

# سیسکو به پارسی



## VLAN Trunking Protocol - VTP

نوشته:

شفق زندگی

<http://blog.shafagh.com/persian>

<http://forum.shafagh.com>

سایت سیسکو به پارسی

انجمن سیسکو به پارسی

## آشنایی با VTP

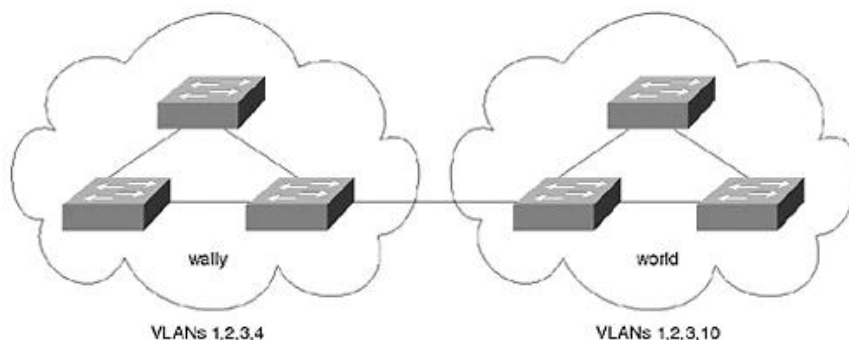
VLAN Trunking Protocol یا VTP برای مدیریت کل VLAN ها بین سویچ های سیسکو استفاده میشود. در یک شبکه بزرگ، مدیریت و ایجاد VLAN ها روی همه سویچ های شبکه کاری دشوار است. پس سیسکو VTP را برای مدیریت افزودن، حذف و نامگذاری VLAN ها ارائه کرده است. VTP برای ساده کردن کار مدیریت VLAN ها توسط سیسکو ارائه شده است.

برای این که ترافیک یک VLAN از سویچ اول به سوم برسد، آن VLAN باید در هر سه سویچ (اول، دوم و سوم) ایجاد شده باشد. توسط VTP این کار به سادگی انجام شده و اطلاعات VLAN ها بین سویچ ها رد و بدل میشود. نظیر: شماره VLAN، اسم VLAN و MTU.

VTP پروتکلی متعلق لایه دو است و روی ترانک بین سویچ های سیسکو بصورت Native یا بدون Tag ارسال میگردد. برای استفاده از VTP بین سویچ ها و ساده کردن ایجاد VLAN روی همه آنها و نهایتاً قرار دادن پورت ها درون VLAN خود، باید سه کار انجام دهیم:

- ساختن VTP Domain – که در برگرفته همه سویچ های تحت یک مدیریت است.
- ساختن و نامگذاری VLAN
- اختصاص پورت به VLAN

بوسیله VTP دو مرحله اول برای سوئیچ ها ساده و در صورت تنظیم روی یکی به بقیه کپی میشود. کفایت در یک سوئیچ این کار را انجام دهیم، بقیه سوئیچ ها نیز خود را با این تنظیمات منطبق میکنند. تنها مرحله اختصاص پورت به VLAN باید بصورت دستی درون هر سویچ انجام شود.



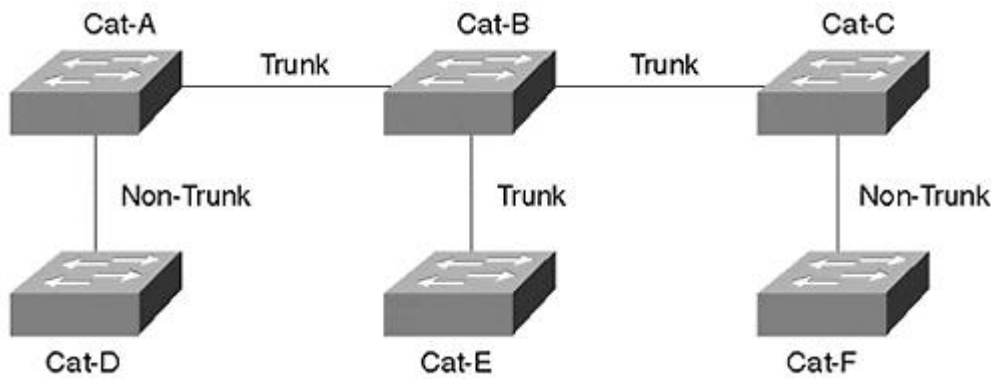
از آنجا که VTP متعلق به سیسکو است، پروتکل استاندارد ارائه شده برای ترانک های IEEE 802.1Q که مشابه VTP عمل میکند، GVRP نام دارد - GARP VLAN Registration Protocol.

