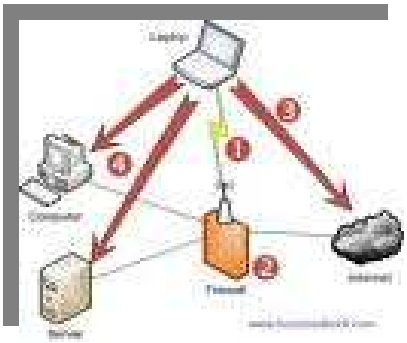
Router



عصام سرحان ذياب

ROUTER
ISSAM SERHAN DYIB

المسيّر أو الموجه، (بالإنجليزية: router)، هو جهاز للربط بين شبكتين أو أكثر ببعضهم وتتكون الشبكة العنكبوتية من آلاف مؤلفة من المسيرات والخواديم، يتكون من ٣ طبقات من نموذج التفتيش (OSI.) . يقوم المسير بتحديد الجدول وتحديد مسارات التحول من مجموعات بينية لأخرى. وينبغي عدم الخلط مع محول (طبقة ٢) وبوابة (طبقة ٣ أو أعلى).

تعريف مصطلحات الروتر

PPPOA , PPPOE, NAT, MTU , wireless , SSID , WEP , WPA, WPA2, IGMP

PPPOE

<!--[if !supportLists]--> <!--[endif]-->

<!--[if !supportLists]--> يعتمد ال **PPPOE** علي الشبكات من النوع **Frame Relay** الذي يقوم بتقسيم ال **Data** إلي **Frames** مختلفة في الحجم<!--[endif]-->

- وقد قامت ال ***Internet Engineering Task Force*** **(*IETF*)** (فريق عمل هندسة الانترنت) باعتماده واعطاءه رقم **RFC 2516** وهذا ما نجده في اعدادات روتر ال **Link sys**<!--[endif]-->

- تسمح باعادة ارسال ال **Data** التي حدث لها تشوه اثناء الارسال او لم تصل بطريقة صحيحة دون الحاجة الي ارسال ال **data** كلها مرة اخري مما يؤدي الي زيادة سرعة الارسال<!--[endif]-->

- تتميز ال **Ethernet** علي ال **ATM** في انه من السهل زياده حجم الشبكة وتوسيع انتشارها<!--[endif]-->

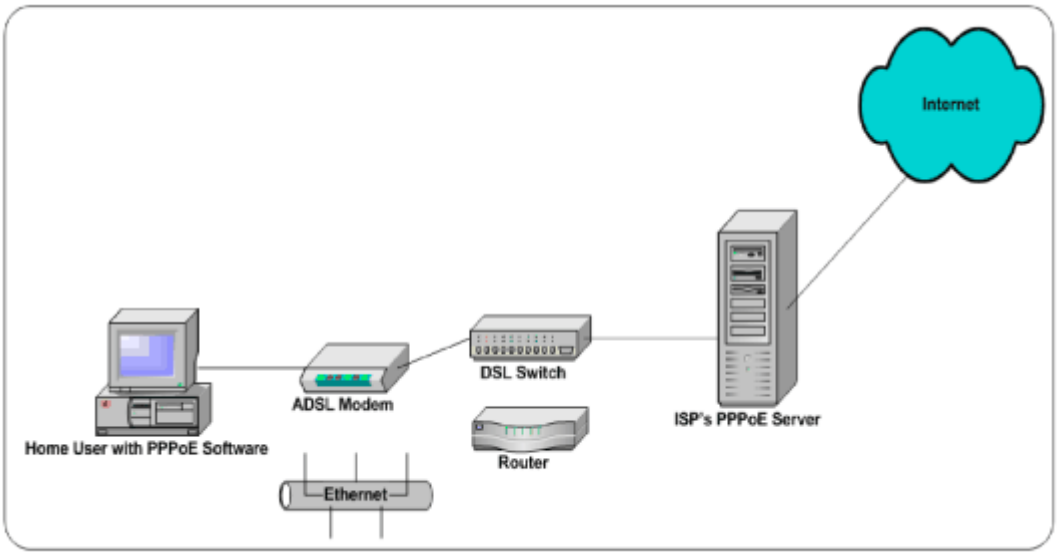
- الاجهزة الخاصة بال **Ethernet** اقل تكلفة من الاجهزة الخاصة بال **ATM**<!--[endif]-->

- تستطيع حمل سرعات عالية<!--[endif]-->

- تستخدم VCs واحده بين الروتر وال ISP وهذا يظهر في اختيارنا الدائم لل VCI ب ٣٥ مع جميع العملاء ، فال PPPOE لا تحتاج الي VCs مختلفة لكل session<!--[endif]-->

- توفر اتصال دائم وBandwidth مشترك لجميع العملاء بحيث يكون مناسب لنقل ال Voice وال Data بدون اي تاخير ، وهذا يتم عن طريق توزيع ال Bandwidth الكلي علي معظم المشتركين وليس كلهم علي اعتبار انه في الاحوال العادية لن يقوم جميع المستخدمين بالدخول علي الانترنت في نفس الوقت<!--[endif]-->

- لذلك فان ال PPPOE هو البروتوكول المناسب في ال LANs<!--[endif]-->



PPPOA

<!--[supportLists! if]--> <!--[endif]-->

<!--[supportLists! if]--> <!--[endif]-->يعتمد ال **PPPOA** علي شبكات ال **ATM** التي تقوم بتقسيم ال **Data** إلي اجزاء ثابته (**53 bytes**)الحجم تسمي **Cells**

- <!--[endif]-->تحتاج ال **PPPOA** إلي **Bandwidth** اكبر لكي تحمل نفس مقدار ال **Data** التي تحمله ال **Network** التي تستخدم **PPPOE** ، لان ال **Data** تكون مقسمة إلي اجزاء متساوية الحجم (**53 bytes**) وهذا الحجم صغير نسبيا بالمقارنة بحجم ال **Frame** في حاله ال **PPPOE**

- <!--[endif]-->ال **PPPOA** تحتاج الي **PVCs** و **SVC** حتي تستطيع ان تنقل ال **Data** ، كما انها تسمح بوجود اكثر من **VC** علي نفس ال **Line** حتي تستطيع تشغيل تطبيقات محتلفة مثل خدمة ال **IPTV** وغيرها

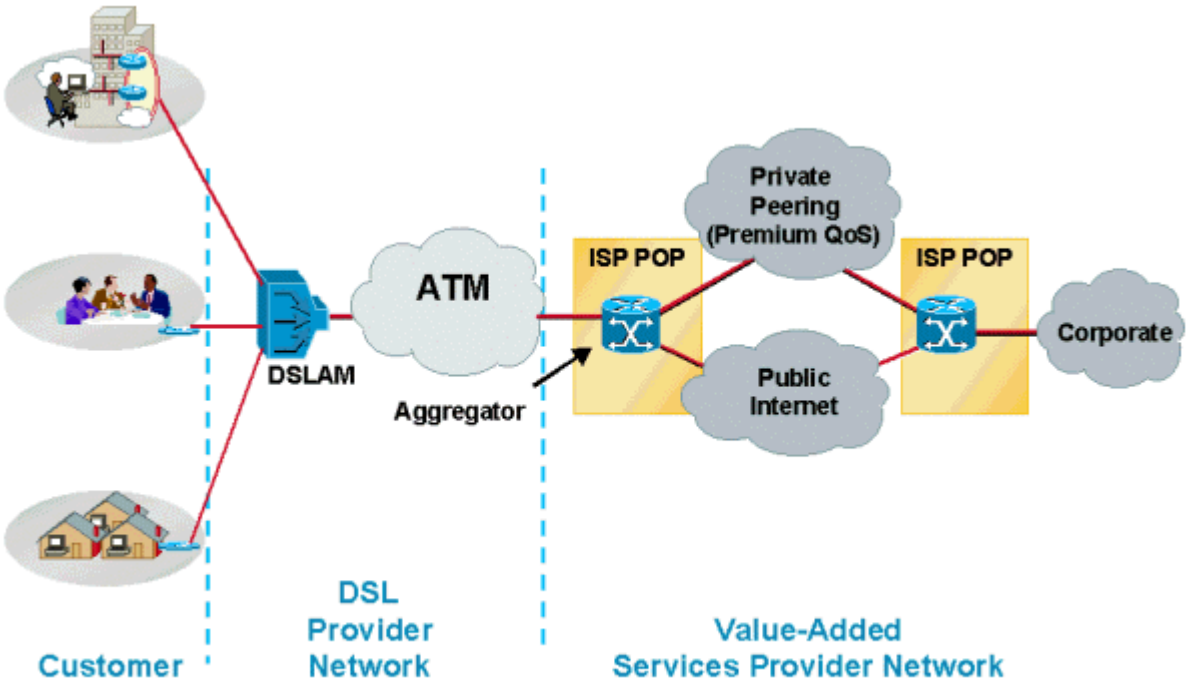
- <!--[endif]-->تتميز بسرعتها العالية في نقل ال **Data** كما توفر سرعات اعلي من ال **PPPOE** تصل إلي **10 Gbps**

- <!--[endif]-->تستطيع ايضا نقل ال **Data** وال **Voice** وال **Video**

- <!--[endif]-->تتميز ايضا بان لها **QOS** عالية وخاصة في التطبيقات التي تعتمد علي الوقت ولا تحتمل التأخير مثل ال فيديو والصوت وذلك لانها تعتمد علي **Bandwidth** كبير

- <!--[endif]-->تتطلب **Authentication** مثل ال **PPPOE** اي انه يمكن وضع **Username and Password**

ROUTER
ISSAM SERHAN DYIB



Bridging Mode

في الشبكات العادية يتم توصيل اجهزة الكمبيوتر بالروتر الذي يقوم بتوزيع ال IPs والتحكم في نقل ال data من وإلي الانترنت

بينما اذا تم توصيل روترين مع بعضهما البعض فيجب تفعيل خاصية ال bridge mode

يمكن استخدام ال bridge mode بطريقتين مختلفتين

في حاله التوصيل بالكابل:

<!--[if !supportLists]--><--[endif]--!> تستخدم ال Bridge mode مع ال ATM حيث تنتقل ال Data من خلال شبكات ال ATM

<!--[if !supportLists]--><--[endif]--!> هذه الشبكات تعتبر هي حلقة الوصل بين الروتر وال ISP

<!--[if !supportLists]--><--[endif]--!> يمكن لل ISP ان يختار من بين ان يعطي Static IP او Dynamic IP لل LAN

<!--[if !supportLists]--><--[endif]--!> واذا قام ال ISP باعطاء Dynamic IP لل network فيجب عليه تفعيل ال DHCP server

<!--[if !supportLists]--><--[endif]--!> وعند استخدام ال Bridging mode فيتم الغاء خاصية ال NAT

في حالة التوصيل بال wireless

<!--[supportLists! if]--><!--[endif]--><يستخدم هذا ال mode في حاله الرغبة في ربط اكثر من روتر بدون استخدام كابل لزيادة مدي ال Wireless

<!--[supportLists! if]--><!--[endif]--><ويشترط ان يكون الروترات والاجهزة المتصله بهم في نفس ال Subnet mask حتي يتم الاتصال بينهم

<!--[supportLists! if]--><!--[endif]--><وهذا ال Mode يقوم باغلاق ال NAT ويجعل الروتر يعمل ك DHCP Server فقط

<!--[supportLists! if]--><!--[endif]--><ولن يكون هناك اي اعدادات اضافية خاصه بال Authentication او نوع البروتوكول المستخدم الخ الخ عند تفعيل هذه الخاصية علي احد الروترات

<!--[supportLists! if]--><!--[endif]--><ولن يكون هناك ايضا اي Troubleshooting اضافية او معقده لهاذا الروتر

مميزات ال Bridging Mode

<!--[supportLists! if]-->١-<!--[endif]--><لا يحتاج الي configuration معقده

<!--[supportLists! if]-->٢-<!--[endif]--> <سهل التشغيل

<!--[supportLists! if]-->٣-<!--[endif]--><مناسب للاستخدام علي المستوي الشخصي في الاماكن الاكثر اتساعا

عيوب ال Bridge mode

<!--[if !supportLists]-->١- <!--[endif]-->تقل كفاءته كلما زاد عدد المستخدمين

<!--[if !supportLists]-->٢- <!--[endif]-->لا يوفر اي حماية لذلك يفضل استخدامه علي المستوي الشخصي فقط

<!--[if !supportLists]-->٣- <!--[endif]-->من السهل التقاط IP من الشبكة والدخول علي الانترنت

MER

تستخدم هذه التقنية في حالة ان ال NSP (Network Service Provider) لا يدعم الانترنت باستخدام ال IP فتقوم ال MER بعمل NATTING باستخدام ال MAC بدلا من ال IP وهي خاصية اكثر امانا more secure

بمعني انه عادة يقوم ال DSLAM يقوم باعطاء كل روتر متصل عليه WAN IP خاص للدخول علي الانترنت بينما في حالة ال NSP فهي تخصص IP واحد فقط لل DSLAM ويكون ال subnetmask هو 32/ لذلك يعتبر هذا ال IP هو ال WAN IP لجميع الروترات المتصلة علي هذا ال DSLAM ويقوم ال DSLAM بمعرفة ال data الخاصة بكل روتر عن طريق ال MAC address الخاص بالروتر ، لذلك فان خاصية ال MER تقوم بعمل NATTING باستخدام ال MAC بدلا من ال IP

وبصورة ابسط فان جميع الروترات المتصله علي ال DSALM تعتبر بمثابة اجهزة كمبيوترمتصله علي SWITCH

