطي صلاحيات معينة لبعض الأجهزة .



A switch connecting three LANs

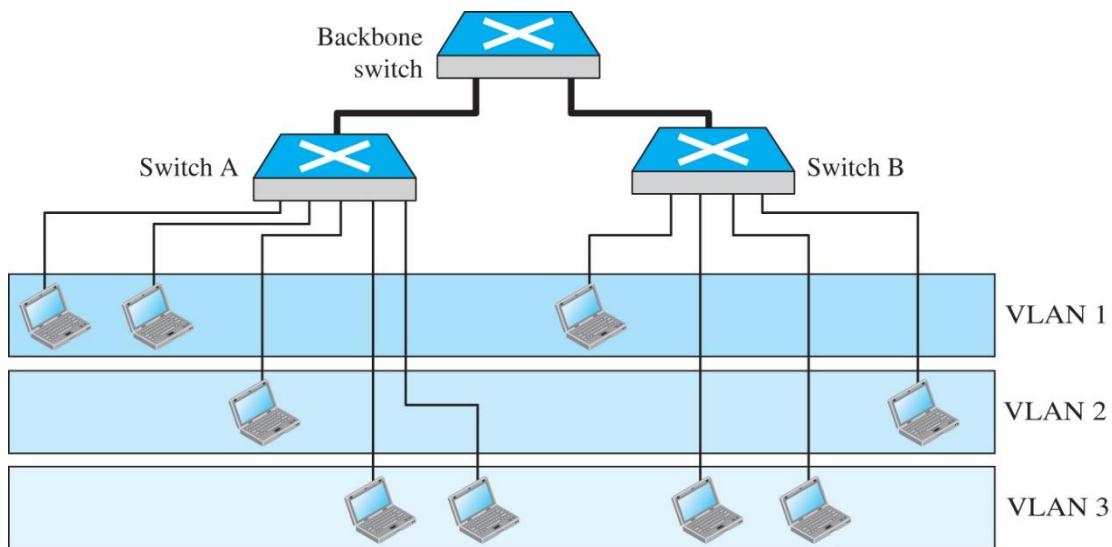
هون بالوضع الطبيعي بدون ال **V LAN** ، في **switch** مسؤول عن كل مختبر، وكلهم مسؤول عليهم **switch** كبير.





A switch using VLAN software

- فعلياً هم كلهم مشبوكين على نفس ال switch . بس كل VLAN بقدر أعمله اشي مختلف عن الثاني بدون ما كل الأجهزة تعرف.



Two switches in a backbone using VLAN software

- هون زي كأنه كلية وفيها طوابق، في مختبر بالطابق الأول وفي الثاني، فبدنا نخلي المختبرين يمتحنوا نفس الامتحان بحطمهم ب VLAN واحدة، حتى لو كان كل جهاز switch مختلف.

Membership

- What characteristic can be used to group stations in a VLAN?
Vendors use different characteristics such as interface numbers, port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these.



Advantages to using VLANs

- Cost and Time Reduction

VLANs can reduce the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.

- Creating Virtual Work Groups

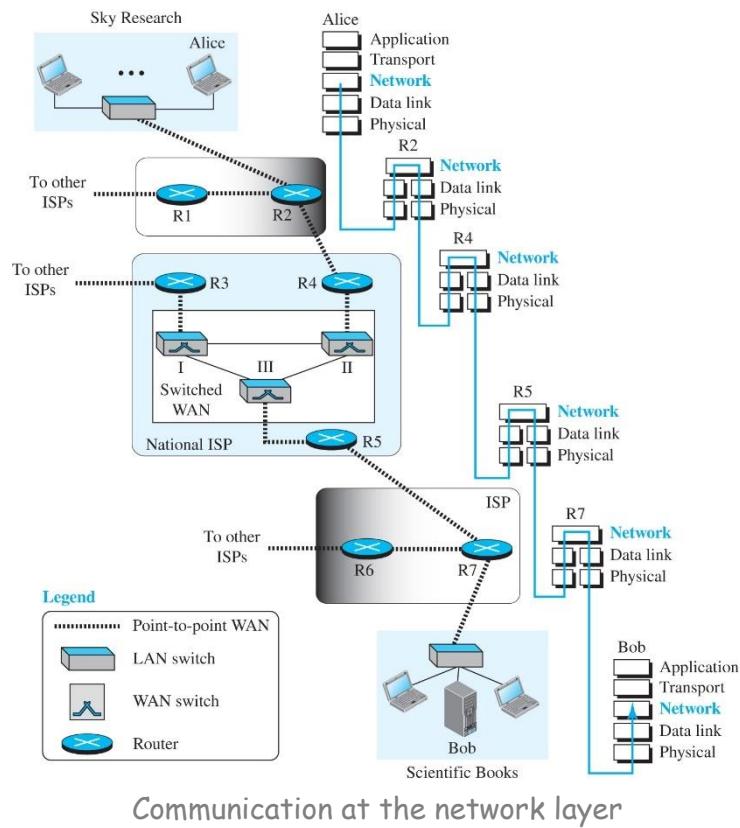
VLANs can be used to create virtual work groups. For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department. This can reduce traffic if the multicasting capability of IP was previously used.

- Security

VLANs provide an extra measure of security. People belonging to the same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.



Chapter 07: Network Layer: Data Transfer



Communication at the network layer

هون لما بعثت الرسالة تفعل ال physical packet . ال network layer . ال destination بعدين data link layer . وبعدنها interface على أي IP address على أي LAN . وبعدنها بتنزل ال frame وبعدها على ال physical layer . وبتحول لموحات وبتطلع على الشبكة .

Services

1. Packetizing

- Encapsulating the payload in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.
- In other words, one duty of the network layer is to carry a payload from the source to the destination without changing it or using it.



- The network layer is doing the service of a carrier such as the postal office, which is responsible for delivery of packages from a sender to a receiver without changing or using the contents.
- فكرة انه الداتا يتنزل من ال transport layer وبتحولها ل source IP address + destination IP ال header المركبة تتعدد ال layers (data link layer - trailer address) وفي حال ما كنت تعرف ال destination IP address بتحكي مع ال layers فوقها وتجبيه.

2. Routing

- Other duties of the network layer, which are as important as the first, are routing and forwarding, which are directly related to each other.
- هون بتاخذ قرار شو ال path الأفضل مشان ال packet تتنقل من ال source next hope (معناته بال network layer هدفنا مش بس نوصل لل destination هدفنا نوصل لل destination .(destination بذنا نفرق ما بين ال routing and forwarding ال source and destination اي أوجد أفضل طريق بين destination هو انه للراوتر الواحد بمسك ال packet وتفقد ال forwarding وبقرر أي مخرج رح يطلعها .routing يعني إذا جمع ال forwarding الي عملوا كل الراوترز على الطريق بطلع

3. Error Control

- Although error control can be implemented in the network layer, the designers of the network layer in the Internet ignored this issue for the data being carried by the network layer.
- One reason for this decision is the fact that the packet in the network layer may be fragmented at each router, which makes error checking at this layer inefficient.
- حييناها بال data link layer انها من إحدى الأشياء الي بتعملها، فال network layer بتعتبرها waste of effort لأنه ال data link layer شيكش ولو الفريم مضروبة ما بترفعها (وهاد الاشي مو بالضرورة صح ، لأنه حينا بتشابتر 3 أنه ممكن يكون الفريم مبين سليم بس هو فعلياً لا)، ف ال network layer مو معنية بال error control .



4. Flow Control

- Flow control regulates the amount of data a source can send without overwhelming the receiver.
- If the upper layer at the source computer produces data faster than the upper layer at the destination computer can consume it, the receiver will be overwhelmed with data.
- To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data.

كمان حكينا عنه بال data link layer ، وحكيانا فكرته انه سرعة إرسال الداتا تكون متزامنة مع استلامها بين ال network . current hope and next hope . بال destination source path كله (من ال source layer احنا بدننا إياها على مستوى ال path) وهوون ال IP protocol ما بعمل اشي .

5. Congestion Control

- Another issue in a network-layer protocol is congestion control.
- Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet.
- Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.

هي الاختناقالي بتصير على مستوى الراوتر . يعني ممكن يكون ال destination سريعين وما فيهن flow control بس الراوتر هو المضغوط . لأنه الراوتر بخدم ناس كثير مش بس البلاكيت الي وصلته فممكنا بيطل ملحق . فهوون كمان ال IP protocol مش معنية فيها .

6. Quality of Service

- As the Internet has allowed new applications such as multimedia communication (in particular real-time communication of audio and video), the quality of service (QoS) of the communication has become more and more important.
- The Internet has thrived by providing better quality of service to support these applications.
- However, to keep the network layer untouched, these provisions are mostly implemented in the upper layer.



- هون مثلًا كان بدننا ما يصير throughput أو delay أو jitter عالي، لكل وحدة في كود بنكتب بال header، الراوتر على الطريق في حال كان قادر يعمله بعمله وإذا لأنّ بطنش ، يعني ما بضملي ايها.

7. Security

- Another issue related to communication at the network layer is security.
- Security was not a concern when the Internet was originally designed because it was used by a small number of users at universities for research activities; other people had no access to the Internet.
- The network layer was designed with no security provision.
- Today, however, security is a big concern.
- To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service.

- ال security ما حدا لما صمم الشبكات شافه، مشان هيكل مشاكلها مزمنة وما بتتعالج والحلول تبعتها ترقيعية وممكن حلها يسبب مشكلة ثانية.

Packet Switching

- From the discussion of routing and forwarding in the previous section, we infer that a kind of switching occurs at the network layer.
- A router, is a switch that creates a connection between an input port and an output port (or a set of output ports), just as an electrical switch connects the input to the output to let electricity flow.

- فكرته أنه الرسالة بتتحول من ال Transport layer بتنزل من ال packets كل source destination packet .

- ممكن كلهم يمشوا بنفس ال path ، وممكن كل مجموعة تخضع ل path مختلف بناءً على ال current state of the network (مع إنهم كلهم بتبعوا لنفس الرسالة).

1. Datagram Approach

- When the Internet started, to make it simple, the network layer was designed to provide a connectionless service in which the network-layer protocol treats each packet independently, with each packet having no relationship to any other packet.



- The idea was that the network layer is only responsible for delivery of packets from the source to the destination.
- In this approach, the packets in a message may or may not travel the same path to their destination.

(شائع أكثر)

- هون نفس ما حكينا قبل شوي أنه مش ضروري كل ال packets الي بتنتمي لنفس الرسالة تسلك نفس الطريق، كل packet باخذه routers قرارات خاصة فيه حتى يقرروا شو أحسن طريق يمرقها منه .
- فهو ممكن لما تبعت الرسالة الوحدة تتقسم لمجموعة من ال packets، وتوصل ال packets out of order delivery .

2. Virtual-Circuit Approach

- In a connection-oriented service (also called virtual-circuit approach), there is a relationship between all packets belonging to a message.
- Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams.
- After connection setup, the datagrams can all follow the same path.
- In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.

فكرة ال Circuit switching مأخوذة من عالم الاتصالات التلفونية الأرضية، لما تتصل برقم الشخص الي بدك تحكي معه ، فيه مقسم بحجز طريق الـ path (path) كامل) لبين ما تنتهي المكالمة، كل الداتا الي بتنقل من ال source الى destination لازم يمشوا على نفس هاد ال path وأول ما تنتهي المكالمة المقسم بفترط هاد ال path، وممكن بمكالمة ثانية يرجع يحجز نفس ال path لحدا ثاني، بس خلال المكالمة ممنوع حدا ثاني يستخدمه.

بالشبكات حاولوا يعملوا محاكا لهاد الموضوع عن طريق ال virtual circuit data link layers physical layers switching sharing فكرة انها تحجز path كامل بالعكس هي بتتشجع فكرة ال virtual physically يعني صعب نعمل هاد الاشي مشان هيك بنعمله عن طريق software circuit switching (على مستوى ال).



Performance

- The upper-layer protocols that use the service of the network layer expect to receive an ideal service, but the network layer is not perfect.
- The performance of a network can be measured in terms of delay, throughput, and packet loss.
- Congestion control is an issue that can improve the performance.

1. Delay

- All of us expect instantaneous response from a network, but a packet, from its source to its destination, encounters delays.
- The **delays** in a network can be divided into **four types**: transmission delay, propagation delay, processing delay, and queuing delay.
- Let us first discuss each of these delay types and then show how to calculate a packet delay from the source to the destination.

حكينا من قبل أنه ال delay من العوامل الرئيسية لتقدير أداء الشبكة على مستوى

ال physical + data link + network layers ال

كل ما كان ال delay كا ما كان وضعنا أحسن.

• Transmission Delay

- A source host or a router cannot send a packet instantaneously.
- A sender needs to put the bits in a packet on the line one by one.
- If the first bit of the packet is put on the line at time t_1 and the last bit is put on the line at time t_2 , transmission delay of the packet is $(t_2 - t_1)$.
- Definitely, the transmission delay is longer for a longer packet and shorter if the sender can transmit faster.
- In other words, the transmission delay is:

$$\text{Delay}_{tr} = (\text{Packet length}) / (\text{Transmission rate})$$



- يعبر عن الزمن اللازم عشان ال packet ينزل إل node على الشبكة، الي بعتمد على اشيين: طول إل packet وال throughput . كلما كان طول الرسالة أكبر كلما كان إل delay أكبر كلما كان إل bitrate أعلى كلما كان إل delay أفضل كلما كان إل delay أقل.

- **Propagation Delay**

- The time it takes for a bit to travel from point A to point B in the transmission media.
- The propagation delay for a packet-switched network depends on the propagation delay of each network (LAN or WAN).
- The propagation delay depends on the propagation speed of the media, which is 3×10^8 meters/second in a vacuum and normally much less in a wired medium; it also depends on the distance of the link.
- In other words, propagation delay is:

$$\text{Delay}_{pg} = (\text{Distance}) / (\text{Propagation speed})$$

- يتحكي عن الزمن اللازم للموجة الي بتمثل الرسالة تتنقل عبر الوسيط وتقطع مسافة متيرية لتوصل لل destination .
- بعتمد على المسافة المتيرية وال propagation speed (سرعة انتقال المادة بالوسط الفيزيائي الي الموجة عم تمثي فيه -عادة تكون سرعة الضوء-).

- **Processing Delay**

- The time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).
- The processing delay may be different for each packet, but normally is calculated as an average.

$$\text{Delay}_{pr} = \text{Time required to process a packet}$$



- يعتمد على مين الي عم بعمل packet لل processing أو source and destination.

في حال كنت بحكي عن ال source and destination بده يمثلي على الباكيت من ال application layer transmission لآخر لحظة قبل ما ينعمللها .processing delay

إذا راوتر ف ال processing delay بتوقف عند ال network layer بس.

- Queueing Delay

- Let the packet is received by the destination, the packet will not be processed by the destination immediately.
- It has to wait in a queue in something called a buffer.
- So the amount of time it waits in queue before being processed is called queueing delay.
- In general, we can't calculate queueing delay because we don't have any formula for that.

$\text{Delay}_{\text{qu}} = \text{The time a packet waits in queues}$

○ الراوتر لما يستلم الباكيت ما بعملاهها processing مباشرة بدها تصف

على الدور وحسب الطابور الي قدامك رح تضل تستنى

مدة الانتظار لبين ما يفضي اسمها ال .queueing delay

○ علمياً فكرة انه لا يقاس غلط بنقدر نقطته بس الموضوع معقد شوي.

- Total Delay

- Assuming equal delays for the sender, routers, and receiver, the total delay (source-to-destination delay) a packet encounters can be calculated if we know the number of routers, n , in the whole path.

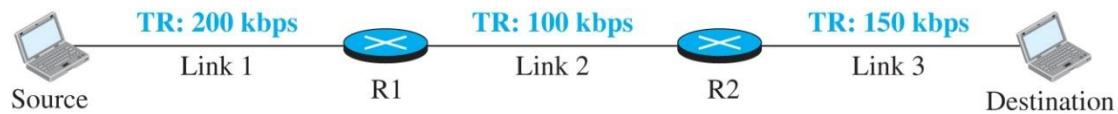
$$T_{\text{total}} = T_t + T_p + T_q + T_{\text{pro}}$$

2. Throughput

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.



- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.



a. A path through three links

TR: Transmission rate

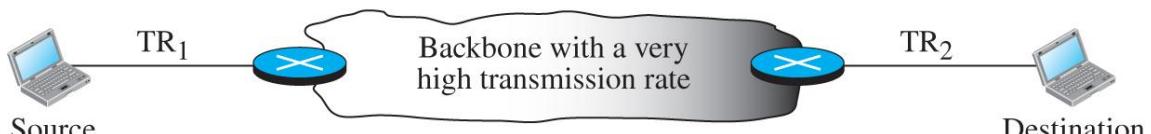


b. Simulation using pipes

Throughput in a path with three links in a series

احنا هون عم نحكي عن ال network layer . فال throughput هو على مستوى ال path كاملاً. ف رح ننطلع عليه على كل link لحال. وأكيد إذا كانت الشبكة كبيرة فمش كل ال links إلها نفس ال bitrate. طيب بيهاي الحالة كيف بدننا نحسب ال path throughout بال path؟ دائمًا اللي بتحكم فيه هو الحلقة الأضعف. يعني بيهاد المثال بنطلع ال link وبعدها بنشوف أقل قيمة وهي اللي بتكون overall throughout

TR: Transmission rate



A path through the Internet backbone

3. Packet Loss

- Another issue that severely affects the performance of communication is the number of packets lost during transmission.
- When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
- A router, however, has an input buffer with a limited size.
- A time may come when the buffer is full and the next packet needs to be dropped.



- The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.
- بحكي عن قديه أنا بخسر packets على الطريق ما بين ال source and destination، بال network layer أهم سبب بخليني أخسر packets هي مساحة الراوتر، بتيجي ال packet على الراوتر وبدها تصنف على ال queue وما في دور فيه فال packet بتوقع.

4. Congestion Control

- Congestion control is a mechanism for improving performance.
 - Although congestion at the network layer is not explicitly addressed in the Internet model, the study of congestion at this layer may help us to better understand the cause of congestion at the transport layer and find possible remedies to be used at the network layer.
 - Congestion at the network layer is related to two issues, throughput and delay, which we discussed in the previous section.
- وجود ال congestion من عدمه هو مقياس لأداء الشبكة
- كلما كان أخف كلما كان أفضل، أما إذا كان مزمن ف رح يصير عنا مشاكل رح تأثر على أداء الشبكة.

Internet Protocol Version 4

- The network layer in the Internet has gone through several versions, but only two versions have survived: IP Version 4 (IPv4) and IP Version 6 (IPv6).
- Although IPv4 is almost depleted, we discuss it because there are still some areas that use this version and also because it is the foundation for IPv6.

IPv4 Addressing

- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.



- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.

ال IPv4 هو ال version اي احنا معنيين فيها . -

ال IP addressing مسؤولة عن ال logical addressing (حينا من قبل أنه في حال كنا بدننا نحي مع حدا خارج ال LAN اي موجودين فيها وبينا وبينه راوتر ما بنقدر نعنونه إلا باستخدام ال IP address. ال IP address اي بتم منحه لجهاز ممكن يكون ثابت وممكن متغير) . -

ال IP address هي ال Network Interface Card . -
ال IP address يتكون من 32 bit (يعني .4 bytes) -

Address Space

- A protocol like IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses b bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion). If there were no restrictions, more than 4 billion devices could be connected to the Internet.

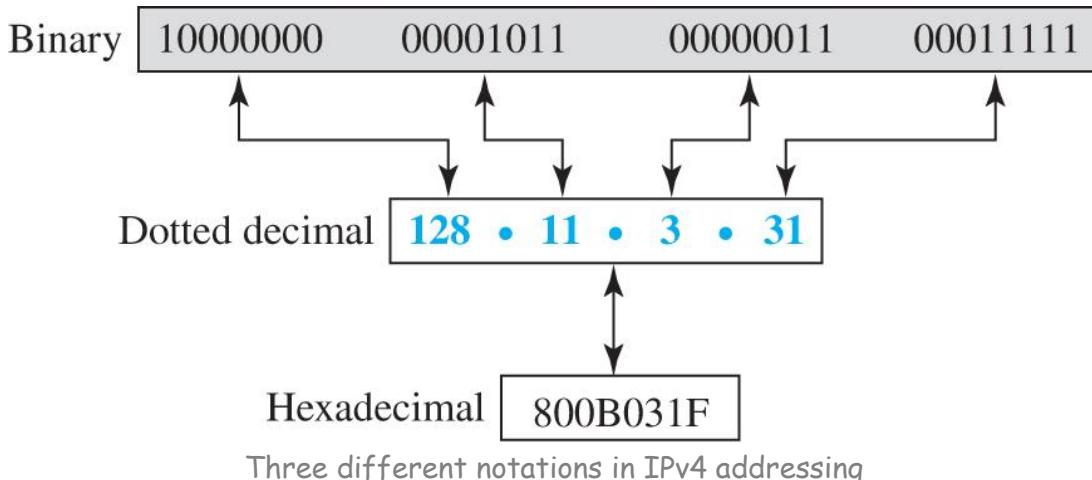
حينا انه ال IP addresses اي بيتكون من 32. معناته ال IP address . -
ممكن انشائها = 2^{32}

نظريًا بنقدر نطلع ال 4 billion addresses على الانترنت، بس عمليًا لا، في نسبة منهم بتكون طالعة على الانترنت والباقي بنسميهم private Ip addresses غير مسموح باستخدامها على الانترنت.

Notation

- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 10): between 0 and 255, and hexadecimal notation (base 16).





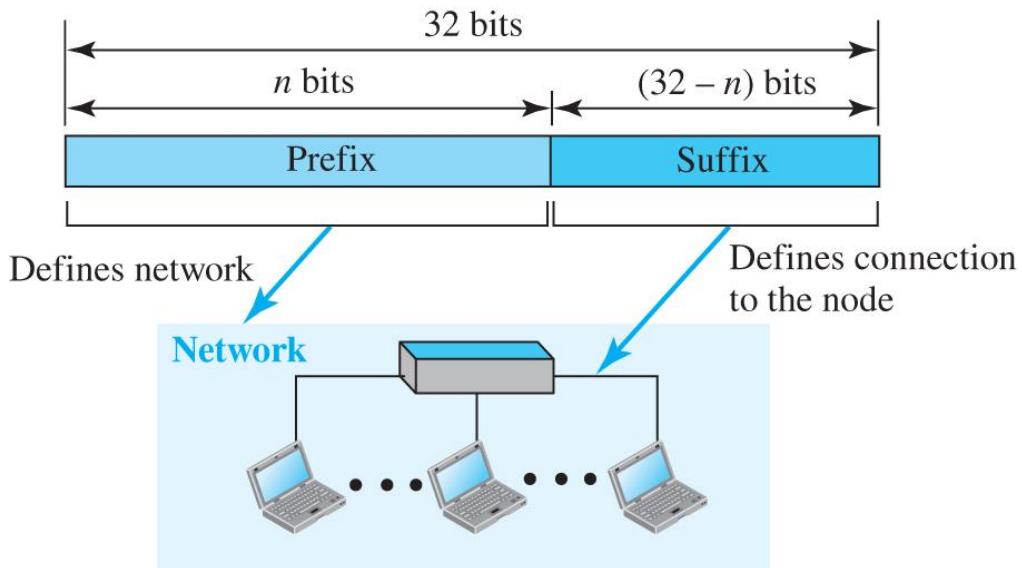
Three different notations in IPv4 addressing

- إل binary عبارة عن 4 مجموعات وكل مجموعة تكون بكون فيها 8 bit . ما بنتعامل بهاي الطريقة لأنه صعب نكتب .32 bit
- بنأخذ كل byte = octet من binary وبنحوله من رقم بالعشري، وبنفصل بين كل بايت وبأيت بنقطة.
- أصغر قيمة مسموحة لل 0s = binary (وبتكون بال 0s) وأكبر قيمة = (وبال 1s = binary 8) - يعني لازم إل IP address يكونوا بينهم .
- أكثر اشي دارج للتعبير عن إل IP address هو إل Hexadecimal.
- بال 8 hexadecimal digits كل byte يمثلوها ب 4 bit (يعني من كل 8 hexadecimal numbers تكون عدي 2) وبالأخير تكونوا بينهم 8 hexadecimal digits = IP address ** للتذكير بس إل IP address وما في بينهم : (يعني مختلف عن إل Mac address).

Hierarchy in Addressing

- In any communication network that involves delivery, such as a telephone network or a postal network, the addressing system is hierarchical.
- A 32-bit IPv4 address is also hierarchical but divided only into two parts.
- The first part of the address, called the prefix, defines the network; the second part of the address, called the suffix, defines the node.





الـ IP address ينقسم إلى **prefix** و **suffix** : جزء اسمه هو **prefix** و جزء آخر هو **suffix**. يستخدم **prefix** للتعبير عن رقم الشبكة (Network) الذي هو في لها. يستخدم **suffix** للتعبير عن رقم الحاسوب (node) الذي هو في الشبكة (LAN).

Classful Addressing

- When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one ($n = 8$, $n = 16$, and $n = 24$).
- The whole address space was divided into five classes (class A, B, C, D, and E), as shown in the Figure.
- This scheme is referred to as classful addressing.
- Although classful addressing belongs to the past, it helps us to understand classless addressing, discussed later.

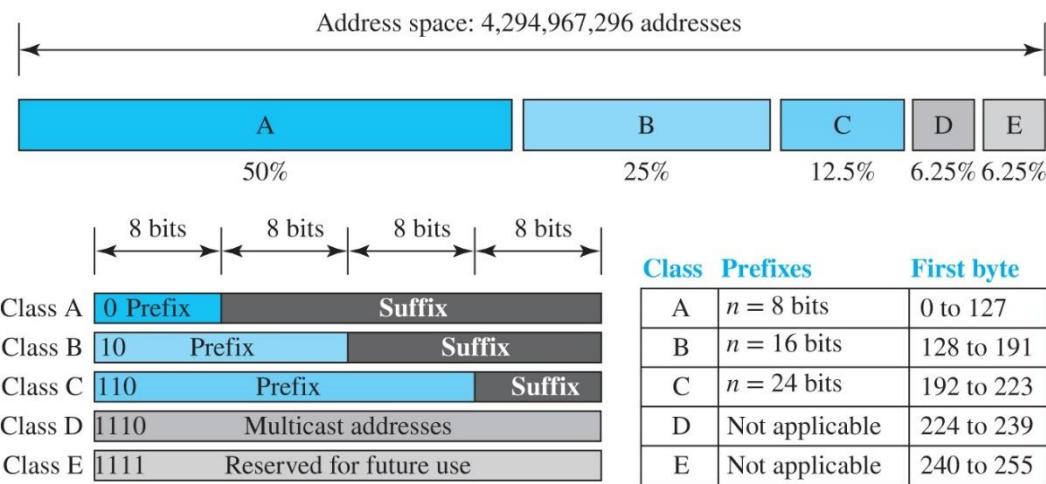
Class	Number of Blocks	Block Size	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved



- ال classful addressing نادر جدًا حدا يستخدمه هلا، الأغلب يستخدم ال classless addressing . بس بناخذه لأنه مقدمة لل العلماء حكوا وبين المفروض يكون الفاصل بين ال suffix and prefix ، يعني كم n المفروض تكون لل prefix ونترك الباقي لل suffix ؟ أول ما قسموا ال IP addresses تبعـت الانترنت قسموها حسب حجمها (عملقة، متوسطة، صغيرة)

الي بده ياخـذ IP addresses لشبـكة عملقة بروح على class A
الي بده ياخـذ IP addresses لشبـكة متوسطة بروح على class B
الي بده ياخـذ IP addresses لشبـكة صغيرة بروح على class C
وبـقي ال addresses ما بطلعـوه على الانترنت بخلـوه لاستخدامـات خاصـة جـزء منـهم محـجـوز لـ multicast
والـباقي بـخلـوه للـ private network لـي بـده يـعمل reserved وما يـطلع على الانترنت بـس بـده يـعمل شبـكة صـغـيرة .
. -24 = suffix class A انه ال 8 = prefix (8 = prefix يعني ال 8 = suffix) معـناـته ال 8 = prefix Class B (16 = suffix) يعني ال 16 = prefix Class C (ال 8 = suffix 24 = prefix) Class C
لـما نطبق 2^n ونـحط مكان ال n ال بـطلعـلي كـم عـدد الشـبـكات المـخـتلفـة
الي بـنـقـدر نـنـشـأـها (How many different networks I can create within)
. (Number of blocks) (الي بالـجدـول اـسـمـها this class)
ولـما أحـط مكان ال n ال 2³²⁻ⁿ suffix بـطلعـ عدد ال PCs الي بـنـقـدر نـعـونـها بالـشبـكة الـوـحدـة (عدد ال prefixes) الي بالـsuffixes (بالـجـدول الـواـحدـ) (بالـجـدول هي block size)
لو اـنـتـبهـنا بالـجـدول رـحـ نـلـاحـظـ انهـ الـأـرـقـامـ تـبـعـتـ الـnum~ber of blocks مشـ زـيـ الحـسـابـاتـ ، يعني class A المـفـروـضـ تكونـ = 265 ، شـوـ السـبـبـ ؟





Occupation of the address space in classful addressing

قرروا أنه يكون في طريقة مباشرة لما نطلع على ال IP address -

هل هو من أول نظرة . Class A or B or C or D or E

مسكوا ال IP address تبع ال binary notation -

أي آخر bit فيه (أقصى اليسار) ببدأ ب 0 بنعتبره class A، معناه

هيك احنا بصير عنا مجال نستخدم من ال 7 bit بس . مثـان هـيك

$$\text{بكون } 128 = 2^7$$

حددوا ال class B الي موجودين أقصى اليسار بال 2 bits = prefix

$$16,384 = 2^{14} = \text{number of blocks}$$

$$.2^{21} = \text{number of blocks}.110 = 3 \text{ bits Class C}$$

32 هو prefix and suffix عن ما في . 1110 = 4 bits Class D

$$2^{28} = \text{number of blocks} . \text{bits}$$

$$.1111 = 4 \text{ bits Class E}$$

Class	Number of Blocks	Block Size	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

الجدول الأول نفس الـ حكيناه قبل بس انتبهوا أنه ال class A+B+C هي -

.reserved E و multicast D هي أما unic平



- الجدول الثاني هي طريقة كلاسيكية كانوا يستخدموها للتعبير عن ال prefix + reserved IP addresses . اصطلحوا انهم يأخذوا مجموعة من ال suffix بتسلس بال 1s = prefix . 0s = suffix .

