Network Introduction

ال : Domain عبارة عن اسم او العنوان الخاص بالموقع على الانترنت , شو يعني هذا الحكي ؟

لما انت بدك تدخل على موقع لنتفرض انه Facebook انت بتكتب في ال search bar في المتصفح مثل كلمة فيسبوك وبعدها بتدخل على الموقع فبتلاحظ في ال search bar مكتوب ال Domain لموقع facebook كالتالي وهو ال URL للموقع :

https://web.facebook.com/

خلينا نفصل هذا ال Domain

1- https : عبارة عن البروتوكول المستخدم لنقل البيانات بين الاجهزة خلال شبكة ال web يشكل امن ويستخدم لطلب وعرض صفحات الويب . هذا التعريف يشكل مبدئي لاحقا بتم التطرق لتفاصيل هذا البروتوكول.

مثل ما حكينا المرة الماضية انه البروتوكول عبارة عن مجموعة قوانين مستخدمة حتى توجه عملية التواصل.

2- facebook.com : عبارة عن ال root domain يعني اسم ال domain الرئيسي وبنقسم لجزئين:

.com وهو يعبر عن نوع ال domain او الموقع ويعتبر . Top Level Domain (TLD) في كثير انواع للمواقع مثل :

1 . .com : للمواقع التجارية

2.edu. : للمواقع التعليمية

3.jo. : للمواقع التابعة لدولة الاردن

وفي كثير امتدادات غيرها

3-facebook : هو ال Domain الرئيسي يلي بعر عن الموقع الرئيسي

4-web : هو يعتبر ال domain الفرعي من ال domain الرئيسي يلي هو facebook

ل facebook كشر من ال sub domains مثل :

business.facebook.com

وهذا ال subdomain خاص للوصول ل facebook's business tools يلي بقدوا من خلالها المستخدمين يديروا صفحاتهم ال business

كل sub domain يتم انشائه لتقيم خدمة معينة .

رح يخطر في بالك سؤال , بما انه جميع الاجهزة على شبكة الانترنت الها ip address خاص فيها ليش ما نستخدمه بدل ال domain ؟

الجواب ببساطة انه ال ip address للمواقع من الصعب تذكره خاصة انه يوجد الكثير من المواقع الموجودة على الانترنت

وهذا الجواب رح ينشئ سؤال ثاني انه كيف ال ip address لموقع معين مربوط مع ال domain تبعه ؟

من خلال خدكمة ال . DNS

يعتبر ال DNS كمترجم . كيف يعني ؟

سيرفرات ال DNS موجود فيها قاعدة بيانات مسجل فيها كل ال Domains لكل المواقع ع الانترنت مع ال ip addresses لهاي المواقع

اتخيل هذا الاشي مثل دفتر التلفونات زمان مكتوب فيه اسماء وارقام هواتف الناس يلي بتعرفهم كل اسم جنبه رقم الهاتف تبعه.

نفس الاشي في ال DNS في قاعدة البيانات مخزن كل domain مع ال ip address الخاص فيه جنبه .

كيف الالية يلي بشتغل فيها الdns ؟

لما تكتب في المتصفح مثلا ال domain لل facebook.com المتصفح رح يبعث request ل local DNSانه بده ال ip address لهذا ال domain فبروح local DNS وبتحقق اذا كان ال domainموجود في ال cashe تبعه او لا

اذا موجود برجع العنوان مباشرة للمتصفح وهيك بقدر المتصفح انه يتواصل مع ال server مباشرة

اما اذا ما كان موجود بروح ال local DNS وببعث ال request لل root server lookup وهو عبارة عن DNS server مخزن فيه كل ال domains الموجودة بالعالم ,هذا السيرفر بستجيب في ال ip addressالخاص في ال TLD server المسؤول عن امتداد معين لل domain في هذا المثال هو .com هون ال Local DNS server ببعث ال request لل TLD server وبالتالي بستجيب في ال ip address لل facebook.com server

وبالتالي بصير التواصل مباشر بين المتصفح و ال facebook.com server

---

NAT(Network Address Translation)

اول اشي لازم نكون عارفين انه في جهاز اسمه الموجه (Router) بقوم في توجيه البيانات من شبكه لشبكة ثانية.

ولازم نعرف انه في private ip address و public ip address

ال private ip address : هو ال ip address يلي بستخدمه الجهاز حتي يرسل بيانات لجهاز اخر داخل الشبكة الواحدة(الشبكة الداخلية)

ال public ip address : هو عنوان الراوتر يلي بستخدمه الجهاز في الشبكة الداخلية حتى يرسل بيانات لجهاز اخر في شبكة احرى على الانترنت.

خلينا نشرحه بمثال من الواقع :

اتخيل معي انه بدك ترسل هدية لصديقك يلي عايش في مجمع سكني في المنطقة, هذا المجمع اله رقم فريد بميزه عن المجمعات الثانية. المجمع السكني بتكون من عدة شقق سكنية متوزعة على الطوابق وكل شقة الها رقم فريد خاص بميزها عن باقي الشقق داخل المجمع وفي هذا المجمع يوجد حارس . لما توصل الهدية باب المجمع رح يسأل الشخص يلي بوصل الطلبات (الديليفري) حارس العمارة عن البيت يلي ساكن فيه صديقك حتى يوصله الهدية ولأنه الحارس بعرف كل الاشخاص داخل العمارة رح يعطي الديليفلري عنوان شقة صاحبك.

هون العنوان الخاص هو عنوان الشقق داخل المجمع والعنوان العام هو عنوان المجمع السكني.

يعني لما حد يسألك شو العنوان تبعك بتحكيله عنوان المجمع السكني ما بتحكيله عنوان الشقة فقط.

هذا الاشي بشبه يلي بيصير في عالم الشبكات . بحيث انه لما بدك تبعث بيانات من جهازك لجهاز ثاني رح تنتقل من خلال جهاز الرواتر والي عمله بشبه عمل الحارس في المجمع السكني يلي بعطي الاجهزة في الشبكة العناوين الخاصة فيها وطبعا في طريقتين بوزع فيها الرواتر العناوين بنتطرق الهم لبعدين.

ولما بدك تبعث من شبكة لشبكة ثانية الراوتر بحول ال private IP address تبع جهازك لل public ip address والي نفس عنوان الراوتر يعني الاجهزه يلي في الشبكات الثانية بتعرف جهازك من خلال عنوان الراوتر الي هو ال public IP address.

شو الهدف من ال NAT ؟

لنتنفترض انه رقم شقة صديقك 5 في الطابق الثالث

وكمان في شقة في الطابق الثالث بتحمل نفس رقم شقة صاحبك 5 لكن في العمارة المقابلة للعمارة التي يسكن فيها صديقك.

