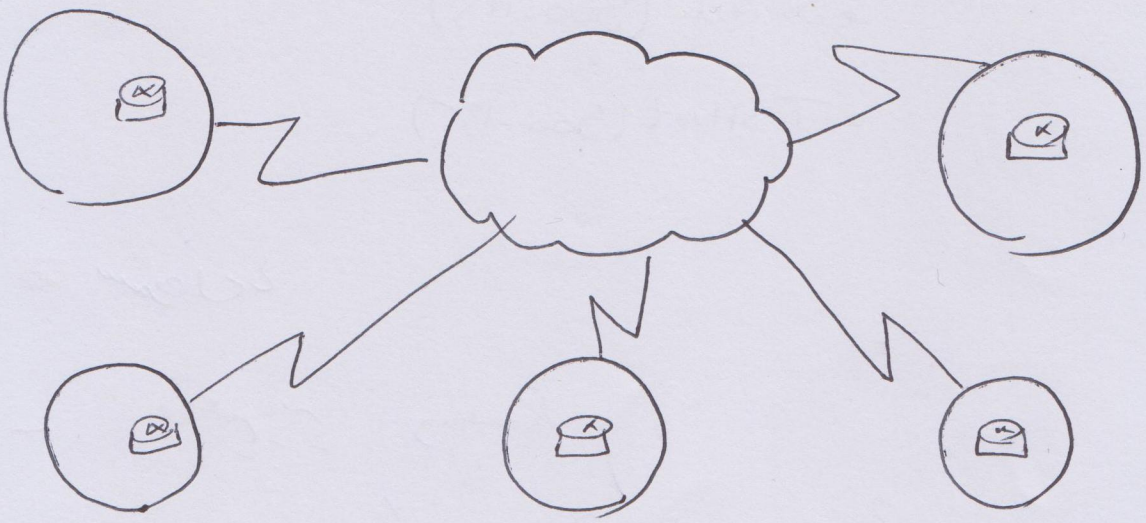
CCNP Routing and Switching

- Route (300-101)
- Switch (300-115)
- TSHoot (300-135)

سيرفيس

- Routing تقنيات
- Routing IGP تقنيات بروتوكول
- Routing Distribution and Selection
- Configuring Internet Connectivity
- Router and Routing Security

نحوه ارتباط بین Router های مرکزی و Branch office ها:



تکنولوژی‌های ارتباط بین Branch ها جهت Remote Connectivity:

- Dedicated (Direct line):

- leased line (T1):

سرعت بالا به دلیل اختصاصی بودن

گران بودن

محدود بودن سرعت T1 : 1.544 Mbps

- Metro Ethernet و Dark Fiber):

سرعت ارتباط از نوع فیبر می‌باشد.

واریس نیز می‌باشد.

- VPN (Virtual Private Network):

شبکه آن اینترنت می‌باشد.

افزایش امنیت در بستری Public مانند اینترنت

دارای Protocol های و تکنولوژی‌های مختلف شامل PPTP، L2TP، SSTP، IKEv2

به صورت Site to Site و یا Singlelink قابل پیاده‌سازی می‌باشد

- DMVPN (Dynamic MultiPoint VPN)

در حالت عادی VPN برای ارتباط Branch های دیگر نیاز به یک واسطه که Router اصلی می‌باشد دارد. اما در حالت DMVPN فقط برای بار اول نیاز به Router اصلی می‌باشد و دفعات بعد Branch ها بعد از انجام تنظیمات (Configuration) می‌توانند به طور مستقیم با یکدیگر در ارتباط باشند

* نکته: VPN برای تکنولوژی VoIP اصلا مناسب نمی‌باشد

از QoS نیز پشتیبانی نمی‌کند. این سرویس مربوط به اولویت‌بندی Frame های ارسالی می‌باشد

- MPLS (MultiProtocol Label Service) :

مبحث IP :

- IPv4
- IPv6 :

در IPv6 ، Zone ID نیز تعریف شده است

ND : Neighbore Discovery ، IP Conflict

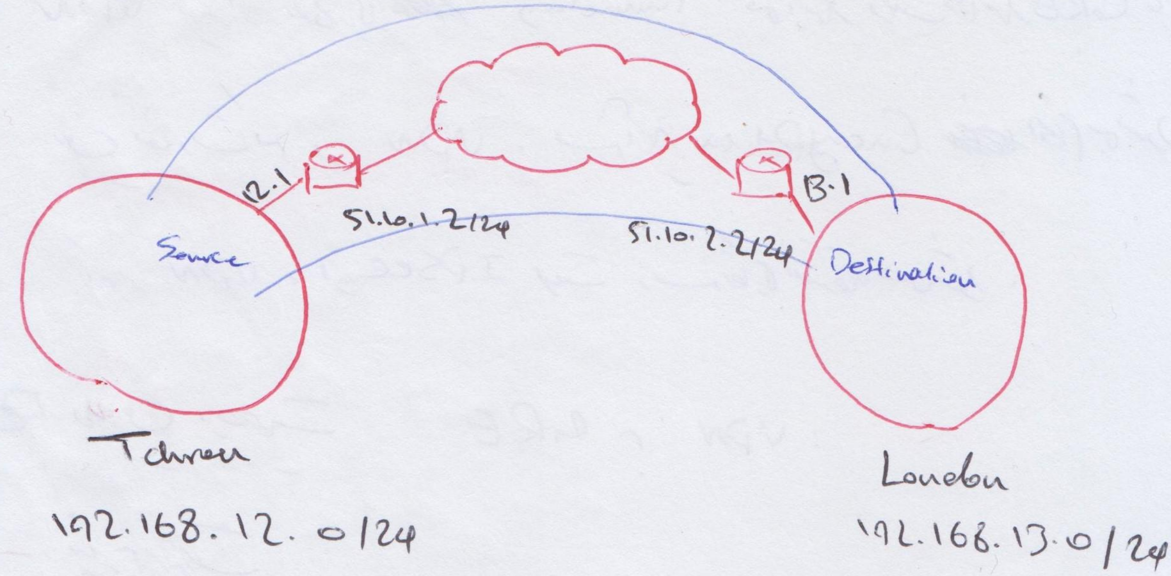
مبحث شبکه سازی :

GNS3 :

- GNS3 GUI
- GNS3 VM

Search : GRE Tunnel , DMVPN !

جلسه دوم ۹۷/۱۰/۷



* نکته: IP هر سمت در Range متفاوت باید مشخص شود

GRE (Generic Routing Encapsulation):

- ساده ترین پروتکل
- یکی از پروتکل های Tunneling میباشد.

Tunneling: چنانچه یک Packet داخل Packet دیگر ارسال شود را Tunneling گویند. بعنوان مثال Private → Public IP

یا IPv6 → IPv4

- چنانچه ساختار مشابه است، در صورتیکه Tunneling فرضاً باید هر Site دارای Router مجزا باشند و ضمن آنکه هیچگونه encryption انجام نمیشود و اطلاعات بصورت clear text ارسال میشود

- VPN نیز از تکنولوژی Tunneling می‌باشد و شبیه GRE ها با این تفاوت که در VPN، مسئله Encryption انجام می‌شود که در VPN، از IPsec جهت رمزنگاری استفاده می‌شود.

دلایل ارجحیت GRE به VPN:

- سربار کمتر
- تکنولوژی‌ای اطلاعات Voice در برابر تأخیر حساس هستند در این شرایط بهتر است از GRE استفاده شود.
- VPN فقط از ارتباط Unicast پشتیبانی می‌کند.

مراحل پیاده‌سازی GRE:

۱- ایجاد یک Tunnel Interface

۲- مشخص کردن Source و Destination برای Tunnel

۳- تعریف یک IP Address برای Tunnel interface

۴- انجام همان تنظیمات در Router دیگر

نکته: Source ها Public Interface می‌باشند

نکته: برای Destination نیاز است در Tunnel Destination فقط Public IP روتر مقابل را وارد کنیم.