- مثلاً ب ال 1s = prefix 8 يعني عنا 8 والباقي 0s .

- 9 classful (Classless Inter-Domain Routing) CIDR : بقدر أمثل فيه ال classful . إذا كان من ال classless ، بنعبر عنه عن طريق /prefix . مضاعفات ال 8 أما إذا classless فمش بالضرورة .

Classless Addressing

- With the growth of the Internet, it was clear that a larger address space was needed as a long-term solution.
- The larger address space, however, requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed.
- Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization.
- The short-term solution still uses IPv4 addresses, but it is called classless addressing.

- وحدة من مشاكل ال classless addressing هي الهدر . لو عنا مؤسسة وبدها IP address 10000 . وكنا على وقت ال classful address ف رح نضطر نستخدم واحد من class A or B or C . وفعلياً هاد الاشي غلط لأنه رح يخلينا المؤسسة تتكلف أضعاف المبلغ وبتخسر مشان هيك اجي محله ال classless addressing . ال classless addressing بعطي الشركة أكثر بشوي من احتياجاتها بس ما تكون في قفزة كبيرة .

Classless Addressing

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.



Address Blocks

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

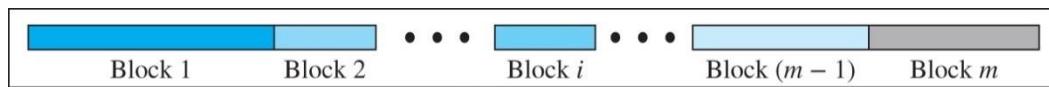
Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...).
3. The first address must be evenly divisible by the number of addresses.

في عنا 3 شروط مشان يكون الـ *classless addressing* صح (زمان حكينا عن

فكرة أنه في مؤسسة بأمريكا هي المسؤولة عن توزيع الـ *IP addresses* عالعالم كله ، بتبعها مجموعة من الـ *ISP* مسؤولين عن القارات وكل قارة مقسمة لأماكن إقليمية والأقاليم فيها مجموعة من الدول. فمزودي الخدمات المحليين (زي زين وأورانج) بجيروا النت من مزود الخدمات الإقليمي. مزود الخدمات الإقليمي بعطيهم *block* أو أكثر، هاد الـ *block* لازم يحتوي على شروط وإلا الـ *ISP* ما بقدر يعطيه):

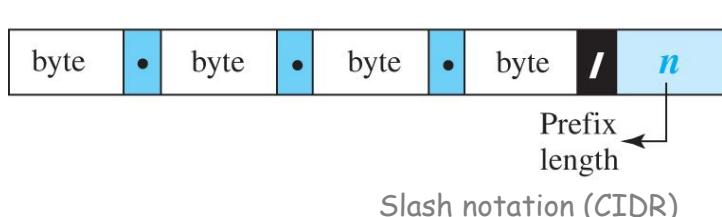
- الـ *IPs* الموحدة بالـ *block* لازم تكون متسلسلة
- حجم الـ *block* لازم يكون من قوى الـ 2 . **مش مضاعفات**
- عنوان الـ *address* الأول لازم يقسم على حجم الـ *block* بدون باقي



Address space

Variable-length blocks in classless addressing

مزود الخدمات لما بده يوزع الـ *IP addresses* على الـ *zbyain* تبعونه مش ضروري يعطيهم كلهم نفس الـ *block* ، هو لما يأخذ الـ *IP addresses* من مزود الخدمات الإقليمي تكون مقسم الـ *zbyain* لقطاعات (أفراد، شركات صغيرة، شركات كبرى....) فبكون عارف انه الشركات الكبرى بدها بـ *blocks* بحجم أكبر



Examples:

12.24.76.8/8
23.14.67.92/12
220.8.24.255/25



هون عم برجع بذكرنا بال slash notation -
 بنكتب ال IP address بس يخلص بنحط /n = طول ال prefix -بنقدر نسميه
 ال mask .

Notes

- In IPv4 addressing, a block of addresses can be defined as $x.y.z.t/n$ in which $x.y.z.t$ defines one of the addresses and the $/n$ defines the mask.
- The first address in the block can be found by setting the rightmost $32 - n$ bits to 0s.
- The last address in the block can be found by setting the rightmost $32 - n$ bits to 1s.
- The number of addresses in the block can be found by using the formula 2^{32-n} .

Example

A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is $2^{32-n} = 25 = 32$ addresses. The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01010010
First address: 167.199.170.64/27	10100111	11000111	10101010	01000000

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/27	10100111	11000111	10101010	01011111
Last address: 167.199.170.95/27	10100111	11000111	10101010	01011111

suffix 27 = prefix ال . معناته ال 167.199.170.82/27 = IP address ال -
 رح يكون .5 = 32-27



أول 5 bits هم ال suffix أماباقي prefix ، وبالتالي كل ال octet بنقريب عليهم إلا ال 82 لأنه جزء منها بال prefix وآخر 5bit suffix .
أول خطوة بتحول ال 82 ل binary :
ال 82 شو أول وأكبر قوة لل 2 قريب منها؟ ال 64

2^7	2^6
<u>0</u>	<u>1</u>

$$16 = 18 - 64 - 82$$

2^7	2^6	2^5	2^4
<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>

بضل 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
<u>0</u>	<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>1</u>	<u>0</u>

أول 5 على اليمين اسمهم suffix
مشان نعمل منهم أصغر قيمة ممكنة بتحط فيهem 0s

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
<u>0</u>	<u>1</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>

وأول 3 ما بنقريب عليهم لأنهم prefix
= 167.199.170.0100000 : IP address
بططلع معنا ال 167.199.170.64

هاد هو ال first address
مشان نجيب ال last IP address لازم يكون أكبر واحد بالبلوك . كيف بنقدر نعتبر
أول 5 bits أكثر اشي؟ بنخليلهم 1s :
167.199.170.01011111
(last IP address هاد هو ال 167.199.170.95/27)

Example

Another way to find the first address, the last address, and the number of addresses is to represent the mask as a 32-bit binary (or 8-digit hexadecimal) number. This is particularly useful when we are writing a program to find these



pieces of information. For example for the block 205.16.37.39/28, the mask is represented as

11111111 11111111 11111111 11110000

(twenty-eight 1s and four 0s).

Find

- a. The first address
- b. The last address
- c. The number of addresses.

a. The first address can be found by ANDing the given addresses with the mask. ANDing here is done bit by bit. The result of ANDing 2 bits is 1 if both bits are 1s; the result is 0 otherwise.

Address:	11001101 00010000 00100101 00100111
Mask:	11111111 11111111 11111111 11110000
First address:	11001101 00010000 00100101 00100000

بالطريقة هاي بنحط ال mask كل ال binary 1s prefix -
وبنعمل AND مع ال IP address الأصلي . وهيك بنطلع ال
.first address

b. The last address can be found by ORing the given addresses with the complement of the mask. ORing here is done bit by bit. The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise. The complement of a number is found by changing each 1 to 0 and each 0 to 1.

Address:	11001101 00010000 00100101 00100111
Mask complement:	00000000 00000000 00000000 00001111
Last address:	11001101 00010000 00100101 00101111

ال last address عن طريق ال ORing مع ال Mask complement -
(بنقلب ال 0 و ال 1).



c. The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.

Mask complement: **000000000 000000000 000000000 00001111**

Number of addresses: $15 + 1 = 16$

الblock size -
وبنجمعله 1 . وبنجده عن طريق تحويل ال decimal J mask complement

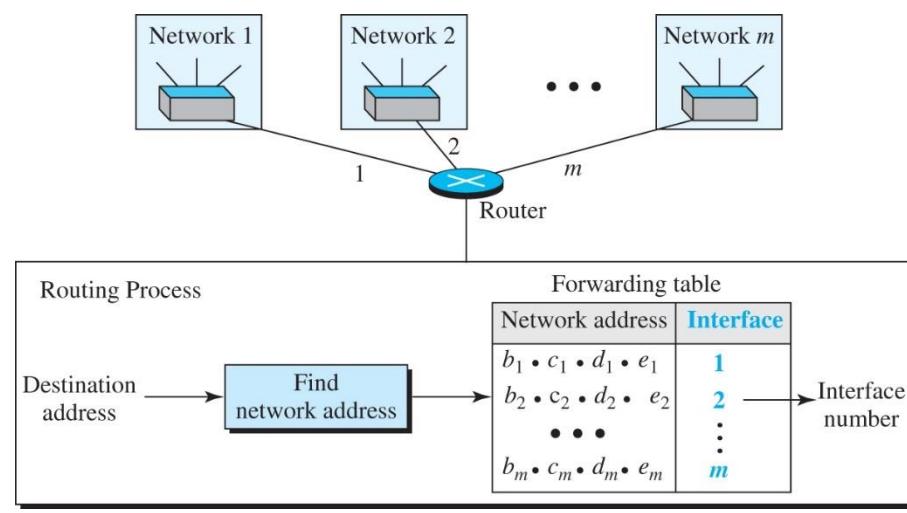
Example

In classless addressing, an address cannot per se define the block the address belongs to. For example, the address 230.8.24.56 can belong to many blocks. Some of them are shown below with the value of the prefix associated with that block.

1110 0110.0000 1000. 0001 1000. 0011 1000

Prefix length:16	→	Block:	230.8.0.0	to	230.8.255.255
Prefix length:20	→	Block:	230.8.16.0	to	230.8.31.255
Prefix length:26	→	Block:	230.8.24.0	to	230.8.24.63
Prefix length:27	→	Block:	230.8.24.32	to	230.8.24.63
Prefix length:29	→	Block:	230.8.24.56	to	230.8.24.63
Prefix length:31	→	Block:	230.8.24.56	to	230.8.24.57

الفكرة من هاد المثال انه ال IP address بدون ال Mask address (ضروري
نحدد ال mask قديه طوله).



- الصورة بتشرح كيف الراوتر بتعامل مع ال IP addresses

الراوتر يكون عنده forwarding table مكتوب فيه الوجهات التي يعترف فيها ، شو ال destination IP addresses التي يفهمها وكل وحدة على أي مخرج destination IP لازم تنزل، الراوتر ما يقدر يحدد بدون ما يعرف ال mask لكل IP address بالجدول اسمه Network address ما يحكي عن ال destination PC محدد .
 بحط لل networks الكبيرة التي موجود هدول ال PCs جواها وبكون معاهem Mask .
 كيف الراوتر بقرر ال interface؟ بتطلع على البلاكيت التي بتدخل عنده على ال Addresses ANDing مع ال destination IP address masking لحد ما ال mask يزيط، أول وحدة بزيط معها ال Routing table تعتبرها ال destination (يمكن هلأ الفكرة مش مفهومة كثير بس لقادم مع الأمثلة بنفهمها).

Example

An ISP has requested a block of 1000 addresses. Since 1000 is not a power of 2, 1024 addresses are granted.

The prefix length is calculated as $n = 32 - \log_2 1024 = 22$.

An available block, 18.14.12.0/22, is granted to the ISP.

It can be seen that the first address in decimal is 302,910,464, which is divisible by 1024.

- هون بس بده يورجينا أنه مش بالضرورة يعطينا ال prefix ويطلب ال suffix .
 ممكن العكس.

Example

An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

Solution



There are $2^{32-24} = 265$ addresses in this block. The first address is 14.24.74.0/24; the last address is 14.24.74.255/24. To satisfy the third requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one.

. $265 = 2^8$ = block size -
ال معناته ال 8 = suffix ، يعني ال 24 = prefix -
ال subblocks الي رح نحصل عليها بدها تكون لازم ال prefix تبعها يكون أكبر
من 24.

ال 24 ما رح نشتغل عليهم، وال 8 رح نأخذ الجزء الي موجود أقصى الشمال فيها
ونضيفهم على ال suffix والمتبقي هو ال prefix .
ال blocks الي احنا بدننا إياهم (مشان نحدد البلاوك بدننا 3 أشياء: ال + suffix + أول
: (address + address

SubLAN1

- The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$. The first address in this block is 14.24.74.0/25; the last address is 14.24.74.127/25.

فيها 120 حاسوب -
حسب الشروط ال 3 الي حكيناهم فوق في وحدة منهم هون مش موجودة وهي
إنه ال 120 مش قوة ال 2 ف رح نخليها 128
إذا الحجم 128 معناته ال 7 = suffix -
إذا ال prefix الجديد = 25 معناته
أول 14.24.74.0/25 = IP address
ال 14.24.74.127/25 = last IP address

SubLAN2

- The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$. The first address in this block is 14.24.74.128/26; the last address is 14.24.74.191/26.

فيها 60 حاسوب -
رح نخليها 64 مشان نمشيها على الشروط
ال 26 = prefix ال 6 = suffix -



الى 14.24.74.128/26 = first IP address -
قبله)

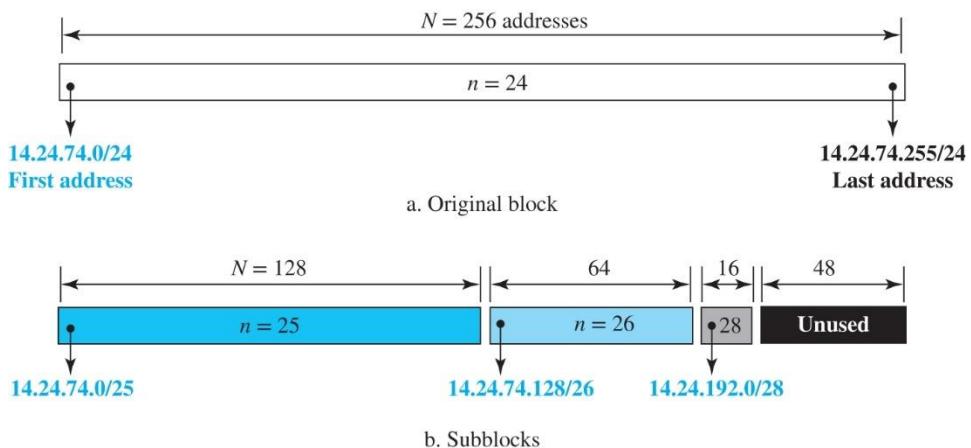
الى 14.24.74.191/26 = last IP address -
SubLAN3

- The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_3 = 32 - \log_2 16 = 28$. The first address in this block is 14.24.74.192/28; the last address is 14.24.74.207/28.

فيها 10 حواسيب -
تحت نظريها 16
28 = prefix 4 = suffix -
الى 14.24.74.192/28 = first IP address -
الى 14.24.74.207/28 = last IP address -

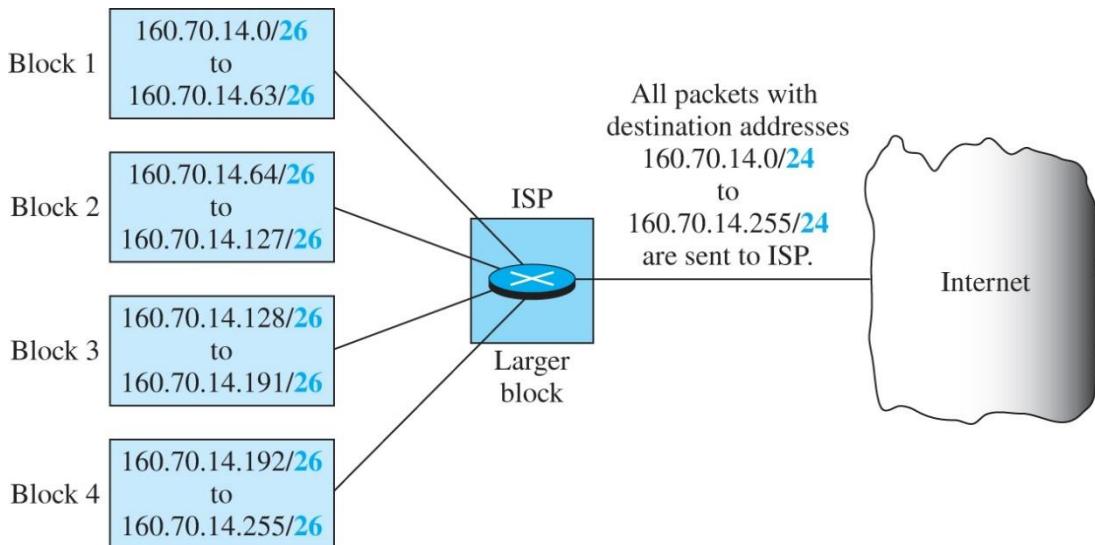
- If we add all addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve. The first address in this range is 14.24.74.208. The last address is 14.24.74.255.

. وبنلاحظ أنه ما استهلكنا كل الـ 256 لأنه احتياجنا 208 -
. يعني علـ 48 extra IP addresses



. هون بالرسمة عم بورجينا وين قطعناهم وراحوا ل LAN1 -
من 0 - 127 قطعناهم وراحوا ل LAN2 . ومن 192 - 207 قطعناهم وراحوا
ل LAN3 ، بضل 48 لوقت الحاجة .





Example of address aggregation

- Figure shows how four small blocks of addresses are assigned to four organizations by an ISP. The ISP combines these four blocks into one single block and advertises the larger block to the rest of the world. Any packet destined for this larger block should be sent to this ISP. It is the responsibility of the ISP to forward the packet to the appropriate organization. This is similar to routing we can find in a postal network. All packages coming from outside a country are sent first to the capital and then distributed to the corresponding destination.

الـ ISP يعطي مؤسسة كبيرة بلوك كبير من الـ IPs زي الي بالصورة، وقسموا لـ 4 بلوك (وبنلأحظ انه الهم نفس الحجم)، الـ router تبع الـ ISP لما تيجي الـ traffic تبعث الانترنت عليه وبده يعملها على الثانية ما يكشف الـ 4 بلوك الي عاملينها، يكشف بس الـ block الأصلـ (تابع الـ 24)-ولقدام رح نفهمها أكثرـ .

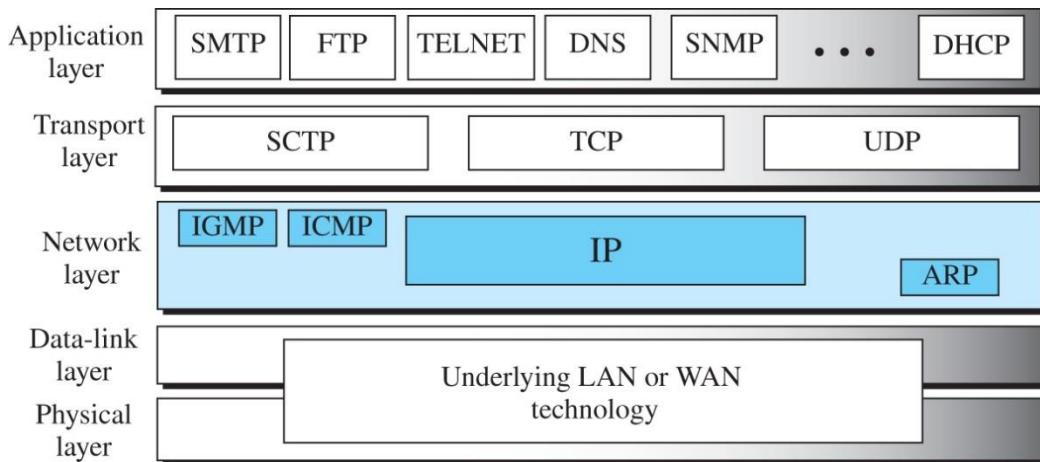
Four Related Protocols

- The network layer in version 4 can be thought of as one main protocol and three auxiliary ones. The main protocol, IPv4, is



responsible for packetizing, forwarding, and delivery of a packet.

The ICMPv4 helps IPv4 to handle some errors that may occur in delivery. The IGMP is used to help IPv4 in multicasting. ARP is used in address mapping.



Position of IP and other network-layer protocols in TCP/IP protocol suite

هون عم بورجونا بنية ال Network Layer . وأنها ما بتتألف بس من ال IP protocol (بس هو ماذن الحصة الأكبر)، مع هيك حكينا من قبل عن الأشياء الي ما بعملها ال IP protocol مثل جودة ال routing (لدرجة أنه ما بحكي إذا ال packet وقعت)، فباقي البروتوكولات بتعزز شغل ال IP، مثل ال ICMP وظيفته يدور ويبلغ عن الأخطاء + error reporting .Multicasting وظيفته يعني بال health check لاحظوا انه ال ICMP + IGMP مرسومين شوي لفوق لأنهم بقربونا لل Transport Layer .
ال ARP وظيفته address resolution أنه أعرف ال MAC address للجهاز الي عندي ال IP address تبعه (وبقدر يعمل العكس وبنسمه reserved ARP) حكينا عنه شوي بتتشابتر 3 ورح نرجع نحوكي عنه لقدمام).

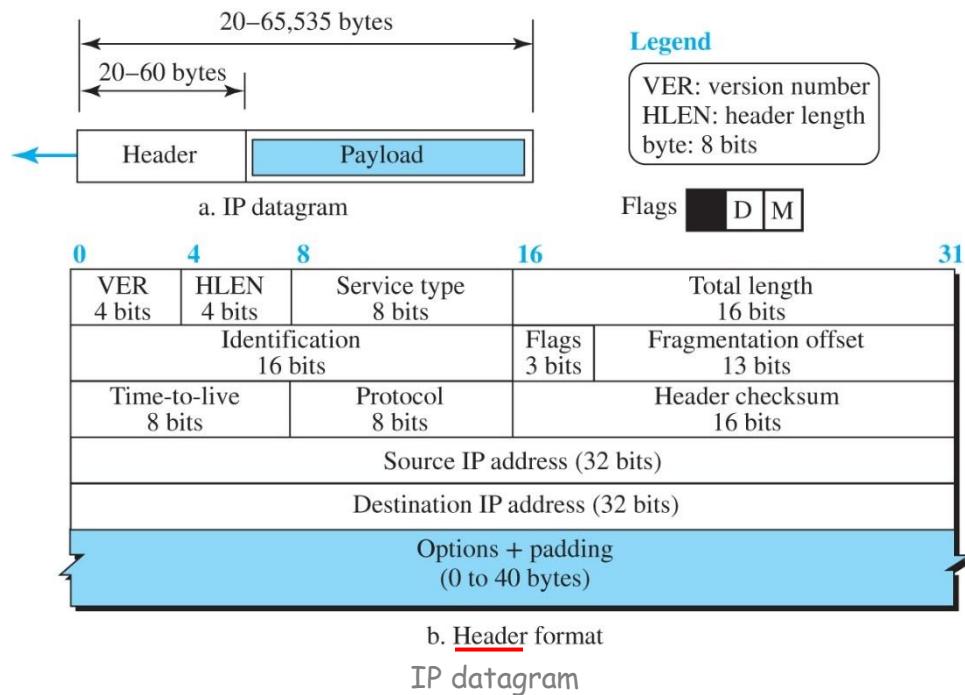
Datagram Format

- Packets used by the IP are called datagrams.



- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.
- It is customary in TCP/IP to show the header in 4-byte sections.

اسمهها (IP packet) أو datagram لأنه بالعادة يستخدموا بالانترنت اشي اسمه ال packet switching لأنه كل packet على راسه ، يعني لو عندي مجموعة من الباكيت وبدى أنقلهم وال application بده رسالة كبيرة فرح نكسر الباكيت وهو شرط كلهم يسلكوا نفس الطريق، يعني ما في اشي بلزمهم أنه يحجزوا نفس الطريق لهم كلهم.



ال packet تكون من 20 bytes . ال header + body . ال header + body ييتكون من 20 bytes .
الأدنى(وهما بالعادة تكون control message مسج من راوتر لراوتر بدون header + payload)، إذا معك 60 bytes .
الحد الأقصى (user data) . 65,535 bytes ما بتتجاوزوا ال payload .

ال 20 bytes مقسمينهم بالرسمة على 5 أسطر وبكل سطر 4 bytes (حفظ بالترتيب):

السطر الأول: أول 4 bits لـ Version (إلي احنا معتمدينها هلاً هي 4 يعني ال 1 . 0100 = 4 bits)



الي بعده لـ header length (الي بنكتب لال) هو الطول مقسوم على 4 ، يعني لو كان مكتوب 15 يكون فعلياً طوله 60 (يعني لازم ال HLEN يكون ما بين 5-15). بس هيك في حال كان عندي الحجم الأصلي 21 ما بربط نقسمه على 4 شوي بنعمل؟ بنعمل Padding وبنخلify ال size يصير 24 .
ال الأمانيات الي بدنها اياها للراوتر في حال قدر يعملها بعملها (بس مش ضروري أي اشي بنحطه يعمله).

الا 16 bits = Total length 2 bytes = الطول الكلي للباكيت، وبنحتاج الى 16 bits
نقدر نعبر عن اكبر حجم (65,535).

السطر الثاني: أول باكيت الهـ identification = 2 bytes كل باكيت الهـ sequence خاص فيه مشان الراوتر يعرف إذا هاد الباكيت أول مرة بشوفه أو لـ ومشان كمان الـ fragmentation

الـ fragmentation بمسك الباكيت وبقسمه لباكيت أصغر بنتموا لنفس الـ باكيت الأصل فياخذوا نفس الـ ID.

عشان نقدر نرجع إلfragments لأصلها لازم يكون عندي sequence number
بتدل على ترتيبه مشان أقدر أرجع أرباب الباكيت وهو بيجي دور إل .13 bits = fragmentation offset

ال flag fragmentation يتساعدني أعرف إذا في fragmentation أو لا وإذا في إضافية.

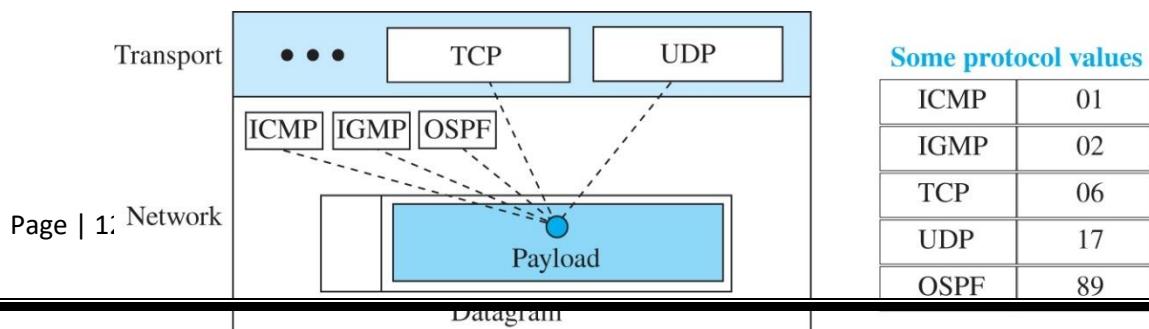
السطر الثالث: `counter = time to live` هو بمثابة كل ما الباقيت تدخل راوتر بنقص منها بالمرحلة اي بوصول فيها ال `next hope = time to live` = 1 ال بدتها تكون با ال `destination` او `ينتهي`.

العبارة عن id بتخزن فيه رقم البرتوكول لأنه ممك يكون protocols byte = 1 . transport layer ال ICMP or IGMP... وممك يقلوا برتوكولات

الـ error control 16 bit = header checksumنفس فكرة الـ error control بتشابهتر.

السطر الرابع والخامس هم ال source + destination IP addresses

.options + padding 0 - 40 bytes وآخر اشي إذا معنا أي إضافات معنا من



Multiplexing and demultiplexing using the value of the protocol field

ال transport layer -
نفس ال source IP address ف ال 3
. IP packet بنزلوا مع بعض ب TCP messages
الجدول الي عاليمين فيه 5 بروتوكولات كل واحد الله رقم بالعشري. ممكن يجي
سؤال عليهم أنه في protocol ID header في واحد من هدول الأرقام
شو البروتوكول.

Example

An IPv4 packet has arrived with the first 8 bits as $(01000010)_2$. The receiver discards the packet. Why?

- There is an error in this packet. The 4 leftmost bits $(0100)_2$ show the version, which is correct. The next 4 bits $(0010)_2$ show an invalid header length ($2 * 4 = 8$). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

المفروض أول 4 bits يكونو version وثاني 4 bits header length -
أول 4 هم 0100 هاد صح لأنه هو version 4
ثاني 4 0010 يعني بالعشري 2 يعني ال header الأصلي طوله 8 وهاد الاشي
مش مقبول لأنه المفروض أقل قيمة أصلية لل header = 20
وهيك الراوتر بهملها.

Example

In an IPv4 packet, the value of HLEN is $(1000)_2$. How many bytes of options are being carried by this packet?

- The HLEN value is 8, which means the total number of bytes in the header is $8 * 4$, or 32 bytes. The first 20 bytes are the base header, the next 12 bytes are the options.



Example

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is $(0028)_{16}$. How many bytes of data are being carried by this packet?

- The HLEN value is 5, which means the total number of bytes in the header is $5 * 4$, or 20 bytes (no options). The total length is $(0028)_{16}$ or 40 bytes, which means the packet is carrying 20 bytes of data ($40 - 20$).

Example

An IPv4 packet has arrived with the first few hexadecimal digits as shown

$(45000028000100000102\dots)_{16}$

How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

- To find the time-to-live field, we skip 8 bytes (16 hexadecimal digits). The time-to-live field is the ninth byte, which is $(01)_{16}$. This means the packet can travel only [one hop](#).
- The protocol field is the next byte $(02)_{16}$, which means that the protocol is [IGMP](#). It is noted that ICMP, IGMP is a network layer protocol.

