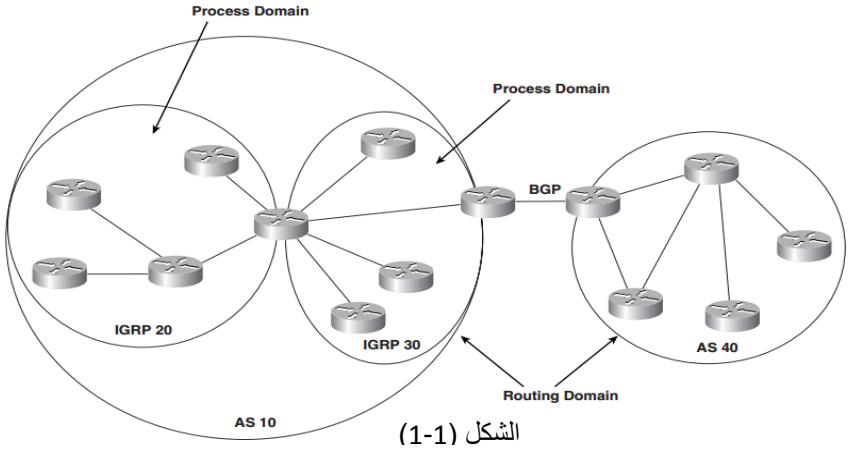
إعداد م/محمد شايع

EIGRP

Process Domain

Process Domain: هو عبارة عن مجموعة من Routers يعمل عليها واحد أو أكثر من (IGP Process) تحت إدارة واحدة (Single Administration domain) أنظر الشكل (1-1).



الشكل (1-1)

EIGRP Concepts

لكي نفهم تكنلوجيا (EIGRP) يجب مقارنتها مع نظيرتها من routing protocols والتي تكون أحد التالي:-

1- Routing by rumor (also called distance-vector) أي التوجية من خلال الشائعات التي تستخدم بواسطة (BGP,IGRP,RIP) والتي تعرف كل المعلومات عن الشبكة من خلال ما يقوم جيرانه بإخباره.
2- Routing by propaganda (also called link-state) التوجية بواسطة الإعلان والتي تستخدم بواسطة (OSPF,IS-IS) والتي كل الراوترات في الشبكة تتشارك معرفتها عن topology للشبكة.

تكنلوجيا (EIGRP) تستخدم (DUAL—Diffused Update Algorithm) والتي تشابه (distance vector protocols)، وبالتالي فإن الراوتر يقوم فقط بإستقبال المعلومات من الجيران المتصلة بشكل مباشرة به لكي يقوم بعملية (routing decisions)، المعلومات المستقبلة تخضع لعملية تنقيح من أجل السرية، وحتى الراوتر المرسل يقوم بعملية التنقيح أيضا قبل الإرسال.

وهنا نورد بعض الميزات التي توجد في EIGRP ولاتوجد في Distance-vector protocols التقليدية:-

1- يقوم EIGRP بتخزين كل المعلومات المستقبلة من كل الجيران في (topology table)، ليس فقط المسارات المفضلة بل كل المعلومات (المسارات) ونستطيع رؤيتها من خلال الامر (show ip eigrp topology)، سنرى كل (the loop-free routes)، لكن في حاله أردنا رؤية كل المسارات حتى التي (not the loop-free routes)، من خلال الامر (show ip eigrp topology all-link).
2- في حالة فقد الوصول إلى (route) معين فإن eigrp تعمل على البحث عن المسار البديل من خلال topology table في حالة عدم وجود مسار بديل يتم إرسال رسائل (queries) إلى كل الجيران، هذا غير متوفر في distance-vector التقليدية التي تنتظر جيرانها لكي تعطيها المعلومات عن المسار، ويتم حذف المسار بعد إنتهاء الوقت، هذه الميزة في EIGRP تجعله سريع في عملية convergence.
3- يستخدم بروتوكول EIGRP (hello packet) لكي يتم معرفته الجيران وإكتشافهم، والبقاء على علاقه معهم.
4- يستخدم EIGRP مايسمى بـ (reliable transport protocol) أو RTP لكي يرسل ويستقبل routing updates والتي تلغى إحتياجنا لعملية إرسال updates بشكل دوري، هذه الميزة تجعلنا نفضل إستخدام EIGRP على غيره من البروتوكولات الذي ينتج عن ذلك توفير في إستخدام link.

Initial IP EIGRP Configuration

فقط لكي نفعل بروتوكول EIGRP نكتب الأمر التالي (router eigrp <as-number>)، أما لتفعيل Interfaces فقط نحتاج لكتابة الأمر التالي (network <major-network>) وبالتالي فكل الشبكات الفرعية التي تنتمى لـ (major network) سوف يتم تحديدها وتفعيلها. بعد عملية كتابة الأمر السابق يتم نقل كل (major network) المعلن عنها إلى Topology table لكي يتم تبادل المعلومات مع الجيران.

ملاحظة:

- يستخدم (as-number) بشكل محلي وليس (globally unique)، أي ليس من قبل ISP، لكن من الممكن إستخدام رقم AS التي تحصل عليه المنظمة من قبل (InterNIC or RIPE).
- تستطيع إستخدام (passive-interface)، التي سنتعرف عليها لاحقاً لكي يتم وقف EIGRP عن interface معين وجميع الشبكات التي تخصه، كذلك تستطيع إستخدام (network major-network mask --.--.--.--) لتحديد الشبكة التي نريد الإعلان عنها فقط.

EIGRP Concepts—Metrics and Distances

لكي يتم إختيار المسار الأفضل يتم إستخدام (metric)، فإنة يوجد نوعين من metrics هما :-

1- the vector metric.

يتضمن هذا النوع ستة عناصر تصف المسافة بين الراوتر والشبكة الهدف ويستخدم بواسطة كل updates والعناصر هي:

- مجموع DELAY من routerإلى الشبكة destination.
- أقل BANDWIDTH على طول المسار إلى الشبكة destination.
- أكبر Load وأقل reliability لأي link على طول المسار إلى الشبكة destination.
- أقل MTU لأي link على طول المسار إلى الشبكة destination .
- Hop count

2- the composite metric.

وهو رقم صحيح ينتج عنة إختيار المسار الأفضل إلى شبكة معينة، وتستخدم (K-values) مع عناصر vector metric لحساب metric لشبكة معينة وهذا يسمى بـ (sometimes distance and composite metric).
ونستطيع إستخدام الأمر التالي لأستعراض شبكة على سبيل المثال (show ip eigrp topology 1.0.0.4 255.255.255.255) لنرى جميع العناصر المكونة للشبكة (1.0.0.4 255.255.255.255).

ملاحظة:

يتم حساب($BW = 10^7/BW_{min}$)، بينما يتم جمع DLY على طول Link ويكون بـ microsecond ولذلك يتم قسمته على (10).
مثلا : sum of DLY=50 وبالتالي يكون DLY=50/10 وبالتالي يكون DLY=5 وهذا يتم التعبير عنه بـ (0x000005)، ويتم التعبير عن عدم القدرة للوصول إلى Route بـ (0xffffff)، وهذا الرقم يقارب s(167.8)، وهذا هو أكبر (DLY)، والجدول أدناه يبين كلا من ($DLY – BW$ and BW_{min}).

Media	Bandwidth	BW_{IGRP}	Delay	DLY_{IGRP}
100M ATM	100000K	100	100μS	10
Fast Ethernet	100000K	100	100μS	10
FDDI	100000K	100	100μS	10
HSSI	45045K	222	20000μS	2000
16M Token Ring	16000K	625	630μS	63
Ethernet	10000K	1000	1000μS	100
T1	1544K	6476	20000μS	2000
DS0	64K	156250	20000μS	2000
56K	56K	178571	20000μS	2000
Tunnel	9K	1111111	500000μS	50000

بالنسبة لـ (Reliability) يعبر عنة بـ (8bits) فعندما تكون القيمة (255 يعني أن (Reliability= 100%)) وعلى العكس = 1.
بالنسبة لـ (Load) كذلك يتم تمثيله بـ (8bits) حيث أن (255 يعني أن load= 100%) أما قيمة 1 فتعني أقل Loadعلى Link.

في حالة تم إستخدام كلا من (Load or Reliability) فإنة يجب عدم وجود أي معدل خطأ في rate أو في channel لانة سوف يسبب في تذبذب في عملة metric لعدم ثباتها (تتغير لحظيا)، ولذلك تم تفضيل عدم إحتسابها من ضمن المعادلة الرياضية.

$$metric = 256 * \left[[(\text{k1} * \text{BWmin}) + \frac{k2 * BWmin}{256 - load} + k3 * DLYsum] * [\frac{k5}{Reliability + k4}]\right]$$

طبعاً (k1 & k3 =1) أما (k2 – k5 - k4 =0) في حالة عدم إستخدام MTU يتم إلغاء $[\frac{k5}{Reliability+k4}]$ من المعادلة. وبالتالي فإن المعادلة تصبح كتالي:

$$metric = 256 * [BWmin + DLYsum]$$

طبعاً (hop count) هي قيمة تتم بواسطة (next-hop routers) وتستخدم فقط لتحديد قطر الشبكة وبشكل إفتراضي تكون تساوي 100، ونستطيع جعلها تساوي 255 عن طريق (metric maximum-hop) ويتم حساب (metric) على outgoing interface

بينما نستطيع تغيير K-values من خلال الأوامر التالية:-

Change EIGRP K-values = metric weights TOS K1 K2 K3 K4 K5

Reset K-values to default values = no metric weights

لكي يعمل EIGRP بشكل صحيح يجب تطابق قيمة (K-values) بين الجيران لأنها أحد العناصر التي ترسل في (Hello packet) ويتم فحصها.

في حالة رغبة في تغيير قيمة K في الشبكة يجب مراعاة التصميم لكي يتوافق مع البروتوكولات الأخرى كما يلي:

1- To emulate RIP, set delays on all interfaces to equal value and set all Ks, except K3, to 0.
2- To emulate OSPF, set interface delay to OSPF cost and set all Ks, except K3, to 0.
3- To select a route with maximum end-to-end bandwidth, set all Ks, except K1, to 0.

لكن في حالة قررت وضع (K-values) كلها تساوي صفر فهذا يعني أن دائما (metric=1)، وهذا يجعل الراوتر يستخدم جميع المسارات المحتملة بعض النظر عن وجود loop فيها.

Computing Vector Metric

لكي نعرف جميع العناصر(vector metrics) لشبكة معينة، فإنها تكون منسوخة من interface ومدرجة في route description في topology table، ونستطيع إستخدام الأمر (show interface s0/0) لمعرفة العناصر المذكورة.

وفيما يلي الجدول التالي يبين القيم الإفتراضية للعناصر:

Default Bandwidth and Delay for Various Interfaces

Interface Type	Bandwidth (kbps)	Delay (microseconds)
Ethernet	10000	1000
Token ring	16000	630
Fddi	100000	100
Serial interface	1544	20000
Low-speed serial interface[1]	115	20000
ISDN BRI	64[2]	20000
ISDN PRI	64	20000
Dialer interface	56	20000
Channelized T1 or E1	n * 64	20000
Async interface	tty line speed	100000
Loopback	8000000	5000

1. Low-speed serial interfaces include WIC on 1600/2600/3600 series, sync/async interfaces on 252x routers, sync/async serial modules on 2600/3600, etc.

القيم الإفتراضية لـ (bandwidth and delay) تبقى في العادة صحيحة في LAN interfaces، بينما على الأقل تميل (bandwidth) لتكون متغيرة في (WAN interfaces). وأحيانا Delay، يجب تحديدها لكل (WAN interface or sub- interface) باستخدام الأوامر التالية:-

Set (sub) interface bandwidth = bandwidth <bw-in-kbps>

Set (sub) interface delay = delay <delay-in-tens-of-microseconds>

ملاحظة:

- التغيير في (bandwidth) في sub-interface يؤثر على (load calculation, EIGRP routing calculations, and EIGRP pacing).
- التغيير في (Delay) في sub-interface يؤثر على (routing calculations EIGRP).
- وضع (bandwidth) المناسبة في (VLAN interfaces) يعتبر أمر عويص وخصوصاً عندما يكون هناك عدة راوترات متصلة إلى نفس (VLAN) من خلال عدة (technologies) مثل (ATM LAN on one end, and Ethernet or Fast Ethernet on the other end)ولذلك يفضل وضع (bandwidth) لقيمة مناسبة تكون متساوية على كل الراوترات المتصلة على نفس (VLAN).

تحسب القيم في (vector metric)، بناء على القيم المستقبلة من الجار وكذلك بناء على قيم interface للراوتر، وتكون كالتالي:

$Delay_{New} = Delay_{Received} + Delay_{Interface}$

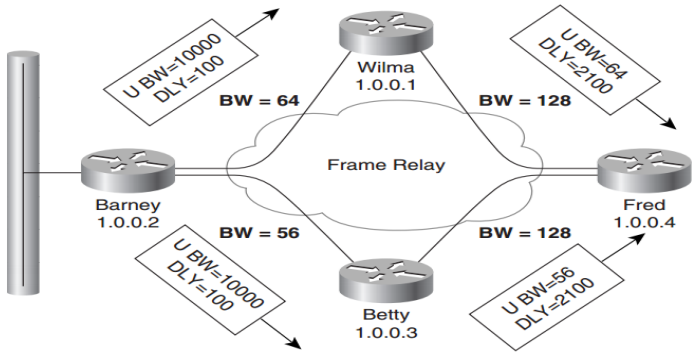
$Bandwidth_{New} = min (Bandwidth_{Received}, Bandwidth_{Interface})$

$MTU\ New = min (MTU_{Received}, MTU_{Interface})$

$Hop\ Count_{New} = Hop\ Count_{Received} + 1$

تيم تخزين القيم في (Topology table)، ويتم تعديل القيم بناء على القيم (Inbound) وليس بناء على (outbound).

المثال التالي يوضح المفهوم:

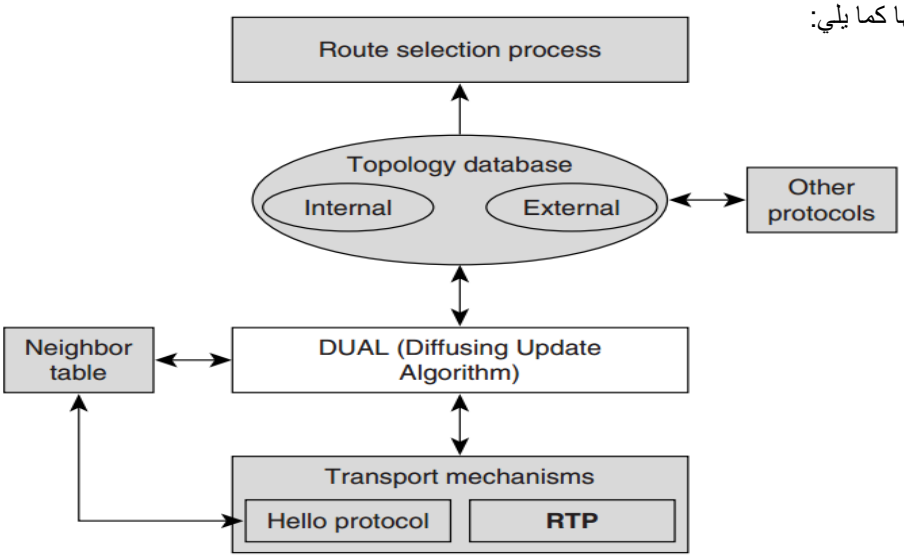


عندما يعلن Barney علن الشبكة المحلية المتصلة من خلال frame-relay نرى أن (Barney) أعلى لكلا من (Betty , Wilma) عن BW=1000 وكذلك DLY=100، بينما قام (Betty) بإختيار أقل Bandwidth وأعلى عنها لـ (Fred) وهي BW=56 بينما جمع DLY = 2100 ، وكذلك الحال مع (Wilma) أعلن عن BW=64 بينما جمع DLY = 2100.

DUAL—The Heart of EIGRP

الخوارزمية المركزية في EIGRP هي (DUAL) والتي تعتمد على بروتوكولات مثل (the reliable transport protocol and hello protocol) وعلى بنية البيانات الموجودة في (topology table and Neighbor table)، لتزود الراوترات بكل المعلومات لكي تختار أفضل مسار لها.

والشكل التالي بين الارتباط بينها كما يلي:

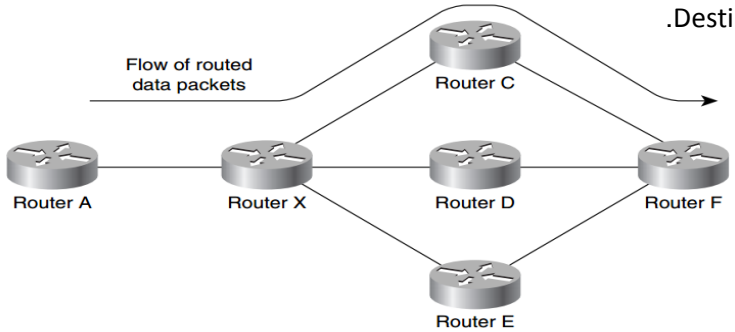


DUAL Terminology

Upstream and Downstream Routers

دعني أشرح ذلك من منظور router X حيث
يعتبر router c هو (downstream)، بينما يعتبر router A هو (upstream).

