

NETWORK Fundamentals



By :

Bassem Hamed

To

My Girl that always support me.

Bassem

About Author:-

Bassem Hamed is a Network and Security Engineer. He began to Building his Knowledge and Experience in Network more than 5 years ago.

He is Interested in information Security and Data Center.

Bassem worked in many Companies with Different Position , but he love Training .

He has Authored books in Microsoft “Active Directory and Infrastructure 2008 “and in Cisco “CCNAx 200-120”

Contacts :-



basem.cloud@gmail.com



/basemhamed.13



/Pasemhamed



01001582348

Network Fundamental

Network Fundamental

is considered as the Basics for anyone want to know what the Network is. This Book is Provides an overview of basic networking concepts, including network architecture, devices, design, components. The Book covers media types and standards and how data is encoded and transmitted.

Speaking in-depth about application coverage includes email, the domain name system, the World Wide Web and multimedia (including voice over IP, Internet radio video on demand, video conferencing, and streaming media. Each chapter follows a consistent approach: the Book presents key principles, and then illustrates them utilizing real-world example networks that run through the Internet, and wireless networks

Copyright © 2015 by Bassem Hamed
All rights reserved. This book or any portion thereof
may not be reproduced or used in any manner whatsoever
without the express written permission of the publisher
except for the use of brief quotations in a book review.

Printed in Egypt

First Edition, 2015

Content :-

<i>Chapter: -</i>	<i>Page</i>
Network Topology	6
Network Devices	17
Network Models	30
TCP/IP Model	42
Encapsulation	44
Headers	46
Addressing	50
Cisco Routing and Switching Components	70
Cables	74

Network Topology

قبل البداية في الحديث عن أي شئ – يجب ان نتعرف سويا على معنى ومفهوم Network هو توصيل الأجهزة مع بعضها بإستخدام Connection لضمان وجود Centralize Device بين الأجهزه وبعضها الغرض منها هو عمل Sharing of Recourses

- Hardware – File Server
- Software – any Application
- Service – Internet or Printer and etc ..



Network Topology

مصطلح يندرج تحته مفهوم طريقة توصيل الأجهزة مع بعضها وايضا طريقة الـ Connection التي تحدث بين الأجهزة وبعضها لها نوعان :-

Virtual or Logical Topology --- and --- Physical Topology

Virtual Topology

معناها كيف يتم نقل الداتا بين الأجهزة وبعضها - How Devices are Communicate

Network Fundamental

مثل :- Bus Topology and Ring Topology with Token

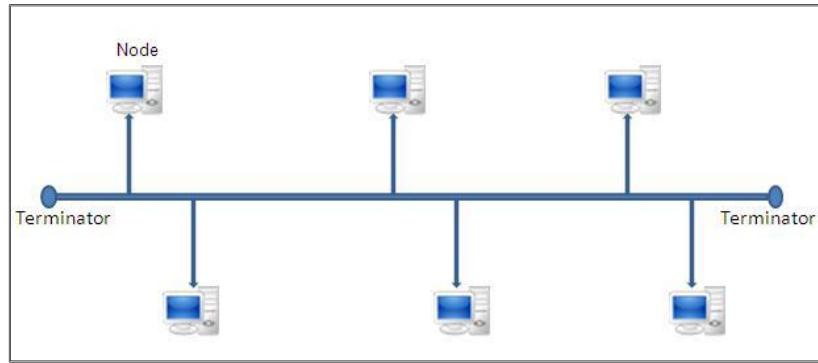
Physical Topology

? How Devices are Connected معناها كيف يتم توصيل الأجهزة مع بعضها البعض وما هو شكل الداتا وطريقه نقلها --

مثل :- Star Topology and Ring Topology with MAU

لنتحدث عن كل منهم بالتفصيل

Bus Topology :- -1

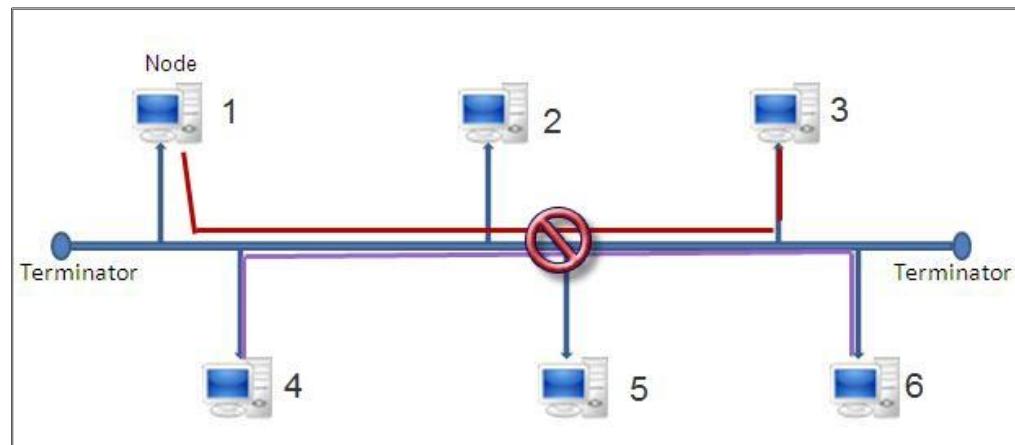


مجموعة من الأجهزة يتم توصيلها على Line واحد كما هو موضح في الشكل .
وكما تم التوضيح من قبل أن هذا النوع هو أول انواع الـ Virtual Topology – أي انه لا يوجد في الـ Real Life توصيل يتم كهذا ولكن !!
كان هذه هي بداية التوصيل من قبل .

في نهاية الـ Line يوجد Device يسمى Terminator
هذا النوع كان أرخص انواع التوصيل وكان بدائي جدا في التوصيل

كان هناك عيوب كثيرة جدا لهذا التصميم من أهم عيوبها هو الـ :-

Collision



لو Source PC1 يقوم بارسال Data او Access على اي service على PC3 Destination وفي نفس الوقت يقوم جهاز آخر مثل PC6 يقوم بعمل Access على PC4 فوجت ان باقي الـ Accounts الخاصه بك سواء على الـ Broadcast المرسلة كل الأجهزة ستقوم بإستلامها لأنها مرسلة

Broadcast معناه :

تخيل انك قمت بفتح حسابك على موقع فيس بوك عندها قمت بعمل Login فوجت ان باقي الـ Accounts الخاصه بك سواء على الـ Social Media او على الـ E.Mail Accounts تم فتحهم في نفس الوقت !!
انت فقط كنت تريد الفيس بوك ولكن .. تم فتح كل الـ Accounts في نفس الوقت
وسينتم توضيحيها تفصيليا لاحقا

نفس الفكرة مع الأجهزة

في الحالة الأولى PC1 مع PC3 ولكن باقي الأجهزة حدث انها استلمت داتا او استلمت طلب ليس لها فستقوم بعمل Drop له ولكن حدث Loop في الشبكة حتى تصل الى الـ Destination المطلوب بالإضافة الى الـ Loop مع وجود جهازين ايضا يقومون بالاتصال مع بعض فسيحدث Collision أي تصادم في نقل الـ Data بين الأجهزة وبعضاها وسيحدث Drop لكل الـ Packets المرسلة

للتغلب على مشكلة الـ Collision :-

CSMA / CD

Carrier Sense Multiple Access / Collision Detection

تحدث فقط في شبكات الـ Wired أي ان اي جهاز يقوم بارسال Data لأي جهاز آخر يقوم بعمل Carrier Sense لـ Carrier او الحامل الذي يقوم بنقل الداتا حتى يتتأكد هل هناك جهاز اخر يقوم بالإرسال في نفس الوقت أم لاMultiple Access حتى يحدث Detect الذي قد يحدث بين الأجهزة ولكن إذا حدث ايضا ارسال في نفس الوقت سيحدث Collision وDrop لـ Packet المرسلة (نقل من حدوث التصادم وليس منهنهائي)

هناك مصطلح آخر يسمى CSMA / CA

Carrier Sense Multiple Access / Collision Avoidance

اي تجنب حدوث الـ Collision من الاساس وهي تحدث في شبكات الـ Wireless لأنه في هذا النوع من الـ Connection لا يجب ان يحدث Collision من الاساس

Jamming of Signal

تحدث بمجرد حدوث الـ Collision وتقوم بإعطاء كل الأجهزة Random of Time وقت عشوائي لكل الأجهزة لغرض انه بعد إنتهاء هذا الوقت يقوم الجهاز بعمل إرسال لـ Data كما يريد لتجنب حدوث الـ Collision بين الأجهزة

وظيفة الـ Terminator

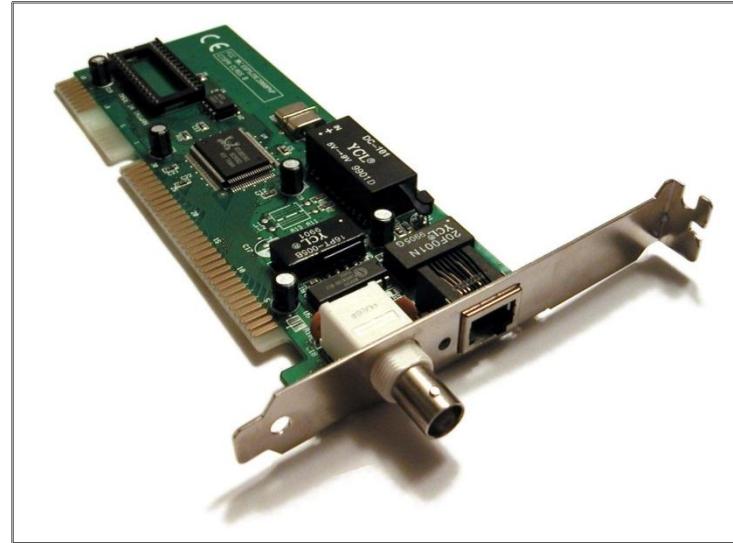
يقوم بإمتصاص الإشارة الموجودة في الـ Line او الـ Carrier بعد ان يتم ارسالها Broadcast لكل الأجهزة -- حتى لا يتم تكرارها مره أخرى في الـ Network

لتجنب حدوث Loop بعد الـ Loop الأساسي الحادث بسبب الـ Broadcast



كان يستخدم في هذه الـ Topology نوع من انواع الـ Cables يسمى Co-Axil Cable - مثل المستخدم في اجهزه الدش - وسيكون هناك Document منفصلة تتحدث عن الـ Cables

وأيضا كان يستخدم Network Interface Card يستخدم في توصيله الـ Co-Axil هنتكلم عنه بالتفصيل في الشابتر الـ Cables



في بداية هذه الـ Topology كان يستخدم الـ Terminator ثم بعد ذلك ظهر الـ Hub -- وكلاهما كان يدعم الـ Co-Axil Cable لأن لا يوجد من ضمن الـ Internal Component الخاصية بهم

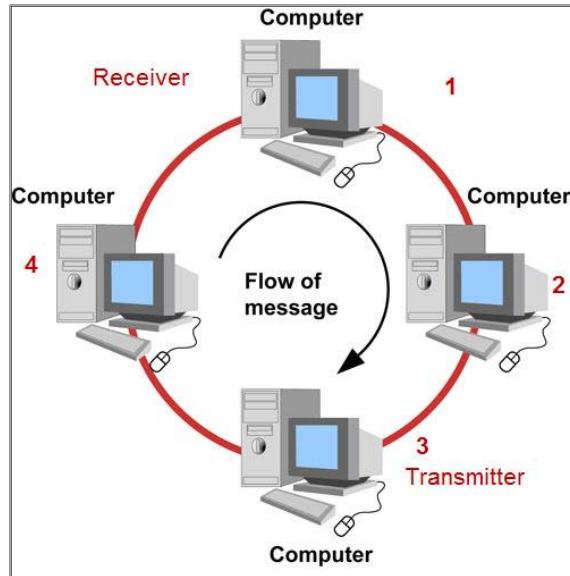
Processor

سندث عنهم في الـ Document القادم

Ring Topology

-2

I – Ring Topology Using Token



ثاني نوع من انواع الـ Virtual or Logical Topology - حينما يقوم PC3 Transmitter بارسال Data الى PC1 Receiver

سيتم انشاء ما يسمى الـ Token بواسطة الـ Transmitter

الـ Token

Destination MAC Address & IP تحتوي على الـ Data المرسلة بالإضافة إلى الـ Virtual Thing

PC3 هيتأكد ان الـ Token Free أي لا يقوم أي PC آخر بارسال Data

سيقوم بعمل الـ Load على الـ Token -- وعمل أيضا Load لـ IP Source and Destination Address

يتم إرسال الـ Broadcast إلى كل الأجهزة المتصلة مع بعض في الـ Network

وظيفة عمل الـ Receiver عند إستلام الـ Data

- 1 - هيعلم Check أن هو الـ Address المطلوب
- 2 - هيأخذ الـ Data المرسلة Copy وليس Cut
- 3 - هيعلم Repeat لـ Data ، إعادة إرسال او إعادة تقوية للإشارة المرسلة
- 4 - يتم وضع Mark انه تم إستلام الـ Data بنجاح

كما وضمنا انه سيتم إرسالها Broadcast – فإن الـ Data سيتم وصولها إلى الـ Transmitter مرة أخرى

بعد وصول الـ Token مرة أخرى إلى الـ Transmitter

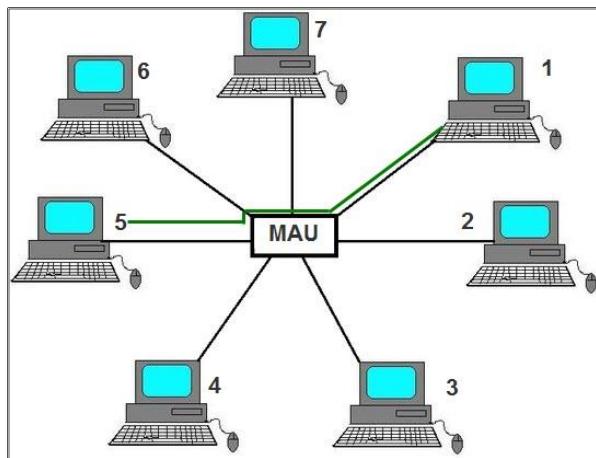
- 1- سيقوم بالتأكد انه تم إستلام الـ Data عن طريق الـ Mark الذي قام الـ Receiver بوضعها
- 2- سيقوم بعمل لـ Data Delete من الـ Token
- 3- ستصبح الـ Token خالية Empty لأي جهاز آخر ليستخدماها

II – Ring Topology Using MAU

أول انواع الـ Physical Topologies - أي ان هناك فعليا Devise يتم من خلاله توصيل الأجهزه مع بعضها البعض

Centralize Device

الـ MAU Media Access Unit هو المسئول عن انشاء الـ Token وإرسالها الى الـ Receiver المطلوب



1- PC1 سيقوم بإرسال الـ Data الى PC5 من خلال الـ MAU

2- سيتم إرسال الـ Data بـ Broadcast الى كل الأجهزة المتصلة مع بعضها من خلاص الـ MAU

3- مثلا PC2 سيقوم بعمل Check على الـ Data المرسلة || هل هو الـ Receiver المطلوب أم لا

4- إذا كان ليس هو المطلوب سيقوم بإرسال الـ Data مرة ثانية الى الـ MAU – وسيحدث هذا مع كل الأجهزة حتى يصل الى الـ Receiver المطلوب

5- حتى يتم إرسالها الى PC5 وهو الجهاز المطلوب .

6- سيقوم بعمل Copy and Mark لـ Data لـ Data Release or Delete من الـ MAU

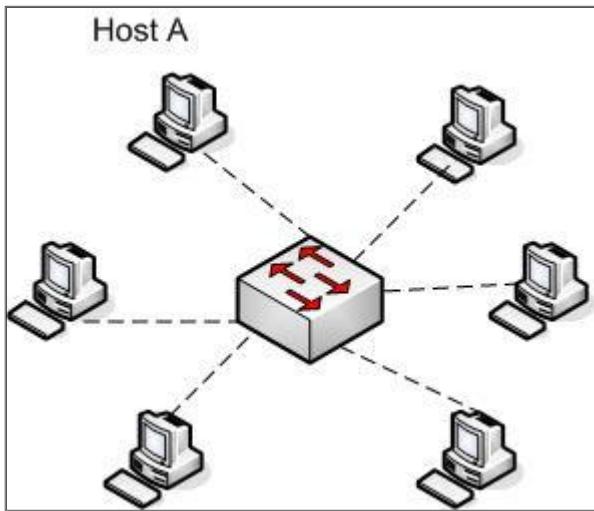
7- بعد ذلك سيقوم بعمل Empty Token وارسالها الى الـ MAU

في الـ Ring Topology بأنواعها لا يحدث Collision

لأن الـ Data يتم ارسالها واستقبالها من خلال الـ Token وطالما الـ Token مشغول فلن يستطيع اي جهاز ارسال Data لجهاز آخر

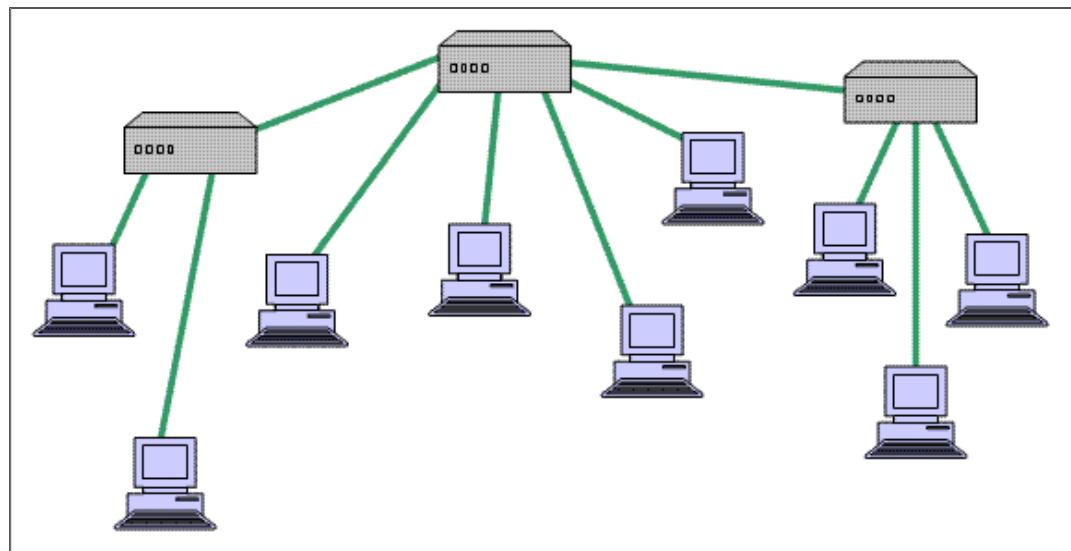
ولكن المشكلة الفعلية كانت في الـ Broadcast

