2023

network+ by al sadek

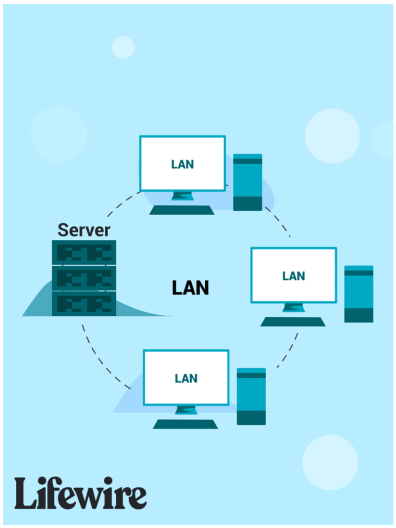
Introduction to network

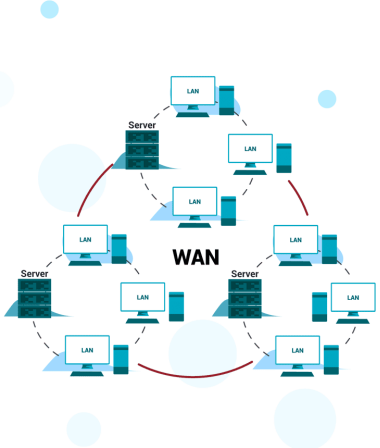
- Network : هى مجموعة من الاجهزة المتصلة معا
- اى device يطلق عليه nodes فى network
- اهمية الnetwork انها تقوم بمشاركة hardware و data

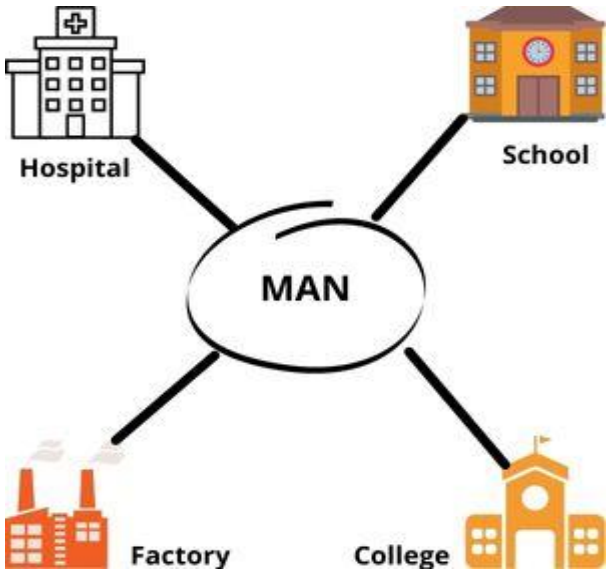
- Any network must have
    1. Computer system
    2. Network media (الوسط المستخدم لنتقال البينات)
    3. Network interface (وهو المسؤل عن تحول البينات الى الشكل الملئم للوسط)
    4. Network protocol

Network type

1. by geographic area
    - Local area network(LAN) : group of computers and other devices are usually located in small area like house or small office or a single building
    - In LAN all computer connect to each other through one or more switches
    - Wide area network(WAN) : A group of one or more LANs over a large geographic area
    - Each LAN in WAN require a router to connect to each other
    - Metropolitan area network (MAN) : used like when a company has two office in the same city
    - MAN similar to WAN but smaller in geographical area
    - WLAN : وهى لاتختلف عن الLAN ولاكنها wireless
    - يطلق على LAN ايضا اسم CAN والفرق هنا ان الCAN تكون LAN او اكثر وكل LAN فى مبنى مختلف
    - PAN(personal area network) وهى network مكونة من عدد صغير من devices متصلة معا وغالبا عن طريق Bluetooth (WPAN)
    - GAN (global area network) هى تماما مثل WAN ولاكنها تكون تحت تحكم شركة واحدة او منظمة واحدة عكس WAN
2. By host role
    - Peer to peer : any computer in the network can be client (request service) or server (provide the service)
    - Advantages of peer to peer is it easy to install and it’s not expensive
    - Disadvantages of peer to peer is that non scalable
    - Client/server : LAN in which the client computer can’t be the server and server can’t be client
    - The disadvantages is it hard to install and it’s expensive
    - The advantages is that is scalable

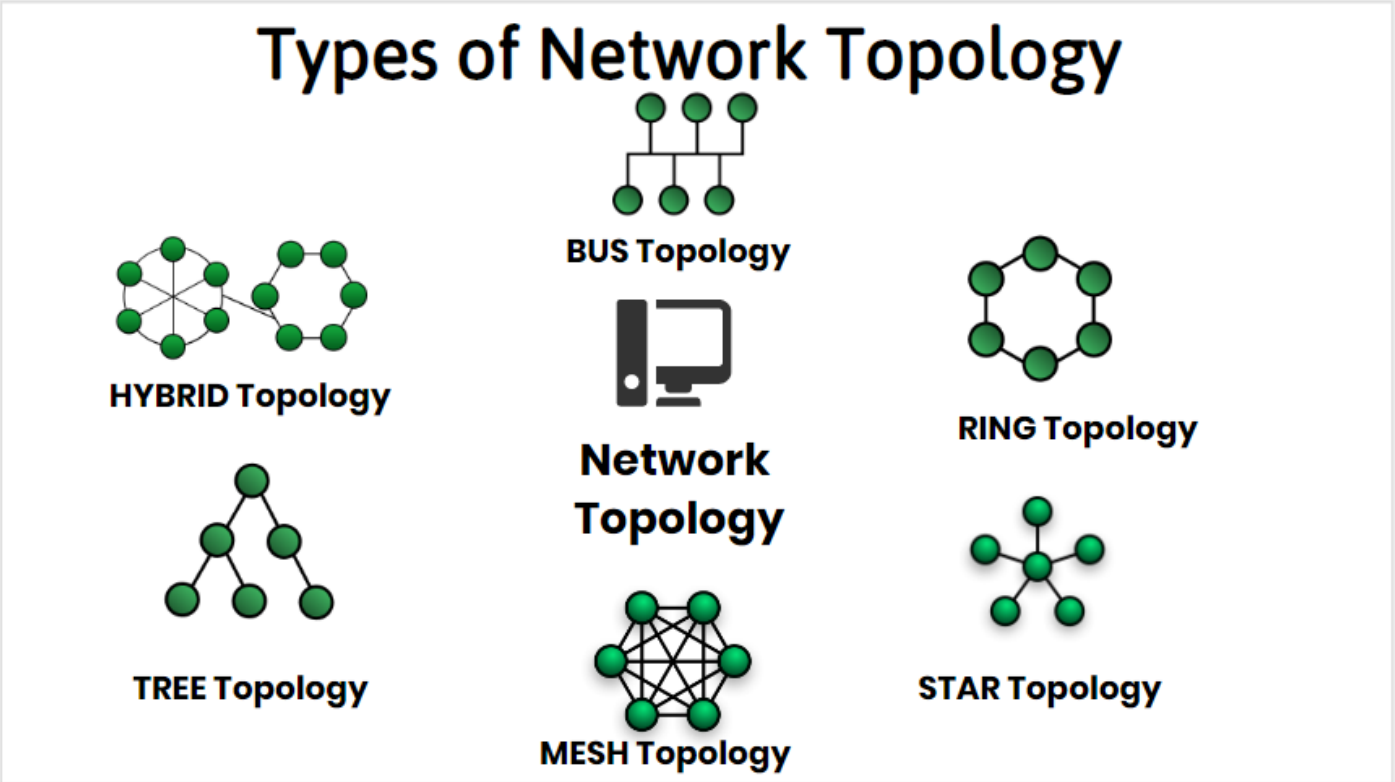






Network topologies

- Network topologies : how the network devices are physically cabled together or how they logically communicate
- Bus topology
  - وهو من اقدم انواع topology والتى لم تعد موجودة وتتصل مع بعضها عن طريق central cable والذى يخرج منه drop cable المسؤل عن توصيل الاجهزة معا
  - يجب ان ينتهى بterminator لكى يلاشى عملية الارتداد للبينات
  - اى ارسال للبينات يتم استلامه من جميع الاجهزة وهذا انوع من الconnection يسمى broadcast connection
- unicast : point to point communication
- multicast : point to specific group communication
  - من مميزاتها انها سهلة الانشاء ومن عيوبها انه لاضافة او اذالة جاهز يلزم ايقاف الشبكة كاملة
- Ring topology
- You must bring the whole network down before computers could be added
- If one connection or one device goes down the network goes down
- The flow of data is unidirectional (flow in one direction)
  - يوجد نوع من ring وهو dual ring topology وهو يكون ring ولاكن يمكن لdata ان تسير فى اتجهان مختلفان
  - هى من الtopology الغير موجدة هذه الايام
- Mesh topology : every device connects to every other device
  - من مميزتها انها تقوم بتوفير fault tolerance عالى جدا
  - من عيوبها انها ذات تكلفة عالية لزلك تكون نادرة ولاكنها موجودة
- Star topology
  - هو النوع الاكثر شيوعا وفيه الاجهزة تتصل عن طريق central device ويمكن ان يكون (hub- switch- access point)
  - عن حدوث مشكلة فى nodes لايؤثر ذالك على الشبكة



Network terms

- Subnet : هو جزء من network تشترك nodes الموجودة فيه فى جزء من العنوان
- Router هو المسؤل عن ربط اجزاء subnet معا فى الnetwork
- الفرق بين network و internetwork ان network اكتر من LAN متصلة معاتحت تحكم شخص واحد او شركة واحدة بينما internet اكتر من LAN متصلة معا ولاكن تحت تحكم اشخاص مختلفة او شركات مختلفة
- internet service provider : ISP
- Client computer هو الكمبيوتر المحتاج الى services بينما الserver computer هو الكمبيوتر االموفر لهذه الservices
- Server computer يحدد بشكل اساسى من operating system ولايس من hardware
- Operating system يوجد منه نوعان الاول client OS والثانى network OS وهو المستخدم فى server ويسمى ايضا server OS
- Host مصطلح يطلق على اى جاهز فى network حاصل على IP
- Intranet وهو WAN متصلة عبر internet ولاكنها private
- Extranet وهى intranet ولاكن يكون مسموح باتصال اجهزة معينة من خارج WAN

Server roles

- File server هو server يتم استخدامه لتخزين عليه البينات ومشركة هذه البينات
- Print server هو server المسؤل عن عملية تنظيم الطباعة فى الشركات
- Web server هو server الذى يدير عملية hosting للمواقع
- اشهر البرامج التى تستخدم فى انشاء web server هما apache لنظام Linux او IIS فى نظام windows server
- Mail server وهو server المسؤل عن ادارة عملية ارسال و استلام الايميلات
- Exchange هو البرنامج المسؤل عن انشاء mail server
- Proxy server هو server المسؤل عن تنظيم عمليه اتصال clients ب internet مثل تحديد المواقع المسموح بها او تحديد كمية البينات المسموح استخدامها
- Active direct server هو برنامج يستخدم على انظمة windows servers لتحقق من صلاحية الوصول من بينات معينة

IP (نبذة بسيطة)

- IP هو نظام لعنونة الاجهزة فى network
- IPv4 يتكون من 4 خانات تسمى octet وكل خانة قيمتها تتروح بين 0-255
- IPv4 يمكن تقسمه الى جزئان وهما network address و host address ويمكن معرفة ذالك من خلال subnet mask حيث اى مكان فى IP يقابله 255 فى subnet mask هو جزء network address بينما الجزء الاخر هو host address
- Host address المقصود به رقم الcomputer فى الشبكة
- الاجهزة التى تحتوى على network address مختلفين يعنى ذالك ان كل جهاز فى شبكة مختلفة ولايمكن توصلهم معا direct الا من خلال router

IPv4 Address. . . . . : 192.168.1.12

Subnet Mask . . . . . : 255.255.255.0

MAC address (نبذة بسيطة)

- Mac address : it’s physically burned on network interface
- IP address it’s logically address and it can be change
- MAC stands for media access control

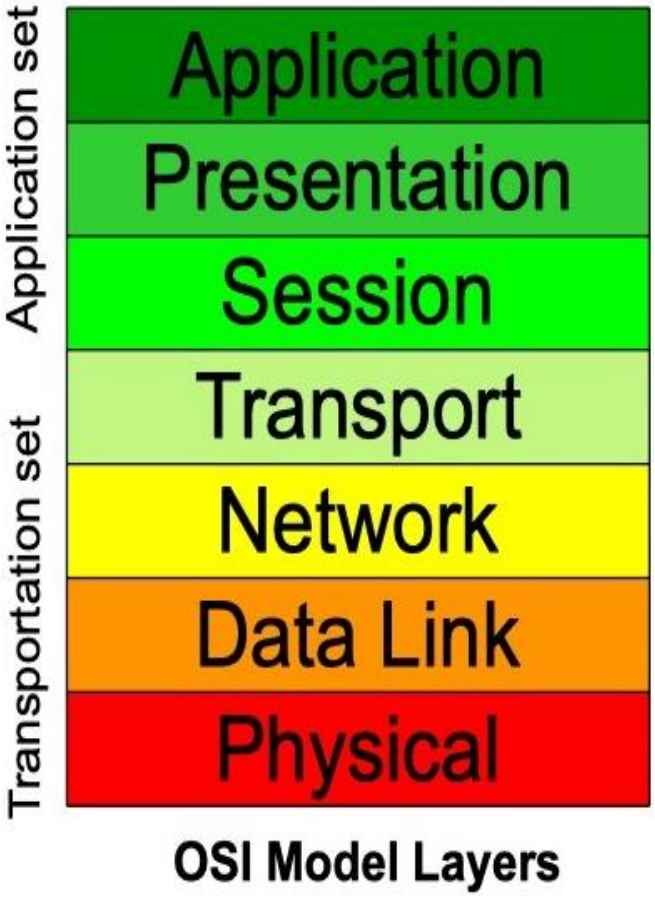
- المنظمة المسؤلة عنه هى IEEE
- يكتب بالاراقم hexa-decimal ويتكون من 6 اجزاء

- يتكون من جزئان الاول وهم الثلاث خانات الاولى ويمثلو اشركة المصنعة (OUI) والجزء الاخر يتكون من الثلاث اجزاء الاخرة ويميز كرت (NIC)network

Physical Address. . . . . : 3C-A9-F4-B7-4B-24

OSI model

- هو اختصار ل open system interconnection
- وهو نظام تم انشائه لوضع معاير للاتصال بين الاجهزة او اشبكات وتم انشاء هذه المعايير بواسطة شركة ISO حيث جعل الاتصال بين الاجهزة او الشبكات ينقسم الى طبقات وكل طبقة تقوم بمهمة معينة لنجاح عملية الاتصال
- قبل وضع نظام OSI كان يصعب على الشبكات المستخدمة لادوات من شركات مختلفة ان تتصل معا
- OSI model يوجد فى كلا جنبى الاتصال (source, destination)
- من مزايا نظام OSI هو انه سهل عملية development و design و troubleshooting
- ترتيب الطبقات يبدا من الphysical وينتهى ب application
- يمكن تقسم الlayers الى مجموعتان
  - الاولة وتضمن physical و data link ويشار لهم ب network architecture
  - الثانى وتشمل باقى الlayers ويشار لهم ب network protocol suit
- توجد تقسيمة اخرى كتالى :
  - من session الى application تسمى application
  - Network و transport يسموا transport
  - Physical و data link يطلق عليهم network architecture
- تقسيم layers الى مجموعات يسهل عملية التعامل معهم



Application layer

- يطلق على اى services فى هذه الطبقة ب protocol
- هى حلقة الوصل بين الuser وباقى الطبقات
- من اشهر protocols الموجدة فى هذه الطبقة وهم(HTTP, FTP, SMTP)
- هى اكثر layer تحتوى على protocols

Presentation layer

- هى المسؤلة عن عملية formatting مثل syntax و compression و encryption
- Syntax المقصود به format الخاص بداتا مثل الformats الخاص بنص كا ASCI او الخاص ب الصوت كا mp3 وهكذا
- Compression هى عملية ضغط البينات وكذالك encryption هى عملية تشفير البينات

Session layer

- هى الطبقة المسؤلة عن عمل sessions بين الاجهزة
- الsession هو اى عملية اتصال بين جهزان
- فى حالة servers اى session يتم له session ID لتميز بين الاجهزة عند اتصالهم بserver فى وقت واحد
- يمكن اعطاء اكثر من session ID لنفس الhost عند وجود اكثر من connection (مثال : فتح موقع من اكثر من متصفح من نفس الجهاز)
- Session period هو وقت يعطيه الserver لsession لتحديد مدة الاتصال به وعند انتهائه وعدم وجود تفاعل من client تلغى session
- Session period من مميزاته ان يقوم بتخفيف loading الموجود فى server

Transport layer

- هى الطبقة المسؤلة عن كيفية نقل البينات الى destination وفيها يتم تحديد port address
- تقوم ب تجزئة data الى segments و ترقيم كل segment وهو ما يساعد destination device على اعادة ترتيب segment مرة اخرى لجعلها فى صورة data مرة اخرى
- يمكن ان تسلك كل segment مسار مختلف للوصول الى destination device

