

FACULDADE DE TECNOLOGIA “PROF. WALDOMIRO MAY”

OUTRAS APOSTILAS EM:
www.projetoderedes.com.br

**APLICAÇÃO DE REDES DE COMPUTADORES PARA
MONITORAMENTO DE VÍDEO EM LOGRADOUROS
PÚBLICOS DA CIDADE DE ITANHANDU/MG**

CASSIANO RICARDO BRAGA

CRUZEIRO/SP

2009

FACULDADE DE TECNOLOGIA “PROF. WALDOMIRO MAY”

**APLICAÇÃO DE REDES DE COMPUTADORES PARA
MONITORAMENTO DE VÍDEO EM LOGRADOUROS
PÚBLICOS DA CIDADE DE ITANHANDU/MG**

CASSIANO RICARDO BRAGA

Trabalho de Conclusão de Curso a ser apresentado à Faculdade de Tecnologia Prof. Waldomiro May como parte dos requisitos para a obtenção do Certificado de Conclusão de Curso da Graduação em Tecnologia em Informática com ênfase em redes de computadores.

Área de Concentração: Tecnologia em Informática

Ênfase: Redes de Computadores

Linha de Estudo: CFTV e Redes Wireless

Orientador: Prof. Esp. Luiz Carlos Rosa Junior

CRUZEIRO/SP

2009

FACULDADE DE TECNOLOGIA PROF. WALDOMIRO MAY

FATEC CRUZEIRO – SP

BRAGA, Cassiano Ricardo.

Aplicação de redes de computadores para monitoramento de vídeo em logradouros públicos da cidade de Itanhandu/MG - 2009.

64 f.

Monografia (TCC)

Orientação: Prof. Esp. Luiz Carlos Rosa Junior.

(1) Redes Wireless, (2) CFTV Digital, (3) Câmera IP.

CASSIANO RICARDO BRAGA

APLICAÇÃO DE REDES DE COMPUTADORES PARA MONITORAMENTO
DE VÍDEO EM LOGRADOUROS PÚBLICOS
DA CIDADE DE ITANHANDU/MG

Monografia apresentada à Faculdade de Tecnologia Prof. Waldomiro May para conclusão da graduação no Curso Superior de Tecnologia em Informática, com ênfase em Redes de Computadores.

Área: Tecnologia em Informática

Ênfase: Redes de Computadores

Linha de Estudo: Circuito Fechado de TV e Redes Wireless.

Orientador: Prof. Esp. Luiz Carlos Rosa Junior

1º Examinador: Prof. Esp. Renan França Nogueira
Instituição: Faculdade de Tecnologia Prof. Waldomiro May

2º Examinador: MSc Carlos Henrique Loureiro Feichas
Instituição: Faculdade de Tecnologia Prof. Waldomiro May

Aprovado em: ___/___/2009.

NOTA: _____

CRUZEIRO

2009

*À minha esposa Cristiane
E aos meus filhos Ricardo e Isabela,
Por serem luz e fortaleza em minha vida.*

Agradecimentos

À Professora Ana Lúcia, pelo comprometimento e entusiasmo incondicionais que me revigoraram e impulsionaram durante a realização do trabalho.

Aos Professores Luiz Carlos e Renan Nogueira, por terem acreditado em meu trabalho e dado todo o suporte necessário para concluí-lo.

À Faculdade de Tecnologia Prof. Waldomiro May, por me proporcionar a oportunidade de realizar um trabalho voltado para a comunidade.

À Polícia Militar do Estado de Minas Gerais, orgulho do povo mineiro, pelo apoio e dedicação durante todo o desenvolvimento do trabalho.

RESUMO

A vigilância eletrônica de locais públicos se tornou uma importante ferramenta de identificação e enfrentamento dos problemas urbanos, tais como a criminalidade e o trânsito caótico. Esses problemas também atingem as médias e pequenas cidades, exigindo o desenvolvimento de soluções adequadas às suas peculiaridades. Este trabalho descreve a aplicação da tecnologia de redes de computadores para a transmissão das imagens geradas por dispositivos de vigilância eletrônica instalados em logradouros públicos da cidade de Itanhandu/MG. Todas essas imagens serão armazenadas, visualizadas e analisadas por um sistema de circuito fechado de TV (CFTV). O projeto parte do estabelecimento dos equipamentos que compõem o CFTV e segue com as redes para a interconexão entre as estações de coleta de imagens e os componentes da estação central de monitoramento, envolvendo tecnologia de transmissão sem fio e redes locais.

ABSTRACT

Electronic surveillance of public places has become an important tool for identifying and coping with urban problems such as crime and chaotic traffic. These problems also affect midsize and small cities, demanding development of case-specific solutions. This paper describes the application of technology of computer networks to transmission of images generated by electronic surveillance devices installed in public places of Itanhandu/MG city. All these images will be stored, viewed and analyzed by a system of closed TV circuit (CCTV). The project was developed over an equipment list and consists of a network of image-capturing devices and central monitoring station, involving both LAN and Wireless technologies.

LISTA DE FIGURAS

Figura 01 – Mapa da Malha Viária de acesso ao Município de Itanhandu/MG	17
Figura 02 – Esquema Básico – CFTV Digital	20
Figura 03 – Câmera IP PTZ Speed Dome.....	20
Figura 04 – Comparativo entre as tecnologias wireless disponíveis.....	27
Figura 05 – Esquema geral do projeto	30
Figura 06 – Mapa da área urbana e distribuição das estações	32
Figura 07 – Diagrama de fluxo de dados do CFTV.....	33
Figura 08 – Sistema de Visualização “Display Wall”.....	38
Figura 09 – Estação de coleta de imagens	41
Figura 10 – Esquema geral da rede de computadores.....	46
Figura 11 – Infra estrutura da rede wireless	47
Figura 12 – Esquema do conjunto: Câmera / Access Point / Antena	47
Figura 13 – Segmentação lógica da rede através de VLANs	49

LISTA DE TABELAS

Tabela 01 – Comparativo entre os padrões IEEE 802.11 disponíveis.....	28
Tabela 02 – Cálculo da distância entre antenas	29
Tabela 03 – Distribuição das Estações de CFTV.....	31
Tabela 04 – Configuração básica das interfaces do roteador	49
Tabela 05 – Configuração básica das interfaces do switch.....	50

SUMÁRIO

INTRODUÇÃO

1. O MONITORAMENTO DE VÍDEO E AS TECNOLOGIAS APLICADAS	13
1.1 SEGURANÇA PÚBLICA	13
1.2 MONITORAMENTO DE VÍDEO APLICADO À SEGURANÇA PÚBLICA.....	13
1.2.1 O FUNCIONAMENTO BÁSICO.....	13
1.2.2 EXPERIÊNCIAS BEM SUCEDIDAS E RESULTADOS ALCANÇADOS	14
1.3 O MUNICÍPIO DE ITANHANDU	16
1.3.1 LOCALIZAÇÃO GEOGRÁFICA E DEMOGRAFIA.....	16
1.3.2 PERFIL SÓCIO-ECONÔMICO.....	17
1.3.3 PERFIL DA SEGURANÇA PÚBLICA.....	17
1.3.4 PONTOS SENSÍVEIS E VULNERÁVEIS.....	17
1.3.5 ASPECTOS TÉCNICOS A SEREM CONSIDERADOS	18
1.4 O CIRCUITO FECHADO DE TV	18
1.4.1 FUNCIONAMENTO BÁSICO.....	18
1.4.2 PRINCIPAIS COMPONENTES DO SISTEMA DE CFTV	18
1.4.3 O MODELO DIGITAL	19
1.4.4 AS CÂMERAS IP	20
1.5 AS REDES DE COMPUTADORES	22
1.5.1 HISTÓRICO	22
1.5.2 O ENDEREÇAMENTO IP	22
1.5.3 A INTERNET.....	24
1.5.4 O MODELO TCP/IP	25
1.5.5 AS REDES SEM FIO (WIRELESS NETWORK)	26
2. DESENVOLVIMENTO DO PROJETO	30
2.1 DESCRIÇÃO GERAL DO PROJETO	30
2.1.1 LOCAIS DE INSTALAÇÃO DAS ESTAÇÕES.....	31
2.1.2 MAPA DA ÁREA URBANA – DISTRIBUIÇÃO DAS ESTAÇÕES.....	32
2.2 PROJETO DO CIRCUITO FECHADO DE TV.....	32
2.2.1 A ESTAÇÃO CENTRAL	32
2.2.2 ESTAÇÕES DE TRABALHO.....	33
2.2.3 SERVIDORES DE CFTV.....	34
2.2.4 GRAVADORES DE VÍDEO EM REDE.....	35
2.2.5 SOFTWARE DE ANÁLISE, GERÊNCIA E SUPERVISÃO	36
2.2.6 TECLADO DE COMANDO	38
2.2.7 SISTEMA DE VISUALIZAÇÃO DISPLAY WALL	38

2.2.8 ESTAÇÕES DE COLETA DE IMAGENS.....	41
2.2.9 CAMERAS IP.....	41
2.2.10 ARMÁRIOS PARA ABRIGO DOS EQUIPAMENTOS	42
2.2.11 PROTETOR DE SURTO.....	43
2.2.12 NO-BREAK DE CAMPO.....	43
2.2.13 POSTE METÁLICO	44
2.2.14 SISTEMA DE ÁUDIO.....	45
2.3 PROJETO DA REDE DE COMPUTADORES.....	45
2.3.1 DESCRIÇÃO GERAL	45
2.3.2 CÁLCULO DA LARGURA DE BANDA E ESPAÇO EM DISCO.....	46
2.3.3 INFRAESTRUTURA DA REDE WIRELESS.....	46
2.3.4 MÓDULO DE CONECTIVIDADE DAS ESTAÇÕES DE COLETA.....	47
2.3.5 ENDERÇAMENTO IP	48
2.3.6 CÁLCULO DAS SUBREDES	48
2.3.7 CONFIGURAÇÃO DOS EQUIPAMENTOS	49
2.3.8 ASPECTOS DE SEGURANÇA.....	50
2.3.9 ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS DA REDE.....	50
CONSIDERAÇÕES FINAIS E PROJETOS FUTUROS	55
BIBLIOGRAFIA	
GLOSSÁRIO	
APÊNDICE. LISTA DE EQUIPAMENTOS	

INTRODUÇÃO

A constante evolução e migração da criminalidade e outros fatores nocivos à ordem pública presentes nas áreas urbanas fez com que os encarregados da manutenção da Segurança Pública evoluíssem na busca de novas ferramentas de controle e monitoramento. Nesse contexto, se passou a utilizar sistemas de monitoramento de vídeo aplicados à Segurança Pública nos Municípios, ferramentas que vêm sendo aplicadas em diversos centros urbanos, obtendo-se resultados significativos. Proporcionalmente, os problemas dos grandes centros urbanos também atingem as médias e pequenas cidades, fazendo com que sejam concebidas soluções que atendam às suas necessidades.

A cidade de Itanhandu/MG é exemplo de uma cidade do interior que sofre com a criminalidade advinda de outras localidades, principalmente devido à sua localização próxima à zona de convergência do eixo Rio - São Paulo - Minas Gerais, além de seu perfil turístico. Surge então a necessidade de se identificar e coibir as ações nocivas à ordem pública com estratégias especificamente voltadas para esse tipo de criminalidade, sendo o monitoramento de vídeo em logradouros públicos importante ferramenta de apoio.

O Sistema de Circuito Fechado de TV (CFTV) funciona basicamente através de uma estação central que recebe as imagens coletadas pelas câmeras instaladas nos logradouros públicos e as distribui para uma estação central de monitoramento operada por agentes de Segurança Pública. Neste local as imagens são exibidas em tempo real, analisadas e armazenadas.

Para a interconexão dos equipamentos do CFTV será aplicada a tecnologia de redes de computadores e a utilização de Câmeras IP, que proporcionam um alto nível de inteligência no gerenciamento dos dispositivos de coleta de imagens, o projeto utiliza as mais recentes tecnologias e padrões para transmissão de dados através de redes sem fio.

1. O MONITORAMENTO DE VÍDEO E AS TECNOLOGIAS APLICADAS

1.1 SEGURANÇA PÚBLICA

Dispõe a Constituição da República Federativa do Brasil que a Segurança Pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através da Polícia Federal, Polícia Rodoviária Federal, Polícia Ferroviária Federal, Polícias Civis, Polícias Militares e Corpos de Bombeiros Militares.

A Segurança Pública é a garantia que o Estado – União, Unidades Federativas e Municípios proporcionam à Nação, a fim de assegurar a Ordem Pública contra violações de toda a espécie. Diferentemente da segurança privada, que está voltada para patrimônio e pessoas determinadas, a Segurança Pública assiste a todos os cidadãos e seus bens. A Ordem Pública é o conjunto de regras formais, coativas, que emanam do ordenamento jurídico da Nação, tendo por escopo regular as relações sociais em todos os níveis e estabelecer um clima de convivência harmoniosa e pacífica, constituindo, assim, uma situação ou condição que conduz ao bem comum.

A Manutenção da Ordem Pública é o exercício do poder de polícia, no campo da Segurança Pública, manifestado por atuações predominantemente ostensivas, visando coibir e/ou prevenir eventos que alterem a Ordem Pública e a dissuadir e/ou reprimir os eventos que violem essa Ordem para garantir sua normalidade (PMMG, 2002, p.15).

1.2 MONITORAMENTO DE VÍDEO APLICADO À SEGURANÇA PÚBLICA

1.2.1 FUNCIONAMENTO BÁSICO

O Sistema de Monitoramento de Vídeo aplicado à Segurança Pública em Municípios caracteriza-se pela utilização de câmeras de vídeo com ângulo de rotação horizontal de 360º e vertical de 180º, com estrutura de transmissão baseada em fibras ópticas, linha telefônica ou redes Wi-fi, quando em sua forma digital, para monitoramento de logradouros públicos à distância. É projetado para operar em regime de uso contínuo, 24 horas por dia e 365 dias por ano.

O sistema de vídeo é baseado em um Circuito Fechado de Televisão – CFTV, que compõe uma rede de comunicações e informações, com uma Central de Operações, monitorado por

agentes de Segurança Pública, que captura e gerencia as imagens, e compartilha os sinais das diversas câmeras localizadas em locais diversos direcionando-os para estações de supervisão predeterminadas. O local de instalação câmeras é definido através de um plano estratégico de segurança pública, priorizando o monitoramento dos locais de maior incidência de crimes das áreas urbanas, com grande fluxo de pessoas e bens, áreas comerciais e bancárias, lugares públicos de lazer.