دستورها :

interface Tunnel

~~Tunnel ...~~ <#> : برای گام (۱) :

Tunnel Source <IP خود> : برای گام (۲) :

Tunnel Destination <IP نقطه مقابل>
Public of Destination

برای گام (۳) : اختصاص IP به Tunnel ایجاد شده جدید :

IP address < = > < Subnet Mask >

Sh r int tunnel 1 : برای مشاهده تنظیمات :

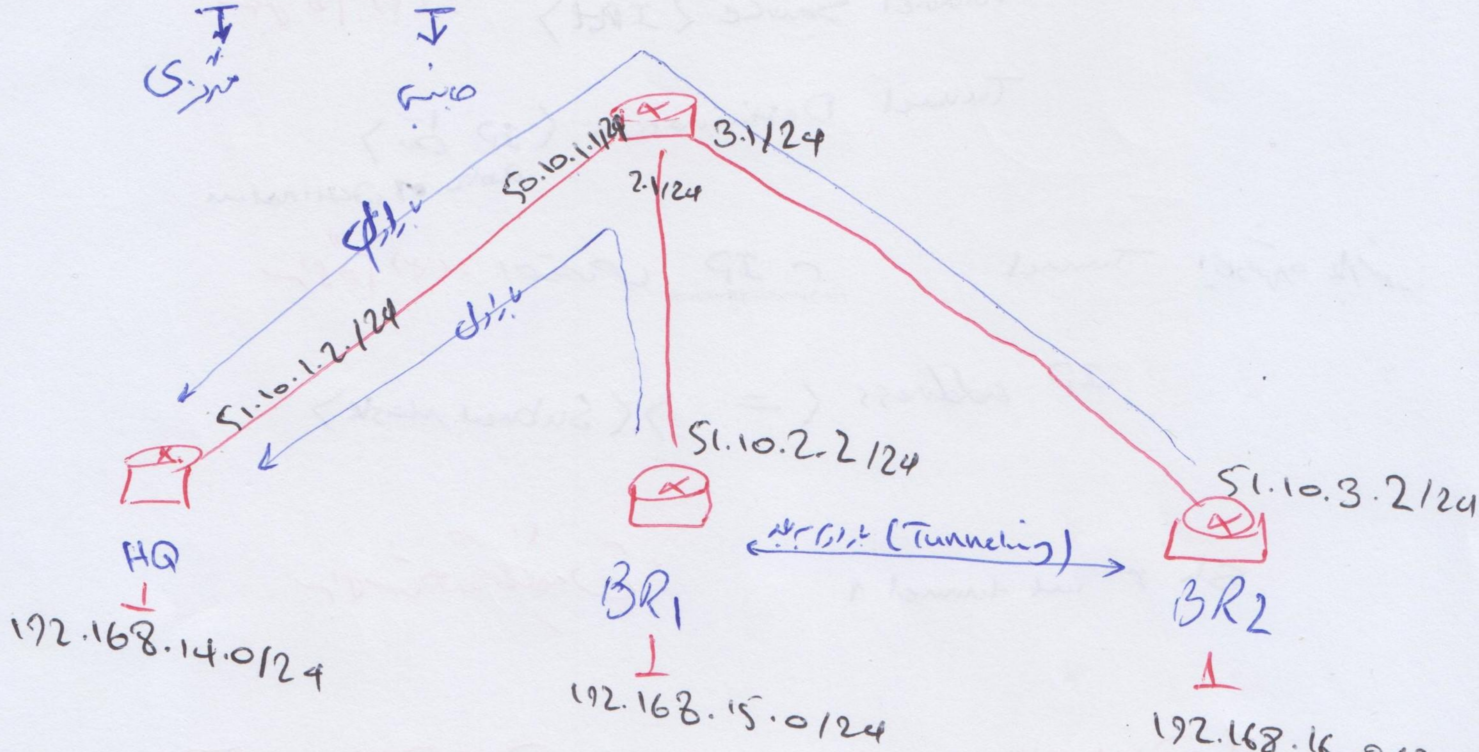
DMVPN یا Dynamic Multipoint VPN :

یکی از روش‌های Tunneling است که کاربرد آن در سناریوهای گسترده که شرکت با تعداد شعب زیادی Router (بیست یا بیشتر) به هم وصل شوند. در چنین شرایطی می‌توان به جای GRE Point to Point از روش DMVPN استفاده کرد.

در GRE استفاده می‌شد از ساختاری به نام Hub and Spoke به نحوی که یکی از office ها به عنوان Hub office یا مرکزی

تعریف شده و ارتباط ساختن و انتقال آن برقرار می‌شود.

EX: Hub and Spoke



NHRP (Next HoP Resolution Protocol):

پروتکلی است که پشت پرده ارتباطات DMVPN از آن استفاده می‌شود.
دلیل آن: پیاده‌سازی تنظیمات DMVPN هم زمانی که Router1 آمین
بخواهد با آمینی دیگری ارتباط یابد NHRP وارد بازی شده و اطلاعات
مربوط به Router مقصد شامل IP Public آن را در اختیار Router
مبدأ قرار می‌دهد. لازم به ذکر است که در کنار پیاده‌سازی تنظیمات DMVPN
تنظیمات NHRP نیز باید انجام می‌شود.

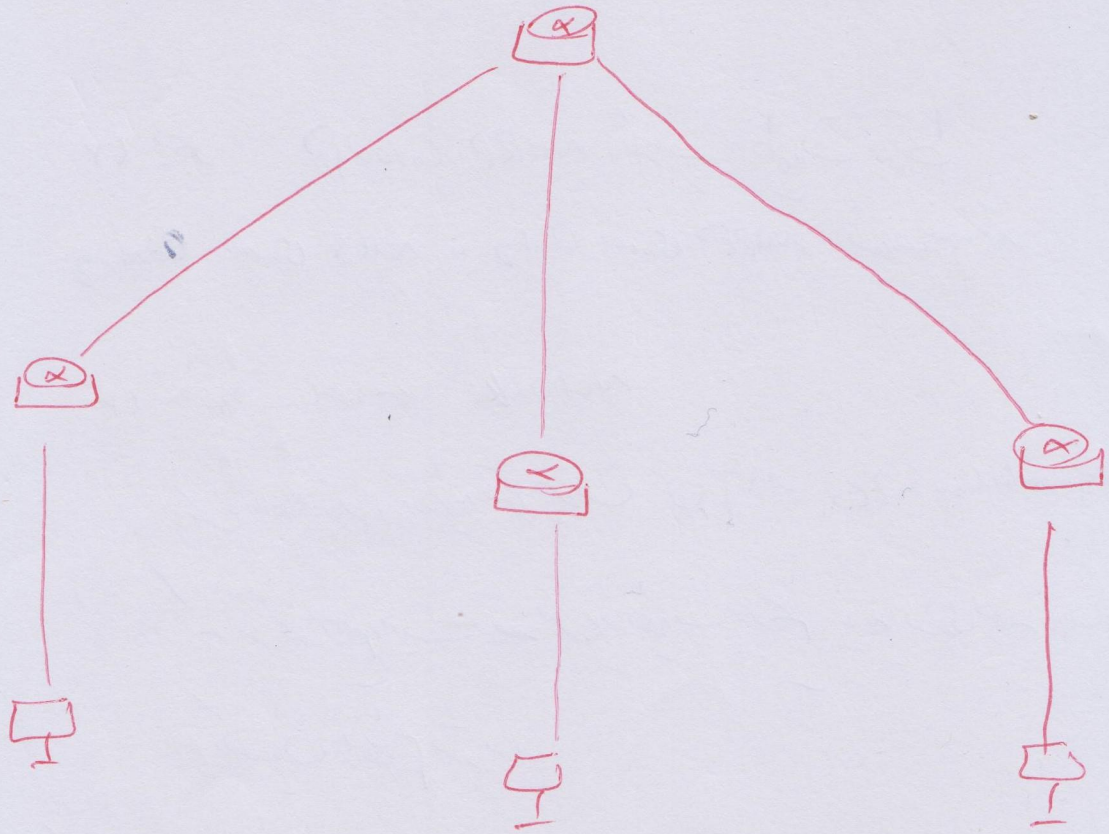
نکته: ①

: NHRP Server (NHS)

: NHRP Client

: NHRP Group

Ex: سناریو تنظیم DMVPN:



مراحل تنظیم DMVPN

١- تنظیم و تعریف کردن IP بر روی Interface های ISP Router

٢- " " " " " " " Branches

٣- " " " " " " " Lo VPCS

٤- تعریف کردن Static Route ها

کانفیگریشن DMVPN:

۱) تنظیمات تونل Tunnel

نکته: DMVPN = Multipoint GRE

این تونل بین کلیه Router ها کلیان می‌شود.

