FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
NÚCLEO DE CURSOS SEQÜENCIAIS
CURSO DE FORMAÇÃO ESPECÍFICA EM PROJETO E GESTÃO DE REDES DE COMPUTADORES

www.projetoderedes.kit.net

FASTFOA

Por
Alexandre Batista Domingues
Christian Luis Mansur
Domingos Sávio Alves de Almeida
José Maurício dos Santos Pinheiro
Marcos Leite dos Santos

VOLTA REDONDA
DEZEMBRO/2002

FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
NÚCLEO DE CURSOS SEQÜENCIAIS
CURSO DE FORMAÇÃO ESPECÍFICA EM PROJETO E GESTÃO DE REDES DE COMPUTADORES

FASTFOA

Elaboração de Proposta de Projeto apresentada como requisito parcial da nota da disciplina de Projeto Final.

Por
Alexandre Batista Domingues
Christian Luis Mansur
Domingos Sávio Alves de Almeida
José Maurício dos Santos Pinheiro
Marcos Leite dos Santos

Professores Orientadores
Jorge Maia
Felipe Maia

VOLTA REDONDA
DEZEMBRO/2002

DEDICATÓRIA

"O mundo que construímos como resultado do nível de pensamento que adquirimos até agora, cria problemas que não podemos solucionar no mesmo nível em que os criamos".

Albert Einstein

AGRADECIMENTO

Gostaríamos de agradecer a todos que estão colaborando com desenvolvimento deste projeto de melhorias da rede de computadores do UniFOA: colaboradores, parceiros, e em especial, a nossos Professores e Orientadores.

A evolução cada vez mais rápida da tecnologia reflete as mudanças e os novos horizontes, resultantes da necessidade cada vez maior da utilização de recursos digitais como páginas informativas, listas de discussões, bases de dados, revistas (periódicos) e livros eletrônicos, bibliotecas (eletrônicas, digitais e virtuais), filmes e tantos outros, principalmente para incentivo de pesquisas acadêmicas. Tudo isto significa avanços tecno-científicos em nossa área.

Agradecemos também aos acadêmicos do Curso Seqüencial de Projeto e Gestão de Redes do UniFOA por colaborarem direta e indiretamente, seja com apoio moral, bem como, partilhando novas informações.

RESUMO

Este projeto tem como objetivo principal, sugerir melhorias e a reestruturação das redes de computadores, administrativa e acadêmica, do UniFOA.

A proposta do projeto especifica a utilização de tecnologia de ponta, que vem de encontro com as necessidades da Instituição. Considera os aspectos imprescindíveis dentro dos modernos fatores de aplicação no ensino, preservando o investimento através de sua capacidade de manutenabilidade e escalabilidade.

O desenvolvimento do projeto segue princípios básicos de segurança em sistemas de comunicação compreendendo:

- Velocidade - Garantir a utilização de recursos modernos de comunicação.
- Confidencialidade – proteger a informação disponibilizada.
- Integridade – Garantir que a informação seja autentica e protegendo-a.
- Autenticidade – Garantir a identidade dos usuários.
- Disponibilidade – Prevenir interrupções na operação da rede através de um plano de contingência.

Deste modo espera-se oferecer aplicabilidade aos conhecimentos construídos no decorrer do curso do Projeto e Gestão de Redes de Computadores.

SUMÁRIO

INTRODUÇÃO

Apresentamos o projeto FastFOA de reestruturação das instalações de rede da Fundação Oswaldo Aranha.

O tema FastFOA foi escolhido pelo fato de um estabelecimento de ensino ser um ambiente dinâmico e dar ênfase no contexto da pesquisa voltada para a área educacional.

Informatizar as instituições de ensino, capacitar os profissionais da educação no conhecimento das novas tendências e tecnologias, preparar os alunos, dando-lhes acesso e mantendo-os em contato com recursos modernos é uma necessidade fundamental não só para que estes possam ingressar no mercado de trabalho, mas também para que possam conviver na sociedade moderna em perfeito sincronismo com suas necessidades e realidades.

A metodologia adotada neste empreendimento se pautará em teorias e aplicação de normas de projeto de forma integrada.

Neste sentido, o projeto se propõe, através de uma rede de computadores (servidores e estações clientes), prover conectividade e interoperabilidade comportando os atuais recursos de comunicação existentes, permitindo o intercâmbio entre os diversos setores da instituição, no intuito de permitir a administração e disponibilidade da informação de uma forma centralizada, segura e mais rápida. Inerente ao trabalho, o objetivo é utilizar os recursos tecnológicos da informática para a transferência de conhecimentos teóricos e práticos das tecnologias existentes. Serão abordados os pontos fundamentais que fazem parte da solução para o ambiente atual, considerando os aspectos humanos, físicos e lógicos de funcionalidade e arquitetura deste.

As recomendações existentes neste projeto darão à instituição a base para um ambiente estável e para definir padrões que possam ser aplicadas em curto, médio e longo prazo, possibilitando um crescimento modular e preservando investimentos.

Como beneficio, será oferecido um melhor atendimento aos alunos e melhor agilidade nos serviços internos e administrativos, oferecendo soluções, respostas, esclarecimentos de dúvidas, treinamentos e cursos aos alunos em tempo real. Para que haja disponibilidade dos sistemas em tempo integral, serão propostos planos de contingência

dos servidores e dispositivos da rede. Junto com a implementação da rede, serão propostas outras vantagens tais como:

Intranet, Internet e Laboratórios de Informática.

Com a implementação da rede corporativa, toda a infra-estrutura necessária para a melhoria da Intranet estará pronta e todas as vantagens e benefícios oferecidos através da mesma poderão ser implementados. Cabe assinalar que a sugestão para implementação da Intranet tem apenas efeito ilustrativo, não fazendo parte do escopo do projeto.

Em relação à Internet será disponibilizado maior velocidade de acesso para os diversos usuários da rede (alunos, professores, administradores, etc.).

Os Laboratórios serão revitalizados com a implementação de novos recursos de comunicação.

Conclui-se que a efetivação deste projeto se faz possível devido à experiência profissional de seus autores.

OBJETIVO

GERAL

Ampliar e melhorar os recursos de informação do UniFOA, através da reestruturação física e lógica, utilizando a rede, com novos equipamentos, remanejando os recursos existentes, equipamentos e pessoal da instituição e de suas parceiras.

ESPECÍFICOS

- Contribuir com a melhoria do acesso à Internet para um melhor aproveitamento nas pesquisas acadêmicas, bem como disponibilização de novos recursos (pesquisa de notas, pesquisa de livros, etc.) na rede.
- prover um plano de contingência para garantir a disponibilidade do uso da informação.
- Implementar segmentos distintos para a rede corporativa e acadêmica para possibilitar uma política de segurança mais eficiente.
- Contribuir com novas pesquisas acadêmicas e profissionais na área tecnológica.
- Fornecer uma documentação de referência ao pessoal envolvido com a implantação da rede e à instituição.

FASE 1 - IDENTIFICAÇÃO DAS NECESSIDADES E DAS METAS DOS CLIENTES

DESCRIÇÃO DO NEGÓCIO DA EMPRESA

A Fundação Oswaldo Aranha foi instituída por uma Assembléia Geral, em sessão solene, realizada no edifício da Prefeitura Municipal de Volta Redonda, no dia 18 de outubro de 1967.

Criada para estimular e desenvolver o ensino superior na região do sul do estado de Rio de Janeiro, objetivando a pesquisa técnica e científica, o estudo e desenvolvimento das ciências e a formação de profissionais de nível superior, a Instituição adotou oficialmente a partir de 1995, o Programa de Qualidade elaborado com o objetivo de proporcionar as Unidades de Ensino do CESVRE (Centro de Ensino Superior de Volta Redonda) melhor desenvolvimento de suas práticas educativas com investimentos na melhoria das Instalações, treinamentos na filosofia da qualidade voltada para o ensino dirigido aos professores, colaboradores e alunos novatos e formação de equipes de trabalho para elaboração de procedimentos necessários à solicitação do CESVRE em se tornar um Centro Universitário.

Em 1999, o Conselho Nacional de Educação aprovou através do parecer n.º 867/99 o credenciamento do Centro Universitário de Volta Redonda, sendo homologado pelo Ministro da Educação Professor Paulo Renato de Souza e por ato do Excelentíssimo Senhor Presidente da República, foi credenciado o Centro Universitário de Volta Redonda. O UniFOA começava então a buscar incessantemente a qualidade de suas atividades acadêmicas, que já eram exercidas pelos cursos de Medicina, Odontologia, Engenharia Civil, Educação Física, Ciências Contábeis e Ciência da Computação.

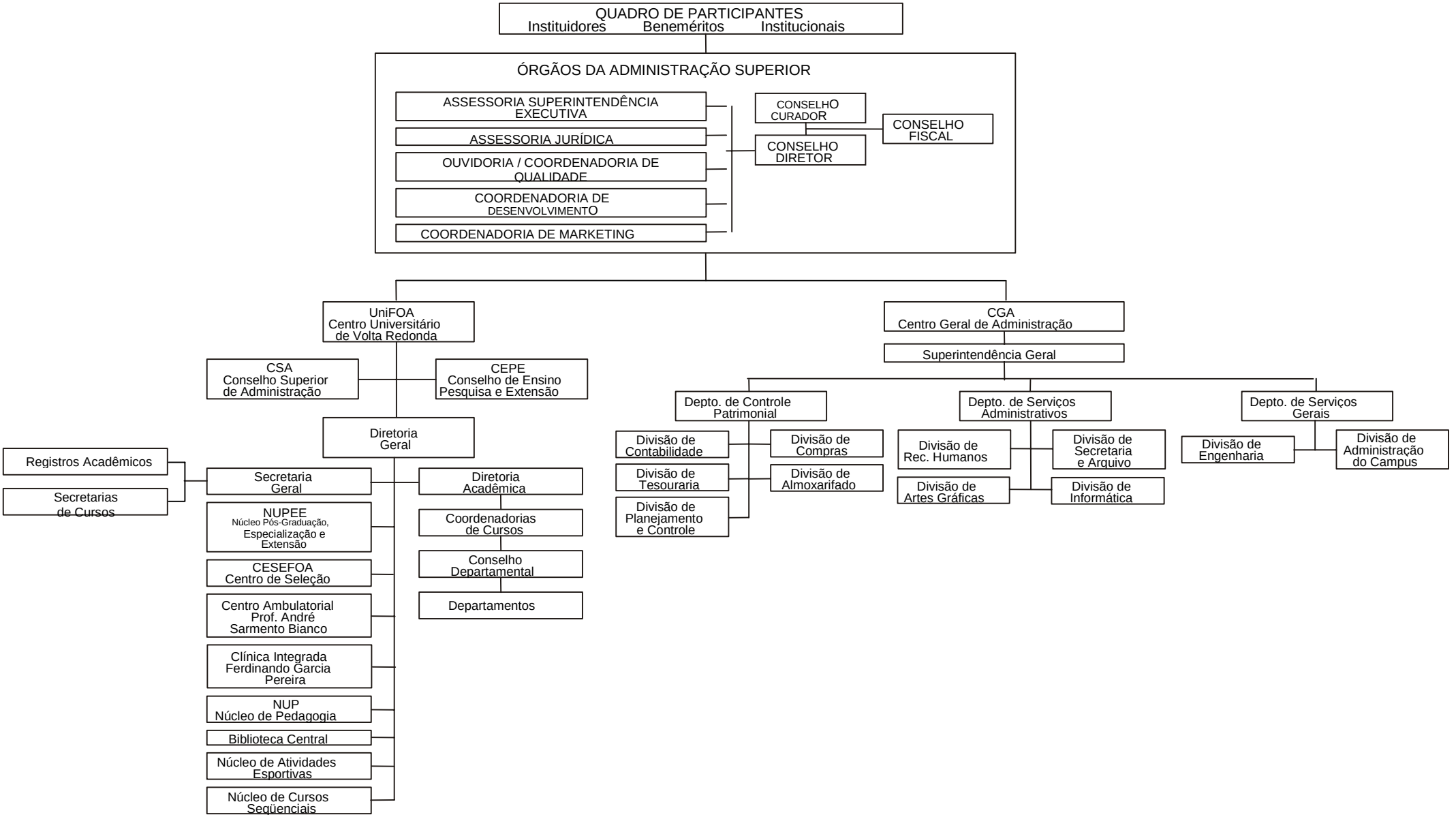
Em sua primeira fase de expansão, o UniFOA abria para o próximo ano letivo, os cursos de Enfermagem e Fisioterapia, além do curso noturno de Educação Física, bem como o primeiro curso de Mestrado em Educação. O Núcleo de Pós-Graduação, Especialização e Extensão e a implantação dos Cursos Seqüenciais com formação específica em 2 anos no ano seguinte enriqueceram ainda mais a instituição, oferecendo uma multiplicidade de cursos do interesse da comunidade regional.

Com o advento do Centro Universitário, a Instituição ampliou seu espaço físico, investiu em hardware, software e peopleware para receber os novos cursos. Novas instalações como o Anexo ao Hospital São João Batista, os dois Campus avançados com destaque para a Clínica Integrada do Campus Aterrado, as instalações do Campus Vila (Tangerinal), a Biblioteca Central com atendimento ao corpo discente por meio de salas de Internet, consulta a acervo e periódicos via quiosque e via Internet com reserva on-line, na qual o aluno poderá efetuar sua reserva de volume do acervo bibliográfico de qualquer browser Internet e os sete Laboratórios de Informática que atendem os alunos dos 36 cursos do UniFOA, a Mantenedora oferece à comunidade regional, serviços a baixo custo executados pelos alunos com acompanhamento direto dos professores.

Com o crescimento da Internet, a Instituição disponibiliza todas as suas informações para os internautas que a visitam pelo endereço http://www.foa.org.br assim como recebe inscrições para o processo seletivo de todas as regiões do Brasil em seu site. Propiciando conforto, agilidade e segurança aos candidatos ao processo seletivo, tanto no preenchimento de um formulário com validações de informação quanto na emissão de boleto bancário com código de barras tão eficiente quanto o da Instituição Bancária que o receber, e emissão do cartão de confirmação de inscrição, liberado mediante pagamento do boleto bancário, só liberado após a Instituição Bancária informar o pagamento efetuado pelo cliente. Todo o processo de inscrição, bem como a classificação e reclassificação dos candidatos, podem ser verificadas no próprio browser cliente, as informações ficam armazenadas em servidor com banco de dados Oracle, que quando solicitadas pelo cliente através de páginas dinâmicas, chegam com a segurança de dados confiáveis.

A utilização da Intranet é um ponto explorado a cada dia com mais intensidade pelo UniFOA, com um sistema de notícias denominado ViaNet, todos os colaboradores da Instituição podem enviar notícias, através de um formulário a ser preenchido via browser, o seu conteúdo passa por triagem na Divisão de Comunicação que analisa a informação e autoriza a exibição em todas as estações de trabalho dos colaboradores. Logo que o usuário conecta na rede UniFOA, a primeira tela a aparecer é a de notícias corporativas. Existe também, uma página de apoio a Clinica Integrada com consultas sobre débitos de seus pacientes, um terminal de consulta rápida para os colaboradores do – CESEFOA - Centro de Seleção, com dados de inscrições dos candidatos aos processos seletivos e uma página que disponibiliza todos os ramais da Mantenedora.

ORGANOGRAMA DA INSTITUIÇÃO



DETERMINAÇÃO DOS CRITÉRIOS DE SUCESSO

Tendo em vista que o link de comunicação de dados do UniFOA não está suportando o elevado tráfego de dados, que sua estrutura atual não permite a utilização de serviços como videoconferência, acesso simultâneo de uma grande quantidade de usuários, bem como a comunicação satisfatória com as escolas externas ao Campus principal e que estes serviços se tornam necessários à instituição assim como a utilização dos sistemas já existentes que tratam da vida acadêmica de seus alunos.

Ainda para o usuário acadêmico é necessária uma velocidade de acesso que comporte tanto pesquisas nacionais e internacionais como também pesquisas as demais atividades acadêmicas como videoconferência, correspondência eletrônica etc. simultaneamente.

Para o usuário corporativo faz-se necessário maior segurança para o tráfego de informações essenciais e prioritárias. tráfego de dados mais estável sem gargalos disponível 24 x 7.

Uma melhoria na velocidade de trafego de informações seria facilmente perceptível por todos os usuários. Da mesma forma, erros nas configurações ou no dimensionamento das modificações propostas pelo projeto seriam facilmente detectados, pois haveria queda na performance e consequentemente um atraso no tráfego das informações pela rede. Uma vez que este fato ocorra, toda a instituição sofreria com a perda de competitividade perante as suas concorrentes na região decorrentes da queda da receita e atraso no cumprimento de suas obrigações acadêmicas, tributárias e comerciais.

DETERMINAÇÃO DAS METAS DE NEGÓCIOS ASSOCIADAS AO PROJETO

O projeto FastFOA visa melhorar as comunicações da instituição de maneira a oferecer novos serviços aos seus clientes (alunos) e colaboradores, tais como, videoconferência, acesso mais rápido à Internet, voz sobre IP e outros serviços disponibilizados no seu Web site, como terminal acadêmico e consulta ao acervo da biblioteca do Campus.

No meio acadêmico a videoconferência pode ser usada como uma ferramenta alternativa para o ensino e aprendizagem, através de programas para o ensino a distância. Através dela, as escolas, universidades e bibliotecas podem compartilhar dados e interagir através do intercâmbio de informações, como na realização remota de aulas e palestras. A troca de experiências entre professores e alunos à grandes distâncias, pode ser realizada, tal como se estivessem juntos em um mesmo local.

Esta tecnologia possibilita que pessoas, distantes umas das outras, possam se comunicar através de um simples computador pessoal, criando assim, um novo conceito de meio de comunicação, com uma interatividade muito maior da oferecida pelos meios convencionais, tais como o e-mail, canais de bate-papo ou telefone

Através de uma melhor distribuição dos equipamentos que a instituição possui e com a aquisição de novos aparelhos, será possível utilizar ferramentas de trabalho que tornarão os serviços mais fáceis e mais rápidos ampliando assim os recursos educacionais mantendo assim um ensino de qualidade e possibilitando a criação de novos cursos e atraindo novos alunos.

O acesso rápido às informações é extremamente importante tanto na área acadêmica quanto na área corporativa, pois um aumento na qualidade de comunicação e o acesso às informações as decisões de negócio serão mais rápidas e seguras.

DETERMINAÇÃO DO ESCOPO DO PROJETO DA REDE

O UniFOA possui uma WAN, formada pelos sites do Campus Universitário de Três Poços, Campus Aterrado (Odontologia) e Campus Tangerinal (Ciências Contábeis, Direito e NUPEE), todos na cidade de Volta Redonda, que se interligam por meio de LPCD's (Linhas Privativas de Comunicação de Dados), de 64kbps, contratados da concessionária de Serviços Públicos local (Telemar).

O Campus Três Poços possui uma CAN formada pelas diversas LANs, existentes em seu perímetro interno, que são interligadas por meio de fibras óticas.

Os Campus Aterrado e Tangerinal possuem LANs e são auto-suficientes em toda infra-estrutura, tais como, servidores de arquivo, de impressão e de autenticação de rede. Sendo que os dados dos sistemas acadêmico e financeiro são atualizados periodicamente, com a base de dados do Campus Três Poços, através do link de 64Kbps, que também é utilizado para prover acesso à Internet. Isto causa algumas vezes degradação na performance da rede.

Com relação ao acesso à Internet, o projeto propõe que se faça uma tomada de preços no mercado e seja contratada uma empresa que possibilite um melhor custo/benefício por byte trafegado, com uma boa qualidade sobre serviços. Deverá ser contratado um link de 1Mbps e o link atual de 384Kpbs será remanejado para o Campus Tangerinal de maneira a substituir a atual conexão de 64Kbps, que existe no site onde se concentra a maior atividade de cursos fora do Campus universitário, possibilitando a melhor integração dos sistemas.

