مقدمة الى عالم الشبكات

كنا قد تحدثنا فيما قبل عن ارتباط الشبكات بالانسان وكيف تتحدث الاجهزة فيما بينها، كيف ترسل وتستقبل بيانات. لو توقفنا وتفكرنا قليلا اثناء ارسال البيانات واستقبالها ما الذي يحافظ على هذه البيانات من الاختراق، او مثلا عند دخولي الى متصفح واجراء بحث عن موقع او خدمة ما، ما الذي يضمن لي خصوصية معلوماتي وحمايتها من خطر الهجمات الالكترونية ؟

ولأن منصات البحث على الانترنت باتت جزءًا لا يتجزأ من يومنا، فتوجب علينا معرفة المتصفحات والشبكات بصورة اشمل واوضح

نبدأها من ما يسمى بشريط البحث (address bar) الموضح في الصورة المرفقة :

ما يظهر لنا في هذا الـ address bar >> URL ويسمى **domain** لنقدم فكرة عامة عن اجزاءه

والذي يبدأ بـ https

لنعلم بالبداية ان https هو بروتوكول، المسؤول عن جلب الموقع الذي تبحث عنه لك، أي يعرض الـ web page

وكل وظيفة تطلبها من الانترنت لها بروتوكول خاص بها، فهناك بروتوكول آخر خاص بتحميل بعض الوسائط من الانترنت وبروتوكول خاص للتعامل مع الايميلات وهكذا.

يلحق بهذا البروتوكول ما يسمى بـ (www) **sub domain**

هذه نطاق فرعي ما يعني ان هذا الجزء من العنوان ليس أساسي (اضافي) في الـDomain، قد حجزه موقع ما، مثل google وتم ربط ال www مع google . وكذلك مثلًا موقع جامعة اليرموك في الاردن قامت بربط موقعها بالـ sub domain (sis) فلو قمت بتغيير هذا الـ sub domain الى آخر لن يتم التعرف على هذا العنوان.

أما ما يعد اساسي في الـ domain فهو جزء الـ google.com والذي يسمى بـ **Root domain**

- Google هي الـ **domain name** (هي الشي الرئيسي الذي ابحث عنه)
- اما (.Com) تسمى بالـ**top-level domain**

هي لواحق تتبع طبيعة الموقع الذي تم البحث عنه فقد ترمز

.com	(comirical)	مواقع تجارية
.org	(organization)	منظمة الصحة العالمية
.gov	(government)	جهة حكومية
.edu	(education)	موقع تعليمي
Etc ...		

*هذا ويعتبر أيضا الـ top-level domain بروتوكول، لانه كتب على صورة واحدة متفق عليها.

اتعلَم ان ما نقوم بكتابته بشكل يومي على الانترنت عندما نبحث عن موقع/خدمة معينة على شكل (site name.com) هو غير موجود بالفعل وغير متعرَّف عليه في الشبكات ! رغم اننا نكتب اسم الـ Domain هذا فقط ومن ثم تظهر لنا نتيجة البحث ! اذًا في عملية بتصير عند ادخال المستخدم لاسم الـ domain

الفكرة انه نحنا بنتعامل في الشبكات على الانترنت او المتصفحات بس مع الـ **IP address**

وحاليا المفروض يتكون عندك سؤال ايش هو الـ IP address ، هو عنوان للشبكة او الجهازعلى الانترنت (عنوان خارجي) مكون من 32 بت - فيك تشبهه بجواز السفر يلي ما بتقدر تتنقل خارجيًا الا من خلاله –

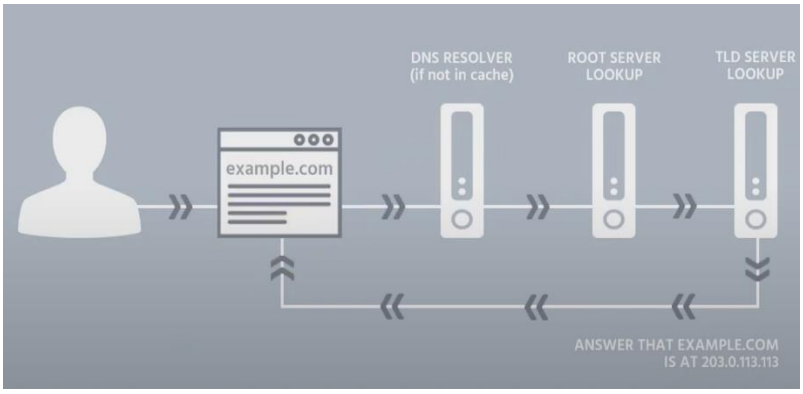
وهكذا هي الشبكات الخارجية (غير المحلية) لا تستطيع التواصل فيما بينها الا عن طريق الاي بي ، ورح نتكلم عنه لاحقًا ان شاء الله

حتتسائل انه هذا الـ IP صعب احفظه وعندي كثير عناوين لا تعد، ما الحل ؟

سؤالك بمكانه واكيد مارح تحفظ عنوانين الشبكات كلها يلي بالعالم

الحقيقة ان ما يحدث عند كتابتك للـ domain name يصل الى DNS ، ما هو الـ DNS؟

DNS اختصار لـ **Domain name system**، هو سيرفر يحوي قاعدة بيانات مخزن فيها الـ IP addresses يلي ع الانترنت كلهم، وكلٌّ بجانب اسم الدومين التابع له.



ثم بدوره (DNS) بعطي الـ IP addresses يلي طلبتها من خلال كتابتك لاسم الدومين للـ web browser ليعرض لك الـweb page

وعلى نفس فكرة تخزين البينات في الـ cache memory & hard desk ففي حالة انه لم يجد اسم الدومين في DNS بروح يبحث عنه في ما يسمى **root server lookup** الذي يعتبر اعلى سيرفر بالعالم حيث يحتوي كل الـ IP addresses & Domains name لهم

واذا ما وجده ممكن يطلب تشيّك على **TLD server lookup** وهكذا ، كما هو موضّح بالصورة >>>

لهيك يا عزيزي المستخدم انت بس عليك تكتب اسم الـDomain واترك الباقي على الـ Dns

طيب نرجع نحكي عن الـ **IP address (internet protocol address)** يلي عرَّفناه فوق بصورة مختصرة ونحكي بالبداية عن **IPv4 (internet protocol version 4)** لانه غالبا ما زالت أجهزتنا كلها شغالة عليه

خلنا نعرف انه هو كـ اسم للجهاز بيتكون من اربع ارقام، وكل رقم مكون من 8 بت يفصل بين كل رقم والاخر dot اي ان الرقم يمتد من 0 الى 255 على هذا الشكل

الشكل العام لل IPv4

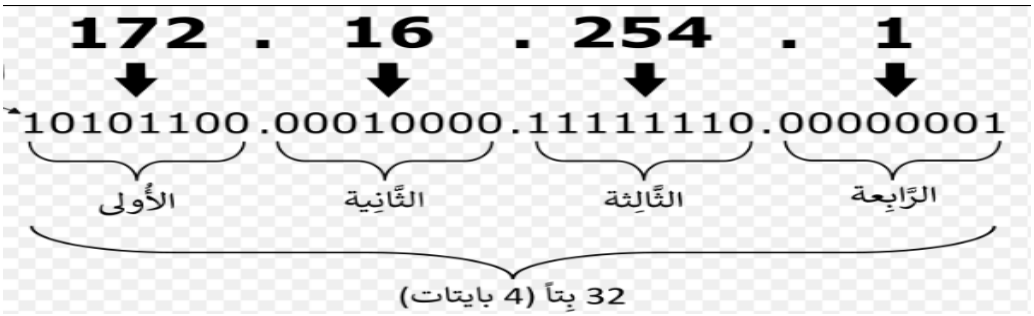
```
____ ____ . ____ ____ . ____ ____ . ____ ____
```

فيكون الرقم بالمجمل 32 بت.

علما ان ترتيب الخانات هذه وتوزيعها بشكل 8 بت ايضًا يعتبر بروتوكول لانه متفق عليها بين كل اجهزة العالم.

مثال على IPv4 :

172.16.254.1 الذي يوزع على هذا الشكل :



حيث تحول الارقام من نظام عشري الى ثنائي في 8 bits على هذا الاساس :

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

طيب لو سألتك كم عدد ال ip addresses في العالم كله

الجواب : 4 مليار addresses تقريبًا (2^32)

استغربت صح ! وانا كمان والله، بس طلعت وراها قصة حلوة خليها لبعدين بحكيلك اياها.

على الرغم من ان اجهزة معينة ومحدودة جدًّا صارت بتدعم IPv6 (بروتوكولات الانترنت النسخة 6) الا انه لسا نحنا بأغلب اجهزتنا ما تطورت ولسا بتشتغل عالفيرجن 4

ايواا !! طيب م عدد سكان العالم 8 مليار ! وتقريبا 6 مليار منهم اونلاين وكثير اشخاص بتشتغل ع جهازين وثلاث وكل هالاجهزة يحملوا ip address !