وال NSP هي الشركة التي تقدم خدمات ال Dial UP لل ISP وتكون بارقام معينه تمكن المستخدمين من الاتصال بال NSP

وهنا يصبح دور ال ISP هو دور تسويقي فقط ودعائي وليس فني ، حيث ان ال NSP هي التي تقوم بجميع العمليات الفنية من routing و maintaining ولكن يمكن ان تقوم ال ISP بتقديم خدمات ال web hosting وال e-mail

وعند عمل configuration للروتر باستخدام ال MER يجب ان يتم وضع WAN IP Address و WAN Subnet Mask وال VPI و ال VCI وال encapsulation mode: LLC/SNAP or VC Multiplexin وال Enable NAPT and Enable DHCP

و يجب ملاحظة الفرق بين ال :

ISP (Internet Service Provider)

فال ISP تقوم بتقديم خدمات الانترنت عن طريق ال IP وكأنها تعتبر ان كل روتر يمثل جزء من ال WAN

NSP (Network Service Provider)

اما ال NSP فهي تقوم بتقديم خدمات الانترنت عن طريق ال MAC وكأنها تعتبر أن جميع الروترات المتصله عبارة عن Local Network

IPOA

<!--[if !supportLists]--><-- <!--[endif]-->هي عملية ارسال ال **IP packets** باستخدام شبكة ال **ATM** وذلك باستخدام ال **VCI**

<!--[if !supportLists]--><-- <!--[endif]-->تحتاج ال **IPOA** إلي اجهزة خاصة لارسال ال **Data** حتي تتمكن من التعامل مع كل من ال **IP** وال **ATM network** ، حيث ان ال **IP** لا يعتمد علي نوع ال **Connection** بينما ال **ATM** تعتمد عليه

<!--[if !supportLists]--><-- <!--[endif]-->ال **IPOA** يدعم خاصية ال **QOS**

<!--[if !supportLists]--><-- <!--[endif]-->كما يقوم بتقيل ال **Traffic** مما يزيد من كفاءة الشبكة

Dial on Demand

<!--[if !supportLists]--><!--[endif]--> تعني **Dial on Demand** ال

الاتصال عند الطلب ، اي ان ال **Connection** تتم عندما يقوم ال **User** بمحاولة الدخول علي الانترنت

<!--[if !supportLists]--><!--[endif]--> عند بداية تصفح المستخدم

للانترنت يتم الاتصال والدخول علي الانترنت وبعد فترة من عدم استخدام الانترنت يتم قطع الاتصال ، وهذه الفترة من الممكن تغييرها

Dial on Demand

<!--[if !supportLists]--><!--[endif]--> تعني **Dial on Demand** ال

الاتصال عند الطلب ، اي ان ال **Connection** تتم عندما يقوم ال **User** بمحاولة الدخول علي الانترنت

<!--[if !supportLists]--><!--[endif]--> عند بداية تصفح المستخدم

للانترنت يتم الاتصال والدخول علي الانترنت وبعد فترة من عدم استخدام الانترنت يتم قطع الاتصال ، وهذه الفترة من الممكن تغييرها

NAT

<!--[if !supportLists]--><!--[endif]--> خاصية ال **NAT** تسمح بان يلعب الروتر دور الوسيط بين الشبكة الداخلية للمستخدمين والانترنت

<!--[if !supportLists]--><!--[endif]--> تقوم ال **NAT** بتحويل ال **Real IP** إلي **Private IP** والعكس

<!--[if !supportLists]--><!--[endif]--> في حالة وجود جهاز واحد فقط وعدم وجود شبكة داخلية فمن الممكن الغاء ال **NAT** حيث يحصل الكمبيوتر علي ال **Real IP address** مباشرة، وهذا يظهر في حاله ال **USB MODEM** الذي يعطي ال **Real IP** لجهاز الكمبيوتر مباشرة ، وللتأكد من ذلك يمكن ان تقوم بكتابه هذا الامر **ipconfig** في شاشة ال **DOS**

<u>وهناك استخدامات عديده لل NAT</u>

<!--[if !supportLists]-١-><!--[endif]--> تقليل عدد ال **Real IP** المستخدمة ، حيث انه بفرض عدم وجود هذه الخاصية فان كل جهاز سوف يحصل علي **Real IP** للدخول علي الانترنت مما يتطلب توفير عدد كبير من ال **Real IP** ، وعلي الرغم من استخدام هذه الخاصية فان ال **Real IP V4** لم تعد تكفي جميع المستخدمين لذلك تم تطوير ال **IP V4** الي **IP V6** الذي يوفر عدد اكبر من ال **Real IPs**

ملاحظة : عدد ال **IP** التي يوفرها **IPV4** هو **4,294,967,296** وعلي الرغم من استخدام ال **NAT** فان كل هذا العدد من ال **IPs** غير كافي

عدد ال IP التي يوفرها IPV6 هو

340,282,366,920,938,463,463,374,607,431,768,211,456

<!--[if !supportLists]-->٢-<!--[endif]-->يوفر امان اكثر للشبكة لان ال IP Private للشبكة يكون مختفي بينما جميع العمليات علي الانترنت تتم بال Real IP

<!--[if !supportLists]-->٣-<!--[endif]-->يوفر ادارة اعلي للشبكة

وهناك انواع مختلفة من ال NAT

Static NAT

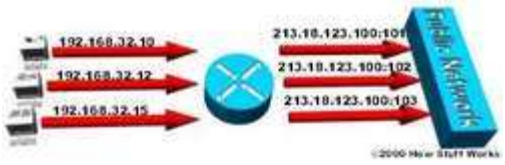
وهذا النوع من ال NAT يخصص لكل جهاز علي الشبكة الداخلية REAL IP خاص به، وهو يستخدم خاصة في حاله ان الشبكة تتكون من اجهزة سيرفرات او ايميل سيرفر

Dynamic NAT

يحتوي علي عدد معين من ال Real IP ثابته ومخصصه لل network فقط ويقوم باستخدامها جميع الاجهزة المتصله علي هذه ال network والتبديل بينها ، ولا يشترط ان يستخدم احد الاجهزة نفس ال IP في كل مرة وانما قد يستخدم IP اخر من المتاحين في ال Pool of Ips المخصصه له

PAR(Port address translation)/NAT overload

وهي الاكثر شهرة بين مستخدمي ال ADSL حيث يحصل الروتر علي Real IP مختلف في كل مرة بناء علي ال Real IP التي يوفرها ال ISP



MTU

<!--[supportLists! if]--><!--[endif]--> ال MTU هي اكبر حجم لل Packet يمكن ارسالها<!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> من المعروف ان اي data يتم ارسالها من جهاز الكمبيوتر علي الانترنت يتم تقسيمها اولا إلي packets وكل packet يكون لها حجم (يقاس بال byte) فاذا كان حجم ال packet اكبر من ال Maximum التي يتم تحديدها في الروتر في خانه ال MTU فان هذه ال packet يتم تقسيمها مرة اخري حتي تصبح مناسبة للارسال <!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> اذا كانت كمية ال data المرسلة كبيرة وكل ال packet اكبر من الحجم المحدد فيتم تقسيمها مرة اخري وهذا سوف يقلل من سرعة الارسال ويسبب بطئ في الشبكة <!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> يستطيع كل Administrator التحكم في ال MTU الخاصه بالشبكة المسئول عنها وتغييرها كما يشاء<!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> ولكن يجب ملاحظة انه يمكن تغيير قيمة ال MTU من ال OS اي نظام التشغيل ، ولكن اذا تم تغيير قيمتها بحيث تصبح اكبر من ال MAX فان ال Data سوف تفقد مما يؤدي الي بطئ الشبكة<!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> ال Default MTU في ال WIN XP تكون ١٤٨٠<!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> ال Default MTU في ال Dial UP تكون 576<!--[supportLists! if]--><!--[endif]-->

<!--[supportLists! if]--><!--[endif]--> ال Default MTU في ال PPPOE وال PPPOA تكون ١٤٩٢ ولذلك نجد ان هذه القيمة موجوده داخل الروتر by default لانها تستخدم مع اشهر البروتوكولات

وللتعرف علي ال MTU الصحيحة واللازمة لوضعها في ال Configuration نقوم باختيار قيم مختلفة لل MTU ونختبر هذه القيم حتي نصل إلي القيمة المناسبة

نذهب إلي ال DOS ونقوم بكتابة الامر

ping www.google.com -f -l xxxx

مع العلم بان XXXX هو قيمة ال MTU التي سوف نختبرها

وال l هي ال Small Letter لحرف ال L

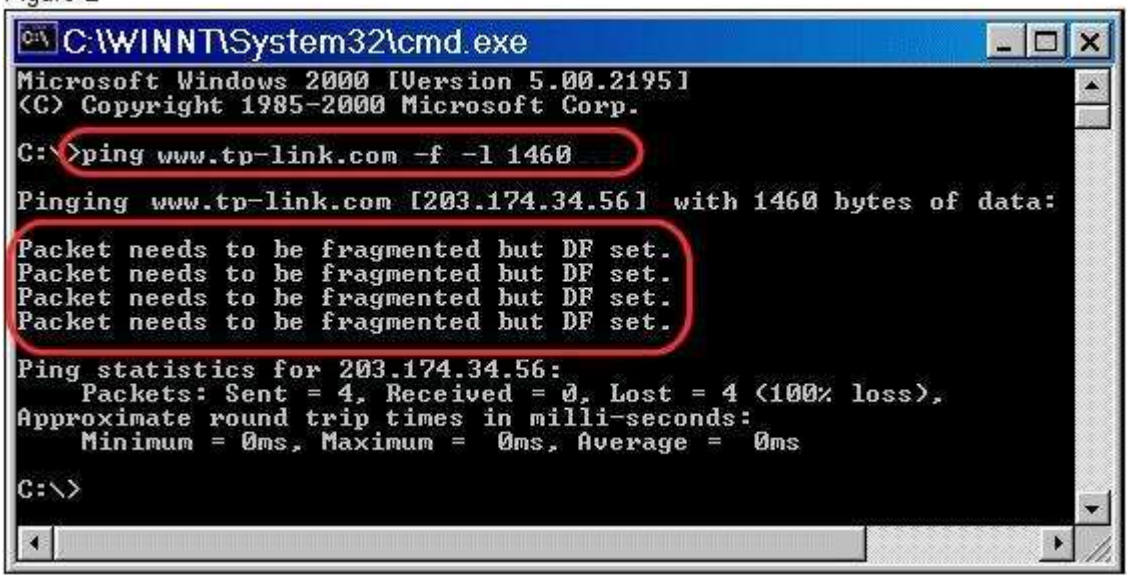
فاذا اعطي Reply فان قيمة ال MTU المختاره تعتبر قيمة مناسبة

فان هذه القيمة تكون Packet needs to be fragmented but DF setاما اذا اعطي رساله اكبر من اللازم

Figure 1

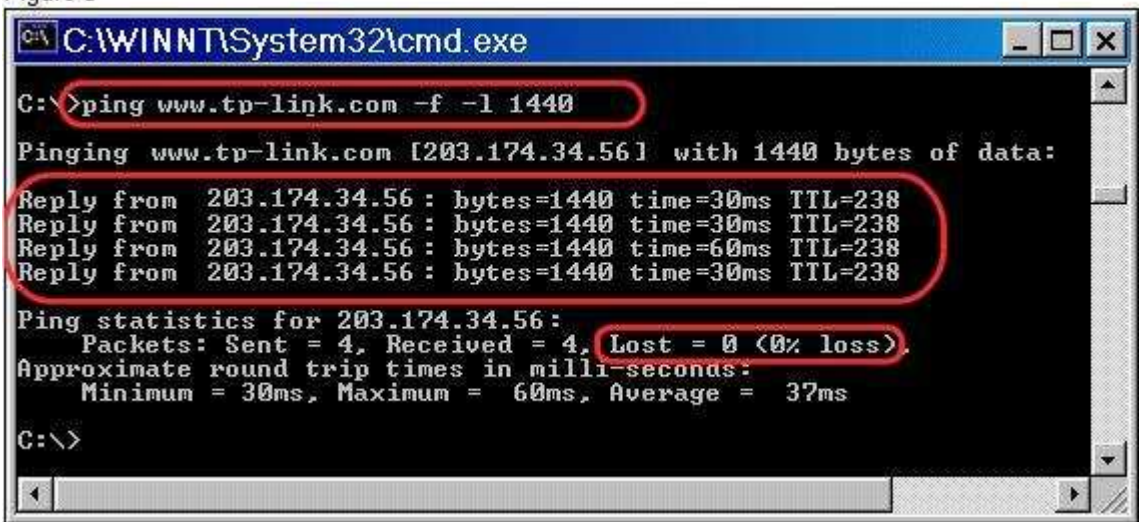
قيمة اكبر من القيمة المناسبة ان المستخدم قد قام بادخال هذه الصورة توضح

Figure 2



مازالت القيمة اكبر من القيمة المناسبة

Figure 3



نجد هنا ان المستخدم قد ادخل قيمة مناسبة

PVC

من المعروف ان ال adsl هي خدمة متاحة ٢٤ ساعه وليست مثل ال dial up ، فحتي اذا كان جهاز الكمبيوتر مغلق فإن الروتر يكون علي اتصال بالانترنت

ومعني هذا ان هناك channel مفتوحة دائما بين الروتر والانترنت (permanent) وهذه ال channel تسمي PVC وهي طبعا وهمية Virtual وليست كابلات Physical

وهذه ال channel لها حالتين :

١. الحالة الاولي هي التي يتم فيها ارسال واستقبال لل data وهي تسمي data transfer

٢. الحالة الثانية هي التي لا يتم فيها ارسال واستقبال لل data وتكون ال channel في حاله active اي انها نشطة ومستعدة لنقل ال data في اي وقت وهذه الحاله تسمي IDLE

