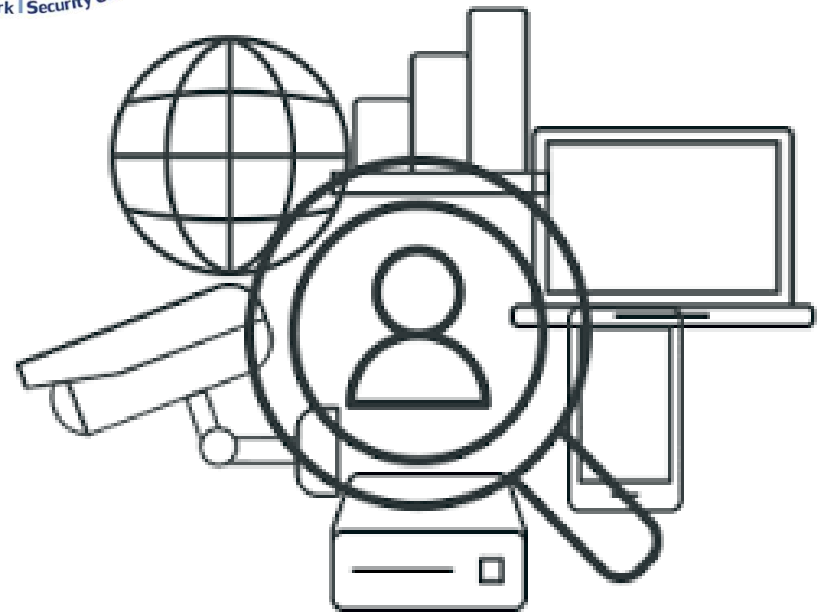
برگزار کننده :
اتحادیه سراسری
شرکت های فنی مهندسی
حفاظت الکترونیک و
شبکه های ایمنی
بهمن ماه ۱۴۰۲

دوره آموزشی دوربین های نظارت تصویری تحت شبکه

معرفی بخش های ارائه



- ✓ معرفی راه کارهای ذخیره سازی تصاویر
- ✓ دسته بندی نرم افزارها از نظر وسعت عملکردی
- ✓ معرفی کمپانی های تولید کننده نرم افزارهای نظارت تصویری
- ✓ پروتکل و ارتباطات شبکه ای در نرم افزارها
- ✓ ساختار نرم افزارهای نظارت تصویری
- ✓ انتخاب و نحوه محاسبه سخت افزارها و بهینه سازی آن ها
- ✓ مشکلات و رخداد در نرم افزارها
- ✓ امنیت در نرم افزارها
- ✓ مدیریت و نگهداری داده ها
- ✓ برخی از ویژگی های نرم افزارهای مدیریت تصاویر

راه کارهای ذخیره سازی و مدیریت تصاویر

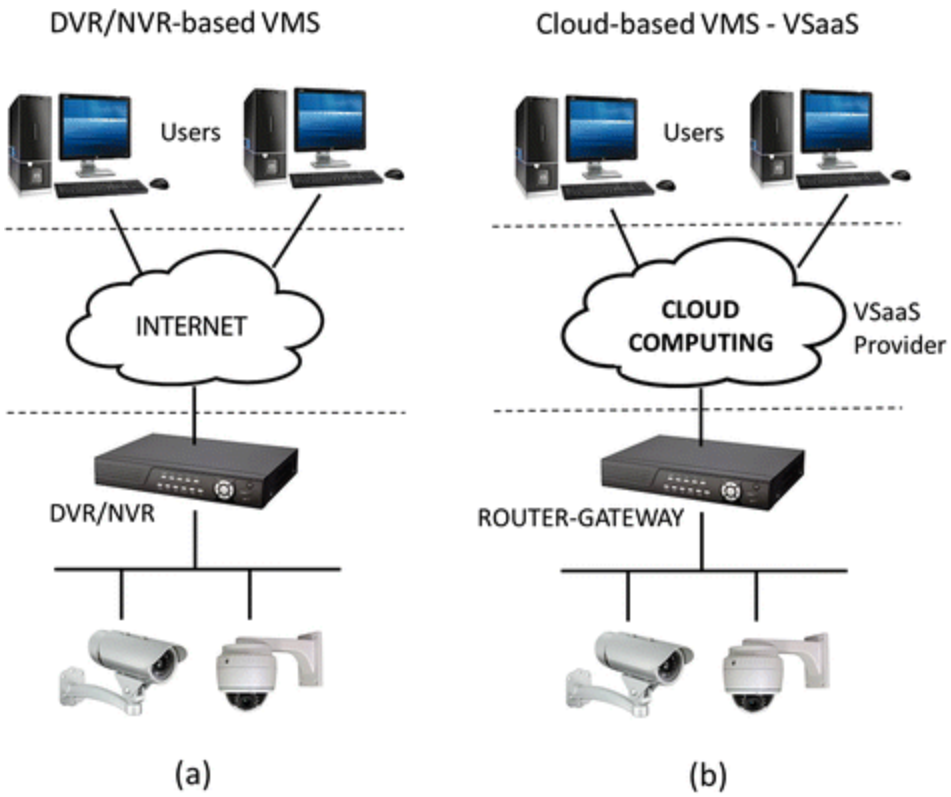
سیستم های ذخیره ساز و مدیریت تصاویر

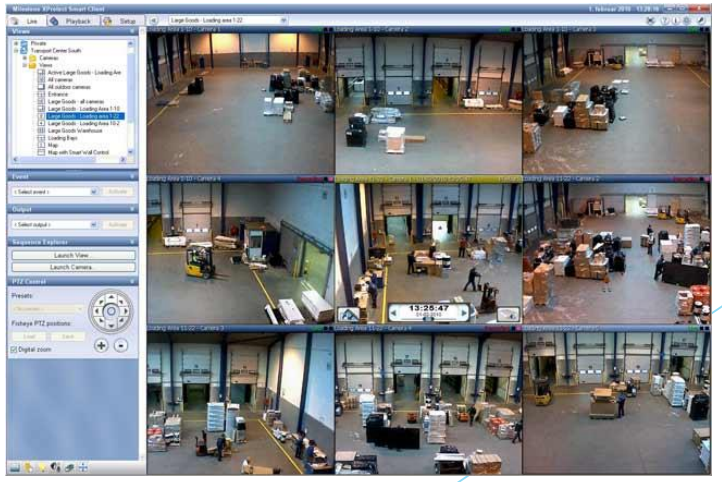
سامانه مدیریت تصاویر

پس از تولید و انتقال تصویر حال نیاز به ذخیره سازی برای چک کردن مجدد و استفاده از آرشیو جهت سند و مدرک می باشد

این سامانه آخرین و اصلی ترین بخش در این سیستم ها می باشند زیرا تمامی اطلاعات و وقایع ثبت شده توسط دوربین ها در این بخش ضبط و نگهداری می شوند.

انتخاب ساختار این بخش بر اساس نیازمندی های پروژه و مقیاس آن از نظر تعداد دوربین و دیگر تجهیزات می باشد





سیستم های ذخیره ساز و مدیریت تصاویر

تاریخچه رکوردرها

اصلی ترین عاملی که باعث پیدایش این سیستم ها گردید ، به وجود آمدن سیستم ضبط VCR می باشند که در ابتدای دهه ۱۹۷۰ کمک به پیدایش این سیستم ها نمود.

VCR مخفف کلمه Video Cassette Recorder می باشد

این دستگاه بر پایه آنالوگ روی کاست تصاویر را ضبط می‌کند.

این سیستم تا دهه ۱۹۹۰ میلادی پرچمدار بازار صوتی و تصویری بود.

دستگاه VCR بر پایه آنالوگ تصاویر را ضبط می‌کند و همانطور که از نام آن پیداست روی کاستCassette یا نوار ویدویی تصاویر ضبط می‌شود.

در این سیستم از یک نوار مغناطیسی عریض ۱۲.۷ میلی‌متری استفاده می‌شود که قادر است تا حدود ۶ ساعت ویدیو با رزولوشن ۲۴۰×۴۸۶ ضبط کند

سیستم های ذخیره ساز و مدیریت تصاویر

معایب سیستم های VCR

با پیشرفت تکنولوژی هر روز سیستم‌های جدید به دلیل قابلیت‌های قدرتمندتر ، سیستم‌های قدیمی را از رده خارج می نمایند.

استفاده از VCR ها محدودیت هایی را موجب می شد که شامل موارد زیر می گردید:

- مدت زمان محدود ضبط
- عمر نوارهای ویدیویی
- بالا رفتن تعداد نوارهای ویدیویی و نگهداری از آن‌ها
- حساسیت نوارهای مغناطیسی و امکان از دست دادن اطلاعات

سیستم های ذخیره ساز و مدیریت تصاویر

دسته بندی سیستم های مدیریت و ذخیره ساز تصویر

تجهیزات ذخیره ساز دیجیتالی یا DVR(Digital Video Recorder)

تجهیزات ذخیره ساز دیجیتالی تحت شبکه یا NVR(Network Video Recorder)

تجهیزات ذخیره ساز سرور و نرم افزار یا CMS(Central Management System) یا VMS(Video Management System

سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر دیجیتالی تحت شبکه NVR

دستگاه NVR از نظر ساختار فیزیکی همانند DVR بوده و تنها نوع و تعداد پورت های آن متفاوت می باشد

دستگاه های NVR ورودی تصاویر را توسط پورت شبکه دریافت می کنند لذا در قسمت پشتی پنل هیچ پورت ورودی آنالوگ تصویر وجود ندارد

برخی از دستگاه های NVR قابلیت PoE یا تغذیه دوربین ها از طریق بستر شبکه را دارند که در این حالت چند پورت شبکه در پنل پشت قرار دارند تا هر پورت یک دوربین را راه اندازی نماید

در این مدل از دستگاه ها یک سوئیچ در داخل یک NVR قرار داده شده تا علاوه بر عملکرد به عنوان یک ذخیره ساز قابلیت ارتباط دهی شبکه را نیز دارا باشد

سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر دیجیتالی NVR

انتخاب دستگاه NVR :

تعداد کانال ورودی تصویرکه به صورت ۴ ، ۸ ، ۹ ، ۱۶ ، ۳۲ ، ۶۴ ، ۱۲۸ و ۲۵۶ کانال می باشند

رزولوشن نمایش تصاویر قابل پشتیبانی از ورودی که با استاندارد ۲ ، ۴ ، ۵ ، ۸ و ۱۲ مگاپیکسل می باشند

رزولوشن ذخیره سازی تصاویر که با استاندارد ۲ ، ۴ ، ۵ ، ۸ و ۱۲ مگاپیکسل می باشند

استاندارد های خواندن داده های فشرده شده تصاویر H.264 ، H.264+ ، H.265 و H.265+

تعداد و ظرفیت هارد دیسک قابل پشتیبانی

دارا بودن انتقال تصویر ابری یا P2P

قابلیت های هوشمند در پردازش تصاویر توسط دستگاه

دارا بودن قابلیت PoE

قابلیت Raid بندی

سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر بر اساس سرور و نرم افزار CMS & VMS

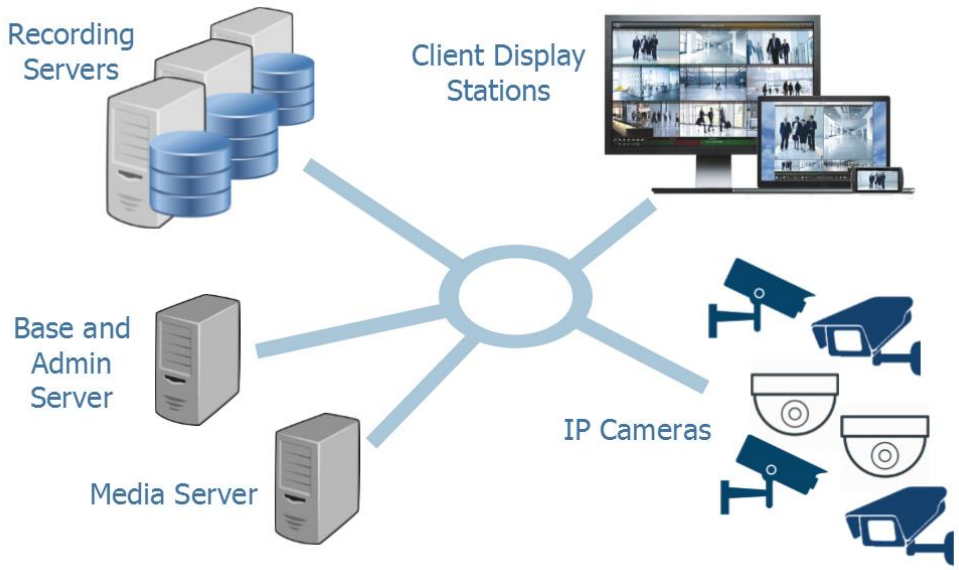
- ✓ در روش مدیریت و ذخیره سازی از یک سخت افزار با مشخصات فنی دلخواه (متناسب با حجم پروژه) و یک نرم افزار به طور جداگانه استفاده می شود

- ✓ انتخاب سخت افزار متناسب با چند فاکتور مانند : تعداد دوربین ، پهنای باند ورودی و خروجی ، نوع سیستم ذخیره سازی و محدودیت های نرم افزار صورت می گیرد
- ✓ این ساختار مدیریتی معمولا به صورت سرور و کلاینت می باشند یعنی یک سرور سرویس دهنده نرم افزار است و کامپیوتر دیگر که کلاینت نامیده می شود سرویس گیرنده می باشد
- ✓ تمامی سرویس ها بر روی بستر شبکه انجام می پذیرد

سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر بر اساس سرور و نرم افزار CMS & VMS

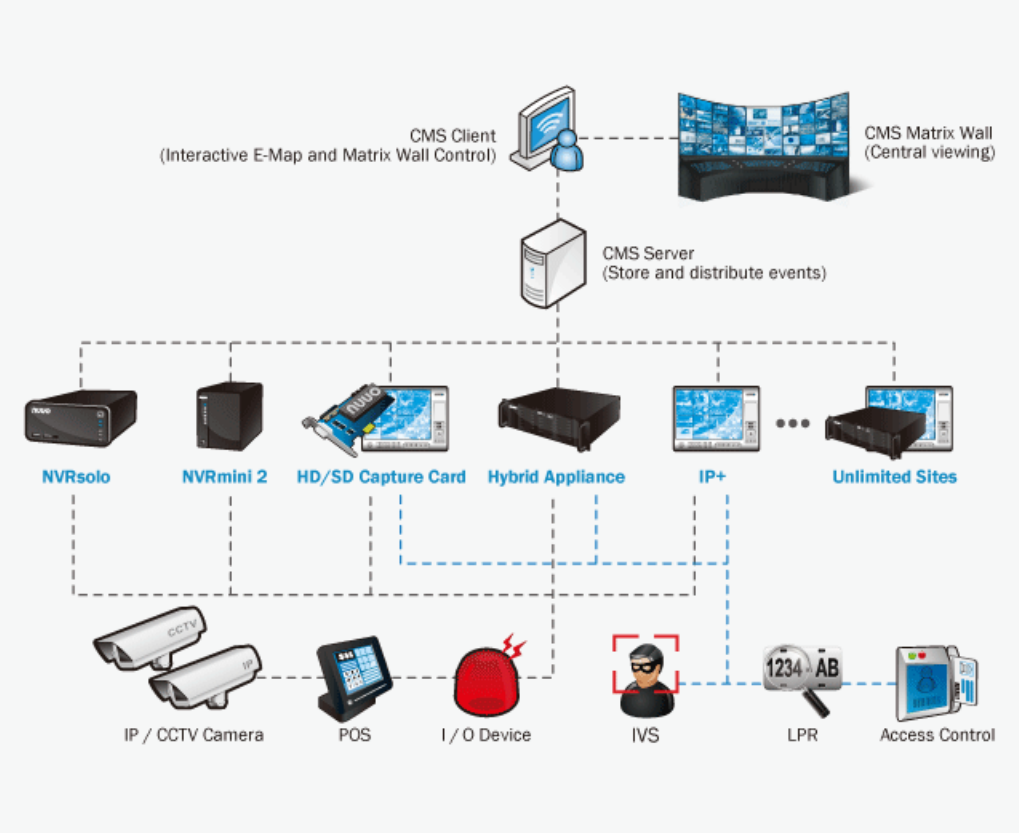
- ✓ این نرم افزار ها با دو نام VMS و CMS در این صنعت شناخته می شوند
- ✓ VMS مخفف واژه Video Management System می باشد که همان سیستم مدیریت تصاویر می باشد
- ✓ با توجه به دیاگرام دوربین ها استریم تصاویر را به یک بستر مشترک شبکه ارسال می کنند که تمامی سرورها در آن شبکه قرار داشته و پس از دریافت استریم ها آن ها را بر روی ذخیره ساز ها بر اساس یک عملیات رمزنگاری آرشیو می کنند
- ✓ کاربران نیز از طریق نرم افزار گرافیکی کلاینت ها به این شبکه دسترسی داشته و با تایید هویت شناسایی وارد سیستم شده و تنظیمات مربوطه و بررسی تصاویر را انجام می دهند
- ✓ هر یک از فرایندهای ذخیره سازی ، مدیریت تصاویر و کاربران ، تایید هویت ورودی و ... یک سرویس گفته شده که تمامی این سرویس ها بر روی یک پلت فرم نرم افزاری قرار دارد.



سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر بر اساس سرور و نرم افزار CMS & VMS

- ✓ پلت فرم های CMS که مخفف Central Management System یا سیستم مدیریت مرکزی می باشند همانند VMS ها وظیفه مدیریت سیستم را به عهده دارند با این تفاوت که علاوه بر سیستم نظارت تصویری سیستم های امنیتی دیگری نیز در این پلت فرم ها گنجانده شده است.



- ✓ سیستم های نظارت تصویری ، کنترل تردد ، اعلام سرقت و حریق ، مدیریت پارکینگ و ... در ساختار CMS ها قرار دارند.

- ✓ ویژگی این سیستم ها ادغام تمامی سیستم ها در یک پلت فرم می باشد که برای مدیریت آن ها دیگر نیاز به نرم افزارهای مختلف نمی باشد

- ✓ همچنین هوشمند سازی و ترکیب تمامی ویژگی ها در این دسته از سیستم ها به راحتی صورت می پذیرد

سیستم های ذخیره ساز و مدیریت تصاویر

تجهیزات ذخیره ساز و مدیریت تصاویر بر اساس سرور و نرم افزار CMS & VMS

- ✓ ویژگی های استفاده از نرم افزارها شامل:
  - قابلیت استفاده بر روی تمام سیستم عامل ها (عدم محدودیت بر روی یک سیستم عامل خاص)
  - توسعه پذیری آسان سیستم به دلیل قابل تغییر بودن سخت افزار و عدم محدودیت در نرم افزارها
  - به دلیل اسفاده از سخت افزار های قدرتمند و باز بودن پلت فرم های نرم افزاری قدرت موتور جستجو گر نر افزارها نسبت به تجهیزات DVR و NVR بسیار بالاتر می باشد
  - عدم محدودیت در ذخیره سازی به دلیل کارکرد و ارسال اطلاعات بر روی شبکه و دارا بودن سرویس ها نرم افزاری قدرتمند جهت ذخیره سازی اطلاعات
  - باز بودن پلت فرم های نرم افزاری و توسعه و ارتقاء راحت سیستم های نرم افزاری
  - قابلیت ادغام و ترکیب چندین سیستم در یک پلت فرم
  - قابلیت کارکرد با برندهای مختلف و پشتیبانی گسترده از نرم افزارهای Third party

سیستم های ذخیره ساز و مدیریت تصاویر

مقایسه ساختارهای نظارت و مدیریت تصاویر:

مشخصه	DVR	NVR	نرم افزار
قدرت جستجو در تصاویر	پایین	متوسط	بسیار بالا
توسعه پذیری سیستم	خیر	خیر	بلی
دانش و کاربری	ساده	متوسط	سطح دانش بالا
هزینه تمام شده	بسیار پایین	پایین	بسیار بالا
مقیاس پروژه	تعداد کم دوربین	تعداد متوسط	تعداد بالای تجهیزات
تنوع برند	بدون تاثیر	محدود	عدم محدودیت
یکپارچه سازی با دیگر سیستم ها	غیر قابل انجام	بسیار محدود	بسیار ساده

تاریخچه و پیدایش

معرفی برخی از نرم افزارهای نظارت تصویری و ساختار آن ها

Genetec

پیدایش نرم افزار

سال ۱۹۹۷ در مونترال کانادا

زمینه های فعالیت

۱- سیستم نظارت تصویری Video surveillance

۲- سیستم های کنترل ترددAccesses control

۳- سیستم های پلاک خوانLicense plate recognition

گستردگی نمایندگی ها

دارای بیش از ۸۰ نمایندگی در ۶ قاره جهان

Omnicast

Synergis

AutoVu

تاریخچه و پیدایش

معرفی برخی از نرم افزارهای نظارت تصویری و ساختار آن ها

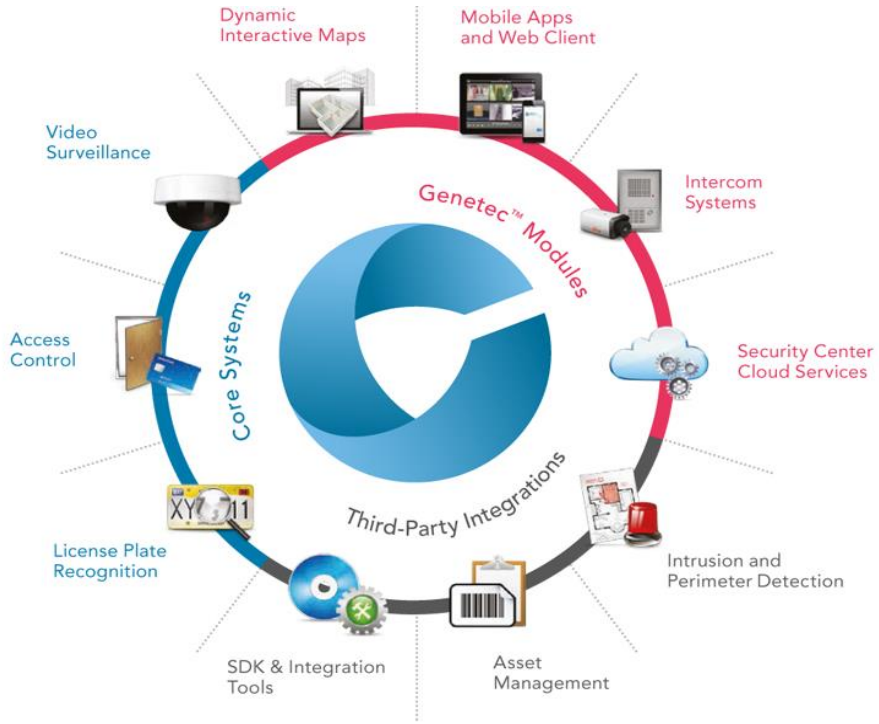
تا سال ۲۰۰۹ این سه ماژول نرم افزار به طور جداگانه توسط این کمپانی عرضه می گردید

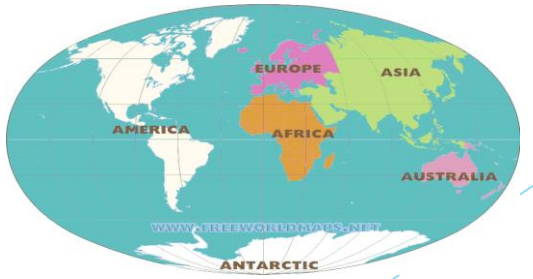
در سال ۲۰۱۰ کمپانی **Genetec** دست به اقدامی بزرگ زده و هر سه پلت فرم نرم افزار را در یک کنسول قرار داده و تحت عنوان **Security Center** وارد بازار نمود

در این پات فرم جدید تمامی امکانات وجود داشته و تنها با فعال سازی لایسنس مربوط به هر پلت فرم امکان استفاده از آن ماژول در نرم افزار فراهم می گردد

کمپانی **Genetec** از نظر گستردگی در نمایندگی و خدمات پس از فروش دارای ۱۵۹ نماینده رسمی در ۶ قاره جهان را دارا می باشد و بیش از ۱۸۰۰ کارمند در این کمپانی مشغول به کار می باشند

این کمپانی در دو کشور کانادا و فرانسه دارای شعبه اصلی می باشد تا بتواند در کل دنیا خدمات مورد نیاز خود را ارائه دهد.

