

CCNA

Contents

Fundamental.....	20
 Components of a Network	20
1. Devices.....	20
2. Media.....	20
3. Services.....	20
 Network Topologies.....	21
1. Mesh Topology	21
 :التعريف.....	21
 : أنواع Mesh Topology.....	21
 :المميزات	21
 :العيوب	21
 :حالات الاستخدام	21
2. Star Topology	22
 Star Topology.....	22
 :التعريف.....	22
 :طريقة العمل	22
 :المميزات	22
 :العيوب	22
 :حالات الاستخدام	22
3. Ring Topology	23
 Ring Topology.....	23
 :التعريف.....	23
 :طريقة العمل	23
 :المميزات	23
 :العيوب	23
 :حالات الاستخدام	23
4. Bus Topology	24
تعريف Bus Topology:	24

شكلها:	24
طريقة العمل:	24
مميزات Bus Topology:	24
عيوب Bus Topology:	24
حالات الاستخدام:	24
 Topology Diagrams	24
1. Physical Topology	24
2. Logical Topology	25
Network Devices	25
1. Router	25
2. Switch	25
3. Hub	25
4. Access Point	25
5. Modem	26
6. Firewall	26
7. Repeater	26
8. Bridge	26
Transmission	26
1. Half Duplex	26
2. Full Duplex	26
مقارنة سريعة	27
 أولاً: RAM (Random Access Memory)	27
التعريف	27
الوظيفة	27
ملاحظات	27
 ثانياً: NVRAM (Non-Volatile RAM)	27
التعريف	27
الوظيفة	27
ملاحظات	27
 ثالثاً: Flash	28
التعريف	28
الوظيفة	28

◆ ملاحظات:	28
 جدول مقارنة سريع:	28
Types of Network Cables and Connections:	28
1. Ethernet Cable	28
2. Fiber Optic Cable.....	29
3. Coaxial Cable	29
Types of Connections (كيف تتصل الأجهزة بالكابلات):	29
1. Straight-Through Cable	29
2. Crossover Cable	29
Wireless Network Connections:	29
What is the OSI Model?	29
1. Application Layer	29
2. Presentation Layer.....	30
3. Session Layer.....	30
4. Transport Layer.....	30
5. Network Layer	30
6. Data Link Layer.....	30
7. Physical Layer	30
What is TCP/IP?	31
The Four Layers of the TCP/IP Model:	31
1. Network Interface Layer	31
2. Internet Layer	31
3. Transport Layer.....	31
4. Application Layer	31
How TCP/IP Works:	31
TCP (Transmission Control Protocol)	32
What is TCP?	32
Features of TCP:	32
The 3-Way Handshake	32
Example of 3-way handshake:	32
TCP is used in:	32
UDP (User Datagram Protocol)	33
What is UDP?	33

Features of UDP:	33
When do we use UDP?	33
Main differences between TCP and UDP:	33
What is Encapsulation in Networking?	34
Why Do We Use Encapsulation?	34
How Does Encapsulation Work?	34
Example in the TCP/IP Model:	34
1. Application Layer	34
2. Transport Layer	34
3. Network Layer	34
4. Data Link Layer	34
5. Physical Layer	35
Encapsulation Summary:	35
Real-World Example:	35
Note:	35
Internet Protocol (IP)	36
◆ What is Internet Protocol (IP)?	36
◆ How Does IP Work?	36
◆ Types of IP Addresses	36
1. IPv4 (Internet Protocol version 4)	36
2. IPv6 (Internet Protocol version 6)	36
◆ Components of an IP Packet	37
◆ IP Features	37
IPv4 In-Depth	37
IPv4 Address Format	37
Address Types	37
IPv4 Address Classes (الأنواع القديمة)	37
Subnetting Basics	38
قواعد أساسية	38
مثال: تقسيم شبكة 24 إلى 4 Subnets	38
IPv4 vs IPv6 Summary	39

■ IPv4 Header Structure	39
■ IPv6 Header Structure	39
💡 Conclusion	40
✓ Basic Configurations:	40
1. Prompt Notation.....	40
2. [REDACTED] توضيح -	40
3. أنواع تشفير كلمات المرور (Password Encryption Types)	40
4. Telnet/SSH (line vty) 5. أمر حفظ الإعدادات	40
6. SSH توليد مفاتيح	41
7. [REDACTED] 8. فلترة نتائج [REDACTED]	41
Cisco Basics Flashcards.....	41
الأساسية Cisco ملخص سريع لمفاهيم - (Visual Mind Map) Flashcards (Mهمة) 1. [REDACTED]	42
43	
2. boot system tftp://IP/isoname.bin..... 3. boot system flash:isoname.bin	44
Practical Use (Boot Sequence)	44
Important Note:	45
✓ Password Recovery Steps: (مثل الرواتر أو السويتش) Cisco على أجهزة	45
1. Connect the Console Cable.....	45
2. Restart the Device (Reload / Power Cycle)	45
3. Send a Break Signal للدخول إلى ROMmon:..... 4. الدخول إلى ROMmon Mode.....	45
5. تغيير قيمة Configuration Register	46
6. الإقلاع بدون كلمة مرور	46
7. استرجاع الإعدادات الأصلية	46
8. تغيير كلمة المرور المنسية	46
9. للوضع الطبيعي Configuration Register إعادة قيمة	47
10. احفظ الإعدادات وأعد التشغيل	47
✓ ملاحظات مهمة	47

no service password-recovery	47
💡 ما هو no service password-recovery؟	47
✓ متى يستخدم؟	47
⚠️ ماذ يحدث عند تفعيل no service password-recovery؟	48
📌 لتفعيل الأمر	48
🔗 إلغاء التفعيل (إذا كنت المدير المخول)	48
🧠 ملخص	48
✓ 1. show controllers interface-name	48
📌 الصيغة الصحيحة	48
✓ الوظيفة	48
💡 مثال	49
✓ 2. clock rate (فقط Serial تستخدم على منافذ)	49
📌 الصيغة	49
✓ الوظيفة	49
💡 مثال	49
💡 ملاحظة	49
✓ 3. show interface interface-name	49
📌 الصيغة	49
✓ الوظيفة	49
💡 مثال	50
🔍 أهم النتائج	50
✓ 4. show ip interface interface-name	50
📌 الصيغة	50
✓ الوظيفة	50
💡 مثال	50
🧠 ملخص سريع	50
LLDP vs CDP : مقارنة بين بروتوكولات اكتشاف الجيران	51
أوامر الاستكشاف	51
ملاحظات عامة	51
1. Destination Unreachable	52
2. Request Timed Out	52

.....	52
Static Route	
.....	52
1. التعريف البسيط	52
2. تعريف متوسط مع مثال	53
3. التعريف الفني	53
4. Cisco صيغة أمر	53
5. أنواع Static Routes	54
6. إمكانيات Static Routes?	54
ما هو Loopback Interface؟	54
• واجهة افتراضية داخل الراوتر أو السويتش	54
• مش متوصلة بأي كابل أو جهاز فعلي	54
• تستخدم لاختبار الاتصال أو ك هوية ثابتة للراوتر	54
الخصائص الأساسية	54
كيفية إنشاء Loopback Interface	55
👉 الأمر التالي Cisco على أجهزة Cisco:	55
الاستخدامات الشائعة لـ Loopback Interfaces	55
مثال عملي	55
هل أقدر استخدامها في Switch؟	56
ما هو Default Route؟	56
• نوع من أنواع Static Route.	56
• يُستخدم لتوجيه أي ترافيك وجهته غير معروفة إلى مسار محدد	56
• أحياناً يتقال عليه	56
صيغة Default Route في Cisco:	56
مثال عملي	56
إمكانيات استخدام Default Route؟	56
الفرق بين Default Route و Static Route	57
التحقق من Default Route	57
أسئلة شائعة	57
1. الفرق بين Routed Protocol و Routing Protocol	58
2. الفرق بين IGP و EGP	58

3. ملخص سريع	58
4. بروتوكول RIP (Routing Information Protocol).....	59
5. Control Plane vs Data Plane	59
6. أوامر Cisco لبروتوكول RIP المهمة	59
7. تفعيل مصادقة RIP باستخدام Key Chain (MD5 / Clear Text).....	60
8. Manual Route Summarization (تخيص المسارات اليدوي).....	60
9. ملخص مبسط لـ EIGRP	60
10. تفعيل مصادقة MD5 باستخدام EIGRP	61
1. ما هو Administrative Distance (AD)?	61
2. الافتراضية لأنواع المسارات المختلفة AD قيمة	61
3. مثال عملي	62
4. كيف تضبط AD لمسار ثابت (Static Route)؟	62
5. ملاحظات مهمة	62
1. تغيير AD في Static Routes	62
2. تغيير AD في EIGRP	63
EIGRP الداخلي (Internal EIGRP):	63
EIGRP الخارجي (External EIGRP):	63
3. تغيير AD في OSPF	63
4. تغيير AD في RIP	64
6. تغيير AD في IS-IS	64
7. ملخص سريع	64
1. بروتوكول OSPF Hello	65
2. شروط الـ OSPF Neighbors (عسان يبقوا جيران)	65
3. Router ID (RID):	65
4. أنواع الروابط في OSPF:	65
5. Wildcard Mask:	65
6. أوامر مهمة لـ OSPF:	66
7. التوثيق (Authentication) في OSPF:	66
8. تحديد المنطقة (Area) لكل واجهة	66
9. تكلفة الـ Cost على واجهة OSPF	67
10. إعلان Default Route في OSPF:	67
1. تعيين عنوان IPv6 على واجهة	67
2. إضافة Static Route إلى IPv6	67

3. RIP لـ IPv6:	68
4. OSPF لـ IPv6:	68
5. أمر اختبار الاتصال مع تحديد المصدر (Ping IPv6):	68
6. أوامر فحص مهمة.	69
✓ على أجهزة DHCP أولًا: شرح أساسيات Cisco.	69
1. Lease Time	69
2. Static IPs	69
✓ على راوتر DHCP ثالثًا: تكوين Cisco	70
:شرح الأوامر	70
✓ ثالثًا: إظهار العملاء اللي حصلوا على IP	70
✓ DHCP Client من IP يأخذ على راوتر DHCP رابعًا: إعداد	70
✓ في IP خامسًا: تجديد أو تحرير عنوان Windows	71
✓ لعميل معين باستخدام IP سادسًا: حجز MAC Address	71
*:الفكرة	71
:الخطوات	71
:شرح	71
✓ ملخص كامل (مرتب)	71
✓ DHCP في IPv4 (Cisco) أولًا	72
1. IP Bindings	72
2. DHCP Pool	72
(تصفيير العناوين المُعطاة) DHCP Binding مسح/حذف	72
4. لتنبيه رسائل debug لتفعيل التصحيح	72
✓ DHCP في IPv6 ثالثًا	73
1. على الراوتر DHCPv6 تمكين Client Side	73
✓ ملخص الأوامر (مرتب)	73
✓ ملاحظات سريعة	73
✓ أولًا: ما هي الـ Access List?	73
✓ أنواع الـ Access List:	74
✓ تركيب أمر Access List	74
1. Standard ACL	74
2. Extended ACL	74
✓ على الواجهة ACL تطبيق الـ interface	74

<input checked="" type="checkbox"/> أمثلة عملية (مع التعديلات المطلوبة منك)	75
<input checked="" type="checkbox"/> مثال 1: منع دخول الأجهزة من شبكة 192.168.10.0	75
<input checked="" type="checkbox"/> ومنع أي بورت ثاني (HTTP) مثال 2: السماح فقط بالبورت 80	75
<input checked="" type="checkbox"/> بورت 3 باسم لمنع Telnet (23) مثال 3	75
<input checked="" type="checkbox"/> ملاحظات مهمة	75
● أولاً: ما هو NAT?	76
◆ (لا يتم استخدامها مباشرة في الإنترنت) Private IP نطاقات الـ	76
✓ أنواع NAT:	76
① Static NAT (ثابت)	76
<input checked="" type="checkbox"/> الأمر	76
<input checked="" type="checkbox"/> تطبيق على الواجهات	76
<input checked="" type="checkbox"/> مثال كامل	76
② Dynamic NAT	77
<input checked="" type="checkbox"/> الخطوات	77
③ PAT (Port Address Translation) أو NAT Overload	77
<input checked="" type="checkbox"/> الخطوات	77
<input checked="" type="checkbox"/> ملاحظات عن PAT:	78
<input checked="" type="checkbox"/> أوامر المراجعة والمتابعة	78
◆ مثال مختصر لاستخدام PAT:	78
<input checked="" type="checkbox"/> ملخص سريع	78
<input checked="" type="checkbox"/> أولاً: الفرق بين Switch و Bridge	79
■ مفاهيم الشبكات في Layer 2:	79
■ أوامر مهمة لمراقبة السويفتش	79
◆ عرض حالة المنافذ	79
◆ عرض جدول الـ MAC Address:	79
◆ عرض محتويات جدول MAC Address:	79
■ أوامر التحكم في MAC Address Table	80
◆ ثابت MAC إضافة	80
◆ كامل MAC مسح جدول	80
◆ معين MAC مسح	80
◆ مسح حسب الانترفيس	80

█	Password Recovery على Switch.....	80
◆	خطوات استعادة كلمة السر على سويتش Cisco:.....	80
█	ملحوظة عن الملفات.....	81
✓	مراجعة أوامر MAC:.....	81
█	VLAN (Virtual LAN)	81
✓	أوامر مهمة:.....	81
⚠	حذف إعدادات VLAN	82
█	متعددة VLANs نقل بيانات (Trunking)	82
█	إعداد منفذ Trunk:.....	82
█	المسموح بها VLANs تحديد	82
█	عرض معلومات Trunk:.....	82
█	عرض وضع المنفذ	82
█	DTP – Dynamic Trunking Protocol	82
⚠	VLAN Hopping (هجمات الشبكة).....	83
1.	VLAN Spoofing	83
2.	Double Tagging	83
█	Voice VLAN (نقل بيانات VoIP)	83
▲	STP – Spanning Tree Protocol	83
✓	الغرض:	83
🔍	أوامر STP:	83
█	إعداد STP:	84
➡	تسريع الاتصال على منافذ المستخدمين (PortFast).....	84
█	عرض حالة المنافذ	84
✓	ملخص سريع:.....	84
⌚	AoLa: DHCP Attack – هجوم DHCP Spoofing.....	85
✓	الفكرة:	85
⌚	DORA Process (الحصول على IP من DHCP).....	85
🔍	أوامر مهمة:	85
✓	DHCP Spoofing باستخدام DHCP Snooping.....	85
█	خطوات التفعيل على السويتش	85
⚠	ثانياً: ARP Attack (ARP Spoofing / Poisoning).....	86

	اللكرة	86
	الحماية باستخدام Dynamic ARP Inspection (DAI)	86
	تفعيل DAI على VLAN:	86
	منفذ موثوق (مثل الموصل بالراوتر)	86
	(على السويفت MAC + IP ربط) إضافة Static Binding:	86
	بديل باستخدام ACL:	86
	أوامر فحص ومتابعة	87
	ملخص سريع للأوامر حسب الوظيفة	87
	ما هو DHCP Spoofing؟	87
	الحل: DHCP Snooping	87
	على السويفت (مصنفة وواضحة) DHCP Snooping أوامر تفعيل	88
1.	عالمياً: تفعيل DHCP Snooping	88
2.	معينة VLAN على DHCP Snooping تفعيل	88
3.	(Option 82): تفعيل خيار المعلومات	88
4.	تحديد المنفذ الموثوق (الذي متصل بالسيرفر)	88
5.	المسماوح بها في الثانية DHCP تحديد عدد باكيتات	88
	أوامر فحص مهمة	89
	تصحيح بعض الأخطاء الإملائية في أوامرك	89
	ملاحظات إضافية	89
	ما هو Port Security؟	89
	متى نستخدم Port Security؟	90
	الشروط	90
	خطوات الإعداد والأوامر	90
1.	(Interface): ادخل على الواجهة	90
2.	خلي البوت في وضع Access	90
3.	Port Security: فعل	90
4.	حدد عدد المالك أدرييس المسماوح به	90
5.	طريقة تسجيل المالك أدرييس	90
	ثالثاً: Errdisable & Recovery	91
	ما هو Errdisable؟	91
	أوامر تفعيل الاسترجاع التلقائي للبورتات	91
	أوامر المراقبة	91

6. حدّ طريقة التعامل مع الاختراق (violation):	91
✎: أوامر العرض والمراقبة	92
عرض معلومات البورت:	92
عرض كل الماك أدريس المرتبطة بالبورتات:	92
عرض حالة البورتات كلها:	92
☒: في حالة حدوث Violation:	92
🔗: لجوء البورت دخل حالة err-disabled:	92
✍: حذف الماك أدريس المسجلة تلقائياً	92
💡: مثال تطبيقي كامل	92
📌: ملاحظات	92
🎯: الهدف	93
🧠: المفاهيم الأساسية	93
💻: الخطوات بالتفصيل	93
✳️ 1. على الراوتر أو السيرفر (DHCP) إعداد IP Phones	93
✳️ 2. على الراوتر (CME) إعداد خدمة الاتصال	93
✳️ 3.تعريف رقم لكل هاتف (Directory Number)	94
✳️ 4.تعريف الهاتف نفسه وربطه بالرقم	94
✳️ 5. إعداد السويفتش لتوصيل IP Phones	94
📋: أوامر مفيدة	95
💻: شكل بسيط للإعدادات كلها (ملخص)	95
☒: أوّلاً CDP (Cisco Discovery Protocol)	96
✅ ما هو CDP؟	96
📌: أهم أوامر CDP:	96
🔌: ما هو PoE؟	96
⚙️: كيف تعمل PoE؟	96
🔧: أنواع أجهزة PoE	97
🌐: الرسمية PoE معايير	97
✅: مميزات PoE	97
🔍: على سويفتش PoE أوامر فحص Cisco	97
📌: ملاحظة مهمة	97
⚡: ما هو EtherChannel؟	98

 خطوات تكوين EtherChannel	98
 تحديد مجموعة المنافذ 1.....	98
 حذف الإعدادات القديمة (اختياري لكن مهم) 2.....	98
 إعداد المنافذ 3.....	98
 عرض حالة الـ EtherChannel.....	98
 مثال للحالة	98
 على القناة الافتراضية IP إعداد (Port-Channel)	99
 التعامل مع أخطاء التكوين !.....	99
 الحل	99
 استرجاع المنافذ للإعدادات الافتراضية	99
 ملاحظات هامة	99
 ما هو VTP؟	100
 أنواع الـ VTP Modes	100
 ملاحظات هامة ✓	100
 الأساسية VTP إعدادات	100
 ملاحظات حول الإصدارات	100
 أوامر متقدمة في VTPv3	100
 ملاحظة	101
 كيف يتم حذف إعدادات VTP؟	101
 أوامر العرض (Show Commands)	101
 VTP Pruning	101
 ما هو؟	101
 التفعيل	101
 شرح	101
 مسموحة على VLANs تحديد Trunk:	101
 محدد VTP على Interface تعطيل	102
 أهم الملاحظات العملية	102
Redundancy Protocols	102
1. HSRP - Hot Standby Router Protocol.....	102
 أوامر HSRP	102
 لتعزيز الاعتمادية (مراقبة المسارات)	103

المصادقة Authentication:	103
لإيقاف البروتوكول:.....	103
2. VRRP - Virtual Router Redundancy Protocol.....	103
أوامر VRRP:	104
3. GLBP - Gateway Load Balancing Protocol.....	104
أوامر GLBP:	104
شرح طرق التحميل Load Balancing:	104
ملخص بسيط للفروقات	105
AAA - Authentication, Authorization, Accounting.....	105
أنواع السيرفرات المستخدمة في AAA	105
1. TACACS+ (Cisco Proprietary).....	105
2. RADIUS (Open Standard)	105
إعداد AAA على أجهزة Cisco.....	106
1. تفعيل نموذج AAA:.....	106
2. (تسجيل الدخول) باستخدام مجموعة سيرفرات Authentication أو Radius (Tacacs+):	106
3. تعريف سيرفر TACACS+ أو RADIUS:	106
4. ربط تسجيل الدخول بالخطوط:	106
5. اختبار المستخدم على السيرفر (Test AAA Group):	107
شرح البروتوكولات والمنافذ	107
Cisco ISE (Identity Services Engine).....	107
ملخص مختصر للأوامر	107
<input checked="" type="checkbox"/> 802.1 ما هو Q (dot1q)؟	108
<input checked="" type="checkbox"/> يعني ايه Tagging؟	108
<input checked="" type="checkbox"/> ليه بنستخدم Q؟	108
<input checked="" type="checkbox"/> شكل إطار 802.1 Q (Untagged و Tagged)	108
802.1Q Tag Structure (4 Bytes):	108
<input checked="" type="checkbox"/> كيف يتم إرسال الإطارات بين السواليشات؟	109
<input checked="" type="checkbox"/> على سويتش Cisco مثال Trunk 802.1 بـ Q مثل عملی – إعداد	109
<input checked="" type="checkbox"/> ما هي Native VLAN في dot1q؟	109
مثال:.....	109
<input checked="" type="checkbox"/> ملخص سريع	109
<input checked="" type="checkbox"/> ما الفرق بين 802.1 Q و 802.1 X؟	110

802.1X Authentication:	110
المكونات الأساسية لـ 802.1X:	110
شرح الأوامر:	110
◆ تفعيل 1. AAA:	110
◆ إعداد طريقة التوثيق 2.	110
◆ على السويفتش dot1x تفعيل 3.	111
◆ على منفذ معين تفعيل 4. 802.1X	111
إعداد الجهاز (PC – Supplicant):	111
◆ خطوات:	111
كيف تتم العملية:	112
تطبيق عملی مشترك مع Cisco ISE:	112
WIFI-Technology	112
ما هو VRF?	113
ليه نستخدم VRF?	113
VRF vs. بدون VRF:	114
مثال واقعي:	114
شركة عندها:	114
على VRF خطوات إعداد Cisco Router:	114
1. إنشاء VRF:	114
2. ربط الواجهات بالـ VRF:	114
3. إنشاء جداول راوتر مستقلة:	115
التحقق من VRF:	115
قائدة مهمة:	115
VRF Lite vs. MPLS VRF	115
مثال تطبيقي سريع:	115
VPN.....	117
أوّلاً: ليه GRE + IPsec?	117
💡 خطوات الإعداد الأساسية:	117
إعداد 1. ISAKMP (Phase 1)	118
➤ ISAKMP Policy:	118
➤ تعريف الـ Pre-Shared Key:	118

	لتحديد نوع الترافيك اللي هيتشفر ACL 2.	118
	3. إعداد Transform Set (IPsec Phase 2)..... 3.	118
	4. إعداد Crypto Map	119
	على الواجهة Crypto Map 5. تطبيق.	119
	6. إعداد نفق GRE:..... 6.	119
	أوامر التحقق (Show Commands):..... 7.	119
	ملخص التسلسل	120
	T-Shoots	120
	في الشبكات Troubleshooting خطوات عملية لعمل 1.	120
	اسأل نفسك: "فين المشكلة؟" (تعريف المشكلة) 2.	120
	ابداً من أسفل لأعلى (OSI Model) 3.	120
	Layer 1: Physical	120
	Layer 2: VLAN / STP / Trunk..... 4.	121
	Layer 3: IP Routing..... 5.	121
	حدد النقطة اللي بتنفشل فيها (Isolate the failure) 6.	121
	حل المشكلة من الزاوية المناسبة 7.	121
	نقد التغيير أو أصلاح المشكلة 8.	122
	:إن المشكلة اتحلت (Verify) اختبر 9.	122
	Logs سجل التغيير وراقب 10.	122
	:سريعة حسب نوع المشكلة Checklists خلي عندك 11.	122
	مثال: TSHOOT VLAN..... 12.	122
	مثال: TSHOOT IP Route..... 13.	122
	Tips: سريعة 14.	123
	:ما traceroute؟ 15.	123
	:الأمر 16.	123
	:على سيسكو 17.	123
	:على ويندوز 18.	123
	:على لينكس / ماك 19.	123
	:كيف يعمل؟ 20.	123
	Cisco: مثال على 21.	124
	:الناتج 22.	124

💡 فايدة traceroute:	124
⚠ في النتيجة * * لو شفت نجوم	124
✓ نصيحة:	124

Fundamental

What is Network?