GARP و GVRP به ترتیب در استاندارد های IEEE 802.1D و IEEE 802.1Q استاندارد شده اند.

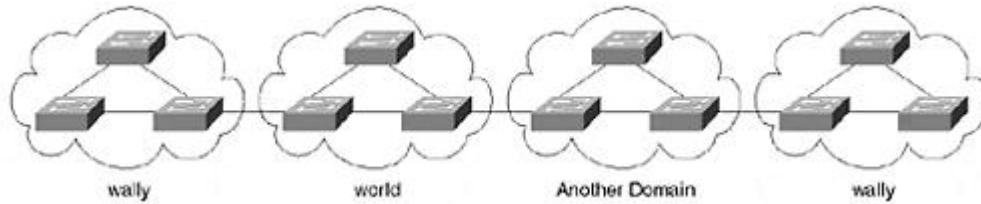


## VTP Domain

VTP محدود به یک VTP Domain است یعنی تا آنجایی پیش میرود که VTP Domain تعریف شده باشد. سوئیچ های یک VTP Domain اطلاعات VLAN مشترکی دارند. پس ناحیه مدیریتی VTP بوسیله VTP Domain مشخص میگردد. یک Domain از یک یا چند سوئیچ تشکیل شده که تحت یک Domain Name کار میکنند. سوئیچ ها در VTP Domain های مختلف با هم هیچ اطلاعاتی را به اشتراک نمیگذارند. وقتی VLAN ی به Domain افزوده شود، سوئیچ های عضو آن Domain بوسیله Advertisement از وجودش مطلع خواهند شد. شکل زیر شکل نمایانگر یک VTP Domain است:



یک LAN ممکن است از چندین VTP Domain مدیریتی مختلف تشکیل شده باشد. در شکل زیر چند VTP Domain با مدیریت مختلف در یک LAN نشان داده شده است:



پیام های VTP به آدرس MAC Multicast 0100:0CCC:CCCC روی ترانکها، درون فریم های VLAN 1 رد و بدل میشوند. برای امنیت اطلاعات VTP، میتوان از VTP Password بین سوئیچ های یک VTP Domain استفاده کرد که بصورت رمزنگاری شده MD5 ذخیره میشود.

## مدهای مختلف VTP

VTP در سه مد در شبکه کار میکند:

- **Server Mode**: هر Domain حداقل به یک VTP Server نیاز دارد تا مدیریت افزودن، حذف و نامگذاری VLAN ها را بعهده گیرد و تغییرات را در شبکه تبلیغ (advertise) کند. هرگونه تغییر در Domain توسط VTP Server به همه سوئیچ های Domain بصورت Multicast اطلاع داده میشود و سوئیچ های عضو Domain اطلاعات VLAN را با سرور (یا سرورها) خود Sync میکنند.

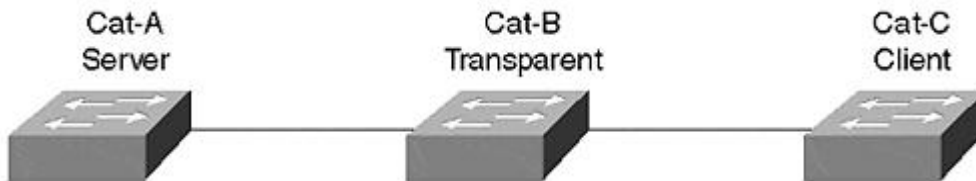
در یک Domain میتوان برای اطمینان و Redundancy چند VTP Server داشت که این سرور ها به هم هیچ اولویتی ندارند بلکه بصورت همعرض، خود را با یکدیگر Sync میکنند. بصورت Default همه سوئیچ ها در مد Server بوده و عضو هیچ VTP Domain ی نیستند. باید توجه داشت که با تنظیم VTP درون یک سوئیچ و ایجاد یک Domain، آن سوئیچ به سوئیچ هایی که عضو هیچ Domain ی نیستند و Domain Name آنها خالی است (NULL است) نام Domain خود را یاد داده و آنها را بصورت اتوماتیک عضو Domain میکند.