بنستنتج انه ال NAT بحل مشكلة نقص ال IP Addresses الموجودة في ال IPV4 يلي حكينا عنها المرة الماضية . يعني ممكن انه يتكرر ال ip address في شبكتين لكن لايمكن انه يتكرر داخل الشبكة الواحدة. وكمان بنستنتج انه ال NAT بعطينا نوع من الامان بحيث انه بخفي ال private ip addressللأجهزة على الانترنت.

MAC (media Access Control) Address

زي ما احنا بنعرف انه كل جهاز بده يتصل بالانترنت لازم يكون في اله NIC(Network Interface Card) هذا ال NIC الها عنوان بميزها كقطعة Hardware هذا العنوان ثابت من قبل الشركة المصنعه ال NIC :

مثال :

MAC = 00:1A:2B:3C:4D:5E

ال MAC Address يسمى Physical IP Address يكتب بالنظام السادس عشر, شو النظام السادس عشر ؟ هو نظام بتكون من 16 رقم :A,B,C,D,E,F,0,1,2,3,4,5,6,7,8,9

الجزء يلي باللون الاصفر في المثال هو الجزء او العنوان الخاص بالشركة المصنعة يعني كل الاجهزة او القطع يلي بتصنعها هاي الشركة لازم يكون في ال MAC Address تبعها هذا الجزء من العنوان يعني هذا الجزء بميز الجهاز انه مصنع من الشركة الفلانية.

بسموه OUI(Organizationally Unique Identifier)

الجزء يلي باللون الاحمر هو العنوان الخاص او الي بميز القطعة او الجهاز عن الاجهزة الاخرى المصنعة من نفس الشركة.

DHCP(Dynamic Host Configuration Protocol)

لما حكيت قبل انه في طريقتين بستخدمها ال Router حتى يوزع ال ip Addresses على الاجهزة في الشبكة, ال DHCP هو بروتوكول بستخدمه ال router حتى يوزع العناوين على الاجهزة بشكل automatically وهي واحدة من الطريقتين يلي بوزع فيهم الراوتر العناوين.

خليني اوضحه بمثال : لنفرض انه عامل حفلة وانت منظم هاي الحفلة الي رح تعمله انه تنظم المقاعد للحضور بحيث انه كل ضيف بيوصل الحفلة بتحجزله مكان معين يجلس فيه . نفس العملية الي بقوم فيها منظم الحفلة بقوم فيها DHCP بحيث انه اي جهاز بتصل عللى الشبكة بحجزله ip address ولما هذا الجهاز يقطع التصال ممع الشبكة ويدخل جهاز اخر بقوم ال DHCP باعطائه نفس عنوان الجهاز الغير متصل بالشبكة .

ARP(Address Resolution Protocol)

عبارة عن مجموعة rules بتسمح لل router انه يخزن ال ip addresss للأجهزة المتصلة بالشبكة مع ال Mac address الخاص فيها بذاكرة ال router على شكل جدول .

لما الجهاز المتصل بشبكة ما بده يبعث بيانات لجهاز اخر سواء كان داخل او خارج الشبكة كل جهاز مخزن داخل ال cache الخاص فيه الاجهزة المتصله معه على نفس الشبكة مع ال ip address الخاص بكل جهازالجدول يسمى ال ARP table

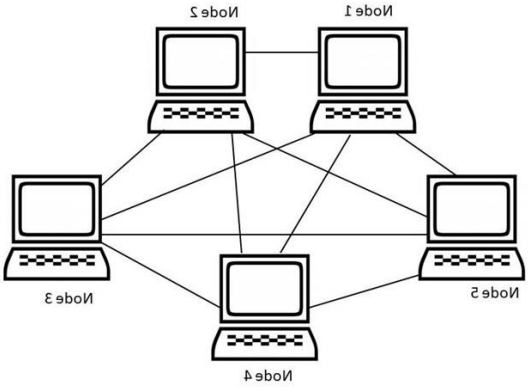
الي بصير انه الجهاز المرسل بطلب ال IP address للجهاز المستقبل من الراوتر ومن خلال ARP protocol بصير عند الجهاز جدول موجود فيه عناوين الاجهزة المتصله معه على نفس الشبكة (ال IP وال MAC addresses واذا كان العنوان المنطقي للجهاز المرسل موجود داخل ال ARP table رح يوخد ال mac addres للجهازويرسل البيانات اله بشكل مباشر.

Network Topology

كيف بكون شكل الشبكة او ال structure تبعها ؟

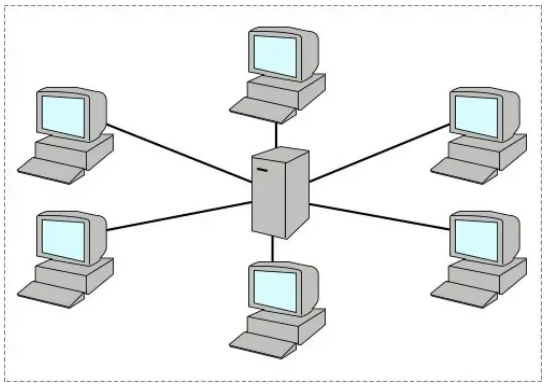
1- Mesh Topology:

هون انه كل الاجهزة بتكون مربوطة مع كل الاجهزة بالشبكة. الحلو في هاي الشبكة انه اذا صار خلل في احد الاجهزة او احد الاسلاك حدث فيه عطل مارح تتأثر الشبكة لانه بكون في link بديل عنه.



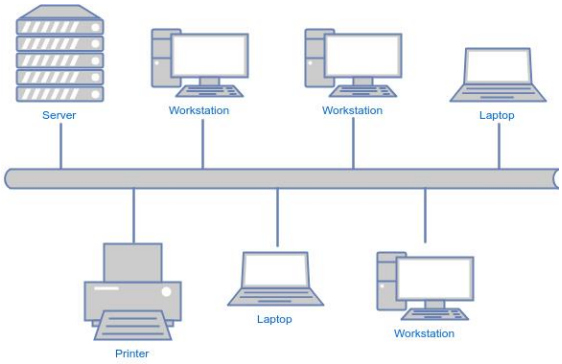
2- Star Topology :

هون انه كل الاجهزة متصلة بجهاز واحد يعتبر المركز. مشكلته اذا صار هذا الجهاز down كل الشبكة بتصير down .