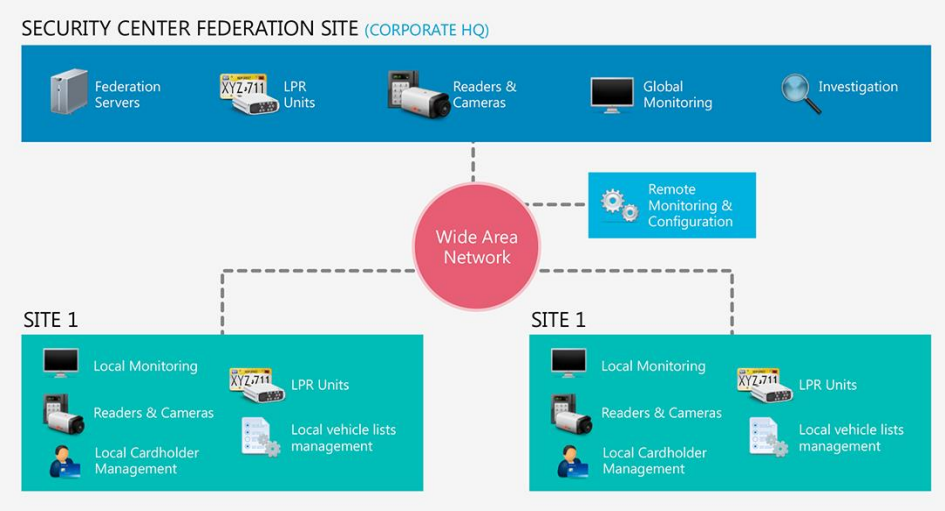




تاریخچه و پیدایش

برخی از ویژگی های نرم افزار Genetec

- ✓ کارکرد در شبکه ها با پروتکل داده های ارسالی مختلف (Multicasting , Unicasting , Broadcasting)
- ✓ دارای امنیت در زیر ساخت های نرم افزار و عدم نفوذ پذیری حتی در لایه های پایین نرم افزار(High Security)
- ✓ دارای امنیت در زیر ساخت های نرم افزار و عدم نفوذ پذیری حتی در لایه های پایین نرم افزار(High Security)
- ✓ هسته قدرتمند نرم افزار در ذخیره سازی و بازیابی اطلاعات و سرعت پردازش بالا
- ✓ فراهم ساختن استفاده نرم افزار با انواع سخت افزار ها و سیستم عامل ها و در نتیجه بهینه سازی اقتصادی در کل سیستم
- ✓ امکان تبادل اطلاعات با سایت های مختلف و به روش های گوناگون (Federation)
- ✓ باز بودن پلت فرم نرم افزار جهت به روز رسانی در کوچکترین موارد مورد نیاز (Modular)
- ✓ دارای خدمات پشتیبانی به صورت ۲۴ ساعت توسط روشهای مختلف در تمام دنیا (SMA)



تاریخچه و پیدایش

معرفی برخی از نرم افزارهای نظارت تصویری و ساختار آن ها

پیدایش نرم افزار

سال ۱۹۹۸ در دانمارک

سال ۱۹۹۹ اولین نسخه نرم افزاری مایلستورن جهت مدیریت تصاویر برای دوربین های آی پی ایجاد گردید

سال ۲۰۰۲ نسخه Xprotect به عنوان یک نرم افزار مدیریت تصاویر Open platform ارائه گردید

سال ۲۰۰۵ اولین نسخه SDK را جهت ارتباط با دیگر نرم افزارها ارائه نمود

سال ۲۰۱۳ اولین NVR بر پایه نرم افزار مایلستون به نام Husky را ارائه نمود

سال ۲۰۲۲ ارائه اولین نسخه Xprotect به صورت Forensic Analytic بر روی دستگاه های Husky و ارتقا آن

سال ۲۰۲۳ ارائه Milestone Kit که یک راه کار در جهت ایجاد VMS بر روی بستر Cloud می باشد

تاریخچه و پیدایش

نسخه های نرم افزار مایلستون

XProtect® Essential+

Supporting up to 8 cameras. Ideal for small businesses

XProtect® Express+

Supporting up to 48 cameras. Designed for smaller, single-site installations with basic security needs

XProtect® Professional+

Supporting an unrestricted number of cameras and servers. Optimized for multi-site companies needing to quickly identify and respond to incidents

XProtect® Expert

Supporting an unrestricted number of cameras. For large-scale installations that require end-to-end protection of video integrity

XProtect® Corporate

Supporting an unrestricted number of cameras. For high-security and mission-critical installations that demand supreme situational awareness of any event and uninterrupted access to live and recorded video

تاریخچه و پیدایش

برخی از ویژگی های نرم افزار مایلستون

مقیاس پذیر بودن نرم افزار

امکان کارکرد و مدیریت بیش از ۱۳۰۰۰ دوربین

استفاده بهینه از منابع سخت افزاری

امکان مدیریت تصاویر وسیستم پلاک خوانی و کنترل تردد توسط یک پلت فرم

قابلیت استفاده از نقشه های آنلاین و از پیش تعریف شده

دارای نرم افزار تحت وب و موبایل (اندروید و آی او اس)

پشتیبانی از نرم افزارهای آنالیتیک

پشتیبانی از دستگاه های POS

تاریخچه و پیدایش

معرفی برخی از نرم افزارهای نظارت تصویری و ساختار آن ها

پیدایش نرم افزار

شرکت اکسون سافت، یک شرکت متخصص درزمینه تولید نرم‌افزار دوربین مداربسته است

دفتر اصلی این شرکت در شهر مسکو قرار دارد

این شرکت دارای ۳۸ دفتر در سراسر دنیا می باشد.

نرم افزار آکسون در دو سری آکسون نکست و آکسون اینتلکت ارائه می شود

سری نکست نرم افزار چهارمین نسخه نرم افزاری هوشمند است که به صورت Open Platform ارائه شده است

از جمله این قابلیت ها می توان به موارد زیر اشاره نمود:

عدم محدودیت در تعداد دوربین، کاربر و سرور؛

برخورداری از تحلیلگر های رایگان؛

پشتیبانی از نقشه های GIS؛

پشتیبانی از لنز های دوربین ۳۶۰ درجه؛

نسخه اینتلکت یک پلتفرم نرم افزار آکسون برای مدیریت اطلاعات مربوط به امنیت فیزیکی (PSIM) فوق العاده پیشرفته است که با استفاده از تجزیه و تحلیل ویدیویی هوشمند، اتصال IP جهانی و قابلیت های اتوماسیون مبتنی بر رویداد ها در یک محیط واحد، ترکیب شده است.

تاریخچه و پیدایش

معرفی برخی از نرم افزارهای نظارت تصویری و ساختار آن ها

digivod
digital video surveillance

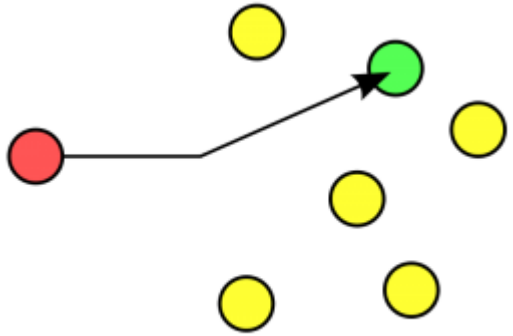
digifort

Security-Vision-Systems
MOBOTIX

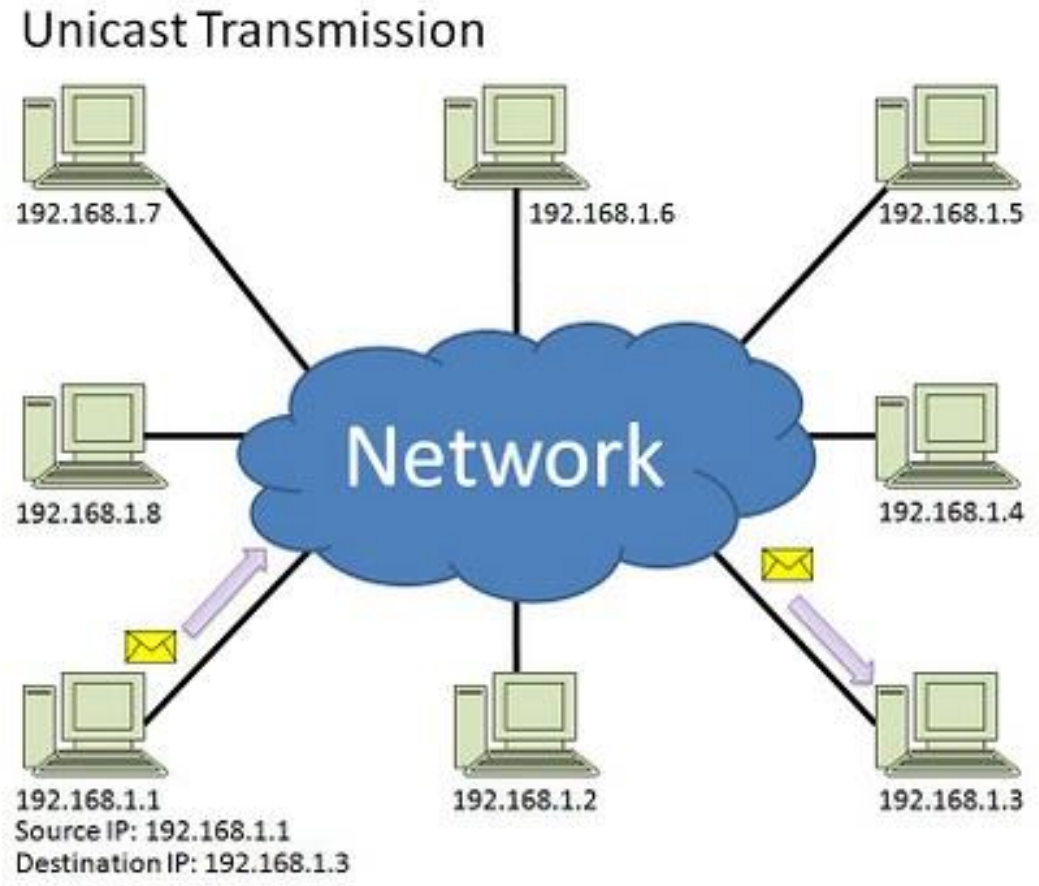
HikCentral

پروتکل و ارتباطات شبکه در نرم افزارها

مفاهیم مقدماتی شبکه های کامپیوتری



- Unicast
  UDP/TCP



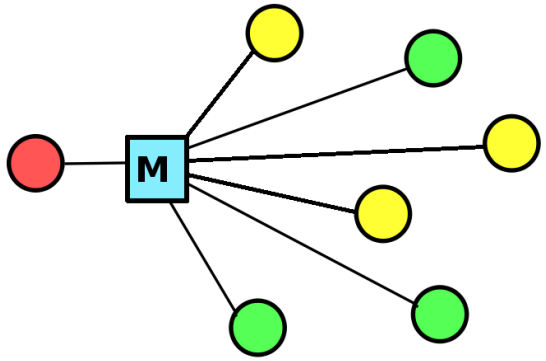
روش های ارتباط داده یا پکت در شبکه های کامپیوتری

به مجموعه پیام هایی که دستگاه ها را قادر می سازد داده های Multicast IP را به یکدیگر ارسال کنند IGMP گفته می شود.

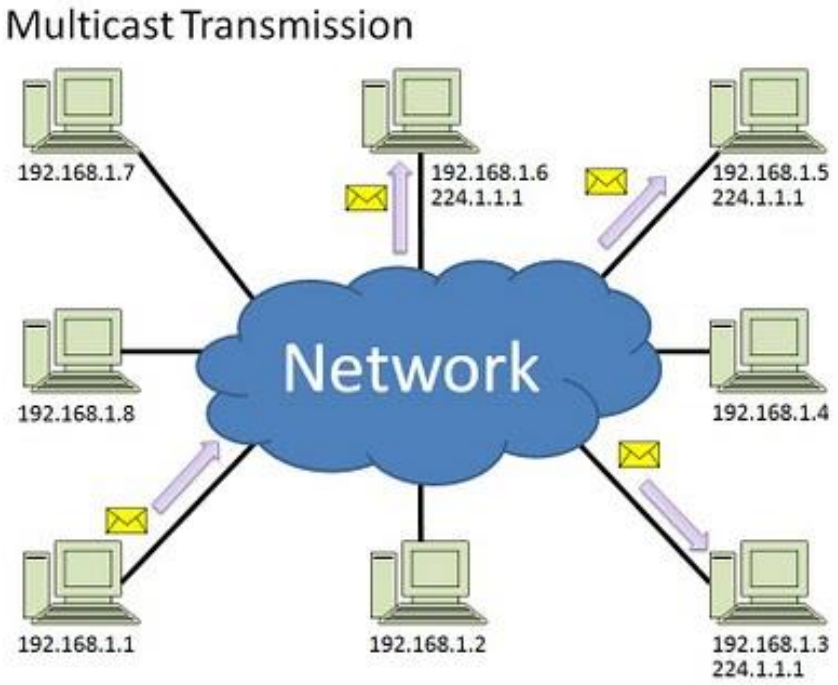
IGMPمخفف پروتکل مدیریت گروه اینترنتی است.

این پیام ها به دستگاه های موجود در شبکه این امکان را می دهد تا خود را به گروه ها اضافه یا از بین ببرند ، هر گروه دارای آدرس گروهی خاصی است.

Multicast عملکرد شبکه شما را بهینه می کند. از آنجا که فقط یک جریان داده Multicast ارسال می شود، پهنای باند را در شبکه شما حفظ می کند و افزایش ترافیک را از بین می برد



- Multicast

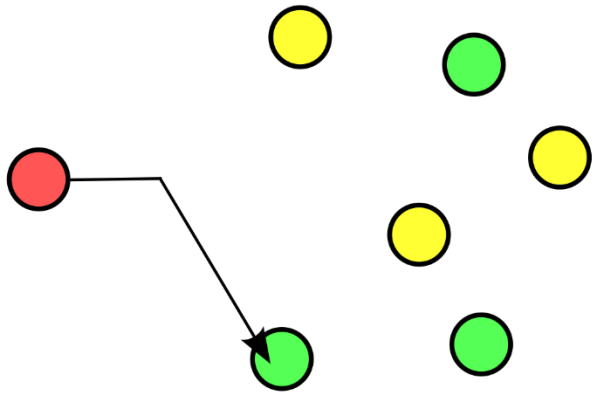


روش های ارتباط داده یا پکت در شبکه های کامپیوتری

براساس این فناوری، یک IP می‌تواند به دو یا چند سرور اختصاص داده‌شود، به صورتی که همه سرورها به صورت همزمان در شبکه قابل دسترس باشند

مزیت این فناوری در انتخاب بهترین مسیر، به‌وسیله مسیریاب‌ها (Routers) برای دسترسی به سرور مورد نظر است

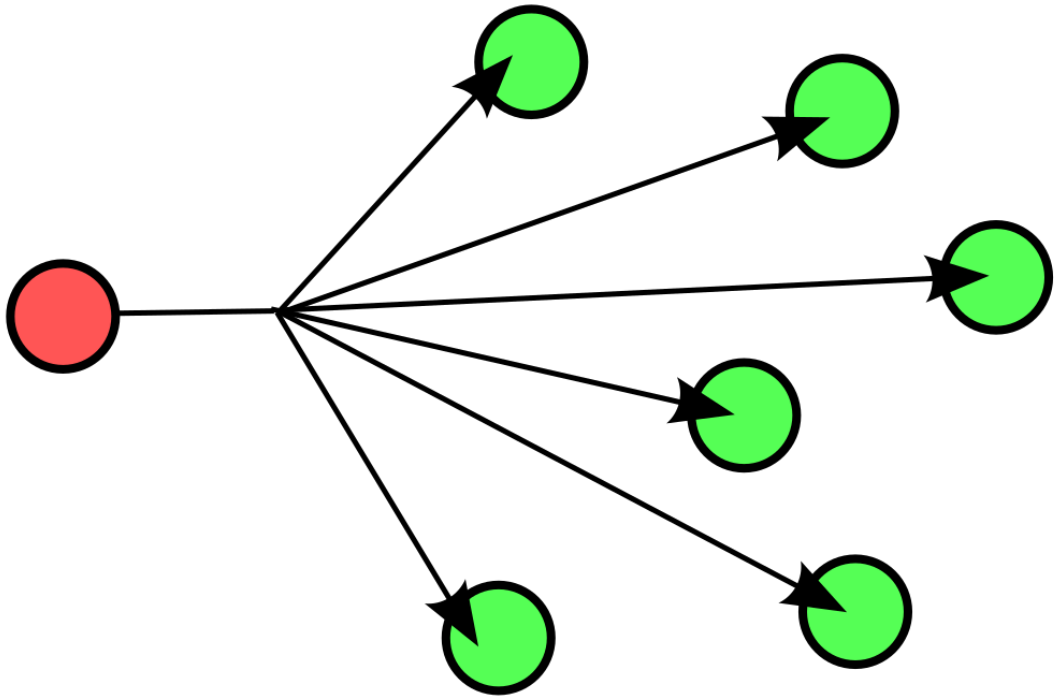
ین تکنیک شبکه‌سازی، به دستگاه‌های متعددی اجازه می‌دهد یک آدرس IP یکسان را با هم به اشتراک بگذارند. براساس مکان درخواست کاربر، مسیریاب‌ها آن را به نزدیک‌ترین دستگاه در شبکه ارسال می‌کنند



- Anycast

روش های ارتباط داده یا پکت در شبکه های کامپیوتری

در این حالت اطلاعات برای تمامی هاست ها در شبکه ارسال می شود



- Broadcast

مفاهیم مقدماتی شبکه های کامپیوتری

Telnet

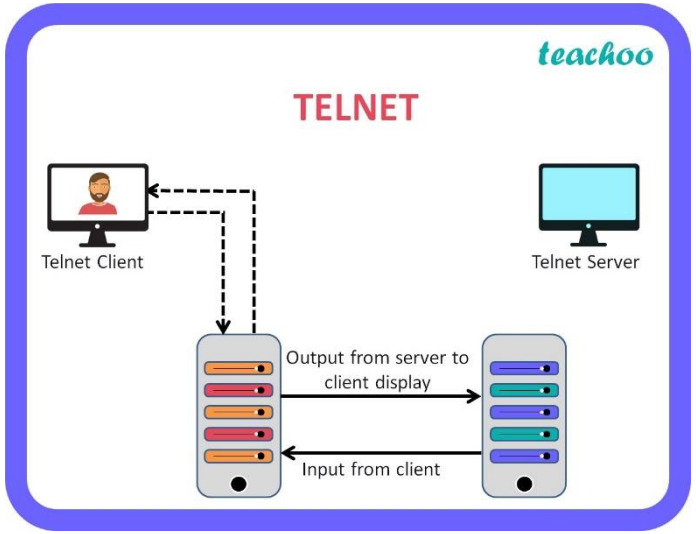
تلنت (Telnet) به عنوان یک پروتکل شبکه از دهه ۱۹۶۰ شروع به توسعه کرد

نوعی پروتکل شبکه است که برای دسترسی به کامپیوترهای راه دور از طریق اینترنت یا شبکه‌های محلی استفاده می‌شود

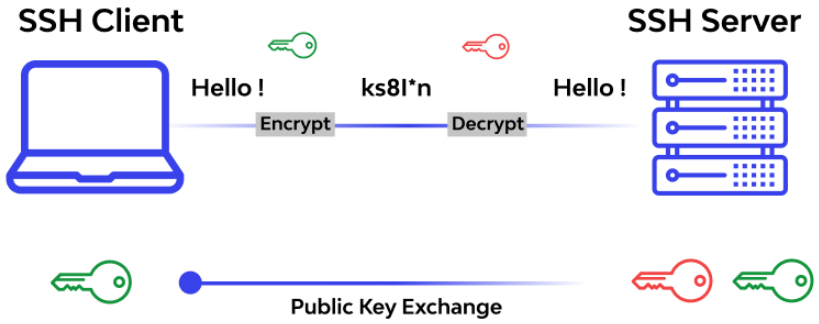
این پروتکل به کاربر اجازه می‌دهد تا به‌عنوان یک کاربر مجازی در کامپیوتر به صورت ریموت وارد شده و دستوراتی را که می‌خواهد اجرا کند و با سیستم‌عامل کامپیوتر از راه دور تعامل داشته باشد.

این پروتکل برای ارتباط با دستگاه‌هایی که دارای command-line interface یا همان رابط خط فرمان (CLI) هستند، مانند روترها، سوییچ‌ها، سرورها و دستگاه‌های شبکه، استفاده می‌شود

تلنت به دلیل نداشتن امنیت کافی، به طور گسترده‌ای توسط پروتکل‌های امن‌تری مانند SSH (Secure Shell)جایگزین شده است



پورت ارتباطی تلنت ۲۳ و پورت ارتباطی SSH عدد ۲۲ می باشد

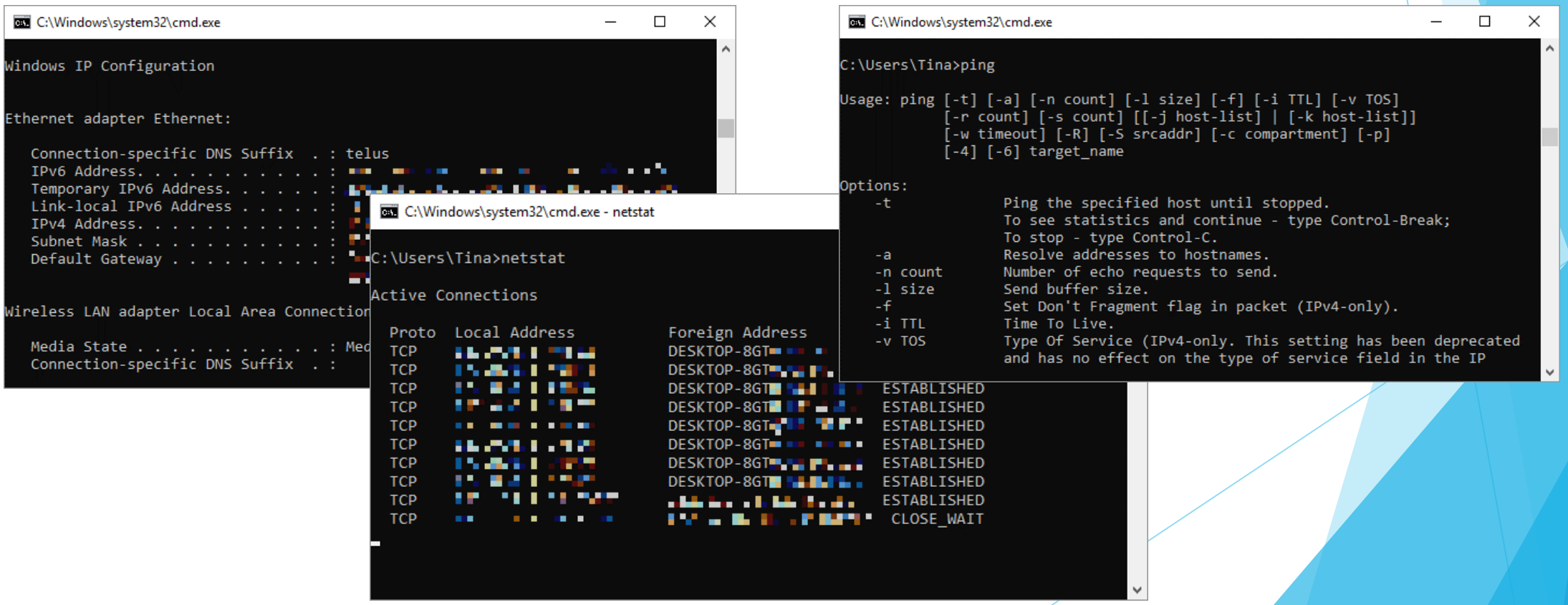


مفاهیم مقدماتی شبکه های کامپیوتری

Command prompt

CMD به معنای خط فرمان است و در واقع یک برنامه دستوری است که به وسیله آن می توان دستورات مورد نظر را اجرا کرد

در سیستم عامل های مختلف خط فرمان یا همان دستورات CMD در یک رابط کاربری متنی اجرایی می‌شوند



ساختار نرم افزارهای نظارت تصویری

ساختارنرم افزارهای نظارت تصویری

سرور های مدیریتی

هسته اصلی نرم افزارها را تشکیل می دهند و بر اساس نوع سیستم دارای سرویس دهنده های بسیاری در جهت مدیریت و حفاظت می باشند

برخی از این سرویس ها شامل : مدیریت لایسنس ها ، مدیریت کاربران و سطوح دسترسی آن ها ، مدیریت و آرشیو بندی تصاویر ، تنظیمات سیستمی ، مدیریت پایگاه های داده و ...