الشبكة هي نمط من الترابط بين مجموعة من الأشياء.

What is Computer Network?

متصلة معاً لتقديم خدمة معينة (Hosts) هي مجموعة من الأجهزة.

"الشبكة الصغيرة للمكاتب والمنازل تسمى SOHO".

التي تعمل عن طريق إرسال البيانات عبر موجات الراديو من Wireless LAN هي التي ابتكرت تقنية الـ IEEE منظمة جهاز إلى آخر.



Components of a Network

1. Devices

- **End Devices:** مثل الحواسيب، الطابعات، والهواتف الذكية – هي الأجهزة التي يتفاعل معها المستخدم مباشرةً.
 - **Intermediate Devices (Mid Devices):** مثل الراوترات، السويفتس، ونقاط الوصول – مسؤولة عن توجيه البيانات بين الأجهزة.
-

2. Media

- **Wired (Cable):** مثل كابلات الإيثرنت أو الألياف الضوئية.
 - **Wireless:** مثل الواي فاي أو البلوتوث – تنقل البيانات بدون الحاجة إلى كابلات مادية.
-

3. Services

هي البرمجيات أو الأنظمة التي توفر وظائف عبر الشبكة، مثل:

- البريد الإلكتروني
- خدمات الويب
- مشاركة الملفات

Network Topologies

1. Mesh Topology

التعريف:

متصل بشكل مباشر مع كل جهاز آخر في الشبكة، مما يوفر مسارات متعددة لنقل (Node) تصميم شبكة حيث كل جهاز قادر على إرسال البيانات إلى أي جهاز آخر.

أنواع Mesh Topology:

1. Full Mesh:

كل جهاز متصل مباشرة بكل الأجهزة الأخرى.

2. Partial Mesh:

بعض الأجهزة متصلة فقط حسب الحاجة.

المميزات:

- موثوقية عالية: إذا فشل مسار ما، يمكن للبيانات أن تستخدم مساراً بديلاً.
- أداء عالي: لا يوجد ازدحام لأن كل جهاز لديه مسارات متعددة.
- أمان أفضل: الشبكة أقل عرضة للفشل الكامل بسبب تعدد الاتصالات.

العيوب:

- تكلفة عالية: تحتاج إلى عدد كبير من الكابلات والاتصالات.
- صعوبة التركيب والصيانة، خاصة في الشبكات الكبيرة.
- مع إضافة كل جهاز، عدد الاتصالات يزداد بشكل كبير (الصيغة $n(n-1)/2$).

حالات الاستخدام:

تستخدم في الشبكات التي تحتاج موثوقية وأمان عالي، مثل:

- شبكات المطارات والطيران
- أنظمة البنوك
- الشبكات العسكرية أو الحكومية

2. Star Topology

★ Star Topology

✓ التعريف:

تصميم شبكة حيث كل الأجهزة متصلة بجهاز مركزي واحد، مثل **Switch** أو **Hub**.

لا تتصل الأجهزة مباشرة مع بعضها، بل تواصل عبر النقطة المركزية.

⌚ طريقة العمل:

- يرسل كل جهاز البيانات إلى الجهاز المركزي.
- يقوم الجهاز المركزي بإعادة توجيه البيانات للجهاز المستهدف.

📈 المميزات:

- سهل التركيب والإدارة.
- في حالة فشل جهاز واحد، الشبكة تستمر في العمل.
- يمكن إضافة أو إزالة أجهزة دون التأثير على باقي الشبكة.

⚠ العيوب:

- فشل الجهاز المركزي (السوبيتش أو الهب) يؤدي إلى توقف الشبكة بأكملها.
- يتطلب كمية كبيرة من الكابلات لأن كل جهاز يحتاج اتصال خاص بالجهاز المركزي.

📌 حالات الاستخدام:

شائعة في:

- الشركات والمكاتب
- المنازل الذكية
- الشبكات المحلية (LANs)

3. Ring Topology

_RING Topology

التعريف:

تصميم شبكة حيث كل جهاز متصل بالجهاز الذي يليه في حلقة مغلقة.

كل جهاز متصل بجهازين فقط: السابق واللاحق.

طريقة العمل:

- تنقل البيانات في الحلقة، تمرر من جهاز لآخر حتى تصل للوجهة.
- الحلقة يمكن أن تكون اتجاه واحد أو اتجاهين حسب التصميم.

المميزات:

- هيكل منظم وسهل التتبع.
- أداء جيد مع عدد متوسط من الأجهزة.
- قد يقل الحاجة إلى جهاز مركزي (بدون سوينتش أو هب).

العيوب:

- إذا تعطل جهاز أو كابل، قد تتوقف الشبكة بأكملها (في التصميم أحادي الاتجاه).
- صعوبة في التوسيع، لأن إضافة جهاز يتطلب تعديل كامل الحلقة.
- تأخير في الإرسال مع الشبكات الكبيرة، لأن البيانات تمر عبر أجهزة متعددة.

حالات الاستخدام:

تستخدم في شبكات قديمة أو أنظمة بحاجة لترتيب دائري، مثل:

- شبكات FDDI (قيمة)
- بعض أنظمة التحكم الصناعية
- شبكات Token Ring

4. Bus Topology

تعريف Bus Topology:

أو خط الاتصال الرئيسي Bus شبكة حيث كل الأجهزة متصلة بقابل واحد طويلاً يسمى.

شكلها:

تشبه خطًا مستقيماً (سلك طويلاً) تتصل به كل الأجهزة.

طريقة العمل:

- عندما يرسل جهاز بيانات، تبث على كامل الحافلة.
- تسمع كل الأجهزة للإشارة، والجهاز المستهدف يستقبل الرسالة ويرد.

مميزات Bus Topology:

- سهل التركيب والاتصال.
- يحتاج كابلات أقل مقارنة ببعض الطوبولوجيات الأخرى.
- تكلفة منخفضة.

عيوب Bus Topology:

- إذا تعطل كابل الحافلة الرئيسي، الشبكة كلها تتوقف.
- صعوبة في استكشاف الأخطاء.
- مع زيادة الأجهزة، تتحسن سرعة الشبكة بسبب التصالات.
- محظوظية طول الكابل وعدد الأجهزة المتصلة.

حالات الاستخدام:

كانت شائعة في الشبكات الصغيرة والقديمة، لكنها أقل استخداماً اليوم بسبب الطوبولوجيات الأكثر كفاءة مثل Star.

Topology Diagrams

1. Physical Topology

- تمثل التخطيط الفعلي للأجهزة والكابلات في العالم الحقيقي.
- تظهر مواقع الأجهزة والكابلات كما هي مركبة.
- تستخدم عادة في مخططات التصميم أو الهندسة.

مثال: موقع الراوتر في غرفة السيرفرات والكابلات الممتدة إلى المكاتب.

2. Logical Topology

- تبين كيفية تدفق البيانات بين الأجهزة بغض النظر عن موقعها الفعلي.
- تستخدم لتمثيل كيفية عمل الشبكة منطقياً، وليس كيفية توصيلها فعلياً.
- تعرض نوع الاتصال المنطقي (Star, Mesh, Ring ...).

يظهر كل الأجهزة متصلة بسويش حتى لو كانت الكابلات تسير بشكل مختلف Star مثل: مخطط شبكة

Network Devices

1. Router

- الوظيفة: يربط شبكات مختلفة (مثلاً: الشبكة المنزلية بالإنترنت).
- يحدد أفضل مسار لمرور البيانات.
- يعمل في الطبقة 3 (Network Layer).
- مثال: الراوتر الموجود في المنزل.

2. Switch

- الوظيفة: يربط الأجهزة داخل نفس الشبكة المحلية (LAN).
- يرسل البيانات فقط للجهاز المستهدف بناءً على عنوان MAC.
- ي العمل في الطبقة 2 (Data Link Layer).
- أكبر كفاءة من الـ hub.

3. Hub

- الوظيفة: يرسل البيانات الواردة لكل الأجهزة المتصلة.
- ي العمل في الطبقة 1 (Physical Layer).
- قديم وبطيء لأنّه يرسل البيانات للجميع بغض النظر عن الهدف.

4. Access Point

- للأجهزة (Wi-Fi) جهاز يوفر الوصول اللاسلكي.
- يربط الأجهزة اللاسلكية بالشبكة السلكية.

5. Modem

- الوظيفة: يحول البيانات بين الإشارات التنازلية والرقمية.
 - يربط الإنترن特 بمزود الخدمة (ISP).
 - يستخدم للاتصال بالإنترنط عبر خطوط الهاتف أو الكابل.
-

6. Firewall

- جهاز أو برنامج يحمي الشبكة من الهجمات والاختراقات.
 - يراقب ويرشح حركة البيانات الداخلة والخارجة.
-

7. Repeater

- يعزز قوة الإشارة لتمديد مسافة الإرسال.
 - يستخدم في الشبكات السلكية واللاسلكية.
-

8. Bridge

- لتعمل كشبكة واحدة (LANs) يربط شبكتين محليتين.
 - يعمل في الطبقة 2 (Data Link Layer).
-

Transmission

1. Half Duplex

- البيانات يمكن أن تنتقل في كلا الاتجاهين، لكن ليس في نفس الوقت.
 - عندما يرسل جهاز، يجب أن ينتظر الجهاز الآخر حتى ينتهي ليبدأ بالإرسال.
 - حيث يتكلم أحدهما والأخر ينتظر Walkie-talkie مثل واقعي: جهاز الـ.
-

2. Full Duplex

- البيانات يمكن أن تنتقل في كلا الاتجاهين في نفس الوقت.
 - كل جهاز يمكنه الإرسال والاستقبال معًا دون انتظار.
 - مثل واقعي: المكالمات الهاتفية العاديّة.
-

مقارنة سريعة:

الميزة	Half Duplex	Full Duplex
وضع الاتصال	ثنائي الاتجاه لكن غير متزامن	ثنائي الاتجاه ومتزامن
السرعة	أبطأ نسبياً	أسرع وأكثر كفاءة
مثال واقعي	جهاز Walkie-talkie	المكالمات الهاتفية العادية



أولاً: RAM (Random Access Memory)

التعريف:

ذاكرة مؤقتة تعمل فقط أثناء تشغيل الجهاز.

الوظيفة:

- الإعدادات الحالية التي تعمل حالياً running-config تخزن.
- الخاصة بالبيانات routing table و ARP table و gbuffer.
- أي تغييرات يتم على إعدادات الجهاز (قبل الحفظ) تخزن هنا.

ملاحظات:

- تمسح بالكامل RAM عند إعادة تشغيل الجهاز، مثل ذكرة الكمبيوتر العادية.



ثانياً: NVRAM (Non-Volatile RAM)

التعريف:

ذاكرة غير متغيرة، تحفظ البيانات حتى بعد إعادة التشغيل.

الوظيفة:

- الإعدادات الدائمة التي يبدأ بها الجهاز عند التشغيل startup-config تخزن.
- إلى الـ NVRAM من الـ startup-config RAM.

ملاحظات:

- لو عايز تحفظ إعداداتك دائماً، تستخدم الأمر:

- copy running-config startup-config
-



ثالثاً: Flash

♦ التعريف:

، وهي وحدة تخزين دائمة(USB) تشبه الفلاشة.

♦ الوظيفة:

- IOS image).
- ممكن تخزن ملفات أخرى مثل: ملفات الإعدادات، ملفات التحديث، إلخ.

♦ ملاحظات:

- ممكن يكون فيها أكثر من نسخة لنظام التشغيل.
 - يمكن التحقق من محتوياتها باستخدام:
 - dir flash:
-



جدول مقارنة سريع:

الخاصية	RAM	NVRAM	Flash
النوع	مؤقتة (Volatile)	دائمة (Non-Volatile)	دائمة (Non-Volatile)
تحمس عند الإقلاع؟	نعم	لا	لا
الوظيفة الرئيسية	إعدادات حية مؤقتة	إعدادات بدء التشغيل	نظام التشغيل (IOS)
مثال محتوى	running-config	startup-config	c1900-universalk9-mz.SPA.bin

Types of Network Cables and Connections:

1. Ethernet Cable

- أكثر أنواع الكابلات السلكية استخداماً في الشبكات.
 - مقسمة لأنواع حسب الجودة والسرعة المدعومة.
 - يدعم سرعات حتى 100 ميجابت في الثانية: **Cat5**.
 - يدعم حتى 1 جيجابت Cat5 نسخة محسنة من: **Cat5e**.
 - يدعم حتى 10 جيجابت لمسافات قصيرة: **Cat6**.
 - سرعات أعلى وتقليل أفضل للضوضاء: **Cat6a** و **Cat7**.
-

2. Fiber Optic Cable

- ينقل البيانات باستخدام الضوء بدلاً من الإشارات الكهربائية.
 - سرعات نقل بيانات عالية جداً لمسافات طويلة.
 - مقاومة للتداخل الكهرومغناطيسي.
 - يستخدم في الشبكات الكبيرة ومرافق البيانات.
-

3. Coaxial Cable

- يستخدم في الشبكات القديمة وكابلات التلفاز.
 - يحتوي على سلك مركزي مع طبقة عازلة ودرع معدني.
 - أقل استخداماً في الشبكات الحديثة.
-

Types of Connections:

1. Straight-Through Cable

- يستخدم لربط أجهزة من نوع مختلف.
- مثل: جهاز كمبيوتر بسوينش، أو سوينش براوتر.
- ترتيب الأسلك نفسه في الطرفين.

2. Crossover Cable

- يستخدم لربط جهازين من نفس النوع مباشرةً.
- مثل: جهاز كمبيوتر بجهاز كمبيوتر، أو سوينش بسوينش.
- ترتيب الأسلك مختلف في كل طرف لتمرير أسلاك الإرسال والاستقبال.

Wireless Network Connections:

- اتصال لاسلكي بين الأجهزة عبر موجات الراديو: **Wi-Fi**.
 - لا تستخدم كابلات وتعتمد على نقاط الوصول والراوترات.
-

What is the OSI Model?

لشرح كيفية تواصل الأنظمة الشبكية المختلفة مع بعضها من خلال 7 طبقات. كل طبقة ISO هو نموذج قياسي أنشأته منظمة لها وظيفة محددة وتتولى جزءاً معيناً من عملية الاتصال.

1. Application Layer

- أقرب طبقة للمستخدم.
- توفر خدمات الشبكة بشكل مباشر للتطبيقات مثل متصفحات الويب وبرامج البريد الإلكتروني وبرامج الدردشة.
- تتضمن بروتوكولات مثل HTTP وFTP وSMTP وDNS.
- مسؤولة عن كيفية طلب البيانات وعرضها للمستخدم.

2. Presentation Layer

- مسؤولة عن تنسيق وتحويل البيانات ليتم فهمها بين الأنظمة المختلفة.
- إلى ASCII مثل تحويل النص من (نحو Unicode).
- تضييف التشفير وفك التشفير (لالأمان).
- تضغط البيانات لتسريع عملية الإرسال.

3. Session Layer

- تدير جلسات الاتصال بين الأجهزة.
- تنشئ وتحافظ وتنهي الجلسات.
- مسؤولة عن مراقبة البيانات وتنظيم الحوار (مثل المكالمات المرئية أو الدردشة).

4. Transport Layer

- مسؤولة عن النقل الموثوق للبيانات بين الأجهزة.
- تقسم البيانات إلى قطع صغيرة (segments).
- تتضمن وصول البيانات بدون أخطاء وبالتالي ترتيب الصحيح.
- (غير موثوق) UDP و (موثوق) TCP تستخدم بروتوكولات مثل.
- تتحكم في تدفق البيانات لتجنب التزاحم.

5. Network Layer

- مسؤولة عن توجيه البيانات من المصدر إلى الوجهة عبر شبكات مختلفة.
- إلى البيانات IP تضييف عناوين.
- تحدد أفضل مسار للبيانات (routing).
- أشهر بروتوكول فيها IP.

6. Data Link Layer

- تنقل البيانات بين الأجهزة في نفس الشبكة المحلية (LAN).
- تغلف البيانات في إطارات (frames).
- تتحكم في التدفق وتكشف وتصحح الأخطاء البسيطة.
- تتعامل مع عناوين MAC.
- من البروتوكولات المستخدمة Ethernet و PPP.

7. Physical Layer

- تهتم بالنقل الفعلي للبيانات عبر الوسائل المادية (كابلات، ألياف ضوئية، إشارات لاسلكية).
- تحدد أنواع الكابلات والموصلات والإشارات الكهربائية والتعديل.
- مسؤولة فقط عن إرسال البيانات.

What is TCP/IP?

- يشير إلى مجموعة من البروتوكولات تُستخدم لنقل البيانات بين الحواسيب عبر الشبكات، خصوصاً الإنترن特.
- هو الأساس الذي يقوم عليه الإنترنرت والشبكات الحديثة.
- يتكون من مجموعة بروتوكولات تعمل معاً لضمان إرسال البيانات بسرعة وأمان.

The Four Layers of the TCP/IP Model:

1. Network Interface Layer

- مسؤولة عن الإرسال الفعلي للبيانات عبر الوسط الفيزيائي (الكابلات، الواي فاي، الألياف...)
- من نموذج Physical Data Link OSI.
- الفiziائة للأجهزة MAC تتعامل مع عناوين.

2. Internet Layer

- مسؤولة عن توجيه البيانات عبر الشبكات المختلفة.
- لكل جهاز (IP Address) ، الذي يعطي عنواناً رقمياً IP البروتوكول الرئيسي هنا هو.
- تحدد كيفية انتقال البيانات بين الشبكات للوصول إلى الوجهة الصحيحة.

3. Transport Layer

- تعامل مع النقل الموثوق أو السريع للبيانات حسب الحاجة.
- البروتوكولين الرئيسيين:
 - يضمن وصول البيانات بشكل صحيح ومرتب ويعد إرسال المفقود منها: TCP
 - يرسل البيانات بسرعة دون ضمان وصولها (يُستخدم في البث المباشر والألعاب والمكالمات) UDP:

4. Application Layer

- تحتوي على البروتوكولات التي يستخدمها المستخدم مباشرة.
- لترجمة أسماء المواقع DNS للبريد الإلكتروني، SMTP لنقل الملفات، FTP للتصفح الويب، HTTP بمثل.

How TCP/IP Works:

عند إرسال البيانات:

- (مثلاً المتصفح يطلب صفحة ويب) Application Layer تبدأ من.
- التي تقسم وتنظم البيانات (TCP أو UDP) Transport Layer تنتقل إلى.

-
- للتوجيه IP ، التي تضيف عنوان Internet Layer ثم إلى 3.
ترسل البيانات عبر الكابل أو اللاسلكي Network Interface Layer بعدها 4.
عند الاستلام، تتعكس العملية من الطبقة الفيزيائية حتى تصل البيانات للتطبيق 5.
-

TCP (Transmission Control Protocol)

What is TCP?

بروتوكول موثوق يعتمد على الاتصال. يعني أنه قبل إرسال البيانات يتم إنشاء اتصال بين الطرفين وترسل البيانات بشكل منظم ومضمون.