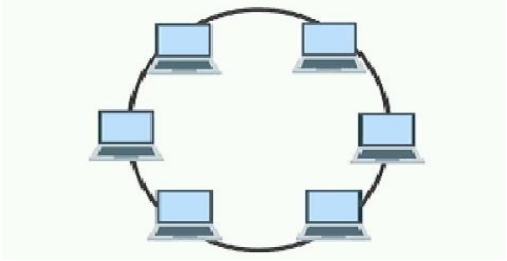
3- BUS Topology:

بكونوا كل الاجهزة مربوطة ب Link واحد فقط , هذه الشبكة فيها كثير عيوب بحيث ان اذا حدث قطع في ال link لاي سبب من الاسباب رح تصير الشبكة down رح ينقطع الاتصال فيها.
والعيب الثاني انه بحدث اثناء نقل البيانات تصادم للبيانات وبالتالي فقدان البيانات. كيف بصير التصادم؟ انه بكون فيه جهازين مثلا بيرسلوا بيانات مع بعض لنفس الجهاز فبالتالي حدوث تصادم



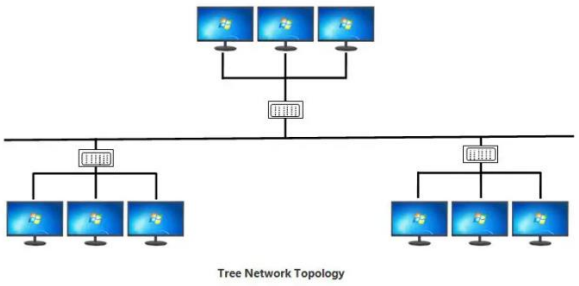
4- Ring Topology :

جميع الاجهزة متصلة ببعضها البعض ب link على شكل حلقة. اذا حدث قطع في ال link بين احد الاجهزة رح يحدث فقدان للإتصال بينهم.



5- Tree Topology :

شبكتين او اكثر من ال Star Topology مربوطة مع بعضها البعض.



OSI module (open System Interconnection)

نتخيل انه بدك ترسل رسالة لصديقك بشكل امن عن طريق الانترنت. حتى توصل الرسالة بأمان وضعوا قوانين تتبع من قبل الاجهزة خلال عملية التواصل للتأكد من الوصول الصحيح والسليم للبيانات خلال شبكة الانترنت.

هاي القوانين بتتجسد في هاي ال module بحيث انها بتتطبق وبتساعد ال data توصبل للوجهة المطلوبة بأمان وبشكل صحيح. وبتساعدنا في فهم كيفية عمل الشبكات وكيفية عملية التواصل بين الاجهزة.

ال OSI module عبارة عن 7 مراحل بتم لنقل ال data من جهاز لاخر:

1- ال Application layer : هي اول مرحلة في عملية التواصل بحيث انها تستخدم في ال Network Applications والي هي مثل : المتصفحات وال GMAIL, OUTLOCK هاي التطبيقات بتستخدم بروتوكولات مثل : HTTP,HTTPS, POP3, FTP, DHCP, SMTP وغيرها الكثير.
FTP: File Transfer Protocol برتوكول مستخدم لنقل الملفات.
SMTP: بروتوكول مستخدم لارسال الايميلات من خلال تطبيقات الايميلات المختلفة.
POP3: مستخدم لاستقبال الايميلات
HTTP: مستخدم لطلب الصفحات من خلال المتصفح.
HTTPS نفس وظيفو يرتوكول ال http لكن يكون الاتصال مشفر.
2- Presentation layer: هاي الطبقة بتتعامل مع كييفية عرض ال data وال formatالها فبتحول الdata لل format يلي بقدر ال جهاز المستقبل انه يفهمها.

المستخدم لما طلب صفحة معينة خلال المتصفح بعث ال Request وفي هاي الطبقة بتم تحويل ال request للغة الالة (النظام الثنائي) واذا كانت ال data كبير حجمها بصير الها ضغط في هاي الطيقة وايضا يتم تشفيرها لارسالها بشكل امن للطرف الاخر.
وعملية فك التشفير تحدث ايضا في هذه الطبقة.
3- Session layer: هس الطبقة المسؤولة عن انشاء الاتصال وادارته وايضا انهاؤه بين الطرفين.
وبتحصل في هذه الطبقة ايضا عمليتي ال authentication وال authorization
1- Authentication هي العملية التي تحدث بعد ارسال طلب الاتصال مع السيرفر بحيث يتم التاكد من هوية المستخدم من خلال الاجابة على السؤوال من انت؟ ويقوم المستخدم بأدخال المعلومات اللازمة للتعرف على هويته مثل بصمة الاصبع اواسم المستخد وال password وبالتالي يمكنه انشاء الاتصال مع السيرفر.
2- Authorization تعني وضع الصلاحيات لكل مستخدم بحيث ان الصلاحيات المعطاه لكل مستخدم على السيرفر للقيام في المهمات المختلفة على السيرفلر تختلف من مستخدم لاخر.

مثلا على جهازك الحاسوب عنددما تدخل عليه تدخل بعد عملية ال authentication ك administrator بحيث انه لديك جميع الصلاحيات للقيام بجميع الانشطة والمهمات على هذا الجهاز. ومع ذلك لو انشأت حساب اخر على نفس الجهاز ولكن كان حساب مستخدم عادي يمكن لهذا المستخدم تسجيل الدخول للجهاز لكنه لديه صلاحيات محدودة للقيام بالمهمات والانشطة على الجهاز.

بعد هاي العمليتين بتم انشاء ال session وجميع الانشطة التي تتم خلاله يتم تعقبها وتسجيلها

4 –Transport layer :

في هذه الطبقة يتم التأكد من ارسال ال data بشكل دقيق للمستقبل وبشكل كلي. يتم هذا المر عن طريق بروتوكولين : TCP,UDP

1- TCP: transmission control protocol هذا البروتوكول يضمن وصول جميع البيانات بشكل كامل ودقيق للمستقبل.

اتخيل انك بتنزل ملف كبير من الانترنت الي بصير انه بتم تقسيم الملف لعدة اقسام كل قسم يسمى segment وكل segment بتم ارفاقها مع رقم تسلسلي ورقم port . شو هو رقم ال port؟ ال port هوالمنفذ يلي بقد من خلاله التواصل مع ال Operating System للجهاز اول ال server

مثال الhttp حتى اقدر اتواصل مع ال http server اله port number من خلاله بقدر اتواصل معه وهكذا. اما الرقم التسلسلي فهو رقم يستخدم للتأكد من وصول ال segment لل distination كيف بتم هذا الحكي ؟ لما المرسل يبعث ال segment لل جهاز المستقبل وتتوصل هاي ال segment لجهاز , المستقبل ببعث ACK انه وصلته ال data لكن اذا ما بعث ack عن segment معينى رح يرجع يبعث نفس ال segment يلي ما وصلت هون بيتأكد انه كل ال data وصلت بشكل امن.

هذا البروتوكول بستخدم تقنية ال oriented connection يلي بصير فيها ال 3-way hand shaking. شو هس ال hand shaking ؟

عبارة عن عملية اتفاق بتصير بين ال client والسيرفر حتى يتم نقل البيانات بنهم بشكل امن :

1- اول اشي ال client برسل SYN packet لل server بكون فيها ال initiate sequence numbers لبدء الاتصال خلينا نفترض انه ال sequence number هو SYN-1 مثلا .