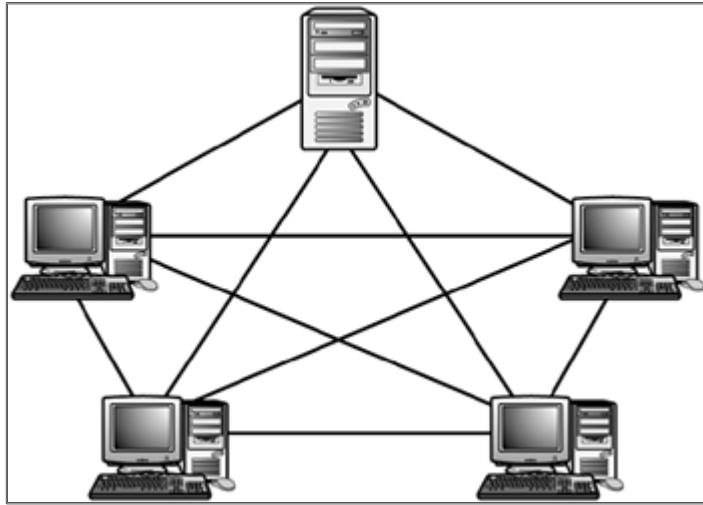
Stat Topology -4



أفضل أنواع الـ Topology والتي يتم استخدامها حالياً كان الـ Devises المستخدمة بدأت في التطور من الـ Repeater → Hub → Bridge → Switch وهذه سيكون محور حديثنا في الـ Document الفادمة Network Devises ومراحل تطورها وما هي الأجهزة المستخدمة حالياً – وكانت تعتمد على الـ Device المركزي الذي متصل عليه كل الـ PC's

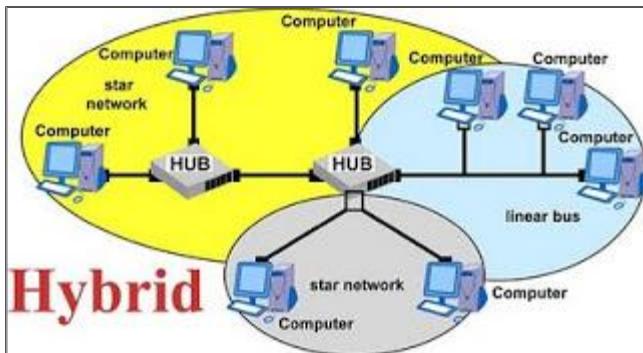
Aktar من Tree Topology ← Star Topology وممكن ايضاً يطلق مصطلح Tree Topology حينما نقوم بدمج Bus and Star Topology





Mesh Topology -5

الغرض منها انني أضمن الـ Stability والـ Redundancy في توصيل الأجهزة ونقل الـ Data بين الأجهزه وهي بالطبع Logical Topology توضح على هذه الصورة – اذا أردت فعلياً توصيلهم على هذه الشكلة ستقوم بإضافة 4 لـ NIC لكل جهاز ولكنها تستخدم للتوصيل بين الـ Switches



Hybrid Topology -6

توصيل أكثر من نوع من أنواع الـ Topologies مع بعضهم كما في الـ Diagram

	Bus Topology	Ring Topology	Star Topology
Speed	10 M.Bit/S	45 M.Bit/S	100 M.Bit/S
Device	Terminator or Hub	Token or MAU	Hub or Switch
Cables	Co-Axil or UTP	UTP	UTP

Communication Type	Description
Simple Duplex	في النوع دا اما الـ Cable بيعت داتا او بيستقبل داتا "زي الـ Cable بناء التليفزيون"
Half Duplex	بيعت داتا وبستقبل داتا بس مش في نفس الوقت "زي اللاسلكي بناء الشرطة"
Full Duplex	بيعت وبستقبل في نفس الوقت زي الـ Cables اللي بستخدمها بين الأجهزة

Networking Type

LAN → Local Area Network

مجموعة من الأجهزة في المكان نفسه أو مترسبة في مساحة صغيرة **Connected** مع بعضها البعض **-** مثل:

- Ethernet 10Mb/S
- Fast Ethernet 100 Mb/S
- Giga Ethernet 1000 Mb/S
- 10 Giga Ethernet 10Gb/S

WAN → Wide Area Network

Used to connect LANs together .Typically, WANs are used when the LANs that must be connected are separated by a large distance

MAN → Metropolitan Area Network

Hybrid between a LAN and a WAN

PAN → Personal Area Network

Like Bluetooth

SAN → Storage Area Networks

Between Storage Devices and File Servers

يتم إنشاؤها وتوصيلها بين أجهزة التخزين والسيرفرات وفي الغالب يتم استخدامها في **الـ Data Center**

Advantage:-

- Performance is fast.
- Availability is high because of the redundancy features available.
- Distances can span up to 10 kilometers.
- Management is easy because of the centralization of data resources.

Disadvantage of SANs is their **Cost**.

This Page Intentionally Left Blank

Network Devices

سنتكلم عن بعض الـ Devices المستخدمة في عالم الـ Network ولكن بشئ من التفصيل نظراً لأهميتهم فيما بعد – أيا كان تخصصك في مجال الـ Network

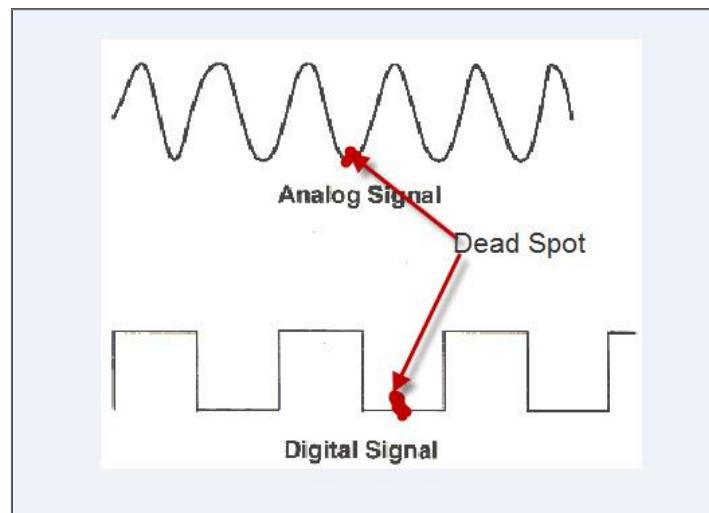
وسنحاول في حديثنا عن الـ Devices ان نقوم بتوضيحها نظراً لنطورة التكنولوجى بداية من الأنواع الأولى حتى ما آلت اليه التكنولوجيا في يومنا الحالى

Terminators -1

تكلمنا عنه في الـ Document السابق وقولنا انه يقوم بإمتصاص الـ Signal حتى لا يحدث Loop أكثر من مرة في الشبكة وكان يستخدم مع الـ Bus Topology

Repeater -2

يقوم بعمل لـ Re-generate Signal



إذا تم نقل الـ Data الى مسافات طويلة يحدث لها Drop وتشویش Noising , لذا يجب من وجود Device يقوم بعمل Re-generate للإشارة لـ Signal التي تحمل الـ Data

وايضاً ينصح بأنه يجب الا يزيد طول الـ Cable الذي يتم توصيله بين الـ PC والـ Device المسئول عن الـ Internet Service عن Digital Signal حتى لا يحدث Drop لـ Signal ويكون الـ Internet بطيء -- يستخدم الـ Repeater مع الـ Meter100

اما مع الـ Analog Signal يستخدم جهاز يسمى الـ Amplifier ولكن وظيفته هو تضخيم الاشاره وليس Re-Generate

- يقوم بارسال الـ Data إلى كل الأجهزة المتصلة أي Broadcast



أنواع الـ Repeater

Wireless Repeater -

Wired Repeater (Booster _ Extender) -



Connector -3

نفس وظيفة عمل الـ Repeater وهي Re-Generate ولكن الإختلاف هنا ان الـ Connector يقوم بتوصيل One Cable فقط – اي جهاز كومبيوتر اما في الـ Repeater يمكننا توصيل أكثر من جهاز كومبيوتر علي نفس الـ Device

يمكننا ان نعتبر :-

Repeater → Multi port Connector



Hub -4

كانت بداية ظهور الـ Multi-Port Devices هي الـ Hub يستخدم الـ Hub كمشترك يقوم بتجميع أكثر من جهاز كومبيوتر في مكان واحد لعمل LAN داخلية

من أهم عيوبه :-

○ انه كان يقوم بعمل Share للـ Bandwidth (السرعة)

المستخدمة في نقل الـ Data

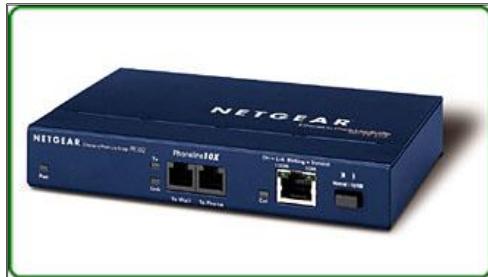
بمعنى انه إذا كان لديك سرعه 100 M.bit/S وتوجد اجهزة تتصل مع بعض سيقوم بتقسيم السرعة علي عدد الأجهزة المتصلة به

○ أيضا انه كان يقوم بإرسال كل الـ Data المرسلة لكل الأجهزة المتصلة معه في الشبكة – فيحدث في الشبكة – لأنه لا يملك من ضمن الـ Component الخاصة به ل يقوم بتخزين الـ MAC Loop . Collision Address

Hub → Multi-port Repeater

Type of Hub

1- Active Hub	<ul style="list-style-type: none"> ➤ Support CSMA/CD ➤ Re-Generate of Data ➤ Sending Data ➤ Using only UTP Cables
2- Passive Hub	<ul style="list-style-type: none"> ➤ Sending Data Only ➤ Using only UTP Cables
3- Hybrid Hub	<ul style="list-style-type: none"> ➤ Support CSMA/CD ➤ Re-Generate of Data ➤ Sending Data ➤ Using Co-Axil and UTP Cables
4- Intelligent Hub	<ul style="list-style-type: none"> ➤ Support IGMP (internet Group Management Protocol) ➤ Using 10 Base.T Co-Axil



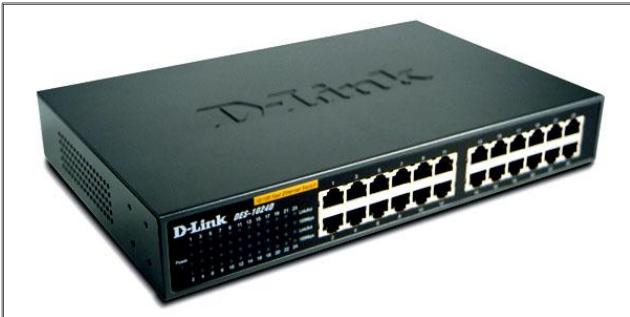
Bridge -5

بداية ظهور الـ Smart Devices التي تستطيع ان تتعامل مع الـ MAC Address للتغلب على مشكلة الـ Collision التي تحدث بقلم بارسال الـ Data للأجهزة Unicast وليس Broadcast

Bridge Type

1- Transparent Bridge	<ul style="list-style-type: none"> ➤ Not Supporting CRC Cyclic Redundancy Check
2- Mixed Media Bridge	<ul style="list-style-type: none"> ➤ Support CRC Error Detection only
3- Local Bridge	<ul style="list-style-type: none"> ➤ Between Rooms in the Same Building ➤ الخاص به غالباً الـ Hardware
4- Remote Bridge	<ul style="list-style-type: none"> ➤ Between More than One Building

سيتم الحديث عن الـ CRC بالتفصيل في الـ Document القادم



Switch - 6

- من اهم الـ Devices التي تتعامل معها في شبكتك او شركتك
- وهذا هو النوع المستخدم حاليا في الشركات لتوصيل الأجهزة مع بعضها البعض حتى يقوم بعمل Sharing of Resources
- Switch is a Smart Device لأنه يملك في الـ Processor الخاصة به MAC Address Component يقوم بتخزين الـ MAC الخاص بالأجهزة حتى يتغلب على مشكله الـ Broadcast ومشكله الـ Collision التي تحدث لأنه يقوم بإرسال الـ Data – Unicast أي محددة الى وجهتها المقصودة ، ولا يتم إرسالها الى كل الأجهزة تغلب على كل العيوب الموجودة في الـ Hub
- لا يقوم بعمل Share للـ Bandwidth المستخدمة

Unicast → One to One

- أغلبية الـ Switches التي نستخدمها في البيوت سيكون نوعها Un-Managed أو End Users ولا يمكننا عمل اي تعديلات عليها او عمل Configuration

Just Only Connecting PC's

- ولكن هناك شركات تقوم بتصنيع Switches يمكنك عمل اي Configuration تريدها عليها مثل CISCO and Juniper وهناك كورسات و Material حتى تستطيع ان تتعامل معها

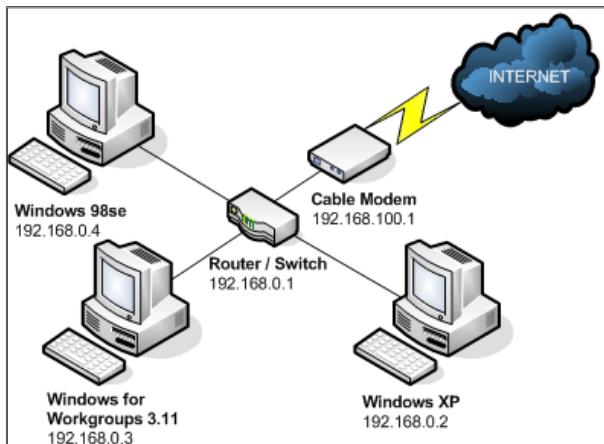
Switching Mode

<p>❖ Cut Throw</p>	<p> يقوم بإرسال الـ Data الى الـ Destination المطلوب دون إجراء اي تعديل فيها او تصحيح</p>
<p>❖ Store and Forward</p>	<p> يقوم بتخزين الـ Frame كاماً ثم يقوم بعمل Check for Errors عن طريق CRC</p>
<p>❖ Fragment Free</p>	<p> يقوم بعمل Check على أول 64 Bit فقط Error التي يحدث بهم الـ</p>

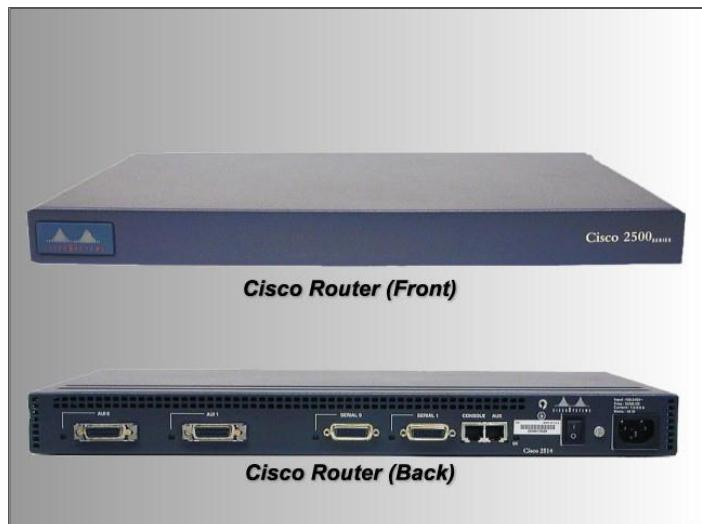


Router -7

- The Gateway for Devices
- يستخدم في ربط الفروع مع بعضها – Connecting More than Different Subnet
- Define the Best Way to Send Data Between Source and Destination
- لا يسمح بمرور رسائل الـ Broadcast ولكن فقط يرسل رسائل الـ Unicast



هناك شركات تقوم بتصنيع Router يمكن عمل اي Configuration CISCO and Juniper عليها مثل و هناك كورسات و Material حتى تستطيع ان تتعامل معها



من الأخطاء التي نقع فيها هو اننا بنقول على الـ Device الموجود في المنزل مصطلح الـ Router لأنه ليس ADSL (Asymmetric Digital Subscriber Line) وإنما يسمى ()



ADSL - 8

هذا هو شكل الـ Device المتواجد عندنا في المنازل وظيفته انه بيعمل Modulation and De-Modulation يعني بيحول الاشارة اللي جياله من السينترال الـ Analog – الي - الـ Digital علشان تقدر تتوصل مع أجهزة الكمبيوتر

بكل بساطة :-

- اغلبيه الأنواع لا تقوم بعمل Router وهذه هي أهم مميزات الـ Router (هناك انواع Routing Protocols)
- وأيضا اغلبيه الـ Routers لا تملك من ضمن الـ Interfaces المتصله بها Input RJ-11 لتوصيل الخط الأرضي المسئول عن خدمة الإنترن特

هنا كتبت أغلبيه - حتى لا أعممها على كل الأجهزة لأن هناك أجهزة يوجد فيها Input RJ-11 علشان يقوم بعملية التحويل Digital to Analog Signal من

طريقه توصيل الـ Internet الى المنزل ؟

هناك مصطلحان أساسيان لمعرفة كيف يتم التوصيل الى المنازل :-

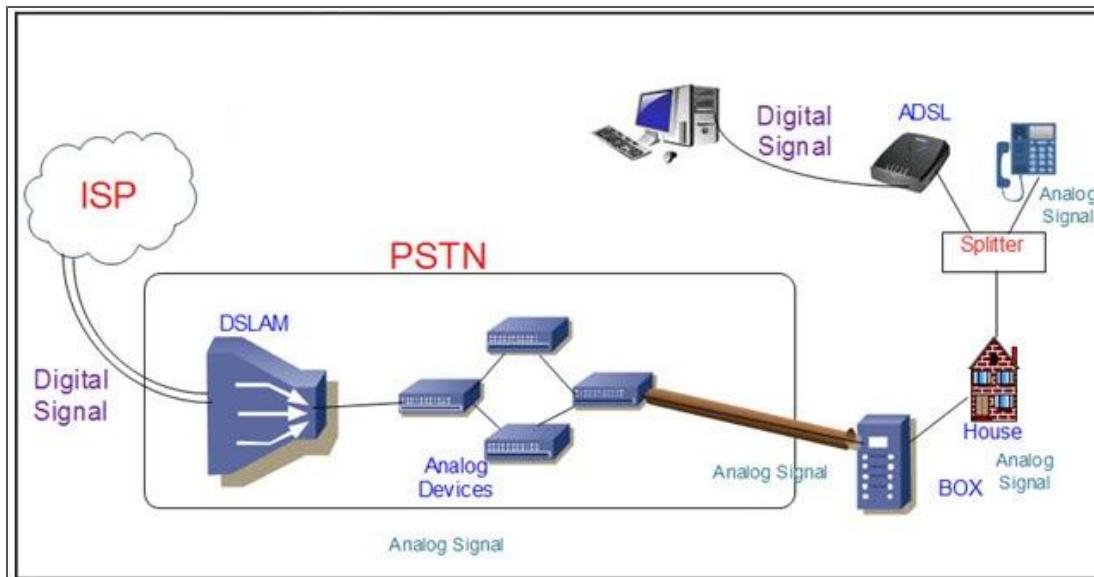
ISP → Internet Service Provider

وهي أي شركة من شركات مزودي خدمة الانترنت مثل :-

TE-Data , Link , Vodafone , etc,,,

PSTN → Public Switched Telephone Network

وهي اي شركه مسؤولة عن خدمه التليفونات الأرضية كالمصرية للإتصالات



لا توجد اي شركة ISP يمكنها توصيل Internet لأي عميل دون إذن من شركة الـ PSTN

يتم توصيل شركات الـ ISP بالـ DSLAM داخل السنترال او الـ PSTN عن طريق Fiber Cables