Features of TCP:

- يجب إنشاء اتصال قبل إرسال البيانات.
 - يضمن وصول كل جزء من البيانات بشكل صحيح ومرتب.
 - يعيد إرسال الأجزاء المفقودة.
 - يمنع إغراق المستقبل ببيانات كثيرة.
 - يقلل من معدل الإرسال إذا كانت الشبكة مزدحمة.
 - يقسم البيانات إلى أجزاء صغيرة (segments).
-

The 3-Way Handshake

: هذه العملية تهدف إلى إنشاء اتصال موثوق بين المُرسل والمستقبل

1. طلب بدء الاتصال SYN المُرسل يرسل رسالة SYN.
 2. SYN-ACK على المستقبل يرد برسالة SYN-ACK.
 3. تأكيد الاستلام، ويبدأ تبادل البيانات ACK المُرسل يرد برسالة ACK.
-

Example of 3-way handshake:

الخطوة	من → إلى	الشرح
1. SYN	B الجهاز → A الجهاز	طلب اتصال برقم تسلسلي 1000
2. SYN-ACK	A الجهاز → B الجهاز	تأكيد الطلب مع رقم تسلسلي 2000 ورد 1001
3. ACK	B الجهاز → A الجهاز	تأكيد الاستلام، ويبدأ الاتصال

TCP is used in:

- تصفح الإنترن特 (HTTP/HTTPS)

- البريد الإلكتروني (SMTP, POP3)
 - نقل الملفات (FTP)
 - التطبيقات التي تتطلب موثوقية عالية
-

UDP (User Datagram Protocol)

What is UDP?

بروتوكول غير موثوق ولا يعتمد على الاتصال. يرسل البيانات دون التأكد من الاستلام أو إعادة المفقود منها.

Features of UDP:

- لا يتطلب إنشاء اتصال قبل الإرسال.
 - سريع لأنّه لا يفحص التسلیم أو الترتیب.
 - لا يحتوي على تحكم في التدفق أو التزاحم.
 - يرسل البيانات في رزم مستقلة تسمى datagrams.
-

When do we use UDP?

- في التطبيقات التي تفضل السرعة على الدقة، مثل:
 - البث المباشر للفيديو أو الصوت.
 - الألعاب الأونلайн.
 - المكالمات الصوتية عبر الإنترنت.
 - خدمات DNS.
-

Main differences between TCP and UDP:

الخاصية	TCP	UDP
نوع الاتصال	يُتطلب اتصال (3-way handshake)	لا يتطلب اتصال
الموثوقية	موثوق	غير موثوق
التحكم في التدفق	نعم	لا
التحكم في التزاحم	نعم	لا
السرعة	أبطأ بسبب الفحص والتصحيح	أسرع
الاستخدامات الشائعة	التصفح، المكالمات، البريد الإلكتروني، نقل الملفات	البث، الألعاب



What is Encapsulation in Networking?

OSI مثل) هو عملية **تغليف البيانات** أثناء انتقالها من **الطبقة السفلية** إلى **الطبقة العليا** في النموذج الشبكي (أو TCP/IP).

كل طبقة تضيف رأساً خاصاً بها (وأحياناً ذيلاً) لمساعدة البيانات على الانتقال بشكل صحيح.



Why Do We Use Encapsulation?

- إضافة معلومات مثل العنوان، البروتوكول، نوع البيانات، رقم المنفذ... الخ.
 - حتى تعرف كل طبقة كيف تعالج البيانات وتنقلها.
 - لضمان توصيل البيانات بشكل منظم وآمن.
-



How Does Encapsulation Work?



Example in the TCP/IP Model:

1. Application Layer

- مثل بريد إلكتروني، طلب (يتم إنشاء البيانات HTTP...).
- = "Data" = البيانات

2. Transport Layer

- تُقسم البيانات إلى أجزاء صغيرة وتضاف رؤوس مثل أرقام المنافذ.
- TCP أو UDP تستخدم بروتوكولات مثل.
- = Segment أو Datagram = تصبح البيانات

3. Network Layer

- لل مصدر وال وجهة IP تضاف معلومات مثل عناوين.
- بروتوكول المستخدم عادة هو IP.
- = Packet = تصبح البيانات

4. Data Link Layer

- (فحص الأخطاء FCS مثل) ، وقد يضاف ذيل MAC تضاف رؤوس مثل عناوين.
- = Frame = تصبح البيانات

5. Physical Layer

- (0 و 1)، و تُرسل إشارات كهربائية أو ضوئية أو لاسلكية Bits تُحول الإطارات إلى
-



Encapsulation Summary:

```
[Bits]  
      ↑  
[Frame]  
      ↑  
[Packet]  
      ↑  
[Segment]  
      ↑  
[Data]
```



Real-World Example:

تخيل أنك ترسل رسالة:

1. **Data** = الرسالة نفسها.
 2. **Segment** = (TCP أو UDP) تضيف الغرض.
 3. **Packet** = (IP) تضيف عنوان المترسل.
 4. **Frame** = (MAC) تضيف اسم الشخص داخل البيت.
 5. **Bits** = يتم إرسال الرسالة كإشارات كهربائية أو ضوئية.
-



Note:

عند وصول البيانات إلى المستقبل، يحدث العكس:

كل طبقة تزيل الرأس الخاص بها حتى تصل البيانات للتطبيق → Decapsulation.



Internet Protocol (IP)

◆ What is Internet Protocol (IP)?

- TCP/IP هو بروتوكول أساسى في طبقة الإنترنط ضمن نموذج (IP) بروتوكول الإنترنط.
- من الجهاز المصدر إلى الجهاز الوجهة باستخدام عناوين (packets) مسؤوليته الأساسية هي توصيل الحزم.
- فريد يميزه IP كل جهاز على الشبكة يمتلك عنوان.

◆ How Does IP Work?

- عند إرسال البيانات عبر الشبكات، يتم تقسيمها إلى حزم (packets).
- كل حزمة تحتوي على:
 - عنوان المصدر (Source IP Address)
 - عنوان الوجهة (Destination IP Address)
- بقراءة عنوان الوجهة وتوجيه الحزمة في المسار الأنسب نحو هدفها (Routers) تقوم أجهزة التوجيه.

◆ Types of IP Addresses

1. IPv4 (Internet Protocol version 4)

- مثل 192.168.1.1: الشكل xxx.xxxx.xxxx.xxxx
- بت 32 يستخدم
- عدد العناوين الممكنة: تقريرياً 4.3 مليار

2. IPv6 (Internet Protocol version 6)

- الشكل xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
- بت 128 يستخدم
- عدد العناوين: غير محدود عملياً

◆ Components of an IP Packet

- **Header** يحتوي على معلومات التحكم والعناوين : (رأس الحزمة)
- **Payload** البيانات الفعلية المنقولة : (الحمولة)

◆ IP Features

- **Routing** اختيار أفضل مسار للوصول إلى الوجهة : (التوجيه)
- **Fragmentation/Reassembly** تقسيم الحزم الكبيرة وإعادة تجميعها : (تجزئة/إعادة تجميع)
- **No Reliability** تسليم الحزم (بدون اتصال)، حيث يتم ذلك عن طريق بروتوكولات IP لا يضمن : (غير موثوق)

🌐 IPv4 In-Depth

✓ IPv4 Address Format

- يُكتب كأربعة أرقام عشرية مفصولة بنقط (0 إلى 255)
- مثال: 192.168.1.10

✓ Address Types

النوع	الوصف
Public	قابل للتوجيه عبر الإنترنت
Private	يُستخدم داخل الشبكات الداخلية (مثال: 192.168.x.x)
Unicast	اتصال من جهاز إلى جهاز
Broadcast	إرسال إلى جميع الأجهزة على الشبكة المحلية
Multicast	إرسال إلى مجموعة من الأجهزة (مثال: مؤتمرات الفيديو)

✓ IPv4 Address Classes (الأنواع القديمة)

الفئة	النطاق	عدد الأجهزة بالشبكة	الاستخدام
A	1-126	16 مليون	للشبكات الكبيرة
B	128-191	65 ألف	للشبكات المتوسطة
C	192-223	254	للشبكات الصغيرة
D	224-239	—	للبث المتعدد (Multicast)
E	240-255	—	للتجارب والاختبارات

Subnetting Basics

- **Subnet Mask** يُستخدم لتقسيم الشبكة إلى شبكات فرعية (قناع الشبكة).
- مثال: $255.255.255.0 = /24$

قواعد أساسية

- تمثل الجزء الخاص بالشبكة → Subnet Mask في 1 البتات
- تمثل الجزء الخاص بالمضيفين → 0 البتات (hosts)
- لحساب عدد الشبكات أو عدد المضيفين n^2 استخدم القانون

مثال: تقسيم شبكة /24 إلى 4 Subnets

- الشبكة الأصلية: $192.168.0.0/24$
- نحتاج 2 بت إضافيين للتقسيم → إنشاء 4 شبكات فرعية $\rightarrow 2^2 = 4$

تحويل Subnet Mask

- $/24 = 255.255.255.0 = 11111111.11111111.11111111.00000000$
- $/26 = 255.255.255.192 = 11111111.11111111.11111111.11000000$ → إضافة 2 بت

تفاصيل الشبكات الفرعية

Subnet #	Network ID	First IP	Last IP	Broadcast Address
1	$192.168.0.0/26$	192.168.0.1	192.168.0.62	192.168.0.63
2	$192.168.0.64/26$	192.168.0.65	192.168.0.126	192.168.0.127
3	$192.168.0.128/26$	192.168.0.129	192.168.0.190	192.168.0.191
4	$192.168.0.192/26$	192.168.0.193	192.168.0.254	192.168.0.255

- منها 62 قابلة للاستخدام IP عنوان كل شبكة /26 تعطي.

扈 IPv4 vs IPv6 Summary

الخاصية	IPv4	IPv6
طول العنوان	بت 32	بت 128
الشكل	عشري (مثال: ...192)	مثال: (سادسي عشري 2001:db8::1)
عدد العناوين	مليار ~4.3	غير محدود (3.4×10^{38}) (عملياً)
Header	معقد، متغير الطول	بسيط، ثابت 40 بait
NAT الحاجة لـ	نعم	لا (العناوين تكفي الجميع)
الأمان	(IPSec) اختياري	مدمج داخل البروتوكول



IPv4 Header Structure

الحق	عدد البتات	الوصف
Version	4	إصدار البروتوكول
IHL	4	طول الرأس
Type of Service	8	أولوية الحزمة
Total Length	16	طول الحزمة بالكامل
Identification	16	معرف الحزمة لتجزئة البيانات
Flags	3	التحكم في التجزئة
Fragment Offset	13	موقع التجزئة داخل الحزمة الأصلية
TTL	8	عدد القفزات (العمر)
Protocol	8	(إلخ, TCP, UDP, ...) البروتوكول التالي
Header Checksum	16	فحص الأخطاء في الرأس
Source IP	32	عنوان المصدر
Destination IP	32	عنوان الوجهة
Options (اختياري)	متغير	نادر الاستخدام
Padding	متغير	لتكميل الرأس إلى 32 بت



IPv6 Header Structure

الحق	عدد البتات	الوصف
Version	4	(6) إصدار البروتوكول
Traffic Class	8	أولوية الحزمة
Flow Label	20	لتعريف التدفقات (مثل البث المباشر)
Payload Length	16	طول البيانات التالية للرأس
Next Header	8	أو UDP TCP يشير إلى Extension Header
Hop Limit	8	مثل TTL
Source Address	128	الخاص بالمرسل IP عنوان
Destination Addr	128	الخاص بالمستقبل IP عنوان

● يتم استخدام Extension Headers الرئيسي على: تجزئة IPv6 ، أو خيارات داخل Header ، أو Checksum على ذلك.



Conclusion

- لا يزال مستخدماً على نطاق واسع، لكنه محدود من حيث عدد العناوين IPv4 بروتوكول.
- يوفر حلاً موسعاً وأمناً وفعالاً للمستقبل IPv6 بروتوكول.
- فهم كلا البروتوكولين ضروري لأي متخصص شبكات أو تكنولوجيا معلومات.
- يعتبر أمراً أساسياً لإدارة الشبكات وحل مشاكلها subnetting ، وأنواع العناوين ، وعمليات headers الإقان في.



Basic Configurations:

1. Prompt Notation

- كالتالي (interfaces) من الأفضل توحيد كتابة أسماء الواجهات:
 - أو الاختصار GigabitEthernet0/0
 - Gig0/0لا تفرق بين الحروف Cisco رغم أن gig0/0 لا تستخدم الحروف الصغيرة مثل

2. no ip domain-lookup - توضيح

- لمنع الرواتر من محاولة حل أي كلمة غير معروفة باسم نطاق (labs) هذا الأمر مفيد جدًا للمبتدئين أو في المختبرات ، مما يقلل تأخير الكتابة الخاطئة (hostname).

3. أنواع تشفير كلمات المرور (Password Encryption Types)

- لتشفيير كلمة المرور MD5 يستخدم enable secret.
- عبر SHA-256 مع خوارزمية 9 Type في الإصدارات الحديثة يمكن استخدام.
- enable algorithm-type scrypt secret MyStrongPass
- enable password يُخزن نصاً عاديًّا إلا إذا فعلت service password-encryption.

4. تكوين خطوط Telnet/SSH (line vty)

- يتيح 5 جلسات متزامنة (من 0 إلى 4).
- يمكنك زيادة العدد حتى 15 line vty 0 15.

5. أمر حفظ الإعدادات

- يعمل بشكل جيد، ولكن الاختصار الشائع هو write memory للأمر.
- write

6. توليد مفاتيح SSH

- لتوليد مفاتيح RSA:
crypto key generate rsa
How many bits in the modulus [512]: 1024
الحجم الموصى به: 1024 أو 2048 بت.

7. أمر clear line

- معينة SSH أو Telnet يستخدم لإنهاء جلسات.
- تحذير: استخدامه بحذر لأنه قد يفصل جلساتك إذا كنت متصلًا عن بعد.

8. فلترة نتائج show running-config

- يمكنك استخدام الفلتر

الفلتر	الوظيفة
include	عرض الأسطر التي تحتوي على كلمة محددة
exclude	عرض الأسطر التي لا تحتوي على كلمة محددة
begin	عرض الإخراج بداية من سطر معين
section	عرض قسم كامل مثل interface أو line vty

- مثال:
- show running-config | include hostname

- بطاقات تعليمية تفاعلية Cisco Basics Flashcards

- لتعطيل خاصية DNS lookup على جهاز Cisco:
no ip domain-lookup
- الفرق بين enable secret و enable password:
enable secret مشفر باستخدام MD5، و enable password مشفر باستخدام service password-encryption.
نص عادي إلا إذا شُفر بأمر service password-encryption.
- تشفير جميع كلمات المرور النصية في إعدادات Cisco:
service password-encryption
- لتتمكن من توليد مفاتيح RSA SSH:
crypto key generate rsa
- حفظ الإعدادات الحالية لتصبح إعدادات بدء التشغيل:

```
crypto key generate rsa general-keys modulus <number>
```

modulus number

— وأقل من 512 أكثر من) حجم المفتاح بالبت، و 1024 هو حجم مقبول للأمان الجيد.

أو

```
write memory
```

- عرض جميع جلسات المستخدمين النشطة:

```
show users
```

- معينة إنتهاء جلسة Telnet:

```
clear line <line_number>
```

- فقط SSH من الوصول البعيد إلا عبر:

- line vty 0 4
- transport input ssh

ملخص سريع - خريطة ذهنية (Visual Mind Map) - الأساسية Cisco لمفاهيم

- **Modes (الأوضاع):**
 - User EXEC
 - Privileged EXEC
 - Global Configuration
 - Interface Configuration
- **Password & Encryption Types:**
 - enable password (نص عادي)
 - enable secret (MD5)
 - service password-encryption
 - Type 9 (SHA-256 في الإصدارات الحديثة)
- **Remote Access:**
 - Telnet (غير آمن)
 - SSH (آمن، يحتاج توليد مفاتيح RSA)
- **Key Commands:**
 - show running-config مع فلاتر (include, exclude, begin, section)
 - clear line <number> لإنهاء الجلسات
 - copy running-config startup-config أو write memory للحفظ
- **Session Management:**
 - show users لعرض الجلسات النشطة
 - line vty 0 4 لتحديد عدد الجلسات البعيدة

البند	الوصف / الشرح	الأمر / الأمثلة
1 كتابة أسماء الواجهات	بـ (interfaces) توحيد كتابة أسماء الواجهات: تجنب GigabitEthernet0/0 أو Gig0/0. الحروف الصغيرة (مع أنها مقبولة).	interface GigabitEthernet0/0 أو int Gig0/0
2 تعطيل DNS lookup	يمنع الرواوتر من محاولة حل أي كلمة غير معروفة. كاسم نطاق، يقلل التأخير عند كتابة أوامر خاطئة.	no ip domain-lookup
3 تشفير كلمات المرور	- enable secret: MD5 مشفر بـ - بالإصدارات الحديثة: نوع 9 مع SHA-256 -	- enable secret pass

	نص عادي إلا إذا فعلت التشفير العام	- service password-encryption
4. تكوين خطوط Telnet/SSH	يسمح لـ 5 جلسات متزامنة: - line vty 0 4: يمكن زيادة العدد حتى 15 جلسة بـ line vty 0 15	line vty 0 15 transport input ssh login local
5. حفظ الإعدادات.	أمر حفظ الإعدادات الجارية إلى ملف الإقلاع	<ul style="list-style-type: none"> • write memory • write • copy running-config startup-config
6. RSA توليد مفاتيح لـ SSH	بحجم 1024 أو 2048 بت RSA توليد مفتاح للأمان عالي	<pre>crypto key generate rsa general-keys modulus <number></pre> <p>How many bits in modulus [512]: 1024</p>
7. إنهاء جلسات Telnet/SSH	لإنهاء جلسة بعينها. يجب الحذر لأنه قد يفصل جلساتك عن بعد.	clear line <line_number>
8. فلترة نتائج show running-config	استعراض أوامر محددة أو أقسام معينة داخل إعدادات التشغيل.	- `show running-config
9. عرض الجلسات النشطة	إظهار جميع جلسات المستخدمين المتصلة بالراوتر	show users
10. منع الوصول إلا SSH عبر فقط	SSH تقييد الوصول البعيد ليكون فقط عبر	line vty 0 15 transport input ssh login local
11. تعيين دومين SSH (ضروري لـ)	تعريف اسم النطاق قبل توليد مفاتيح RSA	ip domain-name example.com

مهمة (Flashcards) بطاقات تعليمية

المفهوم	الشرح	الأمر
DNS lookup تعطيل	يمنع الراوتر من محاولة حل أسماء خاطئة DNS	no ip domain-lookup
الفرق بين enable secret و enable password	enable secret MD5 ، enable password نص عادي	enable secret pass enable password myPass
تشفيير كلمات المرور النصية	تشفيير جميع كلمات المرور النصية في الإعدادات	service password-encryption
لتتمكن RSA توليد مفاتيح SSH	لأمان الاتصال RSA إنشاء مفاتيح	crypto key generate rsa
حفظ الإعدادات الحالية	حفظ الإعدادات حتى تبقى بعد إعادة التشغيل	write memory أو copy running-config startup-config
عرض الجلسات النشطة	إظهار جلسات المستخدمين المتصلة	show users
معينة Telnet إنهاء جلسة	محددة SSH أو Telnet إغلاق جلسة	clear line <line_number>
SSH تقييد الوصول ليكون فقط	فقط SSH السماح بالوصول عبر غير الآمن Telnet لمنع	line vty 0 4 transport input ssh login local

1. `dir flash`

- في الجهاز flash يعرض محتويات ذاكرة الـ **الوظيفة**.
 - **الشرح**:
 - وملفات أخرى (IOS) لتخزين نظام التشغيل flash ستستخدم ذاكرة الـ flash.
 - مثل flash عند تنفيذ هذا الأمر، يتم عرض قائمة بالملفات المخزنة في الـ flash:
 - Switch# `dir flash:`
 - Directory of flash:/
 -
 - 2 -rw- 12345678 <date> c2960-lanbasek9-mz.150-2.SE.bin
 - 3 -rw- 102400 <date> vlan.dat
-

2. `boot system tftp://IP/isoname.bin`

- عنوان) من سيرفر خارجي TFTP من خلال (IOS) يوجه الجهاز لتحميل نظام التشغيل **الوظيفة**.
 - **الشرح**:
 - بدلًا من الـ TFTP موجود على سيرفر IOS يستخدم هذا الأمر عندما تريد أن يقع الجهاز من ملف المحلي.
 - مثل:
 - `boot system tftp://192.168.1.10/c2960-lanbasek9-mz.150-2.SE.bin`
 - من العنوان المحدد IOS المعنى: عند الإقلاع، جرب أولاً تحميل وتشغيل ملف
-

3. `boot system flash:isoname.bin`

- مخزن في الـ IOS يوجه الجهاز للإقلاع من ملف **الوظيفة** flash.
 - **الشرح**:
 - محفوظاً محلياً على الجهاز IOS هذا الخيار يستخدم عادة عندما يكون ملف الـ flash.
 - مثل:
 - `boot system flash:c2960-lanbasek9-mz.150-2.SE.bin`
-

Practical Use (Boot Sequence)

ـ خطوة بديلة، مثل `boot system` من الشائع استخدام أكثر من أمر

```
conf t
boot system tftp://192.168.1.10/ios1.bin
boot system flash:ios2.bin
end
wr
```

- المحلي flash ، وإذا فشل، يحاول من الـ TFTP من IOS سيحاول الجهاز أولاً تحميل الـ **المعنى**.
-

Important Note:

بعد تغيير إعدادات الإقلاع، من الأفضل دائمًا تشغيل الأمر:

```
write memory
```

أو

```
copy running-config startup-config
```

لحفظ التعديلات قبل إعادة التشغيل.

