7/2/2024

CCNA 200-301

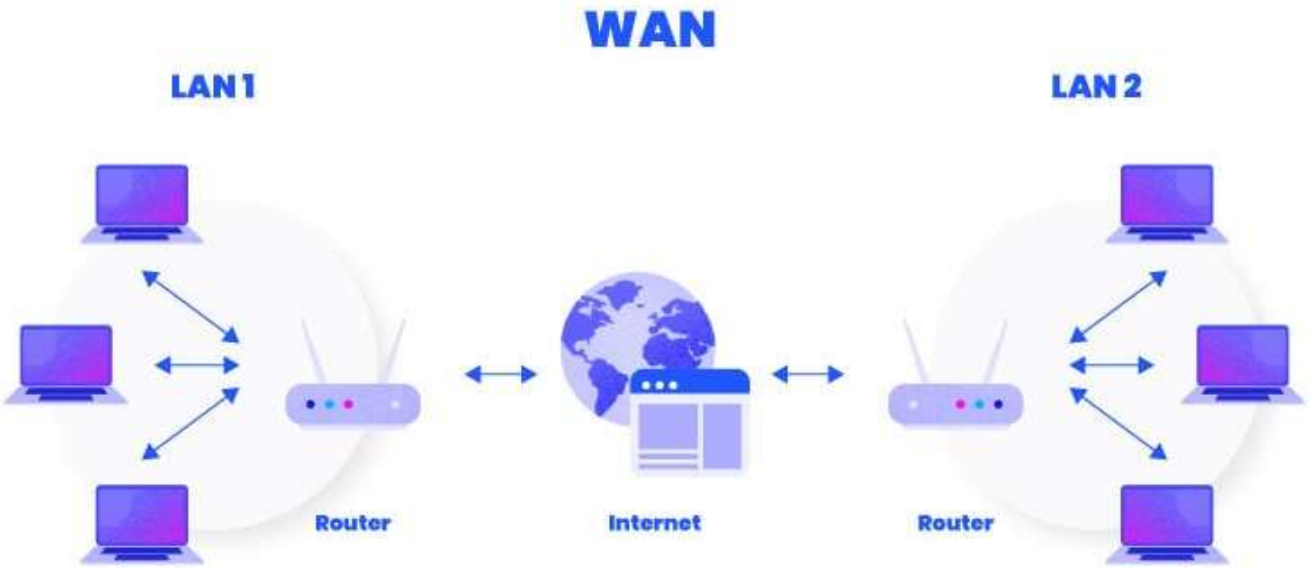
By. Sadek
01127683025

Network fundamentals

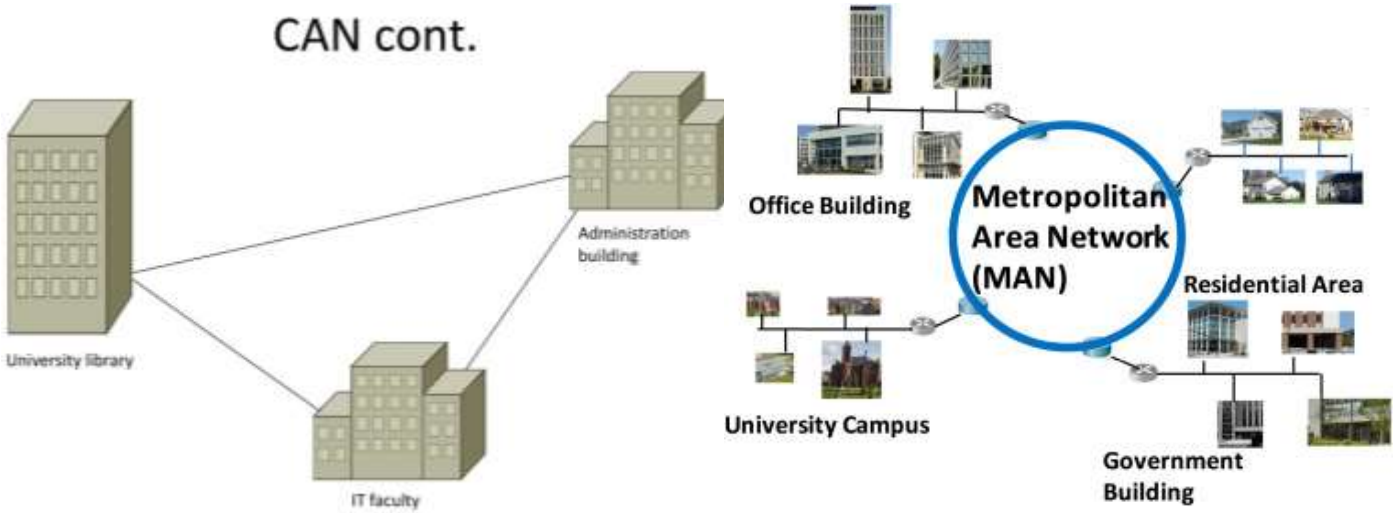
- Network : مجموعة من الاجهزة المتصلة معا قد تكون متصلة من خلال سلك (wire) او قد تكون لاسلكية (wireless)
- الهدف من الشبكة هو مشاركة :
  1. Devices
  2. Applications
  3. Information & data
  4. Resource
  5. Files
  6. Internet

Type of Networks

- من اشهر انواع الnetwork infrastructures هم الLAN (local area network) وWAN (wide area network)
- LAN : هى مجموعة من الاجهزة المتصلة معا فى مساحة جغرافية محدودة (فى نفس المبنى)
- WAN : هى مجموعة من ال LANs المتصلة معا فى مساحة جغرافية كبيرة (بين المدن او بين الدول)
- من اكبر الامثلة على ال WAN هى شبكة الinternet



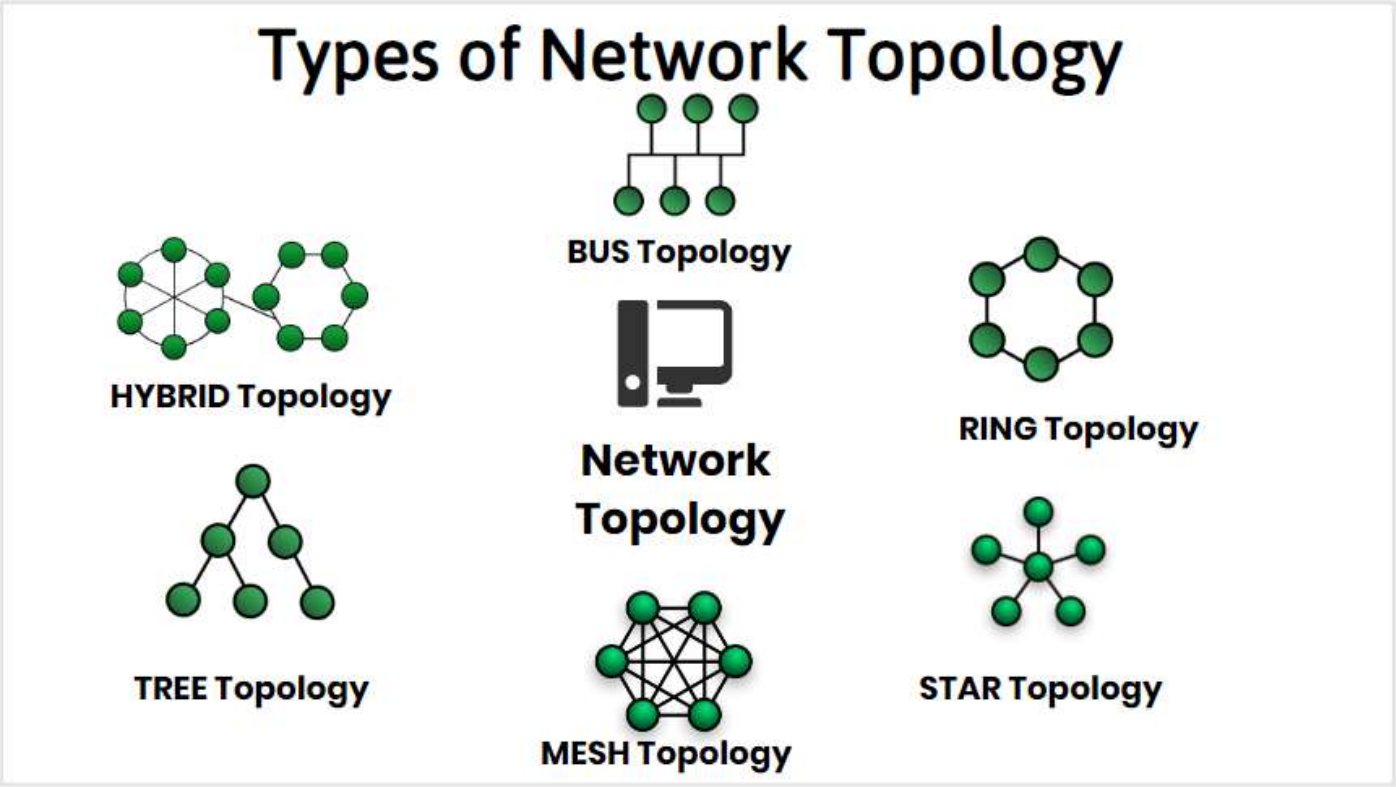
- يوجد نوع اخر من network infrastructure وهو CAN(campus area network) وهى تكون اكثر من LAN متصلة معا ولاكن فى مساحة جغرافية صغيرة (بين اكثر من مبنى)
- MAN : هى عبارة عن مجموعة من الLANs المتصلة معا فى مساحة جغرافية كبيرة نسبيا (فى نفس المدينة)



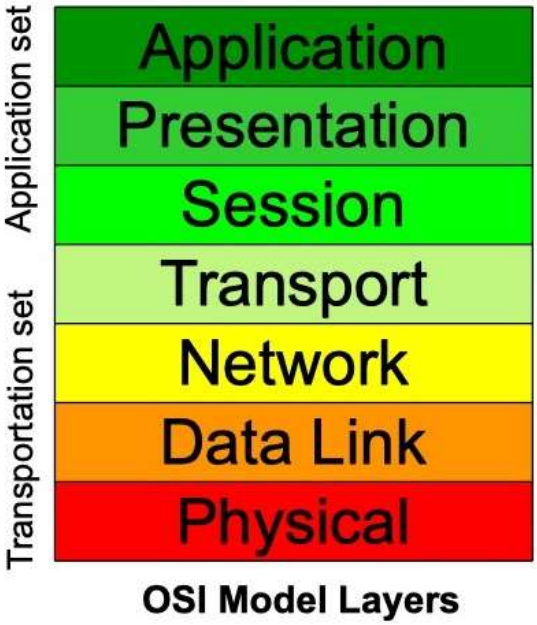
Network topologies

- Network topologies : هى طريقة ربط الاجهزة معا سواء كان بشكل physical او logical
- يوجد انواع كثيرة من الtopologies مثل :

1. Bus topology
   - كان يتم استخدام فيه co-axial cables
   - هو من اقدم الانواع والتى لم تعد موجودة الان
   - فيه يتم توصيل جميع الاجهزة بكيبل واحد فقد ويسمى backbone cable
   - كل جهاز متصل مع الbackbone cable من خلال كيبل فرعى
   - ينتهى الbackbone cable بterminator لكى يلاشى عملية االرتداد البينات عند وصولها الى نهاية الكيبل
   - يمكن حدوث collision ويتم التعامل معه من خلال نظام يسمى CSMA/CD حيث يتم ارسال jam signal لباقى الاجهزة لتنبيههم بحدوث collision وجعلهم يتوقفوا عن ارسال الdata لبعض الوقت
     - CSMA تكون موجودة على الNIC
   - اى ارسال للبينات يتم استلامه من جميع الاجهزة وهذا الconnection يسمى broadcast connection
2. Ring topology
   - هو من الانواع التى لم تعد تستخدم الان
   - فيه كل جهاز متصل بجهزان معا ليكونوا حلقة
   - كل جهاز يحتوى على network card 2 وكل واحد يخرج منه سلك لجهاز اخر
   - مسار انتقال الdata يكون فى اتجاه واجد ويوجد نوع يكون فى اتجهان ويسمى dual ring topology
3. Star topology
   - هو النوع المستخدم حاليا
   - تكون الاجهزة متصلة عن طريق hub او switch
   - يمكن ان يحدث collision فى حالة كان يعمل بhub
   - فى حالة كان متصل بhub فانه يكون bus logical topology
   - من مميزتها انه عند حدوث مشكلة فى جهاز لا يؤثر ذالك على باقى الشبكة
4. Mesh topology
   - يتم استخدامه حاليا ولاكن بشكل قليل لانه يتطلب تكلفة عالية
   - فيه كل جهاز متصل بباقى الاجهزة بشكل direct
   - من مميزاتها انها توفر ما يسمى ب redundancy وهو انه عند حدوث مشكلة فى واحد من الكبلات المتصلة ب device فانه يكون من السهل التواصل معه عن طريق device اخر
   - يسمى ايضا بredundant topology
   - يتم الmesh topology فى اغلب الاحيان بين switches او بين routers
   - Full mesh فيها كل جهاز متصل مع الاخر
   - Half mesh وهى ان كل جهاز متصل مع الاخر ولاكن يمكن ان يوجد اجهزة غير متصلة بشكل direct



OSI layers



OSI Model Layers

- هى اختصار ل open system interconnection
- هى عبارة عن refrence للخطوات التى يجب اتباعها لكى يتمكن 2 PCs من التواصل
- قبل وضع هذا الstandard كان من الصعب على اجهزة من شركات مختلفة التواصل معا
- تم انشاء هذا الstandard من خلال منظمة ISO
- الlayer الاولة هى physical layer والاخيرة هى الapplication
- بنسبة لsender يتم تطبيق الطبقات من الapplication الى physical بينما الreciver يتم فيه تطبيق الphysical الى application
- يتم اطلاق على application و الpresentation و الsession اسم الapplication layers

Application layer

- هى الlayer التى يتعامل معها الuser
- هى اكثر layer تحتوى على protocols
- هى الطبقة التى يحدد فيها الprotocol بناء على الخدمة المطلوبة

Presentation layer

- تقوم ايضا بعمل تشفير لdata لذالك نجد protocols الخاصة بالتشفير مثل TLS و SSL موجودين فى هذه الlayer
- من وظائف هذه الLayer ايضا عمل compression لdata وتحديد الsyntax او الdata format

Session layer

- هى الlayer المسؤلة عن ادارة الsessions و الsession هى اى عملية اتصال مع جهاز او server اخر

Transport layer

- هى الطبقة المسؤلة عن كيفية نقل الdata من الsender الى الrecever
- من اشهر الprotocols الموجودين فيها هم TCP و UDP
- TCP هو connection oriented اى انه يقوم بنقل الdata والتاكد من استلامها
- UDP هو connectionless اى انه لايقوم بتاكد من استلام البينات وانما يقوم بارسالها فقط وهذا ما يجعله اسرع من TCP ولذالك فانه يستخدم فى البثوث المباشرة و فى الالعاب
- TCP يستخدم مع الملفات كبيرة الحجم عكس الUDP والذى يستخدم مع الملفات الصغيرة
- يتم فيها تقسيم الdata و ترقيم اجزائها وتسمى segments وهذا الترقيم مهم لاعادة ترتيبها مرة اخرى فى الrecever
- يتم اضافة header الى الdata وهذا الheader يحتوى على الsource and destination port
- من اهم الوظائف الموجودة فى الtransport layer وهى الflow control وهى تعمل على تحديد عدد الsegment او packet الممكن ارسالها بحيث يستطيع الrecever التعامل معاها وهذه الخاصية تتم بتحديد windowing
- Windowing هى حجم الsegment التى سيتم ارسلها للrecever
- Error recovery هى عملية اعادة ارسال packet مرة اخرى فى حالة حدث خطا ولم تصل الى الrecever

Network layer

- هى الطبقة التى يحدث فيها عملية الrouting لذاالك فا الrouter يستطيع التعامل مع هذه الlayer
- يتم التعامل مع الip فى هذه الlayer
- بتروكول ICMP الخاص بالping يوجد فى هذه الlayer
- يتم اضافة header وهذا الheader هو ما يحتوى على source and destination ip وبذالك تسمى packet

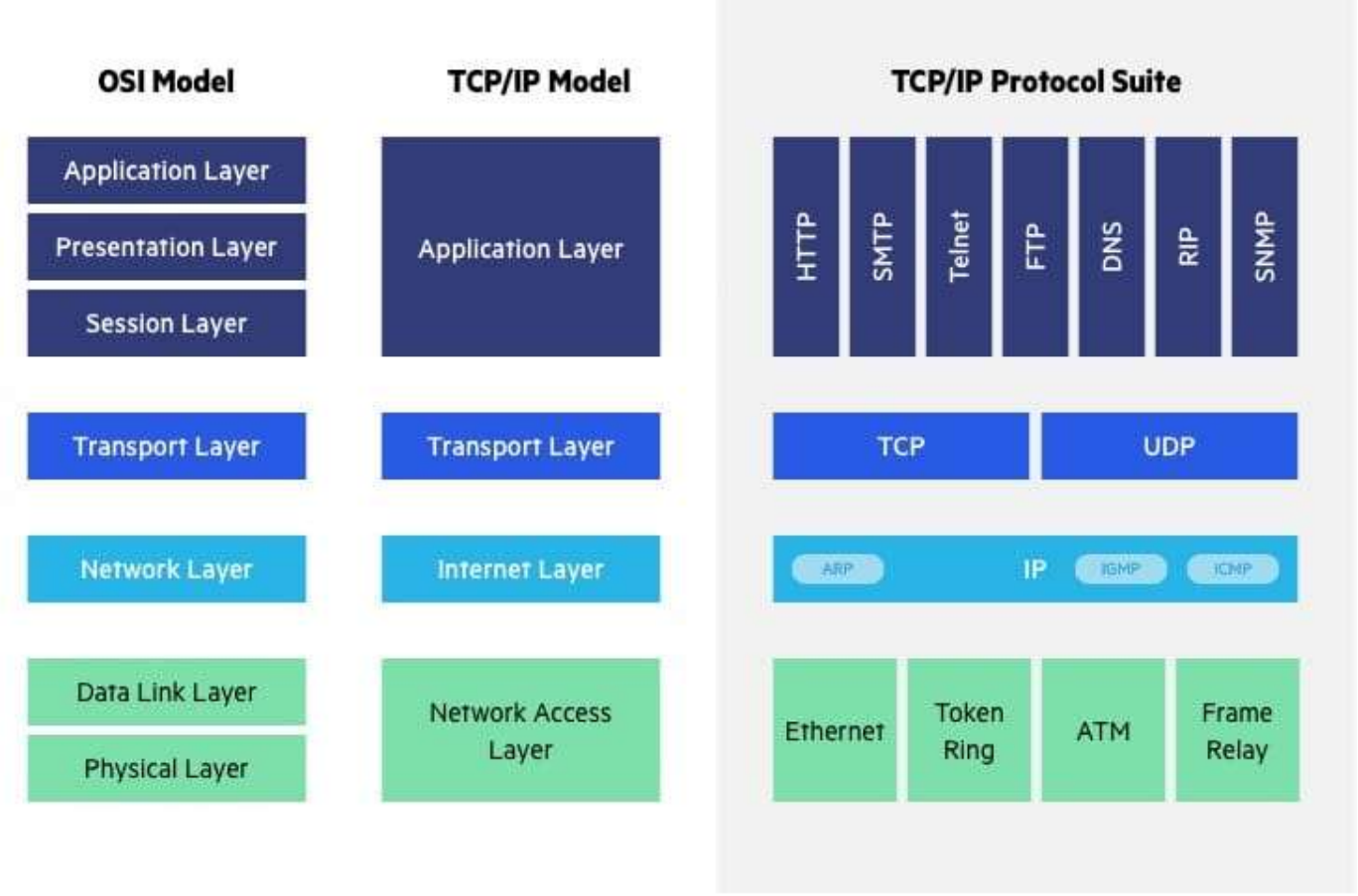
Data link layer

- يتم فيها التعامل مع الMAC address
- يتم اضافةheader يحتوى على source and destination mac وبذالك تسمى fram
- هى الlayer الوحيدة التى بجانب اضافة header تقوم باضافة tail ويكون فيه FCS وهو اختصار fram check sequence وهو مسؤل عن عمل detact للerror
- تنقسم الى جزءان
  1. LLC وهو يساعد فى تنظيم الاتصال من خلال معرفة نوع الaddress الذى يعمل به الجهاز
  2. MAC وهى الجزء الخاص بتعامل مه mac address

Physical layer

- تتعامل مع الmedia الخاص بالnetwork وتقوم بارسال فيه الdata بشكل binary مناسب للوسط

- رغم اهمية الOSI model الا انه لا يتم استخدامه فعليا وانما نستخدم TCP/IP model وهو model اخر يشبه الTCP الى حدا كبير
- تم تفضيل الTCP/IP عن الOSI بسبب :
  1. انه يحتوى على عدد اقل من الlayers حيث يحتوى على 4 layer
  2. برتكول الIP كان موجود ومستخدم فى الTCP/IP عكس الOSI ولاتى كانت ستستخدم protocol يسمى CLNS
- مازال الOSI يتم استخدامه كا reference و يستخدك فى الtroubleshooting
- يتم ايضا اعتبار ان الTCP/IP model يتكون من 5 layer حيث ان الnetwork access layer مقسومة الى data link layer و physical
- فى الOSI كلا من segment و packet و frame يسمو PDU او protocol data unit



Application layer in TCP/IP

- يوجد العديد من الprotocols التى تعمل فى هذه الlayer مثل :

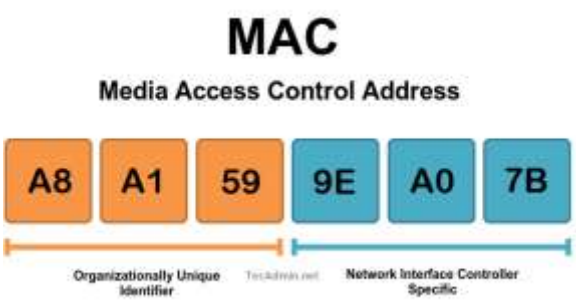
1. HTTP
   - يعمل على port 80
     - الport هو رقم يعبر عن service او application تعمل على الdevice
     - الport number يتكون من 16 bit
     - الport numbers من 0 الى 1023 يسموا ب well-known وهذا يعنى انهم مستخدمين بالفعل من قبل services بينما الports من 1024 الى 65535 يمكن استخدامهم من الusers بشكل طبيعي
     - يوجد امر يستخدم لاظهار الconnections الموجودة على الwindows ويقوم باظهر الip و الport وهذا الامر هو **netstat -n**
     - الip مع الport يسمى بالsoket
   - هو الprotocol المسؤل عن الbroswing فى الinternet
   - يتم تشغيله على server من خلال تصتطيب برنامج مثل IIS او apache
   - الdata فى هذا الprotocol تكون clear text عندما يتم ارسالها فى الشبكة وبتالى يمكن لاى شخص ان يقوم بقرائتها
   - يوجد protocol محسن منه وهو HTTPS وفيه الdata تكون encrypted ويعمل على port 443