مثل : ال DNS server والاتصال PPP او point to multipoint مثل الالعاب ال online

لذلك فهذه ال channel دائما مفتوحة ومخصصه لكل فرد علي حده حتي وان لم يستخدمها لذلك تسمي Permanent ولا تحتاج الي اتصال مبدأي كما في حالة ال dial up

وهذا عكس ال SVC's (Switched Virtual Circuits) الذي تفتح فيه ال channel فقط عند الرغبة في ارسال ال data وتغلق عند انتهاء الارسال لتذهب الي شخص اخر يقوم بعملية نقل data لذلك تسمي Switched

مثل ال email server وأي اتصال غير دائم للانترنت مثل ال Dial up وبعض الخدمات التي تحتاج الي العديد من ال VPI وال VCI

VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier)

<!--[if !supportLists]--><-- الطريق بين الروتر واجهزة ال ISP يسمي channel وهناك channels عديده يمكن تسير فيها ال Data للوصول من روتر لروتر اخر --><!--[endif]-->

<!--[if !supportLists]--><-- يتم تحديد ال channels الذي تسير فيها ال data عن طريق قيم معينه تسمي VCs وهي التي تقوم بتعريف ال data بال channels التي سوف تمر من خلاله حتي تصل للروتر التالي عن طريق قيم ال VPI --><!--[endif]-->

<!--[if !supportLists]--><-- ومجموعة ال channels تسمي مسار Path وكل مسار له رقم ، وتختلف ارقام ال paths من دولة لدولة ومن ISP to ISP وال ISP هو الذي يحدد هذه القيم التي يجب ان توضع في الروتر لكي يتعرف علي طريق الوصول لاجهزة ال ISP--><!--[endif]-->

وهذه بعض قيم ال VPI وال VCI التي تستخدمها بعض الدول

Internet Service Provider	VPI	VCI	Encapsulation
Australia – Telstra	8	35	PPPoA LLC
Brazil – Brasil Telcom	0	35	PPPoE LLC
France	8	67	PPPoE LLC
Germany	1	32	PPPoE LLC
India- BSNL	0	35	LLC PPoA/PPoE
Italy	8	35	PPPoA VC-MUX
New Zealand – Slingshot	0	100	PPPoA VC-MUX
Pakistan- PTCL	0	102	PPPoE LLC
Portugal	0	35	PPPoE LLC
Saudi Arabia (1)	0	33	PPPoE LLC

Saudi Arabia (2)	0	35	PPPoE LLC
Spain – Albura, Tiscali	1	32	PPPoA VC-MUX
Turkey	8	35	PPPoE LLC
United Kingdom	0	38	PPPoA VC-MUX
4DV.Net	0	32	PPPoA VC-MUX
All Tel	0	35	PPPoE LLC
August.net	8	35	1483 Bridged IP LLC
BellSouth	8	35	PPPoE LLC

وال VCs يتم تعريفها باستخدام معاملين : VPI وال VCI

وتعتمد عملية ال Switching او انتقال ال Data علي رقم ال Port وال VPI وال VCI

QOS

اذا كان لدينا شبكة انترنت بها الكثير من ال data المرسلة والمستقبلة ، هذه ال data تكون مختلفة في النوع فهناك فيديو وهناك مكالمات صوتية وايميلات ومحادثات ، لذلك يجب تنظيم عملية نقل هذه ال data

اهمية ال QOS تكمن في اولوية نقل هذه ال data (ال data الاهم هي التي يتم نقلها اولا) وكيفية النقل واهم الاشخاص التي يجب ان تنقل اليهم اولا

وتكون ال QOS هامه جدا في حالة ال VOIP وال Online Games وال IPTV لان هذه ال data تكون LIVE ولا تحتمل التأخير لذلك يتم ارسالها اولا

وهناك خمسة انواع من التصنيفات التي تتحدد علي اساسها درجة الQuality

Unspecified Bit Rate (UBR)

<!--[supportLists! if]--><--[endif]--!>هو اقل درجة من درجات ال **Quality** والتي تستخدم في حالة التطبيقات المتساوية في الاهمية وليس هناك اولوية لتطبيق علي الاخر

- <!--[endif]-->وهي تعتمد علي خاصية ال **best effort**

Available Bit Rate (ABR)

<!--[supportLists! if]--><--[endif]--!>عندما تريد نقل ملفات هامة باكبر قدر من الجوده ومن غير المهم وقت الوصول (قد يحدث تأخير في سرعة الارسال) فان هذا النوع من ال **Quality** هو الواجب اختياره

- <!--[endif]-->وهو درجة من درجات ال **Quality** التي تضمن وصول ال **Data** المهامة بافضل صورة واقل خطأ ولكن لا تضمن وصول باقي ال **Data** بشكل صحيح مع عدم مراعاة عامل الوقت

- <!--[endif]-->وهو يستخدم لنقل الملفات لذلك فان حجم ال **data** المنقوله يكون صغير وعليه فانه لا يتطلب **Bandwidth** كبير

Constant Bit Rate (CBR)

- عندما تريد نقل بيانات صوتية او مرئية علي الانترنت فانت تحتاج الي تدفق مستمر للبيانات بدون انقطاع

وهنا يجب استخدام هذا النوع من ال Quality

- حيث ان هذا النوع من ال Quality صمم خصيصا للتطبيقات التي تحتاج حجم ثابت من ال Bandwidth يخصص لمرورها هي فقط بدون تقاطع مع اي Data اخري اقل اهمية ، حيث يتم تقسيم ال Bandwidth الكلي الي جزئين ، جزء يخصص للتطبيقات الهامة وجزء اخر للتطبيقات الغير هامه

- وتستطيع نقل البيانات باقصي سرعه (PCR) يستطيع الخط حملها

Variable Bit Rate - Non-Real Time (VBR-nrt)

- يستخدم هذا النوع من ال Quality في حاله التطبيقات التي لا تعتمد علي الوقت ولا تتطلب اتصال مستمر كما في حاله الفيديو

مثل مشاهده فيديو مسجل علي اليوتيوب فقد يحدث انقطاع مستمر في الفيديو ولكن لن يتم فقد ال Data لانها سوف ترسل مرة اخري

Variable Bit Rate - Real Time (VBR-rt)

وهي اهم انواع ال Quality واكثرها حساسية لانها تتعامل مع التطبيقات التي تعتمد علي الوقت وتحتاج الي اتصال مستمر بدون انقطاع او تداخل للبيانات الاقل اهمية
مثل ال VOIP وال Video Conference

وهي تختلف عن ال CBR في ان ال CBR يستخدم جزء ثابت من ال Bandwidth

بينما ال **VBR – rt** فهو قد يأخذ ال **Bandwidth** كاملا بحيث قد يؤثر علي وصول اي **data** اخري اقل اهمية وقد لا تصل ابدا

LLC / SNAP

<!--[if !supportLists]--><!--[endif]--> تستخدم ال **LLC** في نقل مختلف انواع ال **data**

- <!--[endif]--> ويتم تقسيم ال **data** الي مجموعة من ال **packets** يتم ارسال كل **packet** باستخدام معرف خاص

- <!--[endif]--> ثم يقوم ال **SNAP** بعمل **Multiplexing** لهذه ال **packets**

- <!--[endif]--> ولكن هذه ليست الوظيفة الوحيده لل **SNAP** فال **SNAP** يقوم بارسال ال **data** بسرعات مختلفة **(transfer rate)** بغض النظر عن نوع ال **Topology** او نوع التوصيل **Ethernet, or Token Ring**

- <!--[endif]--> ويتم دمج ال **LLC** وال **SNAP** مع بعضهما للتاكد من عدم جدوث اي تلف او ضياع لل **data** اثناء النقل بين الانظمة والبروتوكولات المختلفة

<!--[if !supportLists]--><!--[endif]--> اما ال **VC-Mux** فهو يستخدم في نقل مختلف انواع ال **data**

- <!--[if !supportLists]--><!--[endif]--> وهو يستخدم في حاله نقل ال **data** باستخدام بروتوكولات مختلفة حيث يقوم ال **VC-MUX** بتخصيص **VC** لكل بروتوكول ثم يقوم بدمجهم معا **(Multiplexing)** وارسالهم عبر كابل انترنت واحد فقط

- <!--[if !supportLists]--><!--[endif]--> فعلي سبيل المثال يقوم ال **VC-MUX** بتخصيص **VC1** لل **data** التي يتم ارسالها باستخدام بروتوكول ال **IP** وتخصيص **VC2** لل **data** التي يتم ارسالها باستخدام بروتوكول **IPX** ... الخ

PPP IP Extension

<!--[if !supportLists]--><!--[endif]--> لها عدة مسميات مثل DMZ, Public IP assignment, PPP Extension IP, 1:1 NAT

<!--[if !supportLists]--><!--[endif]--> يستخدم لتخصيص ال WAN IP لجهاز واحد فقط في الشبكة ، عن طريق انه يجعل ال DHCP لا يقوم بتوزيع Private IPs علي الاجهزة الموجوده في الشبكة وانما يقوم باعطاء ال WAN IP لجهاز واحد فقط والباقي لن يعمل

<!--[if !supportLists]--><!--[endif]--> تفعيل هذا الاختيار يؤدي الي ايقاف خاصية ال NAT وال Firewall تلقائيا

PPP IP Extension

<!--[if !supportLists]--><!--[endif]-->لها عدة مسميات مثل DMZ, Public IP assignment, PPP Extension IP, 1:1 NAT

<!--[if !supportLists]--><!--[endif]-->يستخدم لتخصيص ال WAN IP لجهاز واحد فقط في الشبكة ، عن طريق انه يجعل ال DHCP لا يقوم بتوزيع Private IPs علي الاجهزة الموجوده في الشبكة وانما يقوم باعطاء ال WAN IP لجهاز واحد فقط والباقي لن يعمل

<!--[if !supportLists]--><!--[endif]-->تفعيل هذا الاختيار يؤدي الي ايقاف خاصية ال NAT وال Firewall تلقائيا

Wireless

يقوم جهاز الكمبيوتر الذي يحتوي علي الوايرلس بالتقاط جميع الشبكات المحيطة بقي والقريبة منه بشكل تلقائي

ولكن قد تختلف قوة الاشارة من جهاز لاخر ومن شبكة لاخري نتيجة لاختلاف التقنية التي يعمل بها الروتر والمسافة التي يبعد بها عن جهاز الكمبيوتر

وفيما يلي انوع التقنيات التي يعمل بها الروتر وخصائصها

802.11a

<!--[if !supportLists]--><!--[endif]-->تعمل في مجال تردد 5 GHz ولا يحدث تداخل بينها وبين اي اجهزة ميكروويف اخري نتيجة لاختلا التردد

<!--[if !supportLists]--><!--[endif]-->وسرعة نقل ال data نظريا تصل الي 54 Mb/s و لكن سرعة نقل البيانات الحقيقية حوالي 30 Mb/s وتختلف من شركة لاخرى

<!--[if !supportLists]--><!--[endif]-->وتستطيع ان تنتشر في مسافة تصل الي 45.7 m فقط

<!--[if !supportLists]--><!--[endif]-->والاجهزة التي تعمل تعمل بهذه التقنية لا تتوافق مع الاجهزة التي تعمل بتقنية Wireless-B, -G and –N نتيجة اختلاف التردد وذلك عند الحاجه لربط روترين لاسلكيا مع بعضهم

<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

802.11b

<!--[if !supportLists]--><!--[endif]-->تعمل في مجال تردد 2.4 GHz ومن الممكن ان يحدث تداخل بينها وبين اي اجهزة ميكروويف اخري نتيجة لان اجهزة الميكروويف تعمل عند نفس التردد

<!--[if !supportLists]--><!--[endif]-->وسرعة نقل ال data تصل الي 11 Mb/s

<!--[if !supportLists]--><!--[endif]-->وتستطيع ان تنتشر في مسافة تصل الي 91 m فقط داخل الاماكن المغلقة

<!--[if !supportLists]--><!--[endif]-->والاجهزة التي تعمل تعمل بهذه التقنية تتوافق مع الاجهزة التي تعمل بتقنية Wireless-G and –N نتيجة تشابه التردد وذلك عند الحاجه لربط روترين لاسلكيا مع بعضهم

<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

802.11g

<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

هو تطوير بسيط على 802.11 b بحيث تغيرت تقنية التشفير الى تقنية افضل بحيث اصبحت

<!--[if !supportLists]--> <!--[endif]-->سرعة نقل ال data تصل الي ٥٤Mb/s

<!--[if !supportLists]--> <!--[endif]-->وتعمل في مجال تردد 2.4 GHz ومن الممكن ان يحدث تداخل بينها وبين اي اجهزة ميكروويف اخري نتيجة لان اجهزة الميكروويف تعمل عند نفس التردد

<!--[if !supportLists]--> <!--[endif]-->وتستطيع ان تنتشر في مسافة تصل الي 91 m وقد تصل الي النصف داخل الاماكن المغلقة

<!--[if !supportLists]--> <!--[endif]-->والاجهزة التي تعمل تعمل بهذه التقنية تتوافق مع الاجهزة التي تعمل بتقنية Wireless-G and –N نتيجة تشابه التردد وذلك عند الحاجه لربط روترين لاسلكيا مع بعضهم <!--[if !supportLineBreakNewLine]-->

802.11n

<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

<!--[if !supportLists]--> <!--[endif]-->سرعة نقل ال data نظريا تصل الي ٥٤٠ MB/s اما السرعة الفعلية فتصل الي 70 Mb/s

<!--[if !supportLists]--><!--[endif]-->وتعمل في مجال تردد 2.4 GHz و 5 GHz ويحتوي الجهاز الواحد علي اكثر من هوائي و يتم الارسال و الاستقبال على الهوائيات في نفس الوقت MIMO او , Multi Input Multi Output

<!--[if !supportLists]--><!--[endif]-->اضافة ان تقنية معالجة هذه الاجهزة تعتبر ذكية للغاية بحيث تستطيع الاستفادة من الاشارة المرتدة و المنعكسة بشكل افضل

<!--[if !supportLists]--><!--[endif]-->وتستطيع ان تنتشر في مسافة تصل الي 250 m

<!--[if !supportLists]--><!--[endif]-->وهي تتوافق في العمل مع جميع الاجهزة التي تعمل في ترددات مختلفة كما في الشكل التالي

Standard	Bandwidth	Frequency	Range	Interoperability
IEEE 802.11a	Up to 54 Mbps	5 GHz band	150 ft (45.7 m)	Not interoperable with 802.11b, 802.11g, 802.11n
IEEE 802.11b	Up to 11 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11g
IEEE 802.11g	Up to 54 Mbps	2.4 GHz band	300 ft (91 m)	Interoperable with 802.11b

ROUTER
ISSAM SERHAN DYIB

SSID

What's New with My Site?