۲) ایجاد NHRP Group، تعریف تنظیمات مربوط

تنظیمات NHRP در سرور NHS و Config در سرور Config

۳) تنظیمات اضافی Network

مانند TCP Fragmentation Size، MTU و ... تنظیمات می‌شود.

نکته: اگر بخواهیم بیشتر این تنظیمات را بر روی همه Router ها اعمال

کلیان انجام شود

نکته: MTU (Maximum transfer Unit):

Search: Routing Protocol Choice

جلسه سوم ۹۷/۱۰/۱۴

• ادامه مبحث DMVPN :

مراحل Configuration DMVPN :

• تنظیمات مربوط به Server Router یا NHS :

۱) a) ایجاد int Tunnel <#>

b) tunnel source <int (Private IP)>

c) فرمان tunnel mode gre multipoint

d) فرمان tunnel key <Password> است. این Password باید روی تمامی Router های ارتباطی یکسان باشد. (اختیاری)

۲) e) فرمان IP nhrp network-id <#>

f) IP nhrp authentication <Password> (اختیاری)

g) IP nhrp map multicast Dynamic امکان ارتباط برای Multicast را فراهم می‌کند

h) اختصاص IP به int tunnel با ... , ... IP Address

۳) i) ip MTU 1400 ساختار سایز را به اندازه بسته تعریف می‌کنیم. (اختیاری)

j) ip tcp adjust-mss 1360 ساختار سایز MSS را تعریف می‌کنیم (باید 40 بایت کمتر از MTU باشد)

(در صورت ... فرمان c ، ... هم باید تعریف شود در صورت کدام ... c ، ... این مرحله است)

• تنظیمات مربوط به Client Router یا NHRP :

a-g) تمام مراحلی که برای Server Router انجام دادیم یکسان است

h) IP nhrp nhs <... Private for Server>

i) IP nhrp map <Private IP for Server> <Public IP for Server>

j) IP nhrp map multicast <51.10.1.2> Public IP of Server

k) اختصاص IP به tunnel int معین شده

l) IP mtu 1400

IP tcp adjust-mss 1360

m)

(*) نکته : کپی (Copy) گرفتن : Sh run int tunnel(#)

Routing Protocol Choice :

- RIP*, OSPF*, EIGRP*, BGP*, IS-IS, IGRP

۱) داخلی یا خارجی بودن

داخلی (IGP) : RIP, OSPF, EIGRP

خارجی (EGP) : BGP

۲) سایز Network

• کوچک (Small) : RIP
  - v1 :
  - v2 :
  - RIPng :

- v1
- v2
- RIPng (مربوط به IPv6)
- Maximum Hop Count (Distance Vector)

• EIGRP (Medium to large):

- Distance Vector
- اول صفر مخصوص Cisco میباشد

• OSPF (Medium to large)

- پرکاربرد ترین

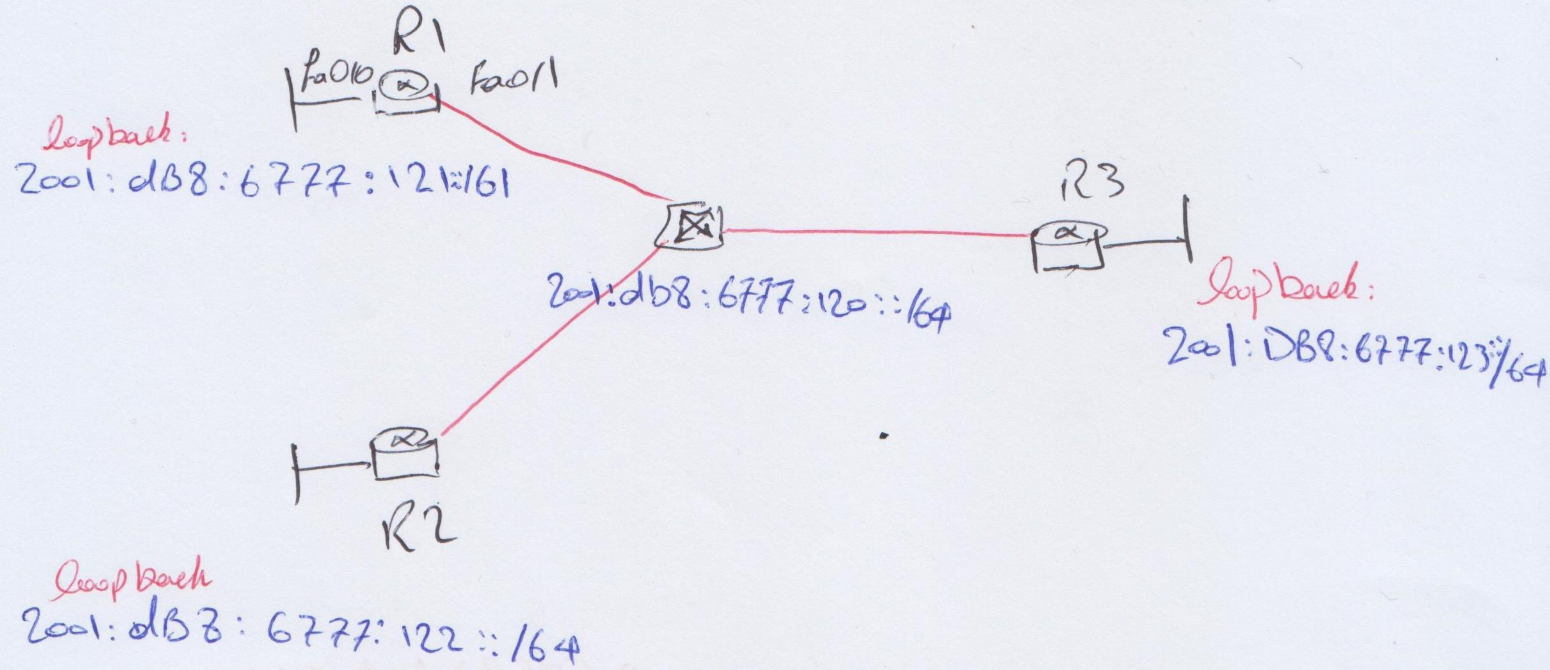
• BGP:

- تنها پروتکل EGP و Exterior میباشد
- Redundancy

englisCentral.com

Payment 24.com

2001:dB8:6777:012::/60



مراحل کانفیگوریشن : RIP ng

⊛ نکته: جهت شروع مسیریابی با استفاده از IPv6 وارد کردن دستور IPv6 Unicast-Routing الزامی است.

EIGRP Packets : ! Search

جلسه چهارم ۹۷/۱۰/۲۱

EIGRP Authentication :

بصورت پیش فرض اگر EIGRP شروع شود هیچ نوع Authentication یا
تایید اعتبار انجام نشده و صرفاً کافیست در Router های AS یکسانی
بوده و Neighbor داشته باشند تا Routing Advertisement
را شروع کنند و به دلیل توجه به اینکه یکی از Router مقابل اطلاعات خود
را برای آن ارسال می‌کند. در این شرایط ممکن است یک کاربر که صاحب یک
Router باشد وارد Network شده و با اتصال آن به یکی از Port های شبکه
و سپس نوشتن تنظیمات EIGRP بر Router های ما اقدام
به تشکیل Neighborship با Router های ما کند و Sniff کند و همه
Route های جعلی و بی ارزش خود را برای آنها ارسال کند

Key chain :

یک جدول یا Database است که از آن می‌توان برای ذخیره‌سازی و نگهداری کلیدهای احراز هویت استفاده کرد. درون یک Key chain می‌توانیم یک یا چند کلید داشته باشیم.

Key :

المان‌های اصلی‌ای درون Key chain می‌باشد که از آن برای تحلیل کلیدهای مختلف و نگهداری آن‌ها استفاده می‌شود.

Key String :

یک مقدار یا Value می‌باشد که به هر کلیدی اختصاص می‌دهیم. به زبان ساده Key String همان پسورد است.