ما بزبط مستحيل يكون هالرقم كافي

الفكرة وين يا حزركم ! خلني اعطيها بمثال لتوضح مية بالمية

بتتذكروا زمان لما كان يصير عند حد فينا مناسبة سواء زواج او نجاح ونروح نعزم الاهل والجيران على هاي الحفلة ! صح كنا نروح نقدملهم بطاقة دعوة لكل بيت بإسم الاب صاحب البيت ؟ فتكون هاي بطاقة الدعوة بمثابة دعوة لكل فرد من افراد العيلة لحضور هاي المناسبة

يعني انت كنت تروح تحضر الحفلة مش باسمك ! كنت تحضر باسم بطاقة دعوة الاب الذي تنتمي له ولبيته ، وكذلك كل حد ساكن فالبيت، فنحن بهذه العادة كنا عملنا على تقليل عدد بطاقات الدعوة وبالتالي قللنا تكلفة وجهد على صاحب المناسبة ان يقوم بتوزيع بطاقات لكل شخص بيعرفه ويروح باعث دعوات للصغير والكبير كلٌّ باسمه.

ايوا مثلها بالضبط ال ipv4 بيعطيني انا وكل اهلي في البيت IP address واحد، يلي هو IP الراوتر يلي كلنا شابكين منه

وضحت الفكرة صح ؟ عرفتوا ليش الكنافة ما كانت تكفي المعزومين ؟ قصدي عرفتوا كيف 4 مليار IP address كافيين لكل الاجهزة الاونلاين يلي بالعالم؟

لحظة انا عارف انه بخاطرك تسألني هالسؤال، اللي هو صح انا الي IP address خاص فيني على الانترنت مثلًا كان 192.168.1.2 وامي واخي واختي برضو لهم IP address خاص فيهم على الانترنت ؟

رح احكيلك انه لا ! هاد هيك اسم الجهاز في نطاق داخلي ضمن الشبكة الداخلية يلي هو راوتر البيت، بينما انا اسمي على الانترنت هو نفس اسم الراوتر (IP address) ويلي هو بكون public IP فأنا كأحد الاجهزة يلي شابكة على الراوتر بس بدي افتح موقع معين على الانترنت ، بروح الراوتر بجيبلي هاد الموقع باسمه (Router IP address) وبرجعلي اياه لجهازي انا ، وبميزني عن باقي اجهزة البيت من خلال الـ IP address الداخلي (الخاص فيني لحالي).

هالمثال يلي اعطيتكم اياه بوضح فكرة شبكة الـ **NAT (network address translation)** باختصار.

نبيجي الان نحكي عن مفاهيم وبروتوكولات مهم جدًا نعرفها في عالم النيتويرك :

بروتوكول الـ DHCP : (dynamic host configuration protocol)

هذا البروتوكول هو المسؤول عن تعيين الـ (IP address) لكل جهاز يتم توصيله علي الشبكة بشكل تلقائي دون تدخل من المستخدم، يعني مثلا الراوتر ماخد اي بي 192.168.1.1 اجيت انا شبكت كأول جهاز عليه ، بروح هذا البروتوكول تلقائي بيعطيني اي بي خاص فيني لوحدي مثلا كان 192.168.1.2 وبعدها شبك عليه جهاز ثاني رح يروح يعطيه اي بي مختلف عن الاي بي حقي وهكذا .

بروتوكول الـ ARP : (Address resolution protocol)

وهو بروتوكول يستخدم لمعرفة الأجهزة يلي موجودة مع الجهاز على نفس الشبكة ومعرفة العنوان الفيزيائي لهذا الجهاز عبر الـ Mac address المخصص لهم عبر الشبكة، يعمل ضمن الشبكات الداخلية فقط، فعندما يريد أن يتصل جهازٌ بالآخر؛ مثلًا عندنا 4 أجهزة A,B,C,D وفي الجهازين A,B بدهم يحكوا مع بعض ولحتى الجهاز A يقدر يتواصل مع الجهاز B ، يجب عليه معرفة الـ MAC Address للجهاز B

MAC Address : media access control

كل جهاز يحتوي قطعة هاردوير صغيرة (chippset) صنَّعتها شركة معينة واطلقت عليها اسم فريد عن باقي الاجهزة الاخرى الموجودة على الانترنت وهو اسم ثابت لا يمكن تغييره ابدًا، نركز شوي انه MAC Address هو اسم لكرت الانترنت مو للجهاز تمام؟

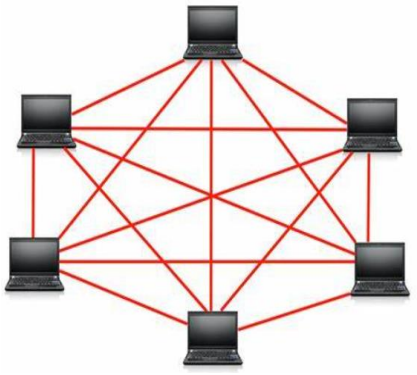
بيبجي على هاي الصورة 4D-55-8A-21-FF-5A تكتب هذه الارقام في النظام السادس عشر الـ Hexa decimal

وكما هو موضَّح في الصورة. >>>

وتتراوح الارقام ما بين 00-00-00-00-00-00 الى FF-FF-FF-FF-FF-FF

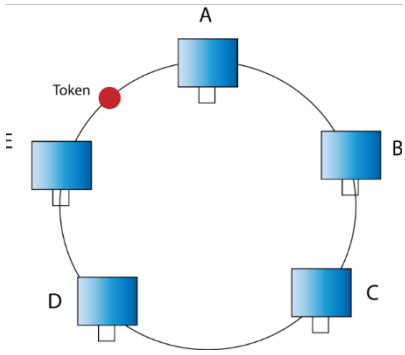
***طبعًا بتغطّي كل اجهزة العالم وبالراحة .**

ولنتعرف الان بصورة عامة على **اشكال النيتويرك ووصف تركيب كل منها (network topology):**



1) mesh topology :

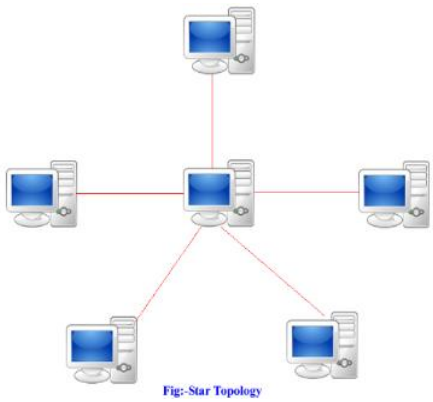
وفيها يكون كل جهاز شابك مع كل الاجهزة يلي موجودة معاه فالشبكة، على هذه الصورة >>>



2) Ring topology :

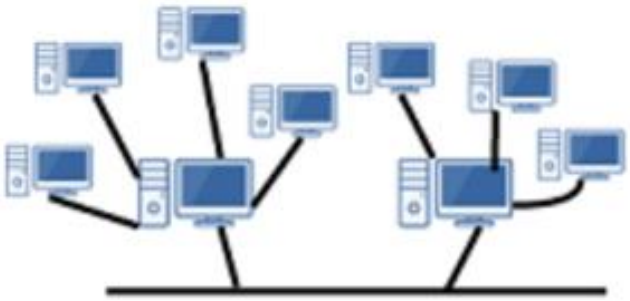
حتى يتواصل اي جهاز مع الاخر بالضرورة

انه تمر الداتا عبر اجهزة اخرى حتى تصل للجهاز المطلوب



3) star topology:

يوجد بينهم جهاز يعمل ك الأم التي تجمع ابنائها حولها وان اراد احد الافراد طلب شي من اخوته الاخرون يجعل الام وسيط بينهم فهكذا تعمل هذه ال topology ، عندما يريد اي جهاز التواصل مع الاخر يرسل الداتا الىcentral device وهو يرسلها فيما بعد الى الجهاز المعنى بالرسالة حسب ال mac address .

