جزوه خلاصه

CCNA 200-301

First Edition

.

.

.

نویسنده : شاهین واثقی

تایپ و ویراست : گروه علمی IT TRIBES

(علی کارگر اسماعیل خانی)

(علیرضا کهن ترابی)

این جزوه خلاصه ای از تنظیمات و کلیات درسنامه کتاب CCNA 200-301 است که تمامی فصل ها را شامل نمی شود و در حال تکمیل شدن است .

ممنون میشم با نظراتتون به اصلاح این جزوه کمک کنید . shahin@shahinvaseghi.ir

Chapter-1
Introduction to TCP/IP Networking

TCP/IP

مدل و معماری شبکه به طور کلی به مجموعه ای از اسناد اشاره دارد که هر سند یک کارکرد در شبکه انجام میدهد و مجموعه ای از اسناد شبکه را تشکیل میدهند.

بعضی از این اسناد پروتکل را تعریف میکنند. که مجموعه ایی از قوانین منطقی است که باعث ارتباط اجزای شبکه میشوند و بعضی از این اسناد الزامات فیزیکی مانند شدت جریان بر روی یک کابل هنگام انتقال دیتا را مشخص میکند.

در ابتدا پروتکل های شبکه استاندارد نبودند و هر شرکت پروتکل های خود را داشت. ابتدا کمپانی IBM در سال 1974 معماری یا مدل شبکه خود را به نام SNA معرفی میکند.

در اواخر دهه 1970 سازمان iso تعریف یک مدل از استاندارد برای شبکه را شروع و آن را OSI نام گذاری کرد.

مدل بعدی مدل TCP/IP که تحت قراردادی برای DOD تعریف شده است و در دهه 1990 مورد استفاده قرار گرفت.

لایه 1. اجزای فیزیکی را کنترل میکند. مانند ولتاژ یک کابل هنگام انتقال داده.

لایه 2. لایه دیتا لینک انتقال دیتا از طریق یک لینک مشخص را کنترل میکند.

لایه 3. لایه نتورک انتقال داده ها از یک مبدا مشخص تا مقصد را در کل مسیر کنترل میکند.

دو لایه بالایی بر روی برنامه هایی که احتیاج به ارسال و دریافت دیتا دارند تمرکز دارد.

مدل TCP/IP مجموعه ای از قوانین است. هر پروتکل با استفاده از سند RFC تعریف میشود. همچنین این مدل از پروتکل های گروه های دیگر مانند IEEE آن را استفاده میکند.

مثلا اترنت در TCP/IP از همان پروتکل IEEE802 استفاده میکند.

امروزه تولید کنندگان تجهیزات شبکه از مدل TCP/IP استفاده میکنند.

*یک نسخه چهار لایه از مدل TCP/IP در RFC 1122 وجود دارد.

یکی از محبوب ترین پروتکل های لایه پنج HTTP است که به این صورت کار میکند که کاربر یک درخواست GET مثلا GEThome.htm به سرور ارسال می کند این درخواست GET از قالب یک http header که در لایه پنج تشکیل میشود به سمت سرور ارسال می شود سپس سرور یک header http با payload با مقدار ok با کد 200 به سمت کاربر ارسال میکند و سپس آن محتوا در خواستی کاربر مثلا home.htm را در tcp header ها ارسال میکند.

یکی از مهمترین اعمال پروتکل TCP در لایه 4 کنترل جریان ارسال داده ها و اطمینان از رسیدن بسته ها به مقصد است.

TCP برای این کار از مفهوم seq برای کنترل و شماره گذاری بسته های ارسال شده از سمت سرور استفاده میکند و از مفهوم ACK برای تایید دریافت یا درخواست ارسال مجدد از سمت کاربر استفاده میکند.

مثلا یک سرور به سمت کاربر یک بسته با seq=1 با payload برابر HTTP header=ok و data بخشی از درخواست کاربر را ارسال می کند سپس در دو بسته دیگر با seq 2 و seq 3 باقی محتوا را به سمت کاربر ارسال میکند.

فرض کنید که seq 2 به کاربر نرسد در این حالت کاربر یک بسته TCP با seq 2 به سرور ارسال می کند و درخواست ارسال دوباره بسته دوم را میکند.

لایه 3 یا نتورک یک پروتکل بسیار مهم به نام IP دارد که ارتباطات راه دور را از طریق این پروتکل به دست می آید.

آدرس Ip چیزی مانند کد پستی در فرایند پست است به دو بخش تقسیم میشود: بخش اول آدرس کلی منطقه را به ما نشان می دهد و بخش دوم آدرس دقیق واحد را مشخص میکند.

مسیریابی Ip در لایه 3 به صورت ارسال هر روتر به روی بعدی تا روتر مقصد به شبکه مورد نظر است .

فرایند Encapsulation در TCP/IP به اضافه کردن HEADER در هر لایه می گویند.

اسم پیام در هر لایه TCP/IP بنابر جدول PDU مشخص میشود:

L5-6-7=data L4=segment L3=Packet L2=frame L1=Bit

Chapter-2
Fundamentals of Ethernet LANs

Ethernet Cable

شبکه SOHO یک شبکه LAN ساده را که از یک روتر، یک سوئیچ LAN و تعدادی محدودی کاربر تشکیل شده است را مشخص میکند.

عموم شبکه های امروز دارای یک دستگاه مرکزی هستند که هم روتر است و هم دارای یک سوییچ 6 یا 8 پورت است و حتی عموما پروتکل IEEEE802:11 یا WLAN را پشتیبانی میکنند.

در این مودم ها WLAN به شکل یک سوئیچ اترنت عمل میکند.

در شبکه SOHO میتوانید 3 دستگاه شبکه متفاوت در نقش های مختلف داشته باشید که هر کدام مجزا یا در ترکیب با هم به درستی عمل کنند.

برای مثال شبکه SOHO می تواند دارای یک ROUTER برای ارتباط با اینترنت، یک سوئیچ اترنت و access point بی سیم برای اتصال بی سیم به یک شبکه باشد یا دستگاهی ترکیبی از اینها داشته باشد مانند مودم های امروزی.

شبکه های Enterprise شبکه هایی هستند که کاربران بیشتری نسبت به شبکه های soho دارند.

در شبکه های enterprise کاربرها به سوییچ هایی محلی خود متصل می شوند وسوییچ ها به سوئیچ مرکزی متصل می شوند

IEEE	formal	type	length	speed
10BASE-T	802.3	COPPER	100M	10M/ETH
100BASE-T	802.3U	COPPER	100M	100M/FETH
1000BASE-LX	802.3Z	FIBER	5KM	1000M/GETH
1000BASE-T	802.3AB	COPPER	100M	1000M/GETH
10GBASE-T	802.3AH	COPPER	100M	10G/10GETH

کابل های 10base-t و100base-t برای ارسال از 2 زوج یا 4 رشته استفاده می کنند که با برقراری یک مدار الکتریکی در هر 2 رشته یا یک زوج استفاده میکند.

کابل های 10base و 100base از2 زوج و 2 مدار برای ارسال استفاده می کنند. کابل های 1000base از 6 زوج و 4 مدار استفاده میکنند.

Fiber Optic

فیبر نوری single mode داری core نازک تر است و از فرستنده به شکل لیزر استفاده می کند و در آن واحد یک پالس نوری ارسال میکند. sfp های single mode به علت لیزر بودن گران تر است اما فیبر single mode مساحت و پهنای باند بیشتری دارد.

- فیبر نوری multi mode دارای core ضخیم تری است پس در آن واحد چندین پالس نوری با استفاده از شکست نور ارسال میکند این فیبر دارای طول کمتر و پهنای باند کمتر نسبت به single mode است.

اما پورت فرستنده آن LED است و قیمت SFP آن کمتر است

STANDARD	TYPE	DISTANCE
10gbase-s	MM	400M
10gbase-lx4	MM	300M
10gbase-lR	SM	30KM

ETHERNET FRAME

Mac address یا آدرس فیزیکی از دو بخش 24 بیتی تشکیل شده است. 24 بیت اول که نام آن organizationally unique identity می باشد باید از osi خریده شود و 24 بیت دوم آن که نام آن vendor assigned است توسط vendor ساخته و روی دستگاه تنظیم می شود.

بخش type در هدر لایه 2 پروتکل لایه 3 بسته را نشان میدهد.

ERROR DETECTION WITH FCS

شبکه های امروزی از سوییچ هایی استفاده میکنند که به صورت Full duplex عمل میکنند: شبکه ها در گذشته با استفاده از hub و به صورت half duplex عمل میکردند دستگاه هایی که از half duplex استفاده میکنند از یک پروتکل به نام CSMA استفاده میکنند.

دستگاه هایی که از CSMA پشتیبانی میکنند برای ارسال فریم ها این مرحله را طی میکند.

1. به شبکه گوش میکند تا ببیند شبکه مشغول است یا نه
2. در صورتی که شبکه مشغول نباشد شروع به ارسال میکند
3. در صورتی که برخورد رخ داده باشد مراحل زیر را انجام میدهد.

در صورت رخ دادن برخورد تمام دستگاه های در حال ارسال مراحل زیر را انجام میدهند.

- تمام NODE ها یک پیام JAMMING ارسال میکند تا تمام دستگاه ها از برخورد آگاه شوند.

- دستگاه ها یک RANDOM TIME برای ارسال انتخاب میکنند تا از برخورد مجدد جلوگیری کنند.
- تلاش بعدی برای ارسال از مرحله شنیدن شروع میشود.

Chapter-3
Fundamentals of WANs and IP Routing

WAN

خطوط WAN از نوع leased-time خطوط اجاره ای هستند که بر روی بسته فیزیکی که بین کاربر و co قرار دارد ارائه میشود.

چون leased time فقط برای لایه یک خدمات می دهد header استاندارد منحصر به فرد را ندارند؛ 2 نوع header به نام های HDLC و PPP برای LEASED TIME استفاده میکنیم .

در هدر HDLC فیلد FLAG همان فیلد SFD و PREAMBLE در هدر اترنت است؛ فیلد address همان destination address است؛ فیلد control در هدر فیلد type و fcs در دو هدر برابر است

خطوط اجاره ایی leased time به صورت ارتباط p2p برقرار میشوند.

در ارسال یک بسته از یک سیستم به سیستم دیگر روترهای در مسیر مراحل زیر را انجام میدهند.

1. fcs چک میشود و اگر مشکل نداشت بسته دریافت میشود.
2. هدر و تریلر data-link از بسته decap میشود و فقط ip packet می ماند
3. روتر مقصد بسته را با جدول مسیریابی چک میکند و مسیر خروجی را انتخاب میکند.
4. بسته با هدر و تریلر data-link جدید encap میشود و ارسال میشود

تمام آدرس هایی که توسط روتر از هم جدا نشده باشند باید هم رنج یا same subnet باشند.

دو آدرس که توسط روتر از هم جدا شده باشند نباید هم رنج یا same subnet باشند.

عموم پروتکل های مسیریابی مراحل زیر را برای یادگیری مسیرها استفاده میکنند.

1.هر روتر به ازای تمام شبکه های متصل به خود یک مسیر در جدول مسیریابی اضافه میکند.

2.پروتکل مسیریابی هر روتر تمام مسیرهای متصل یاد گرفته شده را به همسایگان خود ارسال میکند.

3.پس از یاد گرفتن مسیرهای جدید هر روتر جدول مسیریابی خود را به روز میکنند.

DNS و ARP و ICMP

Chapter-4
Using the Command-Line Interface

IOS

سیستم عامل سوئیچ های سیسکو IOS نام دارد که به معنی Interwork Operating System است.

برای ارتباط cli با سوئیچ سیسکو 3 روش کنسول، تلنت و ssh وجود دارد.

کابل کنسول از pinout به نام rollover استفاده میکند. Rollover سیم ها را به روش زیر میچیند

1به8 - 2به7 - 3به6 و غیره...

سطوح دسترسی در سیسکو به 4 سطح تقسیم میشود:

1. user mode یا user exec یا حالت کاربر : بیشتر دستورات نمایش را اجرا میکند و دستورات اجرایی را ندارد

2. ENABLE MODE: سطح Privilege Mode یا Privilege exec نیز میگویند. این سطح بعضی از دستورات اجرایی را نیز دارد مانند دستور مهم RELOAD . دستوراتی که بین سطح USER و ENABLE مشترک هستند مانند دستورات SHOW دستورات EXEC نام دارند.

3. Configure Terminal: تمام دستورات اجرایی دستگاه در این سطح و زیر دسته های آن است. دستوراتی که در این سطح اجرا میکنید در لحظه بر روی دستگاه اجرا میشوند. در صورتی که میخواهید دستورات سطح enable را در این سطح وارد کنید ابتدای دستور باید عبارت do را اضافه کنید.

4. SUBCONFING: زیرسطح ها زمانی اجرا میشوند که یک کانفیگ با ساب کانفیگ زیاد مانند interface یا vlan یا... را اجرا کنید.

برای امن کردن سطح enable از دستور زیر در سطح conf t استفاده می کنیم :

enable password password

enable secret password

تفاوت password و secret در این است که password به صورت متن ساده یا plain text در حافظه ذخیره میشود اما secret به صورت هش شده ذخیره میشود

دستور show running-config تمام تنظیمات در حال اجرا بر روی دستگاه را نمایش میدهد.

در خط فرمان با وارد کردن ؟ گزینه های بیشتر پیش رو را به شما نمایش میدهد. با نوشتن بخشی از دستور و زدن ؟ تمام دستورات با آن حرف مشترک نمایش داده میشود. با زدن tab در صورتی که حرف کافی از ابتدای یک دستور را نوشته باشید دستور تکمیل میشود.

All Type Of Disk

چهار نوع حافظه در دستگاه های سیسکو وجود دارد.

RAM.1: حافظه اجرایی Running-config در این حافظه است.

FLASH.2: سیستم عامل در این حافظه است.

ROM.3: حاوی BOOTSTRAP یا همان بوت لودر این حافظه است.

NVRAM.3: فایل startup-config در این حافظه ذخیره می شود.

تنظیمات دستگاه های سیسکو در دو فایل running-config و startup-config ذخیره میشود

Running-config : تمام تنظیمات در حال اجرا دستگاه در این فایل ذخیره میشود؛ از طرفی دستوراتی که در سطح conf t وارد میکنید مستقیما این فایل را ویرایش میکند

هنگام که دستگاه را روشن میکنیم تنظیمات اجرایی خود را از فایل startup-config میگیرد.

برای ذخیره تنظیمات running در startup میتوانید از دو دستور در سطح enable استفاده کنید:
copy running-config یا write.

برای پاک کردن startup-config میتوانید از دستورات زیر استفاده کنید.

Erase nvram و erase startup-config وwrite erase

دستور delete vlan.dat تنظیمات vlan را پاک میکند این دستور در سطح enable اجرا میشود.

Chapter-5
Analyzing Ethernet LAN Switching

Layer 2

سوئیچ ها برای ارسال فریم این 3 مرحله را انجام میدهند.

1. تصمیم گیری برای ارسال کردن یا نکردن بسته بر اساس mac مقصد
2. یادگیری مک مبدا بسته
3. ارسال یک کپی از فریم در یک محیط loop free با استفاده از STP

سوییچ برای ارسال بسته های unicast مقصد بسته را در جدول مک خود دارد و از این طریق بسته ها را ارسال میکند.

سویچ ها هنگام دریافت یک فریم آدرس مک مبدا را چک میکنند و در صورتی که در جدول خود نداشته باشند آن را به جدول اضافه میکنند به این فرایند mac learning میگویند.

سوییچ برای ارسال بسته های broadcast و unknown unicast از عمل flood استفاده میکند.

فریم های unknown unicast فریم های دریافتی توسط سوئیچ هستند که مک مقصد آنها در جدول مک سوئیچ وجود ندارد.

عملیات flood به این صورت انجام میشود که کپی هایی از فریم از تمامی پورت ها به جز پورت ورودی ارسال میشود.

STP با مسدود کردن پورت هایی که به مسیر های تکراری میروند جلوی LOOP در بسته های FLOOD شده را میگیرد.

تمام عملیاتی که سوئیچ بر روی یک فریم انجام میدهد به شرح زیر است:

1. سویچ ها بر اساس مک مقصد:

A. اگر مقصد فریم های BROADCAST یا UNKNOWN UNICAST یا MULTICAST باشد فریم FLOOD میشود.

B. اگر مک مقصد یک آدرس UNICAST باشد:

I. اگر پورت خروجی فریم با پورت ورودی برابر نباشد بسته ارسال می شود.

II. در صورتی که پورت خروجی فریم با پورت ورودی یکسان باشد سوئیچ فریم را نادیده میگیرد.

2. سوئیچ برای mac-learning از بررسی src-mac فریم های دریافتی و پورت ورودی فریم سپس بررسی آنها با جدول مک استفاده میکند؛ در صورتی که این پورت در جدول نباشد آن را اضافه میکند
3. سویچ به واسطه STP از لوپ نشدن بسته مطمئن میشود.

سوئیچ های Cisco Catalyst به صورت پیش فرض تنظیماتی دارند که دستگاه آماده به کار سوئیچینگ است.

1. تمام پورت ها فعال هستند. همه پورت ها عضو vlan 1 هستند و پورت ها از auto negotiation برای تعیین سرعت پورت استفاده میکنند.
2. Mac learning و forward و flood فعال است و STP به صورت پیشفرض فعال است.

برای بازگرداندن سوئیچ به حالت کارخانه مراحل زیر را انجام دهید

دستورات مربوط به سطح enable است.

1.با دستور write erase تنظیمات startup را پاک کنید.

2.با دستور delete vlan.dat تنظیمات vlan را پاک کنید.

3.با استفاده از دستور reload دستگاه را راه اندازی مجدد کنید تا بدون تنظیمات روشن شود.

Mac Table

با استفاده از دستور show mac address-table تمام جدول مک سوییچ قابل مشاهده است. در صورتی که میخواهید نوع خاصی از آدرس ها را ببینید در ادامه این دستور عبارت dynamic یا static را وارد کنید.

دستور show interface status وضعیت تمامی پورت های سوئیچ را نشان میدهد.

دستور show interface [num type] counters آمار یک پورت مشخص را نشان میدهد.

برای جستجوی هدف دار تر در جدول مک سوئیچ میتوانید در ادامه دستور show mac address-table dynamic از کلید واژه های address [mac-add] و interface [num type] و vlan [vlan-num] استفاده کنید.

دستور show address-table عمر ردیف های جدول مک را به شما نشان میدهد که این مقدار در سوئیچ های کاتالیست به صورت پیشفرض 300 ثانیه است .

