Flávio Lemos

Metodologia de Organizações Virtuais Aplicada ao Desenvolvimento do Produto em Empresas de Grande Porte

São Paulo

2007

Flávio Lemos

Metodologia de Organizações Virtuais Aplicada ao Desenvolvimento do Produto em Empresas de Grande Porte

Trabalho de Conclusão de Curso apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do Titulo de Mestre em Engenharia Automotiva.

São Paulo

2007

Flávio Lemos

Metodologia de Organizações Virtuais Aplicada ao Desenvolvimento do Produto em Empresas de Grande Porte

Trabalho de Conclusão de Curso apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção de Titulo de Mestre em Engenharia Automotiva.

Área de Concentração:
Engenharia Automotiva

Orientador: Prof. Dr. Marcelo Massarani

São Paulo

2007

DEDICATÓRIA

A minha esposa Simone Maistro pelo companheirismo e dedicação em todas as nossas aventuras, assim como a compreensão e motivação que transmitiu por todos estes anos em que convivemos.

Aos meus pais que sempre me incentivaram a seguir em frente independente das dificuldades encontradas no caminho, o que me trouxe com sucesso a ser quem hoje sou.

AGRADECIMENTOS

Ao Professor Doutor Marcelo Massarani pela orientação e constante estímulo à pesquisa e conclusão deste trabalho.

As empresas UGS e General Motors do Brasil pelo suporte dado.

RESUMO

O objetivo deste trabalho é de elaborar uma metodologia de trabalho, fundamentada nos procedimentos das Organizações Virtuais, que possibilite o desenvolvimento de um projeto com engenharias dispersa geograficamente trabalhando simultaneamente sem que a sinergia seja prejudicada. Desta forma os métodos aqui abordados requereram um forte apelo da tecnologia disponível, porém sem a necessidade de se criar algo novo, com exceção dos métodos de interação entre grupos. Para viabilizar tais métodos serão definidos os meios de comunicações e aplicativos capazes de unir os grupos de forma eficiente, segura e de rápida configuração que mantenham a mesma sinergia de trabalho daqueles que atuam nas formas convencionais.

Palavras chaves: Organização Virtual. Rede de Cooperação. Trabalho Remoto.

ABSTRACT

The Purpose of this work will be development a work methodology for projects that have the engineering groups located in different places and keeping the same synergy of groups that work locally as the regular way of the project development. This concept of work will be based in the Virtual Organization methodology and use the full power of the technology and software that we have available without invent any new tools for this purpose. To create these procedures will be study the networks and software available to connect the remote sites and offer reliability and security keeping the synergy of work.

Keyword: Virtual Organization. Network Engineering. Remote Access.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AH	*Authentication Header*
ADSL	*Asymmetric Digital Subscriber Line*
CAD	*Computer Aid Design*
DHCP	Sistema Automático de endereçamento IP para computadores conectados em rede
DMU	*Digital Mockup*
ESP	*Encapsulating Security Payload*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
IPv4	*IP internet protocol version 4*
IPv6	*IP internet protocol version ;*
ISAKMP	Mecanismo de troca de chaves para redes privadas virtuais que gerencia a troca de chaves de criptografia
ISP	*Internet Service Provide*
LAN	*Local Area NetWork*
Links	Conexão lógica entre computadores dispostos em rede
NAP	*Network Access Point*
NetBEUI	Extended User Interface
PLM	*Product Lifecycle Management*
PPP	*Point-to-Point Protocol*
TCP/IP	*Transmission Control Protocol / Internet Protocol*

VPN	*Virtual Private NetWork*
WAN	*Wide Area Network*

SUMÁRIO

1. Introdução

Observando algumas empresas detentoras de sistemas corporativos de informática nota-se que o percentual de uso pela capacidade disponível é baixo. Aspectos culturais como: métodos tradicionais de desenvolvimento do produto, receio sobre a segurança e o sigilo do projeto, são alguns dos fatores que impedem a otimização de uso dos sistemas.

As Empresas para manter-se competitiva e suportar a pressão global do mercado, devem buscar fornecedores que lhe tragam melhor qualidade, menor preço e tempo de desenvolvimento. Para obter a melhor relação entre estes itens, a nomeação do fornecedor não deve ser limitada à cidade ou país onde a sede da empresa está instalada. Fornecedores de outras localidades, não importando a distância em que eles se encontram, devem ser considerados. Isso pode ser um fator que aumente o tempo de desenvolvimento do produto e prejudique a sinergia de trabalho no desenvolvimento do produto nos moldes convencionais de projeto. A sinergia será maior quanto melhor forem os meios de comunicação e ferramentas utilizadas para a troca de informação. Estes meios estão disponíveis na maior parte das empresas. O objetivo é otimizar o percentual de uso da tecnologia instalada adicionando aplicativos, *softwares,* de gerenciamento e comunicação disponíveis no mercado, possibilitando a introdução de um novo conceito de desenvolvimento do produto. De acordo com Clegg; Hardy e Nord (1999) está ocorrendo a transição da burocracia para a fluidez nas novas formas organizacionais.

A aplicação do conceito de Organizações Virtuais pode criar uma metodologia de trabalho para empresas de médio e grande porte que otimize a troca de informações pelos meios de comunicação já existente. Do ponto de vista institucional a empresa virtual é uma combinação das melhores competências essenciais de empresas (PRAHALAD; HAMEL, 1995).

A criação de uma rede estratégica de colaboração, tendo como nodos os fornecedores centralizando o trabalho no cliente, possibilita a busca das melhores competências a nível global. São necessários conceitos organizacionais que

permitam obter o tamanho ou capacidade (virtual) necessária para aumentar os recursos acessíveis, sem perder a flexibilidade (PRAHALAD; HAMEL 1995).

Como resultado terá o projeto sendo desenvolvido sobre a ótica da Engenharia Simultânea a nível global.

O primeiro estudo para implementação deste conceito é a escolha dos meios em que a informação irá trafegar. Dados os diversos meios de conexão entre *sites,* a escolha objetivará as topologias de redes mais comuns para assegurar a compatibilidade com a maioria das empresas, viabilizando assim, o maior número possível de colaboradores na rede. Estes meios deverão atender o requisito de velocidade mínima de transferência de dados, requerida pelos aplicativos utilizados na rede, para não haver degradação da comunicação e perda da sinergia no trabalho.

Definido os meios e a velocidade mínima de transferência de dados, o próximo passo é a escolha dos protocolos de segurança que irão empacotar as informações em tráfego. Mesmo que os dados fluam por redes públicas, o nodo da rede de colaboração conectado ao cliente deverá ter uma conexão segura.

A sinergia de trabalho a distância será suportada pela escolha de um *software* de conferência e acesso remoto que possibilite a interação entre os fornecedores e o cliente manipulando as informações em tempo real, permitindo interatividade em ambos os lados e seja compatível com os requisitos dos sistemas que estão sendo acessados.

Por esta rede, assim definida, os dados poderão trafegar de maneira segura e eficiente independente da posição geográfica do fornecedor em relação ao cliente. Os dados a serem compartilhados serão centralizados no cliente, sendo que o sistema a ser instalado no cliente deverá gerenciar o controle de acesso, permitindo que o fornecedor tenha direitos de visualização somente das peças que interagem com a que ele está produzindo para garantir o sigilo do projeto como um todo.

O objetivo deste trabalho é otimizar o uso das ferramentas de tecnologia da informação em empresas de grande porte embasada na metodologia de trabalho das Organizações Virtuais, cujos conceitos serão brevemente expostos. Propondo o

desenvolvimento do projeto sob a ótica da Engenharia Simultânea dispersa geograficamente, porém com a mesma sinergia de trabalho de um grupo instalado em um mesmo ambiente. Para assegurar está sinergia será realizada uma análise de domínio com a proposta de uma rede de colaboração, baseada no modelo apresentada por Fuks e Assis (2001), que alicerçara a metodologia de trabalho e auxiliará na identificação dos pontos críticos dos métodos e tecnologia a serem aplicados. Definida as bases conceituais de trabalho passa-se a escolha da tecnologia da comunicação a ser empregada, meios e compatibilidade. Na camada superior estará os aplicativos de comunicação e conferência, gerenciamento e acesso remoto a sistemas. Esses aplicativos serão balanceados com a velocidade de transmissão do meio definindo assim o máximo em aplicativos pela menor velocidade de transmissão do meio admissível.

2. Conceitos de Organizações Virtuais

As Organizações Virtuais é um novo modelo organizacional que utilizam a tecnologia para unir, de forma dinâmica, pessoas, bens e idéias sem, todavia, ser necessário reuni-las em um mesmo espaço físico e/ou ao mesmo tempo (BERTO, 1997).

Suas metodologias aplicadas a empresas de médio e grande porte podem assegurar a flexibilidade e sinergia de trabalho à distância.

O uso da tecnologia da Informação permite que parceiros de cooperação dispersos geograficamente interajam como se estivessem dentro de uma mesma sala de trabalho.

Uma Organização Virtual se refere à coleção temporária ou permanente de indivíduos, grupos, ou unidades organizacionais dispersas geograficamente – que pertençam ou não a uma mesma organização ou organizações no seu todo que dependem de *links* eletrônicos com a finalidade de completar as tarefas ou negociações (ZIMMERMANN, 1997).

A Tecnologia da Informação permite que as corporações não vejam as barreiras de tempo e localização. Como resultado, estas novas formas organizacionais evoluem, e os limites organizacionais são redefinidos.

A comunicação e a rápida troca de informações desempenham um papel essencial na habilitação das companhias que cooperam para responder efetivamente às necessidades dos consumidores. Na concepção de Goldman; Nagel e Preiss (1995) dinamismo é um termo abrangente. Na economia dinâmica e de tempo real de hoje, o recurso gerencial mais importante é a informação. Portanto, deve-se ter uma Tecnologia da Informação que ofereça e dê suporte aos seguintes itens: Concluir transações sem considerar tempo e lugar; criar idéias, conhecimento e confiança mútuos através do compartilhamento da informação e comunicação intensa, com baixo custo; projetar ou re-projetar e coordenar processos distribuídos globalmente; melhorar os relacionamentos entre os parceiros que cooperam bem como com consumidores através do fornecimento de informações atuais e relevantes.

Um outro termo bastante difundido na literatura das Organizações Virtuais é *Core Competency*, que significa competência central ou maior. O termo *Core Competency* se refere a uma habilidade única para uma companhia, que não é facilmente reproduzida pelos seus competidores. Por isso, a Organização Virtual tende a ser a melhor, pois reunirá as *Core Competencies* de todas as empresas que a compõe. Alguns exemplos dessas competências compreendem habilidades organizacionais e tecnológicas, mas também podem incluir recursos humanos, conexões de redes e infra-estrutura.

Existem duas condições necessárias para uma Organização Virtual existir (TRAVICA, 1997):

- Dispersão geográfica das unidades da organização;
- *Link* da tecnologia da informação nos processos de produção e desenvolvimento de projetos.

Ambas as condições são de caráter estrutural. A primeira define Organização Virtual como uma organização dispersa espacialmente com dispersão de indivíduos, grupos, departamentos, companhias no seu todo, em no mínimo duas localizações diferentes. A segunda condiciona o processo de produção na Organização Virtual ao auxílio do suporte da Tecnologia da Informação para a ligação das partes dispersas. As novas tecnologias da informação (internet, intranets, e outras), assim como as novas formas de organização inter-empresas, estão se convergindo no sentido de reforçarem modelos de cooperação, alianças estratégicas e redes internas e externas às empresas, onde se valoriza mais a empresa flexíveis, em que as fronteiras da organização ficam menos nítidas (LEÓN, 1998; SCHWARTZ et al., 1997).

2.1. Características Identificadoras das Organizações Virtuais

As características identificadoras das Organizações Virtuais são bem definidas e exploradas em diversas literaturas que tratam deste assunto, será citada aqui algumas delas mais relevantes a aplicação da metodologia proposta em empresas de médio e grande porte que venham otimizar a sinergia do trabalho a distância (LEÓN, 1998; SCHWARTZ et al., 1997; ZIMMERMANN, 1997);

- Podem rapidamente aproveitar as oportunidades, devido à maior facilidade de configuração;
- Ligam competências centrais e complementares e desta forma conseguem atingir a excelência;
- Aumentam as facilidades e tamanho percebido (uma companhia pequena pode usar uma Organização Virtual para aumentar suas capacidades e permitir-se competir para oportunidades maiores que ela poderia, de outra forma, perder.);
- Ganham acesso a novos mercados e compartilham o mercado atual;
- Requer o uso de todo o potencial da tecnologia;
- Baseiam-se na confiança e na interdependência entre os parceiros;
- Não possuem fronteiras rígidas como as organizações tradicionais;
- A excelência, onde cada parceiro se coloca e contribui através do que sabe fazer melhor;
- O senso de oportunidade, fundamental para a realização dos negócios e das parcerias virtuais;
- A confiança e a confiabilidade recíprocas, que dá sentido e corpo ao lastro técnico e gerencial reunido entre parceiros e clientes;
- A ausência de fronteiras, que lhe atribui a facilidade de reunir competências complementares fisicamente dispersa;

- A cultura, que equilibra a ausência de limites muito bem definidos entre as empresas da rede, mais apropriadamente chamada de teia, pelas muitas formas e lugares passíveis de realização;
- A informação, cujo poder de transformação é imprescindível no apoio à toda a dinâmica e movimentação das Organizações Virtuais;

2.2. Organização Virtual e suas metodologia em uma empresa convencional

Uma empresa virtual é como uma rede onde os nodos estão representados por uma área de especialidade, no caso de grandes organizações pode-se também ver como uma de suas divisões ou um fornecedor trabalhando em parceria. A especialidade pode ser contribuída por empresas ou pessoas. Todas as habilidades e conhecimento levados juntos fazem à empresa virtual ou está metodologia aplicada a empresas convencionais, completa para a tarefa que ela executa no desenvolvimento de um projeto.

