گزارش پروژه شبکه

موضوع پروژه: شبیه سازی شبکه بیمارستان

نام استاد: دکتر محمد احمد نائینی

دانشجو: سید آصف حسینی

شماره دانشجویی: 970073970

توضیحات اولیه

من دوره کارآموزیم رو در **بیمارستان تریتا** واقع در چیتگر گذروندم. برای شبکه کردن این بیمارستان، از قبل با در نظر گرفتن اینکه در هر طبقه به چه تعداد کلاینت، دوربین و چه تعداد تلفن و تجهیزاتی نیاز دارند، کابل کشی‌ها به صورت توکار از انجام شده بود و فضای خالی هم برای کابل‌هایی که ممکنه در آینده بهشون نیاز بشه هم صورت گرفته بود.

هنگام ورود به بیمارستان یه بخش استیشن وجود داره (**Entrance reception**) که تعداد 3 کلاینت و همچنین دوربین وجود داره که همه دوربین‌ها و کلاینت‌های ما به سوئیچی که داخل رک در راه پله اضطراری قرار دارد، متصل هستند.

در طبقه اول یک اتاق به عنوان اتاق سرور وجود دارد که تجهیزات سرور ما داخل اون قرار داره و این اتاق به شدت امنیتی هستش و با اثر انگشت افراد مشخصی در باز میشه.

این بیمارستان ۱۸ طبقه هست و در هر طبقه سوئیچ وجود داره. پس از دید طبقاتی، ۱۸ تا سوئیچ داریم و توی هر طبقه با توجه به نیازی که بوده، تعدادی دوربین وجود داره. تمام سوئیچ‌های ما به اتاق سرور متصل هستند. روی سرور حدود 22 تا ماشین مجازی (VM) نصب شده.

ماشین مجازی کسرا، ماشین مجازی دوربین ها و بسیاری دیگر از نرم‌افزارها که نصب شدن روی سرور ها که در بیمارستان در حال استفاده هستند. با توجه به اینکه امنیت خیلی مهمه و اطلاعات بیمار باید به صورت ۱۵ سال به صورت سیستمی وجود داشته باشه، داخل اطلاعات بیمارستان امنیت این اطلاعات خیلی مهم هستش و من سوال‌های زیادی پرسیدم که امنیت چه جوری صورت می‌گیره و گفتن که این سوال رو نمی‌تونم پاسخ بدن که از چه نوع فایروالی استفاده می‌کنند و اینکه به امنیتشون با چه شرکتی قرارداد دارند و هزینه‌های امنیتی‌شون چقدر هستش چون که گفتن بارها شده بهشون اتک شده.

دو تا سرور دارند که سروراشون بالای یک میلیارد قیمتشونه هر کدوم توی اتاق سرور تجهیزات خنک کننده (Cooling) دارند به علاوه استوریج ها.

یکی دیگر از نرم‌افزارها که توی بیمارستان استفاده میشه، **HIS** است که به منظور اتوماسیون سناریو های:

وقتی که فرد میره اطلاعاتشو وارد می‌کنه، هنگام ورود، وقتی که عکسبرداری صورت بگیره، نسخه نوشته بشه و هر کاری که بیمار تو بیمارستان انجام بده، هر اتفاق که بیفته داخل سیستم هستش و از این بخش به اون بخش بهش دسترسی دارند.

من در نرم افزار Packet Tracer این شبکه رو به طور ساده شبیه سازی کردم. اینکه چه تعداد کلاینتی در یک طبقه و به چه صورت هست، اتاق سرور چه تجهیزاتی داره و این اتصالات چه جوری صورت می‌گیره، طراحی کردم و اینکه نکته‌ای که وجود داشت در این بیمارستان به دوربین‌ها به صورت دستی IP داده می شد و سایر کلاینت‌ها یا دستگاه‌ها با استفاده از DHCP Server.

با چندین شرکت قرارداد دارند و تحت قرارداد های سالانه پشتیبانی دریافت می کنند. بیشتر کارها توسط شرکت‌های پشتیبان صورت می‌گیره.