✓ Password Recovery Steps على أجهزة Cisco مثل الرووتر أو (السويتش):

1. Connect the Console Cable

- لتوصيل جهاز الكمبيوتر بالجهاز (رووتر أو سويتش) **Console** استخدم كابل.
 - :استخدم برنامج طرفي مثل
 - HyperTerminal
 - Tera Term
 - PuTTY
-

2. Restart the Device (Reload / Power Cycle)

- أطفئ الجهاز ثم أعد تشغيله.
 - خلال أول 60 ثانية من الإقلاع، يجب إدخال **ROMmon Mode**.
-

3. Send a Break Signal للدخول إلى ROMmon:

حسب البرنامج الطرفي الذي تستخدمه:

البرنامج	كيفية إرسال إشارة Break
HyperTerminal	Ctrl + Break أو Ctrl + Fn + Break
Tera Term	Alt + B أو اضغط Control > Send Break من القائمة
PuTTY	Ctrl + Break أو كليك يمين Special Command > Break

4. الدخول إلى ROMmon Mode

: يجب أن ترى هذا السطر Break بعد إرسال إشارة

```
rommon 1 >
```

5. Configuration Register تغيير قيمة

(مكان تخزين الباسورد) NVRAM أدخل الأمر التالي لتجاوز إعدادات الإقلاع من:

```
confreg 0x2142
```

- هذا يخبر الجهاز بتجاوز الإعدادات المخزنة عند الإقلاع.

ثم أعد التشغيل:

```
reset
```

6. الإقلاع بدون كلمة مرور

- بعد الإقلاع، سيبدأ الجهاز وكأنه جديد، ولكن الإعدادات الأصلية ما زالت محفوظة.
- عندما يطلب منك إدخال إعداد أولي، اختر "No":

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

7. استرجاع الإعدادات الأصلية

ادخل إلى وضع Privileged EXEC:

```
enable
```

ثم استرجع الإعدادات المحفوظة:

```
copy startup-config running-config
```

الآن تم تحميل الإعدادات الأصلية في الذاكرة، ويمكنك تغيير كلمة المرور.

8. تغيير كلمة المرور المنسية

ادخل إلى الوضع العام للإعدادات:

```
conf t
```

```
enable secret NEWPASSWORD
```

بكلمة السر الجديدة NEWPASSWORD استبدل.

9. Configuration Register [إعادة قيمة اللوحة الطبيعية]

```
config-register 0x2102
```

10. احفظ الإعدادات وأعد التشغيل.

```
end  
write memory  
reload
```

✓ ملاحظات مهمة:

- يتجاهل إعدادات الإقلاع المحفوظة مؤقتاً = **0x2142**.
 - القيمة الافتراضية، تُعيد الإقلاع بالإعدادات الأصلية = **0x2102**.
-

```
no service password-recovery
```

، خصوصاً في البيئات الآمنة Cisco هذا أمر يستخدم لتعطيل عملية استرجاع كلمة المرور على أجهزة



ما هو `no service password-recovery`؟

، وظيفته **global configuration** أمر يدخل من وضع

- عبر إشارة ROMmon منع الدخول إلى وضع Break.
 - مثل (منع تنفيذ خطوات استعادة كلمة المرور `confreg 0x2142`).
 - (مما يمسح كل الإعدادات) في حال نسيان كلمة المرور، الخيار الوحيد هو إعادة ضبط المصنع.
-

✓ متى يستخدم؟

- في الشركات أو البيئات ذات الأمان العالي.
- على أجهزة يمكن الوصول إليها فيزيائياً من قبل غير مخولين.

ماذا يحدث عند تفعيل `no service password-recovery`؟

- أثناء الإقلاع → الجهاز لن يدخل Break إذا أرسلت إشارة ROMmon.
- إذا حاول شخص تجاوز كلمة المرور → المحاولة ستفشل إلا إذا تم مسح كامل للجهاز.
- الطريقة الوحيدة لاسترجاع الجهاز:
 - توصيله عبر الكونسول ○
 - يدوياً بطرق متقدمة (صعبة جدًا) ○ NVRAM مسح

لتفعيل الأمر:

```
conf t
no service password-recovery
end
write memory
```

لإلغاء التفعيل (إذا كنت المدير المخول):

إذا لم يكن مفعل مسبقاً، يمكنك إلغاؤه هكذا:

```
conf t
service password-recovery
end
write memory
```

ملخص:

الامر	الوظيفة
<code>service password-recovery</code>	يسمح باستعادة كلمة المرور (الإعداد الافتراضي)
<code>no service password-recovery</code>	يمنع استعادة كلمة المرور؛ يزيد الأمان

1. `show controllers interface-name`

الصيغة الصحيحة:

```
show controllers [interface-name]
```

الوظيفة:

- يعرض تفاصيل فизيائية من الطبقة الثانية للواجهة مثل

- نوع الكابل
- على منافذ (Serial على سرعة الساعة)
- هل الواجهة DCE أو DTE

💡 مثال:

```
show controllers serial 0/0/0
```

✓ 2. `clock rate` (فقط Serial تُستخدم على منافذ)

📌 الصيغة:

```
interface serial 0/0/0
clock rate [value]
```

✓ الوظيفة:

- لضبط سرعة الإرسال في وصلة **DCE** تُستخدم فقط على الطرف (bps).
- إلخ، 64000, 128000, 2000000: قيم شائعة.

💡 مثال:

```
conf t
interface serial 0/0/0
clock rate 64000
```

💡 ملاحظة:

- `clock rate`, فقط في **Ethernet** لا تُستخدم في منافذ **Serial DCE**.

✓ 3. `show interface interface-name`

📌 الصيغة:

```
show interface [interface-name]
```

✓ الوظيفة:

- يعرض حالة شاملة للواجهة، مثل:
 - حالة الواجهة (up/down)
 - السرعة وازدواجية الإرسال

- عدد الحزم المرسلة/المستلمة
- الأخطاء والمشاكل

 **مثال:**

```
show interface gigabitEthernet 0/1
```

 **أهم النتائج:**

- line protocol is up/down
 - input errors, CRC, output drops
-

4. show ip interface interface-name

 **الصيغة:**

```
show ip interface [interface-name]
```

 **الوظيفة:**

- للواجهة مثل (IP) يعرض إعدادات الطبقة الثالثة
 - مفعل؟ IP هل الـ
 - مطبق؟ هل هناك ACL
 - مفعّل؟ هل Proxy ARP
 - هل تشارك الواجهة في DHCP relay؟

 **مثال:**

```
show ip interface serial 0/0/0
```

 **ملخص سريع:**

الأمر	الوظيفة
show controllers int	DCE/DTE تفاصيل فизيائية، سرعة الساعة،
clock rate VALUE	يضبط سرعة الإرسال في واجهة DCE
show interface int	الحالة العامة والإحصائيات
show ip interface int	على الواجهة IP الإعدادات المرتبطة بالبروتوكول

مقارنة بين بروتوكولات اكتشاف الجيران LLDP vs CDP

الخاصية / الأمر	LLDP (Link Layer Discovery Protocol)	CDP (Cisco Discovery Protocol)
نوع البروتوكول	قياسي مفتوح	خاص بشركة Cisco
الأجهزة المدعومة	معظم الأجهزة غير التابعة لـ Cisco	Cisco مثل) فقط Cisco ASA Firewall)
طبقة العمل	(طبقة ربط البيانات) Layer 2	(طبقة ربط البيانات) Layer 2
الحالة الافتراضية	مفعل على بعض الأنظمة غير Cisco	مفعل تلقائياً على أجهزة Cisco
الاستخدام في شبكات WAN	يمكن استخدامه	لا يُستخدم في شبكات WAN

أوامر الاستكشاف

الوظيفة	أوامر LLDP	أوامر CDP
عرض الجيران	show lldp neighbors	show cdp neighbors
عرض معلومات تفصيلية	show lldp neighbors detail	show cdp neighbors detail
عرض حالة واجهة على LLDP	show lldp interface [interface-name]	-
عرض معلومات جهاز معين	-	show cdp entry [device-name]
تفعيل البروتوكول عالمياً	lldp run	cdp run
تعطيل البروتوكول عالمياً	no lldp run	no cdp run
تفعيل الإرسال على واجهة	lldp transmit	cdp enable (على الواجهة)
تعطيل الإرسال على واجهة	no lldp transmit	no cdp enable (على الواجهة)
تفعيل الاستقبال على واجهة	lldp receive	-
تعطيل الاستقبال على واجهة	no lldp receive	-
مسح جدول الجيران	-	clear cdp table

ملاحظات عامة

- كلا البروتوكولين يستخدمان في:
 - استكشاف المشاكل
 - معرفة الأجهزة المتصلة مباشرة
 - رسم خريطة الشبكة
- بروتوكول مفتوح ومدعوم في أجهزة مختلفة LLDP ، بينما WAN وغير مخصص لـ Cisco خاص بـ CDP.

1. Destination Unreachable

:الأسباب المحتملة. هذه الرسالة تأتي من جهاز وسيط أو راوتر وتفيد بأن الجهاز الهدف غير قابل للوصول

- الجهاز الهدف مغلق أو مفصول.
- المسار إلى الجهاز مفقود أو به خلل.
- أحد الأجهزة الوسيطة لا يستطيع تمرير الحزمة.
- تمنع الوصول VLAN أو ACL مشاكل في الإعدادات مثل.

.يعني أن المشكلة في مسار الشبكة أو الجهاز موجود لكنه غير متاح

2. Request Timed Out

:الأسباب الشائعة. ولم يستلم ردًا في الوقت المحدد (ping مثل) يعني أن جهازك أرسل طلبًا

- الجهاز الهدف مغلق.
- وجود جدار ناري يمنع الرد على ping.
- الشبكة مشغولة أو بها فقدان في الحزم.
- فقدان الرد أثناء الطريق.

.يعني أن الجهاز لم يرد – إما لا يستجيب أو الحزم تضيع

ملخص:

الرسالة	المعنى الأساسي	السبب المحتمل
Destination Unreachable	الجهاز أو المسار غير متوفّر	مشكلة في التوجيه أو الجهاز مفصول
Request Timed Out	لم يتم استلام رد في الوقت المحدد	الجهاز لا يستجيب، أو جدار ناري، أو فقدان حزم



Static Route

1. التعريف البسيط

- هو مسار يتم تكوينه يدوياً بواسطة مسؤول الشبكة ليخبر الراوتر بكيفية الوصول إلى شبكة معينة.
 - أنت اللي بتحدد المسار بنفسك بدل ما الراوتر يحدده تلقائياً ببساطة.
-

2. ● تعريف متوسط مع مثال

- **Static Route** هو إعداد يدوى على الراوتر يخبره بكيفية توجيه الحزم إلى شبكة محددة باستخدام **next-hop IP address** أو **واجهة محددة**.
 - **مثال:** إذا كان لديك راوتر وتريد أن تصل شبكتك الداخلية إلى شبكة أخرى عبر راوتر وسيط، ستضيف Static Route يحتوي على عنوان الوجهة والطريقة للوصول إليها.
-

3. التعريف الفني

- يخبر الراوتر. هو إدخال يدوى في جدول التوجيه الخاص بالراوتر **Static Route**:
"أو استخدم واجهة الخروج دي next-hop IP لو تتبع ببيانات لشبكة معينة، ابعثها إلىـ"
- **الخصائص الرئيسية:**
 - يتم تعيينه يدوياً من قبل المسؤول
 - لا يتغير إلا لو تم تعديله يدوياً

المميزات:

- بسيط، متوقع، وسريع.
- يوفر موارد الراوتر.
- أكثر أماناً لأنه تحت السيطرة الكاملة.

:العيوب

- لا يتكيف مع تغييرات الشبكة تلقائياً.
 - غير عملي في الشبكات الكبيرة أو الديناميكية.
-

4. صيغة أمر Cisco

الصيغة العامة:

```
ip route [destination network] [subnet mask] [next-hop IP address or exit interface]
```

مثلاً:

```
ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

بتابعه IP ، أبعت الترافيك إلى الرووتر اللي 192.168.2.0/24 ده معناه: للوصول إلى شبكة

5. أنواع Static Routes

النوع	الوصف
Next-hop IP route	الخاص بالراوتر المجاور IP بتحدد عنوان.
Exit interface route	: يتحدد واجهة الخروج مباشرة (زى FastEthernet0/0).
Floating static route	مسار احتياطي يشغل لو المسار الأساسي فشل (باستخدام Adminstrative Distance أعلى).

6. إمّي تستخدم Static Routes؟

- في الشبكات الصغيرة أو البسيطة.
 - لربط راوترتين أو شبكات معينة مباشرة.
 - كنسخة احتياطية بجانب بروتوكولات التوجيه البنamiكية.
 - لما تحتاج تحكم بالكامل في مسارات التрафيك.

ما هو Loopback Interface؟

- واجهة افتراضية داخل الراوتر أو السويتش
 - مش متوصلة بأي كابل أو جهاز فعلي
 - تُستخدم لاختبار الاتصال أو ك هوية ثابتة للراوتر.

الخصائص الأساسية

الخاصية	الشرح
افتراضية	لا تعتمد على أي اتصال مادي.
دانماً مفعولة	تظل شغالة إلا إذا تم إيقافها يدوياً.
ثابت IP	ستستخدم غالباً كعنوان ثابت لهوية الراوتر في البروتوكولات.
مفيدة لاختبار OSPF	تساعد في اختبار الاتصال الداخلي أو استقرار البروتوكولات زري.

✓ كيفية إنشاء Loopback Interface

💡 الأمر التالي على أجهزة Cisco :

```
Router(config)# interface loopback 0
Router(config-if)# ip address x.x.x.x x.x.x.x
```

- ◆ (ز) هو رقم الواجهة — تقدر تنشئ أكثر 0 الرقم loopback 1, loopback 2, ...).

✓ الاستخدامات الشائعة لـ Loopback Interfaces

1. اختبار الاتصال (Ping):

عشن تأكيد إن الروتر شغال كويس ping نقدر تستخدموه لـ

◦ في البروتوكولات

2. Router ID:

كـ loopback من الواجهات IP ، غالباً الروتر بيختار أعلى BGP أو OSPF في بروتوكولات زي Router ID.

3. هوية ثابتة:

بما إنها مش مرتبطة بقابل، تكون عنوان موثوق وثابت

◦ يستخدم في التوجيه

4. لتوالرارات static و dynamic routing:

ممكن تستخدم في

✓ مثال عملي

كده راورين. ممكن تستخدم OSPF افترض إنك بتكون

```
interface loopback 0
 ip address 1.1.1.1 255.255.255.255
```

- ◆ 1.1.1.1 هو OSPF Router ID ده بيخلطي الـ

هل أقدر أستخدمها في Switch؟

وتقدر Layer 3 بس بعض سويتشات **loopback interfaces** في الراوترات غالباً **أبوه**، لكن للإدارة IP تستخدمها ك عنوان.

ما هو Default Route؟

- نوع من أنواع Static Route.
- ببسطه توجيه أي ترافيك وجهته غير معروفة إلى مسار محدد.
- أحياناً ينتقل عليه "Catch-all route", "default gateway", أو "last-resort route".

صيغة Default Route في Cisco:

```
ip route 0.0.0.0 0.0.0.0 [next-hop IP address or exit interface]
```

- معناها: "أي شبكة مش معروفة".

مثال عملي

الداخلي بتاعه IP افترض إن عندك راوتر متصل بالإنترنت من خلال راوتر أو موdem خاص بمزود الخدمة، و للتوجيه كل الترافيك غير المحلي ليه 192.168.1.1:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

أو باستخدام واجهة الخروج:

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
```

إمتي تستخدم Default Route؟

السيناريو	الوصف
الوصول للإنترنت	توجيه الترافيك غير المعروف إلى بوابة مزود الخدمة.

شبكة صغيرة	لما تكون مش مستخدم بروتوكولات توجيهه ديناميكية وعايز إعداد بسيط
هيكل مركزي (Centralized)	إرسال كل التрафيك إلى راوتر مركزي يعرف باقي المسارات
راوترات الحدود (Edge)	لربط الشبكات الداخلية بالشبكات الخارجية (زي الإنترنت)

✓ الفرق بين Default Route و Static Route

الخاصية	Static Route	Default Route
الهدف	شبكة محددة	أي شبكة غير معروفة
الوجهة	network + mask	0.0.0.0 0.0.0.0
المرونة	مستهدف	Catch-all

✓ التحقق من Default Route

`show ip route`

- هتشوف سطر زي:

S* 0.0.0.0/0 [1/0] via 192.168.1.1

- المعتمد default route معناها إن ده هو النجمة.

✓ أسئلة شائعة

س: هل أقدر أستخدم Default Route مع Dynamic Routing؟
ج: أيوه، ممكن تكونه وتعيد توزيعه داخل بروتوكولات زي OSPF أو EIGRP.

س: هل أقدر أضيف أكثر من Default Route؟
ج: أيوه، لكن الراوتر هيختار بناءً على Administrative Distance (AD) أو metric.

1. الفرق بين Routed Protocol و Routing Protocol

العنصر	Routed Protocol (لبيانات)	(بروتوكول توجيه) Routing Protocol
التعريف	(IP مثل) بروتوكول يحمل البيانات نفسها	بروتوكول بيحدد أفضل طريق للبيانات
الوظيفة	ينقل البيانات بين الأجهزة	لتوجيه (Routing Table) يبني جدول التوجيه للبيانات
أمثلة	IP, IPX, AppleTalk	RIP, OSPF, EIGRP, BGP
يعتمد على	لتحديد Routing Protocol يعتمد على الطريق	لا ينقل بيانات، بس بيختار الطريق
يظهر في جدول التوجيه؟	(نعم، يظهر كشبكة وجهة) Destination	لا، يظهر فقط في العمليات الداخلية للراوتر

مثال:

- IP → Routed Protocol لأنّه يحمل البيانات
- OSPF → Routing Protocol لأنّه يحدّد الطريق

2. الفرق بين IGP و EGP

العنصر	IGP (Interior Gateway Protocol)	EGP (Exterior Gateway Protocol)
النطاق	(داخلي AS) داخل شبكة أو منظمة واحدة	(بين AS) بين شبكات أو منظمات مختلفة
الاستخدام	التوجيه الداخلي (داخل الشبكة)	التوجيه الخارجي (على الإنترن特)
الهدف	(intra-domain routing)	توجيه بين الشبكات (inter-domain routing)
أمثلة	RIP, OSPF, EIGRP, IS-IS	BGP (البروتوكول الخارجي الأشهر والأكثر استخداماً)

3. ملخص سريع.

- Routed Protocol → IP مثل) ينقل البيانات
- Routing Protocol → OSPF, RIP مثل) يحدّد طريق البيانات
- IGP (RIP, OSPF) توجيه داخلي داخل شبكة واحدة →
- EGP (BGP) توجيه بين شبكات مختلفة →

4. بروتوكول RIP (Routing Information Protocol)

الخاصية	RIP v1	RIP v2
طريقة الإرسال	Broadcast (بث عام)	Multicast (بث موجه)
العنوان المستخدم	255.255.255.255 (بث عام)	224.0.0.9 (فقط RIP بث موجه لموجهين)
دعم VLSM	لا	نعم
دعم المصادقة	لا	نعم
إرسال جدول التوجيه	كل 30 ثانية إرسال الجدول كامل	كل 30 ثانية إرسال الجدول كامل

5. Control Plane vs Data Plane

العنصر	Control Plane	Data Plane
الوظيفة	اتخاذ قرارات التوجيه (حساب الجداول، البروتوكولات)	نقل البيانات فعلياً عبر الشبكة
مكان التنفيذ	الراوتر (البرمجيات) على CPU	أسرع وأكثر تخصصاً - (ASICs) على الأجهزة
أمثلة	بروتوكولات مثل OSPF, BGP, RIP	تحويل وتوجيه الحزم (Packet Forwarding)
السرعة	أبطأ بسبب الحسابات	أسرع لأنها تتنفيذ مباشرةً

6. Cisco RIP المهمة أوامر

- `show ip protocols` يعرض تفاصيل بروتوكولات التوجيه النشطة :
- `router rip` للدخول في وضع تكوين RIP
- `network [network-address]` لتحديد الشبكات التي سُئل عن RIP
- `version [1|2]` لتحديد نسخة RIP
- `no auto-summary` تعطيل التلخيص التلقائي عند حدود الشبكات
- `show ip route protocol rip` يعرض المسارات التي تعلمها RIP
- `debug ip rip` مباشرة لأغراض التشخيص RIP لعرض تحديثات

7. تفعيل RIP باستخدام Key Chain (MD5 / Clear Text)

خطوات التفعيل:

1. إنشاء سلسلة المفاتيح (Key Chain): وتعريف كلمات المرور مع أوقات صلاحية

```
2. key chain <name>
3. key 1
4. key-string <pass>
5. accept-lifetime 00:00:00 Jan 1 2024 infinite
6. send-lifetime 00:00:00 Jan 1 2024 infinite
```

7. تفعيل المصادقة على الواجهة:

```
8. interface FastEthernet0/0
9. ip rip authentication mode md5
10. ip rip authentication key-chain <name>
```

8. Manual Route Summarization (تلخيص المسارات اليدوي)

• دمج عدة شبكات فرعية في شبكة واحدة أكبر لتقليل حجم جدول التوجيه وتحسين الأداء.

• بمثال:

ش�كات: 24/192.168.2.0 و 24/192.168.1.0

بعد المقارنة الثانية، نستخدم 23/192.168.0.0 كشبكة ملخصة

• التفعيل:

```
• interface FastEthernet0/0
• ip summary-address rip x.x.x.x x.x.x.x
```

9. ملخص مبسط لـ EIGRP

• Cisco من تطويره (IGP) بروتوكول توجيه داخلي

• للمصادقة MD5 يستخدم

• يرسل جدول التوجيه كامل مرة واحدة عند بداية التشغيل، ثم يرسل فقط التغييرات عند التغيير

• يحسب المسارات الرئيسية والاحتياطية (successor و feasible successor)

• يدعم الأوامر المهمة مثل `show ip eigrp neighbors` و `show ip eigrp topology`

10. تفعيل مصادقة EIGRP باستخدام MD5

1. إنشاء Key Chain:
2. key chain <name>
3. key 1
4. key-string <pass>
5. تفعيل المصادقة على الواجهة
6. interface GigabitEthernet0/0
7. ip authentication mode eigrp 100 md5
8. ip authentication key-chain eigrp 100 <name>
9. التحقق:
 - o show ip eigrp neighbors
 - o show ip eigrp topology
 - o show run interface GigabitEthernet0/0
 - o debug eigrp packets

1. ما هو Administrative Distance (AD)?