مراحل Configuration :

۱) ایجاد حداقل یک Key chain برای نگهداری کلیدها

۲) ایجاد حداقل یک کلید داخل Key chain

۳) تعریف یک Value برای کلید یا همان Key String

۴) اتصال به Interface در Router و یا Neighbor مورد نظر و سپس تعیین Mode یا روش Authentication و Apply کردن key chain برای آن.

* نکته: Password ها Keysensitive هستند.

* نکته: انتخاب پروتکل MD5 جهت Encryption

١) امر رقم (٧) : key chain <word> ①

٢) امر رقم (٢) : key 1

٣) امر رقم (٣) : key string <word> (identical)

٤) امر رقم (٥) :

داخل interface من جهة شبكة سيتم تشغيل التشفير

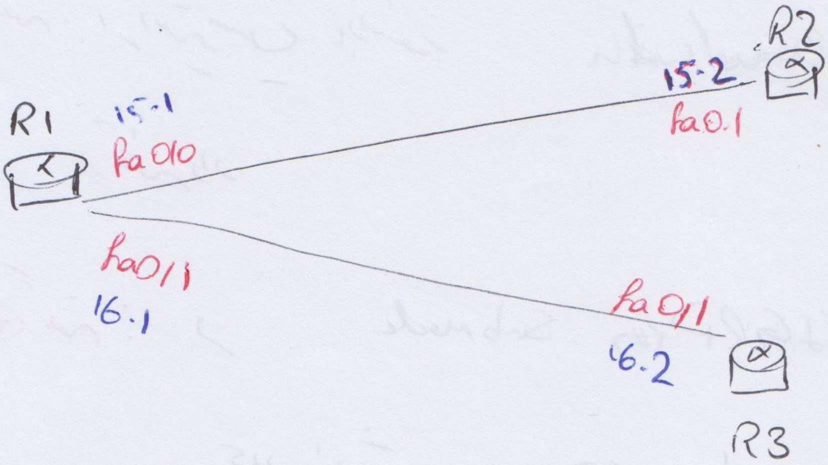
IP authentication mode eigrp <#> md5

IP authentication key chain eigrp <#> <word> ①

EIGRP Load Balancing :

أنواع Load Balancing

• Equal cost :



FD = FD

در صورتی که پهنای باند ، Load ، Relibility ، uptime مساوی باشند، Router می تواند خود ارسال Packet ها را بصورت Equal Cost انجام می دهد.

• Unequal Cost :

- به این مفهوم، از Unequal Cost در EIGRP پشتیبانی می کند، در صورتیکه پهنای باند در لینک ها هم مساوی نباشند EIGRP نیز به نسبت ظرفیت پهنای باند، حجمی از Packet را ارسال می کنند.

Varience : عددی است که با آن می توانیم مقدار FD را با ضریب آن عدد تا اندازه FD یک link بالا ببریم و با مسیر Successor هم وزن شود.

جهت اعمال تنظیمات برای مجاز کردن خاصیت Load Balancing

* نکته: در انتخاب مسیر با پروتکل EIGRP ابتدا Bandwidth مسیرها را بررسی می‌کند و سپس Port!

نکته دارد.

* نکته: در EIGRP (#) Sub Mode دستور Variance (#) را تنظیم می‌کنیم.

کلا در شبکه، FD مربوط به Successor می‌باشد.

* نکته: دستور Reset کردن Neighber

Clear IP eigrp neighbors

EIGRP Stub : Search

جلسه پنجم ۹۷،۱۰،۲۸

تنظیمات پایه برای EIGRP :

Passive interface :

یکی از مباحثی است که Routing Protocol ها مطرح می‌شود. زمانی به آن می‌پردازیم که بخواهیم یک Interface خاصی را Mode Passive قرار دهیم و نسبت به ارسال Hello Packet ها منفعل باشد. در واقع زمانی که این option را برای Interface خاصی فعال می‌کنیم ارسال Hello Packet ها از آن اینترفیس متوقف شده اما Route مربوط آن به بقیه Router ها Addvertise می‌شود.

نکته: هنگامی که Router به دلیل ارسال Hello Packet ارائه دهد یا اتصال کند [illegible] Router [illegible] نفوذ به شبکه برایش امکان‌پذیر می‌شود [illegible]

نکته: دستور مانیتور کردن Hello Packets

eigrp debug Packet Hello

نکته: دو دلیل برای دستور Network Command

۱) ارسال Hello Packet به مبادی همسایگی adjacency

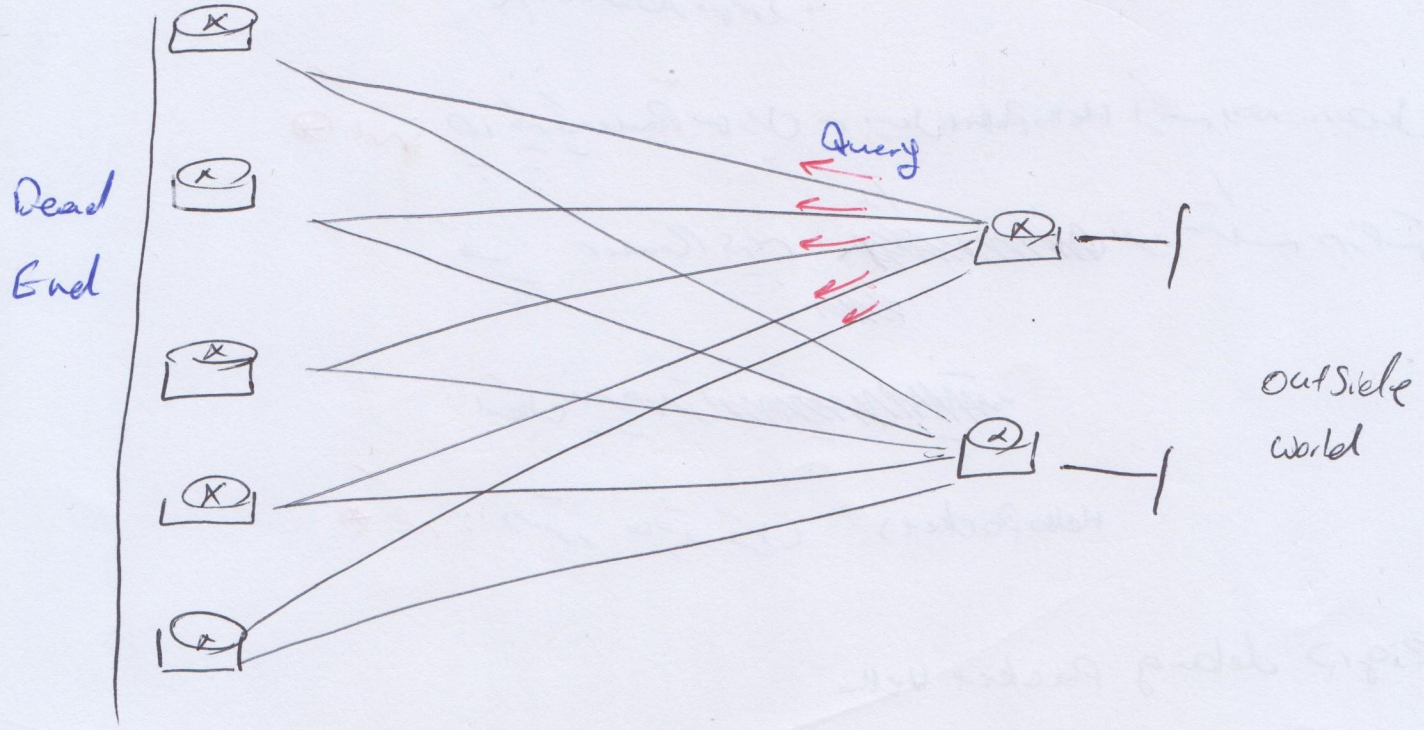
۲) Advertise کردن Lo Interface

اعمال تنظیمات Passive-Interface:

۱) وارد مد روتر می‌شویم

۲) دستور Passive-Interface < نام اینترفیس > (عضو نمی‌شود Hello ارسال نمی‌کند)

*) دستور Sh IP Pro نمایش تنظیمات مربوط EIGRP



Passive : زمانیکه یک حالتی که Router طبق روال معمول کار خود را انجام می‌دهد.