Here I could tell visitors about new additions to my site so they'll be sure to see my most recent pictures and information.

هنا أنا يُمْكِنُ أَنْ أُخبرَ زوّار عن الإضافاتِ الجديدةِ إلى موقعِي لذا هم سَيَكُونونَ متأكّدون لرُؤية صوري الأحدثِ و المعلوماتِي

What's New with My Subject?

ROUTER
ISSAM SERHAN DYIB

If I didn't include a news section about my site's topic on my home page, then I could include it here.
ذا أنا لَمْ أَتضمّنْ a قسم أخبار حول موضوع موقعِي على صفحتي الرئيسيةِ، ثمّ أنا يُمْكِنُ أَنْ أَتضمّنَه هنا.

WEP

<!--[if !supportLists]--> ال WEP هو ال Wired Equivalent Privacy اي انها التقنية المكافئة للتوصيل السلكي وبنفس مستوي الامان الذي يوفره الكابل<!--[endif]-->

<!--[if !supportLists]--> يعمل ال WEP باستخدام ارقام او اكواد سرية لتشفير ال Data تسمي RC4 مثل ال TKIP في ال WPA<!--[endif]-->

<!--[if !supportLists]--> حيث يقوم ال NIC بتشفير (Encryption) اللل Data بواسطة داله تشفير معينه (RC4) وارسالها <!--[endif]-->

<!--[if !supportLists]--> ثم يقوم ال Receiver بفك التشفير (Decryption) <!--[endif]-->

<!--[if !supportLists]--> **وهناك ثلاثه Modes لل WEP** <!--[endif]-->

<!--[if !supportLists]--> **Off** وهي عدم وجود Security <!--[endif]-->

<

<!--[if !supportLists]--> **64-bit** وهو تشفير ضعيف نتيجة استخدام داله تشفير صغيرة وضعيفه<!--[endif]-->

<!--[if !supportLists]--> **128-bit** وهو الاعلي امانا في هذا ال Mode نتيجة استخدام داله تشفير اطول حجما واكثر قوة<!--[endif]-->

<!--[if !supportLists]--> ولكن من السهل اختراق ال WEP واستخدامه يؤدي الي ضعف اداء الشبكة<!--[endif]-->

<!--[if !supportLists]--> حيث ان ال WEP يستخدم كود تشفير واحد فقط بين الاجهزة وبعضها، هذا الكود يوضع في جميع الاجهزة المتصلة علي نفس الشبكة ، بحيث يتم دمجه مع البيانات المتداوله وهو ثابت لا يتغير ، لذلك فمن الممكن تتبع ال Data واستخراج البيانات المتشابهه بها فتكون هي كود التشفير ، ومن هنا اصبح من السهل اختراق ال WEP<!--[endif]-->

WPA

<!--[if !supportLists]--> هو WPA ال<!--[endif]--> WiFi Protected Access وهي تقنية اكثر تطورا وامانا من ال WEP نتيجة استخدام دوال تشفير اكثر تطورا

<!--[if !supportLists]--> وهي حلقة الوصل بين WEP وال <!--[endif]-->

WPA2

<!--[if !supportLists]--> وال WPA تستخدم داله لتشفير تسمي <!--[endif]-->

Temporal Key Integrity Protocol (TKIP) وهي مصممة خصيصا لتغيير كود التشفير في كل مرة تنتقل فيها ال Data بين ال Users ، حيث يستطيع ال TKIP ان يغير كود التشفير الذي يتم دمجه مع ال Data مرات عديده وتوليد اكواد مختلفة تصل الي 500 trillion كود ،

<!--[if !supportLists]--> لذلك فمن الصعب تتبع ال Data <!--[endif]-->

واستخلاص اي بيانات متشابهه منها

WPA2

<!--[if !supportLists]--> ال WPA2 هو الجيل الجديد من ال WPA حيث يوفر مستوي امان اعلي <!--[endif]-->

<!--[if !supportLists]--> حيث يسمح فقط لل Users المخول لهم بالدخول علي الشبكة وذلك عن طريق دوال تشفير جديده ومبتكرة مثل ال Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES)<!--[endif]-->

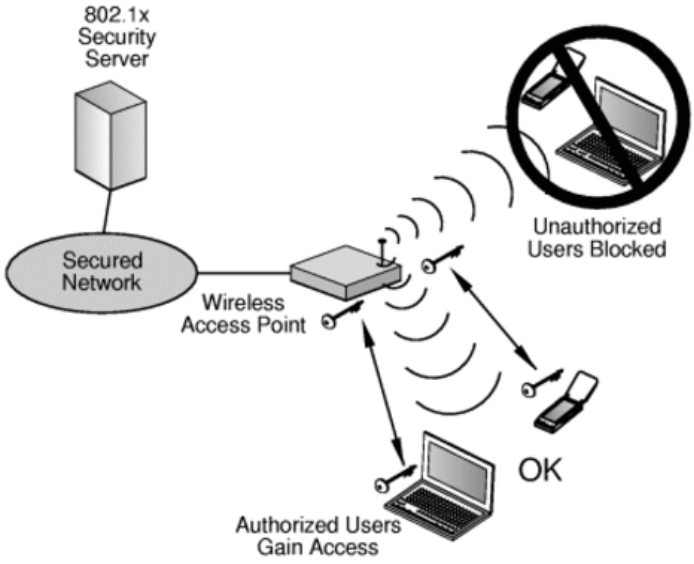
<

<!--[if !supportLists]--> وال WPA2 يدعم استخدام ال Radius كنوع من انواع ال Authorization وال Control التي يتم تطبيقها علي المستخدمين<!--[endif]-->

<!--[if !supportLists]--> وهناك نوعين من ال WPA2 <!--[endif]-->

<!--[if !supportLists]-->o WPA2 Personal وهو للاستخدام الشخصي ويتم عن طريق باسوورد عادي<!--[endif]-->

<!--[if !supportLists]-->o WPA2 Enterprise وهو للشركات ويتم ال Authentication من خلال Server معين او Radius<!--[endif]-->



IGMP

يتم التحدث بين الروتر وباقي اجهزة الشبكة باربع طرق مختلفة

١. الطريقة الاول : unicast

وهي ان يكون الارسال بين الروتر وجهاز واحد فقط في الشبكة

٢. الطريقة الثانية : multicast

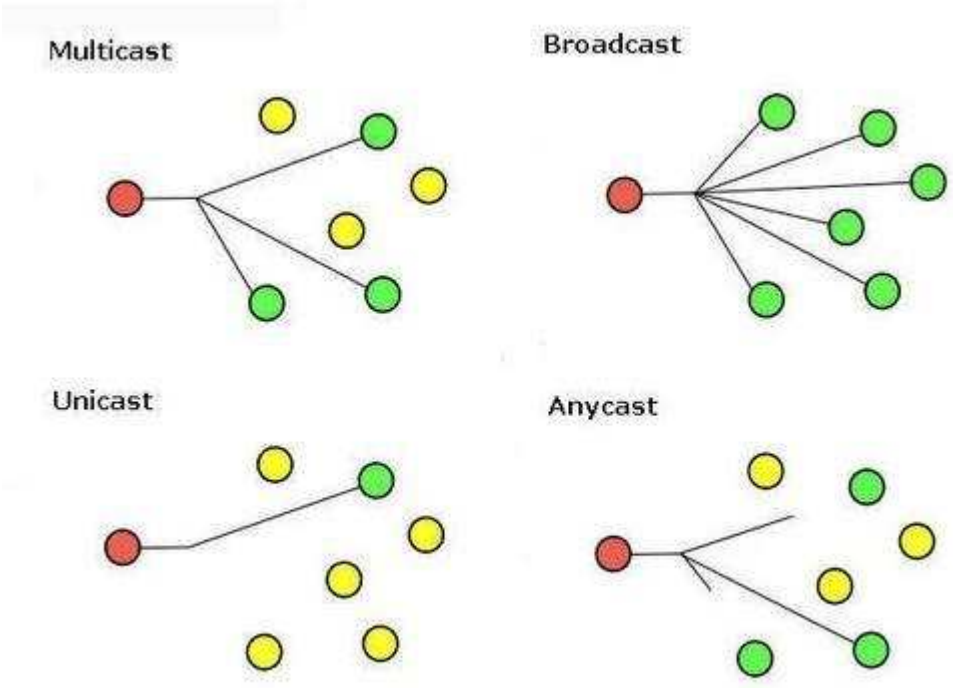
وهي ان يقوم الروتر بإرسال رساله لبعض اجهزة في الشبكة

٣. الطريقة الثالثة : Broadcast

وهي ان يقوم الروتر بارسال رسالة جماعية لجميع الاجهزة علي الشبكة

٤. الطريقة الرابعة : anycast

عليه ان يقوم الروتر بارسال رساله يكون الغرض منها هو ان اي جهاز يهتم بهذه الرساله يجب وهي الرد



وال IGMP هو البروتوكول الخاص بال multicast

<!--[if !vml]-->
<!--[endif]-->

<!--[if !supportLists]--> هــو Internet Group Multicast Protocol (IGMP) الذي يقوم بعمل multicasting <!--[endif]-->

- وتظهر اهميته في ال Video streem ال Online games <!--[endif]-->

- وتقوم الروترات بارسال رسائل بينها وبين بعضها لتحديد الاجهزة المشتركة مع بعــضها في group واحد<!--[endif]-->

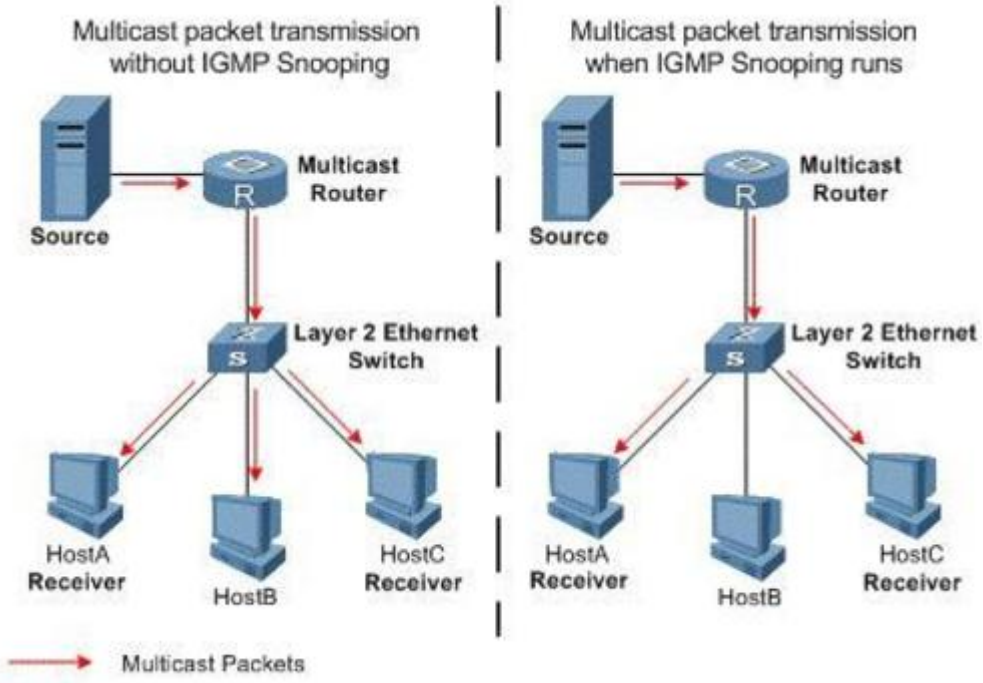
- يقوم الروتر بارسال رســائل اســتعلام الــي ال users) General Membership Queries(لمعرفة اي الاجهزة في اي group او الاجهزة التي تريد ان تنضم الي ال group <!--[endif]-->

- فتقوم ال Users بالرد علي الروتر بــ)Membership Reports(فيقوم الروتــر بعمل قائمة بالاجهزة الموجوده في كل group<!--[endif]-->

- ولا توجد اي قيود علي انضمام اي اجهزة لل group<!--[endif]-->

- وعندما يريد اي جهاز ان يرسل رسالة Multicast للاجهزة الاخري فيرسلها للروتر ب Destination Address من 224.0.0.0 to 239.255.255.255

- <!--[endif]-->لذلك عندما يعاني احد مستخدمي الانترنت من بطئ العاب الــشبكة او انقطاع للفيديو فيجب ان نقوم بتفعيل خاصية ال IGMP في الروتر



PPP Debug Mode

يسمح ال **PPP Debug Mode** بعمل **telnet** (التحكم في الروتر) عن بعد حتي يمكن اجراء اي تعديلات علي الروتر او اصلاح اي مشاكل تحدث به

فوائد جهاز الراوتر-:

1.جهاز الراوتر في الوضع االافتراضي لا يرسل او يستقبل اي بيانات.

