Thiago Silvestre Amâncio

Sistema de Vigilância Interna Através do Uso de uma Arquitetura de Redes TCP/IP

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da obtenção do titulo de Bacharel em Ciência da Computação.

Orientador
Anderson Bernardo dos Santos

Co-Orientador
Rêmulo Maia Alves

LAVRAS
MINAS GERAIS – BRASIL
2003

Thiago Silvestre Amâncio

Sistema de Vigilância Interna Através do Uso de uma Arquitetura de Redes TCP/IP

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da obtenção do titulo de Bacharel em Ciência da Computação.

APROVADA em 16 de junho de 2003

_____
Prof. Rêmulo Maia Alves

_____
Anderson Bernardo dos Santos
(orientador)

LAVRAS
MINAS GERAIS – BRASIL

DEDICATÓRIA

Dedico esse trabalho aos meus pais Paulo Roberto Amâncio e Maria de Fátima Silvestre Amâncio, a minha irmã Mariana Silvestre Amâncio por me darem condições, apoio, carinho e compreensão, aos meus amigos que sempre estiveram comigo nas horas de dificuldade e principalmente a Deus por guiar meus passos e me iluminar sempre.

AGRADECIMENTOS

Deixo registrado aqui meus sinceros agradecimentos ao meu orientador Anderson Bernardo dos Santos e ao meu co-orientador Rêmulo Maia Alves por me auxiliarem neste projeto.

Agradeço também a todas as pessoas que durante esse período conviveram comigo demonstrando o verdadeiro significado da palavra amizade.

RESUMO

Sistema de Vigilância Interna Através do Uso de uma Arquitetura de Redes TCP/IP

Tendo em vista que nos dias atuais as organizações passam por sérios problemas de como guardar seus bens e suas informações, foi proposta a criação de um sistema de vigilância que permitisse remotamente a um vigilante obter informações do que estava ocorrendo em sua área de alcance.

Com ajuda da Universidade Federal de Lavras foi possível criar um esboço do sistema que proporcionasse este tipo de recurso para os vigilantes. Foi então analisado os métodos e tecnologias para que tal sistema fosse criado, de modo que gerasse à instituição uma confiabilidade de que ele não falharia na apresentação de suas imagens e que também obtivesse um custo benefício propício para sua instalação.

Nas demais páginas serão demonstrados as tecnologias e as formas com que elas interagem para a construção do sistema de segurança.

ABSTRACT

System of Surveillance Interns through the Use of an Architecture of Networks TCP/IP

Tends in view that in the current days the organizations go by serious problems of as to keep its goods and its information, it was then proposed the creation of a surveillance system where remotely a vigilant one obtained information than it was happening.

With help of the Federal University of you Plow it was possible to create a sketch of the system that provided this resource type for the watchmen. It was analyzed the methods and technologies then so that such system was created, so that it generated the institution a safety that he would not fail in the presentation of its images and that also obtained a cost I benefit favorable for its installation.

In the others make up the technologies and the forms they will be demonstrated with that those technologies for the construction of safety's system.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

1 – Introdução

A violência urbana se constitui em um dos principais catalisadores do sentimento generalizado de insegurança pública. À reboque do paroxismo das ocorrências fatais, que têm assolado as diversas regiões metropolitanas brasileiras, o sentimento de insegurança muda hábitos e comportamentos[1].

Uma das questões mais discutidas hoje é a respeito de segurança, não somente a segurança do individuo como também a de patrimônios e informações.

Segurança hoje passou de ser uma coisa supérflua e se tornou uma preocupação extremamente importante para qualquer instituição.

Com um crescimento cada vez mais ascendente da violência urbana nas últimas décadas as empresas buscam dispositivos e saídas que garantam a segurança de seu pessoal e de seu patrimônio.

Mas como isso poderia ser feito?

Uma solução seria colocar uma equipe monitorando as dependências de uma instituição dia e noite de modo que a identificação de algo estranho seria feita a qualquer momento.

Porém, em uma instituição de instalações muito grandes seria improvável que um individuo, ou mesmo uma equipe, pudesse cobrir toda área garantindo que nenhuma atividade estranha ocorresse enquanto outra área estivesse sendo monitorada.

Para solucionar problemas como esse é que cada vez mais as instituições estão se apoiando no uso das tecnologias.

Uma forma de garantir segurança e minimizar um gasto seria a elaboração de um sistema de que monitorasse essas áreas.

De forma que esse sistema deve se mostrar robusto e capaz de retornar um nível aceitável de informações que poderiam auxiliar no trabalho de vigilância de uma área.

Tal sistema poderia contar com o auxilio de câmeras de vídeo que captasse sinais de varias áreas e distribuísse os dados a uma central onde um vigilante ficaria monitorando.

Com base nestas necessidades é que este trabalho tentará formular um sistema de segurança baseado em câmeras de vídeo que farão a transmissão de seus dados através de uma LAN (local área network) até o centro de controle dessas informações.

Com o término do trabalho espera-se criar um mecanismo capaz de auxiliar na vigilância de instituições, objetivando cada vez mais protege-la de intrusos.

2 - Referencial Teórico

2.1 - Redes (LANs)

A*s LANs são redes de dados com nível baixo de erros e de alta velocidade que cobrem uma área geográfica relativamente pequena (até alguns milhares de metros). As LANs conectam estações de trabalho, periféricos, terminais e outros dispositivos em um único prédio ou em outra área geograficamente limitada*[2].

Umas das formas mais importantes para definirmos uma LAN está na configuração que sua topologia se encontra.

Topologia define a estrutura da rede. Existem duas partes na definição da topologia, a topologia física, que é o layout atual do fio (meio) e a topologia lógica, que define como os meios são acessados pelos hosts. As topologias físicas que são comumente usadas são barramento, anel, estrela, estrela estendida, hierárquica e rede. Essas são exibidas na figura1.

- Uma topologia de barramento usa um único segmento de backbone (comprimento do cabo) ao qual todos os hosts se conectam diretamente.
- Uma topologia em anel conecta um host ao próximo e o último host ao primeiro. Isso cria um anel físico do cabo.
- Uma topologia em estrela conecta todos os cabos ao ponto central de concentração. Esse ponto é normalmente um hub ou switch, que será descrito mais adiante.
- Uma topologia hierárquica é criada similar a uma estrela estendida mas em vez de unir os hubs/switches, o sistema é vinculado a um computador que controla o tráfego na topologia.

- Uma topologia de rede (malha) é usada quando não pode haver nenhuma interrupção nas comunicações, por exemplo, os sistemas de controle de uma usina de energia nuclear. Como é possível ver na figura, cada host tem suas próprias conexões a todos os outros hosts. Isso também reflete o projeto da Internet, que possui vários caminhos para qualquer lugar.

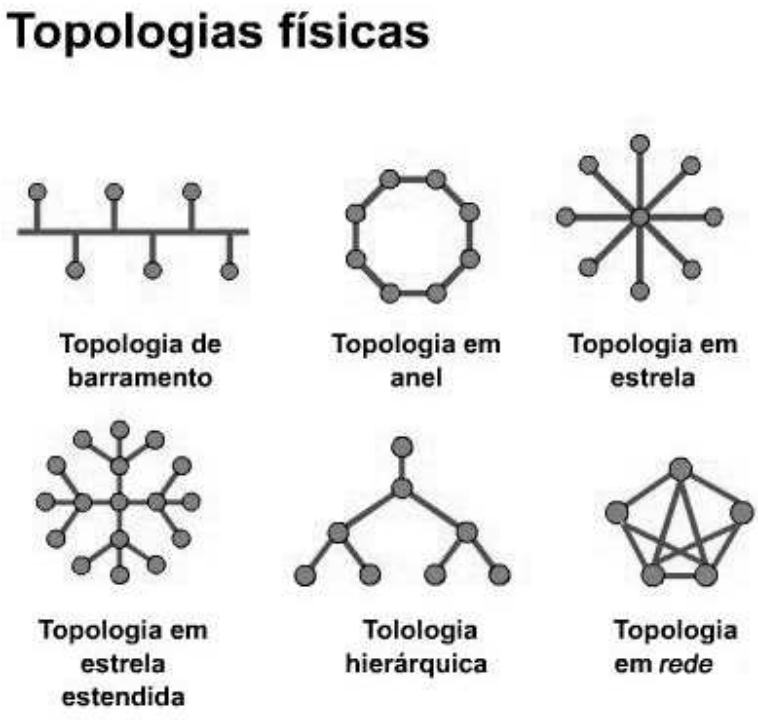

Figura 1 – Topologia Física de LANs

A topologia lógica de uma rede é a forma como os hosts se comunicam através dos meios. Os dois tipos mais comuns de topologias lógicas são broadcast e passagem de token.

A topologia de broadcast simplesmente significa que cada host envia seus dados a todos os outros hosts no meio da rede. As estações não seguem

nenhuma ordem para usar a rede, a primeira a solicitar é a atendida. Essa é a maneira como a Ethernet funciona.

O segundo tipo é a passagem de token. A passagem de token controla o acesso à rede passando um token eletrônico[1] seqüencialmente para cada host. Quando um host recebe o token, significa que o host pode enviar dados na rede. Se o host não tiver dados a serem enviados, ele vai passar o token ao próximo host e o processo se repetirá.

2.1.1 - Dispositivos de rede

Para a conexão de redes de computadores são utilizados alguns dispositivos, os quais têm apresentado um crescimento explosivo pelo fato de permitirem a interligação de diversas redes isoladas, criando verdadeiras redes corporativas.

São eles:

- Pontes (Bridges);
- Roteadores (Routers);
- Gateways;
- Hubs;
- Switches;

Pontes, roteadores e gateways são computadores com finalidades específicas, projetadas para receber o tráfego de comunicações de uma rede local e encaminhá-lo a outra rede.

As pontes são dispositivos que conectam LANS (redes locais de computadores) na camada de Enlace de Dados do modelo ISO/OSI que será explicado mais a frente.

[1] Esse token eletrônico é um pacote mais simples que os que contem dados, possuindo somente a informação se o hub/switch pode transmitir ou não.

A principal função de uma ponte é despachar (caso o pacote endereçado seja para microcomputadores não encontrados na LAN local) e filtrar pacotes, dependendo dos endereços de destino.

Convertendo formatos e interpretando protocolos, os roteadores permitem conectar redes locais de tipos diferentes, ou interligar redes locais a redes de longa distância.

Os roteadores trabalham na camada de rede do modelo OSI e são baseados em protocolos.

Para conectar duas redes, é necessário um equipamento que as unam, e que possa enviar pacotes de uma rede para outra. As máquinas que desempenham esta função são chamadas de “gateways”.

Os gateways são extensões dos roteadores. Simplificando, as pontes e os roteadores recebem mensagens, determinam seu destino, fazem as traduções necessárias e as mandam em frente[3].

Hubs são dispositivos utilizados para conectar equipamentos que compõem uma LAN (computadores, terminais, servidores)[3].

Quando um computador enviar uma mensagem ao hub, ele propagará o pacote por todos os seus seguimentos, de forma que todos os computadores receberão a mensagem. Porém, só o computador que tem o endereço de destino interpretará o pacote.

Swich é um aparelho que particiona uma rede em sub-redes, ou grupos de trabalho. Desta forma, o tráfego de dados é contido no grupo que o originou, não interferindo no tráfego de dados de outro grupo. Apenas quando o destino de um dado está em porta diferente do dado de origem, é que o tráfego se realiza entre os grupos.

2.1.2 - Meios de Transmissão

O cabo da rede (ou mídia) é um conjunto de fios de cobre ou vidro que liga todos os nós de uma rede[3].

Os cabos são componentes da camada física, são neles que trafegam toda a informação de um micro a outro.

Os tipos de cabos mais comuns são:

- Cabo Par Trançado Não Blindado (UTP)

  Este cabo é formado por quatro tipos de pares de fios. Cada par é trançado com um numero diferente de voltas por polegada. Os trançamentos dos fios cancelam correntes elétricos – absolvidas de cabos de força e outra fontes externas – que podem confundir os sinais da rede; cancela também, o ruído elétrico dos pares adjacentes e de outros dispositivos existentes no ambiente.

- Cabo Coaxial

  Os cabos coaxiais são dois condutores compartilhando o mesmo eixo central. Utilizam uma blindagem de cobre para o condutor central, evitando a interferência de correntes elétricas externas. Uma malha forma uma blindagem de cobre que envolve o condutor central e representa metade do circuito elétrico.

- Cabo Trançado Blindado (STP)

  Nesse tipo de cabo, o fio do par trançado contem uma blindagem individual para cada par de fios, a fim de reduzir a difonia (interferência entre os pares), e uma blindagem global, que diminui a interferência externa.

- Cabos de fibra óptica

  Os cabos de fibra óptica carregam pulsos de luz através dos fios de vidro, onde cada fio de vidro passa sinais em apenas uma direção.

Além das taxas de transmissão de dados serem muito maior do que qualquer um desses outros meios, os cabos de fibra óptica são imunes às interferências eletromagnéticas ou de freqüência de rádio e são capazes de transmitir sinais a milhas de distância sem qualquer perda.

- Redes sem fios (wireless)

Os microcomputadores podem ser equipados com pequenas placas de circuito de transmissão de microondas. Essas unidades transmitem os seus sinais de rede através do ar para outras estações de trabalho da rede.

2.1.3 - Hierarquias e Protocolos

A maioria das redes é organizada em camadas (ou níveis). Em todas as redes, o propósito de cada camada é oferecer certos serviços às camadas superiores, protegendo essas camadas dos detalhes de como os serviços oferecidos são de fato implementados.

Protocolo são as regras e convenções utilizadas na conversação das camadas. A camada n, em uma máquina, estabelece uma conversação com a camada n em outra máquina, e tem um protocolo n de conversação[3].

