جامعة المنارة
كلية الهندسة
الهندسة المعلوماتية

أساسيات الشبكات الحاسوبية

مدرس المقرر
أ.د. مثنى علي القبيلي

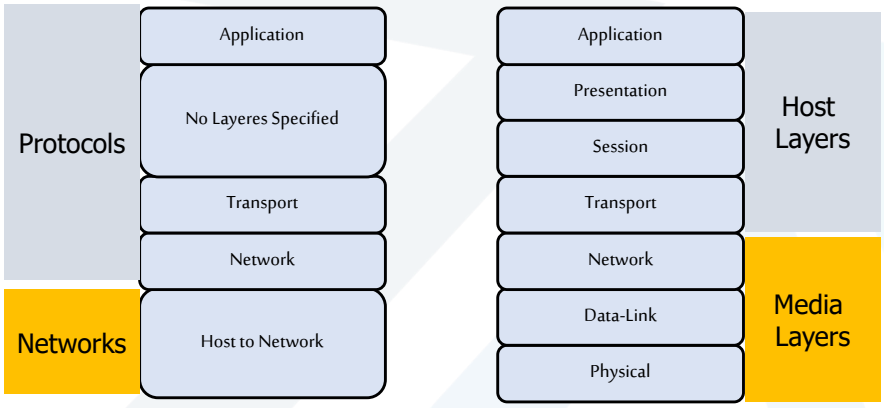
الفصل الدراسي الثاني
العام الدراسي 2024-2023

Chapter 7: Transport Layer Protocols

Learning outcome

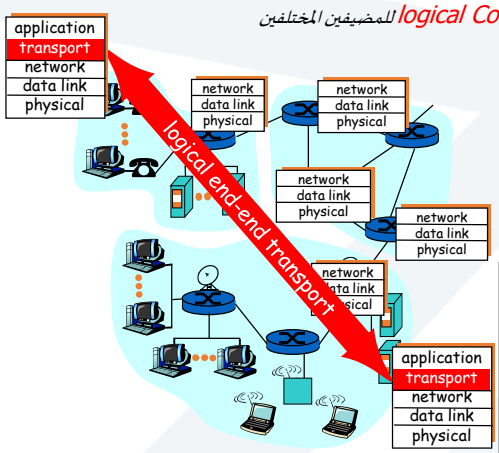
- Transport Layer Overview.
- Multiplexing/demultiplexing.
- UDP Protocol.
- TCP Protocol.

OSI Vs TCP/IP



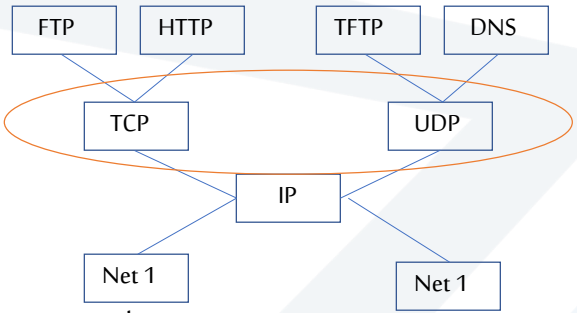
Transport services and protocols

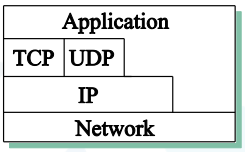
- تزود طبقة النقل الاتصالات المنطقية *logical Communication* للمضيفين المختلفين
- الهدف من طبقة النقل هو تأمين خدمة فعالة، مناسبة وموثوقة، ومعقولة التكلفة لمستخدمي هذه الطبقة والذين عادةً مايكونون جزئيات برمجية من طبقة التطبيقات *application Processes*
- تعمل بروتوكولات النقل في الأنظمة النهائية *(end systems)*



- Network layer: logical communication between hosts
- Transport layer: logical communication between processes
  - ✓ relies on, enhances, network layer services

The Internet Architecture





- Ethernet

FDDI

FTP: File Transfer Protocol

HTTP: Hypertext Transport Protocol

TFTP: Trivial File Transfer Protocol

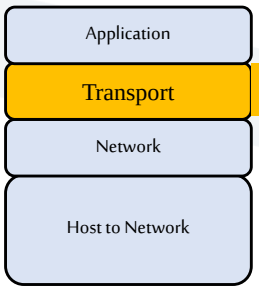
DNS: Domain Name System

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

IP: Internet Protocol

Transport Layer Overview



TCP: Transmission Control Protocol

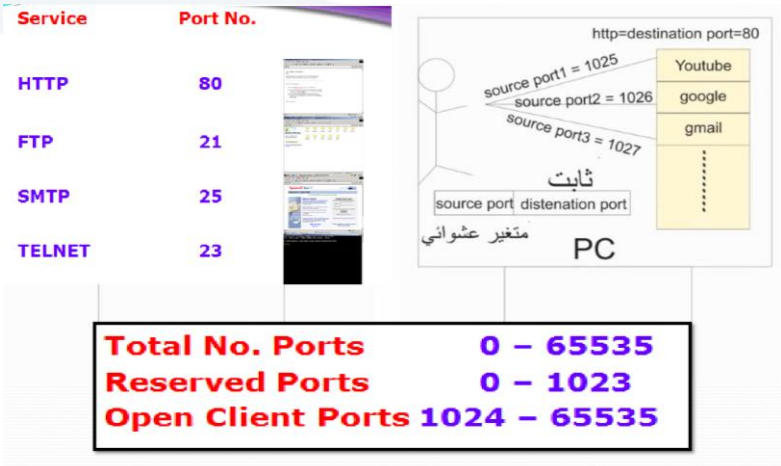
UDP: User Datagram Protocol

- تنجز طبقة النقل وظيفتين أساسيتين:
  - ✓ التحكم بالتدفق flow control: والذي يتم عن طريق sliding windows
  - ✓ الوثوقية Reliability: والذي يتم عن طريق أرقام التسلسل والإفادة بالاستلام sequence numbers and acknowledgments
- تزود هذه الطبقة بروتوكولين:
  - ✓ TCP: وهو بروتوكول موثوق-اتصال موجه، يزود التحكم بالتدفق من خلال sliding windows، والوثوقية من خلال أرقام التسلسل والإفادة بالاستلام. فائدة TCP هو دعمه للتسليم المكفول/المضمون لرزم البيانات guaranteed delivery
  - ✓ UDP: وهو بروتوكول غير موثوق-اتصال غير موجه، مسؤول عن إرسال الرسائل، لا يحوي برنامجا مسؤولاً عن التحقق من تسليم رزم البيانات. فائدة هذا البروتوكول هو سرعته

المنافذ Port

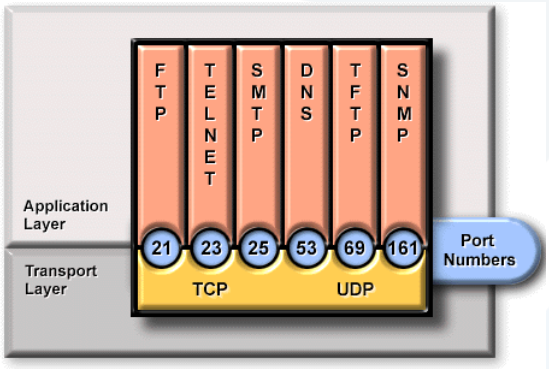
- تحتاج الأنظمة البعيدة للاتصال مع بعضها بغض النظر عن العتاد الكامن تحتها أو نظام التشغيل الذي تعمل عليه
- يسمح TCP/IP للأجهزة بأن تجد بعضها البعض باستخدام العناوين
- لكن بما أن كل جهاز معد للقيام بأكثر من وظيفة واحدة
  - ✓ لايكفي أن نرسل الحزم إلى جهاز محدد وننتظر منه أن يعرف بنفسه ماذا يفعل بها
  - ✓ يجب أن نعطي الجهاز الهدف تلميحاً عن الغرض من الحزمة وذلك ضمن الحزمة نفسها لكي يعرف ماذا يريد أن يفعل المستخدم
- يتم استخدام رقم من قبل البرنامج في UDP/TCP لإيصال البيانات إلى التطبيق المناسب