بعد ان يعاقد العميل مع الـ ISP تقوم هي بدورها بالاتصال مع المصرية للإتصالات وتحديد ما هو وضع البيت وهل هناك اي مشاكل في الخط حتى يسمح له بالتوصيل ام لا

هناك بعض المناطق النائية لا يسمح فيها بالسرعات العالية لالانترنت – لأن الـ Analog Cables مش بتقدر تستحمل الضغط العالي والسرعات الزيادة

DSLAM -9

DSLAM → Digital Subscriber Line Access Multiplexer

من اهم الاجهزه الموجودة في اي سنترال او اي شركة تعمل كـ PSTN



يقوم بتحويل الـ Analog Signal الى Digital Signal حتى يتم توصيلها من خلال السنترال لأنه يتعامل مع الـ Analog فقط
يتم ارسال الـ Analog Signal من خلال كابلات الـ PSTN حتى تصل الى الـ Box المتواجد أسفل كل بيت Customer موردا بالحائط حتى يخرج ويتم توصيله بما يسمى Splitter Premises

من أهم عيوبه انه يقوم بعمل لـ Share Bandwidth حيث انه اذا كان هناك 4 او 5 خطوط متصلين به – وهناك خط الـ Load على أقل من الآخر – يتم اخذ منه سرعة وتوزيعها على الخطوط الـ Over Loaded حتى يستطيع ان يتعامل مع الضغط الغير محتمل

Splitter-10



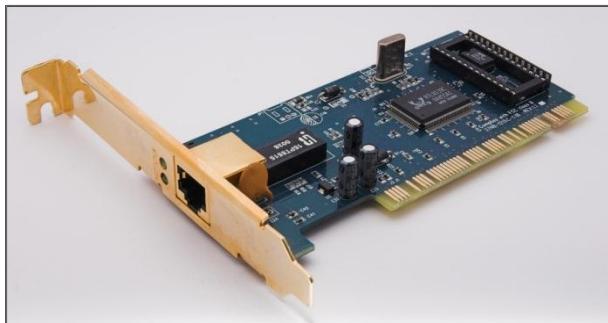
- يقوم بفصل الإشارة إلى اثنين أحدهما إلى التليفون الأرضي والأخر إلى الـ ADSL حتى هذه اللحظه كل هذا عبارة عن Analog Signal ولكن ; الـ PC يتعامل مع الـ Digital Signal لذلك يقوم الـ ADSL بعمل العملية العكسية وهي تحويل الـ Digital إلى Analog

- وأيضاً يقوم بعمل منع للتشویش الذي يحدث عند إجراء اي مكالمات أرضية

Digital Signal → Using RJ-45

Analog Signal → Using RJ-11

الـ Router لا يقوم بأي من هذه الوظائف



NIC (Network Interface Card)-11

Ethernet
Physical Address
MAC Address

الذي يتم توصيله بالـ Switch او الـ ADSL Modem حتى استطيع ان اتصفح الـ Internet



Personal Computer-12

من أهم المكونات الأساسية لعمل أي شبكة سواء كانت LAN او WAN يعتبر هو العنصر الأساسي والمهم في عمل اي نوع من انواع الـ Network

[Server -13](#)



- جهاز له امكانيات خاصة من حيث الـ Hardware حيث يستخدم لعمل Internal Domain حتى يتم التحكم في كل الأجهزة الخاصة بالشركة – ويمكن من خلاله ايضاً عمل Important Data Server حتى يتم تخزين كل الـ File Server لتجنب فقدانها
- اي موقع يتم التعامل معه او الدخول عليه هو في الاساس من خلال Server عليه كل البيانات والبيانات والمعلومات الخاصة بكل المستخدمين مثلًا كالـ فيس بوك – هناكآلاف السيرفرات التي تخدم على هذا الموقع

كورسات شركتي Microsoft and RedHat تتخصص في هذا المجال وتعلمك كيف تدير هذه السيرفرات وكيف تتعامل معها وما هي امكانيات كل شركه عن الاخر



[Access Point-14](#)

تستخدم لاقوية اشارة الـ Wireless وايضا تحويل الـ Wireless إلى Wired Device

يمكن ايضاً ان تجد لها مسميات أخرى

WNAP → Wireless Network Access Point
NAP → Network Access Point



[IP Phone-15](#)

- Phones that Connected Using RJ-45 not RH-11
- يتم استخدامها لإجراء اي مكالمة سواء كانت محلية او دولية من خلال الـ ISP وليس الـ PSTN
- وتعتبر تكنولوجيا VOIP حل مثالي جداً للشركات الكبيرة التي تمتلك اكبر من فرع في اكبر من محافظة او اكبر من دولة

هل تمتلك Skype على Account او هل انت من مستخدمي Viper ؟

هل حدث في مرة من المرات حينما قمت بدفع اشتراكك قام المسؤول بإخبارك ان هناك تكلفة اضافية لمكالمات viper او Skype !! بالطبع لا

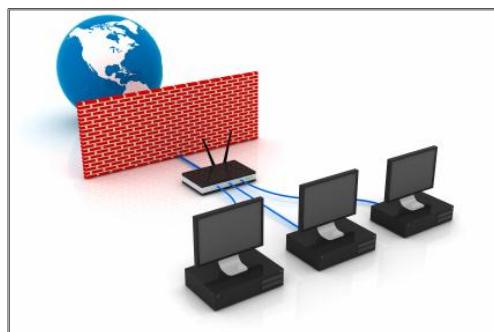
Network Fundamental

لأنه تم حسابها من ضمن الاشتراك المخصص له Internet Service و هكذا مع الـ IP Phone Communication



Multi-layer Switch-16

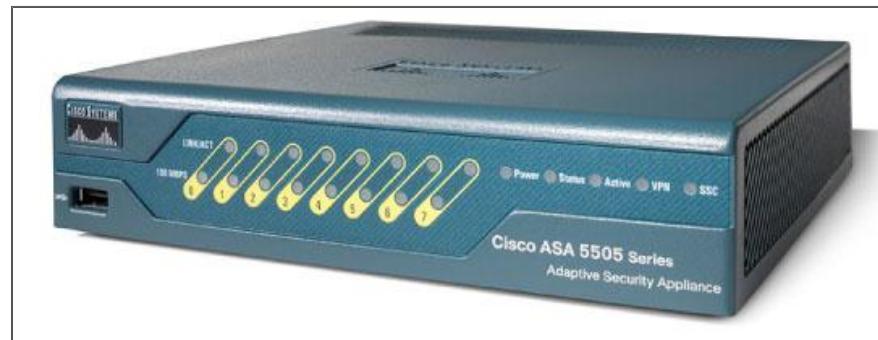
وهو Switch يمكنه ان يقوم بنفس وظائف الـ Router وجاء مسمى Multi-Layer لأنه يمكنه ان يعمل في Layer 2 الخاصة بالـ Router وأيضا Layer 3 الخاصة بالـ Switch



Firewall-17

- يستخدم للتحكم في استخدام الموظفين للـ Internet عن طريق إجراء وتطبيق بعض الـ Restricted Roles على كل الـ Service
- حتى نقوم بعمل Centralize الـ Users يمكن من خلاله منع بعض الـ Protocols من ان يتم استخدامها
- يمكن من ان يتم التعامل معها – بعض الـ Application Service and
- من ان يتم الاتصال بها Ports To Prevent Any Outside External Threats

Cisco ASA Firewall





من أهم الشركات في مجال الـ Firewall Devices هي شركة Fortinet

تعتبر هي المنافس الأقوى لكل من Cisco و Juniper في الـ Firewall Devices



IPS and IDS -18

Intrusion Prevention System – Intrusion Detection System



- من أهم أجهزة الحماية في اي Network
- عبارة عن أجهزة تعمل كـ Sensors حساسات في الشبكة
- أي اتصال غير مسموح به – أي Error – اي Packet حجمها اكبر من الطبيعي | يتم التعامل معها
- عن طريق Internal Database موجودة بداخلهم

الفرق بين الـ نوعين :-

- هو ان الـ IDS يقوم بعمل Alert فقط او عمل Detect لـ Error
- اما الـ IPS يقوم بعمل Action وهو عمل Drop لـ Packet او اي شيء آخر علي حسب الـ Configuration
- المقصود بها هنا :- Any Malicious Connection Error

This Page Intentionally Left Blank

Network Models

حضرتك الجهاز بتاعك بيكون شغال بـ OS معين ايا كان نوعه ايه ! من خالله ممكن تفتح Facebook او انك تعمل شات بينك وبين اي حد بيستخدم موبايل !

طب مسألتش نفسك ازاي الأجهزة المختلفة دي ممكن تتكلم مع بعض ؟؟ ايه هيا الفكرة اننا مش بيطبع عندنا Error ان الحاجات الكبير المختلفة دي Not Compatible مع بعضها ؟

من هنا جت فكرة الـ Network Models – انها تسمح لـ Service المختلفة انها تتكلم مع بعض – عن طريق بعض الـ Standard Roles بتكون ثابتة على كل الأجهزة أيا كان نوعها ايه

زي الـ Tour Guide اللي بيكون مع الفوج السياحي – لو مش فاهم كذا لغة مش هيعرف يتكلم مع كل الناس اللي موجودين

Models → To Allow Different OS – Devices – Services – Infrastructure to be Communicated

انواع الـ Network Models

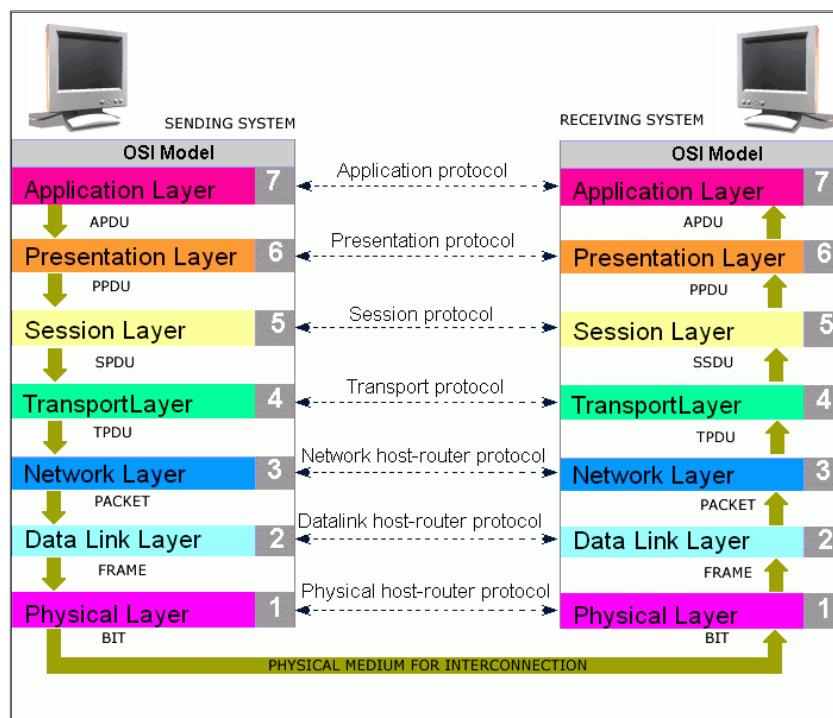
TCP/IP Model

OSI Model

• نبدأ نتكلم على ” OSI Model “Open System Interconnection – Intermediate ”

المنظمة اللي ابتكرته الـ ISO ”International Organization for Standardization“

عبارة عن 7 هما المسؤولين عن نقل الداتا من الـ source لـ Destination Layers



كل Layer مسؤولة عن عملية معينة في نقل الـ **date** او نقدر نقول انها بتقدم خدمة معينة بتسخدم في نقل الداتا وتسهيل عملية الـ communication اللي هتم بين الأجهزة

Receiving = Destination

Sending = Source

- Application Layer -1

دي الـ Layer المسئولة عن تقديم اي خدمة الـ User بحتاجها سواء كان انه يبعث Email لجهاز تاني او انه يعمل Download لأغنية عايزة يسمعها او انه يعمل Browsing لأي موقع زي الفيس مثلا

طب ايه هي الخدمات دي ؟؟

كل خدمة من الخدمات اللي بتقدمها الـ Application Layer بيكون ليها حاجة اسمها Port Number

الـ Port Number دا عبارة عن رقم ثابت للخدمة اللي انت بتعمل عليها Request – وبستخدمه علشان اعرف الـ Users اللي عندي في الـ Network ايه الخدمات اللي بيعملو ليها Access ولو عايزة امنع اي User من انه يعمل Service لأي Port Number – بقفل الـ Firewall وبالتالي بيحصل للـ Disable service او عن طريق الـ Access List – في كورس CCNA

Protocol	Stand for :-	Port	Feature
HTTP	Hypertext Transfer Protocol	80	المسئول عن خدمة الـ Browsing لأي موقع حضرتك بتعمل عليه Connect What is New ؟ ايا كان الموقع اللي حضرتك بتقتحه لازم يكون البروتوكول دا شغال حتى هنلاقي الموقع عندك بيكون دا شكل الـ URL بنطاعه http://www.google.com
HTTPS	Hypertext Transfer Protocol Secure	443	نفس الـ HTTP بس الفرق في الـ Security اللي يقدمها البروتوكول دا – في ان الداتا اللي بتتبعن بيحصل ليها عملية تشفير " TLS or SSL "
DNS	Domain Name System or Server or Service	53	من أهم البروتوكولات كل موقع حضرتك بت Connect انت بتعمل اتصال بإسم الموقع – بس الجهاز بتاع حضرتك ميرعش ايه هو الإسم دا هو يعرف حاجة اسمها الـ IP اللي هو العنوان بتاعه على الشبكة . بالإضافة لكدا ان اي موقع او اي جهاز بيكون ليه حاجة اسمها IP – حضرتك لما بتجي تتصل بأي شخص موجود عندك في الـ Phone Contact انت بتعمل Search علي الإسم بنطاعه وبعد كدا بتعمل Dial نفس الفكرة مع الموقع – علشان نعمل Connect علي اي موقع لازم تكون حافظ الـ IP بنطاعه – بس دا صعب جدا انه يتتحقق فالـ DNS بيقوم بالوظيفة دي بدل من حضرتك انه بيحول ليك من اسم الموقع اللي بتعمل Connectعليه --> للـ IP بنطاعه علشان تتم عملية الاتصال بنطاعك بكل سهولة

Network Fundamental

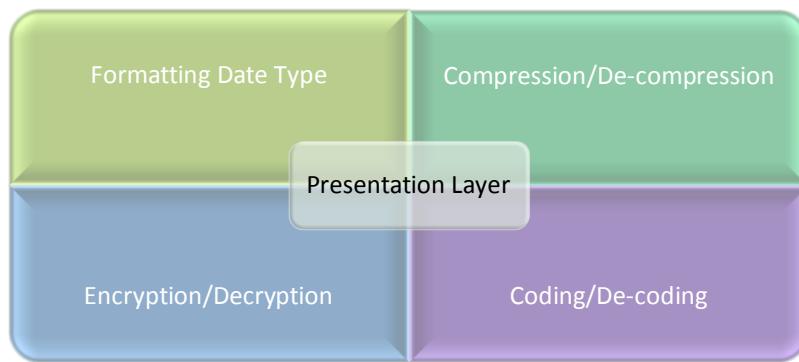
			Resolving from Name to IP والعكس
DHCP	Dynamic Host Configuration Protocol	67 - 68 (IP v4) 546 - 547 (IP v6)	مسئول انه يقوم بعملية Assign لـ TCP/IP Configuration Automatic يعني بدل ما تروح علي كل جهاز في الشركة اللي حضرتك فيها وتعطي الأجهزة الـ Network Configuration Static - لا الـ Protocol دا بيوفرلك طريقة Automatic # شرح بالقصيل في كتاب CCNAx
SMTP	Simple Mail Transfer Protocol	25	مسئول عن خدمة Email Sending يعني حضرتك لما بتبعث اي Mail لأي حد تاني يستخدم البروتوكول دا عشان تبعث بيه
POP2	Post Office Protocol Version 2	109	مسئول عن Receiving Mails المبعوتة من الـ Source Destination
POP3	Post Office Protocol Version 3	110	مسئول عن Receiving Mails المبعوتة من الـ POP2 Update
SNMP	Simple Network Management Protocol	161	مسئول عن عمليات الـ Analysis Monitor - برامج الـ Network علشان تقيس مدي الكفاءة بنطاقه الشبكة بتاعتكم ومسئول انه يكتشف اي خطأ ممكن يحصل واذا اي تعالجه من اشهر الشركات اللي بتقدم Apps في المجال بنطاع الـ Solarwind Monitoring شركة اسمها
FTP	File Transfer Protocol	20	يقدم خدمة الـ Uploading & Downloading اي كان الموقع اللي حضرتك بترفع عليه ملفاتك بتكون شغاله بالبروتوكول دا Source PN 20 مسئول عن انه Open Session بين الـ and Destination
FTP	File Transfer Protocol	21	PN 21 مسئول انه يعمل Start Uploading Process على الملفات اللي بتترفع Apply Security
TFTP	Trivial File Transfer Protocol	69	نفس الفكره بنطاقه FTP - بس كان فيه عيوب : انه بيستخدم مع الملفات اللي حجمها صغير بس وان مكنش فيه Security علشان كدا طوروه وعملوا FTP
Telnet	Remote terminal Access Protocol (unencrypted text communications)	23	يقوم لينا خدمة Remote Connection على الأجهزه سواء كانت Router - Switch - ...etc. المشكله الموجودة في البروتوكول دا ان الـ Username and Password بيتبعتو As Clear Text فباستخدام اي Hacking Connection ممكن اعمل تعقب لل Tool like Wireshark واعرف الـ User and Pass
SSH	Secure Shell (SSH)	22	نفس الـ Telnet بس عالج المشكل اللي كانت فيه انه بيقوم بعمل تشفير للبيانات المرسلة وكمان بيشفر الـ Username and

Network Fundamental

			Password
RTP	Real Time Transport Protocol	16384 - 32767	يستخدم مع ال VOIP Tech

كل دى حضرتك يستخدمها يوميا وانت مش واحد بالك هو ايه اللي بيحصل او حتى ازاي بيحصل دا كله
دي أهم ال Protocols اللي المفترض ان حضرتك تكون عارفها – مش كل ال Protocols تم تناولها
Q : ايه الفرق بين IMAP and POP3 ؟؟

-: Presentation Layer -2



Coding/De-coding -1
هي عملية تحويل اي داتا بتتبع بين الأجهزة الي 0 & 1 ودي اللغة اللي بتقهمها الـ Machine بتاعتك "Binary"
عشان الداتا تقدر توصل بين الأجهزة ايا كان نوعها
De-Coding → on Destination Machine Coding → on Source Machine
بعد ما بتتحول لـ لازم الـ Destination يرجع الـ User يقدر يفهم ايه المبعوت ليه

Encryption / Decryption -2
عليه تشفير الداتا اللي بتتبع بين الأجهزة – كنوع من انواع الـ Security اللي ممكن تضاف على الداتا
الـ Presentation Layer بتستخدم MD5 في عملية التشفير "Message Digit ver.5"
الـ Source بيقوم بعملية التشفير -- وعملية فك التشفير الحاصل على الداتا بيكون من مسؤولية Destination

Compression/De-compression -3
يحصل ضغط للداتا المرسلة بين الأجهزة عشان نقل حجمها وكمان نقل استهلاك الـ Bandwidth المستخدمة
سرعة نقل الداتا جوة الشبكة – على حسب الجهاز المترصل **Bandwidth →**

Formatting Data Type -4
اني ممكن اتحكم في طبيعة الداتا اللي بيعتها او بستقبلها Extensions زي اللي بيحصل لما بنجي نحمل فيديوهات من الـ YouTube

Session Layer -3

لو انت فاتح من الـ Browser بتابعك كذا Tab مثلا facebook – twitter – soundcloud على الـ Refresh على الـ Tab بتابعه الـ Facebook اي اللي هيظهرك في الـ Tab دي ؟؟ طبيعي هتقول الـ Time line for Facebook !! طب ازاي ؟؟

هي دي يقى وظيفة الـ Session Layer انها تتبع الداتا على حسب هيا ميعرفة من انهى Service علشان كدا ميحصلش اي نوع من انواع الـ Errors

دي اول وظيفة من وظائف الـ Session layer اللي هيa Control Sessions تاني حاجة من وظائفها – انها بتعمل Open Connection بين الـ Destination والـ Source وبعد الانتهاء عملية الاتصال بتعمل Close for Connection

الـ Service هي اول Layer بيحتك فيها الـ Users علشان من غير ما نعمل مفيش اي مفاصيل اساس .

