



# مذكرة لـ CCNA العربية

200 - 301

## الجزء الثاني 02



[clickone1.com](http://clickone1.com)



[clickone\\_1](https://twitter.com/clickone_1)



[clickone1](https://t.me/clickone1)

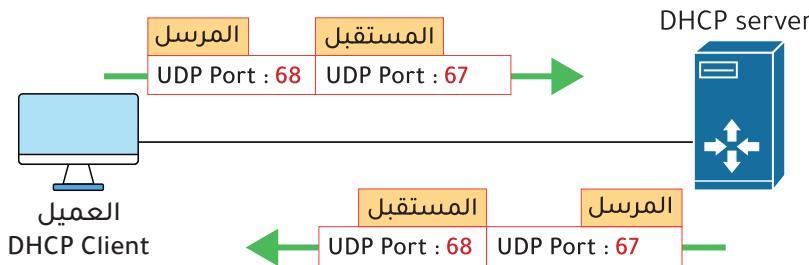


0552102740

## فهرس الجزء الثاني

176	HTTP Request	111	بدائل كلمات المرور	3	بروتوكول التكوين динамический (DHCP)
177	HTTP Response	112	المصادقة - التفويض - المحاسبة	8	DHCP Relay Agents
178	Representational State Transfer (REST)	113	عناصر برنامج الأمان	13	First Hop Redundancy Protocols
181	Cisco SD-Access	114	Port Security	20	قواعد التحكم بالوصول (ACL)
186	أدوات إدارة التكوين	120	DHCP Snooping	35	بروتوكول NAT
		125	Dynamic ARP Inspection (DAI)	47	بروتوكول وقت الشبكة (NTP)
		129	التحكم في الوصول إلى الجهاز	56	بروتوكول إدارة الشبكة البسيط
		130	الشبكة الافتراضية الخاصة	67	Telnet - SSH
		130	Virtual Private Network (VPN)	71	بروتوكولات نقل الملفات (TFTP - FTP)
		134	الشبكات اللاسلكية	73	جودة الخدمة (QoS)
		139	مجموعات الخدمة Service Sets	91	النظام الثنائي Binary
		145	معمارية الشبكات اللاسلكية	91	النظام العشري Decimal
		153	أمان الشبكات اللاسلكية	91	النظام السداسي عشر Hexadecimal
		155	طرق المصادقة	92	التحويل من الثنائي الى السداسي عشر
		159	طرق التشفير و التكامل	92	التحويل من السداسي عشر الى الثنائي
		160	الوصول المحمي بشبكة WiFi	93	بروتوكول IPv6
		162	أتمنة الشبكات	94	طرق اختصار عنوان الـ IPv6
		164	الشبكات المعرفة بالبرمجيات	97	إعدادات الـ IPv6
		168	Southbound Interface (SBI)	98	EUI-64
		168	Northbound Interface (NBI)	100	أنواع عناوين الـ ipv6
		170	JavaScript Object Notation ( JSON )	103	نطاق أو مجال البث المتعدد
		172	Application Programming Interface (API)	104	Security Fundamentals
		173	بروتوكول الـ HTTP	104	مفاهيم الأمان الأساسية
		175	محظى المواقع Resources	105	الهجمات الشائعة

- يستخدم بروتوكول DHCP ببروتوكول UDP للتواصل مع العميل Client : يستخدم بورت أو منفذ 68 للتواصل مع العميل DHCP Server . (UDP Port 67).
- DHCP Server : يستخدم بورت أو منفذ 67 للتواصل مع العميل Client . (UDP Port 68).



### وقت التأجير Lease Time

هو مقدار الوقت بالدقيقة أو الساعات الذي يحتفظ العميل او جهاز الحاسب بعنوان الايبي ip حتى انتهاء صلاحية الحجز . بعد هذا الوقت يجب على جهاز الحاسب أو العميل تجديد عنوان IP .

### طريقة عمل بروتوكول DHCP

يتم توزيع الايبيات على الاجهزه تلقائيا بعد المرور بعده مراحل DORA ونطلق عليها .

- 1 - Discover
- 2 - Offer
- 3 - Request
- 4 - Acknowledgement

## بروتوكول التكوين динамический للمضيف (DHCP)

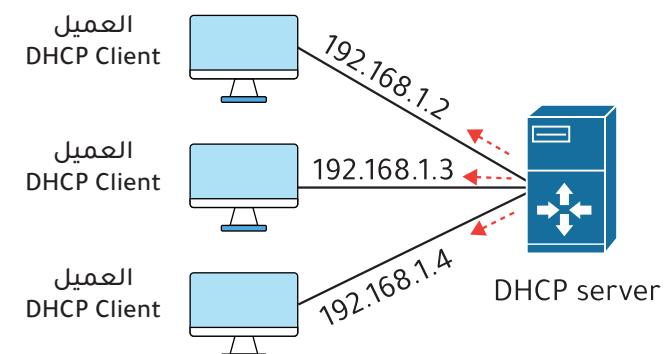
### Dynamic Host Configuration Protocol (DHCP)

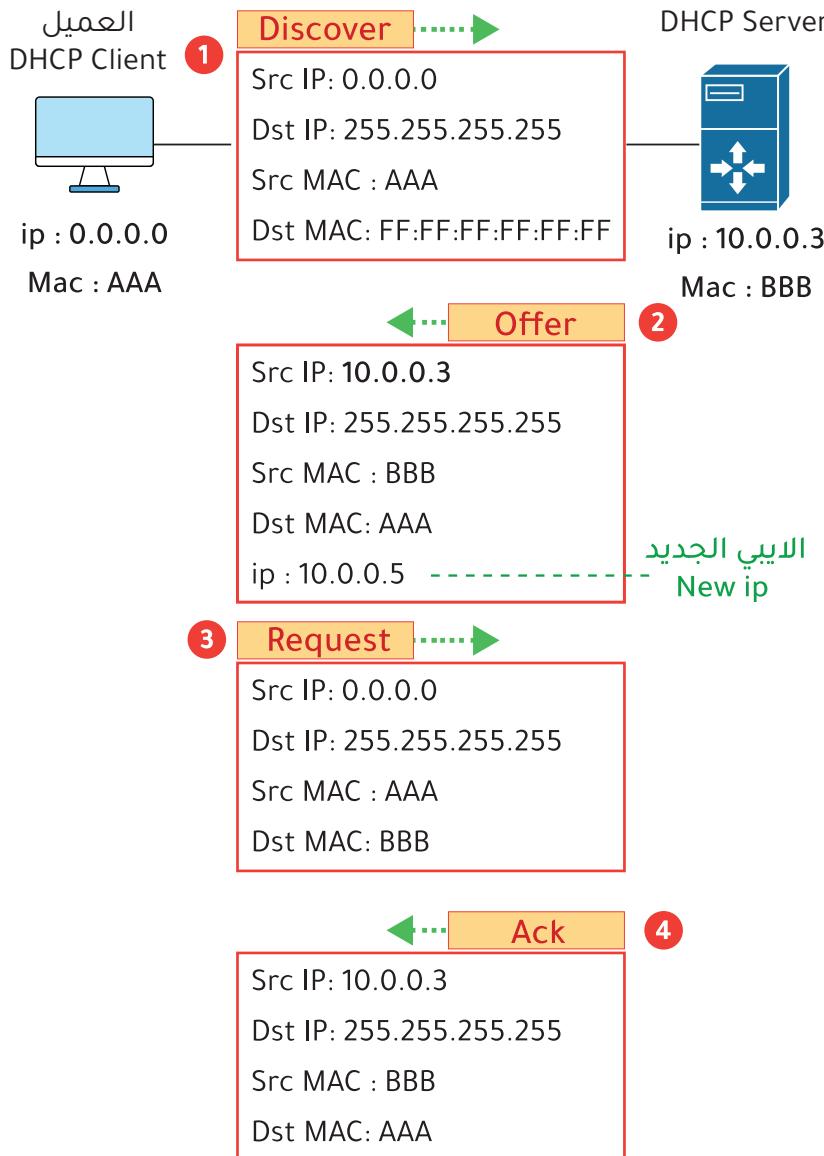
هذا البروتوكول هو المسؤول عن تعيين عنوان (IP Address) مع بعض إعدادات الشبكة لكل جهاز يتم توصيله على الشبكة بشكل تلقائي دون أي تدخل منك .

- مثل عند اتصالك بشبكة الواي فاي بالمنزل فإنك تحصل على عنوان أبيي بشكل تلقائي من جهاز الشبكة . فهذا هو عمل الـ DHCP وهو توزيع العناوين بشكل تلقائي .

- هذه بعض إعدادات الشبكة التي يقوم الـ DHCP بارسالها وتوزيعها للجهاز :

- IP Address - 1
- Subnet Mask - 2
- IP Default Gateway - 3
- DNS Server - 4





يرسل العميل رسالة برودكاست broadcast للجميع يستكشف فيها عن موزع الايبيات DHCP Server لطلب ايبي .



يقوم الـ DHCP Server بالرد على العميل ويرسل له عرض فيه عنوان ايبي IP Address جديد متاح مع بعض الاعدادات الأخرى .



يستلم العميل الرسالة ويقوم بالرد برسالة الموافقة على هذا العرض الذي يحتوي على الايبي الجديد والاعدادات الأخرى



يقوم الـ DHCP Server بالرد على العميل برسالة تأكيد بأنه يمكنه استخدام هذا العنوان الجديد

## مثال :

لدينا هذا النموذج وايضا البيانات التالية :

DHCP Pool : Lan2 -

Network : 192.168.1.0 -

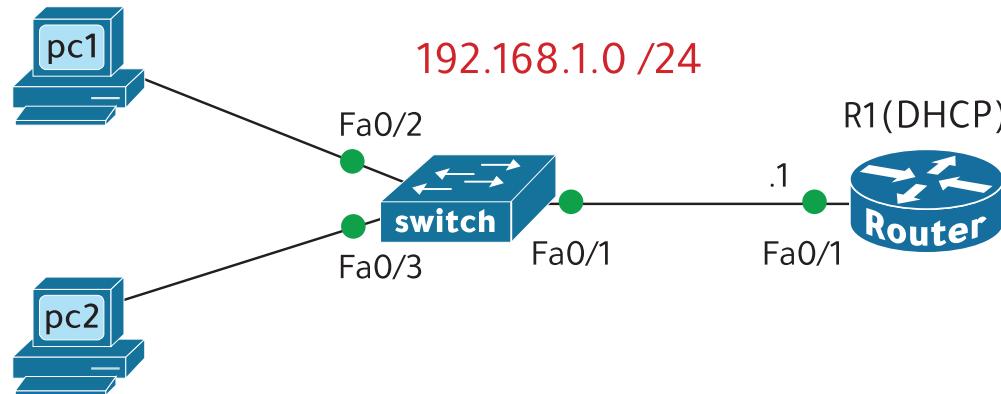
Default Gateway : 192.168.1.1 -

Domain-name : Lan2.com -

dns-server : 8.8.8.8 -

- عمل استثناء لعنوان البوابة الافتراضية حتى لا يتم توزيعه على الاجهزة

Exclude the default gateway address from the pool



أمر استثناء ايبي  
البوابة الافتراضية

أمر انشاء او dhcp  
وتسمية او pool  
بر Lan2

تعيين ايبي البوابة  
الافتراضية  
default gateway

```
R1(config)# int Fa0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# ip dhcp excluded-address 192.168.1.1
R1(config)# ip dhcp pool Lan2
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8
R1(dhcp-config)# domain-name Lan2.com
R1(dhcp-config)# exit
```

تعيين الشبكة التي سيتم توزيع  
الايبيات منها .

## مراحل الحل :

1 تطبيق الإعدادات الأساسية .

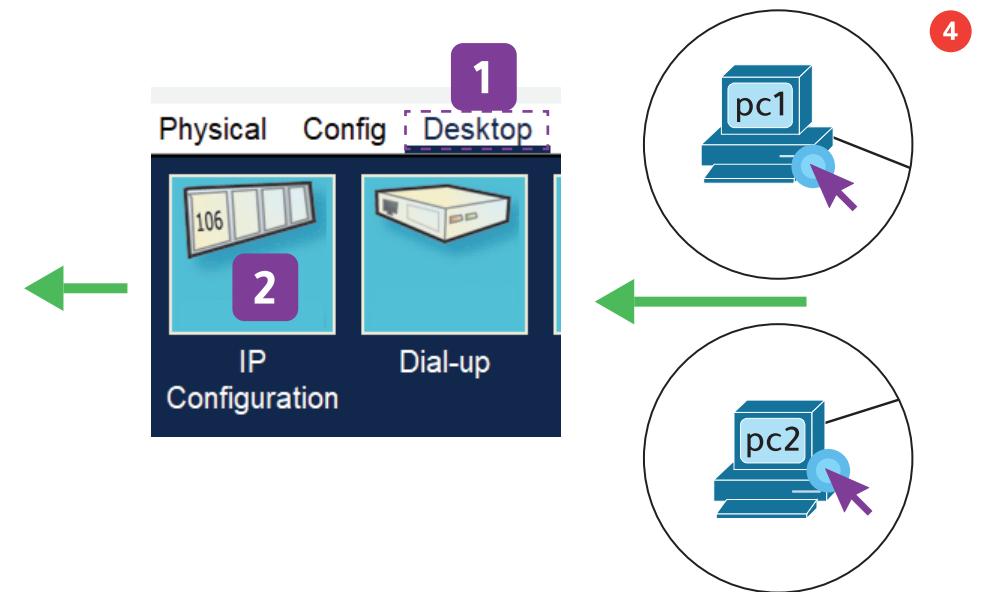
2 عمل استثناء للإيبيات الخاصة مثل ايبي البوابة  
الافتراضية .

3 تطبيق اعدادات بروتوكول DHCP

4 الدخول على الحاسب واختيار اعداد DHCP حتى  
يحصل على عنوان من الموزع للإيبيات

IP Configuration	DHCP request successful
<b>3</b>	<input checked="" type="radio"/> DHCP <input type="radio"/> Static
IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

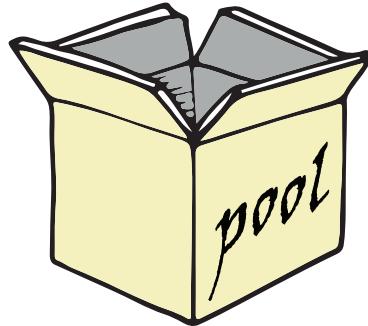
IP Configuration	DHCP request successful
<b>3</b>	<input checked="" type="radio"/> DHCP <input type="radio"/> Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8



نستعرض جدول dhcp binding

R1# show ip dhcp binding			
عنوان الابي الذي تم إعطائه للجهاز	ماك أدرس الجهاز	انتهاء فترة التأجير	نوع التوزيع
IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.2	0001.9694.77DD	-----	Automatic
192.168.1.3	00E0.F9A8.1DBD	-----	Automatic

نستعرض جدول dhcp pool



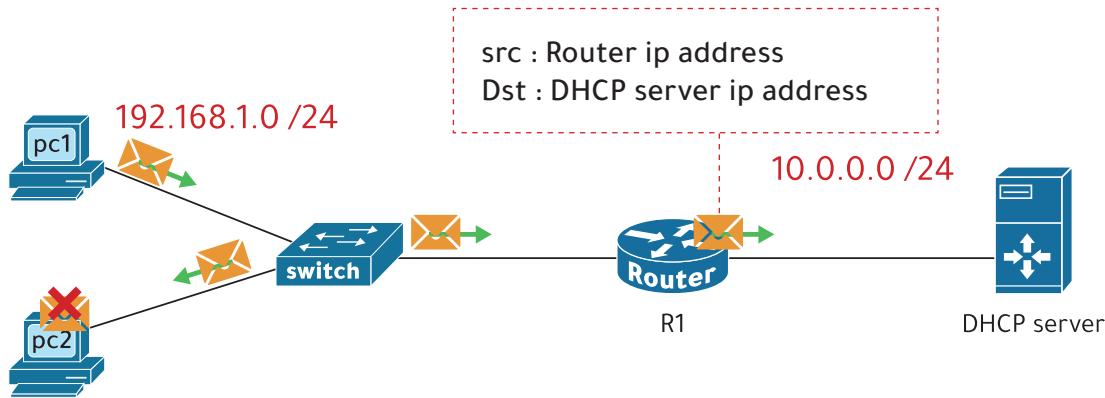
ال pool هو مثل الصندوق أو المخزن ونقصد به انه يحتوي على الايبيات ليكون مستودع للتوزيع

R1# show ip dhcp pool				
Pool LAN2 :				
Utilization mark (high/low)	:	100 / 0		
Subnet size (first/next)	:	0 / 0		
Total addresses	:	254	-----	عدد الايبيات المتاحة
Leased addresses	:	2	-----	عدد الايبيات المُؤجرة
Excluded addresses	:	1	-----	عدد الايبيات المستثناء
Pending event	:	none		
1 subnet is currently in the pool				
Current index	IP address range	Leased	Excluded	Total
192.168.1.1	192.168.1.1 - 192.168.1.254	2	1	254

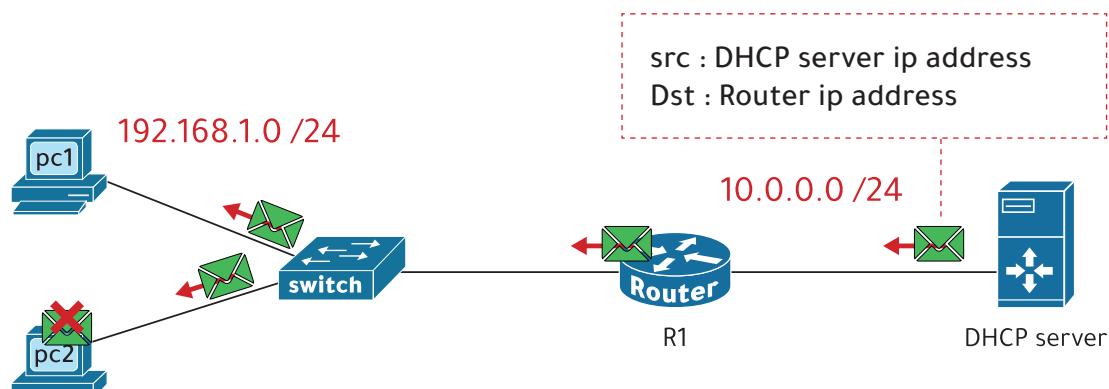
مدى عناوين الايبي المتاحة  
في الشبكة

### كيف تعمل خدمة DHCP Relay

A - عندما يرسل العميل رسالة بروكاست توصيل للسويتش . والسويتش يعيد توجيهها للكل ويستقبلها الراوتر الذي يبدأ بالاتصال مع خادم DHCP وسوف تلاحظ ان الراوتر وضع الايبي الخاص به لانه هو الذي يتواصل مع الخادم .



B - عندما توصل الرسالة للخادم يقوم بالرد عليها ويرسلها للراوتر ثم الراوتر يرسلها الى السويتش ومن ثم الى الجهاز الذي ارسل الرسالة .



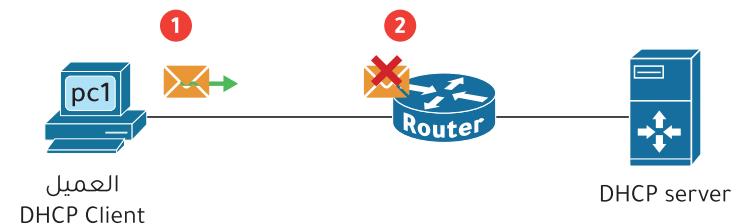
### DHCP Relay Agents

هي خدمة تسمح بمرور حزمة DHCP بين العملاء والخوادم الغير موجودين في نفس الشبكة وذلك لوجود الراوتر بينهم .

انظر هذه الصورة :

1 - بدأ العميل بارسال رسالة بروكاست يستكشف فيها عن خادم DHCP للحصول على عنوان ايبي ip address

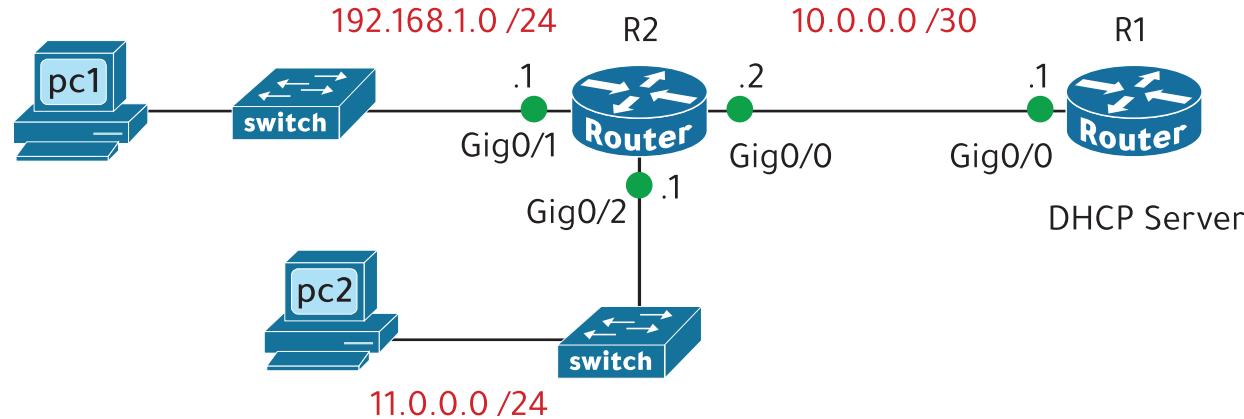
2 - عندما وصلت للراوتر رفض اعادة توجيهها والسبب ان الراوتر لا يعيد توجيه حزم البروكاست نهائياً .



### الحل هو

تفعيل خدمة DHCP Relay على الراوتر لكي يسمح للعملاء بالتواصل مع خادم DHCP وذلك عبر اضافة هذا الامر :

`R1(config-if)# ip helper-address dhcp`



**مثال :**

لدينا هذا النموذج وسوف نوزع ابيهات لشبكتين مختلفة من جهاز واحد R1 .

# بيانات النموذج :

DHCP Pool : Lan1 -

Network : 192.168.1.0 /24 -

Default Gateway : 192.168.1.1 -

DHCP Pool : Lan2 -

Network : 11.0.0.0 /24 -

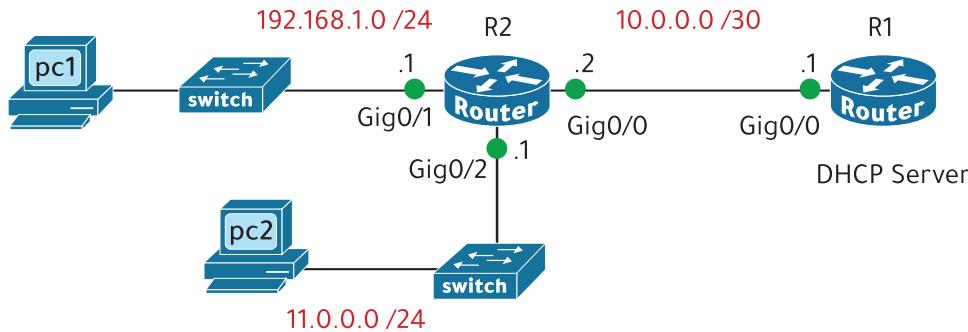
Default Gateway : 11.0.0.1 -

- عمل استثناء لعنوان البوابة الافتراضية حتى لا يتم توزيعه على الاجهزة

Exclude the default gateway address from the pool

### مراحل الحل :

- 1 تطبيق الإعدادات الأساسية .
- 2 تطبيق اعدادات بروتوكول ospf للربط بين الاجهزة
- 3 عمل استثناء لليهات الخاصة مثل ايي البوابة الافتراضية .
- 4 تطبيق اعدادات بروتوكول DHCP
- 5 تطبيق أمر DHCP Relay على R2
- 6 الدخول على الحاسب واختيار اعداد DHCP حتى يحصل على عنوان من الموزع لليهات



تطبيق بروتوكول ospf

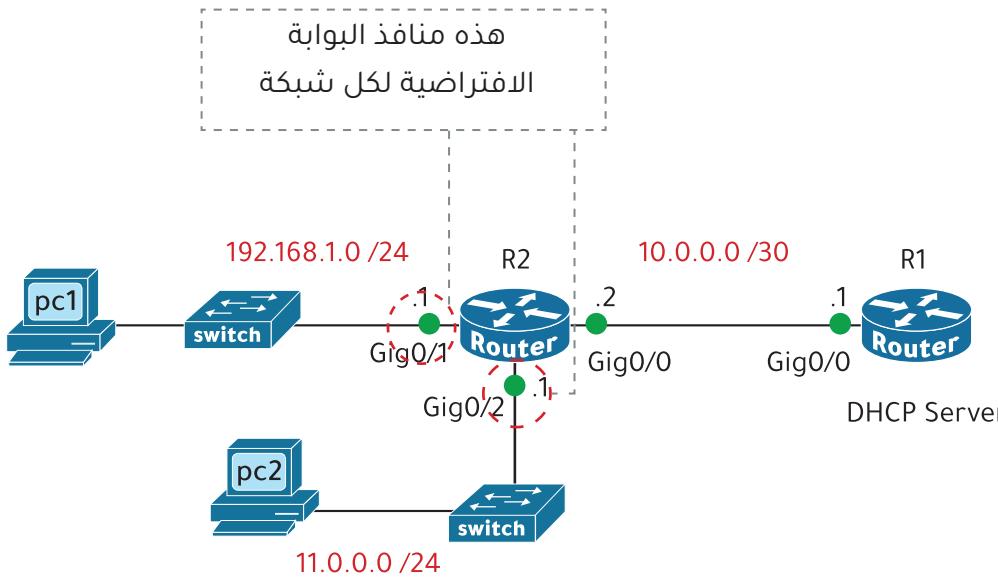
اوامر استثناء أيهات البوابة الافتراضية  
للسبيكتين لأننا لا نريد توزيعها

هذا الـ pool الخاص بالشبكة الاولى 192.168.1.0

هذا الـ pool الخاص بالشبكة الثانية 11.0.0.0

```

R1(config)# int Gig0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 10.0.0.1 255.255.255.252
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 10.0.0.0 0.0.0.3 area 0
R1(config)# ip dhcp excluded-address 192.168.1.1
R1(config)# ip dhcp excluded-address 11.0.0.1
R1(config)# ip dhcp pool LAN1
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# exit
R1(config)# ip dhcp pool LAN2
R1(dhcp-config)# network 11.0.0.0 255.255.255.0
R1(dhcp-config)# default-router 11.0.0.1
R1(dhcp-config)# exit
  
```



تم اضافة هذا الامر الى المنفذ الذي يحتوي على ايبي البوابة الافتراضية للشبكة . لكي يتواصل R2 مع ال DHCP Server لكي يحصل مرسى الرسالة على ايبي .

```

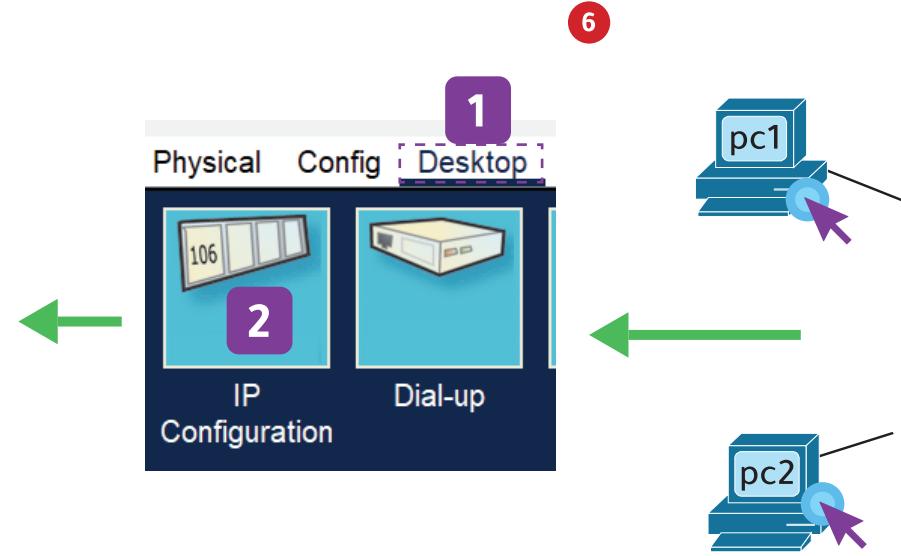
R2
R2(config)# int Gig0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 10.0.0.2 255.255.255.252
R2(config-if)# exit
R2(config)# int Gig0/1
R2(config-if)# no shutdown
R2(config-if)# ip add 192.168.1.1 255.255.255.0
R2(config-if)# exit
R2(config)# int Gig0/2
R2(config-if)# no shutdown
R2(config-if)# ip add 11.0.0.1 255.255.255.0
R2(config-if)# exit
R2(config)# router ospf 1
R2(config-router)# network 10.0.0.0 0.0.0.3 area 0
R2(config-router)# network 11.0.0.0 0.0.0.255 area 0
R2(config-router)# network 192.168.1.0 0.0.0.255 area 0
R2(config-router)# exit
R2(config)# int Gig0/1
R2(config-if)# ip helper-address 10.0.0.1
R2(config)# int Gig0/2
R2(config-if)# ip helper-address 10.0.0.1
R2(config-if)# exit

```

IP Configuration		DHCP request successful
<b>3</b>	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.1.2	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.1	
DNS Server	0.0.0.0	

IP Configuration		DHCP request successful
<b>3</b>	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	11.0.0.2	
Subnet Mask	255.255.255.0	
Default Gateway	11.0.0.1	
DNS Server	0.0.0.0	



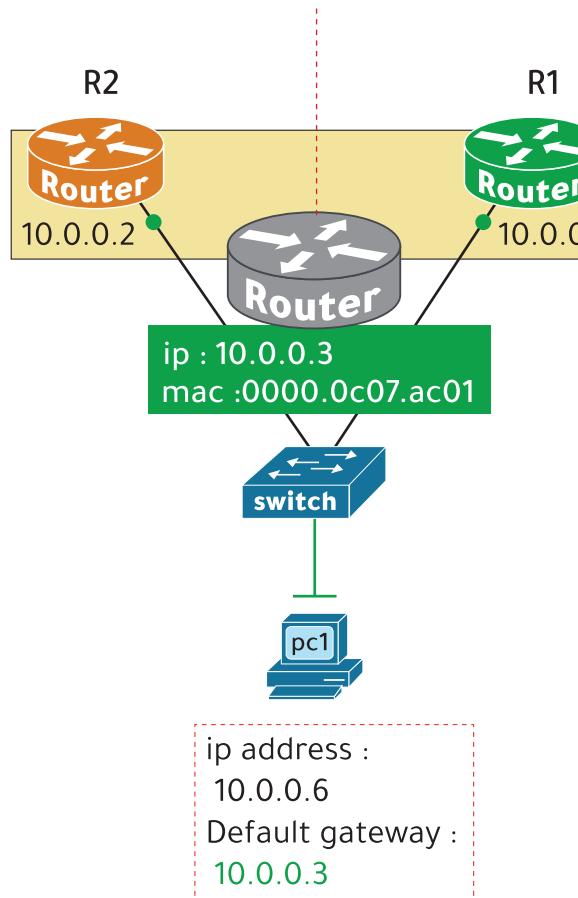
ُشبّه البروتوكول بمثيل هذا الراوتر الوهمي الذي له عنوان IP من نفس مدى الشبكة وماك ادرس خاص ، ايضاً هذا البروتوكول جعل R1 هو الرئيسي (Standby) و R2 الاحتياطي (Active)

## First Hop Redundancy Protocols

**FHRP**

مثلاً لو كان لدينا راوتران أحدهما رئيسي والآخر احتياطي وتعطل أحدهما فسوف يكون هناك انقطاع في الخدمة ولكن مع بروتوكولات FHRP لن يكون هناك انقطاع في الخدمة بل سوف يعمل الراوتر الاحتياطي مباشرةً .

- فكرة هذه البروتوكولات أنها تنشئ راوتر وهمي لمجموعة راوترات ويكون له ايبي وهمي وايضاً ماك ادرس وهمي ووظيفته هو عدم توقف الشبكة عن العمل في حال حدث انقطاع أو فصل لأحد الراوترات الموجودة في الشبكة .



:بروتوكولات هي First Hop Redundancy Protocols

Hot Standby Router Protocol (HSRP) - 1

Virtual Router Redundancy Protocol (VRRP) - 2

Gateway Load Balancing Protocol (GLBP) - 3

**الإصدار الثاني HSRP version 2**

- يعمل مع عناوين الإصدار الرابع IPv4 و الإصدار السادس IPv6
- في الإصدار الرابع IPv4 يستخدم IP 224.0.0.102 كعنوان بث متعدد (multicast address) لكي يرسل رسائل الـ hello.
- في الإصدار السادس IPv6 يستخدم FF02::66 كعنوان بث متعدد (multicast address) لكي يرسل رسائل الـ hello.
- يمكن إنشاء مجموعات (Groups) من 0 - 4095
- الماك أدرس الخاص به يكون مثل هذا : 0000-0C9F-FXXX

**معرف البائع : سيسكو**  
Vendor id (OUI): Cisco

**0000-0c9f-fXXX**

رقم البروتوكول  
HSRP ID

**رقم المجموعة**  
Group Number

**Hot Standby Router Protocol (HSRP) ◆1**

- تم إنشاءه بواسطة شركة سيسكو ويعمل على أجهزتها فقط .
- يستخدم بروتوكول UDP وبورت رقم 1985 .
- يتم إنشاء مجموعة (Group) ولها رقم أثناء الأعدادات ويكون داخل هذه المجموعة : راوتر رئيسي (Active) وراوتر احتياطي (Standby) .
- تبادل الراوترات داخل المجموعة رسائل الـ hello كل 3 ثواني .
- **hold time** : هو مقدار الوقت الذي ينتظره الراوتر الاحتياطي في حالة عدم استلامه رسالة hello من الراوتر الرئيسي لكي يعلن تعطل الراوتر الرئيسي والوقت هو 10 ثواني .
- يمكن إعداد الـ HSRP لكل فيلان ، فمثلاً فيلان 1 يكون R1 رئيسي و R2 احتياطي وفي فيلان 2 يكون R1 احتياطي و R2 رئيسي

**# له إصدارين :****الإصدار الأول HSRP version 1 (افتراضي)**

- يعمل مع عناوين الإصدار الرابع IPv4 .
- في الإصدار الرابع IPv4 يستخدم IP 224.0.0.2 كعنوان بث متعدد (multicast address) لكي يرسل رسائل الـ hello .
- يمكن إنشاء مجموعات (Groups) من 0 - 255 .
- الماك أدرس الخاص به يكون مثل هذا 0000-0C07-ACXX

**معرف البائع : سيسكو**  
Vendor id (OUI): Cisco

**0000-0c07-acXX**

رقم البروتوكول  
HSRP ID

**رقم المجموعة**  
Group Number

- يتم اختيار جهاز رئيسي يسمى (AVG)
- يتم تعين عدد 4 أجهزة احتياطية تسمى:
  - Active Virtual Forwarder (AVF)
- يعمل كل AVF كبوابة افتراضية لكل جزء من الاجهزه في الشبكة ، يعني كل مجموعة أجهزة في نفس الشبكة يكون لها AVF خاص بها ويعمل كبوابة افتراضية .
- في الإصدار الرابع IPv4 يستخدم عناوين بث متعدد (multicast address) لكي يرسل رسائل الـ hello.
- الماك ادرس الخاص به يكون مثل هذا 0007-b400-XXYY



FHRP	المسمى Terminology	الإرسال المتعدد Multicast IP	الماك الافتراضي Virtual MAC	المُلكية
HSRP	Active / Standby	v1: 224.0.0.2 V2: 224.0.0.102	v1: 0000.0c07.acXX v2: 0000.0c9f.fXXX	سيسكو
VRRP	Master / Backup	224.0.0.18	0000.5e00.01XX	مفتوح
GLBP	AVG / AVF	224.0.0.102	0007.b400.XXYY	سيسكو

## Virtual Router Redundancy Protocol (VRRP) ◆2

- هذا البروتوكول يتتطابق تقريبا في الوظائف مع HSRP ولكن مع اختلافات بسيطة :
- المعيار مفتوح يمكن استخدامه لكل الشركات .
- يستخدم UDP بورت رقم 112 .
- يستخدم في الارسال المتعدد (multicast) في ipv4 عناوين 224.0.0.18 لكي يرسل رسائل الـ hello .
- المالك ادرس الخاص به يكون مثل هذا 0000-5e00-01XX
- يتم إنشاء مجموعة (Group) ولها رقم أثناء العددات ويكون داخل هذه المجموعة : راوتر رئيسي يسمى (Master) وراوتر احتياطي يسمى (Backup) .

رقم المجموعة  
Group Number

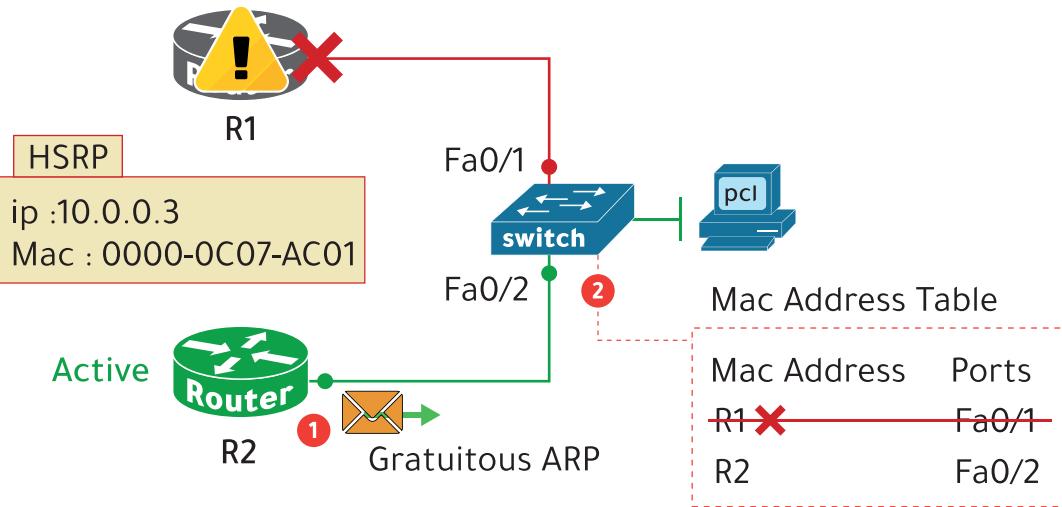
0000-5e00-01XX

## Gateway Load Balancing Protocol (GLBP) ◆3

- تم إنشائه بواسطة شركة سيسكو ويعمل على أجهزتها فقط .
- يستخدم UDP بورت رقم 3222
- يستطيع توزيع الأحمال بين أجهزة التوجيه (الراوترات ) داخل شبكة فرعية واحدة .
- # فمثلاً إذا كان كل من pc1 و pc2 في فیلان 1 ، فيمكن لـ pc1 استخدام R1 كبوابة افتراضية و يمكن لـ pc2 استخدام R2 كبوابة افتراضية .

### عند تعطل الراوتر الرئيسي : R1

يبداً الراوتر الاحتياطي R2 مباشرةً بالعمل ويرسل رسالة برودكاست broadcast للكل تسمى Gratuitous ARP يطلب فيها تحديث العنوان والمسار.



### عندما نقوم بتفعيل بروتوكول الـ HSRP على الراوترات :

- يتم انتخاب راوتر رئيسي وراوتر احتياطي حسب هذا الترتيب :
- الذي لديه أعلى قيمة أولوية (priority) سوف يكون هو الـ Active.

القيمة الافتراضية = 100 .

في حال التساوي

- الراوتر الذي لديه أعلى عنوان آيبي (ip address) سوف يكون هو الـ Active.

طريقة اختيار أعلى آيبي بين عنوانين

البداية

172.16.0.0  
✓ 192.168.0.0

9 أكبر من 7

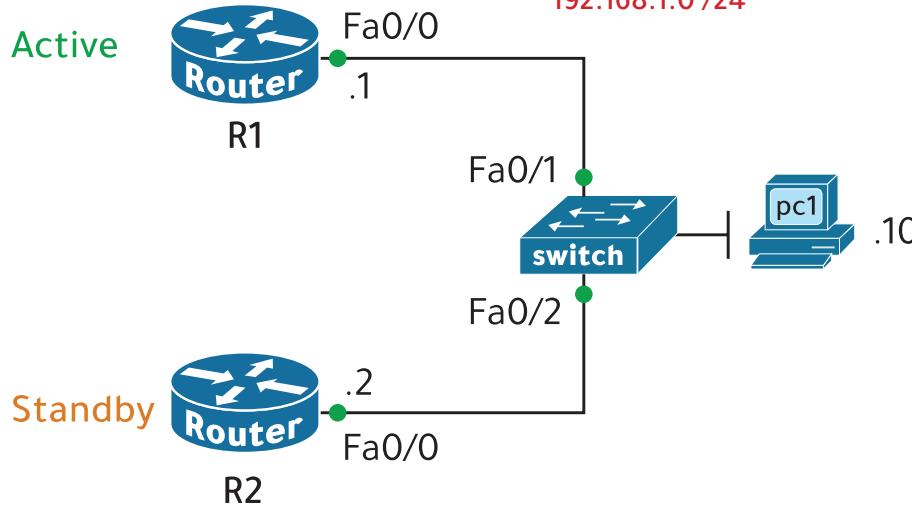
### شرح لأمر بروتوكول HSRP

(group)

R1(config-if)# standby 1 ip 192.168.1.3

الأمر الخاص بالبروتوكول

هنا نضع الآيبي الوهمي  
الخاص ببروتوكول HSRP  
وووضعنا مثلاً انه 192.168.1.3



### مثال :

لدينا هذا النموذج وسوف نطبق عليه بروتوكول : HSRP

HSRP IP : 192.168.1.3  
- الروتر الرئيسي = R1  
- الروتر الاحتياطي = R2

### مراحل الحل :

1 تطبيق الإعدادات الأساسية .

2 تطبيق اعدادات بروتوكول HSRP

```
R1
R1(config)# int Fa0/0
R1(config-if)# no shutdown ①
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# int Fa0/0 ②
R1(config-if)# standby 1 ip 192.168.1.3
R1(config-if)# standby 1 priority 10
R1(config-if)# standby 1 preempt
R1(config-if)# end
R1# wr
```

هذا ايبي الخاص ببروتوكول HSRP  
ويعتبر بوابة افتراضية  
Default Gateway ip

تم تقليل ال priority  
في R2 ليكون احتياطي

: تعني ان الروتر  
يعود رئيسي اذا تم  
اصلاحه

```
R2
R2(config)# int Fa0/0
R2(config-if)# no shutdown ①
R2(config-if)# ip add 192.168.1.2 255.255.255.0
R2(config-if)# exit

R2(config-if)# int Fa0/0 ②
R2(config-if)# standby 1 ip 192.168.1.3
R2(config-if)# standby 1 priority 5
R2(config-if)# end
R2# wr
```

R1

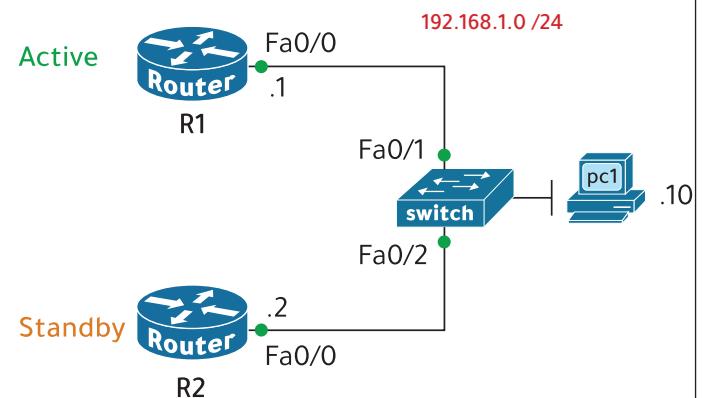
R1# show standby brief

P indicates configured to preempt

المنفذ	رقم المجموعة	قيمة الاولوية	حالة الراوتر R1	عنوان ايبي الراوتر الرئيسي	عنوان ايبي الراوتر الاحتياطي	الايبي الوهمي	
Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	10	P	Active	local	192.168.1.2	192.168.1.3

P : تعني ان هذا الراوتر عليه إعداد preempt وسيعود رئيسي اذا تم اصلاحه

local (محلي) : تعني الراوتر الذي أنا عليه الآن وهو (R1)



R2

R2# show standby brief

P indicates configured to preempt

المنفذ	رقم المجموعة	قيمة الاولوية	حالة الراوتر R1	عنوان ايبي الراوتر الرئيسي	عنوان ايبي الراوتر الاحتياطي	الايبي الوهمي	
Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	5		Standby	192.168.1.1	local	192.168.1.3

```
R1# show standby
```

FastEthernet0/0 - Group 1

State is Active

4 state changes, last state change 00:07:40

Virtual IP address is 192.168.1.3

Active virtual MAC address is 0000.0C07.AC01

Local virtual MAC address is 0000.0C07.AC01 (v1 default)

Hello time 3 sec, hold time 10 sec

Next hello sent in 1.837 secs

Preemption enabled

Active router is local

Standby router is 192.168.1.2

Priority 10 (configured 10)

Group name is hsrp-Fa0/0-1 (default)

رقم القروب

الحالة : Active

الايبي الوهمي

الماك ادرس

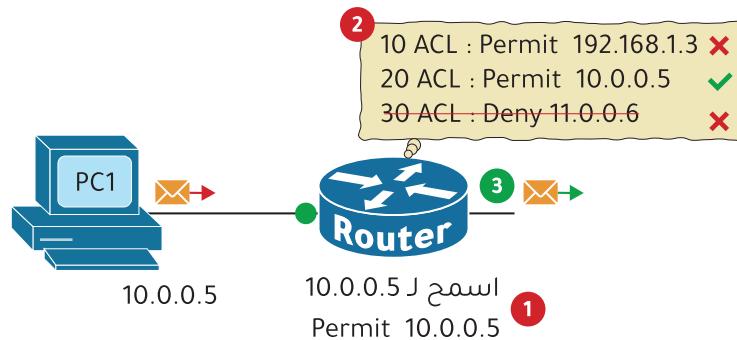
الإصدار الاول وهو الافتراضي

تم تفعيل أمر preempt

عنوان ايبي الراوتر الرئيسي (محلي)

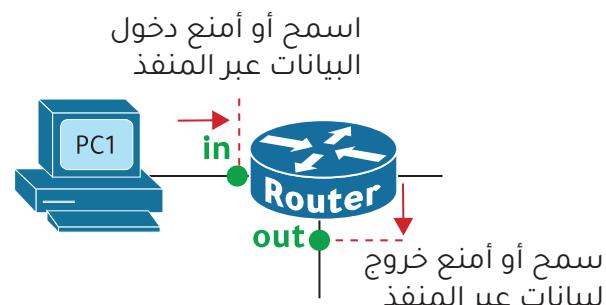
عنوان ايبي الراوتر الاحتياطي

- أول شرط يتتطابق مع الـ ACL سوف يتم تطبيقه ويتجاهل ما بعده .



- بعد إعداد أوامر الـ ACL لابد من تطبيق هذه الأعدادات تحت المنفذ المحدد إما دخول Inbound أو خروج Outbound .

يُسمح لكل منفذ تطبيق أمر دخول in و أمر خروج out **و لا يمكن الجمع بين أمرين دخول + دخول أو خروج + خروج .**  
فلو كتبت أمر دخول جديد على أمر دخول سابق سوف يتم مسح السابق واعتماد الجديد .

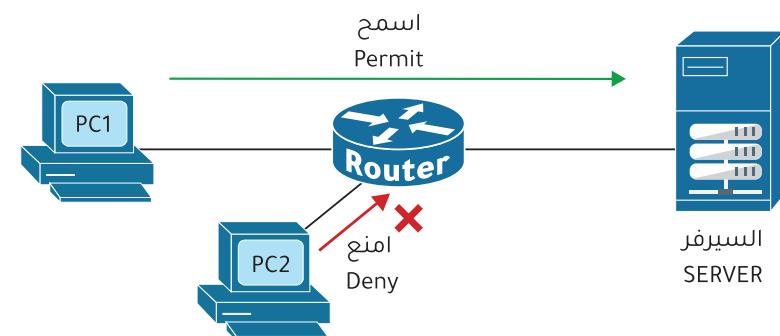


## قواعد التحكم بالوصول (ACL)

### Access Control List (ACL)

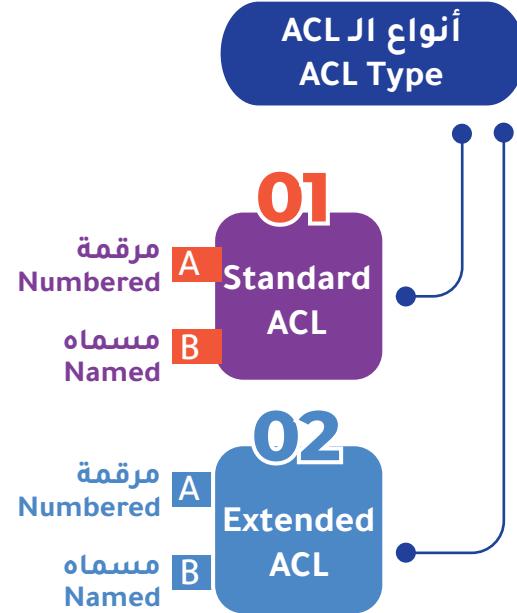
هي أداة تُستخدم لتحديد وفلترة حركة البيانات على أجهزة Cisco حيث يمكن السماح او المنع لحركة البيانات من الوصول الى جهة معينة .  
فمثلاً عند وصول حزمة بيانات الى جهاز الراوتر تستطيع منعها من المرور عبر منفذ محدد .

- الـ ACL تستطيع فلترة حركة البيانات استناداً إلى عناوين الـ IP المصدر والوجهة ، وأيضاً أرقام المنفذ .

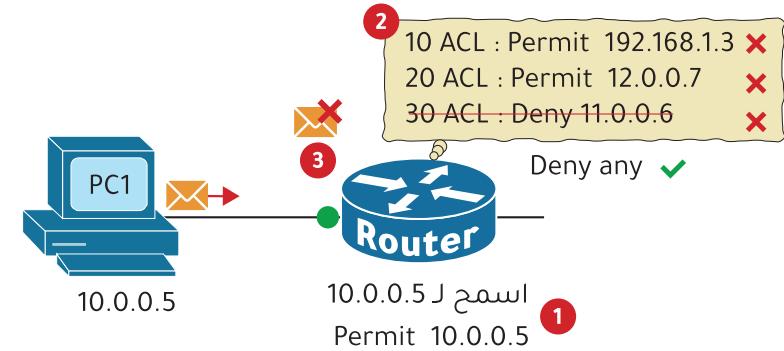


## طريقة إعداد الـ ACL

- يتم إعداد أوامر الـ ACL في وضع التكوين العام (Global config mode) اللي هو ( R1(config) # ). والترتيب مهم جداً . لأن الـ ACL يقوم بترتيب الأوامر برقم تسلسلي بحيث لو وصلت حزمة بيانات سوف يبدأ بالترتيب .



إذا لم يجد الراوتر مطابقة في قائمة الـ ACL فإنه سوف يرفض الحزمة لانه يوجد أمر منع مخفى يسمى بـ implicit Deny يتم اضافته بشكل تلقائي في آخر القائمة .



### : Standard ACL

يتم في هذا النوع فلترة حركة مرور البيانات على أساس عنوان IP المصدر (المرسل ) فقط يفحص جهاز الراوتر عنوان ايبي المرسل فقط ويقرر السماح أو المنع لكل البيانات من هذا الايبي .

**access-list 1 or ACL برقم مثل 1 أو 2 :**  يتم تعريف الـ ACL برقم مثل 1 أو 2 - هذه الأرقام سوف يتعرف عليها الراوتر تلقائيا انها Standard فهي لابد أن تكون من 1 - 99 وإذا انتهت يمكن استخدام من 1300 - 1999

**Named :**  يتم تعريف الـ ACL بكتابة اسم يدل عليه .

## إعدادات الـ Standard ACL



بالطريقة الرقمية

المنع السماح رقم

**R1(config)# access-list number { permit | deny } source\_ip**

أيي المصدر (المرسل )

ملاحظة :

- اي امر يتم اضافته يكون باخر القائمة .

مثال للسماح لايي محدد

```
R1(config)# access-list 4 permit 10.0.0.5
أو
```

```
R1(config)# access-list 4 permit host 10.0.0.5
```

--- مثال للسماح لشبكة 10.0.0.0 /24 كاملة ---

```
R1(config)# access-list 4 permit 10.0.0.0 0.0.0.255
```

نضيف مقلوب او  
(wildcard)

--- مثال للسماح للكل باستخدام any أو بـ wildcard

```
R1(config)# access-list 4 permit any
```

أو

```
R1(config)# access-list 4 permit 0.0.0.0 255.255.255.255
```

## بالطريقة الإسمية

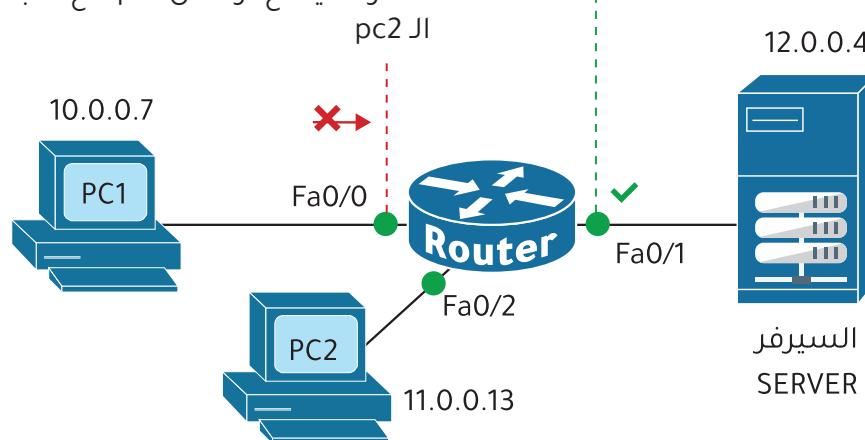
### ملاحظة :

عند إعداد الـ Standard ACL يُفضل تطبيقه على المنفذ الأقرب للوجهه أو المستقبل.

### مثال :

لو أردنا منع PC1 من الوصول للسييرفر فالأفضل وضع تطبيق الـ ACL تحت المنفذ OUT Fa0/1 بوضع .

طبقنا هنا out تحت المنفذ لهه أقرب للوجهه وايضاً يسمح لـ pc2 بالتوالصل مع شبكة الـ PC1



كتابة الاسم  
R1(config)# ip access-list standard **block\_7**  
تكتب هنا الأوامر

### مثال

R1(config)# ip access-list standard **block\_7**  
R1(config-std-nacl)# **permit** 14.0.0.2  
R1(config-std-nacl)# **deny** 13.0.0.0 0.0.0.255

--- توجد في الطريقة الإسمية مميزات أفضل ---

1- تستطيع أن تضيف أمر بين الأوامر برقم تسلسلي

R1(config)# ip access-list standard **block\_7**  
R1(config-std-nacl)# **10 permit** 14.0.0.2

2- تستطيع أن تحذف أمر بواسطة الرقم التسلسلي

R1(config)# ip access-list standard **block\_7**  
R1(config-std-nacl)# **NO 10**

### ملاحظة :

تستطيع حذف اي سطر في الطريقة الإسمية بدون أي ضرر على الـ ACL .

## مثال

لدينا هذا النموذج في برنامج الباكت تريسر وسوف نطبق عليه :

- إعدادات Standard ACL بالطريقتين : الرقمية والاسمية (اختار طريقة واحدة عند التنفيذ )

**الشروط :**

- 1- السماح لـ pc1 بالوصول للسيرفر 1 .
- 2- منع شبكة 10.0.0.0 من الوصول للسيرفر 1 .
- 3- منع pc1 من الوصول الى شبكة pc3
- 4- السماح لشبكة 0.0.0.0 بالوصول لشبكة pc3

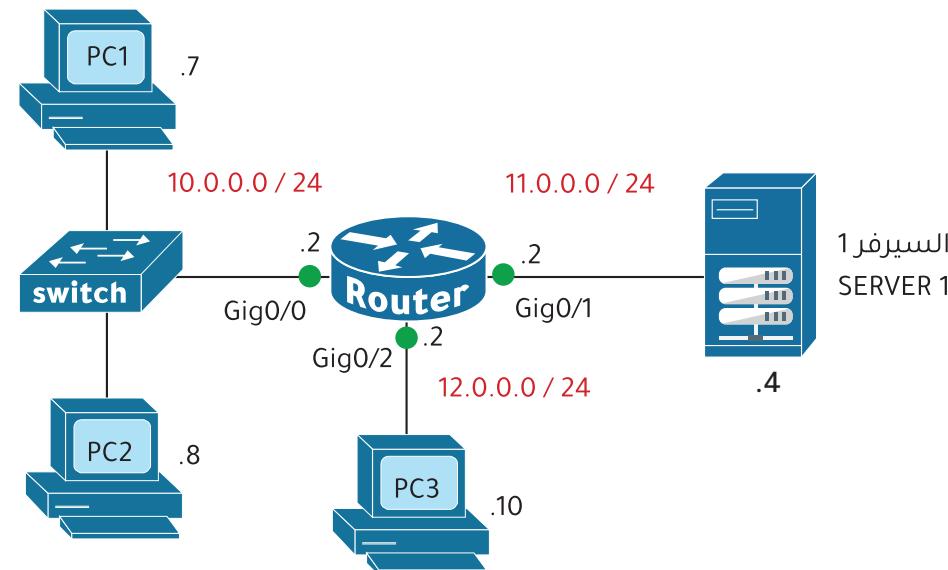
```

R1
R1(config)# int Gig0/0
R1(config-if)# no shutdown ①
R1(config-if)# ip add 10.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

R1(config)# int Gig0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 11.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

R1(config)# int Gig0/2
R1(config-if)# no shutdown
R1(config-if)# ip add 12.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

```



**مراحل الحل :**

- 1- تطبيق الإعدادات الأساسية و ال OSPF للربط بين شبكتين.
- 2- تطبيق JI ACL

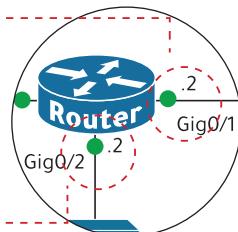
```
R1
R1(config)# access-list 2 permit 10.0.0.7
R1(config)# access-list 3 deny 10.0.0.7
R1(config)# access-list 3 permit 10.0.0.0 0.0.0.255
R1(config)# int Gig0/1
R1(config-if)# ip access-group 2 out
R1(config-if)# exit
R1(config)# int Gig0/2
R1(config-if)# ip access-group 3 out
R1(config-if)# exit
```

**الشرط رقم 1** أمر بالسماح لعنوان pc1 الذي هو 10.0.0.7 وبالوصول للسيرفر 1.

**للحظ** لم نكتب الشرط رقم 2 لأن أمر المنع implicit Deny موجود كافتراضي ومحفي والذي يسمى

**الشرط رقم 3** وهو منع العنوان 10.0.0.7 من الوصول لشبكة pc3 التي هي 12.0.0.0

**الشرط رقم 4** يجب السماح للشبكة 10.0.0.0 كاملة بالوصول إلى شبكة pc3 لأننا لو لم نكتبه سوف يتم تطبيق أمر المنع المحفي .



تم تطبيق الـ ACL تحت المنفذ وفي الموقع الأقرب للوجهه

باستعراض الـ ACL نرى الأوامر  
التي تم تنفيذها

R1

```
R1# show access-lists
```

```
Standard IP access list 2
```

```
10 permit host 10.0.0.7 (4 match(es))
```

```
Standard IP access list 3
```

```
10 deny host 10.0.0.7 (4 match(es))
```

```
20 permit any (4 match(es))
```

**للحظ الأرقام التسلسلية في الـ 2 ACL و في الـ 3 : ACL 2 و في الـ 3**

هذه الأرقام التسلسلية التي يتم المرور عليها بالترتيب في كل الـ ACL .  
- الأرقام تبدأ من الرقم 10 ومعدل الزيادة 10 على كل أمر جديد .