المنافذ Port



المنافذ Port

- تعتمد الطريقة التي يقدم بها التلميح بإعطاء أرقام منافذ مخصصة لمهام معينة مثل: إرسال البريد الالكتروني، بحيث يتم تحديد رقم المنفذ ضمن الحزمة مع عنوان الوجهة للنظام البعيد



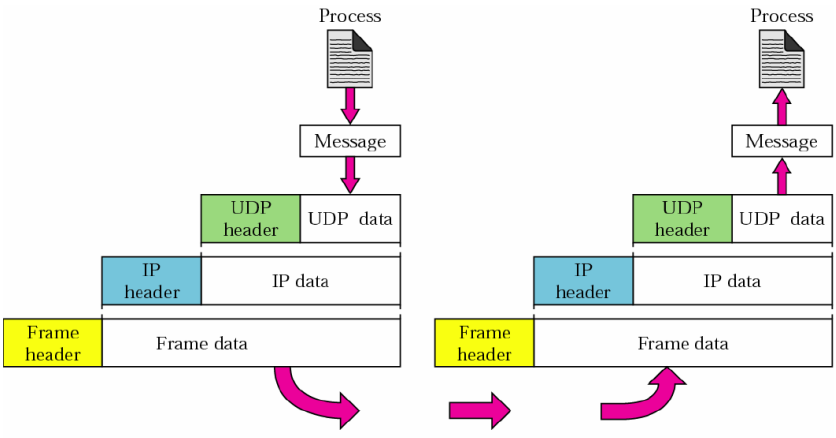
- وهو مايسمى بالمقبس: *Socket: {address, port}*
- في هذا النموذج، يتوافق المستقبلون على انتظار المعطيات على المنافذ المخصصة لها

المنافذ Port

المنفذ	البروتوكول	الخدمة	المنفذ	البروتوكول	الخدمة
21	TCP	FTP/control	464	TCP/UDP	Kerberos
22	TCP	SSH	465	TCP	SMTP over SSL/TLS (SMTPS)
23	TCP	Telnet	500	UDP	IPsec/IKE
25	TCP	SMTP	513	TCP	Rlogin
53	TCP/UDP	DNS	514	UDP	Syslog
67	UDP	DHCP/server	515	TCP	lpd/lpr
68	UDP	DHCP/client	520	UDP	UDP
69	UDP	TFTP	546	TCP/UDP	DHCPv6/client
80	TCP	HTTP	547	TCP/UDP	DHCPv6/server
110	TCP	POP3	563	TCP/UDP	NNTP over SSL/TLS (NNTPS)
119	TCP	NNTP	587	TCP	SMTP/submission
123	UDP	NTP	636	TCP/UDP	LDAP over SSL/TLS (LDAPS)
137	UDP	NetBIOS/name	691	TCP	Microsoft Exchange
138	UDP	NetBIOS/datagram	860	TCP	ISCSI
139	TCP	NETBIOS/session	873	TCP	Rsync
143	TCP	IMAP	902	TCP/UDP	VMware Server
161	UDP	SNMP/agent	989	TCP	FTP over SSL/TLS for data
162	UDP	SNMP/manager	990	TCP	FTP over SSL/TLS for control
179	TCP	BGP	992	TCP/UDP	Telnet over SSL/TLS
201	TCP/UDP	Appletalk	993	TCP	IMAP over SSL/TLS (IMAPS)
389	TCP/UDP	LDAP	995	TCP/UDP	POP3 over SSL/TLS (POP3S)

المنافذ Port

The Encapsulation Process



Port Discovery

- Use well-publicized ports for different services
  - DNS uses to port 53
  - Email uses port 25
  - HTTP uses port 80

- Use one port as a "port-mapper" service
  - Call 411 to learn the port of any other process
  - Allows for dynamic allocation of ports to different services
  - Allows for the assignment of ports to newly created services

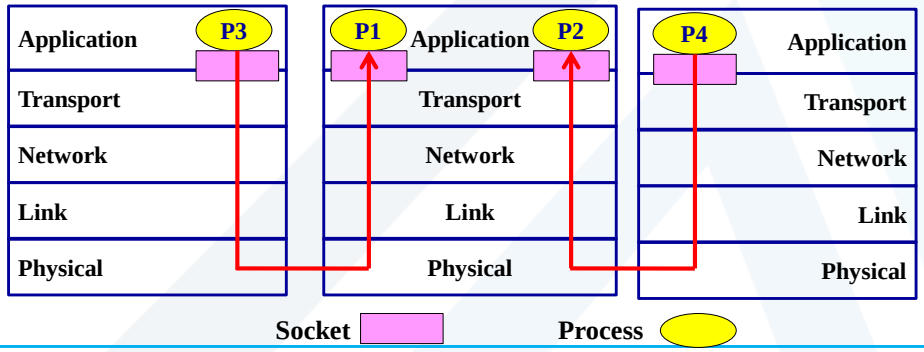
Multiplexing/demultiplexing

Recall: *segment* - unit of data exchanged between transport layer entities

- TPDU: transport protocol data unit

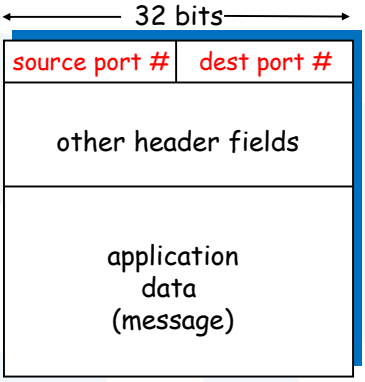
Multiplexing at send host
جمع المعطيات من عدة Sockets، تغليفها مع الترويسة (التي ستستخدم لاحقاً لفك التجميع)

Demultiplexing at rcv host:
تسليم مفاطع البيانات المستقبلة إلى الـ Socket المناسبة
(عملية طبقة التطبيقات الموافقة correct app layer processes)



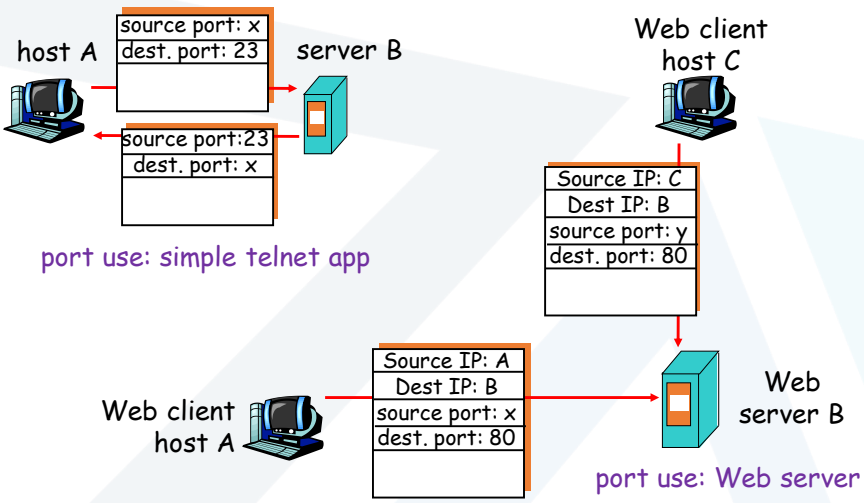
Multiplexing/demultiplexing

- تعتمد على أرقام منافذ المنبع والمستقبل وعناوين IP الخاصة بهم sender, receiver Port numbers, IP addresses
- عندما يستقبل المضيف IP datagrams:
  - تحوي كل datagrams على عنوان IP لكل من المصدر والمستقبل
  - تحمل كل datagrams مقطع طبقة نقل واحد 1 transport-layer segment
  - يحوي كل مقطع أرقام منافذ المصدر والهدف (والتي تكون معروفة بشكل واضح من أجل التطبيق الخاص)
  - يستخدم المضيف عنوان IP وأرقام المنافذ لإرسال المقاطع مباشرةً إلى المقابس الموافقة