لیست کل VLAN ها در حافظه NVRAM سوئیچهای VTP Server ذخیره میشود.

- **Client Mode**: از VTP Server اطلاعات VLAN ها را یاد گرفته و اعمال میکند. در ضمن اطلاعات گرفته شده را به بقیه سوئیچ ها اطلاع (Relay) میدهد. اطلاعات VLAN در حافظه NVRAM ذخیره نخواهد شد و Client مجاز نیست تا VLAN در شبکه ایجاد کرده یا حذف و یا نامگذاری کند.

- **Transparent Mode**: تنها پیام های دریافتی را به بقیه سوئیچ ها (در واقع بقیه پورتهای ترانک) ارسال میکند (Relay) و خودش به آن اطلاعات عمل نمیکند. در VTP نسخه یک، پیام ها تنها وقتی Relay میشدند که مربوط به همان VTP Domain باشند. (که VTP Transparent عضو آن است). اما در VTP V2 پیام های Domain های دیگر نیز Relay میشود.

VTP Transparent اطلاعات VLAN ها را از Server یاد نمیگیرد. این سوئیچ خودش لیست جداگانه ای از VLAN را بصورت Local و در NVRAM خود ذخیره میکند.



اما چند نکته مهم:

- 1- تمام سویچ ها در VTP Domain باید از یک نسخه واحد VTP استفاده کنند.
- 2- VTP v2 با نسخه اولیه سازگار نیست پس تا زمانی که مطمئن نشدید که تمامی سویچ ها توانایی اجرای V2 را دارند، آنرا در هیچ سویچی تنظیم نکنید.
- 3- VTP v2 در سویچ های سیسکو بصورت پیش فرض غیرفعال است و وقتی آنرا فعال کنید بقیه سویچ ها نیز آنرا فعال میکنند و همه V2 با هم صحبت میکنند.
- 4- تنظیم نسخه و Version مورد نظر VTP، تنها در VTP Server و VTP Transparent قابل اجراست.

جدول مقایسه ای VTP Mode:

Feature	Server	Client	Transparent	خصوصیت
Source VTP Messages	Yes	Yes	No	ایجاد پیام
Listen to VTP Messages	Yes	Yes	No	اعمال تغییر
Create VLANs	Yes	No	Yes*	ایجاد VLAN
Remember VLANs	Yes	No	Yes*	ذخیره
*Locally significant only. (تنها درون خود سویچ)				

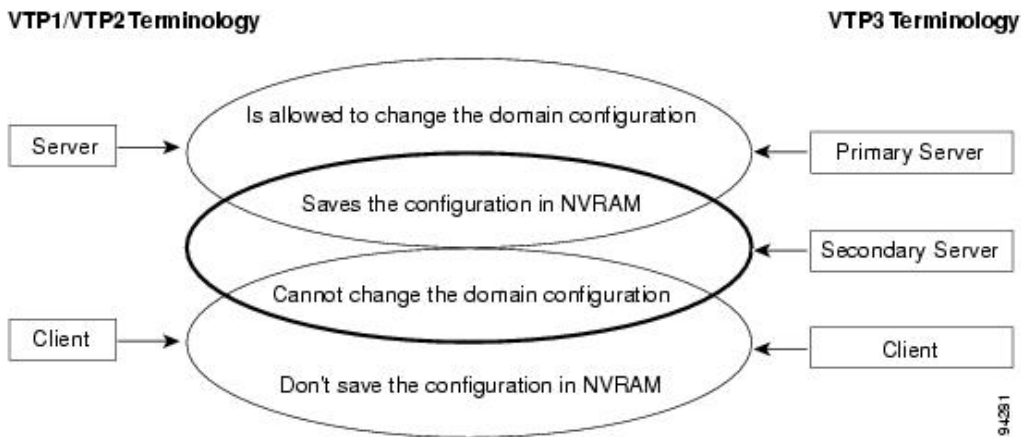
تنظیمات یک سوئیچ بصورت Default و پیش فرض، از قرار زیر است:

- VTP Mode = Server
- VTP Version = 1
- VTP Domain = " " یا NULL یا هیچ
- No Password
- VTP Pruning = Disabled

## VTP Version

VTP در سه نسخه یا Version از طرف سیسکو ارائه شده که آخرین نسخه آن VTP v3 است. مطابق شکل زیر تفاوت های نسخه 1 و 2 با سوم از جمله وجود Primary Server و Secondary Server و قابلیت های Authentication بهتر، مشخص شده است.