A moderna Tecnologia da Informação permite que os nodos ou centros de prestação de serviço, estejam espalhados por todo mundo.

Os nodos de uma organização pode se concentrar na sua área de especialidade deixando as funções que faltam serem manipuladas por outros nodos. Através do processo de focalizar um tipo particular de produto ou serviço, a competitividade e lucro podem ser maximizados, fato que pode ser aplicado ao desenvolvimento do produto sob a ótica da Engenharia Global.

Desde que um nodo se concentre no que ele faz melhor e só existe para fornecer essa função, é muito natural ser parte de várias Organizações Virtuais ao mesmo tempo ou um fornecedor tenha vários clientes geograficamente dispersos. Visto pelo cliente, a necessidade por um produto ou serviço pode ser rapidamente preenchido com adição, pela metodologia da Organização Virtual, por parceiros escolhidos pela sua competência, não mais pela localização.

A cada empresa é permitido concentrar-se na sua área de especialidade e esforçar-se para ser a melhor neste campo. Isso significa que uma corporação virtual poderia realmente adquirir as melhores competências disponíveis para cada função e, por conseguinte criar uma organização "*worldclass*". Do ponto de vista institucional a empresa virtual é uma combinação das melhores competências essenciais de empresas (PRAHALAD e HAMEL, 1995).

Uma corporação virtual pode ser extremamente flexível e adaptável. As habilidades ou funções que estiverem faltando podem ser facilmente obtidas através da adição de uma outra empresa que possua essas habilidades disponíveis, e é onde uma organização tradicional deveria ter de reconstruir fábricas para ajustar a produção para as demandas do mercado, enquanto que uma Organização Virtual poderia somente reestruturar sua organização através da contratação de um parceiro adequado.

3. Análise do Domínio – Rede de Colaboração

O desenvolvimento de um projeto é uma ação de trabalho colaborativo. Não é possível imaginar os membros do grupo atuando individualmente. Em um grupo pode ocorrer à complementação de capacidades, de conhecimentos e de esforços individuais, e a interação entre pessoas com entendimentos, pontos de vista e habilidades complementares (FUKS; GEROSA e LUCENA, 2002). Quando o time está situado dentro da empresa, a inter-relação pessoal facilita para que o grupo atue de forma colaborativa conforme os conceitos de Fuks; Gerosa e Lucena (2002). Está interação é responsável por identificar precocemente inconsistências e falhas em seu raciocínio e, juntos, podem buscar idéias, informações e referências para auxiliar na resolução dos problemas. Ao transpor este ambiente de trabalho para uma metodologia de trabalho distribuído geograficamente, a sinergia de grupos de trabalho pode ser comprometida pela falta da interação pessoal.

Um passo antes de definir e introduzir a tecnologia da informação que possibilitara a interação entre os grupos geograficamente dispersos, é definir o domínio por uma rede de colaboração em que o grupo irá atuar.

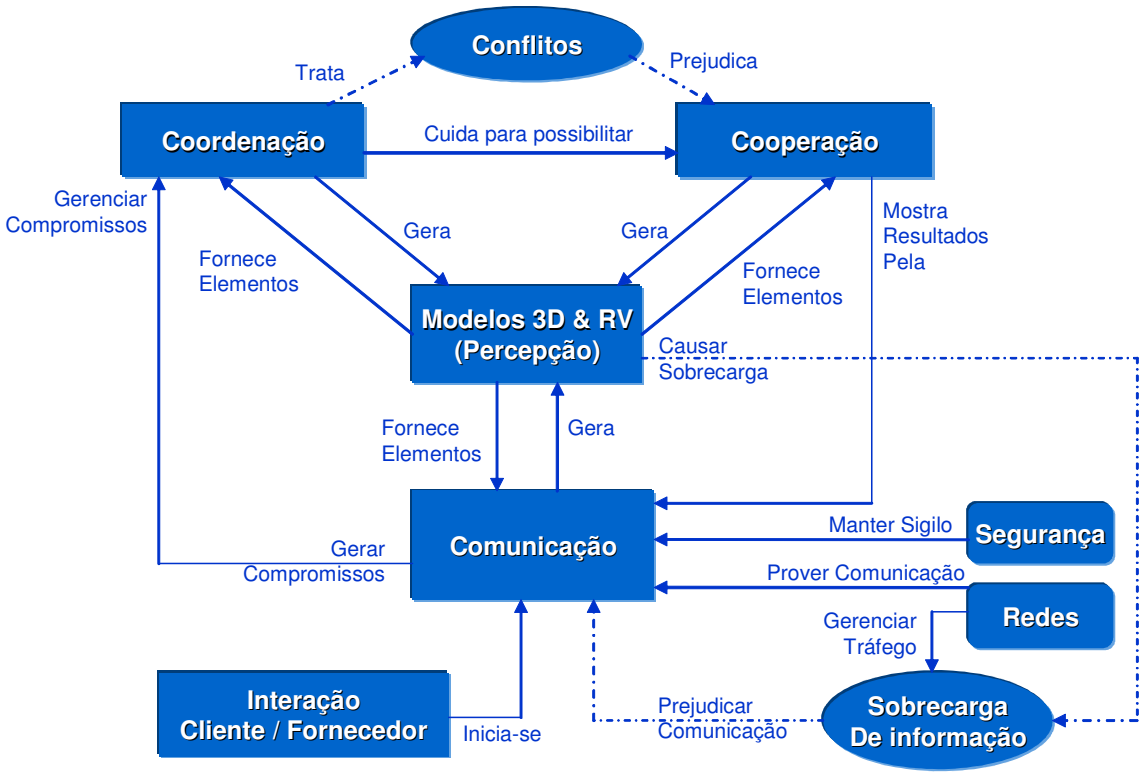

Figura 1 - Modelo de rede de colaboração

O diagrama da Figura 1 sumariza os principais conceitos abordados. Este diagrama é um refinamento do modelo apresentado em Fuks e Assis (2001), que foi baseado em Ellis; Gibbs e Rein (1991). Será abordado agora em mais detalhes os principais elementos do diagrama e suas inter-relações. Vale lembrar que apesar de estarem separados estes conceitos para efeito de análise, não é possível considerá-los monoliticamente, uma vez que são intimamente dependentes e inter-relacionados.

Trabalhar em grupo traz motivação para os membros, pois seu trabalho vai ser observado, comentado e avaliado por pessoas de uma comunidade da qual ele faz parte (BENBUNAN-FICH; HILTZ, 1999). As escolhas dos aplicativos e métodos de coordenação devem cuidar para que os participantes do grupo não se sintam isolados, estes aplicativos devem permitir níveis de comunicações dinâmicos balanceados com a velocidade de transmissão do meio para uma perfeita interação remota entre os nodos da rede.

3.1. Comunicação – Interação Cliente e Fornecedor

Os participantes de uma equipe de trabalho deve se comunicar para conseguir realizar tarefas interdependentes, não completamente descritas ou que necessitem de negociação (FUSSEL et al., 1998). A comunicação deve se dar por vias escritas, verbais e visuais, por estes meios deve se alcançar um entendimento comum e compartilhar idéias, discutir, negociar e tomar decisões. A comunicação se dará no espaço compartilhado, as redes, que dará suporte a canais da percepção e da cognição possibilitando a troca de conhecimentos entre os membros em conferencia remota.

Como o ambiente define o espaço compartilhado de informação entre os indivíduos, ele pode fornecer elementos adicionais não-verbais à estrutura de linguagem utilizada na conversação. Isto simplifica a comunicação verbal, que é complementada pelos elementos presentes no ambiente (GUTWIN e GREENBERG, 1999). Estes elementos não verbais atuarão no campo da percepção, deve-se projetar e avaliar cuidadosamente nos ambientes virtuais colaborativos os elementos disponíveis para o emissor codificar sua mensagem e os elementos de percepção para que o receptor receba a mesma.

3.2. Coordenação

Conversação para ação gera compromissos (WINOGRAD e FLORES, 1987; WINOGRAD, 1988). Para garantir o cumprimento destes compromissos e a realização do trabalho colaborativo através da soma dos trabalhos individuais, é necessária a coordenação das atividades que deverá ser suportado por um aplicativo de PLM (*Product LifeCycle Management*) com capacidade de gerenciar a estrutura do produto de forma hierárquica e o controle do nível de revisão dos dados matemáticos que estão sendo centralizados e acessados no cliente. Esta coordenação organiza o grupo para evitar que esforços de comunicação e

cooperação sejam perdidos e que as tarefas sejam realizadas na ordem correta, no tempo correto e cumprindo as restrições e objetivos (RAPOSO et al., 2001).

Trabalho colaborativo foi definido por Karl Marx como “múltiplos indivíduos trabalhando juntos de maneira planejada no mesmo processo de produção ou em processos de produção diferentes, mas conectados” (BANNON; SCHMIDT, 1991).

Visando o aspecto dinâmico e contínuo da coordenação, ela pode ser definida como “o ato de gerenciar interdependências entre as atividades realizadas para se atingir um objetivo” (MALONE; CROWSTON, 1990). Parte desta responsabilidade é atribuída ao aplicativo de PLM, que gerenciara as informações em último nível de revisão, as liberadas e aquelas que estão em desenvolvimento evitando o de os participantes se envolverem em tarefas conflitantes ou repetitivas.

As atividades mais diretamente voltadas para o trabalho colaborativo exigem sofisticados mecanismos de coordenação para garantir o sucesso da colaboração. Exemplos de ferramentas que dão suporte a este tipo de atividade são: gerenciamento de fluxo de trabalho (*workflow)*, *learningware*, jogos multi-usuários e ferramentas de autoria e de desenvolvimento de software colaborativo.

O ideal é que sistemas colaborativos não imponham padrões rígidos de trabalho ou de comunicação. Devem-se prover facilidades que permitam aos usuários interpretar e explorar estes padrões, decidir usá-los, modificá-los ou rejeitá-los (SCHMIDT, 1991).

As informações de percepção ajudam a medir a qualidade do trabalho com respeito aos objetivos e progressos do grupo e a evitar duplicação desnecessária de esforços (DOURISH; BELLOTI, 1992).

Conflitos podem ocorrer devido a problemas de comunicação ou de percepção, ou por diferenças na interpretação da situação ou de interesse (PUTNAM; POOLE, 1987). A coordenação deve tratar os conflitos que prejudiquem o grupo, como competição, desorientação, problemas de hierarquia, difusão de responsabilidade, etc. (SALOMON; GLOBERSON, 1989).

3.3. Cooperação

Cooperação é a operação conjunta dos membros do grupo no espaço compartilhado. Em um espaço virtual de informação, os indivíduos cooperam produzindo, manipulando e organizando informações, em tempo real por um aplicativo de conferencia remota que possibilite a transmissão de voz e imagem assim como o acesso remoto entre os nodos da rede. O ambiente do PLM controla as permissões de acesso.

A centralização dos dados no cliente gerenciado pelo PLM visa aumentar a confiabilidade da informação.

Perceber é adquirir informação, por meio dos sentidos, do que está acontecendo e do que as outras pessoas estão fazendo, mesmo sem se comunicar diretamente com elas (BRINCK; McDANIEL, 1997). A percepção, que é inerente ao ser humano, torna-se central para a comunicação, coordenação e cooperação de um grupo de trabalho. No trabalho distribuído a percepção vira em quase na sua totalidade pelo campo visual o que demanda a qualidade dos aplicativos de CAD usados e a compatibilidade deste com o meio. Os modelos devem ser desenhados em três dimensões par diminuir a falta dos demais sentidos usados em reuniões de projeto quando se está face-a-face com os colegas de trabalho.

Acompanhar as atividades dos demais parceiros da rede é essencial para garantir o fluxo e a naturalidade do trabalho, assim como para diminuir as sensações de impessoalidade e distância, comuns nos ambientes virtuais.

Um projeto adequado dos elementos de percepção possibilita que os participantes tenham disponíveis informações necessárias para prosseguir seu trabalho, sem ter que interromper seus colegas para solicitá-las. Os ambientes de colaboração devem prover informações necessárias para o trabalho coletivo e o individual, de forma que os participantes possam criar um entendimento compartilhado e construir o seu contexto de trabalho. Alguns exemplos de informações de percepção que podem ser providas são: o objetivo comum, o papel de cada um dentro do contexto, como proceder, qual o impacto das ações, até onde atuar, quem está por perto, o que o

companheiro pode fazer, o que as outras pessoas estão fazendo, a localização, a origem, a importância, as relações e a autoria dos objetos de cooperação.

4. Meios de Comunicação – Redes

Interligar locais geograficamente dispersos e possibilitar a interação entre eles, irá lidar com a tecnologia da informação que está intimamente ligada à tecnologia da transmissão de dados a qual da o suporte ao fluxo de informação entre dois ou mais pontos, assim, tem-se a uma rede com equipamentos ligados a ela com o objetivo de enviar e receber dados. Estes são os meios por onde as informações irão trafegar. Os equipamentos são os computadores os locais os nodos das redes, cliente e fornecedores.

Os nodos da rede podem ser interligados por linhas dedicadas ou por meios, redes públicas.

Linha Dedicada é o circuito ou canal de comunicação fornecido para uso exclusivo de um determinado assinante, caracterizando-se pela ligação permanente entre dois pontos. Usam-se linhas dedicadas para interligar computadores quando é necessário movimentar grandes quantidades de dados entre pontos, normalmente usado por empresas de grandes dimensões (www.anacom.com.br, 2007).