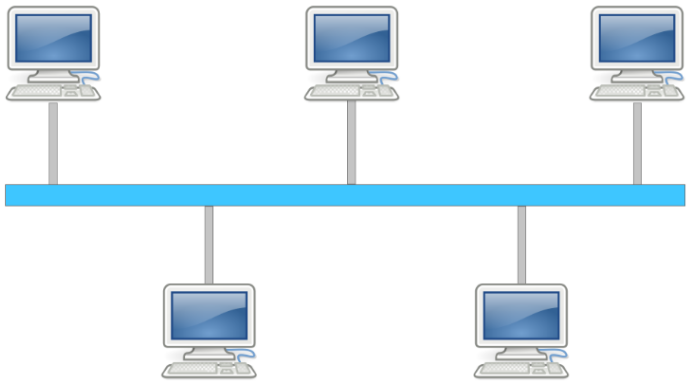


Tree

4) Tree topology :

بكون عندي عائلتين ولحتى يحكوا مع بعض بتتواصل الام من العائلة الاولى مع الام من العائلة الثانية

اي الـ central device من الشبكة الاولى مع central device من الشبكة الثانية



5) Bus topology :

يكون فيها ترتيب الاجهزة على شكل مقاعد الحافلة (الباص) ومنها اخذت التسمية

وكل الاجهزة في هذه الشبكة قادرة تحكي مع بعضها عن طريق line واحد

لكن تكمن المشكلة بأنه اذا قام اكثر من جهاز بارسال معلومات واستقبالها بنفس الوقت رح يصير تخبُّط بالداتا ورح يؤدي لمشاكل

بعد ان درسنا اشكال الشبكات وتكوينها نتطرق الان لمعرفة انواعها

انواع الشبكات :

Pan (personal Area Network) :

هي الشبكة التي يكونها المستخدم بنفسه مثلا عند ربطه جهاز بلوتوث مع الهاتف او اللابتوب ، او ادخاله USB على الجهاز يعمل من خلاله بتبادل بيانات

LAN (local Area Network) :

هي الشبكة التي يكونها المستخدم مع أسرته في المنزل عند شبكهم من نفس جهاز الانترنت سواء اكان ويرلس او ايثرنت

WLAN (wireless local Area Network) :

هي ذاتها الشبكة المحلية التي تتكون في المنزل الواحد لكنها مقتصرة فقط على الربط اللاسلكي

MAN (Metrobolitan Area Network) :

هي شبكة المحافظات والمدن ويتم انتقال البيانات من خلال ابراج الاتصالات المنتشرة في كافة المناطق
حيث اتصلت مدينة اربد بمدينة عمان بغيرها من المدن عن طريق
شركات اتصالات مثل اورنج ، زين وأمنية.

WAN (Wide Area Network) :

هذي الشبكة العالمية التي ربطت العالم ببعضه
كان ذلك عن طريق ان كل دولة تملك محطة
تجمع كل سكانها الموجودة بشبكات الman
وتوصلها ايضًا مع شبكات الMAN الموجودة في
الدول الاخرى
تنتقل البيانات ويتم هذا الاتصال عن طريق
كيبلات ممتدة في قاع المحيطات
يوجد في الاردن محطة هاشم التي تعنى فالقيام
بهذه العملية

تتذكروا معي لما حكينا من قبل هالمرة عن جهاز الـ Modem الموجود في الحاسوب ! والذي يقوم بتحويل البيانات من اشارات رقمية (digital signal) الى اشارات تماثلية (analog signal)، وأطلقوا على هذي العملية اسم modulation

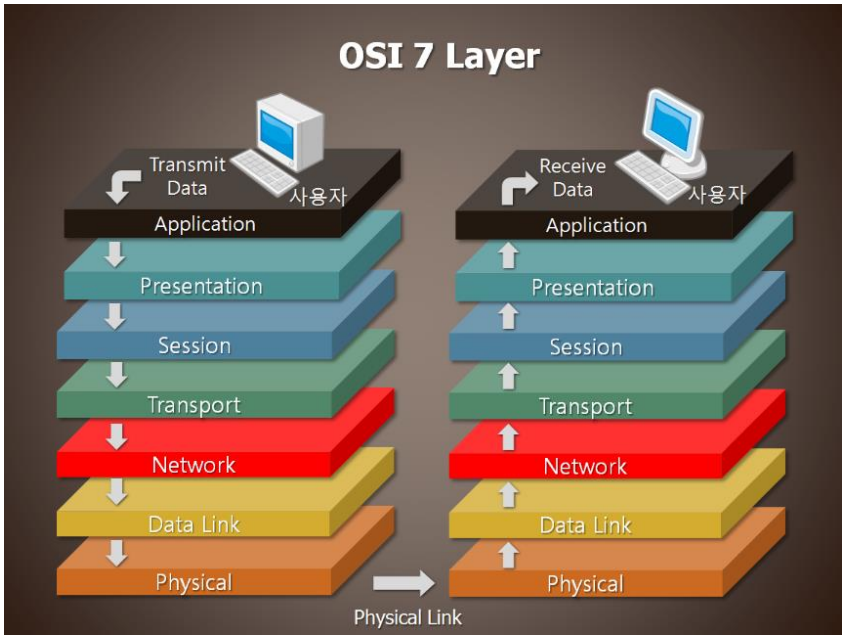
وحكينا بعدها انه تنتقل الداتا عبر كيبلات مخصصة قد تكون سلكية باختلاف انواعها؛ او قد تنتقل بشكل لاسلكي

ولما توصل الجهاز المستقبل تعاد العملية لكن بشكل عكسي حيث تصل بشكل analog signal وتحوَّل الى digital signal ليستطيع الحاسوب فهمها وتسمى هذه العملية demodulation

اجى الوقت لنعرف بالتفصيل كيف بتصير هاي العمليات يلي تندرج تحت 7 layers of OSI model

7 مراحل تمر فيها الداتا بدءًا من كتابتها وارسالها من قبل الـ sender (من المرحلة 7 الى المرحلة 1) بشكل تنازلي، وتعاد هذه الـ 7 مراحل عند الـ Reciever لكن بشكل معكوس (من المرحلة 1 الى المرحلة 7) بشكل تصاعدي.

بسم الله نبدأ نعرف ايش هم الطبقات كـ مُسميات وترتيب ثم نشرح كل منهم بشكل تفصيلي :



بطبيعة الانسان لما بده يتواصل مع انسان اخر ويتناقش معاه بحط معايير ومبادئ لتواصلهم سوا فلو اجى حدا ثالث يدخل يتواصل معهم رح يرجعوا يخبروه بالمعايير اللي اتفقوا عليها يلي على اساسها بتواصلوا لكن لو اجى 100 حد ليتواصوا معهم مش اشي منطقي نقعد نحكيلهم واحد واحد عن هاي الشروط والمعايير يلي وضعوها للتواصل، فبروح هاد الشخص بكتب لوحة عليها شروط وقوانين للتواصل معاه وبعلّقها على باب بيته فلو اجى اي حد ليتواصل معاه رح يقرأ هدول الشروط وعلى اساسهم بيتواصل مع الشخص

نفس الاشي بصير باجهزه الحاسوب، الاجهزه بتكون واضعة معايير وقوانين ستاندرد لتواصلهم سوا اللي هي بتندرج تحت مسمى 7 layers of OSI Model

نيجي لاول طبقة **Application layer** يعني اول خطوة اليوزر بعملها ع الجهاز حتى يبعث او يرسل داتا عن طريق الانترنت هي انه يفتح الـ Browser ويبدأ يبحث عن الموقع الذي يريده ، وحكينا قبل هالمرة انه اي شي انت بتطلبه من المتصفح اله بروتوكول مسؤول انه يعرضلك اياه .

من الامثلة عليهم :

بروتوكول https الخاص بالتصفح واللي يمتاز بخاصية الـ Asymmtric encreption على عكس بروتوكول http .

بروتوكول FTP هذا وظيفته ينزّل اي شيء من الانترنت (for downloading)

بروتوكول SMTP لارسال الايميلات سواء كان عن طريق الـ (gmail,outlook)

بروتوكول POP3 يلي وظيفته يستقبل الايميلات المرسلة بواسطة بروتوكول SMTP

أيضًا تعنى بكافة التطبيقات والبرامج التي تحتاج انترنت لعملها

هذي البروتوكولات تُستخدم في application layer في Network application

ثاني طبقه عندنا يلي هي **Presentation layer** في هذه اللاير بتم تحويل لغة الداتا يلي انا كـ يوزر كتبتها وبدي ابعثها لجهاز اخر من ASCII الى Binary ، و فرضًا كانت الداتا كبيرة بالتالي رح يكون في صعوبة (بُطئ) بارسالها واستقبالها عبر الشبكه فبروح بعمل ضغط (composed) هيك بقل حجم الداتا وبصير سهل على الشبكة تنقلها وبشكل سريع أيضًا ثم بعد هيك بعمل للداتا (encreption) وهيك انا حفظت الداتا من الاختراق

طبعًا فيما بعد لما توصل الداتا للجهاز المستقبل رح يتم عمل فك تشفير الها (decreption) من خلال البروتوكول SSL (secure socket layer)

اذًا بهاي الطبقة صارعندي شغل على الداتا من تحويل لغتها ثم ضغطها لتقليل حجمها ومن ثم تشفيرها لحمايتها

ثالث طبقة عندنا هي **Session layer** هنا تمر الداتا بمرحلة جديدة يكمن دورها في انها تُبقي المستخدم متصل مع الشبكة لحظة بلحظة حيث تطلب مثلًا فتح موقع ما فيأتيك الرد من السيرفر بنفس اللحظة لادخال ايميلك والباسوورد وعندما تقوم بادخالهم يأتيك الرد بأن ادخالك صحيح او لا، هذا ما يسمى بـ Authuntication

ثم لو اردت تعديل او كتابة شي على الموقع فيعطيني موافقة على هذا اولا، هذا ما يسمى بالصلاحيات المحددة لي كمستخدم، يعطيني اياها السيرفر بما يسمى Authorization

وهكذا يتم ابقائي اون لاين مع السيرفر، حيث نكون متصلين لحظة بلحظة دون انقطاع.