نرم افزار Packet Tracer

Packet Tracer یک نرم افزار شبیه سازی شبکه است که توسط سیسکو Systems توسعه داده شده است. Packet Tracer به کاربران این امکان را می دهد تا شبکه های کامپیوتری را بدون نیاز به تجهیزات واقعی طراحی، پیکربندی و آزمایش کنند.

Packet Tracer از طیف گسترده ای از دستگاه های شبکه پشتیبانی می کند، از جمله روترها، سوئیچ ها، کامپیوترها و دستگاه های پزشکی. کاربران می توانند از Packet Tracer برای ایجاد توپولوژی های شبکه مختلف، پیکربندی پروتکل های شبکه و آزمایش عملکرد شبکه استفاده کنند.

Packet Tracer یک ابزار آموزشی ارزشمند برای دانشجویان، متخصصان شبکه و علاقه مندان به شبکه است. این ابزار به کاربران این امکان را می دهد تا مفاهیم شبکه را به صورت عملی یاد بگیرند و مهارت های خود را در زمینه پیکربندی و آزمایش شبکه بهبود بخشند.

Packet Tracer دارای ویژگی های زیر است:

- **رابط کاربری گرافیکی (GUI) آسان برای استفاده:** Packet Tracer دارای یک رابط کاربری گرافیکی آسان برای استفاده است که به کاربران اجازه می دهد تا شبکه های کامپیوتری را به سرعت و به راحتی طراحی کنند.
- **محیط آموزشی:** Packet Tracer شامل مجموعه ای از تمرینات و سناریوهای آموزشی است که به کاربران کمک می کند تا مفاهیم شبکه را یاد بگیرند.
- **قابلیت همکاری:** Packet Tracer از همکاری چند کاربره پشتیبانی می کند که به کاربران امکان می دهد تا پروژه های شبکه را با یکدیگر کار کنند.

Packet Tracer در دسترس است به عنوان یک برنامه مستقل یا به عنوان بخشی از برنامه های آموزشی سیسکو.

در اینجا چند نمونه از کاربردهای Packet Tracer آورده شده است:

- **آموزش شبکه:** Packet Tracer می تواند برای آموزش مفاهیم شبکه به دانشجویان، متخصصان شبکه و علاقه مندان به شبکه استفاده شود.

- **آزمایش شبکه:** Packet Tracer می تواند برای آزمایش عملکرد شبکه و شناسایی مشکلات شبکه استفاده شود.
- **طراحی شبکه:** Packet Tracer می تواند برای طراحی شبکه های کامپیوتری جدید استفاده شود.

Packet Tracer یک ابزار ارزشمند برای هر کسی است که علاقه مند به یادگیری یا کار در زمینه شبکه است.

قسمت های شبکه بیمارستان

- بخش عمومی (**General ward**): بخش عمومی بیمارستان محلی برای بستری بیمارانی است که به مراقبت های پزشکی عمومی نیاز دارند. این بخش معمولاً دارای تخت های بیشتری نسبت به بخش خصوصی است و هزینه کمتری نیز دارد.

- بخش خصوصی (**Private ward**): بخش خصوصی بیمارستان محلی برای بستری بیمارانی است که به مراقبت های پزشکی ویژه نیاز دارند یا تمایل به پرداخت هزینه بیشتر برای امکانات و خدمات بهتر دارند. این بخش معمولاً دارای تخت های کمتری نسبت به بخش عمومی است و هزینه بیشتری نیز دارد.

- منطقه بالینی (**Clinical Area**): منطقه بالینی بیمارستان محلی است که مراقبت های پزشکی به بیماران ارائه می شود. این منطقه شامل اتاق های عمل، اتاق های بستری، آزمایشگاه ها، اتاق های تصویربرداری و سایر بخش های درمانی است.