2. FTP (file transfere protocol)
   - هو protocol مسؤل عن عملية مشاركة الملفات مثل الupload و الdownload
   - يعمل على port 20 و port 21
   - Port 20 هو ما يتم استخدامه لdata بينما port 21 هو ما يتم استخدام عليه الcontrol
3. SMTP
   - هو اختصار ل simple mail transfere protocol
   - يعمل على port 25
   - هو الservice المسؤلة عن عمل manage للemails
   - الsoftwares التى تقوم بتحويل الdevice الى SMTP هم exchange او louts domino او postfix
   - لاستقبال الemails يمكننا استخدام protocols اخرى مثل pop3 او IMAP
   - SMTP يمكنه الارسال و الاستقبل
4. telnet
   - يعمل على port 23
   - يقوم بوظيفة الremot login ويعنى التحكم فى جهاز ما من خلال جهاز اخر
   - يكون التحكم من خلال CLI
   - الdata فيه تنقل كا clear text
   - يوجد protocol افضل يسمى SSH ويعنى secure shell وفيه الdata تكون encrypted ويعمل على port 22
   - يوجد protocol اخر تم تطويره من خلال Microsoft وهو RPD وهو يقوم ايضا بالتحكم بجهاز معين ولاكن من خلال GUI
5. DHCP
   - يعمل على port 67,68 UDP
   - هو service او server تقوم بعمل configuration للاجهزة الجديدة على الشبكة مثل اعطائهم ip و default gateway و DNS
6. DNS
   - يعمل على port 53
   - يقدم خدمة الdomain name وهى خدمة عبارة عن تحويل لاسماء الdomains الى ips والعكس
   - تعمل هذه الخدمة عند تصفح الانترنت حيث يتم تغيير الdoman الذى يدخله الuser مثل facebook.com الى الip وتتم عمليى الاتصال
7. SMB
   - هو الprotocol المسؤل عن الfile sharing فى الwindows
   - المشابه له فى الlinux هو NFS protocol
8. P2P
   - هو protocol اخر لعمل الfile sharing وهو بديل للFTP
   - وهو الprotocol المستخدم فى torrent

Network Devices

Network card (NIC) (Network adapter)

- هو القطعة او الdevice الذى يجعل الجهاز قادر على الاتصال بالشبكة والتعامل معاها
- الNIC يمكن ان تكون wire او wireless
- لكل NIC سرعة وهى تحدد من خلال تقنية الEthernet المستخدمة كتالى :
  - Ethernet تصل الى 10mb/s
  - Fast Ethernet تصل الى 100mb/s
  - Giga Ethernet تصل الى 1000mb/s
- كل NIC يحتوي على MAC address خاص به لايمكن ان يتكرر
- MAC address اختصار ل media access control
- MAC address يحتوى على 6 اجزاء كل منهم يتكون من رقمان من الhexadecimal
- ينقسم الى قسمين الاول وهو اول ثلاث اجزاء وهو الخاص بشركة التصنيع والقسم الاخر وهو اخر ثلاث اجزاء وهو الخاص بNIC
- منظمة IEEE هى من وضعت الstandard الخاصة بmac address
- يرمز ل قسم الMAC address الخاص بالشركة ب OUI
- MAC address يسمى ايضا ب physical address
- لايمكن تغيير MAC address الخاص بNIC
- Mac address يسمى ايضا BIA وهى اختصار ل burned in address



Hub & Switch

- Hub كان يستخدم لربط اجهزة الnetwork معا ولاكن لم يعد يستخدم
- تم استبدال الhub ب switch بسبب الكثير من المميزات فى الswitch

Hub	switch
يحتوى على عدد قليل من ports	يحتوى على عدد كثير من ports
يتعامل مع layer 1 فقط اى انه لايمكنه قرائة MAC address	يوجد منه نوعان الاول وهو الذى يتعامل مع layer 1,2 اى انه يستطيع قرائة MAC address ويسمى layer 2 switch ويوجد نوع اخر يتعامل مع layer 1,2,3 اى انه يستطيع قرائة MAC address و IP address ويسمى ب layer 3 switch او multi-layer switch
يعمل ب half duplex	يعمل ب full duplex
يعمل بbroadcast فقط	يمكن العمل ب unicast و multicast و broadcast
يمكن ان يسبب فى حدوث collision	يقوم بتخصيص مسار لكل connection

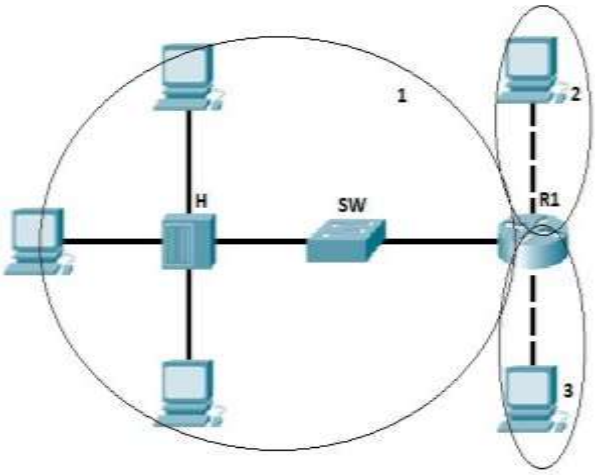
- Switch يقوم بعمل broadcast فى حلات معينة مثل الاتصال بجهاز الMAC address الخاص به غير موجود فى MAC address table بمساعدة ARP

- يوجد device يسمى bridge وتم استخدامه بعد الhub وقبل الswitch وكان يستخدم لتقليل حجم الbroadcast signal
- كان يسمى الswitch ب multi-port bridge
- كلا من switch و hub و bridge يعمل كا repeater
- فى الحالة الطبيعية يقوم الswitch بعمل ما يسمى بnegotiation مع الجهاز المقابل له ومن خلال ذالك يحدد هل سيعمل بfull duplex ام half duplex ولاكن يمكننا عمل configuration وجعله يعمل كا half او full
- الhub او الswitch الذى حدد انه سيعمل half او full لا يقومون بعمل negotiation
- فى حالة اتصال two switches و عند عمل configuration لswitch واحد وجعله half او full فان الجهاز المقابل نتيجة لعدم حدوث negotiation سيعمل كا halfduplex وهذه الحالة تحدث فى الاصدرات القديمة من الswitches
- عند وجود طرفى اتصال واحد يعمل half و الاخر يعمل full سيحصل الكثير من الcollection فى الlink

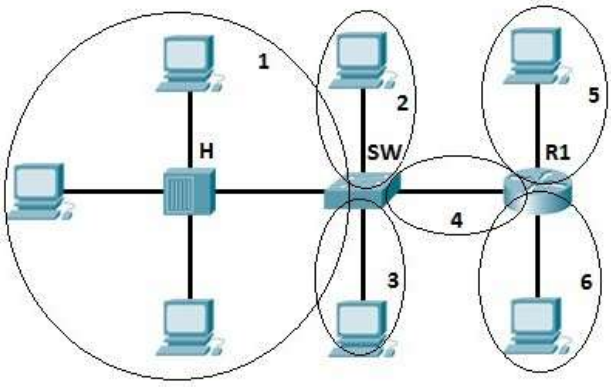
مما سبق يجب جعل الاجهزة تقوم بعمل auto netotion ولاكن اذا تم تحديد طرف للعمل كا full او كا half يلزم جعل الطرف الاخر مثله

Signal type

- يمكن تقسم الsignal تبعا للاتجاه الى :
  1. Simplex : وهى تعنى ان الsignal تذهب فى اتجاه واحد من الsource الى destination فقط مثل radio و television
  2. Half duplex : وهى ان الsignal تذهب فى كلا اتجهى الconnection ولاكن ليس فى نفس الوقت مثل police radio
  3. Full duplex : تعنى ان الsignal تذهب فى كلا اتجهى الconnection فى نفس الوقت مثل telephone
- يمكن انتقال الdata فى network بثلاث طرق :
  1. Unicast : وهو يعنى ان الsignal تذهب الى destination واحد فقط
  2. Broadcast :تعنى ان تذهب الsignal الى كل الdestination المتصلة
  3. Multicast : وهى ان تذهب الsignal الى اكثر من destination
- الrouter من الاجهزة التى تقوم بعمل تقسيم لbroadcast اى انه لايسمح لها بالعبور من شبكة لاخرى
- Broadcast domain : هى المنطقة التى اذا قام جهاز بعمل broadcast فالى اين ستصل
- Collision domain : هى المنطقة التى يمكن ان يحدث فيها unicast دون اعتراض



- ❖ فى هذه الرسمة تم تقسيم الnetwork تبعا لbroadcast domain
- ❖ فى المنطقة الاولة اذا قام ايا من الاجهزة المتصلة بعمل broadcast signal فهى ستنتقل الى جميع الاجهزة الموجودة فى المنطقة الاولة فقط ولن تسطيع ان تعبر من الروتر
- ❖ وفى المنطقة الثانية والثالثة اذا قام الجهاز الموجود بعمل broadcast signal فهى لن تمر من خلال الrouter لذالك فالrouter بقوم بتقسيم ال broadcast domain



- ❖ فى هذه الرسمة تم تقسيم الnetwork تبعا لcollision domain
- ❖ فى المنطقة الاولة اى جهاز فيها يمكنه ان يرسل unicast signal وستصل الى باقى الاجهزة فى المنطقة الاولة دون اعتراض ويمكن لswitch اعتراضها لذالك فالمنطقة الاولة تنتهى عنده
- ❖ يقوم كلا من الrouter و الswitch بتقسيم collision domain

- وجود broadcast domain كبير فى الشبكة هو واحد من اخطاء تصميم الشبكة لانه يؤدى الى ازدحام الشبكة وبطئها
- حل مشكلة الbroadcast domain هو انشاء اكثر من VLAN

Cables

- يوجد ثلاث انواع من الcables المستخدمة فى الnetwork وهم :

1. Coaxial cable

- لم تعد تستخدم الان فى الشبكات ولاكن يستخدم فى مجلات اخرى
- ذات سرعات محدودة
- تتاثر بمجال المغنطيسي

2. Twisted pair

- هو الاكثر استخداما حاليا
- يتكون من 8 اسلاك كل 2 ملفوفين حول بعضهم لذالك يسمي twisted
- عملية الtwist تقلل من تاثير الnoise وكلما ذات الtwist ذادت التكلفة بسبب ذيادة طول السلك
- ترتيب الاسلاك فى الاطراف يتبع standard لمنظمة TIA/EIA وهما اثنان 568A و 568B

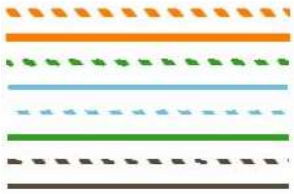
TIA 568A

Pin #	Wire Color Legend	Signal
1	White/Green	TX+
2	Green	TX-
3	White/Orange	RX+
4	Blue	TRD2+
5	White/Blue	TRD2-
6	Orange	RX-
7	White/Brown	TRS3+
8	Brown	TRD3-

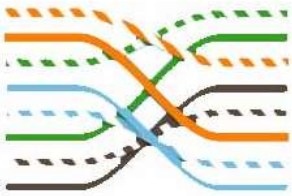
TIA 568B

Pin #	Wire Color Legend	Signal
1	White/Orange	TX+
2	Orange	TX-
3	White/Green	RX+
4	Blue	TRD2+
5	White/Blue	TRD2-
6	Green	RX-
7	White/Brown	TRS3+
8	Brown	TRD3-

Crossover Cable and Straight Through Cable

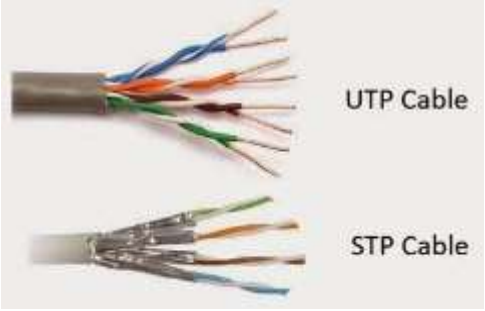


Straight Through



Crossover

- يوجد نوعان اساسيان من الtwisted pair تبعا لترتيب الاسلاك فى كلا الطرفين وهما :
  1) Straight cable
  2) Cross over cable
- فى الstraight cable كلا الطرفى 568B
- فى الcross over طرف منهم 568A والاخر 568B
- Straight cable هو المستخدم ف الاستخدمات العادية
- يستخدم الcross over مع الاجهزة المتشابهة مثل توصيل hub بhub او switch ب switch او pc ب pc او router ب router



- يوجد نوع اخر يسمى rollover وهو يستخدم لعمل configuration لrouter او لswitch
- يمكن تقسيم الtwisted pair الى نوعان تبعا لوجود shield كتالى :
- STP : هى اختصار لshielded twisted pair ويتميز بانه يحتوى على shield ملفوف حول الاسلاك لتخفيف الnoise الخارجية
- UTP : هى اختصار لunshielded twisted pair اى انه لايحتوى على shield وهذا مايجعله ارخص من STP
- تقسم الcables الى categories تبعا الى سرعتها كتالى :

Categories	speed	application
Cat 5	100Mbps	**Fast Ethernet**
Cat 5e	1Gbps	**Gigabit Ethernet**
Cat 6	10Gbps	**Gigabit Ethernet**

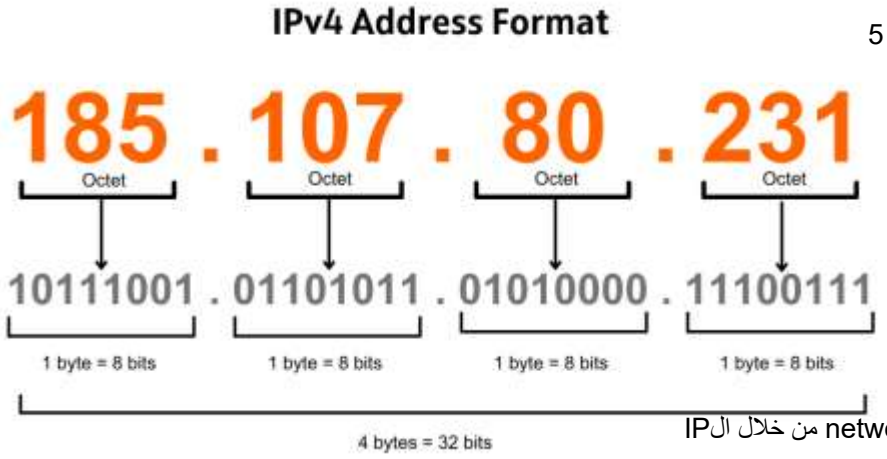
- اقصى مسافة يستعمل فيها الtwisted pair هى 100m وبعد ذالك يلزم استخدام repeater

3. Fiber optic cable

- ذات سرعات عالية جدا
- ذات تكلفة عالية
- عملية اصلاحه فى حالة القطع تكون معقدة

IP Address

- هو عبارة عن عنوان يضاف الى الجهاز لتحديده داخل الnetwork
- المنظمة المسؤلة عن تنظيم الIP addresses فى منظمة IANA
- يوجد نوعان للIP وهما ipv4 و ipv6
- Ipv4 يتكون من 4 اجزاء تسمى octet وتتراوح قيمت الoctet بين 0 و 255 اى نها تكون ذات حجم 8bit
- حجم الIPv4 كامل هو 32bit
- قامت منظمة الIANA بتقسيم الIP الى 5 classes
- class A,B,C هم ما يتم استخدمهم بشكل طبيعى
- Class D يتم استخدامه فى الmulticast
- Class E يتم استخدامه فى الresearches
- يوجد فى class A مايسمى بIP loop back وهو 127.0.0.1 ويستخدم فى اختبار TCP protocol
- الoctet المقابل ل255 فى الsubnet mask يعبر عن network id والمقابل ل0 يعبر عن Host id



- اهم وظيفة لsubnet mask هو معرفة الnetwork id من خلال الIP

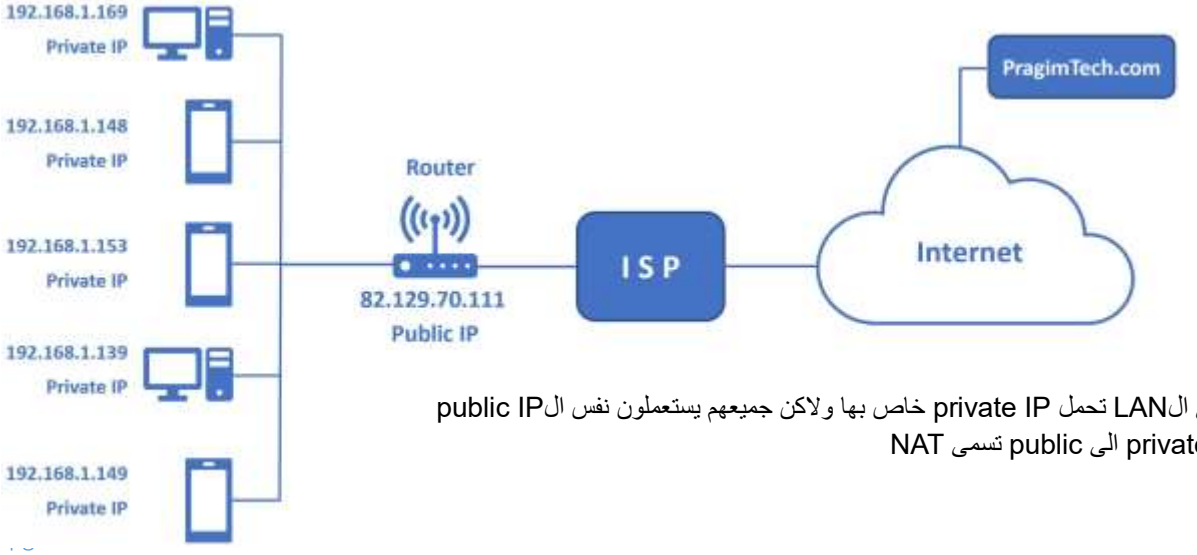
Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

Public IP& private IP

- Private IP : هو الIP يتم استخدامه داخل الLAN فقط ولايتم التعامل به فى الinternet
- Public IP : هو IP يتم استخدامه فى الinternet وهو الذى يتم اخذه من ISP
- يوجد range من private IPs فى كل class كتالى :

classes	from	to
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255



- جميع الاجهزة فى الLAN تحمل private IP خاص بها ولاكن جميعهم يستعملون نفس الpublic IP
- عملية تحويل الprivate الى public تسمى NAT

ARP protocol

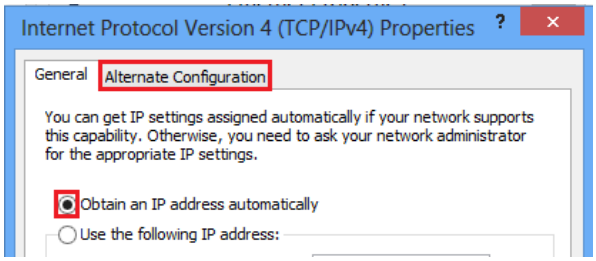
- هو protocol يستخدم داخل الشبكة الواحدة لمعرفة الDestination MAC
- خطواط عمل الARP protocol كتالى :
  1. يقوم الsource بارسال رسالة broadcast تسمى ARP request وهذه الرسالة تحمل الdestination IP
  2. يقوم الجهاز صاحب الdestination IP برد برسالة تحمل MAC address وباقى الاجهزة تتجاهل الرسالة
- Destination MAC فى رسالة الARP يكون FF:FF:FF:FF:FF:FF

Static & Dynamic IP

- Static IP : هو الحصول على IP بشكل يدوى وتسمى static لان الIP يظل ثابتا ولايتغير
- من مزاية الstatic IP انه يظل ثابتا ولذالك يستخدم فى اعطاء IP للاجهزة المهمة مثل printer وdefault gateway و الservers مثل DHCP و DNS
- من عيوب static IP انه فى حالة كانت الشبكة كبيرة سيكون من الصعب اعطائهم IP يدويا
- DHCP : وهى اعطاء IP للاجهزة بشكل تلقائى
- خدمة الDHCP تكون موجودة فى الservers وفى الroutersوالافضل استخدام الservers
- خطوات الحصول على configuration من DHCP server تتم كتالى :
  1. يقوم الجهاز بتحقق من وجود static IP له اولا
  2. اذا لم يجد سيقوم بارسال رسالة تسمى DHCP discover وهى رسالة broadcast
  3. يستقبل الDHCP الرسالة ويرسل رسالة اخرى تسمى DHCP offer وهى عرض على الclient باخذ IP
  4. فى حالة موافقة الclient على الrequest الخاص ب DHCP فانه يرسل رسالة تسمى DHCP request
  5. يقوم الDHCP باستقبال DHCP request ويرسل DHCP pack وفيها الconfiguration

- رسالة الDHCP discover تحتوى على :

Source IP	Destination IP	Source MAC	Destination MAC
0.0.0.0	255.255.255.255	The MAC of source	**FF:FF:FF:FF:FF:FF**



- Alternate IP : وهو IP يدوى يتم استخدامه فى حالة عدم الوصول الى DHCP
- Apipa IP : وهى طريقة لاضافة IP فى حالة عدم الوصول الى DHCP وعدم وجود alternate IP
- الApipa تعطى IP فى شبكة 169.254.0.0
- الIP المعطى من الApipa لايمكن استخدامه للوصول الى الinternet ولاكن يكون مفيد فى حالة التواصل مع اجهزة اخرى لم تستطع الوصول الى DHCP
- ترتيب اولوية الحصول على IP كتالى :

Frist lab

- ipconfig : هو امر لمعرفة الIP و المذيد من الconfiguration الموجودة فى الdevice
- يمكن اضافة /all مع امر ipconfig لعرض المذيد من التفاصيل مثل MAC address

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::206:2AFF:
   IP Address......................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
```

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0006.2A1B.1968
   Link-local IPv6 Address.....: FE80::206:2AFF:FE1B:19
   IP Address......................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 Client DUID..............: 00-01-00-01-85-32-
ED-79-00-06-2A-1B-19-68
```