Para Ferreira (2008), uma gestão proativa de prevenção e repressão aos delitos e concomitante diminuição da sensação de insegurança da população inclui o Sistema de Monitoramento de Vídeo aplicado à Segurança Pública em Municípios que tem por finalidade a inibição de atos nocivos à sociedade, o flagrante em tempo real e a identificação dos infratores. A tecnologia das câmeras possibilita a configuração de rotinas preestabelecidas e operações manuais em tempo real. As Câmeras ficam protegidas por invólucros especificamente projetados e instaladas nos pontos predefinidos, utilizando colunas metálicas, postes ou marquises das edificações como suporte. O Sistema de Monitoramento de Vídeo aplicado à Segurança Pública em Municípios utilizará um Circuito Fechado de Televisão – CFTV. O acesso ao seu conteúdo é restrito, reservando o direito à preservação da imagem prevista em lei.

Ferreira define os componentes do sistema da seguinte forma:

- Estação Central – A estação central do sistema abriga um PC como servidor das câmeras em rede.
- Estação de Coleta – Abriga uma ou mais câmeras. O servidor identifica os endereços IP atribuídos a cada uma das câmeras, controlando-as, proporcionando a obtenção, gravação e geração de imagens por câmera.
- Estação do Monitoramento – Local onde s agentes de monitoramento, devidamente autenticados, acessam as imagens das câmeras através de um navegador de internet, que os direcionará para ao servidor de câmeras. Os agentes de monitoramento podem acessar, reproduzir e coletar imagens gravadas através do servidor de câmeras (FERREIRA, 2008, p.10).

1.2.2 EXPERIÊNCIAS BEM SUCEDIDAS E RESULTADOS ALCANÇADOS

Os sistemas de circuito fechado de televisão já são amplamente utilizados em edifícios, empresas, condomínios e shopping centers. Mas há algum tempo as câmeras de televisão já estão sendo também adotadas nas cidades como o Rio de Janeiro e, desde o ano

passado, em cidades da Região Metropolitana de Campinas, como Valinhos, Vinhedo e Campinas (PAOLI, 2007, p.03) .

O sistema de circuito fechado de televisão está presente desde a década de 80 nas cidades da Inglaterra. Hoje em dia o país tem instaladas mais de 1,3 milhão de câmeras. A instalação dos circuitos de câmeras de televisão (CCTV) tem sido vista como uma boa solução para problemas urbanos, tornando-se parte essencial de muitos projetos de revitalização de centros urbanos ingleses. A dramática redução dos índices de criminalidade nas cidades e a grande ajuda que essas imagens deram na captura de criminosos demonstram a eficiência desse sistema no combate a violência, tanto nas cidades inglesas quanto no Brasil, por exemplo nas cidades da região metropolitana de Campinas, conforme mostrado adiante. A vigilância é importante na medida que, aumentando a visibilidade e o risco de ser visto, desencoraja o possível criminoso em sua prática delituosa. E como o ato criminoso só será realmente desencorajado se o sistema de câmeras de televisão trazer consigo a certeza da intervenção da polícia, o tempo de resposta no caso de uma situação de perigo ser identificada também é muito importante para o seu sucesso. Os sistemas de CCTV devem ser avaliados quanto ao seu poder de inibir crimes, de prisão de criminosos e aumento da percepção de segurança da comunidade. As câmeras aumentam a capacidade de vigilância agindo como:

- um apoio mais eficiente no patrulhamento dos centros urbanos, dependendo do lugar onde estiverem instaladas;
- ajuda na identificação e prisão de suspeitos;
- desencorajador de atos criminosos;
- auxílio no monitoramento do comportamento da própria polícia.

No Brasil o sistema de circuito fechado de televisão já é amplamente utilizado em propriedades privadas, tornando-se às vezes pré-requisito, juntamente com um amplo sistema de segurança, na escolha da compra de um imóvel. Estabelecimentos comerciais, escolas e academias já instalaram seus sistemas de circuito fechado de televisão para garantir maior segurança ao estabelecimento, funcionários e clientes.

Mas as câmeras, os "espões urbanos", estão começando a se espalhar também para os espaços públicos das cidades. Em 2003, um projeto de monitoramento por câmeras foi iniciado em Copacabana no Rio de Janeiro, com aparelhos espalhados pelo bairro. O sistema está ligado a um moderno programa de identificação de placas de carros e futuramente poderá dar todos os dados de uma pessoa quando esta estiver sendo filmada. Inicialmente o projeto já conseguiu inibir a criminalidade e aumentar a sensação de segurança das pessoas que moram e freqüentam Copacabana. Esse projeto estendeu-se

também para a Ilha do Governador em 2004. Na Região Metropolitana de Campinas, RMC, algumas cidades já adotaram a medida desde 2003. Valinhos e Vinhedo conseguiram conter dramaticamente o crescimento da violência e reduzir os índices de criminalidade.

Em Valinhos foram instaladas câmeras em 40 locais, nas entradas e saídas da cidade e na região central onde ficam concentrados o comércio, as agências bancárias, a rodoviária e parte das praças públicas. A média de roubos na cidade caiu pela metade depois da instalação do novo sistema de vigilância. Mas o secretário de segurança de Valinhos também notou uma mudança no comportamento dos infratores, o volume de furtos em locais onde não existe o sistema de monitoramento aumentou. A intenção é de ampliar o número de câmeras para 120, para inibir as ocorrências também nos bairros. O monitoramento é feito 24 horas pela Guarda Municipal, com o apoio da Polícia Militar e Civil. A liberação das imagens só acontece com a autorização do secretário, após requisição policial e judiciária.

Vinhedo foi a primeira a iniciar o combate a violência com o auxílio das câmeras em 2000. Durante os primeiros quatro anos, a ferramenta resultou em índices praticamente nulos de violência e criminalidade. O município tem o menor número de homicídios e ocorrências anuais do Estado de São Paulo e um dos menores do país. Aos poucos, as primeiras câmeras de Vinhedo estão sendo substituídas por aparelhos mais modernos.

1.3 O MUNICÍPIO DE ITANHANDU/MG

1.3.1 LOCALIZAÇÃO GEOGRÁFICA E DEMOGRAFIA

A cidade de Itanhandu possui população de 14.205 habitantes, 2.130 de população rural. Com 144 km² de área territorial, faz divisa com os municípios de Passa Quatro, Itamonte, Pouso Alto, Sebastião do Rio Verde e Virgínia, estando distante 450 km de Belo Horizonte.

O Município é servido por duas vias de acesso asfaltadas, sendo uma rodovia federal (BR-354) e uma rodovia estadual (MG-158) conforme figura abaixo.

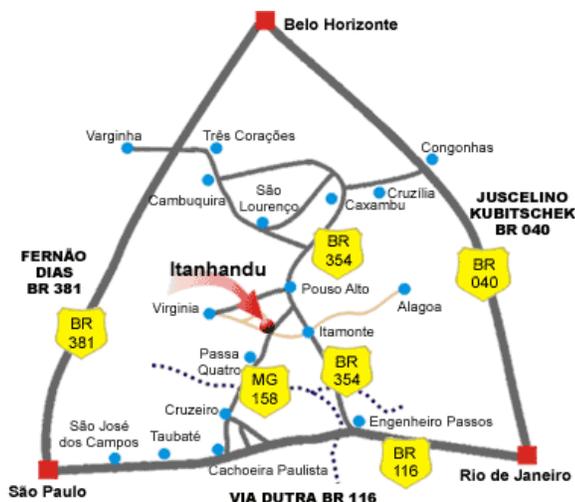


Figura 01: Mapa da Malha Viária de Acesso a Itanhandu/MG.

FONTE: <http://www.itanhandu.com.br>

1.3.2 PERFIL SÓCIO-ECONÔMICO

Itanhandu possui quatro agências bancárias, um hospital, uma agência da Receita Estadual, uma agência dos Correios, sete estabelecimentos de ensino (público, municipal e particular), uma casa lotérica e três postos de combustíveis. As principais atividades econômicas são a avicultura, agropecuária, indústria de calçados, confecções, laticínios e turismo.

1.3.3 PERFIL DA SEGURANÇA PÚBLICA

A cidade de Itanhandu possui uma Delegacia de Polícia Civil, um Fórum (sede de Comarca) e um Pelotão de Polícia Militar, sendo esta composta por 19 militares que atuam no policiamento ostensivo, prevenção e repressão da criminalidade.

1.3.4 PONTOS SENSÍVEIS E VULNERÁVEIS

Os principais pontos sensíveis ou vulneráveis estão localizados na área central, que abriga a maioria dos estabelecimentos comerciais, bancários e instituições como o fórum local, cadeia pública, delegacia e Prefeitura Municipal. Também são considerados pontos vulneráveis os trevos de acesso à cidade, que abrigam um posto de combustível e um estabelecimento comercial de varejo, ambos de grande porte, considerando as características da região. A sede do 6º Pelotão da Polícia Militar também é considerada um ponto sensível e estratégico.

1.3.5 ASPECTOS TÉCNICOS A SEREM CONSIDERADOS

Itanhandu é servida por rede de telefonia móvel e fixa, energia elétrica na tensão 110 V e provedores de Internet com acesso discado, via rádio e através da rede telefônica (ADSL), este último, em fase final de implementação.

1.4 O CIRCUITO FECHADO DE TV

1.4.1 FUNCIONAMENTO BÁSICO

CFTV, Circuito Fechado de Televisão, (do termo inglês *Closed CircuitTeleVision* - CCTV), é um sistema de televisão que distribui sinais provenientes de câmeras localizadas em um local específico, para um ponto de supervisão pré-determinado. Os sistemas de CFTV normalmente utilizam câmeras de vídeo CCD (para produzir o sinal de vídeo), cabos ou transmissores/receptores sem-fio ou redes (para transmitir o sinal), e monitores (para visualizar a imagem de vídeo captada).

O sistema de CFTV não é aplicado somente com propósitos de segurança e vigilância, também é utilizado em outros campos como laboratórios de pesquisa, em escolas ou empresas privadas, na área médica, assim como nas linhas de produção de fábricas.

1.4.2 PRINCIPAIS COMPONENTES DO SISTEMA DE CFTV

Os principais componentes necessários para um sistema de CFTV são: iluminação, lentes, componentes da câmera (câmera, CCD, suporte de montagem, cabeamento ou transmissor sem fio), web câmeras, processadores (sequencial, quad, multiplexador, matriz de vídeo), monitores, gravadores vídeo (time lapse VCR, placa de captura de vídeo, *digital vídeo recorder* – DVR) e alimentação.

Por definição, luz é a forma de energia radiante visível. A luz é indispensável para sensibilizar o sensor CCD e a partir dele transformar as imagens em sinais elétricos. Logo, a qualidade de uma imagem depende do controle da entrada de luz no conjunto lente/câmera. O tipo de local a ser monitorado e a aplicação determinam o tipo de equipamento a ser utilizado. Para aplicações internas, com iluminação garantida e maiores detalhes, podem ser utilizadas câmeras coloridas. Já locais externos, com períodos de baixa iluminação, é essencial o uso de câmeras P&B, pois sua sensibilidade é muito maior.

As Lentes são responsáveis pelo direcionamento, aumento e foco da imagem. Podem variar de acordo com a área a ser visualizada e a distância de trabalho, por isso é muito importante a definição da sua característica. Os modelos de lentes mais utilizadas são as de “íris fixa” para uso interno ou externo, desde que o ambiente não tenha grandes variações de luminosidade. Para uso externo e/ou com grande variação de luminosidade são utilizadas as lentes auto-íris, que fazem a compensação da luz, não deixando ofuscar a imagem. Existem lentes varifocais auto-íris, com zoom manual ou motorizada, para o ajuste de foco (distância de visualização com qualidade).

Velocidade Ótica é a característica que determina a velocidade que uma lente direciona um sinal luminoso e é definido pelo número-f (*f_number*) como $f/1.2$, $f/2.0$, etc. Esta velocidade é determinada pela Distância Focal (DF) e o Diâmetro (D) de uma lente:

$f_number = DF / D$, podemos dizer que quanto menor o *f_number*, maior a quantidade de luz direcionada para o sensor da câmera e melhor é a qualidade da imagem. O *f_number*, normalmente, é marcado no corpo da lente, especialmente no anel de abertura da íris.

1.4.3 O MODELO DIGITAL

O CFTV (Circuito Fechado de Televisão) digital proporciona uma administração mais fácil que outros sistemas disponíveis apresentando maior flexibilidade e possibilidades de expansão. Com recursos de pronto acesso as imagens ao vivo ou até mesmo as que foram gravadas, no caso, armazenadas em HDs (Hard Disk) seu dispositivo é muito simples, não ocorre degradação das imagens pelo fato de serem digitais e de alta qualidade e dispõe de um tempo de autonomia relativamente maior. Sistemas digitais reduzem os custos com operação resultando em um melhor custo e benefício. Oferecer a conexão em rede já é uma grande vantagem, pois o acesso pode ser local ou remoto através da rede/internet, gerenciamento de permissões de acessos e histórico de eventos (PERES, 2006, p.12).

O sistema é baseado na topologia IP (Internet Protocol) na qual o processamento é distribuído não só no sistema, mas também nas câmeras utilizando a base de conexão direta à rede Ethernet ou IP.

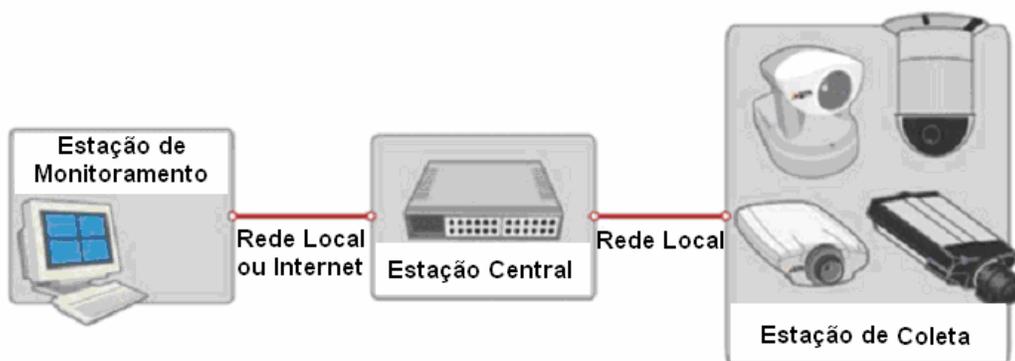


Figura 02: Esquema básico – CFTV Digital

FONTE: <http://www.guiadocftv.com.br>

1.4.4 AS CÂMERAS IP

A câmera IP, também chamada de câmera de rede, é um equipamento eletrônico que permite obter imagens, por meio de uma rede local ou pela internet, com objetivos de visualização, controle, monitoramento e gravação. Basicamente envolve um sensor de imagem, circuito de análise e processamento de vídeo, servidor de vídeo web, sistema operacional próprio e interface de rede. Suas funções e programação são específicas para o trabalho em rede. Peres (2008, p.03), destaca as funções de transmissão e configuração remota, processos de captura e compactação de imagens, configuração remota, controle de periféricos, atualização de aplicação, detecção de movimento, reconhecimento de faces, análise de movimentação, reconhecimento de objetos estranhos e falta de objetos ou mudança de cena, entre outras. A transmissão se faz através de redes Ethernet, com uso de protocolos, em especial o TCP/IP.