دستور show mac address table count آمار جدول مک را به شما نشان میدهد.

برای ویرایش عمر ردیف های جدول مک میتوانید به صورت کلی یا تنها برای یک ویلن از دستور زیر استفاده کنید

Mac address-table aging-time (time = S) vlan [Vlan-num] (انتخابی)

جدول مک سوئیچ ها در یک حافظه به نام cam ذخیره میشود نهایت ظرفیت جدول mac به اندازه cam وابسته است. مثلا در بعضی سوئیچ ها 7299 است.

برای حذف مک های یاد گرفته شده به جای show در دستور دیدن جدول از clear استفاده کنید به همراه تمام کلید واژه های دستور show.

در صورتی که 2 سوئیچ از طریق یک لینک آپ لینک به هم متصل شده باشند تمامی مک آدرس های متصل به سوئیچ 2 مربوط به پورت آپ لینک سوئیچ 1 می شوند و برعکس.

تمام سوئیچ های سیسکو این 5 تنظیم را به صورت پیشفرض دارند.

1. تمام پورت ها فعال و اماده به کار هستند
2. تمامی پورت ها متعلق به vlan 1 هستند
3. بر روی تمامی پورت ها 10/100 و 10/100/1000 فرایند auto negotiation فعال است.
4. mac learning و forwarding و flooding بر روی تمام پورت ها فعال است.
5. STP در حالت پیشفرض است.

Chapter-6
Configuring Basic Switch Management

Console

برای اتصال cli به دستگاه های سیسکو 3 روش console و telnet و ssh وجود دارد.

برای امن کردن console با یک رمز عمومی از دستور line console 0 برای ورود به زیر تنظیم line استفاده می کنیم با دستور password [password] یک رمز تنظیم میکنیم.

برای امن کردن console با یک رمز user خصوصی ابتدا درسطح configure terminal با دستور

username [user] privilege [privilege-num] (password/secret) [password]

نام کاربری ایجاد کرده سپس با دستور line console 0 به زیر دستور line رفته و با دستور

login local برای console از user های محلی دستگاه استفاده کنید.

برای امن کردن سطح enable از دستور زیر استفاده می کنیم :

enable (password/secret) [password]

Telnet

برای راه اندازی telnet کافیست به پورت vlan 1 سوئیچ (یا هر interface vlan دیگری) آی پی بدهید و با دستور

line vty [num num]

وارد زیر دستور ترمینال از راه دور شوید و حالا با دستور

password [password]

یک رمز عمومی انتخاب کنید و با دستور login این رمز را به رابط مرتبط کنید.

با یوزر های خصوصی و دستور login local در محیط line vty می توانید با user و رمز خصوصی از telnet استفاده کنید.

SSH

برای راه اندازی ssh نمیتوانید از رمزهای عمومی استفاده کنید و باید حتما user و رمز خصوصی ایجاد کنید و سپس مانند telnet به یک پورت آدرس بدهید.

Ssh با کلیدهای خصوصی و عمومی کار میکند پس باید در دستگاه کلید را ایجاد کنیم. برای این کار از دستور crypto key generate rsa و سپس تعیین طول کلید استفاده میکنیم. توجه داشته باشید که این

دستور تنها زمانی کار میکند که مقادیر زیر را در سطح configuration terminal تنظیم کرده باشید :

hostname [hostname]

ip domain-name [name.name]

طول کلید به صورت پیشفرض 512 بیت است اما برای ssh.v2 کلیدی با حداقل طول 750 بیت احتیاج است.

به طور پیشفرض هر دو ورژن ssh بر روی دستگاه فعال است با دستور ip ssh version 2 ورژن 1 را غیر فعال کنید.

با استفاده از دستور زیر در زیر دستور line vty میتوانید ورودی های ریموت دستگاه را کنترل کنید.

transport input telnet = (تنها telnet)

transport input all = (هردو ssh & telnet)

transport input ssh = (تنها ssh)

transport input none = (هیچکدام)

General Setting

برای اینکه بتوانید با چند آدرس vlan های مختلف به دستگاه وصل شوید لازم است برای سوئیچ با دستور

ip default gateway [gateway-ip-address]

یک gateway تعیین کنید.

با دستور ip add dhcp زیر میتوانید بر روی یک اینترفیس dhcp client راه اندازی کنید :

interface [type num]

ip address dhcp

با دستور show dhcp lease در سطح enable میتوانید آدرس دریافت شده بر روی اینترفیس را مشاهده کنید

برای فعال یا غیر فعال کردن نمایش لاگ ها در کنسول دستور logging console و no logging console را استفاده کنید .

برای اینکه لاگ های ما بین دستورات یا خروجی های شما نمایش داده نشوند از دستور logging synchronous console استفاده کنید.

زمان timeout پیشفرض برای ترمینال ۵ دقیقه است برای تغییر این مقدار از دستور زیر استفاده کنید :

exec timeout [minute seconds]

هنگامی که عبارت اشتباهی مانند یک دستور اشتباه وارد کنید دستگاه تلاش به ارتباط telnet با DNS وارد شده میکند برای غیر فعال کردن دستور زیر را وارد کنید :

no ip domain-lookup

Chapter-7
Configuring and Verifying Switch Interfaces

Interface Setting

تمام پورت های سوئیچ سیسکو به صورت پیش فرض دارای سرعت و DUPLEX اتومات هستند برای تغییر این تنظیمات از زیر دستور اینترفیس زیر استفاده کنید :

duplex (auto/half/full)

speed (auto/10/100/1000)

با دستور description میتوانید برای یک پورت توضیحات ثبت کنید. دستور

show interface status جزئیات پورت ها را نشان میدهد.

برای انتخاب گروهی از پورت ها از دستور زیر استفاده می کنیم :

interface range type num-num (from-to)

برای خاموش و روشن کردن پورت ها از زیر دستور اینترفیس no shutdown و shutdown استفاده میکنیم .

با استفاده از زیر دستورات اینترفیس زیر تمامی پورت های سوئیچ با استفاده از auto negotiation برای تعیین سرعت و duplex استفاده میکنند. این عمل با پروتکل IEEE802.3U انجام میشود.

no duplex

no speed

اگر یک طرف auto negotiation فعال باشد و یک طرف نباشد توافق شکست میخورد و بنا بر IEEE سرعت و duplex پورت تعیین می شود :

1. حداقل سرعت پورت تعیین میشود

2.برای لینک های 10 و 100 مگ از half duplex و برای باقی لینک ها از full duplex استفاده میکند .

سوئیچ های سیسکو در صورت شکستن auto negotiation روشی متفاوت دارند

1.به لینک گوش میدهد و سرعت پورت روبرو را تشخیص می دهد.

2.duplex را بنابر IEEE انتخاب می کند

در صورتی که در روبه روی یک پورت با auto negotiation فعال یک هاب قرار داشته باشد قوانین IEEE با سرعت عموما 10 مگ انتخاب میشود.

وضعیت پورت یکی از 5 حالت زیر است که در دو شکل یک کلمه ای برای interface یا دو کلمه ای برای Line/status تعیین میشود.

interface	line/status	
disable	admin down/down	(پورت خاموش است)
not connect	down/down	(کابل یا دستگاه روبه رو قطع است)
not connect	up/down	(در سوئیچ اتفاق نمی افتد)
err-disable	down/down(err)	(پورت را غیرفعال کرده port security)
connected	up/up	(پورت فعال است)

Interface Counter

برای دیدن جزئیات یک پورت از دستور show interface [type num] استفاده کنید.

دستور بالا آمار لینک مانند فریم های عبوری و فریم های حذف شده را نشان میدهد. معنی کلید واژه های خروجی دستور بالا به شرح زیر است:

Runts فریم های حذف شده که الزامات حداقل اندازه فریم را رعایت نکرده اند.

Giants فریم هایی که حذف شده اند به دلیل بزرگتر بودن از حداکثر اندازه

Input error جمع آوری شمارنده های مختلف

CRC فریم هایی که مشکل FCS دارند

Frame فریم هایی که فرمت غیر مجاز دارند

Collisions شمارنده تمام اتفاقاتی که هنگام ارسال فریم اتفاق می افتد.

Late collision شمارنده تصادفات تاخیری

Chapter-8
Implementing Ethernet Virtual LANs

Vlan

به صورت پیشفرض تمامی پورت های یک سوئیچ داخل یک Broadcast Domain عضو هستند و تمامی پورت ها با هم ارتباط لایه ۲ ای دارند در صورتی که بخواهیم پورت های سوئیچ در Broadcast Domain های مختلف فعالیت کنند باید جلوی ارسال و دریافت Arp بین این دو پورت گرفته شود تا ارتباط لایه ۲ ای شکل نگیرد و چون بسته های به شکل Broadcast لایه ۲ هستند و جز پورت ورودی از تمامی پورت های دیگر جدول مک ارسال می شوند برای جداسازی Broadcast Domain ها باید پورت ها را در جداول مک مجزا قرار دهید.

این کار با استفاده از Vlan انجام میشود. سوئیچ ها به ازای هر Vlan یک جدول مک تشکیل میدهند و اعضا جداول مختلف در Broadcast Domain های مختلف قرار می گیرند.

Vlan trunking برای انتقال چندین vlan روی یک پورت استفاده میشود. این فرایند با اضافه کردن تگ dot 1q به هر فریم هر vlan استفاده میشود.

بخش dot 1q در هدر Ethernet لایه 2 بین src-mac و type قرار دارد .

برای ایجاد یک vlan در سطح conf t از دستور زیر استفاده می کنیم :

vlan [vlan-id]

فناوری DTP با ایجاد ترانک پویا برای تعیین خودکار وضعیت پورت در حالت trunk استفاده میشود.

Dynamic auto منتظر طرف مقابل می ماند تا ترانک شود

Dynamic desirable به سمت مقابل ترانک شدن را القا میکند

برای تخصیص یک پورت به یک vlan مشخص از دستور زیر استفاده می کنیم :

Switchport access vlan [vlan-id]

برای تعیین وضعیت یک پورت از زیر دستور اینترفیس زیر استفاده میکنیم :

Switch port mode (access/trunk/dynamic)

برای تعیین نام برای یک ویلن از دستور زیر استفاده میکنیم :

vlan [vlan-id]

name [name]

بعضی از سوئیچ های جدید سیسکو علاوه بر dot1q از isl نیز پشتیبانی میکنند برای تعیین نوع تگ پورت ترانک از زیر دستور اینترفیس زیر استفاده کنید :

Switchport trunk encapsulation (dot 1q/isl/negotiation)

خروجی دستور show interface type switch جزئیات دقیقی از وضعیت پورت های سوئیچ به شما میدهد

1. administrative mode حالتی است که تنظیمات به پورت القا میکند

2. operational mode حالتی که که واقعا پورت در آن کار میکند.

مفهوم native vlan در ترانک به اضافه نکردن تگ Vlan به بسته های vlan مشخص شده اشاره دارد.

در منطق ترانک تمام vlan ها بجز native vlan به تگ احتیاج دارند پس بسته های مربوط native vlan تگ نمیخورند.

اگر native vlan در دو سر ترانک یکسان نباشند بسته های یک vlan به vlan دیگری تحویل داده میشود و اصطلاحا native vlan mismatch اتفاق می افتد و پورت up نمیشود.

با دستور show interface trunk تمام پورت های ترانک دستگاه را مشاهده میکند

با زیر دستور اینترفیس switchport nonegotiate پروتکل DTP غیر فعال میشود.

برای تنظیم voice vlan بر روی یک پورت علاوه بر تنظیم یک ویلن با

switchport access vlan [vlan-id]

با دستور

switch port voice vlan [vlan-id]

یک ویلن دیگری روی پورت تنظیم میکنیم.

در صورتی که در دو سمت یک لینک dynamic auto ست شود لینک ترانک نمی شود و در وضعیت access می ماند.

زیر دستور زیر ویلن های مجاز برای یک ترانک را مشخص میکند :

switchport trunk allowed vlan [vlan-id, vlan-id ,vlan-id,...]

Chapter-9

Spanning Tree Protocol Concepts

General

STP وظیفه جلوگیری از LOOP لایه 2 را دارد.

STP با قرار دادن پورت ها در 2 وضعیت FORWARDING و blocking شبکه را کنترل میکند

1.forwarding : به صورت پیش فرض ترافیک کاربر را در vlan خودش ارسال میکند.

2.blocking : هیچ ترافیک را ارسال نمیکند.

عدم وجود stp به سه مشکل زیر منجر میشود :

1.loop لایه 2 ای

2. ارسال چندین نسخه از یک frame به یک کاربر

3. ناپایداری جدول mac

Stp با ترسیم درخت تمام ارتباطات اترنت یک نقشه جامع از شبکه رسم می کند سپس از هر سوئیچ تا ریشه یک مسیر ایجاد میکند.

Stp در سه حالت پورت ها را در حالت forwarding قرار میدهد :

1.تمام پورت های سوئیچ root

2.هر پورت سوئیچ غیر root که به سمت root کمترین فاصله را دارد

3.تمامی پورت هایی که BPDU به سمت سوئیچ های پایین دستی ارسال کنند Designated port تشخیص داده شده و در حالت forward قرار میگیرند (مثلا تمامی پورت های سوئیچ root در حالت dp قرار دارند .

فرایند stp با انتخاب یک سوئیچ root آغاز میشود .

BPDU

هر سوئیچ دارای یک BID هشت بایتی است که از دو فیلد priority+lowest-mac تشکیل میشود.

هر سوئیچ بسته های تنظیمی به نام BPDU تشکیل میدهد که پیام های STP را با آن جابجا می کند.

متداول ترین BPDU به نام HELLO BPDU جزئیات زیادی از جمله BID سویچ را دارد.

HELLO BPDU بخش های زیر را لیست میکند :

1.ROOT BID: شناسه Root bridge سوئیچ فرستنده این BPDU

2.senders BID: فرستنده این BPDU

3. senders root cost: هزینه بین سوئیچ فرستنده و root bridge

4.timers values on the root: شامل تایمر hello و Forward delay و max age

Root Bridge Election

در انتخابات سوئیچ ROOT ابتدا هر سوئیچ یک HELLO BPDU با BID خود به عنوان ROOT BID و ROOT COST ایجاد میکند یعنی خود را ROOT در نظر میگیرد تا وقتی سوئیچ یک HELLO BPDU با BID کوچکتر دریافت نکند به ارسال HELLO به عنوان ROOT ادامه میدهد در صورت دریافت HELLO بهتر ارسال HELLO را متوقف میکند و شروع به عبور دادن HELLO بهتر میکند

Root Port Election

در مرحله بعد STP یعنی انتخاب Root Port هر سوئیچ بین BPDU های دریافتی از پورت های مختلف COST پورت دریافتی که HELLO را از همسایه دریافت کرده است را به cost دریافتی اضافه میکند و پایین ترین COST را به عنوان RP انتخاب میکند.

Designated Port Election

در مرحله بعد از STP یعنی انتخاب DP در هر LAN چه یک LAN مستقیم بین دو سوئیچ، چه یک سوئیچ متصل به چند سوئیچ، از طریق HUB پورتی که BPDU را به سوئیچ های دیگر ارسال کند PD می شود .

پورت های زیر Designated Port می شوند :

1. تمامی پورت های سوئیچ root
2. پورت های روبروی RP سوئیچ های دیگر (یعنی پورت هایی که به سوئیچ های دیگر BDPU ارسال می کنند)
3. تمامی پورت هایی که به سمت کاربران می روند. چه پورت های Access ای که مستقیم به سمت کاربران رفته اند چه پورت هایی که ار طریق یک hub به کاربر متصل هستند (در اینجا کاربر تمامی دستگاه های نهایی شبکه مانند : کامپیوتر های ثابت یا قابل حمل ، تجهیزات هوشمند و ...) به عنوان DP انتخاب می شوند .

پس از آنکه تمامی سوئیچ ها hello خود را ارسال و تمام hello های دیگر را دریافت گردید سوئیچ با کوچکترین BID تبدیل به ROOT BRIDGE میشود.

در صورت تساوی اولویت در انتخابات ROOT دستگاهی با MAC کوچکتر بدون توجه به اولویت برنده است.

Root Port Cost

مرحله دوم STP تعیین پورت به سمت سوئیچ روت با کمترین هزینه است.

هزینه هر لینک در STP یک مقدار مشخص است.

10MBPS	100	2 000 000
100MBPS	19	200 000
1000MBPS	4	20 000
10GBPS	2	200
100GBPS	N/A	20
1TPS	N/A	20

در صورتی که سوئیچ 2 یا چند لینک به سمت سوئیچ ROOT با COST برابر داشته باشد برای انتخاب از 3 مورد زیر استفاده میکند :

1.LOWEST NEIGHBOR BID

2.LOWEST NEIGHBOR PORT PRIORITY

3. LOWEST NEIGHBOR INTERNAL PORT-NUM

پورت های سوئیچ که به سمت LAN میروند و ممکن است در یک ارتباط لایه 1 ای با چند سوئیچ دیگر همسایه شوند مانند وقتی که یک پورت سوئیچ را به یک هاب متصل کرده و پورت های دیگر به سوئیچ های دیگر؛ در این شرایط محیطی ایجاد شده است تا انگار این دستگاه ها در چند سمت یک سیم واحد قرار گرفته اند؛ به این پورت ها DESIGNATED گفته میشود.

یک سوئیچ ROOT در STP هر 2 ثانیه یک فریم HELLO ارسال میکند . سوئیچ های غیر root این HELLO ها را بعد از اضافه کردن مقادیر خودش به فریم از پورت های DP ارسال میکند. (یعنی تغییر sender bid و root cost)

STP Protocols

stp دارای انواع زیر است :

stp 802.1D IEEE standard

Rstp 802.1w IEEE standard

Mstp 802.1s (q) IEEE standard

Pvst+ property Cisco based on stp802.1D

RPvst+ property Cisco based on rstp802.1w

STP 802.1D

Timers

تایمر های STP :

1. HELLO دو ثانیه: به مدت زمان بین ارسال HELLO توسط ROOT
2. MAX AGE مدت 10 HELLO: مدت زمانی که اگر سویچ فریم HELLO دریافت نکند توپولوژی را تغییر میدهد.
3. FORWARD DELAY مدت 15 ثانیه : برای اینکه سوئیچ پورت را از حالت BLOCKING به FORWARDING ببرد باید به مدت زمان FORWARD DELAY در حالت LISTENING سپس به همین صورت در LEARNING بماند سپس به FORWARDING برود.

در صورت 0 شدن زمان سنج max age سوئیچ برای تغییر توپولوژی تمام تصمیمات را دوباره میگیرد.