- ping : هو امر لعمل test للconnection ويكتب بعده الIP او الDomain المراد عمل عليه test
- يمكن اضافة parameter لping وهو l– ويستخدم لتحديد حجم الpacket المرسلة ويكتب بعده الحجم بbytes
- t- هو parameter يتم اضافته الى ping ليجعل عملية الping تتم ولا تتوقف الا اذا تم ايقافها يدويا
- الping يستخدم protocol يسمى ICMP

Subnetting

- Subnetting : هى عملية تقسيم الشبكة الواحدة الى عدة شبكات
- من اهم فوائد استخدام subnetting هو تقليل الbroadcast فى الشبكة
- عملية الsubnetting تتم عن طريق التلاعب فى الsubnet mask
- تقوم الsubnetting ايضا بذيادة الsecurity فى الشبكة حيث تمنع اجهزة فى subnet من الاتصال باجهزة فى subnet اخرى
- يلزم استخدام router فى حالة اننا اردنا ان نجعل جهاز يتواصل مع اخر فى subnet مختلفة
- لكى نفهم طريقة عمل الsubnetting يلزم التعامل مع IP و subnet mask بالbinary كتالى :

0	**00000000**	**128**	**10000000**
192	**11000000**	**224**	**11100000**
240	**11110000**	**248**	**11111000**
252	**11111100**	**254**	**11111110**
		255	11111111

- فى الsubnet mask decimal الـ255 تعبر ان الoctet المقابل لها فى الIP هو الخاص بالشبكة بينما الـ0 يعبر ان الoctet المقابل له فى الIP هو خاص ب devices
- فى الsubnet mask binary يشير 1 الى ان الbit المقابل له فى الIP هو الخاص بالشبكة بينما 0 يعبر ان الbit المقابل له خاص بdevices

IP	**192.168.1.1**	**192.168.1.1**	**192.168.1.1**
mask	255.255.255.0	255.255.255.128	**255.255.255.192**
Classful or less	Classful	Classless	**classless**
no. network	1 network	2 network	**4 network**
Last octet in mask	00000000	10000000	**11000000**

- Classful تعنى ان الsubnet mask طبيعيى بدون تغيير ولايوجد subnetting
- Classless تعنى ان subnet mask ليس طبيعى ويوجد subnetting
- عدد الnetwork يتم حسابه من علاقة $2^{\text{عدد}1}$ (اثنان مرفوعة لاس عدد الوحايد فى subnet mask)
- عدد الdevices يتم حسابه من علاقة 2- $2^{\text{عدد}0}$ (اثنان مرفوعة لاس عدد الاصفار فى subnet mask مطروح منها اثنان)
- فى اى شبكة اول واخر IP لايتم استخدامهم على سبيل المثال 192.168.1.0 لانه هو network ID و 192.168.1.255 لانه هو الخاص بbroadcast

سؤال : كيف يمكننا انشاء اربع شبكات 192.168.1.0 ذات subnet mask وهو 255.255.255.0

الحل :

اربع شبكات تعنى انه يوجد اثنان من 1 فى الsubnet mask اى انه سيكون كتالى 11000000 والتى تعنى انه سيكون 255.255.255.192 وسيتم تقسيم الشبكة الى الاتى :

subnet	binary		decimal	
	from	to	from	to
1	00000000	00111111	192.168.1.0	192.168.1.63
2	01000000	01111111	192.168.1.64	192.168.1.127
3	10000000	10111111	192.168.1.128	192.168.1.191
4	11000000	11111111	192.168.1.192	192.168.1.255

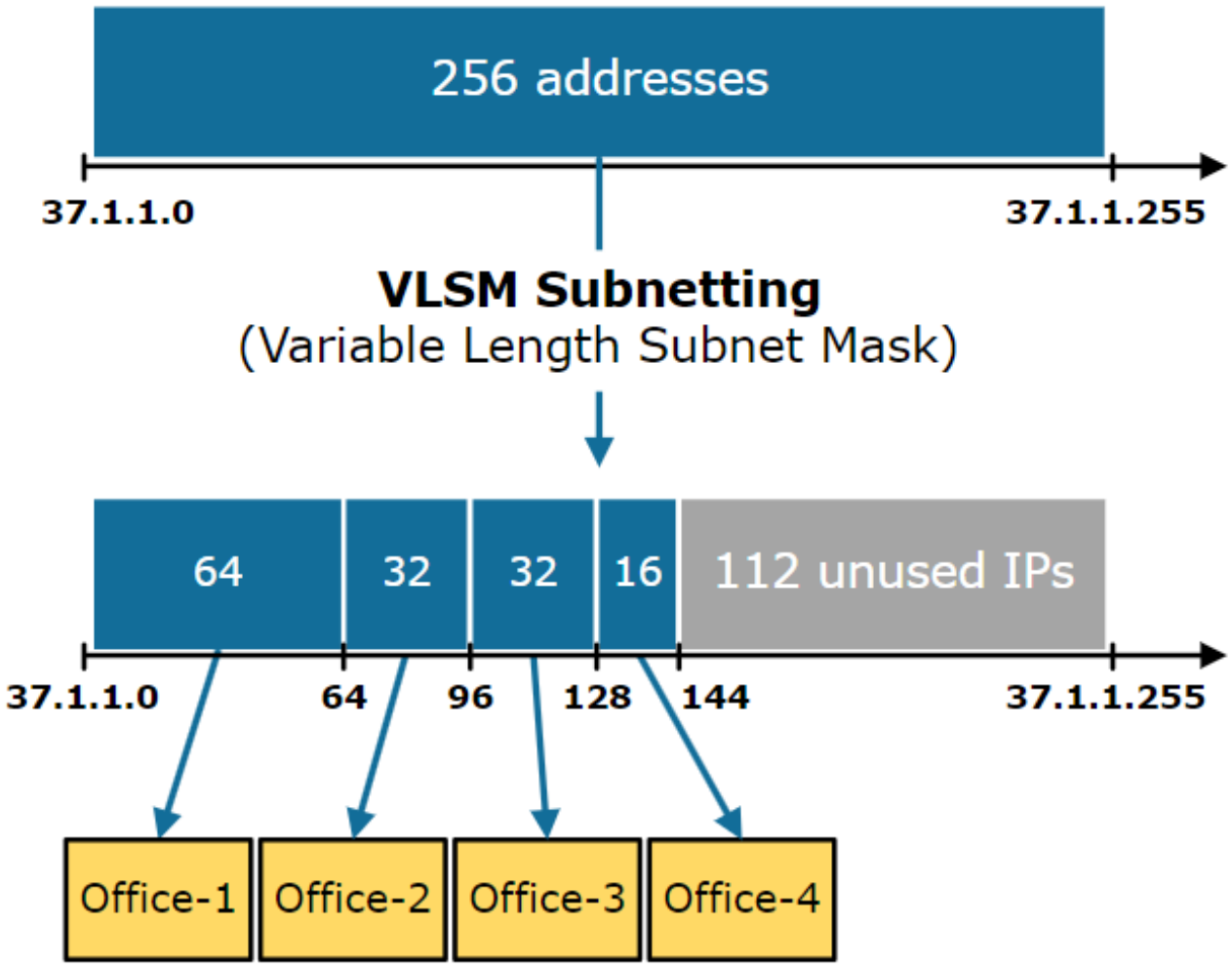
- ❖ فى كل subnet لايتم استخدام اول واخر IP
- ❖ توجد طريقة اخرى فى كتابة الmask وهى اننا نضع / ثم رقم وهذا الرقم هو عدد الوحايد فى الsubnet mask كتالى :

255.255.255.192 ⟶ /26 255.255.255.0 ⟶ /24

ويكتب مع الIP كتالى 192.168.1.0/24

VLSM

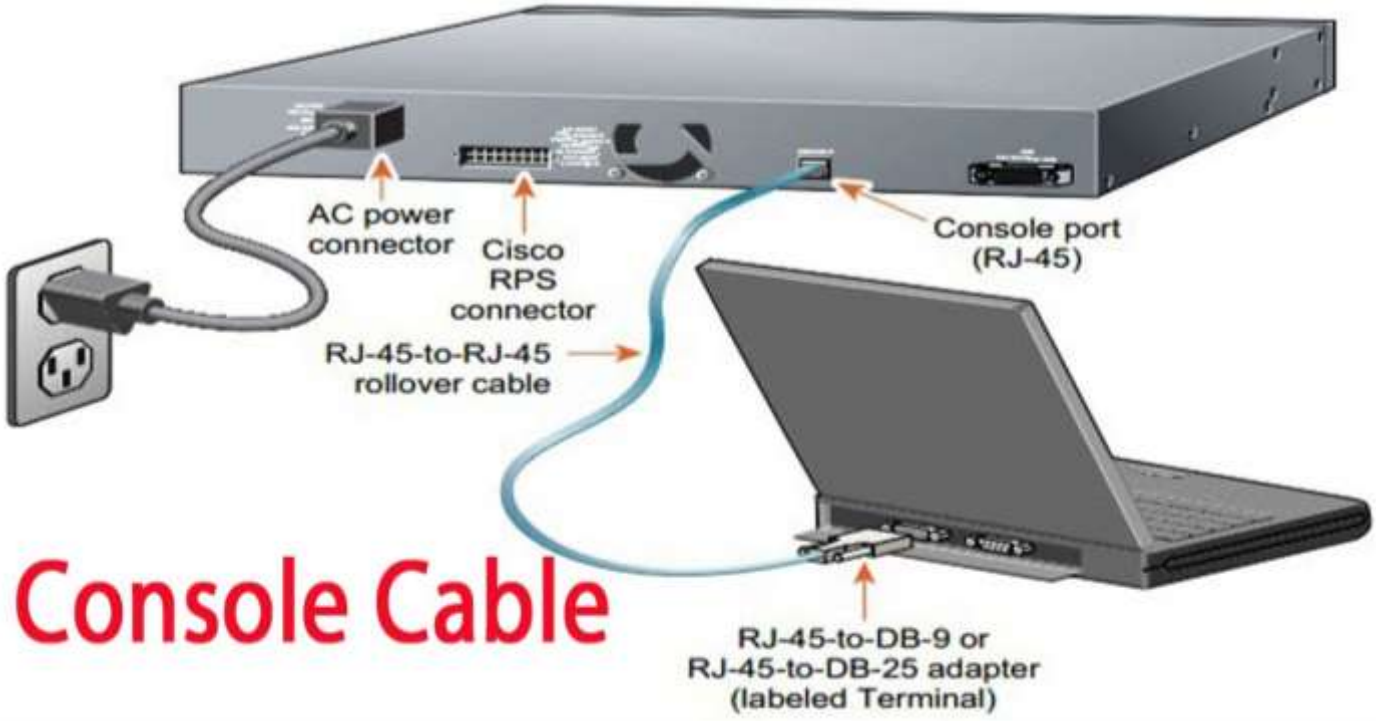
- VLSM : هو اختصار لvariable length subnet mask
- VLSM هو استخدام الsubnetting فى انشاء اكثر من subnet وتحديد عدد hosts لكل subnet
- الsubnetting ينتج عنه عدد متساوى من الhosts فى كل subnet لذالك نحتاج الVLSM
- استخدام subnetting العادى سينتج عنه وجود شبكات تحتوى على hosts اقل من التى تحتاجه الشبكة و شبكات اخرى غير كافيه للاجهزة
- يتم الVLSM عن طريق عمل subnetting لsubnet
- خطواط عمل VLSM كتالى :
  1. ايجاد اكبر شبكة تحتاج الى hosts ومن خلال عدد الhost يمكن معرفة عدد 0 فى الsubnet mask
  2. بعد معرفة عدد 0 يمكننا ايجاد subnet المناسب وتقسيم الشبكة
  3. بعد التقسيم سوف ناخذ جزء ونعطايه لاكبر شبكة تحتوى على hosts
  4. باقى الاجزاء سنقسمها بنفس الطريقة على باقى الشبكات
- VLSM تسمى ايضا supernetting



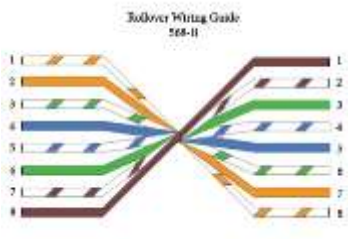
Router basics

- Router : هو device وظيفته الاساسية هو ربط الشبكات معا
- الrouter يحتوى على الاقل على 2 interface

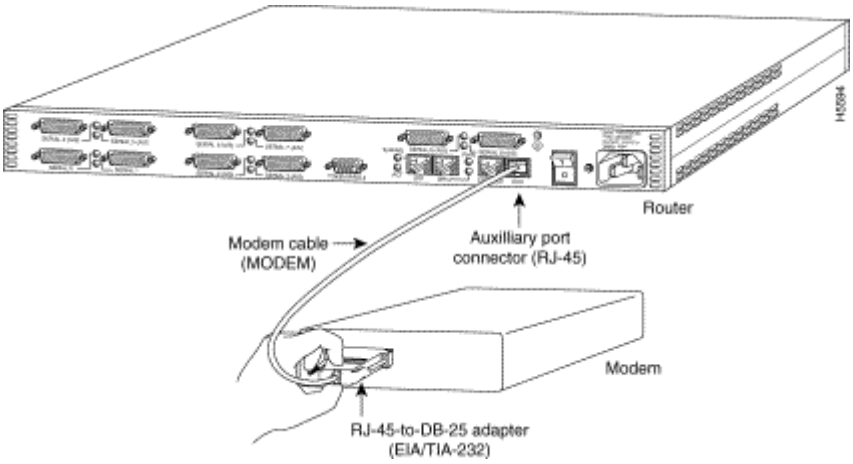
- Serial ports تستخدم ل WAN Technology
- Fast Ethernet و console و auxiliary جميعهم يستخدمون RJ45
- فتحة console و auxiliary يطلق عليهم configuration ports



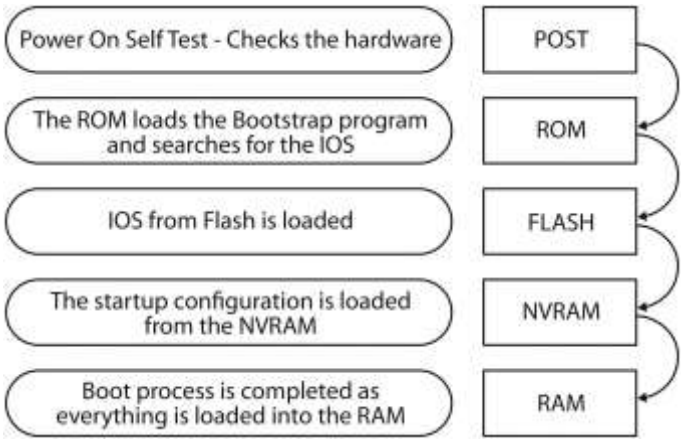
- Fast/Giga Ethernet يطلق عليهم connection ports
- عند وجود عدد قليل من Ethernet port نلجئ الى كرت يسمى wic لذايدة عددهم
- عند استخدام فتحة الconsole لعمل configuration من الpc او laptop نقوم باستخدام الاتى :
  1. PC or laptop
  2. Twisted pair rollover cable
  3. Converter from RJ45 to DB-9 or DB 25
- Rollover cable يكون twisted pair cable ولاكن طرف 568B والاخر 568B ولاكن معكوسة
- اذا لم يتواجد DB-25 or DB-9 فى الPC يمكن الاتيان بconverter من DB-9/DB-25 to USB



- لكى نقوم بعمل الconfiguration سنقوم باستخدام software مثل hyper terminal
- يمكن عمل configuration ولاكن من فتحة الauxiliary والاختلاف بينها وبين الconsole هو ان الauxiliary تتم بشكل remotely وانها تتصل بmodem وليس بpc
- يوجد بداخل اى router المكونات الاتية :



1. ROM
   - اهم وظيفة لها وهى POST وتعنى power on self-test وهى عمليه التحقق من hardware الموجودة قبل بدا التشغيل
   - هى تشبه عملية الbios فى الpc
2. Flash memory
   - هى chip قابلة لتخزين عليها
   - يوضع عليها OS الخاص بrouter
   - الOS يكون comprise فى الflash memory لتوفير مساحة اكثر وحمايته من الviruses
   - يمكن ان تحتوى على اكثر من IOS
3. RAM
   - يتم وضع عليها العمليات التى تتم
   - يوضع عليها routing table و running configuration
   - Running configuration هم الconfiguration التى يتم اضافتها فى الrouter و لم يحدث لها save بعد
   - قابلة لفقد البينات التى عليها بمجرد انقطاع التيار
4. NVRAM
   - هى اختصار ل none volatile RAM
   - تحفظ عليها الconfiguration file
   - لاتفقد البينات بمجرد انقطاع التيار



- عند عمل power up يتم الاتى :
- اول خطوة تتم هى POST وفيها يتم التحقق من جميع الhardware
- بعد التحقق من الhardware تبدا عملية البحث عن الIOS
- تبدا عملية البحث عن الIOS من الNVRAM لانه يحتوى على ملف يشير الى IOS الذى فى الflash الذى سوف يتم استخدامه
- عند ايجاد الIOS يتم عمل له load على الRAM
- بعد ذالك يتم عمل load للconfiguration الموجودة فى NVRAM

Router mode

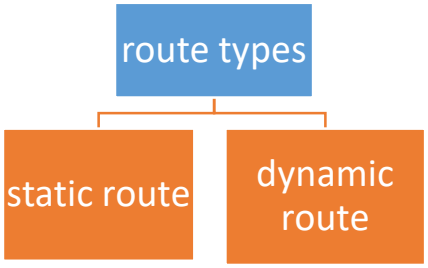
1. User mode
   - يمكن فيه تطبيق الاوامر ولاكن ليست جميعها
   - Tracer الخاص بالكتابة تكون على هذا الشكل **Router>**
2. Privileged mode
   - تطبق فيها جميع الاوامر وهي تشبه الadmin mode فى الpc
   - Tracer الخاصة بالكتابة تكون على شكل **Router#**
   - لدخول الى privileged mode يجب كتابة **ena** وهى اختصار ل enable
   - للخروج منه والعودة الى user mode نكتب **exit**
3. Global configuration mode
   - هو الmode الخاص بعمل الconfiguration
   - Tracer الخاصة بالكتابة تكون على شكل **Router (config)#**
   - لدخول الى configuration mode نكتب امر **config t**
   - لرجوع من الconfiguration mode الى privileged نكتب **exit** واذا اردنا الرجوع الى user mode نكتب **exit** مرة اخرى

Command	Description	Example	mode
hostname	• يقوم بتغير اسم الrouter	Hostname Cairo	Configuration mode
Show clock	• يقوم بعرض الوقت الحالى	Show clock	Privileged/user mode
do	• يقوم بتنفيذ اوامر privileged فى الconfiguration mode	do show clock	Configuration mode
Clock set	• امر يقوم بتعديل الوقت • يلزم وضع الوقت كما هو موضح	Clock set 8:05:00 17 Feb 2024	Privileged mode

wr	• يقوم بحفظ الconfiguration	wr	Privileged mode
Copy run start	• يقوم بحفظ الconfiguration	Copy run start	Privileged mode
interface	• نقوم بدخول من خلاله الى interface معينة لعمل configuration	Interface gigabitEthernet 0/0	Configuration mode
no shutdown	• لتشغيل الinterface	no shutdown	Configuration mode inside interface
shutdown	• يقوم باطفاء الinterface	shutdown	Configuration mode inside interface
ip address	• يقوم باضافة ip وsubnetmask لinterface	ip address 192.168.1.1 255.255.255.0	Configuration mode inside interface
Show ip interface br	• يقوم بعرض حالة كل interface و الip الخاص بها	Show ip interface br	Privileged mode
no ip address	• تستخدم فى اذالة الip من الinterface	no ip interface	Configuration mode inside interface
Show ip route	• يستخدم لعرض routing table	Show ip route	Privileged mode
Ip dhcp pool	• هو امر لانشاء DHCP scope • كلمة pool هنا تعنى scope • يكتب بعده اسم الdhcp scope • يمكن اضافة no قبل الامر لازالته	Ip dhcp pool s1	Configuration mode
network	• هو امر لانشاء شبكة • يكتب بعد انشاء dhcp pool • ياخذ الnetwork ID و ال subnet mask	Network 192.168.1.0 255.255.255.0	DHCP Configuration mode
default-router	• هو امر اعطاء default gateway	default-router 192.168.1.1	DHCP Configuration mode
dns-server	• هو امر اعطاء dns	dns-server 8.8.8.8	DHCP Configuration mode
Ip dhcp excluded-address	• هو امر لعمل exception من ip معين او من range من الips	ip dhcp excluded-address 192.168.1.10 ip dhcp excluded-address 192.168.1.10 192.168.1.20	Configuration mode

Routing

- Routing : هو عمليه توجيه الdata من router الى اخر للوصول الى الdestination
- routerال يستطيع رؤية الشبكات المتصلة به بشكل direct فقط
- فى حالة كان routerال غير متصل بشبكات اخرى بشكل مباشر فانه لكى يراها يجب ان نستعمل routing protocol
- Routing protocol هو protocol يقوم بمشاركة routing tableال بين routerال والاخر
- لكى تتم عملية routingال يلزم معرفة الاتى :
  1. Destination address
  2. Possible routs
  3. Best route



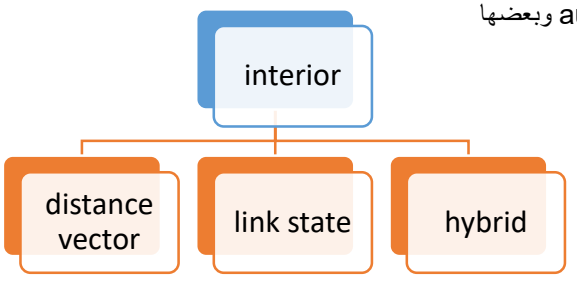
- Static Route : وهى تتم بشكل manual من خلال network administrator
- من عيوب الstatic route انه عند حدوث تغيير فى الشبكة يلزم تعديل الconfiguration
- من مزايا الstatic route انه يقلل الحمل على routerال ويقوم بذيادة الsecurity
- Dynamic route : وهى تتم من خلال واحد من الrouting protocol بشكل dynamic
- لكى نقوم بعمل routing بشكل عملى نقوم بعمل الاتى :

Configuration mode	ip route 200.200.200.0 255.255.255.0 10.0.0.1 no ip route 200.200.200.0 255.255.255.0 10.0.0.1	• هو امر لعمل routing • نكتب بعده الشبكة المراد اضافتها والmask الخاص بها ثم نضيف الnext hop • Next hop هى الinterface التى فى routerال الاخر والذى سيكمل عملية routingال • يمكن اضافة no لنفس الامر لاذالته من route tableال	**Ip route**

