



# مذكرة الـ CCNA العربية

200 - 301

## الجزء الأول

01

تم إتاحة هذا الجزء مجاناً لوجه الله تعالى .  
لا تنسوني من دعائكم



clickone\_1



clickone1



0552102740

## فهرس الجزء الأول

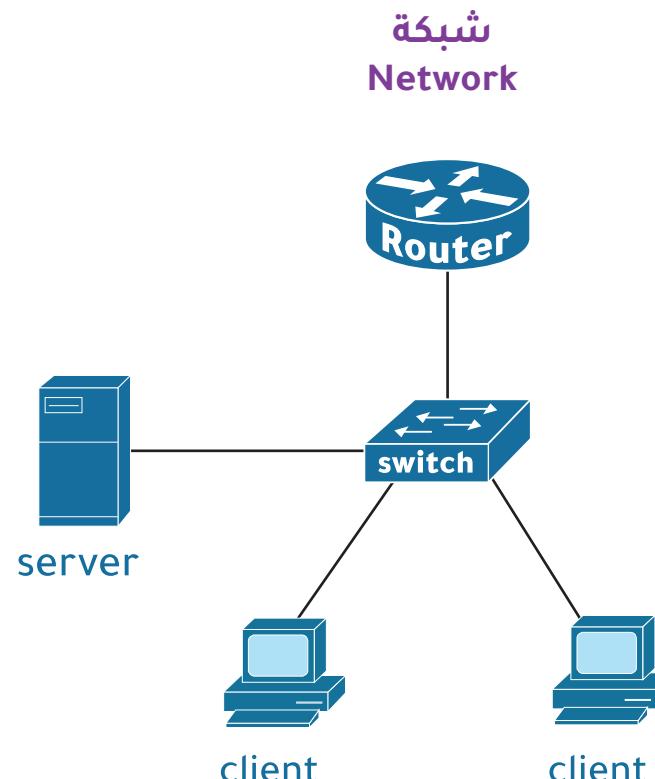
133	Static Routing	61	بروتوكول ARP	3	الشبكات
133	Direct Connected	62	Gratuitous ARP	4	أجهزة الشبكة
135	Default Routing	63	أوضاع السويفت	7	أنواع الشبكات من حيث التصميم الهندسي
136	Dynamic Routing	64	جدول الماك أدرس في السويفت	10	الوسائل المادية ( كيابل الشبكات )
140	Metric	68	برنامج packet tracer	13	البورت والبروتوكول
140	المسافة الإدارية	69	طرق الاتصال بالسويفت والراوتر	15	Network Models
148	Host Route	75	الشبكة المحلية الافتراضية (VLAN)	27	طرق إرسال البيانات في داخل الشبكات
152	Floating Static Route	79	إنشاء الفيللن وربطها بالمنفذ	31	التصميم الهرمي لشبكات سيسكو
154	Longest Prefix Match	85	السماح والمنع في وضع الـ Trunk	32	ipv4 Address
		88	إنشاء فيللن للصوت	33	العناوين المنطقية في الاصدار4
		90	Inter VLAN Routing	35	Binary
		95	بروتوكول VTP	35	Decimal
		102	بروتوكول STP	35	النظام السادس عشر
		104	عملية انتخاب السويفت الرئيسي	36	شرح عنوان الـ ipv4
		111	مراحل المنافذ في STP	37	التحويل من العشري إلى الثنائي
		112	المؤقت في STP	39	التحويل من الثنائي إلى العشري
		113	إصدارات STP	40	شرح فئات أو كلاسات الـ ipv4
		116	Port Fast + BPDU Guard	42	قناع الشبكة
		120	بروتوكول CDP وبروتوكول LLDP	54	(Classless Inter -Domain Routing) (CIDR)
		126	Ether-Channel	54	تقسيم الشبكات
		126	بروتوكولات الـ LACP و PAGP	55	قناع الشبكة الفرعية ثابت الطول (FLSM)
		131	جهاز الراوتر والتوجيه	55	قناع الشبكة متغير الطول (VLSM)
		132	بناء جدول التوجيه	56	الفرق بين Classless و Classful

## الشبكات Networks

هي شبكة اتصالات رقمية بين مجموعة من الأجهزة يتم فيها مشاركة الموارد فيما بينها .

### ≡ أنواع الأجهزة الموجودة في الشبكة :

هذه بعض الأجهزة الموجودة في الشبكة وصورها التي تدل عليها في البرنامج أو الشرح .



Router



جهاز الراوتر



switch



جهاز السويتش



Firewall



جهاز جدار الحماية



server



جهاز السيرفر



client



جهاز العميل

يطلق عليها :  
End hosts  
End points

## أجهزة الشبكة

### Network Devices



#### : Router 2

الموجه يعتبر من أهم الأجهزة المستخدمة في ربط الشبكات المختلفة ويعمل في الطبقة الثالثة Network Layer.

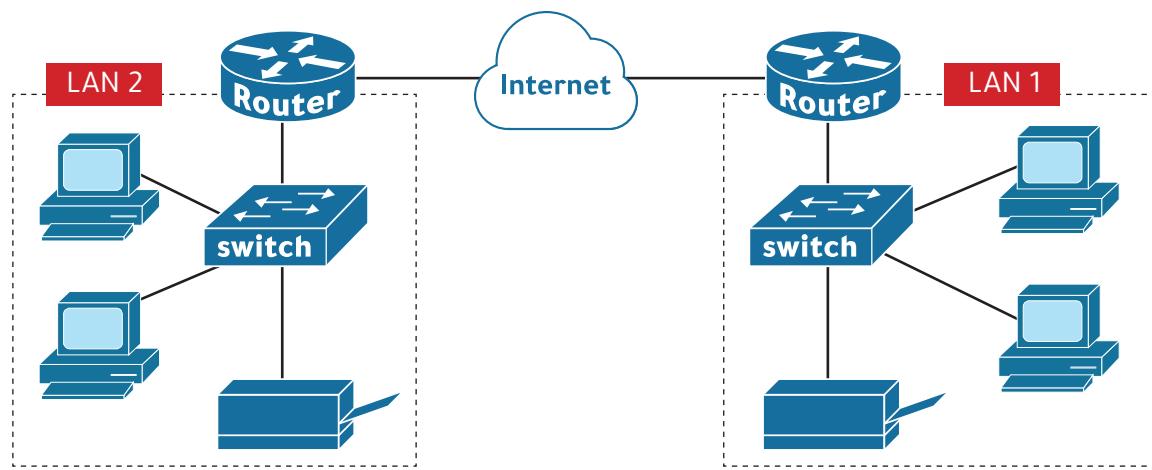
#### وظائفه :

- 1- التعامل مع العناوين المنطقية ip address .
- 2- اختيار افضل المسارات لمرور البيانات من المرسل الى المستقبل .
- 3- ربط عدة شبكات مع بعض فمثلا ربط شبكة بعنوان 10.0.0.0 ب شبكة بعنوان 192.168.1.0 .
- 4- يستخدم لإرسال البيانات عبر الانترنت .

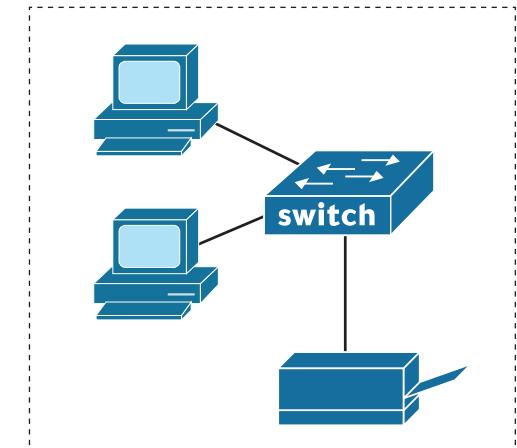


#### : Switch 1

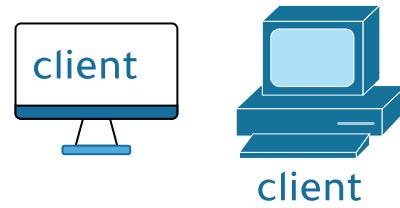
السويتش هو جهاز يعمل على ربط أجهزة الشبكة بعضها البعض مثل (الحاسوب - الطابعة) وذلك ضمن شبكة محلية (LAN) يتميز هذا الجهاز بالسرعة والأداء . و هو من أكثر أجهزة ربط الشبكات استخداما حاليا .



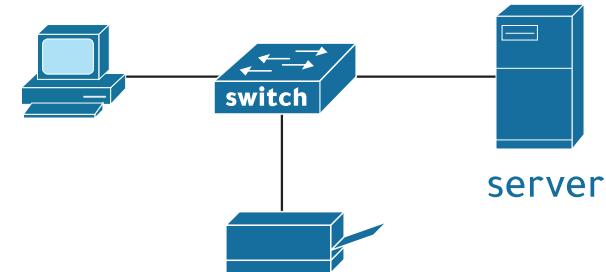
شبكة محلية Lan network



**5 - العملاء Clients** : هو جهاز يصل إلى خدمة يوفرها الخادم أو جهاز آخر، مثل جهاز الحاسب أو اللاب توب أو الجوال أو غيره .



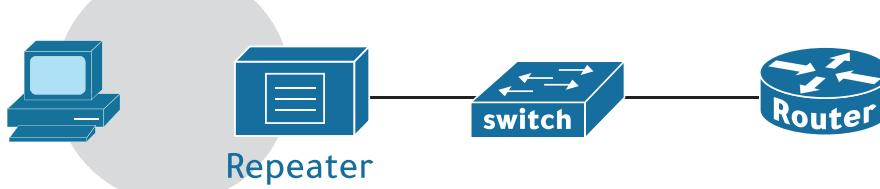
**3 - السيرفر أو الخادم Server** : هو جهاز خاص يوفر خدمات للعملاء .



Repeater

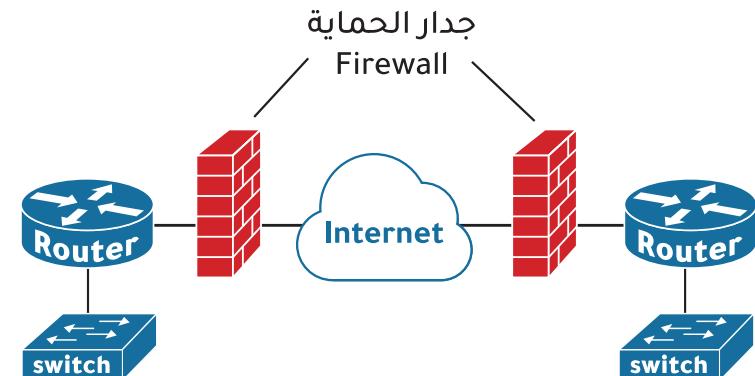
#### 6 - جهاز المكرر Repeater :

يعتبر جهاز الـ Repeater أبسط أجهزة الربط في الشبكات، حيث يقتصر امكانية عمله على تكرار وتقوية كل ما يصل إليه من إشارات. السبب الرئيسي الذي يدعو لاستخدام هذا الجهاز في الشبكة هو زيادة المسافة التي يمكن إليها الكابل والتغلب على ضعف الاشارة المرسلة



**4 - جدار الحماية Firewall** : هو جهاز أو برنامج يساعد على حماية الشبكة من التطفل والاختراق .

- هو مثل الحدود أو البوابات التي تدير حركة نشاط الانترنت المسموح به والمحظوظ في شبكة خاصة.

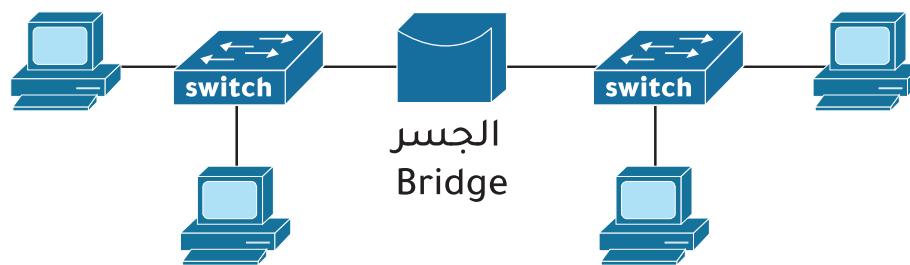
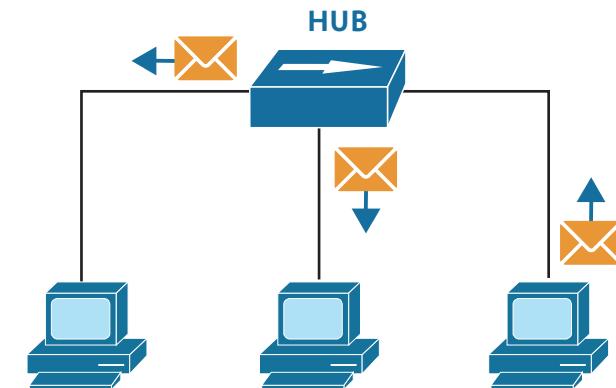
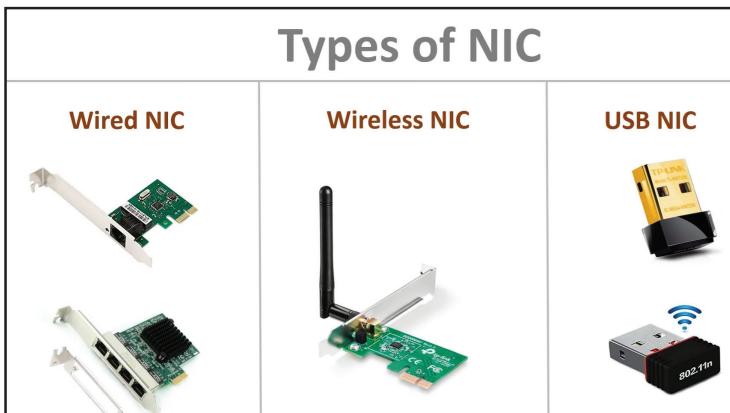


## 7 - الموزع : HUB

هو عبارة عن جهاز يقوم بربط مجموعة من الأجهزة عن طريق كابل الشبكة .

- يحتوي في العادة على 4 او 8 او 16 او 32 منفذ او Port .
- فائدته تقوية الاشارة .

- اي رسالة تصل له من جهاز محدد يقوم بتوزيعها على كل الأجهزة وهذا شيء غير جيد لانه يؤدي لحدوث بطء في الشبكة لذلك هو غير مفضل استعماله .

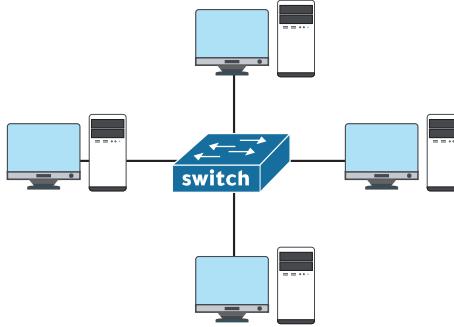


## 9 - الجسر : Bridge

يعمل هذا الجهاز على ربط شبكتي LAN ببعضهما بحيث يعملان كشبكة واحدة ينشيء هذا الجهاز جدول توجية routing table يتضمن العنوانين الفعليتين للأجهزة يحدد هذا الجدول الوجهة الصحيحة للرسالة المارة فيها .

## أنواع الشبكات

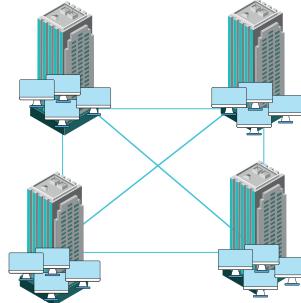
تنوع الشبكات حسب المدى الجغرافي إلى عدة أنواع :



LAN Area Network

الشبكة المحلية

يغطي هذا النوع من الشبكات عادة المناطق الجغرافية الصغيرة مثل الجامعات أو أحد فروع الشركات الكبيرة أو شبكة الحاسوب في منزل ما .



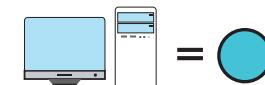
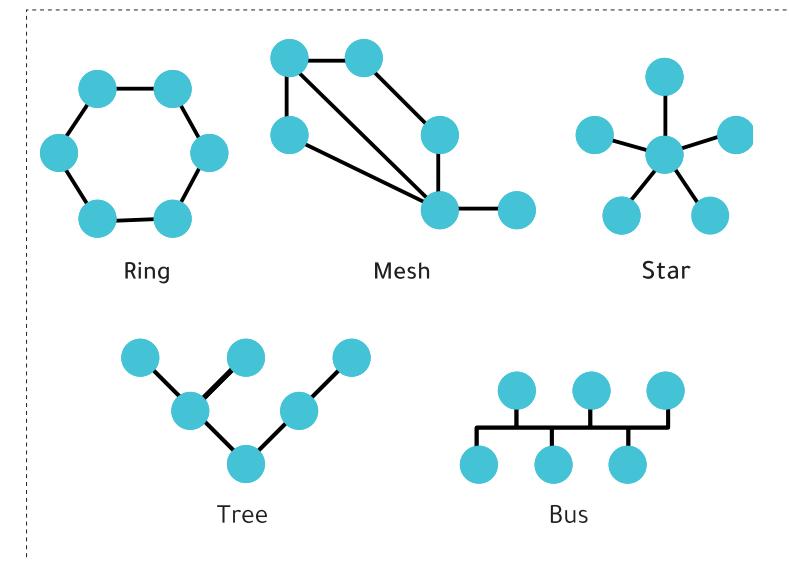
Campus Area Network

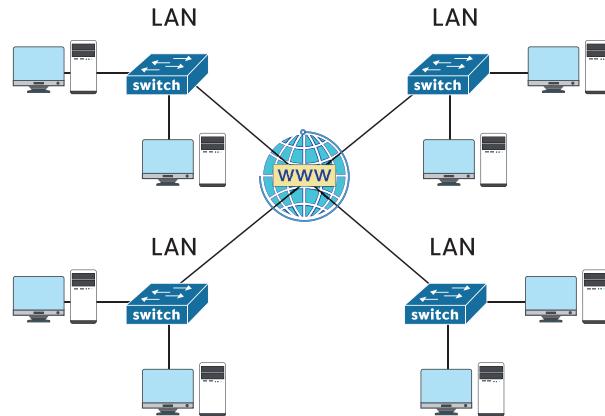
شبكة المباني

تجمع الشبكة الداخلية المحدودة بين الجامعات والكليات المنتشرة بنفس المنطقة ضمن شبكة واحدة مشتركة، وسريعة، ذات خصوصية عالية، لذا تشبه في عملها شبكة (LAN) مع الاختلاف البسيط في الحجم .

## ≡ أنواع الشبكات من حيث التصميم الهندسي

- . mesh Topology 1
- النجمية 2
- الخطية 3
- Tree Topology 4
- . Ring Topology 5

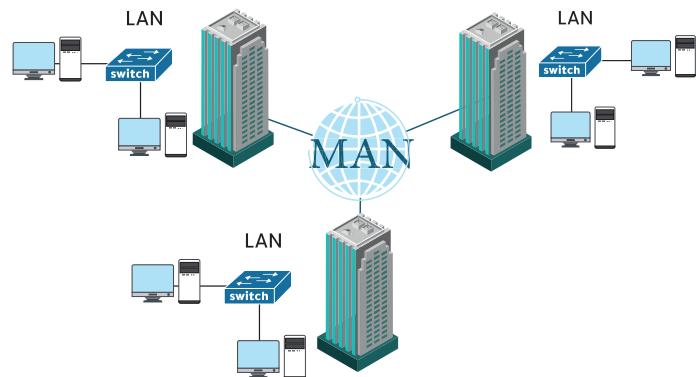




الشبكة الواسعة التي تربط بين الحواسيب على مسافات جغرافية واسعة، ولا ترتبط بمنطقة محددة، والنوع الأكثر شيوعاً هو الانترنت.



Wide Area Network  
الشبكة الواسعة



هذه الشبكة أوسع من الشبكة المحلية LAN وأصغر من الشبكة الواسعة WAN، مثال على هذه الشبكة في المدن، والمدينة الواسعة.



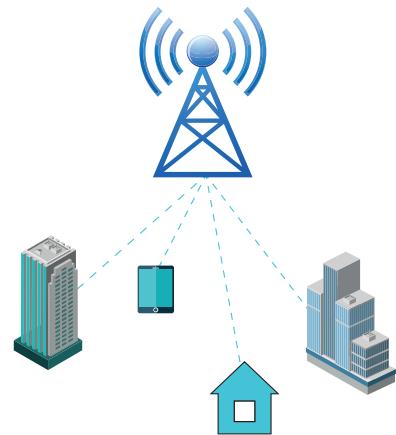
Metropolitan Area Network  
شبكة المدينة



الشبكة الشخصية هي الشبكة الأساسية وتكون مقيدة بشخص واحد، يوفر شبكة تصل إلى 10 أمتار من الشخص إلى الشبكة التي توفر الاتصالات، مثال عليها الهاتف، أو الطابعة.



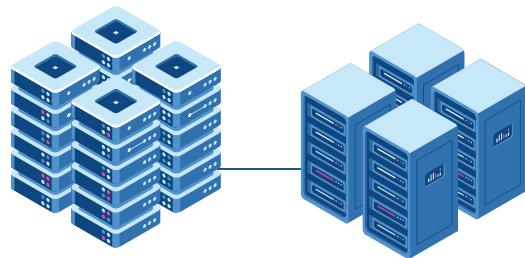
Personal Area Network  
شبكة خاصة



الشبكات التي تسمح بالاتصال للجهاز بشكل لاسلكي .



Wireless Area Network  
الشبكة اللاسلكية



هي شبكة معلوماتية متخصصة تهدف لمشاركة موارد التخزين وتستخدم كيابل عالية السرعة مثل الفايبر .



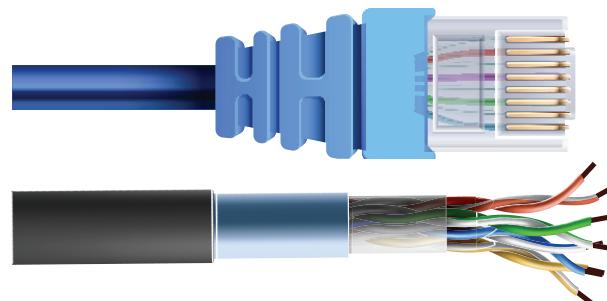
Storage Area Network  
الشبكة التخزينية

## الوسائل المادية ( كيابل الشبكات )

1 - الكيبل المزدوج Twisted Pair Cable

2 - كيبل الألياف البصرية Fiber Optic Cable

3 - الكيبل المحوري Coaxial Cable



### الكيبل المزدوج Twisted Pair Cable

الكيبل الشائع والأكثر استخداما وهو نوعين :

- نوع مغلف ومحمي ( STP ) -

- نوع آخر غير مغلف وغير محمي ( UTP ) -

مثل ( cat5 - cat5e - cat6 )

- قد تجد مكتوب base-T 10 على cat6 أو غيره .

النوع type	السرعة speed
ethernet	10 Mbps
Fast ethernet	10 / 100 Mbps
Gigabit ethernet	10 / 100 / 1000 Mbps

bandwidth  
هي سعة نقل البيانات في الثانية  
الواحدة.

مثل  
Mbps 10  
10 ميقا بت في الثانية  
Mbps 100  
100 ميقا بت في الثانية

# 10 base-T

كيبل مزدوج أو ملفوف  
Twisted Pair

إذا وجدت tx فإن الـ x معناه يدعم  
full duplex - half-duplex

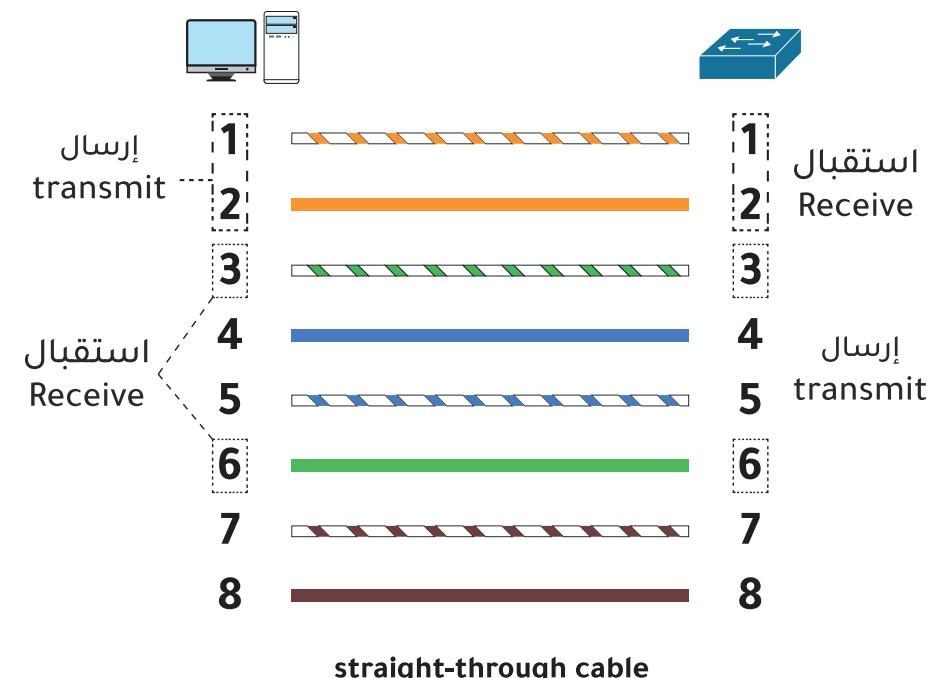
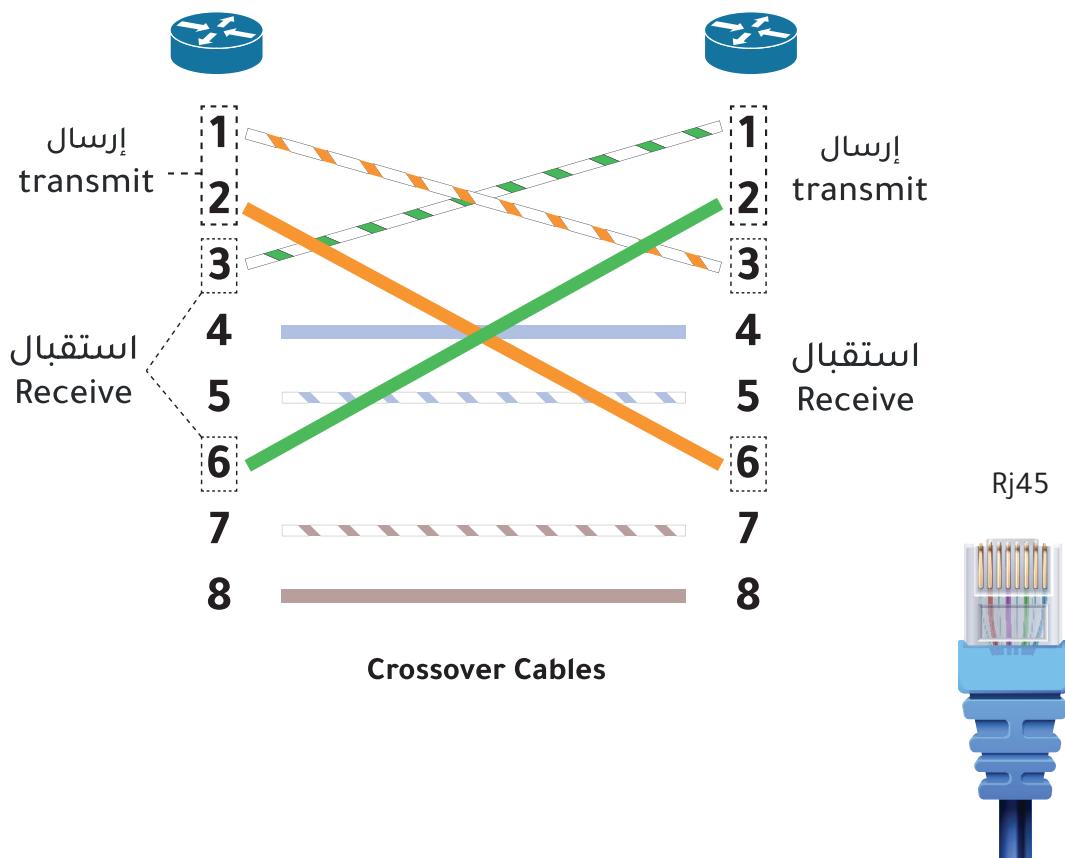
هناك نوعين من التوصيل في كيابل UTP -STP :

A - التوصيل المباشر Straight-Through Cable

يستخدم بشكل أساسى للتوصيل بين جهازى مختلفين من الأجهزة مثل كمبيوتر مع سويفت

B - التوصيل التقاطعى Crossover Cables

يستخدم بشكل أساسى للتوصيل بين جهازى نفس النوع مثل راوتر مع راوتر



## MDI → Auto-MDIX

إرسال  
transmit

يتغير الوضع تلقائيا  
للستقبال  
Receive

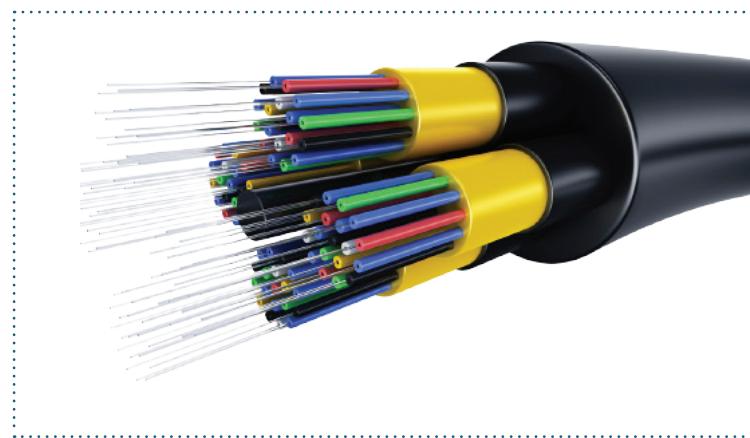
≡ توجد ثلاثة أوضاع (mode) لكروت الشبكة :

MDI : وضع يوجد في أجهزة الكمبيوتر واللاب توب وغيرها

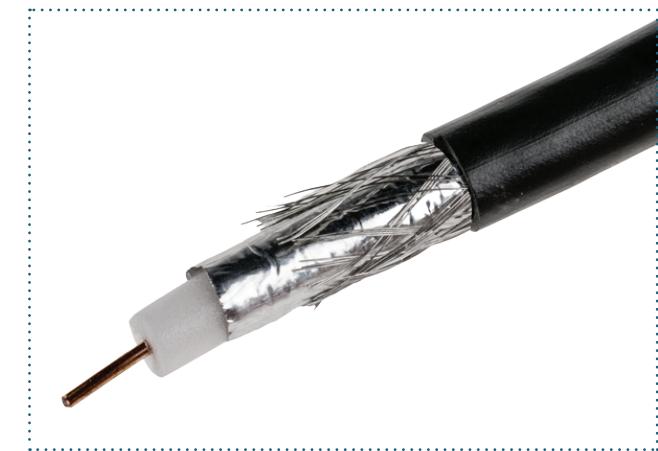
MDIX : وضع يوجد في السويتش والهاب وغيرها

Auto-MDIX هي تقنية موجودة الان في اكثركروت الشبكات وهي تسمح لنا ربط أي كيبل كان نوعه Cross Over أو Straight-Through بجهاز مع اي جهاز اخر لأن البورت بشكل تلقائي سوف يختار ما هو الكيبل الذي يناسبه .

① كيبل الألياف البصرية Fiber Optic Cable  
هي كابلات تستخدم الضوء لنقل المعلومات و البيانات من خلال الزجاج وبسرعات عالية جدا .



② الكيبل المحوري Coaxial Cable  
الكيبل المستخدم في الدش وقد انتهى استخدامه



## البورت والبروتوكول

### Port and Protocol

#### البورت Port

البورت Port : فتحة أو بوابة في أنظمة التشغيل وعدد هذه البوابات ما بين 0 - 65536 بوابة ، وكل بوابة يعمل عليها بروتوكول مختلف عن الآخر.

#### بروتوكول Protocol

البروتوكول هو مجموعة من القواعد والمبادئ التوجيهية لتوصيل البيانات.

- يتم تحديد القواعد لكل خطوة وعملية أثناء الاتصال بين جهازي كمبيوتر أو أكثر حيث يجب على الشبكات اتباع هذه القواعد لنقل البيانات بنجاح .

#### طريقة عمل البروتوكول Protocol :

لكل بروتوكول بنقل الداتا او المعلومات من المستخدم الى الانترنت ومن الانترنت الى المستخدم يلزم وجود بوابة مفتوحة نسماها Port

مثال :

Protocol HTTP + Port 80 بروتوكول تصفح الانترنت يتعامل مع بوابة رقمها 80 ( ثابتة في كل أنظمة التشغيل )

	Protocol	Port	وصف
upload-download	FTP data	20	بروتوكول لنقل الملفات بين الاجهزه
	FTP control	21	
Browsing	HTTP	80	بروتوكول خاص بالتصفح
	HTTPS	443	
remote access	TELNET	23	بروتوكول الدخول او الاتصال عن بعد
	SSH	22	
Domain Name System	DNS	53	نظام يقوم بترجمة أسماء النطاقات من كلمات إلى أرقام تعرف باسم عنوان الـ IP
Dynamic Host Configuration	DHCP Server	67	بروتوكول يستخدم لتوزيع عناوين ايبي للجهزة
	DHCP Client	68	
email	smtp	25	بروتوكول ارسال ايميل
	POP3	110	بروتوكول استقبال الايميل ولابد ان تكون اون لاين لكي تستطيع قراءة الايميل
	imap	143	بروتوكول استقبال الايميل و تحميله لكي تستطيع قراءة الايميل بدون نت

## Network Models

### TCP/IP Model

#### Transmission Control Protocol / Internet Protocol

بروتوكول تم تديثه من وزارة الدفاع الأمريكية وتعتمد معظم عمليات تنفيذ الشبكة التي سيطلب منك إجراؤها على استخدام .TCP/IP

### Osi Model

#### Open Systems Interconnection

### ما هو OSI

هو نظام اصدرته منظمة الايزو iso لكي يستخدم على مختلف انظمة التشغيل المختلفة ( ويندوز - لينكس و غيرها ) وذلك لكي يسهل على انظمة التشغيل أن تtalk معًا بلغة موحدة ، وهذا النظام هو Osi Layers فهو يمثل سبع مراحل تمر من خلالها البيانات من جهاز المرسل مرورا بالشبكة حتى تصلك إلى الجهاز المستقبل .

### فائدة OSI

بعد فهم الطبقات او مراحل ال OSI وكيف تكون البيانات خلالها تستطيع فهم حل المشاكل التي تصادفك على الشبكة . فعندما تعرف كل جهاز او تطبيق او بروتوكول أين يعمل وفي أي مرحلة فعندما تستطيع التوصل لحل المشكلة بطريقة أسرع.

فمثلاً عندما تقوم بعمل Ping على جهاز في الشبكة فتفشل العملية فعلى أي أساس تصلك لسبب المشكلة فهناك عدة أسباب قد تكون احددهما سبب المشكلة مثل الكابل أو كارت الشبكة أو بروتوكول ip / tcp .

## Network Models

### Osi Model

Open Systems Interconnection

- 7 Application | التطبيق
- 6 Presentation | العرض
- 5 Session | الجلسة
- 4 Transport | النقل
- 3 Network | الشبكة
- 2 data link | ربط البيانات
- 1 Physical | المادي

### البروتوكول

DNS , FTP NTP , HTTP , DHCP  
,SMTP , POP3 , IMAP , SSH, Telnet

TCP , UDP

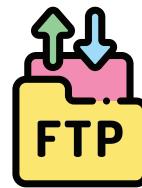
ip , ARP , ICMP

Ethernet

### TCP/IP Model

Transmission Control Protocol /  
Internet Protocol

- 4 Application | التطبيق
- 3 Transport | النقل
- 2 Internet | الانترنت
- 1 الوصول للشبكة  
Network Access



## Application layer - 7

هذه الطبقة المسؤولة عن التطبيقات مثل برمج التصفح Google Chrome وبرامج النقل FTP لنقل الملفات وبرامجه البريد Outlook لرسال واستقبال الايميل .

## Presentation layer - 6

طبقة العرض هي الطبقة المسؤولة عن تهيئة البيانات ليتم اخذ صيغتها وامتدادها المناسب وأيضا ضغط البيانات من قبل المرسل حتى تصل للمستقبل .

و عند استلام المستقبل للبيانات سيتم فك الضغط وكذلك عملية التشفير و فك التشفير .

وظائفها :

### **coding , decoding -**

تعمل كودنل للبيانات بتحويلها من لغة الالة 0 و 1 الى ASCII code والعكس .

### **compression , decompression -**

ضغط البيانات عند الارسال وفكها عند الوصول .

### **encryption , decryption -**

تشفيير البيانات عند الارسال وفكها عند الوصول

### **formatting data -**

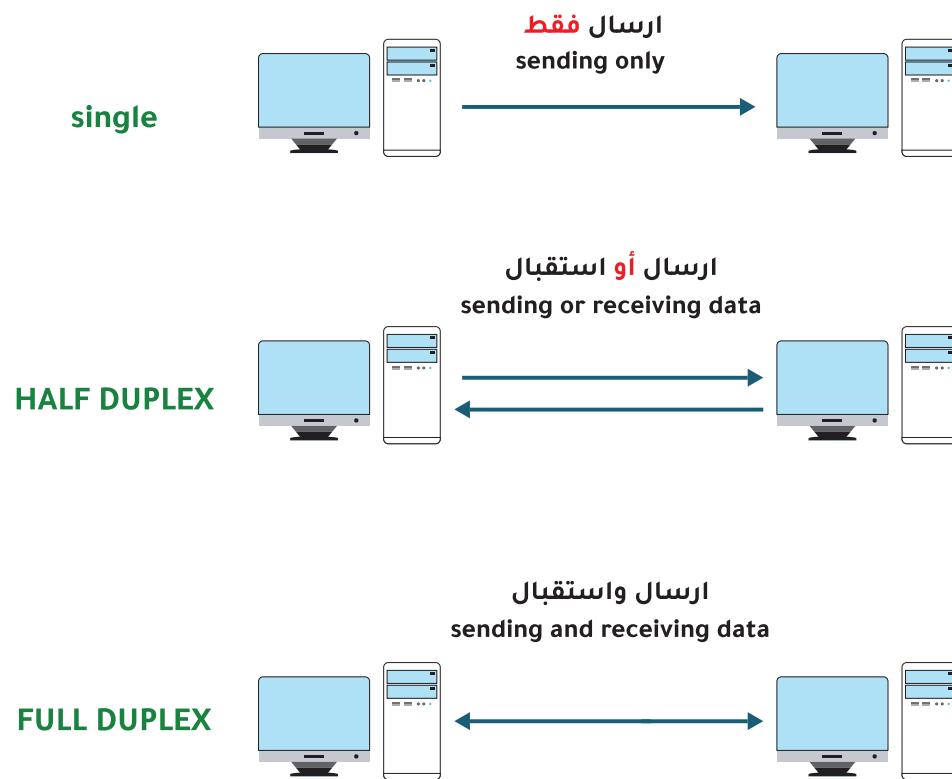
تهيئة البيانات وخذ صيغتها حسب كل امتداد .



## Session layer - 5

هي الطبقة المسؤولة عن جلسات العمل وإدارة وفتح وإغلاق الاتصالات ما بين المستخدمين.

فمثلاً لو أردت فتح عدة مواقع (يوتيوب - فيسبوك - تويتر) فإن الجلسة (session) تفتح اتصال وبورت لكل موقع.



ايضاً هذه الطبقة تقوم بتحديد نوع الاتصال المستخدم:  
- **single** : يعني الإرسال في اتجاه واحد من غير القدرة على الرد مثل التلفاز والراديو حيث انك تشاهد وتسمع ولكن لا تستطيع الرد .

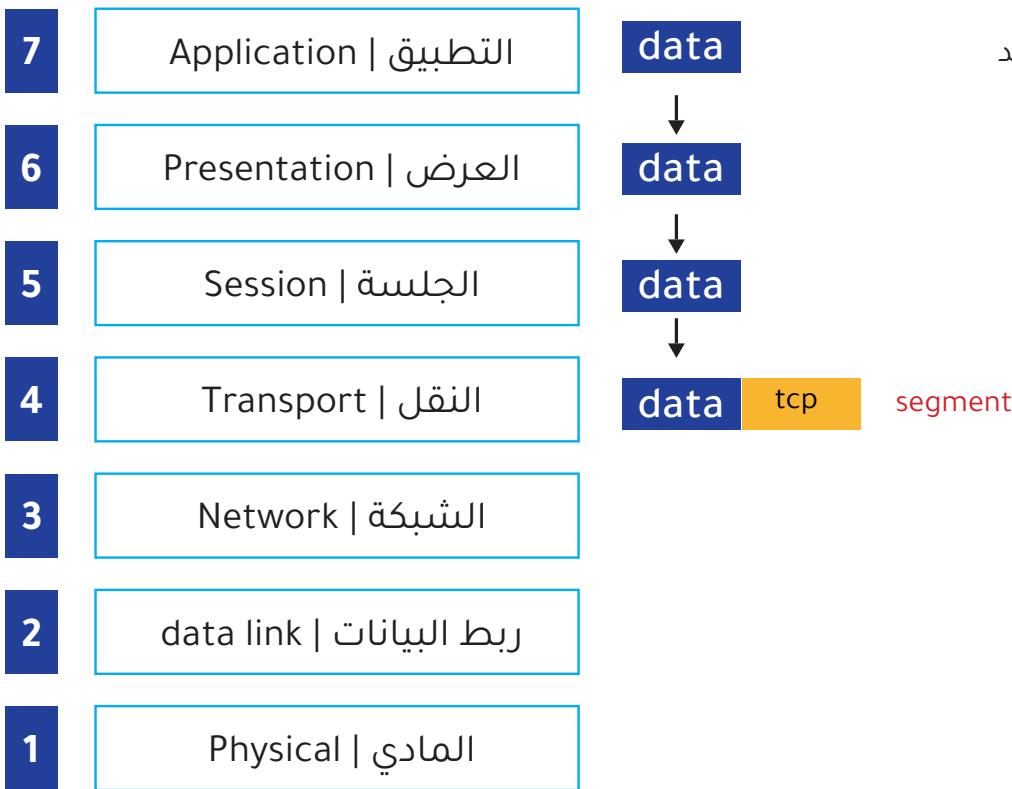
- **half duplex** : يعني الإرسال والاستقبال في نفس الوقت ولكن بشكل متقطع . (أجهزة التواصل اللاسلكي)  
عندما يبدأ أحد الأطراف باستقبال إشارةً ما، فإنه يبقى متظراً حتى يتوقف المرسل عن عملية الإرسال قبل الرد

- **Full duplex** : يعني الإرسال والاستقبال في نفس الوقت وبشكل مباشر مثل الاتصال بصديق فيكون هناك حديث مباشر بين الطرفين

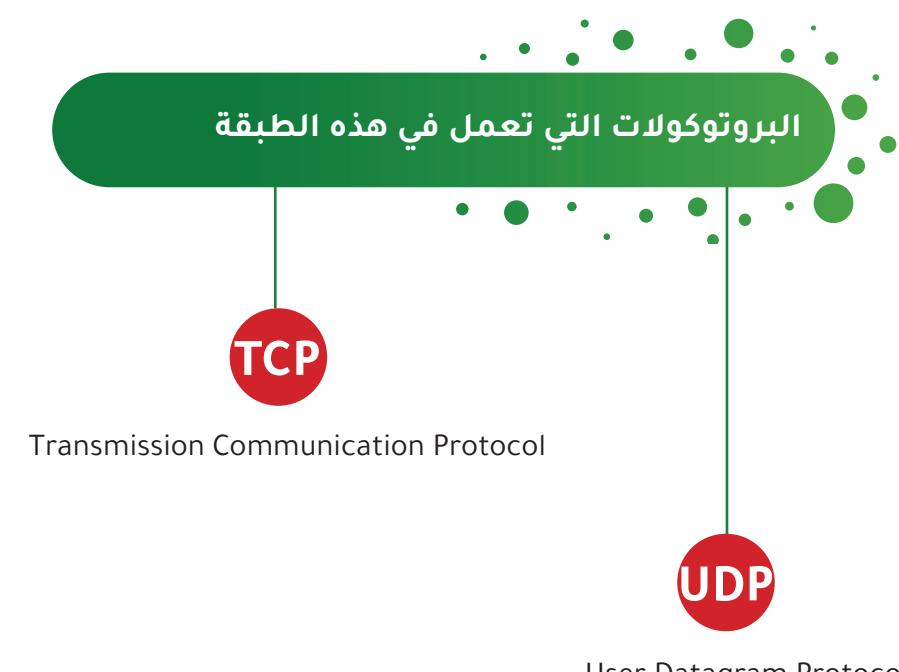
## Transport layer - 4

هي الطبقة المسئولة عن إدارة نقل البيانات ( flow control ) وتصحيح الأخطاء ( error Correction ) ومن ثم تحديد البروتوكول المستخدم في عملية نقل البيانات . وتسمى الداتا في هذه الطبقة بعد اضافة بروتوكول segment ( UDP ) أو ( TCP )

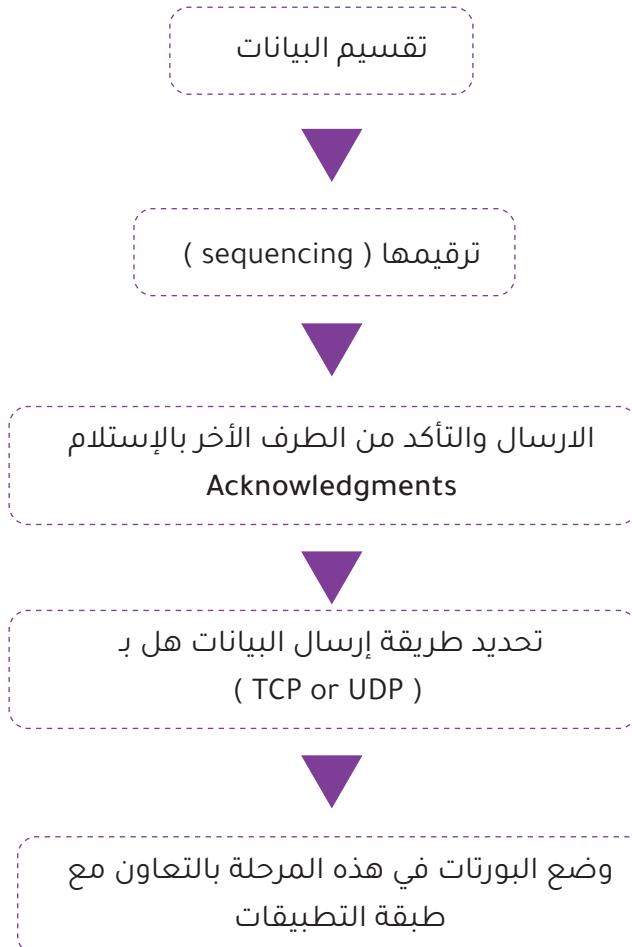
بعض البيانات تستخدم ( TCP ) وهو بروتوكول يقوم بعملية ارسال البيانات ويتأكد من سلامتها وصولها أولاً .



او يستخدم ( UDP ) وهو بروتوكول يقوم بعملية نقل البيانات دون التأكد من وصولها مثل على ذلك التلفاز والراديو



## عملية نقل البيانات ( flow control )



## وظيفة الطبقة



- تتم عملية نقل البيانات ( flow control ) وذلك بتقسيم الداتا ثم ترقييمها ( sequencing ) ثم الارسال والتأكد من الطرف الآخر بالإستلام ( Acknowledgments ) .

- تحديد طريقة إرسال البيانات هل بـ ( TCP or UDP ) .

- يتم وضع البورتات في هذه المرحلة بالتعاون مع طبقة التطبيقات .  
هناك نوعين من البورتات :

- المنافذ المعروفة : هي البورتات المحفوظة لتطبيقات معينة وهو يستخدم للدخول من خلاله على الجهاز الآخر ( 0 إلى 1023 ) .