TCP/UDP segment format

Multiplexing/demultiplexing



UDP: User Datagram Protocol [RFC 768]

UDP: User Datagram Protocol [RFC 768]

- ماهو سبب وجود UDP؟
  - ✓ عدم بناء الاتصال (والذي يمكن أن يسبب زيادة التأخير): حيث أنه يعتمد طريقةً لإرسال رزم بيانات IP مغلفةً وإرسالها دون الاضطرار إلى إنشاء وصلة
  - ✓ بسيط: لا يوجد حالة اتصال عند المرسل، المستقبل
  - ✓ ترويسة صغيرة للمقطع small segment header
  - ✓ يتم استخدامه عادةً في تطبيقات الوسائط المتعددة streaming multimedia

➢ ينقل UDP مقاطع مؤلفة من ترويسة بطول 8 bytes متبوعةً بالحمولة الصافية

Source Port	Destination Port
2 bytes	2 bytes
UDP Length	**UDP Checksum**
2 bytes	2 bytes

➢ عند وصول طرد UDP، يتم تسليم حمولته الصافية إلى الجزئية البرمجية المرتبطة إلى المنفذ الهدف. حيث أنه بدون حقول هذه المنافذ، لا تعرف طبقة النقل ماتفعله بالطرد

➢ نحن بحاجة إلى منفذ المصدر بشكل أساسي من أجل رد يجب أن يرسل إلى المصدر

➢ من أهم البروتوكولات التي تستخدم UDP هو البروتوكول RTP: Real-Time Transport Protocol

UDP: User Datagram Protocol [RFC 768]

➢ لكن:

✓ لايوجد تفحص للبيانات بين المرسل والمستقبل

✓ لايوجد تحكم بالازدحام (no congestion control): لذا يمكن أن يتجه بعيداً أسرع من المرغوب به away as fast as desired

✓ يوجد ضياع lost

✓ يتم تسليم البيانات بدون تنسيق إلى التطبيق

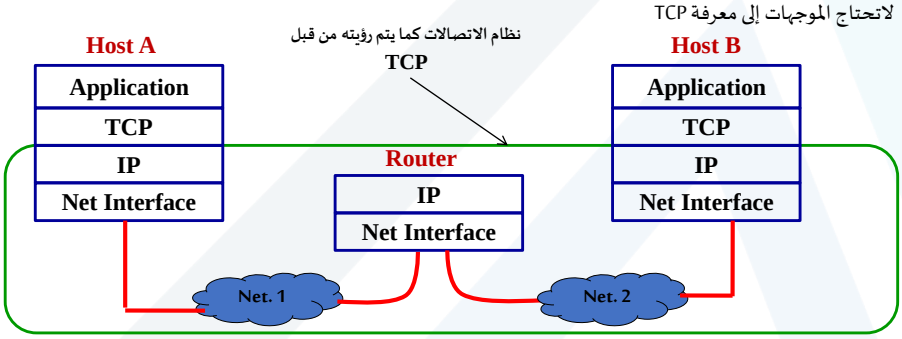
Fragmentation in UDP

- بشكل بسيط، يتم تقسيم رسالة UDP الكبيرة إلى عدة وحدات بيانات IP، بحيث تحوي كل منها رقماً متسلسلاً
- يتم تسجيل البت "fragmented" If one في ترويسة رسالة
- في حالة ضياع جزء من رسالة UDP، يتم إهمال الرزمة كاملةً
- كما يتم إهمال الرزمة في حالة فشل تفحص الرسالة

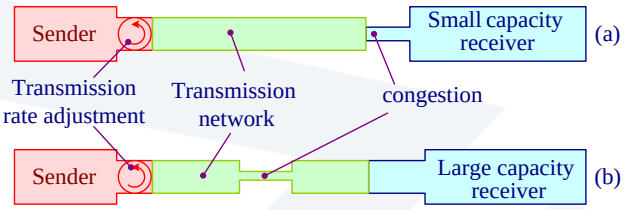
TCP (Transmission Control Protocol)

TCP

- يسمى خدمة نهاية-إلى-نهاية end-to-end على اعتبار أنه يضمن الاتصال بين التطبيقات على كمبيوترات مختلفة (نهايات الطريق)، حيث تحتاج العقد النهائية endpoints فقط إلى برنامج TCP
- تسمى وصلات TCP افتراضية virtual على اعتبار أنها تبنى كاملةً من قبل البرنامج
- يتم تغليف رسائل TCP في رزم IP وإرسالها عبر الشبكة. ينظر TCP إلى IP كنظام إرسال الرزم packet delivery system، بينما يعالج IP رسائل TCP كمعطيات يجب تسليمهاdata to be delivered
- لاتحتاج الموجهات إلى معرفة TCP



TCP congestion control

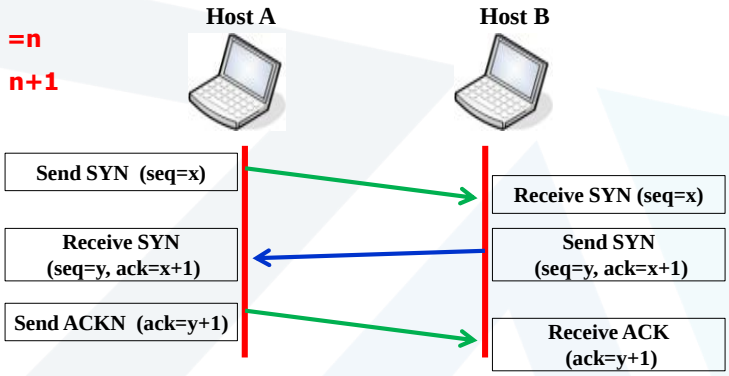


- الازدحام هو الحالة عندما يتواجد عدد كبير جداً من رزم البيانات في جزء من الشبكة الجزئية، مسببةً تدمير أداء الشبكة
- يمكن أن يحدث الازدحام بسبب:
  - فيضان الذاكرة المؤقتة لطرف المستخدم .buffer overflow at the receiving end (receiver capacity) (a)
  - ازدحام داخلي ضمن الشبكة .internal congestion within the network (network capacity) (b)
- يحتفظ كل مرسل بنافذتين:
  - the window the receiver has granted
  - the congestion window
- النافذة الفعلية هي أدنى مايعتبرها المرسل بأنها صحيحة ومايعتبرها المستقبل بأنها صحيحة The effective window is the minimum of what the sender thinks is all right and what the receiver thinks is all right