- في الطريقة الرقمية إذا أضفت أمر فإنه يتم إضافته في آخر القائمة .

**مثل** في الـ 3 ACL إذا أضف أمر سوف يتم إضافته في الأخير برقم تسلسلي 30 .

R1

2

```
R1(config)# ip access-list standard block_1
R1(config-std-nacl)# permit 10.0.0.7
R1(config-std-nacl)# exit

R1(config)# ip access-list standard block_2
R1(config-std-nacl)# deny 10.0.0.7
R1(config-std-nacl)# permit 10.0.0.0 0.0.0.255
R1(config-std-nacl)# exit

R1(config)# int Gig0/1
R1(config-if)# ip access-group block_1 out
R1(config-if)# exit

R1(config)# int Gig0/2
R1(config-if)# ip access-group block_2 out
R1(config-if)# exit
```

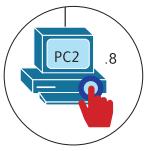
في الطريق الاسمية تضيف  
كلمة ip قبل كلمة access-list

الإسمية

R1

```
R1# show ip access-lists
Standard IP access list block_1
  10 permit host 10.0.0.7 (4 match(es))
Standard IP access list block_2
  10 deny host 10.0.0.7 (4 match(es))
  20 permit 10.0.0.0 0.0.0.255 (4 match(es))
```

هذه أوامر إدخال لـ ACL وتسمى  
Access List Entries (ACE)  
إدخالات قائمة التحكم بالوصول



pc 2

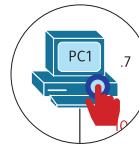
C:\>ping 11.0.0.4

Reply from 10.0.0.2: Destination host unreachable.

Ping statistics for 11.0.0.4:

    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

لا يمكن  
الوصول إليه



pc 1

C:\>ping 11.0.0.4

Reply from 11.0.0.4: bytes=32 time<1ms TTL=127

Reply from 11.0.0.4: bytes=32 time=1ms TTL=127

Reply from 11.0.0.4: bytes=32 time=1ms TTL=127

Reply from 11.0.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 11.0.0.4:

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

نتأكد من الشروط التي تم تنفيذها



pc 1

الشرط 3 : تم منع جهاز pc1 من الوصول  
الى جهاز pc3

لا يمكن  
الوصول إليه



pc 2

C:\>ping 12.0.0.10

Reply from 12.0.0.10: bytes=32 time=10ms TTL=127

Reply from 12.0.0.10: bytes=32 time<1ms TTL=127

Reply from 12.0.0.10: bytes=32 time<1ms TTL=127

Reply from 12.0.0.10: bytes=32 time=1ms TTL=127

Ping statistics for 12.0.0.10:

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

ملاحظة :

- إذا حذفت اي سطر من الطريقة الرقمية مثلا:

```
R1(config)# no access-list 4 permit 10.0.0.5
```

سوف يتم حذف ا JL ACL بشكل كامل .

= نتعرف على الطريقة الصحيحة :

لو مثل أخطأت بكتابة 150 بدلًا من 15 :

15.0.0.0 والصحيح هو 150.0.0.0

```
R1(config)# access-list 2 permit 150.0.0.0
```

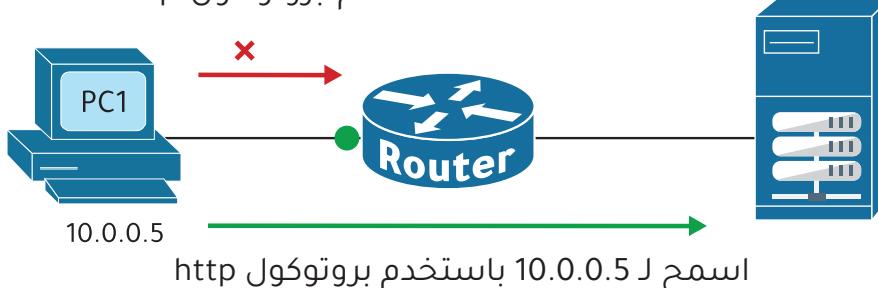
الطريقة الصحيحة بالحذف هي :

```
R1(config)# ip access-list standard 2
```

الحذف -----

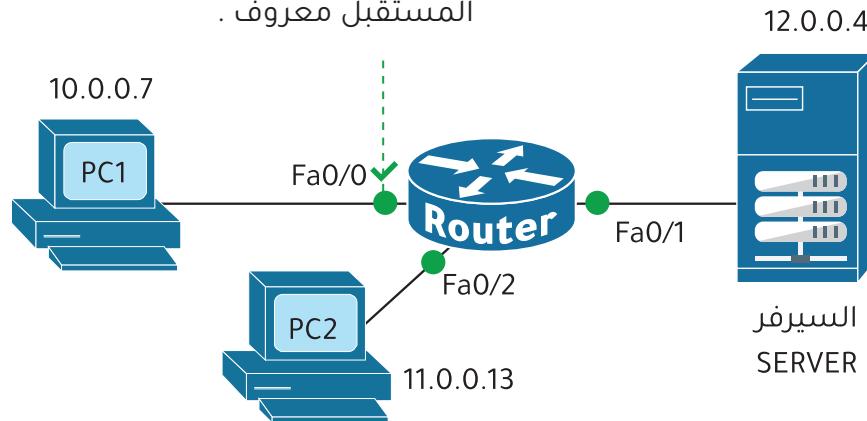
الاضافة والتعديل permit 15.0.0.0 ---

امنع الـ 10.0.0.5 من  
استخدم بروتوكول ftp



**ملاحظة :**  
عند إعداد الـ Extended ACL يُفضل تطبيقه على المنفذ الأقرب للمرسل  
**مثال :**  
لو أردنا منع PC1 من الوصول للسيرفر فالأفضل وضع تطبيق الـ ACL  
تحت المنفذ Fa0/0 بوضع in .

طبقنا هنا in تحت المنفذ لانه  
أقرب للمرسل والسبب لأن عنوان  
المستقبل معروف .



### : Extended ACL

هذا النوع يشبه النوع السابق ولكن أكثر مرونة حيث يتم فلترة حركة  
مرور البيانات على أساس عنوان IP المصدر وعنوان IP الوجهة وأرقام  
المنفذ .

- يفحص جهاز الراوتر عنوان ايبي المصدر وايبي الوجهة واي شروط  
إضافية أخرى وبعدها يقرر السماح أو المنع .
- يمكن في هذا النوع السماح والمنع لبروتوكولات محددة مع مرور  
البيانات الأخرى من نفس الايبي .

- يوجد أمر منع مخفى يسمى بـ implicit Deny يتم اضافته بشكل  
تلقيائي في آخر القائمة .

R1(config)# Deny ip any any

**Numbered - 1** : يتم تعريف الـ ACL برقم مثل 100 أو access-list 102

هذه الأرقام سوف يتعرف عليها الراوتر تلقائياً إنها Extended ACL فهي لابد  
أن تكون من 100 - 199 وإذا انتهت يمكن استخدام من 2000 - 2699  
**مثال :**

R1(config)# access-list 102 permit ip host 10.0.0.5 host 12.0.0.6

**Named - 2** : يتم تعريف الـ ACL بكتابه اسم يدل عليه .

R1(config)# ip access-list extended block\_2

R1(config-ext-nacl)# permit ip host 10.0.0.5 host 12.0.0.6

## إعدادات الـ Extended ACL



R1(config)# access-list number {**permit** | **deny**} ip\_protocol source\_ip destination\_ip protocol\_information

تضع الكلمة host قبل أيبي المرسل اذا كان محدد ، اذا كانت شبكة تضع الوايبلد كارد wildcard مع الايبي

ايبي المستقبل  
(شبكة)

رقم بورت او اسم  
البروتوكول الموجود في  
ايبي المستقبل

R1(config)# access-list 102 **permit** TCP host 10.0.0.6 12.0.0.0 0.0.0.255 eq www

البروتوكول المستخدم

- ip
- ICMP
- TCP**
- UDP
- EIGRP
- OSPF

نضع المقارنة

<b>eq</b>	مطابقة الحزم لرقم البروتوكول
<b>gt</b>	مطابقة الحزم لرقم أكبر من
<b>lt</b>	مطابقة الحزم لرقم أصغر من
<b>neq</b>	مطابقة الحزم لرقم ليساوي
<b>range</b>	مطابقة الحزم للمدى

- ftp
- pop3
- smtp
- telnet
- www**

مثال للسماح لايبي محدد بالوصول لايبي محدد

```
R1(config)# access-list 102 permit ip host 10.0.0.5 host 12.0.0.6
```

مثال لمنع ايبي محدد بالوصول لشبكة كاملة

```
R1(config)# access-list 102 deny ip host 10.0.0.5 12.0.0.0 0.0.0.255
```

مثال لمنع ايبي محدد بالوصول لاي شبكة في الشبكة الكاملة

```
R1(config)# access-list 102 deny ip host 10.0.0.5 any
```

مثال لمنع ايبي محدد في استخدام بروتوكول Http الموجود بالسيرفر 15.0.0.5

```
R1(config)# access-list 102 deny tcp host 10.0.0.5 host 15.0.0.5 eq 80
```

## مثال

لدينا هذا النموذج في برنامج الباكت ترييسروسوف نطبق عليه :

- إعدادات Extended ACL بالطريقتين :

الرقمية والاسمية (ختار طريقة واحدة عند التطبيق )

```

R1

R1(config)# int Gig0/0
R1(config-if)# no shutdown 1
R1(config-if)# ip add 10.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

R1(config)# int Gig0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 11.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

R1(config)# int Gig0/2
R1(config-if)# no shutdown
R1(config-if)# ip add 12.0.0.2 255.255.255.0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

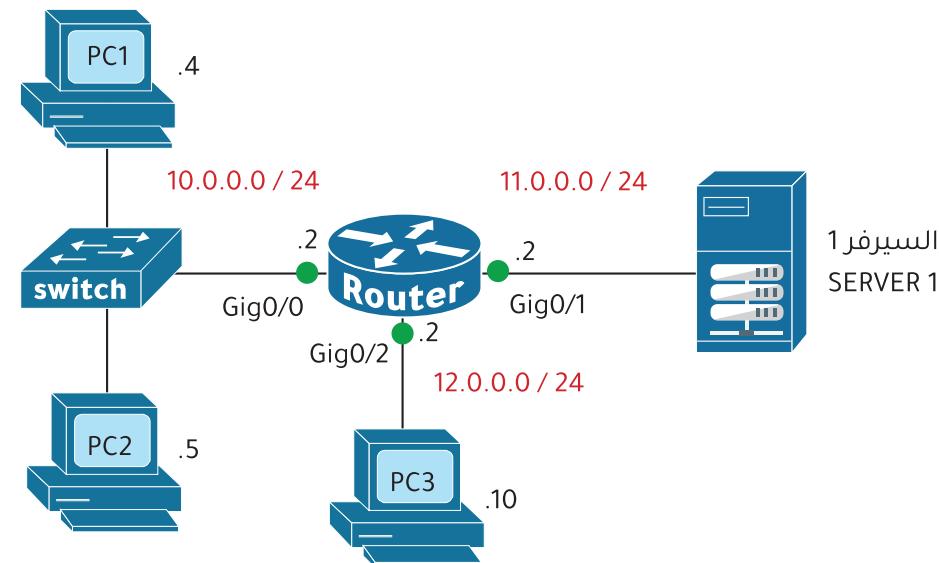
```

**الشروط :**

1 - السماح لـ pc1 باستخدام بروتوكول http عند اتصاله بالسيرفر 1 .

2 - منع شبكة 10.0.0.0 من الوصول للسيرفر 1 .

3 - السماح لشبكة الـ 10.0.0.0 الوصول لشبكة الـ 12.0.0.0 .



**مراحل الحل :**

1 - تطبيق الإعدادات الأساسية و JI OSPF للربط بين شبكتين .

2 - تطبيق JI ACL

## الرقمية

R1

2

```
R1(config)# access-list 105 permit tcp host 10.0.0.4 host 11.0.0.4 eq www
R1(config)# access-list 105 deny ip 10.0.0.0 0.0.0.255 host 11.0.0.4
R1(config)# access-list 105 permit ip 10.0.0.0 0.0.0.255 any

R1(config)# int Gig0/0
R1(config-if)# ip access-group 105 in
R1(config-if)# exit
```

3 - السماح لشبكة  
الـ 10.0.0.0 بالوصول  
لشبكة الـ 12.0.0.0

1 - السماح لـ pc1 باستخدام بروتوكول  
http عند اتصاله بالسيرفر 1.

2 - منع شبكة الـ 10.0.0.0 من الوصول للسيرفر 1.

باستعراض الـ ACL نرى  
الأوامر التي تم تنفيذها

R1

R1# show access-lists

Extended IP access list 105

```
10 permit tcp host 10.0.0.4 host 11.0.0.4 eq www
20 deny ip 10.0.0.0 0.0.0.255 host 11.0.0.4
30 permit ip 10.0.0.0 0.0.0.255 any
```

## الإسمية

R1

2

```
R1(config)# ip access-list extended blk_to_server
R1(config-ext-nacl)# permit tcp host 10.0.0.4 host 11.0.0.4 eq www
R1(config-ext-nacl)# deny ip 10.0.0.0 0.0.0.255 host 11.0.0.4
R1(config-ext-nacl)# permit ip 10.0.0.0 0.0.0.255 any
```

```
R1(config)# int Gig0/0
R1(config-if)# ip access-group blk_to_server in
R1(config-if)# exit
```

باستعراض الـ ACL نرى  
الأوامر التي تم تنفيذها

R1

R1# show access-lists

Extended IP access list blk\_to\_server

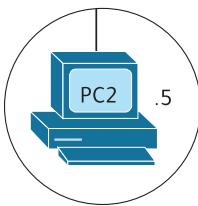
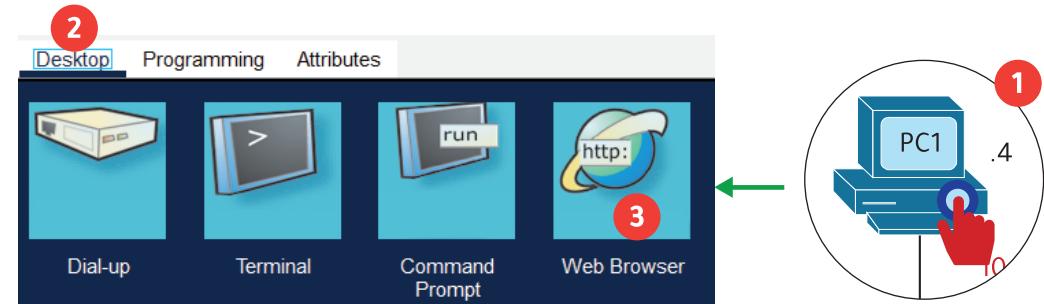
```
10 permit tcp host 10.0.0.4 host 11.0.0.4 eq www
20 deny ip 10.0.0.0 0.0.0.255 host 11.0.0.4
30 permit ip 10.0.0.0 0.0.0.255 any
```

الشرط 1 : تم التصفح تشغيل بروتوكول التصفح http بنجاح ✓



## Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunity.  
Mind Wide Open.

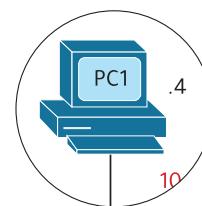


الشرط 2 : منع شبكة 10.0.0.0 من الوصول للسيرفير 1 وذلك بالتجربة من جهاز pc2

```
pc2
C:\>ping 11.0.0.4
Reply from 10.0.0.2: Destination host unreachable.-----
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.
Reply from 10.0.0.2: Destination host unreachable.

Ping statistics for 11.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

لا يمكن  
الوصول إليه



الشرط 3 : يوجد اتصال بين شبكة 10.0.0.0 الى شبكة الـ 12.0.0.0 بواسطة جهاز pc1

```
pc1
C:\>ping 12.0.0.10
Reply from 12.0.0.10: bytes=32 time<1ms TTL=127
Reply from 12.0.0.10: bytes=32 time=1ms TTL=127
Reply from 12.0.0.10: bytes=32 time=2ms TTL=127
Reply from 12.0.0.10: bytes=32 time=1ms TTL=127

Ping statistics for 12.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

## بروتوكول إن NAT

### أنواع بروتوكول NAT

#### Static NAT (One To One) 01

هو ان يكون لكل عنوان ايبي محلي عنوان ايبي عام مرتبط به .



### Network Address Translation (NAT)

لكي تصل بالانترنت لابد من وجود عنوان ايبي عام public IP تستطيع الخروج به الى الانترنت ، فكرة بروتوكول إن NAT هو السماح للأجهزة المحلية التي لها عناوين خاصة بالوصول إلى الإنترت من خلال عنوان ايبي عام .

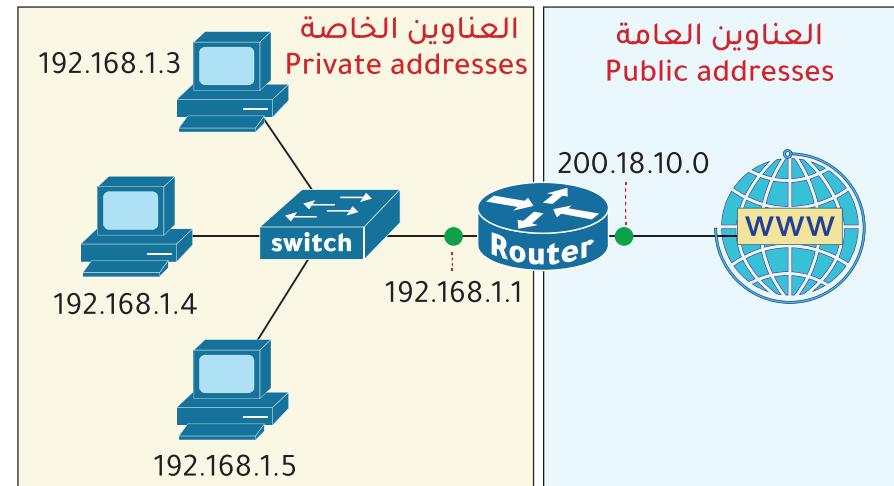
**أسماء العناوين في بروتوكول إن NAT :**

#### - العناوين الخاصة

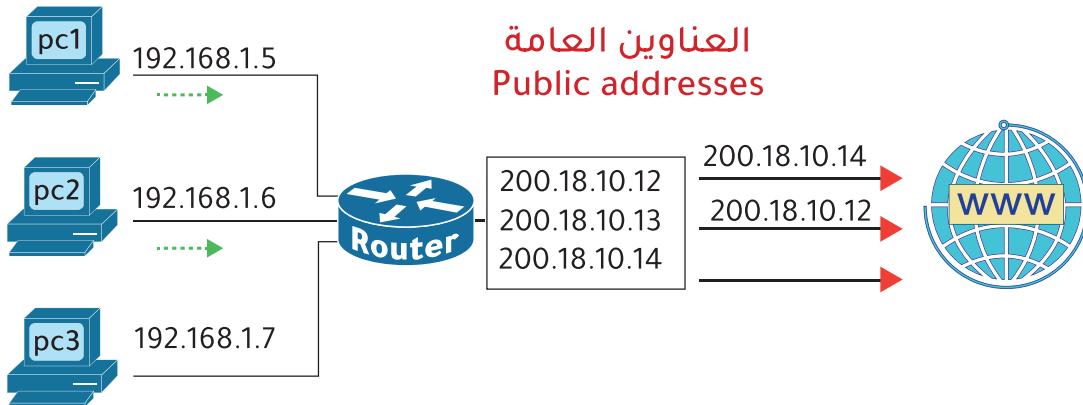
يطلق عليها أيضا Local Address وهي العناوين التي تكون في شبكة محلية ولا يمكن لها الخروج للاتصال بالانترنت الا عن طريق عنوان عام Public address .

#### - العناوين العامة

يطلق عليها أيضا Global Address وهي العناوين التي يتم شراءها من مزود الخدمة ليتم الخروج بها للاتصال بالانترنت .



### العناوين الخاصة Private addresses



### Dynamic NAT (Group To Group) 02

هو أن يكون لكل مجموعة عناوين محلية مجموعة عناوين عامة.

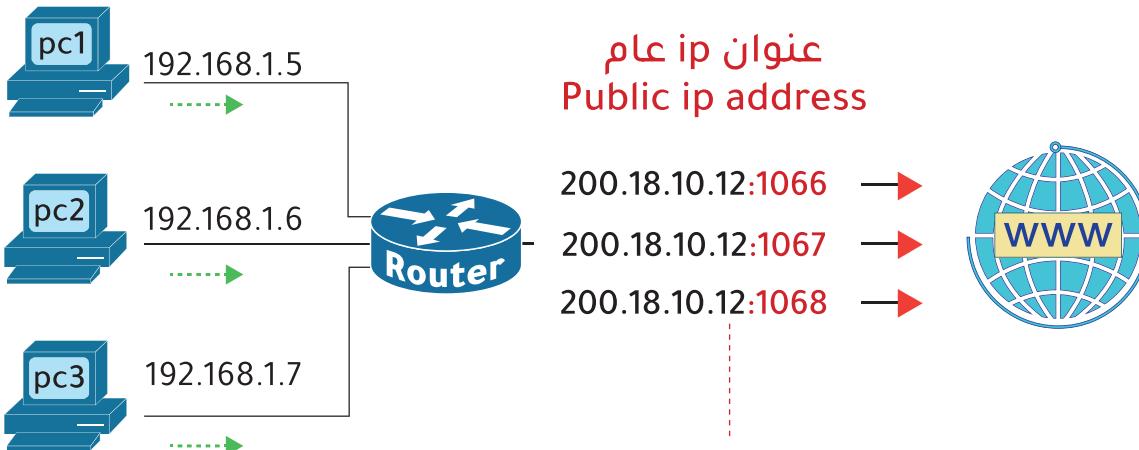
- فمثلاً لو لدينا 3 عناوين عامة، وعندنا ثلاثة أجهزة محلية تريد الوصول للإنترنت فسوف يحصلون على ثلاثة عناوين عامة.

لكن لو أراد جهاز رابع الوصول للإنترنت فلن يستطيع حتى يتوقف أحد الأجهزة الـ 3 عن الاستخدام لكي يكون له عنوان عام متاح له.

هذا النوع مكلف لأنه يتطلب من الشركة شراء العديد من عناوين IP العامة.

- استخدامه قليل جداً.

### العناوين الخاصة Private addresses



### Port Address Translation (PAT) 03

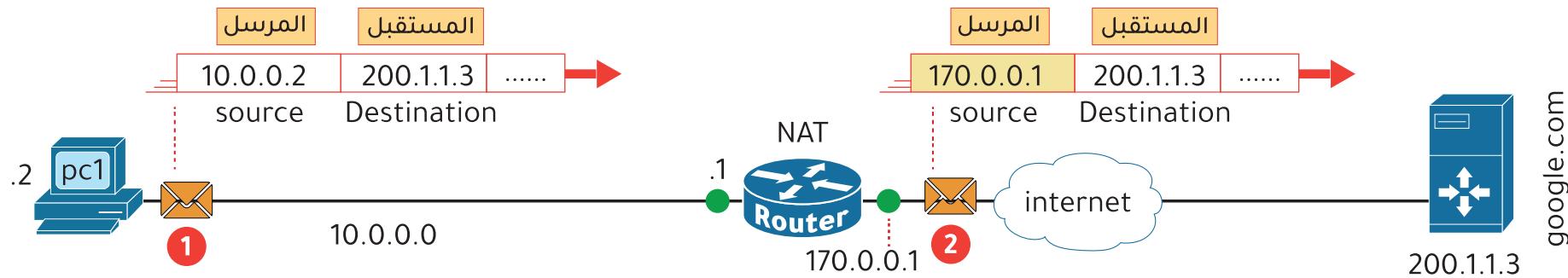
يسمى أيضاً باسم NAT Overloading وهو أن يكون عنوان عام واحد فقط لكل العناوين المحلية.

- يتم التفريق بينهم باستخدام IP TCP/UDP port number.

- هذا النوع أكثر الانواع استخداماً وأفضلها لأنه مناسب من حيث التكلفة وايضاً يمكن توصيلآلاف المستخدمين بالإنترنت باستخدام عنوان IP عام واحد فقط.

للحظ هنا يوجد عنوان عام IP public واحد فقط ولكن هذا النوع يضيف رقم بورت للايبي العام.

## # كيف يعمل بروتوكول الـ NAT

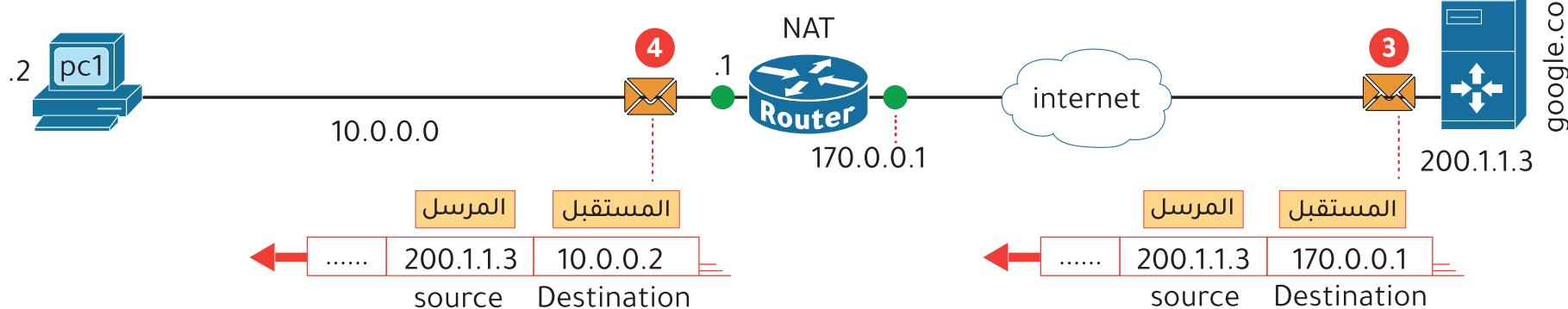


1 - يرسل pc1 رسالة طلب ، يوجد فيها عنوانه وعنوان المستقبل google.com مثلًا

2 - توصل الرسالة للراوتر فيقوم باستبدال عنوان الـ pc1 بالعنوان العام public IP ويكملا بارسال الرسالة

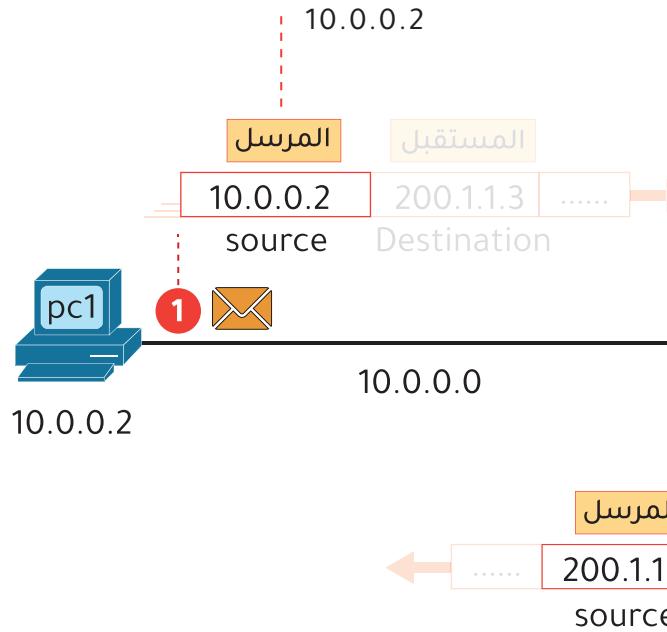
4 - توصل الرسالة للراوتر فيقوم باستبدال عنوان المستقبل بعنوان أيبي pc1

3 - يتم الرد عليه من المستقبل برسالة فيها عنوانه وعنوان الراوتر الذي استقبل منه الرسالة



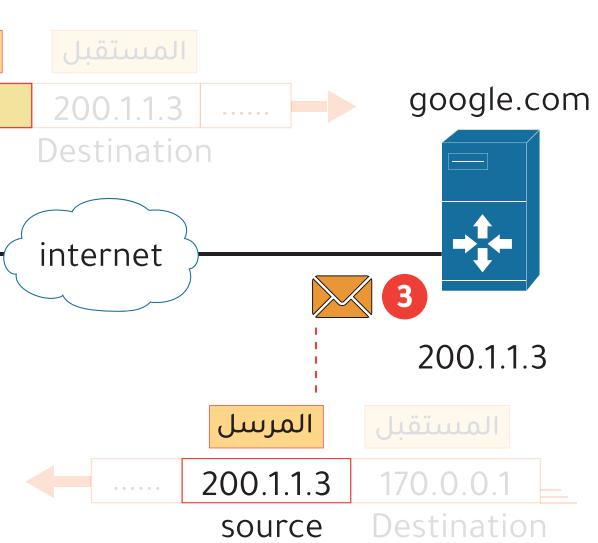
## # بعض المسميات في بروتوكول الـ NAT

**Inside local**  
هو عنوان الجهاز الموجود في الشبكة المحلية مثل هذا الجهاز اللي عنوانه

**Inside Global**

هو عنوان الابي العام الذي يخرج بك للانترنت بعد تنفيذ عملية الـ Nat . مثل الموجود بهذا الراوتر

**outside Local**  
هو عنوان الجهاز الخارجي والذي يكون ظاهرا عندك في الشبكة المحلية . مثل الموجود بالاعلى اللي هو 200.1.1.3

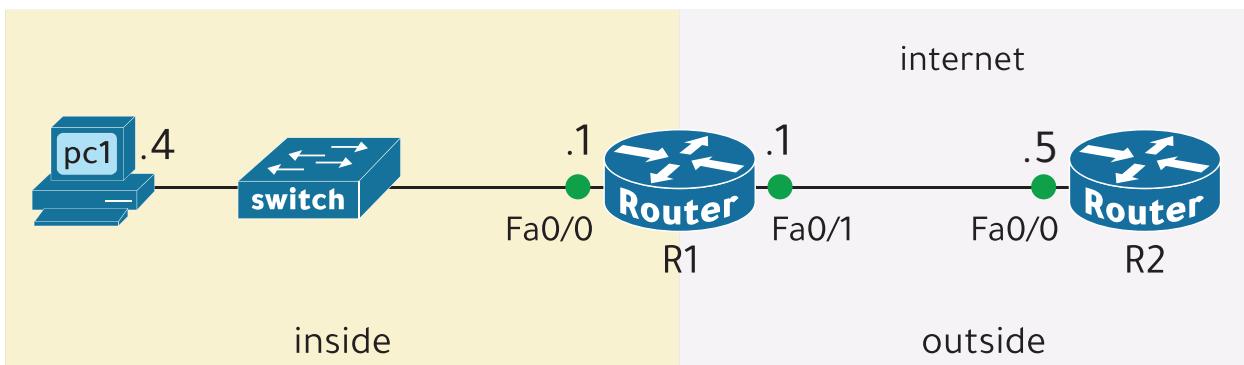
**Outside Global**

هو عنوان الجهاز الخارجي والذي يكون عنوانه معروفا في شبكة الانترنت

192.168.1.0 /24

5.0.0.0 /24

## إعدادات بروتوكول NAT



## Static NAT 1

سوف نطبق النوع الاول على هذا النموذج  
- العنوان العام 5.0.0.1

## مراحل الحل :

```
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# int Fa0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 5.0.0.1 255.255.255.0
R1(config-if)# exit
```

1

```
R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 5.0.0.5 255.255.255.0
R2(config-if)# exit
```

1

تطبيق الاعدادات الاساسية . 1

تطبيق اعدادات بروتوكول NAT : 2

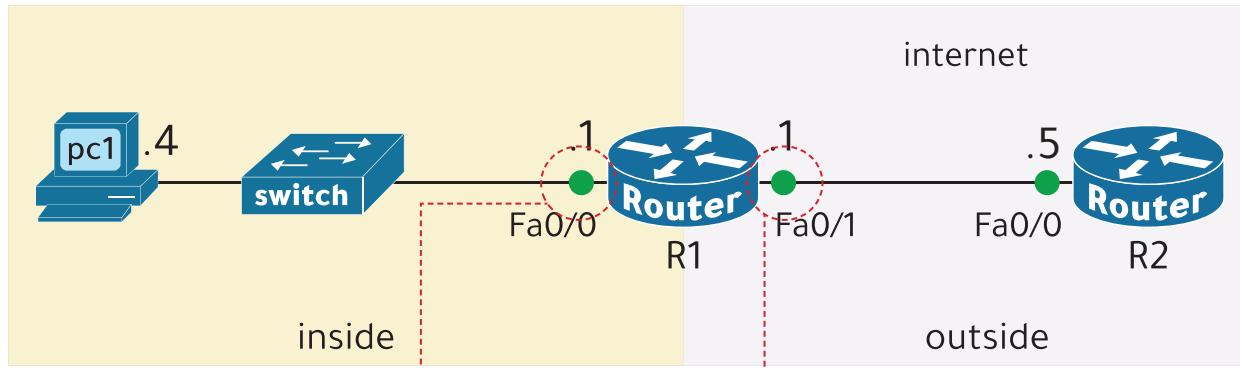
تعيين المنافذ outside g inside a

تطبيق إعداد static nat b

اختبار الاتصال بعمل ping بين R2 و pc1 3

192.168.1.0 /24

5.0.0.0 /24



نضيف امر inside لمنفذ البوابة الافتراضية (Default Gateway) للشبكة الداخلية لأن هذا المنفذ واقع داخل الشبكة الداخلية المحلية

نضيف امر outside لمنفذ البوابة الافتراضية (Default Gateway) للشبكة الخارجية لأن هذا المنفذ هو المنفذ الخارج من الراوتر والذي يصل بالانترنت

```
R1
R1(config)# int Fa0/0
R1(config-if)# ip nat inside
R1(config-if)# exit
R1(config)# int Fa0/1
R1(config-if)# ip nat outside
R1(config-if)# exit
```

2 a

2 b

```
R1
R1(config)# ip nat inside source static 192.168.1.4 5.0.0.1
```

ربط الايبي المحلي بالعام  
حيث نجعل ايبي PC1 يخرج عبر الايبي العام 5.0.0.1

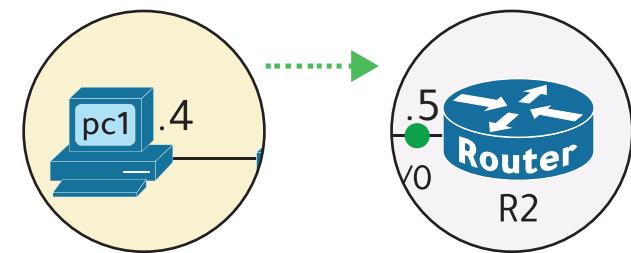
هذا أمر بروتوكول NAT

هذا نوع البروتوكول NAT

ثم نستعرض جدول بروتوكول الـ nat في R1

R1				
Pro	Inside global	Inside local	Outside local	Outside global
icmp	5.0.0.1:1	192.168.1.4:1	5.0.0.5:1	5.0.0.5:1
icmp	5.0.0.1:2	192.168.1.4:2	5.0.0.5:2	5.0.0.5:2
icmp	5.0.0.1:3	192.168.1.4:3	5.0.0.5:3	5.0.0.5:3
icmp	5.0.0.1:4	192.168.1.4:4	5.0.0.5:4	5.0.0.5:4
-----	5.0.0.1	192.168.1.4	-----	-----

نعمل ping من جهاز pc1 الى R2 (5.0.0.5) ③



. pro : تعني البروتوكول المستخدم .

### icmp هو بروتوكول رسائل التحكم في الإنترنت :

ينتمي الى بروتوكولات الطبقة الثالثة Network في الـ Osi Model و هو احده اكثربروتوكولات استخداماً لفحص الشبكة ولتحديد ما إذا كانت البيانات تصل إلى وجهتها المقصودة في الوقت المناسب أم لا .

- من الادوات المستخدمة داخل البروتوكول :

#### 1 - أداة Ping

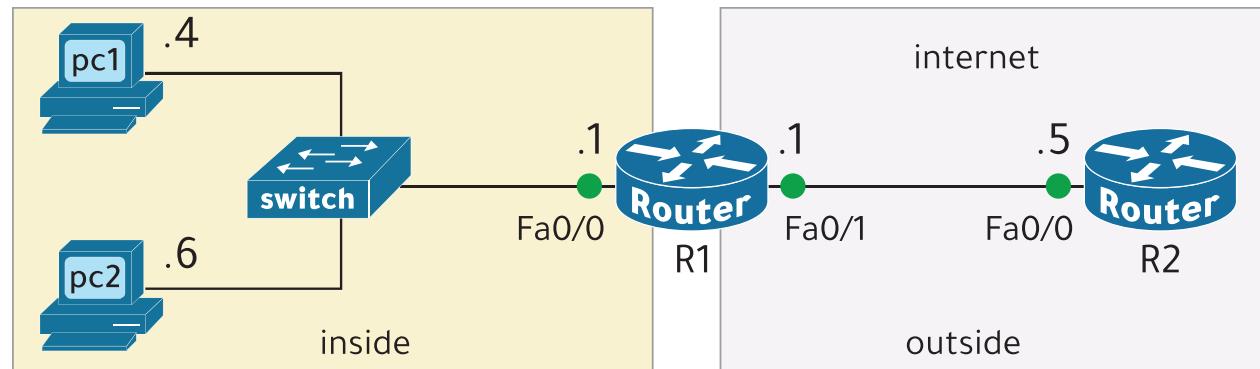
تحتير الاتصال وسرعة الاتصال بين جهازين واظهار المدة التي تستغرقها حزمة البيانات للوصول إلى وجهتها والعودة إلى جهاز المرسل

#### 2 - أداة Traceroute

تُستخدم لعرض مسار التوجيه بين جهازي إنترنت ، بمعنى انها توضح لك الايبيات المضافة للمنفذ والتي عبرت من خلالها حتى الوصول الى الوجهه .

## Dynamic NAT 2

سوف نطبق النوع الثاني على هذا النموذج  
- العناوين العامة من 5.0.0.3 الى 5.0.0.6



### مراحل الحل :

```
R1
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# int Fa0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 5.0.0.1 255.255.255.0
R1(config-if)# exit
```

```
R2
R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 5.0.0.5 255.255.255.0
R2(config-if)# exit
```

```
R1
R1(config)# int Fa0/0
R1(config-if)# ip nat inside
R1(config-if)# exit

R1(config)# int Fa0/1
R1(config-if)# ip nat outside
R1(config-if)# exit
```

1 - تطبيق الإعدادات الأساسية .

2 - تطبيق اعدادات بروتوكول NAT :

a - تعيين المنافذ و inside و outside

b - تطبيق إعداد Dynamic nat

● إنشاء Pool (مخزن) يحتوي على عناوين الشبكة المحلية .

● إنشاء قائمة دخول access list

● ربط الـ access list بالـ pool

3 - اختبار الاتصال بعمل ping بين R2 و pc1

تم إنشاء Pool (مخزن)  
وتسميته بـ Sales

نكتب العناوين العامة التي من 5.0.0.3 الى 5.0.0.6  
مع قناع الشبكة 5.0.0.6

R1

```
R1(config)# ip nat pool Sales 5.0.0.3 5.0.0.6 netmask 255.255.255.0
```

```
R1(config)# access-list 20 permit 192.168.1.0 0.0.0.255
```

```
R1(config)# ip nat inside source list 20 pool Sales
```

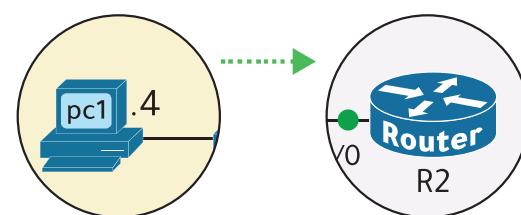
② b

لشبكة wildcard mask  
192.168.1.0 / 24

تم إنشاء قائمة دخول وإعطائها رقم 20  
: السماح لهذه الشبكة في هذه القائمة

أمر بروتوكول الـ  
access list باستخدام القائمة  
pool وربطها بالـ list

③ نعمل ping من جهاز pc1 و جهاز pc2 الى R2  
(5.0.0.5)



R1

```
R1# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	5.0.0.4:13	192.168.1.4:13	5.0.0.5:13	5.0.0.5:13
icmp	5.0.0.4:14	192.168.1.4:14	5.0.0.5:14	5.0.0.5:14
icmp	5.0.0.4:15	192.168.1.4:15	5.0.0.5:15	5.0.0.5:15
icmp	5.0.0.5:13	192.168.1.6:13	5.0.0.5:13	5.0.0.5:13
icmp	5.0.0.5:14	192.168.1.6:14	5.0.0.5:14	5.0.0.5:14
icmp	5.0.0.5:15	192.168.1.6:15	5.0.0.5:15	5.0.0.5:15

نستعرض جدول بروتوكول الـ nat في R1

C:\> ping 5.0.0.5

Pinging 5.0.0.5 with 32 bytes of data:

Reply from 5.0.0.5: bytes=32 time<1ms TTL=126

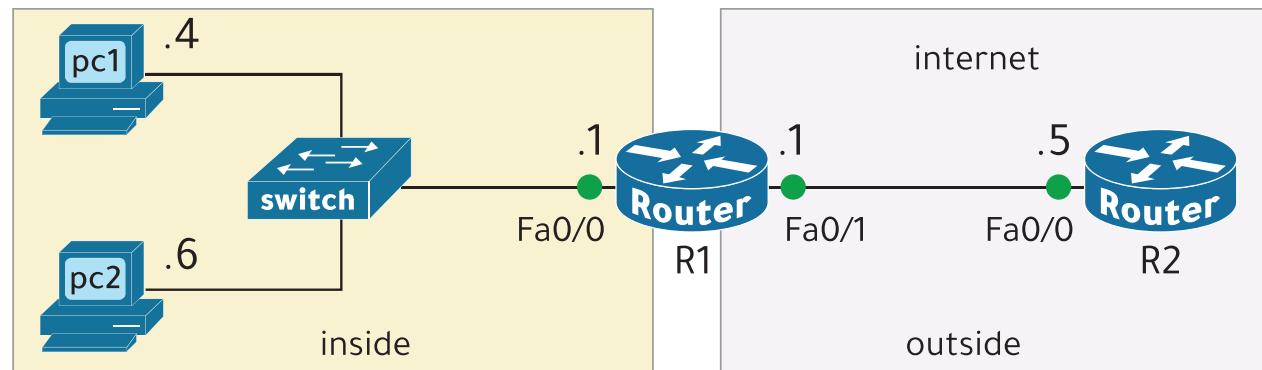
Reply from 5.0.0.5: bytes=32 time<1ms TTL=126

Reply from 5.0.0.5: bytes=32 time=2ms TTL=126

Reply from 5.0.0.5: bytes=32 time<1ms TTL=126

Ping statistics for 5.0.0.5:

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



### PAT NAT 3

سوف نطبق النوع الثالث على هذا النموذج

- العنوان العام 5.0.0.1

**مراحل الحل :**

1 - تطبيق الإعدادات الأساسية .

2 - تطبيق اعدادات بروتوكول NAT :

a - تعين المنفذ outside و inside a

b - تطبيق إعداد PAT NAT :

إنشاء قائمة دخول access list ●

● استخدام القائمة access list وربطها بالمنفذ

3 - اختبار الاتصال بعمل ping بين R2 و pc1

**R1**

```
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# int Fa0/1
R1(config-if)# no shutdown
R1(config-if)# ip add 5.0.0.1 255.255.255.0
R1(config-if)# exit
```

1

**R2**

```
R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 5.0.0.5 255.255.255.0
R2(config-if)# exit
```

1

**R1**

```
R1(config)# int Fa0/0
R1(config-if)# ip nat inside
R1(config-if)# exit

R1(config)# int Fa0/1
R1(config-if)# ip nat outside
R1(config-if)# exit
```

2 a

تم إنشاء قائمة دخول وإعطائها

رقم 10

: السماح لهذه الشبكة

في هذه القائمة

R1  
R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255  
R1(config)# ip nat inside source list 10 interface fa0/1 overload

b  
لشبكة wildcard mask  
192.168.1.0 / 24

أمر بروتوكول الـ nat باستخدام  
القائمة list وربطها بالمنفذ

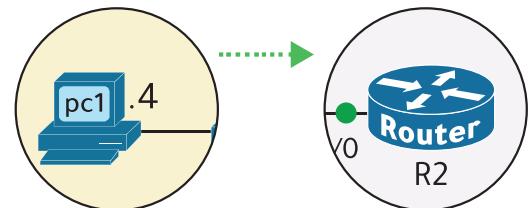
overload : تسمح لكل الأجهزة استخدام العنوان العام .  
**ملاحظة :**

إذا لم يتم كتابة هذه الكلمة فإنه لن يسمح الرواتر لكل الأجهزة  
المحلية باستخدام العنوان العام وإنما يسمح لجهاز واحد فقط .

نعمل ping من جهاز pc1 و جهاز pc2 الى ( 5.0.0.5 ) R2 ( 5.0.0.5 ) 3

R1# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	5.0.0.1:29	192.168.1.6:29	5.0.0.5:29	5.0.0.5:29
icmp	5.0.0.1:30	192.168.1.6:30	5.0.0.5:30	5.0.0.5:30
icmp	5.0.0.1:31	192.168.1.6:31	5.0.0.5:31	5.0.0.5:31
icmp	5.0.0.1:89	192.168.1.4:89	5.0.0.5:89	5.0.0.5:89
icmp	5.0.0.1:90	192.168.1.4:90	5.0.0.5:90	5.0.0.5:90
icmp	5.0.0.1:91	192.168.1.4:91	5.0.0.5:91	5.0.0.5:91



PC1  
C:\> ping 5.0.0.5  
Pinging 5.0.0.5 with 32 bytes of data:  
Reply from 5.0.0.5: bytes=32 time<1ms TTL=126  
Reply from 5.0.0.5: bytes=32 time<1ms TTL=126  
Reply from 5.0.0.5: bytes=32 time=2ms TTL=126  
Reply from 5.0.0.5: bytes=32 time<1ms TTL=126  
Ping statistics for 5.0.0.5:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

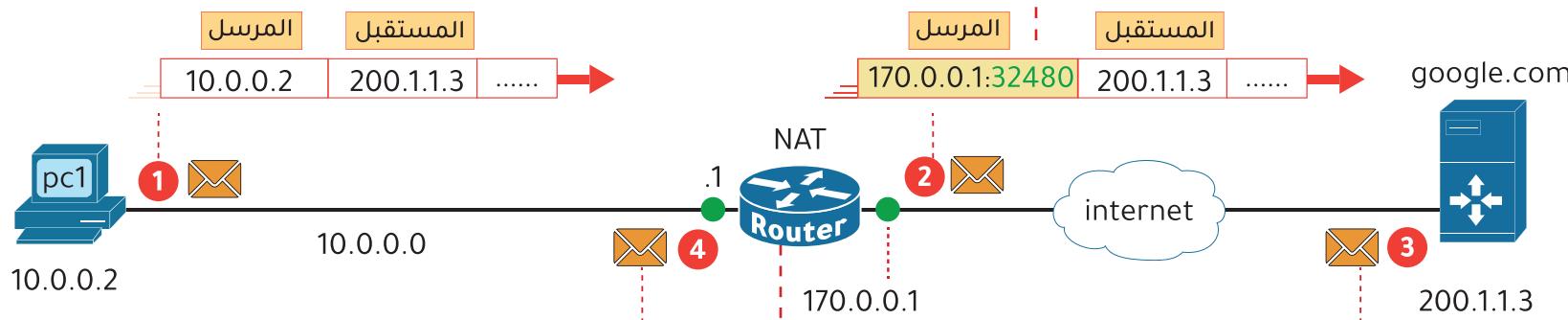
سؤال :

اذا عرفنا ان الراوتر R1 يستخدم عنوان عام واحد لكل الاجهزة المحلية فكيف يفرق الراوتر R1 بين الاجهزة المحلية اذا وصلت له رسالة من الخارج ؟

الجواب :

عن طريق اضافة رقم port عشوائي للابي المرسل ويسجله في جدول الـ NAT

لاحظ هنا عندما وصلت الرسالة من PC1 قام الراوتر باستبدال الابي المحلي بالابي العام واضاف عليه الرقم (32480)



يقوم الراوتر R1 بالبحث في جدول الـ NAT ومقارنة الرقم 32840 لاي جهاز ارسل هذه الرسالة ومن ثم يتم توجيهها له

الجهاز المستقبل يتواصل مع الراوتر بنفس الابي والرقم المضاف معه

## بروتوكول وقت الشبكة (NTP)

Network Time Protocol (NTP)



هو بروتوكول يعمل على ضبط ومزامنة الوقت تلقائياً داخل أجهزة الشبكة الداخلية بحيث تحصل أجهزة الشبكة على وقت متطابق ،

- تعرف الأجهزة على الوقت من خلال تبادل رسائل NTP مع بعضها البعض .

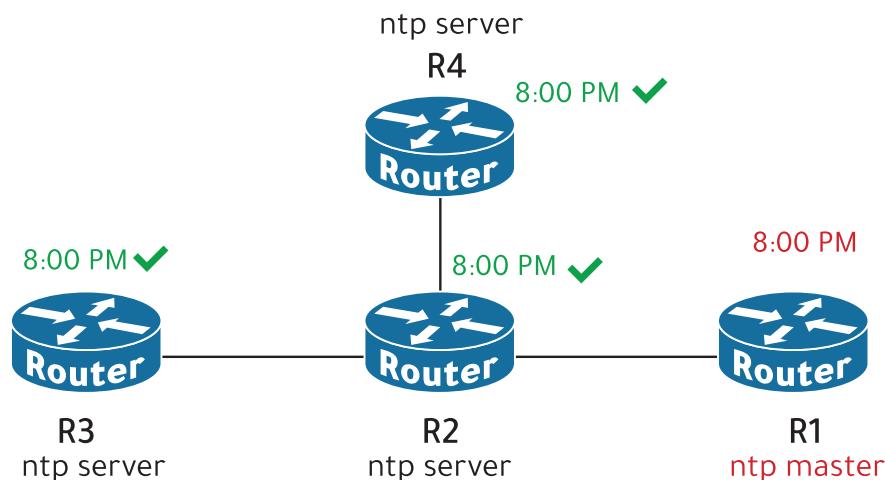
- يستخدم بروتوكول UDP ويعمل على بورت 123 .

- له فائدة في رسائل الاحداث التي تحصل في الشبكة فهو يظهر الوقت الصحيح للرسالة .

- يمكن للجهاز ان يكون :

- خادم ntp server حيث ان الأجهزة تضبط وقتها من هذا الخادم .

- وايضا يكون عميل ntp client يضبط وقته من أجهزة server .



**مصادر الوقت أو الساعة لبروتوكول NTP:**

1 - الساعة الداخلية Internal Clock

هي التي يتم ضبطها من القطعة الداخلية لجهاز الراوتر او السيرفر .

2 - الساعة الخارجية External Clock

هي التي تكون من مصدر خارجي (موقع انترنت او ساعة الذرية او ساعة GPS )

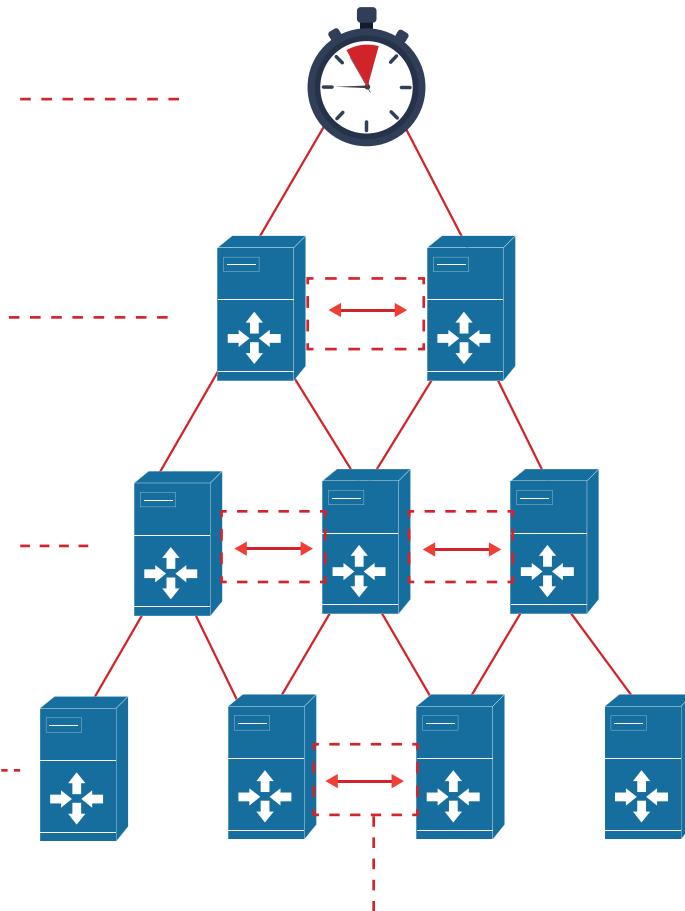
## السلسل الهرمي لـ NTP

الساعة المرجعية الأصلية : Stratum 0  
Reference Clock

خوادم هذه الطبقة Stratum 1  
تضبط وقتها من خوادم الطبقة 0

خوادم هذه الطبقة Stratum 2  
تضبط وقتها من خوادم الطبقة 1

خوادم هذه الطبقة Stratum 3  
تضبط وقتها من خوادم الطبقة 2



وضع النظير mode  
أجهزة في نفس الـ Stratum تفيد  
احتياطية في حال العطل .

# المسافة التي تبعد الجهاز عن مصدر الساعة  
المرجعية الأصلية (Reference Clock) تسمى  
المستوى أو الطبقة (Stratum)  
الساعة المرجعية الأصلية (Reference Clock) :  
هي جهاز وقت دقيق جدا مثل الساعة الذرية أو  
ساعة GPS

### NTP Stratum

هي القيمة التي تمثل عدد القفزات بعيداً عن مصدر  
الساعة الأصلي .

### NTP Modes

عند إعداد البروتوكول فإن له وضعين :  
**ntp master - 1**

في هذا الوضع الجهاز يأخذ الوقت من الساعة  
الداخلية Internal Clock .

**ntp server / client - 2**  
هذا الوضع يكون خادم يرسل الوقت وأيضاً كعميل  
client يستقبل الوقت .

**Symmetric active mode - 3**  
وضع النظير peer وهو أن يتشاربه جهازان في نفس  
الطبقة Stratum بمعنى أنهما يتداولان الوقت و  
لهم رقم Stratum متشاربه

## شرح إعدادات تغيير الوقت والمنطقة الزمنية

### عرض الوقت

```
R1# show clock
```

\*0:5:7.527 UTC Mon Mar 5 1993

### تعديل الوقت

```
R1# clock set 7:10:0 5 Mar 2023
```

### تغيير وقت المنطقة الزمنية

```
R1# conf t
```

```
R1(config)# clock timezone AST 3
```

### تفاصيل أكثر عن الساعة

```
R1# show clock detail
```

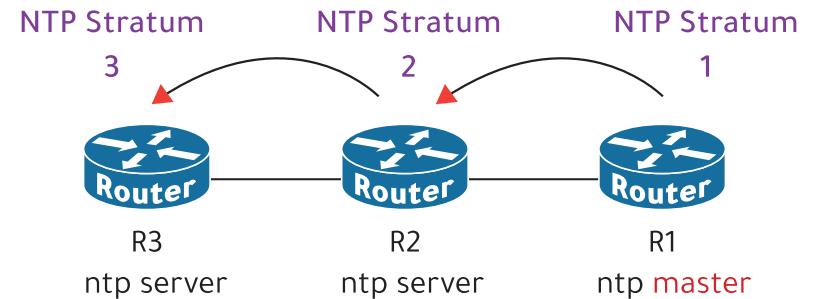
10:15:43.744 AST Sun Mar 5 2023

Time source is user configuration

**مصدر الوقت هو تكوين المستخدم**

السعودية متقدمة عن  
التوقيت العالمي  
UTC ب 3 ساعات

هو اختصار للتوقيت  
ال رسمي العربي  
Arabia Standard Time



- لاحظ إن الراوتر R1 رقمه 1 وعند وصول رسالة الوقت لـ R2 يتم زيادة رقم فيصبح 2 وهكذا . فيكون R3 يبعد قفزيتين عن مصدر الساعة الأصلي .

- كلما كان قيمة الـ Stratum أقل كلما كان أكثر دقة .

- الحد الأقصى لمستوى الـ Stratum هو 15 .

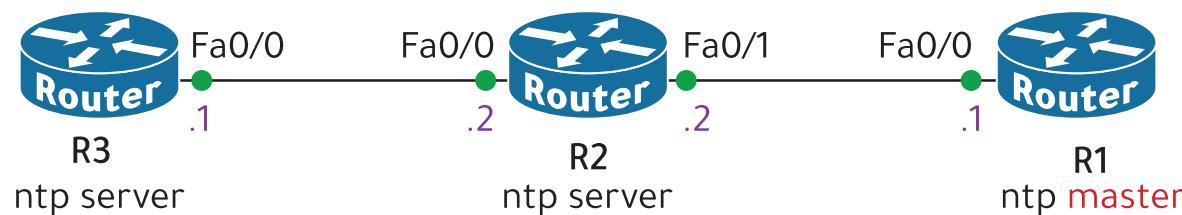
- أي رقم بعد 15 راح يكون الجهاز غير موثوق ولا يمكن أخذ او مزامنه الوقت منه .

- القيمة الافتراضية لـ Stratum في أجهزة سيسكو هي 8 .

السنة	اليوم	الدقائق	الثواني	ساعة
15	feb	2023	00	09:26:00



## إعدادات بروتوكول NTP



### مثال :

لدينا هذا النموذج وسوف نطبق عليه بروتوكول NTP :

- الراوتر الرئيسي (MASTER) هو R1

```
R1
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 14.0.0.1 255.255.255.252
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 14.0.0.0 0.0.0.3 area 0
R1(config-router)# end
R1(config)# clock timezone AST 3
R1 # clock set 09:26:00 15 feb 2023
R1(config)# ntp master
```

### مراحل الحل :

1 تطبيق الإعدادات الأساسية .

2 تطبيق اعدادات بروتوكول OSPF لربط الأجهزة .

3 تغيير الا\_timezone (التوقيت الدولي) من UTC الى AST +3 (من

النظام العالمي إلى توقيت السعودية +3).

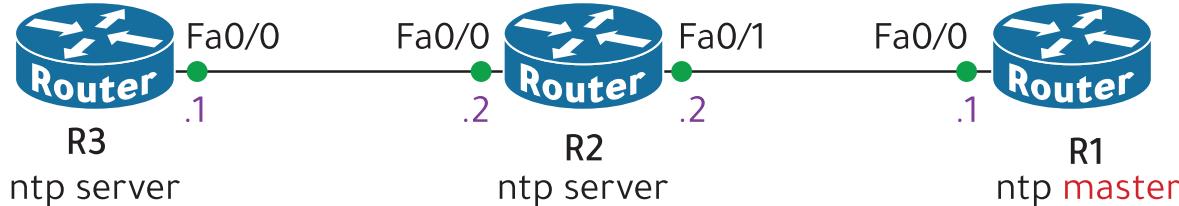
4 تغيير الوقت في الجهاز الرئيسي .

5 تطبيق اعدادات بروتوكول NTP .

الـ Master يعني  
الـ Stratum رقم الـ  
المصدر الرئيسي الذي  
تنزامن منه الأجهزة

12.0.0.0 /30

14.0.0.0 /30



R2

```

R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 12.0.0.2 255.255.255.252
R2(config-if)# exit
  
```

```

R2(config)# int Fa0/1
R2(config-if)# no shutdown
R2(config-if)# ip add 14.0.0.2 255.255.255.252
R2(config-if)# exit
  
```

```

R2(config)# router ospf 1
R2(config-router)# network 12.0.0.0 0.0.0.3 area 0
R2(config-router)# network 14.0.0.0 0.0.0.3 area 0
R2(config-router)# end
  
```

```

R2(config)# clock timezone AST 3
R2(config)# ntp server 14.0.0.1
  
```

1

2

3

5

R3

```

R3(config)# int Fa0/0
R3(config-if)# no shutdown
R3(config-if)# ip add 12.0.0.1 255.255.255.252
R3(config-if)# exit
  
```

```

R3(config)# router ospf 1
R3(config-router)# network 12.0.0.0 0.0.0.3 area 0
R3(config-router)# end
  
```

```

R3(config)# clock timezone AST 3
  
```

```

R3(config)# ntp server 12.0.0.2
  
```

1

2

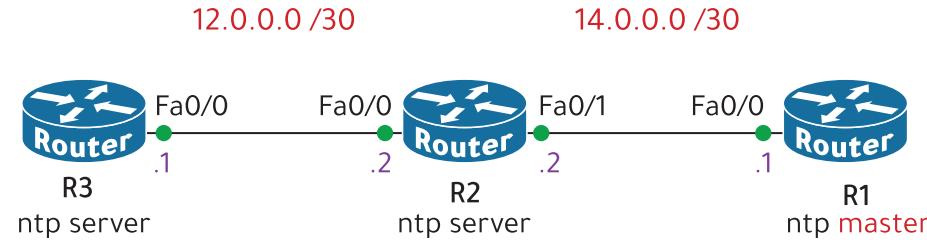
3

5

يأخذ الوقت من R2  
ويتزامن معه

يأخذ الوقت من R1  
ويتزامن معه

نستعرض جدول بروتوكول الـ ntp



عرض الساعة والتأكد من الوقت

R1# show clock

20:5:6.338 AST Wed Feb 15 2023

R2# show clock

20:5:20.10 AST Wed Feb 15 2023

R3# show clock

20:5:40.15 AST Wed Feb 15 2023

R1

R1# show ntp associations

عنوان مرجعية	الساعة المرجعية	Stratum
address	ref clock	st
*~127.127.1.1	.LOCL.	5
* sys.peer, ~ configured		

عنوان القطعة التي  
دخل الجهاز

علامة (\*) تعني انه تمت  
مزامنه الوقت

من عنوان القطعة  
المحلية

رقم الـ stratum هنا

للسنوات

والذي هو عنوان القطعة  
الداخلية في الراوتر.

R1

R1# show ntp status

Clock is synchronized, stratum 6, reference is 127.127.1.1

الساعة متزامنة

رقم الـ stratum الذي  
أدخلناه في الإعدادات

عنوان المرجع  
للساعة

R2

R2# show ntp associations

عنوان مصدر الساعة	الساعة المرجعية	Stratum
address	ref clock	st
*~14.0.0.1	127.127.1.1	6
* sys.peer, ~ configured		

رقم الـ stratum للعنوان 14.0.0.1 هو 6

R3

R3# show ntp associations

عنوان مصدر الساعة	الساعة المرجعية	Stratum
address	ref clock	st
*~12.0.0.2	14.0.0.1	7

رقم الـ stratum للعنوان 12.0.0.2 هو 7

R2

R2# show ntp status

Clock is **synchronized**, stratum 7, reference is 14.0.0.1

الساعة متزامنة  
R2 J stratum 7  
عنوان مصدر  
الوقت لـ R2

R3

R3# show ntp status

Clock is **synchronized**, stratum 8, reference is 12.0.0.2

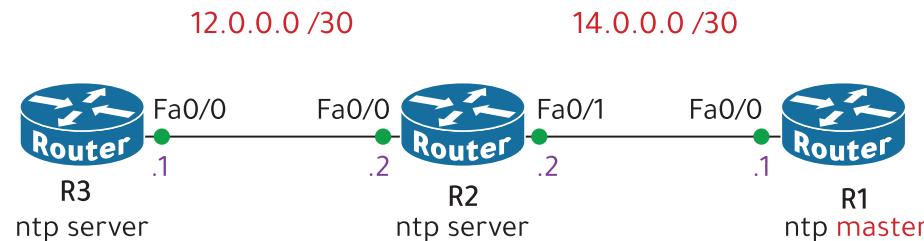
الساعة متزامنة  
R3 J stratum 8  
عنوان مصدر  
الوقت لـ R2

**ملاحظة :**

- تحتاج ان تنتظر دقائق حتى تظهر مزامنة الساعة عند استعراض جدول بروتوكول ntp.

## المصادقة في لـ NTP

NTP Authentication



- يمكن اضافة مصادقة بين جهازين عند عملية المزامنة . وهي اختيارية .

**مثال :**

لدينا نفس المثال السابق وسوف نطبق عليه  
NTP Authentication

R1 هو الراوتر الرئيسي (MASTER)

**مراحل الحل :**

1 تطبيق الإعدادات الأساسية و بروتوكول OSPF لربط الأجهزة.

2 تطبيق اعدادات تغيير الا Timezone (التوقيت الدولي) من UTC الى

3 من النظام العالمي إلى توقيت السعودية (+3).

4 تغيير الوقت في الجهاز الرئيسي .

4 تطبيق اعدادات بروتوكول NTP + Authentication .