Port State

در stp 802.1D سوئیچ برای تغییر وضعیت یک پورت از BLOCKING به FORWARDING ابتدا پورت را به ترتیب به این وضعیت میبرد :

1.LISTENING: در این مرحله مانند BLOCKING پورت فریم ها را عبور نمیدهد و تمام ردیف های مربوط به این پورت در MAC TABLE را پاک میکند.

2.LEARNING: پورت ها همچنان فریم عبور نمی دهند اما شروع به MAC LEARNING از فریم های دریافتی میکند.

سوئیچ برای تغییر از BLOCKING به FORWARDING ابتدا پورت را برای 15 ثانیه به حالت LISTENING و سپس 15 ثانیه به وضعیت learning میبرد این مقادیر forward delay پیشفرض stp است. توجه داشته باشید که سوئیچ ممکن است قبل از آغاز فرایند تغییر وضعیت 20 ثانیه منتظر بماند یعنی کل فرایند تغییر از blocking به forwarding 50 ثانیه طول بکشد.

RSTP 802.1w

مسائل مربوط به RSTP802.1w :

مراحل زیر در هر دو پروتکل stp و rstp یکسان است .

سوئیچ های غیر root قبل از ارسال HELLO از DP ها بخش SENDERS BID را تغییر میدهند و COST خودشان تا ROOT را به فریم اضافه میکنند.

سوئیچ تا زمانی که به طور مرتب فریم HELLO را از طریق RP خود دریافت کند معتقد است که شبکه به درستی کار میکند.

در صورتی که به مدت 10 بار HELLO فریم HELLO از RP دریافت نشود سوئیچ به این نتیجه میرسد که شبکه دچار اشکال شده است سوئیچ در این مرحله شروع به تغییر توپولوژی میکند.

فرایند مخصوص به RSTP :

1. فرایند انتخاب ROOT با stp802.1D یکسان است.
2. فرایند انتخاب ROOT PORT با stp802.1D یکسان است.
3. فرایند انتخاب DESIGNATED PORT با stp802.1D یکسان است.
4. هر دو پورت را در دو وضعیت BLOCKING و forwarding قرار میدهند فقط RSTP به جای BLOCKING از DISCARDING استفاده میکند.

Port State , Timers

تغییرات RSTP نسبت به STP به شرح زیر است :

RSTP.1 یک قابلیت جدید برای جایگزین کردن سریع RP دارد بدون اینکه منتظر انتخاب مجدد RP و عبور مراحل از Blocking به FORWARDING بماند.

RSTP.2 زمان انتظار برای عبور از مراحل پورت را کمتر کرده است.

RSTP .3 از مرحله Listening استفاده نمی کند .

RSTP برای کمتر کردن زمان CONVERGENCE دو تغییر ایجاد کرده است.

1.زمان MAX AGE را به 3 HELLO کاهش داده است.

2.برای اطلاع از خرابی بعد از گذر MAX AGE اگر HELLO دریافت نکند از NEIGHBOR خرابی شبکه را میپرسد.

Port Role

RSTP علاوه بر 3 نقش پورت STP دو نقش دیگر نیز دارد :

1.Alternate port: پورت جایگزین root port

2.backup port: پورت جایگزین designated port

در rstp بر خلاف stp که سوئیچ های غیر root تنها hello سوئیچ root را update و ارسال می کردند سوئیچ های غیر روت hello خود را ارسال میکنند.

Alternate port در rstp یک جایگزین سریع برای root port است هنگامی که root port قطع شود یا hello دریافت نشود سوئیچ سریع root port را به disable port تغییر میدهد و وضعیت آن را به discarding سپس alternate port بدون انتظار به نقش root port در می آید و سریع به وضعیت forwarding می رود .

وضعیت پورت ها در rstp چند تفاوت با stp دارد:

1.وضعیت blocking و disable هر دو به discarding تغییر کرده اند.

2.وضعیت listening وجود ندارد .

Stp برای خالی کردن و یادگرفتن جدول mac نیاز به زمان forward delay داشت اما rstp با ارسال پیام به neighbor ها و اطلاع Topology change فرایند convergence را تسریع کرده است.

Backup port در شبکه های امروزی بسیار غیرممکن است زیرا تنها در صورتی ایجاد می شود که ما hello خود را از پورت دیگری دریافت کنیم و این یعنی 2 پورت از یک سوئیچ به 2 پورت از یک hub متصل باشد.

Port Type

پورت ها در rstp سه نوع هستند:

1.point-to-point: پورت های مستقیم بین دو سوئیچ

2.point-to-point edge port: پورت های بین سوئیچ و یک endpoint

3.shared port: پورت هایی که در آن یک collision domain گسترش پیدا میکند مانند پورت های متصل به hub .

Additional Feature

برای کاهش convergence time میتوانید از ether channel استفاده کنید. با این کار شما میتوانید تا 8 لینک را با هم ترکیب کنید و به عنوان یک interface ببینید این عمل باعث میشود تا در صورت بروز خطا بر روی یک لینک root port تغییر نکند.

Port fast به پورت اجازه میدهد که سریعا بدون عبور از listening و learning مستقیم از blocking به forwarding برود .

Bpdu guard باعث میشود که پورت هیچ فریم bpdu دریافت نکند .

Chapter-10
RSTP and EtherChannel Configuration

PVST+,RPVST+

STP در سیسکو دو MODE انحصاری دیگر نیز دارد که IEEE آنها را نپذیرفته است

PVST.1 : همان STP پروتکل 802.1D اما با یک درخت به ازای هر VLAN

RPVDTT.2 : همان RSTP پروتکل 802.1W اما با یک درخت به ازا هر VLAN

البته IEEE نیز یک پروتکل STP با چند درخت دارد به نام MSTP

برای ایجاد چند درخت STP بایستی PRIORITY در هر BIT نسبت به VLAN به مقدار یکتا تبدیل شود.

در STP با یک درخت برای انتخاب ROOT اولین گزینه برای بررسی PRIORITY است که یک مقدار 16 بیتی است که 6 بیت اول آن میتواند 0 یا 1 باشد اما 12 بیت پایانی همیشه 0 است مانند

1111 0000 0000 0000

VID یک مقدار 12 بیتی که برای ایجاد درخت به ازاء هر VLAN باید PRIORITY و VID ترکیب شوند و VID جای 12 بیت خالی پایانی PRIORITY را بگیرد برای مثال VLAN شماره 18 که مقدار باینری زیر را دارد

0000 0001 0010

هنگامی که با PRIORITY 32768 یعنی

1000 0000 0000 0000

1000 0000 0001 0010

ترکیب شود می شود 32786

PVST Config

با دستورات زیر میتوانید هر سوئیچ را به ROOT اصلی و جایگزین در هر VLAN تبدیل کنید.

SPANNING-TREE VLAN [VID] ROOT PRIMARY

SPANNING-TREE VLAN [VID] ROOT SECONDARY

تفاوت های RSTP و RPVST :

RSTP.1 دارای یک درخت برای کل شبکه است اما RPVST+ دارای یک درخت به ازاء هر VLAN است.

RSTP.2 یک مسیج BPDU برای کل شبکه ارسال میکند اما RPVST+ یک مسیج به ازاء هر VLAN ارسال میکند

RSTP.3 از آدرس C200:0000:BROADCAST:0180 که توسط IEEE تعیین شده استفاده میکند اما سیسکو از آدرس منتخب خودش 0100:0CCC:CCCD

RSTP.4 هنگام ارسال یک پیام از یک پورت ترانک آنرا از NATIVE VLAN ارسال میکند اما RPVST+ هر پیام را با تگ dot1q مربوط به vlan خودش ارسال میکند.

rpvst.5+ یک بخش TLV به hello اضافه کرده: Vlan-ID

RSTP .6 دوازده بیت های پایانی را در PRIORITY مقدار 0 میگذارد یعنی هیچ VLAN اما RPVST+ شماره VID را میگذارد.

با دستور زیر میتوانید به طور مستقیم برای هر VLAN یک PRIORITY تعیین کنید

spanning-tree vlan [VID] priority [num]

با دستور زیر میتوانید COST مسیر برای یک VLAN و یا برای همه تغییر دهید

spanning-tree vlan [VID] cost num

Ether-Channel

برای تنظیم دستی ether-channel بر روی پورت زیر دستور اینترفیس زیر را وارد کنید.

Port-group [pg-num] mode on

تنظیم خودکار ether-channel قبل از اضافه کردن هر لینک به port-group ابتدا با طرف مقابل مذاکره میکند و الزامات فیزیکی لینک را بررسی میکند. در صورتی که همه چیز درست بود لینک اضافه میشود در غیر این صورت به وضعیت down میرود.

برای ether-channel خودکار دو فناوری IEEE و cisco pagp وجود دارد که تنها تفاوت در آنها این است که lacp از 16 لینک در هر کانال پشتیبانی میکند. اما pagp از 8 لینک.

برای راه اندازی ether-channel خودکار در ادامه زیر دستور channel-gr روبروی mode برای lacp از دستور active و passive و برای pagp از دستور desirable و auto

Mode های active و desirable مذاکره کننده هستند حداقل یک طرف باید در این وضعیت ها باشد.

یک لینک برای اینکه در حالت های خودکار به گروه اضافه شود باید تمام تنظیماتی که شبیه لینک های دیگر باشد برای اضافه شدن تنظیمات زیر چک شود

- Speed
- duplex
- وضعیت operational access یا ترانک؛ همه ی پورت ها باید یا access باشند یا trunk
- اگر ترانک هستند باید لیست allowed vlan یکسانی داشته باشند
- اگر ترانک هستند native ویلن یکسانی داشته باشد
- تنظیمات port در stp یکسان باشد

برای اینکه ether-channel به درستی کار کند باید تمام ترافیک های مربوط بر روی یک لینک ارسال شوند. فرض کنید کاربر در حال دانلود است سوئیچ باید تمام ترافیک های مربوط به این ارتباط را از یکی از لینک ها ارسال کند تا مشکلی پیش نیاید به این کار Load-balancing یا ether-channel load distribute on میگویند.

سوئیچ با دستور زیر می تواند بنابر مدل با یکدیگر از متد های زیر load-balancing انجام دهد.

پورت مبدا یا مقصد. مک مبدا یا مقصد. آی پی مبدا یا مقصد

Port-channel load-balancing [method]

Chapter-11

Perspectives on IPv4 Subnetting

IP Subnet

آدرس های کلاس a b c شبکه هایی با طول مشخص می سازند؛ منظور از طول خط تعداد host های هر شبکه است.

هر شبکه یا رنج یا subnet به تمامی آدرس هایی گفته میشود که net id یکسان با host id متفاوت دارند.

بیشتر مهندسان it نیاز به کار با subnet ها را دارند، نه طراحی آن به خاطر انکه احتمال زیاد قبل از شما طراح شبکه را طراحی کرده است و شما تنها باید آن را به کار بگیرید.

برای طراحی سابنت ها در شبکه 3 مرحله زیر را طی کنید :

1. آنالیز نیازها
2. طراحی سابنت

3. برنامه پیاده سازی

برای آنالیز نیازها باید به سوال های زیر پاسخ داده شود

1.کدام سیستم ها با هم گروه هستند و باید در یک سابنت باشد؟

2.شبکه ها به طور کلی به چند سابنت نیاز دارد؟

3.هر شبکه به چند شناسه کاربر احتیاج دارد؟

4.برای تمام سابنت ها از یک سایز استفاده کنیم یا سایز های مختلف؟

به طور کلی علت نیاز به subnet های مختلف این است که در صورتی که کاربران در یک شبکه باشند یعنی همه ارتباط لایه 2 ایی داشته باشند و هم ادرس هم رنج داشته باشند بدون کنترل و نظارت باهم ارتباط برقرارمیکنند

جدا کردن subnet ها باعث میشوند سیستم های غیر هم رنج برای ارتباط از روتر عبور کنند و این کار باعث میشود بتوانیم روی ارتباط نظارت کنیم.

موضوعات بالا دو قانون کلی را تعریف میکند:

1.تمام سیستم های هم رنج نباید توسط روتر جدا شوند.

2.تمام سیستم های غیر هم رنج باید توسط روتر جدا شوند.

به بیان دیگر هر پورت روتر یک رنج متفاوت دارد یا اصطلاحا هر پورت یک broadcast domain است.

برای شمارش تعداد سابنت های لازم به ازاء هر یک از موارد زیر یک سابنت میخواهید.

1.هر vlan یک سابنت

2.لینک های سریال p2p

3.لینک های wan اترنت

Subnet Mask

Net id هر آدرس با subnet mask مشخص میشود سابنت ادرس 32 بیتی نظیر ip است. سابنت بیت های net id را 1 بیت های host id را 0 میدهد.

در سابنت مسک همیشه 1ها از سمت چپ شروع میشوند و هر جا یک ها تمام شود 0 ها شروع میشوند تا پایان آدرس.

تعداد آدرس های هر سابنت به تعداد bit های host id بستگی دارد اگر هر بیت host id را H در نظر بگیریم شبکه 2 به توان h منهای 2(2 $-$ 2^h)کاربر ظرفیت دارد.

اگر در شبکه چندین سایز سابنت استفاده کنیم vlsm کرده ایم در صورتی که میخواهید در شبکه vlsm استفاده کنید باید subnet را بر اساس بزرگترین شبکه در نظر بگیرید.

در ابتدای اینترنت شرکت ها با خرید یک رنج ip آدرس عمومی در یک کلاس ها به کل سیستم آدرس عمومی مستقیم می دادند اما در اواسط دهه 90 و با به وجود آمدن ip private این کار ساده تر شد.

با تمام شدن آدرس های عمومی سه راهکار معرفی شد.

ipv6.1

nat.2

classless .3 یا CIDR شدن آدرس های پابلیک و خریدن بخشی از یک رنج به جای کل رنج

با استفاده از nat چنین شبکه از یک رنج ip استفاده میکنند.

تا اینجا فهمیدیم برای طراحی آدرس های یک شبکه :

*تعداد شبکه ها لازم است.

*تعداد کاربر ها در شبکه لازم است.

*انتخاب برای استفاده از یک طول سابنت یا vlsm

*cidr در آدرس های پابلیک.

Subnetting

برای انجام عمل سابنتینگ باید چند بیت از HOST ID به NET ID قرض بدهیم که آن بیت ها subnet id میگوییم .

برای تعداد شبکه دلخواه تعداد بیت هایی که باید از host id به net id قرض دهید برابر با فرمول زیر است :

$(x \leq 2^n)$

x تعداد شبکه پس از سابنتینگ است و n بیت هایی که باید از host id به net id بدهیم.

برای تعداد کاربر مشخص در هر شبکه از فرمول زیر استفاده میکنیم :

$(x \leq 2^n - 2)$

x تعداد کاربر در هر شبکه پس از سابنتینگ است و n بیت هایی که باید برای host id باقی بماند و باقی بیت ها را به net id بدهیم.

برای به دست آوردن سابنت ماسک شبکه های جدید سابنت شده به تعداد بیت های قرض داده شده از host id به net id به سابنت ماسک قبلی 1 اضافه میکنیم .

ما می دانیم چیزی که شبکه ها را از هم جدا می کند Net ID است پس ما برای قطعه قطعه کردن باید کمی از Host ID که تعداد کاربران در این شبکه را مشخص میکند را به Net ID بدهیم . در عمل Subnetting ما با خود آدرس شبکه کاری نداریم و در ابتدا تغییراتمان را روی Subnet Mask اعمال می کنیم و از سابنت جدید آدرس شبکه ها را پیدا میکنیم

در لیست زیر نشان داده شده که هر کلاس ای پی چند کاربر را آدرس دهی میکند :

Address Class	Assignable IP Addresses
Class A	16,777,214 (2^{24}–2)
Class B	65,534 (2^{16}–2)
Class C	254 (2^{8}–2)

منفی 2 ای که در پایان همه ی شبکه ها است علت ساده ای دارد اولین ادرس شبکه که تمام بیت های Host ID آن 0 است آدرس شبکه است و آخرین آدرس که تمام بیت های Host ID آن 1 است آدرس Broadcast این شبکه است.

برای تقسیم IP دو حالت وجود دارد :

1. تقسیم به تعداد شبکه مورد نظر (مثلا به ما میگویند یک آدرس را طوری سابنت کنید که در آخر به 4 شبکه تقسیم شود)
2. تقسیم به تعداد Host (در این حالت دیگر برای ما تعداد شبکه مهم نیست بلکه برای مهم است که مثلا هر شبکه 25 سیستم را حداقل آدرس دهی کند)

1. برای این کار ما از فرمول $X=2^h-2$ استفاده می کنیم در اینجا X تعداد شبکه درخواستی از ما است و h تعداد بیت هایی است که باید از Host ID به Net ID اضافه کنیم .

این موضوع را با چند مثال توضیح میدهم :

فرض کنید میخواهیم شبکه 192.168.1.0 با سابنت 255.255.255.0 را به دو شبکه تقسیم کنیم .

خب ما میدانیم که فرم باینری سابنت این شبکه به شکل زیر است:

11111111.11111111.11111111.00000000

بخش هایی که شامل عدد 1 است Net ID است و بخش های 0 Host ID . پس ما میخواهیم از 0 ها بگیریم و به 1 ها اضافه کنیم .