Network layer

- هى المسؤلة عن نقل البينات بين network او بين internetworks من خلال عملية routing
- عملية routing هى عملية نقل البينات من router الى اخر للوصول الى destination device
- تسمى data فى هذه المرحلة ب packet
- فى هذا الطبقة يتم تحديد source IP و destination IP

Data link layer

- هو وسيط بين transmission medium الموجود فى physical layer و network layer
- تسمى data فى حذه الطبقة ب frame
- تنقسم الى two sub layer كتالى :
  - الطبقة الاولة يوجد بها protocol يسمى LLC وهو interface بين network layer و physical layer
  - الطبقة الثانية يوجد بها protocol يسمى Media access control(MAC) وفى هذه الطبقة يتم تحديد logical topology وتتم عملية MAC addressing

Physical layer

- فى هذه الlayer تتحول الdata الى bits ثم ترسل عبر network medium

---

- Transport, network, data link هم الطبقات التى تتم فيهم عملية addressing كتالى
  - Transport تتم فيها عملية port addressing اى انها توفر source port address and destination Port address
  - Network تتم فيها IP addressing اى انها توفر source IP address and destination IP address
  - Data link تتم فيها MAC addressing اى انها توفر source MAC address and destination MAC address

Port address

- الport هنا هو logically port
- Port address هو رقم يحدد الخدمة او المكان المرسل اليه البينات
- يوجد بعض ports المشهورة مثل 80 الذى يستخدم للاشارة الى web service او 53 الذى يشير ال DNS service او 25 و يدل على email service
- المنظمة المسؤالة عن port address هى iana
- عدد ports هو 65534 (من 0 الى 65533)
- الports من 0 الى 1023 يتطلق عليهم well known ports هو ports محجوزة لخدمات معينة مثل :

Well-Known Ports

Service	Port	Function
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20, 21	File transfer
DNS	53	Name resolution
SMTP	25	Internet mail
POP3	110	Post Office Protocol (POP) mailbox
IMAP	143	Internet Message Access Protocol (IMAP) Mailbox
Telnet	23	Remote login
SSH	22	Secure remote logn

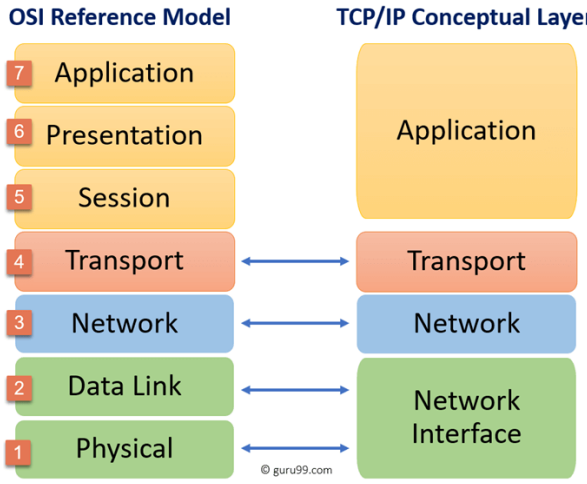
How the OSI make connection in transport, network, data link layer

- يلزم لانشاء اتصال ان يتم تحديد source و destination لكل من port و IP و MAC
- يتم تحديد source port من client device (اكبر من 1023) ويتم تحديد destination port من خلال protocol المطلوب
- يتم تحديد source IP من خلال client device و destination IP من خلال server device
- يتم تحديد source MAC من خلال client device بينما تحديد destination MAC يلزم استخدام address resolution protocol (ARP)
- لكى يقوم ARP بتحديدMAC address بقوم بارسال طلب باستخدم IP(source and destination) وباستخدام source MAC ويجعل destination MAC بقيمة FF:FF:FF:FF:FF:FF والذى يعنى ان هذه الاشارة من نوع broad cast (تصل الى جميع الاجهزة)فيقوم الجهز الذى يحمل الIP destination الصحيح فقط بالرد على الطلب بARP اخر موجود فيه MAC address المطلوب والرد يكون من نوع unicast
- يقوم ARP بتخزين MAC address فى ARP Cash فى حالة التعامل مع الserver device مرة اخرى
- فى حالة تغير network card الخاص ب server device يلزم عمل clear ل ARP cash فى حالة عدم الحصول على اتصال من server device

TCP/IP Protocol suite(DOD model)

- Protocol : rules for communication and data exchange
- Stands for transmission control protocol / internet protocol

- تم انشائه بواسطة وزارة الدفاع فى امريكا لذلك يطلق عليه احينا DOD model
- تم انشائه فى سنة 1974 وتم تقسيمه الى two protocol اساسين وهما TCP و IP فى سنة 1978
- وتم استخدامه فى سنة 1983 كا الprotocol الرسمى لشبكة ARPAnet وهى الشبكة التى تحولت بعد ذالك الى internet
- لايتم استخدام OSI model فى الحياة العملية وانما يستخدم كمرجع لشرح
- DOD model هو ما يتم استخدامه فى الحياة العملية
- DOD model هو نموزج ابسط من OSI model حيث ان DOD model يحتوى على 4 طبقات عكس OSI الذى يحتوى على 7 طبقات



- جميع المهام التى تحصل فى application و presentation و session فى OSI model تحصل فى طبقة application فى DOD model
- Application layer فى DOD model تسمى ايضا ب process
- Transport layer فى DOD model تسمى ايضا host to host
- Network layer فى DOD model تسمى ايضا internet layer
- Data link layer و physical layer يماثلو network access layer

Protocols

- HTTP(port 80)
- Stands for hyper text transport protocol
- هذا protocol هو ما يحدد طريقة تبادل html document مع web server
- البينات المرسلة باستخدام HTTP تكون clear text لزلك يمكن بسهولة قرائة البينات فى حالة التوسط فى الاتصال(مثل man in the meddle attack)
- HTTPS(port 443)
- وهو عبارة عن HTTP و برتوكول اخر هو SSL

Secure protocols

- SSL (port 465)
- SSL stands for secure socket layer
- SSL : method of encryption

- TLS (port 995)
- TLS protocol يستخدم ايضا لتشفير مثل SSL protocol

Transport protocols

- هى الprotocols التى تحدد كيفية نقل البينات وقواعد وصول البينات وطريقة التعامل فى جالة فقدنها
- TCP وهو connection oriented protocol اى انه يقم بتاكد من وصول البينات الى destination device
- UDP وهو connectionless protocol اى انه لا يقوم بتحقق من استلام البينات ولاكن ميزته انه سريع لذالك يستخدم فى live streaming و game
- TCP و UDP يوجدان فى transport layer فى DOD model لذالك اى protocol فى application layer يجب ان يستخدم واحدا من هما

File transfer protocols

- FTP(TCP port 20,21) وهو protocol يستخدم لارسال الملفات والتاكد من استلامها
- TFTP(UDP port 69) وهو protocol يستخدم لاتاكد من ارسال الملفات بشكل سريع ويستخدم فى بعض الحالات مثل نقل الملفات داخل الشبكة الواحدة
- FTP و TFTP يتم استخدامهم فى عملية ارسال او استلام الملفات ذات الحجم الكبير لذالك يتم استخدام FTP فى عملية download
- SFTP(TCP port 22) و SCP(TCP port 22) وكلاهما يستخدم ايضا لنقل الملفات ولاكن بشكل اكثر امنا

Email transfer protocols

- SMTP(TCP port 25)
- POP3 (TCP 110)
- IMAP(TCP 143)
- فى عملية ارسال الemail من جهاز الى اخر الprotocol المستخدم للارسال هو SMTP
- لاكى تصل الرسالة الى الجهاز المستقبل لها يمكنها المرور عبر اكثر من server

- لاستلام الemail يمكن استخدام SMTP ويمكن استخدام POP3 لانه يمكنه عمل download للemail على الجهاز المستقبل ورؤيته فى حالة offline
- فى POP3 فى حالة فقد الرسالة من الجهاز المستقبل لها فانها لاتكون موجود فى mail server
- IMAP هو الprotocol الافضل لاستلام الرسائل لانه يمكنه عمل download للرسائل على الجهاز المستقبل او جعلها موجودة على mail server لذالك يفضل استخدامه

Network services protocols

- DHCP(UDP port 67)
- اى جهاز على الnetwork يلزم عمل له بعض configuration مثل تحديد IP و DNS يمكن عملها بشكل يدوى او من خلال DHCP server
- DNS(TCP & UDP port 53) هو المسؤل عن عملية تحويل domain name الى IP
- NTP(UDP 123) وهو الprotocol المسؤل عن عمل تزامن فى الوقت

Network management protocols

- SNMP(UDP port 161) ويستخدم لجمع ومعرفة معلومات عن الاجهزة المتصلة على الشبكة
- LDP ويستخدم لتنظيم مشاركة الطابعات
- TELNET(TCP port 23) وكان يستخدم لتحكم فى جهاز اخر من خلال command prompt ولاكن لم يعد يستخدم لانه غير امن
- SSH(TCP port 22) وهو بديل TELNET لانه يتميز بالامان
- RDP(TCP port 3389) تم انشائه من خلال Microsoft لremote desktop
- TELNET و SSH يتم استخدامهم من خلال CMD بينما RDP يتم استخدامه من خلال GUI (واجهة رسومية)

Control protocols

- ICMP ويستخدم من قبل router فى حالات معينة ويستخدم ايضا فى application/function ping
- IGMP يستخدم مع multicast connection

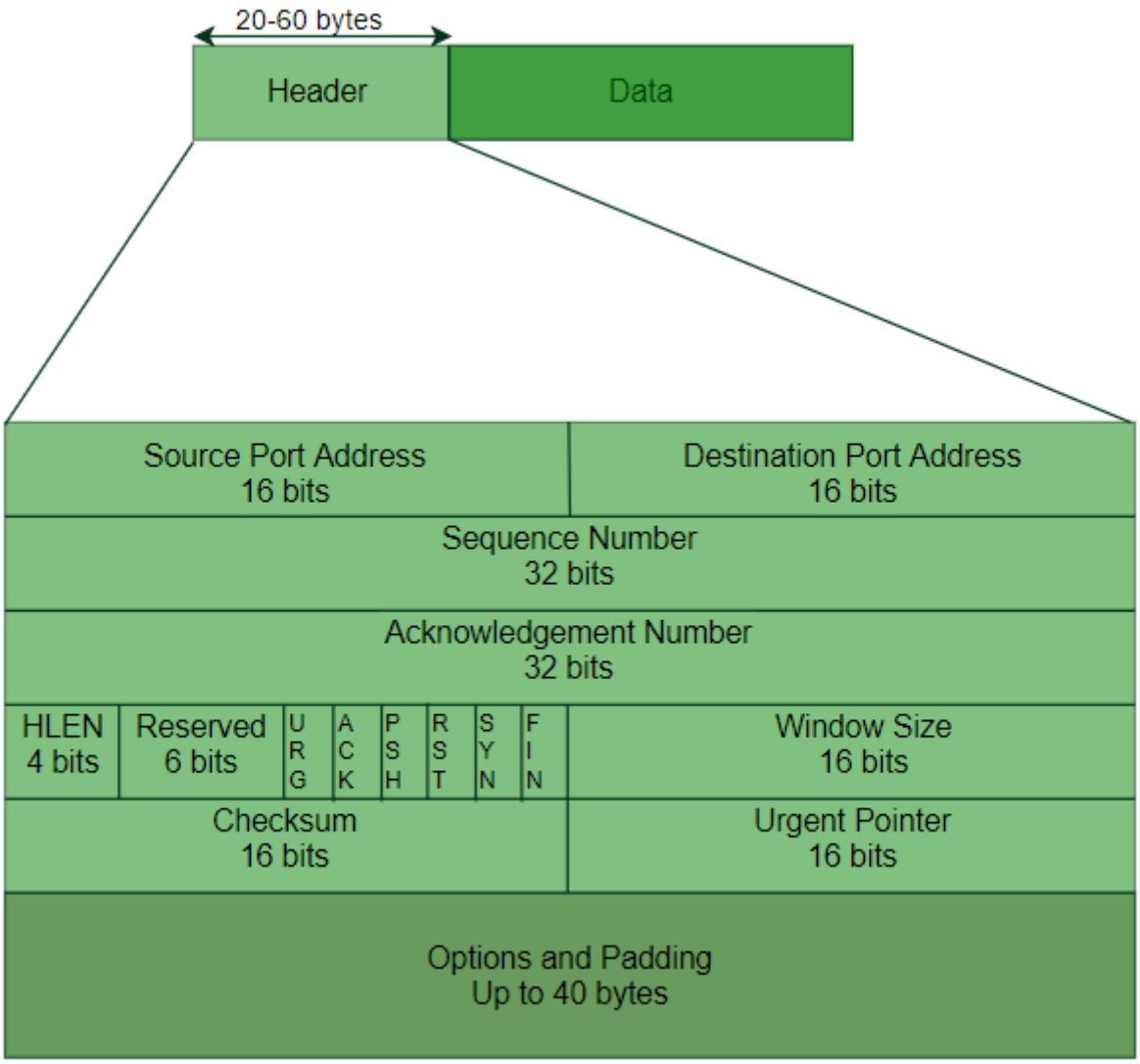
Multimedia/communication protocols

- SIP(VOIP)(TCP/UDP port 5060/ TCP port 5061) يستخدم فى voice and video calls و chatting و online games
- RTP(VOIP)(UDP port 5004/ TCP port 5005) يستخدم فى voice over IP
- ويوجد ايضا MGCP و H.323 والذى يستخدم ايضا فى multimedia communication

---

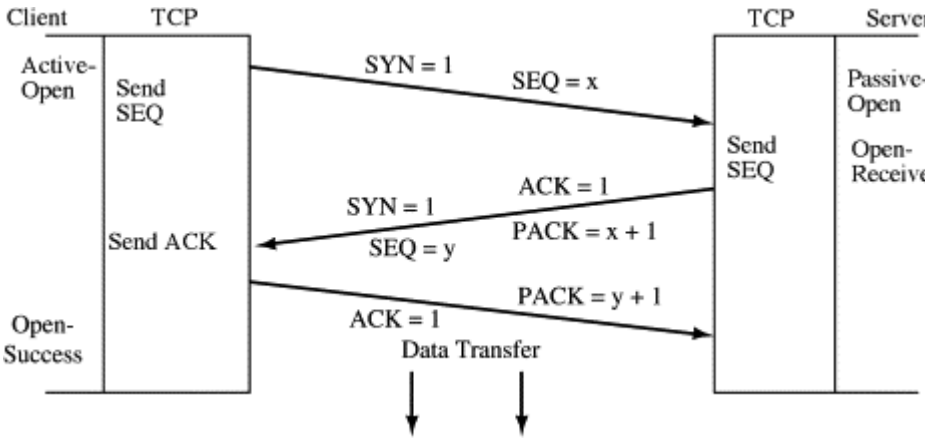
TCP

- Stands for transmission control protocol
- Connection oriented protocol بمعنى انه يتحقق من الاتصال اولا قبل ارسال البينات
- عملية التحقق من البينات تسمى three way handshake
- يقوم بعملية sequencing وهى عملية ترقيم segments لترتبها مرة اخرة فى جهاز destination
- يقوم بعملية checksums وهى عملية استخدام رمز او حرف فى كل segments لتاكد من سلامة البينات
- يقوم بعملية flow control وهى عملية التحكم فى كم data المرسلة
- يقوم destination device بتخزين segments فى مكان يدعى buffer وعدم التحكم فى flow control قد يؤدى الى امتلائه مما يؤدى الى اتلاف البينات
- كل من connection oriented و sequencing و checksums و flow control يحدث فى segment header ويسمى ايضا TCP header



- Header وهى data المضافة الى segment للاستخدام فى عملية الارسال
- الجزء الاول هو الجزء الخاص ب source and destination port
- Sequence number هو الجزء الخاص بترقيم segment
- Acknowledgement هو الجزء المستخدم من قبل destination لرد والتاكد من استلام البينات من خلال رسالة تسمى ACK
- Header length(HLEN) ويحتوى على اجمالى طول header
- Reserved هو مكان محجوز لستخدمات معينة
- Flags يتكون من 6 flag وكل واحد قيمته bit 1 وكل flag يحمل القيمة 1 يشير الى مكان فى segment يجب قرائته من قبل destination بينما عندما يحمل القيمة 0 يدل على عدم اهمية قرائة المكان الذى يشير اليه
  1. URG يشير الى Urgent pointer
  2. ACK يشير الى acknowledgement
  3. PSH يقوم بتنبيه destination بان segment يجب ان تصل الى الapplication الذى يريد البينات مباشرة بدون وضعها فى buffer
  4. RST وهو تنبيه الى destination بضرورة عمل reset ل connection
  5. SYN يستخدم لعملية synchronization وهى عملية ارسال sequence number وانتظاره من destination مضاف اليه واحد وهذه العملية لايتم ارسال فيها data فى segment
  6. FIN وهى ل destination لتعلمه بان هذه segment هى الاخيرة
- Window size ويستخدم فى عملية flow control بحيث يستخدم فى تحديد حجم segment وعددها
- Checksum وهى التى تحتوى على character لتاكد من سلامة ارسال البينات