سرور های کارگذار

مسئولیت ارتباطات سرور اصلی و ماژولها، مدیریت ذخیره سازی و نیز مدیریت آلارمهای مربوط به کلیه **Device** ها از قبیل دوربین ها را بر عهده دارد

بطورکلی وظایف این بخش از سیستم به شرح زیر می باشد: ذخیره سازی داده های تصویری، صوتی و نیز متا دیتا و نیز بازیابی این داده های از دوربینها ، ایجاد امکان دسترسی به تصاویر زنده و ذخیره سازی شده ، ایجاد امکان دسترسی و نمایش وضعیت سخت افزارهایی از قبیل دوربین ، مدیریت آلارمها

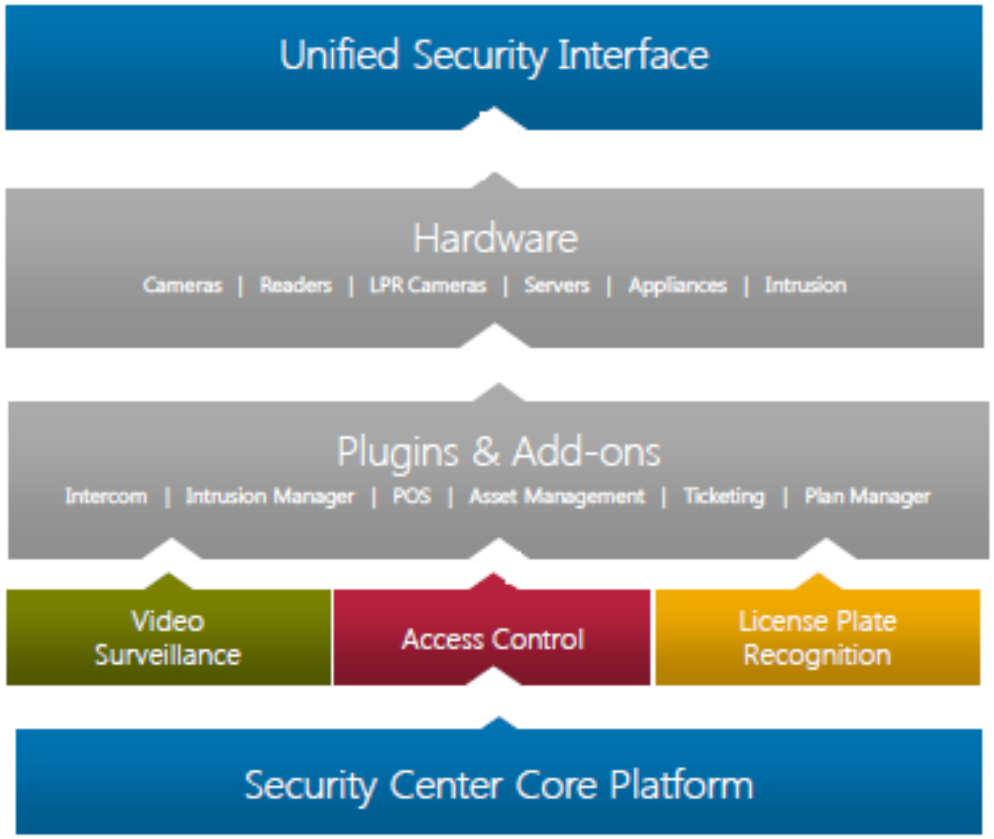
کلاینت یا سرویس گیرنده

کلاینت‌ها به عنوان استفاده‌کننده نهایی سیستم شناخته می‌شوند. نقطه خروجی کلیه سرویس‌ها، اطلاعات و نقطه ارتباطی کاربر نهایی با سیستم، کلاینت می‌باشد.

به طور کلی ساختار سرور و نرم افزار به این صورت می باشد که سرور ها سرویس داده و همانند که واحد Master عمل می کنند و کلاینت ها سرویس دریافت کرده و به عنوان یک Slave عمل می نمایند

لایه های نرم افزار

ساختار پلت فرم نرم افزار



لایه نرم افزاری جهت یکپارچه سازی

لایه سخت افزاری از قبیل دوربین ها و ...

پلت فرم نرم افزاری جهت ادغام برخی نرم افزار ها با نرم افزار Genetec

هسته اصلی نرم افزار که یکپارچه سازی سیستم نظارت تصویر ، کنترل تردد و پلاک خوانی در آن قرار دارد

بررسی رول های نرم افزار

Default Server Roles

Roleچیست؟

یک ماژول نرم افزاری است که وظیفه انجام یک عملکرد منحصر به فرد را در نرم افزار دارا می باشد

Role های پیش فرض در نرم افزار

Directory

این رول بالا ترین سطح را دارا می باشد. توسط این رول سرور اصلی تشخیص داده می شود.از وظایف این رول می توان به : مدیریت لایسنس ، دسترسی و ارتباط کلاینت ها و ... اشاره نمود.

Archiver

این رول برای سیستم نظارت تصویری به کار می رود. این رول جهت فرمان و پیکر بندی دوربین ها مورد استفاده قرار می گیرد.

Media Router

این رول نیز برای سیستم نظارت تصویر مورد استفاده قرار می گیرد. این رول یک مسیر برای ارسال Stream های صدا و تصویر از مبدا به مقصد ایجاد میکند.

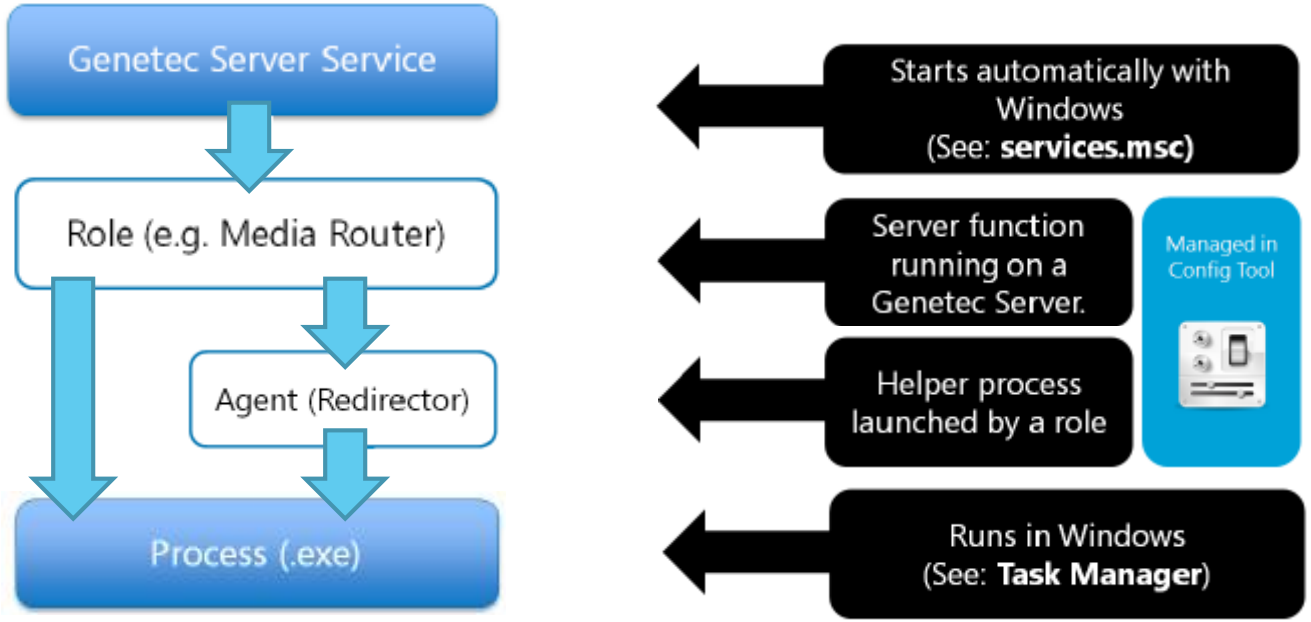
بررسی رول های نرم افزار

Additional Server Roles

رول تجمیع
چند سیستم با یکدیگر

رول آرشیو کمکی

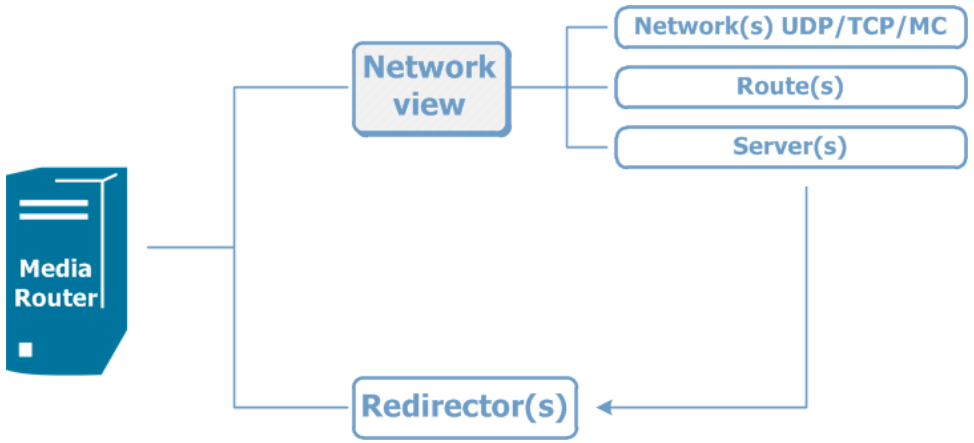
رول پلاگین های خارجی



ساختار عملکرد رول ها در نرم افزار

مفهوم Media Routing

Media Router یک رول در نرم افزار Security Center می باشد که وظیفه آن مشخص ساختن بهینه ترین مسیر Route برای ارسال Stream از مبدا که Archiver بوده به مقصد که کلاینت ها می باشد

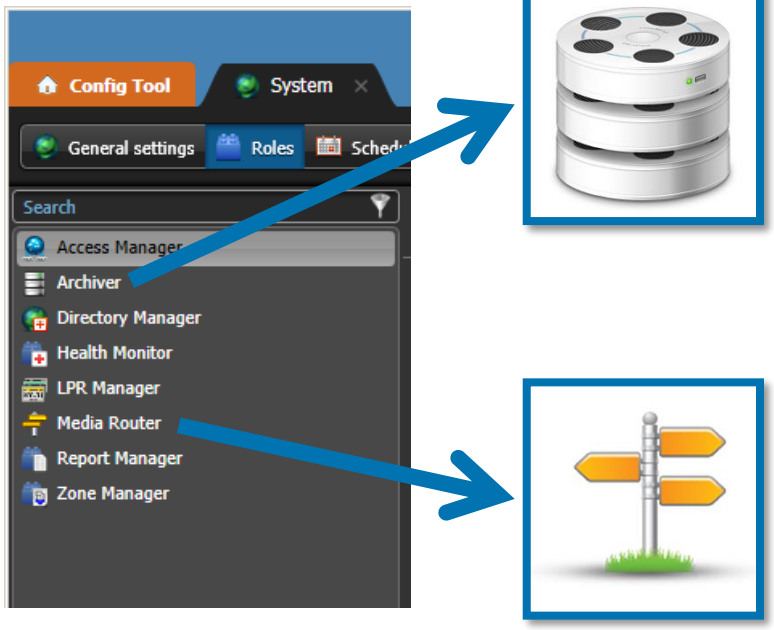


Media Router برای عملکرد بهتر رول شبکه یا Network در نرم افزار را در نظر می گیرد

بخش Network view توصیف کننده توانایی های درون شبکه ای نرم افزار برای مسیریابی بین شبکه ها و سرورهای در دسترس می باشند

وقتی که نیاز به Redirector می باشد ، Media Router به Redirector Agent مناسب بر روی سرور فرمان ارسال پکت ویدئو به یک آدرس آی پی مشخص در مقصد توسط یک پروتکل ارتباطی مشخص مانند TCP/UDP/Mul را می دهد

مفهوم Media Routing



Archive ها ویدئوها را از دوربین دریافت می کنند

هر رول Archiver دارای یک Redirector می باشد

Redirectorها دستوراتی را از Media Router دریافت می کنند که به آنها دستور می دهد تا Stream های ویدئویی را به مقصدهای خاصی ارسال کنند.

Media Router معمولا در سرور اصلی یافت می شود

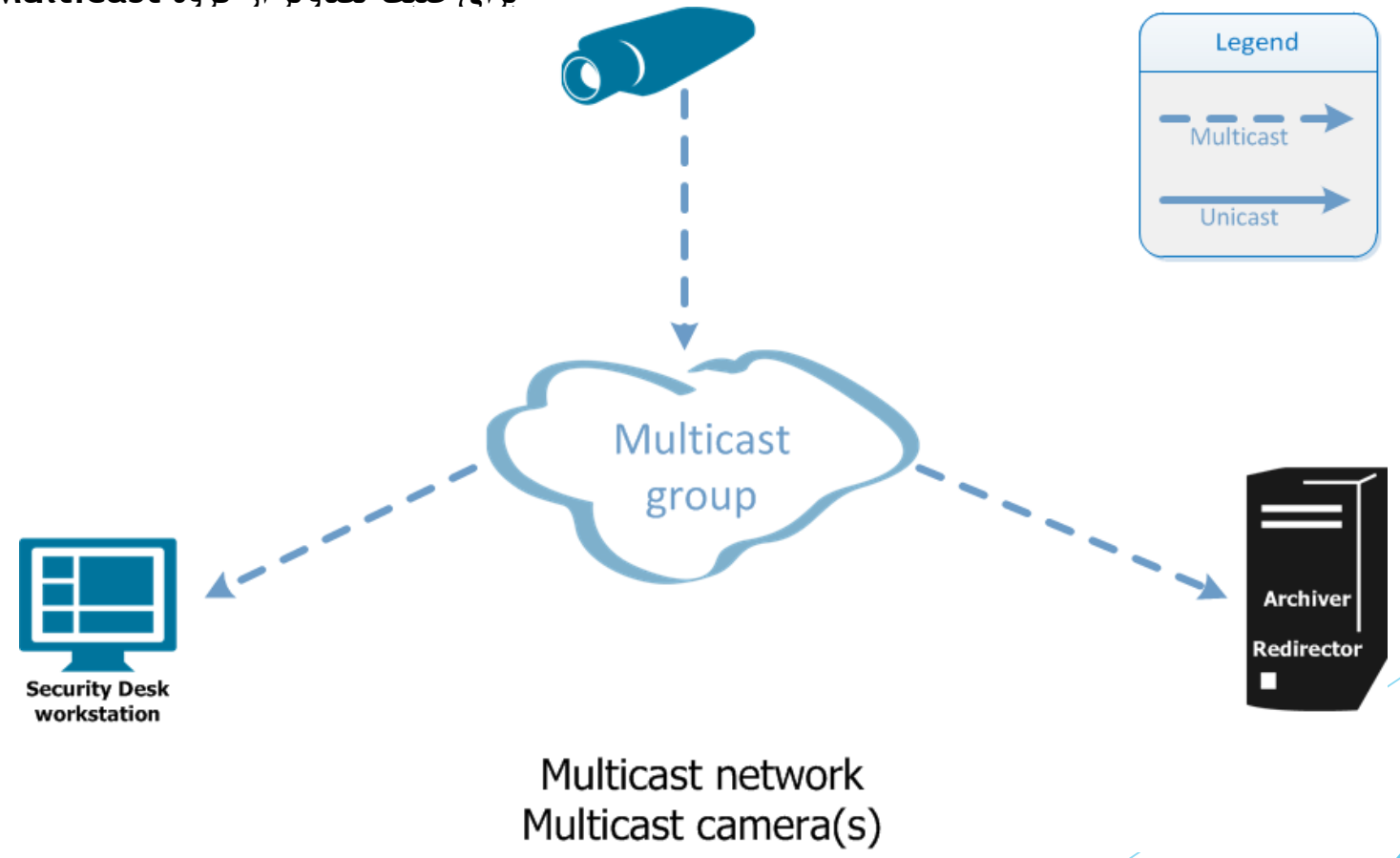
Media Router یک رول یا سرویس نرم افزاری می باشد

رول Media Router مشخص کننده بهینه ترین مسیر برای ارسال Stream از مبدا که Archiver بوده به مقصد که کلاینت می باشد

مفهوم Media Routing

در شبکه هایی که از قابلیت Multicast استفاده می کنند Redirection برای Video نیاز نمی باشد که Stream های دوربین را به صورت Multicast ارسال کنند

در این سناریو دوربین تولید داده بر اساس بستر Multicast داشته و نرم افزار کلاینت به گروه Multicast پیوسته می شود در حالی که Archiver برای ضبط تصاویر از گروه Multicast استفاده می کند



مفهوم Media Routing

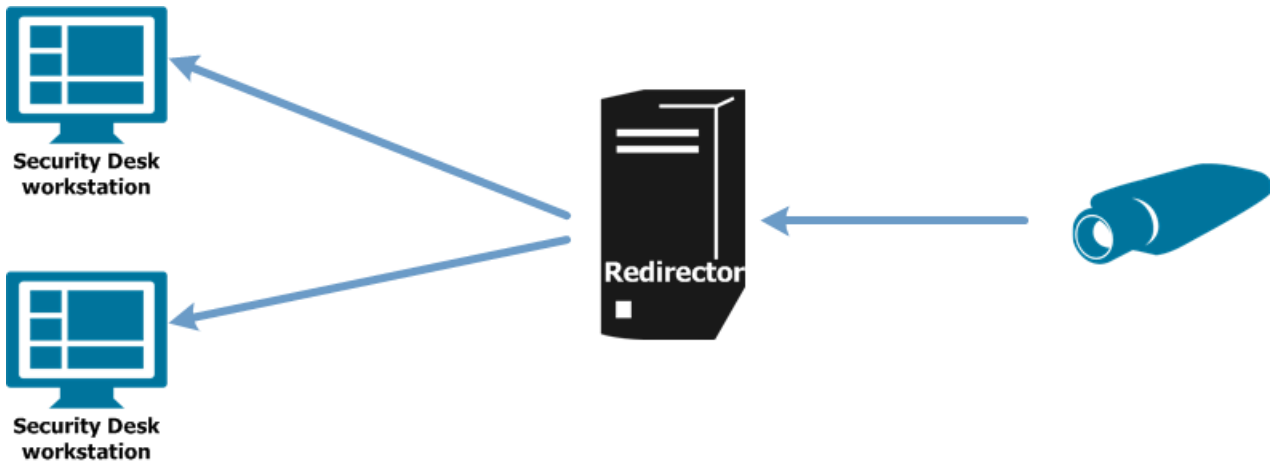
Redirector

فرآیندی که طی آن یک Stream ویدئویی که از یک دوربین منشا می گیرد، توسط یک سرور به یک مقصد هدایت می شود

معمولاً این مقصد یک یا چند کلاینت خواهد بود

Redirector در واقع یک Agent نرم افزاری می باشد که مشخص کننده مسیر اطلاعات Stream ها می باشد

Agent ها به عنوان عامل های نرم افزاری شناخته می شوند و خصیصه های Object را دارند

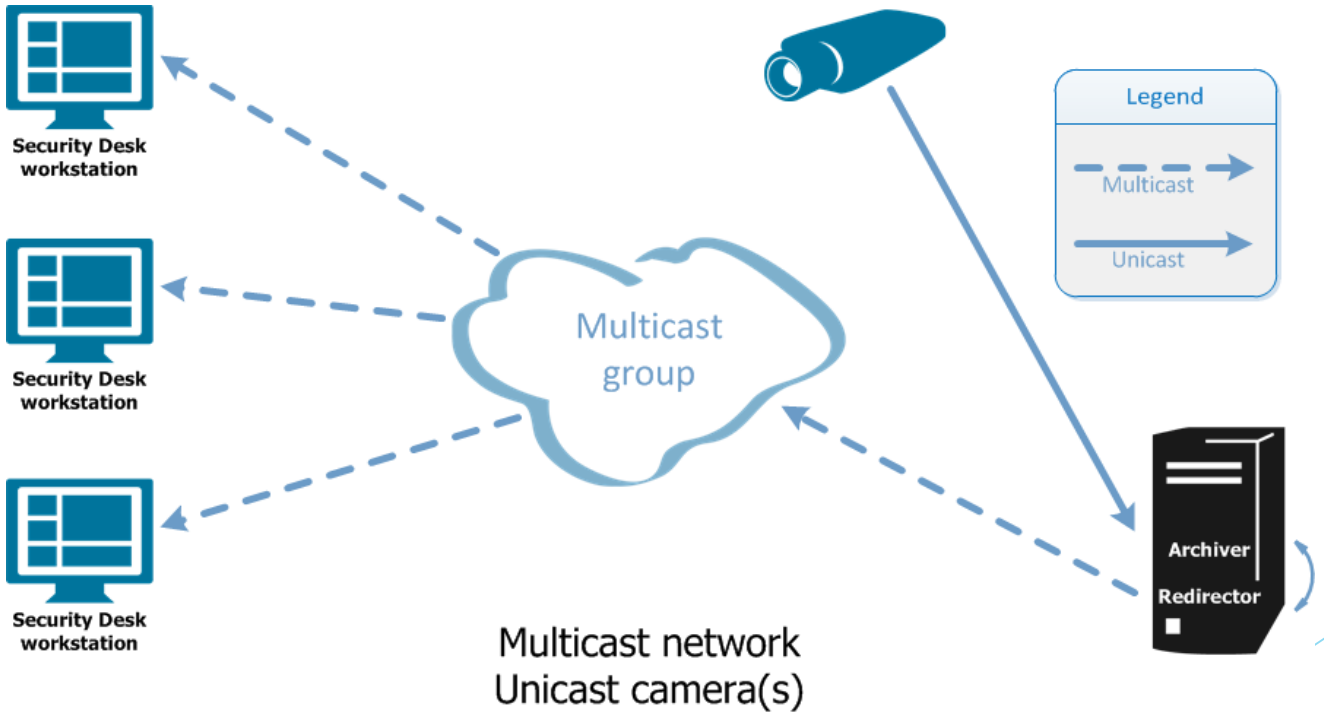


مفهوم Media Routing

در این سناریو وجود Redirector الزامی می باشد. در این حالت شبکه Multicast را پشتیبانی می کند ولی دوربین توسط پروتکل Unicast اطلاعات ارسال می کند

ارسال Stream بر پایه ارتباط Unicast به Archiver میباشد و Archiver در صورت نیاز رکورد انجام داده و Stream را منتقل به Redirector خواهد کرد

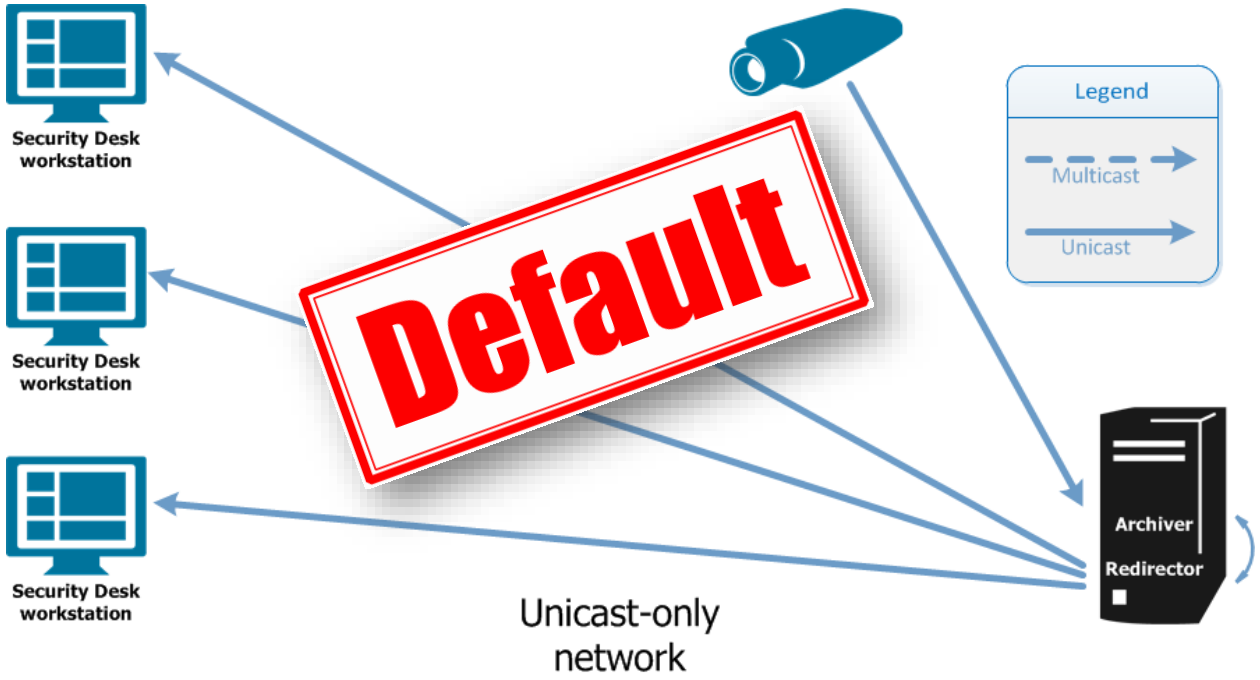
سپس Redirector محتوای Stream را به صورت Multicast به کلاینت ها ارسال می کند



مفهوم Media Routing

در این سناریو هیچ پروتکل Multicast در شبکه وجود ندارد و تمام Stream ها باید مسیر دهی شوند و از پروتکل Unicast برای ارسال به هر کلاینت استفاده کنند

تمامی ارتباطات و تنظیمات Redirector در رول Media Router بوده و مستقیما تاثیر به سزایی در بخش Network نرم افزار دارد



Media Routing مفهوم

Media Router	Redirector
The *Media Router* is a server role	The *Redirector* is an agent
A Security Center system can only have one *Media Router*	A Security Center system can have as many *Redirectors* as needed
The *Media Router* is usually found on the Main Server (hosting the *Directory* role)	The *Redirectors* are usually found on *Archivers*.
The *Media Router* is the “brains” of the network topology	The *Redirectors* are the “muscle” that actually move video packets from one place to another.
The *Media Router* gets its “intelligence” from your Network view design/configuration	The *Redirector* is a “dumb” agent who simply does what it’s told by its boss, the *Media Router*.