Fragmentation

- A datagram can travel through different networks.
- Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
- The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

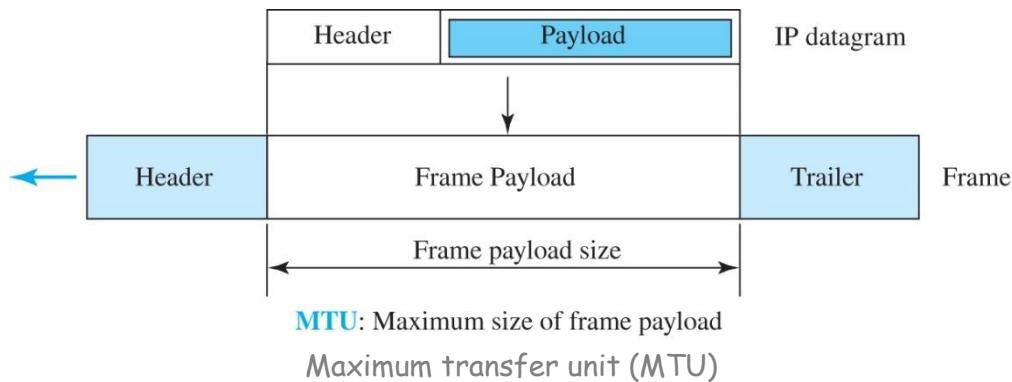


- For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Maximum Transfer Unit

- Each link-layer protocol has its own frame format.
- One of the features of each format is the maximum size of the payload that can be encapsulated in a frame, total size of the datagram must be less than the maximum size.

الباكيت لما تنزل على ال data link layer لازم ما تكون تتجاوز ال maximum size (هي أكبر frame payload size) إذا كان حجمها أكبر بنعمل ال fragmentation



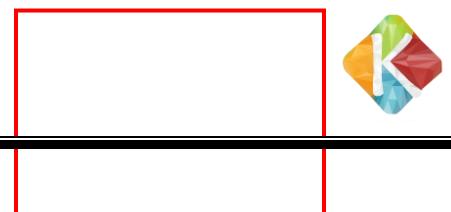
Fields Related to Fragmentation

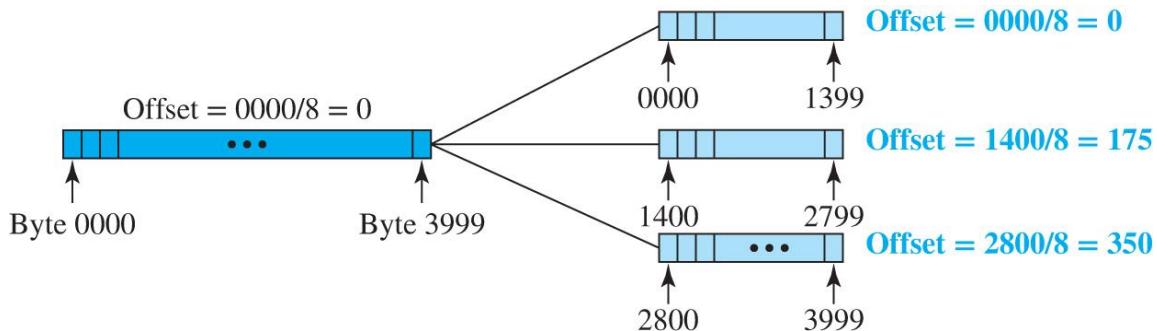
We mentioned before that three fields in an IP datagram are related to fragmentation: identification, flags, and fragmentation offset.

- The 16-bit identification field identifies a datagram originating from the source host.
- The 3-bit flags field defines three flags.
- The 13-bit fragmentation offset field shows the relative position of this fragment with respect to the whole datagram.

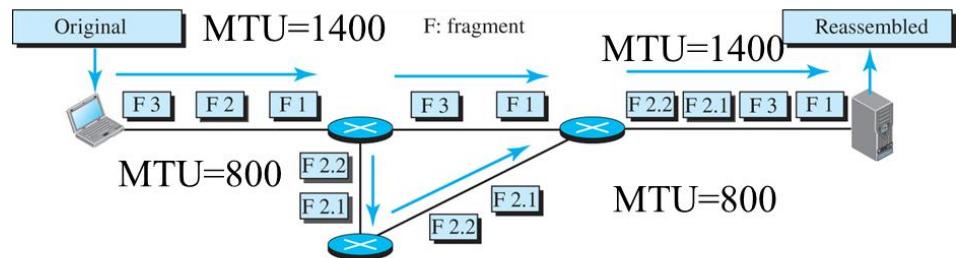
Fragmentation example: MTU 1400 bytes

$4000/1400=2.857$: so we will have 3 fragments





الي بنعمله بال fragmentation هو أنه بنمسك الداتا الي بال payload وبنعطي كل بايت رقم . بأماكن محددة بنقرر أنه بذنا نقسم الباكيت ل fragment offset وأول بايت بال fragment رقمته هو ال fragments طول ال 13 bits = fragment offset ممكن تكون كبيرة وتحتاج ل 16 bits الحل كان نفس الي عملناه بال header بس بنقسم على 8 ، معناته ال bytes الي بنقطع عندها بذها تكون من مضاعفات ال 8.

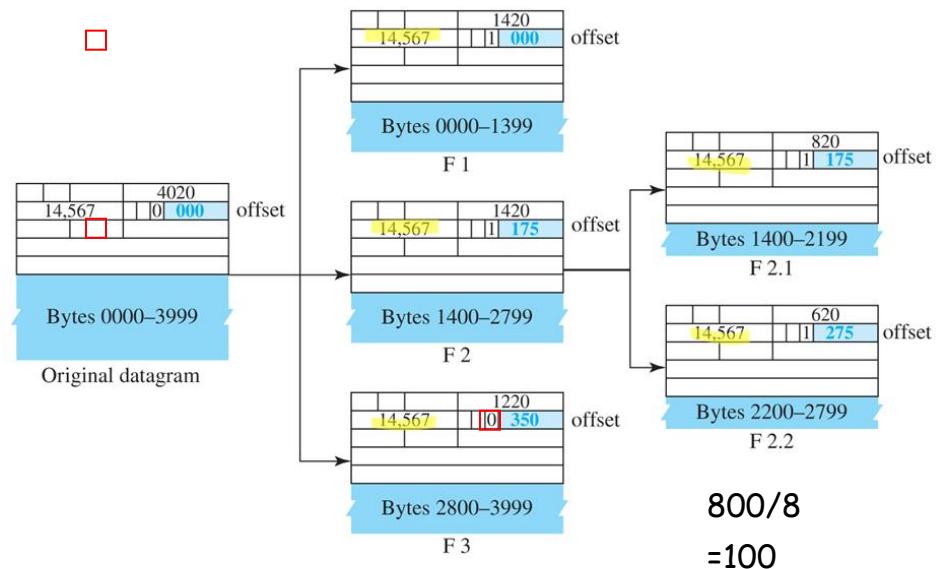


4020: the 20 for header

Note $175 \times 8 = 1400$

Note $175 + 175 = 350$

Note: $4000 - (1400 + 1400) = 1200$



هون ال original node الي طلعت منها الرسائل اضطررت أنها تعمل .F2 ل fragmentation



*الباكيت الأصلي قبل ال fragmentation كان رقمه 14567 كل ال fragments الي بتتنمي لهاد الباكيت وأي متفرع منها بحملوا نفس الرقم .

*الحجم الي بالرسمة مكتوب 4020 لأنها عبارة عن payload + header ، يعني مو هاد الرقم الي بنقسمه على 1400 لازم نشيل منه ال header .

ال more bit دائمًا = 1 إلا عند آخر fragment = 0 لأنه مافي اشي بعده .

*ممكن يجي بالامتحان زي هيكل رسماة وبدنا نعيي جوا المربعات فمهم تكونوا عارفين كل مربع شو بمثل وكيف بنحسب .

Example

A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

- If the M bit is 0, it means that there are no more fragments; the fragment is **the last one**. However, we **cannot** say if the original packet was fragmented or not. A non-fragmented packet is considered the last fragment.

Example

A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

- If the M bit is 1, it means that **there is at least one more fragment**. This fragment **can** be the first one or a middle one, but not the last one. We don't know if it is the first one or a middle one; we need more information (the value of the **fragmentation offset**).

Example

A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

- Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the **first fragment**.

Example



A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

- To find the number of the first byte, we **multiply the offset value by 8**. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data.

ال 100 هي عشرى . -

Example

A packet has arrived in which the offset value is **100**, the value of HLEN is 5, and the value of the total length field is **100**. What are the numbers of the first byte and the last byte?

- The first byte number is $100 * 8 = 800$. The total length is 100 bytes, and the header length is 20 bytes ($5 * 4$), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879.
- Note: The Total Length=MTU (80 i.e. payload)+Header(20, no option).

Options

- The header of the IPv4 datagram is made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long and was discussed in the previous section.
- The variable part comprises the options that can be a maximum of 40 bytes (**in multiples of 4 bytes**) to preserve the boundary of the header.
- Options, as the name implies, are not required for a datagram.
- They can be used for network testing and debugging.
- Although options are not a required part of the IP header, option processing is required of the IP software.

حجم 0 من . -



- الراوتر لازم إذا في options يحللها ويطلع عليها.

Single-Byte Options

1- No Operation: a 1-byte option used as a filler between options.

لو بدن نرص أكثر من option بفهم الراوتر انه الأول خلص والثاني خلص عن طريق ال no operation فهو زي فاصل.

2- End of Option: 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option.

زي القفل بنستخدمه بالآخر لما ال options تخلّص.

Security of IPv4 Datagrams

*بال اعتبر لل security اي ترتب عليها عدد ثغرات كبيرة وهما جزء منهم:

Packet Sniffing

An intruder may intercept an IP packet and make a copy of it.

يعطيوني صورة عن الشبكة ، بس ما بتدخل بعمل الشبكة بس بتسمع عليها.

Packet Modification

The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.

التغيير على محتوى البيانات الي بالباكيت، هدفه يغير على الداتا تبعت اليوزر بدون ما حدا يلاحظ فما بتلاعب بال header.

IP Spoofing

An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.

يتتحل شخصية حدا وتبعد traffic باسمه.

IPSec

- The IP packets today can be protected from the previously mentioned attacks using a protocol called IPSec (IP Security).



- This protocol, which is used in conjunction with the IP protocol, creates a connection-oriented service between two entities in which they can exchange IP packets without worrying about the three attacks discussed above.

ICMPv4

- The IPv4 has no error-reporting or error-correcting mechanism.
 - The IP protocol also lacks a mechanism for host and management queries.
 - The Internet Control Message Protocol version 4 (ICMPv4) has been designed to compensate for the above two deficiencies.
- اله علاقة بال -
management

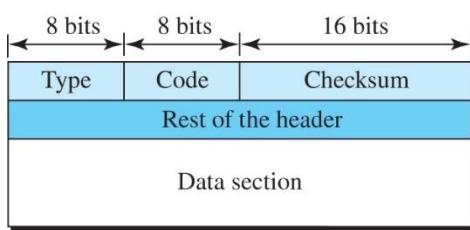
Messages

- ICMP messages are divided into two broad categories: **error-reporting messages** and **query messages**.
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.
- For example, nodes can discover their neighbors.
- Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

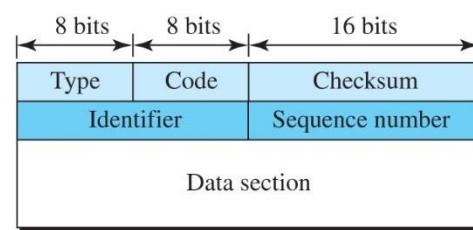
الـ error هي رد فعل ، صار error فبنبعتوا. ما صار ما بنبعتوا .

الـ query message مسح استعلامية لـ management ما بستن المشاكل

تصير وبشوف الـ traffic كيف ماشي عشان يجمع بيانات.



Error-reporting messages



Query messages

Type and code values

Error-reporting messages

- 03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)

Query messages

- 08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)





General format of ICMP messages

- الثنين حجمهم 8 bytes

- بال بال error reporting type كل السطر الأول (الي بالمربيع الأحمر وحفظ).

ال errors

03: كنت بحاول أوصيل host أو راوتر ممكن لأنه طافي أو الشبكة طافية أو رفض يحيى معى.

04: في احتمال يصير اختناق بالراوتر، فالراوتر برجعها لل source مشان يخفف الضغط.

05: بتبعن من راوتر لراوتر عادة مشان يصلح سطر بال routing table براوتر معين يعني يكون في راوتر طلّع باكيت من عنده بس ما لازم بال shortest path (هاد النوع خطير لأنه ممكن يسأء استخدامه عن طريق أنه حدا يعمله . (attacker لل redirection

11: أنه بعثت والمفترض يوصل رد بس الوقت تجاوز وما وصلني.

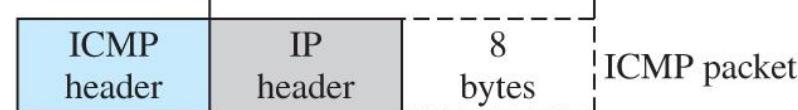
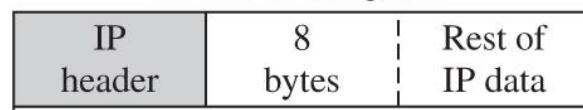
12: الباكيت الي عم تطلع من هاد الراوتر فيها مشكلة (مثلاً ال header مضروب).

- ال query messages

00 + 08: بذنا نشيّك على راوتر معين إذا صاحي وبرد أو لا بدون ما أبعثله داتا وبشوف إذا أخذ وقت زيادة عن الي بالعادة باخذه أو لا.

13 + 14: إذا في نود مش لاقي الساعة تبعته أو مش متأكد فبسأل.

Received datagram



Contents of data field for error messages

هون عم بحكي عن ال ICMP messages بورجينا إياها ك -
ال بعدين كيف بتطلع ك bode . IP packet
ال ICMP messages بتطلع من الحاسوب على هيئة IP packet . يعني بتكون -
ماخذة ال ICMP messages (20 bytes) ولازم يكون مسجل فيه كود ال ICMP .
يعني لو مافيها هاد الكود بنفكرها IP عادي
ال ICMP body + ICMP header بتكون من ال ICMP messages
بحاله ال ICMP message body تكون فيها ال ICMP header اي
بحتوي على معلومات عن ال IP packet (ال header + أول 8 bytes منها) اي
سببيت وجود ال ICMP message (ال ICMP message بتتولد كرد فعل عن ال
error حصل على source IP packet معينة) يعرف شو الباكيت الى
عم تضرب ، غير ال IP كمان بنأخذ أول 8 Bytes from the body (هدول ال 8
.IP packet عن ال transport layer اي بني ال

Deprecated Messages

Three pairs of messages are declared obsolete by IETF:

- Information request and replay messages
- Address mask request and reply messages
- Router solicitation and advertisement messages

Debugging Tools

- There are several tools that can be used in the Internet for debugging.
- We can determine the viability of a host or router.
- We can trace the route of a packet.
- We introduce two tools that use ICMP for debugging: ping and traceroute.

عبارة عن مجموعة من ال Applications المبنية على ال ICP protocol وأكثر -
.ping اشي شائع هو



Ping

- We can use the ping program to find if a host is alive and is responding.

Example

The following shows how we send a ping message to the auniversity.edu site.

\$ ping auniversity.edu

```
PING auniversity.edu (152.181.8.3) 56 (84) bytes of data. ttl=62 time=1.91 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=0 ttl=62 time=2.04 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=1 ttl=62 time=1.90 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=2 ttl=62 time=1.90 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=3 ttl=62 time=1.97 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=4 ttl=62 time=1.93 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=5 ttl=62 time=2.00 ms
--- auniversity.edu statistics ---
6 packets transmitted, 6 received, 0% packet loss
rtt min/avg/max = 1.90/1.95/2.04 ms
```

عشان نشيك عن destination هل بقدر أوصله أو لا وهل ال path بيناتنا آمن -

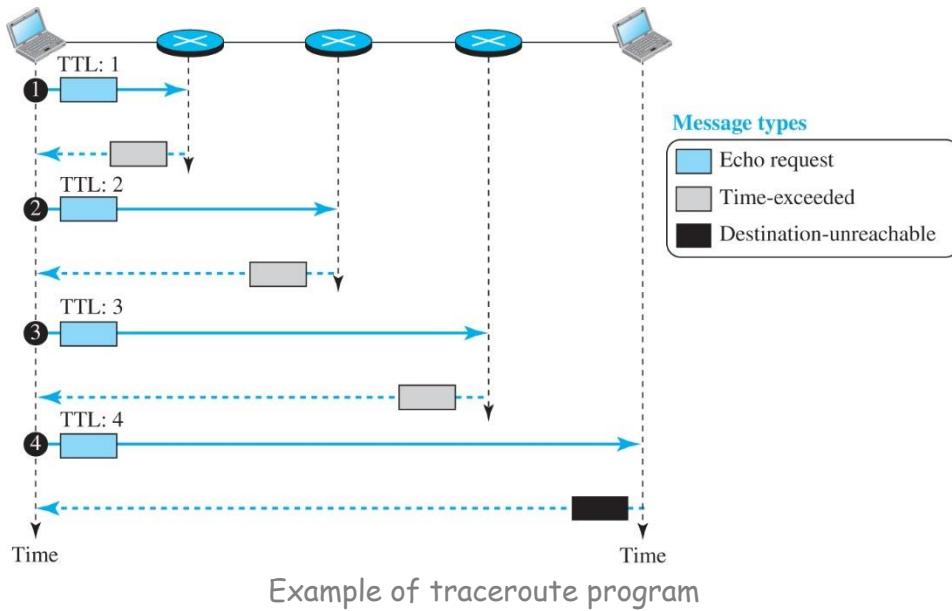
...

Traceroute or Tracert

- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- The number of hops in the Internet is normally less than this.
- Since these two programs behave different in Unix and Windows, we explain them separately.



- يشبه فكرة ال ping بس هون بشيك على كل pop على الطريق بيني وبين ال destination مثل بس على ال destination .



- يعطيني ال echo request في حال صار في error ممكن يرجع time destination unreachable error أو exceeded error
بلاول بتفرج على كل ال path وبمسك كل راوتر عالطريق وبشيك عليه ب إذا تجاوب معه بنتقل للي بعده.

Forwarding of IP Packets

- As we discussed before, forwarding means to place the packet in its route to its destination.
- Since the Internet today is made of a combination of links (networks), forwarding means to deliver the packet to the next hop (which can be the final destination or the intermediate connecting device).
- Although the IP protocol was originally designed as a connectionless protocol, today the tendency is to change it to connection-oriented protocol. We discuss both cases.

- الفرق بين ال forwarding and routing

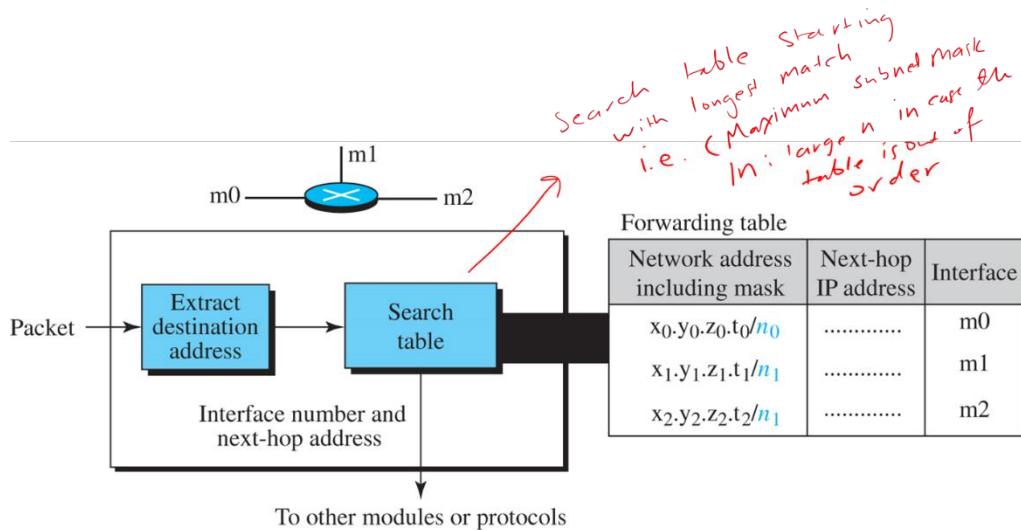
ال routing أي أكتشف الطريق الأقصر ما بين نقطتين عن طريق أنه كل راوتر . shortest path algorithm بشغل ال



بعد ما عملنا routing table وبنينا ال routing table وصرنا جاهزين ننطلق بتوجيه
باكيت كيف بدی أقرر عای مخرج بدها تنزل؟ بشيکها على ال forwarding table
وبناءً على ال destination IP address الي فيها بنقر المخرج وهاد هو ال
. (routing forward لـ (تطبيق forward

Forwarding Based on Destination Address

- We first discuss forwarding based on the destination address.
This is a traditional approach, which is prevalent today.
- In this case, forwarding requires a host or a router to have a forwarding table.
- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.



Simplified forwarding module in classless address

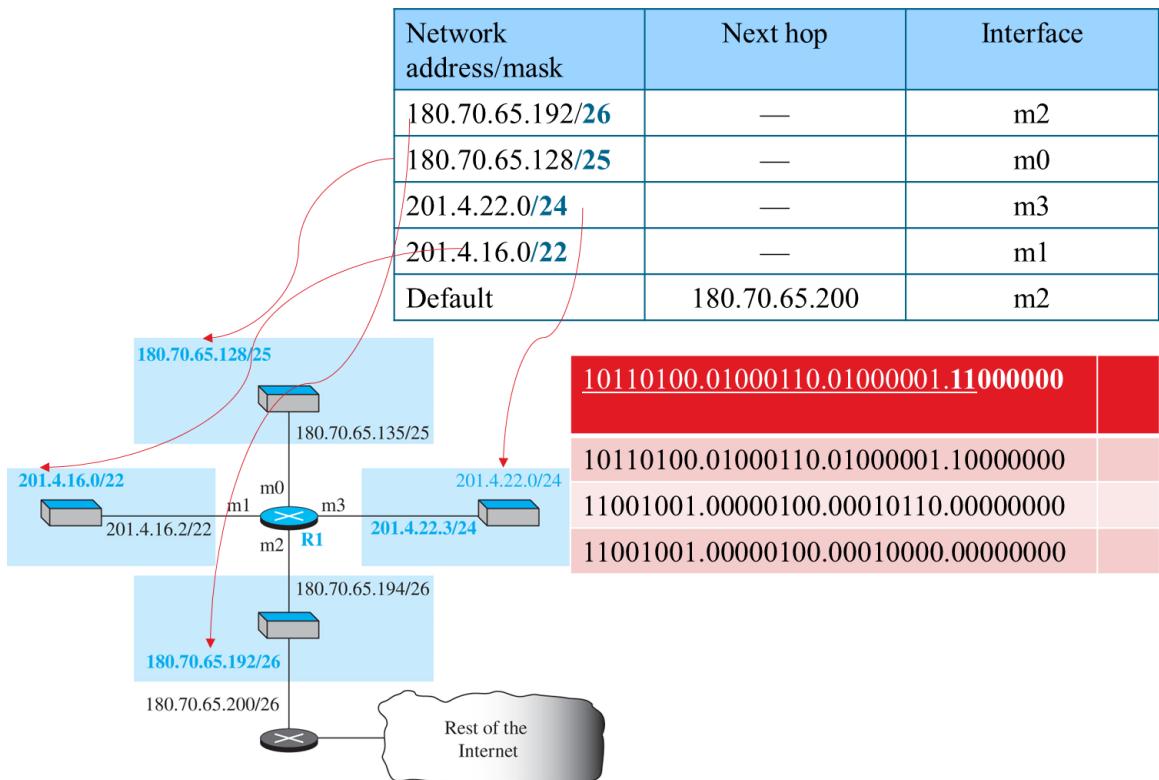
عنا راوتر وإله packet بتفوت عليه ال forwarding table (ال مرقت على ال network layer + physical layer + data link layer فھي بتبيّن انھا valid) بتفوت على ال destination IP وبتاخذ ال forwarding table معينة على ال search algorithm address باستخدامه، بتترتب على هاد ال search مقارنة هاد ال destination IP address بالأسطر الموجودة بال forwarding table أول سطر بتطبق يؤخذ وبتططلع من المخرج تبعه، إذا ما نطبقت على ولا اشي (0 تكون عندي اشي زي ال switch default بجملة ال) بنطعلها لراوتر ثاني أعلى منها يتعامل فيها.



. network address including mask - انتبهوا بالجدول

Example

Make a forwarding table for router R1 using the configuration in the Figure.



الي بالأزرق هم عنوان الشبكة، والي بالأسود هم ال next لـ MAC address - hope .

لما ال destination يكون بعيد عن بكون موجود بال next hope -
ال default دائمًا فاضية إلا بحالة ال IP لي؟ لأنه إذا لقيت ال IP دائمًا next hope -
عندني خلص ما في داعي أعطي الممسح لحدا ثانٍ يوصلّها فالراوتر بوصلّها بدون وسيط، أما بال default لازم أوصله لحدا ثانٍ فبنحط ال IP address .

ال default دائمًا آخر سطر -
ال blocks بترتيبها تنازليًا بالجدول بناءً على طول ال prefix (وهي تكون تصاعديًا بنفس الوقت لـ suffix).

Example



Show the forwarding process if a packet arrives at R1 in the Figure with the destination address 180.70.65.140. 1000 1100

Mask	Network Address	Next Hop	Interface
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	m1
Any	Any	180.70.65.200	m2

The router performs the following steps:

1. The first mask (/26) is applied to the destination address.

The result is 180.70.65.128, which does not match the corresponding network address.

2. The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address and the interface number m0 are passed to ARP for further processing.

180.70.65.1000 1100

Example

Show the forwarding process if a packet arrives at R1 in the Figure with the destination address 201.4.22.35. 0010 0011

Mask	Network Address	Next Hop	Interface
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	m1
Any	Any	180.70.65.200	m2

The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address.



2. The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).

3. $121 \rightarrow 201.4.22.0 \xrightarrow{\text{match}} m_3$ (row 3)

Example

Show the forwarding process if a packet arrives at R1 in the Figure with the destination address 18.24.32.78.

Mask	Network Address	Next Hop	Interface
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	m1
Any	Any	180.70.65.200	m2

This time all masks are applied, one by one, to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to someplace else in the Internet.

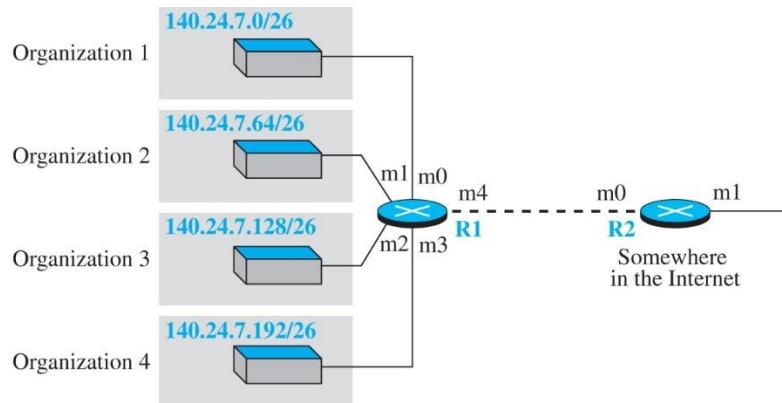
* بهاي الحالة بدون نحول ونحل مبين أنه ما حدا بتطابقه.

Address Aggregation

- When we use classful addressing, there is only one entry in the forwarding table for each site outside the organization.
- The entry defines the site even if that site is subnetted.
- When a packet arrives at the router, the router checks the corresponding entry and forwards the packet accordingly.
- When we use classless addressing, it is likely that the number of forwarding table entries will increase.



Address aggregation 10001100.00011000.00000111.00000000



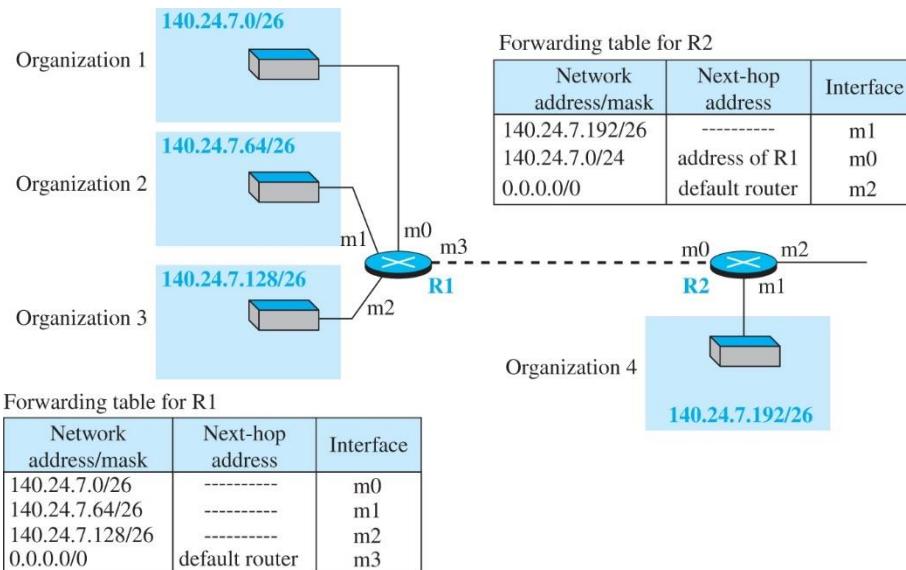
Forwarding table for R1

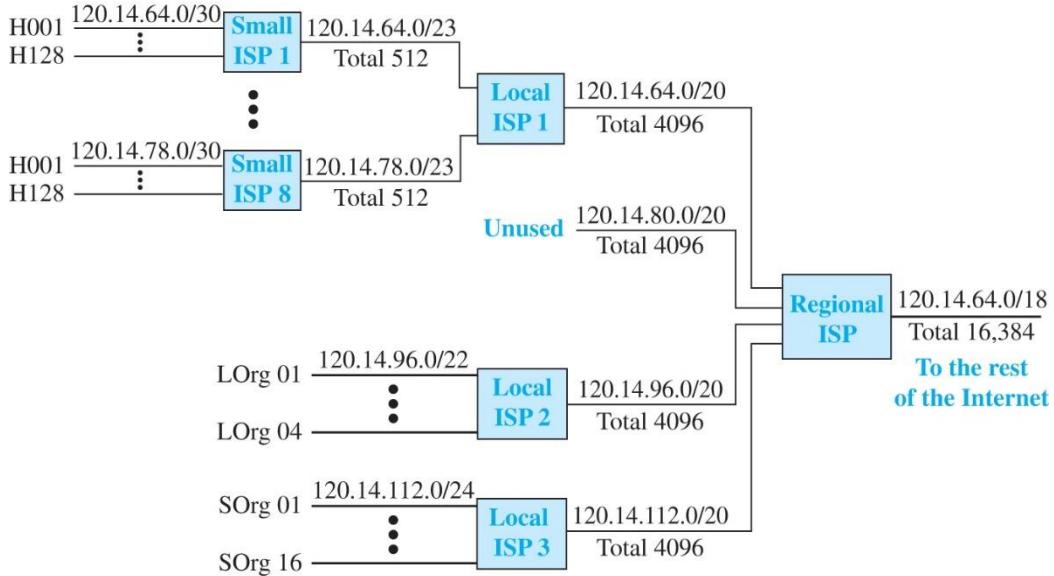
Network address/mask	Next-hop address	Interface
140.24.7.0/26	-----	m0
140.24.7.64/26	-----	m1
140.24.7.128/26	-----	m2
140.24.7.192/26	-----	m3
0.0.0.0/0	address of R2	m4

Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.0/24	-----	m0
0.0.0.0/0	default router	m1

الشي الي ما بعرف R1 أنه يتعامل معه بيعنته ل R2 بنفس الوقت ما
بشوf المؤسسات بشوف R1 لي؟ مثـان نقصـر من ال routing table تبعـت
وهيـك عمـلية الـبحث بتـصـير أسرـع .