Com a liberação deste link de 64Kbps, também será possível a interligação das instalações do Anexo UHG, que atualmente está isolado, dificultando até a manutenção que alguns casos pode ser feita remotamente.

IDENTIFICAÇÃO DOS APLICATIVOS DA REDE

Nome do Aplicativo	Tipo do Aplicativo	Novo Aplicativo	Nível de Importância	Comentários
Protheus	Sistema de Controle Administrativo	Não	Crítico	
SAGRES	Sistema de Controle Acadêmico	Não	Crítico	
MailSite	Sistema de Correio Eletrônico	Não	Crítico	
IIs	Servidor Web	Não	Extremanente Crítico	Será preparado um servidor de back up.
Pacote Office	Aplicativos	Não	Médio	
Outlook	Correio eletrônico	Não	Médio	
Odonto Way	Sistema de Controle Odontológico	Não	Médio	
Portaria	Sistema de Controle de Veículos	Não	Baixo	
Vestibu	Sistema Emissão de Cartões do Vestibular	Não	Médio	
JuriSíntese	Sistema de Controle de processos Jurídicos	Não	Médio	
Telefonia	Sistema de Controle de Telefonia	Não	Médio	

RESTRIÇÕES DOS NEGÓCIOS

Por se tratar de uma Fundação sem fins lucrativos e com recursos limitados, o UniFOA determina que o projeto deve ser elaborado de maneira a aproveitar grande parte dos recursos ou equipamentos existentes na empresa e adquirir o estritamente necessário.

É política da Fundação Oswaldo Aranha realizar cotações de preços para todas os produtos e serviços contratados, não havendo compromissos com fornecedores.

Dessa forma, a empresa que apresentar a melhor proposta dentro das condições apresentadas será escolhida.

Tratando-se de um serviço que deverá atender toda a instituição e sem remoção de nenhum posto de trabalho não deverá portanto sofrer nenhuma repressão.

A proposta da empresa, que se propuser a disponibilizar o serviço, não deverá ultrapassar o orçamento atual, possibilitando assim um melhor custo / benefício.

Atualmente na instituição não existe padrões pré determinados de marcas e fabricantes apenas recomendações para equipamentos de qualidade e de maior interoperabilidade para garantir um melhor aproveitamento por mais tempo.

CRONOGRAMA

DETERMINAÇÃO DAS METAS DE ESCALONAMENTO DA REDE

As instalações de rede atual não apresenta condições de crescimento. Para tanto, serão necessárias intervenções visando a reestruturação da infra-estrutura existente.

O Projeto, após implantado, possibilitará e facilitará o crescimento da rede, uma vez que, através de uma melhor distribuição dos recursos existentes disponibilizará mais conexões, aumentando assim os seguimentos hoje existentes e a criação de outros novos com a mesma capacidade.

O Site Tangerinal utiliza um link e 64kbps que não é suficiente para suportar o tráfego de dados atual. Com a contratação do link de 1Mbps para o acesso à Internet, substituiremos os 384Kbps existentes atualmente que será remanejado para Site Tangerinal. Criaremos assim condições para que seja expandida sua capacidade de estações, que também terá mais um Hub instalado aumentando o número de portas disponíveis.

Com a futura aquisição de um Switch de nível 3 para o backbone central UniFOA, pretende-se dar condições também para criação novos sites dentro do Campus, como novos prédios e cursos que são previstos para os próximos anos.

DETERMINAÇÃO DAS METAS DE DISPONIBILIDADE DA REDE

O link principal de comunicação do UniFOA não possui redundância. Isso é um fato preocupante se considerarmos que a maior parcela das inscrições para o processo seletivo é realizado via Internet, dependendo assim da utilização dos recursos da Web para proporcionar um maior alcance e comodidade aos candidatos.

O servidor Web também é um ponto crítico, tendo em vista que, o mesmo não possui redundância.

A proposta então, é preparar um servidor de back up, para que em caso de pane ele possa ser rapidamente substituído, tendo assim um bom nível de recuperabilidade e os danos de inoperância sejam os menores possíveis.

Quanto ao link principal de comunicação será consultada também a proposta das empresas que se dispuserem a prestar o serviço para a implementação de redundância.

Dentro das propostas deverão também ser analisados os tempos máximos aceitáveis de inoperância e recuperabilidade.

Para pequenas panes de energia os servidores e equipamentos principais de comunicação estão protegidos por no-break. No caso de uma pane mais prolongada será utilizado os recursos de um gerador já adquirido e instalado pela própria instituição em breve, dando assim uma maior garantia de disponibilidade para a rede e servidores críticos.

DETERMINAÇÃO DAS METAS DE SEGURANÇA DA REDE

Hoje, o sistema de autenticação é baseado em Windows NT 4.0, não tendo limite mínimo para o tamanho das senhas, e não existe política de troca de senhas, ou seja, elas nunca expiram. Sendo assim pretende-se criar para o novo projeto uma política de troca mensal de senha.

O sistema atual de detecção de intrusos se baseia apenas na segurança nativa do NT, que recusa o login do usuário após um determinado número de tentativas e registra o fato em um arquivo de log. Com a criação de uma DMZ e a instalação de um IDS daremos à nova rede mais segurança de maneira que, com o servidor Web estando nesta DMZ os acessos externos não entrarão na rede interna.

A política de backup da rede é baseada na cópia diária das pastas principais e do banco de dados acumulado durante uma semana. É mantida uma copia mensal, e após doze meses é acumulada uma fita anual. Vale ressaltar que todo processo se dá de forma manual e que se usa o utilitário de backup do próprio sistema.

O antivírus instalado é o Norton Corporate, que está instalado em um servidor de aplicação e serve também como servidor de atualização para as estações onde é instalada a versão cliente do antivírus. Sendo assim uma vez que o servidor é atualizado, replica-se automaticamente esta atualização para as estações.

Não existe política de verificação de conteúdo das pastas depositadas nos servidores, valendo apenas o bom senso no que diz respeito ao tamanho dos arquivos ou quantidade de material armazenado.

O sistema de Firewall atual é baseado em um servidor rodando Windows NT Server com três placas de rede instaladas, nelas encontram-se os seguimentos de rede administrativo, acadêmico e a conexão com a Internet. Esse servidor roda um produto de roteamento e Firewall da Tiny Software que permite a segurança do acesso às redes por meio de configurações de permissão de passagem de pacotes para determinados destinos e negação de pacotes nocivos.

A fim de economizar banda de Internet reduzindo o acesso a páginas freqüentemente visitadas, é utilizado um servidor de Proxy. Nesse servidor também aproveita-se para negar a visita a páginas de conteúdo impróprio. É feito isso tanto a nível acadêmico quanto administrativo.

DETERMINAÇÃO DAS METAS DE GERENCIAMENTO DA REDE

A necessidade de qualidade, a diversificação e a complexidade cada vez maior dos serviços de rede implica em uma necessidade tão vital quanto o próprio serviço: a sua gerência.

A rede do UniFOA ainda não possui um gerenciamento adequado, sendo que a Instituição não tem nenhum software para controle de tráfego da rede, o que possibilitaria um melhor controle do desempenho e segurança com atuação sobre possíveis falhas que seriam detectadas com antecedência.

Devido a grande quantidade de equipamentos de diferentes marcas, e ausência de Switches gerenciáveis, será feito um estudo para definir qual software mais adequado para fazer a gerência de rede com um Switch gerenciável que será adquirido e instalado no backbone central da rede.

A interligação de todas as estações da rede facilitará um gerenciamento mais adequado. Será proposto a instalação de software de gerenciamento para o monitoramento constante de utilização, bem como as falhas, desempenho e segurança.

A configuração em algum caso poderá ser feita também remotamente diretamente da central de gerenciamento, com o auxílio de softwares específicos a serem instalados no novo projeto.

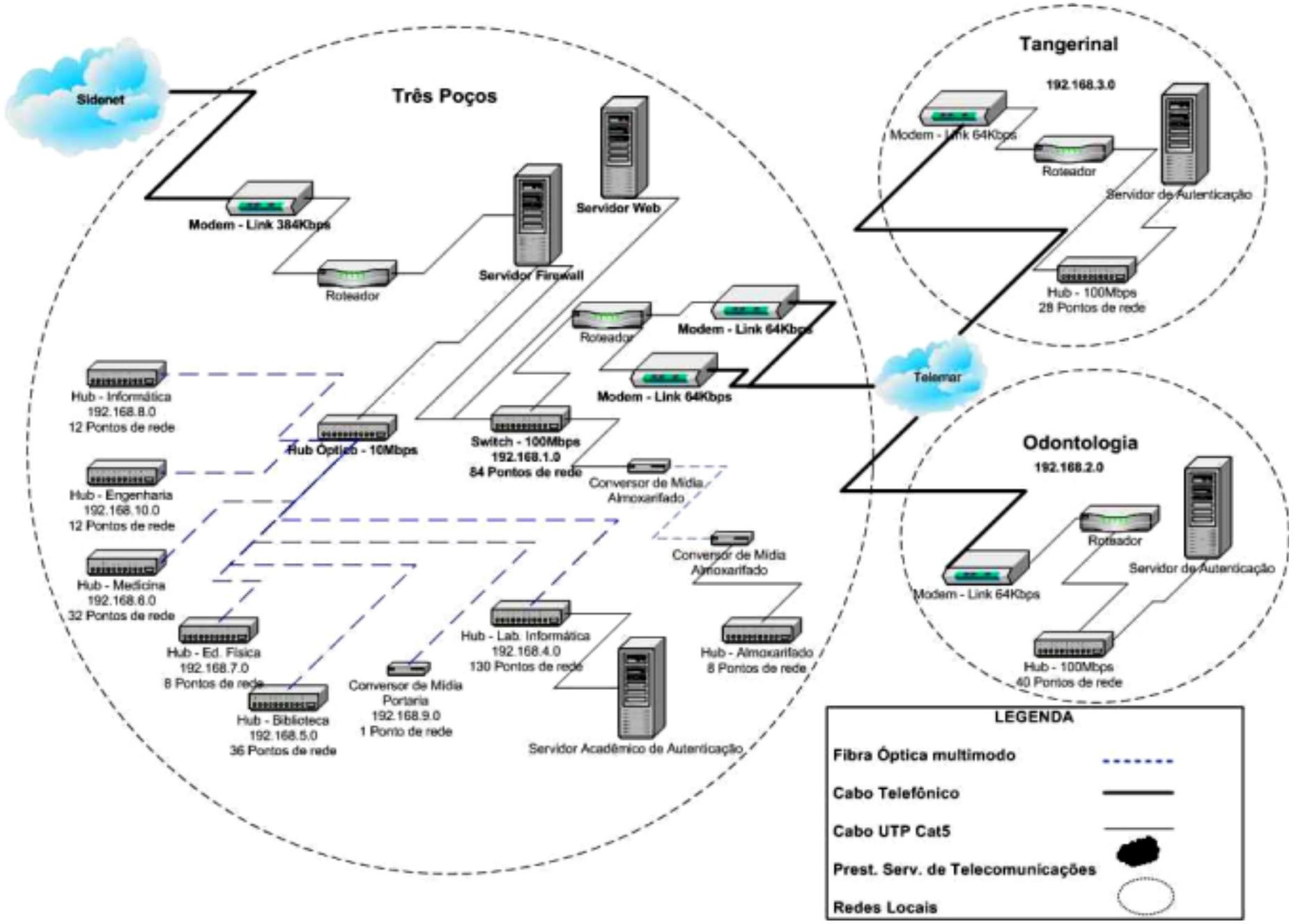
DETERMINAÇÃO DAS METAS DE FACILIDADES DE USO DA REDE

Para facilitar os serviços de configuração das estações e devido à imensa movimentação das mesmas, utiliza-se o serviço de endereçamento de IP dinâmico por meio de DHCP. Apenas algumas estações que desempenham funções mais específicas, como, por exemplo, servidores de impressão e os servidores principais, trabalham com endereços IP fixos. A resolução de nomes que facilitam tanto o acesso interno, como aos sites da Internet, fica a critério dos serviços de WINS e DNS que estão ativos em diferentes servidores para balanceamento de carga.

O serviço de DNS atual é baseado no Windows NT sendo que em alguns momentos esse serviço deixa de responder as solicitações das estações. Para solucionar tal problema implantaremos um servidor de DNS baseado em LINUX tornando o serviço mais estável.

A implementação de novos recursos, usuários e políticas de segurança mais rigorosas que normalmente tende a reduzir as facilidades de uso da rede, portando propõe-se que seja feito o mais transparente possível para o usuário com a implementação de recursos velozes e automáticos facilitando além da usabilidade a gerenciabilidade.

MAPA DA REDE EXISTENTE


Sidenet
Três Poços
Modem - Link 384Kbps
Roteador
Servidor Firewall
Servidor Web
Roteador
Modem - Link 64Kbps
Modem - Link 64Kbps
Hub - Informática
192.168.8.0
12 Pontos de rede
Hub Optlink - 10Mbps
Switch - 100Mbps
192.168.1.0
84 Pontos de rede
Conversor de Mídia
Almoxarifado
Hub - Engenharia
192.168.10.0
12 Pontos de rede
Conversor de Mídia
Almoxarifado
Hub - Medicina
192.168.6.0
32 Pontos de rede
Hub - Ed. Física
192.168.7.0
8 Pontos de rede
Hub - Lab. Informática
192.168.4.0
130 Pontos de rede
Hub - Almoxarifado
8 Pontos de rede
Conversor de Mídia
Portaria
192.168.9.0
1 Ponto de rede
Hub - Biblioteca
192.168.5.0
36 Pontos de rede
Servidor Acadêmico de Autenticação
Telemar
Tangerinal
192.168.3.0
Modem - Link 64Kbps
Roteador
Servidor de Autenticação
Hub - 100Mbps
28 Pontos de rede
Odontologia
192.168.2.0
Roteador
Servidor de Autenticação
Modem - Link 64Kbps
Hub - 100Mbps
40 Pontos de rede
LEGENDA
Fibra Óptica multimodo
Cabo Telefônico
Cabo UTP Cat5
Prest. Serv. de Telecomunicações
Redes Locais

CARACTERIZAÇÃO DO ENDEREÇAMENTO E NOMENCLATURA DA REDE EXISTENTE

Toda a rede está baseada no protocolo TCP/IP com endereçamento e máscara de rede classe C.

A opção por utilizar o TCP/IP é devido a sua grande flexibilidade e interoperabilidade. Podendo adaptar-se a uma grande variedade de equipamentos e tecnologias de redes existentes hoje e também futuras. Facilitando dessa forma o novo projeto FastFOA.

Cada prédio no Campus determina um segmento de rede com máscara 255.255.255.0. Os endereços utilizados são reservados para uso interno e para o acesso à Internet é usado o serviço de NAT no Firewall para conversão dos mesmos.

O protocolo utilizado nos roteadores é o RIP, devido à sua fácil implementação devendo ser aproveitado para o futuro projeto que prevê a implementação de videoconferência e voz sobre IP.

CARACTERIZAÇÃO DO CABEAMENTO DA REDE EXISTENTE

O sistema de cabeamento existente é composto por cabos metálicos em par trançado e fibra óptica multimodo, que suportam aplicações de voz e dados.

No interior de cada prédio do Campus e nos prédios dos sites distantes, a rede física está baseada no modelo de cabeamento estruturado desenvolvido pela EIA/TIA 568-B e ISO 11801, em par trançado, categoria 5. O cabeamento do backbone do Campus de Três Poços utiliza fibra óptica multimodo 62,5/125 micrômetros, em conformidade com o padrão EIA 492-AAAA. A tecnologia implantada na rede é a Ethernet e a topologia da rede física é em estrela hierárquica, com a instalação de painéis de conexão em cada prédio do Campus e nos sites distantes.

Os prédios do Campus de Três Poços são conectados ao backbone do UniFOA por cabos de fibra óptica multimodo 62.5/125 micrômetros, encaminhados através de tubulação subterrânea, terminando em estruturas modulares (racks) e interligados através de roteadores e hubs instalados em Salas de Equipamentos. Todas as conexões do backbone estão centralizadas na administração, local onde se encontram o núcleo da rede local do Campus e os demais equipamentos de comunicação da rede do UniFOA.

A técnica de conexão adotada para os componentes ativos e passivos da rede não está padronizada. Na administração usa-se a técnica de conexão cruzada, onde o cabeamento dos equipamentos do backbone é terminado em painéis de conexão (patch panels), sendo utilizados cordões de manobra (patch cords) entre eles para a conexão dos equipamentos da rede. Os demais prédios mesclam as técnicas de conexão cruzada e de interconexão, ou seja, em alguns casos os cabos terminados em um painel de conexão são interligados diretamente aos equipamentos por um cabo de manobra. Em todos os casos, esse cabo de manobra também não está padronizado e são utilizados cabos com comprimentos e cor de capa externa variáveis. O cabeamento horizontal de cada prédio é constituído por cabo UTP CAT 5 e terminações em conformidade com o padrão EIA 568-B. Entretanto, alguns segmentos encontram-se fora de conformidade com a norma, utilizando materiais não homologados ou desrespeitando os padrões de instalação para os segmentos da rede.

O novo projeto contemplará o acerto das não conformidades de cabeamento, mantendo assim uma maior padronização.

RESTRIÇÕES DO AMBIENTE EXISTENTE

O ambiente hoje existente para os servidores da rede é suficiente para a estrutura montada. Os equipamentos se localizam em uma sala dotada de aparelho de ar condicionado, bem iluminada, com rede elétrica estabilizada e aterrada.

O espaço disponível é também suficiente para acomodar com praticidade novos equipamentos e o acesso a eles.

A sala possui uma localização estratégica, que possibilita uma fácil abordagem de cabos, tanto internamente ao prédio, como externamente.

para todo o cabeamento externo utiliza-se fibra óptica para evitar possíveis interferências e devido à distância dos pontos.

Caso no futuro seja necessária a utilização de comunicação wireless ou infra vermelho não existe dentro Campus restrições geográficas para essa tecnologia.

ANÁLISE DA DISPONIBILIDADE DA REDE EXISTENTE

Numa instituição do porte da FOA e por suas atividades educacionais torna-se imprescindível uma disponibilidade de suas atividades de comunicação constante.

A inexistência hoje na Instituição de equipamentos e planos de contingência como também redundâncias de rotas faz com que as quedas e paralizações da rede sejam freqüentes.

De acordo com os logs existentes foi notado períodos de indisponibilidade da rede, motivada também pela falta de energia elétrica resultando na queda dos servidores e demais equipamentos críticos do backbone central.

Recentemente houve uma queda no link de comunicação com a Internet devido a um acidente envolvendo a rede aérea da Telemar. Queda essa que durou quase 24 horas, causando vários problemas à Instituição.

Freqüentes paralizações também acontecem pela falta de equipamentos back up's e monitoramento constante 24 x 7.

IDENTIFICAÇÃO DAS PRINCIPAIS ORIGENS DO TRÁFEGO DA REDE EXISTENTE

Nome do grupo de Trabalho	N.º de Usuários	Localização	Aplicativos Utilizados
Labinfo	115	Laboratório de informática	Tráfego de Internet
FOA	7	Biblioteca Central	Sagres
FOA	15	Curso da Ciência da Saúde	Sagres
FOA	8	Site Tangerinal	Sagres
FOA	10	Site Odontologia	Tráfego de Internet

Obs. Toda a rede é baseada no protocolo TCP/P

IDENTIFICAÇÃO DOS PRINCIPAIS LOCAIS DE ARMAZENAMENTO DA REDE EXISTENTE

Local de Armazenamento dos Dados	Localização	Aplicativo(s)	Usado(s) pelo Grupo de Trabalho
Servidor de BD	CPD	BD Oracle	Compras, Almox., Contabilidade, Tesouraria.
Servidor de BD	CPD	BD SQL	Secretaria Geral, Secretarias de Curso e Biblioteca.
Servidor de Arquivos	CPD	MS Office	Todos os Depts.

FASE 2 - PROJETO DA REDE LÓGICA

TOPOLOGIA

A rede atual possui uma estrutura Collapsed Backbone (conexão estrela), usando uma topologia Hub-and-Spoke.