انتخاب و محاسبات تجهیزات سخت افزاری

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

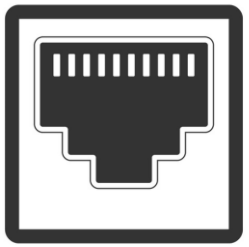
برای مشخص ساختن ساختار و نوع سخت افزار مورد نیاز برای سرور و کلاینت نیاز به جمع کردن برخی اطلاعات از سیستم می باشد

این اطلاعات شامل موارد زیر می باشد:

۱- اطلاعات مربوط به سرورها و مشخص ساختن تعداد سرور های آن ها:
تعداد دوربین ها به همراه رزولوشن آن ها
مقدار فریم های تصویر برداری
قرارگیری بر روی حرکت یا خیر
روش ذخیره سازی به صورت دائم یا حرکت
نوع فشرده سازی
به طور کلی می بایست مقدار پهنای باند و حجم ذخیره سازی مصرفی توسط نرم افزارهای مربوطه محاسبه گردد

۲- جمع آوری اطلاعات مربوط به کلاینت ها براساس مینیمم نیازمندی ها :
تعداد دوربین قابل نمایش بر روی یک کلاینت
نوع فرمت فشرده سازی
کیفیت تصاویر و تعداد فریم ها
تعداد مانیتورهای متصل به کلاینت
همزمانی در بازپخش انجام می پذیرد؟

۳- جمع آوری اطلاعات مربوط به شبکه و زیرساخت:
مقدار پهنای باند مورد نیاز
پروتکل های توسعه دهنده در شبکه وجود دارد
سرعت ارتباطی سوئیچ ها
وجود VLAN ، Firewall ، NAT



محاسبه بهینه سیستم سخت افزار سرور و کلاینت

برای مشخص ساختن سخت افزار سرورها می بایست برخی پارامترها و اصطلاحات آن را بدانیم. این پارامترها شامل موارد زیر می باشند:

۱- تعداد پردازنده مورد پشتیبانی

اصلی ترین واحد در یک کامپیوتر می باشد که کلیه عملیات های منطقی و ریاضی و صدور فرمان به واحد های مختلف را عهده دار می باشد.

پردازنده های دارای معماری های مختلفی می باشند

بر اساس نیازمندی قدرت پردازش تعداد آن ها متفاوت خواهد بود

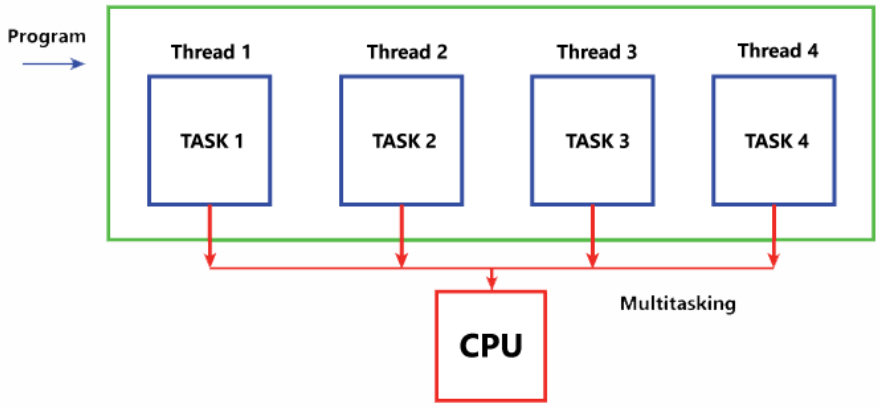
نسل های متفاوتی از پردازنده ها وجود دارند که می توان به Core i3,i5,i7,i9,Xeon

۲- تعداد کور مورد نیاز در هر پردازنده

Coreیا هسته سی پی یو، پردازنده‌ای کوچکتر در داخل پردازنده اصلی است.

در واقع هر Core به تنهایی یک پردازنده کامل است

Core یا هسته در پردازنده کامپوتر ها با نام Thread شناخته می شود که به هسته پردازشی معروف می باشد.



بنابراین اگر شما یک پردازنده Dual Core داشته باشید، پردازنده شما از دو ریزپردازنده تشکیل شده است

به طور مثال تعداد هسته های core i7 بین ۲ تا ۸ هسته است. core i5 بین ۲ تا ۶ هسته دارد و Core i3 بسته به نسل سی پی یو، ۲ یا ۴ هسته دارد.

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

۳- سرعت کلاک در عملکرد پردازنده

کلاک یا سرعت ساعت در CPU نشان‌دهنده تعداد سیکل پردازش CPU در هر ثانیه است

در واقع اگر فرکانس کاری یک CPU 2 گیگاهرتز باشد به این معناست که این پردازنده در هر ثانیه ۲میلیون کار پردازشی را می تواند انجام دهد

۴- میزان حافظه نهان در پردازنده یا Cache

حافظه پنهان حافظه‌ای سریع درون پردازنده مرکزی است که جهت صرفه جویی در زمان مراجعه به حافظه اصلی بکار می‌رود

زمانی که درخواست پردازشی شامل داده‌هایی باشد که در حافظه نهان ذخیره شده اند، داده‌های درخواستی به سرعت به جزء درخواست دهنده تحویل داده می‌شود

این واحد تاثیر قابل توجهی در سرعت و عملکرد پردازنده‌ها دارد

پردازنده های Xeon

این دسته از پردازنده ها همانند خانواده Core ها می باشند با این تفاوت که از حافظه نهان بیشتری جهت پردازش استفاده کرده و یا خود یک حافظه نهان جداگانه دارند.

سرعت پردازش بیشتر و فرکانس کاری بالا تر

بالا تر رفتن فرکانس باعث تلفات بیشتر می شود ولی ساختار این پردازنده ها به گونه ای می باشد که تلفات پایین تری را دارا می باشند

دارا بودن حجم حافظه نهان بیشتر

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

GPU(Graphic Process Unit)

واحدی در بخش سخت افزارهای گرافیکی می باشد که وظیفه نمایش تصاویر ایجاد شده در خروجی خود را دارا می باشد

GPU محاسبات تکراری را به‌طور هم‌زمان انجام می‌داد، درحالی‌که بقیه برنامه همچنان روی CPU اجرا می‌شد.

GPU سریع‌تر از سرعت CPU است و بر توان عملیاتی بالا تأکید دارد

CPU نسبت به GPU حافظه بیشتری مصرف می‌کند یا به حافظه نیاز دارد.

CPU برای پردازش دستورات سریال مناسب است.

GPU و کارت گرافیک دو اصطلاحی هستند که گاهی اوقات به‌جای هم استفاده می‌شوند.

بااین‌حال، تفاوت‌های مهمی بین این دو وجود دارد. تفاوت اصلی این است که GPU یک واحد خاص در یک کارت گرافیک است. GPU چیزی است که پردازش واقعی تصویر و گرافیک را انجام می‌دهد. کارت گرافیک چیزی است که تصاویر را به واحد نمایش می‌دهد.

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

برای مشخص شدن مشخصات فنی در یک سرور و کلاینت باید بر اساس اطلاعات به دست آمده و همچنین محدودیت های نرم افزارها به یک سخت افزار بهینه دسترسی پیدا کنیم

محدودیت های نرم افزاری توسط کمپانی تولید کننده نرم افزار اعلام کی گردد و همچنین بر اساس محدود سازی مشخصات فنی سرور و کلاینت را مشخص می سازد

به طور مثال در نرم افزار Genetec با توجه به کارکرد دو Role با نام های Archiver و Directory که در دسته اصلی قرار دارند ، هر کدام مقداری از منابع سخت افزاری را درگیر کرده و بر اساس این موضوع که چه تعداد از این Role ها به صورت سرویس بر روی سخت افزار قرار می گیرند نرخ پهنای باند مشخص می گردد

If the Directory and Archiver role are running on the same server, do not exceed 100 cameras or 200mbps.

If a system contains more than 300 cameras, the Directory Role must be installed on a standalone machine.

Limitations of MS SQL Express Edition

- Supports 1 Processor
- Up to 1 GB of Memory
- Maximum Database Size : 4 GB for SQL Express 2005, **10 GB** for SQL Express 2008 R2
  - *A database can reach 4 GB on a 120 camera Archiver with 60 days of storage*

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

مشخصات سخت افزاری مورد نیاز بر اساس کمپانی تولید کننده نرم افزارسرور

		Directory & Archiver	Standalone Archiver	Directory & Access Manager	Standalone Access Manager	Directory, Archiver, Access Manager
Minimum	Intel® Core™ 2 Duo E6850 3.0 GHz or better 4 GB of RAM or better 80 GB hard drive for OS and Security Center applications 100/1000 Mbps Ethernet network interface card Standard SVGA video card[3]	50 cams or 50 Mbs	75 cams or 75 Mbs	150 readers 10,000 CH's	150 readers 10,000 CH's	50 cams or 50 Mbs 64 reader 5,000 CH's
Recommended	Quad Core Intel® Xeon® E5640 2.66 GHz or better 16 GB of RAM or better 64-bit operating system 80 GB SATA II hard drive or better for OS and Security Center applications GbE network interface card Standard SVGA video card[3]	100 cams or 200 Mbs	300 cams or 300 Mbs	300 readers Unrestricted CH's	425 readers Unrestricted CH's	100 cams or 200 Mbs 200 readers 40,000 CH's

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

مشخصات سخت افزاری مورد نیاز بر اساس کمپانی تولید کننده نرم افزار برای سرور

		Directory & Archiver	Standalone Archiver	Directory & Access Manager	Standalone Access Manager	Directory, Archiver, Access Manager
High performance standalone archiver	BCDVideo BCD380V8 Enterprise Video Recording Server4 Dual Intel® Xeon® E5-2430L V2 @ 2.4 GHz 16 GB of RAM Microsoft® Windows Server 2012 R2 Standard Edition 64-bit Intel® I350 Quad-Port Gigabit 330i Network Interface Card Smart Array P430 RAID controller with 4096 Mb Cache Size Module 2 SAS 10K RPM hard drives in RAID1 configuration for OS and Security Center applications 8 or more SAS 7200 RPM hard drives in RAID5 configuration for video recording	100 cams or 200 Mbs	500 cams or 500 Mbs + 200 Mbs redirection	300 readers Unrestricted CH's	425 readers Unrestricted CH's	100 cams or 200 Mbs 200 readers 40,000 CH's

محاسبه بهینه سیستم سخت افزار سرور و کلاینت

مشخصات سخت افزاری مورد نیاز بر اساس کمپانی تولید کننده نرم افزار برای کلاینت

		CIF 352 x 240 500 Kbps	VGA 640 x 480 1500 Kbps	HD 1280 x 720 3500 Kbps	Full HD 1920 x 1080 6000 Kbps	Ultra HD 3840 x 2160 10 mbps	H.264 @ 30 FPS
Minimum	Intel® Core™ 2 X6800 @ 2.93 GHz 2 GB of RAM or better 80 GB hard drive for OS and Security Center applications 256 MB PCI-Express x16 video card 1280 x 1024 or higher screen resolution 100/1000 Mbps Ethernet network interface card	32 cameras	9 cameras	6 cameras	4 cameras	0 cameras	
Recommended	4th Generation Intel® Core™ i7-4770 or better 8 GB of RAM or better 64-bit operating system 120 GB Solid State Drive for OS and Security Center applications GbE network interface card NVIDIA® QUADRO K620 2 GB video card	64 cameras	48 cameras	15 cameras	8 cameras	2 cameras	

		CIF 352 x 240 500 Kbps	VGA 640 x 480 1500 Kbps	HD 1280 x 720 3500 Kbps	Full HD 1920 x 1080 6000 Kbps	Ultra HD 3840 x 2160 10 mbps	H.264 @ 30 FPS
High performance	4th Generation Intel® Core™ i7-4770 or better 16 GB of RAM or better 64-bit operating system 240 GB Solid State Drive for OS and Security Center applications GbE network interface card 2 x NVIDIA® GeForce GTX970 - 4GB video card	90 cameras	60 cameras	40 cameras	30 cameras	8 cameras	

پیش نیازهای نصب نرم افزارها

پیش از نصب نرم افزاری و فعال سازی لایسنس ها باید نکاتی را رعایت کرده تا از آسیب وارد شدن به نرم افزار یا لایسنس ها جلوگیری شود

بررسی کانکتورهای شبکه و اتصالات آن ها : برخی از فعال سازی لایسنس ها به صورت آنلاین صورت می گیرد به همین دلیل اتصال اینترنت و شبکه مهم می باشد

بررسی فایروال : فایروال ها بر روی سیستم عامل ها امکان مسدود سازی و غیر فعال کردن برخی پورت ها یا حتی خود نرم افزار را به هنگام نصب در جهت بالا بردن امنیت سیستم دارا می باشند

سطح دسترسی کاربران : حتما در تنظیمات میزان دسترسی کاربر جهت نصب نرم افزار در بالاترین حالت باشد

نصب نرم افزارهای جانبی : قبل از نصب نرم افزار مدیریت تصاویر نیاز به راه اندازی نرم افزارهای جانبی می باشد که باید از قبل نصب گردند

عدم قرارگیری در حالت دومین : سرورهای اصلی در زمان نصب و راه اندازی نرم افزار به هیچ عنوان در حالت دومین نباید قرار داشته باشند

پایگاه داده : حتما قبل از نصب نرم افزار از نصب و فعال بودن پایگاه داده مطمئن بوده و دسترسی های آن را بررسی نمایید

درایورها: با توجه به وجود سخت افزارهای مختلف بر روی سرور ، درایورهای آن ها می بایست به طور کامل نصب شده باشد زیرا به هنگام فعال سازی لایسنس از اطلاعات درایور برخی از تجهیزات بر روی سرور استفاده می شود و در صورت نصب آن ها بعد از فعال سازی لایسنس مشکلات جدی پیش خواهد آمد

نصب فریم ورک های .NET : بیشتر نرم افزارها برای کامپایل کردن نیاز به یک نرم افزار واسط به نام .NET دارند که باید پیش از نصب نرم افزار مدیریت تصاویر نصب گردد

مشکلات و رخداد در نرم افزارها

آسیب های بکارگیری از نرم افزارهای قفل شکسته

آسیب های امنیتی

استفاده از نرم افزارهای کرک شده در هر حوزه ای امکان وارد آوردن آسیب های جدی به ساختار سیستم را بسیار محتمل می سازد.

۱. **احتمال متوقف شدن عملکرد نرم‌افزار** به هرحال با توجه به بکارگیری غیرقانونی و بدون مجوز نرم‌افزار احتمال توقف عملکرد یا کارکرد نامناسب نرم‌افزار در شرایط مختلف در کلیه نرم افزارهایی که به صورت کرک مورد استفاده قرار می گیرند وجود دارد.

۲. **عدم امکان بروز رسانی نرم‌افزار و یا در صورت امکان، این پروسه بسیار طولانی می باشد.** لذا امکان دسترسی به قابلیت‌های جدید نرم‌افزار بسیار مشکل و زمانبر خواهد بود. همچنین شرکت سازنده هیچگونه مسئولیتی در قبال مشکلات احتمالی نرم‌افزار و یا باگ‌های امنیتی نخواهد داشت.

آسیب های بکارگیری از نرم افزارهای قفل شکسته

آسیب های امنیتی

۳. **اضافه شدن یک واسطه (فرد کرک کننده نرم‌افزار) به فرآیند تحویل نرم افزار به مشتری**، خود می‌تواند یک آسیب پذیری امنیتی به شمار آید. قابلیت اطمینان به این فرد و نحوه فعالیت وی در فرآیند کرک نمودن نرم‌افزار و عدم وارد نمودن بدافزار به هنگام انجام عملیات کرک امری حیاتی خواهد بود. همچنین با توجه به اینکه افراد کرک کننده عموما" فاقد دانش پایه در تولید نرم افزار می باشند، ممکن است کلیه ملاحظات مربوط به عملکرد صحیح نرم افزار در شرایط مختلف را در نظر نگرفته و نرم افزار تحت شرایط خاص و یا پس از مدتی از کار بیفتد.

۴. **خطر نفوذ بدافزار به سیستم**. استفاده از نرم افزارهای کرک و به صورت غیر قانونی، عموما" سیستم را در خطر مواجه با بدافزارها قرار میدهد. براساس گزارشات مختلف (گزارش شرکت Cybereason) درخصوص آسیب پذیری‌های امنیتی نرم افزارها می‌توان این گونه برداشت نمود که بسیاری از سیستم‌هایی که از نرم‌افزار کرک استفاده نموده‌اند، مورد تهاجم بدافزارها قرار گرفته‌اند.

پیش نیازهای نصب نرم افزارها

وقتی یک یا چند فریم از استریم دریافتی دوربین از دست می رود **Frame drop** رخ می دهد.

Frame Drop

Frame Drop در سطوح مختلفی می تواند رخ دهد:

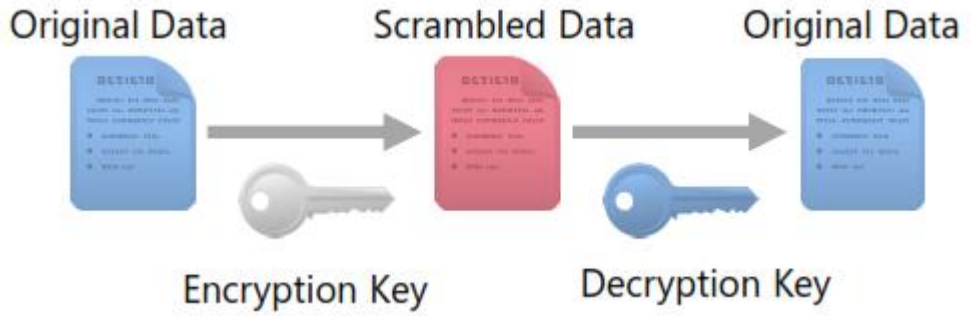
- سرور تا دوربین: این مشکل به دلیل اختلال در این شبکه ارتباطی بوجود می آید.
- سرور تا کلاینت: این مشکل به دلیل اختلال در این شبکه ارتباطی بوجود می آید.
- دوربین: مواردی از قبیل تعداد بالای استریمهای درخواستی از دوربین و یا فعال شدن هر قابلیت خاصی در دوربین (از قبیل آنالیتیک) که به نحوی مصرف منابع **RAM** و **CPU** دوربین را افزایش دهد باعث ایجاد **Frame Drop** خواهد شد.
- سرور: مصرف بالاتر از استاندارد از منابع سخت افزاری سرور
- کلاینت: مصرف بالاتر از استاندارد از منابع سخت افزاری کلاینت

به منظور کاهش **Frame drop** ضروریست هر یک از موارد ذکر شده بالا بررسی و اشکالات ذکر شده برطرف گردند.

امنیت در نرم افزارها

رمزنگاری اطلاعات

رمزگذاری فرآیند ایمن نگه داشتن اطلاعات با تبدیل آن به یک کد مخفی است.



زمانی که شخص مجاز اطلاعاتی را دریافت می‌کند، برای فهم یا رمزگشایی آن به یک کلید برای رمزگشایی داده‌ها نیاز دارد

به عبارت دیگر از کلیدهای عمومی و خصوصی برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌شود

Symmetric:

Encryption key is the same as the decryption key (private keys used)

Asymmetric:

Encryption key different but mathematically linked to the decryption key

One key is commonly distributed (public key), other is kept secure (private key)

رمزنگاری اطلاعات

رمزگذاری کلید عمومی چیست؟

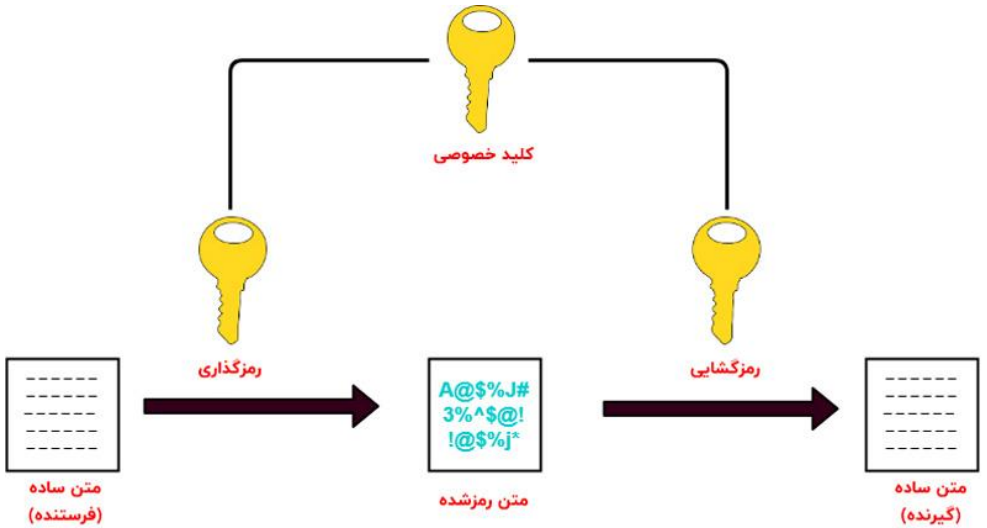
رمزگذاری کلید عمومی به صورت «رمزگذاری نامتقارن» است؛ زیرا از دو کلید مختلف برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌کند.

این روش، برای رمزگذاری اطلاعات از یک کلید عمومی استفاده می‌کند و گیرنده اطلاعات برای رمزگشایی به یک کلید خصوصی نیاز دارد

رمزگذاری کلید خصوصی چیست؟

در رمزگذاری کلید خصوصی فقط از یک کلید خصوصی برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌شود. به همین دلیل، در گروه «رمزگذاری متقارن» قرار می‌گیرد.

به یاد داشته باشید که کلیدهای خصوصی فقط در اختیار مالکین داده و افرادی است که داده‌ها را با آن‌ها به اشتراک می‌گذارند.



رمزنگاری کلید متقارن

الگوریتم های رمزنگاری اطلاعات

به یاد داشته باشید که کلیدهای خصوصی فقط در اختیار مالکین داده و افرادی است که داده‌ها را با آن‌ها به اشتراک می‌گذارند.

Rivest-Shamir-Adelman (RSA)
قدیمی‌ترین سیستم رمزنگاری کلید عمومی-خصوصی. معمولا برای انتقال کلیدهای مشترک برای رمزنگاری کلید متقارن استفاده می‌شود.

Digital Signature Standard (DSS)
یک استاندارد پردازش اطلاعات فدرال با تعیین الگوریتم‌هایی است که می‌تواند برای تولید امضاهای دیجیتالی استفاده شود و برای اولین بار توسط NISTتوسعه یافته و استفاده شده است.

Elliptic Curve Cryptography (ECC)
همانطور که از نام آن پیداست، ECCبرای تولید کلید به منحنی‌های بیضوی متکی است. اغلب برای تطابق کلید و امضاهای دیجیتالی استفاده می‌شود.

مزایا و معایب روش های رمزنگاری اطلاعات

مزایا و معایب روش های رمز نگار خصوصی شامل:

۱- سریع بودن
۲- پیاده سازی آسان توسط سخت افزار
۳- به طور معمول برای رمزنگاری داده های انبوه مورد استفاده قرار می گیرد

۱- مشکلات توزیع و کنترل کلید های خصوصی

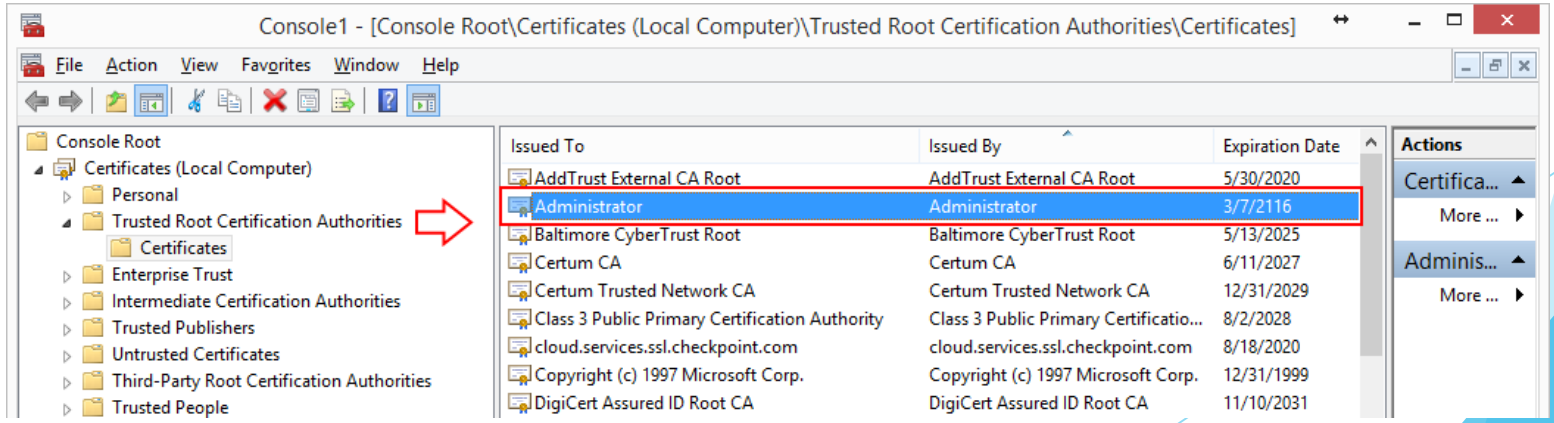
example: AES, RC4, DES

مزایا و معایب روش های رمز نگار عمومی شامل:

۱- ریسک کلید کمتر از زمان ایمن شدن کلیدهای خصوصی
۲- معماری زیربنایی را فراهم می کند تا بتوان از گواهی ها و امضاها استفاده کرد

۱- بسیار کندتر از رمزگذاری کلید خصوصی
۲- به منابع بیشتری نیاز دارد

example: RSA, DSS, DSA



تئوری پروتکل SSL

این واژه مخفف Secure Socket Layer و به معنای لایه اتصال امن می باشد

به طور کلی این فناوری برای ایمن نگه داشتن اتصال به اینترنت و محافظت از هرگونه اطلاعات حساس است که بین دو سیستم ارسال می شود و از خواندن مجرمان و تغییر هرگونه اطلاعات منتقل شده توسط هکرها، از جمله جزئیات شخصی احتمالی جلوگیری می کند

SSL از الگوریتم های رمزگذاری برای مخلوط کردن داده ها در حین انتقال استفاده می کند و از خواندن آن توسط هکرها هنگام ارسال از طریق اتصال جلوگیری می کند

SSL قادر به رمزگذاری توسط دو روش کلید متقارن و نامتقارن می باشد

از ویژگی های پروتکل SSL :

امنیت اطلاعات را افزایش می دهد: عملکرد اصلی یک گواهی نامه SSL محافظت از اطلاعات و ارتباطات سرور و مشتری است.

هویت ما را تایید می کند:تایید هویت یکی از مهم ترین جنبه های امنیت وب است و متاسفانه فریب های اینترنتی به صورت فزاینده ای وجود دارند و بسیاری از مردم روزانه متحمل خسارت های مالی و جبران ناپذیری می شوند که این فناوری می تواند از آنها جلوگیری کند.

اعتماد مشتری را جلب می کند: وب سایت های فاقد SSL با عبارت not secure نمایان می شوند که این موضوع باعث سلب اعتماد مخاطب می شود. در نتیجه SSL می تواند این مشکل را نیز، حل کند.

تئوری پروتکل TLS

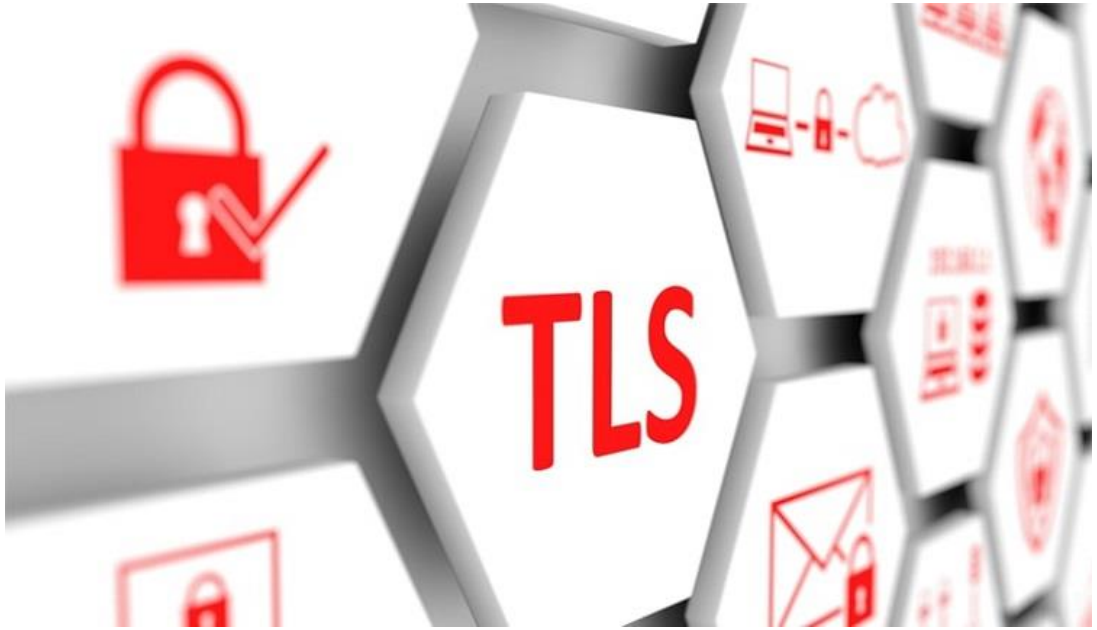
پروتکل TLS مخفف عبارت Transport Layer Security است.

این یک پروتکل رمزنگاری است که برای ایمن‌سازی داده‌های ارسال شده از طریق شبکه مانند ترافیک اینترنت استفاده می‌شود.

موارد استفاده عمومی شامل ایمن‌سازی ایمیل، VOIP، تراکنش‌های آنلاین، انتقال فایل و پیام‌های فوری است.

در ورژن های قدیمی تر نرم افزار Security Center از پروتکل SSL(Secure Sockets Layer) برای کدسازی بین عناصر استفاده می شد

اما در ورژن های جدیدتر از پروتکل TLS استفاده می شود تا از ثبت اطلاعات در بین تبادل و دستکاری کردن آن جلوگیری شود



TLS از رمزگذاری برای مخفی کردن داده ها و Certificate ها برای احراز هویت موجودیت ها استفاده می کند

TLS از رمزگذاری نامتقارن برای ایجاد یک اتصال (ایمن تر) و سپس از رمزگذاری متقارن برای ادامه مکالمه (سریع تر) استفاده می کند.

تئوری پروتکل TLS

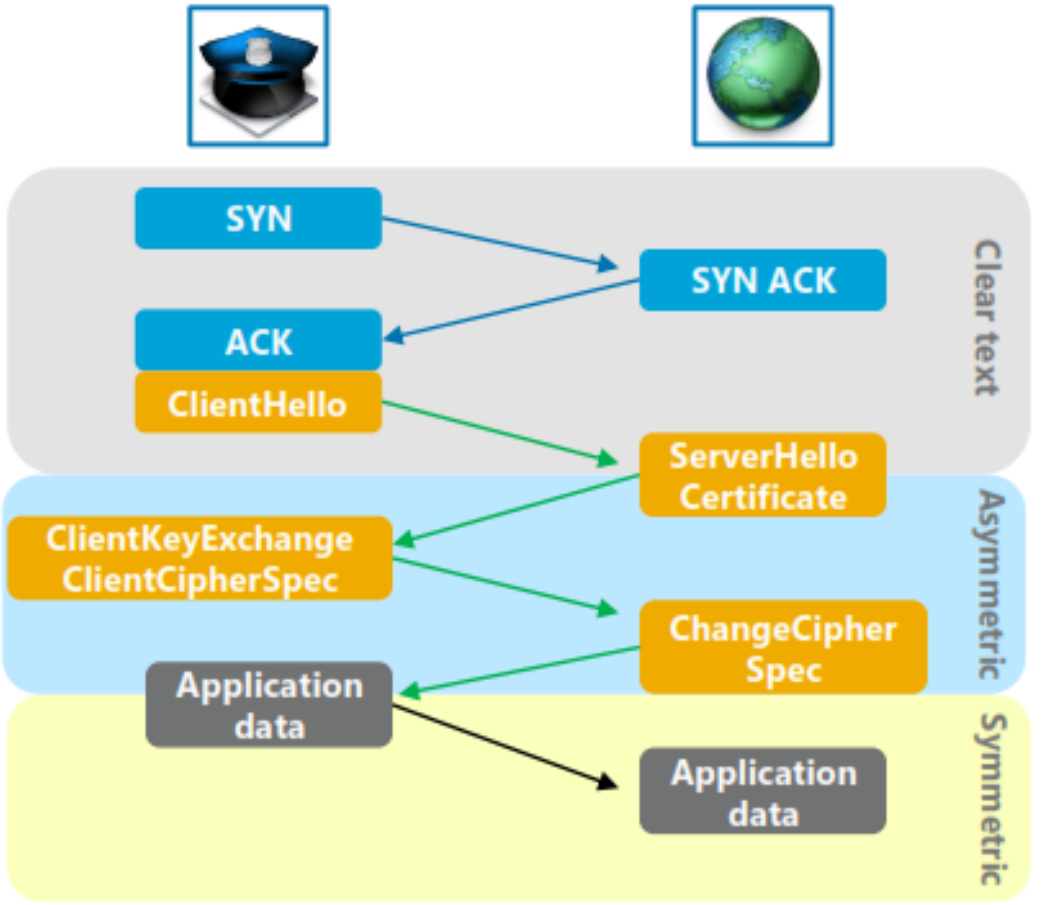
The client establishes a TCP connection with the server using the 3-way handshake (Synchronize and Acknowledge)

The client sends a TLS "hello" message to the server. This includes the version of the TLS protocol it is running and the list of supported *ciphersuites*

The server picks the TLS protocol version for further communication, decides on a *ciphersuite* from the list provided by the client, attaches its certificate containing its public key, and sends the response back to the client

The client then establishes a symmetric session key which is encrypted with the server's public key and sent back to the server

Both parties can then use the shared symmetric session key to communicate



روش های احراز هویت

نوع اول احراز هویت :

۱- رمزهای عبور | Passwordها | OTPها

رمز های عبور ممکن است افشا شوند و به همین دلیل بایستی از آنها محافظت شود .
اگر بخواهیم ایده آل در مورد امنیت فکر کنیم ، هر رمز عبور فقط بایستی یکبار استفاده شود. به این نوع رمز های عبور ، رمز های عبور یکبار مصرف یا One Time Passwordگفته می شود .

۲- توکن های رمزهای عبور ایستا (Static Password Tokens)

مالک خود را به توکن احراز هویت می کند

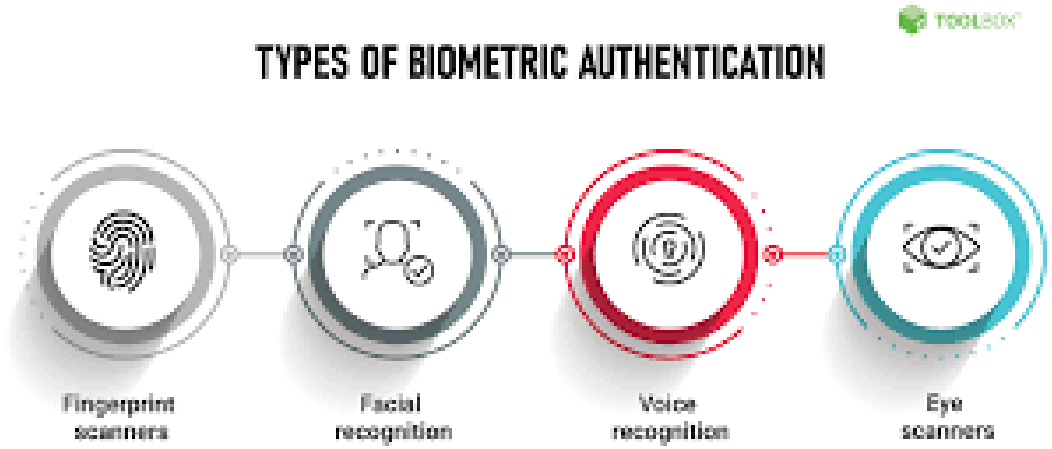
توکن مالک را برای استفاده از یک سیستم اطلاعاتی احراز هویت می کند

۳- توکن های رمزهای عبور پویای همگام

توکن در وهله های زمانی معین و تعیین شده رمزهای عبور منحصر به فرد جدید ایجاد می کند .(این رمزعبور می تواند با یک کلید دیگر رمزنگاری شود)

نوع دوم احراز هویت :

۱- سیستم های بایومتریک یا Biometric



روش های احراز هویت

نوع سوم احراز هویت :

۱- پروتکل | Kerberosکربروس

Kerberos نام یک پروتکل قابل اعتماد احراز هویت است که توسط انیستیتو تکنولوژی دانشگاه ماساچوست یا همان MIT تحت عنوان پروژه Athena طراحی و تولید شد

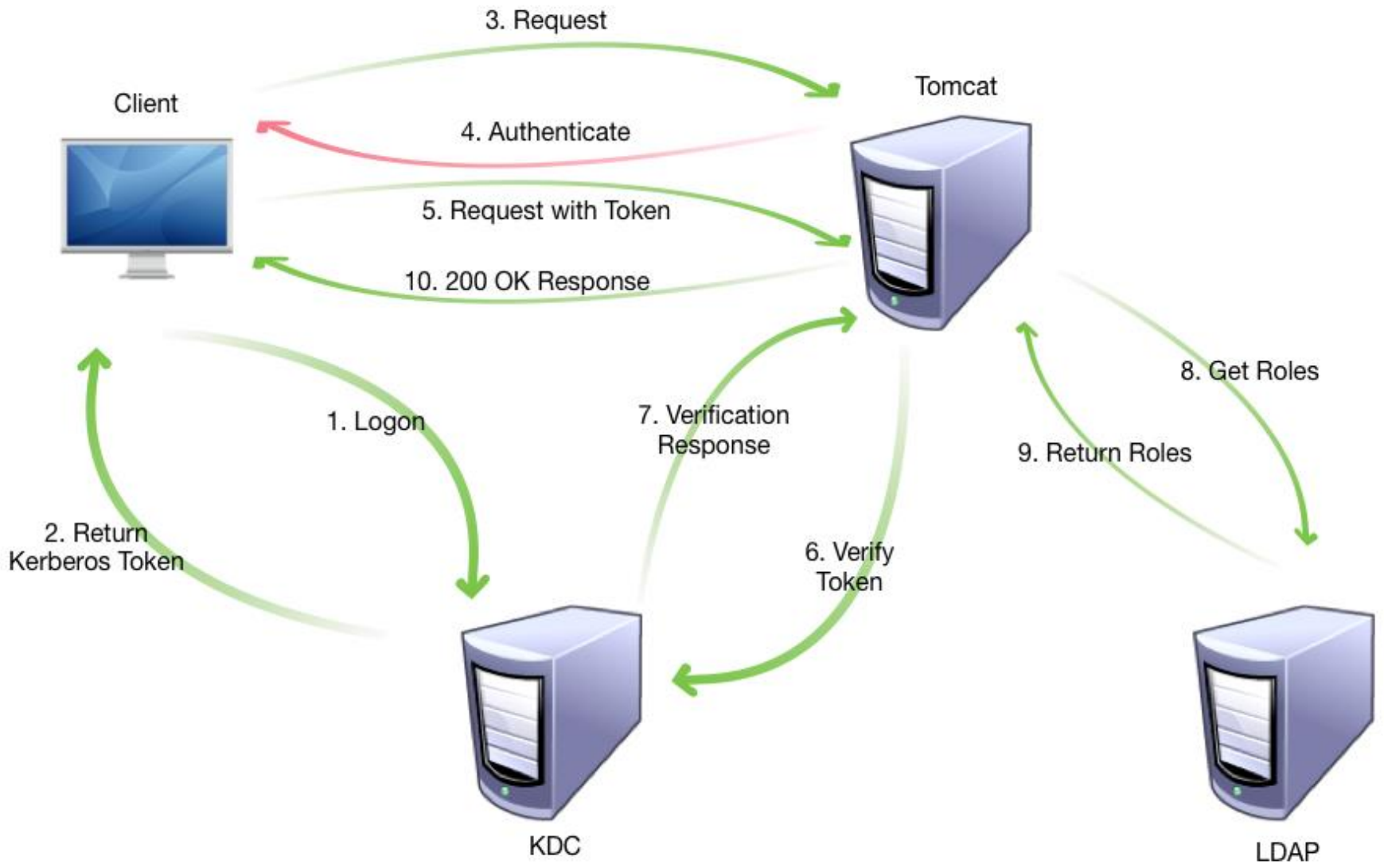
کربروس از رمزنگاری کلید متقارن و یک مرکز توزیع کلید DC (Key Distribution Center) استفاده می‌کند. از این رو برای تائید هویت کاربر به مجوز ثالث مورد اعتماد نیاز دارد.

کربروس به ۳ عنصر مجزا برای احراز هویت نیاز دارد و از یک سیستم رهگیری و نظارتی قدرتمند برای امن‌تر نگه‌داشتن محاسبات استفاده می‌کند.

احراز هویت کربروس در حال حاضر فناوری احراز هویت پیش‌فرض ویندوز مایکروسافت است.

کاربران، رایانه‌ها و سرویس‌هایی که از Kerberos استفاده می‌کنند به KDC متکی هستند که دو عملکرد را در یک فرآیند واحد ارائه می‌کند: احراز هویت و صدور تیکت. به اصطلاح " برچسب های KDC همه طرف ها را با تایید هویت همه گره ها – نقاط شروع و پایان اتصالات منطقی – احراز هویت می کنند.

روش های احراز هویت



روش های احراز هویت

۲- پروتکل Kryptonite

سیستم Kryptonite متعلق به شرکت IBM است که سرویس های احراز هویت ، SSO و توزیع کلید را در یکجا در خود ارائه می دهد

این سیستم برای استفاده در کامپیوترهایی طراحی شد که قابلیت های محاسباتی متنوعی داشتند

۳- احراز هویت چند مرحله ای

در سیستم احراز هویت تک عاملی، کاربر با دانستن نام کاربری و رمز عبور امکان ورود به سیستم را دارد

اما در یک سیستم چند عاملی، بعد از ورود نام کاربری و رمز عبور، در صورتی که مشخصات وارد شده صحیح باشند؛ مرحله بعد احراز هویت صورت می گیرد. برای مثال برای کاربر پیامک و یا ایمیل ارسال می شودیا از Two Authenticate Factor استفاده می شود

امضای دیجیتال

امضای دیجیتال دقیقاً همان چیزی است که بنظر می‌رسد و معادل مدرن و دیجیتالی امضای دست‌نویس یا مهر و موم نامه‌ها محسوب می‌شود

این نوع امضاها که مبتنی بر استانداردهای **PKI** هستند، از یک تکنیک ریاضی پیشرفته برای احراز هویت امضاءکننده استفاده می‌کند و تضمین می‌کنند که اسناد و پیام‌های دیجیتالی ارسال شده به صورت الکترونیکی در حین انتقال تغییر نکرده و دستکاری نشده است. همچنین امضاءکنندگان می‌توانند از این نوع امضاء برای تأیید اسناد دیگر استفاده کنند.

PKI اختصار واژه Public Key Infrastructure یا زیر ساخت کلید عمومی می باشد

امضای دیجیتال مبتنی بر "رمزنگاری کلید عمومی" است که با عنوان رمزنگاری نامتقارن نیز شناخته می‌شود.
در این نوع امضاء، با استفاده از یک الگوریتم کلید عمومی، ۲ کلید (یکی خصوصی و دیگری عمومی) تولید می‌شود که از نظر ریاضی با هم مرتبط هستند.

امضای دیجیتال از طریق ۲ کلید رمزنگاری که دارای اعتبار متقابل هستند کار می‌کنند. فردی که امضای دیجیتال را ایجاد می‌کند از یک کلید خصوصی برای رمزگذاری داده‌های مربوط به امضا استفاده می‌کند، در حالی که تنها راه برای رمزگشایی آن داده‌ها با کلید عمومی امضاءکننده است.
اگر گیرنده نتواند سند را با کلید عمومی امضاءکننده باز کند، این نشانه وجود مشکلی در سند یا امضاء است. اینگونه است که امضای دیجیتال احراز هویت می‌شود.

برای ایجاد یک امضای دیجیتال، از نرم افزاری که قابلیت امضای دیجیتال دارد مانند نرم افزارهای ایمیل استفاده می‌شود. این نرم‌افزارها با استفاده از یک الگوریتم، یک هش (مجموعه‌ای از حروف و اعداد) از داده‌های الکترونیکی به عنوان یک امضاء ایجاد می‌کنند. سپس از کلید خصوصی خالق امضای دیجیتال برای رمزگذاری هش استفاده می‌شود. این هش رمزگذاری شده – همراه با اطلاعات دیگر، مانند الگوریتم هش‌کردن – امضای دیجیتال محسوب می‌شود.

Active Directory

اکتیو دایرکتوری یک سرویس برای مدیریت منابع شبکه است که توسط شرکت مایکروسافت و به منظور کار در محیط‌های ویندوزی تهیه شده است.

