أولاً : مقدمة

نموذج OSI

ثانياً : طبقات OSI

- Physical Layer
- Data Link Layer
- Network Layer
- Transport layer
- Session Layer
- Presentation Layer
- Application Layer

ثالثاً : البروتوكولات

- بروتوكولات الاتصال : Connection Oriented
- بروتوكولات عديمة الاتصال :TCP/IP Connectionless
- TCP/IP

- DoD(Department of Defense Model Layers)
  - Process/Application Layer
  - Host-to-Host Layer
  - Internet Layer
  - Network Access Layer

- Transmission Control Protocol TCP(Package Détails)
  - Source Port
  - Destination Port
  - Sequence Number
  - Acknowledgement Number
  - Offset
  - Reversed
  - Flags
  - Window
  - Urgent Pointer
  - Options
  - Padding
  - Start of Data

- Internet Protocol IP(Package Détails)
  - Packaging
  - Internet Header Length أوIHL
  - Type of Service أوTOS
  - Total Length
  - Identification
  - Flags
  - Fragmentation Offset
  - Time to Live
  - Protocol
  - Header Checksum
  - TCP Header
  - Start of Data

عنوان الشبكة IP

- IPv4
- IPv6

رابعاً : بروتوكولات الشبكة

- SNMP
- FTP
- TFTP
- SMTP
- POP
- IMAP
- Telnet
- ICMP
- HTTP
- ARP
- NTP
- UDP

خامساً : PORTS and Sockets

سادساً : Linux and Networking

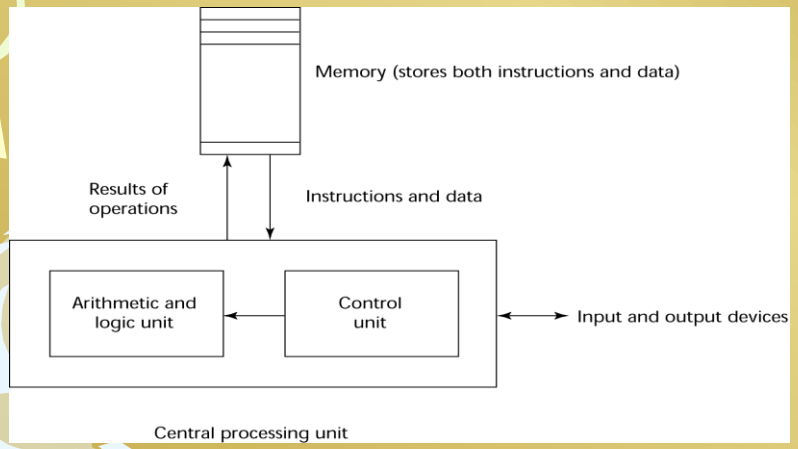
بروتوكولات الشبكة

THE OSI Model - TCP/IP

أولاً : مقدمة

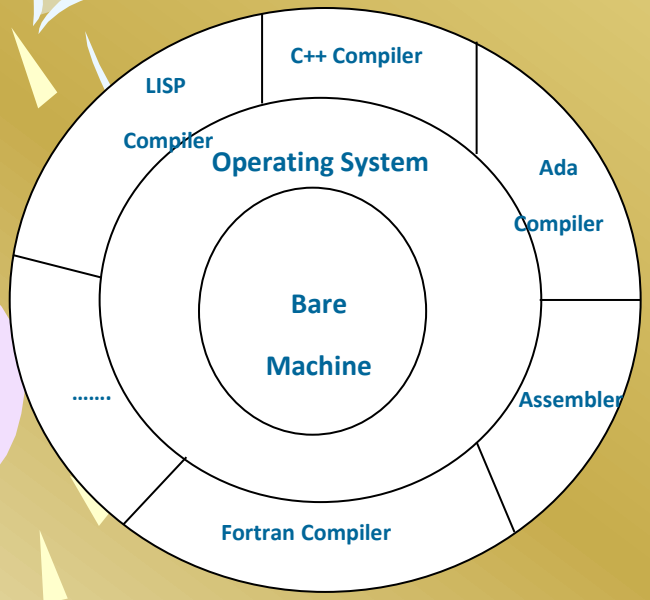
الحاسب ونظرية الطبقات البرمجية

Layered View of Computer



Von Neumann Model

- **Data** and **Instructions** are stored in Single **R/W Memory**
- Contents of This Memory are addressable by **Location**
- Execution occurs **Sequentially**, from one Instruction to next