2.1.4 - O modelo de referência OSI

O modelo OSI (Open System Interconnect) foi criado em 1977 pela ISO (International Organization for Standardization) com o objetivo de criar padrões de conectividade para interligar sistemas de computadores locais e remotos. Os aspectos gerais da rede estão divididos em 7 camadas funcionais sobre a rede.

A figura2 mostra o modelo ISO/OSI e a atuação dos produtos de comunicação em cada uma das camadas desse modelo.

Este modelo lida com a conexão de sistemas abertos, isto é, sistemas que são abertos à comunicação com outros sistemas.

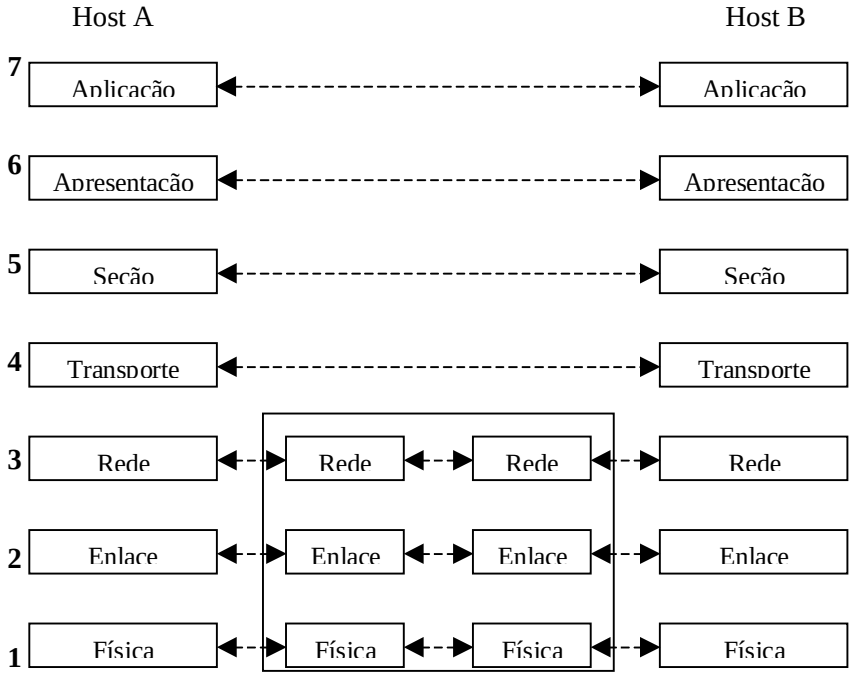

Figura 2 – Esquema do Modelo de referencia OSI

2.1.4.1 - A camada Física

A camada física trata da transmissão de bits brutos através de um canal de comunicação. O projeto da rede deve garantir que, quando um lado envia um bit 1, o outro lado receberá como um bit 1, e não como um bit 0.

2.1.4.2 - A camada de Enlace de Dados

A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruta de dados em uma linha que pareça livre dos erros de transmissão não detectados na camada de rede[4]. Para executar esta tarefa, a camada de enlace de dados faz com que o emissor divida os dados de entrada em quadros (que, em geral, tem algumas centenas ou milhares de bytes), transmita-os seqüencialmente e processe os quadros de reconhecimento retransmitidos pelo receptor. Como a camada física apenas aceita e transmite um fluxo de bits sem qualquer preocupação em relação ao significado ou a estrutura, cabe à camada de enlace de dados criar e reconhecer os limites do quadro. Para tal, são incluídos padrões de bit especiais no início e no fim do quadro. Se esses padrões de bit puderem ocorrer acidentalmente nos dados, será preciso um cuidado especial para garantir que os padrões não sejam incorretamente interpretados como delimitadores de quadro.

No caso de haver um ataque de um ruído na linha de transmissão e o quadro for completamente destruído, a camada de enlace de dados deverá retransmitir o quadro. No entanto várias transmissões do mesmo quadro criam a possibilidade de quadros repetidos. Um quadro repetido poderia ser enviado caso o quadro de reconhecimento enviado pelo receptor fosse perdido. Cabe a essa camada resolver os problemas causados pelos quadros repetidos, perdidos e danificados.

Outra questão decorrente da camada de enlace de dados (assim como da maioria das camadas mais altas) é a forma como impedir que um transmissor rápido seja dominado por um receptor de dados muito lento. Deve ser empregado algum mecanismo de controle de tráfego para

permitir que o transmissor saiba o espaço do buffer disponível no receptor.

2.1.4.3 - A camada de rede

A camada de rede controla a operação da sub-rede[4]. Uma questão de fundamental importância para o projeto de uma rede diz respeito ao modo de como os pacotes são roteados da origem para o destino. As rotas podem se basear em tabelas estáticas, "amarradas" à rede e que raramente são alteradas. Estas podem ser determinadas no início de cada conversação, como, por exemplo, em uma seção terminal. Elas podem também ser altamente dinâmicas, sendo determinadas para cada pacote, a fim de refletir a carga atual da rede.

Se houver muitos pacotes na sub-rede ao mesmo tempo, eles dividirão o mesmo caminho, provocando engarrafamentos. O controle desse congestionamento também pertence à camada de rede.

Quando um pacote tem que viajar de uma rede para outra até chegar ao seu destino, podem surgir muitos problemas. O endereçamento utilizado pelas redes pode ser diferente. Talvez a segunda rede não aceite o pacote devido a seu tamanho. Os protocolos também poderão ser diferentes. É na camada de rede que esses problemas são resolvidos, permitindo que redes heterôgeneas sejam interconectadas.

2.1.4.4 - Camada de Transporte

A função básica da camada de transporte é aceitar dados da camada de seção, dividi-los em unidades menores em caso de necessidade, passa-los para a camada de rede e garantir que todas

essas unidades cheguem corretamente á outra extremidade. Alem disso, tudo tem de ser feito com eficiência e de forma que as camadas superiores fiquem isoladas das inevitáveis mudanças da tecnologia de hardware [4].

Em condições normais, a camada de transporte cria uma conexão de rede diferente para cada conexão de transporte exigida pela camada de seção. No entanto, se houver uma necessidade de um ***throughput*** muito alto, a camada de transporte deverá criar varias conexões de rede, dividindo os dados entre as conexões de rede para melhorar o ***throughput***. Agora, se a criação ou manutenção de uma conexão de rede for cara, a camada de transporte poderá multiplexar diversas conexões de transporte na mesma conexão de rede para reduzir o custo.

A camada de transporte também determina o tipo de serviço que será oferecido à camada de seção e, em última instância, aos usuários da rede. O tipo de conexão de transporte mais popular é o canal ponto a ponto livre de erros que libera mensagens ou bytes na ordem em que eles são enviados. No entanto, outros tipos possíveis de serviço de transporte são as mensagens isoladas sem garantia em relação à ordem de entrega e à difusão de mensagens para muitos destinos. O tipo de serviço é determinado quando a conexão é estabelecida.

A camada de transporte é uma verdadeira fim a fim, que liga a origem ao destino [4]. Em outras palavras, um programa da máquina de origem mantém uma nova conversa com um programa semelhante instalado na máquina de destino, utilizando cabeçalhos de mensagens e mensagens de controle.

2.1.4.15- Camada de sessão

A camada de sessão permite que os usuários de diferentes máquinas estabeleçam sessões entre eles. Uma sessão permite o transporte de dados normal, assim como faz a camada de transporte, mas ela oferece também serviços aperfeiçoados que pode ser de grande utilidade em algumas aplicações [4]. Uma sessão pode ser usada para permitir que um usuário estabeleça um ***login*** com um sistema remoto de tempo compartilhado ou transfira um arquivo entre máquinas.

Um dos serviços da camada de sessão é gerenciar o controle de tráfego. Elas podem permitir o trafego em ambas as direções ao mesmo tempo ou apenas em uma direção de cada vez. Se esse tráfego puder ser feito em uma direção de cada vez, então a camada de seção poderá ajudar no monitoramento do controle do tráfego.

A camada de seção também tem a função do gerenciamento de ***token***. Para alguns protocolos, é de fundamental importância que ambos os lados não executem a mesma operação ao mesmo tempo. Para gerenciar essas atividades, a camada de sessão oferece tokens para serem trocados. Conseqüentemente, determinadas operações só puderam ser executadas pelo lado que está mantendo o token.

Um outro serviço da camada é a sincronização, ou seja, considere os problemas que podem ocorrer quando se está tentando fazer uma transferência de arquivos que tem duração de duas horas entre duas máquinas cujo tempo médio entre falhas seja de uma hora. Para eliminar esse problema, a camada de seção oferece uma forma de inserir pontos de sincronização no fluxo de dados, de moda que, quando ocorrer uma falha, apenas os dados transferidos depois do ponto de sincronização tenham de ser repetidos.

2.1.4.6- Camada de Apresentação

A camada de apresentação executa determinadas funções solicitadas com muita freqüência [4]*;* portanto, é necessário encontrar uma solução geral para todas elas, ao invés de deixar essa responsabilidade a cargo de cada usuário. Ao contrário de todas as camadas inferiores, que só estão interessadas em tornar confiável o processo de movimentação de bits de uma extremidade a outra ligação, a camada de apresentação se preocupa com a sintaxe e a semântica das informações.

2.1.4.7- A camada de Aplicação

A camada de aplicação contém uma série de protocolos que são comumente necessários [4].

Considere o trabalho de um editor de tela inteira que deve trabalhar com vários tipos de terminal, que, por sua vez, têm diferentes tipos de ***layouts*** de tela e seqüências de escape para inserção e exclusão de textos, movimentação do cursor etc. Isso provocaria um problema de incompatibilidade na hora de se tratar esses dados, a função dessa camada seria resolver esse tipo de problema.

Uma maneira de se resolver esse problema é definir um terminal virtual de rede, para o qual possam ser desenvolvidos editores e outros tipos de programa. Pra manipular cada tipo de terminal, deve ser criado um elemento de software que permita mapear as funções do terminal virtual de rede para o terminal real.

Outra função dessa camada é a transferência de arquivos. Diferentes sistemas de arquivos têm diferentes convenções de denominação de

arquivos e diferentes formas de representação de linhas de texto, entre outras coisas. Para transferir um arquivo entre dois sistemas diferentes, é necessário tratar essas outras incompatibilidades. Esse trabalho também pertence à camada de aplicação, assim como o correio eletrônico, a entrada de tarefas remotas, a pesquisa de diretórios e uma serie de outros recursos específicos e genéricos.

2.1.5 – O modelo de referencia TCP/IP

O modelo de referencia TCP/IP é baseado no modelo OSI, sendo assim, do mesmo modo que o OSI o TCP/IP também é dividido em camadas.

2.1.5.1 – Camada de Inter-redes

Todas as necessidades levaram à escolha de uma rede de comutação de pacotes baseada em uma camada de ligação de inter-rede. Segundo Andrew S. Tanembaum em seu livro *Redes de Computadores* [4] essa camada é definida de inter-redes, pois integra toda a arquitetura. Tanembaum também cita que a função dessa camada é permitir que hosts injetem pacotes em qualquer rede e garantir que eles sejam transmitidos independentemente do destino (que pode ser outra rede). É possível, inclusive, que esses pacotes cheguem em outra ordem diferente daquela em que foram enviados, obrigando as camadas superiores a reorganiza-los, caso a entrega tenha de respeitar algum tipo de ordem.

A camada de inter-redes define um formato de pacote oficial e um protocolo chamado de IP (Internet Protocol). A tarefa da camada de inter-redes é entregar pacotes IP onde são necessários. O roteamento é

uma questão de grande importância nessa camada, assim como evitar congestionamentos. Por essas razoes, é razoável dizer que a função da camada inter-redes TCP/IP é muito parecida com a da camada de rede OSI.

2.1.5.2 – Camada de Transporte

No modelo TCP/IP, a camada localizada acima da camada de inter-redes é a camada de transporte. *A finalidade dessa camada é permitir que as entidades par (peer entily) dos hosts de origem e destino mantenham uma conversação*[4], exatamente como acontece na camada de transporte OSI. Dois protocolos fim a fim foram definidos aqui. O primeiro deles, o TCP (Trasmission Control Protocol), é um protocolo orientado a conexão confiável que permite a entrega sem erros de um fluxo de bytes originado de uma determinada máquina em qualquer computador da inter-rede. Esse protocolo fragmenta o fluxo de bytes de entrada em mensagens e passa cada uma delas para a camada inter-redes. No destino, o processo TCP remonta as mensagens recebidas no fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens muito grande.

O segundo protocolo dessa camada, o UDP (User Datagram Protocol), é um protocolo sem conexão não confiável para aplicações que não necessitam nem de controle de fluxo, nem da manutenção da seqüência das mensagens enviadas. Ela é amplamente usada em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como a transmissão de dados de voz e vídeo.

2.1.5.3 – Camada de Aplicação

Acima da camada de transporte, está a camada de aplicação. *Ela contém os protocolos de alto nível. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP)* [4], como mostra a figura3. O protocolo do terminal virtual permite que um usuário de um computador estabeleça ***login*** em uma máquina remota e trabalhe nela. O protocolo de transferência de arquivos permite mover dados com eficiência de uma máquina para outra. Originalmente o correio eletrônico era um tipo de transferência de arquivos; no entanto, posteriormente um protocolo especializado foi desenvolvido para essa função. Muitos outros protocolos foram incluídos com o decorrer dos anos, como o DNS (Domain Name Service), que mapeia os nomes de ***hosts*** para seus respectivos endereços de rede, e o HTTP, o protocolo usado para buscar paginas na WWW (Word Wide Web), entre outros.