A Exploração Industrial de Linha Dedicada ("EILD") é fornecida por uma prestadora de serviços de telecomunicações que detenha concessão, permissão ou autorização a outra prestadora de serviços de telecomunicações e consiste no aluguel de circuitos dedicados, transparentes a protocolos ("clear channel"), para a prestação de Serviços de Telecomunicações a terceiros (www.embratel.com.br, 2007)

Estas linhas são regulamentada pela Anatel (www.anatel.gov.br, 2007) ANEXO À RESOLUÇÃO NO 402, DE 27 DE ABRIL DE 2005, artigo segundo parágrafo VIII como segue:

VIII – Linha Dedicada: oferta de capacidade de transmissão de sinais analógicos, telegráficos ou digitais entre dois pontos fixos, em âmbito nacional e internacional, utilizando quaisquer meios dentro de uma área de prestação de serviço;

A segunda opção será conectar os nodos por meio de redes públicas, ou seja, pela Internet a Rede Mundial de Computadores que nasceu nas décadas de 60/70 no

período em que a guerra fria pairava no ar entre as duas maiores potências da época, os Estados Unidos e a ex-União Soviética. Criada pela ARPA, sigla para *Advanced Research Projects Agency*, ou Agência de Pesquisa de Projetos Avançados, uma subdivisão do Departamento de Defesa dos Estados Unidos, ficou conhecida como ARPANET. O objetivo era deixar espalhados em vários lugares os dados americanos, ao invés de centralizados em apenas um servidor. Isso evitaria a perda desses dados no caso de, por exemplo, uma bomba explodisse no campus. Em seguida, ela foi utilizadas por universidades, onde os estudantes, poderiam trocar de forma ágil, os resultados de seus estudos e pesquisas. Um esquema técnico denominado IP (*Internet Protocol* – Protocolo da Internet) permitia que o tráfego de informações fosse encaminhado de uma rede para outra. Todas as redes conectadas na Internet comunicam-se em IP, para que todas possam trocar mensagens. Através da *National Science Foundation*, o governo americano investiu na criação de *backbones* (espinha dorsal), que são poderosos computadores conectados por linhas que tem a capacidade de dar vazão a grandes fluxos de dados, como canais de fibra óptica, elos de satélite e elos de transmissão por rádio. Além desses backbones, existem os criados por empresas particulares. A elas são conectadas redes menores, de forma mais ou menos anárquica. É basicamente isto que consiste a Internet, que não tem um dono específico, um conglomerado de redes em escala mundial de milhões de computadores interligados que permite o acesso a informações e todo tipo de transferência de dados.

4.1. Analise para a escolha entre Linha Dedicada e Redes Públicas

As linhas dedicadas conectam dois pontos, cliente e fornecedor, e requerem instalações físicas especificas com equipamentos, *hardware,* dedicados. Para cada fornecedor que queira se conectar ao cliente uma nova linha dedicada deve ser implantada. Por esta rede ambos os fornecedores se comunicam ao cliente, mas, um fornecedor não pode se comunicar com o outro, esta possibilidade só será possível se o cliente instalar equipamentos que conectem as duas linhas, roteador, para que seja criada uma infra-estrutura de redes entre os nodos, cliente e

fornecedores. São as vantagens e desvantagens para a rede criada por linhas dedicadas os seguintes itens:

Linhas Dedicadas

- Custo alto de implementação
- Custo alto de manutenção
- Tempo alto para instalação e configuração
- O cliente deve ser um servidor *Host* para a infraestrutura de rede.
- Alta velocidade de transmissão
- Excelente nivel de segurança para transporte das informações

As redes públicas estão presentes em todos os lugares e paises, a infraestrutura está pronta o que garante a conecção entre redes, não é necessario um roteador para cada par de redes, as tecnologias das redes nos nodos podem ser diferentes, a rede pode ser vista como única e global.

Os seguintes itens descrevem as vantagens e desvantagens das redes públicas:

Redes Públicas

- Baixo custo de implementação
- Baixo custo de manutenção
- Baixo tempo de instalação e configuração
- Velocidades ds transmissões menores que as das linhas dedicadas
- Baixo nível de segurança
- Alta interoperabilidade
- Protocolo de transmissão já definido

Pelos conceitos de Organizações Virtuais os nodos devem entrar e sair da rede dinamicamente conforme a necessidade do projeto como foi exemplificado por Goldman, Nagel e Preiss (1995). Este fato só pode se dar se o meio, as redes, que os interligam for algo comum pronta e já instalada, bastando unicamente dizer o endereço e dar a permissão de acesso, similar quando infoma-se o endereço a

alguém que ao chegar ao local lhe é dado permissão para que entre. Por este prisma a escolha recai nas redes públicas.

Por este meio soluciona-se a dinâmica de interoperabilidade entre os nodos da rede viabilizando ter qualquer colaborador conectado ao cliente instantaneamente e estes se comunicando entre si.

Dada à alta vulnerabilidade das redes públicas Internet, os dados a serem trafegados por este meio não estão seguros, para que está escolha seja viabilizada devem-se buscar sistemas de segurança para os dados em transito e balancear os aplicativos a serem usados pela velocidade desta rede.

5. Segurança nas redes públicas

Os dados que trafegam pelas redes publicas está sujeito serem interceptados e capturados. Os nodos da rede que desejam conectar-se entre precisam de um controle e permissão de acesso seguro evitando a quem não esteja autorizado de entrar nos sistemas compartilhados.

Com o explosivo crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação associado a um grande aumento nas velocidades de acesso e *backbone,* esta passou a ser vista como um meio conveniente para as comunicações corporativas.

No entanto, a passagem de dados sensíveis pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio altamente inseguro em um meio confiável. Com essa abordagem, o uso de redes privadas sobre a Internet parece ser uma alternativa viável e adequada.

A implantação de redes privadas pressupõe que não haja necessidade de modificações nos sistemas utilizados pelas corporações, sendo que todas as necessidades de privacidade que passam a ser exigidas sejam supridas pelos recursos adicionais que sejam disponibilizados nos sistemas de comunicação.

5.1. Redes Privadas Virtuais - *Virtual Private Network* (VPN)

O grande estímulo para o uso de VPNs é o baixo custo de implementação, aproveitar a infra-estrutura das redes publicas e o fato de não necessitar de modificações nas redes corporativas. No entanto, para que esta abordagem se torne efetiva, a VPN deve prover um conjunto de funções que garanta confidenciabilidade, Integridade e Autenticidade assim definidos:

Confidenciabilidade

Tendo em vista que estarão sendo utilizados meios públicos de comunicação, a tarefa de interceptar uma seqüência de dados é relativamente simples. É imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos.

Integridade

Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN.

Autenticidade

Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados em por um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

5.2. Aplicações para redes privadas virtuais

Abaixo, são apresentadas as três aplicações ditas mais importantes para as VPNs.

Acesso Remoto Via Internet

O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso *Internet Service Provider* - ISP. A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

Conexão de redes locais via Internet

Uma solução que substitui as conexões entre redes locais, *Local Área Network* - (LAN), através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a rede corporativa de larga abrangência, *Wide Área Network* (WAN) corporativa.

A depender das aplicações também, pode-se optar pela utilização de circuitos discados em uma das pontas, devendo a LAN corporativa estar, preferencialmente, conectada à Internet via circuito dedicado local, ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.

Conexões de Computadores em uma intranet

Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa.

Esta solução, apesar de garantir a "confidenciabilidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador possibilitaria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva. Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidenciabilidade" das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.

Requisitos Básicos

No desenvolvimento de soluções de rede, é bastante desejável que sejam implementadas facilidades de controle de acesso a informações e a recursos corporativos. A VPN pode dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interconexão de LANs de forma a possibilitar o acesso dos fornecedores, compartilhando recursos e informações e, finalmente, assegurar privacidade e integridade de dados ao atravessar a Internet bem como a própria rede corporativa. A seguir são enumeradas características mínimas desejáveis numa VPN:

- **Autenticação de Usuários**

  Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados - quem acessou, o quê e quando foi acessado.

- **Gerenciamento de Endereço**

  O endereço do cliente na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

- **Criptografia de Dados**

  Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

- **Gerenciamento de Chaves**

  O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

- **Suporte a Múltiplos Protocolos**

  Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos padrão de fato usadas nas redes públicas, tais como o protocolo nativo da internet. *Internet Protocol* (IP), *Internetwork Packet Exchange* (IPX), etc.

5.3. Modo de transmissão das redes VPN

As redes virtuais privadas baseiam-se na tecnologia de transmissão denominada tunelamento, túnel fictício que interliga dois nodos da rede de maneira segura, cuja existência é anterior às VPNs. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde são desencapsulado e decriptografado, retornando ao seu formato original. Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote.

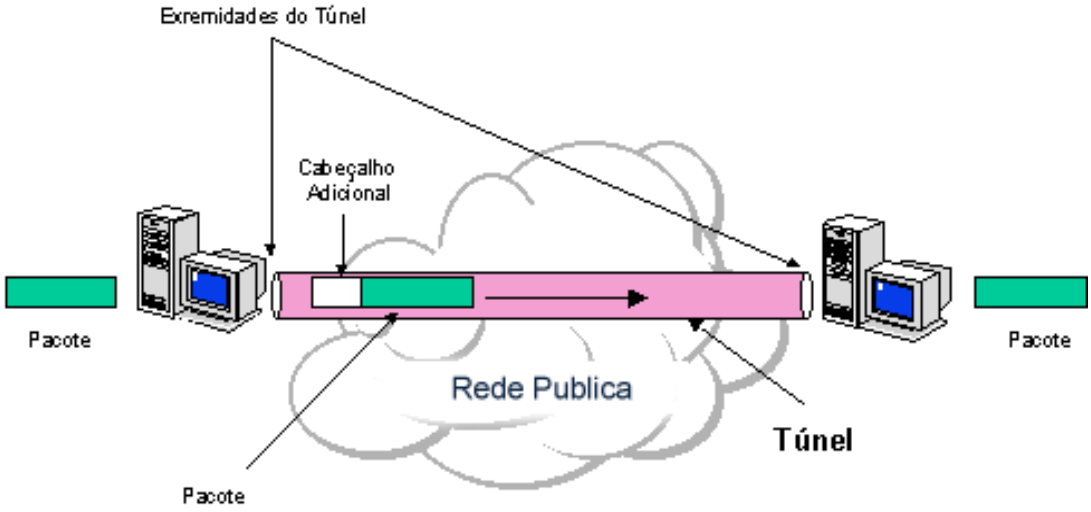

Figura 2 – Tunelamento das redes VPNs

5.4. Tunelamento

Para se estabelecer um túnel é necessário que as suas extremidades utilizem o mesmo protocolo de tunelamento.

O tunelamento pode ocorrer na camada 2 ou 3 (respectivamente enlace e rede) do modelo de referência Open Systems Interconnection (OSI).

- Tunelamento em Nível 2 - Enlace - (PPP sobre IP).
- O objetivo é transportar protocolos de nível 3, tais como o IP e IPX na Internet. Os protocolos utilizam quadros como unidade de troca, encapsulando os pacotes da camada 3 (como IP/IPX) em quadros *Point-to-Point Protocol* (PPP). Segue alguns exemplos:
- *Point-to-Point Tunneling Protocol* (PPTP) da Microsoft (www.microsoft.com/techne, 2007) permite que o tráfego IP, IPX e

NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas como a Internet.

- *Layer 2 Tunneling Protocol* (L2TP) da *Internet Engineering Task Force* (IETF) permite que o tráfego IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto tais como IP.
- Layer 2 Forwarding (L2F) da Cisco (www.cicso.com.br, 2007) é utilizada para VPNs discadas.
- Tunelamento em Nível 3 - Rede - (IP sobre IP) encapsulam pacotes IP com um cabeçalho adicional deste mesmo protocolo antes de enviá-los através da rede.

O IP Security Tunnel Mode (IPSec) permite que pacotes IP sejam criptografados e encapsulados com cabeçalho adicional deste mesmo protocolo para serem transportados numa rede IP pública ou privada. O IPSec é um protocolo desenvolvido para IPv6, devendo, no futuro, se constituir como padrão para todas as formas de VPN caso o protocolo IP versão 6 (IPv6) venha de fato substituir o protocolo IP versão 4 (IPv4). O IPSec sofreu adaptações possibilitando, também, a sua utilização com o IPv4.

5.5. O funcionamento dos túneis

Nas tecnologias orientadas à camada 2 (enlace), um túnel é similar a uma sessão, onde as duas extremidades do túnel negociam a configuração dos parâmetros para estabelecimento do túnel, tais como endereçamento, criptografia e parâmetros de compressão. Na maior parte das vezes, são utilizado s protocolos que implementam o serviço de datagrama. A gerência do túnel é realizada através protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada 3, não existe a fase de manutenção do túnel.

Uma vez que o túnel é estabelecido os dados podem ser enviados. O cliente ou servidor do túnel utiliza um protocolo de tunelamento de transferência de dados que acopla um cabeçalho preparando o pacote para o transporte. Só então o cliente envia o pacote encapsulado na rede que o roteará até o servidor do túnel. Este recebe o pacote, desencapsula removendo o cabeçalho adicional e encaminha o pacote original à rede destino. O funcionamento entre o servidor e o cliente do túnel é semelhante.

5.6. Protocolos × Requisitos de tunelamento

Os protocolos de nível 2, tais como PPTP e L2TP, foram baseados no PPP, e, como conseqüência, herdaram muito de suas características e funcionalidades. Estas características e suas contrapartes de nível 3 são analisadas juntamente com alguns dos requisitos básicos das VPNs:

5.7. Autenticações de Usuários

Os protocolos de tunelamento da camada 2 herdaram os esquemas de autenticação do PPP e os métodos *Extensible Authentication Protocol* (EAP). Muitos esquemas de tunelamento da camada 3 assumem que as extremidades do túnel são conhecidas e autenticadas antes mesmo que ele seja estabelecido.

Uma exceção é o IPSec que provê a autenticação mútua entre as extremidades do túnel. Na maioria das implementações deste protocolo, a verificação se dá em nível de máquina e não de usuário.