- Options وهى تحتوى على مجموعة من الاعدادات الخاصة
- Padding يستخدم لتاكد من ان segment header مضعفات ل 32 bit
- Data لا يتم ارسالها فى segment الا بعد حدوث عملية three way handshake
- Three way handshake وهى عملية تتم قبل بدا ارسال البينات ويتم فيها ارسال 3 رسائل بين source و destination لتاكد من قابلية ارسال واستلام البينات كتالى :
  1. رسالة SYN وهى تكون من source الى destination وفيها يقوم source بنشاء sequence number عشوائى ويكون فى sequence number field ويحدث activation لSYN flag اى تكون قيمته ب 1
  2. رسالة ACK وهى ترسل من destination الى source ويتم تفعيل فيها ACK flag ويوضع فى acknowledgement field ال sequence number ولاكن مضاف اليه 1 بلاضافة الىsequence number منشئ من خلال destination اى ان SYN flag تكون ب1
  3. يقوم source بالرد برسالة فيها الsequence number الخاص ب destination مضاف اليه 1 ويكون موضوع فى خانة acknowledgement ويضع فى خانة sequence number الsequence الاول

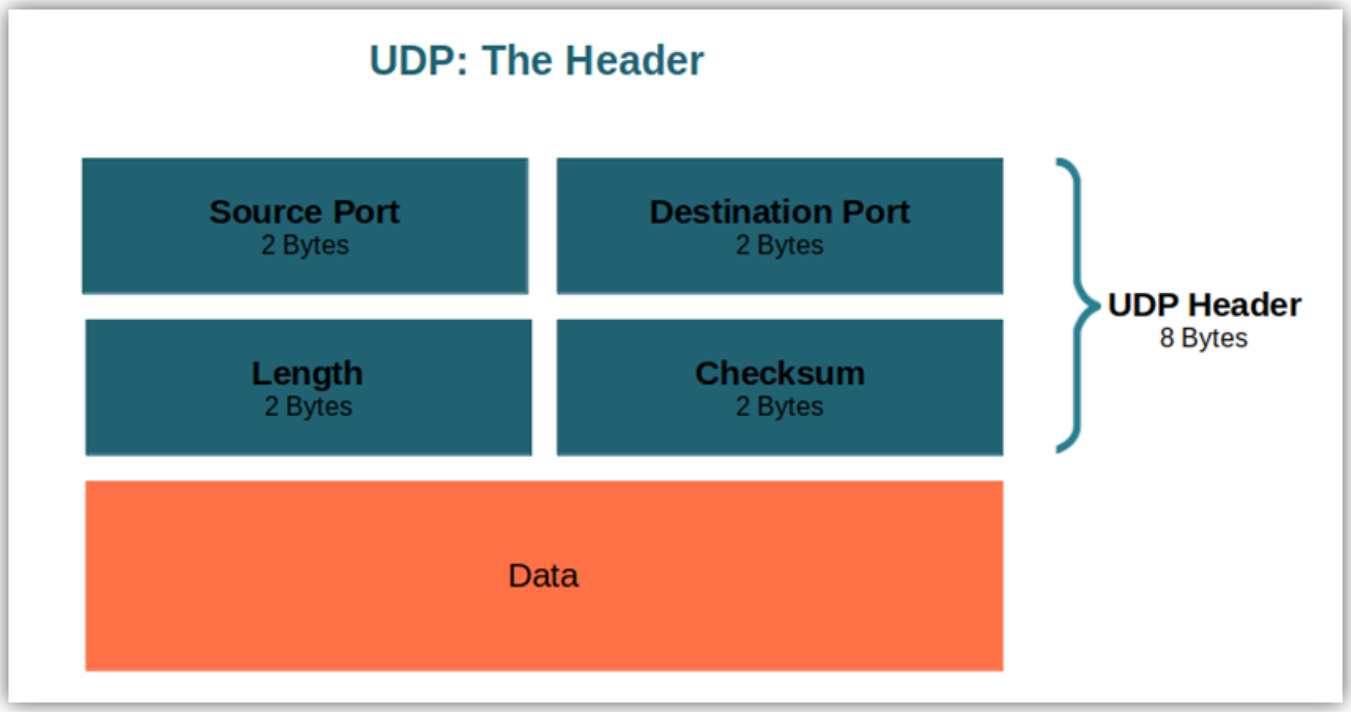


- بعد three way handshake يتم ارسال البينات فى segment
- Sequence number لايتم انشائه بشكل عشوائى وانما يتم من خلال algorithms ويمكن استخدامها كا ثغرة لتاكد من host's availability
- Flow control يستخدم لعمل تنسيق فى ارسال البينات مثل تحديد عدد وحجم segments ويتم من خلال عمليتان وهما windowing و acknowledgments
- Acknowledgment وهى رسالة destination يقوم بارسالها لاستقبال segment التاليه وتدل على وصول segments بشكل صحيح الى destination
- Windowing وهى العملية التى تحدد عدد segments التى يستطيع destination استقبالها او source ارسالها
- فى حالة استقبال destination ل segments اكثر مما يستطيع التعامل معها يقوم بوضعها فى buffer ولاكن فى حالة امتلاء buffer تبدا حدوث فقدان فى البينات
- فى حالة تحديد ان windowing سيكون بsegment 3 يتم ارسال ACK لستقبال segment الرابعة وترسال segment التالية لستقبال السابعة وهكذا
- فى حالة حدوث مشكلة فى segment ولتكن مثلا 5 فيقوم destination بارسال ACK 5 ليعاد ارسال segment مرة اخرى

UDP

- Stands for user datagram protocol
- لايقوم بعمل three way handshake او flow control اى انه يقوم بارسال البينات دون التحقق من وجود اتصال
- يستخدم فى الاحتياج الى السرعة عن صحة استلام البينات

- يطلق عليه بانه unreliable او انه connectionless protocol



- الفرق بين interface و port ان interface تاخذ IP و MAC ADRESS بينما لا يحدث هذا فى port
- ARP يستخدم فقط داخل الشبكة الواحدة لذالك عند الاتصال ب جهاز من خارج الشبكة المحلية يقوم ARP بالبحث عن MAC الdefault gateway
- Default gateway وهى interface الخاص ب الrouter المواجه لشبكة الlocal والمستخدم للاتصال بجهاز خارج الشبكة

Cables

Transmission basics

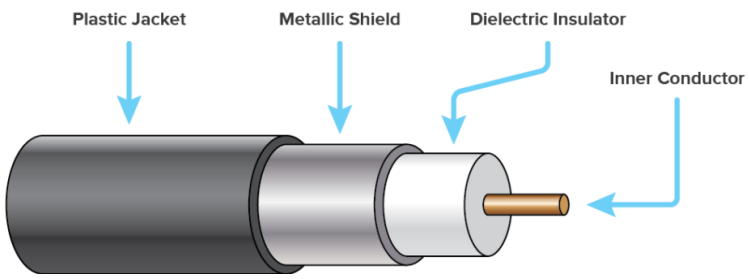
- Bandwidth : the amount of data that could theoretically be transmitted during a given period of time
- Throughput : the measure of how much data is actually transmitted during a given period of time
- Throughput are also called payload rate or effective data rate
- Bandwidth and throughput expressed by bit per second

Transmission flaws

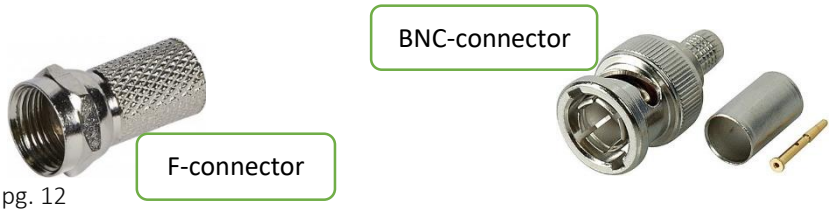
- Noise : noise can degrade or distort a signal and on a network is measured by dB (decibels)
  - يوجد مصدران اساسيان يسببان noise
    1. EMI(electromagnetic interference) ويوجد نوع من EMI يسمى RFI وهى موجات راديو broadcast
    2. Crosstalk وتحدث عندما تنتقل signal من سلك الى اخر ملامس له
- Attenuation : loss of signal's strength as it travels away from it source
  - لتغلب على هذه المشكلة يمكن استخدام اجهزة تقوم بتقوية الاشارة مثل repeater
  - Switch يعتبر repeater فى توصيلات Ethernet لذالك يطلق عليه multiport repeater
- Latency
  - يوجد عوامل مسببة ل latency مثل طول مسار اننتقال البينات و الاجهزة التى تمر عليها البينات مثل router و modem
- The most common way to measure latency on data networks is by calculating a packet's RTT(round trip time) or the length of time it takes for a packet to go from sender to receiver and back from receiver to sender
- RTT is usually measured in millisecond
  - Latency تسبب احينا بعض المشاكل اثناء الاتصال المباشر ومن هذه المشاكل Jitter وهى حدوث مشكلة ف تزامن وصول البينات
  - Full duplex(duplex) هى نوع من connection يعنى ان كلا طرفى الاتصال يمكنهم الارسال والاستلام فى نفس الوقت
  - Half duplex نوع من connection طرفى الاتصال يمكنهم الارسال او الاستلام ولاكن ليس فى نفس الوقت
  - Simplex ان طرفى الاتصال واحد منهم يقوم ب الارسال فقط والاخر يقوم بالاستلام فقط
  - Full duplex يمكن ان يتم بطريقتان :
    1. ان يكون cable مكون من اكثر من wire وكل wire يستخدم للارسال او الاستلام
    2. ان يكون cable عبارة عن single wire ولاكن مقسم الى logical channel وكل channel مخصصة الى عملية معينة

Copper cables

1. Coaxial cable

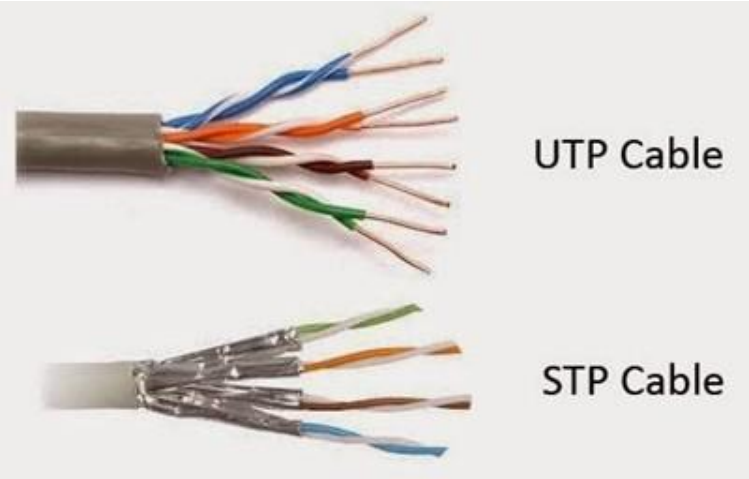


- لم يعد يستخد فى هذه الايام فى network
- conductor هو الذى يقوم بتوصيل البينات ويكون من النحاس
- Insulation (العازل) يكون من مادة Teflon او PVC
- Metallic shield يقوم بحماية cable من noise
- Sheath او jacket يحمى الcable من العوامل الخارجية ويمكن تصنيعه من PVC او من مواد مضادة للاشتعال
- RG هى وحدة لقياس جودة المواد المستخدمة فى shielding and conducting
- When discussing the size of the conducting core in coaxial cable we are refer to its AWG (American wire Gauga)size



- يوجد منه انواع من RG-59 و RG-6
- يلزم وضع connector فى نهاية الcable
- يوجد نوعان من connector فى coaxial وهما

2. Twisted pair cable



- هو النوع الاكثر استخدام
- كل زوجان من wires ملفوفان حول بعضهما لتقليل noise الناتج عن EMI المولد من سريان البينات داخل كل wire
- قطره يترواح من 0.4 الى 0.8 مليمتر
- Fast Ethernet networks تكون سرعتها القصوى 100mbps وفيها يتم استخدام زوج واحد لارسال البينات وزج اخر للاستلام والزوجان المتبقيان لا يقومو بعملية ارسال الدتا
- Gigabit Ethernet تبلغ سرعتها الى 1000mbps وفيها يتم استخدام جميع pairs لارسال واستلام البينات
- كلما ذات عدد twisted لنفس الطول كلما ذادت المقاومة الى noise و crosstalk وتسمى عدد twisted للمتر الواحد ب twisted ratio
- يؤدى ذيادة twisted الى ذيادة طول wire مما يؤدى الى حدوث مشكلة فقد البينات بسبب طول المسار
- فى سنة 1991 قامت منظمة تسمة TIA/EIA بوضع معايير تسمى TIA/EIA 568 standard والتى قسمت الtwisted pair الى اكثر من categories مثل cat 3 , cat 5, cat 5e, cat 6, cat 6e, cat 7

UTP Categories - Copper Cable

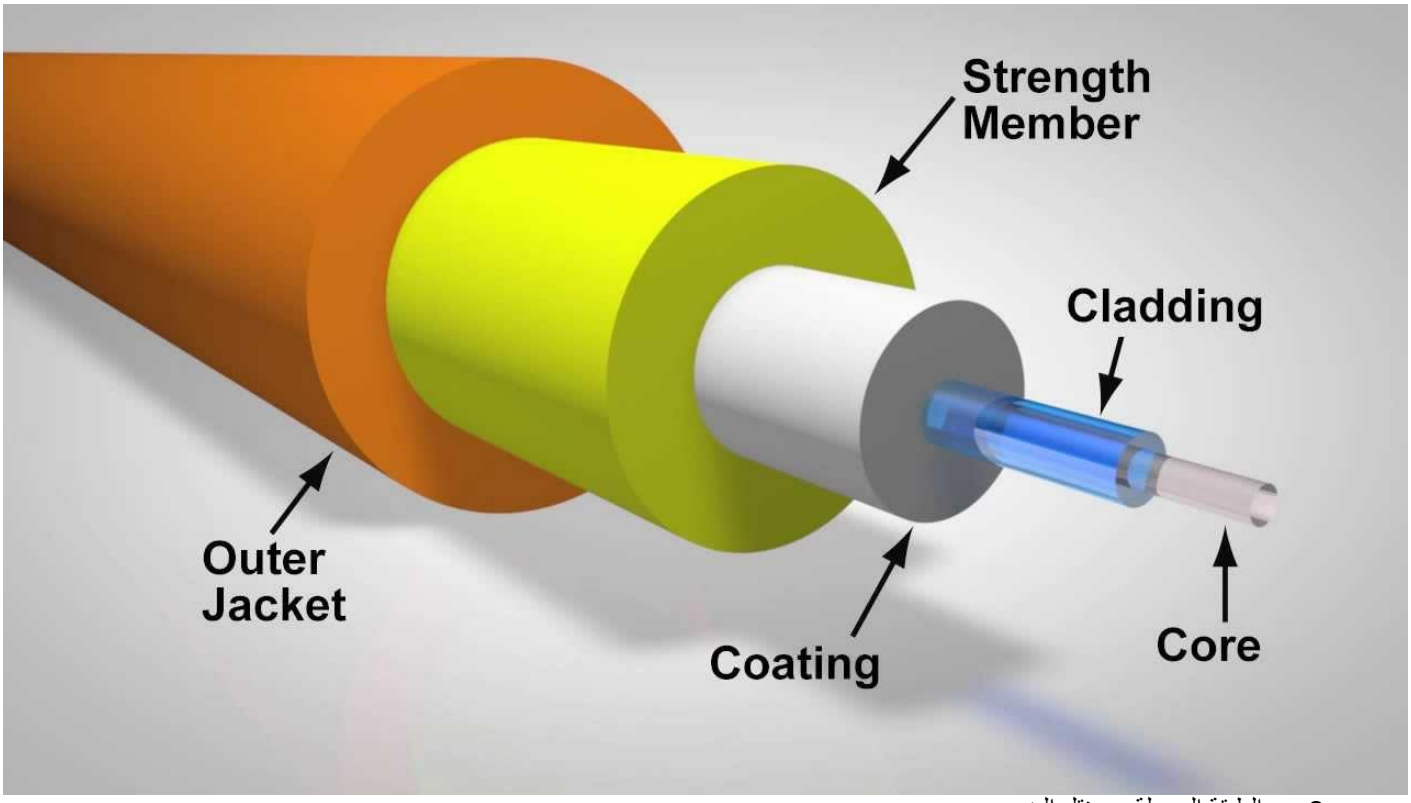
UPT CATEGORY	DATA RATE	MAX. LENGTH	CABLE TYPE	APPLICATION
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10 Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10 Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