از فرمول استفاده میکنیم :

2 بتوان x = h چون تعداد شبکه درخواستی 2 است پس x می شود 2 و h می شود 1 حالا ما می دانیم برای اینکه شبکه بالا به 2 شبکه تقسیم شود باید 1 بیت از Net ID به Host ID اضافه کنیم آدرس شبکه را به شکل باینری مینویسیم و بیت را جدا میکنیم :

11000000.10101000.00000001.**0**0000000

این بیت به صورت کلی دو حالت بیشتر نمی تواند داشته باشد یا باید 1 باشد یا 0 پس ما هر دو حالت را در نظر میگیریم و آدرس شبکه های جدید را می نویسیم :

1. در حالتی که بیت 0 باشد :

192.168.1.0 = 11000000.10101000.00000001.**0**0000000

2. در حالتی که بیت 1 باشد :

192.168.1.128 = 11000000.10101000.00000001.**1**0000000

خب حالا دو آدرس شبکه (Network Address) داریم پس ابتدا و انتها هر شبکه را مینویسیم :

192.168.1.0 ادرس شبکه

192.168.1.1 – 192.168.1.126 ادرس های قابل ارائه به سیستم ها

192.168.1.127 ادرس Broadcast شبکه (یکی کمتر از Network Address شبکه بعدی)

192.168.1.128 ادرس شبکه

192.168.1.129 – 192.168.1.254 ادرس های قابل ارائه به سیستم ها

192.168.1.255 ادرس Broadcast شبکه

حالا باید Subnet Mask جدید شبکه را بنویسیم :

Subnet قبلی به صورت دسیمال 255.255.255.0 و به صورت باینری 11111111.11111111.11111111.**0**0000000 است. حالا که ما 1 بیت دیگر به Host ID قرض دادیم باید این تغییر را در سابنت جدید اعمال کنیم

11111111.11111111.11111111.**1**0000000 و به صورت دسیمال 255.255.255.128

مثال 2 :

فرض کنید میخواهیم شبکه

192.168.10.0/24

را به 4 شبکه تقسیم کنیم :

فرمول را می نویسیم 2 بتوان h برابر 4 . مقدار h می شود 2 پس 2 بیت را باید به Host ID بدهیم . ابتدا آدرس شبکه را صورت باینری می نویسیم :

11000000.10101000.00001010.00000000

حالا 2 بیت را جدا میکنیم . چون ما تنها مقدار 0 و 1 را داریم و 2 جایگاه برای قرار گیری این اعداد میدانیم تعداد جایگشت این اعداد 4 می شود . پس با این 2 بیت 4 حالت مختلف را می نویسیم :

1. 192.168.10.0 = 11000000.10101000.00001010.00000000
2. 192.168.10.64 = 11000000.10101000.00001010.01000000
3. 192.168.10.128 = 11000000.10101000.00001010.10000000
4. 192.168.10.192 = 11000000.10101000.00001010.11000000

خب حالا که ما آدرس شبکه (Network Address) هر 4 شبکه را داریم میتوانیم از حد فاصل این آدرس ها هر شبکه را محاسبه کنیم

1- 192.168.10.0

192.168.10.0 ادرس شبکه

192.168.10.1 – 192.168.10.62 ادرس های قابل ارائه به سیستم ها

192.168.10.63 ادرس Broadcast شبکه

2- 192.168.10.64

192.168.10.64 ادرس شبکه

192.168.10.65 – 192.168.10.126 ادرس های قابل ارائه به سیستم ها

192.168.10.127 ادرس Broadcast شبکه

3- 192.168.10.128

192.168.10.128 ادرس شبکه

192.168.10.129 – 192.168.10.190 ادرس های قابل ارائه به سیستم ها

192.168.10.192 ادرس Broadcast شبکه

4- 192.168.10.192

192.168.10.192 ادرس شبکه

192.168.10.193 – 192.168.10.254 ادرس های قابل ارائه به سیستم ها

192.168.10.255 ادرس Broadcast شبکه

حالا سابنت جدید را می نویسیم :

11111111.11111111.11111111.11000000 و به صورت دسیمال 255.255.255.192

برای تمرین ادرس 192.168.2.0 / 24 را به 8 شبکه تقسیم کنید

2. برای تقسیم شبکه بنا بر تعداد Host از فرمول $x=2^h-2$ استفاده میکنیم (منفی دو در اینجا نیز به علت آدرس شبکه و آدرس Broadcast است) در اینجا X مقدار Host درخواستی و H تعداد بیت هایی است که برای Host ID نگه میداریم (توجه کنید در روش بالا برای تقسیم بنا بر تعداد شبکه مشخص شده H تعداد بیتی بود که به Net ID میدادیم اما در اینجا H تعداد بیتی است که برای Host ID نگه میداریم و باقی را به Net ID می دهیم)

برای مثال فرض کنید به ما گفتن شبکه

192.168.1.0/24

را طوری سابنت کنید که هر شبکه شامل 62 سیستم باشد

فرمول را می نویسیم 62 = 2 بتوان h منهای 2 . میدانیم که 2 به عدد 62 اضافه میشود و 64 میشود 2 بتوان 6 پس حاصل H میشود 6

حالا ادرس شبکه را به صورت باینری می نویسم و این بار راست به چپ 6 بیت را جدا میکنیم :

11000000.10101000.00000001.00000000

همانطور که گفتیم در این روش بیت های جدا شده برای Host ID باقی میماند و 2 بیتی که باقی ماند را به Net ID اضافه میکنیم .

از اینجا طبق روش قبل عمل میکنیم و جایگشت های دو بیت را می نویسیم :

1. 192.168.1.0 = 11000000.10101000.00000001.00000000
2. 192.168.1.64 = 11000000.10101000.00000001.01000000
3. 192.168.1.128 = 11000000.10101000.00000001.10000000
4. 192.168.1.224 = 11000000.10101000.00000001.11000000

حالا که آدرس شبکه ها به دست آمد میتوانیم رنج شبکه ها را بنویسیم:

.1

Net Add 192.168.1.0

Net Range 192.168.1.62 – 192.168.1.1

Broadcast Add 192.168.1.63

.2

Net Add 192.168.1.64

Net Range 192.168.1.126 – 192.168.1.65

Broadcast Add 192.168.10.127

.3

Net Add 192.168.1.128

Net Range 192.168.1.222 – 192.168.1.129

Broadcast Add 192.168.1.223

.4

Net Add 192.168.1.224

Net Range 192.168.1.254 – 192.168.1.225

Broadcast Add 192.168.1.255

سابنت جدید را نیز می نویسیم :

192.168.1.192

حالا کمی مثال را سخت می کنیم :

فرض کنید به ما ادرس شبکه 192.168.1.0 را با سابنت 255.255.255.0 را میدهند و شبکه های زیر را میخواهند :

1. یک شبکه با 126 آدرس

2. یک شبکه 62 آدرس

3. چهار شبکه با 14 آدرس

این نمونه مسئله هارا باید مرحله به مرحله حل کرد یعنی ابتدا ما ملاک را 126 سیستم قرار میدهیم و مسئله را حل میکنیم :

128 = 2 بتوان h نهای 2 که در اینجا H می شود 6 پس 6 بیت را برای Host ID نگه میداریم و باقی را که 1 بیت است به Net ID می دهیم :

192.168.1.00000000

این بیت دو آدرس شبکه زیر را به ما میدهد :

1. 192.168.1.00000000 = 0

2. 128 = 192.168.1.10000000

که رنج های زیر را به ما دهد:

1.

Net Add 192.168.1.0

Net Rang 192.168.1.126 – 192.168.1.1

Broadcast Add 192.168.1.128

2.

Net Add 192.168.1.128

Net Range 192.168.1.254 – 192.168.1.129

Broadcast Add 192.168.1.255

سابنت جدید این شبکه 255.255.255.128

شبکه اولی که به دست آوردیم را برای شرط اول مساله حفظ میکنیم و با شبکه دوم به سراغ شرط دوم مساله میرویم :

آدرس شبکه دوم را می نویسیم و با استفاده از فرمول تعداد بیت ها را به دست می آوریم:

2=62 بتوان h نهای 2 ، H مقدار 6 است:

192.168.1.10000000

(توجه کنید که در ادرس جدید بیت 8ام Octet آخر 1 می شود زیرا ما یکبار سابنت کردیم و این شبکه را تقسیم کرده ایم)

این بیت دو آدرس شبکه به ما میدهد:

1. 128 = 192.168.1.10000000

2. 192 = 192.168.1.11000000

که رنج های زیر را به ما دهد:

1.

Net Add 192.168.1.128

Net Range 192.168.1.190 – 192.168.1.129

Broadcast Add 192.168.1.191

2.

Net Add 192.168.1.192

Net Range 192.168.1.254 – 192.168.1.193

Broadcast Add 192.168.1.255

سابنت جدید 255.255.255.192

دوباره شبکه اولی که به دست آوردیم را برای شرط دوم مساله حفظ میکنیم و با شبکه دوم به سراغ شرط سوم مساله میرویم :

آدرس شبکه دوم را می نویسیم و با استفاده از فرمول تعداد بیت ها را به دست می آوریم:

2=14 بتوان h منهای 2 ، H مقدار 4 است:

192.168.1.11000000

این دو بیت چهار آدرس شبکه به ما می دهد:

1. 192 = 192.168.1.11000000
2. 208 = 192.168.1.11010000
3. 224 = 192.168.1.11100000
4. 240 = 192.168.1.11110000

که رنج های زیر را به ما دهد:

.1

Net Add 192.168.1.192

Net Rang 192.168.1.206 – 192.168.1.193

Broadcast Add 192.168.1.207

.2

Net Add 192.168.1.208

Net Range 192.168.1.222 – 192.168.1.209

Broadcast Add 192.168.1.223

که رنج های زیر را به ما دهد:

.3

Net Add 192.168.1.224

Net Range 192.168.1.238 – 192.168.1.225

Broadcast Add 192.168.1.239

.4

Net Add 192.168.1.240

Net Range 192.168.1.254 – 192.168.1.241

Broadcast Add 192.168.1.255

سابنت جدید 255.255.255.224

برای تمرین شبکه 192.168.10.0 با سابنت 255.255.255.0 را به شبکه های زیر تقسیم کنید:

1. چهار شبکه با 62 سیستم
2. دو شبکه با 30 سیستم
3. 4 شبکه با 6 سیستم

پیاده سازی آدرس بعد از انتخاب رنج کار ساده ای است کافیست که به هر سابنت یک رنج اختصاصی دهید.

سابنت مسک عبارتی نظیر آدرس آی پی است که مشخص کننده net id است.

این آدرس به سه شکل prefix binary DDN نوشته میشود.

PREFIX به طور مشخص تعداد بیت های NET ID را مشخص میکند مثلا 172.16.1.1/16 از سمت چپ دارای 16 بیت NET ID است یعنی 172.16

BINARY و ddn از تبدیل prefix به راحتی به دست می آید برای مثال در مثال بالا مقدار باینری

11111111.111111111.00000000.00000000

و همانطور که مشخص است مقدار ddn

255.2555.0.0 است

Chapter-12
Operating Cisco Routers

Routing

روترها اصلی ترین قابلیت لایه network یعنی ارسال بسته ها به صورت نقطه به نقطه از طریق شبکه را ارائه میدهند.

به طور معمول یک شبکه enterprise دارای یک سایت مرکزی و چندین سایت کوچک دور است. برای اتصال در هر سایت معمولا یک سوئیچ Lan داریم که کاربرها را به هم متصل میکنند از طرفی هر سایت حداقل یک روتر دارد که یک دست آن در شبکه lan و یک دست آن در wan است و ارتباط بین سایت ها را برقرار میکند.

روترهای ISR سیسکو تنها قابلیت مسریابی ندارند بلکه چندین قابلیت را به طور همزمان دارند.

دو تفاوت مهم در روترهای soho و enterprise است :

1.روتر های soho عموما برای اتصال به wan از اینترنت و vpn استفاده میکنند

2.روترهای soho عموما روتر، سوئیچ ، wlan ap و... به طور همزمان هستند.

سیستم عامل سوئیچ و روتر سه تفاوت دارند :

1.روترها دستور show mac... را ندارند

2.روتر ها دستور show ip route را دارند

3.سویچ ها از show interface stat استفاده میکنند اما روتر از show ip int br

برای استفاده از روتر های enterprise سیسکو به سه نکته توجه داشته باشید:

1.اینترفیس های بیشتر روترهای سیسکو به طور پیش فرض Shutdown است.

2. روترهای سیسکو بسته های ip را تا زمانی که یک ip و ماسک مناسب روی یکی از interface ها تنظیم نکنید مسیریابی نمیکنند

3.روترهای سیسکو بسته ها را از interface های up/up مسیریابی میکنند

دستور show protocols جزئیات لایه 2ای پورت را نمایش میدهد به علاوه آدرس ip .

Chapter-13

Configuring IPv4 Addresses and Static Routes

IPv4 Routing Concept

Ip routing همان فرایند ارسال و دریافت بسته های ip است؛ بسته های کاربران را از کاربری که بسته را ساخته تحویل میگیرد و آن را به گیرنده حقیقی بسته تحویل میدهد.

کاربران فرستنده از مفاهیم لایه 3 برای تشکیل یک بسته ip استفاده میکنند و آن را به default gateway ارسال میکنند.

روتر ها بنابر منطق لایه 3 برای ارسال بسته های ip آدرس مقصد بسته ها را با جدول مسیریابی خود تطبیق میدهند و تصمیم میگیرند بسته را از کدام پورت ارسال کنند.

فرایند مسیریابی به جزییات لایه data-link در هر لینک نیز وابسته است. مسیریابی به پروتکل های data-link و ارتباطات لایه physical وابسته است.

لایه data-link بسته های ip را در frame های لایه دویی قرار میدهند و در سراسر شبکه جابه جا میکنند.

فرایند مسیریابی زمانی شروع میشود که یک HOST یک بسته IP تشکیل میدهد. برای ارسال این بسته یک سوال اینجا می شود آیا بسته در سابنت خود HOST است یا خیر؟

1.اگر مقصد بسته در سابنت HOST است:

A. آدرس MAC مقصد را از طریق جدول ARP سیستم یا ارسال بسته ARP پیدا کند.

B. بسته IP را با اطلاعات صحیح Data-link در یک encapsulate frame کن.

2. اگر مقصد بسته در سابنت خود host نیست:

A: آدرس مک Default-gateway را از طریق جدول arp یا ارسال بسته arp پیدا کن.

B.بسته ip را با اطلاعات صحیح data-link گیت وی Encapsulate کن.

روتر در 5 مرحله یک بسته را دریافت و ارسال میکند.

1.برای هر فریم دریافت شده data-link تصمیم به دریافت کردن یا نکردن گرفته میشود.

A.فریم CRC-Error نداشته باشد.

B.ادرس مقصد Data-link بسته یکی از ادرس های روتر یا یکی از آدرس های multicast یا broadcast معقول باشد.

2.بسته از داخل فریم decapsulate شود

3.روتر یک تصمیم برای مسیریابی میگیرد. آدرس مقصد بسته را با جدول مسیریابی بررسی میکند. اینترفیس خروجی را انتخاب میکند.

4.بسته داخل یک فریم data-link، encapsulate میشود. هنگام ارسال بسته در یک lan نیاز به arp برای اطلاعات مقصد data-link بسته است.

5.بسته از اینترفیس خروجی منطبق با مسیر ارسال میشود.

به صورت پیشفرض ipv4 routing globally بر روی روترهای سیسکو فعال است. برای اینکه روتر شروع به ارسال و دریافت بسته بکنند کافیست بر روی یک interface up/up ادرس ip تنظیم کنید.

روترها به سه روش مسیرها را به جدول خود اضافه میکنند :

*connected routes : مسیرهایی که در اثر زیر دستور ip add ایجاد میشود.

*static routes : مسیرهایی که در اثر دستور ip route به وجود می آیند.

*routing protocol : یک قابلیت که با تنظیم و فعال کردن بر روی همه روترها ایجاد میشود و مسیرها به طور خودکار اضافه میشوند.

Connected Route

روتر سیسکو به طور پیش فرض یک مسیر برای هر سابنت متصل به هر اینترفیس در جدول ایجاد میکند.

وجود یک connected route در جدول مسیریابی 2 موضوع را راجع به اینترفیس مشخص میکند :

1.اینترفیس در وضعیت up/up است.

2.اینترفیس دارای آدرس ip است.

روتر از طریق subnet mask هر اینترفیس آدرس subnet هر اینترفیس را به دست می آورد و یک مسیر برای آن مینویسد.

Static Route

Static route در صورتی که به مقصد یک شبکه باشد network route است ، هنگامی که به تمامی آدرس ها باشد default route است و هنگامی که به مقصد یک آدرس باشد host route است.

برای ایجاد یک static route دستور زیر را وارد کنید.

Ip route A B C

A: آدرس مقصد شامل یک آدرس یک شبکه یا default

B: سابنت ادرس مقصد

C: آدرس Gateway شامل آدرس next-hop یا اینترفیس های خود دستگاه

با administrative distance می توانید بین مسیرها اولویت بین 1 تا 255 با برتری کمترین انتخاب کنید.

برای عیب یابی static route ها با دستور زیر جدول مسیریابی را بررسی کنید سپس ریشه مشکل را در یکی از سه گزینه زیر پیدا کنید:

Show ip route

1.مسیر در جدول وجود دارد اما درست نیست

A. آدرس Subnet id به درستی انتخاب شده اند؟

B. ادرس Next-hop درست است؟ و آدرس یکی از روترهای همسایه است؟

C. آیا next-hop روتر مناسبی برای مسیر است؟

D. اینترفیس خروجی به درستی تنظیم شده است ؟

2.مسیر در جدول وجود ندارد:

A: وضعیت اینترفیس خروجی UP/UP است؟

B.یک مسیر برای رسیدن به NEXT-HOP وجود دارد؟

3.مسیر درست است اما به درستی کار نمیکند: در فصل 18 برسی میشود.

با دستور show ip route [dst-add] اطلاعات دقیق تری از یک مسیر به دست می آورید.

Chapter-14
IP Routing in the LAN

Router On a Stick (RoaS)

امروزه بیشتر روترهای ENTERPRISE از VLAN ها برای ارسال و دریافت بسته استفاده میکنند. برای این کار نیاز است که بر روی اینترفیس هر VLAN یک آدرس مناسب تنظیم شود. این کار باعث میشود که سابنت مناسب با آن اینترفیس ایجاد شود .

هنگامی که یک سوئیچ از طریق یک لینک TRUNK به یک پورت روتر متصل باشد و روتر وظیفه مسیریابی بین VLAN های این TRUNK را داشته باشد ROAS نام دارد.

روتر برای خواندن تگ های DOT.1Q فریم های لینک TRUNK از Sub-interface استفاده میکند.

توجه داشته باشید که روتر ها از DTP پشتیبانی نمیکنند.

برای تنظیم یک ترانک بر روی روتر مراحل زیر را اجرا کنید:

1.با دستور زیر برای هر vlan یک sub-interface بسازید

Int [type][num.subnum]

2.سپس با زیر دستور زیر تگ dot1q را بخوانند

Encapsulation dot1q [vlan-id]

3.سپس به هر sub-interface ادرس مناسب با سابنت vlan مرتبط بدهید

در صورتی که در یک Sub-interface زیر دستور encapsulation را وارد نکنید vlan مرتبط را native vlan در نظر میگیرد.

زیر دستور ساب اینترفیس encapsulation dot1q vlan id native به روتر میگوید این اینترفیس به native-vlan متصل است

توجه داشته باشید در صورتی که اینترفیس اصلی down باشد Sub-interface ها هم down میشوند.

دستور show vlan جزییات vlan های روتر را نمایش میدهد.

