VLAN

ماندانا ایزدی

فهرست

مقدمه

VLAN (Local Area Networks Virtua)l ، یکی از جدیدترین و جالبترین تکنولوژی های شبکه است که اخیرا" مورد توجه بیشتری قرار گرفته است . رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گرانقیمت بدون از دست دادن کارآئی و امنیت ، اهمیت و ضرورت توجه بیشتر به VLAN را مضاعف نموده است .

با استفاده از شبکه های محلی مجازی می توان سگمنت های شبکه را از یکدیگر تفکیک و برای هر یک از آنها قوانین دستیابی بر اساس سیاست های امنیتی مختص به خود را تعریف کرد . توجه داشته باشید که یک VLAN کارآئی شبکه را بهبود می بخشد ولی الزاما" امنیت را ارائه نخواهد کرد . با محدود سازی استفاده از VLANs برای شبکه perimeter (پشت فایروال) ، امکان استفاده تعداد زیادی از اینترفیس های غیرایمن موجود توسط مهاجمان سلب می گردد .

تمامی مسائل اشاره شده در بخش قبل را و تعداد بیشتری را که به آنان اشاره نشده است را می توان با ایجاد یک VLAN به فراموشی سپرد . به منظور ایجاد VLAN ، به یک سوئیچ لایه دوم که این تکنولوژی را حمایت نماید ، نیاز می باشد . تعدادی زیادی از افرادیکه جدیدا" با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفا" می بایست به منظور فعال نمودن VLAN ، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند . (برداشتی کاملا" اشتباه !) . با توجه به این که در شبکه های VLAN ، میلیون ها محاسبات ریاضی انجام می شود ، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است ، استفاده گردد (دقت در زمان تهیه یک سوئیچ)،در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده ، وجود نخواهد داشت .

هر VLAN که بر روی سوئیچ ایجاد می گردد ، به منزله یک شبکه مجزا می باشد . بدین ترتیب برای هر VLAN موجود یک broadcast domain جداگانه ایجاد می گردد . پیام های broadcast ، به صورت پیش فرض ، از روی تمامی پورت هائی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند . ویژگی فوق ، یکی از مهمترین دلایل متداول شدن VALN در شبکه های بزرگ امروزی است (تمایز بین سگمنت های شبکه) . شکل زیر یک نمونه شبکه با دو VLAN را نشان می دهد :

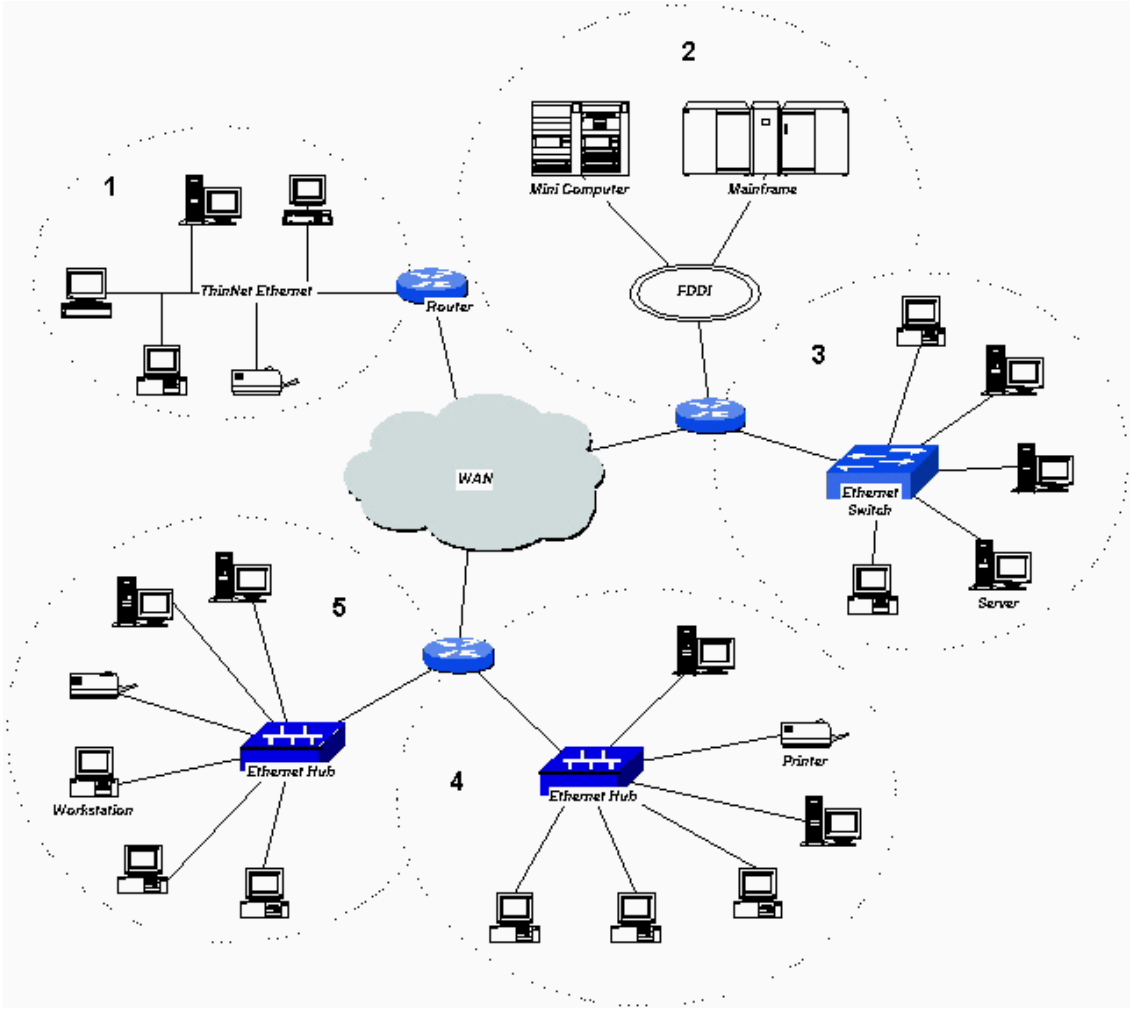
در شکل فوق ، یک شبکه کوچک با شش ایستگاه را که به یک سوئیچ (با قابلیت حمایت از VLAN) متصل شده انـد ، مشاهده می نمائیم . با استفاده از پتانسیل VLAN سوئیچ ، دو VLAN ایجاد شده است که بـه هـر یـک سـه ایـستگاه متصل شده است (VLAN1 و VLAN2) . زمانی که ایستگاه شماره یک متعلق به VLAN1 ، یک پیـام Braodcast را ارسال می نماید (نظیر : FF:FF:FF:FF:FF:FF) ، سوئیچ موجود آن را صـرفا" بـرای ایـستگاههای شـماره دو وسـه فورووارد می نماید . در چنین مواردی سـایر ایـستگاههای متعلـق بـه VLAN2 ، آگـاهی لازم در خـصوص پیـام هـای broadcast ارسـالی بـر روی VLAN1 را پیـدا نکـرده و درگیـر ایـن موضـوع نخواهنـد شـد . در حقیقت ، سوئیچی که قادر به حمایت از VLAN می باشد ، امکان پیاده سازی چندین شبکه مجزا را فراهم می نماید (مشابه داشتن دو سوئیچ جداگانه و اتصال سه ایستگاه به هر یک از آنـان در مقابـل اسـتفاده از VLAN) . بـدین ترتیـب شاهد کاهش چشمگیر هزینه های برپاسازی یک شبکه خواهیم بود .

فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمـائیم . بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاههای مورد نظر به هر یک از آنان ، دوازده شبکه مجـزا کـه امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم . یکی دیگر از روش هـای تـامین خواسـته فـوق ، اسـتفاده از VLAN است. بدین منظور می توان از یک و یا چندین سوئیچ کـه VLAN را حمایـت مـی نماینـد ، اسـتفاده و دوازده VLAN را ایجاد نمود . بدیهی است ، هزینه برپاسازی چنین شبکه هایی بـه مراتـب کمتـر از حـالتی اسـت کـه از دوازده سـوئیچ جداگانه ، استفاده شده باشد .

در زمان ایجاد VALN ، می بایست تمامی ایستگاهها را به سوئیچ متصل و در ادامه ، ایستگاههای مرتبط بـا هـر VLAN را مشخص نمود. هر سوئیچ در صورت حمایت از VLAN ، قادر به پشتیبانی از تعداد مشخصی VLAN است . مثلا" یـک سوئیچ ممکن است ۶۴ و یا ۲۶۶ VLAN را حمایت نماید.

VLAN چیست ؟

برای درک بهتر VLAN بایستی ابتدا شبکه های محلی یا LAN را به درستی درک شناخت. از LAN میتوان در حالت کلی به بستر انتشار اطلاعات یاد نمود . اجزای شبکه همانند Hub ها و سوییچ ها وظیفه ایجاد ارتباط بین گره های شبکه را بر عهده دارند. هر گره می تواند بدون نیاز به مسیر یاب [1] به هر گره دیگر متصل گردد. گره های شبکه در واقع همان ایستگاه های کاری یا رایانه ها هستند.در صورتیکه گره های شبکه بخواهند با گره هایی در LAN های دیگر ارتباط بر قرار سازند باید از مسیر یاب ها استفاده کرد. شکل ۱ این موضوع را نشان داده است.



شکل ۱ – شمای کلی یک شبکه با مسیر یاب

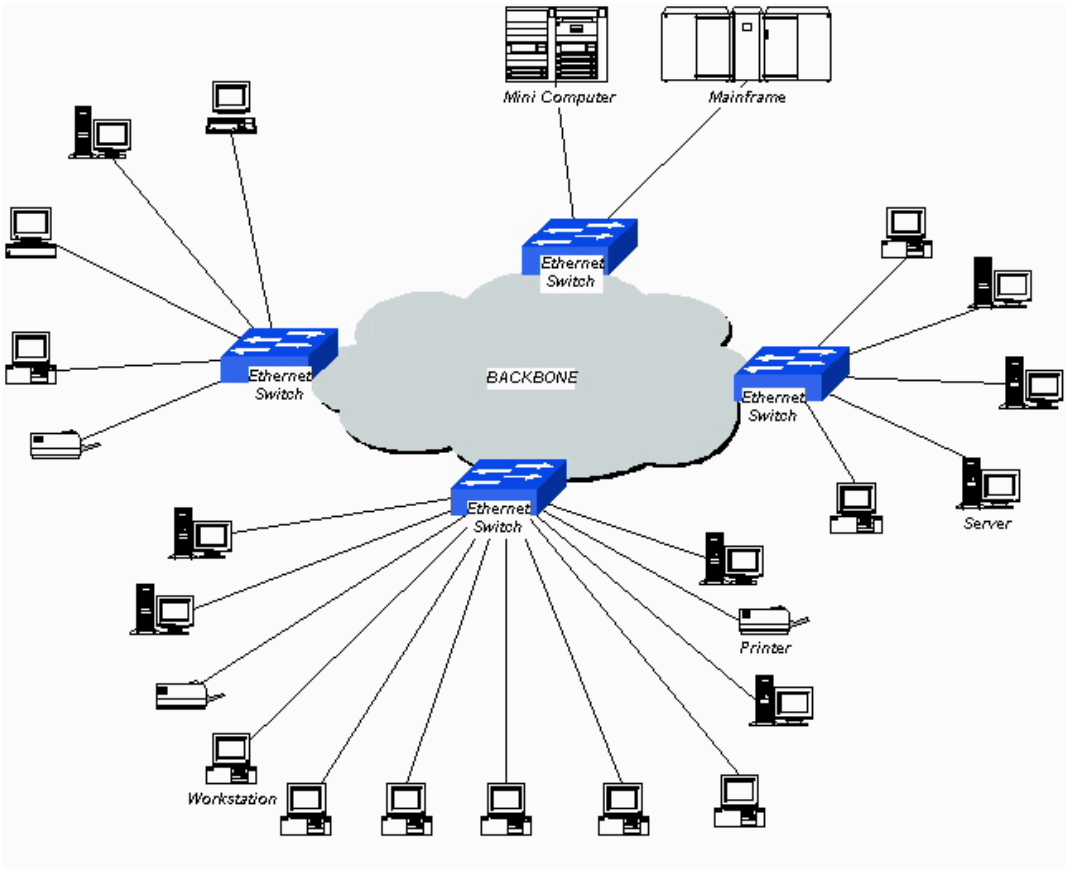
در شکل ۱ هر LAN توسط مسیر یاب به LAN دیگر مرتبط گشته است. این توپولوژی UCDNet نام دارد. در شکل فوق محدوده شبکه های محلی با خط چین نشان داده شده و از ۱ تا ۵ شماره گذاری شده است. توجه کنید که مسیر یاب های هر LAN بخشی از بستر انتشار همان LAN در نظر گرفته شده است.