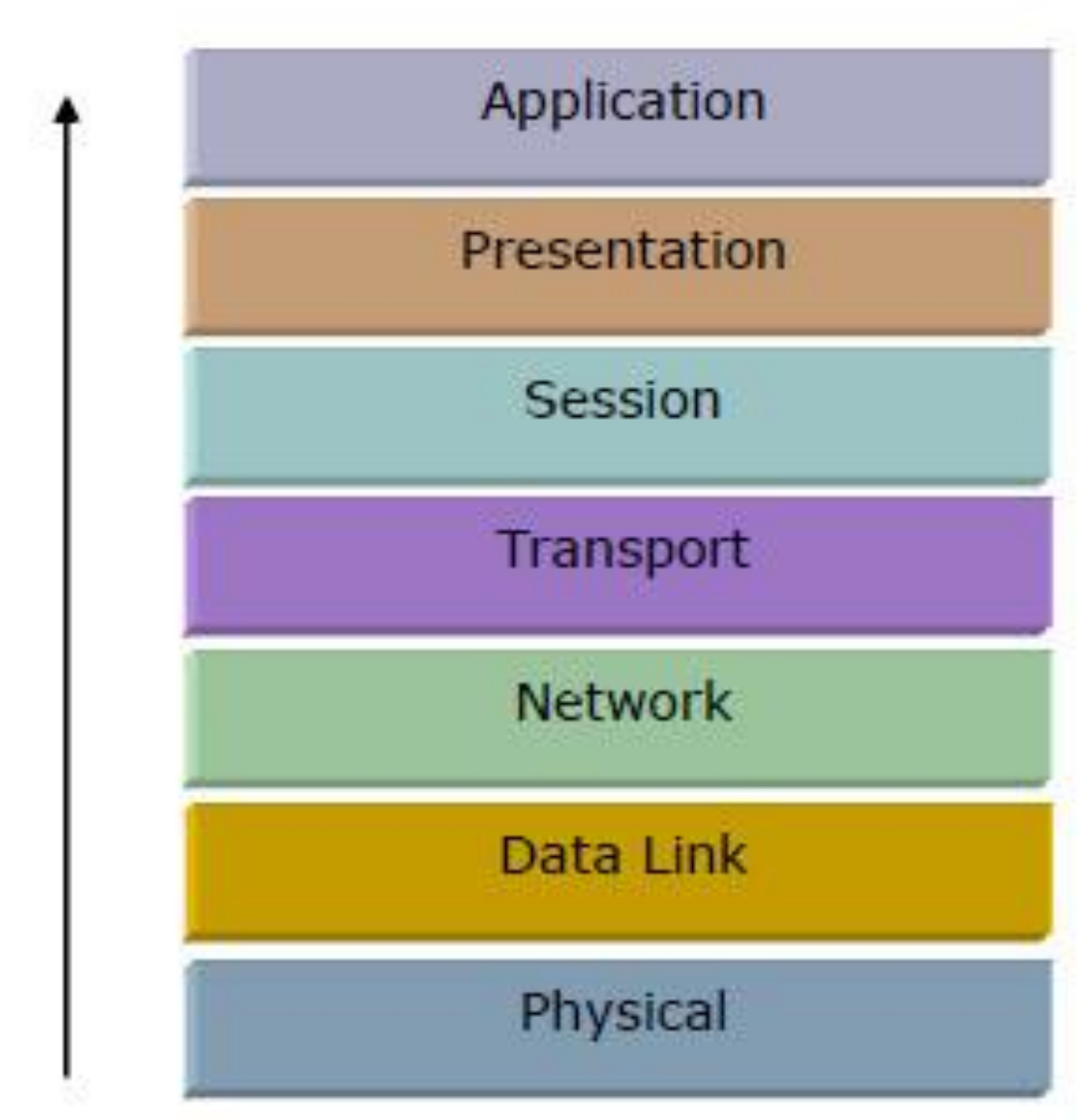


The operating system and language implementation are layered over Machine interface of a computer