Switched Virtual Interface (SVI)

سوئیچ های لایه 3 برای مسیریابی بین vlan ها از svi استفاده میکنند که هر interface vlan را مانند یک پورت روتر در نظر میگیرد و مسیرهای متصل به این اینترفیس ها در جدول مسیریابی اضافه میکند.

برای فعال کردن svi مراحل زیر را انجام دهید:

1.با دستور زیر یا چیزی شبیه به این مسیریابی را در سوئیچ فعال کنید.

Sdm prefer lanbase-routing

2.با دستور reload سویچ را ریست کنید تا تنظیمات اعمال شوند.

3. با دستور ip routing مسیریابی را آغاز کنید.

در SVI پورت های سوئیچ همچنان در واقع لایه 2 ایی عمل میکنند و فرایند مسیریابی بین 2 پورت مجازی VLAN انجام میشود اما پورت سوئیچ میتواند در وضعیت ROUTED قرار گیرد و مانند یک پورت روتر عمل کند.

برای فعال کردن ROUTED PORT کافی است زیر دستور no switchport را روی اینترفیس مورد نظر وارد کنید.

Layer3 Ether-Channel

برای راه اندازی ether channel لایه 3 ای کافیست زیر دستور no switchport بر روی تمام اینترفیس های port-group و خود اینترفیس port channel وارد شود بر روی این اینترفیس ادرس تنظیم شود.

Chapter-15
Troubleshooting IPv4 Routing

Ping

برای عیب یابی IPV4 بسیاری از مواقع از PING استفاده میکنیم

PING پیامی شبیه به متن زیر به مقصد ارسال میکند:

*در صورتی که این بسته را دریافت می کنید و آدرس مقصد این بسته آدرس تو است یک پاسخ برای فرستنده ارسال کن.

در واقع ping از پروتکل icmp استفاده میکند که این پروتکل با دو پیام echo request و echo reply ارتباط بین دو دستگاه را چک میکند. icmp پیام های دیگر نیز دارد.

پروتکل icmp به هیچ یک از پروتکل های tcp یا udp یا پروتکل های لایه app وابسته نیست و بخشی از لایه network است.

با وارد کردن دستور ping میتوانید پارامترهای دلخواه برای ping مانند آدرس فرستنده و حجم و...انتخاب کنید.

Trace Route

دستور traceroute یک بسته icmp ایجاد میکند که از تمام روترهای سر راه reply ارسال میکند.

Trace route با پیام icmp ttl exceeded کار میکند.

با وارد کردن دستور traceroute می توانید مانند ping پارامترها را شخصی سازی کنید.

گاهی برای بررسی اتصال از ssh و telnet استفاده میکنیم.

Chapter-16
Understanding OSPF Concepts

Routing Protocol

تفاوت بین Routing Protocol و Routed Protocol :

routing protocol: به پروتکل های مسیریابی گفته میشود که به صورت خودکار با الگوریتم های خود مسیرها را شناسایی کرده و به جدول اضافه می کنند.

routed protocol: را به پروتکل هایی که ساختار آدرس در بسته ها را تشکیل می دهند و قابلیت مسیریابی شدن را دارند گفته میشود مانند ipv6 و ipv4

قابلیت های عمومی تمامی پروتکل های مسیریابی به شرح زیر است:

- Routing Information روترهای همسایه را یاد میگیرند.
- شبکه های خود را تبلیغ میکنند.
- در صورتی تغییر توپولوژی یا قطع شدن یک لینک این مساله را تبلیغ میکند و در صورت نیاز مسیرهای جدیدی انتخاب میکنند.

مساله دیگر در پروتکل های مسیریابی convergence است. این به معنای آن است که هنگامی که تغییری رخ دهد روترها چطور به این تغییر واکنش نشان داده و آن را برطرف میکنند.

پروتکل های مسیریابی به دو دسته خارجی EGP و داخلی IGP تقسیم میشوند.

پروتکل های داخلی یا IGP برای مسیریابی داخلی LAN یا درون یک AS استفاده میشوند اما پروتکل های EGP برای مسیریابی در WAN یا بین AS ها استفاده میشود.

Autonomous system به یک شبکه تحت کنترل یک سازمان خاص میگویند. مانند شبکه یک isp یا شبکه یک سازمان بزرگ مانند google.

AS ها با یک شماره به نام AS NUMBER یا ASN شناخته میشوند. مانند ادرس های پابلیک ASN باید از IANA خریداری میشود.

پروتکل های مسیریابی داخلی از نظر الگوریتم انتخاب بهترین مسیر 3 دسته هستند.

- distance vector
- advance distance vector
- link state

Metric هر مسیر به پروتکل در انتخاب بهترین مسیر کمک میکند. مثلا در rip متر یک تعداد روتر سر راه است اما در ospf مقدار cost این عدد را تعیین میکند.

تمامی مسیرهای که یک پروتکل ایجاد میکند مقدار AD یکسان دارند مثلا AD-OSPF 110 است و EIGRP 80 .

OSPF

روترها هنگام استفاده از پروتکل های link-state عملا باید تمام جزییات مربوط به شبکه های خود را تبلیغ کنند.

بعد از انجام عملیات flooding اطلاعات تمامی روترها در شبکه اطلاعات یکسانی دارند.

Ospf با استفاده از LSA و LSDB عملیات های خود را انجام میدهد LSA ساختار داده ایی از اطلاعاتی از شبکه را دارند و LSDB مجموع تمامی LSA های دریافتی هر روتر است.

هنگامی که یک روتر LSA را flood میکند تمامی روترهای دیگر حاضر در پروتکل این LSA را دوباره ارسال میکند تا تمامی روترها یک نسخه از این LSA داشته باشند.

درواقع روترها قبل از ارسال این LSA از روترهای همسایه یک سوال میکنند ایا این LSA را دارد یا خیر؟ در صورتی که نداشت برایش ارسال میکنند.

در صورت ایجاد تغییر در شبکه روتر دوباره LSA ارسال می کنند همچنین هر روتر در پایان aging timer دوباره LSA ارسال میکند.

فرایند flooding در link-state باعث تکمیل LSDB جامع میشود این برای اضافه کردن مسیر به جدول کافی نیست.

Ospf از الگوریتم shortest path first برای انتخاب بهترین مسیر استفاده می کند.

Ospf با spf کل LSDB را بررسی کرده و مسیرهایی که باید به جدول اضافه شوند را انتخاب میکند.

OSPF برای داد و ستد LSA ها و ایجاد مسیرها 3 مرحله اصلی زیر را طی میکند:

1. همسایه شدن: ارتباط بین 2 روتر که بر روی یک DATA-LINK قرار دارند است تا روترها LSDB خودشان را مبادله کنند.
2. ارسال دیتابیس: مرحله ای که LSA ها ارسال می شوند تا روترها دیتابیس های یکسانی داشته باشند.
3. اضافه کردن بهترین مسیر: مرحله ای که هر روتر جداگانه فرایند SPF را بر روی LSDB محلی خود انجام میدهد و بهترین مسیر را به جدول مسیریابی اضافه میکنند.

از بین چیزهایی که در این فصل می آموزید همسایگی OSPF بیشترین چیزی است که در خطا یابی OSPF به کار شما می آید.

Neighboring

شما روترها را تنظیم می کنید تا OSPF را اجرا کنند و با روترهای دیگر همسایه شوند باقی کار را OSPF انجام میدهد.

روترها برای همسایه شدن علاوه بر بودن بر روی یک لینک باید پیام های OSPF ارسال کنند و همسایگی را قبول کنند.

روترها با ارسال OSPF HELLO MASSAGE خود را به عنوان همسایه بالقوه معرفی میکنند.

برای دیدن وضعیت همسایگی در OSPF دستور زیر را وارد کنید.

show ip ospf neighbor

وضعیت همسایگی OSPF میتواند به روتر بگوید چه زمانی همسایه برای مسیریابی بسته ها مناسب نیست.

HELLO MASSAGE شامل RID هر روتر است. RIDیک مقدار 32 بیتی است که به شکل DDN نمایش داده میشود. به طور پیش فرض روتر از یکی از IP هایش برای RID استفاده میکند.

روترها HELLO MASSAGE را به هر اینترفیس MULTICAST میکنند و انتظار دارند روی آن لینک ها HELLO دریافت کنند.

روترها به طور مداوم در بازه زمانی HELLO TIME بسته های HELLO ارسال میکنند.

مشخصات HELLO PACKET به شرح زیر است :

*بسته های HELLO دارای هدرIP است با پروتکل 89

*بسته های HELLO به آدرس مالتی کست 224.0.0.5 برای دریافت HELLO گوش میدهند.

روتر هنگامی که یک HELLO دریافت کند وضعیت همسایگی با آن روتر را init در نظر میگیرد و هنگامی که Hello بعدی را با شناسه خودش از همان RID دریافت کند وضعیت همسایگی WAY-2 میشود.

هنگامی که یک روتر یک همسایه در وضعیت 2WAY دارد به این معنی است که:

1. روتر یک HELLO دریافت کرده با RID روتری که به عنوان همسایه INIT در نظر گرفته بود.
2. روتر تمام پارامترهای HELLO را بررسی کرده و مشکلی وجود نداشته روتر در این مرحله مایل است که همسایه شود.
3. اگر 2 روتر روبه رو به وضعیت 2WAY در بیاید به این معناست که روترها تمام تنظیمات مربوط به همسایگی OSPF را بررسی کرده و مشکلی وجود نداشته: الان هر دو روتر آماده جابه جایی LSDB هستند.

Exchanging Database

در مرحله مبادله دیتابیس روترها در ابتدا تمامی LSDB را ارسال نمیکنند بلکه تمامی LSA هایی که در LSDB دارند را لیست میکنند و به روتر روبرو ارسال میکنند: در این حالت هر روتر متوجه میشود کدام LSA ها را دارد و کدام ها را نیاز دارد.

بسته هایی که LSA ها را بین روترها جابجا میکنند با جزئیات هر LSA یا LSU نام دارند.

بسته هایی که بعد از 2WAY لیست کلی LSA ها را جابجا میکنند DBD یا DATABASE DESCRIPTION نام دارد.

به مرحله ایی که روترها DBD ارسال میکنند EXCHANGE ، مرحله که LSU ها را مبادله میکنند LOADING و مرحله ای که تمام دیتابیس ها تطابق داده میشود FULL گفته میشود.

Maintaining Neighbour

بعد از انجام همسایگی روترها تلاش میکنند تا بر برقراری این همسایگی نظارت کنند برای این کار از دو زمان سنج HELLO INTERVAL و DEAD INTERVAL استفاده میکنند.

به طور معمول روترها در مدت HELLO خود یک بسته HELLO ارسال میکنند یک روتر در صورتی که در مدت DEAD INTERVAL که برابر با 3 زمان HELLO است از یک همسایه HELLO دریافت نکنند آن همسایه را از بین رفته در نظر می گیرد.

مورد بعدی نگهداری همسایگی اطلاع تغییرات است هنگامی که تغییری در شبکه ایجاد شود یک یا چند LSA تغییر میکند و روترها باید این LSA جدید را FLOOD کنند.

مورد سوم نگهداری ارسال مجدد LSA ها است هر روتری که یک LSA تشکیل داده و آن را FLOOD کرده است موظف است که به طور پیشفرض هر 30 دقیقه مجدد آن LSA ارسال کند.

OSPF Network Type

به طور پیشفرض نوع اینترفیس OSPF از نوع BROADCAST است و این باعث ایجاد DESIGNATED ROUTER میشود.

DR نقش کلیدی در تبادل دیتابیس بازی میکند.

با وجود DR دیگر هر روتر دیتابیس را با تمام روترهای دیگر تبادل نمیکند بلکه DR با همه ی روترها دیتابیس را تبادل می کند و مطمئن میشود هر روتر یک نسخه کامل از LSDB را دارد BDR در صورت شکست DR نقش DR را بر عهده میگیرد.

DR برای ارسال LSA ها به تمامی روترها آنها را به سادگی به آدرس مالتی کست 224.0.0.5 ارسال میکند و تمام روترها بر روی این آدرس LSA ها را دریافت میکنند.

226.0.0.5* برای OSPF به معنای تمام روترهای OSPF ذخیره شده است.

روترهای غیر DR برای ارسال بسته به DR کافیست بسته را به آدرس 226.0.0.6 به معنی تمام DR های OSPF ارسال کنند تا DR و DBR دریافت کنند.

در شبکه های OSPF با نوع اینترفیس برادکست روترهای غیر DR یا DrOther نام دارند. وضعیت همسایگی هر روتر با dr ها بعد از مبادله که دیتابیس full میشود اما وضعیت همسایگی با روترهای drother چون تبادل دیتابیس انجام نمی شود در وضعیت 2way میماند و این درست است .

Adding Best Route To Table

الگوریتم spf دیتابیس ospf را بررسی میکند ؛ برای هر سابنت مسیر مناسب و مسیر مناسب برای رسیدن به هر gateway را بررسی میکند در صورتی که بیشتر از یک مسیر برای رسیدن به یک شبکه مقصد داشته باشد با استفاده از کمترین متریک یک مسیر را انتخاب میکند.

Spf برای محاسبه متریک cost تمام اینترفیس های خروجی برای رسیدن به شبکه مقصد را باهم جمع میزند و کمترین متریک را انتخاب میکند.

Area

در شبکه های کوچک ospf در یک منطقه(area backbone) به خوبی کار میکند اما در شبکه های بزرگی مانند شبکه های ENTERPRISE باید شبکه دارای مناطق مختلف باشد.

استفاده از OSPF تنها با یک منطقه در شبکه های ENTERPRISE با دیتابیس های خیلی بزرگ باعث مشکلات زیر میشود:

*دیتابیس بزرگ نیاز به RAM بیشتر برای نگهداری در هر روتر دارد.

*دیتابیس بزرگ فرایند SPF را بر روی دیتابیس کند میکند.

*تغییر تنها یک اینترفیس در شبکه باعث بررسی مجدد SPF در تمامی روتر ها میشود.

مدارک مرز استفاده از AREA های مختلف را نهایتا تا زمانی می دانند که شبکه 50 روتر دارد بعد از آن توصیه میشود حتما از AREA های مختلف استفاده کنید.

برای راه اندازی OSPF با AREA های مختلف به موارد زیر توجه کنید:

1. تمام اینترفیس های مربوط به یک سابنت باید در یک AREA باشند.
2. یک منطقه باید به هم پیوسته باشد.
3. بعضی روترها ممکن است داخلی باشند و تمامی اینترفیس های آن عضو یک AREA باشد
4. بعضی روترها ممکن است مرزی باشند یعنی ABR و یک پورت در AREA 0 و پورت های دیگر در AREA دیگر باشند
5. AREA های غیر BACKBONE باید یک مسیر مستقیم به AREA 0 با یک روتر ABR که از یک سمت در AREA 0 است داشته باشند.

LSA

LSA ها در OSPF انواع مختلفی دارند که الان به بررسی نوع 1 تا 3 می پردازیم

ROUTER LSA.1 : به ازا هر روتر یکی وجود دارد این LSA شامل IP ADD ، INTERFACES، RID MASK، و وضعیت کنونی اینترفیس ها است.

NETWORK LSA.2: به ازا هر شبکه که DR دارد یکی وجود دارد که شامل آدرس DR و bdr سابنت id و ماسک است.

summary LSA.3 به ازا هر سابنت در یک area دیگر به وجود می آید که شامل سابنت id، ماسک و rid روتر BDR که این LSA را تبلیغ کرده است.

OSPF با استفاده از بررسی از LSA های تایپ 1و2 نقشه توپولوژی شبکه را رسم میکند.

Chapter-17
Implementing OSPF

OSPF Config

برای راه اندازی OSPF بر روی روتر مراحل زیر را دنبال کنید:

1. با دستور زیر فرایند OSPF را روی روتر فعال کنید:

route ospf [process-id]

*توجه داشته باشید که این یک مقدار لوکال است نیازی نیست که در صورت یک همسایگی یکسان باشد یا با شماره AREA یکسان باشد.

2. در صورت تمایل به یکی از 3 روش زیر RID را تنظیم کنید:

A- با استفاده از زیر دستور router-id [value]

B- تنظیم آی پی آدرس بر روی یک اینترفیس LOOPBACK توجه داشته باشید بزرگترین آدرس میان LOOPBACK ها انتخاب میشود.

*برای ایجاد یک اینترفیس LOOPBACK از دستور زیر استفاده کنید

interface loopback [num]

C- بر روی یک اینترفیس غیر LOOPBACK آدرس تنظیم کنید و باز توجه داشته باشید بزرگترین آدرس انتخاب میشود

3. با استفاده از زیر دستور زیر شبکه ها را به OSPF اضافه کنید

network [ip wide-mask] area [area-num]

Show OSPF

برای بررسی ospf در مراحل مختلف از دستورات زیر استفاده کنید:

- برای بررسی تنظیمات ospf

Show running-config / show protocol

- برای دیدن اینترفیس های فعال در ospf :

Show ip ospf interface [brief/type]

- برای دیدن وضعیت همسایگی:

Show ip ospf neighbor [type]

- برای دیدن دیتابیس :

Show ip ospf database

- برای دیدن تمام مسیر های آموخته شده بدون توجه به متریک:

Show ip ospf rib

- برای دیدن مسیر های اضافه شده به جدول مسیریابی

Show ip route [ospf/subnet-mask/section subnet]

Passive Interface

ospf وضعیت پورتی که از طریق آن Hello ارسال و دریافت نکند را Passive در نظر میگیرد .

شرایط Passive Interface به شرح زیر است:

- ospf همچنان سابنت متصل به این اینترفیس ها را از طریق LSA ها تبلیغ می کند.
- دیگر در این اینترفیس ها Hello ارسال نمی کند.
- دیگر هیچ Hello دریافتی از این اینترفیس ها را بررسی نمیکند.

معمولا Passive Interface ها اینترفیس هایی هستند که به سمت Lan بدون هیچ روتری در آن می روند.

برای فعال سازی Passive Interface از دستور زیر استفاده کنید :

با زیر دستور ospf زیر تمام اینترفیس های روتر Active هستند و فقط اینترفیس های مشخص شده Passive می شوند :

passive-interface [type num]

با زیر دستور ospf زیر تمام اینترفیس های روتر Passive هستند و باید به صورت دستی با دستور no اینترفیس هایب مورد نظر را Active کنید :

passive-interface default

Default Route Advertise

برای اینکه DEFAULT-ROUTE را از طریق OSPF تبلیغ کنید مراحل زیر را انجام دهید :

1. ابتدا به صورت دستی بر روتر همه شبکه DEFAULT-ROUTE ایجاد کنید.
2. با دستور زیر DEFAULT-ROUTE را در همان روتر تبلیغ کنید:

default-information originated

Interface Cost

برای تغییر COST یک مسیر در OSPF 3 روش وجود دارد

با زیر دستور مستقیم بر روی اینترفیس

ip ospf cost [value]

OSPF از محاسبه Reference Bandwidth / Interface Bandwidth ,COST هر مسیر را به دست می آورد.