[1] router

طبیعتا با گسترش LAN ، برای ایجاد ارتباط بین LAN ها و کاهش تداخلات، نیاز به روتـر هـای بیـشتری خواهـد بـود. شکل ۱ جداسازی LAN های ۱ و ۴ را با استفاده از یک روتر از بستر های چند گانه انتشار نشان می دهد.

یکی از مهمترین اشکالات این نوع طراحی شبکه اینست که با افزایش تعداد روتر ها تاخیر[۲] ارسال نیز افزایش می یابـد. بدیهی است این افزایش تاخیر به دلیل افزایش میزان پردازش اطلاعات در روتر ها است .دلیل عمده افـزایش پـردازش نیز به نوبه خود نتیجه افزایش بسته های داده برای مشخص کردن مقصد ها و یافتن مسیر ها و تخـصیص گـره هـای انتهایی است.

شبکه های مجازی یا VLAN ها میتوانند بعنوان گروهی از دستگاه ها تصور شوند که اگرچـه در بخـش هـای فیزیکـی متفاوتی قرار دارند اما می توانند بطوری که گویی اجزای یک شبکه محلی هستند با هم ارتباط برقرار سـازند. اسـتفاده از VLAN ها فواید زیادی دارد که در بخش های بعدی به آن خواهیم پرداخت. برای برشماری این فوایـد بایـد توپولـوژی متفاوتی را تشریح کنیم .



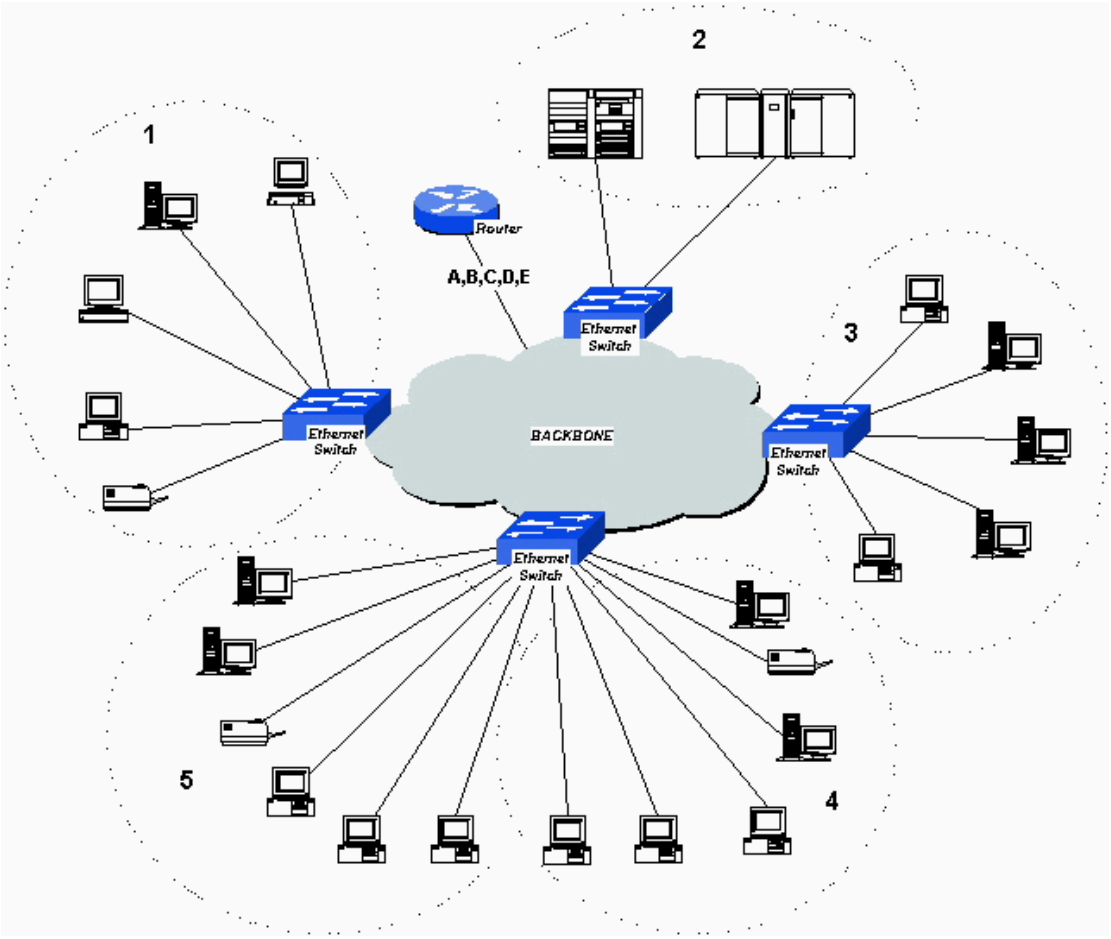
شکل ۲ – شمای کلی یک شبکه با سوییچ

[2] Latency

درشکل ۲ همان گره های شبکه ی شکل ۱ نشان داده شده و تنها از سوییچ بجای هاب و روتر استفاده شده است. اگر چه توپولوژی فوق دارای سرعت و تاخیر بهتری نسبت به توپولوژی شکل قبل است (شکل ۱) ، اما هنوز دارای اشکالات جدی است.