- وبالتالي فإن ((The downstream router (for a subnet) هو الراوتر الذي يكون أقرب إلى destination subnet من الراوتر الحالي المستخدم لتوجية البيانات إلى Destination subnet.
- وبالتالي فإن ((The upstream router (for a subnet) هو الراوتر الذي يكون أبعد إلى destination subnet من الراوتر الحالي المستخدم لتوجية البيانات إلى Destination subnet.

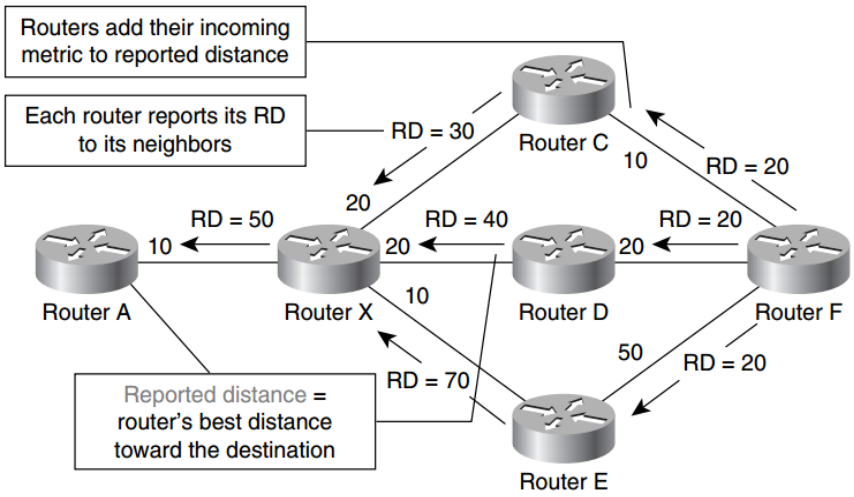


Reported Distance and Feasibility Distance

كل (EIGRP router) يستخدم (topology table) لكي يختار أفضل مسار إلى كل (destination) في الجدول. (vector metric) لأفضل مسار بناء على رؤية الجارترسل إلى الراوتر. أما ((composite metric (or distance)) للمسار المحدد يسمى بـ ((reported distance(RD)).

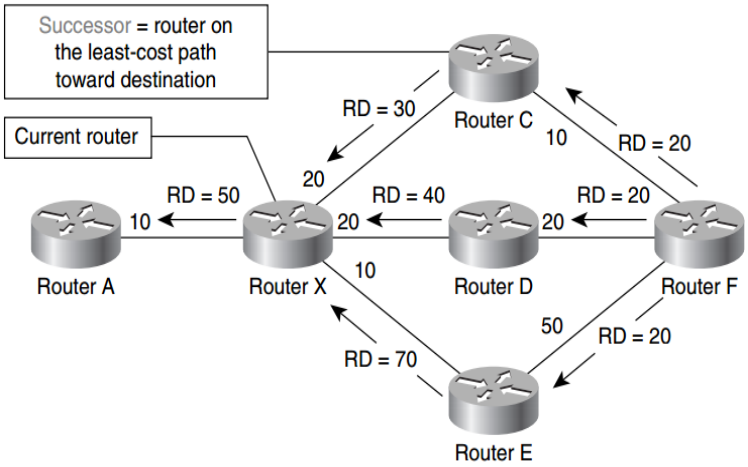
RD: - هي أفضل مسار إلى شبكة معينة بالنسبة للجار.

يقوم بعدها الراوتر بإضافة (composite distances) الخاصة بـ interface المتصلة بالجار المعلن عن RD ليشكل مايسمى بـ (Feasible Distance(FD)).



Successor

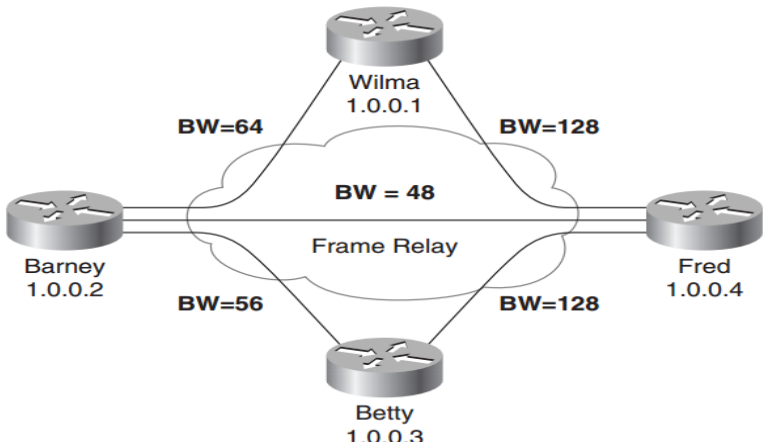
وهو راوتر (next-hop) في إتجاة downstream ويعتبر جار للراوتر الحالي ويعتبر أُقرب جار لشبكة معينة.



Feasible Successor

عندما لايكون الجار (Successor) ربما ليس دائما يكون ((feasible successor (FS)، وهو مسار إلى شبكة معينة لا يعد أفضل مسار ولكن يضمن (loop-free)، أي أن (AD) للمرشحين (FS)، تكون أقل من FDوهذا يسمى بـ (FC(Feasible Condition.

Simple DUAL Operation—Adding New Routes



ما الذي يحصل عندما نضيف التالي:

```
Barney(config)#interface loopback 1
Barney(config-if)#ip address 1.0.0.5 255.255.255.255
```

عندما يتم إضافة الشبكة أعلاه إلى شبكات EIGRP تحصل الخطوات التالية:

1- يتم وضع route في الصف على الـ Interface المحدد لأرساله للجيران.
2- يتم وضع update أي route الناتج من الخطوة الأولى في packet لتجهيزه للأرسال من خلال interface.
3- يتم إرسال packet للجيران الموجودين في neighbor table القادر للوصول لهم.

نستطيع تتبع ذلك من خلال الاوامر التالية: (debug eigrp packet query update reply) وكذلك من خلال الأمر (debug eigrp fsm).

Basic DUAL Rules

1- القاعدة (1) لـ DUAL: في أي وقت يختار الراوتر (new successor) فإنة يخبر جميع الجيران عن (new reported distance) الجديدة.
2- القاعدة (2) لـ DUAL: كل وقت يختار الرواتر (successor)، يرسل (poison update) إلى ((successor (a poison reverse) الخاص به.
3- القاعدة (3) لـ DUAL: الـ (poison update) يرسل إلى كل الجيران على interfaces من خلال (successor) في حالة إغلاق خاصية (split-horizon)، وإلا سيتم الإرسال فقط للـ (successor).

DUAL Behavior on Route Loss

دعنا نضع كود بسيط يحاكي ما الذي يحصل أثناء إستقبال أي route بمسار أفضل أو route جديد:

```
Receiving update packet:
  Install information in topology table
  If ReceivedUpdate is better or equal than the current best route then
    Select the new best route
    Send update packets to all neighbors
  Else
     ????
  End If
```

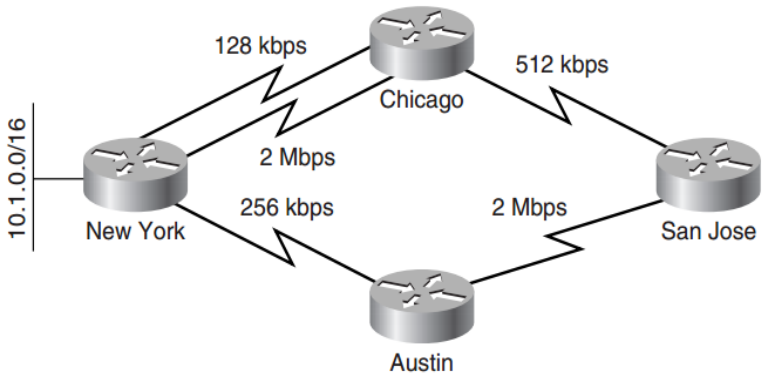
الكود التالي يبن بشكل أكبر ما الذي يحدث في الكود السابق:

```
Receiving update packet:
  Install information in the topology table
  If ReceivedUpdate is better or equal than the current best route then
    Select the new best route
    Send update packets to all neighbors
  Else
    If ReceivedUpdate was not received from current successor then
    Store the information in topology table, ignore the update
    Else
      Try to find a better route
    End If
  End If
```

إعداد م/محمد شايع
قبل الخوض في التفاصيل يجب الإجابة عن التالي:

1- لماذا يجب على EIGRP أن يحاول البحث عن مسار أفضل كل مرة successor يرسل تحديث بزيادة في metric.
2- كيف يتعامل الـ EIGRP في route loss معين.
3- كيف يعالج EIGRP الأحداث في حالة (link failure) أو في حالة (neighbor loss).

للإجابة على الأسئلة السابقة نأخذ المثال التالي:



بالنسبة للسؤال الأول نأخذ السيناريو التالي:

في حالة أن link = 2Mbps مابين (Chicago) و(New York) انقطع (fail)، فإن الرواتر (Chicago) سوف يستخدم link = 128 kbps، ثم سيخبر (San Jose)، ففي حالة قرر (San Jose) إستخدام نفس المسار الذي يستخدمه (Chicago) للوصول إلى (New York) فإن المسار الأخر من خلال (Austin) سيكون هو الأفضل لأن الـ (metric) هي الأفضل.

للأجابة على السؤال الثاني والثالث نأخذ التالي:

1- عندما يفقد الراوتر أي route يقوم بإرسال update عادي لجميع الجيران يحوي على route لكن في قسم (-1) delay = infinity.
2- في حالة كان route المفقود تم معرفته من خلال مصدر خاري (redistributed into EIGRP) فإنة يعامل بنفس طريقة الشبكة الفرعية المتصلة.
3- طبعا في حالة فقدان الوصول الى link فإنة سيفقد الوصول إلى (neighbor) المتصل من خلال link وسيعامل بنفس الطريقة السابقة.
4- في حالة (neighbor loss) فإنة سوف يتم إرسال update يحتوي على ((-1) delay = infinity) لجميع routes التي تمت معرفتها من خلال neighbor.

نستطيع تتبع ذلك من خلال الاوامر التالية: (debug eigrp packet query update reply) وكذلك من خلال الأمر (debug eigrp fsm).

Local Computation

عندم الـ link لأي راوتر إلى destination معين يتغير إلى down وكان هذا router هو successor فإنة يتم البحث عن Feasible Successor في حالة وجد فقط يتم نقل هذا route من topology table إلى routing table ويظل destination في حالة passive أي لا يحدث أي (diffusing computation)، طبعاً يتم إرسال update بذلك إلى الجيران، والشكل التالي يوضح مايحدث بطريقة code.

```
Try to find a better route:
  Find the new best route in topology table
  If NewBestRoute goes through a feasible successor then
    Select the NewBestRoute
    Send update packets to all neighbors
  Else
    Ask other neighbors about an alternate route
  End If
```

Diffusing Computation

ما الذي يحدث في حالة لم يجد (EIGRP router)، مسار بديل أو (FS)، طبعاً يبدا بتشغيل خوارزمية تسمى (diffusing computation) عن طريق سؤال كل الجيران عن مسار بديل للـ route.

ويتم تنفيذ الـ (Diffusing computation) في الخطوات التالية:

1- يتم وضع علامة (Active) في topology table أما route الذي سيتم البحث عن مسار بديل للوصول له، وجود هذه العلامة بغرض منع حدوث loop، يتم تحديد زمن معين لكي يرد كل الجيران على query.
2- يتم إنشاء جدول يسمى بـ (reply-status table) لتتبع (replies) الذي يصل من الجيران.
3- يتم إرسال (query) إلى الجيران وذلك بسبب التالي:
   - New neighbor
   - Change in cost مثل تغيير في bandwidth
   - Link failure
4- يتم تجميع الرد من كل الجيران و يتم تخزينه في (topology table)، ويتم تدوين حالة الرد لكل جار على حده في (status table reply).
5- يتم إختيار أفضل رد من (topology table) ويتم وضع (the new best route) في (the routing table).
6- إذا كان ضروري يتم إرسال (update) إلى الجيران لإخبارهم عن التغيير الجديد في (network topology).

Receiving a Query Packet and Responding to It

يعمل الراوتر على إستقبال (query packet) باستخدام القواعد الموضحة في الجدول لمعالجة query:

Action Taken upon Receiving an EIGRP Query

Condition	Action
Route not in topology table	Reply with infinity.
Route already active	Reply with current best metric (could be infinity).
Query received from nonsuccessor	Reply with current best route.
Query received only from successor, no other EIGRP neighbors	Reply with infinity.
Query received from successor	Select new best route. If it goes through a feasible successor, reply with new best route, otherwise extend diffused computation.

بالإضافة إلى ماسبق في الجدول في حالة أن الرواتر وصله (query) عنroute محدد كان هو قد أرسل (query) لنفس الـ route فإن المعلومات الجديدة هى التي سوف تعتمد عوضا عن المعلومات السابقة.

Finishing a Diffusing Computation

في حالة بدأت عملية إرسال query فإنه سوف يبدا الرواتر في إستقبال reply من الجيران ويتم تخزين المعلومات في topology table ويتم وضع علامة في الجدول المسمى (reply table)، بعد إكتمال عملية إستقبال جميع (reply) عن كل query تبدا عملية (diffusing computation)، لجميع البيانات المستقبلة وبعد الإنتهاء من العملية، تبدا عملية (computation) لإختيار أفضل مسار بناء على النيجة المسبق حسابها، ويتم إعلام الجيران بعد ذلك بنتيجة (computation)، أي best route، وكذلك إختيار downstream router المناسب.

Monitoring Diffusing Computation

تستطيع مراقبة (Diffusing Computation) بعدة طرق هي:

1- في الشبكات الصغيرة نستطيع إستخدام (EIGRP debugging commands).
2- إستخدام (EIGRP event log in the router)، وذلك لفهم عملية (Diffusing Computation).

3- إستخدام أوامر مثل (commands and show ip eigrp neighbor show ip eigrp topology).

الجدول يعطينا إيضاح أكثر عن الأوامر المستخدمه لهذا الغرض:

Commands Used in Diffused Computation Monitoring

To Display . . .	. . . Use the Following Command
Routes currently under diffused computation	**show ip eigrp topology active**
Routes currently being converged	**show ip eigrp topology pending**
Whether this router is a potential bottleneck	**show ip eigrp neighbor detail**

بعد عملية إرسال (query) إلى (neighbors) قد تحدث مجموعة من المشاكل والتي هي:

1- في حالة وجود عدد كبير من (active routes) فإنة يشير إلى (route flaps and network instabilities).
2- عندما يطول وقت (active times) فإنة يشير إلى بطء في (network convergence) وإحتمال وجود bottlenecks (routers that don't reply to queries).
3- عندما يطول (active times) المستقطع في الإنتظار لـ (reply) من عدد قليل من الجيران فإنة يشير أيضا إلى وجود bottlenecks (routers that don't reply to queries)، أو وجود مشكلة في الإتصال مع الجيران.
4- عندما يطول (active times)المستقطع في الإنتظار للـ (reply) من عدة جيران فإنة يشير إلى interface bottleneck or a highly redundant topology.

Stuck-in-Active Routes

طبعا في ما سبق تعرفنا عندما يصل الراوتر query فإنة يرد بـ reply لكن هناك عدة حالات ربما يفضل الراوتر في الرد بـ reply هي:

1- في حالة أن الجار في حالة (failure or shutdown) في نفس لحظة إرسال query.
2- في حالة كانت media في حالة (congestion or overload) في نفس لحظة الإرسال.
3- في حالة كانت هناك error في (software or hardware).

في الحالات السابقة فإن الراوتر يتوقف من مواصلة (diffusing computation) لكي يكمل عملية (computation)، ولكي نمنع مثل هذه الحالات فإن EIGRP يقدر وقت كحد أقصى لإكتمال الـ (diffusing computation).

في حالة إنتهي الوقت المحدد تتم مقاطعة عملية (diffusing computation)، ثم تقطع العلاقة مع الجيران التي لم تستجيب بإرسال reply، وتسمى الجيران التي لم ترسل reply بإنها دخلت في حالة (stuck in active(SIA)).