- Default route : تعنى انه فى حالة ارسال رسالة الى network اخرى فانه سيتم توجيه الرسالة الى routerال التالى مهما كانت هذه الnetwork
- مستخدمة بكثرة فى شبكة الinternet خاصة فى routersال المتصلة ب ISP
- تتم عن طريق كتابة امر ip route 0.0.0.0 0.0.0.0 ثم الnext hop فى routerال التالى
- AD وهى اختصار ل administrative distance وهو رقم لكل routing protocol
- Static route الADال الخاص به هو 1
- يمكن تشغيل اكثر من routing protocol فى نفس الوقت ولاكن الافضليه تكون لصاحب اقل AD
- Default route الADال الخاصة به هى 255

Dynamic route

- من اهم مزاية الdynamic route انه فى حالة حدوث اى تغيير فى الشبكة فان الrouting protocol يقوم بتبليغ routersال بهاذا التغيير
- Autonomies system هو نظام مكون من مجموعة من routersال تحت تحكم منظمة واحدة
- تختلف انواع routing protocol تبعا لوجودها داخل او خارج الautonomies system الى interior و exterior
- Interior هو الrouting protocol الموجود داخل الautonomies system
- Exterior هو الrouting protocol الموجود خارج او بين الautonomies systems وبعضها
- من الprotocols المستخدمة فى الexterior هو BGP
- interiorال ينقسم الى ثلاث انواع كما هو موضح
- الprotocol الذى يمثل الdistance vector هو RIP protocol
- كل نوع من انواع الinterior protocol له metric مختلفة
- Metric : هى الطريقة التى من خلالها يحدد الprotocol افضل path فى عملية routing
- فى الdistance vector يتم تحديد الmetric بناء على hop count اى انه يعتبر افضل path هو الذى يحتوى على اقل عدد من routersال
- الprotocol الذى يمثل الlink state هو OSPF
- الmetric فى الOSPF هو speed اى انه يفضل المسار الاسرع
- الprotocol الذى يمثل الhybrid هو EIGRP والmetric الخاصة به هى speed و Reliability و delay
- فى حالة تساوى الmetric فى اى routing protocol سيتم عمل load balance



RIP

- RIP له العديد من الversion منهم 1 و 2 و3 حيث ان v1 و v2 يتم استخدمهم فى IPv4 بينما v3 تعمل على IPv6
- يتم اطلاق احيانا على RIP v3 ب RIP_{NG} وتعنى next generation
- الفرق بين RIP v1 و RIP v2 ان v1 هو classfull اى انه لا يدعم subnetting بينما v2 يكون classless

- RIP v1 يقوم بمشاركة الrouting table عن طريق رسالة broadcast بينما باقى الprotocols يقوموا بذالك عن طريق multicast
- RIP v2 يقوم بعمل multicast على 224.0.0.9
- RIP نادر الاستخدام حاليا
- لكى نقوم بتشغيل الRIP فى الrouter نستعمل الاوامر الاتية :

Configuration mode	Router rip	
Configuration mode inside rip protocol	Version 2	**Router rip** • يستخدم لتشغيل RIP v1 فى الrouter
Configuration mode inside rip protocol	Network 192.168.1.0	**Version 2** • يستخدم لتغيير الversion الى v2
		network • تستخدم لاضافت network المتصلة ب الrouter الى rip لكى يقوم بنشرها • اذا لم تضاف شبكة فان الrip لن يقوم بنشرها وتستخدم هذه الحالة لاغراض الsecurity • ياتى بعدها network ID المراد اضاقتها

- الRIP يشارك الrouting table كل 30 ثانية وهى ايضا من عيوبه لانه يملئ الشبكة
- Trigger update هى مشاركة الrouting table عند حدوث تغيير
- الRIP يدعم trigger update حيث انه فى حالة حدوث تغيير فى الnetwork سيتم ارسال التغيير قبل انتهاء ال30 ثانية
- يمكن اضافة no قبل امر network لازالة شبكة من الrip او no قبل امر router rip لازالة الrip
- الAD الخاصة ب rip هى 120

EIGRP

- هو من الprotocol التى تستخدم الان
- هو اختصار ل enhanced interior gateway routing protocol
- يتميز الEGRP بالاتى :
  1. Classless protocol ای انه یدعم الsubnetting
  2. Fast convergence ای انه فى حالة حدوث خطاء فى path فانه ينتقل بشكل سريع جدا الى path اخر وهذه من اهم مميزاته
     - عندما يتصل الEIGRP بbest path فانه ياخذ backup من باقى الpaths ويقوم بحفظها وهذا ما يجعله سريعا جدا فى عملية fast convergence
  3. Sent packet on 224.0.0.10
  4. Administrative distance = 90
  5. Metric = bandwidth + delay +reliability
- EIGRP يهتم ب الautonomous system ولذالك اذا كان هناك اكثر من router فى autonomous systems مختلفة فلن يستطيعو التواصل
- يمكن ترقيم الautonomous system من 1 الى 65535
- يتم تشغيل الEIGRP فى الrouter بالاوامر الاتية :

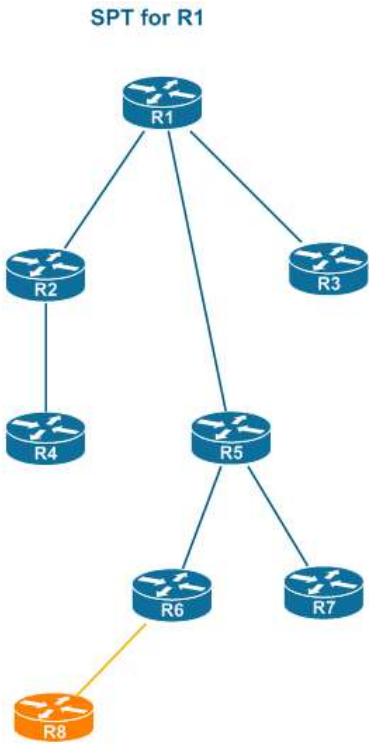
Configuration mode	Router EIGRP 2	
Configuration mode inside rip protocol	Network 192.168.1.0	**Router EIGRP** • يستخدم لتشغيل EIGRP • يلذم اتباع الامر ب رقم ال autonomous system
		network • تستخدم لاضافت network المتصلة ب الrouter الى EIGRP لكى يقوم بنشرها • ياتى بعدها network ID المراد اضاقتها

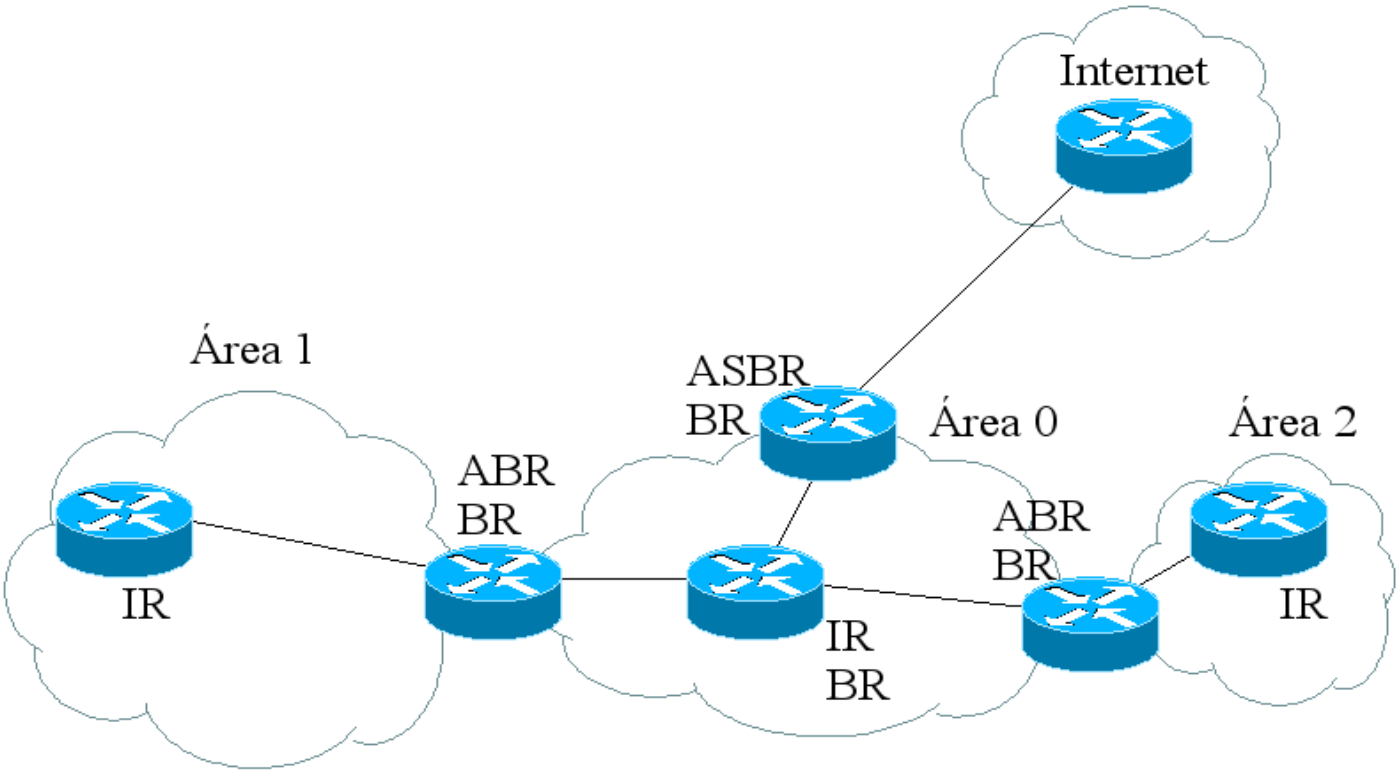
OSPF

- هو اختصار ل open shortest path first
- يتميز بالاتى :
  1. Standard protocol ای انه یعمل على جميع الvendor
  2. Classless protocol ای انه یدعم الsubnetting
  3. Sent packet in 224.0.0.5
  4. AD الخاص به هى 110
  5. Metric= cost =2^8/bandwidth

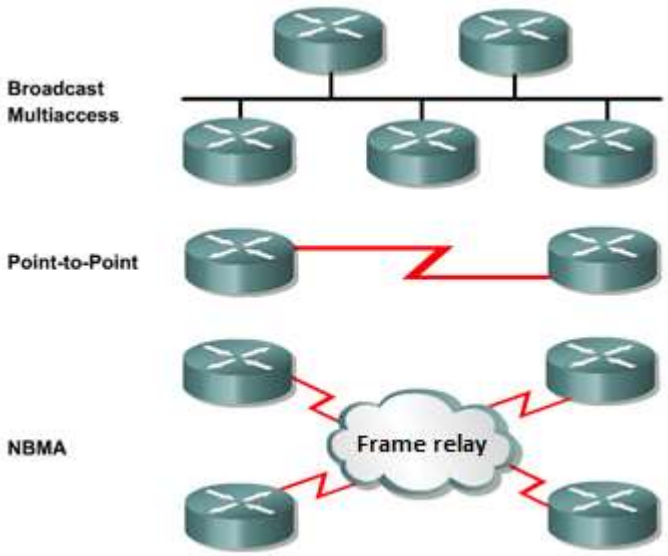
6. Loop free topology
7. Unlimited Number of hop count
   - اى انه يعمل فى الشبكات الكبيرة

- فى الOSPF الroutersلايقومو بتبادل الrouting table ولاكن يتبادلو ما يسمى ب LAS
- عند استعمال الOSPF فان كل router سيملك خريطة كاملة باماكن الroutersالاخرى وكيف يصل اليهم
- عند تفعيل الOSPF يحدث الاتى :
  1. كل router يقوم بارسال رسالة تسمى hello message لكى يستكشف الnetwork المحيطة
  2. يقوم كل router بارسال رسالة LSA وهى اختصار ل link state advertisement
     - رسالة الLSA تحتوى على معلومات من الrouter مثل router ID و الinterfaces و الIP لكل interface
  3. الroutersالتى ستستلم رسالة LSA ستقوم بحفظ الinformation فى database تسمى link state database واحيانا تختصر ل LSDB
     - LSDB يتم اطلاق عليها ايضا topological database
  4. يقوم كل router برسم ما يسمى ب shortest path first Tree (SPF tree) ويكون هو الroot
  5. بناء على الSPF يتم انشاء الrouting فى الrouter
- بناء على ما سبق فانه يوجد ثلاث انواع من الtable
  1. Neighbor table وهو الlink stat database
  2. Topology table هو الSPF tree
  3. Routing table وهو الشكل النهائى
- لكى نقوم بتشغيل OSPF من الrouter نقوم باستخدام امر router ospf ثم نتبعه برقم وهو process id
- الprocess id هو رقم لتنظيم لا اكثر
- لاضافة network الى الOSPF نستخدم امر network ولاكن لانعطيه الsubnet mask الطبيعي بل نعطيه wild card mask ثم نكتب area 0
- Wild card mask هو عكس الsubnet mask اى ان ال255 تصبح 0 و 0 تصبح 255
- الwild card mask هو الsubnet من وجه نظر الhosts
- Area هى طريقة ظهرت لكى تقلل الاذدحام الناتج عن OSPF protocol وهى تقوم على تقسيم الnetwork الى areas
- كل area تقوم بارسال الupdates التى تحدث فى network للroutersالموجودين فى نفس الareaفقط
- الareaالاساسية هى area 0 وهى يجب ان تكون موجودة وتسمى backbone area وتتصل كل area





- اى update يحدث لاى area يذهب الى area 0 وكذالك area 0 ترسل التغيرات الى باقى الareas
- هناك ثلاث انواع من الconnection ستكون موجودة فى OSPF كتالى :
- Broadcast multi-access هو عندما تكون جميع الroutersمتصلة معا بswitch اى انهم يكونو فى broadcast domain واحد
- Point to point عندما يتصل two routers بشكل مباشر
- NBMA هى حالة حيث تتصل الroutersب frame relay وهو نوع من الWAN technology
- NBMA يتطلق عليها hub & spoke
- NBMA هى اختصار ل non broadcast multi-access
- فى OSPF يقوم الrouterبارسال الupdate كل 30 دقيقة
- فى حالة توصيل الroutersبشكل broadcast multi-access وتفعيل عليهم OSPF سيتم تحديد router منهم لكى يكون DR (designated router)
- designated router هو الrouterالاساسى اى ان باقى الroutersيقومو بارسال الupdate اليه فقط وهذه العملية تتم من تجل تخفيف الاحمال فى الnetwork
- يتم اختيار ايضا BDR وهو backup designated router وهو router سيحل محل الDR فى حالة تم فقد الاتصال به
- عمليه اختيار DB تتم فى 40 ثانية
- DR election (عملية اختيار الDR) تتم بناء على :
  1. Router priority
     - تتراوح قيمتها بين 1 الى 255
     - القيمة الdefault لكل router تكون 1
     - صاحب القيمة الاعلى هو ما سيحصل على لقب DR
  2. Router ID
     - بمكن اعطائه لrouterبشكل manual
     - اذا لم يعطى بشكل manual سيتم اخذه تبعا لhighest ip address
     - يمكن ان تحدث مشكلة عند استخدام highest ip address وهو سقوط الinterfaces التى تحتوى على اعلى ip ولتفادى هذه المشكلة نقوم بانشاء loop back interface وهى interface وهمية نضع لها الhighest ip

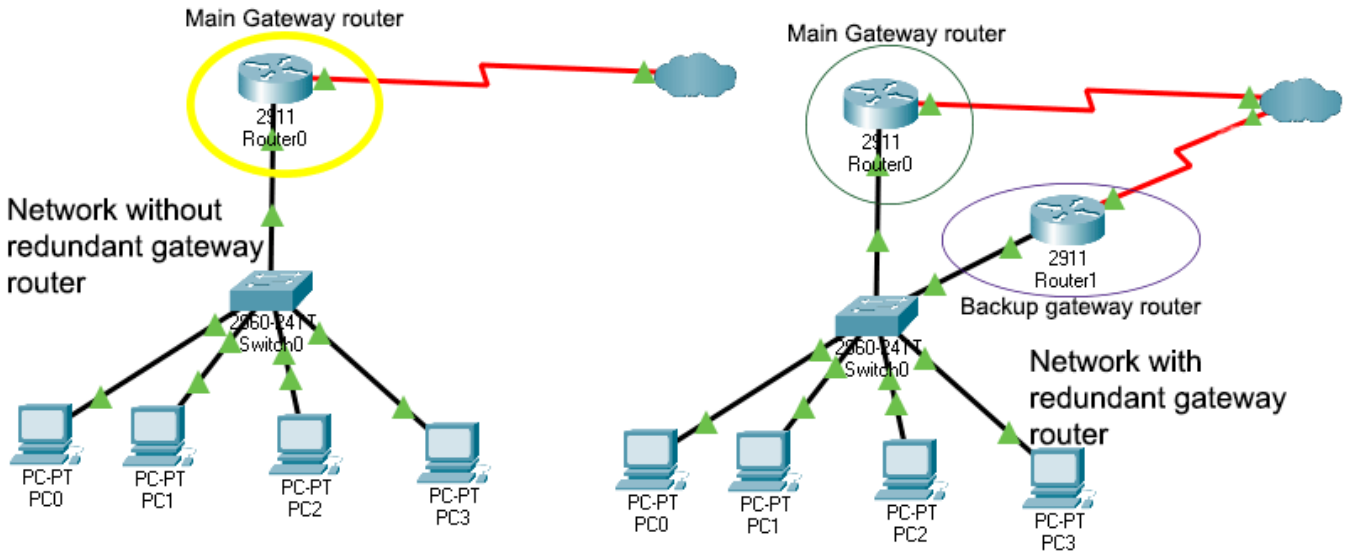


Show ip ospf ne	• هو امر لرؤية من هو DR ومن هو BDR • يستخدم هذا الامر على اى router	Show ip ospf ne	Privilege mode
Router-id	• يستخدم لاعطاء id للrouterبشكل manually • يكتب الidعلى شكل ip	Router-id 66.0.0.1	Configuration mode inside ospf
Int loopback	• تستخدم فى عمل loopback interface • تكتب بعدها رقم الinterface • يمكن استخدام امر ip address لاضافة ip لهذه الinterface	Int loopback 1	Configuration mode
Ip ospf priority	• يستخدم لاضافة priority • يجب استخدامه داخل interface معينة	Ip ospf priority 35	Configuration mode inside interface
Show ip protocols	• هو امر لظهار الprotocolsالتى تعمل على الrouterمع المذيد من التفاصيل	Show ip protocol	Privilege mode
Show ip route ospf	• يقوم بعرض المعلومات الخاصة بospfفقط فى ال routing protocol	Show ip route ospf	Privilege mode
Show ip ospf interface	• يقوم بعرض معلومات مفصلة عن كل interface ومعلومات الospfلها	Show ip ospf interface	Privilege mode

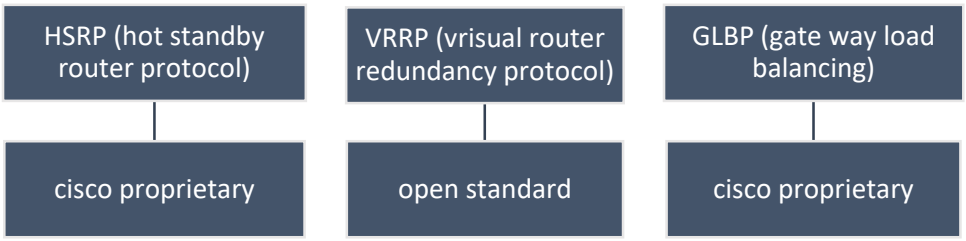
- عند تغيير ال priory او router ID لكى نغير الdesignated routerلا يحدث هذا التغير فورا
- باقى الroutersترسل الLSA ل DR والDR هو من يقوم بجمعهم معا ويرسلهم الى باقى الrouters
- عمليه ارسال الLSA لDR فقط مثلها مثل عملية ارسال LSA ل area 0 فقط تقوم على تخفيف الاحمال على الnetwork
- عمليه ارسال LSA الى DR تتم على 224.0.0.6 بينما عملية ارسال LSA من DR الى باقى الroutersتتم على 224.0.0.5

Redundancy protocol

- عملية الredundancy هى عملية المقصود منها توفير اكثر من طريقة لانشاء connection لتغلب على fault tolerance
- عملية الredundancy فى الrouter تستخدم لوضع اكثر من router لعمل نفس الconnection



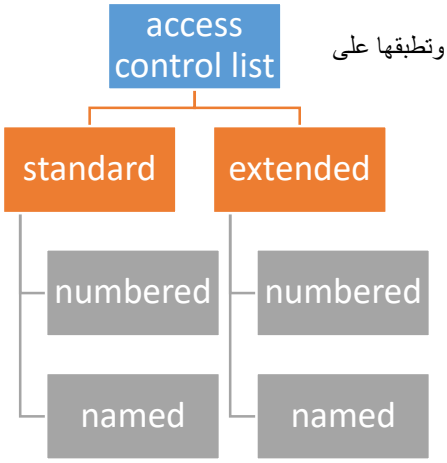
- عند عمل redundancy فى الrouter يلزم ايجاد طريقة لتغيير الdefault gateway بشكل automatically وهذه الطريقة هى redundancy protocol
- يوجد ثلاث انواع من الredundancy protocol وهم :



- عند تفعيل واحد من الprotocols على routers يتم اختيار واحد هو الactive والاخر هو standby
- فى HSRP يقوم active router بارسال رسالة كل 3 ثوانى وتسمى hello message ل standby لاعلامه انه مازال يعمل واذا لم يتلقى الstandby هذه الرسالة خلال 10 ثوانى سيقوم بجعل نفسه الactive
- VRRP يعمل بنفس الطريقة ولاكن الhello message تتم كل ثانية وhold ياخذ 3 ثوانى فقط
- الHSRP و VRRP كلاهما لا يستخدمان اكثر من 2 gateway
- الGLBP يعمل بطريقة مختلفة وهى انه لايوجد active و standby ولاكن كل الrouters تعمل معا فى نفس الوقت وتوزع المهام بينهم ب load balance
- الGLBP يسمح ب 4 gateway
- فى الHSRP و VRRP يتم انشاء virtual ip ونجعلعه هو default gateway

Standby # ip	• يستخدم لتشغيل HSRP • لا يستعمل الا بعد عمل الconfiguration الطبيعية للinterface • # هنا يوضع مكانه رقم والرقم غير مهم • بعد ذالك يتم كتابة الvirtual ip • يجب الالتزام بالرقم والvirtual ip فى الrouter المقابل	Standby 5 ip 192.168.1.50	Configuration mode inside interface
Show stand	• يستخدم لمعرفة هل الrouter هو الactive ام الstandby	Show stand	Privileged mode