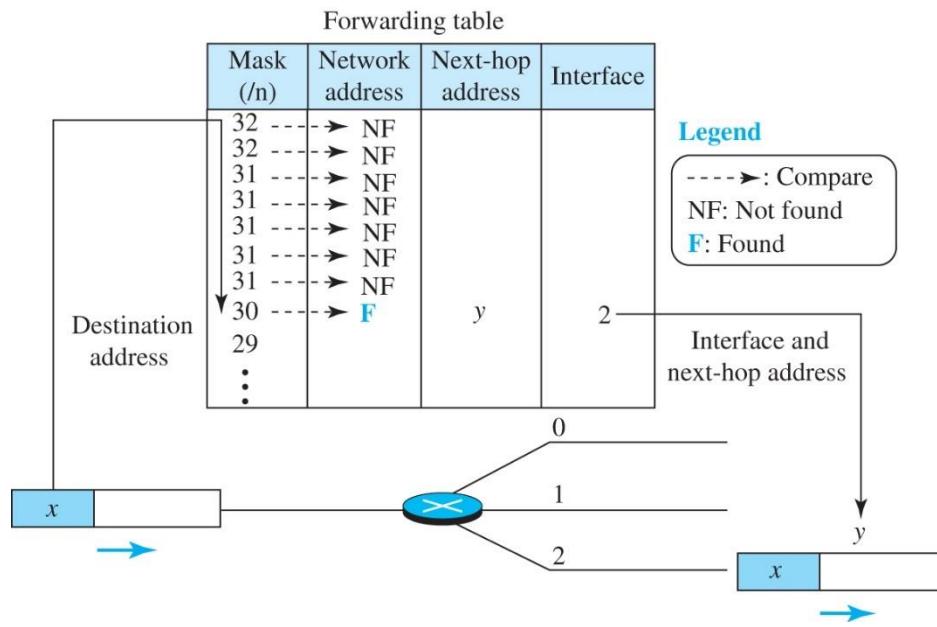


- As an example of **hierarchical routing**, let us consider . A regional ISP is granted 16,384 addresses starting from 120.14.64.0. The regional ISP has decided to divide this block into 4 subblocks, each with 4096 addresses. Three of these subblocks are assigned to three local ISPs, the second subblock is reserved for future use. Note that the mask for each block is /20 because the original block with mask /18 is divided into 4 blocks.

Forwarding Table Search Algorithm

- In classless addressing, there is no network information in the destination address.
- The simplest, but not the most efficient, search method is called the **longest prefix match** (as we discussed before).
- The forwarding table can be divided into buckets, one for each prefix.
- The router first tries the longest prefix. If the destination address is found in this bucket, the search is complete. If the address is not found, the next prefix is searched, and so on.
- It is obvious that this type of search takes a long time.





Next Generation IP (IPv6)

- The address depletion of IPv4 and other shortcoming of this protocol prompted a new version of IP protocol in the early 1990s, which is called Internet Protocol version 6 (IPv6) or IP new generation (Ipng).

IPv6 Addressing

The main reason for migration from IPv4 to IPv6 was the small size of the address space of IPv4. An IPv6 address is 128 bits or 16 bytes, four times the address length in IPv4.

Representation

An IPv6 address is 128 bits or 16 bytes long; four times the address length of IPv4.
 $\overline{2^{128} \text{ (IPv6)}} \leftrightarrow \overline{2^3 \text{ (IPv4)}}$

Binary (128 bits)	11111110111101101011 ... 1111111000000000
Colon hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

Address Space

The address space of IPv6 contains 2^{128} addresses. This address space is 296 times the IPv4 address—definitely no address depletion—as shown, the size of the space is

340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456



Address Space Allocation

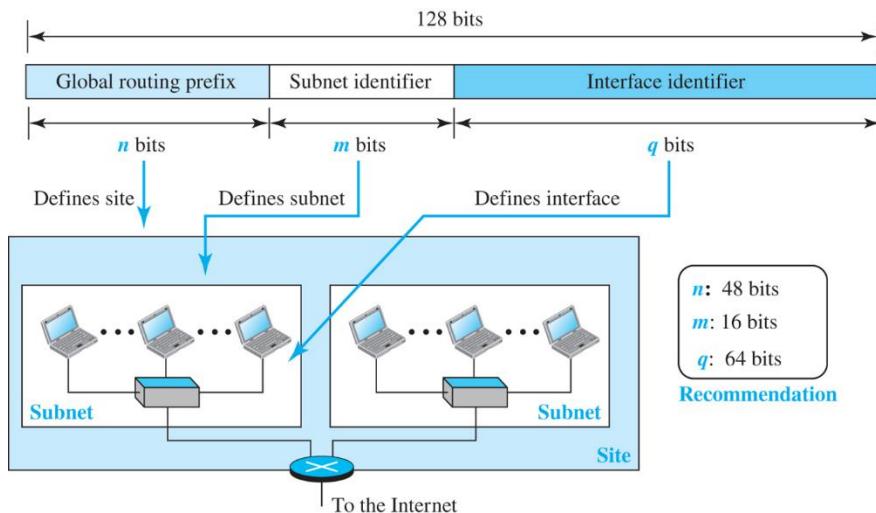
- Like the address space of IPv4, the address space of IPv6 is divided into several blocks of varying size and each block is allocated for a special purpose. Most of the blocks are still unassigned and have been set aside for future use.

Block prefix	CIDR	Block assignment	Fraction
0000 0000	0000::/8	Special addresses	1/256
001	2000::/3	Global unicast	1/8
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

Prefixes for assigned IPv6 addresses

- الرقم الي محظوظ بعد ال / بدل على الأرقام الي رح تكون ثابتة.
- Global unicast اي بطلع عالانترنت.
- ال unique local unicast إنهم ما بطلعوا عالانترنت بس لشبكة محلية بس ممكن يكون الها شبكات فرعية (زي الجامعة والمختبرات).
- ال link local addresses switch مش راوتر (يعني بس مختبر).
- ال multicast حكينا عنه من قبل زي جروبات الوايـس بس الفرق انه بعطيـنـي multicasting لل different scope (يعني الجروب هاد بـس للمختبر أو لكل الكلية أو لكل البلد ...).

Global unicast address



بال IPv6 لازم نعرف 3 معلومات:-
 يعني لأي بلوك بتنتهي من الي فوق.
 لو موجود بشبكة محلية وفي حواليك شبكات ثانية فشوا
 الشبكة الي موجود فيها.
 رقم الحاسوب Interface Identifier

$$n + m + q = 128$$

مرات يفضل يكونوا ال $64 = q$ ، $16 = m$ ، $48 = n$ بالضرورة.

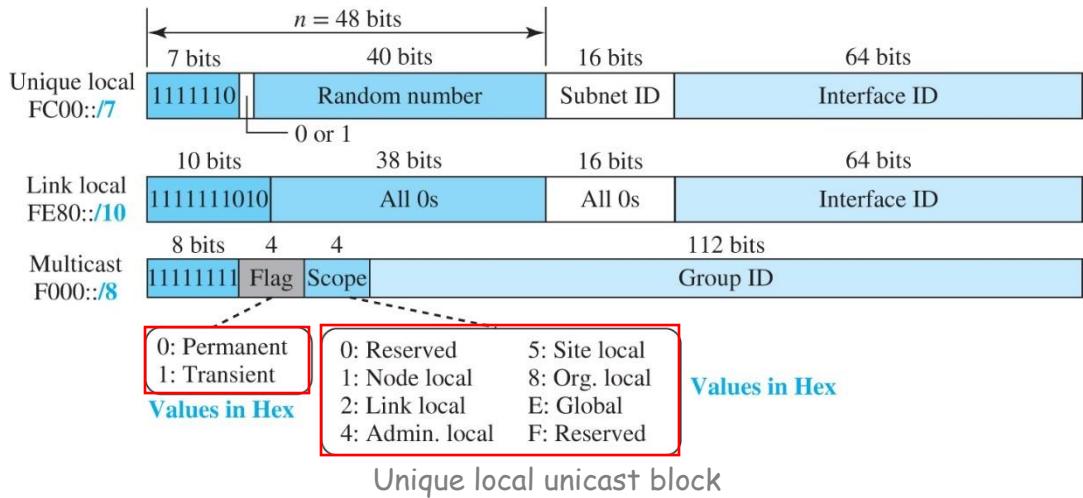


.default زي ال Unspecified -
 بخليني أحكي مع حالي.
 IP address هو version 4 وعم بكتبه ك version 6 (يعني Compatible)
 الراوترز بفهموا ال 2 versions .
 كان 4 version Mapped بس بطل ، تحول ل 6.
 بنقدر نميّز بينهم حسب ال bits الي بعد ال 32. إذا كانو 1s معناته mapped
 وإذا 0s معناته compatible .

Other Assigned Blocks

- IPv6 uses two large blocks for private addressing and one large block for multicasting.





Autoconfiguration

- One of the interesting features of IPv6 addressing is the auto-configuration of hosts.
- As we discussed in IPv4, the host and routers are originally configured manually by the network manager.
- However, the Dynamic Host Configuration Protocol, DHCP, can be used to allocate an IPv4 address to a host that joins the network.
- In IPv6, DHCP protocol can still be used to allocate an IPv6 address to a host, but a host can also configure itself.



Chapter 08: Network Layer: Routing of Packets

- Unicast routing in the Internet, with a large number of routers and a huge number of hosts, can be done only by using hierarchical routing: routing in several steps using different routing algorithms.
- In this section, we first discuss the general concept of unicast routing in an internet. After the routing concepts and algorithms are understood, we show how we can apply them to the Internet.

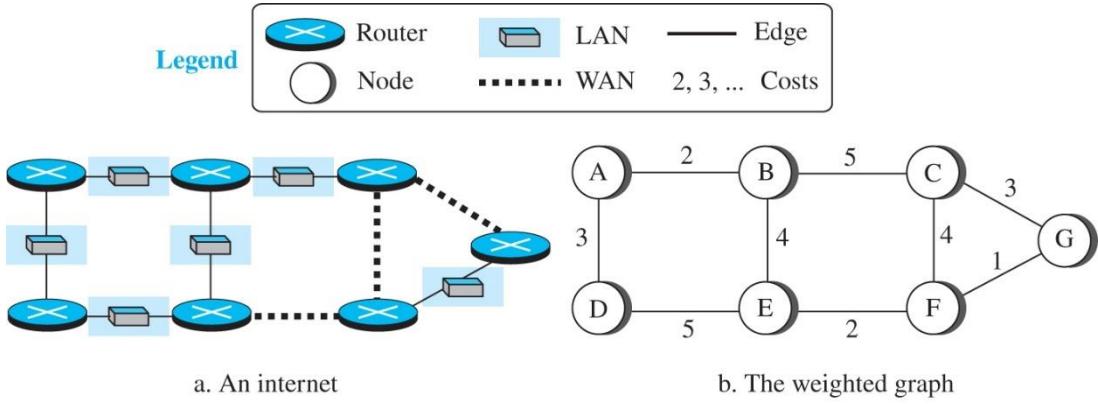
General Idea

- In unicast routing, a packet is routed, hop by hop, from its source to its destination by the help of forwarding tables.
- The source host needs no forwarding table because it delivers its packet to the default router in its local network.
- The destination host needs no forwarding table either because it receives the packet from its default router in its local network.
- This means that only the routers that glue together the networks in the internet need forwarding tables.

An Internet as a Graph

- To find the best route, an internet can be modeled as a graph.
- A graph in computer science is a set of nodes and edges (lines) that connect the nodes.
- To model an internet as a graph, we can think of each router as a node and each network between a pair of routers as an edge.
- An internet is, in fact, modeled as a weighted graph, in which each edge is associated with a cost.





- هدفنا نعرف شو أقصر طريق بين كل الراوترز(أقصر طريق يعني مجموع الأوزان فيها أقل اشي) ، فبدنا نجد الشبكة.

Routing Algorithms

- Several routing algorithms have been designed in the past. The differences between these methods are in the way they interpret the least cost and the way they create the least-cost tree for each node.
 - In this section, we discuss the common algorithms; later we show how a routing protocol in the Internet implements one of these algorithms.

1. Distance-Vector Routing

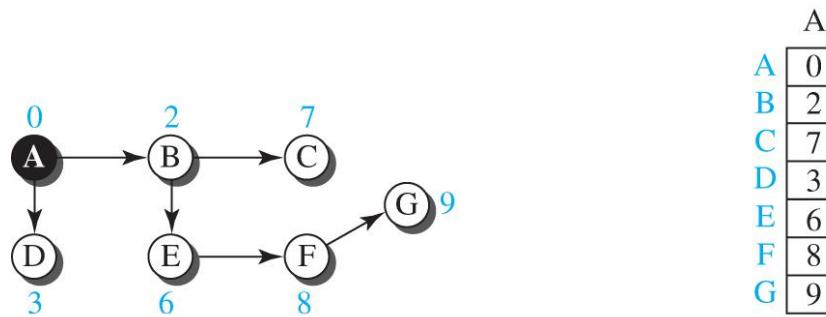
- The distance-vector (DV) routing uses the goal we discussed in the introduction, to find the best route. In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors.
 - The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet. We can say that in distance-vector routing, a router continuously tells all of its neighbors what it knows about the whole internet (although the knowledge can be incomplete).

- هو قد يم ببس مشكلته أنه مكلف فيه تراسل كثير للبيانات ، ميشان أعرف أقصر طريق بيبي و بين الي حوالي مش بحاجة نعرف اشي إلا عن الجيران، يعني بالرسمة الي فوق لو بدبي أوجد طريق ل A فأنا بحاجة أني أعرف معلومات D + B ببس (بس الي بينهم لينك مباشرة).



Distance Vector

- The concept of a distance vector is the rationale for the name distance-vector routing.
- A least-cost tree is a combination of least-cost paths from the root of the tree to all destinations.
- These paths are graphically glued together to form the tree.
- Distance-vector routing unglues these paths and creates a distance vector, a one-dimensional array to represent the tree.



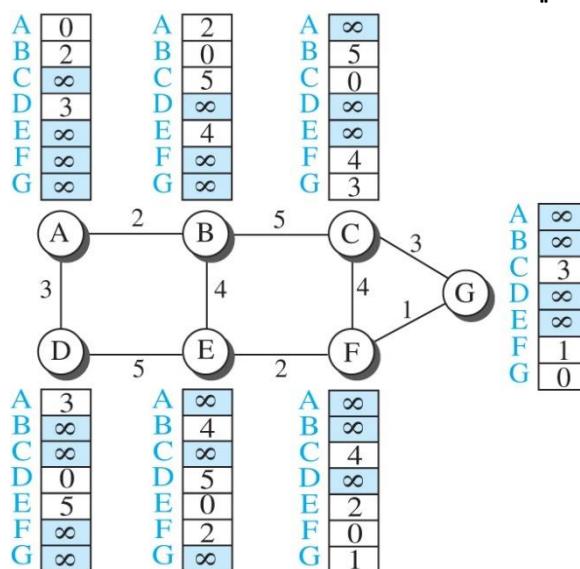
a. Tree for node A

b. Distance vector for node A

The distance vector corresponding to a tree

نود A بدها تعرف أقصر طريق بينها وبين الباقي. -

بأول بنعبي ال distance vector



كل وحدة بتتشرف مين جيرانها وبتعبي وإذا ما كان جارها بتحطه ∞ -

بتبلش تيجي ل A ال distance vector وبمسكها وبحاول يستفيد منها .



مثلاً وصله تبع B . بيلش يشوف أقصر اشي المسافة بين A و $A = 2$.
 بعدين من A إل B ،
 C لساتها مجھولة فبحكيلها B أنه بوصل ل C والمسافة بينهم 5 هيک بتصرير
 المسافة 7 بتقارن ال 7 بال ∞ وبختار ال 7
 وبتفضل تكر العملية زي هيک لحد ما يختار أحسنdistance vector

New B	Old B	A	Old B	E
A 2	A 2	A 0	A 2	A ∞
B 0	B 0	B 2	B 0	B 4
C 5	C 5	C ∞	C 5	C ∞
D 5	D ∞	D 3	D 5	D 5
E 4	E 4	E ∞	E 4	E 0
F ∞	F ∞	F ∞	F ∞	F 2
G ∞				

$$B[] = \min(B[], 2 + A[])$$

New B	Old B	E
A 2	A 2	A ∞
B 0	B 0	B 4
C 5	C 5	C ∞
D 5	D 5	D 5
E 4	E 4	E 0
F 6	F ∞	F 2
G ∞	G ∞	G ∞

$$B[] = \min(B[], 4 + E[])$$

a. First event: B receives a copy of A's vector.

b. Second event: B receives a copy of E's vector.

Note:

X[]: the whole vector

Updating distance vectors

Distance-vector routing algorithm for a node

```

1  Distance_Vector_Routing()
2  {
3      // Initialize (create initial vectors for the node)
4      D[myself] = 0
5      for (y = 1 to N)
6      {
7          if (y is a neighbor)
8              D[y] = c[myself][y]
9          Else
10             D[y] =  $\infty$ 
11     }
12     send vector {D[1], D[2], ..., D[N]} to all neighbors
13     // Update (improve the vector with the vector received from a neighbor)
14     repeat (forever)
15     {
16         wait (for a vector Dw from a neighbor w or any change in the link)
17         for (y = 1 to N)
18         {
19             D[y] = min [D[y], (c[myself][w] + Dw[y])] // Bellman-Ford equation
20         }
21         if (any change in the vector)
22             send vector {D[1], D[2], ..., D[N]} to all neighbors
23     }
24 }
```

*بس للطلاع



2. Link-State Routing

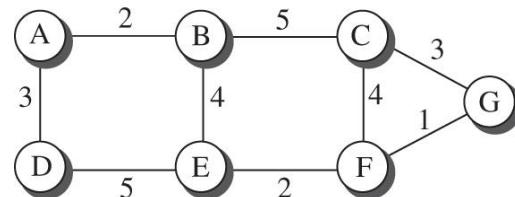
- A routing algorithm that directly follows our discussion for creating least-cost trees and forwarding tables is link-state (LS) routing.
- This method uses the term link-state to define the characteristic of a link (an edge) that represents a network in the internet.
- In this algorithm the cost associated with an edge defines the state of the link.
- Links with lower costs are preferred to links with higher costs; if the cost of a link is infinity, it means that the link does not exist or has been broken.

أكثر، بتعتمد على ال shortest path algorithm . مشكلته أنه لازم Efficient -

يكون شايف الشبكة كلها .

ال link state routing وال Distance-Vector Routing -

.bellman ford equation مشترك انهم مبنين على معادلة

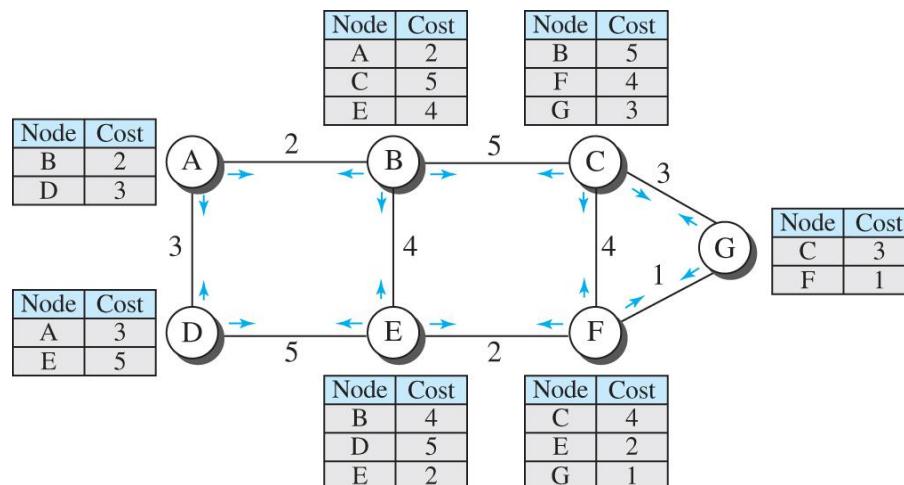


a. The weighted graph

	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. Link state database

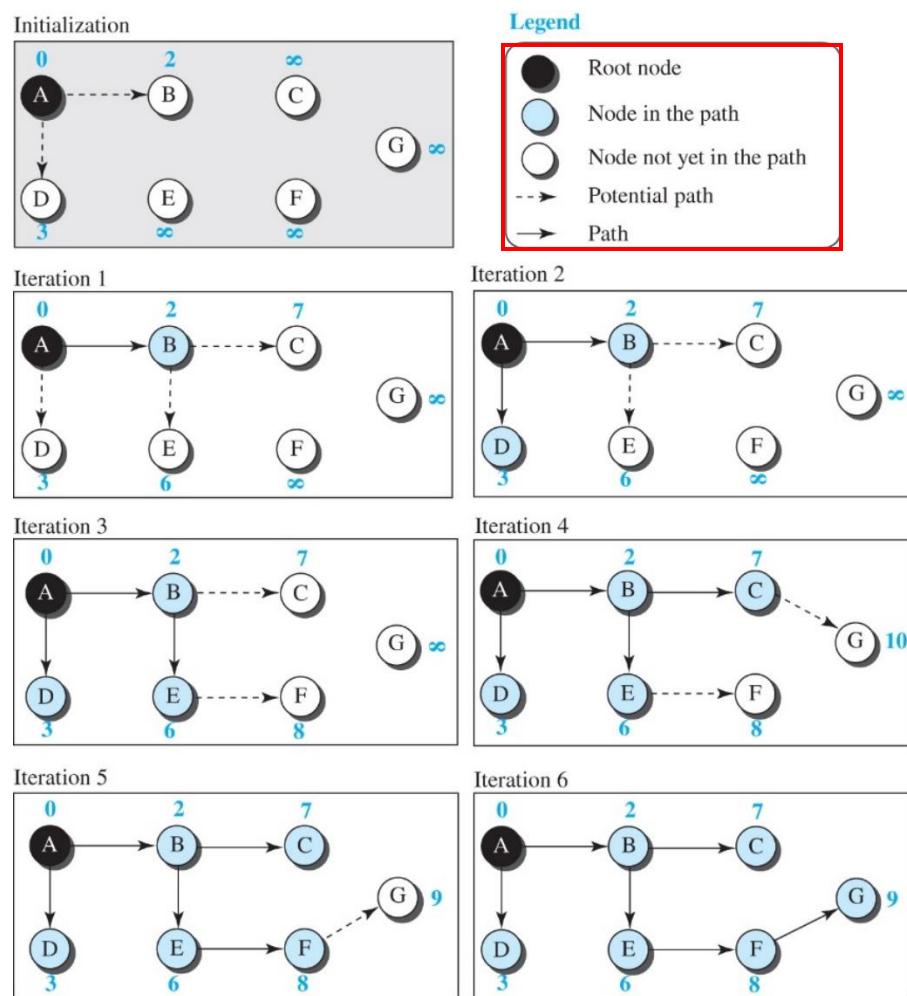
لازم تكون عارف كل الشبكة . -



Formation of Least-Cost Tree

To create a least-cost tree for itself, using the shared LSDB, each node needs to run the famous [Dijkstra Algorithm](#). This iterative algorithm uses the following steps:

1. The node chooses itself as the root of the tree, creating a tree with a single node, and sets the total cost of each node based on the information in the LSDB.
2. The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree.
3. The node repeats step 2 until all nodes are added to the tree.



```

1   Distance_Vector_Routing ()
2   {
3       // Initialization
4       Tree = {root}      // Tree is made only of the root
5       for (y = 1 to N) // N is the number of nodes
6       {
7           if (y is the root)
8               D [y] = 0    // D [y] is shortest distance from root to node y
9           else if (y is a neighbor)
10              D [y] = c[root][y] // c [x] [y] is cost between nodes x and y in LSDB
11           else
12              D [y] =  $\infty$ 
13       }
14       // Calculation
15       repeat
16       {
17           find a node w, with D [w ] minimum among all nodes not in the Tree
18           Tree = Tree  $\cup$  {w}    // Add w to tree
19           // Update distances for all neighbor of w
20           for (every node x, which is neighbor of w and not in the Tree)
21           {
22               D[x] = min {D[x], (D[w] + c[w][x])}
23           }
24       } until (all nodes included in the Tree)
25   }

```

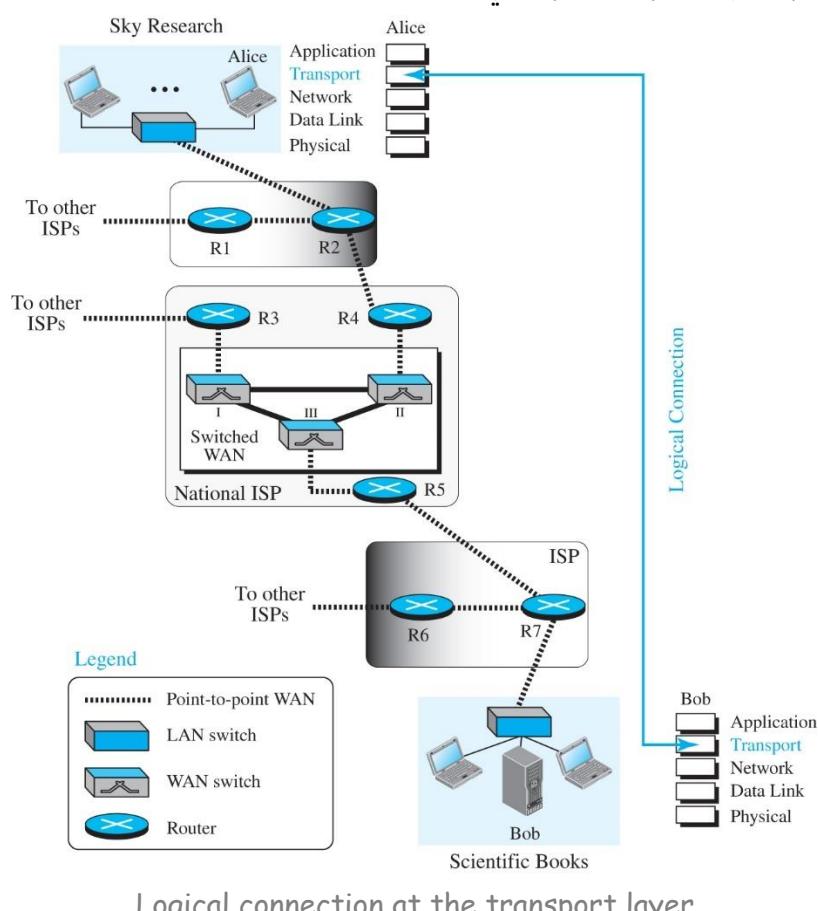
بس لِسْطَلَعُ *



Chapter 09: Transport Layer

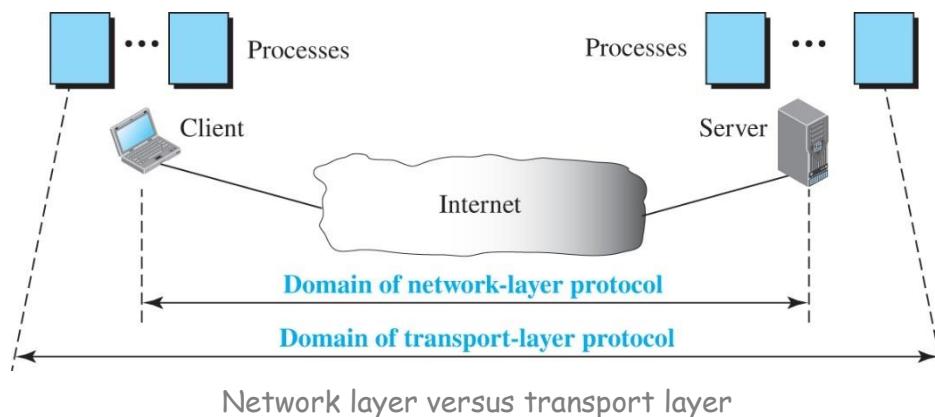
- The transport layer is located between the application layer and the network layer.
- It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host.
- Communication is provided using a logical connection.

ما بنشوف ال path logical ← transport layer بال destination source من ال path pops (abstraction link transport layer). (يعني بصير عنا ظهر كأنه end to end = transport layer بال communication في ناس بسموها process to process (لأنه لما نكون بال transport layer على برنامج عم يعمل run بحاسوب ما، رح يجي مع برنامج آخر كمان يعمل run بحاسوب ثان).



