# آشنایی با شبکه های مجازی (VLAN)

نیوشا صدری

* افزایش عملکرد
* بهبود قابلیت های مدیریتی
* تنظیم شبکه و ساده سازی پیکربندی های نرم افزاری
* استقلال توپولوژی فیزیکی
* افزایش گزینه های امنیتی

## چکیده:

شبکه های مجازی (VLANs) امکانی است که بر اساس آن می‌توان چندین شبکه مجازی مجزا را در یک بستر فیزیکی یکپارچه شبکه ای ایجاد کرد. اهمیت این مکانیزم در برقراری امنیت و کنترل ترافیک شبکه‌ها نمود پیدا می‌کند.

## فهرست:

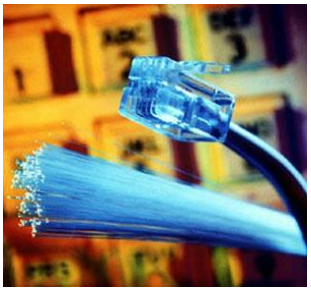


### ۱ – مقدمه:

یک **شبکه مجازی**، که معمولا به نام **VLAN** خوانده می شود، مجموعه ای است از نودهایی که در یک Broadcast Domain قرار دارند. VLAN همان صفات شبکه فیزیکی را دارد، اما به End Station ها اجازه می دهد تا باهم گروه بندی شوند حتی اگر آنها در همان بخش از شبکه واقع نشده باشند. با استفاده از VLAN می توان پیکر بندی دوباره شبکه را بجای جابجایی فیزیکی دستگاه ها، از طریق نرم افزاری انجام داد.

VLAN ها برای ارائه سرویس های تقسیم بندی که به طور سنتی توسط روترها در تنظیمات شبکه فراهم می شد، ایجاد شده اند. از مشکلات VLAN می توان به مقیاس پذیری، امنیت و مدیریت شبکه اشاره کرد. روترها در توپولوژی VLAN انتشار فیلترینگ، امنیت، خلاصه سازی آدرس و مدیریت جریان ترافیک را فراهم می نمایند. بر اساس تعریف، سوئیچ ها نمی تواند ترافیک آی پی بین VLAN ها را پل (Bridge) کنند چرا که یکپارچگی دامنه پخش VLAN را نقض خواهند کرد. شبکه های مجازی و IP Subnet ها ساختار لایه ۲ و لایه ۳ مشترکی که به یک دیگر Map می شوند را فراهم می کنند و این ساختار در حین مراحل طراحی شبکه مفید خواهد بود.

## ۲ – تشریح:



VLAN ها از طریق نرم افزار به جای سخت افزار پیکربندی شده است که آنها را بسیار قابل انعطاف است. یکی از بزرگترین مزایای VLAN این است که هنگامی که محل فیزیکی کامپیوتر تغییر می کند، می تواند در همان شبکه VLAN بدون هرگونه نیاز به پیکر بندی دوباره سخت افزاری بمانند.

## ۳ – دلایل گرایش:

در یک شبکه سنتی، کاربران بر اساس جغرافیا اختصاص داده شدند و توسط توپولوژی فیزیکی و فاصله محدود شده است. با استفاده از VLAN می توان منطقاً می تواند شبکه های گروهی و دیگر محدود به فاصله های فیزیکی است. این موضوع شامل فن آوری های پرسرعت می شود که در زیر به آنها اشاره شده است:

- حالت انتقال ناهمگام یا Asynchronous Transfer Mode (ATM)
- رابط فیبر توزیع داده یا Fiber Distributed Data Interface (FDDI)
- اترنت سریع یا Fast Ethernet
- اترنت گیگابیت یا Gigabit Ethernet
- اترنت ۱۰ گیگابیت یا 10 Gigabit Ethernet

با استفاده از VLAN می توان الگوهای ترافیک را کنترل کرد و در جابجایی ها به سرعت واکنش نشان داد. همچنین VLAN علاوه بر فراهم کردن انعطاف پذیری لازم برای تطبیق با تغییرات مورد نیاز در شبکه، مدیریت شبکه را آسان و امنیت آن را افزایش می دهند. این مزایا در قسمت های زیر به ترتیب توضیح داده شده اند.