- اما البورتات الأخرى : ( 1024 إلى 65535 ) تستخدم هذه البورتات من قبل التطبيقات لكي يخرج منها التطبيق إلى الشبكة ثم يصل إلى الجهاز الآخر ليدخل من البورتات السابقة .

وضع البورتات في هذه المرحلة بالتعاون مع طبقة التطبيقات

طرق الاتصال بين جهاز المرسل والمستقبل

### Connectionless

لا يقوم بتأسيس وإعداد اتصال ما بين المرسل و المستقبل بل إنه يرسل رسالة لعنوان المستقبل بدون أي تفاضل أو اتفاق مسبق ويعتمد بروتوكول UDP على هذه الطريقة .

### Connection-Oriented

يقوم بتأسيس وإعداد اتصال كامل و مباشر ما بين المرسل و المستقبل قبل عملية تبادل البيانات ويعتمد بروتوكول TCP على هذه الطريقة.

**UDP**

User Datagram Protocol

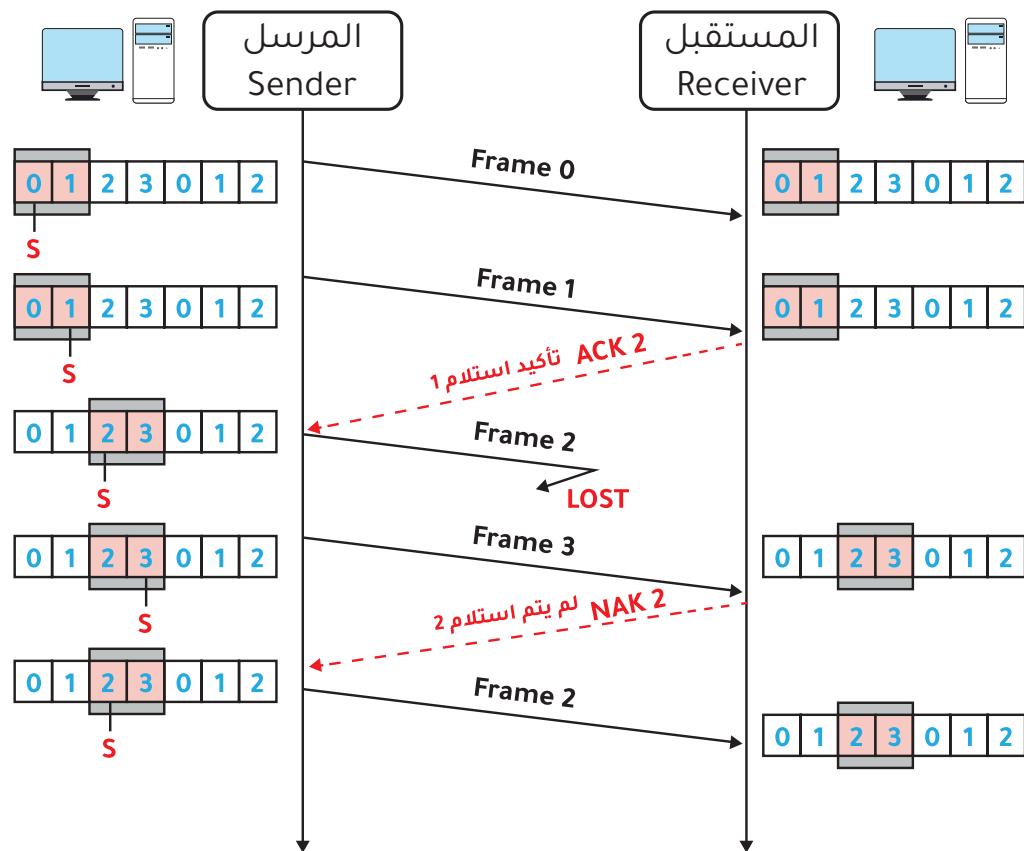
هو بروتوكول لا يتحقق من وصول البيانات المرسلة ولا يحتاج إلى جلسة عمل قبل إرسال البيانات بل ان عليه الارسال فقط مثل التلفاز والراديو .

**TCP**

Transmission Communication Protocol

هو بروتوكول يتحقق من وصول البيانات المرسلة و هو يحتاج إلى جلسة عمل قبل إرسال البيانات إلى الجهاز الآخر و تسمى هذه العملية **Three Way handshake** ، و من خلال هذه العملية يقوم بناء جلسة عمل ما بين الجهاز المرسل و المستقبل .

### عملية ارسال البيانات بين الجهازين عبر بروتوكول TCP

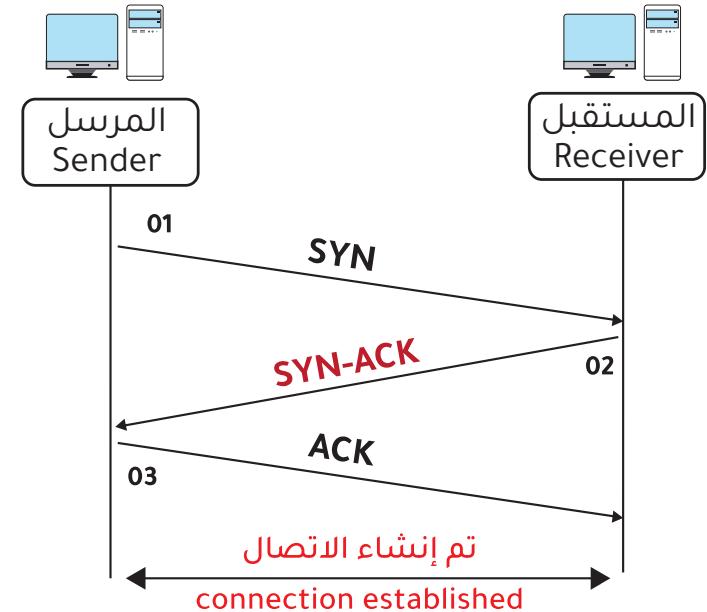


### عملية المصادقة الثلاثية Three Way handshake

- يقوم الجهاز A بإرسال حزمة تتضمن إشارة تدعى SYN (إختصار SYNchronize) إلى الجهاز B.

- تصل الحزمة إلى الجهاز B فيرد عليهما بإرسال حزمة تتضمن SYN-ACK (إختصار SYNchronize-ACKnowledge) إلى الجهاز A.

- عندما يصل الرد إلى الجهاز A، يعيد إرسال حزمة أخرى مع إشارة ACK إلى الجهاز B، إيذاناً باتمام التفاوض وعندها يتم إنشاء الاتصال Connection Established



## Network layer - 3

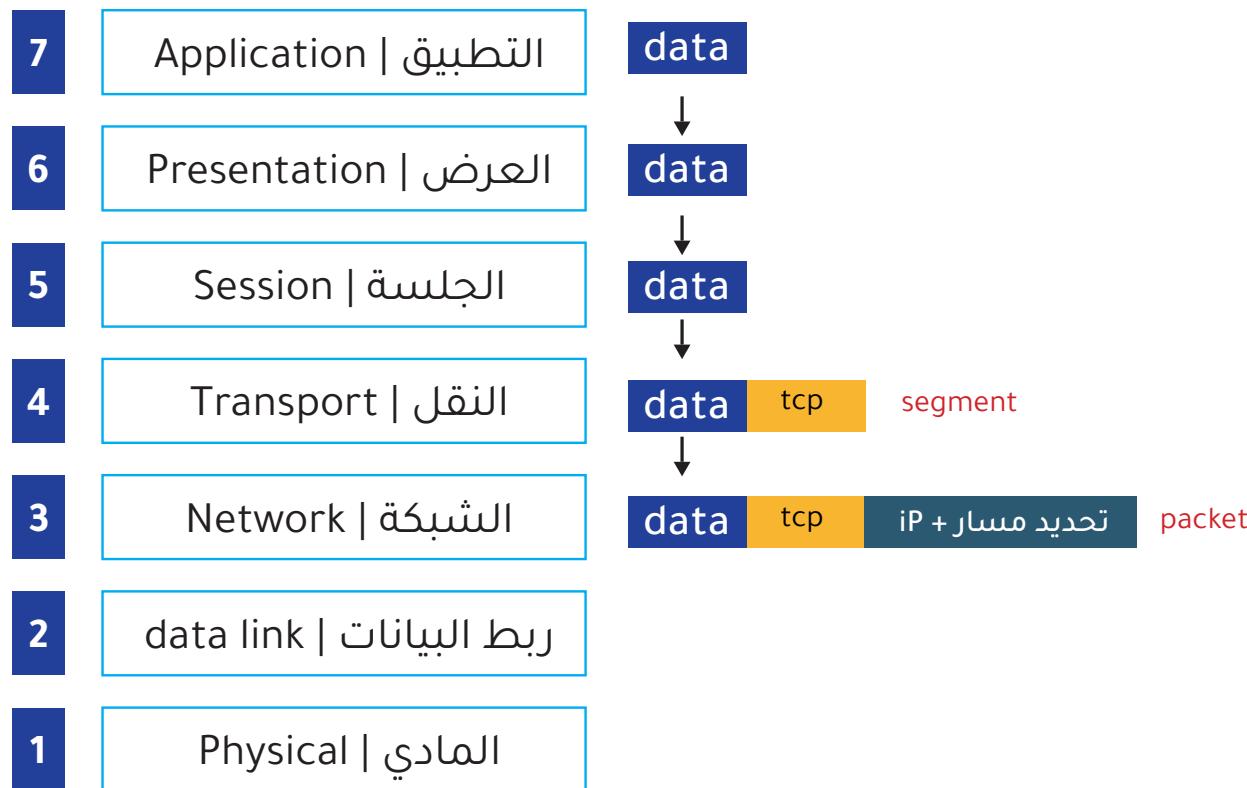
بعد أن تنتقل البيانات أو الداتا من الطبقة السابقة Transport layer وهي على شكل

segment فتحول هنا الى شكل (packet) بعد :

1- إضافة IP جهاز المرسل و جهاز المستقبل .

2- تحديد المسار المستخدم في نقل البيانات وهو ما يسمى بالتوجيه (routing)

وذلك طبقاً للبروتوكول المستخدم بين الراوتر في الشبكة مثل ospf او rip او غير ذلك .



الجهاز او الهاردوير الذي يفهم ويتعامل مع هذه الطبقة هو الراوتر



الجهاز او الهاردوير الذي يفهم ويعامل مع هذه الطبقة هو السويتش

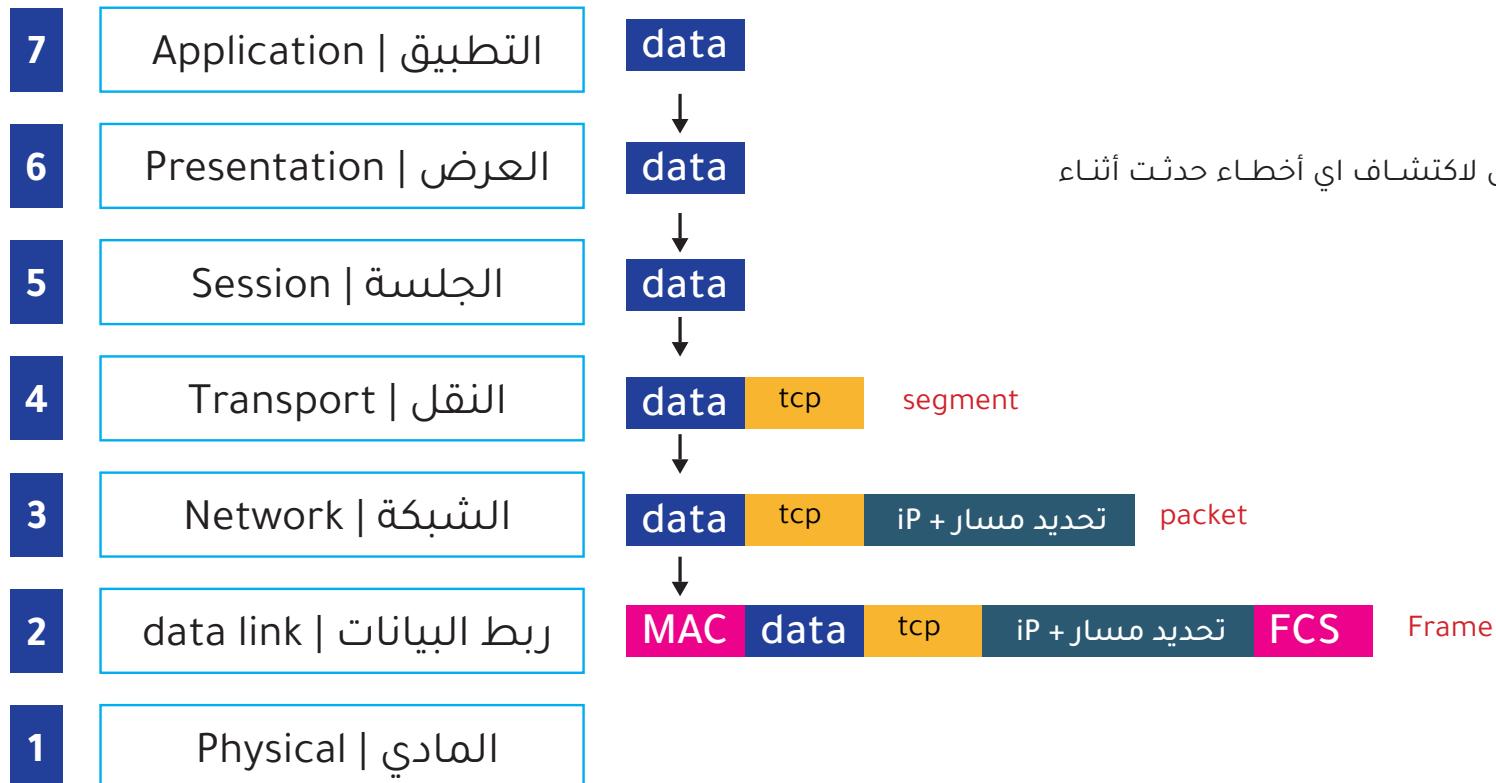


data link layer - 2

تسمى البيانات أو الداتا في هذه الطبقة بـ فريم (Frame) وسميت بهذا الاسم لأنها تضع للباكيت القادمة من طبقة الشبكة رأس (header) . وذيل (trailer)

## الرأس مكون من :

- طبقة التحكم المنطقية LLC logical link control
  - عنوان الماك ادرس Mac Address ( للمرسل والمستقبل )



يتم استخدامه من الجهاز المستقبل لاكتشاف اي اخطاء حدثت أثناء الارسال error detection

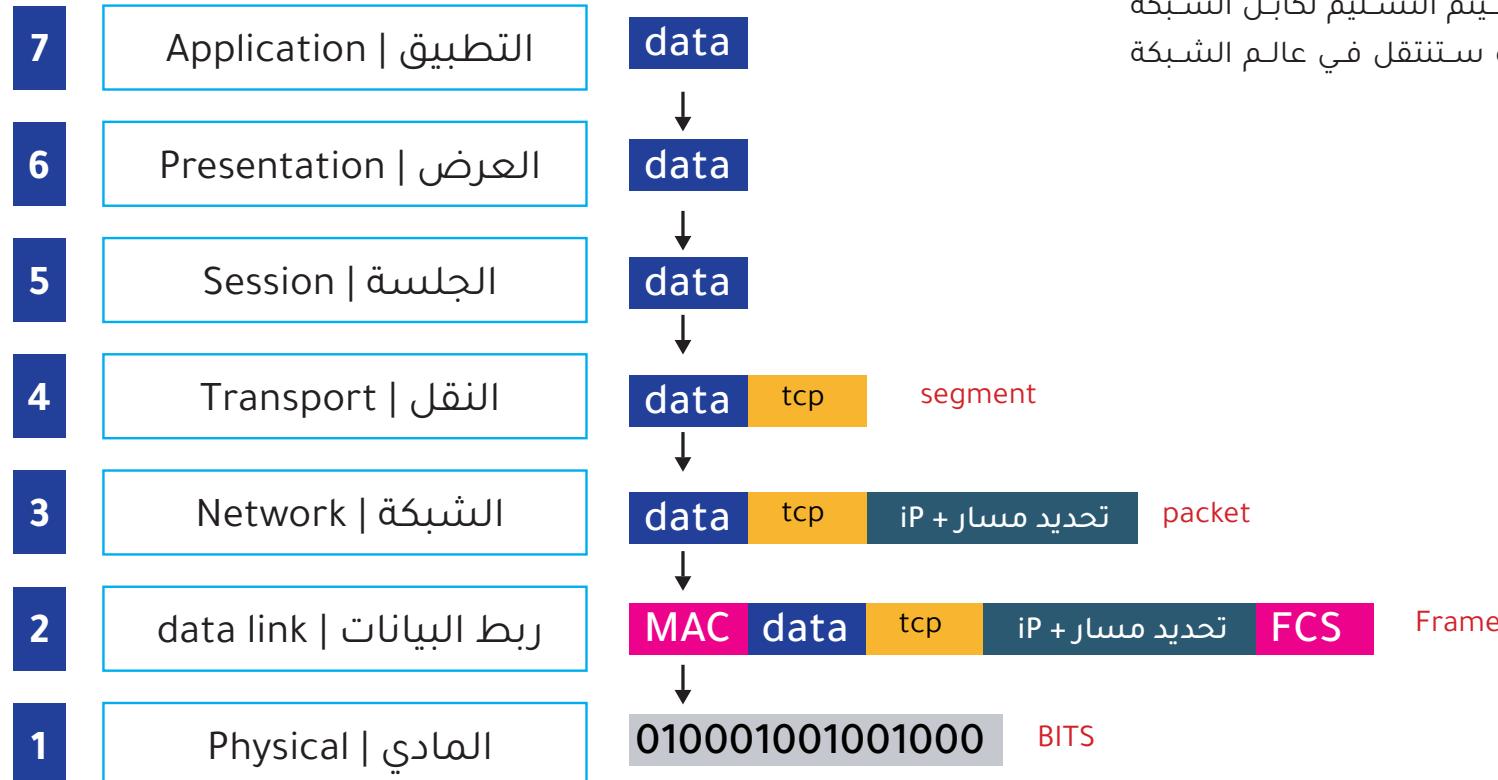
والذيل مكون من :

frame check sequence ( fcs )

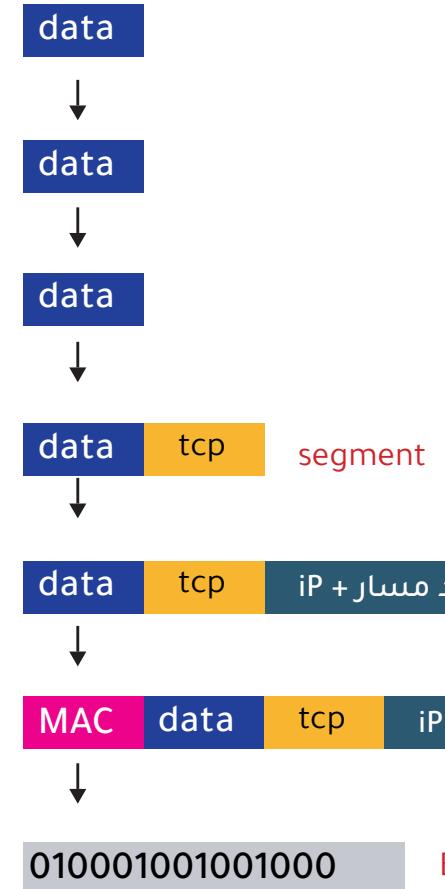
## Physical layer - 1

وهي المراحل التي يتم فيها تحويل البيانات أو الdata (Data) إلى اشارات كهربائية ( Bits ) ويقوم بهذه الوظيفة كل من كارت الشبكة والمودم .

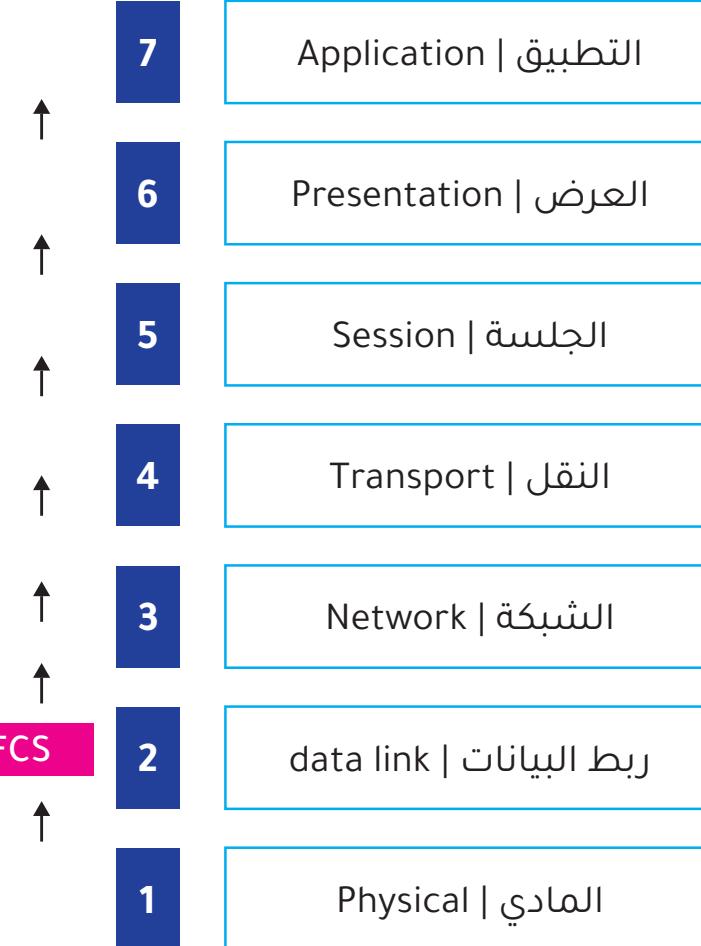
وبعد الانتهاء من هذه العملية سيتم التسليم ل CABL الشبكة المتوصلاً في كرت الشبكة وبعد ستنقل في عالم الشبكة للوصول إلى الجهاز المطلوب .



## الجهاز المرسل



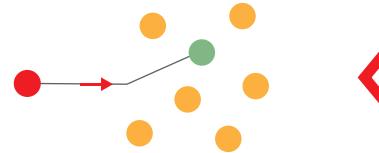
## الجهاز المستقبل



عند الوصول لجهاز المستقبل تحدث  
العمليات ولكن بالعكس

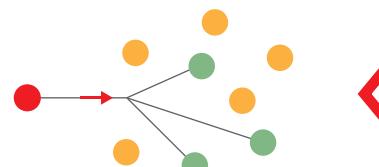
## طرق إرسال البيانات في داخل الشبكات

### Methods of Sending Data in the Network



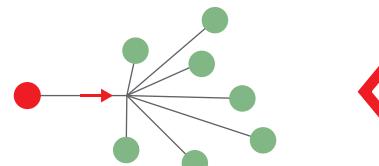
**Unicast**

الإرسال يتم بين مرسل واحد  
ومستقبل واحد فقط أي انه يتم  
اخذ البيانات وارسالها الى الجهاز  
المطلوب فقط.



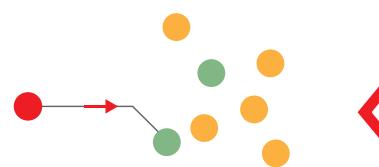
**Multicast**

إرسال البيانات من الجهاز المصدر  
إلى مجموعة محددة من الأجهزة في  
نفس الوقت.



**Broadcast**

وتعني ارسال البيانات لجميع الاجهزه  
في الشبكة



**Any cast**

فيه يتم ارسال البيانات من الجهاز  
المرسل الى اقرب جهاز مستقبل  
حسب قواعد معينة مثل المسافة او  
المسار .

### نطاق البث

#### Broadcast Domain

هو عبارة عن مجموعة أجهزة متصلة في شبكة واحدة تحت نطاق واحد و تحت فئة واحدة من عناوين الـ IP و تكون نهاية الـ Broadcast Domain عند أخرى نقطة للوصول لجهاز الراوتر .

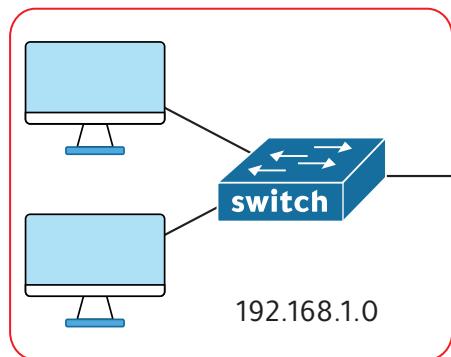
### الفرق بين الـ Broadcast Domain و الـ Collision Domain

### نطاق التصادم

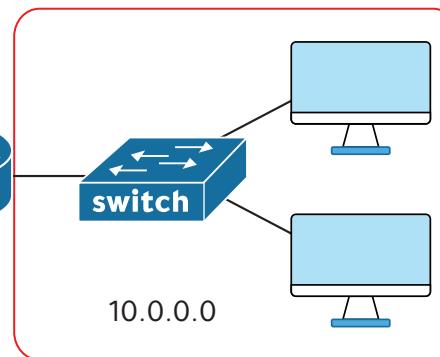
#### Collision Domain

هو عبارة عن التصادمات التي تحصل عندما تلتقي البيانات في مسار واحد مما يسبب بطء و اختناق في الشبكة .

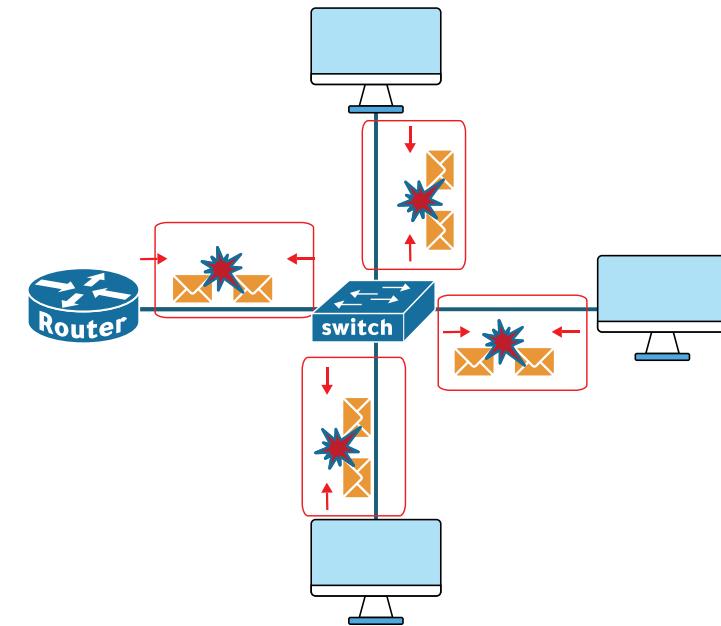
#### Broadcast Domain A



#### Broadcast Domain B

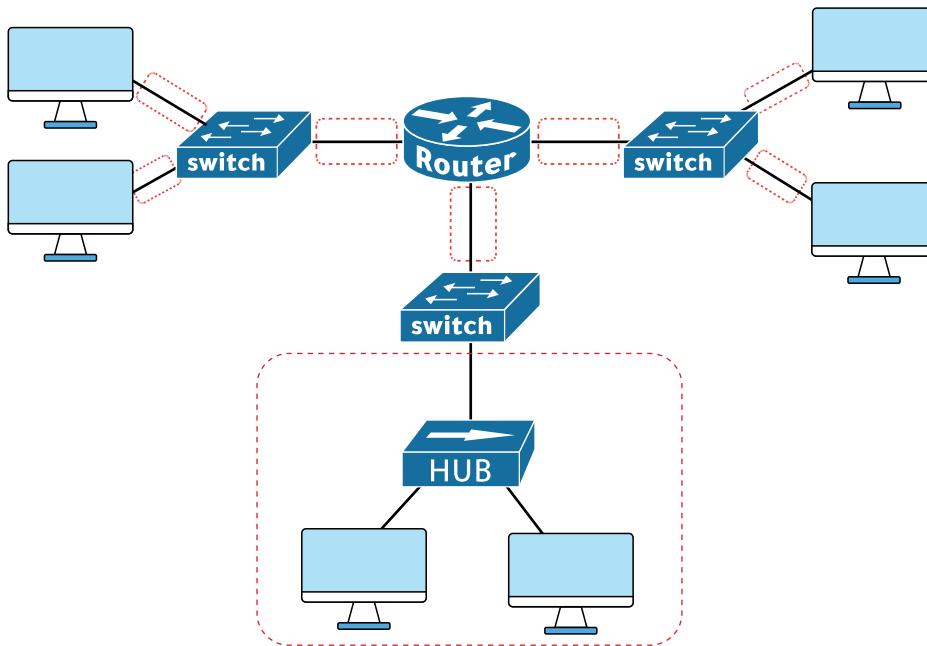


لاحظ هنا نطاق البث في شبكة الـ 10.0.0.0 ، فلو تم ارسال رسالة بروكاست من جهاز الكمبيوتر فان الرسالة سوف تصل لجميع المتصلين في شبكة الـ 10.0.0.0



**ملاحظة:** مع إصدارات حديثة لبروتوكول Ethernet تم القضاء على مشكلة التصادم نهائياً ، فقط تم استخدام تقنية تمكن الوصلة من إرسال و استقبال البيانات في نفس الوقت ، تسمى هذه الطريقة بـ Full Duplex

### Collision Domain = 8



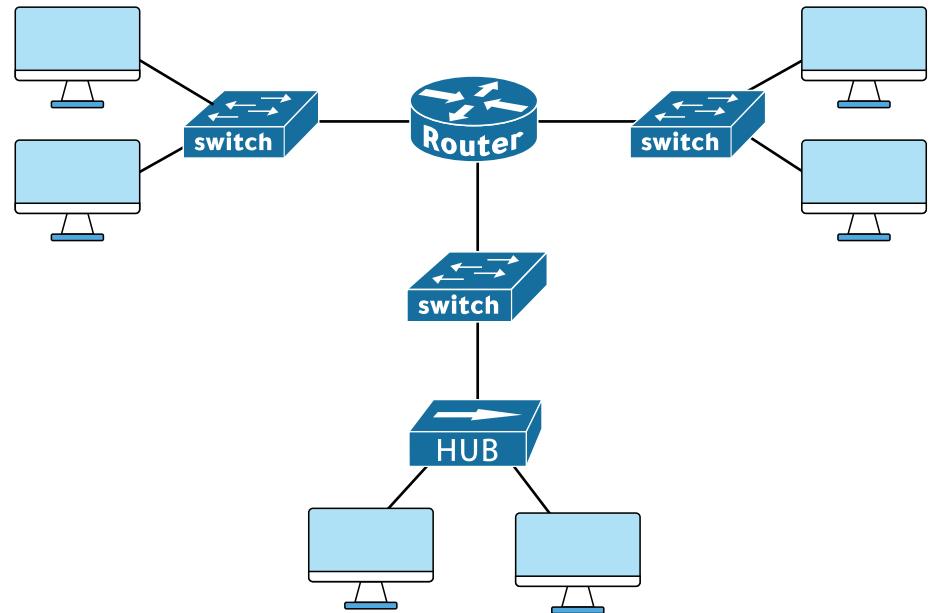
### ملاحظة:

في حالة إرسال جهازين أو أكثر في نفس الوقت فإن:  
1- أجهزة الراوتر والسويتش والجسر تفصل مجالات التصادم

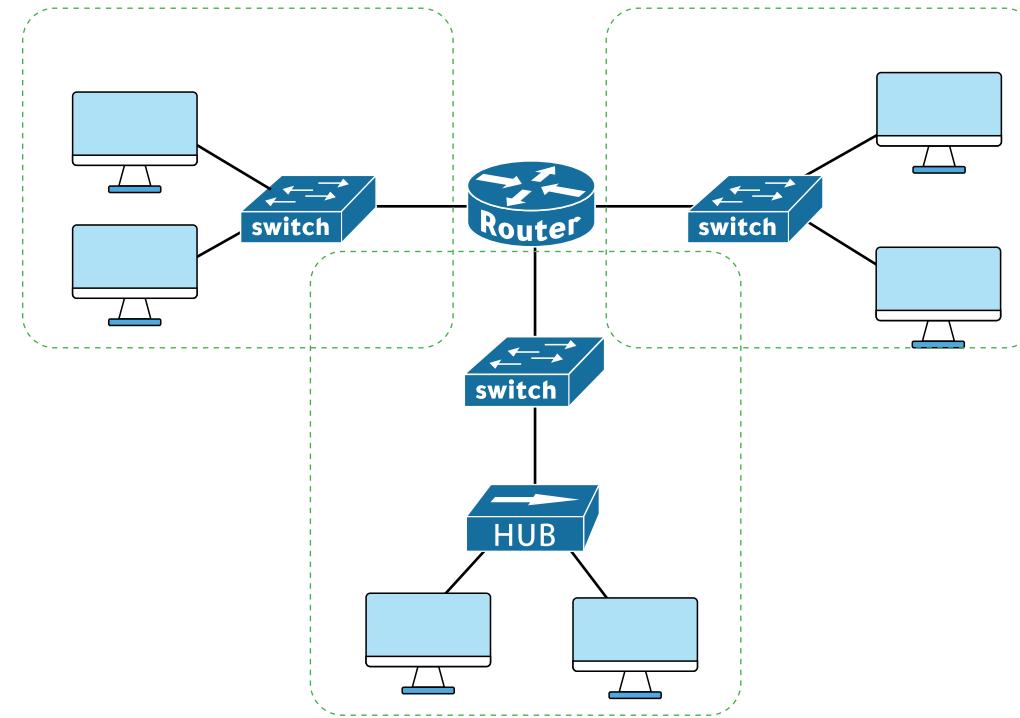
Collision Domain عند منفذها .

2- أجهزة الموزع Hub والمكرر Repeater تفصل مجالات التصادم  
Collision Domain عند منفذها بل يجعلها مجال تصادم واحد .  
يعنى أن الرسالة التي سوف تدخل على أحد منافذ الموزع سوف  
تصطدم بالرسالة القادمة من المنفذ الآخر

**مثال:** أوجد عدد نطاق البث Broadcast Domain وعدد مجالات التصادم في الشكل التالي ؟

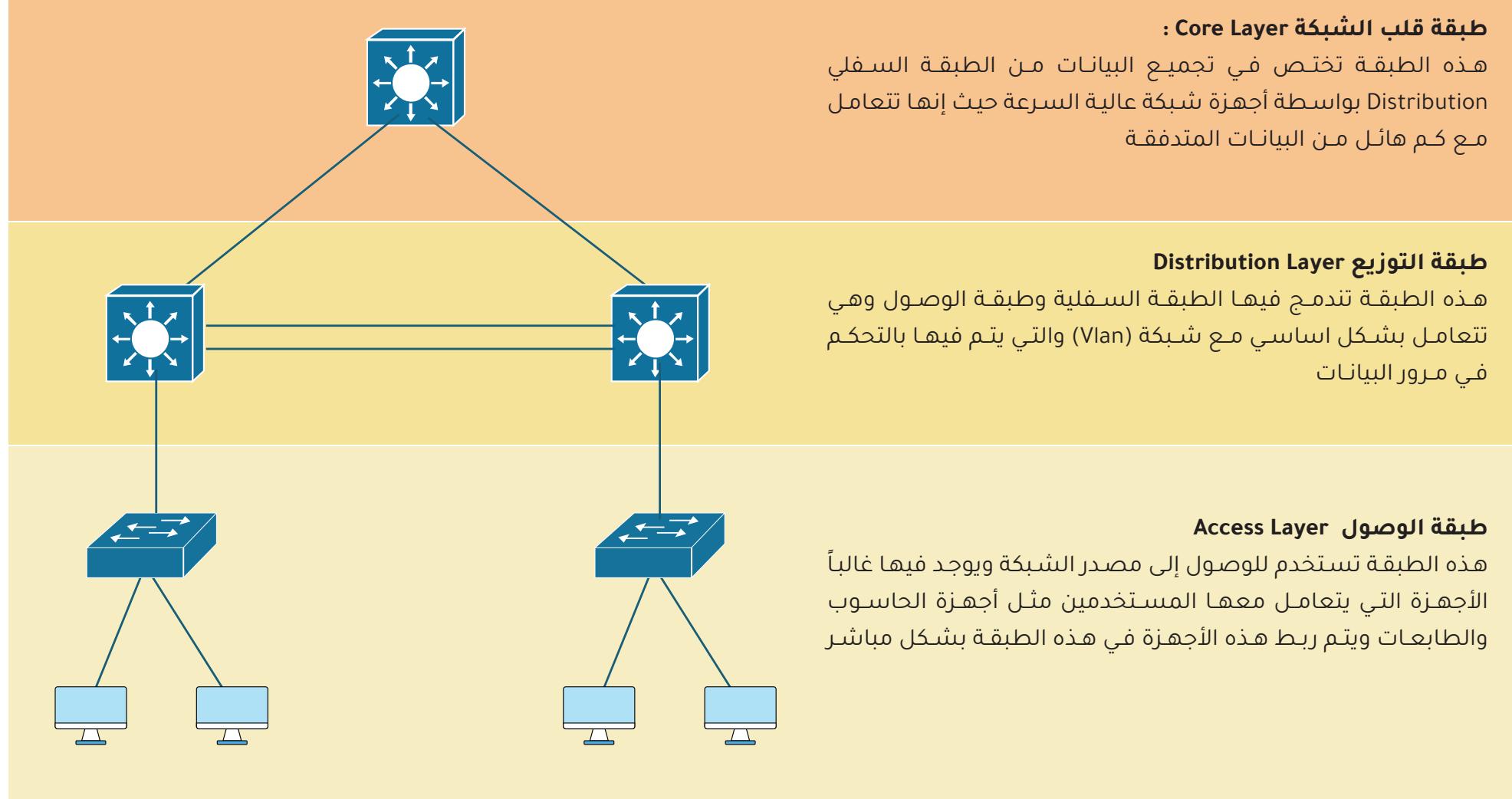


Broadcast Domain = 3



## التصميم الهرمي لشبكات سيسكو

Cisco Three Layers Hierarchical Model



### طبقة قلب الشبكة : Core Layer

هذه الطبقة تختص في تجميع البيانات من الطبقة السفلية Distribution بواسطة أجهزة شبكة عالية السرعة حيث إنها تعامل مع كم هائل من البيانات المتداولة

### طبقة التوزيع Distribution Layer

هذه الطبقة تندمج فيها الطبقة السفلية وطبقة الوصول وهي تعامل بشكل اساسي مع شبكة (Vlan) والتي يتم فيها بالتحكم في مرور البيانات

### طبقة الوصول Access Layer

هذه الطبقة تستخدم للوصول إلى مصدر الشبكة ويوجد فيها غالباً الأجهزة التي يتعامل معها المستخدمين مثل أجهزة الحاسوب والطابعات ويتم ربط هذه الأجهزة في هذه الطبقة بشكل مباشر

الإصدار السادس  
ip v6

## IP Address

له إصدارين

الإصدار الرابع  
ip v4

### ipv4 Address

هي عناوين يتم توزيعها على الحواسيب و يكون لكل حاسوب عنوان على الشبكة ليس قادراً على مشاركة باقي الحواسيب الأخرى التي على الشبكة .  
منظمة الایانا IANA هي مسؤولة عن الأسماء حيث قامت بتقسيم IPv4 إلى كلاسات وحددت لكل كلاس بداية ونهاية.

الفئة Class	المدى Range	
A	10.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D عناوين محفوظة للبث المتعدد الخاص في الشبكة	224.0.0.0	239.255.255.255
E عناوين محفوظة للأبحاث	240.0.0.0	255.255.255.255

أجهزة الكمبيوتر لا تفهم الكلمات أو الأرقام بالطريقة التي يتعامل بها البشر لأن أجهزة الحاسوب لا تفهم إلا **الصفر والواحد** (نظام ثنائى Binary) .  
- يتم تمثيل كل شيء من خلال إشارة كهربائية ثنائية Binary تسجل في إحدى الحالتين : **تشغيل** أو **إيقاف** وذلك لفهم البيانات المعقدة في ملف ثنائى Binary

0      1  
off      on  
إيقاف      تشغيل

## ≡ العنوان المنطقية في الاصدار4 ipv4

### Public ip Address العنوان العام

ثانياً

العناوين العامة هي التي تستطيع الخروج فيها الى شبكات الانترنت .  
ويتم منح هذه العناوين من قبل مزود الخدمة .

الفئة Class	المدى Range	
A	1.0.0.0	9.255.255.255
B	128.0.0.0	172.15.255.255
	172.32.0.0	191.255.255.255
C	192.0.0.0	192.167.255.255
	192.169.0.0	223.255.255.255

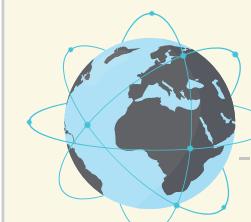
### private ip address العنوان الخاصة

أولاً

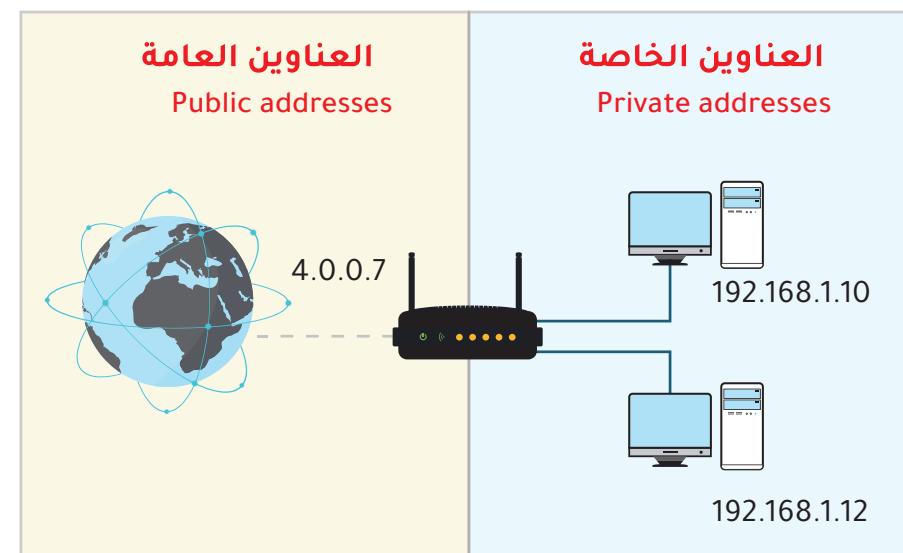
العناوين الخاصة يتم استخدامها في الاجهزة التي في الشبكة المحلية ولا يمكن الخروج بها الى الانترنت .

الفئة Class	المدى Range	
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

### العناوين العامة Public addresses



4.0.0.7



### العناوين الخاصة Private addresses

## عنوان البث المتعدد Broadcast

ثالثاً

255.255.255.255

## عنوان كرت الشبكة الداخلي loop back interface

رابعاً

127.0.0.0 - 127.255.255.255

هذه العناوين تم تخصيصها لكرت الشبكة الداخلية ولا يمكن استخدامها في عنونة الأجهزة

## عنوان APIPA

خامساً

169.254.0.0

هذا العنوان يأتي بشكل مؤقت في حال عدم دخال عنوان للجهاز وفي حال عدم وجود التوزيع التلقائي للبيهات عبر تقنية بروتوكول ار DHCP

**النظام السادس عشر (Hexadecimal)**

هو نظام ذو الأساس 16 و الذي يتكون من 16 حرف ورقم . وهي كال التالي :

( 0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F )

- يسمى أيضا ب base 16 .

- قد تجد أمام الرقم هذه البدائة (0x) مثل 0x45A8D وتعني ان هذا الرقم من النظام السادس عشر .

- نجد استخدام هذا النظام في الأبيي الاصدار السادس IPv6 وايضا في الماك ادرس Mac address .

**Binary** = **النظام الثنائي**  
**Decimal** = **النظام العشري**  
**Hexadecimal** = **النظام السادس عشر**

**النظام الثنائي Binary System**

هو نظام ذو الأساس 2 يعني أن هناك رقمين فقط 1 و 0

- يسمى أيضا ب base 2

- قد تجد أمام الرقم أو الرقمين 0 و 1 هذه البدائة (0b) مثل 0b1011 وتعني ان هذا الرقم من النظام الثنائي .

- في عنوان الابيي ipv4 سنجده في الخانة بشكل 0 أو 1

00000000.00000000.00000000.00000000

11111111.11111111.11111111.11111111

**Decimal System**

هو النظام ذو الأساس 10 و الذي يتكون من عشرة أرقام تمثل به الأعداد مهما كبرت وهي : (0.1.2.3.4.5.6.7.8.9)

- يسمى أيضا ب base 10 .

- قد تجد أمام الرقم هذه البدائة (0d) مثل 0d223 وتعني ان هذا الرقم من النظام العشري .

في عنوان الابيي ipv4 سنجده في الخانة بشكل ارقام تبدأ من 0 حتى 255 .

0.0.0.0

255.255.255.255

النظام العشري Decimal System	النظام الثنائي Binary System	النظام السادس عشر (Hexadecimal)
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

## ≡ شرح عنوان الـ ipv4

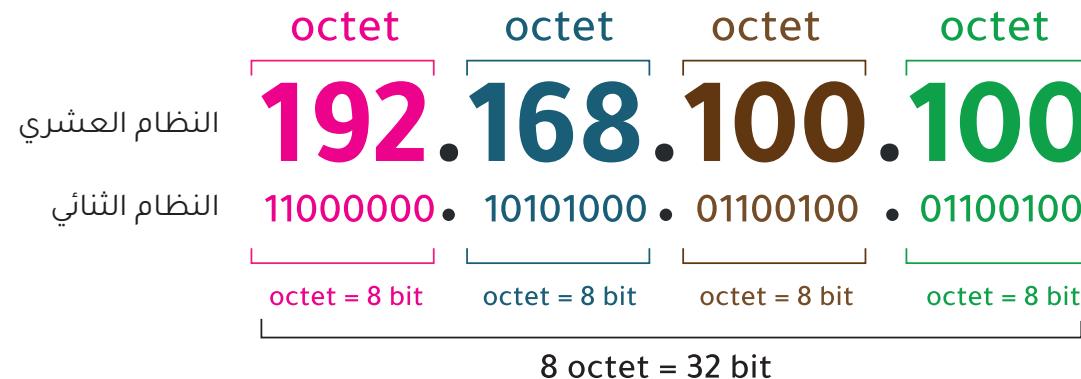
- يكون نظام العناوين في الـ ipv4 على هيئة نظامين :  
النظام العشري Decimal System أو النظام الثنائي

- يتكون عنوان الـ ipv4 من 4 خانات كل خانة يطلق عليها اوكتت octet .