Como resultado, qualquer usuário com acesso às máquinas que funcionam como extremidades do túnel podem utilizá-lo. Esta falha de segurança pode ser suprida quando o IPSec é usado junto com um protocolo de camada de enlace como o L2TP.

5.8. Endereçamento Dinâmico

O tunelamento na camada 2 suporta alocação dinâmica de endereços baseada nos mecanismos de negociação do *Network Control Protocol* (NCP). Normalmente, esquemas de tunelamento na camada 3 assumem que os endereços foram atribuídos antes da inicialização do túnel.

5.9. Compressão dos Dados

Os protocolos de tunelamento da camada 2 suportam esquemas de compressão baseados no PPP. O IETF está analisando mecanismos semelhantes, tais como a compressão de IP, para o tunelamento na camada 3.

5.10. Criptografia dos Dados

Protocolos de tunelamento na camada de enlace suportam mecanismos de criptografia baseados no PPP. Os protocolos de nível 3 também podem usar métodos similares. No caso do IPSec são definidos vários métodos de criptografia de dados que são executados durante o ISAKMP. Algumas implementações do protocolo L2TP utilizam a criptografia provida pelo IPSec para proteger cadeias de dados durante a sua transferência entre as extremidades do túnel.

5.11. Gerenciamento de Chaves

O *Microsoft Point-to-Point Encryption* (MPPE); /technet2.microsoft.com/WindowsServer/pt-PT/Library, 2007) , protocolo de nível de

enlace, utiliza uma chave gerada durante a autenticação do usuário, atualizando-a periodicamente. O IPSec negocia uma chave comum através do ISAKMP e, também, periodicamente, faz sua atualização.

5.12. Suporte a Múltiplos Protocolos

O tunelamento na camada de enlace suporta múltiplos protocolos o que facilita o tunelamento de clientes para acesso a redes corporativas utilizando IP, IPX, NetBEUI e outros. Em contraste, os protocolos de tunelamento da camada de rede, tais como o IPSec, suportam apenas redes destino que utilizam o protocolo IP.

5.13. Tipo de Túneis

Os túneis podem ser criados de 2 diferentes formas - voluntárias e compulsórias:

- Túnel Voluntário - um cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel.
- Túnel Compulsório - um servidor de acesso discado VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

5.14. Tunelamento Voluntário

Ocorre quando uma estação ou servidor de roteamento utiliza um software de tunelamento cliente para criar uma conexão virtual para o servidor do túnel desejado.

O tunelamento voluntário pode requerer conexões IP através de LAN ou acesso discado.

No caso de acesso discado, o mais comum é o cliente estabelecer a conexão discada antes da criação do túnel.

Nas LANs, o cliente já se encontra conectado à rede que pode prover o roteamento de dados encapsulados para o servidor de túnel selecionado. Este é o caso de clientes numa LAN corporativa que inicializa túneis para alcançar uma sub-rede privada na mesma rede.

5.15. Tunelamento Compulsório

O computador ou dispositivo de rede que provê o túnel para o computador cliente é conhecido de diversas formas: *Front End Processor* (FEP) no PPTP, *L2TP Access Concentrator* (LAC) no L2TP ou IP *Security Gateway* no caso do IPSec. Doravante, adotado o termo FEP para denominar esta funcionalidade - ser capaz de estabelecer o túnel quando o cliente remoto se conecta.

No caso da Internet, o cliente faz uma conexão discada para um túnel habilitado pelo servidor de acesso no provedor (ISP). Por exemplo, uma companhia pode ter um contrato com uma ou mais provedores para disponibilizar um conjunto de FEPs em âmbito nacional. Estas FEPs podem estabelecer túneis sobre a Internet para um servidor de túnel conectado à rede corporativa privada, possibilitando a usuários remotos o acesso à rede corporativa através de uma simples ligação local.

Esta configuração é conhecida como tunelamento compulsório porque o cliente é compelido a usar um túnel criado pelo FEP. Uma vez que a conexão é estabelecida, todo o tráfego "de/para" o cliente é automaticamente enviado através do túnel. No tunelamento compulsório, o cliente faz uma conexão PPP. Um FEP pode ser configurado para direcionar todas as conexões discadas para um mesmo servidor de túnel ou, alternativamente, fazer o tunelamento individual baseado na identificação do usuário ou no destino da conexão.

Diferente dos túneis individualizados criados no tunelamento voluntário, um túnel entre o FEP e o servidor de túnel pode ser compartilhado por múltiplos clientes discados. Quando um cliente disca para o servidor de acesso (FEP) e já existe um túnel para o destino desejado, não se faz necessária a criação de um novo túnel redundante. O próprio túnel existente pode transportar, também, os dados deste novo cliente. No tunelamento compulsório com múltiplos clientes, o túnel só é finalizado no momento em que o último usuário do túnel se desconecta.

5.16. IPSEC – Internet Protocol Security

O IPSec é um protocolo padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.

Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser utilizado de forma conjunta ou separada, de acordo com a necessidade de cada usuário:

- Autenticação e Integridade;
- Confidenciabilidade.

Para implementar estas características, o IPSec é composto de 3 mecanismos adicionais:

- *Autentication Header* (AH)

- *Encapsulation Security Payload* (ESP)
- Internet Security Association and Key Management Protocol (ISAKMP)

5.17. Negociações do Nível de Segurança

O ISAKMP combina conceitos de autenticação, gerenciamento de chaves e outros requisitos de segurança necessários às transações e comunicações governamentais, comerciais e privadas na Internet. Com o ISAKMP, as duas máquinas negociam os métodos de autenticação e segurança dos dados, executam a autenticação mútua e geram a chave para criptografar os dados.

Trata-se de um protocolo que rege a troca de chaves criptografadas utilizadas para decifrar os dados. Ele define procedimentos e formatos de pacotes para estabelecer, negociar, modificar e remover as *Security Associations* (SAs). As SAs contêm todas as informações necessárias para execução de serviços variados de segurança na rede, tais como serviços da camada IP (autenticação de cabeçalho e encapsulamento), serviços das camadas de transporte, e aplicação ou auto-proteção durante a negociação do tráfego. Também define pacotes para geração de chaves e autenticação de dados. Esses formatos provêm consistência para a transferência de chaves e autenticação de dados que independem da técnica usada na geração da chave, do algoritmo de criptografia e do mecanismo de autenticação.

O ISAKMP pretende dar suporte para protocolos de segurança em todas as camadas da pilha da rede. Com a centralização do gerenciamento dos SAs, o ISAKMP minimiza as redundâncias funcionais dentro de cada protocolo de segurança e também pode reduzir o tempo gasto durante as conexões através da negociação da pilha completa de serviços de uma só vez.

5.18. Autenticação e Integridade

A autenticação garante que os dados recebidos correspondem àqueles originalmente enviados, assim como garante a identidade do emissor. Integridade significa que os dados transmitidos chegam ao seu destino íntegro, eliminando a possibilidade de terem sido modificados no caminho sem que isto pudesse ser detectado.

O AH é um mecanismo que provê integridade e autenticação dos datagramas IP. A segurança é garantida através da inclusão de informação para autenticação no pacote a qual é obtida através de algoritmo aplicado sobre o conteúdo dos campos do datagrama IP, excluindo-se aqueles que sofrem mudanças durante o transporte. Estes campos abrangem não só o cabeçalho IP como todos os outros cabeçalhos e dados do usuário. No IPv6, o campo *hop-count* e o *time-to-live* (TTL) do IPv4 não são utilizados, pois são modificados ao longo da transferência.

Para alguns usuários o uso da autenticação pode ser suficiente não sendo necessária a "confidenciabilidade".

No IPV6, o AH normalmente é posicionado após os cabeçalhos de fragmentação e *End-to-End*, e antes do ESP e dos cabeçalhos da camada de transporte (TCP ou UDP, por exemplo).

5.19. Confidenciabilidade

Propriedade da comunicação que permite que apenas usuários autorizados entendam o conteúdo transportado. Desta forma, os usuários não autorizados, mesmo tendo capturado o pacote, não poderão ter acesso às informações nele contidas. O mecanismo mais usado para prover esta propriedade é chamado de criptografia.

O serviço que garante a "confidenciabilidade" no IPSec é o ESP. O ESP também provê a autenticação da origem dos dados, integridade da conexão e serviço *anti-reply*. A "confidencialidade" independe dos demais serviços e pode ser implementada de dois modos - transporte e túnel. No primeiro modo, o pacote da camada de transporte é encapsulado dentro do ESP, e, no túnel, o datagrama IP é encapsulado inteiro dentro do cabeçalho do ESP.

5.20. Infra-estrutura para redes VPNs

Em empresas de grande porte onde se deseja receber vários clientes e aconselhável que dedique um computador como servidor de rede VPN.

São vários os softwares para está aplicação disponíveis para os diversos sistemas operacionais existentes e na maioria das vezes configuráveis no próprio sistema operacional como o Windows Server da Microsoft (http://www.microsoft.com/workshop/server/feature/vpnovw.asp.).

Para o Linux os procedimentos de configuração e instalação das redes VPNs pode ser consultadas no site http://br-linux.org/tutoriais/000210.html.

5.21. Conclusão sobre as rede VPNs

As VPNs podem se constituir numa alternativa segura para transmissão de dados através de redes públicas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os links dedicados de longa distância, de alto custo, na conexão de WANs.

Entretanto, em aplicações onde o tempo de transmissão é crítico, o uso de VPNs através de redes externas ainda deve ser analisado com muito cuidado, pois podem ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a

organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos.

6. Definição das tarefas entre os nodos da rede

A primeira definição se refere a uma Organização Virtual como uma empresa que faz mais uso das tecnologias de informação e comunicação do que a presença física, para interagir e conduzir seus negócios (STRAUSAK, 1998).

Ao se projetar um produto, os aplicativos de simulação já conseguem virtualizar a realidade, auxiliando sobremaneira os projetistas (DAVIDOW; MALONE, 1993).

A comunicação e a rápida troca de informações relevantes desempenham um papel essencial para o sucesso desta metodologia. Portanto, deve-se ter uma Tecnologia da Informação que ofereça e dê suporte aos seguintes itens (MERKLE, 1997).

- Criar idéias, conhecimento e confiança mútuos através do compartilhamento da informação e comunicação intensa;
- Projetar ou reprojetar e coordenar processos distribuídos globalmente;
- Melhorar os relacionamentos entre os parceiros que cooperam bem como com consumidores através do fornecimento de informações atuais e relevantes

Para que estes objetivos sejam desempenhadas com sucesso, além dos meios um conjunto de aplicativos de comunicação e acessos remotos devem ser definidos baseados nas tarefas de interoperabilidade que os nodos devem executar entre si.

O objetivo da criação desta rede de cooperação é o desenvolvimento do produto, pelo conceito da rede de colaboração que definida a partir do modelo apresentado por Fuks e Assis, (2001), a interação Cliente e Fornecedor inicia a comunicação que por sua vez gera a percepção que são os modelos matemáticos do produto em desenvolvimento. São definidas para este enlace como tarefas básicas entre os nodos:

- Comunicação oral e escrita;
- Visualização do modelo matemático em tempo real;
- Acesso Remoto ao modelo matemático

Os modelos matemáticos fornece elementos para a coordenação do projeto que realimenta a rede com o desenho de conjunto para analise e estudo do produto final que possibilitara a cooperação dos fornecedores na solução de problemas. Assim têm-se os seguintes requisitos:

- Estrutura do conjunto sendo armazenada de forma lógica e hierárquica
- Acesso dos fornecedores somente aos componentes que interagem com a peça que ele está desenvolvendo.
- Controle de revisões de modificações dos componentes armazenados no cliente para evitar conflitos.

6.1. Escolhas dos aplicativos, *softwares*

Pelas tarefas definidas entre os nodos um software de compartilhamento de aplicações supre as tarefas de comunicação, visualização e acesso remoto.

Para armazenamento dos modelos no cliente, gerenciamento do controle de acesso aos dados e controle do histórico das revisões dados matemáticos, recai em um aplicativo de *Product LifeCycle Management* (PLM) e por fim um *software* que faça desenhos digitais em 2D e 3D (CAD) para geração dos modelos.

Nada impede que cada um destes aplicativos seja de diferentes fabricantes, porém a recomendação é que sejam todos de um mesmo produtor para que os conflitos entre aplicativos sejam minimizados e haja boa interação no transporte de dados entre eles.

Dentre os desenvolvedores de software pesquisados quatro são os que apresentam soluções de PLM e CAD como segue:

- IBM – Apresenta soluções de engenharia para desenvolvimento do produto em um aplicativo de PLM – (www.ibm.com, 2007)

- Autodesk – Tem varias soluções de CAD, porém mais voltadas as áreas de manufatura e engenharia civil – (www.autodesk.com, 2007)
- Catia – Proprietária de um bom pacote de de PLM e CAD para com soluções voltadas para diferentes áreas de engenharia inclusive engenharia de projetos. (www.catia.com, 2007)
- UGS – A mais completa em soluções para engenharia, além dos aplicativos de PLM e CAD para as diversas áreas da engenharia possue também aplicativos para trabalho a distancia com suporte a conferencias e acesso remoto. (www.ugs.com, 2007)

Pelo exposto acima e visando atender a propostas de metodologia de trabalho, a escolha recai a solução apresentada pela empresas UGS com os seguintes aplicativos:

- Team Center Community (TCC) – Aplicação para conferencia e compartilhamento de aplicações, Application Share, com suporte a varios usúarios simultaneamente.
- Team Center Engineer (TCE) - Aplicativo de PLM com suporte a controle de acesso, histórico de revisões.
- UGNX3 – Software de CAD que trabalha em sincronia com o TCE, ambos em conjunto pode manter um ambiente seguro de trabalho evitando evasão de informação e acesso a outras partes da rede do cliente.