Transport Layer -4

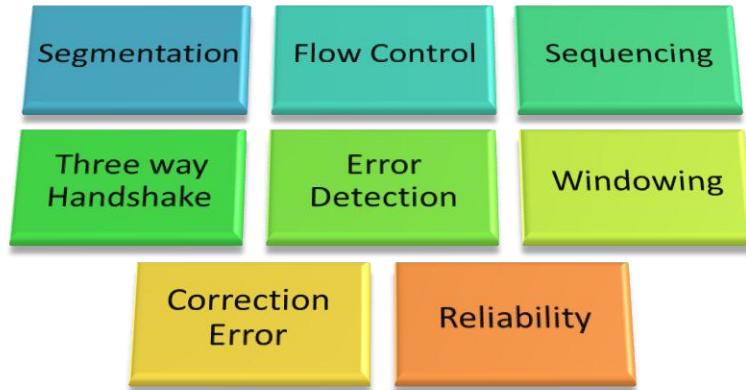
من اهم الـ Layers بل تعتبر هي الـ Backbone Layer اول الـ Data Three Layers بتكون فيها *as Data* يعني محصلش عليها اي Encapsulation اضافات تانية "Headers"

الـ Transport Layer هي اول Layer في عملية الـ Encapsulation لما انكلمنا في الـ Application Layer قولنا ان دي الـ Service اللي بنسخدمها – بس كل Service ليها نوع معين في الاستخدام هل بتعتمد على الـ Security وان الداتا توصل كاملة ولا بتعتمد على السرعة فقط

بيجي هنا مصطلحين مهمين او اي UDP TCP وهذا دول اللي بيحددو نوع الـ Service اللي بنسخدمها اول ما بنضيف نوع الـ Service على الـ Data بتتحول لـ Segment

"UDP "User Datagram Protocol	TCP " Transmission Control Protocol "
<p>يعتمد على السرعة فقط يتستخدم حاجة اسمها <i>Real Time</i> يعني اللي بيحصل عند الـ Destination Source بشوفه لحظيا زي اي Live Matches or Live Broadcasting</p> <p>لو بتفرج على ماتش اونلاين وحصل اي Error في الانترنت – هل لما النت بينضبط الماتش بيستوي عند الحنة اللي حصل فيها الـ Error ولا بيكمي عادي وبيسبب اللي فات ؟ ودي بتسخدم اكتر مع الـ Voice and Video Over IP</p>	<p>يتكون فيها الداتا بتعتمد على الـ Reliability والـ Security يعني انها توصل كاملة ولو حصل اي Error في عملية نقل الداتا بتعمل ليه Detect and Correct ويعمل كمان حاجة اسمها <i>Flow Control</i> يعني ان معدل النقل يكون مناسب لكل الأجهزة اللي بتتكلم مع بعض زي اي عملية اسمها <i>Connection</i> بنسخدمها كـ <i>Users</i> <i>Email Service –Uploading</i></p>

وظائف الـ Transport Layer

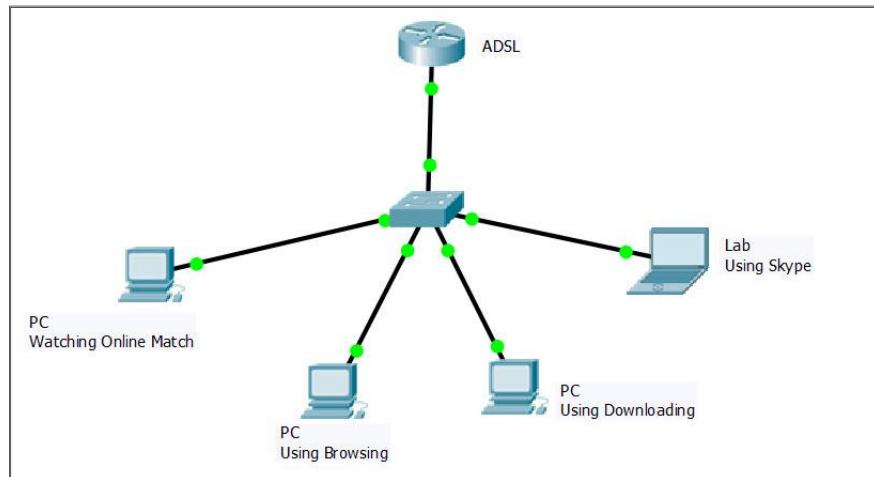


Segmentation -1

قولنا ان اسم الـ Data في الـ Transport Layer تكون Segment بيكون حجمها كبير بالنسبة لعملية Communication فعملية الـ Segmentation وظيفتها انها تقسم الـ Segment الكبيرة لمجموعة Segments صغيرة . طب ليه ؟

اولا : علشان تتبعت بسرعة
ثانيا : علشان لو حصل Error في جزء معين اعرف اعمل ليها Detect and Correct بسهولة بدل ما اعمل للـ Segment الكبيرة كلها

ثالثا : علشان لو عندي اكتر من Service



لو عندي اكتر من Service زي اللي موجودة بالشكل دا – هنلاقي في حاجات بتعتمد على TCP و بعضهم بيعتمدوا على الـ UDP

لو مثلا الجهاز اللي بيعمل Download دا هو اول جهاز بعث الـ Request هيسحب الـ Traffic كله – وبالتالي اللي بيستخدم او Online Service او Skype مش هيستخدم الـ Real Time Feature بتاعه الـ Data علشان كدا بيحصل عملية Segmentation علشان يحصل Mix بين الـ Segments وتحقق كل شروط نقل الـ

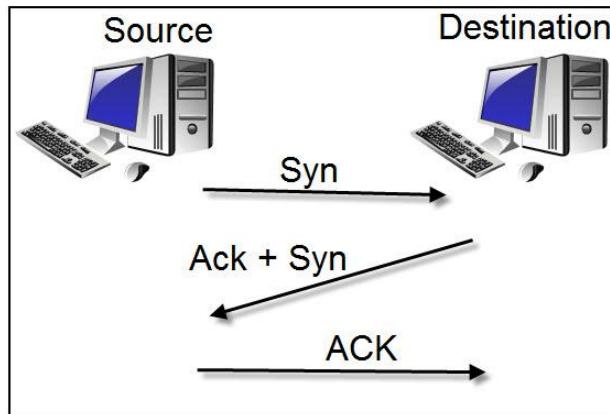
Sequencing -2

وهي عملية ترقيم لـ Data اللي اتجزأت علشان الـ Destination يبقى عارف هو استلم قد ايه ولسه فاضل قد ايه ؟

Three Way Handshake -3

Network Fundamental

يتستخدم لغرض انها تعمل Test لا Source Connection بين الـ Destination عن طريق ارسال Source and Acknowledge message

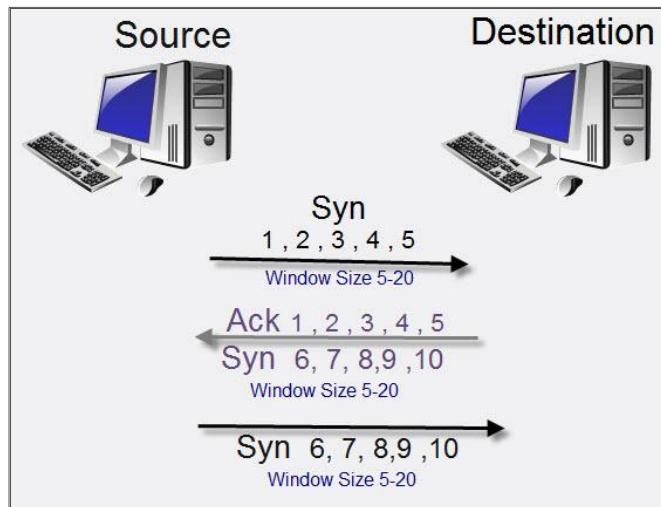


الـ Source بيعت للـ Destination علشان يتلقوا على عدد الـ Segments اللي هتبعدت ف كل مرة - الـ Source Msg بيكون اسمها Acknowledgement Msg ، ولو الـ Destination متاح واسلم الـ Segments دي بيرد على الـ Source بـ الـ Synchronous وبيطلب منه باقي الـ Segment الباقية

لو عندي Segment حجمها 150 Byte وحصلها Segmentation وبقي كل Segment حجمها 10 Byte

يعني دا معناه ان هيكون عندي 15 جزء هيتبعدوا - الـ Source بيحدد عدد عشوائي من الـ Segments على حسب الـ Process بتاعته وبيجيها للـ Destination وبيكون عندي كذا حالة في الموضوع دا :-

-: Case 1



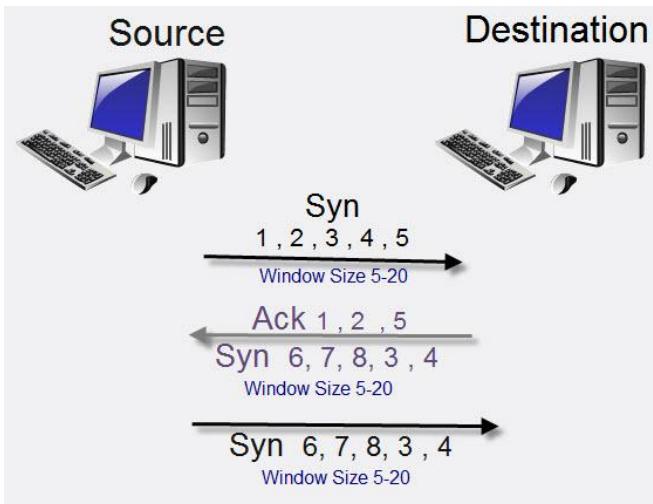
ان الـ Source هيحدد انه هيبيت 5 Segment في المرة ودي بيكون اسمها الـ Window Size اللي هي عدد الـ Segments المبعونة في المرة الواحدة من العدد الاجمالي

لو الـ Destination استلمهم كلهم هيبيت يقوله انه Ack وتمام وابعد الـ 5 اللي بعدهم وهكذا

الـ Source بيعرف ان الـ Segments كلها وصلت من الـ Value بتاعه الـ Window Size

وبعد كدا تبدأ عملية الـ *Windowing* :-
الـ Windowing هي عملية بداية الإتصال الفعلي بينهم

Network Fundamental



-: Case 2

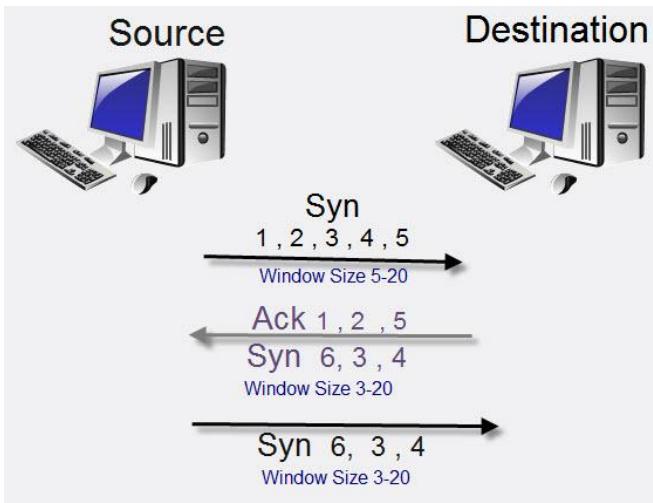
نفس طريقة الـ Source انه يحدد عدد عشوائي ويبعدt على اساسه ، ولكن هنا حصل عن لـ Destination Error في الـ Segments 3 , 4

نتيجة لأي مشكلة في الـ Internet مثل

بس حجم الـ Window Size فضل ثابت زي ما هو والـ Destination بعثت له Source قاله ايه اللي استلمه وايه اللي لسه فاضل ليه

المسؤول عن اكتشاف وتصحيح الـ Errors هي الـ CRC

Error Detect وظيفتها انها بتعمل Cyclic Redundancy Check لو حصلوا على الـ Segments او and Error Correct المسئولة بين الأجهزة المستلمة



-: Case 3

نفس طريقة الـ Source انه يحدد عدد عشوائي ويبعدt على اساسه ، ولكن هنا حصل عن لـ Destination Error في الـ Segments 3 , 4

ولكن الـ Error اللي حاصل هنا في مشكلة عند الـ Destination علشان حصل عنده Over Flow

معناه :- ان سرعة نقل الـ Date من الـ Source من الـ Destination اكبر من معدل استيعاب الـ Destination للداتا المعبوطة

وبالتالي الـ Destination هيطلب من الـ Source انه يعدل الـ Window Size على حسب مقدار استيعابه

الـ Destination ي يعمل حاجة اسمها Flow Control انه هيتتحكم في معدل ارسال الداتا اللي بتجيشه من الـ Source

ودي الـ Case الوحيدة اللي بتتغير فيها الـ Window Size وبرضه المسئولة عنها هي الـ CRC

بعد كدا ايا كان الـ Case اللي حاصلة - كل دا بيتم في عملية Test for Connection

عملية بداية الـ Connection الفعلي اسمها Windowing

وبكدا تكون خلصنا كل وظائف الـ Transport Layer

تاني Layer بتصيف IP Address وتحول الـ Data -- بتضيف الـ Segment على الـ IP Address هو عنوان الجهاز على الشبكة او عنوان الموقع اللي انا عايز اعمل عليه Connect - هنكلم عنه بالقصيل في الشابير الخاص بيه

-: Network Layer

Routing Protocols

وظيفه الـ Routing Protocols انها تحدد افضل مسار في عملية نقل الداتا بين الأجهزة

Define the Best Path - Route- Way to Send Data

وكمان وظيفتها انها تخلي الشبكات المختلفة تقدر تتكلم مع بعض علشان الرووتر بيقدر يفهم اكتر من شبكة

Type of Routing Protocols :-

RIP
OSPF
EIGRP
BGP

هنكلم عنهم بالقصيل في Routing Track

Routed Protocols

مسؤولة عن عملية الـ Addressing يعني ازاي الجهاز بيأخذ IP بإختلاف الـ OS بتاعه

Other Protocols

ARP

وظيفته انه بيجيب الـ IP بدلالة الـ MAC Address والـ RARP يقوم بالوظيفة العكسية ،

ICMP

وظيفته انه يعمل للـ Test ويسوف الـ Connection مناخ لا Destination وممكن كمان نستخدمه علشان نشوف الانترنت شغال ولا لا عن طريق اتنا بنعمل ping sitename حسب الـ Responce بنشوف ايه الوضع
1- Request time out
2- Destination host unreachabile
3- Reply from

[Data Link Layer](#) -6

Network Fundamental

يتحول الـ Frame عن طريق انها بتضيق الـ MAC Address بناء الاجهزة

ايه هو الـ MAC ؟
الـ Physical Address اللي يكون محفور على الـ NIC بناء الجهاز حضرتك ، مينفعش الـ MAC بتكرر على الأجهزة
وبتالي هو Unique ، بيكون من 48 bit يعني 6 Byte
مكتوب بلغة اسمها Hexa Decimal يعني بيكتب بالارقام والحروف
علشان تعرف الـ MAC بناء جهازك - على الـ CMD هتكتب امر اسمه ipconfig /all