2.جهاز الراوتر يستخدم رقم IP وهو رقم منطقي يعمل في طبقة الشبكة والذي يحدد الراوتر الذي ستنتقل اليه البيانات.

3.جهاز الراوتر يستخدم Access List وهي جدولة عناوين الشبكة حتى يتم السماح لها او لا ويتم

انشائها من قبل مدير الشبكة للتحكم في مستوى الامان والحجز على المخارج.
.4جهاز الراوتر يزود الطبقة الثانية بوظيفة الجسر للتوصيل بين المخارج

المعدات والبرمجيات

- **التسيير أو التوجيه في يومنا هذا كثيرا ما يرتبط مع الميثاق الشبكي النسخة ٤ (IPv4)، في حين أن الهجرة إلى الميثاق الشبكي النسخة ٦ (IPv6) انطوت على توجيه هذا الميفاق.**
- **المسيرات الأولى في عام ١٩٦٠ كانت ببساطة حواسيب عادية مصغرة. ورغم أن الحواسيب العادية يمكن أن تستخدم للتسيير، فإن المسيرات الحديثة بصفة عامة تشمل معدات إضافية لتسريع المهام الحساسة مثل نقل الحزمات. هذه المسيرات المتخصصة ليست دائما متوافقة مع (IPv6)، ذاكرة ذات قياس صغير غير متقلبة قادرة على حفظ الظبط الرئيسي في حالة خرق لحظات القطاع.**
- **المسيرات الحالية لنقل البيانات تلعب دورا مماثل من خلال المقاسم الهاتفية للصوت.**

هذا النوع من المعدات لا يتطلب التخزين المغناطيسي

١ - سيسكو (Cisco)

٢- بلكن (belkin)

٣- جونيبر (Juniper)

٤- سبيد تاتش (Speedtouch)

٥- شرونوس (chronos trendchip) صنع في تايوان

وهناك أنواع كثيرة لمهام أكبر :

نوع لاستقبال إشارة dsl أو شبكات الربط local loop (دائرة مغلقة) نوع لربط الشبكات ببعضها البعض.

تعريف الموجه

الموجّه Router هو جهاز شبكي يتألف من مجموعة من العتاد والبرمجيات يستخدم لربط اثنتين أو أكثر من الشبكات الفرعية المختلفة بواسطة

الإشارات السلكية واللاسلكية. يستخدم في الشبكات الواسعة مثل شبكة الإنترنت. يعمل الموجه في طبقة الشبكة Network layer وهي الطبقة الثالثة من الطبقات التي اصطلحت عليها منظمة

(OSI (Open System Interconnection

مستويات عمل الموجه

يعمل الموجه على مستويين :

١. مستوى تحكم : حيث يقوم بإيجاد أفضل طريق (أو أفضل واجهة) لإرسال الطرود عبره إلى المستقبل.

٢. مستوى تمرير ونقل : حيث يقوم بعملية النقل الفعلي للطرود المستقبلة من واجهة الاستقبال لواجهة الإرسال التي اختارها في المرحلة السابقة.

يعتمد الموجه على جدول التوجيه Routing table لإيجاد أقصر طريق للطرد.

أنواع الموجهات

للموجهات عدة أنواع من حيث الحجم والخدمة المقدمة :

١. موجهات للمكاتب الصغيرة والاستخدامات المنزلية Small Office Home Office (SOHO)

٢. موجهات لمزودات الخدمة والمؤسسات الكبيرة.

إن أشهر أنواع الموجهات تلك التي تنتجها شركة CISCO. لكنها باهظة الثمن نسبياً، فيما يلي يوجد أقسام موجهات Cisco.

أقسام الموجهات

سندرس كمثال عليها أقسام موجهات CISCO.

يتألف الموجه من لوحة أم Mother board تتوضع عليها وحدة معالجة مركزية CPU وذاكرة وقطع داخلية أخرى هي :

- ذاكرة ROM للقراءة فقط.
- ذاكرة Flash.
- ذاكرة وصول عشوائية RAM.
- ذاكرة وصول عشوائي غير قابلة للإزالة NVRAM.
- واجهة Interface.

الذاكرة ROM

ذاكرة قراءة فقط تحوي الكود المصدري للوظائف الأساسية. تتألف من أربعة مكونات أساسية :

- Post (power on self test) : هي أول ما يتم تحميله عند الإقلاع تقوم بتفحص العتاد.
- Bootstrap : كل نظام تشغيل يملك نوعين من الملفات : ملفات الإقلاع وملفات النظام، بداية يتم تحميل ملفات الإقلاع ثم تقوم ملفات الإقلاع بتحميل ملفات النظام. Bootstrap هو محمل الإقلاع من cisco، وهو يملك مسار ملفات الإقلاع.
- Mini IOS : يُحمل تلقائياً من الـ ROM يمثل مجموعة صغيرة من الـ IOS CISCO.
- ROM Monitor :يمكنك استخدامه للإقلاع يدوياً باستخدام الأوامر.

الذاكرة Flash

و هي نمط من الذواكر تستخدم في تخزين نسخة مضغوطة من ملفات نظام IOS CISCO ،عادة يتوضع فيها ملف وحيد. يختلف حجم هذه الذاكرة حسب السلسلة ونوع الموجه وهي تتراوح بين ٨-٦٤ KB. يقوم محمل الإقلاع الـ BootStrap بتحميل النظام IOS من الذاكرة Flash في عملية الإقلاع الطبيعية. يستخدم الأمر show flash في عرض معلومات هذه الذاكرة ومحتوياتها.

ذاكرة الوصول العشوائي RAM

و هي ذاكرة وصول عشوائي لكنها سريعة الزوال لا تحفظ البيانات بشكل دائم تتضمن الإعدادات الحالية للموجه، كما تزودنا بواجهة للتعامل مع المستخدم، تؤثر هذه الواجهة بشكل مباشر على أداء الموجه، وتكون ملفات النظام فيها غير مضغوطة وتعرف بمشغل الإعدادات

.

يستخدم الأمر show running-configuration في الكشف عن حالة هذه الذاكرة.

] ذاكرة الوصول العشوائي غير القابلة للإزالة NVRAM

و هي ذاكرة وصول عشوائي لكنها سريعة الزوال لا تحفظ البيانات بشكل دائم تتضمن الإعدادات الحالية للموجه، كما تزودنا بواجهة للتعامل مع المستخدم، تؤثر هذه الواجهة بشكل مباشر على أداء الموجه، وتكون ملفات النظام فيها غير مضغوطة وتعرف بمشغل الإعدادات

.

يستخدم الأمر show startup-configuration في الكشف عن حالة هذه الذاكرة.

الواجهة Interface

الموجه هو عبارة عن نقطة اتصال ذات واجهات متعددة، تتصل كل واجهة مع شبكة مختلفة، ويقوم الموجه بنقل البيانات المارة بين هذه الشبكات عبر الواجهات

. كل واجهة لها عنوان خاص بها. هنالك العديد من الواجهات المتاحة على الموجه مثل واجهة كبل الـ Ethernet للشبكات المحلية LAN وسلسلة من الواجهات المتزامنة و

غير المتزامنة للشبكات الواسعة WAN، يختلف عدد هذه الواجهات ونوعها بحسب سلسلة الموجه ونوعه. يحتوي الموجه على الأقل على منفذ Ethernet واحد ومنفذ WAN واحد (عادة يكون ISDN BRI) تعرض بعض الموجهات أوامر تتعلق بالواجهات مثل :

• الأمر show interface الذي يعرض الحالة الكاملة لجميع الواجهات في الموجه.

• الأمر Show interface serial 0 الذي يعرض الحالة الكاملة لواجهة معينة.

• الأمر Show ip interface brief الذي يعرض معلومات قصيرة ومختصرة ولكنها كافية مثل

IPaddresses، وحالة كل واجهة بالموجه.

CISCO ROUTER

راوتر السيسكو

تسلسل الإقلاع في موجهات cisco

١. تشغيل الفحص الذاتي POST.

٢. تحميل وتشغيل كود bootstrap.

٣. البحث عن برمجيات النظام.

٤. تحميل برمجيات النظام.

٥. البحث عن الإعدادات.

٦. تحميل الإعدادات.

٧. التشغيل.

إيجاد النظام IOS cisco

بعد تحميل الـ bootstrap، يتم البحث عن النظام IOS CISCO بداية، في حالة الإقلاع الطبيعي تبحث

عن نسخة ملفات النظام في الذاكرة Flash وإن لم توجد تحاول الإقلاع من الشبكة. إذا وجد أي مشكلة في شبكة الإقلاع عندها يعمل وضع RXBOOT، وإن لم ننجح يبقى أمامنا الخيار الأخير وضع الـ ROMMON. ترتيب عمليات البحث :

١. تفحص إعدادت السجل.

٢. تفحص إعدادت الـ NVRAM.

٣. يبحث في الذاكرة Flash.

٤. يحاول الإقلاع من الشبكة.

٥. اللجوء لوضع RXBOOT.

٦. اللجوء لوضع ROMMON.

ملاحظة : لمحاولة الإقلاع من الشبكة يجب أن نعرف عناوين IPs الموجهات المجاورة وهذا ممكن من خلال مساعدة CDP (CISCO Discovery Protocol) بروتوكول الاستكشاف الخاص بـ CISCO.

شركة سيسكو وانتاج الموجهات

تركز CISCO على إنتاج الموجهات Routers التي تستخدم في ربط أكثر من شبكة ببعضها البعض ، هذه الموجهات مزودة بنظام تشغيل Operating System يمثل ال Software المستخدم و تطلق عليه اسم IOS اختصاراً لكلمة . Interconnecting Operating System
كما تنتج الشركة أيضاً المبدلات Switches و الكثير من الأجهزة المتخصصة (و خصوصاً فيما يتعلق بدعم تقنيات VOIP الجديدة) و التي بدأت تحل مكان تقنيات الاتصالات المعروفة سابقاً .
سنحاول في هذه العجالة التطرق إلى بعض المفاهيم المتعلقة بعمل الموجه Router و جل ما يتم تطبيقه هنا يمكن إسقاطه على مبدأ عمل المبدلات Switches مع بعض التعديلات بما يتناسب و طبيعة عمل كل تقنية .

مكونات الموجه: Router

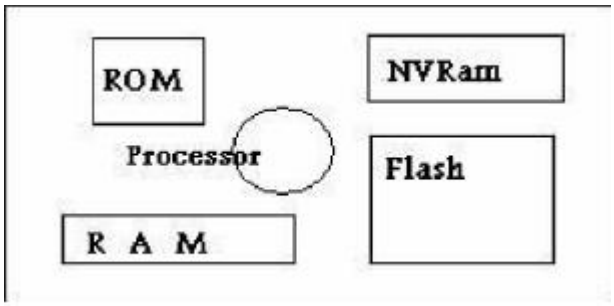
*الموجه هو جهاز يستخدم للربط بين الشبكات ، وظيفته الأساسية تحديد مسار اتجاه البيانات المتنقلة بين هذه الشبكات التي يربط بينها ، بمعنى أنه يحقق الاختيار الأفضل لانتقال هذه البيانات عبر أجهزة الربط ، و ليست هذه الوظيفة هي الوحيدة لمنها الوظيفة الأساسية .

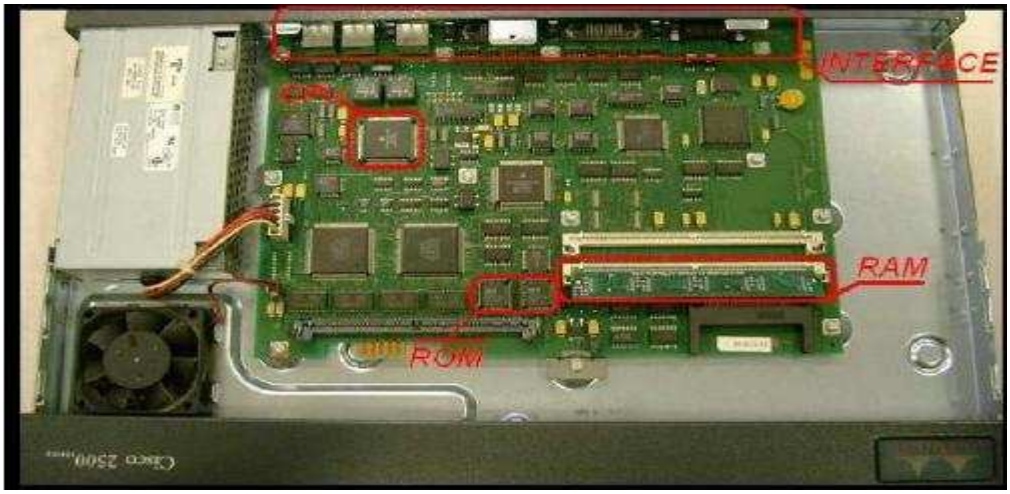
*الميزة الرائعة في Cisco Router , أنه مهما اختلف نوع أو حجم الموجه فإنه يمتلك نفس المكونات الداخلية الموجودة في أي موجه آخر ، و يقوم أيضاً بنفس عملية الإقلاع متشابهاً بذلك مع أنظمة تشغيل مايكروسوفت النى مهما اختلفت إصداراتها فهي تتميز بطابع وحيد و متشابه في عملية الإقلاع ضمن الحاسب و هو ما يماثل نظام التشغيل الخاص بموجهات Cisco و التي تنهج الطريقة ذاتها مع اختلاف أنواع الموجهات و إصدارتها و إصدارات أنظمة التشغيل IOS الخاصة بها .