هدف اصلی آن فراهم کردن سرویسی متمرکز برای احراز هویت(Authentication) و تعیین مجوزها (Authorization) برای سیستم های داخل شبکه می‌باشد

اکتیو دایرکتوری همچنین امکان تعیین سیاست‌ها، نصب نرم‌افزارها و اعمال به‌روز رسانی‌های مهم را برای مدیران شبکه (Administrator)فراهم می‌کند.

داده‌هایی که در اکتیو دایرکتوری ذخیره می‌شوند، مانند اطلاعات کاربران، تماس‌ها، پرینترها، سرورها، پایگاه‌های داده، گروه‌ها، کامپیوترها، پوشه‌ها و سیاست‌های امنیتی، همه تحت عنوان اشیا ذخیره می‌شوند.

علاوه‌بر ذخیره‌سازی این اشیاء، اکتیودایرکتوری امکاناتی را برای سازماندهی کردن و تعیین دسترسی به این اشیاء فراهم می‌کند.

Active Directory در هسته خود به عنوان یک مخزن فراگیر عمل می کند که به هر موجودیت شبکه، اعم از کاربران، رایانه ها یا منابع، یک هویت مجازی می دهد.

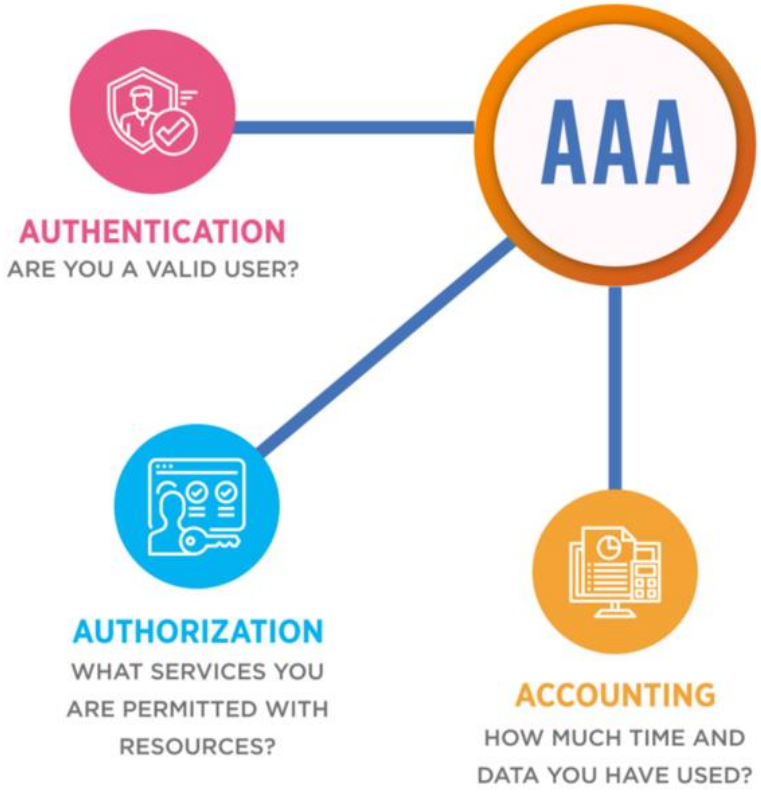
در طرف مقابل، Domain Controller به عنوان نگهبان ظاهر می شود که مسئول اعتبارسنجی درخواست های دسترسی در قلمرو تعیین شده خود است

AAA Authentication Authorization Accounting

AAAشامل سه بخش (Authentication) احراز هویت یا تایید اعتبار(Authorization) تعیین مجوز یا سطح دسترسی و (Accounting) جمع آوری گزارش از فعالیت کاربران می باشد.

مکانیزمی است که به کمک آن می توان امنیت شبکه را ساده تر پیاده سازی نمود.

این مکانیزم دارای یک دیتابیس متمرکز امن، برای نگهداری نام کاربری، کلمه عبور تمام کاربران، Logهای ایجاد شده و غیره است.



Authentication : این بخش وظیفه تایید هویت کاربران را بر عهده دارد و اجازه دسترسی کاربر به منابع شبکه را با پرسیدن برخی از مدارک معتبر مانند نام کاربری و رمز عبور مشخص می کند.

Authorization : کاربران دارای سطوح دسترسی متفاوت به منابع و دستگاه های شبکه می باشند. این بخش برای مشخص کردن سطح دسترسی کاربران به کار می رود و این امکان را فراهم می کند تا پس از دسترسی کاربر به منابع شبکه از طریق Authentication، سیاست های مربوط به سطح دسترسی به منابع شبکه اجرا شود.

Accounting : بعد از انجام Authenticationو Authorization، کاربر به شبکه دسترسی پیدا می کند و شروع به استفاده از منابع و سرویس های شبکه می کند. این بخش وظیفه نظارت و ضبط وقایع انجام شده توسط کاربر در هنگام دسترسی به منابع و سرویس ها را بر عهده دارد و گزارش آن ها را تهیه می کند. همچنین در این بخش می توان بر مدت زمان دسترسی کاربر به شبکه نیز نظارت داشت.

ضرایب امنیتی در نرم افزارها

تست نفوذ (Penetration Testing) به فرآیند هک اخلاقی گفته می‌شود که شامل ارزیابی برنامه یا زیرساخت یک سازمان در برابر انواع مختلف تهدیدات می‌شود

این تست کمک می‌کند تا از آسیب پذیری‌های مختلف سیستم جلوگیری شود و دلایل احتمالی این آسیب پذیری‌ها مانند تنظیمات نادرست و طراحی ضعیف تشخیص داده شود.

انواع مختلف پن تست

پن تستر شبکه
در تست شبکه ابتدا ساختار فیزیکی سیستم به منظور شناسایی خطرات موجود در شبکه سازمان بررسی می‌شود. در این روش شخص انجام دهنده تست (penetration tester) آزمایش‌ها و تست‌هایی را در شبکه سازمان انجام می‌دهد تا نقایص و ایرادها را در طراحی و عملکرد شبکه مورد نظر پیدا کند. تست گیرنده تمام اجزای مختلف سازمان که شامل رایانه‌ها، مودم‌ها و remote access devices می‌شود را بررسی می‌کند تا حملات احتمالی را تشخیص دهد

پن تستر فیزیکی
تست فیزیکی به منظور شبیه سازی‌های دنیای واقعی انجام می‌شود. فرد انجام دهنده تست به عنوان یک مهاجم سایبری عمل می‌کند و سعی دارد سد فیزیکی امنیت را بشکند. این تست برای تشخیص آسیب پذیری‌های موجود در کنترل‌های فیزیکی مانند دوربین‌های امنیتی و سنسورها انجام می‌شود.

ضرایب امنیتی در نرم افزارها

پن تستر برنامه وب

تستر برنامه وب برای بررسی حملات احتمالی و نقاط ضعف برنامه‌های مبتنی بر وب انجام می‌شود. این روش برای مسائل امنیتی استفاده می‌شود که ممکن است به دلیل توسعه غیر ایمن ناشی از طراحی یا کد رخ دهد. همچنین این تست برای شناسایی حملات احتمالی در وب سایت‌ها و برنامه‌ها استفاده می‌شود.

پن تستر شبکه بی سیم

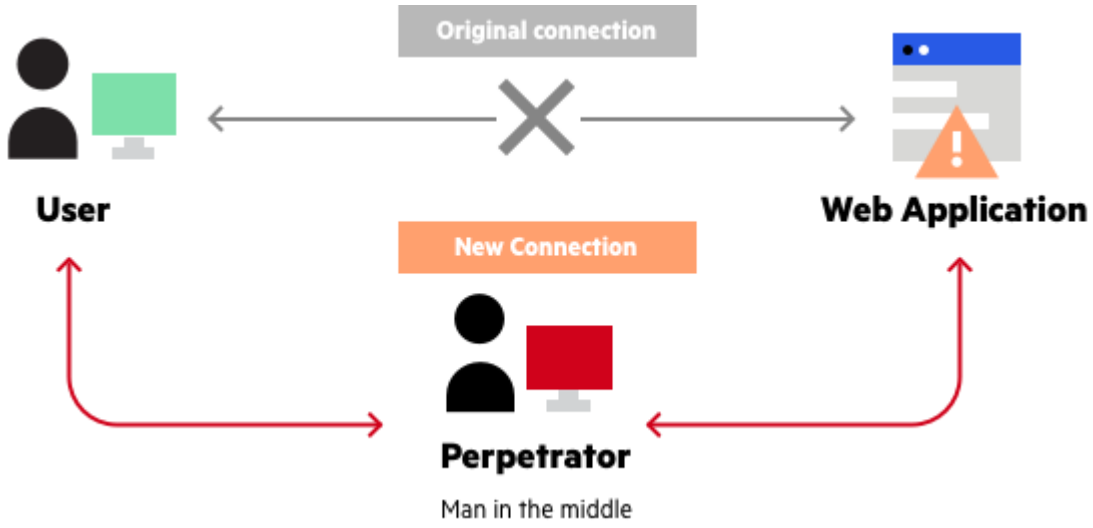
این نوع تست برای بررسی ارتباط بین تمام دستگاه‌ها مانند: تبلت‌ها، لپ‌تاپ‌ها، رایانه‌ها و گوشی‌های هوشمند انجام می‌شود. از این روش به منظور جلوگیری از هرگونه نشت داده که ممکن است هنگام به اشتراک گذاری اطلاعات از یک دستگاه به دستگاه دیگر از طریق شبکه Wi-Fi رخ دهد، استفاده می‌شود.

ضرایب امنیتی در نرم افزارها

پدیده حمله روز صفر یا Zero day attack

حمله روز صفر یا Zero Day Attack یک حمله اینترنتی است که آسیب پذیری های نرم افزاری و سخت افزاری را هدف قرار می دهد

این حملات به گونه ای هستند که برای فروشندگان نرم افزارها و سخت افزارها یا آنتی ویروس ها ناشناخته می باشند.



اهداف استفاده از حمله روز صفر

نفوذ به سازمان های دولتی
نفوذ به شرکت های بزرگ
حملات سازمان یافته توسط دولت ها
استفاده از آسیب پذیری سیستم های خانگی برای ایجاد botnetها
نفوذ به دستگاه های IoT

مدیریت و نگهداری داده ها

پایگاه داده

«پایگاه داده» یا Database یک بانک اطلاعاتی است که به مجموعه‌ای سازمان‌یافته از اطلاعات یا داده‌های ساختارمند گفته می‌شود و معمولاً به صورت الکترونیکی در یک سیستم کامپیوتری ذخیره می‌شوند

در واقع به مجموعه داده‌ها، «سیستم مدیریت پایگاه داده» (DBMS) به همراه برنامه‌های کاربردی مرتبط با آن‌ها، «سیستم پایگاه داده» می‌گویند

در حقیقت پایگاه داده صندوق اطلاعات شماست که در آن نگهداری می شود.

مدیریت داده‌ها به وسیله پایگاه داده بسیار آسان می‌شود. برای مدیریت داده‌ها در یک بانک اطلاعاتی از سیستم مدیریت پایگاه داده (Database Management System) یا همان DBMS استفاده می‌شود.

پایگاه های داده رابطه ای : Oracle ، MySQL ، Microsoft SQL ، SQLite

پایگاه های داده شیءگرا : PostgreSQL

پایگاه های داده توزیع شده

پایگاه داده مبتنی بر فایل

امنیت در پایگاه داده

امنیت پایگاه داده به اقدامات مختلفی اطلاق می‌شود که سازمان‌ها از آن‌ها برای اطمینان از حفظ شدن پایگاه‌های اطلاعاتی خود در برابر تهدیدات داخلی و خارجی استفاده می کنند

منظور از امنیت پایگاه داده، محافظت از خود پایگاه داده، داده‌های موجود در آن، سیستم مدیریت پایگاه داده مربوطه و برنامه‌های کاربردی مختلفی است که دسترسی به آن‌ها در ارتباط با بانک اطلاعاتی وجود دارد

تهدیدات احتمالی امنیت پایگاه داده

اولین و به طور بالقوه، خطرناک‌ترین تهدیدی که امنیت پایگاه داده را به خطر می‌اندازد، دسترسی غیرمجاز هکرها و دستکاری‌کنندگان به سیستم‌های امنیتی و ایجاد مخاطره در اطلاعات مهم کاربر خارج از پایگاه داده است.

حملات مختلف از طریق نرم‌افزار، اسکریپت یا سایر سیستم‌های غیرقانونی بالقوه مضر که شامل استفاده از بدافزارها و ویروس‌ها می‌شوند

ممکن است تمام تهدیدات فوق منجر به بروز سربار سیستم، عملکرد نادرست برنامه‌های مختلف و قطع دسترسی مدیر مجاز به سیستم شود.

اگر فایل‌های آلوده حذف یا از سیستم سرور پاک نشوند، ممکن است منجر به بروز آسیب‌های فیزیکی مختلفی مانند داغ شدن بیش از حد یا حتی خرابی کامل در موارد شدید شوند.

امنیت در پایگاه داده

برای اطمینان از ایجاد امنیت در پایگاه داده روش‌هایی وجود دارند:

پس از نصب پایگاه داده، باید رمز عبور تغییر داده شود. علاوه بر این، بررسی‌های دوره‌ای گوناگونی لازم است تا این اطمینان به وجود بیاید که رمز عبور در خطر قرار نگرفته است.

باید آن دسته از حساب‌های کاربری که استفاده نمی‌شوند، قفل شوند. در شرایطی که یک حساب کاربری به طور قطعی هیچ‌گاه دوباره استفاده نخواهد شد، بهترین اقدام حذف آن است.

لازم است سیاست‌های پیشرفته مختلفی برای رمزهای عبور قوی ایجاد شوند. یکی از ایده‌های کارامد در این خصوص، الزام در تغییر رمز عبور به صورت ماهانه است.

بررسی نقش‌ها و تنظیم دسترسی‌ها بر اساس آن‌ها بسیار اهمیت دارد. در واقع، باید این اطمینان حاصل شود که کاربران تنها به مواردی دسترسی دارند که مجاز به استفاده از آن‌ها هستند. با وجود اینکه بررسی این موضوع برای پایگاه داده‌های بزرگ بسیار زمان‌بر است، اما اگر دسترسی‌ها به درستی تنظیم شوند، ورود یا دسترسی غیرمجاز به راحتی قابل بررسی خواهد بود.

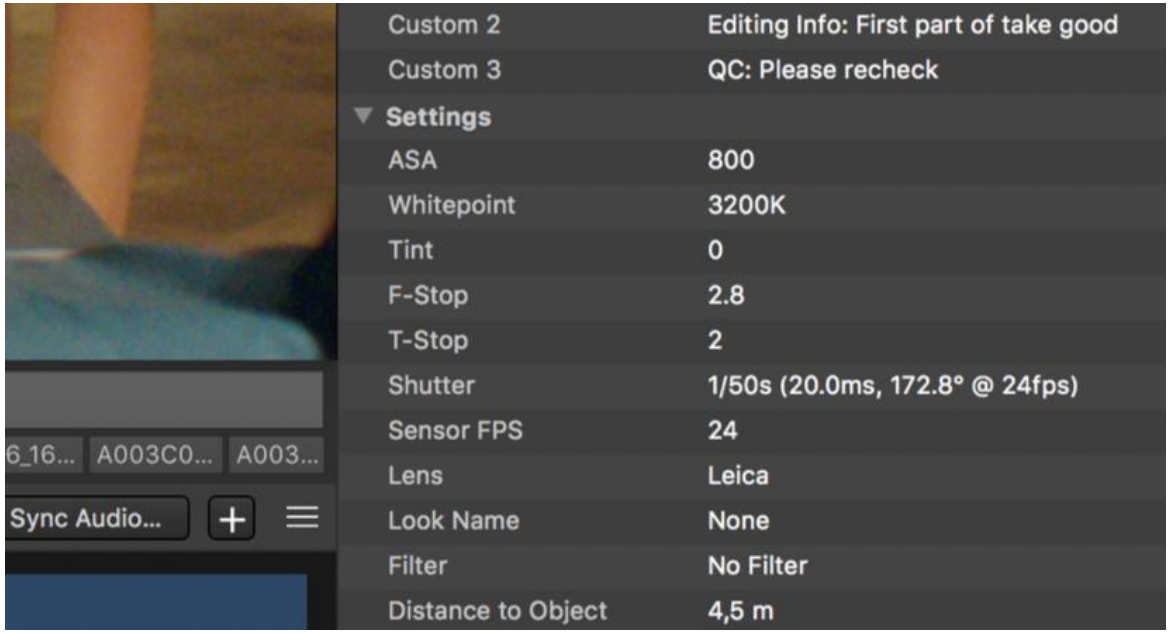
متا دیتا

هر توضیحی که در مورد داده وجود دارد را متا دیتا می نامند

به طور مثال توضیحات همراه یک عکس گرفته شده توسط یک دوربین مانند ، حجم ، سایز آن ، تاریخ و ساعت و همچنین لوکیشن عکس گرفته شده به عنوان متا دیتا شناخته می شوند

در نرم افزارهای نظارت تصویری داده ها هستند که در ارتباط با تغییرات یا رخداد ها در Stream های ویدئویی تغییر می کنند

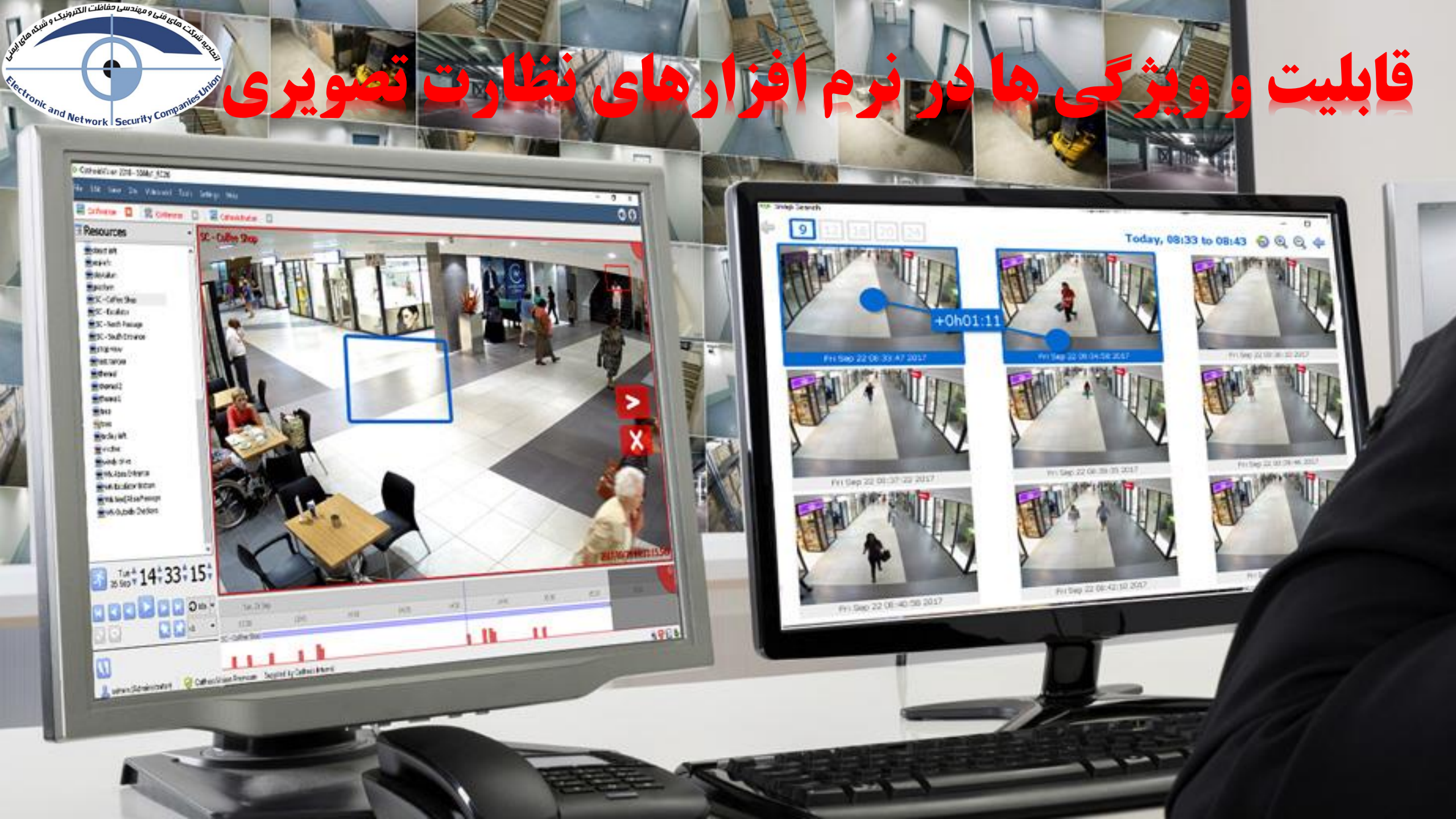
Meta data ها هویت و زمینه را برای رویدادها فراهم می کند



بنا براین با استفاده از متادیتا ها می توان دسته بندی ، جداسازی ، جستجو و بازیابی در اطلاعات یا داده ها صورت پذیرد. مثال ساده در بخش آلارم ها و نوتیفیکیشن های نرم افزارها

این فرا داده ها را می توان در اطلاعات مربوط به فرمت های استخراج شده مانند فرمت تصویر ، تعداد فریم و ... و همچنین در آنالیتیک ها نیز جستجو نمود

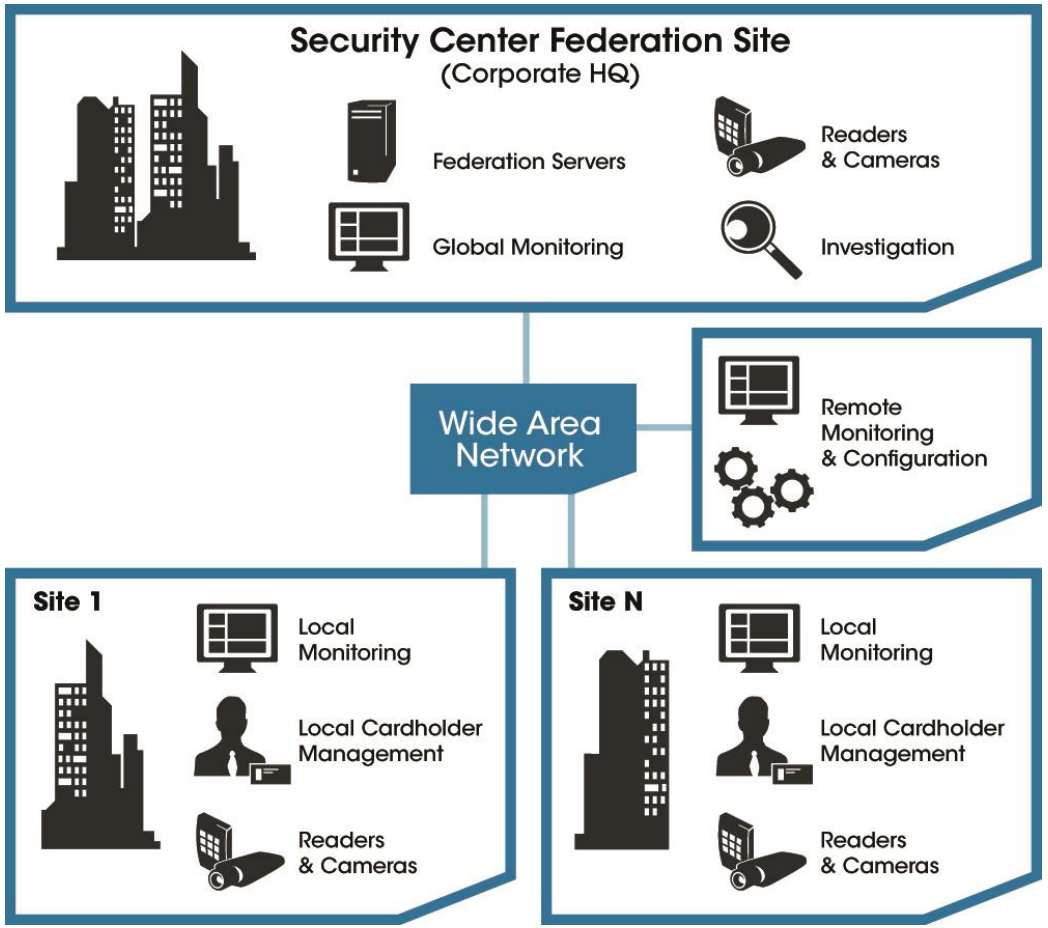
قابلیت و ویژگی ها در نرم افزارهای نظارت تصویری



تجمیع سازی سایت های نرم افزاری

تجمیع سازی به معنای انتقال داده های سایت های مختلف به یک سایت مرکزی جهت نمایش و ذخیره سازی می باشد

عمل تجمیع سازی هنگامی مورد استفاده قرار می گیرد که چندین سایت در محل های مختلف دارای سیستم کنترل مدیریت می باشند و با تعریف یک سایت مرکزی کلیه نیازها بر اساس یک بستر مناسب به سایت مرکزی انتقال یابند



امکاناتی که می توان در تجمیع سازی به سایت مرکزی انتقال داد :

تصاویر دوربین ها

هشدارها

وقایع

سیستم های کنترل تردد

سیستم های پلاک خوانی و ...