ومن الأمثلة عليها ترقُّب اكتمال تنزيل ملف او برنامج ما، الذي يسمى بـ (tracking downloading files)

نيجي للطبقة الرابعة يلي هي **Transport layer** في هذه الطبقة تمر الداتا في ثلاثة مراحل:

1- Segmentation
2- Flow control
3- Error control

اول مرحلة segmentation يحدث فيها تقسيم للداتا الى اجزاء، كل جزء او قسم اسمه data unit كل data unit تحتوي port , sequence هاد البورت هو المنفذ الضروري تواجده في كل ابليكيشن او جهاز لتبادل الداتا من خلاله ورح ندرسه لقدام بالتفصيل ان شاء الله اما الـ sequence فهي توضح ترتيب هذه القطع من الداتا المقسمّة، حتى ما يصير في لخبطة الداتا عند اعادة دمج القطع لاحقًا.

المرحله الثانية في Transport layer هي الـ flow control

وهي المسؤولة عن ادارة نقل البيانات والتحكم بتدفقها، مثلا انا بروح طالب من السيرفر انه يرسللي بيانات ايًا كان نوعها وراح باعتللي اياها بحجم وسرعة كبيرة لانه طبيعي سرعة نقل البيانات في السيرفرات اكبر بكثير من سرعة نقل البيانات في الكمبيوتر فجهازي هون بكون غير قادر على استيعاب السرعة او حجم البيانات اللي بيرسلها السيرفر بقوم انا ببعتله طلب انه يخفِّض حجم الداتا اللي بيبعتللي اياها ليقدر جهازي يستوعبها، فالسيرفر بيقلل هاي الكمية او بيقلل السرعة اللي بيبعتللي فيها الداتا، هذا الشيء والاتفاق يلي صار بيناتنا انا والسيرفر يحدث في مرحلة الـ flow control في الـ Transport layer

نحكي عن اخر مرحله في Transport layer اسمها error control في هذه المرحله يتم تصحيح اخطاء نقل الداتا، استكمالًا للمرحلة السابقة انا بكون بستنى توصلني الداتا يلي طلبتها ، فمثلًا وصلتني داتا انا ظنيت انها مش صحيحة فبروح عاملة hash sum للداتا وبشوف اذا متطابقة مع الهاش المعطى او لا هاد الاشي يلي انا عملته اسمه check sum، بعد هيك لو توصلت للداتا انها خطأ او منقوصة مثلا فبروح ببعث طلب اعادة تدقيق ع الداتا وبعدها بتم التأكد من صحة الداتا والتدقيق عليها وبتوصلني بشكل صحيح، ولو كانت لسا منقوصة وفيها اخطاء برجع ببعث طلب بإعادة تدقيقها هذه العملية تسمى بـ (Automatic repeat request)

طبعا البروتوكولات المسؤولة عن الثلاثة مراحل هدول هن :

بروتوكول TCP (Transmition control protocol) هذا البروتوكول يمتاز بنقل الداتا بدقة والمحافظة عليها تماما لكن المشكلة انه بطيء جدا

بروتوكول UDP (User datagram protocol) هذا يعطي الداتا بشكل عشوائي، غير دقيق في نقلها لكن ميزته انه سريع جدا

ثم الطبقة الخامسة وهي **Network layer** فيها تمر الداتا أيضًا في ثلاثة مراحل:

1- logical address
2- Routing
3- path determine

في هذه الطبقة تصل الداتا التي قُسّمت في مرحلة الـ segmentation على شكل data unit ثم يتم اضافة عنوان المرسل والمستقبل (sender & receiver IP) على كل segment وتسمى بـ packet هذا ما يحدث في المرحلة الاولى من هذه الطبقة التي تسمى logical address

ثاني مرحله في الـ network layer هي Routing وفيها يتم تحديد المسار المستخدم في نقل البيانات عن طريق public IP وعند وصولها الى الشبكة المحددة يقوم الراوتر بدوره بإيصال هذه البيانات (as a packets) الى الجهاز المحدد حسب الـ local IP ، وحتى يتم تمييز الشبكات عن بعضها وضمان عدم حصول اخطاء، يقوم سيرفر الموقع بإضافة ما يسمى بـ net mask والذي يحتوي على standard address ويحدد فيه ما يراد تثبيته من bits في IP address وما يمكن تغييره في هذا الـ IP (IP الشبكة يلي بعثت request) سيتم

ثم في مرحلة الـ path determine تقوم هذه الطبقة (network layer) باختيار اقصر مسار تسلكه البيانات (as a packets) بين المرسل والمستقبل لتناقلها بسرعة وسهولة اكبر.

الطبقة السادسة **Data link layer**

هاي الطبقة باختصار ما بيعجبها وضع الداتا بهالشكل (packets) لازم يضيفلها معلومات تفصيلية اكثر ،

فببدأ بإضافة Mac address for sender & receiver ثم بضيف tail على الـ packets، وظيفة هذا الـ tail اكتشاف الاخطاء فقط (error detection).

Mac address : عنوان داخلي في شبكة محلية

فتصبح على هذا الشكل فيما بعد

طبعًا للتوضيح الفريم بتكون على شكل (0,1) set of bits

واللي بصير بعد هيك انه بتتحول الداتا (frame) من اشارات رقمية 0,1 الى اشارات تماثلية تكون على شكل sinusoidal تسمى اشارات الكهربائية ثم تنتقل في الوسط الى الجهاز المستقبل

وهاد الشي بصير في طبقة 1 ويلي تندرج تحت اسم physical layer

حيث تمثل ارسال البيانات سواء بشكل سلكي عن طريق الكيبلات باختلاف انواعها – سندرسها لاحقًا - او لاسلكي (wirless) عن طريق الـ wi-fi

وهذي الطبقات بمراحلها تعاد كلها بشكل معكوس عند الجهاز المستقبل لتتم عملية ارسال البيانات واستقبالها بشكل صحيح وتحت بروتوكولات ثابتة.

وهيك بنكون خلصنا شرح الـ 7 layers of OSI Model

ننتقل بعده الى موضوع الـ **Ports**

قصة الـ ports وما فيها تخيلوا معي اثنين اصحاب انقطعوا عن بعض فترة طويلة من وقت المدرسة وما كان بوقتها سوشال ميديا وبعد سنين وسنين اجت السوشال ميديا وولعت العالم تواصل بين بعض

وبيوم من الايام، تذكّر حدا فيهم الثاني وانشغل تفكيره فيه بده يتواصل معاه ويعرف شو اخباره وكيف احواله

صار يبحث ويبحث عنه وما لقاه

فكّر انه المشكلة من عنده مش قادر يوصلله راح يبحث عن ناس ثانيين كلهم لقاهم وتواصل معهم

هون اكتشف انه سبب عدم قدرته ليتواصل مع صاحبه الثاني انه صاحبه ما بملك حساب ع السوشال ميديا

ف بهاي القصة البيض يلي حكيتها يعتبر الاكاونت ع السوشال ميديا هو باب تواصلهم

ف انت ما بتقدر تتواصل مع حد وتعرف اخباره الا ليكون عنده اكاونت على السوشال ميديا

تمامًا تمامًا نفس الفكرة تنطبق على الاجهزة، بأنه من الضروري تواجد منفذ (باب تواصل) بينهم ليتم تبادل الداتا ومعرفتها من خلاله

بهمنا نعرف قبل ما ابدأ شرح تفصيلي انه كل بروتوكول هو عبارة عن application or servies لـه port محدد ،

شوي احكيلكم افكار مبعثرة وبعدها نرجع نلمها بعقلنا

عرفنا انه كل بورت هو تابع لبروتوكول واحد فقط

طيب شو يعني بورت ؟ البورت هو ممر يسمح بنقل نوع معين من الداتا خلالها من الجهاز الى الشبكة والعكس

يمكن فقط لبروتوكول TCP وبروتوكول UDP الاشارة الى المنفذ اللي يجب أن تنتقل اليه الداتا (هم اصحاب القرار(:)

كل بورت يؤدي وظيفة معينة وخاص بشيء معين

عدد البورتات 65535 بورت

كل بورت يسمح بمرور نوع معين من الداتا

ما بصير كل البروتوكولات يكونلهم نفس البورت لانه رح يصير فيه تضارب في الداتا

طيب فرضًا انا رحت طلبت من جوجل موقع معين، بتتذكروا فكرة الـ DNS لما كنت ابعث اسم الدوماين لل DNS وتروح هي تجيبلي ip address الموقع وبعدها بيفتح عندي وبيظهرلي URL ومن خلاله بنقدر نتواصل سوا بالبيانات

ايضا الـ segment يلي تم تقسيمها في Transport layer كانت تحتوي على منفذين؛ منفذ الجهاز المصدر ومنفذ الجهاز المستقبل (source port & destination port)

يحتوي ip address الموقع يلي بده منه خدمة يتبعها [:] ثم اسم البورت يلي بدها تدخل منه هاي الريكويست ويسمى بـ (destination port)

يكون على هذه الصيغة مثلًا 192.164.2.8:443

اذًا يتم اختيار البورت حسب البروتوكول اللي مسؤول عن الخدمة اللي انا طلبتها من الموقع

هاد المقصود بأنه كل بروتوكول له بورت خاص فيه مثلا :

Http بياخذ بورت 80

و https يعمل على بورت 443

SMTP يعمل على بورت 25

FTP يعمل على بورت 21 وهكذا.