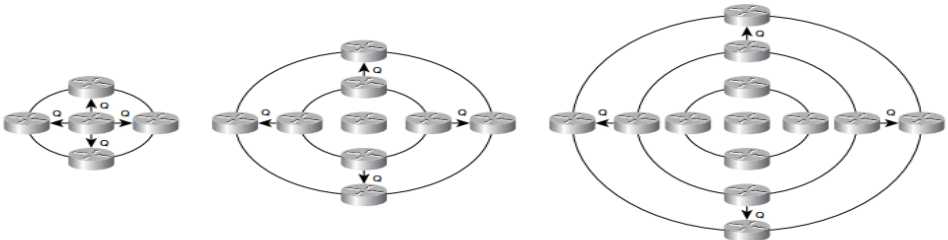
وتعتبر المدة التي ستنتظرها الرواتر حتي تصل إليه reply هي (3 دقائق)، وإلا سيعلن عن الجار الذي لم يرسل reply أنه (Dead)، وفي الجدول أدناه نستطيع تعديل الوقت (SIA) من خلال الأوامر التالية:

Changing the SIA Timeout

Task	Command
Change the Stuck-in-Active timeout	**router eigrp <AS>** **timers active-time <timeout-in-minutes>**
Disable the Stuck-in-Active check	**router eigrp <AS>** **timers active-time disabled**

SIA عادة يصاحبه عدة (route flaps) ، أو فقدان عدة routes مع (slow-speed or lossy links) في الشبكات الكبيرة وهذة الأسباب تصنف إلى:

1- (Flapping interface) طبعا عندما (interface) ينتقل إلى حالة (down)، كل الراوترات في الشبكة ترسل query في حالة عدم وجود route بديل، طبعا تزداد (queries) في الشبكة وهذا يسبب بـ (SIA timeout).



2- (Configuration change): في حالة تغيير في الإعدادات يتم مسح علاقة الجوار بين الرواتر الذي تم تغيير إعدادته وبين جيرانه، وهذا يتسبب في حالة كانت الشبكة (low-speed media) في الدخول في حالة SIA.
3- (Heavily loaded links) في حالة الحمل الزائد على Link فإنة يتسبب في إعادة الإرسال لمرات عديدة وهذا يدخل الراوتر في حالة (SIA).
4- (Misconfiguration of the bandwidth parameter) طبعا الإختلاف في BW يؤدي إلى وجود خط يحمل BW عالى والآخر يكون أقل مما يتسبب في وجود query بشكل كبير وهذا يدخل الرواتر في حالة SIA.
5- (Old EIGRP code) طبعا يجب مراعاة إصدار IOS للتوافق بين الأوامر.
6- Frame-Relay.

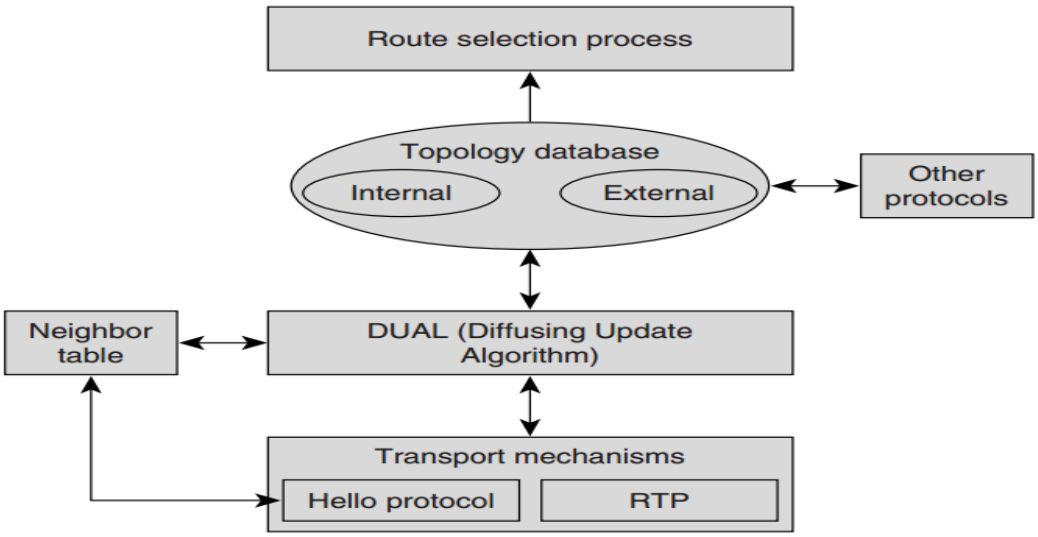
EIGRP Transport Mechanisms and Protocols

عند التراسل بين الجيران في EIGRP فإن بعض البيانات يجب أن تسلم بشكل (Reliable Transport Protocols (RTP))، هذا يقودنا إلى أنه يوجد إختيارين لدى مصممي (EIGRP transport protocol) هما :

1- إختيار برتوكول موجود يستخدم (RTP) طبعا على سبيل المثال هو (TCP).
2- تصميم بروتوكول خاص يقوم بعملية RTP.

الخيار الأول لن يجدي بسبب أن بروتوكول EIGRP لابد من إستخدام بعض الميزات مثل (multicast data delivery)، وبالتالي لم يبقى سوى الخيار الثاني.

Overall Map of EIGRP Processes, Protocols, and Data Structures



طبعاً (EIGRP transport protocol) يحقق التالي:

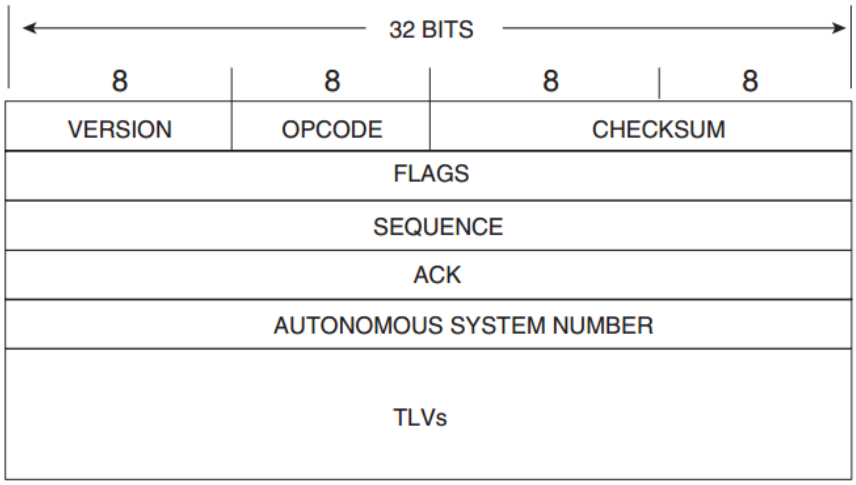
1- يتم إكتشاف الجيران بشكل ديناميكي بإستخدام (EIGRP hello protocol).
2- كذلك (hello protocol) يكتشف (neighbor loss).
3- جميع البيانات تنقل بشكل (reliable).
4- يتم نقل البيانات إما (unicast) أو (multicast).
5- (transport protocol) يعمل على مؤامة التغير في (network conditions) لكي يتناسب مع الجيران.

6- مع (proper configuration)، فإن EIGRP يخفض في إستخدام (bandwidth)، يصل في حالة أعلى درجة فقط سيتم تخصيص 50% من BW لبيانات EIGRP فقط.

EIGRP Encapsulation Methods and Packet Format

The EIGRP Packet Header

كل EIGRP Packet سوف يستخدم (common header) المبين في الشكل أدناه،



وفيما يلي توضيح للحقول الخاصة بـ (*Header Field*):

1- *Version*تحدد إصدار خاص من *(Originating EIGRP Process)* وهذا لايتغير.

2- *Opcode* : موضح في الجدول المقابل.

EIGRP packet types.

Opcode	Type
1	Update
3	Query
4	Reply
5	Hello
6	IPX SAP
10	SIA Query
11	SIA Reply

3- *Checksum* تعمل على فحص كامل *EIGRP Packet* ماعدا *IP header*.

4- *Flags* تشير في حالة كان (*0x00000001*)إلى أنه أول *route* يتم إرسالة إلى (*new neighbor*).

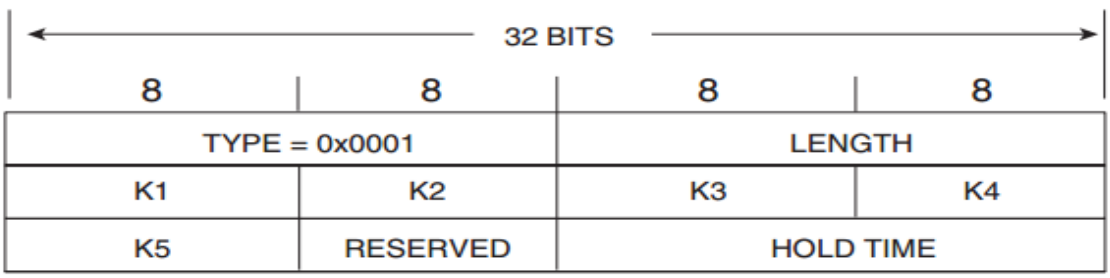
5- *Sequence* وهو عبارة عن *32bit* يشير إلى الرقم التسلسلي الذي يستخدم من قبل *RTP*.

6- *ACK* وهو عبارة عن *32bit* تشير إلى التاكيد على أخر باكيت تم إستقباله، وهو عبارة عن *hello packet* بدون اي بيانات، ودائما يكون *unicast*.

7- *AS* ويشير إلى (*number of the EIGRP domain*).

8- *TLV* وتشير إلى (*Type/length/Value*)، وهو عبارة عن (*2bytes*) لكل من *type* وكذلك (*2bytes*) لـ *Length*، بالإضافة إلى معلومات أخرى، يشمل :

EIGRP Parameters TLV.



Hello Packet

يقوم *hello packet* بالوظائف التالية:

1- يعمل على إكتشاف وجود جار جديد.
2- يحمل مجموعة من الحقول من خلالها تتم التأكد من قبول الجار أو لا.
3- يعمل على مراقبة الجيران للتحقق من فقدان جار من خلال إرسال الرسائل بشكل دوري.

طبعا تتم الإرسال للـ (*hello packet*) في (*unidirectional protocol*) بشكل *multicast* في كل الإتجاهات، كذلك يحمل المعلومات الاساسية عن الراوتر الذي أرسل الباكيت:

a. *Its IOS version and EIGRP code version*
b. *The K-values the router is using*
c. *The hold time that should be used to detect neighbor loss*

بعد وصول (*hello packet*) إلى الرواتر يعمل على فحص (*K-values*) التي لابد أن تتطابق مع (*K-values*) التي لديه، كذلك تتم فحص (*source address*) والذي لابد أن يكون من نفس *subnet*.

طبعا تتم عملية الإرسال من (*primary IP address*) التي لابد أن تتطابق (*primary IP address*)، وليس مهم مع (*secondary*)، لانة عملية الجوار من شروطها فحص (*primary IP address*).

يستخدام (*hello protocol*) وقتين (*two timers*) لفحص (*neighbor loss*)، هما:

1- *Hello interval* والذي يعني كم من الوقت يلزم مابين إرسال *hello* والتي تليها.
2- *Hold time* والذي يعني كم من الوقت ينتظر الرواتر طالما أنه لم يستقبل (*hello packet*) قبل أن يعلن عن (*neighbor dead*).

وطبعا يعتمد الوقت على (*interface and encapsulation*).

والجدول التالي يبين الوقت كما يلي :

Default EIGRP Hello and Hold Timers

Interface Type	Encapsulation	Hello Timer (sec)	Hold Timer (sec)
LAN interface	Any	5	15
WAN interface	HDLC or PPP	5	15
	NBMA interface (X.25, Frame Relay, SMDS or Dialer) with bandwidth <= T1	60	180
	NBMA interface with bandwidth > T1	5	15
	Point-to-point subinterface over NBMA interface	5	15

ولكي نغير في (*hello timer*) وكذلك (*hold timer*) من خلال الأوامر التالية:

Changing the Hello and Hold Timers

To Change . . .	. . . Use the Following Command
EIGRP/IP hello timer	**ip hello-interval eigrp <as> <seconds>**
EIGRP/IP hold timer used by other routers to detect this router's failure	**ip hold-time eigrp <as> <seconds>**

وكذلك نستطيع إغلاق (*hello*) لكل *interface* من خلال الأوامر التالية:

Disabling and Enabling EIGRP Hello Protocol on a Per-Interface Basis

Task	Command
Disable EIGRP hello protocol on a single interface	**router eigrp <as>** **passive-interface <interface>**
Re-enable EIGRP hello protocol	**router eigrp <as>** **no passive-interface <interface>**

نستطيع إستخدام (*passive-interface*) فقط يستخدم مع (*Interfaces*) التي عناوينها تقع داخل الشبكة المحددة بواسطة (*EIGRP routing process*).

ويؤثر (*command passive-interface*) على التالي:

1- لا يتم عمل أي علاقة جوار مع أي *interface* يحمل أمر *passive*.
2- لا يتم إرسال أي *updates* من خلال *passive interface*.
3- الـ (*subnet*) في (*passive interface*) يبقى في (*EIGRP process*) ويظهر في (*EIGRP topology table*) على أنها (*internal route*).

Monitoring EIGRP Hello Protocol

ليس من السهل مراقبة *Eigrp hello protocols* لكن لكي نحدد بالضبط جار معين نستجدم الأوامر التالية:

1- *Debug eigrp packet hello*
2- *Debug ip eigrp neighbor 10.1.1.1*
3- *service timestamps debug datetime msec*

ولكي نعرض معلومات عن *hold time* لكل جار على حدة يجب إستخدام الأمر التالي:

Show ip eigrp neighbor

Reliable Transport Protocol

RTP يضمن تبادل بيانات التوجية في *EIGRP* بين الجيران باستخدام تقنية مثل (*sequencing, ack, retransmission, flow control*)، وطبعا من الجدول التالي نفند أنواع *packet* وطبيعة الإرسال.

Unicast and Multicast EIGRP Packets

Packet Type/Reliability	Unreliable	Reliable
Unicast	ACK	Reply IPXSAP Response
Multicast	Hello	Update Query IPXSAP Flash Update IPXSAP General Query

ولكي نعرف هل تم الإرسال *unicast* تكون عملية *enqueued* للـ *interface*

multicast تتم من خلال *Un/reliable mcasts* فإن كانت القيمة غير الصفر فإن عملية الإرسال *multicast* وإلا فإنها تكون *unicast*

```
Un/reliable mcasts: 0/0 Un/reliable ucasts: 13/41
```

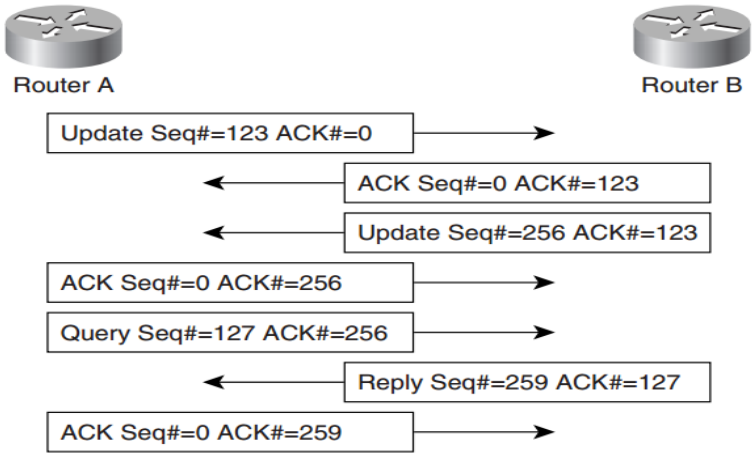
Sequence Numbers and Acknowledgments

كل (*reliable transport protocol*) يجب تنفيذ عملية (*sequencing and sequence numbers*) لكي تتم معرفة (*lost packets*) لكي تتم عملية إرسالها وكذلك ترتيبها وقد تتم من خلال إحدى التقنيات التالية:

1. *Use different sequence numbers for unicast peer-to-peer flows and multicast peer-to interface flows.*
2. *Use the same sequence numbers for all packets, but accept that the sequence numbers received by the peer are nonsequential.*

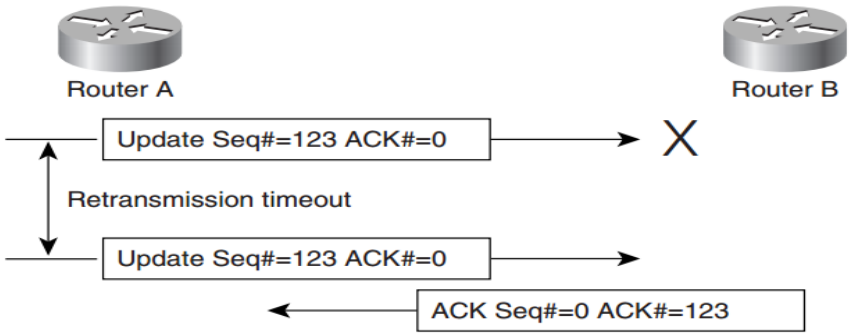
ومن خلال الشكل التالي نستطيع ملاحظة كيف تتم إرسال (*sequence number*):

Simple RTP Sequencing and Acknowledging



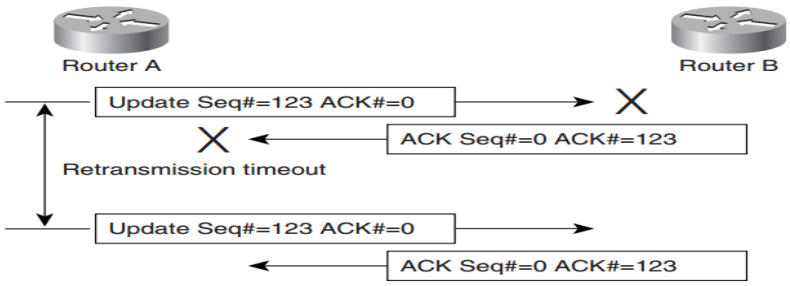
Retransmissions and Retransmission Timers

في حالة تم إرسال *Update* ولم يصل فسوف ينتظر المرسل وقت معين ثم سيعادو إرسال نفس*Update* والشكل التالي يوضح ذلك.