Active : زمانیکه یک حالتی که Router با اتفاقاتی که پیش‌بینی نشده مواجه می‌شود و باید برای حل آن اقدام کند.

Stuck in Active (SIA) :

زمانیکه یک Router درخواست Query Packets را ارسال می‌دهد اما جوابی از روترها بعد از گذشت زمان مورد انتظار دریافت نمی‌کند، در این شرایط Router وضعیت Active باقی می‌ماند و این شرایط شرایط نامطلوبی است.

EIGRP Stub : مفید برای اجرای Configuration

Stub Mode ها :

۱) Recieve - only : فقط دریافت

۲) Connected : فقط ارسال آدرس‌هایی که به طور مستقیم Connect است

۳) Static : فقط به Query هایی مربوط به Static Routing است پاسخ می‌دهد

۴) Summarized : Route هایی که Summarized شده اند

۵) Redistributable : برای ارتباط EIGRP به پروتکل‌های دیگر

⊛ نکته: اگر هیچ Mode برای آن روتر تعریف نشده باشد، به طور پیش‌فرض Connected + Summarized تعریف شد.

⊛ مراحل کانفیگ EIGRP با استفاده از IPV6 :

۱) انجام تنظیمات اولیه IPV6

۲) فعال کردن IPV6 Routing

۳) فعال‌سازی کانفیگ EIGRP برای IPV6

۴) Apply کردن تنظیمات برای اینترفیس‌های مورد نظر EIGRP

Resume برای کارش

Python programming for network engineering

۱) دستور گام اول: IPV6 Address

⊛ نکته: Router برای Convergence در IPV6 ، از advertise ها Linked Local IP استفاده می‌کند.

۲) دستور گام دوم: IPV6 Unicast-routing

ipv6 router eigrp 1

۳) مرحله گام سوم:

eigrp router_id <IP Address Format>

IPV6 Router eigrp برای no shutdown
نیاز داره که فعال بشه

٤) مرحله گام چهارم: وارد اینترفیس می‌شویم

IPV6 eigrp < # > شماره
مرحله

این تنظیمات روی این Port اختصاصی داده می‌شود.

(۱)

جلسه هفتم ۹۷/۱۱/۱۲

OSPF Authentications :

Clear Text Authentication :

در شبکه‌ی Public توصیه نمی‌شود چرا که اطلاعات به صورت Clear-text می‌باشد

MD5 Authentication :

در شبکه‌های Public استفاده می‌شود اطلاعات پسورد به صورت رمزنگاری شده ارسال می‌شود.

مراحل Clear Text Config :

۱) اتصال به Interface مشترک که Hello Packet ها از طریق آن ارسال می‌شوند

۲) فعال کردن Authentication برای OSPF با اجرای دستور

IP OSPF Authentication

۳) تعریف یک کلید یا پسورد با اجرای دستور IP OSPF Authentication-key (key)

۴) تکرار این مراحل برای روتر مقابل

* نکته: تنظیمات فوق در سطح interface انجام می‌شود نه در سطح روتر و برای هر Router باید تنظیمات جداگانه‌ای انجام داد

* نکته: جهت مشاهده تنظیمات OSPF مربوط به interface

Sh IP OSPF fa (شماره)

* نکته: پسوردها Key Sensitive هستند

* نکته: وضعیت Aut را با استفاده از دستور Sh ip OSPF Packet نشان می‌دهد

aut = 0 ← تعریف نشده ، aut = 1 ← Clear text ، aut = 2 ← MD5 Authentication

★ نکته : برای تعریف Authentication در سطح Area میتوان به این صورت

در گام اول دستور زیر را وارد میکنیم . که در سطح روتر میباشد نه در سطح اینترفیس و نیازی نیست

Area <Area-ID> Authentication

بعد از دستور router ospf 1 میباشد.

★ نکته : برای غیرفعال کردن هم باید گام سوم هم گام چهارم را غیرفعال کنیم

مراحل MD5 Authentication :

۱) اتصال به interface مشترک

۲) تعریف یک کلید با فرمت MD5 که با اجرای دستور

IP OSPF Message-digest-key <Key-ID> md5 <Key-Value>

۳) فعال سازی Authentication با اجرای دستور

IP OSPF authentication Message-digest

★ نکته : Key-ID ها باید یکسان باشد

(۲۷)

: OSPF Path preference

$$\text{Cost} = \frac{\text{Refrence Bandwidth}}{\text{interface Bandwith}} \Rightarrow 100 \text{ Mb/s}$$ پیش‌فرض

تعریف: Cost : معیار، کوالیتی Metric در پروتکل OSPF

نکته: دستور نمایش Refrence Bandwidth جهت انتشار

sh ip pro | include Refrence

sh in fa < > | include BW

sh ip ospf int fa0/1 |

sh ip ospf int fa0/1 | include cost

نمایش Cost

مراحل تنظیم هزینه Cost :

۱) وارد تنظیمات پروتکل OSPF می‌شویم

router ospf <#>

۲) هزینه را اجرا می‌کنیم

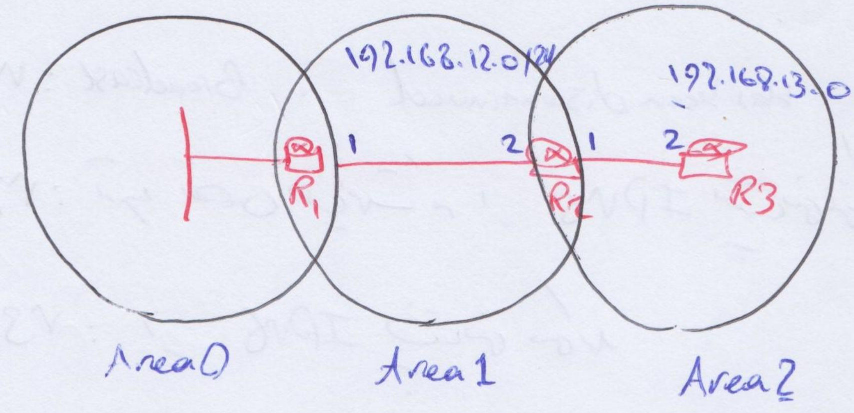
auto-cost refrence-Bandwidth <1000>

۳) تمام تنظیمات فوق برای Neighbour Router

نکته: فاکتور فوق کمی از لایه ۲ کیفیت هزینه باشد را انتخاب مسیر تحت فاکتورهای دیگر کنترل هستند.

(۴) Star is born

Virtual LINK :



★ نکته: اینترفیس ها فقط مجاز به Area <#> متصل باشند.

مراحل Virtual link Configuration :

۱) وارد OSPF # میشویم

Router OSPF < >

۲) دستور زیر را تایپ میکنیم

Area <Area ID> Virtual link <next Router RID>

(*) نکته: دستور مشاهده تنظیمات Virtual link

Sh ip ospf virtual link

(*) نکته: Transit Area :

به Area های میانی یا بین دو Area که باعث اتصال Virtual link می شود Transit Area گویند

Configuring OSPF v3 :

v1 : Broadcast ؛ Has been discontinued

v2 : تنها قسمتی از اینترنت که از IPv6 پشتیبانی نمی‌کند

v3 : از IPv6 پشتیبانی می‌کند

مراحل OSPF v3 Configuration :

۱) انجام تنظیمات پایه Networking

۲) فعال‌سازی روتینگ از طریق IPv6 با دستور

IPv6 Unicast-routing

۳) فعال‌سازی OSPF v3 را با استفاده از دستور زیر فعال می‌کنیم

ipv6 Router OSPF <PID> (Process)