الاوكتت الواحد فيه 8 بت

اوكتات فيها 32 بت

- كل بت (bit) من الرقم الثنائي له إحتمالين : 1 أو 0



## التحويل من النظام العشري إلى النظام الثنائي

11000000.10101000.01100100.01100100

← 192.168.100.100

هذا الجدول الذي سوف نطبق عليه اي تحويل للنظام الثنائي **Binary** او النظام العشري **Decimal System**

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

→ نبدأ من اليسار

اذا الرقم الموجود في الـ ip أكبر أو يساوي رقم الجدول نضع 1 وإذا أصغر نضع 0

الشرح

192.168.100.100

الباقي 64 وهو مساوي للقيمة التي بعدها .  
نضع 1 وبكذا انتهينا والخانات المتبقية تكون اصفار

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

سوف نحول كل خانة (أوكتت) من الـ ip :  
192 اكبر من 128 نضع رقم 1 ونطرحه من 192  
 $192 - 128 = 64$

128	64	32	16	8	4	2	1
1							

الخانة الأولى (192) = 11000000

192.168.100.100

الباقي 40 أصغر من 64 نضع 0 وننتقل للخانة اللي بعدها

40 أكبر من 32 نضع 1 ونطرح  $40 - 32 = 8$

8 أصغر من 16 نضع 0 وننتقل للذى بعده

= 8 نضع 1 وبكذا لم يتبقى شي ونكتب الباقي اصفار

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

أكبر من 128 نضع رقم 1 ونطرح

$$168 - 128 = 40$$

128	64	32	16	8	4	2	1
1							

$$10101000 = 168$$

الخانة الثالثة (100)

الخانة الرابعة (100)

بالنظام العشري

192.168.100.100

بالنظام الثنائي

11000000.10101000.01100100.01100100

192.168.100.100

نضع 0 وننتقل للآخرى

$36 = 64 - 100$  نضع 1 ونطرح (64) < 100

$4 = 32 - 36$  نضع 1 ونطرح (32) < 36

(16) > 4 نضع 0 وننتقل للآخرى

(8) > 4 نضع 0 وننتقل للآخرى

(4) = 4 نضع 1 وبكذا لم يتبقى شي ونكتب الباقي اصفار

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

## التحويل من النظام الثنائي إلى النظام العشري

**192.168.100.100**

**11000000.10101000.01100100.01100100**

الشرح

**ملاحظة :**

لو جمعنا الأرقام اللي باللون الأخضر:

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

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$$

هذا هو المدى (range) للخانة الواحدة

0.0.0.0

إلى

255.255.255.255

الطريقة سهلة جدا

مثل اعطانا هذا الرقم **11010011**  
نقوم بتوزيعهم بالجدول بداية من اليسار  
نقوم بجمع الأرقام التي تحتها العدد **1**

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

$$128 + 64 + 16 + 2 + 1 = 211$$

اذاً الرقم هو **211**

### ◆ معرفة عنوان الشبكة

- يتم معرفة عنوان الشبكة عبر معرفة قناع الشبكة (Subnet Mask) .
- يتكون قناع الشبكة (Subnet Mask) من 32 bit من النظام الثنائي أو النظام العشري .
- بعد استخدام قناع الشبكة (Subnet Mask) تستطيع اجهزة الحاسب معرفة اي جزء من الـ IP address هو عنوان للشبكة وأي جزء هو عنوان للأجهزة (Host) .

هذا الـ Subnet Mask يستخدم لكي نعرف كم Bit من الـ IP address يمثل عنوان الشبكة وكم Bit يمثل عنوان الـ Host.

**255.0.0.0**

النظام العشري

**11111111.00000000.00000000.00000000**

النظام الثنائي



**N.H.H.H**

**10.0.0.0**

**255.0.0.0**

عندما تجد في Subnet Mask الرقم 255 فإن هذا يدل على ان الجزء المقابل له هو ثابت ويكون عنوان للشبكة .

### شرح فئات أو كلاسات الـ ipv4

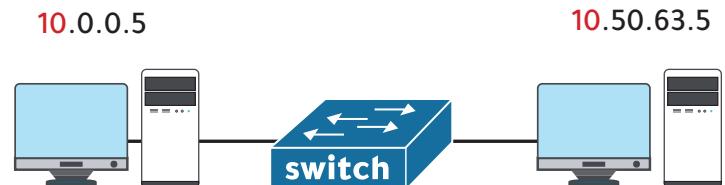


**N = NETWORK**

عنوان الشبكة ويكون ثابت

**H = HOSTS**

يقصد به العناوين المتاحة في الشبكة والتي سوف تتوزع على الأجهزة .



هنا يستطيع الجهازين التواصل مع بعضهم البعض لأن الجزء الثابت متساوي في كل العنوانين .

N = NETWORK

عنوان الشبكة ويكون ثابت

H = HOSTS

يقصد به العناوين التي سوف تتوزع على الأجهزة وهي عناوين متغيرة



**N . N . N . H**  
**192.168.0.0**  
**255.255.255.0**

عندما تجد في Subnet Mask الرقم 255 فإن هذا يدل على أن الجزء المقابل له هو ثابت ويكون عنوان للشبكة.



**N . N . H . H**  
**172.16.0.0**  
**255.255.0.0**

## ≡ قناع الشبكة ≡

**قناع الشبكة هو اللي يحدد لنا :**

1- **عنوان الشبكة**

2- **Hosts** : عدد الأجهزة الممكحة في الشبكة

مثله لدينا هذا العنوان مع الـ Subnet Mask

192.168.1.0

255.255.255.0

255.255.255.0

نكتب هذا القناع بنظام الباینری Binary

1111111.1111111.1111111.00000000

كم عدد الوحدات ( رقم واحد ) اللي باللون الأحمر ؟

الإجابة 24

نستطيع كتابة هذا الرقم مع الـ ip ويكون بعد علامة السلاش (/) : prefix ويطلق عليه

192.168.1.0 /24

يعني هذا ان الايبي هو 192.168.1.0 وقناع الشبكة هو 255.255.255.0

1111111.1111111.1111111.00000000

( subnet mask ) هو عدد الوحدات في قناع الشبكة ( prefix )

192.168.1.0 / 24

( subnet mask ) يكتب كاختصار عن قناع الشبكة

255.255.255 . 0

1111111.1111111.1111111.00000000

الفئة Class	المدى Range		قناع الشبكة Subnet Mask	Prefix
A	10.0.0.0	10.255.255.255	255.0.0.0	/ 8
B	172.16.0.0	172.31.255.255	255.255.0.0	/ 16
C	192.168.0.0	192.168.255.255	255.255.255.0	/ 24

## تمرين

ما هو الـ Subnet Mask لهذا العنوان

؟ 192.168.8.3 /28

## مثال

ما هو الـ Subnet Mask لهذا العنوان

؟ 192.168.10.5 /27

المعروف ان عندنا 32 خانة تمثل عدد الاصفار والوحيد.

نقوم بكتابه 27 وحيد (رقم واحد) والباقي اصفار

11111111.11111111.11111111.11100000

وقد تعرفنا ان الخانة اللي كلها وحيد = 255  
اذاً بقي علينا الخانة الاخيرة نوزعها على الجدول

وبالرجوع للجدول وتحويلها الى عشري

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

$$128 + 64 + 32 = 224$$

اذن الـ Subnet Mask هو :

255.255.255.224

## 2 - معرفة عدد الشبكات Networks

**مثال 27**

نحسب عدد الوحدات في الخانة اللي فيها أصفار

11111111.11111111.11111111.**11100000**

عدد الوحدات = n

$$n = 3$$

### قانون معرفة عدد الشبكات

$$2^n = \text{عدد الشبكات}$$

$$2^3 = 8$$

اذاً عندنا 8 شبكات

**طريقة معرفة : عدد الأجهزة - عدد الشبكات -**  
**عنوان الشبكة ( Network id )**

**1 - معرفة عدد الأجهزة hosts**

**مثال 27**

لدينا 27 وحدة ونعرف ان عدد البتات الكلي للبي بي  
32 بت

$$32 - 27 = 5 \text{ bit}$$

اذن عندنا 27 وحدة و 5 أصفار

11111111.11111111.11111111.**11100000**

### قانون معرفة الأجهزة

$$2^h - 2 \geq H$$

**h = (number of 0 bit)**

**H = (hosts)**

$$2^5 - 2 = H$$

$$32 - 2 = H$$

$$30 = H$$

اذاً عدد الأجهزة 30 جهاز متاح

موقعها	الشبكات Networks	( عنوان الشبكة) Network id	أول ايبي متاح first valid ip	آخر ايبي متاح last valid ip	نهاية الشبكة ايبي البرودكاست broadcast ip
الأولى	172.16.0.0	172.16.0.0	172.16.0.1	172.16.0.30	172.16.0.31
الثانية	172.16.0.32	172.16.0.32	172.16.0.33	172.16.0.62	172.16.0.63
الثالثة	172.16.0.64	172.16.0.64	172.16.0.65	172.16.0.94	172.16.0.95
الرابعة	172.16.0.96	172.16.0.96	172.16.0.97	172.16.0.128	172.16.0.127
الخامسة	172.16.0.128	172.16.0.128	172.16.0.129	172.16.0.158	172.16.0.159
السادسة	172.16.0.160	172.16.0.160	172.16.0.161	172.16.0.190	172.16.0.191
السابعة	172.16.0.192	172.16.0.192	172.16.0.193	172.16.0.222	172.16.0.223
الثامنة	172.16.0.224	172.16.0.224	172.16.0.225	172.16.0.254	172.16.0.255

بالرجوع للجدول بالأعلى :

الآن الايبي اللي عندنا هو 172.16.0.2 وهو يقع في مدى الشبكة الاولى

اذاً عنوان الشبكة id هو **172.16.0.0** :

الطريقة الثانية :

### مثال 27 / 27

نقوم بكتابة 27 أواحد (رقم واحد) والباقي اصفار

انظر لآخر رقم واحد وشوف أين  
موقعه بالجدول

**11111111.11111111.11111111.11100000**

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

موقعه = 32

سوف تكون الشبكات من مضاعفات 32

ونبحث عن موقع الايبي في اي مدى

172.16.0.0

172.16.0.32

172.16.0.64

لدينا هذا الايبي 172.16.0.2 وهو موجود في مدى الشبكة 0

لان 172.16.0.32 تعتبر شبكة ثانية

اذاً عنوان الشبكة هو **172.16.0.0**

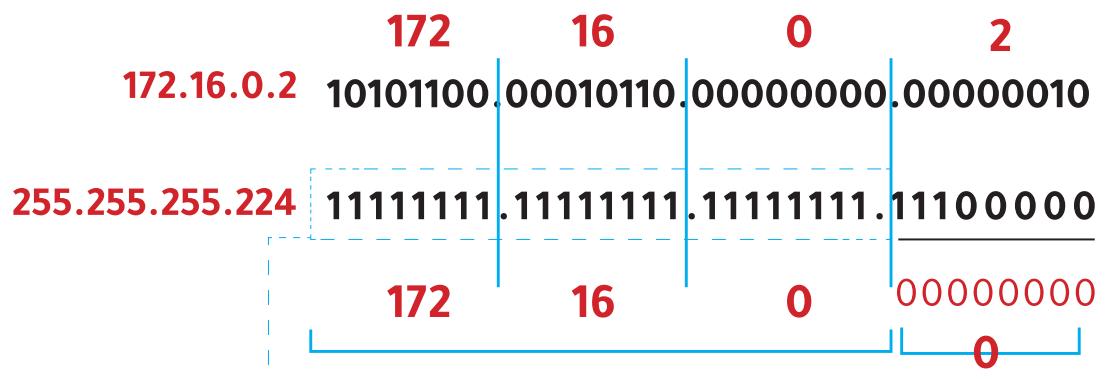
### 3 - معرفة عنوان الشبكة id

### مثال 27 / 27

توجد 3 طرق لمعرفة عنوان الشبكة :

الطريقة الأولى :

نحو الايبي وقناع الشبكة الى الباینری ونعملanding



اي خانة في قناع الشبكة كلها اواحد  
ينزل رقم الايبي نفسه لانه ثابت

اي تشابه 1 مع 1 ينزل 1 اذا اختلفوا 0

اذاً عنوان الشبكة هو **172.16.0.0**

الطريقة الثالثة :

**مثال اخر****192.168.29.155 / 29**

- نكتب هذا الايبي بالنظام الثنائي .
- تعلمنا أن العدد الكلي لبتات الايبي = 32
- نطرح :  $32 - 29 = 3$

**192 . 168 . 29 . 155**  
**11000000.10101000.00011101.10011011**

نحول الـ 3 ببات الاخيرة لأصفار .  
الآن نحسب قيمة الخانة الاخيرة

**11000000.10101000.00011101.10011000**

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

$$128 + 16 + 8 = 152$$

اذاً عنوان الشبكة هو **192.168.29.152**

**مثال اخر****172.16.0.2 / 27**

- نكتب هذا الايبي بالنظام الثنائي .
- تعلمنا أن العدد الكلي لبتات الايبي = 32
- نطرح :  $32 - 27 = 5$

**172 . 16 . 0 . 2**  
**10101100.00010110.00000000.00000010**

نحول الـ 5 ببات الاخيرة لأصفار .  
الآن نحسب قيمة الخانة الاخيرة

**10101100.00010110.00000000.00000000**

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

اذاً عنوان الشبكة هو **172.16.0.0**

موقعها	الشبكات Networks	عنوان الشبكة (Network id)	أول ايبي متاح first valid ip	آخر ايبي متاح last valid ip	نهاية الشبكة ايبي البرودكاست broadcast ip
الأولى	172.16.0.0	172.16.0.0	172.16.0.1	172.16.0.30	172.16.0.31
الثانية	172.16.0.32	172.16.0.32	172.16.0.33	172.16.0.62	172.16.0.63

4 - كيف نعرف:

أول ايبي متاح first valid ip

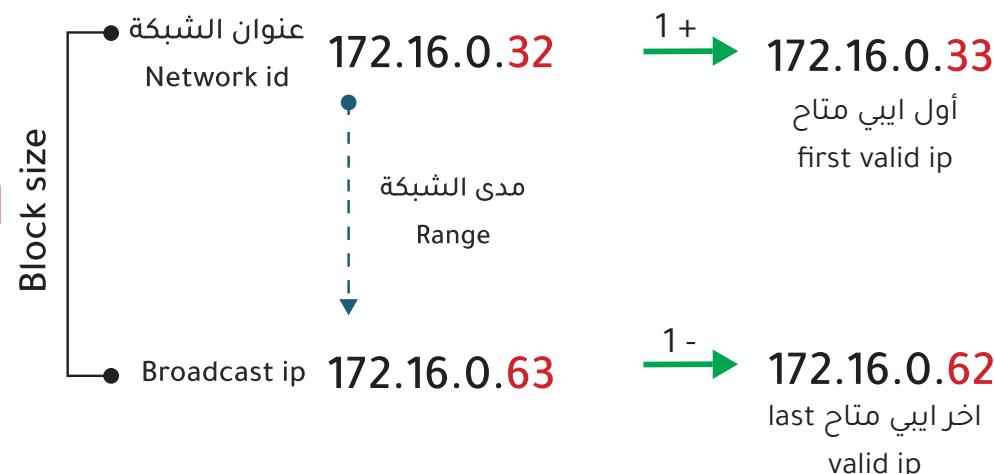
آخر ايبي متاح last valid ip

ايبي البرودكاست broadcast ip

- نقصد بالايبهات المتاحة هي اللي تستطيع الاجهزة الحصول عليها.

- ايبي عنوان الشبكة هو لا يمكن ان يتوزع على اي جهاز. ويكون رقمه زوجي دائمًا.

- ايبي البرودكاست لا يمكن ان يتوزع على اي جهاز لانه عنوان البث الخاص في الشبكة ويكون رقمه فردي



## أمثلة

لديك شبكة 192.168.10.2 والمطلوب :

شبكة تسع لـ 120 جهاز مع ار subnet mask لهذه الشبكة؟

الحل :

نطبق القانون السابق :

$$2^h - 2 \geq H$$

$$2^h - 2 \geq 120$$

2 أس كم لكي يعطينا 120 ؟

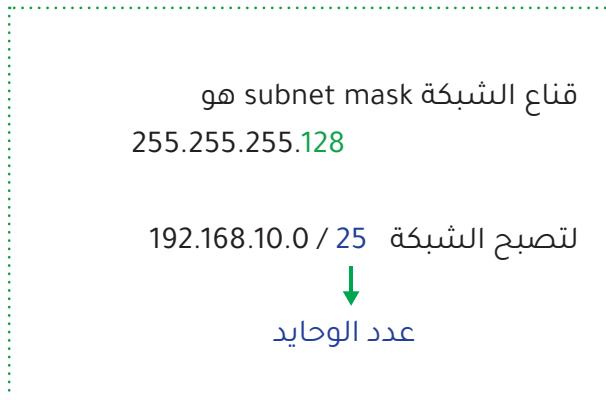
$2^6 = 64$  هذا لا يكفي لأنه أقل من المطلوب

$2^7 = 128$  هذا هو المطلوب حتى لو زاد قليلاً

جهاز 126 = 128 - 2

ايبي متاح للجهزة

اذاً نحتاج سبعة أصفار (7 bit) فقط تكفي لـ 120 جهاز .



11111111.11111111.11111111.10000000

128	64	32
1	0	0

## أمثلة

10.0.1.0 / 20

عندنا / 20 يعني 20 وحيد.  
اذاً نطرح  $32 - 2 = 30$   
يعني عندنا 30 صفر

**11111111.11111111.11110000.00000000**

نعرض بالقانون الذي تعلمناه

$$2^h - 2 \geq H$$

$$2^{12} - 2 \geq H$$

$$H = 4094$$

اذاً عدد الاجهزة هو 4094 جهاز

- 192.168.8.0 / 28
- 10.0.1.0 / 20
- 255.255.255.224

كم عدد الاجهزه hosts في هذه :

**192.168.8.0 / 28**

الحل :

عندنا / 28 يعني 28 وحيد.  
نحن نعرف ان العدد الكلي 32 بت وهنا اعطانا 28 وحيد  
اذاً نطرح  $32 - 28 = 4$   
يعني عندنا 4 اصفار

**11111111.11111111.11111111.11110000**

نعرض بالقانون الذي تعلمناه

$$2^h - 2 \geq H$$

$$2^4 - 2 \geq H$$

$$14 = H$$

اذاً عدد الاجهزة هو 14 جهاز

ما هو قناع الشبكة ( subnet mask ) المناسب لهذه الاجهزة:

10 pc - 1000 pc

$$2^{\text{h}} - 2 \geq 10$$

$$2^4 - 2 \geq 10$$

$$16 - 2 \geq 10$$

pc نعوض بالقانون :

اذاً نحتاج 4 أصفار لهذه الاجهزة  
اوحاد 28 = 4 - 32

11111111.11111111.11111111.11110000

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

$$128 + 64 + 32 + 16 = 240$$

اذاً قناع الشبكة المناسب هو 255.255.255.240

255.255.255.224

نلاحظ ان الخاتم الثلاث الاولى من اليسار اوحاید وكلهم ثابتين  
والأخيرة متغيرة .

نرجع للجدول الخاص بالباينري و نبدأ نجمع الاعداد من اليسار حتى  
نصل للرقم 224 ونضع رقم واحد تحت كل واحد منهم  
 $224 = 32 + 64 + 128$

128	64	32	16	8	4	2	1
1	1	1					

11111111.11111111.11111111.11110000

اذاً لدينا 27 اوحاید  
 $5 = 27 - 32$

لدينا 5 أصفار نعوض بالقانون الذي تعلمناه

$$2^{\text{h}} - 2 \geq H$$

$$2^5 - 2 \geq H$$

$$30 = H$$

اذاً عدد الاجهزه هو 30 جهاز

لديك هذا العنوان : 200.100.60.200 / 19

استخرج مما يأتي :

- 1 - عنوان الشبكة id
- 2 - الأولي الاول
- 3 - الثانيي الاخير
- 4 - ايبي البرود كاست
- 5 - قناع الشبكة subnet mask

الحل : 1 - عنوان الشبكة id

قناع الشبكة هو 19 / يعني ان لدينا 19 اوحايد .  
سوف يكون العمل في الخانة الثالثة

11111111.11111111.11110000.00000000

ننظر لآخر رقم واحد ونشوف موقعه بالجدول

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

الموقع 32 . سنضاعف هذا العدد لنستخرج الشبكات ونببدأ من الشبكة صفر وفي الخانة الثالثة .

الايبى الموجود لدينا هو 200.100.60.200 وهو يقع

200.100.0.0

في مدى الشبكة 200.100.32.0

200.100.64.0

200.100.32.0 - 200.100.63.255

200.100.96.0

عنوان الشبكة id هو

200.100.32.0

pc نعوض بالقانون :

$$2^{\text{h}} - 2 \geq 10$$

$$2^{10} - 2 \geq 10$$

$$1024 - 2 \geq 10$$

اذاً نحتاج 10 أصفار لهذه الاجهزة  
 $22 - 10 = 32$  اوحايد

11111111.11111111.11111100.00000000

سوف يكون العمل في الخانة الثالثة

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

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

اذاً قناع الشبكة المناسب هو 255.255.252.0

**5 - قناع الشبكة :**

لدينا 19 وحيد و سوف يكون العمل في الخانة الثالثة

**11111111.11111111.11100000.00000000**

نرجع للجدول ونجمع اماكن الوحدات ويظهر لنا رقم قناع الشبكة

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

$$224 = 32 + 64 + 128$$

قناع الشبكة هو 255.255.**224**.0

الشبكة Network	200.100.60.200
( عنوان الشبكة) Network id	200.100. <b>32</b> .0
الايبي الأول first ip	200.100. <b>32</b> .1
الايبي الاخير first ip	200.100. <b>63</b> .254
نهاية الشبكة ايبي البرودكاست broadcast ip	200.100. <b>63</b> .255

## تقسيم الشبكات Subnetting

**Subnetting** هو عملية تقسيم الشبكات الرئيسية الى شبكات فرعية ، والغرض من ذلك هو التقليل من خسارة الايبيات ضمن نطاق الشبكة الرئيسية .

طرق تقسيم الشبكات الفرعية :

**Fixed length subnet mask (FLSM)-1** قناع الشبكة الفرعية ثابت الطول (FLSM) هو طريقة تقسيم الشبكة إلى عدة شبكات فرعية متساوية في قناع الشبكة . Hosts (Subnet Mask)

**Variable length subnet mask (VLSM) - 2**

قناع الشبكة الفرعية متغيرة الطول (VLSM) هو طريقة تقسيم الشبكة إلى عدة شبكات فرعية مختلفة في قناع الشبكة (Subnet) و مختلفة في عدد الأجهزة أو الـ Hosts (Mask)

عندما تم انشاء الانترنت لأول مرة لم يتوقع المبدعون لهذه التقنية التوسع والانتشار الكبير لهذه الشبكة . لهذا واجهوا مشكلة استنفاد العناوين في الـ IPv4 .

- فمثلا شركة تحتاج 5000 عنوان ايبي هل تستعمل عناوين الفئة C أو B ؟ عناوين الفئة C التي هي 192.168.0.0 /24 تكفي فقط لـ 254 جهاز فقط . لذلك سوف تتجه للفئة B التي هي 172.16.0.0 /16 ولكن سعة هذه الشبكة 65534 جهاز، وعند استعمال 5000 جهاز سوف نخسر 60534 عنوان متاح للستخدام !!

الحل :

### Classless Inter -Domain Routing (CIDR)

تم تقديمه ليكون بدل من نظام العنونة Classful في النظام السابق :

الفئة A كان الزامية تستخدم 8 /  
الفئة B كان الزامية تستخدم 16 /  
الفئة C كان الزامية تستخدم 24 /

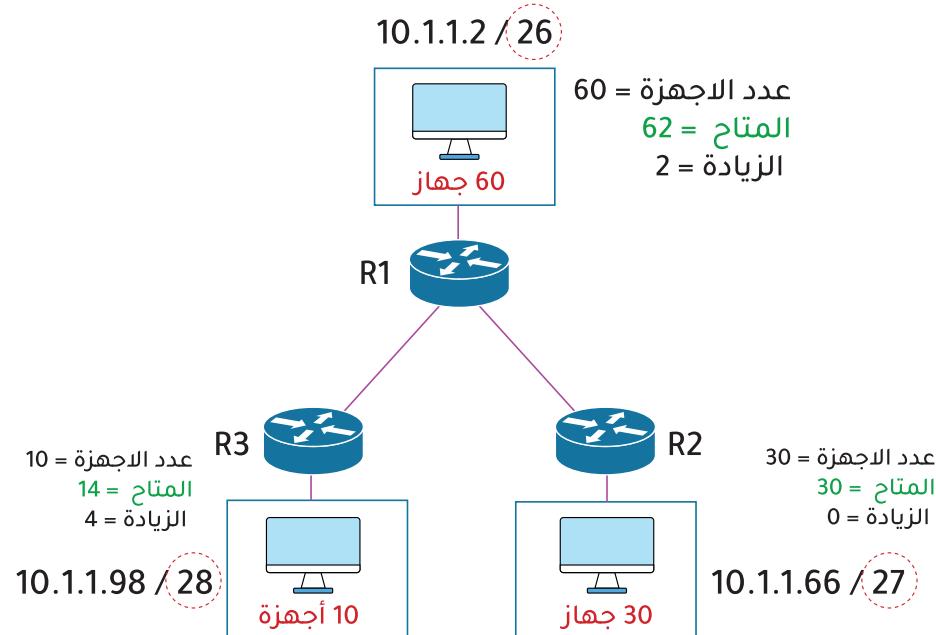
مع الـ CIDR تم الغاء هذه الالزامية وصار يسمح باستخدام اي رقم subnet مع اي فئة فمثلا mask يمكن استخدام 20 / مع الفئة A أو B أو C .

- هذا الـ CIDR سمح لنا بتقسيم الشبكات الى شبكات أصغر تسمى شبكات فرعية ( subnets ) .

## قناع الشبكة متغير الطول (VLSM) Variable Length Subnet Mask

**VLSM**

= **VLSM** هو تقسيم الشبكة إلى عدة شبكات فرعية مختلفة في قناع الشبكة (Subnet Mask) و مختلفة في عدد الأجهزة أو الـ Hosts .

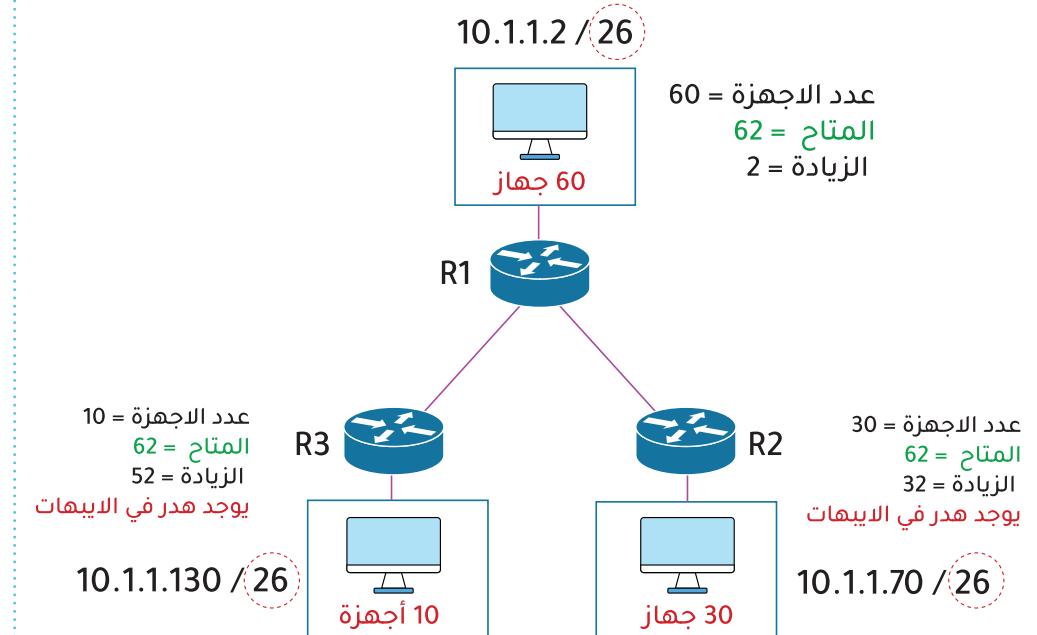


للحظ الدوائر الحمراء ستجد ان الأقنعة مختلفة . و كل شبكة مقسمة بحسب عدد الأجهزة المطلوب فيها

## قناع الشبكة الفرعية ثابت الطول (FLSM) Fixed length subnet mask

**FLSM**

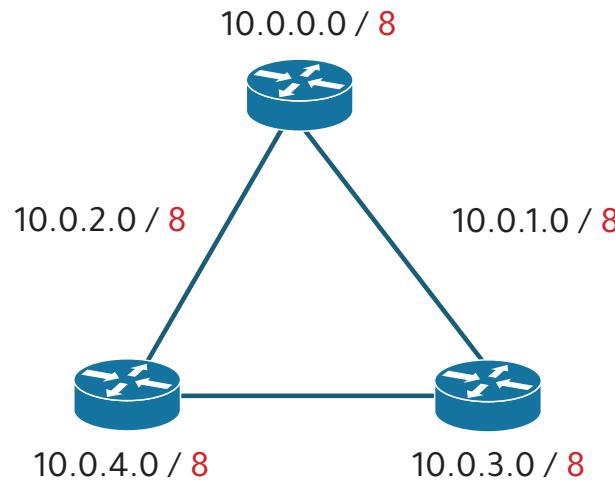
= **FLSM** هو تقسيم الشبكة إلى عدة شبكات فرعية متساوية في قناع الشبكة (Subnet Mask) و متساوية في عدد الأجهزة أو الـ Hosts .



للحظ الدوائر الحمراء ستجد ان الأقنعة متشابهه وان كل شبكة فيها 62 جهاز متاح مما سبب هدر في الايبيات

## الفرق بين Classless و Classful

الفئة class	المدى Range		قناع الشبكة subnet mask	قيمة الوحدات
A	10.0.0.0	-	255.0.0.0	/ 8
B	128.0.0.0	-	255.255.0.0	/ 16
C	192.0.0.0	-	255.255.255.0	/ 24



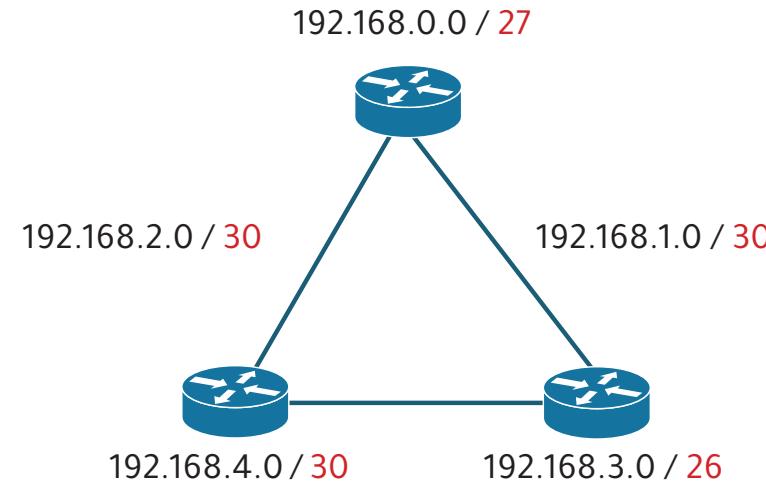
هي التقنية التي تم تقسيم عناوين IP الى الفئات الخمس A , B , C , D , E المحددة بـ subnet mask ثابت لكل فئة والذي لن يتغير عند تقسيم الشبكات . انظر للصورة سترى 8 ثابت .



**لماذا لم يتغير ؟؟**  
لان الـ Classful ينظر دائمًا إلى الرقم الموجود في الخانة الأولى من عنوان الشبكة و الخانة الاولى في رقم 10.0.0.0 هي 10 وهي من مدى class A لذلك البروتوكول لن يقبل اي subnet mask اخر غير / 8

- عند تبادل عناوين الشبكات بين الراوترات تُرجع كل شبكة لاعداداتها الافتراضية .  
- يعني قيمة الـ subnet mask الافتراضية للفئة A هي / 8 . فلو أرسل راوتر شبكة من فئة A بقمية 20 / فإنه سوف يعتمد الـ 8 / لانه لن يقبل اي قيمة غير الافتراضية .

هي تقنية تساعد على تقسيم عناوين الـ IP للشبكات مع subnets mask مختلف لكل شبكة بهدف تقليل استنفاد وهدر العناوين . انظر للصورة سترى subnet mask (أقنعة الشبكة) مختلفة .



Classless	Classful
يتجاهل هذه القاعدة ويتم توزيع الأبيهات بشكل حر وأعتمادا على تقنية الـ VLSM	يعتمد على قاعدة الـ IP Classes في توزيع الأبيهات
يرسل الـ Subnet Mask مع كل الأبيهات المرسلة إلى روترات أخرى لأنه متغير وبحسب الطلب.	لا يرسل الـ Subnet Mask مع التحديبات الخاصة به على الشبكة لأن الماسك ثابت ومعروف عند كل الروتات

## مثال

القسم A يحتاج 100 جهاز:

$$\text{نوعض بالقانون } H = 2^h - 2 \geq 100$$

أى س كم حتى يعطينا 100 جهاز؟

$$\text{الجواب: } 2^7 = 128$$

نحتاج 7 برات (أصفار)

نطرحها من العدد الكلى للاىي 32 بت

$$32 - 7 = 25$$

اذاً لدينا 25 أوحايد

الشبكة الاولى :

تبدأ من 10.1.2.0 / 25 وتنتهي 10.1.2.127 / 25

القسم B يحتاج 60 جهاز:

الشبكة الثانية تبدأ من 10.1.2.128 / 25

وسوف نقصيم الشبكة لعدد 60 جهاز

$$2^6 = 64$$

نحتاج 6 برات (أصفار)

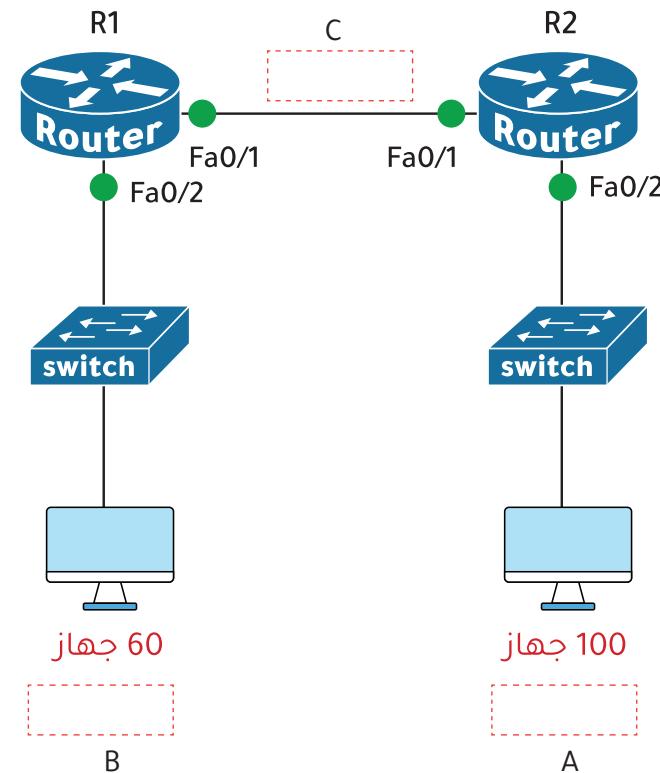
نطرحها من العدد الكلى للاىي 32 بت:

$$32 - 6 = 26$$

اذاً الشبكة الثانية :

تبدأ من 10.1.2.128 / 26 وتنتهي 10.1.2.191 / 26

لديك شبكة 10.1.2.0 / 24 قسم هذه الشبكة على حسب الاجهزة لكل شبكة؟



الحل:

اولاً لابد ان نبدأ بـ **باكبر** رقم للجهازة وهو 100 ومن ثم نكمل بالترتيب الى اصغر شبكة

القسم C يحتاج 2 ايبي فقط :

نحتاج عدد 2 ايبي فقط للمنفذين المتصلين بين الراوترين .

الشبكة الثالثة تبدأ 10.1.2.192 / 26

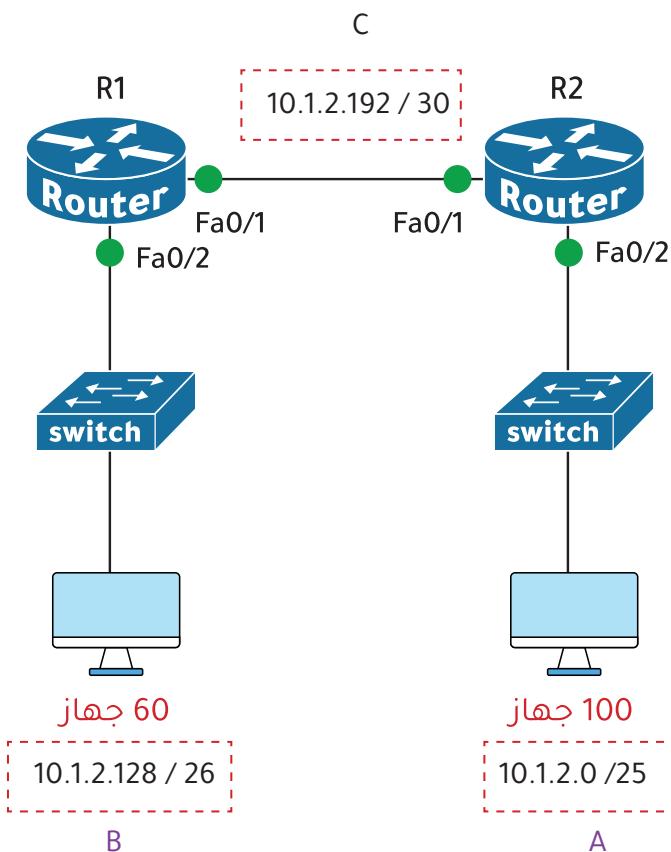
وسوف نقسم الشبكة لعنوانين فقط

$$2^2 = 4$$

$$32 - 2 = 30$$

اذاً الشبكة الثالثة :

تبدأ من 10.1.2.192 / 30 وتنتهي 10.1.2.195 / 30



هذا الجزء محدد للشركة المصنعة لكرت الشبكة (مثل- hp-dell- cisco ) من قبل  
Organizationally Unique Identifier(OUI)

**3A-34-62-F5-88-D6**

OUI

NIC

رقم مميز لا يتكرر خاص  
بكل كارت

octet 8 bit

**3A-34-62-F5-88-D6**

24 bit

24 bit

48 bit

**Media Access Control**  
(Mac Address)  
الماك ادرس

Mac

Media Access Control Mac

ويُعرف بأنه رقم ثابت يُميز كل جهاز عن الآخر ولا يمكن أن يتكرر في اي جهاز في العالم .

فهو عنوان يتم وضعه في كرت الشبكة (network interface card) من قبل المصنع .

- قد تجده باسم آخر مثل physical Address .
- يعمل في الطبقة الثانية (Data Link) حسب التصنيف OSI .

- الحجم الكلي للماك ادرس = 48 بت

- يُكتب بالنظام السداسي عشر (Hexadecimal)

0 1 2 3 4 5 6 7 8 9 A B C D E F

## Address Resolution Protocol ARP

هو بروتوكول يستخدم لایجاد الماك ادرس للجهاز الآخر في الشبكة عبر معرفة الـ IP المخصص لهذا الجهاز .

# بروتوكول ARP

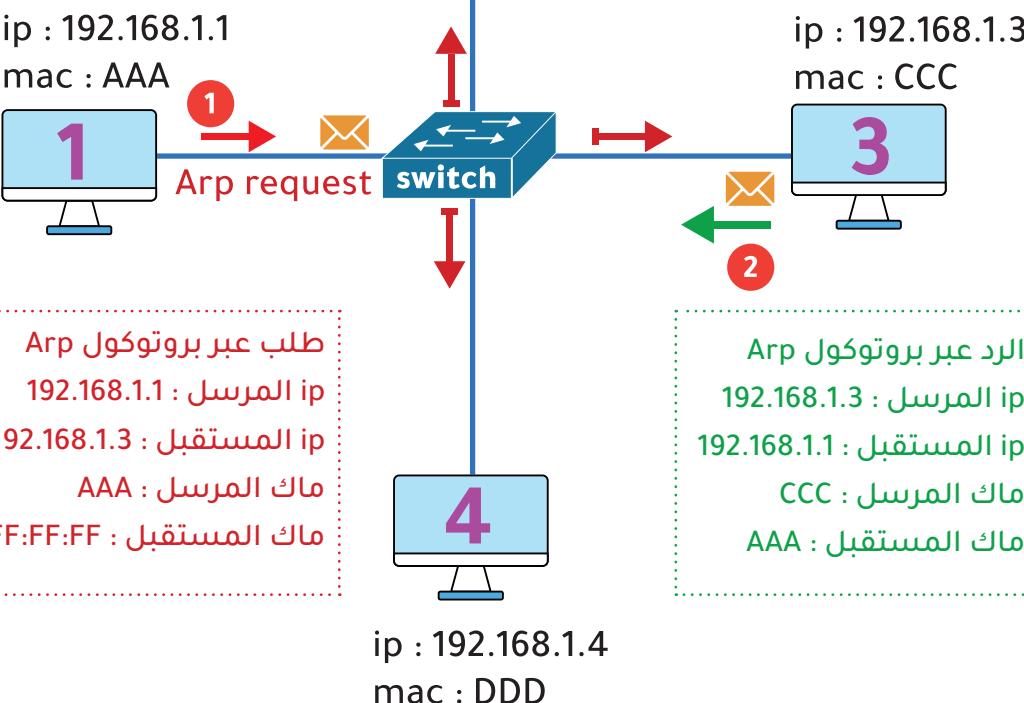
ARP

نفرض أن الجهاز 1 يريد التواصـل مع الجهاز 3 وهو يـعرف ايـبيـ الجهاز 3 ولكن لا يـعرف الماك ادرسـ للجهاز 3 .

فيـقومـ الجهازـ 1ـ بإـرسـالـ طـلـبـ عـبـرـ بـرـوـتـوكـولـ ARPـ يـضـعـ فيهـ IPـ الجـهاـزـ 3ـ .ـ وـيـكـونـ عنـوانـ الـوجـهـةـ هوـ العنـوانـ العـامـ (FF:FF:FF:FF:FF:FF) .

(FF:FF:FF:FF:FF:FF) : هوـ عنـوانـ ماـكـ أـدرـسـ عـامـ يـسـتـخـدـمـهـ الجـهاـزـ لـلـإـرـسـالـ لـكـلـ الـاجـهـزـةـ فـيـ الشـبـكـةـ .

وهـنـاـ يـأـتـيـ دورـ السـوـيـتـشـ Switchـ فـيـ إـرـسـالـ الـطـلـبـ إـلـىـ كـافـةـ الـأـجـهـزـةـ الـمـتـصـلـةـ مـعـهـ عـدـاـ الـجـهاـزـ الـذـيـ تـمـ صـدـورـ الـطـلـبـ مـنـهـ .ـ وـلـنـ يـرـدـ عـلـىـ الرـسـالـةـ إـلـاـ الـجـهاـزـ الـمـطـلـوبـ أيـ الجهازـ 3ـ الـذـيـ بـدـورـهـ سـيـسـتـقـبـلـ الرـسـالـةـ وـيـرـدـ عـلـيـهـ بـرـوـتـوكـولـ ARPـ Re~plyـ إـلـىـ الـجـهاـزـ 1ـ مـصـحـوبـاـ بـالـماـكـ اـدـرـسـ .



طلبـ بـرـوـتـوكـولـ ARPـ

ipـ المرـسـلـ : 192.168.1.1ـ

ipـ الـمـسـتـقـبـلـ : 192.168.1.3ـ

ماـكـ المـرـسـلـ : AAAـ

ماـكـ الـمـسـتـقـبـلـ : FF:FF:FF:FF:FF:FFـ

الـردـ بـرـوـتـوكـولـ ARPـ

ipـ المرـسـلـ : 192.168.1.3ـ

ipـ الـمـسـتـقـبـلـ : 192.168.1.1ـ

ماـكـ المـرـسـلـ : CCCـ

ماـكـ الـمـسـتـقـبـلـ : AAAـ

رسـائـلـ بـرـوـتـوكـولـ ARPـ :

1 - طـلـبـ ARPـ Requestـ

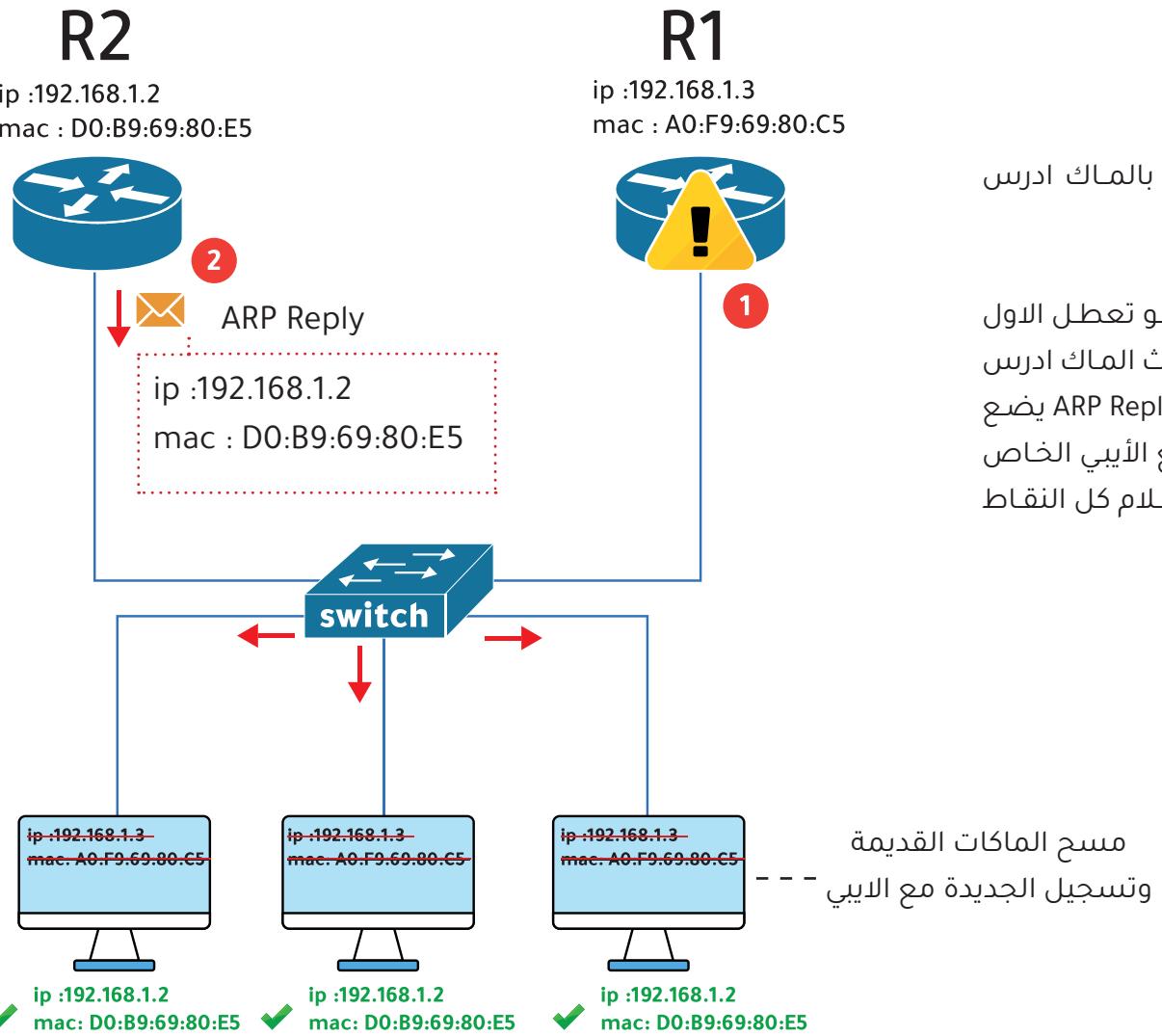
ترـسلـ بـطـرـيقـةـ الـبـرـوـدـكـاستـ (broadcastـ)ـ ،ـ يـعـنيـ لـلـكـلـ .

2 - الـردـ ARP~Replyـ

يـتمـ اـرـسـالـ الـردـ بـطـرـيقـةـ الـعـيـنـيـ (unicastـ)ـ ،ـ يـعـنيـ لـلـجـهاـزـ الـذـيـ اـرـسـلـ الـطـلـبـ فـقـطـ .

## جدول الـ ARP = ARP Table

عندما يتعرف جهاز في الشبكة على عنوان الماك أدرس للجهاز الآخر بواسطة بروتوكول الـ arp فإنه سوف يخزن هذا العنوان في جدول خاص يسمى جدول الـ arp لكي يستطيع مستقبلاً الارسال لهذا الجهاز ولا يكون هناك حاجة لارسال arp جديد .



### Gratuitous ARP

هو بروتوكول Arp ولكن يُستخدم لتحديث الشبكة بالماك ادرس الجديد عبر الـ ip .

مثلا يوجد لديك راوتران واحد مفعل والآخر احتياط فلو تعطل الاول فان الثاني يريد إعلام باقي الأجهزة بهذا التغيير لتحديث الماك ادرس الجديد الخاص بالراوتر لذا فهو يقوم بإرسال رسالة ARP Reply يوضع فيه الماك ادرس الخاص به كمرسل (Source) ويوضع الأبيي الخاص به ويقوم بالأرسال على شكل Broadcast لكي يتم إعلام كل النقاط الموجودة على الشبكة .