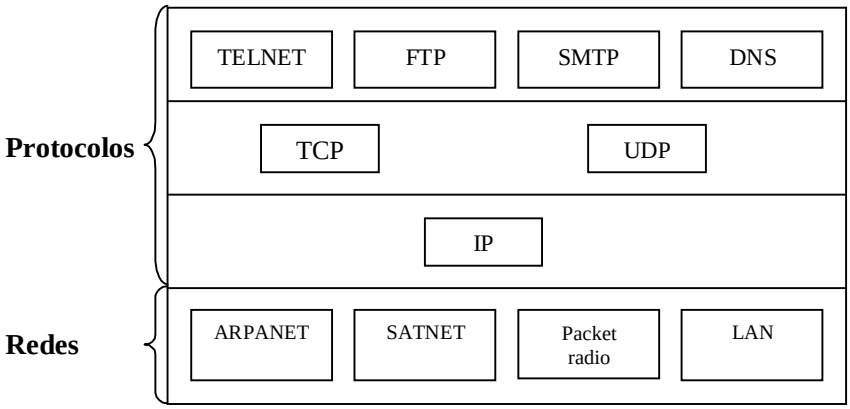

Figura 3 – Protocolos e redes no modelo TCP/IP

2.1.5.4 – Camada Host/Rede

Abaixo da camada inter-redes, encontra-se um grande vácuo. O modelo de referencia TCP/IP não especifica coisa alguma, exceto pelo fato de que o ***host*** tem de se conectar com a rede utilizando um protocolo, para que seja possível enviar pacotes IP. Esse protocolo não é definido e varia de host para host e de rede para rede.

2.2 - Digitalização de Imagens

Os novos computadores, programas e dispositivos vêm tornando os procedimentos para a transmissão de vídeo cada vez mais fácil e a tecnologia utilizada para tal finalidade cada vez mais acessível.

Podemos separar o processo da disponibilização de áudio e vídeo numa rede em três etapas:

1. Captura do sinal (câmeras, microfones).
2. Recepção e compactação digital do sinal de vídeo (encoder).
3. Transmissão do vídeo digital (server).

2.2.1 - Captura do sinal de áudio e vídeo

A primeira etapa é a captura do sinal que envolve basicamente a escolha dos dispositivos (câmeras e microfones) e a preparação do ambiente (iluminação, posicionamento, equalização do som)[5]. Existem diversos padrões de câmeras de vídeo no mercado, a escolha de um modelo adequado deve levar em conta o equipamento utilizado para a codificação, e a finalidade do vídeo, considerando-se os formatos de saída

de sinal, o formato de mídia utilizada e os recursos extras como zoom, autofoco e compensação de luminosidade.

O som pode ser capturado de um simples microfone de computador, para uma solução que não exige muita qualidade, ou através de uma mesa de som e amplificador, que possibilite balanceamento de sinal e ajuste de volume.

2.2.2 – Recepção e Compactação Digital do Sinal de Vídeo (encoder)

O sinal gerado pela câmera e microfones deve chegar em um equipamento preparado para receber, tratar e compactar a imagem e o som capturados[5]. Existem diversas maneiras de receber este sinal, dependendo do tipo de dispositivo utilizado. Os meios mais comuns de recepção de sinal são:

- **Serial/Paralelo (webcams)** - Foram os primeiros modelos de webcam, porém com taxas de transmissão e qualidade baixas.
- **USB (webcams)** - Padrão comercial mais utilizado hoje em soluções desktop que não exigem alta qualidade, devido ao preço e à facilidade de instalação e utilização.
- **Placa de Captura de Vídeo Analógico (webcams / câmeras de vídeo)** - Possui entradas padrões de vídeo analógico (RCA, S-Video, BNC), digitaliza o sinal analógico de entrada, tornando-o processável pelo computador, neste caso é importante ressaltar a compatibilidade da saída do sinal da câmera de vídeo com a entrada da placa.
- **Placa de Edição de Vídeo Analógico (webcams / câmeras de vídeo)** - Semelhante à anterior, porém possui também saídas de vídeo, e CODECS (responsáveis pela compactação) adicionais de processamento de vídeo.

- **Firewire (IEEE 1394) (webcams / câmeras de vídeo)** - Porta de transmissão de dados de alta velocidade, é utilizada para conexão de câmeras de padrão digital (DV), permite trabalhar com vídeo de alta qualidade, e permite comunicação bidirecional com a câmera (envia e recebe dados).
- **Placas de Edição DV (webcams / câmeras de vídeo)** - Placas com conectores IEEE 1394, e processadores de vídeo e CODECS em hardware, que "economizam" processamento principal.

A captura do vídeo gera um arquivo binário de vídeo. Algumas características desse arquivo, como tamanho, qualidade, extensão, dependem do formato utilizado pelo programa de gravação. A maioria dos programas trabalha com CODECS, que diminui o tamanho do arquivo armazenado em disco. É através desses softwares que é possível a configuração do tipo de transmissão, tamanho da imagem, largura de banda e outras.

2.2.3 – CODECS

O Codec é um programa para codificação/decodificação de áudio e vídeo.

Ao desenvolvermos uma aplicação multimídia que inclua vídeo é necessário garantir a instalação do Codec no sistema em que vai correr a aplicação, para que o vídeo seja descomprimido e visualizado.

"Vídeo para o Windows" contém Codecs que conseguem efetuar a descompressão de diversos formatos de vídeo.

Os Codecs mais usuais são:

- AVI
- INDEO

- Quicktime
- Targa DVM
- Cinepak
- Gif animation’s

2.2.4 – Digitalização

A digitalização de vídeo usa o mesmo princípio da transmissão, porém o que é digitalizado é o conteúdo visual que estará numa fita. Cada quadro do vídeo é uma imagem estática que é ***pixalisada****, ou seja, a informação de cor de cada ponto da imagem é armazenada em um pixel*[5].

A qualidade do vídeo digitalizado vai depender da quantidade de quadros capturados por segundo e da qualidade de cada quadro, que pode ser exprimida pela quantidade de pixels utilizados (dimensão da tela) e da quantidade de informação em cada pixel (variação das cores). Pode-se perceber que a digitalização de vídeo requer um grande espaço de armazenamento, por exemplo, para um vídeo a 30fps (frames por segundo), com dimensões de 620X560 e qualidade de 24 bits de cores, são necessários aproximadamente 30Mbs por segundo de vídeo gravado.

Porém já foram desenvolvidas diversas técnicas para a compactação e posteriormente para a transmissão de vídeo digital. Existem hoje diversas CODECS (compressão e descompressão) que utilizam técnicas avançadíssimas de algoritmos matemáticos, para comprimir dados redundantes e reduzir a demanda de espaço de armazenamento de banda para a transmissão.

2.3 - Transmissão de vídeos

Os arquivos gerados podem ser editados e disponibilizados em servidores de arquivos para ***download***. Alguns formatos de arquivo permitem o "progressive-download", que proporciona a visualização da parte do vídeo que já foi baixada, possibilitando acompanhar o conteúdo sem a necessidade de baixar todo o arquivo.

Outra opção de transmissão é utilizar formatos de stream, que possibilitam a transmissão de áudio e vídeo ao vivo pela Internet (ou outros meios como ISDN)[5].

Para realizar ***stream*** de áudio e vídeo pela Internet, é preciso garantir o fluxo contínuo de som e imagem, tarefa realizada por servidores de vídeo, que retransmitem aos ***players*** o sinal já digitalizado e compactado pelo encoder, gerenciando as taxas de transmissão para cada usuário. Alguns softwares de encoder realizam funções de servidor, dispensando o uso de um terceiro programa ou equipamento.

Para colocar um clip de vídeo numa página Web, pode-se optar pelo formato AVI ou Quick Time. Ao incluir um vídeo num destes formatos numa página Web, o cliente terá que telecarregar o vídeo completo e só depois é que este poderá ser executado.

O *streaming* de vídeo permite, apesar das larguras de banda serem bastante limitadas, transmitir vídeo na Internet com performances mais aceitáveis.

Na tecnologia de streaming a informação é estruturada usando ***buffers***, de forma a que chegue uma pequena parte do vídeo ao cliente para ser iniciada a visualização, enquanto decorre a visualização vai chegando constantemente mais informação de forma a tornar o processo ininterrupto. Esta técnica é uma forma de contornar o problema de restrição de largura de banda existente, pois dá a

sensação que o vídeo está a correr localmente, isto quando a largura de banda permite que a informação chegue mais rapidamente ao cliente do que é vista por este.

Para efetuar o *streaming* de vídeo é necessário criar o vídeo, *digitaliza-lo* e coloca-lo no servidor de *streaming*.

O vídeo pode ser criado através de um câmara, Camcorder ou VCR.

Formatos de vídeo apresentados por ordem decrescente de qualidade:

- D-1, D-2, D-3
- Formato Beta e 6.35 mm
- Laserdisk, CD-ROM e DVD
- Hi 8 e Super VHS-C
- Super VHS
- 8 mm e VHS-C
- VHS

Para digitalizar o vídeo é necessário ter uma placa de aquisição de vídeo (ex. Miro DC30), software de digitalização (ex. Miro capture) e o software de pós-produção (ex. Adobe Premier).

Depois de obtido o arquivo de vídeo digital, este terá que ser comprimido/codificado para depois ser colocado no servidor (ex. Netshow ou RealServer G2). O cliente terá que possuir um descompressor/descodificador (ex. MediaPlayer ou o RealPlayer).

Tem havido uma grande evolução nas tecnologias de compressão sendo a MPEG-2 a mais promissora, permitindo que com pouca largura de banda se efetue streaming de vídeo com bastante qualidade.

2.3.1 – MPEG-2

O MPEG (Motion Picture Experts Group) é uma norma de compressão de dados que permite codificar e decodificar uma seqüência de imagens assim como o áudio associado.

O MPEG-1 consiste num para armazenamento digital até 1.5 Mbit/s. Foi considerado um standard em Outubro de 1992.

O MPEG-2 foi normalizado em Novembro de 1993, possui muitas melhorias em relação ao MPEG-1. Encontra-se estruturado em 9 partes, As primeiras três partes foram normalizadas como standard Internacional, enquanto que as restantes são de níveis diferentes de competição.

As três camadas standard são:

Layer 1 - Camada de sistema

Largura de banda de 192 Kbps

Taxa de compressão de 1:4

Aplicações: DCC (cassetes digitais)

Layer 2 - Camada de vídeo

Largura de banda de 128 Kpbs

Taxa de compressão de 1:8

Aplicações: MiniDisk, MusicCam, e DVD

Layer 3 - Camada de Áudio

Largura de banda de 64 Kpbs

Taxa de compressão 1:10

Aplicações: MP3 (MPEG-1 layer 3)

A figura4 mostra como é feita a comunicação entre a captação de imagem até a chegada ao usuário

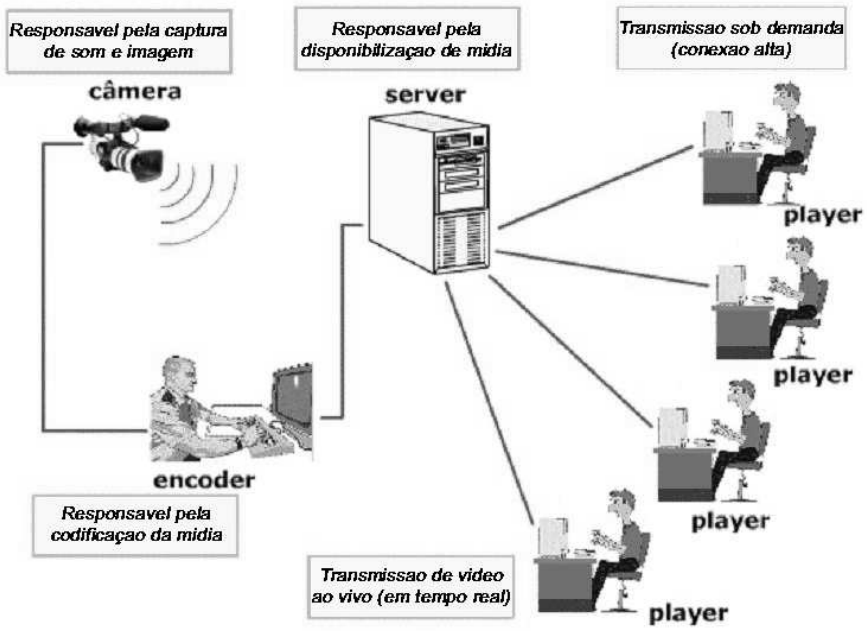

Figura 4 – Transmissão de vídeo

Uma observação importante a respeito da figura anterior é que existem dispositivos que eliminam o encoder e o servidor, ou seja, já existem câmeras que já codificam (encoder) e transmitem os dados a uma estação (player) sem a necessidade de passar por essas duas etapas de transmissão.

2.4 – Sistemas de Segurança

Um sistema de segurança muito utilizado por empresas é a vigilância de suas dependências através de circuitos fechados de televisão (CFTV).

Um circuito fechado de televisão se baseia em câmeras que captam o sinal do ambiente (as imagens) e as transmite até um terminal (um monitor).

2.4.1 - Circuito Fechado de Televisão – CFTV

A disponibilidade de circuitos fechados de televisão há vinte anos atrás foi recebida por potenciais usuários e consumidores com alguma suspeita.Em muitas circunstâncias, instalações foram levadas a cabo com base na mística do novo sistema gerado, do que a efetividade do sistema e a sua capacidade de assistir no gerenciamento global da segurança.

Hoje em dia o CFTV é aceito como uma efetiva ferramenta de gerenciamento e um meio através do qual os programas de prevenção em segurança podem ser estabelecidos e fortalecidos.As imagens produzidas pelo CFTV são, inclusive, aceitas como provas no indiciamento de meliantes em casos criminais.

Quais são os benefícios antecipados como resultado da instalação e uso do CFTV?