عملية إعادة إرسال *Update* سوف ينطبق في حالة لم يصل *ACK* فسوف يفترض المرسل عدم وصول *Update* فسوف يعاد إرسال *Update* مرة أخرى وطبعا المستقبل سيرى وجود نسختين من نفس *Update* وذلك من خلال حقل *Sequence* ولذلك سوف يأخذ نسخة واحدة ويتجاهل الثانية والشكل التالي يوضح ذلك.

RTP Recovery after Acknowledgment Loss



يسمى الوقت الذي سوف ينتظره الراوتر بـ (*retransmission timeout (RTO)*)، بينما الوقت الذي سوف يأخذه *Update* قبل وصول *ACK* يسمى (*Round Trip Time (RTT)*)، كما يوجد وقت يسمى بـ (*Smoothed Round Trip Time (SRTT)for every neighbor*).

ومن المهم أن ننوه على أن (*RTP*) لن يستمر إلى ملا نهاية في إنتظار التأكيد أو إعادة الإرسال لكن بعد *16* محاولة فسيتم إعلان أن الجار في حالة (*Hold time*) أي أن الجار (*dead*).

ومن خلال الأمر نستطيع ملاحظة جميع الرموز السابقة من خلال الأمر:

Show ip eigrp neighbors

من الأمر السابق نلاحظ أن التالي أن (*RTO =SRTT*×6).

لكن من خلال الأمر التالي (*show ip eigrp neighbor details*)، فإننا نستطيع ملاحظة كم مرة تم اعادة الإرسال من خلال (*retans*)، أما (*retries*) فيعبر عن عدد المحاولات في إعادة الإرسال.

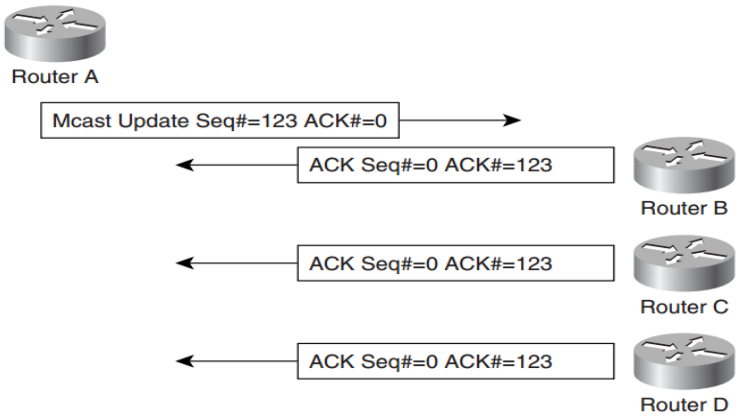
ولكي نرى معدل الإرسال من كل *interface* نستطيع رؤيته من خلال الأمر (*show Ip eigrp interface*).

Mixed Multicast/Unicast Operation

في حالة إرسال (*packet*) بطريقة *multicast* تتم من خلال أن الراوتر يتتبع من الذي أرسل *ACK* ومن لم يرسل حيث أن الجار الذي لم يرسل *ACK* سيتم إعادة إرسال *packet*، هذا التحويل من *multicast* إلى *unicast*

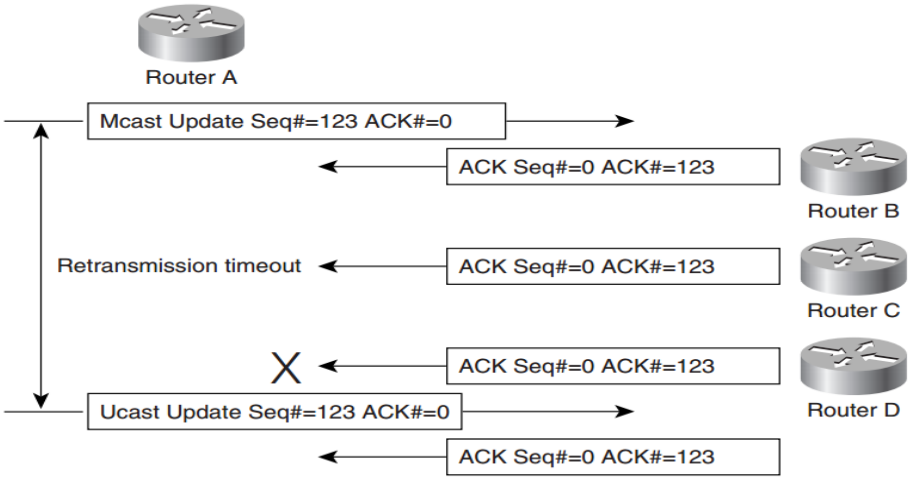
في الشكل التالي إفترض أنه تم إرسال *updates* من *A* إلى *B,C and D* بطريقة *multicast* وتم الرد من الجميع ولكن *ACK* القادم من *D* لم يصل.

Sample Multicast Transmission with Proper Acknowledgments



هنا سوف تتم إعادة إرسال *update* فقط بطريقة *unicast* إلى راوتر واحد فقط وهو *D*.

Multicast Transmission with Unicast Retransmission



طبعا سوف ينتظر *router A* حتي ينتهي *(RTO)* وسوف يعاود إرسال *unicast packet* إلى *router D*، ونستطيع مراقبة كم مرة تمت إعادة الإرسال بطريقة *multicast* أو *unicast* من خلال الأمر التالي: (*show ip eigrp interface details*).

EIGRP Neighbors

نستطيع متابعة ومراقبة الجيران من خلال الأوامر التالية:

Enabling EIGRP Neighbor Debugging and Logging

Task	Command
Debug EIGRP neighbor events	**debug eigrp neighbor**
Log adjacency establishments and losses	**router eigrp <as>** **eigrp log-neighbor-changes**

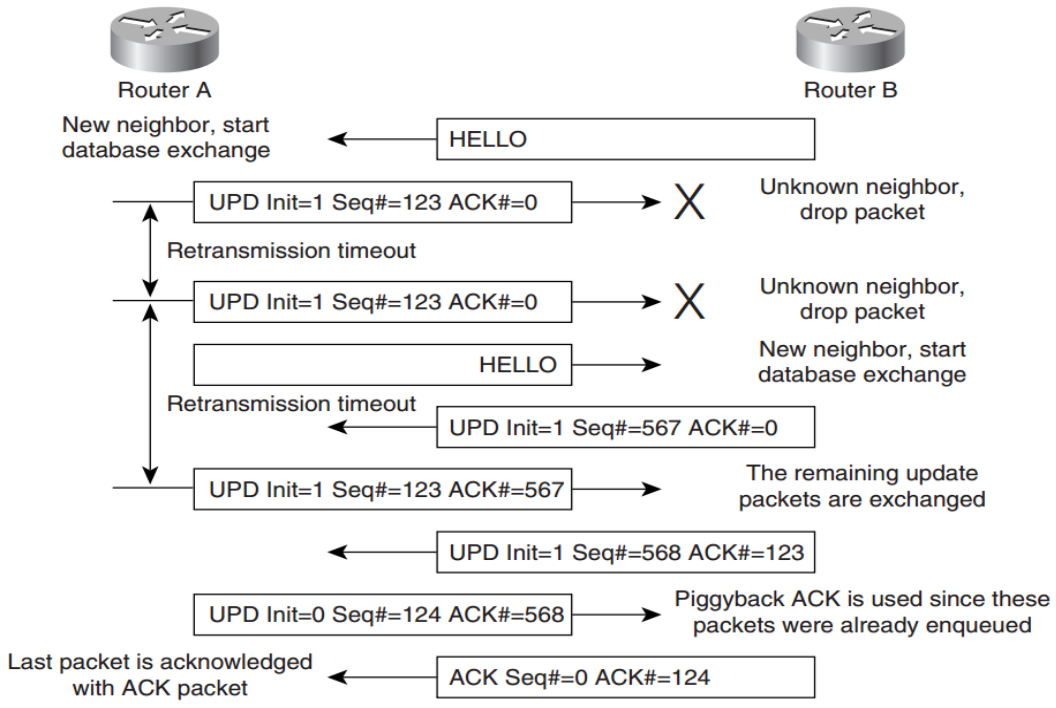
Discovering New Neighbors

من خلال *hello packet* نستطيع إكتشاف الجيران كما سبق وتتم إرساله بطريقة *multicast* من خلال كل *Interfaces* التي تم تعريف *EIGRP process* عليها.

Initial Topology Table Exchange

بعد عملية إكتشاف وجود جار ومطابقة *hello packet parameters* مع الجار تبدا مرحلة محاولة تبادل *topology table* والتي يشار إليها بـ *INIT* في أول حقل *update* يتم إرساله إلى الجارالجديد، الشكل التالي عبارة عن صورة توضيحية للسيناريو الذي يحدث بين الراوتران.

Initial Database Exchange—Typical Scenario



ونستطيع مراقبة ذلك من خلال الأمر التالي:

debug eigrp packet hello

Adjacency Resets—Causes and Consequences

في حالة (*Hello Protocol*) من الممكن نرى بعض الأسباب التي تدفعنا إلى (*adjacency resets*)، والجدول التالي يوضح بعض الأسباب.

Various Reasons to Reset EIGRP Adjacency

Action	Effects on EIGRP Adjacencies
No packets are received from the neighbor within *hold timer*.	Neighbor is declared dead (see the section "Hello Protocol").
A single reliable packet is retransmitted at least 16 times and for a period larger than the *hold timer*.	Neighbor is declared dead (see the section "Retransmissions and Retransmission Timers" for additional details).
The interface goes down (line down or line protocol down).	All neighbors reachable over that interface are declared dead.
The interface is shut down by an operation action.	Same as the previous entry.
A network is removed from EIGRP process.	All neighbors belonging to that network are declared dead.

في حالة تمت (*adjacency reset*) فإنة سوف ينتج عنه التالي:

1. *The neighbor (or several neighbors) is removed from the neighbor table and EIGRP loses all information about that neighbor.*
2. *A link down()event is generated for the neighbor. All the routes received from the neighbor are removed from the topology table and either local or diffused computation is started for all those routes where the now-dead neighbor was the successor.*

وهنا بعض الأوامر التي نستخدمها في العملية:

Commands Used to Clear EIGRP Neighbors

To Clear Adjacency with . . .	. . . Use the Following Exec Command
A single IP neighbor	**clear ip eigrp neighbor** <ip-address>
All IP neighbors reachable over one interface	**clear ip eigrp neighbor** <interface>
All IP neighbors of all EIGRP processes	**clear ip eigrp neighbor**

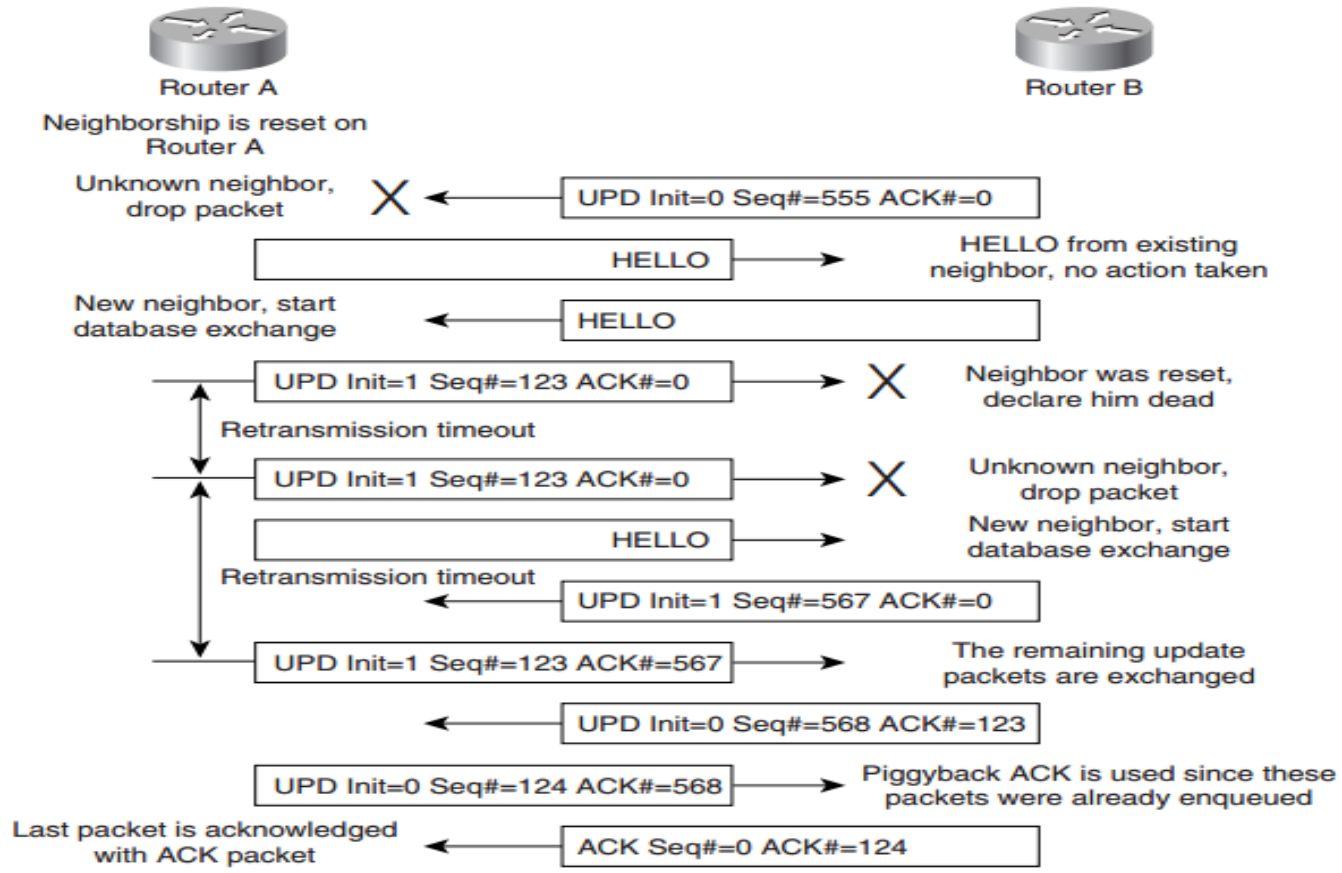
وفيما يلي بعض التغيرات التي تحدث عملية (*adjacency reset*).