۴) قرار دادن یک Router ID از جنس IPv4 با استفاده از دستور

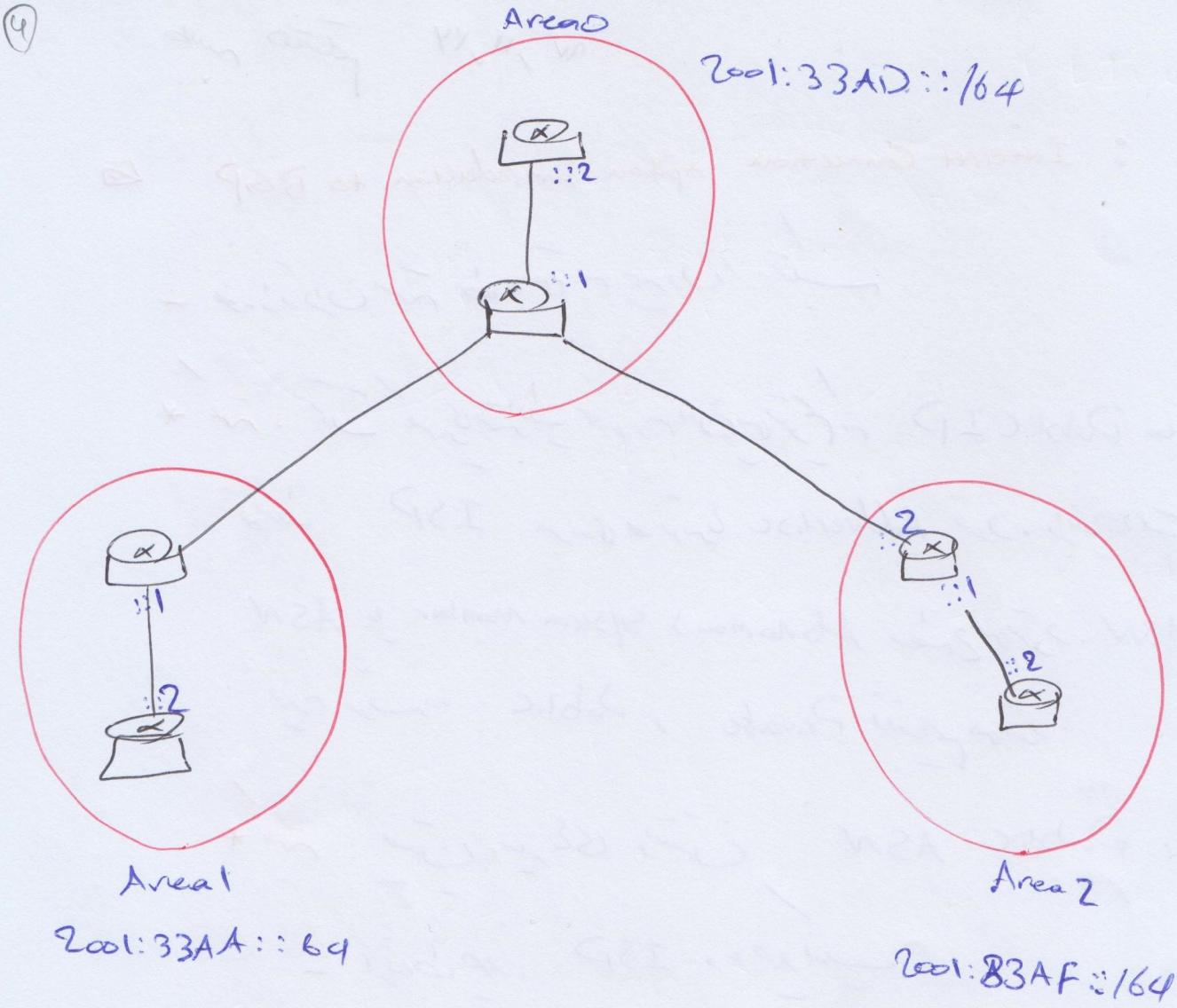
Router ID <IPv4>

۵) انتخاب اینترفیسی که می‌خواهیم Hello Packet ها از طریق آن ارسال شود

۶) دستور IPv6 OSPF <Pid> area <area ID>

۷) مراحل فوق را برای دیگر Router ها اجرا می‌کنیم

(4)


Area0
2001:33AD::/64
::2
::1
::1
::2
2
::1
::2
Area1
2001:33AA::64
Area 2
2001:B3AF::/64

جلسه هشتم ۹۷,۱۱,۲۶

Internet Connection option Introduction to BGP :

- خود وارد دادن شبکه اطلاعاتی به بیرون از شبکه

* نکته: یک سری شرایط مجبور به این میشویم که Public IP ما توسط ISP جزودی ما توسط Addvertise شود. واندر حالت ASN یا Atonomous System Number مشخص میشود. ASN نیز به دو دسته Public و Private تقسیم میشود.

* نکته: پیش نیازهای داشتن Public ASN :

- ارتباط چند ISP و یا چند شبکه
- Addvertise کردن شبکه Public IP

* نکته: تحت چه شرایطی از BGP نباید استفاده کرد:

- زمانی Router های قدرتمند نداریم
- توانایی اطلاعات با حجم بالا از ISP های گوناگون را داشته باشند
- حافظه مناسب جهت ذخیره سازی آن اطلاعات را داشته باشند.
- پهنای مناسب نداشته باشیم (اینترنت باید مناسب برای دریافت آپدیت های BGP)
- فقط به یک ISP متصل باشیم
- عدم شناخت کامل BGP

* نکته: در چه مواقعی باید از BGP استفاده کنیم؟

- زمانیکه نیاز به در دسترس بودن در سطح بالا باشیم و باید چندین لینک با چندین ISP داشته باشیم.
- زمانیکه خودمان یک ISP باشیم

* نکته: به BGP در ISP ها، Transit BGP گویند.

* نکته: در BGP می‌توان با شبکه ها untrusted نیز ارتباط برقرار کرد.

✍ ویژگی های پروتکل BGP :

- از TCP Port 179 استفاده می‌کند
- updateها در زمانهای مختلف فرستاده می‌شود
  - هر 5 ثانیه یکبار برای Routerهای یک AS
  - هر 30 ثانیه یکبار برای Routerهای AS مجزا
- محاسبه شرط بسیار پیچیده می‌باشد (برای انتخاب بهترین مسیر)
- تنها پروتکل دنیای اینترنت
- Convergence بین Routerهای Trusted , Untrusted
- روتینگ از طریق ASN بجای IP
- کندترین Routing PROTOCOL دنیا
- در دو مد Mode تنظیمات اعمال می‌شود
  - IBGP : هر دو در یک AS باشند
  - eBGP : در دو AS متفاوت باشند

(۹)

تنظیمات پایه ای BGP : با تشریح کد مسئله به توضیح این مبحث می پردازیم:

R1 برای : AS 227

IP : Internal •

192.226.13.1 255.255.255.248

IP با : External •

86.23.11.1 255.255.255.252

R2 برای

IP با : Internal •

198.226.13.2 255.255.255.248

ISP1 برای : AS 718 (ISP)

~~ISP1~~

IP با : External •

86.23.11.2 255.255.255.252

: Loopback •

10.10.10.1 255.255.255.0

۱) آیپی (IP) دادن به Port یا interface ها

*نکته: فرمان desc برای اختصاص دادن توضیحات به int استفاده می‌شود

۲) با فرمان Router BGP(ASN) ، BGP را فعال می‌کنیم

*نکته: برای نشان دادن اینکه ISP 1 مشخص می‌کند Interne Service Provide

سوال نکرده، یک Default Route روی آن Configure می‌کنیم.

IP Route 0.0.0.0 0.0.0.0 LO

LO → به تعریف دادیم Loopback int

۳) وارد کردن Network ها به شکل زیر Network Command

Network <IP> Mask <SubnetMask>

(*) نکته: Neighbor ها را نباید به صورت دستی وارد شوند.

(*) نکته: حالت Optimal برای ASN advertis را باید منتشر کرد.

(*) نکته: در دنیای BGP هیچگاه Private IP ها Addvertise نمی‌شوند

۴) شناساندن Neighbor ها به شکل زیر

Neighbor <Neigbor IP Address> remote-as <Target Network AS>

۵) اعمال تغییرات مشابه برای Router های دیگر

* نکته : دستور Sh ip bgp در تشخیص کمک میکند

*<> : بهترین مسیر

: Weight

* نکته : دستور Sh ip bgp summary

* نکته : دستور Sh ip bgp Neigbors

مهم *** : پارامترهای تصمیم گیری BGP در انتخاب بهترین مسیر و توضیح آن :

به ترتیب اولویت انتخاب بهترین مسیر (attribute)

۱) Weight <#> :

- روترهای با Weight بیشتر شانس انتخاب بیشتر

- مخصوص روترهای Cisco می‌باشد

۲) Local Preference :

- داخل یک AS مطرح می‌شود

۳) Originate :

- روتی را ترجیح قرار میدهد که از خود او نشات گرفته باشد

یعنی اگر Default Route در روتر تعریف کند

Default Route را انتخاب نمیکند آن را خود BGP را انتخاب می‌کند.