و في الصفحة التالية مجموعة من الموجهات الخاصة بشركة CISCO باختلاف إصداراتها و اختلاف أنواعها و أحجامها بما يتناسب و المتطلبات.

*الراوتر في تركيبه يشبه جهاز الكمبيوتر العادي ف ي مكوناته الداخلية ، فهو لديه Processor و لديه أيضاً ذاكرة مؤقتة RAM , لكن الذاكرة في الموجه تنقسم إلى ٤ أجزاء تمثل أهم مكونات الموجه ، و يبين هذان الشكلان مكونات الموجه الداخلية .

ROUTER
ISSAM SERHAN DYIB





المكونات :

1- RAM : ذاكرة مؤقتة تحمل الإعدادات التي تم إدخالها للموجه و التي لم تحفظ بعد ، و هي تشبه عمل الجهاز الذاكرة في الجهاز العادي بمعنى أنه في حالة إغلاق النظام فإن ما كان في محتواها قد ضاع إذا لم يحفظ في مكان آخر .

2- ROM : تحمل في داخلها Boot Strap و التي تحمل في داخلها أكثر من حاله يقلع منها الموجه،و من أحد هذه الحالات حالة Password Recovery التي تستخدم للدخول للموجه من دون إدخال كلمة سر حتى و إن كانت مثبته عليه.

3- Flash Memory : و التي تشبه في عملها عمل القرص الصلب Hard Disk في الحاسوب العادي ، و هذه الذاكرة تحمل نسخة أو أكثر من نظام الإعداد IOS الخاص بالموجه و الذي يستخدم لإدخال البيانات إلى الموجه لإعداده للاستخدام.

4- NVRam : و هي اختصار لكلمة Non Volatile Ram أي الذاكرة الغير متطايرة (الثابتة) و فيها يتم حفظ Startup Configuration Fie أي الملف المستخدم لإقلاع الموجه ، و هذا الملف لا يتواجد إلا بعد إعداد الموجه باستخدام الأوامر و حفظها بعد الإعداد ، أي أن هذا الملف لا يتواجد إلا بعد عملية الإعداد ثم حفظها .

و يبين الشكل التالي التركيب الداخلي الخاص ب Cisco Router من فئة ٢٦٠٠ Series.

و هذه هي المكونات الأربع للذاكرة في الموجه و التي تمثل المكونات الرئيسية له و سوف يتم التطرق إلى شرح كيفية إقلاع هذا الموجه و كيف تتكامل هذه المكونات لتحقيق إقلاع ناجح للموجه حتى يتم تهيئته للعمل في بيئة ناجحة .

عملية الإقلاع (Boot Process) :

يمكن تلخيص عملية الإقلاع في ست مراحل
1-و هي مرحلة تشغيل الموجه و تبدأ بعمل ما يسمى ب (POST (Power On Self Test و فيها يجري الموجه اختبار للتأكد من أن الذاكرة والطاقة و غيرها بحالة جيدة حتى يتأكد من أن كل شيء يعمل بصورة وظيفية صحيحة.
2-و هي مرحلة تحديد الحالة التي سيقلع عليها الموجه من خلال حزام الإقلاع Boot Strap و هو حزمة فيها اختيارات عديدة تعتمد على ما إذا تدخل المستخدم في عملية الإقلاع أم لا ، و سيلي شرح هذه الحالات لاحقاً .
3-يتم فيها البحث عن نسخة من نظام الإعداد IOS تعمل بصورة صحيحة ، و هي عبارة عن ملف صغير مساحته تقع ما بين ٧ و ١٢ ميغا أو قد تزيد في أنواع مختلفة من الموجهات .
4-يتم تحميل النسخة الناجحة من الذاكرة Flash إلى الذاكرة المؤقتة. RAM
5-يتم البحث عن ملف Startup Config صحيح و جاهز للإقلاع من الذاكرة , NVRam و هناك حالتان إما أن يتواجد هذا الملف أو لا ، و هذا ينقلنا إلى المرحلة التالية .
6-إذا تواجد هذا الملف و الذي هو عبارة عن ملف مجهز و معد مسبقاً للعمل على هذا الموجه ، فإنه يتم تشغيله و تكون عملية الإقلاع ناجحة ، أما إذا لم يتواجد فمعنى ذلك أن الموجه يتم تهيئته لأول مرة أو أن هذا الملف قد تم إلغاؤه بواسطة المستخدم ، و في هذه الحالة يتم الدخول إلى حالة التهيئة Setup Modeلكي يتم برمجة الراوتر حتى يكون صالح للعمل .

و هنا قد يسأل سائل ، كيف يمكنني الاتصال بالموجه و ما هو المطلوب توافره حتى نتمكن من الاتصال به ، و هذا ينقلنا إلى الخطوة التالية ، حيث سوف يتم التطرق إلى وسائل و طرق الاتصال و أشكالها و أنواعها .

طرق برمجته

جميع الراوتر بصفة عامة يتم برمجتها عن طريق الوسائل التالية:
-عن طريق ال Menu حيث يكون هناك نقاط لكل شئ ويتم التنقل بينها
-عن طريق ال Command Line أي طريقة برمجة بالأوامر
-طريقة Setup Express وهي تعتبر طريقة برمجة سريعة تتم عن طريق اسالة ويتم الأختيار بين الأجابات سواء بنعم مثلا
تعتبر طريقة ال Command Lineمتقدمة فمن خلالها يمكن التحكم بجميع الوظائف داخل الراوتر

يتم برمجة الراوتر عن طريق الدخول عليه بالوسائل التالية

Telnet -حيث يتم الدخول للراوتر والبدأ في البرمجة عن طريق التلنت
-عن طريق ال Consol Port or Data Serial حيث يتم التوصيل بين الراوتر والكمبيوتر مباشرة ويتم البرمجة عن طريق ال Hyper Terminal
-عن طريق ال Browser حيث يتم الدخول للراوتر عن طريق متصفح العادي على الكمبيوتر عن طريق كتابة IP Address Http://

اعداد راوتر السيسكو

لو كان لدينا راوترين Router و Router1 وسنبدأ بـــ:Router

-للدخول اليه يجب أن يكون موصلاً مع الكمبيوتر وندخل عليه بواسطة الـــ Telnetأو الـــ Commandأ ، نفترض الآن أننا متصلين مع الراوتر Router
سيكون الوضع كالتالي :

كود:PHP

```
Router>
```

-الآن اذا قمنا بإضافة علامة الإستفهام ؟ سيعطينا مجموعة كبيرة من الأوامر

كود:PHP

```
Router> ?
```

-للبدء بإعداد الراوتر يجب ان نضيف الأمر enable وبعدها ستظهر علامة # وهذا يعني اننا داخل الراوتر الآن

كود:PHP

```
Router> enable

Router#
```

-وإذا اضفنا ايضاً علامة الإستفهام ؟ فهذا يعني اننا سنرى الأوامر التي يمكننا استخدامها

كود:PHP

```
Router# ?
```

-للخروج من الراوتر نكتب أمر Disable

كود:PHP

```
Router# disable
Router>
```

-الىن سنبدأ بإعداده وذلك باستخدام أمر Configure terminal ليكون الأمر على هذا الشكل

كود:PHP

```
Router> enable

Router# configure terminal

Router(config)#
```

-نريد الآن تسميته Router1 نكتب هذا الأمر hostname router1كما نرى في الشكل

كود:PHP

```
Router(config)# hostname router1

router1(config)#
```

-نريد وضع كلمة مرور وكلمة سر نكتب الأوامر بهذا الشكل مع العلم بأن ccnalab هو كلمة المرور و cisco كلمة السر

كود:PHP

```
router1(config)# enable ?

router1(config)# enable password ccnalab

router1(config)# enable secret cisco
```

-سنضعطي الراوتر الآن IP اذا كتبنا
intوبعدها ضغطنا على أمر tab على الكيبور ستظهر
بهذا الشكل تلقائياً interface ، طبعاً
ethernet0هو مخرج كرت الشبكة في الراوتر ، كما نرى نضيف
الآيبي ip ثم subnet على
التوالي بينهما فراغ واحد، أمر no shutdown يبقي كرت الشبكة على اتصال ولا يفصله:

كود:PHP

```
router1(config)# int

router1(config)# interface ethernet0

router1(config-if)# ip address 160.10.1.1 255.255.255.0

router1(config-if)# no shutdown
```

-الآن سنستخدم مخرج serial0 وهو مخرج السيريال على
الراوتر ونكتب نفس الأوامر السابقة ونعطيه ip

كود:PHP

```
router1(config-if)# int s0

router1(config-if)# ip address 175.10.1.1 255.255.255.0

router1(config-if)# no shut
```

-اذا ضغطنا على Ctrl ثم ضغطنا على حرف
zفسيخرجنا من الاعدادات بشكل كامل، كما نرى بالشكل:

كود:PHP

```
router1(config-if)# ctrl-z

router1#
```

-للخروج من الراوتر نهائياً نكتب الأمر: logout

كود:PHP

```
router1# logout
```

-الآن سنعود داخل الراوتر لنجرب أوامر جديدة، لاحظ هذه المرة طلب الباسورد:

كود:PHP

```
router1> enable

password: cisco

router1#
```

-هذا الأمر يعطينا ملخص عن معلومات الشبكة:

كود:PHP

```
router1# show ip interface brief
```

-هذا الأمر يعطينا تفصيلاً لكل مخرج Interfaceعلى حدى:

كود:PHP

```
router1# show interfaces

17. Display the active configuration in DRAM by typing:

router1# show running-config
```

-يعطينا هذا الأمر ملخص ما تم حفظه في NVRAM الخاص بالراوتر:

كود:PHP

```
router1# show startup-config
```

-يحفظ هذا الأمر الإعدادات الفعالة في: NVRAM

كود:PHP

```
router1# copy running-config startup-config
```

-سترى الإعدادات الفعالة التي تم حفظها في: NVRAM

كود:PHP

```
router1# show startup-config
```

-سترى رقم النسخة لنظام تشغيل الراوتر:

كود:PHP

```
router1# show version
```

-ستشاهد البروتوكولات الفعالة في الراوتر:

كود:PHP

```
router1# show protocols
```

-الآن سنبدأ بإعداد الراوتر رقم ٢:

كود:PHP

```
Router> enable

Router# configure terminal

Router(config)#
```

-سنقوم بتسميته:router2

كود:PHP

```
Router(config)# hostname router2

router2(config)# enable secret cisco
```

-هذه الخطوة جديدة، حيث الراوتر الذي نستخمه رقمه هو ٢٦٠٠ ويوجد به مخرج شبكة من نوع Fast Ethernet ويسمى Fa 0/0
لذا سنعطيه IP كما في هذا الأمر:

كود:PHP

```
router2(config)# interface Fa 0/0
```

```
router2(config-if)# ip address 160.10.1.2 255.255.255.0

router2(config-if)# no shut
```

-سنخرج من وضع الإعدادا ونطلب أن نرى تقريراً عن باستخدام امر show ip interface brief:

كود:PHP

```
router2(config-if)# ctrl-z

router2# show ip interface brief
```

-نستخدم أمر Ping لنتأكد من اتصال الطرفين بنجاح:

كود:PHP

```
router2# ping 160.10.1.1
```

مثال للبرمجة

Specify the level to execute the following commands ?
حدّدْ المستوى لتَنفيذ الأوامرِ التاليةِ؟

- Copy Privileged
- Show Run Privileged
- Show Flash User & Privileged
- Hostname Global
- Interface S0/0/0 Global
- Enable Secret Global

ROUTER
ISSAM SERHAN DYIB

Lab 3.1.3 Configuring Router Passwords – Instructor Version 2600

Objective

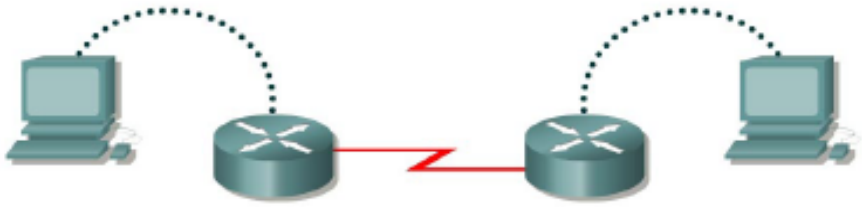
- Configure a password for console login to user EXEC mode.
- Configure a password for virtual terminal (Telnet) sessions.
- Configure a secret password for privileged EXEC mode.

Router > enable
Router # conf t
Router (config) # hostname Waleed
Waleed (config) # line console 0
Waleed (config – line) # password cisco
Waleed (config – line) # login
Waleed (config – line) # exit
Waleed (config) # line VTY 0 4
Waleed (config – line) # password cisco
Waleed (config – line) # login
Waleed (config – line) # exit
Waleed (config) # enable password cisco ! From user – privil.
Waleed (config) # exit
Waleed # disable
Waleed > enable

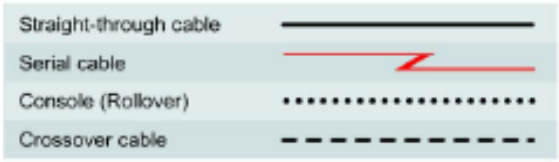
Password : cisco
Waleed #
Waleed # conf t
Waleed (config) # enable secret class ! From user – privil.
Waleed (config) # exit
Waleed # disable
Waleed > enable
Password : cisco
Password : cisco

Password : cisco
Bad secrets
Waleed > enable
Password : class
Waleed #

Lab 3.1.5 Configuring a Serial Interface – Instructor Version 2600



Router Designation	Router Name	Interface type	Serial 0 Address	Subnet mask	Enable secret password	Enable/VTY/ Console passwords
Router 1	GAD	DCE	192.168.15.1	255.255.255.0	class	cisco
Router 2	BHM	DTE	192.168.15.2	255.255.255.0	class	cisco



Objective

- Configure a serial interface on each of two routers so they can communicate.