Figura 03: Câmera IP PTZ Speed Dome

FONTE: www.guiadocftv.com.br

Uma câmera IP oferece diversas vantagens quanto a sua utilização, como a redução na utilização de banda, uso da infraestrutura de rede existente, utilização de dispositivos de rede wireless (Wi-Fi), possibilidade de Pan/Tilt/Zoom Integrados, áudio, entradas e saídas digitais. Com resoluções de até 2592 x 1944 ou aproximadamente 5Megapixel a verificação de detalhes em uma imagem é maior devido a definição e recursos como o zoom em parte da imagem (PERES, 2008).

Peres, 2008 citou algumas das vantagens das câmeras IP:

- Utilização de infra-estrutura de rede e cabeamento estruturado, reduzindo os custos de implantação e manutenção de redes distintas.
- Permissão da utilização de soluções abertas ou híbridas para gravação e gerenciamento.
- Maior confiabilidade e segurança na transmissão de imagens;
- Uso de tecnologias de cabeamento com padrões de qualidade superiores, obtendo custos reduzidos para instalações de grande porte ou de missão crítica. (Uso de cabo CAT5e ao invés de cabos coaxiais RG-59).
- Possibilidade de alimentação via POE (Power over Ethernet), ou seja alimentação através do cabo de rede, que faz a transmissão de dados e alimentação.
- Possibilidade de atualização de aplicação (Firmware) e configuração remota via rede ou internet.
- Suporte a múltiplos padrões de vídeo e resoluções inclusive megapixel.
- Transmissão de comandos PTZ (pan, tilt e zoom) para câmeras móveis e speed-domes através do mesmo cabo.
- Possibilidade de transmissão de áudio, áudio bi-direcional, interface de entrada e saída de alarme, etc.
- Envios de alertas automáticos por e-mail e armazenamento de imagens por FTP.
- Suporte a diferentes codecs e formatos de compactação de vídeo, assim como diferentes protocolos de acordo com a aplicação.
- Possibilidade de integração com sistemas avançados de controle, incluindo funções de vídeo, supervisão, controle de acesso, alarme, automação, controle de tráfego, etc.
- Equipamentos prontos para crescerem de acordo com as necessidades da aplicação e desenvolvimento dos sistemas, permitindo uma vida útil maior sobre esta expansão.

Para o cálculo da largura de banda é necessário saber o tamanho do arquivo a ser transmitido. O tamanho do arquivo vai depender de diversos fatores como o tipo de compressão de vídeo (MJPEG, Wavelet, MPEG4), resolução da imagem (tamanho 640x480, 320x240, etc), número de frames por segundo (fps), número de usuários concorrentes.

O cálculo acontece da seguinte maneira: (N.º câmeras) X (tamanho da imagem em KB) X (número de frames transmitidos por segundo) X (número de usuários concorrentes) X (8(bits por byte)) = Largura de Banda

1.5 AS REDES DE COMPUTADORES

1.5.1 HISTÓRICO

O Departamento de Defesa do governo americano iniciou em 1966, através de sua agência DARPA (Defense Advanced Research Projects Agency) projetos para a interligação de computadores em centros militares e de pesquisa, com o objetivo de criar um sistema de comunicação e controle distribuído com fins militares. Esta iniciativa teve como um dos motivadores o surgimento de mini-computadores com grande poder de processamento, que poderiam ter seu emprego enriquecido com o acesso a uma grande rede de comunicação. Segundo Fatec 2009, esta rede recebeu o nome de ARPANET. Na década de 70 até 1983, a ARPANET era baseada em IMPs (Interface Message Processors), rodando diversos protocolos, sendo o principal o NCP (Network Control Protocol). O TCP/IP ainda estava sendo projetado e a Internet era formada por máquinas de grande porte e minicomputadores ligados aos IMPs.

O protocolo TCP/IP começou a ser projetado em 1977 com o objetivo de ser o único protocolo de comunicação da ARPANET. Tanenbaum 2006, afirma que em 1/1/1983, todas as máquinas da ARPANET passaram a utilizar o TCP/IP como protocolo de comunicação. Em 1993, foram criados os protocolos HTTP e o browser Mosaic, dando início ao World Wide Web (WWW). O World Wide Web foi o grande responsável pela crescimento exponencial da Internet, pois permitiu o acesso a informações com conteúdo rico em gráficos e imagens e de forma estruturada. No Brasil, o acesso à Internet foi iniciado com a conexão de instituições acadêmicas como a Fapesp, USP, Unicamp, PUC-Rio, UFRJ e outras em 1989. Foram formados dois backbones regionais, a RedeRio e a ANSP (An Academic Network at São Paulo) interligando as principais instituições destes estados.

1.5.2 O ENDEREÇAMENTO IP

O Protocolo IP é responsável pela comunicação entre máquinas em uma estrutura de rede TCP/IP. Ele provê a capacidade de comunicação entre cada elemento componente da rede para permitir o transporte de uma mensagem de uma origem até o destino. O protocolo IP provê um serviço sem conexão e não-confiável entre máquinas em uma estrutura de rede.

Qualquer tipo de serviço com estas características deve ser fornecido pelos protocolos de níveis superiores. As funções mais importantes realizadas pelo protocolo IP são a atribuição de um esquema de endereçamento independente do endereçamento da rede utilizada abaixo e independente da própria topologia da rede utilizada, além da capacidade de rotear e tomar decisões de roteamento para o transporte das mensagens entre os elementos que interligam as redes.

Um endereço IP é um identificador único para certa interface de rede de uma máquina. Este endereço é formado por 32 bits (4 bytes) e possui uma porção de identificação da rede na qual a interface está conectada e outra para a identificação da máquina dentro daquela rede. O endereço IP é representado pelos 4 bytes separados por . e representados por números decimais. Desta forma o endereço IP: 11010000 11110101 00111100 10100011 é representado por 208.245.28.63.

O destino de um mensagem IP sendo enviado por uma máquina pode ser a própria estação, uma estação situada na mesma rede ou uma estação situada numa rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e a mensagem é enviada por meio do protocolo de rede.

O protocolo IP define a unidade básica de transmissão, que é o pacote IP. Neste pacote são colocadas as informações relevantes para o envio deste pacote até o destino. Um datagrama IP consiste de um cabeçalho e uma área de dados. O cabeçalho ocupa uma área fixa de 20 bytes e uma área de tamanho variável (correspondente ao campo options).

O número de redes interligando-se à Internet a partir de 1988 aumentou, causando o agravamento do problema de disponibilidade de endereços na Internet, especialmente o desperdício de endereços em classes C e B. Desta forma, buscou-se alternativas para aumentar o número de endereços de rede disponíveis sem afetar o funcionamento dos sistemas existentes. A melhor alternativa encontrada foi flexibilizar o conceito de classes - onde a divisão entre rede e host ocorre somente a cada 8 bits.

A solução encontrada foi utilizar a identificação de rede e host no endereçamento IP de forma variável, podendo utilizar qualquer quantidade de bits e não mais múltiplos de 8 bits conforme ocorria anteriormente. Um identificador adicional, a máscara, identifica em um endereço IP, que porção de bits é utilizada para identificar a rede e que porção de bits para host.

O protocolo ICMP é um protocolo auxiliar ao IP, que carrega informações de controle e diagnóstico, informando falhas como TTL do pacote IP expirou, erros de fragmentação, roteadores intermediários congestionados e outros.

Uma mensagem ICMP é encapsulada no protocolo IP. Apesar de encapsulado dentro do pacote IP, o protocolo ICMP não é considerado um protocolo de nível mais alto.

Em uma estação e em um roteador, as informações constantes na tabela de rotas podem ser obtidas de diversas formas. As rotas podem ser obtidas por uma estação ou em um roteador de diversas formas, com limitações dependendo da implementação do TCP/IP em cada sistema operacional.

1.5.3 A INTERNET

Tanenbaum (2006, p.54) afirma que uma máquina está na Internet quando executa a pilha de protocolos TCP/IP, tem um endereço IP e pode enviar pacotes IP a todas as outras máquinas da grande rede.

Basicamente, a Internet é uma rede pública de comunicação de dados, com controle descentralizado e que utiliza o conjunto de protocolos TCP/IP como base para a estrutura de comunicação e seus serviços de rede. Isto se deve ao fato de que a arquitetura TCP/IP fornece não somente os protocolos que habilitam a comunicação de dados entre redes, mas também define uma série de aplicações que contribuem para a eficiência e sucesso da arquitetura. Entre os serviços mais conhecidos da Internet estão o correio-eletrônico (protocolos SMTP, POP3), a transferência de arquivos (FTP), o compartilhamento de arquivos (NFS), a emulação remota de terminal (Telnet), o acesso à informação hipermídia (HTTP), conhecido como WW (WorldWideWeb). A Internet é dita ser um sistema aberto uma vez que todos os seus serviços básicos assim como as aplicações são definidas publicamente, podendo ser implementadas e utilizadas sem pagamento de royalties ou licenças para outras instituições.

O conjunto de protocolos TCP/IP foi projetado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte direto a comunicação entre redes de diversos tipos. Neste caso, a arquitetura TCP/IP é independente da infra-estrutura de rede física ou lógica empregada.

1.5.4 O MODELO TCP/IP

O TCP/IP é um acrônimo para o termo Transmission Control Protocol/Internet Protocol Suite, ou seja é um conjunto de protocolos, onde dois dos mais importantes (o IP e o TCP) deram seus nomes à arquitetura. Para Tanenbaum, 2006, o modelo surgiu da necessidade de uma arquitetura flexível, capaz de se adaptar a aplicações com requisitos divergentes como, por exemplo, a transferência de arquivos e a transmissão de dados de voz em tempo real.

O protocolo IP, base da estrutura de comunicação da Internet é um protocolo baseado no paradigma de chaveamento de pacotes (packet-switching). A arquitetura TCP/IP, assim como OSI realiza a divisão de funções do sistema de comunicação em estruturas de camadas. Em TCP/IP as camadas são: Aplicação, Transporte, Inter-Rede e Rede.

A camada de rede é responsável pelo envio de datagramas construídos pela camada Inter-Rede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-rede para um endereço físico ou lógico do nível de Rede. A camada Inter-Rede é independente do nível de Rede. Os protocolos deste nível possuem um esquema de identificação das máquinas interligadas por este protocolo. Por exemplo, cada máquina situada em uma rede Ethernet, Token-Ring ou FDDI possui um identificador único chamado endereço MAC ou endereço físico que permite distinguir uma máquina de outra, possibilitando o envio de mensagens específicas para cada uma delas. Tais rede são chamadas redes locais de computadores. (X.25, Frame-Relay, ATM)

A Camada Inter-rede realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede onde estas estão situadas, é definido um identificador, chamado endereço IP, que é independente de outras formas de endereçamento que possam existir nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP em um endereço deste nível.

A Camada de Transporte reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário. Pode-se separar os protocolos de aplicação em protocolos de serviços básicos ou protocolos de serviços para o usuário.

A Internet é controlada pelo IAB (Internet Architecture Board) em termos de padronizações e recomendações. Este gerencia as funções de definição de padrões de protocolos, criação de novos protocolos, evolução, etc. OIAB é um fórum suportado pela Internet Society (ISOC), cujos membros organizam as reuniões e o funcionamento do IAB, além de votarem os seus representantes.

O UDP é um protocolo de nível de transporte orientado à transmissão de mensagens sem o estabelecimento de uma conexão entre máquina fonte e destino, fornecendo uma comunicação menos confiável que o TCP. Ele envia as mensagens (sem conexão) e não oferece nenhuma garantia de entrega ou seqüência.

O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de fluxo, o controle de erro, a sequenciação e a multiplexação de mensagens.

1.5.5 AS REDES SEM FIO (WIRELESS NETWORK)

A comunicação digital sem fios não é uma idéia nova. Em 1901, o físico italiano Guglielmo Marconi demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código morse (afinal de contas, os pontos e traços são binários)(TANENBAUM, 2006, p.33).

A comunicação sem fio é uma tecnologia que faz a transmissão dos dados sem a utilização de cabos fazendo uso da radiofrequência, tecnologia baseada no padrão IEEE 802.11, que estabelece normas para a criação e o uso de redes sem fio. Essa tecnologia torna possível desenvolver redes que proporcionam a conexão entre computadores e demais dispositivos que estejam dispostos geograficamente próximos. Com a vantagem de não utilizar cabos o usuário faz uso da rede em qualquer ponto respeitando os limites de alcance de transmissão e possibilita inserir outros computadores com facilidade na rede.

As principais semelhanças entre uma rede Wireless e uma rede Ethernet são que ambas permitem a troca de frames entre elemento da rede, são definidas pelo IEEE, possuem

cabeçalhos e trailers e implementam métodos para determinar quando um elemento pode ou não transmitir.

Para Fillipetti (2008, p.72), a principal diferença está no modo como os dados são transmitidos. Enquanto na rede Ethernet os frames são transmitidos por meio de sinais elétricos em cabo metálico ou sinais luminosos através da fibra óptica, a rede Wireless utiliza onda de rádio para transmitir os frames. O padrão Ethernet prevê a transmissão de dados em modo full-duplex, o que não acontece plenamente em redes wireless, que ao enviarem ondas de radiofrequência em um mesmo espaço e em uma mesma frequência, tornará ambas as ondas inteligíveis. Para definir a frequência utilizada para cada transmissão, redes wireless utilizam o algoritmo CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) para apoiar a transmissão em half-duplex.