مهمترین نکته قابل توجه در این توپولوژی این است که تمامی میزبان[3] ها (گره های شبکه) در یک بستر انتشار قرار دارند و این بدین معنی است که ترافیک شبکه را تمامی گره های شبکه خواهند دید. در این صورت با افزایش تعداد گره ها ، ترافیک شبکه نیز رشد کرده و شبکه اساسا پایداریش را از دست خواهد داد.

سوییچ هایی که در VLAN ها استفاده می شوند همان تقسیم بندی شبکه ها به بستر های انتشار مجزا را بوجود می آورند با این تفاوت که مشکلات تاخیر روتر ها را ندارند بعلاوه راه حل های کم هزینه تری نیز هستند. شکل ۳ توپولوژی یک شبکه سوییچ را با استفاده از VLAN نشان می دهد.



شکل ۳ – شمای کلی یک شبکه VLAN با سوییچ

توجه کنید که توپولوژی شکل فوق همان توپولوژی شکل ۱ است با دو تفاوت :

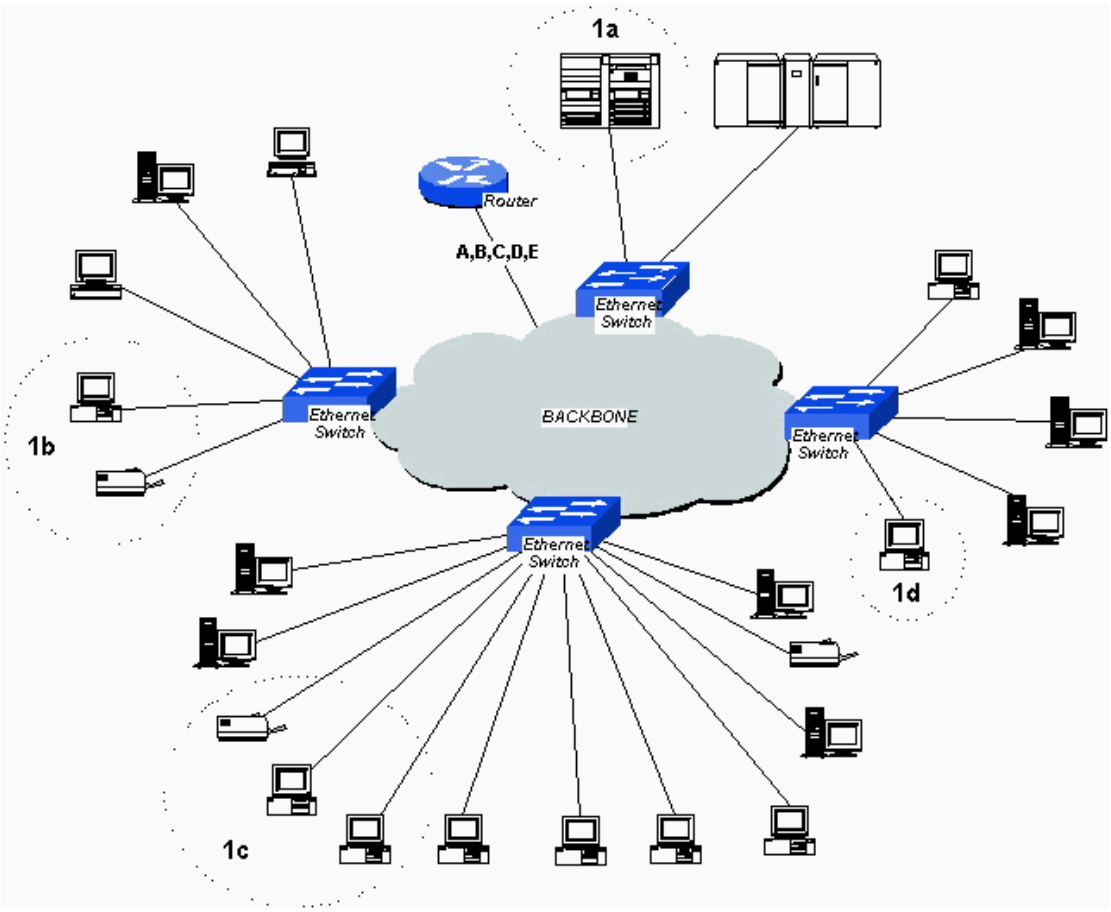
استفاده از سوییچ بجای هاب و روتر

[3] Host

استفاده از تنها یک روتر

همچنین توجه کنید که شناسه های شبکه روی تنها یک واسط مسیر یابی ظاهر می شود. حتی در این صورت نیز هنوز به یک مسیر یاب برای حرکت بین بستر های انتشار نیاز خواهیم داشت. در مثال حاضر واسط های مسیر یابی بخش از VLAN ها می باشند. در حال حاضر راه حل های متفاوتی برای ایجاد و طراحی VLAN ها دارد که بیشتر آنها نیز متناسب با نیاز کاربر بوده و بطور خلاصه هنوز اکثر راه حل ها مختص مشتری ها است.

حال ممکن است این سوال پیش آید که اساسا فایده اینگونه طراحی چیست و چرا تصور " قرار داشتن در یک شبکه " از سوی گره های شبکه سود مند است ؟ شکل ۴ به تشریح این موضوع می پردازد.