```
R1(config)# int Fa0/0
R1(config-if)# no shutdown ①
R1(config-if)# ip add 14.0.0.1 255.255.255.252
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit

R1(config)# clock timezone AST 3 ②
R1 # clock set 09:26:00 15 feb 2023 ③

R1(config)# ntp master 6 ④
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 a123
R1(config)# ntp trusted-key 1
      تحديد الا key 1 كمفتاح موثوق
```

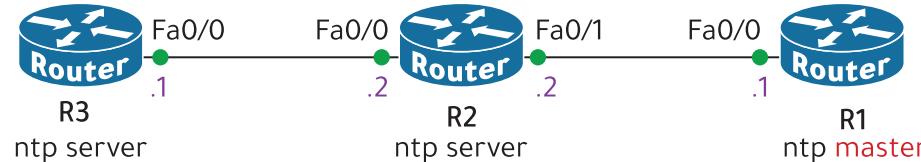
تفعيل المصادقة

كلمة المرور password

رقم المفتاح

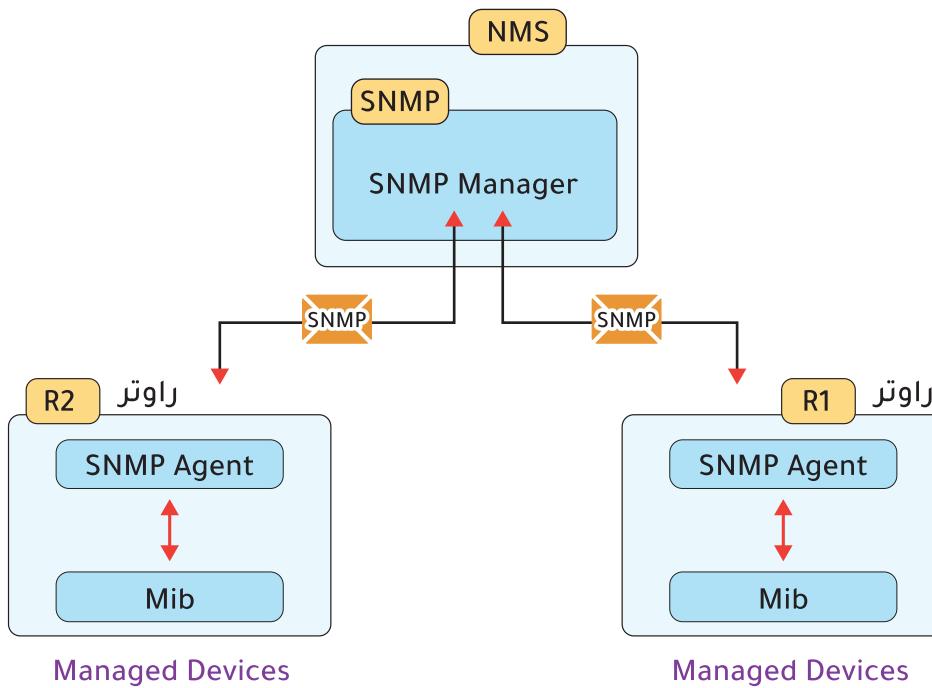
انشاء مفتاح مصادقة

12.0.0.0 /30      14.0.0.0 /30



```
R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 12.0.0.2 255.255.255.252
R1(config-if)# ip ospf 1 area 0
R2(config-if)# exit
R2(config)# int Fa0/1
R2(config-if)# no shutdown
R2(config-if)# ip add 14.0.0.2 255.255.255.252
R1(config-if)# ip ospf 1 area 0
R2(config-if)# exit
R2(config)# clock timezone AST 3
R2(config)# ntp authenticate
R2(config)# ntp authentication-key 1 md5 a123
R2(config)# ntp trusted-key 1
R2(config)# ntp server 14.0.0.1
```

```
R3(config)# int Fa0/0
R3(config-if)# no shutdown
R3(config-if)# ip add 12.0.0.1 255.255.255.252
R1(config-if)# ip ospf 1 area 0
R3(config-if)# exit
R3(config)# clock timezone AST 3
R3(config)# ntp authenticate
R3(config)# ntp authentication-key 1 md5 a123
R3(config)# ntp trusted-key 1
R3(config)# ntp server 12.0.0.2
```



## بروتوكول إدارة الشبكة البسيط

Simple Network Management Protocol (SNMP)

هو بروتوكول يستخدم للمراقبة والتحكم وادارة الأجهزة في الشبكة (راوترات - سويتشات - خوادم - طابعات وغيرها). مثل الاستعلام عن حالات الاجهزة والتعديل بالاعدادات وايضا استقبال اشعارات الاحداث التي تحصل للجهاز.

### هناك نوعان من الاجهزة في بروتوكول SNMP

#### 1 - نظام إدارة الشبكة (NMS)

هو الجهاز الذي يتم تحميل عليه نظام إدارة الشبكة (SNMP) ويتم عن طريقه ادارة واستعلام ومراقبة الشبكة. ونطلق عليه .SNMP Manager

#### 2 - الأجهزة المُدارَة

هي الأجهزة الموجودة في الشبكة وتحت ادارة الـ NMS وتم تفعيل بروتوكول SNMP عليها مثل (الراوتر - السويتش - ...). هذه الأجهزة تتفاعل مع الـ snmp manager مثل ارسال اخطارات واستقبال رسائل من NMS . ونطلق عليهم وكلاء SNMP Agents

- قاعدة المعلومات الإدارية
- Management information base **Mib** وهي اختصار لم
- فيها كل المتغيرات التي يديرها بروتوكول snmp ويستعمل منها .
- لكل متغير له رقم يتخزن في قاعدة البيانات يسمى **object id (OID)**
- هذه المتغيرات مثل حالة المعالج ودرجة الحرارة ومعدل نقل البيانات.

## إصدارات SNMP

**SNMP v1 -**

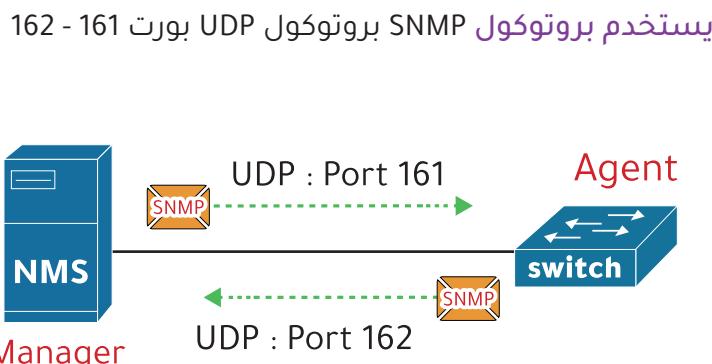
هو الاصدار الاصلي

**SNMP v2c -**

اصدار مطور يستطيع اخذ معلومات بكميات كبيرة من الراوتر او السويتش او غيره باستخدام طلب واحد مما يجعله اكثر كفاءة .

**SNMP v3 -**

هو افضل اصدار لانه أكثر أمانا ويدعم التشفير القوي والمصادقة . authentication



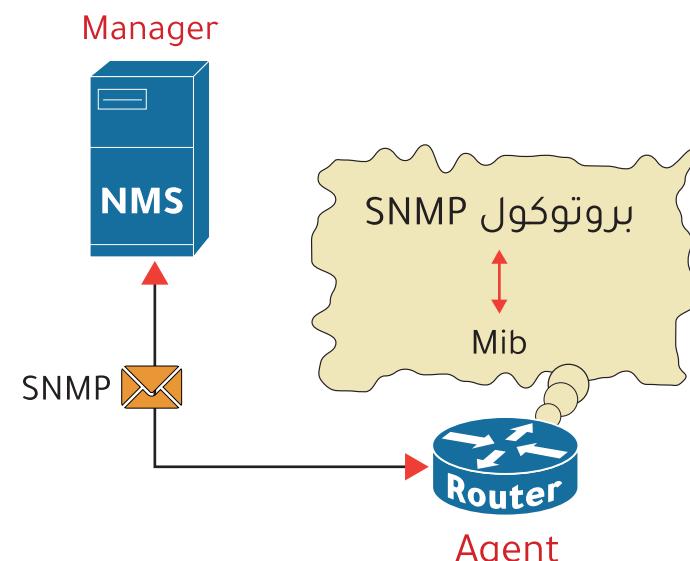
يستخدم بروتوكول SNMP بروتوكول UDP بورت 161 - 162

• هناك ثلاثة عمليات رئيسية مستخدمة في NMS :

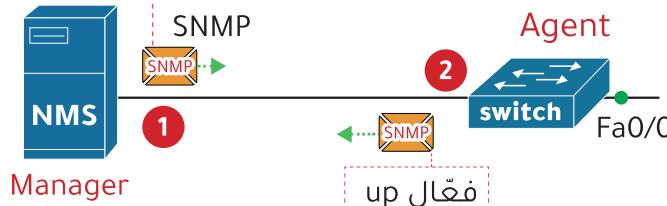
A - يمكن للجهاز ابلاغ الـ NMS بالاحداث التي تحصل له مثل اقفال بورت او عطل حصل بالجهاز .

B - يمكن للـ NMS طلب الحصول على معلومات عن حالة الاجهزة مثل حالة المعالج للتأكد من عدم تحميل الجهاز بجهد كبير .

C - يمكن لـ NMS اخبار الاجهزة بتغيير اعداداتها ، مثل طلب تغيير عنوان منفذ معين او اضافة ايبي وغيرها وسيتم الرد من الاجهزة بالتنفيذ .



ما هي حالة المنفذ Fa0/0 ؟



طلب يرسله المدير الى الوكيل يستعلم فيه عن متغير أو عدة متغيرات مثل حالة منفذ فيرد الوكيل برسالة استجابة عن حالة المنفذ إنه فعال.

### نوع الرسالة Message type

#### Get

رسائل مرسلة من المدير (NMS) لقراءة المعلومات من الاجهزة المدارة مثل حالة المعالج .

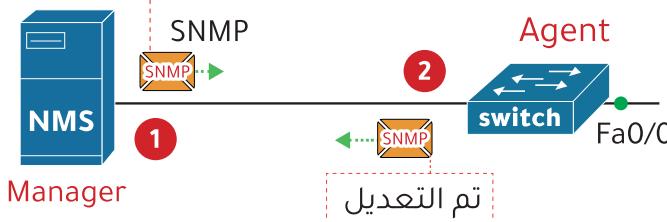
#### GetNext

طلب يرسله المدير الى الوكيل لاستكشاف المتغيرات المتاحة والمخزنة في قاعدة بياناته . mib

#### GetBulk

إصدار مطور من GetNext وأكثر كفاءة .

قم بتعديل اسم الجهاز الى SW2



### رسائل التعيين ونوعها Set

رسائل التعيين وهي رسائل مرسلة من المدير (NMS) الى الوكيل Agent لتخفيير اعدادات متغير مثل تغيير عنوان ايبي . فيتم الرد من الوكيل بالاستجابة بتغيير الاعدادات .

## رسائل SNMP



فئة الرسالة  
Message class

الوصف  
description

01

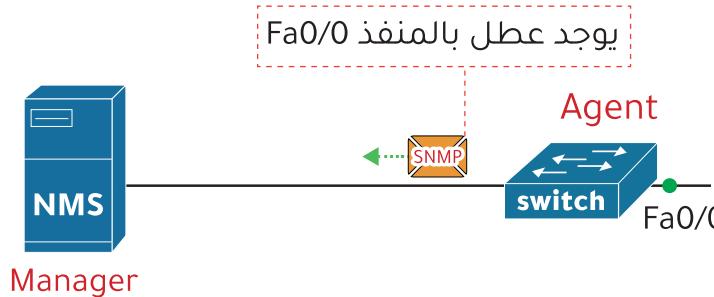
read

02

write

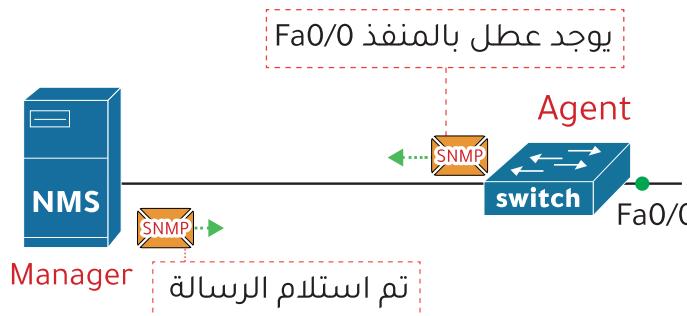
### Trap

رسالة إعلام من الوكيل agent الى المدير manager ، لكن المدير لا يريد باستلام الرسالة .

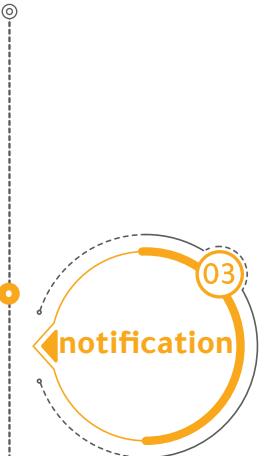


### Inform

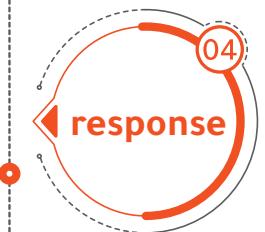
رسالة إعلام من الوكيل agent الى المدير manager ، لكن المدير يقوم بالرد باستلام الرسالة .



رسائل الإعلام و هي رسائل ترسل من الأجهزة او الوكلاء الى المدير لإعلامه بتغيرات حدثت . مثل تعطل منفذ .



رسائل الاستجابة وهي الرسائل المرسلة للرد على رسالة أو طلب سابق .

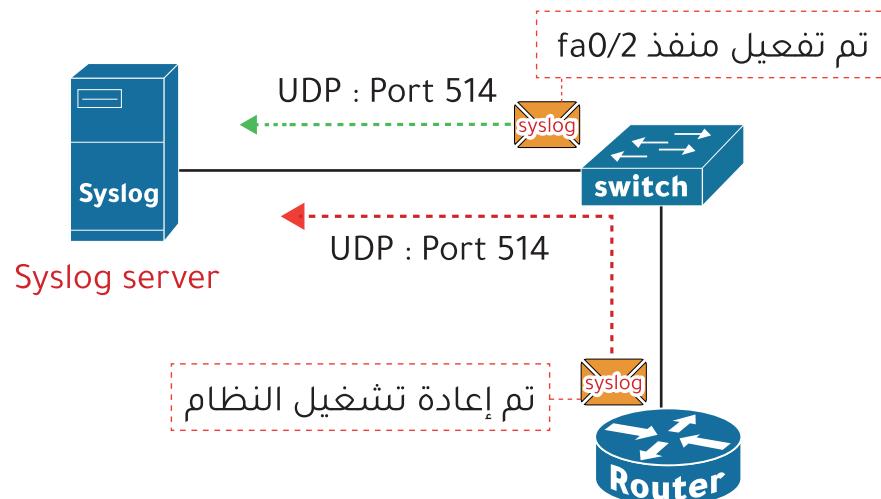


## رسائل سجل النظام System Log Messages (Syslog)

R1

```
R3(config)# int fa0/5
R3(config-if)# no sh
رسالة النظم
08:01:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to up
```

لاحظ هذه الرسالة ظهرت بعد تفعيل منفذ fa0/5 .



- Syslog هو بروتوكول قياسي لتسجيل رسائل النظام تستخدمه أجهزة الشبكة لإرسال سجلات الأحداث إلى خادم Syslog للتخزين. ووظيفه هذا الخادم مراقبة الأجهزة التي تعمل داخل الشبكة، مثل السيرفرات والطابعات والسوبيتشات والراوترات وغيرها.

- في الشبكات الصغيرة نستطيع تتبع هذه الرسائل ولكن عندما نتعامل مع شبكات كبيرة راح يصعب علينا تتبع كل هذه الرسائل ولكي نغلب على هذه المشكلة ، نستخدم بروتوكول Syslog مع خادم Syslog

- يمكن استخدام Syslog لتسجيل الأحداث مثل اطفاء منفذ او اكتشاف جار عبر ospf ايضا اعادة تشغيل النظام .

- هذه الرسائل ضرورية جدا عند استكشاف المشكلات وإصلاحها.

- يستخدم بروتوكول UDP ومنفذ 514 .

المستوى Level	الكلمة الرئيسية Keyword	الوصف Description	
0	Emergencies	طوارئ	النظام غير قابل للاستخدام
1	Alerts	تنبيه	يلزم اتخاذ إجراءات فورية
2	Critical	هام جداً	وجود ظروف هامة جداً
3	Errors	أخطاء	يوجد خطأ قد حدث
4	Warnings	تحذيرات	تحذيرات عند حدوث شيء
5	Notification	إشعار	إشعار طبيعي ولكنه مهم
6	Informational	إعلان	رسائل إعلام
7	Debugging	التصحيح	رسالة حدث مباشر

## مستويات الخطورة في الـ Syslog

### Syslog severity levels

- توجد 8 مستويات للخطورة في الـ Syslog :
- أعلى مستوى هو المستوى 0 (emergencies) .
- أدنى مستوى هو المستوى 7 (debugging) .

## تنسيق رسالة سجل النظام

### Syslog message format

عند ظهور رسائل النظام فإن لها تنسيق معين يبين لنا وصف الرسالة ومستوى الخطورة وتاريخ الرسالة وغيرها .

الصفحة التالية



facility هي كلمة مختصرة تدل على أن الموضوع يخص بروتوكول او شيء آخر، يعني مثلًا ستجد اسم ospf لو اكتشف أحد الجيران

رقم تسلسلي  
لترتيب الرسائل

تاريخ ووقت  
انشاء الرسالة

الخطورة وهي تشير الى خطورة الحدث وهنا ستجد رقم يدل على مستوى الخطورة التي تم عرضها في الجدول 8

كلمة مختصرة تدل الى حدث  
معين تم في داخل الـ facility

الوصف : وهي المعلومات  
التفصيلية حول الحدث

**seq : time stamp : %facility - severity - MNEMONIC : description**

```
R1
R3(config)# int fa0/5
R3(config-if)# no sh

08:01:13 %LINEPROTO-5-UPDOWN : Line protocol on Interface FastEthernet0/5, changed state to up

00:00:45 %OSPF-5-ADJCHG : Process 1, Nbr 3.3.3.3 on FastEthernet0/1 from LOADING to FULL, Loading Done
```

تفعيل الـ time stamp

Router(config)# service timestamps log datetime msec

تفعيل الـ seq

Router(config)# service sequence-numbers

ملاحظة :

قد لا يتم عرض time stamp و seq في  
الرسالة حسب اعدادات الجهاز .

لتفعيل الـ seq و time stamp

## موقع تسجيل رسائل النظام Syslog logging locations

### Console Line - 1

يتم عرض رسائل النظام Syslog عند الاتصال بالجهاز عبر كيبيل الكونسول وستظهر في شاشة الامر CLI .

- افتراضيا سوف يتم اظهار كل الرسائل من المستوى 0 الى المستوى 7 .

R1# Show logging

### External Server - 4

يمكن إعداد الجهاز لارسال رسائل الـ Syslog الى خادم خارجي external server وهذا مفيد جدا في الشبكات الصغيرة وبالاخص الشبكات الكبيرة .

اوامر الاعداد :

```
R1(config)# logging host [أبي السيرفر]  
R1(config)# logging trap [اسم مستوى الخطورة]
```

### Vty Lines - 2

تعني انه سيتم عرض رسائل النظام Syslog في شاشة الامر CLI عند الاتصال بالجهاز او الدخول عليه عبر بروتوكول telnet أو ssh ( هي بروتوكولات للاتصال بجهاز في الشبكة ولكن من بعد وليس مباشر ) .

- ملاحظة : رسائل الـ Syslog لن تظهر لك اذا دخلت عبر هذه البروتوكولات من بعيد لانها غير مفعولة افتراضيا وتحتاج الى تفعيلها .  
للتفعيل تدخل هذا الامر وانت في شاشة الجهاز البعيدة بعد الدخول على الجهاز المراد .

[رقم أو اسم مستوى الخطورة]

R1# terminal monitor

ملحوظة :

عند وضع رقم 6 مثلا فإنه يشمل الرقم وما دونه :

0-1-2-3-4-5-6

### مثال :

لدينا هذا النموذج وسوف نطبق عليه :

- بروتوكول Syslog

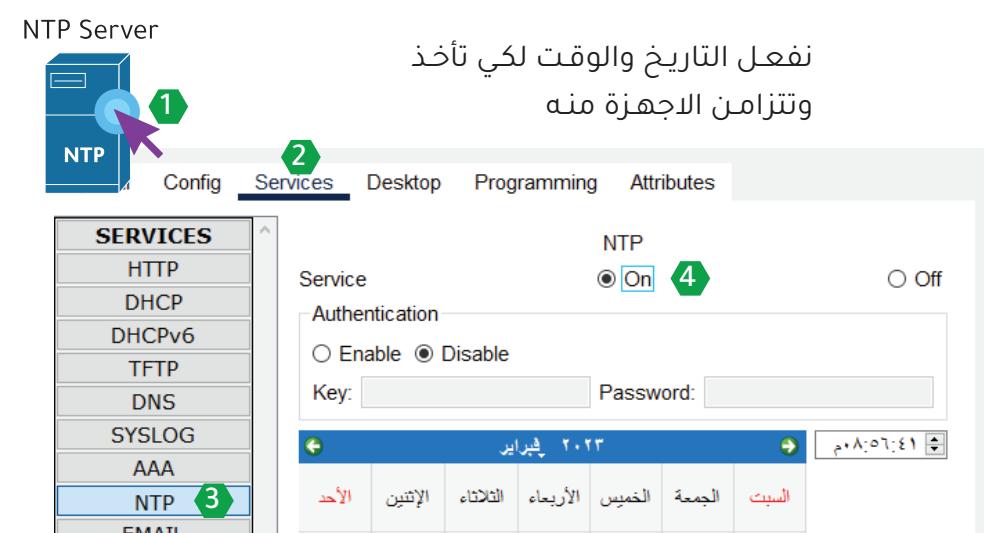
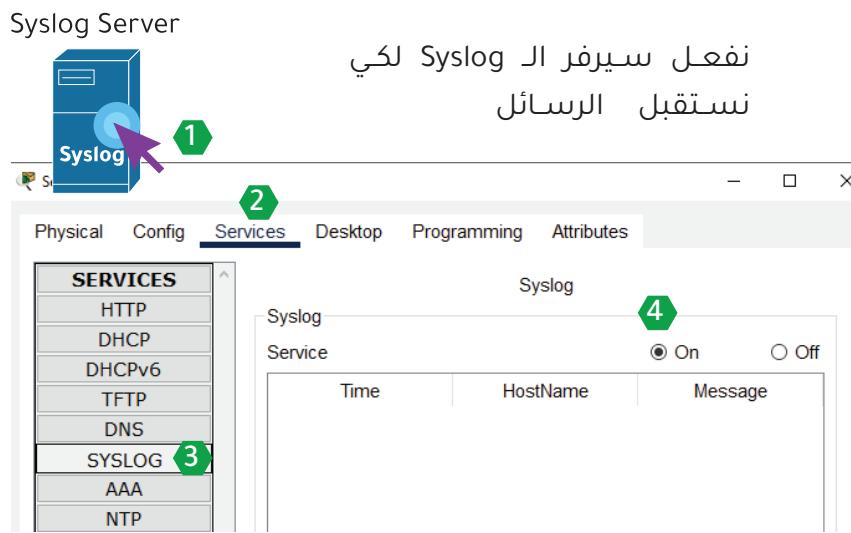
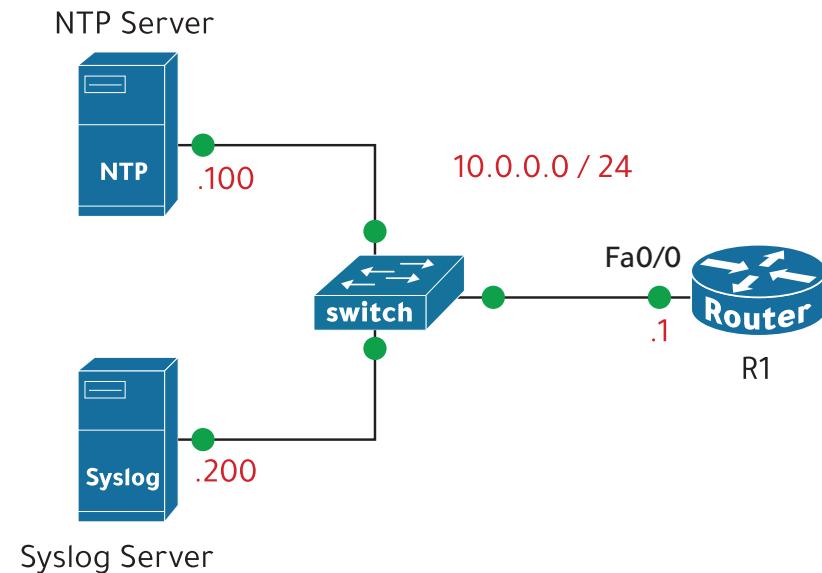
- بروتوكول NTP

### مراحل الحل :

تطبيق الإعدادات الأساسية . ①

. إعداد الـ Syslog ②

. إعداد الـ NTP ③



**IP Configuration**

DHCP       Static

IPv4 Address:

Subnet Mask:

Default Gateway:

DNS Server:

**IP Configuration**

DHCP       Static

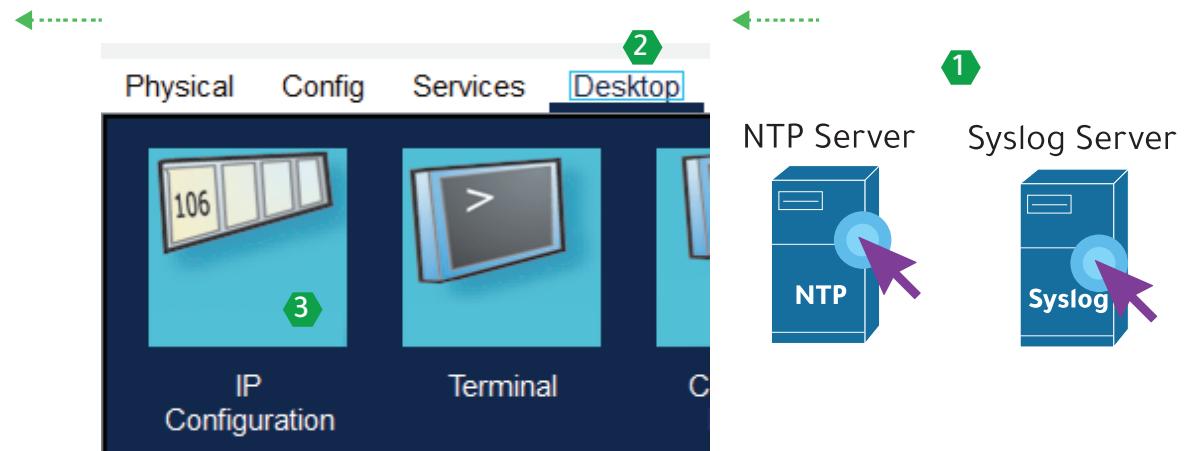
IPv4 Address:

Subnet Mask:

Default Gateway:

DNS Server:

نعطي ايبيهات للسيرفرات من نفس  
مدى الشبكة



أمر تحويل الرسائل الى السيرفر الذي عنوانه 10.0.0.200

أمر لكي يظهر الوقت أثناء عرض الرسالة

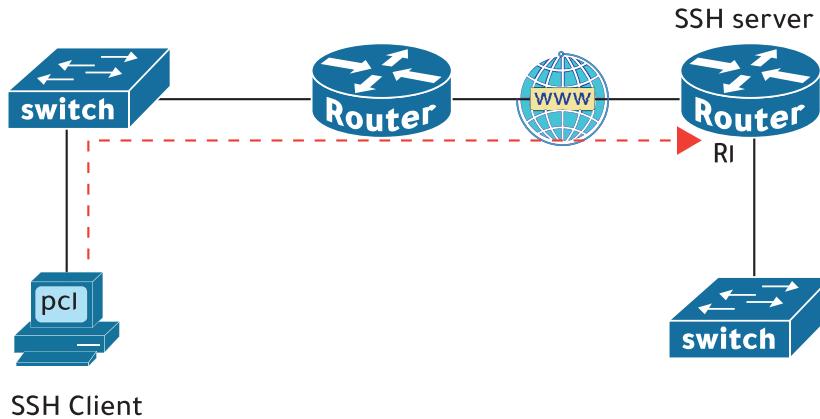
أمر لكي يتزامن الوقت مع السيرفر الذي عنوانه 10.0.0.100

```
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 10.0.0.1 255.255.255.0
R1(config-if)# exit
```

```
R1(config)# logging host 10.0.0.200
R1(config)# service timestamps log datetime msec
R1(config)# ntp server 10.0.0.100
```

نلاحظ وصول  
الرسائل للسيرفر

Time	HostName	Message
1 02.18.2023 09:48:27.660 PM	10.0.0.1	Loopback0, changed state to up
2 02.18.2023 09:48:27.660 PM	10.0.0.1	...
3 02.18.2023 09:48:18.612 PM	10.0.0.1	...
4 02.18.2023 09:48:18.612 PM	10.0.0.1	...



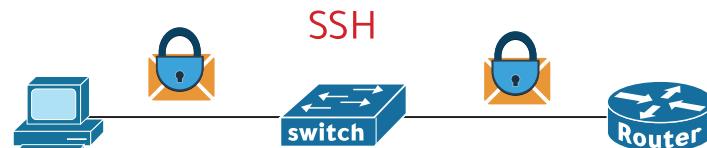
### بروتوكول الـ SSH ( Secure Shell )

هو بروتوكول شبكة يوفر اتصال آمن ومشفر عند الدخول على الأجهزة البعيدة وتنفيذ الأوامر عليها وتعديلها.

- هذا البروتوكول هو المستخدم الان والمعتمد لدى الكل بسبب تشفيره للبيانات التي تنتقل عبر الشبكة .

- يستخدم الـ SSH منفذ 22 ( port 22 ) - **SSH Client** هو الجهاز الذي انت عليه والذي تستخدمه للدخول على جهاز بعيد .

**SSH server** - هو الجهاز البعيد الذي تريد الدخول عليه .



### Telnet - SSH

#### Remote Access with ssh - telnet protocol



هي بروتوكولات تحكم وإدارة عن بعد تسمح للمستخدمين بالاتصال بالحوادم والأجهزة البعيدة وتعديلها عبر الإنترنيت ، وايضا تنفيذ الأوامر عليها و نقل الملفات بين الأجهزة.

- الفائدة أنه لو كان عندك راوترات وسويتاشات كثيرة في الشركة فليس من المعقول أن تذهب لكل راوتر وتقوم بتوصيل الكابل به لكي تقوم بعمل الاعدادات لذلك سوف تستفيد من طريقة الاتصال عن بعد وذلك بالدخول لاي راوتر او سويتش من جهاز واحد فقط .

- ايضا يجب ان نعمل كلمة مرور أمان للدخول عن بعد بحيث لو أراد أحد الاتصال بالراوتر فيجب عليه ادخال كلمة المرور .

### بروتوكول الـ Telnet

هو بروتوكول شبكة يوفر اتصال غير آمن وغير مشفر عند الدخول على الأجهزة البعيدة لتنفيذ الأوامر عليها وتعديلها .

- هذا البروتوكول غير مستخدم ولا يفضل استخدامه .

- يستخدم الـ Telnet منفذ 23 ( port 23 ) - **Telnet Client** هو الجهاز الذي انت عليه والذي تستخدمه للدخول على جهاز بعيد .

**Telnet server** - هو الجهاز البعيد الذي تريد الدخول عليه .





## إعدادات SSH



**مثال :**

لدينا هذا النموذج في برنامج الباكت تريسر  
وسوف نطبق عليه :  
- إعدادات ssh

R2

```

R2(config)# int Fa0/0
R2(config-if)# no shutdown
R2(config-if)# ip add 10.0.0.2 255.255.255.252
R2(config-if)# exit
    
```

**مراحل الحل :**

1 تطبيق الإعدادات الأساسية .

2 تطبيق إعدادات ssh

السماح لعدد 5 جلسات أو 5 مستخدمين يستطيعوا الدخول على الجهاز

Login local لكي يظهر له أمر طلب ادخال اسم المستخدم و كلمة المرور

نعمل كلمة مرور للدخول في وضع enable mode JI

إنشاء اسم دومين مثل cisco.com لتحديد اصدار الـ SSH

```
R1
R1(config)# int Fa0/0
R1(config-if)# no shutdown ①
R1(config-if)# ip add 10.0.0.1 255.255.255.252
R1(config-if)# exit

R1(config)# line vty 0 4 ②
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit

R1(config)# username hani secret 1236
R1(config)# username ahmad pri 15 secret 1235

R1(config)# enable secret 1234

R1(config)# ip domain-name cisco.com
R1(config)# crypto key generate rsa
R1(config)# ip ssh version 2

How many bits in the modulus [512]: 1024
R1(config)# exit
```

نسمح بالدخول على هذا الجهاز ببروتوكول ssh فقط والهدف هو منع الدخول بالـ telnet لأنه غير مشفر

إنشاء مستخدم وكلمة مرور لكي يدخل على الـ user mode

هذه طريقة ثانية لانشاء مستخدم وكلمة مرور

R1 > (user mode)  
R1 # (enable mode)

أمر إنشاء وتوليد مفتاح التشفير من نوع rsa

سوف يطلب منك ادخال حجم مفتاح التشفير ويفضل ان لا يقل عن 1024 بت

R2# show sessions نستعرض الاجهزه اللي تم الدخول عليها

- علامة (\*) تعني آخر جلسة كنت داخل عليها



سوف ندخل الى جهاز الراوتر R1 عن طريق بروتوكول SSH