- Token ring هو نظام كان منافس ل Ethernet ولاكن لم يعد موجود
- Cat1, cat2,cat3, cat4 لم تعد موجودة لليوم
- Cat5 قليلة الوجود ولاكنها مازالت موجودة مثل cat 5e وهو النوع المحسن من cat 5 والe اختصار ل enhanced
- Cat 6 يتميز بانه يحتوى على plastic core لمنع crosstalk ويجود به foil insulation يغطى wire بالاضافة الىfire resistant plastic sheath
- يوجد نوعان من twisted pair من حيث التصنيع وهما :
  1) Shielded twisted pair(STP) ويكون مغلف بطبقة من الالمونيوم او القصدير لمنع noise مثل EMI القادمة من خارج cable
     - STP يقلل noise ولاكن يذيد من التكلفة
  2) Unshielded twisted pair(UTP) لايحتوى على طبقة خارجية عازلة وهو النوع الاكثر شيوعا واستخداما بسبب تكلفته الاقل

- يوجد نوعان لconnector فى twisted pair وهما
- RJ11 يحتوى على 4 pins
- RJ45 يحتوى على 8 pins

3. Fiber-optic cable

- Fiber optic تنتقل فيه الداتا على هيئة اشارات ضوئية ويوجد مصدران لتوليد هذه الاشرات وهما
  1) Laser وينتج ضوء يتميز بانه مكثف وسريع وينتقل الى مسافات اكبر
  2) LED ولاكنه يختلف عن laser فى انه ينتج ضوء ينتقل الى مسفات اقل ويمكن استخدامه عند التوصيل فى نفس المبنى او بين switch و الrouter



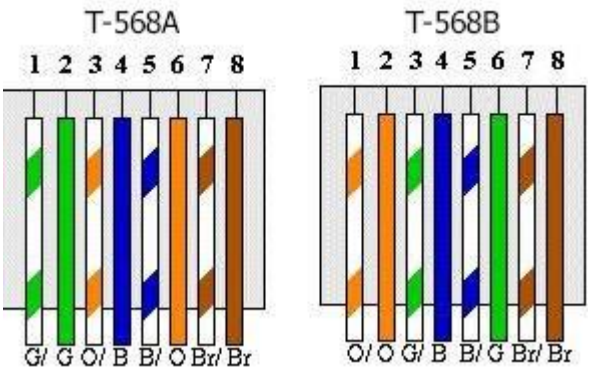
- Core هى الطبقة المسؤلة عن نقل الضوء
- Cladding هى الطبقة المسؤالة عن اعادة توجه الاشارة الضوئية فى حالة انحرافها
- مميزات fiber optic كتالى :
  1) Extremely high throughput
  2) Very high resistance to noise
  3) Excellent security
  4) Ability to carry signals for much longer distances before requiring repeaters
- يوجد انواع مختلفة من ال fiber optic منها :

1) SMF(single mode fiber)
   - وهو يقوم بارسال اشارة ضوئية واحد at a time لذالك يتميز بانه ينقل data بشكل سريع جدا والى مسفات كبيرة
   - يتميز بقطره الصغير جدا والذى يصل الى micro 8-10 وهو ما يسبب سرعة ومسافة نقل البينات كما ان مصدر الضوء الخاص به هو laser
   - يستخدم فى backbone internet cable لذالك يكون ذا سعر على جدا
2) MMF(multimode fiber)
   - قطره يكون اكبر micro 50-60
   - يقوم بنقل اكثر من اشارة ضوئية فى نفس الوقت مما يؤدى الى حيود احد الاشارات عن مسارها وهنا ياتى دور طبقة cladding
   - طبقة cladding لاتقوم بوظيفتها فى المسفات الكبيرة لزالك فا MMF يستخدم فى المسفات الصغيرة
   - مصدره يمكن ان يكون laser او LED

- من انواع الconnector فى fiber optic :

Cable pinouts

- TIA/EIA هى شركة قامت بتحديد طريقتان لترتيب الwire فى twist pair وانشاء RJ45 connector
- الطريقتان هما TIA/EIA 568 A(T568A) و TIA/EIA 568 B(T568B)
- T568B هو المستخدم بشكل اكبر
- فى fast Ethernet الorange و green يتم استخدمهم فى ارسال واستلام البينات حيث TX ترمز الى transmission و RX ترمز الى receive وباقة الwire لاتستخدم (unused)
- فى gigabit Ethernet جميع wire يتم استخدمها فى send و receive وهذا ما يجعل gigabit Ethernet افضل فى نقل الdata من fast Ethernet
- Type of network twist pair cable : (من ناحية ترتيب wire فى الطرفين)
  - Straight through
    - ✓ هو النوع الاكثر شيوعا
    - ✓ يعرف ايضا ب patch cable
    - ✓ يتكون من T568B فى كلا طرفيه
    - ✓ يسمى straight لان الdata تنتقل من طرف الى اخر بشكل مستقيم بسبب ان كلا الطرفين واحد
  - Crossover cable
    - ✓ يتكون من طرفان منهم T568B والاخر T568A
    - ✓ تسمى crossover لان المسار الخاص ب data يقوم بالانحراف بسبب ان كلا الطرفان مختلفان
    - ✓ يستخدم عن توصيل الاجهزة المتشبهة مثل computer to computer او switch to switch او router to router او **computer to switch** بينما فى توصيل الاجهزة المختلفة نستخدم straight through



- لم يعد يستخدم crossover بسبب ان معظم Ethernet اصبحت من النوع gigabit Ethernet وان الاجهزة الحالية اصبحت تمتلك خاصية لتحديد wire المسؤلة عن send و receive وتسمى هذه الخاصية auto sense function
- يوجد نوع ثالث وهو rollover cable وهو نوع يتم فيه تغيير جميع اماكن الwire فى الطرفان بشكل معكوس حيث ان رقم 1 فى طرف يكون رقم 8 فى الطرف الاخر وهكذا وكان يستخدم فى عمل configuration لrouter وكان يوضع فى port يسمى console ولاكن لم يعد يستخدم الان
- من انواع الport القديمة التى كانت تستخدم فى الnetwork هى serial port مثل DB-9 و DB-25
- POE (power over Ethernet) وهى خاصية فى الtwisted pair تسمح بنقل الكهرباء بجانب data
- من اوائل المنظمات التى وضعت معايير POE وهى منظمة IEEE حيث وضعت standard تسمى 802.3af standard وفيه يتم تحديد method المستخدمة لامداد twisted pair بالكهرباء
- كمية الكهرباء المستخدمة فى 802.3af standard هى 15.4 watts بينما فى الstandard الاحدث وهو 802.3at يتم الامداد بمقدار 25.5 watts ويسمى POE+
- يوجد نوعان من الdevices بنسبة لخاصية POE وهما :
  1. PSE(power sourcing equipment) وهى الاجهزة المسؤلة عن تزويد الكهرباء فى twisted pair مثل بعض من router وهى POE router وبعض من switch مثل POE switch
  2. PDs(powered devices) وهى الاجهزة التى تكتفى بالكهرباء القادمة من twisted pair مثل wireless access point و IP phones و IP camera
- فى حالة استخدام اجهزة PDs مع اجهزة ليست PSE نقوم باستخدام اداة تسمى injector او midspan وهو جهاز يحتوى فى طرف على مدخل لpower ومدخل للEthernet المتصل بالجهاز الذى لايدعم POE بينما الطرف الاخر يحتوى على مدخل واحد Ethernet وهو الذى يوفر data و power ل PDs
- فى حالة توصيل جهاز PSE باخر ليس PDs نستخدم splitter وه ادة تقوم بفصل data و power من Ethernet القادم من PSE

splitter

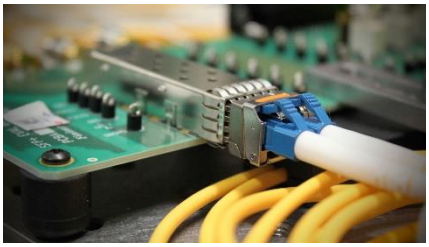
Injector

Network devices

Network adapters

Network interface card (NIC)

- الnetwork adapter هو وسيط يقوم بتحويل frames الى الشكل المناسب لانتقال الداتا عبر medium
- NIC هو واحد من network adapter ويمكن ان يكون build in (مبنى فى الdevice) او انه يتم تركيبه كقطعة منفصلة
- Transceiver وهى وحدة توجد فى اى network adapter وهى المسئولة عن اخذ الdata من device فى صورة binary وتحويلها الى الشكل المناسب لنتقلها فى الوسط مثل الكهرباء فى copper wire او موجات كهرومغناطيسية فى wireless او نبضات ضوئية فى fibber
- encoding scheme هى الطريقة المستخدمة لتمثيل ال binary بالشكل الذى يناسب الوسط وتختلف من architecture الى اخرى او حسب network media
- modem وهو network adapter وكان يستخدم فى حالة الاتصال بinternet عن طريق phone wire حيث انه يعمل ك وسيط يقوم بتحويل binary الى analog signal او العكس



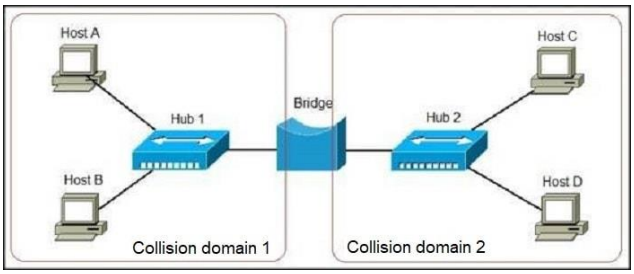
- SFP module هو converter يقوم بتحويل نوع port الى نوع اخر يناسب medium اخر مثل التحويل من fiber optic الى twisted pair كما فى الصورة
- يوجد version اخر من SFP مثل +SFP وهو يدعم نقل البينات الى 16Gbps على عكس SFP والتى لاتتجاوز سرعته 1Gbps ويوجد اصدار اخر وهو XFP والذى يتميز بانه يدعم لنقل البنات الى سرعة 10Gbps ويستهلك طاقة اقل من SFP
- يوجد نوع قديم كان يشبه الSFP ولاكن لم يعد يستخدم حاليا يسمى GBIC module وكان يقوم بنفس وظيفة SFP
- Media converter هى ايضا من اشباه SFP والاختلاف بينهم يكون فقط فى form factor

Network devices in LAN

1. Hub

- يمكن الاشارة الى hub ك repeater (مقوى لsignal)
- يقوم بربط مجموعة من الاجهزة معا وعند ارسال signal من جهاز الى اخر من خلال hub يقوم الhub باخذ الsignal وارسلها الى جميع الاجهزة (broadcast signal)
- الhub يقوم بتكوين physical topology من النوع star ولاكن logical topology من النوع bus
- يتعامل hub فقط مع الطبقة الاولى فى OSI model حيث انه لا يتعامل مع IP address او مع MAC address

2. bridge



- عند توصيل two hubs او اكثر معا يلزم استخدامه لتقليل كمية broadcast signals ويوضع فى وسط connection بين two hubs
- يمكنه التعامل مع الطبقة الاولى والثانية لذالك فانه يستطيع التعامل مع MAC address وهو ما يجعله يقرر مرور او عدم مرور الsignal من hub الى الاخر ويسمى هذا القرار بforwarding decision ويكون بالعتماد على forwarding database
- Forwarding database هى قاعدة بينات فى bridge توجد فيها mac address اخاص بالاجهزة المتصلة بكلا hubs واماكن تواجدهم فى اى من جانبى الاتصال

3. Switch

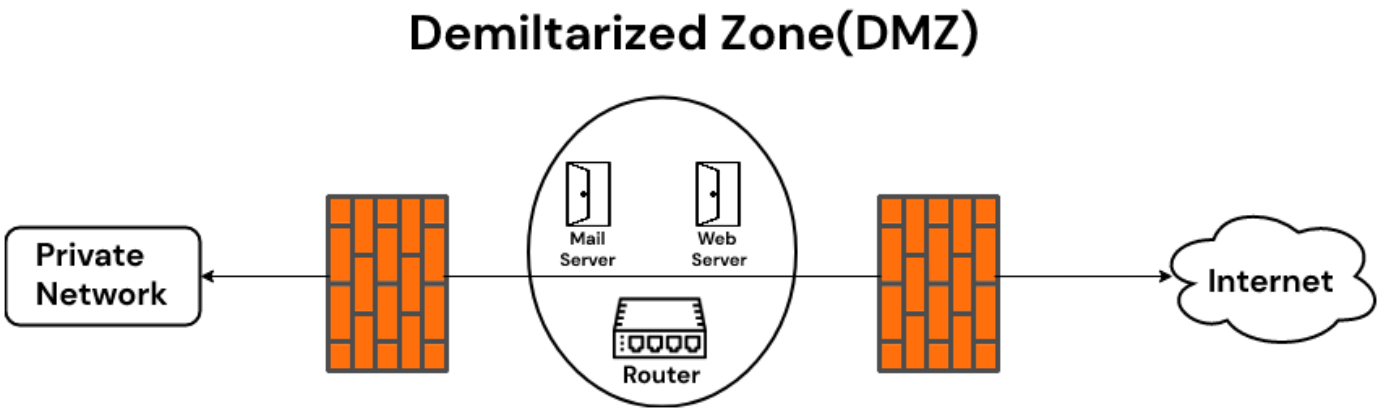
- يعتبر نسخة محسنة من الbridge لذالك يطلق عليه احيانا multi-port bridge
- يحتوى على MAC address table وهو مثل forwarding database فى bridge وفيه تحفظ MAC address الخاص بكل جهاز بجانب رقم الport المتصل به device

- فى البدايه قبل ملئ MAC address table يستخدم الswitch نوع broadcast connection بينما بعد ذالك يستخدم نوع unicast connection

4. Wireless access point
   - يستخدم لربط الdevices معا بشكل wireless عن طريق الelectromagnetic wave
   - احيانا يعمل مثل switch واحيانا يعمل مثل hub
   - Mac address filter هى خاصية فى wireless access point نستطيع من خلالها تحديد الاجهزة المسموح لها الاتصال من خلال MAC address

Internetwork devices

1. Router
   - يستخدم لربط بين اكثر من شبكة
   - يحتوى على اكثر من interface (وليس port) وكل interface متصل بشبكة وقد تكون كل شبكة بـarchitecture مختلفة
   - Layer three device اى انه يتعامل مع اول ثلاث طبقات لذالك فهو يستطيع التعامل مع IP address
   - يقوم بمهمة forwarding decision بناء على IP address وليس MAC address
   - Routing table هو جدول يشير الى كل شبكة والinterface المتصل بيها وهذا يشمل الشبكات الغير متصل بها بشكل مباشر
   - Interface الخاص بrouter بنسبة للاجهزة المتصلة على نفس الشبكة يسمى default gateway
   - عند ارسال signal من شبكة الى اخرى الrouter هو المسؤل عن توجيه الرسالة حيث ان اثناء توجيه الرسالة كل من source and destination IP يظل سابت بينما source and destination MAC يتغير من شبكة الى اخرى ويشار اليه ب next hop address
2. Firewall
   - هو المسؤل عن مرور او عدم مرور signals معينة من والى الشبكة لاغراض الحماية وهو شئ ضروري فى network لابد منه
   - يشبه router ولاكن الforward decision لا يعتمد فقط على network address بل على عوامل اخرى
   - يوجد منه نوعان :
     1) Hardware firewall ويعرف ايضا ب stand alone firewall وهو يكون موجود بشكل فزيائي فى network لذالك يكون غالى الثمن ولاكنه يحتوى على مميزات افضل
     2) Software based firewall ويكون موجود فى برمجة الcomputer او router كا software وهو المستخدم عادا من end user
   - يستخدم firewall فى انشاء منطقة فى الشبكة تسمى DMZ وهى منطقة توضع فيها انواع الserver المختلفة مثل database server و DNS server و web server وتوجد بين هذه المنطقة و internet الfirewall وايضا يوجد firewall بين DMZ و الinternal network



3. Multilayer switch
   - وهو يقوم بنفس وظيفة switch ولاكنه اصدار افضل حيث يستطيع ان يتعامل مع network layer اى انه يستطيع ان يتعامل مع IP ولاكن لايمكنه التعامل الى فى الشبكة ذات نفس network architecture وغالبا تكون Ethernet

Other specialized devices

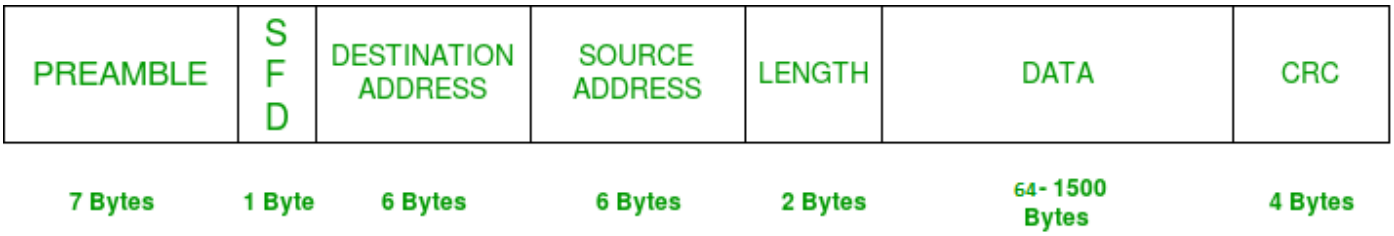
1. Load balancer وهو router ولاكن خاصية forwarding مضافة اليها بعض العوامل الاخرى التى تحقق performance افضل الى network
2. Proxy server وهو device يوضع بين end user و internet لجعل عملية التعامل مع internet تتم بشكل افضل او بتحكم افضل مثل انه يذيد من privacy عن طريق استخدم public IP مختلف عن الموجود فى الشبكة الداخلية او انه يذيد من control على الusers الموجودين فى الشبكة مثل تحديد مواقع معين للاستخدام
3. Encryption devices ويمكن لكل من الrouter او server القيام بencryption ولاكن لا يفضل ذالك لانه يؤدى الى ذيادة load على هذه الdevices لذالك يفضل فى حالة اهمية التشفير استخدام اجهزة مخصصة لذالك
4. Packet shaper ويستخدم عند الحاجة الى توزيع اولوية الtraffic مثل استخدام خاصية تسمى QOS