- هو رقم يستخدمه الراوتر ليقرر أي مصدر مسار يثق فيه أكثر عندما يعرف أكثر من طريق للشبكة نفسها.
- كلما كان الرقم أقل، يكون المصدر أكثر ثقة.

2. قيم AD لأنواع المسارات المختلفة: الافتراضية

نوع المسار	قيمة AD	معنى القيمة
Connected	0	المسار الأكثر ثقة لأنه مباشر (موصل مباشرة)
Static Route	1	مسار مضاد يدوياً، جدًا موثوق
EIGRP (داخلي)	90	بروتوكول خاص بسيسكو، موثوق جدًا
OSPF	110	بروتوكول مفتوح واسع الاستخدام
IS-IS	115	مشابه لـ OSPF
RIP	120	أقدم بروتوكول، الأقل ثقة بين بروتوكولات IGP
EIGRP (خارجي)	170	الداخلي EIGRP أقل ثقة من
BGP (خارجي)	20	يستخدم على الإنترنت، موثوق جدًا
BGP (داخلي)	200	الخارجي BGP أقل ثقة من
DHCP Route	254	مسارات تعلمها الراوتر من DHCP
غير معروف/غير صالح	255	لا يستخدم، يُرفض

3. مثال عملی:

عبر 10.0.0.0/24 لو الراوتر تعلم عن الشبكة:

- OSPF → AD = 110
- EIGRP → AD = 90

أقل → أي أكثر ثقة AD لأنـه لديه EIGRP فالراوتر سيختار مسار

4. بيدوياً (Static Route) لمسار ثابت كيف تضبط.

```
ip route 192.168.1.0 255.255.255.0 10.1.1.1 5
```

- لهذا المسار له أولوية(EIGRP) اليدوي، وهي أقل من 90 AD هي 5 هنا القيمة.
-

5. ملاحظات مهمة:

- يُستخدم لاختيار أفضل مسار بين بروتوكولات مختلفة AD.
 - يُستخدم لاختيار أفضل مسار داخل نفس البروتوكول(hops) مثل الكلفة أو عدد القفزات (Metric) المترک.
-

(Routing) داخل أشهر بروتوكولات التوجيه **Administrative Distance (AD)** تمام! هنا طريقة تعريف أو ضبط بشكل عام يمكن تغييره في بعض البروتوكولات والبعض الآخر لا يمكن أو يكون AD ، لأن Cisco في أجهزة (Cisco) محدود التغيير.

1. تغيير AD في Static Routes

هي مع AD أسهل وأشهر طريقة للتغيير static routes:

```
ip route [network] [mask] [next-hop-address] [administrative-distance]
```

مثال:

```
ip route 192.168.10.0 255.255.255.0 10.1.1.1 5
```

2. تغيير AD في EIGRP

EIGRP الداخلي (Internal EIGRP):

للوبروتوكول الداخلي AD تغيير (Default AD = 90):

```
router eigrp 100
  distance [AD_value] [ip-address]
```

- distance [AD_value] يغير AD كل المسارات.
- [ip-address] اختياري لتحديد مسار معين AD.

مثال:

```
router eigrp 100
  distance 95
```

تساوي 95 بدلاً من 90 EIGRP AD هذا يجعل.

EIGRP الخارجي (External EIGRP):

للمسارات الخارجية AD لتغيير (Default AD = 170):

```
router eigrp 100
  distance eigrp 100 170
```

لكن عادة نستخدم:

```
router eigrp 100
  distance 170 200
```

الأول للداخلي، الثاني للخارجي.

3. تغيير AD في OSPF

- داخل الرووتر لأنه ثابت على 110 OSPF الخاص بـ AD بشكل عام لا يمكن تغيير.

مع تغيير static routes أو route-map redistribution لكن يمكن عمل.

أثناء إعادة توزيع AD مثل لتغيير (redistribution):

```
router ospf 1
  redistribute eigrp 100 metric 10 metric-type 1 subnets route-map SET_AD
route-map SET_AD permit 10
```

```
set metric 10  
set metric-type type-1
```

، هو ثابت OSPF نفسها لا تغير داخل AD لكن

4. في AD تغيير RIP

- باستخدام RIP داخل AD يمكن تغيير:

```
router rip  
distance [value]
```

مثال:

```
router rip  
distance 150
```

6. في AD تغيير IS-IS

- ثابت (115) ولا يمكن تغييره بشكل مباشر في AD عادة.

ملخص سريع:

البروتوكول	داخلي؟ AD يمكن تغيير	الأمر/كيفية التغيير
Static	نعم	ip route ... [AD]
EIGRP	نعم	router eigrp ... distance
OSPF	لا (ثابت 110)	مباشرة AD لا يمكن تغيير
BGP	نعم	router bgp ... distance bgp ...
RIP	نعم	router rip distance ...
IS-IS	لا	مباشرة AD لا يمكن تغيير

1. بروتوكول OSPF Hello والمراحل:

- اللي جنبهم (Routers) علشان يعرف جيرانه Hello الراتر بيستخدم رسالة اسمها Init State ، تانية منه، بنسمي الحالة دي Hello ، لو استلم رسالة Hello بيعت رسالة R1 مثلاً لما الراتر يعني بدأ يتعرف على الجار
 - يعني الراترين اتفقوا 2-Way Communication من الراتر الثاني، العلاقة بتتطور لـ Hello لما يستلم رد يكونوا جيران ويتبادلوا معلومات
-

2. شروط الـ Neighbors في OSPF (عشان يبقوا جيران):

لكي يكون الراترين جيران في :

- على نفس الشبكة (Directly Connected) يكونوا متصلين مباشرة ببعض
 - وقناع الشبكة (Network ID) يكونوا على نفس معرف الشبكة (Subnet Mask).
 - ، لو مفغل (Authentication) يستخدموا نفس نوع التوثيق
 - يكونوا في نفس المنطقة (Area ID) داخل OSPF.
-

3. Router ID (RID):

- هو معرف فريد للراتر داخل بروتوكول OSPF.
 - مكون من 32 بت IP يشبه عنوان.
 - بيتحدد بأحد الطرق دي (بالترتيب):
 - معرف يدوى بيحدده المسؤول.
 - واجهة افتراضية (Loopback) على واجهة IP أعلى عنوان.
 - على أي واجهة فعلية شغالة IP أعلى عنوان.
-

4. أنواع الراترات في OSPF:

- ABR (Area Border Router):** زي جسر بين المناطق (Area) في OSPF راتر بيربط بين أكثر من منطقة.
 - ASBR (Autonomous System Border Router):** زي مع شبكة خارجية أو نظام مستقل ثاني OSPF راتر بيربط شبكة BGP.
-

5. Wildcard Mask:

- معناها لازم نتحقق من القيمة دي في عنوان الـ (0s) أصفار
-

- معناها "مش مهم" أو مش لازم تتحقق منها، أي رقم ممكن يكون في المكان ده (1s) واحdas
-

6. أوامر مهمة لـ OSPF:

- عرض معلومات عامة عن OSPF:
 - show ip ospf
 - معلومات عن الشبكات والروابط (OSPF) عرض قاعدة بيانات:
 - show ip ospf database
 - على واجهة معينة OSPF عرض تفاصيل:
 - show ip ospf interface <interface-name>
 - لتحريك معرف الراوتر (Router ID):
 - router ospf <process-id>
 - router-id <new-router-id>
 - لازم تعيد تشغيل البروتوكول Router ID بعد تحريك الـ:
 - clear ip ospf process
 - في الوقت الحقيقي (مفید للتصحیح) Hello لمراقبة رسائل:
 - debug ip ospf hello
-

7. التوثيق في OSPF (Authentication):

- تفعيل توثيق بسيط على واجهة معينة:
 - interface <name>
 - ip ospf authentication
 - ip ospf authentication-key <password>
 - (أكثـر أمانـاً) MD5 تفعـيل تـوثـيق باـسـتـخدـامـ:
 - interface <name>
 - ip ospf authentication message-digest
 - ip ospf authentication message-digest-key <key-number> md5 <password>
 - تفعـيل التـوثـيق عـلـى مـسـتـوى مـنـطـقـة مـعـيـنة فـيـ OSPF:
 - router ospf <process-id>
 - area <area-id> authentication
-

8. تحديد المنطقة (Area):

- لـ OSPF إـلـى مـنـطـقـة مـعـيـنة فـيـ (Interface) لـ تعـيـينـ كلـ وـاجـهـةـ:
 - interface <name>
 - ip ospf <process-id> area <area-id>
-

9. على واجهة OSPF تغيير تكلفة الـ (Cost):

لواجهة معينة للتحكم في اختيار الطريق. التكلفة الأقل تعني أفضليّة أكبر (Cost) ممكّن تعين تكلفة:

- `interface <name>`
 - `ip ospf cost <number>`
-

10. إعلان Default Route في OSPF:

(طريق افتراضي) داخل الشبكة اللي يستخدم Default Route لجعل الرووتر يعلن OSPF:

- `router ospf <process-id>`
 - `default-information originate`
-

1. على واجهة IPv6 تعين عنوان:

```
interface <name>
ipv6 address <IPv6-address>/<prefix-length>
```

مثال:

```
interface GigabitEthernet0/0
ipv6 address 2001:db8::1/64
```

- لكل واجهة IPv6 مع البادئة IPv6 بنحدد عنوان **شرح** prefix length.
 - **الترويت**:
 - تأكّد أن الواجهة Up no shutdown.
 - تتحقّق من عدم وجود تضارب في العناوين.
 - لمراجعة العنوانين استخدم أمر `show ipv6 interface brief`.
-

2. إضافة Static Route IPv6:

```
ipv6 route <destination-network>/<prefix-length> <next-hop-address>
```

مثال:

```
ipv6 route 2001:db8:1::/64 2001:db8::2
```

- نوجه الباكيجات الموجّهة لشبكة معينة عبر الرووتر التالي **شرح** (next-hop).
 - **الترويت**:
 - متاح ويمكن الوصول إليه next-hop تأكّد من أنّ عنوان (Ping).
 - متتضاربة بأولويّات أعلى routes تأكّد من عدم وجود.
 - راجع جدول التوجيه بأمر `show ipv6 route`.
-

3. تفعيل RIP لـ IPv6:

```
ipv6 unicast-routing
ipv6 router rip <name>
interface <name>
ipv6 rip <name> enable
```

مثال:

```
ipv6 unicast-routing
ipv6 router rip MyRIP
interface GigabitEthernet0/0
ipv6 rip MyRIP enable
```

ونعرفه على الواجهات المطلوبة لـ RIP ببن فعل بروتوكول: شرح.

• الترويت:

- تتحقق من حالة الواجهات باستخدام `show ipv6 interface`.
- مفعل على جميع الواجهات المشاركة RIP تأكيد أن.
- راجع جدول التوجيه `show ipv6 route rip`.
- الحياة RIP لمراقبة عمليات استخدم `debug ipv6 rip events`.

4. تفعيل OSPF لـ IPv6:

```
interface <name>
ipv6 ospf <process-id> area <area-number>
```

مثال:

```
interface GigabitEthernet0/0
ipv6 ospf 1 area 0
```

• على الواجهة مع تحديد المعرف والمنطقة (IPv6 الإصدار الخاص بـ OSPFv3) تفعيل: شرح.

• الترويت:

- تأكيد من Router ID باستخدام `show ipv6 ospf`.
- تتحقق من جيران OSPF `show ipv6 ospf neighbor`.
- صحيح راجع حالة الواجهات ووجود cost.
- لمتابعة الأحداث استخدم `debug ipv6 ospf events`.

5. أمر اختبار الاتصال مع تحديد المصدر (Ping IPv6):

```
ping <destination-ipv6-address> source <source-interface>
```

مثال:

```
ping 2001:db8::2 source GigabitEthernet0/0
```

- مع اختيار واجهة المصدر IPv6 اختبار الوصول لعنوان شرح:
 - الترويت
 - تأكد من أن واجهة المصدر Up.
 - تحقق من جداول التوجيه (routing tables).
 - لمعرفة مسار البالكيجات traceroute استخدم.
-

6. أوامر فحص مهمة:

- عرض جدول ARP (ARP لـ IPv4):

```
show arp
```

- عرض جيران IPv6:

```
show ipv6 neighbors
```

- الترويت
 - استخدم هذه الأوامر للتأكد من تعيين العناوين الفيزيائية بشكل صحيح.
 - للتأكد من أن الرووتر قادر على التواصل على الشبكة IPv6 تحقق من جيران.
-

✓ 6. أوامر فحص مهمة: أوّلاً: شرح أساسيات Cisco على أجهزة DHCP

1. Lease Time

- (1) هي يوم واحد (Lease Time) معناها مدة صلاحية الإيجار → lease 1 → 1 day.
 - (يعني 1 يوم و 0 ساعة و 0 دقيقة) في Cisco: lease 1 0 0 أو lease 1 0 أو.
 - مثلاً، يمكن تختلف الواجهة لكن المفهوم هو نفسه 8 في Windows.
-

2. Static IPs

- الأجهزة المهمة زي:
 - السيرفرات
 - الطابعات
 - الرووترات

الفايروول

- مش من DHCP. ثابت IP لازم يكون ليها

✓ ثانية: تكوين Cisco على راوتر DHCP

```
ip dhcp pool POOL_NAME
network 192.168.1.0 255.255.255.0
domain-name yourdomain.local
dns-server 8.8.8.8 1.1.1.1
netbios-name-server 192.168.1.10
default-router 192.168.1.1
lease 1
```

شرح الأوامر:

- ip dhcp pool POOL_NAME: إنشاء Pool جديد.
- network: تحدد الشبكة التي هيطلع منها IPs.
- domain-name: اسم الدومين.
- dns-server: ممكن تحط لحد 8 خوادم DNS.
- netbios-name-server: لو فيه WINS server.
- default-router: هو الـ Gateway.
- lease 1: مدة الإيجار يوم واحد.

✓ ثالثاً: إظهار العملاء اللي حصلوا على IP

```
show ip dhcp binding
```

- من الـ IP يعرض جدول بكل العملاء اللي حصلوا على DHCP.

✓ رابعاً: إعداد DHCP Client على راوتر من IP يأخذ (Client) DHCP Server.

```
interface GigabitEthernet0/1
ip address dhcp
no shutdown
```

- IP من DHCP Client ، ويأخذ Client (Client) DHCP Server.

خامسًا: تجديد أو تحرير عنوان IP في Windows

ipconfig /release ← يحرر عنوان IP
ipconfig /renew ← جديد من DHCP يطلب عنوان IP

سادسًا: حجز لعميل معين باستخدام MAC Address

* الفكرة:

- ثابت من IP بعض الأجهزة زي الطابعات أو الكاميرات لازم تأخذ DHCP.
- معين IP علشان نحجز بنسخدم MAC Address.

الخطوات:

1. إلى تنسيق MAC Address تحويل الـ

- لو الماك مثلاً A1:B2:C3:D4:E5:F6
- ده يمثل (في البداية 01) بنصيف Cisco في Ethernet
- أو بصيغة بدون نقاط ← 01.00.A1B2.C3D4.E5F6 : النتيجة تكون 01A1B2C3D4E5F6

2. خاصة بالعميل Pool تكوين:

```
ip dhcp pool Printer1
host 192.168.1.100 255.255.255.0
client-identifier 01A1B2C3D4E5F6
default-router 192.168.1.1
```

شرح:

- host: المحوز IP هو الـ.
- client-identifier: مع 01 في البداية HEX بعد تحويله لصيغة MAC Address هو.
- default-router: التي هيتبعت مع الـ IP. التي هيتبعت مع الـ IP.

ملخص كامل (مرتب)

العنصر	الوصف
ip dhcp pool	لإنشاء مجموعة توزيع DHCP
network	تحدد شبكة التوزيع
default-router	الجيتوائي
dns-server	خوادم DNS حتى 8
domain-name	اسم الدومن
netbios-name-server	لو مطلوب WINS Server
lease	مدة الإيجار باليوم

<code>show ip dhcp binding</code>	يعرض الأجهزة التي حصلت على IP
<code>ip address dhcp</code>	يجعل الواجهة تأخذ IP ك Client
<code>ipconfig /release</code>	من الجهاز IP تحرير
<code>ipconfig /renew</code>	جديد من الجهاز IP طلب
<code>client-identifier</code>	مسبق بـ MAC Address بصيغة HEX 001

✓ أوامر DHCP في IPv4 (Cisco) أولاً

1. عرض الأجهزة التي أخذت IP (IP Bindings)

`show ip dhcp binding`

- يعرض قائمة بالأجهزة التي حصلت على IP من DHCP Server.
-

2. عرض تفاصيل DHCP Pool

`show ip dhcp pool`

- يعرض عدد العناوين المستخدمة، وعدد العناوين المتاحة، وغيرها من معلومات DHCP pool.
-

3. (تصفير العناوين المُعطاة) DHCP Binding مسح/حذف

`clear ip dhcp binding *`

- (أي يعيد توزيع العناوين من جديد عند الطلب) bindings يمسح جميع الـ.

أو لمسح عنوان معين:

`clear ip dhcp binding 192.168.1.10`

4. تفعيل رسائل debug لتبني التصحيح DHCP

`debug ip dhcp server packet`

- DHCP يستخدم لتصحيح المشاكل ومعرفة ما إذا كانت رسائل تعمل بشكل صحيح (DISCOVER, OFFER, REQUEST, ACK).

ثانياً: DHCP في IPv6

1. على الراوتر DHCPv6 تمكين (Client Side)

على واجهة جهاز عميل (client interface):

```
interface GigabitEthernet0/1  
  ipv6 address autoconfig
```

- تلقائياً باستخدام IPv6 هذا الأمر يجعل الجهاز يحصل على عنوان SLAAC (Stateless Address Autoconfiguration).
- فتحتاج إلى إعداد (مثل DHCPv4 تماماً) إذا كنت تستخدم DHCPv6 stateful، DHCP server + relay.

ملخص الأوامر (مرتب)

الأمر	الوظيفة
show ip dhcp binding	عرض الأجهزة التي حصلت على IP
clear ip dhcp binding *	مسح كل DHCP bindings
show ip dhcp pool	عرض تفاصيل DHCP Pool
debug ip dhcp server packet	تتبع رسائل DHCP
ipv6 address autoconfig	IPv6 SLAAC أو DHCPv6 client تمكين

ملاحظات سريعة:

- الحجز الثابت يتم عبر IPv4 في حالة client-identifier.
- هناك طريقتين IPv6 في حالة:
 - SLAAC: DHCP Server بدون.
 - DHCPv6: يعمل بطريقة تشبه DHCPv4.

أولاً: ما هي الـ Access List?

داخل أو خارج جهاز (traffic) بتحكم في حركة البيانات (rules) هي مجموعة من القواعد (ACL) التي تحكم (Zi) الراوتر أو السوينتش.

الهدف منها:

- معين أو شبكة معينة IP السماح أو المنع لـ.
- تستخدم في الفاير وول، الفلترة، التحكم في الوصول، و NAT.