```

R2
R2# ssh -L ahmad 10.0.0.1
Password: 1235
R1#
R1#
R1# x Ctrl + Shift + 6
R2# show sessions
Conn Host Address Byte Idle Conn Name
* 1 10.0.0.1 10.0.0.1 0 0 10.0.0.1
  
```

ايبي الجهاز البعيد .--> رقم الجلسة



لو اردت الرجوع الى جهاز R2 وهو الجهاز اللي انت شابك عليه الكيبل بدون الخروج من الجلسة (sessions) بدون قطع اتصالك بالجهاز البعيد )

تضغط مع بعض على الا 3 مفاتيح :

x Ctrl + Shift + 6 ثم ارفع يدك وارجع اضغط حرف x

**للدخول الى الجهاز البعيد مرة اخرى**

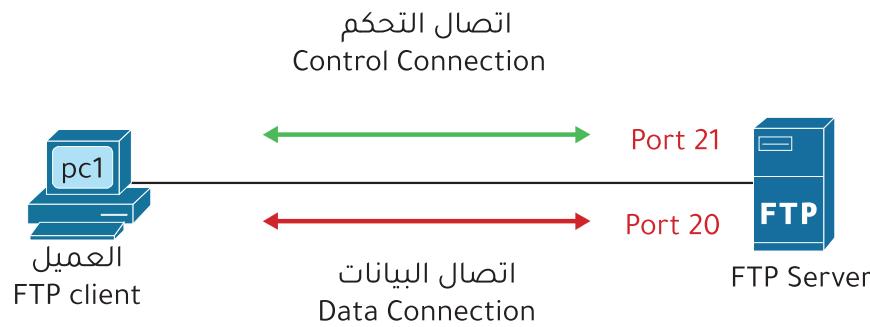
اضغط Enter مرتين راح ترجع تدخل على الجهاز البعيد . R1

أو تكتب رقم الجلسة وتضغط enter بهذه الطريقة 1 R2# 1



يستخدم بروتوكول FTP ببروتوكول TCP لانشاء نوعين من الاتصال :  
1- اتصال التحكم : Control Connection

يستخدم منفذ 21 ( TCP Port 21 ) ويتم فيه ارسال اوامر التحكم ( control commands ) والطلبات .



#### 2 - اتصال البيانات : Data Connection

يستخدم منفذ 20 ( TCP Port 20 ) ويتم فيه ارسال البيانات بين الجهازين .

- هناك نوعين من اتصالات البيانات :

**A - Active mode**

**B - Passive mode**

## بروتوكولات نقل الملفات (TFTP - FTP)

File Transfer Protocol (FTP)

Trivial File Protocol (TFTP)

### File Transfer Protocol (FTP)

هو بروتوكول شبكة يُستخدم لنقل الملفات من جهاز الكمبيوتر إلى جهاز آخر عبر بروتوكول TCP ، مثل بروتوكولات الـ Telnet - SSH .

- يتم الاتصال بين الخادم server والعميل client لنقل الملفات .

- كمهندس شبكة ، فإن الاستخدام الأكثر شيوعاً لـ TFTP و FTP هو عملية ترقية نظام التشغيل لجهاز الشبكة .

- يمكن استخدام هذه البروتوكولات لنقل جميع أنواع الملفات بين الأجهزة المختلفة عبر الشبكة .

- في بروتوكول FTP يتم استخدام أسماء المستخدمين وكلمات المرور للمصادقة والتوثيق .

- لا يوجد تشفير في الـ FTP لذلك يتم إرسال جميع البيانات بنص عادي لكن يمكن استخدام بروتوكول FTPS أو بروتوكول SFTP (SSH File transfer protocol) لمزيد من الأمان .

Trivial File Protocol (TFTP)  
هو بروتوكول بسيط لنقل الملفات . يمتلك مميزات أساسية فقط عند مقارنته بـ FTP.

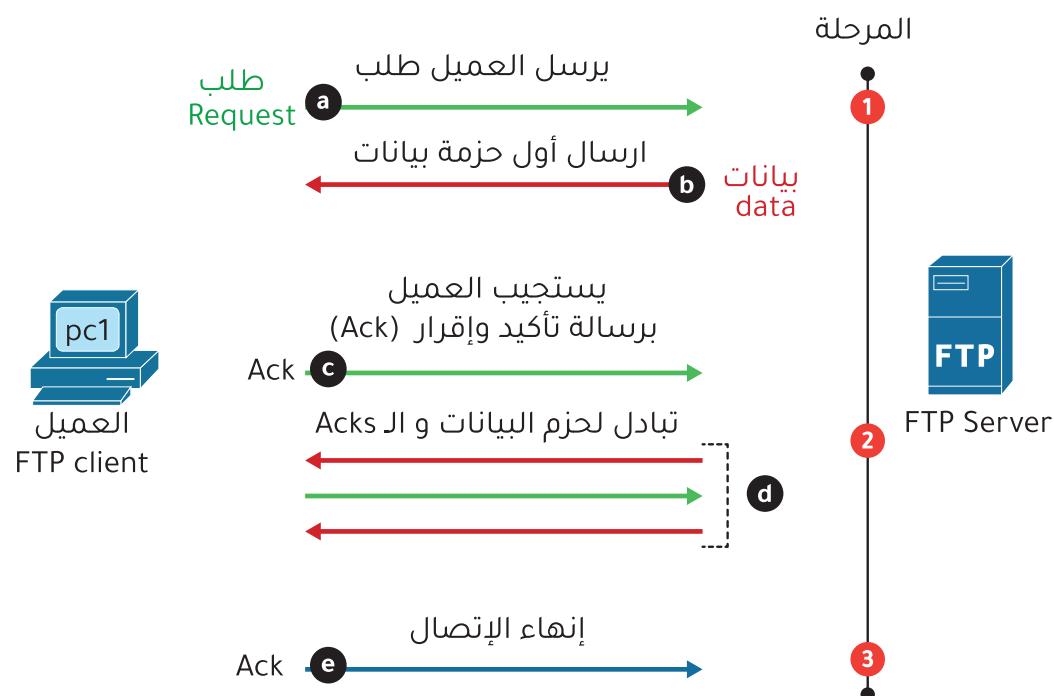
- لا يستخدم TFTP أي مصادقة أو توقيع . مما يعني عدم وجود أسماء مستخدمين وكلمات مرور .
- لا يوجد تشفير في الـ TFTP لذلك يتم إرسال جميع البيانات بنسق عادي.
- يستخدم الـ TFTP بروتوكول UDP ومنفذ 69 (UDP Port 69)

#### مراحل نقل الملفات في بروتوكول TFTP

1 - مرحلة الاتصال Connection

2 - نقل البيانات Data Transfer

3 - إنهاء الاتصال Connection Termination

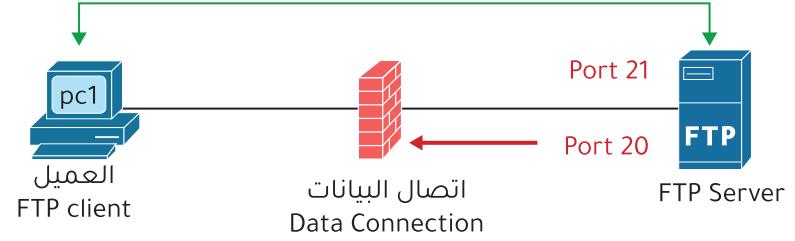


#### Active mode

هو الوضع الذي يبدأ فيه الخادم ببدأ الجلسة وفتح اتصال بيانات .

- في هذا الوضع قد تحصل مشكلة فلو كان هناك جدار حماية في الشبكة فسوف يمنع جدار الحماية اي اتصالات واردة من الخارج بدون تهيئة مسبقة .

#### اتصال التحكم Control Connection



#### Passive mode

هو الوضع الذي يبدأ فيه العميل ببدأ الجلسة وفتح اتصال بيانات .

#### اتصال التحكم Control Connection



## 2 - التأخير Delay

هناك طريقتين رئيسيتين لقياس التأخير:

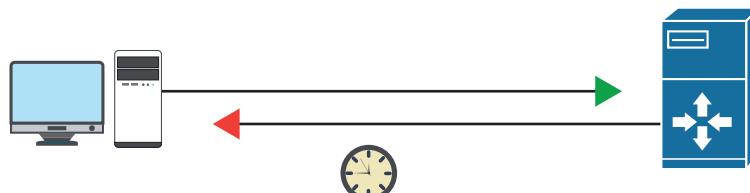
## A - التأخير في اتجاه واحد one way delay

هو الوقت الذي تستغرقه البيانات للانتقال من الجهاز المرسل إلى الجهاز المستقبل في اتجاه واحد فقط.



## B - التأخير في اتجاهين Two way delay

هو الوقت الذي تستغرقه البيانات للانتقال من الجهاز المرسل إلى الجهاز المستقبل والعودة مرة أخرى



## جودة الخدمة (QoS) Quality of Service (QoS)



**QoS** هي تقنية تدير حركة مرور البيانات حيث تعطي أولويه أعلى لمجموع حزم بيانات محددة عن الأخرى التي لها أولوية أقل.

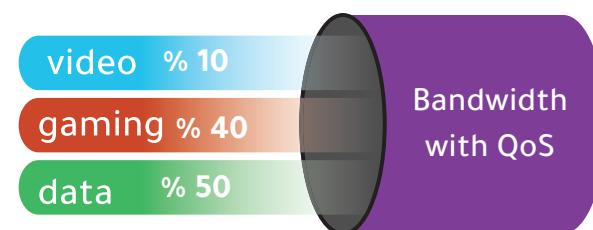
- تستخدم المؤسسات الـ QoS لتلبية متطلبات حركة المرور للتطبيقات الحساسة، مثل الصوت والفيديو في الوقت الفعلي، ولمنع تدني الجودة الناتجة عن فقدان الحزمة والتقطيع والتأخير.

## خصائص حركة مرور البيانات في الشبكة:

## 1 - الباندويث Bandwidth

هي سعة نقل البيانات في الثانية الواحدة.

- تسمح أدوات QoS بحجز قدر معين من الباندويث لزنوج معينة بالمرور على سبيل المثال . يمكن حجز 20% من الباندويث لحركة مرور الصوت ، و 30% لأنواع معينة من حركة البيانات المهمة وترك 50% لجميع حركة المرور الأخرى.



## الأدوات المستخدمة في تقنية QoS



### 1 classification and marking

### 2 Congestion Management Queuing - Scheduling

### 3 Shaping and Policing

### 4 Congestion Avoidance

### 3 - التأخير المتغير أو التقطيع Jitter

هو وصول طابور البيانات المؤلف من عدد من الحزم packets الى جهاز المستقبل بعد فواصل زمنية مختلفة وغير متساوية ..



### 4 - الخسارة Loss

هي فقدان بعض حزم البيانات المرسلة التي لا تصل إلى وجهتها . قد يكون ذلك بسبب مشكلة في الكابلات ، أو كانت الشبكة مزدحمة وامتلأت قوائم الانتظار، فيحصل تجاهل للحزم التي لا يمكن وضعها في قائمة الانتظار.



## Classification and Marking

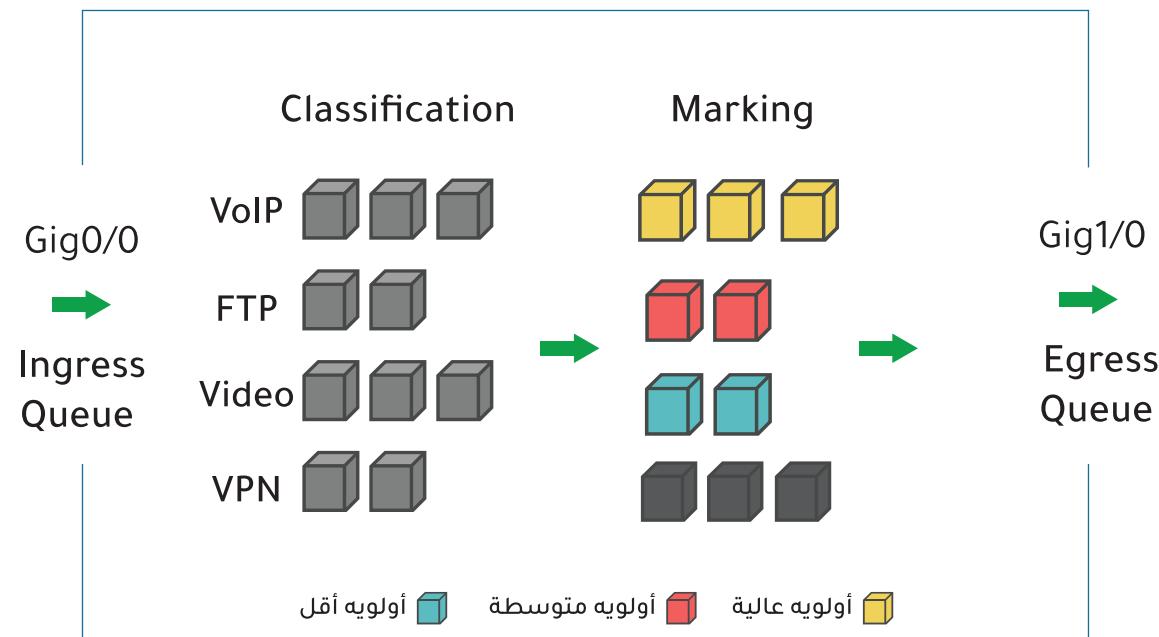


### Marking -

- إضافة علامات رقمية مختلفة لكل فئة وتمييزها عن بعضها البعض من حيث الاولوية والأهمية في حركة المرور.
- مثلا الطرود البريدية عندما يكون عليها استiker الشحن العاجل فان لها اولوية أعلى في التنقل والوصول الى مالكها .
  - ايضا عندما يرسل الهاتف حزمة بيانات إلى شبكة يحتاج إلى تمييز هذه الحزم على أنها مهمة حتى يتمكن كل جهاز راوتر او سويتش على التعامل مع الحزمة بشكل مختلف عند مقارنتها ببيانات أخرى .

### Classification -

- هو تصنیف البيانات الى فئات مختلفة، وتم علمیات التصنیف بناءً على محتويات هذه البيانات أو نوعها .
- فإذا كانت صوت فانها تتنقل الى فئة معینة واذا كانت فيديو فانها تتنقل الى فئة مختلفة .



يتم اضافة علامات أو أرقام الـ **Marking** في :

### الطبقة الثانية Layer 2

يتم اضافة الارقام داخل الفريم المغلق بـ 802.1Q ويكون في الجزء المسمى بـ **(CoS)**.

### الطبقة الثالثة Layer 3

يتم اضافة الارقام في باكت الابيبي 4 او 6 او Type of Service (TOS) (الجزء القديم أو الجديد والذي يسمى بـ IP Precedence (IPP)) .

**القديم :** IP Precedence (IPP)

**الجديد :** Differentiated Services Code Points (DSCP)

يمكن إجراء تصنیف الـ **Classification** عن طريق :

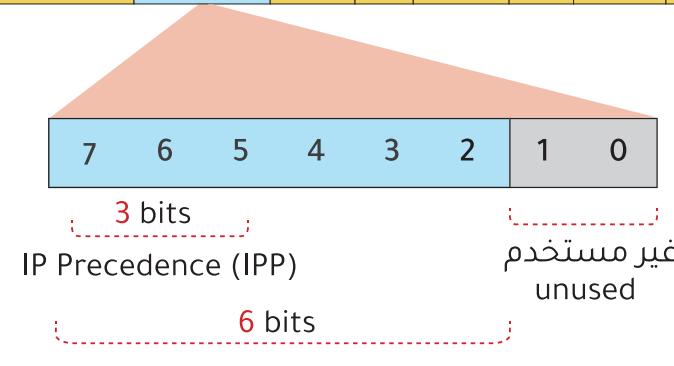
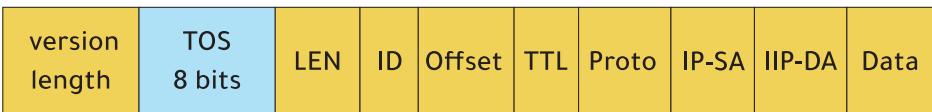
### Access List (ACL)

يمكن استخدام قائمة الدخول في تصنیف البيانات اعتمادا على عناوين الابيبي او ارقام البورت او عناوين الماك ادرس .

### Network Based Application Recognition (NBAR)

تطبيق يمكنه تصنیف البيانات بشكل دقيق جدا اعتمادا على البروتوكول المستخدم في طبقة الـ application .

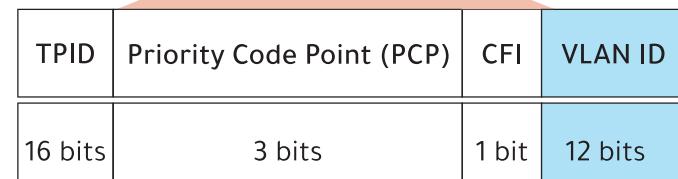
### Layer 3



Differentiated Services Code Points (DSCP)

### Layer 2

فريم الانترنت مع تغليف 802.1Q  
Ethernet Frame with 802.1Q Tag



Class of Service (CoS)

## Layer 2

فريم الايثرنت مع تغليف 802.1Q  
Ethernet Frame with 802.1Q Tag



TPID	Priority Code Point (PCP)	CFI	VLAN ID
16 bits	3 bits	1 bit	12 bits

هذه القيمة هي التي تحدد أولوية حركة المرور بشكل أساسي PCP<sup>X</sup>

تعني حركة مرور عادية وهي ذات أولوية عادية وهي أيضاً افتراضية . رقمها في الحقل PCP0

البيانات ذات أهمية ، رقمها في الحقل PCP2

إشارة بدء الاتصال الصوتي ، رقمها في الحقل PCP3

الفيديو ، رقمها في الحقل PCP4

الصوت ، رقمها في الحقل PCP5

## : Marking Layer 2

طريقة وضع الأرقام وأولويات حركة المرور في هذه الطبقة .

لتعرف كم قيمة أولوية تعطينا الـ 3 bits :

$$2^3 = 8$$

$$2 \text{ أوس } 3 = 8 \text{ قيم ( } 0 - 7 \text{ )} .$$

إذا 3 بات تعطينا 8 قيم في أولوية حركة مرور البيانات

قيمة الاولوية أو قيمة PCP Value / Priority	نوع حركة المرور Traffic Type
0 (default) (lowest) (الأقل)	Best effort
1	Background
2	Critical Data
3	Call Signaling
4	Video
5	Voice
6	Internet control (Routing)
7 (highest) (الأعلى)	Network control

**: Marking Layer 3**

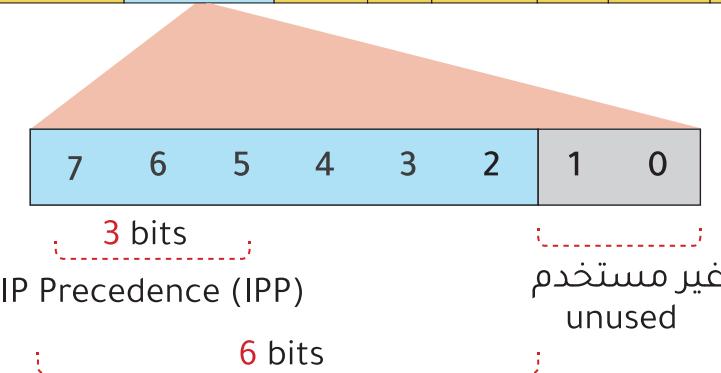
طريقة وضع الارقام وأولويات حركة المرور في هذه الطبقة .

لنتعرف كم قيمة أولوية تعطينا لـ 6 bits :

$$2^6 = 64$$

2 أوس 3 = 64 قيمة ( 63 - 0 ) .

اذا 6 بات تعطينا 64 قيمة في أولوية حركة مرور البيانات .

**Layer 3**

Differentiated Services Code Points (DSCP)

**IP Precedence (IPP) TOS**

كان هو المستخدم في تصنیف اولويات حركة المرور ولكن الـ 3 بات كانت لا تکفي لاعطاء اولوية للبيانات .

- الـ 3 بات تعطی 8 قیم في الاولوية وهي نفس قیم PCP أو Class of Service (CoS) الـ .

**Differentiated Services Code Points (DSCP) TOS**

هو المستخدم الان والمعتمد عند إعداد الـ QoS في الاجهزة الحديثة ومؤلف من 6 بات .

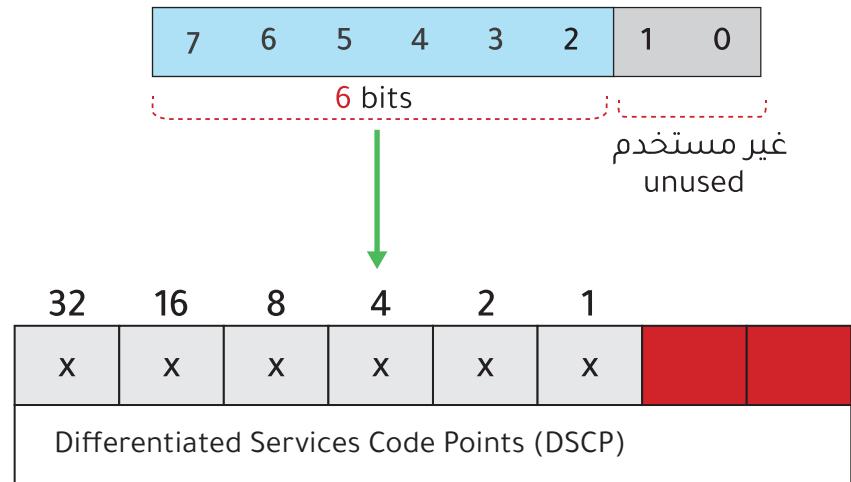
## default forwarding (DF) 01

هي تمثل البيانات العادية التي ليست بها اي أهمية أو أولوية عند تمرير البيانات . وتكون قيمتها 0

32	16	8	4	2	1
0	0	0	0	0	0

نظام الباینری = 000000

نظام العشري = 0



## Expedited Forwarding (EF) 02

هذا القسم يمثل البيانات التي لا تحتمل التأخير Delay أو التأخير المتغير او المقطوع jitter او الخسارة loss مثل بيانات الصوت . ولها قيمة واحدة هي 46.

32	16	8	4	2	1
1	0	1	1	1	0

(Binary) نظام الباینری = 101110

(Decimal) نظام العشري = 46 =  $32 + 8 + 4 + 2$

الـ DSCP مؤلفة من 6 بت والتي سمحتنا بـ 64 قيمة .  
وتم تصنيف هذه القيم الى 4 أقسام :



## مثال

4	2	1	<b>2</b>	<b>1</b>			
0	1	1	<b>0</b>	<b>1</b>	0		

**AF31**

- رقم احتمالية سقوط البيانات هو 1
- رقم فئة أولوية تمرير البيانات هو 3

النظام الثنائي      النظام العشري  
**AF31**      |      26      |      011010

الرقم 26 هو مجموع جزء  
أو DSCP كامل

32	16	8	4	2	1		
0	1	1	<b>0</b>	<b>1</b>	0		

$$26 = 16 + 8 + 2$$

- AF31 أو DSCP26 تكتب أيضاً

### Assured Forwarding (AF) 03

هذا القسم يعطينا أربع فئات من حركة مرور البيانات وكل فئة تعطينا 3 مستويات لإحتمال أو أسبقية سقوط الحزم أو drop Precedence و خسارتها أثناء إزدحام البيانات .

4	2	1	<b>2</b>	<b>1</b>			
x	x	x	y	y	0		

**AFxxy**

: الصفر ثابت لا يتغير

و : رقم احتمالية سقوط البيانات أو Drop Probability .

x : رقم فئة أولوية تمرير Class البيانات

## جدول أولويات حركة مرور البيانات واحتمالات سقوط الحزم

فئات أولوية تمرير البيانات	إحتمال سقوط الحزم قليلة Low Drop Probability			إحتمال سقوط الحزم متوسطة Medium Drop Probability			إحتمال سقوط الحزم عالية High Drop Probability		
	AF	عشري Decimal	ثنائي Binary	AF	عشري Decimal	ثنائي Binary	AF	عشري Decimal	ثنائي Binary
Class 4 أعلى أولوية Highest priority	AF41	34	100 010	AF42	36	100 100	AF43	38	100 110
Class 3	AF31	26	011 010	AF32	28	011 100	AF33	30	011 110
Class 2	AF21	18	010 010	AF22	20	010 100	AF23	22	010 110
Class 1 أقل أولوية Lowest priority	AF11	10	001 010	AF12	12	001 100	AF13	14	001 110

مثال 2 :  
ما هو الـ DSCP للرقم AF43 ؟  
الحل :

$$\begin{aligned}DSCP &= (8 * 4) + (2 * 3) \\DSCP &= 32 + 6 \\DSCP &= 38\end{aligned}$$

مثال 1 :  
ما هو الـ DSCP للرقم AF21 ؟  
الحل :

$$\begin{aligned}DSCP &= (8 * 2) + (2 * 1) \\DSCP &= 16 + 2 \\DSCP &= 18\end{aligned}$$

هذه المعادلة لاستخراج الـ DSCP في حال معرفة الـ AFxy :

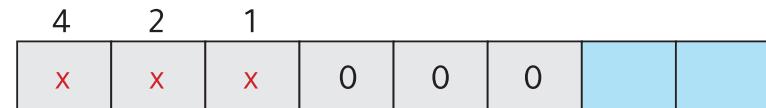
$$\text{AFxy} \\DSCP = (8 * x) + (2 * y)$$

## Class Selector (CS)

04

CS Value	IP Precedence (IPP) Value	DSCP Value
CS0	0	0
CS1	1	8
CS2	2	16
CS3	3	24
CS4	4	32
CS5	5	40
CS6	6	48
CS7	7	56

هذا التصنيف خاص بالأجهزة التي تريد التعامل مع أجهزة أخرى تعتمد على الـ IP Precedence من النوع القديم (IPP) لكي يتم التوافق بالطريقة القديمة.



- يستخدم فقط 3 بات (3 bits) ليعطينا 8 قيم CS7 (7 - 0 ) يعني من CS0 الى

- هذه أهم القيم التي تناصح بها سيسكو عند إجراء الـ Marking للبيانات :

Standard Recommendations:

**EF**: Voice payload.

**AF4x**: Interactive video.

**AF3x**: Streaming video.

**AF2x**: High priority data.

**CS0**: Standard data.

صفوف الانتظار تنقسم الى نوعين :  
Hardware Queue - 1

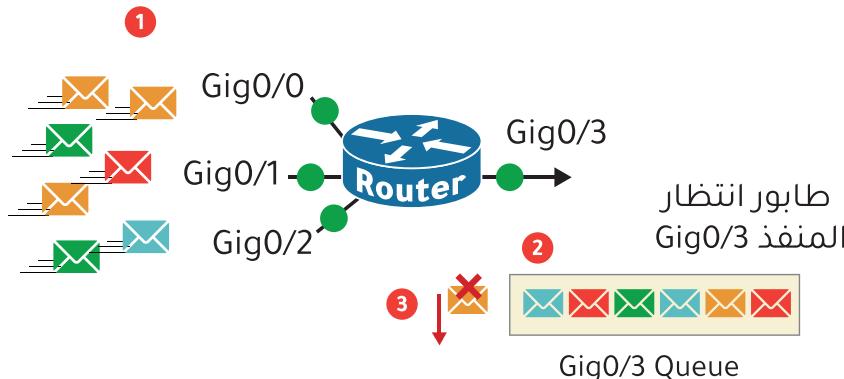
يسمى (Tx-Ring Queue) وهو موجود في كل منفذ من منافذ الجهاز.

Software Queue - 2

هو خاص بـنظام تشغيل الجهاز نفسه ويتم فيه معالجة طوابير الانتظار .

# ما هو الـ ? Tail Drop

هو إسقاط الحزم عندما لا تكون هناك مساحة كافية في طابور الانتظار .

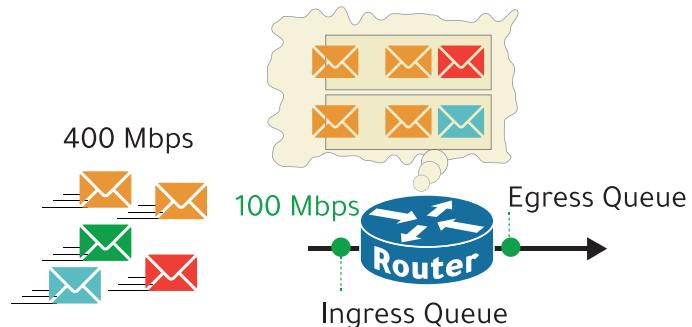


## Congestion Management Queuing - Scheduling



نقصد بها طابور انتظار أو قائمة انتظار هي آلية تسمح بالتحكم وإدارة البيانات عند الازدحام في أجهزة الشبكة.

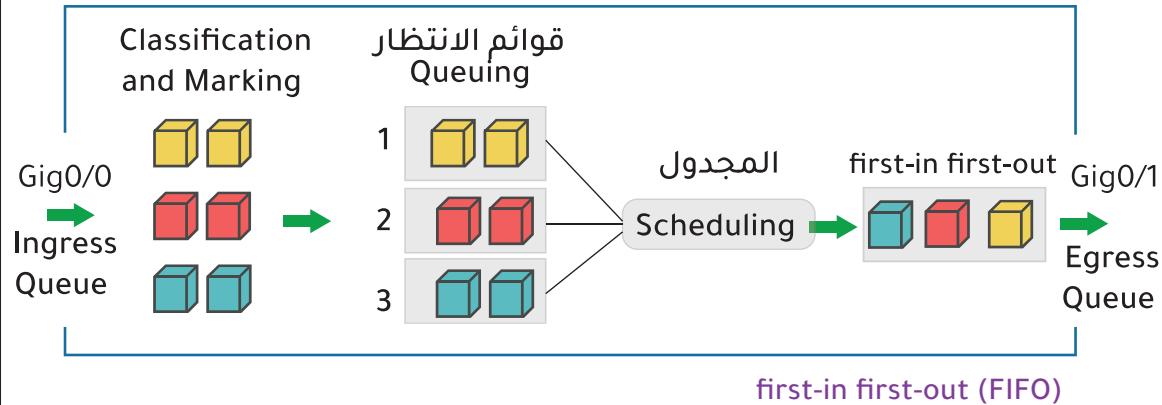
- عندما يستلم منفذ حزم بيانات اكبر من مقدرة وسرعة المنفذ على معالجتها سوف يتم إنشاء صفوف انتظار أمام المنفذ لمنع ازدحام البيانات ومعالجتها وإرسالها لاحقا .



تسمى المنفذ التي فيها طابور انتظار :

: هي قائمة انتظار الدخول ( الإستقبال).

: هي قائمة انتظار الخروج ( الإرسال ) .



هي الترتيب في الارسال ، يعني الحزمة التي تدخل الصنف أولا هي التي سوف يتم ارسالها وهكذا بالترتيب

### Scheduling

عملية تنظيم وجدولة حزم قوائم الانتظار واضافتها الى قائمة الانتظار الداخلية للمنفذ استعدادا لارسالها للجهاز الآخر، وتم الجدولة بناء على معلومات الـ QoS الخاصة بها .

توجد نوعين لعملية الجدولة :

#### Strict priority scheduling 01

في هذا النوع يتم تفريغ الطابور الاول وإرساله بشكل كامل ومن ثم الانتقال لتفريغ الطابور الثاني ، وقبل الانتقال للطابور الثالث يتأكد من الطابور الاول اذا وجد فيه حزمة بيانات عاد للدول او اذا لم يجد يكمل للثالث وهكذا .

- العيب فيه ان الطوابير الاخرى سوف تتأخر في الدور في حال كانت الحزم مستمرة في الاول والثاني .

#### Round-robin scheduling 02

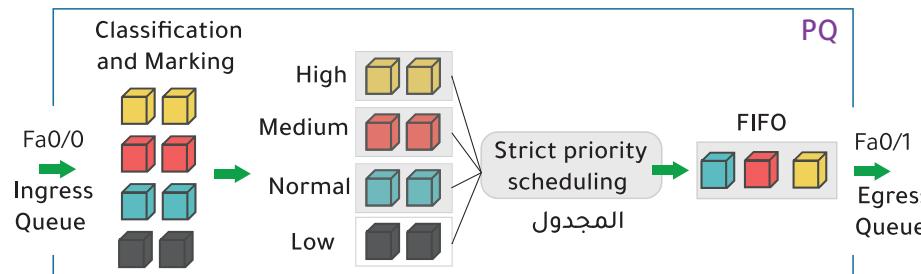
في هذا النوع يتم تفريغ الطابور الأول وإرساله بشكل كامل ثم الثاني ثم الثالث حتى ينتهي من جميع الطوابير ويعود من جديد للدول وهكذا .

## أنواع أنظمة الطابور

- 1 • First In First Out (FIFO) Queuing.
- 2 • Priority Queuing (PQ).
- 3 • Custom Queuing (CQ).
- 4 • Weighted Fair Queuing (WFQ).
- 5 • Class-Based WFQ (CBWFQ).
- 6 • Low-Latency Queuing (LLQ).

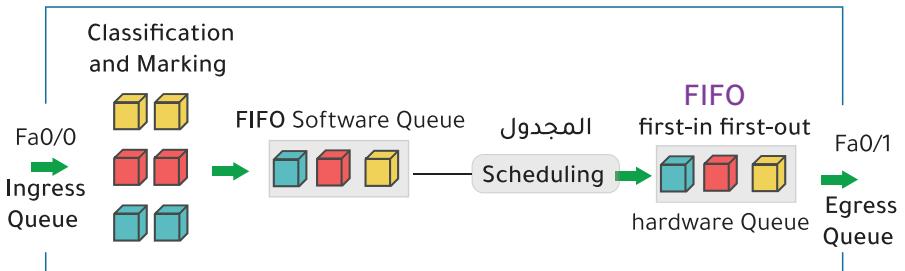
### Priority Queuing (PQ)

- هذا النوع يتم فيه إنشاء 4 طوابير انتظار ذات أولويات مختلفة.
- High - Medium - Normal (default) - Low
  - يتم تفريغ الطابور ذو الأولوية العالية الأولى ثم الطابور الثاني في الأولوية ولا ينتقل للطابور الثالث حتى يتتأكد من فراغ الطابور الأول



### First In First Out (FIFO) Queuing

- في هذا النوع يتم إنشاء طابور من نوع Software Queue لتخزين البيانات بشكل مؤقت قبل إرسالها إلى الطابور الرئيسي hardware Queue .
- هذا النوع افتراضي في المنفذ التي لها باندويث أكبر من 2 ميقا بت.



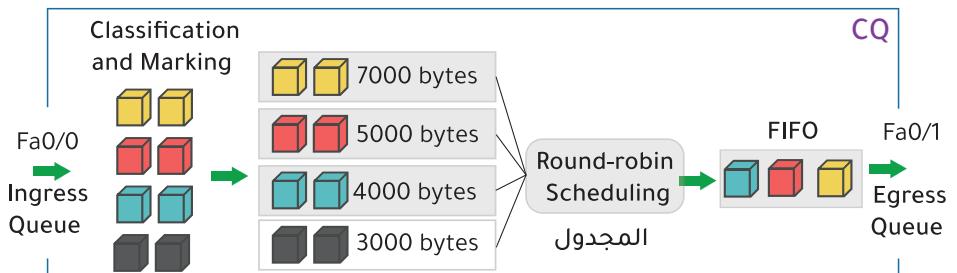
### Weighted Fair Queuing (WFQ)

- هذا النوع يتم فيه إنشاء الطوابير من نوع Software Queue بشكل تلقائي اعتمادا على تدفق البيانات data flow .
- يقوم أيضا بتقسم الباندويث بشكل تلقائي على طوابير أو صفوف الانتظار.
  - يمكن إنشاء 256 صف .

- هذا النوع افتراضي في المنفذ التسلسلي Serial Interface التي فيها الباندويث أقل من 2 ميقا بت.

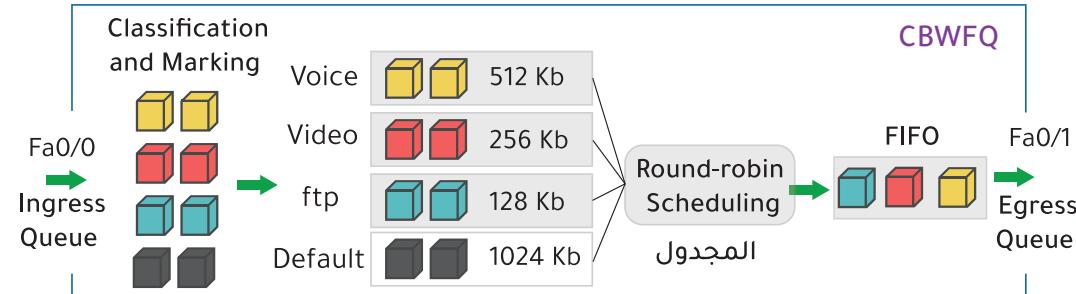
### Custom Queuing (CQ)

- هذا النوع يتم فيه إنشاء 16 صف أو طابور انتظار وتحديد كمية البيانات التي يمكن معالجتها من كل صف قبل الانتقال إلى الصف الآخر وبطريقة Round-robin

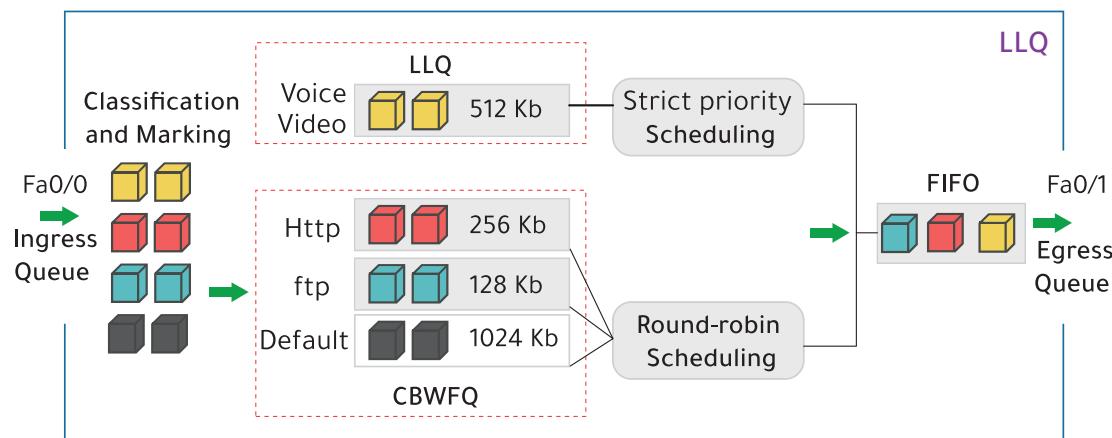


### Class-Based WFQ (CBWFQ)

هذا النوع يتم فيه إنشاء كلاسات classes أو فئات وتحديد نوع البيانات داخل هذا الكلاس اعتماداً على access list او NBAR .



- يتم انشاء طابور لكل كلاس واعطائه اسم خاص به مثل الكلاس الاول للصوت - Voice - الكلاس الثاني للفيديو وهكذا .. اما الكلاس الاخير يكون افتراضي للبيانات الاخرى .
- يمكن انشاء حتى 64 صف .
- يتم توزيع الباندويث لكل صف بشكل يدوي ، ويتم تحديدها بالكيلو بايت أو بالنسبة المئوية .
- يتم الجدولة باستخدام الطريقة . Round-robin scheduling
- هذا النوع غير مناسب لبيانات الصوت والفيديو .



### Low-Latency Queuing (LLQ)

هذا النوع يشبه النوع السابق CBWFQ لكنه يتميز بصف أو عدة صفوف لها جدولة خاصة ومستمرة للبيانات الأكثر أهمية مثل الصوت والفيديو وتستخدم الجدولة طريقة ال Strict priority .

- يتم الجدولة في الصفوف الباقية باستخدام الطريقة Round-robin

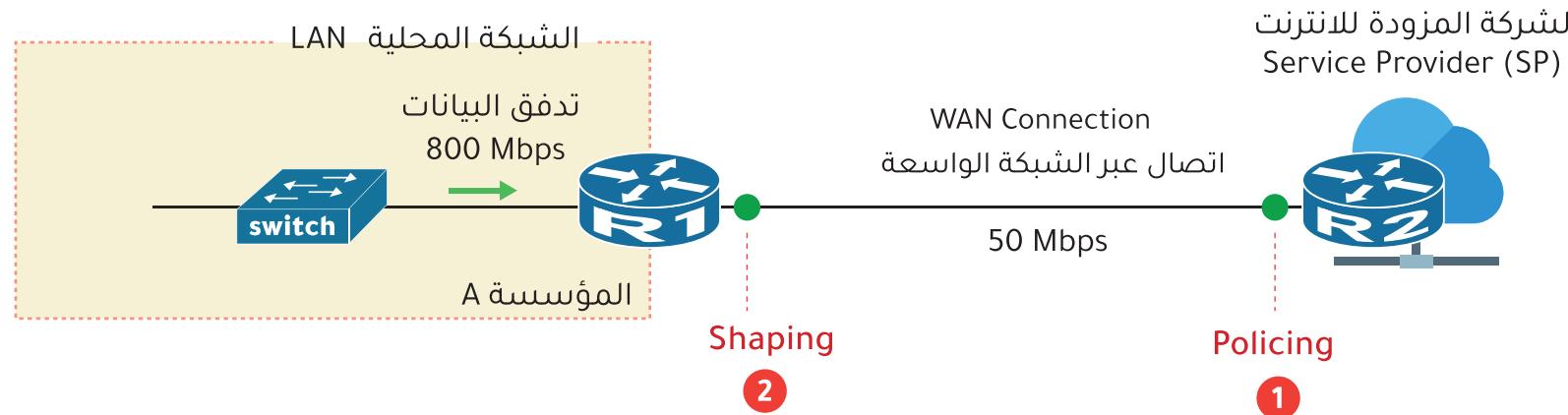
## Shaping

هي آلية تعمل على تأخير بعض حزم البيانات التي تجاوزت المعدل وذلك بتخزينها في المخزن المؤقت لكي يتم ارسالها بتوافق مع الجهاز الآخر. انظر للشكل الذي بالأسفل.

## Shaping and Policing

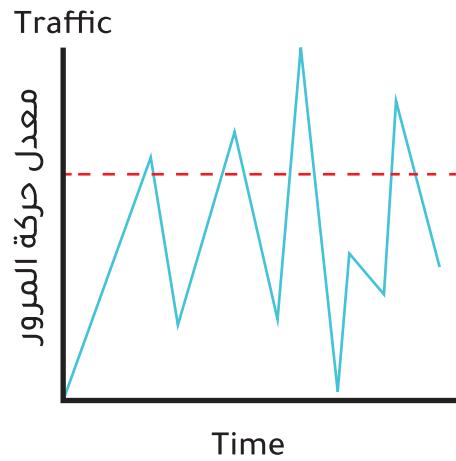
## Policing

هي آلية تحكم ومراقبة حركة المرور لحزم البيانات حسب معدل معين بحيث لو زادت هذه الحزم عن المعدل المعين سوف يتم اسقاط هذه الحزم . انظر للشكل الذي بالأسفل

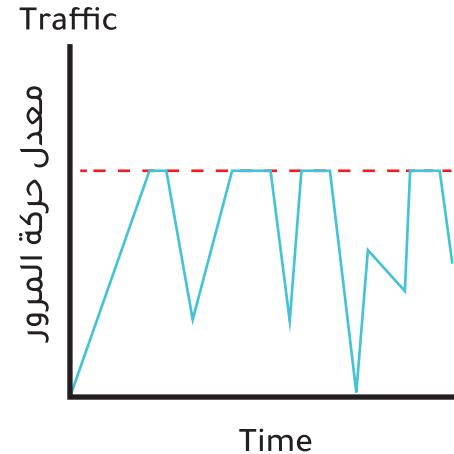


تقوم المؤسسة بتطبيق الـ Shaping على هذا المنفذ لكي تأخر بعض الحزم الزائدة عن المتفق عليه وتخزينها مؤقتا بحيث يكون الارسال لجميع الحزم متوافقا مع معدل النقل الـ 50 ميغا بت في الثانية ولا تزيد عنه .

تقوم الشركة المزودة للانترنت بتطبيق الـ Policing على هذا المنفذ لكي تمنع زيادة معدل نقل البيانات عن المتفق عليه وهو 50 ميغا بت .

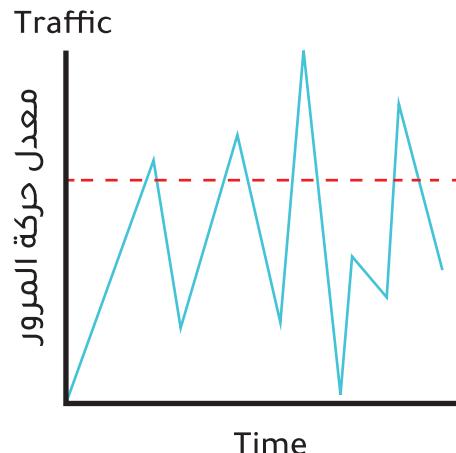


Policing  
→

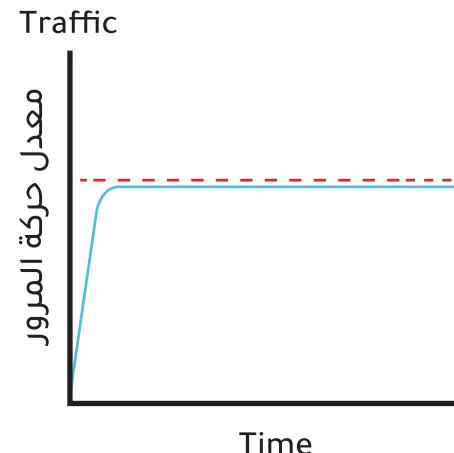


لاحظ ان Policing لم يسمح بتجاوز المعدل ولم يعمل على تخزين البيانات بل اسقط بعض الحزم الزائدة عن المعدل واصبح الارسال غير مستقر.

- **الخط الاحمر** هو الحد المعين الذي تم الاتفاق عليه ولنقل 50 ميكابت
- **الخط الازرق** هو معدل نقل البيانات .



Shaping  
→



لاحظ ان Shaping كيف جعل الارسال في حالة مستقرة .

## Congestion Avoidance Tools

أدوات تجنب الازدحام

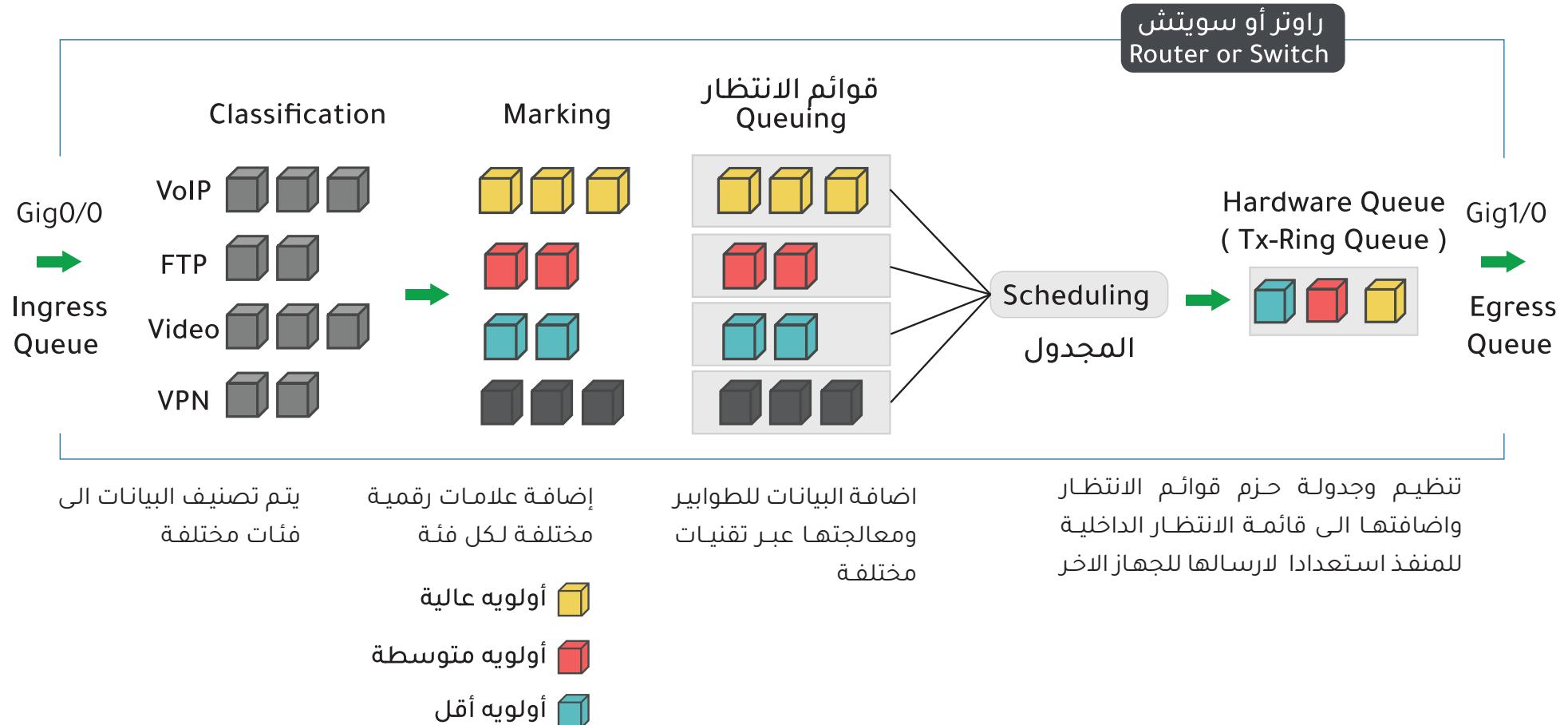
### Weighted Random Early Detection (WRED)

يقوم بحذف الباكت أو الحزم عندما يوشك صف الانتظار على الامتناع ، ويكون الحذف حسب قيمة الاولوية ( IP Precedence ) أو ( DSCP ) ( IPP ) .

### Random Early Detection (RED)

يقوم بحذف الباكت أو الحزم بشكل عشوائي عندما يوشك صف الانتظار على الامتناع بدون النظر الى أهمية أولوية الإرسال وذلك لتجنب الازدحام في البيانات .  
- هذا النوع غير مدعوم في أجهزة سيسكو .

## مختصر لتقنية الـ QoS



**النظام السداسي عشر (Hexadecimal)**

هو نظام ذو الأساس 16 و الذي يتكون من 16 حرف ورقم . وهي كالتالي :  
 ( 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 البايطة (0x) مثل 0x45A8D وتعني ان هذا الرقم من النظام السداسي عشر .
- نجد استخدام هذا النظام في الأبيي الاصدار السادس IPv6 وايضا في الماك ادرس Mac address .

**النظام الثنائي Binary****النظام العشري Decimal****النظام السداسي عشر Hexadecimal****النظام الثنائي Binary System**

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

- يسمى أيضا ب base 2
- قد تجد أمام الرقم أو الرقمين 0 و 1 هذه البايطة (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

**النظام العشري 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 البايطة (0d) مثل 0d223 وتعني ان هذا الرقم من النظام العشري .

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

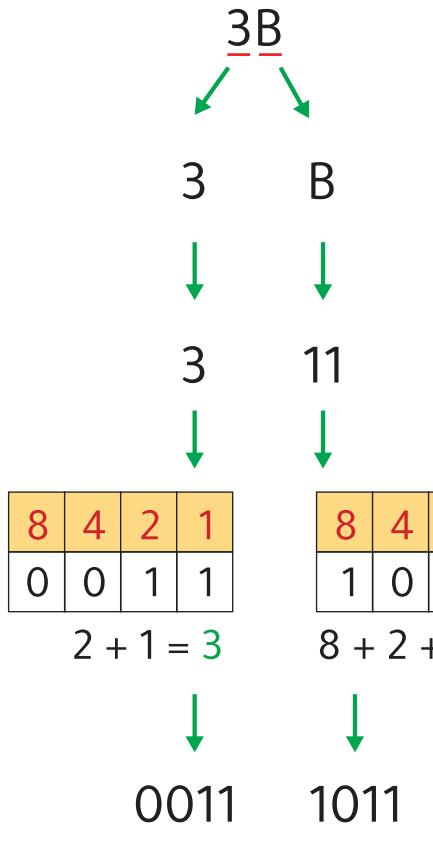
0.0.0.0

255.255.255.255

النظام العشري Decimal System	النظام الثنائي Binary System	النظام السداسي 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

## التحويل من النظام السداسي عشر الى النظام الثنائي

Convert Hexadecimal to Binary



1 - نقسم الرقم الى جزأين

2 - بالرجوع لجدول النظام السداسي عشر يظهر لنا ان  $B = 11$

3 - نحول الرقم الى النظام الثنائي

4 - يظهر لنا الرقم في النظام الثنائي كامل

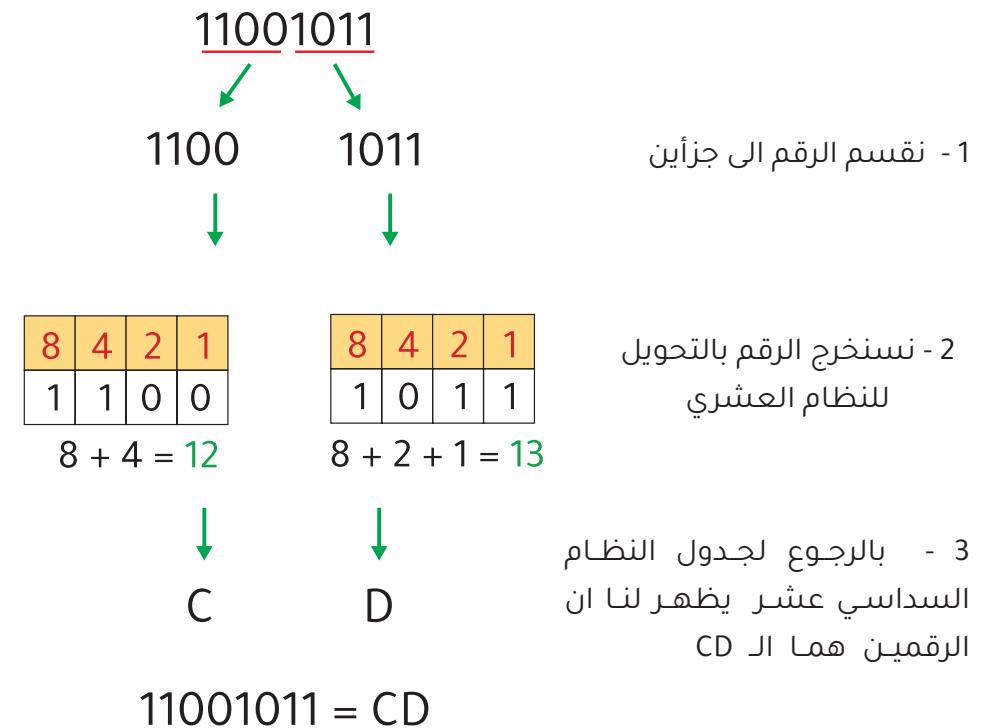
## التحويل من النظام الثنائي الى النظام السداسي عشر

Convert Binary to Hexadecimal

طريقة التحويل من النظام الثنائي الى النظام السداسي عشر:

مثال:

تحويل هذا الرقم الثنائي : 11011011



1 - نقسم الرقم الى جزأين

2 - ننسخنخ الرقم بالتحويل للنظام العشري

3 - بالرجوع لجدول النظام السداسي عشر يظهر لنا ان الرقمين هما الـ CD

النظام العشري Decimal System	النظام الثنائي Binary System	النظام السداسي عشر (Hexadecimal)
12	1100	C
13	1101	D



## بروتوكول IPv6

IPv6 هو إصدار جديد ومحسن من بروتوكول IP.

- سبب اصدار هذا البروتوكول هو أنه مع تطور وزيادة أعداد المستخدمين والأجهزة أصبحت عناوين الـ IPv4 غير كافية.

- الـ IPv6 يستخدم 128 بت في 8 مجموعات.

- الـ IPv6 يستخدم النظام السنتي عشربي والمكون من 16 حرفاً ورقم، وهي كالتالي : (A.B.C.D.E.F.0.1.2.3.4.5.6.7.8.9)

- في الـ IPv6 عدد المجموعات = 8 ويفصل بين كل مجموعة بعلامة (:).

- كل رقم حجمه 4 بت.

- كل مجموعة حجمها 16 بت

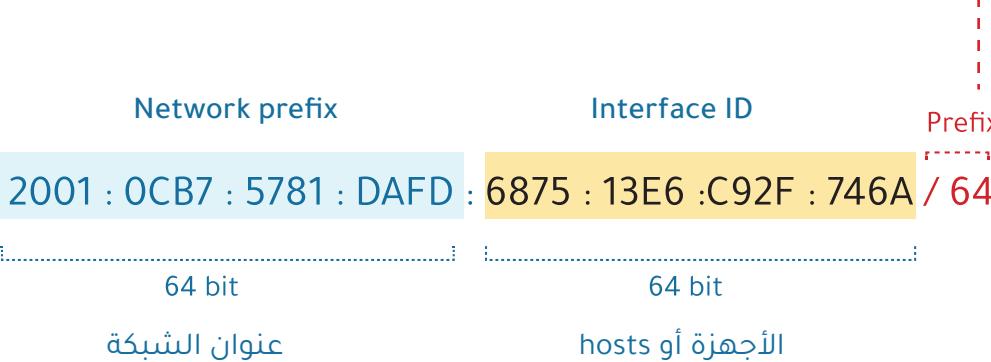


### ملاحظة :

- لا يوجد في بروتوكول IPv6 :
  - . arp
  - . nat

- 1 - قسم ثابت لعنوان الشبكة والمسمى Network prefix .
- 2 - قسم للأجهزة والمسمى بالـ (host) interface id وهذا القسم يختلف من جهاز آخر .

الـ **Prefix** هو الذي يحدد عدد الـ (bits) الثابتة في قسم عنوان الشبكة .



في هذا الجزء هناك 3 احتمالات لانشاءه :

- 1 - **يدوي Manual** : يكون الديني منشأً من قبل المهندس .
- 2 - **EUI-64** : طريقة متبعة في أجهزة سيسكو وهي إنشاء جزء الـ interface id (host) من الماك أدرس الخاص بالمنفذ بشكل تلقائي .
- 3 - **عشوائي Random** : وهذا يتم تلقائي وعشوائي بواسطة نظام ويندوز 10 .

### ≡ سبب عدم استخدام علامة (::)

أنظر لهذا العنوان :

746A :: 6005 :: 2001

- نعرف أن عدد مجموعات عنوان الـ ipv6 هي 8 مجموعات وفي العنوان الذي بالأعلى 3 مجموعات ومتبقى 5 مجموعات **فالسؤال الان :**

**كل علامة (::) تدل على كم مجموعة؟!!!!!!**

لذلك تم منع وجود علامتين اختصار (::) لهذا السبب لأننا لن نستطيع معرفة عدد المجموعات لكل علامة في حال وجودهما مع بعض ولذلك نكتفي بعلامة اختصار واحدة فقط .

### ≡ إعادة عنوان الـ ipv6 بعد الاختصار

هذا عنوان ipv6 مختصر ونريد كتابته بشكل كامل :  
FD20 :: 3 : AC: 0 : 1678

أولاً : نضع الأصفار من اليسار للمجموعات التي فيها عدد أقل من 4 أعداد ، مثل المجموعة اللي فيها رقم (3) فهي ناقصة منها 3 أعداد .

FD20: 0003 : 00AC: 0000 :: 1678

ثانياً : نحسب كم المجموعات الموجودة الان :  
الموجود 5 مجموعات .

اذا بقي 3 مجموعات والتي تم اختصارها بعلامة (::) وسيتم تعويضها بالأصفار .

FD20 : 0000 : 0000 : 0003 : 00AC: 0000 : 1678

### ≡ طرق اختصار عنوان الـ IPv6

1 - يمكن إزالة الأصفار التي في بداية كل مجموعة من اليسار

2001 : 0CB0 : 0081 : 0AFD : 6005 : 00E6 : 002F : 746A



2001 : CB0 : 81 : AFD : 6005 : E6 : 2F : 746A

-----  
2 - يمكن إزالة المجموعة التي كلها أصفار ووضع علامة (::)  
هذا الاختصار مسموح لمرة واحدة ، يعني لايمكن وضع علامة (::) مرتين .

2001 : 0000 : 0000 : 0000 : 0000 : 0005 : 0000 : 002F : 746A

لاحظ تم اختصار الثلاث  
خانات ووضع علامة (::)



2001 :: 6005 : 0 : 2F : 746A

هنا وضعنا فقط صفر لأننا لن نستطيع  
الاختصار بالعلامة (::) مرة أخرى

### - مثال آخر مع Prefix مختلف :

2001 : 0CB0 : 0081 : 0AFD : 6005 : 00E6 : 002F : 746A / **56**

- عرفنا أن كل رقم يساوي 4 بت :

2001 : 0CB0 : 0081 : 0AFD : 6005 : 00E6 : 002F : 746A / **56**



$$\begin{array}{r} \text{48} \\ + \quad 8 \\ \hline = 56 \end{array}$$

- نحول جزء الـ hosts للأصفار

2001 : 0CB0 : 0081 : 0A00 : 0000 : 0000 : 0000 / **56**

- ثم نختصرها باضافة علامة (::)

2001 : 0CB0 : 0081 : 0A00 :: / 56

### ≡ طريقة معرفة عنوان الشبكة بمعرفة الـ Prefix

مثلًا لدينا هذا العنوان :

2001 : 0CB0 : 0081 : 0AFD : 6005 : 00E6 : 002F : 746A / **64**

- الـ Prefix هو 64 يعني عدد البتات 64 بت ، وعرفنا أن كل رقم يمثل 4 بت :

2001 : 0CB0 : 0081 : 0AFD : 6005 : 00E6 : 002F : 746A



64 بت

هذا هو عنوان الشبكة

64 بت

hosts للجهاز أو الـ

- نحول جزء الـ hosts للأصفار ثم نختصرها باضافة علامة (::)

2001 : 0CB0 : 0081 : 0AFD :: /64

## - مثال آخر مع Prefix مختلف :

2001 : 0CB0 : 0081 : 0AFD : 60B5 : 00E6 :002F : 746A / 73

- عرفنا أن كل رقم يساوي 4 بت ونحتاج ل 73 بت :

2001 : 0CB0 : 0081 : 0AFD : **60B5** : 00E6 :002F : 746A / 73



2001 : 0CB0 : 0081 : 0AFD : **6085** : 00E6 :002F : 746A / 73

- نحول جزء الـ hosts لأصفار ثم نختصرها باضافة علامة (::)

2001 : 0CB0 : 0081 : 0AFD : **6080** :: / 73

## إعدادات الـ IPv6

### 1- يدوى : Manual

- يكون هنا الايبي معروف لدى المهندس ليقوم بادخاله في الجهاز ويتم ادخاله بنفس طريقة اعداد الـ IPv4 ولكن يتم زيادة أمر في الـ IPv6 في وضع الاعداد

R1(config)# ipv6 unicast-routing

- لدينا هذا النموذج

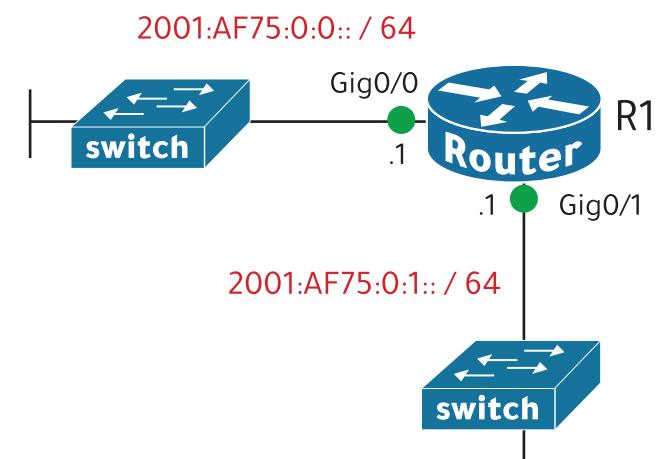
```
R1# conf t
R1(config)# ipv6 unicast-routing
R1(config)# int Gig0/0
R1(config-if)# ipv6 add 2001:AF75:0:0::1/64
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# int Gig0/1
R1(config-if)# ipv6 add 2001:AF75:0:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1# wr
```

هذا الامر يسمح للراوتر بالتعامل مع ايبيات IPv6 وايضا تمرير وتجيه البيانات

```
R1# sh ipv6 int br
GigabitEthernet0/0      [up/up]
  FE80::201:42FF:FE32:7801
  2001:AF75::1
GigabitEthernet0/1      [up/up]
  FE80::201:42FF:FE32:7802
  2001:AF75:0:1::1
```

هذه الايبيات التي تم ادراجها للمنفذ



## EUI-64 - 2

EUI-64 هي اختصار ل Extended Unique Identifier و هي طريقة لتحويل عنوان الماك أدرس إلى جزء الـ interface id (host) بشكل تلقائي .

- كل منفذ في الجهاز له عنوان ماك أدرس .

- يقوم الجهاز بهذه العملية بشكل تلقائي ولكن يجب علينا معرفة طريقة التحويل :

- طبعا حجم الماك أدرس هو 48 بت وحجم الـ interface id هو 64 بت ، لذلك نحتاج زيادة 16 بت للماك أدرس لكي يكون نفس حجم الـ interface id

الماك أدرس  
Mac Address

12E6 5A2F 746A

48 بت

بعد عملية  
التحويل

Network prefix

Interface ID

2001:0CB7:5781:DAFD : 10E6:5AFF:FE2F:746A / 64

64 bit

64 bit

12E6 5A2F 746A

نقسم العنوان الى جزأين

12E6 5A**FF** FE2F 746A

نضيف هذه الاحرف  
بالوسط  
FFFFE

12E6 5A**FF** FE2F 746A

نعكس البت رقم 7 :  
- اذا كانت 0 نحولها ل 1  
- اذا كانت 1 نحولها ل 0

0001 0010

نعكس من 1 ل 0

0000

النظام العشري

0

النظام السداسي عشر

## طريقة التحويل

10E6 5A**FF** FE2F 746A

R1

```
R1# conf t
R1(config)# ipv6 unicast-routing
R1(config)# int Gig0/0
R1(config-if)# ipv6 add 2001:AF75:0:0::/64 eui-64
R1(config-if)# no shutdown
R1(config-if)# exit

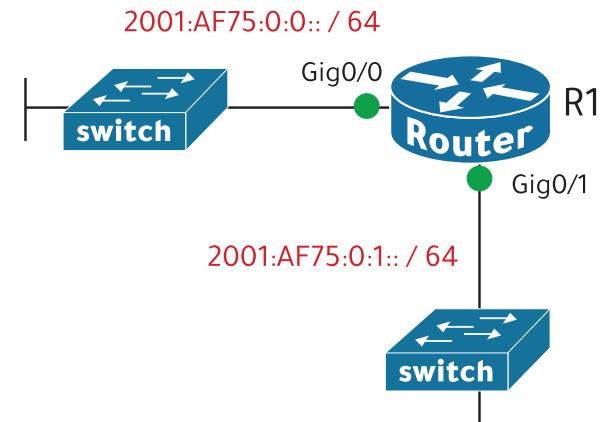
R1(config)# int Gig0/1
R1(config-if)# ipv6 add 2001:AF75:0:1::/64 eui-64
R1(config-if)# no shutdown
R1(config-if)# end
R1# wr
```

نكتب عنوان الشبكة  
(Network id)

نضيف هذا لكي يتم انشاء الـ  
interface id من ماك ادرس  
المنفذ

لدينا هذا النموذج

سنستخدم طريقة الـ EUI-64 لـ انشاء الـ  
interface id



هذا عنوان الـ IPv6 تم إنشاعها بعد استخدام  
EUI-64

R1

```
R1# sh ipv6 int br
GigabitEthernet0/0      [up/up]
  FE80::20A:41FF:FE69:A801
  2001:AF75::20A:41FF:FE69:A801
GigabitEthernet0/1      [up/up]
  FE80::20A:41FF:FE69:A802
  2001:AF75:0:1:20A:41FF:FE69:A802
```

هذا عنوان ماك ادرس للمنفذ Gig0/0 g Gig0/1

R1

```
R1# show interfaces gig0/0
GigabitEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is CN Gigabit Ethernet, address is 000a.4169.a801 (bia 000a.4169.a801)