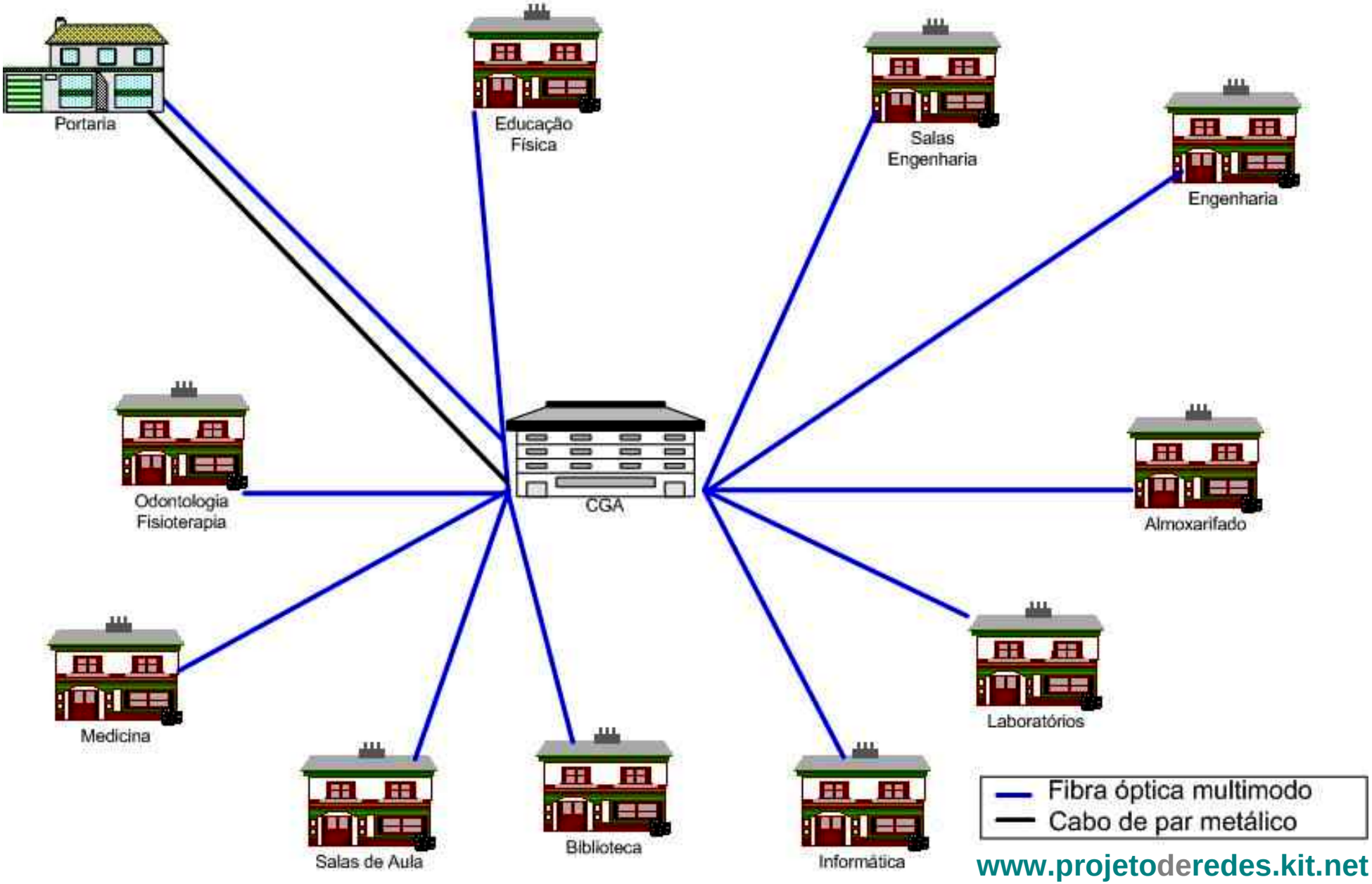
Não existem rotas alternativas entre os sites da instituição, por questão de redução de custos, a única rota que dispõe de redundância é a conexão com a Internet. Dentro do Campus Universitário existem fibras óticas reserva, em todas as conexões entre prédios, o que garante alguma segurança em caso de problema em um dos pares. Todas estas fibras óticas são subterrâneas, o que também garante alguma segurança, porém, se houver algum acidente com rompimento das fibras, o prédio correspondente ficaria sem comunicação.

A proposta então, é a aquisição de switches gerenciáveis e migrar para um modelo hierárquico de 3 camadas, de maneira a melhorar e facilitar as mudanças, já que torna-se mais simples as interconexões e a replicação de elementos, e também para minimizar custos. A topologia proposta será a mesh parcial para que se tenha maior disponibilidade em caso de queda dos links.

O processo seletivo acontece duas vezes ao ano, e é totalmente dependente do serviço de Web, propõe-se uma rota alternativa de saída para a Internet, ficando assim garantida a acessibilidade a pagina.

Gostaríamos de propor também, que seja contratado como medida de segurança um serviço de hospedagem de servidor, para os servidores de Web e Banco de Dados a fim de garantir a disponibilidade da Pagina Web, mesmo em caso de queda do link do Campus Universitário. Desta forma ficaríamos com uma cópia da pagina publicada em um Site seguro assim com uma cópia do Banco de Dados. Estas atualizações poderiam ser feitas de forma automática no período da noite, aproveitando o próprio link de Internet que neste momento tem pouca utilização.

Topologia do cabeamento do campus de Três Poços



PLANO DE ENDEREÇAMENTO

O plano de endereçamento de rede segue um Modelo Estruturado utilizando endereços de classe “c” reservada. É utilizada somente uma máscara de rede (255.255.255.0) e os endereços a partir do endereço 192.168.0.0 que garantem uma quantidade significativa de endereços de rede e de host.

Os servidores de rede, de impressão e algumas estações que possuem funções específicas, estão configurados com endereços de rede estáticos, já as demais estão utilizando endereçamento dinâmico através de um servidor de DHCP.

Como a rede possui classe de endereçamento IP reservado é utilizada a tradução para endereço real (NAT) por meio de software de tradução instalado no Firewall, proporcionando maior segurança, não divulgando os endereços internos da rede.

A estrutura de endereçamento não sofrerá mudanças.

A proposta é que seja configurado um servidor de DHCP de backup, de maneira que em caso de falha de um dos servidores a rede não fique inoperante.

Que a administração da rede seja feita de forma centralizada, à partir da Divisão de Informática, já que este é o backbone central da rede deve ser instalado também um Switch gerenciável que ajudará a segmentar melhor a rede e identificar os pontos de maior tráfego.

Tabela de Endereçamento	
Endereços reservados*	**192.168.1.1 à 192.168.1.30**
Endereços DHCP	**192.168.1.31 à 192.168.1.137**
Endereços DHCP backup	**192.168.1.138 à 192.168.1.254**

* Obs. Os endereços reservados serão subdivididos da seguinte maneira:

192.168.1.1 à 192.168.1.15 reservado a servidores

192.168.1.16 à 192.168.1.20 reservado para servidores de impressão

192.168.1.21 à 192.168.1.30 reservado para equipamento de rede (roteadores, switches, hubs etc.)

PROTOCOLO DE ROTEAMENTO

Encontramos na rede da UniFOA atualmente o seguinte cenário: Roteadores utilizando o protocolo PPP (Point to Point Protocol) e tabelas de roteamento estáticos. Esta estrutura atende as necessidades atuais da rede, mas para usufruir dos benefícios dos serviços de voz sobre Ip (VoIP) e videoconferência propostos neste projeto, se faz necessária a implantação de protocolos de roteamento dinâmico.

Os protocolos de roteamento interno existentes são o OSPF (Open Shortest Path First) e o RIP (Routing Information Protocol). O protocolo OSPF apresenta varias vantagens sobre o protocolo RIP sendo um protocolo hierárquico, baseado no algoritmo de Estado de Enlace (Link-State) e especificamente projetado para operar com redes grandes. Tem como desvantagens o fato de ser muito complexo e exigir muito do hardware.

O protocolo de roteamento escolhido para este projeto é o RIP (Routing Information Protocol). A escolha recai sobre este protocolo devido a sua facilidade de implementação, baixa utilização de processamento nos roteadores e os bons resultados obtidos em redes de pequeno porte, alem de ser implementado pela grande maioria dos roteadores o que permite o aproveitamento dos roteadores existentes.

IMPLEMENTAÇÕES ADICIONAIS NA TOPOLOGIA DA REDE

Tecnologias atuais como VLAN'S, protocolo Spanning Tree (IEEE 802.1d) e outras adicionais não se aplicam ao escopo do projeto FastFOA. Porém, todos os equipamentos adquiridos já possibilitam estas melhorias, podendo as mesmas serem implantadas futuramente.

Segue um exemplo de um dos equipamentos que possibilita atender as futuras melhorias citadas acima:

Switch PowerConnectTM 3024

Especificações:

- Capacidade de Switching 12,8 Gb/s
- Taxa de Encaminhamento 9,5 Mpps
- Portas 10/100BaseT 24 portas RJ-45, IEEE 802.3/802.3u
- Portas 10/100/1000BaseT 2 portas RJ-45, IEEE 802.3ab
- Fibra Óptica: 2 slots GBIC (Obs: os slots GBIC são utilizados em vez das portas 10/100/1000BaseT integradas)
- Portas de Empilhamento Gigabit: 144 portas Fast Ethernet por pilha
- Número Máximo de Endereços MAC : 8,000
- Auto-Negociável: Velocidade, modo duplex e controle de fluxo, exceto nas portas GBIC
- Auto MDI/MDIX: Sim
- Rede Local Virtual (VLAN): Tagging IEEE 802.1Q, até 256 VLANs por porta
- Classe de Serviço: Tagging IEEE 802.1p e prioridade baseada em portas, Suporte a IP Multicast: IGMP snooping
- Disponibilidade: Spanning Tree, Agregação de Link IEEE 802.3ad e espelhamento de portas
- Gerenciamento: Baseado na Web, Console/Telnet; SNMPv1, 4 grupos RMON, múltiplas MIBs
- Gabinete: 1U de altura, com kit para montagem em rack incluso.

PROJETO DA SEGURANÇA DA REDE

Identificação dos Ativos da Rede

Devido a grande quantidade de ativos na rede do UniFOA , o escopo do projeto visa analisar somente os ativos referentes às melhorias efetuadas nos backbones central e demais sites, sendo os mesmos descritos como segue:

- Equipamentos: Roteadores, switches, hubs e servidores;

As ameaças a serem analisadas seguem abaixo:

Situações de insegurança

As ameaças podem ser oriundas das seguintes situações de insegurança:

A. Físicas

A1. Incêndio acidental ou intencional

A2. Alagamento por inundação de ou salas com risco potencial, por vazamento dos encanamentos ou por goteiras

A3. Explosão intencional ou provocada por vazamentos de gás

A4. Desabamento parcial ou total do prédio

A5. Impacto de escombros da cobertura (teto de gesso, forração ou telhado)

A6. Sobrecarga na rede de alimentação elétrica ou relâmpagos que podem causar danos aos equipamentos

B. Problemas ambientais

B1. Variações térmicas – excesso de calor prejudica as mídias e excesso de frio danifica fisicamente dispositivos mecânicos

B2. Umidade – inimigo potencial de todas as mídias magnéticas

B3. Poeira depositada nas cabeças de leitura e gravação de drivers pode destruir fisicamente disquetes e fitas

B4. Radiações – além de causarem danos as pessoas, podem provocar problemas diversos em computadores

B5. Ruído excessivo causa estresse no pessoal

B6. Vapores e gases corrosivos – em qualquer incêndio, bastam 100ºC para transformar a água cristalizada nas paredes em vapor, que destrói mídias e componentes

B7. Fumaça – A fumaça do cigarro deposita uma camada de componentes químicos nas cabeças de leitura e gravação dos drives que pode inviabilizar a utilização de disquetes e fitas; Fumaça de incêndios próximos é muito mais perigosa.

B8. Magnetismo – Prejudicial às mídia magnéticas, pode desgravar disquetes, fitas e discos rígidos.

B9. Trepidação – Pode afrouxar placas e componentes em geral, além de destruir discos rígidos.

C. Supressão de Serviços

C1. Falha Prolongada de Energia Elétrica – Grande risco potencial, a medida que paralisa totalmente todas as funções relacionadas à informática.

C2. Queda das Comunicações

C3. Pane nos equipamentos

C4. Pane na Rede – Isola um ou mais computadores com risco potencial de perda de dados.

C5. Problemas nos Sistemas Operacionais – risco potencialmente explosivo, pois podem comprometer a integridade de todos os dados do sistema e até mesmo inviabilizar a operação.

C6. Parada de Sistema

D. Comportamento anti-social

D1. Acesso de pessoas não autorizadas

D2. Hacker – Indivíduo que conhece profundamente um computador e um sistema operacional e invade o site sem finalidade destrutiva

D3. Disputas exacerbadas entre outras pessoas podem levar a sabotagem e alteração ou destruição de dados ou de cópias de segurança

D4. Falta de espírito de equipe – falta de coordenação, onde cada funcionário trabalha individualmente; risco de omissão ou duplicação de procedimentos

D5. Inveja pessoal/profissional – podem levar um profissional a alterar ou destruir dados de outro funcionário

E. Ação criminosa

E1. Furtos e roubos – conseqüências imprevisíveis

E2. Fraudes – modificação de dados com vantagens para o elemento agressor

E3. Sabotagem – modificação deliberada de qualquer ativo da entidade

E4. Terrorismo – conseqüências imprevisíveis

E5. Seqüestros – ação contra pessoas que tenham alguma informação

E6. Espionagem industrial – captação não autorizada de software, dados ou comunicação

E7. Cracker – indivíduo que conhece profundamente um computador e um sistema operacional e invade o site com finalidade destrutiva

F. Incidentes variados

F1. Erros em back ups – risco sério de perda de dados; o backup sempre deve ser verificado

F2. Uso inadequado dos sistemas – normalmente ocasionado por falta de treinamento, falta de documentação adequada ao sistema ou falta de capacidade de quem utiliza o sistema de forma inadequada

F3. Manipulação errada de arquivos – pode causar perda de arquivos e contaminar as cópias de segurança

F4. Treinamento insuficiente – causa erros e uso inadequado de recursos

F5. Ausência/demissão de funcionário – problemático se a pessoa ausente for básica para determinados procedimentos

F6. Estresse/sobrecarga de trabalho – um operador sobrecarregado é mais propenso a cometer erros e a adotar atitudes anti-sociais

F7. Equipe de limpeza – deve receber um treinamento adequado sobre segurança

G. Contaminação eletrônica

G1. Vírus – programa que insere uma cópia sua em outros programas executáveis ou no setor de boot; os vírus replicam através da execução do programa infectado

G2. Bactéria – programa que reproduz a si próprio e vai consumindo recursos do processador e memória

G3. Verme – programa que se reproduz através de redes

G4. Cavalo de Tróia – programa aparentemente inofensivo e útil mas que contém um código oculto indesejável ou danoso

G5. Ameba – usuário que sem ter conhecimento para tanto, mexe na configuração do computador ou do software, causando problema, perda de dados, travamento da máquina, etc

G6. Falhas na segurança dos serviços – os serviços da Internet são potencialmente sujeitos a falhas de segurança, basicamente devido ao fato de ter sido desenvolvido em ambiente universitário, que visava um processamento cooperativo e não a segurança

Legenda	
Grau de Ameaça	Variação de 0 a 10
Grau de Vulnerabilidade	Variação de 0 a 10
Risco	Soma do Grau de Ameaça com o Grau da Vulnerabilidade

Equipamento			Quantidade	
Roteadores			**5**	
Ameaça	**Grau da Ameaça**	**Vulnerabilidade**	**Grau de Vulnerabilidade**	**Risco**
A1	2	Falta de monitoramento e controle automático em caso de incêndio	4	6
A4	1	Infiltração na estrutura do prédio	2	3
A6	4	Grande ocorrência de descargas elétricas na região.	3	7
B1	3	Falta de climatização de alguns ambientes	3	6
C1	5	Falta de gerador de energia.	5	10
C3	3	Falta de equipamentos de backup	3	6
D1	3	Falta de uma política de restrição de acesso de funcionários.	2	5
E3	3	Grande quantidade de usuários acadêmicos	3	6
F4	4	Falta de uma padronização dos equipamentos dificultando o treinamento.	3	7

Equipamento			Quantidade	
Switches			**3**	
Ameaça	**Grau da Ameaça**	**Vulnerabilidade**	**Grau de Vulnerabilidade**	**Risco**
A1	2	Falta de monitoramento e controle automático em caso de incêndio	4	6
A4	1	Infiltração na estrutura do prédio	2	3
A6	4	Grande ocorrência de descargas elétricas na região.	3	7
B1	3	Falta de climatização de alguns ambientes	3	6
C1	5	Falta de gerador de energia.	5	10
C3	3	Falta de equipamentos de backup	3	6
D1	3	Falta de uma política de restrição de acesso de funcionários.	2	5
E3	3	Grande quantidade de usuários acadêmicos	3	6
F4	4	Falta de uma padronização dos equipamentos dificultando o treinamento.	3	7

Equipamento			Quantidade	
Hubs			**7**	
Ameaça	**Grau da Ameaça**	**Vulnerabilidade**	**Grau de Vulnerabilidade**	**Risco**
A1	2	Falta de monitoramento e controle automático em caso de incêndio	4	6
A4	1	Infiltração na estrutura do prédio	2	3
A6	4	Grande ocorrência de descargas elétricas na região.	3	7
B1	3	Falta de climatização de alguns ambientes	3	6
C1	5	Falta de gerador de energia.	5	10
C3	3	Falta de equipamentos de backup	3	6
D1	3	Falta de uma política de restrição de acesso de funcionários.	2	5
E3	3	Grande quantidade de usuários acadêmicos	3	6
F4	4	Falta de uma padronização dos equipamentos dificultando o treinamento.	3	7

Equipamento			Quantidade	
Servidores			**7**	
Ameaça	**Grau da Ameaça**	**Vulnerabilidade**	**Grau de Vulnerabilidade**	**Risco**
A1	2	Falta de monitoramento e controle automático em caso de incêndio.	4	6
A4	1	Infiltração na estrutura do prédio	2	3
A6	4	Grande ocorrência de descargas de eletricidade atmosférica na região.	3	7
B1	3	Falta de climatização de alguns ambientes	3	6
B3	3	Os equipamentos não ficam numa posição adequada proporcionando um maior acúmulo de poeira.	3	6
C1	5	Falta de gerador de energia elétrica.	5	10
C3	3	Falta de equipamentos de backup	3	6
D1	3	Falta de uma política de restrição de acesso.	2	5
E3	3	Grande quantidade de usuários acadêmicos	3	6
F4	4	Falta de uma padronização dos equipamentos dificultando o treinamento.	3	7

Política de Segurança

1. Objetivo

Definir normas, padrões e procedimentos que:

- Protejam os colaboradores da Fundação
- Resguarde os ativos e instalações da entidade de dano, roubo ou destruição
- Instituam boas práticas de uso dos recursos de informática

2. Abrangência

Ativos Computacionais

- Equipamentos
- Programas
- Dados
- Senhas

Ativos Imobilizados e Suprimentos

- Equipamentos
- Suprimentos

Instalações

- Acesso

3. Documentos

- Classificação, Divulgação, Guarda e Destruição de Documentos

4. Comitê de Segurança

- Responsabilidades
- Membros

5. Procedimentos

5.1. Ativos Computacionais

5.1.1. Equipamentos

O uso dos equipamentos, independente de sua classe (de mesa, portátil, etc...), é destinado à utilização em necessidades legítimas de atividades da entidade.

A utilização particular, como no caso de trabalhos escolares, deverá ser previamente aprovada pela chefia da área à qual pertença o usuário, desde que não interfira nas atividades normais tanto do usuário como de sua área.

É permitido o uso particular, desde que com moderação, para:

- Acesso a Contas de e-mail particulares
- Realização de Transações Bancárias

É proibida a utilização para as seguintes finalidades: entretenimento, jogos (inclusive de azar), comércio.