Ethernet

- هو عبارة عن communication standard اى انها مجموعة من المعايير والتى تحدد كيفية الاتصال بين الاجهزة فى wired LAN
- Token ring وهى standard اخرى تم انشائها من خلال شركة IBM و كانت تنافس Ethernet ولاكن لم تعد موجودة
- تم انشاء Ethernet ووضع معيرها من خلال منظمة IEEE وتم الاشارة الى هذا standard بIEEE 802.3
- Ethernet يقوم بتعامل مع physical and data link layer

Ethernet architecture

1. topology
   - Ethernet يدعم topologies مثل bus topology و star topology
   - Star topology باستخدام hub يكون logical topology من النوع bus
2. Network media
   - الnetwork media التى يستخدم فيها Ethernet هى twisted pair و fiber optic وكان يستخدم ايضا مع coaxial ولاكن لم يعد يستخدم
3. Network access media
   - Network media access هى مجموعة من القواعد التى تحدد متى وكيف سيتم استخدام network media وتسمى فى حالة Ethernet ب carrier sense multiple access /collision detection (CSMA/CD)
   - من القواعد الموجودة فى CMSA هو انه لكى يبدا device فى network بارسال signals يقوم اولا بعمل carrier sense اى انه يقوم بتاكد من انnetwork متاحة وفى حالة انها ليست متاحة سيقوم بالانتظار ثم سيقوم بعملcarrier sense مرة اخرى وهكذا الى ان تصبح network متاحة
   - فى حالة ارسال لdata من اجهزة مختلفة فى wire واحد(مثل bus topology) فى اتجهات مختلفة يحدث ما يسمى collision او التصادم
   - بعد عملية collision تقوم الdevices المسبب له بارسل jam signal وهى مجموعة من bits لتنبيه باقى devices بحدوث collision وجعلهم يتوقفو عن ارسال اى بينات وهو ما يسمى بback off وهذا الانتظار يختلف فى كل device
   - فى حالة bus topology او star topology with hub(logical bus topology) عمليات حدوث collision تكون عالية جدا وهذا من مساوئ استخدام نظام bus topology لذالك يفضل استخدام star topology باستخدام switch
   - Switch من ميزاته التى تجعله جيد فى حل مشكلة collision هو انه يقوم بانشاء مسار افتراضى بين كل جهزين مخصص فقط فى تبادل data بينهم مما يلغى مبدا carrier sense
   - من المميزات الاخرى التى سمح بها switch انه يمكن زيادة سرعة انتقال البينات داخل الشبكة بالاضافة الى استخدام اتصال full duplex
4. Frame type
   - يتكون frame فى data link layer وهو الوحيد الذى يضاف اليه tail بالاضافة الى header
   - اول جزء فى frame (header)يتكون من preamble وهى مجموعة من bits وتبدا ب010101 وتنتهى ب11 ويكون حجمها 8bit وتدل على بدا frame ثم destination MAC ثم source MAC
   - منتصف frame يوجد فيه الdata وتتروح حجمها من 64 byte الى 1500 byte وفى حالة ان data تم استلامها وهى اقل من 64 byte يقوم destination باكمالها بداتا لسيت لها قيمة الى ان تصل الى 64 byte وتسمى هذه الdata المضافة ب padding
   - نقص الdata عن 64 byte هو ما يعلم destination device عن حدوث collision وبتالى يقوم بارسال jam signal
   - Tail يكون فى نهاية الframe ويحتوى على CRC وهى اختصار cyclic redundancy check وهى مجموعة من العمليات الحسابية والتى تتاكد من سلامة frame اثناء ارساله



IEEE 802.3 ETHERNET Frame Format

Ethernet specifications

1. Speed
   - تكتيب السرعة بشكل معين حيث تبدا ب رقم وهو المعبر عن السرعة ثم -base– ثم حرف وهو يعبر عن نوع network media
   - الحرف المعبر عن twisted pair media هو T واحيانا يكون TX او TC
   - in twisted pair
     - رقم السرعة يكون بMbps ومن امثلة السرعات ال10 و100 و1000 و10G وهناك standards اخرى قد وصلت سرعتها الى 100G وكل سرعة تستخدم فى cat معين حيث 10 تستخدم فى cat3 و100 فى cat5 و 1000 فى cat5e
     - اقصى مسافة تستخدم فى twisted pair هى 100 meter
   - In fiber optic
     - رقم السرعات ايضا تكون 10 و 100 و1000 و10G
     - الحروف المعبرة عن network media تختلف من سرعة الى اخرى حيث :
       - 10-base-FL فى multi-mode fiber
       - 100-base-FX فى multi-mode fiber
       - 1000-base-SX فى MMF و 1000-base-LX فى SMF
       - 10G-base-SR/LR/ER و 10G-base-SW/LW/EW
     - الحروف لها دلالات حيث ان S اختصار الى short و L اختصار لlong و E اختصار لextreme long
- Ethernet standard تفضل ان يكون اقصى عدد لhost داخل الشبكة الواحدة هو 1024

IP addressing

IPv4

- هو اختصار ل internet protocol
- هو logical address يستخدم لعنونة الاجهزة مما يسهل التعامل بينهم حتى لو كانو فى شبكات مختلفة
- عبارة عن اربع خنات تسمى octet يفصل بينهم علامة .
- يكتب من decimal numbers
- تتراوح قيمة octet من 0 الى 255
- يتم وصف IPv4 بانه doted decimal اى انه يتكون من ارقام decimal و يفصل بين كل octet ب .
- عند قرائة IPv4 من قبل computer يتم تحويله الى binary وكل octet يتكون من 8-bit و علامة . ليست موجودة وانما توضع لتسهيل قرائة user
- يلزم لكى يحصل اتصال بين جهزان على الاقل يجب توفر IP و subnet mask
- يمكن كتابة subnet mask بطريقة اخرى وهى ان يكون هناك / ثم رقم بجانب IP والرقم يدل على عدد 1 فى subnet mask عند تحويله الى binary وتسمى هذه الطريقة فى كتابة subnet mask ب slash notation
- Subnet mask فى حالة binary يكون عبارة عن مجموعة من 1 ثم مجموعة من 0 كتالى **11111111.11111111.11110000.00000000**
- Anding هى عملية جمع 0 مع ال1 مثل and logical gate
- تستطيع devices معرفة network ID/address من خلال عملية anding بين IP و subnet mask

- فى بداية ارسال البينات يلزم على الاقل ان يتواجد IP و subnet mask فى كلا طرفى الاتصال ومن خلال ذالك يستطيع source معرفة ان destination معه على نفس الشبكة او لا فاذا كان معه فسيقرر التعامل مع destination من خلال MAC address وذا كان لا فسيقرر التعامل مع default gateway لارسلها الى الشبكة الاخرى التى تحتوى على destination
- يلزم ان تكون defaulted gateway(interface) تحمل نفس network address المتصلة بها
- IP يوصف بانه Hierarchical address اى انه هيكلى بمعنى اننا يمكن ان نقسمه الى جزاءان وهما network address و host address او يمكننا تقسيمه الى ثلاث اجزاء network address و subnet ID و host ID وكل هذا التقسيم يشارك فى تسهل عملية routing
- iana هى المنظمة المسؤلة عن IP وهى جزء من منظمة اكبر تسمى ICANN
- قامت منظمة iana بتقسم IP الى classes منها 3 اساسين و2 فرعيان

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			

- يختلف subnet mask من class الى اخر
- الفائدة من تقسم IPs الى classes هو انشاء شبكات تختلف فى استخدمها لعدد network و host لذلك فا class A يستطيع استيعاب عدد network قليل لاكنه يستطيع استيعاب عدد hosts اكثر ويمكننا معرفة ذالك من خلال subnet mask
- كل class يتم التحكم فى قيمته او الrang من خلال قيمته فى binary لذالك فى class A يكون اول رقم من اليسار دائما ب0 وبتالى يكون rang من 0 الى 127 وتختلف من class الى اخر كما موضح فى الجدول
- فى class A لايمكن استخدام network address هذا 00000000 (0)لانه محجوز ويتم استخدامه فى عملية routing ويسمى default route
- فى class A لايمكن استخدام network address هذا 01111111 (127) لانه محجوز ويستخدم فى عملية loop back address
- فى host address اول رقم (x.0.0.0) لايستخدم لhost وانما يكون محجوز لما يسمى network ID وهذا ينطيق على جميع classes
- فى host address اخر رقم (x.255.255.255) لايستخدم لhost لانه يكون محجوز لما يسمى broad cast ID (يستخدم لمخاطبة جميع الاجهزة)

IPv4 subnetting

- هى تقسيم ال networkالواحدة الى شبكات فرعية او مايسمى subnet
- يستخدم فى حالات مثل تقسم وتوزع public IP من خلال ISP
- تتم عملية subnetting من خلال subnet mask من خلال طريقتان

1) هى اخذ IP من class A,B وتغيير subnetmask ليتحول الى class C مثل : IP: 81.25.1.0
Subnetmask: 255.255.255.0
   - هذه الطريقة هى الاقل شيوعا او استخداما

2) VLSM (variable length subnet mask)
   - هذه الطريقة تستخدم فى حالة تقسم الشبكة الى اكثر من subnet وكل subnet يحتوى على عدد معين من hosts عكس الطريقة السابقة والتى فيها عدد host يتحدد بشكل تلقائي وغير متحكم فيه من خلال subnetmask
   - هى الطريقة الاكثر شيوعا واستخداما
   - Classeful IP المقصود به التعامل مع شبكة او IP من الشكل الdefault (default classes- default subnetmask- default number of host) وعند تغيير هذه القيم يتطلق عليه classless IP
   - فى هذه يتم التلاعب فى subnetmask بجزء من octet عكس الطريقة السابقة والتى تتلاعب بoctet كامل

- فى subnetmask (binary) يرمز 1 الى network ID بينما 0 الى host ID
- تتم هذه الطريقة كتالى :

(classeful IP) IP: 192.168.1.0/24

Binary Subnetmask: 11111111.11111111.11111111.00000000

Decimal subnetmask: 255.255.255.0

الى :

(classless IP) 192.168.1.0/26

Binary subnetmask: 11111111.11111111.11111111.11000000

Decimal subnetmask: 255.255.255.192

وهنا اصبحت الnetwork الواحدة تحتوى على four subnet كتالى :

من 192.168.1.0 الى 192.168.1.63

ومن 192.168.1.64 الى 192.168.1.127

ومن 192.168.1.128 الى 192.168.1.191

ومن 192.168.1.192 الى 192.168.1.255

- فى كلsubnet اولIP يستخدم لnetwork ID واخرIP يستخدم لbroadcast ID اى ان كلsubnet يستخدمhost 62
- الاجهزة ذات subnet المختلفة لاتستطيع التواصل بشكل مباشر حتى لو كانو متصلين بنفس physical network

- Supernetting وهى عملية عكس الsubnetting حيث انها تستخدم لدمج بين two networks لتحويلهم الى شبكة واحدة ووتتم ايضا من خلال التلاعب ب subnetmask

IP address assignment

- هى الطرق المختلفة لعمل configuration لhost فى network مثل تحديد IP address و تحديد subnetmask بالضافة الى default gatewayوغيرهم
- IP addressing method :

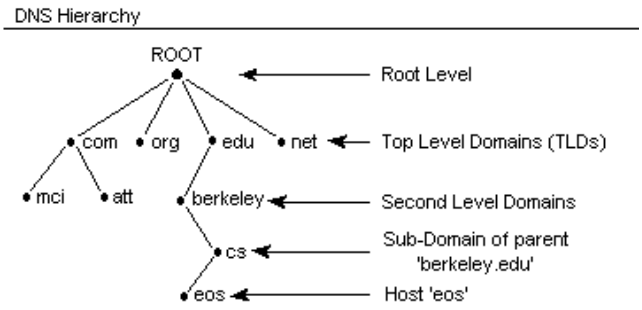
1) Static
   - وهى ان عملية configuration تتم بشكل يدوى
   - تصلح فقط فى حالة ان عدد الاجهزة قليل
   - يستخدم ايضا مع dynamic method لعمل configuration لاجهزة معينة مثل server و router و network printer والتى تستخدم static IP
2) Dynamic
   - وهى تعتمد فى عملية configuration على server مثبت عليه خدمة تسمى DHCP
   - فى حالة دخول اى host جديد الى الشبكة يقوم server الموجود عليه خدمة DHCP باعطائه IP و subnetmask و default gateway و DNS وغيرها من configuration
   - فى حالة ان host الجديد فى الشبكة لم يستطع الوصول الى DHCP وعمل configuration يلجئ الى APIPA
3) APIPA
   - اختصار ل automatic private IP addressing
   - وهى serves موجودة فى operating system تقوم بعمل configuration لhost فى حالة عدم اتصاله ب DHCP
   - IP المعطى من قبل APIPA يكون 169.254.X.Y (x و y يمثلو اى قيمة)
   - عيوب APIPA :
     i. IP الhost الخاص بAPIPA مختلف عن باقى الhosts الموجودة على نفس الشبكة مما يجعل عملية اتصاله معهم غير ممكنة
     ii. APIPA لا تقوم باضافة default gateway لذالك لن يستطيع host الوصول الى الrouter
   - ممزتها : انها تسمح لاكثر من host غير قادر على الوصول الى DHCP بالتواصل بينهم الى ان تحل المشكلة

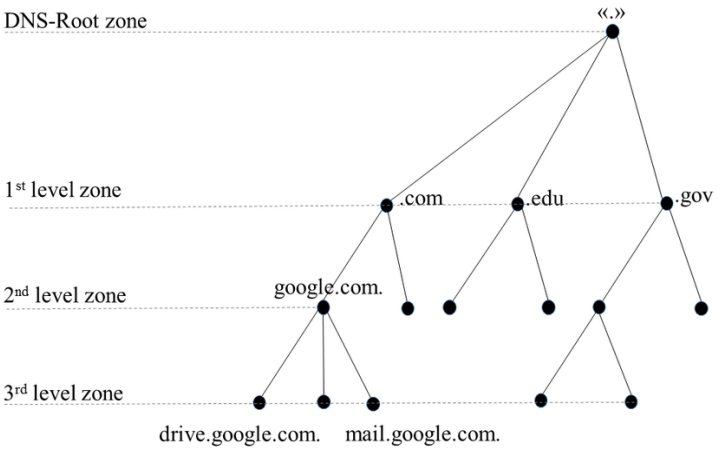
4) Alternate configuration
   - وهى طريقة بديلة لAPIPA تستخدم ايضا فى حالة عدم الوصول الى DHCP
   - تتم من قبل الuser حيث يتم اعطاء لhost كل من IP و subnetmask و default gateway و DNS ولاكن لايتم استخدامها الى فى حالة عدم الوصول الى DHCP server

- DHCP يتم تحديد فيه ما يسمى scope وهى range لIP التى سيعطيها DHCP الى host
- اثناء تحديد scope فى DHCP server يمكن وضع Exclusions وهى IPs استسنائية لايقوم DHCP باعطائها لاى host وغالبا ما تكون ل servers او printer او لاجهزة معينة اخرى
- APIPA هى واحدة من اسباب بعض المشاكل فى network لذالك يفضل فحص IP فى حالات troubleshooting لمعرفة امكانية وصول الhost الى DHCP
- APIPA لا تظل بشكل دائم وانما يقوم host من فترة الى اخرى بالبحث عن DHCP server
- العملية التى تتم بين الDHCP و host فى حالة الاحتياج الى configuration احيانا تطلق عليها DORA وتتم كنالى :
  1) يقوم host بارسال signal من النوع broadcast الى DHCP وتسمى DHCP Discover massage
  2) اى DHCP server فى network سيقوم بالرد على discover massage برسالة تسمى DHCP Offer massage وفيها يقوم DHCP بعرض IP على host وغالبا ما يتم قبول offer القادم من اول DHCP
  3) يقوم host برد برسالة تسمى DHCP Request massage وهى رسالة قبول لIP المعروض من DHCP وهذه الرسالة تكون ايضا من النوع broadcast لتنبه باقى DHCP بقبول عرض DHCP اخر
  4) يقوم DHCP بالرد على host برسالة تسمى DHCP ACK وهى رسالة تاكيد وتحتوى ايضا على مجموعة من المعلومات مثل IP release وهى فترة استخدام IP من قبل host
- Lease duration هى خاصية يتم تحديدها فى DHCP server لتحديد فترة استخدام IPs من قبل hosts وتعتمد على حالة وجود hosts فى الnetwork
- لتغيير IP من APIPA الى DHCP او لاخذ IP جديد من DHCP نستخدم امر ipconfig /renew فى CMD
- لعرض معلومات بشكل اكثر عن connection نستخدم امر ipconfig /all