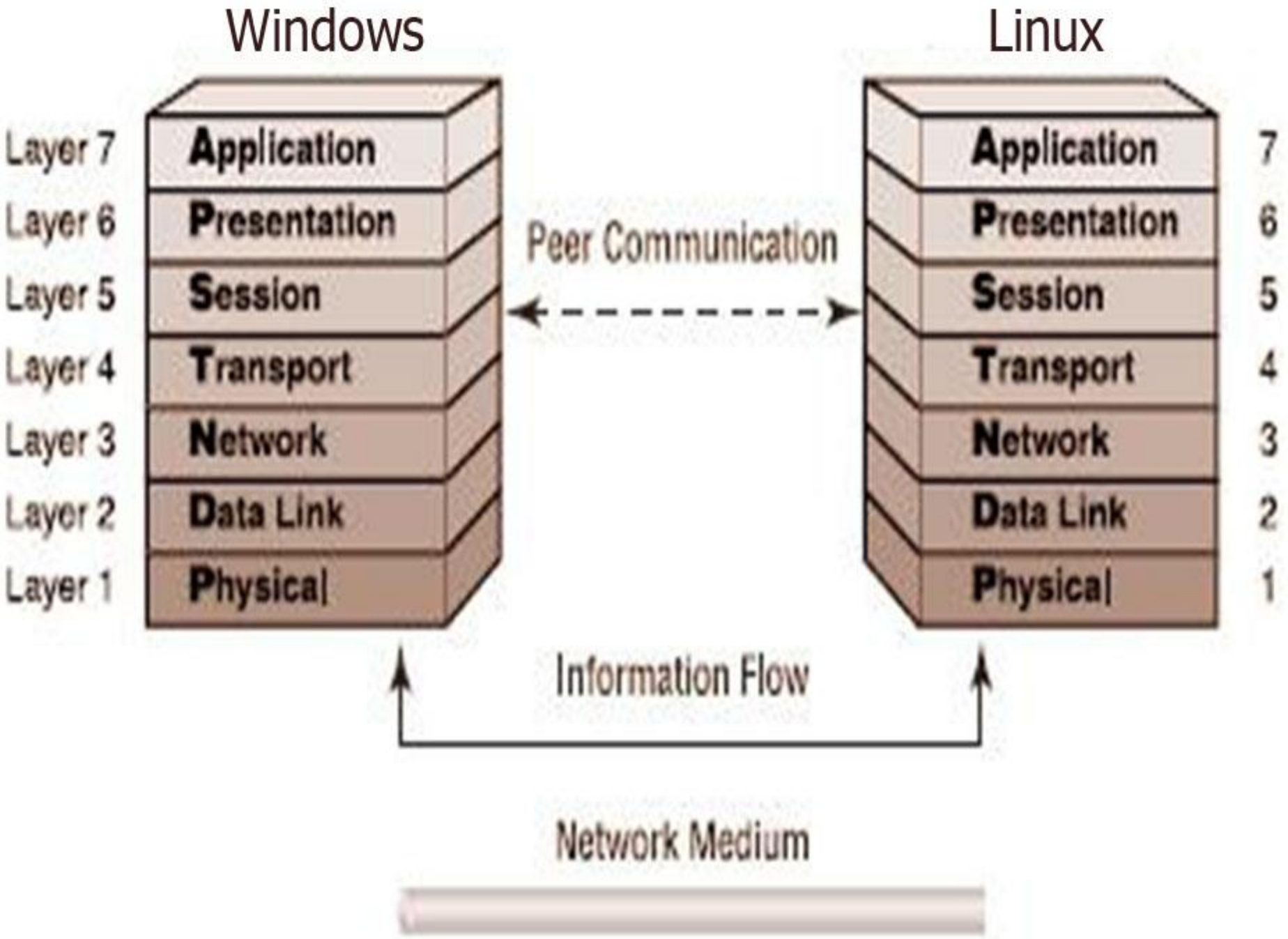
مقدمة- ٢

- OSI هي اختصار لـ Open System Interconnect
- هي الطريقة التي بها تستطيع أن تفهم كيفية نقل البيانات عبر الشبكات، وكما هو معلوم أن الشبكات ربما تحتوي على أجهزة Hardware مختلفة وأيضاً برامج وأنظمة تشغيل متنوعة ، إذاً كيف نوجد علاقة للتعامل مع هذه الأجهزة على الشبكة في إطار واحد إذ ليس من المنطق أن تتعامل مع بعضها البعض بدون طريقة وسطية وأيضاً نقل الملفات مثلاً عبر الشبكة قد تكون مسألة بسيطة بالنسبة لك لا تتعدي نقرة زر إلا أن الأمر- فى الخلفية - يحتاج إلى عمليات أكثر تعقيداً لنقل هذه البيانات عبر الشبكة من جهاز إلى آخر وهنا يأتي دور الـ OSI Model لنفهم ما الذي يحدث بالضبط

نموذج OSI


Application
Presentation
Session
Transport
Network
Data Link
Physical

- يتكون نموذج OSI من سبع طبقات
- يؤمن هذا التقسيم للطبقات إمكانية الاتصال بين أجهزة بأنظمة تشغيل مختلفة مثل Linux وWindows
- ضع في اعتبارك أن الـ OSI هو مجرد Model أو نموذج يشرح فقط كيفية الاتصال وليس بروتوكول مستخدم في الاتصال من قبل الأجهزة والبرمجيات


Windows
Linux
Layer 7
Application
Layer 6
Presentation
Layer 5
Session
Layer 4
Transport
Layer 3
Network
Layer 2
Data Link
Layer 1
Physical
Peer Communication
Application
Presentation
Session
Transport
Network
Data Link
Physical
7
6
5
4
3
2
1
Information Flow
Network Medium

ثانياً : طبقات OSI

١) Physical Layer
٢) Data Link Layer
٣) Network Layer
٤) Transport layer
٥) Session Layer
٦) Presentation Layer
٧) Application Layer

Physical Layer - ١

- هي الطبقة أو الجزء الذي يهتم بتسجيل بيانات الاتصال الخاص بالـ Hardware مثل نوع البطاقة وعدد الـ Pins وغير ذلك
- تحوي أيضاً معلومات التشبيك المختلفة أي طبولوجيا الشبكات وتتمثل في

  (Star, Ring, Mesh, and Bus) Topologies
- الأجهزة التي تعمل على هذه الطبقة

  NIC , Transceivers , Repeaters – Hubs

Data Link Layer - ٢

- تقوم بتحويل البيانات واستلامها من Physical Layer وتحويلها إلى (بنية منطقية)
- تحوي اسم الكمبيوتر والبيانات المرسلة وأيضاً تنتظر كود ACK
- وتتكون هذه الطبقة من قسمين هامين هما :
  - LLC Logical Link Control
  - MAC Media Access Control
- الأجهزة التي تعمل في هذه الطبقة
  Bridge , Switch , NIC

Network Layer - ٣

- في هذه الطبقة يتم تحويل الأسماء المنطقية للأجهزة إلى عناوين فيزيائية
- أيضاً هناك خدمة تدعى Quality Of Service تعمل على هذه الطبقة وهي مسؤولة عن عدم حدوث تأخير في بعض الخدمات على الشبكة مثل الصوت والفيديو
- أيضاً مهام التوجيه Routing تتم في هذه الطبقة
- الأجهزة التي تعمل على هذه الطبقة
  Routers , Layer 3 Switches

Transport layer - ٤

- مسؤولة عن التأكد من نقل البيانات دون حدوث أخطاء
- تقسم الرسائل الكبيرة إلى عدة رسائل صغيرة وأيضاً العكس تحول الأجزاء الصغيرة من الرسالة إلى رسالة طويلة مرة أخرى
- مسؤولة عن التحقق من وصول البيانات بشكل صحيح عن طريق ما يسمى ACK أي التحقق من الوصول أو إشعار الاستلام

Session Layer-٥

- يتم فيها يتم الاتصال المباشر ما بين الجهازين حيث يتم التأكد من رقم الجهاز وعنوانه وهل تم إرسال المعلومات أم لا؟
- وأيضاً كلمات السر وتأمين البيانات يتم هنا في هذه الطبقة وأي عملية يتم فيها التأكد من المعلومات تتم هنا أيضاً

Presentation Layer-٦

- كما هو واضح من المعنى تقديم الـ Data وتهيئتها للتبادل
- حيث يتم تشفير البيانات أو حتى ضغط للبيانات

٧- Application Layer

- هي أعلى طبقة وهي لا تعني الـ Applications كبرنامج الـ Word والـ Access بقدر ما تعني الـ Application المسئول عن تنفيذ الأمر المتعلق بالشبكة الذي يطلبه برنامج مثل الـ Word
- مثلاً عندما تقوم بفتح برنامج عبر الشبكة فأنه يستخدم بعض الأدوات التي لا تراها تسمى Tools وهي المقصودة في المعنى
- وتتضمن أيضاً الطباعة والرسائل ولا تقتصر على ذلك بل تتعداه

ثالثاً : البروتوكولات

- البروتوكولات هي أساليب التخاطب أو تقنيات التخاطب ما بين الأجهزة على الشبكة أو بين الشبكات المختلفة
- تنقسم البروتوكولات إلى قسمين :
  - بروتوكولات الاتصال : Connection Oriented وهي بروتوكولات تقوم بإجراء الاتصال المباشر بين أجهزة الشبكة . و من أشهرها بروتوكول TCP
  - بروتوكولات عديمة الاتصال : Connectionless وهي بروتوكولات لا تسمح بالاتصال المباشر مع الكمبيوتر . ويعد بروتوكول IP هو أشهر تلك البروتوكولات .