The TCP Three-way Handshake/Open Connection

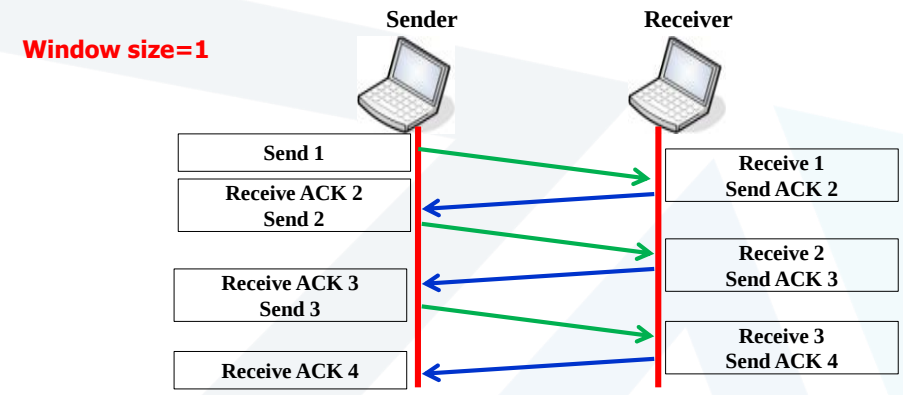
Host A -- seq =n

Host B -- seq= n+1



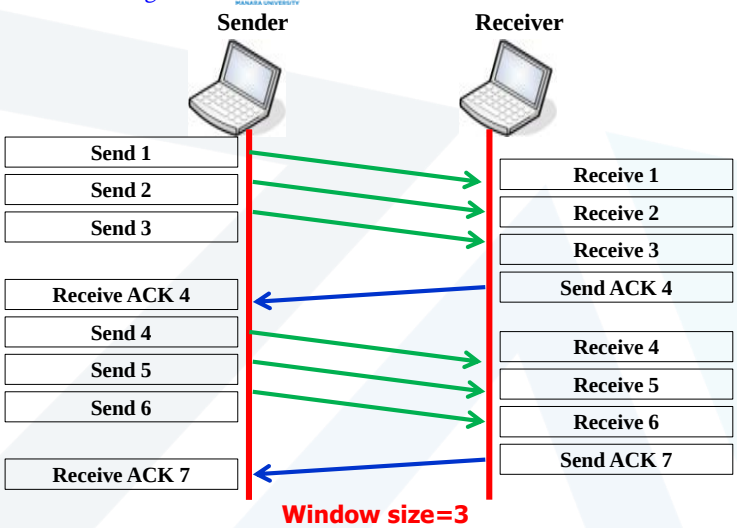
يتم مزامنة كلا طرفي اتصال ما مع تسلسل اتصال بثلاثة طرق فتح/تفحص three-way handshake/open connection sequence. يؤكد تبادل أرقام التسلسل بأنه يمكن تغطية فقدان المعطيات إذا حدثت مشكلة ما خلال الاتصال

The TCP Simple Acknowledgement



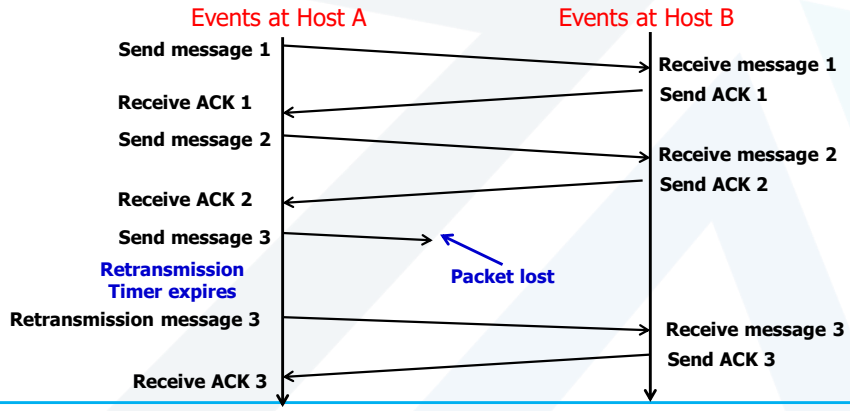
- يحدد حجم النافذة: ما هو حجم المعطيات الذي يستطيع المستقبل استقباله في المرة الواحدة one time
- مع حجم نافذة=1، كل مقطع تقوم بإرساله، يجب أن تحصل على إفادة باستلامه قبل أن ترسل المقطع التالي
- لكن هذه الطريقة هي عبارة عن استعمال غير فعال لعرض حزمة هؤلاء المستخدمين

The TCP Simple Acknowledgement



الوثوقية: إعادة الإرسال Retransmission

- التقنية الأساسية/الأولية لضمان الوثوقية هي إعادة الإرسال:
  - عندما يتم إرسال البيانات، يتم تشغيل مؤقت timer
  - عندما يستقبل الهدف البيانات، فإنه يرسل إفادة بالاستلام إلى المصدر
  - إذا انتهى زمن مؤقت المصدر قبل وصول إفادة الاستلام، يعيد المصدر إرسال البيانات



رسالة TCP

Source Port 2 bytes			Destination Port 2 bytes
Sequence Number 4 bytes			
Acknowledgement Number 4 bytes			
HLEN 4 bits	Reserved 6 bits	Code bits 6 bits	Window 2 bytes
Checksum 2 bytes			Urgent Pointer 2 bytes
Options 0 or 4 bytes			
Data			

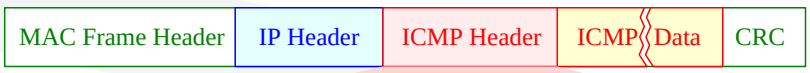
- ***Source Port***: the number of the calling port
- **Destination *Port*** : the number of the called port
- ***Sequence Number***: the number used to ensure correct sequencing of the arriving data
- ***Acknowledgment Number*** : the next expected TCP octet
- ***HLEN***: the number of 32-bit words in the header
- ***Reserved*** : set to 0
- ***Code bits*** : the control functions (e.g. setup and termination of a session)
- ***Window***: the number of octets that the sender is willing to accept
- ***Checksum*** : the calculated checksum of the header and data fields
- ***Urgent Pointer*** : indicates the end of the urgent data
- ***Option*** : one currently defined: maximum TCP segment size
- ***Data***: upper-layer protocol data

ICMP (Internet Control Message Protocol)

Internet Control Message Protocol (ICMP)

- هو بروتوكول خدمة service protocol ويعد جزءاً من البروتوكول IP
- يؤشر على الأحداث غير العادية في الشبكة
- تكون رزمة بيانات ICMP مغلفة ضمن الـ IP datagram
- تسمح بالتحكم بتدفق البيانات وباكتشاف الأخطاء
- يدعم بسهولة الاتصال مع منبع ما في حالة وجود مشكلة
- كما يدعم تقنية/آلية لتحديد فيما إذا لم يتم الوصول إلى الهدف
- يفحص الشبكات الوسطية على طول الطريق إلى الهدف
- تعتبر رسالة PING هي رسالة ICMP والتي تحاول معرفة توضع المحطات الأخرى على الانترنت ورؤية إن كانت فعالة ومعرفة إن كان هناك طريق باتجاهها

ICMP v4 Packet format and encapsulation

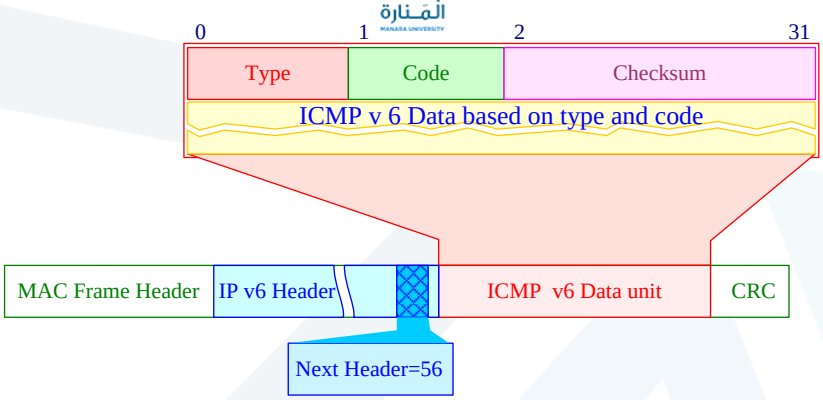


❖Message Type indicates which ICMP message is present

❖Message Code qualifies this for meaning specific to the type of message

ICMP is a TCP/IP network layer protocol used by routers and TCP/IP hosts for building and maintaining routing tables, adjusting data flow rates, and reporting errors and control messages for TCP/IP network communication

ICMP Version 6 Protocol



ICMP redirects can modify a router's routing table, so sometimes hackers try to subvert routers by issuing forged ICMP redirects in order to perform a denial of service attack.