أنواع الـ Access List:

النوع	الاستخدام	الرقم
Standard	المصدر فقط IP تتحكم حسب	1–99 / 1300–1999
Extended	المصدر + الوجهة + البروتوكول + الپورت IP تتحكم حسب	100–199 / 2000–2699
Named	ACL باسم بدل رقم	ip access-list باستخدام
IPv6 ACL	ACL خاصة بـ IPv6	باسم فقط

تركيب أمر Access List

1. Standard ACL

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

- 10 = رقم الـ ACL
- permit = سماح
- 192.168.1.0 = الشبكة
- 0.0.0.255 = Wildcard mask (عكس بتات العMasque de sous-réseau)

2. Extended ACL

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
```

- من الشبكة دي لأي وجهة HTTP (port 80) يسمح بtrafik.

تطبيق الـ ACL على الواجهة (interface)

: لازم تطبقها على واجهة الرواتر ACL بعد ما تعمل

```
interface GigabitEthernet0/0
  ip access-group 10 in
```

- 10 = رقم الـ ACL.
- in = الترافيك الداخل للواجهة.
- out = الترافيك الخارج من الواجهة.

أمثلة عملية (مع التعديلات المطلوبة منك)

مثال 1: منع دخول الأجهزة من شبكة 192.168.10.0

```
access-list 15 deny 192.168.10.0 0.0.0.255
access-list 15 permit any

interface GigabitEthernet0/0
 ip access-group 15 in
```

ومنع أي بورت ثاني (HTTP) مثال 2: السماح فقط بالبورت 80

```
access-list 110 permit tcp any any eq 80
access-list 110 deny ip any any

interface GigabitEthernet0/0
 ip access-group 110 in
```

مثال 3 بورت Telnet (23) باسم لمنع ACL

```
ip access-list extended BLOCK_TELNET
 deny tcp any any eq 23
 permit ip any any

interface GigabitEthernet0/1
 ip access-group BLOCK_TELNET in
```

ملاحظات مهمة:

- ، هيتمكن كل حاجة permit يعني لو نسيت) غير مرئية all deny تنتهي تلقائياً بـ كل ACL.
- لعرض القواعد show access-lists.
- استخدم no access-list [number] لمسح ACL.

Subnet Mask	Wildcard Mask
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255
255.0.0.0	0.255.255.255
Host only (one IP)	0.0.0.0

● أولاً: ما هو NAT؟

NAT = Network Address Translation

، والعكس. تُستخدم عادةً للسماح (Public) إلى شبكة عامة (Private) هي تقنية تُستخدم لترجمة العنوانين من شبكة خاصة واحد أو أكثر Public IP لأجهزة داخلية باستخدام الإنترنت من خلال عنوان.

◆ (لا يتم استخدامها مباشرة في الإنترن特) **Private IP** نطاقات الـ:

الفئة	النطاق	الملاحظات
A	10.0.0.0/8	
B	172.16.0.0 – 172.31.255.255	
C	192.168.0.0/16	

✓ أنواع NAT:

1. Static NAT (ثابت)

- لكل IP خارجي (Public) يوجد IP داخلي (Private).
- مفيد للسيرفرات داخل الشبكة التي تحتاج أن تصل إليها الأجهزة من الإنترن特.

✓ الأمر:

```
ip nat inside source static [Private_IP] [Public_IP]
```

✓ تطبيق على الواجهات:

```
interface G0/0
 ip nat inside

interface G0/1
 ip nat outside
```

✓ مثال كامل:

```
ip nat inside source static 192.168.1.10 203.0.113.5

interface G0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
```

```
interface G0/1
ip address 203.0.113.1 255.255.255.0
ip nat outside
```

2 Dynamic NAT

- خارجية IPs داخليين يستخدمو مجموعة IP عدة.
- ، الباقي لا يترجم إذا خلصت عناوين الـ Public.

الخطوات:

1. من العناوين العامة Pool إنشاء:

```
ip nat pool MYPOOL 203.0.113.10 203.0.113.20 netmask 255.255.255.0
```

2. تحديد من يسمح له باستخدام الـ NAT:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

3. ربط الـ Access List بالـ Pool:

```
ip nat inside source list 1 pool MYPOOL
```

4. تحديد الواجهات:

```
interface G0/0
ip nat inside
```

```
interface G0/1
ip nat outside
```

3 PAT (Port Address Translation) أو NAT Overload

- الأكثر شيوعاً في الشبكات المنزلية.
- العام، ولكن تفرق حسب البروتوكول IP جميع الأجهزة تستخدم نفس.

الخطوات:

1. تحديد Access List:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

2. ربط الـ Access List بالـ Interface (الـ IP Public) الذي فيها العناوين العامة:

```
ip nat inside source list 1 interface G0/1 overload
```

3. تحديد الواجهات:

```
interface G0/0
 ip nat inside
```

```
interface G0/1
 ip nat outside
```

✓ ملاحظات عن PAT:

- يعمل عن طريق تغيير رقم الپورت من نطاق 49152 - 65535 (ephemeral/dynamic ports)
- مختلف Socket (جلاة اتصال) بقى لها كل Session
- IP + Port → Public IP + Random Port

✓ أوامر المراجعة والمتابعة:

الأمر	الوظيفة
show ip nat translations	عرض الجلسات المترجمة
show ip nat statistics	إحصائيات الترجمة
clear ip nat translation *	مسح كل الترجمة

📌 مثال مختصر لاستخدام PAT:

```
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface G0/1 overload
interface G0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
interface G0/1
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
```

✓ ملخص سريع:

النوع	الداخلي IP عدد	الخارجي IP عدد	ملاحظات
Static NAT	1	1	خارجي خاص IP لكل جهاز
Dynamic NAT	مجموعة	مجموعة	عام دائم IP يحتاج توافر
PAT	مجموعة	1	يعتمد على الپورتات (أكثر استخداماً)

■ أولاً: الفرق بين Switch و Bridge

العنصر	Switch	Bridge
الأداء	أسرع	أبطأ
المعالجة	(مخصص لتبديل البيانات) ASIC chip يستخدم	يستخدم CPU
عدد المنافذ	يحتوي على عدة منافذ (ممكن 24 أو 48)	غالباً يحتوي على منفذين أو ثلاثة
الجدول	MAC Address Table	Bridge Table
الكافأة	أكثـر كفـاءة في الشـبـكات الكـبـيرـة	أقل كفـاءة

■ مفاهيم الشبكات في Layer 2:

- **Broadcast Domain:**

كل الأجهزة التي تستقبل broadcast.

مستقل broadcast domain في السويفتش: كل VLAN تعتبر broadcast domain.
يتم فصل broadcast domains باستخدام router أو Layer 3 switch.

- **Collision Domain:**

منفصل collision domain هو interface كل منفذ في السويفتش.

، كل الأجهزة تكون في نفس hub بينما في collision domain.

■ أوامر مهمة لمراقبة السويفتش:

- ◆ عرض حالة المنافذ:

```
show interface status
```

- ◆ عرض جدول MAC Address:

```
show mac address-table
```

- ◆ عرض محتويات جدول MAC Address:

```
show mac address-table dynamic
```

أوامر التحكم في MAC Address Table

- ◆ ثابت MAC إضافة:

```
mac address-table static [MAC] vlan [VLAN-ID] interface [INTERFACE]
```

- ◆ كامل مسح جدول MAC:

```
clear mac address-table
```

- ◆ معين مسح MAC:

```
clear mac address-table dynamic address [MAC]
```

- ◆ مسح حسب الانترفيس:

```
clear mac address-table dynamic interface [INTERFACE]
```

Password Recovery على Switch

- ◆ خطوات استعادة كلمة السر على سويتش Cisco:

أعد تشغيل السويتش.

- في السويتش (يكون بجواره) **Mode** أثناء الإقلاع، اضغط على زر **Reset**.
- ، أدخل الأوامر التالية **CLI** في:

flash_init	تهيئة الفلاش ←
load_helper	تحميل أدوات المساعدة ←
dir flash:	عرض محتويات الفلاش ←
rename flash:config.text flash:config.old	إعادة تسمية ملف ←
boot	إعادة تشغيل السويتش ←

(أي بدون إعدادات قديمة) الآن السويتش سيقلع بدون ملف config.text.

- بعد الدخول إلى وضع **privileged exec mode**:

```
copy flash:config.old system:running-config
```

كده رجعت الإعدادات من غير إعادة تشغيل، وتقدر تعدل كلمة السر.

- أدخل إلى إعدادات الـ **console**:

```
configure terminal  
line console 0  
password NEWPASSWORD
```

```
login  
end  
write memory      لحفظ التغييرات
```

أخيراً، يمكن ترجيع اسم الملف 6:

```
rename flash:config.old flash:config.text
```

ملحوظة عن الملفات:

اسم الملف في الفلاش الجهاز

Switch config.text

Router startup-config

✓ مراجعة أوامر MAC:

الغرض	الأمر
عرض الجدول	show mac address-table
ثابت MAC إضافة	mac address-table static [mac] vlan [id] interface [int]
مسح الجدول كله	clear mac address-table
معين MAC مسح عنوان	clear mac address-table dynamic address [mac]
مسح حسب منفذ معين	clear mac address-table dynamic interface [int]

VLAN و Trunking و DTP و VLAN Hopping و Voice VLAN و VLAN تمام، هشرح لك كل المواضيع اللي ذكرتها عن STP و مفصل و منظم و سهل الحفظ ✓

VLAN (Virtual LAN)

✓ أوامر مهمة:

- الحالية عرض VLANs:
- show vlan brief
- إنشاء مدى من VLANs:
- vlan 4-9
- إنشاء VLANs غير متتابعة:
- vlan 4,9
- ربط مجموعة من المنافذ بـ VLAN:
- interface range fastEthernet 0/1 - 5
- switchport mode access

- switchport access vlan 10
 - تحديد منفذ مخالفة
 - interface range f0/1, f0/3, f0/5
-

حذف إعدادات VLAN

- حذف الإعدادات القديمة:
 - erase startup-config
 - reload
 - حذف ملف VLAN:
 - delete flash:vlan.dat
 - عرض الملفات على الفلاش:
 - dir flash:
 - more flash:vlan.dat
-

Trunking (متعددة VLANs نقل بيانات)

إعداد منفذ Trunk:

```
interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
```

المسموح بها تحديد VLANs:

```
switchport trunk allowed vlan 10,20
```

عرض معلومات Trunk:

```
show interfaces trunk
```

عرض وضع المنفذ:

```
show interfaces switchport
```

DTP – Dynamic Trunking Protocol

- تلقائيا Access أو Trunk بروتوكول يحدد إذا كان المنفذ هيستغل (لأمان الشبكة):

```
interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
switchport nonegotiate
```

nonegotiate: يمنع إرسال أو استقبال DTP.

⚠ VLAN Hopping (هجمات الشبكة)

1. VLAN Spoofing

- حتى يدخل لكل Trunk المهاجم يحاول جعل الكابل VLAN.
 - فقط إجبار المنفذ يكون: **Access**:
 - interface f0/1
 - switchport mode access
-

2. Double Tagging

- بدون أن يكون المنفذ VLAN للغريم لاختراق **Tags** المهاجم يضيف 2:
 - لا يوجد حل مباشر على المنفذ، لكن: **الحل**:
 - فقط استخدم **Access mode**.
 - على VLAN 1 هي default لا تجعل Trunk.
-

🎙 Voice VLAN (VoIP)

- Voice VLAN بجانب Data VLAN:

```
interface f0/2
switchport mode access
switchport access vlan 10
switchport voice vlan 20
```

🌲 STP – Spanning Tree Protocol

✓ الغرض:

- في الشبكة loops منع الـ
- ويحجب المسارات الزائدة **Root Bridge** يختار

💡 أوامر STP:

- كامل STP عرض:
 - show spanning-tree
 - عرض STP لـ VLAN معينة:
 - show spanning-tree vlan 10
-

إعداد STP:

- تحديد Root Bridge:
- spanning-tree vlan 10 root primary
- تحديد Root احتياطي:
- spanning-tree vlan 10 root secondary
- كلما زاد احتمال أن يكون (Root):
• spanning-tree vlan 10 priority 24576

القيم تكون مضاعفات 4096:
0, 4096, 8192, ... 61440.

▶ STP PortFast (تسريع الاتصال على منافذ المستخدمين)

- يستخدم في المنافذ المتصلة بأجهزة وليس بسوبرنات
 - interface f0/5
 - switchport mode access
 - spanning-tree portfast
-

◀ عرض حالة المنافذ:

show interface status

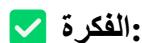
✓ ملخص سريع:

الغرض	الأمر
عرض VLANs	show vlan brief
ربط منافذ بـ VLAN	interface range ... + switchport access vlan
إعداد Trunk	switchport mode trunk + encapsulation dot1q
منع DTP	switchport nonegotiate
عرض Trunk	show interfaces trunk

عرض وضع منفذ	show interfaces switchport
تفعيل Voice VLAN	switchport voice vlan <vlan>
عرض STP	show spanning-tree vlan <id>
تعيين Root Bridge	spanning-tree vlan <id> root primary
تفعيل PortFast لمنافذ PCs	spanning-tree portfast + switchport mode access



أولاً: DHCP Attack – هجوم DHCP Spoofing



على الضحايا، فيخدعهم ويحول التрафيك عليه مزيف ويوزع DHCP Server المهاجم يعمل جهازه كأنه.



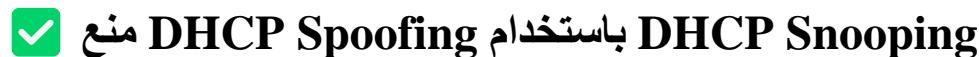
DORA Process (الحصول على IP من DHCP)

الخطوة	من	إلى	النوع	الشرح
D	PC	Broadcast	Discover	الجهاز يبحث عن DHCP server
O	DHCP Server	Unicast	Offer	المقترن للجهاز IP السيرفر يرد بعنوان
R	PC	Unicast	Request	من السيرفر IP الجهاز يطلب
A	DHCP Server	Unicast	Ack	للجهاز IP السيرفر يؤكّد ويخصص الـ



أوامر مهمة:

- عرض الأجهزة التي أخذت IP:
- show ip dhcp binding
- عرض معلومات الـ DHCP Pools:
- show ip dhcp pool
- ، لكن المحتمل تقصد لا يوجد أمر اسمه (خطأ كتابي عنك) shoooping
 - (الأجهزة الموثوقة) عرض DHCP snooping bindings
 - show ip dhcp snooping binding



منع DHCP Spoofing باستخدام DHCP Snooping

خطوات التفعيل على السويفت:

- تفعيل DHCP Snooping:
- ip dhcp snooping
- معينة VLAN تفعيله على:
- ip dhcp snooping vlan 10

- تحديد منفذ موثوق (الموصل بالسيرفر الحقيقي)**
5. interface f0/1
 6. ip dhcp snooping trust
 7. ip arp inspection trust
 8. **المنفذ اللي موصل بالأجهزة يكون غير موثوق (افتراضياً)**
- يعتبر غير موثوق لأن أي منفذ غير معروف بـ untrust لا تحتاج كتابة
-

⚠ ثانياً: ARP Attack (مثل ARP Spoofing / Poisoning)



مزيف في الشبكة ويدعو الأجهزة الأخرى لتحولوا الترافيك إليه ARP المهاجم يرسل رد



الحماية باستخدام Dynamic ARP Inspection (DAI)

تفعيل DAI على VLAN:

```
ip arp inspection vlan 10
```

منفذ موثوق (مثل الموصل بالراوتر)

```
interface f0/1  
ip arp inspection trust
```



(على السويتش إضافة Static Binding MAC + IP ربط)

يدوياً IP + MAC:

```
1. ip source binding 0011.2233.4455 vlan 10 192.168.1.10 interface f0/10
```

اللي انت عرّفته MAC/IP ده بيخلify السويتش يصدق بس الترافيك الجاي من



ACL بديل باستخدام:

إنشاء ARP Access List:

```
1. arp access-list arpcheck  
2. permit ip 192.168.1.10 0.0.0.0 mac 0011.2233.4455 0000.0000.0000
```

4. معينة VLAN → ACL ربط الـ:

5. ip arp inspection filter arpcheck vlan 10



أوامر فحص ومتابعة:

- عرض ARP inspection bindings:
 - show ip arp inspection
 - show ip arp inspection vlan 10
 - عرض DHCP snooping bindings:
 - show ip dhcp snooping binding
 - عرض ARP ACLs:
 - show arp access-list
-



ملخص سريع للأوامر حسب الوظيفة:

الوظيفة	الأمر
تفعيل DHCP Snooping	ip dhcp snooping
معينة VLAN تفعيله على	ip dhcp snooping vlan 10
جعل منفذ موثوق	ip dhcp snooping trust
عرض الأجهزة التي أخذت IP	show ip dhcp binding
عرض السيرفرات الموثوقة	show ip dhcp snooping binding
Dai على VLAN تفعيل	ip arp inspection vlan 10
جعل منفذ موثوق في ARP	ip arp inspection trust
يدوياً IP + MAC ربط	ip source binding <mac> vlan <id> <ip> int <name>
ACL لحماية ARP	arp access-list + ip arp inspection filter



ما هو DHCP Spoofing؟

على جهازه ويدي DHCP server من أكثر من مصدر، غالباً المهاجم يشغل IP addresses هو هجوم يتم فيه توزيع مزيفة للأجهزة عشان يوجه الترافيك من خلالها IPs.



الحل: DHCP Snooping

عن طريق DHCP spoofing هي ميزة في السوينتش بتحمي الشبكة من:

- من المنافذ غير الموثوقة منع DHCP replies.

- زي اللي واصل فيها الـ real DHCP server).
-

على السويفت (مصنفة واضحة) أوامر تفعيل DHCP Snooping :

1. عالمياً تفعيل DHCP Snooping :

```
ip dhcp snooping
```

2. معينة VLAN تفعيل DHCP Snooping على VLAN :

```
ip dhcp snooping vlan 10
```

حسب شبكة VLAN غير رقم الـ

3. تفعيل خيار المعلومات (Option 82):

```
ip dhcp snooping information option
```

يساعد السيرفر إنه يعرف البورت اللي جاي منه الطلب (بيفيد في الحماية والتحقيقات)

4. تحديد المنفذ الموثوق (اللي متوصّل بالسيرفر) :

```
interface f0/1  
ip dhcp snooping trust
```

ما تكتبش فيها (زي أجهزة الموظفين) كل المنافذ اللي فيها **trust**.

5. المسموح بها في الثانية DHCP تحديد عدد باكيتات :

```
interface f0/10  
ip dhcp snooping limit rate 3
```

بيتم إرسال تقريرياً 3 رسائل، فـ "3" هو رقم معقول DORA لأنه في عملية

أوامر فحص مهمة:

الامر	الشرح
<code>show ip dhcp snooping</code>	يعرض حالة DHCP snooping
<code>show ip dhcp snooping binding</code>	بنائهم MAC وعنوان IP يعرض قائمة الأجهزة اللي أخذت

تصحيح بعض الأخطاء الإملائية في أوامرك:

الخطأ	التصحيح
<code>ip dhcp shooping</code>	<code>ip dhcp snooping</code>
<code>trusyrt port</code>	<code>trust port</code> أو <code>الأفضل تكتب ip dhcp snooping trust</code>
<code>backet</code>	<code>packet</code>
<code>shooping</code>	<code>snooping</code>



ملاحظات إضافية:

- **DHCP snooping** من النوع **L2 managed**. يشتغل فقط على **Switches**.
- الحقيقي عشان توصله على منفذ "موثوق" DHCP ضروري تكون عارف مكانه".
- ممكن تكون مفيدة جداً في تتبع مصدر الطلب option 82 المعلومات اللي بتضاف عن طريق

نظام 

بالكامل من الصفر، خطوة بخطوة، مع كل الأوامر المهمة وأمثلة توضيحية **Port Security** خليني أشرح لك.



ما هو Port Security؟

Port Security هي ميزة في سوينتشات سيسكو (Layer 2 Switches) ببساطة:

- اللي تقدر توصل على كل منفذ (MAC addresses) تحدد عدد الأجهزة.
- تمنع أي جهاز غير معروف من الاتصال بالشبكة.
- تقدر تخافر رد الفعل لما يحصل خرق أمني.

متى نستخدم Port Security؟

في الشبكات الداخلية (مثل شركات أو مدارس) لما تحب تمنع موظف مثلاً من توصيل جهاز شخصي أو تمنع اختراق داخلي عن طريق جهاز خارجي.

الشروط:

- البورت لازم يكون في وضع Access mode.
 - Port Security مش بيشغل على Trunk ports (إلا في حالات خاصة جداً).
-

خطوات الإعداد والأوامر:

1. ادخل على الواجهة (Interface):

```
interface FastEthernet0/1
```

2. خلي البورت في وضع Access:

```
switchport mode access
```

3. فعّل Port Security:

```
switchport port-security
```

4. حدد عدد الماك أدریس المسموح به:

```
switchport port-security maximum 1
```

يسمح فقط لجهاز واحد بالاتصال على البورت.

5. طريقة تسجيل الماك أدریس:

✓ بيدوياً

switchport port-security mac-address 0011.2233.4455

✓ (Sticky) تلقائياً:

switchport port-security mac-address sticky

السويتش يسجل أول جهاز يتصل تلقائياً.

ثالثاً: Errdisable & Recovery

✓ ما هو Errdisable؟

هو وضع يتم فيه تعطيل البورت تلقائياً بسبب مخالفة مثل port security, bpdu guard, etc.

📌 أوامر تفعيل الاسترجاع التلقائي للبورتات:

bash	
CopyEdit	
errdisable recovery interval 30	← الوقت بالثوانى قبل
محاولة الاسترجاع	
errdisable recovery cause psecure-violation	← تفعيل الاسترجاع في
حالة Port Security Violation	

📋 أوامر المراقبة:

الأمر	الوظيفة
show errdisable recovery	يعرض الوقت المتبقى لاسترجاع البورتات
show interfaces status err-disabled	يعرض البورتات الموجودة في حالة errdisable

6. حدّ طريقة التعامل مع الاختراق (violation):

switchport port-security violation shutdown	افتراضي، يقفل البورت ←
switchport port-security violation restrict Log	يمنع الجهاز الغريب ويظهر ←
switchport port-security violation protect Logs	يمنع الجهاز الغريب بدون ←



أوامر العرض والمراقبة:

عرض معلومات البورت:

```
show port-security interface f0/1
```

عرض كل الماك أدريس المرتبطة بالبورتات:

```
show port-security address
```

عرض حالة البورتات كلها:

```
show port-security
```



في حالة حدوث Violation:

لو البورت دخل حالة err-disabled:

```
interface f0/1
shutdown
no shutdown
```



حذف الماك أدريس المسجلة تلقائياً:

```
clear port-security sticky interface f0/1
```



مثال تطبيقي كامل:

```
interface fastethernet0/10
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
```



ملاحظات:

المعلومة	الترضيب
Sticky MAC	يُسجل الماك ويُخزن في running-config

Trunk	إلا في سيناريوهات معينة Port Security ما يشتغلش عليه
Shutdown	أقوى وضع من ناحية الأمان لكنه يحتاج تدخل يدوي بعد أي اختراق

الهدف:

في الشبكة بحيث IP تشغيل تليفونات Cisco IP Phone (مثل) :

- تلقائي من IP تأخذ DHCP.
 - تسجل على الراوتر ك Call Manager Express (CME).
 - تتخصص لها أرقام داخلية (extensions).
-

المفاهيم الأساسية:

المكون	وظيفته
DHCP Pool	يوزع IPs على التليفونات.
Option 150 / 43	عنوان الراوتر IP Phone (CME) عشان تسجل عليه يعرف الـ.
Voice VLAN	فصل صوت التليفونات عن باقي الشبكة.
Telephony Service	على الراوتر Call Manager Express تفعيل خاصية الـ.
ephone / ephone-dn	تعريف الهاتف والرقم المخصص ليه.

الخطوات بالتفصيل:

❶ إعداد DHCP لـ IP Phones (على الراوتر أو السيرفر)

```
ip dhcp pool IP-PHONES
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.1
  option 150 ip 10.10.10.1      ← (CME) دا عنوان الراوتر
```

عادة نفس عنوان الراوتر CME اللي هو TFTP Server ده أهم حاجة، بيدي التليفون عنوان 150 (CME).

❷ إعداد خدمة الاتصال (CME) على الراوتر