فهذه الارقام ثابته ومحجوزة لهم لا تتغير ابدا.

طيب و الـ destination port !

هذا يتم اختياره بشكل عشوائي من 0 - 65535 باستثناء رقم البورت المستخدم عند السيرفر .

عندما تصل ريكويست الداتا الى السيرفر يتم تجهيز الخدمة لهذا للجهاز المرسل لكن كيف يتم ارسالها الى نفس الجهاز بدون ضياع ؟

بنفس عملية الارسال لكن بشكل معكوس يتم ارجاع الداتا حيث يحدد عنوان الجهاز المستقبل وبجانبه يوضع نفس الـ source port الذي تم اختياره عشوائيًا في العملية الاولى

طيب وأكيد عارفين مين اللي بتحكم بوصول الداتا بأمان وسلامة !

بروتوكول TCP وبروتوكول UDP

TCP هاد بمثِّل الانسان المحترم ابن الاصول لما يتصل على حدا بسأل عنه وعن أحواله ثم ببدا يطلب يلي بده اياه، هاد البروتوكول نفس الشي قبل ارسال واستقبال البيانات بعمل طلب اتصال مع السيرفر(request connection) بيتفقوا من خلاله ان تكون حجم الداتا كذا وسرعة انتقالها كذا من كذا بما يناسب قدرة الجهاز الاستيعابية، ايضًا خلال عملية نقل الداتا يبقى يتفقدها حتى تصل الداتا بكل سلامة وامان بدون اي نقصان او اخطاء

لكن سلبية هذا البروتوكول انه بطيء وعملية الاتصال يلي بيعملها بتاخد وقت وهالشي يؤدي الى تأخر وصول البيانات للجهاز

بينما بروتوكول UDP لا يوجد اي اتصال بين هذا البروتوكول والشبكة ولا يتم الاتفاق على شي لاتمام وصول البيانات بسلامة فقط ما يفعله وما يريده هو ارسال واستقبال بيانات

ولو تم فقدان بعضها لا يهتم بأمرها بقدر اهتمامه على ان يستجيب بسرعة عالية للـ client (مقدم الطلب).

بعد ما حكينا عن البروتوكولات والبورتس تعالوا نتعرف سوا على مجموعة devices تساعد على اتصال اجهزة الحاسوب بالشبكات الاخرى المحلية او غير المحلية >>>

1) **Repeater** : هاد يجماعة بحل اغلب مشاكل الراوتر في بيوتنا ، مشكلة أنه الراوتر بنشر موجات انترنت قوية فقط في مدى قريب منه وكلما بعُد الجهاز عن الراوتر ضعفت موجات الانترنت (electrical signal)

طيب كيف بحل هاي المشكلة ؟ عن طريق اعادة توليد هذه الموجات الكهربائية وتكرارها من مكان ما يتم وضعه فيه وهكذا يكون قد عمل على تقوية الاشارة.

من الامثلة عليه بواقعنا لما بدك تشتري جهاز راوتر بتقدملك الشركة عرض مع الراوتر على جهاز extend لشبكة الراوتر وهذا هو الـ Repeater بحد ذاته ، طبعًا له اشكال وصور منوعة حسب الشركة المصنعة او حسب استخداماته ومزاياه، وهذه احدى اشكاله الشهيرة :

2) **HUB** : هاد الجهاز اتت فكرته من ضرورة ايجاد حل لربط الاجهزة كلها سويًا عبر كيبلات حتى تتم عملية تواصلهم، فقاموا بصناعة جهاز يمتلك مداخل يعمل ك حلقة وصل بين هذه الاجهزة لتصبح الشبكة star topology وبالتالي قللوا تكلفة وجهد، وهذه الصورة المدرجة توضح احد اشكال الـ HUB >>>

وكان مبدأ عمله بأن كل جهاز في الشبكة يريد ان يبعث داتا معينة الى جهاز اخر في نفس الشبكة يرسل الداتا عبر الhub وهو يقوم بتحويل هذه الرسالة الى جميع الاجهزة في الشبكة وهيك بكون عمل (Broadcast all)

، طبعا هاد الاشي عمل مشكلة كبيرة بأنه ما عاد فيه خصوصية للاجهزة والداتا المتنقلة بينهم اثناء تواصلهم، فهذا أدى الى ضرورة وضع mac addrress الذي يميز كل جهاز عن الاخر في destination address وعند ارسال ال hub هذه الداتا مع الdestination mac address فلا يستقبل هذه الداتا الا الجهاز المطلوب.

الان ماذا لو قررت الشبكة بأن تتواصل مع شبكة ثانية أخرى يربط بينها HUB ايضا؟

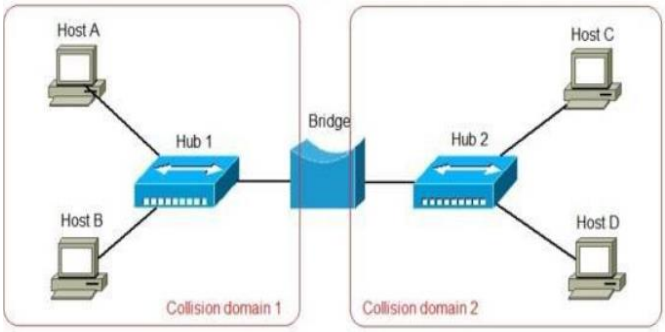
الجواب ببساطة ومثل ما خطر ع بالكم انه بربط بين الـ hub's 2 بكيبل وعندما يريد جهاز من شبكة 1 التواصل مع جهاز في شبكة 2 ، فتُرسل الـ Packets data من الشبكة الاولى الى hub الاول ثم يقوم الhub بارسالها الى الـ hub في الشبكة الثانية وهذا بدوره يرسلها الى جميع الاجهزة على الشبكة ولان الـHUB جهاز يعمل على اعادة الداتا التي تلقاها بشكل دوري فسيتم ارجاع نفس الداتا الى الhub الاول وهذا ايضًا يعيدها له وهكذا تكون دخلت الداتا في infinite loop، وحدث عندي (collesion) فيها، الامر الذي يؤدي الى سقوط الشبكة

ايضًا مشكلة اخرى تحصل في الـ hub

وهي عند تواصل اي جهازين داخل الشبكة لا يسمح بتواصل جهازين أخريات بذات الوقت لانه سيتسبب في collesion data بالتالي ايضًا يؤدي الى سقوط الشبكة

هذه المشاكل ادت الى ضرورة وجود جهاز يوقف تبادل الداتا بين ال hub's 2 فأتت فكرة ال bridge

Bridge (3



هذا الجهاز يوضع بين الHub's 2 يعمل على استقبال الداتا من الHUB الاول وارسالها الى الHUB الثاني مع منع اعادة ارسالها مرة اخرى .

ثم عملوا على جهاز يجمع عمل الbridge والhub سويًا بما يسمى جهاز الـ switch

switch (4

هو جهاز قادر على ربط مجموعة اجهزة ببعضها عبر مداخل خاصة (ports)

يعمل على مبدأ أن كل جهاز يتم ربطه في السويتش عن طريق كيبل الايثرنت، يأخذ منه الmac address ويخزّنه تبعًا للجهاز التابع له وعلى أي بورت تم اضافته، في ما يسمى بِـ mac address table

لتوضيح مبدا عمله

مثلا جهاز ١ اراد ارسال داتا الى جهاز ٤

ف رح تطلع الداتا من جهاز ١ تصل الى البورت الخاص فيها في السويتش هون بتعرّف عليها عن طريق source address ومعها الـ destination mac address

ثم يفحص الـ destination mac address هل هو address لجهاز تم تخزينه في ال table ام لا وبعمل تشيك على الادريسيز الموجودة في الماك ادريس تيبل وفي حالة انه مخزّن في هذا التيبل يأخذ رقم البورت يلي شابك عليه هذا الجهاز

ولا يسمح بحصول collesion data لان بين كل جهازين يتواصلون في bridge ، فلا يحدث اي تصادم وتداخل فالبيانات اثناء انتقالها

ثم نأتي لاهم جهاز في عالم الشبكات الذي يعتبر صاحب الدور الاكبر :

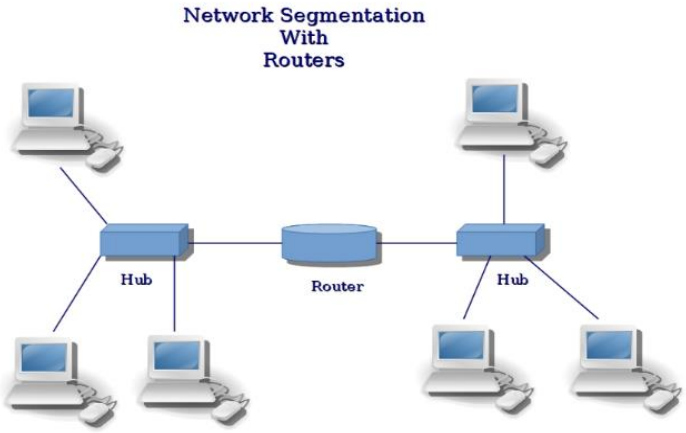
5) Router

الراوتر يعمل للشبكات الخارجية ويستخدم الـ IP address على عكس السويتش الذي يعمل بالـ Mac address للشبكات الداخلية

فتكمن حاجتنا له عند ربط شبكتين ببعضهما

وكل شبكة بأجهزتها لها ip address فريد (خاص بها) فلا يمكن ربط هذه الشبكات عبر switch أو Hub

لان هذه الاجهزة تتعامل فقط مع الـ mac address العناوين الداخلية.