TCP/IP

- هو اختصار Transfer Control Protocol/Internet Protocol
- حقيقة هو ليس برتوكول في حد ذاته أكثر منه مجموعة من الأدوات. وهو الأكثر استخداما في الإنترنت ويستخدم للربط والتخاطب ما بين الأجهزة عبر الشبكة المحلية وأيضاً عبر الإنترنت وهو البروتوكول الأكثر استخداماً وشيوعاً

لمحة تاريخية

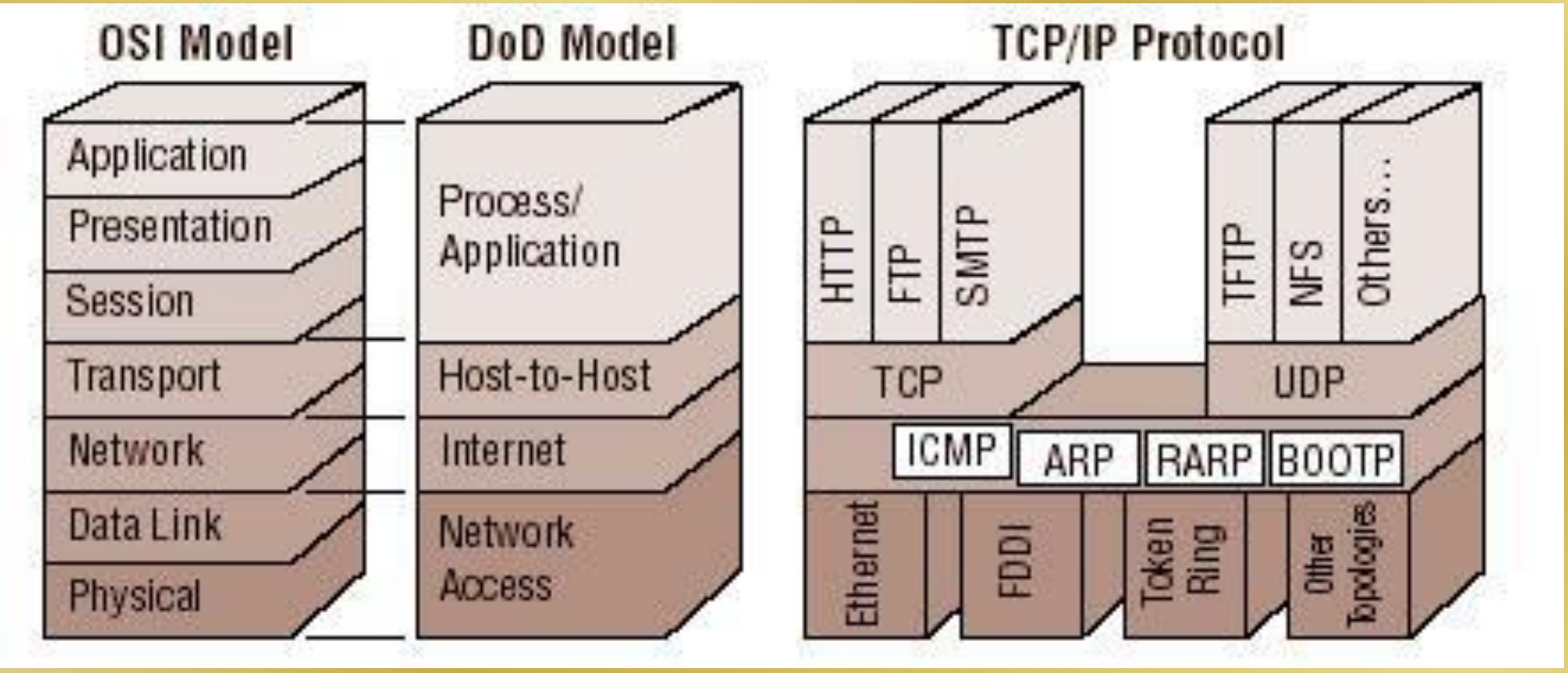
- تم ابتكار هذا البروتوكول عام ١٩٧٣ لكنه لم يكن قياسياً حتى عام ١٩٨٣ حتى أصبح الطريقة الافتراضية في الاتصال عبر الإنترنت أو عبر ARPAnet كما كانت تدعى شبكة الإنترنت في ذلك الوقت
- وقد خرج هذا الابتكار من معامل جامعة كاليفورنيا الأمريكية في Berkeley عندما كان علماء الكمبيوتر عاكفون على إخراج نسخة UNIX BSD أي Berkeley Software Distribution
- بدأ انتشاره في الجامعات نظرا لبدء انتشار Unix في الحياة الأكاديمية حتى أصبح ثورة في عالم الإنترنت والشبكات المحلية

- السبب الذي أدى إلى تطوير هذا البروتوكول هو دعم وزراة الدفاع الأمريكية للأمر بحيث وضعت شروطاً ومعايير وقيود على التطوير طبقاً لمعايير معينة على سبيل المثال :

١) لا يخضع لشركة معينة أو برامج معينة أو عتاد معين
٢) يجب أن يحوي في داخله أدوات للصيانة حيث أن هذا كان متعلقاً بالمسائل العسكرية بوزراة الدفاع حيث إذا حدثت مشكلة في جزء من الشبكة هذا ليس معناه سقوط الشبكة كلياً
٣) إمكانية الاتصال ما بين الشبكات والأجهزة والبرمجيات المختلفة