مسح الماكات القديمة  
وتسجيل الجديدة مع الايبи - - -

## السويتش Switch

السويتش هو جهاز يعمل على ربط أجهزة الشبكة بعضها البعض مثل (الحاسب - الطابعة) وذلك ضمن شبكة محلية (LAN) ويعمل في الطبقة الثانية - Data Link Layer في الـ OSI Model .

### Cut-through

يعمل على ارسال البيانات فورا بمجرد إستلام الفريم Frame حيث يقوم بإرسالها للمستقبل Destination بعد قراءة ماك ادرس المستقبل .

- سريع في ارسال البيانات .
- قد يحدث فيه نسبة من الخطأ
- يستخدم في البيانات المباشرة مثل الصوت او الفيديو

### Fragment-free

يقوم بفحص أول 64 بت من الفريم Frame اذا هو سليم راح يعيد توجيهه للمستقبل .

اما اذا وجد خطأ في اول 64 بت فلن يعيد توجيهه للمستقبل

### Switching modes

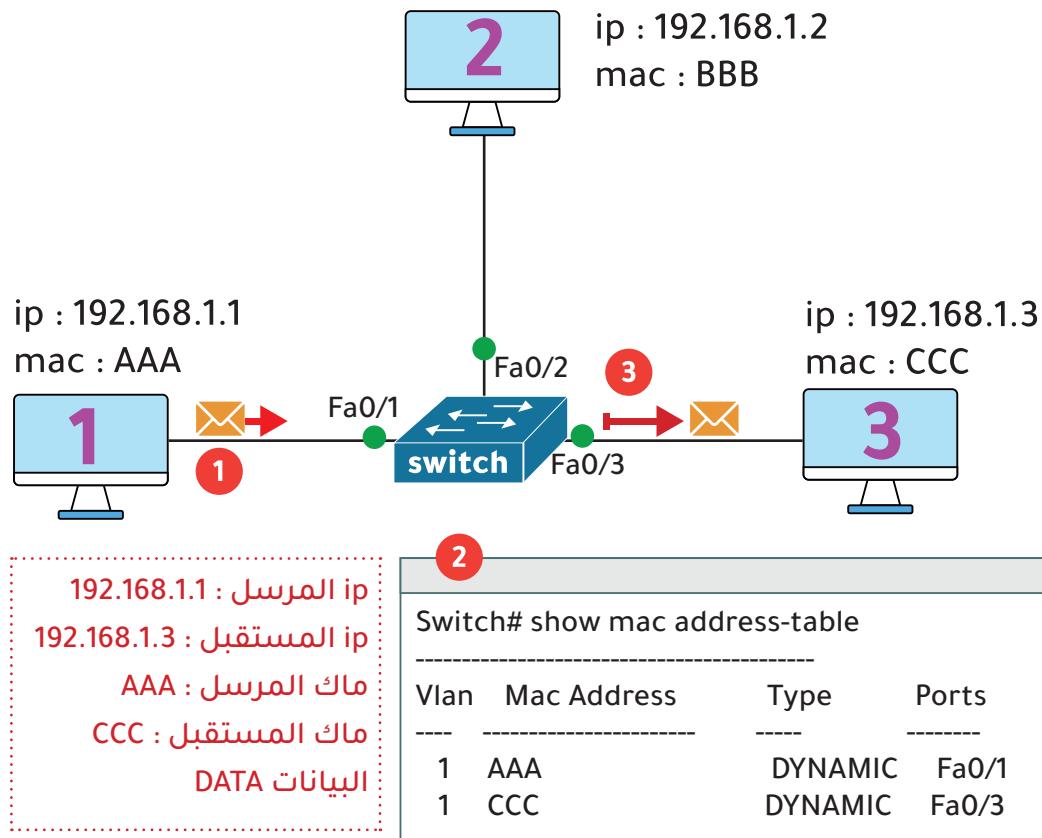
#### Store-and-forward

يقوم بتخزين الفريم Frame الواصل له من المرسل ويعمل عملية CRC وهي عملية التاكد من الاخطاء وسلامة البيانات المرسلة ثم يعيد توجيهها (forwarding) الى المستقبل Destination ثم

- آمن وقوى في طريقة العمل
- أبطئ من الـ cut-through .

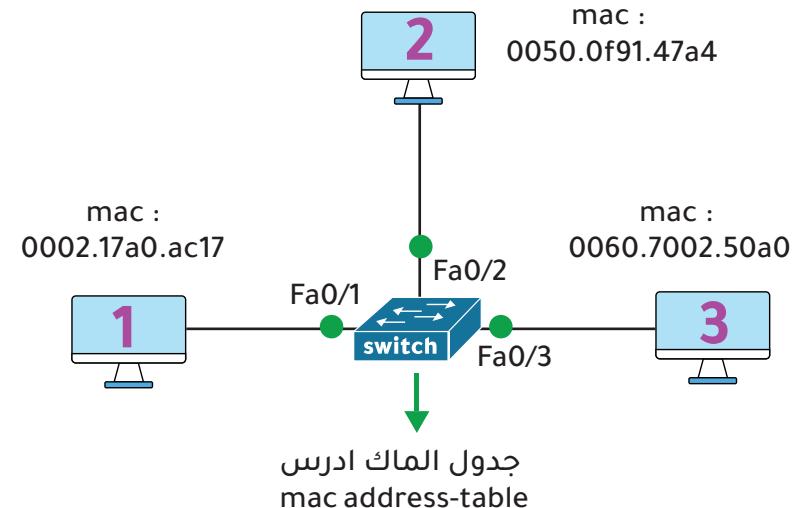
## كيف تتوصل الأجهزة عبر السويفت؟؟

عندما يتلقى السويفت الفريم من PC1 (المرسل) ينظر مباشرة للجدول المسجل عنده والمنفذ المرتبط به ويرسل الفريم مباشرة إلى PC3 (المستقبل) لأن الماكولات مسجلة جميعها بالجدول

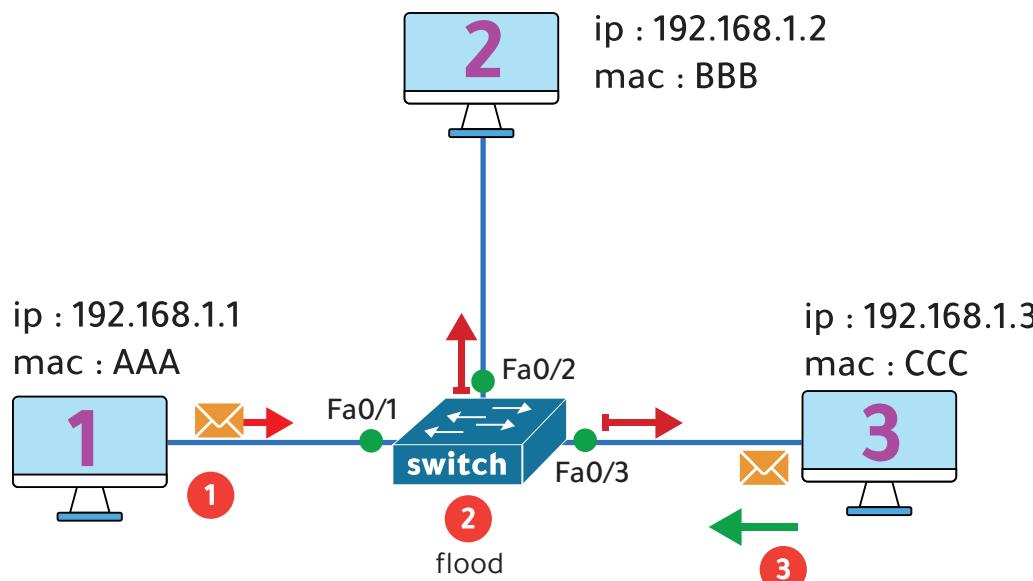


## جدول الماك أدرس في السويفت Switch mac address table

- يوجد في السويفت جدول يخزن الماكولات ادرس فيه ويربط كل ماك بالمنفذ (port) المتصل عليه الجهاز لكي يسرع من تواصل الأجهزة مع بعضها البعض.



Switch# show mac address-table			
Vlan	Mac Address	Type	Ports
1	0002.17a0.ac17	DYNAMIC	Fa0/1
1	0050.0f91.47a4	DYNAMIC	Fa0/2
1	0060.7002.50a0	DYNAMIC	Fa0/3



طلب عبر بروتوكول Arp  
ip المرسل : 192.168.1.1  
ip المستقبل : 192.168.1.3  
ماك المرسل : AAA  
ماك المستقبل : FF:FF:FF:FF:FF

الرد عبر بروتوكول Arp  
ip المرسل : 192.168.1.3  
ip المستقبل : 192.168.1.1  
ماك المرسل : CCC  
ماك المستقبل : AAA

### كيف يسجل السويفتش الماكولات بالجدول ؟؟

مثلا يريد pc1 التواصل مع pc3:

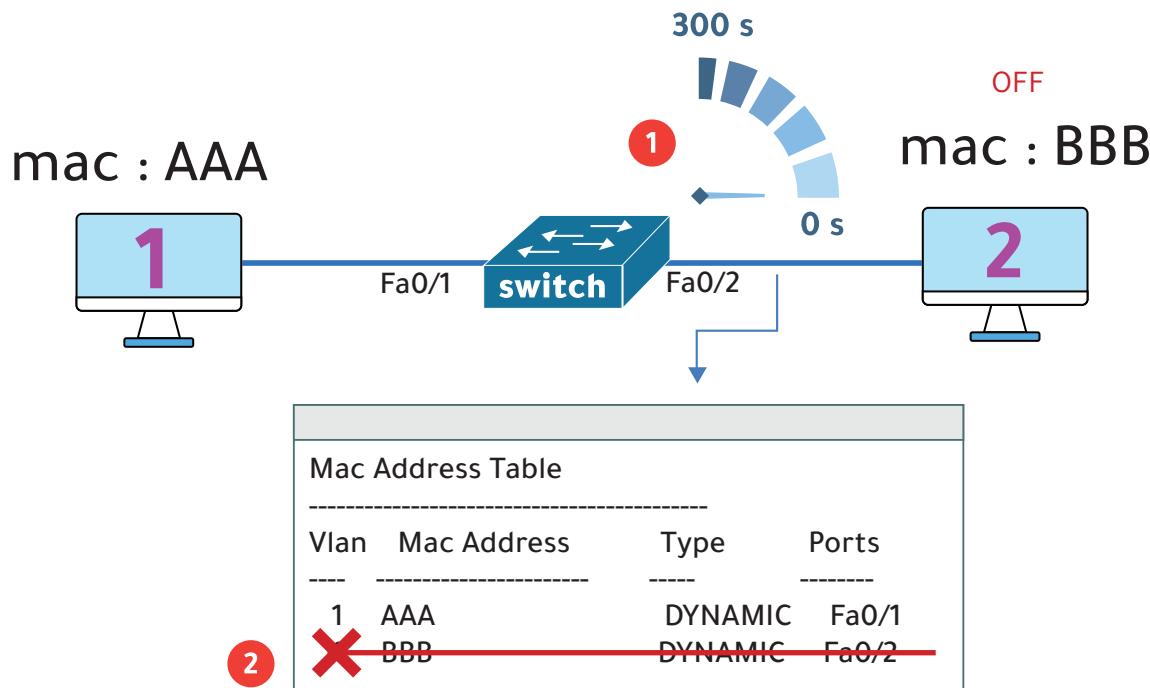
1 - يرسل pc1 رسالة ARP فيها الايبي جهاز المستقبل 3 لمعرفة ماك ادرس المستقبل .

2 - يستقبل السويفتش الرسالة وينظر هل لديه ماك ادرس PC3 فإذا لم يجده في الجدول فسوف يعيد السويفتش ارسالها لكل الاجهزه المتصلة عليه (flood) ما عدا الجهاز المرسل PC1 ويقوم بتسجيل ماك PC1 في الجدول ويربطه بالمنفذ اللي وصل عليه .

3 - وعند رد PC3 يقوم السويفتش أيضا بتسجيل عنوان 3 في الجدول ويربطه بالمنفذ اللي وصل عليه .

flood = تعني ارسال الرسالة لكل الاجهزه المتصلة بالسويفتش )

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	AAA	DYNAMIC	Fa0/1
1	CCC	DYNAMIC	Fa0/3



### aging time

ما هو الـ aging time  
هو الفترة المسموحة لوجود الماك أدرس في جدول السويتش بدون ترافيك أو تبادل بيانات.

يظل الماك أدرس مسجل في جدول السويتش  
مادام هناك تبادل بيانات مع هذا الماك ولكن اذا لم  
يكن هناك ترافيك (بيانات) لمدة 300 ث يتم مسح  
الماك من الجدول . الفائدة انه لكل سويتش قدرة  
في تخزين الماكينات وبسبب طبيعة عمله المتواصلة  
فإنه سوف يسبب مشاكل مستقبلية في حال  
وجوده بلا فائدة

### ملاحظة :

وقت aging time الافتراضي في السويتش هو 300  
ثانية ولكن تستطيع تغييره حسب رغبتك ولكن  
الافضل تركه على الافتراضي .

## أوضاع منافذ السويتش

### أوضاع السرعة في منافذ السويتش

النوع type	السرعة speed
ethernet	10 Mbps
Fast ethernet	10 / 100 Mbps
Gigabit ethernet	10 / 100 / 1000 Mbps

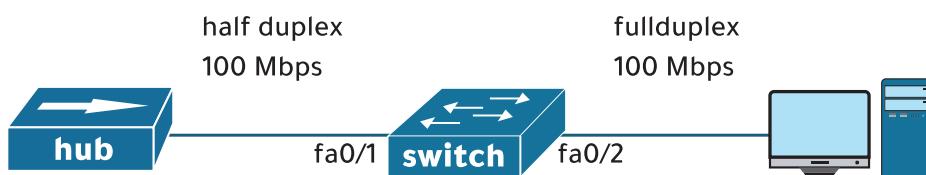
بشكل افتراضي ستتفاوض أجهزة Cisco تلقائياً على إعدادات السرعة (speed) والإرسال المزدوج (duplex) عندما تقوم بتوصيل جهاز (سويتش - راوتر او اي جهاز اخر) بمنفذ على جهاز سيسكو (Cisco) حيث ستحدد عملية التفاوض وستوافق الأجهزة على اوضاع الإرسال والاستقبال والسرعة .

- **أوضاع الإرسال والاستقبال في منافذ السويتش**

half duplex

Full duplex

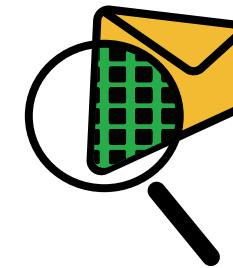
auto-negotiate



لاحظ كيف الجزء اليسير توافقوا على الـ half duplex والجزء الأيمن على الـ full duplex

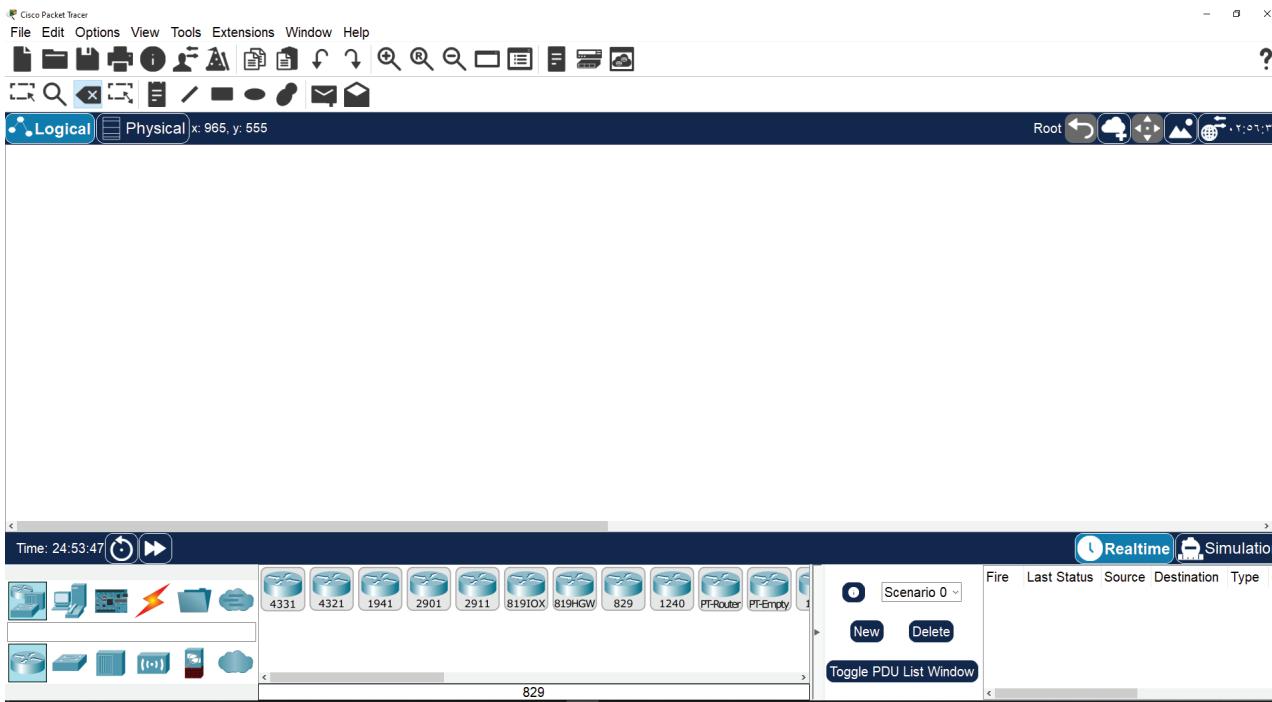
ملاحظة :

الإعدادات الافتراضية في أجهزة سيسكو (Cisco) هي :  
auto-negotiate (التفاوض التلقائي) .  
الأفضل تركها على الأعدادات الافتراضية .

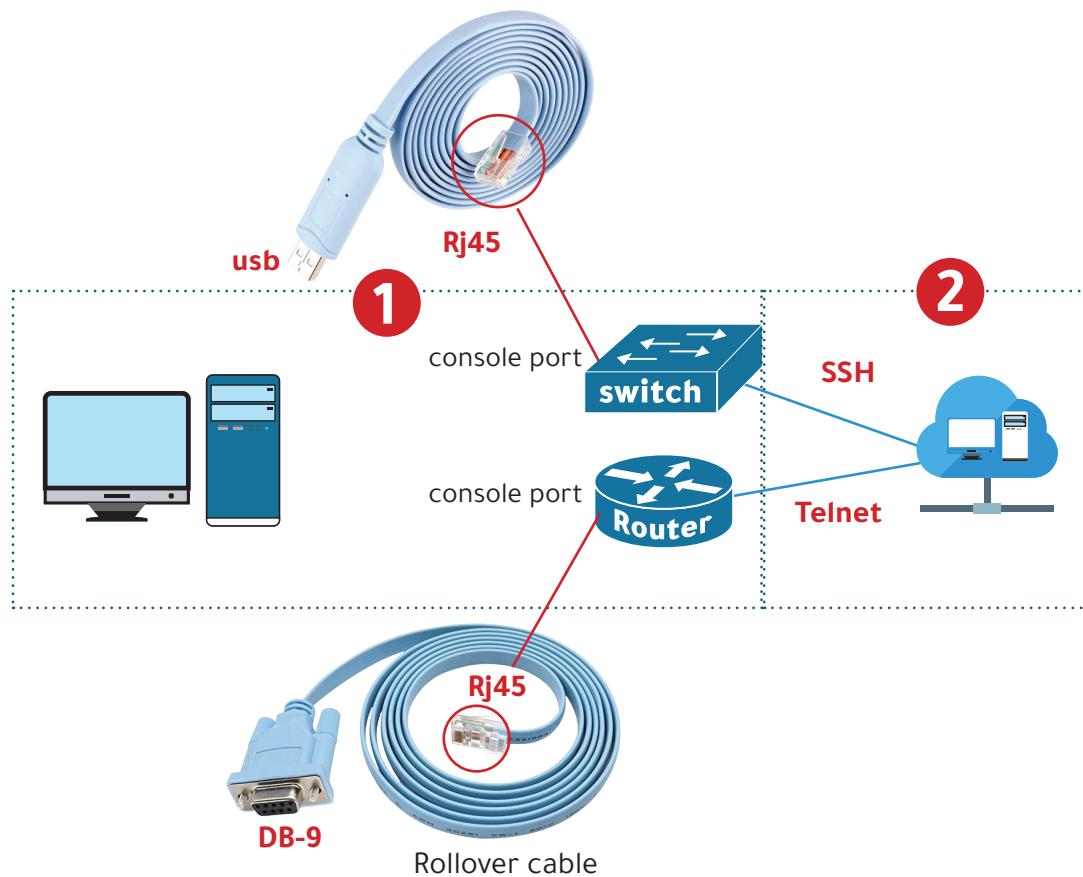


## برنامج packet tracer

برنامج محاكي الشبكات Cisco Packet Tracer من عبارة عن برنامج تعليم وتعلم شامل للتكنولوجيا الشبكات ، حيث تستطيع فيه التعلم على بناء الشبكات وإعداداتها واستكشاف الأخطاء ومتابعة وختبار الاتصال بين الأجهزة .



## طرق الاتصال بالسويتش والراوتر



**فتحات الراوتر والسويتش نوعين :**

**منفذ الاتصالات communication port** يتم توصيل الأجهزة فيه مثل الحاسب واللاب توب والراوتر والسويتش وغيرها .

**منفذ الأعدادات configuration port** يتم توصيل اللاب توب أو الكمبيوتر فيه لعمل الإعدادات الخاصة بالراوتر أو السويتش ويسمى بالكونسول . console

**1** - نستطيع الدخول إلى اعدادات الراوتر والسويتش عن طريق توصيل كابل الكونسول **console** .

**2** - نستطيع الدخول إلى اعدادات الراوتر والسويتش عن بعد عن طريق بروتوكول **ssh or telnet** بعد تحميل برنامج **PuTTY**

منفذ الكونسول **console port**



الآن داخل نمط المستخدم (User Mode) وهو عرض للمعلومات بدون اجراء اي تعديل

```

Switch >
Switch>

Switch > enable ..... نكتب enable للدخول للوضع المميز

Switch# ..... يسمى وضع الدخول enable mode أو الوضع المميز Privileged Mode ويكون اخره علامة # . تستطيع عرض كافة المعلومات والاعدادات المحفوظة بالجهاز

Switch# configure terminal ..... نكتب configure terminal للدخول لوضع الاعداد

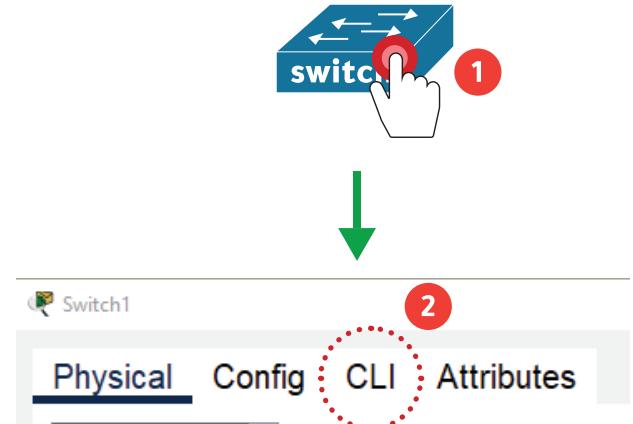
Switch(config)# ..... وضع الاعداد CONFIGURATION MODE
للخروج الى الوضع السابق
Switch(config)# exit
Switch# exit
Switch>

```

### الدخول على سطح الاوامر (CLI) في السويتش

الـ CLI هو اختصار لـ Command line interface وفيه يتم كتابة الأوامر واستعراض الإعدادات .

بعد فتح برنامج packet tracer اختر السويتش واضغط كلك عليه .



**ملاحظة :**

تستطيع كتابة اول حروف الاوامر كاختصار .

مثلًا : enable --> en

configure terminal ---> conf t

exit ---> ex

أو كتابة الحروف الأولى ثم الضغط على زر tab ليكمل لك الامر

```

Switch> en
Switch# conf t
Switch(config)# line console 0
Switch(config-line)# password 1234
Switch(config-line)# login
Switch(config-line)# exit
Switch(config)# exit
Switch#

```

- ..... ندخل على الكونسول
- ..... نضع كلمة مرور
- ..... يجب كتابة Login لكي يظهر له أمر
- ..... طلب ادخال كلمة المرور

وللأمان أكثر نعمل كلمة مرور للدخول في  
وضع الـ enable mode  
واستخدمنا كلمة بدل من  
password  
لأنها أقوى تشفير من الـ password

```

Switch>en
Switch# conf t
Switch(config)# enable secret 123
Switch(config)# exit
Switch#

```

نكتب هذا الأمر لكي يشفّر لنا جميع كلمات  
المرور عند عرضها

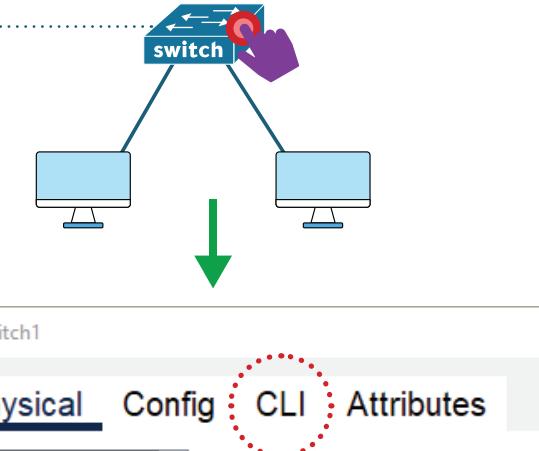
```

Switch>en
Switch# conf t
Switch(config)# service password-encryption
Switch(config)# exit
Switch#

```

## ضبط كلمة المرور للكونسول ووضع الدخول enable mode

لتؤمن الجهاز يقوم بإنشاء كلمة مرور عند توصيل  
كابل الكونسول بالراوتر أو السويتش فإنه هو المنفذ  
الرئيسي الذي سيتم منه الدخول للجهاز عند عمل  
الإعدادات.



- انشاء اسم مستخدم وكلمة مرور .
- تغيير اسم الجهاز .

```

Switch>en
Switch# conf t
Switch(config)# username ali secret 1234 ..... لانشاء اسم مستخدم وكلمة مرور
Switch(config)# hostname Sw1 ..... لتغيير اسم الجهاز
Sw1(config)# exit

```

```

Sw1# copy running-config startup-config ..... لحفظ الاعدادات ويامكانك كتابة wr أو write
Destination filename [startup-config]? ..... كطريقة أخرى للحفظ
Building configuration... ..... نضغط enter
[OK]

```

Sw1#?	علامة الاستفهام تعرض لك جميع الاوامر المتوفرة في هذا الوضع
Sw1#ena?	علامة الاستفهام بعد الحروف تعرض لك الكلمة التي بدأت بهذه الحروف
CNTL + Z	تخرجك الى وضع الدخول enable mode (Sw1#)
Sw1#logout	تسجيل خروج من الراوتر وظهور رسالة الترحيب
Sw1# sh run	يظهر لك جميع الاعدادات

**ملاحظة :**

- اذا اردنا الغاء اي امر نضيف كلمة NO في اول الامر مثلا :

```

Sw1 (config)# enable secret 123
Sw1 (config)# no enable secret 123

```

connected متصل بكابل  
notconnect غير متصل بكابل

حالة المنفذ

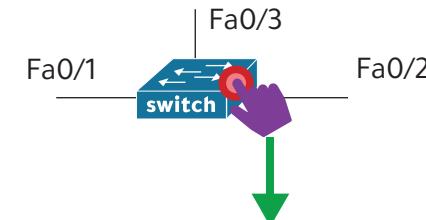
Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	1	auto	auto	10/100BaseTX
Fa0/2		connected	1	a-full	a-100	10/100BaseTX
Fa0/3		connected	1	auto	auto	10/100BaseTX
Fa0/4		notconnect	1	auto	auto	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Gig0/1		notconnect	1	auto	auto	10/100BaseTX
Gig0/2		notconnect	1	auto	auto	10/100BaseTX

منافذ السويفت

eth	ethernet	10 Mbps
Fa	Fast ethernet	10 / 100 Mbps
Gig	Gigabit ethernet	10 / 100 / 1000 Mbps

## منافذ السويفت

جميع منافذ السويفت جاهزة للعمل وب مجرد توصيela بالكابل فإنها تتفعل بشكل تلقائي .



ملاحظة :

- a-full : تدل على انه تم التفاوض التلقائي على full duplex  
- a-100 : تدل على انه تم التفاوض التلقائي على السرعة 100

- تستطيع استعراض حالة منفذ معين عبر الامر التالي :

Switch# show interfaces f0/1 status

بشكل مختصر

Switch# sh int f0/1 st

## الدخول لاحد منافذ السويفت

```

Switch> en
Switch #conf t
Switch(config)# interface fa0/1
Switch(config-if)#
      الان داخل وضع منفذ fa0/1
Switch(config-if)# exit
      للخروج
Switch(config)# exit

```

يظهر لك جدول الماك الادرس للسويفتش

Switch# show mac address-table

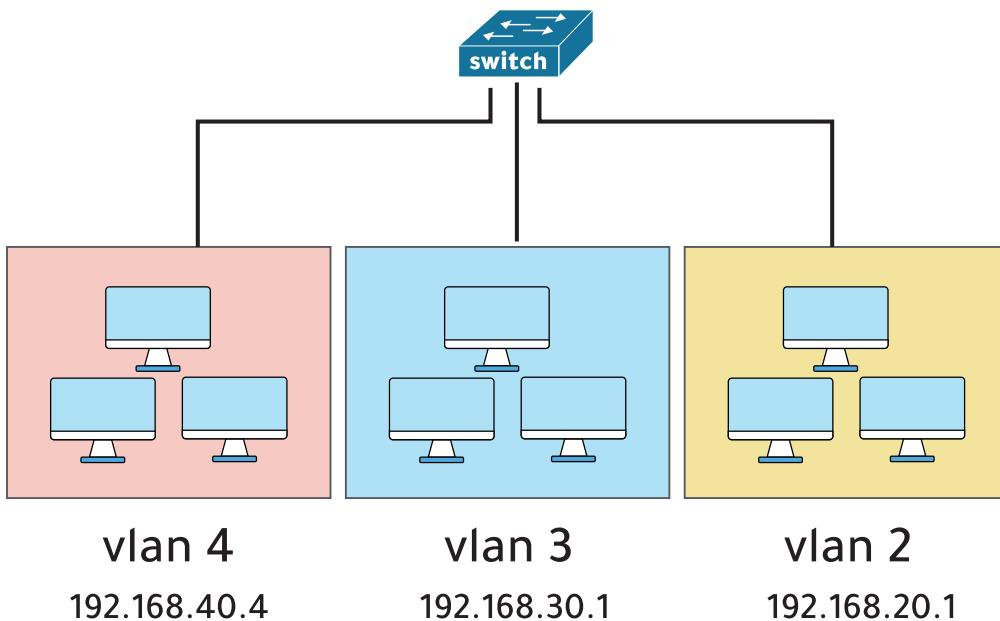
لحذف الماکات بداخل الجدول

Switch# clear mac address-table

Switch# show mac address-table

Vlan	Mac Address	Type	Ports
1	AAA	DYNAMIC	Fa0/1
1	CCC	DYNAMIC	Fa0/3

لاحظ إن كل شبكة منفصلة عن شبكة أخرى ولها آي بي (ip) مختلف.



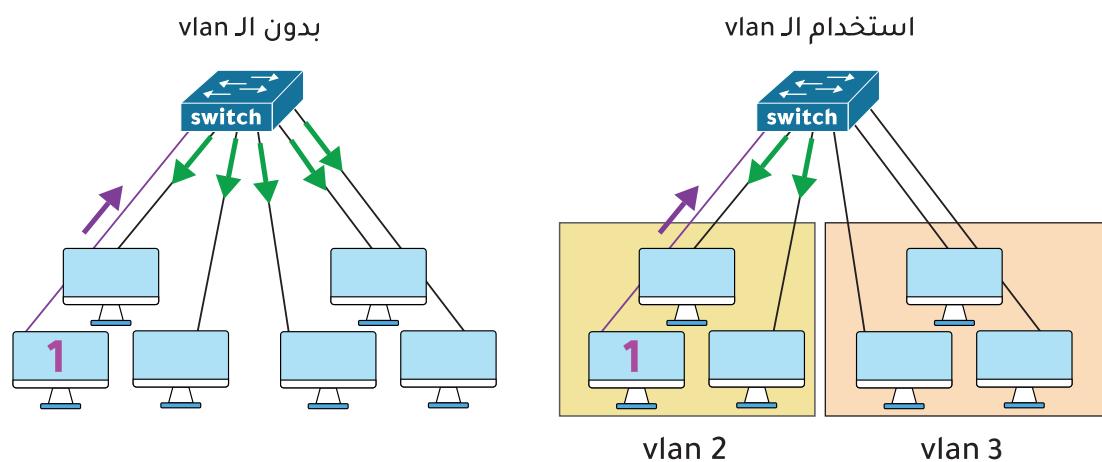
## الشبكة المحلية الافتراضية (VLAN) Virtual Local Area Network (VLAN)

هي عبارة عن شبكة وهمية موجودة في داخل سويفتات سيسكو فقط حيث يتم تقسيم منافذ السويفت إلى عدة شبكات كل منها منفصلة عن الآخر بشكل وهمي وغير مرئي.

- تفصل كل شبكة لها فيلان (vlan) عن الشبكة الأخرى.
- كل فيلان (vlan) تمثل广播 domain (شبكة مستقلة).

### فوائد شبكة VLAN :

- 1- التقليل من عملية البث المباشر .BroadCast
- 2- السهولة في ادارة و صيانة الشبكات .
- 3- الحماية والامن ، حيث لو حصل اختراق في شبكة 2 مثلاً فلن يستطيع الوصول للشبكة الأخرى مثلًا 3 .
- 4- تقليل الجهد والحمل على السويفت .



لاحظ كيف تم التقليل من إلـ Broadcast عند استخدام نظام الشبكات الـ VLAN .

## أنواع VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Gig0/1, Gig0/2
10 VLAN0010	active	
20 VLAN0020	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	
محجوزة في النظام		

### Data VLAN - 1

شبكة تستخدم في تبادل البيانات بين المستخدمين .

### Default VLAN - 2

شبكة الـ Default VLAN تكون موجودة داخل السويفت بشكل تلقائي وافتراضي ورقمها واحد . ويكون جميع منافذ السويفت تحت هذه الشبكة ، ولا يمكن حذفها أو إعادة تسميتها أو تعديلها .

### Native VLAN - 3

هي فيلان تكون فيها الفريمات بدون تاق untagged (بدون رقم للفيلان أو غير مختومة برقم فيلان ) .

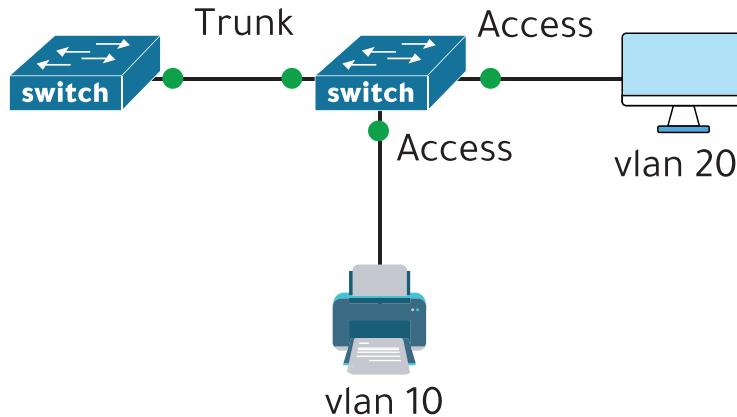
### Voice VLAN - 4

هي تقوم بنقل بيانات الصوت فقط وأعطائها أفضليه في التوجيه وعدم الانتظار لأنها مهمة .

## أنواع منافذ شبكة الـ VLAN

### VLAN Port Type

كل منفذ في السويفت يكون له وضعان :



#### Access Port - 1

- يستخدم منفذ (Access Port) في توصيل منفذ السويفت بالاجهزة الاخيرة (end device) مثل (الحاسوب - الطابعة - السيرفر ) .
- يستخدم منفذ (Access Port) لنقل فيلان واحدة فقط . one vlan
- اي ان المنفذ لا يقبل اكثرب من فيلان .

#### Trunk Port - 2

- يستخدم منفذ (Trunk Port) في توصيل منفذ السويفت بسويفت اخر او براوتر آخر .
- يستخدم هذا الوضع لنقل اكثرب من فيلان vlan بين السويفتات .
- عند تفعيل الـ trunk port على أحد منافذ السويفت فإنه يتفعل تلقائيا على منفذ السويفت الآخر .

#### IEEE 802.1Q - 2

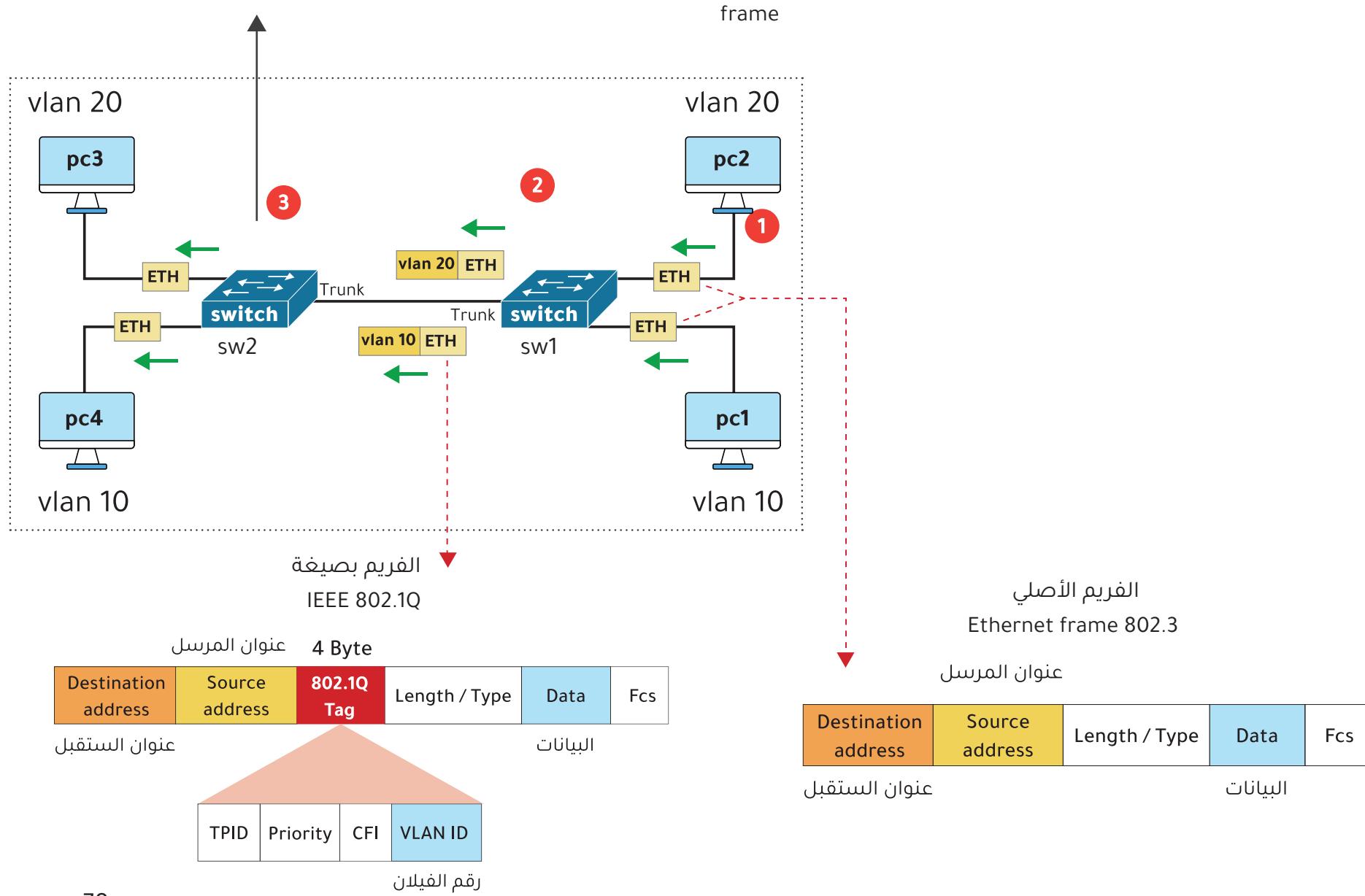
هو بروتوكول قياسي عالمي أنشئته منظمة الـ IEEE وهو المستخدم الان في كل أجهزة سيسكو والشركات الأخرى ويسمى بـ dot1q .

- يعمل بروتوكول الـ 802.1Q على تغليف الفريم (Encapsulation) ليكون على صيغة IEEE 802.1Q ويضيف له تاق ( مثل اضافة بطاقة فيها بيانات ) حجمه 4 بايت يكون فيه ارقام الفيلنات التي يحملها للسويفت الآخر .

هناك نوعين من بروتوكولات الـ trunking :

- Inter-Switch Link (ISL) بروتوكول قديم مملوك لشركة سيسكو وغير مدعوم في الاجهزة الحديثة .

يقوم السويفت الثاني بقراءة الـ Tag الموجود لمعرفة الـ VLAN المراد الوصول اليها و من ثم يحذف هذا الـ Tag فيعود الفريم الى وضعه الاصلی Ethernet 802.3

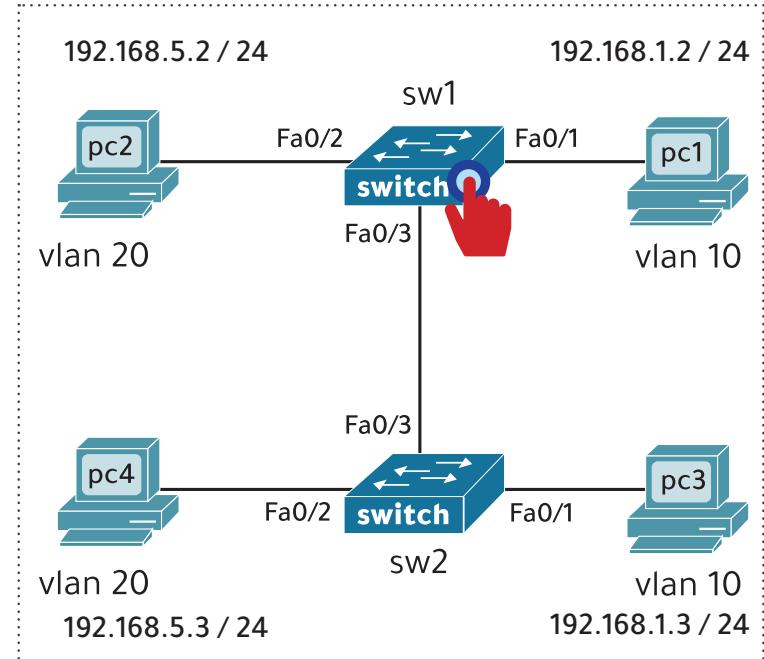


## ≡ إنشاء الفيلان وربطها بالمنفذ

SW1	
SW1> en	
SW1#conf t	
SW1(config)# vlan 10	إنشاء الفيلان
SW1(config-vlan)# name HR	تسمية الفيلان
SW1(config-vlan)# exit	
SW1(config)# vlan 20	
SW1(config-vlan)# name sales	
SW1(config-vlan)# exit	
SW1(config)# interface fa0/1	الدخول على المنفذ
SW1(config-if)# switchport mode access	تشغيل وضع الـ Access
SW1(config-if)# switchport access vlan 10	ربط فيلлан 10 بالمنفذ 1
SW1(config-if)# exit	
SW1(config)# interface fa0/2	ربط فيللان 20 بالمنفذ 2
SW1(config-if)# switchport mode access	
SW1(config-if)# switchport access vlan 20	
SW1(config-if)# exit	
SW1(config)# interface fa0/3	تغيير وضع الكيبل الذي بين السويتشين الى trunk
SW1(config-if)# switchport mode trunk	

- تستطيع إنشاء عدد 4094 فيللان .
- توجد ارقام محجوزة في النظام لا تستطيع انشاء فيللانات بنفس أرقامها وهي فقط : 0 - 1 - 1002 - 1003 - 1004 - 1005
- لايمكن ان يكون اكثرا من فيللان في المنفذ الواحد ما عدا فيللان الصوت وهذا استثناء حيث يمكن ان يكونان معا في منفذ واحد .

فتح برنامج الـ packet tracer  
ننفذ مثل هذا النموذج



SW1

SW1# show interfaces fa0/3 switchport

Name: Fa0/3

Switchport: Enabled

Administrative Mode: **trunk**Operational Mode: **trunk**Administrative Trunking Encapsulation: **dot1q**Operational Trunking Encapsulation: **dot1q**

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Trunking VLANs Enabled: **All**

تم إعداد هذا المنفذ يدوياً إلى trunk  
 ( يعني المهندس هو من غيره إلى trunk )

هنا وضع المنفذ fa0/3 ولللحظ أنه في وضع  
 trunk إلى

أيضاً نلاحظ التغليف هنا بـ dot1q

نستعرض عملياً السابق بكتابة أمر  
 show vlan brief

SW1# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Gig0/1, Gig0/2
10	HR	active	Fa0/1
20	sales	active	Fa0/2

الفيلنات التي تم إنشائهما

SW1# show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/3	on	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/3 1-1005

Port Vlans allowed and active in management domain  
 Fa0/3 1,10,20

الفيلنات الفعالة والمسموحة لها بالمرور

نطبق الخطوات السابقة على  
السويتتش الآخر

```

SW2

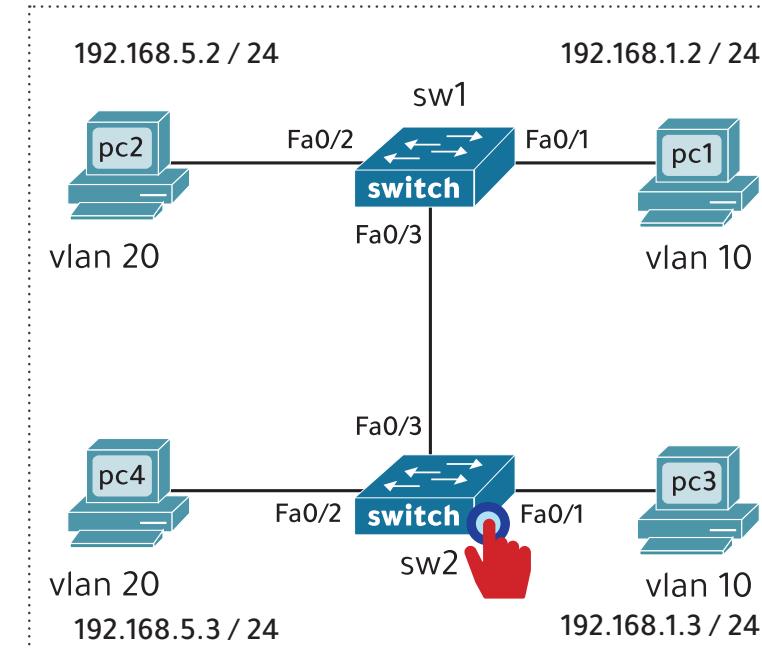
SW2> en
SW2 #conf t
SW2(config)# vlan 10
SW2(config-vlan)# name HR
SW2(config-vlan)# exit
SW2(config)# vlan 20
SW2(config-vlan)# name sales
SW2(config-vlan)# exit

SW2(config)# interface fa0/1
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 10
SW2(config-if)# exit

SW2(config)# interface fa0/2
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 20
SW2(config-if)# exit

SW2(config)# interface fa0/3
SW2(config-if)# switchport mode trunk

```



```
SW2# show interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: All
```

هنا حالة وضع المنفذ في السويفتث الشان  
وهو الافتراضي تلقائي(auto)

نتيجة التفاوض التي تم  
ال اختيار عليها وهي trunk  
ايضا نلاحظ التغليف هنا بـ dot1q

```
SW2# show interfaces trunk
Port      Mode       Encapsulation  Status        Native vlan
Fa0/3    auto      n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/3    1-1005

Port      Vlans allowed and active in management domain
Fa0/3    1,10,20
```

لاحظ هنا أن البورت Fa0/3 تحول  
تلقائياً إلى وضع الـ trunk .