Podemos afiançar que a redução de mão de obra é um benefício direto, além do fator psicológico de dissuasão no controle de áreas.Assim tem-se observado que áreas tais como suporta de informações ao gerenciamento de segurança, prevenção ao fogo e alocação de recursos humanos são primariamente beneficiados quando o sistema é usado em seu efeito máximo.Todas essas áreas operam com maior eficiência, contribuindo por último com maiores lucros e menores perdas.

2.4.1.1 - Aplicação do Sistema CFTV

Há numerosas áreas em uma instalação, onde a vigilância por circuito fechado de televisão pode ser paliçada. A maioria delas são apresentadas a seguir, contudo, a discussão não pretende limitar o uso deste tipo de vigilância[6].

A aplicação do CFTV tem dois níveis de projeto:

- **Nível Tático**

O planejamento tático permite obter em uma visão globalizada do emprego do CFTV. Propõe, também, as várias alternativas disponíveis para cada plano de ação adotado, mostrando as conseqüências futuras dessa opção e as possibilidades de execução e realização.No nível tático, se descreverá o posicionamento de cada câmera, acompanhado da respectiva justificativa tático-operacional.Preconizará também as fases de implantação e sua prioridade, de acordo com o grau de segurança desejado.

- **Nível Técnico**

Nesse nível se definirá os tipos de CFTV a serem utilizados em cada um dos locais propostos, incluindo desde o memorial descritivo.Descreverá por exemplo se há a necessidade de implantar uma câmera colorida, o tipo de lente, o tipo de movimento, etc.

Aplicações Táticas

As aplicações táticas do CFTV podem ser divididas em quatros níveis :

- a primeira seria a de realizar o patrulhamento preventivo e ostensivo em áreas com grandes concentrações de público ou de veículos. O objetivo deste patrulhamento é o de identificar situações de risco e ajudar as equipes de pronta resposta, segurança, a responder a ação de agressão com melhor rapidez.Esta aplicação só será eficiente com a integração da equipe de segurança e o operador da central de monitoramento. Neste caso específico, as imagens devem ficar

"acesas" 24 horas, devendo a central identificar pessoas, veículos ou situações de risco.É um trabalho de equipe, onde o patrulhamento por CFTV ajudará no controle de área. A aplicação desta tática é em aeroportos, shopping centers, estacionamentos, controle de tráfego, estradas, etc.

- a segunda aplicação tática seria a gravação de imagens, através de video-tape, onde as áreas estariam patrulhadas 24 horas.O objetivo desta aplicação seria o de implantar o valor dissuasivo, onde a simples colocação do "espião do céu" inibe uma agressão por parte do meliante.Ou o registro das imagens poderá elucidar dúvidas e ou comprovações de furtos e roubos.Podemos citar como exemplo o emprego de uma câmera elevada para observar uma área das 18 hs às 06 hs da manhã. Ninguém estará controlando a câmera, por estar sendo utilizado o vídeo-tape. No dia seguinte, em cerca de uma hora, tudo o que a câmera gravou durante as 12 horas da noite poderá ser revisto. Esta tática é a mais comum em ser aplicada em agências bancárias, saídas e entradas de estacionamento, áreas de embarque e desembarque de mercadorias, etc.

- a terceira aplicação tática é o emprego direto na substituição da mão de obra.O CFTV irá ser implantado com o objetivo de ser uma força de segurança.É a aplicação mais complexa de ser considerada como eficaz e eficiente, pois exige uma integração com os demais sistemas de segurança, tais como controle de acesso, intrusão, iluminação, etc.

- Podem ser utilizados como método de vigilância, operado eletronicamente no qual portões perimetrais de veículos ou de pessoal são controlados à distância.Essa possibilidade é indicada particularmente para aplicação em controles de diversos portões utilizados intermitentemente.Um guarda, junto ao mais movimentado ponto de entrada e saída, poderá controlar diversos portões de modo eficaz.

Esta aplicação deve proporcionar economia superior à tentativa de controle de portões com diversos seguranças, e aumentará a segurança junto a esses portões, principalmente se no passado eram deixados abertos, por certo período de tempo, sem controle.

A vigilância em cercas perimetrais, particularmente em áreas afastadas, pode ser realizada com mais eficiência e economia com o CFTV, atrelado a sensores de intrusão, do que por patrulhas da equipe de vigilância. Em caso de uma intrusão a câmera automaticamente se deslocará para a área sinistrada, mostrando a imagem exata do ponto de intrusão em tempo real ao operador da central de segurança.

Em operações de embarque e desembarque de mercadorias, em especial quando as operações cobrem grandes áreas e o material que está sendo manuseado pode ser rapidamente surrupiado.Este tipo de vigilância em docas e plataformas de carga e descargas pode ser utilizado em conjunto com rondas da equipe de vigilância.

Outra aplicação casada do CFTV é no controle de identificação e controle de pessoal e veículo, onde a câmera é instalada para verificar e patrulhar a área de acesso e respectivamente a situação de risco. Ou em áreas de alta segurança que o CFTV irá checar, em conjunto com o sistema de controle de acesso, se aquela pessoa autorizada a entrar é a mesma detentora do cartão.

Na realidade, hoje, as aplicações do circuito fechado de televisão no campo da segurança são realmente ilimitados.

- o quarto e último nível de aplicação tática é sua utilização em áreas onde a empresa quer monitorar sem que as pessoas percebam. Na realidade a aplicabilidade é para a realização de investigações empresariais, com o objetivo de detectar ou identificar situações concretas de furto e fraude.

Operação e Localização da Câmera

A exata localização da câmera, incluindo a altura em que será instalada, pode ser determinada pelo movimento de pessoas, dentro da posição que o equipamento tomar.

Geralmente, o que esta pessoa vê num certo período de tempo do dia e da noite, é, aproximadamente, a quantidade de observações permitidas pela câmera, a menos que haja pouca iluminação. Antes da montagem definitiva, a câmera deve ser instalada temporariamente para dupla verificação das posições mais vantajosas.

Estabelecida à localização de cada câmera, a decisão seguinte será totalmente integrada com outros sistemas ou será manual ou através de combinação de ambos. Deverá ser decidido o ponto de controle de cada câmera, quem irá controlá-las e o treinamento que será exigido para assegurar operações corretas. A manutenção é o passo seguinte a ser considerado como de extrema importância nas operações de segurança.

Relação Custo X Benefício

A aplicação correta do CFTV num plano de proteção, pode e deve reduzir substancialmente o custo da mão de obra.Mesmo exigindo capital inicial, a redução em mão de obra num período de tempo resultará em enorme economia de custos. Planos de leasing, por exigirem pouca saída de capital, são oferecidos pela maioria dos fornecedores.

A maior economia poderá ser obtida de um sistema que permite que cada câmera seja utilizada durante 24 horas do dia. A aplicação correta deste tipo de vigilância, normalmente, resultará na total e constante monitoração da área.

Em segundo plano, devem ser feitas considerações sobre o método a ser empregado para controlar a câmera. A eficiência de qualquer sistema de CFTV, num plano de segurança, dependerá quase que exclusivamente do sistema de monitoração, a ser realizado pela central.

Em terceiro plano, devem ser previstas providências para a resposta e início da ação corretiva se forem detectadas condições desfavoráveis na área monitorada.

Se essas condições puderem, efetivamente ser reunidas, sem aumentar as horas de mão - de - obra de segurança, é quase certo que poderá ser justificada a quantia que foi dispendida na aquisição do sistema de CFTV.

Erros Táticos Mais Comuns

Podemos selecionar três distorções mais comuns em projetos de segurança são:

- a aplicação de câmeras no interior de edificações e depósitos, sem estarem atreladas a outros sistemas.Esta aplicação tem como ótica a tática de que o operador da central de monitoramento será capaz de identificar situações de risco na frente de uma dezena de câmeras, com inúmeros monitores. É uma ilusão a montagem de centrais com variados monitores, onde o recurso humano é o responsável direto em identificar situações de risco;

- a aplicação de câmeras no patrulhamento externo, principalmente na barreira perimetral em toda sua extensão. Da mesma forma que o tópico anterior, é nula esta aplicação em toda sua extensão. O ideal é que seja instalada em pontos realmente considerados críticos e que estejam integrados com os sistemas de intrusão e de pânico. Ao ser acionado um destes sensores as câmeras entram em ação, em conjunto com uma série de medidas, tais como acionamento de luzes, sirenes e a imagem pode ser focado no ponto sinistrado. A câmera pode

estar atrelada com um detector infravermelho, acompanhando os respectivos movimentos. Os projetos de CFTV têm de estarem focados no cobrimento de áreas, integrados com outros conjuntos. Só se justifica a aplicação deste conceito, implantação de CFTV em patrulhamento externo, em áreas ou regiões consideradas críticas para atos de terrorismo, onde as câmeras estariam identificando situações "anormais" ao redor da edificação;

- a instalação de câmeras que não são, tecnicamente, condizentes, com os locais a serem monitorados.Geralmente falta iluminação, não possuem zoom, não coloridas, não possuem definição clara, etc. Este erro acontece por falta de conhecimento do homem de segurança ou por redução efetiva da verba.Cabe ressaltar que o gerente de segurança tem de contar com o apoio técnico para a especificação do equipamento, evitando desta forma instalar sistema inoperante. A redução de verba sempre prejudica a eficácia de sistemas. O que tem que ficar claro é que existem sistemas para todas as necessidades, dentro de um nível de segurança e que a empresa tem de ficar consciente de que as instalações de sistemas sem as características precisas fazem com que gaste a verba desnecessariamente, pois a inoperância será comprovada ao longo do tempo de sua utilização.

Estas distorções têm como conseqüência direta a ineficiência do sistema, pois fica inócua a função preventiva e a de pronta resposta, prejudicando sobre maneira o emprego e imagem do Circuito Fechado de Televisão.

É função da gerência, supervisão de segurança empresarial lutar para que estas distorções não venham a acontecer, sempre justificando cada item, no nível tático, técnico e financeiro.

2.4.2 – Centrais de Segurança

Uma outra questão que deve ser olhada com muito cuidado é a respeito de onde ficará a central de dados.

A central de segurança é o cérebro e o centro nervoso de qualquer organização.A central otimiza os recursos empregados, além de coordenar de forma ágil e em tempo real as contingências na edificação[7].

Na maior parte dos edifícios e empresas, existentes hoje no Brasil, os espaços das centrais sempre estão relegados a um segundo plano, localizadas em pontos considerados não estratégicos e, por conseguinte inseguros.

As organizações acabam esquecendo que os sistemas implantados por si só não garantem a segurança da central.É um detalhe que põe em risco todo um investimento, derrubando por terra sistemas sofisticados.

A central de segurança mantém em constante vigilância os pontos críticos levantados, possibilitando gerenciar e comandar as situações críticas de modo direto.As reações são automatizadas, reduzindo desta forma o erro humano.Os impactos são reduzidos, tendo como conseqüência direta a preservação do patrimônio e vidas humanas.

A operacionalidade da Central depende basicamente de dois fatores:

-a rapidez da identificação da anormalidade;

-a reação rápida e eficaz da equipe e coordenação.

A identificação rápida da anormalidade está alicerçada, especificamente nos meios que a central dispõe.Há a necessidade do operador possuir a visão globalizada dos pontos críticos de todo o complexo monitorado.

A resposta dependerá do treinamento e principalmente no acionamento das equipes.O acionamento e treinamento serão mais eficazes quando forem direcionados ao ponto exato da área sinistrado.

Dentro deste enfoque a central tem e deve ser olhada sob uma ótica diferenciada, ou seja, a central deve ser encarada como um castelo medieval, e a ponte elevadiça seu acesso.Fica claro que na queda da ponte todas as defesas se anulam automaticamente, inviabilizando qualquer tipo de sistema.

Localização da Central de Segurança

O local das centrais de segurança deve ser de difícil acesso e com proteção especial.A entrada da central deve ser controlada e restrita.

Infelizmente isto não ocorre, pois a maior parte das centrais de segurança foi adaptada a prédios já existentes, nos quais não houve a preocupação de segurança.A maioria das centrais estão localizadas em locais de fluxo intenso de pessoas e veículo, tais como sub-solos, mezaninos e em portarias.

Outro ponto comum e de insegurança é que a maior parte das centrais de segurança estão juntos também das centrais de utilidades prediais.A junção pode economizar espaço físico da incorporação, mas deixa extremamente vulnerável a questão do acesso.Numa central de utilidades prediais os respectivos sistemas de multifunção, muita gente deve e tem de ter acesso.Por esta razão a autonomia da central de segurança se torna, sem dúvida um item de suma importância.

3 - Metodologia

A metodologia utilizada nesse trabalho pode ser dividida em 3 grandes grupos: a fase de estudo das tecnologias existentes que poderiam ser utilizadas para concretização desse projeto, o estudo do local e métodos para uma perfeita instalação do sistema e por último a implantação visando uma melhor performance.

Na primeira fase foram estudadas tecnologias de redes, digitalizações e transmissões de vídeo pela rede e sistemas de segurança.

Ao estudar as tecnologias de rede foi realizado um aprofundamento nos temas transmissão de dados e protocolos utilizados em LAN's, isso foi feito analisando modelos de referencia tipo OSI e o TCP/IP. Foram verificadas também as tecnologias para transmissão utilizando fibras ópticas, cabos UTP categoria5 e wireless (tecnologia IEEE 802.11-b).

Observou-se então que o processo para a disponibilização de áudio e vídeo numa rede segue em três etapas:

1. Captura do sinal (câmeras, microfones).
2. Recepção e compactação digital do sinal de vídeo (encoder).
3. Transmissão do vídeo digital (server).

Visto essa separação, um estudo de quais tecnologias existentes para cada uma dessas três etapas foi realizado, tentando assim obter uma melhor base de conhecimento para elaboração do sistema, utilizando uma solução mais eficaz.

No tópico que diz respeito à transmissão de vídeos por redes estudou-se, dentre todas as tecnologias existentes, uma melhor forma para transmitir esses dados até a guarita de vigia continuamente, parecido com um filme, para não haver nenhuma falha de segurança no que está ocorrendo no local.