Access control list



- Access control list هى طريقة ل security تقوم بتحديد امكانية اتصال جهاز او شبكة بجهاز او شبكة اخرى
- يوجد انواع كثيرة من access list ولاكن اشهرهم هم standard و extended
- تتم الaccess control list تتم عن طريق عمل list بكل الaccess المسموحة والغير مسموحة وتطبقها على Interface معين فى الrouter
- لا يمكن وضع اكثر من access list 2 على الinterface الواحدة
- يلزم تحديد الaccess ان كان على الsignal الذاهبة للinterface او لsignal الخارجة منها
- يتم تحديد اتجاه الsignal من و الى الinterface بناء على مسار الsignal من الsource الى destination

extended	standard
ياخذ ترقيم من 100 الى 199	**ياخذ ترقيم من 1 الى 99**
يتم التحكم من خلال عنوان source و destination و الprotocol(port)	**يتم التحكم من خلال عنوان الsource**
يمكن تحديد جهاز او عدد اجهزة فقط الغير مسموع بالاتصال بها والباقى يمكن الاتصال به او تحديد خدمة واحدة او اكثر الغير مسموح او المسموح الاتصال بها	**تسمح او تمنع الاتصال كامل**
يفضل تحديد الaccess list على اقرب interface للsource	**يفضل تطبيق الaccess list على اقرب interface لل destination**

- الترتيب فى الlist مهم والاولوية للسطور الاولة
- يوجد سطر ف الaccess list غير مرئى وهو deny any وهو اخر سطر ويقوم بمنع باقى الاجهزة او باقى protocols التى لم تحدد فى الaccess list
- فى حالة اننا اردنا ايقاف سطر deny any نقوم بوضع سطر permit any فى اخر الaccess list
- اثناء عمل deny او permit لشبكة يجب استخدام الwild card mask

Standard

Access-list	• هو امر لعمل access list او لاضافة permit او deny لaccess list موجودة بالفعل • يكتب بعده رقم الaccess list وهو بين 1 و 99 • لايجب نسيان وضع permit any لسماح بباقى الاجهزة بالاتصال	Access-list 1 deny 192.168.1.2 Access-list 2 deny 10.0.0.0 0.255.255.255 Access-list 1 permit any	Configuration mode
Ip access-group	• تستخدم لتطبيق access list على interface معينة • يكتب بعده رقم الaccess list المراد تطبيقها على الinterface • بعد تحديد رقم الaccess list يتم تحديد هل هى in ام out	Ip access-group 1 out	Configuration mode inside interface
Show ac	• يستخدم لمعرفة الaccess list الموجودة	Show ac	Configuration mode
No access-list	• يستخدم لازالة access list من الrouter • يتم وضع رقم الaccess list بعده • لا يمكن ازالة سطر من ال access list وانما تزال كلها	No access-list 1	Configuration mode

Extended

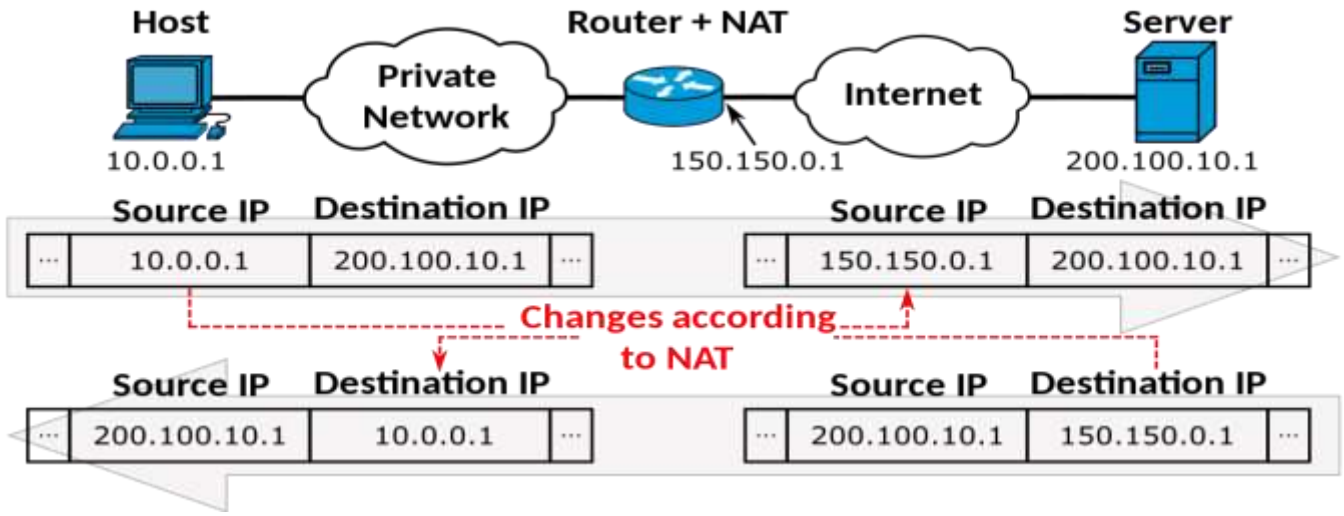
Access-list	• عند استخدمها كا extended نقوم باعطائها رقم ثم امر deny او permitال ثم نكتب tcp host ثم source ip ثم host ثم destination ipال وفى النهاية eq ثم port number	Access-list 100 deny tcp host 192.168.0.2 host 10.0.0.9 eq 80 Access-list permit ip any any Access-list deny tcp 192.168.1.0 0.0.0.255 eq 80	Configuration mode

	• كتابة tcp ليست ثابتة وانما تتغير من protocol الى اخر حسب استخدامه للTCP او للUDP • عند وضع ip بدل كلمة tcp فانه سيقوم بتطبيق الdeny او الpermit على كل الprotocols القادمة من الsource • كلمة host تضاف فقط عند التعامل مع الhosts وليس الشبكة • عند التعامل مع الشبكة نضيف wild card mask	Access-list 150 Deny ICMP 10.0.0.0 0.255.255.255 host 192.168.1.100 echo	
Ip access-group	• يتم استخدامها كما تستخدم فى الstandard • لايمكن للinterface استيعاب اكثر من access list 2 ويجب ان يكونوا واحدة in وواحدة out	Ip access-group 100 in	Configuration mode inside the interface

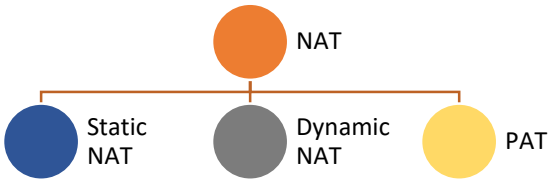
- الشكل السابق يسمى الnumbered access list حيث اننا نستخدم ارقام لتسمية الlist ولاكن يوجد نوع اخر وهو named access list
- الnamed access list عند اشائها بدل كتابة رقم الlist نقوم بكتابة standard او extended على سبيل المثال : ip access-list extended sales

Network address translation

- هى تقنية تم انشائها لتقليل استهلاك IPv4 عن طريق تحويل public ip الى private ip



- الpublic IP يتم اخذه من خلال ISP وهو يتغير فى كل مرة يتم اتصال الrouter بها ولاكن يمكن شراء الIP من ISP وهذا يضمن عدم تغييره
- فى حالة انشاء VPN يلزم ان يكون الIP ثابت ولا يتغير
- يوجد انواع مختلفة من الNAT وهم static NAT و dynamic NAT و PAT
- Static NAT فيه كل private IP له public IP
- Dynamic NAT فيه نقوم بتحويل مجموعة من الprivate IPs الى مجموعة من public IPs ولايكون كل private مقيد بواحد public
- PAT هو اختصار لport address translation وهو الNAT المقصود به والمستخدم حاليا
- يعمل ال PAT عن طريق ان كل الprivate IPs ستستخدم public IP 1 والتغير الذى سيحدث سيكون فى ال port number
- عمد استعمال الPAT يقوم الrouter بعمل جدول يسمى الNAT table يقوم بتخزين كل private ip مقابله من الpublic+port number
- الports المستخدمة فى الPAT تكون ما بعد 1024



Ip nat inside source static	• هو امر لعمل static nat ويتم اتباعه ب private ip ثم public ip	Ip nat inside source static 192.168.1.1 55.10.1.2	Configuration mode
Ip nat inside/outside	• يستخدم داخل الinterface لتحديد الinterface الموجودة فى الجزء الprivate والموجودة فى الجزء الpublic • Inside للجزء الprivate و outside للجزء الpublic	Ip nat inside Ip nat outside	Configuration mode inside interface

- لكى نقوم بعمل dynamic NAT
  1. نقوم بعمل access list والسماع للشبكة الprivate كلها
  2. نقوم بعمل pool يحتوى على range من الIPs الpublic
  3. نقوم باستعمال امر ip nat inside لكى نربط الaccess list ب pool

Access-list 1 permit	• نقوم من خلاله بعمل access list والسماح لالشبكة الprivate بالاتصال	Access-list 1 permit 192.168.1.0 0.0.0.255	Configuration mode
Ip nat pool	• يستخدم لعمل pool من ال public IPs • ياتى بعده اسم الpool ثم range الpublic IPs وفى النهاية نكتب netmask 255.255.255.0	Ip nat pool na 63.25.2.2 63.25.2.10 netmask 255.255.255.0	Configuration mode
Ip nat inside source	• سنقوم باستخدامه لعمل ربط بين access list و الpool • ياتى بعده list ثم رقمها ثم pool ثم اسمه • بعده يتم الدخول على كل interface وتحديد هل هى inside ام outside	Ip nat inside source list 1 pool na	Configuration mode

- تحدث الPAT مثل dynamic ولاكن فى الPAT نجعل الpool range هو ip واحد على سبيل المثال من 63.25.2.10 الى 63.25.2.10 ونضيف كلمة overload الى امر ip nat inside source

Network time protocol (NTP)

- اهمية الnetwork time protocol هو ضبط الوقت بين الrouters
- من المهم جدا جعل الوقت فى الrouters يكون صحيح
- عند استعمال الNTP فاننا نقوم بجعل router كا server اى انه هو من يعلم باقى الrouters بالوقت والrouters الاخرى تكون clients
- يمكن اضافة الوقت فى الrouter server بشكل يدوى او اننا نعطيه مصدر موثوق ليحصل منه على الوقت
- **Pool.ntp.org** هو افضل مصدر موثوق يمكن الاتيان بالوقت من خلاله
- يطلق على درجة المصدقية ب stratum
- يتم اعطاء الوقت بشكل يدوى من خلال امر clock set

ntp master	• هو امر يعطى لrouter الذى سيعطى لباقى الrouters الوقت	ntp master	Configuration mode
ntp server	• امر اعطار الrouter للمكان الذى سيحصل منه على الوقت • يعطى بعد الامر الIP الخاص بالinterface الخاصة ب master router • لن يتم تغيير الوقت فورا استخدام الامر وانما سيظل مدى معينة الى ان يتغير •	ntp server 168.23.2.1	Configuration mode
Show ntp status	• يستخدم لعرض معلومات عن الntp	Show ntp status	Privileged mode

Securing routers

- يوجد طريقتان لعمل configuration للrouter
  1. عند طريق console port
  2. من خلال telnet او SSH
- طريقة الtelnet و الSSH هى الطريقة الاحترافية
- يلزم وضع security للrouter لتحكم فى امكانية الدخول عليه

Line console	• هو امر لدخول الى ال console interface • يتم اتباعه برقم الconsole ويبدا الترقيم من 0	Line console 0	Configuration mode
Password	• يستخدم لعمل password ل console interface	Password 12345678 login	Configuration mode inside console interface

	• يجب كتابة امر login لتحديد متى سيقوم بطلب الpassword	no password	
Username * password *	• هو امر انشاء username و password فى الrouter • يوضع مكان * الusername و password	Username ahmed password 12345678	Configuration mode
Login local	• يقوم باستخدام الusernames الموجودة على الrouter لعمل login من خلالها • لاذالتها نستخدم امر no	Login local No login	Configuration mode inside console interface
Show run	• يستخدم لرؤية الconfiguration التى تمت	Show run	Privileged mode
Username * secret *	• هو امر يستخدم ايضا لانشاء username و password ولاكن يختلف فى انه بقوم بتشفير الpassword فى ملف الconfiguration بنوع MD5		Configuration mode
Enable password **Enable secret**	• يستخدمان لعمل password لprivileged mode • نستخدم no لالغائهم	Enable password 12345678 Enable secret 12345678	Configuration mode
Line vty	• يستخدم لعمل line من خلال telnet • Vty هى اختصار ل virtual telnet • يوضع بعده رقمين وهما المسؤلين عن تحديد عدد الاجهزة الممكن لها عمل configuration فى نفس الوقت • فى هذا المثال تم السماح ل 5 اجهزة • بعد انشاء الline سنكون بداخله تلقائيا وعند ذالك نقوم بستعمال الاوامر كما فى consoleال	Line vty 0 4	Configuration mode

- نقوم بدخول من الtelnet على الrouter عن طريق استخدام امر telnet ونتبعه بIP الinterface
- لايمكن الدخول على الtelnet الا عند انشاء password لها
- لا يمكن الدخول على الPrivileged mode من الtelnet الى عندما يكون له password
- الtelnet لايكون مفعل بشكل default على الwindows عكس الSSH
- لايتم استخدام الtelnet حاليا لانها ليست secure على عكس الSSH والتى تعنى secure shell
- هذه الطريقة فى الsecure تتم على الrouter و الswitch بنفس الكيفية

Backup & restore

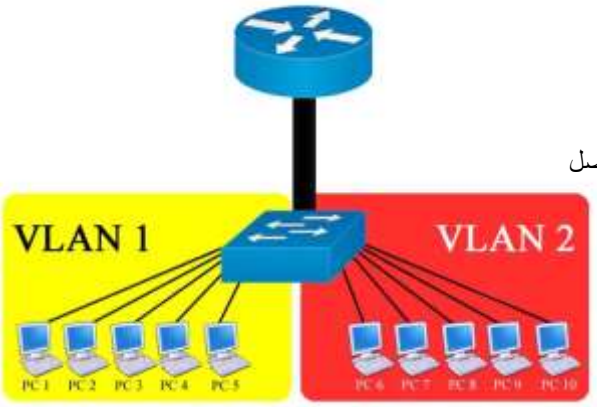
- من المهم اخذ backup من الIOS الموجود فى الflash او من الconfiguration files الموجودة فى الNVRAM
- لاخذ الbackup من pc متصل برouter يلزم استخدام برنامج يدعم برتكول TFTP

Copy run tftp	• يستخدم لعمل backup من الconfiguration ورسالها من خلال tftp • بعد ادخال الامر سيطلب منا عنوان الip الخاص بالجهاز الذى سيخزن عليه backupال • ثم سيطلب الاسم الذى سضعه للconfiguration backup	Copy run tftp	**Privileged mode**
Copy tftp run	• يستخدم لاسترجاع backup من جهاز ووضعها على الrouter • بعد ادخال الامر سيطلب منا ادخال الip الخاص بالجهاز • ثم سيطلب منا اسم الملف	Copy tftp run	**Privileged mode**
Show flash	• هو امر يستخدم لمعرفة الfiles الموجودة على flash drive فى الrouter	Show flash	**Privileged mode**
Copy flash tftp	• يستخدم لاخذ backup من flash الى جهاز معين • يلزم معرفة اسم الملف لذالك سنحتاج الى امر show flash	Copy flash tftp	**Privileged mode**

	Copy tftp flash	• يمكن عكس الامر لكى ناخذ الملف من الجهاز الى الrouter	

VLAN

- VLAN هى عملية تقسيم (segmentation) للشبكة وتقسيم الاجهزة الى مجموعات
- VLAN اصبحت شئ اساسى يجب تطبيقه فى الشبكة
- VLAN تستخدم لتقليل الbroad cast الموجود فى الشبكة حيث انها تذيد عدد الbroadcast domain ولاكن تجعل الscope الخاص به داخل الVLAN فقط
- عملية انشاء VLAN تعتمد على عمل configuration لل switch وتحديد الports الخاصة بكل مجموعة من الاجهزة
- لا يمكن لجهاز من VLAN التواصل مع اخر فى VLAN مختلفة
- فوائد الVLAN كتالى :
  1. تذيد من مستوى الsecurity
  2. تقليل الbroadcast الموجودة فى الشبكة
  3. تسهل عملية الmanagement حيث سيتم التعامل مع كل vlan بشكل منفصل
- عملية انشاء vlan على الswitch تنمم على خطوتين :
  1. انشاء الvlan
  2. عمل distribution لل port
- اى switch بشكل default يحتوى على vlan رقمها 1 وتسمى default vlan
- لايمكن الغاء الdefault vlan ولايمكن تغير اسمها
- يتم استخدام امر **ena** و امر **config t** فى الswitch كما فى الrouter
- يتم حفظ الconfiguration على الswitch ايضا من خلال امر **do wr**
- يتم التعامل مع الvlan من خلال رقمها (id) وليس اسمها



Configuration mode	Show vlan	Show vlan
Configuration mode	Vlan 2	• يقوم بعرض الvlan الموجودة على الswitch • اول vlan تظهر هى الdefault
Configuration mode inside the vlan	Name HR	• يستخدم هذا الامر لانشاء vlan ويتم اتباعه برقم الvlan
Configuration mode	Int f0/1 Int range f0/2-7	• هو امر يستخدم لتعديل اسم الvlan ويتم اتباعه باسمها
Configuration mode inside port	Switchport access vlan 2	• هو امر لدخول الى interface معينة • يمكن اضافة له امر rang لدخول على اكثر من interface وتطبيق عليهم نفس الconfiguration

Switchport access vlan	• هو امر لاضافة الinterface الى vlan ويتم اتباعه برقمها

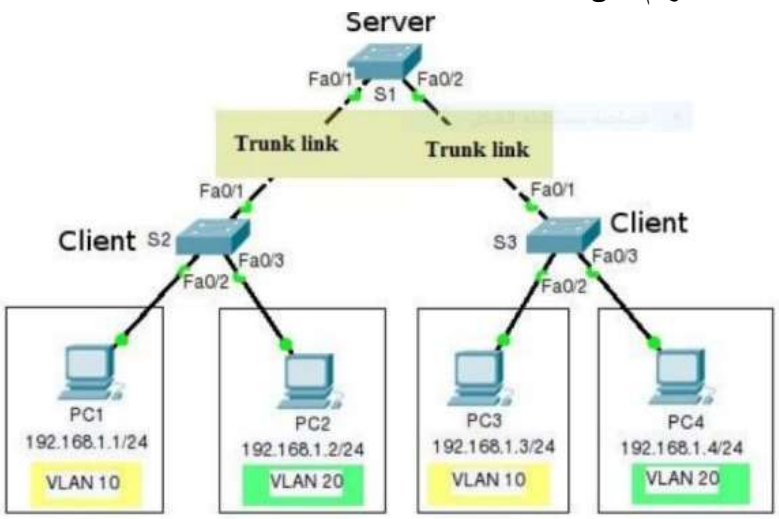
- range **Id** الخاص ب vlan الذى يمكن انشائه يكون من 1 الى 1001
- يوجد Ids بعد 1001 ولاكن لايمكن استخدمها لانها تستخدم للtoken ring ولشركات الISP
- لكل port فى الswitch مايسمى بالmode ويكون له قيمة من اثنان
  1. Access وهى تستخدم عند الاتصال من switch الى pc
  2. Trunk وهى تستخدم عند اتصال من switch الى switch اخر
  3. Dynamic وهى القيمة الdefault للport وهى تعنى انها تصبح access او trunk بناء على الinterface المقابلة
- الport صاحب access mode يسمح فقط بمرور vlan الخاصة به بينما الtrunk mode يسمح بمرور جميع الvlan عبره
- يمكن ضم اكثر من جهاز متصلين على switches مختلفة الى نفس الvlan ولاكن يجب ان يكون الMod الخاص بالinterfaces بين switches على trunk

Switchport mode trunk	• هو امر يقوم بتحويل الport الى trunk mode	Switchport mode trunk	Configuration mode inside port

- بعد تحويل الmode الخاص بالport سيقوم الswitch بعمل restart له
- يمكن تحويل الى trunk من خلال switch واحد فقط والswitch الاخر سيغيره تلقائيا ولاكن يفضل تحويله من الاثنان
- فى حالة اننا اردنا ان نجعل الاجهزة التى فى vlan مختلفة ترى بعضها سنحتاج الى عمل routing بينهم من خلال multilayer switch او router
- عملية الsubnetting هى عملية مصاحبة للVLAN

VTP

- هو اختصار ل VLAN trunking protocol
- هو protocol يستخدم فى عمل VLAN على اكثر من switch فى نفس الوقت من خلال switch واحد فقط
- عند انشاء الVLAN على switch او حذفها او تعديلها سيتم تطبيق التغيير على باقى الswitches
- عند انشاء VTP على switch يلزم تحديد الmode الخاص بالswitch وهم كتالى :
  1. Client
  2. Server
  3. Transparent
- الserver هو الذى يمكنه عمل اى التعديلات على الVLAN
- الclient switch يقوم باخذ نسخة من الVLANs الموجودة على server switch ويقوم بتمريرها اذا كان متصل ب switches اخرى
- الclient لايمكنه انشاء او اذالة VLAN
- Transparent switch لا يقوم بتطبيق الVTP عليه ولاكن يمكنه نقل ال configuration الخاصة ب VTP عبره الى ال switches الاخرة
- يمكن للtransparent switch انشاء او حذف او تعديل ل vlan ولاكن هذه الvlan تكون خاصة به فقط
- الdefault mode الخاص بswitch يكون server



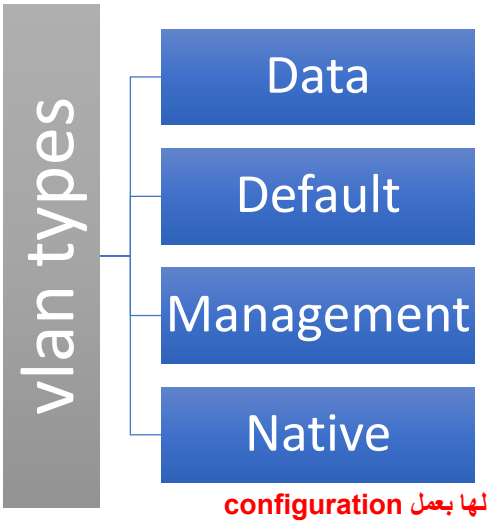
Configuration mode	vtp mode client	vtp mode
Configuration mode	vtp domain domain1	vtp domain • يستخدم لعمل domain واعطاءه اسم ويتبع هذا الامر الاسم
Configuration mode	Vtp password pass123	Vtp password • هو امر لاعطاء password للvtp • اعطاء password هى عملية اختيارية ولاكن يفضل عملها لذيادة الsecurity
Privileged mode	Show vtp st	Show vtp st • هو امر لرؤية المعلومات عن الvtp بما فى ذالك اسمه ونوع الmode • الst اختصار ل status