حرف n بجانب كلمة 802.1q يعني أنه اختار  
البروتوكول 802.1q عن طريق التفاوض  
(Negotiation)

أولاً : ندخل الـ IP لـ كل جهاز بـ شكل يـ دوي

IP Configuration

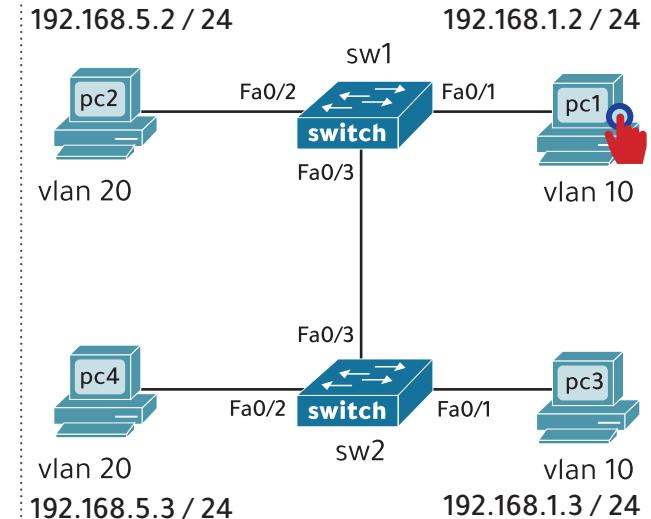
DHCP  Static **4**

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0



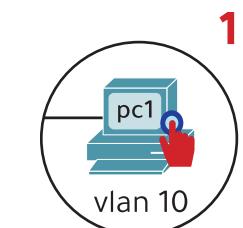
```
pc 1
C:\> ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

هذا الرد من الجهاز  
الآخر PC3

ثانياً : نعمل اختبار الاتصال بين PC1 و PC3 في نفس الفيلان 10 عبر الأمر : ping

ping 192.168.1.3



نجح الاتصال مع الجهاز حيث ارسل 4 بكتات  
واستقبل الرد من الجهاز 4 بكتات

ملاحظة :

- 2 - اذا كان السوينتشات يدعم هذا النوع IEEE 802.1Q فإنه يكفي هذا الأمر لإعداد الـ trunk .

```
SW1(config)# interface fa0/3  
SW1(config-if)# switchport mode trunk
```

- 1 - بعض السوينتشات تدعم النوعين ( IEEE 802.1Q - ISL ) الخاصين بـ trunk ، لذلك عند ادخالك لهذا الأمر

```
SW1(config)# interface fa0/3  
SW1(config-if)# switchport mode trunk
```

ستظهر لك هذه الرسالة :

Command rejected : An interface whose trunk encapsulation is ( Auto ) can not be configured to ( trunk ) mode

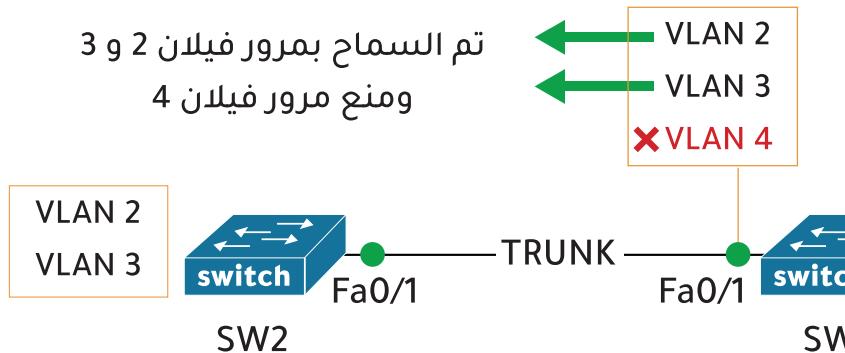
الحل : ادخال أمر التغليف بـ dot1q قبل أمر الـ trunk فيصبح الأمر كاملاً :

```
SW1(config)# interface fa0/3  
SW1(config-if)# switchport trunk encapsulation dot1q  
SW1(config-if)# switchport mode trunk
```

## السماح والمنع في وضع الـ Trunk

### VLAN Trunks Allowed

نستطيع عبر منافذ السويفت التي يكون الوضع بينهما أن نسمح ونمنع مرور فيلنانات محددة . تفينا من ناحية الأمان وايضاً من ناحية عدم الحاجة لفيلنانات محددة على السويفتشات الأخرى .



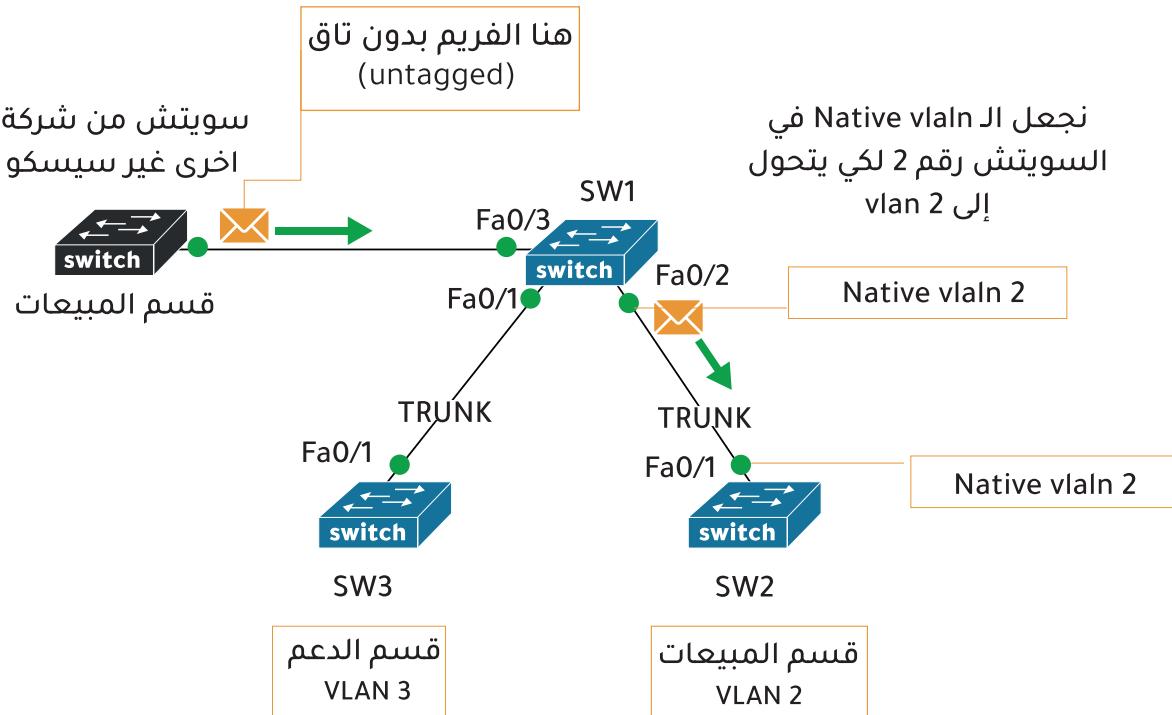
VLAN 2  
VLAN 3  
VLAN 4

إعدادات السماح والمنع عبر بروتوكول الـ trunk

```
SW1> en
SW1#conf t
SW1(config)# interface fa0/1
SW1(config-if)# switchport trunk allowed vlan ?
WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
add     add VLANs to the current list
all    all VLANs
except  all VLANs except the following
none   no VLANs
remove  remove VLANs from the current list
SW1(config-if)# switchport trunk allowed vlan remove 4
SW1(config-if)# end
SW1# wr
```

الدخول على المنفذ أو البورت  
نستعرض الخيارات المتاحة :  
تكتب رقم الفيلنان المراد السماح له فقط بالمرور  
اضافة فيلنان آخرى للقائمة الحالية للمرور  
السماح لكل الفيلنانات  
السماح لكل الفيلنانات ما عدا  
لا يسمح لاي فيلنان بالمرور  
حذف رقم الفيلنان من القائمة المسماحة لها بالمرور

حذف فيلنان 4 من القائمة لكي لا يسمح لها بالمرور



## Native vlan ≡

هي فيلان يكون فيها الفريم بدون تاق (بدون رقم للفيلان) .

- مثلا سوپریش من شركة اخرى عليه اجهزة وهذا السوپریش لا يعمل بنظام الفیلان ، ولکي نجعله يتواصل مع الاجهزه الاخرى في نفس القسم نوجهه للفیلان المخصصة بذلك القسم باعطائه رقم vlan نفس رقم فيلان القسم ، انظر الصورة لكي تتضح لك

- مهم جدا ان يكون رقم الـ Native vlan متساوي في المنفذين .

- نقوم بتحديد رقم الـ Native vlan في وضع الـ trunk لكي توجه الفیلانات التي بدون تاق الى فيلان محددة مسبقا .

- يُنصح بتحديد الـ Native vlan الى فيلان غير مستخدمة وذلك لأسباب أمنية .

نستعرض حالة الـ interface fa0/2 عن طريق كتابة الامر

`show interfaces fa0/2 switchport`

وبالمختصر

`sh int fa0/2 sw`

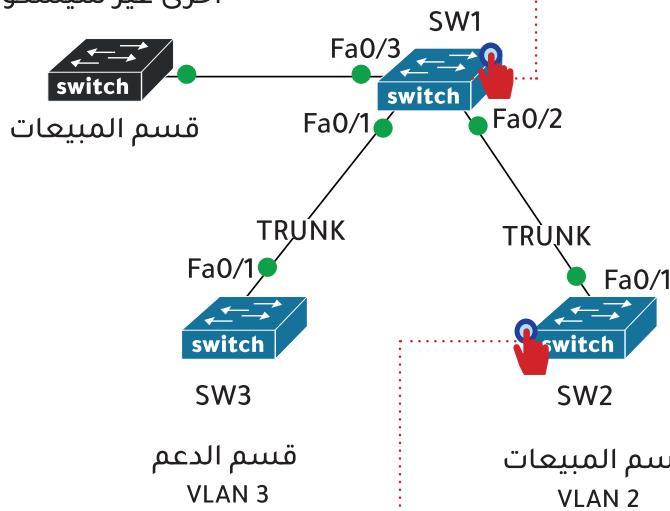
```
SW1(config)# sh int fa0/2 sw
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 2 (Inactive)
Voice VLAN: none
....
```

تم التغيير الى native vlan 2

إعدادات الـ Native vlan

```
SW1(config)# interface fa0/2
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 2
SW1(config)# exit
SW1# wr
```

سويفتش من شركة  
اخري غير سيسكو



```
SW2(config)# interface fa0/1
SW2(config-if)# switchport mode trunk
SW2(config-if)# switchport trunk native vlan 2
SW2(config)# exit
SW2# wr
```

## إنشاء فيلان للصوت

### Create Voice VLAN

نتعرف أولاً على الهاتف بنظام الآيبي (ip phone) مثل هواتف سيسكو .

- تستخدم هواتف الـ IP تقنيات نقل الصوت عبر الآيبي VoIP وهي اختصار (Voice over IP) لتمكين المكالمات الهاتفية عبر شبكة الـ ip .

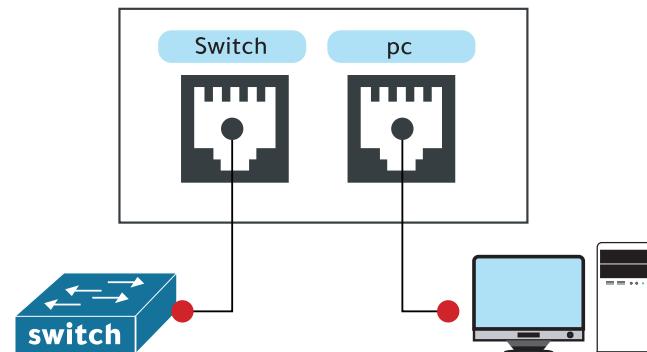
- تستخدم Voice VLAN لنقل الصوت الى هاتف سيسكو .

- يعني يتم نقل الصوت بين هواتف سيسكو عبر هذه الفيلان - كما تعرفنا سابقاً ان الفيلانات العادية تنقل البيانات وتسمى data vlan اما فيلان الصوت تنقل الصوت بين هواتف سيسكو وتسمى voice vlan حيث يستطيع المتصل الاتصال والحديث مع الطرف الآخر .

- يتم توصيل السويفت بالهاتف ويتم توصيل الكمبيوتر بالهاتف .



منفذ هاتف سيسكو



السويفت سوف يستخدم بروتوكول CDP ليخبر الهاتف بوضع علامة (TAG) في الفيلان رقم 11



فتح برنامج لـ packet tracer  
ننفذ مثل هذا النموذج

```

Switch> en
Switch #conf t
Switch(config)# vlan 100
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# exit

Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 200
Switch(config-if)# exit
Switch(config)# exit
Switch# wr

```

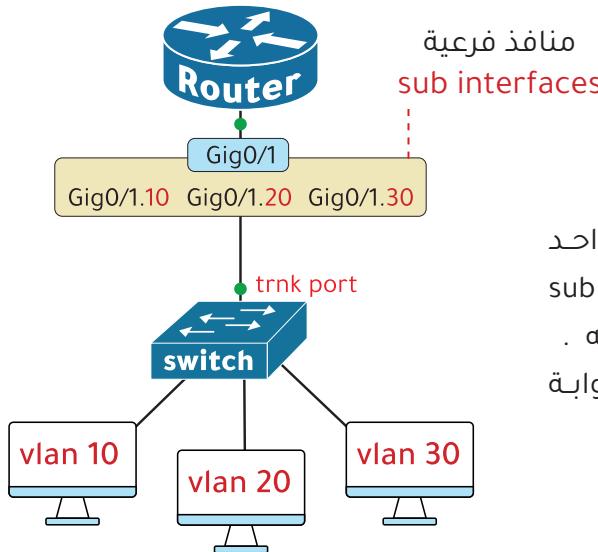
نشأ الفيلنات

ربط الفيلنات بالمنفذ

حفظ الاعدادات

ملاحظة :

وضع المنفذ fa0/1 سوف يكون access وليس trunk

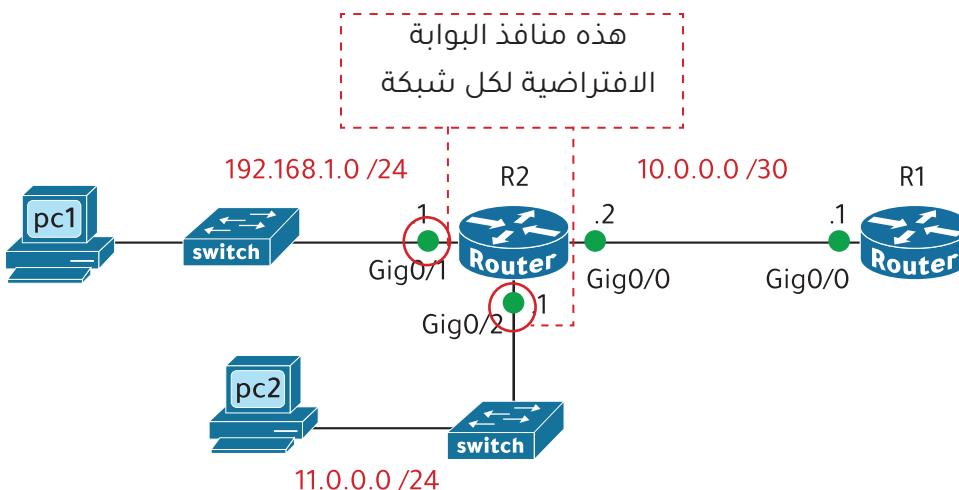


### Router on a stick (ROAS) - 2

في هذه الطريقة يتم تقسيم منفذ واحد على الراوتر الى منفذ فرعية sub interfaces ويكون لكل منفذ فرعي فيلنان خاص به .  
- هذا المنفذ الفرعي يكون عنوان البوابة الافتراضية للفيلنان .

ملاحظة :

الـ **Default Gateway** هي البوابة او الممر بين الشبكات المختلفة .  
يعني اذا انت في شبكة A مثلاً وأردت الخروج لشبكة B فلابد أن تعبّر من الباب الذي يخرج بك للشبكة الأخرى وهذا الباب يسمى البوابة الافتراضية (Default Gateway).  
انظر الصورة للتوضيح أكثر .



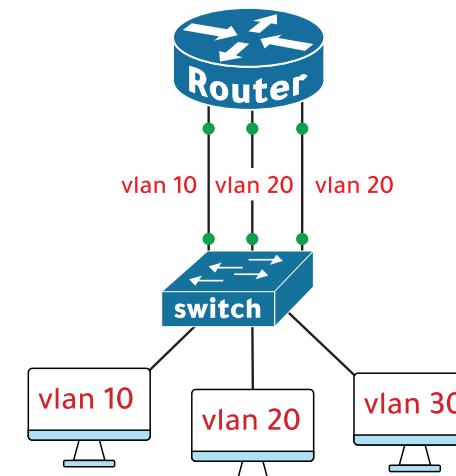
## Inter VLAN Routing

فكرة الـ Inter VLAN Routing هي السماح للفيلنان المختلفة بالتواصل مع بعضها البعض .

هناك 3 طرق لتنفيذ وتطبيق الـ Inter VLAN Routing :

### Traditional Inter-VLAN Routing - 1

في هذه الطريقة يكون لكل فيلنان منفذ خاص لها على الراوتر وهي طريقة ليست جيدة و غير مستعملة لأنها تحتاج لمنافذ كثيرة على الراوتر .

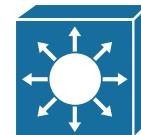


- عند إنشاء منفذ افتراضي (SVI) يجب أن يكون مطابق للفيilan الموجودة داخل السويتش .
- . فمثلاً أنشأنا 10 vlan ، إذاً يكون المنفذ الافتراضي للـ 10 vlan . هذه طريقة التنفيذ :

```
SW1 (config) # int VLAN 10
SW1 (config-if) # ip address 192.168.10.1 255.255.255.0
```

- أيضاً يجب تفعيل أمر التوجيه (Routing) في وضع الاعداد لكي يسمح للفيilanات بالتواصل مع بعضها البعض .

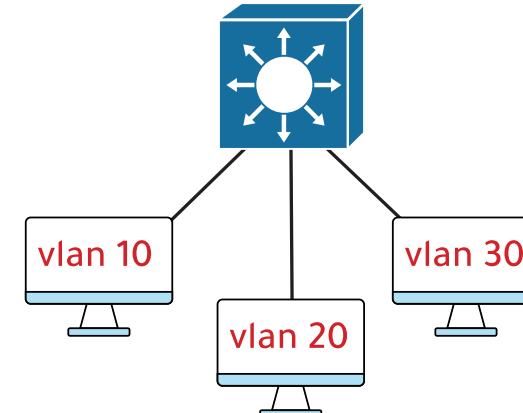
```
SW1 (config) # ip routing
```



### Multilayer Switch - 3

الـ **Multilayer** هو سويتش من الطبقة الثالثة Layer 3 يستطيع التعامل مع الآيبي وعمل توجيه للبيانات (routing) ، فهو يؤدي وظائف الراوتر والسويتش معاً

- في هذه الطريقة يتم إنشاء **منفذ افتراضي** لكل فيilan داخل السويتش واعطائه آيبي يمثل البوابة الإفتراضية لهذا الفيilan .
- يطلق على **المنفذ الافتراضي** بالـ (SVI) .
- الـ SVI هو منفذ أو واجهة افتراضية يتم إنشاؤه على فيilan محدد حيث يمكن استخدام الآيبي كبوابة افتراضية لشبكة الفيilan .



## التطبيق بطريقة الـ Router-on-a-stick

لدينا هذا النموذج في الباكت تريسيروسوف نفعل  
التوجيه بطريقة الـ Router-on-a-stick

```

SW1
SW1 > en           إنشاء الفيلنات
SW1# conf t
SW1(config)# Vlan 10
SW1(config-vlan)# Vlan 20
SW1(config-vlan)# exit

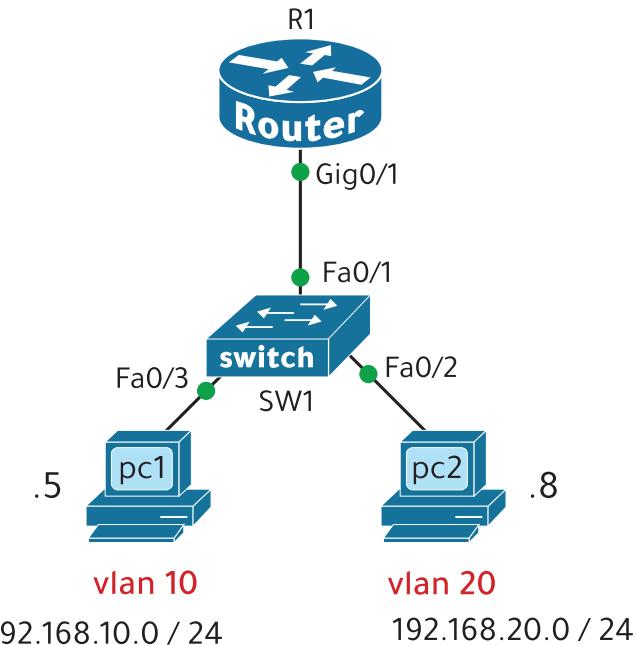
1
SW1(config)# int fa0/2      الربط بالمنفذ
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# exit

SW1(config)# int fa0/3
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# exit

SW1(config)# int fa0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# end
SW1# wr

```

تحويل المنفذ لوضع الـ trunk لأنه سوف يعبر عن  
طريقه عده فیلنات



### مراحل الحل :

- 1 إنشاء الفيلنات في السويفت وربطها بالمنفذ
- 2 تفعيل منفذ الراوتر الذي سوف يتم انشاء منفذ فرعية منه.
- 3 إنشاء المنفذ الفرعية واضافة الايبيات لها .

نكتب اسم المنفذ ونضع نقطة (.) وبعدها رقم الفيلان

لابد أن نوضح للراوتر انه يعمل بنظام الـ dot1Q وأن الفيلان رقم 10 تكون لهذا المنفذ g0/0.10

نضيف الايبي ويكون هذا الايبي هو البوابة الافتراضية ( default gateway ) ويكون من نفس مدى شبكة الفيلان

#### ملاحظة :

في حال تغيير الـ native vlan . يجب أن تكون متطابقة في السويفتش والراوتر .

فمثلا لو أردنا أن يكون الـ native vlan هو 10 فنرجم لسويفتش وندخل هذا الأمر على المنفذ fa0/1

```
SW1(config)# int fa0/1
SW1(config-if)# switchport trunk native vlan 10
```

ونذهب للراوتر وندخل على المنفذ الفرعى الخاص بفيلان 10 native vlan ونضيف له أمر الـ

```
R1(config)# int g0/0.10
R1(config-subif)# encapsulation dot1Q 10 native
```

```
R1# conf t
R1(config)# int Gig0/0
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
R1(config)# int g0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# int g0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# end
R1# wr
```



pc 1

يوجد اتصال بين pc1 و pc2

```
C:\> ping 192.168.20.8
Reply from 192.168.20.8: bytes=32 time<1ms TTL=127
Reply from 192.168.20.8: bytes=32 time=1ms TTL=127
Reply from 192.168.20.8: bytes=32 time=1ms TTL=127
Reply from 192.168.20.8: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```

SW1

SW1> en
SW1# conf t
SW1(config)# Vlan 10
SW1(config-vlan)# Vlan 20
SW1(config-vlan)# exit
1

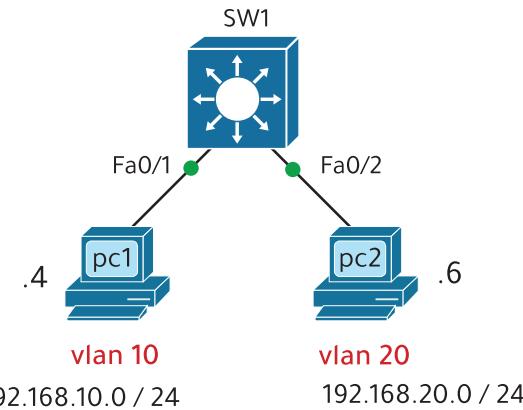
SW1(config)# int fa0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# exit

SW1(config)# int fa0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# exit

SW1(config)# ip routing
2

SW1(config)# int vlan 10
3
SW1(config-if)# ip add 192.168.10.1 255.255.255.0
SW1(config-if)# exit
SW1(config)# int vlan 20
SW1(config-if)# ip add 192.168.20.1 255.255.255.0
SW1(config-if)# end

```



## التطبيق على الـ Multilayer Switch

لدينا هذا النموذج في الباكت تريسر وسيتم تطبيق الـ Inter VLAN Routing

### مراحل الحل :

- 1 إنشاء الفيلنات في السويتش وربطها بالمنافذ
- 2 تفعيل التوجيه (Routing)
- 3 إنشاء الـ SVI لكل فيلان واضافة الايبي لكل فيلان (يعتبر هذ الايبي بوابة افتراضية للفيلن).
- 4 اختبار الاتصال بين pc1 و pc2

**pc 1**

يوجد اتصال بين pc1 و pc2

```

C:\> ping 192.168.20.6
Reply from 192.168.20.6: bytes=32 time<1ms TTL=127
Reply from 192.168.20.6: bytes=32 time=1ms TTL=127
Reply from 192.168.20.6: bytes=32 time=1ms TTL=127
Reply from 192.168.20.6: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

```

**4**

## بروتوكول VLAN Trunk Protocol

- بروتوكول خاص بشركة سيسكو يعمل على أجهزة السويفت و فكرة الـ VTP إنه يتيح لك إنشاء شبكات الـ VLAN على سويفت رئيسي يسمى بـ (VTP Server) وستقوم السويفت الأخرى التي تسمى بـ (VTP Client) بمزامنة ونسخ هذه الفيلنات من السويفت الرئيسي .
- يعني إذا انشأت عدد 4 فيلنات في السويفت الرئيسي فإن السويفت الأخرى تأخذ نسخة من هذه الفيلنات .
  - مصمم للشبكات الكبيرة بحيث لا تضطر إلى إنشاء كل فيلن على كل سويفت .
  - نادراً ما يتم استخدامه ويوصي بعدم استخدامه .

### أوضاع الـ VTP

VTP Mode

#### 1 - الخادم : VTP Server

- هو السويفت الرئيسي بمعنى أنه هو من ينشئ الفيلنات ويعدها ويرسل التحديثات للجهاز الآخر الذي هي المستضاف (Client) (يعني الإصدار) في كل مرة يتم
- سبب زيد رقم المراجعة Revision Number (يعني الإصدار) في كل مرة يتم فيها إضافة / تعديل / حذف شبكة محلية ظاهرية (VLAN) .

#### 2 - العملاء : VTP Client

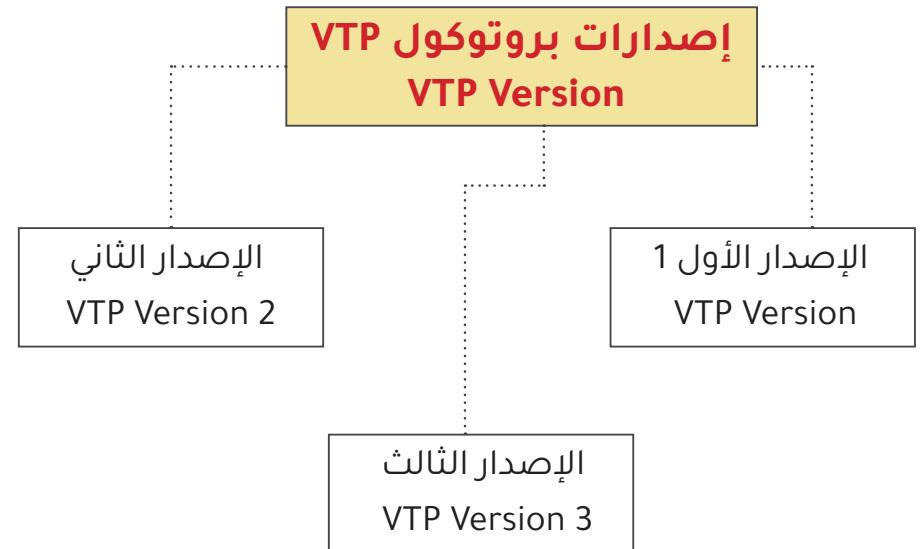
- هذا النوع سيكون السويفت المستقبل للتحديثات والبيانات والشبكات من السويفت الرئيسي وهذا النوع لا يمكن له أن ينشأ أو يعدل أو يضيف أو يحذف فيلنات .

- تقوم سويفت الـ VTP Client بتحديث نسخ الفيلنات التي عندها بناءً على رقم المراجعة ، إذا رقم أعلى يتم التحديث أما إذا أقل فلا يتم التحديث .

#### 3 - المحايد أو الشفاف : VTP Transparent

- يعمل بشكل مستقل ولا يطبق أي تعليمات أو تحديثات من السويفت الرئيسي .

- فهو يستخدم في عملية نقل المعلومات والتحديثات الخاصة في بروتوكول VTP لجهاز السويفت الآخر .



## الفروق بين الأنواع الثلاثة

### VTP Transparent

### VTP Client

### VTP Server

ينشأ فيلرانات

لا ينشأ فيلرانات

ينشأ فيلرانات

يحذف الفيلرانات

لا يحذف الفيلرانات

يحذف الفيلرانات

يعدل على الفيلرانات

لا يعدل على الفيلرانات

يعدل على الفيلرانات

لا يرسل الفيلرانات

لا يرسل الفيلرانات

يرسل الفيلرانات

يتزامن مع التحديثات (يعني  
يحدث نفسه بالجديد)

يتزامن مع التحديثات (يعني  
يحدث نفسه بالجديد)

يتزامن مع التحديثات (يعني  
يحدث نفسه بالجديد)

يعيد توجيه تحديثات الفيلرانات

يعيد توجيه تحديثات الفيلرانات

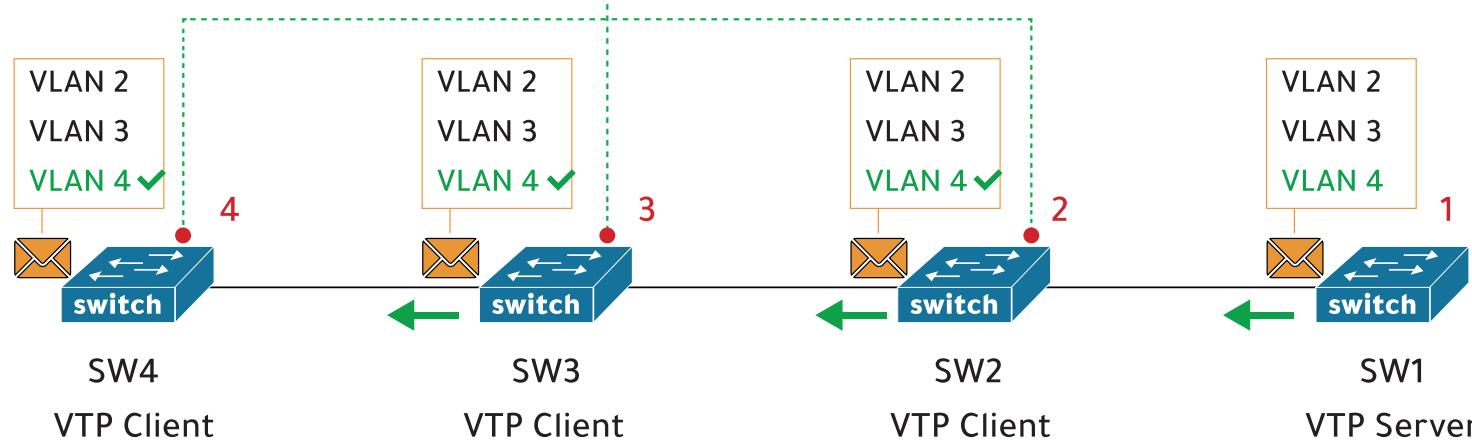
يعيد توجيه تديثات الفيلرانات

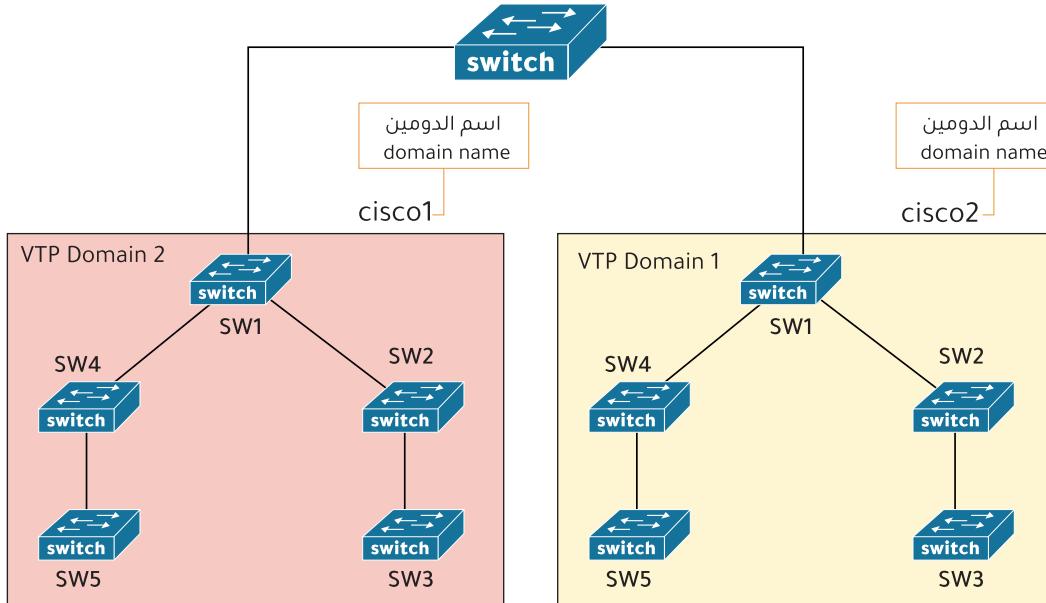
يتخزن في الـ Nvram

يتخزن في الـ flash

يتخزن في الـ flash

- ✓ يعمل تحديث (update) بالمعلومات الجديدة
- ✓ يعيد توجيه الرساله لل التالي forwards





## النطاق (المجال) VTP Domain

فكرة هذا النطاق هي أن تقوم بتنظيم جميع السويتشات تحت نطاق واحد (قسم واحد) بأسم نطاق معين . يعني لكل نطاق او قسم اسم محدد له . شاهد الشكل لتوضح لك الصورة

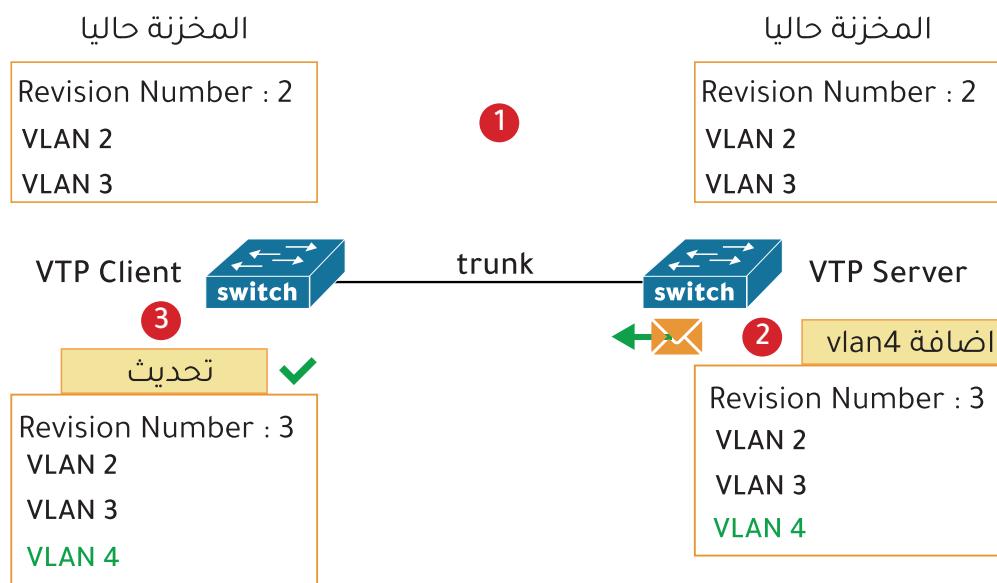
## أرقام الريفيجن (المراجعة) Revision Number

هذا عدد يزيد عند حدوث تعديل فيلران أو اضافة فيلران أو حذف فيلران ، وقيمة الافتراضية صفر .

- اي سويتش Client يستقبل تحديثات من السويتش الرئيسي ينظر أولا لهذا الرقم :

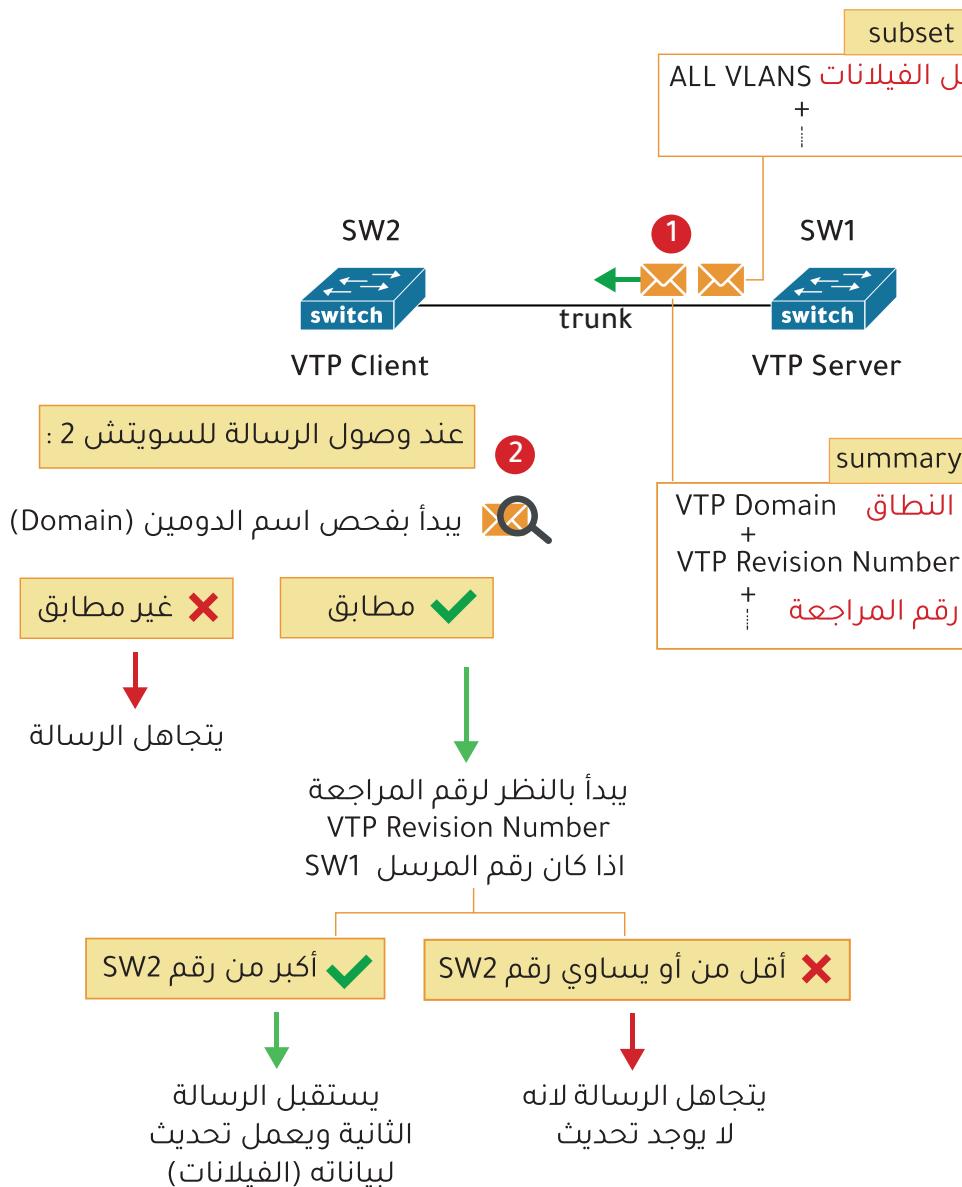
- اذا كان اصغر أو يساوي من الرقم الذي عنده فإنه لا يوجد تحديث .

- اذا أكبر من الرقم الذي عنده فإنه يستقبل التحديث الجديد وينفذه.



## ملاحظة: سبب عدم استخدام بروتوكول الـ VTP

لو كان رقم المراجعة في سويتشات الشركة مثلا 5 وتم اضافة سويتش قديم او معدل عليه بفيلرات مختلفة ورقم مراجعة 8 فإنه سوف يتم تحديث كل سويتشات الشركة من هذا السويتش القديم أو المعدل لأن لديه رقم مراجعة أعلى وستخسر جميع الفيلرات التي تم اعدادها على سويتشات الشركة .



## VTP Messages

أنواع الرسائل في هذا البروتوكول:

**summary advertisement - 1**

رسالة فيها ملخص المعلومات ومنها رقم المراجعة (VTP Revision Number) و النطاق (VTP Domain) . هذه الرسالة لا تحمل معلومات عن الفيالنات .

**subset advertisement - 2**

رسالة فيها المعلومات عن الفيالنات المخزنة  
رسائل الـ 1 و 2 يرسلهم الخادم VTP Server

**request advertisement - 3**

رسالة يرسلهم الـ VTP Client للـ VTP Server لطلب تحديث الفيالنات التي عنده .

## إعدادات بروتوكول VTP

### VTP Configuration

```

SW2> en
SW2 #conf t
SW2(config)# vtp domain sky1 ..... نضع اسم للدومين
SW2(config)# vtp password 123 ..... ننشأ كلمة مرور
SW2(config)# vtp version 2 ..... نحدد إصدار البروتوكول
SW2(config)# vtp mode client ..... نحدد وضع البروتوكول
SW2(config)# exit
SW2# wr

```

نضع اسم للدومين  
نشأ كلمة مرور  
نحدد إصدار البروتوكول  
نحدد وضع البروتوكول



```

SW1> en
SW1 #conf t
SW1(config)# vtp domain sky1 ..... نضع اسم للدومين
SW1(config)# vtp password 123 ..... ننشأ كلمة مرور
SW1(config)# vtp version 2 ..... نحدد إصدار البروتوكول
SW1(config)# vtp mode server ..... نحدد وضع البروتوكول
SW1(config)#
SW1(config)# int fa0/1 ..... الدخول على المنفذ fa0/1
SW1(config)# switchport mode trunk ..... تشغيل وضع الـ trunk
SW1(config)# exit
SW1# wr

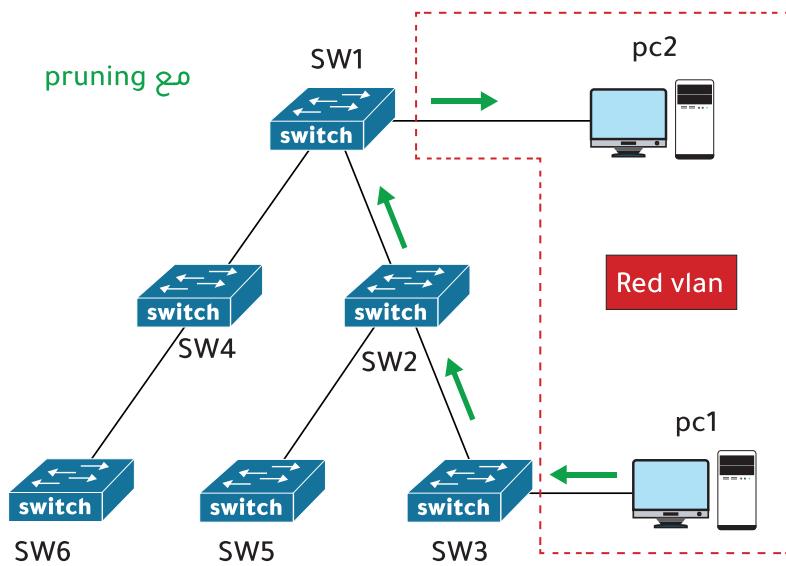
```

نضع اسم للدومين  
نشأ كلمة مرور  
نحدد إصدار البروتوكول  
نحدد وضع البروتوكول  
الدخول على المنفذ fa0/1  
تشغيل وضع الـ trunk

فتح برنامج الـ packet tracer  
- ننفذ مثل هذا النموذج

نستعرض حالة الـ vtp عن طريق كتابة الامر  
show vtp status

SW1		SW2	
SW1> en		السويتش يدعم الإصدارين	
SW1 #conf t		2 و 1	
SW1# show vtp status		الإصدار المفعل الان 2	
VTP Version capable : 1 to 2		اسم الدومين	
VTP version running : 2		وضع الـ pruning	
VTP Domain Name : sky1			
VTP Pruning Mode : Disabled			
VTP Traps Generation : Disabled			
Device ID : 0060.2F30.5700			
Feature VLAN :			
-----			
VTP Operating Mod : Server		وضع الـ vtp الان server وهو	
Maximum VLANs supported locally : 1005		عدد الفيئرانات الموجودة الان	
Number of existing VLANs : 8			
Configuration Revision : 4			
SW1#		رقم المراجعة Revision Number	
		: Client	
		: 1005	
		: 8	
		: 4	
		SW2#	



لاحظ كيف اتجه البرودكاست عبر المنفذ المخصص له والى الاجهزة التي لها وجود في الفيلان الاحمر