DNS

- Stands for domain name system
- يقوم بتقديم خدمة تسمى name resolution system وهى خدمة تحويل host name الى IP
- طريقة عمل DNS تكون على شكل hierarchical (شجرى)





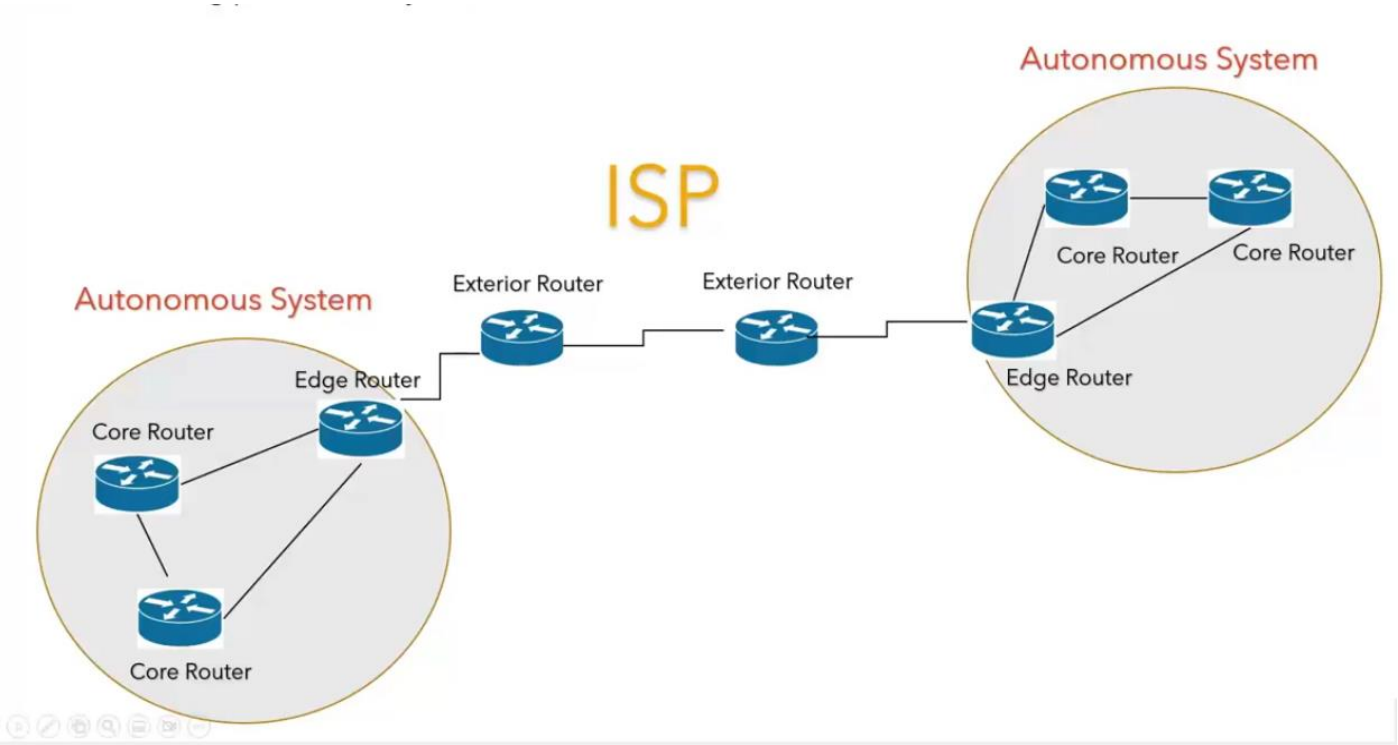
- نقطة بداية هذا النظام تسمى Root.
- اول مستوى يسمى top level domain او TLDs مثل (.com, .net, .cov)

- المنظمة الرئيسية المتحكمة فى first domain level و التى تحتوى على عنواين IP والdomain name و الذى تقوم بتوزيعها على شركات ISP هى منظمة ICANN
- الdomain second level يسمى ايضا sub domains ومن امثلة ذالك (Google, Microsoft)
- DNS server يقوم بقرائة domain name بسكل عكسى حيث انه فى www.google.com يقوم اولا بقرائة .com ثم يقرء google. ثم www
- يطلق على domain name الكامل مصطلح (FQDN) fully qualified domain name
- فى بداية الاتصال عن طريق domain name يتم اللجوء اولا الى ملف فى operating system يسمى hosts يكون بدون امتداد وكان يستخدم قديما ولاكن مع تطور شبكة الانترنت اصبح من الصعب استخدامه لان الdomain name اصبحت تتغير بسرعة كبيرة لذالك كان من الافضل استخدام DNS server
- عندما ياخذ DNS server الطلب من client يقوم بالبحث بداخله فى ملف host ثم يبحث فى zone وهو قاعدة البينات المخزنة فيها domain names وعادا ما تكون هى الاجهزة المدارة بواسطة المنظمة او الشركة التابع لها هذا DNS فاذا لم يجد IP الخاص بdomain يقوم بذهاب الى احد ال DNS server الاساسين (root.) وتسمى هذه العملية ب recursion
- بعد حصول client على domain name يقوم بتخزينه فى ما يسمى DNS cache
- مسار طلبIP من خلال host name تسمى forward lookup بينما عند الاستعلام عنhost name من خلالIP يسمى هذا المصارreverse lookup
- تسجل hosts الموجودة فى zone فى ما يسمى ب record و www هى واحدة من hosts
- ملاحظة alternate DNS هو DNS server بديل فى حالة عدم الوصول الى DNS الاساسي
- لستعراض DNS cache فى CMD نستخدم امر ipconfig /displaydns
- لازالة DNS Cashe نستخدم امر ipconfig /flushdns

Routing

- هى عملية توجيه packet من network الى اخرى
- الdevice المستخدم فى routing هو router
- الrouter الخاص بالمنزل يفضل اطلاق علية ADSL modem او ADSL router ولاكن عن ذكر مصطلح router يقصد به المستخدم فى الشركات
- الوظيفة الاساسية لrouter انه يقوم بربط شبكات معا حتى لو كانو مختلفين فى routing protocol مثل LAN و WAN وانه يقوم بتحديد افضل مسار لنتقال data من نقطة الى اخرى
- يستطيع router التعامل مع layer 3 (network layer) واحيانا يتعامل مع layer 4 (transport layer) فى خدمات مثل خدمة quality of serves

- فى حالة حدوث مشكلة فى مسار انتقال البينات يقوم router بايجاد مسار جديد لنتقال البينات
- بجانب الوظائف الاساسية لrouter فهو يستطيع القيام ببعض الاعمال الاخرى مثل :
  1) يقوم بعمل filter ل broadcast transmission
  2) بعض الوظائف البسيطة كا firewall (اتحكم فى مرور او عدم مرور packet من او الى network)
  3) يدعم حصول remote control من خارج LAN
  4) يوفر fault tolerance عالى
  5) يستطيع تعقب network traffic
  6) يستطيع التعامل مع بعض مشاكل الاتصال والتحزير بشئنها
- يمكن تقسيم router من حيث location او من حيث routing protocol المستخدم الى :
  1) Core router
     - هى الroutersالمستخدمة فى location يسمى ب autonomous system وهى مجموعة من LANs المتصلة معا تحت تحكم شركة او منظمة واحدة فتسمى الroutersالمستخدمة لربط بين LANs ب core router
  2) Edge router
     - هو router ينتمى ايضا الى autonomous system ولاكن الختلاف بينه وبين core router هو انه المسؤل عن ربط LANs الموجود فى autonomous system مع الinternet و يفضل ان يتحتوى الedge router على firewall عالى
  3) Exterior router
     - هو router الموجود فى الشبكة الخارجية (ISP , Internet)



- Autonomous system يتم تميزة برقم من خلال ISP
- Routing table : هى قاعدة بينات فى router يقوم باستخدامها فى توجه packet الى الشبكة الصحيحة
- Router يحتوى على الاقل على two interface
- Routing table يحتوى على مجموعة من المعلومات عن الشبكات الخارجية مثل network IP و subnetmask و interface وتتكون هذه المعلومات تلقائا عن توصيل router بشكل مباشر مع الشبكة
- لعرض routing table من خلال CMD نستخدم امر route print
- لمعرفة hop (routers) التى بيننا وبين destination IP نستخدم امر tracerRT ثم الIP او domain name

```
C:\Users\ahmed>tracert google.com

Tracing route to google.com [172.217.19.142]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    23 ms    23 ms    23 ms  host-156.210.1.192-static.tedata.net [156.210.192.1]
  3    24 ms    23 ms    24 ms  10.29.94.29
  4    25 ms    31 ms    24 ms  10.36.7.66
  5    65 ms    86 ms   219 ms  10.39.14.173
  6   488 ms   196 ms   163 ms  60-60-60-40.rev.home.ne.jp [60.60.60.40]
  7   567 ms   656 ms   231 ms  10.39.16.61
  8    64 ms    63 ms    63 ms  72.14.205.114
  9    62 ms    62 ms    62 ms  172.253.69.97
 10    67 ms    63 ms    64 ms  66.249.94.127
 11    64 ms    63 ms    63 ms  par03s12-in-f142.1e100.net [172.217.19.142]

Trace complete.
```

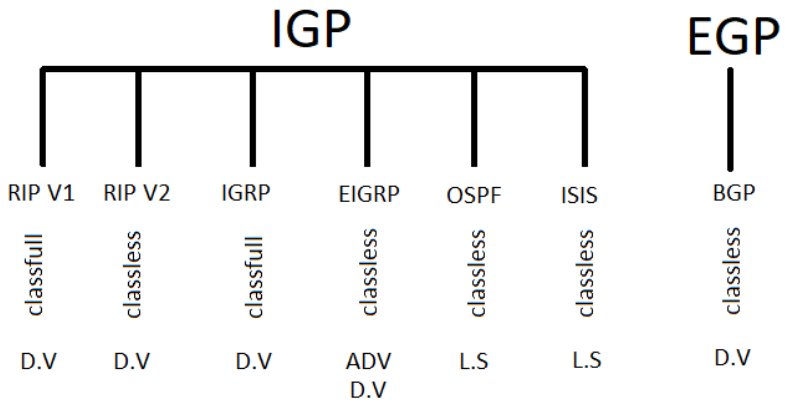
- يوجد امر اخر يؤدى عمل tracerrt ولاكن بتفاصيل اقل وهو pathping ثم IP او domain name

```
C:\Users\ahmed>pathping google.com

Tracing route to google.com [172.217.19.142]
over a maximum of 30 hops:
  0  DESKTOP-H2C5LH1.home [192.168.1.12]
  1  192.168.1.1
  2  host-156.210.1.192-static.tedata.net [156.210.192.1]
  3  10.29.94.29
  4  10.36.7.66
  5  10.39.14.173
  6  60-60-60-40.rev.home.ne.jp [60.60.60.40]
  7  10.39.16.61
  8  72.14.205.114
  9  172.253.69.97
 10  66.249.94.127
 11  par03s12-in-f142.1e100.net [172.217.19.142]

Computing statistics for 275 seconds...
```

Static routing VS dynamic routing

- الrouter يقوم باضافة الشبكات المتصل بها بشكل تلقائى فى routing table
- لاضافة الشبكات المتصلة مع router بشكل غير مباشر فى routing table يمكن عمل ذالك بشكل manual وهو مايسمى بstatic routing
- Static routing تصلح فقط فى الشبكات الصغيرة ولاكن فى حالة الشبكات الكبيرة و التى تحدث فيها تغيرات كثيرة لا يمكن استخدامها ابدا
- Dynamic routing وهى معرفة الrouter ب الشبكات المتصلة به بشكل غير مباشر بشكل تلقائى وتحدث باستخدام routing protocol
- Routing protocol هو طريقة يستخدمها الrouter لكى يعلم بشان الشبكات المتصلة به بشكل غير مباشر
- يوجد انواع مختلفة من routing protocol ويمكن التمييز بينهم بعدة عوامل منها :

1) Scope
   - وهو قصى مدى يمكن للprotocol مشاركة المعلومات مع routers اخرى
   - فى autonomous system يتم استخدام routing protocol وهو IGP و الScope الخاص به يكون فى حدود autonomous system
   - فى شبكة الانترنت يتم استخدام routing protocol اخر وهو EGP



2) Metric
   - هى قيمة تحدد المسافة او cost الازم ليصال massage ودائما ما تكون القيمة الاصغر هى الافضل
   - من العوامل التى يمكن ان يقاس بها metric وهى hop count
   - Hop هو router الذى سيوجه signals للوصول الى destination لذالك فا hop count هو عدد routers الذين سيوجهوا الsignal للوصول فى النهاية الى destination
   - لذالك كلما كان عدد الhops الازمة فى وصول signals اقل كلما كان افضل
   - Bandwith-delay وهى عوامل اخرى يمكن ان تقاس بها metric حيث ان كلما قلت delay كلما كان افضل
   - Relative وهى قيمة يتم تحديدها من قبل admin والتى تحدد مرور الsignal من مسار معين
   - Relative احيانا تسمى ب link cost

3) Sharing method
   - هو من احد اهم العوامل التى تفصل بين protocol عن الاخر
   - Sharing method المقصود بها هى طريقة مشركة المعلومات مع routers الاخرى

- Distance vector وهى method تجعل مشاركة المعلومات فقط مع routers المتصلة بها بشكل تلقائي
- عند مشاركة المعلومات من router الى اخر تتغير قيمة matric
- عملية تبادل المعلومات تسمى convergence او flooding
- Link state هى method اخرى لمشاركة البينات وتشبه distance vector ولاكن يوجد بينهم اختلاق مثل ان link state تقوم بمشاركة البيانت فى حالة حدوث تغيير فقط فى network بينما distance method تحدث بغض النظر عن وجود تغيير ام لا
- Hybrid وهى طريقة خليطة من الdistance و link state

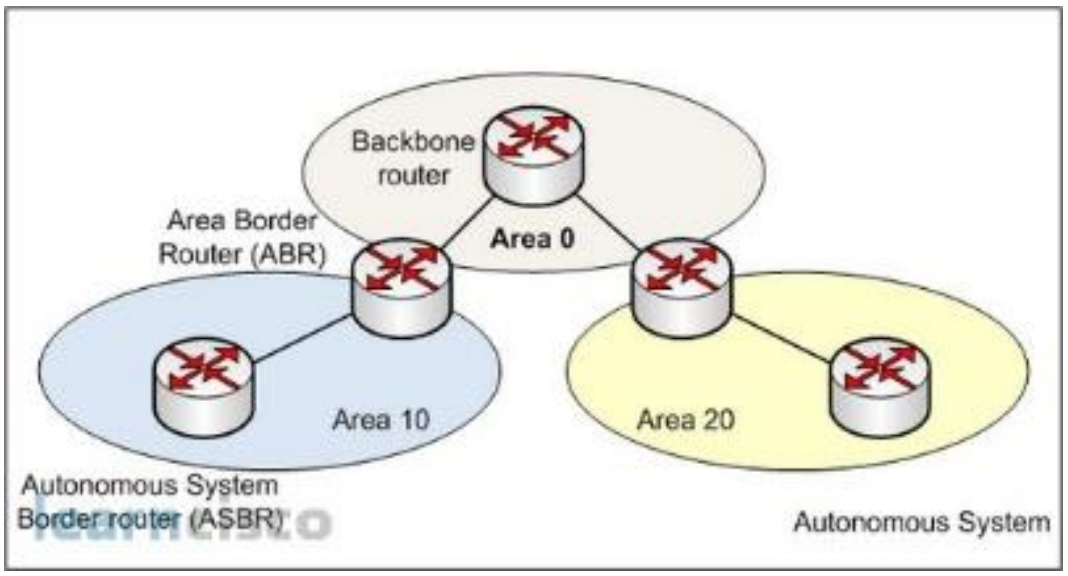
4) Support VLSM
- يتم تفضيل بعض routing protocol عن اخرى بسبب دعمها ل VLSM (subnetting)
- تسمى الprotocols التى تدعم subnetting ب classless routing protocol بينما تسمى protocols التى لاتدعم subnetting ب classeful protocol

5) Administrative distances
- هو العامل الاول التى يتم الاجوء اليه من router لتفضيل الارسال عبر router معين وهو مثل عامل metric ولاكن الrouter يلجئ اليه اولا
- قيمة AD تتروح بين 0 الى 255
- فى حالة تساوى قيمة الAD من two routers يتم الجوء الى metric
- فى حالة تساوى قيم AD و metric يقوم الrouter بعمل load balance وهى تنظيم ارسال signal بين two routers