Types of ICMP Messages

- Many ICMP messages types exist, each with its own format.
- A Selection:

Type Field:	Message Type:
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (Change Route)
8	Echo Request
11	Time Exceeded
12	Parameter Problem in Datagram
13	Timestamp Request
17	Address Mask Request

Types of ICMP Messages

- ICMP messages are either **query messages** or **error messages**.
- ***ICMP query messages:***
  - Echo request / Echo reply
  - Router advertisement / Router solicitation
  - Timestamp request / Timestamp reply
  - Address mask request / Address mask reply
- ***ICMP error messages:***
  - Host unreachable
  - Source quench
  - Time exceeded
  - Parameter problem

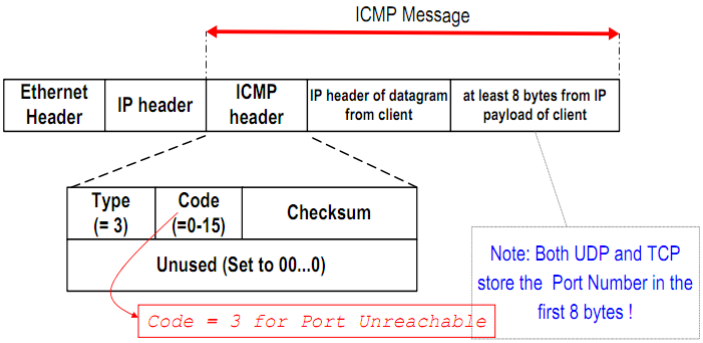
Example of an Error Message: Port Unreachable

- There are 16 different ICMP error messages ('codes') of type "Destination Unreachable"(Type = 3)

Code:	Message Type:	Code:	Message Type:
0	Network unreachable	9	Destination network administratively prohibited
1	Host unreachable	10	Destination host administratively prohibited
2	Protocol unreachable	11	Network unreachable for TOS
3	**Port unreachable**	12	Host unreachable for TOS
4	Fragmentation needed but bit not set	13	Communication administratively prohibited by filtering
5	Source route failed	14	host precedence violation
6	Destination network unknown	15	precedence cutoff in effect
7	Destination node unknown		
8	Source host isolated		

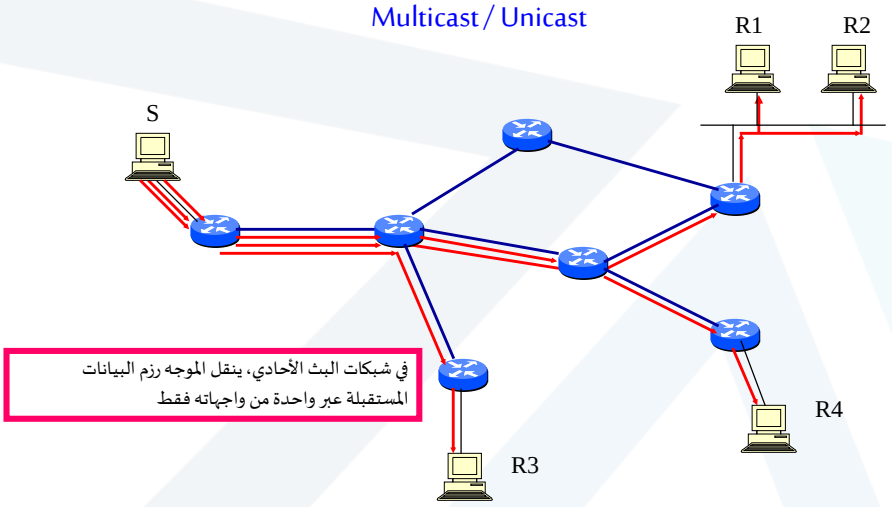
Example of an Error Message: Port Unreachable

⌘Format of the Port Unreachable Message



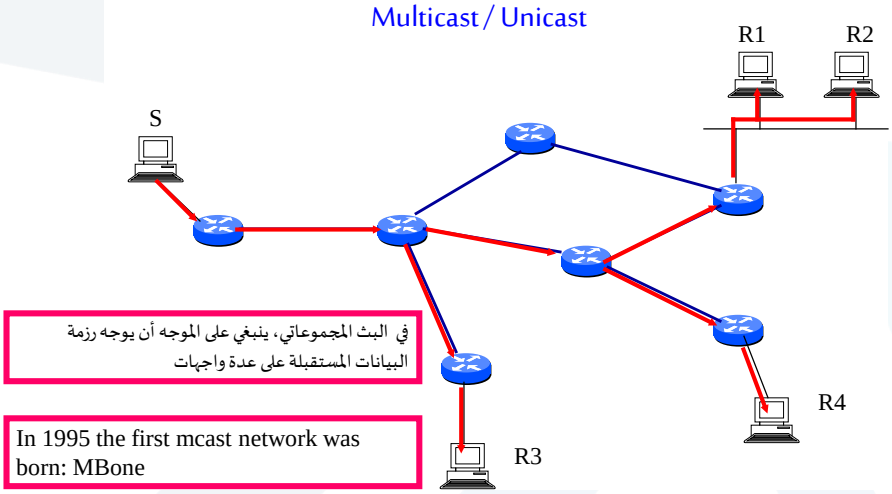
IP Multicast

Multicast / Unicast



في شبكات البث الأحادي، ينقل الموجه رزم البيانات المستقبلة عبر واحدة من واجهاته فقط

Multicast / Unicast



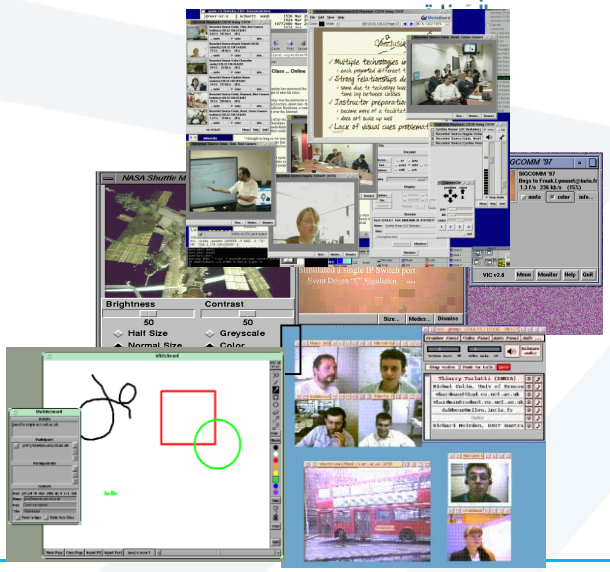
في البث المجموعاتي، ينبغي على الموجه أن يوجه رزمة البيانات المستقبلة على عدة واجهات

In 1995 the first mcast network was born: MBone

لماذا شبكات البث المجموعاتي

- استثمار عرض الحزمة بطريقة فعالة
- منع حصول التزاحم في الشبكة
- تخفيض الحمل عن السيرفرات
- منع وصول نسخ مكررة إلى المستخدمين

تطبيقات شبكات البث المجموعاتي



- ✓ بث الملتيميديا
- ✓ الفيديو كونفرنس
- ✓ التعليم عن بعد
- ✓ تطبيقات شركات .مستخدمين
- ✓ فيديو على الطلب
- ✓ الألعاب التفاعلية الموزعة

....