درون یک Domain تنها باید یک نسخه واحد از VTP تنظیم گردد.



همانطور که اشاره شد، بوسیله VTP تغییرات در VLAN های 1 تا 1005 را تنها روی یک سوئیچ اعمال میکنیم و بقیه سوئیچ ها از آن مطلع میشوند. (VTP V1 - V2 از VLAN های 1025 تا 4094 پشتیبانی نمیکنند).

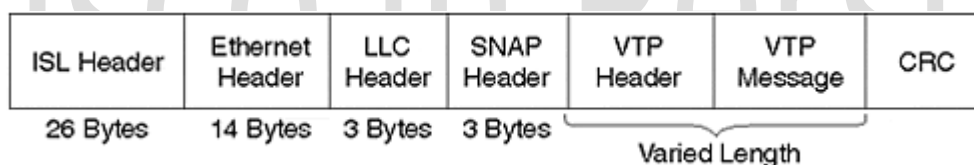
وقتی VTP V2 روی یک سوئیچ فعال گردد بقیه سوئیچ ها در Domain نیز به VTP V2 تبدیل میشوند (در صورتیکه VTP V2 بلد باشند. در حالت Default همه VTP v1 صحبت میکنند).

از خصوصیات VTP V2 به موارد زیر میتوان اشاره کرد:

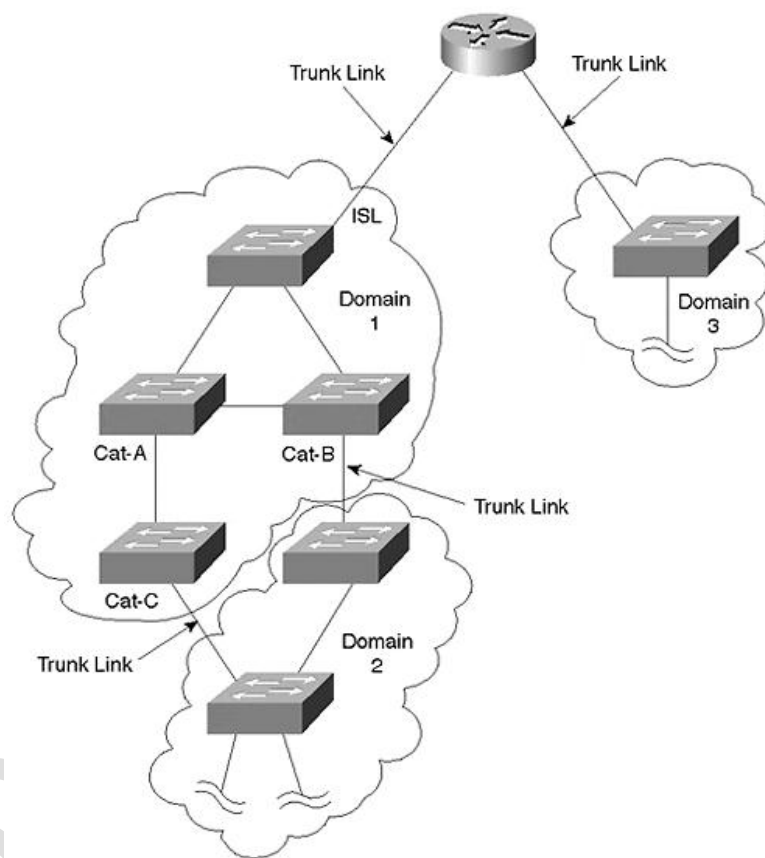
- پیام Domain های دیگر نیز توسط VTP Transparent, Relay میشود. به یاد داریم که در VTP V1 پیام ها تنها وقتی Relay میشدند که مربوط به همان VTP Domain ی باشند که VTP Transparent در آن عضو است.
- سازگاری با شبکه Token Ring.
- تصحیح در خطا و تضمین صحت اطلاعات VLAN ها.
- پشتیبانی و رله کردن پیام های TLV یا Type-Length-Value حتی اگر برای سویچ قابل فهم نباشند، به بقیه ارسال خواهد شد.