Routing protocols

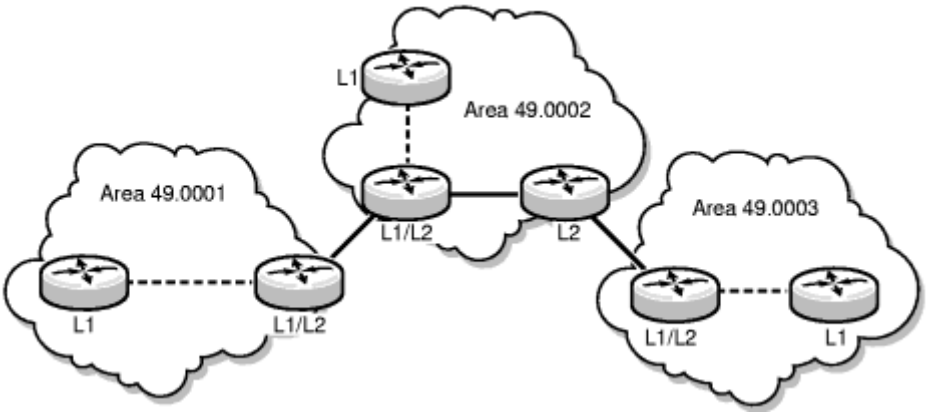
1. Routing information protocol(RIP)
   - يستخدم distance vector فى عملية مشاركة معلومات الشبكة ويقوم بها كل 30 ثانية
   - يستخدم hop count فى ايجاد افضل مسار لارسال البينات
   - اقصى عدد من hop هو 15 اى انه لا يستطيع ارسال البينات الى destination يبعد عنه ب15 router وهو ما جعله يصلح فقط للشبكات الصغيرة
   - RIP version 1 يستخدم classful routing بينما الاصدار الثاني يستخدم classless protocol
   - من مميزاته انه سهل فى التعامل وانه ثابت
   - ومن عيوبه
     1) لايمكن استخدامه فى الشبكات الكبيرة
     2) يشغل network بسبب انه يقوم بعمل sharing لمعلومات الشبكة كل 30 ثانية
     3) تاخر عملية convergence
     4) ابطئ واقل من ناحية secure
     5) غير مستخدم هذه الايام
2. (enhanced interior gateway routing protocol) EIGRP
   - يستخدم طريقة hybrid routing فى مشاركة المعلومات عن الشبكة
   - يصلح للشبكات الكبيرة
   - يستخدم طريقة bandwidth and delay فى ايجاد افضل مسار لنقل البينات (metric)
   - سريع جدا فى عملية converges لذالك يكون مفضل لكثير من network administrator
   - يمكن استخدامه مع IPv4 و IPv6
   - يدعم classless IP (VLSM)
   - يقوم بتحديد افضل مسار عن طريق algorithm يسمى diffusing Update
   - يتعامل مع مبدا autonomous system
3. Open shortest path first (OSPF)
   - يستخدم algorithm يسمى Dijkstra
   - يقوم بعملية converges بشكل سريع ولاكن اقل من EIGRP
   - يستخدم link state لكى يشارك معلومات الشبكة
   - يمكن استخدامه مع IPv4 و IPv6 ولاكنه يفصل بين database الخاصة بIPv4 و database الخاصة ب IPv6 مما يجعله يستطيع استخدام two type protocols فى نفس الوقت ومع ذيادة عدد routers يجعل network مزدحمة
   - يتعامل مع مبدا areas و autonomous systems مما يقلل routing update traffic

- يدعم VLSM
- يمكن استخدامه مع عدد لا محدود من hop (unlimited hop count)
- سريع فى عملية converges



- تقسيم ال networkالى areas يستخدم لتقليل overhead
- يلزم ان تكون هناك area 0 وتسمى ايضا ب backbone area و router الموجود بداخلها يسمى بbackbone router
- الrouter الذى يربط بين كل area والاخرى يسمى ب area border router (ABR)
- Autonomous system border router (ASBR) هو router الذى يمكن استخدامه فى الربط بين autonomous system والاخر
- هذا البرتكول هو المفضل فى مشركة المعلومات بين autonomous systems

4. IS-IS (intermediate system to intermediate system)
   - هو IGP protocol اى انه يستخدم داخل autonomous system
   - يستخدم link state فى sharing مثل OSPF
   - يستخدم ايضا dijkstra algorithm
   - OSPF يستخدم الIP فى التواصل بين routers بينما IS-IS يستخدم protocol يسمى connectionless network service (CLNS)
   - يتعامل IS-IS من areas ولاكن لايشطرت وجود area 0 عكس OSPF
   - يفضل استخدامه فى ISP لانه يتعامل مع IPv4 و IPv6 معا فى database واحدة عكس OSPF



- Level 1 router هم router الموجدين داخل area ولا يتصلون بrouter خارج area
- Level 2 router هم routers المتصلين ب routers خارج الشبكة فقط
- Level 1/ 2 هو router المتصلين بlevel 1 و level 2 معا

5. BGP (Border gateway protocol)
   - من النوع EGP
   - هو المتسخدم فى شبكة internet
   - يتم استخدامه بواسطة edge router
   - يستخدم distance vector ولا نسخة محسنة منها
   - تستخدم ايضا فى ISP

	Scope	Metric	Type	VLSM
RIP	IGP	Hop-count	Distance Vector	✗
RIPv2	IGP	Hop-count	Distance Vector	✓
EIGRP	IGP	Bandwidth-delay	Hybrid	✓
OSPF	IGP	Link Cost	Link State	✓
IS-IS	IGP	Link Cost	Link State	✓
BGP	EGP	Policies	Distance Vector	✓

- عند وجود device فى نظام autonomous system يريد الاتصال مع network فى internet يتم تعيين يدويا ما يسمى ب default route فى edge router ويكون IP الخاص به هو 0.0.0.0 و subnetmask هو 0.0.0.0

NAT

- Stands for network address translation
- هى طريقة مثل subnetting فى غرضها حيث ان NAT و subnetting كلاهما يستخدمان لتقليل استهلاك IP address
- تعتمد NAT فى تقليل استهلاك IP addresses على تحويل public IP الى private IP
- Public IP هو IP الذى سيستخدم فى internet بينما private IP يستخدم فى local network
- يوجد private IP فى كل class كتالى :

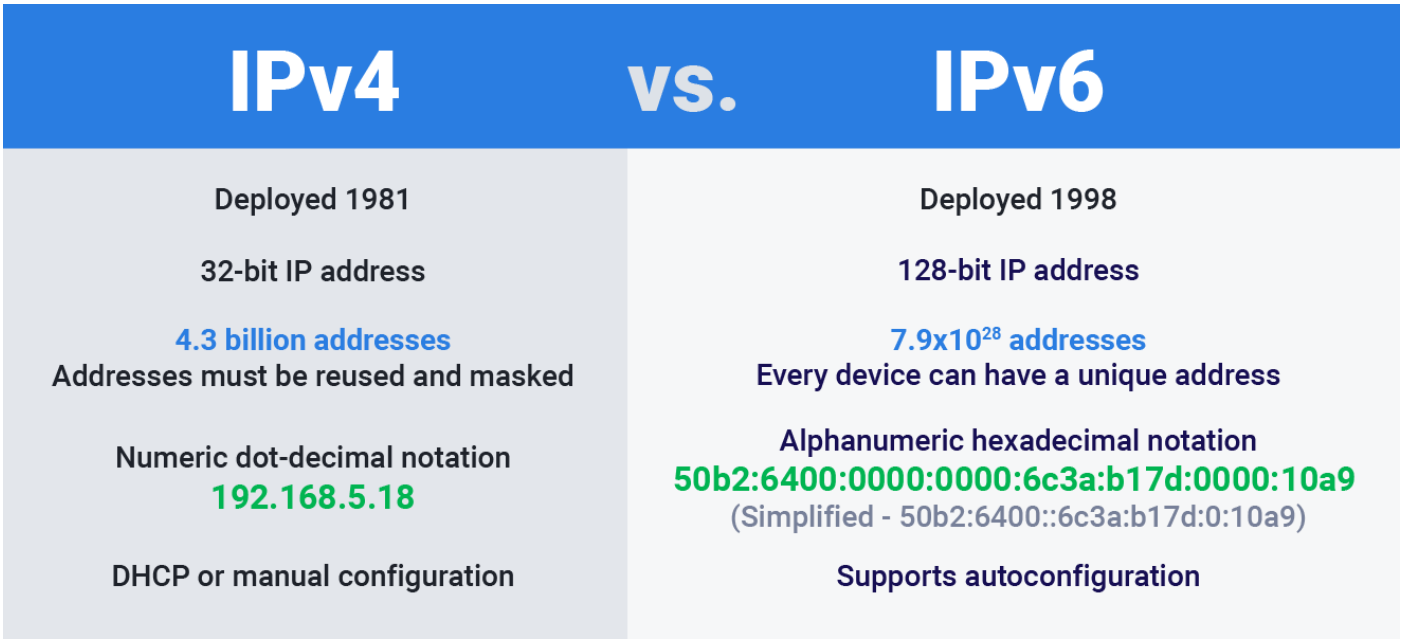
Class	Private IP address range	Subnet mask
A	10.0.0.0 – 10.255.255.255	255.0.0.0
B	172.16.0.0 – 172.16.31.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

- عند اتصال device من داخل local network الى internet يتم تحويل private IP الى public IP
- كل جهاز فى private network يحتوى على private IP مختلف ولاكن جميعهم يستخدموا نفس public IP
- يمكن اطلاق على private IP مصطلح local address و public IP مصطلح Global address
- Static NAT (SNAT) هو ان لكل private IP يكون له Public IP خاص به
- Dynamic NAT هو ان اى جهاز يحمل private IP عند اتصاله ب internet ياخذ public IP المتاح اى انه يوجد اكثر من public IP وعملية التحويل من private الى public تتم على حسب الpublic IP المتاح وليس ان كل private له public محدد مثل static NAT
- Overloading ويسمى ايضا ب PAT وهو الذى يمثل الفكرة الاساسية لNAT اى ان كل جهاز private يستخدم نفس public IP
- فى حالة static NAT يحتوى router على NAT table وفيه يشير كل private IP الى public IP الخاص به

- يقوم NAT بتعديل packet القادمة من local device لتغيير source IP من private الى public
- Port address هو ما يستخدمه router لتحديد packet الخاصة بكل local device لذالك فا PAT اختصار لى port address translation

IPv6

- تم انشائه كبديل لIPv4 بسبب كثرة الdevices الموجودة على internet



- IPv6 يتكون من 8 خانات كل خانة تسمى Quartet تكون حجمها 16 bit لذالك فحجم address كامل يكون 128 bit
- قيم quartet تكون من hexa-decimal وتتراوح من 0000 الى ffff ويفصل بين كل quartet والاخرى ب :
- من طرق تسهيل قراءة وكتابة IPv6 ان نزيل الاصفار الموجودة فى شمال quartet كتالى 00CD <------ CD او 09DA <----- 9DA
- من طرق التسهيل ايضا اختصار الquartet المتتالية التى تحتوى جميع قيمها على صفر الى :: كتالى

  ABCD:0000:0000:0000 <---------- ABCD::
- الطريقة الثانية فى الاختصار تحدث مرة واحدة فقط
- IPv6 فيه اول 4 quartet مخصصة لnetwork ID وتسمى prefix بينما اخر 4 quartet لhost ID وتسمى interface ID
- مصطلح link او local link يقصد به LAN عند التعامل مع IPv6
- يوجد اشكال مختلفة من IPv6 وكل شكل له استخدام كتالى

IP address type	Address prefix	Notes
Global unicast	2000::/3	First 3 bits are always 001
Link local unicast	FE80::/64	First 64 bits are always 1111 1110 1000 0000 0000 0000 0000
Unique local unicast	FC00::/7	First 7 bits are always 1111 110
	FD00::/8	First 8 bits are always 1111 1101
Multicast	FF00::/8	First 8 bits are always 1111 1111

- Unicast address هو address مخصص لhost واحد فقط ويوجد من نوعان
  1) Global address وهو المستخدم فى شبكة الانتر نت مثل public address فى IPv4
  2) Link local address وهو يستخدم للاتصال بhosts فى نفس link (LAN) وهو يشبة APIPA
- Multicast address وهو ارسال packet الى كل الاجهزة المحددة وهو مثل multicast الموجود فى IPv4
- Anycast address هو ارسال packet الى اقرب destination

- يتم توليد IPv6 من جزء interface ID بطريقتان
  1) يتم توليد interface ID بشكل عشوائي من خلال operating system
  2) يتم توليده من خلال MAC address
- فى حالة اتصال host باخر وكان احدهم يستعمل IPv4 والاخر IPv6 يلزم وجود router فى المنتصف لتعديل الIP

Wireless Networks

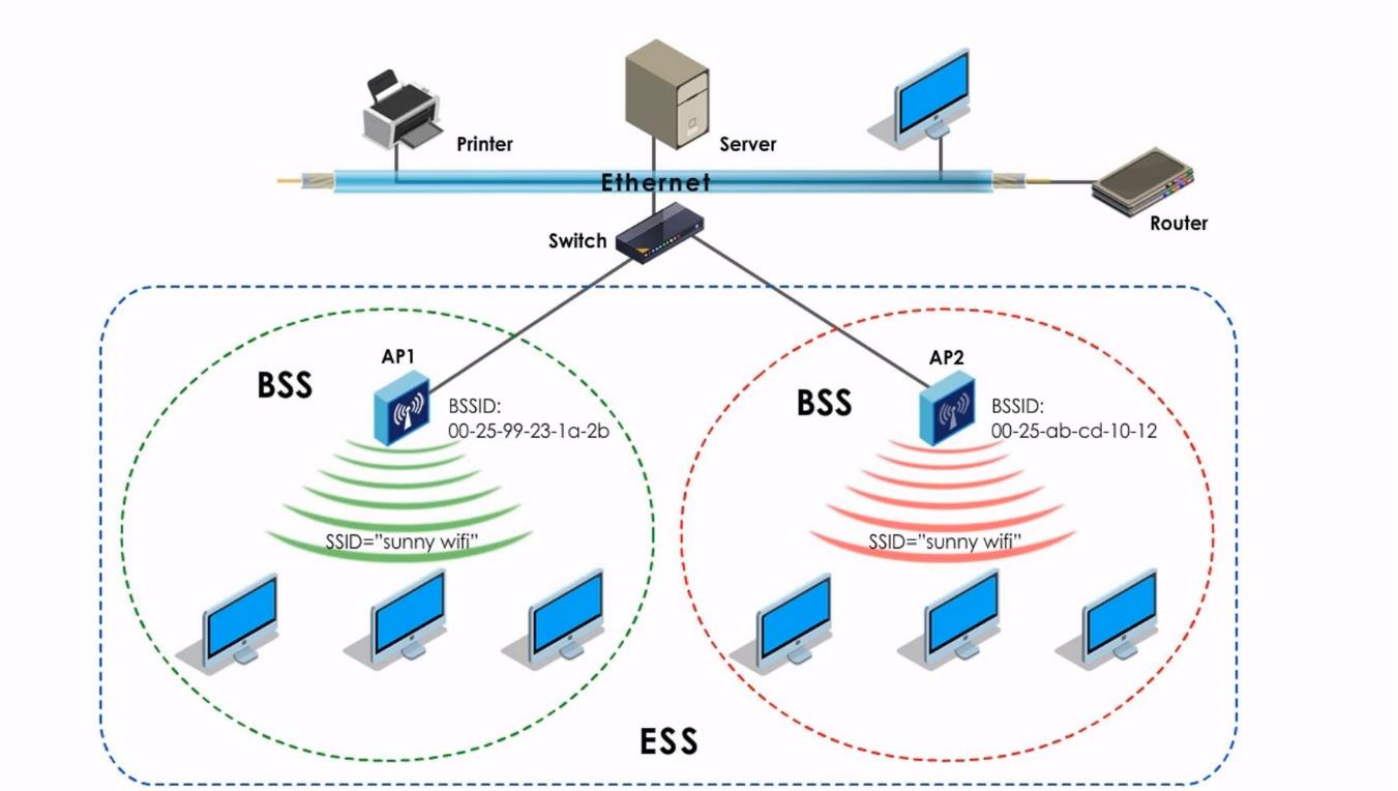
- هى من اهم الnetworks الموجودة حاليا بسبب انها تقوم بربط الاجهزة معا من خلال الموجات الكهرومغناطيسية دون الحاجة الى cables وتسمى WLAN
- يشترك كل من LAN و WLAN فى الlayers من network الى الapplication بينما يختلفوا فى physical و الdata link
- Wireless spectrum هو مدى الfrequices الخاصة بالموجات الهرومغناطيسية
- FCC (Federal communication commission) هى الشركة المنظمة لعملية توزيع الRanges وقد سمحت باستخدام الترددات من 9 KHz الى 300 GHz
- فى حالة اعتماد اكثر من مصدر على نفس الترددات فان ذالك يؤدى الى حدوث interference ومن اشهر الترددات هو 2.4 GHz
- لسماح باكثر من مصدر فى استخدام نفس التردد تم انشاء ترددات فرعية وهى الchannels
- 2.4 GHz الخاصة بالWIFI يتم تقسيمه الى 11 channel وفى بعض الاماكن تم تقسيمه الى 13 كل channel تكون 20MHz wide
- Bluetooth يتم تقسيم ترددها الى 79 channel
- يوجد technology تسمى zigBee وهى تستخدم فى الmedical devices وفى scientific devices وتستخدم 16 channel
- ANT1 هى technology تستخدم فى activity monitoring devices ولاتستخدم channels بل تكون fixed frequency