A figura abaixo ilustra as tecnologias Wireless mais comuns e suas respectivas velocidades e alcances:

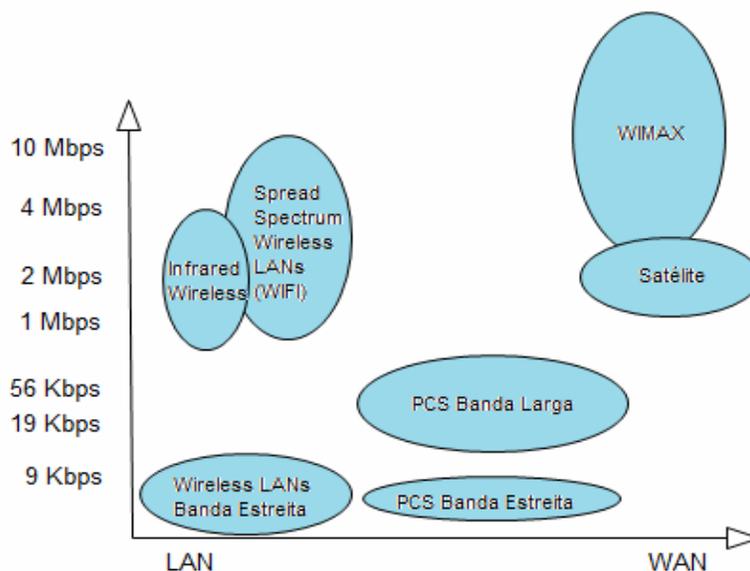


Figura 04: Comparativo entre as tecnologias Wireless disponíveis atualmente

FONTE: (FILLIPETTI, 2008, p.73)

Infrared Wireless LANs: Tecnologia de transmissão por infravermelho muito comum para transferência de dados entre dispositivos fisicamente próximos, desde que não existam barreiras entre eles. Pode atingir velocidades de até 4 Mbps, porém fica restrita à necessidade de proximidade física entre os pontos.

Wireless LANs Banda Estreita: Utiliza transmissão via ondas de rádio, porém sua baixa velocidade a torna inadequada para os requisitos atuais.

Spread Spectrum Wireless LANs: São as redes WIFI, regidas pelos padrões do IEEE, conforme ilustra a figura a seguir:

Tabela 01: Padrões IEEE 802.11 disponíveis

Padrão IEEE Wireless	802.11b	802.11^a	802.11g
Popularidade	Amplamente adotado e disponível em qualquer lugar	Tecnologia relativamente nova	Relativamente novo mas crescendo exponencialmente
Velocidade	Até 11 Mbps	Até 54 Mbps	Até 54 Mbps
Custo	Baixo	Mais elevado do que o 802.11b	Relativamente baixo
Frequência	2.4 Ghz	5 Ghz	2.4 Ghz
Alcance	Entre 100 – 150ft	Entre 25 – 75ft	100 – 150ft
Acesso Público	Alta disponibilidade de hotspots	Nenhum	Pode utilizar os hotspots compatíveis com o padrão 802.11b
Compatibilidade	Compatível com o padrão 802.11g	Incompatível com os dois padrões	Compatível com o padrão 802.11b

FONTE: (FILLIPETTI, 2008, P.74)

PCS Banda Estreita: PCS (Personal Communications Services) abrange os dados transmitidos através de microondas por dispositivos de uso pessoal, como pagers e celulares, entre outros, também como principal vantagem o alcance, sendo prejudicado pela velocidade de transmissão.

PCS Banda Larga: É a tecnologia adotada pelas redes celulares para transmissão de dados e voz.

Satélite: Tecnologia de transmissão de dados que alcança velocidades respeitáveis, porém devido às grandes distâncias sofre com os atrasos. Sua vantagem é a alta disponibilidade e abrangência.

WIMAX: Sigla para Worldwide Interoperability for Microwave Access ou Interoperabilidade global via acesso Microondas, refere-se a uma tecnologia extremamente nova, ainda de alto custo, que terá o mesmo alcance da rede celular à velocidade de um LAN Ethernet (100 Mbps).

Basicamente, existem dois modos de operação de uma rede WLAN: Modo Ad-Hoc, onde os dispositivos WIFI podem se comunicar sem o intermédio de um ponto de acesso e no modo

infraestrutura, onde é implementado um ou mais pontos de acesso wireless conectados à rede Ethernet por cabo metálico UTP.

O modo de operação infraestrutura suporta dois tipos de serviços: BSS (Basic Service Set), que utiliza apenas um ponto de acesso e o ESS (Extended Service Set) que disponibiliza vários pontos de acesso, o que permite a mobilidade dos usuários da rede.

A transmissão via ondas de rádio necessita de uma licença específica do órgão regulador, que no caso do Brasil é a ANATEL, o que reduz a chance de interferências com as outras formas de transmissão que utilizam a radiofrequência.

A área de cobertura, velocidade e capacidade de um determinado ponto de acesso serão determinadas principalmente pela potência de transmissão, frequência utilizada, interferências, obstruções e objetos que possam interferir na transmissão.

Tabela 02: Cálculo da distância de cobertura entre antenas em km.

Ganho da antena em dBi	24	21	18	15	12	10	8	5
24	6,5	5,5	4,2	4,0	3,2	5,5	2,0	1,8
21	5,5	4,5	3,7	3,0	2,5	2,1	1,8	1,5
18	4,2	3,7	3,0	2,5	2,1	1,8	1,5	1,2
15	4,0	3,0	2,5	2,5	2,0	1,8	1,3	1,0
12	3,2	2,5	2,1	2,0	1,8	1,5	1,0	0,8
10	2,2	2,1	1,8	1,8	1,5	1,3	0,8	0,5
8	2,0	1,8	1,5	1,3	1,0	0,8	0,5	0,3
5	1,8	1,5	1,2	1,0	0,8	0,5	0,3	0,2

FONTE: <http://www.underlinux.com.br>

A coluna vertical esquerda e a linha horizontal superior (laranja) mostram o ganho de cada antena direcional em decibéis dB. Os valores da tabela cruzada estão representados em km. Quando se quer, por exemplo, calcular a distância suportada utilizando uma antena de 21 dB no ponto 1 e outra antena de 15 dBi no ponto 2, a distância suportada seria de 3 km. Isto ajudará muito a ter uma idéia na hora de cobrir uma distância e que tipo de antenas e combinações pode-se usar. Estes cálculos são com visada limpa e equipamento de 63mw de potência.

A maioria dos Pontos de Acesso não necessita de configurações adicionais, mas alguns parâmetros podem e em alguns casos devem ser configurados tais como o padrão IEEE a ser utilizado, o canal (frequência de transmissão, o SSID (Service Set Identifier) e a potência de transmissão. Os clientes geralmente não necessitam de configurações adicionais.

As principais vulnerabilidades das redes sem fio são as invasões de redes não protegidas para obter acesso gratuito à Internet, furto e destruição de informações, funcionários que não seguem políticas de segurança e clonagem de pontos de acesso. As principais ferramentas contra essas vulnerabilidades são os recursos de Autenticação Mútua, Criptografia e outras ferramentas anti-intrusão. Os principais padrões de segurança WLAN são o WEP, WPA e WPA2, sendo os dois últimos os mais utilizados e eficazes atualmente.

2. DESENVOLVIMENTO DO PROJETO

2.1 DESCRIÇÃO GERAL DO PROJETO

A partir do estabelecimento dos componentes do Sistema de Circuito Fechado de TV (CFTV), será desenvolvido o projeto da rede de computadores sem fio para realizar a interconexão de 25 câmeras de monitoramento do tipo IP PTZ tipo Speed Dome a prova de vandalismo na área urbana da cidade de Itanhandu/MG e concentrar o seu sinal em uma estação central. A instalação das câmeras se dará em postes próprios, que também abrigarão antenas, abrigos para os dispositivos (fontes e proteções) bem como alto-falantes para comunicação direta entre a estação central e o local onde a câmera estará instalada. Todas as câmeras deverão ser instaladas em postes de pelo menos 15 (quinze) metros de altura a partir do solo.

O projeto contempla também o desenvolvimento rede de computadores da estação central, que abrigará os equipamentos gerenciados pelo Sistema de Circuito Fechado de TV, conforme figura abaixo:

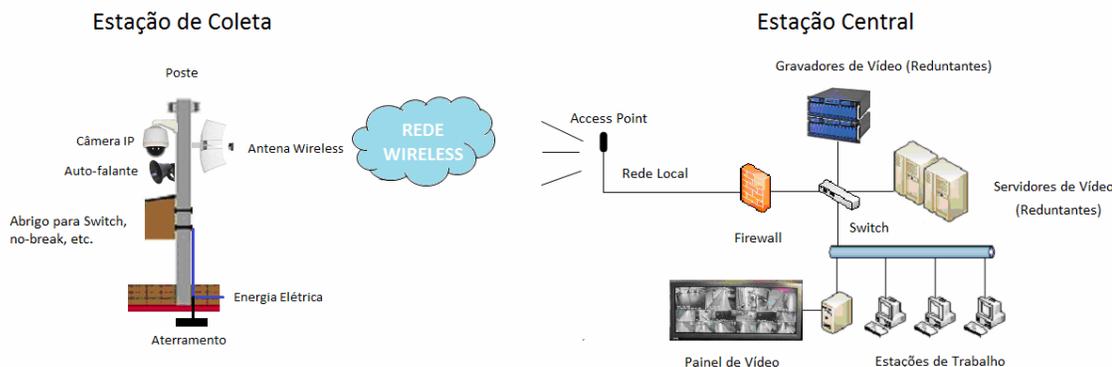


Figura 05: Esquema geral do projeto

FONTE: (SSPDS, com adaptações do autor)

2.1.1 LOCAIS DE INSTALAÇÃO DAS ESTAÇÕES

Tabela 03: Distribuição das Estações de CFTV

Estação	Localização	Distância aproximada da Estação Central	Pontos de Abrangência
A	Av. Fernando Costa	5 m	Futuras instalações do 6° Pel PM Estação Central
B	Av. Fernando Costa	100 m	Agência dos Correios / Banco Postal
C	Av. Fernando Costa	300 m	Fórum Área Bancária Área Comercial
D	Av. Fernando Costa	400 m	Área Comercial Área Bancária Calçadão
E	Av. Professor Brito	100 m	Área escolar
F	Av. Professor Brito	400 m	Área Comercial / Eventos
G	Av. Professor Brito	500 m	Área Comercial / Eventos
H	Praça Amador Guedes	500 m	Praça Municipal/Eventos populares Prefeitura Municipal Área Comercial Posto de Combustíveis
I	Praça Amador Guedes	600 m	Praça da Matriz
J	Rua Arlindo Luz	700 m	Unidade de Polícia Judiciária Cadeia Pública Posto de Combustíveis
K	R. Alexandre Moreira	1000 m	Hospital Área Escolar
L	R. Alexandre Moreira	1200 m	Acesso à área central
M	Trevo de Acesso à Rodovia MG-158	1300 m	Acesso à área urbana Posto de Combustíveis
N	Rua Zequinha Pinto	1500 m	Área escolar
O	Av. Fernando Costa	50 m	Terminal Rodoviário
P	Av. Tereza Guedes	400 m	Acesso à área central.
Q	Trevo de Acesso à Rodovia MG-158	700 m	Acesso à área urbana Estabelecimento comercial de varejo
R	Av. Professor Brito	200 m	Área escolar
S	Rua Nicolau Scarpa	350 m	Acesso à área central
T	Av. José de Lourdes Salgado Scarpa	800 m	Área escolar
U	Av. José de Lourdes Salgado Scarpa	1200 m	Acesso à área urbana
V	Rua Pedro Cunha	700 m	Ginásio Poliesportivo
W	Rua Pedro Cunha	900 m	Acesso à área central
X	Av. João da Silva Costa	1000 m	Área escolar
Y	Av. Ary Carneiro	1200 m	Acesso à área central

ESTAÇÃO CENTRAL

Estação	Localização	Pontos de Abrangência
Z	Av. Fernando Costa	Futuras instalações do 6° Pel PM

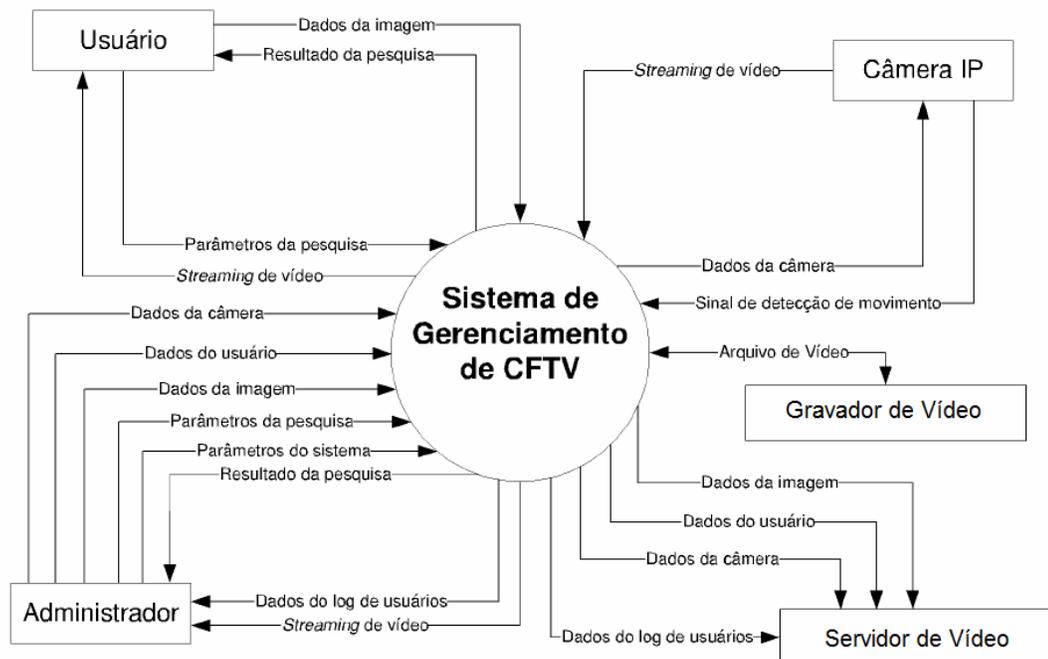


Figura 07: Diagrama de Fluxo de dados do CFTV

FONTE: (SIMÕES, 2007, p.119)

2.2.2 ESTAÇÕES DE TRABALHO (WS – WORKSTATION)

a) Descrição

O sistema de CFTV será composto de 03 (três) estações de trabalho, com dois monitores LCD cada. O acesso às imagens do sistema deverá ser controlado através dos privilégios de acesso designados para cada operador.