برای تغییرات cost یک لینک اصلا توصیه نمیشود که BW یک اینترفیس را تغییر دهید این کار بر روی سرعت انتقال اطلاعات تاثیر دارد به جای آن RED-BW را تغییر دهید.

REF-BW پیشفرض 100 مگ است پس برای لینک های 100 مگ به بالا COST برابر با 1 است

برای تغییر REF-BW از زیر دستور OSPF زیر استفاده کنید.

auto-cost reference bandwidth bw

Load Balance

در صورتی که روتر به یک مقصد چندین مسیر با cost های برابر داشته باشد میتواند بین این مسیرها load balance انجام دهد تعداد مسیر همزمان را با زیر دستور تنظیم کنید

maximum-paths value

Chapter-18
OSPF Network Types and Neighbors

OSPF Network Type

در CCNA 200-301 در مورد دو نوع شبکه OSPF صحبت میکنیم

- POINT-TO-POINT
- BROADCAST

در شبکه های BroadCast روترهای DR و BDR انتخاب میشوند.

انتخاب DR و BDR به شما کمک میکند که در صورت خراب شدن DR روتر BDR به راحتی نقش DR را بر عهده بگیرید و اگر روتر بهتری به شبکه اضافه شد DR نشود.

OSPF برای انتخاب DR ابتدا PRIORITY پورت ها را بررسی میکند در صورتی که برابر بود بزرگترین RID به عنوان DR و دومین BRD میشود.

برای انتخاب دستی DR باید PRIORITY را از زیر دستور اینترفیس تغییر دهید

ip ospf priority value-0-to-255

POINT TO POINT : این شبکه برای زمانی است که بر روی یک لینک DATA-LINK تنها دو روتر داریم در این صورت نیاز به DR و BDR نیست.

شبکه P2P با زیر دستور اینترفیس زیر تنظیم میشود:

ip ospf network point-to-point

OSPF برای تشکیل همسایگی نیاز دارد که هر دو روتر مقادیر یکسانی NEIGHBOR REQUIREMENTداشته باشند.

1. اینترفیس ها باید در وضعیت UP/UP باشند.
2. ACL ها نباید به بسته های پروتکل مسیریابی را فیلتر کنند.
3. اینترفیس ها باید در یک سابنت باشند.
4. در صورت نیاز باید از احراز هویت پروتکل عبور کنند.
5. زمان سنج ها HELLO و DEAD یکسان باشند.
6. RID ها باید همسان باشند.
7. در یک AREA باشند.
8. فرایند OSPF نباید غیرفعال باشد.
9. اینترفیس های همسایه باید MTU برابر داشته باشند.
10. اینترفیس های همسایه باید نوع شبکه یکسانی داشته باشند

- ردیف های 9 و 10 جلو همسایگی را نمی گیرند.

Chapter-19
Basic IPv4 Access Control Lists

Access Control List

:IPV4 ACCESS CONTROL LIST

IP ACL از طریق فیلدهای داخل هدر IP، TCP و udp بسته ها را شناسایی میکند.

برای مثال برای اعمال QOS بر روی بسته ها از ACL استفاده میکنیم.

در ACL دو چیز خیلی مهم است : محل قرار گیری و جهت قرارگیری. این به این معناست که ACL ها برای اجرا شدن باید بر روی یکی از 2 ترافیک IN و OUT بر روی یکی از اینترفیس ها تنظیم شود.

برای فیلتر کردن بسته ها با استفاده از ACL دو اکشن وجود دارد permit و deny

انواع ACL ها:

- Standard numbered 99.1
- extended numbered 122.100
- additional acl numbered 1999.1300 standard
- named acl
- improved editing with sequence num

Acl استاندارد فقط نسبت به src-ip فیلتر می کند اما extended نسبت به پروتکل src و dst-ip و در tcp و udp مقدار src/dst پورت هم بررسی می شود .

هنگامی که یک بسته اولین ردیف همخوان ACL مطابق شود دیگر در جدول پیش نمی رود و متوقف میشود.

Standard ACL

برای تنظیم یک ACL استاندارد از نوع NUMBERED از دستور زیر استفاده کنید

access-list (1-99/1300-1999) (permit/deny) [target-ip wildmask]

در قسمت آدرس در ACL می توانید از یک آدرس استفاده کنید یا با استفاده از WILD MASK رنج تعیین کنید.

با استفاده از ANY در قسمت آدرس این ACL شامل تمام بسته ها میشود.

توجه کنید هنگام راه اندازی ACL بر روی یک اینترفیس به صورت پیش فرض تمامی ورودی هایی که شامل ACL نشود DENY میشوند پس حتما باید در پایان ACL یک PERMIT ANY برای باقی ترافیک فیلتر نشده بزارید.

برای فعال کردن ACL بر روی یک اینترفیس از زیر دستور اینترفیس زیر استفاده کنید:

ip access-group [acl-num]

در صورتی که در پایان ACL از کلید واژه LOG استفاده کنید روتر آمار تمام بسته های همسان شده با این ACL را به شما نشان میدهد.

Chapter-20
Advanced IPv4 Access Control Lists

Extended ACL

در صورتی که میخواهید یک EXTENDED ACL بر روی تمامی بسته های IPV4 اعمال شود از پروتکل IP استفاده کنید. شامل تمام بسته های IPV4 مانند ICMP، TCP و UDP میشود.

در extended acl هایی با پروتکل های tcp و udp میتوانید بسته ها را نسبت به SRC و DST پورت نیز فیلتر کنید.

برای تعیین پورت ACL های EXTENDED از کلید واژه های زیر استفاده کنید.

نابرابر با=EN کمتر از=IT برابر با = eq بین = range بزرگتر از=gt

برای تنظیم یک extended acl از دستور زیر استفاده کنید.

access-list (199-100 1200-2699) (permit l deny) [Protocol] src-ip src-port dst-ip dst-port

هم src-ip و هم dst-ip میتواند یک آدرس باشد یا با دادن wildmask یک رنج باشد.

Named acl هیچ تفاوتی در فیلتر کردن بسته ایجاد نمیکند بلکه مدیریت acl را ساده تر میکند.

Named acl سه تفاوت اصلی با numbered acl دارد:

1. به خاطر سپردن و نگهداری ACL را ساده تر میکند.
2. به جای دستور global از زیر دستور استفاده میکنید
3. یک قابلیت خاص ادیت کردن به کاربر CLI میدهد که به جای اصلاح کل ACL تنها یک خط آن را اصلاح کنید

در حالت پیشرفته ACL چه در حالت NUMBERED چه در حالت NAMED می توانید از ادیت خط ها توسط SEQ-NUMBER استفاده کنید.

هنگامی که دارید با استفاده از زیر دستور IP ACCESS LIST یک لیست ایجاد میکنید میتوانید با وارد کردن عدد در ابتدای خط شماره Seq را انتخاب کنید در صورت وارد نکردن عدد seq به صورت پیشفرض اعداد ضریب 10 وارد میشود .

Ip access -list (1-2147483674) acl

برای حذف یک ردیف کافی از دستور no seq در زیر دستور استفاده کنید.

Chapter-21
Policy Based Routing (PBR)

در شبکه‌های سیسکو، route-map یک ابزار قدرتمند برای کنترل و تغییر مسیرهای شبکه است. با استفاده از route-map ، می‌توانید سیاست‌های مسیریابی پیچیده‌ای را تعریف کنید که بر اساس معیارهای مختلف، ترافیک شبکه را تغییر دهند یا هدایت کنند. این ابزار شامل دو دستور کلیدی match و set است که به شما اجازه می‌دهد تا معیارهای تطبیق و تغییرات مورد نظر را تعریف کنید.

Route-Map چیست؟

route-map ابزاری است که به شما امکان می‌دهد مسیرها را بر اساس شرایط مختلف تغییر دهید یا کنترل کنید. این ابزار به ویژه در پروتکل‌های مسیریابی دینامیک مانند BGP و OSPF استفاده می‌شود، اما می‌تواند در بسیاری از سناریوهای مسیریابی و کنترل ترافیک مورد استفاده قرار گیرد. هر route-map می‌تواند شامل یک یا چند بخش باشد که هر بخش شامل دستورات match و set است.

فرض کنید یک روتر 2 عدد Default route با Distance های مختلف دارد یکی 1 و یکی 100 . همانطور که میدانید مادامی که مسیر اول فعال باشد ترافیکی از مسیر با Distance مقدار 100 عبور نمیکند. حالا با استفاده از PBR میتوانید شرایطی را تعیین کنید که ترافیک هایی که مشخص میکنید بی توجه به Distance از مسیر دوم عبور کنند .

یا هنگامی که چند اینترنت متفاوت دارید و نیاز دارید چند Nat متفاوت داشته باشید با PBR می توانید این کار را انجام دهید .

دستور Match :

دستور match برای تعیین معیارهای تطبیق استفاده می‌شود. این معیارها مشخص می‌کنند که کدام بسته‌های داده باید توسط route-map پردازش شوند. معیارهای match می‌توانند شامل موارد زیر باشند:

1. تطبیق آدرس IP:

- تطبیق آدرس‌های IP مبدا و مقصد با استفاده از access-list ها.

match ip address [access-list-number | access-list-name]

2. تطبیق prefix-list:

- تطبیق بر اساس لیست‌های پیشوندی (prefix lists).

match ip address prefix-list [prefix-list-name]

4. تطبیق metric:

- تطبیق بر اساس متریک‌های خاص.

match metric [metric-value]

دستور Set :

دستور set برای اعمال تغییرات و تنظیمات بر روی ترافیک تطبیق داده شده توسط دستورات match استفاده می‌شود. این تغییرات می‌توانند شامل موارد زیر باشند:

1. تغییر next-hop:

- تعیین آدرس IP جدید برای next-hop.

set ip next-hop [ip-address]

2. تغییر متریک:

- تنظیم متریک مسیر.

set metric [value]

3. تغییر interface:

- تعیین اینترفیس برای ارسال ترافیک.

set interface [interface-type]

مثال‌های عملی

مثال 1: هدایت ترافیک به Next-Hop خاص

این مثال نشان می‌دهد که چگونه می‌توانید ترافیک یک شبکه خاص (192.168.1.0/24) را به یک next-hop مشخص هدایت کنید.

access-list 10 permit ip 192.168.1.0 0.0.0.255 any

route-map EXAMPLE permit 10

```
match ip address 10
set ip next-hop 10.1.1.1
```

مثال 2: تغییر متریک برای یک مسیر

این مثال نشان می‌دهد که چگونه می‌توانید متریک مسیر را برای ترافیک یک شبکه خاص تغییر دهید.

```
access-list 20 permit ip 192.168.2.0 0.0.0.255 any

route-map EXAMPLE permit 10
match ip address 20
set metric 100
```

نتیجه‌گیری

با استفاده از route-map و دستورات match و set ، می‌توانید سیاست‌های مسیریابی پیچیده و دقیقی را در شبکه‌های خود پیاده‌سازی کنید. match به شما اجازه می‌دهد تا ترافیک خاصی را شناسایی کنید و set به شما امکان می‌دهد تغییرات دلخواه خود را بر روی آن ترافیک اعمال کنید. این ابزارها به شما کنترل کاملی بر جریان ترافیک شبکه می‌دهند و به بهینه‌سازی عملکرد شبکه کمک می‌کنند.

Chapter-22
Implementing Switch Port Security

Port Security

پورت سکیوریتی می تواند از اتصال دستگاه های ناخواسته از طریق بررسی src-mac فریم های ارسال شده از دستگاه ها جلوگیری کند.

تنظیمات port-security به طور مجزا با تنظیمات متفاوت به ازا هر پورت بر روی اینترفیس ها اجرا میشود.

هر پورت یک ماکزیمم تعداد mac متصل دارد که اگر از این تعداد بیشتر شود port-security تشخیص میدهد که تخلف اتفاق افتاده است.

فعال سازی پورت سکیوریتی بر روی پورت موارد زیر را فعال می کند :

1. فریم های دریافتی بر روی پورت بررسی میشوند تا وقوع تخلف را متوجه شود.
2. ماکزیمم تعداد mac مجاز بر روی هر پورت را تعریف میکند.
3. آمار تمام mac های غیر تکراری بر روی پورت را نگه میدارد.
4. mac های جدید یاد گرفته شده را مانیتور می کند تا اگر یاد گرفتن mac جدید باعث تخلف در تعداد mac مجاز پورت شد متوجه شود.
5. فریم های دریافتی از mac متخلف را بنابر تنظیمات نابود و... میکند.

علاوه بر موارد بالا پورت سکوریتی میتواند:

1. حد مجاز mac عدد 3 تعریف شود و 3تا دستی تعریف شوند.
2. حد مجاز mac عدد3 تعریف شود و 3تا اتومات تعریف شوند.
3. حد مجاز mac عدد 3 تعریف شود و یکدستی و 2 تا اتومات باشد.

port -security روی هر پورت trunk و یا access تعریف میشود اما این پورت ها باید دستی ترانک یا access شده باشند.

برای راه اندازی port-security مراحل زیر را انجام دهید :

1.با دستور زیر به صورت دستی پورت را ترانک یا access کنید.

Switch port (mode access/trunk)

2.با زیر دستور زیر port security را بر روی پورت فعال کنید.

Switchport port-security

3.با زیر دستور زیر حد مجاز mac را مشخص کنید.

switchport port-security maximum [num]

4.با دستور زیر برخورد در صورت اتفاق تخلف را تعین میکند

Switchport port-security violation(protect/restrict/shut down)

5.با دستور زیر تعیین کنید به صورت mac-sticky یاد گرفته شود

Switchport port-security mac-address sticky

6.با دستور زیر برای mac ،port دستی تعیین کنید.

Switchport port-security mac-address [mac]

این موارد اختیاری بوده و با نادیده گرفتن آنها port-security با مقادیر پیش فرض خود کار میکند.

با دستور show port-security [type num] وضعیت امنیت یک پورت را میتوانید بررسی کنید .

رفتار های port security به شرح زیر است:

عملیات	protect	restrict	shutdown
نابود کردن ترافیک مجاز	Yes	yes	yes
ارسال مسیج به Snmp سرور	No	yes	yes
قرار دادن پورت در وضعیت err-dis	No	yes	yes

به طور پیش فرض port-security حد مجاز mac را 1 و رفتار را shutdown قرار میدهد

در رفتار shut down وقتی تخلف رخ می دهد سه اتفاق زیر رخ میدهد :

1. وضعیت پورت بنابر دستور show interface به err-disable تغییر میکند.
2. وضعیت پورت در port-sec به secure-down تغییر میکند.
3. سوئیچ ارسال و دریافت فریم از پورت را متوقف میکند.

در صورتی که پورت err-disable شود برای فعال شدن مجدد باید پورت را shutdown و سپس no shutdown کنید.

یا برای اجرای خودکار هنگامی که فقط توسط port sec غیر فعال شود.

errdisable recovery cause psecure-violation

برای فعال شدن مجدد پس از زمان مشخص :

errdisable recovery interval [sec]

Chapter-23
Network Address Translation

Source Nat

برای راه اندازی SRC NAT دستی از دستورات زیر استفاده کند.

1. برای تعیین INT ورودی بسته ها فرایند NAT زیر دستور اینترفیس زیر را وارد کنید :

ip nat inside

2. برای تعیین INT خروجی بسته فرایند NAT زیر دستور اینترفیس زیر را وارد کنید :

ip nat outside

1.3. برای تعیین آدرس هایی که باید به هم ترجمه شوند :

ip nat inside source static [local-ip public-ip]

3.2. با روش بالا تنها یک آدرس NAT میشود برای اینکه یک رنج را NAT کنید ابتدا باید یک ACL برای این رنج بسازید و به جای STATIC با گزینه LIST.ACL را معرفی کنید

3-2-1 access-list [num] permit [subnet-id wildmask]

3-2-2 ip nat inside source list [num] interface [out-interface]

3-3 برای اینکه از گروهی آدرس PUBLICE برای NAT استفاده کنیم لازم نیست تمام آنها را روی روتر ست کنیم کافی است تمام آنها به سمت ما ROUTE شوند سپس با تنظیم یک NAT POOL تمام آدرس ها را استفاده کنید.

3-3-1 SETUP ACL

3-3-2 ip nat pool [name] [start-ip] [end-ip] network [mask]

3-3-3 ip nat inside source list [num] pool [name]

در صورتی که چند اینترنت با Distance های مختلف داشته باشیم باید به ازاء هر اینترفیسی که از آن اینترنت دریافت میکنیم یک Route-map ایجاد کنیم و سپس برای Route-map ها Nat ایجاد کنیم .

Chapter-24
FHRP (First Hop Redundancy Protocol)

مقدمه:

FHRP یا First Hop Redundancy Protocol مجموعه‌ای از پروتکل‌ها است که به منظور افزایش دسترسی‌پذیری و پایداری شبکه‌های محلی (LAN) طراحی شده‌اند. این پروتکل‌ها تضمین می‌کنند که همیشه یک روتر فعال برای مدیریت ترافیک شبکه وجود دارد و در صورت خرابی روتر اصلی، روتر دیگری به سرعت جایگزین آن می‌شود. این امر باعث می‌شود که کاربران نهایی و دستگاه‌های شبکه بدون قطع شدن سرویس به شبکه متصل باقی بمانند.

انواع پروتکل‌های FHRP:

1. HSRP یا (Hot Standby Router Protocol):

- توسعه‌دهنده: سیسکو
- عملکرد : در این پروتکل، یک روتر به عنوان روتر فعال و یک یا چند روتر به عنوان روتر آماده به کار تنظیم می‌شوند. پیام‌های Hello به صورت دوره‌ای برای نظارت بر وضعیت روترها ارسال می‌شود. اگر روتر فعال از کار بیفتد، روتر آماده به کار به سرعت جایگزین آن می‌شود.

2. VRRP یا (Virtual Router Redundancy Protocol) :

- توسعه‌دهنده : IETF (استاندارد باز)
- عملکرد : VRRP مشابه HSRP عمل می‌کند اما به عنوان یک استاندارد باز، سازگار با تجهیزات مختلف از تولیدکنندگان مختلف است. در این پروتکل، یک روتر به عنوان Master و بقیه به عنوان Backup عمل می‌کنند.