- بخش فناوری اطلاعات (**IT Department**): اداره فناوری اطلاعات مسئول مدیریت شبکه کامپیوتری بیمارستان است. این اداره مسئول نصب و نگهداری نرم افزار و سخت افزار کامپیوتری بیمارستان، همچنین امنیت شبکه و دسترسی کاربران به اطلاعات است.

- پذیرش ورودی (**Entrance Reception**): پذیرش ورودی محلی است که بیماران و بازدیدکنندگان هنگام ورود به بیمارستان از آن عبور می کنند. این بخش مسئول ثبت نام بیماران، صدور کارت شناسایی و ارائه اطلاعات عمومی در مورد بیمارستان است.

- لابی و پارکینگ (**Lobby and Parking**): لابی و پارکینگ بخش های عمومی بیمارستان هستند که برای استفاده بیماران، بازدیدکنندگان و کارکنان استفاده می شوند. لابی معمولاً دارای مبلمان، تلویزیون و سایر امکانات رفاهی است. پارکینگ معمولاً در نزدیکی ورودی اصلی بیمارستان قرار دارد.

ارتباطات بین قسمت های شبکه بیمارستان

قسمت های مختلف شبکه بیمارستان با یکدیگر ارتباط دارند تا خدمات پزشکی به بیماران به طور موثر ارائه شود. این ارتباطات معمولاً از طریق شبکه کامپیوتری بیمارستان انجام می شود.

به عنوان مثال، بخش عمومی و بخش خصوصی بیمارستان از طریق شبکه کامپیوتری به سیستم پرونده های پزشکی دسترسی دارند. این امر به پزشکان و پرستاران این امکان را می دهد تا اطلاعات پزشکی بیماران را به اشتراک بگذارند.

منطقه بالینی بیمارستان نیز از طریق شبکه کامپیوتری به سیستم های مانیتورینگ بیمار و تجهیزات پزشکی متصل است. این امر به پزشکان و پرستاران این امکان را می دهد تا وضعیت بیماران را به طور مداوم کنترل کنند.

بخش فناوری اطلاعات نیز از طریق شبکه کامپیوتری به سایر قسمت های بیمارستان متصل است. این امر به این بخش امکان می دهد تا نرم افزار و سخت افزار کامپیوتری بیمارستان را مدیریت کند و امنیت شبکه را تضمین کند

در این توپولوژی شبکه، گره ها (یعنی رایانه ها، سوئیچ ها، روترها یا سایر دستگاه ها) از طریق پیوندها (کابل سیم مسی جفت تابیده - twisted pair - یا کابل فیبر نوری) به یک شبکه محلی (LAN) و شبکه متصل می شوند.

ما همچنین از SSH برای امنیت استفاده کرده ایم. الزامات شبکه ما شامل دستگاه های شبکه مانند روترها، سوئیچ ها، سرور است.

پیکر بندی

در نمودار دیاگرام، قسمت های مختلف به طور مناسب توضیح داده شده. دیاگرام به 6 قسمت که بالاتر به آن ها اشاره شد، تقسیم شده. در ادامه، پیکربندی اتصالات این بخش ها به یکدیگر آمده است:

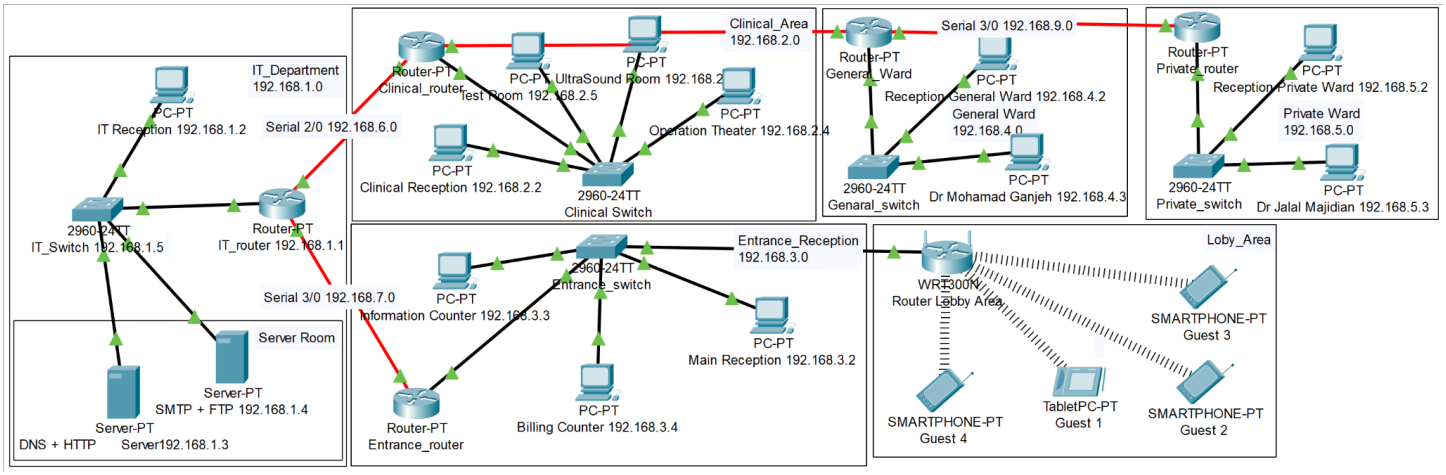
General Ward Switch	General Ward Router
Private Ward Switch	Private Ward Router
Clinical Area Switch	Clinical Area Router
IT Department Switch	IT Department Router
Entrance Switch	Entrance Router

در این شبیه سازی از 5 سویچ **2960**، 5 روتر برای اتصال Area های مختلف به یکدیگر، یک روتر بی سیم برای بخش انتظار، دو سرور در اتاق سرور بخش IT، و چندین گره یا Node به عنوان کلاینت استفاده شده.
در هر یک از بخش های تعریف شده، یک بخش پذیرش وجود دارد که از کلاینت PC استفاده شده.
نکته) بخش لابی هنوز به صورت عملی در بیمارستان پیاده سازی نشده.
نکته) دوربین های مدار بسته و پرینتر ها به منظور پرهیز از پیچیدگی، لحاظ نشده.

تعریف مفاهیم:

- **DHCP**: پروتکل تنظیم پویای میزبان (DHCP) یک پروتکل مدیریت شبکه است که در شبکه‌های UDP/IP استفاده می‌شود. سرور DHCP به طور پویا یک آدرس IP و سایر پارامترهای تنظیمات شبکه را به هر دستگاه در شبکه اختصاص می‌دهد تا آن‌ها بتوانند با دیگر شبکه‌های IP ارتباط برقرار کنند.
- **DNS**: سامانه نام دامنه (DNS) یک سیستم نامگذاری سلسله مراتبی و غیرمتمرکز برای رایانه‌ها، سرویس‌ها یا منابع دیگری است که به اینترنت یا یک شبکه خصوصی متصل هستند.
- زیرشب (**Subnet**): زیرشبکه یا subnet، یک بخش‌بندی منطقی از یک شبکه IP است. فرآیند تقسیم یک شبکه به دو یا چند شبکه را subnetting می‌گویند.
- **HTTPS**: پروتکل انتقال ابرمتن امن (HTTPS) یک توسعه از پروتکل انتقال ابرمتن (HTTP) است. از آن برای ارتباط امن در شبکه‌های رایانه‌ای استفاده می‌شود و به طور گسترده در اینترنت کاربرد دارد.
- **SSH**: پوسته امن (SSH) یک پروتکل رمزنگاری شبکه برای اداره و استفاده از سرویس‌های شبکه به صورت امن در شبکه‌های غیر امن است.
- **SMTP**: پروتکل ساده انتقال نامه (SMTP) یک پروتکل ارتباطی برای انتقال ایمیل است.
- **FTP**: پروتکل انتقال فایل (FTP) یک پروتکل شبکه استاندارد است که برای انتقال فایل‌های رایانه‌ای بین یک کلاینت و سرور در یک شبکه رایانه‌ای استفاده می‌شود.
- **WIFI**: وای‌فای نام فناوری شبکه بی‌سیم است که از امواج رادیویی برای ارائه اینترنت پرسرعت بی سیم و اتصالات شبکه استفاده می‌کند.
- **VLSM**: ماسک زیرشبکه با طول متغیر (VLSM) یک استراتژی طراحی برای زیرشبکه ها است، که در آن قسمت‌های مختلف یک شبکه بزرگتر، می‌توانند ماسک‌های زیرشبکه با اندازه‌های متفاوت داشته باشند. این فرایند که به آن «زیرشبکه بندی زیرشبکه ها(Subnetting subnets)» هم گفته می‌شود، به مهندسین شبکه این امکان را می‌دهد تا برای زیرشبکه های مختلف در یک شبکه کلاس A، B یا C، از ماسک‌های متفاوتی استفاده کنند.