```
telephony-service
  max-dn 10          ← عدد الأرقام اللي ممكن توزع
```

```
max-ephones 10          ← عدد التليفونات اللي ممكن تسجل
ip source-address 10.10.10.1 port 2000 ← CME + بروتوكول SCCP
auto assign 1 to 10      ← أوامر لتوزيع الأرقام تلقائياً
auto assign 1 to 10
exit
```

- بيفصل العنوان اللي التليفونات هتنواصل عليه ip source-address الأمر.
-

✳ 3. تعريف رقم لكل هاتف (Directory Number)

```
ephone-dn 1
number 1001
name Admin
```

هو الرقم الداخلي اللي بيتحصص لل்தليفون ephone-dn.

✳ 4. تعريف الهاتف نفسه وربطه بالرقم

```
ephone 1
mac-address 0011.2233.4455
type 7960
button 1:1
```

- الخاص بال்தليفون عشان يتسجل MAC Address لازم نكتب.
-

✳ 5. إعداد السويفت لتوصيل IP Phones

```
interface range fastethernet0/1 - 10
switchport mode access
switchport access vlan 10           ← مخصصة لل்தليفونات
switchport voice vlan 20           ← VLAN
spanning-tree portfast
                                         ← لأجهزة الكمبيوتر VLAN
```

- التليفون فيه مدخلين: واحد داخلي للكمبيوتر وواحد للاتصال بالشبكة.
 بيفصل الصوت عن الداتا Voice VLAN بـ.
-

أوامر مفيدة:

الأمر	الوظيفة
show telephony-service ephone	يعرض الأجهزة المسجلة على الرواتر
show ephone registered	يعرض التليفونات المتصلة
debug ephone	لمراقبة التسجيل ومشاكل الاتصال
show ip dhcp binding	يشوف الأجهزة اللي خدت IP

شكل بسيط للإعدادات كلها (ملخص)

```
ip dhcp pool VOICE
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  option 150 ip 192.168.10.1

telephony-service
  max-ephones 5
  max-dn 5
  ip source-address 192.168.10.1 port 2000
  auto assign 1 to 5
  exit

ephone-dn 1
  number 1010

ephone 1
  mac-address 00D0.BA98.7654
  type 7960
  button 1:1

interface range fa0/1 - 10
  switchport mode access
  switchport access vlan 10
  switchport voice vlan 20
  spanning-tree portfast
```

بالتفصيل وبشكل تمام، نبدأ نشرح كل حاجة مرتبطة بـ CDP و Port Security و Error Disable Recovery و منظم و سهل الفهم.

أولاً CDP (Cisco Discovery Protocol)

ما هو CDP؟

هو بروتوكول طبقة 2 من سيسكو يُستخدم لاكتشاف أجهزة سيسكو الأخرى المتصلة بالشبكة مباشرة (سواء كانت روتارات أو سوينتشات).

أهم أوامر CDP:

الأمر	الوظيفة
<code>show cdp neighbors</code>	يعرض الأجهزة المجاورة المتصلة بالسوينتش أو الروتر
<code>show cdp neighbors detail</code>	يعرض معلومات تفصيلية (IP, platform, interface)
<code>show cdp entry *</code>	يعرض كل الجيران المسجلين بالبروتوكول
<code>show cdp interface</code>	يوضح الواجهات المفعل عليها CDP
<code>show cdp traffic</code>	يعرض الإحصائيات الخاصة بحركة CDP
<code>no cdp run</code>	على الجهاز بالكامل CDP إغلاق
<code>no cdp enable</code>	على واجهة محددة CDP إغلاق

ما هو PoE؟

، وهي تقنية تتيح تمرير التيار الكهربائي مع البيانات عبر كابل الشبكة Power over Ethernet هي اختصار لـ (Ethernet cable) إلى الأجهزة الطرفية مثل:

- كاميرات المراقبة (IP Cameras)
 - الهواتف الشبكية (IP Phones)
 - نقاط الوصول اللاسلكية (Wireless Access Points)
 - أجهزة إنترنت الأشياء (IoT Devices)
-

كيف تعمل PoE؟

عن طريق PoE بشكل عام، يعمل:

- PoE أو Power Injector. إرسال البيانات + الطاقة عبر نفس الكابل من خلال سوينتش يدعم باستهلاك الطاقة لتشغيل نفسه دون الحاجة إلى مصدر طاقة خارجي (مثل IP Phone) يقوم الجهاز المستقبل.
-

أنواع أجهزة PoE

النوع	الوظيفة
PSE (Power Sourcing Equipment)	أو PoE هو الجهاز المرسل للطاقة، مثل سويتش Power Injector.
PD (Powered Device)	أو كاميرا IP Phone هو الجهاز الذي يستقبل الطاقة، مثل IP.



الرسمية PoE معايير

المعيار	الطاقة القصوى (لكل منفذ)	الاستخدام
IEEE 802.3af (PoE)	15.4W	- كاميرات خفيفة (أجهزة صغيرة IP Phone)
IEEE 802.3at (PoE+)	30W	أجهزة أكبر (بعض نقاط الوصول والكاميرات)
IEEE 802.3bt (PoE++ Type 3/4)	60W - 100W	قوية PTZ شاشات، لابتكارات، كاميرات



مميزات PoE

- يقلل من عدد الأسلام، لا حاجة لمصدر طاقة منفصل .
- تسهيل عملية التركيب في الأماكن التي لا تحتوي على فيش كهرباء .
- قطع الطاقة تلقائياً PSE حماية: في حالة زيادة الحمل، يقوم .
- توفير في التكاليف والصيانة .



أوامر فحص Cisco على سويتش PoE

show power inline يعرض حالة الطاقة على البورتات
show power inline interface fa0/1 يعرض تفاصيل الطاقة لبورت محدد



ملاحظة مهمة:

- أو **PoE**، لازم تتأكد إن السويتش عليه كلمة PoE مش كل السويتشات تدعم **PWR**.
- لو كانت تستهلك طاقة أكثر من 15.4W بعض الأجهزة ممكن تتطلب **PoE+**.

ما هو EtherChannel؟

EtherChannel هو تقنية من سيسكو تسمح بربط عدة منافذ (interfaces) لتعمل كأنها رابط واحد (logical link) بين جهازين (مثل سوينشين)، مما يوفر:

- زيادة في سرعة النقل (bandwidth)
- توفير حماية ضد فشل أحد الكواكب (redundancy)
- تقليل الضغط على STP (Spanning Tree Protocol)

خطوات تكوين EtherChannel

1. تحديد مجموعة المنافذ:

```
interface range fa0/1 - 4
```

2. حذف الإعدادات القديمة (اختياري لكن مهم):

```
default interface range fa0/1 - 4
```

3. إعداد المنافذ لل EtherChannel:

```
no switchport  
channel-group 1 mode active  
channel-group 1 mode desirable  
channel-group 1 mode on  
(تفاوض)
```

على البورت الوهمي IP إذا كنت تستخدم
← LACP (active/passive)
← PAgP (desirable/auto)
بدون بروتوكول ()

ملاحظة:

- mode active/passive** = مفتوح المصدر LACP بروتوكول
- mode auto/desirable** = خاص بسيسكو PAgP بروتوكول
- mode on** = تفعيل مباشر بدون بروتوكول

عرض حالة ال EtherChannel

```
show etherchannel summary
```

- يعرض الفتوات وأرقام البورات المشتركة فيها وحالتها

مثال للحالة:

الرمز	المعنى
P	منفذ مشارك بنجاح
I	غير متوافق (Incompatible)
D	لا يعمل

على القناة الافتراضية IP إعداد (Port-Channel)

بعد ما تنشئ القناة:

```
interface port-channel 1
ip address 192.168.1.1 255.255.255.0
no shutdown
```

التعامل مع أخطاء التكوين

لو حصل تضارب في الإعداد بين الطرفين، المنفذ ممكן تدخل في وضع err-disabled.

الحل:

```
errdisable recovery interval 30
errdisable recovery cause channel-misconfig
show errdisable recovery
```

استرجاع المنافذ للإعدادات الافتراضية

```
default interface range fa0/1 - 4
```

- هذا الأمر يحذف كل الإعدادات السابقة على المنفذ (IP – VLAN – EtherChannel – الخ).

ملاحظات هامة:

- يكون لهم نفس EtherChannel لازم كل البورتات في:
 - السرعة (speed)
 - الطور (duplex)
 - VLANs (لو سويفتش) الـ layer 2
- لو فيه اختلاف، مش هيستغل ويدخل وضع خطأ.

ما هو VTP؟

بينالسوبيتشات تلقائياً عبر الترانك. هذا يسهل VTP يستخدم لنقل وتوزيع معلومات الـ Cisco هو بروتوكول من VTP إداره الشبكة وتوزيع الـ VLANs.

أنواع الـ VTP Modes

Mode	Create/Delete/Modify VLANs	Synchronize VLANs	Forward VLAN Info	Store Location
Server	<input checked="" type="checkbox"/> نعم	<input checked="" type="checkbox"/> نعم	<input checked="" type="checkbox"/> نعم	Flash
Client	<input checked="" type="checkbox"/> لا	<input checked="" type="checkbox"/> نعم	<input checked="" type="checkbox"/> نعم	Flash
Transparent	<input checked="" type="checkbox"/> نعم (محلياً فقط)	<input checked="" type="checkbox"/> لا	<input checked="" type="checkbox"/> نعم	NVRAM

✓ ملاحظات هامة :

- **Server** هو المسؤول عن تحديث باقي الأجهزة.
- **Client** لا يمكنه تعديل أو إنشاء VLANs.
- **Transparent** يمرر المعلومات ويحتفظ بالـ VLANs لا يشارك في مزامنة VLANs.

إعدادات الأساسية VTP

```
vtp domain [domain-name]
vtp mode [server | client | transparent]
vtp version [1 | 2 | 3]
vtp password [password]
```

ملاحظات حول الإصدارات:

- **VTP Version 1 & 2** متوافقة سوياً.
- **VTP Version 3** غير متوافقة مع 1 و 2، ويجب أن تكون جميع السوبيتشات في الشبكة على 3.

أوامر متقدمة في VTPv3

```
vtp password [password] hidden
vtp mode off
vtp primary vlan
```

إخفاء الباسورد
على السوبيتش VTP إلغاء تفعيل
تحويل السوبيتش إلى Primary Server

ملاحظة:

- لا يمكنك إجراء تغييرات على السيرفر إلا إذا كان VTPv3 في Primary Server.
-

➡️ كيف يتم حذف إعدادات VTP؟

```
delete flash:vtp.dat  
vtp mode transparent  
reload
```

📋 أوامر العرض (Show Commands)

```
show vtp status  
show vtp password  
show vlan brief  
show vlan internal usage  
show interfaces trunk  
show interfaces pruning
```

✂️ VTP Pruning

✓ ما هو؟

VTP Pruning غير مستخدمة على السوينتشات الأخرى عبر الترانك broadcast/multicast في VLANs يمنع إرسال.

🔧 التفعيل:

```
vtp pruning
```

شرح:

- فقط VLAN 2 عليه B و 3، وسوينتش VLAN 2 عليه A لو سوينتش.
 - مش عليه B رغم إن B هيتبعد إلى VLAN 3 من broadcast كل: دون VTP Pruning.
 - هيتم منها تلقائياً VTP Pruning: باستخدام.
-

💡 تحديد VLANs مسموحة على Trunk:

```
interface [interface-name]  
switchport trunk allowed vlan [vlan-id or range]
```

محدد VTP على Interface تعطيل:

```
interface [interface-name]
no vtp
```

أهم الملاحظات العملية:

- هو من يرسل التحديث **Revision Number** السويفت الذي يحمل أعلى.
- قبل توصيل سويفت جديد في الشبكة **vtp.dat** لتجنب المشاكل، امسح.
- قبل التعديل **show vtp status** استخدم دائمًا أمر.

Redundancy Protocols

1. HSRP - Hot Standby Router Protocol

- فكرة البروتوكول:
يمثل البوابة الافتراضية (Virtual IP) وهي IP يدخلها مجموعة من الروابط تشارك للشبكة (Default Gateway).
- (هو الذي يستقبل ويرسل الباكيتات)، والروابط الثاني **Active Router** واحد يكون **Standby Listener** ، والباقي (وقع Active جاهز يأخذ مكانه لو ال).
- بيتم حسب اختيار ال **Active Router**:
 - الروابط الذي يبدأ يعلن أول في أول 10 ثواني.
 - افتراضي) أعلى Priority = 100).
 - أعلى IP ، الروابط الذي عنده Priority لو نفس ال.
- يأخذ مكانه فوراً وقع ال **Standby Active Router** لو ال.
- يعني يدخله يرجع عليه **Preempt** إلا لو فعلت خاصية **Active Router رجع ثاني مش هيقى** لو ال **Active Router** لو ال **Priority أعلى** لو **Priority أعلى**).

مهمة أوامر HSRP:

```
interface int-name
standby [group-number] ip [virtual-ip]
```

- المشتركة بين الروابط **Virtual IP** بتحدد ال.

```
show standby
show standby brief
```

- لعرض حالة البروتوكول.

```
standby [group-number] priority [number > 100]
standby [group-number] preempt
```

- لما يرجع شغال router عشان active preempt لتحديد الأولوية وفعّل.
-

لتعزيز الاعتمادية (مراقبة المسارات)

```
track [number] interface [int-name] line-protocol
interface [int-name]
standby [group-number] track [number] decrement [number]
```

- يأخذ مكان Priority عشان بتعمل مراقبة لواجهة معينة. لو وقعت، تقل stand-by active.
-

المصادقة Authentication:

```
standby [group-number] authentication md5 key-string [password]
standby [group-number] authentication md5 key-chain [keychain-name]
```

- من التلاعب لحماية الـ HSRP.
-

لإيقاف البروتوكول:

```
interface int-name
no standby [group-number]
```

2. VRRP - Virtual Router Redundancy Protocol

- لكن يختلف في HSRP شبيه جداً بالـ VRRP:
 - فيه ماستر واحد والباقي backup.
 - جديد بسرعة Master وقع يتم انتخاب Master لو الـ TCP.
 - خاص رقم 112 وليس IP لأنّه يستخدم بروتوكول HSRP أسرع شوّبة من TCP.
 - جديد Master يحتاج وقت انتخاب Master أسرع في الاستجابة في بعض الحالات لكن في حالة فشل الـ Master.
-

أوامر VRRP:

```
interface int-name
  vrrp [group-number] ip [virtual-ip]
show vrrp
```

3. GLBP - Gateway Load Balancing Protocol

- بروتوكول خاص بـCisco (Cisco proprietary).
 - يتيح توزيع التحميل بين أكثر من روتر مشتبئين: Active و Standby HSRP.
 - يوجد:
 - Active Virtual Gateway (AVG): هو المسؤول عن توزيع الطلبات على باقي الروترات.
 - Active Virtual Forwarders (AVFs): وتعمل AVG الروترات التي تستقبل البالكتيات من: التوجيه.
 - الهدف: تحميل متوازن و حقيقي بين الروترات.
-

أوامر GLBP:

```
interface int-name
  glbp [group-number] ip [virtual-ip]
show glbp
show glbp brief
glbp [group-number] priority [number]
glbp [group-number] preempt
```

- لتحديد الأولوية وال preempt.

```
glbp [group-number] load-balancing [host-dependent | round-robin | weighted]
```

شرح طرق التحميل Load Balancing:

- العميل IP توزيع ثابت حسبنفس العميل يستخدم نفس الروتر دائمًا.
 - يوزع الطلبات بشكل متساوي على الروترات بالتتابع: round-robin.
 - يوزع الطلبات بحسب أوزان (أولوية) كل روتر: weighted.
-

ملخص بسيط للفرق بين الفروقات:

البروتوكول	آلية العمل	عدد الروتارات النشطة	بروتوكول النقل	سرعة الانتقال للنسخة النشطة	ملاحظات
HSRP	Active-Standby	1 Active + 1 Standby	TCP	متوسط	Cisco proprietary ، ضروري لإعادة Active Preempt
VRRP	Master-Backup	1 Master + Backups	بروتوكول خاص 112	أسرع من HSRP	مفتوح المصدر، انتخاب Master جديد تلقائي
GLBP	Load Balancing	1 AVG + Forwarders	Cisco خاص	سريع	يوزع الحمل بين عدة روتارات

AAA - Authentication, Authorization, Accounting

- **Authentication:** التحقق من هوية المستخدم (مثلاً: يطلب يوزر وباسورد عند تسجيل الدخول).
- **Authorization:** تحديد صلاحيات المستخدم (هل له حق الدخول على أوامر معينة أو موارد محددة).
- **Accounting:** تسجيل ومراقبة أنشطة المستخدم (تسجيل الدخول، الأوامر المنفذة، مدة الجلسة، الخ).

أنواع السيرفرات المستخدمة في AAA

1. TACACS+ (Cisco Proprietary)

- بروتوكول خاص بسيسكو.
- (عادة على بورت 49) TCP يستخدم.
- (يعني كل وحدة تتحكم فيها لوحدها) Authentication، Authorization، Accounting.
- ، وأفضل للتعامل مع الأوامر الإدارية (مثل إدارة أجهزة الشبكة) TCP أكثر أمائة لأنه يستخدم.
- يشفّر كامل المحتوى (بما في ذلك بيانات التوثيق والأوامر).

2. RADIUS (Open Standard)

- بروتوكول مفتوح ومستخدم على نطاق واسع.
- (عادتاً على بورت 1812 لـ Authentication و 1813 لـ Accounting).
- في خطوة واحدة Authentication و Authorization.
- لا يشفّر كل البيانات (يشفر فقط كلمة المرور).
- ، الشبكات الكبيرة، والوصول إلى الشبكات Wi-Fi أكثر استخداماً في شبكات الـ Network Access Servers).

إعدادات AAA على أجهزة Cisco

1. تفعيل نموذج AAA:

```
aaa new-model
```

2. إعداد Authentication (تسجيل الدخول) باستخدام مجموعة سيرفرات (Radius أو Tacacs+):

```
aaa authentication login [default | list-name] group [radius | tacacs+]
[local | enable | line]
```

- **default:** الطريقة الافتراضية لتسجيل الدخول.
 - **list-name:** اسم خاص لقائمة المصادقة يمكنك استخدامها لاحقاً.
 - **group radius:** تستخدم مجموعة سيرفرات RADIUS.
 - **group tacacs+:** تستخدم مجموعة سيرفرات TACACS+.
 - **local:** fallback إلى المستخدمين المحليين على الجهاز.
 - **enable:** يستخدم للتحقق من صلاحيات الدخول لوضع Enable (privileged exec mode).
 - **line:** يستخدم للخطوط مثل (console, vty).
-

3. تعريف سيرفر TACACS+ أو RADIUS:

```
tacacs server SERVER_NAME
address ipv4 IP_ADDRESS
key YOUR_SECRET_KEY
```

أو

```
radius server SERVER_NAME
address ipv4 IP_ADDRESS auth-port 1812 acct-port 1813
key YOUR_SECRET_KEY
```

4. ربط تسجيل الدخول بالخطوط:

الخطوة مثلاً لتحديد مصادقة الخطوط console و vty (Telnet / SSH):

```
line con 0
login authentication default

line vty 0 4
login authentication default
```

5. اختبار المستخدم على السيرفر (Test AAA Group):

```
test aaa group [radius | tacacs+] username PASSWORD legacy
```

شرح البروتوكولات والمنافذ:

البروتوكول	النوع	البروتوكول المستخدم	المنفذ	ملاحظات
TACACS+	Cisco proprietary	TCP	49	أكثر أماناً، تشفير كامل، يستخدم لإدارة أجهزة الشبكة
RADIUS	Open standard	UDP	1812 (Auth) / 1813 (Accounting)	شائع في الشبكات اللاسلكية و NAS ، تشفير جزئي فقط

Cisco ISE (Identity Services Engine)

- هو برنامج متكامل لإدارة الهوية والصلاحيات في الشبكات.
- حسب التهيئة TACACS+ وأو RADIUS يُستخدم كسيرفر مركزياً (يوجد السيرفر والواجهة لإدارة السياسات) AAA يدير إدارة المصادقة، التفويض، والتسجيل بشكل مركزي Cisco يمكن ربطه بأجهزة AAA.
- يدعم أنواع متعددة من الأجهزة وبروتوكولات AAA.

ملخص مختصر للأوامر:

```
aaa new-model

aaa authentication login default group tacacs+ local

tacacs server TACACS1
address ipv4 10.0.0.1
key MySecretKey

radius server RADIUS1
address ipv4 10.0.0.2 auth-port 1812 acct-port 1813
key RadiusSecret

line con 0
login authentication default

line vty 0 4
login authentication default

test aaa group tacacs+ username testuser legacy
```

ما هو 802.1Q (dot1q)?

عشن يحدد IEEE 802.1Q (Ethernet Frames) لاطارات الإيثرنت Tagging هو بروتوكول قياسي يستخدم لعمل VLAN اللي الإطار ينتمي لها.

يعني إيه Tagging؟

عشن نقول لـ (frame) داخل الإطار (Tag) هو ببساطة إضافة علامة "رقم VLAN" الإطار ده يخص Switch أو Router.

ليه بنستخدم 802.1Q؟

لازم (trunk link) على نفس الكابل VLAN لما يكون عندك سوينشات متصلة بعض، ويتقلل بيانات من أكثر من عشن كل سوينش يعرف الإطار ده من أي VLAN يستخدم Tagging.

شكل إطار 802.1Q الفرق بين Tagged و Untagged)

الإطار الطبيعي فيه:

- MAC Source
- MAC Destination
- EtherType
- Payload
- CRC

زيادة بين MAC و EtherType بـ 4 بايت (Bytes)، بنضيف dot1q لما نستخدم:

802.1Q Tag Structure (4 Bytes):

Field	Size	Description
TPID (Tag Protocol ID)	2 Bytes	يحدد أن الإطار ده فيه – 0x8100 VLAN Tag
TCI (Tag Control Info)	2 Bytes	يحتوي على:

- Priority (3 bits)
- CFI (1 bit)
- VLAN ID (12 bits) → رقم VLAN (4094) | من 1 إلى

كيف يتم إرسال الإطارات بين السوينتشات؟

- **Trunk Port:** يبيغت **Tagged Frames** (dot1q).
 - **Access Port:** يبيغت **Untagged Frames** (واحدة فقط VLAN تخص).
-

على سويتش Cisco: مثال عملی – إعداد Trunk 802.1Q