Também foi estudado sobre sistemas de segurança para que fosse possível elaborar um sistema, sem a existência falhas de vigilâncias.

Depois de feito o estudo teórico das tecnologias existentes começou a ser realizado um levantamento dos equipamentos disponíveis no mercado (como câmeras e equipamentos de transmissão) para que o sistema pudesse se tornar operante.

Dentre as tecnologias estudadas optamos em analisar uma câmera da fabricante AXIS, visto que essa apresenta uma melhor adequação as exigências e ao custo beneficio para a implantação.

Terminado o estudo da câmera foi realizado então uma pesquisa de onde seriam colocados os pontos[2] de vigilância (as câmeras), e as melhores formas de transmissão de seus dados até a guarita de vigilância.

Depois de formulado todo o projeto foi realizado então entrevistas com os responsáveis pela administração da Universidade (a Pró-Reitora de Administração – Iara) e com o chefe dos seguranças da Universidade para solidificar as dificuldades e os interesses da obtenção do sistema.

[2] (esses pontos são ditos pontos críticos e suas finalidades são as de cobrir o edifício em questão de modo a não deixar falhas de vigilância)

4 - Resultados e Discussões

Durante a realização do projeto alguns pontos se caracterizaram com uma maior importância. Estes pontos a partir de agora serão analisados e discutidos para melhor compreendermos o conteúdo desse projeto.

È importante antes de analisarmos a construção do sistema, sabermos um pouco como funciona essa idéia.

O sistema deve consistir de uma tecnologia que possa transmitir imagens de segurança através de uma rede LAN (como demonstrado na figura5), ou seja, devemos criar uma forma de enviarmos essas imagens do local vigiado até a guarita de vigia.

Figura 5 – Esquema de funcionamento do sistema

4.1 - O Protocolo e a forma de Transmissão

O primeiro ponto a ser analisado é com relação as redes existentes e seus protocolos. No nosso caso, os métodos de transmissão e os protocolos utilizados, para que o sistema funcione de uma forma otimizada, considerando os aspectos tecnológicos e financeiros.

Analisando assim podemos começar pela escolha de transmissão, utilizando o protocolo TCP/IP. Sua escolha ocorreu pela tamanha dimensão que

este protocolo tomou nos dias atuais nas redes e, por ser bastante difundido conseguimos distribuir os sinais capturados pelas câmeras a uma maior porcentagem de estações de visualização sem possíveis ocorrências de incompatibilidade e conflitos.

Com relação à transmissão desse sinal no nosso caso fica mais fácil, por já existir uma infra-estrutura, utilizando transmissões via cabo e wireless (IEEE 802.11-b).

Quando falamos dessa infra-estrutura queremos dizer a Rede UFLA que já existe no campus, contendo em seu backbone uma grande extensão de fibras ópticas e cabos UTP categoria5, além de seus elementos ativos como conversores ópticos, switches, servidores, etc. Alem disso ela conta também com uma estrutura já montada de wireless (IEEE 802.11-b).

As escolhas pela melhor forma de transmissão foram feitas baseando-se nas facilidades ou limitações encontradas para instalação do sistema.

O primeiro ponto observado para a instalação foi à forma de conectar as câmeras de vídeo até o rack que contem o switch gerenciador dessa rede. A melhor solução encontrada para esse primeiro problema foi fazer um cabeamento através de cabos de cobre (cabos UTP categoria5 rígidos ou cabos coaxiais). A escolha entre qual desses cabos proporcionaria uma melhor instalação ocorreu após a analise de qual tipo de câmera seria utilizada, onde serão citados no decorrer do texto.

Um outro ponto crucial, falando em transmissão desses dados, seria a forma de enviarmos essas informações até a guarita de controle (guarita de vigia). Por ser uma longa distancia dos pontos de captura até a guarita e ela apresentar-se em um local de difícil acesso a cabos de cobre (cabos UTP categoria5) ou de fibras ópticas, trabalhou-se então com a idéia de se formar essa parte da rede utilizando transmissão wireless. Como a Universidade já possui

este tipo de sistema foi então estudado a forma de adaptamos a ele o envio de nossos dados.

Feito esse estudo chegamos à tecnologia wireless de transmissão de dados conhecida como IEEE 802.11-b, onde com dois kits conseguimos enviar tais dados até a guarita e assim criarmos uma WLAN (Wireless Local Área Network) nessa parte da rede.

4.2 - A escolha das câmeras

Um outro problema encontrado foi o de escolher qual a tecnologia das câmeras seria melhor para a criação do sistema.

Dentre vários sistemas encontrados no mercado, dois desses apresentaram uma melhor adaptação para as necessidades que o projeto exigia. Esses dois sistemas serão discutidos e analisados a seguir.

A primeira tecnologia baseia-se em câmeras que após captar o sinal o enviam até um micro onde são capturadas as imagens por uma placa especial.

Analisando melhor o funcionamento dessa tecnologia temos que a placa de vídeocaptura e gravação de imagens digitaliza os sinais e produz uma varredura, trazidas em frames por segundo (FPS); assim as imagens são formadas e a sensação de movimento é mostrada no monitor do computador. Todo o conteúdo dos eventos pode ser comprimido e armazenado no HD do computador através de um algoritmo matemático. Através de um software fornecido junto com a placa DSR (Digital Surveillance Recorder), o usuário, no nosso caso o vigilante, pode também monitorar varias câmeras ao mesmo tempo, ativando a função QUAD, monitorar as câmeras seqüencialmente, verificar as imagens gravadas com a função play-back, enfim, uma série de recursos que estão incorporados no utilitário.

Alem das funções apresentadas, a placa possui a função vídeo motion detection technology, onde faz com que sejam gravadas somente cenas com movimentos, ou seja, atua como sensor de mudança de quadro (pixel). A gravação das cenas é registrada com data, hora e em alguns modelos, uma marca d'agua é feita para impossibilitar cortes ou edições nas gravações, permitindo dar veracidade às cenas gravadas.

A placa também tem a função de central de alarme e pode enviar via modem/TCP-IP/IPX em alta velocidade as imagens do evento ocorrido ou um arquivo de som (wav) pré-gravado, discando automaticamente para telefones programados. A transmissão das imagens é feita num modo acelerado e o formato dos arquivos enviados é compactado, diminuindo assim o tamanho dos mesmos. A sensibilidade da imagem gerada por câmera pode ser ajustada, permitindo que as instruções sejam registradas sem o emprego de sensores de qualquer tipo.

Um outro recurso e, um dos mais importantes para nosso projeto, é a possibilidade de ligar esse sistema de vigilância digital numa rede local (LAN) e acessar as câmeras através de estações de trabalho (Clients) que fazem parte dessa rede, ou de locais remotos co acesso a Internet, conforme a figura6. Desta forma, um usuário (o vigilante) pode acessar qualquer câmera instalada no sistema e verificar as imagens on-line ou usar o playback com histórico de eventos, mediante uma senha de acesso.

Terminais permitem a colocação de conectores (DB9, DB15 ou DB25) por intermédio de flat cables, disponibilizando entradas e saídas utilizadas para a inclusão de sensores do tipo NA/NF ou interface de acionamento de dispositivo eletrônico. Associa-se a cada zona protegida uma câmera, e, no ato da violação, teremos alteração no nível lógico da entrada que estiver acoplada ao sensor, portanto começará a gravação das cenas. Por outro lado, o nível lógico na saída

também será alterado, possibilitando, por exemplo, que uma sirene seja disparada pela interface.

A comunicação dessa câmera ate a placa de vídeocaptura é realizada por meio de cabos coaxiais para vídeo, proporcionando assim a utilização de qualquer câmera existente no mercado com essa característica de transmissão.

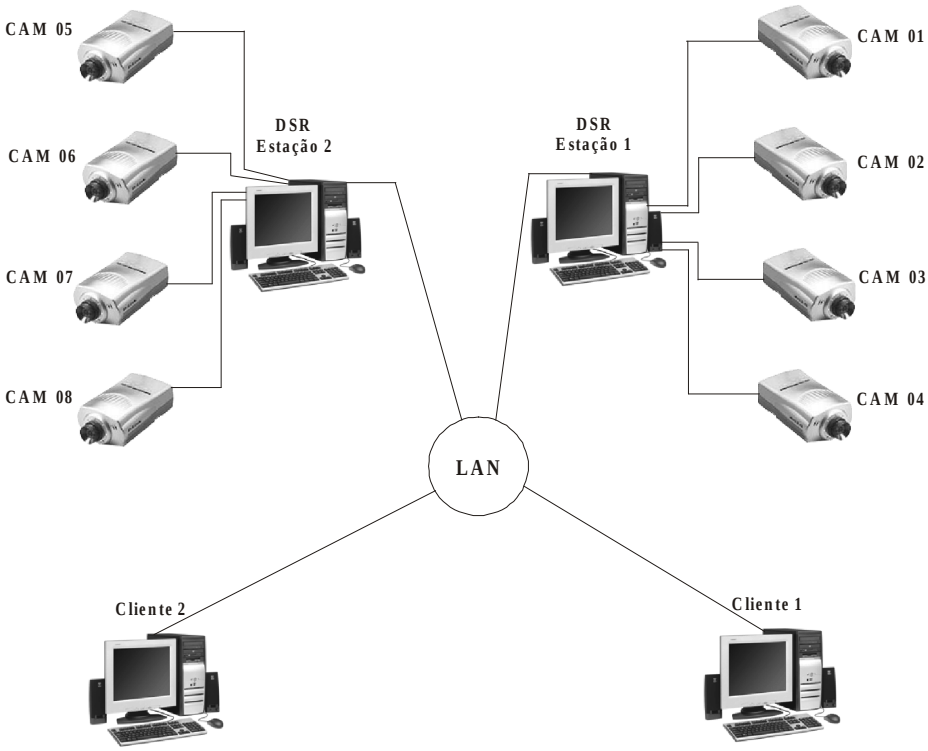

Figura 6 – Configuração do sistema remoto de vigilância.

A segunda tecnologia encontrada foi a de transmissão dessas imagens a partir da própria câmera, ou seja, uma tecnologia de transmissão onde ela mesma já digitaliza as imagens e as transmite sem auxilio de um micro para captura.

Isso foi encontrado em uma câmera fabricada pela empresa AXIS, conhecida como AXIS 2110, onde maiores detalhes serão apresentados a seguir.

A AXIS 2110 Network Câmera é uma solução com excelente custo-benefício para uso em ambientes externos e internos, para monitoramento à distância ou atração da Web. A AXIS 2110 envia até 15 imagens/segundo através de um navegador padrão.

Ela é melhor do que as câmeras de Rede comuns, pois vem com um servidor de Rede, e se conecta como uma unidade independente diretamente a uma rede ou via modem -- não precisa de um PC ou de programas adicionais.

Os recursos encontrados na câmera em questão são:

- Imagens de alta qualidade - até 15 quadros/seg – isso implica na taxa de transmissão dessas imagens, ou seja, conseguimos uma transmissão a 15 FPS (quadros por segundo) resultando assim em algo parecido com um filme.
- Dispensa acessórios adicionais, programas e cabos de vídeo – essa câmera é capaz de enviar seus dados para um simples browser (Internet Explorer ou Netscape, por exemplo) sem a necessidade de programas para visualização e digitalização dessas imagens, um outro ponto é que com um simples cabo UTP categoria 5 conseguimos conecta-la a rede de um determinado local.
- Servidor de Rede embutido – graças a esse servidor embutido em seu interior essa câmera é capaz de digitalizar as imagens e servi-las a rede sem a necessidade de um servidor ou um micro para digitaliza-las.
- Lentes para ambientes externos com muita luz – devido a ambientes externos varias vezes possuírem muita luz ela é preparada para não perder resolução por vazamento de imagens (imagens que se tornam

ilegíveis devido à concentração de muita luz na lente captadora) logo que suas lentes são preparadas especialmente para ambientes externos.

- Zoom manual 2.3 x – são preparadas pra aproximarem ate 2.3 vezes o objeto focalizado, porem lentes adicionais podem ser adquiridas para uma aproximação maior e automática.
- Funciona com o AXIS 2191 Audio Module – esse equipamento citado é fabricado pela própria empresa e proporciona a câmera um aspecto de áudio, ou seja, a zona captadora passa a ter noções de áudio do ambiente vigiado mesmo como envia áudio para mesma área.

Além dos recursos proporcionados pela câmera seria interessante também apresentar as especificações técnicas para assim melhor compreendermos seu funcionamento.

Geral

- Servidor da Web embutido e interface de rede. Não necessita de um PC para operar.
- Poderoso Sensor de Movimento com múltiplas janelas de detecção.
- Sistema operacional baseado em Linux.

Instalação

- Instalação rápida e fácil - é só conectar a sua rede e atribuir um endereço de IP ou usar o cabo de modem nulo incluído para instalação por modem.

Câmera

- Digital, 24-bit cores.

Sensor de imagens

- 1/3 inch Sony super HAD interlaced CCD.
- HxV: 768x495 (NTSC), 752x582 (PAL).
- Resolução (pixels): 704x480 (NTSC) 704x576 (PAL).

Exposição

- Compensação de Luz de Fundo.
- AGC automático.
- Equilíbrio Automático e fixo de Branco.
- Desligamento automático: 1/60s (1/50s)-1/10.000 seg. NTSC (PAL).

Sensibilidade

- Mínimo de luz: 1 ▪ 200,000 Lux com lentes F1.0 DC-Iris. De 1 a 5,000 Lux com lentes de íris fixa.

Lentes

- Suporte de lente ajustável padrão CS.
- DC-Iris vari-focal (zoom) lentes 3.5 ▪ 8.0mm eqv. a 25-55mm em uma câmera de 35mm. Ideal para monitoramento externo (em quintais de casas).