Entities that can be Federated:

- Areas
- Alarms
- Cameras
- Camera Sequences
- Doors
- Elevator Cabs
- Elevator Floors
- Inputs
- Outputs
- Zones
- Cardholders
- Cardholder Groups
- Credentials
- Maps

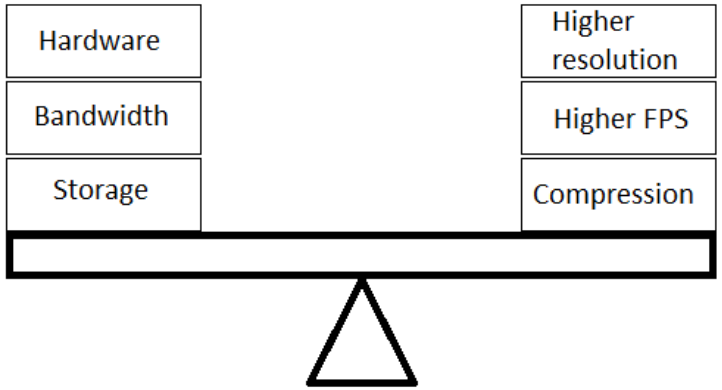
محاسبه بهینه سیستم سخت افزار سرور و کلاینت

افزایش Resource ها در کلاینت ها

- افزایش تعداد کانالهای تصویر در کلاینت
- افزایش روزلوشن تصاویر
- افزایش بیت ریت تصاویر
- استفاده و یا عدم استفاده از چند مانیتور
- قابلیت نرم افزار در پشتیبانی و یا عدم پشتیبانی از قابلیت Adaptive Streaming

✓ قابلیت کارکرد وضوح پویا

در واقع Dynamic Resolution عمل توازن بین کیفیت تصویر و پهنای باند را به وجود می آورد. به این صورت که با تعریف جریان داده های مختلف بر اساس نیاز کاربر تنها همان کیفیت تصویر را دریافت کند. نحوه عملکرد و ایجاد این توازن در شکل زیرنشان داده شده است.

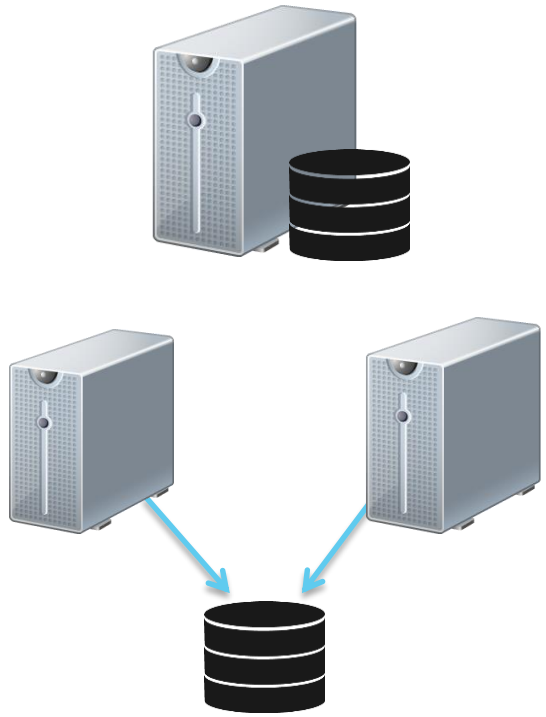


بررسی ویژگی ها در نرم افزارهای VMS

Failover Directory

Failoverتوانایی تغییر خودکار و یکپارچه به یک سیستم پشتیبان قابل اعتماد هنگام بروز مشکل یا اختلال است.

هنگامی که یک مؤلفه یا سیستم اولیه خراب می‌شود، یک سیستم آماده به کار یا در حالت افزونگی باید **Failover**را محقق کرده و تأثیر منفی روی کاربران را کاهش داده یا حذف کند.



Certain roles require databases to operate
By default, the role DB server is hosted on the same machine as the role:

(local)\SQLExpress

Databases can be hosted on separate servers to help:

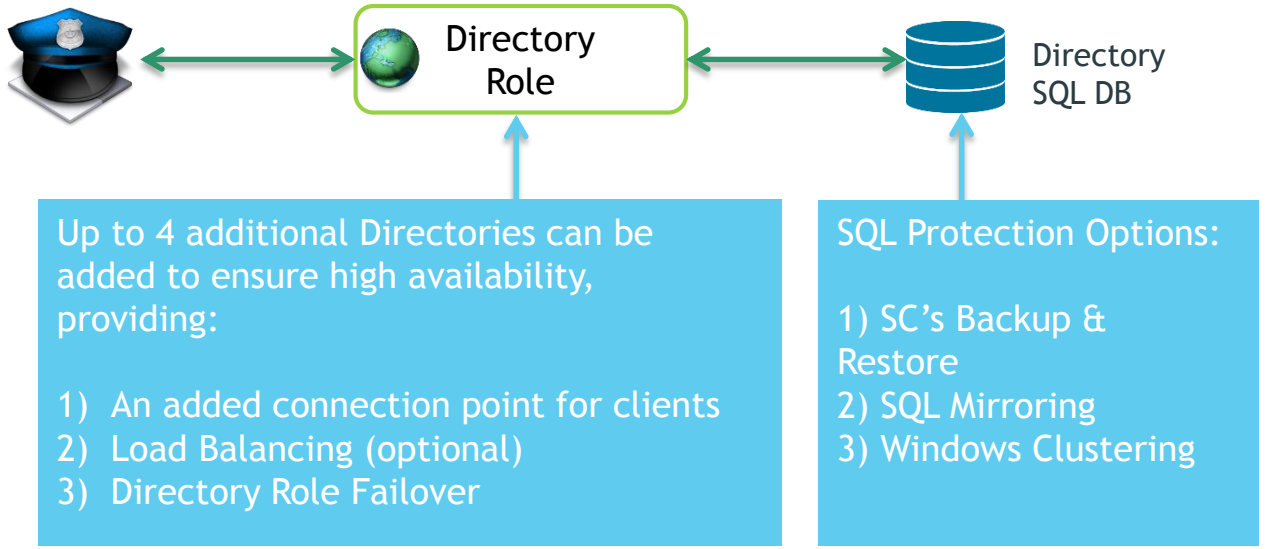
1. Move the role from one server to another
2. Configure standby functionality

For example:

DATASERVER\SQLExpress

بررسی ویژگی ها در نرم افزارهای VMS

- To accept client connections, a Directory must also be connected to a SQL database.
- To ensure high availability, it is possible to protect both the Directory & the SQL layers.

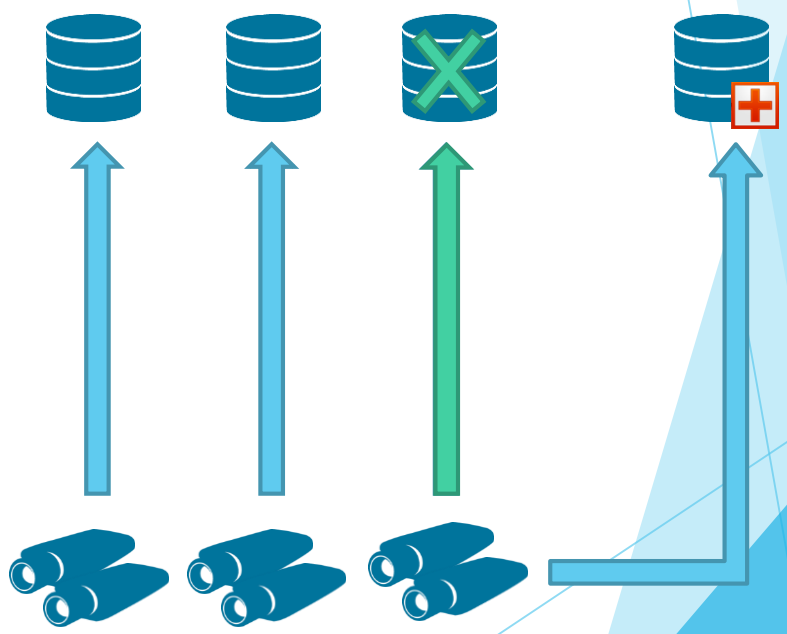


بررسی ویژگی ها در نرم افزارهای VMS

Failover Archiver

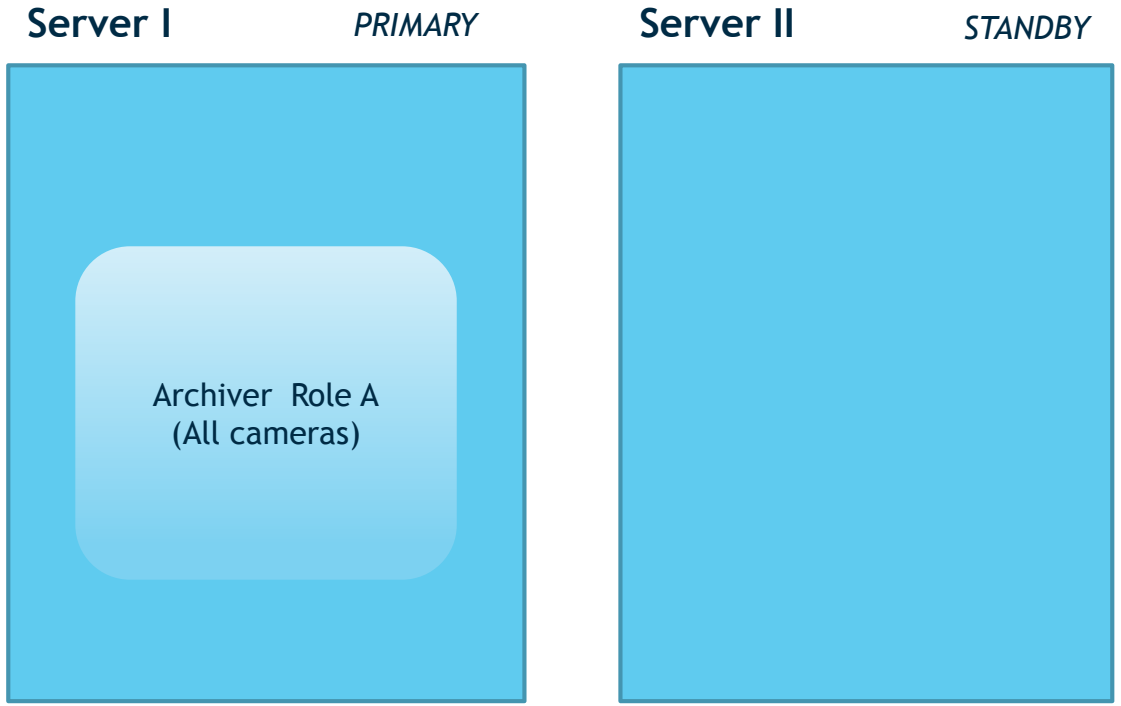
قابلیتی است که به هنگام از دست رفتن رول مرتبط با ضبط تصاویر ، یک رول جایگزین به محموعه اضافه شده و ادامه ذخیره سازی را انجام می دهد

- Protect one or multiple Archivers with one Failover Archiver (1:N)
- Protect recordings against hardware, network or storage failure
- Protect access to live and recorded video
- Minimal failover time

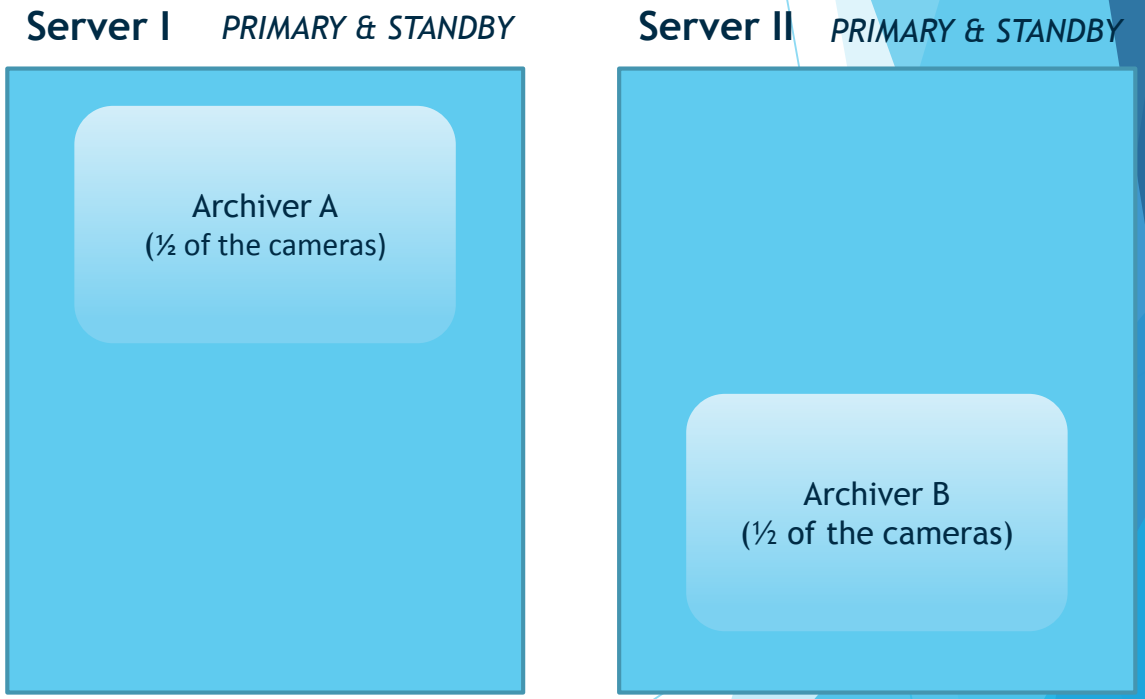


بررسی ویژگی ها در نرم افزارهای VMS

Archiver Failover: *Primary & Backup*

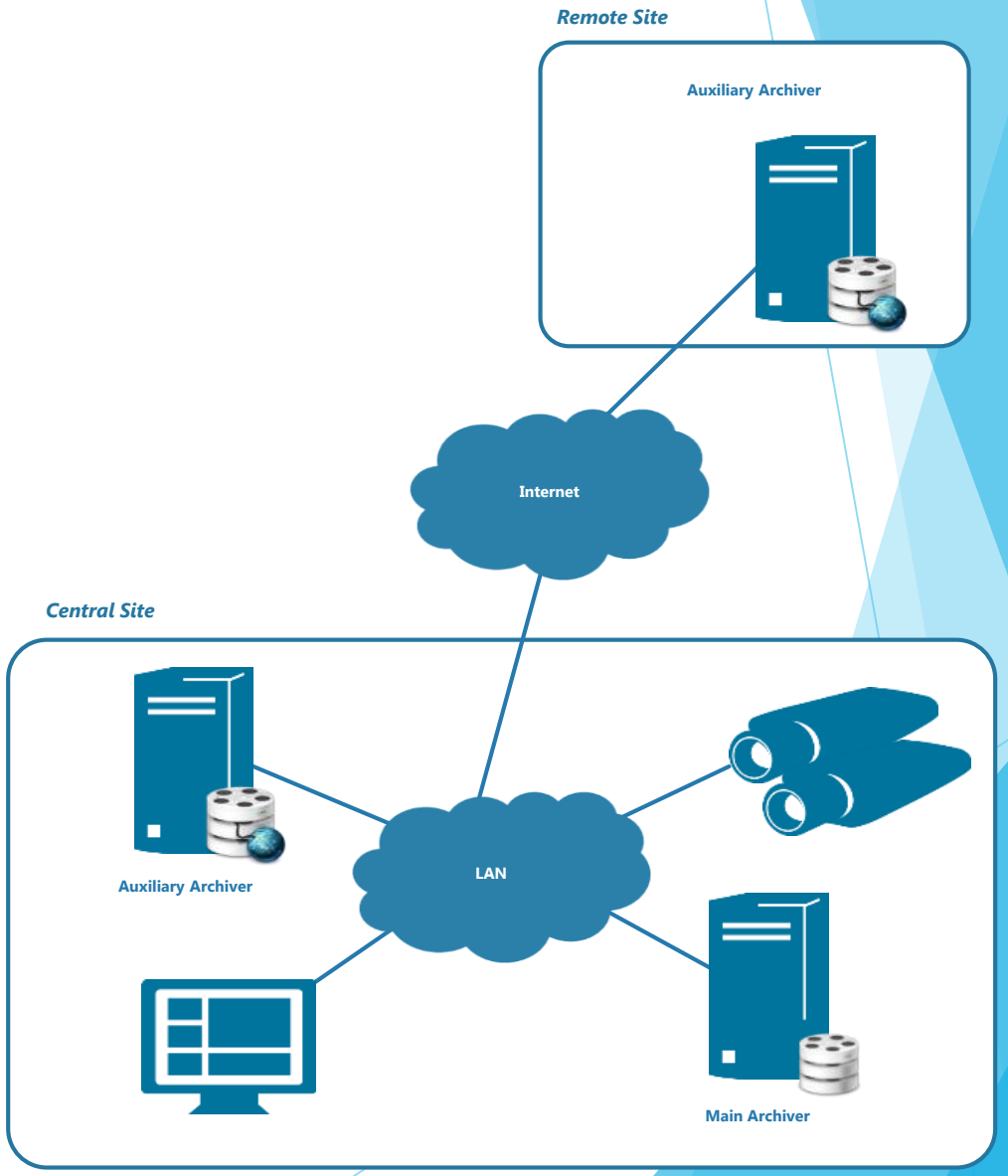


Archiver Failover: “Cross-Failover”



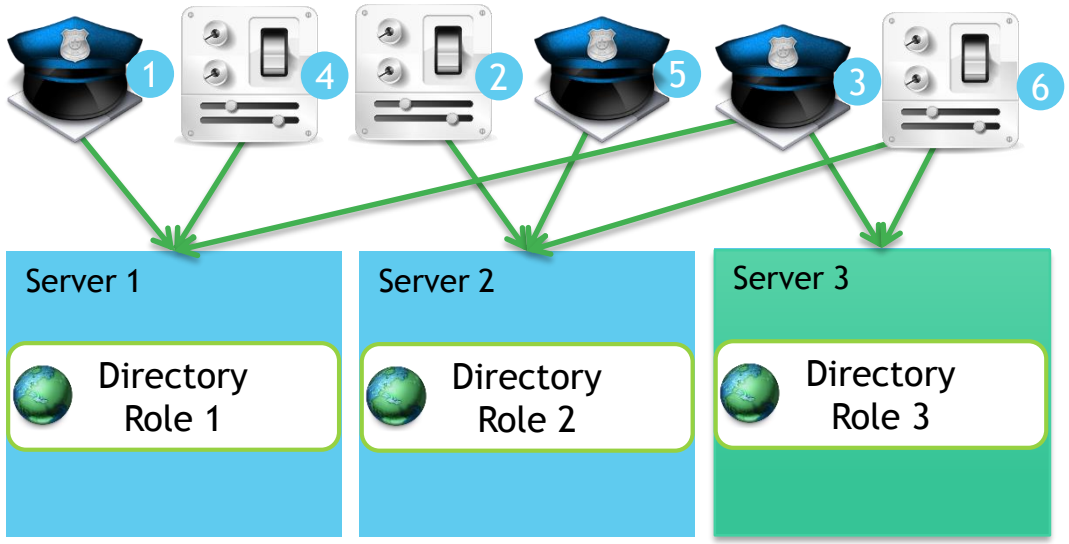
Auxiliary Archiver

- Record a camera in a remote location
- Record the same camera on a different schedule than the main Archiver
- Record a different stream (different quality) of the same camera
- Good solution if pre-alarm needs to be recorded at a higher quality
  - Low quality stream recorded continuously on the main Archiver
  - High quality stream recorded on motion on the Auxiliary Archiver.
- Work across federation
- Limitation: A standard Archiver needs to be online. The Auxiliary Archiver has no command & control connection to the camera.



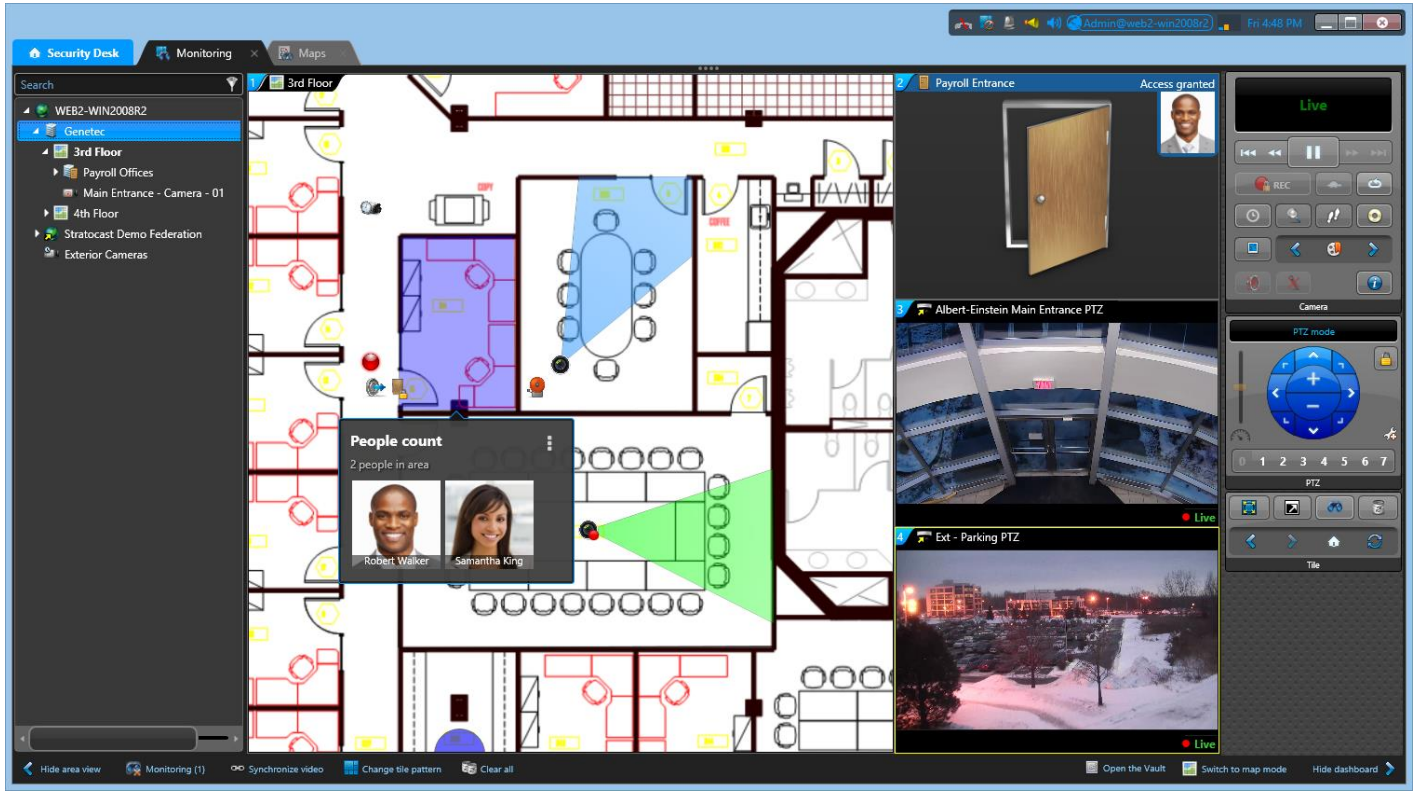
بررسی ویژگی ها در نرم افزارهای VMS

Directory load balancing



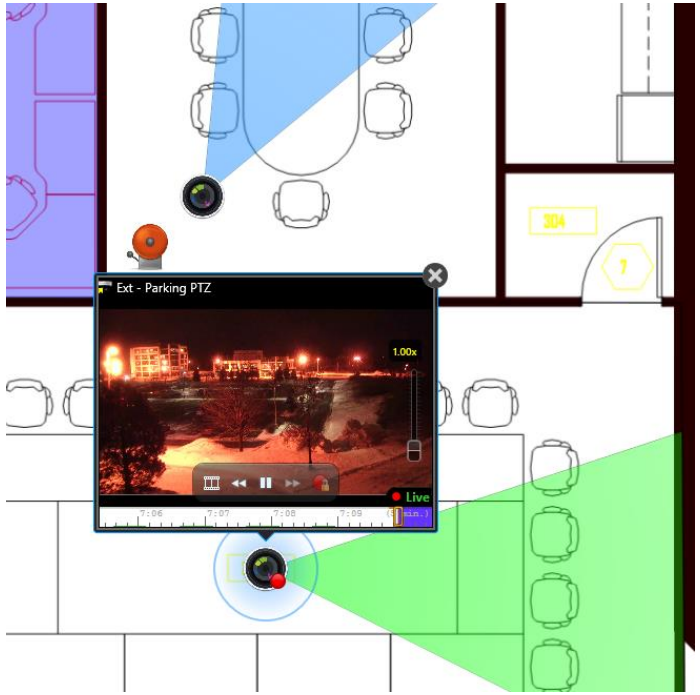
- Supports up to 5 Directory Servers
- Each can act as a connection point to the same system
- Directories automatically load balance incoming client connections (Round robin)
- If disconnected, clients will attempt to connect to other Directories within the System.
- Note: Redirection can be disabled in the client Options page.