As estações de trabalho deverão ser responsáveis pela interação homem máquina do sistema de CFTV. As imagens deverão ser visualizadas através destas estações, sempre levando em consideração os níveis e privilégios de acesso de cada usuário do sistema. As estações de trabalho deverão ainda suportar as seguintes aplicações: Ferramentas de Configuração, Reprodução de Arquivos Gravados e Geração de Relatórios;

Cada estação de trabalho operando o sistema de CFTV deverá ter a possibilidade de utilizar um teclado de CFTV (mesa de comando) que possa controlar todo o conjunto de câmeras do sistema. Estas estações deverão ter a capacidade de exibir até 16 streamings de vídeos simultâneos, processando as imagens a 30 frames por segundo, com resolução 4CIF (704 x 480);

O sistema deverá ainda ter log de eventos, exibir interface de alarmes, possuir capacidade de exportar vídeo gravado e imagens em diversos formatos incluindo formato nativo e AVI;

A estação de trabalho deve oferecer recursos para facilitar a operação do sistema. Dentre estes recursos devem estar contemplados: controle PTZ on-screen, configuração de diversos tipos de mosaicos, botão para playback instantâneo com tempo pré configurável;

As estações de trabalho deverão possibilitar busca inteligente de vídeo, ou seja, deverá ser possível parametrizar as buscas de vídeos baseado nas regras definidas no sistema de análise inteligente de vídeo;

b) Especificações técnicas das Estações de Trabalho

Processador: Intel® Core®2 Extreme 2.93 GHz, 4 MB cache, 1066 MHz FSB

Memória RAM: 2 GB

Sistema Operacional: Windows XP Pro

Vídeo: 512 MB Dual Head

Padrão de Vídeo: VGA (1280 x 1024)

Velocidade de Visualização: Até 30 imagens/segundo a 4CIF

Interface PTZ: On-screen ou via Teclado Joystick

Interface de Rede: Gigabit Ethernet RJ-45, (1000BaseT)

Mídia DVR-RW 16x

Alimentação: 100-240 VAC, 50/60 Hz, Automático

Monitor: 19" LCD TFT com alta resolução

2.2.3 SERVIDORES DE CFTV

a) Descrição

O sistema de CFTV será composto de 2 (dois) servidores de CFTV. Estes servidores controlarão o acesso às imagens pelas estações de trabalho, controlando privilégios e

prioridades de acesso. Os dois servidores deverão trabalhar de forma totalmente redundante (hot standby) de forma a garantir a disponibilidade mínima de 99,80% ao ano.

b) Especificações técnicas dos Servidores de CFTV

Processador: 2 Processadores Intel Xeon E5450 Quad-Core de 3.00 GHz com 2 x 6 MB de memória cachê (1333 FSB)

Memória RAM: 4 GB, 667 MHz (2 x 2 GB), 2R

Discos Rígidos: 06 discos rígidos de 73GB SAS 3.5" de 15.000 rpm

Controlador RAID: Controladora de array integrada SAS 3Gb/s para até 6 discos, com 256 MB de memória cachê ECC e com bateria, com capacidade para RAID 5.

Sistema Operacional: Windows 2003 Server Standard

Vídeo: 256 MB Dual Head

Padrão de Vídeo: VGA (1280 x 1024)

Interface de Rede: 2 interfaces Gigabit Ethernet RJ-45, (1000BaseT)

Mídia DVR-RW 16x

Alimentação: 100-240 VAC, 50/60 Hz, Automático

Monitor: 19" LCD TFT com alta resolução

Teclado: Teclado USB

Mouse: Mouse Ótico USB 2 botões com scroll

2.2.4 GRAVADOR DE VÍDEO EM REDE (ARQUIVADOR)

a) Descrição

O sistema de CFTV deverá ser composto por sistema de Gravação de Vídeo em Rede redundante, ou seja, as imagens deverão ser armazenadas, simultaneamente, em dois NVRs.

O Gravador de Vídeo em Rede deverá armazenar todos os streams por 5 dias e trabalhar de maneira totalmente redundante. Deverá ser totalmente compatível com calendários de gravação, alarmes e eventos, pré-alarme e pós-alarme, bem como possibilidade de gravação por movimento;

Cada arquivador deverá ter capacidade interna de armazenar no mínimo 6TB, sendo que o sistema deve suportar expansões ilimitadas na capacidade total de armazenamento, dependendo unicamente da aquisição, configuração e limitação técnica de hardware;

O sistema deverá utilizar padrão de gravação de alta performance, devendo oferecer suporte a no mínimo RAID 5. Deverá ter fonte redundante e porta de rede Gigabit dual;

Para dimensionamento dos storages devem ser levados em consideração os seguintes parâmetros: gravação redundante, 4CIF / 30fps, armazenamento de 5 dias com taxa de movimentação de 100%. Deve ser considerado um fator de segurança de 15%.

b) Especificações técnicas dos gravadores de vídeo em rede

Processador: IBM RISK ou similar

Hard Drives: 500 GB cada, com suporte a hot-swapping

Montagem: Rack 19"

Interface de Usuário: Remota via WS ou via Aplicação

Capacidade de Armazenagem: No mínimo 6TB por arquivador

Interface: SATA

RAID Level: 5

Compressão de vídeo: MPEG-4 parte 10 ou H.264

Resolução: 4CIF, CIF, QCIF

Alimentação: 100-240 VAC, 50/60 Hz

Fonte de Alimentação: Interna e redundante

Temperatura de Operação: 0 a 40° C

2.2.5 SOFTWARE DE VISUALIZAÇÃO, ANÁLISE, GERENCIAMENTO E SUPERVISÃO

a) Descrição

O software deverá operar em redes heterogêneas (Fibra óptica, Ethernet, sem fio e até uma rede celular GPRS), as imagens armazenadas devem estar na qualidade máxima para análise posterior, permitir a transmissão para monitoramento real e consultas na taxa disponível, ou definida pelo cliente, independente da imagem gravado, trabalhando conforme figura abaixo

b) Módulo de gerenciamento e análise inteligente de vídeo

O sistema deverá contemplar análise de conteúdo de vídeo em todas as câmeras que irão compor a solução de CFTV. Esta análise deverá prever no mínimo as seguintes regras:

- Geração de alarme quando a câmera é coberta ou obstruída por algum tipo de objeto;

- Geração de alarme quando houver uma variação brusca da luminosidade ambiente, como por exemplo em casos onde um foco de luz muito intensa é apontado diretamente para a câmera;

- Geração de alarme de contagem de pessoas que ultrapassam uma linha virtual, para análise estatística ou para reunir informações relevantes;
- Geração de alarme conforme a direção de um movimento para controle do fluxo de pessoas e/ou veículos;

- Geração de alarme quando algum objeto for removido do seu local de costume;

- Geração de alarme quando algum objeto for deixado numa cena por um determinado período de tempo;

- Geração de alarme quando for detectado que uma pessoa ou veículo está parado por muito tempo em determinado local;

- Geração de alarme quando for ultrapassada uma barreira horizontal ou vertical previamente configurada.

O sistema de análise inteligente de vídeo deverá estar integrado ao sistema de CFTV, ou seja, o sistema de análise de vídeo deverá gerar metadados para o sistema de CFTV possibilitando a busca de imagens armazenadas, através das regras definidas no sistema de análise de vídeo.

c) Módulo Visualizador do Sistema e Operação/Supervisão do CFTV

O software deverá permitir aos operadores interagir com câmeras de vídeo PTZ e visualizar imagens em tempo real ou armazenadas (suportando câmeras individuais ou em grupos). Este software deverá ser composto de um módulo servidor e um módulo cliente.

O módulo cliente deverá prover uma interface simples para controle e visualização das câmeras. O controle das câmeras PTZ deverá ser feito utilizando um controle tipo joystick e através de navegação utilizando controles na interface do software de supervisão.

O módulo servidor deverá gerenciar o controle de acesso às câmeras. Assim quando mais de um módulo cliente requisitar controle de uma câmera PTZ ao mesmo tempo, o módulo servidor deverá arbitrar (por meio de prioridades de acesso pré-configuradas) qual cliente receberá controle da câmera. Deverão ser fornecidas 05 licenças do módulo de operação/supervisão do CFTV, para as estações de operação da sala de vídeo-monitoramento.

2.2.6 TECLADO DE COMANDO

O sistema deverá contar com 01 (um) teclado de comando para cada operador. Estes dispositivos deverão ter a capacidade de chavear imagens nos monitores próprios de cada estação. Além de chavear imagens para os monitores, os teclados de comando também deverão suportar a movimentação (pan / tilt / zoom) de todas as câmeras móveis do sistema.

ESPECIFICAÇÕES TÉCNICAS

Interface: Serial ou USB

Alimentação: 12 VDC

Teclado: Teclas 0-9, câmera, monitor, teclas multi view

Joystick: Três eixos (pan / tilt / zoom)

2.2.7 SISTEMA DE VISUALIZAÇÃO DISPLAYWALL

O sistema de visualização “display wall” deverá ser integrado ao sistema de CFTV via rede Ethernet TCP/IP. Este sistema deverá possuir as seguintes características, conforme ilustração abaixo:

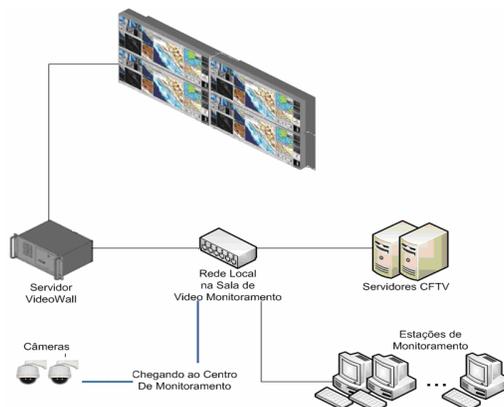


Figura 08: Sistema de visualização “Display Wall”

FONTE: (SSPDS, com adaptações do autor)

- Sistema de visualização formado por cubos de retroprojeção dispostos em matriz, unidos mecanicamente, constituindo uma única tela lógica; Dimensões total da área de visualização: 3,20m x 2,40m.
- Tecnologia DLP (digital light processing);
- Operação em regime contínuo (7 dias/semana x 24 horas);
- Chip de alto desempenho 0,95" com contraste otimizado e roda de cores de velocidade 3X;
- MTBF do Chip de alto desempenho: 650.000 horas;
- Life Time do Chip de alto desempenho: 100.000 horas;
- MTTR de 45 minutos;
- Roda de cores, com controle de saturação automático das cores, com mais de 16,7 milhões de cores;
- Resolução nativa (por cubo): 1400x1050 pixels (nativos);
- Lâmpadas de 100 W = MTBF de (2x) 10.000 horas (de acordo com IEC 61947-1);
- Alinhamento de lâmpadas automatizado após troca de lâmpada para otimização da uniformidade de cores e brilho;
- Cada cubo com lâmpada e fonte de iluminação redundantes e auto-chaveamento;
- Mecanismo de redundância de lâmpadas permite que elas operem dos seguintes modos:
Hot-Standby: As duas lâmpadas ficam acesas. A lâmpada redundante garante que haja imagem todo tempo.
Cold-Standby: A lâmpada redundante é acesa em até 30 segundos após uma falha da lâmpada principal.
Auto-Switch: As duas lâmpadas são usadas seqüencialmente o que garante que ambas terão a mesma utilização a todo o momento.

- Telas com compensação de dilatação térmica de modo a não apresentar abaulamento ou distorções na faixa de temperatura de 15°C a 40° C;
- Tela de alta precisão tipo Black Screen totalmente anti-reflexiva de alta performance em contraste, capaz de operar em ambiente interno, com iluminação natural ou artificial;
- Ângulo de visão de 180 graus na horizontal e vertical;
- Ângulo de meia luz (half gain) de até 35 graus;
- Dimmer óptico para o controle automático de brilho de duas telas adjacentes, para obter os mesmos valores de luminância entre os cubos;
- Contraste 1600:1;
- Uniformidade de brilho: maior que 95%;
- Alimentação 100~240 VAC;
- Lente tipo Fresnel para manter o foco uniforme em toda a área da tela;
- Estrutura metálica em liga leve de alumínio anodizado;
- Possuir espelho para minimizar a distância de projeção da imagem;
- Altura da base de sustentação configurável durante o projeto;
- Todos os cabos, conectores, adaptadores e conversores necessários à interconexão dos componentes do sistema fazem parte do deste fornecimento;
- Fácil acesso para manutenção ao interior da matriz e dos cubos isoladamente através de tampas destacáveis;
- Projetores com auto-diagnóstico de operação e falhas, para um menor custo de manutenção;

De forma a complementar a operação do VideoWall deverá ser disponibilizada 01 (uma) televisão de LCD de 42”, que será instaladas ao lado do VideoWall.

2.2.8 ESTAÇÕES DE COLETA DE IMAGENS

As estações de coleta de imagens serão compostas câmeras de monitoramento que serão instaladas em postes metálicos a 12,5 metros do solo e os equipamentos de proteção e alimentação elétrica e transmissão de dados serão instalados em um abrigo a 5 metros do solo. Também será acoplado um auto-falante à saída de áudio da câmera. As especificações técnicas de todos componentes seguem adiante.