Router#show interfaces gig0/1
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
  Hardware is CN Gigabit Ethernet, address is 000a.4169.a802 (bia 000a.4169.a802)
```

## Global Unicast Addresses

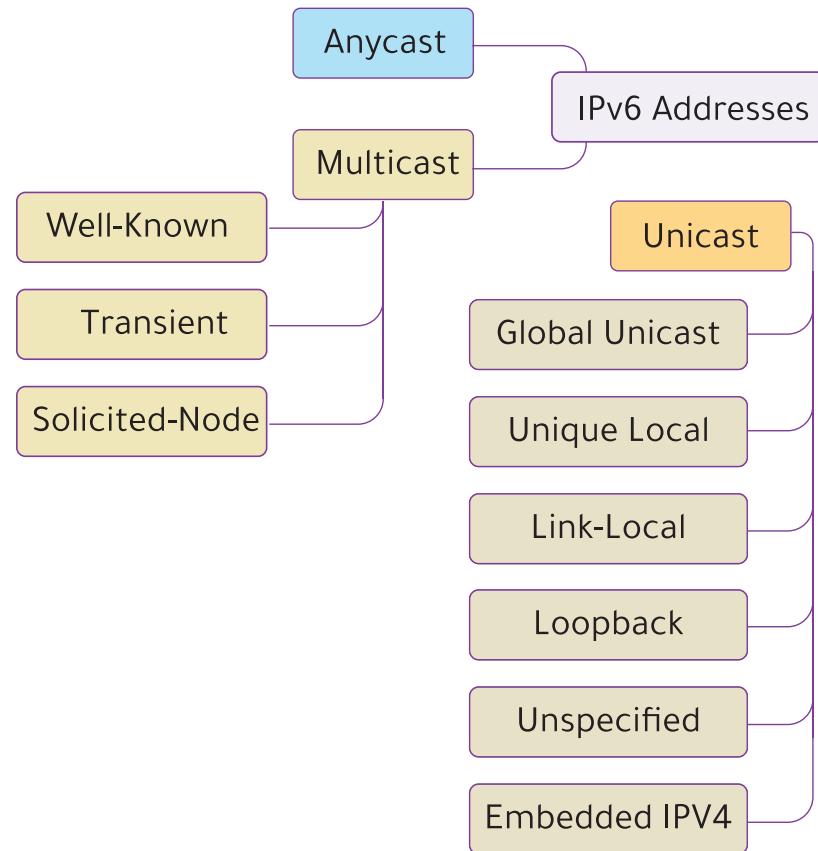
### 1 Unicast

هي عناوين عامة (Public Addresses) يمكن استخدامها عبر الإنترنت.  
- لاستخدام هذه العناوين يجب شراؤها من مزود الخدمة لأنها عناوين عامة.

- العناوين العامة هي  $3000 :: /3$  و  $2000 :: /3$
  - أي عناوين تبدأ بـ 2 أو بـ 3 هي عناوين عامة.
  - نطاق أو مدى هذه العناوين :
- (  $2000 ::$  ) to (  $3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF$  )



## ≡ أنواع عناوين لـ ipv6



- هذه العناوين مثل عناوين الـ APIPA في IPv4 .
- يتم إنشاء جزء id interface من نوع LINK LOCAL في الراوتر باستخدام EUI-64 .
- الأجهزة التي تعمل بنظام ويندوز فإنها تنشئ جزء id interface بشكل عشوائي .
- يتحقق الجهاز من العنوان الذي اختاره لنفسه من نوع LINK LOCAL أنه لا يوجد مثله في الشبكة بواسطة تقنية تسمى بـ : Duplicate Address Detection (DAD) .

## Loopback Addresses

**4** Unicast

- يستخدم لاختبار حزمة البروتوكول على نفس الجهاز.
- عنوانه الوحيد فقط في الـ ipv6 هو : ::1 / 128
- عنوانه في الـ ipv4 هو في مدى هذه الشبكة : 127.0.0.0 / 8

## Unspecified Addresses

**5** Unicast

- يستخدم عندما لا يكون هناك عنوان للجهاز .
- عنوانه في الـ ipv6 هو : ::0
- عنوانه في الـ ipv4 هو : 0.0.0.0

## Unique Local Addresses

**2** Unicast

- هي عناوين خاصة لا يمكن استخدامها عبر الإنترن特 .
- لا تحتاج إلى التسجيل أو الشراء لاستخدامها ويمكن استخدامها داخل الشبكات المحلية الداخلية .
- يتم استخدامها داخل المؤسسات والشبكات الداخلية ولا يمكن السماح لها بالخروج للإنترنت .

- العنوان الخاص تبدأ من FC00 :: / 7
- نطاق أو مدى هذا العنوان :

( FC00 :: / 7 ) to ( FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF )

## Link Local Addresses

**3** Unicast

- هو عنوان من نوع الـ Unicast يستخدم لتمييز منفذ معين عن المنفذ الآخر الواقع في نفس الشبكة .
- كل منفذ يقبل عنوان واحد فقط من نوع link local .
- يمكن للمنفذ استخدام عنوانه لرسال البيانات داخل الشبكة ولكنها لن تخرج من منفذ الراوتر (default gateway) .
- هذه العناوين يتم إنشاؤها تلقائياً على الأجهزة أو المنافذ التي تدعم IPv6 .

- العنوان تبدأ من FE80 :: / 10
- نطاق أو مدى هذا العنوان :

( FE80 :: / 10 ) to ( FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF )

## Multicast

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

- لا يوجد في IPv6 البرودكاست Broadcast ولكن هناك طريقة لإرسال رسالة إلى جميع الأجهزة في الشبكة باستخدام الـ Multicast

- العنوانين تبدأ من **FF00 :: /8**  
 - نطاق أو مدى هذا العنوان :  
 $(\text{FF00 :: /8}) \text{ to } (\text{FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF})$

ipv4 address	ipv6 address	
224.0.0.1	FF00 :: 1	يستخدم للرسالة لكل الأجهزة
224.0.0.2	FF00 :: 2	تستخدمه كل الراوترات
224.0.0.5	FF00 :: 5	يستخدمه بروتوكول الـ OSPF في الراوترات
224.0.0.6	FF00 :: 6	يستخدمه بروتوكول الـ OSPF في عملية الانتخاب DRs / BDRs في الراوترات
224.0.0.9	FF00 :: 9	يستخدمه بروتوكول الـ RIP
224.0.0.10	FF00 :: A	يستخدمه بروتوكول الـ EIGRP

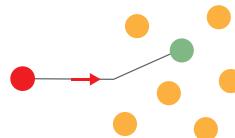
## طرق إرسال البيانات في داخل الشبكات

### Methods of Sending Data in the Network

الإرسال يتم بين مرسل واحد ومستقبل واحد فقط أي انه يتم أخذ البيانات وارسالها إلى الجهاز المطلوب فقط.

#### Unicast

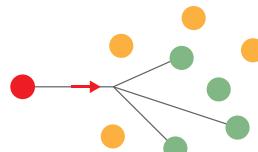
##### One to One



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

#### Multicast

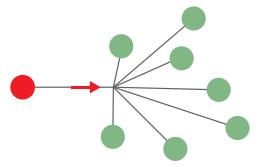
##### one to Many



تعني إرسال البيانات لجميع الأجهزة في الشبكة

#### Broadcast

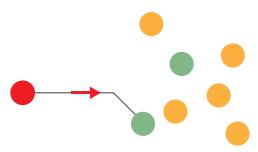
##### one to ALL



فيه يتم إرسال البيانات من الجهاز المرسل إلى أقرب جهاز مستقبل حسب قواعد معينة مثل المسافة أو المسار .

#### Anycast

##### one to one of many



**FF08 : تبدأ من Organization-local**

المجال فيه أوسع من الـ Site-local ويمكن أن يمتد لجميع الشبكات الفرعية للمؤسسة ايضاً. هنا يكون الامر متروك للمهندس لتحديد المجال.

**FF0E : تبدأ من Global**

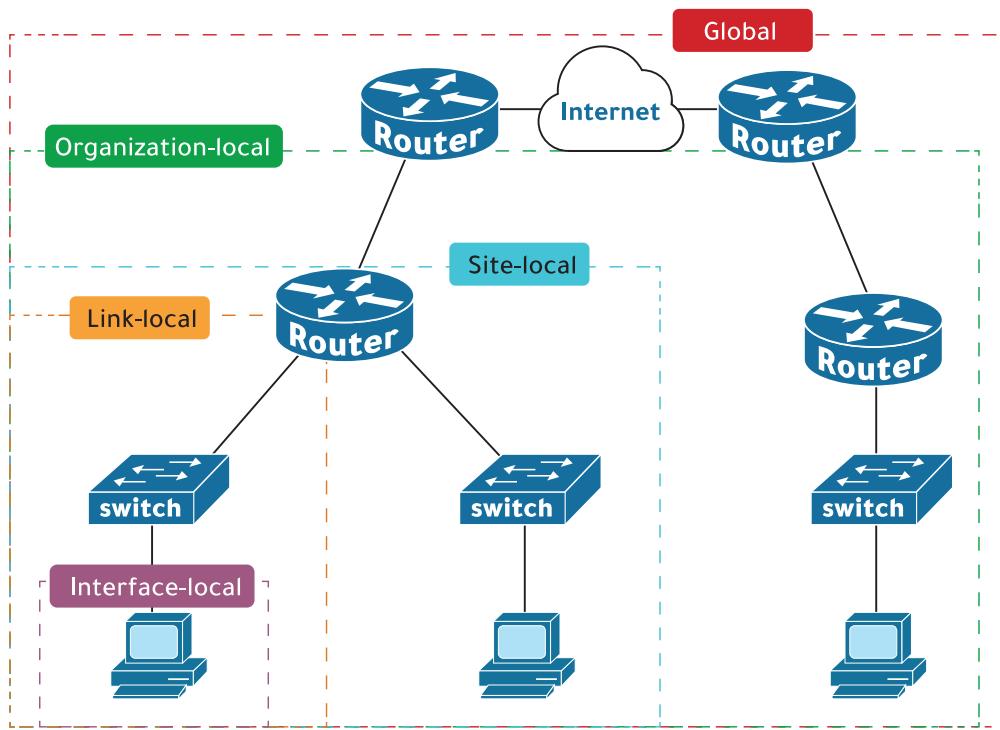
يكون المجال هنا عالمي وأوسع من الـ Organization حيث يمكن ان تنتقل البيانات الى الانترنت ويمكن لـ مستلم يريد استلام هذه البيانات ان يستلمها.

**نطاق أو مجال البث المتعدد****Multicast Address Scope**

الـ Scope هو مجال الذي تنتشر فيه البيانات التي تم ارسالها بواسطة البث المتعدد (Multicast) في داخل الشبكة.

- يتم تحديد هذا المجال عن طريق :  
- عنوان الابيبي نفسه .

- أو من خلال بعض المعلومات التي يتم تزويدها لبروتوكولات التوجيه . هذه المعلومات تساعد جهاز الراوتر في تحديد ان إمكانية تمرير هذه البيانات من شبكة الى اخرى أو ايقافها عند المنفذ .

**مجالات البث المتعدد في الـ ipv6  
Multicast Scope in ipv6****FF01 : تبدأ من Interface-local**

لا تغادر رسائل الـ Multicast الجهاز المحلي أو المنفذ .

- يمكن استخدامه لإرسال حركة المرور إلى خدمة تعمل داخل نفس الجهاز .

**FF02 : تبدأ من Link-local**

مجال الـ Multicast يكون داخل الشبكة المحلية ولا يتم توجيهها بين الشبكات الفرعية الاخرى .

**FF05 : تبدأ من Site-local**

مجال الارسال في الـ Multicast يمر عبر الراوتر الذي يمكن له اعادة التوجيه لشبكة اخرى . هنا يكون الامر متروك للمهندس لتحديد المجال .

## Security Fundamentals



### لماذا نحتاج للأمان في الشبكات ؟

في شبكات المؤسسات أو الشركات نحتاج إلى حماية أجهزتها ومعلوماتها الخاصة من المتسللين أو المهاجمين (الهاكرز) الذين يستهدفون الشبكة عبر البرامج الضارة الباحثة عن أي ثغرة تستغلها في الشبكة لتدمير أو سرقة البيانات .

### CIA (Confidentiality, Integrity, and Availability)

الـ CIA هو نموذج لتطوير سياسة الأمان يتكون من 3 عناصر :

#### 1 - الخصوصية أو السرية Confidentiality

هذا يعني أن المستخدمين المصرح لهم هم فقط من يمكنهم الوصول إلى البيانات .

#### 2 - السلامة أو التكامل Integrity

هذا يعني أنه لا ينبغي التلاعب بالبيانات أو تعديلها عن طريق المستخدمين الغير المصرح لهم .

#### 3 - التوافر Availability

هذا يعني أن شبكة وأنظمة المؤسسة يجب أن تكون متاحة للمستخدمين المصرح لهم .  
مثلا الموظفين يكونوا قادرين على الوصول إلى الموارد الداخلية التي يحتاجون إليها لأداء واجباتهم داخل الشبكة .

## مفاهيم الأمان الأساسية

### • الثغرة الأمنية vulnerability

هي أي ضعف محتمل أو ثغرات في النظام أو المعلومات يمكن أن تهدد خصوصية وسلامة وتوافر البيانات (CIA)

### • الإستغلال Exploit

هو استغلال الثغرات الأمنية التي تحدث في النظام .

### • التهديد Threat

التهديد هو احتمال استغلال الثغرات الأمنية التي تهدد البيانات وتعمل على اتلافها .

### • تقنية الـ mitigation

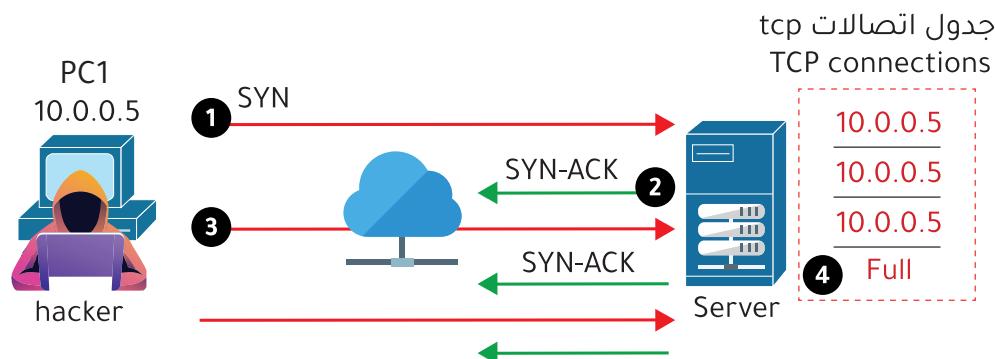
هي تقنية تساعد على الحماية من التهديدات .  
يجب استخدام تقنيات الـ mitigation المناسبة في كل مكان يمكن أن يحدث فيه استغلال للثغرات الأمنية ، مثل أجهزة العميل والخوادم والروابط والسوسيتشات وجدران الحماية .

### • Asset

هي البيانات المهمة وذات قيمة عالية في الشبكة . مثل معلومات البنوك أو بيانات الشركات الخاصة وغيرها .

### 1 - هجمات رفض الخدمة (DoS denial-of-service) attacks

أحد الهجمات الشائعة هي استغلال المصادفة الثلاثية في بروتوكول TCP وذلك باستخدام الـ TCP SYN Flood .  
- تعرفنا أن بروتوكول الـ TCP يستخدم في المصادفة الثلاثية (SYN - SYN-ACK - ACK)



- 1 - يرسل المهاجم عبر بروتوكول TCP رسالة SYN .
- 2 - يستقبل السيرفر الرسالة ويسجلها في جدوله الخاصة ويرسل رسالة SYN-ACK لـ PC1 لكي يكمل الاتصال ولكن رسالة الـ ACK لن تأتيه لأن الهاكر سوف يعيد ارسال الـ SYN بعدد كبير جدا .
- 3 - يكرر المهاجم ارسال رسائل الـ SYN الى السيرفر والسيرفر يرد على كل رسالة حتى يمتلئ جدول اتصالات السيرفر.
- 4 - بعد إمتلاء جدول اتصالات السيرفر تحصل مشكلة رفض الخدمة denial of service

## الهجمات الشائعة Common Attacks

هي التهديدات التي من المحتمل أن تستغل نقاط الضعف لتهديد سرية أو سلامة أنظمة ومعلومات المؤسسات والشركات .



هناك الكثير من الهجمات ولكن هذه بعض من الهجمات الشائعة :

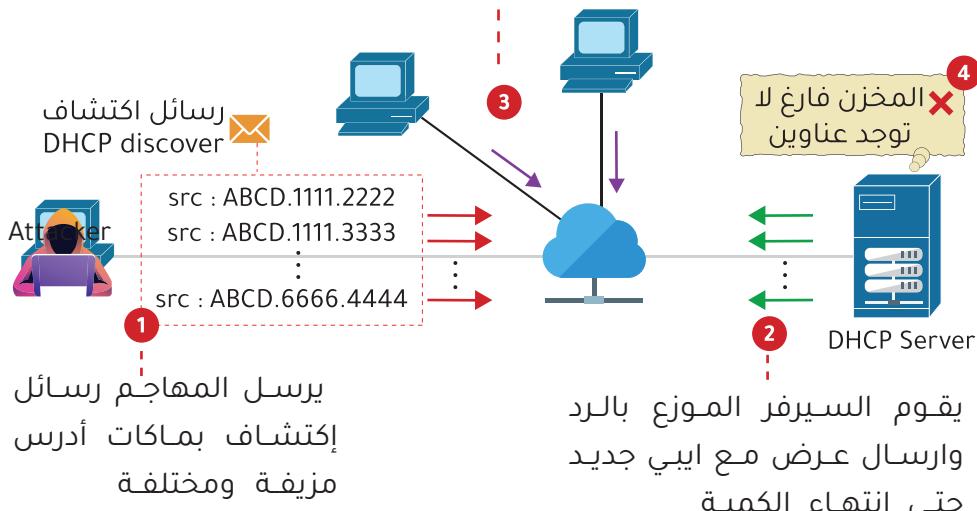
- 1 - DoS (denial-of-service) attacks
- 2 - Spoofing attacks
- 3 - Reflection / amplification attacks
- 4 - Reconnaissance attacks
- 5 - Malware
- 6 - Social engineering attacks
- 7 - Man in the middle attacks
- 8 - Password related attacks

## 2 - هجمات الإنتهاك Spoofing attacks

هو استخدام عنوان مصدر مزيف لاستهداف الضحية مثل عنوان IP مزيف أو ماك ادرس MAC address مزيف.  
- من أمثلة هذا النوع : (DHCP exhaustion - ARP Spoofing)

### لأخذ مثلاً هجوم استنفاد عناوين الـ DHCP (DHCP exhaustion)

في حال طلبت هذه الأجهزة عناوين ايبي IP فإنها لن تجد لأن الـ POOL (المخزن) فارغ

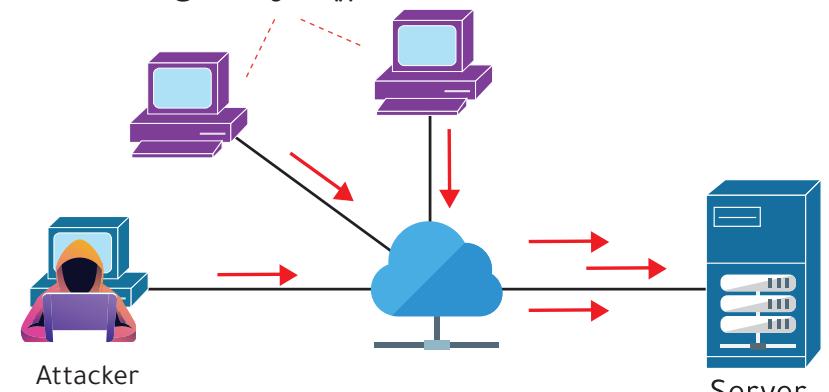


يوجد نوع آخر وهو أقوى ويسمى

## DDoS (distributed denial of service) attacks

يشبه هجوم الـ DoS ولكن من عدة أجهزة ، حيث يقوم المهاجم باصابة الأجهزة ببرامح خبيثة لكي تهاجم السيرفر و إخراجه عن الخدمة .

أجهزة مصابة ببرنامج خبيث وتسمى Botnet



#### 4 - هجمات الاستطلاع Reconnaissance attacks

هذا النوع يهدف إلى جمع أكبر قدر من المعلومات عن الشبكة مثل عناوين الآيبي وأنظمة التشغيل وخدمات السيرفر والمنفذ المفتوحة وغيرها.

- يتم استخدام مجموعة من الأوامر والادوات خلال جمع المعلومات مثل :

- . الأوامر ( nslookup - whois - ping )
- . الادوات ( Nmap - Netcat - Zenmap )

#### 5 - البرمجيات الخبيثة Malware

هي البرمجيات الخبيثة التي تسبب تهديد لأجهزة الكمبيوتر والشبكات والأنظمة وتستخدم في عمليات الهجوم لغرض الإتلاف والسرقة والإضرار وغيرها.

#### أشهر أنواع البرمجيات الخبيثة :

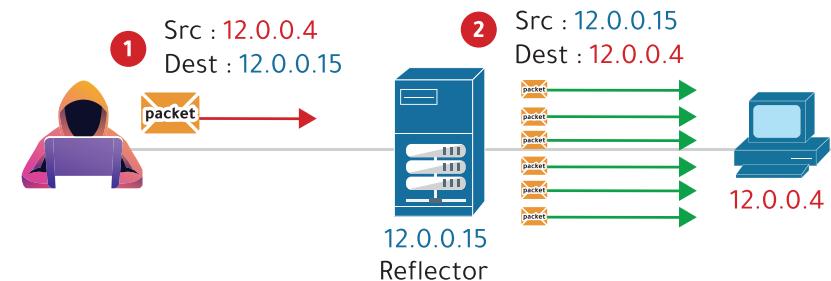
##### A - الفايروسات Virus

الفايروس هو كود برمجي يدخل نفسه إلى تطبيق معين ويتم تنفيذه عند تشغيل التطبيق ، ويمكن للفايروس استنساخ نفسه والانتشار عبر أنظمة المستخدم.

- تنتشر الفايروسات عبر الموقع الإلكتروني المصابة أو مشاركة الملفات أو تزيلات مرافق البريد الإلكتروني

#### 3 - هجمات الانعكاس / التضخيم Reflection / amplification attacks

في هذا النوع من الهجوم يتحل المهاجم عنوان ايبي الضحية ويقوم بارسال رسالة الى السيرفر ليجبره على ارسال كميات كبيرة من البيانات الى جهاز الضحية لإغراق جهاز الضحية وإستهلاك الباندويث في الشبكة .



1 - يرسل المهاجم باكت الى السيرفر منتحلا عنوان جهاز الضحية .

2 - يقوم السيرفر بالرد وارسال كمية كبيرة من البيانات لجهاز الضحية .

هناك أنواع مختلفة من هجمات الهندسة الاجتماعية:

تصيد احتيالي يهدف إلى إغراء المستخدم بالدخول إلى صفحة أو موقع مصايب بهدف إجباره على كتابة اسم المستخدم وكلمة المرور في صفحة تسجيل دخول مزيفة بهدف السرقة مثل الرابط في رسائل الإيميل		Phishing	1
تصيد احتيالي عن طريق إرسال رسالة إيميل إلى موظفين في شركة معينة.	Spear Phishing		2
تصيد احتيالي يستهدف شخصياً عالية وبارزة في الشركات أو الحكومات	Whaling		3
تصيد صوتي وهو تصيد احتيالي يتم إجراؤه عبر الهاتف، قد يتظاهر المهاجم بأنه من بنك الهدف ، أو من قسم آخر في الشركة.	Vishing	4	
هو التصيد الاحتيالي عبر الرسائل القصيرة	Smishing	5	
هو هجوم يستخدم موقع نظامي والهدف هو تحويله إلى موقع مشبه	Pharming	6	
هو هجوم يستهدف مستخدم معين ، هذا المستخدم يقوم بزيارة موقع بشكل متكرر من أجل جمع أو سرقة معلومات منه .	Watering Hole	7	



## B- الديدان Worms

هي برامج قائمة بذاتها تستنسخ نفسها من أجل إصابة الأجهزة أخرى دون الحاجة إلى اتخاذ إجراء من أي شخص .

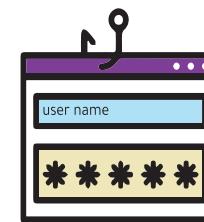
- تنتشر عبر شبكات الكمبيوتر من خلال استغلال الثغرات في أنظمة التشغيل .

- من أمثلتها : حذف ملفات النظام - تشفير بيانات - سرقة معلومات وغيرها .

## C- حصان طروادة Trojan Horse

هو فيروس يخفي نفسه في برنامج نظامي بحيث عند تنصيب هذا البرنامج يتم تفعيل الـ Trojan بشكل تلقائي ليقوم بمهامته الخاصة .

- هذا الـ Trojan منتشر بكثرة عند تنزيل برامج من غير مصدرها الأصلي مثل تفعيل البرنامج عبر كراكات أو باشات .



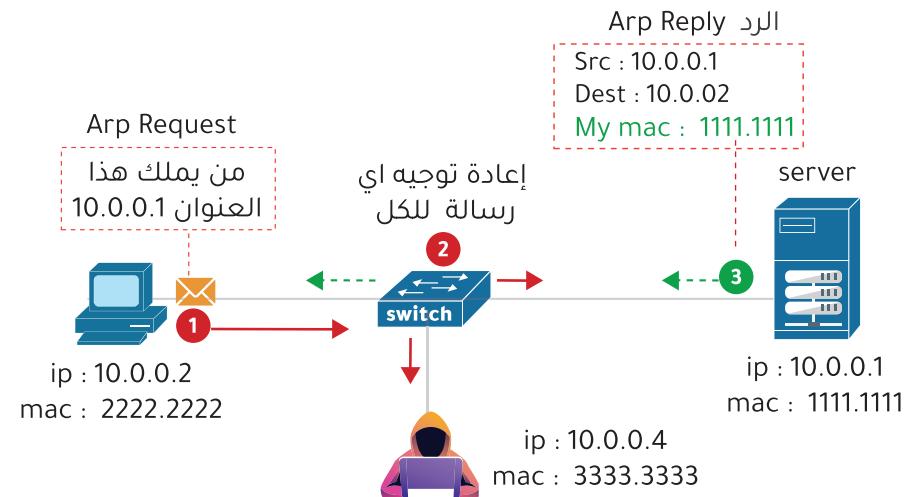
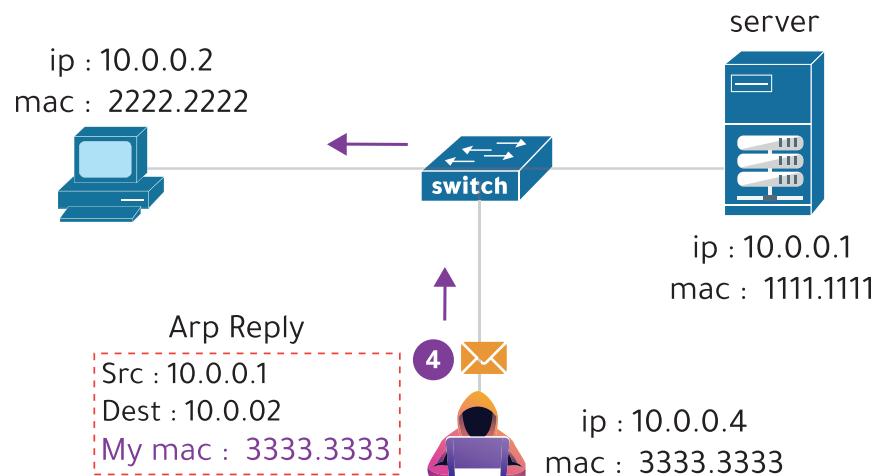
## 6- هجمات الهندسة الاجتماعية Social engineering attack

الهندسة الاجتماعية هي نوع من التقنيات تتضمن تلاعباً نفسياً يستخدمها المهاجمون بهدف استدراج المستخدمين لإرسال بياناتهم السرية أو إصابة حواسيبهم ببرامج ضارة، أو فتح روابط إلى مواقع مصابة .

## 7 - هجمات رجل في منتصف

في هذا النوع من الهجوم ، يضع المهاجم نفسه بين المرسل والمستقبل للتنصت على الاتصالات ، أو لتعديل حركة المرور قبل وصولها إلى المستقبل .

- 1 - يرسل جهاز الحاسب رسالة Arp Request يبحث عن ماك ادرس هذا الايبي 10.0.0.1 للتواصل معه .
- 2 - يقوم السويفتش بإعادة التوجيه للكل ويستلمها المهاجم والسيرفر .
- 3 - يقوم السيرفر بالرد عليه مباشرة Arp Reply بالماك ادرس الخاص به .
- 4 - بعد وصول الرسالة لجهاز الحاسب يقوم المهاجم بانتهال ايبي السيرفر ويرسل رسالة فيها ايبي السيرفر والماك الخاص بالمهاجم ، ويبحث جهاز الحاسب جدول الـ Arp بالبيانات الجديدة .



#### 8 - الهجمات المتعلقة بكلمة المرور

تستخدم معظم الأنظمة والموافق في صفحات تسجيل الدخول اسم المستخدم وكلمة المرور لمصادقة المستخدمين والسماح لهم بتسجيل الدخول .

- يمكن للمهاجمين معرفة كلمة مرور المستخدم من خلال طرق متعددة :

#### A - تخمين اسم المستخدم وكلمة المرور

وذلك بوضع الايميل وادخال كلمات مرور سهلة التخمين مثل 12345 .

#### B - هجوم القاموس

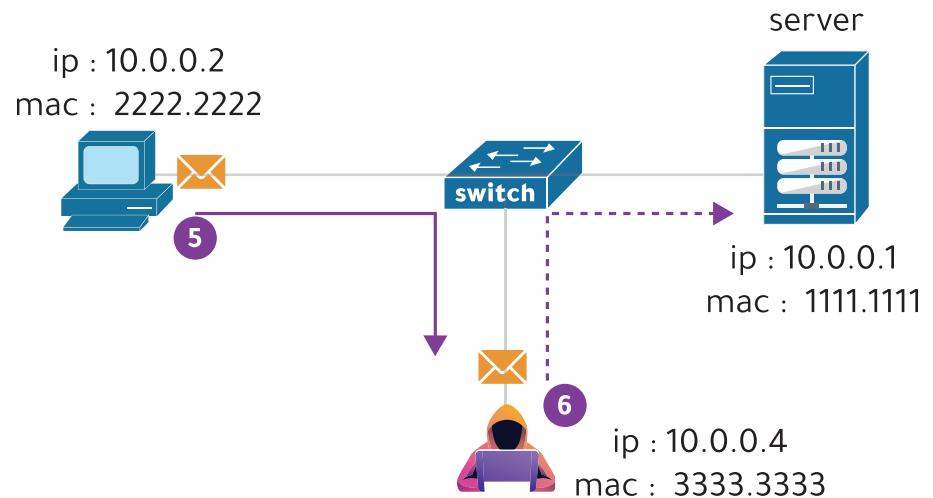
في هذا النوع المهاجم يمتلك ملف يحتوي على كلمات مرور كثيرة يستخدمها عبر سوفتوير خاص الذي يقوم بتجربة جميع الكلمات الموجودة داخل الملف .

#### Brute force Attack - C

في هذا النوع يتم استخدام برنامج يقوم من تلقاء نفسه بتخمين كلمات المرور وذلك عن طريق تركيب كل الأحرف والرموز والأرقام مع بعضها ومحاولة تجريبها على الموقع .

- هذا النوع من الهجوم يتطلب جهاز ذو إمكانيات عالية .

- عندما يريد جهاز الحاسوب التواصل مع السيرفر راح يرسل الرسالة ولكنها تصل للمهاجم لأن الماك أدرس المخزن خاص بالمهاجم .



- يعيد المهاجم ارسال الرسالة بعد الاطلاع عليها وتعديلها للسيرفر

## بدائل كلمات المرور Password Alternatives



- 4 - المصادقة متعددة العوامل (MFA)**
- هي عملية متعددة الخطوات لتسجيل الدخول إلى الحساب ، تتطلب من المستخدمين استخدام طرق إضافية مع كلمة المرور.
- اذا اجتمعت هذه الفئات فإنه تم تطبيق المصادقة متعددة العوامل :
  - A - **الفئة الأولى : شيء أنت تعرف :**  
مثل اسم المستخدم وكلمة المرور.
  - B - **الفئة الثانية : شيء لديك وتحلله :**  
مثل الضغط على شعار يأتيك من الهاتف أو مسح إشارة عبر الهاتف .
  - C - **الفئة الثالثة : شيء عليه ويميزك عن الكل :**  
مثل السمات الجسمانية biometrics الخاصة بك حيث تتم المصادقة عبر مسح الوجه - مسح بصمات الأصابع - فحص شبكة العين .

بعد انتشار أساليب واستهداف كلمات المرور أصبح المهاجم لديه إمكانيات للتخمين أو سرقة هذه المعلومات لذلك وجدت بدائل قوية وذات أمان عالي في المصادقة والتوثيق ومنها :

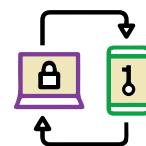
**1- الشهادة الرقمية Digital Certificate**

هي شكل من أشكال المصادقة والتي تُستخدم لإثبات هوية حامل الشهادة يتم استخدامها بشكل أساسى وليس حصرياً لموقع الويب للتحقق من شرعية موقع الويب الذي يتم الدخول إليه.

**2- القياسات الحيوية biometrics**

نقصد بالقياسات الحيوية هي السمات الجسمانية الفريدة والمميزة لكل شخص عن الآخر مثل بصمة الأصبع - الصوت - الوجه .

- الـ **biometrics** هي عملية تسجيل الدخول والمصادقة عبر استخدام بصمة الأصبع أو مسح الوجه أو الصوت .



**3 - المصادقة الثنائية (2FA)**

هي طريقة بسيطة وأكثرها فعالية لتوفير أمان عالي عند المصادقة على بيانات اعتماد تسجيل الدخول.

- فمثلاً بعد أن يقوم المستخدمون بإدخال اسم المستخدم وكلمة المرور، فإنهم بحاجة إلى التحقق من هوبيتهم باستخدام أداة إضافية واحدة مثل البريد الإلكتروني أو الرسائل القصيرة أو أسئلة الأمان وغيرها .

## المصادقة - التفويض - المحاسبة

**AAA (Authentication, Authorization, Accounting)**

### المحاسبة Accounting

هي عملية تسجيل جميع العمليات التي يقوم بها المستخدم على النظام أو الشبكة بهدف المراقبة ومعرفة العمليات التي تم إجراؤها .

هو إطار عمل يُستخدم للتحكم في من يُسمح له باستخدام موارد الشبكة من خلال :

- المصادقة Authentication لتسجيل الدخول

- وما هو مصريح له بالقيام به من خلال التفويض Authorization

- وتسجيل العمليات التي يتم تنفيذها بعد دخوله للشبكة من خلال المحاسبة Accounting .

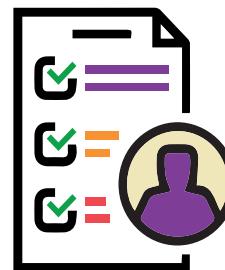
### التفويض أو الصلاحية Authorization

بعد نجاح المصادقة والدخول ، يمكن استخدام التفويض لتحديد بعض الصلاحيات التي يُسمح للمستخدم بالوصول إليها للقراءة أو التنفيذ أو التعديل وغيرها .

- مثل منح المستخدم حق الوصول إلى بعض الملفات والخدمات مع تقييد الوصول إلى الملفات والخدمات الأخرى .

### المصادقة Authentication

العملية التي يمكن من خلالها التعرف على أن المستخدم الذي يريد الوصول إلى موارد الشبكة صحيحة أم لا عن طريق طلب بعض بيانات الاعتماد مثل اسم المستخدم وكلمة المرور .



**1 - برامج توعية المستخدم** *User awareness programs*  
وهي مصممة لتوعية الموظفين بالتهديدات والمخاطر الأمنية المحتملة.

- ليس كل الموظفين خبراء في الأمان السيبراني قد لا يكون الشخص الذي يعمل في الشركة على دراية بجميع التهديدات الإلكترونية التي تواجهها الشركة. لذلك ستساعد برامج توعية المستخدم في توعية هؤلاء الموظفين.

**2 - برامج تدريب المستخدم** *User training programs*  
وهي الأفضل لجميع الموظفين في الشركة حيث يتم عقد جلسات تدريبية مخصصة لهم لتنقيف المستخدمين حول سياسات أمان الشركة وكيفية إنشاء كلمات مرور قوية وكيفية تجنب التهديدات المحتملة.

**3 - التحكم في الوصول المادي** *Physical access control*  
التحكم في الوصول المادي هو نظام إلكتروني يسمح للمؤسسات بتقييد وتنظيم من يمكنه الدخول إلى موقع أو أصول مختلفة. وهي أفضل طريقة للتعرف على المستخدمين والموظفين ، والتأكد من هويتهم من خلال طرق مختلفة والسماح لهم بالوصول إلى العناصر أو المناطق.

تستخدم الشركات عادةً خادم AAA لتقديم خدمات AAA على سبيل المثال شركة سيسكو لديها سيرفر يمكن تفعيل الـ AAA عليه ويسمى : Identity Services Engine (ISE)

تستخدم سيرفرات الـ AAA بروتوكولين عند توصيلها بأجهزة السوينتش أو الراوتر :

**TACACS+ - 1**

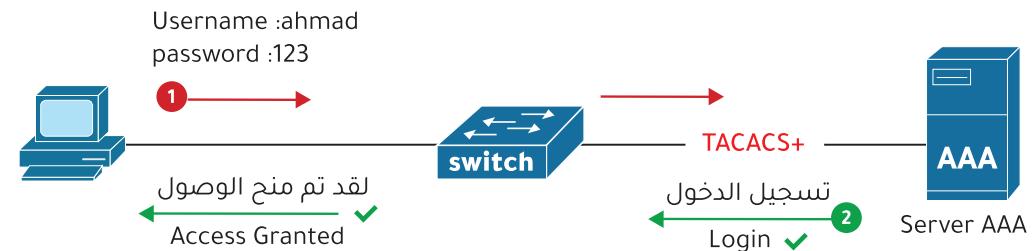
بروتوكول خاص يعمل على شركة سيسكو فقط .

- يستخدم بروتوكول TCP ومنفذ 49 (TCP Port 49).

**RADIUS - 2**

بروتوكول عالمي يمكن استخدامه على أي جهاز .

يستخدم بروتوكول UDP ومنفذ 1812 و 1813 ( UDP Port 1812 - 1813 )

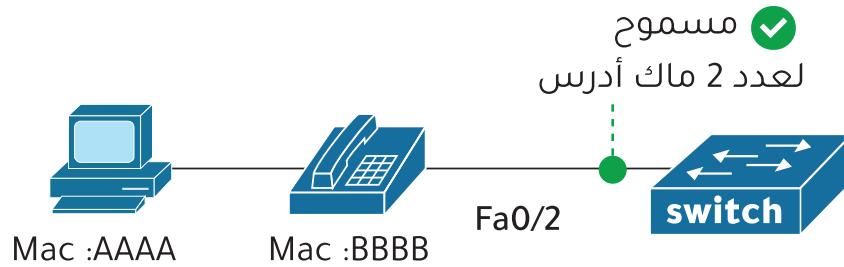


### عناصر برنامج الأمان security program elements

برنامج الأمان هو مجموعة من سياسات وإجراءات الأمان الخاصة بالمؤسسة .

- هذه بعض العناصر التي يجب أن يكون لدى الشخص دراية وعلم بها :

- عند تفعيل الـ Port Security على أحد منافذ السويتش في الوضع الافتراضي فان العدد سوف يكون ماك أدرس واحد فقط.
- تسطيح السماح بالربط لعدد أكبر من ماك أدرس واحد.
- تستطيع إعداد وربط منفذ السويتش بماك أدرس الحاسوب يدويا

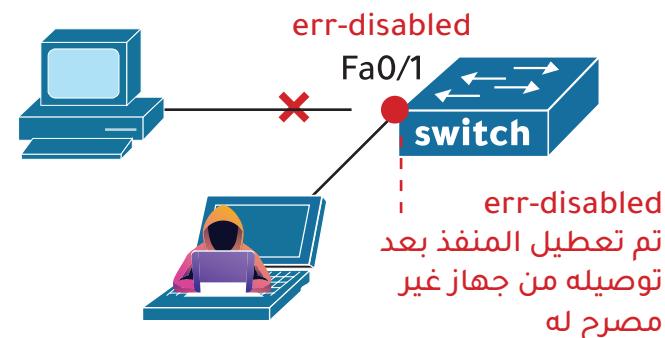


## Port Security



أمان المنفذ نقصد به تأمين منافذ السويتش من الأجهزة الغير مصرح لها وذلك بربط المنفذ interface ب ماك أدرس الحاسوب أو غيره من الأجهزة الـ (end device).

- عند توصيل جهاز حاسب غير مصرح له بمنفذ سويتش مؤمن عليه وأراد ارسال واستقبال البيانات فإن السويتش سوف يغلق المنفذ مباشرةً وينعه من ارسال واستقبال البيانات .



- يستطيع مسؤول الشبكة ربط منفذ السويتش بأجهزة الموظفين وذلك عبر ربط كل منفذ بماك أدرس جهاز الموظف .

- تزداد فائدة هذا الامان عند محاولة أحد المهاجمين بتوصيل جهازه بأحد منافذ السويتش حيث أنه يمنع هذا المهاجم من ارسال واستقبال البيانات التي يرغب بسرقتها أو تعطيلها .

## أوضاع منفذ السويتش عند إغفاله بسبب توصيل جهاز غير مصرح له :

الوصف Description	الوضع Mode
هذا الوضع الافتراضي - يقوم السويتش بإغلاق المنفذ وتعطيله مباشرة	shutdown
يبقى المنفذ مفتوح للإجهزة المصرحة لها <b>ويمنع إرسال واستقبال</b> البيانات من الماك أدرس الغير مصرح له وأيضا لا يظهر إشعار ورسائل للبلاغ بهذا الوضع	protect
هو نفس وضع الـ protect ولكن يظهر إشعار ورسائل للبلاغ بهذا الوضع	restrict

في حال أردت تغيير الوضع الافتراضي اختر من هذه الخيارات عبر الأمر

SW1(config-if)# switchport port-security violation ?

```
protect  Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown mode
```

مثلاً نختار restrict

SW1(config-if)# switchport port-security violation restrict

في هجوم الانتحال Spoofing attacks الذي يتم على سيرفر الـ DHCP ينتحل المهاجم الآلاف من عناوين الـ MAC المزيفة ويهاجم بها سيرفر الـ DHCP مما يؤدي إلى استنفاد عناوين الرابعية من السيرفر، لكن عند تفعيل الـ Port Security على المنفذ لن يستطيع المهاجم تمرير الماك أدرس عبر منفذ السويتش لانه سوف يتم إغفاله مباشرة بفضل هذه الخاصية .

## شرح إعدادات الـ Port Security configurations



تم الشرح في الصفحة التالية

تفعيل وضع الـ Access وهذا مهم لانه لن يعمل إذا كان وضع dynamic auto المنفذ تلقائي

تفعيل وضع الـ port-security

هو الفترة المسموحة لوجود الماك أدرس في جدول ماقات السويتش

هذا الخيار لربط المنفذ بماك أدرس معين ، ويتم

كتابة الماك أدرس بعد هذا الخيار

هذا الخيار إذا أردت زيادة عدد الماقات أدرس المرتبطة بهذا المنفذ

الوضع في حال اذا تم انتهاء المنفذ بتوصيل جهاز غير مصرح له ، يوجد

بعد اختيار هذا الخيار 3 اختيارات موجودة بالجدول في الصفحة السابقة

كتابة الماك أدرس يدوي

هو أن المنفذ سوف يسجل عنوان الماك أدرس

تلقائيا بمجرد توصيل الحاسوب بالمنفذ

تحديد عدد الماقات المسموح لها بتوصيل على المنفذ (الافتراضي =1)

تحديد الوقت المسموح بالدقائق لبقاء الماك الدرس في جدول ماقات السويتش والذي تم تسجيله عن طريق الـ port-security

يتم حذف الماك بعد انتهاء الفترة المسموحة بالدقائق من أول ظهوره في جدول الماك أدرس السويتش وهو الافتراضي

يتم حذف الماك الغير نشط ( ليس عليه حركة بيانات أو ترافيك )  
بعد انتهاء الفترة المسموحة بالدقائق

## SW1

```
SW1(config)# int Fa0/0
```

```
SW1(config-if)# switchport mode access
```

```
SW1(config-if)# switchport port-security
```

```
SW1(config-if)# switchport port-security ?
```

aging Port-security aging commands

mac-address Secure mac address

maximum Max secure addresses

violation Security violation mode

```
SW1(config-if)# switchport port-security mac-address ?
```

H.H.H 48 bit mac address

sticky Configure dynamic secure addresses as sticky

```
SW1(config-if)# switchport port-security maximum 1
```

```
SW1(config-if)# switchport port-security aging ?
```

time port-security time

type port-security type

```
SW1(config-if)# switchport port-security aging time 2
```

```
SW1(config-if)# switchport port-security aging type ?
```

absolute Absolute aging (default)

inactivity Aging based on inactivity time period

**مثال :**

لدينا هذا النموذج في برنامج الباكت  
تريسر وسوف نطبق عليه :

- إعدادات Port Security

**SW1**

```
SW1(config)# int Fa0/0
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security mac-address 000D.BD0C.4B23
SW1(config-if)#switchport port-security maximum 1
```

**SW1**

```
SW1# show port-security
```

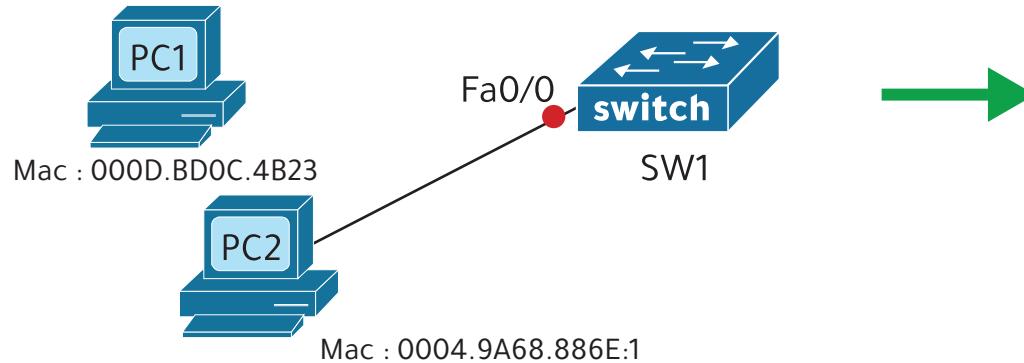
المنفذ المطبق عليه Port Security	العدد الأقصى للعناوين الآمنة MaxSecureAddr (Count)	العدد الحالي للعناوين الآمنة CurrentAddr (Count)	عدد الانتهاكات التي حدثت على المنفذ SecurityViolation (Count)	إجراء الأمان المطبق على المنفذ اذا حصل انتهاك Security Action
Fa0/0	1	1	0	Shutdown

SW1

SW1# show port-security int fa0/1

Port Security	: Enabled	الـ port-security مفعل
Port Status	: Secure-up	حالة المنفذ الآمن فعال
Violation Mode	: Shutdown	وضع الـ shutdown : وضع الـ انتهاك
Aging Time	: 0 mins	
Aging Type	: Absolute	
SecureStatic Address Aging	: Disabled	الـ العدد الأقصى للـ ماكـات أـدرس المـسمـوـحة لـهـا
Maximum MAC Addresses	: 1	عـدـد جـمـيـع الـ ماـكـات الـ مـسـجـلـة عـلـى هـذـا الـ منـفـذ
Total MAC Addresses	: 1	عـدـد الـ ماـكـات الـ تـسـجـيلـهـا يـدـوـيـا
Configured MAC Addresses	: 1	عـدـد الـ ماـكـات الـ تـسـجـيلـهـا تـلـقـائـيـا عـبـر الـ اـلـمـر
Sticky MAC Addresses	: 0	عـدـد الـ ماـكـات الـ تـسـجـيلـهـا تـلـقـائـيـا عـبـر الـ اـلـمـر
Last Source Address:Vlan	: 0000.0000.0000:0	أـخـر ماـكـاـرـد أـدرـس حـاـول اـنـتـهـاك الـ منـفـذ وـارـسـال بـيـانـات
Security Violation Count	: 0	

عدد الـ اـنـتـهـاكـات الـ حـدـثـت عـلـى الـ منـفـذ

بعد توصيل جهاز غير مصرح له  
ومحاولة ارسال بيانات

SW1

SW1# show port-security int fa0/1

Port Security	: Enabled
Port Status	: Secure-shutdown
Violation Mode	: Shutdown
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1
Total MAC Addresses	: 1
Configured MAC Addresses	: 1
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0004.9A68.886E:1
Security Violation Count	: 1

**الطريقة التلقائية لا تعمل على برنامج الباكت ترييسر packet tracer**

**ملاحظة :**

لاحظ اسم الخطأ **err-disabled** الذي ظهر  
عند استعراضنا لمعلومات المنفذ fa0/1

**تلقائية :**

**SW1**

نغير توقيت الانتظار (من بعد اقفال المنفذ حتى يعود الى التفعيل)

SW1(config)# errdisable recovery interval 30

ثم نضيف هذا الامر

SW1(config)# errdisable recovery cause psecure-violations

**SW1**

SW1# show int fa0/1 status

Port	Status	Vlan
Fa0/1	err-disabled	1

**ملاحظة :**

عند إعادة توصيل الجهاز الصحيح والمصرح له لن يعمل المنفذ لذلك يجب عليك تفعيل المنفذ وذلك **بطريقتين** : **يدوية أو تلقائية**

**ملاحظة :**

هذه للدروس القادمة وتم وضعها هنا لكي يتم معرفة جميع الأوامر الـ 3

هذا الأمر لـ DHCP Snooping لإعادة تفعيل المنفذ تلقائياً بعد ظهور خطأ err-disabled

SW1(config)# errdisable recovery cause dhcp-rate-limit

هذا الأمر لـ arp Inspection لإعادة تفعيل المنفذ تلقائياً بعد ظهور خطأ err-disabled

SW1(config)# errdisable recovery cause arp Inspection

**يدوية :** بالدخول على المنفذ

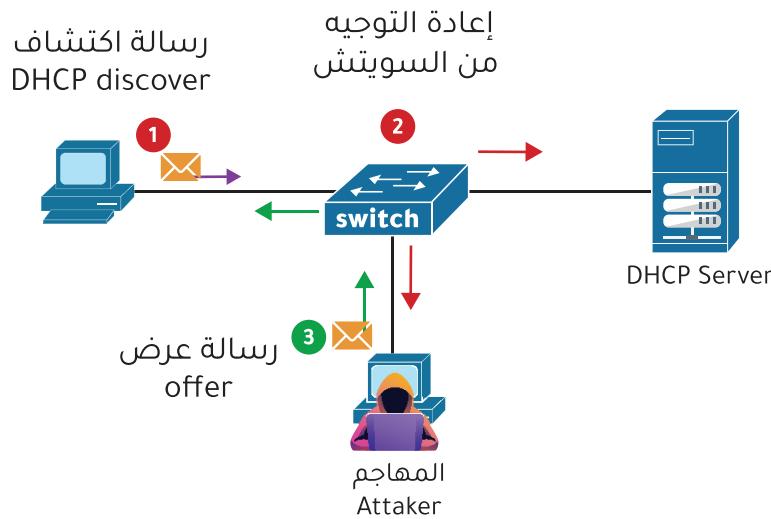
**SW1**

SW1(config)# int Fa0/0

SW1(config-if)# shutdown

SW1(config-if)# no shutdown

- 2 - تنصيب المهاجم نفسه كموزع dhcp sever : يستغل المهاجم نفسه داخل الشبكة كموزع DHCP حيث يراقب رسائل الا Discover الصادرة من جهاز الحاسوب و يرد عليهما بعرض offer فيستجيب الحاسوب لهذا العرض ويقبل الايبي منه .  
يسمى هذا الهجوم بـ **DHCP Spoofing Attack**



- فائدة الـ DHCP Snooping :**
  - حماية الشبكة من مثل هذه الهجمات .
  - التحقق من صحة رسائل الا dhcp المرسلة عبر المنفذ .
  - يراقب عدد البواكيتات أو الرسائل التي تمر عبر المنفذ والمرسلة من الجهاز الذي يتطلب الايبي .
  - تستطيع تفعيل الـ DHCP Snooping على فيلان vlan محددة أو عدة فيلانات .

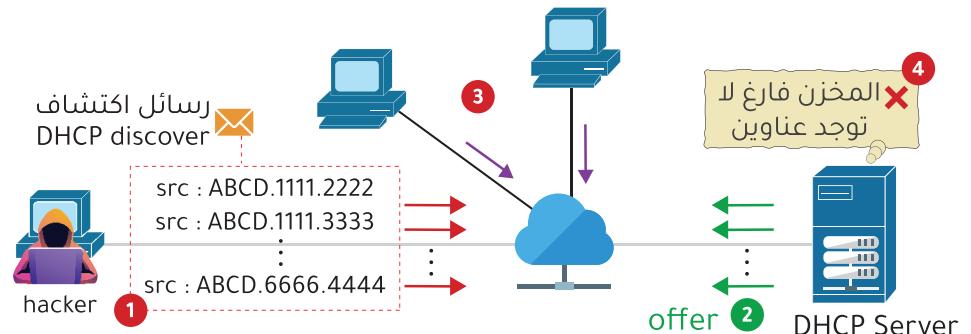
## DHCP Snooping ≡

هي ميزة أمان متوفرة على السويتشات تُستخدم للتحقق من رسائل وبيانات الا DHCP المزيفة والتي يرسلها المهاجم لغرض توزيع ايبيات للجهزة داخل الشبكة والإضرار بسيرفر الا DHCP الرئيسي .

- **كيف تتم عملية الهجوم من المهاجم (Attacker) على الا DHCP Server ؟**

1- **تعطيل المهاجم لـ DHCP Server** : يقوم المهاجم بمهاجمة سيرفر الا DHCP عبر إرسال رسائل استكشاف وبكثرة لكي يرد عليه سيرفر الا DHCP بالعرض مع ايبيات مقتراحه منه حتى تنتهي جميع الايبيات من الموزع الرئيسي .

- يسمى هذا الهجوم بـ (DHCP exhaustion) استنفاد الا dhcp وأيضا يسمى بـ **DHCP Starvation Attack**

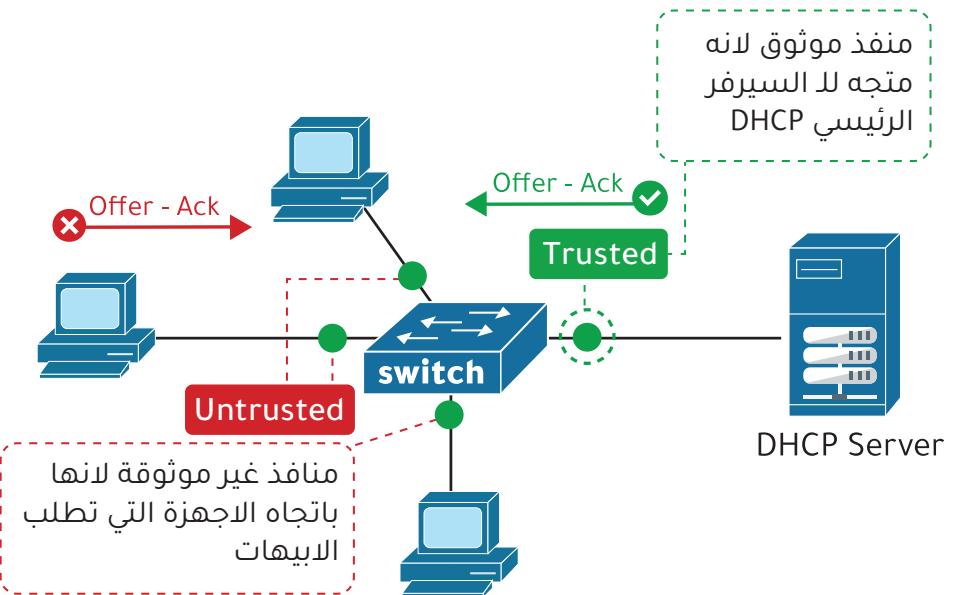


: (DHCP Client) الرسائل التي يرسلها عميل DHCP ويسمى (DHCP Server) .  
 : رسالة اكتشاف موزع الأبيهات Discover -  
 : الرد بطلب الموافقة على عرض الـ dhcp offer - Request -  
 : إخبار الـ DHCP Server بأن العميل لا يحتاج الـ IP الخاص به Release -  
 : يستخدم لرفض عنوان IP الذي يقدمه الـ DHCP Server Decline -

**الرسائل التي يرسلها الـ DHCP Server :**  
 - Offer : تقديم عرض للعميل بآي بي جديد .  
 - Ack : رد على العميل بتأكيد استخدام العنوان الجديد .  
 - Nak : رسالة تستخدم لرفض طلب العميل .

**كيف تم الحماية بواسطة DHCP Snooping ؟**  
 عند تفعيل الـ DHCP Snooping تحول جميع المنفذ إلى وضع غير موثوق ( Untrusted ) لمنع استقبال الرسائل التي يرسلها الـ DHCP وهي الـ ( Offer - Ack ) .

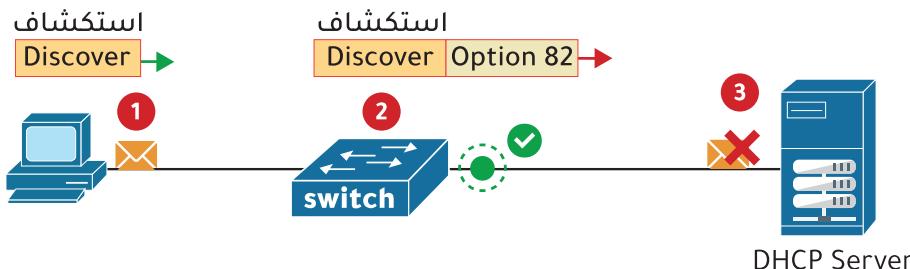
1 - يقوم مسؤول الشبكة بتحديد المنفذ الموثوق ( Trusted ) يدوياً وهو المنفذ المتجه للـ DHCP Server الرئيسي حتى يسمح له بمرور هذه الرسائل ( Offer - Ack ) .  
 - سبب منع استقبال الرسائل الـ ( Offer - Ack ) عبر المنفذ الغير موثوقة لمنع المهاجم من إرسالها للأجهزة الأخرى .



## DHCP Option 82 (Information Option)

هي خيار يضيف معلومات على رسالة الـ DHCP التي وصلت له من العميل ، فيها معلومات عن المنفذ الذي وصلت الرسالة منه والفیلان الموجود فيه العميل وايضاً معلومات عن الـ relay agent (الجهاز الذي تلقى رسالة العميل وهو السوتش).

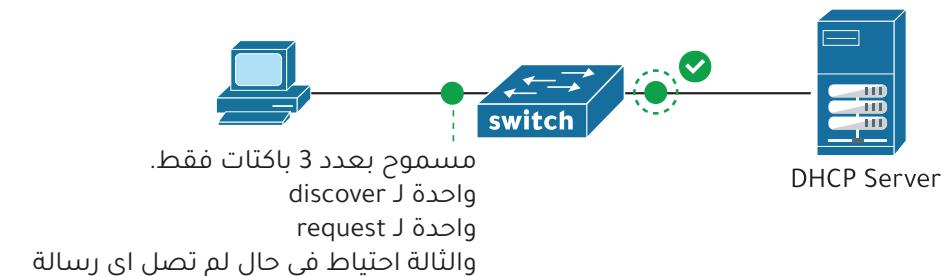
- عند تفعيل الـ DHCP Snooping سيضيف السوپينگ تلقائياً الخيار 82 على رسالة العميل ويكمّل إرسالها إلى الـ DHCP Server.
- بشكل افتراضي وتلقائي سوف يرفض الـ DHCP Server هذه الرسالة ولن يعطي العميل أي آي بي جديد **والحل هو الغاء تفعيل هذا الخيار**.



## DHCP Snooping Rate-Limiting

**تحديد معدل DHCP Snooping :** يمكن لتقنية الـ DHCP Snooping تحديد عدد الباكتات أو الرسائل في الثانية الواحدة والتي تدخل من المنفذ الغير موثوقة . فإذا تجاوز معدل رسائل DHCP الحد الذي تم تحديده أو تكوينه . فسيتم تعطيل المنفذ ويظهر الخطأ err-disabled .

- يمكن إعادة تفعيل المنفذ يدوياً أو تلقائياً مثل طريقة الـ Port Security مع تغيير السبب إلى dhcp-rate-limit .
- يقوم مسؤول الشبكة بتحديد عدد الباكتات التي تدخل من المنفذ الغير موثوقة ، مثل العدد 3 باكتات .
- نعرف أنه هناك رسالتين يرسلها العميل لطلب الآي بي من الـ DHCP Server وهي : ( discover - request ) وهذا الرسائل مسمومة لها بالمرور عبر المنفذ الغير موثوقة ولكن يجب تحديد العدد لكي لا يستغل المهاجم بتمرير عدد كبير جداً من رسائل الـ discover .
- **تحديد المعدل للـ DHCP Snooping يساعد على الحماية من هجوم الـ DHCP exhaustion .**



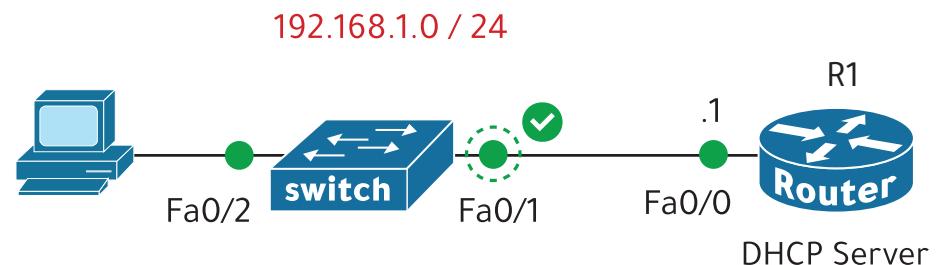
R1

```
R1(config)# int Fa0/0
R1(config-if)# no shutdown
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# exit

R1(config)# ip dhcp excluded-address 192.168.1.1
R1(config)# ip dhcp pool LAN2
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8
R1(dhcp-config)# exit
```

## إعدادات DHCP Snooping DHCP Snooping configurations

لدينا هذا النموذج في برنامج الباكت تريسر وسوف نطبق عليه :  
- إعدادات DHCP Snooping -



SW1

```
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 1
SW1(config)# no ip dhcp snooping information option