## پیام های VTP

پیام های VTP روی Default VLAN منتقل میشوند مثلا برای Ethernet روی VLAN 1 و برای FDDI روی VLAN 1002 و روی ATM روی ELAN (برای این کار باید تنظیم شود). از آنجائیکه Default VLAN قابل حذف نیست، پیامهای VTP همیشه روی Trunk عبور خواهند کرد. در شکل زیر یک VTP Message روی ترانک ISL را می بینیم:



توجه داشته باشید که پیام های VTP تنها روی ترانک ها رد و بدل میگردند که در شکل زیر بعنوان نمونه به آن پرداخته شده است:



Cisco in Persian

چهار نوع Message یا پیام در VTP مبادله میشود:

- Summary advertisements
- Subset advertisements
- Advertisement requests
- VTP join messages

سه پیام اول بین Server و Client در Domain مبادله شده، اما نوع چهارم بصورت معمول غیر فعال است مگر اینکه VTP Pruning فعال گردد که بعداً به آن خواهیم پرداخت.

- **Summary Advertisements**: هر پنج دقیقه Client و Server در شبکه این پیام Summary را ارسال میکنند که گویای آنچه میدانند است. دریافت کننده Revision Number روی پیام را چک میکند و اگر از عدد مطابق با Configuration Revision Number خود بزرگتر بود، به معنی آن است که تغییراتی در VLAN ها پدید آمده و دریافت کننده، درخواست اطلاعات بیشتر (Advertisement Request) خواهد کرد.

Version	Type	Number of Subnet Advertisement Messages	Domain Name Length
Management Domain Name (Padded to 32 Bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 Bytes)			
MD5 Digest (16 Bytes)			

- **Subset Advertisements**: VTP Server ها بعد هر تغییر، بقیه را بوسیله این پیام از تغییرات آگاه میسازند.

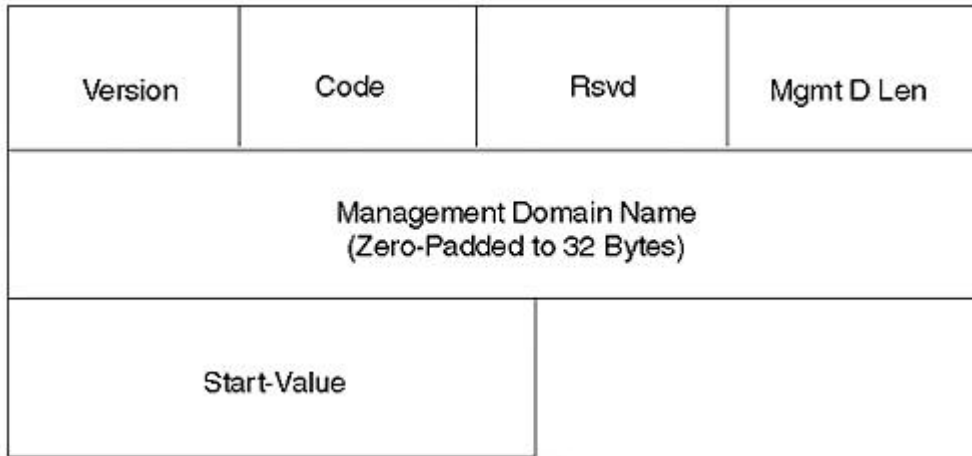
Version	Code	Seq-Number	Domain Name Length
Management Domain Name (Zero-Padded to 32 Bytes)			
Configuration Revision Number			
VLAN-info Field 1			
⋮			
VLAN-info Field N			

The VLAN-info Field Contains Information for Each VLAN and is Formatted as Follows:

Info Length	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 Index			
VLAN-name (Padded with zeros to Multiple of 4 Bytes)			

این تغییر میتواند یکی از موارد زیر باشد:

- ایجاد یا حذف VLAN
  - تغییر نام VLAN
  - فعال کردن یا غیر فعال کردن یک VLAN
  - تغییر MTU یک VLAN
- **Advertisement Requests**: این پیام در زمان درخواست اطلاعات ارسال میگردد. زمان درخواست اطلاعات، میتواند وقتی باشد که Client تازه بالا آمده یا به عضویت Domain درآمده باشد یا زمانی که یک Summary Advertisement با شماره Configuration Revision بالاتر دریافت شود.