Process-to-Process Communication

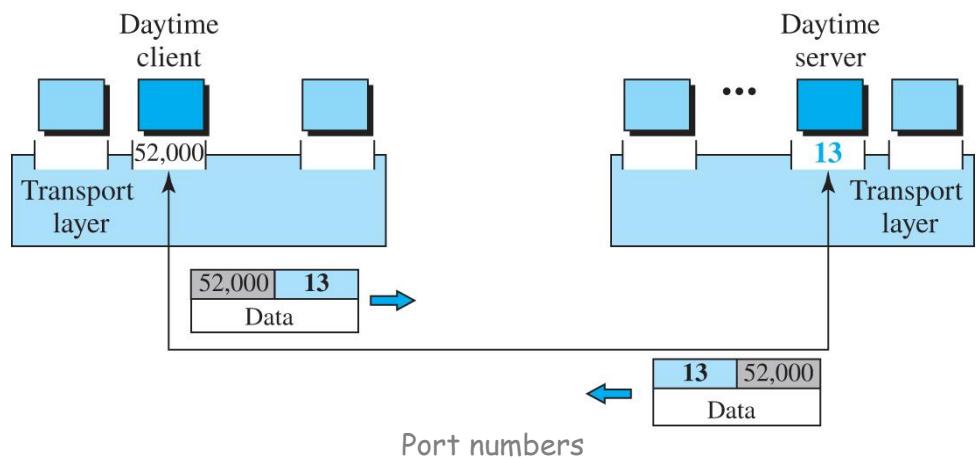
- The first duty of a transport-layer protocol is to provide process-to-process communication.
- A process is an application-layer entity (running program) that uses the services of the transport layer.
- Before we discuss how process-to-process communication can be accomplished, we need to understand the difference between host-to-host communication and process-to-process communication.



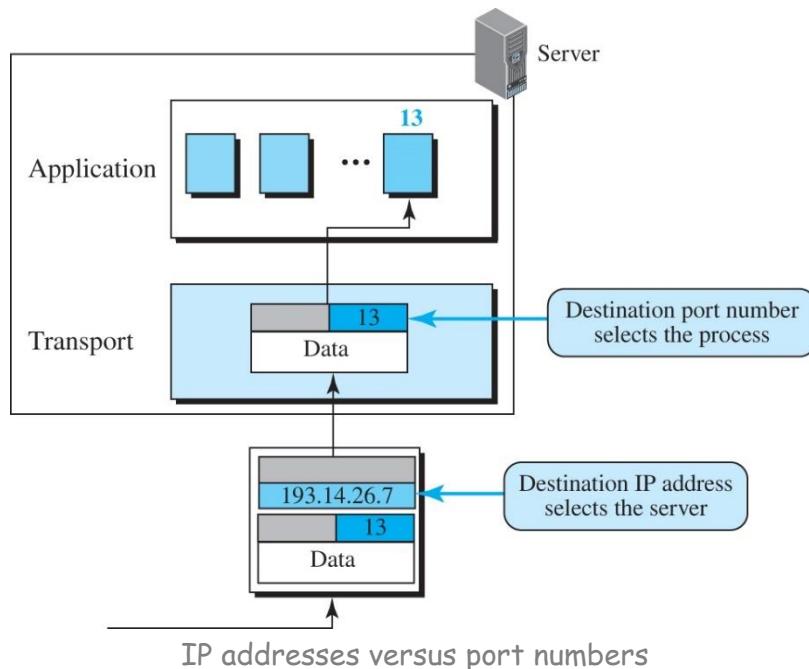
Addressing: Port Numbers

- Although there are a few ways to achieve process-to-process communication, the most common is through the client-server paradigm. A process on the local host, called a client, needs services from a process usually on the remote host, called a server.
 - However, operating systems today support both multiuser and multiprogramming environments. A remote computer can run several programs at the same time, just as several local computers can run one or more client programs at the same time.
- بعطي رقم مشان نميز process عن process بنفس الجهاز





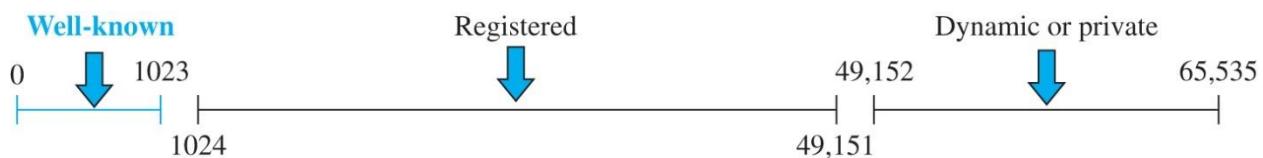
- كل الـ **process** فيها بال **port** خاص .
- **client and server** هون بتعبر عن أدوارهم .
- ال **server** هو اللي عايز يقدم الخدمة أما ال **client** اللي عايز بحصل عالخدمة .
- ال **source port number** فيه **heard** **destination port number** .
- $52,000 = \text{Source port number}$.
- ال **13 = destination port number** (ومعروف انه 13 لـ **day time**) .
- لما الرد يجي الأدوار بتبدل بينهم (بصير ال **source destination** والعكس) .



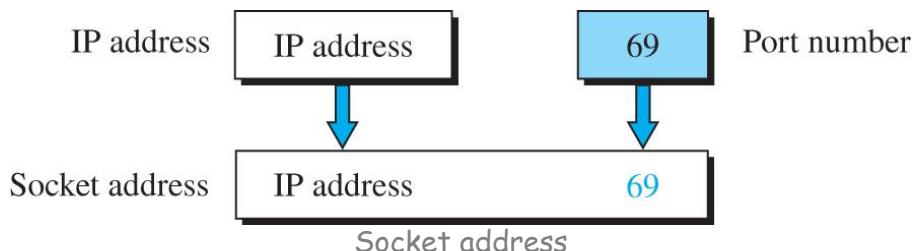
application وي ما بتشتغل بال الها انعکاس بال transport process -
 .layer
 بتنزل الرسالة على ال network layer وبتحيط بباکیت و بتلزق عليها من برا IP
 . header
 ال port numbers ما بتحددوا بال network layer بنزلوا من ال .transport
 مهم تكونوا عارفين موقع ال port number بالرسمتين *

ICANN Ranges

(Internet Corporation for Assigned Names and Numbers) has divided the port numbers into three ranges: well-known, registered, and dynamic (or private).



منظمة مسؤولة عن ال port numbers قسمتهم ل 3 أنواع:
 ال port numbers من 0 - 1023 (المعروفين لمين
 وممنوع حدا يلعب فيه).
 business or 1024 - 49,151 هدول ممكن نعمل فيهم Registered
 .port number يشبّك الناس عالانترنت بس لازم ندفع سعر ال application
 من 49,152 - 65,535 هدول لعامة الشعب (أي Dynamic or private
 بده يشبّك على ال server ، ال port number client site application
 محجوز، وال client مافي أهكل هم من وين بدبي أجبله server
 dynamic or private number لأنه نظام التشغيل بختار من ال number يعني
 ما دخلنا فيه) بالوقت الواحد تكونوا معطّيين لنفس ال process
 .(16 = log 65,535) port number بنحتاج 16 bits للتعبير عن ال



أي حدا بكتب كود ل client/server ضروري يعرف اشي اسمه socket (هي
 TCP/IP)(يعني ما في عنصر حقيقي اسمه socket موجود بال abstract



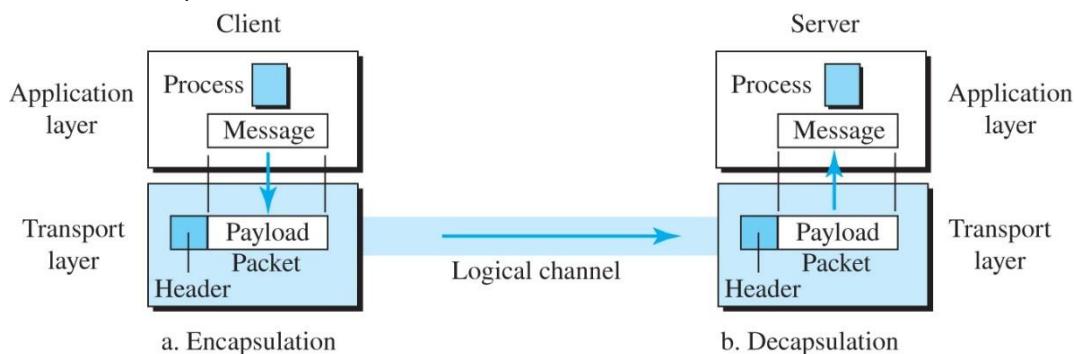
port number (protocol) وهو عبارة عن أي أخط إل IP address واحدة.

لو بدي اختيار إل process ضمن الحاسوب الي أنا عليه بدي .port number .
لو بدي الحاسوب بدون إل process IP address بكتفي .

لو أنا بالشبكة وبدي أعرف شو إل process الي بدي إياها ضمن كل الأجهزة بدي .socket address إل .

Encapsulation and Decapsulation

- To send a message from one process to another, the transport-layer protocol encapsulates and decapsulates messages.
- Encapsulation happens at the sender site. When a process has a message to send, it passes the message to the transport layer along with a pair of socket addresses and some other pieces of information, which depend on the transport-layer protocol.
- The transport layer receives the data and adds the transport-layer header.

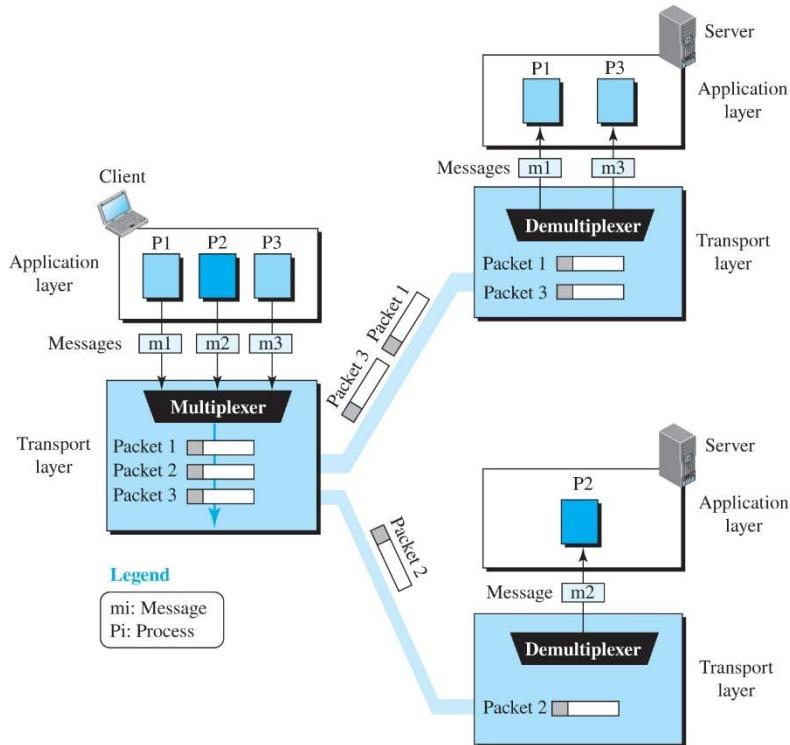


بال destination بتصريره العملية بال transport layer - .

Multiplexing and Demultiplexing

- Whenever an entity accepts items from more than one source, this is referred to as multiplexing (many to one); whenever an entity delivers items to more than one source, this is referred to as demultiplexing (one to many).
- The transport layer at the source performs multiplexing; the transport layer at the destination performs demultiplexing.





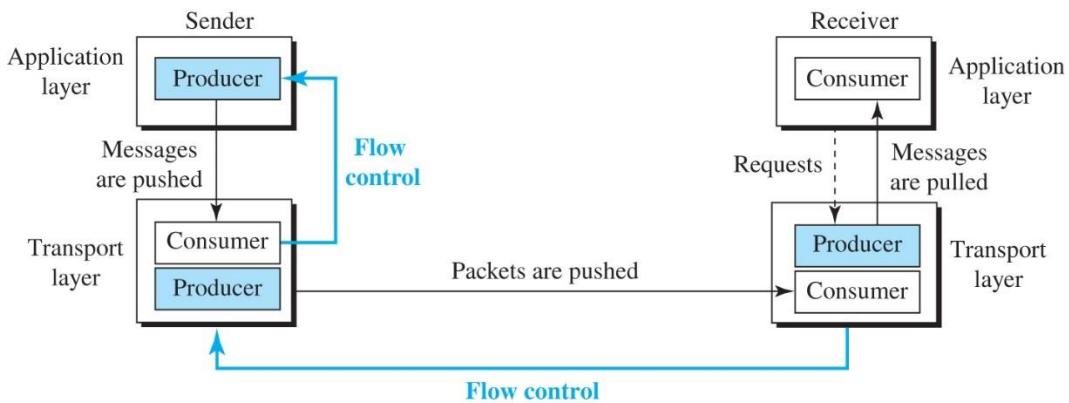
بكون عنا أكثر من process عم تبعث packets وكلهم بكونوا رايحين على نفس الحاسوب، كل رسالة حجمها صغير.
بالمثال 3 نفس ال IP address معناته رايحين على نفس المكان وأحجامهم صغيرة فبلزقهم بعض بباكتكب كبيرة وبطلعهم مرة واحدة لل destination .(transport layer) في destination بال transport layer بال destination . و packet 2 راجحة على جهاز ثاني فبتطلع لحالها.

Flow Control

- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.
- If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.
- If the items are produced more slowly than they can be consumed, the consumer must wait, and the system becomes less efficient.
- Flow control is related to the first issue. We need to prevent losing the data items at the consumer site.

حكينا من قبل فكرته أنه نمضن بين source and destination أنه ال ما يكون عم بضخ بيانات بقدرة أسرع من قدرة ال destination على الاستيعاب





ال consumer هي application layer بالنسبة لل transport layer -
بيانات

وبالنسبة لل producer هي network layer بتنزل عليها بيانات.
*ال producer مش بنس بين ال source + destination حتى على مستوى
النود الواحد موجود.

Error Control

In the Internet, since the underlying network layer (IP) is unreliable, we need to make the transport layer reliable if the application requires reliability. Reliability can be achieved by adding error control services to the transport layer. Error control at the transport layer is responsible for:

- 1- Detecting and discarding corrupted packets.

عند القدرة أنه يشيك ويهمل ال corrupted packets .

- 2- Keeping track of lost and discarded packets and resending them.

يقدر يميز الباكيت الي ضيعها او الي رفض يستلمها لأنها corrupted packets .

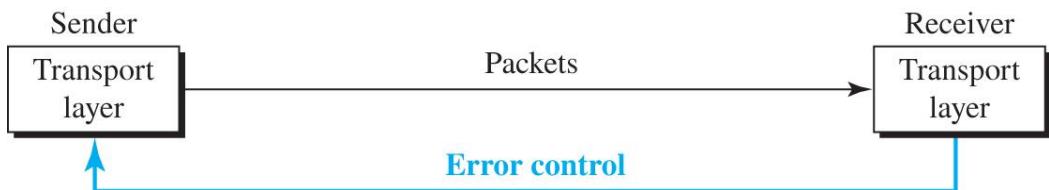
- 3- Recognizing duplicate packets and discarding them.

يقدر يميّز إذا هاد الباكيت أول مرة بشوفه أو مكرر.

- 4- Buffering out-of-order packets until the missing packets arrive.

لو مثلاً عندي باكيت أرقامها من 1 - 5 . ووصلتني باكيت 1 بعدين 5 . طيب و 2 و 3 و 4 .
فبكون عندي زي array [1, 5] فإذا وصلوا 1 و 5 عادي بس ما بنرفعهم لل application إلا إذا أجو 2 و 3 و 4 .

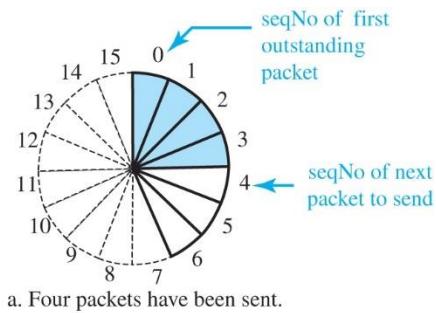




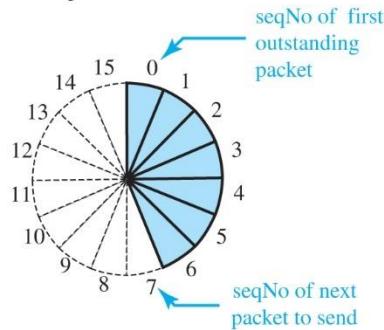
الـ *ACK* يبعثه *sender* -
والـ *receiver* يعطيه تغذية راجعة بخصوص الـ *error control* (أي ما
يوصلي *ACK* هو فعلياً فيدبك عن الإيرور، أو ممكن يبعث *ACK* أنه ما وصله
إلي بده إيه).

Combination of Flow and Error Control

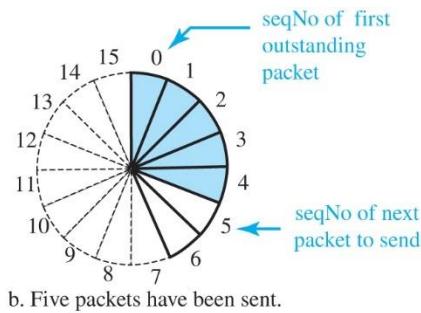
- We have discussed that flow control requires the use of two buffers, one at the sender site and the other at the receiver site.
- We have also discussed that error control requires the use of sequence and acknowledgment numbers by both sides.
- These two requirements can be combined if we use two numbered buffers, one at the sender, one at the receiver.



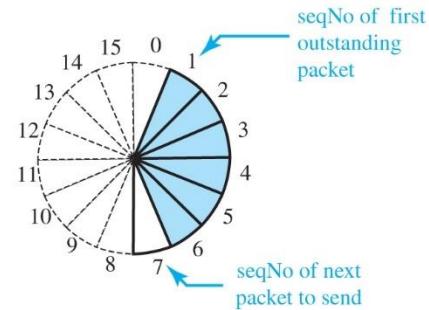
a. Four packets have been sent.



c. Seven packets have been sent;
window is full.



b. Five packets have been sent.



d. Packet 0 has been acknowledged;
window slides.

Sliding window in circular format

في عندي *sender* برقم الباكيت من 0 - 15 (يمثلوا packets -
. (packets



- نفس فكرة الـ go back N and selective repeat أنه بنبعث دفعه من الباكيت لحد ما نوصل للحد الأقصى بنوقف وبنستنى الـ Ack في حال ما وصلت.

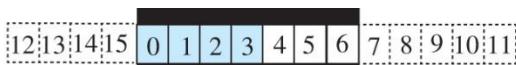
- عادة حجم الـ window = نصف المساحة تبعه الـ address أو الـ sequence 7 = window numbers (يعني زي هون الـ 15 ، حجم الـ window معناه كـ sender مسموح بيعت لغاية 7 باكيت بدون ما تيجي ACK ، وإذا بعثت الـ 7 كلهم ولسا ما وصلني ممنوع أبعت الثانيين) حسب الـ ACK الي بتيجي بنعمل shifting window (بنعمل shifting window).

وإذا ما اجت ACK والـ timer خلص بدي أرجع أبعتها مرة ثانية .
بشكل a : الباكيت الي لونها أزرق بعثناها أما الي بالأبيض لسا ما بعثناهم بس بإمكاننا بعثهم

ما إجا عليها ACK (أقدم باكيت من الي نبعتوا).

بشكل b: الـ Application نزل داتا زيادة وحى أنه نبعتهم وبعث 4 .
بشكل c: الـ application كمان بعث 5 و 6 . 7 ما بقدر أبعتها لأنها مش بالـ window .

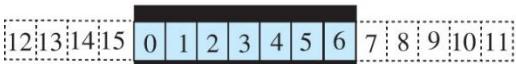
بشكل d: 0 أخذت الـ ACK فبطل لونها أزرق، وبنعمل shifting window وبتصير تبليش من 1.



a. Four packets have been sent.



b. Five packets have been sent.



c. Seven packets have been sent;
window is full.



d. Packet 0 has been acknowledged;
window slides.

Sliding window in linear format

- هاي نفس الي فوق بس بدل ما يرسمها دائرة رسمها خط.



Congestion Control

- An important issue in a packet-switched network, such as the Internet, is congestion. Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle. Congestion control refers to the mechanisms and techniques that control the congestion and keep the load below the capacity.

في بروتوكولات بال transport layer بتعالج ال congestion. وهدف ال congestion protocols أنه الروائز الي عالطريق ما تخنق.

يعني ممكن ال sender + receiver يكون وضعهم تمام بس المشكلة بالروائز الي عالطريق في كثير senders عم بيعتوا عليه داتا فبكون مازم وبصير أبطء.

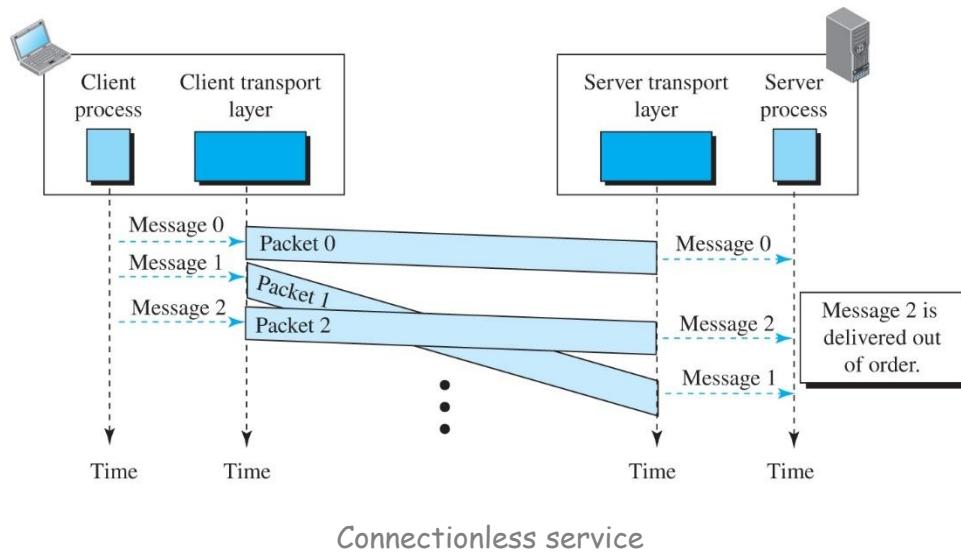
Connectionless and Connection-Oriented Protocol

- A transport-layer protocol, like a network-layer protocol, can provide two types of services: connectionless and connection-oriented.
- The nature of these services at the transport layer, however, is different from the ones at the network layer.
- At the network layer, a connectionless service may mean different paths for different datagrams belonging to the same message.
- Connectionless service at the transport layer means independency between packets; connection-oriented means dependency. Let us elaborate on these two services.

Connectionless Service

- In a connectionless service, the source process needs to divide its message into chunks of data of the size acceptable by the transport layer and deliver them to the transport layer one by one.
- The transport layer treats each chunk as a single unit without any relation between the chunks.
- When a chunk arrives from the application layer, the transport layer encapsulates it in a packet and sends it.



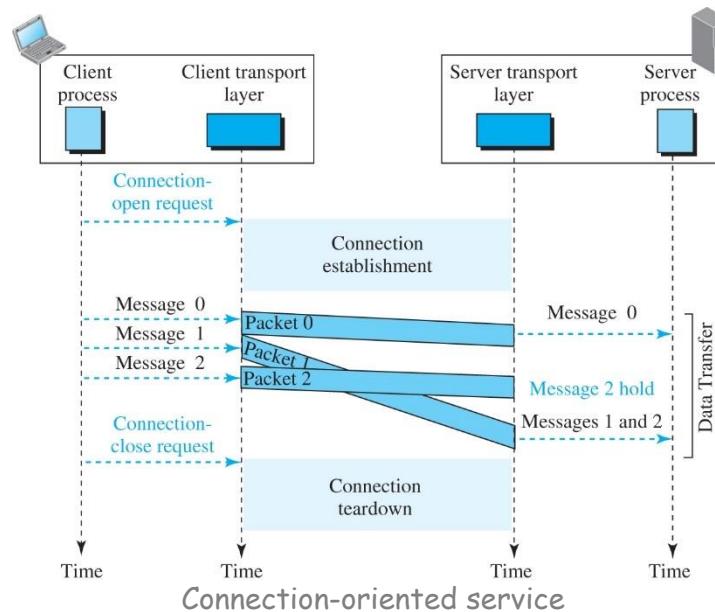


Connectionless service

ال **connection less** فكرته زي لما الضيوف بيجوا على البيت فجأة . -
نفس الاشي بالرسمة ال **server** فجأة صارت الداتا تنزل عليه (بدون أي إذن لما
تبعدت وحتى لما تخلص بدون إذن)، وحتى لما المESSAGES توصل ال **server**
ما بكلف حاله يرتبها حتى، **process**

Connection-Oriented Service

- In a connection-oriented service, the client and the server first need to establish a logical connection between themselves.
- The data exchange can only happen after the connection establishment.
- After data exchange, the connection needs to be torn down.

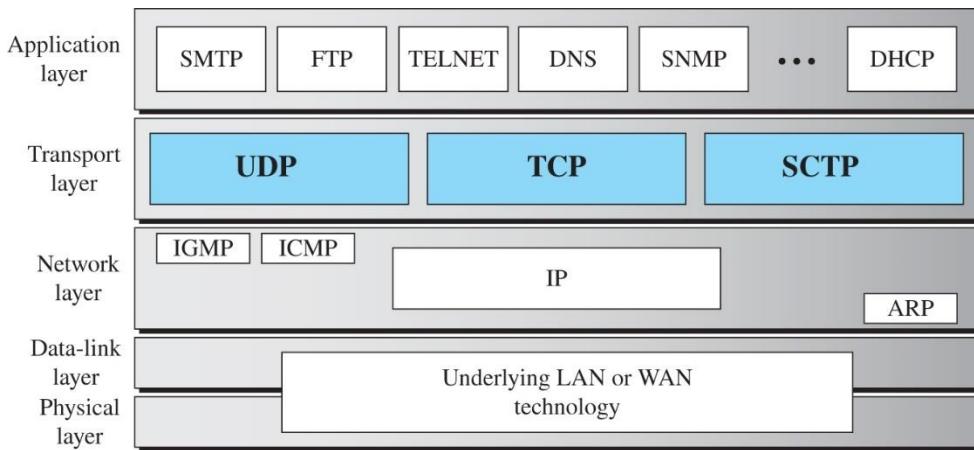


الـ **connection oriented service** مهذب، أي process بدها تبعث داتا بتأخذ إذن (connection establishment).

ولما تنهي التواصل تتبعها **connection teardown** (فصل لـ connection) وكمان لما توصل الداتا **out of order** بتعمللها buffering.

الفرق بين الـ **Reliable protocol** و الـ **Unreliable protocol**
Reliable data guaranteed to arrive complete, correct and inorder
Unreliable No guarantees whatsoever on data

Transport Layer Protocols



Position of transport-layer protocols in the TCP/IP protocol suite

1- UDP: An unreliable connectionless transport-layer protocol used for its simplicity and efficiency in applications where error control can be provided by the application-layer process.

بسط وسريع و efficient بما يقدر أثقل بالداتا وما ضمان على الـ reliability. (لما يكون بدبي الداتا تنتقل بسرعة زي الليفات فبنستخدم الـ UDP).

2- TCP: A reliable connection-oriented protocol that can be used in any application where reliability is important.

(بنستخدمه لما بدنا نبعث إيميل أو نعمل access على داتا بيس لأنه بدبي الداتا تكون على التكّة ما فيها مجال للخطأ ، حتى لو عحساب الوقت وبده bitrate and bandwidth مقابل نحصل على داتا سليمة).

3- SCTP: A new transport-layer protocol that combines the features of UDP and TCP.



Port Numbers

- A transport-layer protocol usually has several responsibilities.
 - One is to create a process-to-process communication; these protocols use port numbers to accomplish this.
 - Port numbers provide end-to-end addresses at the transport layer and allow multiplexing and de-multiplexing at this layer, just as IP addresses do at the network layer.

<i>Port</i>	<i>Protocol</i>	<i>UDP</i>	<i>TCP</i>	<i>SCTP</i>	<i>Description</i>
7	Echo	✓	✓	✓	Echoes back a received datagram
9	Discard	✓	✓	✓	Discards any datagram that is received
11	Users	✓	✓	✓	Active users
13	Daytime	✓	✓	✓	Returns the date and the time
17	Quote	✓	✓	✓	Returns a quote of the day
19	Chargen	✓	✓	✓	Returns a string of characters
20	FTP-data		✓	✓	File Transfer Protocol
21	FTP-21		✓	✓	File Transfer Protocol
23	TELNET		✓	✓	Terminal Network
25	SMTP		✓	✓	Simple Mail Transfer Protocol
53	DNS	✓	✓	✓	Domain Name System
67	DHCP	✓	✓	✓	Dynamic Host Configuration Protocol
69	TFTP	✓	✓	✓	Trivial File Transfer Protocol
80	HTTP		✓	✓	Hypertext Transfer Protocol
111	RPC	✓	✓	✓	Remote Procedure Call
123	NTP	✓	✓	✓	Network Time Protocol
161	SNMP-server	✓			Simple Network Management Protocol
162	SNMP-client	✓			Simple Network Management Protocol

Some well-known ports used with UDP and TCP

- بَدْنَا نَعْرِفُ بِهادِ الْجَدْوَلِ:

خانہ ال transport application layer protocols میں protocols -

كل وحدة من هذه الـ protocols تتبنى على إما نوعه TCP أو UDP أو SCTP أو اثنين منهم أو ثلاثة.

الـ ICMP health check على نود إذا صاحية أو طافية، مدعوم على الـ port 7، ومدعوم على الـ 3 أنواع (بس 7 على الـ UDP، على الـ TCP غير عن الـ SCTP).
الـ Echo فكرة الـ ICMP وأنه يعمل بشيك على health check.

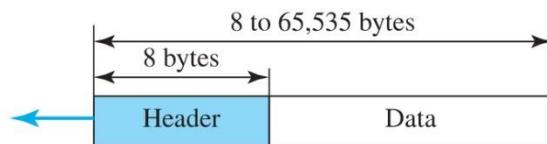
الـ well known port ممنوع نلمسهم زي الكلمات الممحوّزة ، ممنوع أي حدا يأخذهم وحطّهم لتطبيقاته الخاصة فيه.

*لزム تكونوا عارفين كل وحدة شو ال Description تبعها بتخييه بالامتحان.