الان رح نتطرق لموضوع حساب الـ **Subnet mask**

في البداية نحنا عندنا في IP address جزئين رئيسيات هن IP & Mask

اليوم رح نتعلم كيفية حساب الـMask لهذا الـ IP

كنا علمنا ان الـ IP مكون من 32 بت مقسمات على شكل(4 octet) كل octet مكون من 8 bits

وعلمنا لماذا نتوقف عند رقم 255 كـ أكبر رقم يمكن ان يوضع في الـ octet ،حيث ذكرناه في شرح الـIP address ويمكنك مراجعته

فهو يعتبر الـ last address فيكون مثل الـ cycle بعد ان تصل الى اكبر رقم ترجع تكمل من الصفر تلقائي

طيب بتتذكروا لما حكينا عن الـlan nework : وحكينا انه الها public IP تتصل بالشبكات الاخرى من خلاله فهو عنوان الشبكة على الانترنت

اما الـ IP address الخاص بالاجهزة فهو عنوان فرعي داخل هذه الشبكة الداخلية (LAN)

الـ Host : هو الجهاز الموجود جوا النيتويرك كالغرفة داخل البيت

Broadcast : هو last address في النيتويرك اي آخر رقم ممكن الشبكة تاخذه، وهو يلي ببث لجميع الـ Hosts يلي في النيتويرك

ومن ثم لتحديد الـsubnet mask تم تقسيم النيتويرك الى classes على هذا الشكل :

Class A : 255.0.0.0
Class B : 255.255.0.0
Class C : 255.255.255.0

يقسموا الـ networks ويميزوها جابوا مصطلح اسمه prefix size يرتبط بالـIP address على هذا الشكل :
192.168.1.10/28

ويأخذ ارقام من 0-31 اي 32 رقم على اساس ان كل octet يأخذ 8 بت

فكيف رح احسب الـ subnet mask وكيف اعرف شو الـ broadcast ، تبعوا معي نفهم كيف بنحسبهم عن طريق ال prefix size

على 4 ثمانيات حيث تقسَّم 32 الى (8+8+8+8)على حجم ال octet (اي انها تصل الى 8 كـ حد الاعلى)

فهذه ال28 يتم تقسيمها فتكون 8+8+8+4 الرقم 4 هي متممة جمع الثمانيات الى 28 حيث نقول 4=(8+8+8)-28

والان نضع 255 على حسب اذا كانت الoctet مكتملة الى 8 ام لا !

فستكون بهذا المثال 255.255.255._ لانني املك ثلاث ثمانيات مكتملة فوضعت 255 ثلاث مرات

هكذا وضعنا 255 على عدد رقم 8 ، والان بقي لدينا رقم 4 !

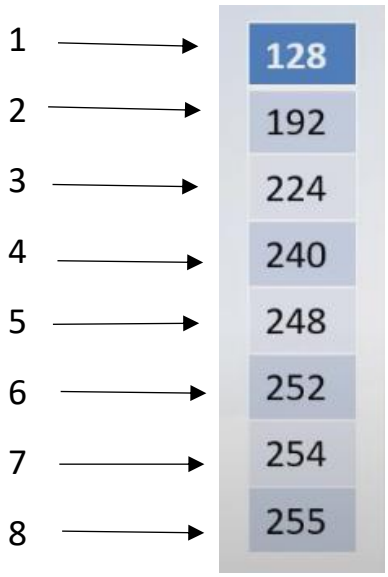
فلدينا هذا الجدول >>

نأخذ من خلاله ترتيب الرقم الذي لدينا

فعندنا 4 >> نأخذ الرقم 240 ونضعه في ال subnet mask

ليصبح 255.255.255.240

ولو كان لدينا الرقم 3 فنأخذ الرقم 224 ، وهكذا.



نأخذ مثال اخر بحالة اخرى :

192.168.1.10/18

اول شي سنقوم بتقسيم الرقم 18 على ثمانيات فيكون (8+8) والباقي (المتمم الى 18) هو 2

اصبح لدينا 0+2+8+8 وعليها فإن الـ subnet mask هو 255.255.192.0 ولو تسائلت لماذا 192 ومن اين اتت ؟ فهي من الجدول اعلاه، اعد النظر اليه وقم بحفظه لتسهيل الحل عليك.

بعد ان علمنا كيفية حساب subnet mask نأتي لتعلم كيفية حساب مفاهيم last addres اخرى

من نفس هذا العنوان مع ال prefix size

ونأخذ المثال نفسه 192.168.1.10/28

نبدأها بعناصر هذا الجدول

IP Address:	192.168.1.10
Network Address:	192.168.1.0
Usable Host IP Range:	192.168.1.1 - 192.168.1.14
Broadcast Address:	192.168.1.15
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240

IP Address : عنوان الجهاز في الشبكة (المعطى) بدون الـ prefix size وهنا يكون قد حجز رقم 10 في الشبكة

Network address : عنوان الراوتر الذي يعتبر اول جهاز في هذه الشبكة ودائمًا يقوم بحجز اول جهاز في النيتويرك وهو الـ public ip على الانترنت

معلومة يجب عليك فهمها وادراكها جيدًا

ليس شرطًا ان يكون رقم جهاز الراوتر في الشبكة 192.168.1.0

بصفته أول جهاز يأخذ الرقم 0 ، لا ليس دومًا !

سيتم توضيح المعلومة لاحقًا، فكل ما عليك الان هو ادراك هذا الشي.

Usable host IP range : هاد بوضحلي كم جهاز بقدر يشبك على هذه الشبكة (سعة الشبكة من الاجهزة)

رح تسألني كيف يعني من جهاز 1-14 وايش علاقتهم بالرقم 28 الـ prefix size

ركز معي ورح اجاوبك ، بتتذكر لما قسمنا ال28 الى 4+8+8+8 ، تعال وجيب رقم 4 معك وتابع معي

انظر الى هذا الجدول الذي يبين توزيع الـ 8 بت في ال octet الواحد

وابدا بكتابة رقم 1 على مدار 4 خانات (لان الرقم في هذا المثال هو 4) من اليسار الى اليمين بهذا الشكل الموضح في الصورة جانبًا >>>

ومن ثم انظر عند اي رقم توقفت ؟

عند الرقم 16 صحيح

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

هذا الرقم يُعنى بـ عدد الاجهزة في هذه الشبكة (*Total number of hosts*) ، لكن العنوان الاول صاحب الاي بي 192.168.1.0 هذا محجوز للراوتر نفسه فهو غير متاح، والاي بي الاخير (last address) رقم 192.168.1.15 محجوز ايضًا للـ broadcast ايضا هو غير متاح

اذا الاجهزة المتاح استخدامها لي في هذه الشبكة هي 16-2 =14 جهاز

وهكذا دومًا نقوم بطرح 2 من عدد الاجهزة الكلي للحصول على الـ Usable host IP range

أفهمت الان كيف تم تحديد الرينج بـ 192.168.1.1 – 192.168.1.14 ؟

نكمل حساب ما تبقى من مفاهيم في الجدول ادناه :

IP Address:	192.168.1.10
Network Address:	192.168.1.0
Usable Host IP Range:	192.168.1.1 - 192.168.1.14
Broadcast Address:	192.168.1.15
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240

Broadcast Address : هو last address وقد أخذ العنوان 192.168.1.15 في هذا المثال

لكون الرقم 15 يمثل الحد الاعلى من الاجهزة المسموح استخدامها في هذه الشبكة ، فلا عنوان بعده.

Number of Usable hosts : هي عدد الاجهزة المسموح استخدامها في هذه الشبكة

وتمثل *[Total number of hosts – 2]* ، حيث يمثل الرقم 2 >> ip الراوتر و ip البرودكاست (اول وآخر address)

Total number of hosts : هي عدد الـ Hosts الكُلي في الشبكة (الاجهزة المرتبطة بشبكة ما) وتعلمنا سابقًا كيفية حسابها ، يمكنك الرجوع اليها.

Subnet mask : هو ما تعلمنا حسابه في بداية الدرس.

أتذكُر عندما تحدثنا بهذه ؟

معلومة يجب عليك فهمها وادراكها جيدًا

ليس شرطًا ان يكون رقم جهاز الراوتر في الشبكة 192.168.1.0

بصفته أول جهاز يأخذ الرقم 0 ، لا ليس دومًا !