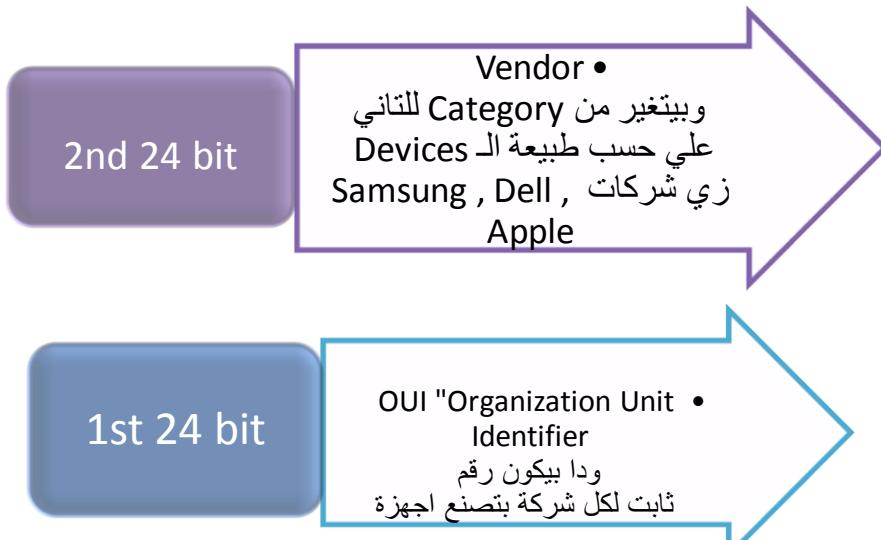
```
C:\Windows\system32\cmd.exe
C:\Users\...>ipconfig /all
Windows IP Configuration

Host Name . . . . . : [REDACTED]
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Wireless Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Broadcom 802.11n Network Adapter
Physical Address. . . . . : 88-9F-FA-85-A0-18
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device <Personal Area Network>
Physical Address. . . . . : 1C-65-9D-F6-8E-65
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

الـ MAC Address بيتقسم لجزئين



وظائف الـ Data Link Layer

-: Arbitration -1

انها كانت بتحدد ايه هو افضل وقت في عملية ارسال الداتا . وكانت اهميتها في الـ Bus and Ring Topologies

Define the Best Time for Sending Data

Error Detection -2

-: Parity Check

بحسب عدد الـ Bits اللي بتساوي 1 في الداتا المرسلة

لديها Two Algorithms شغالة بيهم :-

Even or Odd

لو انا يستخدم الـ Odd لازم عدد الـ Bits بتاعه الـ 1 يكون عدد فردي

لو هستخدم الـ Even لازم عدد الـ Bits بتاعه الـ 1 يكون عدد زوجي

ممكن يحصل Error في عدد الـ Bits بتاعه الـ 1 وبالتالي هيكون في ناتج تبع نفس الـ algorithm بس مش هنعرف

نعمل ليه Detect بسهولة

ومعديش يستخدم

-: CRC with FCS

الـ CRC في الـ Data Link Layer بتعمل Error Detect Only يعني لو حصل

الـ User Error هيسلمه عادي علشان حصل بعد الـ Transport Layer

الـ FCS بتشتعل مع الـ CRC ليها نفس الطريقة بس الاختلاف انها بتصرف في الـ Header Tailer بتاع الـ

Data Link Sub Layers



Physical Layer -7

يتبعه Coding الـ Destination Medium وبتحوله لـ 0/1 علشان يتبع في الـ Header

وبيشتغل فيها اي أجهزة Not Smart وايضا الـ Cables

وهنتكلم عن الـ Cables ببساطة في شابتر منفصل

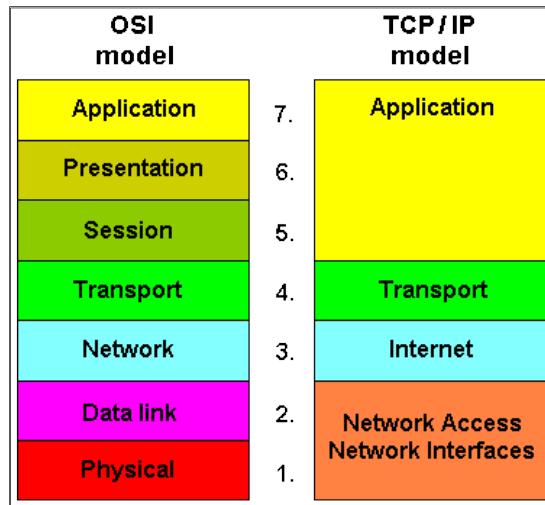
This Page Intentionally Left Blank

TCP/IP Model

المنظمة اللي ابتكرت الـ Model دا هي الـ DOD “Department of Defense”

علشان يكون اسرع من الـ OSI في عملية نقل الداتا – وكمان يكون كـ Backup ليه علشان لو حصل فيه اي مشاكل يكون في ثابت لنقل الداتا Standard

وتم اعتماده كنظام ثابت لكل الأجهزة



عبارة عن 4 ليهم نفس الوظائف بتاعه الـ OSI بس الفكره ان الـ Process علي الداتا بقى اسرع
حصل دمج في بعض الـ Layers وتغيير في بعض اسماء Layers اخري

Application, Presentation and Session → Application

Network → Internet

Data link and Physical → Network Access or Network
Interfaces

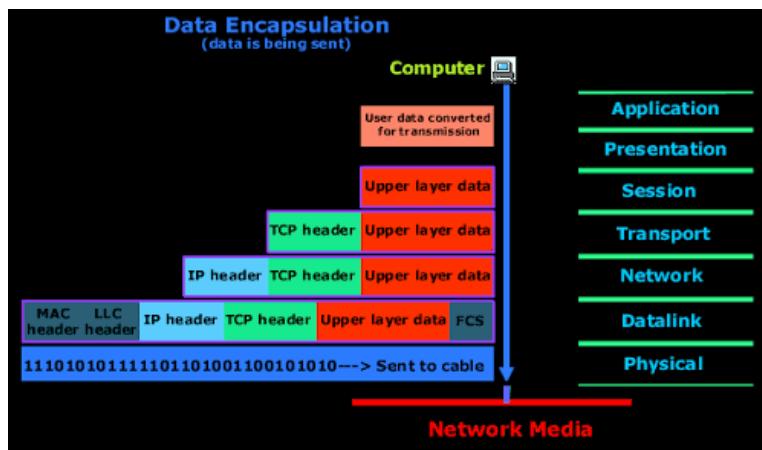
Encapsulation Techniques in Models:-

Encapsulation		
OSI Layer	Wrapper Name	Header Name
Application	N/A	Layer 7 Header
Presentation	N/A	Layer 6 Header
Session	N/A	Layer 5 Header
Transport	Segment	TCP Header UDP Header
Network	Packet	IPv4 Header IPv6 Header
Data Link	Frame	Ethernet Type II Header IEEE 802.2 802.3 802.3 SNAP Other Frame Headers
Physical	Bits	N/A

- ببتدأ تحصل من اول الـ Transport Layer انها بتضيف نوع الـ Service اللي الـ User بيستخدمها وبيتحول الـ Data لـ Segment
- بعد كدا بتجي وظيفة الـ Network Layer انها بتضيف الـ IP Addresses والـ Routing and Routed علشان الداتا تتبع في المسار الصحيح بتاعها وميحصلش ليها اي Failures ، وبيتحول الـ Segment لـ Packet
- الـ Data Link Layer بتضيف الـ MAC Address وكمان بتضيف الـ Header FCS في الـ Tailer علشان الداتا يحصل ليها تغليف من الناحيتين وبيتحول الـ Frame لـ Packet
- الـ Physical Layer بتعمل عملية Coding لكل الأجزاء دي اللي بتسمى الـ Header وبيتحولها لـ 0/1 علشان تمشي في الـ Cables

عملية الـ Coding بتحصل مرتبة في عملية نقل الداتا :-

مرة في الـ Physical وتحصل على الـ Data فقط – ومرة تانية بتحصل في الـ Presentation Layer وبتتم على الـ Header كل



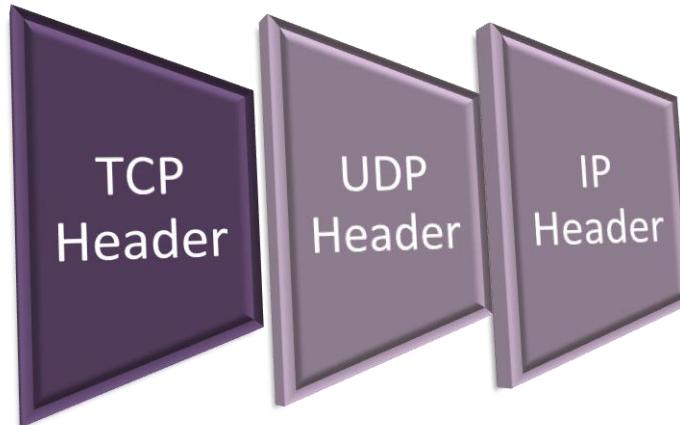
Network Devices with its Layers

Device	Layer
Hub , Connector , Repeater , Cables	Physical Layer
Switch , Bridge , Access Point , NIC	Data Link Layer
Router , Multi-Layer Switch	Network Layer
IPS , IDS	Presentation Layer
Firewall	Filter All Traffics in All Layer
Server	It's about the Service type that Provide

This Page Intentionally Left Blank

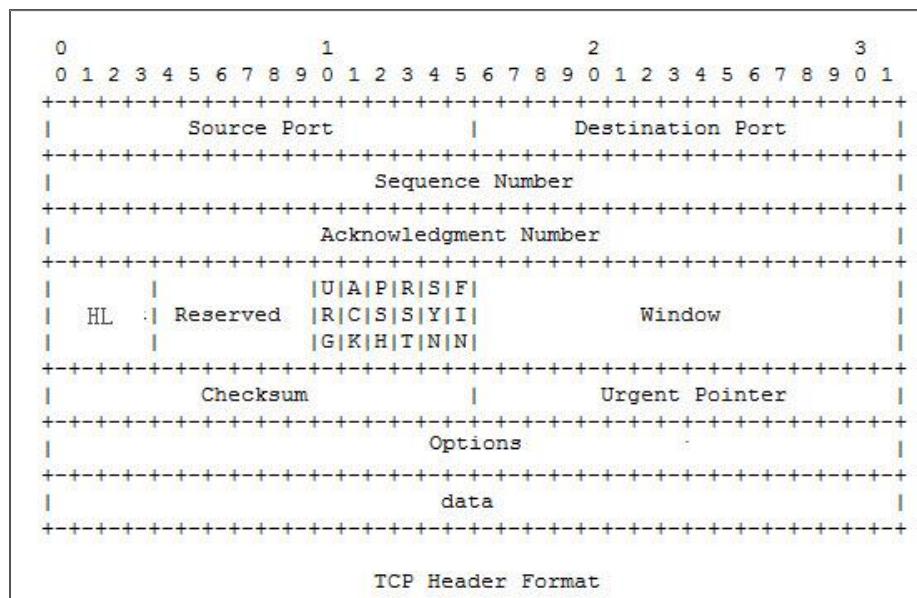
Headers

اتكلمنا في الـ Models على ان بتحصل عملية Encapsulation على الـ Data
ان بيحصل Add Layer بتاع الـ Service اللي بنستخدمها علشان تغلف الداتا وتحولها لاسمها في الـ Header بتاعتتها



TCP Header

- ❖ بيستخدم مع الـ Data اللي بتعتمد على الـ Security and Reliability
- ❖ الحجم الإجمالي بتاعه 20 Byte
- ❖ بيقسم لـ 5 Byte العرض بتاعه - والطول 32 bit



-: Source and Destination Port

الـ Port زي ما اتكلمنا عنه قبل كدا قولنا انه عبارة عن مدخل او مخرج الـ User لـ Service اللي هو عايز يعمل ليها لازم لـ User يكون ليه Port Number يخرج منه

عدد الـ Ports الإجمالي 65535

بتنقسم لجزئين :-

0 : 1023 و دا بيكون بتاع الـ Application Layer اللي اتكلمنا علي جزء منهم في الـ Online , Public , Reserved Service

الباقي بتوع الـ Users -- حجم كل جزء منهم بيكون 16 Bit

-: Sequence Number

مسئولي عن عملية الترقيم اللي بتتم علي الـ Segments اللي بيحصل ليها علشان الـ Destination بيقي عارف استلم قد ايه و فاضل قد ايه -- حجمها 32 Bit

-: Acknowledgement

بتعمل Check علي ان الـ Segments كلها , هل وصلت لـ User كاملة ولا ؟

-: Header Length

قيمة ثابتة وبيتحدد فيها ان حجم الـ Header ثابت انه 20 Byte

-: Reserved

جزء محجوز لأي Update ممكن يتضاد على الـ Header في الـ Future Use

-: TCP Flags

بستخدمهم علشان اعمل Test لـ Connection بين الـ Source و الـ Destination - بس ليهم كذا نوع وكل نوع ليه خدمة معينة بيقسمها

الـ Default Value بتاعة كل Flag منهم انها بتتساوي 0 حتى يتم استخدامها

بالنسبة لـ PSH – RST – URG إستخدامها أكثر في عمليات الـ Hacking وفي شابير كامل في كورس C/EH بيتكلم عنهم وازاي استخدموهم

في برامح بتخليني اقدر اتحكم في نوع الـ Flags اللي عايز استخدمه زي : NMAP

Flag Name	Service
Synchronous “ SYN ”	دا اللي الـ Source بيعته للـ Destination علشان بيبدأ معاه عملية الـ Connection
Acknowledgement “ ACK ”	الرد بتاع الـ Destination على الـ SYN بتاعة الـ Source
Push “ PSH ”	بستخدمه في حالة لو انا عايز ابعث كل الـ Segments بتاعتي مرة واحدة بغض النظر عن الـ Window Size المتفق عليه بينهم علشان اعمل عند الـ Destination حاجه اسمها Over Flow
Urgent “ URG ”	بستخدم في حالة ان عندي محدد عايز ابعتها دلوقت ومش عايز اخليها تستني في الـ Queue بتاع الـ Segments
Reset “ RST ”	فایدته اني اعمل Reset للـ Connection إجاري عند الـ Destination
Finish “ FIN ”	لو خلاص كل الـ Segments ابتعنت وتم استلامها ومعتش في اي غرض تاني من الـ Connection كل واحد منهم بيقول الـ Connection وبنته هي عملية الاتصال

-: Window Size

دي اللي بتحدد فيها حجم الـ Header بالإضافة الي حجم الداتا المرسلة ، الـ Data ملهاش حجم معين و هيا مش جزء من الـ 20 Byte بتوع الـ Header .

المسؤول عن عمل Detect لحجم الـ Data المرسلة هو الجزء بتاع الـ Window Size

-: Check Sum

و دي المسؤولة عن عملية الـ Error Detection and Correction اللي بتشتغل فيها الـ CRC

-: Urgent Pointer

لو حصل اي Error في اي جزء من أجزاء الـ Header ، هي بتحل محله في الشغل ، الحجم بتاعها 16 Bit وبالتالي لو حصل اي Error في جزء حجمه اكتر من حجم الـ urgent Pointer هتعتبر الـ Segment دي مرفوضة والـ Destination هيطلبها من الـ Source تاني

-: Option

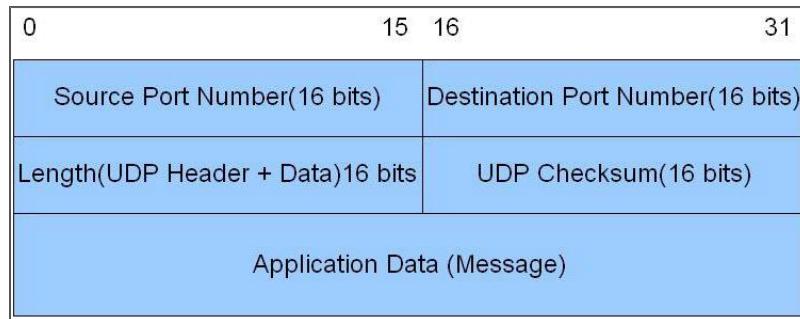
دي بتخص اي OS – Vendor – Infrastructure كل واحد منهم ليه Option مختلف عن الثاني فلازم يحصل ليها Add في الـ Header

-: Data

ودي الداتا المرسلة – ملهاش اي حجم ثابت في الـ Header بس زي ما وضحتنا المسؤول عن اضافة حجمها في الـ Header هو الـ *Window Size*

UDP Header

- ❖ يستخدم مع الـ Data اللي بتعتمد على السرعة وشرط ارسالها هو الـ Real Time
- ❖ حجم الـ Header اجمالاً 8 Byte ، العرض 2 Bit 32 والطول 2 Byte
- ❖ واللي واضح من الـ Diagram بتاعه ان في اجزاء كتير كانت في الـ TCP Header مش موجودة فيه علشان هو ملوش اي علاقه باي Security او حتى ان الداتا توصل كاملة او لا .



-: Source and Destination Port

نفس الكلام اللي قولناه في الـ TCP Header

-: Length

هنا مختلفة عن الـ TCP ، اللي بيساويها هناك هو الـ Window Size لأنها هنا بتحدد حجم الـ Header بالإضافة لحجم الـ Data المرسلة

-: UDP Checksum

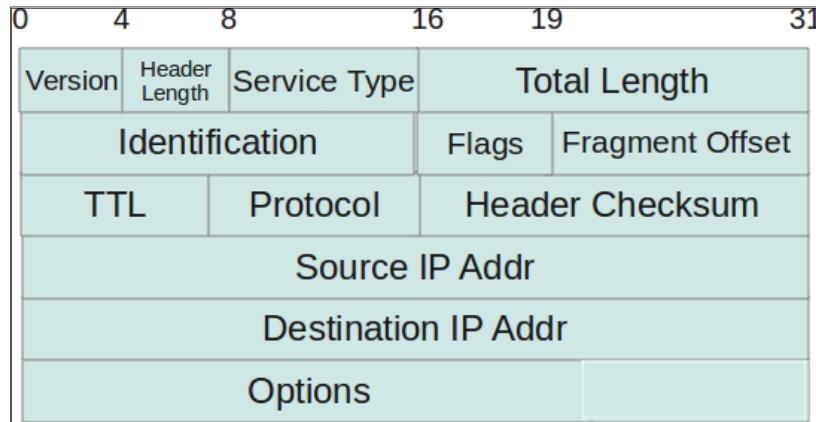
مسؤوله عن عمل Correction Only Detect Error علشان تعرف الـ Destination ان حصل Error بس مبيحصلش ليه اي عملية إطلاقاً ، وبرضه المسؤول عنها هي الـ CRC

-: Data

ودي الداتا المرسلة - ملهاش اي حجم ثابت في الـ Header بس زي ما وضحنا المسؤول عن اضافة حجمها في الـ Header هنا هو الـ Header Length

IP Header

دا اللي بيتضاف على الـ Segment علشان يحولها لـ Packet -- الحجم بتاعه نفس حجم الـ TCP Header



-: Version

بتحدد هل الـ IP المستخدم دا IPv4 or IPv6

-: Header Length

بتعمل Detect لحجم الـ Header فقط اللي هو 20 Byte

-: " TOS " Type of Service

نوع الـ Service اللي هتنقل باستخدام الـ IP وبتحدد الـ QoS Quality of Service وكمان بتحدد ازاي الـ Router هيتعامل مع الداتا اللي جياله , هل هيبيعتها على طول ولا هتسنني في الـ Queue

ليها مصطلح تاني اسمه IP Differentiated Services Code Point (DSCP)

ToS Value	ToS Description
0 (000)	Routine
1 (001)	Priority
2 (010)	Immediate
3 (011)	Flash
4 (100)	Flash Override
5 (101)	CRITIC/ECP
6 (110)	Internet Control
7 (111)	Network Control

-: Total Length

ودي بتحدد حجم الـ Segment بالإضافة لحجم الـ Header المضافة ليه من الـ Transport Layer

-: Identification

قبل ما نتطرق ليها – في مصطلح اسمه MTU *Maximum Transmission Unit* ودا بيحدد ايه هو اقصى حجم للـ Packet ممكن تمر من الـ Interface او الـ Device – قيميتها انها تكون **1500 Byte by Default**

لو حصل والـ User بعث حجمها اكبر من الـ MTU المفروض انه هيعمل ليها Reject !! لا طبعا !!

الـ Router هيعمل ليها حاجة اسمها *Fragmentation* يعني هيجزئها – ويعطي لكل جزء ID علشان عملية الترقيم ليهم وهيجمع كل مجموعة Fragments مع بعضها بحاجة اسمها Flag

علشان تقدر تمر منه وتوصلك الـ Destination -- وبكدا نكون اتكلمنا عن الـ Fragment Offset – Identification – Flags

-: TTL

فترة حياة الـ Packet اللي هتفضل تلف فيه وتدور على الـ Destination بقىها او يحصل ليها Drop – الـ Packet مش هتفضل تلف كدا في الفاضي في الشبكة علشان ميحصلش Loop

TTL Default Value	Why
64	في حالة لو انت بتعمل Ping على أي Online Site وفي الحالة دي الناتج اللي بيكون موجود الفرق بينه وبين 64 هو عدد الـ Hops اللي عدت عليهم
128	في حالة لو انت بتعمل Ping على جهاز شغال معاك على نفس الـ LAN بقىها
256	لو انت بتعمل Ping على الـ Gateway او على Router