```

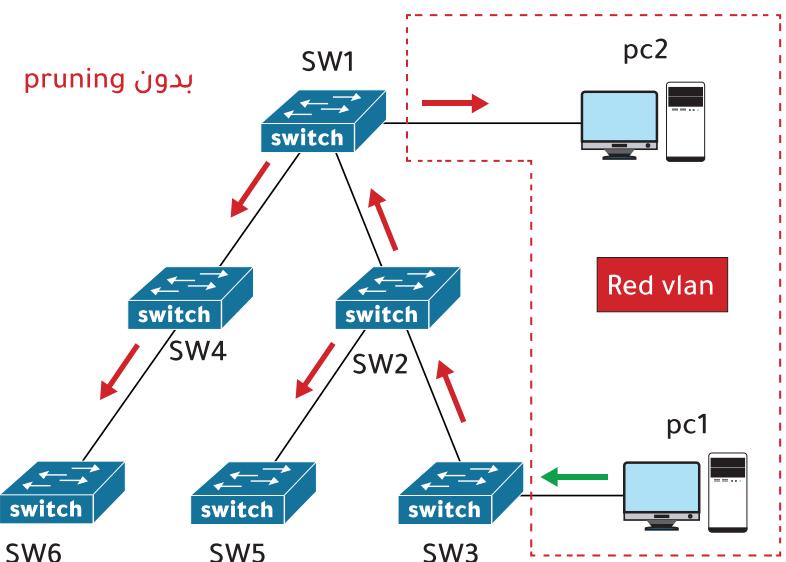
SW2> en
SW2 #conf t
SW2(config)# vtp pruning
SW2(config)# exit
SW2# wr

```

يتم كتابة الامر في السويتش الذي يكون الوضع فيه vtp server وسيتم تفعيله على باقي السوويتشات

**VTP Pruning**

بروتوكول vtp يرسل معلومات الفيلانات لجميع أجهزة السوويتش في الشبكة حتى لو ان بعض الاجهزه لا تستخدم بعض الفيلانات .  
لكي نقلل من حجم البيانات المرسلة والمهدرة بلا فائدة نخبر السوويتشات بارسال الفيلانات المشتركة بينهم والتي عليها اتصال وتبادل بيانات فقط



ارسل برودكاست للجهاز pc2 لأنهم في نفس الفيلان الحمراء ولكن البرودكاست تم ارساله لجميع أجهزة السوويتش والتي ليس عليها منفذ للفيلان الاحمر والتي هي 4 و 5 و 6

## بروتوكول STP

### Spanning Tree Protocol

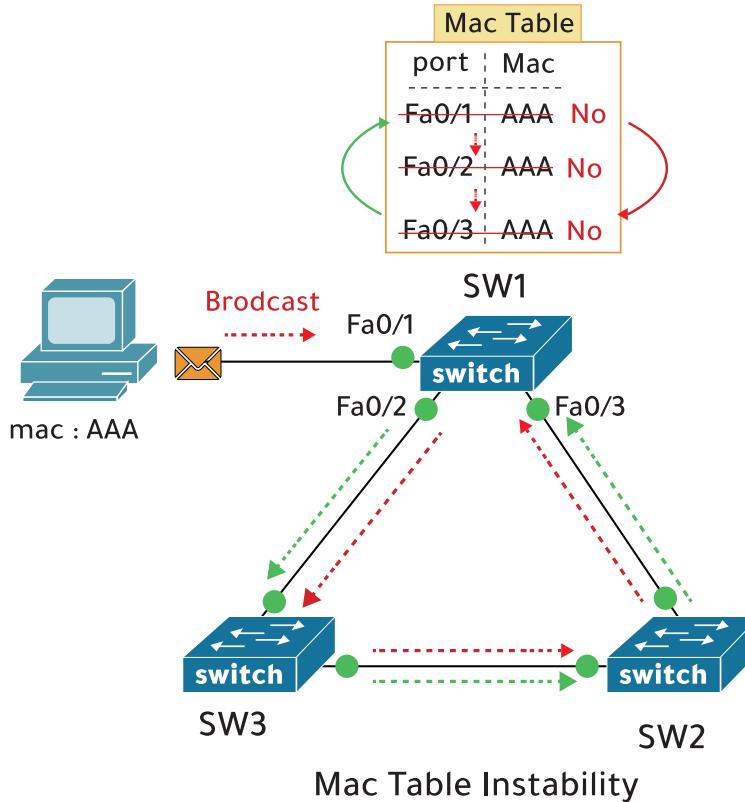
- بروتوكول يرمز له بـ 802.1D .

- وظيفته منع دوران البيانات في السويتشات وهو يعمل في الطبقة الثانية (Layer 2) على اجهزة السويتش.  
هذا البروتوكول يعمل بشكل **تلقائي** ولا يحتاج تفعيله على السويتش .

#### Mac Table Instability - 2

عدم استقرار الماك ادرس او عنوان الجهاز في جدول الماك ادرس في السويتش .

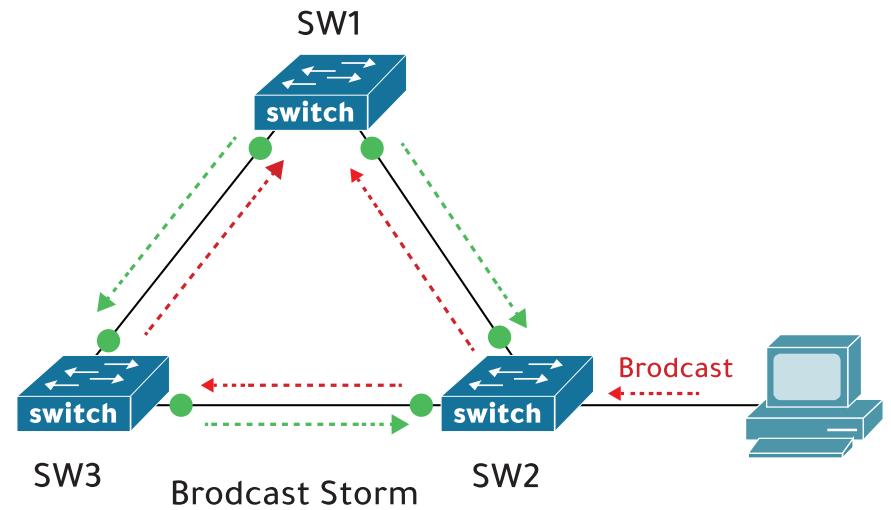
حيث ان السويتش يسجل الماك ادرس من منفذ ومن ثم يأتيه نفس الماك ادرس من منفذ اخر فيقوم بحذف الاول وتسجيل الجديد وهكذا .



#### المشاكل التي تحصل عند عدم عمل بروتوكول STP

##### Broadcast Storm - 1

عاصفة من البث وهي عبارة عن Loop أو دوران البيانات داخل الشبكة بشكل مستمر والتي تبدأ عندما يتم توصيل السويتشات على شكل حلقي بحيث انه لو حدث broadcast داخل الشبكة ستحدث مشكلة تكرار مستمرة للبيانات داخل الشبكة .



## الحل

## بروتوكول STP

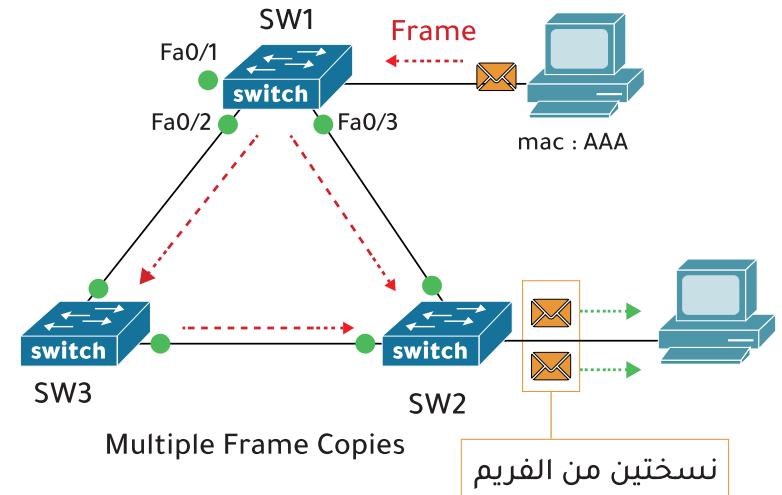
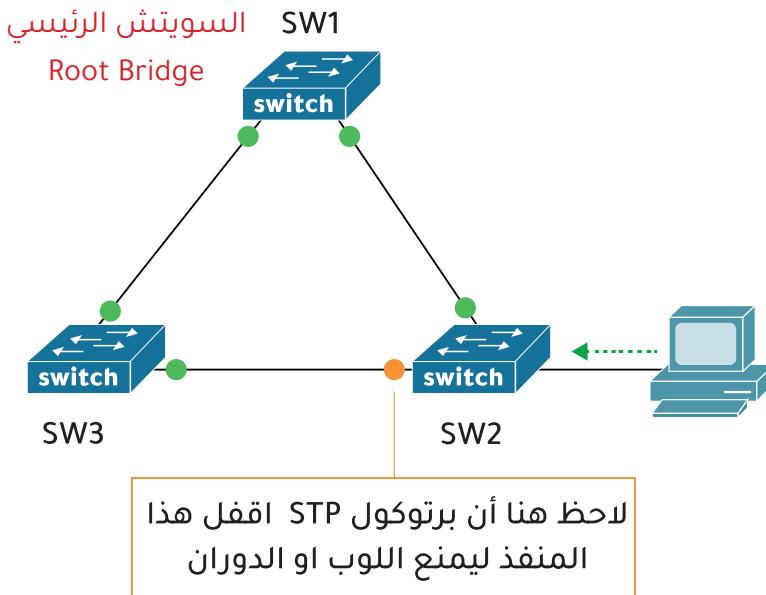
هنا تأتي وظيفة بروتوكول الـ STP ليقوم بتنظيم الوصلات و منع دوران البيانات في السويتشات حيث انه يعمل على

- 1 - تحديد سويتش واحد رئيسي في الشبكة عن طريق Root Bridge التي تتم بين السويتشات ويسمى به Best Path يوصل بالجهاز الرئيسي.
- 2 - اختيار افضل مسار Best Path .
- 3 - قفل وصلات محددة لمنع دوران البيانات .
- 4 - تشغيل المسار الإضافي تلقائياً عند حدوث عطل في المسار الذي تم اختياره .

## Multiple Frame Copies - 3

تعني نسخ متعددة من الفريم . اي ان الجهاز يستلم نسختين من الفريم بسبب عدم وجود بروتوكول stp فمثلاً pc1 ارسل رسالة لـ pc2 فسوف تصل نسختين من الفريم لـ pc2 .

انظر الصورة بالأسفل ليتضح لك المعنى .



### A : الإنتخاب لاختيار الجهاز الرئيسي (Root Bridge)

- عند توصيل السويتتشات بعضها تبدأ بارسال رسالة تسمى : BPDU (Bridge Protocol Data Units)
- يتم تبادل رسائل او BPDU بين أجهزة السويتتش كل ثانيةين .
- لاختيار الجهاز الرئيسي (Root Bridge) يعتمد بروتوكول (STP) على قيمة خاصة في داخل رسالة او BPDU تسمى بـ معرف الجسر (Bridge ID) .

- يتكون او Bridge ID من قسمين :

- 1 - قيمة الأولوية (Priority) : القيمة الافتراضية = 32768 و تبدأ من 0 - 61440
  - 2 - الماك ادرس (Mac Address)
- الجهاز الذي له قيمة Bridge ID اقل سيم اختياره ليكون هو الجهاز الرئيسي . (Root Bridge)

رسالة او BPDU

Root id	Root Path Cost	Bridge id	Port id	Message Age	Max Age	Hello Time
---------	----------------	-----------	---------	-------------	---------	------------

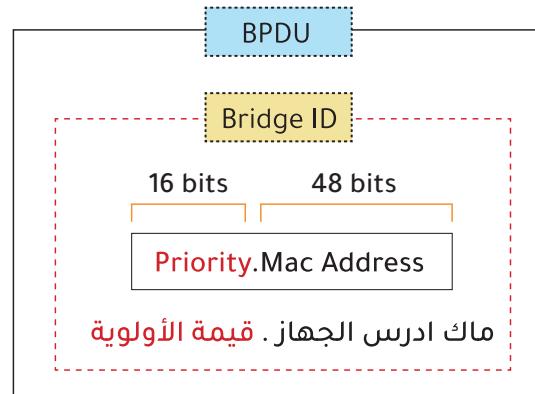
Bridge Priority	Mac Address
-----------------	-------------

يكتب او Bridge ID (BID) بهذه الطريقة

$$BID = \text{Priority}.\text{Mac Address}$$

مثل

$$BID = 32768.0145.A3D1.FBE4$$



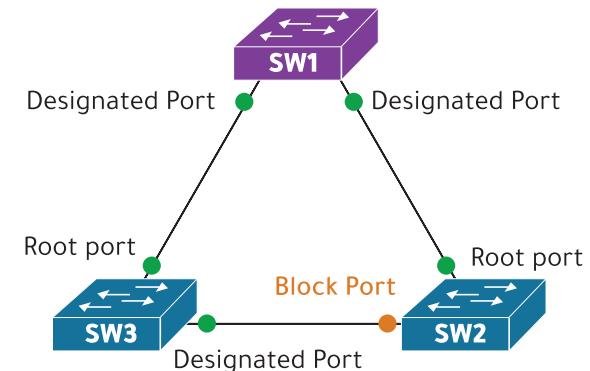
### عملية انتخاب السويتش الرئيسي

#### Root Bridge Election

طريقة عمل بروتوكول او STP :

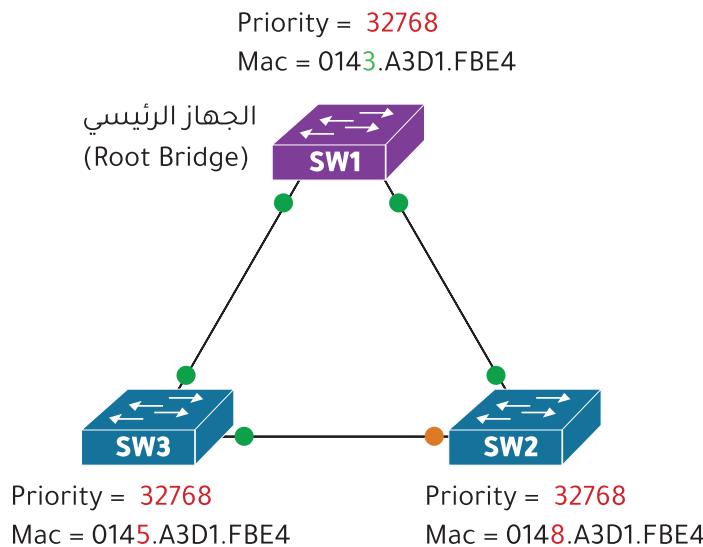
- الإنتخاب لاختيار الجهاز الرئيسي (Root Bridge).
- كل سويتش يحدد منفذ واحد خاص به ك منفذ Root port .
- اي منفذ مقابل لا port يجب أن يكون Root port .
- تحديد منفذ او Designated Port ومنفذ او Block Port .

(Root Bridge)



- بما أن قيمة الأولوية (Priority) متساوية في الأجهزة لأنها جميعاً على القيمة الافتراضية يتم الانتقال للخيار الآخر وهو الأقل في الماك ادرس .

- ننظر إلى الصورة فعندما يقارن السويتش 2 (SW2) عنوانه الماك ادرس مع عنوان السويتش الاول (SW1) يجد ان السويتش الاول أقل منه لذلك يتوقف عن اعلان نفسه انه سويتش رئيسي وكذلك الوضع مع السويتش 3 فيتم انتخاب السويتش الاول سويتش رئيسي .



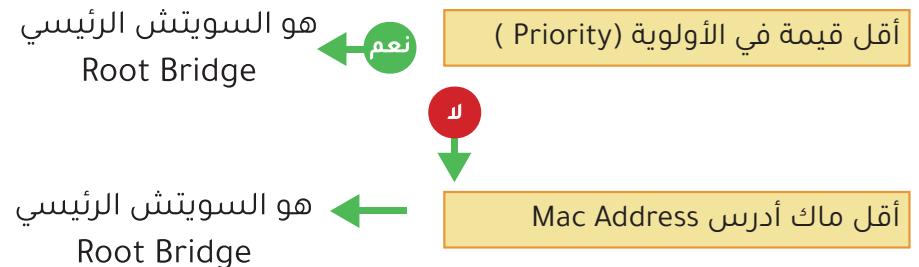
ملاحظة :

- تستطيع تحديد السويتش الرئيسي يدوياً وذلك بتغيير قيمة الأولوية (Priority) .  
- بمضاعفات الرقم 4096 .  
يعني مثل 0 - 8192 - 4096 - 12288 .  
ويتم عبر كتابة الامر:

`Switch# spanning-tree vlan 1 priority 4096`

- كما قلنا عند توصيل السويتشات بعضها تبدأ بارسال رسالة BPDU لكل سويتش أنها هي السويتش الرئيسي .  
طبعاً كل رسالة فيها رقم الأولوية الخاص بالسويتش وعنوان الماك ادرس .

- تبدأ الانتخابات (Election) بالاختيار والمفاضلة :



طريقة المقارنة بين عنوانين ماك ادرس

البداية → ✓MAC:0145.A3D1.FBE4  
MAC:0168.C3F1.F904

العدد 4 أقل من العدد 6

## Root Port (RP) تحديد منفذ الـ

B

كل سويفيتش يحدد منفذ واحد خاص به ك منفذ Root port ماعدا السويفيتش الرئيسي.

- اي منفذ مقابل لـ Root port يجب أن يكون Designated Port
- يقوم كل جهاز غير رئيسي باختيار افضل مسار للجهاز الرئيسي Root Bridge
- وفقاً لقيمة تسمى تكلفة المسار (Path Cost) فالمسار الاقل تكلفته هو المسار الافضل.

### تكلفة المسار :Path Cost

هي قيمة تعتمد على تكلفة المنافذ الواقعة على هذا المسار، فكل منفذ له تكلفة Port Cost

النوع type	السرعة speed	تكلفة المنفذ Port Cost
ethernet	10 Mbps	100
Fast ethernet	100 Mbps	19
Gigabit ethernet	1 Gbps	4
10 Gigabit	10 Gbps	2

## أوضاع المنافذ مع بروتوكول STP

### STP Port Mode



### DP = Designated Port

هو منفذ يعمل بشكل طبيعي ويقوم بعملية إرسال واستقبال البيانات فهو في حالة إعادة توجيهه (forwarding state).  
- الجهاز الرئيسي (Root Bridge) تكون حالة المنفذ عليه DP.

### RP = Root Port

هذا المنفذ يعمل على استقبال وإرسال البيانات فهو في حالة إعادة توجيهه (forwarding state) ولكن يكون فقط على السويفيتش الغير رئيسي (Non Bridge) ويكون صاحب التكلفة الاقل في المسارات الى السويفيتش الرئيسي.

### BLK = Alternate Port (Block Port)

هذا المنفذ يكون مغلق.  
- يستقبل رسائل او BPDU ولا يعيد توجيهها.

### طريقة تحديد منفذ الـ Root port في السوينتشات

يتم تحديد منفذ الـ Root port بأحد هذه الخيارات وبالترتيب :

**Lowest root cost - 1**

أقل تكلفة مسار للوصول إلى السوينتش الرئيسي

↓  
في حال التساوي

**Lowest neighbor bridge ID - 2**

أقل رقم في الـ ID bridge من الجيران (السوينتشات المتصلة به مباشرة).

↓  
في حال التساوي

**Lowest neighbor port ID - 3**

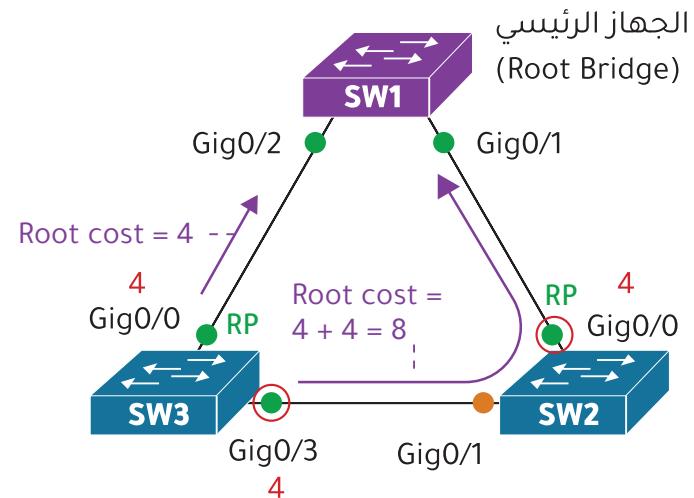
أقل رقم في منفذ الجيران ، (كل منفذ له رقم خاص به).

- طريقة حساب تكلفة المسار هي **جمع تكلفة منفذ الخروج** على هذا المسار.

فإذا وجد الجهاز ان هناك مسارين يصلان للجهاز الرئيسي Root Bridge فسيقوم بروتوكول الـ STP بإختيار المسار ذو التكلفة الأقل و يسميه تكلفة الوصول للجهاز الرئيسي (Root Cost).

**Root cost -**

هو مجموع تكلفة المسار الذي يصل للسوينتش الرئيسي



منفذ الخروج لهذا المسار محدد بالدوائر الحمراء

لكي نحدد الـ Root port في سوينتش 3 نحسب مجموع تكلفة المسار الذي يصل للسوينتش الرئيسي :

يوجد مسار من منفذ **Gig0/3** ومجموع التكلفة = 8 .

ويوجد مسار من منفذ **Gig0/0** ومجموع التكلفة = 4

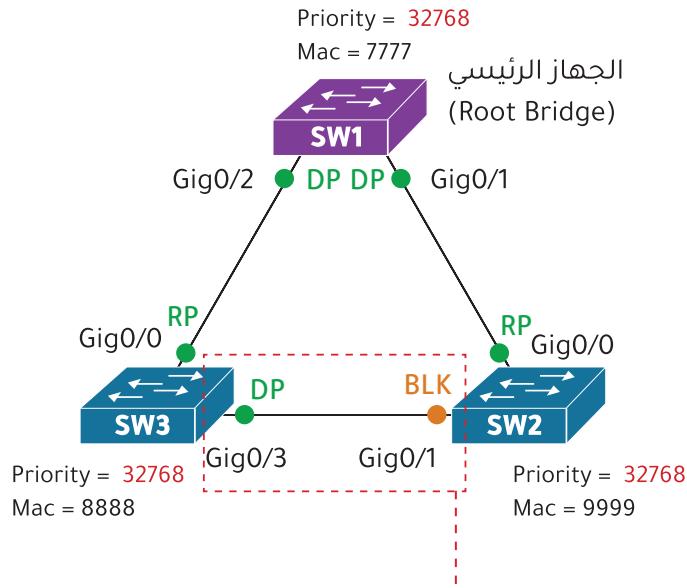
إذاً المنفذ **Gig0/0** في السوينتش 3 يعتبر (RT) لأنه أقل تكلفة ويعتبر المسار الأسرع في الوصول للسوينتش الرئيسي

### تحديد منفذ الـ Designated Port

#### Alternate Port (Block Port)

C

- لاحظ في الصورة أن منفذ السويتش الرئيسي كلها DP .



هنا يتم تحديد الـ Designated Port بأحد هذه الخيارات وبالترتيب :

Lowest root cost - 1

أقل تكلفة مسار للوصول إلى السويتش الرئيسي

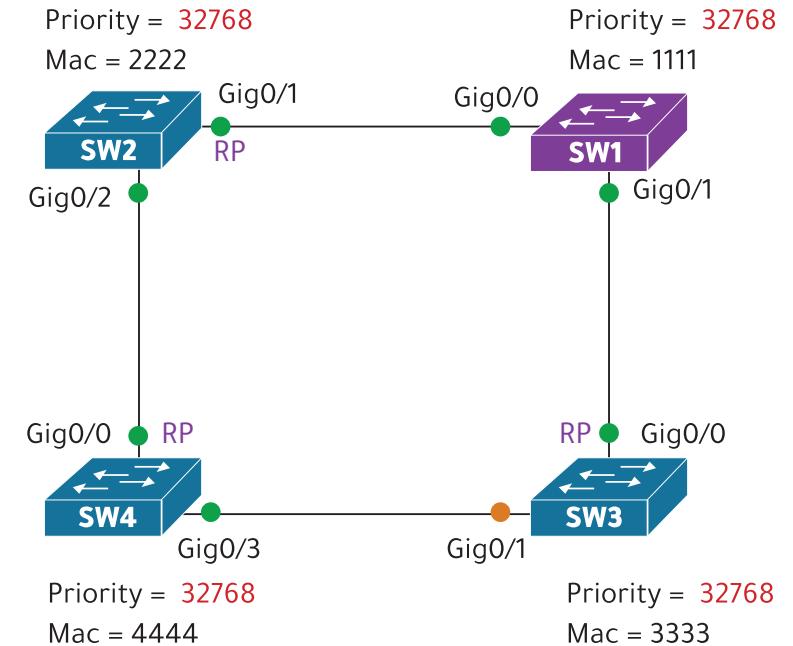
في حال التساوي

Lowest bridge ID (Switch) - 2

أقل رقم في الـ bridge ID بين السويتشين .

- التكلفة بين SW2 و SW3 متساوية

الـ bridge ID في SW3 أقل ✓



مثلا هنا في السويتش 4 :

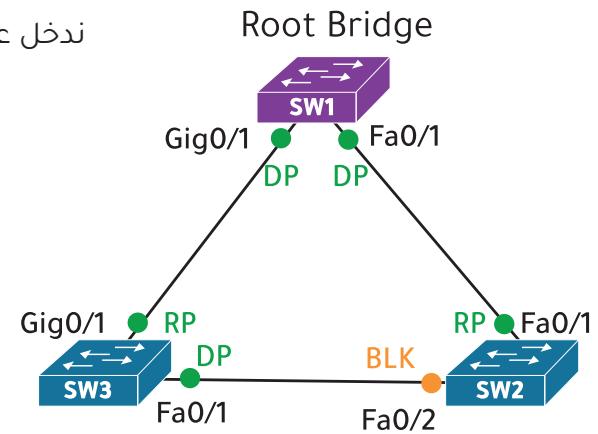
تكلفة المسار في الوصول الى السويتش الرئيسي متساوية .  
لذلك تم الاتجاه للخيار الثاني وهو أقل رقم في الـ bridge ID في السويتشات المجاورة له ( SW2 - SW3 ) .

رقم الأولوية ( Priority ) متساوي في السويتشين 2 و 3 .  
لكن رقم الماك آدرس أقل في السويتش 2 لذلك قام السويتش 4 باختيار منفذه Gig0/0 المقابل للسوitch 2 كـ Root port .

ندخل على سوتش 1 ونستعرض أوضاع المنفذ مع بروتوكول STP  
عن طريق كتابة الأمر  
`show spanning-tree`

هذا السطر يدل على أن هذا السويتش الذي انت عليه هو  
السوتش الرئيسي

SW1																													
SW1# <code>show spanning-tree</code>																													
VLAN0001																													
Spanning tree enabled protocol ieee																													
Root ID Priority 32769																													
Address 0002.17E5.DE0C																													
<b>This bridge is the root</b>																													
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec																													
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)																													
Address 0002.17E5.DE0																													
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec																													
Aging Time 20																													
<table border="1"> <thead> <tr> <th>المنفذ</th> <th>حالة المنفذ</th> <th>وضع المنفذ</th> <th>تكلفة المنفذ</th> <th>أولوية المنفذ</th> <th>نوع التوصيل</th> </tr> <tr> <th>Interface</th> <th>Role</th> <th>Sts</th> <th>Cost</th> <th>Prio.Nbr</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>Fa0/1</td> <td>Desg</td> <td>FWD</td> <td>19</td> <td>128.1</td> <td>P2p</td> </tr> <tr> <td>Gi0/1</td> <td>Desg</td> <td>FWD</td> <td>4</td> <td>128.25</td> <td>P2p</td> </tr> </tbody> </table>						المنفذ	حالة المنفذ	وضع المنفذ	تكلفة المنفذ	أولوية المنفذ	نوع التوصيل	Interface	Role	Sts	Cost	Prio.Nbr	Type	Fa0/1	Desg	FWD	19	128.1	P2p	Gi0/1	Desg	FWD	4	128.25	P2p
المنفذ	حالة المنفذ	وضع المنفذ	تكلفة المنفذ	أولوية المنفذ	نوع التوصيل																								
Interface	Role	Sts	Cost	Prio.Nbr	Type																								
Fa0/1	Desg	FWD	19	128.1	P2p																								
Gi0/1	Desg	FWD	4	128.25	P2p																								
Desg = Designated Port																													



هذا الجزء ثابت في كل سويتشات الشبكة  
لأنه يعرض بيانات السويتش الرئيسي مثل  
الماك ادرس وال Priority

هذه بيانات السويتش اللي  
انت داخل عليه الان

**Prio.Nbr**  
(Priority) : تعني أولوية المنفذ (Prio)  
وقييمته 128 افتراضية .  
(port id) : رقم المنفذ (Nbr)

ندخل على سوتش 2 ونستعرض أوضاع المنفذ  
مع بروتوكول STP عن طريق كتابة الامر  
`show spanning-tree`

هذه بيانات السوйтиش  
الرئيسي

هذه بيانات  
السوйтиش الثاني  
SW2

SW2					
SW2 # show spanning-tree					
VLAN0001					
Spanning tree enabled protocol ieee					
Root ID	Priority	32769			
	Address	0002.17E5.DE0C			
	Cost	19			
	Port	1(FastEthernet0/1)			
	Hello Time	2 sec	Max Age	20 sec	Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)					
	Address	000D.BDAE.CB39			
	Hello Time	2 sec	Max Age	20 sec	Forward Delay 15 sec
	Aging Time	20			
Interface Role Sts Cost Prio.Nbr Type					
-----	-----	-----	-----	-----	-----
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p

هذا المنفذ وضعه (RP)  
FWD

وحالته ارسال واستقبال (توجيه البيانات

هذا المنفذ وضعه (Altn)  
BLK

وحالته مغلق (BLK)

Point-to-Point (P2P)  
يعني التوصيل والربط بين الاجهزة يكون  
. (full duplex)

Shared  
يعني التوصيل والربط بين الاجهزة يكون  
. (half duplex)

.Edge  
يطلق على المنفذ الذي يتم توصيله بال (End hosts ) مثل الحاسب والطابعة وغيرها

## مراحل المنافذ في STP STP Port States

تببدأ المراحل من بداية الانتخابات وفيها تتحول المنافذ من حالة الاغلاق (Blocking) الى حالة الارسال والاستقبال (Forwarding) في 50 ثانية



## المؤقت في STP

### Spanning Tree Timers

تعني به الزمن بالثواني عند ارساله رسالة أو الانتقال من حالة إلى حالة أخرى أو الاحتفاظ بالرسالة بمدة معينة .

يفضل أن تكون على الأعدادات الافتراضية ولكن لو أردت تعديل هذه الأعدادات تدخل على السويتش وتضيف هذه الأوامر

تستطيع هنا تغيير رقم الفيلان

```
Switch(config)# spanning-tree vlan 1 hello-time 2
Switch(config)# spanning-tree vlan 1 forward-time 15
Switch(config)# spanning-tree vlan 1 max-age 20
```

تستطيع هنا تغيير الدراقام بالثواني

#### Hello time

رسالة (BPDU) يرسلها السويتش الرئيسي كل ثانيةين (2 ث) بعد انتهاء الانتخابات و استقرار السويتشات ليتأكد من المسارات والاجهزة وعدم وجود أخطاء .

- تقوم السويتشات الأخرى باعادة توجيه هذه الرسالة من منفذ ال (Designated Port) DP فقط وتحديث المعلومات مثل : (root cost - bridge ID - port ID)
- لا يتم إعادة توجيه هذه الرسالة من منفذ ال Root port و منفذ ال blocking port .
- تستطيع تغييرها من 1 - 10 ثواني.

#### Forward delay

الوقت المحدد لكل حالة استماع (Listening) وحالة تعلم (Learning) للانتقال من حالة ال blocking الى Forwarding . الافتراضي 15 ث لكل مرحلة .

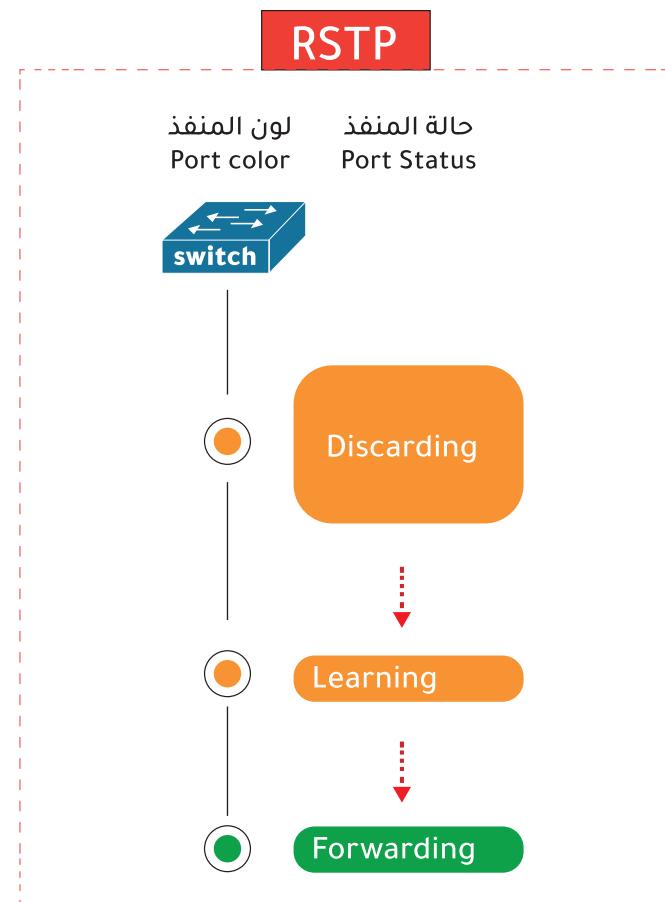
- بمعنى ان حالة الاستماع تأخذ 15 ث وحالة التعلم 15 ث

#### Max age

الوقت المحدد للاحتفاظ برسالة Hello time وهي 20 ث . فلو انتهت الـ 20 ث ولم تصل رسالة Hello time فإن السويتشات تبدأ مرحلة انتخابات جديدة لأن السويتش الرئيسي تعطل .

## (RSTP) Rapid Spanning Tree Protocol 02

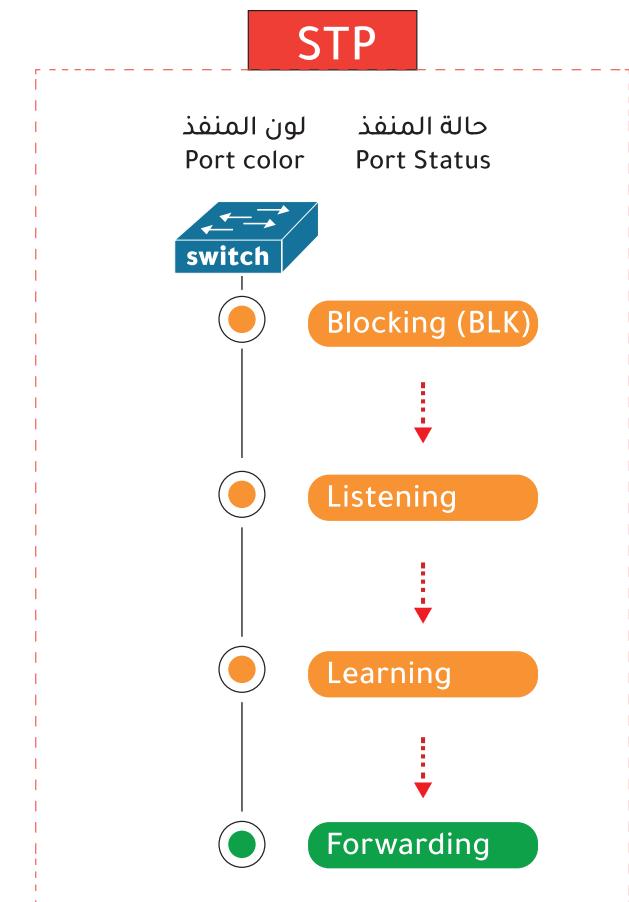
- نسخة مطورة من النسخة العاديّة STP
- مطورة بواسطة منظمة ieee
- يُعرّف بـ 802.1w
- سريع في الانتخابات
- هو بروتوكول واحد لجميع الفيلانات



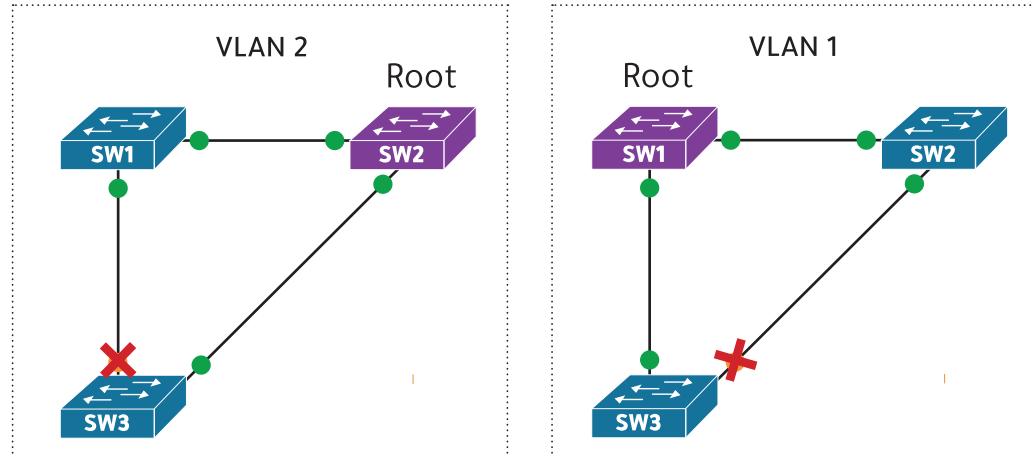
## إصدارات STP STP Versions

## (STP) Spanning Tree Protocol 01

- النسخة العاديّة لبروتوكول STP
- مطورة بواسطة منظمة ieee
- يُعرّف بـ 802.1D
- بطئ في الانتخابات
- هو بروتوكول واحد لجميع الفيلانات



الفرق في مراحل المنفذ في  
الإصدارات



نلاحظ في هذه الصورتين ان لكل فیلان بروتوكول STP خاص فيها

### (PVST+) Per-VLAN Spanning Tree Plus

◆ 03

- يعتمد على النسخة العاديـة STP
- مطورة بواسطة Cisco
- يُعرّف بـ 802.1D
- بطيء في الـ انتخـابات
- يخصـص بـ بـروتوكـول STP لـ كل فـيـلان
- هو الـ **الوضـع الافتـراضـي** على جميع سـويـتشـات Cisco

لتغيير الـ اصدـار إلى rapid-pvst+ مثلاً فيـجب عـلـيك التـغـيـير عـلـى كـل السـويـتشـات

```
Switch# show run
spanning-tree mode pvst
هذا الوضع الافتراضي
```

**تـغيـير اـصـدار البرـوـتـوكـول إـلـى rapid-pvst+**

```
Switch(config)# spanning-tree mode rapid-pvst
```

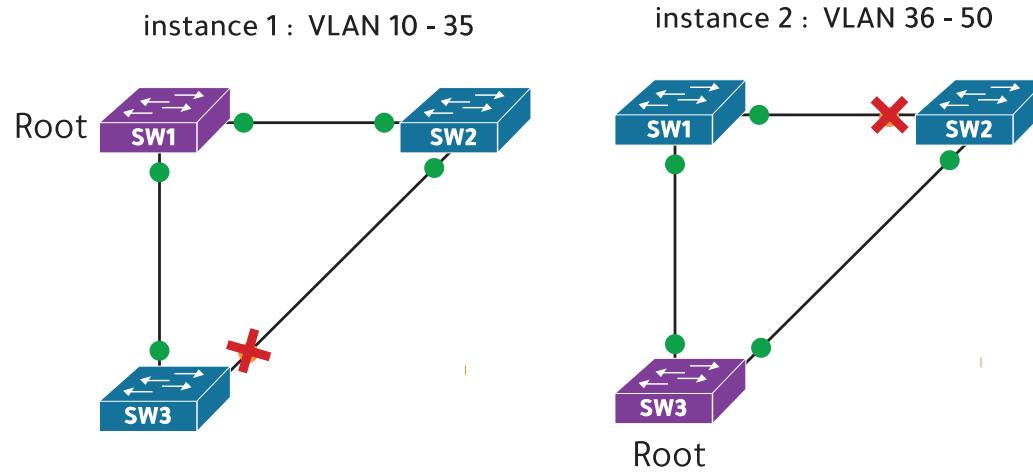
### (RPVST+) Rapid Per-VLAN Spanning Tree Plus

◆ 04

- يعتمد على النـسـخـة المـطـورـة RSTP
- مـطـورـة بواسـطة Cisco
- يـُـعرـف بـ 802.1W
- سـريع في الـ انتـخـابـات
- يـخصـص بـ بـروـتـوكـول STP لـ كل فـيـلان ( تـتم فـيه الـ انتـخـابـات وـيـكون لـه سـويـتشـ رـئـيـسي وـمـسـارـات خـاصـة )

## (MSTP) Multiple Spanning Tree Protocol

05



Cisco + ieee مطورة بواسطة

802.1S يُعرف بـ

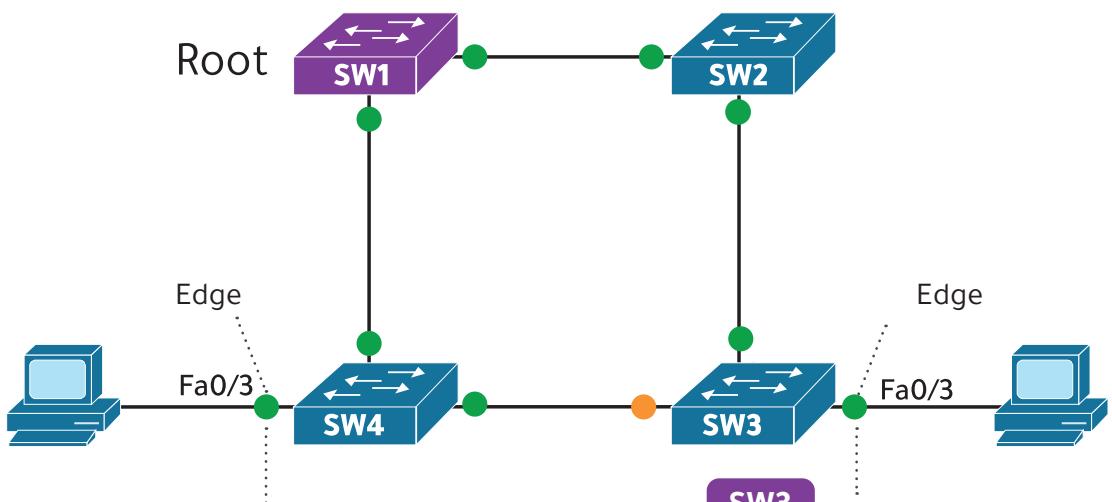
سرير في الانتخابات

يخصص بروتوكول STP لكل مجموعة فیلانات

```
Switch# show run
spanning-tree mode pvst
هذا الوضع الافتراضي

تغيير اصدار البروتوكول إلى
Switch(config)# spanning-tree mode mst
```

البروتوكول	المطور	يسمى بـ	السرعة	عدد البروتوكولات
STP	ieee	802.1D	بطيء	بروتوكول واحد لكل الفيلانات
PVST +	cisco	802.1D	بطيء	بروتوكول لكل فيلان
RSTP	ieee	802.1w	سرير	بروتوكول واحد لكل الفيلانات
Rapid PVST+	cisco	802.1w	سرير	بروتوكول لكل فيلان
MSTP	ieee + cisco	802.1s	سرير	بروتوكول لكل مجموعة فیلانات ( قروب )



### Port Fast + BPDU Guard

#### Port Fast

خاصية مميزة تساعد على تسريع بروتوكول STP في المنفذ التي ترتبط بالـ (end hosts) مثل أجهزة الحاسب والطابعات و تسمى هذه المنفذ بالـ Edge .

- عند تفعيل الـ Port Fast في المنفذ فإن المنفذ يتتحول مباشرةً من حالة الإغلاق (Blocking) إلى حالة التوجيه (Forwarding) (إرسال + استقبال) عند ربطه بجهاز حاسب.

- يمنع توصيل السويتش باي منفذ مفعل عليه الـ Port Fast لانه سوف يسبب دوران للبيانات في الشبكة، لذلك يجب تفعيل الـ BPDU Guard .

#### ما هو الـ BPDU Guard

هو حماية المنفذ من توصيل اي سويتش عليه .

- اذا تم تفعيل الـ BPDU Guard على منفذ فإنه سوف يقفل هذا المنفذ مباشرةً اذا تم توصيل السويتش عليه .

- يعني بمجرد استقبال منفذ السويتش رسالة الـ BPDU فإنه سيتم قفل المنفذ مباشرةً ، لأن هذه الرسالة يرسلها السويتش فقط.