C -> S: SYN (Client sends a SYN packet to the server)

2- ال server برد ب SYN-ACK packet هاي ال packet بكون فيها ال sequence number مختلف خاص بالسيرفر خلنا نعتبره SYN-2 وكمان موجود فيها Ack بتعبر انه السيرفر وصلته ال packet من الclient . طبعا ال Sequence numbers هي

الرقام يلي بتم ايتخدامها بعدين من قبل ال client وال receiver حتي يكملوا ويواصلوا الاتصال بينهم.

S -> C: SYN-ACK (Server responds with a SYN-ACK packet)

3- ال client برسل Ack packet لل سيرفر حتى يأكد انه وصلته ال packet يلي بعثها ال server

C -> S: ACK (Client acknowledges the SYN-ACK packet)

وبعدها بتم ارسال البيانات بين الطرفين.

خلينا نشرح عن الport number :

انت لما بدك تطلب صفحة الويب من ال google.com هذا السيرفر لازم عشان ال users على الانترنت يوصلوا للصفحات الموجودة فيه لازم يكون مشغل خدمة اوApplication ال http او ال https واذا بده يشغله لازم يكون فاتح منفذ لهاي الخدمة وهذا المنفذ اله رقم خاص فيه. الان انت طلبت هاي الصفحة من ال سيرفر الي بصير انه اول اشي الطلب بطلع من جهازك من منفذ برقم عشوائي وفي الطلب بكون رقم منفذ الخدمة المطلوبة وهي ال https مثلا ورقمه 443 فالسيرفر بتأكد من انه المنفذ يلي طالبه فاتح او لا اذا فاتح ممكن يصير التواصل بينك وبين السيرفر تحديدا خدمة ال http من خلال هذا المنفذ او ما يسمى با port number

كل ال responses من السيرفلر رح توصلك من خلال نفس المنفذ يلي طلع منه الطلب يعني لو طلع الطلب من منفذ رقم 4455 رح يرجع الرد الك من السيرفر خلال نفس المنفذ.

الطلب يلي انت طلبته على ال browser كالتالي :

www.google.com:443

يلي باللون الاصفر هو اسم ال domain يلي بتم تحويله ل IP من قبل ال DNS server

ويللي باللون الاحمر هو رقم المنفذ لخدمة ال HTTPS

كل خدمة او بروتوكول اله port number خاص فبه مثل ال http رقمه 80

SSH رقمة 22

وفي كمان ارقام ports بقدر انا احددها اذا بدي افتح port number على جهازي بنسميهم ال custom ports بس ما لازم يكون نفس الرقام المحجوزين لخدمات ثانية.

2- UDP: User Datagram Protocol :

تخيل انك بتلعب online gameعلى الانترنت مع اصحابك مثل ال pupg gameالتواصل بين جهازك وسيرفر اللعبة بكون عن طريق بروتوكول ال udp ويلي بنقل الdata بحيث انه ما بضمن وصول كل ال data. يعني ممكن انه يصير فيه فقدان لبعض ال data خلال اللعب.

في هذا البروتوكول ما بستخدم ال 3-way hand shake يلي بتحدث في ال TCP وانما بتم ارسال البيانات بطريقة not reliable

خلينا نلخص وظائف هاي الطبقة :

1- Segmentation تقسيم ال data ل segments
2- Flow control: يلي بتتأكد من خلالها بنقل البيانات بالسرعة المناسبة.
يعني انه لو السيرفر برسل البيانات بسرعة 30 Mbps وجهازك برسل البيانات بسرعة 10 Mbps فالسيرفر بيصير يبعث في نفس سرعة جهازك.
3- Error control: هون المرسل والمستقبل بقوموا بعملية ال checksum وهاي العملية هي حساب قيمة الchecksum بشبه عملية حساب ال hash value لملف معين هون بحسب ال checksum للsegments اذا كانت القيمة متشابهة في الطرفين ما رح يكون في تغيير او ضياع لل segments المرسلة اما اذا كانت قيمة ال checksum مختلفة عند destination رح يرجع ويبعث ال segment من اول وجديد.

5 – Network Layer:

هاي الطبقة المسؤوله عن توجيه ال packet للوجهة الصحيحة . كمان مسئولة عن تحديد ال path فبتحدد اقصر مسار ممكن تسلكه ال packet للوصول لل destination.
ال packet عبارة عن مسمى لل| dataيلي بتم نقلها خلال هاي الطبقة ويلي ببتكون من ال segments الجاية من الطبقة السابقة مع ال ip address لل source وال destination يعني بتعمل Encapsulation .

طبعا هون بكون شغل الراوتر يلي بوجه packets للمكان الصحيح.

شو الي بصير في الراوتر ؟
اتخيل انه في شبكتين شبكة رقمها 192.168.1.0 وهي نفس الشبكة يلي جهازك من ضمنها وبحمل ال ipرقم 192.168.1.6 والشيكة الثانية بتحمل ال ip 172.16.1.0, وهاي الشبكة من ضمنها server الخاص ب google.com والي بحمل ال ip رقم 172.16.1.3 ويلي انت بدك تعمل اتصال بينك وبينه . فانت بتبعث ال packet للراوتر وبقوم الراوتر بحساب ال subnet mask لل ip address تبع ال google.com .
ال subnet mask هو بحدد من خلاله عنوان الشبكة المراد ارسال ال packet الها فال subnet maskلل google.com هو 255.255.255.0 بحيث يلي باللون الاصفر هو عنوان الشبكة والي باللون الاحمر عنوان الجهاز في ال IP address
يعني 172.16.1.3 يلي باللون الاصفر عنوان الشبكة التي يكون سيرفر ال google.com من ضمنها والي باللون الاحمر عنوان الجهاز داخل الشبكة . فالراوتر بعد ما يشوف ال subnet mask بعرف ال packet لوين متجهة وبقدر يحدد اقصر طريق ممكن تسلكه هاي ال packet

.

6 - Data Link layer : هاي الطبقة مسؤولة عن ارسال ال frame داخل الشبكة الواحدة .

ال Frame هي عبارة عن ال packet مضاف البها MAC Address لل source وال destination وكمان مضاف اليها ال Tail وال header يللي بحددوا نهاية وبداية الframe.

Header	Destination MAC address	Source MAC Address	Packet	Tail

هذا شكل ال frame بس كل هاي المعلومات بتكون مكتوبة في ال frame بالنظام الثنائي.

7 – physical Layer : وهي الطبقة المسؤولة عن نقل ال data خلال الوسط الناقل يعني اما الاسلاك او بالطريقة ال wireless فتقوم بتحويل ال frame ل electric signals لتستطيع الانتقال خلال الوسط الناقل.