Configuration Changes That Can Cause EIGRP Adjacency Resets

Configuration Change	Effect on EIGRP Adjacency
Change in interface bandwidth, delay, or MTU size	All neighbors reachable over that interface are reset
EIGRP split horizon is configured on the interface	
EIGRP summarization is configured on the interface	
IP, IPX, or AppleTalk address of the interface is changed	
Interface is configured as **passive-interface**	
Per-interface **distribute-list in** or **distribute-list out** is configured or removed	
ACL referenced in per-interface **distribute-list** is changed	
Autosummary is configured or removed	All adjacencies of the EIGRP process are reset
metric maximum-hop is configured	
Per-process **distribute-list in** or **distribute-list out** is configured	
ACL referenced in per-process **distribute-list** is changed	

في حالة تم عمل (*adjacency reset*) فإنة الراوتر يقوم بعملية إزالة الجار من (*neighbor table*) ولايخبر جاره عن ذلك وتستمر عملية إستقبال (*data receiving*)، لكن تتم عملية حذفها لأنها تأتي من حار غير معروف، والشكل التالي يبين ذلك:

Recovery from Operator-Initiated or IOS-Triggered Adjacency Reset



Monitoring EIGRP Neighbors

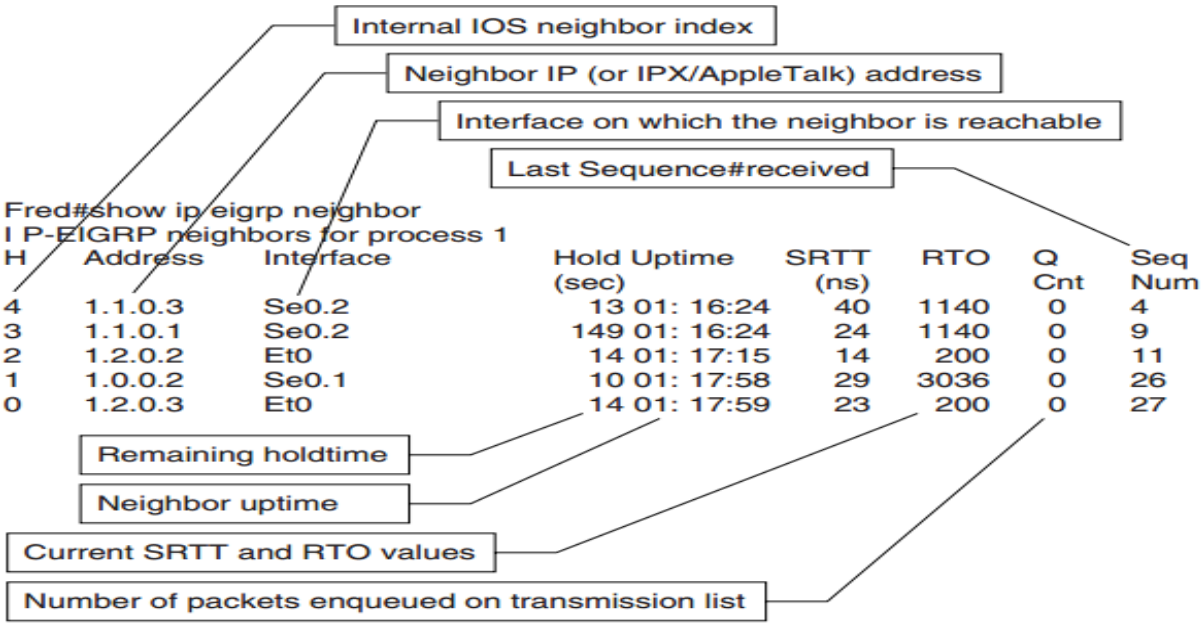
نستطيع عمل مراقبة للـ *(EIGRP)* من خلال بعض الأوامر الموضحة في الجدول:

IOS Show Commands Used to Display the EIGRP Neighbor Table

To Display . . .	. . . Use the Following Command
Summary information on all neighbors	**show ip eigrp neighbor**
Detailed information on all neighbors	**show ip eigrp neighbor detail**
Summary information on neighbors belonging to one EIGRP process and/or reachable over one interface	**show ip eigrp neighbor [<as>] [<interface>]**
Detailed information on neighbors belonging to one EIGRP process and/or reachable over one interface	**show ip eigrp neighbor detail [<as>] [<interface>]**

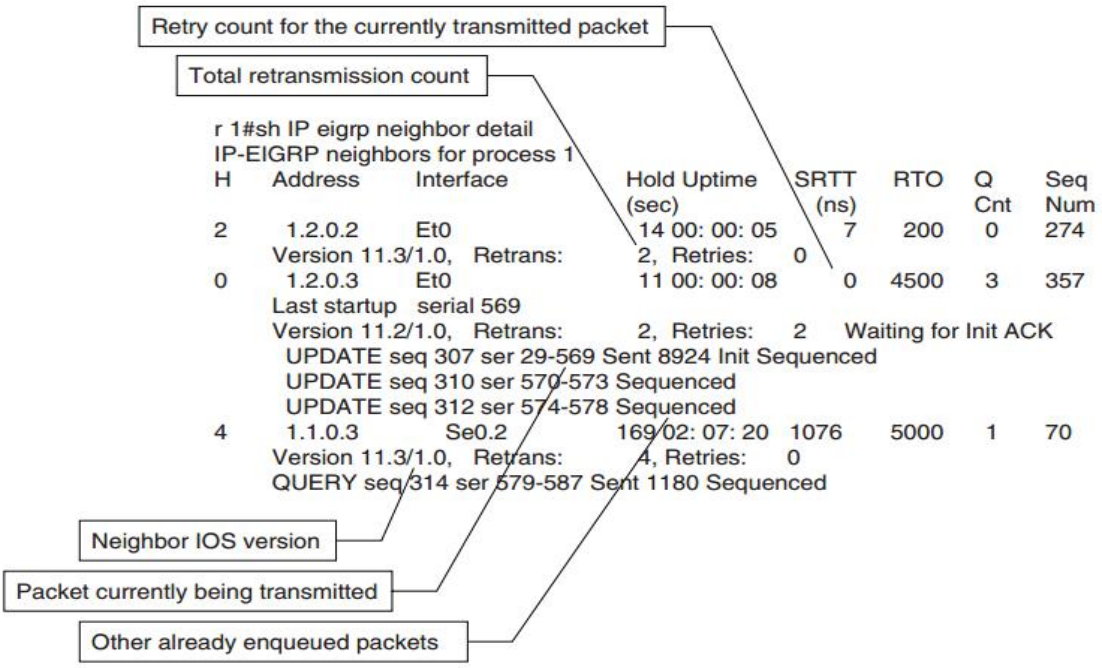
بالنسبة للأمر الأول نستطيع ملاحظة التالي:

*Information Displayed by the **show ip eigrp neighbor** Command*



ولكي نطلع بشكل أكثر تفصيل نلاحظ في الشكل التالي:

*Additional Information Displayed by the **show ip eigrp neighbor detail** Command*



لكن السؤال كيف يعلم الجار أنة حدثت عملية (adjacency reset) عند الجار؟

الجواب من خلال الحقل INIT=1.

EIGRP Topology Table

يعتبر واحد من العناصرا لأساسية في EIGRP ويستخدم في بواسطة DUAL لتخزين المعلومات المستقبلة من الجيران أو من (other routing protocols)، ومن ثم تتم عمليات حسابية لكي تتم إدخاله إلى (routing table).

قبل ذلك يجب ما هي الطرق التي من خلالها تتم إضافة route من topology table وهي :

1. An update packet with a no infinity delay is received.
2. A reply packet with a no infinity delay is received.
3. A route is redistributed from another routing protocol.
4. A directly connected subnet that falls within one of the networks configured in the EIGRP process becomes active.

في حالة تم إستقبال (reply) من الجار بـ (no infinity delay) فإنة لايتم عمل (new route) بل يتم عمل (update).

أما الطرق التي تتم فيها (delete route) من topology table وهي:

1. A directly connected subnet becomes unreachable (layer 1 or layer 2 failure or the interface is shut down by the operator).
2. An update, query, or reply packet is received with infinite delay.
3. A redistributed route disappears from the source routing process.
4. A neighbor is found dead.

EIGRP Topology Table Contents

نتسطيع إظهارالمعلومات الأساسية عن (EIGRP topology table) من خلال الأوامر التالية:

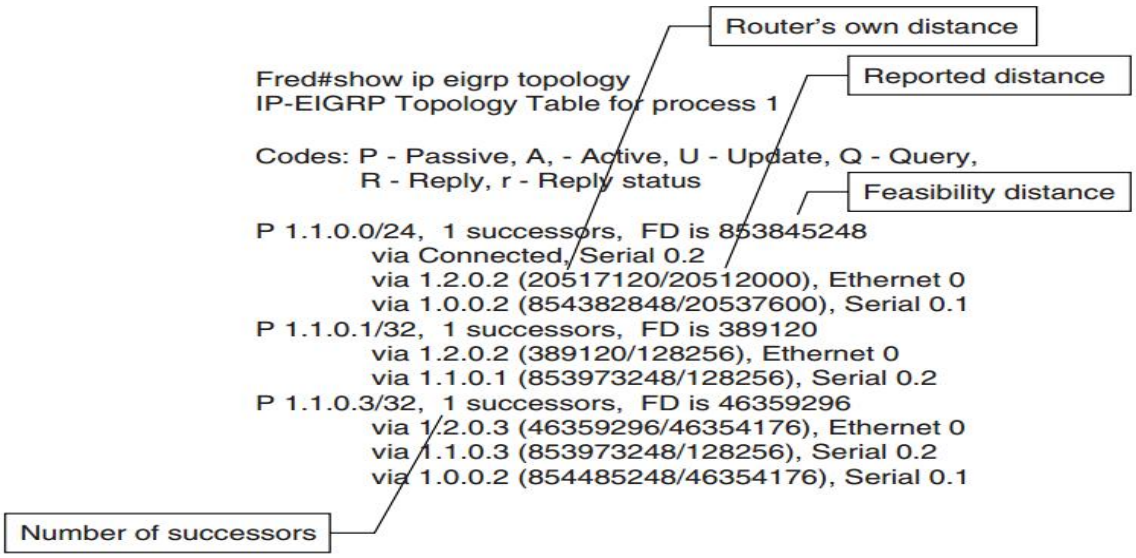
Show Commands to Display Summary Information on the EIGRP Topology Table

To Display . . .	. . . Use This Command
Summary information on all EIGRP topology tables	**show ip eigrp topology summary**
Summary information on the topology table of a single EIGRP process	**show ip eigrp topology <as> summary**
Routes that are used or could be potentially used in the topology table	**show ip eigrp topology [<as>]**
Summary information on all routes stored in the EIGRP topology table	**show ip eigrp topology [<as>] all-links**

زيادة المعلومات في Topology Table تؤثر على كلا من (memory usage and convergence speed)، وبالطبع دائما المعلومات الموجودة في (topology table)، تكون أكبر من routes الموجودة (routing table)، ولكن في حالة كانت أكبر بكثير جدا فإنة يعني أن الشبكة (highly meshed)، أو (EIGRP split horizon is turned off in the wrong place).

في الشكل التالي توضيح للأمر (show ip eigrp topology)

*The **show ip eigrp topology** Command*



Internal and External EIGRP Routes and Additional Route Attributes

لكي نر تفاصيل أكثر عن route معين يجب إستخدام الأمر التالي:

show ip eigrp topology <address> <mask>

وبالتالي نستطيع تحديد نوع route هل تم معرفته من Internal أو من External.

الجدول التالي يبين بعض المصادر الخارجية التي من الممكن أي يحصل الراوتر من خلالها على routes.

Attributes of External EIGRP Routes

Attribute	Meaning
Originating router	Router ID of the router redistributing external route into this EIGRP process. The router ID is an IP address that follows the same rules as the router ID for OSPF or BGP.
AS number	AS number of originating BGP or EIGRP process.
External protocol	The originating protocol from which the route was redistributed into EIGRP.
External metric	The metric of the redistributed route in the originating protocol. For routes redistributed from OSPF this would be the OSPF cost, for RIP routes the hop count, and for the EIGRP routes the composite metric.
Administrator tag	32-bit quantity that can be set in the redistribution point with a route map. The administrator tag has no meaning for EIGRP itself. It can be used, however, to fine-tune redistribution.

Monitoring Network Convergence through the EIGRP Topology Table

نستطيع من خلال الأوامرالتالية معرفة معلومات أكثر عن topology table.

***Show** Commands That Display Routes in the Convergence Phase*

Command	Printout
show ip eigrp topology active	Displays only the routes for which the diffused computation is performed
show ip eigrp topology pending	Displays the routes that haven't converged yet (for example, diffused computation is performed or outgoing updates are still pending)

Building Routing Tables from EIGRP Topology Tables

أخر خطوة هي عملية تكوين (Routing Table) من (the EIGRP topology table)، ولا تتم عملية نسخ ولصق من (Routing Table) إلى (the EIGRP topology table)، لأن (administrative distance) تستخدم لمقارنة (routes) من عدة مصادر لإختيار أفضل route.

طبعا يتم وضع أفضل مسار (successor)، والذي مسموح به حتي ستة والذي يسمى (equal-cost load balancing)، وفقط EIGRP هو من يدعم (unequal-cost load balancing)، من خلال تقنية تسمى بـ (variance).

Administrative Distance of EIGRP Routes

تعتبر إختيار (EIGRP route) من عدة (administrative distances) سوا كان (Internal = 90) أو (External = 170)، ونستطيع تغييرها من خلال التالي:

Different Ways of Setting Nondefault Administrative Distances of EIGRP Routes

To Change . . .	. . . Use This Command
Default distances for internal and external routes in an EIGRP process	**router eigrp <as>** **distance eigrp <default-internal-distance> <default-external-distance>**
Distance of all internal routes received from a neighbor or a set of neighbors	**router eigrp <as>** **distance <distance> <neighbor-ip-address> <wildcard-bits>**
Distance of a select set of internal routes received from a neighbor or a set of neighbors	**router eigrp <as>** **distance <distance> <neighbor-ip-address> <wildcard-bits> <route-selection-ACL>**

EIGRP Variance and Its Influence on Traffic Load Sharing

من خلال الاوامر الموضحة في الجدول أدناه نستطيع عمل (load-balance) بين (unequal cost routes) من خلال الامر variance.

Configure Unequal-Cost Load-Sharing with EIGRP

Task	Configure With
Configure unequal-cost load balancing	**router eigrp <as>** **variance <factor>**
Configure proportional load balancing between unequal-cost routes	**router eigrp <as>** **traffic-share balanced**
Use only minimum-cost routes for load balancing	**router eigrp <as>** **traffic-share min across-interfaces**
Configure the maximum number of equal-cost or unequal-cost routes for a given destination	**route eigrp <as>** **maximum-paths <1 to 6>**
Configure per-packet load balancing over an interface on all platforms	**interface <int>** **no ip route-cache**
Configure Cisco Express Forwarding (CEF) per destination load balancing	**interface <int>** **ip route-cache cef** **ip load-sharing per-destination**
Configure CEF per-packet load balancing	**interface <int>** **ip route-cache cef** **ip load-sharing per-packet**

يعتبر الأمر (variance) مهم لـ (unequal-cost balancing) تحت الشروط التالية:

1. The router's own distance from the topology table entry is less than feasibility distance × variance.
2. The alternate path toward the destination goes through a feasible successor.

ولكي نتحكم بالمسار البديل تتم من خلال الأمر (maximum-paths)، والتي يجب أن تتطابق الشرط (feasibility condition).

نستطيع عمل (traffic-share) والذي يتناسب مع (unequal-cost routes)، والذي يتناسب مع لـ (EIGRP composite metric).

أما الأمر (traffic-share min across-interfaces)، فإنة تتم من خلاله عمل (balancing) فقط عبر (minimum-cost paths)، لكن بقية (paths) تكون موجودة مسبقا في (IP routing table).

طريقة عمل (load-balancing) تعتمد على (switching path) لكل Interface والجدول التالي يوضح ذلك.

Load Sharing Mechanism Used Depending on the Switching Path

Switching Path	Load Sharing Mechanism
Process switching	Per-packet load sharing
Fast switching, Optimum switching, Autonomous switching, Silicon switching, Netflow switching	Per-prefix load sharing (for example, all traffic for a certain prefix in the routing table flows over one interface)
Cisco Express Forwarding	Per source-destination-pair load sharing (for example, all traffic for a certain source-destination IP address pair flows over one interface)
Cisco Express Forwarding with per-packet load sharing configured	Per-packet load sharing

إستخدام (unequal load balancing) يجب فيها مراعاة التصميم الناجح والذي يجب أن يخضع للشروط التالية:

Variance Rule 1

يجب معرفة المسار الذي سيتم تحميل (traffic) لـ (successors and feasible successors)، والذي سيكون من خلال (not a feasible successor).

Variance Rule 2

يجب التأكد من عمل (load-balancing) في كلا الأتجاهين أي تذهب البيانات وتعود.

Variance Rule 3

في حالة أردنا عمل (load-balance) من خلال شبكة LAN فإنة لابد من ألية مثل (Hot Standby Routing Protocol (HSRP)) لإختيار أنسب نقطة للخروج من LAN.

Variance Rule 4

طبعا في حالة وجود مشكلة من الممكن حلها في حالة كان (load-balancing) يعمل، لكن في حالة لم يكن يعمل فإن (feasible successor) معرض لعدم العمل بطريقة جيدة.

إعداد م/محمد شايع

EIGRP Route Summarization

Auto summarization

عملية (Auto summarization) تعتبر من الميزات التي تعطي (EIGRP) نفس (classful behavior) للـ (IGRP)، والتي نستطيع عمل (summarized) وفقا للقاعدة التالية:

لاتتم الإعلان عن (subnets) في (one major network) إلى (another major network)، فقط (major network prefix) تعلن مع (metric) لأقرب (subnet) والذي غالبا هو الـ interface المتصل بشكل مباشر.

دائما الـ EIGRP يدعم الـ (VLSM)، لكن يدعم (discontiguous subnets) والتي تتم إعدادها بشكل يدوي.

وفي الجدول التالي بعض أوامر auto-summarization:

Configure Support for Discontiguous Networks in EIGRP

Router Configuration Command	Meaning
No auto-summary	Enables support for discontiguous networks in EIGRP. No automatic summarization across major network boundaries is performed.
auto-summary (default setting)	Reverts to IGRP compatibility mode where only major networks are announced across network boundaries and the subnets are suppressed.