العناوين في شبكات البث المجموعاتي (IP Multicast)

- تمتد العناوين بين 224.0.0.0 حتى 239.255.255.255
- يتم تعريف كل مجموعة في شبكات البث المجموعاتي بعنوان من الصنف D
  - ✓ يعرف كل عنوان من الصنف D مجموعة من المحطات
  - ✓ في العنوان من الصنف D، هناك 28 بت متاحة لتعريف المجموعات
    - من الممكن تواجد أكثر من 250 مليون مجموعة في وقت واحد

العناوين في شبكات البث المجموعاتي (IP Multicast)

- العناوين المحجوزة من قبل IANA(Internet Assigned Numbers Authority (http://www.iana.org/assignments/multicast-addresses)
  - ✓ **224.0.0.0 – 224.0.0.255 Reserved for Routers and group management**
    - 224.0.0.1: جميع محطات شبكات البث المجموعاتي على شبكة محلية
    - 224.0.0.2: جميع موجهات شبكات البث المجموعاتي على شبكة محلية
    - 224.0.0.4: جميع موجهات DVMRP على شبكة محلية
    - 224.0.0.5: جميع موجهات OSPF على شبكة محلية
    - 224.0.0.6: Designated Router OSPF
    - 224.0.0.9: جميع موجهات RIP v2 على شبكة محلية
    - 224.0.0.13: جميع موجهات PIM على شبكة محلية
  - ✓ **239.0.0.0 – 239.255.255.255 Administratively scoped Applications**
    - 239.192.0.0 – 239.192.63.255 IPv4 Organizational Scope
    - 239.255.0.0 – 239.255.255.255 IPv4 Local Scope

العناوين في شبكات البث المجموعاتي (IP Multicast)

➢ العناوين المحجوزة من قبل IANA(Internet Assigned Numbers Authority
(http://www.iana.org/assignments/multicast-addresses)

✓ **224.0.1.0 – 238.255.255.255 Largely unreserved but some addresses have already been "bought"**

- 224.0.19.0 – 224.0.19.63 owned by Walt Disney

✓Addresses in the ranges 224.0.2.0 to 224.0.255.255, 224.3.0.0 to 224.4.255.255 and 233.252.0.0 to 233.255.255.255 are individually assigned by IANA and designated the AD-HOC block.

Multicast Packet Format

- Source is ALWAYS a unicast address
- Destination is a multicast group address
- Packet payload is typically UDP
- Need to map multicast group IP addresses to Layer 2 multicast MAC addresses
- Sender does NOT need to be a member of the group

➢ TTL value defines scope and limits distribution

✓ IP multicast packet must have TTL > interface TTL or it is discarded

✓ Values are: 0=host, 1=network, 32=same site, 64=same region, 128=same continent, 255=unrestricted

Multicast Groups

- Groups may be of any size
- Group members may be located anywhere in the Internet
- Hosts can join and leave groups at will
- There is no list of group members

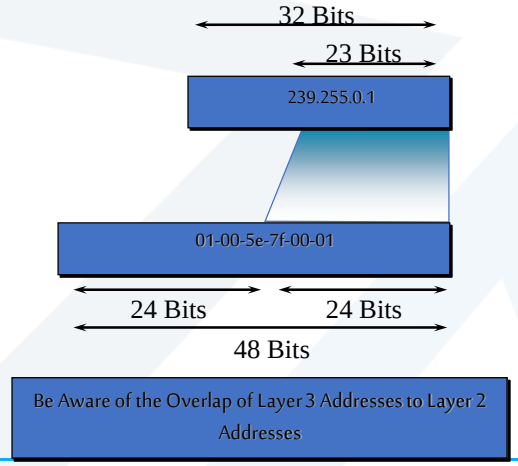
➢ A sender cannot tell who (or if anyone) received any message

➢ Hosts can always send and receive locally generated multicast packets by themselves

➢ To receive multicast packets from the outside, a multicast router must be present

Layer 2 Multicast Addressing—(Ethernet)

A Layer 3 IPmc Address Maps to a Layer 2 Multicast Address:



Ethernet Multicast Addressing

- IANA has defined that all Ethernet multicast addresses always begin with the hex values 01 00 5E in the first three bytes

➢ **The next bit of the address is 0**

➢ That takes car of **25 of the 48 bits** in the Ethernet MAC address

➢ The remaining **23 bits** are derived from the lowest order 23 bits from the IP multicast address

➢ Here is an example of how this multicast-addressing scheme works. For the multicast address 224.0.1.1, the resulting Ethernet MAC address is derived as follows:

224.0.1.12=1110 0000.0**000 0000.0000 0001.0000 1100**

lowest 23 bits =000 0000.0000 0001.0000 1100

Ethernet MAC address =**01-00-5E-0**000 0000.0000 0001.0000 1100

= 01-00-5E-00-01-0C

Ethernet Multicast Addressing

IP address 32 bits			
224	65	10	154
1110 0000	0100 0001	0000 1010	1001 1010
E 0	4 1	0 A	9 A

Ethernet MAC address 48 bits					
01	00	5E	00	00	00
0000 0001	0000 0000	0101 1110	0000 0000	0000 0000	0000 0000

Result Ethernet MAC address 48 bits					
0000 0001	0000 0000	0101 1110	**0**100 0001	0000 1010	1001 1010
01	00	5E	41	0A	9A

Ethernet Multicast Addressing

- Note that because 23 bits of 32-IP multicast address are mapped to a MAC multicast address, a chance exists that two different IP multicast groups can have the same multicast MAC address
- For example, map the following IP multicast addresses to multicast MAC addresses: 224.1.1.1 and 225.1.1.1

224.1.1.1=1110 0000.0**000 0001.0000 0001.0000 0001**

Ethernet MAC address =**01-00-5E-0**000 0001.0000 0001.0000 0001

= 01-00-5E-01-01-01

225.1.1.1=1110 0001.0**000 0001.0000 0001.0000 0001**

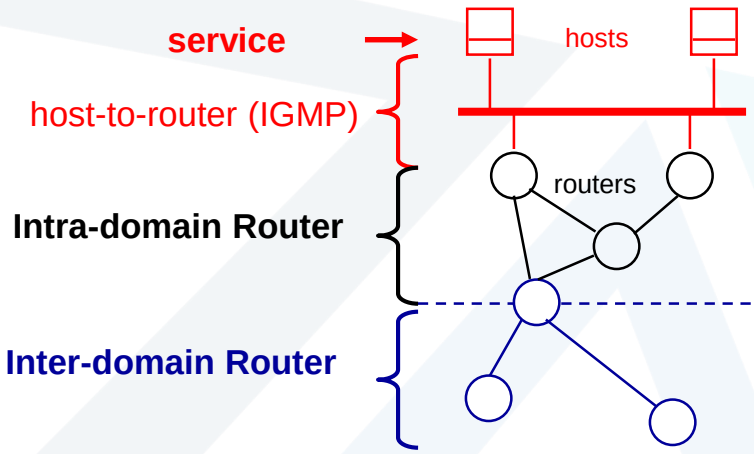
Ethernet MAC address =**01-00-5E-0**000 0001.0000 0001.0000 0001