SW1(config)# int fa0/1
SW1(config-if)# ip dhcp snooping trust
SW1(config)# exit
SW1(config)# int fa0/2
SW1(config-if)# ip dhcp snooping limit rate 3
SW1(config)# exit
```

- تفعيل DHCP Snooping
- تفعيل DHCP Snooping على الفيلان الأولي (VLAN 1)
- إلغاء تفعيل خيار 82 (Option 82)
- تحديد المنفذ fa0/1 كمنفذ موثوق
- تحديد معدل الرسائل أو الباكتات في الثانية الواحدة عبر المنفذ fa0/1 إلى 3 فقط

عندما يتم توزيع الأبي على الأجهزة يقوم الـ DHCP Snooping بإنشاء جدول يوضح فيه الأبي الذي تم إرساله من سيرفر الـ DHCP ويربطه برقم المنفذ والماك أدرس الخاص فيه.

SW1					
ماك أدرس pc1	أبي pc1	فترة تأجير عنوان الأبي	النوع	رقم الفيلان الموجود فيه العميل	المنفذ المتصل بالعميل
MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:D0:58:8C:A0:3D	192.168.1.2	86400	dhcp-snooping	1	Fa0/2

SW1		
المنفذ	موثوق	تحديد معدل الرسائل في المنفذ
Interface	Trusted	Rate limit (pps)
Fa0/1	yes	unlimited
Fa0/2	no	3

## Dynamic ARP Inspection (DAI) ≡

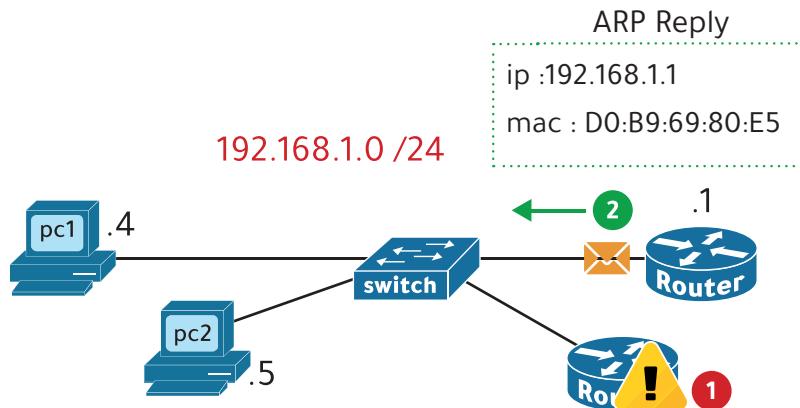
هي ميزة أمنية في السويفت تستخدم لفحص وفلترة رسائل الـ ARP التي يتم استقبالها عبر المنفذ الغير موثوقة.

- بعد تفعيله تصبح جميع المنفذ غير موثوقة (Untrusted) افتراضيا.

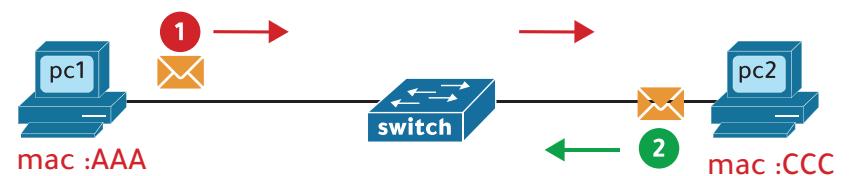
- يتم إعداد المنفذ المتصلة بالأجهزة مثل السويفت والراوتر كمنفذ موثوقة (Trusted) بشكل يدوي والمنفذ المتصلة بالأجهزة المضيفة (Hosts) مثل الحاسوب والطابعة وغيرها كمنفذ غير موثوقة.

### ما هو الـ ARP ؟

يسخدم لمعرفة ماك ادرس الجهاز الآخر الذي عنوانه الايبي معروف . مثلا PC1 يرسل رسالة ARP لمعرفة عنوان الماك ادرس للجهاز الذي عنوانه الايبي 10.0.0.5 ويرد عليه PC2 برسالة ARP Reply فيه الماك ادرس الخاص به



192.168.1.1    192.168.1.3



طلب Arp Request  
ip المرسل : 192.168.1.1  
ip المستقبل : 192.168.1.3  
ماك المرسل : AAA  
ماك المستقبل : FF:FF:FF:FF:FF

الرد ARP Reply  
ip المرسل : 192.168.1.3  
ip المستقبل : 192.168.1.1  
ماك المرسل : CCC  
ماك المستقبل : AAA

## نتعرف على كيفية الحماية بواسطة الـ DAI

عندما تصل للسويتشر رسالة عبر منفذ غير موثوق يقوم الـ DAI بفحصها وفلترتها عبر مطابقة بيانات الرسالة مع جدول الـ dhcp snooping binding.

- تعرفنا أن جدول الـ dhcp snooping binding يخزن عنوان أيبي وماك أدرس الجهاز الذي استلم عنوان أيبي من الخادم DHCP ويربطه بالمنفذ المتصل بهذا الجهاز.

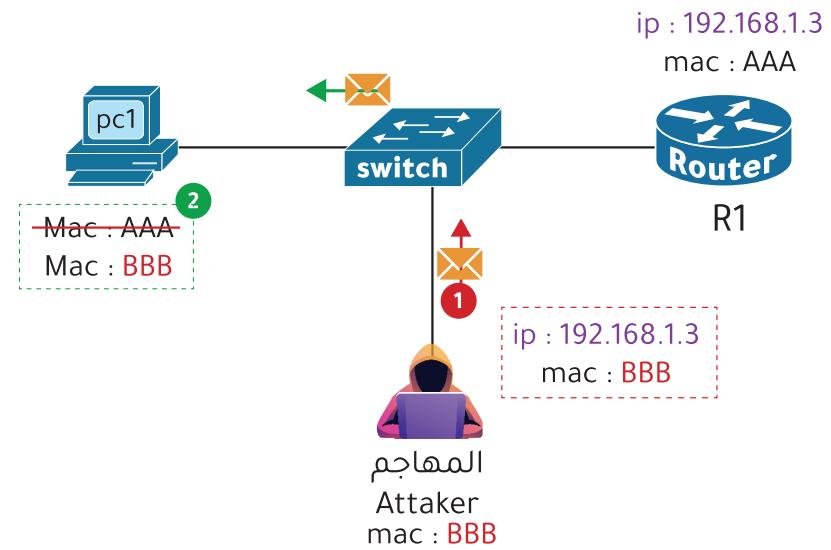
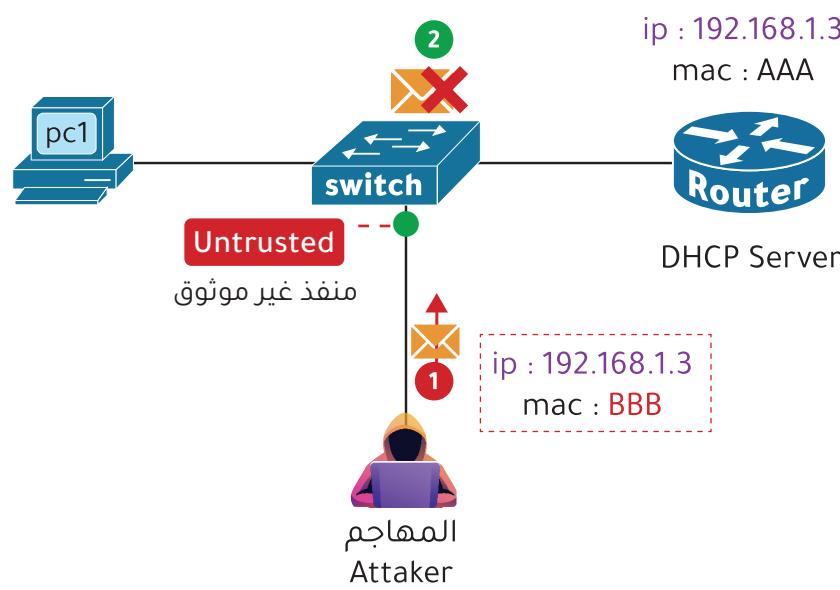
- فإذا كانت الرسالة بيانات لها مطابقة كما في الجدول من ناحية عنوان الآي بي والماك أدرس والمنفذ فإنه يسمح بتمريرها.

## نتعرف على كيفية هجوم الـ ARP Spoofing

عندما يتصل المهاجم بالشبكة يرسل رسالة ARP Reply بطلب منهم **تحديث الماك أدرس القديم** للأجهزة الموجودة يطلب منهم **بالماك أدرس الخاص بالمهاجم**.

لذلك جميع الأجهزة عندما تريد ارسال بيانات سوف تتجه إلى المهاجم لانه حدث عنوان الماك أدرس المرتبط بالبوابة الافتراضية (default gateway).

طبعاً المهاجم يستطيع الإطلاع والتعديل على البيانات ومن ثم إعادة ارسالها إلى الجهاز الأساسي في الشبكة.



R1

```

Dhcp(config)# int Fa0/0
Dhcp(config-if)# no shutdown ①
Dhcp(config-if)# ip add 192.168.1.1 255.255.255.0
Dhcp(config-if)# exit
②

Dhcp(config)# ip dhcp excluded-address 192.168.1.1
Dhcp(config)# ip dhcp pool LAN2
Dhcp(dhcp-config)# network 192.168.1.0 255.255.255.0
Dhcp(dhcp-config)# default-router 192.168.1.1
Dhcp(dhcp-config)# dns-server 8.8.8.8
Dhcp(dhcp-config)# exit

```

SW1

```

SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 1 ③
SW1(config)# no ip dhcp snooping information option

SW1(config)# int fa0/1
SW1(config-if)# ip dhcp snooping trust
SW1(config-if)# exit
SW1(config)# int fa0/2
SW1(config-if)# ip dhcp snooping limit rate 3
SW1(config-if)# exit

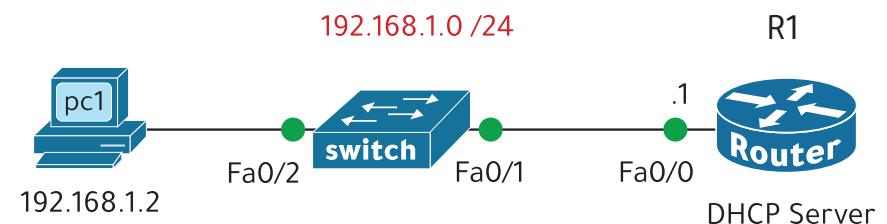
```

## إعدادات لـ ARP Inspection configurations



لدينا هذا النموذج في برنامج الباكت ترييسر  
وسوف نطبق عليه :

- إعدادات لـ Dynamic ARP Inspection (DAI) -



### مراحل الحل :

1. تطبيق إعدادات الأساس.

2. تطبيق إعدادات لـ DHCP

3. تطبيق إعدادات لـ DHCP Snooping

4. تطبيق إعدادات لـ ARP Inspection

تفعيل arp snooping على الفيلن الأول (vlan 1)

SW1

SW1(config)# ip arp inspection vlan 1

SW1(config)# int fa0/1

SW1(config-if)# ip arp inspection trust -----

تحديد المنفذ 1  
كمنفذ موثوق

SW1(config-if)# exit

SW1(config)# int fa0/2

SW1(config-if)# ip arp inspection limit rate 15 burst interval 1

SW1(config)# exit

هنا نستطيع تحديد معدل الرسائل أو الباقاتات في الثانية الواحدة عبر المنفذ 2

SW1# show ip arp inspection interfaces

معدل تحديد  
الثوابي  
الرسائل  
المنفذ  
حالة الثقة  
الباكتات أو

Interface	Trusted	Rate(pps)	Burst Interval
Fa0/1	Trusted	15	1
Fa0/2	Untrusted	15	1
Fa0/3	Untrusted	15	1

: معدل تحديد الرسائل في الثانية الواحدة في الـ Limit Rate يكون افتراضياً 15 باكت في الثانية الواحدة .

SW1

SW1# show ip dhcp snooping binding

ماك ادرس	آبي pc1	فترة تأجير	نوع	رقم الفيلن	المنفذ
MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:00:0C:CA:35:1B	192.168.1.2	86400	dhcp-snooping	1	Fa0/2

```

SW1>en
SW1# conf t
SW1(config)# username hani secret 1236
SW1(config)# username ahmad pri 15 secret 1235

----- --- ندخل على الكونسول
----- --- Login local لكي يظهر له أمر
----- --- طلب ادخال اسم المستخدم و
----- --- كلمة المرور

----- --- يظهر له أمر طلب ادخال
----- --- Login
----- --- كلمة المرور فقط فلو أردت أن
----- --- يظهر اسم المستخدم اضف
----- --- local
----- --- كلمة