É dever do usuário zelar pelo bom uso e conservação dos equipamentos colocados à sua disposição, pelos quais assinará um termo de responsabilidade para os equipamentos portáteis. Qualquer prejuízo ou dano decorrente de mal-uso ou negligência será imputado ao usuário, que responderá pecuniariamente por ele.

A área de Informática será responsável pela pesquisa e implantação de melhorias técnicas que vise aumentar a segurança nos equipamentos, tais como instalação de programas que impeçam o uso do computador sem a devida identificação do usuário.

A área de Informática será responsável por todos os recursos computacionais da entidade, otimizando-os e além de garantir o melhor aproveitamento de recursos financeiros quando da compra destes recursos.

5.1.1.1 Portáteis

Equipamentos portáteis deverão empregar cadeado e corrente próprias, que os fixará à mesa do usuário.

Em caso de transporte, o portátil jamais deverá ser guardado à vista dentro de veículos: é recomendável trancá-lo no porta-malas. Em aeroportos e terminais de embarque, jamais deixa-lo fora de vista ou solicitar sua guarda a terceiros, a não ser em serviço de guarda em cofres.

5.1.2. Programas

Para ser usado na entidade, qualquer programa necessita ser adquirido e homologado, e instalado, pelo pessoal técnico competente.

Não são permitidas as seguintes práticas:

- uso de programas não homologados pela área técnica competente;
- cópia e distribuição ilegal de programas
- empréstimo dos meios magnéticos/ópticos dos programas de propriedade da entidade a usuários ou a terceiros
- armazenamento e o uso de programas do tipo: jogos, protetores de tela (outros que não os da instalação-padrão), programas multimídia (música, filmes, fotos, desenhos, cartões comemorativos, etc...) e programas de comunicação instantânea (mIRC, ICQ, etc...).

As violações destas diretrizes sujeitarão o infrator a sanções legais e disciplinares.

5.1.2.1. E-Mail

Constituem práticas proibidas:

- divulgação de conteúdos incompatíveis com as atividades profissionais do usuário a destinatários tanto internos como externos;
- propagação de “correntes”, “abaixo-assinados”, “promoções” e campanhas políticas e eleitorais
- propagação de informações que constituam difamação, injúria, calúnia, ameaças, conspirações e incentivo a práticas ou comportamentos ilegais
- abertura de arquivos recebidos por e-mail que:
    - não sejam relativos ao exercício das funções do usuário
    - que não sejam Texto (.txt), Documento (.doc), Planilha (.xls), Apresentação (.ppt), a menos que você tenha certeza absoluta que o conteúdo é seguro e assuma a responsabilidade por abri-lo.

5.1.2.2. Internet

Constituem práticas proibidas:

- Acesso a sites com conteúdo incompatível com as atividades profissionais do usuário, tais como:
  - entretenimento
  - jogos de azar
  - jogos on-line
  - bate-papo (“chat”)
  - programas ilegais (“warez”)
  - pornografia
- Obtenção (“download”) de programas “shareware” e “freeware” de qualquer natureza, tais como:
  - protetores de tela
  - música digital
  - imagens
  - vídeo-clips
- Uso dos recursos técnicos da entidade para invasão de outros sites, ou execução atividades ilegais

5.1.3. Dados

Os dados da entidade a que os usuários têm acesso são confidenciais, e não devem ser divulgados indiscriminadamente. Requisições de informação oriundas de terceiros deverão ser encaminhadas à área de Informática.

Cada usuário dispõe de um espaço na rede para armazenar seus dados e e-mails mais importantes. A guarda de dados importantes somente no equipamento do usuário não terá qualquer garantia de recuperação em caso de perda ou corrupção. Caso seja do interesse do usuário este poderá solicitar ao Help-Desk para que seja providenciado um Backup em CD ou Fita desde que a informação a ser guardada seja estritamente de interesse da entidade.

A Área de Informática é responsável pela administração dos recursos de

contingência (back ups), pelos quais estabelecerá e cumprirá rotinas de geração, armazenamento e recuperação.

Dados importantes, em quaisquer meios, não devem ser deixados em locais de fácil acesso, sendo que é recomendável que sejam guardados e trancados sempre que não estiverem sendo usados.

5.1.5. Senhas

Os equipamentos deverão, sempre que possível, ser programados com senhas de acesso que bloqueiem o acesso não autorizado aos equipamentos, programas e arquivos. A senha deverá ser pedida ao se acionar o equipamento e programa, e após período de inatividade do usuário.

A senha de BIOS será colocada pelo pessoal de Informática quando da instalação do equipamento. O usuário fica proibido de trocar esta senha, caso venha a descobrir a mesma, ou colocar qualquer outra senha sem o prévio consentimento da área responsável, ou seja, Informática.

As senhas deverão expirar periodicamente, e sua revelação a terceiros ou a outros usuários é proibida, exceto em casos de força maior autorizados por chefes de divisão ou o Presidente da Fundação. Sempre que isto acontecer, a senha deverá ser trocada tão logo possível. As senhas pessoais devem ser memorizadas e não escritas.

A extensão e periodicidade da troca serão definidas de acordo com as características técnicas do recurso que visa proteger, e serão reguladas por procedimentos de cada área técnica responsável.

Com o objetivo de dificultar a dedução de senhas por terceiros, elas devem ser escolhidas segundo as seguintes recomendações:

- Extensão mínima de 6 caracteres, preferencialmente uma combinação de letras e algarismos
- Evitar conjuntos seqüenciais ou repetidos de letras, algarismos e teclas, como:
    - ABCDEF
    - 123456
    - QWERTY
    - 999999
- Evitar datas de eventos públicos ou acontecimentos pessoais (aniversários)

- Evitar nomes próprios e apelidos, nomes de entidades, ou palavras relacionadas aos passatempos e preferências do usuário
- Evitar o emprego de uma regra de formação ou fórmula mnemônica para renovação de senhas, como:
    - MARIA07, MARIA08, MARIA09...
    - JAN2000, FEV2000, MAR2000...

5.1.5.1 Administradores, Supervisores e Super-Usuários

As contas de usuários Administradores ou Supervisores, que têm plenos poderes nos sistemas, deverão ter seus nomes-padrões mudados sempre que possível.
Exemplo:

o usuário Administrator de um servidor Windows NT deverá ser renomeado para Einstein, ou Galileu, ou Superman.

Sempre que possível, as contas de Administrador não devem ser usadas. Em favor da auditoria do sistema, cada administrador deverá ter duas contas pessoais, uma com poderes de usuário comum para atividades corriqueiras, e outra com poderes equiparados à conta de Administrador para atividades que necessitem de plenos poderes.

5.1.5.2. Senhas Não-Pessoais

As senhas que permitem acesso a equipamentos que não reconhecem a existência de mais de um usuário, e as senhas de administração com poderes plenos, deverão ser documentadas e guardadas em local seguro.

5.2. Ativos Imobilizados e Suprimentos

5.2.1. Equipamentos

Os equipamentos colocados à disposição dos funcionários destinam-se à execução de atividades profissionais.

É dever do usuário zelar pelo bom uso e conservação dos equipamentos colocados à sua disposição, pelos quais poderá assinar um termo de responsabilidade, conforme seu

valor ou importância (recomendação). Qualquer prejuízo ou dano decorrente de mal-uso ou negligência será imputado ao usuário, que responderá pecuniariamente por ele.

Sempre que possível, o equipamento deverá ser guardado em local seguro quando não estiver sendo utilizado.

5.2.2. Suprimentos

Os suprimentos e material de escritório colocado à disposição dos funcionários destinam-se à execução de atividades profissionais. O consumo dos mesmos para fins pessoais é proibido.

5.3. Instalações

5.3.1. Acesso

O acesso às instalações depende de identificação prévia, através de crachá fornecido na portaria do Campus.

Não é permitido o trânsito de terceiros desacompanhados nas dependências da entidade, sob qualquer pretexto.

É proibido o acesso de vendedores de bens ou serviços pessoais. Entregadores deverão se limitar à recepção do andar, a menos que sejam necessários para o transporte de material volumoso ou pesado.

O acesso fora dos horários comerciais deverá ser previamente autorizado, e será regulado por procedimento a ser definido pela Área Administrativa.

5.3.1.1. Áreas Restritas

São consideradas Áreas Restritas:

- CGA e dependências de controle operacional
- Almoxarifado
- Tesouraria
- Salas dos Diretores e dos Gerentes de Recursos Humanos e Jurídico
- Qualquer local onde se encontrem ativos valiosos ou perigosos, ou que facilitem o

acesso a eles

Estes locais deverão ser fechados, com portas e trancas (manuais ou eletrônicas). Os usuários autorizados deverão sempre portar a chave que permitam o acesso, e deverão sempre manter as portas fechadas.

5.4. Documentos

Os documentos gerados e mantidos na Fundação, em qualquer meio (papel, meio magnético ou óptico), são exclusivamente para uso interno. A menção “Uso Interno” deve estar explícita em todos os documentos, no rodapé de cada página se for o caso.

A divulgação de informações à Imprensa e ao público é de responsabilidade das áreas competentes, conforme atribuído pela Direção da Fundação.

5.4.1 Classificação, Divulgação, Guarda e Destruição

Os documentos são classificados conforme seu conteúdo em:

- confidenciais: quando sua revelação ou uso indevido possa causar quaisquer danos, prejuízos ou embaraços à UniFOA, seus controladores, parceiros ou funcionários;
- públicos: quando sua divulgação não causar os efeitos mencionados no item anterior.

Um documento classificado como público não implica que ele possa ser divulgado para fora da Entidade.

Os documentos confidenciais devem ser divulgados somente às pessoas interessadas. Para notificar a outrem de seu envio ou recepção por e-mail, deve-se excluir os arquivos confidenciais anexados.

Os documentos confidenciais devem ser guardados em local seguro, preferencialmente de acesso restrito. Jamais devem ser deixados em cima de móveis ou em gavetas ou armários destrancados.

As cópias não mais necessárias de documentos confidenciais devem ser destruídas, se em papel, no fragmentador; se em disquete ou CD, quebrá-lo ao meio.

A Informática é responsável pela pesquisa e instalação de recursos que facilitem a guarda e destruição de arquivos magnéticos contendo informações confidenciais.

5.5. Comitê de Segurança

Fica estabelecido o Comitê de Segurança para gerenciar os diversos aspectos de segurança da Entidade.

5.5.1. Responsabilidades

- Avaliar os riscos existentes na entidade, sob os aspectos:
  - Ativos da Entidade
  - Instalações e Infra-estrutura
  - Acesso e Segurança do Pessoal
- Elaborar e implantar normas e procedimentos para reduzir ou eliminar os riscos apontados, e sugerir ações para a Direção da entidade.

5.5.2. Membros

Membros Executivos:

São membros permanentes, representando as principais áreas de responsabilidade.

- Informática (Oficial de Segurança)
- Administração Geral
- Infra-estrutura

Membros Consultivos:

São membros que serão chamados conforme necessário ao desenvolvimento das atividades, preferencialmente a chefia das áreas envolvidas.

- Informática
- Administração e Finanças
- Jurídico
- Recursos Humanos

5.5.3. Matriz de Responsabilidades:

Atividades	Áreas			
	Informática	Administração	Infra-Estrutura	Operações
Rede Corporativa (hw/sw/dados)	X			
Cabeamento Estruturado	X			
Energia Elétrica/Quadros/Shafts			X	
Acesso (sensores/câmeras)			X	
Recepcionistas / Vigias		X		
Fax / Copiadoras		X		
Extintores / Ar Condicionado / Saídas		X		
Tecnologias de Operações (hw/sw/dados)				X

PROJETO DE GERENCIAMENTO DA REDE

Por menor e mais simples que seja, uma rede de computadores precisa ser gerenciada a fim de garantir aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável.

À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle afim de diagnosticar e registrar eventos que possibilitam detectar o mau funcionamento e prever falhas que interrompam sua operação proporcionando assim um bom gerenciamento proativo.

A simples adoção de um software de gerenciamento não resolve todos os problemas da pessoa responsável pela administração da rede. Geralmente o usuário de um software de gerenciamento espera muito dele e consequentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, esses mesmos softwares quase sempre são sub-utilizados, isto é, possuem inúmeras características inexploradas ou utilizadas de modo pouco eficiente. Para gerenciar um recurso, é necessário conhecê-lo muito bem e visualizar claramente o que este recurso representa no contexto da rede

➢ Estratégia para implantação do sistema de gerência

De uma maneira simplificada, podemos estabelecer uma estratégia metodológica para a implantação de um sistema de gerência:

- Conhecimento do plano estratégico da empresa a fim de identificar seus objetivos e prioridades;
- Definição dos objetivos a serem alcançados com o sistema a ser implantado;
- Especificação dos serviços necessários para o alcance dos objetivos;
- Identificação das prioridades para identificar os serviços mais urgentes;
- Seleção da plataforma de integração considerando o atendimento aos serviços e/ou facilidades para o desenvolvimento de aplicações que proporcionem o seu atendimento;
- Modelagem das informações identificando aquelas que realmente serão úteis para

o alcance dos objetivos;

- Desenvolvimento de novas aplicações para complementar o trabalho.

➢ Arquitetura Adotada

Por se tratar de uma rede totalmente baseada no protocolo TCP/IP e também devido à sua simplicidade e seus conceitos optou-se por utilizar a arquitetura SNMP.

O modelo arquitetural SNMP é uma coleção de estações de gerenciamento e elementos de rede. As estações de gerenciamento executam aplicações de gerenciamento que monitoram e controlam os elementos de rede. Os elementos de rede são equipamentos tais como hospedeiros, gateways, servidores de terminais, e similares, que possuem agentes de gerenciamento, responsáveis pela execução das funções de gerenciamento de rede, requisitadas pelas estações de gerenciamento. O protocolo SNMP é usado para transportar a informação de gerenciamento entre as estações de gerenciamento e os agentes existentes nos elementos de rede.

O modelo proposto busca minimizar o número e a complexidade de funções de gerenciamento realizadas pelos agentes de gerenciamento. As razões que tornam este objetivo atrativo, são:

- o custo de desenvolvimento do software de agente de gerenciamento, necessário para suportar o protocolo é significativamente reduzido;
- o grau de funcionalidade suportado remotamente é proporcionalmente aumentado, à medida que se aumenta a utilização dos recursos Internet na tarefa de gerenciamento;
- a quantidade de funções de gerenciamento, que são suportadas remotamente, é gradativamente aumentada, através da imposição de algumas restrições sobre a forma e sofisticação das ferramentas de gerenciamento.
- conjuntos simplificados de funções de gerenciamento são facilmente entendidos e utilizados pelos desenvolvedores de ferramentas de gerenciamento de redes.

➢ Gerenciamento Centralizado

A proposta é que o gerenciamento da rede seja feito de maneira centralizada, sendo o seu monitoramento realizado a partir da divisão de informática onde se localiza o Backbone Central da rede.

Modelo de Gerenciamento Adotado Por menor e mais simples que seja, uma rede de computadores precisa ser gerenciada a fim de garantir aos seus usuários, a disponibilidade de serviços a um nível de desempenho aceitável.

À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle afim de diagnosticar e registrar eventos que possibilitam detectar o mau funcionamento e prever falhas que interrompam sua operação proporcionando assim um bom gerenciamento proativo.

A simples adoção de um software de gerenciamento não resolve todos os problemas da pessoa responsável pela administração da rede. Geralmente o usuário de um software de gerenciamento espera muito dele e consequentemente, fica frustrado quanto aos resultados que obtém. Por outro lado, esses mesmos softwares quase sempre são sub-utilizados, isto é, possuem inúmeras características inexploradas ou utilizadas de modo pouco eficiente. Para gerenciar um recurso, é necessário conhecê-lo muito bem e visualizar claramente o que este recurso representa no contexto da rede

➢ Modelo de Gerenciamento Adotado

Existem dois modelos adotados para gerência de redes: o Modelo Internet e o Modelo OSI.

No projeto FastFOA optou-se por utilizar o gerenciamento do modelo OSI da ISO que baseia-se na teoria da orientação a objetos. Com isso, o sistema representa os recursos gerenciados através de entidades lógicas, as quais recebem a denominação de objetos gerenciados.

Existem cinco área funcionais no gerenciamento num ambiente OSI:

Falhas – funções que possibilitam a detecção, isolamento e correção de operações normais na rede: Manter logs de erros; Receber e agir sobre notificações de erros; Rastrear e identificar falhas; Gerar seqüências de testes de diagnósticos; Corrigir falhas.

Configuração – funções que habilitam o usuário a criar e modificar recursos físicos e lógicos da rede: Indicar parâmetros de controle de rotinas de operação do sistema; Associar nomes aos objetos gerenciados e configurá-los; Inicializar e excluir objetos gerenciáveis; Coletar informações em tempo real a respeito das condições atuais do sistema;
Obter avisos a respeito de modificações significativas do sistema;
modificar a configuração do sistema.

Desempenho – funções relacionadas com a avaliação e relato do comportamento dos equipamentos bem como sua eficiência na rede: Manter informações estatísticas; Manter logs de históricos de estados; Determinar o desempenho do sistema sob condições normais e adversas; Alterar os modos de operação do sistema com o propósito de conduzir atividades de gerenciamento de desempenho.

Segurança – algumas de suas funções são: criação e controle de serviços e mecanismos de segurança; Distribuição de informações relevantes à segurança; armazenamento de eventos relativos à segurança.

Contabilização – funções que possibilitam a determinação do custo associado ao uso da rede: Informar aos usuários os custos associados aos recursos consumidos; habilitar limites de tarifação e indicar agendamentos a serem associados com a utilização dos recursos; combinar custos quando um requisito de comunicação exigir múltiplos recursos combinados.

- Protocolos

Dentre os protocolos de gerenciamento comumente utilizados destacam-se:

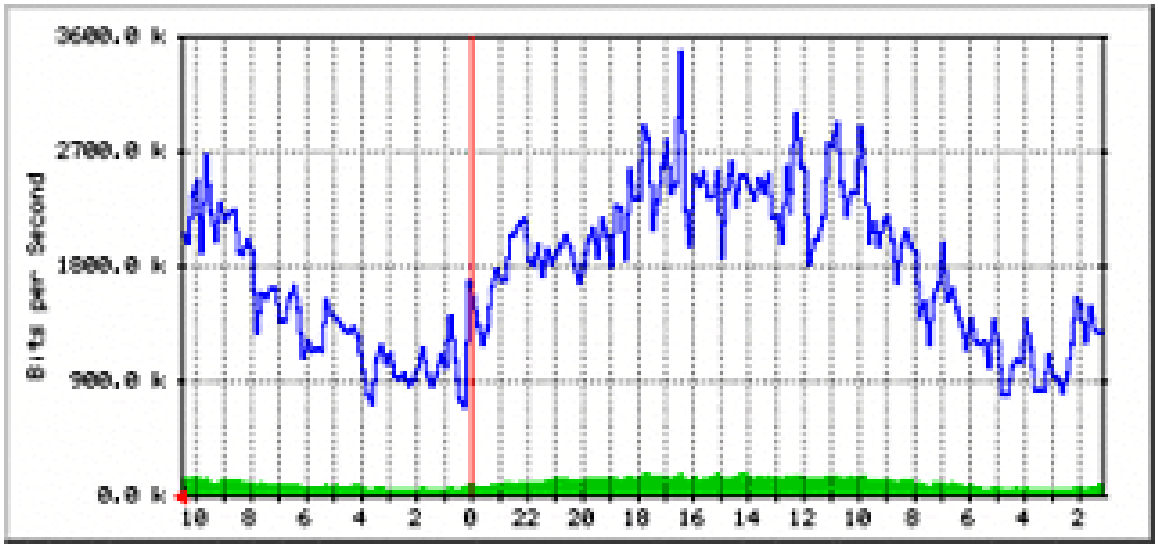
PROTOCOLO	DESCRIÇÃO
RMON	Padrão para monitoramento remoto oferece uma arquitetura de gerenciamento distribuída para análise de tráfego, resolução de problemas, demonstração de tendências e gerenciamento pró-ativo de redes de modo geral. Criado pelos mesmos grupos que desenvolveram o TCP/IP e o SNMP, o RMON é um padrão IETF de gerenciamento de redes cuja sigla representa Remote Network Monitoring MIB.
CMIP	Protocolo de gerenciamento definido segundo o padrão OSI, da mesma maneira que o SNMP, o CMIP especifica como vai ser realizada a troca de informações entre o gerente e o agente no sistema de gerenciamento. Os tipos de informação a serem trocadas levam em conta o CMIS (*Common Management Information Service*), especificando o conjunto de serviços a que os sistemas gerenciador e gerenciado poderão acessar para que seja realizado o gerenciamento. Juntos CMIS e CMIP formam o que é chamado de CMISE (*Common Management information Service Element*).