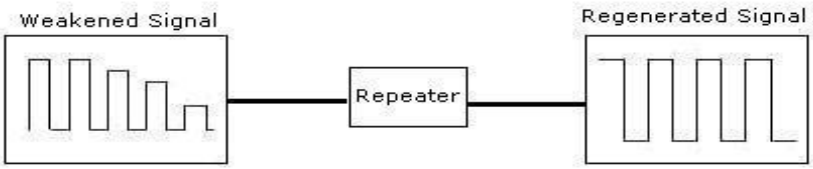
كل هاي العملية بتصير لكن بالعكس عند ال Destination يعني بتوصل ال data لل Physical layer ببتكول من اشارات كهربائية الى 1, 0 وبتصير كل طبقة تعمل decapsulation وتنقل البيانات من طبقة لطبقة بالضبط مثل الي صار عند ال source لكن بالعكس.

Network Devices

هي عبارة عن الاجهزة يلي بتربط الاجهزة فيما بينها على ال network

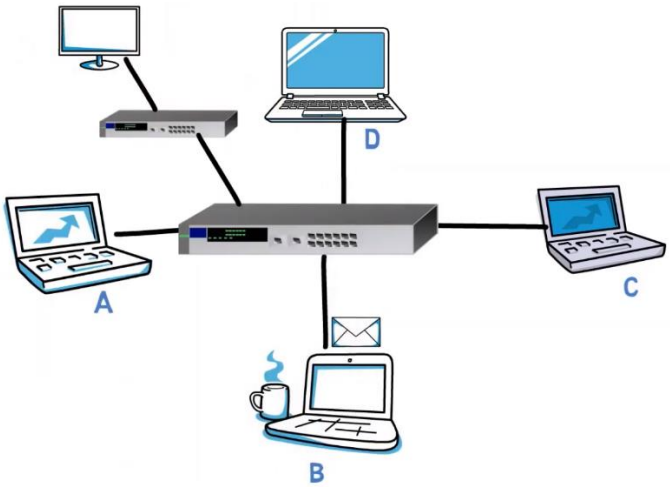
1- Repeater او extended: هو جهاز مستخدم حتى يساعد في نقل الاشارة الى مسافات ابعد.
اقرب مثال هو الراوتر الموجود داخل البيت لما تكون الاشارة في احد الغرف ضعيفة فحتى اقوي الاشارة واخليها توصل لمسافات ابعد بشتري مقوي اشارة لل wifi بسموه Wi-Fi Repeater
بعمل على تقوية الاشارة يعني بتصير تغطي مسافات ابعد.
هاي صورة لل Wi-Fi Repeater.

وهذا مبدأعمل ال repeater:
الاشارة اول ما تطلع من الرواتر بتكون قوية جدا وبعدها بتبدأ انها تضعف لحتى تتلاشى نهائيا مع بعد المسافة عن الراوتر



2- Hub:

هو جهاز يستخدم حتى يربط الاجهزة في الشبكة مع بعضها البعض. بحيث ان هذه الجهزة يتم توصيلها في جهاز ال HUB عن طريق الINTERFACES الموجودة في الجهاز. ال hub بشتغل في طبقة ال physical layer .



شو مبدأ عمله؟

لما جهاز B بده يبعث رسالة لجهاز D الي بصير انه B بوصل الرسالة لل HUB وال HUB ببعثها D لكن في مشكلة بتصير انه جهاز الhub ما ببعث الرسالة فقط لجهاز D فبروح برسل الرسالة لكل الاجهزة المتصلة عليه بما في ذلك جهاز ال HUB الثاني المتصل عليه ما عدا جهاز B يعني بعمل broadcasting او flooding , ولانه الجهاز الثاني HUB في هذا المثال بروح يبعث المسج لكل الاجهزة المتصلة عليه .بعدين الاجهزة بتقارن ال mac address الخاص فبها مع ال mac address الخاص في ال packet اذا ما كانوا متطابقين الجهاز رح يتجاهل ال packet

ليش ال hub بيرسل ال packet لكل الاجهزة؟ لانه ما بيعرف اشي عن ال mac address فبالتالي ببعث broadcast لكل الاجهزة.

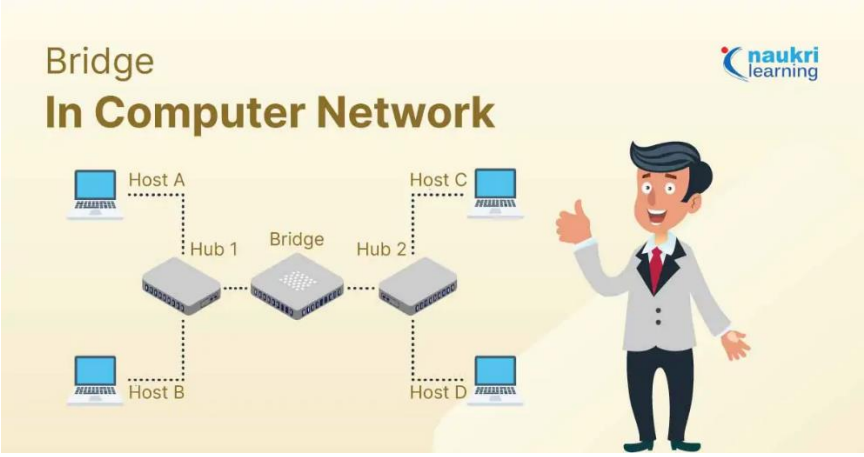
فبصير هون مشكلة: اول مشكلة هي السرية طبعا لانه الرسالة بتنبعث لكل الاجهزة فأكيد ما رح يكون في سرية للبيانات.

ثاني مشكلة انه ممكن يصير تصادم للبيانات بحيث انه يوجد في الجهاز single collision domain يعني انه لما يصير في ارسال لل packet من قبل جهازين في نفس الوقت رح يصير في تصادم لهاي البيانات لانه ال hub بشتغل مثل مبدأ عمل ال bus topology بالرغم من انه شكل ال topology الظاهرة star topology

طيب لو زادت عدد الاجهزة يلي بدي اياها تتصل مع ال hub وما ضل interfaces فاضية تكفي لعدد الاجهزة؟ يلي بصير اني بشبك احد المنافذ في سلك مشبوك في hub اخر وبشبك الاجهزة الاخرى معه. بس هيك لما بدي ابعث من جهاز متصل في hub1 لجهاز متصل في hub2 رح تضل نفس المشكلة ال broadcasting لكل الاجهزة.