Imagem

- Quadros por segundo: até 30 (25) quadro/s com 352x240 (352x288) de resolução. até 12 (10) quadro/s com 704x480 (704x576) de resolução. NTSC (PAL).
- Vídeo motion-JPEG, e imagens fotográficas de JPEG.
- Compactação de imagem em alta velocidade baseada em hardware, gerando imagens JPEG de alta qualidade.
- 5 níveis de compactação disponíveis. O tamanho do arquivo de uma imagem JPEG compactada depende do conteúdo real da imagem. Imagens com muitos detalhes geram arquivos maiores. A qualidade da imagem é controlada pelo nível de compactação. A alta compactação garante arquivos menores, porém a qualidade de imagem cai, enquanto a baixa compactação resulta em arquivos maiores, mas conserva a qualidade de imagem. A tabela abaixo apresenta uma média de tamanhos de arquivo, derivada de testes práticos.
- Controle da amplitude de banda variável evita a saturação de dados na rede. 30 quadros/segundo normalmente exigem aproximadamente 1,5 Mbps.

A tabela1 demonstra o nível de compressão atingida nos níveis ultrabaixo, baixo, médio e alto dependendo da resolução utilizada.

Nível de Compressão e Resolução				
	Muito Baixo	**Baixo**	**Médio**	**Alto**
640x480	250Kb	20Kb	13Kb	8Kb
320x240	70Kb	8Kb	5Kb	3Kb

Tabela1 – Intensidade de compactação dependendo da resolução

Condições de luminosidade e grados por segundo

- Como podemos ver no gráfico abaixo quanto maior a luminosidade melhor será a transmissão de quadros por segundo, estabilizando-se a 40lux a uma transmissão de 15 quadros por segundo.

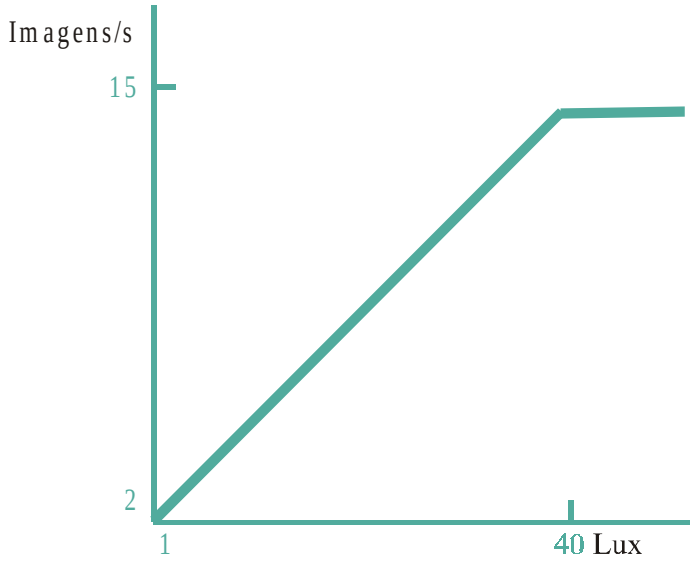

Grafico1 – intensidade de luz com imagens transmitidas por segundo

I/O Geral

- Aceita dial-in and dial-out via modem externo (não incluído).
- Armazenamento de imagens remota acionada por eventos via e-mail e FTP.

Exigências de Sistema

- Compatível com sistemas operacionais como Windows 98, Windows 2000, Windows XP, Windows NT, Windows ME, Linux, Mac OS e Mac OS X.
- Internet Explorer 4.x, 5.x, 6.x ou Netscape Navigator 4.x, ou superiores.

- Sem rede, ex. instalação por modem exige Windows PC com Dial-up.

Protocolos Suportados

- TCP/IP, HTTP, FTP, SMTP, ARP, BOOTP, PPP, CHAP, PAP, DHCP e outros.

Segurança

- Proteção por senha/nome de usuário para acesso restrito a câmeras.

Hardware

- Chip de compactação ARTPEC-1.
- Processador ETRAX 100, RISC de 32 bit, CPU de 100 MIPS para alto desempenho.
- 16 Mbytes RAM
- 4 Mbytes FLASH PROM.

Updates de Firmware

- Memória flash para upgrade simples e armazenamento de arquivos html criados pelo usuário.

Conexões

- Conexão direta de rede através de cabo duplo torcido RJ45 para 100baseTX Fast e 10baseT Ethernet.
- Porta RS-232 para conexão com modem ou controle de dispositivos RS-232.
- Adaptador de Entrada/Saída para acionar a câmera em eventos externos
- Adaptador para lentes DC-Iris.
- Botão de controle para padrões de fábrica.

Fonte de Energia

- Adaptador externo de fonte de energia de 13V DC, 25W.

Ambiente Operacional

- Exige compartimento próprio para uso externo.
- Temperatura operacional: 5 ▪ 50 ▪ C.
- Humidade: 20-80% RHG, antecondensante.
- Deve-se usar lentes DC-Iris e configurá-las corretamente para ambientes com luminosidade intensa. Evite apontar a câmera diretamente para objetos extremamente brilhantes como o sol, pois isso pode danificar o sensor de imagens CCD.

Dimensões / Peso

- Altura: 5.7 cm
- Largura: 8.6 cm
- Comprimento: 13.8 + 4.5 cm (lentes)
- Peso: 0.25 kg (sem a fonte de energia e o tripé)

Aprovações

- EMC: FCC Classe A, Parte 15 subparte B
- CE : EN 55022 Class B, EN55024
- Segurança: EN 60950, UL, CSA.

Através das figuras seguintes conseguimos ter uma noção do que é realmente a câmera AXIS 2110.

Figura 7 – Visualização frontal da câmera AXIS 2110

Figura 8- Visualização Frontal com a base de sustentação da câmera AXIS 2110

Figura 9 – Visualização da parte traseira e seus conectores de rede da câmera AXIS 2110

Figura 10 - Visualização da parte frontal e lateral da câmera AXIS 2110

Após analise dos recursos das tecnologias, pôde ser feita uma comparação entre as duas, para assim melhor adaptarmos ao sistema.

A primeira tecnologia apresenta a necessidade de um microcomputador para digitalização das imagens, já a segunda não necessita disso, logo que contem um processador embutido que possibilita assim a digitalização ser feita pela própria câmera.

Um outro ponto a ser ressaltado nessa comparação é a facilidade de visualização dessas imagens, a segunda tecnologia não necessita de software algum adicional para serem vistas as imagens disponíveis na rede, já na primeira torna-se necessário um software especial para digitalização e visualização. O resultado dessa necessidade ou não do software é a facilidade de se observar essas imagens em qualquer lugar, ou seja, a tecnologia da câmera AXIS 2110 proporciona uma portabilidade maior, já que em qualquer micro podemos visualizar as imagens apenas digitando o endereço IP correspondente à câmera em um browser.

Observamos também que a preparação das lentes e dos chips de captura de AXIS 2110 proporciona uma visualização melhor das imagens em situações de pouca luz, (ela consegue capturar sinal com apenas 1lux de luminosidade) e com muita luz tendo sua lente preparada contra vazamento de imagem como foi citado anteriormente.

Uma outra comparação possível é a respeito do numero de quadros que cada tecnologia consegue enviar por segundo, onde a tecnologia baseada em captura do sinal através de placa de captura proporciona uma melhor velocidade de frames por segundo (FPS) podendo chegar até a 60 frames por segundo dependendo dos componentes utilizados, e a tecnologia da AXIS 2110 apresenta-nos até 15 frames por segundo. Isso pode ser considerado relevante se o objetivo for transmitir um filme perfeito como de cinema, mas para vigilância

o interesse é apenas em movimentos estranhos o que leva a velocidade de 15 frames por segundo ser muito bem aceitável.

Um outro ponto a ser analisado é a compactação dessas imagens para serem distribuídas pela rede, onde a AXIS 2110 consegue uma compactação em quatro níveis diferentes, fazendo assim com que a rede não fique carregada em momentos que não sejam necessários, ou seja, podemos configurar a câmera para um nível de compactação mais alto quando a necessidade de vigilância não for tão preocupante.

As demais funções das tecnologias são parecidas, mudando somente o meio de como são implementados.

Após essas observações chegamos a conclusão que a tecnologia da AXIS 2110 é a melhor para finalizarmos a construção do sistema de vigilância.

Com a escolha da tecnologia que iremos utilizar podemos definir qual cabeamento irá levar o sinal das câmeras até o switch gerenciador dessa rede. O cabeamento adequado então passa a ser o cabo UTP categoria 5 rígido.

4.3 - Identificação dos Pontos Críticos e do Local da Guarita de Vigilância

A escolha desses pontos foi baseada no prédio da reitoria da Universidade Federal de Lavras (UFLA) de forma a cobrir todo o território do edifício, ou seja, precisaríamos escolher pontos que cobrissem todas as entradas, mesmo como as dependências ao seu redor.

Assim foram escolhidos os pontos da seguinte forma:

- O primeiro ponto foi no canto superior esquerdo no fundo do prédio, onde, a câmera captará o lado esquerdo do prédio até a entrada principal e parte do estacionamento.

- O segundo ponto foi no canto superior esquerdo, porém na frente do prédio, onde irá capturar as imagens da parte frontal até seu ponto médio e parte de seu gramado.
- O terceiro ponto foi no canto superior direito do prédio na parte frontal, visto que a área de visualização desse ponto limita-se a capturar imagens desse lado direito até o ponto médio e parte de seu gramado.
- O quarto ponto foi o canto direito do prédio na parte dos fundos, porém esse ponto não poderá ficar no próprio edifício tendo que se localizar afastado, para conseguir assim cobrir todas as entradas; e sua área de visualização se restringira ao lado direito observando a entrada especial para o reitor e a entrada do DRCA.
- O quinto ponto se localizara na entrada principal do prédio para conseguirmos assim vigiar toda a movimentação nesse importante ponto de acesso.

Os pontos citados anteriormente geram um esquema como é demonstrado na figura11.

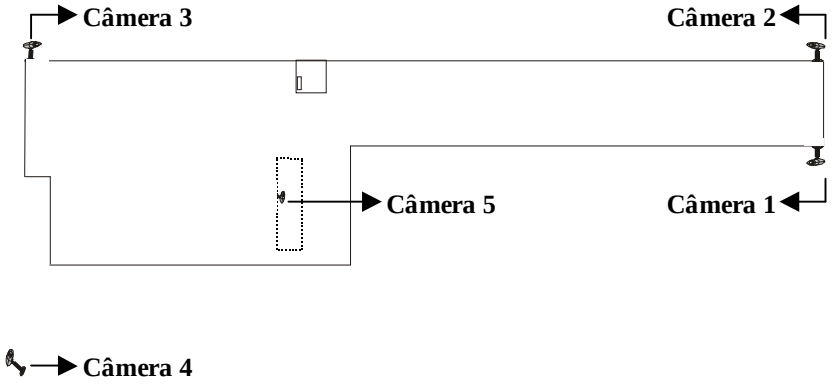

Figura 11 – Esquema de Pontos Críticos

Feito a escolha dos pontos será pesquisado um local para a instalação do centro de monitoramento.

Como a Universidade já possui uma guarita de vigia, foi escolhido então que este local funcionasse como o centro de monitoramento, as formas de como chegaremos esse sinal até esse centro serão explicadas no próximo tópico.

4.4 - O Projeto

Com todas as tecnologias necessárias para implantação do projeto devemos analisar como foram agrupadas para que o sistema de vigilância torna-se operante.

Conforme demonstrados na figura11, os pontos de vigilância foram demarcados; porém é preciso agora conecta-los a rede, ou seja, devemos conecta-los ao switch gerenciador para que esses dados possam ser distribuídos pela rede local.

Para realizarmos essas conexões foi escolhido o cabo UTP categoria 5 rígido, ficando o nosso esquema do projeto da seguinte forma:

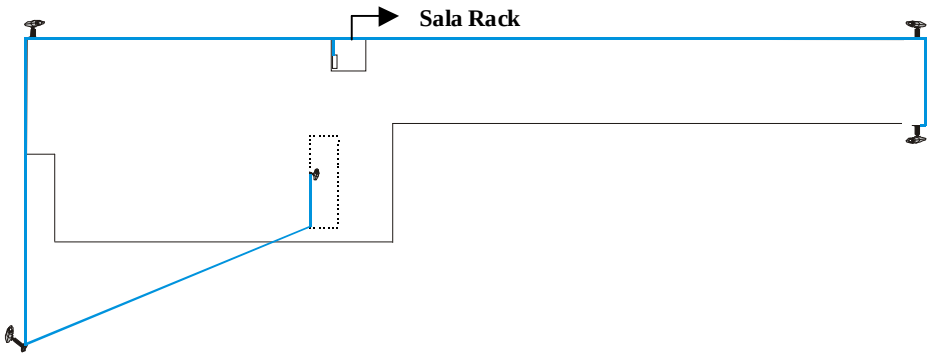

Figura 12 – Esquema de pontos das câmeras com as conexões até o Rack Central

, onde o que está descrito em azul significa a conexão entre as câmeras até o switch encontrado no rack principal do prédio.

A escolha desse tipo de cabo para esta parte do sistema ocorreu pelo motivo de se escolher a tecnologia da câmera AXIS 2110 como parte integrante do sistema.

Um novo problema surgiu depois de realizada à conexão das câmeras ao switch, o de enviar o sinal do prédio em questão até a guarita de vigia.

Para resolução desse problema foram estudadas duas formas: a de se utilizar um cabeamento por fibra óptica ou a transmissão via radio (wireless).

A escolha pela transmissão wireless (IEEE 802.11-b) ocorreu pelo fato de já existir uma rede desse tipo na Universidade e de que assim conseguiríamos uma banda exclusiva para envio desse sinal até a zona de monitoramento.