```
SW3(config)# interface fa0/3
SW3(config-if)# switchport mode access
SW3(config-if)# spanning-tree portfast
SW3(config-if)# spanning-tree bpduguard enable
SW3(config-if)# end
SW3# wr
```

SW4

```
SW4(config)# interface fa0/3
SW4(config-if)# switchport mode access
SW4(config-if)# spanning-tree portfast
SW4(config-if)# spanning-tree bpduguard enable
SW4(config-if)# end
SW4# wr
```

نستطيع الدخول على عدة منافذ لتطبيق أمر range عليها بالإضافة كلمة range

```

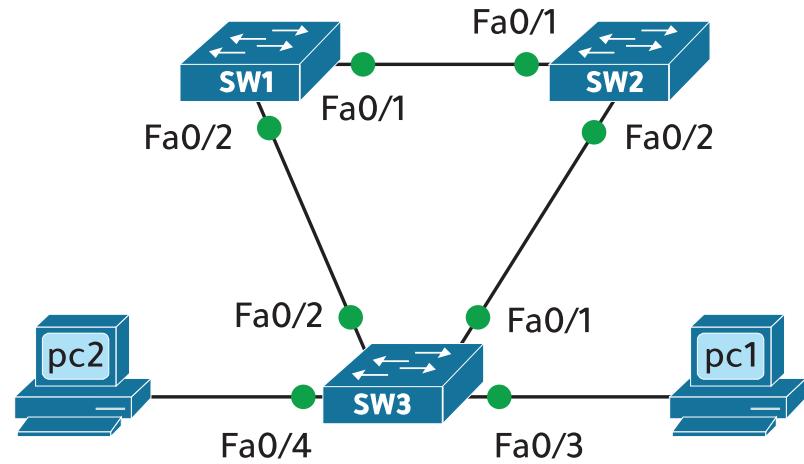
SW1> enable
SW1# conf t
SW1(config)#interface range fa0/1-2
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)#exit
1

إنشاء الفيلنات
2
SW1(config)# vlan 10
SW1(config-vlan)# vlan 20
SW1(config-vlan)# vlan 30
SW1(config-vlan)# vlan 40
SW1(config-vlan)# vlan 50
SW1(config-vlan)# exit

rapid pvst
3
SW1(config)# spanning-tree mode rapid-pvst
4

تخصيص السويتش الاول كرئيسي للفيلنات 10 و 20 و 30
SW1(config)# spanning-tree vlan 10,20,30 root primary

```



1 - جيمع الوصلات بين السويتشات تكون في وضع Trunk .  
2 - انشئ الفيلنات التالية 50 40 30 20 10 على جميع السويتشات.

3 - غير وضع الاصدار الى rapid pvst لكل السويتشات  
4 - اجعل السويتش الرئيسي رقم 1 للفيلنات 10 و 20 و 30 .  
5 - اجعل السويتش الرئيسي رقم 2 للفيلنات 40 و 50 .  
6 - فقل الـ BPDU Guard و الـ Port Fast على منفذ السويتش 3 المتصلة

باجهزة الحاسب

**SW3**

```

SW3> enable
SW3# conf t
SW3(config)#interface range fa0/1-2
SW3(config-if-range)# switchport mode trunk
SW3(config-if-range)#exit

إنشاء الفيلنات
SW3(config)# vlan 10
SW3(config-vlan)# vlan 20
SW3(config-vlan)# vlan 30
SW3(config-vlan)# vlan 40
SW3(config-vlan)# vlan 50
SW3(config-vlan)# exit

تغيير وضع الاصدار الى rapid pvst
SW3(config)# spanning-tree mode rapid-pvst

BPDU Guard على Port Fast
SW3(config)# interface range fa0/3-4
SW3(config-if)# switchport mode access
SW3(config-if)# spanning-tree portfast
SW3(config-if)# spanning-tree bpduguard enable

```

**SW2**

```

SW2> enable
SW2# conf t
SW2(config)# interface range fa0/1-2
SW2(config-if-range)# switchport mode trunk
SW2(config-if-range)#exit

إنشاء الفيلنات
SW2(config)# vlan 10
SW2(config-vlan)# vlan 20
SW2(config-vlan)# vlan 30
SW2(config-vlan)# vlan 40
SW2(config-vlan)# vlan 50
SW2(config-vlan)# exit

تغيير وضع الاصدار الى rapid pvst
SW2(config)# spanning-tree mode rapid-pvst

تخصيص السويفت كرئيسي للفيلنات 40 و 50
SW2(config)# spanning-tree vlan 40,50 root primary

```

## استكشاف الأخطاء وإصلاحها

### Troubleshooting (VLAN - STP-VTP)

هذه بعض الاوامر المخصصة تستكشف فيها عن التفاصيل  
للفيالنات والبروتوكولات

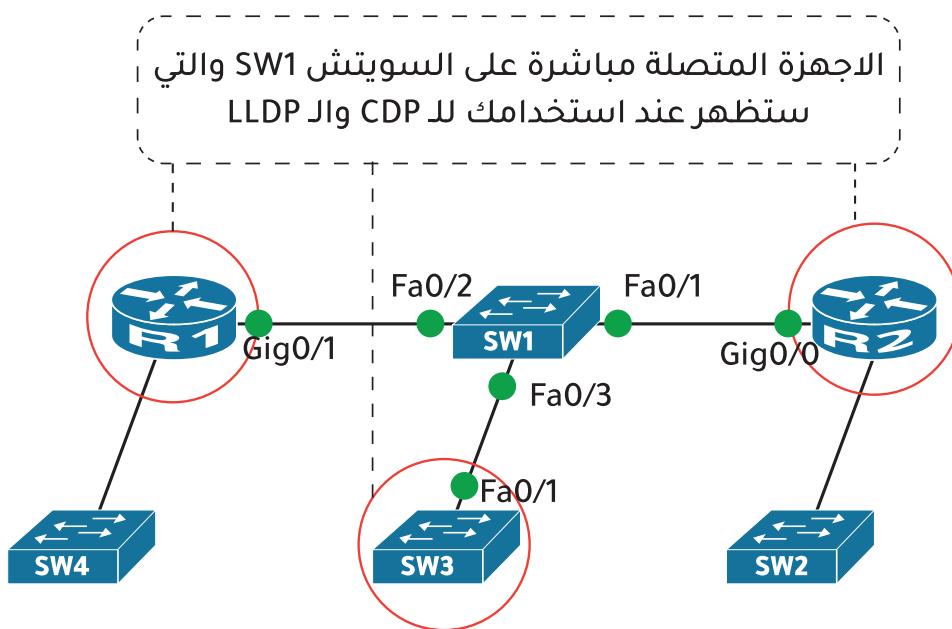
vlan + vtp	كتابة مختصرة
show vlan brief	sh vl b
show interfaces status	sh int st
show interfaces switchport	sh int sw
show interface trunk	sh int tr
show vtp status	sh vtp st
show vtp password	sh vtp pass

spanning-tree	كتابة مختصرة
show spanning-tree	sh sp
show spanning-tree detail	sh sp d
show spanning-tree summary	sh sp s
show spanning-tree interface fa0/1	sh sp int fa0/1
show spanning-tree active	sh sp a

## ≡ بروتوكول CDP وبروتوكول LLDP

- 6 - امكانية تفعيل ارسال فقط (Receive) أو استقبال (Transmit) فقط على منفذ او على الجهاز .
- 7 - يفضل تطبيق هذا البروتوكول لانه قد تحتاج في شبكتك أجهزة من شركات مختلفة وهذا البروتوكول يدعمها جميعا .
- يتم إرسال رسائل الـ LLDP بشكل دوري إلى عنوان MAC متعدد الإرسال multicast MAC address وهو ( 0180.C200.000E )

- بروتوكولات يتم استخدامها لجمع واستكشاف معلومات الأجهزة المجاورة للسويتشر .
- بروتوكولات تعمل في الطبقة الثانية Layer 2 .
- هذه البروتوكولات لا تستخدم عناوين الـ IP في الاكتشاف .
- تبادل المعلومات المشتركة مثل (اسم الجهاز - عنوان الـ IP - وضع الجهاز .... الخ )
- لها فائدة كبيرة تساعد المهندسين باستكشاف الأجهزة المجاورة وبياناتها عند عدم وجود دليل تعليمات للشبكة .

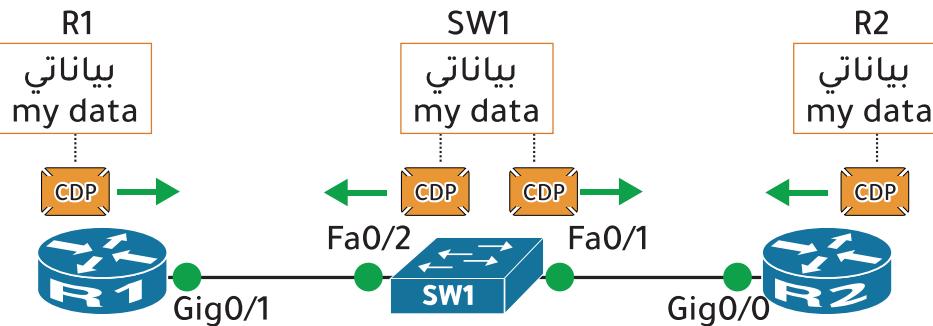


### : CDP ≡

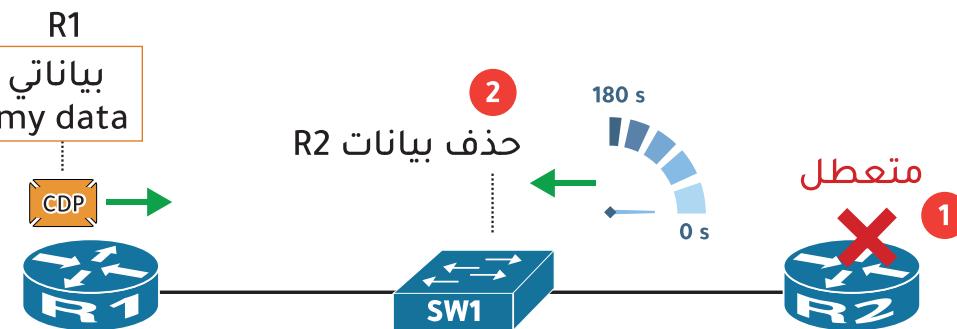
- هو اختصار Cisco Discovery Protocol
- 1- خاص بأجهزة سيسكو فقط .
- 2- يرسل رسالة CDP packets كل 60 ثانية .
- 3- قيمة الـ hold time تساوي 180 ثانية .
- 4- مفعل تلقائيا على أجهزة سيسكو .
- 5- يتم إرسال رسائل الـ CDP بشكل دوري إلى عنوان MAC متعدد الإرسال Multicast MAC Address ( 0100.0CCC.CCCC ) وهو

### : LLDP ≡

- هو اختصار Link Layer Discovery Protocol
- 1- أصدرته منظمة IEEE ويسمى 802.1AB .
- 2- مفتوح للكل يدعم جميع أجهزة الشركات .
- 3- يرسل رسالة (LLDP packets) كل 30 ثانية .
- 4- قيمة الـ hold time تساوي 120 ثانية .
- 5- غير مفعل على الأجهزة ، لابد من تفعيله على كل جهاز .

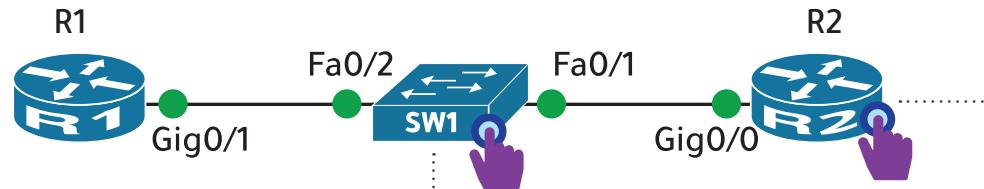


**packets -**  
كل جهاز يرسل رسالة أو حزمة CDP فيها بياناته للجهازة المتصلة  
بها مباشرة  
اذا كان البروتوكول CDP فانه يرسل كل 60 ثانية .  
اذا كان البروتوكول LLDP فانه يرسل كل 30 ثانية .



**hold time -**  
المدة الزمنية التي ينتظراها الجهاز بدون ما يستقبل رسالة أو حزمة  
CDP packets أو LLDP packets  
اذا الجهاز المجاور والمتصل بالسويفت او الراوتر لم يرسل رسالة  
أو LLDP فانه يتم حذف بياناته لانه يعتبر جهاز متعطل .

اذا كان البروتوكول CDP فـان المدة 180 ثانية .  
اذا كان البروتوكول LLDP فـان المدة كل 120 ثانية .



### SW1

SW1# show cdp neighbors

Capability Codes: R - Router , T - Trans Bridge, B - Source Route Bridge

S - Switch , H - Host, I - IGMP, r - Repeater, P - Phone

اسم جهاز الجار	المنفذ المحلي	مدة الانتظار	نوع الجهاز	موديل الجهاز	منفذ جهاز الجار
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R2	Fa 0/1	160	R	ISR4300	Gig 0/0
R1	Fa 0/2	160	R	ISR4300	Gig 0/1

### R2

R2# show cdp neighbors

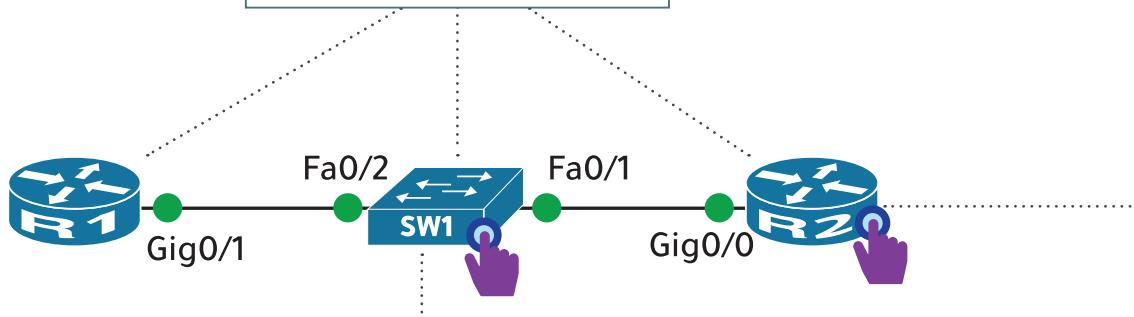
Capability Codes: R - Router , T - Trans Bridge, B - Source Route Bridge

S - Switch , H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
SW1	Gig 0/0	152	S	2960	Fa 0/1

تفعيل البروتوكول  
على كل جهاز

```
switch(config)# lldp run
```



## LLDP ≡

تحتاج تفعيل بروتوكول LLDP على كل جهاز لكي يتم استعراض بيانات الأجهزة المتصلة على نفس السويفتش او الراوتر .

أمر التفعيل :

```
switch(config)# lldp run
```

```
SW1# show lldp neighbors
```

Capability codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

اسم جهاز الجار	المنفذ المحلي	مدة الانتظار	نوع الجهاز	منفذ جهاز الجار
Device ID	Local Intrfce	Hold-time	Capability	Port ID
R2	Fa 0/1	140	R	Gig 0/0
R1	Fa 0/2	140	R	Gig 0/1

```
R2# show lldp neighbors
```

Capability codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID	Local Intrfce	Hold-time	Capability	Port ID
SW1	Gig 0/0	110	B	Fa 0/1

: يقصد بها السويفتش

## استكشاف الأخطاء وإصلاحها

### Troubleshooting (CDP - LLDP)

أوامر أعدادات cdp CDP Configuration	وظيفتها
(config)# cdp run	تفعيل البروتوكول بشكل عام على الجهاز
(config)# no cdp run	الغاء تفعيل البروتوكول
(config-if)# cdp enable	تفعيل البروتوكول على منفذ محدد
(config-if)# no cdp enable	الغاء تفعيل البروتوكول من على المنفذ
(config)# cdp timer <seconds>	تحديد وقت ارسال رسالة cdp ، الافتراضي 60 ثانية
(config)# cdp holdtime <seconds>	تحدد المهلة الزمنية التي يجب أن يحتفظ بها جهاز الاستقبال بالمعلومات قبل التخلص منها. الافتراضي 180 ثانية

CDP	وظيفتها
clear cdp table	هذا الامر لمسح الجدول المخزن
show cdp neighbors	استعراض الاجهزه المتصلة بي مباشرة
show cdp entry [ device name ]	استعراض التفاصيل باسم الجهاز
show cdp interface [type number]	استعراض تفاصيل منفذ محدد
show show cdp neighbors detail	استعراض جميع تفاصيل الاجهزه المتصلة بي مباشرة

## استكشاف الأخطاء وإصلاحها

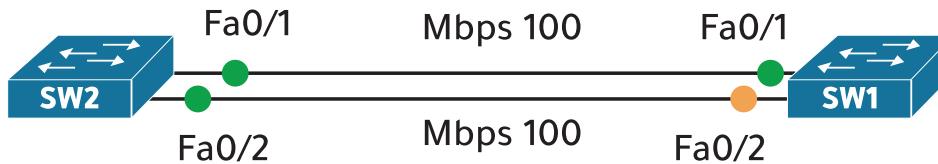
### Troubleshooting (CDP - LLDP)

أوامر أعدادات LLDP LLDP Configuration	وظيفتها
(config)# lldp run	تفعيل البروتوكول بشكل عام على الجهاز
(config)# no lldp run	الغاء تفعيل البروتوكول
(config-if)# lldp transmit	تفعيل ارسال رسالة lldp من الداخل على منفذ محدد
(config-if)#no lldp transmit	الغاء تفعيل ارسال رسالة lldp من الداخل على منفذ محدد
(config-if)# lldp receive	تفعيل استقبال رسالة lldp من الخارج على منفذ محدد
(config-if)#no lldp receive	الغاء تفعيل استقبال رسالة lldp من الخارج على منفذ محدد
(config)# lldp timer <seconds>	تحديد وقت ارسال رسالة lldp الافتراضي 30 ثانية
(config)# lldp holdtime <seconds>	تحدد المهلة الزمنية التي يجب أن يحتفظ بها جهاز الاستقبال بالمعلومات قبل التخلص منها. الافتراضي 120 ثانية
(config)# lldp reinit <seconds>	مدة وقت الانتظار بعد الغاء الـ LLDP على منفذ حتى العودة الى تفعيله مرة اخرى على نفس المنفذ

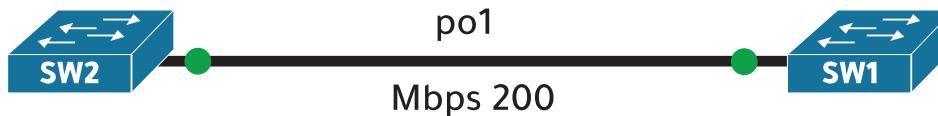
LLDP	وظيفتها
clear lldp table	هذا الامر لمسح الجدول المخزن
show lldp neighbors	استعراض الاجهزه المتصلة بي مباشرة
show show lldp neighbors detail	استعراض جميع تفاصيل الاجهزه المتصلة بي مباشرة

**ملاحظة :**

- عند دمج المنفذين يطلق عليهم **Port-Channel** وتجدها مختصرة بـ **po**.
- بعد دمج المنفذين فإن بروتوكول الـ **STP** يعتبره منفذًا واحدًا، لانه قبل الدمج سوف يغلق بروتوكول الـ **STP** احد المنافذ ليمنع دوران البيانات بين الاجهزه.



**بعد دمج الوصلتين**



## Ether-Channel وبروتوكولات الـ PAgP و LACP

هي عبارة عن تقنية يتم فيه دمج أكثر من منفذ موجود على نفس جهاز السويفت ليتم العمل وكأنهم منفذ واحد بسرعة عالية جداً.

نستفيد من دمج المنافذ :

- سعة اكبر في نقل البيانات
- سرعة عالية في النقل .

- يتم تطبيق هذه البروتوكولات على أجهزة الطبقة الثانية Layer2 مثل السويفت وأجهزة الطبقة الثالثة Layer3 مثل الراوتر وسويفت L3.

**شروط تكوين وإعداد الـ Ether-Channel**

**يجب أن تكون جميع المنافذ في الجهازين متساوية في :**

- 1 - سرعة نقل البيانات (كلهم 100 Mbps أو كلهم 1 Gig).
- 2 - جميع الوصلات **full duplex**.
- 3 - حالة المنفذ وهي **Trunk**.
- 4 - الـ **Native VLAN**.
- 5 - السماح لممرور الفيلنات (allowed VLAN).

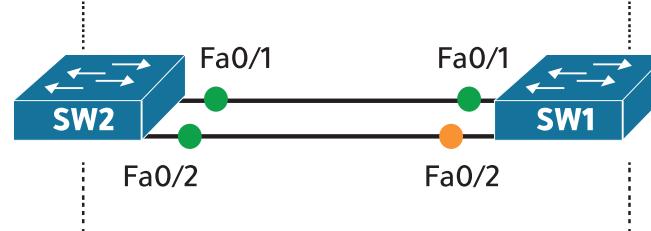
## LACP ≡

### طريقة تهيئة وتنفيذ بروتوكول LACP

الدخول على منفذ هذا الجهاز

3

وإنشاء Port-Channel



الدخول على منفذ هذا الجهاز

1

وإنشاء Port-Channel

هو اختصار ل Link Aggregation Control Protocol وهو بروتوكول خاص بمنظمة IEEE يعمل مع جميع أجهزة الشركات وأيضاً مع أجهزة سيسكو و تم تعريفه بـ 802.3AD .

- يُفضل تطبيق هذا البروتوكول لأنّه قد تحتاج في شبكتك أجهزة من شركات مختلفة وهذا البروتوكول يدعمها جميعاً .

- يمكن دمج من 2 - 8 وصلات في الجهاز الواحد .

الحالات التي يتم تهيئة وتكوين بروتوكول LACP :

**Active - 1**

في هذه الحالة يبدأ هذا الجهاز بالمبادرة ومفاوضة الجهاز الآخر بالتحول إلى Ether-Channel .

**Passive - 2**

في هذه الحالة سيصبح المنفذ جزءاً من EtherChannel في حالة طلب البوت المقابل فقط ، بمعنى انه في حالة استماع وانتظار لاي طلب .

		SW2	SW2
LACP		Active	Passive
SW1	Active	Yes	Yes
	Passive	Yes	No

جدول يقارن لك نجاح ا JL Ether-Channel

## طريقة تهيئة وتنفيذ بروتوكول PAgP

- 1 الدخول على منفذ هذا الجهاز
- 2 جعل هذا الجهاز هو الاول في بداية المفاوضات باعطائه الحالة **Desirable**
- 3 وانشاء Port-Channel
- 4 اعطاء هذا الجهاز الحالة **Auto** لكي يتسمع للمفاوضات ويقبلها



- 1 الدخول على منفذ هذا الجهاز

وانشاء Port-Channel

- 2 جعل هذا الجهاز هو الاول في بداية المفاوضات باعطائه الحالة **Desirable**

المفاوضات باعطائه الحالة **Desirable**

		SW2	SW2	
		PAgP	Desirable	Auto
SW1	Desirable	Yes	Yes	
	Auto	Yes		No

جدول يقارن لك نجاح الـ Ether-Channel

## بروتوكول PAgP ≡

هو اختصار لـ Port Aggregation Protocol وهو بروتوكول خاص بأجهزة سيسكو فقط ، ولن يعمل على اي اجهزة من شركات اخرى .

الحالات التي يتم تهيئة وتكوين بروتوكول PAgP :

### Desirable - 1

في هذه الحالة يبدأ هذا الجهاز بالمبادرة ومفاوضة الجهاز الآخر بالتحول إلى Ether-Channel

### Auto - 2

في هذه الحالة سيصبح المنفذ جزءاً من EtherChannel في حالة طلب البورت المقابل فقط ، بمعنى انه في حالة استماع وانتظار لا يطلب .



**SW2**

الدخول على المنفذ بإضافة الامر  
SW2(config)# int range fa0/1-2

إدخال امر دمج المنفذ ووضعه في حالة passive  
SW2(config-if-range)# channel-group 1 mode passive  
SW2(config-if-range)#{

Creating a port-channel interface Port-channel 1  
SW2(config-if-range)#end  
SW2#

رسالة تظهر لك بانشاء منفذ اسمه 1  
الخاص بالدمج وتجده مختصر بـ po1

SW2(config)# interface po1

**SW1**

الدخول على المنفذ بإضافة الامر  
SW1(config)# int range fa0/1-2

إدخال امر دمج المنفذ ووضعه في حالة active  
SW1(config-if-range)# channel-group 1 mode active  
SW1(config-if-range)#{

Creating a port-channel interface Port-channel 1  
SW1(config-if-range)#end  
SW1#

رسالة تظهر لك بانشاء منفذ اسمه 1  
الخاص بالدمج وتجده مختصر بـ po1

هنا ضع رقم  
من اختيارك  
واخترنا هنا رقم  
1

#### ملاحظة :

1 - اي اوامر تريد تنفيذها ستكون على المنفذ po1 لانه المنفذين fa0/1 و fa0/2 أصبحا مدمجين .

ف عند الدخول على المنفذ لتنفيذ الاوامر نكتب :

SW1(config)# interface po1

## نستعرض معلومات ا JL Ether-Channel

```
SW1# show etherchannel summary
```

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

رقم	المنفذ التي تم دمجها	بروتوكول المدحوم	رقم المنفذ
القرب	المستخدم	المدمج	البروتوكول

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

-----+-----+-----+			
1	Po1(SU)	LACP	Fa0/1(P) Fa0/2(P)
.....			

S : تعني أن الأجهزة التي تعمل من الطبقة الثانية

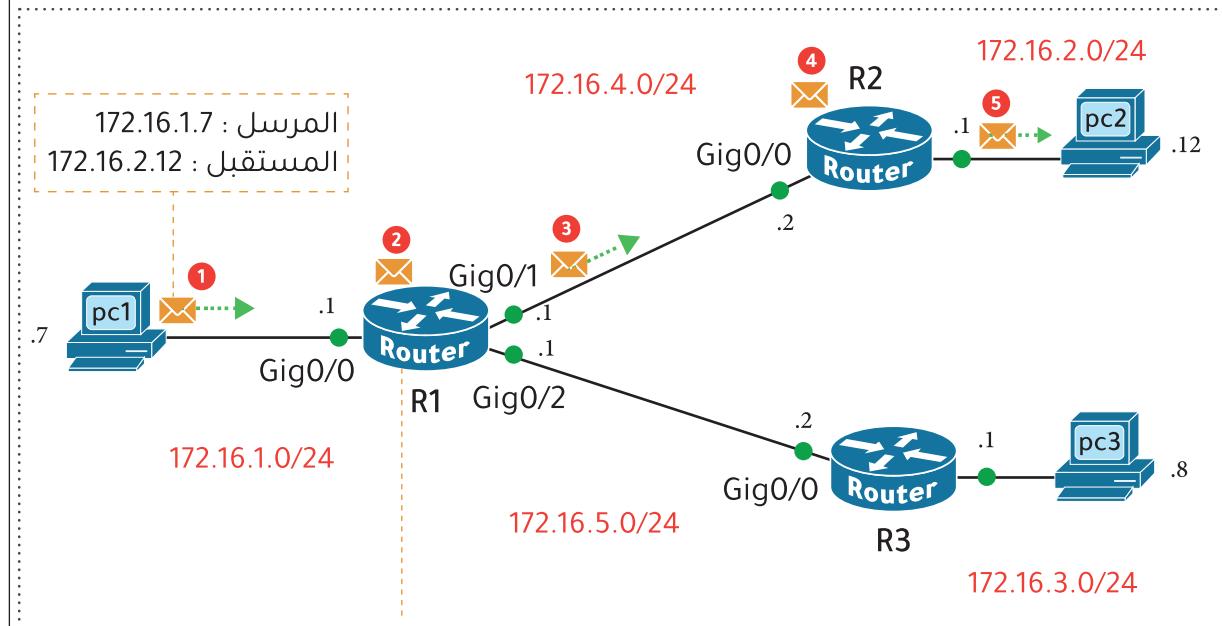
U : تعني أن المنفذ يعمل الان P : تعني أن المنفذين مندمجين مع بعض في ا JL (po1)

```
SW1# show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Po1		connected	1	auto	auto	
Fa0/1		connected	1	auto	auto	10/100BaseTX
Fa0/2		connected	1	auto	auto	10/100BaseTX

لاحظ هنا وجود المنفذ الجديد والذي تم دمج المنفذين fa0/1 - fa0/2 و سيكون عملك واعداداته على هذا المنفذ po1

## جهاز الراوتر والتوجيه Router And Routing



- فحص الرسالة للتأكد من عدم وجود أخطاء
- البحث في جدول التوجيه عن ايبي المستقبل
- توجيه البيانات للجهة المستقبلة

الشبكة	Mask	إلى الراوتر التالي	المنفذ الخارج من R1
172.16.1.0	/24		
172.16.2.12	→ 172.16.2.0	/24 → 172.16.4.2 (R2)	Gig0/1 →
172.16.3.0	/24	172.16.5.2 (R3)	Gig0/2
172.16.4.0	/24		
172.16.5.0	/24		

شرح مرور الحزمة داخل جدول التوجيه Routing Table

الراوتر هو الجهاز المسؤول عن ادارة وربط الشبكات المختلفة بعضها ببعض.

- الراواتر يعمل في الطبقة الثالثة Layer 3 .

### وظائف الراوتر:

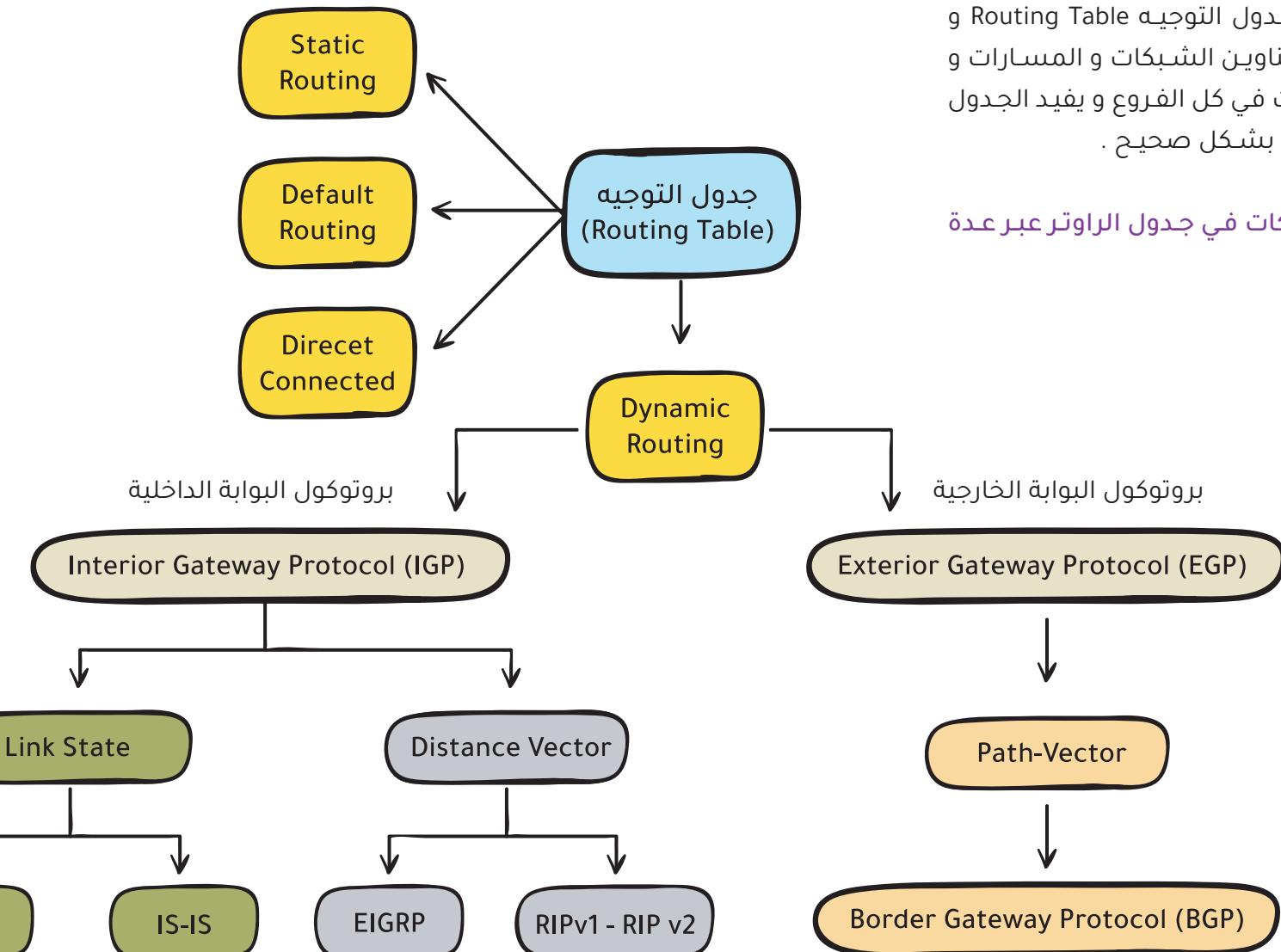
- 1 - تحديد أفضل مسار للوجهه باستخدام جدول التوجيه (Routing Table) .
- 2 - توجيه البيانات (forwarding traffic) الى الوجهه المطلوبه وذلك بعد تحديد المسار .

### التوجيه : Routing

هو العملية التي تستخدمها أجهزة التوجية (الراوتر) لتحديد المسار الذي يجب ان تتخذه حزمة الـ ip عبر الشبكة للوصول الى وجهتها .

- تقوم أجهزة التوجية بتخزين المسارات إلى جميع وجهاتها في جدول التوجيه . Routing Table

## بناء جدول التوجيه



شبكات بعيدة عن R1

R1  
Router

R2  
Router



R3  
Router



## Static Routing

تعني اتصال وربط الشبكات بعضها البعض عن طريق اوامر وإعدادات يدوية يقوم بها مهندس الشبكة.

- في هذه الحالة يتم إنشاء جدول التوجيه بشكل يدوي .

- عندما نريد إضافة شبكات بعيدة (remote networks)

فيجب علينا اضافتها بشكل يدوي ، ويكون رمزها في جدول التوجيه بحرف S اختصار ل (Static).

الشبكات المتصلة مباشرة بالراوتر 2  
Directly connected networks in R2

الشبكات المتصلة مباشرة بالراوتر 1  
Directly connected networks in R1

## Direct Connected

هي الشبكات المتصلة بالراوتر مباشرة .

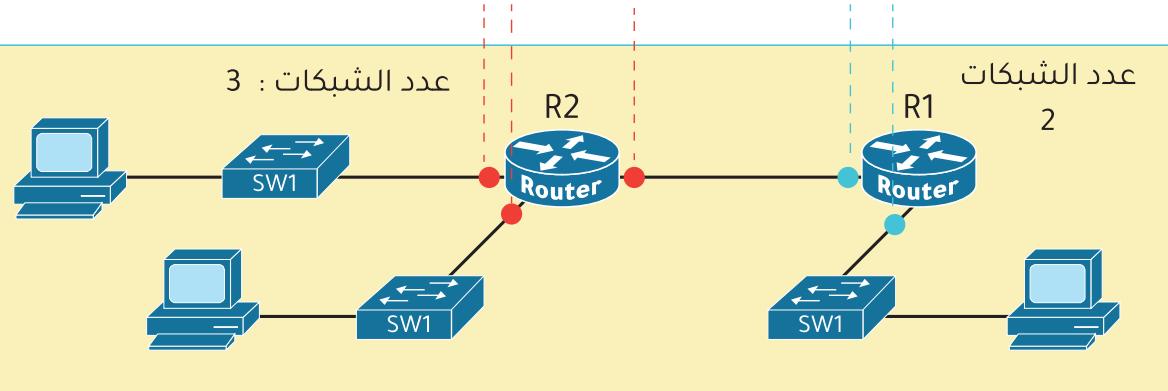
- بعد إضافة الشبكات (الايبي ip + قناع الشبكة subnetmask ) الى منافذ الراوتر فإن الراوتر وبشكل تلقائي يسجل الشبكات المتصلة به مباشرة في جدول التوجيه بدون استخدام اي بروتوكولات ربط .

ويرمز لها في جدول التوجيه Routing Table بالحرف C اختصارا ل Connected

عدد الشبكات : 3

عدد الشبكات

2



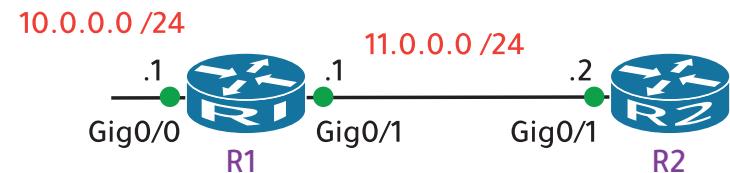
• **C - connected :** يرمز له بحرف **C** وتعني المسارات الى هذه الشبكة التي تتصل بهذا المنفذ.

يعني اذا وصلت حزمة IP عنوانها موجود في مدي هذه الشبكة فإن الراوتر يعيد توجيهها الى هذه الشبكة عبر المنفذ المتصل بها.

• **local :** يرمز له بحرف **L** يعني توجيه مسار الحزمة إلى عنوان الـ IP الذي تم اضافته الى منفذ الراوتر.

وتم تحديده بـ قناع شبكة (subnet mask) /32 لأن هذا العنوان هو عنوان المنفذ واي حزمة تصل للراوتر فانه يرسلها لهذا المنفذ.

مثال لدينا هذه الشبكة البسيطة الراوتر الاول R1 :



يعني اذا وصلت حزمة IP عنوانها موجود في شبكة الـ 10.0.0.0 / 24 فإن الراوتر يعيد توجيهها الى هذه الشبكة عبر المنفذ المتصل بها

**GigabitEthernet0/0** وهو مباشرة وهو

يعني اذا وصلت حزمة IP عنوانها محدد بـ 10.0.0.1 / 24 فإن الراوتر يرسلها الى هذا المنفذ وهو عنوان **GigabitEthernet0/0** منفذ الـ

```

R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,
      M - mobile, B - BGP, D - EIGRP, EX - EIGRP external,
      O - OSPF, IA - OSPF inter area
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  10.0.0.0/24 is directly connected, GigabitEthernet0/0
L  10.0.0.1/32 is directly connected, GigabitEthernet0/0
11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  11.0.0.0/24 is directly connected, GigabitEthernet0/1
L  11.0.0.1/32 is directly connected, GigabitEthernet0/1
  
```

بعد إضافة عنوان أبيي لأي منفذ في الراوتر فإن الراوتر وبشكل تلقائي ينشئ له مسارات في جدول التوجيه Routing Table

- مسار الى الشبكة a connected route

- مسار الى المنفذ a local route

## Default Routing

المسار الافتراضي هو المسار الذي يتم استخدامه في حالة عدم وجود مسار معروف لعنوان IP في جدول التوجيه.

- إذا لم يتم اعداد هذا المسار فسوف يتغافل الراوتر جميع الرسائل التي تحتوي على عناوين وجهة غير موجودة في جدول التوجيه الخاص به.

- يكون رمز المسار الافتراضي في جدول التوجيه بحرف \* .

- يكون المسار الافتراضي الى هذا العنوان 0.0.0.0 /0

- غالباً ما يتم استخدام المسار الافتراضي لتوجيه البيانات الى الانترنت .

لاحظ تعامل الراوتر مع الايبي في الحالات الثلاثة

لا يوجد مسار أو توجيه.  
لا يوجد مسار افتراضي.  
سيتم تجاهل هذه الرسالة

1

40.0.0.1 /8



الشبكة	المنفذ
10.0.0.0 / 8	Gig0/1
20.0.0.0 / 8	Gig0/2
30.0.0.0 / 8	Gig0/3

الشبكة موجودة في جدول التوجيه  
عبر المنفذ Gig0/2 . سيتم توجيه  
الباكت عبر هذا المنفذ

2

172.170.0.1 /16



الشبكة	المنفذ
10.0.0.0 / 8	Gig0/0
20.0.0.0 / 8	Gig0/1
172.170.0.0 /16	Gig0/2
0.0.0.0/0	Fa0/0

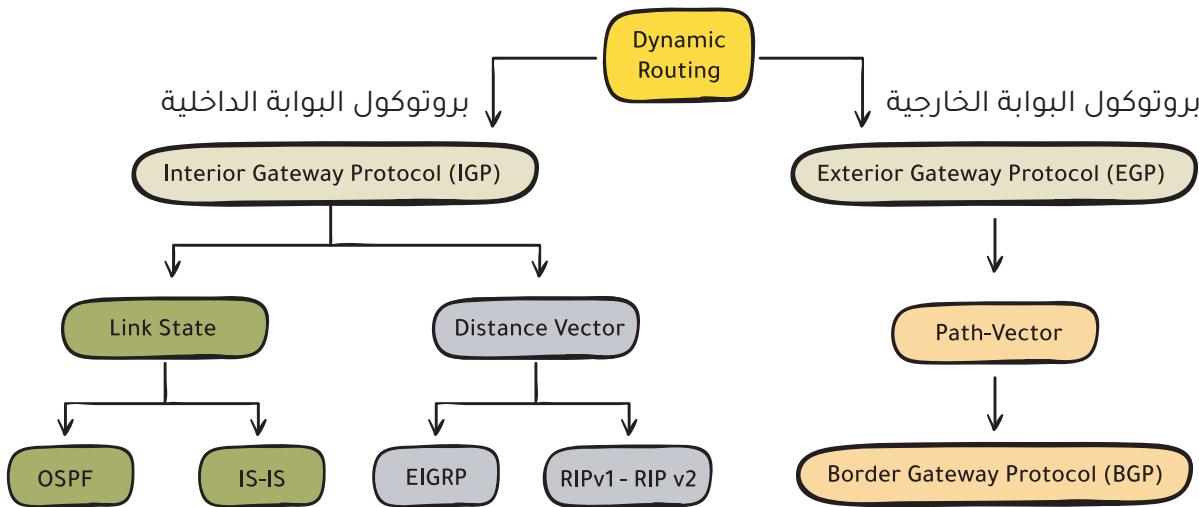
لا يوجد مسار أو توجيه.  
سيتم استخدام التوجيه  
الافتراضي لتوجيه هذا الباكت

3

192.168.5.1 /24



الشبكة	المنفذ
192.168.0.0 /24	Gig0/1
192.168.2.0 /24	Gig0/2
192.168.3.0 /24	Gig0/3
0.0.0.0/0	Fa0/1



### أنواع بروتوكولات التوجيه динاميки ( Dynamic Routing )

#### 1 - بروتوكول البوابة الداخلية (IGP)

هو بروتوكول يستخدم لمشاركة المسارات داخل نظام مستقل (autonomous system (AS)) واحد مثل بروتوكول OSPF و بروتوكول IS-IS.

#### 2 - بروتوكول البوابة الخارجية (EGP)

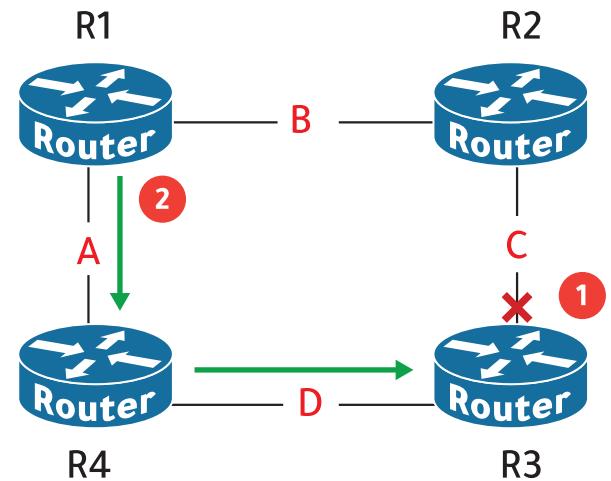
هو بروتوكول يستخدم لمشاركة المسارات بين الأنظمة المستقلة المختلفة مثل بروتوكول BGP .

## Dynamic Routing

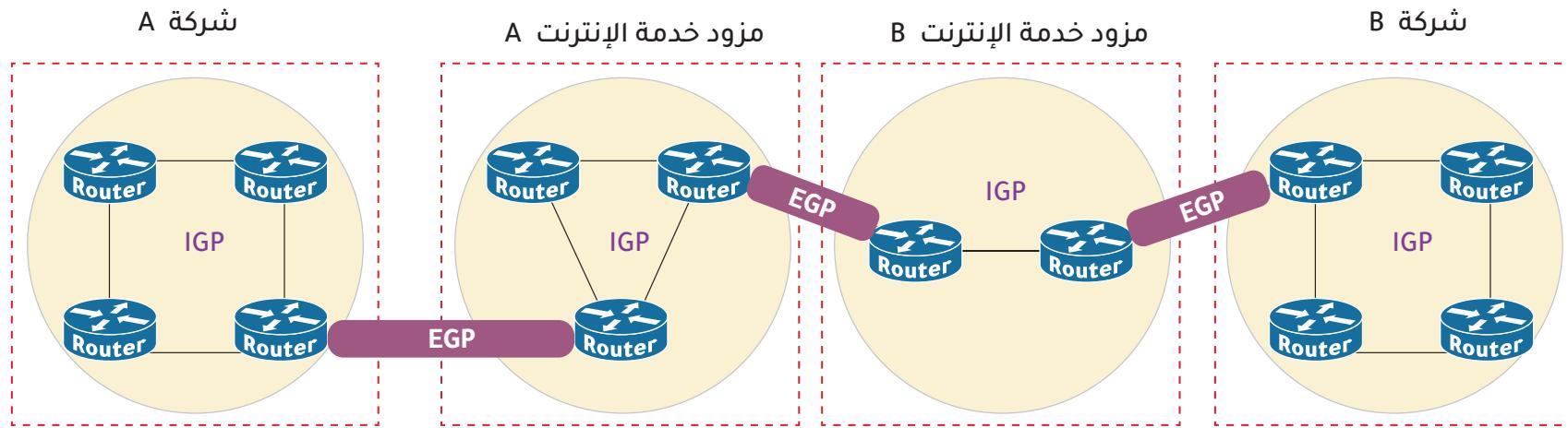
التوجيه динамики هو آلية يتم من خلالها تبادل معلومات التوجيه بين أجهزة الراوتر لربط الشبكات و تحديد أفضل مسار بين أجهزة الشبكة للوصول إلى الوجهه .

- عند حدوث خلل في أحد المسارات تقوم بروتوكولات التوجيه динاميки وبشكل تلقائي بتحديد مسار اخر للوصول للوجهه.

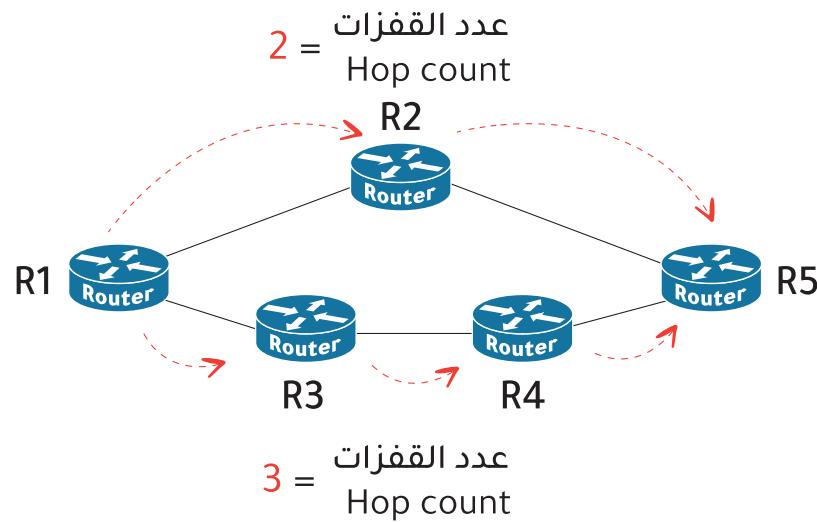
- يتم تطبيق إعدادات بروتوكول توجيه على كل راوتر في الشبكة لكي يتم التعرف على الشبكات و بناء جدول التوجيه بشكل اوتوماتيكي ما بين الشبكات من غير تدخل مهندس الشبكة في بناء جدول التوجيه.



لاحظ هنا عند تعطل منفذ R3 بدأ R1 بتغيير مساره بشكل تلقائي عبر R2 للوصول لـ R3 .



≡ أنواع الخوارزميات المستخدمة في بروتوكولات  
البوابة الداخلية IGP



### Distance Vector

هي بروتوكولات تعتمد على المسافة كمقاييس ( Metric ) ولا تهتم للسرعة.

1- المسافة هنا يقصد بها عدد القفزات ( Hop count ) من الجهاز المرسل إلى الجهاز المستقبل ، وسيتم اختيار المسار ذو عدد القفزات الأقل .

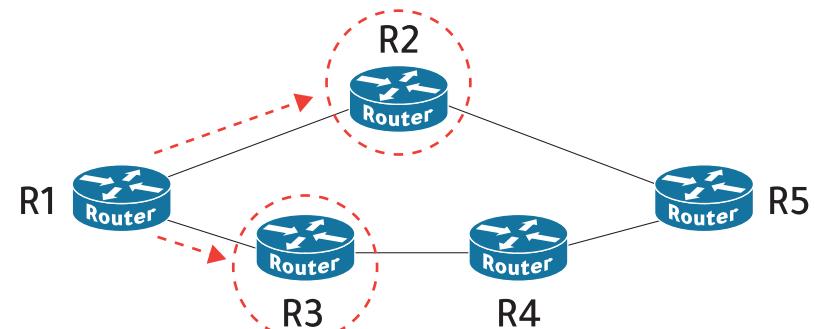
- المقاييس لـ Distance Vector هو عدد القفزات ( Hop count ) .

4 - الراوترات ترسل كل فترة معينة معلومات جدول التوجيه الى الراوترات المتصلة فقط بمنفذه مباشرة ، فلو حصل تحدث او تغير في راوتر فعليه الانتظار هذه المدة الزمنية المحددة وبعدها يرسل التحدث.

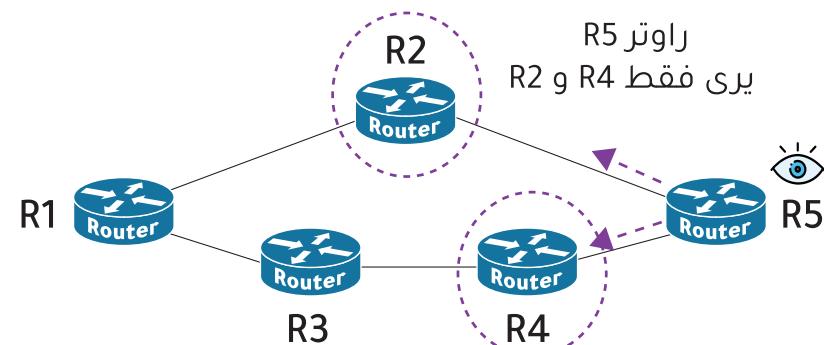
5 - يستخدم لوغاريتم تسمى bellman-ford .

6 - مثل بروتوكولات (RIP - EIGRP)

2 - الراوتر يتواصل فقط مع الراوترات المتصلة بمنفذه مباشرة (الجيران) وتسمى بـ (routing by rumor).



3 - الراوتر يعرف الجيران المتصلين بمنفذه مباشرة ولا يعرف ما بعدهم من أجهزة .

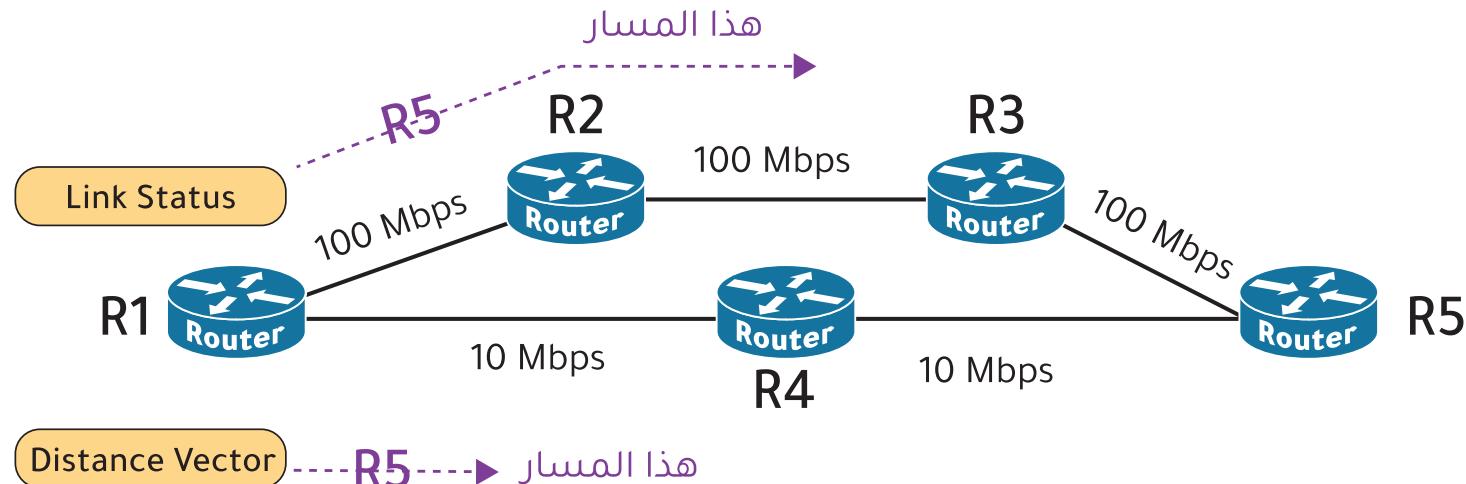


## Link State

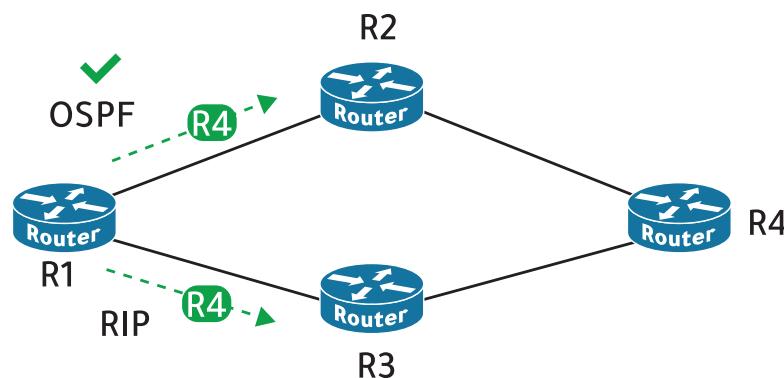
- 4 - كل الراوترات تتبادل معلومات link state information مع بعضها لتكوين خريطة الشبكة كاملة .
- 5 - كل راوتر لديه تصور شامل لكل الشبكة الداخلية .
- 6 - الراوترات ترسل التحديثات الجديدة مباشرة بدون اي انتظار .
- 7 - يستخدم لوغاريتم يسمى shortest path first
- 8 - مثل بروتوكولات (OSPF - IS-IS)

هي بروتوكولات التي تعتمد على السرعة (Bandwidth) كمقاييس (Metrics) ولا تهتم للمسافة .