Devido à arquitetura escolhida anteriormente o protocolo a ser utilizado será o SNMP.

SNMP é um padrão de gerenciamento amplamente usado em redes TCP/IP, fornecendo um método de gerenciamento de *hosts* de rede como: computadores servidores, firewall, estações de trabalho, roteadores, bridge e concentradores a partir de um computador com uma localização central em que esteja sendo executado o software de gerenciamento de rede (estação de gerenciamento). Executa serviços de gerenciamento utilizando uma arquitetura distribuída de sistemas de gerenciamento e agentes.

Com a implementação da rede, serão utilizados programas de gerência disponíveis na Internet, como o MRTG (Multi Router Traffic Grapher) , baseado no protocolo SNMP. Foram encontradas outras soluções de programas, porém esta apresentada foi a que melhor correspondeu às necessidades, permitindo um grande avanço do estudo da gerência de rede pois foi possível conhecer o funcionamento prático das MIB’s, do protocolo SNMP e das características dos objetos gerenciáveis dos equipamentos.

MRTG consiste em um script em Perl que usa SNMP para ler os contadores de tráfego de seus roteadores e um rápido programa em C que loga os dados do tráfego e cria belos gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas Web que podem ser visualizadas de qualquer Browser moderno.



Somadas a detalhada visão diária o MRTG também cria representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses. Isto é possível porque o MRTG mantém um log de todos os dados que ele conseguiu do roteador. Este log é automaticamente consolidado, e com isso ele não cresce com o tempo, mas ainda contém todos os dados relevantes de todo o tráfego dos últimos 2 anos. Isto tudo é realizado de uma maneira muito eficiente. Então você pode monitorar mais de 200 links de rede de qualquer estação.

O MRTG não se limita a monitorar somente tráfego, é possível monitorar qualquer variável SNMP que você escolher. Você pode até usar um programa externo para pegar os dados que você deve monitorar via MRTG. As pessoas usam o MRTG, para monitorar coisas como Carga do Sistema, Sessões Logadas, Disponibilidade de Modems e muito mais. O MRTG ainda permite a você acumular 2 ou mais fontes de dados em um único gráfico.

SERVIDORES

Existem atualmente no Campus da UniFOA 13 servidores instalados e operacionais, sendo que a maioria deles se concentra no site Três Poços (CGA), destes servidores alguns serão retirados permanecendo no projeto FastFOA somente 7. O plano de instalação dos servidores versará apenas sobre os novos servidores que serão implementados, no caso o servidor Web, o servidor Backup, e os servidores Firewall. Os demais servidores atendem as necessidades atuais e não estão previstas alterações.

Os servidores serão nomeados de forma a especificar sua função (servidor Web, Backup, Firewall), localização dentro do Campus (Aterrado, Tangerinal, Três Poços) e índice numerado para mais de um servidor na mesma função e localidade (Firewall 1 e 2). Para especificar a função do servidor serão utilizados 02 dígitos, para localidade serão 03 dígitos e para o índice numerado serão 02 dígitos nessa mesma seqüência.

O nome do servidor será composto então por um código de sete dígitos que o identificará de forma simples, prática e rápida. O servidor nomeado como SWCGA01 será a identificação do Servidor Web de Três Poços 01, onde SW se traduz em Servidor Web, CGA é a sigla para Três Poços e 01 o índice identificador.

➢ Plano de Instalação

O servidor escolhido para hospedar o Web Server será um IBM NETFINIT, os demais servidores serão microcomputadores simples montados conforme a tabela abaixo:

Servidor	Processador	Memória	Disco	Rede
Web	Intel PIII 650 Mhz	256MB	04 HDs U.W. SCSI 9GB	IBM 10/100
Backup	Intel PIII 750 Mhz	128MB	01 HD 20GB IDE	Sys 900 on
Firewall 1	Intel PIII 750 Mhz	128MB	01 HD 20GB IDE	Sys 900 on
Firewall 2	Intel PIII 750 Mhz	128MB	01 HD 20GB IDE	Sys 900 on

O sistema operacional escolhido para implementação dos novos servidores é o Windows 2000 Server. A escolha foi realizada com base nas suas facilidades de controle e administração remotos, assim como o gerenciamento e rotinas administrativas entre outras, e especialmente em função do aumento da confiabilidade, disponibilidade, escalabilidade e desempenho desse sistema operacional em relação ao seu antecessor o Windows NT Server 4.0 descontinuado pela Microsoft.

Segue abaixo a listagem dos softwares a serem instalados nos servidores:

Servidor	Softwares
WEB	Microsoft Windows 2000 Server SP3
	Microsoft Internet Information Server (IIS)
	Microsoft Proxy 2.0
BACKUP	Microsoft Windows 2000 Server SP3
FIREWALL 1 & 2	Microsoft Windows 2000 Server SP3

O endereçamento IP dos servidores seguirá o modelo atual da UniFOA que é um endereçamento estático de Classe C recebendo os servidores os seguintes endereços:

Servidor	Endereço
WEB	192. 168.1.4
BACKUP	192. 168.1.5
FIREWALL 1	192. 168.1.6
FIREWALL 2	192. 168.1.7

Foi encontrada na rede UniFOA uma brecha para falhas que é a utilização de um único servidor DHCP para todos os clientes da rede. Procurando implementar uma forma de tolerância

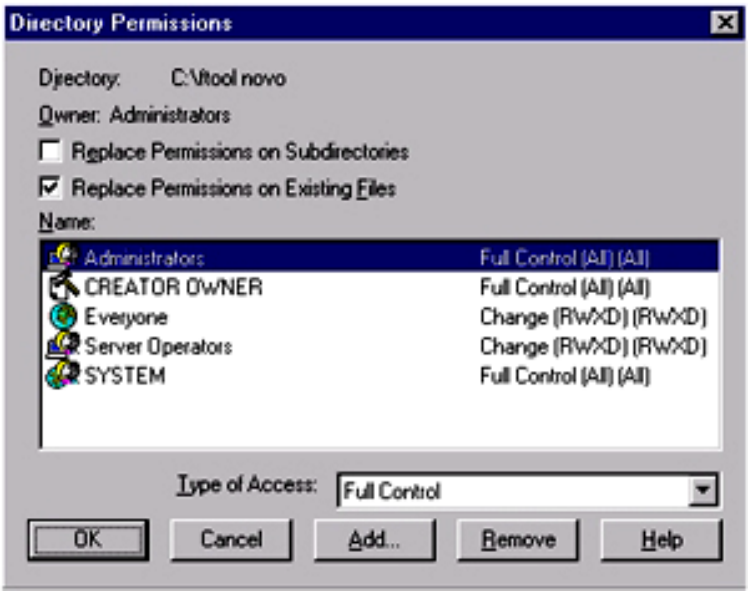
➢ Configuração de Disco

O servidor Web terá quatro (04) discos rígidos Ultra Wide SCSI com capacidade de nove (09) Gibabytes cada e tolerância a falha RAID 5 implementada via hardware o que totaliza 18GB de espaço para o sistema operacional e aplicativos e um disco spare que será ativado em caso de falha. Os demais servidores terão dois (02) discos IDE de vinte (20) GB com tolerância a falha RAID 1 implementada via software.

➢ Configuração de contas e grupos

A nomenclatura adotada atualmente atende perfeitamente à instituição, não sendo necessária a mudança deste padrão. Cada departamento e secretaria de curso possui os seus grupos e pastas que são estruturados da seguinte maneira:

- Cada departamento possui uma pasta com seu nome. Ex. Departamento Tesouraria, pasta da rede = Tesouraria.
- Os grupos são criados com os nomes dos departamentos sendo que somente os membros dos departamentos e o administrador de rede pertencem a estes grupos. Por exemplo: Divisão de Informática (DI) → Nome do Grupo = DI
- Todos os grupos são globais de maneira que de qualquer localidade da rede do UniFOA o usuário pode acessar a pasta de seu respectivo departamento. Isto ocorre devido ao fato de alguns departamentos mudarem de localidade com certa freqüência.

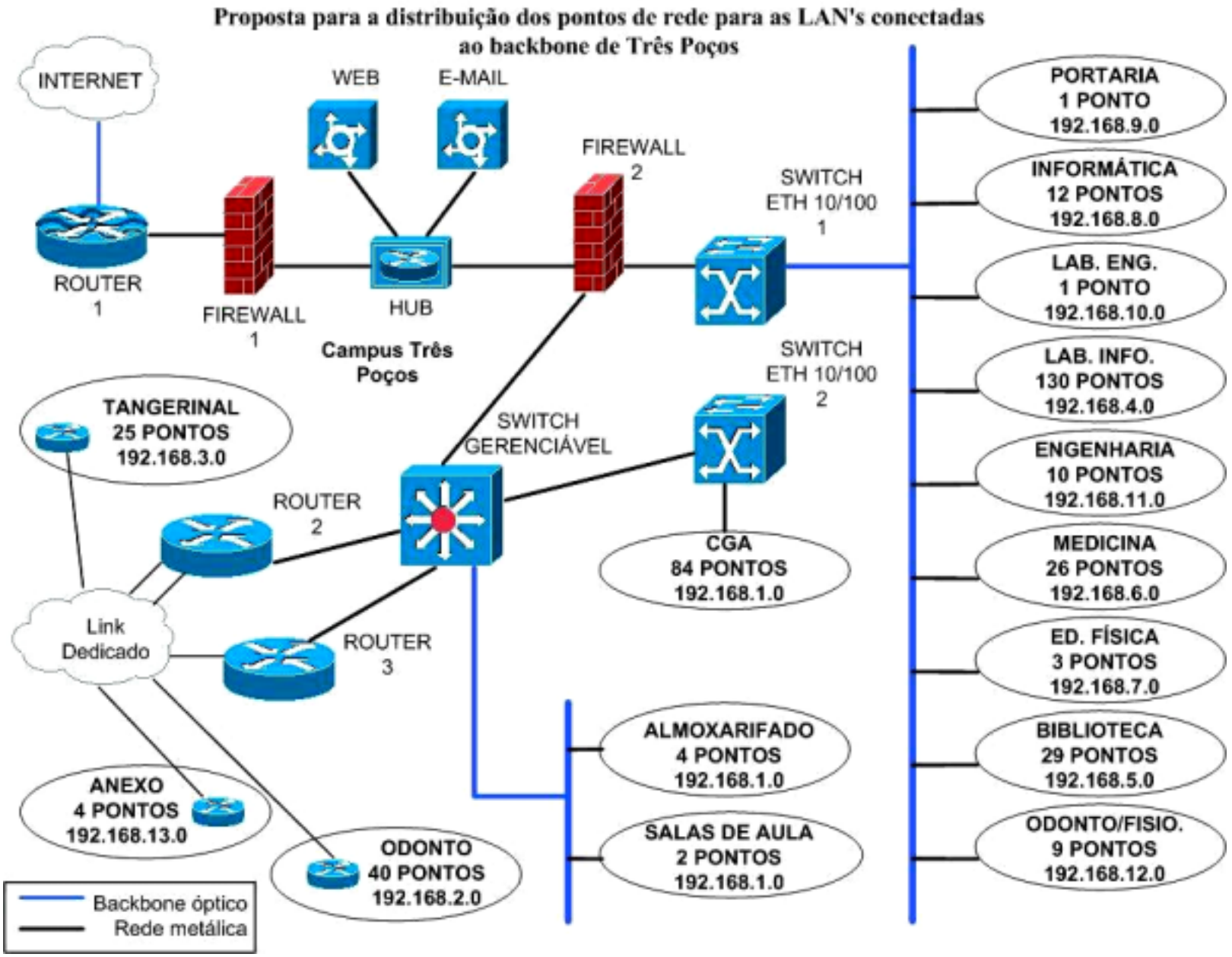


Exemplo da nomenclatura e organização das pastas no Laboratório de Informática

➢ Topologia de Firewall

O Firewall implementado atualmente no UniFOA, é uma máquina com Windows NT com um software especializado instalado, Winroute. Este software implementa filtro de pacotes, NAT e também funciona como gateway para os diversos segmentos da rede.

A proposta é que se crie uma Demilitarized Zone (DMZ) com um roteador, onde seriam colocados servidores de Web, Mail e um servidor de BD para que se disponibilize as notas dos alunos on-line, esta estrutura estaria localizada entre dois Firewalls com políticas implementadas de maneira a não permitir acessos externos não autorizados.


Proposta para a distribuição dos pontos de rede para as LAN's conectadas ao backbone de Três Poços
INTERNET
WEB
E-MAIL
FIREWALL 2
SWITCH ETH 10/100 1
ROUTER 1
FIREWALL 1
HUB
Campus Três Poços
SWITCH ETH 10/100 2
SWITCH GERENCIÁVEL
TANGERINAL 25 PONTOS 192.168.3.0
ROUTER 2
CGA 84 PONTOS 192.168.1.0
Link Dedicado
ROUTER 3
ALMOXARIFADO 4 PONTOS 192.168.1.0
SALAS DE AULA 2 PONTOS 192.168.1.0
ANEXO 4 PONTOS 192.168.13.0
ODONTO 40 PONTOS 192.168.2.0
Backbone óptico
Rede metálica
PORTARIA 1 PONTO 192.168.9.0
INFORMÁTICA 12 PONTOS 192.168.8.0
LAB. ENG. 1 PONTO 192.168.10.0
LAB. INFO. 130 PONTOS 192.168.4.0
ENGENHARIA 10 PONTOS 192.168.11.0
MEDICINA 26 PONTOS 192.168.6.0
ED. FÍSICA 3 PONTOS 192.168.7.0
BIBLIOTECA 29 PONTOS 192.168.5.0
ODONTO/FISIO. 9 PONTOS 192.168.12.0

FASE 3 – PROJETO DA REDE FÍSICA

Entende-se por rede estruturada aquela que é projetada de modo a prover uma infra-estrutura que permita a evolução e flexibilidade para os serviços e tecnologias de telecomunicações atuais e futuros.

Dentro deste conceito, verificou-se a necessidade da implementação de modificações no backbone do Campus do UniFOA em Três Poços, para que este satisfaça as necessidades atuais e futuras de todos os sites da entidade e que também garanta a possibilidade de reconfigurações ou mudanças, sem a necessidade de investimentos adicionais, principalmente em obras civis. Esse fato foi detectado a partir da quantidade e complexidade dos equipamentos e sistemas de informação atualmente existentes no Campus do UniFOA de Três Poços e nos sites Tangerinal, Odontologia e Anexo.

O escopo do projeto da rede física tem como objetivo propor metas técnicas para a atualização do backbone do Campus de Três Poços e demais conexões aos sites distantes, bem como melhorias na conexão à INTERNET, através de modificações na rede física existente e seleção de provedor(es) de serviços de telecomunicações.

As alterações propostas visam os seguintes aspectos:

1. Oferecer facilidade de gerenciamento da rede com a introdução de ferramentas para o Administrador (ou Gerente da rede), com a reestruturação da sala de equipamentos do Campus de Três poços, utilizando os procedimentos previstos nas normas para implementação de redes de computadores;
2. Aumento da largura de banda da conexão da Internet para admitir novos equipamentos e aplicativos e a expansão do uso dos equipamentos e aplicativos atuais;
3. Contratação de um novo link de dados para interligação do site ANEXO que atualmente encontra-se isolado do restante da rede do UniFOA;
4. Aumento da largura de banda do link de dados do Tangerinal;
5. Fornecer uma estrutura de rede que facilite a adaptação para upgrades de equipamentos e que permita aumentar de escala e admitir o uso expandido futuro de novos equipamentos e aplicativos multimídia que usem tecnologias de última geração.

6. Facilitar o uso da rede sob o ponto de vista do usuário, possibilitando o acesso dos colaboradores, alunos e professores em todos os pontos da instituição, a todos os serviços proporcionados pela nova rede estruturada;
7. Facilitar o escalonamento da rede com um planejamento visando expansões futuras e manter (ou reduzir) o nível de investimentos em alterações ou correções na rede física;
8. Oferecer condições para implementação de ferramentas de segurança necessárias para a rede;
9. Metas de Desempenho esperado da rede – Contratação de serviços especializados e controle dos parâmetros de desempenho para oferecer uma rede de Campus com alta disponibilidade, alto MTBF e baixo MTTR. A disponibilidade pode ser calculada pela fórmula: DISPONIBILIDADE = MTBF / (MTBF+MTTR), em horas.

Não faz parte do escopo deste projeto a atualização de qualquer LAN do UniFOA, utilizada pelos colaboradores, alunos e professores, em quaisquer desses pontos, seja Campus Três Poços ou sites distantes.

No projeto de melhoria do backbone do Campus de Três Poços, a associação dos diversos dispositivos eletrônicos e a elaboração do projeto físico que possuem influência direta no custo final da rede a ser modificada, compreenderam a análise de aspectos importantes da rede atual como distâncias entre as estações, infra-estrutura e meios físicos existentes e desempenho esperado do sistema.

Nesta etapa do projeto são estabelecidos os critérios mínimos necessários para a melhoria do backbone do Campus de Três Poços, benefícios estes, que se refletirão para os demais sites distantes.

As referências normativas usadas para a elaboração deste projeto foram:

- “Procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada” – NBR 14565. Esta Norma se aplica aos edifícios e conjuntos de edifícios situados dentro do Campus e demais sites, com o objetivo de configurar uma nova disposição para o sistema Campus. (Anexos: 1, 2 e 3)
- IEEE 802.3 – padrão para redes Ethernet 10Mbps;
- IEEE 802.3u – padrão para redes Ethernet 100Mbps (FastEthernet);
- TIA/EIA 492-AAAA e ISO 11801 – padrão para cabeamento de redes ópticas.

Ao desenvolver-se o projeto, utilizando essas normas, pretende-se estabelecer a correta forma de aplicação dos conceitos de rede estruturada, envolvendo todos os seus elementos constitutivos.

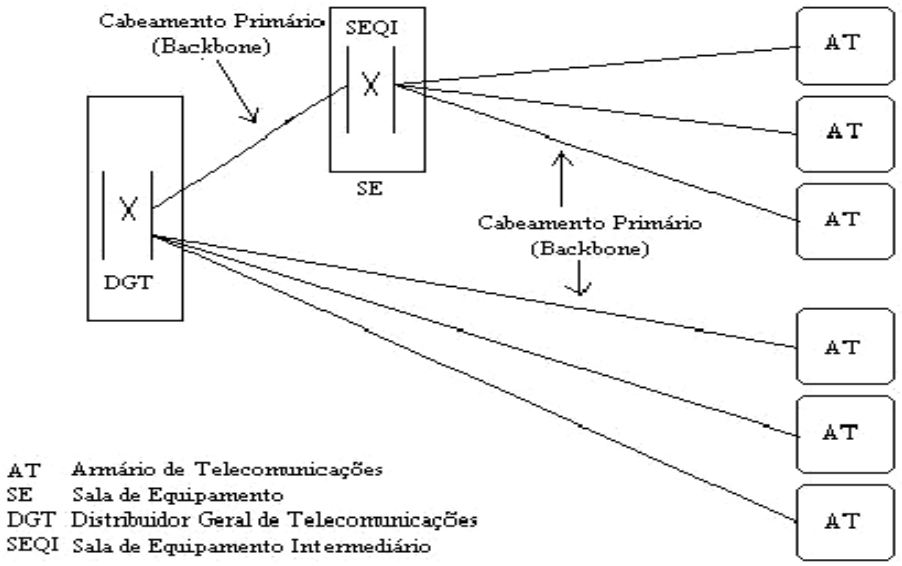
Entende-se que os materiais a serem utilizados na implementação das modificações do cabeamento da rede devem ser rigorosamente adequados às finalidades a que se destinam e devem satisfazer às normas vigentes dentro de cada categoria.