Ahmed # conf terminal
Ahmed (config) # Int S0/0
Ahmed (config – if) # IP Address 192.168.15.1 255.255.255.0
Ahmed (config – if) # Clock rate 56000 ! It is DCE (Female)
Ahmed (config – if) # no shut down
Ahmed (config – if) # exit
Ahmed (config) # exit
Ahmed # show int S0/0
Ahmed # show run-conf

Huda # conf terminal
Huda (config) # Int S0/0
Huda (config – if) # IP Address 192.168.15.2 255.255.255.0
Huda (config – if) # no shut down
Huda (config – if) # exit

Huda (config) # exit
Huda # show int S0/0
Huda # show run-conf
Huda # copy run start ! To save the current configuration

Huda # ping 192.168.15.1 ! should work
Ahmed # ping 192.168.15.2 ! Should work

Lab 3.1.7 Configuring an Ethernet Interface – Instructor Version 2600

Router Designation	Router Name	Router Type	FA0/0 Address	Subnet mask	Enable Secret password	Enable/VTY/ Console passwords
Router 1	GAD		192.168.14.1	255.255.255.0	class	cisco

Objective

- Configure an Ethernet interface on the router with an IP address and a subnet mask.

Huda # conf terminal
Huda (config) # Int Fa0/0
Huda (config – if) # IP Address 192.168.14.1 255.255.255.0
Huda (config – if) # no shut down
Huda (config – if) # exit
Huda (config) # exit
Huda # show int Fa0/0
Huda # show run-conf ! Remember this does not work from user

كيفية عمل اعدادات الراوتر و الشبكة

لنفترض ان لدينا ٦ اجهزة مستخدم , 1 جهاز مضيف

-1قم بتوصيل الاجهزة ب switch/hub ثم اوصله بالمضيف

-2لجميع الاجهزة قم بتعطيل ال dhcp لتحصل على static ip

-3طبعا سافترض ان النظام لديك هو windows لذلك protocol هوip/tcp مثبت افتراضي

-4ادخل على جهاز المستخدم (ال ٦ اجهزة) وقم بتغيير الاعدادات لكل جهاز

مثلا الجهاز الاول يكون له ip محدد مثلا192.168.1.2 :
الجهاز الثاني يكون مختلف مثلا : ١٩٢,١٦٨,١,٣
وهكذا للجميع

الان اضبط الGateway
لتكون واحدة للكل مثلا
Gateway: 192.168.1.1

واخيراDNS
هذا على موزع الخدمة لديك

-5قم بمشاركة الطابعة Printer / الماسح الضوئي

علاقة المودم بالراوتر

المودم هو جهاز لإستقبال إشارة الديجتل (DSL)يحول الموجات الكهربائية الي تنتقل من شركة الاتصالات بالتلفون لموجات مفهومة للغة الكمبيوتر .DATA Signal بينما الراوتر يأخذ اشارة الداتا ويوزعا على الأجهزة بشكل منتظم (يعني جهاز ١ طلب موقع ياهو وجهاز ٢ طلب موقع هوتميل .. الراوتر يستقبل الطلبات ويسجل ان هالطلب من رقم IP 10.0.0.1 مثلا يروح يستقبل البيانات من الانترنت ويرجع يحولها لرقم IP الجهاز الي طلبها من خلال للشبكة الداخلية (بشكل مبسط ..

المودم = استقبال الاشارة .
الراوتر = التوزيع .

<u>الفرق بين الراوتر العادي والراوتر الذي معه مودم</u>

هو ان بالراوتر الذي معه مودم يمكنك توصيل خط التليفون او ال ISDN او Leased Line به ويقوم هو بعمل الطلب والدخول للأنترنت ومن ثم يزود الشبكة كلها بالأنترنت وبعض انواعه يطلق عليها IPSharer وفكرته هي العمل كأن المودم هذه هي Interface فيقوم بربط شبكتها بالشبكات الأخرى.

الية العمل الطبيعية للموجهات

تطرقنا سابقا الى فكرة عمل الراوتر هو ان يتم توصيل كل شبكة على Interface معين او شئ قد يشبه كارت النيتورك داخل الراوتر ومن ثم يقوم الراوتر بعمل Routing أي ربط ما بين هذه الشبكات عن طريق بروتوكولات معينة تسمى Routing Protocols وظيفتها توصيل ال Packetsمن شبكة لأخرى

يوجد نوعان من الموجهات:

1-موجه يعرف ويحدد المسارات التي سوف يتخذها للوصول للطرف الأخر.
2-موجه يقوم بإرسال الحزم إلى المسار القادم مباشرة بدون تحديد مسار أفضل

ولكن ماهي المسارات وكيف يوجد مسار افضل من الاخر وكيف يحددها الراوتر؟؟

بالطبع هناك مسارات افضل من الاخرى (اي اقصر او توفر وقتاً) فإذا قلنا ان هناك بيننا وبين دولة فرنسا ٥٠ راوتر كلاً واصلين تلو الاخر (وهذا ما يحدث في الحقيقة) كلاً من هذه الموجهات موجود في مدن عدة منها اقرب ومنها ابعد – يقوم الراوتر لدينا بالتحدث مع الراوتر الذي يليه وبالتالي يرسل للذي يليه وهكذا حتى يحدد اقرب طريق (وهذه طريقة واحدة من عدة طرق (وبهذا يحدد اي مسار افضل واذا كان هناك مسار مشغول يمكن ان يتجنبه عن طريق مسار اخر.

يوجد عدة انواع من الموجهات من حيث الخدمة والحجم:

بالطبع اجهزة ADSL Modem والتي نراها في منازلنا لا يتعدى حجمها حجم كتاب كبير - ولكن هل تعلم ان هناك موجهات يتعدى حجمها الثلاجة؟

1-موجهات للإستخدام المنزلي والإستخدام الداخلي:

تعمل هذه الموجهات على نطاق صغير بمعنى انها تخدم وسائل الانترنت وتحديد المسارات القادمة

ولكنها بعد ان ترسل الحزمة لا تقوم بالإحتفاظ بالمسار الذي استخدمته.

ايضاً من عيوب هذه الموجهات ان في بعض الاحيان تصلها حزم كبيرة لا تستطيع تحويلها كاملة وبالتالي تفقد هذه الحزم.

-2موجهات تستخدم للمكاتب الصغيرة:

يتم إطلاق لقب Gateway عليها وهي تعني المعبر - وتقوم بإيصالك بشكبات اكبر منها مثل الانترنت ومن مميزاتها انها تجعل عدة اجهزة كمبيوتر تعمل عليها بأن تظهر كجهاز واحد فقط على شبكة الانترنت Residental Gatewar

-3موجهات تستخدم على نطاق المؤسسات الكبرى:

يكون حجم هذه الاجهزة ضخم ويمكن وجودها في الجامعات ومراكز تزويد خدمة الانترنت ISPs تعتبر من افضل الموجهات نظراً للخدمات العدة التي تقوم بها ويطلق عليها دائما مصطلحLevel 3 Model

الاجهزة المستخدمة في الشبكات اللاسلكية
بالنسبة للشبكات اللاسلكية تستخدم هذه الأجهزة كالتالي
١- Router (وهو جهاز يرتبط بين شبكتين ويعمل كمنظم لأحداها كأن يرتبط بمودم dsl من جهة وبأربعة كمبيوترات من الجهة الأخرى سلكيا بالإظافة لأجهزة لاسلكية (إذا كان يدعم لاسلكيا (ويعمل عمل السوتش بين الكمبيوترات وبالتالي فهو يربط الشبكة الداخلية مع الشبكة الخارجية (dsl) وتوجد أجهزة يكون المودم مدمج مع الراوتر ولكن ليس بالضرورة

(2Access point وهو جهاز يرتبط بالراوتر لإيصال الذبذبة لأجهزة طرفية في مناطق بعيدة عن الراوتر (كأن يكون عندك راوتر مرتبط به أجهزة سلكيا ولا سلكيا في الدور الأرضي ولكن الذبذبة لا تصل للدور الثاني فيمكنك وضع أكسس بوينت في الدور الثاني مربوط سلكيا بالراوتر بالدور الأرضي وبالتالي يبث الذبذبة لكامل الدور الثاني لاسلكيا(

(3Bridge وهو يربط بين شبكتين لاسلكيا (كأن يكون راوتر في دور وراوتر آخر في دور مختلف فتحتاج جهاز بردج لكل شبكة لربطهما)

طريقة شبك راوتر الـSpeedTouch

لتحميل سي دي الراوتر

من هنا!!!!!!!

ROUTER
ISSAM SERHAN DYIB

بالنسبة لكيفية إعداد راوتر السبيد تاتش

يوجد مع الجهاز رقم مطبوع وهو غالبا يكون

192.168.0.1

10.0.0.138

أو اي رقم

تضعه على المتصفح ثم تضغط كونترول+إنتر معا Control+Enter ليفتح صفحة الراوتر

ROUTER
ISSAM SERHAN DYIB

تفتح معنا صفحة جديدة لكي نبدأ بالإعدادات

هذه الصورة مصغره .. نقره على هذا الشريط لعرض الصوره بالمقاس الحقيقي .

ROUTER
ISSAM SERHAN DYIB

هنا علينا تحديد إستخدام راوتر السبيد تاتش ؛ هل نريده بدون راوتر Bridge

أو لكي يعمل راوتر Router

وهذه ميزة رائعة بهذا الراوتر

ROUTER
ISSAM SERHAN DYIB

هنا أهم خطوة

الخيار الأول User Name : وهو عبارة عن إسم المستخدم (تختاره شبكة الإتصالات(

الخيار الثاني Password : تضع فيه الرقم السري الخاص فيك والمزود لك من قبل الشركة

الخيار الثالث Confirm Password : وهو خاص بتأكيد الرقم السري وبعدهاNext

هنا تستطيع وضع يوزر نيم وباسوورد خاص بك لكي لا يستطيع احد الدخول على الراوتر إلا بيوزر نيم وباسوورد ؛ وتستطيع عدم تحديد أي شيء وتركها وبهذا لا يطلب منك الإسم وتصريح الدخول عند إعادة إعداد الراوتر

ROUTER
ISSAM SERHAN DYIB

ROUTER
ISSAM SERHAN DYIB

ROUTER
ISSAM SERHAN DYIB

التعامل مع الراوتر المخترق و الشبكة

توجد في بعض الدول طريقة أو أسلوب للحصول و للمشاركة في خط الانترنت المفرد ، حيث تحصل عدة بيوت متقاربة على إمكانية المشاركة في خط ADSL واحد ، من خلال ADSL Router ، يتم وصل ٨ بيوت (حواسب على الأقل) حسب المخطط التالي-:

Users ----> ADSL Router (Firewall) ---> Internet

حيث لأي شبكة يتم فيها وصل الانترنت فأنها تواجه إخطار أمنية (من داخل الشبكة و خارجها.(

طريقة مشاركة الانترنت بهذه الطريقة تواجه مشاكل عديدة من ناحية الأمن سوف أحاول ذكر بعضها بقليل من التفصيل إضافة إلى التعامل مع الراوتر.

هناك ثمانية نقاط رئيسية يجب الاهتمام والتعامل بها هي:-
-1إمكانية السيطرة على الراوتر
-2أخطاء شائعة لدى المشرفين و المدراء
-3التعامل مع الجدار الناري
-4التعامل مع بروتوكول DHCP الرائع
-5عمل Listening على الراوتر نفسه للحزم المارة به
-6الحصول على معلومات في منتهى الاهمية و الخطورة
-7اتخاذه محطةGateWay
-8ملاحظات مهمة

-1إمكانية السيطرة على الراوتر:

إذا استطاع الهاكر السيطرة على الراوتر الذي يقوم بتوزيع الانترنت على اعضاء الشبكة ففي هذي الحالة يسمى هذا الهاكر مخترق شبكات Networks Hacker ، حيث لا يمر شئ بهذه الشبكة دون علمه ، بسيطا او مهما ، جمل دردشة او كلمات سر كلها تمر من خلال الشبكة الى الانترنت ، فلو قام الهاكر بانشاء عضوية جديدة لمدير جديد و لم يعلم عنه المدير الاصلي، فيمكننا القول ان مدير الشبكة الاصلي يمكنه توديع شبكته الا عند قيامه بمسح الراوتر و اعادة برمجته ، لان في هذه الحالة يمكن للهاكر القيام بأفعال خطيرة قد تؤدي الى مشاكل كبيرة.