```
C:\>ping www.cisco.com
Pinging e144.dsrb.akamaiedge.net [23.218.240.170] with 32 bytes of data:
Reply from 23.218.240.170: bytes=32 time=40ms TTL=60
Reply from 23.218.240.170: bytes=32 time=37ms TTL=60
Reply from 23.218.240.170: bytes=32 time=38ms TTL=60
Reply from 23.218.240.170: bytes=32 time=38ms TTL=60

Ping statistics for 23.218.240.170:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 37ms, Maximum = 40ms, Average = 38ms
```

في حالة لو انت بتعمل Ping على جهاز شغال معاك على نفس الـ LAN بقىها

```
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data
Reply from 192.168.1.1: bytes=32 time=3ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254
Reply from 192.168.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Network Fundamental

لو انا عايز اشوف اي هيا الـ Hops اللي عدت عليهم الـ Packets اللي بتعمل توصيل لك Destination Packets يستخدم بروتوكول من ضمن الـ Network Layer Protocols اسمه tracert المبعوثة Packets

الفرق بين قيمة الـ TTL والقيمة الـ Default بتعملها - هي عدد الـ Hops اللي عدت عليها الـ Packet علشان توصل لك Destination بتعملها

```
C:\>tracert www.cisco.com
Tracing route to e144.dsrb.akamaiedge.net [23.218.240.170]
over a maximum of 30 hops:
  1      1 ms      <1 ms      <1 ms    192.168.1.1
  2     48 ms      51 ms      42 ms    172.31.1.200
  3     34 ms      31 ms      32 ms    172.21.29.181
  4     39 ms      38 ms      39 ms    172.21.16.222
  5     39 ms      38 ms      39 ms  a23-218-240-170.deploy.static.akamaitechnologies
.com [23.218.240.170]
Trace complete.
```

-: Protocols

نوع الـ Protocol المنقول بإستخدام الـ Header في آخر الشابتر هيكون في توضيح لكل الـ Protocols المستخدمة وايه هي الـ Values بتعملها

-: Header Checksum

مسئولة عن عمل Error Detect Only لو حصل في اي Packet

-: Source and Destination IP

عناوين الأجهزة اللي بتعمل Connect مع بعضها علشان الـ Packet تبقى عارفه هيأ راحة من مين لفين

-: Options

لو في اي اضافة هتحصل على الـ Header دا - نفس الكلام الذي تم ذكره في الـ TCP Header

IP Header “TOS” - for Read only

Value	Protocol	References
0	HOPOPT, IPv6 Hop-by-Hop Option.	RFC 2460
1	ICMP , Internet Control Message Protocol.	RFC 792
	IGAP , IGMP for user Authentication Protocol.	
2	IGMP , Internet Group Management Protocol.	RFC 1112
	RGMP , Router-port Group Management Protocol.	
3	GGP , Gateway to Gateway Protocol.	RFC 823
4	IP in IP encapsulation .	RFC 2003
5	ST , Internet Stream Protocol.	RFC 1190, RFC 1819
6	TCP , Transmission Control Protocol.	RFC 793
7	UCL, CBT .	
8	EGP , Exterior Gateway Protocol.	RFC 888
9	IGRP , Interior Gateway Routing Protocol.	
10	BBN RCC Monitoring.	
11	NVP , Network Voice Protocol.	RFC 741
12	PUP.	
13	ARGUS.	
14	EMCON, Emission Control Protocol.	
15	XNET, Cross Net Debugger .	IEN 158
16	Chaos.	
17	UDP , User Datagram Protocol.	RFC 768
18	TMux , Transport Multiplexing Protocol.	IEN 90
19	DCN Measurement Subsystems.	
20	HMP , Host Monitoring Protocol.	RFC 869
21	Packet Radio Measurement.	
22	XEROX NS IDP.	
23	Trunk-1.	
24	Trunk-2.	
25	Leaf-1.	
26	Leaf-2.	
27	RDP , Reliable Data Protocol.	RFC 908
28	IRTP , Internet Reliable Transaction Protocol.	RFC 938
29	ISO Transport Protocol Class 4.	RFC 905
30	NETBLT , Network Block Transfer.	
31	MFE Network Services Protocol.	

Network Fundamental

32	MERIT Internodal Protocol.	
33	DCCP , Datagram Congestion Control Protocol.	
34	Third Party Connect Protocol.	
35	IDPR , Inter-Domain Policy Routing Protocol.	
36	XTP , Xpress Transfer Protocol.	
37	Datagram Delivery Protocol.	
38	IDPR , Control Message Transport Protocol.	
39	TP++ Transport Protocol.	
40	IL Transport Protocol.	
41	IPv6 over IPv4.	RFC 2473
42	SDRP , Source Demand Routing Protocol.	
43	IPv6 Routing header.	
44	IPv6 Fragment header.	
45	IDRP, Inter-Domain Routing Protocol.	
46	RSVP , Reservation Protocol.	
47	GRE , General Routing Encapsulation.	
48	DSR , Dynamic Source Routing Protocol.	
49	BNA.	
50	ESP , Encapsulating Security Payload.	
51	AH , Authentication Header.	
52	I-NLSP, Integrated Net Layer Security TUBA.	
53	SWIPE, IP with Encryption.	
54	NARP , NBMA Address Resolution Protocol.	
55	Minimal Encapsulation Protocol .	
56	TLSP, Transport Layer Security Protocol using Kryptonet key management.	
57	SKIP.	
58	ICMPv6 , Internet Control Message Protocol for IPv6. MLD , Multicast Listener Discovery.	
59	IPv6 No Next Header.	
60	IPv6 Destination Options.	
61	Any host internal protocol.	
62	CFTP.	
63	Any local network.	
64	SATNET and Backroom EXPAK.	
65	Kryptolan.	
66	MIT Remote Virtual Disk Protocol.	
67	Internet Pluribus Packet Core.	

Network Fundamental

68	Any distributed file system.
69	SATNET Monitoring.
70	VISA Protocol.
71	Internet Packet Core Utility.
72	Computer Protocol Network Executive.
73	Computer Protocol Heart Beat.
74	Wang Span Network.
75	Packet Video Protocol.
76	Backroom SATNET Monitoring.
77	SUN ND PROTOCOL-Temporary.
78	WIDEBAND Monitoring.
79	WIDEBAND EXPAK.
80	ISO-IP .
81	VMTP , Versatile Message Transaction Protocol.
82	SECURE-VMTP
83	VINES.
84	TTP.
85	NSFNET-IGP.
86	Dissimilar Gateway Protocol.
87	TCF.
88	EIGRP.
89	OSPF , Open Shortest Path First Routing Protocol. MOSPF , Multicast Open Shortest Path First.
90	Sprite RPC Protocol.
91	Locus Address Resolution Protocol.
92	MTP , Multicast Transport Protocol.
93	AX.25 .
94	IP-within-IP Encapsulation Protocol.
95	Mobile Internetworking Control Protocol.
96	Semaphore Communications Sec. Pro.
97	EtherIP .
98	Encapsulation Header.
99	Any private encryption scheme.
100	GMTP.
101	IFMP , Ipsilon Flow Management Protocol.
102	PNNI over IP.
103	PIM , Protocol Independent Multicast.

Network Fundamental

104	ARIS.	
105	SCPS.	
106	QNX.	
107	Active Networks.	
108	IPPCP , IP Payload Compression Protocol.	RFC 2393
109	SNP, Sitara Networks Protocol.	
110	Compaq Peer Protocol.	
111	IPX in IP.	
112	VRRP , Virtual Router Redundancy Protocol.	RFC 3768, RFC 5798
113	PGM , Pragmatic General Multicast.	
114	any 0-hop protocol.	
115	L2TP , Level 2 Tunneling Protocol.	RFC 3931
116	DDX, D-II Data Exchange.	
117	IATP, Interactive Agent Transfer Protocol.	
118	ST, Schedule Transfer.	
119	SRP, SpectraLink Radio Protocol.	
120	UTI.	
121	SMP, Simple Message Protocol.	
122	SM.	
123	PTP , Performance Transparency Protocol.	
124	ISIS over IPv4.	
125	FIRE.	
126	CRTP, Combat Radio Transport Protocol.	
127	CRUDP, Combat Radio User Datagram.	
128	SSCOPMCE.	
129	IPLT.	
130	SPS, Secure Packet Shield.	
131	PIPE, Private IP Encapsulation within IP.	
132	SCTP , Stream Control Transmission Protocol.	
133	Fibre Channel.	RFC 6172
134	RSVP-E2E-IGNORE .	RFC 3175
135	Mobility Header .	RFC 3775
136	UDP-Lite, Lightweight User Datagram Protocol.	RFC 3828
137	MPLS in IP.	RFC 4023
138	MANET protocols.	RFC 5498
139	HIP , Host Identity Protocol.	RFC 5201

Network Fundamental

140	Shim6 , Level 3 Multihoming Shim Protocol for IPv6.	RFC 5533
141	WESP, Wrapped Encapsulating Security Payload.	RFC 5840
142	ROHC , RObust Header Compression.	RFC 5858
143 - 252		
253 254	Experimentation and testing.	
255	reserved.	

This Page Intentionally Left Blank

IPv4 Address

- الـ IP Address هو عنوان الجهاز على الشبكة اللي هو متصل بيه - لازم كل جهاز يكون ليه IP علشان يقدر يتواصل مع اي جهاز تاني علشان دا العنوان بتاعه - بيكتب بلغة الـ " 0 to 9 " Decimal
- الـ IP Address بيكتب علي شكل 4 مقاطع - المقاطع الواحد بيسمي Octet ويفصل بين كل Octet والثاني بـ '.'

100.90.55.10

- الـ IP Address كما ذكرنا في الـ Header ان العرض بتاعه 32 Bit ويتكون من 4 Octet يعني دا معناه ان الـ Octet الواحد بيكون من 8 Bit
- يعني اي رقم بتكتب في اي Octet بيتمثل بـ 8 Bit - اللي هي لغة الـ Binary ودي اللغة اللي بيفهمها الـ Machine

طب ازاي الرقم الـ Decimal بتحول لـ ?? Binary

- احنا عندنا الـ Bit الواحد ليها احتمالين يا إما 0 يا أما 1 - فدایما الأساس بتاعنا هو احتمالين يعني 2 - وهما 8 Bit

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

- يعني احنا كدا عندنا لو جمعنا كل قيم الـ 2 هتديننا 255 ودا اقصي رقم ممكن اكتبه في الـ Octet وأقل رقم هو 0

✓ في طرق كتير للتحويل - بس انا استخدم طريقة الطرح زي ما هووضحها كالتالي :-

لو قولنا عايزين نحول رقم زي 100 مثلا :-

هل الـ 100 اكبر ولا اصغر من 128 ؟ اصغر منها وبالتالي مش هستخدمنها ، نشوف 64 هنلاقيها اكتر منها هنطرحهم من بعض الناتج هيكون 36 وبكدا استخدمنا الـ Bit دي

نشوف اللي بعدها هل 36 اكبر من 32 ؟ اها اكتر هنطرحهم من بعض والناتج هيكون 4 وهنلاقى ان الباقي كله مش هسيستخدم الا رقم 4 فقط

ودا الناتج الإجمالي 100 → 01100100

نشوف مثلا رقم زي 211

نشوفهم Bit by Bit زي الطريقة اللي فاتت بالضبط

اكبر من الرقم هنسخدم الـ Bit بقائه لو اقل منش هستخدمنها وحط مكانها 0

اكبر من 211 فهنسخدمها ونشوف الباقي كام ؟ الباقي 83 هنشوف اللي بعده اللي هو 64 اكبر منها فهنسخدمها وبالتالي الناتج بيكون 19 , هنشوف اللي بعده اكبر فمش هستخدمنه , نشوف الـ 16 هنلقيها اصغر هستخدمنه والناتج هيكون 3 ودي مجموع 2¹⁺

211 → 11010011

ودا الناتج الإجمالي

طيب نشوف العكس كدا لو معانا رقم زي دا وعايزين نجيب الـ Decimal بقائه :-

10101100 علشان نحسبها بشوف قيم الـ 1 كام وبجمعهم مع بعض وبالتالي دا بيكون الرقم يعني $128 + 4 + 8 + 32 = 172$

- الـ IP المسئول عنـه هو منظمة الـ " Internet Assigned Numbers Authority " IANA
- قولنا انـ IP ككل عبارة عن 32 Bit وانـ الـ Bit الواحدة ليها احتمالـين - فعلـشان نحسب عددـ الـ IP's كلـهم هنقول انه 2^{32}

هنلقي الناتج بقائه 4.292.967.296

الـ IP Address العدد دارـ غم ضخامتـه الا انه قليل جدا مقارنةـ بعدـ الـ Online Sites – Machines – Smart Phones – Laptops الأجهـزـه دي كلـها بتـاخـدـ IP's وبالتالي العـددـ دـا صـعبـ اوـيـ انهـ يـغـطـيـهم

- منظمةـ الـ IANA حـاولـتـ تـعـاملـ معـ المـوـضـوعـ دـا وـقـسـمـتـ الـ IP لـحـاجـهـ اسمـها Classes وـحدـدتـ لـكـلـ Class بداـيةـ وـنـهاـيةـ فيـ عددـ الـ IP's ، اـولـ الـ Octet هوـ الـ IPـ الليـ بيـحدـدـ نوعـ الـ Class بـقـائـهـ

• Class A	1 – 126
• Class B	128 – 191
• Class C	192 – 223
• Class D	224 – 239
• Class E	240 – 254

- هنـلاحظـ انـ فيـ 3 اـرقـامـ لمـ يتمـ ذـكرـ هـمـ ؟
- الـ 0 وـدا بـيـكونـ بـمـثـابـةـ الـ Default Network وـدا مـيـنـعـشـ جـهاـزـ يـاخـدـهـ
- الـ 127 مـخـصـصـ لـ الـ Loopback Interface الـ لـيـ هوـ الـ NIC لـوـ عـاـيزـ تـعـملـ عـلـيـهـ Test وـتشـوفـ هلـ هوـ شـغـالـ ولاـ فيهـ مشـاـكـلـ . فيـ حـالـةـ لـوـ عـنـدـكـ ايـ مشـكـلـهـ فـيـ الـ Internet Connection

Network Fundamental

- الـ 255 ودا بيستخدم مع الـ *Broadcasting*
 - الـ *Routing Protocols* :- بيستخدم مع الـ *Multicast* اللي بيستخدم كمثال بين الـ *Class D*
 - الـ *New Technology and Experiments* :- مع الـ *Class E*

بعد كدا عملت حاجه اسمها الـ Subnet Mask ودي ليها استخدامين :-

- 1 بتحدد عنوان الشبكة اللي انا شغال عليهما
 - 2 بتحدد عدد الأجهزة في كل شبكة

• Class A		255.0.0.0
• Class B		255.255.0.0
• Class C		255.255.255.0

بالنسبة لـ E ملهمش Subnet Mask علشان مش بيستخدموا مع الأجهزة

طب دا معناه ایه بر پرسه؟

- عشن نحسب الـ Network ID الي هو عنوان الشبكة اللي انا شغال عليها بسوف الـ IP اللي معايا دا من انهي Class والـ Subnet Mask بتاعتتها Class دي اساسا اي هيا الـ Subnet Mask بتاعتتها بعد كدا بتحول كل منهم لـ Binary - ونعمل عملية Anding بين الـ IP and Subnet Mask عشن نجيب عنوان الشبكة الـ Anding اني بعمل عملية ضرب بينهم الاتنين زي ما هنشوف دلوقت في المثال دا Subnet Mask 100.50.40.17 دا IP عايزين نجيب عنوان الشبكة بتاعتته , الواضح من الـ IP دا من Class A يعني الـ 255.0.0.0 بتاعتته

100.50.40.17 01100100.00110010.00101000.00010001

255.0.0.0 11111111.00000000.00000000.00000000

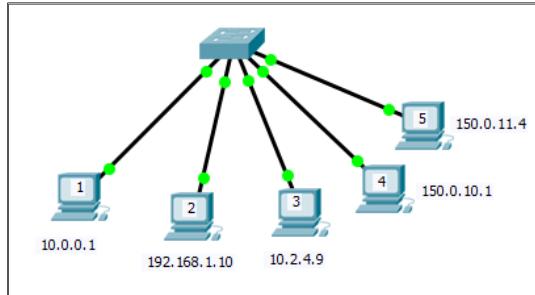
- الـ Anding Bits المتشابهة بتنزل زى ما هيا ، المختلفة بتنزل بـ 0

01100100.00000000.00000000.00000000

○ نحو له تانی لـ Decimal هنلاقي الناتج 100.0.0.0

طیب استفادت ایه انا من الحوار دا؟

- ٥ استفادت ان لازم الأجهزة اللي على نفس الـ Switch تبدا كلها بأول Octet تكون فيمته 100 واي حاجة في باقي الـ Octets



لو جينا نشوف الـ Topology دي هنلاقي ان جهاز 1 مش هيعرف يتواصل مع اي جهاز متصل معاه على السوتش الا الجهاز رقم 3 بس علشان دا معاه في نفس الشبكة

والجهاز رقم 2 مش هيعرف يكلم اي حد اساسا عشان مفيش حد معاه واحد نفس الشبكة بتاعته

اي Network ID ينقسم لجزئين - جزء بيسمى Network والجزء الثاني بيسمى Host .