في حالة تم تطبيق الأمر الأول فإنة تتم عملية (reset) لجميع الجيران المتصلة بـ (router).

عملية تطبيق (auto-summarization) عملية معقدة وفيما بعض القواعد التي يجب مراعاتها أثناء عملية التطبيق:

EIGRP Autosummarization Rule 1

متى ما كان لدى (EIGRP process) أكثر من شبكة معرفة فإنة يعمل على إنشاء (summary route) لكل الشبكات طالما وأن على الأقل واحدة من الشبكات الفرعية من الشبكة موجودة في (EIGRP topology table).

EIGRP Autosummarization Rule 2

عملية (summary route) الذي تم إنشاءه في القاعدة الأولى يشير إلى (Null 0 interface) والذي لدية أقل (metric) في كل الشبكات الفرعية، ويتم إدراج هذا الـ route في (IP routing table) مع (administrative distance of 5).

EIGRP Autosummarization Rule 3

الشبكات التي تمت إنشاءها في (Rules 1 and 2) تكون (suppressed) عندما يتم إرسال (updates) إلى الجيران، أي فقط يتم إرسال (summary routes).

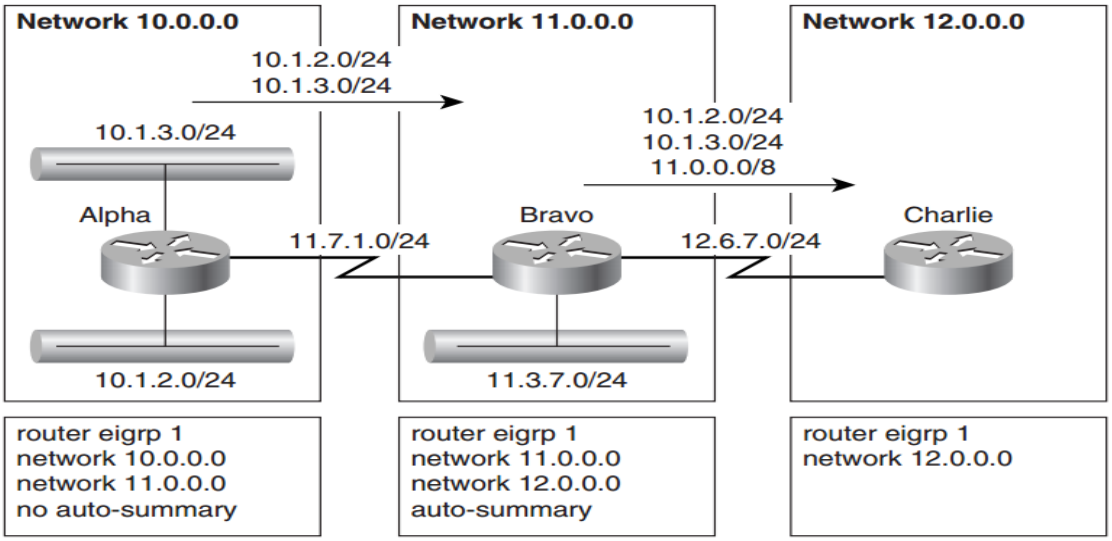
EIGRP Autosummarization Rule 4

الشبكات التي لا تنتمي إلى أي شبكات موجودة في (EIGRP process) لا يتم عمل (summarized) عليها.

القواعد السابقة هي في حالة تم ترك (auto-summary) بشكل إفتراضي.

إذا خلاصة ما سبق أنه في حالة ترك (auto-summary) بشكل إفتراضي، فإنة تتم عمل (summary) عند(boundary) لكن لدينا السيناريو التالي:

EIGRP Autosummarization Only Applies to Networks Defined in EIGRP Process

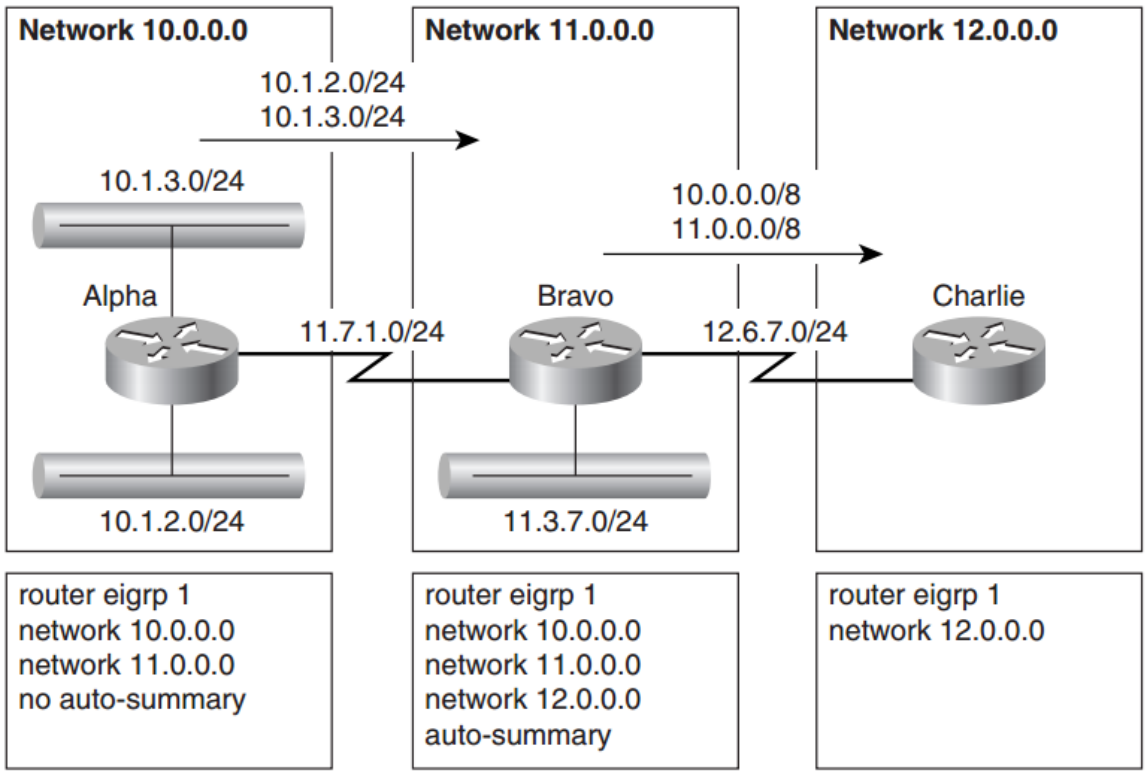


نرى أنة فقط الراوتر (Alpha) تم إيقاف عملية (summary) فتم إرسال الشبكتين (10.1.3.0/24 – 10.1.2.0/24) كما هو موضح، بالنسبة للراوتر (Bravo and Charlie)، فـ (summary) يعمل بشكل إفتراضي، وبالتالي فـ (Bravo) أرسل (11.0.0.0/8) بعد عملية (summary)، لكن بما أنة لايملك أي (interface) ينتمي للشبكة (10.1.3.0/24 – 10.1.2.0/24) ولم يتم تعريفهما في (EIGRP Process) للراوتر (Bravo) فإنة قام بإرسالهما كما وصلا إلية من (Alpha).

لكن ماذا يحدث لو تم تعريف الشبكة (network 10.0.0.0) في (Bravo)؟

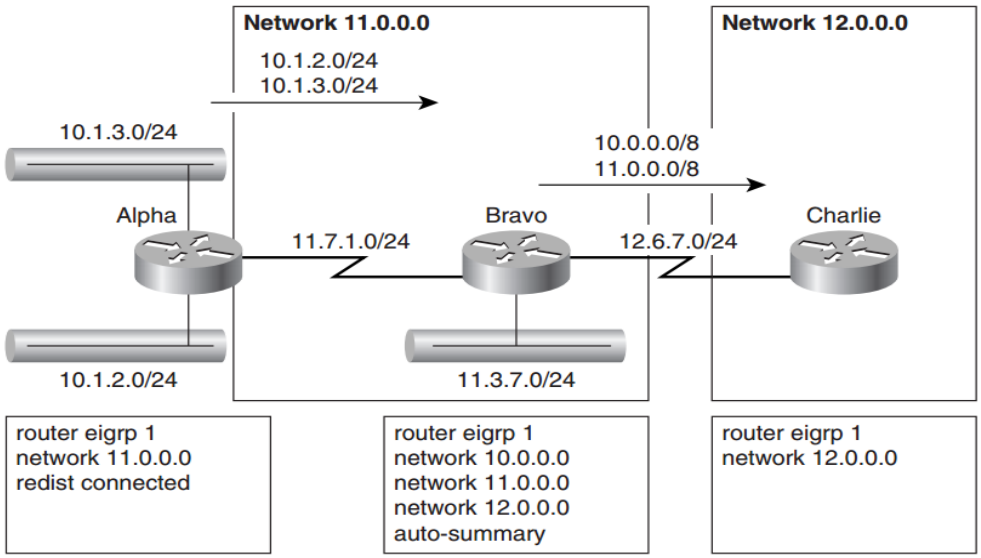
الجواب: سوف يقوم بعملية إرسالها بعد (summary)، والشكل التالي يوضح ذلك.

Autosummarization after Addition of Network 10.0.0.0 in EIGRP Process



دعنا نأخذ المثال التالي في حالة وجود (external route) ما الذي يحدث هل تتم عمل (summary) أما لا؟

External Routes Being Autosummarized



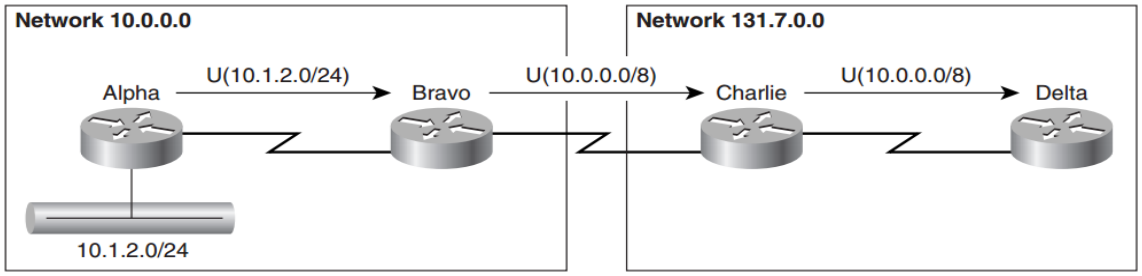
سوف نلاحظ أنة لم يتم عمل (summary) للـ (10.1.2.0/24 – 10.1.3.0/24) بالرغم من وجود أمر (auto-summary) بشكل إفتراضي.

هذا بسبب أن عملية (redistribution) لاتشملها عملية (summary)، أي بإختصار لن يتم عمل (summary) إلا في حالة أمر (network) داخل (EIGRP Process).

وبالتالي فجميع الراوترات سوف تستقبل (10.1.2.0/24 – 10.1.3.0/24) بدون summary.

Query Boundaries with Autosummarization

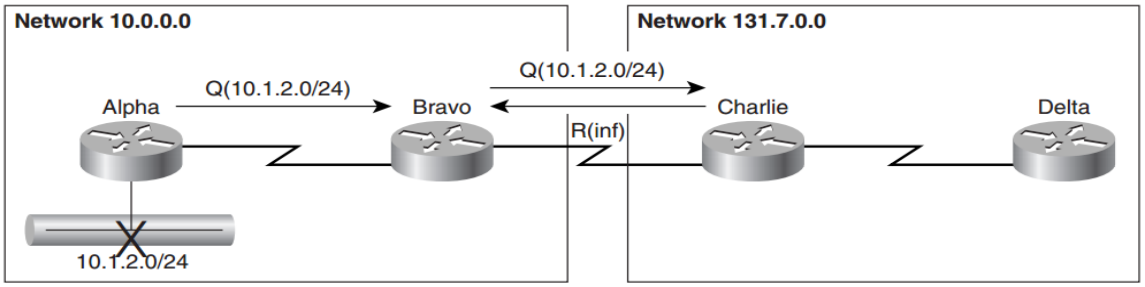
دعني أقول لك أن (auto-summary) تعتبر عملية غير مفيدة لك في الشبكة، وذلك إعتماد على تصميم الشبكة.



في البداية سو تتم عملية إرسال update بين الجيران ولن تتم عملية summary إلى على boundary بين الشبكتين كما هو موضح في الشكل أعلاه.

لكن السنياريو الذي سوف يحدث مثلا في حالة أن الشبكة (10.1.2.0/24) فقدت، فسوف يتم إرسالة query إلى الجار Bravo والذي بدوره سوف يرسله إلى الجار الآخر Charlie ولكن في الشبكة التي تفصل الحد لن يتم إرسال إلى الراوتر (Delta)، بل سوف يتوقف. لماذا؟

الجواب: بما أن الراوتر (Charlie) أستقبل الشبكة (10.0.0.0/8) ولم يستقبل الشبكة (10.1.2.0/24) لأنة حدثت عملية summary فمباشرة سوف يرد (infinite metric). كما في الشكل أدناه.



من ما سبق يتضح أهمية أن يكون تتم عملية إغلاق (auto summary) في حالة كانت الشبكة discontiguous networks، وإستبداله بـ manual summary per-interface.

Manual Per-Interface Summarization

إذا ستيم عمل summary لكن بطريقة per-interface وفي الجدول التالي يوضح الأمر المستخدم في ذلك.

EIGRP Per-Interface IP Address Summarization

Command	Results
ip summary-address eigrp <as-number> <prefix> <mask>	Configures per-interface IP address summarization for single EIGRP process

طبعا في سبق عرفنا أن عملية (Configuring or removing an IP summarization range on an interface) سوف يجعل الراوتر يقوم بعملية (clear all EIGRP adjacencies) التي أتت من interface التي تمت عملية summary علية، وقد يصاحب ذلك تغيير في topology table.

نفس القواعد التي طبقت على auto-summary سوف يتم تطبيقهاعلى manual summary per-interface،

EIGRP Manual Summarization Rule 1

لكل (summary range) على interfaces في (EIGRP process) فإن (EIGRP process) سوف ينشئ (summary route) يحتوى على الأقل (more specific route) التي يقع ضمن (range) وسوف يظهر في (EIGRP topology table).

EIGRP Manual Summarization Rule 2

سوف يظهر (summary route) الذي تم إنشاءة في rule 1 سوف يشير إلى (Null 0 interface)، ويكون بأقل (metric)، وطبعا سوف يتم إدراجة في (main IP routing table) وبـ (an administrative distance of 5)

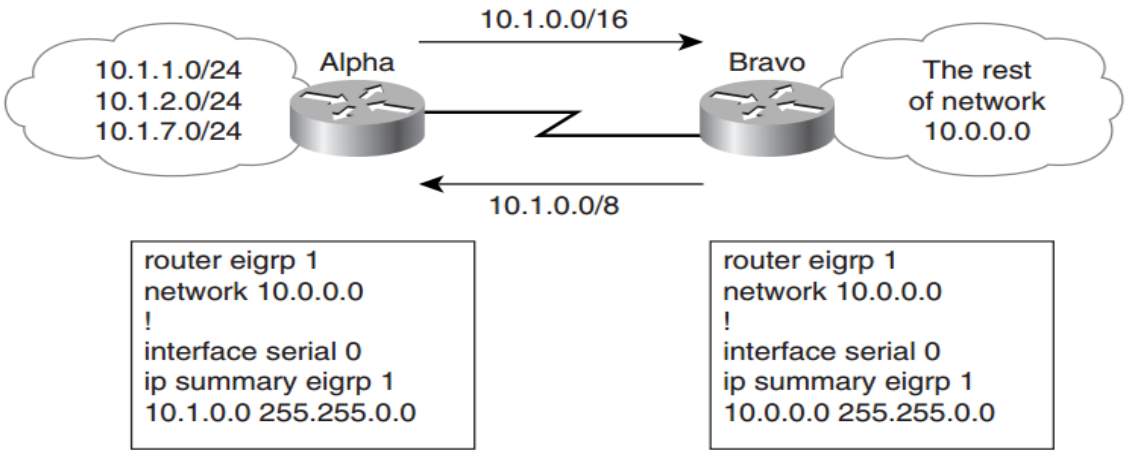
EIGRP Manual Summarization Rule 3

الشبكات التي تمت إنشاءها في (Rules 1 and 2) تكون (suppressed) عندما يتم إرسال (updates) إلى الجيران، أي فقط يتم إرسال (summary routes).

Why Do We Need a Summary Route to Null 0?

طبعا الهدف من عملية إدخال route Null 0 interface هو عملية منع حدوث loop بين الراوترات مع إختلاف (IP address space) في (routing tables).