فالحل كان ال bridge :

3- Bridge: عبارة عن جهاز يوضع بين جهازين hub كالصورة التالي:

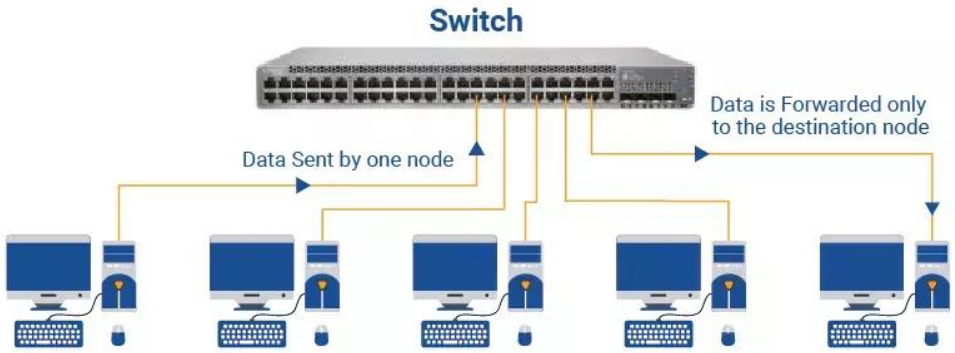


هذا الجهاز شو مبدأ عمله ؟

لما جهاز A بده يبعث لجهاز C ال hub1 رح يبعث الpacket لكل ال ports لما توصل ال packet للbridge بقوم بارسال ال packet الى ال destination اعتمادا على MAC address لل destination

4- Switches: عبارة عن جهاز بربط الاجهزة داخل ال LAN الواحدة.

داخل الشبكة في الشركة مثلا يوجد مجموعة اجهزة متصلة مع بعضها البعض كل قسم في الشركة تتصل الاجهزة الخاصة فيه مع بعضها البعض عن طريق ال Switch.



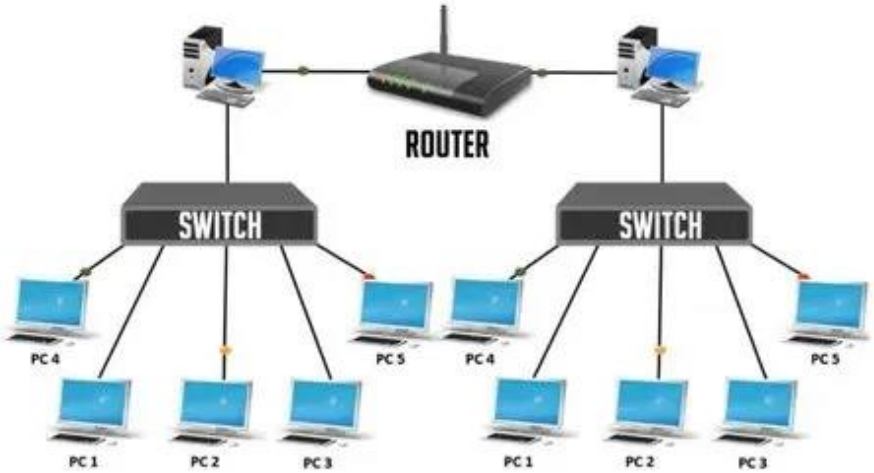
عملية نقل البيانات من جهاز لاخر خلال هذا الجهاز بحيث يكون النقل للجهاز المعني مباشرة.
مبدأ عمل الswitch:

1- اول اشي لما تتوصل الاجهزة مع ال switch بروح ال switch وببعث broadcast لكل الاجهزة المتصلة بحيث انه يسجل عنده في ال MAC table ال mac addresses لكل الاجهزة مع ال interfaces او ال port الشابكين عليه. هاي العمليه تسمى MAC learning.
2- بعد ما سجل كل العناوين للاجهزة المتصلة, لما جهاز بده يبعث data لجهاز اخر بقوم ال Switch بمقارنه ال mac address في ال mac table يلي عنده اذا كان ال destination mac address الموجود في ال data frame مخزن وبشوف على اي port شابك فبالتالي ببعث ال frame لل distination .
3- اذا صار وكان في جهازين بدهم يبعثو data في نفس اللحظة فبكون بين port والثاني bridge يعني رح يمنع عملية التصادم.

5 – router : عبارة عن الجهاز المسئوول عن ربط اكثر من شبكة مع بعض كذلك انه بقوم بتوجيه ال packets بين الشبكات.

هذا الجهاز بتعامل مع ال ip addresses على عكس ال switches بحيث انهم ما بيفهموا ال ip addresses وبنقلوا البيانات عن طريق ال mac addresses .

وما بتقدر انك تطلع ع الانترنت من دون هذا الجهاز لانه هو الجهاز يلي بتعامل مع ال ip addresses



Calculation of IPV4 address

IP addresss بتقسم لجزئين :

1- Network ID.
2- Host ID.

مثال: 192.168.1.100

اللون الاصفر Network ID واللون الاحمر ال Host ID

كيف بتم حساب هذا الIP Address؟

اول اشي لازم نعرف شو هو ال subnet mask :

عبارة عن قيمة 32-bit يتم حسابها لاستخدامها لعملية تحديد ال Network ID وال Host ID

ولازم نعرف شو هو ال broadcast ip : عبارة ip المستخدم لنقل الداتا لجميع الاجهزة في الشبكة وبكون اخر ip في ال subnet

لازم نعرف كمان انه ال IP address بنقسم لعدد من ال classes

1- Class A: هذا ال class بكون اول 8-bit تعبرعن ال network
وال 24-bit يلي بضلوا بعبروا عن ال hosts
وال default subnet mask هون بكون 255.0.0.0 او /8.(prefix size) شو يعني /8؟ انه
اول 8-bit هي بعبر عن عنوان الشبكة
يلي باللون الاحمر بعبر عن الشبكة واللي باللون الاصفر بعبر عن ال host.

2- Class B:
بكون اول 16-bit بتعبر عن الشبكة
ال subnet mask بكون : 255.255.0.0 او /16

3- Class C :
بكون ال subnet mask : 255.255.255.0 أو /24

بنستنتج انه class A بعطي IP Address لعدد كبير من الاجهزة يعني يتم استخدام هذا ال class في المؤسسات الكبيرة الي بتحتوي على عدد كبير من الاجهزة

لنتفترض هذا المثال :

192.168.1.10/22

ومطلوب حساب ال subnet mask ؟
حكينا فوق انه ال prefix size بدل على الشبكة يعني عدد ال 1's في ال subnet mask ويلي ما بقدر اغيره لانه عنوان الشبكة.

حكينا انه ال ip Address عبارة عن 32-bit كل 8-bit بفصل بينهم (.)