شکل ۴ – شمای کلی گروه بندی یک شبکه VLAN با استفاده از الگوی ترافیک

در مثال های قبلی LAN هایی که در یک گروه قرا داشتند از لحاظ فیزیکی و محل قرار گیری نیز دارای جایگاه یکسانی بودند. شکل ۴ یک *شبکه مجازی* را نشان می دهد (VLAN 1) که دارای الگوی های ترافیکی ذهنی است. تمام دستگاه های موجود در بخش های 1b ، 1c و 1d به میکروکامپیوتر 1a دسترسی دارند. با استفاده از VLAN ها میتوان تمام دستگاه های فوق را بصورت یک بستر انتشار واحد فرض نمود. این فرض به ما اجازه می دهد که ترافیک انتشار

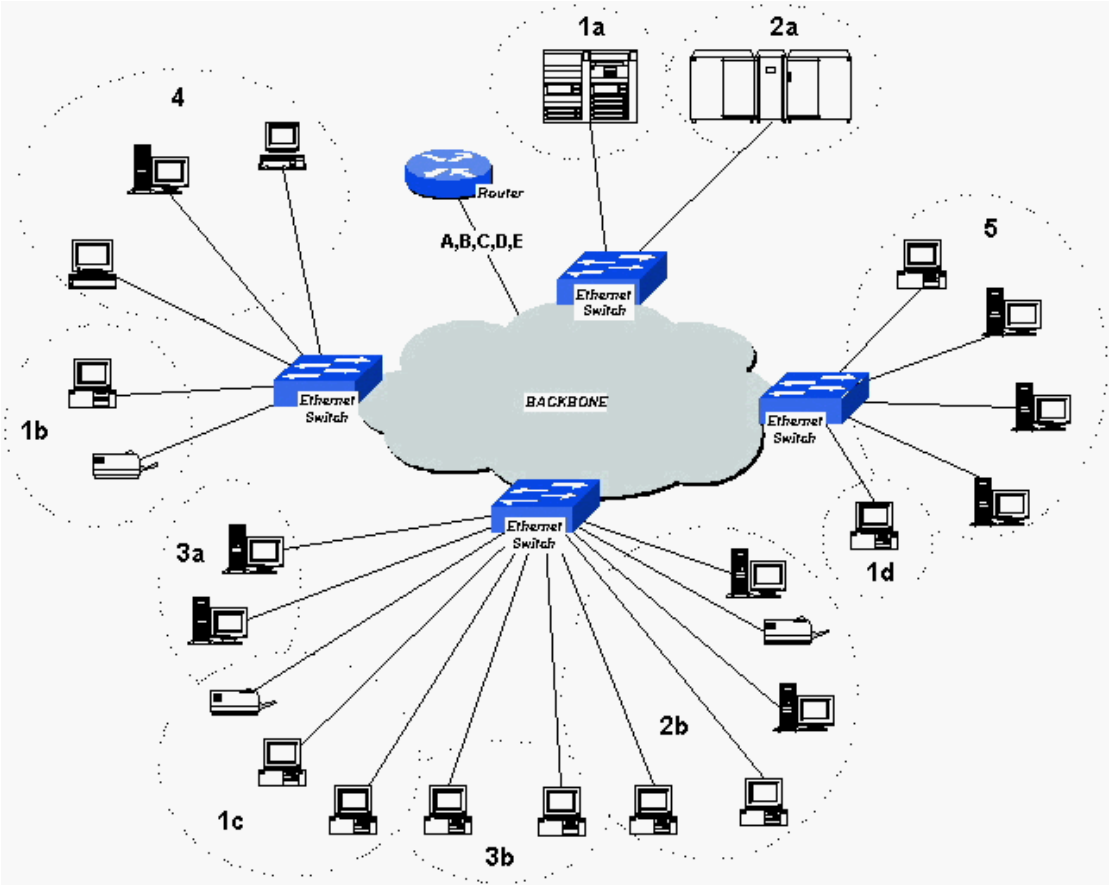
را به همین گروه کاری[۴] محدود کرده و در نتیجه ترافیک کاری شبکه را کاهش دهیم. این موضوع ما را قادر مـی سـازد که ترافیک شبکه را فقط به محدودهایی که لازم است ترافیک در آن دیده شود ، محدود نمـاییم و ایـن یعنـی افـزایش سرعت ارتباط در نتیجه حذف تاخیر ارتباط روتر ها.

فایده دیگر استفاده از این روش افزایش امنیت شبکه هاست چرا که می توان به گره های دیگر زیر شـبکه هـا [۵] اجـازه دسترسی به شبکه مورد نظر را نداد. بطور دقیق تر می توانیم فرض می کنیم که اجزای یک شبکه مجازی در یک گروه کاری قرار داشته و بر این اساس دسترسی به آنها را محدود می نماییم.

با گسترش این تفکر و استفاده از این روش ، می توان شبکه ای ایجاد نمود که وابسته به مکان فیزیکی نبوده و گسترده باشد. با این تفاسیر اگر شرکتی سه ساختمان مختلف در سطح شهر داشته باشد ، میتوان با این روش سرورها ،پرینتر هـا و ایستگاه های کاری را همانگونه پیکر بندی و استفاده کرد که اگر در یک مکان واحد قرار داشتند، از آنها اسـتفاده مـی شد.

همانطور که در شکل ۴ نشان داده شده است ، VLAN1 گروهی از کاربران است که قصد اصلی آنها دسترسـی بـه بانـک اطلاعاتی یک مینی کامپیوتر است. VLAN2 نیز شامل گروه مشابهی از کاربران است که نیازشان دسترسی به سرورهای محلی و مین فریم است. VLAN3 دپارتمانی است با سرورها و گروه های کـاری در طبقـات مختلـف و سـاختمان هـای جداگانه. VLAN های ۴ و ۵ نیز شامل دپارتمان های مختلف با سرور ها و ایستگاه های کاری متفـاوت ولـی مـستقر در یک ساختمان واحد را نشان می دهد.