- يجب اعطاء vtp domain و vtp password الخاص بserver switch ل client switch لكى يستطيع اخذ نسخة منه
- لا يجب نسيان تحويل الports بين الswitches لtrunk
- Configuration revision هو رقم يذيد كلما حدث انشاء او حذف او تعديل فى الVLANs ويمكن رؤية هذا الرقم باستعمال امر show vtp st
- فى حلات استثنائية يمكن للclient switch ارسال البينات الى الserver switch وهى عندما يكون الrevision number فى الclient اكبر من الserver ويحدث هذا فى حلات معينة مثل حدوث عطل فى switch server او توقفه عن العمل لفترة

عند توصيل switch جديد الى الشبكة يجب التاكد مما اذا كان هذا الswitch ليس لديه اى configuration للvlan لانه فى حالة كان لديه وكان الrevision number الخاص به اعلى من الموجود فى الشبكة سيتم اخذ نسخة من هذا الswitch وتوزيعها على باقى الswitches

لاتحدث الحالة السابقة الا عند تشابه الdomain الموجود فى الswitch والموجود فى الشبكة واذا كان هناك password يجب تشابهه ايضا لتتحقق

- يمكن حل مشكلة السيناريو السابق عن طريق تحويل الrevision number الخاص بالswitch الى 0 ويحدث ذالك بطريقتان :
  1. تحويله الى transparent ثم الى client
  2. تغير الdomain
- يوجد اثنان من trunking protocol وهما :
  1. ISL وهو protocol تم انشائه بواسطة cisco ولاكنه لم يعد يستخدم حاليا
  2. 802.1Q وهو open standard protocol يمكن استخدامه من خلال اى vendor وهو المستخدم حاليا
- عند ارسال data من vlan الى نفس الvlan ولاكن المتصلة عند switch اخر فسيقوم الswitch الاول المتصل باول vlan بتغليف الframe اولا قبل ارساله الى الswitch الاخر وفى هذا التغليف سيتم تحديد الvlan الذى تنتمى له هذه الdata
- عملية التغليف تسمي tagging
- 802.1Q هو المفعل بشكل تلقائي على الswitches
- الpc لايفهم الtagging عكس الswitch و ip phone
- الكبل بين الip phone و الswitch يكون trunk



VLAN types

- Data vlan هى التى يتم انشائها على الswitch بشكل يدوى واستخدمها هو مشاركة البيانات بين الاجهزة
- Default vlan هى الموجودة على الswitch بشكل افتراضي وتوجد بها كل الports التى لم توزع على الdata vlan
- لايمكن الغاء او تعديل الdefault vlan بينما يمكن عمل ذالك على الdata vlan
- Management vlan هى vlan يتم انشائها لتسهيل عملية الconfiguration على ال switch
- لكى نقوم بعمل management من خلال telnet او من خلال ssh سيلزم وضع ip ل vlan المراد السماح لها بعمل الconfiguration وهذه ما يطلق عليها Management vlan
- يجب ان يكون الip المعطى ينتمى الى range ال vlan فى حالة وجود subnetting

مما سبق الmanagement vlan هى عبارة عن data vlan ولاكن مضاف لها ip ومسموح لها بعمل configuration

Configuration mode	Int vlan 4		Int vlan
		• Int هو الامر المستخدم لدخول على الports ولاكن هنا سنتبعه بvlan ثم رقمها لدخول عليها كا interface	

- عند الدخول على الvlan كا interface نستخدم اوامر الinterface الموجودة فى الrouter مثل
  1. **no shutdown** ويتم تنفيزه بعد الدخول على الvlan مباشرة
  2. **ip address** لاعطائها ip
  3. **enable secret/password** لاعطاء password لprivileged mode
     - يجب اعطاء password لprivileged mode لاستخدامه عبر الtelnet
  4. **Line vty** لتفعيل الtelnet على الvlan
     - بعد تفعيل الtelnet يجب اعطائها password لكى نستطيع استخدامها

- Native VLAN هى vlan لايحدث لها tagging عند ارسالها من switch الى اخر
- Vlan 1 تكون هى الnative بشكل default
- يجب ان تكون native vlan واحدة فى جميع الswitches
- يتم استخدامه فى بعض السيناريوهات مثل عمل vlan للاجهزة المتصلة عبر ip phone

Inter VLAN

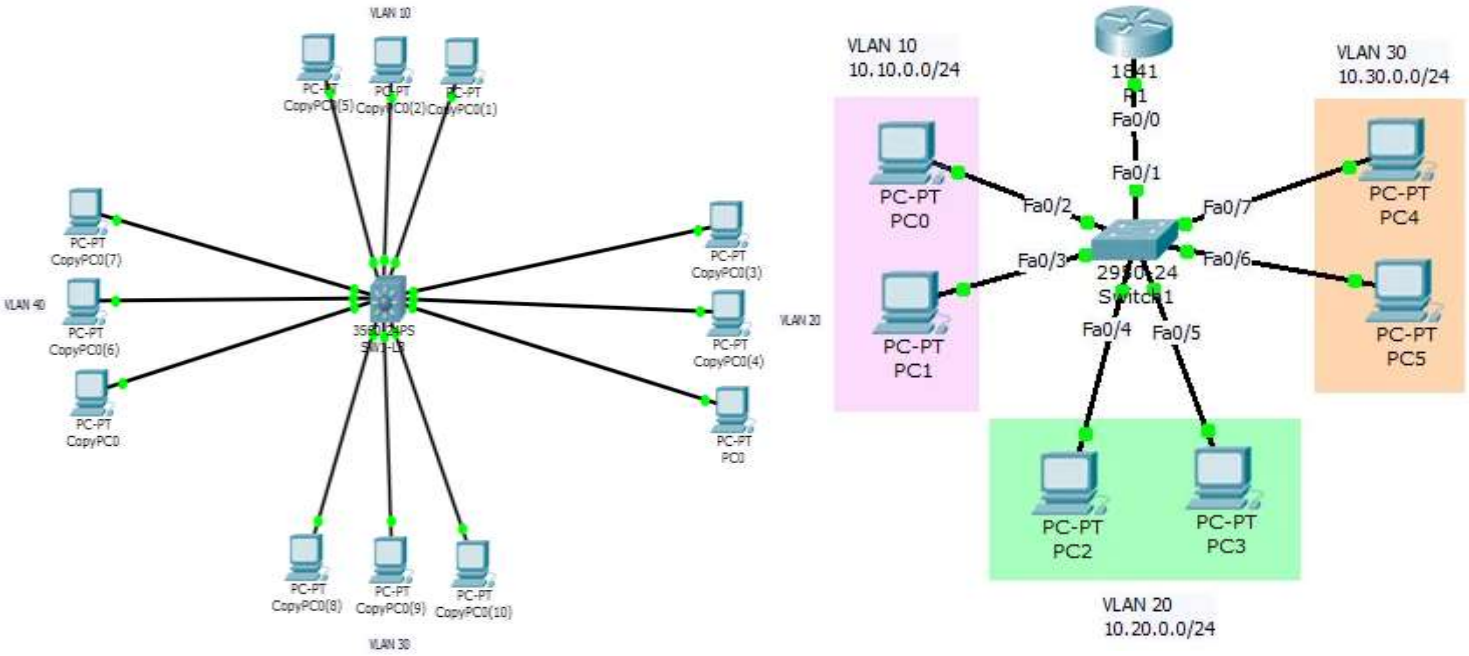
- تسمي ايضا inter VLAN ب router on stick
- فكرة الinter vlan هى اننا سنقوم بوضع كل vlan فى شبكة او subnet مختلفة ونضيف router الى الشبكة لكى يتمكنو من الاتصال فيما بينهم
- يمكن الاستغناء عن router و الlayer 2 switch ونقوم باستخدام layer 3 switch
- عند استخدام router يلزم وجود interface لكل vlan وبسبب قلة الinterfaces الموجودة فى الrouter سنقوم بعمل مايسمى ب subinterface
- Sub interface هى عملية تقسيم الInterface الواحدة الى مجموعة من الinterfaces وكل واحدة تحمل ip مختلف من شبكة مختلفة

Configuration mode	Int g0/0/0.1 Int g0/0/1.1 Int g0/0/1.3	• **يتم استخدام هذا الامر فى الشكل الطبيعى لدخول على الinterface ولاكن هنا نقوم بستخدامه لتجزءة الinterface والدخول عليها** • **G0/0/0 هى الinterface التى سنقوم ب تجزائتها** • **1. هو الجزء الاول من الinterface وعدد الاجزاء ليس مهما**	**Int g0/0/0.1**
Configuration mode inside sub interface	encapsulation dot1Q 2 encapsulation dot1Q 3	• يلزم استخدام هذا الامر لكى نتمكن من اعطاء ip ل sub interface • هذا الامر يقوم بتفعيل ال trunking protocol فى الsub interface ويتم اتباعه ب رقم الvlan الذى سيستقبل منها الdata • بعد تنفيذ هذا الامر يتم اعطاء ip لل sub interface من خلال امر ip address وكل sub interface تاخذ الip الذى سيكون الdefault gateway للvlan المراد اخذ منها الdata	Encapsulation dot1Q

- يلزم جعل الport الذى بين الswitch بين الrouter يكون trunk mode

- فى حالة قمنا باستخدام layer 3 switch بدلا من router سنقوم بعمل نفس الconfiguration الخاصة ب switch كما هى ولاكننا سنقوم بانشاء interfaces وهمية ونعطيها الIPs الخاصة بdefault gateways

Configuration mode	**Interface vlan2**	• يتم استخدام هذا الامر على layer 3 switch لكى يقوم بانشاء interface وهمية وياتى بعده اسم الinterface	**interface**
Configuration mode	lp routing	• يتم استخدام هذا الامر على ال layer 3 switch لكى يبدا العمل كا router • بدون هذا الامر لن يتم الاتصال بين الاجهزة التى فى vlan مختلفة ولن تعمل اوامر الrouter على ال layer 3 switch	**ip routing**



Port security

- هو نوع من الsecurity يتم تطبيقه على الswitches لمنع دخول اجهزة غير مصرح لها
- تتم عملية port security على الports الaccess لذالك يجب تطبيق امر switchport mode access لتحويل الport من dynamic الى access

Configuration mode inside the port	**Switchport port-security**	• يستخدم هذا الامر فى بداية كتابة امر الport security وبعده نقوم بكتابة الاوامر	**Switchport port-security**
Configuration mode inside the port	Switchport port-security mac-address 1A:5F:36:B1:28:FC Switchport port-security mac-address sticky	• هو امر يستخدم لتحديد الجهاز المسموح له فقط بالاتصال على هذا الport • يتم اتباعه ب الmac address الخاص بالجهاز او نقوم باضافة sticky وهى تعنى ان الswitch سيقوم بوضع الmac الخاص بالجهاز المتصل حاليا	**Switchport port-security mac-address**

- بعد تنفيذ الport security فى حالة تم اكتشاف جهاز غير مصرح له سيتم ايقاف الport من قبل الswitch ووضع الport فى حالة تسمى error disable وهى حالة اشد من الshutdown
- لارجاع الport للعمل مرة اخرى بعد حدوث error disable يلزم عمل shutdown ثم no shutdown

Configuration mode inside port	**Switchport port-security violation protect** **Switchport port-security violation restrict** **Switchport port-security violation shutdown**	• يستخدم هذا الامر لتحديد الاجراء الذى سيحدث فى حالة اتصال جهاز غير مصرح له • يضاف الى الامر قيمة من ثلاث قيم وهم : 1. Protect لن يتم ارسال او استلام اى data لالجهاز الغير مصرح له	**Switchport port-security violation**

		2. Restrict هى مثل الprotect ولاكن هذا الخيار يقوم باعطاء تنبيه الى الswitch بحدوث اتصال بجهاز غريب 3. Shutdown وهو القيمة الdefault	

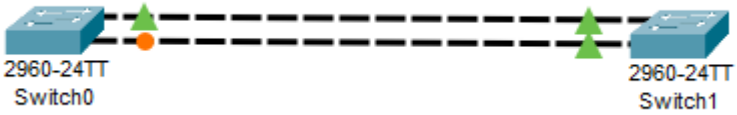
- هناك هجوم يمكن ان يتم على الswitch وهو ان يقوم جهاز بملئ الmac address table الخاص بالswitch ويؤدى ذالك الى تحول الswitch الى العمل كا hub ويتم الحماية من هذا الهجوم عن طريق وضع حد لعدد الmac address التى يمكن تسجيلها من هذا الport

Configuration mode inside the port	Switchport port-security maximum 2		Switchport port-security maximum
		• هو الامر المستخدم لوضع حد لعدد الmac addresses التى يمكن تسجيلها من هذا الport ويتم اتباع الامر بالعدد	

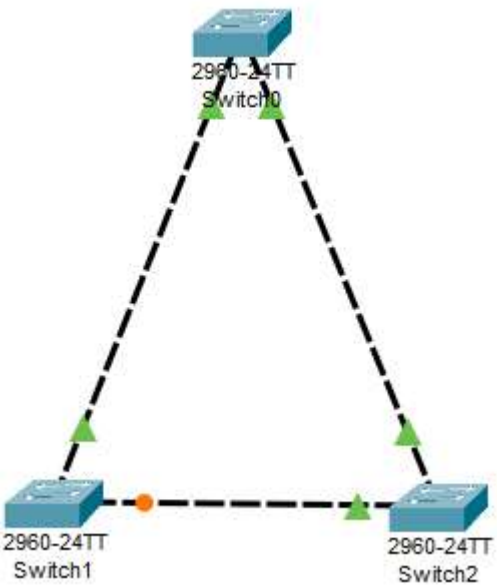
Spanning tree protocol (STP)

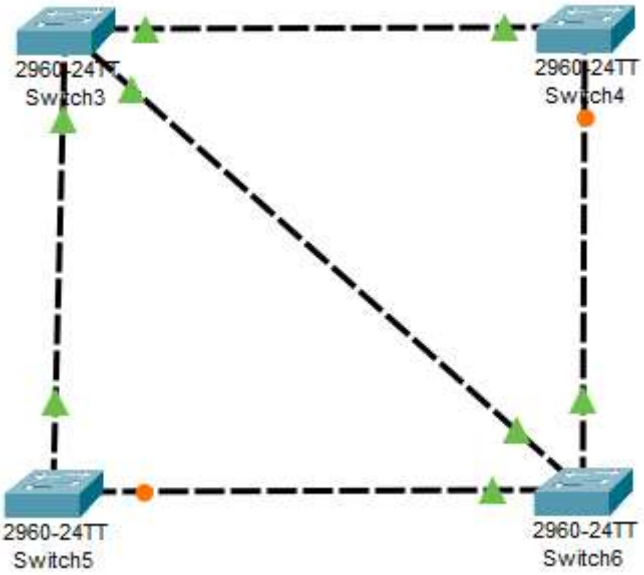
اتصال switch باخر يجب ان يتم باكثر من connection وهذا لتحقيق الredundancy حيث اننا اذا قمنا بتوصيلهم معا ب connection واحد سنواجه مشاكل فى حالة فقدان هذا الconnection ولاكن عندما يوجد اكثر من connection فيمكننا تفادى هذه المشاكل .

- وجود اكثر من connection بين الswitches يحقق الredundancy ولاكنه يظهر مشكلة اخرى وهى انه يمكن للbroadcast signal ان تذهب من switch الى اخر فى loop بدون توقف وهذه المشكلة تم حلها بواسطة STP
- STP مفعل تلقائيا على الswitches
- STP سيقوم بحل مشكلة الloop عن طريق انه سيسمح لواحد من الconnection بالعمل والباقى سيقوم بتعطيلها عن طريق تعطل الports بشكل مؤقت
- فى حالة فقدان لconnection الذى يعمل سقوم الSTP بتفعيل الconnection الاخر
- هناك معادلة من خلالها يمكننا حساب عدد الports التى سيتم ايقافها من خلال STP وهى كتالى



عدد ports = عدد الكبلات + عدد السوتشات + 1





- عند اتصال الswitches مع بعضهم وتفعيل الSTP سيتم اختيار switch منهم لكى يكون root bridge وهذا الswitch يجب ان تمر به اى signal ذاهبة من switch الى اخر
- عملية اختيار الroot bridge تتم على خطوات كتالى :
  1. يقوم كل switch بارسال رسالة تسمي BPDU وهى رسالة يوجد بها bridge Id
     - Bridge id يتم حسابه من priority number وهو رقم ياتى من الشركة المصنعة للswitch وغالبا يكون متشابه فى الswitches + mac address
  2. الswitch صاحب اقل bridge هو من يتم تينه كا root bridge
- الswitches الاخرى غير root bridge تسمى بswitch designated
- الswitch root جميع الports الخاصة به تعمل وتسمى designated port (DP)

- كل designated switch له root port وهو الportالذى سيصل منه الى root switch وهذا الportيتم تحديده من المسار الاسرع الى root switch

speed	cost
10	**100**
100	**19**
1000	**4**
10000	**2**

- تحديد root port يتم بناء على السرعة او الcost وهذا تم من خلال منظمة IEEE كتالى

Privileged mode	Show sp		Show sp
		• يستخدم هذا الامر لمعرفة الroot switch وبعض المعلومات الاخرى مثل priority number و الmac address	

- فى حالة وقوع الconnectionالذى يعمل سيتم تشغيل الconnection الاخر خلال 50 ثانية وهذه المدى تعتبر كبيرة لذالك تم اصدار protocol اخر وهو Rapid STP وهو قام بتغيير هذه المدى الى ثانية او ثانيتان
- لاستخدام الRapid STP يجب تشغيله على جميع الswitches

Configuration mode	Spanning-tree mode rapid-pvst		Spanning-tree mode rapid-pvst
		• يستخدم لتفعيل Rapid STP على الswitches	

- فى حالة اتصال PC ب switch سيتم تطبيق الconnection خلال 30 ثانية ولاكن مع استخدام الRapid STP يمكن جعل الconnection بشكل سريع جدا وهذه التقنية بتسمى port fast
- الport fast يتم تطبيقها على الport access ولايجب ابدا تطبيقها على trunk ports

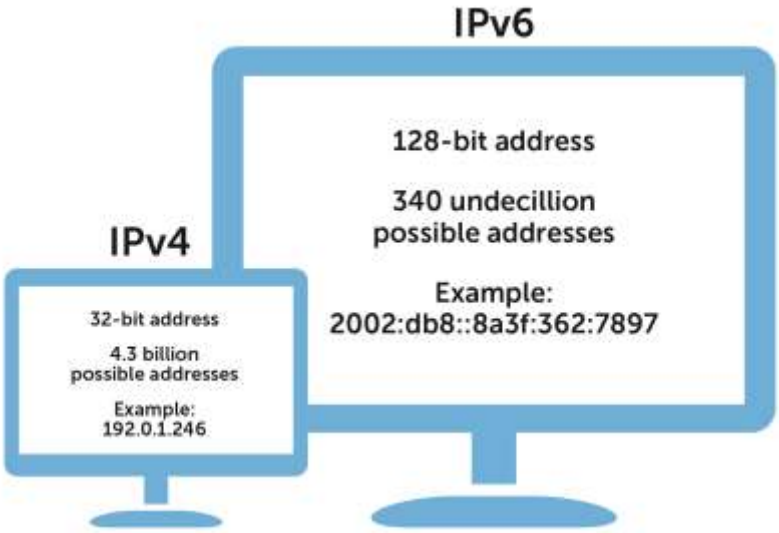
Configuration mode inside interface	Spanning-tree portfast		Spanning-tree portfast
		• يستخدم هذا الامر داخل الinterface التى نريد تشغيل فيها port fast	

- عند تطبيق STP مع مبدا الVLAN ينتج لدينا ما يسمى ب PVSTP وهو ان كل vlan تصبح لديها root switch مختلف عن باقى الvlan ويكون هناك blocked ports لكل vlan مختلف عن الاخرى

Configuration mode	Spanning-tree vlan 2 root primary		Spanning-tree vlan * root primary
		• هو امر يقوم بجعل الswitch هو الroot switch لvlan معينة • * توضع مكانها رقم الvlan	

IPv6

- IPv6 تم انشائه لتغلب على انتهاء عدد الIPs من IPv4
- هناك بعض المسميات التى تغيرت باستخدام IPv6 كتالى :
  a) Private IP اصبح يسمى site local
  b) Public IP اصبح يسمى global
  c) Apipa ip اصبح يسمى link local
- IPv4 كان يتكون من اربع خانات تسمى octet وتكون decimal ويفصل بينهم بنقطة وحجكه يكون 32 BIT بينما IPv6 يتكون من 8 خانات يفصل بينهم ب : وتسمى group وتكون hexadecimal وحجمها هو 128 bit
- من مزايا IPv6 الاتى :
  1. يقوم بتوفير عدد كبير من الIPs
  2. اسرع من IPv4 بسبب قلة الheader
  3. Secure لان اى data يتم نقلها من خلاله تكون مشفرة
  4. ميزة الautoconfiguration وهى تعنى ان الجهاز يمكنه الحصول على IP بدون وجود DHCP



- لايوجد classes فى IPv6
- اول اربع خانات تعبر عن network ID وتسمى prefix بينما اخر اربعة تعبر عن host ID
- هناك طرق لاختصار IPv6 الى شكل ابسط يسهل قراته وكتابته كتالى :
  1. الصفر الذى ع الشمال يمكن تجاهله
  2. اى group مكون من اصفار فقط او اكثر من group بشكل متتابع يمكن اذالتهم ووضع ::
     - هذا الاختصار يحدث مرة واحدة فقط

FE40:AF2::ABCD:0:0:AB2 <---------- FE40:0AF2:0000:0000:ABCD:0000:0000:0AB2

- يتم اضافة احيانا /64 فى نهاية IPv6 لتحديد ان اول 64bit هم لNetwork ID ويجب كتابتها عند اعطاء ip لجهاز
- كلا من unicast و multicast موجودين فى IPv6 كما فى IPv4 بينما الbroadcast لم يعد موجودا وتم استبداله بمايسمى بAnycast