= 01-00-5E-01-01-01

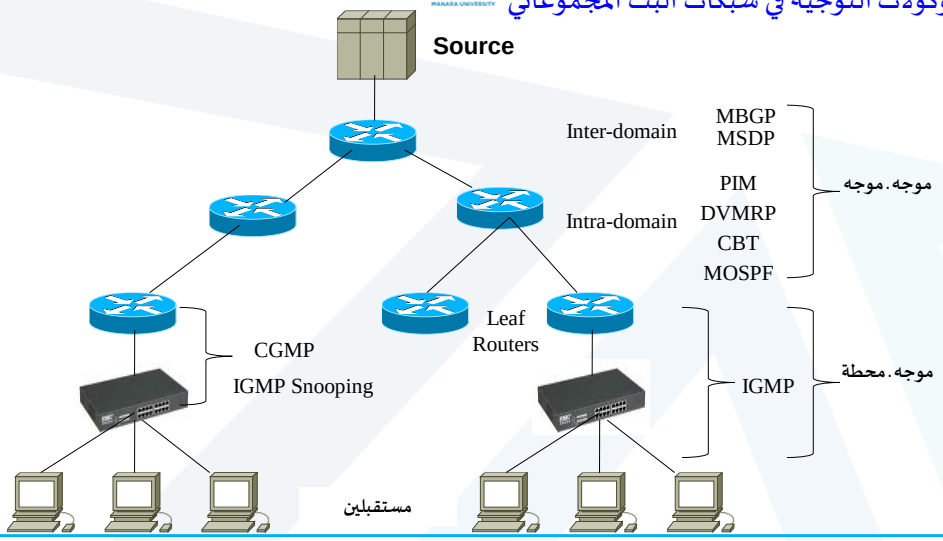
- Both of the MAC addresses are identical for different IP multicast addresses:

Note that applications typically use UDP port numbers in multicasting to distinguish what stream belongs to particular application on a host. A host would not be able to distinguish two multicast streams with identical destination MAC addresses and identical UDP port addresses. Fortunately, this is an unlikely case.

بنية شبكات البث المجموعاتي



بروتوكولات التوجيه في شبكات البث المجموعاتي



بروتوكولات التوجيه في شبكات البث المجموعاتي

بروتوكولات التوجيه في شبكات البث المجموعاتي

Dense-Mode: [DVMRP, MOSPF, PIM-DM…]

شجرة حسب المصدر، الغمر والانتقاء

Spars-Mode: [CBT, PIM-SM, …]

شجرة مشتركة، انضمام مباشر

Inter-Domaine: [MBGP, MSDP, …]

إدارة المجموعة في شبكات البث المجموعاتي

- **Adressage**: SDR, MASC, …
- **Join/Leave**: IGMP,MLD
- **…**

IGMP : Internet Group Management Protocol

IGMP: Internet Group Management Protocol

- بروتوكول لنقل المعلومات إلى المجموعة
- بروتوكول تفاعلي بين الموجه(ات) والمستخدمين لشبكات البث المجموعاتي في LAN
- يسمح لمستخدم أن يشترك (أو يلغي اشتراكه) في المجموعة، ويطلب من الموجه:
  - "أرسل لي نسخة من رزم البيانات لعنوان هذه المجموعة d.d.d.d"
- يوجد ثلاث إصدارات من هذا البروتوكول:
  - IGMP v1: RFC 1112 (1989)
  - IGMP v2: draft-ietf-idmr-igmp-v2-06.txt
  - IGMP v3: draft-cain-igmp-00.txt

IGMP: طريقة العمل

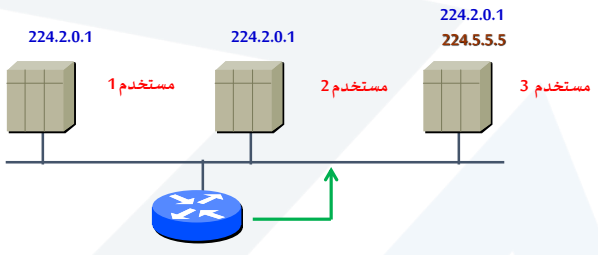
- يرسل الموجه نداء "query" كل 60(120) ثانية على العنوان 224.0.0.1 @ مع TTL=1

"إلى أي مجموعة تريد الانضمام؟"

وينتظر الإجابات

- يتم اختيار موجه واحد في شبكة الـLAN لإرسال النداءات
- يجيب المستخدم أو المضيف من خلال رسالة "REPORT" بحيث يدل على المجموعة أو المجموعات التي تهمه
- إذا لم يتلقى الموجه أي إجابة من أجل مجموعة معينة، فإنه يوقف إرسال الرزم إلى هذه المجموعة

IGMP: الانضمام إلى المجموعة



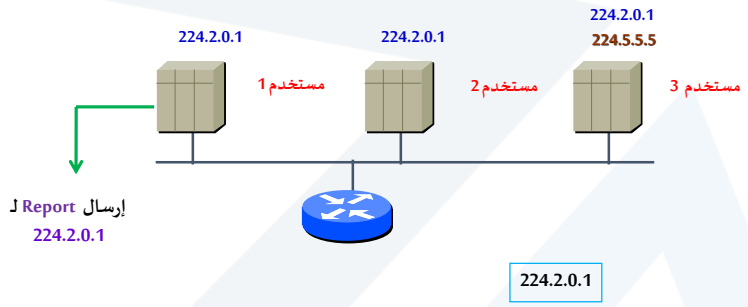
IGMP: حالة وجود موجه واحد في الشبكة المحلية

- عندما يستقبل المستخدم نداء الـ query :
  - يقوم بتأخير إجابته لمدة عشوائية
    - ليتفادى وصول كل الإجابات بنفس الوقت

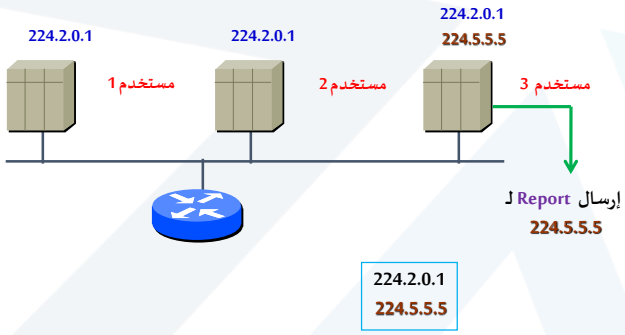
- عندما يجيب أحد المستخدمين:
  - المستخدمين الآخرين ليسوا بحاجة للإجابة
  - الموجه بحاجة لمعرفة إذا كان هناك على الأقل مستخدم موجود في هذه المجموعة