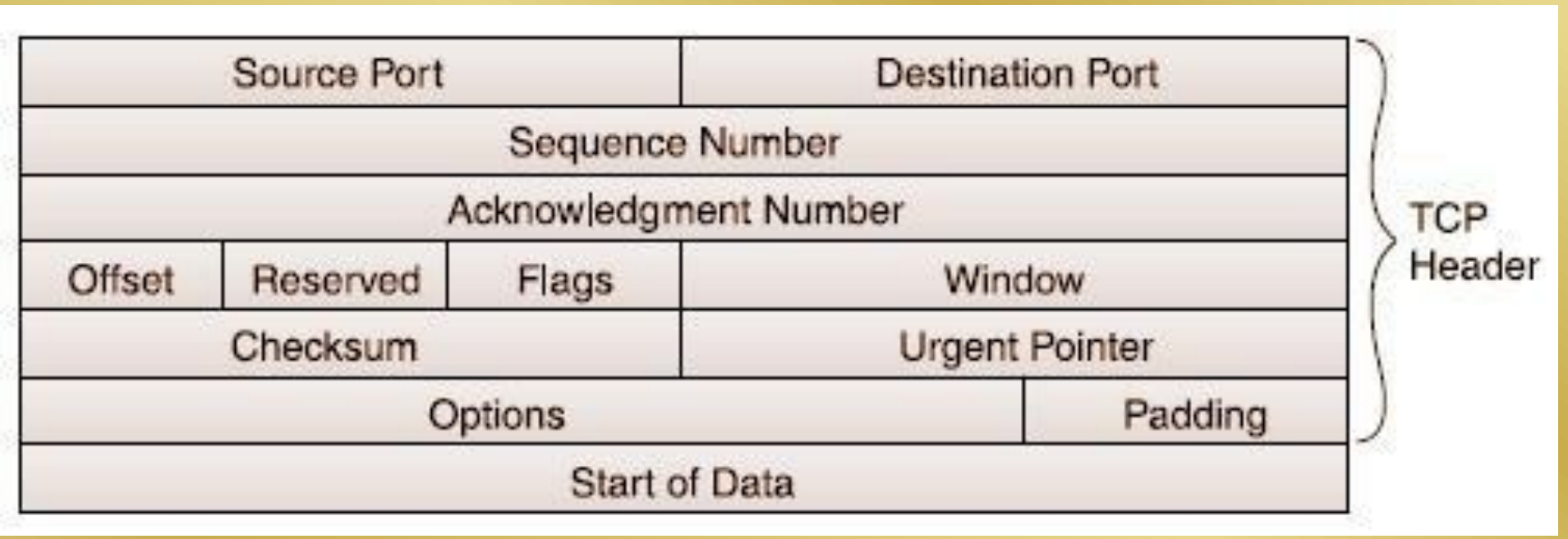
DoD Model

- يستخدم TCP/IP ما يسمى Department of Defense Model
- والذي يصف الاتصال في أربعة طبقات فقط خلافاً للـ OSI Model والشكل التالي يوضح الفرق
- Process/Application Layer هي المسئولة عن البرمجيات مثل FTP, Telnet , HTTP
- Layer Host-to-Host طبقة الوسيط للوسيط وهي التي يتم فيها إضافة TCP والبروتوكولات الأخرى للـ Packet
- Internet Layer يتم فيها إضافة الـ IP
- Network Access Layer هي المسئولة عن الربط ما بين وسائط النقل مثل الكابلات وأيضا كروت الشبكة


OSI Model
DoD Model
TCP/IP Protocol
Application
Presentation
Session
Transport
Network
Data Link
Physical
Process/
Application
Host-to-Host
Internet
Network
Access
HTTP
FTP
SMTP
TFTP
NFS
Others...
TCP
UDP
ICMP
ARP
RARP
BOOTP
Ethernet
FDDI
Token
Ring
Other
Topologies

Transmission Control Protocol TCP

- هو الجزء المسئول عن نقل البيانات والربط ويقسم هذا الجزء البيانات إلى أجزاء صغيرة للتعامل معها تسمى هذه الأجزاء Datagram الذي يحوي على معلومات عن المكان الذي سوف ترسل له البيانات وعنوان المرسل وأيضاً رقم ميز للـ datagram هذه البيانات تسمى الـ Header
- كما تحتوي على ما يسمى Checksum للتأكد من وصول البيانات إلى النقطة المرسل إليها البيانات والشكل التالي يوضح أهم مكونات datagram في الـ TCP


Source Port
Destination Port
Sequence Number
Acknowledgment Number
Offset
Reserved
Flags
Window
Checksum
Urgent Pointer
Options
Padding
Start of Data
TCP Header