شکل دیاگرام شبکه



سناریو ها

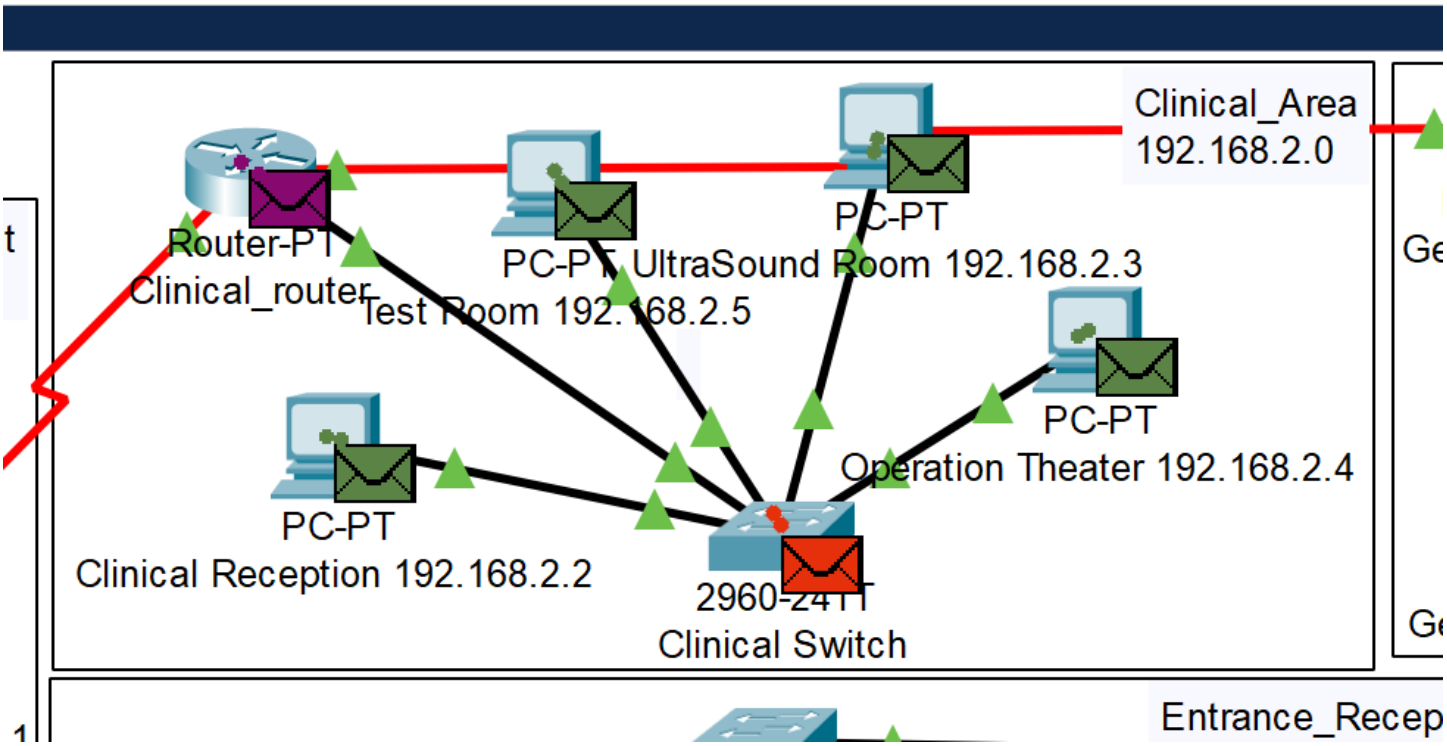
1. سناریو دستور Ping: به منظور پینگ گرفتن از کلاینت ها از بخش IT ایجاد شده. یعنی در Source آدرس IP کامپیوتر IT Reception وارد شده و در بخش destination هر رکورد، مقدار IP کلاینت مقصد. این سناریو به منظور تست کردن برقراری اتصال شبکه کلاینت ها ایجاد شده.