7. Desempenho e Perdas nas Redes – Ensaios e testes.

O primeiro estudo para implementação deste conceito é a escolha dos meios em que a informação irá trafegar. Dados os diversos meios de conexão entre *sites,* a escolha objetivará as topologias de redes mais comuns para assegurar a compatibilidade com a maioria das empresas, viabilizando assim, o maior número possível de colaboradores na rede. Estes meios deverão atender o requisito de velocidade mínima de transferência de dados, requerida pelos aplicativos utilizados na rede, para não haver degradação da comunicação e perda da sinergia no trabalho.

Para avaliar a velocidade de transmissão e a dinâmica de trabalho remoto foram feitos quatro experimentos de transmissão de dados entre computadores, com redes experimentais. Em cada uma delas foram enviados pacotes de dados com 32 bytes e mediu-se o tempo de transmissão destes pacotes, tempo de atraso. A cada fase, um teste prático de acesso remoto é realizado, verificado subjetivamente se é possível trabalhar dinamicamente a está velocidade. Com isto foram obtidos valores de atraso que referenciam os limites de velocidades do meio admissível para acesso remoto a sistemas.

Em todas as fases utilizaram-se os mesmos softwares de acesso remoto e CAD, neles foram manipulados modelos matemáticos de 30Mb.

Os primeiros testes foram realizados entre computadores dentro da mesma rede local, para obter um parâmetro da melhor qualidade de acesso. Seguindo com o experimento os próximos foram entre redes dentro da mesma cidade, em redes entre estados e em redes entre paises. Por fim foi feito uma simulação onde a rede experimental de teste simulou um fornecedor se conectando ao cliente.

As redes experimentais foram criadas propositadamente de forma bem heterogenia com equipamentos diferenciados entre elas e provedores de acesso a rede pública distintos com diferentes velocidades de link.

7.1. Modelo das redes experimentais

Com o objetivo de mensurar a possibilidade de trabalho remoto em função do tempo de atraso nas transmissões foram criadas duas redes de computadores experimentais, dentro de um mesmo ambiente, com velocidades diferentes de conexão ao provedor.

A primeira rede, denominada de LAN 1 e mostrada na tabela 1, tinha como o provedor de acesso a rede pública o serviço da Virtua fornecida pela empresa NET (www.nettvdigital.com.br, 2007) com velocidade de conexão de 2Mbs por cabo coaxial e endereçamento de rede "IP" variável, DHCP. Internamente era composta de um "Cable Modem", equipamento para recepção e transmissão de dados pela internet por cabo coaxial, para distribuição do sinal aos computadores foi instalado um Roteador, parte responsável em direcionar os dados a rede externa ou interna conforme a solicitação, com "Hub", parte responsável em conectar fisicamente os computadores na rede interna, incorporada no mesmo aparelho que possibilitava a rede a trabalhar internamente a uma velocidade de 100Mbs para os computadores conectados a ela por cabo e 54Mbs classe G à aqueles conectados por meios de comunicação sem fio, "WiFi". Nesta rede estavam conectados 3 computadores, sendo dois deles modelos de mesa "DeskTop". O primeiro denominado M2L1 equipado com processador Pentium 1.13Mhz e sistema operacional "Windows XP Home" da Microsoft (www.microsoft.com/brasil/windowsxp, 2007) o outro denominado M3L1, equipado com processador Athlon 2.4 Mhz com sistema operacional "Windows 2000", da Microsoft (www.microsoft.com/brasil/windows2000, 2007), e um computador modelo portatil "LapTop" equipado com processador Pentium Celerom M, denominado M1L1 com sistema operacional "Windows XP Professional", da Microsoft. Os computadores Desktop estavam conectados a rede via cabo, tipo par trançado nivel 5, enquanto o LapTop via WiFi.

A segunda rede, denominada de LAN 2 e mostrada na tabela 2, conectada a rede publica pelo serviço da empresa Telefônica denominado Speedy (www.speedy.com.br, 2007), com velocidade de conexão de 1Mbs por linha telefônica e endereçamento de rede "IP" fixo. Internamente era composta de um

“Modem ADSL”, equipamento para recepção e transmissão de dados pela internet pela linha telefônica, com roteador incorporada no mesmo aparelho e uma Hub para distribuição do sinal aos computadores internamente com velocidade de 10Mbs a aqueles que conectados a ela por cabo. Nesta rede estavam conectados 2 computadores ambos modelos de mesa “DeskTop”. O primeiro denominado M1L2 equipado com processador Pentium 1.13Mhz e sistema operacional “Windows XP Home” da Microsoft (www.microsoft.com/windowsxp, 2007, o outro denominado M2L1, equipado com processador Pentium 2.0 Mhz com sistema operacional “Windows XP Home”, da Microsoft. Os computadores Desktop estavam conectados a rede via cabo, tipo par trançado nível 5.

A figura 3 ilustra a estrutura das redes LAN 1 e LAN 1 conectadas as redes públicas pelos seus provedores de acesso.

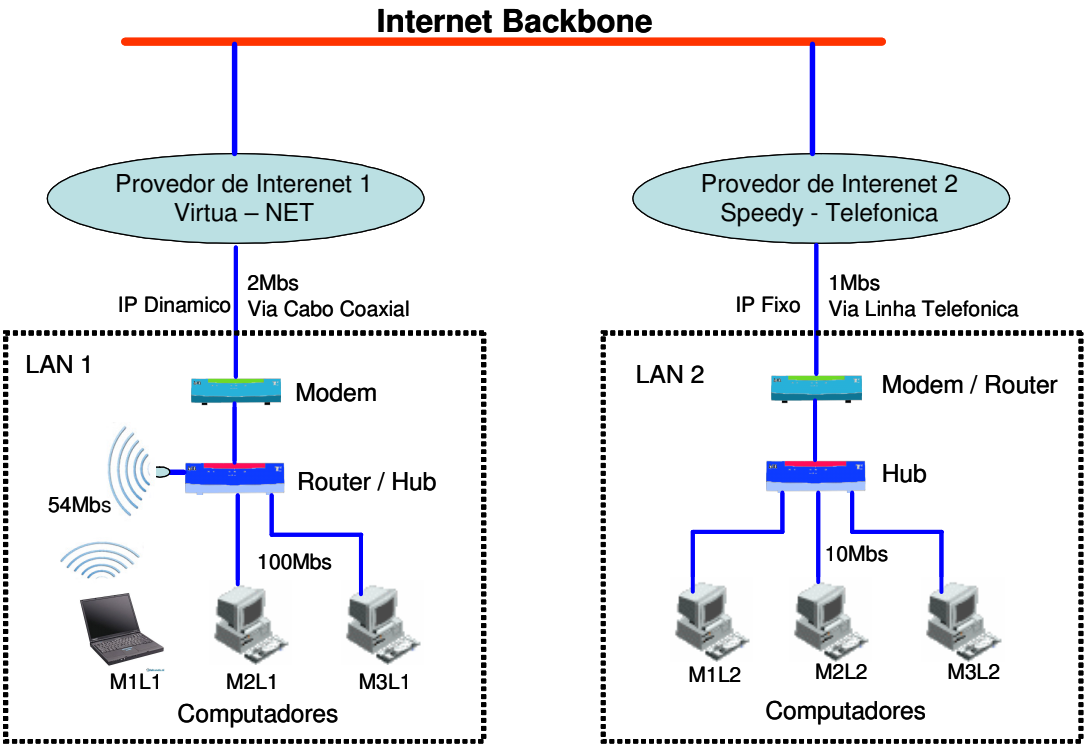

Figura 3 – Modelo de rede utilizada nos testes

Tabela 1 – Rede experimental 1

Rede Local 1 - LAN 1		
Provedor de Acesso	Empresa	NET
	Serviço	Virtua
	Velocidade de Conexão	2Mbs
	Tipo de Conexão	Cabo Coaxial
	Endereçamento IP	Variavel - DHCP
Infraestrutura de rede interna	Cable Modem	Motorola SBV5120
	Router	Linksys WRT54GC com WiFi integrado
	Hub	Incorporada a Router
	Conexão por Cabo	Padrão Ethernet 802.1 100Mbs
	Conexão WiFi	Padrão Ethernet 802.1 54Mbs Classe G
Computadores	DeskTops	Pentiun 1.13 - Windows XP Home Atlhon 2.4 - Windows 2000
	Lap Top	Pentiun Celerom M - Windows XP Home

Tabela 2 – Rede experimental 2

Rede Local 2 - LAN 2		
Provedor de Acesso	Empresa	Telefônica
	Serviço	Speedy
	Velocidade de Conexão	1Mbs
	Tipo de Conexão	Linha Telefonica
	Endereçamento IP	Fixo
Infraestrutura de rede interna	Modem ADSL	Zyxel Parks Prestige 600
	Router	Incorporada ao Modem
	Hub	Encore ENH708 10Mbs
	Conexão por Cabo	Padrão Ethernet 802.1 10Mbs
Computadores	DeskTops	Pentiun 1.13 - Windows XP Professional Atlhon 2.4 - Windows 2000

7.2. Procedimento dos testes

Dando continuidade as fases de testes foram criadas procedimentos para os quatro experimentos de comunicação entre os computadores, tanto pela rede pública quanto pela rede privada local. O experimento feito na rede local, por ser o meio mais rápido e sem tráfego feito pelo roteamento nas redes públicas, sinalizou a melhor qualidade de acesso entre os computadores. Em todos os experimentos foram enviados pacotes de dados com 32 bytes medido o tempo de transmissão destes pacotes verificando subjetivamente a acesso remoto pela execução de um desenho 3D sendo executado pelo software de CAD UG-NX3 da empresa UG Solutions.

Teste 1:

Foi efetuado entre os computadores M2L1 e M3L1 conectados por cabo dentro de uma mesma rede local, LAN 1, a velocidade de 100Mbs tendo como software de conexão e acesso remoto o NetMeeting. O computador M2L1 solicitou a acesso ao M3L1 o compartilhamento da aplicação de CAD onde foram manipulados um desenho 3D com 30Mb de tamanho de arquivo.

Teste2:

Foi efetuado entre os computadores M1L1 e M3L1 conectados por cabo e por WiFi dentro de uma mesma rede local, LAN 1, a velocidade de 100Mbs e 54Mbs respectivamente por cabo e WifI. O software de conexão e acesso remoto foi o NetMeeting. O computador M1L1 solicitou a acesso ao M3L1 o compartilhamento da aplicação de CAD onde foram manipulados um desenho 3D com 30Mb de tamanho de arquivo.

Teste 3:

Foi efetuado entre os computadores M3L1 da rede local 1, LAN 1, e o M1L2, da rede local 2 LAN 2, conectados por cabo na infra-estrutura local de rede LAN1 e LAN2 e 100Mbs e 10Mbs respectivamente. As redes locais LAN 1 e LAN2 estavam conectadas uma a outra pelas redes públicas acessada via os provedores de acesso Virtua (www.nettvdigital.com.br, 2007) e Speedy (www.speedy.com.br, 2007). O

software de conexão e acesso remoto foi o NetMeeting. O computador M3L1 solicitou acesso ao M1L2 para compartilhamento da aplicação de CAD onde foram manipulados um desenho 3D com 30Mb de tamanho de arquivo.

Teste 4:

Foi efetuado entre os computadores M1L1 da rede local 1, LAN 1, e um computador convidado localizado em um hotel nos Estados Unidos que utilizou do acesso a rede pública via WiFi proporcionado pela infra-estrutura de rede do próprio hotel oferecido com um serviço de cortesia aos hospedes. As redes locais LAN 1 e a do hotel estavam conectadas uma a outra pelas redes públicas. O software de conexão e acesso remoto foi o NetMeeting. O computador convidado solicitou acesso ao M2L1 para compartilhamento da aplicação de CAD onde foram manipulados um desenho 3D com 30Mb de tamanho de arquivo.

7.3. Resultados

Teste 1:

Neste experimento o acesso deu-se pelos computadores M2L1 e M3L1, ambos conectados por cabo internamente a rede local LAN 1 conforme procedimento descrito no item 8.2 e ilustrado na figura 4.

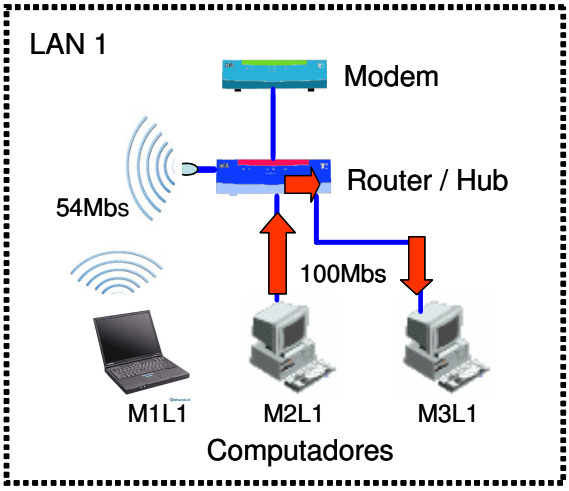

Figura 4 – Experimento de conexão entre os micros M2L1 e M3L1

O tempo de atraso entre os dois computadores foi menor que 1ms (um milisegundo). Este experimento serviu para parametrisar a melhor condição de acesso remoto entre dois equipamentos. Por estes meios o acesso foi satisfatório e com boa sinergia de trabalho. A tabela 3 resume os resultados obtidos no teste 1.

Tabela 3 - Resultados do teste 1

Origem		Destino		Atraso	Acesso Remoto
Rede	**Equipamento**	**Rede**	**Equipamento**	**(ms)**	
LAN 1	M2L1	LAN 1	M3L1	1	Satisfatório

Teste 2:

Neste experimento o acesso deu-se pelos computadores M1L1, conectado via WiFi, e M3L1, conectado por cabo, internamente a rede local LAN 1 conforme procedimento descrito no item 8.2 e ilustrado na figura 5.