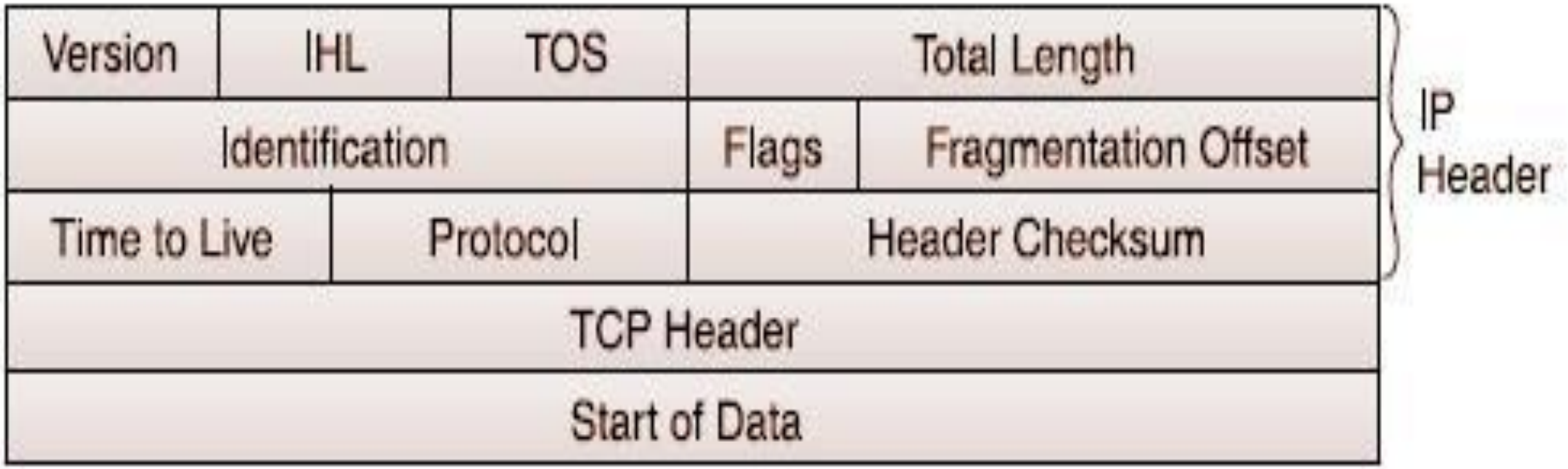
- Source Port يعبر عن رقم المكان الذي يرسل البيانات
- Destination Port رقم المكان أو النقطة المرسل إليها البيانات
- Sequence Number الرقم المسلسل الخاص بالـ datagram لتسهيل عملية إعادة تنظيم البيانات على الكمبيوتر المستقبل
- Acknowledgement Number رقم يمكن الكمبيوتر المرسل من معرفة أن البيانات تم نقلها بنجاح
- Offset تعبر عن طول الـ Header ككل
- Reversed عبارة عن متغير يمكن الاستفادة منه في أي شيء آخر إضافي

- Flags تعبر عن أن هذه المعلومات هامة جدا أو أنها نهاية المعلومات المنقولة
- Window تعطي إمكانية زيادة حجم الـ Packet مما يؤدي إلى دقة نقل البيانات
- Urgent Pointer يعطي تصريحاً بأهمية البيانات
- Options مجموعة من المتغيرات ربما تستخدم فيما بعد من قبل المستخدم
- Padding للتأكد من أن الـ Header انتهى عند 32 Bit
- Start of Data بداية المعلومات الحقيقية التي سوف يتم نقلها

Internet Protocol IP

- هو المسئول عن نقل البيانات من نقطة إلى نقطة أخرى على الشبكة وهو لا يحمل أو يحوي أي نوع من البرمجيات الخاصة بالاتصال لكنه يعتمد كلياً على الـ TCP ولكنه فقط يقوم بعمليتي Route توجيه أو نقل للمعلومات و Packaging (تشطير الرزم وإعادة الرزم)
- ودائما يكون الـ Header الخاص بـ IP متصلاً بالـ Header الخاص بـ TCP
- من دون الـ Header الخاص بـ IP لن تتم معرفة وجهة الـ Datagram أو لن يتم عمل توجيه لها

- فالتوجيه Routing يقوم بفحص العنوان الموجود على الرزمة الـ Packet ويعطيه تصريح تجول في أرجاء الشبكة
وهذا التصريح له مدة محددة TIME TO LIVE فإذا انتهت هذه الفترة الزمنية فقدت تلك الرزمة ولم تعد تسبب ازدحام داخل الشبكة
- وعمليه تشطير الرزم وإعادة الرزم Packaging
تستخدم في التوليف بين بعض أنواع الشبكات المختلفة مثل شبكة الـ Token Ring و Ethernet
بسبب ما لشبكة الـ Token Ring من سعة في نقل الإشارات لذلك وجب تشطيرها ثم إعادة تجميعها مره أخرى


Version
IHL
TOS
Total Length
Identification
Flags
Fragmentation Offset
Time to Live
Protocol
Header Checksum
IP Header
TCP Header
Start of Data

- Version تعبر عن رقم إصدار الـ IP المستخدم والإصدار الافتراضي المستخدم حاليا هو IPv4 إلا أن هناك الإصدار السادس IPv6 إلا انه لم يدعم إلا من بعض الأجهزة الحديثة حاليا إلا انه سوف يصبح الإصدار الافتراضي قريباً جداً
- IHL أو Internet Header Length
وهو طول الـ Header والرقم الافتراضي له هو خمسة كلمات من طول 32bit
- TOS أو Type of Service
تعبر عن أهمية البيانات المطلوبة
- Total Length تحدد طول الـ Datagram وتأخذ قيمة بين ٥٧٦ بايت و ٦٥٥٣٢ بايت
576 Byte – 65.532 Kbyte

- Identification تعريف يسهل على الجهاز المستقبل إعادة ترتيب الـ Datagram
- Flags أول بت يعبر عن أن الـ Datagram لا يمكن أن يكون مقسماً إلى أجزاء صغيرة والبت الأخير يعبر عن آخر قسم في أي Packet مقسمة إلى أقسام
- Fragmentation Offset

تعبر عن المكان المحدد للمعلومات وهي تستخدم في عملية إعادة تجميع البيانات من قبل المستقبل

- Time to Live

الوقت المستخدم أو المخصص لنقل الـ Packet بعد أن ينقضي هذا الوقت ستصبح بعدها الـ Packet مفقودة Lost ولها معنى آخر هو Hop ودائما تجدها 32Hops

- **Protocol**

تعبر عن نوع البروتوكول لأنه من الممكن استخدام بروتوكولات أخرى غير الـ TCP/IP

القيمة ٦ تعبر عن TCP

والقيمة ١٧ تعبر عن UDP User Datagram Protocol

- **Header Checksum**

قيمة للتحقق من عدم وجود الأخطاء في الـ Header

- **TCP Header**

هو كما تعرفت عليه سابقا الـ Header الخاص بـ TCP

- **Start of Data**

بداية المعلومات الحقيقية التي سوف يتم نقلها

عنوان الشبكة IP

- الرقم المميز لكل جهاز على الشبكة وإذا استخدمت بروتوكول TCP/IP فهذا يحتم عليك أن يكون هناك رقم مميز لكل جهاز على الشبكة.
- هناك نوعان أو إصداران من الـ IP هما IPv4 و IPv6