[4] workgroup
[5] subnet

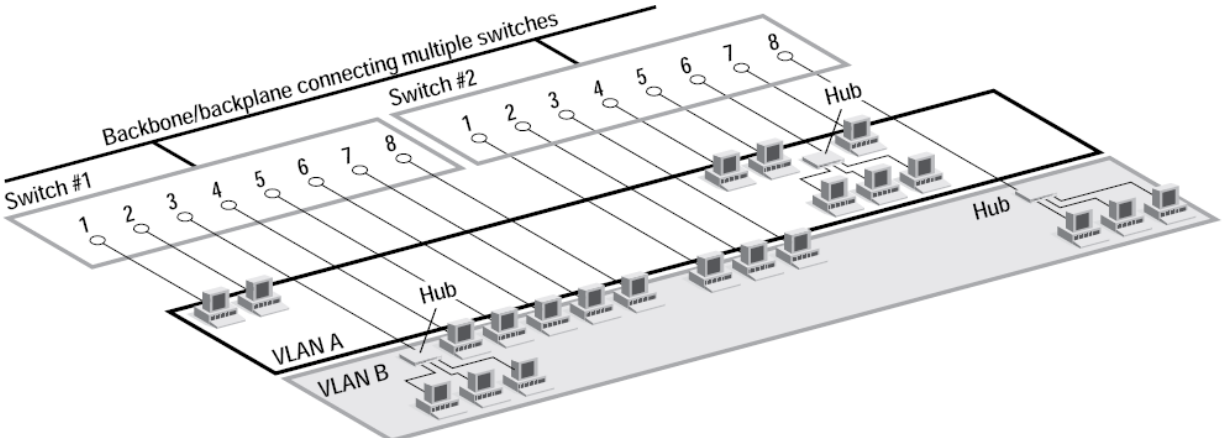


شکل ۵ – گروه بندی لاجیکی VLAN ها

در این نوع پیاده سازی ، مدیر شبکه هر یک از پورت های سوییچ را به یک VLAN منتسب می سازد برای مثال درگاه های ۱ تا ۳ به VLAN بخش فروش ، درگاه های ۴ تا ۶ به VLAN بخش مهندسی و درگاه های ۷ تا ۹ به VLAN مدیریت شبکه.در این روش شناسه هر بسته اطلاعاتی با توجه به پورتی که از آن رسیده است تعیین می گردد.

در این روش تغییر مکان کاربران شبکه خللی در گروه بندی آنها پدید نمی آورد چون که براحتی می توان با جابجایی سوکت ها افراد و ایستگاه های کاری را گروه بندی نمود. به هر حال این روش دارای یک عیب اساسی است که در بخش محدودیت های VLAN به آن می پردازیم. اما بطور اجمال می توان گفت که اگر یک تکرار کننده [۶] به درگاه سوییچ متصل باشد ، تمامی کاربران متصل به آن تکرار کننده بایستی اعضای همان VLAN باشند.

[6] repeater



شکل۶ VLAN مبتنی بر درگاه

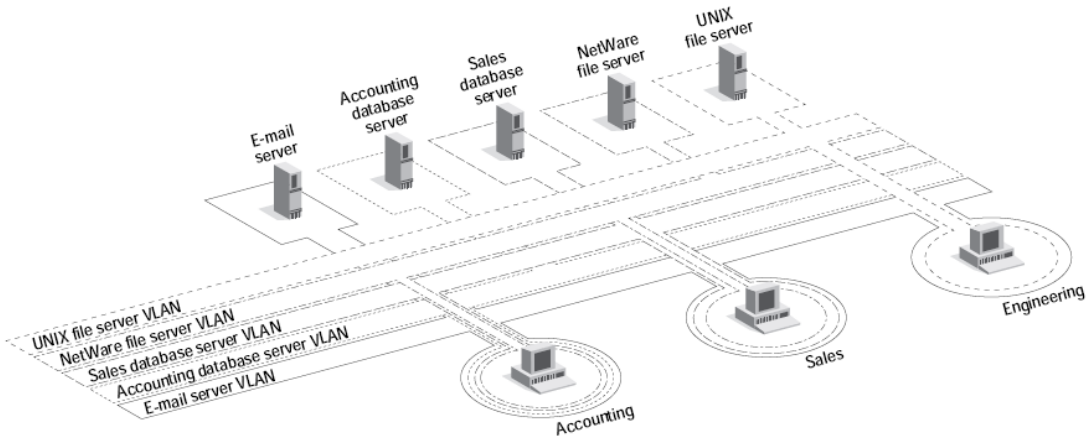
در این روش هر یک ار پورت های سوییچ باید به یک VLAN خاص منسب شود.

VLAN های مبتنی بر آدرس های کارت شبکه[۷]

شناسه بسته اطلاعات در این روش بر مبنای آدرس سخت افزاری مبدا و مقصد کارت های شبکه، تعیین می گردد. هر سوییچ جدولی از MAC آدرس ها را نگهداری کرده و بر اساس آن عضویت در یک VLAN را تصدیق می کند. برتری این روش نسبت به روش قبلی اینست که در این صورت نیازی به جابجایی کابلها و کانکتور ها در صورت تغییر مکان فیزیکی کاربران نیست.ولی عیب آن اینست که این روش هم وقت گیر بوده و هم اینکه نمی توان بسادگی یک کاربر را در چند VLAN عضو نمود.این محدودیت میتواند در به اشتراک گذاری منابع یک سرور اشکالات جدی به وجود آورد. اگر چه این موضوع در تئوری قابل انجام است اما در عمل ممکن است روتر ها و بریج های شبکه را دچار مشکل سازد.

VLAN های مبتنی بر لایه سوم (لایه پروتکل) در این روش شناسه اعضای یک شبکه مجازی بر اساس پروتکل مورد استفاده آنها معیین می گردد. این پروتکل ها می تواند IP ، IPX ، Netbios و یا آدرس های لایه سوم باشند. این روش یکی از ثبات ترین روش ها ی گروه بندی است و بطور مثال می توان یک زیر شبکه با پروتکل IP و یا یک شبکه IPX را به یک VLAN منتسب نمود.

[7] Media Access Card



شکل۶ VLAN مبتنی بر لایه سوم و نوع سرویس

یکی از مزایای این روش این است که به مدیر شبکه امکان میدهد؛ شبکه هایی را که از پروتکل های غیر قابـل مـسیر یابی [۸] مانند Netbios یا DECNET استفاده می کنند، به شبکه هایی منتسب سازد که از پروتکل های قابل مسیر یـابی استفاده می کنند مانندIPX یا IP.