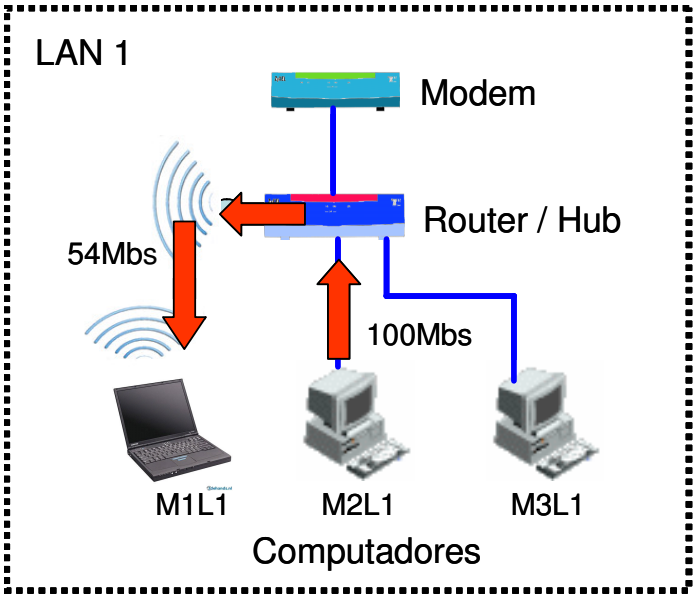

Figura 5 – Experimento de conexão entre os micros M1L1 e M3L1

O tempo de atraso entre os dois computadores foi e média 3ms (três milisegundos). Este experimento serviu para verificar o comportamento da conexão entre dois equipamentos, quando um deles se dá por tecnologia de rede sem fio, WiFi.

Por estes meios o acesso também foi satisfatório com boa sinergia de trabalho. A tabela 4 resume os resultados obtidos no teste 2.

Tabela 4 – Resultados do teste 2

Origen		Destino		Atraso (ms)	Acesso Remoto
Rede	**Equipamento**	**Rede**	**Equipamento**		
LAN 1	M1L1	LAN 1	M3L1	3	Satisfatório

Teste 3:

Neste experimento o acesso deu-se pelos computadores M3L1, conectado por cabo na infra-estrutura da rede local 1, ao computador M1L2 da rede local LAN 2, também conectado por cabo na infra-estrutura da rede local 2. conforme procedimento descrito no item 8.2 e ilustrado na figura 6.

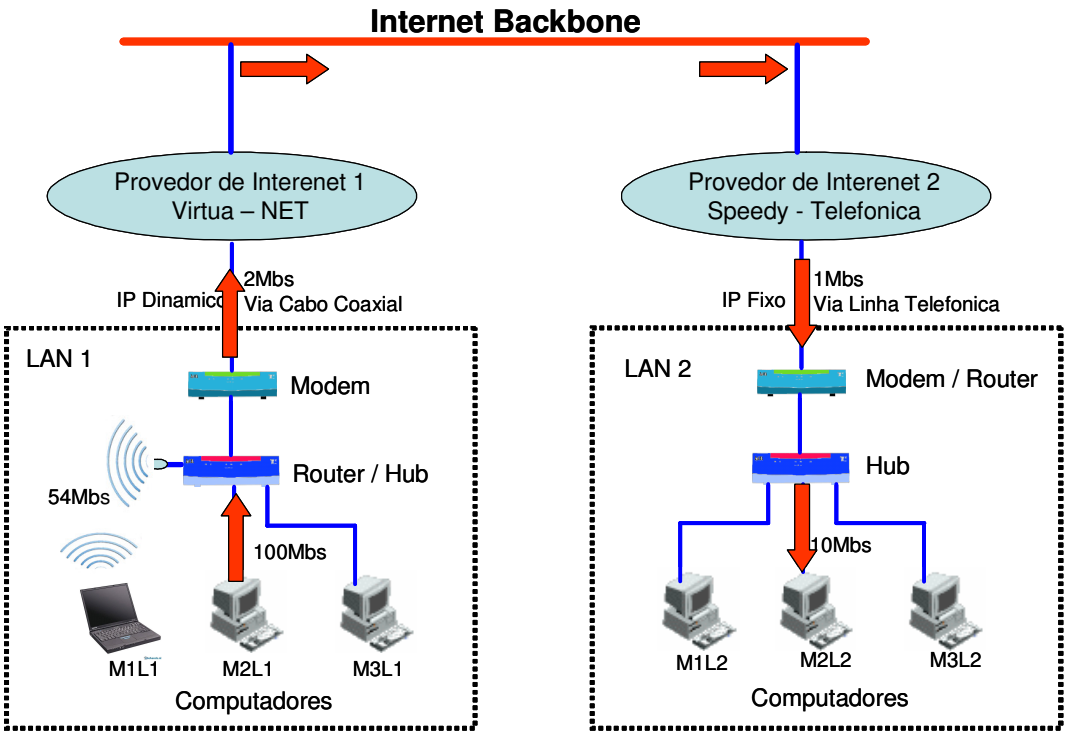

Figura 6 – Experimento de conexão entre os micros M3L1 e M1L2

O tempo de atraso entre os dois computadores foi e média 38ms (trinta e oito milisegundos). Este experimento serviu para avaliar o acesso remoto entre dois equipamentos em redes locais distintas conectadas via rede pública. Por estes meios o acesso foi satisfatório com boa sinergia de trabalho. A tabela 5 resume os resultados obtidos no teste 3.

Tabela 5 – Resultados do teste 3

Origen		Destino		Atraso (ms)	Acesso Remoto
Rede	**Equipamento**	**Rede**	**Equipamento**		
LAN 1	M2L1	LAN 2	M1L2	38	Satisfatório

Neste caso é interessante analisar o roteamento, caminho que os dados percorrem desde a origem até o destino pelas redes públicas. Originado na LAN 1 ele caminha ao provedor de acesso (ISP) onde é manobrado por três roteadoras até ser enviado "NAP" NetWork Access Point, que é uma empresa responsável pelo acesso dos dados ao BackBone, ramo principal da rede publica que interliga os "NAP" neste caso a empresa é a Embratel. Uma vez no Backbone o dado é capturado pelo provedor de acesso da LAN 2 e encaminhado ao seu destino final. A tabela 6 mostra o roteamento com os seus tempos desde a origem ao seu destino nas redes públicas.

Tabela 6 – Roteamento dos dados pela rede pública entre a LAN 1 e LAN 2

URL	IP	Tempo Medio (ms)
c953793b.virtua.com.br	[201.83.121.59]	<1
10.15.0.1		26
c9060002.virtua.com.br	[201.6.0.2]	11
c9060005.virtua.com.br	[201.6.0.5]	11
embratel-G6-0-gacc05.spo.embratel.net.br	[200.178.78.1]	22
ebt-C1-gacc03.spo.embratel.net.br	[200.230.242.13]	30
telefonicaempresas-net-P2-0-gacc03.spo.embratel.net.br	[200.174.250.2]	13
201-0-3-158.dsl.telesp.net.br	[201.0.3.158]	13
200-204-207-155.dsl.telesp.net.br	[200.204.207.155]	12
200-171-135-41.dsl.telesp.net.br	[200.171.135.41]	32

Teste 4:

Este experimento objetivou a avaliação de um computador remoto em outro pais sem estar conectado a uma rede local empresarial. O computador convidado ao teste estava localizado em um hotel nos Estados Unidos, acessando a rede pública através da infra-estrutura de rede WiFi oferecida de cortesia aos hospedes.

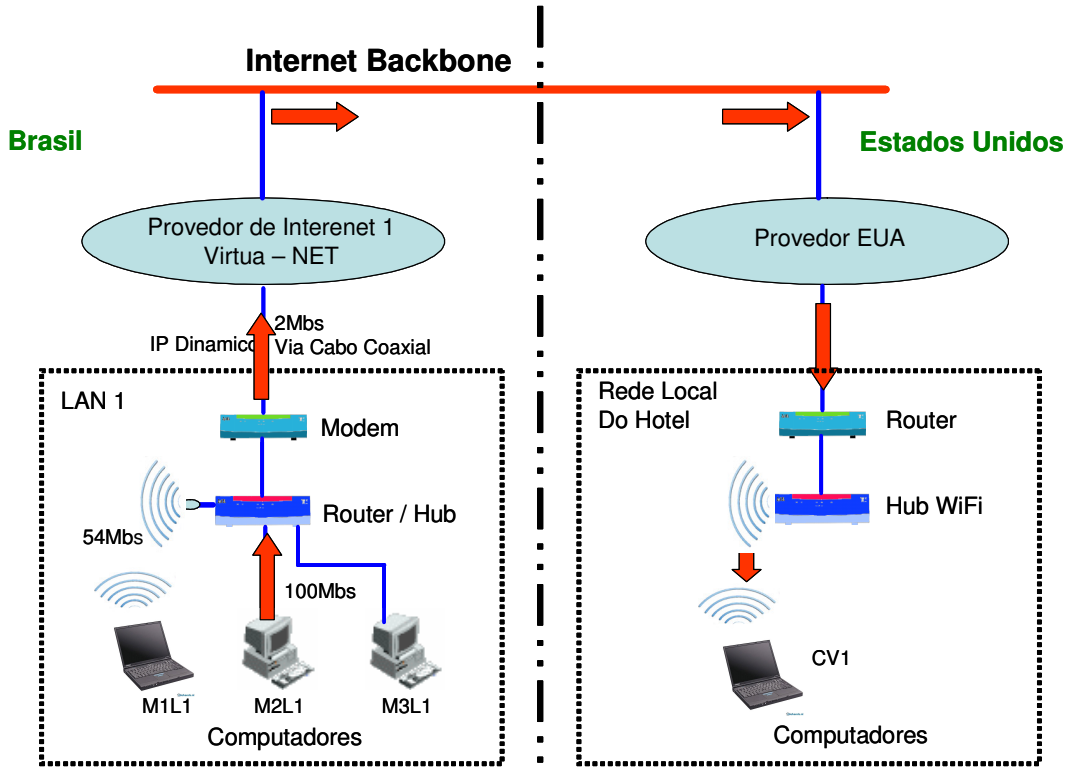

Figura 7 – Experimento de conexão entre computadores em diferentes paises

O tempo de atraso medido neste experimento foi em media de 140ms, dados resumidos na tabela 7.

Tabela 7 – Resultados do teste 4

Origen		Destino		Atraso	Acesso Remoto
Rede	**Equipamento**	**Rede**	**Equipamento**	**(ms)**	
LAN 1	M1L1	EUA	Lap Top	140	Satisfatório

Neste caso, também é interessante analisar o roteamento, caminho que os dados percorrem desde a origem até o destino pelas redes públicas. Originado na LAN 1 ele caminha ao provedor de acesso (ISP) onde é manobrado por três roteadoras até ser enviado NAP que desta vez fez um encaminhamento diferenciado não passando

pelo NAP Embratel. Uma vez no Backbone o dado é capturado pelo NAP do país de destino, encaminhado para o ISP que por sua vez direciona ao destino final. A tabela 8 mostra o roteamento com os seus tempos desde a origem ao seu destino nas redes públicas entre paises

Tabela 8 – Roteamento dos dados pela rede pública entre diferentes paises

URL	IP	Tempo Medio (ms)
c953793b.virtua.com.br	[201.83.121.59]	<1
c9060002.virtua.com.br	[201.6.0.2]	152
c9060009.virtua.com.br	[201.6.0.9]	13
ge-4-2-0.400.ar2.GRU1.gblx.net	[64.209.94.225]	24
tbr2031901.wswdc.ip.att.net	[12.122.80.50]	132
gbr5-p40.wswdc.ip.att.net	[12.122.11.186]	132
gar3-p360.wswdc.ip.att.net	[12.123.9.65]	135
mdf1-gsr12-2-pos-7-0.atl1.attens.net	[12.122.255.154]	144
mdf1-bi8k-1-eth-2-2.atl1.attens.net	[12.129.65.70]	144
ip2.v70.workscape.net	[12.129.70.2]	148
ip20.v70.workscape.net	[12.129.70.20]	145

8. Controle de acesso no Team Center

Com base nos procedimentos e testes até aqui descritos consegui-se um método de transmissão de dados pelas redes públicas com a segurança suportada pelas redes VPN. Voltando ao modelo da rede de colaboração da representada na figura 1, já se fazem definidos a comunicação responsável pela interação entre cliente e fornecedor a segurança na transmissão dos dados, possibilitando a percepção. A coordenação visa gerenciar, gerar e fornecer elementos à percepção, os modelos matemáticos, garantir o sigilo do projeto e gerenciar o controle de acesso.

Está coordenação deve ser feita de forma mais automatizada possível isto nos leva aos aplicativos de PLM Product Lifecycle Management os quais mantém um histórico das revisões sofridas controla o acesso de usuários a sua base de dados e permissão a determinados arquivos ao usuário que está acessando a base de dados no cliente. Isto garante o sigilo do projeto, pois, é dado permissões, ao colaborador, somente as peças que interagem com aquela em que ele está projetando.

Exemplificou-se neste trabalho o aplicativo de PLM o TcAE, Team Center Engineer, fornecido pela empresa UGS, www.ugs.com, que possui todas estas potencialidades. Por este meio o fornecedor ao acessar o cliente via VPN terá como porta de entrada o TcAE que solicitara o segundo nível de autenticação no cliente, o primeiro é dado pelo acesso VPN. O TcAE “segura” quem estiver acessando dentro da sua base de dados, não permitindo o acesso as demais dependências da rede.

9. Estrutura dos Dados no Cliente

OS dados no cliente deverão ser mantidos de forma organizada para garantir o uso das potencialidades de coordenação do aplicativo de PLM. Uma das formas sugeridas para trabalho com PLM e estruturar os dados hierarquicamente criando o então conhecido DMU, *Digital Mockup,* conforme definido por, SCHUTZER 2002, é a combinação de geometrias de CAD dispostas hierarquicamente em componentes, subconjuntos e conjuntos. Está sistemática vem sendo amplamente utilizada nas indústrias, principalmente a automobilística.