برای تست کردن اتصال، میتوان به صورت Real-time روی دکمه های Fire این رکورد ها کلیک کرد تا به صورت بلادرنگ این تست انجام شود:

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	IT Reception 192.168.1.2	Clinical Reception 192.168.2.2	ICMP		0.000	N	0	(edit)	
	Successful	IT Reception 192.168.1.2	Test Room 192.168.2.5	ICMP		0.000	N	1	(edit)	
	Successful	IT Reception 192.168.1.2	192.168.2.3	ICMP		0.000	N	2	(edit)	

همچنین می توان از منوی گوشه سمت راست و پایین، در حالت Simulation این عمل را انجام داد. در این صورت رکورد های سناریو یکی پس از دیگری اجرا شده و شکل ارسال Packet ها به صورت انیمیشن ترسیم می شود:



نکته ها

- در اولین بار هر تست Failed می شود تا اتصال برقرار شود و طرفین یکدیگر را بشناسند.
- همونطور که مشاهده می کنید، Packet بعد از رسیدن به سوئیچ، به صورت Broadcast در شبکه محلی خود پخش می شود تا بسته میزبان خود را پیدا کند.
- پس از رسیدن بسته به مقصد، یک Packet از نوع Acknowledge به مبدا ارسال می شود.
- برای هر رکورد سناریو، میتوان رنگ بخصوصی انتخاب کرد تا در زمان شبیه سازی، به منظور شناسایی بهتر، بسته ی ارسالی به همان رنگ ترسیم شود

امنیت پورت های میکروتیک

میکروتیک یک روتر و سوئیچ شبکه است که معمولاً در شبکه های کوچک و متوسط استفاده می شود. میکروتیک دارای پورت های مختلف است که می توانند برای اهداف مختلف استفاده شوند.

برای افزایش امنیت میکروتیک، باید پورت های غیرضروری را ببندید. این کار می تواند به جلوگیری از دسترسی غیرمجاز به دستگاه و شبکه کمک کند.

برای بستن پورت های میکروتیک، مراحل زیر را دنبال کنید:

1. به کنسول میکروتیک وارد شوید.
2. دستور زیر را وارد کنید:

```
ip firewall filter/
```

3. یک لیست فیلتر جدید ایجاد کنید.

```
"add chain=input action=drop comment="Block all ports
```

4. پورت هایی را که می خواهید مسدود کنید، به لیست فیلتر اضافه کنید.

```
add chain=input src-port=80 action=drop
add chain=input src-port=443 action=drop
```

5. تنظیمات را ذخیره کنید.

```
save/
```

با انجام این کار، تمام ترافیکی که از پورت های 80 و 443 می آید، مسدود می شود. این شامل ترافیک HTTP و HTTPS است.

نتیجه‌گیری

این گزارش نحوه طراحی توپولوژی شبکه‌ی بیمارستان (سیستم مدیریت سلامت) را شرح می‌دهد. با استفاده از VLSM برای زیر Subneting، دیاگرام را به ۵ بخش مجزا تقسیم کردیم. این توپولوژی همچنین می‌تواند در سطوح بالاتر بیمارستان‌ها نیز پیاده‌سازی شود.