- يسمى الAnycast ايضا ب one to nearest
- عملية حصول الجهاز على IPv6 تتم من خلال واحد من الاتى :
  1. Manual من خلال الnetwork admin
  2. Link local وتسمى ايضا ب EUI-64
  3. Dynamic من خلال DHCP وهم ثلاث طرق
     1) Statful
     2) Statless
     3) Slaac
- Link local وهى طريقة مثل الAPIPA فى IPv4 وهى تبدا ب FE80 ثم نضع الmac address الخاص بالجهاز ثم نضع FFFE فى منتصف الmac وبهذا نكون اكملنا اول 64 BIT الخاصة ب network ID
- لايمكن استعمال ال link local فى الinternet ابدا وانما داخل الشبكة الlocal فقط
- يظل الجهاز محتفظ ب link local ip حتى وان تم اعطائه ip بشكل manual او من خلال DHCP
- Statful هى الحالة عندما يكون لدينا DHCP server او router مفعل عليه DHCP ويقوم باعطاء Ips للاجهزة
- Slaac وهى تحدث عندما لايوجد DHCP ولاكن من خلال الrouter سيتم عمل autoconfiguration ويتم اعطاء IP للجهاز ويحدث ذالك كتالى :
  1. يقوم الجهاز بالبحث عن DHCP ولاكن لايجد
  2. يقوم الrouter باعطاء الجهاز الnetwork ID الخاصة به وبقوم الجهاز بانشاء الHost ID من خلال الMAC address الخاص به
     - بجانب الnetwork ID سيقوم الrouter باعطاء الجهاز gateway
- Statless وهى الحالة عندما يوجد DHCP ولاكن يقوم الrouter بعامل مع الجهاز مثل Slaac ويوجد اختلاف اخر وهو انه يعطيه الDNS بجانب الdefaul gateway

IPv6 routing

- يجب قبل عمل routing باستخدام ipv6 ان نفعله من الrouter وهذا يحدث باستخدام امر ipv6 unicast routing

Configuration mode	**Ipv6 unicast-routing**	• يلزم استخدام هذا الامر قبل عمل routing ب IPv6	**Ipv6 unicast-routing**
Privileged mode	**Show ipv6 route**	• يستخدم لمعرفة routing table الخاص ب IPv6	**Show ipv6 route**
privialged mode	**Show IPv6 int br**	• يستخدم لمعرفة كل IPv6 لكل interface	**Show ipv6 int br**
Configuration mode inside interface	**Ipv6 address 2000:1::1/64** **No ipv6 address**	• يستخدم لاعطاء IPv6 للinterface • لازالة الip نضع no قبلها	**Ipv6 address**
Configuration mode	**Ipv6 route 2000:1::/64 2000:3::**	• يستخدم هذا الامر لعمل routing بشكل static لIPv6 • بعض وضع ip الشبكة نضع ال next hop • لايتم اضافة subnetmask لان ipv6 لايحتوى على subnetmask	**Ipv6 route**

- تختلف الconfiguration الخاصة ب rip فى IPv6 حيث اننا نقوم بتفعيله واعطائه اسم ثم نقوم بتفعيله على كل interface

Configuration mode	**Ipv6 router rip rip1**	• يستخدم لتفعيل rip الخاص بipv6 على الrouter ويتم اتباعه باسمه	**Ipv6 router rip**
Configuration mode inside interface	**Ipv6 rip rip1 enable**	• يستخدم داخل الinterfaces لتفعيل الrip الخاص ب IPv6 ويوضع مكان * اسمه	**Ipv6 rip * enable**
Privileged mode	**Show ipv6 pr**	• يستخدم هذا الامر لمعرفة اى من الrouting protocol يعمل على هذا الrouter	**Show ipv6 pr**

- عندما نريد تفعيل الospf routing فى IPv6 يجب اولا اعطاء الrouter الrouter id ويعطى على شكل ip

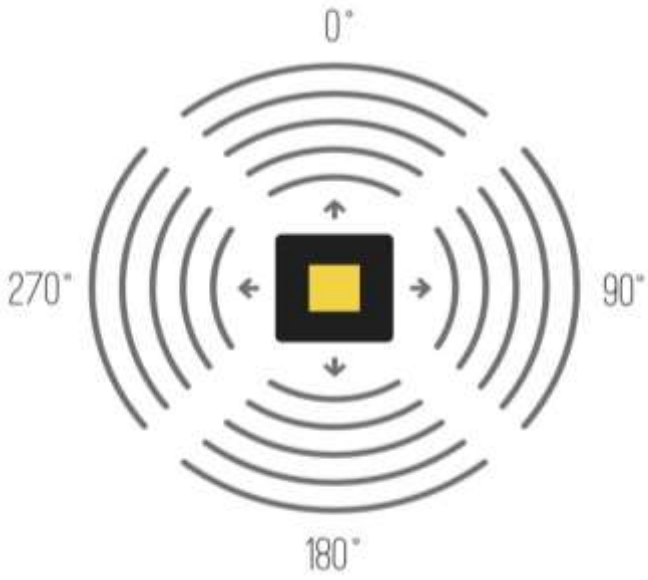
Configuration mode inside ipv6	**Router-id 10.0.0.0**	• يستخدم لاعطاء الrouter id ويعطى فى شكل ip	**Router-id**
Configuration mode	**Ipv6 router ospf 1**	• يستخدم لتشغيل الospf على الrouter ويتبعه رقم الprocess	**Ipv6 router ospf**
Configuration mode inside interface	**Ipv6 ospf 1 area 0**	• يستخدم لتفعيل ospf على الinterfaceses ويوضع مكان * رقم الprocess ويتم اتباعه برقم الarea	**Ipv6 ospf * area**

- عند تفعيل EIGRP فى IPv6 يجب اعطاء EIGRP router id ويجب استخدام امر no shutdown

Configuration mode	Ipv6 router eigrp 1	• يستخدم لتفعيل protocol الeigrp على الrouter ويتم اتباعه برقم	Ipv6 router eigrp
Configuration mode inside EIGRP	Eigrp router-id 10.0.0.0	• يستخدم لاضافة EIGRP router id ويكون فى شكل ip • لايجب نسيان استخدام امر no shutdown	Eigrp router-id
Configuration mode inside interface	Ipv6 eigrp 1	• يستخدم لتشغيل الEIGRP داخل الinterfaces ويتم اتباعه برقمه	Ipv6 eigrp

Wireless network (WLAN)

- عند انشاء LAN هناك طريقتان الاولة عن طريق كبلات وتسمى Ethernet والثانية بدون كبلات وتسمى wireless
- الstandard الخاص بشبكات الEthernet هى 802.3 والstandard الخاص ب 802.11 wireless
- الوسط المستخدم فى الwireless يمكن ان يكون الهواء او الفضاء او حتى الماء وينقل فى شكل موجات كهرمغنطيسية
- الجهاز البديل للswitch فى الWLAN هو الaccess point
- بجب ان يدعم الPC او الlabtop الاتصال الwireless عن طريق wireless adapter
- Antennas هى الجزء الطويل فى الaccess point او فى wireless adapter والمسؤل عن ارسال الاشارة او ذيادة مداها
- Antennas يوجد منها نوعان
  1. Omnidirectional وهو نوع اشارته ترسل الى جميع الاتجهات
  2. Unidirectional وهو نوع اشارته ترسل الى اتجاه واحد



- كون الdata تنتقل على شكل موجات كهرومغنطيسية فاننا نتعامل مع بعض الخصائص مثل frequency و channel
- اشهر قيمتان يتم استخدمهم فى الwireless connection هم

1. 2.4 MHZ

- يتم استخدام هذا التردد من خلال الكثير من الجهزة المنزلية مثل microwave او الاجهزة غير المنزلية مثل wireless printer وهذا ما يؤدى الى حدوث interference و noise مما يؤدى الى قلة كفائة الaccesspoint
- سرعتها اقل من 5 MHZ ولاكنها تصل الى مسافة اكبر
- تخترق الحوائط افضل من 5 MHZ

2. 5 MHZ

- قليل من الاجهزة التى تستخدم نفس التردد مما يجعله افضل فى نقل الdata لقلة حدوث noise
- سرعتها اعلى من 2.4 MHZ ولاكنها تصل الى مسافة اقل
- اختراقه للحوائط ليس بكيفية 2.4 MHZ

- يوجد العديد من الstandard ل wireless وهى تختلف فى الbandwidth و الrange وفى transmission method

802.11 Standards Comparsion

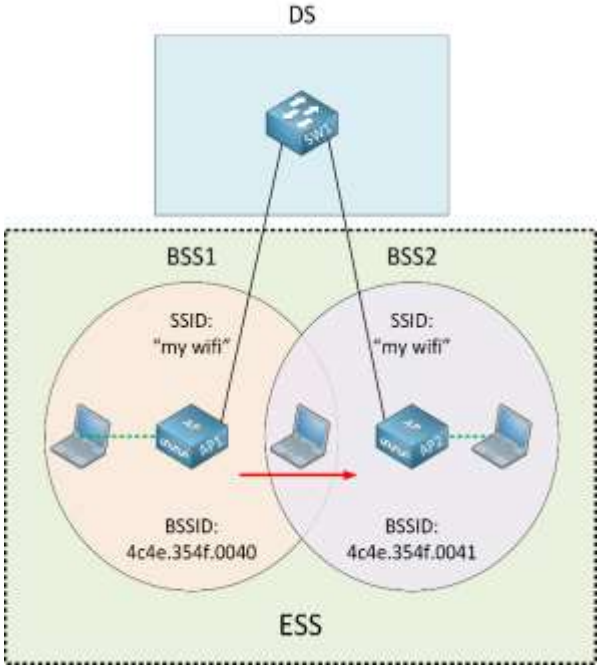
CBO connecting technolegy

STANDARD	YEAR RELEASED	FREQUENCY (GHZ)	SPEED	RANGE (INDOOR)	RANGE (OUTDOOR)
802.11	1997	2.4	2Mbps	20m	100m
802.11A	1999	5	1.5-54Mbps	35m	120/5000m
802.11B	1999	2.4	11Mbps	35m	120m
802.11G	2003	2.4	54Mbps	38m	140m
802.11N	2009	2.4/5	600Mbps	70m	250m
802.11AC	2013	2.4/5	450/1300Mbps	35m	-
802.11AX	2019	2.4/5	10-15Gbs	30m	120m

www.cbo-it.de

- 802.11 لم تعد موجودة اليوم
- فى حالة اتصال الاجهزة معا بشكل wireless بدون وجود acess point تسمى هذا الشبكة AD-HOC
- BSS WLAN هى الnetwork حيث تتصل الاجهزة معا ب access point
- ESS WLAN هى network مثل الBSS ولاكن فى الESS يوجد اكثر من access point لتغطية مساحة اكبر وتسمى المنطقة المشتركة بين الtwo access point ب overlabbing
- SSID الخاص بالشبكة هو الاسم الظاهر لها
- عند انشاء ESS فاننا نقوم باعطاء كل الaccess pointes نفس الاسم ونفس ونفس الpassword وهذا يؤسس ما يسمى ب Roaming وهى ان نجعلهم شبكة واحدة بغض النظر عن اى Access point متصل بها الجهاز

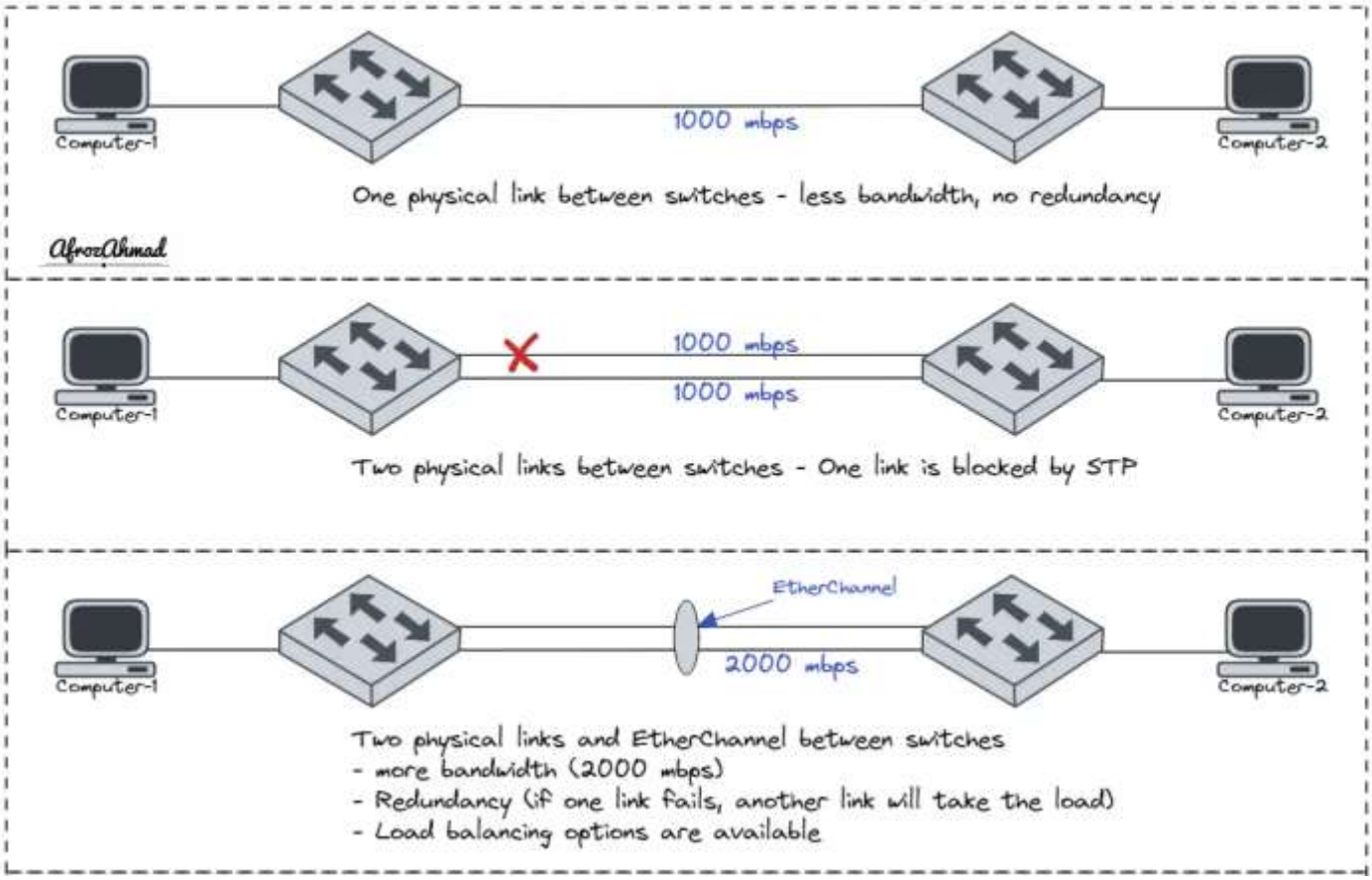
Securing wireless LAN

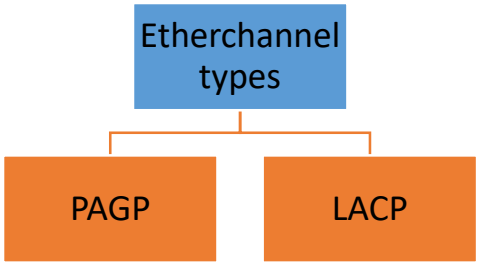


- اول شكل لحماية الWLAN هو وضع password لشبكة
- MAC Address Filtering وهى طريقة اخرى لحماية WLAN وهى تقوم على تحديد الاجهزة المسموح لها الاتصال وذالك يحدث من خلال ال MAC
- Disabling SSID Broadcast وهى تعنى عدم ارسال الSSID لاى جهاز مما يؤدى الى اختفاء الشبكة للجهزة المحيطة
- IEEE 802.1X وهو standard يقوم على ان الaccess point تكون متصلة بserver ولكى يقوم اى جهاز بالاتصال على الaccess point يجب ان يقوم بادخال username و password ويكونو مخزنين على الserver
- توجد العديد من انواع التشفير فى الWLAN وهم
  1. WEP وهى طريقة قديمة لتشفير ولم تعد تستخدم ويسهل فكها
  2. WPA وهو نوع افضل فى التشفير ويعتمد على protocol يسمى TKIP
  3. WPA2 وهو افضل نوع فى التشفير وهو المستخدم اليوم بكثرة
- لكى نفعل IEEE 802.1X يجب ان نضع الsecurity فى الacces point على WPA2 Enterprise ونقوم باضافة الIP الخاص بالserver ويسمى ب radus server او ال AAA server ونضيف password لهذه الخدمة
- يجب للserver ان يكون مفعل عليه AAA service ونقوم باعطائها الIP الخاص ب الaccess point بجانب اسم الaccess point والباسورد الذى اعطيناه للخدمة فى الaccess point ثم نقوم باضافة الusernames و الpasswords الخاص ب الclients

EtherChannel

- الetherchannel هى تقنية تقوم بجعل اكثر من Ethernet cable يعملوا كا cable واحد فقط
- تقنية الetherchannel تقوم بالغاء الSTP لانها تجعل الcables كانهم cable واحد فقط مما يلغى فكرة حدوث loop
- تقنية الehterchannel نقوم بتنفذها على كلا طرفى الاتصال
- يلزم ان تكون الports فى كلا طرفى الاتصال نفس السرعة
- مميزات عمل EtherChannel هو زيادة السرعة بين طرفى الاتصال و زيادة الredundancy بدون التفكير فى حدوث loop
- Etherchannel يطلق عند تنفيذه بين two switch ولاكن اذا اردنا تنفيذ ذالك بين switch و server يطلق عليها Nicteaming





- يوجد نوعان من الetherchannel وهما :
  1. PAGP وهو خاص بشركة CISCO
  2. LACP وهو multivendor اى انه يعمل على اى vendor
- عند تفعيل PAGP على الswitch فسوف نجد ان له قيمتان
  1. Desirable وتعنى انه يعمل
  2. Auto وتعنى انه لن يعمل الا اذا كان الطرف المقابل desirable
- عند تفعيل LACP على الswitch فسوف نجد ان له قيمتان
  3. Active وتعنى انه يعمل
  4. Passive وتعنى انه لن يعمل الا اذا كان الطرف المقابل desirable
- لذالك لكى يعمل PAGP/LACP يجب على الاقل وجود طرف يكون Desirable/Active
- يجب للports ان تكون trunk

Configuration mode	Channel-group 1 mode desirable	Channel-group * mode
Privileged mode	Show eth	Show eth

- يستخدم لتشغيل الetherchannel على الports ويفضل استخدام امر rang لدخول على الinterfaces جميعها وتنفيذ عليها الامر
- يجب تحويل الports اولا الى trunk
- * يوضع مكنها رقم الetherchannel
- يتم اتباع الامر ب قيمة الmode والتى يمكن ان تكون desiable او auto او active او passive او on
- يستخدم لرؤية الetherchannels الموجودة فى الswitch

DHCP spoofing

- عند وجود two DHCP فى الشبكة يلزم ان يقومو بتوزيع IPs من نفس الrange ولا سوف يتم اعطاء اجهزة من rangs مختلفة يجعلهم غير فادرين على الاتصال
- DHCP spoofing هو attack يحدث عن طريق ايهام الاجهزة ان PC الخاص ب attacker يعمل كا DHCP ومن ذالك يمكنه اعطائهم default gateway مزيفة تسمح له بتحقيق man in the maddle attack كما يريد على سبيل المثال يعطيهم configuration
- يتم الحماية من هذا الattack عن طريق تحديد port فى الswitch ويكون هذا الport هو المسموح له فقط بارسال رسالة DHCP offer وتسمى هذه الطريقة DHCP snooping

Configuration mode	Ip dhcp snooping	• يقوم بتفعيل dhcp snooping على switchال	Ip dhcp snooping
Configuration mode	No ip dhcp snooping information option	• يستخدم هذا الامر لازالة الoption التى كانت موجود على الswitch سابقا	no ip dhcp snooping information option
Configuration mode	Ip dhcp snooping vlan 1	• يستخدم لتحديد الvlan التى سيعمل عليها الsnooping ونتبعه برقم الvlan • يجب كتابة هذا الامر لكل vlan على switchال	Ip dhcp snooping vlan
Configuration mode inside port	Ip dhcp snooping trust	• يستخدم هذا الامر داخل الport لجعله trusted ومسموح له بارسال رسالة dhcp offer	Ip dhcp snooping trust
Privileged mode	Show ip dhcp snooping	• يستخدم لرؤية اعدادات ال dhcp snooping على الswitch	Show ip dhcp snooping

CDP/LLDP

- CDP و LLDP هما برتكولان يستخدمان لمعرفة بنية الnetwork بشكل اسهل
- يتم استخدمهم من خلال الswitch
- CDP اختصار ل cisco descover protocol وهو لايعمل الا على اجهزة cisco عكس LLDP الذى يعمل على اى vendor
- CDP يكون مفعل بشكل تلقائى بينما LLDP يلزم تفعيله
- CDP و LLDP لايقوموا باظهار الPCs

Privileged mode	Show cdp ne Show cdp ne de	• يستخدم لمعرفة البنية الشبكة من خلال CDP • يمكن اضافة de الى الامر للحصول على بينات اكثر عن الrouters	Show cdp ne
Configuration mode	No cdp run Cdp run Cdp enable	• يستخدم لايقاف تشغيل الcdn • يمكن اذالة no واستخدام الامر لتشغيله مرة اخرى + انه يلزم استخدام امر cdp enable على جميع الports فى switchال	No cdp run

- لتشغيل LLDP نستخدم تمر LLDP run فقط ولا نحتاج لدخول الى الinterface

SNMP

- SNMP اختصار ل simple network management protocol
- SNMP هو protocol يتم استخدامه لمراقبة الroutres و الswitches فى الشبكة وعمل لهم management او configuration
- فى عملية المراقبة يمكننا معرفة
  1. Traffic الموجودة فى الnetwork
  2. Bandwidth
  3. CPU , RAM , Temperature الخاص ب الrouter
- SNMP هو open standard protocol اى يمكنه العمل على اى vendor
- يعمل فى الapplication layer اى انه يعمل على PCs ويسمى الPC فى هذه الحالة ب SNMP_Manger
- من البرامج التى يمكن العمل من خلالها على SMTP
  1. PRTG
  2. Solar winds
- اى router او switch سيتم تفعيل عليه SNMP يسمى SNMP_Agent

- اى agent يقوم بارسال ما يسمى ب MIB وهى اختصار ل management information base وهذه هى المعلومات الخاصة ب الagent ويقوم بارسالها الى manger
- يوجد من SNMP اصدرات مثل V1 و V2 و V3 وافضلهم هو V3 لان البينات فيه تكون مشفرة عند ارسالها ولاكن V3 غير مدعوم على كل الاجهزة لذالك فالمستخدم بكثرة هو V2