سيتم توضيح المعلومة لاحقًا، فكل ما عليك الان هو ادراك هذا الشي.

الآن سنأتي لتوضيحها ..

في المثال السابق كان لدينا prefix size = 28

وتم تقسيمه على اساس 8+8+4+4 الرقم 4 اوصلَنا الى ان *Total number of hosts =16*

الان سنصل الى معلومة جديدة عن طريق رقم 16 الذي توصلنا اليه

فهذا الرقم يعني عدد الاجهزة المرتبطة بكل شبكة كما تحدثنا سابقًا، لكن ما الذي يحصل لو كان IP جهازي يحمل رقم 192.168.1.40 وهو اعلى من رقم الـbroadcast المفترض له - كما تحدثنا سابقًا - لا جهاز على الشبكة بعده !

دعني اخبرك بأن الرقم 16 هنا في هذا المثال عمل على تقسيم العناوين الى شبكات كل شبكة تحوي 16 جهاز تبدأ الشبكة الاولى بأخذ حزمة من الاجهزة تكون من (0-15) ثم الشبكة الثانية تأخذ من (16-31) والثالثة تأخذ من (32-47) والرابعة تأخذ كذلك من(48-63) فـ لو كان IP جهازك 192.168.1.40 فهو ينتمي الى الشبكة الثالثة حيث يأخذ فيها الراوتر IP 192.168.1.32 ويأخذ البرودكاست IP 192.168.1.47

لو لاحظت انهم حجزوا اول وأخر Addresses في الشبكة .

سؤال : ماذا لو كان بدل الرقم 28 في prefix size [29] ما التغيير الذي سيصاحبه ؟

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

في البداية سيتغير ***hosts IP range*** عن 16 لاننا نكون قد قمنا بتعبئة 5 بت

في ال octet بدلًا من 4 (انظر الشكل) وبهذا نكون توقفنا عند رقم 8 ، ما يعني

ان الشبكة ستتسع فقط الى 8 اجهزة ككل ، ثم احذف منهم جهازين للراوتر والبرودكاست سيبقى 6 اجهزة متاحة لترتبط في الشبكة .

طيب بتتذكروا لما حكينا عن الوسط الناقل بين المرسل والمستقبل وحكينا انه ممكن يكون ناقل سلكي او لاسلكي !

اليوم سنوضّح ما هي الناقلات السلكية (cables)

تندرج انواع ال cables تحت نوعين رئيسيات :

1) Fiber optic cables : هذا ينقلها على شكل ضوء

2) Cobber cables : هذا ينقلها عن طريق الكهرباء

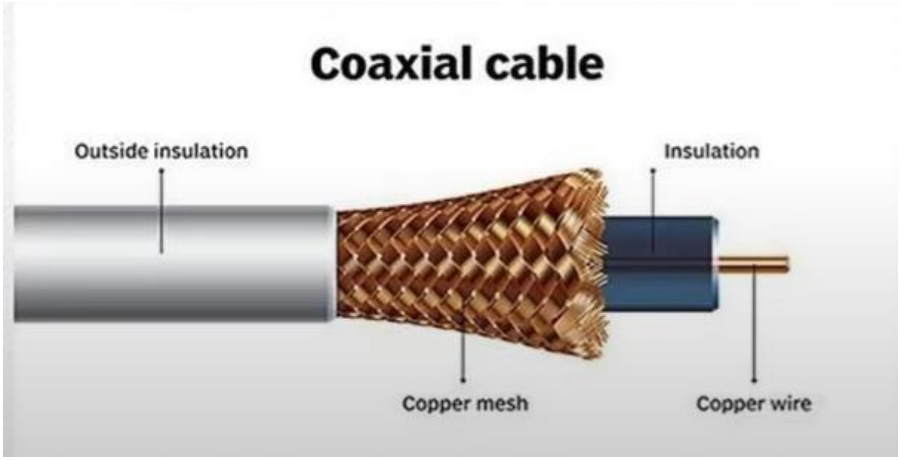
تعالوا نفصّل اكثر

ال cobber cables تنقسم الى نوعين

1- Coaxial cable
2- Twisted pair cables

Coaxial cable :

كنا قد درسنا عن البيانات انها تكون على صورة اشارات رقمية (0,1) ثم تتحول عن طريق المودم الى اشارات تماثلية تعتبر (electric signal)
هذا الكيبل يحوي البيانات (electric signal) في ما يسمى copper wire الذي يعد الناقل الرئيسي للبيانات ويوجد داخل عدة عوازل وطبقات
اول طبقة هي ال outside insulation وهي طبقة بلاستيكية خارجية تغلف طبقة اخرى بداخلها تدعى copper mesh وهي مجموعة اسلاك نحاسية تقوم على حماية الكيبل من الموجات المغناطيسية تحوي بداخلها طبقات اخرى هي شعيرات دقيقة تغلف مادة عازلة بلاستيكية بيضاء تدعى insulation داخل هذه الـ insulation يوجد الـ copper wire الذي يعد الناقل الرئيسي للبيانات في هذا النوع من الكيبلات .



هذا ال copper wire

يمتلك مقاومة صغيرة جدا

ونحن نعلم ان السلك الناقل للداتا التي هي على شكل موجات تماثلية قد تتأثر بأي شي حولها ، فماذا لو ان هناك كيبل كهربائي يسري فيه تيار عالي بجانب هذ الكيبل الناقل للداتا ؟ سيؤثر عليه بالفعل، وذلك لأنه ينشئ حول الكيبل الكهربائي مجال مغناطيسي يؤثر فيه على المحيط حوله اي ستتأثر الموجات التماثلية (الداتا) المنتقلة في الكيبل المجاور له

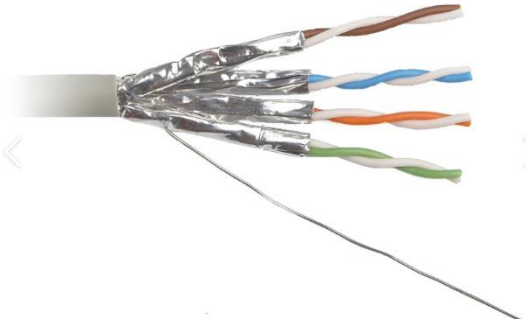
تأثر هذه الموجات يعني تغيير طرء عليها ، اي تغيرت الداتا ووردت مشاكل واشكالات

لهذا وجب علينا حماية هذه الموجات المنتقلة في الـ copper wire داخل طبقات عوازل تحمي بعضها من المجالات المغناطيسية

علمًا ان هذا الكيبل اصبح نادر الاستخدام بظهور نوع اخر من الكيبل يدعى **Twisted pair**

وهي كيبلات مجدولة تندرج تحت نوعين :

1- STP : shielded twisted pair
2- UTP : Unshielded twisted pair

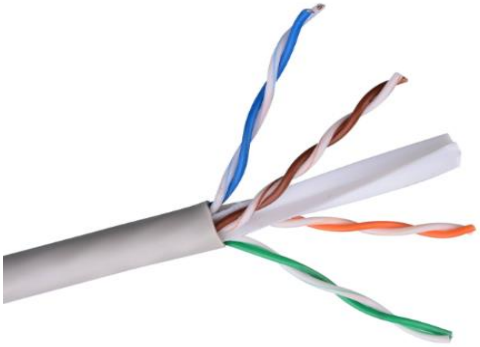


النوع الاول: **shielded** (المحمي)

محمي بواسطة القصدير الذي يغلفه ومن فوقه طبقة بلاستيكية خارجية.

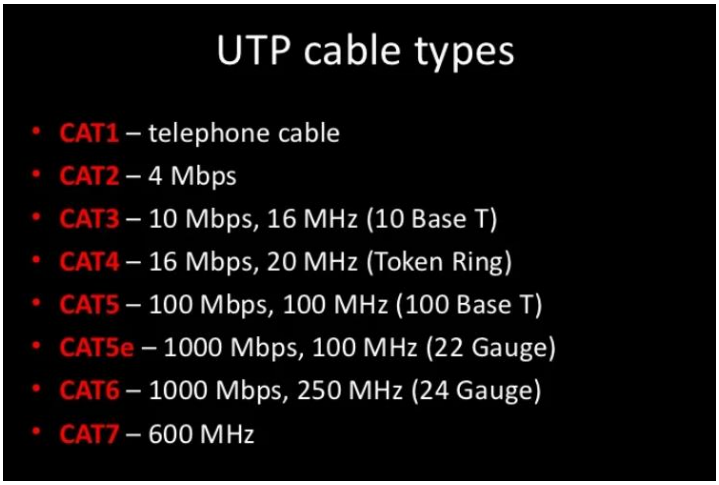
النوع الثاني : **Unshielded** (الغير محمي)

سميت بهذا لوجود طبقة واحدة خارجية فقط تحمي هذه الاسلاك، وبداخلها يوجد قطعة بلاستيكية تعمل كمنظّم لهذه الاسلاك وتحافظ على جدولتها بهذا الشكل في الصورة المرفقة :



هذا النوع - الكيبلات المجدولة غير المحمية(UTP) - هو ما يستخدم في غالب الاحيان

له انواع متعددة بسرعات مختلفة كما يظهر في الشكل ..