O projeto constitui-se, pois, no detalhamento das modificações que se fazem necessárias para a perfeita distribuição do cabeamento e demais elementos do backbone do Campus de Três Poços, contemplando a infra-estrutura existente.

PLANTA DE CABEAMENTO PARA LAN´S

Topologia de cabeamento do Campus de Três Poços

A proposta do projeto é implementar um sistema centralizado de distribuição, com a rede de cabos do backbone do Campus e demais sites seguindo a topologia estrela com hierarquia. Neste tipo de rede, os usuários situados no CGA, nas áreas de trabalho (AT), comunicam-se diretamente com o nó central (DGT), situado na sala de equipamentos no próprio CGA. Os demais usuários das diversas LAN's do Campus se comunicam com a sala de equipamentos situada no nó central através de salas de equipamento intermediárias (SEQI). Já para as redes dos sites distantes (Tangerinal, Anexo e Odontologia), propõe-se um DGT local em cada site e as áreas de trabalho (AT), conectadas diretamente a este. O esquema seguinte exemplifica a proposta.



Para cumprir essa finalidade, propõe-se a instalação de racks fechados, equipados com blocos e painéis de conexão, com conectores modulares tipo CM8V (RJ45), em número suficiente para atendimento dos pontos de rede em cada localidade.

Na parte final deste trabalho encontra-se o anexo 2 contendo detalhes da NBR 14565 quanto à representação esquemática, identificação das terminações e elementos construtivos da rede interna. Esse material tem como objetivo servir de referência para as modificações que se façam necessárias na adequação das redes locais conectadas ao backbone, apesar destas não fazerem parte do escopo deste projeto.

Tipos de cabos

A escolha dos cabos é a parte mais importante da implementação das melhorias na rede física. O item 6.4 da NBR 14565, considera as seguintes alternativas para cabeamento:

- STP (Shielded Twisted Pair) – Par trançado blindado, 2 pares, 150Ω, para aplicações até 100MHz.
- UTP (Unshielded Twisted Pair) – Par trançado, 4 pares, 100Ω, para aplicações de 16MHz até 100MHz;

  Existem cinco categorias de cabo UTP:

  - CAT1 e CAT2 – não são recomendados para a transmissão de dados;
  - CAT3 - para transmissões até 16 Mbps;
  - CAT4 - certificado para transmissões até 20 Mbps;
  - CAT5 - O cabo mais comum hoje em dia. Em condições ideais permite transmissões até 100 Mhz.

- Fibra óptica. Existem dois tipos de fibras: monomodais e multimodais.
  - Monomodo - Cabo de 8/125μm de diâmetro. Permite somente 1 via à luz, o que o torna menos susceptível a refrações internas e por isso, melhor. Porém, é mais caro e difícil de trabalhar.
  - Multimodo - Cabos de 50/125μm ou 62.5/125μm de diâmetro. Como a luz pode tomar mais de um caminho por dentro da fibra, é passível de interferências internas. Porém, mais barato e fácil de usar.

Caracterização do cabo UTP CAT5 para o projeto

Aplicações

Para o cabeamento interno dos edifícios do Campus de Três Poços e demais sites do UniFOA, propõe-se a manutenção do cabo UTP categoria 5, pois o mesmo é indicado na instalação de redes locais de computadores tipo Ethernet (10Mbps) ou FastEthernet (100 Mbps), vindo de encontro às necessidades do projeto. Além disso, trata-se de um cabo consagrado no mercado é o cabo atualmente utilizado no cabeamento das instalações de redes do campus.

É importante observar a disposição dos pontos de rede atuais para aferir se os mesmos encontram-se de acordo com o proposto na Norma, ou seja, para cada área de trabalho de 10,00m², devem ser previstos no mínimo dois pontos de telecomunicações, suportados por cabo UTP 100Ω, 4 pares, categoria 5. Para os locais que se encontram fora da Norma será necessário seu redimensionamento.

Material

O cabo UTP Categoria 5 é formado por condutores de cobre, isolados por composto especial, com marcação no isolamento, torcidos em pares, com capa externa em PVC não propagante à chama.

Recomendam-se modificações na atual codificação de cores para a capa externa dos cabos, prevendo uma diferenciação visual do cabo UTP para as várias funções e aplicações necessárias:

- Dados (pinagem direta): cor da capa externa verde;
- Dados (pinagem cruzada): cor da capa externa vermelho;
- Voz (Telefone): cor da capa externa amarelo;
- Vídeo (P&B e Colorido): cor da capa externa violeta.

Neste projeto, para os cabos de manobra em rede de dados, recomenda-se a distribuição de ligações aos conectores CM8V utilizando-se a disposição de fiação T568B como configuração padrão (standard) e a utilização de cabos de manobra com

comprimentos de 30 centímetros, 50 centímetros e um metro e a cor azul na capa externa. Todos os cabos que estiverem fora dessa especificação devem ser substituídos.

Instalação

A instalação do cabo UTP Categoria 5 compreende vários procedimentos necessários para que o cabo seja instalado convenientemente e, com isto, a rede possa aproveitar ao máximo suas vantagens.

Os cabos UTP Cat.5 são embalados em caixas tipo fastbox com comprimento padrão de 300 metros e acomodados no interior das caixas de tal forma que não se encontre dificuldade em retirar os mesmos do interior das caixas.

Basicamente, a instalação de novos pontos de rede utilizando cabos UTP Cat.5 deverá observar as seguintes etapas:

- Lançamento - Os cabos UTP Cat.5 devem ser lançados mediante o auxílio de cabos-guia, obedecendo-se os seguintes procedimentos:
  1. Devem ser lançados ao mesmo tempo em que são retirados da embalagem, ou seja, nos trechos onde devam ser lançados mais de um cabo em um duto, todos os cabos devem ser lançados juntos, de uma só vez, respeitando-se a taxa de ocupação dos dutos.
  2. Os cabos devem ser lançados obedecendo-se o raio de curvatura mínimo do cabo que é de 4 vezes seu diâmetro, ou seja, 21,2 mm.
  3. Os cabos não devem ser estrangulados, torcidos e prensados ou mesmo "pisados" com o risco de provocar alterações nas suas características originais.
  4. No caso de haver grandes sobras de cabos UTP, os mesmos deverão ser armazenados preferencialmente em bobinas, devendo-se evitar o bobinamento manual que pode provocar torções no cabo.
  5. Evitar reutilizar os cabos UTP de outras instalações, pois o mesmo foi projetado para suportar somente uma instalação.
  6. Cada lance de cabo UTP não deverá, em nenhuma hipótese, ultrapassar o comprimento máximo de 90 m permitido por norma.
  7. Todos os cabos UTP devem ser identificados com materiais identificadores padronizados, resistentes ao lançamento, para que os mesmos possam ser reconhecidos e instalados em seus respectivos pontos.

8. Nunca utilizar produtos químicos como vaselina, sabão, detergentes, etc, para facilitar o lançamento dos cabos UTP no interior de dutos, pois estes produtos podem atacar a capa de proteção dos cabos reduzindo a vida útil dos mesmos.
9. Jamais lançar os cabos UTP no interior de dutos que contenham umidade excessiva.
10. Não permitir que os cabos UTP fiquem expostos a intempéries, pois os mesmos não possuem proteção para tal.
11. Os cabos não devem ser lançados em infra-estruturas que apresentem arestas vivas ou rebarbas, tais que possam provocar danos aos cabos.
12. Evitar que os cabos sejam lançados próximos de fontes de calor, pois a temperatura máxima de operação permissível ao cabo é de 60º C.
13. Os cabos UTP devem ser decapados somente o necessário, isto é, somente nos pontos de conectorização.
14. Jamais poderão ser feitas emendas nos cabos UTP, sob risco de provocar um ponto de oxidação e com isto, possíveis falhas na comunicação. Nos casos em que o lance não tiver um comprimento suficiente, o correto é a substituição deste por outro com comprimento adequado.
15. Jamais instalar os cabos UTP na mesma infra-estrutura com cabos de energia e/ou aterramento.
16. Nunca instalar os cabos UTP em infra-estruturas metálicas que não estejam em concordância com as normas de instalações elétricas.
17. Quando a infra-estrutura for composta de materiais metálicos, nunca instalar os cabos próximos a fontes de energia eletromagnética como condutores elétricos, transformadores, motores elétricos, reatores de lâmpadas fluorescentes, estabilizadores de tensão, no-breaks, etc. É aconselhável que se deixe a distância mínima de 127 mm para cargas de até 2 KVA. Em ambientes que apresentem altos níveis de ruídos eletromagnéticos, recomenda-se que seja utilizada infra-estrutura metálica e totalmente aterrada para reduzir os riscos de interferências indesejáveis.

- **Acomodação** - Após o lançamento, os cabos UTP devem ser acomodados adequadamente de forma possam receber acabamentos, isto é, amarrações e conectorizações.

  A acomodação deverá obedecer aos seguintes cuidados:

1. Os cabos devem ser agrupados em forma de "chicotes", evitando-se trançamentos, estrangulamentos e nós. Devem ser amarrados com abraçadeiras plásticas, o suficiente para que possam permanecer fixos sem, contudo, apertar excessivamente os cabos.
2. Manter os cuidados tomados quando do lançamento, como os raios de mínimos de curvatura, torções, prensamento e estrangulamento.
3. Nas caixas de passagem deve ser deixada pelo menos uma volta de cabo contornando as laterais da caixa, para ser utilizada com uma folga estratégica para uma eventual manutenção do cabo.
4. Nos pontos de conectorização devem ser deixadas folgas nos cabos UTP, nas seguintes situações:
    a. Tomadas: Deve ser deixada folga de, no mínimo, 50 cm para conectorização e manobra do cabo.
    b. Racks e Brackets: Irá depender de cada situação, contudo é aconselhável que se deixe, no mínimo, 4 metros de cabo para conectorizações, acomodações e eventuais manutenções.
5. Nas terminações evitar que o cabo fique exposto, minimizando os riscos de o mesmo ser danificado acidentalmente.

- **Conectorização** - Os cabos UTP Cat.5 devem ser conectorizados com materiais apropriados e devem ser tomados os seguintes cuidados:
    1. Na conectorização ou qualquer outra situação, os pares trançados dos condutores não deverão ser destrançados mais que a medida de 13 mm. Na medida do possível, os cabos deverão ser destrançados e decapados o mínimo possível.
    2. No momento da conectorização, atentar para o padrão de pinagem dos conectores RJ-45 e patch panels (T568B).
    3. Após a conectorização, tomar o máximo cuidado para que o cabo não seja prensado, torcido ou estrangulado.

Caracterização do cabo de fibra óptica no projeto

A escolha da fibra óptica multimodo como mídia de distribuição do backbone veio atender às necessidades características das aplicações específicas do Campus. Para o cabeamento externo do backbone e conexões interedifícios do Campus fica mantido o cabo de fibra óptica de 62,5/125µm existente, pois este atende às condições da Norma. Fatores que influenciaram nesta escolha foram: flexibilidade, serviços suportados, vida útil do cabo, tamanho do local e população de usuários.

Para padronização da rede óptica existente no Campus de Três poços, é proposta a utilização de cabo de fibra óptica multimodo 62,5/125µm, com dois pares e construção do tipo *tigth buffer* para uso externo, em conformidade com o padrão TIA/EIA 492-AAAA e ISO 11801, para novos percursos de cabos e em substituição aos trechos de cabo óptico que apresentarem defeito.

Material

Trata-se de um cabo de fibra óptica multimodo 62,5/125µm, índice gradual, totalmente dielétrico, contendo quatro fibras e atenuação máxima de 3,0dB a 850nm e 1,0dB a 1.300nm, revestimento primário de acrilato, com 250µm de espessura e revestimento secundário de poliamida ou PVC com 900µm de espessura. Sobre o revestimento secundário são colocados elementos de tração de fios sintéticos (kevlar ou aramida) e capa externa de material termoplástico, não inflamável na cor preta.

Instalação

É um cabo que proporciona fácil conectorização com os conectores ópticos podendo ser instalados diretamente no cabo, sem a necessidade de acessórios especiais.

Tecnologias de LAN’s Ethernet (padrão IEEE 802.3)

Não estão previstas no escopo desse projeto as utilizações de outras tecnologias de LAN’s como FDDI, Token Ring e ATM, pois o objetivo é fundir as propostas aqui apresentadas com o projeto existente, utilizando as tecnologias de LAN’s semelhantes às que estão em uso.

Dessa forma, optou-se pela manutenção da atual tecnologia de camada de enlace Ethernet padrão IEEE 802.3, baseada no método de acesso CSMA/CD (Carrier Sense Multiple Access with Collision Detection), já existente no Campus do UniFOA, por esta oferecer facilidade de escalonamento superior e facilidade de gerenciamento. Aliado a esse fato está o aspecto de que a implementação de Ethernet a 100Mbps sobre o cabeamento óptico existente é uma solução mais escalonável e gerenciável do que a mudança para outra tecnologia como, por exemplo, o FDDI.

Migração para Fast Ethernet (padrão IEEE 802.3u)

As diversas redes do UniFOA já possuem instalados cabeamento UTP Cat.5, bem como interfaces de rede 10BASE-T nos equipamentos de rede. Estas redes apresentam uma boa performance a 10 Mbps mas não estão preparadas para novas aplicações como videoconferência e voz sobre IP.

Assim, a proposta é um upgrade da rede existente, com a migração para Ethernet 100BaseTX para cabeamento UTP e 100BaseFX para o cabeamento óptico, com a substituição aos dispositivos ativos de 10Mbps por dispositivos de rede de 10/100 Mbps, visto que estes podem trabalhar com base na infra-estrutura de cabos já existente, viabilizando o uso de elementos gerenciáveis de 100 Mbps.

O 100BaseTX foi escolhido porque utiliza as mesmas configurações de pares de fios e pinos do 10BaseT, facilitando assim a migração dos elementos de rede existentes.

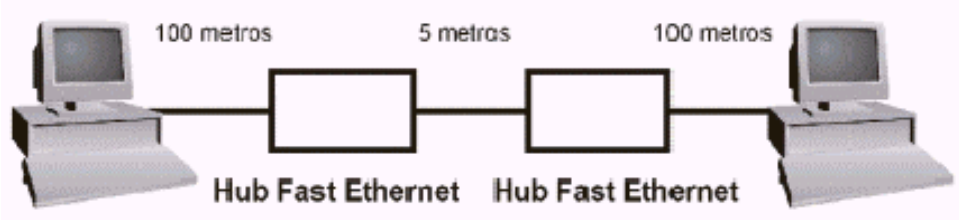
Para tornar a migração completa, recomenda-se a substituição dos hub’s e switches não gerenciáveis em uso por outros equipamentos "dual speed", gerenciáveis, disponíveis no mercado, permitindo a plena utilização e gerenciamento das conexões do Backbone.

O trecho do backbone baseado em fibra óptica operando com velocidades 10BASE-FL não podem ser integrados com os dispositivos que estão operando com velocidades 100BASE-FX. Para fazer a atualização, é necessário substituir os conversores de mídia e hub óptico utilizados.

Outro cuidado que deverá ser observado para o sucesso da migração é quanto às limitações de distância para Ethernet a 100Mbps em relação aos hubs utilizados. Na especificação de 100BaseT do IEEE, são definidos dois tipos de repetidores (hubs):

- Classe I – latência de 0,7 μseg ou menos e apenas um salto de repetidor;
- Classe II – latência de 0,46μseg ou menos e um ou dois saltos de repetidores.

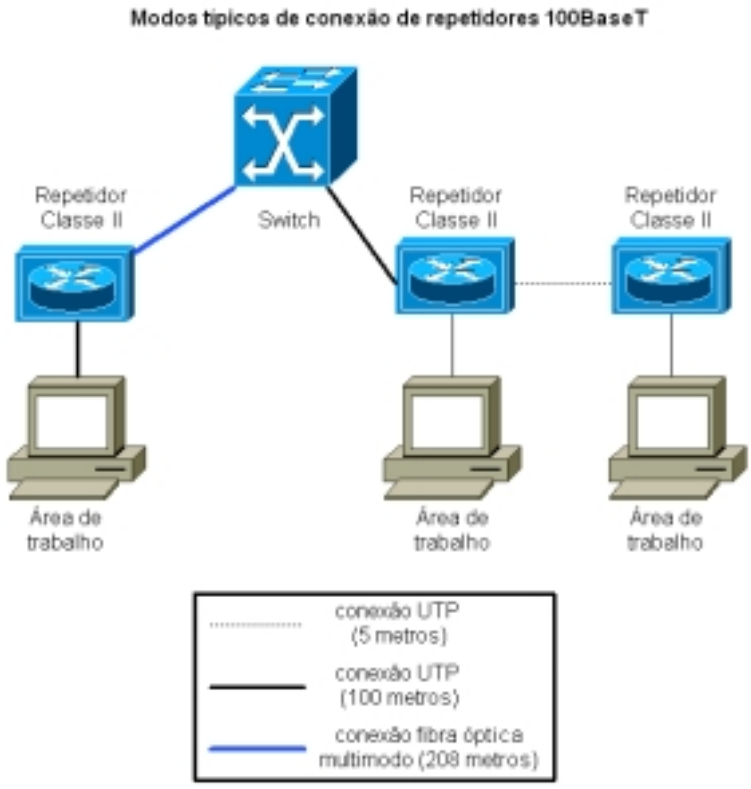
De acordo com a norma IEEE802.3u para redes Fast Ethernet 100 Mbps, a distância máxima de conexão com o Hub em 100BASE-TX é de 100 metros utilizando cabo par trançado (UTP) categoria 5. Quando conectar vários Hubs em série, não poderá existir mais do que dois Hubs 100 Mbps entre dois dispositivos de rede. A distância máxima do cabo entre dois dispositivos não pode exceder a 205 metros.



A tabela seguinte mostra o tamanho máximo de um domínio de colisões para Ethernet de 100Mbps, dependendo do tipo de repetidor e cabeamento usado.

	UTP	UTP e Fibra	Fibra Multimodo
DTE-DTE	100 metros	NA	412 metros
Repetidor classe I	200 metros	260 metros	272 metros
Repetidor classe II	200 metros	308 metros	320 metros
Dois repetidores classe II	205 metros	216 metros	228 metros

A figura seguinte mostra exemplos de conexões Ethernet 100BaseT



Convém salientar que, em muitos casos, durante a montagem dos Patch Cords existentes, podem não ter sido obedecidos os padrões de ligação estabelecidos por norma e, neste caso, quando a rede está trafegando a 10 Mbps não chega a apresentar problemas aparentes. Porém, quando são instalados equipamentos Ethernet 100Mbps e passa-se a exigir mais do cabeamento é neste momento que os problemas aparecem e alguns pontos da rede deixam de funcionar. Caracteriza-se assim que o problema não está relacionado ao equipamento ativo e sim aos padrões de ligação do cabeamento que foram configurados de maneira incorreta.