SW1(config)# line console 0
SW1(config-line)# login local
SW1(config-line)# exit

SW1(config)# line aux 0
SW1(config-line)# password 1234
SW1(config-line)# login
SW1(config-line)# exit

```

## التحكم في الوصول إلى الجهاز

### Device Access Control

التحكم في الوصول إلى الجهاز :

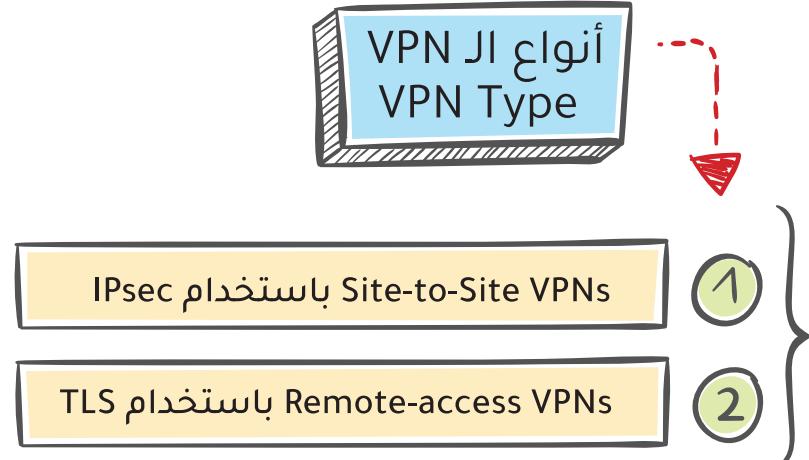
تعرفنا سابقاً أننا نستطيع الدخول إلى إعدادات الراوتر والسويتش عن طريق توصيل الكابل عبر منفذ الكونسول لا console أو منفذ ال

(Aux) Auxiliary

- في هذا القسم يجب علينا حماية هذين المنفذين من أي شخص غير مصرح له بالتوصيل والدخول على إعدادات الأجهزة .

## وظائف الـ VPN

- 1 - سرية البيانات Data Confidentiality يتم تشفير البيانات لكي لا يمكن لأحد الاطلاع عليها
- 2 - تكامل البيانات Data Integrity أي إن البيانات تم تمريرها دون تغيير أو تلاعب بها .
- 3 - مصادقة البيانات Data Authentication يمكن للمتلقى التحقق من أن البيانات نشأت وارسلت من المرسل فقط
- 4 - مكافحة تكرار البيانات Anti replay هي منع إعادة إرسال حزمة البيانات مرة أخرى .

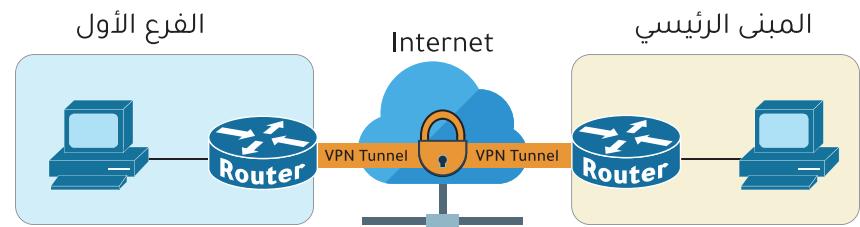


## الشبكة الإفتراضية الخاصة Virtual Private Network (VPN)

هي اتصال مشفر بين الشبكات الخاصة عبر شبكة عامة مثل الانترنت .

- لذلك هي شبكة افتراضية ترسل البيانات بأمان عبر شبكة غير آمنة (الانترنت) ، لأن عالم الانترنت مليء بالهكرز والمتجمسين الذين يستطيعون التقاط حركة البيانات والتجسس عليها لذلك

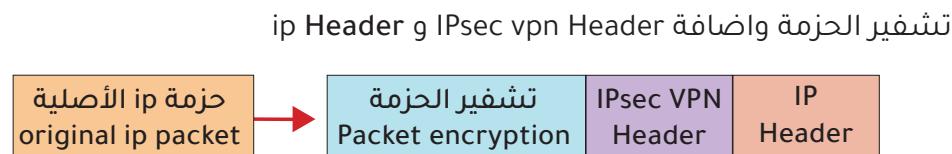
الـ VPN توفر الاتصال المشفر والأمن لدى كثير من الشركات .



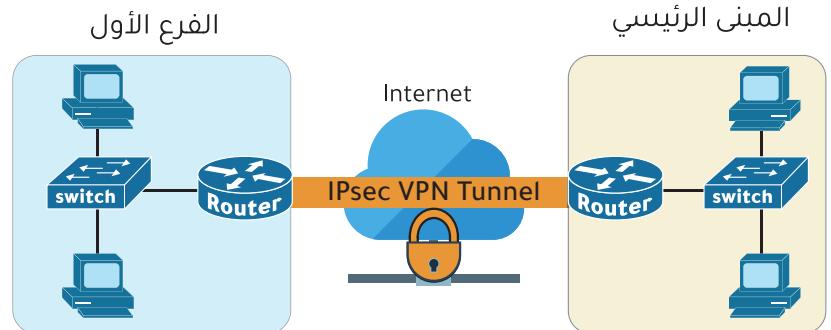
## IPsec باستخدام Site-to-Site VPNs

1

- عند استخدام IPsec يتم تشفير الحزمة الأصلية قبل تغليفها حتى لا يتم قراءتها.
- يتم إنشاء نفق (VPN) بين الجهازين من خلال تغليف حزمة IP الأصلية بالإضافة هيدر VPN وهيدير IP جديد.



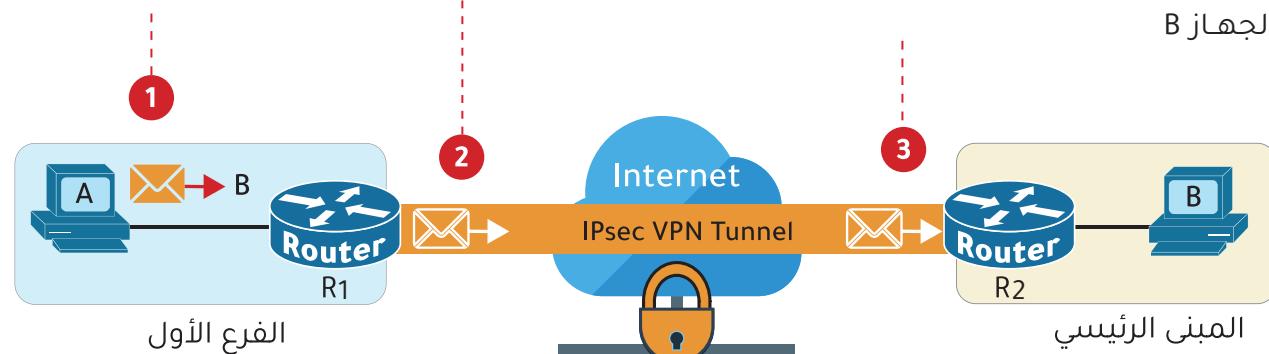
- هو اتصال VPN مشفر بين موقعين عبر الانترنت .
- يتم إنشاء نفق (VPN Tunnel ) آمن ومشفر باستخدام بروتوكول IPsec بين الموقعين .



الجهاز A يرسل رسالة الى الجهاز B في المبني الرئيسي (البيانات هنا غير مشفرة)

توصل للراوتر R1 فيقوم بتشفييرها وتغليفها باضافة VPN هيدر و ip هيدر

توصل للراوتر 2 فيقوم بفك التشفير للحصول على الرسالة الأصلية وإعاده توجيهها إلى الجهاز B



### GRE (Generic Routing Encapsulation)

الـ GRE يستطيع إنشاء أنفاق الـ vpn مثل الـ IPsec لكنه لا يقوم بتشифير الحزمة الأصلية لذلك هو غير آمن.

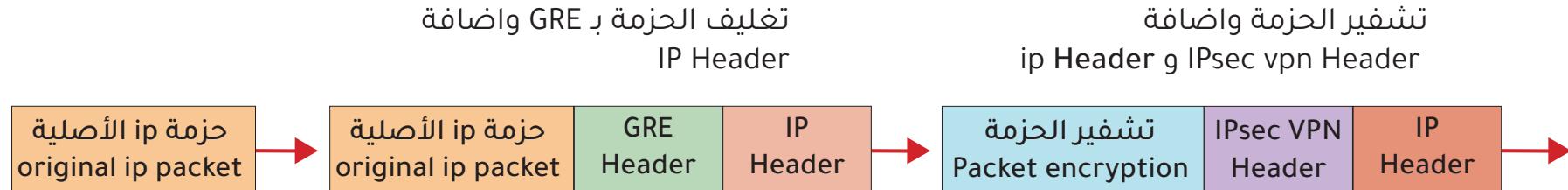
لكنه يتميز بكونه قادرًا على تغليف مجموعة متنوعة من بروتوكولات الطبقة الثالثة التي تعتمد على البث والبث المتعدد ( broadcast - multicast ) .

لذلك يمكننا استخدام الـ GRE للحصول على مرونة الـ GRE مع أمان الـ IPsec بمعنى أننا ندمج الـ GRE مع الـ IPsec .

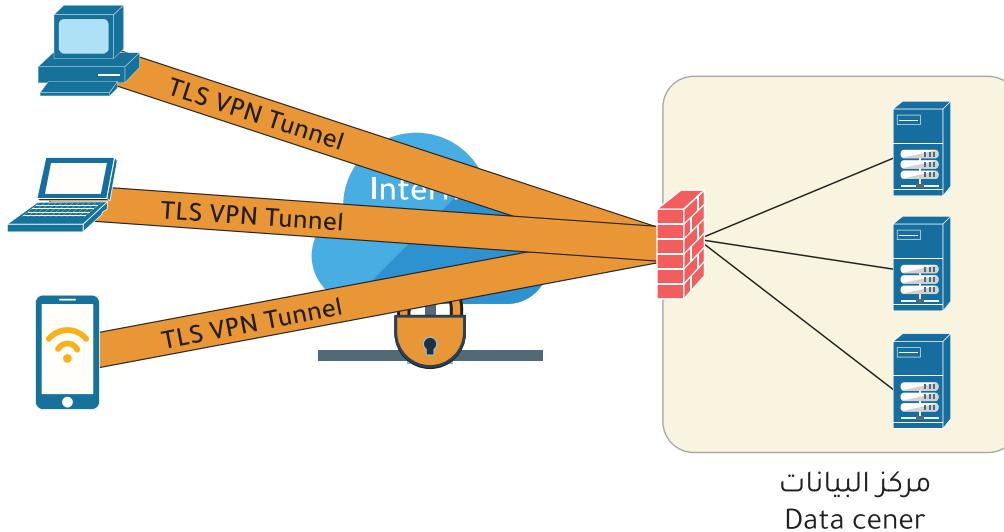
### ملاحظة :

الـ IPsec لا يدعم البث broadcast والبث المتعدد multicast إنما يدعم البث الأحادي unicast ، هذا يعني أنه لا يمكن استخدام بروتوكولات التوجيه مثل الـ ospf عبر النفق tunnel .

لأن بروتوكولات التوجيه تعتمد على حركة المرور بنظام الـ multicast لذلك يمكن حلها باستخدام GRE عبر الـ IPsec .



## TLS باستخدام Remote-access VPNs



شبكات الـ VPN للوصول عن بعد :  
تُستخدم هذه الشبكات للسماح للأجهزة الطرفية (أجهزة الكمبيوتر والهواتف المحمولة) بالوصول إلى موارد الشركة الداخلية بشكل آمن عبر شبكة الإنترنت.

- بمعنى أنه يتم تثبيت برنامج عميل VPN (VPN Client) على الأجهزة الطرفية مثل أجهزة الكمبيوتر المحمولة التي يستخدمها الموظفون للعمل من المنزل لكي يتم الاتصال بشكل آمن والدخول على موارد الشركة الداخلية عبر الانترنت .

- تستخدم شبكات VPN التي يمكن الوصول إليها عن بعد ببروتوكول الـ Transport Layer Security (TLS) أمان طبقة النقل .
- أيضاً الـ TLS يوفر الأمان لبروتوكول الـ HTTPS

## الشبكات اللاسلكية

### Wireless Networks



#### في الشبكات اللاسلكية ، من المهم جداً :

- 1 - تشفير البيانات حتى داخل الشبكة المحلية ، وإلا فإن أي شخص لديه جهاز في نطاق جهاز الإرسال يمكنه الوصول إلى تلك البيانات.
- 2 - استخدام الـ CSMA / CA لتجنب الاصطدامات في البيانات لكي يتم اكتشاف التصادمات قبل حدوثها وتجنبها .

الفرق بين CSMA / CD و CSMA / CA : تستخدم في الشبكات اللاسلكية لتجنب الاصطدامات في البيانات وايضاً لاكتشاف التصادمات قبل حدوثها وتجنبها .

CSMA / CD : تستخدم في الشبكات السلكية لاكتشاف الاصطدامات و حلها .

#### الشبكات المحلية اللاسلكية Wireless Lan Network (WLAN)

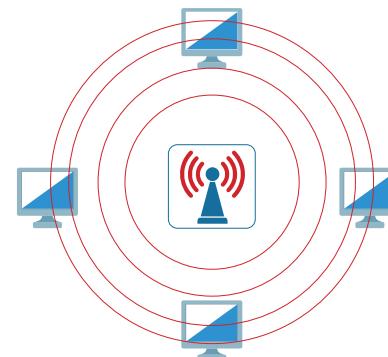
- المعايير التي تستخدمها للشبكات المحلية اللاسلكية معرفة بـ IEEE 802.11 .



- مصطلح Wi-Fi هو علامة تجارية لتحالف IEEE و هو غير متصل مباشرة بـ IEEE . يمكن للأجهزة التي تم اعتمادها لشبكة Wi-Fi أن تستخدم علامة Wi-Fi المعتمدة مثل هذه الصورة

- الشبكات اللاسلكية بها بعض المشكلات التي تحتاج إلى التعامل معها :

عندما يرسل جهاز لاسلكي إطاراً ، ستمكن جميع الأجهزة التي تدعم اللاسلكي داخل النطاق من التقاط هذا الإطار وهذا قد يؤدي هذا إلى مخاوف تتعلق بخصوصية البيانات . بالإضافة إلى مخاوف حدوث تصادم البيانات عند اتصال الأجهزة على نفس القناة في نفس الوقت .



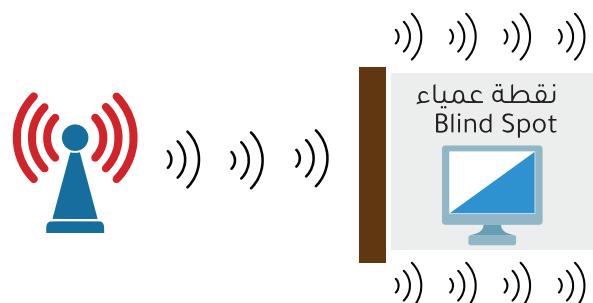
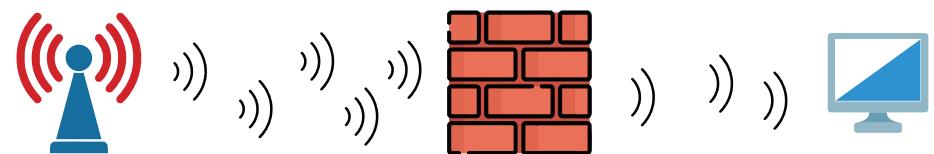
في التوصيلات اللاسلكية هناك عوامل قد تضعف جودة الإشارة  
فيجب أن نأخذها في الاعتبار ومنها :

### 1- مدى الإشارة :

تعني إلى أي مدى يمكن للإشارة أن تصل وبعدها تقطع الإشارة  
وهناك عوامل تؤثر على المدى الذي يمكن للإشارة أن تنتقل فيه  
بشكل سليم :

### A- الامتصاص absorption

عندما يرسل الجهاز إشارة لاسلكية فإن الجدار يمتص بعض الإشارات  
، مما ينتج عنه ضعف في الإشارة التي تصل للكمبيوتر.



B- الانعكاس reflection

يحدث الانعكاس عندما ترتد الإشارة من مادة ما ، على سبيل المثال  
المعدن.

- إذا كان هناك جدار معدني بين نقطة وصول وجهاز كمبيوتر ، فعلى  
الأرجح لن يتلقى الكمبيوتر إشارة جيدة من نقطة الوصول لأن الكثير  
من الإشارة ستتردد من الجدار المعدني .



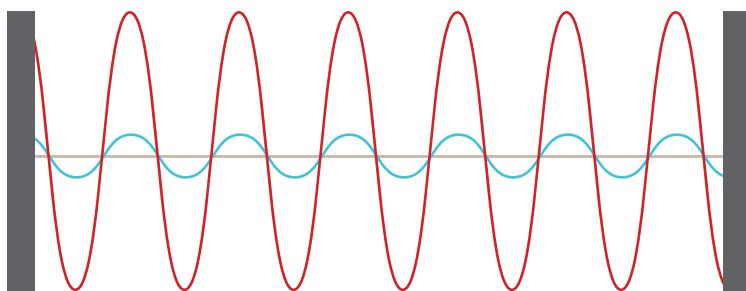
**تردد الراديو****Radio Frequency (RF)**

هو نطاق من ترددات الموجات الكهرومغناطيسية التي تم تخصيصها لأغراض مختلفة، بما في ذلك راديو AM و FM وأجهزة الميكروويف والرادار والواي فاي.

يمكن قياس الموجات الكهرومغناطيسية بعدة طرق، على سبيل المثال السعة **amplitude** و التردد **frequency**.

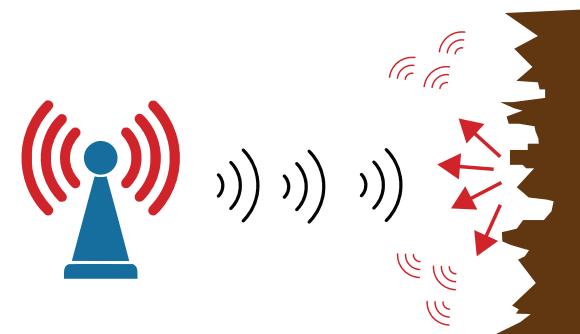
**السعة**

السعة هي أقصى قوة للمجالين الكهربائي والمغناطيسي. على سبيل المثال، انظر إلى هاتين الموجتين.



الأحمر: سعة أعلى  
الأزرق: سعة أقل

- D - **التشتت** Scattering
  - يحدث التشتت عندما تتسبب المادة في تشتت الإشارة في جميع الاتجاهات.
  - مثل امكانية أن يتسبب الغبار والضباب الدخاني والأسطح الغير مستوية إلى تأثير الإشارة.
  - فمثلاً عندما تضرب إشارة من نقطة الوصول اللاسلكية هذا السطح غير المستوي، تنتشر الإشارة في جميع الاتجاهات.

**2 - التداخل** : interference

هي تداخل القنوات التي تستخدمها الأجهزة في بث الإشارة. فقد تتسبب الأجهزة الأخرى التي تستخدم نفس القنوات في حدوث تداخل.

على سبيل المثال، شبكة جارك اللاسلكية تكون بثها على نفس قناة جهازك الذي يبث إشارة لا سلكية.

- ترددات الراديو التي نهتم بها هي التي تكون من 30 هرتز إلى 300 جيجا هرتز ويتم استخدامها لأغراض عديدة.

### بعض ترددات الـ Wi-Fi المهمة لنا :

**الأول : تردد 2.4 جيجا هرتز (GHz band 2.4)**

( من 2.4 GHz إلى 2.4835 GHz )

يغطي التردد 2.4 جيجا هرتز مساحات أكبر في المناطق المفتوحة واختراقاً أفضل للعقبات مثل الجدران.

**الثاني: تردد 5 جيجاهertz (GHz band 5)**

( من 5.150 GHz إلى 5.825 GHz )

**الثالث : تردد 6 جيجا هرتز (GHz band 6)**

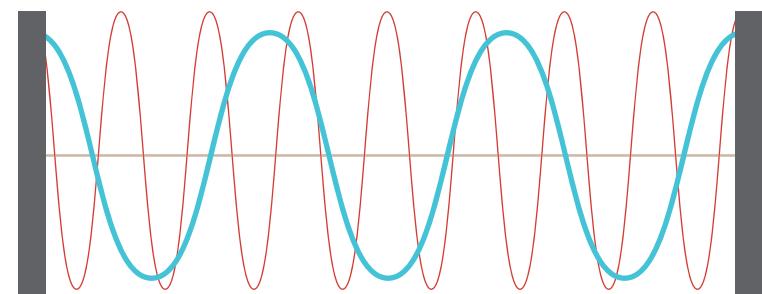
هو واي فاي 6 (Wi-Fi 6) ذو معيار قياسي من منظمة ieee يسمى بـ 802.11ax .

### ● التردد frequency

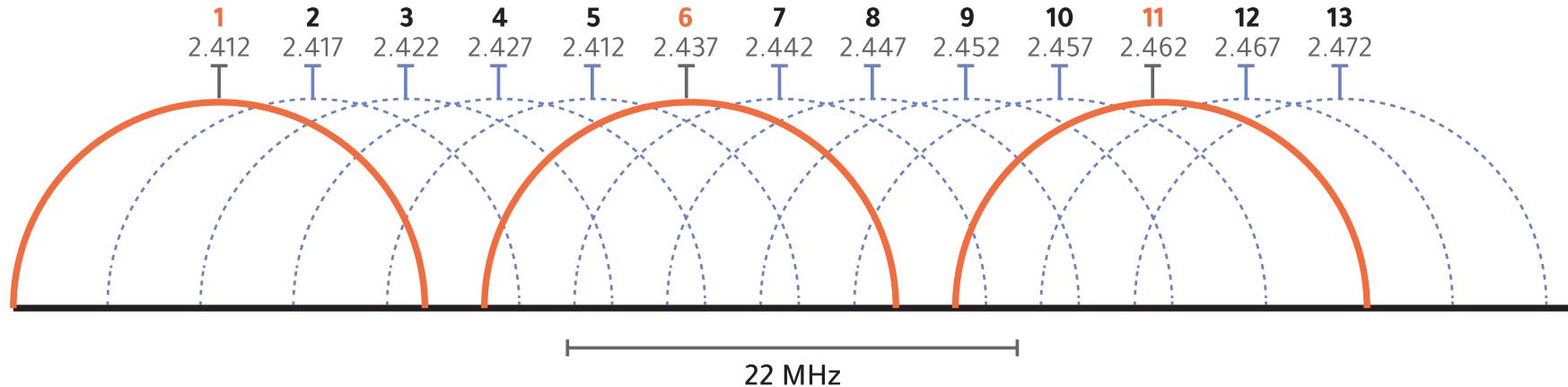
يقيس التردد عدد الدورات لأعلى / لأسفل لكل وحدة زمنية معينة.

يُقاس التردد بمقاييس يسمى هرتز (Hz) هو عدد الدورات في الثانية (s).

Hz (Hertz)	:	دورة واحدة في الثانية
kHz (Kilohertz)	:	ألف دورة في الثانية
MHz (Megahertz)	:	مليون دورة في الثانية
GHz (Gigahertz)	:	مليار دورة في الثانية
THz (Terahertz)	:	تيرابايت دورة في الثانية



المعيار standard	التردد frequency	سرعة النقل	المسمى
802.11	2.4 GHz	2 Mbps	-
802.11b	2.4 GHz	11 Mbps	-
802.11a	5 GHz	54 Mbps	-
802.11g	2.4 GHz	54 Mbps	-
802.11n	2.4 / 5 GHz	600 Mbps	Wi-Fi 4
802.11ac	5 GHz	6.93 Gbps	Wi-Fi 5
802.11ax	2.4 / 5 / 6 GHz	4 * 802.11ac	Wi-Fi 6



القناة Channel	التردد بالهرتز (MHz)	مدى التردد Frequency range
1	2412	2401-2423
2	2417	2406-2428
3	2422	2411-2433
4	2427	2416-2438
5	2432	2421-2443
6	2437	2426-2448
7	2442	2431-2453
8	2447	2436-2458
9	2452	2441-2463
10	2457	2446-2468
11	2462	2451-2473
12	2467	2456-2478
13	2472	2461-2483

### القنوات ≡

يتم تقسيم كل نطاق إلى قنوات متعددة ، ويتم إعداد الأجهزة لنقل واستقبال حركة المرور على واحدة أو أكثر من هذه القنوات.

على سبيل المثال ، يتم تقسيم النطاق 2.4 جيجا هرتز إلى عدة قنوات ، كل منها بمدى 22 ميجا هرتز.

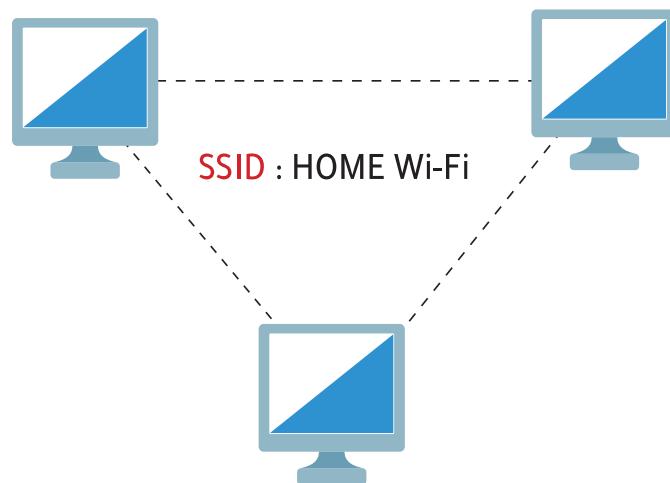
- أحد الجوانب المهمة لهذه القنوات هو أنها تتدافع مع بعض .

- على سبيل المثال ، القناة 1 تتدافع مع القنوات 2 و 3 و 4 و 5 و 6 و 7 .

لتجنب التدالع بين نقاط الوصول اللاسلكية المجاورة نستخدم قنوات لا تتدالع مع بعض .

- في التردد 2.4 جيجا هرتز، يوصى باستخدام ثلاث قنوات ، 1 و 6 و 11 .

**أولاً : مجموعة الخدمات الأساسية المستقلة**  
**Independent Basic Service Set (IBSS)**  
 هي شبكة لاسلكية يتصل فيها جهازان لاسلكيان أو أكثر مباشرة دون استخدام نقطة وصول (Access Point).



————— شبكة سلكية  
----- شبكة لاسلكية

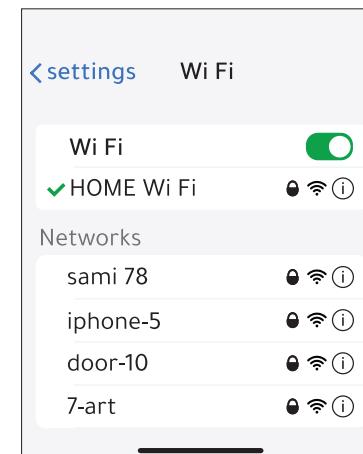
### مجموعات الخدمة Service Sets

تعني «مجموعات الخدمة» هي مجموعة من أجهزة الشبكات اللاسلكية التي لها نفس المعايير ومن ضمنها الواي فاي. يعرّف معيار الـ 802.11 802.11 أنواعاً مختلفة من مجموعات الخدمة . Service Sets

**هناك ثلاثة أنواع رئيسية :**

- أولاً : - مجموعات الخدمة المستقلة Independent Basic Service Set
- ثانياً : - ومجموعات خدمات البنية التحتية Infrastructure
- ثالثاً : - مجموعات خدمات الشبكة Mesh

**تعريف مجموعة الخدمة Service Set Identifier (SSID)**  
 الـ **SSID** هو اسم الشبكة التي يظهر لك أثناء البحث عن شبكة واي فاي والاسم يمكن قراءته من قبل الإنسان مثل (HOME Wi-Fi) .



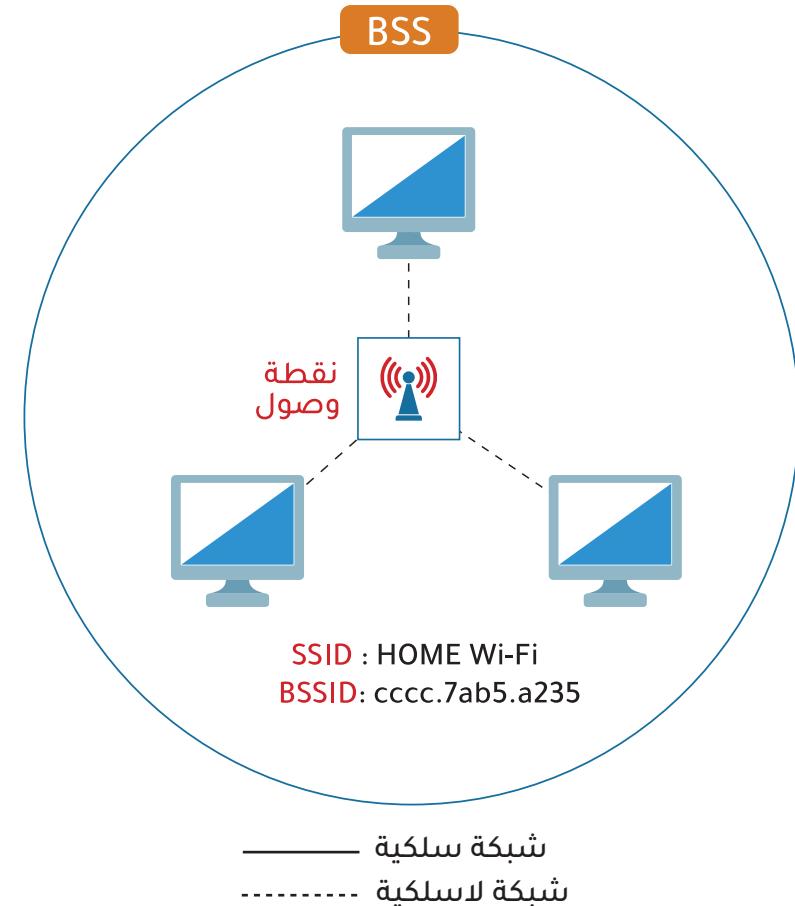
- معرف مجموعة الخدمات الأساسية (BSSID) . Access Point يقصد به عنوان الماك أدرس لنقطة الوصول . تسمى الأجهزة اللاسلكية المرتبطة بـ BSS (أجهزة متواصله مع بعضها لاسلكيًّا عبر نقطة وصول ) بالعملاء clients أو بالمحطات stations .

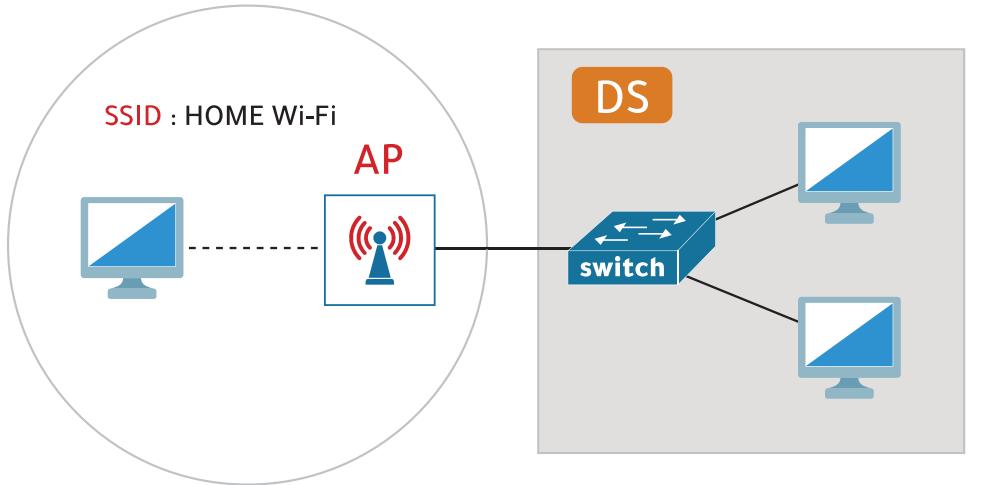
#### (Basic Service Area) BSA -

الـ BSA هي المنطقة المغطاة بالإشارة اللاسلكية التي تبئها نقطة الوصول في الـ BSS حيث يمكن للأجهزة الارتباط بهذه الشبكة الموجودة في الـ BSS .

#### ثانياً : - مجموعات خدمات البنية التحتية Infrastructure Basic Service Set (BSS) - A

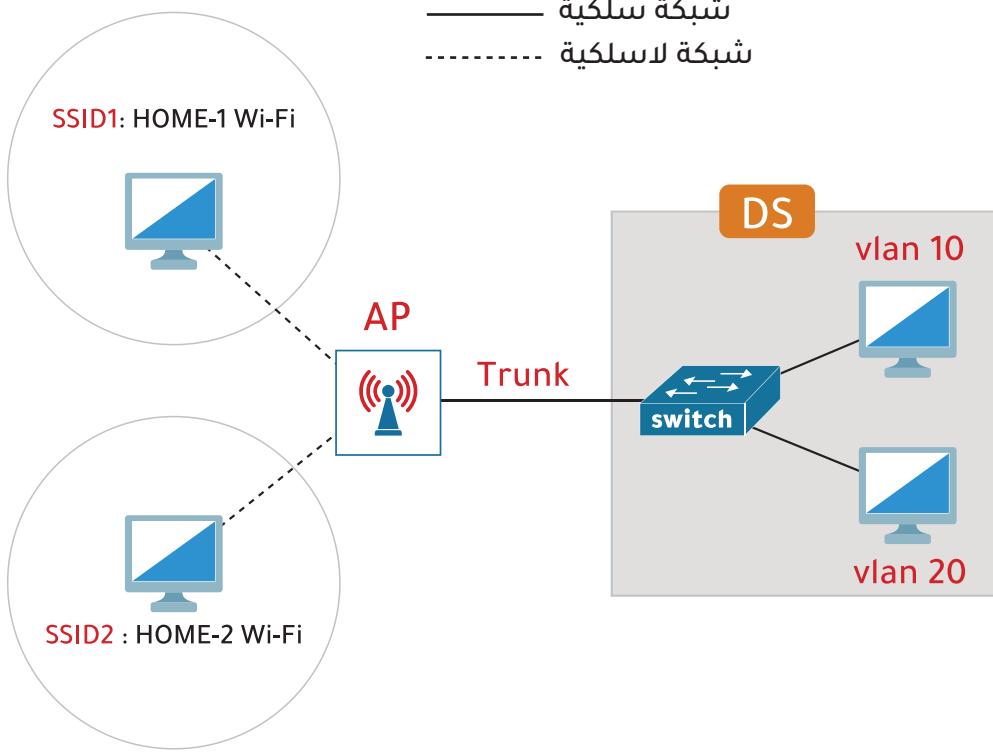
هي مجموعة أجهزة متواصله مع بعضها البعض لاسلكيًّا عبر نقطة وصول ( Access Point ) . في هذا النوع يتواصل العملاء مع بعضهم البعض لاسلكياً عبر نقطة وصول ( Access Point ) ولكن ليس مع بعضهم البعض مباشرة .





**Distribution System (DS) - B**

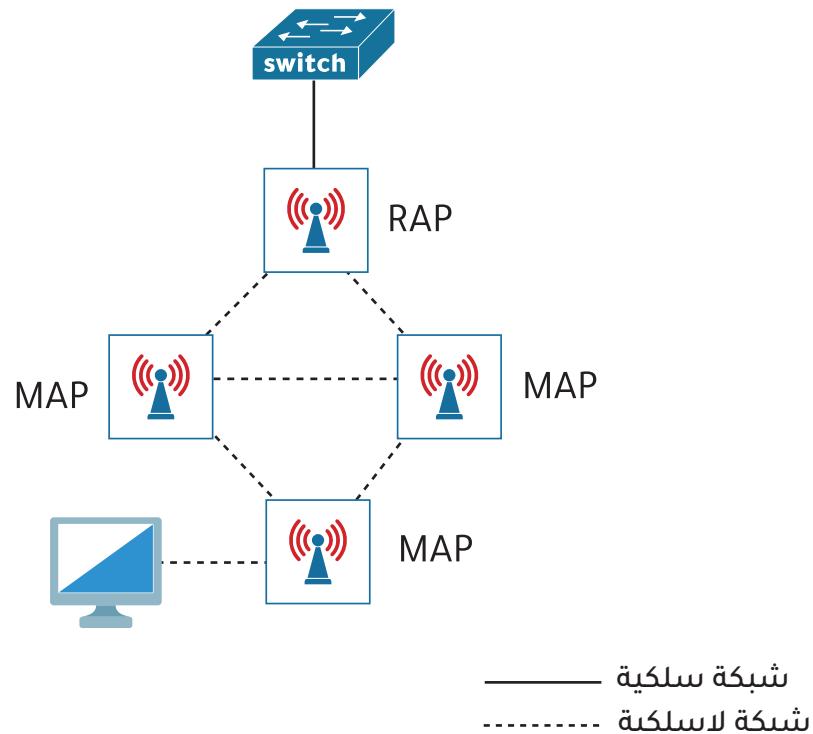
هي نظام التوزيع في الشبكة السلكية التي تقع ما بعد نقطة الوصول .  
-معنی ربط الشبكة السلكية المحلية بنقطة الوصول اللاسلكية المحلية .



**ربط الفيلان بالSSID في نظام التوزيع**  
**Mapping a VLAN to an SSID**

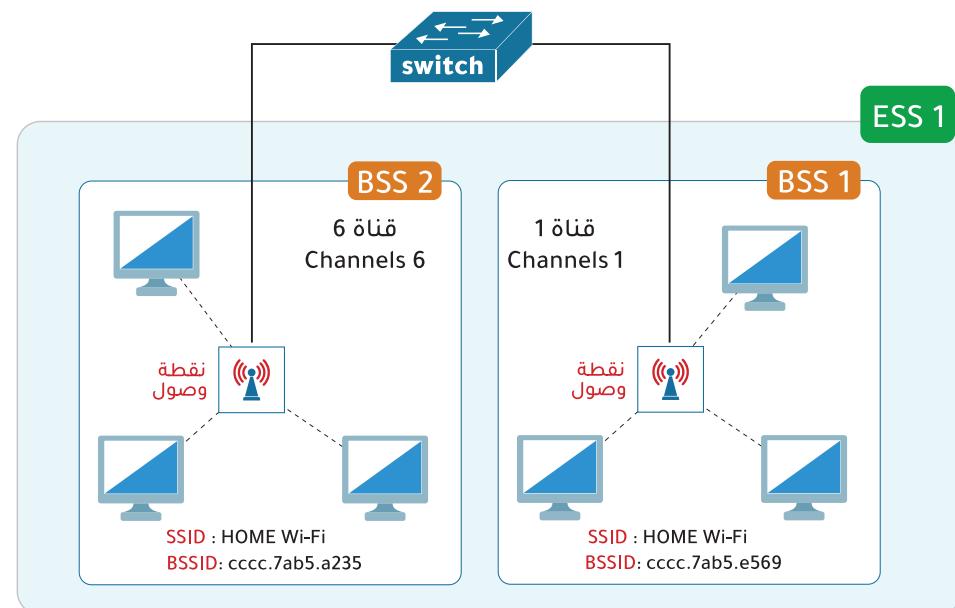
يتم ربط الفيلانات في نظام التوزيع مع اسماء الشبكات اللاسلكية  
بشرط أن يكون وضع المنفذ الموصول بنقطة الوصول في وضع  
. Trunk .

**ثالثاً : مجموعات خدمات الشبكة المتداخلة**  
**Mesh Basic Service Set (MBSS)**  
 هي شبكة مكونة من عدة نقاط وصول متصلة مع بعضها البعض لا سلكياً بهدف توسيع نطاق البث والسرعة واستمرارية الاتصال .  
 يتم توصيل نقطة وصول واحدة على الأقل بالشبكة السلكية ، وتسمى (RAP) (Root Access Point)  
 والأجهزة الباقيه تسمى بـ (MAPs) (Mesh Access Points)



**C - مجموعة خدمات موسعة (ESS)**  
 تستخدم لإنشاء شبكات LAN لاسلكية أكبر من نطاق نقطة وصول واحدة .  
 - يتم توصيل نقاط الوصول بـ BSS1 و BSS2 بواسطة السويتش .  
 - كل BSS تستخدم نفس الـ SSID مع اختلاف الـ BSSID .  
 - كل BSS يستخدم قناة مختلفة لتجنب التداخل . لاحظ الاولى قناة 1 والاخرى قناة 6 .

هو تنقل العملاء بين نقاط الوصول في الـ ESS دون الحاجة إلى إعادة الاتصال بالشبكة .



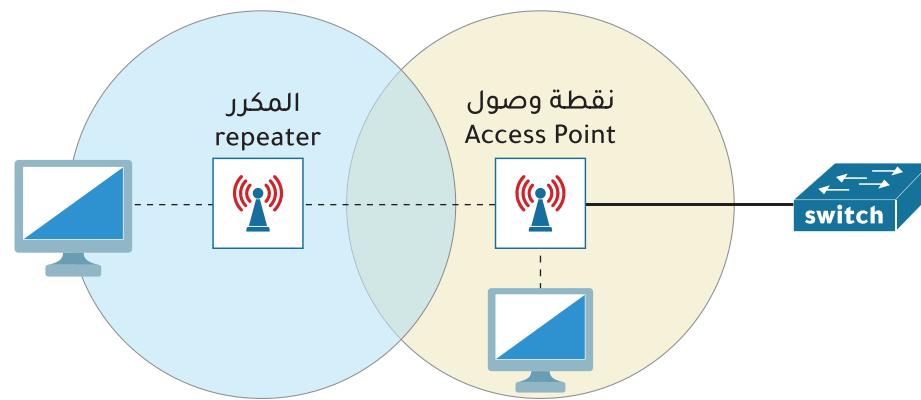
### بعض الأوضاع التي يمكن أن تعمل بها نقاط الوصول في الشبكات اللاسلكية

#### - المكرر repeater

نقطة وصول في وضع التكرار repeater يمكن استخدامها لتوسيع نطاق BSS.

- سيعيد المكرر ببساطة إرسال أي إشارة يتلقاها من نقطة الوصول ، مما يوسع نطاق BSS الخاص بنقطة الوصول.

- يمكن للمكرر أن يستقبل على قناة واحدة ثم يعيد الإرسال على قناة أخرى.



#### - outdoor bridge

هو ربط خارجي لموقعين أو نقطتين وصول لتوصيل الشبكات عبر مسافات طويلة لا سلكيا.

- الربط قد يكون من نقطة وصول إلى نقطة وصول أو من نقطة وصول إلى عدة نقاط وصول .



### workgroup bridge (WGB) -

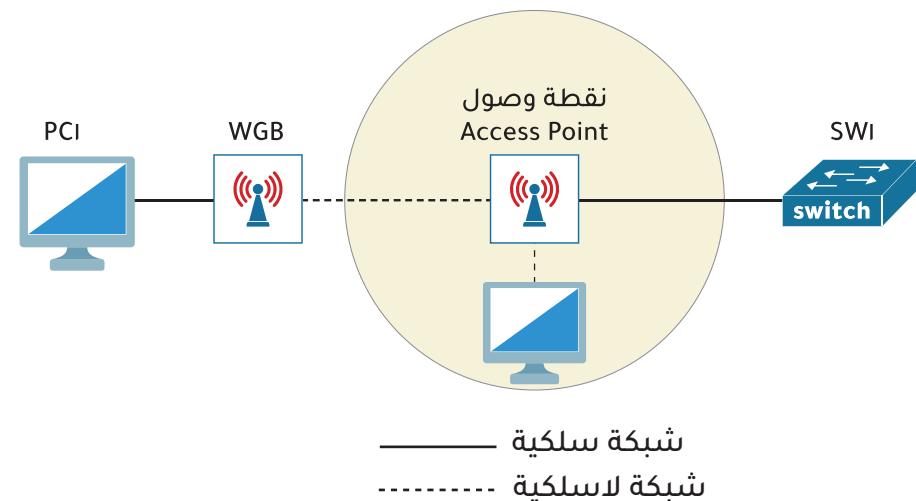
هو الذي يسمح للعملاء الذين لا يدعمون الاتصالات اللاسلكية بالاتصال بالشبكة اللاسلكية عبر نقطة وصول تعمل كجسر مجموعه عمل.

ينقسم الـ **WGB** الى نوعين:  
**Universal WGB (uWGB) - 1**

هو معيار 802.11 يسمح بتوصيل جهاز واحد سلكيا بالشبكة اللاسلكية.

**WGB - 2**

هو الذي يسمح بتوصيل عدة أجهزة سلكيا بالشبكة اللاسلكية.



جهاز PC1 لا يملك طريقة للاتصال لاسلكيا ولا يمكنه الوصول سلكيا بالسويفتش لذلك يتم عمل نقطة وصول تعمل كجسر تربط الـ PC1 سلكيا ونقطة الوصول الأخرى لاسلكيا .

## معمارية الشبكات اللاسلكية

### Wireless Architecture

نقصد بها المعايير التي تحتاجها لتصميم الشبكات اللاسلكية المحلية .

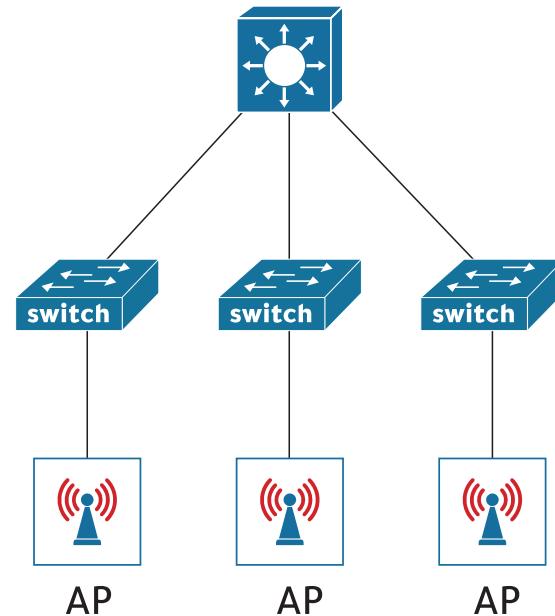
#### Autonomous AP (01)

طريقة بناء شبكة لا سلكية محلية تستخدم أجهزة نقاط وصول مستقلة بحد ذاتها ، ولا تعتمد على وحدة تحكم لاسلكية محلية Wireless LAN controller (wlc) .

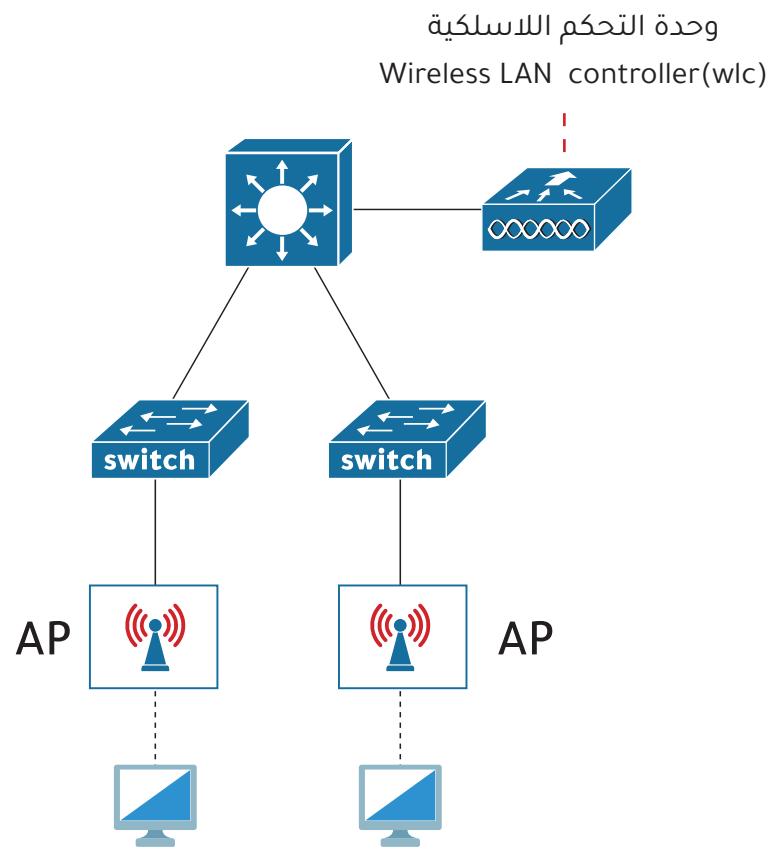
- هذا يعني أنه يتم تهيئة وتكوين إعدادات كل نقطة وصول بشكل فردي ومستقل بواسطة كيبيل الوكونسول أو عن بعد عبر telnet أو SSH ، أو أيضًا عبر اتصال ويب (GUI) HTTP/HTTPS connection(ip -password -SSID- Channel) .

- الإعدادات في نقطة الوصول مثل اسم الشبكة والايبي والقنوات وكلمة المرور (ip -password -SSID- Channel) .

- يمكن استخدام نقاط الوصول المستقلة في الشبكات الصغيرة ، لكنها غير قابلة للتطبيق في الشبكات المتوسطة إلى الكبيرة .  
فلو كان لديك مئات نقاط الوصول فمن غير المعقول الدخول على كل نقطة وصول وعمل إعدادات لها .



## Split MAC AP 02



- تسمى ب Lightweight APs نقاط وصول خفيفة الوزن .
- تنقسم وظائف الادارة والعمليات بين نقاط الوصول AP وبين وحدة التحكم اللاسلكية wlc .

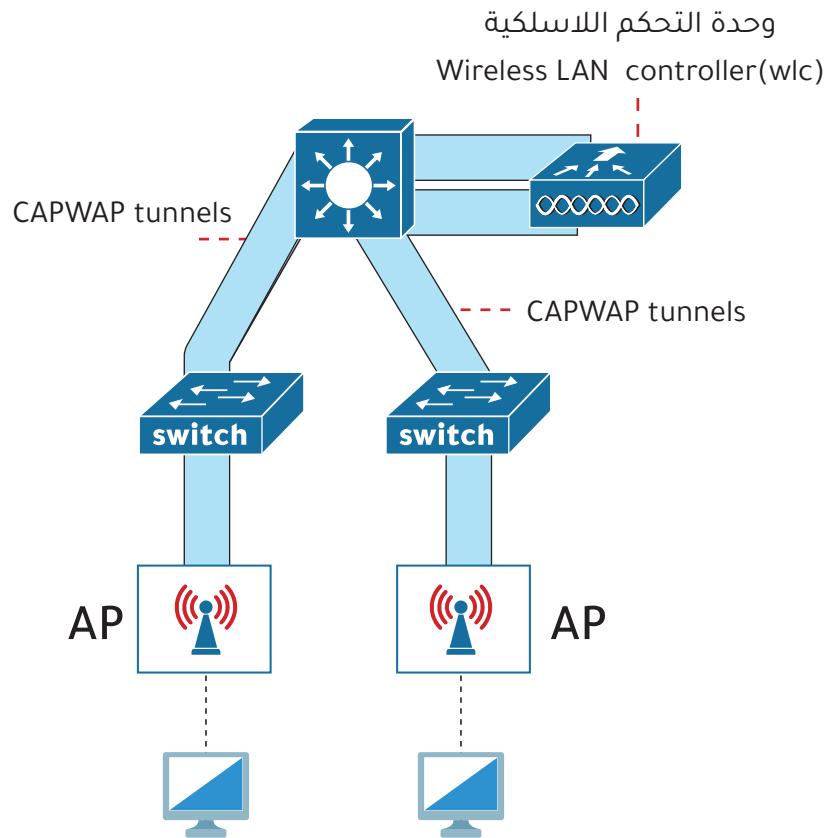
- تعامل نقاط الوصول الا Lightweight مع بعض العمليات مثل إرسال / استقبال حركة مرور (transmitting / receiving traffic) و تشفير / فك تشفير حركة المرور (encryption/decryption of traffic) .

بينما يتم تنفيذ الوظائف الأخرى بواسطة الـ WLC . على سبيل المثال :

- إدارة الترددات اللاسلكية (RF management) - الأمان (security)
- جودة الخدمة (QoS) - الإدارة (management) - مصادقة العميل (client association)

- يتم استخدام الـ wlc لتكوين إعدادات نقاط الوصول مركزيا .  
- تقوم وحدة التحكم اللاسلكية (wlc) ونقاط الوصول خفيفة الوزن (Lightweight APs) بالصادقة والتوثيق بين بعضهما البعض باستخدام الشهادات الرقمية المثبتة على كل جهاز .

- تستخدم وحدة التحكم اللاسلكية (wlc) ونقاط الوصول خفيفة الوزن (Lightweight APs) بروتوكولًا يسمى CAPWAP (Control And Provisioning Of Wireless Access Points) للتحكم في نقاط الوصول اللاسلكية وربطها مع بعض للتواصل .



- يتم إنشاء نفقين ( tunnels ) بين كل نقطة وصول وـ WLC :

#### Control tunnel (UDP port 5246) - A

نفق التحكم يستخدم منفذ UDP 5246 .

يستخدم هذا النفق لتكوين إعدادات نقاط الوصول والتحكم وإدارة العمليات.

- كل حركة المرور في هذا النفق مشفرة بشكل افتراضي.

#### Data tunnel (UDP port 5247) - B

نفق البيانات يستخدم منفذ UDP 5247

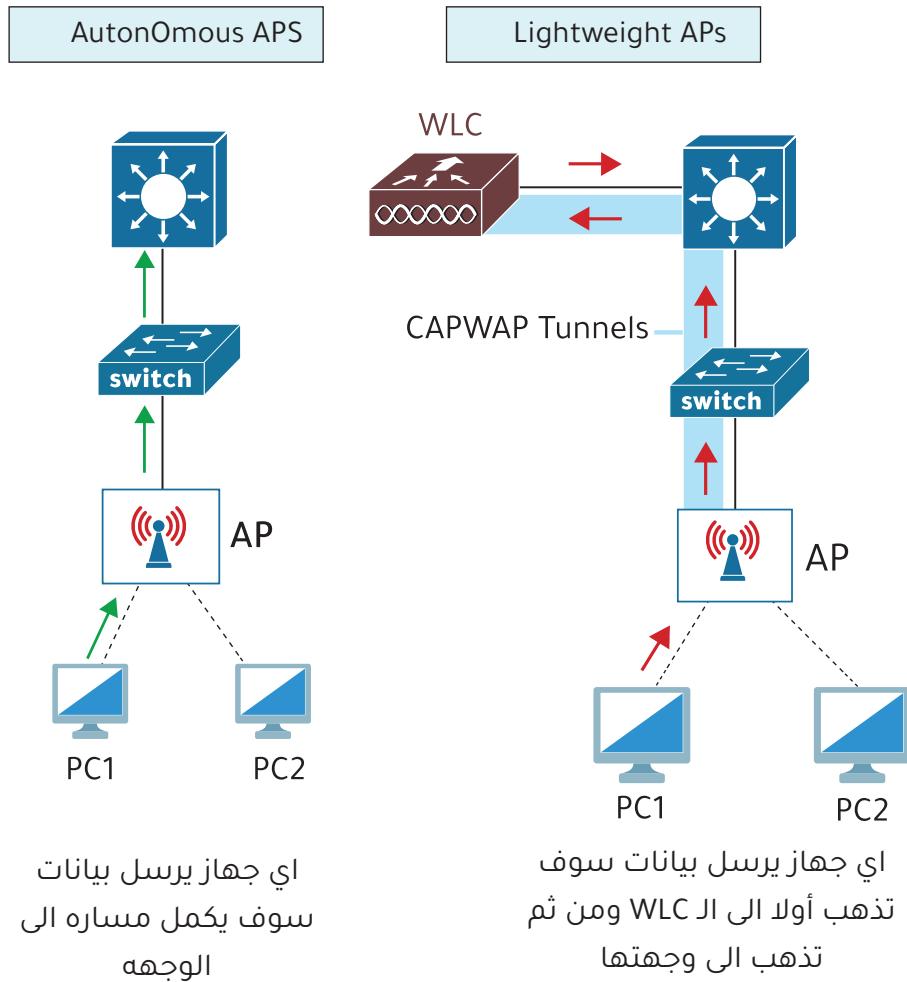
- كل البيانات التي تأتي من العملاء اللاسلكين يتم ارسالها عبر هذا النفق الى وحدة التحكم اللاسلكية WLC أولا ثم تذهب الى وجهتها.

- لا يتم تشفير حركة المرور في هذا النفق افتراضياً ، ولكن يمكن تشفيره باستخدام

**DTLS** (Datagram Transport Layer Security)

## بعض الفوائد الرئيسية لاستخدام Lightweight APs أو Split MAC AP

### الفرق بين الـ AutonOmous APS و Lightweight APs



1 - قابلية التوسيع : Scalability  
مع وحدة التحكم اللاسلكية (wlc) يمكن بناء ودعم شبكة كبيرة تتكون من آلاف من نقاط الوصول .

2 - تخصيص القناة بشكل ديناميكي Dynamic channel assignment  
يمكن لوحدة التحكم اللاسلكية (wlc) تحديد القناة التي تستخدمها كل نقطة وصول بشكل تلقائي .

3 - تحسين قدرة الإرسال Transmit power optimization  
يمكن لوحدة التحكم اللاسلكية (wlc) ضبط قدرة الإرسال المناسبة لكل نقطة وصول لتوفير تغطية كافية دون التداخل مع نقاط الوصول الأخرى.

4 - التجوال السلس Seamless roaming  
يمكن للعملاء التجوال بين نقاط الوصول دون قطع الاتصال ودون أي تأخير ملحوظ.

5 - موازنة حمل العميل Client load balancing  
إذا كان العميل في نطاق اثنين من نقاط الوصول ، فيمكن لوحدة التحكم اللاسلكية (wlc) ربط العميل بنقطة الوصول الأقل استخداماً ، لموازنة الحمل بين نقاط الوصول.

## ≡ يمكن تكوين نقاط الوصول خفيفة الوزن أو Lightweight أو Split MAC AP في أوضاع مختلفة :

### : Local - 1

هذا هو الوضع الافتراضي لنقطة الوصول خفيفة الوزن Lightweight حيث يتم ارسال كل حركة المرور (التحكم والبيانات) إلى وحدة التحكم (wlc) إلى وحدة التحكم (wlc) . إذا فقدنا الاتصال بوحدة التحكم اللاسلكية (wlc) ، فسيتم فصل نقطة الوصول .

### Sniffer Mode - 4

يقوم جهاز AP المفعل عليه هذا الوضع بالاستماع والتقط حركة البيانات في قناة مخصصة بين نقطة الوصول وبين العميل وارسالها الى برنامج مثل الـ Wireshark للتحليل والكشف .

### Monitor - 5

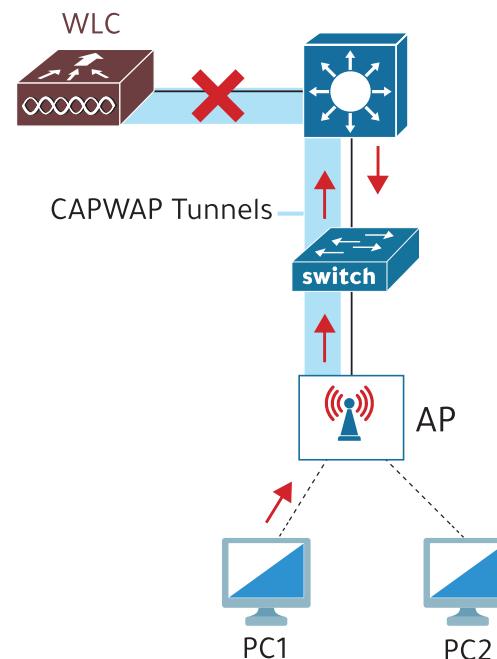
إذا كان العميل في نطاق اثنين من نقاط الوصول ،فيمكن لوحدة التحكم اللاسلكية (wlc) ربط العميل بنقطة الوصول الأقل استخداماً ، لموازنة الحمل بين نقاط الوصول.

### Rogue Mode - 6

هذا الوضع للكشف عن الأجهزة المحتالة والداخلة على شبكة سلكية.

### FlexConnect - 3

وضع الـ Flex connect هو نفس الوضع المحلي Local ولكن هو أكثر مرونة حيث لو تم فقد الاتصال بوحدة التحكم اللاسلكية (wlc) فإنه سوف يتم تبادل البيانات محليا عبر نقاط الوصول أو الأجهزة الرابطة بهم مثل السواليشات وغيرها وسيبقى العملاء الحاليين مرتبطين مع بعضهم البعض .

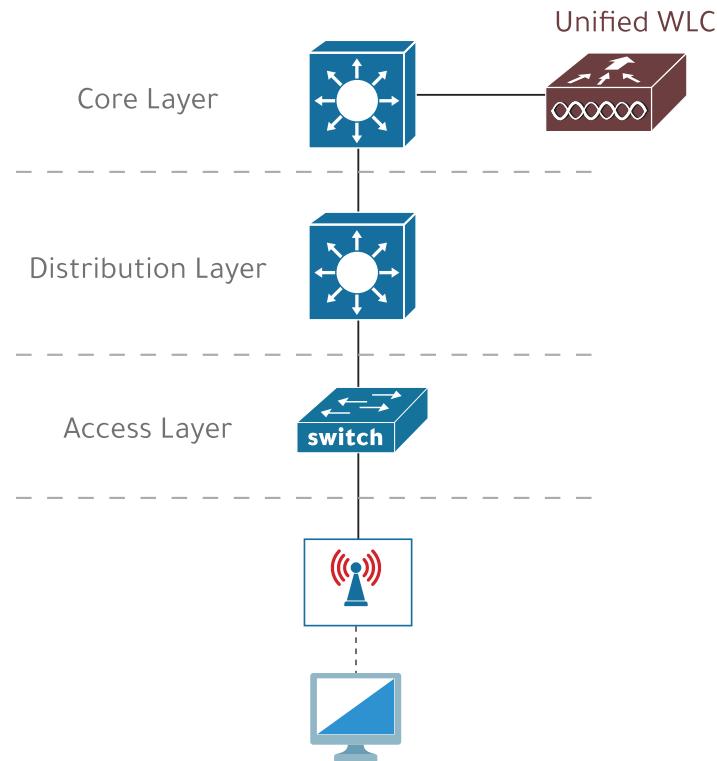


## WLC Deployments

- توجد 4 أماكن لنشر ووضع وحدة التحكم اللاسلكية WLC لدارة نقاط الوصول :

### Unified WLC - 1

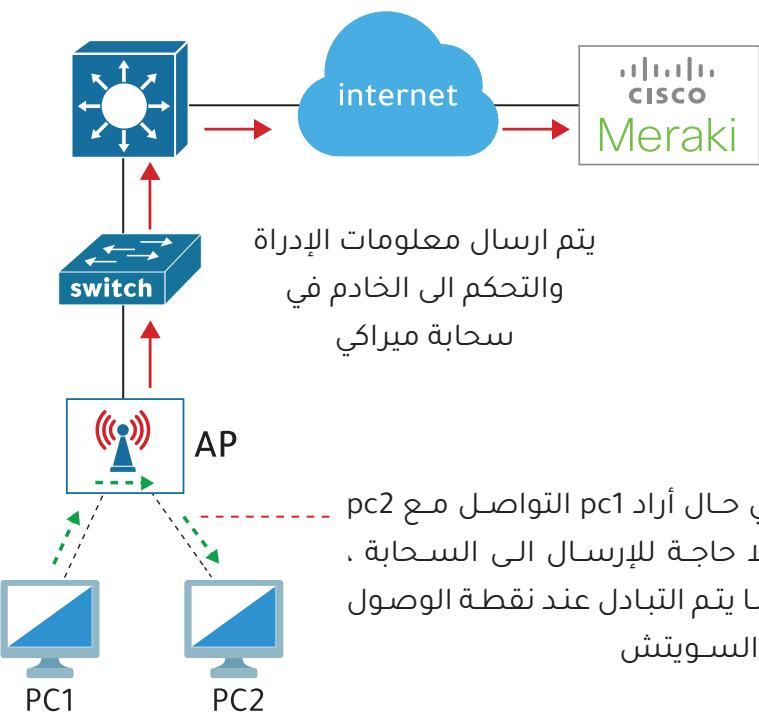
هو جهاز منفصل يتم نشره في نفس الشبكة.  
- يمكن لـ Unified WLC دعم ما يصل إلى 6000 نقطة وصول



## Cloud-based APs 03

نقاط وصول قائمة على السحابة يتم إدارة نقاط الوصول والتحكم بها مركزاً في السحابة، ومثال على ذلك Cisco Meraki.

- Cisco Meraki هو موقع إلكتروني تقوم بتسجيل الدخول إليه لتكوين إعدادات نقاط الوصول ومراقبة الشبكة وإنشاء تقارير الأداء وغيرها.
- يتم إرسال ملفات التحكم والإدارة فقط إلى السحابة أما حركة البيانات العادية لا يتم إرسالها إلى السحابة إنما يتم إرسالها مباشرة إلى الشبكة السلكية وتذهب إلى وجهتها.



يتم إرسال معلومات الإدراة والتحكم إلى الخادم في سحابة ميراكى

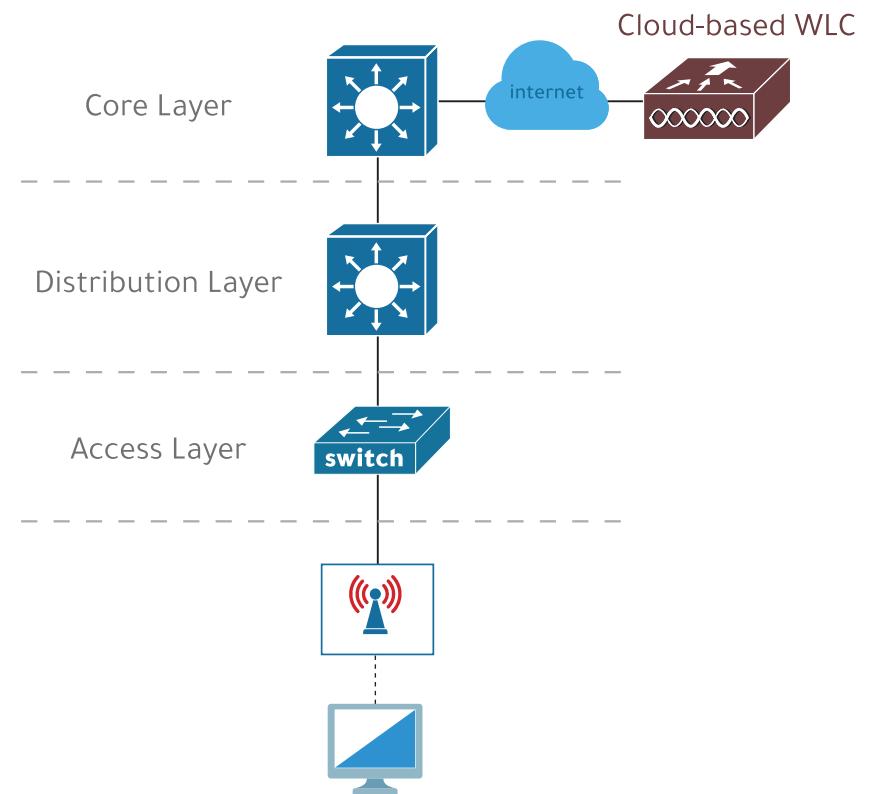
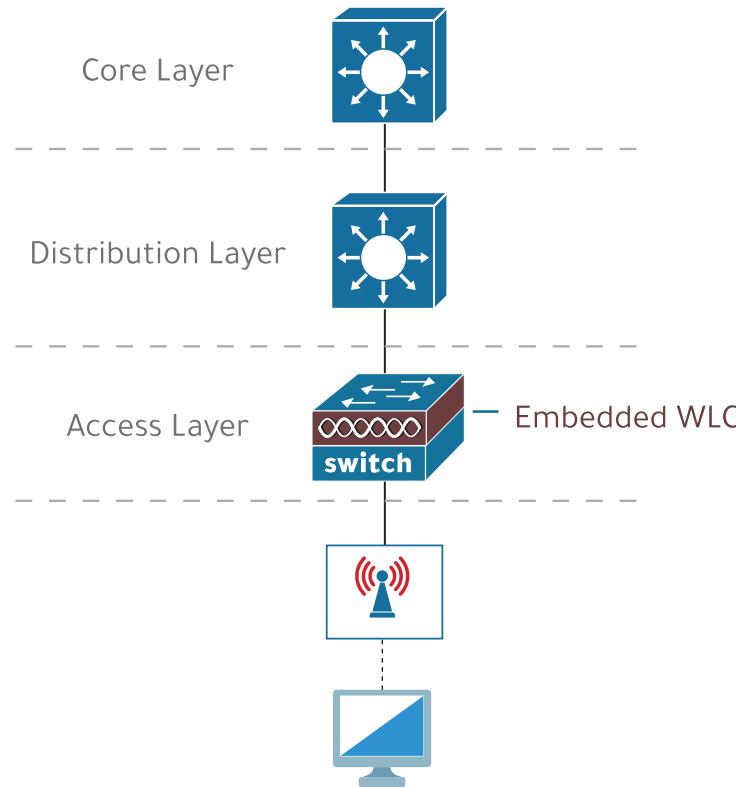
في حال أراد pc1 التواصل مع pc2 فلا حاجة للإرسال إلى السحابة. إنما يتم التبادل عند نقطة الوصول أو السويفت

### Embedded WLC - 3

يكون الـ WLC مدمجاً داخل السويفتش الأساسي .  
يدعم WLC Embedded إلى 200 نقطة وصول .

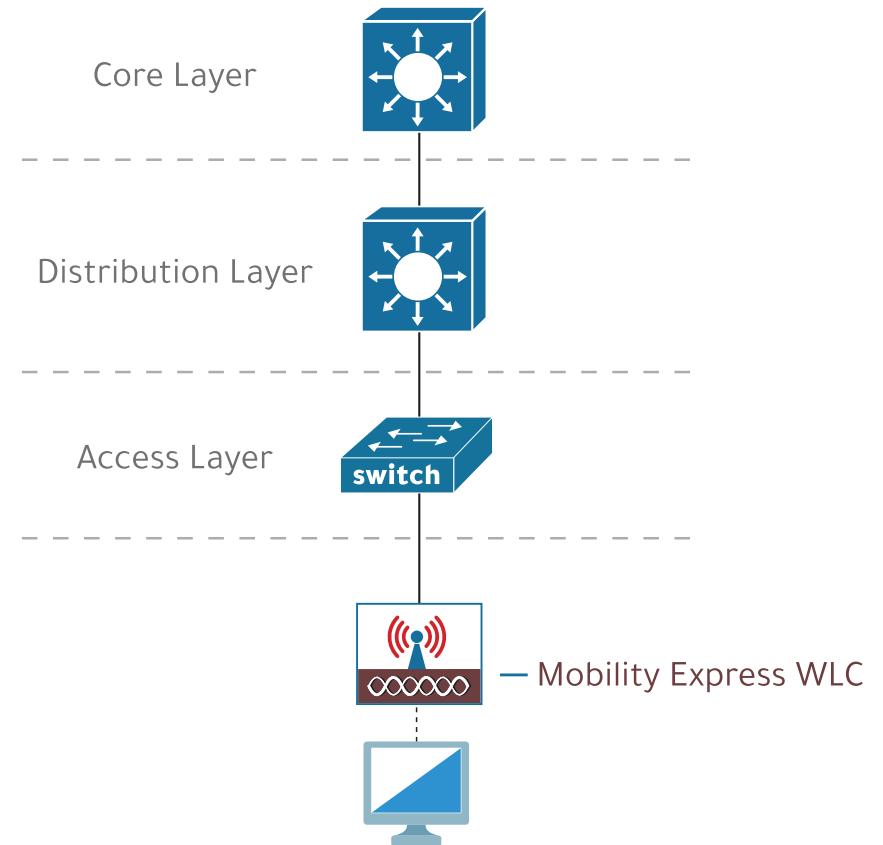
### Cloud-based WLC - 2

هو جهاز يتم وضعه في موقع ي العمل على السحابة .  
- يمكن لـ Cloud-based WLC دعم ما يصل إلى 3000 نقطة وصول .



#### Mobility Express WLC - 4

يكون إل WLC مدمجاً داخل نقطة الوصول .  
يدعم Mobility Express WLC إل 100 نقطة وصول.





## أمان الشبكات اللاسلكية Wireless Network Security

الأمان مهم في جميع الشبكات ، ولكن الأكثر أهمية يكون في الشبكات اللاسلكية، حيث يمكن لأي جهاز في نطاق الإشارة استقبال حركة المرور .

- في الشبكات اللاسلكية من المهم جداً تشفير حركة المرور المرسلة بين العملاء اللاسلكيين ونقطة الوصول .

- يلعب التشفير دوراً في جميع أنواع الشبكات ، ولكنه مهم بشكل خاص في الشبكات اللاسلكية لأن الإشارة يمكن أن يستقبلها أي شخص داخل نطاق المرسل ، وليس فقط المستلم المقصود .

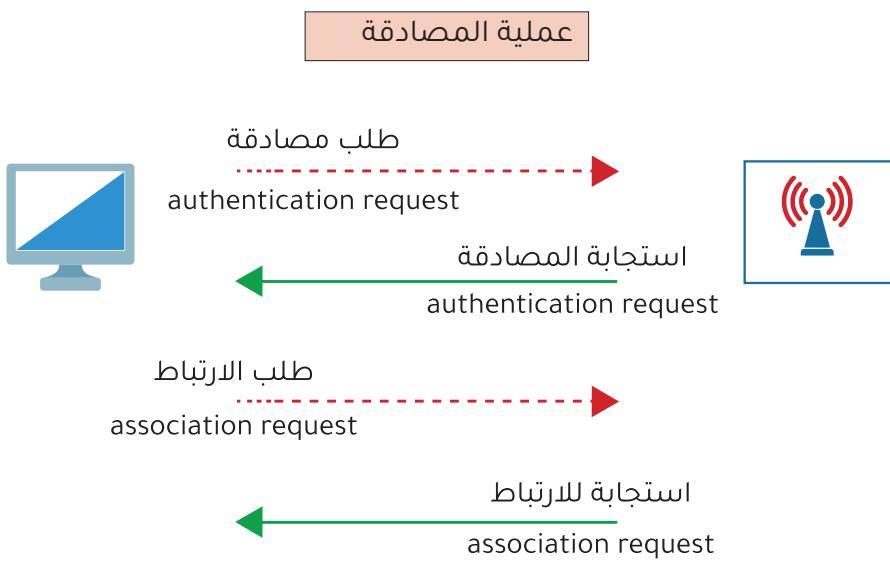
### مفاهيم الأمان الرئيسية حسب المعيار القياسي 802.11 :

- A - المصادقة Authentication
- B - التشفير Encryption
- C - السلامة أو التكامل Integrity

في إعداد الشركة ، يجب منح حق الوصول إلى الشبكة للمستخدمين والأجهزة الموثوق بهم فقط. أما الضيوف فيمكن توفير شبكة SSID منفصلة خاصة بهم بحيث لا يمكنهم الوصول إلى شبكة الشركة الخاصة ومواردها الداخلية .

#### طرق يمكن من خلالها إجراء المصادقة :

- استخدام كلمة مرور
- استخدام اسم مستخدم وكلمة مرور
- شهادات رقمية مثبتة على الأجهزة



### A - المصادقة Authentication

المصادقة هي التحقق فقط من هوية المستخدم أو الجهاز وليس التشفير.

- يجب أن تتم المصادقة لجميع العملاء قبل أن يتمكنوا من الارتباط بنقطة وصول.

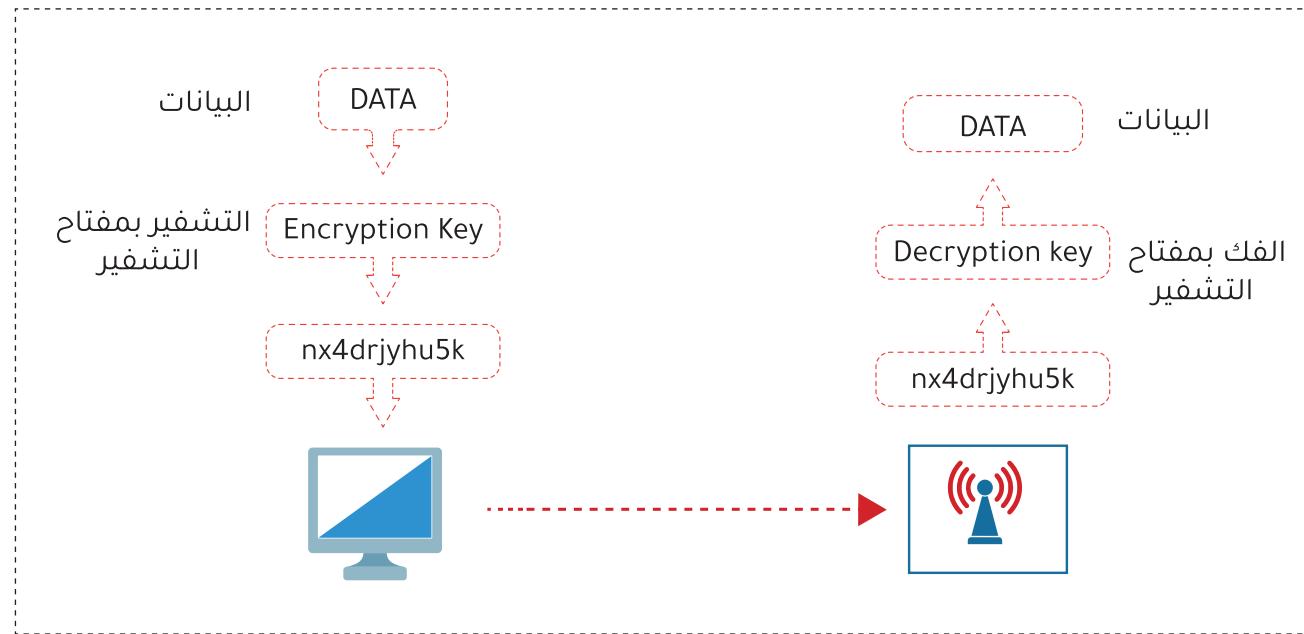
**B - التشفير Encryption**

- يجب تشفير أي حركة مرور لاسلكية بين العملاء ونقاط الوصول ، بحيث لا يمكن قراءتها من قبل أي شخص باستثناء AP والعميل.
- من المهم جداً أن يستخدم المرسل والمتلقي نفس بروتوكول التشفير .

- سيستخدم كل عميل مفتاح تشفير وفك تشفير فريد ومميز حتى لا تتمكن الأجهزة الأخرى من قراءة حركة المرور الخاصة به.

- سيكون لدى AP فقط المفتاح المناسب لفك تشفير حركة مرور العميل . ولن يمكن العملاء الآخرون من فك تشفيرها لأنهم يستخدمون مفاتيح مختلفة.

- سيكون لدى نقطة الوصول AP ( مفتاح مجموعة ) تستخدمه لتشفي حركة المرور التي تريد إرسالها إلى جميع عملائها . يحتفظ جميع هؤلاء العملاء بنسخة من مفتاح المجموعة هذا حتى يتمكنوا من فك تشفير حركة المرور.



## طرق المصادقة Authentication Methods



يتضمن معيار الـ 802.11 القياسي 3 خيارات للمصادقة :

### Open Authentication - 1

مصادقة مفتوحة : هو أن يرسل العميل طلب مصادقة إلى نقطة الوصول AP فيتم قبول طلبه.

- طريقة المصادقة المفتوحة ليست آمنة لأن نقطة الوصول تقبل جميع طلبات المصادقة.
- يمكن إضافة طريقة أخرى مثل صفحة ويب لتسجيل دخولك كما يحصل في المطارات .

### WEP (Wired Equivalent Privacy)- 2

- يستخدم الـ WEP لتوفير كل من المصادقة والتشفير لحركة المرور اللاسلكية.

- عند التشفير يستخدم الـ WEP خوارزمية RC4 .
- في بروتوكول الـ WEP يكون لدى كل من المرسل والمستقبل مفتاح مشترك shared-key، ويجب أن يكون نفس هذا المفتاح عند الاثنين .

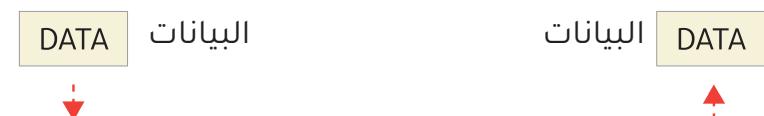
- تشفير الـ WEP ليس آمن ويمكن كسره بسهولة. لذلك بفضل عدم استخدامه في الشبكات اللاسلكية .

### C - السلامة أو التكامل Integrity

هو عدم تعديل الرسالة من قبل طرف ثالث ، وعدم تعديلها أثناء النقل بين المرسل والمستقبل .

- يجب أن تكون الرسالة التي يرسلها المرسل هي نفس الرسالة التي يتلقاها المستقبل.

- يتم إضافة الـ MIC (Message Integrity Check) إلى الرسائل لزيادة الأمان والحماية . وتعني فحص سلامة الرسالة .



تم عملية حسابية  
بخوارزمية معينة ويتم  
إضافة الـ mic



التشفير بمفتاح التشفير

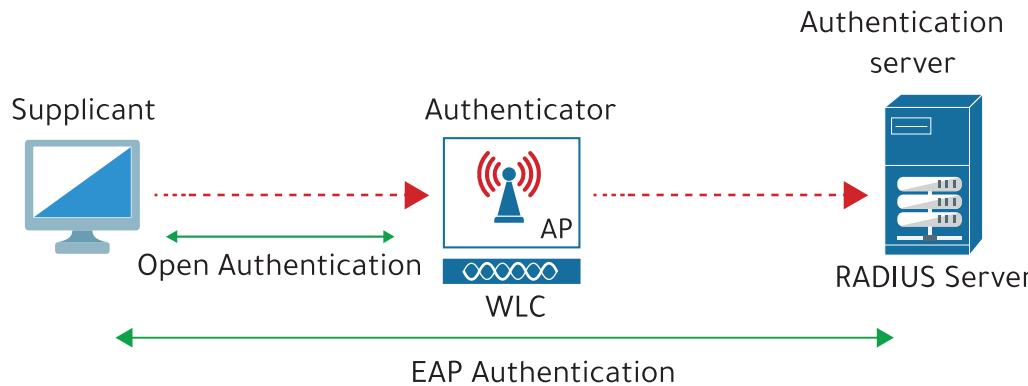
Encryption Key



فك التشفير

Decryption key



**802.1x/EAP - 3****(Extensible Authentication Protocol)**

هو إطار مصادقة تستند إليه العديد من البروتوكولات الأخرى ، التي تسمى طرق أو أساليب الـ EAP. ومن هذه الطرق :

.LEAP - EAP-FAST - PEAP - EAP-TLS

- يمكن دمج الـ EAP مع بروتوكول 802.1x :

a - السماح للعميل بارسال بيانات المصادقة فقط حتى يستكمل عملية المصادقة .

b - منع العميل من ارسال بيانات عادية قبل عملية المصادقة أو التوثيق .

**الخطوة الاولى المصادقة المفتوحة :**

يرتبط العميل بنقطة الوصول بمصادقة مفتوحة عبر بروتوكول اللاسلكي 802.11 .

- حركة المرور الوحيدة المسموح بها فقط للعميل هي حركة المرور المطلوبة التي تحتاج لمصادقة الـ EAP.

- العميل الان لا يتمتع حتى الان بوصول كامل إلى الشبكة لانه لم يتم مصادقة الـ EAP.

**الخطوة الثانية مصادقة الـ EAP :**

طرق مصادقة EAP المختلفة المستخدمة في الشبكات المحلية اللاسلكية :

.LEAP - EAP-FAST - PEAP - EAP-TLS

**802.1x Roles**

يمكن لأجهزة شبكة 802.1x استخدام الأدوار أو الوظائف التالية:

**Suplicant - 1**

هو الجهاز الذي يريد الإنضمام للشبكة .

**Authenticator - 2**

هو الجهاز الذي يوفر خدمة المصادقة أو التوثيق في الشبكة مثل نقطة الوصول Access point ووحدة التحكم اللاسلكية wlc .

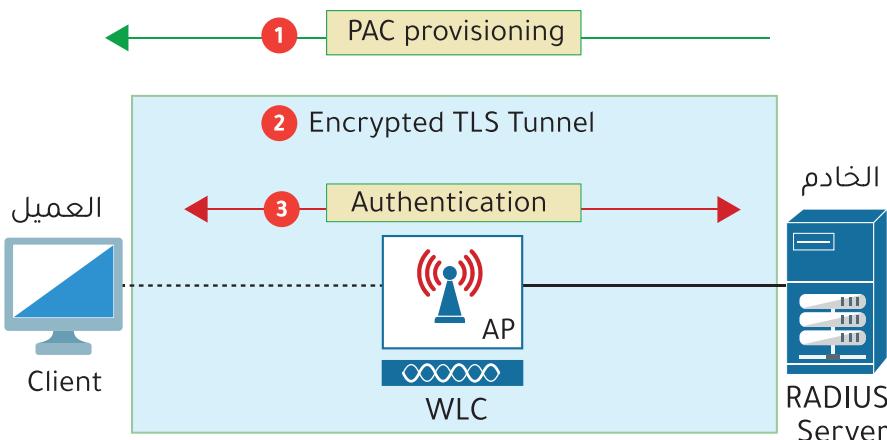
**Authentication server - 3**

خادم المصادقة هو الذي يقرر بالموافقة او الرفض لعملية المصادقة للعميل بعد عملية التحقق ، ومثال على ذلك جهاز .RADIUS Server

### EAP-FAST

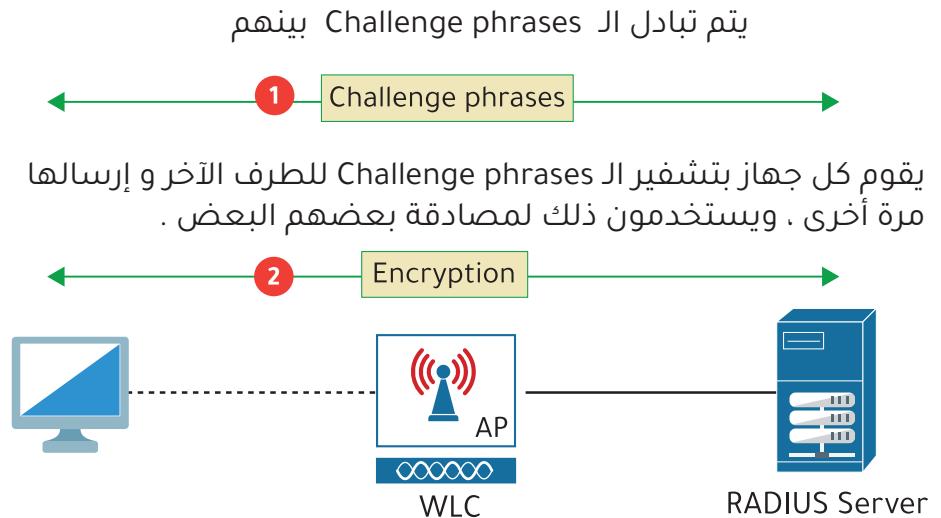
(EAP Flexible Authentication via Secure Tunneling)

- تم تطوير EAP-FAST بواسطة Cisco.
- **تكون من ثلاثة مراحل:**
  - 1) يتم إنشاء PAC (بيانات اعتماد الوصول المحمي) وتمريرها من الخادم إلى العميل.
  - 2) يتم إنشاء نفق TLS آمن بين العميل وخادم المصادقة.
  - 3) يتواصل العميل والخادم مع مصادقة العميل داخل نفق TLS.



### LEAP (Lightweight EAP)

- تم تطوير LEAP بواسطة Cisco كتحسین على الـ WEP.
- يجب على العملاء تقديم اسم مستخدم وكلمة مرور للمصادقة.
- بالإضافة إلى ذلك ، يتم توفير المصادقة المتبادلة من قبل كل من العميل والخادم الذي يرسل بعضها البعض بعد التشفير.
- يعتبر تشفير الـ LEAP ضعيفاً ويجب عدم استخدامه بعد الآن.

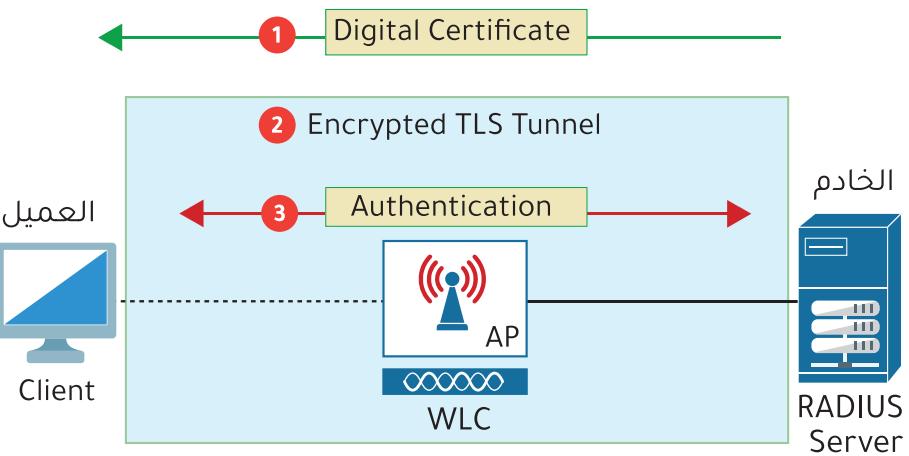


## EAP-TLS (EAP Transport Layer Security) ≡

- في حين أن الـ PEAP يتطلب فقط أن يكون لدى خادم المصادقة شهادة رقمية ، فإن الـ EAP-TLS يتطلب شهادة على خادم المصادقة وأيضاً على كل عميل على حدة .
- يعد EAP-TLS أكثر طرق المصادقة اللاسلكية أماناً ، ولكن تنفيذه أصعب لأن كل جهاز عميل يحتاج إلى شهادة.

## PEAP (Protected EAP) ≡

- هو مثل الـ EAP-FAST ، لانه يتضمن إنشاء نفق TLS آمن بين العميل والخادم. ولكنه يختلف عنه بوجود شهادة رقمية .
- يمتلك الخادم شهادة رقمية digital certificate بدلًا من الـ PAC .
- سيُظهر شهادته الرقمية للعميل ، ويستخدمها العميل لمصادقة الخادم داخل النفق الآمن .
- تُستخدم هذه الشهادة أيضًا لإنشاء نفق TLS الآمن.
- أحد البروتوكولات التي يمكن استخدامها لهذه المصادقة يسمى : **MS-CHAP**
- . Microsoft Challenge Handshake Authentication Protocol
- PEAP مثل PEAP JL يستخدم شهادة رقمية.
- . PAC مثل EAP-FAST يستخدم الـ PAC .



### CCMP (Counter/CBC-MAC Protocol) - 3

- تم تطوير الـ CCMP بعد الـ TKIP وهو أكثر أماناً.
- يتم استخدامه في تشفير من نوع WPA2 .
- يجب أن تكون الأجهزة مدعومة لاستخدام الـ CCMP . أما الأجهزة القديمة التي بُنيت لاستخدام الـ WEP / TKIP لا يمكنها استخدام الـ CCMP .

- يستخدم الـ CCMP خوارزميتين للتشفير:
  - : AES - خوارزمية الـ A

هو بروتوكول التشفير الأكثر أماناً المتاح حالياً. يستخدم على نطاق واسع في جميع أنحاء العالم.

### : CBC-MAC B

#### (Cipher Block Chaining Message Authentication Code)

يستخدم الـ MIC لضمان سلامة الرسائل.

### GCMP (Galois/Counter Mode Protocol) - 4

- هو أكثر أماناً وفعالية من الـ CCMP .
- يتم استخدامه في تشفير من نوع WPA3 .
- يستخدم الـ GCMP خوارزميتين للتشفير:
  - خوارزمية الـ AES
  - خوارزمية الـ CBC-MAC

## ≡ طرق التشفير والتكامل

### Encryption and Integrity Methods

الطرق المستخدمة في التشفير والمحافظة على خصوصية وسلامة البيانات :

#### Wired Equivalent Privacy (WEP)- 1

تشفر الـ WEP ليس آمن ويمكن كسره بسهولة .

- يستخدم الـ WEP :

- . خوارزمية RC4
- . خوارزمية CRC-32
- .

#### Temporal Key Integrity Protocol (TKIP) - 2

بعد اكتشاف ضعف تشفير الـ WEP كان لابد من حل مؤقت لذلك كان الحل هو الـ TKIP .

- تم تطويره واضافة مميزات له مثل : MIC (message integrity code)

## الوصول المحمي بشبكة WiFi WiFi Protected Access



قامت مؤسسة الـ Wi-Fi بتطوير ثلاث شهادات للأجهزة اللاسلكية :



- Enterprise mode**
- يحتاج وجود خادم لتفعيل هذا الوضع .
- . RADIUS server
- يستخدم بروتوكول 802.1X مع خادم مصادقة مثل EAP .
- يدعم جميع طرق مصادقة الـ EAP .

### WPA

تم تطوير أول شهادة الـ WPA بعد أن ثبت أن الـ WEP ضعيف .  
يتضمن الـ WPA البروتوكولات التالية :

- TKIP - 1
- 802.1X authentication - 2

### WPA2

تم إصداره عام 2004 .  
يتضمن الـ WPA2 البروتوكولات التالية :

- CCMP - 1
- 802.1X authentication - 2

- لكي يحصل الجهاز على شهادة WPA ، يجب اختباره في مختبرات اختبار معتمدة . هذا تماماً مثل كيفية اعتماد شبكات WiFi 4 و WiFi 5 و WiFi 6 و WiFi 5
- أيضاً تقوم المؤسسة باعتماد الأمان للنوع الثلاثة (WPA - WPA2 - WPA3) على الأجهزة .

### أوضاع المصادقة للنوع الثلاثة : (WPA - WPA2 - WPA3) الأول : الوضع الشخصي Personal mode

- يُستخدم مفتاح مشترك مسبقاً (PSK) للصادقة .
- على سبيل المثال عندما تتصل بشبكة WiFi منزلية وتقوم بإدخال كلمة المرور وتتم مصادقتها . هذا هو الوضع الشخصي .
- يُستخدم في المنازل والشبكات الصغيرة .

**WPA3 ≡**

تم إصداره عام 2018 .

يتضمن الـ WPA3 البروتوكولات التالية :

GCMP - 1

802.1X authentication - 2

- يوفر WPA3 أيضًا العديد من ميزات الأمان الإضافية على سبيل المثال :

**Protected Management Frames (PMF) ●**

حماية إطارات الـ 802.11 من التنصت والتزوير .

**Simultaneous Authentication of Equals (SAE) ●**

تحمي المتصفحات الرباعية عند استخدام المصادقة في personal mode authentication .

**Forward secrecy ●**

يمنع فك تشفير البيانات بعد إرسالها عبر الهواء ، هذا يحمي من الهجمات التي يقوم فيها المهاجم بالتقاط إطارات لاسلكية ، ثم يحاول فك تشفيرها لاحقًا لقراءة المحتويات .

**الوضع الشخصي (WPA-Personal) Mode**

	WPA	WPA2	WPA3
المصادقة Authentication	PSK	PSK	SAE
التشفير Encryption	TKIP/MIC	AES-CCMP	AES-CCMP

**وضع المؤسسة (WPA-Enterprise) Mode**

	WPA	WPA2	WPA3
المصادقة Authentication	IEEE 802.1x/EAP	IEEE 802.1x/EAP	IEEE 802.1x/EAP
التشفير Encryption	TKIP/MIC	AES-CCMP	AES-GMAC

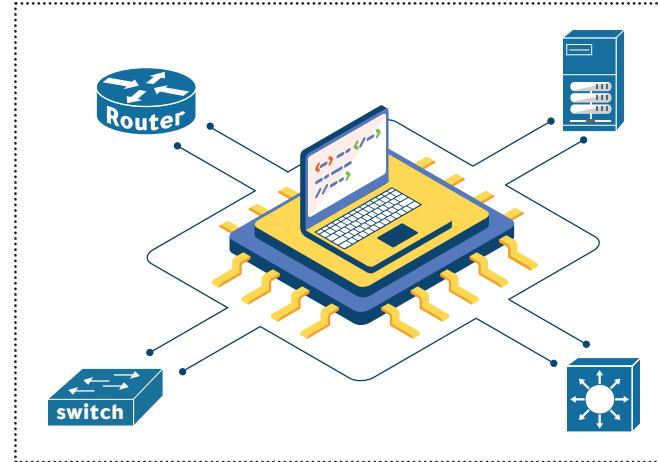
هذه بعض الجوانب السلبية التي ستواجهك أثناء ادارة الشبكة في هذا الوضع :

1- الأخطاء المطبعية والأخطاء الصغيرة الأخرى . فمثلاً حدثت مشكلة في الشبكة واستغرق الأمر وقتاً طويلاً في استكشاف الخطأ وإصلاحه لتكتشف أن المشكلة كانت مجرد خطأ إملائي في عنوان IP .

2- مثلاً كمهندس شبكات من الصعب التأكد من أن جميع الأجهزة تلتزم بالإعدادات الخاصة للمؤسسة . بعض الأحيان يكون لدى المؤسسة إعدادات قياسية أو سياسات خاصة أو معيار قياسي تستخدمها المؤسسة لأجهزتها في جميع أنحاء الشبكة .

ومع قيام مهندسي الشبكات الفردية بإجراء تغييرات فردية على مر السنين ، يمكن أن تبدأ الإعدادات والتكونيات في الابتعاد عن المعيار القياسي الذي وضعته المؤسسة .

لهذا السبب يمكن أن يتسبب هذا في حدوث مشكلات مستمرة داخل الشبكة . على سبيل المثال جعل استكشاف الأخطاء وإصلاحها أكثر صعوبة لأن الأجهزة لا تحتوي جميعها على إعدادات متماثلة .



## أتمتة الشبكات

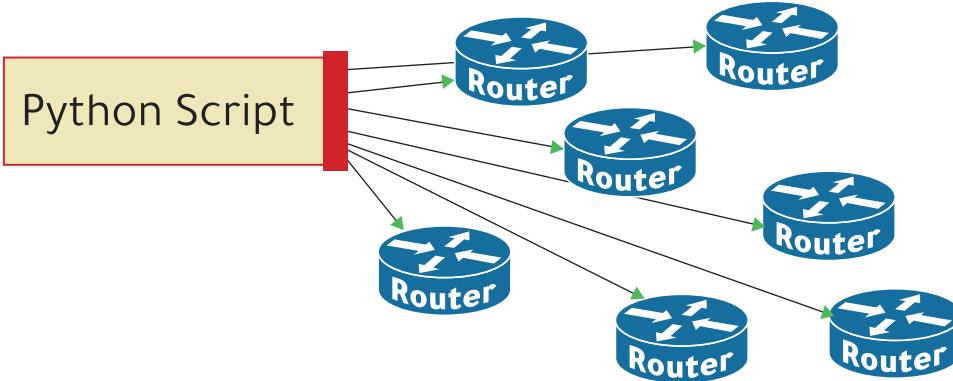
### Network Automation

هي تقنيات تساعد على إتمام المهام وتقديمها بأقل قدر من التدخل البشري . - يؤدي تنفيذ تقنيات وعمليات الأتمتة إلى تحسين كفاءة وموثوقية وسرعة العديد من المهام التي كان يقوم بها البشر سابقاً . - في النموذج الشبكات العادي التقليدية ، يدير المهندسون الأجهزة واحداً تلو الآخر عن طريق الاتصال بـ CLI الخاص بهم عبر SSH أو عن طريق الكونسول .

**مثال :** لنفترض أن المؤسسة تريد إضافة منفذ وهو مي loopback interface لجميع أجهزة الراوتر الخاصة بها .

سوف تقوم بالاتصال بـ R1 باستخدام SSH مثلاً . وإضافة المنفذ وهو مي loopback interface وتقوم بالحفظ والخروج من R1 . ثم بتكرار ذلك في R2 وهكذا في جميع الراوترات .

**السؤال** كيف لو كان لديك المئات في شبكتك !! ما هي الجوانب السلبية التي سوف تواجهها في ادارة الشبكة ؟



بعض الأدوات والطرق التي يمكن استخدامها لأتمتة المهام في الشبكة. مثل :

- SDN -
- Ansible -
- Puppet -
- Python scripts -

إن إدارة الشبكة وتشغيلها باستخدام الأتمتة تقدم لنا العديد من الفوائد الرئيسية منها :

**1- تقليل الأخطاء البشرية ، مثل الأخطاء المطبعية.**

بدلًا من قيام مهندس الشبكة بتسجيل الدخول مباشرةً إلى CLI وإدخال الأوامر يدوياً، يمكن أتمتة المهمة في وقت قصير.

**2- أصبحت الشبكات أكثر قابلية للتتوسيع**

حيث يمكن تنفيذ عمليات وتغييرات جديدة على مستوى الشبكة بالإضافة إلى استكشاف الأخطاء وإصلاحها في جزء صغير من الوقت.

**3- يمكن ضمان الامتثال لسياسة المؤسسة على مستوى الشبكة**

على سبيل المثال التأكد من أن جميع الأجهزة بها الإعدادات القياسية المناسبة ، وأن جميع الأجهزة بها إصدارات البرامج الصحيحة وغيرها .

**4- إن الكفاءة المحسنة لعمليات الشبكة تقلل من النفقات التشغيلية**

فمثلاً عندما أردنا إضافة منفذ وهو `loopback interface` جديد لمئات الراوترات ، فبدلًا من تسجيل الدخول إلى كل راوتر وإعداده بشكل يدوي ، والذي قد يستغرق ساعات من الوقت ، يمكن لبرنامج نصي بلغة بايثون أداء المهمة وإجراء الإعداد في جزء صغير من الوقت.

## الشبكات المعرفة بالبرمجيات

### SDN (Software-Defined Networking)

لفهم الـ SDN (Software-Defined Networking) . يجب أولاً معرفة وفهم المستويات المنطقية (Logical planes) لوظائف الشبكة :

**فمثلاً ما هي وظيفة الراوتر ؟ وما هي وظيفة السويفت ؟**

**جهاز الراوتر :**

- يقوم بإعادة توجيه الرسائل بين الشبكات عن طريق فحص المعلومات الموجودة في رأس الطبقة الثالثة LYER3.

- يستخدم الراوتر أيضًا بروتوكول توجيه مثل OSPF لمشاركة معلومات التوجيه مع أجهزة الراوتر الأخرى وإنشاء جدول توجيه.

- يستخدم الـ Syslog للاحتفاظ بسجلات الأحداث التي تحدث.
- يمكن أيضًا استخدام بروتوكول الـ SSH للاتصال بجهاز الراوتر وإدارته.

**جهاز السويفت :**

- يقوم السويفت بإعادة توجيه الرسائل داخل شبكة LAN المحلية عن طريق فحص المعلومات الموجودة في رأس الطبقة الثانية.

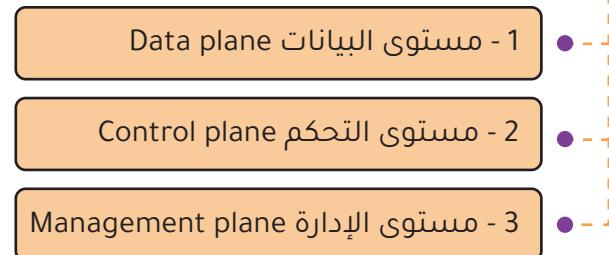
- يستخدم السويفت بروتوكول الـ STP لضمان عدم وجود دوران للبيانات في الشبكة.

- يقوم ببناء جدول عناوين MAC من خلال فحص عنوان MAC المصدر للإطارات (Frames).

- أيضاً يستخدم أيضًا بروتوكولات مثل SSH و Syslog .

- هذه الوظائف المختلفة التي تقوم بها أجهزة الراوتر والسويفت وغيرها نسميها بـ Logical planes .

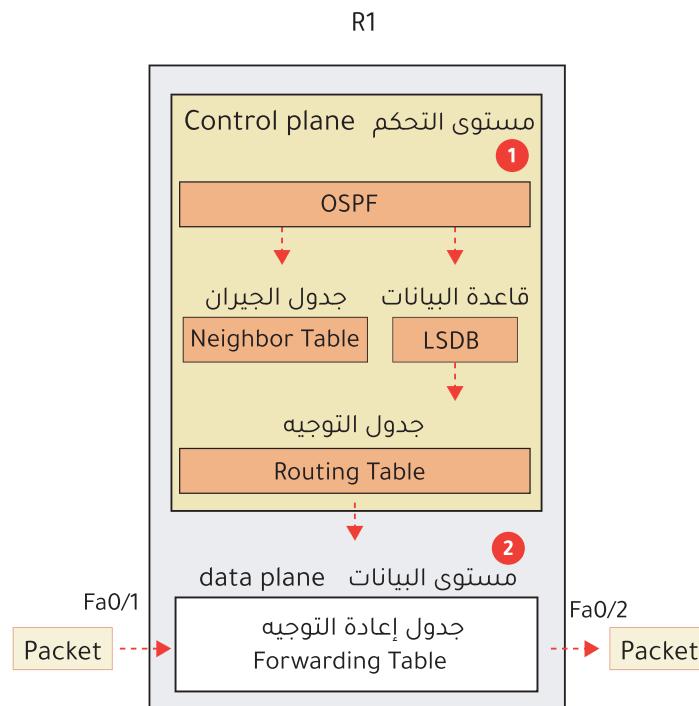
**تنقسم هذه الـ Logical planes إلى ثلاثة مستويات :**



## 2 - مستوى التحكم Control plane

هو مستوى أعلى من مستوى البيانات وهو الذي يتخذ القرارات التي يتم تنفيذها في مستوى البيانات مثل :

- إنشاء جدول توجيه الراتر واتخاذ القرار لتوجيه الحزمة لاي منفذ.
- لا يقوم بروتوكول الـ OSPF نفسه بإعادة توجيه حزم بيانات المستخدم ولكنه يعلم مستوى البيانات حول كيفية إعادة توجيه الحزم.
- ايضا لا يشارك بروتوكول الـ STP بشكل مباشر في عملية إعادة توجيه الإطارات ، ولكنه يعلم مستوى البيانات بالمنفذ التي يجب استخدامها والتي يجب عدم استخدامها لإعادة توجيه الإطارات.



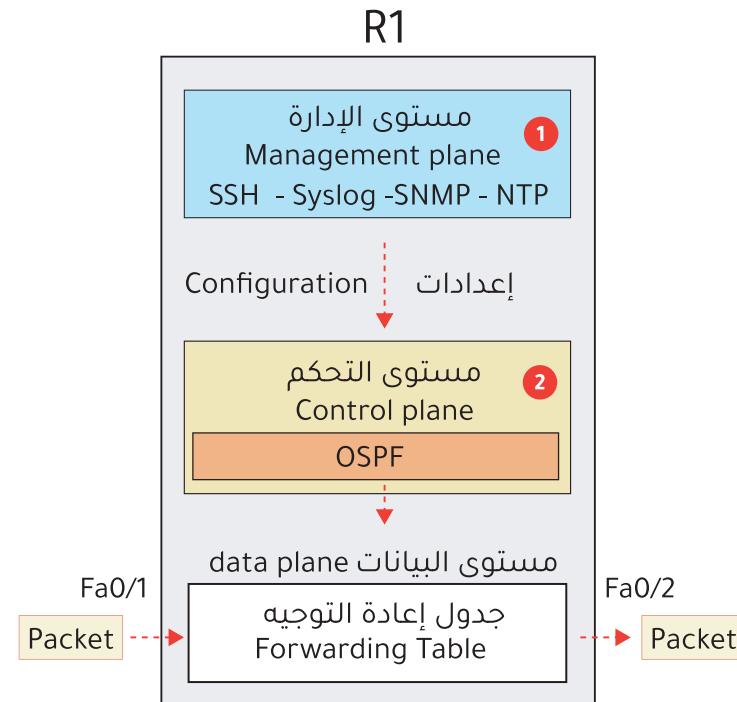
## 1 - مستوى البيانات data plane

مستوى البيانات هو المسؤول عن إعادة توجيه حركة المرور ويعتمد على المعلومات التي يوفرها مستوى التحكم (Control plane).

فيما يلي بعض المهام التي يعني بها مستوى البيانات:

- تغليف وفك تغليف الحزم.
- إضافة أو إزالة الرؤوس مثل رأس 802.1Q.
- مطابقة عناوين الـ MAC لإعادة التوجيه.
- مطابقة وجهات الـ IP في جدول التوجيه.
- تغيير عناوين المصدر والوجهة عند استخدام NAT.
- يُطلق على مستوى البيانات أيضا اسم مستوى إعادة التوجيه forwarding plane





### 3 - مستوى الإدارة Management plane

هذا المستوى هو أعلى من مستوى التحكم ولكنه لا يؤثر بشكل مباشر على إعادة توجيه الرسائل في مستوى البيانات.

**إنما يتكون من بروتوكولات تُستخدم لإدارة الأجهزة .**

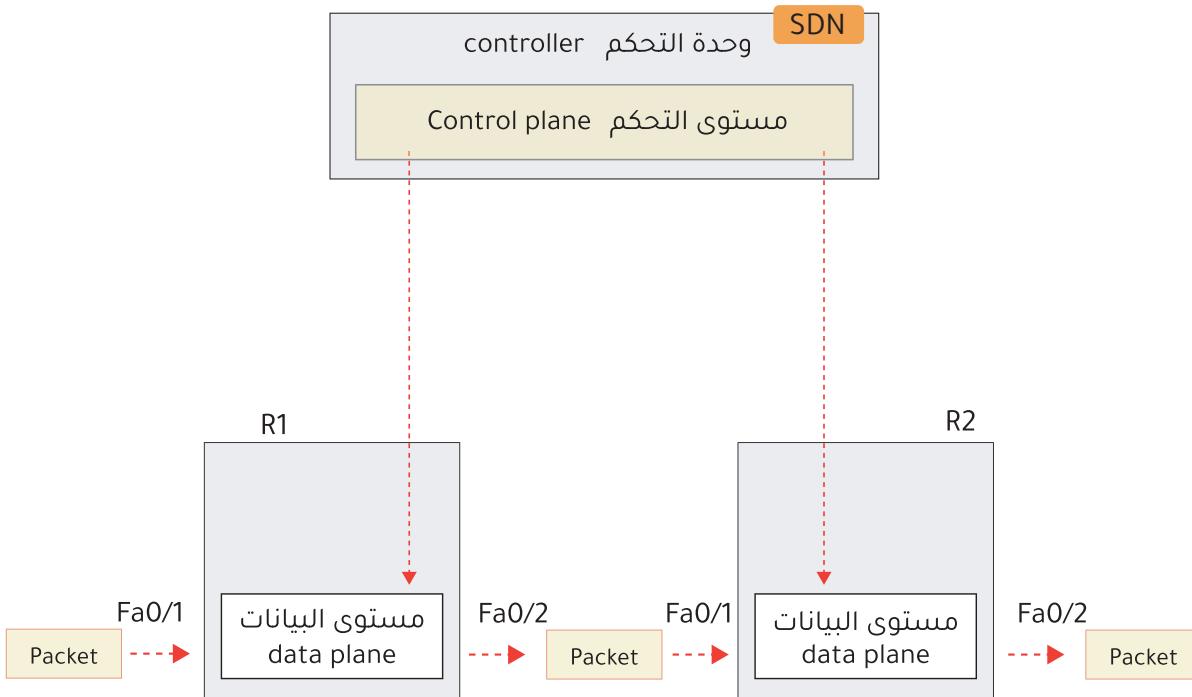
على سبيل المثال :

- بروتوكولين الـ SSH و الـ Telnet ، اللذان يتم استخدامهما للاتصال بـ الأجهزة لتكوين الإعدادات وإدارتها.
- بروتوكول الـ Syslog . والذي يستخدم لاحتفاظ بسجلات الأحداث التي تحدث على الجهاز.
- أيضًا بروتوكول الـ SNMP . والذي يستخدم بشكل أساسى لمراقبة عمليات وحالة الجهاز.
- أيضًا بروتوكول الـ NTP يستخدم لحفظ دقة الوقت على الجهاز.

١ يستخدم مهندس الشبكة بروتوكول الـ SSH للاتصال بأجهزة الراوتر والقيام ببعض التكوينات والإعدادات .

٢ مثلًا تم اعداد بروتوكول الـ OSPF للربط ولتبادل معلومات التوجيه. تتحكم جداول التوجيه هذه في إجراءات مستوى البيانات ، حيث يتم إعادة التوجيه الفعلية لحزم البيانات .

وحدة التحكم تعمل على تشغيل مستوى التحكم للتحكم بـكامل الشبكة .



مثال : بدلاً من استخدام R1 و R2 لبروتوكول الـ OSPF لتبادل معلومات التوجيه بينهم ثم حساب المسارات . تقوم وحدة التحكم بالتواصل مع R1 و R2 لبرمجية مستويات البيانات (data plane) وتعريفهم بجداول التوجيه الخاصة بهم .

## الشبكات المعرفة بالبرمجيات

### SDN (Software-Defined Networking)

عرفنا سابقاً أنه يوجد في كل جهاز في أجهزة الشبكة مستوى تحكم control plane خاص بكل جهاز . لكن في الـ SDN يكون مستوى التحكم مركزاً ، يعني control plane واحد متتحكم بكل الأجهزة في الشبكة يسمى بال controller - أيضاً يسمى بر :

### Software-Defined Architecture (SDA) -

### Controller-Based Networking -

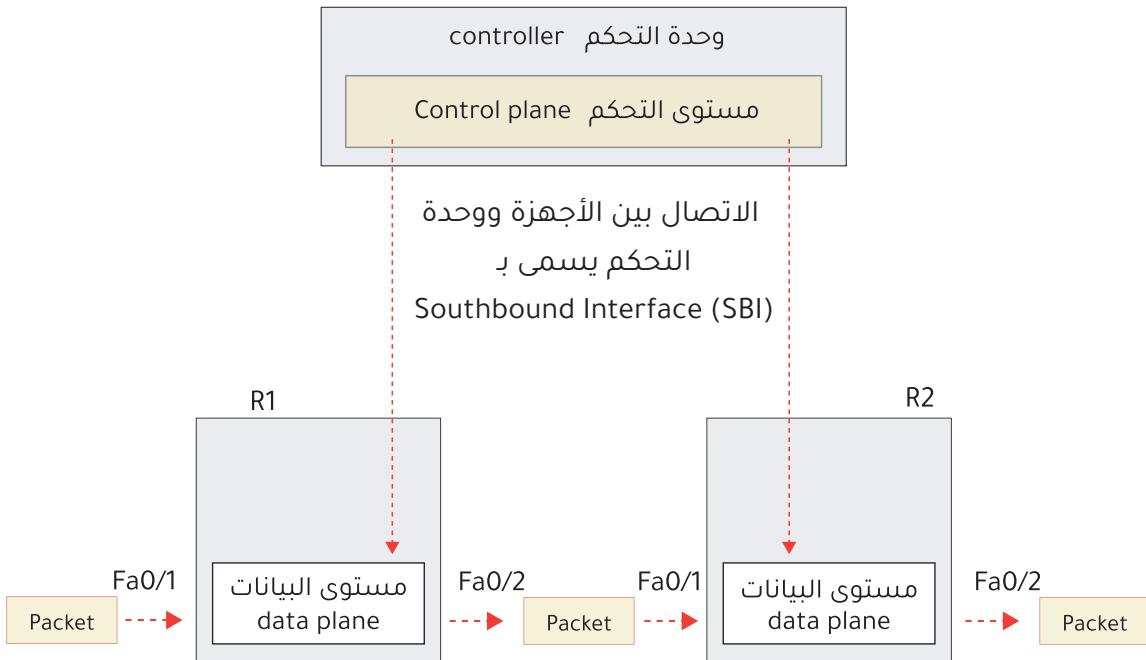
- للتوضيح أكثر تعرفنا سابقاً عن وحدة التحكم اللاسلكية WLC حيث أنها تحكم مركزاً بنقاط الوصول . فأصبحت نقاط الوصول وظيفتها فقط إعادة توجيه حركة المرور الـ SDN نفس الطريقة حيث أنه المتحكم بأجهزة الشبكة مركزاً .

- يمكن لوحدة التحكم التفاعل برمجياً مع أجهزة الشبكة باستخدام واجهات برمجة التطبيقات Application Programming Interface (APIs).

## Southbound Interface (SBI) & Northbound Interface (NBI)

فيما يلي بعض الأمثلة على (SBI)

- 1 - OpenFlow
- 2 - Cisco OpFlex
- 3 - Cisco onePK (Open Network Environment Platform Kit)
- 4 - NETCONF



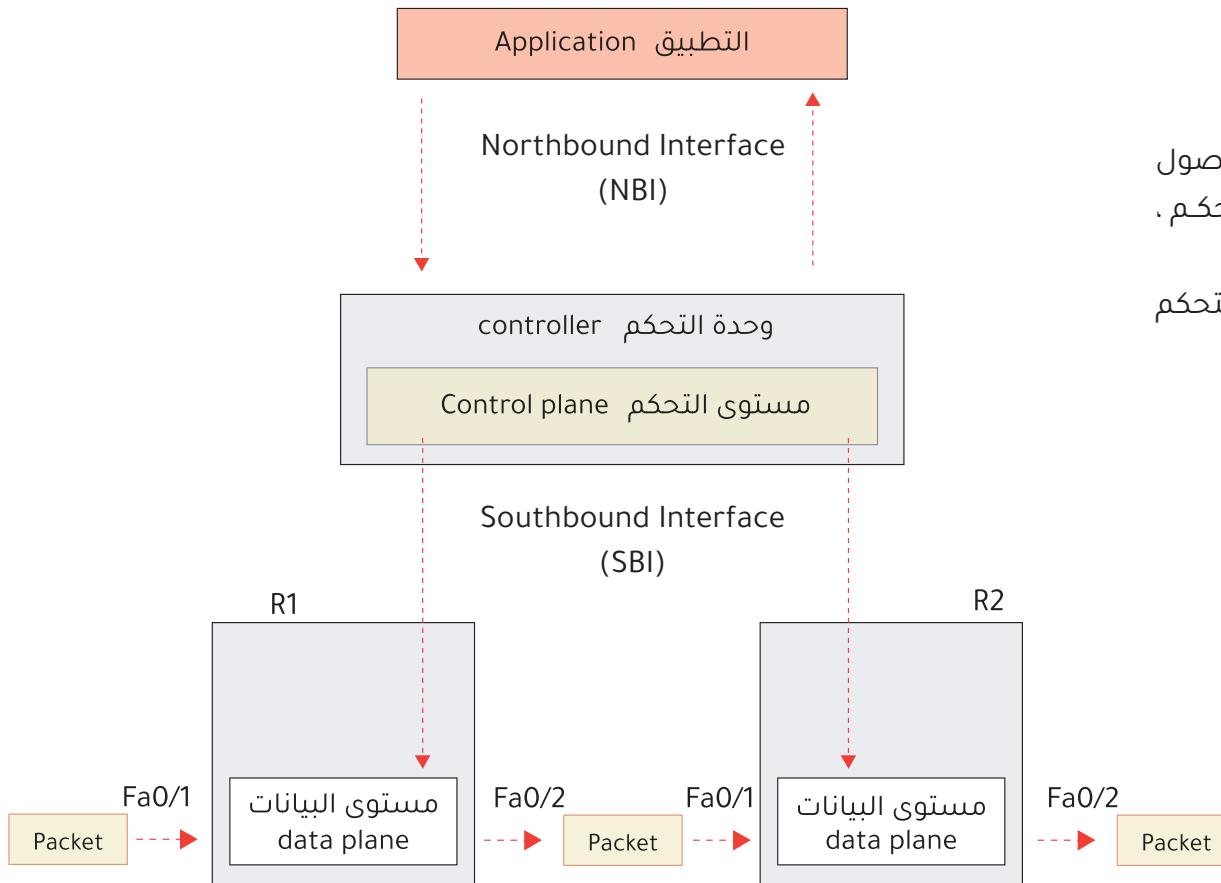
### Southbound Interface (SBI) ≡

- يتم استخدام SBI للاتصالات بين وحدة التحكم وأجهزة الشبكة التي تحكم فيها.
- في الصورة التالية نرى أنه يتم التحكم في R1 و R2 بواسطة وحدة التحكم ، ويتم استخدام SBI للتواصل بينهما.
- يتكون الـ SBI من بروتوكول اتصال وواجهة برمجة تطبيقات (API).

- يتم استخدام الـ API لتسهيل تبادل البيانات بين البرامج.
- وحدة التحكم عبارة عن برنامج وأجهزة الشبكة هي أيضًا برامج تعمل داخل أجهزتها لذلك يتم تبادل البيانات بين وحدة التحكم وأجهزة الشبكة .

### على سبيل المثال

يمكن لواجهة برمجة التطبيقات (API) على جهاز الشبكة أن تسمح لوحدة التحكم بالوصول إلى المعلومات عنها ، والتحكم في جداول مستوى البيانات الخاصة بها التي تُستخدم لإعادة توجيه الحزم ، وغيرها .



**ملاحظة :**

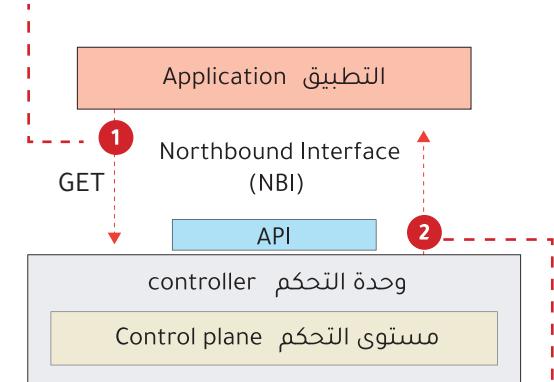
الـ API هي واجهة على وحدة التحكم وهي واجهة برمجية تسهل الاتصال بين وحدة التحكم والتطبيقات

### Northbound Interface (NBI)

الـ (NBI) هي التي تسمح لنا بالتفاعل مع وحدة التحكم والوصول إلى البيانات التي تجمعها حول الشبكة ، وبرمجة وحدة التحكم ، وإجراء التغييرات في الشبكة عبر الـ API .

- يتم استخدام واجهة برمجة تطبيقات REST API على وحدة التحكم كواجهة للتطبيقات للتفاعل معها .
- الـ REST هي نوع من أنواع واجهة برمجة التطبيقات .

مثلًا يرسل التطبيق رسالة إلى API وهي عبارة عن طلب لبعض البيانات .



سترد وحدة التحكم بالبيانات المطلوبة بتنسيق منظم مثل XML أو JSON

## Object = { " key " : " value" }

- المفتاح (key) هو الذي نستعمل به لمعرفة القيمة (value).
- فمثلاً نستعمل عن الاسم name فتظهر لنا قيمته وهي : ali.
- وايضاً نستعمل عن العمر age فتظهر لنا قيمته 25

### ملاحظة :

- الأرقام تكون بدون علامة ( " ) اي كتابة داخل ال ( " ) تكون نصية.
- " 8 " <<> نص
- 8 <<> رقم
- لو وجدت رقم داخل علامة التنصيص ( " ) فإنه يعتبر نص لأن علامة التنصيص تحوله إلى نص .
- مثلاً " 5 " هذا يعتبره البرنامج نص وليس رقم .

## JavaScript Object Notation ( JSON )



هو تنسيق ملف لمشاركة وتبادل البيانات بين الأجهزة والتطبيقات المختلفة . قابل للقراءة بسهولة من قبل الإنسان يمكن استخدامه لتخزين البيانات كملفات أو لإرسال البيانات عبر شبكة .

- تم تصميم الـ JSON بشكل أساسى لتبادل البيانات بين التطبيقات والأجهزة .
- تنسيق الـ JSON مدعوم في كثير من لغات البرمجة .
- تنسيق الـ JSON يسهل التواصل بين التطبيقات المختلفة في لغات البرمجة .
- يمكن تخزين البيانات بصيغة الـ JSON ، ستتجدد اسم الملف الخاص بالطقس مثلـ weather.json .

### تنسيق الـ JSON Format

- المحتوى المكتوب داخل الأقواس { } يسمى أوجبكت (Object).
- الـ أوجبكت (Object) يكون بداخله مفتاح (key) وقيمة (value) .
- يفصل بين الـ key و الـ value بعلامة نقطتين فوق بعض ( : )
- يفصل بين كل أوجبكت وأوجبكت آخر بعلامة فاصلة ( , ) أو ( , )