-2أخطاء شائعة لدى المشرفين و المدراء:

ما يضحك الهاكرز المتمرسين هو عندما يقوم مدير الشبكة و صاحب الراوتر بوضع كلمة سر سهلة و احيانا ينسى تغيير الكلمة الاصلية Default و احيانا لا يضع كلمة سرية على الراوتر ، فعند عدم وضع كلمة سرية على الراوتر ، لا يجب على الهاكر الا الاتصال بالراوتر عن طريق اي منفذ Port مفتوح و معظم الاوقات يكون منفذ Telnet مفتوحا لكي يقوم المدير بالتعديل في تضبيطات الراوتر ، و احيانا ترى كلمات سرية سهلة فما عليك الا الاتصال بالراوتر بواسطة اداة (سواء وندوز او لينكس ،

لينكس افضل) تقوم بعملية تجريب كلمات سرية بأي طريقة سواء عن طريق وسيلة Dictionary أو BruteForceففي غضون ساعات الى ايام سوف تحصل على الكلمة السرية و ثمتها بأمكانك القيام بأنشاء مدير جديد للنظام ، و أحيانا تكون الكلمة السرية نفسها الاصلية Default و احيانا تكون مشابهة لأسم المدير. Username

-3التعامل مع الجدار الناري:

عند معرفتك للجدار الناري (الخاص بال Serversو ليس الجدار الناري العادي) و معرفة التعامل معه فأنك تضمن حمايتك الشبكية ، قمت انا بتطوير فكرة تحميني من المشاكل الامنية و لقد استخدمتها و نجحت الطريقة و لله الحمد ، و هي عندما تقوم بعملية هكرية سواء كانت سهلة او صعبة ، و كنت تخاف و تخشى من الملاحقة و التقصى Trace تقوم بتضبيط الراوتر على عدم استقبال اي حزم من العنوان المحدد ، سوف اقوم بشرح العملية بالتفصيل في موضوع قادم ان شاء الله اذا سمح الوقت في المستقبل ، حيث بالجدار الناري يمكنك منع الاشخاص من دخول شبكة الانترنت ، او حجب خدمات خاصة عليهم مثل KaZaA او اي برنامج او اداة تستخدم منفذا معينا، و ايضا يصبح لك امكانية التحكم بالراوتر من حيث سماحه لأتصالات من خارج الشبكة او داخلها.

-4التعامل مع بروتوكول: DHCP

DHCPهو اختصار لجملة Dynamic Host Control Protocol حيث يقوم هذا البروتوكول بتوزيع عناوين IP للأشخاص في الشبكة ، و ذلك يشبه اعطائهم عضوية في الشبكة ، و ذلك من خلال الاتصال بالشبكة ، فكل من يتصل بالشبكة يحصل عضوية تخوله من الاستفادة من الشبكة (انترنت - موارد – افكار – ملفات) ، و لكن هناك حيل يستطيع الهاكر القيام بها و ذلك ليستفيد من الشبكة و مواردها لوحده فقط (لو كان متصلا بها من الداخل و ليس اتصال خارجيا (، فمثلا يوجد لهاكر (استطاع اختراق راوتر معين) حاسبان متصلان بالشبكة ، و يريد هو الحصول و الاستفادة من الشبكة لوحده لفترة معينة فمثلا في هذه الفترة يقوم بتنزيل ملف كبير جدا مهم و هو يواجه مشكلة بطأ الانترنت فيقوم بتعديل الراوتر و بخاصة تضبيطات DHCP بحيث تقوم الشبكة و الراوتر باعطاء عنوانان IP فقط لكي يحصل حاسباه عليهم و هو الوحيد الذي يملك عضوية في الشبكة ، و يمكن ايضا ان يحدد MAC Adressخاص قادر على الحصول على عضوية في الشبكة ، اذا هو الوحيد القادر على الاستفادة من الشبكة ، و عندما يدخل اي شخص اخر على الشبكة فأنه لا يحصل على عضوية في الشبكة ، و مهما حاول هذا الشخص الاخر و قام بتضبيط عنوانه IP الى عنوان IP الشبكة (يدويا) فلن يحصل على عضوية.

-5عمل Listening على الراوتر نفسه للحزم المارة به:

بواسطة هذه الطريقة ، اي حزمة بها معلومات تشق طريقها الى عنوان محدد في الشبكة العنكبوتية تمر بالراوتر و الذي يفحصها و عدم احتوائها على اضرار او اكواد مضرة ، فيقوم الراوتر (بأمر من الهاكر) بتخزين جميع الحزم المارة به الى ملف واحد او عدة ملفات حسب ما يحدد الهاكر ، وتسمى العملية نفسها Sniffing و قد شرحتها من قبل في موضوع سابق ، بعدها يمكنك تفحص مصدر

الحزمات و تحويلها الى ASCII ليمكنك قرائتها بدلا من Hex او النظام العشري.

-6الحصول على معلومات في منتهى الاهمية و الخطورة:

فعند سيطرتك التامة على راوتر يمكنك معرفة User & Pass لهذه الشبكة مع ISP التابع لها ، من خلال فحص ملفات تضبيطات بروتوكول PPP : Point to Point Protocol الذي يأمن اتصال مع ISP عن طريق خط هاتف ، بالاضافة الى قدرتك على الحصول معلومات DNS الخاصة بالشبكة و امتلاكه الى الابد ، بأمكانك الحصول على معلومات البريد الالكتروني ، الحصول على معلومات كل شخص على الشبكة مثل معلومات PC ID - MAC Adress - Time Taken بالاضافة الى معلومات بالغة الخطورة يمكنك ان تعرفها مثل رقم هاتف صاحب الشبكة ، بريده الالكتروني و احيانا عنوانه.

-7اتخاذه محطة: GateWay

لو قدرت ان تسيطر على الراوتر فأنه بأمكانك اتخاذه على شكل Server لتستخدمه في عمليات هكرية و احيانا غير قانونية ، فأنك تتصل به عن طريق اي بروتوكول بواسطة بورت مفتوح ثم تتصل بالضحية (تذكر ان الضحية هي Server او GateWay و ليست حاسب ضحية برورات او Trojan)و عندك انتهائك من العملية بأمكانك مسح Logs من الراوتر ، فعندها تنقطع كل الدلائل عنك ، بالاضافة الى امكانية عمل Ping من الراوتر.

Hacker ----> Internet ----> Hacked Router(GateWay) ---> Internet ----> Victim

تسمى هذه العملية Bouncing ، فأذا قام الضحية بالتقصى Tracing على طريقة Passive Traceفسوف تنقطع سلسلته عن الراوتر المخترق ، و عندها تنجو انت من فعلتك.

-8ملاحظات مهمة-:

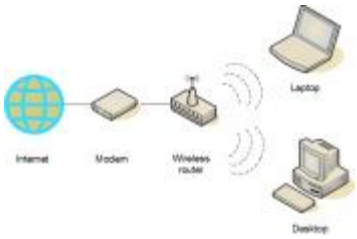
-عمل الفايروول بالتحديد هو التحكم بالاتصالات من داخل الى خارج الشبكة OutBound ، و ايضا من اي اتصال من خارج الى داخل الشبكة.InBound

-عند تشغيل الراوتر فأنه يحصل على عنوانين) IP داخلي و خارجي ، الداخلي هكذا أحيانا ١٩٢,١٦٨,١,١ أو10.0.0.1 ، اما الخارجي فهكذا ٨٢,١٩٤ XXX.XXX.أحيانا(

-عندما نقول راوتر فأننا لا نقصد بالتحديد ذاك الجهاز الذي يحوي عدة منافذ فيزيائية ، واحد لخط ADSLو الاخريات من أجلRJ45 ، احيانا يمكن ان يكون حاسب يقوم بعمل الراوتر و الغالب في هذه الانواع وجود نظام Linux لأنه اقوى مع الشبكات.

ROUTER
ISSAM SERHAN DYIB

اعداد شبكه لاسلكيه بسيطه بين اكثر من جهازين باستخدام الراوتر



ان استعمال تكنولوجيا الشبكات اللاسلكيه تجعل عمليه التعامل مع حاسوبك اكثر مرونه حيث تستطيع ان تتصفح الانترنت و تشاهد افلامك الخاصه و حتى ان تتسلى بالعابك المفضله عليه و انت تتنقل في انحاء منزلك و ذلك لانك دائما تكون متصلا.
ان اضافه شبكه لاسلكيه لجهاز الحاسوب الخاص بك نتبع مجموعه من الخطوات
-1اختيار الادوات و القطع و الراوتراتrouters
-2نقوم بتوصيل القطع و الادوات
-3ضبط اعدادات القطع و الادوات
-4توصيل الحاسوب الخاص بك الى الشبكه
-1اختيار الادوات و القطع و الراوتراتrouters
الخطوه الاولى هي باختيار الادوات اللازمه و هنا نحتاج الى شيئين أ) راوتر لاسلكي wireless Router وب) كرت شبكه لاسلكي Wireless network adapter و جميعها متوفره في السوق
ان الراوتر اللاسلكي Wirelss Router هو الجهاز او الاداة التي تقوم بتوزيه الاشارة الاسلكيه على الاجهزه المعنيه و ايضا يقوم بعمليه الاتصال بالانترنت و توزيع الاتصال الى الاجهزه المعنيه عبر الاشارة اللاسلكيه . انظر الصوره ادناه

اما كرت الشبكه الاسلكي wireless network adapter فيركب على الحاسوب الخاص بك و يقوم بعمليه وصل جهازك الحاسوب مع الراوتر الاسلكي . Wireless Router انظر الصورة ادناه
Pic2

-2توصيل القطع و الادوات
أ)نقوم بازاله الكابلات الخاصه بالشبكه السلكيه الموصوله بين الحاسوب و الموديم او اي راوتر قديم
ب)نقوم بتوصيل موديم ال DSLبالراوتر الاسلكي بواسطه سلك الشبكه العادي الذي له راس RJ45 بحيث يكون طرفه الاول في الموديم و الثاني في الراوتر الاسلكي في البورت المخصص للانترنت Wireless Router Internet portكما الصوره
Pic3

نقوم بتشغيل الموديم و الراوتر و نلاحظ اضائه البورت الخاص بالانترنت عليه كما الصوره

Pic4

-3ضبط الاعدادات للراوتر الاسلكي Configure the wireless router

بعد تشغيل الراوتر اللاسلكي نقوم بتوصيله بالسلك الذي ياتي معه بكرت الشبكه العادي في الحاسوب و ذلك لنقوم ببرمجته و ضبط اعداداته و تعريف الشبكه اللاسلكيه عليه. انظر الى الصوره و لاحظ السلك الازرق

Pic5

pic 6

نفتح النترنت اكسبلور Internet Explorer و ندخل على الصفحه الخاصه باعدادات الراوتر و التي تكون عباره عن IP address خاص به و يمكن الحصول عليه من دليل الاستخدام manual الذي ياتي معه

Pic7

ندخل اسم المستخدم و كلمه المرور الخاصتان بالراوتر الاسلكي

Pic8

هنا اسم المستخدم و كلمه السر و ال ip address لمجموعه من الراوترات المشهورة و الاكثر تداولا في السوق

RouterAddress Username Password
admin Adminhttp://192.168.1.13Com
admin (leave blank)http://192.168.0.1D-Link
admin Adminhttp://192.168.1.1Linksys
admin passwordhttp://192.168.0.1Netgear

الان سوف تفتح صفحه الاعدادات و منها نبحث عن التبويب لاسلكي Wireless Tab كما الصورة
نقوم بضبط لاعدادات لنوع الشبكه ل Mixedوذلك حتى نكون قادرين على استعمال الراوتر في حالتيه السلكيه و اللاسلكيه
نضع اسما للشبكه في خانه و SSID or naming your networkو يمكن ان يكون اي شيء تختاره.
نفعل الخيار Enable ثم نحفظ الاعدادات باضغط على الزر save sittings
Pic9

الان الى اعدادات الحمايهSSID or naming your network
نذهب الى التبويب الخاص بامن و حمايه الشبكه الاسلكيه wireless security
Pic10

نختار اولا نوع التشفير web encryption و هنا ١٢٨ بت ثم نضع في مربع phrases اي شيء نريده و نضغط على الزر Generate و تظهر لنا مجموعه من الارقام في key1 , key2 , key3 key4,و هي مفاتيح التشفير وهذه يجب ان تكتبها او ان تقوم بنسخها و حفظها في مستند لانك سوف تحتاجها فيما بعد

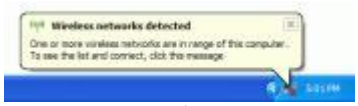
-4اعداد جهاز الحاسوب للاتصال بالشبكه اللاسلكيه

الان تستطيع ان تفصل السلك الازرق المتصل بين الحاسوب و الراوتر الاسلكي ثم نضيف كرت الشبكه الاسلكي الى الحاسوب
P

ic12وهنا هو عباره عن قطعه USB تشبه الفلاش و نقوم بتعريفه الى الحاسوب و تثبيت البرامج الخاصه

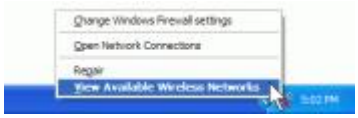
به و التعريفات من القرص المرفق حتى يصبح جاهزا و عندها نلاحظ الايقونه التي تظهر بجانب الساعه

Pic13



و نقوم بالضغط بالفاره عليها بالزر الايمن

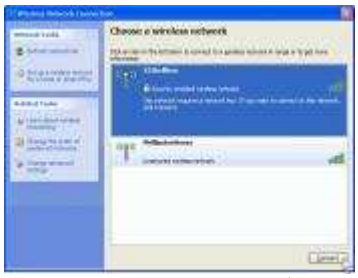
Pic14



و نختار **view available wireless network**

و تظهر لنا الشاشه التاليه و نلاحظ انها تحتوي على اسم الشبكه الذي قمنا بوضعه في الاعدادات في لالعلى و لاحظ رمز القفل الذي يدل على انها سبكه امنه

Pic15



نضغط على الزر **connect** و عندها يظهر مربع الحوار الذي يطالب بادخال مفتاح الشبكه و هو ما قمنا بكتابته جانبا في خطوة الاعدادات ا