Summarization Scenario Leading to a Potential Routing Loop



أفترض أنه لايوجد (Null 0 interface) في كلا من (Alpha and Bravo)، في هذه الحالة فإن أي باكيت سوف يستقبله (Alpha) سوف يعيد توجيهه إلى (Bravo)، وهذا سوف ينتج عنه Loop، لكن مع وجود Null 0 فإنة سوف يتم حذف هذا النوع من Packet.

EIGRP Query Boundary with Per-Interface Summarization

ما الذي سوف يحدث في (Per-interface summarization ranges)؟

الجواب : نفس الطريقة في (Autosummarization)، أي (one hop farther) سوف يتم عمليا عدم وصول (query) إلي بقية الشبكات الأخرى, وهذا تم شرحه مسبقاً.

EIGRP Route Filters

طبعا نعرف أن طريقة (EIGRP) في عملية (propagating routes through the network) تشبة (distance vector protocol) من خلال الشبكة والخطوات التالية توجز ذلك:

1- إستقبال أي (incoming update) لـ (new route) و تطبيق (inbound interface metrics) على (update) الذي تم إستقباله.
2- إدخال المعلومات إلي قاعدة البيانات (EIGRP topology)، وإختيار أفضل route.
3- إعلان (best route) إلى كل (EIGRP neighbors).

(Route filters) نستطيع إدخاله بشكل إجباري ما بين الخطوات (Steps 1 and 3)، والتي سوف تستقبل من الجيران وترسل كذلك إلى جيران آخرين.

يجب أن نلاحظ أن (Route filters) تعتبر (security mechanism)، بسبب أنها تزيد في (security and reliability) للمعلومات المتبادلة.

EIGRP offers a rich set of filtering options:

1. Inbound or outbound route filters can be applied globally (to all EIGRP neighbors) or on a per-interface basis (to all neighbors reachable over the specified interface).
2. Additional route filters can be applied to routes redistributed into EIGRP from other routing protocols.

وهنا الأوامر التي تستخدم في route filter

Configuring EIGRP Route Filters

Router Configuration Command	Results
distribute-list <ACL> in	Applies specified ACL to all updates received from all neighbors.
distribute-list <ACL> in <interface>	Applies specified ACL to all updates received through specified interface.
distribute-list <ACL> out	Specified ACL is applied to all updates sent.
distribute-list <ACL> out <interface>	Specified ACL is applied to all updates sent through specified interface.
distribute-list <ACL> out <routing-process>	Specified ACL is applied to all routes received through redistribution from specified routing process before these routes are stored in EIGRP topology database.

في حالة تم إستخدام (distribute-list per interface) فإنة أي جيران تم معرفتهم من هذا (interface) سوف تتم عمل (reset).

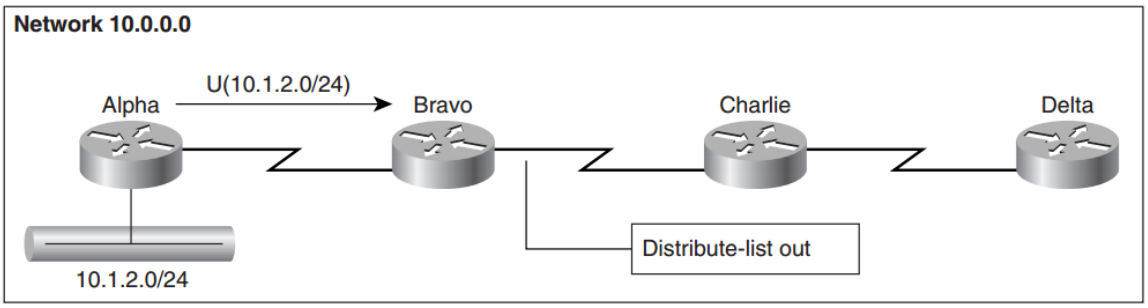
كما يجب التنويه إلى أنه لايتم تطبيق (EIGRP route filters) على كل (EIGRP packets)، حيث أن (query packets) لاتتأثر بها، بينما تتأثر بقية (EIGRP packets) طبقا للقواعد التالية:

1- أي route يتم إستقباله في (update packet)لكن يخضع لـ (distribute-list in) سوف يتم حذفه وهذا يعني أن (route with infinite metric).
2- أي (Route) في (topology database) لكن يخضع لـ (distribute-list out) لن يتم إرساله (outgoing).
3- الـ (reply packet) لـ (route) تمت (filtered) بواسطة (global or per-interface)، بشكل (distribute-list out) سوف يتم إرساله بطريقة (infinite metric).
4- الـ (reply packet) المستقبل لأي route تمت (filtered) بواسطة (global or per interface)، بشكل (distribute-list in)، سوف تتم معالجته على أنه (infinite metric).

Query Boundaries Established by EIGRP Route Filters

عملية (EIGRP route filters) دائماً تنشئ (query boundaries)، بسبب أن الراوتر نفسة أو الجار لايملكون أي entry في (topology databases) لبعض الشبكات التي تمت فلترتها بواسطة (inbound or outbound filters).

(Outbound route filters) دائما تنشئ (query boundary)، والتي تكون (one hop)، والتي بنفس التأثير لـ (route summarization).



وضع (distribute-list out) أو (distribute-list out in) بعد (Bravo) سوف يجعل الشبكة (10.1.2.0/24) لاتصل إلى كلا من (Charlie and Delta)، وبالتالي لن يصل (query)، إلى بقية الشبكة.

Prefix Lists—Improved Route Filters

تعتبر (Prefix List) أنسب الأدوات عند (the network design) يتطلب عملية فلتره بـ (subnet mask).

وبذلك نستطيع إستخدامها في أي مكان، وفي الجدول التالي يبين بعض الأوامر التي تسخدم في prefix list.

IP Prefix List Syntax

Command	Results
ip prefix-list <name> permit|deny <cond>	Inserts the line at the end of the prefix list. The line is automatically numbered.
no ip prefix-list <name> seq <seq#> …	Deletes the specified line from the prefix list.
ip prefix-list <name> seq <seq#> …	Inserts the specified line at the desired insertion point in the prefix list. Cannot be used to overwrite an existing line; the existing line has to be deleted first.
ip prefix-list <name> description <line>	Assigns description to the prefix list.

وفيما يلي كيفية (IP prefix list condition).

IP Prefix List Conditions

Command	Results
ip prefix-list <name> permit|deny <ip prefix>/<prefix-length>	Matches the specified prefix
ip prefix-list <name> permit|deny <ip prefix>/<prefix-length> ge <pfx-len>	Matches all routes that fall within the specified IP address space and have subnet masks longer or equal (in number of prefix bits) than the specified prefix length
ip prefix-list <name> permit|deny <ip prefix>/<prefix-length> le <pfx-len>	Matches all routes that fall within the specified IP address space and have subnet masks shorter than or equal to the specified prefix length
ip prefix-list <name> permit|deny <ip prefix>/<prefix-length> ge <min-len> le <max-len>	Matches all routes that fall within the specified IP address space and have subnet masks lengths between min-len and max-len (inclusive)

نستطيع تطبيق (prefix list) في مع distribute list والجدول التالي يوضح ذلك.

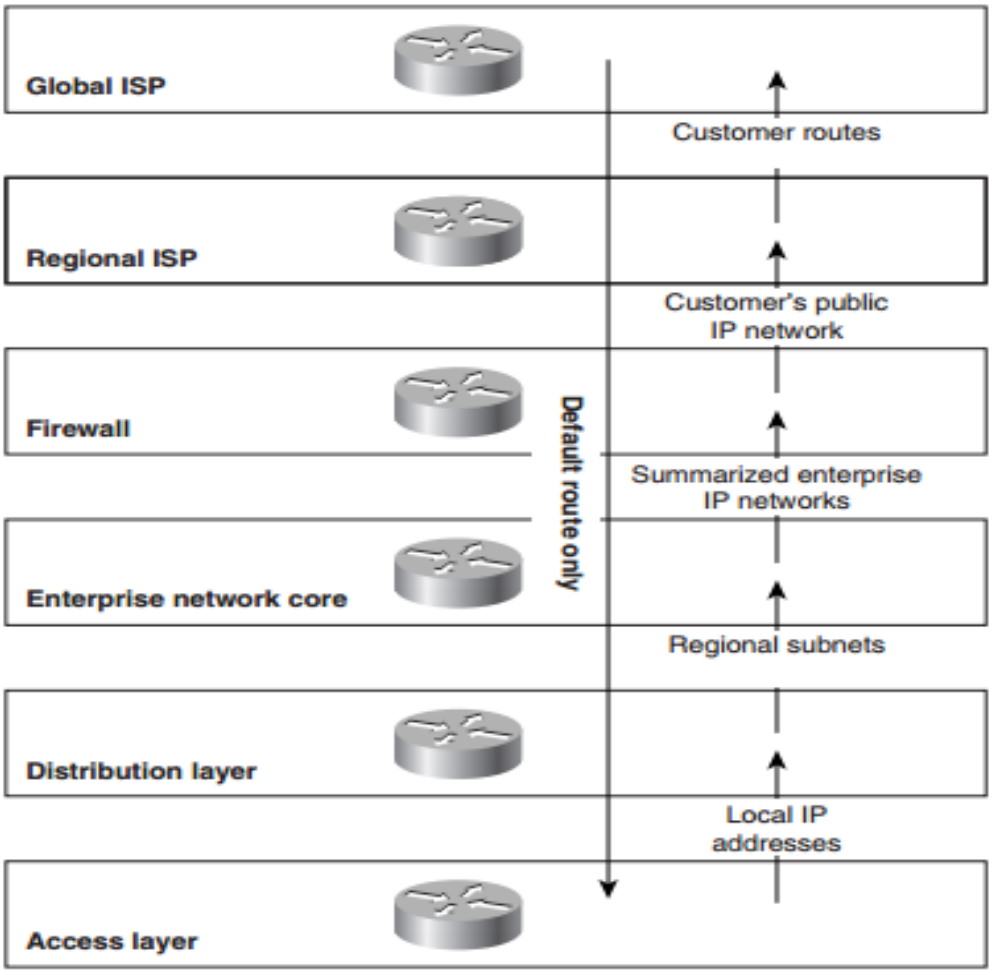
Configuring EIGRP Route Filters

Router Configuration Command	Results
distribute-list prefix <prefix-list> in	Applies specified prefix list to all updates received from all neighbors.
distribute-list prefix <prefix-list> in <interface>	Applies specified prefix list to all updates received through specified interface.
distribute-list prefix <prefix-list> out	Specified prefix list is applied to all updates sent.
distribute-list prefix <prefix-list> out <interface>	Specified prefix list is applied to all updates sent through specified interface.
distribute-list prefix <prefix-list> out <routing-process>	Specified prefix list is applied to all routes received through redistribution from specified routing process before these routes are stored in EIGRP topology database.

Default Routes

في الشكل التالي يتبين لنا كيف أن طبقات الراوتر تتم عبرها توجيه البيانات حيث أن الطبقة العليا تعرف جميع ماتحتها وهكذا بينما لاتعرف الطبقة الأولى (access layer) سوى جيرانها و (default route) يشير إلى الطبقة التي تليه.

Multilayer Structure in an Enterprise Network Connected to the Internet



IP Default Routing and IOS Specifics

عملية البحث داخل (IP routing table) تتم بطريقتين :

1- أن يجد (longest matching prefix) لـ (destination) معين في (routing table).
2- يتم حذف أي (packets)، عندما لا يجد أي (matching prefixes).

وجود (route 0.0.0.0/0) يسمى بـ (default rou) في (Routing table) يجعل عملية البحث تتم بالشكل التالي

عندما لايتم إيجاد أي (matching) لـ (destination address) في (routing table) فإنة سوف يتم إستخدام route يعتبر أصغر route في routing table يسمى بـ (default route).

Default Candidates and Gateways of Last Resort

يتم إختيار فقط route واحد من (the default candidates) وهي تلك الـ (routes) الموجودة في (IP routing table)، وهذا route يحمل مواصفات (minimum administrative distance and minimum routing metric) ثم تجعله (best default candidate)، و (next hop router) لـ (best default candidate) تصبح (gateway of last resort). ويستخدم (default route) لعملية (forward packet) لـ (unknown destinations).

وفيما يلي بعض الأوامر المستخدمة في ذلك:

*The **ip default-network** Command*

Command	Results
ip default-network <major-network> for connected networks	Marks the network as default candidate in the IP routing table. Starts redistributing the network in all IGRP and EIGRP processes. Marks the network in the EIGRP topology database with default candidate flag.
ip default-network <major-network> for nonconnected networks	Marks the network as default candidate in the IP routing table. If the network is already in EIGRP topology database, marks the network with default candidate flag. Takes no further actions to insert the network into EIGRP topology database.
ip default-network <subnet>	Equivalent to **ip route <major-network> <mask> <subnet>**. Inserts the summary route for the major network into which the subnet belongs in the routing table.

Default Routes and Default Candidates in EIGRP

EIGRP تدعم (IP default route (0.0.0.0/0)) على أنه candidate default routes وهناك مجموعة من الإختلافات مع بقية البروتوكولات:

1. EIGRP is the only classless routing protocol that supports default candidates.
2. Although EIGRP can carry the default route (0.0.0.0/0) as a regular IP route, it never generates it in the topology database. To insert the default route into the EIGRP topology database, you have to manually configure redistribution of the default route.
3. Whenever the default route is redistributed into the EIGRP topology database, the default candidate marker is set automatically on the entry in the topology database.
4. EIGRP automatically redistributes connected network (or subnets) marked as ip default-network in to the EIGRP process.

كما يسمح لنا EIGRP نستطيع عمل (fine-tune)، نستطيع حذف (default candidate flag) من (incoming or outgoing routing updates)، بإستخدام الأوامر التالية:

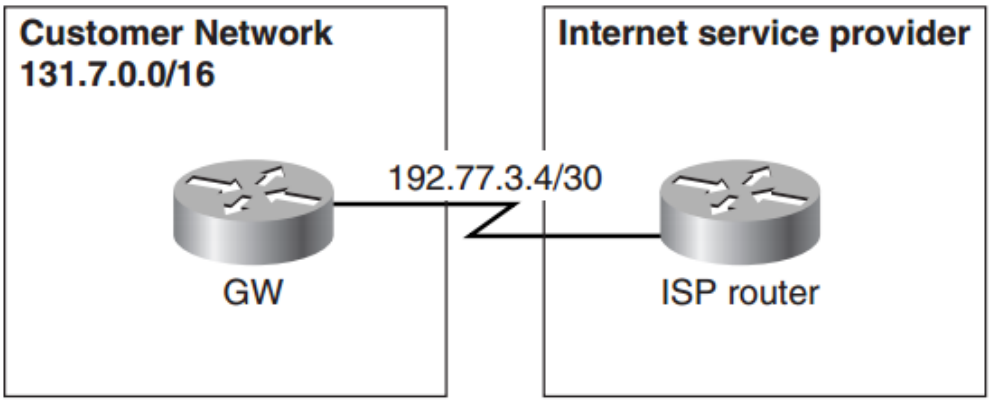
Default Information Propagation Control in EIGRP

EIGRP Router Configuration Command	Result
default-information in <ACL>	Erases the default candidate marker from all received routes not matched by the IP access list <ACL>
default-information out <ACL>	Erases the default candidate marker from all routes not matched by <ACL> when they are advertised to EIGRP neighbors
no default-information in	Does not accept any default candidate markers
no default-information out	Does not mark any routes as default candidates in outgoing updates. The router itself still uses the default candidate markers on the routes in the EIGRP topology database to select its own gateway of last resort.

EIGRP Default Routes—Design Examples

عملية وضع () في () نستطيع عمله بطريقتين هما :

1- عملية الإعلان عن الشبكة الفرعية المتصلة بـ (the GW router) و(ISP)على أنها (default network)، بعد ذلك تتم عملية (redistributed) إلى EIGRP بـ (vector metric) للـ (interface) الذي يصل (to the ISP the GW router)، ويتم وضعه على أنه (default candidate) والذي يجعل كل الروترات الأخرى تشير له على أنه (next-hop router) نحو على أنه (gateway of last resort).




```
hostname GW
!
interface serial 0
ip address 192.77.3.6 255.255.255.252
bandwidth 64
!
interface ethernet 0
ip address 131.7.13.5 255.255.255.0
!
router eigrp 42
network 131.7.0.0
!
ip default-network 192.77.3.0
```

2- الطريقة الأخرى هي إعداد (static default route) يشير إلى (to the physical interface itself external subnet or)، ثم (manually redistribute the default route) إلى (EIGRP)، هذه العملية سوف تجعل (redistributed route) يرث (interface parameters) لكن يجب عليك وضع(interface metrics) بشكل يدوي في أمر (redistribute).