قابلیت اداره بهتر:

VLAN ها یک راه راحت، انعطاف پذیرو کم هزینه برای اصلاح گروههای منطقی در محیطهای تغییر پذیر فراهم می کنند. VLAN ها شبکه های بزرگ با قابلیت اداره بیشتر را بوسیله پیکربندی متمرکز شده از وسایل واقع در مکان فیزیکی گوناگون می سازند.

وفق دادن شبکه و ساده سازی برنامه های پیکر بندی:

VLAN ها به مدیرهای LAN ها اجازه می دهند تا شبکه های خود را با کاربران گروهی منطقی به طورصحیح وفق دهند.نرم افزار های پیکر بندی می توانند وسایل را با تقویت یک دپارتمان و تبدیل آن به یک زیر شبکه تنها سرتاسر شبکه را یکنواخت سازند. IP آدرس و Subnet و پروتکل های شبکه می توانند به شبکه تحکیم بیشتری بخشند.

توپولوژی فیزیکی مستقل:

VLAN ها با اتصال منطقی گروه های کاربران داخل یک قلمرو Broadcast یک استقلال خاص از توپولوژی فیزیکی شبکه را فرآهم می کنند. اگر زیر ساخت های از قبل کار گذاشته شده باشند، اضافه کردن پورتها در یک محل جدید برای ایجاد VLAN کار ساده ای خواهد بود. این واگذاری ها می تواند در یک حرکت پیشرفته صورت گیرد. و حرکت وسایل با پیکر بندی کنونی آنها از یک محل به محل دیگر ساده می شود.

افزایش گزینه های امنیتی:

VLAN ها این قابلیت را دارند که ایمنی های اضافی که در رسانه های به اشتراک گذاشته شده در دسترس نمی باشد را فراهم کنند. شبکه های سوئیچی بطور طبیعی فریم ها را فقط به گیرنده های مورد نظر تحویل می دهند ولی فریم های broad cast به دیگر اعضای شبکه نیز منتقل می شوند. این امر به مدیر شبکه اجازه می دهد تا کاربران را برای دستیابی به اطلاعات حساس به VLAN های مجزا تقسیم کند. این کار بدون توجه به موقعیت فیزیکی آنها انجام می گیرد.

از مزایای تجاری VLAN می توان به موارد زیر اشاره کرد:

۱- به وسیله VLAN به راحتی می توان نیازهای شبکه ای یک سازمان مجازی را برطرف کرد. استفاده از Switch هایی که قابلیت تعریف VLAN را دارند باعث می شود که مدیریت شبکه های مختلف توسط یک Switch به راحتی انجام شود و تغییرات و تحرکات به راحتی قابل کنترل باشد.

۲- با استفاده از VLAN پهنای باند به صورت بهینه مصرف می شود، به این معنا که Frame ها و یا Packetهایی که توسط یک Station در یک VLAN خاص، فقط برای Station های اعضای آن VLAN ارسال می شوند و دیگر VLAN های دیگر، مشغول به دریافت Packetهای مربوط به آن VLAN نمی شوند. همچنین روشهایی برای محدود سازی پهنای باند برای هر VLAN پس از تعریف VLAN وجود دارد.

۳- به وسیله VLAN امنیت شبکه بالا می رود. به این معنا که افرادی که در یک VLAN خاص قرار دارند مطمئن خواهند بود که افراد دیگری که به VLAN های دیگر در آن شبکه متصل هستند نمی توانند از آدرسهای آنها و منابع آن VLAN برای دسترسی به اطلاعات آنها استفاده کنند. همچنین ابزاری مانند Sniffer ها و امثال آنها دیگر مورد استفاده ای در VLAN های دیگر برای دسترسی به اطلاعات بقیه Stationها نخواهند داشت.