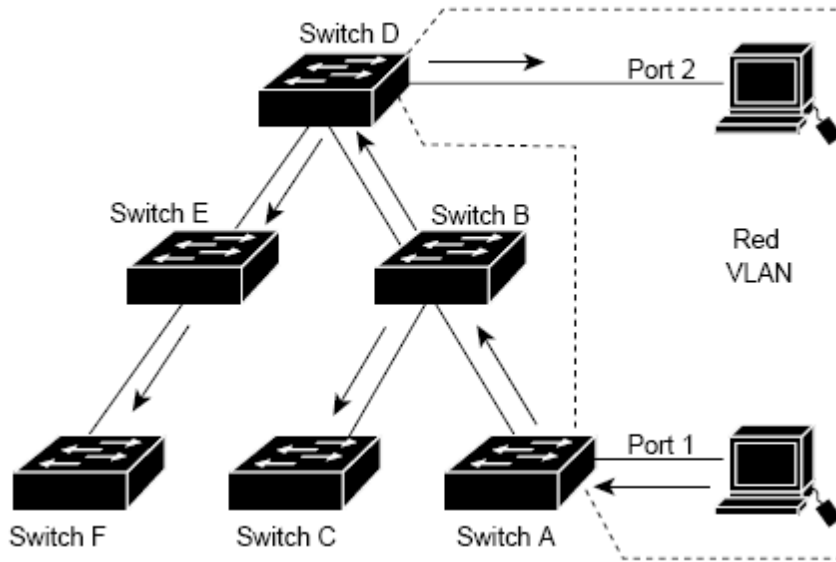
اما در پیام های VTP چه اطلاعاتی در مورد VLAN ها گزارش میشود؟

- VLAN IDs (ISL and 802.1Q)
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

## VTP Pruning

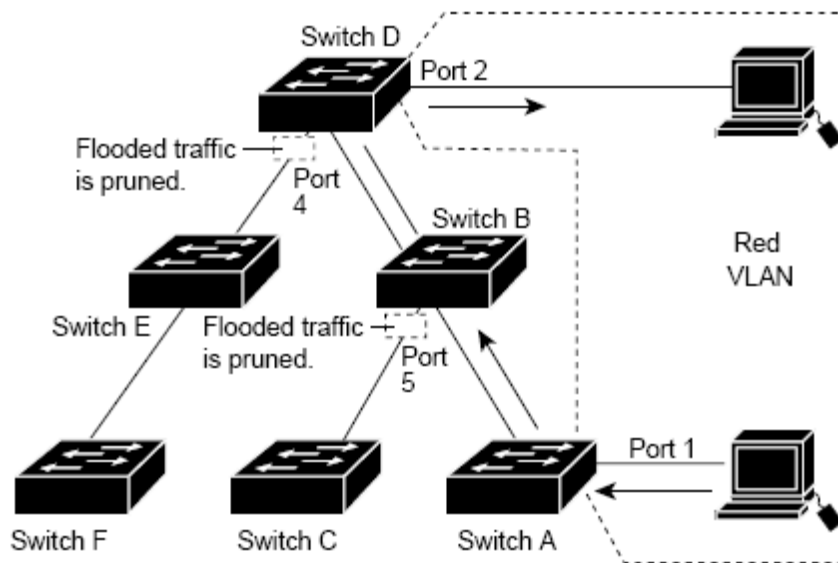
از آنجاییکه با VTP تمامی VLAN ها درون همه سوئیچ ها ایجاد میگردد، روی Trunk ها ترافیک Broadcast تمامی VLAN ها به سمت همه سوئیچ های عضو VTP سرازیر میشود. یعنی حتی سوئیچی که پورتی در یک VLAN ندارد، ترافیک آن VLAN را روی ترانک خود میگیرد که مسلماً ترافیکی زائد است. این ترافیک میتواند از نوع Broadcast، Unknown Unicast و یا Multicast باشد.