محاسن استفاده از VLAN ها

همانطور که گفته شد ، استفاده از VLAN ها محاسن زیادی دارد. بطور خلاصه فواید معماری VLAN به قرار زیر است :

- افزایش کارایی
- افزایش قابلیت مدیریت
- سادگی پیکر بندی نرم افزاری و تنظیمات شبکه
- عدم وابستگی به توپولوژی فیزیکی
- افزایش امنیت شبکه
- افزایش کارایی

سوییچ های شبکه امروزی با کاهش اثرات تداخل، موجب افزایش کارایی شبکه می شوند. گروه بندی کـاربران نیـز بـه نوبه خود باعث کم شدن ترافیک شبکه و درنتیجه افزایش سرعت و کارایی آن می گردد. بدیهی است کاهش درخواست مسیر یابی موجب کم شدن مراجعه به روتر ها شده و در این صورت تاخیر ناشی از روتر ها نیز کاهش می یابد.

[8] nonroutable

افزایش قابلیت مدیریت

استفاده از VLAN ها راهی آسان ، مطمئن و کم هزینه برای تعدیل و تغییر گروه های لاجیکی است. با بزرگ تر شدن شبکه ها ، مدیریت گروهی ایستگاه ها و دستگاه های موجود در شبکه ، بصورت مرکزی قابل انجام بوده و درنتیجه ساده تر خواهد شد.

سادگی پیکر بندی نرم افزاری و تنظیمات شبکه

شبکه های مجازی به مدیران شبکه اجازه می دهند تا شبکه مورد نظر شان را با گروه بندی کاربران بصورت لاجیک، دقیقا تنظیم[9] و پیکر بندی کنند. پیکر بندی نرم افزاری بین ماشین های موجود در شبکه و همچنین آدرس های IP [10] ، ماسک[11] و پروتکل های شبکه ، یکنواخت تر خواهد شد. همچنین با کاهش ترافیک شبکه ، وظایف محوله به سرور همانند DHCP[12] و BOOTP[13] کاهش یافته و به علاوه کارایی این سرویس ها نیز با گستردگی شبکه ها افزایش می یا بد.

عدم وابستگی به توپولوژی فیزیکی

VLAN ها توپولوژی های غیر وابسته ای را ایجاد می کنند بدین معنی که گروه های کاری متفاوت می توانند در این ساختار بصورت لاجیکی به یک بستر انتشار واحد متصل گردند. فایده این ساختار اینست که بسادگی می توان ابزار ها و دستگاه ها را از محلی به محل دیگر منتقل کرد بدون این که در ساختار کلی شبکه تغییری ایجاد شود.

افزایش امنیت شبکه

VLAN ها قابلیت های بیشتری نسبت به شبکه های اشتراکی معمولی در قبال امنیت دارند. بطور پیش فرض ، یک سوییچ شبکه ، فریم های داده را به مقصد مورد نظر تحویل می دهد و انتشار آن تنها در محدوده اعضای یک VLAN خواهد بود. این قابلیت به مدیر شبکه این امکان را می دهد که کاربران شبکه را با توجه به حساسیت اطلاعات در گروه های جداگانه دسته بندی نماید. بعلاوه مونیتورینگ یک درگاه خاص با استفاده ازPort Analyzer بسیار ساده تر از مونیتورینگ ترافیک کل شبکه است. البته باید توجه داشت که این به معنی حل کامل مشکلات امنیتی شبکه نخواهد بود و تنها به به امنیت شبکه کمک خواهد کرد.

---

[9] fine tune
[10] IP addresse
[11] subnet mask
[12] Dynamic Host Configuration Protocol
[13] Bootstrap Protocol

محدودیت های استفاده از VLAN ها

محدودیت های استفاده از VLAN ها به سه بخش اصلی تقسیم می شود

– محدودیت های انتشار

برای پشتیبانی از ترافیک انتشار در یک شبکه ATM VLAN نیاز به داشتن یک سرور خاص است که بخشی از زیر ساخت ATM [14] است.برخی از پروتکل های شبکه همانند IPX و AppleTalk موجب ایجاد ترافیک انتشار زیادی خواهند شد که ممکن است سبب از کار افتادن سوییچ های شبکه گردد.بنابراین در این نوع سرور ها بایستی در تعیین اندازه و پیکر بندی VLAN دقت زیادی نمود.

– محدودیت های دستگاه

تعداد آدرس های اترنت قابل پشتیبانی توسط هر یک از دستگاه های حاشیه ای ۵۰۰ عدد است. این بدین معنی است که درگاه Network 21 نمی تواند توزیعی بیش از ۲۰ دستگاه داشته باشد. این تعداد محدودیت سیستم در حال حاضر بوده و با پیشرفت تکنولوژی این محدودیت نیز بهبود می یابد.

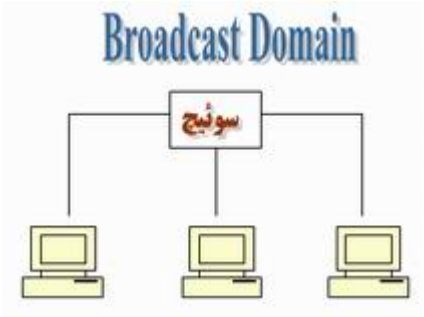
– محدودیت های پورت

در صورتیکه Hub یا سوییچ به درگاه Network 21 متصل گردد ، تمام درگاه های Hub بایستی به همان شبکه مجازی اختصاص یابند. در واقعHub ها قادر به ایجاد VLAN هایی با درگاه اختصاصی نیستند.

وضعیت شبکه های فعلی

تقریبا" در اکثر شبکه ها امروزی از یک (و یا چندین) سوئیچ که تمامی گره های شبکه به آن متصل می گردند ، استفاده می شود . سوئیچ ها روشی مطمئن و سریع به منظور مبادله اطلاعات بین گره ها در یک شبکه را فراهم می نمایند.با این که سوئیچ ها برای انواع شبکه ها ، گزینه ای مناسب می باشند ، ولی همزمان با رشد شبکه و افزایش تعداد ایستگاهها و سرویس دهندگان ، شاهد بروز مسائل خاصی خواهیم بود . سوئیچ ها ، دستگاه های لایه دوم (مدل مرجع OSI) می باشند که یک شبکه Flat را ایجاد می نمایند .