ولحتى يصير في transmition للداتا

في عندي على طرف الكيبل قطعة تسمى RJ-45 Connector سندرس عنها لاحقا، تحتوي هذه القطعة على مجموعة pins عند وصلها بـ pins الجهاز (مداخل الـ USB) تقوم بقراءة الداتا ما بين الكيبل والجهاز

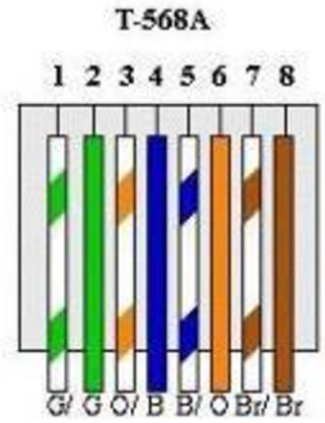
يتم ربط هذه القطعة (الرأس) RJ-45 Connector بالكيبل عن طريق 2 standard edition :

1- T-568A
2- T-568B

T-568A :

كان هذا الاصدار يأتي بترتيب ثابت لمداخل الوان الاسلاك من اليسار الى اليمين بهذه الصورة

(اخضر وابيض ، اخضر ، برتقالي وابيض ، أزرق ، ازرق وابيض ، برتقالي ، بني ، بني وابيض)

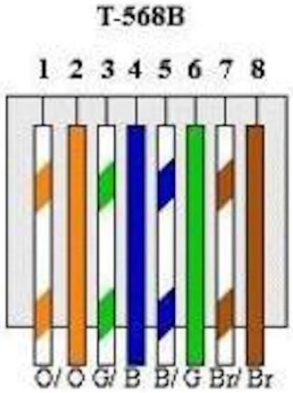


T-568B :

هذا الاصدار مشابه للقديم ، وكل ما هنالك تم تبديل اماكن الوان البرتقالي مع الاخضر.

ثم نتطرق الى طرق ربط الكيبل برأسية RJ-45 :

1) Straight through
2) Cross over

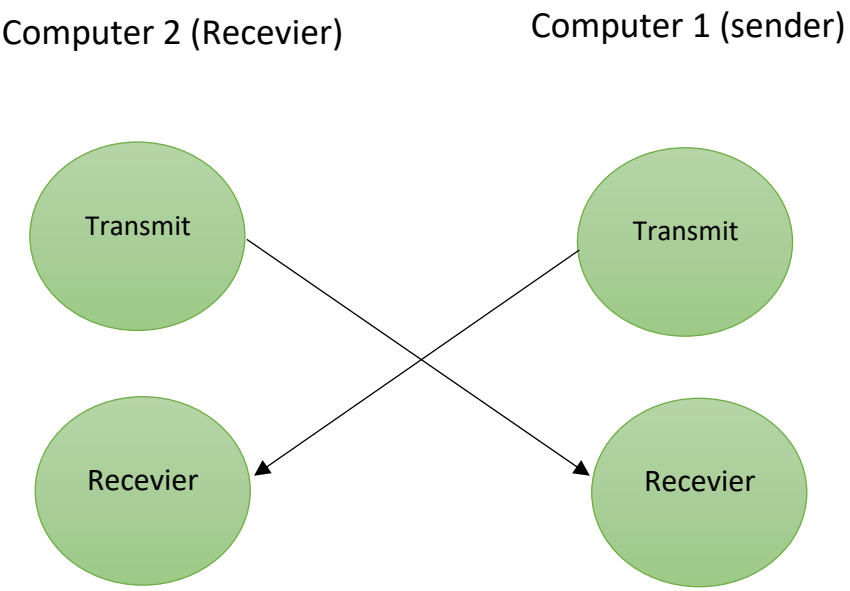


Cross over :

ويكون بشبك جهازين من نفس النوع (computer with computer) or (Router with router) .. او اجهزة تشبه بعضها في العمل كالـ (switch & Hub)

فطبيعي ان يتم ايصال مركز الارسال مع مركز الاستقبال ، ولا يجوز ربط الارسال مع الارسال بين الجهازين

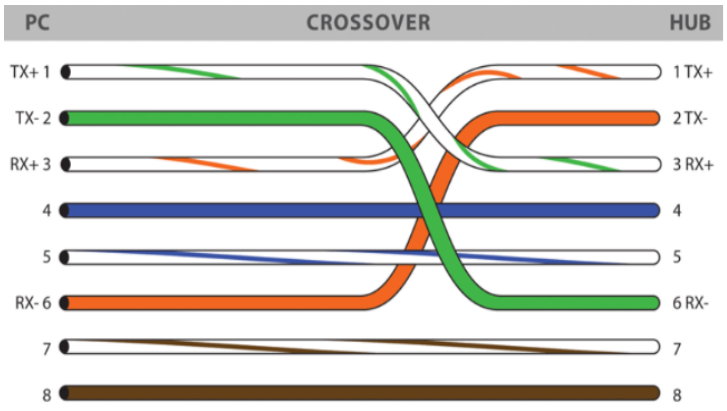
ومن الربط بينهم تكون عندي (Cross) ، ومنها أتت تسمية هذا النوع .



وهكذا هي حقيقة شبك هذه الاطراف ببعضها عند الجهاز

فكل جهاز لديه قناة ارسال تسمى بـ (TX) وأخرى للاستقبال تسمى (RX) ولكلٍّ منهم طرف موجب وآخر سالب عند الجهاز نفسه فيكون لدى الجهاز (TX+ & TX-) ايضا (RX+ & RX-)

ويكونوا في ترتيب واضح وثابت حيث يكون



TX+ في الـ pin 1

TX- في الـ pin 2

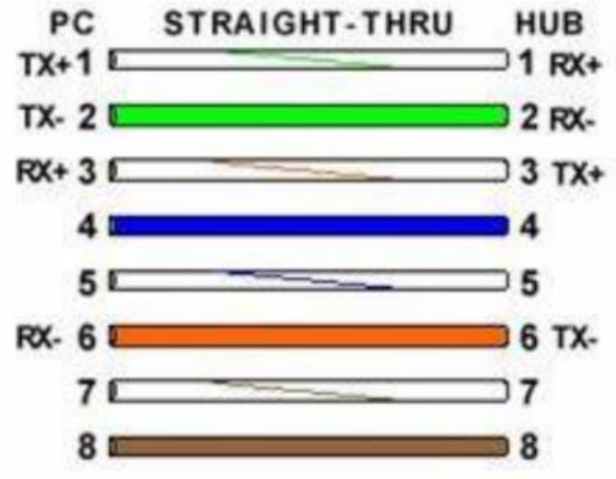
RX+ في الـ pin 3

RX+ في الـ pin 6

ويتم وصلهم ببعض كما في الصورة الموضحة امامك

<<<

أما الـ **straight – thru :**

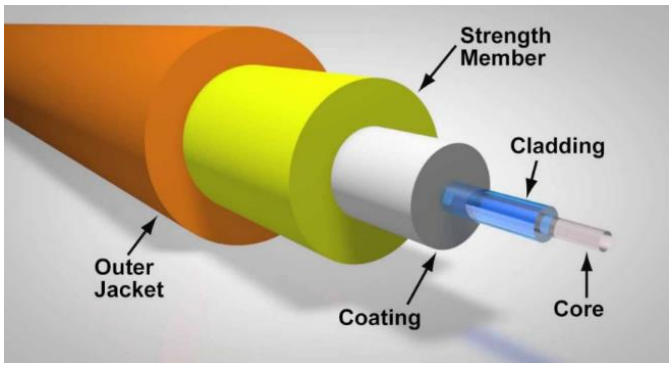


فيتم فيها وصل اجهزة غير متشابهة ببعضها البعض مثل (computer & switch) او (switch & Router) وهكذا

حيث لا يكون ترتيب مراكز الارسال والاستقبال في الجهاز المرسل كما في الجهاز المستقبل

فيقابل كل قناة ارسال موجبة (TX+) قناة استقبال موجبة (RX+) وهكذا على هذه الصورة

ثم مع تقدم الزمن أصبحت حاجتهم للسرعة تزداد يومًا عن يوم



ومن هذا المنطلق اتت فكرة كيبلات الالياف الضوئية (**fiper optic cable**) والتي امتلكت سرعات هائلة في نقل الداتا

وما ينقل الداتا فيه تحديدًا يسمى بالـ (core) المكون من زجاج حيث تُنقل فيه الداتا عن طريق انعكاسات تحدث بداخله

وهذه صور توضح تركيبه :

هذا و يكون تواصل الاجهزة مع الشبكة بثلاث حالات :

1- Unicast : ويكون فيها الجهاز يتصل بجهاز واحد فقط في الشبكة ولا يتصل بالاجهزة الاخرى.
2- Broadcast : يكون الجهاز يتصل مع اجهزة الشبكة جميعها في نفس الوقت.

3- Multicast : يكون الجهاز متصل مع جهازين او أكثر في الشبكة (ليس جميعهم).