IPv4

- هذا الإصدار هو الأكثر استخداما الآن وهو عبارة عن ٤ خانات تتكون من رقم 32bit ودائماً يتم الفصل بين الأربع خانات إما بنقطة أو بعلامة عشرية وهو يبدأ بالأرقام من صفر حتى ٢٥٥ في كل خانة من الخانات الأربعة مثلاً 192.168.1.33
- نسمي كل خانة Octet أو Byte
- وتقسم أرقام الـ IP إلى فئات أو صفوف حسب حجم الشبكات والأجهزة المتوفرة عليها وهي

Class A, Class B, Class C, Class D, Class E

IPv6

- التقنية القادمة في الـ IP وتم ابتكاره خصيصا لأن الأرقام المتوفرة في النظام السابق أصبحت قليلة لكثرة المستخدمين على الشبكة ويستخدم 128bit ويعطي حوالي 79Octellion أي 79.000.000.000.000.000.000.000.000.000
- يستخدم نظام Hexadecimal بدلاً من النظام الثنائي
- في ثمانية خانات منفصلة تتكون خانة من أربعة أرقام وحروف على سبيل المثال
3FFE:0B00:0800:0002:0000:0000:0000:000C

رابعاً : بروتوكولات الشبكة

- SNMP
- FTP
- TFTP
- SMTP
- POP
- IMAP
- Telnet
- ICMP
- HTTP
- ARP
- NTP
- UDP

1 – SNMP
Simple Network Management Protocol

- ويستخدم هذا البروتوكول من قبل مديري الشبكة لمعرفة معلومات إضافية عن الشبكة وأيضاً الأجهزة الموجودة على الشبكة كالمبدلات Switches ومرشدات المسار Routers وأية أجهزة أخرى

2 – FTP
File Transfer Protocol

- هو أداة مهمة جداً لنقل الملفات عبر الشبكة وما بين الأجهزة التي تدعم هذه التقنية والتي تسمى FTP Servers
وبالتأكيد إذا كنت تتعامل مع مواقع الإنترنت فقد سمعت بهذا البروتوكول

3 – TFTP
Trivial File Transfer Protocol

- نسخة مصغرة من FTP تستخدم لنقل الـ Boot Image
  للأجهزة التي لا يوجد بها Boot Disk
  وأيضاً من وإلى الـ Routers

4 – SMTP
Simple Mail Transfer Protocol

- المسئول عن نقل الرسائل الإليكترونية عبر الشبكة ومن جهاز إلى جهاز آخر وهو المسئول عن الإرسال الخاص بالـ Emails

5 – POP
Post Office Protocol

- ويوفر مساحة تخزينية لاستقبال الرسائل الإليكترونية وهو معروف باسم POP3 وفي بعض الأحيان يستخدم الـ IMAP (**Internet Mail Access Protocol**) بدلاً من POP3

6 – IMAP
Internet Mail Access Protocol

- ويوفر مساحة تخزينية للمستخدم لتخزين الرسائل وأيضا قراءة الـ Email Header وتخزين جزء من الرسالة على الـ Server وهو المستخدم في Yahoo

7 – Telnet
Terminal Emulation

- ويتيح الاتصال عن بعد بالأجهزة على الشبكة

8 – ICMP
Internet Control Message Protocol

- والمثال الواضح لهذا البرنامج هو الأمر Ping الذي تستخدمه للتحقق من وجود الـ Host على الشبكة حيث يقوم بإرسال رسالة للـ Host واستقبالها منه مرة أخرى
- يوجد على نفس الطبقة مع بروتوكول IP حيث يوفر بروتوكول IP خدمة عديمة الاتصال Connectionless، فإذا حصلت أي مشاكل في الإرسال فإنه لا يوجد أي طريقة لبروتوكول IP للتعرف على هذه المشاكل أو حلها ، وهنا يأتي دور بروتوكول ICMP ليصدر تقريراً عن المشكلة


TELNET
FTP
SNMP
SMTP
TCP
IP
UDP
ICMP
DATA-LINK
PHYSICAL

9 – HTTP
Hypertext Transfer Protocol

- وهو وسيلة التخاطب ما بين الأجهزة والـ Web Servers والمستخدم في فتح المواقع على الـ Internet Browser

10 – ARP
Address Resolution Protocol

- أداة أو برنامج يمكنك من معرفة معلومات عن الـ Physical Hardware الخاصة ببطاقات الشبكة والعناوين IP الخاصة بها
- فهو مسئول عن تحديد عنوان بروتوكول IP وإيجاد عنوان الـIP الهدف باستخدام عنوان الـ MAC الموجود في الشبكة
- فإذا وجده قدم خريطة دقيقة للعنوان فإذا كان الحاسب بعيد (في شبكة بعيدة) يقوم الـ ARP بتوجيه الـ IP إلى عنوان الموجة الـ ROUTER ثم بعد ذلك يقوم هذا الموجه بتسليم الطلب لـ ARP حتى يبحث عن العنوان الفيزيائي MAC Address لرقم الـIP

11 – NTP
Network Time Protocol

- هذه الأداة مهمة جدا وقد تم ابتكارها من قبل البروفيسور David Mills في جامعة Delaware

والغرض الأساسي منها هو جعل جميع الأجهزة في الشبكة تعمل بتوقيت واحد أو Synchronize وهذا التوقيت حسب ساعة معينة لأنه لو حصل اختلاف في التوقيت بين الأجهزة على الشبكة هذا معناه اختلال العمل وضياع المعلومات .