```
{
  "interface": "fa0/0",      string نصي
  "speed": 1000,            number رقمي
  "is_up": true,           boolean
}

{
  "router1": {
    "hostname": "R1",
    "Model": "2961",
  },
  "interfaces": ["fa0/0", "fa0/1", "fa0/2"]
}

```

مصفوفة array

الاوجكت داخل اوجكت يسمى nested objects

```
{ "router1": { "hostname": "R1", "Mode": "2961" } }
```

### أنواع البيانات التي يقبلها الـ JSON :

: string - 1

هو أحرف نصية عادية التي تشكل كلمة وتكون مكتوبة بين

علامة " " مثل ( " age " )

: number - 2

رقم صحيح أو بفواصل عشرية .

: object (JSON object) - 3

يسمى كائن ويكون من مفتاح (key) وقيمة (value) ويكتب بين

{ "age": 20 } مثل { "age" : 20 }

: array - 4

تسمى مصفوفة وهي مجموعة من القيم المترابطة تكتب بين

[ 10, "ali", 20 ] مثل [ 10, "ali", 20 ]

: boolean - 5

تسمى قيمة منطقية ولها احتمالين false or true

: null - 6 تعني لا شيء

### أنواع البيانات التي لا يقبلها الـ JSON :

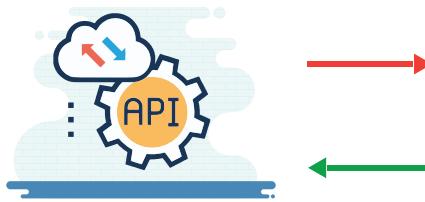
: الدالة البرمجية function -

: التاريخ date -

: الغير معروفة undefined -



طلب  
Request  
الاستجابة  
Response



سيرفر

## Application Programming Interface (API)



واجهة برمجة التطبيقات API هي واجهة برمجية تسمح لتطبيقين بالتواصل مع بعضهما البعض. وهي ضرورية لأنوثة الشبكات ، وأيضاً لجمع جميع أنواع التطبيقات.

[انظر لهذه الصور للتوضيح أكثر](#)

هذا مثال للتшибه :  
النادل مثل الـ API يأخذ طلبات ويسلم النتائج



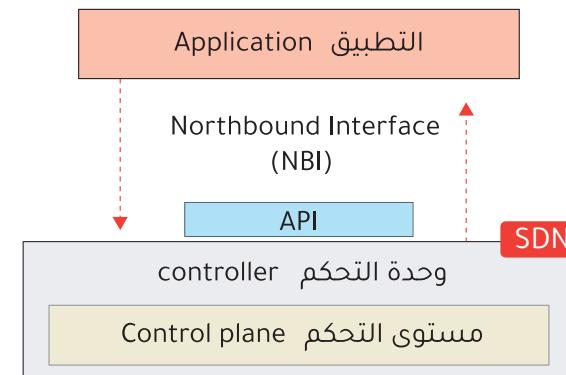
قدم الطلب  
Customer places the order



خذ طلب العميل  
Waiter takes the customer's order  
إحضار الطلب من المطبخ  
Bring the order from the kitchen



المطبخ



- في بنية الـ SDN ، تُستخدم الـ API للتواصل بين التطبيقات ووحدة تحكم SDN عبر الواجهة الشمالية ( NBI ) ، وبين وحدة تحكم SDN وأجهزة الشبكة عبر الواجهة الجنوبية ( SBI ).

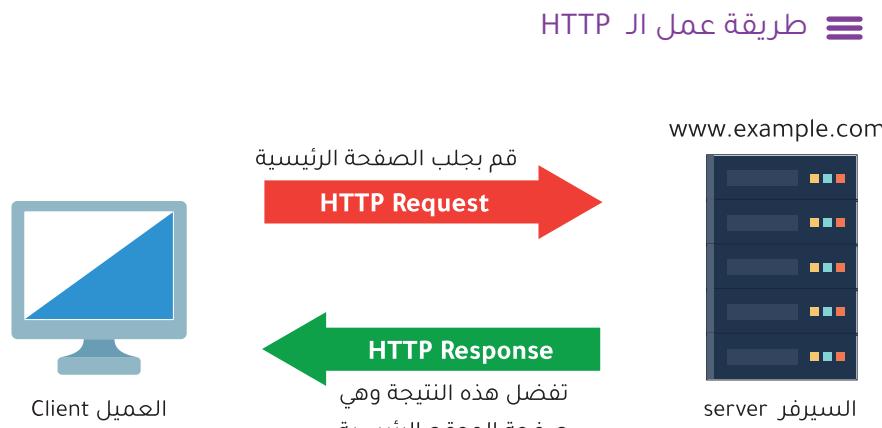
- يستخدم الـ NBI عادةً واجهات برمجة تطبيقات الـ REST api .  
- تستخدم واجهات برمجة تطبيقات الـ REST api عادةً بروتوكول الـ HTTP كبروتوكول للتواصل عبر الشبكة.

## بروتوكول الـ HTTP



Hypertext Transfer Protocol (HTTP) هو مجموعة قواعد نقل الملفات على شبكة الويب مثل (النصوص والصور الرسومية والصوت والفيديو وملفات الوسائط المتعددة الأخرى).

- تم إنشاء هذا البروتوكول لتأمين نقل بيانات بين السيرفر والعميل حيث يتم التواصل بينهم عن طريق الطلب والاستجابة Request / Response.



## CRUD (Create, Read, Update, Delete)

تعني [إنشاء ، قراءة ، تحديث ، حذف] وهي تشير إلى العمليات التي تقوم بها باستخدام واجهات برمجة تطبيقات الـ REST API.

- يستخدم بروتوكول الـ HTTP هذه الطرق أو العمليات المعروفة ب CRUD .

### Create

تُستخدم لإنشاء متغيرات جديدة وتعيين قيمها الأولية. على سبيل المثال ، يمكنك إنشاء متغير " ip\_address " وتعيين القيمة على " 10.1.1.1 ".

### Read

تُستخدم عمليات القراءة لاسترداد قيمة متغير.

### Update

تُستخدم عمليات التحديث لتغيير قيمة المتغير. على سبيل المثال يمكنك تغيير قيمة المتغير " ip\_address " إلى " 10.2.3.4 ".

### Delete

تُستخدم عمليات الحذف لحذف المتغيرات ، لذا يمكنك حذف المتغير " ip\_address ".

## أفعال الـ HTTP أو طرق الـ HTTP (HTTP Verb or HTTP Methods )

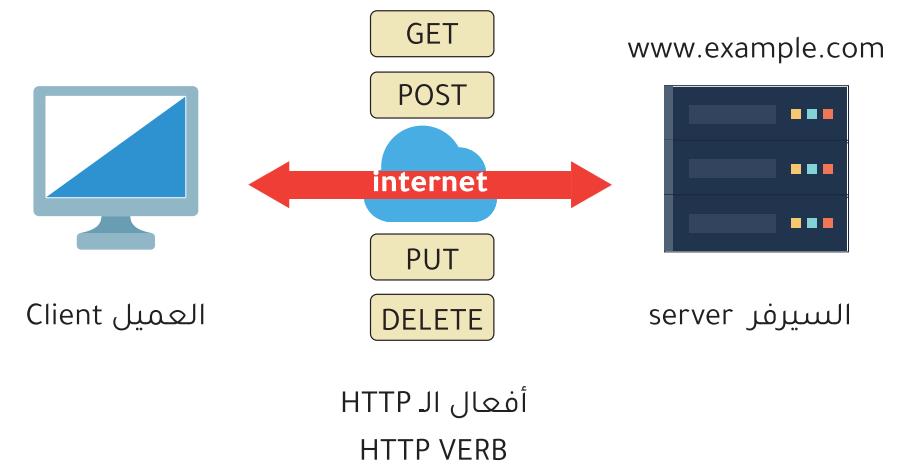
GET : جلب الـ resource المحدد اسمه من السيرفر.

POST : ارسال البيانات الى السيرفر.

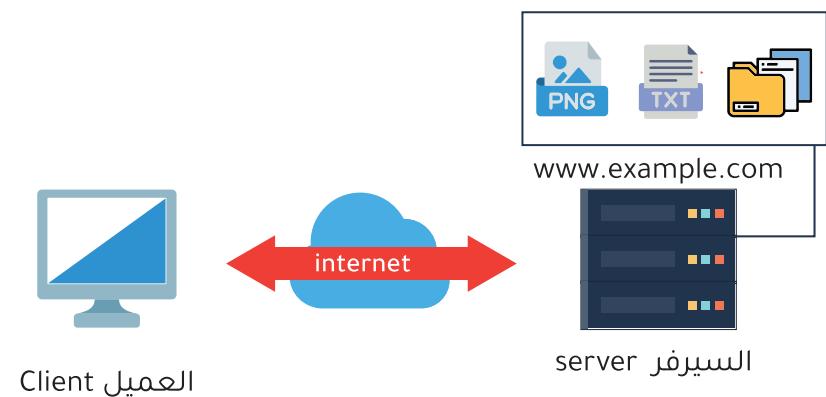
PUT : لتخزين أو تحديث البيانات المرسلة الى الـ resource المحدد اسمه.

DELETE : حذف الـ resource المحدد اسمه من السيرفر.

عملية الـ CRUD CRUD Operation	أفعال الـ HTTP HTTP Verb	الوصف
Read	GET	جلب الـ resource المحدد اسمه من السيرفر.
Create	POST	ارسال البيانات الى السيرفر
Update	PUT	لتخزين أو تحديث البيانات المرسلة الى الـ resource المحدد اسمه
Delete	DELETE	حذف الـ resource المحدد اسمه من السيرفر.



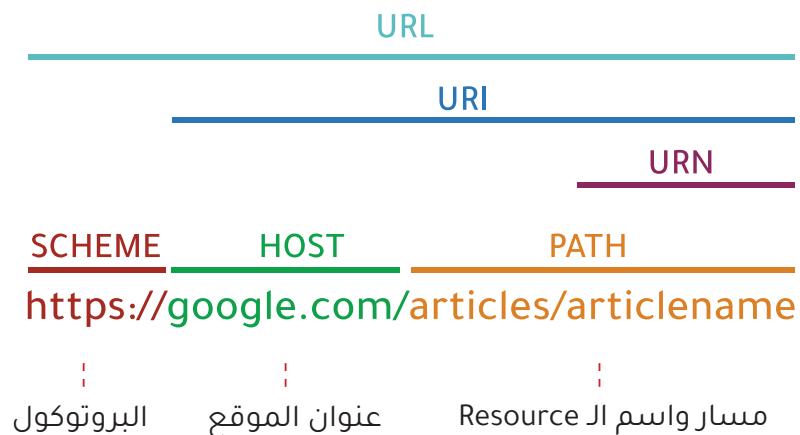
- يستخدم بروتوكول الـ HTTP هذه الطرق أو العمليات المعروفة بـ CRUD .



## ≡ محتوى المواقع

في السيرفر توجد جميع محتويات موقع الويب من صفحات وصور وملفات وهذا المحتوى نسميه بالـ Resources (موارد أو مصادر).

- يوجد في داخل السيرفر العديد من الـ Resources لكل الموقع المخزن فيه.



- كل الـ Resources في السيرفرات يمكن الوصول إليها عبر الـ URI وهي اختصاراً لـ Uniform Resource Identifier .

## ≡ أنواع الـ URI :

### Uniform Resource Locator (URL) - 1

. وهو الرابط الذي يحدد مسار الـ Resources  
Uniform Resource Name (URN) ( - 2

يُستخدم للوصول إلى الـ Resources من خلال الاسم .

## 2 - جسم الطلب HTTP Request Body

هو عبارة عن البيانات أو الملفات التي يتم إرسالها مع الطلب Request مثل أن تقوم بإرسال بيانات من نوع JSON لإرسال معلومات مهمة مثل بيانات تسجيل دخول أو إرسال ملفات مثل صور أو فيديوهات أو مستندات أو غيرها.

يمكن أن يتضمن طلب الـ HTTP Request رؤوساً إضافية تمرر معلومات إضافية إلى الخادم.



مثال على ذلك :

**Accept Header** رأس القبول والذى يخبر الخادم بنوع أو أنواع البيانات التي يمكن إرسالها مرة أخرى إلى العميل. مثل ان العميل يفهم البيانات بصيغة الـ json فيجب على الخادم ان يرسل البيانات بنفس الصيغة (Accept: application/json)

**ملاحظة :**

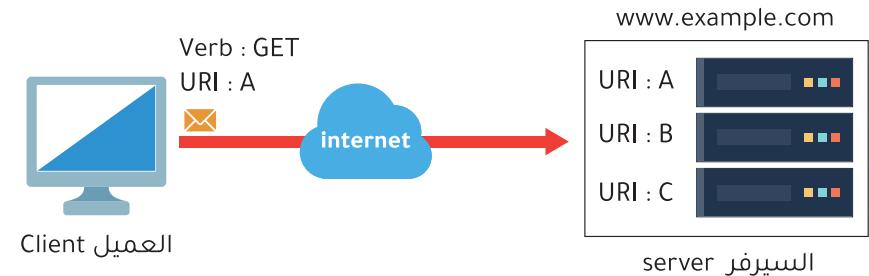
سبب تعلمنا لـ HTTP Request لأنه عندما يقوم عميل الـ REST بإرسال طلب إلى خادم الـ REST عبر واجهة برمجة التطبيقات (API) فإنه سيرسل الطلب بطريقة الـ HTTP Request .

## HTTP Request



عندما يرسل عميل الـ HTTP طلباً إلى خادم باستخدام HTTP Request فإنه يتضمن بعض المعلومات مثل :

- طلب البيانات من السيرفر : **HTTP GET** -
- يشير الـ **URI** : إلى الموارد الموجودة في السيرفر.
- (HTTP Response) فيتم الرد عليه من السيرفر



يحتوي الـ **HTTP Request** على قسمين مهمين هما :

**1 - رأس الطلب HTTP Request Headers** وهو يحتوي على معلومات مهمة للطلب (Request) مثل :

- بيانات الارتباط (Cookies)
- نوع الطلب
- عنوان الموقع أو المضيف (Host)
- اللغة التي تقبلها
- نوع التشفير الذي تقبله
- نوع البيانات أو الملفات التي تقبلها.

**5xx: Server Error -**  
تعني أن الخادم لم يتمكن من معالجة الطلب بسبب خطأ داخلي في السيرفر.

وهذه قائمة بأشهر رموز الردود :

- **الرمز 102**

والذي يعني المعالجة وهو يشير إلى أن السيرفر قد تلقى الطلب ويقوم بمعالجته ، لكن الاستجابة غير متاحة بعد.

- **الرمز 200**

يعني موافق وهو يشير إلى نجاح الطلب.

- **الرمز 301**

تعني تم نقل المورد المطلوب (Resource) بشكل دائم .

- **الرمز 403**

تعني غير مصرح به وهذا يعني أنه يجب على العميل المصادقة للحصول على رد.

- **الرمز 404**

يشير إلى أنه لم يتم العثور على المورد المطلوب. مثلاً يظهر لك الصفحة غير موجودة .

- **الرمز 500**

تعني وجود مشكلة داخلية بالسيرفر.

## HTTP Response



بعد إرسال طلب الـ HTTP Request من العميل (غالباً متصفح الويب أو تطبيق أو برنامج) يقوم السيرفر بمعالجة الطلب وإرسال الرد (Response) مرة أخرى إلى العميل.

ويكون الرد من ثلاثة أجزاء:

1- رقم الحالة للرد Status Code

2- رأس الرد Response header

3- قد يحتوى على الرد على جسم Body

### رقم الحالة للرد Status Code

هي مجموعة من الأرقام المتفق عليها يمثل كل رقم حالة معينة من حالات معالجة الطلب على سبيل المثال 200 تعنى تم بنجاح.

و تنقسم أرقام الردود إلى 5 فئات رئيسية:

**1xx : Informational**

تعني أن الطلب تم استلامه وأن السيرفر يعمل على المزيد من المعلومات.

**2xx : Successful**

تعني أن الطلب تم استلامه وتم معالجته بنجاح.

**3xx : Redirection**

تعني أنه يتوجه العميل إجراء إعادة توجيه لإنكماش الطلب.

**4xx : Client Error**

تعني أن السيرفر لم يتمكن من معالجة الطلب بسبب خطأ في الطلب المرسل من العميل.

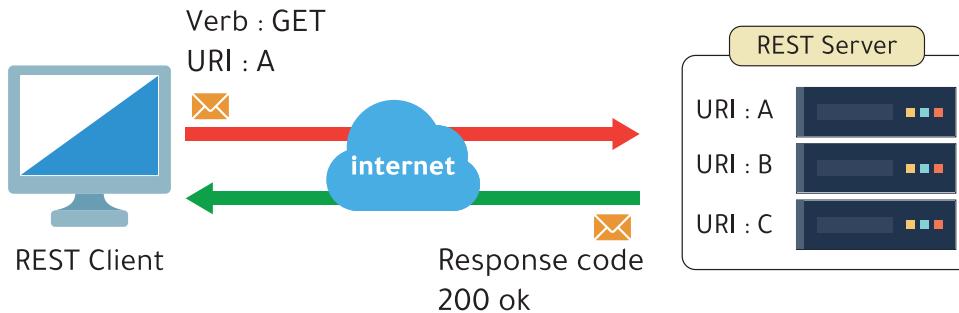


## Representational State Transfer (REST)

راح نتعرف على ثلاثة منهم فقط وهم : Cacheable و Stateless .

### Client-Server

- تستخدم الـ REST APIs بنية الخادم والعميل .
- يستخدم العميل الـ API للوصول إلى الموارد (Resources) الموجودة على الخادم عبر طلبات الـ HTTP Request .
- العميل هو شخص يطلب الموارد والخادم هو الذي يخزن و يحتفظ بالموارد . لذلك العميل والخادم بإمكانهما التغيير والتطور بشكل مستقل عن بعضهما البعض . فلا يعتمد كل منهما على الآخر .
- عندما يتغير تطبيق العميل أو يتغير تطبيق الخادم ، فإن الواجهة بينهما مستمرة في العمل .



الـ REST وهي مجموعة من القواعد التي تحدد كيفية عمل واجهة برمجة التطبيقات (API)

- أحد أهم وأشهر أنواع واجهة برمجة التطبيقات هي واجهات برمجية تسمى REST-based APIs أو RESTful APIs أو REST APIs .

- الأكثر شهرة الـ REST APIs وهي واجهات برمجة تطبيقات مبنية وفق مواصفات الـ REST .

**القيود أو القواعد الستة لبنية الـ REST APIs هي:**

- Uniform Interface .
- Stateless .
- Cacheable .
- Client-Server .
- Layered System .
- Code on Demand .

**Cacheable**

- يجب أن تدعم الـ REST APIs التخزين المؤقت للبيانات .
- يخبر جهاز السيرفر جهاز العميل بـان هذه الموارد (Resources) التي يرسلها له تـدعم التخزين المؤقت (Cacheable) عندئذ يقوم جهاز العميل بتخزينها بشكل مؤقت وعدم طلبها فيما بعد .

- على سبيل المثال :  
عندما تتصفح موقع فإن جهاز الكمبيوتر الخاص بك يقوم بالتخزين المؤقت للعديد من عناصر صفحة الموقع بحيث عند زيارة الموقع مرة أخرى فإن الكمبيوتر لا يحتاج إلى إرسال طلب للخادم لنفس الصفحة مراًواً وتكراراً. يؤدي ذلك إلى تحسين أداء العميل وتقليل الحمل على الخادم.

**Stateless**

- هو أن السيرفر أو الخادم لا يسجل ولا يخزن أي معلومات عن طلب العميل المرسل أو الرد الذي يرسله السيرفر للعميل بعد انتهاء عملية تبادل البيانات .

- يعتبر الـ REST APIs بروتوكول عـديم الحـالة (Stateless) .
- لا يتطلب بروتوكول الـ Stateless من الخادم الاحتفاظ بمعلومات الجلسة أو حالة كل عـميل لأن كل طلب جديد هو حدث منفصل تماماً.
- إذا كانت المصادقة مطلوبة في الطلب، فهذا يعني أنه يتـعـين على العـميل المصادقة مع الخـادـم لـكل طـلـب يـقـدمـه.

**على سبيل المثال لبروتوكول الـ Stateless :**

- بروتوكول الـ HTTP A
- بروتوكول الـ UDP B فهو بروتوكول لا يتحقق من وصول البيانات المرسلة ولا يحتاج إلى جلسة عمل قبل إرسال البيانات بل ان عليه الـرسـال فقط.

**وهـنـاك يـوجـد بـروـتـوكـولـ الـحـالـة :** Stateful Protocol

في بـروـتـوكـولـ الـحـالـةـ عـنـدـما يـرـسـلـ العـمـيـلـ طـلـباـ إـلـىـ الـخـادـمـ ،ـفـإـذـاـ لمـ يـصـلـ فـإـنـ العـمـيـلـ يـقـوـمـ بـإـعـادـةـ إـرـسـالـ الـطـلـبـ إـلـىـ الـخـادـمـ .

**على سبيل المثال بـروـتـوكـولـ TCP :**

### طبقة التطبيقات

#### Application Layer

تحتوي هذه الطبقة على تطبيقات تخبر وحدة تحكم SDN بسلوكيات الشبكة المطلوبة.

### طبقة التحكم

#### Control Layer

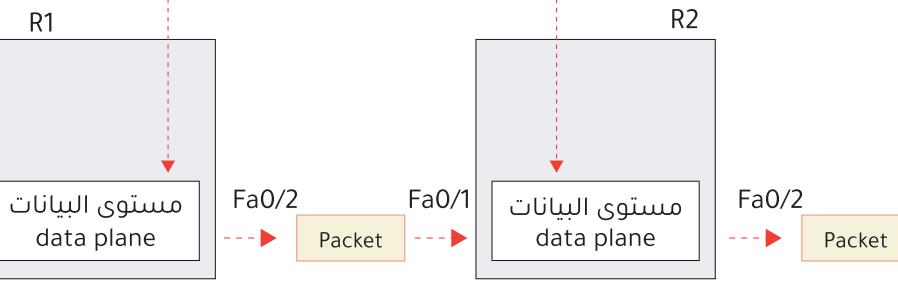
تحتوي هذا على وحدة تحكم SDN التي تتلقى وتعالج التعليمات من طبقة التطبيق. المطلوبة.

#### التطبيق

#### REST API

#### وحدة التحكم

#### مستوى التحكم



### طبقة البنية التحتية

#### Infrastructure Layer

والتي تحتوي على الأجهزة الفعلية المسؤولة عن إعادة توجيه الرسائل عبر الشبكة.

### مراجعة سريعة لـ SDN :

- الـ SDN هو نهج للشبكات يجعل مستوى التحكم مركزيًا في تطبيق يسمى وحدة التحكم.

- تعمل وحدة التحكم SDN على مركبة وظائف مستوى التحكم مثل حساب المسارات وغيرها. معنى أن أجهزة الشبكة لم تعد تستخدم الـ OSPF لمشاركة المعلومات مع بعضها البعض ، وبدلًا من ذلك فإنها تشارك المعلومات مع وحدة التحكم ، التي تأخذ هذه المعلومات وتحسب المسارات للشبكة بأكملها.

- يمكن لوحدة التحكم SDN التفاعل برمجيًا مع أجهزة الشبكة باستخدام واجهات برمجة التطبيقات (API).

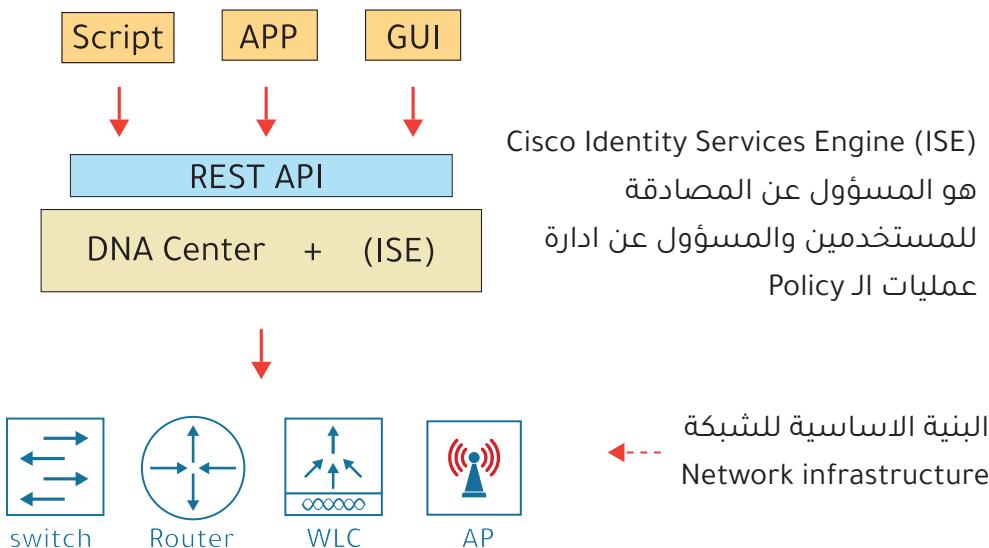
- يتم استخدام الـ SBI للاتصالات بين وحدة التحكم وأجهزة الشبكة التي تحكم فيها.

- يتم استخدام الـ NBI للتفاعل بين وحدة التحكم وبين البرامج النصية والتطبيقات الخاصة.

### بعض مميزات الـ SD-Access :

- أتمتة الاعدادات الخاصة باجهزة الشبكة
- اتمتة اعدادات السياسة الخاصة (Policy) التي نريد تطبيقها في الشبكة
- امكانية وضع الاجهزه والمستخدمين في مجموعات منفصلة عن بعضها البعض بناءً على الهوية وهذا مايسمى بmacro segmentation.

- توفير امكانية التنقل للاجهزه السلكية واللاسلكية بشكل تلقائي مع الحفاظ على السياسة المطبق عليها بدون ان تفقدها عندما تنتقل من السويتش الى اخر.

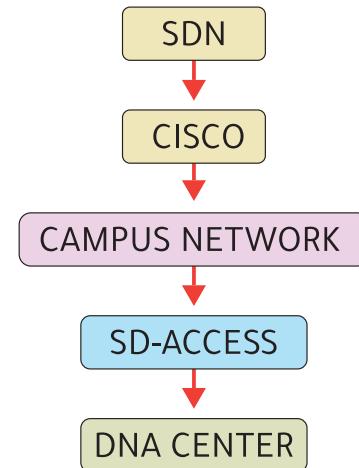


Cisco Identity Services Engine (ISE)  
هو المسؤول عن المصادقة  
للمستخدمين والمسؤول عن ادارة  
عمليات الـ Policy

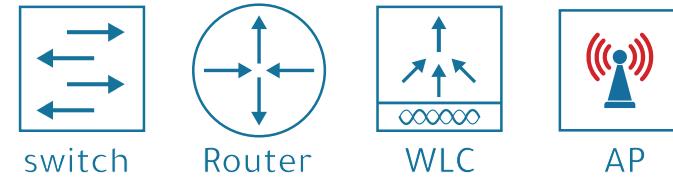
البنية الاساسية للشبكة  
Network infrastructure

## Cisco SD-Access (Software-Defined Access)

من ضمن حلول شبكات الـ SDN والخاصة بشركة سيسكو :  
هي أحد حلول الـ SDN لأتمتة الشبكات المحلية (LAN) : **SD-Access**



- في الـ SD-Access يوجد وحدة التحكم Cisco DNA باعتباره جهاز تحكم حيث يقوم المستخدمون الذين يديرون الشبكة عبر واجهة مستخدم رسومية برمجية (GUI) بتوفير أتمتة الشبكة باستخدام واجهات برمجة التطبيقات (API) .  
ـ Cisco DNA (Digital Network Architecture) هي اختصاراً لـ Cisco DNA



هناك طريقتين لبناء الشبكة واستخدام تقنية الـ SD-Access فيها :

### Greenfield Deployment - 1

في هذه الطريقة يتم بناء الشبكة من الصفر ويتم شراء الأجهزة المتوافقة مع تقنية الـ SD-Access ويتم أتمتة هذه الأجهزة بشكل تلقائي من قبل الجهاز المركزي DNA Center .

### Brownfield Deployment - 2

في هذه الطريقة يتم ضبط الإعدادات الأساسية للأجهزة السويتش والراوتر في الشبكة الموجودة مسبقاً بشكل يدوي ، يتم ضبط بعض الإعدادات الأساسية ومن ثم بالسماح بذلك للجهاز المركزي DNA Center بأتمتة الإعدادات المتبقية مثل إعدادات الـ Policy .

## ≡ طريقة عمل الـ SD-Access

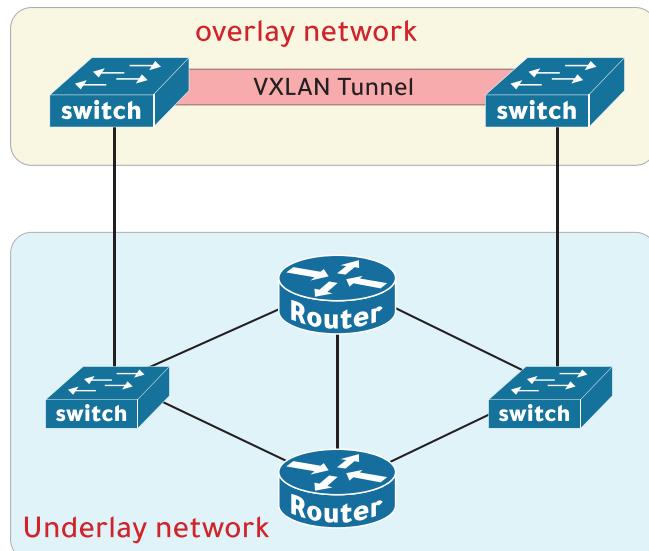
هناك ثلاثة مكونات يجب معرفتها عن الـ SD-Access :

A - Underlay network    B - overlay network    C - Fabric

### overlay network - B

(Underlay network) هي شبكة افتراضية مبنية فوق الشبكة الأساسية وتعتمد عليها .

- على سبيل المثال : يستخدم الـ SD-Access بروتوكولًا يسمى الـ VXLAN لبناء الأنفاق (tunnels).
- يقوم بتغليف إطار Layer 2 Ethernet ونقله في نفق عبر شبكة الـ VXLAN من الطبقة الثالثة Layer 3 .



### Underlay network - A

- الـ Underlay network هي عبارة عن الشبكة الأساسية المكونة من مجموعة من الراوترات والسوبيتشات متصلة مع بعضها البعض .
- يتم تفعيل أحد بروتوكولات التوجيه فيها مثل الـ OSPF أو IS-IS من أجل تبادل معلومات عن الشبكات الموجودة فيها وبناء جداول التوجيه .

- يمكن للجهاز المركزي DNA Center أتمتة شبكة الـ Underlay بشكل تلقائي ولكن دائمًا في هذه الحالة يختار جهاز الـ بروتوكول الـ IS-IS لذلك

- تسمى أيضًا بـ Physical Underlay

هناك ثلاثة أدوار مختلفة للسوبيتشات في الـ SD-Access :

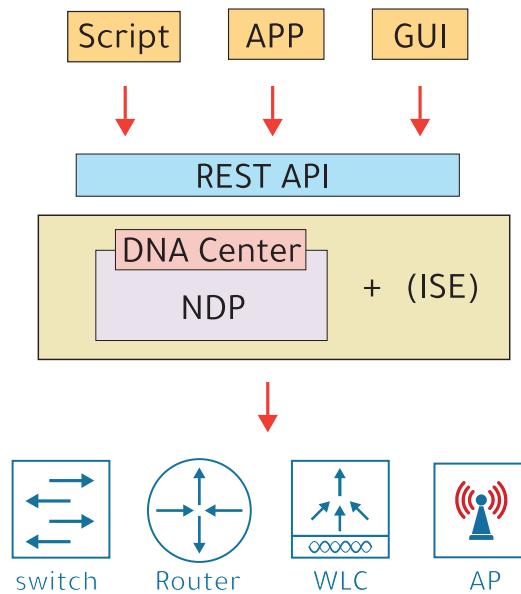
- 1 - Edge nodes : هي الأجهزة القريبة من المستخدم و المتصلة بالمضيفين النهائيين (end hosts)
- 2 - Border nodes : هي الأجهزة المتصلة بأجهزة خارج نطاق الـ SD-Access
- 3 - Control nodes : تستخدم بروتوكول الـ LISP لأداء وظائف مستوى التحكم المختلفة .

- تستطيع التحكم بالـ DNA Center عبر واجهة المستخدم الرسومية (GUI).

يتيح مركز الـ DNA شيئاً يسمى : Intent Based Networking (IBN) وهي عملية أتمتة مدعومة بالبرمجيات تستخدم مستويات عالية من الذكاء والتحليلات والتنسيق لتحسين عمليات الشبكة ووقت التشغيل.

### من مكونات الـ Cisco NDP (Network Datagram Platform)

هو محرك تحليلي يجمع معلومات حول الشبكات ويدعم الذكاء الاصطناعي والتعلم الآلي لتحديد المشكلة واستكشاف الأخطاء وإصلاحها.



**Middle Box Components :**

### DATA Plane - 1

وهو الجزء الخاص بتغليف البيانات الأصلية وفق تقنية الـ VXLAN .

### Control Plane - 2

هو الجزء المسؤول عن تحديد الطريق الذي يجب أن تسلكه البيانات قبل ارسالها من جهاز السويفت الى اخر وطبعاً تستخدم بروتوكول الـ Locator ID Separation Protocol (LISP) .

### Policy Plane - 3

هو الجزء المسؤول عن الأمان والحماية وتقسيم الشبكات الافتراضية

وتعتمد على تقنية الـ Cisco TrustSec (CTS) .

### Management Plane - 4

هو الجزء المسؤول عن عمليات الأتمتة والممثل بالجهاز центральный DNA Center

### Fabric - C

هو المصطلح الذي نطلقه على الشبكة المكونة من الـ Underlay والـ overlay

## Cisco DNA Center

هي اختصار لـ Digital Network Architecture هي وحدة تحكم وإدارة الـ SDN تسمح بالتحكم في الشبكة وتحسينها ومراقبتها وتحليلها وتكوينها .

- يحتوي مركز الـ DNA Center على واجهة برمجة تطبيقات الـ REST API والتي يمكن استخدامها للتفاعل معها.

## الفرق بين إدارة الشبكات التقليدية وإدارة الـ DNA Center

### Traditional network management vs DNA Center

إدارة الشبكات التقليدية Traditional network management	إدارة الـ DNA Center DNA Center management
<p>1 - يتم تكوين وإعداد الأجهزة يدوياً عبر الكونسول .</p> <p>2 - يتم تكوين الأجهزة واحداً تلو الآخر عبر SSH أو عن طريق الوكونسول Consol .</p> <p>3 - تم إدارة التكوينات والسياسات لكل جهاز.</p> <p>4 - عمليات إعداد الشبكة الجديدة تأخذ وقت طويل بسبب العمل اليدوي .</p> <p>5 - احتمال وجود الأخطاء والفشل بسبب زيادة الجهد اليدوي.</p>	<p>1 - تم إدارة الأجهزة ومراقبتها مركزياً من خلال واجهة المستخدم الرسومية (GUI) لمركز DNA أو تطبيقات أخرى باستخدام واجهة برمجة تطبيقات REST الخاصة بها.</p> <p>2 - الإعدادات والتكوينات والسياسات الخاصة يتم تخزينها مركزياً وإدارتها في مركز الـ DNA .</p> <p>3 - يمكن لمركز DNA إدارة إصدارات البرامج مركزياً وتحديثها عند الحاجة.</p> <p>4 - يمكن للأجهزة الجديدة أن تتلقى إعداداتها تلقائياً من مركز الـ DNA بدون تدخل يدوي هذا يساعد على تقليل الأخطاء البشرية والسرعة في عملية الإعداد .</p>

- يمكن لأدوات إدارة التكوين أن تساعد في حل المشكلات مثل منع انحراف التكوين ، وأيضا في توفير التكوين Configuration provisioning.
- الـ Configuration provisioning يشير إلى كيفية تطبيق تغييرات التكوين على الأجهزة ، يتضمن ذلك أيضًا تكوين إعدادات الأجهزة الجديدة .
  - في الطريقة التقليدية في إعداد الأجهزة يتم الإعداد عن طريق الاتصال بالأجهزة واحداً تلو الآخر عبر الـ SSH ، أو عبر الكونسول consol ، طبعاً هذا ليس عملياً في الشبكات الكبيرة التي تحتوي على مئات أو ألف الأجهزة .
  - تتيح لنا أدوات إدارة التكوين مثل Ansible و Puppet و Chef إجراء تغييرات على الأجهزة على نطاق واسع بجزء بسيط من الوقت والجهد .



: (Chef و Puppet و Ansible) المكونات الأساسية لهذه الأدوات الثلاث

- 1 - القالب Template
- 2 - المتغيرات Variables

## أدوات إدارة التكوين

### Configuration Management Tools

#### انحراف التكوين (الإعدادات) Configuration Drift

لفهم أحد الأسباب التي تجعل أدوات إدارة التكوين مفيدة ، لابد من معرفة مفهوم انحراف التكوين .

- يحدث انحراف التكوين عندما تؤدي التغييرات الفردية التي يتم إجراؤها بمرور الوقت إلى انحراف تكوين الجهاز عن التكوينات القياسية والصحيحة المحددة من قبل الشركة .

طبعاً هذا الشيء غير جيد ويجب تجنبه قدر الإمكان .

- يتم تحديد معظم إعدادات الجهاز في قوالب قياسية مصممة بواسطة مهندسي الشركة .

على سبيل المثال ، يمكنك أن تتوقع أن يكون لجميع أجهزة الراوتر الخاصة بك نفس تكوينات الـ SNMP ، ونفس تكوينات الـ Syslog .

- بعض المهندسين الفرديين يقومون بإجراء تغييرات على الأجهزة ، على سبيل المثال لاستكشاف مشكلات الشبكة وإصلاحها ، واختبار التكوينات ، فإن تكوين الجهاز يمكن أن ينحرف بعيداً عن المعيار الخاص بالشركة .

- غالباً لا يتم الاحتفاظ بسجلات هذه التغييرات الفردية وأسبابها ، وقد يؤدي ذلك إلى حدوث مشكلات في المستقبل . على سبيل المثال ، قد يكون من الصعب معرفة ما إذا كان تكوين معين ضروريًّا عند النظر إليه بعد بضع سنوات .

تستخدم أداة الـ Ansible بروتوكول الـ SSH للاتصال بالأجهزة . وإجراء تغييرات على التكوين ، واستخراج المعلومات ، وما إلى ذلك.

- تستخدم أداة الـ Ansible طريقة تسمى بـ الدفع (PUSH) . وهي تعني أن الخادم الرئيسي يتصل عبر الـ SSH بالأجهزة ويستخدم وضع الـ PUSH الخاص بالـ Ansible لدفع تغييرات التكوين لهذه الأجهزة .

- بعد تثبيت الـ Ansible يجب إنشاء عدة ملفات نصية :

#### Playbooks - 1

هذه الملفات هي ( مخططات مهام الأتمتة ) وهي التي تحدد أفعال المهام التي يجب على الـ Ansible القيام بها .

#### Inventory - 2

تسرد هذه الملفات الأجهزة التي ستديرها الـ Ansible . بالإضافة إلى خصائص كل جهاز.

#### Templates - 3

القوالب : تمثل هذه الملفات ملف تكوين الجهاز . ومتقيدة بتنسيق Jinja2

#### Variables - 4

المتغيرات : تسرد هذه الملفات المتغيرات وقيمها ويتم استبدال هذه القيم لإنشاء ملفات تكوين كاملة في القوالب .

هذه هي أدوات أتمتة الشبكة التي تسهل التحكم المركزي لعدد كبير من أجهزة الشبكة.

- هذه الأدوات مفيدة في الشبكات من أي حجم ، وعادةً يتم استخدامها في الشبكات الكبيرة .

- يمكن استخدام هذه الأدوات لأداء مهام مثل:

- إنشاء تكوينات للأجهزة الجديدة على نطاق واسع.

- إجراء تغييرات التكوين على الأجهزة (جميع الأجهزة في شبكتك ، أو مجموعة فرعية معينة من الأجهزة).

- التحقق من تكوينات الجهاز في مطابقتها للمعايير المحددة.

- مقارنة التكوينات بين الأجهزة وبين الإصدارات المختلفة للتكوينات الموجودة على نفس الجهاز.



### Ansible

Ansible هي أداة لإدارة التكوين مملوكة لشركة Red Hat ، المشهورة بـ Red Hat Linux .

- أداة الـ Ansible مكتوبة بلغة الباليون.

- أداة الـ Ansible تعتبر agentless بمعنى أنه لا يحتاج إلى تثبيت برامج محددة على الأجهزة المدارية .

: Puppet master هذه بعض الملفات النصية المطلوبة في الـ

### Manifest - 1

يحدد حالة التكوين المطلوبة لجهاز الشبكة. ثم يستخدم الـ Puppet master هذا البيان لإنشاء تكوينات محددة للأجهزة المدارسة.

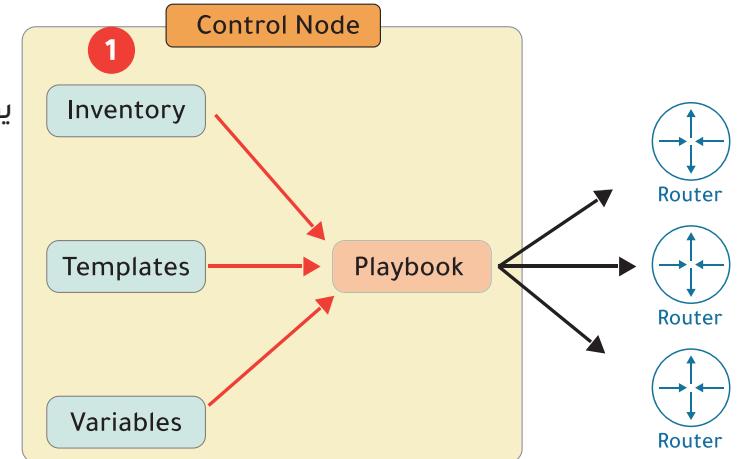
### Templates - 2

القوالب: تمثل هذه الملفات ملف تكوين الجهاز. ومكتوبة بتنسيق Jinja2

يوفر قائمة بالأجهزة

توفر ملفات القوالب  
قوالب تكوين للأجهزة

توفر المتغيرات  
متغيرات محددة  
وقيمها.



يتم إعطاء هذه المدخلات إلى Playbook الذي يتخذ الإجراءات اللازمة لدفع التكوين إلى الأجهزة المدارسة.



**CHEF**

## Chef

Chef هي أداة لإدارة التكوين.

- أداة الـ Chef مكتوبة بلغة Ruby.

- أداة الـ Chef تعتبر agent-based بمعنى أنها يجب تثبيت برامج محددة على الأجهزة المدارسة.

- لا تدعم جميع أجهزة Cisco.

- تستند أداة الـ Chef وضع السحب (PULL)

- يستخدم سيرفر الـ Chef بروتوكول TCP ومنفذ 10002 للتواصل مع الـ العملاء.

: Chef هذه بعض الملفات النصية التي يستخدمها الـ

### Resources - 1

### Recipes - 2

### Cookbooks - 3

### Run-list - 4

## Puppet

Puppet هي أداة لإدارة التكوين.

- أداة الـ Puppet مكتوبة بلغة Ruby.

- أداة الـ Puppet تعتبر agent-based بمعنى أنها يجب تثبيت برامج محددة على الأجهزة المدارسة.

- لا تدعم جميع أجهزة Cisco.

- يُطلق على سيرفر الـ Puppet بـ (Puppet master).

- يستخدم العملاء بروتوكول TCP ومنفذ 8140 للتواصل مع الـ Puppet master.

- تستخدم أداة الـ Puppet وضع السحب (PULL) حيث أن العملاء يسحبون الإعدادات والتكونيات من الـ Puppet master.