Wireless Topologies

1. Ad-hoc
   - هى technology تقوم على وجود اتصال بشكل wireless بين الجهزة بشكل point to point بدون جهاز وسيط
   - من عيوبه انه ليس جيدا فى حالة انه يوجد اكثر من جهازان ويريدون الاتصال معا
2. Infrastructure
   - وهى تقوم على ان الاجهزة تتصل معا من خلال جهاز وسيط يسمى access point
   - يصبح عند وجود عدد كثير من الاجهزة عكس الad-hoc

- يتم التحكم فى الchannel من خلال الaccess point ويسمى المدى الخاص بnetwork ب BSS (basic service set)
- فى حالة كان هناك اكثر من access point بينهم مسافة قليلة فاننا نستخدم channel مختلفة
- فى حالة وجود اكثر من BSS لنفس الشركة او المؤسسة فانهم جميعا يسمو ESS (extended service set)
- يتم تمييز ESS من خلال ما يسمى بال SSID (service set identifier) وهو يكون اسم الشبكة الwireless
- عند اتصال الجهاز بaccess point فانه يستطيع ان يميز انه ضمن شبكة وانه متصلة بaccess point معينة من خلال BSSID وهو الMAC الخاص بالaccess point
- Rooming هى طريقة التنقل من BSS الى اخرى والتبديل بين الAccess point بشكل تلقائى ولاكن يجب ان يكون كلا الBSS لديهم نفس الname والpassword

- عند الجمع بين النظام الwireless مع النظام الwire فان هذا النظام يسمى distribution system وهنا يعمل الaccess point على انه bridge



- شبكات الwireless غير قابلة للاستقبال و الارسال فى نفس الوقت بجانب انها غير قادرة على منع عملية الcollision ولذالك فان الstand 802.11 يعمل على اسلوب يسمى CSMA/CA (carrier sense multiple access/collision avoidance)
- CSMA يقوم بتقليل حدوث الcollision ولاكنه لايستطيع اكتشافه
- فى الCSMA عندما يريد الnode ارسال data فانه يقوم بعمل check for transmission ويرى هل هناك activity ام لا واذا لم يجد سيقوم بانتظار وقت قليل ثم سيقوم بارسال الdata واذا وجد ان هناك activity فانه سيقوم بالانتظار ثم سيقوم بعمل check مرة اخرى
- لكى يتمكن الnode من معرفة ان الdata تم ايصالها ولم يحصل لها collision فانه سيقوم بانظار رسالة الACK من الreceiver
- نظرا لصعوبة ارسال رسالة الى nods خارج نطاق الشبكة تم استخدام protocol مع CSMA وهو RTS/CTS
- فى الRTS/CTS عندما يريد node ارسال الdata فانه يقوم بتحقق من الtransmission واذا لم توجد فانه يقوم بارسال رسالة الى الaccess point تسمى RTS وهذه تجعل الaccess point يقوم بعمل CTS وهى ان يقوم بايقاف جميع الtransmission ويجعل الوسط فقط لهذا الnode وفى حالة ان الnode وجدت ان هناك activity فى الشبكة ستقوم بالانتظار ثم ستقوم بعمل check for transmission مرة اخرى
- RTC يقوم بعمل delay اكثر فى الشبكة بسبب انه يقوم بجعل الوسط متاح لtransmission واحد فقط

Wireless standard

- Wi-Fi هو اختصار ل wireless fidelity وهو عبارة عن collection من الstandards التى تمت تطويرها بواسطة شركة IEEE
- من اهم الstandards التى تم تطويرها من IEEE 802.11 هم :
  1. 802.11 a
     - كان يعمل على تردد 5GHz وممن مميزاته انه تردد غير مستخدم بكثرة اى لن يحدث Interference بكثرة
     - يتميز بانه high throughput
     - من عيوبه انه يحتاج طاقة اعلى للارسال وانه يصل الى مسفات قليلة ولذالك فسيتم استخدام عدد اكثر من access point لتغطية نفس المسافة المغطى ب 2.4GHz
  2. 802.11 b
     - هو اول standard تم تقديمه وكان يعمل على 2.4 GHz
  3. 802.11 g
     - من اهم مميزاته انه متوافق مع 802.11 b وانه قام بذيادة الthroughput

4. 802.11 n
   - تم تصميمه للحصول على throughput اعلى من الstandard السابقة كما انه متوافق مع جميع الstandard السابقة
5. 802.11 ac
   - يعمل على تردد 5GHz واصبح يعطى نفس قدرة gigabit Ethernet
   - اصبح يعطى wireless connection لاكثر من client فى نفس الوقت مما جعل الaccess point التى تعمل به تعمل على انها switch وليس hub

Standard	Frequency	Maximum Speed	Backwards compatibility
802.11	2.4 GHz	2 Mbps	-
802.11a	5 GHz	54 Mbps	-
802.11b	2.4 GHz	11 Mbps	-
802.11g	2.4 GHz	54 Mbps	802.11b
802.11n	2.4 and 5 GHz	600 Mbps	802.11a/b/g
802.11ac	5 GHz	1300 Mbps	802.11a/n
802.11ad	2.4 GHz, 5 GHz and 60 GHz	7 Gbps	802.11a/b/g/n/ac

- مدى وقوة الاشارة يعتمد على عوامل كثيرة منها :
  1. قوة الانتنة وهى عمود الارسال
  2. الحواجز
  3. عدد الاجهزة التى يمكن ان تسبب Interference
- MIMO هى تقنية ظهرت فى 802.11 n وهى اختصار ل multiple input multiple output وهى تستخدم اكثر من antennas فى ال access point لعمل data processing فى كل واحدة فى نفس الوقت
- هناك تقنية ظهرت اخرى وهى MU-MIMO وهى ظهرت فى 802.11 ac wave 2
- فى MIMO كان يتم الاتصال بclient واحد فى نفس الوقت ويتم التبديل بينهم بشكل سريع بينما فى الMU-MIMO سيتم التعامل مع كل الclients معا فى نفس الوقت
- Channel bonding هى تقنية ظهرت ايضا لرفع كفائة شبكات الwireless وتقوم على دمج 2 channel او اكثر معا وقد ظهرت من 802.11 n
- فى ال802.11 ac يمكن عمل bonding لانشاء channel تكون 20MHz او 40MHz او 80MHz او 160MHz

Wifi security

- عملية اتصال الuser على الwireless يجب ان تتم تحت طريقة فى الauthentication واشهر طريقة هى password & username
- Open authentication وهى طريقة فى الauthentication تقوم على عدم وجودpassword وان اى جهاز يستطيع الاتصال عليها بشرط وجود MAC address
- Shared Key authentication وهى ان الاتصال يجب ان يتم من خلال معرفة shared key وهو الpassword
- 802.1x وهى تقوم على ان للاتصال بالwireless سنحتاج على username و password وعندما نريد الاتصال سيقوم الAP بالاتصال مع server يسمى RADIUS وهو الذى يحتوى على جميع الusernames و الpasswords

- تاتى بعد ذالك خطوة الencryption وكان اول standard يتم تقديمه هو WEP وكان يقدم 64/128 encryption
- WPA وهو نوع ماذال موجود الى الان ويستخدم 128/256 bit encryption ويعتمد على protocol يسمى TKIP
- WPA2 وهو الاكثر استخداما الان ويستخدم protocol اخر وهو AES
- WPA3 وهو افضل ولاكن ليس مستخدما بكثرة

Antennas

- هى الجزء المسؤل عن تحويل الdata الى electromagnatic wave وارسالها فى الجوة او استلام الموجات وتحويلها الى data
- تتوجد بعض الخصائص للantennas مثل :
  1. Antenna's power output
  2. Frequency
  3. Radiation pattern

- Radiation pattern هو عبارة عن وصف لمقدار قوة الattennas فى الdimensional 3 الموجودة حولها
- يقوم radiation pattern بتقسيم الantennas الى :
  1. Unidirectional antenna تستخدم عندما يريد الsource ارسال الdata فى اتجاه واحد لتكوين point to point link
     - من اشهر انواعه الطبق المستخدم فى استقبال القنوات الفضائية

  2. Omnidirectional antenna وهى تقوم بارسال الاشارات فى جميع الاتجهات
     - من اشهرها هى ابراج الاتصال فى الازاعة و التلفزيون
- المدى الذى يمكن للanttana الوصول اليه يسمى ال range واى جهاز داخل هذا المدى يمكنه الاتصال بالantennas ولاكن قد يكون هناك بعض المونثرات الخارجية التى تمنع هذا الاتصال

Signal propagation

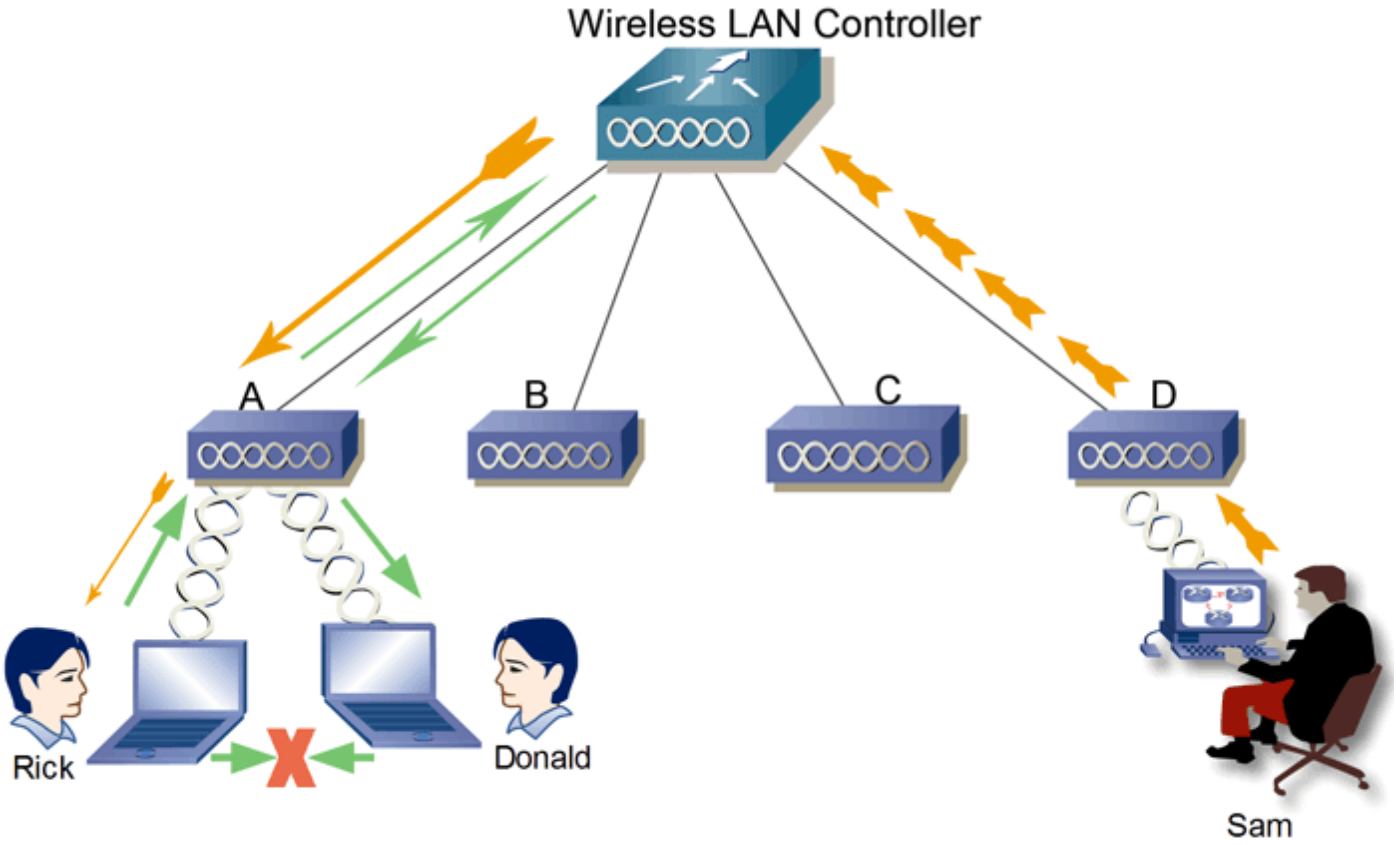
- وهى العوامل المسببة لضعف وانحراف الاشرات داخل الوسط (الهواء) ومن امثلتها
  1. Fading
     - هو التلاشى ويعنى انه كلما ذادت العوائق مثل الجدران كلما ذاد نسبة التلاشى
  2. Attenuation
     - هو ضعف الاشارة مع ذيادة طول مسارها وهذه المشكلة كانت تقابل انتقال الdata خلال الwire وكانت يتم معالجتها باستخدام repeater ولاكن فى حالة الwireless يتم معالجتها ب range extender
  3. Interference
     - فى الwireless يصبح هذا العامل قوى جدا بسبب عدم وجود اساليب حماية ضده كما توجد فى الwires
     - يتم قياس الnoise بما يسمى SNR او S/N
     - يوجد اجهزة تسبب ايضا ضعف فى الsignals مثل microwave
  4. Refration
     - وهو الانكسار وهو عامل يحدث عند انتقال الsignals من وسط الى اخر كما يحدث لضوء
  5. Reflection
     - وهى تحدث ايضا بسبب الحواجز مثل الحوائط
  6. Scattering
     - وتعنى التشتت وهى تحدث ايضا بسبب الحواجز
  7. Diffraction
     - وتعنى التفرق حيث تتفرق الsignlas الى اكثر من signal اخرى وتحدث ايضا بسبب العوائق
- بسبب كل العوائق السابقة يمكن ان تصل مجوعة من الsignals قبل الاخرى بترتيب خاطئ
- الfrequences هى الترددات التى تعمل عليها الwireless مثل 2.4 و 5 ولاكن لكى يتم استخدام اكثر من شبكة بنفس الfrequences فاننا ناتى الى التفرقة بينهم من خلال الchannels
- الchannels هى عبارة عن ranges مختلفة داخل نفس الfrequence وفى ال 2.4 يكونو 11 او 13 من الchannel
- عند استخدام channel معينة فانه ايضا يتم استخدام الchannels التى حولها حيث يفضل استخدام 1 و 6 و 11 للاتى :

- عند استخدام channel 1 فانه سيتم فعليا استخدام كلا من 1 و 2 و 3
- عند استخدام channel 6 فانه يتم فعليا استخدام كلا من 4 و 5 و 6 و 7 و 8
- عند استخدام 11 فانه يتم استخدام 11 و 10 و 9

- كلا من 1 و 6 و 11 يتم اطلاق عليهم non over labing channels
- فى الG.Hz 5 يوجد 23 channels و 12 non overlabing channels

Mesh topology in wireless

- هو topology اخر فى الwireless يقوم على وجود اكثر من access point متصلين جميعهم بجهاز واحد وهو wireless controller



- يمكن لل wireless controller ان يكون جهاز فى شكل phiscal او حتى cloud base او حتى virtual
- هناك الكثير من الprotocols التى سهلت عملية التحكم فى الwireless access points من خلال wireless controller مثل LWAPP و CAPWAP
- يقوم الwireless controller يقوم بمهمة centralized authentication و load balancing وchannel management وAP redundancy
- AP redundancy تعنى انه فى حالة توقف access point معينة سيتم توجيه الuser الى اخرى بشكل تلقائى للحفاظ على اتصاله
- يمكن ربط اكثر من wlan معا بشكل wireless من خلال تحويل omnidirectional antennan الى unidirectional antennan فى الاتجاه الموجود فيه الwlan الاخرى ويكون هذا الlink من النوع point to point

Determine the design

- فى الشركات الصغيرة او المكاتب الصغيرة يفضل استخدام ما يسمى بالSOHO router
- SOHO هى اختصار ل small office home office
- SOHO router يقوم بمهام كثيرة منها عملية switching و routing و natting و الfirewall والمذيد من الfunction

- من اهم الاشياء التى يجب مراعتها عند الاتيان ب AP وهى الdistance التى من المفترض العمل بها
- يفضل وضع الaccess point ان يكون فى منتصف المكان او فى الموضع المرتفع
- يفضل وضع الAP بعيدا عن مسببات الموجات مثل المواتير او microwave او المبات الفرسنت
- عند العمل على شركات او اماكن كبيرة فانه يجب التاكد من عدد الAP المحتاجة وايضا الاماكن المناسبة لوضع الAP ويفضل عمل ذالك من خلال ما يسمى ب Site survey وهو application لتسهيل هذه الخدمة
- يلزم تذويد site survey application ب map وهو سيقوم بعمل مسح للمنطقة وارجاع ما يسمى بالheat map للمكان