User Datagram Protocol (UDP)

- A connectionless, unreliable transport protocol.
- If UDP is so powerless, why would a process want to use it? With the disadvantages come some advantages.
- UDP is a very simple protocol using a minimum of overhead.



a. UDP user datagram

0	16	31
Source port number	Destination port number	
Total length	Checksum	

b. Header format
User datagram packet format

- تكون ال header من 8 bytes . الرسالة كاملة مع ال header من 8 bytes (يعني ممكن أعمل UDP بس بدون داتا)
- source port number (16 bits) and destination port number (16 bits) لازم يكونوا موجودين
- datagram variable size Total length
- checksum هو هي نمط بدائي لل error control يعني إذا البأكية عند تعبانة بعملها بال UDP .

Connectionless Services

- As mentioned previously, UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram.
- There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program. The user datagrams are not numbered.



Flow Control

- UDP is a very simple protocol. There is no flow control, and hence no window mechanism.
- The receiver may overflow with incoming messages.
- The lack of flow control means that the process using UDP should provide for this service, if needed.

Error Control

- There is no error control mechanism in UDP except for the checksum. (يعني في بس قليل)
- This means that the sender does not know if a message has been lost or duplicated.
- When the receiver detects an error through the checksum, the user datagram is silently discarded.
- The lack of error control means that the process using UDP should provide for this service, if needed.

Congestion Control

- Since UDP is a connectionless protocol, it does not provide congestion control.
- UDP assumes that the packets sent are small and sporadic and cannot create congestion in the network.
- This assumption may or may not be true today, when UDP is used for interactive real-time transfer of audio and video.

Typical Applications

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control.
- UDP is suitable for a process with internal flow- and error-control mechanisms.
- UDP is a suitable transport protocol for multicasting.
- UDP is used for management processes such as SNMP.



- UDP is used for some route updating protocols such as Routing Information Protocol (RIP).
- UDP is normally used for interactive real-time applications that cannot tolerate uneven delay between sections of a received message.

Transmission Control Protocol

- Transmission Control Protocol (TCP) is a connection-oriented, reliable protocol.
- TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service.
- TCP uses a combination of GBN and SR protocols to provide reliability.

الـ TCP يستخدم комination of GBN AND SR -

الـ windowSelective repeat والـ go back N يستفيدوا من فكرة الـ window ببساطة، الفرق بينهم أنه الـ go back N يحيط بالـ window على مستوى كلها، يعني إذا طفا التايمير يعتبر أنه كل الـ window ما تم إستلامها وبعيد إرسالها كلها.

أما الـ SR كل مسح إلها تايمير خاص فيها يعني الـ destination قادر يحكى انه مثلًا استلم 3 بس ما استلم 4 فما بعيد كل الـ window بعيد بس الي ما استلمهم.

TCP Services

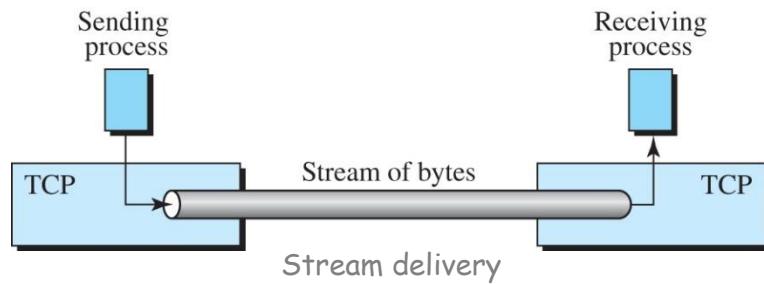
1- Process-to-Process Communication

2- Stream Delivery Service

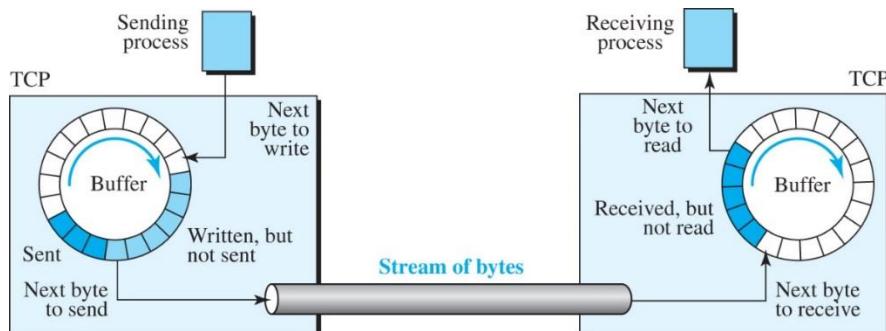
- TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their bytes across the Internet.
- The sending process produces (writes to) the stream and the receiving process consumes (reads from) it.



- الـ TCP يبتعد عن الـ destination زي كأنها بكتب بایت على ملف.



- receiving وال streams of bytes (write) بتضخ Sending process . Stream بتقرأه من ال process



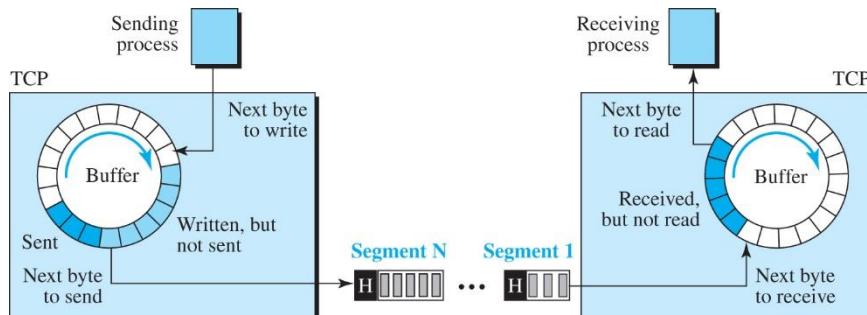
Sending and receiving buffers

- الاشي الي حكيناه فوق بعزوze فكرة ال sending and receiving buffers ، لأنه فعلياً لما نكتب بنكون بنكتب على circular buffer

بال sending process بنكون محددين البايت الي كتبناها بس لسا ما بعتناها (أزرق فاتح) وكمان البايت الي بعثناها (أزرق غامق) والبايت الي لسا ما كتبتها (أبيض)

بال receiving process في عندها داتا ووصلت بس لسا ما قرأتها (أزرق فاتح). وداتا لسا ما استلمتها (أبيض).

.(عكس مبدأ ال file io)



TCP segments



- هون بس بورجيني كيف ال segments عباره عن bytes .

Full-Duplex Communication

- TCP offers full-duplex service, where data can flow in both directions at the same time.
- Each TCP endpoint then has its own sending and receiving buffer, and segments move in both directions.

- ال TCP بدعم ال full duplex ، بفترض أنه لما بدك تعمل connection هاي ال
قد استخدمناها مثثان تروح من ال client لـ server أو ترجع
بالعكس في آن واحد.

Multiplexing and Demultiplexing

- Like UDP, TCP performs multiplexing at the sender and demultiplexing at the receiver.
- However, since TCP is a connection-oriented protocol, a connection needs to be established for each pair of processes.

Connection-Oriented Service

- TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send to and receive data from another process at site B, the following three phases occur:
 - o The two TCP's establish a logical connection (3-way handshake).
 - o Data are exchanged in both directions.
 - o The connection is terminated (3-way connection teardown).

Reliable Service

- TCP is a reliable transport protocol.
- It uses an acknowledgment mechanism to check the safe and sound arrival of data.

- كيف بحقق مفهوم ال reliable بستخدم ال sequence number



TCP Features

- To provide the services mentioned in the previous section, TCP has several features that are briefly summarized in this section and discussed later in detail.

Numbering System

- Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header.
- Instead, there are two fields, called the sequence number and the acknowledgment number.
- These two fields refer to a byte number and not a segment number.

Example

Suppose a TCP connection is transferring a file of 5,000 bytes. The first byte is numbered 10,001. What are the sequence numbers for each segment if data are sent in five segments, each carrying 1,000 bytes?

Segment 1	→	Sequence number:	10,001	Range:	10,001	to	11,000
Segment 2	→	Sequence number:	11,001	Range:	11,001	to	12,000
Segment 3	→	Sequence number:	12,001	Range:	12,001	to	13,000
Segment 4	→	Sequence number:	13,001	Range:	13,001	to	14,000
Segment 5	→	Sequence number:	14,001	Range:	14,001	to	15,000

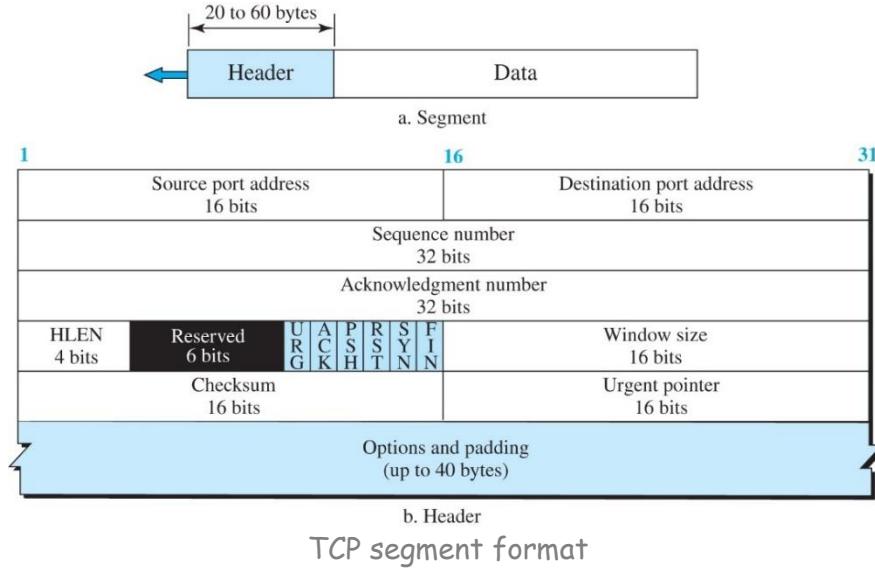
Segment

A packet in TCP is called a segment.

Format

- The segment consists of a header of 20 to 60 bytes, followed by data from the application program.
- The header is 20 bytes if there are no options and up to 60 bytes if it contains options.





: ACK number(32 bits) -

The sequence number of the next byte (next segment) expected from the other end point

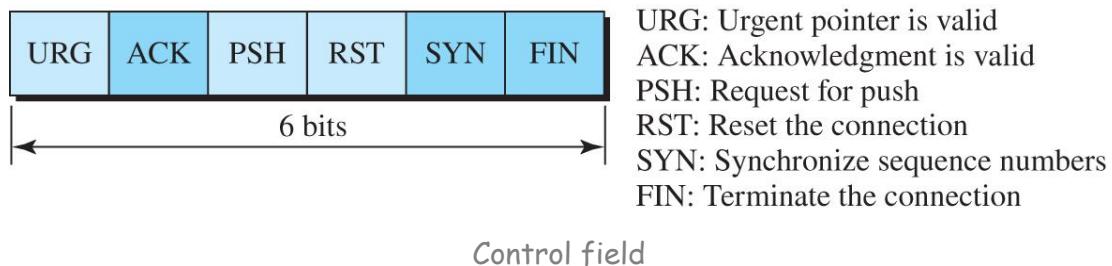
أما ال sequence number (first byte in this segment) -

ال HLEN نفس ال IP بقسمها على 4 -

إلي بعد ال reserved هم عبارة عن 6 bits كل flag بمثيل bit وإذا كان مضوي

URG, ACK, PSH, RST, SYN,) TCP segment ال flag يعني لـ (FIN -

ال window size مشان ال flow control قد يه ال Window size -
مشان تتفاهم مع ال destination .



Encapsulation

- A TCP segment encapsulates the data received from the application layer.
- The TCP segment is encapsulated in an IP datagram, which in turn is encapsulated in a frame at the data-link layer.



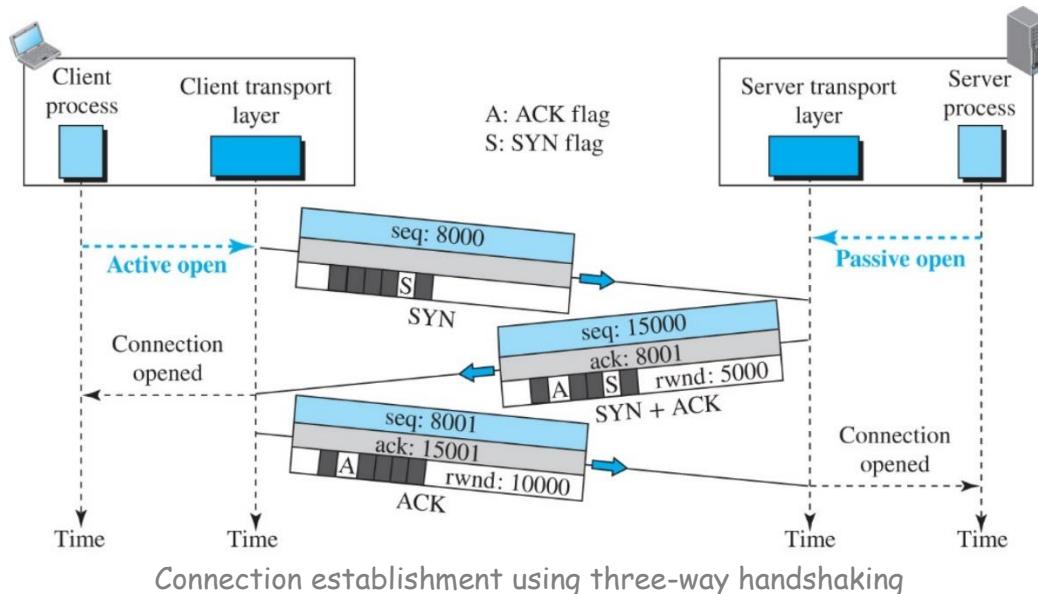
A TCP Connection

- TCP is connection-oriented.
- All of the segments belonging to a message are then sent over this logical path.
- Using a single logical pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames.
- You may wonder how TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented.
- The point is that a TCP connection is logical, not physical.
- TCP operates at a higher level.
- TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself.

.IP protocol بعوض عن الموجود بالTCP protocol -

Connection Establishment

- TCP transmits data in full-duplex mode.
- When two TCPs in two machines are connected, they are able to send segments to each other simultaneously.
- This implies that each party must initialize communication and get approval from the other party before any data are transferred.



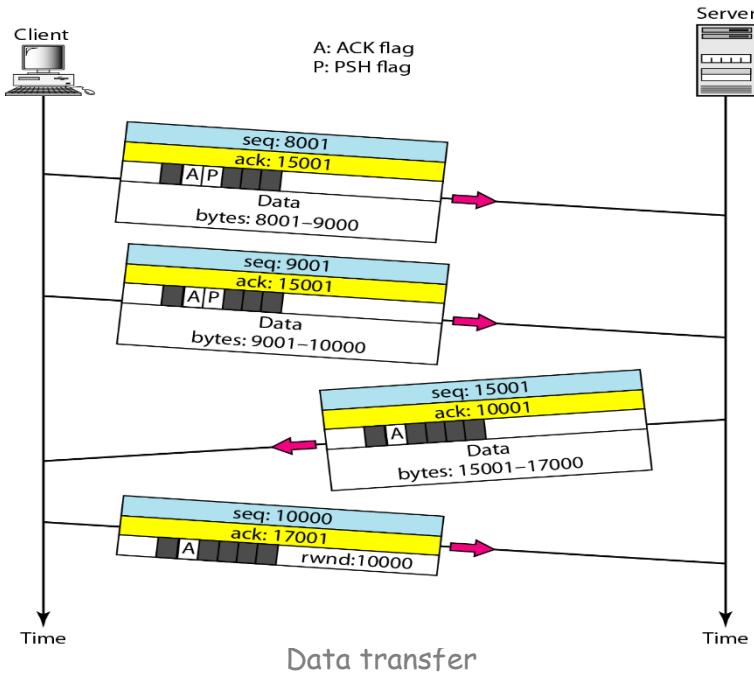
****هـى الرسمة مهمة و نتيجـى بالامتحانات.**

- السيناريو أنه في client بده يشبّك على server الـ seqNO = 8000 (ما في داتا) والـ client بلش يرقم البايتس من 8001 الـ Active open يلي طالب الخدمة هو الي بيادر والي بطلب connection الي يكون Active (الي ببعثت الـ SYN).
الي وظيفته يعطي رد فعل للـ SYN هو الـ passive.
بالـ SYN ما في ACK number لأنّي ما بعرف إذا الـ server بده يرد علي أصلًا أو لـ، وبس تكون الـ SYN flag هي الـ on وبيعتها
الرسالة هاي لما توصل للـ server بفهم أنه مطلوب منه establishment . 3-way handshaking
بالـ SYN+ACK والـ server وافق أنه يحكي مع الـ client ببعثت للـ seqNO. والـ next segment الي رح توصل من الـ client لازم تكون 15000، يعني الرقم الي بنحط بالـ ACK هون ما دخله بالرسالة نفسها قصده عن الرقم الي لازم يجي بعدها.
الـ receive window هو الـ buffer الي بستقبل الداتا منه بوسع 5000 بايت هون، وانتبهوا أنه رد عليه بـ SYN+ACK.
بالـ ACK ببعثت معها كمان الداتا (piggybacking).

Data Transfer

- After connection is established, bidirectional data transfer can take place.
 - The client and server can send data and acknowledgments in both directions.
 - Data traveling in the same direction as an acknowledgment are carried on the same segment.
 - The acknowledgment is piggybacked with the data.



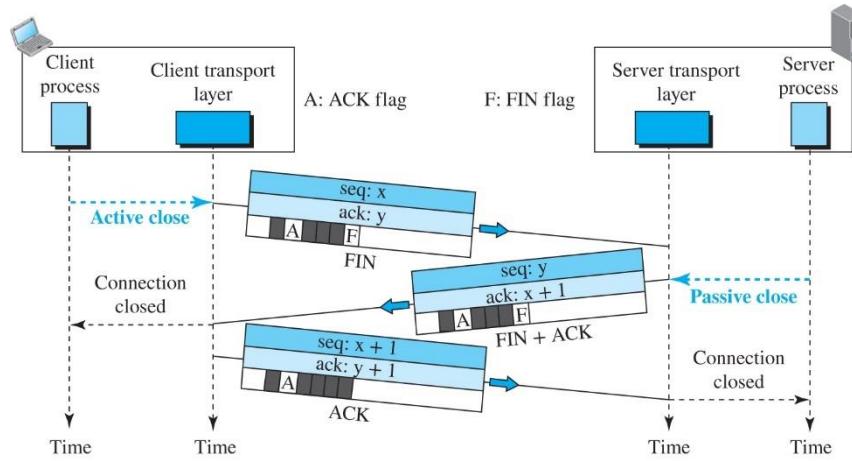


هون احنا عديننا مرحلة الـ 3-way handshaking وعم نبعث داتا عاديّة.
الـ ACK تراكميّة -

بتشبه فكرة الي قبله، لو لسا مو فاهمين ارجعوا لهالي المحاضرة الدقيقة: 1:00:30

Connection Termination

- Either of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client.
- Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

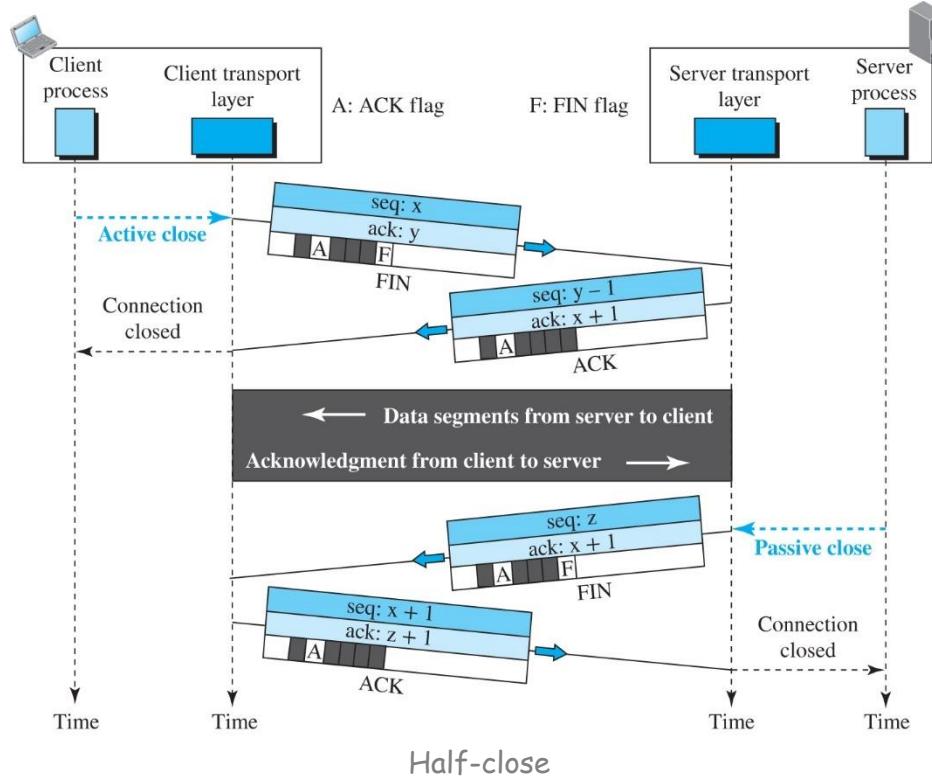


Connection termination using three-way handshaking



- هون کمان عم نعمل بس بأنواع 3-way handshaking مختلفه.
- بما أنه هو الي بادر بال active open معناته لازم يبادر بال active close.
- هون ال هون تكون FIN flag
- ال full close or half close بعتمد على هل سحبت بيانتي من ال server أو لا.

*انتبهوا على استهلاك ال sequence window مهم تكونوا عارفينهم.



- هون بسکر بوجه ال client انه ييعتله بس مسموح يستقبل منه، بس مسموح ييعتله ACK.
- بنعرف انه half duplex لأنه لما رد عليه ال server ما حط FIN وكمان برجع خطوة للخلف بال seqNO (لأنه سمعه بس مو جاهز يسکر هلا).
- ال client تكون بتكون بعد ما أخذ ال ACK من ال server على آخر .bit



Connection Reset

- TCP at one end may deny a connection request, may abort an existing connection, or may terminate an idle connection. All of these are done with the RST (reset) flag.

.connection reset يفصل سبب أو لآخر فبنعمل server -

Windows in TCP

- Before discussing data transfer in TCP and the issues such as flow, error, and congestion control, we describe the windows used in TCP.
- TCP uses two windows (send window and receive window) for each direction of data transfer, which means four windows for a bidirectional communication.
- To make the discussion simple, we make an unrealistic assumption that communication is only unidirectional.
- The bidirectional communication can be inferred using two unidirectional communications with piggybacking.

لما حكينا عن ال connection establishment أو ال data transfer كانوا -

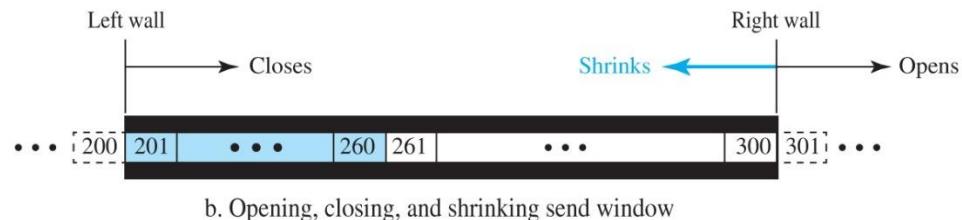
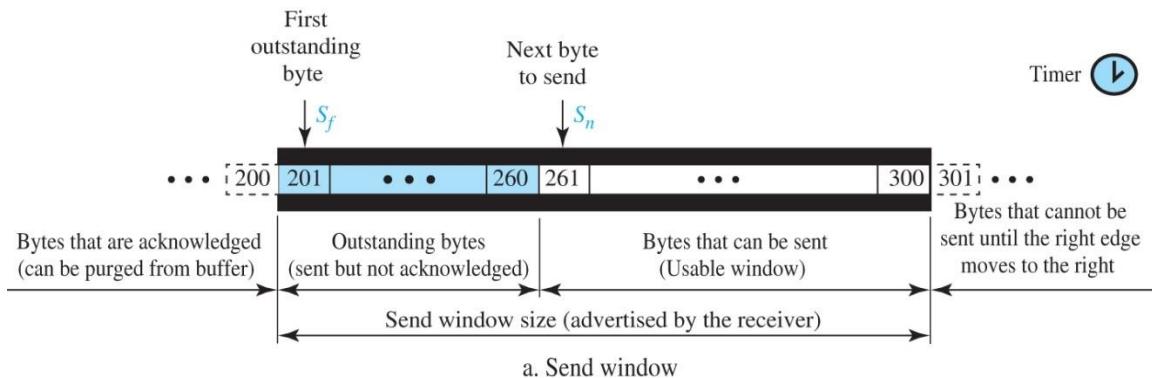
يعني قد يه عندي مساحة أتحمل داتا تضخ على عشان نضبط

.flow control

Send Window

- Figure shows an example of a send window. The window size is 100 bytes but later we see that the send window size is dictated by the receiver (flow control) and the congestion in the underlying network (congestion control). The figure shows how a send window opens, closes, or shrinks.

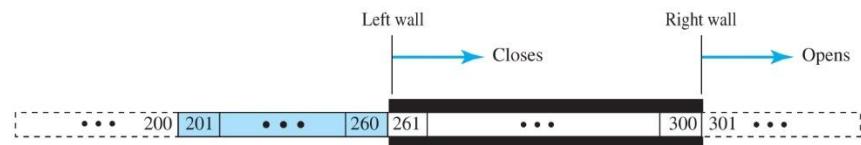
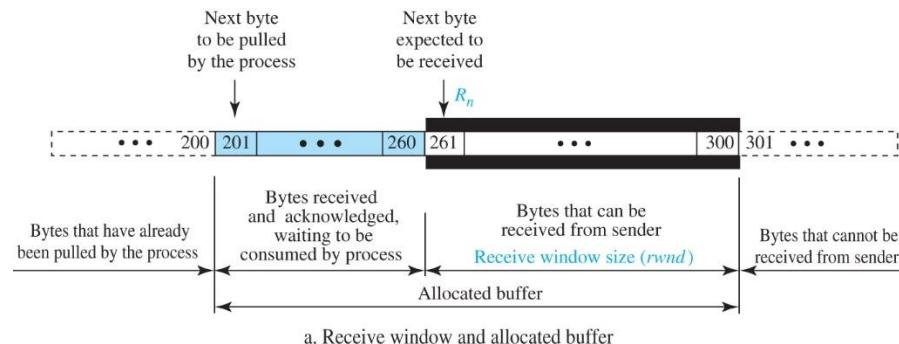




- حسب تدفق البيانات وسرعتك بالحصول على ال ACK اول send window ممكن أنها تتواز أو تضيق.
- بالرسمة مستخدمين ال linear format

Receive Window

- Figure shows an example of a receive window. The window size is 100 bytes. The figure also shows how the receive window opens and closes; in practice, the window should never shrink.

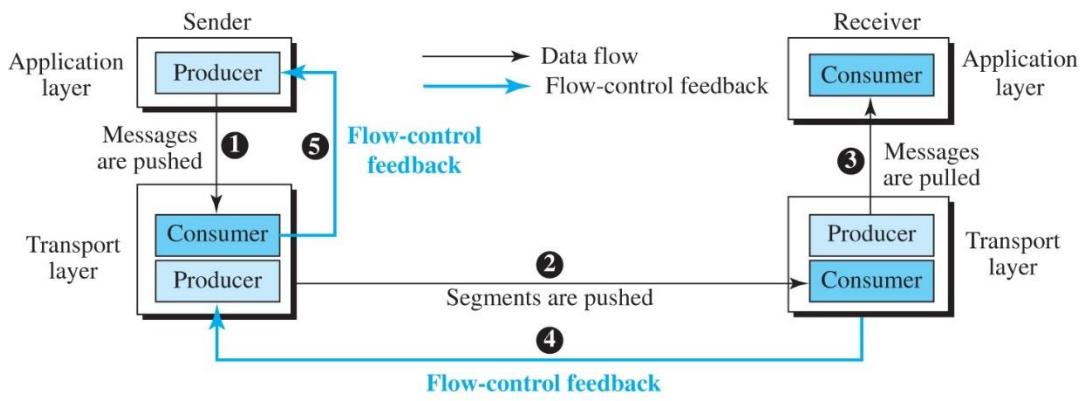


- عم بستلم الداتا الي جاي من ال sender



Flow Control

- As discussed before, flow control balances the rate a producer creates data with the rate a consumer can use the data.
- TCP separates flow control from error control.
- In this section we discuss flow control, ignoring error control. We assume that the logical channel between the sending and receiving TCP is error-free.



Data flow and flow control feedbacks in TCP

Opening and Closing Windows

- To achieve flow control, TCP forces the sender and the receiver to adjust their window sizes, although the size of the buffer for both parties is fixed when the connection is established.
- The receive window closes (moves its left wall to the right) when more bytes arrive from the sender; it opens (moves its right wall to the right) when more bytes are pulled by the process.
- We assume that it does not shrink (the right wall does not move to the left).

Error Control

- TCP is a reliable transport-layer protocol. This means that an application program that delivers a stream of data to TCP relies on TCP to deliver the entire stream to the application program on the other end in order, without error, and without any part lost or duplicated.



Acknowledgment

- TCP uses acknowledgments to confirm the receipt of data segments.
- Control segments that carry no data, but consume a sequence number, are also acknowledged.
- ACK segments are never acknowledged.

Retransmission

- The heart of the error control mechanism is the retransmission of segments. When a segment is sent, it is stored in a queue until it is acknowledged.
- When the retransmission timer expires or when the sender receives three duplicate ACKs for the first segment in the queue, that segment is retransmitted.

يسمح لـ TCP protocol أنه يشير لما الداتا ما توصل أو توصل -

. retransmission فتفعل ال ACK بحجب corrupted

Out-of-Order Segments

- TCP implementations today do not discard out-of-order segments.
- They store them temporarily and flag them as out-of-order segments until the missing segments arrive.
- Note, however, that out-of-order segments are never delivered to the process.
- TCP guarantees that data are delivered to the process in order.

TCP Congestion Control

- When we discussed flow control in TCP, we mentioned that the size of the send window is controlled by the receiver using the value of rwnd, which is advertised in each segment traveling in the opposite direction.
- The use of this strategy guarantees that the receive window is never overflowed with the received bytes (no end congestion).