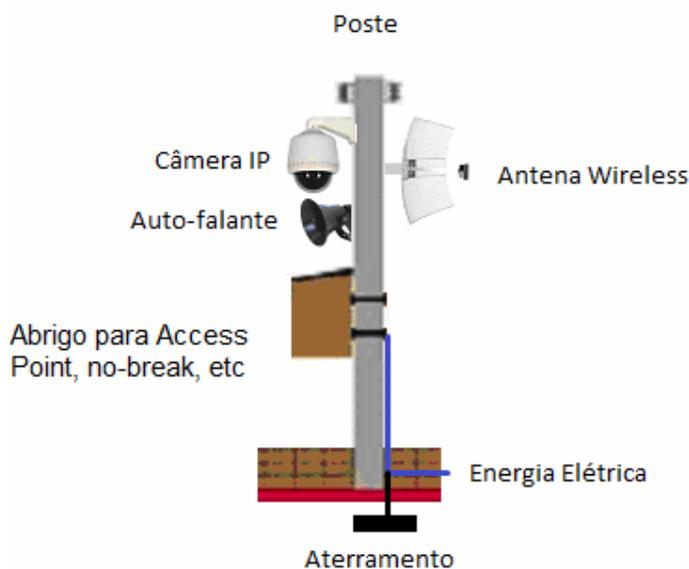


Figura 09: Estação de Coleta de Imagens
 FONTE: (SSPDS, com adaptações do autor)

2.2.9 CAMERAS IP

Em cada uma das estações de coleta de imagens será instalada uma Câmera IP Móvel 36X a Prova de Vandalismo (Dia e Noite – Externa) que deverá ser Colorida Tipo Speed Dome e apresentar as seguintes especificações:

- Sensor de imagem em estado sólido do tipo CCD (Charged Coupe Device) de 1/4” (um quarto de polegada);
- Lente com zoom ótico de pelo menos 36x e com Zoom digital de 12X;
- Padrão de cores NTSC;

- Resolução mínima de 520 linhas;
- Compensação automática para tomada de imagem contra luz de fundo;
- Sensibilidade deverá ser compatível com a operação vinte quatro horas por dia, apresentando imagens com qualidade e resolução adequadas ao perfeito funcionamento do Sistema;
- A câmera deverá se manter colorida durante a luz do dia e, visando uma melhor visualização, preto e branca durante a noite. O chaveamento entre o modo dia e modo noite deve ser automático, com corte no filtro de IR;
- Sensibilidade mínima deverá ser igual ou inferior 0,01 lux;
- Lente auto-íris;

Conter plataforma móvel na câmera com as seguintes características:

- Deverá apresentar, no mínimo, movimento de rotação horizontal ("pan") de 360° contínuos e movimento de rotação vertical com Autoflip;
- Velocidade de varredura variável de 0,1° até 120° por segundo;
- Conter caixa de proteção do tipo dome pendante e caixa em alumínio a prova de vandalismo, que deverá proteger totalmente a câmera das vibrações causadas pelo tráfego, potenciais tentativas de vandalismo, chuva, poeira, umidade e altas temperaturas; (Com grau de proteção IP66);
- Dispositivo anti-embaçante;
- Deverá dispor no mínimo 80 posições programáveis (Presets), rotinas e varreduras múltiplas, com precisão de posicionamento de 0,1°;
- Deverá possuir o receiver/driver multiprotocolo integrado;
- Deverá possuir ao menos 24 zonas de mascaramento de imagem programáveis;
- Deverá dispor de no mínimo 3 entradas e 1 saída programável;
- Deverá ser acompanhada do suporte de fixação completo para Poste ou parede do mesmo fabricante com fonte de alimentação a ser instalada no quadro elétrico;
- Deverá acompanhar invólucro (caixa de proteção) à prova de vandalismo com cúpula em policarbonato.

2.2.10 ARMÁRIOS PARA ABRIGO DOS EQUIPAMENTOS

O armário abrigará os componentes de transmissão de dados, alimentação e Sistemas de Proteção elétrica das Câmeras, devendo possuir as seguintes características:

- Caixa em chapa de aço SAE 1008;
- Dobras adicionais de 15° que protegem a caixa contra a entrada de água e pó;
- Placa de Montagem: É removível, permitindo a montagem dos equipamentos em bancada;

- Flange é removível facilitando a furação e a passagem de cabos ou eletrodutos;
- Possibilidade de comportar: Switch, encoder, Fonte de alimentação, Nobreak e sistemas de proteção de surto;
- Possuem borracha para vedação;
- Fecho: O fecho é standard de fenda em metal;
- Porta removível, sendo as dobradiças com pinos desmontáveis;
- Modo de fixação: Parede ou poste;
- Grau de Proteção: IP 54 IK10;
- Microventiladores (4) axial e exaustor 127V;
- Termostato digital para ventilador e exaustor;
- Projetados, ensaiados e aprovados perante os requisitos da NBR IEC 62208.

2.2.11 PROTETOR DE SURTO

Devem ser instalados os equipamentos de Proteção de Surto em todos os postes, seguindo as seguintes especificações:

- IEC classe I, II e III;
- Montagem em trilho DIN;
- Pólo simples corrente de pico de 60 KA (10/350 micros) para classe I;
- Pólo múltiplo corrente de pico de maior que 100 KA (10/350 micros) para classe I;
- Atende todas as ranges de alimentação corrente alternada;
- Proteção de surto IEC 61312; recomendação IEC 61643.

2.2.12 NO-BREAK DE CAMPO

Devem ser fornecidos e instalados os equipamentos de No-break em todos os postes, obedecendo as seguintes especificações técnicas:

Entrada de Alimentação:

- Tensão nominal de entrada: 127V - 60 Hz;
- Frequência nominal 60 Hz;
- Fator de potência: 0.97 ou superior.

Saída do No-Break:

- Capacidade de Potência de Saída: 800 Watts / 1000 VA.

- Tensão nominal de saída: 120V – 60Hz configurável para 110/120 VCA.
- Eficiência em carga total: 87% ou superior.
- Distorção da Tensão de Saída Inferior a 6% na carga máxima
- Frequência de Saída: sincronizada com rede elétrica.
- Fator de Crista: até 3 : 1
- Tipo de Forma de Onda: senoidal.
- Regulação automática de voltagem.
- Tomadas de saída: 4.

Baterias:

- Tipo de bateria: Bateria selada livre de manutenção, a prova de vazamento.
- Montagem: interna no gabinete do no-break.
- Tempo de recarga: recuperação de 90% da carga em no máximo 6 horas após descarga.
- Tempo de autonomia típico em meia carga: 13.6 minutos.
- Capacidade de instalação de banco de bateria de extensão (montagem interna ou externa).

Gerenciamento:

Gerenciamento SNMP com acesso remoto através da rede de dados.

Painel/Operação:

- Painel de controle: do tipo LCD ou do tipo Display de LED com indicação de estado de funcionamento, carga e sobrecarga.
- Alarme sonoro e visual na ocorrência de falhas.
- Operação em bypass de forma automática nos casos de sobrecarga ou de operação em sobre-temperatura com indicação no painel.
- Proteção contra surtos e filtragem:
- Proteção contra surtos e filtragem de “ruídos” da rede elétrica.

2.2.13 POSTE METÁLICO

Os postes serão instalados em locais de instalação das câmeras, observando-se os critérios para as licenças e permissões necessárias para a colocação de postes em vias públicas.

Os postes devem possuir as seguintes características:

- Poste Metálico. Altura total de 15 metros.
- Suporte para câmera (s) dome (fixas) em ferro galvanizado.

- Suporte para antena de comunicação em ferro galvanizado
- Aterramento
- Tubos em aço galvanizados a fogo em chapa dobrada de alta resistência mecânica e resistência a corrosão e galvanizadas por imersão a quente;
- Parafusos dos flanges em aço;
- Cabo para sistema trava-queda em aço inoxidável diâmetro 8mm;
- Chumbadores em aço;
- Deve ser dotado ainda de mecanismo de pára-raio com aterramento na base a fim de evitar quaisquer danos aos mecanismos e prover segurança aos transeuntes.
- O acesso dos cabos de energia e rede será resguardado por uma proteção (seguido por dentro da estrutura do poste) de modo a proteger contra vandalismos, deve ter resistência a fogo, corrosão e a violações que comprometam a continuidade da comunicação da solução.

2.2.14 SISTEMA DE ÁUDIO

Além da câmera, cada poste do sistema terá um alto-falante instalado (loud-speaker). Estes alto-falantes serão próprios para áreas com altos índices de ruído e serão conectados à saída de áudio da câmera IP.

O sistema de áudio será utilizado com a finalidade de alertar e afastar possíveis suspeitos das áreas próximas das câmeras. Ou seja, caso os operadores do sistema visualizem alguma atitude suspeita, ou alguma pessoa precisando de auxílio, terão o recurso do áudio para um primeiro contato.

Os alto-falantes deverão ser capazes de gerar um SPL mínimo de 110dB à uma distância de 3 (três) metros.

2.3 PROJETO DA REDE DE COMPUTADORES

2.3.1 DESCRIÇÃO GERAL

O Projeto da Rede de Computadores será composto por uma solução híbrida onde será aplicada uma Rede Wireless para a transmissão do sinal das câmeras até a estação central operando conforme o Padrão 802.11g (com alcance limitado a 5 Km, o que é completamente viável às características da cidade) e uma rede local na própria estação central, que irá interconectar os equipamentos de controle, monitoramento e gerenciamento do CFTV, seguindo o padrão Gigabit Ethernet, conforme diagrama abaixo:

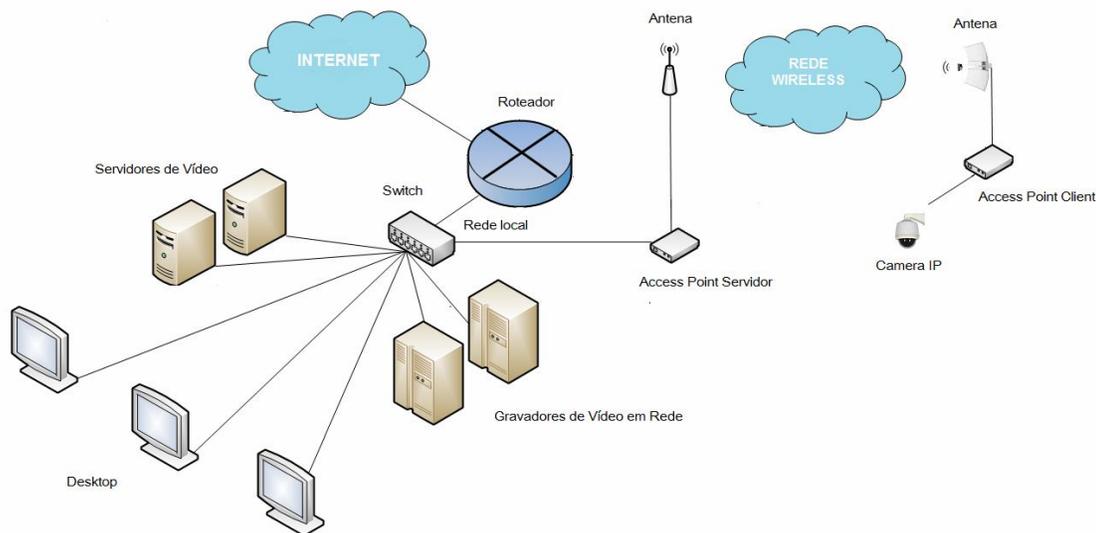


Figura 10 – Esquema geral da Rede de Computadores

FONTE: (O autor)

2.3.2 CÁLCULO DA LARGURA DE BANDA E ESPAÇO EM DISCO

Considerando apenas um usuário visualizando as 25 câmeras a 10fps com um tamanho de imagem de 19 Kbytes (padrão de compressão MPG-4), o que é perfeitamente viável no ambiente em que se dará a implementação do projeto, irá requerer uma largura de banda de 38 Mbits/seg.

O cálculo acontece da seguinte maneira: 25 (câmeras) X 19KB (tamanho da imagem) X 10 fps(número de frames transmitidos por segundo) X 1(número de usuários concorrentes) X 8 (bits por byte) = 38 Mbits/seg

Considerando os dados acima e a necessidade de se armazenar as imagens por 5 dias, será necessário aproximadamente 1957 Gbytes de espaço em disco.

2.3.3 INFRAESTRUTURA DA REDE DE TRANSMISSÃO WIRELESS

A rede de transmissão sem fio será licenciada pela Anatel, conforme legislação em vigor e será desenvolvida conforme o padrão IEEE 802.11g, operando na frequência de 2.4 Ghz e velocidade de até 54 Mbps, com um radiotransmissor de 400mW de potência, transmitindo à distância máxima de 5 quilômetros.

Os sinais de vídeo e dados de cada uma das 25 câmeras IP que compõem o projeto, serão transmitidos por um Access Point Client conectado a um antena direcional de 24 dBi até a antena Omni de 15 dBi da estação central, instalada em uma torre de 40 metros, de forma a oferecer visada para todas as estações, conforme ilustração abaixo:

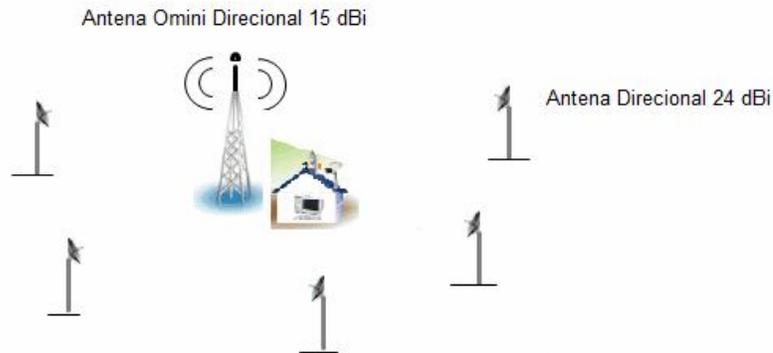


Figura 11: Infra-estrutura da rede wireless.

FONTE: (SSPDS, com adaptações do autor)

2.3.4 MÓDULO DE CONECTIVIDADE DAS ESTAÇÕES DE COLETA DE IMAGENS

Este módulo será composto de 01 cabo Pig Tail de 04 metros, 01 cabo Crossover Nível 5, 01 access point cliente conectado à interface de rede da câmera IP e uma Antena Direcional de 24 dBi e deverá receber o sinal dos dispositivos de coleta de imagens e conectá-los à Rede Wireless.

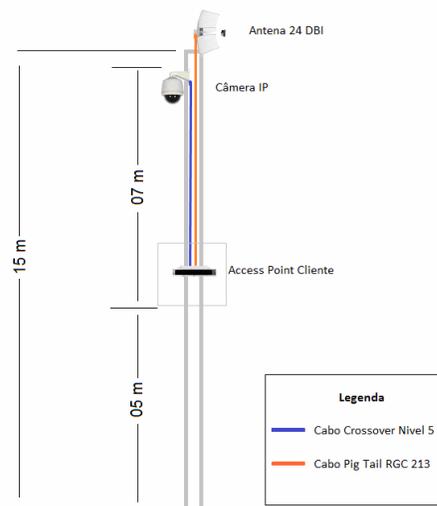


Figura 12: Esquema do conjunto câmera / access point client / antena

FONTE: (O autor)

2.3.5 ENDEREÇAMENTO IP

O Switch instalado na Estação Central receberá os dados das 25 câmeras IP, realizando a interconexão com os servidores, gravadores, estações de trabalho e demais equipamentos. Todos os componentes da rede receberão um endereço IP fixo.