۴) AS Path Length :

- در eBGP مطرح می‌شود

- طول پایینتر شماره AS ملاک انتخاب است

(۱۲)

۵) Origine Code :

- بین ~~iBGP~~ IGP ، ~~eBGP~~ EGP ، ~~iBGP~~ IGP اولویت دارد

- بین در iBGP ها ، بین در پروتکل EIGRP ، OSPF

Administrative Distance را مقایسه می‌کند

- بین در iBGP ها ، با پروتکل‌های یکسان ، به ازای مقدار AS های مشترک

و با cost (بسته به نوع پروتکل یکسان) مقایسه و بهترین مسیر انتخاب

می‌شود

۶) MED (Multi exit discriminator) :

- مسیرهای با MED کمتر اولویت انتخاب دارند

- فقط Contigue هستند

۷) eBGP Path over iBGP Path :

۸) Oldest Path :

- هرچه سن مسافت Path بیشتر باشد در اولویت هستند

۹) Route-ID :

- روترهای با ID پایین‌تر در اولویت هستند

۱۰) IP Address

- آنهایی که IP Address کمتر داشته باشند

٩٧, ١٢, ٣

: Connection

: Logical Security

: Line Password

: Normal telnet Connection

Line password (١

Enable login command (٢

Transport input (٣

: Remote Connection with a username & pass

* نکته: فعال کردن Telnet در windows

* نکته: سطح دسترسی و تعیین آن را حتماً طبق کتاب بنویسید

* نکته: local login: یعنی افرادی که از دسترسی حضوری به روتر و سوئیچ برخوردار باشند login کنند.

AAA Authentication:

- Local Authentication:

هر دیوایس خودش مسئول تنظیمات آن می‌باشد
که تنظیمات به جای دیگر ارسال نمی‌شود.

مانند workgroup بودن در windows تنظیمات به هم مشترک نمی‌باشد.

- AAA (Accounting Authorization Auditing) می‌باشد.
- مدیریت و ثبت Username و Pass به صورت متمرکز است که آن را Remote Authentication نیز می‌گویند.
- استانداردهای Remote Authentication (Cisco)

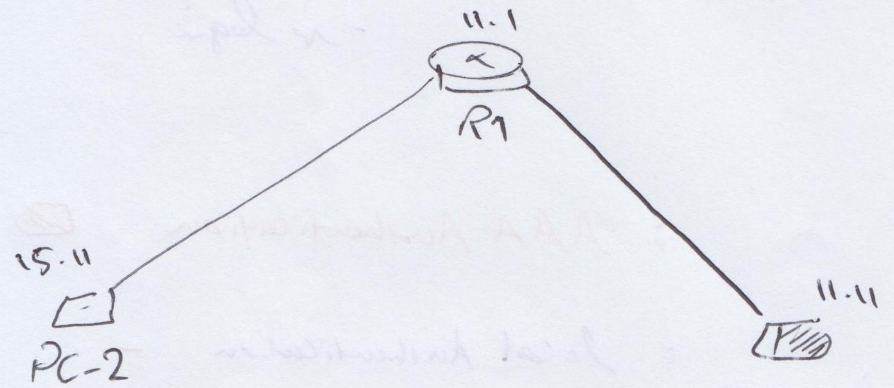
RADIUS :

- متنی Platform ، مورد پشتیبانی توسط سازمان IETF
- قابلیت Assign کردن یک user دستور برای Privileged

TKACAS :

- سرویس مشترک بین Cisco , Linux

* نکته : امنیت RADIUS ضعیف‌تر می‌باشد



Tina : Admin Mode 15

Farhad : IP Addressing

Bob: 1

* نکته :

○ NPS : برای نصب RADIUS Role نصب این سرویس الزامیست

○ IAS :

توضیحات در چند مرحله بیان شود:

(۱۷)

جلسه دهم ۸۷,۱۲,۱۰

Configur and verify Access List :

- فیلتر کردن یا محدود کردن دسترسی Packet های ارسالی
- هر Packet دارای هدر مشخصی است

Header
Data

Header → Source Address, Destination ", Source Port, Destination "

- تطبیق Rull ها از ابتدا تا انتها
- Implicit Deny Rull : آخرین Rull نامرئی به همه پکت‌ها را Deny می‌کند

انواع Access List :

- **Standard :**
- پرکاربردترین نوع Access List
- بر اساس Source Address یک Packet را Permit یا Deny می‌توان کرد.
- Syntax

Permit / Deny

AccessList ⟨1-99⟩ ⟨Action P/D⟩ ⟨Source info⟩

- Assign کردن Rull ها به یک interface خاص، مشخص کردن inbound یا outbound بودن آن.
- طبق استاندارد Cisco بهتر است این نوع Access List به نزدیک‌ترین int به مقصد اختصاص داده شود.

(۱۸)

Extended ACL :

- هر سمت Source هر سمت Destination اعمال تعریف را داریم

- Syntax کدنویسی

Permit / Deny

Access List <100-199> <Action PID> <Port or Protocol>

TCP/UDP/IP/ICMP

<Source info> <Destination info>

- پیشنهاد Cisco بر این است که این نوع Access List را تا نزدیک‌ترین interface به مبدا اختصاص دهیم.

*نکته:

Game، instante Messaging، Voice، ویدئو، فیلم : UDP پروتکل : Delay Sensitive

TCP پروتکل : TCP هم پروتکل‌ها را شامل می‌شود

IP پروتکل : تمام پروتکل‌ها

Trace، Ping پروتکل‌های مخصوص چک کردن شبکه. Echo : ICMP

- دستور Syntax اختصاص دادن Rull به interface

IP Access-group <#> in

Deny Host 1 from Access List to Facebook.com : EX ☐

بعد از host IP شماره پورت هم می‌باشد

Access List 101 deny TCP host 192.168.1.11 ①

<eq : دقیقاً همین پورتی که وارد کنیم اعمال شود ②

gt : بالاتر از Port Range

lt : پایین‌تر

neq : همه بسته شوند بجز پورتی که وارد می‌شود

* نکته: در شبکه سری پورت‌های Network یک Source Port داریم و یک Destination Port داریم. Destination همیشه ثابت هستند چرا که وقتی سایت Facebook می‌روید همیشه HTTPS می‌باشد. اما Source پورت همیشه متغیر است

Named ACL : ☐

Syntax

ip Access-List <Standard / Extended> <اختصاص دادن یک نام>

* نکته: Sequence Number در Named Access list امکان‌پذیر است.

Reflexive (Established) :

— از ورود ترافیک های ناخواسته جلوگیری می‌کند.

Time-based ACL :

- Priodic : شروع دستور در دوره‌ی خاصی از زمان به طور متوالی و مکرر
- Absolute : یکبار شروع می‌شود و اجرا می‌شود تا زمان توقف زمان اتمام

— Configuration :

۱) وارد کردن دستور

Key sensitive ↑

Time-range weekends

۲a) دستور وارد کردن دستور

Periodic <روزهای هفته> <ساعت> to <ساعت>

۲b) وارد کردن

absolute start <end/start>

۳) تعریف و وارد کردن دستور

null <Time-range <TimeRange نام>>

جلسه یازدهم ۹۷/۱۲/۱۷

مراحل انجام یک پروژه از ابتدا تا انتها:

۱- برنامه ریزی و طراحی اولین مرحله از انجام پروژه (Design and planning)

بررسی نیازها و بررسی امکانات موجود و تشخیص و طراحی تجهیزات مناسب برای پروژه

۲- پیاده سازی و اجرای پروژه (Deployment)

۳- مانیتورینگ شبکه

مانیتورینگ در Cisco :

پروتکل SNMP را برای مانیتورینگ به کار می‌برند.