Depois de resolvido a forma de transmissão até a guarita o nosso esquema passou a se comportar da seguinte forma, como mostra a figura13:

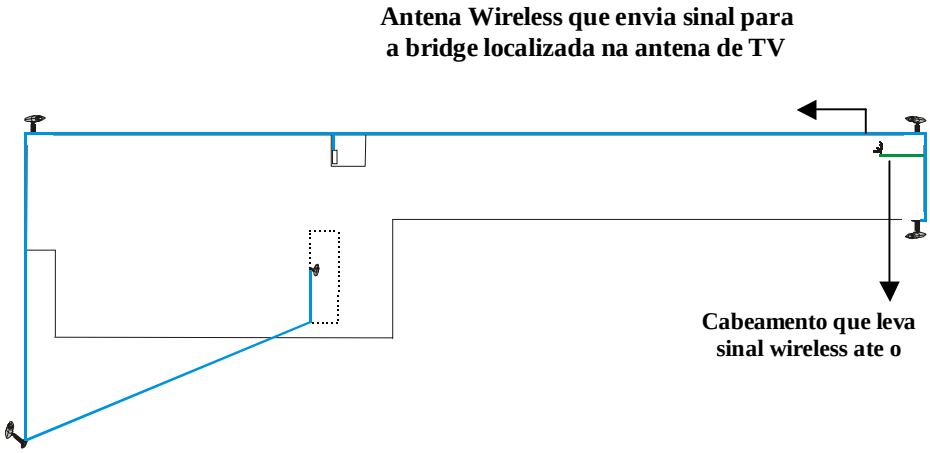

Figura 13: Esquema com adicionamento da parte wireless do sistema

A explicação para temos que enviar o sinal para a bridge da antena de TV e depois recaptura-la na guarita é devido a não visualização de uma antena a outra, já que nesse tipo de sistema é requerido algo desse tipo.

É interessante demonstrar o local de visualização dessas imagens, isto é, a guarita de vigilância. A figura14 demonstra como ficará o posicionamento da antena e seu cabeamento na guarita.

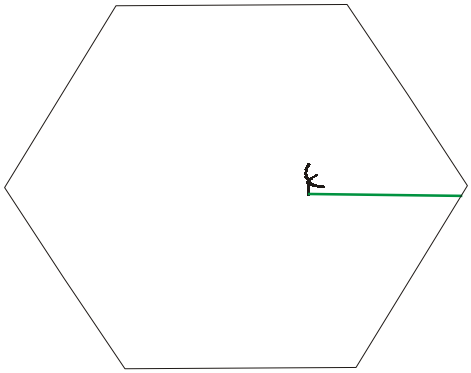

Figura 14 – esquema do recebimento do sinal pela guarita de vigilância

Para maiores detalhes sobre o projeto dos cabos e posições das câmeras segue no apêndice as plantas estruturais apresentadas anteriormente com os devidos dispositivos demonstrados.

4.5 - Visualização de funcionamento

Podemos fazer uma demonstração sobre o funcionamento do sistema através de fotos retiradas do local e de como o vigia iria receber essas informações.

Como podemos perceber pela figura 15 a Câmera 1 visualiza toda a área esquerda do prédio na parte dos fundos e uma parte do estacionamento.

Figura 15 – Visão da Câmera 1

Percebendo a figura16 vemos que a Câmera 2 observa a parte frontal do prédio do lado esquerdo com uma parte do gramado.

Figura 16 – Visão da Câmera 2

Agora olhando a figura17 verificamos que ela observa o lado direito frontal do prédio e uma outra pare do gramado.

Figura 17 – Visão da Câmera 3

A figura18 nos demonstra o lado direito do prédio na parte dos fundos e também uma parte do estacionamento.

Figura 18 – Visão da Câmera 4

E por ultimo a figura19 nos demonstra a visualização da porta de entrada do prédio.

Figura 19 – Visão da Câmera 5

Agora analisando a figura20 observamos a visualização do vigia de todas as câmeras instaladas, porem essa visualização de todas as câmeras pode ser alterada para somente uma, dependendo da preferência ou situação que o vigia encontre, passando a ser como nas figuras acima citadas.

Figura 20 – Visão do Micro da Vigilância

Um outro ponto importante a se ressaltar é que nessa visualização demonstrada não há a sensação de um filme, logo que são figuras estáticas. Na visualização original do vigia ele teria a impressão de um filme, podendo assim notificar qualquer movimento suspeito com uma melhor precisão.

4.6 – As Entrevistas

Foi realizado para constatarmos os pensamentos da Universidade perante a instalação do sistema entrevistas com a Pró-Reitora de Administração e com o Chefe da Segurança da Universidade.

As idéias das entrevistas serão demonstradas a seguir.

4.6.1- Entrevista com a Pró-Reitora de Administração (Iara)

Em uma entrevista realizada com a Pró-Reitora de Administração da Universidade Federal de Lavras foi constatado o grande interesse da Universidade em adquirir um sistema como esse.

No decorrer da entrevista a Pró Reitora demonstrou a carência que a Universidade encontra em conseguir uma vigilância eficaz para todas as suas dependências.

Ela chegou a demonstrar um exemplo ocorrido recentemente, onde o dono de uma vaca buscou seu animal no pasto sem que ninguém ficasse sabendo do ocorrido, gerando, no outro dia pelos responsáveis pelo tratamento do animal uma denuncia de roubo, o que na verdade depois foi constatado como um mal entendido.

Isso não demonstra irresponsabilidade do pessoal da segurança, mas sim uma carência nítida de recursos para que esse setor consiga suprir as necessidades da Universidade.

Para resolver essa carência ela demonstrou que só esse ano será aberto uma licitação para contratação de 30 novos vigilantes, sendo que o custo dessas novas contratações geram um déficit para a Universidade de R$1100,00 em media por vigilante mês.

Se analisarmos esses novos gastos com vigilância chegaremos a um total de R$396000,00 por ano.

Esses altos gastos foi um dos motivos que levou a Pró-Reitora a se interessar pelo sistema e pedir com que fossem feitos outros estudos sobre o custo de instalação, para que o sistema de alguma forma possa ser implantado na Universidade.

Na entrevista também foram questionadas formas de se adquirir recursos para a implantação, sendo que uma delas foi à designação da responsabilidade a cada departamento da Universidade, ocasionando assim com que cada sistema se tornasse operante com recursos próprios de cada setor, expandindo a vigilância por todo o campus.

4.6.2 – Entrevista com o chefe de segurança (Antônio da Silva Rosa)

A visão do chefe de segurança não é diferente da Pró-Reitora, ambos acham que um sistema como esse facilitaria muito a cobertura da extensão territorial da Universidade e proporcionaria uma vigilância mais eficaz das dependências, porém ele adota a política de que a implantação só deve ser executada se proteger o empregos dos funcionários de segurança.

No decorrer da entrevista foram informadas algumas dificuldades encontradas pelo setor de segurança para conseguir executar a vigilância. Dentre elas encontra-se o grande numero de entradas que o campus possui, a grande faixa territorial que se aproxima de 505 hectares, a disposição das edificações, a iluminação precária em torno dos prédios (sendo bem iluminado apenas a avenida principal), o numero baixo de efetivos (que conta hoje com o quadro de 25 membros, onde entre esses 2 estão afastados e todo mês 2 obtêm o direito de retirar férias reduzindo esse numero para 21), problemas nas divisas com proprietários de animais que violam a proteção e inserem seus animais no campus para utilizar as pastagens e etc.

Porém, a segurança não é somente esse desastre informado anteriormente, ela conta além do efetivo de 25 pessoas com a ajuda do 8º Batalhão de Policia Militar de Lavras, onde rondas e blitz são feitas com os membros da segurança da UFLA para tentar minimizar ao máximo o risco de atos ilícitos serem cometidos no interior da Universidade.

Foi citado também pelo chefe da segurança o fato de que se algum individuo conhecer bem as dependências territoriais da Universidade, saídas, fronteiras, seria muito difícil hoje conseguir capturar-lo no caso de ele cometer alguma infração contra os bancos presentes no Campus.

5 – Conclusões

A instalação de um sistema desse tipo em instituições passou nos dias atuais de um bem supérfluo de proteção para um item de suma importância. Evidencias são demonstradas através de varias instituições, como UFMG e UFJF, que hoje julgam essencial a aquisição de um projeto como esse e experimentam, em fase de aplicação, os benefícios que ele traz.

No decorrer desse estudo vimos que existem varias tecnologias presentes no mercado proporcionando sistemas de segurança com custo beneficio bastante propício.

No nosso caso chegou-se a conclusão que a instalação de tal sistema pouparia um recurso enorme para a instituição, visto que os gastos com pessoal de vigilância não precisariam ser tão altos.

Notou-se também que a instalação desse sistema não é justificável somente por fatores financeiros, mas também pelo fato que a cobertura total da Universidade se torna impossível de ser feita sem o auxilio de uma tecnologia desse tipo, ou seja, por mais vigilantes contratados nunca seria possível cobrir toda a extensão da Universidade 24horas por dia sem deixar falhas na segurança.

Um outro ponto também concluído nesse projeto é a questão de que por mais eficaz que seja o sistema, nunca será possível uma instalação que substituísse o vigilante. Ele corta gastos em números excessivos de funcionários, porém a presença desse se torna indispensável logo que rondas ainda precisam ser feitas e movimentos suspeitos devem ser verificados.

Apesar do projeto ter sido realizado baseando-se no edifício da reitoria notamos que a ampliação dele para as demais localidades seria de fácil implementação, visto que o grande entroncamento da rede já está presente nas dependências do campus.

6 – Bibliografia

[1] – site: http://www.pbh.gov.br/informacoes-estatisticas/anuario2000/anuariobh2000-segurancapublica101.htm acessado em 22 de novembro de 2002.

[2] – site: www.w2k.kit.net/Cisco/redesloacis_lans.htm acessado em 22 de novembro de 2002.

[3] – Lacerda W.S. – Rede de Computadores - Uma visão Geral Boletim técnico anoVI – Numero 14 – 1997 – Editora UFLA.

[4] - Livro: Redes de Computadores – Tanembaum Andrew S. - 1997 – Editora Campus – 5ª edição.

[5] – site: http://www.ead.unicamp.br acessado em 25 de novembro de2002.

[6] – site : http://www.brasiliano.com.br/download/artigo_696.doc acessado em 25 de novembro de 2002.

[7] – site : http://www.brasiliano.com.br/download/artigo_496.doc acessado em 25 de novembro de 2002.

RESUMO

Sistema de Vigilância Interna Através do Uso de uma Arquitetura de Redes TCP/IP

O projeto apresentado constituiu em elaborar um sistema de vigilância utilizando tecnologias de rede como: protocolos TCP/IP, cabeamentos (cabos UTP, Fibras Ópticas), transmissões wireless (IEEE 802.11b).

A idéia de elaborar tal sistema surgiu do crescente índice de violência que observamos nos dias atuais e da opção de se poupar recursos para vigilância, uma vez que esta poderá ser feita remotamente.

Pouparíam-se recursos do tipo de rondas em veículos por volta do edifício, uma vez que estas poderiam ser executadas com menos freqüência e também no caso de averiguar-se uma forma suspeita no local.

O Sistema

O sistema se baseia em um conjunto de câmeras capazes de se conectar a uma rede LAN ou até mesmo a INTERNET enviando dados captados ate uma central de vigilância ou ate mesmo a um micro conectado a INTERNET.

Esse sistema é feito da seguinte forma:

- Primeiramente foi feito um estudo de câmeras que podem ser utilizadas nesse determinado tipo de ambiente, ou seja, estudou-se vários tipos de câmeras ate chegarmos à tecnologia que melhor se enquadra nas nossas necessidades.
- Foi elaborado, logo após o estudo das câmeras, pontos críticos (pontos onde deveram ser instaladas as câmeras de vigilância). Esses pontos foram escolhidos de forma a cobrir toda a estrutura do edifício de modo que não sobre nenhuma área de sombra (área onde a câmera não pode detectar o que esta ocorrendo).
- Depois de feito o estudo dos pontos, elabora-se então como essas câmeras iriam se conectar a rede, ou seja, escolheu-se a melhor forma de transmissão de dados, podendo esses ser via cabos ou via wireless.
- Escolhidos os meios de transmissão foi feito um levantamento dos matérias necessários para instalação do sistema.
- Logo após viria a implantação do sistema e o treinamento dos usuários para podemos otimizar seu funcionamento.

O nosso sistema foi desenvolvido baseando-se no prédio de reitoria da Universidade Federal de Lavras (UFLA).

Esse sistema esta constituído da seguinte forma:

Após estudos de varias tecnologias de câmeras apresentadas no mercado foi escolhido a AXIS 2110, cujo, o custo beneficio dessa câmera é o melhor para implantação nesse tipo de projeto.

Os pontos críticos do prédio foram escolhidos de forma a cobrir toda a sua extensão, conseguido assim cobrir todas as áreas de risco de possíveis invasões e os meios de transmissões escolhidos foram via cabos e wireless.

Sistema de Vigilância Interna Através do Uso de uma Arquitetura de Redes TCP/IP

Thiago Silvestre Amâncio
Anderson Bernardo dos Santos
Rêmulo Maia Alves

UFLA – Universidade Federal de Lavras
DCC – Departamento de Ciência da Computação
manso@comp.ufla.br
anderson@ufla.br
remulo@comp.ufla.br

Resumo: Tendo em vista que nos dias atuais a preocupação das instituições com respeito à proteção das suas informações e sues bens tem aumentado bastante, buscou-se formular através desse trabalho um sistema eficiente que atingisse todas as expectativas de segurança exigidas.
Palavras Chaves: Segurança, Câmera de Vídeo, Rede.

1 Introdução

Uma das questões mais discutidas hoje é a respeito de segurança, não somente a segurança do individuo como também a de patrimônios e informações.