Para proporcionar uma melhor gerência dessa rede híbrida, será realizada uma segmentação lógica através de VLANs implementadas no Roteador de forma a separar as câmeras IP, as estações de trabalho e os equipamentos de gerência e supervisão do Sistema de CFTV.

2.3.6 CÁLCULO DAS SUBREDES

Considerando as 25 Câmeras IP, os equipamentos da estação central, as necessidades de segmentação da rede e possíveis ampliações, foi realizado o cálculo para 4 subredes, com 60 hosts cada, utilizando o endereço IP 200.0.0.0 de classe C.

1ª SUBREDE

Endereço de rede: 200.0.0.0
Endereço do primeiro host: 200.0.0.1
Endereço do último host: 200.0.0.62
Endereço de broadcast: 200.0.0.63

2ª SUBREDE

Endereço de rede: 200.0.0.64
Endereço do primeiro host: 200.0.0.65
Endereço do último host: 200.0.0.126
Endereço de broadcast: 200.0.0.127

3ª SUBREDE

Endereço de rede: 200.0.0.128
Endereço do primeiro host: 200.0.0.129
Endereço do último host: 200.0.0.190
Endereço de broadcast: 200.0.0.191

4ª SUBREDE

Endereço de rede: 200.0.0.192
 Endereço do primeiro host: 200.0.0.193
 Endereço do último host: 200.0.0.254
 Endereço de broadcast: 200.0.0.255

2.3.7 CONFIGURAÇÃO DOS EQUIPAMENTOS

a) Distribuição das subredes

Será atribuído um endereço IP fixo para cada host da rede, sendo utilizado o padrão 802.1Q para a criação de redes virtuais (VLANs) para a distribuição das subredes, conforme ilustração abaixo:

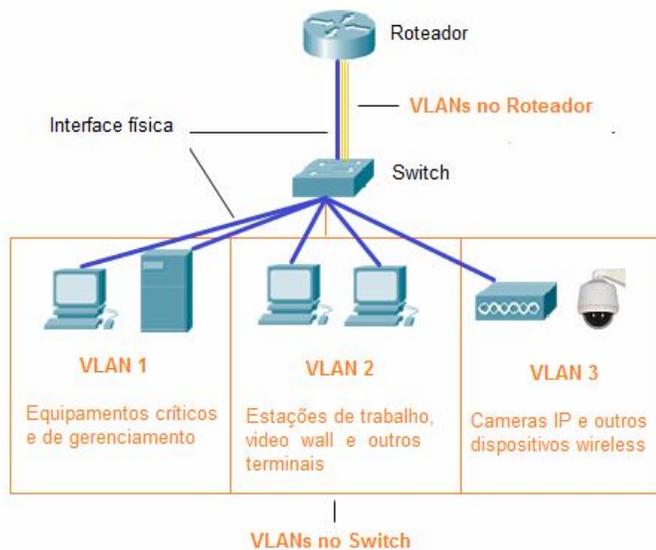


Figura 13: Segmentação lógica da rede através de VLANs

FONTE: (O autor)

b) Configuração do Roteador

Tabela 04: Configuração básica das Interfaces do Roteador

INTERFACE	ENDEREÇO IP	MODO	VLAN
Fast Ethernet 0/0	200.0.0.1	Simplex	-
Fast Ethernet 0/0.1	200.0.0.65	VLAN 802.1Q	VLAN 1
Fast Ethernet 0/0.2	200.0.0.129	VLAN 802.1Q	VLAN 2
Fast Ethernet 0/0.3	200.0.0.193	VLAN 802.1Q	VLAN 3

c) Configuração do Switch da Estação Central

Tabela 05: Configuração básica das Interfaces do Switch

INTERFACE	ENDEREÇO IP	GATEWAY	VLAN	HOST
Fast Ethernet 0/1	200.0.0.70	200.0.0.65	1	PC - Gerenciamento
Fast Ethernet 0/2	200.0.0.71	200.0.0.65	1	Gravador (NVR)01
Fast Ethernet 0/3	200.0.0.72	200.0.0.65	1	Gravador (NVR)02
Fast Ethernet 0/4	200.0.0.73	200.0.0.65	1	Servidor de Vídeo 01
Fast Ethernet 0/5	200.0.0.74	200.0.0.65	1	Servidor de Vídeo 02
Fast Ethernet 0/6	200.0.0.134	200.0.0.129	2	PC - Workstation
Fast Ethernet 0/7	200.0.0.135	200.0.0.129	2	PC - WorkStation
Fast Ethernet 0/8	200.0.0.136	200.0.0.129	2	PC – Vídeo Wall
Fast Ethernet 0/9	200.0.0.200	200.0.0.193	3	Access Point / Cameras

2.3.8 ASPECTOS DE SEGURANÇA

Rede Ethernet: Considerando que a rede wireless está mais susceptível a ataques e invasões o firewall poderá ser instalado antes da interconexão com a rede Ethernet da Estação Central, local crítico onde as imagens serão analisadas, manipuladas e gravadas.

Rede WIFI: Todos s dispositivos da rede WIFI suportarão a implementação do padrão WPA, possibilitando a troca de chaves utilizando o protocolo TKIP (Temporal Key Integrity Protocol), realizando a autenticação através do padrão 802.1x. A identificação das câmeras IP através de seu endereço MAC também pode aumentar o nível de proteção da rede.

2.3.9 ESPECIFICAÇÕES TÉCNICAS DOS COMPONENTES DA REDE DE COMPUTADORES

a) Access Point / link de rádio

Equipamento Ponto de Acesso (AP) Autônomo com suporte a antenas externas para redes locais de computadores wireless (WLAN) com arquitetura distribuída com as seguintes características técnicas mínimas obrigatórias:

- Tipo autônomo para utilização em redes wireless com arquitetura distribuída;
- Modos de operação Access Point, Repetidor e Bridge Wireless;
- Compatibilidade com os padrões IEEE 802.11a, IEEE 802.11g e IEEE 802.11b;
- Operação nas faixas de frequência licenciadas e não licenciadas de 2,4 GHz (IEEE 802.11b/g) e 5 GHz (IEEE 802.11a);
- Seleção dos canais de transmissão dos rádios IEEE 802.11a e IEEE 802.11b/g por software;

- Operação simultânea nos padrões IEEE 802.11a e IEEE 802.11b/g;
 - Configuração e operação simultânea de um rádio em modo Access Point e outro rádio em modo Bridge;
 - Quando um dos rádios estiver configurado em modo Bridge o Access Point deve operar em modo híbrido para a transferência de frames ethernet tagged e untagged conforme padrão IEEE 802.1Q;
 - Suporte para as seguintes taxas de transmissão: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps e 6 Mbps no padrão IEEE 802.11g; 11 Mbps, 5,5 Mbps, 2 Mbps e 1 Mbps no padrão IEEE 802.11b; 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps e 6 Mbps no padrão IEEE 802.11a;
 - Implementação de Diversity Antennas para transmissão e recepção nos dois rádios;
 - Ajuste de potência de transmissão nos dois rádios por software;
 - Possuir as seguintes sensibilidades de recepção: IEEE 802.11a: -86 dBm ou superior; IEEE 802.11g: -86 dBm ou superior;
 - Possuir as seguintes potências de transmissão: Rádio IEEE 802.11a: +17 dBm ou superior;
 - Rádio IEEE 802.11g: +17 dBm ou superior;
 - Possuir no mínimo Led indicador de *Status ou Activity*;
 - Operar em temperaturas de 0 a 40°C e umidade relativa do ar de 15 a 90% não-condensada;
 - Possuir uma porta Ethernet 10/100BaseT autosensing;
 - Permitir upgrade de firmware;
 - Autenticação em servidor externo (Radius e Tacacs) dos usuários com permissão de acesso administrativo ao Access Point;
 - Permitir armazenamento e recuperação de configurações em servidor externo ao access point;
 - Permitir no mínimo a configuração e a monitoração via interface Web, interface CLI (command line interface) e SNMP;
 - Apresentar estatísticas com o número de clientes associados a cada rádio e a cada SSID e para cada cliente associado informar no mínimo o endereço MAC, endereço IP, SSID e rádio associado, criptografia e autenticação utilizada, taxa de transmissão, nível de potência recebida, tempo da conexão, tempo decorrido desde a última atividade, total de pacotes e bytes transmitidos e recebidos, total de erros de recepção e de transmissão.
 - Apresentar relatório eventos (log) do sistema com no mínimo eventos de atividade do sistema, eventos críticos, alertas, erros e advertências. Permitir colocar o equipamento em modo “debug” para a análise, detecção e resolução de problemas técnicos.
- Implementar criptografia AES em hardware;

Implementar autenticação IEEE 802.1x com suporte para no mínimo os métodos EAP-PEAP (MSCHAPv2), EAP-TLS e EAP-TTLS;

- Permitir a configuração do endereço de no mínimo dois servidores Radius (primário e secundário) para as autenticações IEEE 802.1x para cada SSID;
- Permitir a configuração de no mínimo 16 SSIDs, cada um associado a uma VLAN e com perfis de segurança, autenticação e políticas de QoS independentes;
- Permitir configurar o número máximo permitido de associações de clientes wireless a cada rádio ou a cada SSID;
- Implementar mecanismo de escaneamento da rede wireless para a detecção de Access Points clandestinos;
- Implementar mecanismos para QoS com priorização de tráfego baseado em DSCP;
- Implementar mecanismo para ARP Caching ou ARP Proxy (responder as requisições ARP pelos clientes associados);
- Possuir suporte para SNMP V1, V2 e V3;
- Possuir certificação da Wi-Fi Alliance para IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise e WMM.
- Possuir fonte de alimentação bivolt para operação nas tensões de 127/220 VAC, 60 Hz;
- Possuir suporte para alimentação elétrica via Power Over Ethernet em conformidade com o padrão IEEE 802.3af;

b) Antena OMNI direcional 15 dBi

Especificação Elétrica

- Frequência 2400-2500 GHz
- Ganho 15 dBi
- Polarização Vertical
- Polarização Vertical 8°
- Polarização Horizontal 360°

Especificação Mecânica

- Impedância 50 Ohm
- Max. Input Power 400 Watts
- VSWR < 1.5:1 avg.
- Radiação Omni Direcional
- Conector Integral N-Fêmea
- Comprimento 970mm
- Diâmetro Base 30mm

- Diâmetro Corpo 25mm
- Material Policarbonato / Alumínio
- Temperatura Operação -40° C / 85° C
- (-40° F / 185° F)
- Pig Tail SMA
- Fixador de Antena Até 2,5"
- Resistencia Vento 100Km

c) Antena direcional 24 dBi

Especificação Elétrica

- Frequência 2400-2500 GHz
- Ganho 24 dBi
- Polarização Vertical
- Polarização Vertical 45°
- Polarização Horizontal 360°

Especificação Mecânica

- Impedância 50 Ohm
- Max. Input Power 400 Watts
- VSWR < 1.5:1 avg.
- Radiação Direcional
- Conector Integral N-Fêmea
- Material Policarbonato / Alumínio
- Temperatura Operação -40° C / 85° C
- (-40° F / 185° F)
- Pig Tail SMA
- Resistencia Vento 100Km

d) Switch Gigabit-Ethernet de 24 Portas

- Mínimo de 24 portas Switch Fast Ethernet Switch Gigabit Ethernet 10/100/1000BaseT com conectores RJ 45 diretamente no equipamento;
- Suporte às tecnologias Ethernet, Fast Ethernet, Gigabit Ethernet;
- Todas as portas em par trançado deverão ser auto configuráveis MDI/MDIX dispensando o uso de cabos cross-over ou qualquer configuração para conexão a outro switch;
- Controle de fluxo em full duplex e half duplex;

- Suporte a VLAN 802.1Q e RMON;
- Priorização de tráfego 802.1p;
- Implementação de IGMP Snooping;
- Implementação do protocolo IEEE 802.3X;
- Suporte a fonte redundante;
- Implementação do protocolo Spanning Tree;
- Implementação do protocolo Rapid Spanning Tree (IEEE 802.1w);
- Suporte ao gerenciamento SNMP;
- Configuração através de TELNET e gerenciamento via Web;
- Suporte às MIBs: MIB II, Bridge MIB e RMON MIB;
- Suporte a configuração de endereço IP através de DHCP;
- Suporte à agregação de links possibilitando que no mínimo 2 links Gigabit Ethernet operando como um único link lógico com balanceamento de carga segundo o padrão IEEE 802.3ad;
- Tabela de endereços MAC com capacidade para no mínimo 8000 endereços MAC;
- Deve possuir fonte interna AC bivolt, com seleção automática de voltagem, de 100 a 240 V (50-60 Hz);
- Deve operar nas temperaturas de 0 a 40° C;
- Deve operar na umidade relativa não-condensada de 5 a 90%;
- Deve vir acompanhado do kit para montagem em Rack de 19".

e) Bastidor / Rack

- Quadro frontal e traseiro em chapa de aço bitola 18;
- Com controle de temperatura por termostato com microventiladores e proteção solar (caixa).
- Quantidades de Unidades "U" suficiente para fixação dos equipamentos da Estação Central;
- Com alarme de abertura com aviso remoto e posicionamento da câmera com imagem
- Perfis laterais parafusadas em chapa de aço bitola 18;
- Teto, laterais e tampa traseira em chapa de aço bitola 18;
- Venezianas laterais para ventilação;
- 1 plano móvel com espaçamento universal (EIA 310-D);
- Pintura cinza RAL 7032;
- Segundo plano removível para fixação dos equipamentos;
- Barra com terminais de terra para todos equipamentos.
- Tomadas elétricas 3 pinos
- Tomadas de dados apropriadas

CONSIDERAÇÕES FINAIS E PROJETOS FUTUROS

Ao se trabalhar com redes de computadores como meio de comunicação, inúmeras possibilidades surgem durante o desenvolvimento do projeto. Este trabalho explorou apenas uma dessas aplicações, através da transmissão de vídeo e áudio digitais. A tecnologia de redes tem a grande vantagem de permitir o incremento de novas aplicações e tecnologias, independentemente da complexidade e dimensão do projeto.