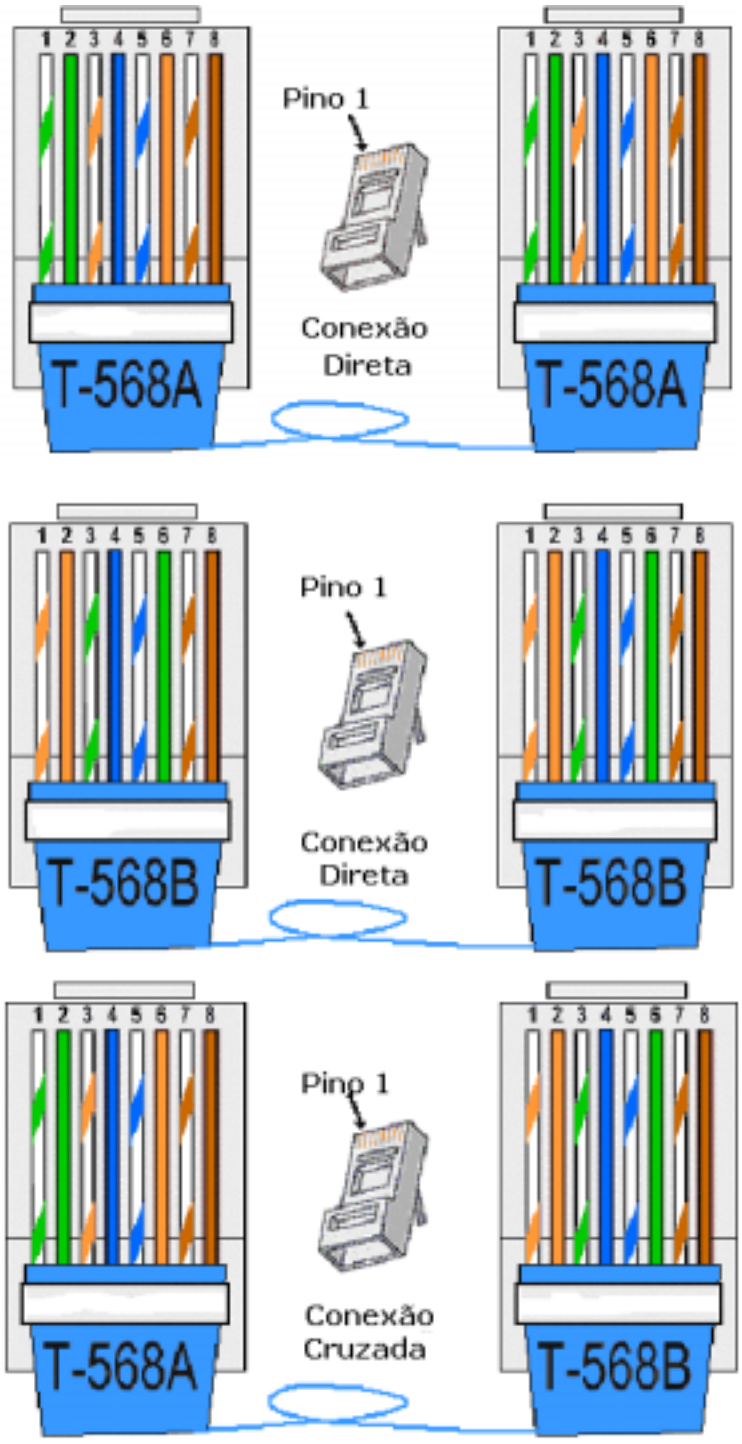
Conforme o item 6.2.4 da norma NBR 14565, são reconhecidos dois esquemas de ligação para os conectores padrão RJ-45, identificados na Norma como CM8V (Conector Modular de oito vias), denominados T568A e T568B. Somente estes dois esquemas de ligação são reconhecidos por norma e devem ser utilizados durante a conectorização do cabeamento da rede. As tabelas seguintes identificam a distribuição das ligações.

Ligação dos conectores CM8V – Padrão T568A		
COR	BORNE	PAR
Branco - Verde	1	3
Verde	2	
Branco - Laranja	3	2
Laranja	6	
Azul	4	1
Branco - Azul	5	
Branco – Marrom	7	4
Marrom	8	
OBS: Com a face superior do conector voltada para cima		

Ligação dos conectores CM8V – Padrão T568B		
COR	BORNE	PAR
Branco - Laranja	1	2
Laranja	2	
Branco - Verde	3	3
Verde	6	
Azul	4	1
Branco - Azul	5	
Branco – Marrom	7	4
Marrom	8	
OBS: Com a face superior do conector voltada para cima		

Para conexões DTE-DCE (computador-hub, por exemplo), deve-se optar pelo padrão T568B para ambas as pontas dos cabos. Para conexões DTE-DTE e DCE-DCE (hub-hub, por exemplo), optar pelo cabo cross-over, onde uma ponta do cabo utiliza padrão T568A e a outra ponta, padrão T568B.

Distribuição das conexões para o conector CM8V (RJ45)



OBS: Face superior do conector voltada para cima.

Pelo exposto anteriormente, recomenda-se que todas as conexões existentes nos patch cords existentes sejam verificadas e testadas e, caso não estejam de acordo com o estabelecido pela norma, devem ser refeitas para garantir o perfeito funcionamento de toda a rede.

Padrão 100BASE-SX

O padrão 100BASE-SX define a estratégia de migração da rede que funciona com taxas de transmissão de 10 Mbps em fibra óptica no Campus de Três Poços para uma rede a 100 Mbps utilizando a mesma infra-estrutura de cabeamento óptico existente e capaz de suportar aplicações com altas taxas de transmissão.

Este padrão define uma nova interface PMD (Physical Media Dependent), assim como um meio para implementar "auto negociação". O padrão proposto não define nada de novo acima da camada física. Pretende-se utilizar este padrão em conjunto com a norma IEEE 802.3 para prover uma completa definição. Acima da camada física, o padrão 100BASE-SX é o IEEE 802.3. Isto significa que este padrão vai trabalhar com todos os equipamentos Ethernet e Fast Ethernet que se encontram instalados nas redes locais do Campus.

CRITÉRIOS PARA SELEÇÃO DE DISPOSITIVOS PARA INTERLIGAÇÃO DE REDE DE CAMPUS

O mais simples dos equipamentos capazes de operacionalizar uma rede física, em concordância com as especificações anteriores, é o hub que, em conjunto com as placas de rede das estações, torna possível o intercâmbio de dados. Os hub's devem ter características mínimas de desempenho, capacidade de empilhamento, gerenciamento por SNMP e de segurança, tais como proteção contra intrusão e contra interceptação. Proteção contra intrusão significa que em cada porta do hub só será permitida a ligação de estações com o endereço físico Ethernet (MAC address) configurado na porta do equipamento. Proteção contra interceptação significa que um dado transmitido só será reconhecido e válido na porta configurada com o endereço físico Ethernet de destino (enviado junto com o cabeçalho da mensagem). Nas demais portas a mensagem não é reconhecida evitando-se assim, a monitoração do tráfego.

Outros equipamentos podem ser utilizados em conjunto com, ou em substituição aos hub's, quando existir a necessidade de melhor desempenho na transmissão, gerenciamento ou segurança. São diferenciados pela capacidade de processamento e pela camada do protocolo em que operam, sendo classificados como Bridges, Switches, Routers, etc.

➢ Comparação entre hubs, bridges, switches e routers

Hub's - Um hub, concentrador ou Multiport Repeater, nada mais é do que um concentrador de fiação. É um repetidor que promove um ponto de conexão física entre os equipamentos de uma rede. São equipamentos usados para conferir uma maior flexibilidade a LAN's Ethernet e são utilizados para conectar os equipamentos que compõem esta LAN.

O Hub é basicamente um pólo concentrador de fiação e cada equipamento conectado a ele fica num seguimento próprio. Por isso, isoladamente um hub não pode ser considerado como um equipamento de interconexão de redes, ao menos que tenha sua função associada a outros equipamentos, como repetidores.

Os Hub’s permitem dois tipos de ligação entre si. Os termos mais conhecidos no mercado para definir estes tipos de ligações são: cascateamento e empilhamento.

- Cascateamento: Define-se como sendo a forma de interligação de dois ou mais hub's através de portas de interface com a rede (RJ-45, BNC, etc).
- Empilhamento: Define-se como sendo a forma de interligação de dois ou mais hub’s através de portas especificamente projetadas para tal, ou seja, cada fabricante possui um tipo de interface. Desta forma, os hub’s assim empilhados se tornam um único repetidor.

Com o uso de hubs no backbone do UniFOA, o gerenciamento da rede é favorecido e a solução de problemas facilitada, uma vez que o defeito fica isolado no segmento da rede, bem como facilita muito a inserção de novas estações nas LAN’s existentes.

Os hub’s devem suportar empilhamento e suportar as MIBs (Management Information Base) – Base de Informação para Gerenciamento por SNMP.

Quando acontece de ocorrer muitas colisões, o hub permite isolar automaticamente qualquer porta (autopartição do segmento). Quando a transmissão do primeiro pacote é satisfatória, o hub faz uma reconfiguração automática do segmento. Os hubs mais comuns são os hubs Ethernet 10BaseT (conectores RJ-45) e eventualmente são parte integrante de bridges e roteadores.

Bridges - As Bridges ou pontes são equipamentos que possuem a capacidade de segmentar uma rede local em várias sub-redes, e com isto conseguem diminuir o fluxo de dados (o tráfego). Desta forma quando uma estação envia um sinal, apenas as estações que estão em seu segmento a recebem, e somente quando o destino esta fora do segmento é permitido a passagem do sinal. Assim, a principal função das bridges é filtrar pacotes entre segmentos de LAN’s.

As Bridges também podem converter padrões, como por exemplo, de Ethernet para Token-Ring. Porém, estes dispositivos operam na camada "interconexão" do modelo OSI, verificando somente endereços físicos (MAC address), atribuídos pelas placas de rede. Deste modo, os "pacotes" podem conter informações das camadas superiores, como protocolos e conexões, que serão totalmente invisíveis, permitindo que estes sejam transmitidos sem serem transformados ou alterados. As Bridges conseguem, como os repetidores, transferir quadros entre meios diferentes e, da mesma forma, esse procedimento é invisível para todos os usuários da rede.

As bridges se diferem dos repetidores porque manipulam pacotes ao invés de sinais elétricos. A vantagem sobre os repetidores é que não retransmitem ruídos, erros, e por isso não retransmitem frames mal formados. Um frame deve estar completamente válido para ser retransmitido por uma bridge.

São funções da Bridge:

- Filtrar as mensagens de tal forma que somente as mensagens endereçadas para ela sejam tratadas;
- Ler o endereço do pacote e retransmití-lo;
- Filtrar as mensagens, de modo que pacotes com erros não sejam retransmitidos;
- Armazenar os pacotes quando o tráfego for muito grande;
- Funcionar como uma estação repetidora comum.

A bridge atua nas camadas 1 e 2 do modelo de referência ISO/OSI, lendo o campo de endereços de destino dos pacotes de mensagens e transmitindo-os quando se tratar de segmentos de rede diferentes, utilizando o mesmo protocolo de comunicação.

As bridges atuam também como modelos passivos gerenciadores de rede, podendo coletar dados estatísticos de tráfego de pacotes para elaboração de relatórios. Por esse fato, a inclusão de softwares especiais (chamados agentes) nas bridges pode oferecer informações de volume de tráfego e erros da rede.

Switches – são uma evolução do hub, com funções de pontes e roteadores e hardware especial que lhe confere baixo custo e alta eficiência. Ele possui barramentos internos comutáveis que permitem chavear os seguimentos do backbone, tornando-o temporariamente dedicado a dois nós que podem assim usufruir toda capacidade do meio físico existente.

Em outras palavras, o switch permite a troca de mensagens entre várias estações ao mesmo tempo e não apenas permite compartilhar um meio para isso, como acontece com os hub´s. Desta forma estações podem obter para si taxas efetivas de transmissão bem maiores do que as observadas anteriormente.

A aquisição de um switch com maior capacidade de processamento e características de gerenciamento torna-se necessário devido às demandas por maiores taxas de transmissão e para melhor utilização dos meios físicos existentes.

Roteadores (routers) – O Roteador é o equipamento responsável pela interligação das redes locais no Campus entre si e redes dos sites remotos em tempo integral. Em outras palavras, permite que as máquinas de uma dada rede LAN comunique-se com máquinas de outra rede LAN remota, como se as redes LAN fossem uma só. Para isso, ele usa protocolos de comunicação padrão como PPP, TCP/IP, SPX/IPX, etc.

Têm a função de decidir o melhor caminho para os "pacotes" percorrerem até o seu destino entre as várias LAN's e dividem-nas logicamente, mantendo a identidade de cada sub-rede. Na prática os roteadores são utilizados para o direcionamento de "pacotes" entre redes remotas, atuando como verdadeiros "filtros" e "direcionadores" de informações. Recursos como "compressão de dados" e "spanning tree" (técnica que determina o percurso mais adequado entre segmentos, podendo inclusive reconfigurar a rede, em casos de problemas no cabo, ativando um caminho alternativo), compensam inconvenientes como velocidades de transmissão ao utilizarmos modems ou linhas privadas como meio de transmissão de redes remotas.

A tabela seguinte fornece um resumo das principais diferenças entre os hub's, Bridges, switches e routers.

EQUIPAMENTO	NÍVEL OSI IMPLEMENTADO	SEGMENTAÇÃO DA LARGURA DE BANDA	SEGMENTAÇÃO DOS DOMÍNIOS DE DIFUSÃO	DISTRIBUIÇÃO TÍPICA	RECUSROS ADICIONAIS
HUB	1	Todas as portas estão no mesmo domínio	Todas as portas estão no mesmo domínio	Conecta dispositivos individuais em LAN's	Particionamento automático para isolar nós com problemas
Bridge	1 e 2	Todas as portas estão no mesmo domínio	Todas as portas estão no mesmo domínio	Conecta redes	Filtragem de pacotes configurada pelo usuário
Switch	1 e 2	Cada porta define um domínio	Todas as portas estão no mesmo domínio	Conecta dispositivos ou redes individuais	Filtragem, recursos multimídia
Router	1 ,2 e 3	Cada porta define um domínio	Todas as portas estão no mesmo domínio	Conecta redes	Filtragem, firewalls, links WAN de alta velocidade, multicast, etc.

SELEÇÃO DE TECNOLOGIAS PARA REDES CORPORATIVAS

➢ Tecnologias de Acesso Remoto PPP

Para a tecnologia de acesso remoto do projeto da rede corporativa do UniFOA foi escolhido o PPP (Point-to-Point Protocol). Trata-se de um protocolo padrão da camada de enlace de dados para o transporte de diversos protocolos da camada de rede, através de links seriais ponto a ponto. Pode ser usado com ISDN, linhas analógicas, linhas dedicadas digitais e outras tecnologias, fornecendo os seguintes serviços:

- Multiplexação de protocolos da camada de rede;
- Configuração de link;
- Teste de qualidade de links;
- Negociação de opções de link;
- Autenticação;
- Detecção de erros.

A camada física se baseia em padrões internacionais para comunicações seriais como, por exemplo, o EIA/TIA-232.

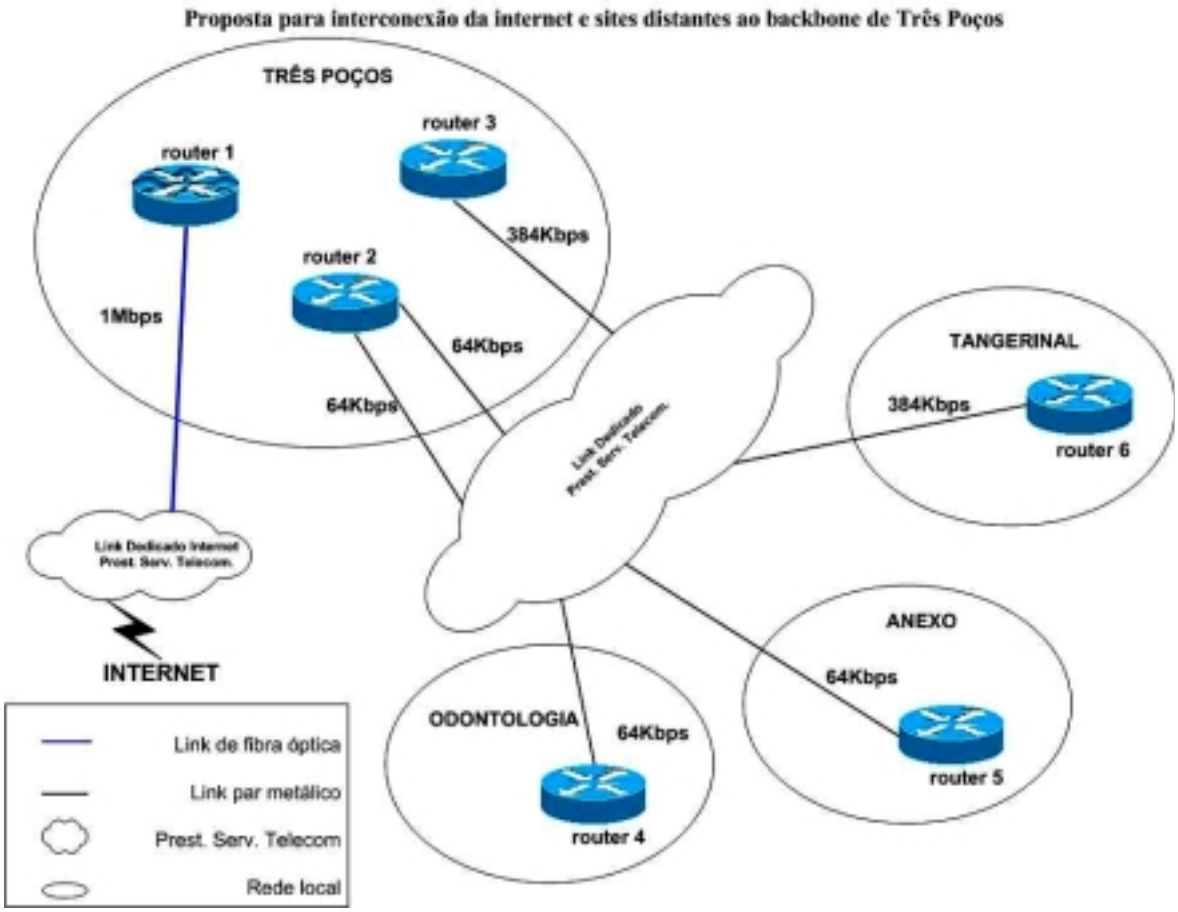
O PPP é muito usado em ISDN (Integrated Services Digital Network), que é um serviço de transporte de dados digitais oferecidos pelas operadoras de telecomunicações. O PPP proporciona encapsulamento de dados, integridade de links e autenticação para serviços ISDN.

➢ Linhas dedicadas

Faz-se a opção por linhas dedicadas para a conexão do Campus de Três Poços com os sites distantes. A empresa de telecomunicações deverá fornecer um meio e equipamentos para o tráfego de dados em alta velocidade entre os seguintes pontos:

- Campus de Três Poços e Tangerinal, com largura de banda de 384Kbps;
- Campus de Três Poços e Odontologia, com largura de banda de 64Kbps;
- Campus de Três Poços e Anexo, com largura de banda de 64Kbps.

Para a conexão do Campus de Três poços e Internet, faz-se uma opção por contratação de link dedicado em fibra óptica, com redundância do serviço de conexão e largura de banda de 1Mbps.



- Seleção de dispositivos de acesso remoto e para o site central

O nó central, situado no Campus de Três Poços, deverá incluir servidor de acesso remoto com serviços de nó remoto, que irão aceitar os pedidos de conexão dos sites remotos, permitindo que seus usuários se conectem à rede central simultaneamente possibilitando o acesso aos serviços de rede mesmo que não estejam ligados diretamente a ela, como no caso dos sites remotos.

- Ênfase para a seleção de switches e roteadores WAN

Para a seleção dos roteadores que farão a interligação dos sites ao nó central da rede, faz-se a opção pelo remanejamento dos equipamentos atualmente em uso no Campus de Três Poços e demais sites distantes uma vez que os mesmos atendem ao objetivo do projeto.

Quanto aos switches, recomenda-se a compra de equipamentos destinados a WAN's. Os switches de WAN's devem ter memória e capacidade de processamento suficiente para controlar o elevado tráfego e os recursos de otimização da rede.

Deve-se optar por switches com características que facilitem a redundância e a repetição rápida e automática do roteamento em caso de falha e gerenciamento automático das conexões.