- 1 - يقصد بال Bandwidth هي سعة نقل البيانات في الثانية الواحدة مثل (100 ميغابت في الثانية ) .
- 2 - المقياس لل Bandwidth هو Link State وتسمي العملية بال COST .
- 3 - كل راوتر يتواصل مع جميع الراوترات في الشبكة .



بروتوكول التوجيه Routing Protocol	المسافة الإدارية Administrative Distance
Directly connected	0
Static route	1
External BGP (eBGP)	20
internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External EIGRP	170
Internal BGP (iBGP)	200
Unknown	255



110 = المسافة الإدارية لـ OSPF ✓

120 = المسافة الإدارية لـ RIP

140

## المسافة الإدارية Administrative Distance (AD)

المسافة الإدارية هي الميزة التي تستخدمها أجهزة التوجيه (الراوتر) لتحديد أفضل مسار عندما يكون هناك مساران مختلفان أو أكثر لنفس الوجهة من بروتوكولي توجيه مختلفين .

- قيمة المسافة محددة مسبقاً (انظر الجدول التالي).
- الراوتر يعتمد ويستخدم المسار الذي له رقم أقل في حالة وجود بروتوكولين مختلفين .

## Metric

هو رقم يحدد عدد الموجهات ضمن الطريق المسلوك للوصول إلى الوجهة فهو يحدد كلفة الإرسال وبالتالي فهو يستخدم لتحديد الطريق الأفضل .

- فهو رقم يتم الاعتماد عليه للوصول إلى الشبكة المطلوبة ( في حالة تساوي المسافة الإدارية للمسارين ) .

يتم تحديد قيمة ال metric في كل بروتوكول بطريقه مختلفه عن الآخر :  
1- في الـ RIP تكون قيمة ال metric هي عدد القفزات للوصول الى الشبكة المطلوبة.

- 2- في الـ EIGRP يتم استخدام ال [ Bandwidth - Delay - Reliability - Load ] ووفقاً معادلة معينة يتم حساب ال metric .
- 3- في الـ OSPF يتم حسابه عن طريق ال bandwidth .

يتم ربط الشبكات البعيدة يدويا عن طريق مهندس الشبكة .

- في حال تعطل أحد مسارات الشبكة يتدخل المنهدس يدويا لحل المشكلة وتغيير المسار .

## Static Routing

### إعداد الـ Static Routing

#### أمر اضافة الـ Static

نختار واحدة من هذه الثلاث  
والأفضل هو الأول

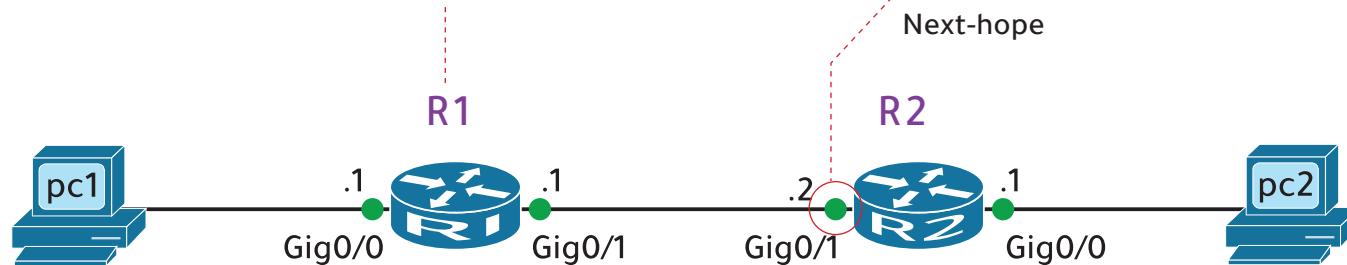
أمر الـ Static Routing

```
R1(config)# ip route ip-address subnetmask
```

نضع أيبي الشبكة  
الغير معروفة لدى  
الراوتر  
الغير معروفة  
للراوتر

أيبي المنفذ المقابل  
Next-hop  
مخرج منفذ الراوتر  
exit-interface  
... Gig0/1 ... exit-interface Next-hop  
... Gig0/1 11.0.0.2 ... exit-interface Next-hop

```
R1(config)# ip route 12.0.0.0 255.255.255.0 11.0.0.2
```



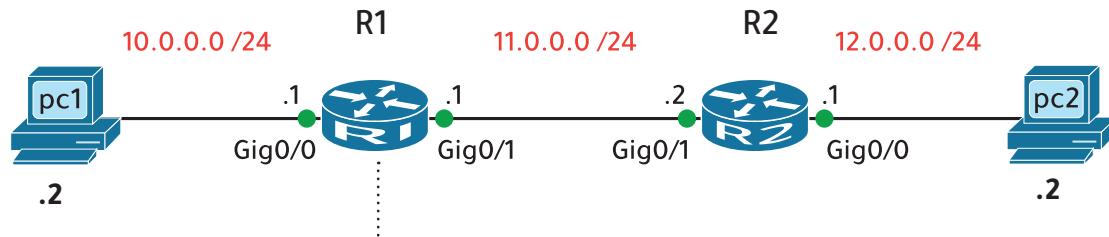
10.0.0.0 /24

11.0.0.0 /24

12.0.0.0 /24

## مثال :

سنطبق إعدادات الـ Static Routing على هذا المثال .



### مراحل التطبيق

- 1 اضافة الـ ip + subnet mask لمنافذ الراوتر .
- 2 أمر الـ Static لربط الشبكات .
- 3 اضافة الايبيات للجهزة PC2 و PC1 .
- 4 اختبار الاتصال بين PC2 و PC1 .

عند الدخول على الراوتر ستجد هذه الرسالة والتي تعني هل تريد تكوين الاعدادات عبر الاسئلة

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no      اكتب no



ندخل على المنفذ (interfaces) ونضيف الايبي(ip) + قناع الشبكة (subnet mask). ثم نستعرض جدول التوجيه.

```
R1# conf t
R1(config)# int g0/0
R1(config-if)# ip add 10.0.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# ip add 11.0.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#end
R1# wr
```

A

اضافة ip + mask  
نفعل المنفذ لانه  
مغلق افتراضيا

```
R2# conf t
R2(config)# int g0/0
R2(config-if)# ip add 12.0.0.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# int g0/1
R2(config-if)# ip add 11.0.0.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#end
R2# wr
```

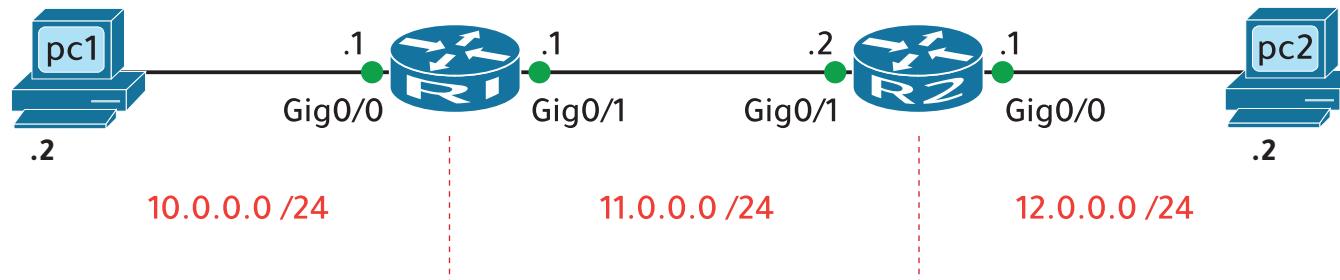
B

نستعرض جدول التوجيه routing table في الراوتر الاول [ show ip route ]  
عبر الامر R1  
ونلاحظ عدم وجود الشبكة (12.0.0.0) .  
سيتم اضافتها بطريقة JL Static

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, GigabitEthernet0/0
L    10.0.0.1/32 is directly connected, GigabitEthernet0/0
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    11.0.0.0/24 is directly connected, GigabitEthernet0/1
L    11.0.0.1/32 is directly connected, GigabitEthernet0/1
```

٢  
ندخل على الراوتر ونضيف أمر `ip route` لربط الشبكات واضافتها لجدول التوجيه table



**R1**

```
R1> en
R1# conf t
R1(config)# ip route 12.0.0.0 255.255.255.0 11.0.0.2
R1(config)#end
R1# wr
```

**R2**

```
R2> en
R2# conf t
R2(config)# ip route 10.0.0.0 255.255.255.0 11.0.0.1
R2(config)#end
R2# wr
```

نستعرض جدول التوجيه routing table في الراوتر الاول R1 والثاني R2 عبر الامر [ show ip route ]

**R1**

```
R1# show ip route
Codes: L - local, C - connected,
S - static, R - RIP, O - OSPF, D - EIGRP
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  10.0.0.0/24 is directly connected, GigabitEthernet0/0
L  10.0.0.1/32 is directly connected, GigabitEthernet0/0
  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  11.0.0.0/24 is directly connected, GigabitEthernet0/1
L  11.0.0.1/32 is directly connected, GigabitEthernet0/1
  12.0.0.0/24 is subnetted, 1 subnets
S  12.0.0.0/24 [1/0] via 11.0.0.2
```

الشبكة المخضافة في R1

ايبي المنفذ المقابل في الراوتر R2

Next hop ip address

**R2**

```
R2# show ip route
Codes: L - local, C - connected,
S - static, R - RIP, O - OSPF, D - EIGRP
Gateway of last resort is not set

  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  11.0.0.0/24 is directly connected, GigabitEthernet0/0
L  11.0.0.2/32 is directly connected, GigabitEthernet0/0
  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  12.0.0.0/24 is directly connected, GigabitEthernet0/1
L  12.0.0.1/32 is directly connected, GigabitEthernet0/1
  10.0.0.0/24 is subnetted, 1 subnets
S  10.0.0.0/24 [1/0] via 11.0.0.1
```

للحظ وجود حرف S والذي

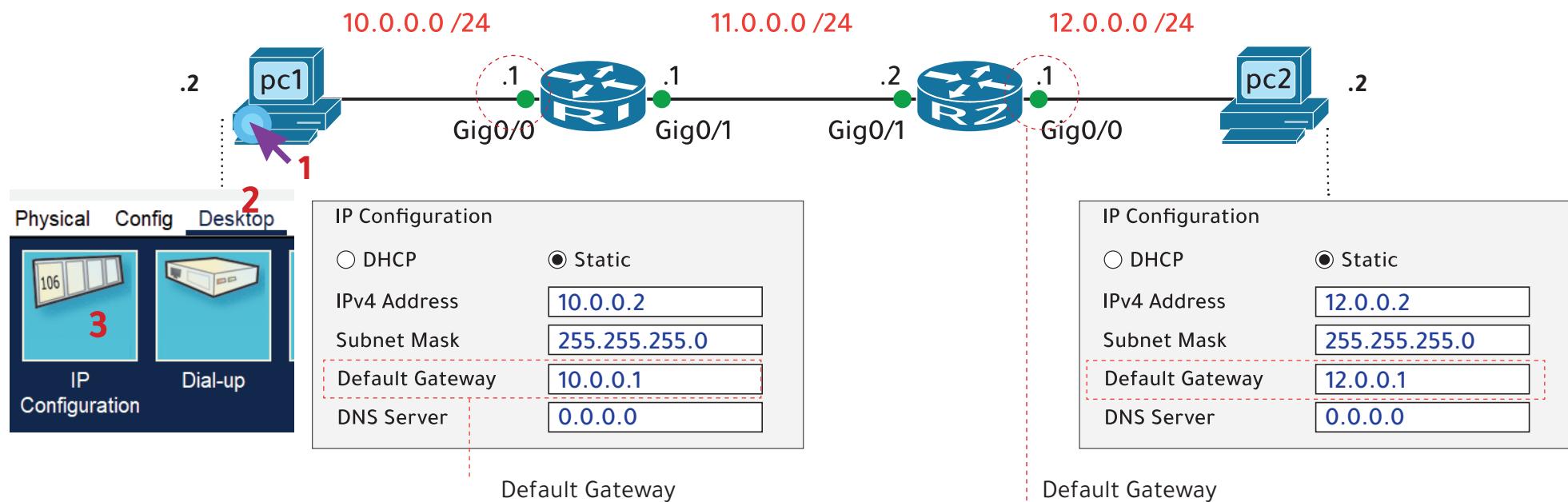
يرمز لـ static

[ 1 / 0 ]

1 : رقم المسافة الادارية (AD)

0 : هذا قيمة مقياس (Metric)

بروتوكول الـ static لا يتستخدم الا Metrics وستجده دائماً صفر



هي البوابة او الممر بين الشبكات المختلفة .

فلكي نخرج من شبكة الـ 10.0.0.0 نضع اىي المنفذ اللي يخرجنا الى شبكات اخرى و هو 10.0.0.1 وهو يعتبر البوابة .

هي البوابة او الممر بين الشبكات المختلفة .

فلكي نخرج من شبكة الـ 12.0.0.0 نضع اىي المنفذ اللي يخرجنا الى شبكات اخرى و هو 12.0.0.1 وهو يعتبر البوابة .

نختبر الاتصال في كل جهاز عبر الامر PING



PC1	تم الاتصال والرد بنجاح ✓
<pre>C:\&gt; ping 12.0.0.2 Pinging 12.0.0.2 with 32 bytes of data:  Reply from 12.0.0.2: bytes=32 time&lt;1ms TTL=126 Reply from 12.0.0.2: bytes=32 time&lt;1ms TTL=126 Reply from 12.0.0.2: bytes=32 time=2ms TTL=126 Reply from 12.0.0.2: bytes=32 time&lt;1ms TTL=126 Ping statistics for 12.0.0.2:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)</pre>	

PC2	تم الاتصال والرد بنجاح ✓
<pre>C:\&gt; Ping 10.0.0.2 Pinging 10.0.0.2 with 32 bytes of data:  Reply from 10.0.0.2: bytes=32 time&lt;1ms TTL=126 Reply from 10.0.0.2: bytes=32 time&lt;1ms TTL=126 Reply from 10.0.0.2: bytes=32 time=2ms TTL=126 Reply from 10.0.0.2: bytes=32 time&lt;1ms TTL=126 Ping statistics for 10.0.0.2:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)</pre>	

## الفرق بين الـ Host Route و Network Route

### Network Route

هو مسار الحزمة إلى شبكة كاملة (مكونة من عدة أجهزة).

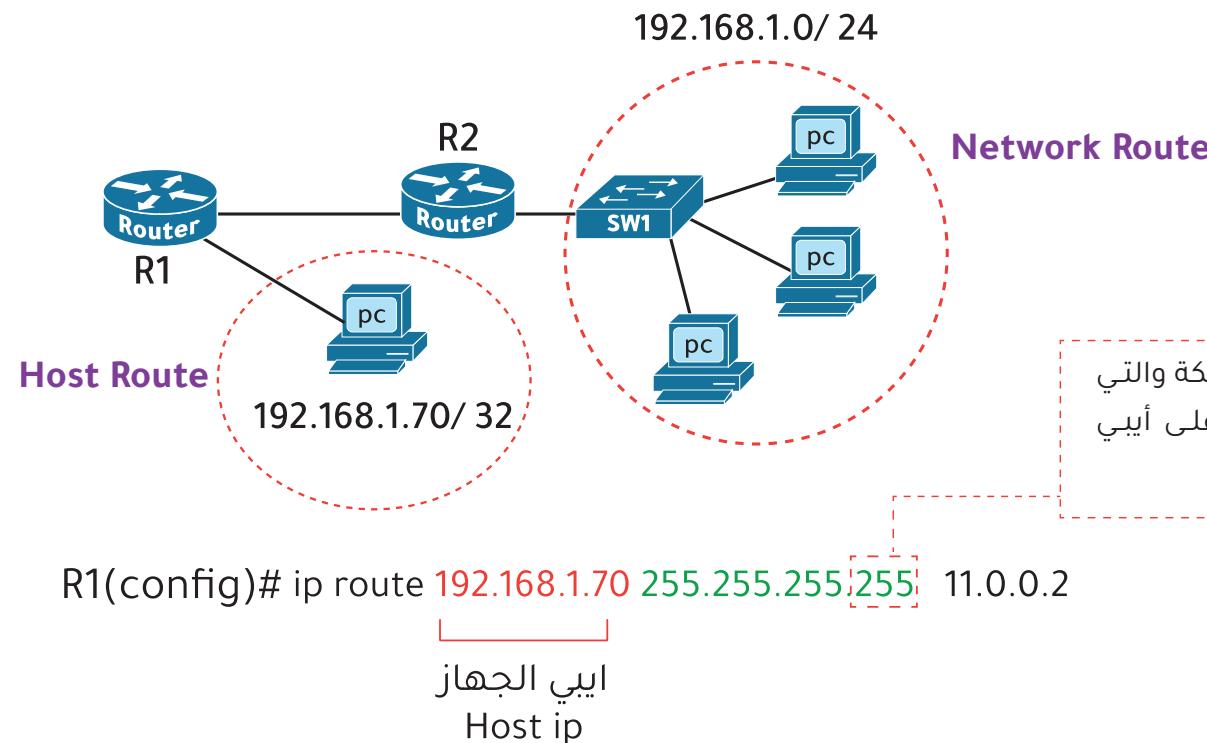
### Host Route

هو مسار الحزمة إلى عنوان محدد.

عنوان الشبكة  
Network ID

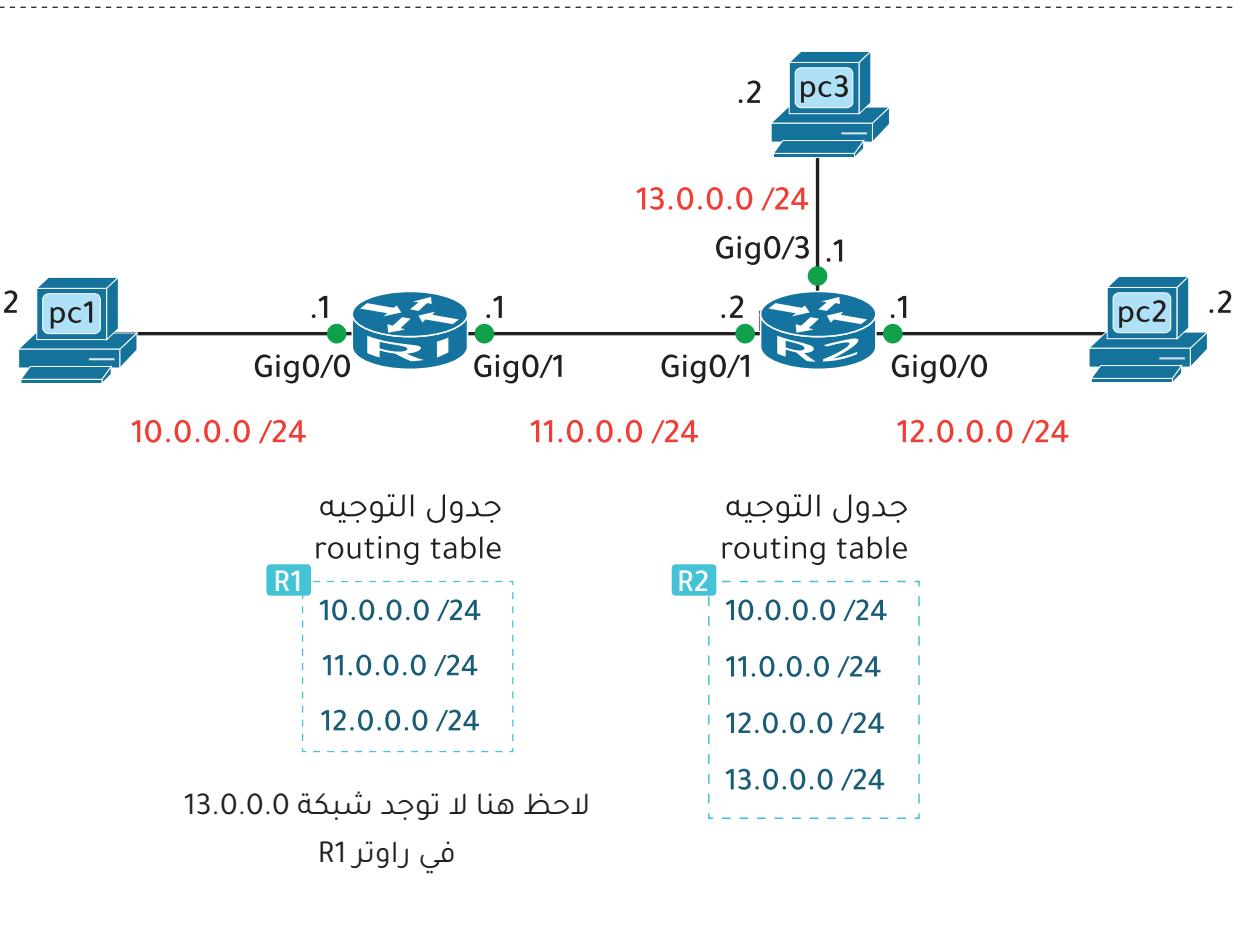
**Network Route**    R1(config)# ip route **192.168.1.0 255.255.255.0** **10.0.0.2**

لاحظ آخر خانة في قناع الشبكة والتي تدل على 24 / فهي تحتوي على 254 آيبي للأجهزة.



لاحظ آخر خانة في قناع الشبكة والتي تدل على 32 / فهي تحتوي على آيبي واحد فقط لجهاز محدد.

## Default Routing



تعرفنا أن المسار الافتراضي هو المسار الذي يتم استخدامه في حالة عدم وجود مسار معروف لعنوان IP في جدول التوجيه.

سنعمل التطبيق على المثال السابق.

تم اضافة شبكة جديدة وجهاز جديد.

- سيتم تطبيق الـ Default Routing على R1

- سيتم اختبار الاتصال من PC1 إلى PC3

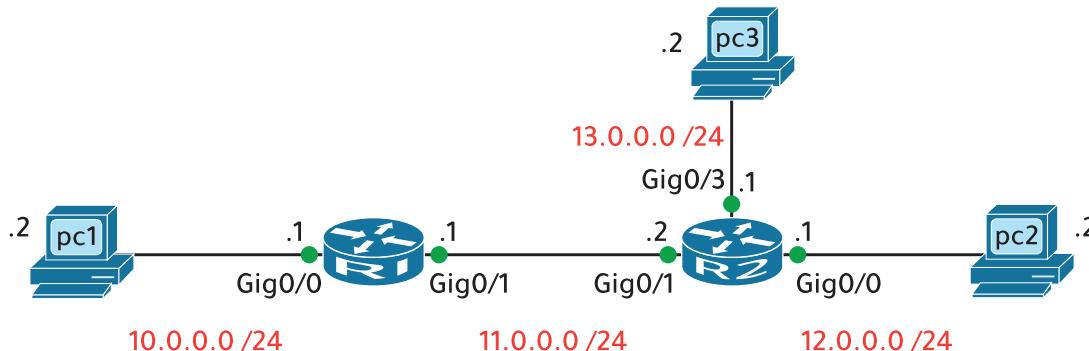
البداية :

1 - اضافة الشبكة الجديدة في المنفذ Gig0/3 الموجود في R2.

2 - اضافة أمر الـ Default Routing في R1

3 - اختبار الاتصال من PC1 الى PC3

4 - نستعرض جدول التوجيه routing table للراوتر R1



R2

```
1
R2(config)# int g0/3
R2(config-if)# ip add 13.0.0.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#ex
R2# wr
```

R1

```
2
R1(config)# ip route 0.0.0.0 0.0.0.0 11.0.0.2
R1(config)# end
R1# wr
```

نخبر الراوتر انه اذا وصل اليك اي ايبي (ip) غير معروف وغير موجود  
بجدول التوجيه اعمل له توجيه الى الـ 0.0.0.2  
(Next hop) 11.0.0.2

اختبار الاتصال من PC1 الى PC3

PC1

```
3
C:\> ping 13.0.0.2
Pinging 13.0.0.2 with 32 bytes of data:
Reply from 13.0.0.2: bytes=32 time<1ms TTL=126
Reply from 13.0.0.2: bytes=32 time<1ms TTL=126
Reply from 13.0.0.2: bytes=32 time=2ms TTL=126
Reply from 13.0.0.2: bytes=32 time<1ms TTL=126
Ping statistics for 13.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

نستعرض جدول التوجيه routing table للراوتر R1

**R1**

```

R1# show ip route
Codes: L - local, C - connected,
S - static, R - RIP, O - OSPF, D - EIGRP
Gateway of last resort is 11.0.0.2 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/24 is directly connected, GigabitEthernet0/0
L 10.0.0.1/32 is directly connected, GigabitEthernet0/0
 11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 11.0.0.0/24 is directly connected, GigabitEthernet0/1
L 11.0.0.1/32 is directly connected, GigabitEthernet0/1
 12.0.0.0/24 is subnetted, 1 subnets
S 12.0.0.0/24 [1/0] via 11.0.0.2
S* 0.0.0.0/0 [1/0] via 11.0.0.2

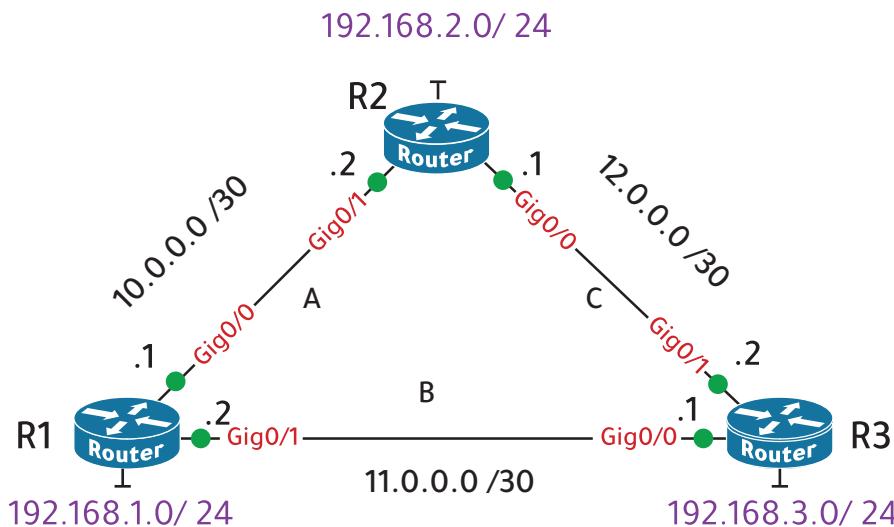
```

4

هذا السطر يخبرنا ان الحل الأخير في حالة لم تكن الشبكة موجودة ضمن الجدول هو التوجيه إلى العنوان التالي 11.0.0.2

للحظ وجود حرف \* والذي يرمز

للـ Default Routing

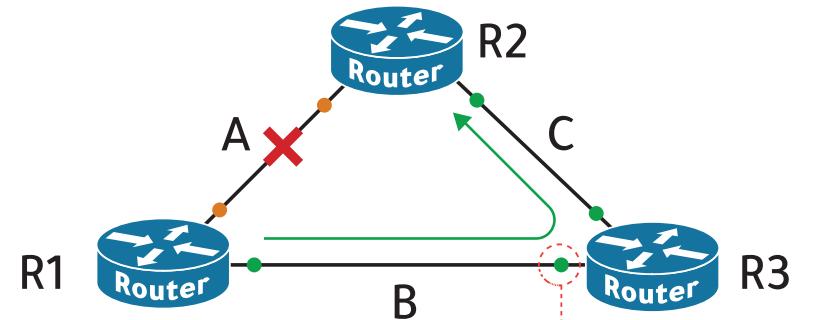


## Floating Static Route

هو static route عادي ولكن بمسافة إدارية أعلى من العادي ويستخدم كتوجيه احتياطي .  
- في حالة تعطل المسار الاول يتم توجيه البيانات عبر المسار الاحتياطي تلقائي.  
- المسافة الادارية الافتراضية لـ static route هو 1  
- سيكون بيانات الـ Floating Static Route مخفية في جدول التوجيه وستظهر عند تعطل مسار static route الاول .  
- نضيف لـ Floating Static Route رقم أعلى من رقم المسافة الادارية لـ static route ويكون في اخر السطر.

**مثال :**

```
R3
R3(config)# int g0/0
R3(config-if)# ip add 11.0.0.1 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# int g0/1
R3(config-if)# ip add 12.0.0.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)#ex
R3(config)# ip route 192.168.2.0 255.255.255.0 12.0.0.1
R3(config)# ip route 192.168.1.0 255.255.255.0 11.0.0.2
R3(config)# end
R3# wr
```



في حالة تعطل المسار  
A يجعل الراوتر R1 يتخد  
المسار الاحتياطي B

جعل الراوتر R2 يرى R1  
عبر هذا المنفذ لأنه يُعتبر  
الـ Next hop للراوتر R1

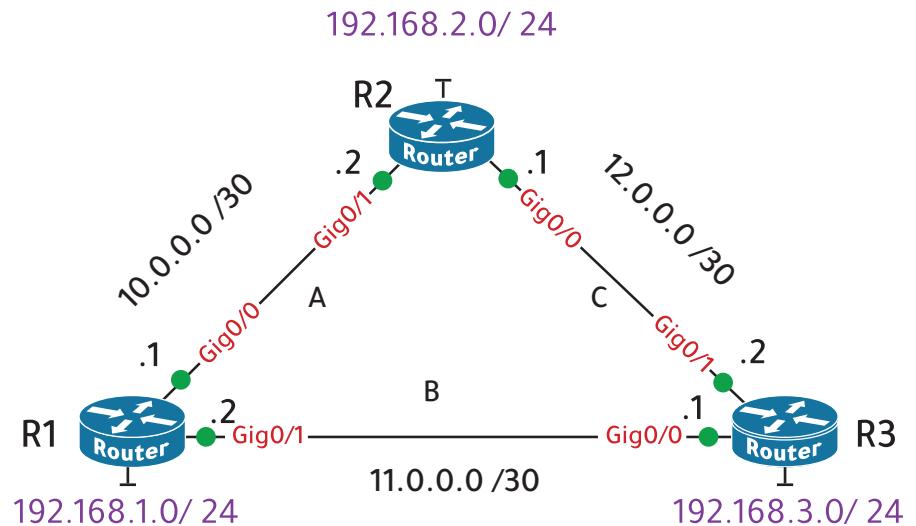
```
R1(config)# int g0/0
R1(config-if)# ip add 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# ip add 11.0.0.2 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)#ex
R1(config)# ip route 192.168.3.0 255.255.255.0 11.0.0.1
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.2.0 255.255.255.0 11.0.0.1 5
R1(config)# end
R1# wr
```

هذا امر ال Floating Static Route الذي يجعل المسار B--> C احتياطي في حال تعطل المسار A.

لان R1 يرى R2 عبر ال Next hop اللي هو 10.0.0.2 وفي حال تعطل المسار A سوف يتخد R1 المسار B--> C ويصبح 11.0.0.1 Next hop اللي هو R2 عبر ال R2 اللي هو 10.0.0.1

اضفنا رقم مسافة إدارية أعلى من رقم ال static route

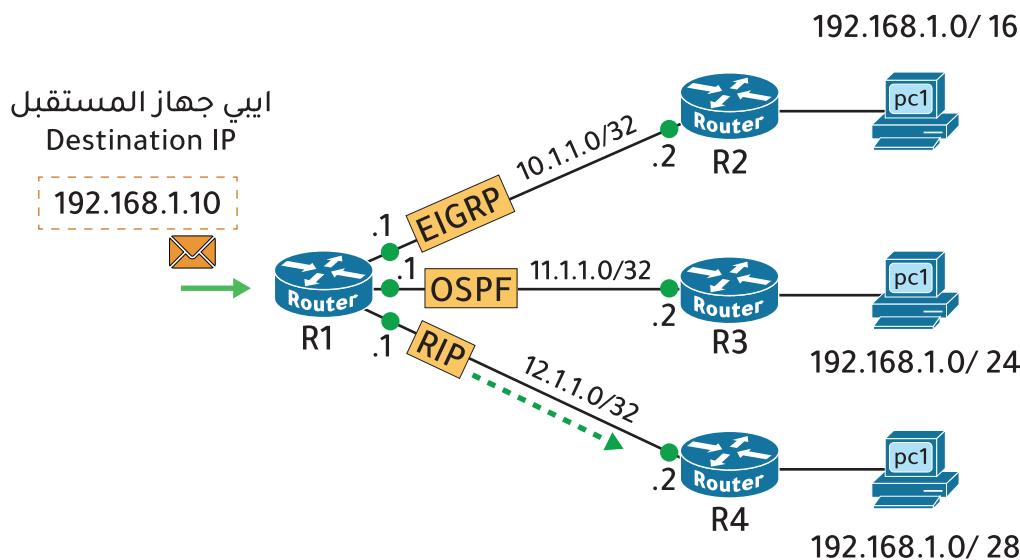
هذا امر ال Floating Static Route الذي يجعل المسار B--> C احتياطي في حال تعطل المسار A.  
لان R2 يرى R1 عبر ال Next hop اللي هو 10.0.0.1 وفي حال تعطل المسار A سوف يتخد R2 المسار C--> B ويصبح R2 يرى R1 عبر ال R1 اللي هو 12.0.0.2



```
R2(config)# int g0/1
R2(config-if)# ip add 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# int g0/0
R2(config-if)# ip add 12.0.0.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)#ex
R2(config)# ip route 192.168.3.0 255.255.255.0 12.0.0.2
R2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
R2(config)# ip route 192.168.1.0 255.255.255.0 12.0.0.2 5
R2(config)# end
R2# wr
```

## Longest Prefix Match

في هذا المثال : ايبي جهاز المستقبل يقع في مدي الشبكات الثلاث ، فالراوتر اختار المسار الثالث لأن ايبي جهاز المستقبل يقع ضمن مدي هذه الشبكة . وهي أقل مدي في الشبكات الثلاث ، ايضا هي أطول Prefix متطابق



طريقة الراوتر في تحديد أفضل مسار ، سوف يبدأ بهذا الترتيب :

Longest Prefix Match - 1

2 - أقل رقم في المسافة الإدارية

3 - أقل رقم في الـ Metric

- في حال تساوي Longest Prefix Match في كل المسارات يتوجه الراوتر للخيار الثاني (المسافة الادارية AD) .

- في حال تساوي الخيار الاول والثاني في كل المسارات يتوجه الراوتر للخيار الثالث Metric .

فعملا يتلقى جهاز الراوتر حزمة IP ، عليه أن يقرر إلى أي مسار سوف يوجهها في حال كان أكثر من مسار وكان الـ ip ضمن مدي هذه الشبكات .

- فهو يختار أفضل وأعلى Prefix متطابق . وأقل مدي شبكة يقع فيها هذا الايبي .

← توضيح المثال بالصفحة التالية

نجد أن الايبي 192.168.1.10 موجود في كل الشبكات الثلاث ولكن هذه الشبكة 192.168.1.0 /28 هي أعلى في الـ Prefix وهو /28 و أقل مدي .

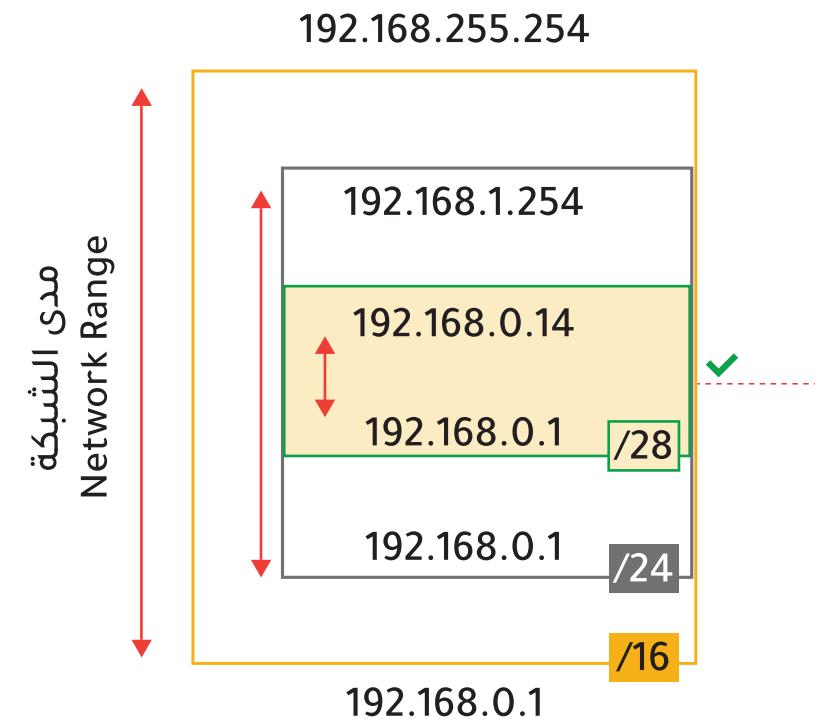
### توجد طريقة أخرى :

نحول الايبيات الى النظام الثنائي ثم نحدد عدد البتات ونرى أطول prefix مشابه لايبي المستقبل 192.168.1.10

النظام العشري Decimal System	النظام الثنائي Binary
192.168.1.10	11000000.10101000.00000001.0000
192.168.1.0 /16	11000000.10101000.00000001.0000
192.168.1.0 /24	11000000.10101000.00000001.0000
192.168.1.0 /28	11000000.10101000.00000001.0000

لاحظ وضعنا خط عمودي عند اول اختلاف بين ايبي المستقبل والايبيات الاخرى وبكذا وجدنا ان 28 / هو اطول prefix مطابق لايبي المستقبل .

الشبكات Networks	أول ايبي متاح first valid ip	آخر ايبي متاح last valid ip
192.168.1.0 /16	192.168.1.1	192.168.255.254
192.168.1.0 /24	192.168.1.1	192.168.1.254
192.168.1.0 /28	192.168.1.1	192.168.1.14



هذا الامر لكي يعمل المنفذ كمنفذ راوتر و يتقبل اضافة الابيبي ip وال subnet mask

```

SW1(config)# int Fa0/1
SW1(config-if)# no switchport
SW1(config-if)# ip add 11.0.0.1 255.255.255.252
SW1(config-if)# exit

SW1(config)# int Fa0/2
SW1(config-if)# no switchport
SW1(config-if)# ip add 192.168.1.1 255.255.255.0
SW1(config-if)# exit

SW1(config)# ip routing

SW1(config)# ip route 192.168.5.0 255.255.255.0 11.0.0.2

```

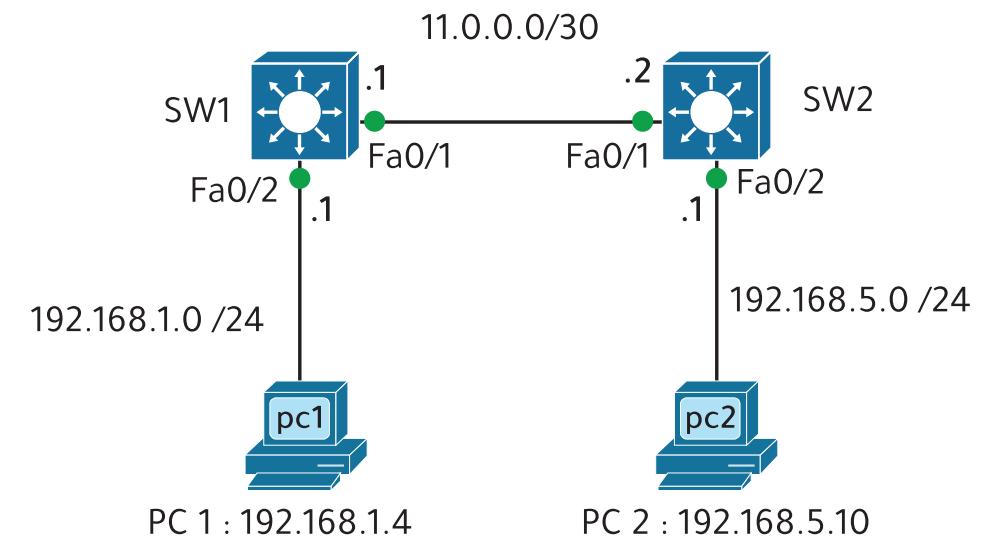
لتفعيل عملية التمرير او التوجيه (Routing) داخل السويتش

## إعداد الـ static route على سويتش متعدد الطبقات (Multi Layer Switch switch)



- سويتش متعدد الطبقات (Multi Layer Switch) : هو جهاز شبكة لديه القدرة على العمل في طبقات أعلى في نموذج OSI .
- يعمل في الطبقات LAYER 2 + LAYER 3 وأعلى .
- يقوم بوظائف السويتش و الراوتر معا .

**مثال :**



PC1

تم الاتصال والرد بنجاح ✓

C:\&gt; ping 192.168.5.10

Pinging 192.168.5.10 with 32 bytes of data:

Reply from 192.168.5.10: bytes=32 time&lt;1ms TTL=126

Reply from 192.168.5.10: bytes=32 time&lt;1ms TTL=126

Reply from 192.168.5.10: bytes=32 time=2ms TTL=126

Reply from 192.168.5.10: bytes=32 time&lt;1ms TTL=126

Ping statistics for 192.168.5.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

PC2

تم الاتصال والرد بنجاح ✓

C:\&gt; Ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time&lt;1ms TTL=126

Reply from 192.168.1.4: bytes=32 time&lt;1ms TTL=126

Reply from 192.168.1.4: bytes=32 time=2ms TTL=126

Reply from 192.168.1.4: bytes=32 time&lt;1ms TTL=126

Ping statistics for 192.168.1.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

SW2

SW2(config)# int Fa0/1

SW2(config-if)# no switchport

SW2(config-if)# ip add 11.0.0.2 255.255.255.252

SW2(config-if)# exit

SW2(config)# int Fa0/2

SW2(config-if)# no switchport

SW2(config-if)# ip add 192.168.5.1 255.255.255.0

SW2(config-if)# exit

SW2(config)# ip routing

SW2(config)# ip route 192.168.1.0 255.255.255.0 11.0.0.1

R1

```

1 R1(config)# ipv6 unicast-routing
2 R1(config)# int Gig0/0
R1(config-if)# ipv6 add 2001::1/64
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# int Gig0/1
R1(config-if)# ipv6 add fec4::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 route fec2::0/64 2001::2
3

```

تفعيل أمر التوجيه في الاصدار السادس و هو كافي لتهيئة الراوتر لاستقبال اى بثات الاصدار السادس

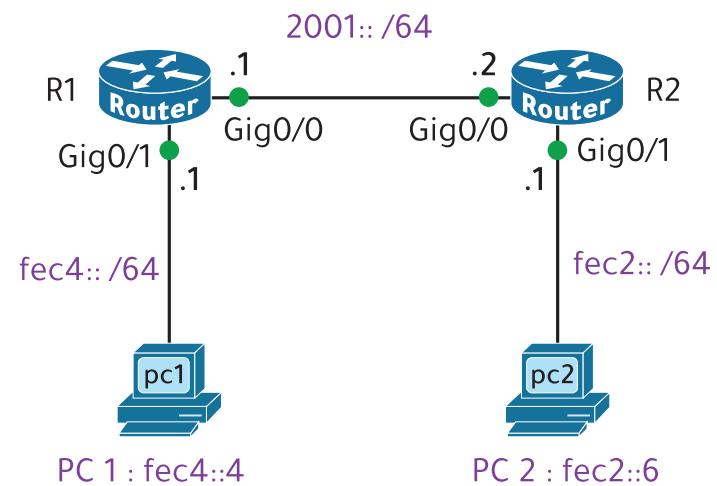
## إعداد الـ **static route** مع **ipv6**



سنعرف على كيفية اضافة اى بثات الاصدار السادس static route .

- 1 - تفعيل امر توجيه الاصدار السادس **ipv6**
- 2 - اضافة الابثات للمنفذ . static route
- 3 - ادخال امر الـ static route

**مثال :**

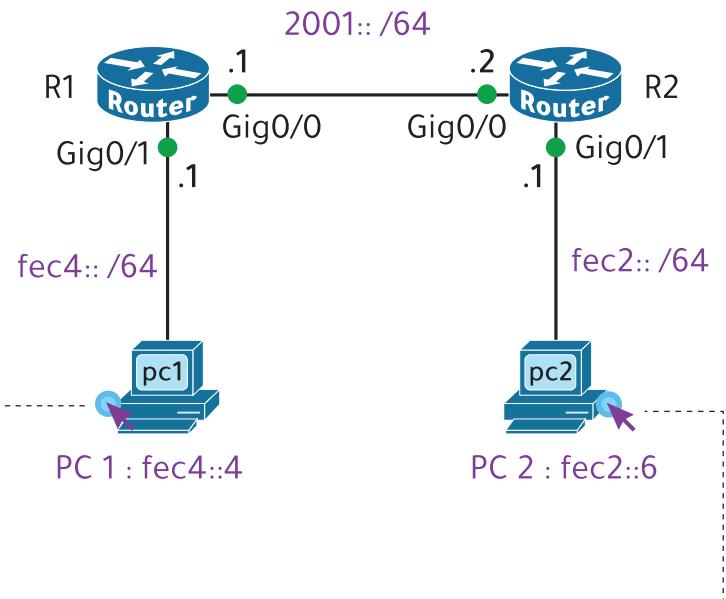


```

1 R2(config)# ipv6 unicast-routing
2 R2(config)# int Gig0/0
R2(config-if)# ipv6 add 2001::2/64
R2(config-if)# no shutdown
R2(config-if)# exit

R2(config)# int Gig0/1
R2(config-if)# ipv6 add fec2::1/64
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# ipv6 route fec4::0/64 2001::1
3

```



**IPv6 Configuration**

Automatic  Static

IPv6 Address: **fec4::4** / **64**

Link Local Address: **FE80::202:4AFF:FE0D:9C2C**

Default Gateway: **fec4::1**

**IPv6 Configuration**

Automatic  Static

IPv6 Address: **fec2::6** / **64**

Link Local Address: **FE80::202:4AFF:FE0D:9C2C**

Default Gateway: **fec2::1**

**R1**

```
R1# show ipv6 route
Codes: L - local, C - connected,
S - static, R - RIP, O - OSPF, D - EIGRP

C 2001::/64 [0/0]    via GigabitEthernet0/0, directly connected
L 2001::1/128 [0/0]   via GigabitEthernet0/0, receive
S  FEC2::/64 [1/0]    via 2001::2
C  FEC4::/64 [0/0]    via GigabitEthernet0/1, directly connected
L  FEC4::1/128 [0/0]  via GigabitEthernet0/1, receive
L  FF00::/8 [0/0]     via Null0, receive
```



لشراء الجزء الثاني  
واتساب فقط

 0552102740