Simple Network Management Protocol

SNMP v1 : 1988

SNMP v2 : v1 (Authentication, Encryption ندارد)

SNMP v3:

SNMP Components :

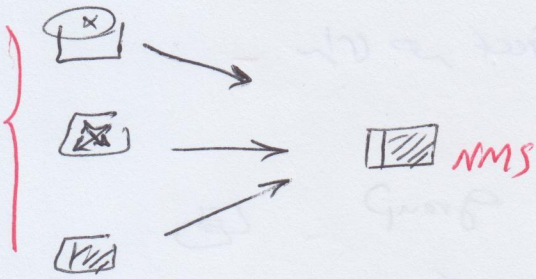
SNMP Manage Devices and resources :

هر آن چه در دیوایس و سرویس یا برنامه‌ای که آن را به وسیله‌ی SNMP مانیتور می‌کنیم.

NMS (Network Management Server) :

دیوایس مستقلی که logها و گزارشات دریافتی آن ذخیره می‌شود و از آن می‌توان دیتا را پیدا کرد.

: SNMP agent



: OID (object IDentifier)

: MIB (Management Information Base)

: Basic SNMP Configurations

: SNMP View

: SNMP group

: SNMP User

SNMP View :

- برای هر object که می‌خواهیم دسترسی بدهیم یک view باید ایجاد کنیم

SNMP group :

- ساخت یک گروه به منظور تعیین سطح دسترسی را گروه که گفته شد

SNMP User :

- ساخت یک user جهت تعیین تا مقدار اعتبار، که عضو گروه تعریف شده باشد در بر

مراحل Configuration :

۱) اجرای دستور زیر برای ساخت View

SNMP_Server View ⟨name⟩ ⟨MIB⟩ ⟨include/Ex⟩

↓ object ID یا name

۲) اجرای دستور زیر برای ساخت group

SNMP_Server group ⟨name⟩ ⟨V1, V2c, V3⟩ ⟨auth/noauth/Priv⟩ –

⟨نوع سطح دسترسی⟩ ⟨View نام⟩

- auth: فقط auth
- noauth: نه auth نه Encryp
- Priv: هم auth هم Encry

۳) اجرای دستور زیر جهت ساخت User

SNMP_Server User ⟨User نام⟩ ⟨مشخص کردن گروه برای user⟩ ⟨V3⟩ ⟨auth⟩ ⟨Encry پروتکل⟩ –

(گروه برای user، مثال: Ali، نیوز) (پروتکل: Md5/Sha)

⟨Password⟩ ⟨auth/noauth/Priv⟩ ⟨Encryption Protocol between two devices⟩ –

↓ APP پروتکل برای Encryption

⟨Pre shared key⟩

* نکته: PRTG نرم افزار مدیریتی جهت کنترل دیوایس ها می باشد و Agentless می باشد.

درس: Configure and verify logging :

گزارش تغییرات تنظیمات که بلافاصله پس از انجام دادن آن تنظیمات نمایش داده می شود، که به آن SYS log messages گویند.

* نکته: در صورت مدیریت و انجام تنظیمات از طریق Remote این گزارشات به طور پیش فرض نمایش داده نمی شود که با دستور زیر می توان امکان آن را فعال کرد

terminal Monitor : Show دید

logging Con Conf دید

غیرفعال کردن گزارش پس از هر تغییرات بر روی خود دیوایس (Local)

Show logging : نمایش تغییرات قبلی

logging Buffered : فضای اختصاصی

* نکته: فضای [illegible] SYS log به طور پیش فرض 8122 که حجم گزارشات می باشد

* نکته: اگر بخواهیم گزارشات بیشتری بر روی RAM ذخیره شود از دستور زیر استفاده می کنیم

logging Buffered < ظرفیت دلخواه >

* نکته: دستور نمایش میزان RAM اختصاص داده شده برای حجم گزارشات

Show logging | include Log Buffer

[نکته] SYS log Server :

از آنجایی که گزارشات اول در RAM ذخیره می‌شود و سپس در Local ذخیره می‌شوند

پس هیچ گونه پشتیبانی ندارد، مجبور می‌شویم که یک SYS log Server راه‌اندازی

کنیم که بعد از آن این گزارشات در روی یک دیوایس دیگری ذخیره می‌شوند.

برای این منظور نیاز به نصب یک APP می‌باشد. APPهای کوی: Manage Engine

و TFT32 ، نرم‌افزارهایی هستند که می‌توان از آنها برای SYS log server

استفاده شود.

[نکته] SYS log Server Configuration :

۱) اجرای دستور زیر

دستور logging <IP>

IP سروری که نرم‌افزار SYS log Server نصب کردیم

[نکته] تنظیمات Time Service : مهم مهم مهم

هماهنگ کردن زمان سروری سیستم‌های شبکه از نظر امنیت ضروری است

[نکته] مراحل Config :

جلسه دوازدهم ۲۳/۱/۹۸

DHCP :

Static

Dynamic

DHCP Component :

DHCP Server :

سرویس‌دهنده‌ی DHCP Server می‌تواند Routers، Servers، L3 Switches باشد.

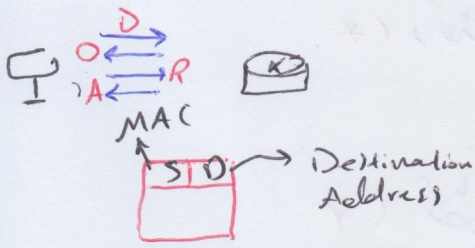
DHCP client :

Client درخواست IP خود را از DHCP Server دریافت می‌کند.

DHCP Pool :

تنظیمات مربوط به آدرس‌دهی در DHCP Pool تعریف می‌شود.

IP Addressing Process :



۱) Discover
۲) Offer
۳) Request
۴) Acknowledge

DORA

Minimal DORA ← ۳ و ۴

* نکته: IP سرور DHCP Server باید از نوع Static باشد.

۱) فعال کردن سرویس DHCP

IP DHCP Pool < name >

۲) IP Range تعریف می‌کنیم

Network 192.168.12.0

۳) تعیین IP for DNS Server

DNS Server < >

۴) تعیین Default Router

Default-Router < Gateway >

۵) Lease Duration

Lease < day hour min >

*) در تعداد زیادی مصاحبه آمده است سوال می‌پرسند که چه چیزهایی را تعریف می‌کنیم -

۶) نقش سرور DHCP را Router هم می‌تواند داشته باشد

وارد اینترفیس می‌شویم

IP address DHCP

* ۱ برای Exclude کردن

IP DHCP exclude-address

*) مشاهده‌ی Address Pool

Sh IP dhcp Pool

DHCP Relay Agent (Microsoft) :

IP ~~[illegible]~~ Helper (Cisco) :

بر روی Router Agent دستور روی اینترفیس

IP helper-Address (DHCP Server Address)

DHCP Troubleshooting :

۱) در صورتیکه Client از DHCP هیچ‌گونه IP نمی‌گیرد

a) اجرای دستور Sh IP int b روی کلاینت

اولا اینترفیس up باشد

ثانیا روی DHCP تنظیم شده باشد

b) اجرای دستور sh ip int b روی سرور

اولا مشخص می‌شود اینترفیس DHCP فعال می‌باشد یا خیر

ثانیا آن اینترفیس IP آن Static باشد

c) اجرای دستور Debug DHCP Detail روی کلاینت

خواندن خط Discover Attempt # Entry

← باید بالاتر از صفر باشد

~~d~~ e) اجرای دستور sh IP DHCP statistics

قسمت اول اطلاعات آماری هیچ ستونی نباید مقدارش صفر باشد

اگر صفر بود با اجرای دستور Show IP Socket باید Port 67 حالت Open باشد.

اگر این Port فعال نبود در Conf Mode دستور Service DHCP را اجرا می‌کنیم

و Port 67 با این دستور Open می‌شود.

تنظیمات ← Time Service :

- هماهنگ کردن زمان سرور سیستم‌های کلاینت با استفاده از پروتکل NTP.

سوال ← Configure

پروتکل مورد استفاده

---

d) دستور نمایش Show ip DHCP Pool تنظیمات انجام شده در Pool را نمایش می‌دهد.