Configuration mode	Snmp-server community 123 rw	• يستخدم هذا الامر على الroutersاو الswitches لتشغيل عليهم الSNMP ويتم اتباعه بkey ثم قيمة من اثنان 1. Ro وتعنى read only وتعنى ان الmanager يمكنه عمل monitoring فقط 2. Rw وتعنى read write وتعنى ان الmanager يستطيع عمل monitoring و management	Snmp-server community

- ليس من المفضل عمل rw لاغراض security

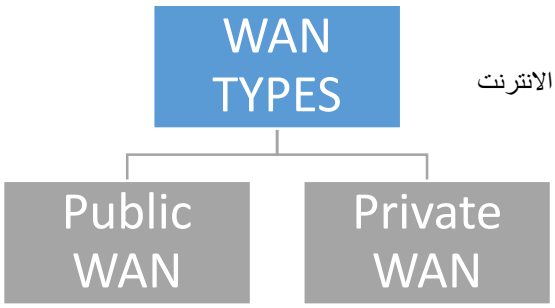
SysLog

- Syslog هى طريقة اخرى لمعرفة ما تم على الswitch او الrouter من خلال ملف يتم حفظ فيه اى alert او debug حصل على الrouter
- يتم تخزين ملف الSysLog فى الRAM ولاكن يمكن تخزينه على PC فى الnetwork من خلال TFTP
- فى الطبيعي لايتم تسجيل الdebuging messages ولاكن يمكن تفعيل التسجيل لها يدويا

Configuration mode	Logging on Logging on 192.168.1.50	• يستدخم لتشغيل خدمة SysLog على الrouter ويتم اتباعه برقم الIP الخاص بالPC الذى سيوضع عليه ملف syslog • يمكن عدم اضافة الIP ذالك لتشغيل الخدمة فقط ووضع الملف على الram	Logging on
Configuration mode	Logging trap 7	• يستخدم لتشغيل وضع الdebuging فى الsyslog • الرقم يعبر عن نوع الشئ الذى سيسجل لذالك فارقم 7 يرمز الى الdebuging	Logging trap 7

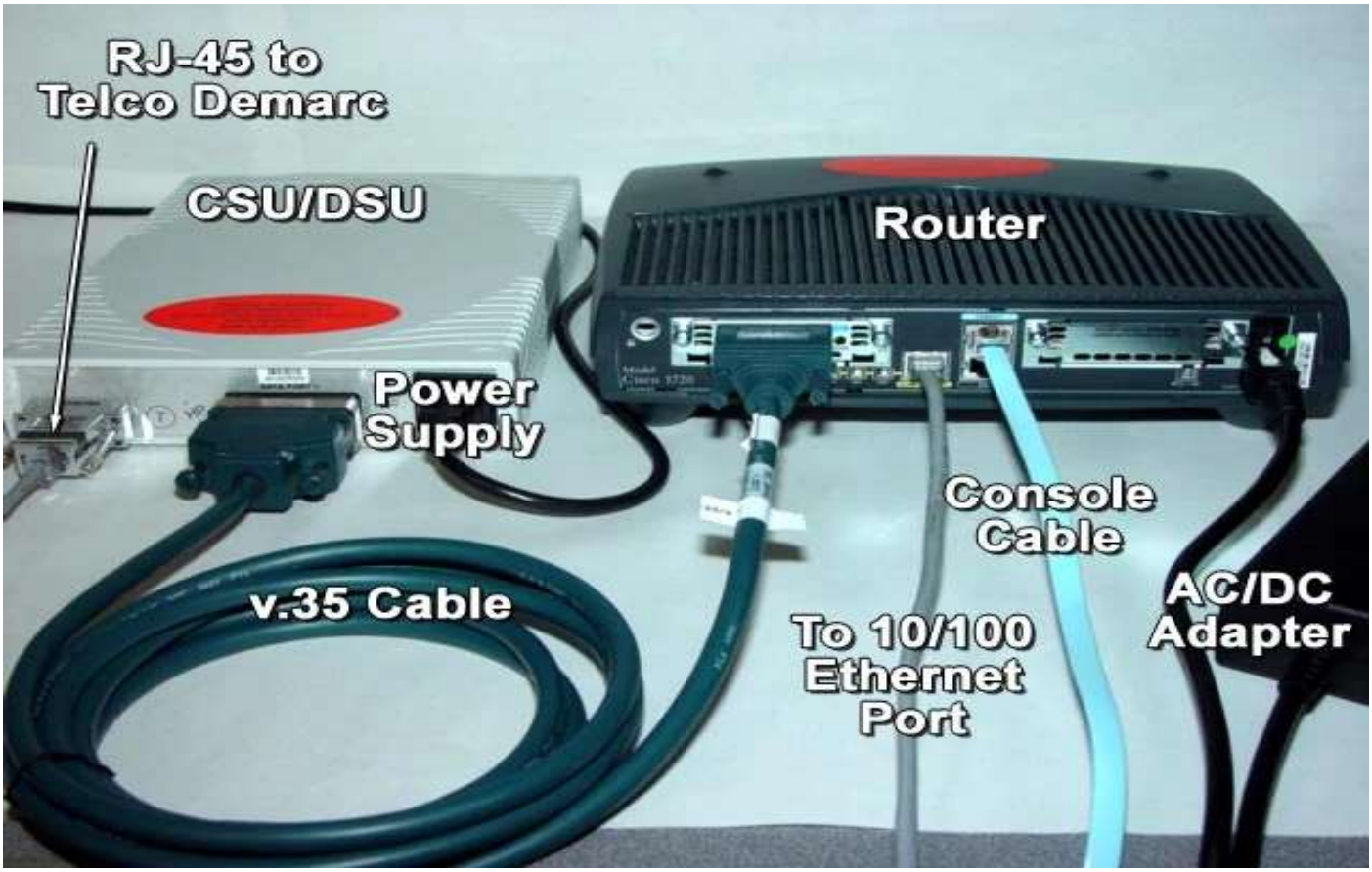
WAN Technology

- عند وجود اكثر من LAN وليكن لنفس الشركة ولاكن فى مدن مختلفة او فى دول مختلفة ونريد ان نقوم بتوصيلهم معا فاننا نستخدم WAN technology
- يوجد نوعان من ال WAN وهما
  1. Public WAN هى الinternet
  2. Private WAN وهى عندما نملك two LAN ونريد توصلهم معا وليس عبر الانترنت
- يوجد انواع مختلفة من الconnection التى يمكن استخدامها مثل
  1. LEASD Line
  2. Circuit switching
  3. Packet switching
  4. ATM switching
  5. Lable switching



LEASD Line

- وهى طريقة اتصال حيث توفر شركة الISP اتصال عبر line خاص محجوز ولايسمح لاى احد باستخدامه غير الشركة الحاجزة
- من مميزاته انه
  - Dedicated اى انه لشركة الحاجزة له فقط
  - Securie لانه يكون point to point ولايمكن لاحد استخدام هذا الline
  - الخدمة تكون متاحة دائما
  - سرعة الline تكون ثابتة
- من اهم عيوبه انه ذا تكلفة عالية جدا
- عندما نريد توصيل الفرعين معا فاننا ناتى بجهاز يسمى CSU/DSU وهو جهاز يعمل كا modem اى انه يقوم بتحويل digital signal الى analog siginal ويقوم بارسالها عبر سلك التلفون الى PSTN (الbox الخاص ب ISP)
- يتم توصيل الCSU/DSU بالRouter عن طريق serial cable ويسمى V35



Circuit switching

- هى طريقة لم تعد موجودة وظهرت فى بداية اختراع التلفون الارضى
- سرعتها قليلة جدا
- ظهرت منها اصدرات مثل dial-up و isdn
- ميزتها انها ذات تكلفة قليلة
- الاتصال فيه يكون ايضا point to point

Packet switching

- يطلق عليه ايضا Frame relay
- التصال فيه يكون point to multipoint اى انه لا يوجد dedicated path لنتقال الdata
- ترسل فيها الdata على شكل frams

ATM switching

- هى مثل الframe relay ولاكن الdata هنا ترسل فى شكل Cells
- اسرع من الframe relay

Lable switching

- يطلق عليه ايضا اسم MPLS
- وهو مستخدم حاليا بسبب سرعته العالية وقلة تكلفته
- فى MPLS عند ارسال data من lan الى ISP هانها تكون فى شكل ip packet وداخل الISP يتم تحويلها الى lable packet ويتم ارجعها مرة اخرى كى تكون ip packet عند وصولها الى الLAN الاخرى

- الprotocols المستخدمة فى LEASD line و circuit switching هما اثنان HDLC و PPP وجميعهم برتكولات point to point ولاكن HDLC لشركة CISCO و PPP هو open standard
- فى ال packet switching يتم استخدام protocol اخر وهو frame lelay

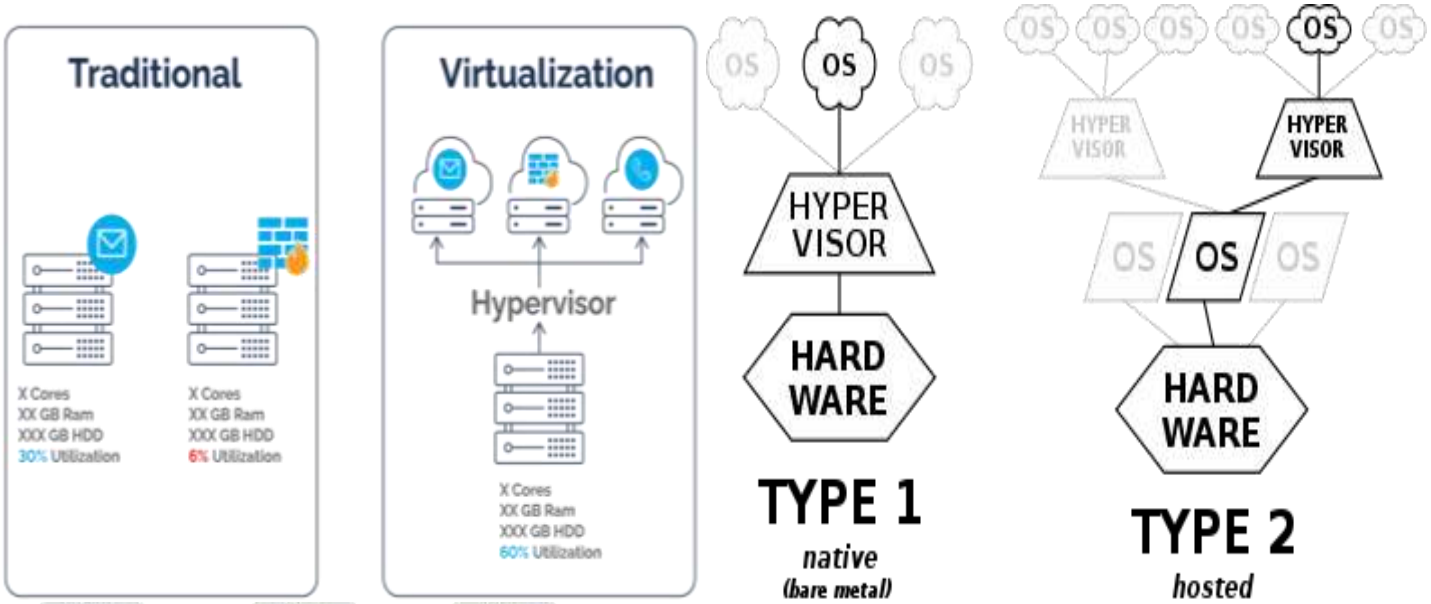
QOS

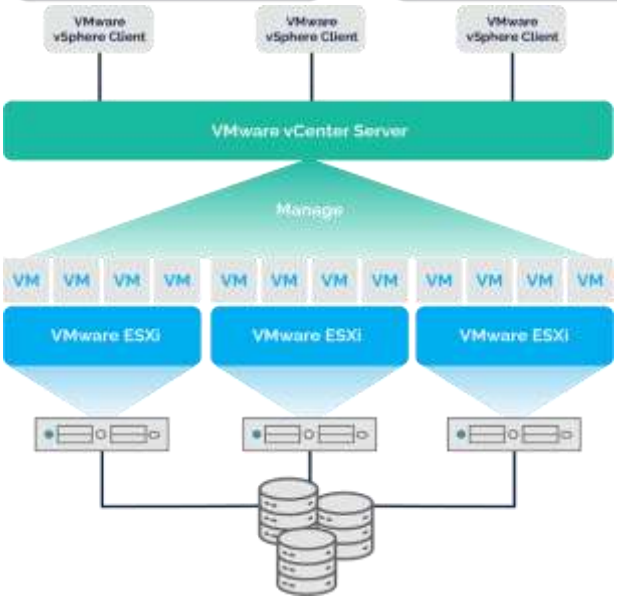
- هى اختصار ل quality of service
- يمكن للtraffic الموجودة فى الشبكة ان تكون voice او video او data وبسبب اختلاف انواعها ينتج اختلاف فى اولوية مرورها
- اى شكل من اشكال الdata التى يتم ارسلها من خلال الUDP تكون لها الاولوية بسبب كونها لاترسل مرة اخرى اذا لم تصل
- الاؤلوية تكون اكثر للvoice
- QOS تم انشائه بسبب وجود بعض المشاكل الممكنة فى الشبكة والتى تؤدى الى سوء الخدمة وهذه المشاكل مثل :
  1. نقص الbandwidth
     - نقص الbandwidth يؤدى اضرارا الى جعل بعض من الtraffic يتم تاخيره الى ان يقل ازدحام الnetwork
     - هنا يلزم استخدام الQOS لتحديد اولوية الtraffic التى يجب ايصالها اولا والtraffic الاخرى التى يجب ان تنتظر
     - بدون استخدام QOS فان مرور الtraffic يعمل بمبدا first in first out
  2. Packet loss
     - امكانية وجود packet يمكن ان تفقد عند ايصلها من الsource الى الdestination ولايعاد ارسلها مرة اخرى كما فى UDP يسبب الى تلف البينات وعدم وصولها بشكل سليم مثل الvoice او الvideo
     - وهنا يجب استخدام QOS لجعل ارسال هذا النوع من الdata يكون له الاولوية الاعلى ويتم بشكل لايؤدى الى فقدان الpacket
  3. Delay
     - عدم وجود تنظيم فى عملية ارسال الpacket قد يودى الى حدوث delay فى الشبكة ولذلك فاننا نستخدم QOS لتقليل هذا الdelay قدر الامكان
  4. Jetter
     - الjetter هو عدم انتظام الdelay او عدم وجود .syn فى ارسال الdata ومن هذه المشكلة حالة معروفة وهى عدم تزامن الصوت مع الصورة والjetter هو الفرق الزمى بين التزامن
- الادوات او الطرق التى يمكن من خلالها تحقيق الQOS كتالى :
  1. Classification & marking
     - وهى امكانية وضع اولوية او تصنيف بناء على نوع الdata ويحدث هذا التصنيف بناء من خلال
       a) access list عن طريق الport او الprotocol المستخدم
       b) NBAR وهو protocol يساعد الrouter فى تحديد نوع الdata ومن ذالك يتم تحديد اولويتها
     - الmarking هى عملية تتم بعد الclassification وتقوم باضافة خانة الى الpacket وهى TOS (type of servec) وهذه الخانة يوضع فيها رقم وكلما كان الرقم اكبر كلما ذادت اولويته و هذه الخانة اذا تم اضافتها من خلال الswitch تسمى COS
     - Marking تجنب الrouter التالى الذى سيستلم البينات الى عمل classification مرة اخرى
  2. Queing
     - وهى خاصية ارسال الdata صاحبة الاولوية الاعلى وجعل الاقل فى الاولوية تنتظر
  3. Conjestion avoidnes
     - وهى عملية تجنب حدوث اختناق فى ارسال البينات والذى قد يؤدى الى حدث packet loss
  4. Policing and shaping
     - وهم طريقتين لتعامل فى حالة امتلاء الbandwidth
     - Policing تقوم بايقاف ارسال الpacket فى حالة امتلاء الbandwidth
     - Shaping تقوم بتخفيف ارسال الpacket فى حالة امتلاء الbandwidth عن طريق وضع جزء منهم فى الbuffer
  5. Link effincey
     - وهى ضغط الdata عند ارسالها لتوفير bandwidth فى الline

Virtualization

- هى تقنية انشاء مجموعة من virtual devices من خلال phiscal device عن طريق تقسيم الresources عليهم
- فى حالة استخدام one phiscal device موجود عليه جميع الservices بدون عمل virtualization سيؤدى ذالك الى حدوث بعض المشكلات مثل
  1. حدوث load على السيرفر مما يؤدى الى توقفه
  2. امكانية تاثير خدمة على الاخرى
- الresources التى سيتم توزيعها تشمل الCPU و RAM و HDD و NIC
- من اهم مميزات الvirtualization :
  1. يقلل التكلفة
  2. تذيد الsecurity حيث ان كل virtual device مستقل عن الاخر
- يتم تحقيق virtualization من خلال ما يسمى بhypervisor والذى يمكن ان يكون software او frameware

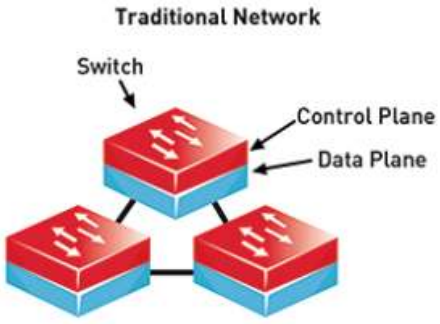
- يوجد نوعان لhypervisor وهما type 1 و type 2



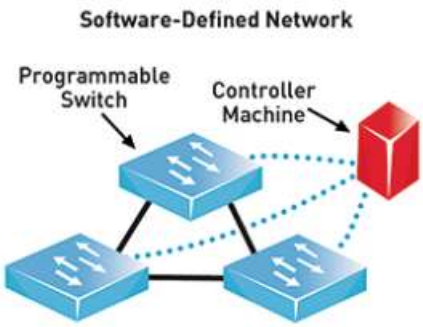


- Type 1 يستخدم اكثر فى الشركات بينما Type 2 يستخدم فى التدريب
- الاختلاف بين type 1 و type 2 ان type 2 يكون موضوع على operating system بينما type 1 يكون على الhardware بشكل مباشر ولذالك فا type 1 يكون frameware و type 2 يكون software
- اشهر hypervisor type 2 هم VM workstation من شركة VM ware و virtyal box من شركة Oracle
- اشهر hypervisor type 1 هم ESXI من شركة VM ware و hyper-v من شركة Microsoft و VM server من خلال شركة oracle وهم يكونو فى شكل operating system نقوم بعمل boot من خلال usb او CD عند تثبيتهم
- يوجدما يسمى ب vcenter وهو software يقوم بعمل manage للانظمة الموجودة على الhypervisors

SDN



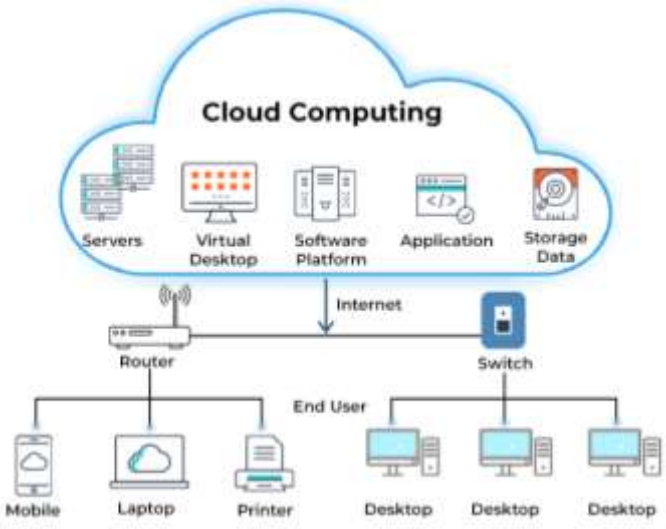
- هى اختصار ل software defined networking
- اى router او switch يحتوى على ثلاث اجزاء وهم :
  1. Management plane
     - وهو الجزء المسؤل عن عمل management فى الswitch او الrouter
  2. Control plane
     - هو الجزء المستخدم فى الlogic وتنفيذ الالجورزم واعطاء الاوامر
  3. Data plane
     - هو الجزء الخاص بتنفيذ اوامر الcontrol plane
- تقنية الSDN تقوم على الغاء الcontrol plane من الswitches وجعل جهاز واحد هو ما يقوم بها والswitches تعمل كا data plane فقط



- الجهاز الخاص بعمل control يسمى controller وقوم بعمل monitor للشبكة كما يقوم ايضا بعمل الconfiguration و الtrobleshooting ويحدث ذالك من خلال application على الcontroller
- الapplication الموجود على الcontroller يمكن ان يتم شرائه او برمجته من خلال لغة برمجة python وغالبا ما تستخدم
- برتوكول الopen flow هو من يعمل بين الswitches وبين الcontroller

Cloud computing

- Data center هو مكان تحفظ فيه الservers و الswitches و الrouters وغالبا توضع فى حامل يسمى RAC
- الdata center يلزم اضافة لها تكيفات لمراعة درجة الحرارة والتاكد من امداد الكهرباء الثابت لها
- Cloud computing هو استخدام data center من شركة اخرى او من ISP وهذه الشركة او ISP هى من يجب عليها الاهتمام بال data center من تثبيت درجة الحرارة والمحافظة على الكهرباء ومواجهة الاخطار مثل الحرائق
- لذالك فا كلمة cloud تشير الى الinternet او الى ISP
- من اشهر الشركات التى توفر cloud computing هم شركتى Microsoft و Amazon
- من مميزات الcloud computing :
  1. Copute power
     - وتعنى ان الاجهزة التى سيتم توفيرها فى cloud ستكون قوية من ناحية الامكنيات
  2. Secure connection
     - ستم توفير حماية للبينات الموجودة فى الcloud
  3. High availability
     - سيتم الحفاظ على توفر البينات
  4. Scalability
     - سهولة تطوير الاجهزة والresources
  5. Global access
     - امكانية الوصول لها من اى مكان



- يوجد لل3 cloud model وهم
  1. Public cloud
     - جميع الاجهزة فى الcloud
  2. Private cloud
     - جميع الاجهزة لاتكون على الcloud وتسمى on premise
  3. Hybrid
     - وهو النظام الاكثر استخدما وفيه يكون جزء من الخدمات على الcloud و الجزء الاخر على ارض الواقع

puplic cloud

private cloud

Hybrid