- معنى كلمة Network انه لازم يكون ثابت علي كل الأجهزة اللي في شبكة واحدة علي نفس الـ Switch , اللي هو عدد الـ Bits اللي قيمتها بـ 1 في الـ Subnet Mask
- انما الـ Host بيتغير من جهاز للثاني , اللي هو عدد الـ Bits اللي قيمتها بـ 0 في الـ Subnet Mask

IP Address Classes				
Class	Format	Purpose	Address range	Max hosts
A	N.H.H.H	A few large organisations	1.0.0.0 - 126.0.0.0	16,777,214
B	N.N.H.H	Medium-size organisations	128.1.0.0 - 191.254.0.0	65,534
C	N.N.N.H	Relatively small organisations	192.0.1.0 - 223.255.254.0	254

(N = Network number, H = Host number)

- الـ Diagram دا بيوضح كل Class فيها كام Network and Host Octet لـ Class A وكمان بيوضح عدد الأجهزة المتاح في كل Class

الـ Class A لازم Octet 1 يكون ثابت , Class B لازم Two Octets يكونوا ثابتين , Class C لازم Three Octets يكونوا ثابتين في الشبكة الواحدة

- عدد الـ Zero's هو اللي بيحدد عدد الـ Hosts اللي هما عدد الأجهزة اللي هو برضه عدد الـ IP's علشان دي قيمة متغيرة

لو انا عندي شبكه فيها 50 جهاز و عايز استخدم Network معينة على قد عدد الأجهزة اللي عندي - هل هينفع ولا لا؟

- لو جينا نشوف اقل شبكة ممكن تدينا's IP هنلاقي من Class C وبتدinya 256 علشان انا عندي Octet واحد بس في الـ Subnet Mask هو اللي قيمته بـ 0
- بس انا عايز 50 بس !! في الحالة دي انا بعمل حاجه اسمها Subnetting
- يعني بقل عدد الـ Bits بتاعه الـ Host علشان اعمل Customize لشبكة معينة تديني احتياجاتي من الـ Subnetting

$$2^h - 2 = H \quad \text{في قانون احنا بنشتغل بيه اللي هو : -}$$

بالنسبة للـ H دي بتعبر عن عدد الـ Bits اللي هستخدموها من الـ Octets بتاعه الـ Hosts

بالنسبة للـ H بتعبر عن عدد الـ Hosts المطلوبة

ليه بنطرح 2 ؟

علشان اي شبكة احنا شغالين عليها فيها IP's 2 مش بيعتخدمو اللي هما الاول والأخير

- الاول بيكون اسمه الـ ID Network ودا مش بيتوزع لأي جهاز في اي شبكة ، والآخر بيكون بتاع حاجه اسمها Broadcast

نرجع للمسألة

$$2^h = 52 \quad 2^h - 2 = 50$$

هنشوف ايه هو اقرب رقم لو بقى اوس للـ 2 هيدبني الرقم اللي عايزه !! هنلاقي اقرب حاجة هو 6

يعني انا محتاج 6 Bit من الـ Host بس

الـ Hosts Bits دايما بتتحسب من جهة اليمين

الـ Subnet Mask دا هيكون الـ 11111111.11111111.11111111.11000000

عدد الـ Bits بتاعه الـ 1 ممكن نعبر عنهم بـ /26

مثال

ايه هو افضل Subnet Mask لو انا عايز شبكة تديني 500 جهاز باستخدام الشبكة اللي عنوانها 10.0.0.0/8

$$2^h = 502 \quad 2^h - 2 = 500$$

هنشوف ايه هو اقرب رقم لو بقى اوس للـ 2 هيدبني الرقم اللي عايزه !! هنلاقي اقرب حاجة هو 9

$$2^9 = 512$$

يعني انا محتاج Bit 9 من الـ Host مش الـ 24 اللي موجودين كلهم في المعطيات
والـ Subnet Mask هنعرض عن كل قيم الـ 1 وه يكون الناتج هو 10.0.0.0/23
255.255.254.0

مثال تاني :-

لو قولنا ايه هو عدد الأجهزة المتاح في الـ Subnet Mask دا 255.240.0.0
هنشوف عندي كام Bit بتساوي 0 علشان دي بناعة الـ Hosts وعلشان نعرفها لازم حول الـ لـ Binary Subnet Mask
هناقي عندي 20 - 11111111.11110000.00000000.00000000

$$H = 1.048.574$$

$$2^{20} - 2 = H$$

ممكن تيجي بشكل تاني اللي هو يديك الرقم علي طول بعد / يعني زي دي مثلا :-
ايه هو عدد الأجهزة وايه هو الـ Subnet Mask في الشبكة دي 21/؟؟

لو عندنا مثلا سؤال بيقول ايه هي الـ ID Network الخاص بالـ IP دا - 170.55.99.17/20 ؟

كما ذكرنا علشان نحسب الـ Network ID بنقوم بعمل عملية Anding بين الـ IP and Subnet Mask .

هنا انا عندي 20/ يعني دا معناه ان عندي 20 Bit قيمتهم بـ 1

فانا ممكن محو لش اول اتنين Octet علشان هما كدا هيحصل ليهم Anding مع الـ 1 وهينزلو زي ما هما

170.55.99.17 → 170.55.01100011.00010001

255.255.240.0 → 255.255.11110000.00000000

هناقي الناتج اللي هيطلع من عملية الـ Anding هو دا :- 170.55.01100000.00000000

اللي هو 170.55.48.0/20

زي ما قولنا ان الـ Subnetting بيقل عدد الـ Bits بتاعة الـ Host , كمان بيقسم الشبكة بتاعتي لأكتر من شبكة صغيرة وكل شبكة
يبكون فيها عدد أجهزه معين " محدد "

مثال ثاني :-

لو انا عايز اجيب الشبكة الثالثة من الـ IP دا – 192.168.10.13/29

اول حاجة بنعملها اننا هنجيب الـ Network ID الأول زي المثال السابق :

192.169.10.00001101

255.255.255.11111000

هلاقى الناتج بناء على الـ Anding هيكون – 192.168.8.0/29

طيب ايه بقى حكایة الشبكة الثالثة ؟ لو جينا نشوف الـ Subnetting اصلا وظيفته انه بيقلل عدد الأجهزة وبيقسم الشبكة بتاعتي علشان اعرف عدد الأجهزة او ايه هو المقدار اللي هزود على اساسه بحسب عدد الـ Bits بتاعه الـ Host قد ايه وبيكون دا عددهم في الشبكة دي بس ، واي زيادة ه تكون في شبكة تانية

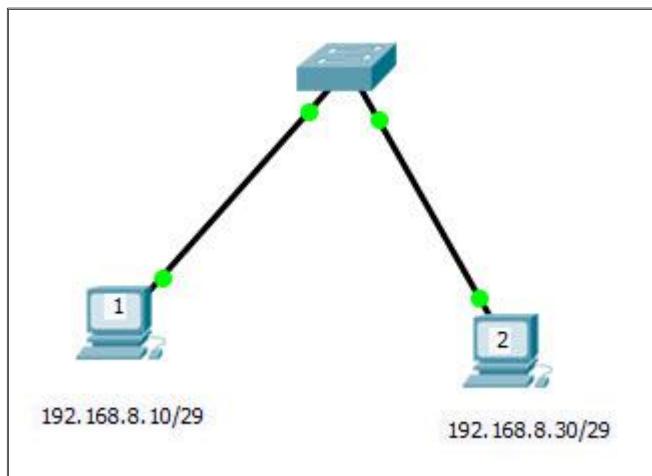
علشان اجيب الشبكة الثالثة – بروح على الـ Octet الـ Mix بين الـ 0 and 1 واسوف ايه هي اقل قيمه لـ 1 في الـ Subnet Mask

Interest Octet 1000 – اقل قيمة هنا هلاقى انها بـ 8 والـ Octet دا بيكون اسمه الـ 255.255.255.11111000

ازاي يعني ؟ طب تعالى نحسبها بالقانون اللي كنا شغالين بيها في الأول اللي هو $H = 2^h - 2$

احنا عندنا 3 بتوع الـ Bit وهلاقى ان الناتج بتاعها انه هيدبني 6 Valid IP's انتا عدده الـ IP's الإجمالي 8 . في Two IP's يتم طرحهم اللي هما الـ Network ID & Broadcast IP

الشبكة الأولى ه تكون 192.168.8.0/29 والشبكة الثانية هزود 8 في آخر Octet علشان دا اللي فيه الـ Mix في الـ Subnet Mask فهتبقى 192.168.8.16/29 والشبكة الثالثة ه تكون 192.168.8.30/29



لو بصينا على الديزاين اللي قدامنا دا

هلاقى ان PC1 مش هيرجع يعمل اي Connection مع PC2 لأن كل واحد منهم في شبكة مختلفة

اللي حدد دا هو الـ Subnet Mask بتاع كل جهاز

Subnet =Network

مثال ثاني :-

ممکن يقولك انا عايز الشبكة الخامسة من الـ IP دا – 100.60.45.10/18 ؟

اول حاجة بنعملها اننا هنجيب الـ Network ID الأول زي المثال السابق :

100.60.45.10 → 100.60.00101101.00001010

Subnet Mask → 255.255.11000000.00000000

بعد الـ Anding هنلاقي الناتج اللي طلع :- 100.60.0.0/18

طيب ايه بقى حكایة الشبكة الخامسة ؟ لو جينا نشوف الـ Subnetting اصلا وظيفته انه بيقلل عدد الأجهزة وبيقسم الشبكة بتاعتي علشان اعرف عدد الأجهزة او ايه هو المقدار اللي هزود على اساسه بحسب عدد الـ Bits بتاعه الـ Host قد ايه وبيكون دا عددهم في الشبكة دي بس , واي زيادة ه تكون في شبكة تانية

علشان اجيب الشبكة الخامسة - بروح علي الـ Octet Mix بين الـ 0 and 1 واسوف ايه هي اقل قيمة لـ 1 في الـ Subnet Mask

Interest Octet 255.255.1 1000000.00000000 - اقل قيمة هنا هنلاقي انها بـ 64 والـ Octet دا بيكون اسمه الـ

يعني انا عندي الشبكة الأولى ه تكون 100.60.0.0/18 - والشبكة الثانية هزود 64 في الـ Octet بتاعها ,

و هفضل ازود لحد ما اوصل للشبكة الخامسة

طيب خلينا ناخذ مثال كدا يجمع الليلة دي كلها :-

ايه هو عدد الأجهزة والـ Subnet Mask وعنوان الشبكة - والشبكة رقم خمسة - و اول IP - وآخر IP متاحين فيها من 192.168.50.32/27 ؟

What is the Network ID and Number of Valid Hosts and 5th Network and 1st IP in it ?

نجيبها وحدة وحدة كدا :-

192.168.50.00100001

Subnet Mask → 255.255.255.223 → 255.255.255.11100000

Network ID → 192.168.50.00100000 → 192.168.50.32

عدد الأجهزة المتاحة في كل شبكة اللي هو عدد الـ Bits اللي بتساوي 0 وبنحسبها من القانون :-

$$H=30$$

$$2^5 - 2 = H$$

$$2^5 - 2 = H$$

Valid Hosts = 30 IP

طيب علشان نجيب الشبكة الخامسة - هنشوف قيمة الـ Interest Octet بكم ونزوودها على الـ ID اللي معانا

القيمة بتاعه الـ 1 في الـ Subnet Mask بتساوي 32 ودي اللي هنزوودها

Network Fundamental

هلاقي ان الشبكة الثانيه 192.168.50.64/27 والثالثه 192.168.50.96/27 والرابعه 192.168.50.128/27 ونيجي للخامسة اللي هي مطلوبة 192.168.50.160/27

اول IP متاح في الشبكة دي هو 192.168.50.161/27 علشان الـ Network ID مش بيتوزع اساسا هو مجرد عنوان للشبكة ومينفعش الأجهزة تاخده

آخر IP متاح ؟ علشان نحسبه لازم الاول نجيب الشبكة اللي بعدها 192.168.50.192/27

علشان نحسب آخر IP بنطرح 1 وبيكون الناتج هو 192.168.50.191/27 بس دا اللي هو الـ Broadcast علشان نجيب الـ Last Valid بنطرح 1 كمان وبيكون الناتج هو 192.168.50.190/27

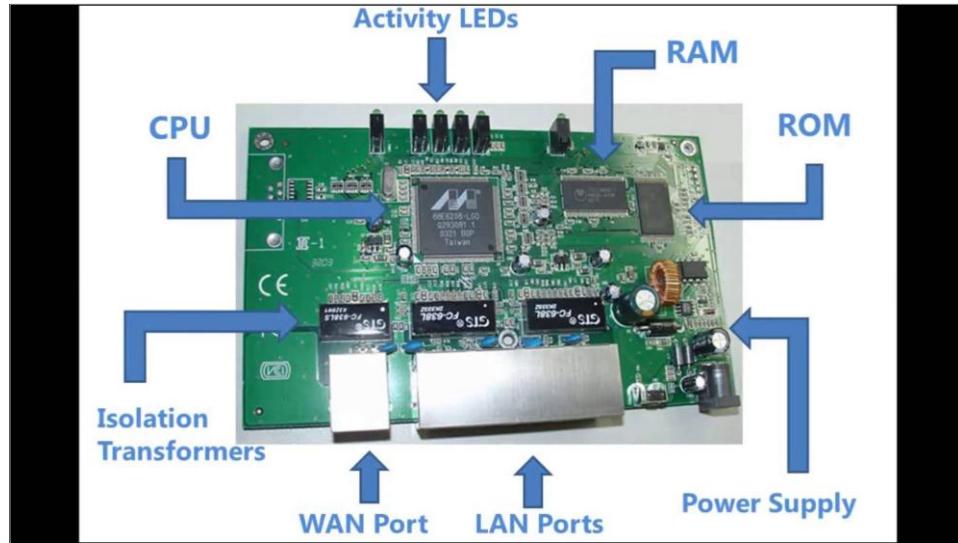
او ممكن تزود 30 مره واحده اللي هي عدد الأجهزة المتاح في كل شبكة

في المثال دا : ممكن يقولك انا عايز الشبكة الخامسة من الـ IP دا – 100.60.45.10/18 ؟

جرب كدا تحسب ايه هو اول IP وآخر IP في الشبكة الخامسه ؟؟

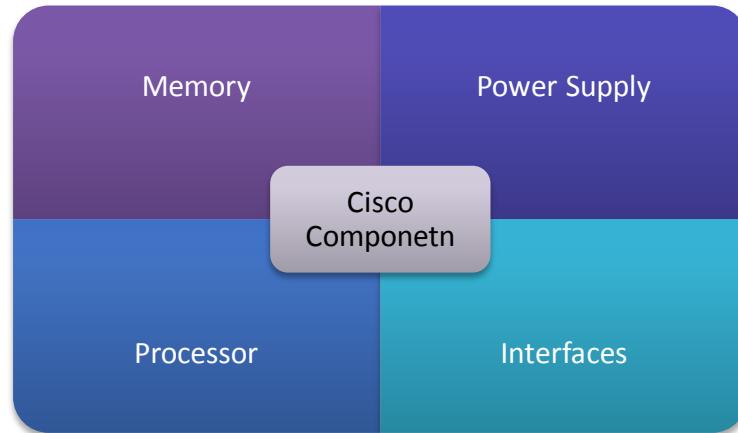
This Page Intentionally Left Blank

Cisco Router and Switch Component



الشابتير دا هيتكلم علي الأجهزة اللي احنا ممكن نعمل ليها Service Configuration لـ Service Configuration اللي عايزينها مش الأجهزة اللي موجودة عندنا في البيت

في فرق كبير جدا بين الـ Switches اللي بنشتريها علشان نعمل LAN داخلية في البيت وبين الأجهزة اللي Cisco or Juniper بتقدمهم
الكلام اللي هينقال دلوقت في الشابتير دا علي الأجهزه اللي بتقدمها Cisco



-: Power Supply -1

دا بيكون المسئول عن تزويد كل الـ Power Component بالـ Power اللي لازم علشان يشتغلوا ويدبونا الـ Performance اللي احنا عايزينه

بيحول من التيار المتردد بتاع البيوت لتيار ثابت علشان مفيش اي Component يتفرق لو جاله Volt زيادة
Convert from AC to DC

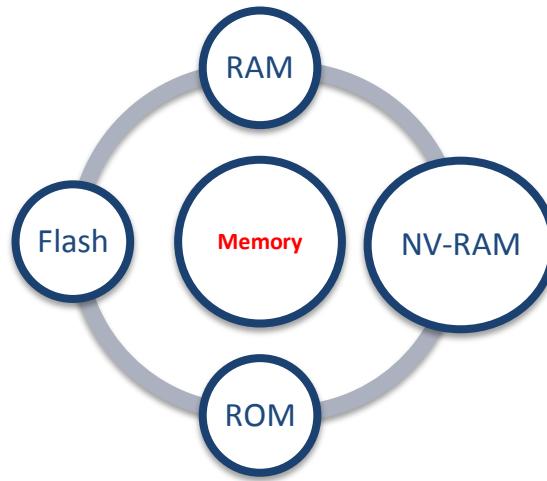
Interfaces -2

ودي بتحدد طبيعة الأجهزة اللي هتوصل بالـ Device هل هو سوتش ولا جهاز ولا راوتر وكل Interface ليه مميزات عن الثاني ودي هتعرفواها بالتفصيل في كورس CCNAx

-: Processor -3

مسؤول عن تنفيذ اي Configuration بنعملها على الـ Device بيعتبر هو العقل بتاع الجهاز علشان مفيش اي حاجه بتعمل الا ولازم يتعمل ليها Process

-: Memory -4



-: RAM

Random Access Memory دyi بيكون فيها الـ Running Configuration يعني اي اعدادات احنا عملنا ليها تعديل او انشاء بس لسه معملناش ليها اي Save , بمجرد ما الجهاز يحصل ليه Restart هتلaci الاعدادات دي كلها راحت

-: NV-RAM

دي اللي بيتحفظ فيها الإعدادات اللي انا عملتها على الـ Device بتاعي - بيكون اسمها Saved Configuration علشان تبدأ تشغيل اول ما الجهاز يعمل Reload او يتقطع ويتفتح تاني

-: Flash

دا المكان اللي بيكون عليه الـ Operating System بتاع الـ Router or Switch وبيكون اسمه IOS " Internetwork Operation System " - الإصدار الحالي منه 15.3 دا الاصدار الجديد اللي نزل مع منهج CCNAx 200-120

ROM

ودي بيكون فيها الإعداد الأولية بتاعه الجهاز Read Only Memory

ROM - Component	Responsible for :-
1 POST	Power on Self-Test هي مسؤولة عن ان اول ما تفعل Check Device هي مسؤولة عن ان اول ما تفعل Check Device على كل الـ LED's اللي موجودة هل واحدة Configuration ولا لا وهل معنده ليها Shutdown ولا لا علشان لو في اي Error في اي LED نقدر نعرفه
2 Boot Strap	ليها وظيفة مهمة او هي – ان اول ما تفعل Check Device بتنزل بتروح على الـ Flash وتحب منه الـ IOS بتاع الـ Device . وتروح على الـ NV-RAM وتحب الـ Saved Configuration وتعمل ليهم Compile مع بعض وتوديهم للـ RAM علشان يحصل لهم Running مع بعض وبالتالي الـ Device يشتغل بالإعدادات بتاعتة
3 Rommon – RX-Boot	دي بيكون فيها حاجة اسمها Configuration Register اللي هي بتحدد طبيعة الـ Device Booting نفسه وبيكون فيها الـ Device Configuration بتاعة الـ Basic Configuration .