## ۴ – پروتکل ها و طراحی:

در زمینه VLAN ها یک استانداردی توسط IEEE تهیه شده است به نام IEEE 802.1q که در آن روشی برای ایجاد VLAN و تشخیص آنها برای Switch ها و Router ها پیشنهاد شده است که امروزه اکثر Switch ها و Router های استاندارد از آن به عنوان استاندارد VLAN پشتیبانی می کنند.

با استفاده از تعدادی سوئیچ و اتصال به سوئیچ از طریق Telnet به راحتی می توان یک شبکه VLAN را طراحی کرد. بعد از ساخت شبکه مجازی هر یک از سگمنت هایی را که به درگاه های معین وصل می شوند جزئی از این شبکه مجازی می گردند.
مادامی که در یک سوئیچ چندین شبکه VLAN داشته باشیم، این شبکه ها نمی توانند به صورت مستقیم با شبکه دیگری که به آن سوئیچ متصل می باشد ارتباط برقرار کنند. در غیر این صورت می توانست منجر به عدم استفاده از شبکه های مجازی شود البته برای برقراری ارتباط ما بین چندین VLAN به وجود روتر نیاز است.
شبکه های VLAN می توانند از چندین سوئیچ برای برقراری ارتباط استفاده کنند و همچننی چندین شبکه مجازی VLANمی توانند به یک سوئیچ متصل شوند شبکه های مختلفی که به سوئیچ های مختلفی متصل می باشند قادرند تا از طریق لینک ما بین سوئیچ ها با هم ارتباط برقرار کنند. برای تحقق آن از پروتکل موسوم به Trunking بهره می گیرند. پروتکل مذکور تکنولوژیی می باشد که به اطلاعات این امکان را می دهد تا از بین چندین شبکه VLAN و از طریق لینک سوئیچ ها عبور کنند.

طراحی و پیاده سازی یک شبکه کامپیوتری کار ساده ای نمی باشد و شبکه های VLAN نیز از این قاعده مستثنی نخواهند بود، چراکه در این نوع شبکه ها مجموعه ای متنوع از پروتکل ها به منظور نگهداری و مدیریت شبکه بکار گرفته می شود.

**طراحی اولین VLAN**

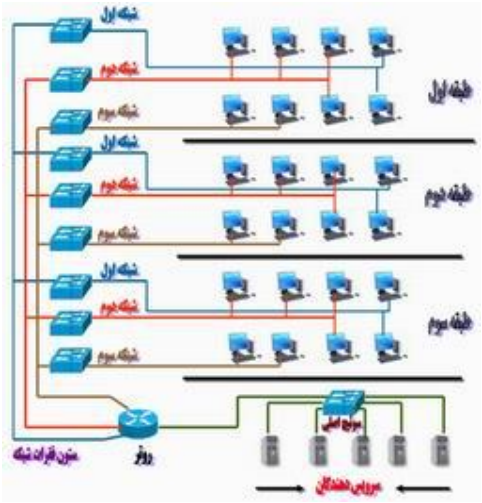
در اکثر پیکربندی های VLAN، محوریت بر اساس گروه بندی دپارتمان ها صرفنظر از محل استقرار فیزیکی آنان در یک شبکه می باشد. بدین ترتیب مدیریت دپارتمان ها متمرکز و امکان دستیابی به منابع مهم و حیاتی شبکه محدود و صرفا در اختیار کاربران مجاز قرار خواهد گرفت.

در ادامه به بررسی یک سازمان فرضی خواهیم پرداخت که قصد طراحی و پیاده سازی یک شبکه کامپیوتری را دارد. مدل پیشنهادی را بدون در نظر گرفتن VLAN و با لحاظ نمودن VLAN بررسی می نمائیم.