3. GLBP یا (Gateway Load Balancing Protocol) :

- توسعه‌دهنده : سیسکو
- عملکرد : علاوه بر افزونگی، GLBP توانایی توزیع بار ترافیک شبکه بین چندین روتر را دارد. در این پروتکل، چندین روتر به عنوان دروازه فعال (Active Gateway) عمل می‌کنند و بار ترافیک را تقسیم می‌کنند.

ویژگی‌های کلیدی FHRP:

- افزونگی (Redundancy) : اطمینان از اینکه همیشه یک روتر فعال برای مدیریت ترافیک وجود دارد.

- پایداری (Stability) : کاهش زمان قطع سرویس در صورت خرابی روتر اصلی.
- آدرس IP مجازی : استفاده از یک آدرس IP مشترک که توسط چندین روتر پشتیبانی می‌شود، بنابراین کاربران و دستگاه‌های شبکه نیازی به تغییر تنظیمات خود ندارند.
- تشخیص و جایگزینی سریع : استفاده از پیام‌های دوره‌ای برای تشخیص خرابی و جایگزینی سریع روترها.

Priority (اولویت) و Preempt (پیش‌دستی):

Priority (اولویت):

- Priority یک عدد عددی است که به هر روتر در گروه FHRP اختصاص داده می‌شود و تعیین می‌کند که کدام روتر باید به عنوان روتر فعال (Active) انتخاب شود.
- مقدار پیش‌فرض Priority معمولاً 100 است، اما می‌توان آن را تغییر داد تا اولویت‌بندی روترها مشخص شود.
- هرچه مقدار Priority بالاتر باشد، احتمال انتخاب آن روتر به عنوان روتر فعال بیشتر است.

Preempt (پیش‌دستی):

- Preempt یک ویژگی است که به روتر اجازه می‌دهد تا در صورتی که Priority بالاتری دارد، روتر فعال فعلی را جایگزین کند.
- اگر ویژگی Preempt در روتر فعال باشد و روتر دیگری با Priority بالاتر وارد گروه شود، روتر جدید می‌تواند جایگزین روتر فعال فعلی شود.
- این ویژگی تضمین می‌کند که همیشه روتر با بالاترین Priority به عنوان روتر فعال عمل کند.

نحوه کار FHRP:

- در شبکه‌های LAN، دستگاه‌ها برای دسترسی به شبکه‌های دیگر معمولاً به یک روتر به عنوان دروازه پیش‌فرض متکی هستند.
- با استفاده از FHRP، چندین روتر می‌توانند به عنوان یک روتر مجازی واحد عمل کنند.
- یک روتر به عنوان روتر فعال انتخاب می‌شود و بقیه به عنوان روترهای آماده به کار در حالت آماده باش قرار می‌گیرند.
- در صورت خرابی روتر فعال، یکی از روترهای آماده به کار به سرعت جایگزین آن می‌شود.

بسته‌های تبادل اطلاعات در FHRP :

در پروتکل‌های FHRP (First Hop Redundancy Protocol)، روترها برای هماهنگی و تبادل اطلاعات از بسته‌های خاصی استفاده می‌کنند. این بسته‌ها به منظور نظارت بر وضعیت روترها، انتخاب روتر فعال و آماده به کار، و مدیریت وضعیت پروتکل استفاده می‌شوند. هر پروتکل FHRP بسته‌های خاص خود را دارد، اما اصول کلی تبادل اطلاعات مشابه هستند. در ادامه، بسته‌های تبادل اطلاعات در HSRP و VRRP را توضیح می‌دهیم.

بسته‌های HSRP یا (Hot Standby Router Protocol):

1. بسته‌های Hello:

- هدف : ارسال پیام‌های Hello به صورت دوره‌ای برای اعلام وضعیت روترها.
- محتوا : شامل اطلاعاتی مانند شناسه گروه، اولویت (Priority)، و وضعیت فعلی روتر (Active یا Standby).
- پورت مقصد : UDP 1985
- آدرس چندپخشی : 224.0.0.2

2. بسته‌های Coup:

- هدف : این پیام‌ها توسط یک روتر آماده به کار ارسال می‌شوند تا اعلام کنند که اکنون به عنوان روتر فعال عمل می‌کنند.
- زمان استفاده : هنگامی که روتر آماده به کار تشخیص می‌دهد که روتر فعال از کار افتاده و باید جایگزین آن شود.

3. بسته‌های Resign:

- هدف : این پیام‌ها توسط روتر فعال ارسال می‌شوند تا اعلام کنند که دیگر نمی‌خواهند روتر فعال باشند.
- زمان استفاده : هنگامی که روتر فعال تشخیص می‌دهد که دیگر نمی‌تواند به عنوان روتر فعال عمل کند و باید جایگزین شود.

بسته‌های VRRP یا (Virtual Router Redundancy Protocol):

1. بسته‌های Advertisement:

- هدف : ارسال پیام‌های Advertisement به صورت دوره‌ای برای اعلام وضعیت روترها.
- محتوا : شامل اطلاعاتی مانند شناسه گروه، اولویت (Priority)، و وضعیت فعلی روتر (Master یا Backup).
- پورت مقصد : UDP 112
- آدرس چندپخشی : 224.0.0.18

عملکرد بسته‌ها در FHRP:

1. نظارت بر وضعیت روترها :

- بسته‌های Hello (در HSRP) و Advertisement (در VRRP) به صورت دوره‌ای ارسال می‌شوند تا روترها از وضعیت یکدیگر مطلع باشند.
- این بسته‌ها شامل اطلاعاتی نظیر شناسه گروه، اولویت و وضعیت فعلی روتر می‌باشند.

2. انتخاب و جایگزینی روترها :

- روترها با استفاده از این بسته‌ها اولویت‌های یکدیگر را مقایسه می‌کنند.
- روتر با بالاترین اولویت به عنوان روتر فعال (در HSRP) یا Master (در VRRP) انتخاب می‌شود.
- در صورت خرابی روتر فعال، روتر آماده به کار یا Backup با ارسال بسته‌های Coup (در HSRP) یا ادامه ارسال بسته‌های Advertisement (در VRRP) به عنوان روتر فعال جدید عمل می‌کند.

3. اعلام تغییر وضعیت :

- بسته‌های Resign (در HSRP) برای اعلام اینکه یک روتر دیگر نمی‌خواهد یا نمی‌تواند به عنوان روتر فعال عمل کند، ارسال می‌شوند.
- این اعلام باعث می‌شود تا روترهای دیگر در گروه آماده شوند تا جایگزینی صورت گیرد.

مثال‌های پیکربندی در سیسکو:

مثال 1: پیکربندی HSRP در سیسکو

```
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# standby 1 ip 192.168.1.1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-string mykey
```

- standby 1 ip 192.168.1.1 : تنظیم آدرس IP مجازی برای گروه HSRP.
- standby 1 priority 110 : تنظیم Priority به 110، که این روتر را به عنوان روتر فعال انتخاب می‌کند اگر Priority بالاتری نسبت به سایر روترها داشته باشد.
- standby 1 preempt : فعال کردن ویژگی Preempt برای اینکه این روتر بتواند جایگزین روتر فعال فعلی شود اگر Priority بالاتری داشته باشد.
- standby 1 authentication md5 key-string mykey : تنظیم احراز هویت برای امنیت بیشتر.

مثال 2: پیکربندی VRRP در سیسکو

```
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# vrrp 1 ip 192.168.1.1
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 preempt
```

- vrrp 1 ip 192.168.1.1 : تنظیم آدرس IP مجازی برای گروه VRRP.

- vrrp 1 priority 110 : تنظیم Priority به 110، که این روتر را به عنوان روتر Master انتخاب می‌کند اگر Priority بالاتری نسبت به سایر روترها داشته باشد.
- vrrp 1 preempt : فعال کردن ویژگی Preempt برای اینکه این روتر بتواند جایگزین روتر Master فعلی شود اگر Priority بالاتری داشته باشد.

این مثال‌ها نشان می‌دهند که چگونه می‌توانید Priority و Preempt را در روترهای سیسکو برای پیکربندی پروتکل‌های HSRP و VRRP تنظیم کنید تا از دسترسی‌پذیری و پایداری بالاتری در شبکه‌های خود برخوردار شوید.

Chapter-25
DHCP

مقدمه:

پروتکل DHCP یا (Dynamic Host Configuration Protocol) برای مدیریت و تخصیص خودکار آدرس‌های IP و سایر اطلاعات پیکربندی شبکه به دستگاه‌های شبکه طراحی شده است. با استفاده از DHCP، مدیران شبکه می‌توانند به صورت پویا و خودکار آدرس‌های IP را به دستگاه‌ها تخصیص دهند، بدون نیاز به پیکربندی دستی هر دستگاه.

اجزای DHCP:

1. DHCP Server : سرور DHCP وظیفه دارد آدرس‌های IP و سایر اطلاعات پیکربندی شبکه را به دستگاه‌های کلاینت اختصاص دهد.
2. DHCP Client : دستگاه‌هایی که نیاز به دریافت آدرس IP و اطلاعات پیکربندی دارند.
3. DHCP Relay Agent : اگر کلاینت‌ها و سرور DHCP در شبکه‌های مختلف قرار داشته باشند، DHCP Relay Agent پیام‌های DHCP را بین کلاینت و سرور ارسال می‌کند.

فرایند DHCP:

1. DHCP Discover : کلاینت DHCP یک پیام DHCP Discover به صورت پخش (broadcast) به شبکه ارسال می‌کند تا سرورهای DHCP موجود را شناسایی کند.
2. DHCP Offer : سرور DHCP پس از دریافت پیام DHCP Discover، یک پیام DHCP Offer به کلاینت ارسال می‌کند که شامل یک آدرس IP پیشنهادی و سایر اطلاعات پیکربندی است.
3. DHCP Request : کلاینت پس از دریافت پیام‌های DHCP Offer از سرورهای مختلف، یک پیام DHCP Request به سرور انتخابی ارسال می‌کند تا آدرس IP پیشنهادی را درخواست کند.
4. DHCP Acknowledgment : سرور DHCP پس از دریافت پیام DHCP Request، یک پیام DHCP Acknowledgment به کلاینت ارسال می‌کند که تأیید می‌کند آدرس IP به کلاینت اختصاص داده شده است و شامل سایر اطلاعات پیکربندی می‌باشد.

پیکربندی DHCP در سیسکو:

1. پیکربندی یک DHCP Server:

```
Router(config)# ip dhcp pool MYPOOL
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
Router(dhcp-config)# domain-name example.com
Router(dhcp-config)# lease 7
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

- ip dhcp pool MYPOOL : ایجاد یک pool DHCP با نام MYPOOL.
- network 192.168.1.0 255.255.255.0 : مشخص کردن شبکه و ماسک زیر شبکه برای pool.
- default-router 192.168.1.1 : تنظیم آدرس IP روتر به عنوان دروازه پیش‌فرض.
- dns-server 8.8.8.8 8.8.4.4 : تنظیم سرورهای DNS.
- domain-name example.com : تنظیم نام دامنه.
- lease 7 : تنظیم مدت زمان اجاره آدرس IP به 7 روز.
- ip dhcp excluded-address 192.168.1.1 192.168.1.10 : آدرس‌های IP از 192.168.1.1 تا 192.168.1.10 را از pool DHCP مستثنی می‌کند.

سایر دستورات DHCP در سیسکو:

بررسی وضعیت DHCP Server:

برای مشاهده وضعیت فعلی DHCP Server و اطلاعات مربوط به اجاره‌های IP:

```
Router# show ip dhcp binding
```

بررسی پیام‌های DHCP:

برای مشاهده پیام‌های DHCP که توسط روتر دریافت و ارسال شده‌اند:

```
Router# debug ip dhcp server events
```

پاکسازی اجاره‌های IP:

برای پاک کردن همه اجاره‌های DHCP:

```
Router# clear ip dhcp binding
```

DHCP Relay Agent:

مقدمه:

در یک شبکه کوچک، کلاینت‌ها و سرور DHCP معمولاً در یک شبکه محلی (LAN) قرار دارند و پیام‌های DHCP به صورت پخش (broadcast) در همان شبکه محلی ارسال می‌شوند. با این حال، در شبکه‌های بزرگتر و پیچیده‌تر، ممکن است کلاینت‌ها و سرور DHCP در شبکه‌های مختلف (subnet) قرار داشته باشند. در چنین مواردی، پیام‌های broadcast نمی‌توانند از یک شبکه به شبکه دیگر عبور کنند. برای حل این مشکل، از DHCP Relay Agent استفاده می‌شود.

DHCP Relay Agent چیست؟

DHCP Relay Agent یک دستگاه شبکه (معمولاً روتر یا سوئیچ لایه 3) است که پیام‌های DHCP را از کلاینت‌ها دریافت کرده و به سرور DHCP در شبکه دیگری ارسال می‌کند. همچنین پاسخ‌های سرور DHCP را به کلاینت‌ها برمی‌گرداند.

عملکرد DHCP Relay Agent:

1. دریافت پیام DHCP Discover: کلاینت DHCP یک پیام DHCP Discover به صورت broadcast در شبکه محلی خود ارسال می‌کند.
2. انتقال پیام به سرور DHCP Relay Agent: DHCP این پیام را دریافت کرده و آن را به صورت unicast به سرور DHCP در شبکه دیگری ارسال می‌کند. برای این کار، آدرس IP سرور DHCP باید از قبل در DHCP Relay Agent تنظیم شده باشد.
3. دریافت پاسخ از سرور DHCP: سرور DHCP پس از دریافت پیام، یک پیام DHCP Offer به DHCP Relay Agent ارسال می‌کند.
4. بازگشت پیام به کلاینت: DHCP Relay Agent این پیام را به صورت broadcast به شبکه محلی کلاینت ارسال می‌کند تا کلاینت بتواند آن را دریافت کند.
5. تکرار فرآیند برای پیام‌های بعدی: این فرآیند برای پیام‌های DHCP Request و DHCP Acknowledgment نیز تکرار می‌شود.

کجا از DHCP Relay Agent استفاده کنیم؟

- شبکه‌های بزرگ : در سازمان‌ها و شرکت‌های بزرگ که شبکه‌های مختلفی دارند و نیاز به مدیریت مرکزی DHCP دارند.
- شبکه‌های WAN : در شبکه‌های گسترده (Wide Area Networks) که کلاینت‌ها و سرور DHCP در مکان‌های جغرافیایی مختلف قرار دارند.
- شبکه‌های جداگانه : در مواردی که شبکه‌های مختلف نیاز به ارتباط با یک سرور DHCP واحد دارند.

پیکربندی DHCP Relay Agent در سیسکو:

1. پیکربندی DHCP Relay Agent در یک روتر سیسکو:

```
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# ip helper-address 192.168.1.100
```

- ip helper-address 192.168.1.100 : این دستور آدرس IP سرور DHCP را مشخص می‌کند که پیام‌های DHCP به آن ارسال می‌شوند.

2. پیکربندی DHCP Relay Agent در یک سوئیچ سیسکو:

```
Switch(config)# interface Vlan10
Switch(config-if)# ip address 192.168.3.1 255.255.255.0
Switch(config-if)# ip helper-address 192.168.1.100
```

سایر تنظیمات و ملاحظات:

تنظیمات پیشرفته DHCP Relay Agent:

- پیکربندی چندین سرور DHCP : در صورتی که بیش از یک سرور DHCP وجود داشته باشد، می‌توانید چندین آدرس IP را با استفاده از چندین دستور ip helper-address مشخص کنید.

```
Router(config-if)# ip helper-address 192.168.1.100
Router(config-if)# ip helper-address 192.168.1.101
```

- تنظیمات تبدیل DHCP به BOOTP : برخی دستگاه‌ها از پروتکل قدیمی BOOTP استفاده می‌کنند. با استفاده از دستورات زیر می‌توانید تبدیل پیام‌های DHCP به BOOTP را پیکربندی کنید:

```
Router(config-if)# ip forward-protocol udp bootps
```

- تنظیم فیلترهای امنیتی : برای افزایش امنیت، می‌توانید دسترسی به DHCP Relay Agent را محدود کنید تا فقط پیام‌های DHCP از شبکه‌های خاصی را قبول کند.

بررسی و عیب‌یابی DHCP Relay Agent:

بررسی وضعیت DHCP Relay Agent:

برای مشاهده وضعیت DHCP Relay Agent و آدرس‌های سرور DHCP پیکربندی شده، از دستور زیر استفاده کنید:

```
Router# show ip interface GigabitEthernet0/1
```

بررسی پیام‌های DHCP:

برای مشاهده پیام‌های DHCP که توسط روتر دریافت و ارسال شده‌اند، از دستور زیر استفاده کنید:

```
Router# debug ip dhcp server packet
```

نکات مهم:

- زمان اجاره (Lease Time) : مدت زمانی که یک آدرس IP به یک کلاینت اختصاص داده می‌شود. پس از پایان زمان اجاره، کلاینت باید آدرس IP خود را تمدید کند یا آدرس جدیدی درخواست کند.
- آدرس‌های مستثنی شده (Excluded Addresses) : آدرس‌هایی که نباید توسط DHCP Server به کلاینت‌ها اختصاص داده شوند. این آدرس‌ها معمولاً برای دستگاه‌های شبکه‌ای مهم مانند روترها، سوئیچ‌ها و سرورها رزرو می‌شوند.
- پیکربندی صحیح آدرس‌های سرور DHCP : اطمینان حاصل کنید که آدرس‌های سرور DHCP به درستی در DHCP Relay Agent تنظیم شده باشند.
- محدودیت‌های پخش (Broadcast) : توجه داشته باشید که پیام‌های DHCP به صورت broadcast ارسال می‌شوند و ممکن است در برخی از شبکه‌ها محدودیت‌هایی برای ترافیک broadcast وجود داشته باشد.
- امنیت : از فیلترها و ACL ها برای محدود کردن دسترسی به DHCP Relay Agent استفاده کنید تا از سوءاستفاده و حملات احتمالی جلوگیری شود.

مقدمه DHCP Spoofing، DHCP Snooping و ARP Poisoning :

امنیت شبکه یکی از مهم‌ترین جنبه‌های مدیریت شبکه است. تهدیدهای مختلفی مانند DHCP Snooping، DHCP Spoofing، و ARP Poisoning می‌توانند عملکرد شبکه را به خطر بیندازند و باعث نشت اطلاعات یا دسترسی غیرمجاز شوند. در این مقاله، به توضیح این تهدیدها و راهکارهای مقابله با آنها در سیسکو می‌پردازیم.

DHCP Snooping

تعریف:

DHCP Snooping یک ویژگی امنیتی لایه 2 است که برای جلوگیری از حملات مخرب DHCP مانند DHCP Spoofing استفاده می‌شود. این ویژگی ترافیک DHCP را نظارت و فیلتر می‌کند تا فقط ترافیک معتبر DHCP به کلاینت‌ها برسد.

عملکرد:

- تعیین پورت‌های معتبر و نامعتبر: پورت‌های سوئیچ به عنوان "معتبر" یا "نامعتبر" علامت‌گذاری می‌شوند. فقط ترافیک DHCP از پورت‌های معتبر پذیرفته می‌شود.
- نگهداری پایگاه داده: سوئیچ پایگاه داده‌ای از آدرس‌های MAC و IP کلاینت‌های DHCP نگهداری می‌کند.

راهکارهای مقابله:

1. فعال‌سازی DHCP Snooping:

- DHCP Snooping را بر روی سوئیچ‌های خود فعال کنید تا ترافیک DHCP معتبر را از ترافیک مخرب جدا کند.

2. پیکربندی پورت‌های معتبر و نامعتبر:

- پورت‌های متصل به سرور DHCP را به عنوان پورت معتبر و پورت‌های متصل به کلاینت‌ها را به عنوان پورت نامعتبر پیکربندی کنید.

پیکربندی در سیسکو:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
```

```
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# exit
Switch(config)# interface range GigabitEthernet0/2 - 24
Switch(config-if-range)# ip dhcp snooping limit rate 10
Switch(config-if-range)# exit
```

- ip dhcp snooping: فعال‌سازی DHCP Snooping.
- ip dhcp snooping vlan 10: فعال‌سازی DHCP Snooping بر روی VLAN 10.
- ip dhcp snooping trust: تنظیم پورت به عنوان پورت معتبر.
- ip dhcp snooping limit rate 10: محدود کردن نرخ ترافیک DHCP بر روی پورت‌های نامعتبر.