[14] Asynchronous Transfer Mode



همانگونه که در شکل فوق مشاهده می نمائید ، به یک سوئیچ ، سه ایستگاه متصل شده است . ایستگاههای فوق قادر به ارتباط با یکدیگر بوده و هر یک به عنوان عضوی از یک domain Broadcast مشابه می باشند. بدین ترتیب ، در صورتی که ایستگاهی یک پیام broadcast را ارسال نماید ، سایر ایستگاههای متصل شده به سوئیچ نیز آن را دریافت خواهند داشت.

در یک شبکه کوچک ، وجود پیام های Broadcast نمی تواند مشکل و یا مسئله قابل توجهی را ایجاد نماید، ولی در صورت رشد شبکه ، وجود پیام های braodcast می تواند به یک مشکل اساسی و مهم تبدیل گردد . در چنین مواردی و در اغلب مواقع ، سیلابی از اطلاعات بی ارزش بر روی شبکه در حال جابجائی بوده و عملا" از پهنای باند شبکه،استفاده مطلوب نخواهد شد. تمامی ایستگاههای متصل شده به یک سوئیچ ، پیام های Braodcast را دریافت می نمایند . چراکه تمامی آنان بخشی از یک Broadcast doamin مشابه می باشند .

در صورت افزایش تعداد سوئیچ ها و ایستگاهها در یک شبکه ، مشکل اشاره شده ملموس تر خواهد بود .همواره احتمال وجود پیام های Braodcast در یک شبکه وجود خواهد داشت .

یکی دیگر از مسائل مهم ، موضوع امنیت است . در شبکه هائی که با استفاده از سوئیچ ایجاد می گردند ، هر یک از کاربران شبکه قادر به مشاهده تمامی دستگاههای موجود در شبکه خواهند بود . در شبکه ای بزرگ که دارای سرویس دهندگان فایل ، بانک های اطلاعاتی و سایر اطلاعات حساس و حیاتی است ، این موضوع می تواند امکان مشاهده تمامی دستگاههای موجود در شبکه را برای هر شخص فراهم نماید . بدین ترتیب منابع فوق در معرض تهدید و حملات بیشتری قرار خواهند گرفت . به منظور حفاظت اینچنین سیستم هائی می بایست محدودیت دستیابی را در سطح شبکه و با ایجاد سگمنت های متعدد و یا استقرار یک فایروال در جلوی هر یک از سیستم های حیاتی، انجام داد .

معرفیVLAN

تمامی مسائل اشاره شده در بخش قبل را و تعداد بیشتری را که به آنان اشاره نشده است را می توان با ایجاد یک VLAN به فراموشی سپرد . به منظور ایجاد VLAN ، به یک سوئیچ لایه دوم که این تکنولوژی را حمایت نماید ، نیاز می باشد . تعدادی زیادی از افرادیکه جدیدا" با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص

نمی باشند و اینگونه استنباط نموده اند که صرفا" می بایست به منظور فعال نمودن VLAN ، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند . (برداشتی کاملا" اشتباه !) . با توجه به این که در شبکه های VLAN ، میلیون ها محاسبات ریاضی انجام می شود ، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است ، استفاده گردد (دقت در زمان تهیه یک سوئیچ)،در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده ، وجود نخواهد داشت .

هر VLAN که بر روی سوئیچ ایجاد می گردد ، به منزله یک شبکه مجزا می باشد . بدین ترتیب برای هر VLAN موجود یک broadcast domain جداگانه ایجاد می گردد . پیام های broadcast ، به صورت پیش فرض ، از روی تمامی پورت هائی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند . ویژگی فوق ، یکی از مهمترین دلایل متداول شدن VALN در شبکه های بزرگ امروزی است (تمایز بین سگمنت های شبکه) . شکل زیر یک نمونه شبکه با دو VLAN را نشان می دهد :

در شکل فوق ، یک شبکه کوچک با شش ایستگاه را که به یک سوئیچ (با قابلیت حمایت از VLAN) متصل شده اند ، مشاهده می نمائیم . با استفاده از پتانسیل VLAN سوئیچ ، دو VLAN ایجاد شده است که به هر یک سه ایستگاه متصل شده است (VLAN1 و VLAN2) . زمانی که ایستگاه شماره یک متعلق به VLAN1 ، یک پیام Braodcast را ارسال می نماید (نظیر : FF:FF:FF:FF:FF:FF) ، سوئیچ موجود آن را صرفا" برای ایستگاههای شماره دو وسه فوروارد می نماید . در چنین مواردی سایر ایستگاههای متعلق به VLAN2 ، آگاهی لازم در خصوص پیام های broadcast ارسالی بر روی VLAN1 را پیدا نکرده و درگیر این موضوع نخواهند شد .

در حقیقت ، سوئیچی که قادر به حمایت از VLAN می باشد ، امکان پیاده سازی چندین شبکه مجزا را فراهم می نماید (مشابه داشتن دو سوئیچ جداگانه و اتصال سه ایستگاه به هر یک از آنان در مقابل استفاده از VLAN) . بدین ترتیب شاهد کاهش چشمگیر هزینه های برپاسازی یک شبکه خواهیم بود .

فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمائیم . بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاههای مورد نظر به هر یک از آنان ، دوازده شبکه مجزا که

امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم . یکی دیگر از روش های تامین خواسته فوق ، استفاده از VLAN است . بدین منظور می توان از یک و یا چندین سوئیچ که VLAN را حمایت مـی نماینـد ، اسـتفاده و دوازده VLAN را ایجـاد نمود . بدیهی است ، هزینه برپاسازی چنین شبکه هایی به مراتب کمتر از حالتی است کـه از دوازده سـوئیچ جداگانـه ، استفاده شده باشد .

در زمان ایجاد VALN ، می بایست تمامی ایستگاهها را به سوئیچ متصل و در ادامه ، ایستگاههای مرتبط بـا هـر VLAN را مشخص نمود. هر سوئیچ در صورت حمایت از VLAN ، قادر به پشتیبانی از تعداد مشخصی VLAN است . مثلا" یـک سوئیچ ممکن است ۶۴ و یا ۲۶۶ VLAN را حمایت نماید.