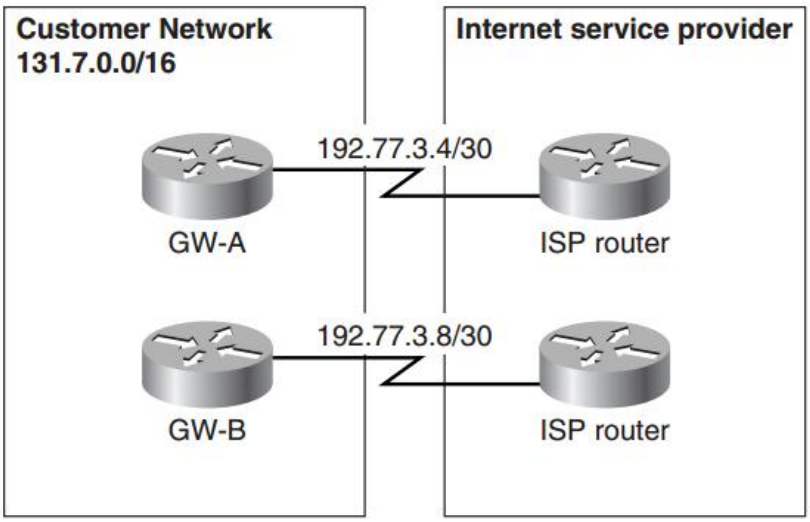
```
hostname GW
!
interface serial 0
ip address 192.77.3.6 255.255.255.252
!
interface ethernet 0
ip address 131.7.13.5 255.255.255.0
!
router eigrp 42
network 131.7.0.0
redistribute static metric 64 20000 255 1 1500
!
ip route 0.0.0.0 0.0.0.0 192.77.3.5
```

تتشابة الطريقتين مع بعض الإختلاف البسيط:

1- (EIGRP vector metric) لـ (the default route)، نستطيع التحكم بها بشكل أكبر في (redistribution).
2- طريقة (redistribution) سوف تعمل حتى عندما (IP subnet) في link بين (GW router and the ISP) ينتمى إلى (customer's address space).

Enterprise Network with Multiple Connections to the Internet

في حالة وجود (multihomed customer) كما في الشكل التالي، ليست معضلة بل سوف يتم عمل إعدادات بنفس الطريقة في حالة (one gateway)،بل يجب فقط إختيار أفضل (exit point)، وهذا يتوقف على السرعة و load.



إعداد م/محمد شايع

Integrating EIGRP with Other Enterprise Routing Protocols

يحتاج EIGRP إلى الدمج مع (other routing protocols) في الحالات التالية:

1- عندما يكون لدينا بروتوكول EIGRP نريد دمجه مع شبكة أخرى لديه بروتوكول أخر.
2- عندما يكون لدينا عدة أجهزة routers من عدة منتجين غير شركة cisco أي منتجين لا يدعمون EIGRP.

وبالتالي سنعمد إلى استخدام الأمر (redistribute) للقيام بهذه المهمة

Redistribution between Routing Processes

لكي ننفذ عملية (redistribution) فانة نستطيع استخدام الأوامر التالية:

***redistribute** Command Syntax*

```
redistribute <source-protocol>
[metric <metric>]
[route-map <route-map>]
[match internal | external ...]
```

والأن نأتي إلى شرح (Parameters) الموجود في الأمر السابق.

***redistribute** Command Parameters*

Parameter	Meaning
source-protocol	Protocol from which the routing information is redistributed into the target protocol. Any routing protocol supported by the router can be used (including **static**, **mobile**, or **connected**). If the source-protocol supports AS numbers or process IDs, the AS number or process ID has to be specified.
metric (optional)	The metric of the redistributed route.
route-map (optional)	The route-map used to filter redistributed routes and optionally set attributes of redistributed routes (for example, route tags).
match	Applies only to specific source protocols. For example, when you redistribute from OSPF into EIGRP, you can specify that you only want to redistribute internal OSPF routes.

لكن هناك بعض الاسئلة التي يجب معرفتها عند تصميم (route redistribution) وهي:

1- هل تتم عملية (redistribution) في اتجاه واحد (for example, from the access layer into the core)، أو في كلا الاتجاهين كـ (core network) تنفذ عليه (two routing protocols) أو شبكتين يتم دمجهم؟
2- هل تتم عملية (redistribution) بين أي (two routing protocols) في نقطة واحدة فقط مثلا (single router)؟ أو في عدة نقاط (several routers)؟ لمزيد من (redundancy)؟

مسألة التصميم مسألة في غاية الأهمية وعملية (redistribution) لها العديد من المميزات والعيوب، ومسالة التنفيذ نستطيع الإجابة عليها بشكل سهل. أي معلومات نريد عملية (redistributed) من (source) إلى (target)، فقط (source routing protocol) للراوتر نفسة تستخدم

(packet) التي توجه سوف يتم توزيعها إلى (target routing protocol)، بكلمة أخرى عملية redistribution تتم استخدامها من (routing table) وليس من (EIGRP topology table) أو (OSPF topology database).

ونستطيع استعراضها من خلال الأمر (show ip route <routing-protocol>)، والـ (metric) يتم حساب أفضل (EIGRP metric)، للـ (route) التي يتم الإعلان عنها، بينما يقوم (EIGRP) بحساب (metric) للـ (routes) القادمة من (IGRP or EIGRP processes,)، أو (connected routes redistributed into EIGRP) أو (static routes that have a next-hop for which EIGRP metric is computable)

بقية (redistributed routes) فإن الـ (metric) المناسبة يتم وضعها بشكل يدوي، إما باستخدام (metric option) الموجود في أمر (redistribute) أو باستخدام أمر (default-metric).

إما في حالة عدم وضع الـ (metric) فإنه لن يتم (redistributed) إلى (EIGRP).

Are subnets from the source routing protocol redistributed or not?

عملية (Redistribution) إلى (EIGRP) دائما (classless)، أي تتم عملية نقل (routes) إلى EIGRP مع mask التابع لها.

Can I filter the information while doing redistribution?

نستطيع وضع (filtered) على (redistribution routes) باستخدام (route-map) أو (distribute-list) في (target routing protocol).

يعتبر أمر (distribute-list out)، عملية فلتر لـ (outbound).

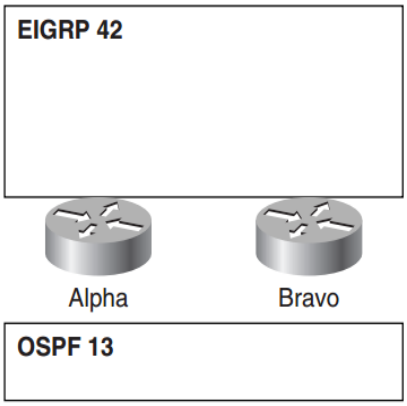
How are the routes received through different routing processes compared to when they try to enter the IP routing table?

فقط تتم عملية المقارنة بين routes التي تتم استقبالها خلال (different routing processes) بواسطة مقارنة (administrative distances) للـ (routes).

Redistribute Only Internal Routes

أبسط طريقة تتم من خلالها تنفيذ (multipoint, two-way redistribution) عملية (redistributes) لـ (internal routes) من (one routing protocol) إلى (other routing protocol)، كما في الشكل التالي من (OSPF-to-EIGRP).

Stable Two-Way OSPF to EIGRP Redistribution



Two-Way Redistribution of Internal Routes

```
hostname Alpha
!
router eigrp 42
redistribute ospf 13 match internal
!
router ospf 13
redistribute eigrp 42 route-map InternalOnly
!
route-map InternalOnly permit 10
match route-type internal
```

لن يكون هناك أي loop بسبب وجود route-map والتي ستعمل على فلتره (internal route).

Redistribute Routes Using Route Tags

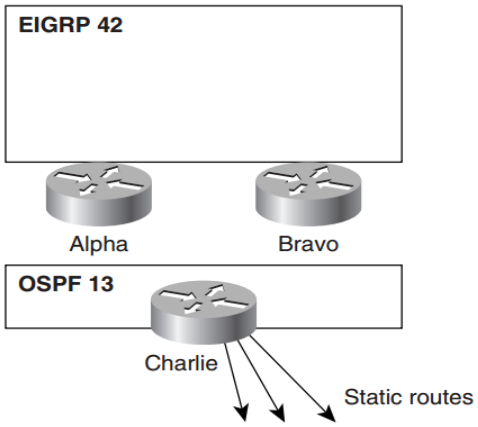
عملية (two-way redistribution) عندما يكون هناك بعض (external routes) نريد عمل (redistributed) إلى (other routing protocol) تعتبر أكثر تعقيدا، ولذلك نستطيع استخدام (route tags).

ملاحظة:

(Route tags) هي أرقام نستطيع ربطها إلى (route) بدون إجبار اختيار (route). ولاتعني بروتوكول التوجيه نفسة لكن نستطيع استخدام (route maps) لعملية فلتره (redistributed routes).

ولشرح (route tags) نستطيع اعتبار الشبكة في الشكل التالي، عندما (OSPF) يحمل (external static routes) يتم توزيعها إلى (OSPF) بواسطة (router Charlie).

Two-Way OSPF to EIGRP Redistribution with External Routes



تتم عملية (Alpha) بين (Bravo) كما في التالي:

1- عمل (Tagging) لكل (routes) التي سوف توزع من (OSPF 13) إلى (EIGRP 42) بواسطة (tag 13).
2- عمل (Tagging) لكل (routes) التي سوف توزع من (EIGRP 42) إلى (OSPF 13) بواسطة (tag 42).
3- لن يتم عملية (redistributing) لأي (routes) من (EIGRP 42) إلى (OSPF 13) يحمل (tag 13).
4- لن يتم عملية (redistributing) لأي (routes) من (OSPF 13) إلى (EIGRP 42) يحمل (tag 42).

Secure EIGRP Operation

موضوع (Security and reliability)من المواضيع المهمة جدا في عالم الشبكات، لكن لاتزال (routing protocols) معرضة لعدة مشاكل في (intrusion or denial of service).

من ضمن المشاكل التي من الممكن أن تكون الشبكة معرضه لها في مجال السرية:

1- أن (Remote office routers) تتنصت لـ (EIGRP updates) على (LAN interfaces).
2- عدم وجود أي (filtering) على أي راوتر.
3- عدم محاولة أي راوتر القيام بعملية (adjacency) لتبادل (routing information) مع جهاز غير موثوق به.

نستطيع الحد من المشاكل التي من الممكن أن تظهر فيما سبق من خلال التالي:-

1- إعداد (LAN interfaces) لكل (remote office routers) بإمر (passive interface) لمنع تشكيل أي علاقات جوار مع (routers) في (remote LAN).
2- إعداد (route filters) في (distribution-layer routers) لضمان أن (remote office routers) عدم دخول أي (fake routes) في (core network).
3- استخدام (EIGRP MD5 authentication) خلال الشبكة لضمان قبول علاقات الجوار مع جيران موثوق بهم.

EIGRP MD5 Authentication

عملية (EIGRP MD5 authentication) تعتبر لضمان أن (routers) فقط تقبل استقبال (EIGRP packets) من مصادر موثوق بها، بعد عملية إعداد (MD5 authentication) على (interface) فإن كل (EIGRP packet) يرسل بواسطة الراوتر على (interface) سوف يتم تضمين (MD5 authentication)، وكل (EIGRP packet) سوف يتم استقباله على (interface) سوف يتم فحص (MD5) لضمان تطابق بين القيم المرسلة وكذلك المستقبلة.

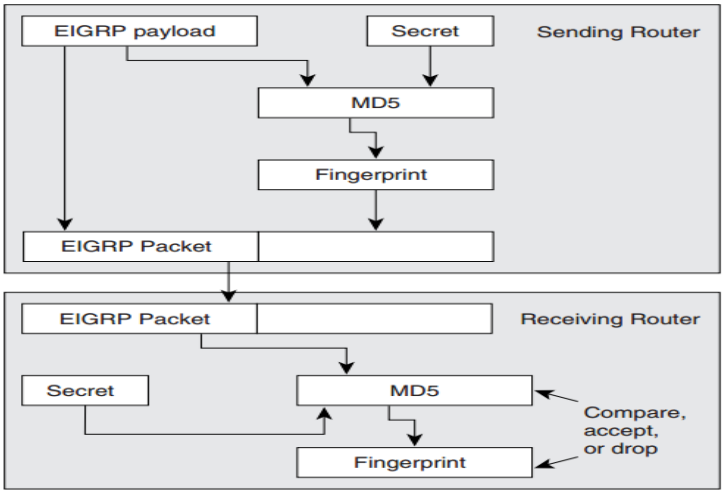
خوارزمية (MD5) عبارة عن ((EIGRP packet) message) وتولد (128 bits) لكن تكون قيم (hash) والتي تسمى بـ (message digest or fingerprint)

قيمة (MD5) المولدة من (EIGRP message) سوف يتم إلحاقها بـ (EIGRP packet) ويتم إرسالها إلي الجار، الجار الذي سوف يستقبلها سوف يبدا بـ عملية فحص (integrity) للـ (packet) بواسطة إعادة حساب قيمة (MD5) ومن ثم عملية مقارنة النتيجة مع (MD5 fingerprint) في packet.

نستطيع تلخيص العملية في التالي:

1- الراوتر المرسل يولد (EIGRP information) لإرسالها.
2- (MD5) تحسب على (over EIGRP information) وتكون معلومات (shared secret).
3- النتيجة (MD5 hash value) تلحق بـ (packet) لأرسالها إلي الجيران.
4- في الراوتر المستقبل يتم حساب (MD5) على (received EIGRP information) وتكون (shared secret)، في حالة التطابق يتم قبول (packet) وإلا يتم حذفه.

EIGRP MD5 Authentication



إعداد م/محمد شايع

وفيما الأوامر المستخدمة في عملية (MD5).

Configuring EIGRP MD5 Authentication on an Interface

Task	Interface Configuration Command
Specify the shared secret used between adjacent routers reachable over specified interface	**ip authentication key-chain eigrp <as-number> <key-chain-name>**
Specify the type of authentication used in EIGRP packets (only MD5 is available)	**ip authentication mode eigrp <as-number> md5**

(shared secret) هو عبارة عن مجموعة من المفاتيح لها (Send Life time) وكذلك (Accept life time).

ومن خلال الجدول التالي نطلع على جميع خيارات key chain

Configuring a Key Chain

Task	Global Configuration Command
Define a key chain	**key chain <name>**
Define a key in the key chain	**key <sequence-number>**
Define key value for the specified key	**key-string <value>**
Define the time interval during which the key will be accepted by the router. If you don't specify the time interval, the key is always valid. The earliest acceptable start time is January 1, 1993.	**accept-lifetime <start-time> {<end-time> | infinite | duration <seconds>}**
Define the time interval during which the key will be used by the router to sign the packets. If you don't specify the time interval, the key is always used.	**send-lifetime <start-time> {<end-time> | infinite | duration <seconds>}**

قد يكون هناك تداخل بين Keys لكن لمنع احتمال حدوث أي (overlaps) بين keys فان IOS تطبق القواعد التالية:

1- في حالة كان هناك تداخل في عدة (keys) في (send-lifetime) يتم استخدام المفتاح الذي يحمل أقل رقم لـ (outgoing EIGRP packets).
2- في حالة كانت (overlapping accept-lifetime) لأي (incoming packets)، فإنه يتم استخدام أي واحد من هذه المفاتيح.

Shortcomings of EIGRP MD5 Authentication

يوجد هناك بعض أوجه القصور ومنها :

1- في (MD5 authentication of EIGRP) ومنها أن البيانات تكون (authenticated) لكن ليست (encrypted) والمعلومات المتبادلة تكون (reliable) لكن ليست (confidential).
2- كذلك يتم إعداد المفاتيح بشكل يدوي وليس بشكل ألي.

Troubleshooting EIGRP MD5 Authentication

في أوقات تتعرض عملية (EIGRP adjacency) إلي بعض المشاكل مع وجود EIGRP MD5 authentication ولذلك نقوم بعملية debugging كما في التالي:

debug ip eigrp packets verbose

وهناك أربعة أسباب لانهيار علاقة الجوار بسبب (authentication) وهي كتالي:

1- إعداد (**MD5 authentication**) في راوتر واحد وعدم إعدادها في الثاني.
2- إعداد (Keys) بشكل خاطئ أو عدم وجود (Key chain)، وللتأكد من ذلك يجب استخدام الأمر Show key chain.
3- الاختلاف في التوقيت يجب أن نستعرض وجود كلمة (valid now) من خلال الأمر (Show key chain).
4- الاختلاف في توقيت الراوتر الحقيقي وهذا نستطيع معرفته من خلال الأمر (show clock detail)

ولكي نقوم بعملية (EIGRP MD5 troubleshooting) يجب إتباع الخطوات التالية:

1- التأكد من أن (adjacency is not established) بسبب (EIGRP MD5 authentication).
2- التأكد من أن (EIGRP MD5 authentication) مفعلة على كل (adjacent routers).
3- التأكد من أن كل (router configurations) تشير إلى (valid key chain).
4- التأكد من أن (key chain) متطابقة بين (routers).
5- التأكد من أن (routers) تستخدم نفس keys.
6- التأكد من عملية (synchronized) في التوقيت بين (routers).