```
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
```

يرسل البيانات بين VLANs 10 ، 20 ، و 30 باستخدام trunk هذا يجعل البورت dot1q.

ما هي Native VLAN في dot1q؟

- **Native VLAN** على Tag اللي تمر بدون VLAN هي الـ trunk port.
- ، لكن يمكن تغييرها 1 VLAN بشكل افتراضي تكون

مثال:

```
interface FastEthernet0/1
switchport trunk native vlan 99
```

VLAN 99 سيتم اعتبارها تابعة لـ Tag يعني الإطارات اللي بدون

ملخص سريع:

المصطلح	المعنى
802.1Q	بروتوكول VLAN Tagging
Trunk Port	يمرر عدة VLANs بين السوينتشات
Access Port	يمرر واحدة فقط VLAN
VLAN Tag (4 Bytes)	يضاف داخل الإطار لتحديد الـ VLAN
Native VLAN	VLAN تمر بدون Tag على trunk port

✓ ما الفرق بين 802.1Q و 802.1X؟

البروتوكول

الوظيفة الأساسية

802.1Q VLAN Tagging (تمييز الإطارات حسب VLAN)

802.1X Port-Based Authentication (التحكم في من يدخل الشبكة)

مش 802.1، 802.1X إنت هنا بتتكلم عن Q.

⌚ 802.1X Authentication:

- التحكم في الوصول إلى الشبكة.
 - المستخدم (أو الجهاز) لازم يتم التحقق منه قبل ما يحصل على صلاحية الدخول.
 - يستخدم عادة مع AAA Server (مثل Cisco ISE و RADIUS).
-

🧠 المكونات الأساسية لـ 802.1X:

العنصر

الوصف

Supplicant هو اللي بيطلب الدخول (مثلاً: كمبيوتر أو لابتوب).

Authenticator هو اللي بيمنع أو يسمح بالمرور – Access Point أو السوينتش أو الـ.

Authentication Server هو اللي بيقرر هل يدخل ولا – RADIUS سيرفر.

✓ شرح الأوامر:

♦ 1. تفعيل AAA:

aaa new-model

على السوينتش AAA يفعل نظام.

♦ 2. إعداد طريقة التوثيق:

aaa authentication dot1x [default | NAME] group [radius | tacacs+] [local | enable | line]

- للصادقة باستخدام policy dot1x.
- في حالة فشل التحقق من السيرفر local يمكن الرجوع إلى.

مثال:

```
aaa authentication dot1x default group radius
```

◆ **3. على السويفتش dot1x تفعيل:**

```
dot1x system-auth-control
```

- على السويفتش (يعني يصبح مستعد يتحكم في المنافذ) 802.1X يفعل globally.

◆ **4. 802.1X تفعيل معنف:**

```
interface FastEthernet0/1
dot1x port-control auto
```

- **auto** (معناها: المنفذ هيفتح بس لو حصل توثيق ناجح Authentication Success).
- **force-authorized** (يعني أي حد)، و **force-unauthorized** (يمنع الكل).

 **إعداد الجهاز (PC – Supplicant):**

مثلاً في Windows:

◆ **خطوات:**

1. افتح **Services** (الخدمات).
2. ابحث عن خدمة اسمها **Wired AutoConfig**.
3. Startup Type: Automatic.
4. ثم اضغط "Start".

على كارت الشبكة السلكية X authentication 802.1 دyi الخدمة المسؤولة عن تنفيذ.

كيف تتم العملية:

- الجهاز يتصل بالسويفتش.
 - السويفتش يمنع المرور لحد ما يحصل Authentication.
 - الجهاز يرسل بيانات الدخول (username/password).
 - السويفتش يرسلهم للسيرفر (RADIUS).
 - السيرفر يرد OK أو Reject.
 - السويفتش يفتح البورت، والجهاز يدخل الشبكة → OK لو.
-

تطبيق عملی مشترك مع Cisco ISE:

الخطوة	أين تتم؟	الوصف
إعداد aaa new-model	السويفتش	لتفعيل AAA
إعداد authentication dot1x	السويفتش	تحديد نوع المصادقة
إعداد dot1x system-auth-control	السويفتش	802.1X Globally لتفعيل
dot1x port-control auto	على كل منفذ	المنفذ لا يسمح بالوصول إلا بعد المصادقة
إعداد RADIUS	على السويفتش	تحديد السيرفر
خدمة Wired AutoConfig	على الجهاز	في ويندوز supplicant لتفعيل

WIFI-Technology

 أولاً: مقارنة بين Ethernet و Wi-Fi

العنصر	Ethernet (سلكي)	Wi-Fi (لاسلكي)
المعيار (Standard)	802.3	802.11
(Media) الوسيط	نحاس أو ألياف زجاجية	الهواء
طريقة نقل البيانات	كهرباء أو ضوء (Fiber)	موجات راديوية (Radio Waves)

يعني ببساطة، الشبكات السلكية تستخدم الكابلات وال WAVES لنقل البيانات، أما الواي فاي فيستخدم موجات الراديو عبر الهواء.

 ثانياً: أنواع الشبكات اللاسلكية (Wi-Fi Topologies)

- شبكة مؤقتة مباشرة (Ad-Hoc)
 - كل جهاز يتصل بالثاني مباشرة بدون Access Point.
 - الاسم الفي ليها: IBSS (Independent Basic Service Set).
 - مثال: لو عندك جهازين لاب توب بينكلموا بعض بدون راوتر.
- بنية تحتية (Infrastructure)
 - (راوتر أو نقطة وصول) Access Point كل الأجهزة تتصل به.

- الاسم الفنی: BSS (Basic Service Set).
 - النوع المستخدم في المنازل والمكاتب.
3. Mesh Network (شبكة شبکية)
- بيتواصلوا مع بعض Access Point أكثر من ESS (Extended Service Set).
 - الاسم الفنی: ESS (Extended Service Set).
 - يتغطي مساحة أوسع وتوفر استقرار أكبر.

ثالثاً: خيارات الأمان في الشبكات اللاسلكية (Wireless Security Options)

1. Captive Portal:
 - نوع من الحماية بتشوفه في الكافيهات والفنادق قبل ما تقدر تدخل (Web Authentication) لما توصل على الواي فاي، ببيظهر لك صفحة تسجيل دخول الإنترنت.
2. Hidden SSID:
 - الشبكة مش بتظهر في البحث لازم تعرف اسم الشبكة وتدخله يدوياً.
3. WPA/WPA2 (كلمة مرور):
 - نوعين
 - كل الناس بتدخل نفس كلمة المرور: Personal.
 - كل موظف عنده اسم مستخدم وكلمة مرور مختلفة: Enterprise.
 - عشان يتأكدوا من بيانات RADIUS Server بيستخدموا حاجة اسمها Enterprise في الدخول لكل شخص.

توضيح إضافي على الـ Enterprise:

- بيعتخدموه في الشركات.
- كل موظف عنده حساب خاص بيه.
- عشان يسمح أو يمنع الدخول بناءً على بيانات كل موظف RADIUS Server بيتواصل مع Access Point.

ما هو VRF؟

VRF = Virtual Routing and Forwarding

مستقلة على نفس (Routing Tables) (وغيرها) عشان تعمل عدة جداول توجيه Cisco هو تقنية تُستخدم في أجهزة الراوتر أو السويفت.

يعني كأن عندك راوترات متعددة داخل راوتر واحد، كل شبكة تشغّل في "عالم خاص" ما يتدخل مع الثاني

ليه نستخدم VRF؟

- لفصل حركة البيانات بين عملاء أو أقسام مختلفة في نفس الشبكة.

- (عدة عملاء على نفس الجهاز بدون ما يشوفوا بعض) **Multi-Tenancy** التطبيق مفهوم.
 - لدعم الـ **MPLS VPNs**.
-

VRF vs. مع VRF:

الحالة	النتيجة
كل VRF بدون	كل الشبكات تشارك في نفس جدول التوجيه، وممكن يحصل تضارب.
كل VRF مع	كل شبكة لها جدول توجيه مستقل، وكأن كل شبكة على راوتر خاص بها.

مثال واقعي:

شركة عددها:

- شبكة داخلية للموظفين 10.1.1.0/24
- شبكة للكاميرات 10.1.1.0/24

= ، لكن لازم يفصلهم. الحل IPs الاتنين بنفس الـ **VRF**.

خطوات إعداد VRF على Cisco Router:

1. إنشاء VRF:

```
ip vrf HR
  rd 100:1
!
ip vrf IT
  rd 100:2
```

- **rd** = Route Distinguisher (للتمييز في) MPLS VPN)
-

2. ربط الواجهات بالـ VRF:

```
interface GigabitEthernet0/0
  ip vrf forwarding HR
  ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/1
  ip vrf forwarding IT
  ip address 10.1.1.1 255.255.255.0
```

مختلف VRF في واجهتين مختلفتين لأنهم في IP تقدر تستخدم نفس الـ

3: إنشاء جداول راوت مستقلة:

```
ip route vrf HR 0.0.0.0 0.0.0.0 192.168.1.1  
ip route vrf IT 0.0.0.0 0.0.0.0 192.168.2.1
```

✓ التحقق من VRF:

```
show ip route vrf HR  
show ip route vrf IT
```

```
show ip vrf
```

💡 فائدة مهمة:

الفائدة	الشرح
عزل الشبكات	له جدول توجيه مستقل VRF كل
IP نفس الـ	ات بدون تعارض IP تقدر تكرر الـ
دعم Multi-Tenant	أو بيئات الشركات (ISP) مفید لمزودي الخدمة.

✓ VRF Lite vs. MPLS VRF

النوع	الوصف
VRF Lite	، على أجهزة داخلية عادية MPLS يعمل بدون
VRF MPLS	يستخدم داخل بيئه MPLS VPNs.

📌 مثال تطبيقي سريع:

```
ip vrf CUSTOMER_A  
rd 10:1  
  
interface g0/0  
ip vrf forwarding CUSTOMER_A  
ip address 192.168.10.1 255.255.255.0
```

تقنيات الشبكات الواسعة – WAN Technologies : عنوان الدرس

، وهي تقنية بتسمح بوجود أكثر Virtual Routing and Forwarding وهي اختصار لـ (VRF) مكتوب فوق كلمة على نفس الرووتر (تستخدم في الشبكات الموزولة مثلاً بين شركات على نفس البنية Routing Table من جدول توجيه التحتية).

أول جزء: أنواع الشبكات

- (عامة): زي الانترنت، أي حد يقدر يستخدمها Public.
- (خاصة): زي الشبكات المغلقة للشركات Private.

التحويل عبر الدارات Circuit Switching (ثاني جزء)

- Line-Based Communication: يعني بيتم إنشاء خط فعلي بين المرسل والمستقبل قبل بدء الاتصال، ومثال عليه:
 - Leased Line (خط مؤجر دائم بين موقعين)
 - Dial-Up (اتصال مؤقت عن طريق رقم هاتف)
 - ISDN (شبكة رقمية لخدمات الصوت والبيانات)

:مكتوب

- on-demand circuit switching → Dial-Up و ISDN زي

التحويل عبر الحزم Packet Switching (ثالث جزء)

- وكل حزمة تسلك طريق مختلف (packets) البيانات بت分成 إلى حزم.
- أفضل للشبكات الحديثة لأنه أكفاء وأقل تكلفة.

:أمثلة

- Frame Relay
- ATM
- X.25

MPLS – Multi Protocol Label Switching (رابع جزء)

- تقنية توجيه سريعة ومستخدمة في الشبكات الكبيرة.
- (ملصقات) لتوجيه البيانات العادي، بيسخدم IP Routing Labels بدل ما يستخدم بدل ما يستخدم.
- مكتوب:
 - "MPLS = 3 حالات" → غالباً المقصود 3 أنواع من الأجهزة P:
 - جهاز داخلي للمزود (Provider Router)

- PE = Provider Edge (الراوتر المتصل مع العميل)
- CE = Customer Edge (جهاز العميل)

ADSL و SDSL خامس جزء: مقارنة بين

الخاصية	ADSL (Asymmetric)	SDSL (Symmetric)
المتماثل	أقل من Upload (غير متماثل)	Upload = Download (متماثل)
الاستخدام	المنازل (إنترنت + صوت)	الشركات (بيانات + صوت بجودة عالية)
Upload	بطئ	سريع
Download	سريع	غالباً أقل أو متساوي

- مناسب للمستخدم المنزلي اللي غالباً بيحمل أكثر ما يرفع: ADSL.
- مناسب للشركات اللي بترفع وتنزل بيانات بنفس القدر، مثل السيرفرات والـ VoIP.

VPN



أولاً: ليه GRE + IPsec؟

البروتوكول	الوظيفة
GRE (Generic Routing Encapsulation)	بين الفروع لنقل البيانات (Tunnel) ينشئ نفق
IPsec (Internet Protocol Security)	يؤمن هذا النفق بالتشفيير والمصادقة

آمنة ومشفرة VPN = يؤمنها IPsec + ينقل البيانات GRE: إذن



خطوات الإعداد الأساسية:

- إعداد نقط GRE.
- إعداد ISAKMP (لتكوين الاتصال الآمن).
- إعداد IPsec (لتشفيير البيانات).
- ربط كل ده باستخدام Access List + Crypto Map.

✓ 1. إعداد ISAKMP (Phase 1)

► ISAKMP Policy:

هي مرحلة التفاوض بين الجهازين لتحديد شروط الحماية.

```
crypto isakmp policy 10
  encr aes           ← نوع التشفير: des, 3des, aes
  hash sha          ← نوع الـ hashing (sha أو md5)
  authentication pre-share ← نوع التوثيق (لتبادل المفاتيح)
  group 2            ← Diffie-Hellman Group
  lifetime 86400     ← وقت الجلسة (اختياري)
```

►تعريف الـ Pre-Shared Key:

```
crypto isakmp key MyKey123 address 192.168.2.1
```

- مفتاح مشترك بين الطرفين: MyKey123.
- الطرف الآخر (الراوتر الثاني).
- لو مش فارق مين الطرف الثاني بشرط يشارك نفس المفتاح address 0.0.0.0 ممكن تستخدم.

✓ 2. إعداد ACL لتحديد نوع الترافيك الذي هيتشفر:

```
ip access-list extended GRE-TRAFFIC
  permit gre host 192.168.1.1 host 192.168.2.1
```

- ده وده → شيفه IP بين الـ GRE هنا بتقول: لو فيه ترافيك الـ ACL.

✓ 3. إعداد Transform Set (IPsec Phase 2)

```
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
```

- esp-aes: نوع التشفير.
- esp-sha-hmac: المصادقة باستخدام SHA.

4. إعداد Crypto Map

```
crypto map VPN-MAP 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set MYSET
  match address GRE-TRAFFIC
```

- set peer: IP الطرف الثاني.
- match address: ACL اللي هتطبق عليها التشفير.
- set transform-set: Transform Set اللي اتعمل قبل كده الرابط.

5. تطبيق Crypto Map على الواجهة:

```
interface FastEthernet0/0
  crypto map VPN-MAP
```

6. إعداد نفق GRE:

```
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel destination 192.168.2.1
```

- السورس الحقيقي (مثلاً: الإنترنت) IP هو الـ Tunnel Source.
- الطرف الثاني على الإنترت IP هو Tunnel Destination.

أوامر التحقق (Show Commands):

الأمر	المعنى
show crypto isakmp sa	هل الاتصال آمن قائم؟ – Phase 1 حالة
show crypto ipsec sa	حالة التشفير والترافيك المشفر فعلياً
show crypto isakmp policy	عرض السياسات المعرفة
show crypto isakmp key	عرض المفاتيح المخصصة
show crypto ipsec transform-set	عرض الترانسفورم سيسس المستخدمة

ملخص التسلسل:

1. ISAKMP Policy (Phase 1).
 2. Pre-shared Key.
 3. Access-list لحماية الترافيك.
 4. Transform Set (IPsec – Phase 2).
 5. Crypto Map (ربط الكل).
 6. GRE Tunnel (النقل).
 7. بـالإنترفيس Crypto Map ربط.
-

T-Shoots

في الشبكات خطوات عملية لعمل Troubleshooting

● 1. اسأل نفسك: "فين المشكلة؟" (تعريف المشكلة)

- هل المشكلة على جهاز واحد؟ ولا كل الشبكة؟
- Local ولا Remote؟
- دائمًا ولا متقطعة؟

 اكتب وصف المشكلة باختصار:

على Ping مثلًا: "جهاز مش قادر يعمل Default Gateway"

● 2. ابدأ من أسفل لأعلى (OSI Model)

◆ Layer 1: Physical

- اتأكد من الكابلات والتوصيلات والإضاعة في الـ port
-  أوامر:
- show interfaces status
- show interfaces int-name

◆ Layer 2: VLAN / STP / Trunk

- اتأكد إن الپورت في VLAN صح
- اتأكد إن الپورت STP مثـن موـقـف الپورـت
- أوامر :
 - show vlan brief
 - show spanning-tree
 - show mac address-table

◆ Layer 3: IP Routing

- هل الجهاز عنده IP؟
- هل Default Gateway شغال؟
- هل فيه Route يوصل؟
- أوامر :
 - ping x.x.x.x
 - traceroute x.x.x.x
 - show ip route
 - show ip interface brief

● 3. (Isolate the failure) حدد النقطة اللي بتفشل فيها.

- للراوتر التالي → للسيرفر النهائي → لـGateway من الجهاز → لـPing متابع كل خطوة، أول نقطة تفشل فيها = عندها تبدأ تحقق.

● 4. حل المشكلة من الزاوية المناسبة.

نوع المشكلة	خطوات التحليل
Routing	show ip route, show ip protocols
Switching/VLAN	show vlan, show interfaces trunk
ACL/NAT	show access-lists, show ip nat translations
HSRP/VRRP	show standby, show vrrp
VPN/GRE	show crypto isakmp sa, show crypto ipsec sa
DHCP	debug ip dhcp, show ip dhcp binding
ARP	show arp, clear arp-cache

نفذ التغيير أو أصلح المشكلة 5.

- غلط؟ VLAN؟ ACL؟ IP NAT؟
- فعل؟ static route؟ priority؟ interface؟ أخذ؟ عمل؟

☞ اكتب التغيير وخطة الرجوع rollback لو بتشتغل في production

إن المشكلة اتحلت (Verify) اختبر 6.

- Ping
 - Traceroute
 - show commands
-

سجل التغيير وراقب 7. Logs

- سجل الخطوات (التوثيق)
 - لو شغال syslog أو debug راقيب الـ
 - أوامر :
 - show logging
 - terminal monitor
-

سريعة حسب نوع المشكلة Checklists خلي عندك 8.

مثال TSHOOT VLAN

- أو access هل البورت trunk؟
- هل البورت في VLAN مظبوطة؟
- هل الـ VLAN مترففة على السويفت؟
- هل الـ STP blocking؟
- هل trunk شغالة؟

مثال TSHOOT IP Route

- في جدول التوجيه؟ هل فيه route
- هل next-hop reachable؟
- هل فيه ACL تمنع الترافيك؟
- هل فيه NAT أو VRF مأثرة؟

Tips: سريعة

- عشان ت Shaw run | section بس استخدم X
 - عشان تتأكد من التوصيلات استخدم show cdp neighbors
 - بذر وقت الحاجة فقط استخدم debug
-

يستخدم عشان تتبع مسار الباكت من جهازك لوجهة معينة (Windows في traceroute أو traceroute (جهاز وسيط) الباكت بتمر عليه hop ، ويرفه على أي destination IP or domain).

ما هو traceroute؟

الأمر:

على سيسكو:

```
traceroute [ip-address]
```

على ويندوز:

```
tracert [ip-address or domain]
```

على لينكس / ماك:

```
traceroute [ip-address or domain]
```

كيف ي عمل؟

- أول راوتر يرد إنه حذفها $TTL = 1$ بيعت باكت بـ.
 - ثانوي راوتر يرد... وهكذا $TTL = 2$ بعدين.
 - لحد ما توصل للهدف أو لحد آخر hop.
-

مثال على Cisco:

```
Router# traceroute 8.8.8.8
```

: الناتج

```
Type escape sequence to abort.  
Tracing the route to 8.8.8.8
```

```
1 192.168.1.1 1 msec 1 msec 1 msec  
2 10.1.1.1      3 msec 3 msec 2 msec  
3 172.16.5.1    9 msec 8 msec 8 msec  
4 8.8.8.8       11 msec 11 msec 10 msec
```

فوائد traceroute:

- تعرف فين الترافيك بيتوقف أو يتأخر
- مفید جدًا في troubleshooting
- تقدر تكتشف مشاكل في:
 - Routing
 - ACL
 - NAT
 - VPN
 - ISP

في النتيجة * * لو شفت نجوم :

يمنع الرد Firewall أو إن فيه ACL أو ICMP Time Exceeded ده معناه إن الراوتر مش بيرد على الـ

نصيحة:

معين → يبقى المشكلة هناك، وغالبًا hop وافق عند traceroute لكن Ping لو حصل مشكلة في:

- ناقص route فيه
- أو ACL فيه أو firewall
- أو فيه سويتش وافق (مثلًا STP)