- Seleção de um provedor de serviços WAN

Na a seleção do(s) provedor(es) de serviço de WAN, para a contratação dos serviços de interligação dos sites e Internet, devem ser levados em conta os seguintes critérios:

1. A extensão dos serviços e tecnologias oferecidas;
2. Área de cobertura geográfica do provedor;
3. Características da rede interna do provedor;
4. Os níveis de segurança oferecidos;
5. O suporte técnico proporcionado.

Contratação do SLA – Service Level Agreement ou Acordo de Nível de Serviços, para definir os termos específicos do serviço e como este será medido e garantido.

O SLA também deve especificar o nível de suporte técnico. No caso do UniFOA propõe-se um SLA com suporte 24hs, sete dias por semana para o serviço de Internet e conexões do nó central de Três poços com os sites remotos do Tangerinal, Odontologia e Anexo.

FASE 4 – TESTES, OTIMIZAÇÃO E DOCUMENTAÇÃO DO PROJETO DE REDE

Determinação do escopo de um sistema protótipo

Como o projeto FastFOA tem como objetivo a proposta de melhorias e melhor utilização dos recursos do backbone atualmente existente no UniFOA, não foi adotado um sistema protótipo.

A seleção dos procedimentos de testes e das ferramentas para monitoração da rede backbone foi feita segundo as metas propostas pelo projeto, incluindo os seguintes objetivos:

1. Verificar que o projeto atende aos objetivos de melhoria da rede atual;
2. Validar as tecnologias escolhidas e as seleções dos dispositivos;
3. Identificar gargalos ou problemas de conectividade;
4. Analisar os efeitos de falhas de links de rede sobre o desempenho do backbone;
5. Monitoração e análise dos efeitos da atualização dos links e dispositivos da rede do backbone de Três Poços em relação ao desempenho (análise condicional). A monitoração das modificações da rede deve ser contínua para verificar que satisfazem os requisitos propostos;
6. Identificar riscos que possam impedir a implantação do projeto e fazer planos de contingência.

➢ Objetivos dos testes e critérios de aceitação

- Medir o tempo de resposta dos aplicativos de rede atualmente em uso no Campus e demais sites, durante as horas de pico de utilização (horário do expediente administrativo). O critério de sucesso e aceitação é a melhoria do tempo de resposta em, pelo menos 50% dos valores obtidos na medição da rede atual;

- Medir o período de tempo para que um usuário da Internet receba uma determinada página, solicitada via browser. O critério de aceitação é que o período de tempo para exibição dessa página seja visualmente menor que o atual.
- Medir a taxa de colisões nos seguimentos Ethernet entre backbone e redes locais e comparar os resultados com uma medição de linha de base da rede atual. O critério de aceitação é haver 25% menos colisões do que ocorre hoje.
- As informações para linha de base serão obtidas a partir da utilização de ferramentas nativas das aplicações em uso e auxílio de analisadores de protocolos e redes para examinar os tamanhos de estruturas atuais e após a implementação das mudanças.

➢ Ferramentas para testes

1. Analisador de protocolos – captura de tráfego de rede, decodificação de pacotes e estatísticas;
2. Ferramentas para monitoração remota – Probes RMON, com resultados obtidos por SNMP, para levantamento estatístico da rede, com análise de CRC, colisões nos segmentos Ethernet, taxa de tráfego em cada interface e taxa de broadcast.
3. Utilização do modelo Cliente-Servidor para determinar o tráfego da nova rede.

➢ Documentação da rede

Com o objetivo de documentação da rede, a proposta é relacionar as informações referentes ao cabeamento, software e hardware utilizado para a conexão do backbone com as redes locais do Campus de Três Poços e sites distantes. Para esse fim sugere-se a criação de documentação específica com as informações referentes ao inventário do hardware e software existente, da localização do cabeamento, armários e outros recursos de rede.

Também é sugerida a criação de um sistema de gerenciamento de chamadas de suporte através da intranet do UniFOA, com a finalidade de se criar um banco de dados com registros que possibilitarão a solução de problemas futuros, servindo inclusive, como ferramenta de treinamento para os novos colaboradores encarregados da solução dos problemas ligados à rede.

- Material necessário para implementação das mudanças na rede

Na tabela seguinte encontram-se relacionados os materiais necessários para a implementação das modificações propostas pelo projeto FastFOA para o backbone do UniFOA em Três Poços e demais sites distantes.

Descrição	Fabricante	Unidade	Quant.	Custo unitário R$	Custo total R$
Cabo de fibra óptica multimodo tipo thight duplex para uso geral	Black Box	Bobina de 300m	1	717,00	717,00
Conversor de mídia 10/100Mbps multimodo com detecção automática	Black Box	Peça	22	383,00	8426,00
Hub 10/100Mbps – 4 portas	3Com	Peça	13	261,00	3393,00
Switch PowerConnect – camada 3 - 3024	DELL	Peça	1	4610,00	4610,00
Cabo UTP cat5 flexível 24AWG capa azul	Belden	Bobina de 300m	1	148,00	148,00
Cabo UTP cat5 flexível 24AWG capa verde	Belden	Bobina de 150m	1	148,00	148,00
Cabo UTP cat5 flexível 24AWG capa vermelho	Belden	Bobina de 150m	1	148,00	148,00
Cabo UTP cat5 flexível 24AWG capa amarelo	Belden	Bobina de 150m	1	148,00	148,00
Cabo UTP cat5 flexível 24AWG capa violeta	Belden	Bobina de 150m	1	148,00	148,00
Conector modular CM8V (RJ45)	Black Box	Pcte c/ 25	12	17,00	204,00
Capa para conector RJ 45 cor azul	Black Box	Pcte c/ 50	1	16,00	16,00
Capa para conector RJ 45 cor verde	Black Box	Pcte c/ 50	1	16,00	16,00
Capa para conector RJ 45 cor vermelho	Black Box	Pcte c/ 50	1	16,00	16,00
Capas para conector RJ 45 cor amarelo	Black Box	Pcte c/ 50	1	16,00	16,00
Capas para conector RJ 45 cor violeta	Black Box	Pcte c/ 50	1	16,00	16,00

CONCLUSÃO

A implementação das melhorias para o backbone da rede de computadores do UniFOA, propostas neste projeto, dará à instituição a base para um ambiente estável e dinâmico, oferecendo condições para um crescimento modular e estruturado das redes atualmente existentes, possibilitando a interconexão de todas as redes locais da instituição, com a racionalização da aplicação dos recursos existentes, preservando os investimentos já feitos, bem como servindo de base para a implantação de novas redes de computadores.

Como benefício em curto prazo, poderão ser oferecidos serviços mais eficientes aos alunos e colaboradores da instituição, com maior agilidade na área acadêmica e nos serviços internos e administrativos no Campus de Três Poços e sites distantes do Tangerinal, Odontologia e Anexo.

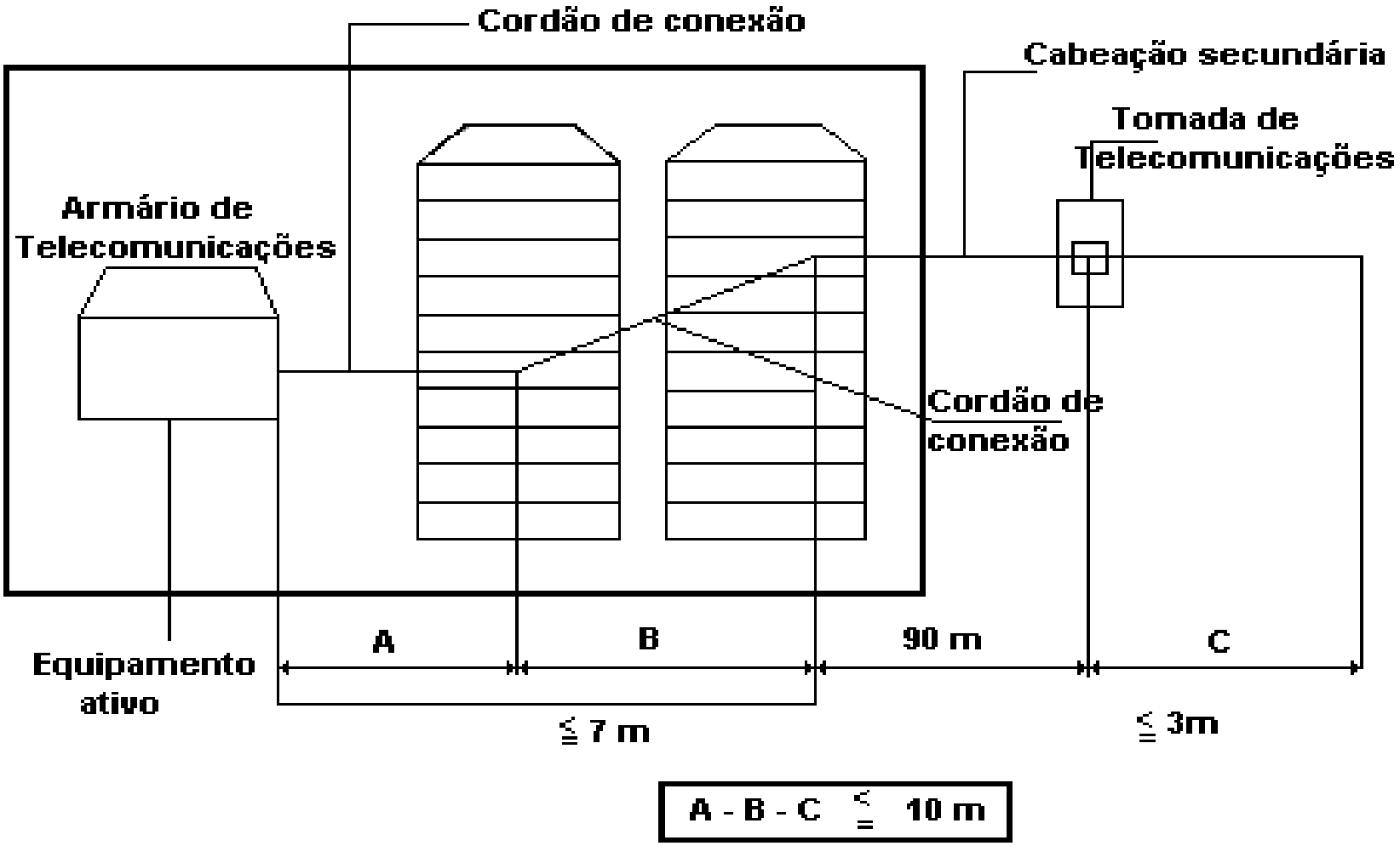
O retorno do investimento poderá ser medido pelo grau de satisfação dos usuários dos serviços de rede e Internet, bem como pela entrada de novos alunos, baseada nas referências positivas dos serviços prestados pela instituição.

REFERÊNCIAS BIBLIOGRÁFICAS

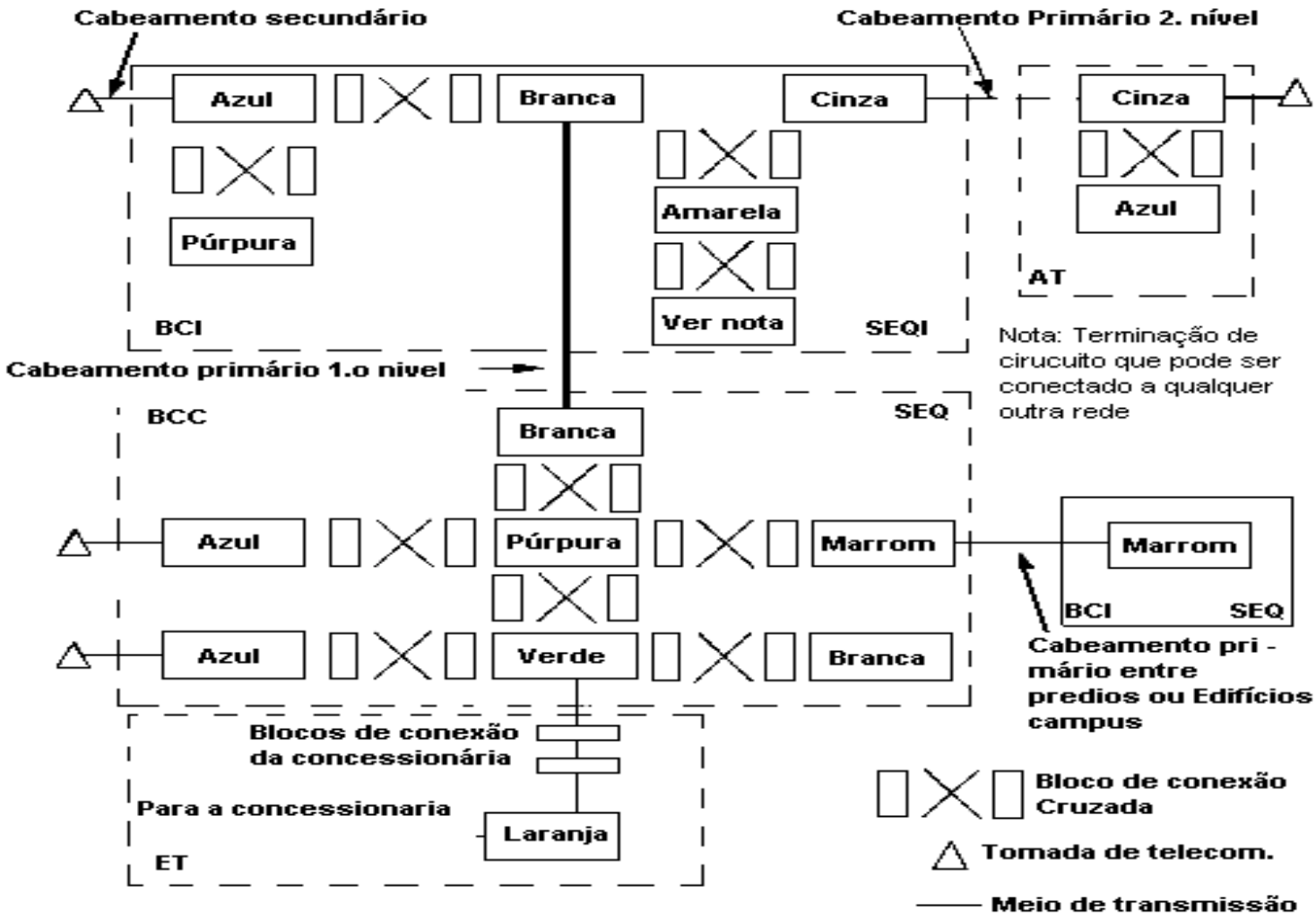
- OPPENHEIMER, Priscila “Projeto de Redes Top-Down” Rio de Janeiro: Campus, 1999
- CAMPBELL, Patrick T. “Instalando Redes em Pequenas e Médias Empresas” São Paulo: Makron Books, 1997
- GASPARI, Anteu Fabiano L./ BARRELLA, Francisco Eugênio/ BORTOLLI, Luis Fernando de/ DAL’BÓ, Paulo Henrique “Projetos para Redes Metropolitanas e de Longa Distância” São Paulo: Érica, 1999
- JR, Frank J. Derfler e FREED, Les “Tudo Sobre Cabeamento de Redes” Rio de Janeiro: Campus, 1994
- NBR 14565 “Procedimento Básico para Elaboração de Projetos de Cabeamento de Telecomunicações para Rede Interna Estruturada” Rio de Janeiro: ABNT, 2002
- PINHEIRO, José Mauricio dos Santos “Apostila de Noções Básicas de Redes Estruturadas” Rio de Janeiro: MetroRED Telecomunicações LTDA, 2002
- SOARES, L.F./SOUZA, G.L./COLCHER, S. “Redes de Computadores – Das LAN’s, MAN’s e WAN’s às Redes ATM” Rio de Janeiro: Campus, 2000

ANEXOS

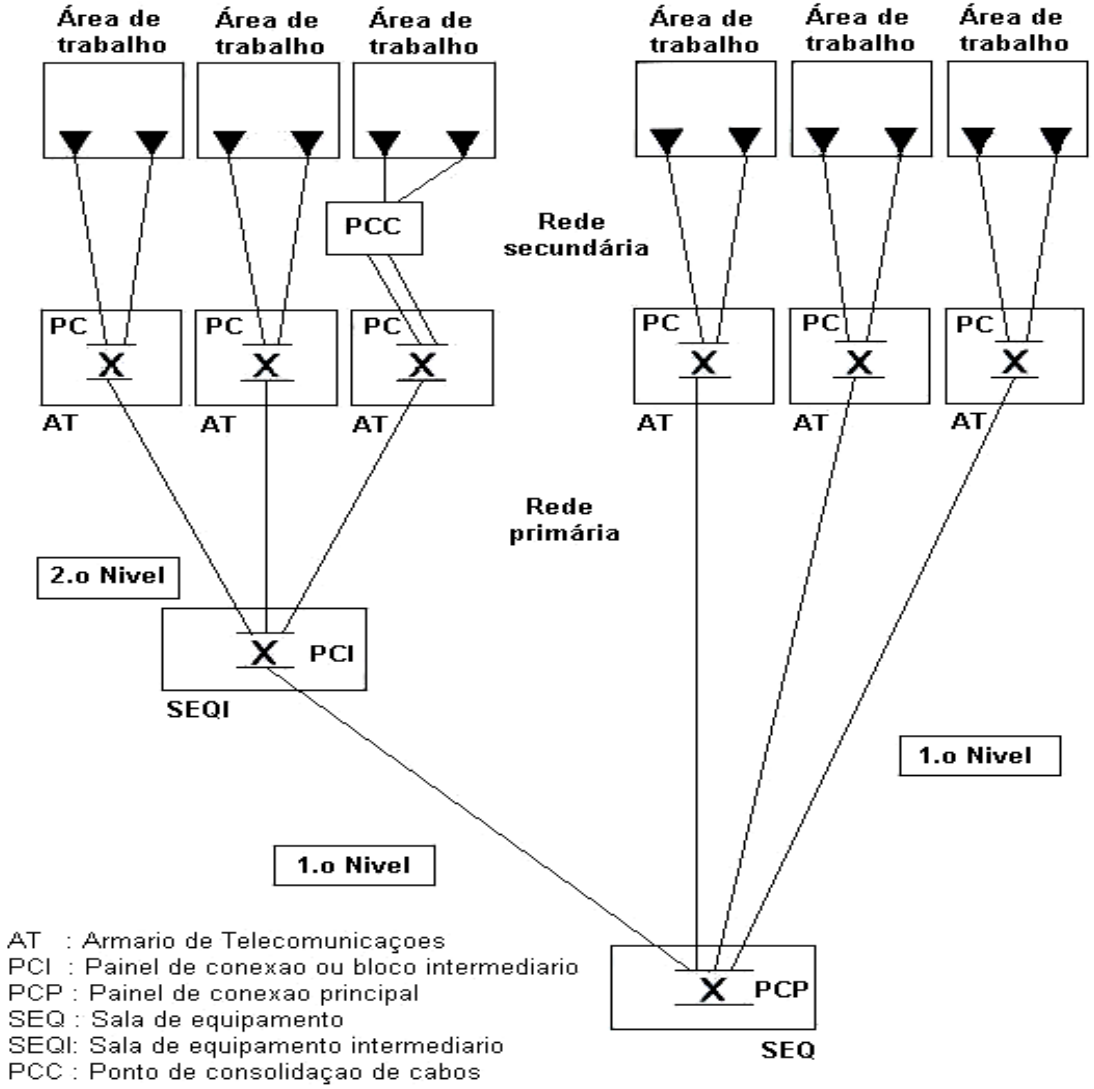
Anexo 1 - Distâncias admitidas para o cabeamento interno



Anexo 2 - Identificação das terminações do cabeamento



Anexo 3 - Elementos construtivos da rede primária



Alexandre B. Domingues	alexandre.domingues@foa.org.br
Christian Luiz Mansur	Alexandre B. Domingues
José Mauricio Santos	Alexandre B. Domingues
Marcos Leite Santos	Alexandre B. Domingues
Savio A. Almeida	Alexandre B. Domingues