ال 22 في المثال بتدل على عدد 1's يلي هم 22 bit بداية ال subnet mask والباقي بكونوا اصار وبدلوا على عناوبت ال hosts

11111111.11111111.11111100.00000000

بعد تحويل ال bits من binary الى النظام العشري:

255.255.252.0

هاي النتيجة تسمى ال subnet mask

طيب كيف حولت للعشري ؟ خليني اشرح كيف حولت يلي باللون الاخضر فوق في 1-Octet:

128	64	32	16	8	4	2	1
1	1	1	1	1	1	0	0

بروح بجمع الاعداد يلي باللون الازرق بس بجمع فقط الاعدلد يلي بقابلهم بالعدد 1

يعني بجمع فقط كالتالي:

$$128 + 64 + 32 + 16 + 8 + 4 = 252$$

كل Octet بحولهم بنفس الطريقة بعطيني ال subnet mask التالي :
255.255.252.0

طيب من هذا ال subnet mask شو بقد اطلع ؟
اول اشي Network IP :
وهو عنوان الراوتر.
كيف بتم حسابه؟ عندي ال ip Address وال subnet mask بعمل AND operation بينهم
والنتيجة بحولها لعشري وهي بتكون ال network ip
Ip address = 192.168.1.10
Subnet mask =255.255.252.0
بعد تحويلهم للنظام الثنائي :

Ip address	11000000	10101000	00000001	00001010
Subnet mask	11111111	11111111	11111100	00000000
AND result	11000000	10101000	00000000	00000000

بعد تحويل نتيجة ال AND operation للعشري :
Network IP = 192.168.0.0

ال broadcast : اخر ip ممكن
Prefix = 22
والي هي محجوزين للشبكة
عدد ال bits لل ip address = 32
بعد طرح 22 من 32 = 10 والي ال bits المحجوزين لل hosts
الان بجيب ال Network address وبحول اخر 10-bits في ال host ip ل 1's

Network Address	11000000	10101000	00000000	00000000
Broadcast	11000000	10101000	00000011	11111111

بعد التحويل للعشري :
Broadcast = 192.168.3.255
ال range لل IP addresses :

$$192.168.0.0 - 192.168.3.255$$

عدد الاجهزة داخل ال Subnet ؟

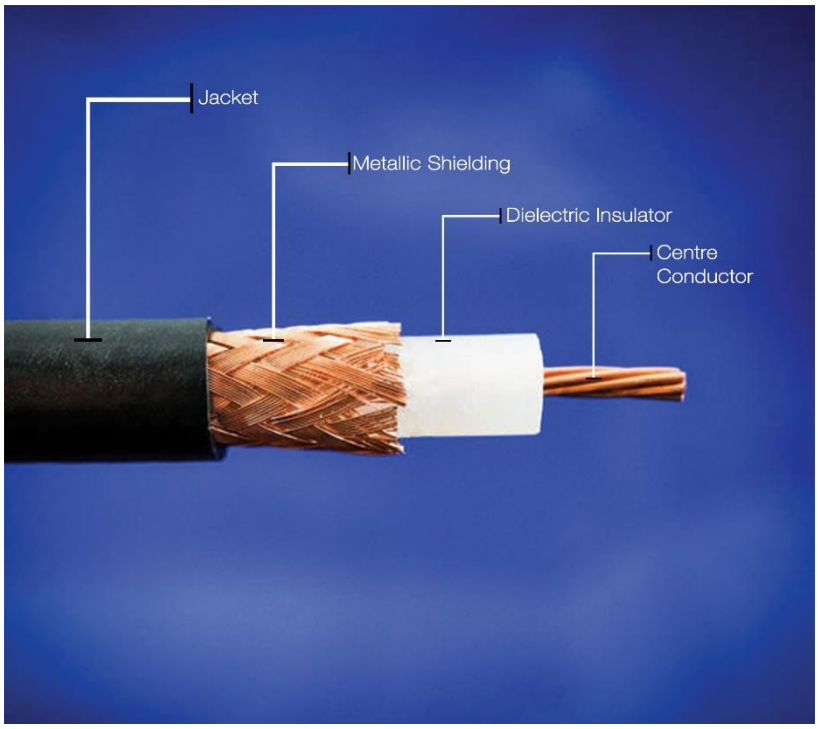
$$2^{10} - 1 = 1023$$

Cables Types

1- Copper cables : هي الكيبلات النحاسية الي بتنقل البيانات عن طريق الكهرباء.

- اول نوع هو coaxial cable:

عبارة عن الاسلاك نفسها يلي كانت تستخدم في شبكات التلفزيون وكانت تستخدم قديما ايضا توصيل كيبل الايثرنت.



هذا الكيبل ينقل البيانات خلال الcenter conductor حيث ان ينقل الاشارات الكهربائية التي يتم تحويلها فيما بعد عند الريسيفر الى اشارات رقمية 0 و1 .

تعتبر الطبقات الخارجية العازلة المحيطة بالسلك النحاسي مهمة لحماية البيانات المنقلة من الضياع والتداخل مع الاشارات الكهرومغناطيسية. طبعا تستخدم عاي الاسلاك لنقل البيانات في مسافات قصيرة.

خلينا نشرح كيف يعني :

اي سلك او موصل مر فيه كهرباء بنشيء مجال كهرومغناطيسي . فهنا في هذا الكيبل الطبقات العازلة المحيطة تمنع تداخل المجالات الكهرومغناطيسية والتأثيرات الخارجية.

- Twisted Pair : هو عبارة عن 8 اسلاك كل سلكين مجدولين مع بعضهم البعض وسبب التوائها لحماية الاشارات المنقلة من التداخل الكهرومغناطيسي والتأثيرات الخارجية.

في منها نوعين : 1- Shielded Twisted Pair (STP) :

هذا النوع يتكون من ازواج من اسلاك النحاسية الملتوية والمحاطة بتغليف يزيد من الحماية من التداخلات والتأثيرات الخارجية والتي تستخدم لنقل البيانات لمسافات طويلة

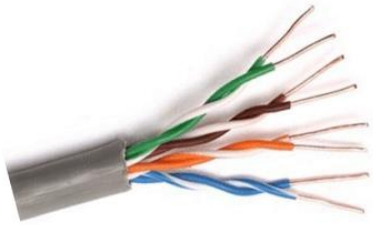
Sheilded Twisted Pair (STP)

2- النوع الثاني (Unshielded Twisted Pair) UTP:

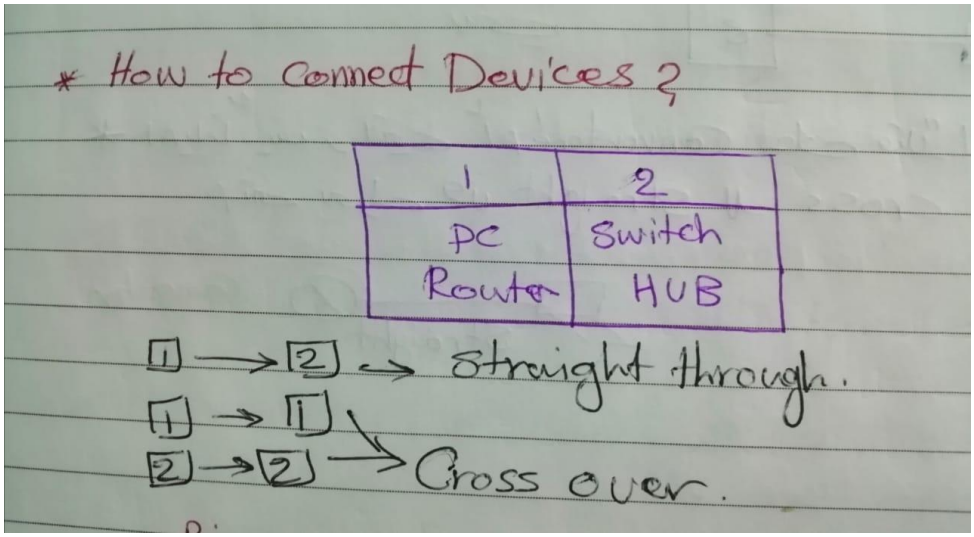
هذا النوع نفس ال STP لكن غير محاط بالطبقة العازلة الخارجية (الالمنيوم)وينقل البيانات لمسافات اقصر من الSTP .هذا النوع اله انواع :