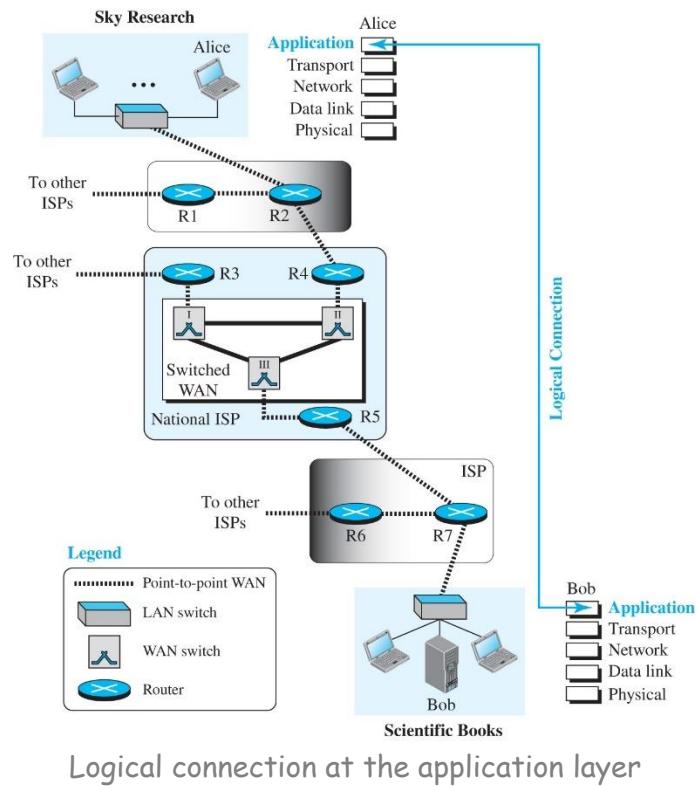


- This, however, does not mean that the intermediate buffers, buffers in the routers, do not become congested.
- A router may receive data from more than one sender.
 - ال windows بشكل أساسی بخدم ال flow control وكمان بساهم بطريقة غير
مباشرة بتخفيف ال congestion .



Chapter 10: Application Layer

- The application layer provides services to the user.
- Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages.



Logical connection at the application layer

نفس ال transport layer ما بتشفوف ال path بتفاصيله، مجرد ما صار في logical destination من ال source path .
- معلوم من ال source path بريطهم connection

Application-Layer Paradigms

- It should be clear that to use the Internet we need two application programs to interact with each other: one running on a computer somewhere in the world, the other running on another computer somewhere else in the world.



- The two programs need to send messages to each other through the Internet infrastructure. However, we have not discussed what the relationship should be between these programs.
- Two paradigms have been developed: the client-server paradigm and the peer-to-peer paradigm.

آلية لعب الأدوار ما بين الـ process والـ sender الموجودة على الـ receiver .

التطبيقات التي تستخدم عبر الشبكة نوعين: -

client-server paradigm and peer-to-peer paradigm . هدول الاثنين يعرفوا مين الأدوار لما يكون في application عالجهاز الأول بحكي معاه نسخة ثانية عالجهاز الثاني فتكون في تحديد للأدوار.

الـ client-server paradigm تكون في طرف يلعب دائماً دور الـ client (حدا بطلب الخدمة) وطرف دائماً server (التطبيق الي بيعطي الخدمة) وما بتبدل الأدوار بينهم .

الـ peer-to-peer paradigm أي application شابك على الشبكة ممكن بأي لحظة يتطلب أو يقدم خدمة (هون بصير في تبادل للأدوار).

وفي الـ Application هو الـ Hybrid مرة بتصرف بطريقة الـ client server ومرة بطريقة peer to peer .

1- Client-Server

- The traditional paradigm is called the client-server paradigm.
- It was the most popular paradigm until a few years ago.
- In this paradigm, the service provider is an application program, called the server process; it runs continuously, waiting for another application program, called the client process, to make a connection through the Internet and ask for service.
- There are normally some server processes that can provide a specific type of service, but there are many clients that request service from any of these server processes.
- The server process must be running all the time; the client process is started when the client needs to receive service.

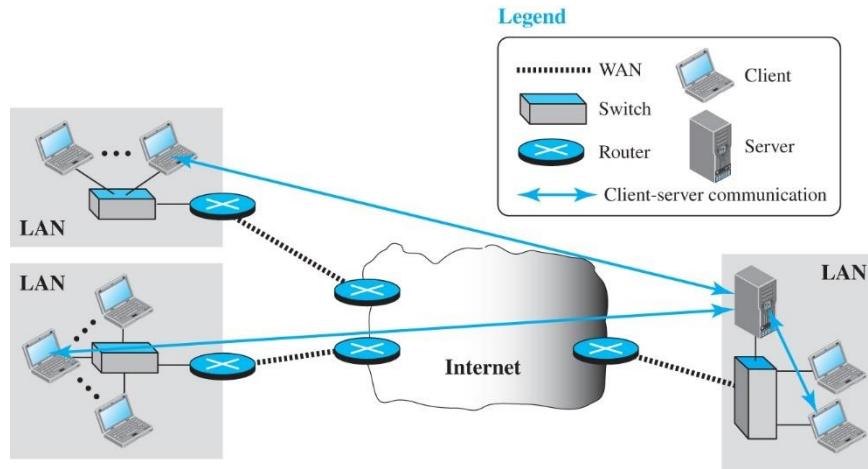
كلاسيكي وقديم .

هون الـ server process بشتغل 24/7 يعني ما بطفي . وحتى لما نكتب له كود infinite loop بنكتبه .



- أما الـ **client process** بيجي وبروح، الكود تبعه تكون مؤقت بس بعمل مجموعة من التعليمات وبحصل من خلالها على خدمات من الـ **server** وبنتهي الكود.

- قبل ما الـ **client** يطلب خدمة من الـ **server** لازم الـ **server** أصلًا يكون شغال وجاهز يستقبل طلبات (مش **hardware** مش **application process**).



Example of a client-server paradigm

- الرسمة بتوضح على مستوى الـ **application**.
اللابتوب بمثلاوا الـ **clients**. والـ **server** بمثلاوا الـ **case**.
الـ **clients** ما بحكوا مع بعض. الكل بحكي بس مع الـ **server**

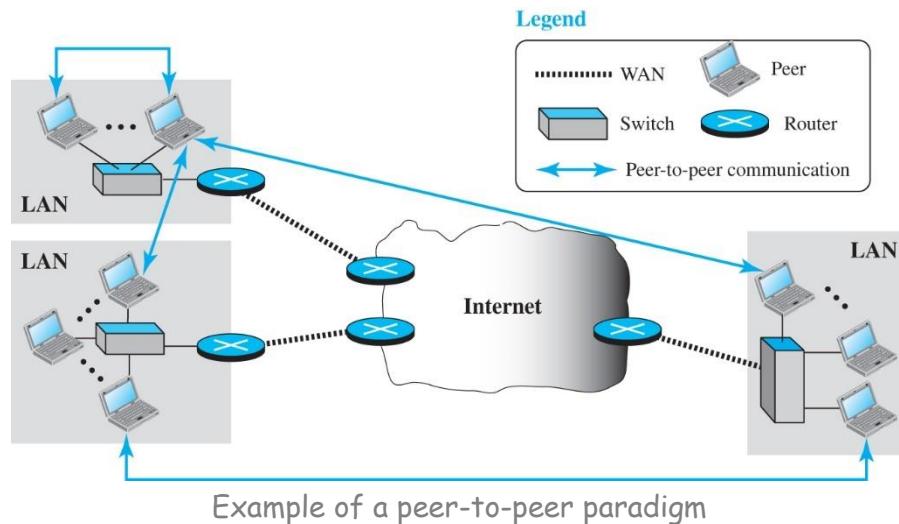
2- Peer-to-Peer

- A new paradigm, called the peer-to-peer paradigm (often abbreviated P2P paradigm) has emerged to respond to the needs of some new applications.
- In this paradigm, there is no need for a server process to be running all the time and waiting for the client processes to connect.
- The responsibility is shared between peers.
- A computer connected to the Internet can provide service at one time and receive service at another time.
- A computer can even provide and receive services at the same time.

- مثال عليها: لما يكون الحاسوب مخزن أجزاء من الملفات ، مثل **server** واحد بخزن كل الملف، كل مستخدم يكون عنده جزء من هاي الملفات (**blocks**). ولو



بـدك ملف معين بتحكي مع ال peers وكل واحد بعطيك الشقة الـي عنده من الملف وبتجمـعـه (هـيك انت بتكون client وهم server).
بس بـلحـظـة ثـانـيـة مـمـكـن يـجي وـاحـدـ من الـpeers يـطـلـبـوا مـنـكـ المـلـفـ الـيـ عنـدـكـ .client وـتـخـدمـهـمـ وـتـعـطـيـهـمـ ايـاهـ فـهـيـكـ اـنتـ بتـصـيرـ server وـهمـ



- الاختلاف هون انه بـطلـ فيـ صـارـواـ كلـهمـ زـيـ بعضـ وـأـيـ 2ـ مـمـكـنـ يـحـكـواـ معـ بعضـ.

Mixed Paradigm

- An application may choose to use a mixture of the two paradigms by combining the advantages of both.
- For example, a light-load client-server communication can be used to find the address of the peer that can offer a service.
- When the address of the peer is found, the actual service can be received from the peer by using the peer-to-peer paradigm.
الـيـ هوـ الـhybridـ بـدمـجـ بـيـنـ النـوـعـيـنـ.

World Wide Web and HTTP

- In this section, we first introduce the World Wide Web (abbreviated WWW or Web). We then discuss the HyperText Transfer Protocol (HTTP), the most common client-server application program used in relation to the Web.

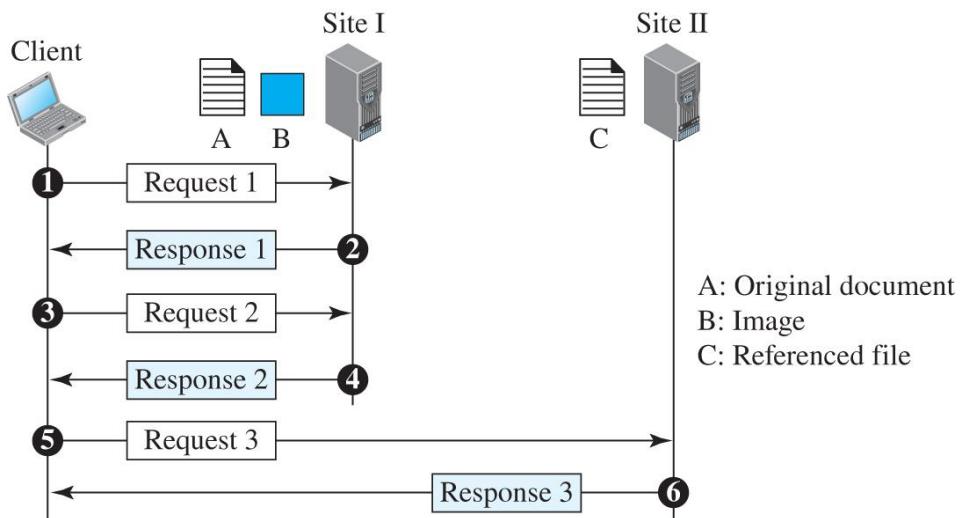


- الشبكة العنكبوتية العالمية التي تحتوي على كل الملفات والويبسait
صفحات الويب.

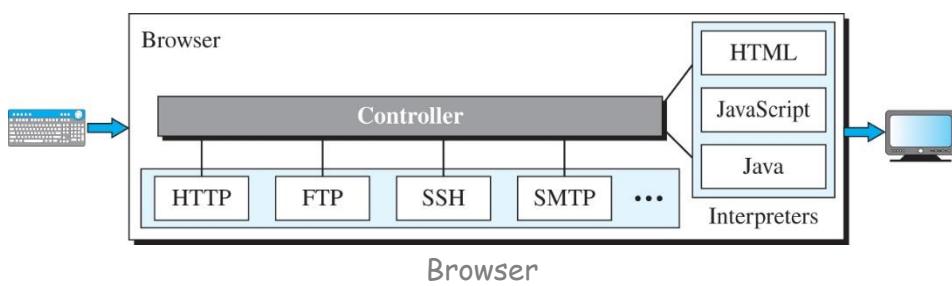
- The idea of the Web was first proposed by Tim Berners-Lee in 1989 at CERN, the European Organization for Nuclear Research, to allow several researchers at different locations throughout Europe to access each others' researches.
- The commercial Web started in the early 1990s.

Example

Assume we need to retrieve a scientific document that contains one reference to another text file and one reference to a large image.



أكتر اشي بساعدني أتعامل مع الويب هو ال web browsers -
آلية العمل بالويب هي client server هي -
ال client يطلب بـ page or document أو أي محتوى على الانترنت فبنعمت -
. response وبحصل على ال request



Web browser -
البروتوكول الوحدى الي بفهمه، وظيفته أني يفتحي الصفحات الموجودة على الانترنت.

- تكون من controller الى بخلينا نختار لل browser على أي protocol رح يشتغل واي بفهم الكود (جافا، جافا سكريبت، html) بنسميهم .Interpreters

- Hypertext Transfer Protocol) HTTP (امتدادات ال HTML) تنقلها بين clients و servers .
يعني لما تفتح صفحة جوجل ال HTTP protocol بتفعل من خلال ال browser وبجيبيك محتويات الصفحة.

File Transfer Protocol) FTP (بساعدي أعمل download + upload للملفات ومش شرط خلال الانترنت ممكن خلال الشبكة المحلية.
Secure Shell Protocol) SSH (طريقة مشان نشبك على desktop .(Any desk remotely

Simple Mail Transfer Protocol) SMTP (Bفهم شغلات الايميل (attach, .(forward, reply,...

- The URL <http://www.mhhe.com/compsci/forouzan/> defines the web page related to one of the computers in the McGraw-Hill company (the three letters www are part of the host name and are added to the commercial host). The path is compsci/forouzan/, which defines Forouzan's web page under the directory compsci (computer science).

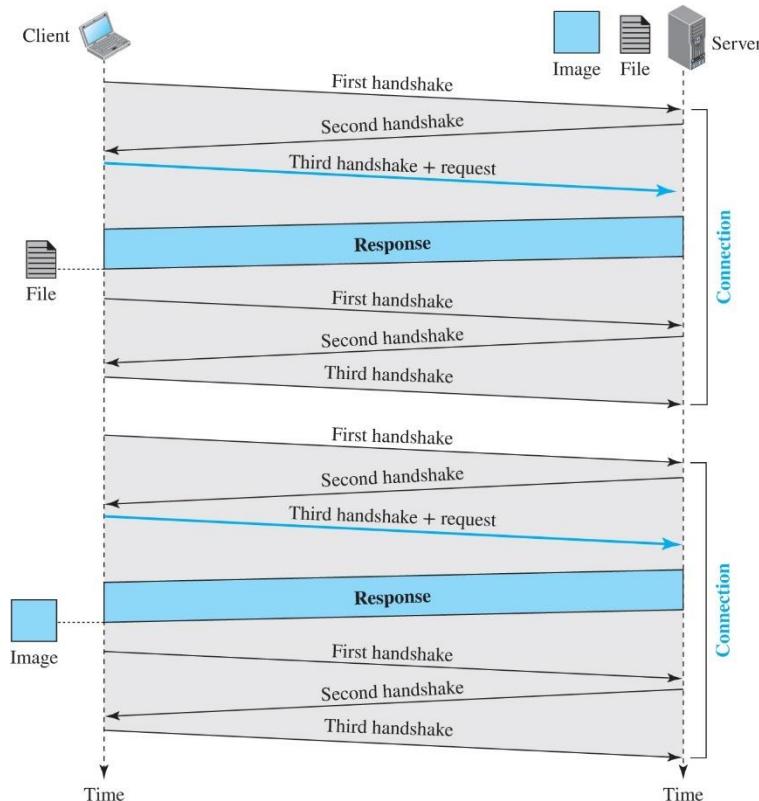
- احنا بنعطي ال browser هاد العنوان وهو وظيفته انه يصل لـ server المعنى ويجيبيه.
- اسم البروتوكول http://

HyperText Transfer Protocol (HTTP)

- A protocol that is used to define how the client-server programs can be written to retrieve web pages from the Web.
- An HTTP client sends a request; an HTTP server returns a response.
- The server uses the port number 80; the client uses a temporary port number.



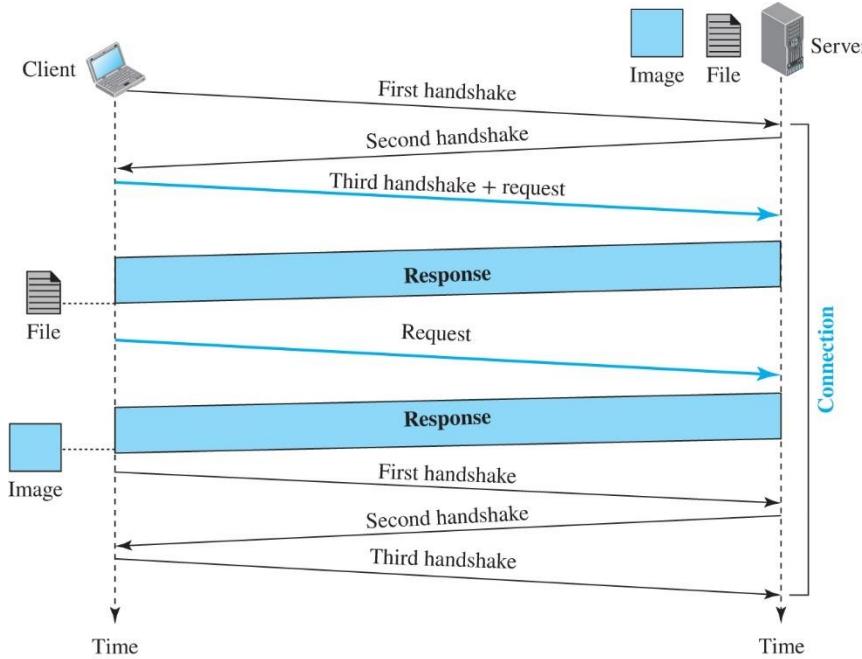
The Figure shows an example of a nonpersistent connection. The client needs to access a file that contains one link to an image. The text file and image are located on the same server. Here we need two connections. For each connection, TCP requires at least three handshake messages to establish the connection, but the request can be sent with the third one. After the connection is established, the object can be transferred. After receiving an object, another three handshake messages are needed to terminate the connection.



- **الـ TCP مبني علىـ http .**
- **مشان نحصل علىـ صفحة ويب معاها (ملفات الصوت أو صورة).**
- **الـ Non-Persistent and Persistent http connection نوعين:**
- **بالرسمة هون الـ Non-Persistent لي؟ لأنه إذاـ صفحة الويب الي بدنـ اياها فيها مجموعة منـ الملفات، كلـ ملف بدهـ TCP connection خاصـ فيه معـ إنه عمـ تحكي نفسـ الـ client عنـ نفسـ server . بسـ الـ server ماـ بعطيـ لهمـ بعطيـ لهمـ كلـ غرضـ الحالـ .**



The Figure shows the same scenario as in last figure, but using a persistent connection. Only one connection establishment and connection termination is used, but the request for the image is sent separately.



هون نوعه **persistent** ، كل الأغراض من نفس ال client لنفس ال server -
ومتعلقة بنفس ال URL . ال TCP connection واحد كافي.

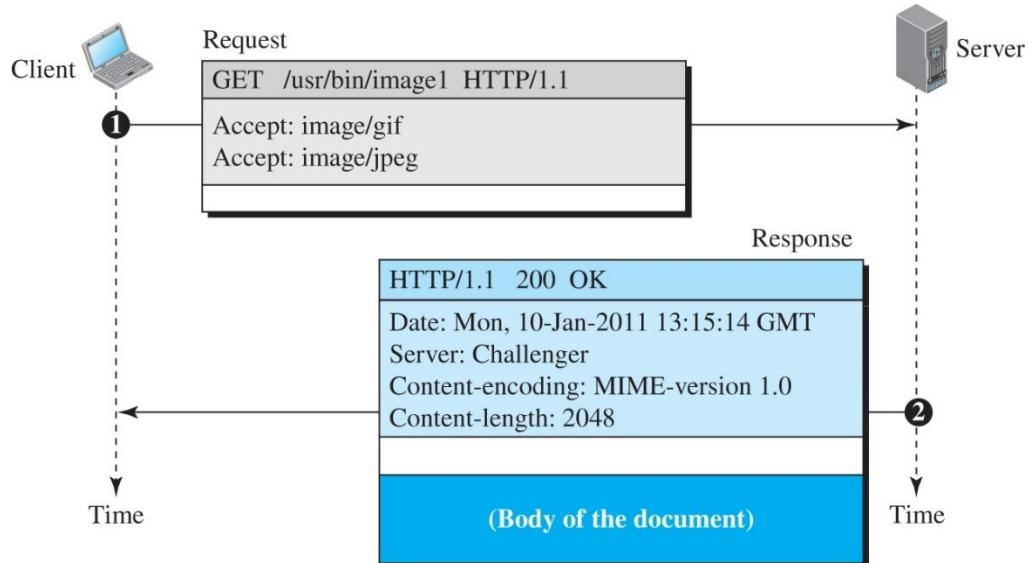
Methods

	<i>Method</i>	<i>Action</i>	
بياناته مثل آخر مرة نعملله تعديل	GET	Requests a document from the server	ملف، صفحة ويب، صورة، صوت
	HEAD	Requests information about a document but not the document itself	
	PUT	Sends a document from the client to the server	لما نعمل attach
	POST	Sends some information from the client to the server	لما نعمل log in
	TRACE	Echoes the incoming request	لما نعمل تبع للموقع
	DELETE	Removes the web page	
	CONNECT	Reserved	
	OPTIONS	Inquires about available options	

.أمثلة على بعض ال commands الموجدة بال http request -



This example retrieves a document (see the Figure). We use the GET method to retrieve an image with the path /usr/bin/image1. The request line shows the method (GET), the URL, and the HTTP version (1.1). The header has two lines that show that the client can accept images in the GIF or JPEG format. The request does not have a body. The response message contains the status line and four lines of header. The header lines define the date, server, content encoding (MIME version, which will be described in electronic mail), and length of the document. The body of the document follows the header.

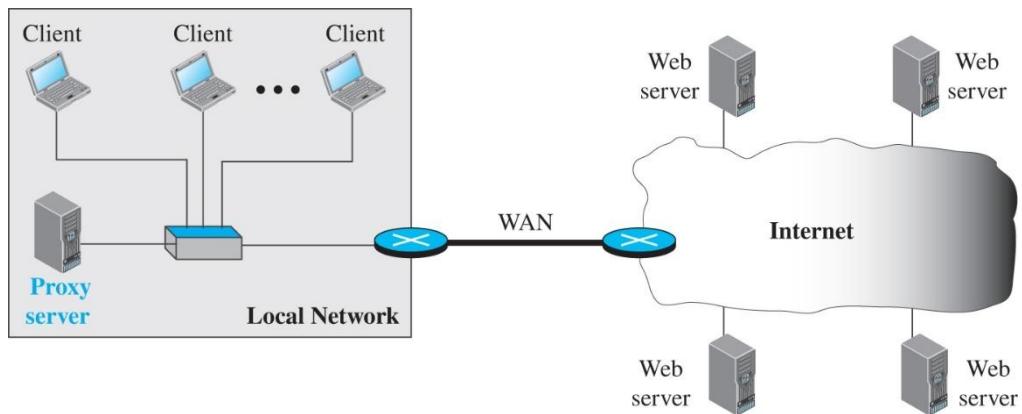


- . فتنا على http request وبس كتبنا ال URL . ال browser بترجمه ل -
- بيعث get command للسيرفر ، والامتدادات الي قبلها (gif, jpeg)
- ال server برد وبعطيه شوي داتا كيف يستخدم الصورة أو إذا صار خطأ يعرف
- شو هو .
- 200 يعني ملف تم تنفيذه بنجاح .

The Figure shows an example of a use of a proxy server in a local network, such as the network on a campus or in a company. The proxy server is installed in the local network. When an HTTP request is created by any of the clients (browsers), the request is first directed to the proxy server. If the proxy server already has the corresponding web page, it sends the response to the client. Otherwise, the proxy server acts as a client and sends the request to the web server in the Internet.



When the response is returned, the proxy server makes a copy and stores it in its cache before sending it to the requesting client.



- ال proxy هو عبارة عن وسيط ما بين ال Local network and the Internet
- ال proxy لما يشوف اليوزر زعم بطلبيوا صفحات معينة بالتكرار بتحفظ بنسخة
- عنده، مشان بدل ما يغلب حاله كل مرة على الانترنت ويحكي مع بتحفظ فيها.
- بختصر وقت وجهد بدل ما كل مرة يجيب الصفحات ويرجعهم لل clients
- فبنخفف الضغط على الشبكة.

HTTP Security

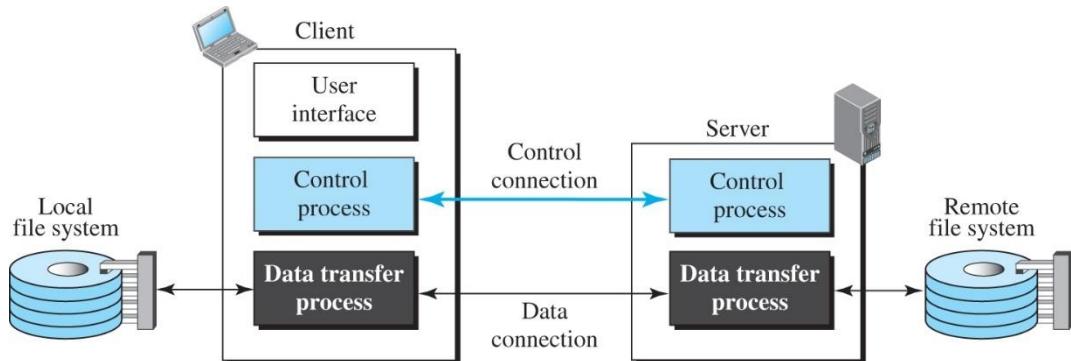
- HTTP per se does not provide security.
- However, HTTP can be run over the Secure Socket Layer (SSL).
- In this case, HTTP is referred to as HTTPS.
- HTTPS provides confidentiality, client and server authentication, and data integrity.

FTP

- File Transfer Protocol (FTP) is the standard protocol provided by TCP/IP for copying a file from one host to another.
- Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.
- For example, two systems may use different file name conventions.
- Two systems may have different ways to represent data.
- Two systems may have different directory structures.



- All of these problems have been solved by FTP in a very simple and elegant approach.
 - Although we can transfer files using HTTP, FTP is a better choice to transfer large files or to transfer files using different formats.
- بدي أنسخ ملف من جهاز لجهاز أو أعمل download لملف عندي أو أطلع ملف .file server على ال عندي



بكون عندي ال client بدعمه نظام التشغيل تبع ال local file system وفي user interface, control process, data transfer) 3 process عندنده (process

ال FTP ما فتح بس connection وحدة بفتح connection الأول responsible عن control process connection الها علاقة بال processes commands الثانيه data transfer process : بس تدفق بيانات.

Electronic Mail

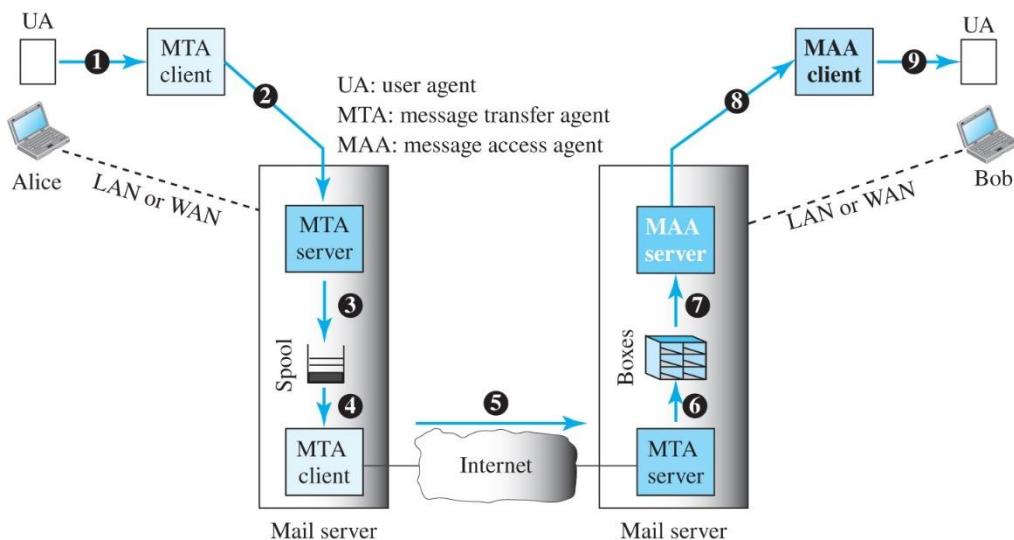
- Electronic mail (or e-mail) allows users to exchange messages.
- The nature of this application, however, is different from other applications discussed so far.
- In an application such as HTTP or FTP, the server program is running all the time, waiting for a request from a client.
- When the request arrives, the server provides the service.
- There is a request and there is a response.
- In the case of electronic mail, the situation is different.
- First, e-mail is considered a one-way transaction.



- When Alice sends an e-mail to Bob, she may expect a response, but this is not a mandate.

Architecture

To explain the architecture of e-mail, we give a common scenario, as shown in the Figure. Another possibility is the case in which Alice or Bob is directly connected to the corresponding mail server, in which LAN or WAN connection is not required, but this variation in the scenario does not affect our discussion.