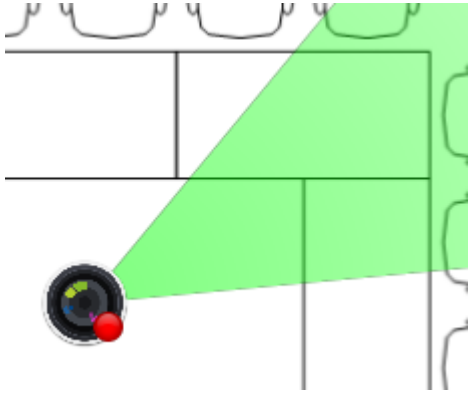
What is Plan Manager?



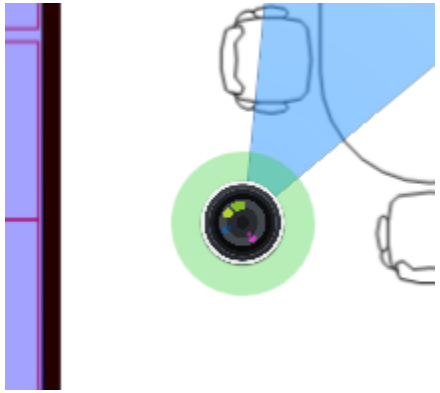
- Plan Manager is the included Security Center component that supports mapping for access control, LPR, video streaming and intrusion detection

Camera views



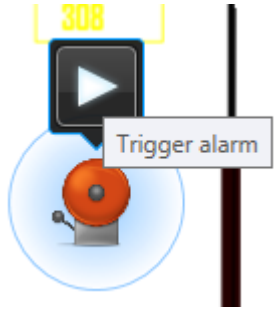


Camera recording state and field of view can be shown from the object: green = PTZ, blue = fixed



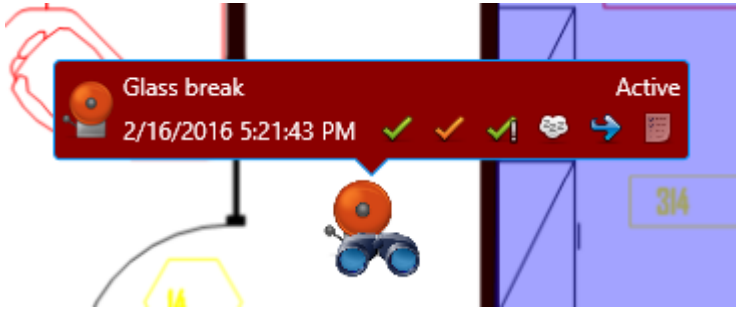
Motion detection can be shown on the camera object
Recording, FoV, and motion detection configurable on a per-camera basis

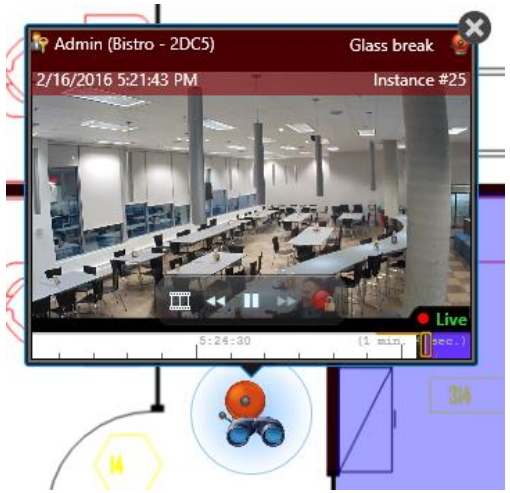
Alarm management



Alarms can be triggered directly from the object.

Can perform alarm functions from an active alarm.





بررسی ویژگی ها در نرم افزارهای VMS

✓ ذخیره سازی بر روی کارت حافظه بیرونی

برخی از دوربین ها این قابلیت را دارا می باشند تا علاوع بر ارسال تصویر بر روی سرور ، ذخیره سازی بر روی یک حافظه بیرونی را نیز دارا باشند. دراین نرم افزار جهت افزایش ضریب امنیتی در سیستم قابلیتی وجود دارد که به نام چکانیدن است. عملکرد **Trickle** به این صورت می باشد که در صورت قطع ارتباط شبکه (تنها شبکه نه تغذیه **PoE**) دوربین به صورت اتوماتیک ذخیره سازی را بر روی کارت حافظه انجام دهد و به محظ اتصال مجدد شبکه تصاویر ضبط شده از کارت حافظه بر روی سرور مرکزی انتقال یابند. این امکان باعث افزایش امنیت به هنگام قطع شبکه شده تا وقایع اتفاق افتاده از دست نروند.

پیش نیازهای نصب نرم افزارها

✓ ساختار پارتیشن و تعریف کاربر

در Security Center قابلیتی به نام تعریف پارتیشن وجود دارد که در سیستم های بزرگ می توان قسمت های بزرگ یک مجموعه را بر اساس نیاز مشتریان و مسئولین امنیتی تفکیک نمود و شخصی را به عنوان مسئول در آن پارتیشن مشخص کرد.

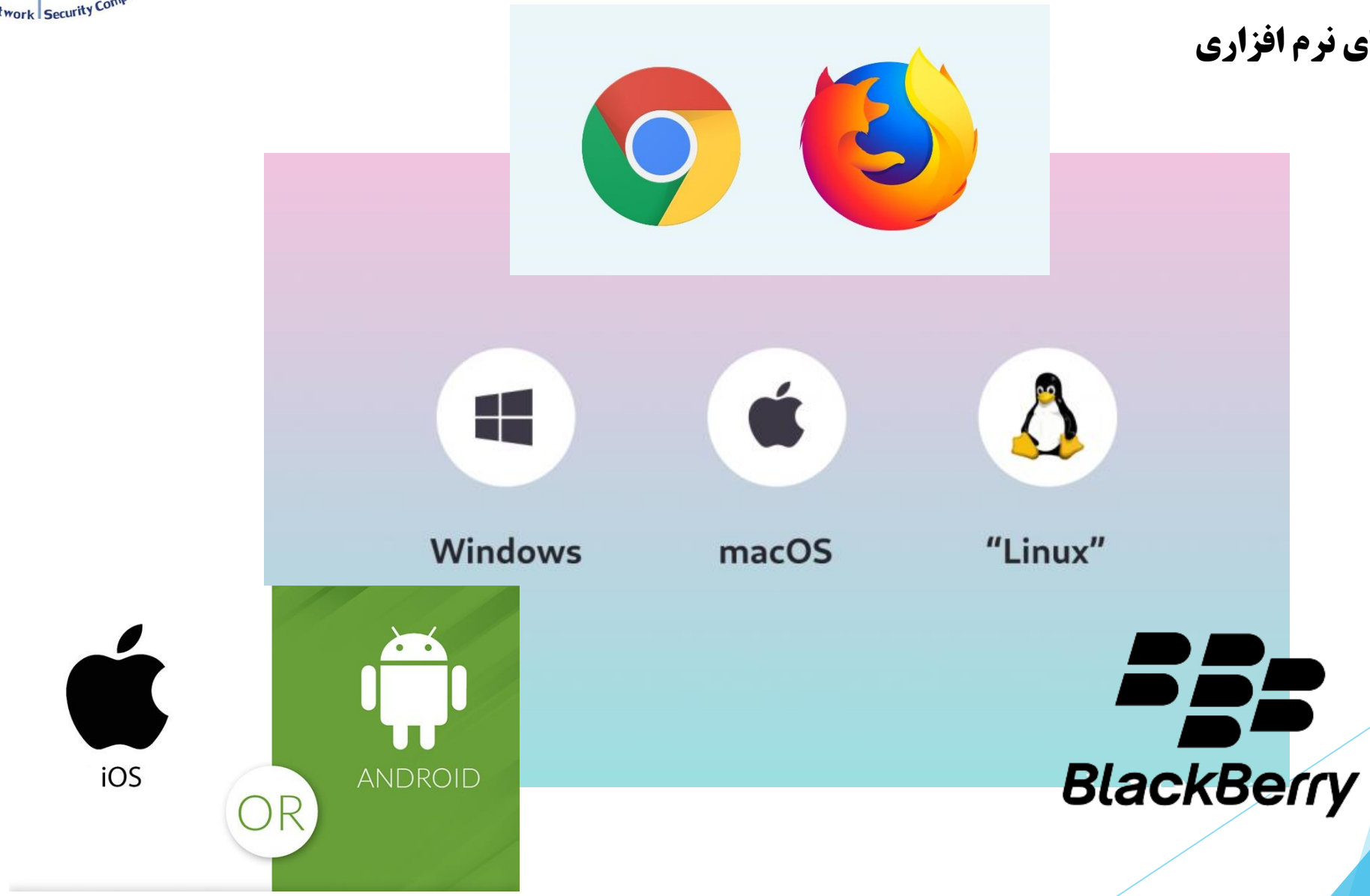
نرم افزار Security Center به دلیل تفکیک ریز به ریز دسترسی ها برای کاربران یکی از قدرتمند ترین نرم افزار ها جهت کنترل دسترسی می باشد. در Security Center محدودیتی جهت تعریف کاربر و پارتیشن در سه نسخه وجود ندارد.

به طور مثال اولویت دسترسی به دوربین های PTZ

به منظور مدیریت فرایند دسترسی به دوربینهای PTZ و جلوگیری از تداخل در کنترل این دوربینها ساختار اولویت بندی دوربینهای PTZ در نرم افزارهای مدیریت تصاویر طراحی شده است. بر این اساس با توجه به نیاز مجموعه و سیاست های کاربری سیستم به هر کاربر و یا گروه کاربری سطح دسترسی مستقلی داده می شود. بدیهیست در شرایط کنترل همزمان یک دوربین متحرک، کاربری با سطح دسترسی و اولویت بالاتر امکان کنترل دوربین را خواهد داشت.

بررسی ویژگی ها در نرم افزارهای VMS

- ✓ انواع پلت فرم های نرم افزاری



بررسی ویژگی ها در نرم افزارهای VMS

✓ گزارشگیری از سیستم

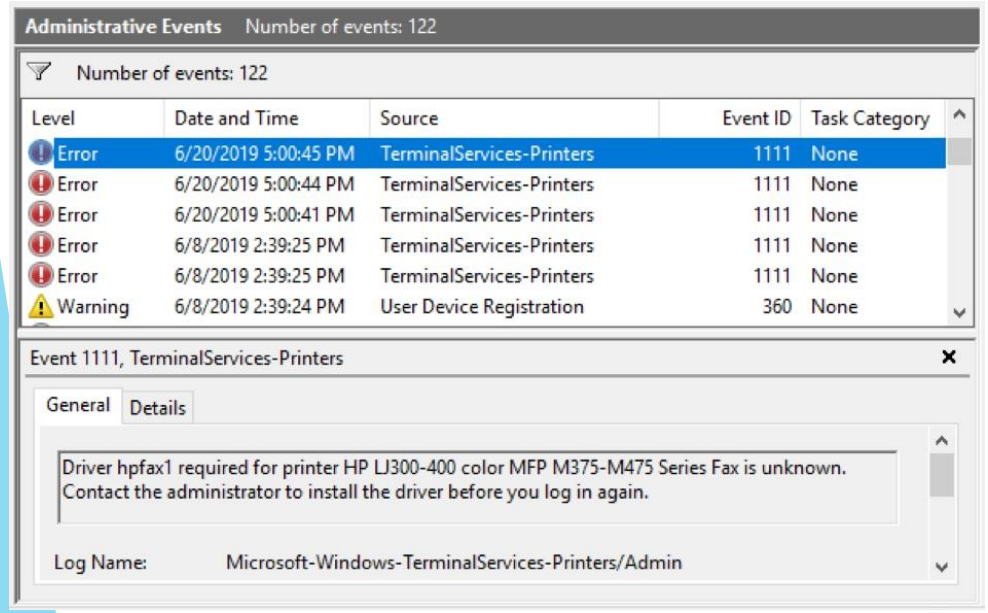
هدف از گزارشگیری از سیستم دریافت اطلاعات از تمامی تغیرات در نرم افزار می باشد

توسط این ویژگی به راحتی می توان عوامل تغییرات ، خرابکاری ، رویدادها و ... را به آسانی بازیابی ، بررسی و به بررسی آن ها پرداخت

در گزارشگیری می توان موارد زیر را جستجو نمود:

۱. تغییرات در پیکربندی با توضیحات زمانی ، مقصد ، کاربر ، نام کاربری و نوع تغییرات
۲. دسترسی های مختلف کاربران به بخش های نرم افزار
۳. ثبت و رسیدگی به رویدادها و عملکردها
۴. ازکار افتادن یا عدم کارکرد صحیح بخش های مختلف در نرم افزار
۵. دریافت خروجی اطلاعات با فرمت های مختلف

و ...



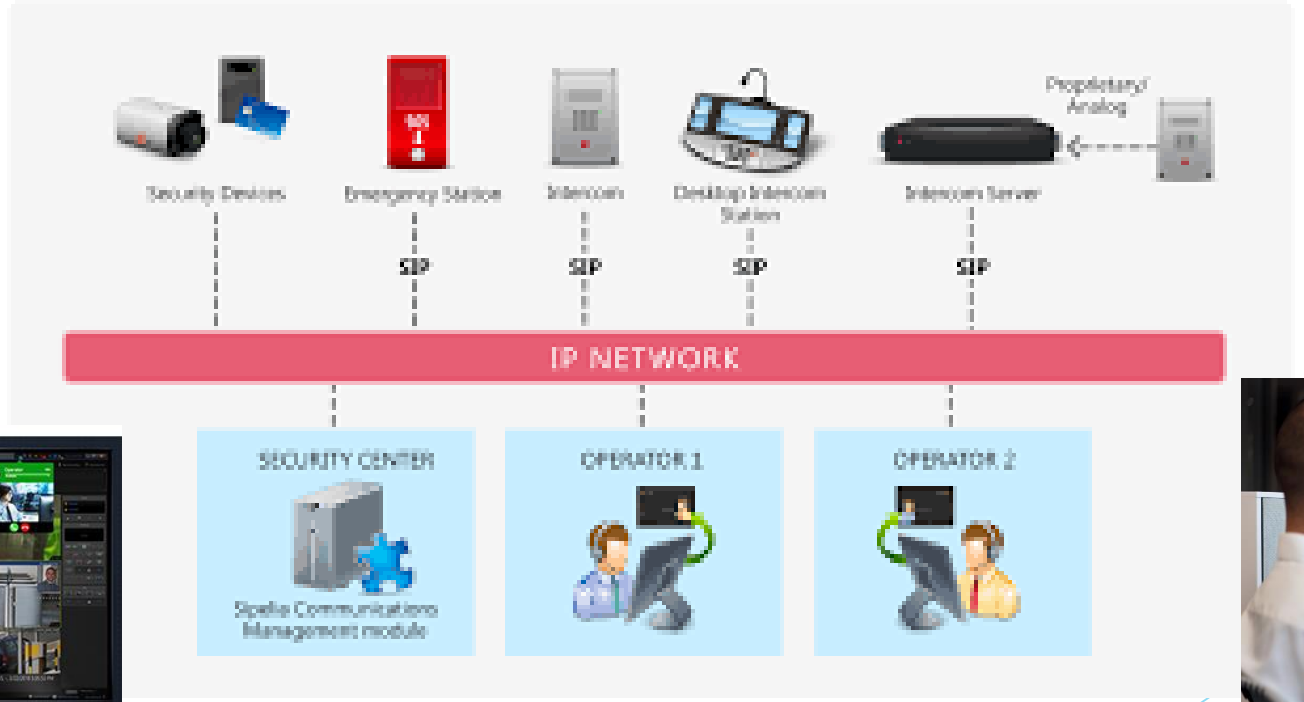
بررسی ویژگی ها در نرم افزارهای VMS

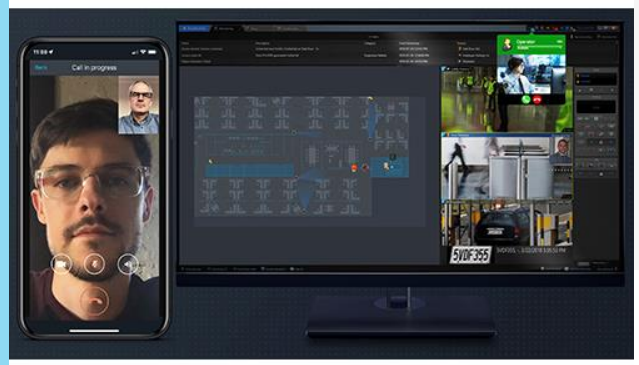
- ✓ **ارتباط صوتی و سرورهای SIP**

برقراری ارتباط صوتی در دسته سیستم های امنیتی از دیگر ویژگی ها دراین دسته از تجهیزات می باشد

به این معنی که کاربران در داخل محیط نرم افزار علاوه بر پایش تصاویر قادر به تماس و مکالمه با یکدیگر نیز باشند

جهت برقراری ارتباط صوتی در پلت فرم نرم افزار نیاز به پروتکل های مرتبط با سرورهای SIP می باشد که در مباحث Voip کاربردی هستند





بررسی ویژگی ها در نرم افزارهای VMS

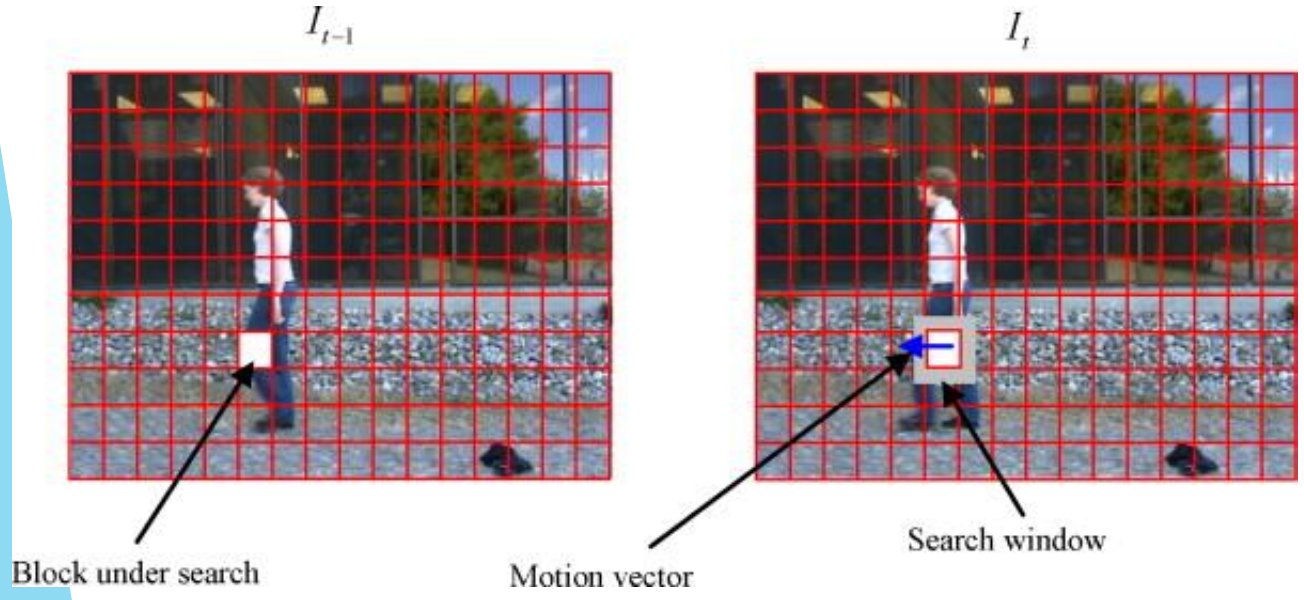
- ✓ **انواع روش های جستجوی تصویر بازپخش**

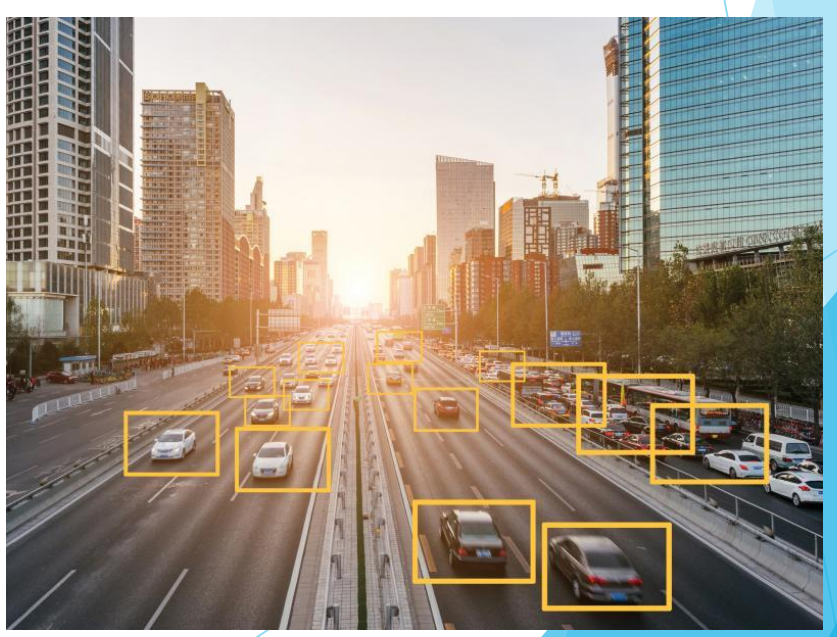
جستجو بر اساس یک ساعت و زمان مشخص

جستجو بر اساس روز کامل

جستجو بر اساس نرم افزارهای آنالیتیک مانند:
Motion Search ، Cross line ، Intrusion Area ، Missing Object ، Heat map و ...

جستجو بر اساس نرم افزارهای فارنسیک:
Face detection ، Face Recognition ، License plate recognition ، Vehicle detection و ...





بررسی ویژگی ها در نرم افزارهای VMS

Visual Tracking

پایان
با تشکر از توجه شما

برگزار کننده : اتحادیه سراسری شرکت های فنی مهندسی
حفاظت الکترونیک و شبکه های ایمنی
بهمن ماه ۱۴۰۲