9.1. Estrutura do DMU para Garantir o Sigilo do Projeto do Acesso Remoto

A montagem final do DMU é centralizada no cliente, o fornecedor envolvido no projeto a fim de estudos, conferencia e aprovação de componentes ou conjuntos, se conectará a rede do cliente e iniciará a transferência do arquivo referente ao componente ou parte do conjunto que está desenvolvendo e por fim acessa a porção do DMU que interage com o seu componente.

O reconhecimento pelo sistema dos arquivos que terá acesso, a fim de que o sigilo do projeto seja mantido, será limitada pelo grupo de usuários a que pertence ou a arquivos em que tem o direito de visualização.

A lógica de formação do DMU, exemplificada na figura 8, permitirá criar usuários pertencentes a grupos específicos a sua área divididos em níveis que limita a profundidade de acesso ao DMU (figura 2) além de ter o acesso limitado a determinados arquivos dentre desse grupo.

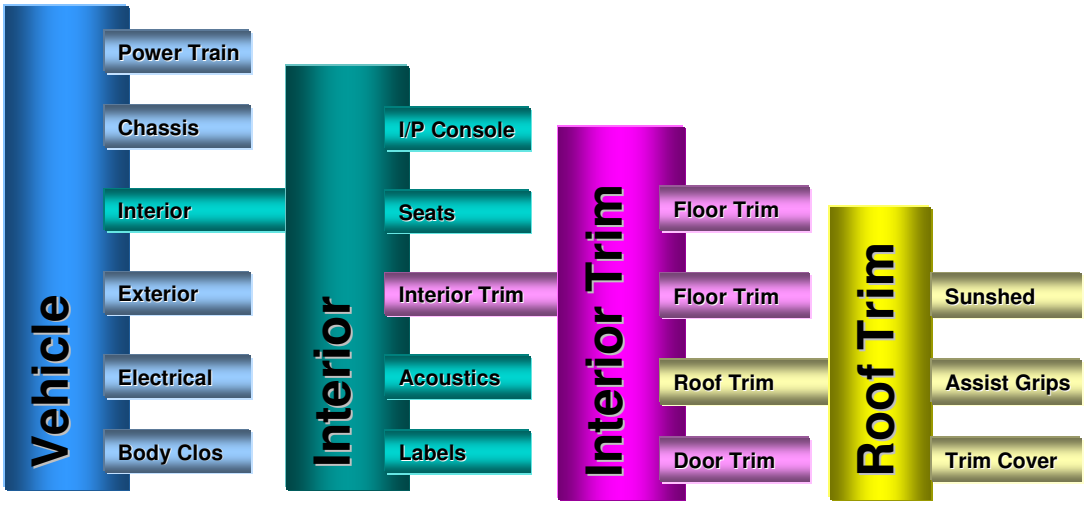

Figura 8 – Exemplo de divisão de conjuntos, subconjuntos e componentes do DMU

10. Requisitos e procedimentos aos potencias participantes da rede de colaboração

Com base no exposto neste trabalho, a sinergia de desenvolvimento do produto a distancia se torna possível, desde que algumas padronizações e pré-requisitos sejam atendidas, para que o fornecedor seja um nodo da rede de colaboração. A padronização de aplicativos e velocidade da conexão a rede pública são itens que devem ser obrigatoriamente atendidos, assim definiu-se os requisitos mínimos de equipamentos e aplicativos. O cliente por ser o centralizador das informações e proprietário do projeto define estes requisitos mínimos que são:

Aplicativos:

- Aplicativo de comunicação e acesso remoto
- Aplicativo de PLM para gerenciamento do projeto
- Aplicativo de CAD

Conexão a rede publica e segurança:

- Velocidade mínima de conexão ao provedor
- Sistema de segurança para trafego de dados nas redes públicas.

Equipamentos.

- Com recursos mínimos exigidos para executar os aplicativos.

Pelas definições e testes levantados, conclui-se que os aplicativos devem ser de um mesmo fornecedor para garantir assim a compatibilidade entre os módulos. O fabricante UGS foi o que possuía os aplicativos que atendam todas as necessidades de comunicação e gerenciamento do produto. Com referencia a segurança na transmissão dos dados o modelo teria que atender a facilidade e rapidez de

implementação assim como os de segurança. Desta forma para exemplificar um pacote para a perfeita sinergia entre cliente e fornecedor tem-se:

Aplicativos

- **Comunicação – Team Center Comunity**

Tem a possibilidade de realizar conferências áudio-visual e acesso remoto.

- **PLM – Team Center Engineer**

Gerencia controle de revisões dos modelos neles arquivados, controla acesso de usuários e permissões a arquivos nele armazenados assim como gerenciamento de grupos de trabalho.

- **Aplicativo de CAD – UGNX3**

Além de ser um software completo para geração dos modelos 3D interagem totalmente com o Team Center Engineer

Conexão a rede publica e segurança:

- Velocidade de conexão mínima 2Mbs
- Uso de redes VPN para a segurança da transmissão de dados.

Equipamentos:

Conforme recomendado pela UGS os computadores para executar este pacote de aplicativos de ter seguinte configuração mínima:

- Processador – Pentiuim Dual Core 3.6Mhz
- Memória Ram – 2Gb
- Interface de vídeo com 256Mb

11. Melhoria Proposta

Nas diversas reuniões que houve com a UGS para definição dos aplicativos desempenho deles nas redes públicas e demais configurações necessárias para aplicar a metodologia de trabalho proposta nesta dissertação, um dos itens críticos discutidos foi o acesso remoto ao aplicativo de CAD. Pela tecnologia presente até o momento a visualização da peça que está sendo trabalhada e compartilhada entre os nodos da rede se dá no transporte das informações contidas na tela (imagens gráficas) do computador em que se está operando aos demais computadores conectados a ele.

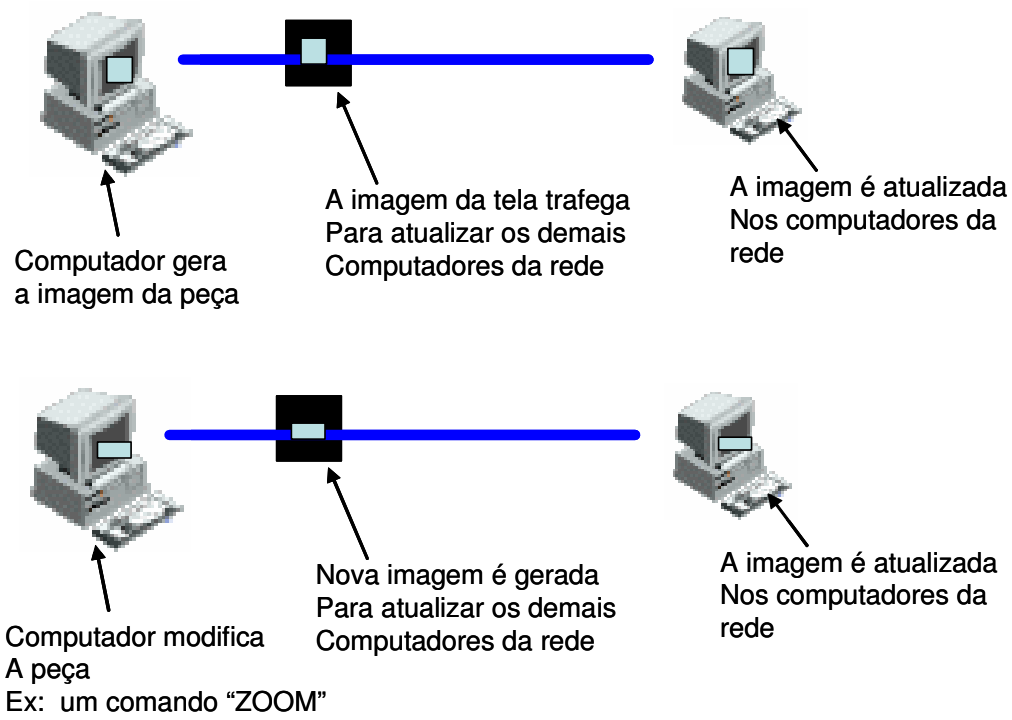

Figura 9 – Acesso Remoto método atual

Este pacote de informações, por ser gráfico, tem um volume de informações consideráveis, e a cada atualização da imagem na tela novos pacotes são mandados sistematicamente para atualizar a imagem dos demais computadores da rede. A proposta para melhoria da sinergia de trabalho dentro das limitações de velocidade das redes públicas, será de diminuir a quantidade de informações a serem enviadas pela rede. Como definido, os pacotes de aplicativo têm que ser o mesmo a todos os membros da rede de cooperação, isto significa que todos os nodos têm o mesmo aplicativo de CAD, assim, ao invés de enviar a imagem da tela para atualizar os demais a ela conectada será enviado somente o comando e cada computador executa este comando localmente.

Figura 10 – Acesso Remoto, método proposto.

Embora não tenha sido possível até o momento mensurar o ganho de tempo que este procedimento produz, pode-se observar subjetivamente em testes preliminares que é grande a agilidade produzida.

12. Discussão

Pelos métodos pesquisados e definidos, fica evidente a possibilidade de execução de um projeto por grupos de engenharia dispersos geograficamente, utilizando-se de todo o potencial da tecnologia disponível. As Organizações Virtuais propriamente ditas executam hoje trabalhos menos complexos, embora detenham o potencial para tarefas mais detalhadas. Tais tarefas é proposta neste trabalho pela metodologia das Organizações Virtuais para buscar as melhores competências em engenharias de projeto otimizando qualidade, tempo de desenvolvimento e custo. Apesar da tecnologia da comunicação que as grandes empresas detêm o trabalho ainda é executado ainda de forma quase tradicional. O funcionário da empresa local, apesar de ter seus parceiros distantes, ele ainda se desloca da casa para o trabalho.

Há um aspecto da necessidade da inter-relação pessoal, conforme citado por Fulks; Gerosa e Lucena (2002), o profissional tende a se sentir isolado na forma de trabalho das Organizações Virtuais.

A tecnológica para esse tipo de organização não é mais uma barreira, este obstáculo fica por ora ao fator cultural que por vezes atua com maior peso. Mas será que hoje pessoas comuns já não atuam desta forma? Revendo o conceito de Berto (1997) onde ele diz que as Organizações Virtuais é um novo modelo organizacional que utilizam a tecnologia para unir, de forma dinâmica, pessoas, bens e idéias sem, todavia, ser necessário reuni-las em um mesmo espaço físico, com este conceito em mente e observando as novas formas de aquisição de bens que, com freqüência é utilizado por parte da população nota-se que muitos deixam de ir a loja. Fica mais fácil consultar a internet pelo produto procurado aliando o melhor produto pelo menor preço do mercado.

Por esse prisma o comprador reuniu pela tecnologia as melhores capacidades de oferta disponível na rede.

Pelo crescente públicos de compradores que utilizam este meio, hoje existem lojas “Virtuais”, as quais não possuem uma cede onde se possa ir e efetuar a compra.

Está modalidade de loja, Virtual, tem um faturamento que supera qualquer negócio do mundo real: 68% ao ano é o exemplo de crescimento da empresa de vendas pela internet a loja Submarino (www.submarino.com.br), até dezembro, o faturamento do Submarino será de R$ 570 milhões, graças aos 5 mil itens vendidos diariamente a clientes de todo o Brasil conforme publicado no site “Isto é Dinheiro” (www.terra.com.br/istoedinheiro/417/ecommerce/reis_vendas_internet.htm, 2007).

Estás lojas virtuais somente tem o deposito das mercadorias a serem enviadas. O grupo de funcionários que cuidam dos pedidos podem estar alocados em qualquer lugar. Pode-se ir mais longe, o pedido do item vendido pela loja pode cair direto no fabricante do produto que efetuara a entrega, deste modo nem o deposito ela teria.

Pode-se dizer que esta metodologia está entrando na cultura do mundo atual, lentamente.

O uso da tecnologia da comunicação tende a evoluir o aspecto cultural caminha para aceitação desta metodologia, assim quando desmistificado, a tendência será de o ser humano se sentir próximo e fazendo parte de tudo que ele pode alcançar por este meios, sentado em seu computador.

Poderá chegar um dia que a maioria dos profissionais não terá a necessidade de se locomover à sede da empresa para uma jornada de trabalho, tudo está ao se alcance pelas redes públicas, informações, reuniões por teleconferência, uma lista de colegas de trabalho *on-line* no aplicativo de conferencia onde se podem trocar idéias, conversar e se sentir presente.

Propositadamente não serão citados os ganhos com stress no tráfego diário e outros benefícios similares que são o obvio desta metodologia. Dando continuidade no foco que não se depende mais do espaço físico, se é possível ter a sinergia via os meios propostos, o mercado de trabalho não precisa estar restrito a cidade, estado ou pais onde o profissional resida, não há impedimento de ser funcionário de empresas locadas fora destas áreas, assim o mercado de trabalho torna-se mais abrangente, basta para isso que as barreiras culturais sejam rompidas e a visão vá adiante do mundo real.

A facilidade de comunicação visual, escrita e oral, lembra-se aqui que até a telefonia já está trafegando na rede utilizando protocolos IP, deixa um horizonte infinito de possibilidades de novos negócios e forma de trabalho dos negócios já existentes, para ativá-los, basta a criatividade de quem for usá-la.

13. Conclusões

O objetivo deste trabalho foi de elaborar uma metodologia de trabalho que se possibilita o desenvolvimento de um projeto com engenharias trabalhando simultaneamente e dispersas geograficamente, fundamentada na metodologia das Organizações Virtuais.

Desta forma os métodos aqui abordados requereram um forte apelo da tecnologia disponível, porém sem a necessidade de se criar algo novo a menos dos métodos de interação entre grupos.