- Cat5: بنقل بسرعة 100mb/s
- Cat5e: بنقل في سرعة 1-Gb/s
- Cat 6: بنقل في سرعة 10 Gb/s

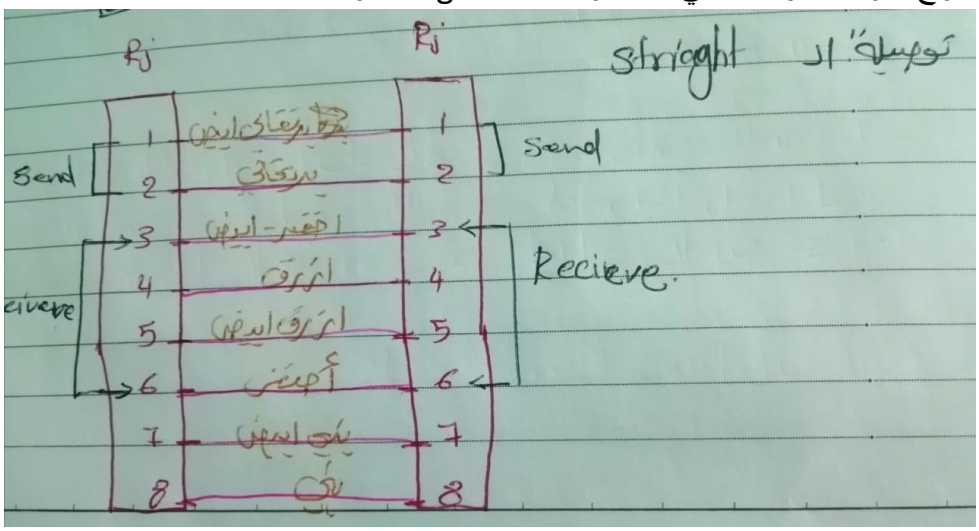
Unshielded Twisted Pair Cable

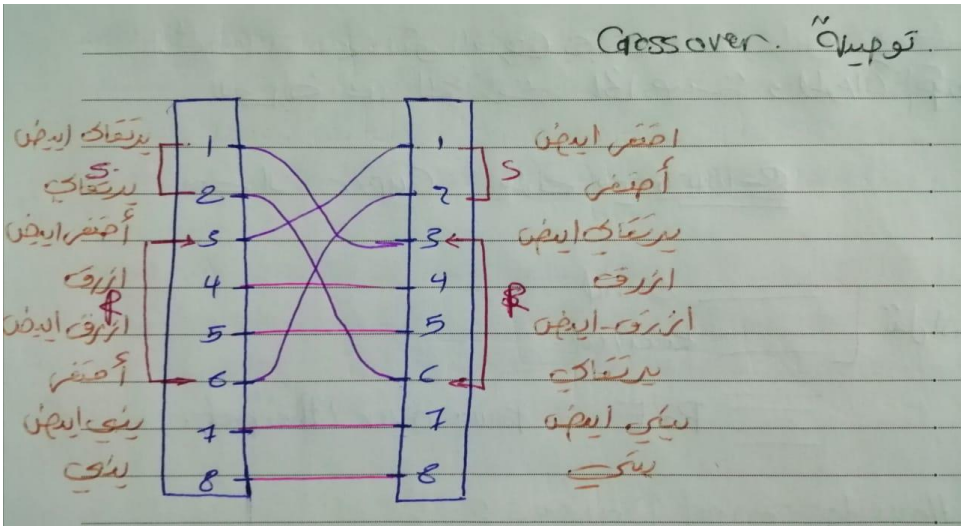


هذه الانواع عند توصيلها في اجهزة الشبكات يتم وضع نهاية السلك الذي يتم توصيله مع اجعزة الشبكات بقطعة تسمى RJ-45



شرح طريقة التوصيل في كل طريقة : ال Straightوال cross over





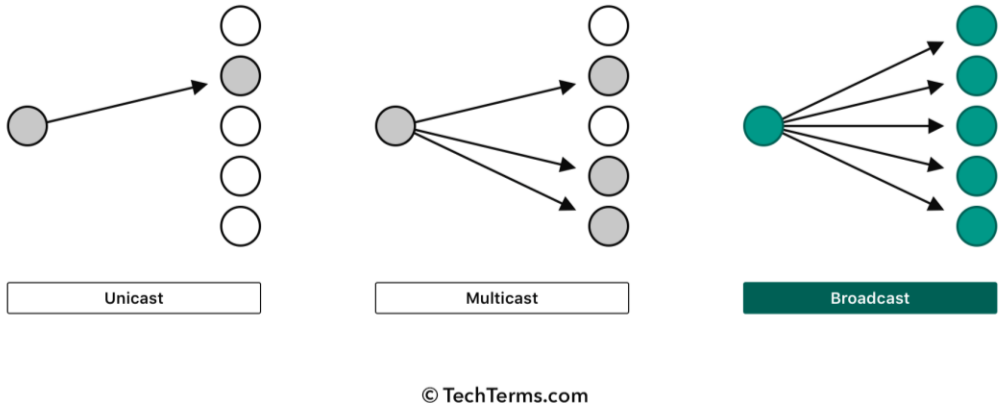
احيانا بقدر اني احط convertor على مثلا الراوتر حتى يحول من Straight لcross over من دون ما انا ارتب الاسلاك حسب الالوان.

Fiber Optic cables -2

هاي ابكوابل بتستخد الضوء لنقل البيانات بسرعات عالية جدا وتتكون من انبوب زجاجي رفيع جدا ينقل من خلاله ال data ليش زجاج بالذات لانه الضوء لما ينتقل خلال الزجاج بكون سريع جدا لانه بصير انعكاسات للضوء.

هذه الخيوط الزجاجية مغطاه بالبلاستيك. لحمايتها من التأثيرات الخارجية مثل التراب.

Multicast& Unicast & Broadcast



- Broadcast: الراوتر بتواصل مع كل الاجهزة المتصلة معه مرة واحدة
- Unicast : الراوتر بتواصل فقط مع جهاز واحد في الشبكة
- Multicast : الراوتر بتواصل مع مجموعة اجهزة محددة متصلة معخ على الشبكة