12 – UDP
User datagram Protocol

- هذه الأداة أو البرنامج تعطي اتصال مباشراً بين البرمجيات وهي تعمل في طبقة Transport وأيضاً تتيح الاتصال بخدمة معينة أو برنامج معين عبر Port محدد في كمبيوتر آخر على الشبكة
- يستخدم في نقل الوسائط المتعددة مثل الصوت، الفيديو لأنها وسائط لا تحتاج إلى الدقة في الوصول كما أنه ذو فعالية كبيرة وسريع الأداء
- من أهم الأسباب التي أدت إلى إنشاء البروتوكول UDP أن الإرسال عبر هذا البروتوكول لا يتطلب إلا القليل من التحميل والوقت فهو بروتوكول غير موثوق

Ports and Sockets : خامساً

- في شبكات TCP/IP تنتقل المعلومات من الـ Port في الكمبيوتر المرسل للمعلومة إلى الـ Port في الكمبيوتر المستقبل للمعلومة حسب رقم الـ Port (المنفذ) والبرنامج الذي يستخدمه هذا المنفذ
- كل برنامج له منفذ معين يعمل عليه في الاتصال
- كل منفذ عبارة عن رقم 16bit وبالتالي تأخذ قيماً من صفر حتى ٦٥٥٣٥
- هذه المنافذ تقسم إلى TCP Ports و UDP Ports حسب البروتوكول الذي يعمل عليه المنفذ
- جميع المخدمات التي تتصل على خدمة Telnet تستخدم الـ Port ٢٣ وهو TCP Port
- جميع مخدمات الويب تعمل على المنفذ ٨٠

- **Socket** is generally a SW component that is used to connect a computer to the internet sites or to communicate with other computers. It contains address of the other side computer as well as the port number.
- **Port number** is the number that specify a particular process on that machine. As so many processes can be running on machine some time it is needed to specify a port. Many time it is optional.

PORT	*PROTOCOL*
UDP Port 15	NETSTAT
TCP Port 21	FTP
TCP Port 23	Telnet
TCP Port 25	SMTP
UDP Port 53	DNS
UDP Port 69	TFTP
TCP Port 70	Gopher
TCP Port 79	Finger
TCP/UDP Port 80	HTTP
TCP/UDP Port 443	HTTPS
TCP Port 110	POP3
UDP Port 111	RPC
TCP Port 119	NNTP
TCP Port 123	NTP
UDP Port 137	NetBIOS Name Service
UDP Port 161	SNMP (Network Monitor)
UDP Port 2049	NFS

- المداخل SOCKETS

هي عبارة عن تطبيقات جزئية مسئولة عن السماح بالدخول إلى معظم الأنظمة من خلال بروتوكول TCP/IP، الذي لا يستخدم فقط للدخول إلى الانترنت، وإنما يستخدم أيضاً على نطاق واسع لبناء الشبكات الخاصة.

وقد تكون هذه الشبكات الخاصة مرتبطة بالانترنت، وقد لا تكون مرتبطة بأي شبكة أخرى

ونسمي الشبكة الخاصة التي تستخدم بروتوكول TCP/IPوبرمجيات الانترنت، بشبكات انترانيت

سادساً: Linux and Networking

- Linux نظام مبني من الأساس وفي كل جزئية بما يتوافق مع الشبكات والأمن وهو يوفّر في نواته مجال ودعم أكبر للبروتوكولات الشبكية الشهيرة كما تأتي أغلب التوزيعات وهي مزودة بالعديد من الأدوات والخدمات الخاصة بإدارة وإعداد الشبكات كل هذا الدعم وأكثر من بروتوكولات وأدوات وبرامج تشكل بمجموعها دعم يتفوق على كثير من الأنظمة الأخرى في مجال الشبكات .
- سنتناول الإعداد بما يتوافق مع أنظمة RedHat ولكن لن تختلف طريقة الإعداد والأدوات في غير توزيعات لأن أدوات RedHat هي أقوى الأدوات وهي مستخدمة في أكثر من توزيعة وما يعمل على RedHat يعمل على غيرها

أسرع TCP/IP

- Linux يحتوي على قدرات متقدمة للشبكات. حيث أن مطوريه تعاونوا واستخدموا الإنترنت لتطويره دعم الشبكات أتى في المراحل الأولى لعملية التطوير
- تعتبر قدرات دعم الشبكات في نظام Linux أعلى من قدرات أغلب أنظمة التشغيل الأخرى. حيث يدعم الاتصال بشبكة الإنترنت أو أي شبكات أخرى بواسطة بروتوكولات TCP/IP أو IPX عن طريق Ethernet، Fast Ethernet، ATM و Token Ring وغيرها الكثير
- يمكن استخدام نظام لينكس كخادم Server لشبكة الإنترنت

- يدعم نظام Linux جميع أشهر بروتوكولات الإنترنت، متضمناً البريد الإلكتروني، أخبار UseNet، Gopher، Telnet، Web، FTP، Talk، POP، NTP، IRC، NFS، DNS، NIS، SNMP، Kerberos، WAIS وغيرها الكثير.
- يمكن لنظام Linux أن يعمل كتابع/كزبون أو كخادم لجميع البروتوكولات السابقة وتم استخدامه وفحصه بانتشار للتأكد من ذلك
- يمكن أيضاً لنظام Linux أن ينخرط في الشبكة المحلية LANبكل سهولة ويسر بغض النظر عن مختلف الأجهزة التي تستخدمها. حيث يدعم دعماً كاملاً لأنظمة : Macintosh، DOS، Windows، Windows NT، Windows95، Novel، OS/2 كلٌ يستخدم بروتوكولاته الخاصة. يمكن لنظام لينكس أن يعمل كل ذلك بوجود فقط ١٦ ميجابايت من الذاكرة أو حتى أقل من ذلك بوجود خاصية التبديل Swapspace