DHCP Spoofing

تعریف:

DHCP Spoofing حمله‌ای است که در آن یک مهاجم خود را به عنوان سرور DHCP معرفی می‌کند و آدرس‌های IP نادرست به کلاینت‌ها ارائه می‌دهد. این حمله می‌تواند منجر به مسیریابی نادرست ترافیک شبکه و دسترسی غیرمجاز به اطلاعات شود.

راهکارهای مقابله:

1. استفاده از DHCP Snooping:

- DHCP Snooping را فعال کنید تا فقط سرورهای DHCP معتبر بتوانند به کلاینت‌ها پاسخ دهند.

2. پیکربندی ACLها (Access Control Lists):

- از ACLها برای محدود کردن دسترسی به سرورهای DHCP معتبر استفاده کنید.

ARP Poisoning

تعریف:

ARP Poisoning حمله‌ای است که در آن یک مهاجم پیام‌های ARP جعلی به شبکه ارسال می‌کند تا جداول ARP دستگاه‌های شبکه را تغییر دهد. این حمله می‌تواند منجر به حملات مرد میانی (Man-in-the-Middle) و دزدیدن اطلاعات حساس شود.

راهکارهای مقابله:

1. استفاده از Dynamic ARP Inspection یا (DAI):

- DAI پیام‌های ARP را بررسی می‌کند و تنها پیام‌های معتبر را می‌پذیرد.

2. پیاده‌سازی Static ARP Entries:

- آدرس‌های MAC و IP دستگاه‌های حیاتی را به صورت دستی در جداول ARP تنظیم کنید.

پیکربندی در سیسکو:

فعال‌سازی Dynamic ARP Inspection:

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# ip arp inspection trust
Switch(config-if)# exit
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping
```

- ip arp inspection vlan 10: فعال‌سازی DAI بر روی VLAN 10.
- ip arp inspection trust: تنظیم پورت به عنوان پورت معتبر.

پیکربندی Static ARP Entries:

```
Router(config)# arp 192.168.1.1 00a0.c9f0.1234 ARPA
```

- arp 192.168.1.1 00a0.c9f0.1234 ARPA: اضافه کردن یک ورودی ثابت در جدول ARP.

Chapter-26
Gre Tunnel

مقدمه:

پروتکل GRE یا (Generic Routing Encapsulation) یک پروتکل تونل‌سازی است که توسط سیسکو توسعه یافته است. GRE برای ایجاد تونل‌های مجازی بین دو نقطه در شبکه استفاده می‌شود و

این امکان را فراهم می‌کند که بسته‌های مختلف لایه 3 در یک بسته GRE کپسوله شوند و از طریق یک شبکه واسطه عبور کنند.

ویژگی‌های GRE:

1. تونل‌سازی (Tunneling): پروتکل GRE امکان ایجاد تونل‌های مجازی را فراهم می‌کند که می‌توانند ترافیک لایه 3 را از طریق یک شبکه IP منتقل کنند.
2. کپسوله‌سازی (Encapsulation): پروتکل GRE می‌تواند پروتکل‌های مختلف لایه 3 را در یک بسته GRE کپسوله کند. این بسته‌ها سپس در بسته‌های IP قرار می‌گیرند تا از طریق شبکه واسطه منتقل شوند.
3. پشتیبانی از پروتکل‌های چندگانه (Multi-Protocol Support): پروتکل GRE می‌تواند ترافیک پروتکل‌های مختلف مانند IPX، IPv6، IPv4 و AppleTalk را کپسوله کند.
4. ساده و سبک (Simple and Lightweight): پروتکل GRE یک پروتکل سبک و ساده است که با کمترین سربار اضافی کار می‌کند.

ساختار بسته GRE:

بسته GRE شامل بخش‌های زیر است:

- IP Header خارجی (Outer IP Header): حاوی آدرس‌های مبدا و مقصد IP شبکه واسطه است.
- GRE Header: حاوی اطلاعات کپسوله‌سازی و نوع پروتکل کپسوله شده است.
- بسته اصلی (Payload): شامل بسته پروتکل لایه 3 اصلی است که باید از طریق تونل منتقل شود.

GRE Header:

GRE Header اطلاعات لازم برای کپسوله‌سازی و دکپسوله‌سازی بسته‌ها را فراهم می‌کند. GRE Header شامل فیلدهای زیر است:

1. Flags: شامل اطلاعاتی در مورد قابلیت‌های اختیاری GRE مانند کلید گذاری و checksum.
2. Version: نسخه پروتکل GRE.
3. Protocol Type: نوع پروتکلی که در بسته اصلی کپسوله شده است (مثلاً IPv4 یا IPv6).

فرآیند کپسوله‌سازی (Encapsulation) و دکپسوله‌سازی (Decapsulation) در GRE:

کپسوله‌سازی (Encapsulation):

1. دریافت بسته اصلی: روتر مبدا یک بسته لایه 3 را که باید از طریق تونل GRE ارسال شود، دریافت می‌کند.
2. اضافه کردن GRE Header: روتر GRE Header را به بسته اصلی اضافه می‌کند. این Header شامل اطلاعاتی مانند نوع پروتکل کپسوله شده و قابلیت‌های GRE است.
3. اضافه کردن IP Header خارجی: سپس IP Header خارجی به بسته اضافه می‌شود. این Header شامل آدرس‌های IP مبدا و مقصد تونل (روترهای مبدا و مقصد تونل GRE) است.
4. ارسال بسته: بسته کپسوله شده از طریق شبکه واسطه به سمت روتر مقصد ارسال می‌شود.

دکپسوله‌سازی (Decapsulation):

1. دریافت بسته کپسوله شده: روتر مقصد بسته کپسوله شده را دریافت می‌کند.
2. حذف IP Header خارجی: روتر IP Header خارجی را حذف می‌کند تا به GRE Header برسد.
3. حذف GRE Header: سپس GRE Header را حذف می‌کند تا به بسته اصلی دست یابد.
4. ارسال بسته اصلی: بسته اصلی (که اکنون بدون کپسوله‌سازی GRE است) به مقصد نهایی خود در شبکه محلی روتر مقصد ارسال می‌شود.

کاربردهای GRE:

1. اتصال شبکه‌های مختلف (Connecting Different Networks): GRE می‌تواند برای اتصال دو شبکه محلی (LAN) از طریق یک شبکه واسطه مانند اینترنت استفاده شود.
2. پشتیبانی از پروتکل‌های غیر-IP (Non-IP Protocol Support): GRE امکان انتقال ترافیک پروتکل‌های غیر-IP را از طریق شبکه‌های IP فراهم می‌کند.
3. VPN: GRE به عنوان بخشی از راهکارهای VPN استفاده می‌شود، به خصوص در ترکیب با پروتکل‌های امنیتی مانند IPsec.

پیکربندی GRE Tunnel در سیسکو:

مراحل پیکربندی:

1. ایجاد اینترفیس تونل (Create Tunnel Interface):

- یک اینترفیس تونل جدید ایجاد کنید و آدرس IP را برای آن تنظیم کنید.

2. تنظیم مبدا و مقصد تونل (Set Tunnel Source and Destination):

- آدرس‌های IP مبدا و مقصد برای تونل را تنظیم کنید.

3. فعال‌سازی تونل (Activate Tunnel):

- تنظیمات اضافی مانند ماسک زیر شبکه و پروتکل‌های مسیریابی را انجام دهید.

مثال پیکربندی:

در این مثال، یک تونل GRE بین دو روتر (Router1 و Router2) پیکربندی می‌شود. آدرس‌های IP واسطه 192.0.2.1 و 192.0.2.2 هستند، و آدرس‌های IP تونل 10.0.0.1 و 10.0.0.2 هستند.

پیکربندی در Router1:

```
Router1(config)# interface Tunnel0
Router1(config-if)# ip address 10.0.0.1 255.255.255.252
Router1(config-if)# tunnel source 192.0.2.1
Router1(config-if)# tunnel destination 192.0.2.2
Router1(config-if)# tunnel mode gre ip
```

پیکربندی در Router2:

```
Router2(config)# interface Tunnel0
Router2(config-if)# ip address 10.0.0.2 255.255.255.252
Router2(config-if)# tunnel source 192.0.2.2
Router2(config-if)# tunnel destination 192.0.2.1
Router2(config-if)# tunnel mode gre ip
```

بررسی و عیب‌یابی GRE Tunnel:

بررسی وضعیت تونل (Check Tunnel Status):

برای مشاهده وضعیت تونل GRE و اطمینان از اینکه تونل فعال است، از دستور زیر استفاده کنید:

```
Router# show interfaces Tunnel0
```

بررسی مسیرها (Check Routes):

برای بررسی جدول مسیریابی و اطمینان از اینکه مسیرهای صحیح برای تونل پیکربندی شده‌اند، از دستور زیر استفاده کنید:

```
Router# show ip route
```

بررسی بسته‌های GRE یا (Check GRE Packets):

برای مشاهده بسته‌های GRE که توسط روتر دریافت و ارسال شده‌اند، از دستور زیر استفاده کنید:

```
Router# debug tunnel
```

نکات مهم:

1. پیکربندی صحیح آدرس‌های IP یا (Correct IP Address Configuration): اطمینان حاصل کنید که آدرس‌های IP مبدا و مقصد به درستی تنظیم شده‌اند.
2. مسیرهای صحیح (Correct Routing Paths): بررسی کنید که مسیرهای مسیریابی به درستی پیکربندی شده‌اند تا بسته‌ها بتوانند از طریق تونل عبور کنند.
3. امنیت (Security): پروتکل GRE به تنهایی رمزنگاری ندارد. برای افزایش امنیت، می‌توانید از IPsec در کنار GRE استفاده کنید تا داده‌ها رمزنگاری شوند.

ترکیب GRE و IPsec:

برای افزایش امنیت تونل GRE، می‌توانید IPsec را برای رمزنگاری ترافیک استفاده کنید. در زیر یک مثال ترکیب GRE و IPsec آورده شده است:

پیکربندی IPsec برای GRE Tunnel:

پیکربندی در Router1:

```
Router1(config)# crypto isakmp policy 1
Router1(config-isakmp)# encryption aes
Router1(config-isakmp)# hash sha256
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 2
Router1(config-isakmp)# lifetime 86400
```

```
Router1(config-isakmp)# exit
Router1(config)# crypto isakmp key MY_SHARED_KEY address 192.0.2.2

Router1(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-aes
esp-sha-hmac
Router1(config)# crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
Router1(config-crypto-map)# set peer 192.0.2.2
Router1(config-crypto-map)# set transform-set MY_TRANSFORM_SET
Router1(config-crypto-map)# match address 101
Router1(config-crypto-map)# exit

Router1(config)# access-list 101 permit gre host 192.0.2.1 host 192.0.2.2
Router1(config)# interface Tunnel0
Router1(config-if)# tunnel protection ipsec profile MY_IPSEC_PROFILE
```

پیکربندی در Router2:

```
Router2(config)# crypto isakmp policy 1
Router2(config-isakmp)# encryption aes
Router2(config-isakmp)# hash sha256
Router2(config-isakmp)# authentication pre-share
Router2(config-isakmp)# group 2
Router2(config-isakmp)# lifetime 86400
Router2(config-isakmp)# exit
Router2(config)# crypto isakmp key MY_SHARED_KEY address 192.0.2.1
```

Router2(config)# crypto ipsec transform-set MY_TRANSFORM_SET esp-aes esp-sha-hmac

Router2(config)# crypto map MY_CRYPTO_MAP

10 ipsec-isakmp

Router2(config-crypto-map)# set peer 192.0.2.1

Router2(config-crypto-map)# set transform-set MY_TRANSFORM_SET

Router2(config-crypto-map)# match address 101

Router2(config-crypto-map)# exit

Router2(config)# access-list 101 permit gre host 192.0.2.2 host 192.0.2.1

Router2(config)# interface Tunnel0

Router2(config-if)# tunnel protection ipsec profile MY_IPSEC_PROFILE

Chapter-27
QOS

مقدمه:

QoS یا (Quality of Service) به مجموعه‌ای از فناوری‌ها و تکنیک‌ها گفته می‌شود که برای مدیریت و بهینه‌سازی عملکرد شبکه در زمینه ترافیک شبکه استفاده می‌شوند. QoS تضمین می‌کند که ترافیک حیاتی و حساس به تأخیر مانند صدا (VoIP) و ویدئو، پهنای باند و اولویت مناسب را دریافت کند.

1. طبقه‌بندی و علامت‌گذاری (Classification and Marking):

- طبقه‌بندی (Classification): فرآیند شناسایی و جداسازی انواع مختلف ترافیک شبکه.
- علامت‌گذاری (Marking): فرآیند اضافه کردن برچسب‌ها به بسته‌های داده برای مشخص کردن اولویت و نوع ترافیک.
- DSCP یا (Differentiated Services Code Point) و CoS یا (Class of Service): استانداردهای مورد استفاده برای علامت‌گذاری ترافیک.

2. مدیریت ازدحام (Congestion Management):

- Queuing: فرآیند قرار دادن بسته‌های داده در صف‌ها برای مدیریت ترافیک.
- FIFO یا (First In, First Out): ساده‌ترین نوع صف‌بندی که بسته‌ها به ترتیب ورود پردازش می‌شوند.
- PQ یا (Priority Queuing): صف‌بندی اولویتی که ترافیک با اولویت بالا ابتدا پردازش می‌شود.
- CQ یا (Custom Queuing): صف‌بندی سفارشی که ترافیک بر اساس تنظیمات سفارشی پردازش می‌شود.
- WFQ یا (Weighted Fair Queuing): صف‌بندی عادلانه وزنی که پهنای باند به صورت نسبی بر اساس وزن ترافیک تخصیص می‌یابد.

3. جلوگیری از ازدحام (Congestion Avoidance):

- RED یا (Random Early Detection): مکانیزمی که بسته‌ها را به صورت تصادفی حذف می‌کند تا ازدحام کاهش یابد.
- WRED یا (Weighted Random Early Detection): نسخه بهبود یافته RED که وزن‌های متفاوتی برای انواع مختلف ترافیک اعمال می‌کند.

4. کنترل پهنای باند (Policing and Shaping):

- Policing: مکانیزمی که سرعت ترافیک ورودی را محدود می‌کند و بسته‌های اضافی را حذف یا تغییر می‌دهد.
- Shaping: مکانیزمی که سرعت ترافیک خروجی را تنظیم می‌کند و بسته‌های اضافی را در صف قرار می‌دهد تا به تدریج ارسال شوند.

پیکربندی QoS در سیسکو:

1. طبقه‌بندی و علامت‌گذاری با استفاده از ACL و MQC:

```
Router(config)# access-list 101 permit ip any any
Router(config)# class-map match-any MY_CLASS_MAP
Router(config-cmap)# match access-group 101
Router(config)# policy-map MY_POLICY_MAP
Router(config-pmap)# class MY_CLASS_MAP
Router(config-pmap-c)# set dscp af41
Router(config)# interface GigabitEthernet0/0
Router(config-if)# service-policy output MY_POLICY_MAP
```

- access-list 101 permit ip any any: ایجاد یک ACL که تمامی ترافیک را شناسایی می‌کند.
- class-map match-any MY_CLASS_MAP: ایجاد یک class-map برای مطابقت با ترافیک مشخص شده.
- policy-map MY_POLICY_MAP: ایجاد یک policy-map و اعمال class-map به آن.
- set dscp af41: تنظیم DSCP برای ترافیک مطابقت یافته.
- service-policy output MY_POLICY_MAP: اعمال policy-map به اینترفیس خروجی.

2. مدیریت ازدحام با استفاده از WFQ:

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# fair-queue
```

- fair-queue: فعال‌سازی WFQ بر روی اینترفیس.

3. جلوگیری از ازدحام با استفاده از WRED:

```
Router(config)# policy-map MY_POLICY_MAP
Router(config-pmap)# class MY_CLASS_MAP
Router(config-pmap-c)# random-detect dscp-based
```

- random-detect dscp-based: فعال‌سازی WRED بر اساس DSCP.

4. کنترل پهنای باند با استفاده از Policing و Shaping:

```
Router(config)# policy-map MY_POLICY_MAP
Router(config-pmap)# class MY_CLASS_MAP
Router(config-pmap-c)# police 1000000 conform-action transmit exceed-action drop
```

- police 1000000 conform-action transmit exceed-action drop: تنظیم نرخ Policing به 1 مگابیت بر ثانیه و حذف بسته‌های اضافی.

```
Router(config)# policy-map MY_POLICY_MAP
Router(config-pmap)# class MY_CLASS_MAP
Router(config-pmap-c)# shape average 1000000
```

- shape average 1000000: تنظیم نرخ Shaping به 1 مگابیت بر ثانیه.