Para viabilizar tais métodos foi iniciada a pesquisa dos meios de comunicações capazes de unir os grupos de forma eficiente, segura e de rápida configuração. Assim fora definido as redes públicas como os meios com a segurança suportada em rede privadas VPN que utiliza as públicas para conectar os nodos.

O desenvolvimento de engenharia requer fortemente a troca e coordenação de modelos matemáticos, gerados em CAD, que devem ser visto e compartilhados remotamente entre os colaboradores da rede. Este requisito se completa com a utilização de software comercial de PLM que coordene de forma lógica as diversas partes do produto em desenvolvimento. O aplicativo escolhido foi o produto da empresa UGS chamado TeamCenter Engineer que mostrou ótimo potencial em gerenciar as informações nele armazenada de forma hierárquica com histórico de modificações ocorridas e gerenciamento de grupos de usuários de forma que a base de dados possa ser acessada sem que a sigilo do projeto fosse quebrado.

Para haver a comunicação e acesso remoto entre os grupos, definiu-se um software também da UGS, TeamCenter Comunication capaz de interagir desta forma com a limitação de velocidade das redes públicas e total interação com o TeamCenter Engineer e ambos com o software de CAD da mesma empresa o UGNX3.

A qualidade de comunicação pelas redes públicas usando este pacote de aplicativos fora mensurado pelo tempo de atraso entre pontos remotos localizados dentro e fora

do país. Entre cidades do mesmo país observou-se um tempo de atraso na comunicação na ordem de 40ms e entre Brasil e Estados Unidos na ordem 140ms. Os testes de acesso remoto a essas velocidades pelos aplicativos citados acima se mostraram satisfatório, viáveis para manter a sinergia de trabalho entre os grupos.

Tais testes foram feitos de maneira subjetiva, baseando-se no maior tempo de atraso admissível para tarefas mais criticas como da tele-cirurgia, que por pesquisas feita pelo Dr. Ivan Pisa do Departamento de informática em Saúde da Universidade Federal de São Paulo – UNIFESP – cita que este tempo máximo admissível para esta aplicação é de 155ms. Também considerado que o tempo em que se começa a perceber que há atraso é de 80ms. Porém fica uma sugestão para próximos trabalhos, de uma forma de mensurar matematicamente para a nossa aplicação o tempo de atraso máximo admissível.

Considerando os itens aqui expostos conclui-se que é possível a metodologia de trabalho a distancia mantendo a sinergia de trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

BENBUNAN-FICH, R.; HILTZ, S.R. Impacts of Asynchronous Learning Networks on Individual and Group Problem Solving: A Field Experiment. **Group Decision and Negotiation**, Vol.8, 1999, p. 409-426.

BERTO, R. S. Organizações Virtuais: Revisão Bibliográfica e Comentários. In: ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 1997, Gramado, RS. **Anais**... Porto Alegre: UFRGS.PPGEP, 1997.

BRINCK, T.; MCDANIEL, S.E. **Awareness in Collaborative Systems**: Workshop Report. SIGCHI Bulletin 29, (4), 1997, p.68-71.

CLEGG, S. R.; HARDY, C.; NORD, W. R. **Handbook de estudos organizacionais**. São Paulo: Atlas, 1999. 1 v.

DAVIDOW, W. H.; MALONE, M. **A Corporação Virtual**: estruturação e revitalização da corporação para o século 21. São Paulo: Pioneira, 1993.

DOURISH, P.; BELLOTI, V. Awareness and coordination in shared workspaces. In: Computer Supported Cooperative Work 1992, Toronto, Ontario. **Proceedings...**USA: ACM Press, 1992, p. 107-114.

ELLIS, C.A.; GIBBS, S.J.; REIN, G.L. Groupware - Some Issues and Experiences, **Communications of the ACM**, Vol. 34, N. 1, 1991, p. 38-58.

FUKS, H.; ASSIS, R.L. Facilitating Perception on Virtual Learningware-based Environments, **The Journal of Systems and Information Technology**. Australia: Edith Cowan University, v 10 n. 1, 2001. 93-113 p.

FUKS, H.; ASSIS, R.L. Facilitating Perception onVirtual Learningware-based Environments, **The Journal of Systems and Information Technology**, Vol 5., No. 1, Edith Cowan University, Australia, 2001, p. 93-113.

FUKS, H.; GEROSA, M.A.; LUCENA, C.J.P. The Development and Application of Distance Learning on the Internet, **The Journal of Open and Distance Learning**, Vol. 17, N. 1, 2002, pp. 23-38.

FUSSEL, S.R.; KRAUT, R. E.; LEARCH, F.J., SCHERLIS, W.L., MCNALLY, M.M.; CADIZ, J.J. Coordination, overload and team performance: effects of team communication strategies, In: ACM conference on Computer supported cooperative work, 1998, Seattle, USA. **Proceedings...** New York: ACM Press , 1998. p. 275-284.

GOLDMAN,S.L; NAGEL, R. N.; PREISS, K. **Agile Competitors: Concorrência e Organizações Virtuais e estratégias para valorizar o cliente**. São Paulo: Érica, 1995.

GUTWIN, C., GREENBERG, S**.** A framework of awareness for small groups in shared-workspace groupware, **Technical Report** 99-1, Saskatchewan University, Canada, 1999.

LEON, M.E.: **Uma Análise de Redes de Cooperação das Pequenas e Médias Empresas do Setor das telecomunicações**. 1998. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo, São Paulo, 1998.

MALONE, T.W.; CROWSTON, K. What Is Coordination Theory and How Can It Help Design Cooperative Work Systems?. In: COMPUTER SUPPORTED COOPERATIVE WORK, 1990, Los Angeles, USA. **Proceedings….**New York: ACM Press, 1990. p. 357-370.

MERKLE, M. **Virtual Organizations:** how quality management paves the way for it. Institute for Technology Management, University of St. Gallen, Switerland.

PRAHALAD, C.K.; HAMEL, G. **Competindo pelo futuro:** estratégias inovadoras para obter o controle do seu setor e criar os mercados de amanhã. 15 ed. Rio de Janeiro: Campus, 1995.

PUTNAM, L.; POOLE, M.S. Conflict and Negotiation**.** In F. Jablin, L. Putnam, K. Roberts & L. Porter (Eds.), **Handbook of Organizational Communication: An Interdisciplinary Perspective**. Newbury Park: Sage Publications, 1987. 549-599 p.

RAPOSO, A.B.; MAGALHÃES, L.P.; RICARTE, I.L.M.; FUKS, H. Coordination of collaborative activities: A framework for the definition of tasks interdependencies. In: International Workshop on Groupware – CRIWG, 7**.** 2001, Darmstadt, Germany. **Proceedings…** IEEE: Computer Society Press, 2001. p.170 – 179.

SALOMON, G.; GLOBERSON, T. WhenTeams do not Function the Way They Ought to, **Journal of Educational Research**, USA, 13, (1), 1989, p. 89-100.

SCHIMTZ, H. **Small Firms and Flexible Specialization.** Sussex: The University of Sussex: IDS, 1989.

SCHUTZER, K. **Implantação do digital mockup na indústria automobilística: conquistando vantagens competitivas**. São Paulo: UMP, 2002.

STRAUSAK, N. Resume of VoTalk. In: SIEBER, P.; GRIESE, J.(eds). Organizational Virtualness. **Proceedings of the VoNet - Workshop**, April 27-28, 1998. Bern, Simona Verlag Bern, 1998, p. 9-24

TRAVICA, B. The Design of the Virtual Organization: A Research Model. In: ASSOCIATION FOR INFORMATION SYSTEMS - AMERICAS CONFERENCE 1997, Indianopolis, Indiana. **Proceedings**.. Indianopolis, Indiana, 1997

WINOGRAD, T. A Language/Action Perspective on the Design of Cooperative Work, IN**: Computer Supported Cooperative Work** - A book of readings, Edited by Irene Greif, Morgan Kaufmann Publishers, USA, 1998.

WINOGRAD, T.; FLORES, F. **Understanding Computers and Cognition***.* Addison-Wesley, USA, 1987.

BRANCATO, P. **Infra-Estrutura de Internet**. Disponível em: http://www.projetoderedes.com.br/. Acesso em: 01 maio 2006.

BUENO, R. A. **Endereçamento IP com Subredes.** Disponível em: http://www.projetoderedes.com.br/. Acesso em 01 maio 2006.

CHIN, L. K. **Rede Privada Virtual**. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acesso em: 01 abr. 2006.

CISCO. **VPN Client;** Disponível em: http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html. Acesso em: 04 maio 2006.

MICROSOFT. Step-by-Step Guide to Internet Protocol Security (IPSec). Disponível em: http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.mspx Acesso em: 10 Jun. 2006.

MICROSOFT. **Virtual Private Networks;** Redes Privadas Virtuais, Windows Server. Disponível em: http://www.microsoft.com/technet/network/vpn/default.mspx; Acesso em: 21 set. 2006.

NETO, J. A. **As Organizações Virtuais Como Rede Globais de Empresa.** Disponível em: http://www.empresario.com.br/artigos/artigos_html/artigo_061000.html; Acesso em: 12 Jul. 2006.

SILVA, A. B. **Redes de Computadores Cabamento e Topologia** Disponível em: http://www.inf.pucrs.br/~benso/redesanalise/20042/cabeamento_topologia. Acesso em: 10 maio 2006.

TRÖGER, A**. Um Estudo Sobre Organizações Virtuais**. Disponível em: http://palazzo.pro.br/artigos/organiza.htm. Acesso em: 12 Jul. 2006.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. Grupo de Teleinformática e Automaação. **IPSec. Protoclo de Segurança IP.** Disponível em: http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/ipsec.html. Acesso em: 10 Jun. 2006.

VILLHA, A. P. **Organizações Virtuais Um Novo Paradigma Organizacional do Século XXI.** Disponível em: http://www.ccuec.unicamp.br/revista/infotec/artigos/anapatr.html. Acesso em: 23 ago. 2006.

ZIMMERMANN, F.O. **Structural and Managerial aspects of Virtual Enterprises**, WZL-Aachen, Germany, 1997. Disponivel em: http://www.seda.sowi.inibamberg.de/persons/zimmermann/paper. Acesso em: 03 Ago. 2006.

GLOSSÁRIO

AH	*Authentication Header* Modelo de autenticação de cabeçalho para tráfego de dados. Adiciona autenticação e integridade, ou seja, garante a autenticidade do pacote e também que este não foi alterado durante a transmissão;
ADSL	Tecnologias que fornecem um meio de transmissão digital de dados, aproveitando a própria rede de telefonia.
BACKBONES	Ramo Principal das redes públicas;
CAD	*Computer Aid Design* – Sistema responsável em criar desenhos por computador em duas ou três dimensões
DHCP	Sistema Automático de endereçamento IP para computadores conectados em rede;
DMU	*Digital Mockup* – Sistema de criação de conjuntos dispostos hierarquicamente feitos em computador;
ESP	*Encapsulating Security Payload*. – Protocolo de comunicação para redes com segurança de dados. Adiciona autenticação e confidencialidade**,** garantindo que somente os destinatários autorizados terão acesso ao conteúdo do pacote;
HOP-COUNT	Contador de pacotes encaminhados entre computadores
IP	*Internet Protocol* – Protocolo de comunicação entre computadores conectados em rede;
INTERNET	Conglomerado de redes em escala mundial de milhões de computadores interligados que permite o acesso a informações e todo tipo de transferência de dados.

INTRANET	Redes coorporativas privadas de larga abranjencia
IPSec	*Internet Protocol Security* – Especificação que define procedimentos de segurança em redes públicas;
IPv4	*IP version 4* – Protocolo de comunicação entre computadores conectados em rede com capacidade de dados de 32Bits
IPv6	*IP version 6*, ou ainda, *IPng IP Next Generation*, é a nova versão do protocolo IP desenvolvida para suprir as deficiências de seu precursor, o IPv4, tais como, a adição de mecanismos de segurança e qualidade de serviço, além do aumento do espaço de endereçamento;
ISAKMP	Mecanismo de troca de chaves para redes privadas virtuais que gerencia a troca de chaves de criptografia;
ISP	*Internet Service Provide* – Provedor de conexão as redes públicas;
LAN	*Local Area NetWork* – Rede Local de Computadores;
Links	Conexão logica entre computadores dispostos em rede;
NAP	*Network Access Point* – Empresa responsavel em ligar os ISP ao Backbone das redes públicas;
NetBEUI	Acrônimo para NetBIOS Extended User Interface (Interface de Usuário Estendida NetBIOS). Ele é uma versão melhorada do protocolo NetBIOS usado por sistemas operacionais de rede;
PLM	*Product Lifecycle Management* – Aplicativo de gerenciameto do ciclo de vida do produto;
PPP	*point-to-point protocol*, protocolo de rede responsavel em transportar todo o tráfego entre 2 dispositivos de rede através de uma conexão física única. Embora seja um protocolo, o PPP encontra-se na lista de interfaces;

ROUTEADOR	Roteador ou *router* ou encaminhador é um equipamento usado para fazer a comunicação entre diferentes redes de computadores. Este equipamento provê a comunicação entre computadores distantes entre si
TCP/IP	*Transmission Control Protocol/Internet Protocol*, conjunto de protocolos da Internet;
TUNELAMENTO	Termo usado para representar uma conexão segura entre dois ou mais computadores conectados a rede pública
UDP	Potocolo orientado à conexão, que inclui vários mecanismos para iniciar e encerrar a conexão, negociar tamanhos de pacotes e permitir a retransmissão de pacotes corrompidos.
VPN	*Virtual Private NetWork* – Redes privadas que estão suportadas pelas redes públicas
WAN	*Wide Area Network* – Redes de abrangencia global
Wifi	Redes de computadores por conexões sem fio.