Após a implementação, será possível, por exemplo, desenvolver novos mecanismos para análise e gerenciamento da rede, adição de equipamentos móveis para a utilização da rede wireless, como laptops em veículos de rádio-patrolhamento, entre tantas outras aplicações possíveis.

BIBLIOGRAFIA

- BRASIL, Congresso Nacional. **Constituição da República Federativa do Brasil**. Brasília, 1997.
- DAMJANOVSKY, Vlado. **CCTV Networking and Digital Technology**. Editora Butterworth – Heinemann.2005
- FERREIRA, Tércia Maria. **Monitoramento Eletrônico de Logradouros Públicos**. REBESP, Goiânia, 2008
- FILIPPETTI, Marco Aurélio. **CCNA 4.1 – Guia Completo de Estudo**. Visual Books, Florianópolis, 2008.
- KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. Pearson Addison Wesley. São Paulo, 2006.
- PERES, Marcelo. **Sistemas de CFTV Digital**. Guia do CFTV. 24 Set.. 2006. Disponível em <<http://www.guiadocftv.com.br/modules/smartsection/item.php?itemid=17>>. Acesso em 30 abr. 2009.
- PERES, Marcelo. **O que são câmeras IP**. Guia do CFTV. 31 Out. 2008. Disponível em <<http://www.guiadocftv.com.br/modules/smartsection/item.php?itemid=50>>. Acesso em 30 abr. 2009.
- PMMG, Polícia Militar de Minas Gerais. **Diretriz para Produção de Serviços de Segurança Pública N.º1/2002**. Belo Horizonte, 2002.
- SIMÕES, André. **Sistema de Gerenciamento de Circuito Fechado de TV com câmeras IP**. Faculdade de Tecnologia de São Paulo. Disponível em <<http://www.scribd.com/doc/887967/Sistema-de-Gerenciamento-de-CFTV-com-CamerasIP>>. Acesso em 30 mar. 2009.
- SSPDS, Governo do Estado do Ceará. **Edital de Concorrência Pública N°119/2008**. Fortaleza, 2008.
- TANENBAUM, Andrew S. **Redes de Computadores**. 4ª Ed.; Editora Campus. 2003.
- UNDERLINUX. **Tabela de cálculo para distâncias entre antenas**. Disponível em <<http://under-linux.org/f117006-tabela-de-calculo-para-distancias-entre-antenas>>. Acesso em 15 nov. 2009.

GLOSSÁRIO

ADSL. Asymmetric Digital Subscriber Line: Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um modem convencional.

ANSI. American National Standards Institute: Instituto Nacional Americano de Normas.

AP. Access Point: Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

ASCII. American Standard Code for Information Interchange: Código de 128 caracteres (em formato binário) para as letras maiúsculas e minúsculas do alfabeto, algarismos, símbolos especiais, além dos 32 códigos para controles. Cada caractere é representado por um número de 7 bits, em formato binário. Dessa forma, um caractere qualquer desse código, poderá ser estocado em um byte de memória de computador.

Aspect ratio: Relação entre eixos. Refere-se à relação entre largura e a altura da imagem apresentada na tela de televisão ou de cinema. A 'relação entre eixos' atualmente usada é de 4: 3, ou seja, quatro unidades na largura X três unidades na altura. Essa proporção foi escolhida durante os primeiros anos da televisão, quando a maioria dos filmes era de um mesmo formato. Na televisão de alta definição moderna, a proporção de 16: 9 estamos sendo sugeridas para a 'relação entre eixos'.

ATM. Asynchronous Transfer Mode: Sistema de transferência e comutação no qual a informação é aperiódica (i.e., não-periódica), com relação a um tipo qualquer de referência, como por exemplo, o número de telas apresentado por unidade de tempo.

Bit: Contração das palavras 'binary' + 'digit'. Dado elementar para a informação digitalizada, somente podendo assumir os valores '0' ou '1'. A menor parte de um dado (informação) no sistema de notação binário. Um 'bit' será sempre um único '1' ou um '0'. Um grupo de bits, como por exemplo, 8 ou 16 bits, constituem um 'byte'. O número de bits em um byte depende no sistema de processamento em uso. Os tamanhos típicos de bytes são de 8, 16 e 32 bits.

Bitmap. BMP: A descrição de uma imagem, feita pixel por pixel (pixel picture element). Cada pixel constitui um elemento em separado. É também um formato de arquivo de computador.

Bit rate: Velocidade de transmissão de bits, sendo o equivalente digital de largura de banda, o 'bit rate' é medido em 'bits por segundo'. É utilizado para designar a velocidade de transmissão de uma corrente de bits. Quanto mais alta for a 'velocidade de transmissão de bits', tanto maior será a quantidade de informação transmitida.

Bluetooth: Termo que se refere a uma tecnologia de radiofrequência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

Bot: Programa que, além de incluir funcionalidades de worms, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o bot, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam, etc.

Botnets: Redes formadas por diversos computadores infectados com bots. Podem ser utilizados em atividades de negação de serviço, esquemas de fraude, envio de spam, etc.

Byte: Palavra em formato digital, contendo 8 bits, cada um deles sendo '0' ou '1'.

Cable modem: Modem projetado para operar sobre linhas de TV a cabo.

CCD. Charge-coupled Device. Dispositivo de carga acoplada: O dispositivo mais moderno para a transmissão de imagens, que substitui as antigas válvulas eletrônicas. Ao ser inventado, na década de 1970, era previsto inicialmente para uso como dispositivo de memória. É utilizado mais freqüentemente em câmeras, e também em tele-cine, máquinas de fax, scanners, etc.

CCD aperture. Abertura de CCD: A parte da área total de um chip CCD que é sensível à luz.

CCTV. Closed Circuit Television: Circuito Fechado de Televisão. Sistema de televisão destinado a um número limitado de espectadores/usuários, ao contrário dos sistemas públicos de transmissão de TV.

CCTV Câmera: Câmera de CFTV. Unidade contendo um dispositivo de captação de imagens, que gera um sinal de vídeo com a largura de banda básica.

CODEC. Code / Decode: Um codificador e um decodificador, montados num mesmo dispositivo eletrônico, usado para comprimir e descomprimir o sinal digital.

dB Decibel: Logaritmo da relação entre dois sinais (ou valores), geralmente referentes à potência (elétrica, mecânica), mas também a tensão e corrente. No cálculo de potências, o logaritmo é multiplicado por 10 e, no cálculo de tensão e corrente, será multiplicado por 20.

DNS. Domain Name System: Serviço que traduz nomes de domínios para endereços IP e vice-versa.

Duplex: Referência ao sistema de comunicação em que a informação é transportada nos dois sentidos [sistema duplex] . Em CFTV, o sistema duplex é usado para indicar um tipo de multiplexador capaz de executar duas funções simultaneamente, fazendo a gravação e a reprodução no modo multiplex.

Encryption: Redistribuição de uma cadeia de bits de um sinal já codificado digitalmente, num padrão sistemático, destinado a tornar a informação irreconhecível até ser restaurada ou passar através de uma chave de decodificação, devidamente autorizada. É uma técnica utilizada para proteger a informação transmitida através de um canal de comunicação, com a finalidade de evitar que usuários não-autorizados possam interpretar essas mensagens. Poderá ser utilizado na transmissão de voz, vídeo os outros sinais de comunicação.

Firewall: Dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.

Frame. Quadro: Em CFTV, refere-se ao conjunto de linhas que formam a os 'quadros' da imagem na tela de TV. Nos sistemas CCIR/PAL, cada quadro é formado por 625 linhas, e por 525 linhas nos sistemas EIA/NTSC. Tem-se 25 quadros/segundo nos sistemas CCIR/PAL e 30 quadros/segundo, nos sistemas EIA/NTSC.

HTML. HyperText Markup Language: Linguagem universal utilizada na elaboração de páginas na Internet.

HTTP. HyperText Transfer Protocol: Protocolo usado para transferir páginas Web entre um servidor e um cliente (como por exemplo, o browser).

HTTPS: Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

IDS. Intrusion Detection System: Programa ou um conjunto de programas cuja função é detectar atividades mal-intencionadas ou anômalas.

IEEE. Institute of Electrical and Electronics Engineers: uma organização composta por engenheiros, cientistas e estudantes, que desenvolve padrões para a indústria de computadores e eletro-eletrônicos.

ISO. International Standardization Organization: Organização Internacional para Padronização / Normalização.

LAN. Local Área Network: Rede de comunicação de dados para distâncias curtas (tipicamente, no interior de um edifício ou no campus de uma universidade) utilizada na interligação de computadores e dispositivos periféricos através de um sistema de controle padronizado.

LCD. Liquid crystal display: Tela utilizada para a apresentação de textos/gráficos com base em uma tecnologia denominada 'cristal líquido', em que a reflexão ou transparência de uma tela variam em função de diminutas correntes elétricas nela aplicadas. As vantagens das telas de LCD são o baixo consumo de energia (podem ser facilmente alimentadas por baterias) e o preço baixo das unidades produzidas em massa. As desvantagens são os pequenos ângulos do campo de visão, resposta muito lenta (lenta demais para ser utilizada em sistemas de vídeo), invisibilidade no escuro, a não ser se houver iluminação de fundo para a tela, e a dificuldade de reproduzir as cores verdadeiras nessas telas.

Lens. Lente: Sistema óptico utilizado para focalizar determinada cena no dispositivo gerador de imagens de uma câmera de CFTV.

MMS. Multimedia Message Service: Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como, por exemplo: texto, imagem, áudio e vídeo.

MPEG: Padrão usado na compressão de sinais de vídeo apresentados em varredura progressiva e com 'interlace', e com sinais de áudio de alta qualidade, numa larga faixa de relações de compressão. Adotado como padrão de codificação de vídeo/áudio em HDTV e DVC.

P2P. Peer-to-peer: Arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Esse tipo de rede é normalmente implementado via softwares P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados como MP3, jogos, vídeos, imagens, etc.

Pixel. Picture element: A menor unidade visível que é manipulada num arquivo de rastreamento, geralmente uma célula única, em uma malha de números que descreve uma imagem.

Protocol. Protocolo: Conjunto de regras ou convenções específicas relacionadas com o formato e a temporização da transmissão de dados entre dois dispositivos / equipamentos. Procedimento padronizado que deverá ser aplicado e usado por dois dispositivos, para que um possa se comunicar com o outro. Os protocolos de comunicação de dados abrangem aspectos tais como a sincronização, manipulação de erros, transparência e controle de linhas.

Proxy: Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte a internet. Proxies mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na internet, como o ataque a outras redes ou envio de spams.

PTZ câmera: Câmera equipada com os recursos de 'pan' (giro no plano horizontal), tilt (giro no plano vertical) e lente 'zoom'.

Resolution: Valor numérico que indica a capacidade de uma câmera (ou sistema de TV) para reproduzir detalhes da imagem, referente ao número de 'pixels' que podem ser reproduzidos com boa definição.

Scanning. Varredura: O movimento rápido do feixe descrito pelo feixe de elétrons no tubo de raios catódicos de um monitor ou de um receptor de TV. É formatado linha por linha ao longo da superfície foto-sensível, para produzir ou reproduzir a imagem de vídeo. Quando se refere a uma câmera PTZ, esse termo significa o deslocamento dessa câmera no plano horizontal ('panning').

Simplex: Em geral, refere-se aos sistemas de comunicação capazes de transmitir dados (informação) num único sentido. Em CFTV, 'simplex' é usado para indicar uma operação de multiplexação onde somente uma função pode ser executada por vez, p.ex., a gravação ou a reprodução.

SMS. Short Message Service: Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferentemente do MMS, permite apenas dados do tipo texto. Cada mensagem é limitada em 160 caracteres alfanuméricos.

SSH. Secure Shell: Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, etc.

SSID. Service Set Identifier: Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

SSL. Secure Sockets Layer: Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor por meio do uso de criptografia.

Streaming: Em inglês, possui significado similar a "fluxo contínuo". É uma tecnologia que permite a transmissão de áudio e vídeo em tempo real através da rede de computadores. A principal característica de uma transmissão em Streaming é que não é necessário "baixar" o arquivo para reproduzi-lo, o que permite, dentre outras possibilidades, a transmissão de eventos ao vivo.

Twisted-pair. Par trançado: Cabo formado por dois condutores isolados e retorcidos / trançados juntos. Já que ambos os condutores ficam quase igualmente expostos às interferências, o ruído diferencial é sempre mais reduzido.

URL. Universal Resource Locator: Seqüência de caracteres que indica a localização de um recurso na internet, como, por exemplo, <http://cartilha.cert.br/>.

UTP. Unshielded Twisted Pair: Par trançado sem blindagem. Cabo elétrico com um (ou mais) par de condutores de cobre isolados, formado com uma única envoltória. Atualmente é o meio mais comum para trazer o sinal do telefone e dados para o computador 'desktop'.

Video wall: Conjunto de vários receptores de vídeo, dispostos lado a lado que, ao ser visto à distância, se apresenta como uma tela gigante.

VPN. Virtual Private Network: Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a internet) como infra-estrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

WEP. Wired Equivalent Privacy: Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Esse protocolo apresenta algumas falhas de segurança.

Wi-Fi. Wireless Fidelity: Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

WLAN. Wireless Local-Area Network: Refere-se a um tipo de rede que utiliza ondas de rádio de alta freqüência (em vez de cabos) para a comunicação entre os computadores.

WPA. Wi-Fi Protected Access: Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP por causa das suas falhas de segurança. Essa tecnologia foi projetada para, por meio de atualizações de software, operar com produtos Wi-Fi que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

APÊNDICE - LISTA DE EQUIPAMENTOS

EQUIPAMENTO	QTD
Câmera IP Speed Dome	25
Servidor de CFTV	02
Gravador de Vídeo em Rede (NVR)	02
Estação de Trabalho (Desktop PC)	04
Display Wall	01
TV LCD de 42"	01
Access Point Servidor	01
Access Point Cliente	27
Protetor de Surto	26
No-break	26
Amplificador de Áudio	25
Alto Falante (loud Speaker)	25
Fonte de Alimentação para Câmera	25
Armário Abrigo de Campo	25
Bastidor Rack	01
Roteador	01
Switch 24 portas	01
Antena Omni Direcional 15 dbi	01
Antena Direcional 24 dbi	25
Cabo Pig Tail 3 metros c/ conectores	26
Cabo de par trançado 5 metros c/ conect.	26
Teclado de Comando (Joystick)	02
Poste Metálico de 15 metros	25
Software Gerenciamento e Análise CFTV	05
Rádio Transmissor	01