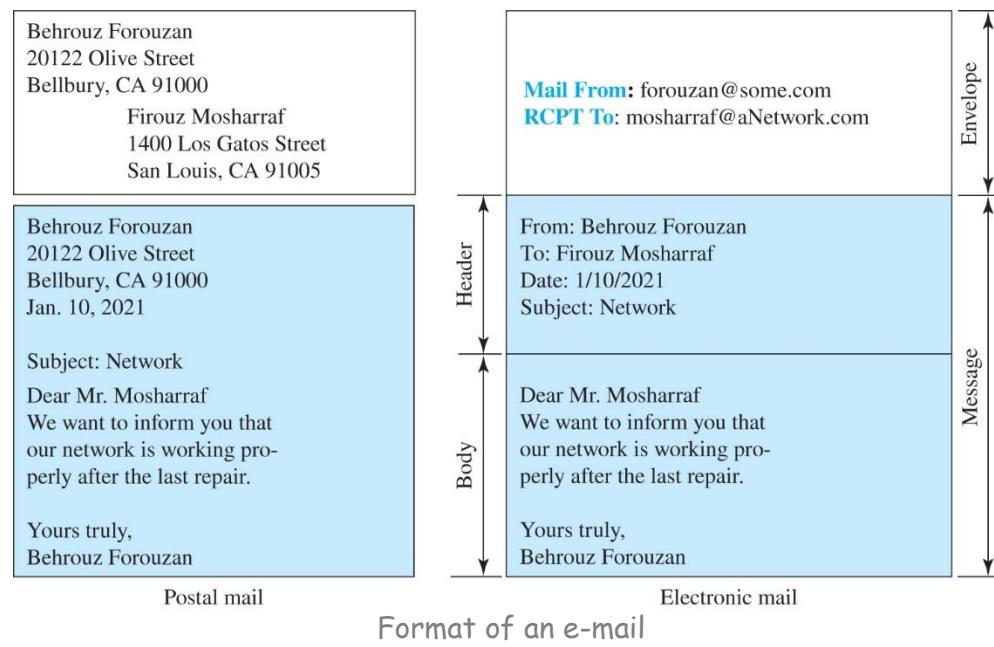


مشان تشبك من خلال الايميل، الي بحکوا مع بعض تكونوا
وبشبکوا على الانترنت من خلال mail server .
الل client واحده تكون mail server والثاني server ممكن بعدين يعكسوا
الأدوار عادي
أما بين ال MTA server و MTA client ما بتغيروا ال server بضل زي ما هو
وال client نفس الشي (ونفس الشي لل MMA server and MTA
.server
ال MTA server بيأخذ الرسالة وبفوت على الأنبوت وبتحول ل client بالنسبة
ل السيرفر الي رح يستلم الرسالة. السيرفر يستلم الرسالة عبر الانترنت
وبحطها بصندوق بريد(لكل اليوزر) بتروح على ال MMA server بعدين بوديها
على ال inbox الخاص بيوزر معين.



User Agent

- The first component of an electronic mail system is the user agent (UA).
- It provides service to the user to make the process of sending and receiving a message easier.
- A user agent is a software package (program) that composes, reads, replies to, and forwards messages.
- It also handles local mailboxes on the user computers.



Local part

@

Domain name

Mailbox address of the recipient

The domain name of the mail server

E-mail address

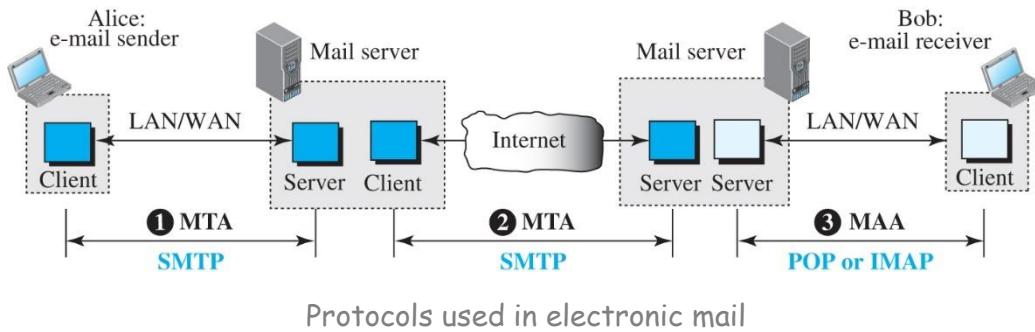
شكل من أشكال الـ Application specific addressing -

Message Transfer Agent: SMTP

- We can say that the e-mail is one of those applications that needs three uses of client-server paradigms to accomplish its task.
- It is important that we distinguish these three when we are dealing with e-mail.



- Figure shows these three client-server applications.
- We refer to the first and the second as Message Transfer Agents (MTAs), the third as Message Access Agent (MAA).

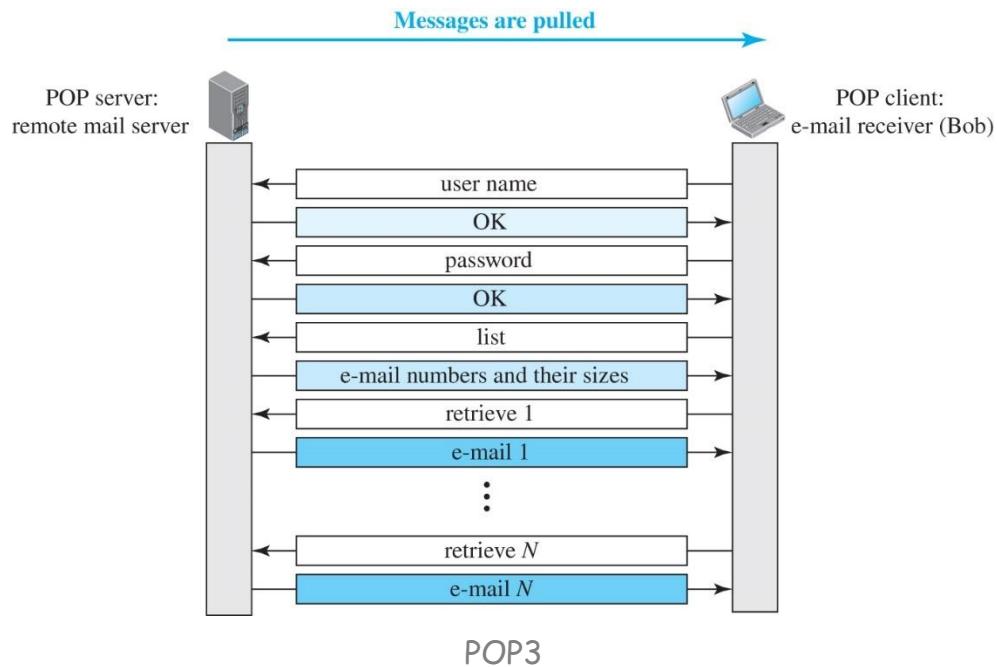


عشنان ال client يشبك على ال server المسؤول عنه يستخدم .SMTP -
آخر اشي استخدمنا POP or IMAP لأنهم بسمحولي استحوذ على الرسالة من inbox تبعي.

Message Access Agent: POP and IMAP

- The first and second stages of mail delivery use SMTP.
- However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- In other words, the direction of the bulk data (messages) is from the client to the server.
- On the other hand, the third stage needs a pull protocol; the client must pull messages from the server.
- The direction of the bulk data is from the server to the client.
- The third stage uses a message access agent.





هون عم بورجينا كيف الشخص يستحوذ على الرسالة تبعته . -

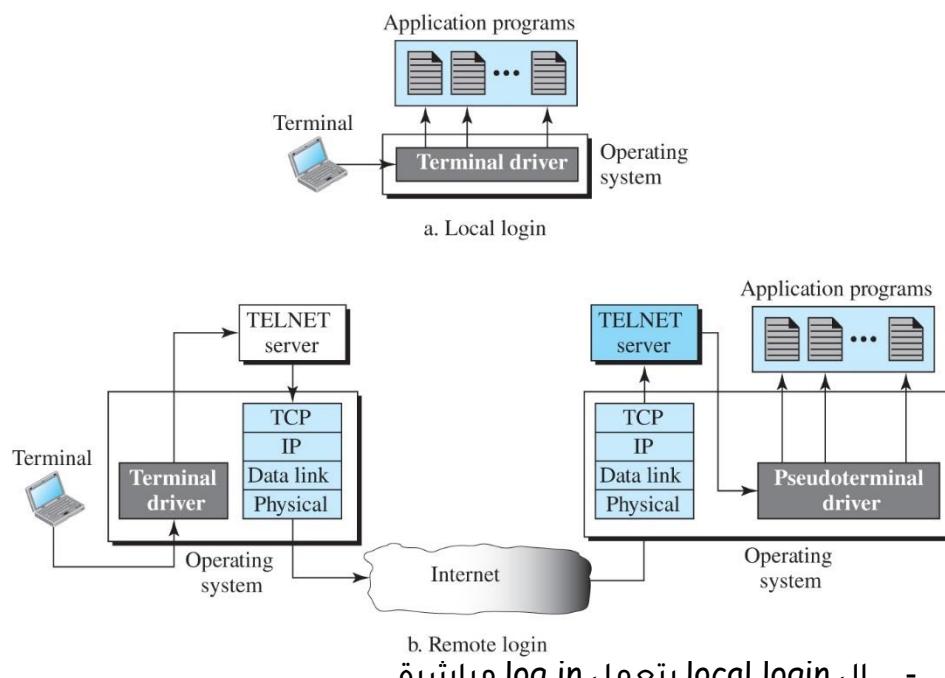
Telnet

- A server program can provide a specific service to its corresponding client program.
- However, it is impossible to have a client/server pair for each type of service we need; the number of servers soon becomes intractable.
- One of the original remote logging protocols is TELNET, which is an abbreviation for TErminal NETwork.
- Although TELNET requires a logging name and password, it is vulnerable to hacking because it sends all data including the password in plaintext (not encrypted).

بروتوكول الهدف منه أنى أشبك عالحاسوب عن بعد . -



Local versus Remote Logging



ال local login بتعمل log in مباشرة . -

Telnet الي مشانه موجود ال Remote login -

بكون عندي جهاز وعاملة عليه login بشغل منظومة من خلال ال telnet وبوصل من خلال الانترنت عن طريقه بوصل لـ application (الكود الي بتحكم بالكمبيوتر) وبفوت عالجهاز pseudoterminal driver

Operation

- TELNET lets the client and server negotiate options before or during the use of the service.
- Options are extra features available to a user with a more sophisticated terminal.
- Users with simpler terminals can use default features.

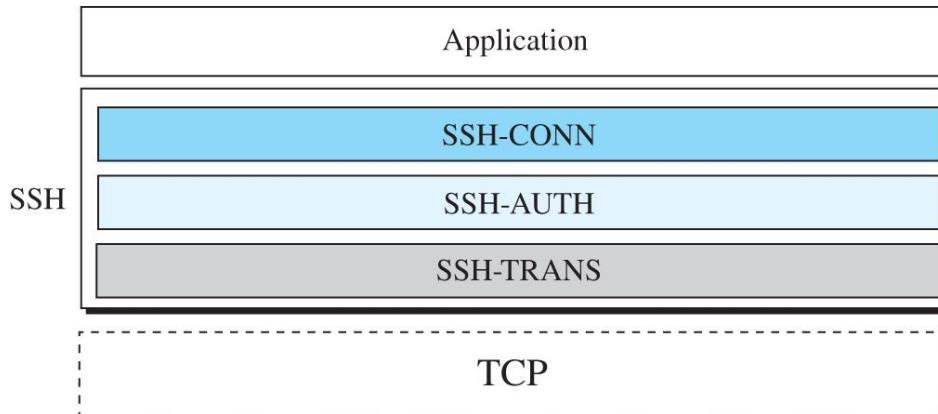
Secure Shell (SSH)

- A secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET.
- There are two versions of SSH: SSH-1 and SSH-2, which are totally incompatible.



- The first version, SSH-1, is now deprecated because of security flaws in it. In this section, we discuss only SSH-2.

(أضعف وحدة فيهם تتضمن الـ Telnet)



أهم اشي نعرف انه ال ssh مبني على ال TCP -

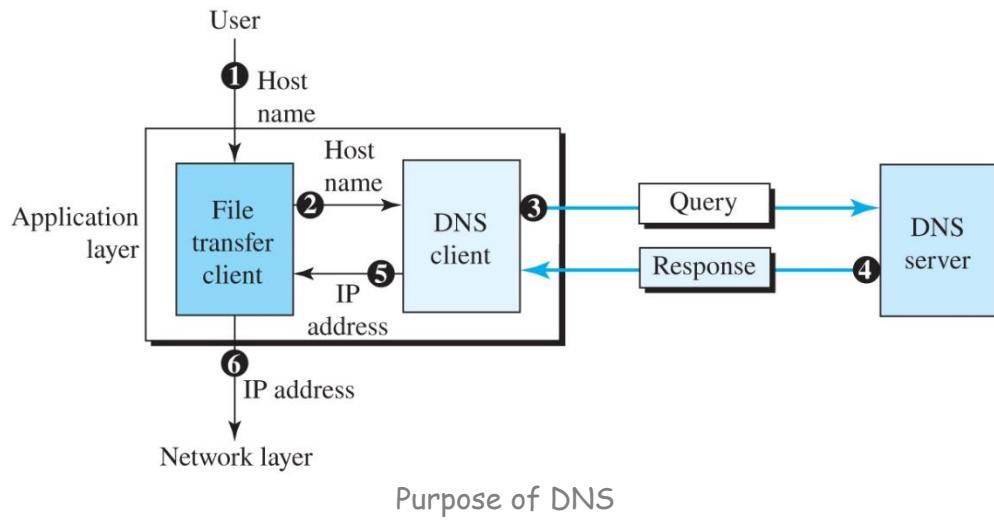
Applications

- Although SSH is often thought of as a replacement for TELNET, SSH is, in fact, a general-purpose protocol that provides a secure connection between a client and server.

Domain Name System (DNS)

- The last client-server application program we discuss has been designed to help other application programs.
- The Internet needs to have a directory system that can map a name to an address.
- This is analogous to the telephone network. The Figure shows how TCP/IP uses a DNS client and a DNS server to map a name to an address.



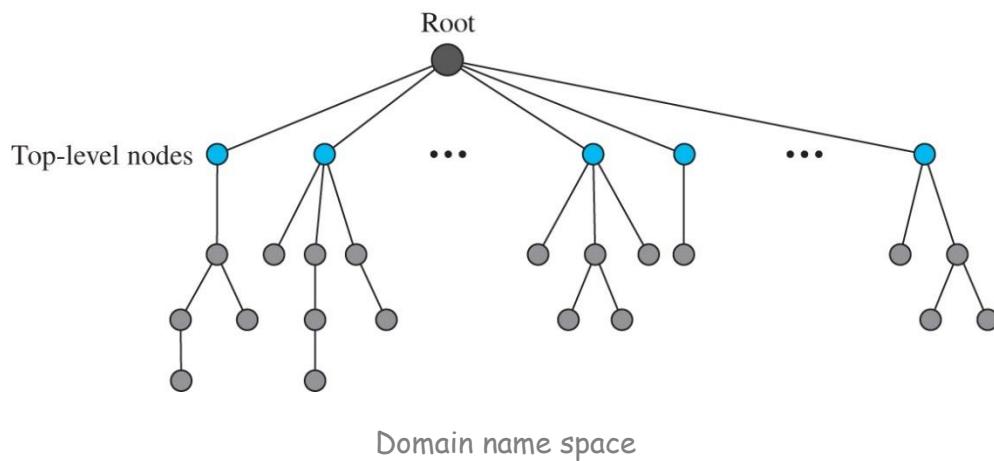


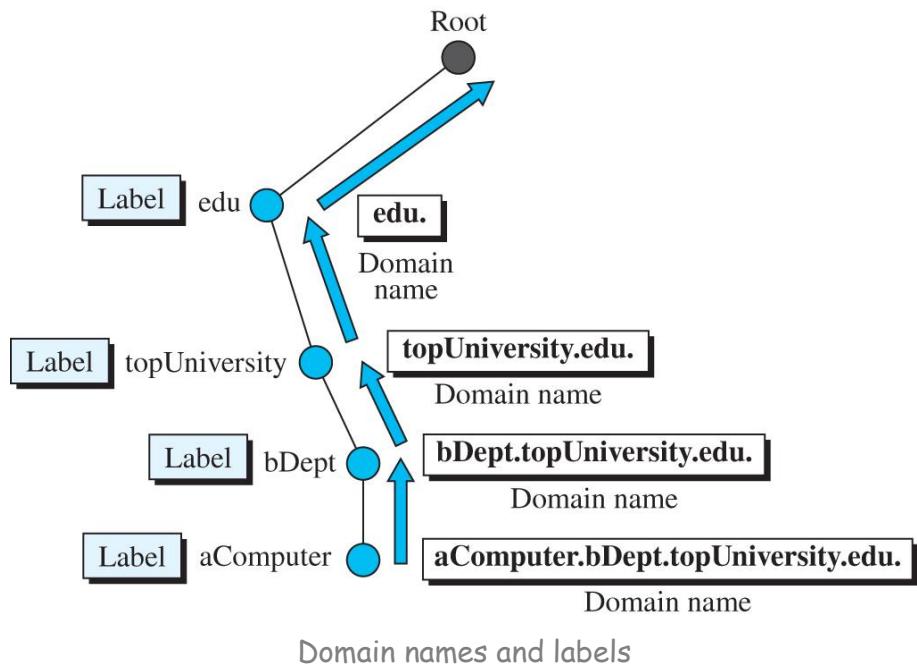
- **IP address** يعطيني host name - **ويمكن العكس**.

Name Space

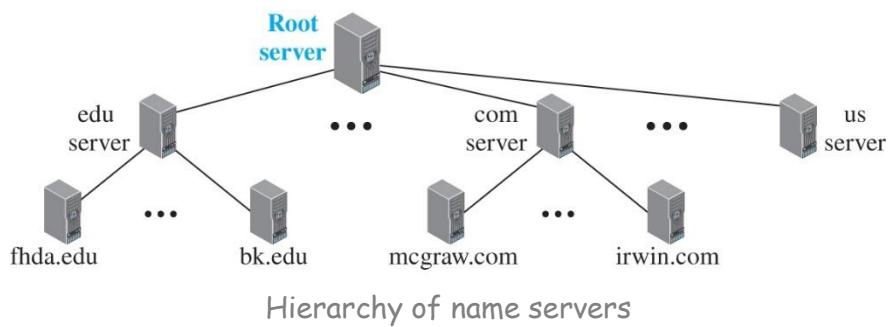
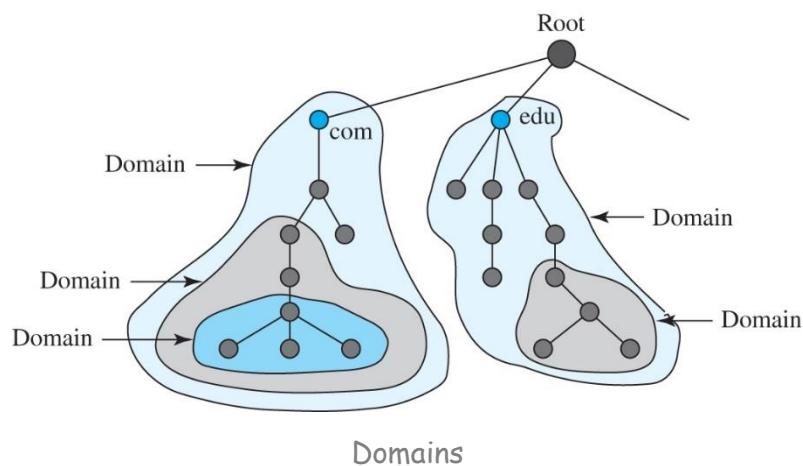
- To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- In other words, the names must be unique because the addresses are unique.
- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

- **الـ host name** لـزم يتبع لنـطـم معـيـن.





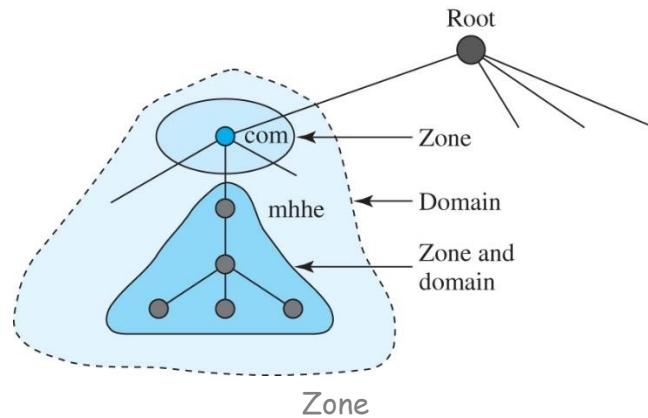
های ال hierarchy بالتسمية هي الی بتخلی اسماء ال hosts غير عشوائية . -



ال root server ما عليه بيانات ولا عن أي حدا عليه pointers عن كل ال servers الثانية بدلنا على أي server نحكي . -



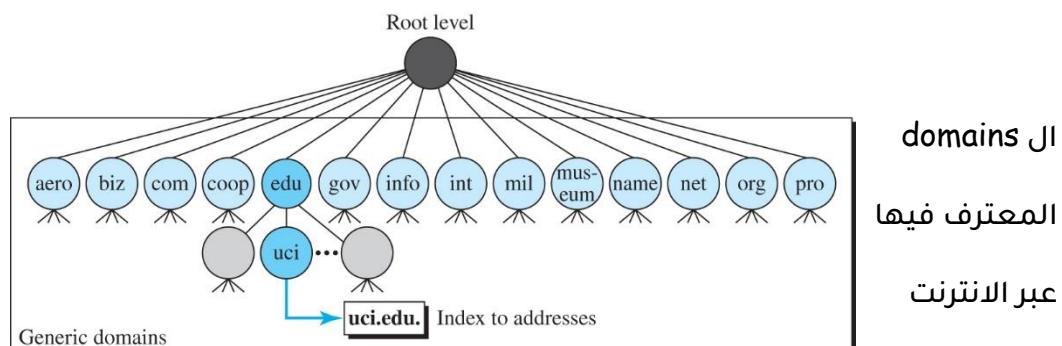
آخر server موجودة هي الـ IP addresses + host تكون مسجلة فيها الـ .name



zone = حالها com الـ .domain = مع كل اشي بتفرع منها Com

DNS in the Internet

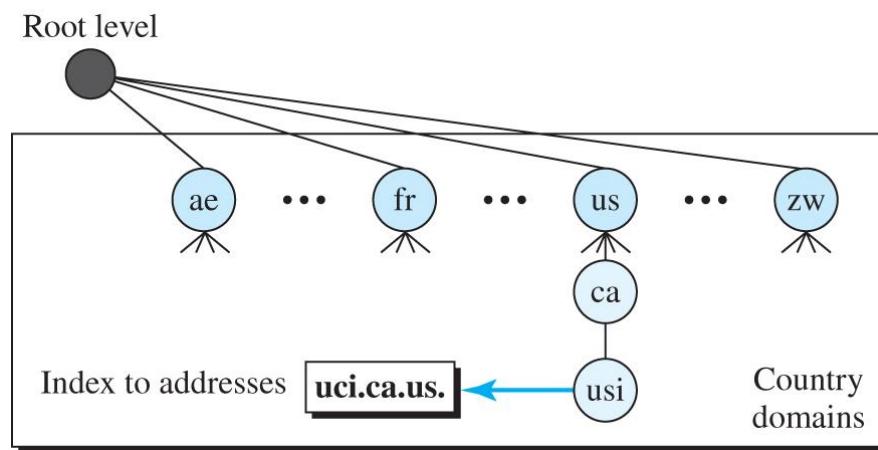
- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) was originally divided into three different sections: generic domains, country domains, and the inverse domains.
- However, due to the rapid growth of the Internet, it became extremely difficult to keep track of the inverse domains, which could be used to find the name of a host when given the IP address.
- The inverse domains are now deprecated.
- We, therefore, concentrate on the first two.



Generic domain labels

<i>Label</i>	<i>Description</i>	<i>Label</i>	<i>Description</i>
aero	Airlines and aerospace	int	International organizations
biz	Businesses or firms	mil	Military groups
com	Commercial organizations	museum	Museum
coop	Cooperative organizations	name	Personal names (individuals)
edu	Educational institutions	net	Network support centers
gov	Government institutions	org	Nonprofit organizations
info	Information service providers	pro	Professional organizations

Country domains

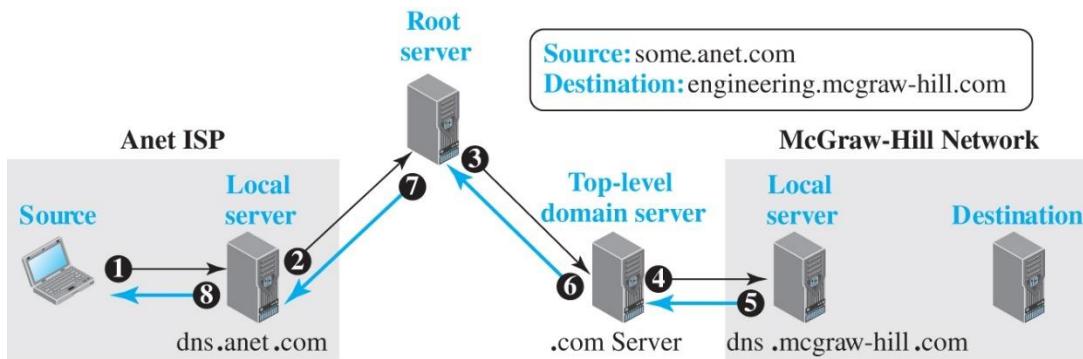


Resolution

- Mapping a name to an address is called **name-address resolution**.
- DNS is designed as a **client-server application**.
- A host that needs to map an address to a name or a name to an address calls a DNS client called a **resolver**.
- The resolver accesses the closest DNS server with a **mapping request**.
- If the server has the information, it **satisfies** the resolver; otherwise, it either **refers** the resolver to other servers or asks other servers to provide the information.

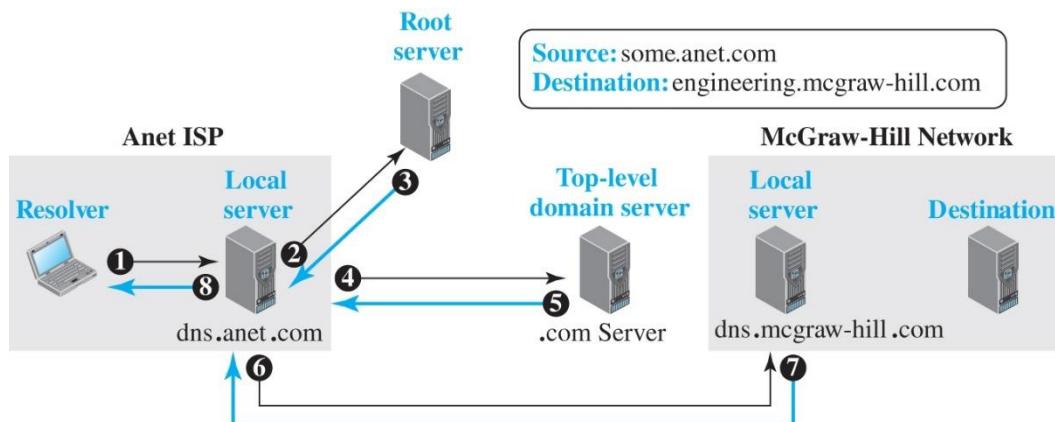


Recursive resolution



- بتتواصل مع local server المسئول عنك وهو بعمل المهمة بالنيابة عنك
وبعطيك الجواب

Iterative resolution



- هون بدل ما root server يعمل المهمة عنك بيعتلك ال IP address تبعن top level domain server . ونفس الاشي ال top level domain server يبعث ال server لـ IP address ...

Resource Records

The zone information associated with a server is implemented as a set of resource records. In other words, a name server stores a database of resource records. A resource record is a 5-tuple structure, as shown below:

(Domain Name, Type, Class, TTL, Value)



بعد فترة **TTL** (Time to live) لا يعيش للأبد في الـ **DNS server** ما معينة الـ **DNS server** لازم يتخلص منه ويضطر انه يسأله السؤال.

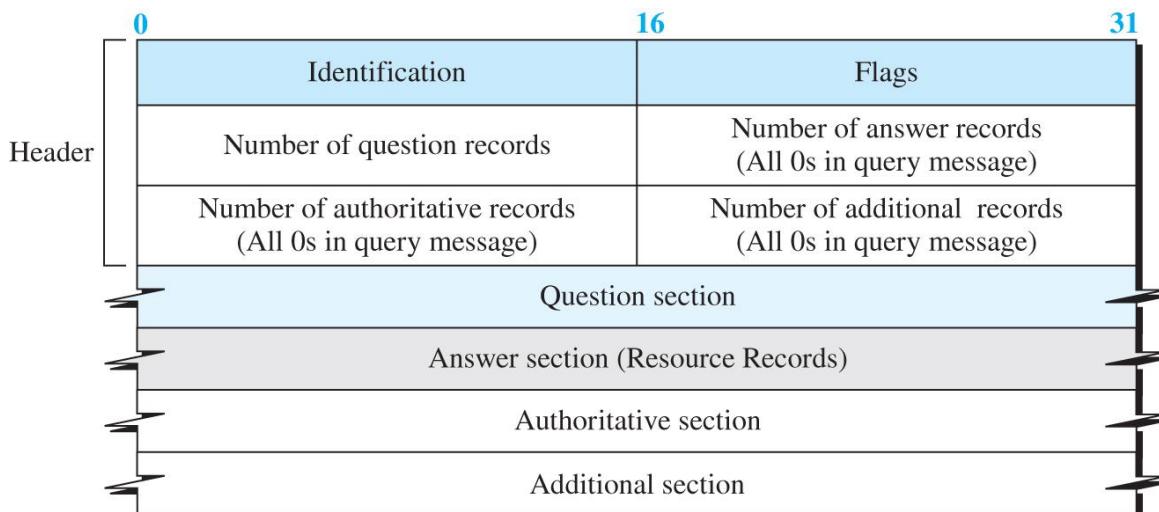
DNS types

Type	Interpretation of value
A	A 32-bit IPv4 address (see Chapter 7)
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address (see Chapter 7)

*أهم اشي الي عليهم أحمر

DNS Messages

To retrieve information about hosts, DNS uses two types of messages: query and response. Both types have the same format as shown in the Figure.



Note:

The query message contains only the question section.
The response message includes the question section, the answer section, and possibly two other sections.