در شکل زیر ترافیک زائد پخش شده در شبکه نشان داده میشود:



برای جلوگیری از ترافیک زائد، میتوانیم VTP Pruning را در شبکه روی سوئیچ ها فعال کنیم. VLAN هایی که در یک سوئیچ عضو ندارند، به سمت او ارسال نخواهند شد مگر آنکه سوئیچ پائینتری از آن سوئیچ، پورتی عضو آن VLAN داشته باشد و تبادل آن اطلاعات بخاطر وجود انشعاب های دیگر اجتناب ناپذیر باشد.

اما تغییر وضعیت ترانک ها را پس از اجرای VTP Pruning در شکل زیر میبینیم:



در واقع Pruning ترافیک VLAN های اضافی در یک شاخه را روی ترانک، هرس میکند. بصورت پیش فرض VLAN های 2 تا 1001 روی ترانک قابل Prune شدن هستند. هرچند که Pruning باید ابتدا روی سوئیچ ها فعال گردد که بصورت پیش فرض غیر فعال است. (روی سوئیچ های IOS-Based)

حتی موقعی که یک VLAN از شاخه ای Prune (هرس) میشود، اطلاعات STP (بخاطر PVST) روی آن ترانک منتقل خواهند شد که در صورت تمایل توسط دستور `switchport trunk allowed vlan` (روی Interface) میتوان از ترافیک اضافی مربوط به هر VLAN جلوگیری کرد.

## تنظیم VTP

تنظیمات یک سوئیچ باید قبل از اتصال آن به شبکه، مد نظر قرار گیرد. اگر Configuration Revision Number یک سوئیچ بالاتر باشد، منجر به تغییر تنظیمات سوئیچ های دیگر میشود و VLAN ها را بهم خواهد ریخت. به این رخداد **VTP Synchronization Problem** میگوئیم. در VTP V3 برای حل اشتباهات این چنینی تدابیری اندیشیده شده است که فعلا روی سوئیچ های رده بالا پشتیبانی میشود. برای حل این مساله میتوانیم یک سوئیچ را به مد **Transparent** برده و بعد به مد **Server** برگردانیم تا Configuration Revision Number آن صفر شود. (یا اسم Domain آنرا به نامی دیگر تغییر داده و دوباره به حالت اول برگردانیم).

اگر خواستیم یک سوئیچ در کنار VTP Server بعنوان Redundant کار کند میتوانیم اول آن را Client کنیم، سپس به مد Server تبدیل کنیم.

```
Switch(config)# vtp domain domain-name
Switch(config)# vtp mode {server | client | transparent}
Switch(config)# vtp password password
Switch(config)# vtp version {1 | 2}
```

در صورت تنظیم Password باید رمز روی همه سوئیچ های داخل آن Domain تنظیم گردد.

برای فعال کردن Pruning از دستور زیر استفاده میکنیم:

```
Switch(config)# vtp pruning
```

برای تغییر Pruning و حذف یا اضافه Pruning روی ترانک از دستور زیر استفاده میکنیم:

```
Switch(config-if)# switchport trunk pruning vlan {add | except | none |
remove} vlan-list
```

عملیات Pruning توسط VTP بصورت خودکار انجام میشود (در صورت فعال بودن VTP Pruning) پس نیازی به تنظیم خاصی ندارد اما اگر بخواهیم VLAN خاصی را از هرس شدن منع کنیم بکمک دستور switchport trunk pruning vlan لیست VLAN هایی که مجاز به هرس شدن هستند را به سوئیچ اعلام میکنیم. در واقع VLAN ی که در لیست نباشد بصورت خودکار Prune نمیشود.

دستور switchport trunk allowed vlan برای تنظیم دستی VLAN های مجاز روی ترانک است و ارتباط و نیازی به VTP Pruning ندارد. مثلا اگر سوئیچ بکمک dot1q با فیروال یا روتر ترانک برقرار کرده باشد امکان استفاده از VTP وجود ندارد (فراموش نکنید که VTP مختص به سوئیچ هاست) بکمک دستور فوق تنها VLAN هایی که مد نظر داریم را به سمت دیگر هدایت میکنیم.