Segurança hoje passou de ser uma coisa supérflua e se tornou uma preocupação extremamente importante para qualquer instituição.

Com um crescimento cada vez mais ascendente da violência urbana nas ultimas décadas as empresas buscam dispositivos e saídas que garantam a segurança de seu pessoal e de seu patrimônio.

Mas como isso poderia ser feito?

Uma solução seria colocar uma pessoa monitorando as dependências de uma instituição dia e noite de modo que a identificação de algo estranho seria feita a qualquer momento.

Porém, em uma instituição de instalações muito grandes seria improvável que um individuo pudesse cobrir toda área garantindo que nenhuma atividade estranha ocorresse enquanto outra área estivesse sendo monitorada.

Para solucionar problemas como esse é que tentamos cada vez mais apoiarmos a uma tecnologia.

Uma forma de garantir segurança e minimizar um gasto

seria a elaboração de um sistema de que monitorasse essas áreas.

De forma que esse sistema deve se mostrar robusto e capaz de retornar um nível aceitável de informações que poderiam auxiliar no trabalho de vigilância de uma área.

Tal sistema poderia contar com o auxilio de câmeras de vídeo que captasse sinais de varias áreas e distribuísse os dados a uma central onde um vigilante ficaria monitorando.

Com base na necessidade de um sistema como esse é que este trabalho tentará formula-lo baseado em câmeras de vídeo que farão a transmissão de seus dados através de uma LAN (local área network) até o centro de controle dessas informações.

Com o termino do trabalho espera-se como objetivo criar um mecanismo capaz de auxiliar na vigilância de instituições visando cada vez mais protege-la de intrusos.

2 – Protocolo e forma de Transmissão

Primeiramente, os métodos de transmissão e os protocolos utilizados deveram ser analisados, considerando os aspectos tecnológicos e financeiros.

Para começar podemos escolher a transmissão dos dados utilizando o protocolo TCP/IP. Sua escolha ocorre pela tamanha dimensão que este protocolo tomou nos dias atuais e, por ser bastante difundido conseguimos distribuir os sinais capturados pelas câmeras a uma maior porcentagem de estações de visualização sem ocorrências de incompatibilidade e conflitos.

Com relação à transmissão física desse sinal fica mais fácil, por já existir uma infra-estrutura, utilizando transmissões via cabo e wireless (IEEE 802.11-b).

Quando falamos dessa estrutura queremos dizer a rede UFLA que já existe no campus, contendo em seu backbone uma grande extensão de fibras ópticas e cabos UTP categoria5, além de seus elementos ativos como conversores ópticos, switches, servidores, etc. Além disso, ela conta também com uma estrutura já montada de wireless (IEEE 802.11-b).

Um ponto observado para a execução da instalação foi a forma de conectar as câmeras de vídeo até o rack que conteria o switch gerenciador dessa rede, onde a melhor solução encontrada foi fazer um cabeamento utilizando fiações de cobre (cabos UTP categoria5 rígidos ou cabos coaxiais).

Um outro ponto crucial, falando em transmissão desses dados, seria a forma de enviar essas informações até a guarita de controle (guarita de vigia).

Por ser uma longa distância dos pontos de captura até a guarita e ela se apresentar em um local de difícil acesso a cabos de cobre (cabos UTP categoria5) ou de fibras ópticas, trabalhou-se então com a

idéia de se formar essa parte da rede utilizando transmissão wireless.

Como a Universidade já possui este tipo de sistema foi então estudado uma forma de adaptamos a ele o envio de nossos dados.

Feito esse estudo chegamos à tecnologia wireless de transmissão de dados conhecida como IEEE 802.11-b, onde com dois kits conseguimos enviar esses dados até a guarita e assim criarmos uma WLAN (Wireless Local Área Network) nessa parte da rede.

3 – As Câmeras

A escolha por qual tipo de câmera seria utilizada ocorreu pela analise de duas tecnologias: a tecnologia onde o sinal era digitalizado por meio de um micro computador e depois enviado pela rede e a tecnologia onde a própria câmera de vídeo proporcionasse esta digitalização e a transmissão dos dados.

Varias comparações entre essas tecnologias foram executadas e algumas delas são:

- A primeira tecnologia apresenta a necessidade de um microcomputador para digitalização das imagens, já a segunda não necessita disso, logo que contem um processador embutido em seu interior que possibilita assim a digitalização ser feita pela própria câmera.
- Existe uma facilidade de visualização dessas imagens na segunda tecnologia que não necessita de softwares adicionais para serem vistas as imagens disponíveis na rede, porém a primeira necessita de um software especial para digitalização e visualização.
- Observamos também que a preparação das lentes e dos chips de captura de AXIS 2110 (câmera da segunda tecnologia) proporciona uma visualização melhor das imagens em situações de pouca luz, (ela consegue capturar sinal com apenas 1lux de luminosidade), já a primeira tecnologia citada dependera qualidade das câmeras adquiridas.
- Porém, a primeira tecnologia citada proporciona uma melhor velocidade de frames por segundo (FPS) podendo chegar até a 60 frames por segundo dependendo dos componentes utilizados, já a AXIS 2110 apresenta-nos somente até 15 frames por segundo.
- Um outro ponto importante a ser analisado é a compactação dessas imagens para serem distribuídas pela rede, onde a AXIS 2110 consegue uma compactação em quatro níveis diferentes podendo assim não carregar a rede em momentos que não sejam necessários, ou seja, podemos configurar a câmera para um nível de compactação mais alto quando a necessidade de vigilância não for tão preocupante.

As demais funções das tecnologias são parecidas, mudando

somente o meio de como são implementados.

Após essas observações chegamos a conclusão que a tecnologia da AXIS 2110 é a melhor para finalizarmos a construção do sistema de vigilância.

4 - Identificação dos Pontos Críticos e do Local da Guarita de Vigilância

A escolha desses pontos foi baseada no prédio da reitoria da Universidade Federal de Lavras (UFLA) de forma a cobrir todo o território do edifício, ou seja, precisaríamos escolher pontos que cobrissem todas as entradas, mesmo como as dependências ao seu redor.

Assim foram escolhidos os pontos da seguinte forma:

- O primeiro ponto foi no canto superior esquerdo no fundo do prédio, onde, a câmera captará o lado esquerdo do prédio até a entrada principal e parte do estacionamento.
- O segundo ponto foi no canto superior esquerdo, porém na frente do prédio, onde irá capturar as imagens da parte frontal até seu ponto médio e parte de seu gramado.
- O terceiro ponto foi no canto superior direito do prédio na parte frontal, visto que a área de visualização desse ponto limita-se a capturar imagens desse lado direito até o ponto médio e parte de seu gramado.
- O quarto ponto foi o canto direito do prédio na parte dos fundos, porém esse ponto não poderá ficar no próprio edifício tendo que se localizar afastado, para conseguir assim cobrir todas as entradas; e sua área de visualização se restringira ao lado direito observando a entrada especial para o reitor e a entrada do DRCA.
- O quinto ponto se localizara na entrada principal do prédio para conseguirmos assim vigiar toda a movimentação nesse importante ponto de acesso.

5 – O Projeto

A instalação dessas câmeras no prédio da Reitoria da Universidade Federal de Lavras ocorreu da seguinte forma:

Primeiramente foram escolhidos os pontos onde as câmeras seriam instaladas.

Feito isso uma pesquisa foi realizada para escolher a forma de como essa câmera se conectaria com o swich gerenciador, sendo que o cabo UTP categoria 5 foi escolhido para a instalação logo que a câmera foi a AXIS 2110 foi optada para fazer parte integrante do sistema.

Após a escolha do cabeamento de transmissão das câmeras até o swich, preocupou-se então com o envio desses dados até a guarita de vigia, levando a implantação utilizando a tecnologia wireless (IEEE 802.11-b).

6 – As Entrevistas

Foi realizado para constatarmos os pensamentos da Universidade perante a instalação do sistema entrevistas com a Pró-Reitora de Administração e com o Chefe da Segurança da Universidade.

As idéias das entrevistas serão demonstradas a seguir.

6.1 - Entrevista com a Pró-Reitora de Administração (Iara)

Em uma entrevista realizada com a Pró-Reitora de Administração da Universidade Federal de Lavras foi constatado o grande interesse da Universidade em adquirir um sistema como esse.

No decorrer da entrevista a Pró Reitora demonstrou a carência que a Universidade encontra em conseguir uma vigilância eficaz para todas as suas dependências.

Ela chegou a demonstrar um exemplo ocorrido recentemente onde o dono de uma vaca buscou seu animal no pasto sem que ninguém ficasse sabendo do ocorrido, gerando, no outro dia ao chegar os responsáveis pelo tratamento do animal, uma denuncia de roubo, o que na verdade depois foi constatado como um mal entendido.

Esse ocorrido não demonstra irresponsabilidade do pessoal da segurança, mas sim uma carência nítida de recursos para esse setor conseguir suprir as necessidades da Universidade.

Para resolver essa carência ela demonstrou que só esse ano será aberto uma licitação para contratação de 30 novos vigilantes, sendo que o custo dessas novas contratações gera um déficit para a Universidade de R$1100,00 em media por vigilante mês.

Se analisarmos esses novos gastos com vigilância chegaremos a um total de R$396000,00 por ano.

Esses altos gastos foi um dos motivos que levou a Pró-Reitora a se interessar pelo sistema e pedir com que fossem feitos outros estudos sobre o custo de instalação, para que o sistema de alguma forma possa ser implantado na Universidade.

Na entrevista também foram questionadas formas de se adquirir recursos para a implantação, sendo que uma delas foi à designação da responsabilidade a cada departamento da Universidade, ocasionando assim com que cada sistema se tornasse operante com recursos próprios de cada setor, expandindo a vigilância por todo o campus.

6.2 – Entrevista com o chefe de segurança (Antônio da Silva Rosa)

A visão do chefe de segurança não é diferente da Pró-Reitora, ambos acham que um sistema como esse facilitaria muito a cobertura pela extensão territorial

da Universidade e proporcionaria uma vigilância mais eficaz das dependências, porem ele adota a política de que a implantação deve ser executada somente se proteger o empregos dos funcionários de segurança.

No decorrer da entrevista ele informou também algumas dificuldades encontradas pelo setor de segurança para conseguir cobrir a Universidade inteira, dentre elas encontra-se o grande numero de entradas que o campus possui, a grande faixa territorial que se aproxima de 505 hectares, a disposição das edificações, a iluminação precária em torno dos prédios (sendo bem iluminado apenas a avenida principal), o numero baixo de efetivos (que conta hoje com o quadro de 25 membros, onde entre esses 2 estão afastados e todo mês 2 obtêm o direito de retirar férias reduzindo esse numero para 21), problemas nas divisas com proprietários de animais que violam a proteção e inserem seus animais no campus para utilizar as pastagens e etc.

Porém, a segurança não é somente esse desastre informado anteriormente, ela conta alem do efetivo de 25 pessoas com a ajuda do 8º Batalhão de Policia Militar de Lavras, onde rondas e blitz são feitas com os membros da segurança da UFLA para tentar minimizar ao máximo o risco de atos ilícitos serem cometidos no interior da faculdade.

Foi questionado também segurança que se algum individuo conhecer bem as dependências territoriais da Universidade, saídas, fronteiras, seria muito difícil, hoje, conseguir capturar alguém que cometesse alguma infração contra os bancos presentes no Campus.

5 – Conclusões

A instalação de um sistema desse tipo em instituições passou nos dias atuais de um bem superfulo de proteção para um item de suma importância. Evidencias são demonstradas através de varias instituições, como UFMG e UFJF, que hoje julgam essencial a aquisição de um projeto como esse e experimentam, em fase de aplicação, os benefícios que ele traz.

No decorrer desse estudo vimos que existem varias tecnologias presentes no mercado proporcionando sistemas de segurança com custo beneficio bastante propício.

No nosso caso chegou-se a conclusão que a instalação de tal sistema pouparia um recurso enorme para a instituição, visto que os gastos com pessoal de vigilância não precisariam ser tão altos.

Notou-se também que a instalação desse sistema não é justificável somente por fatores financeiros, mas também pelo fato que a cobertura total da Universidade se torna impossível de ser feita sem o auxilio de uma

tecnologia desse tipo, ou seja, por mais vigilantes contratados nunca seria possível cobrir toda a extensão da Universidade 24horas por dia sem deixar falhas na segurança.

Um outro ponto também concluído nesse projeto é a questão de que por mais eficaz que seja o sistema, nunca será possível uma instalação que substituísse o vigilante. Ele corta gastos em números excessivos de funcionários, porém a presença desse se torna indispensável logo que rondas ainda precisam ser feitas e movimentos suspeitos devem ser verificados.

Apesar do projeto ter sido realizado baseando-se no edifício da reitoria notamos que a ampliação dele para as demais localidades seria de fácil implementação, visto que o grande entroncamento da rede já esta presente nas dependências do campus.

6 – Bibliografia

[1] – site: http://www.pbh.gov.br/informacoes-estatisticas/anuario2000/anuariobh2000-segurancapublica101.htm acessado em 22 de novembro de 2002.

[2] - site: www.w2k.kit.net/Cisco/redesloacis_lans.htm acessado em 22 de novembro de 2002.

[3] - Lacerda W.S. – Rede de Computadores - Uma visão Geral Boletim técnico anoVI – Numero 14 – 1997 – Editora UFLA.

[4] - Livro: Redes de Computadores – Tanembaum Andrew S. - 1997 – Editora Campus – 5ª edição.

[5]–site: http://www.ead.unicamp.br acessado em 25 de novembro de2002.

[6]–site: http://www.brasiliano.com.br/download/artigo_696.doc acessado em 25 de novembro de 2002.

[7]–site: http://www.brasiliano.com.br/download/artigo_496.doc acessado em 25 de novembro de 2002.