**وضعیت موجود سازمان فرضی** :

- سازمان فرضی دارای چهل دستگاه ایستگاه کاری و پنج سرویس دهنده است.
- در سازمان فرضی دپارتمان های متفاوتی با وظایف تعریف شده، وجود دارد : دپارتمان مدیریت، دپارتمان حسابداری، دپارتمان فنآوری اطلاعات
- دپارتمان های اشاره شده در سه طبقه فیزیکی توزیع و پرسنل آنان ممکن است در طبقات مختلف مشغول به کار باشند.

**سناریوی اول : عدم استفاده از VLAN**

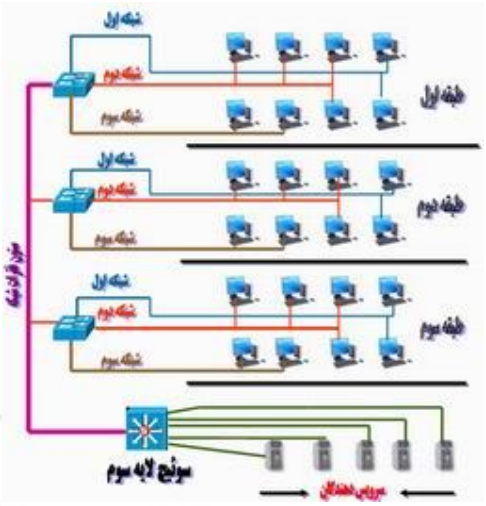



دپارتمان فنآوری اطلاعات به عنوان مجری طراحی و پیاده سازی شبکه به این نتیجه رسیده است که بدلیل رعایت مسائل امنیتی مناسب تر است که شبکه را پارتیشن نموده و آن را به چندین بخش تقسیم نماید. هر دپارتمان در یک Broadcast domain قرار گرفته و با استفاده از لیست های دستیابی که بین محدوده های هر یک از شبکه ها قرار می گیرد، این اطمینان حاصل می گردد که دستیابی به هر یک از شبکه ها با توجه به سیاست های دستیابی تعریف شده، میسر می گردد. با توجه به وجود سه دپارتمان متفاوت، سه شبکه جدید ایجاد می گردد. مدل پیشنهادی در این سناریو را در شکل مقابل می بینید:

**ویژگی های سناریوی اول :**

- به هر دپارتمان یک شبکه خاص نسبت داده شده است.
- در هر طبقه از یک سوئیچ اختصاصی برای هر یک از شبکه های موجود، استفاده شده است.
- مهمترین دستاورد مدل فوق، افزایش امنیت شبکه است چراکه شبکه های فیزیکی عملا" از یکدیگر جدا شده اند.
- سوئیچ های موجود در هر طبقه از طریق ستون فقرات شبکه با یکدیگر گروه بندی و به روتر اصلی شبکه متصل شده اند.
- روتر مسئولیت پیچیده کنترل دستیابی و روتینگ بین شبکه ها و سرویس دهنده ها را با استفاده از لیست های دستیابی بر عهده خواهد داشت.
- مدیریت شبکه بدلیل عدم وجود یک نقطه متمرکز دارای چالش های مختص به خود می باشد.

**سناریوی دوم : استفاده از VLAN**




در این مدل، طراحی شبکه با در نظر گرفتن فنآوری VLAN همانند شکل روبرو ارائه شده است:

**ویژگی های سناریوی دوم :**

- در هر طبقه از یک سوئیچ استفاده شده است که مستقیما" به ستون فقرات شبکه متصل می گردد.
- سوئیچ های استفاده شده در این سناریو دارای ویژگی VLAN بوده و بگونه ای پیکربندی می گردند که سه شبکه فیزیکی و منطقی جداگانه را حمایت نمایند.
- در مقابل روتر در سناریوی قبل از یک سوئیچ لایه سوم، استفاده شده است. سوئیچ های فوق بسیار هوشمند بوده و نسبت به ترافیک لایه سوم ( لایه IP ) آگاهی لازم را دارند.