==> تكفي إجابة واحدة لكل مجموعة أو لكل شبكة محلية

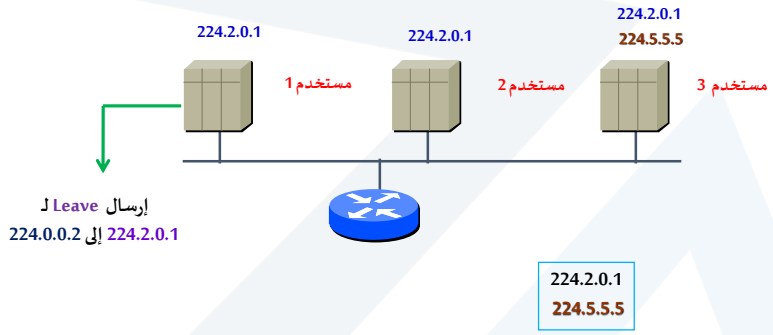
IGMP: الانضمام إلى المجموعة



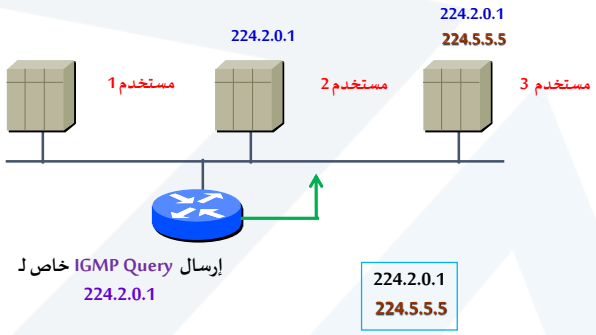
IGMP: الانضمام إلى المجموعة



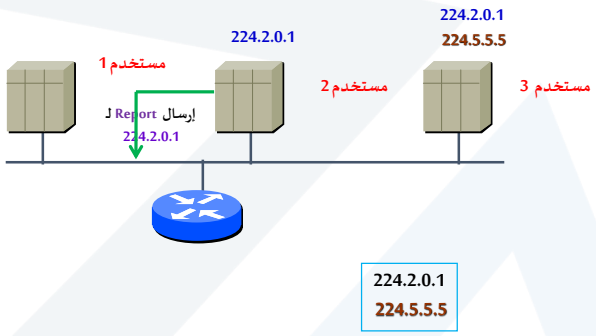
IGMP: مغادرة المجموعة



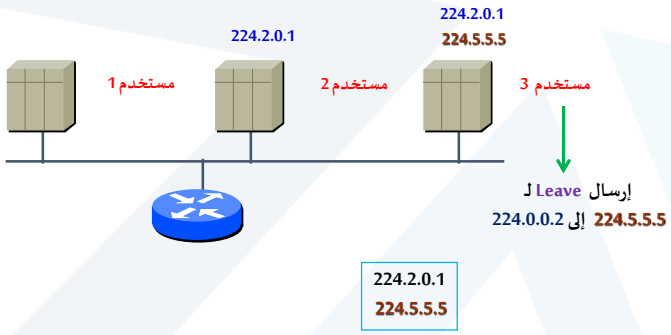
IGMP: مغادرة المجموعة



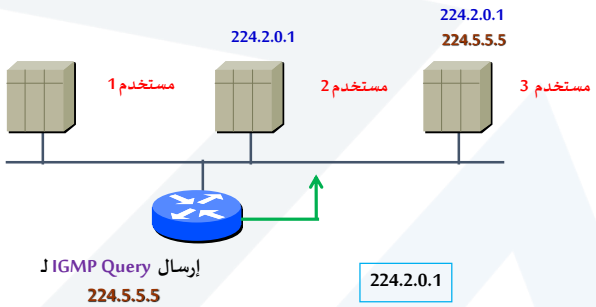
IGMP: الانضمام إلى المجموعة



IGMP: مغادرة المجموعة



IGMP: مغادرة المجموعة



IGMP: عدة موجهات في الشبكة المحلية

- يتم انتخاب موجه واحد من بين هذه الموجهات ليكون:

Designated Router, Dominant Router (DR)

- الموجه المختار هو المسؤول عن إرسال IGMP Query
  - في الإصدار الأول V1: طريقة الانتخاب أو الاختيار هي من وظيفة موجهات البث المجموعاتي ولا تتبع لـ IGMP
  - في الإصدار الثاني V2: الموجه المنتخب (DR) هو الموجه ذو العنوان IP@ الأصغر
- الموجه المنتخب ليس بالضرورة أن يكون الموجه المسؤول عن إرسال رزم البيانات

IGMP

يوجد ثلاث إصدارات من هذا البروتوكول:

- IGMPv1 : Query and Report
- IGMPv2 : Query, Report and Leave
- IGMPv3: حيث يتم الأخذ بالحسبان التسجيل في المجموعة من قبل مصدر أو عدة مصادر خاصة (الترشيح)

البروتوكول IGMP v1: شكل رزمة البيانات

Version 4 bits	Type 4 bits	Unused 8 bits	Checksum 16 bits
Group Address 32 bits			

- ***Version Field: 4 bits that is always 1.***
- ***Type : 4 bits***
  - ✓ ***Value=1, Host Membership Query.***
  - ✓ ***Value=2, Host Membership Report.***
- ***Unused : set to all zero.***
- ***Checksum (2 bytes): Complement of the entire IGMP v1message.***
- ***Group Address (4 bytes): This field is used for a Host Membership Report only. and it is set to all zeros if the packet is a Host Membership Query.***

IGMP

IGMP v2

- يرسل المضيف رسالة Leave Group إلى مجموعة كل الموجهات (224.0.0.2) إذا أراد ترك المجموعة وكان العضو الأخير فيها

✓ وهذا مايقلل من زمن انتظار المغادرة leave latency بالمقارنة مع v1، حيث أنه في v1، لا يوجد رسالة leave بل توجد الرسالتان query and report وبالتالي عند مغادرة جميع العقد علينا الانتظار حتى يرسل الموجه رسالة query وينتظر حتى وصول الإجابات من العقد، وعندها في حال عدم وصول أي إجابة، يوقف الإرسال باتجاه هذه المجموعة

- بعد استقباله لرسالة مغادرة من LAN، يقوم الموجه المسؤول بإرسال طلب Group-Specific Query إلى هذه الـLAN
- إذا لم تكن هناك أي Report كإجابة إلى رسالة الطلب، يتم حذف هذه المجموعة من قائمة الأعضاء المشتركين

<u>ملاحظة:</u> مع IGMP v1, v2 إذا أراد مضيف ما استقبال المعلومات من أي منبع من المجموعة، فسيتم نقل كل حركة البيانات من كل منابع المجموعة إلى هذه الشبكة الجزئية

البروتوكول IGMP v2: شكل رزمة البيانات

Type 8 bits	MaxRTime 8 bits	Checksum 16 bits
Group Address 32 bits		

- ***Type : 8 bits***
  - ✓ ***Value=0x11, Membership Query.***
  - ✓ ***Value=0x12, Version 1 Membership Report.***
  - ✓ ***Value=0x16, Version 2 Membership Report.***
  - ✓ ***Value=0x17, Leave Group.***
- ***Membership Query.***
  - ✓ ***General Query: is used to determine which groups have active members.***
  - ✓ ***Group-specific Query: is used to determine if a particular multicast group has active members***
- ***MaxRTime (8 bites): specifies the maximum amount of time a host can wait before responding to a Membership Query message. It is applicable only to Membership Query messages. The maximum response time is represented in tenth of seconds***

IGMP

IGMP v3

- يمكن لمضيف أن يختار استقبال البيانات من منابع محددة من مجموعة البث المجموعاتي
- تحدد inclusion Group-Source Report قائمة المنابع التي يريد المضيف استقبال البيانات منها
- تحدد exclusion Group-Source Report قائمة المنابع التي لايريد المضيف استقبال البيانات منها
- يطور IGMP v3 عملية دعم رسائل Leave-Group إلى دعم رسائل Group-Source Leave
  - ✓ يمكن لمضيف مغادرة مجموعة أو أن يحدد زوج Source-Group

يتم استخدام البروتوكول MLD(Multicast Listener Discovery) ,

بحيث: MLDv1=IGMPv2

MLDv2=IGMPv3