This Page Intentionally Left Blank

Network Cables

الـ Cables اللي هي الأسلام اللي بتوصل بين الأجهزة وبعضاً وبنقال عليها مصطلح Medium يعني وسيط بين جهازين .
ليها كذا نوع وكل نوع ليه استخدامات معينة :-

Co-Axil
Cable

Twisted
Pair

Phone
Cable

Fiber
Cable

Console
Cable

-: Phone Cable -1

دا Cable اللي بيستخدم مع التليفون الأرضي - واللي بتجي من خلاه خدمة الانترنت زي ما وضحتنا في الشرح بتاع DSLAM
ودا بيتوصل مع التليفون الأرضي عن طريق حاجه اسمها RJ-11



-: Console Cable -2

دا اللي بيستخدم مع Cisco Devices علشان اعمل Initial Configuration او في حالة لو عايز اعمل Password Recovery



-:Co-Axil Cable -3

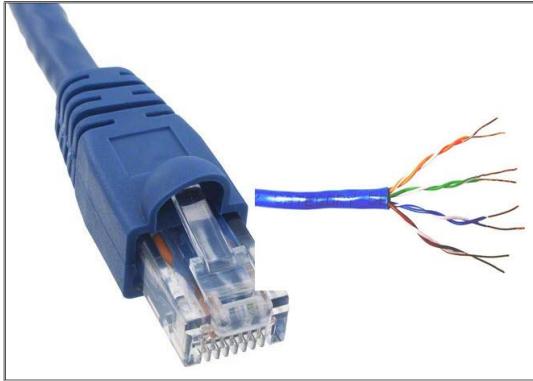
دا كان اول نوع من الـ Cables كان بيستخدم في الـ Network علشان كان رخيص وكان ممكن يتوصّل لمسافات كبيرة او اي وكانت الأجهزة اول ما اتصنعت كانت بتدعّم النوع دا .

The Bandwidth for Co-Axial Cable is 10 Mbps - Megabits per second



هو شبيه للـ TV Cables اللي بنسخدمه في البيت
ليه نوعين :-

Thin (Thinnet) Cable	<ul style="list-style-type: none">- Flexible coaxial cable about $\frac{1}{4}$ inch thick.- Thinnet is used for short-distance.- Thinnet connects directly to a workstation's network adapter card using a British Naval Connector (BNC).- The maximum length of thinnet is 185 meters- RG-58 family
Thick (Thicknet) Cable	<ul style="list-style-type: none">- Thicknet coaxial is thicker cable than thinnet.- Thicknet cable is about $\frac{1}{2}$ inch thick and can support data transfer over longer distances than thinnet.- Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks.



-: Twisted Pair -4

ودا الـ **Cable** اللي بيتوصل بين الأجهزة حاليا - اكثراً الانواع انتشاراً وواكثراً هم استخداماً في الـ **LAN** **Noising** يعني زوجين من الـ **Cables** علشان يتجنب الـ **Twisted** **and Losing** للبيانات اللي ممكن تحصل في عملية نقل البيانات

الاسلاك الواضحة في الصورة بيكون اسمها **Pin** - وبت تكون من الياف نحاسية

الـ **Twisted Pair** ليه نوعين :-

UTP "Unshielded Twisted Pair"

STP "Shielded Twisted Pair"

الفرق بين الاثنين في نوع النحاس المستخدم والطبقة العازلة اللي بتكون موجودة بين الغلاف والـ **Pin** والسعر .
الـ **STP** بيعتبر أغلى من الـ **UTP** علشان النحاس بتاعه بتكون الخامسة بتاعتته افضل من الـ **UDP**

1. STP cables are shielded while UTP cables are unshielded
2. STP cables are more immune to interference and noise than UTP cables
3. STP cables are better at maximizing bandwidth compared to UTP cables
4. STP cables cost more per meter compared to UTP cables
5. STP cables are heavier per meter compared to UTP cables
6. UTP cables are more prevalent in SOHO networks while STP is used in more high-end applications

الـ **UTP** ليه حاجة اسمها **CAT5e** and **CAT6** وبيرمز لها بالـ **CAT** , حاليا اللي موجود في السوق **CAT5e** and **CAT6** وهي المميزات بتاعتتهم :-

- 1000Mbps data capacity
- For runs of up to 90 meters
- Solid core cable ideal for structural installations (PVC or Plenum)
- Stranded cable ideal for patch cables
- Terminated with RJ-45 connectors

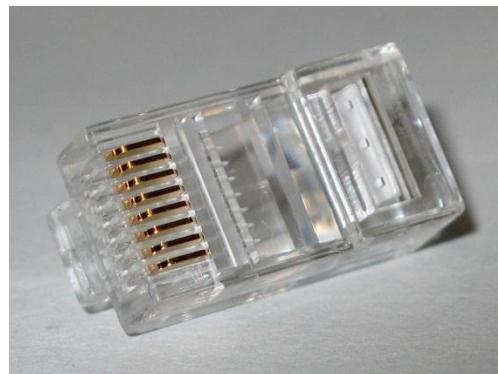
Network Fundamental

UTP Category	Purpose	Transfer Rate
Category 1	Voice Only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps
Category 6	Data	1/10 Gbps

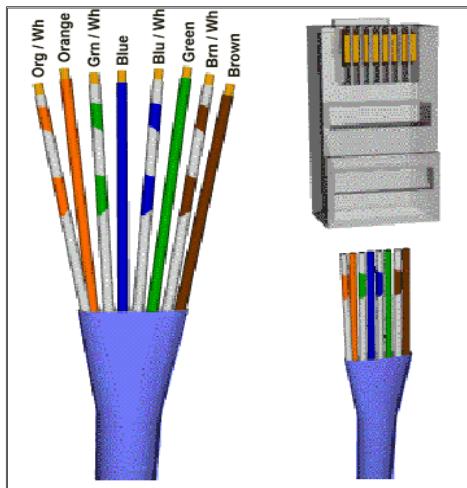
Twisted-Pair Cabling Considerations

- Use twisted-pair cable if:
 - Your LAN is under budget constraints.
 - You want a relatively easy installation in which computer connections are simple.
- Do not use twisted-pair cable if:
 - Your LAN requires a high level of security and you must be absolutely sure of data integrity.
 - You must transmit data over long distances at high speeds

الـ Twisted Pair Cables بتوصيل في حاجة اسمها RJ-45 ودا بيكون المكان اللي بتتحط فيه الـ Pins بتاعة الـ Cables



:: UTP Pins Colors

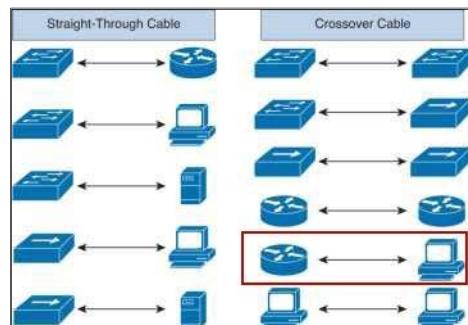


ترتيب الألوان بتاعه الـ Cables بتختلف علي حسب طبيعة التوصيل , هل الأجهزة اللي هنتوصل مع بعض دي أجهزة متشابهة ولا أجهزة مختلفة ترتيب الألوان دا معناه اني بعمل حاجة اسمها "تأريج" يعني بحط الـ Pins في الـ RJ وبيستخدم الـ Crumble اللي هيا الآر اجه عشان اعمل تأريج في نوعين من التوصيل بين الأجهزة , واللي بيحددهم هو طبيعة ترتيب الألوان في الـ RJ :-

- Straight Through - ودا بيستخدم للتوصيل مع الأجهزة المختلفة يعني جهاز

مع سوتش او سوتش مع راوتر

- Cross Over - ودا بيستخدم للتوصيل مع الأجهزة المتشابهة



القاعدة الشاذة الوحيدة في التوصيل هي بين جهاز وراوتر على الرغم من انهم اجهزة مختلفة الا ان نوع الـ Cable اللي بيستخدم بيكون Cross Over

1	White and Orange
2	Orange
3	White and Green
4	Blue
5	White and Blue
6	Green
7	White and Brown
8	Brown

دا بيكون الترتيب بتاع طرف من الطرفين بتوع الـ Cable والطرف الثاني علي حسب الـ Device المتصل بييه اي بمعنى تاني علي حسب طريقة التوصيل , هل هي Cross Over ولا Straight Through

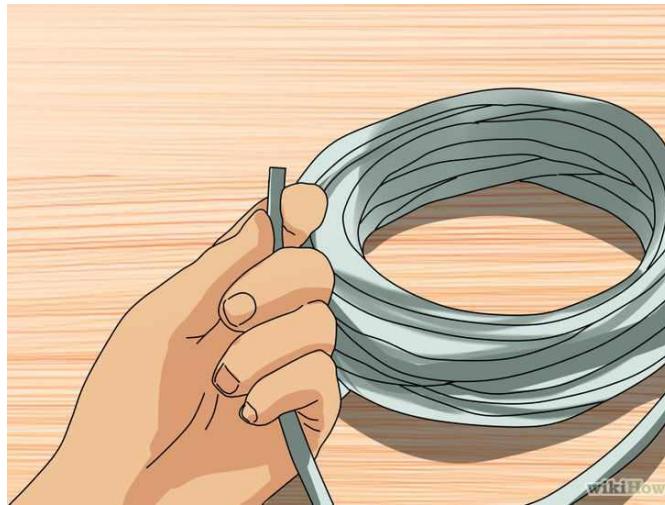
لو الطرف الثاني كان زي الطرف الأول بيفي كذا التوصيل نوعه

Through

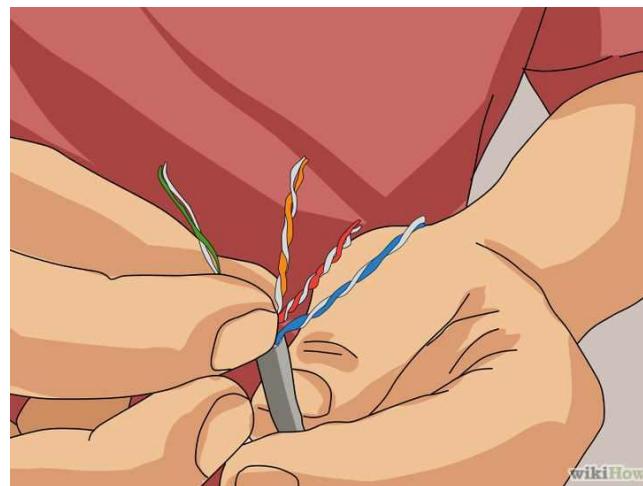
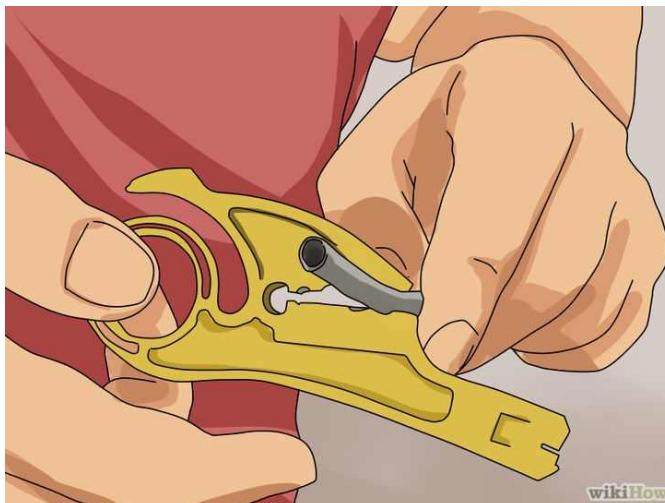
لو عملنا تبديل للـ Cross Over بيفي كذا Cable دا هيتوصل

مش كل الـ Pin 8 بيستخدموا في نقل الداتا - الـ Pins الأساسية هي 1,2,3,6 والباقي بيستخدم كـ Backup ومع تكنولوجى POE " Power Over Ethernet "

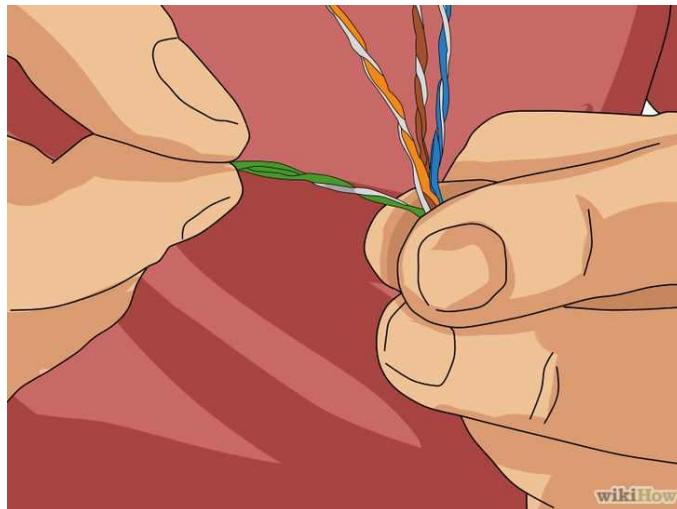
How to Make a Network Cable



بنعمل عملية تقشير لـ Cable علشان نشيل الطبقة العازلة اللي عليه

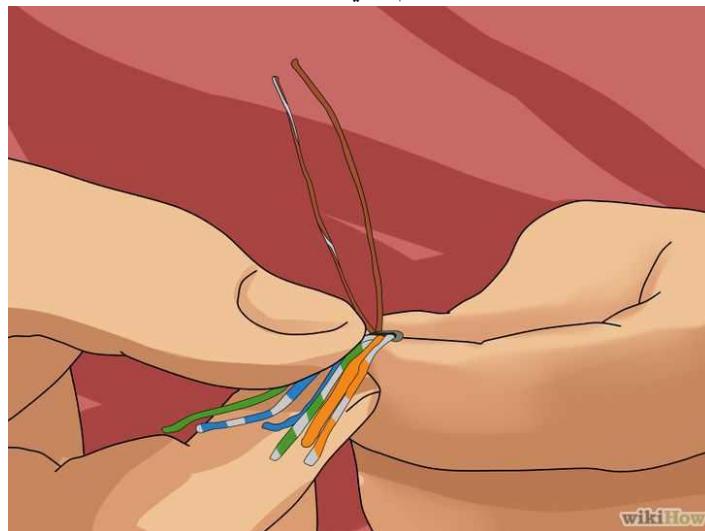


بنفرد كل Pair من بعضه



wikiHow

وبنبدأ نخليلهم على استقامة واحدة



wikiHow

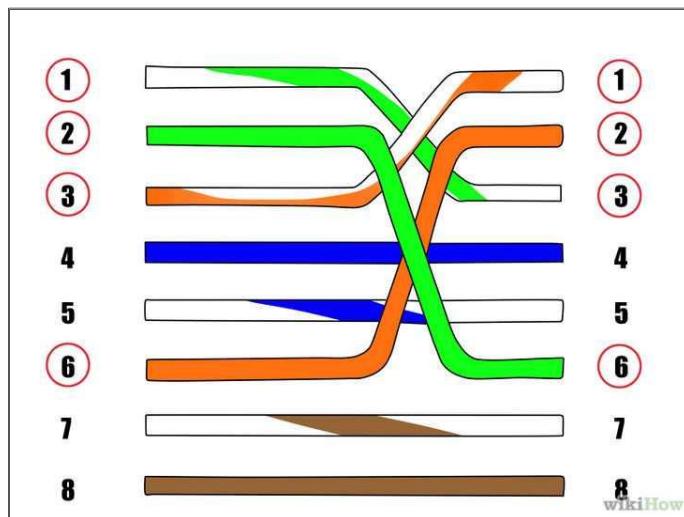
ونشوف ترتيب الألوان اللي هنسخدمه ايه هو ؟

568B - Put the wires in the following order, from left to right:

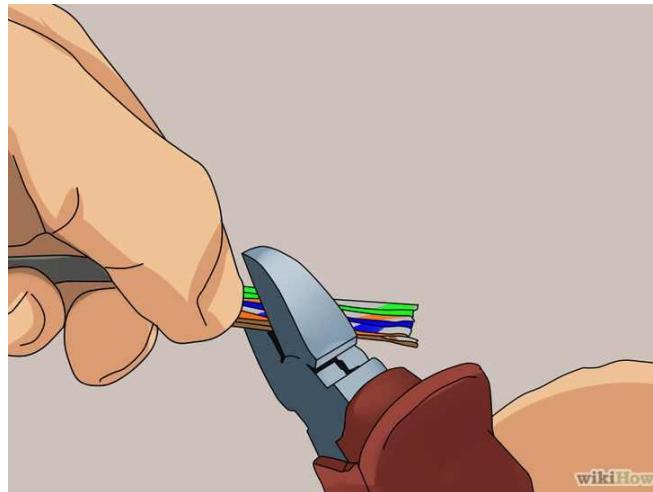
- white orange
- orange
- white green
- blue
- white blue
- green
- white brown
- brown

568A - from left to right:

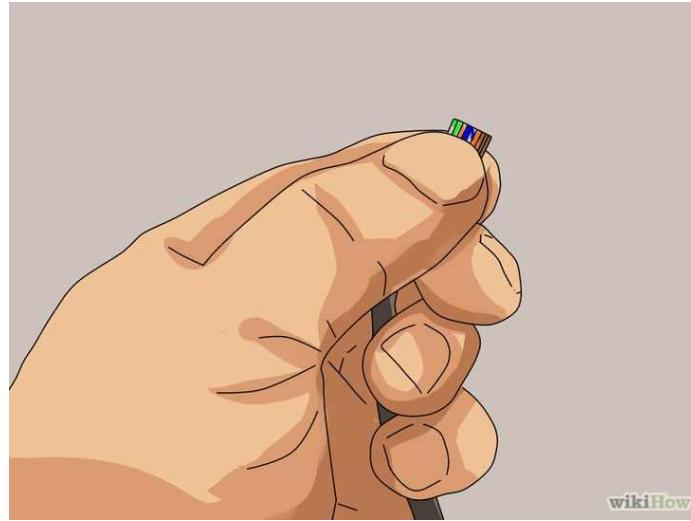
- white/green
- green
- white/orange
- blue
- white/blue
- orange
- white/brown
- brown



نفص الـ Pins بإستقامة واحدة بالتساوي

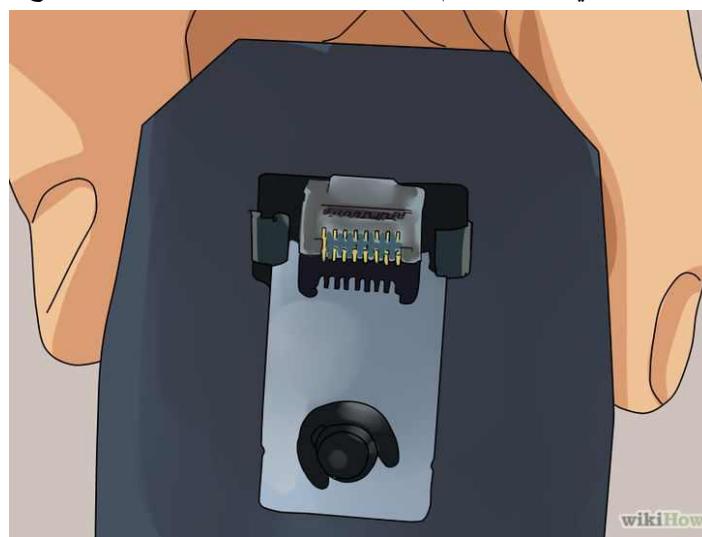


ودا بيكون الشكل اللي المفروض يظهر قدامك



wikiHow

بعد كدا ييجي دور استخدام الـ Crumble علشان نعمل عملية التأرجح



wikiHow

بعد كدا بتعمل Test لـ Cable دا علشان تشفّف عملية التأرجح كانت ناجحة ولا لا



wikiHow