- با استفاده از یک سوئیچ، می توان لیست های دستیابی را به منظور محدودیت دستیابی بین شبکه ها تعریف نمود. دقیقا" مشابه عملیاتی که با استفاده از روتر در سناریوی قبلی انجام می گردد ( روتینگ بسته های اطلاعاتی از یک شبکه منطقی به شبکه منطقی دیگر ). سوئیچ های لایه سوم، ترکیبی از یک سوئیچ قدرتمند و یک روتر از قبل تعبیه شده می باشند.
- مقرون به صرفه بودن ، تسهیل در امر توسعه شبکه، انعطاف پذیری و مدیریت متمرکز از جمله مهمترین ویژگی های سناریوی فوق می باشد.

## ۵ – انواع VLAN:

VLAN ها برحسب روش استفاده به طبقات مختلف تقسیم می شوند. عضویت VLAN ها می تواند به وسیله پورتها، آدرس MAC و نوع پروتکل به طبقات مختلف تقسیم شوند.

۱. عضویت به وسیله پورت:

عضویت در یک VLAN می تواند بر پایه پورتهایی که در یک VLAN قرار دارند صورت گیرد. برای مثال در یک شبکه با ۴ پورت پورتهای ۱و۲و۴ متعلق به VLAN1 و پورت۳ متعلق به VLAN2 می باشد.

| Port | VLAN |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 1 |

تنها عیب این روش این است که اجازه تحرک به کاربران داده نمی شود. اگر کاربری به مکانی غیر از ترتیب قبلی شبکه برود مدیر شبکه باید VLAN را دوباره تنظیم کند.

۲. عضویت بوسیله آدرس MAC:

اگر عضویت بر مبنای آدرس MAC یک گروه باشد، سوئیچ، آدرس MAC هر VLAN را درخود نگه می دارد . به دلیل اینکه آدرس MAC از کارت شبکه کاربران گرفته می شود، در زمانی که یک کاربر جابجا می شود ، تنظیم مجدد نیاز نیست.

| MAC Address | VLAN |
|---|---|
| 1212354145121 | 1 |
| 2389234873743 | 2 |
| 3045834758445 | 2 |

تنها عیب این روش این است که عضویت باید از ابتدا صورت گیرد ودر یک شبکه با هزاران کاربر این کار آسان نیست.

۳. عضویت بوسیله نوع پروتکل:

عضویت در VLANها می تواند بر پایه نوع پروتکل صورت گیرد.

| Protocol | VLAN |
|---|---|
| IP | 1 |
| IPX | 2 |

۲. عضویت بوسیله آدرس IP زیر شبکه:

آدرس IP زیر شبکه نز می تواند معیاری برای عضویت در VLAN باشد. دراین روش تنها از آدرس IP کاربران برای پیدا کردن آنها درشبکه استفاه می شود.

| IP Subnet | VLAN |
|---|---|
| 23.2.24 | 1 |
| 26.21.35 | 2 |

در این روش کاربران می توانند بدون پیکر بندی مجدد مکان خود را تغییر دهند. تنها عیب این روش بزرگتر بودن بسته های اطلاعاتی نسبت به آدرس MAC می باشد.

## ۹ – منابع:


| | |
|---|---|
| ۱. System Disc – VLAN | http://www.systemdisc.com/VLAN |
| ۲. Cisco Systems | http://www.cisco.com/ |
| ۳. WikIPedia | http://en.wikIPedia.org/wiki/Virtual_LAN |
| ۴. Rad Networks | http://www3.rad.com/networks/2006/VLAN/main.htm |
| ۵. پایگاه اطلاع رسانی تخصصی فناوری اطلاعات | http://www.itiran.com/ |
| ۶. افسون صفر و یک | http://www.afson01.com/ |
| ۷. پایگاه اطلاع رسانی تخصصی فناوری اطلاعات | http://www.itiran.com/ |
| ۸. مقاله های کامپیوتری | http://computer-article.blogfa.com/ |