# D O S S I Ê  T É C N I C O

## Como implementar uma rede local na empresa com intenção de compartilhar arquivos e impressoras

Arley Pinheiro Mendes

Centro de Apoio ao Desenvolvimento Tecnológico – CDT/UnB

outubro
2007

## Sumário

## Título

Como implementar uma rede local na empresa com intenção de compartilhar arquivos e impressoras

## Assunto

Outras atividades de telecomunicações não especificadas anteriormente

## Resumo

Uma das grandes dificuldades das MPEs é de possibilitar a utilização completa de uma rede, não só utilizando-a para compartilhamento da internet. Esse dossiê irá descrever como uma rede local entre computadores pode facilitar e melhorar o tempo dos processos eletrônicos de uma empresa, segurança dos documentos, compartilhamento de impressoras e outros aspectos ligados a infra-estrutura e configuração. O documento apresenta todos os passos envolvidos na montagem e configuração, bem como seus aspectos benéficos e diferenciais que uma rede pode oferecer.

## Palavras chave

Informática; computadores; rede; compartilhamento; segurança; telecomunicações;

## Conteúdo

### 1. Introdução

A atual rapidez nas trocas de informações exige que as empresas construam um ambiente que propicie esta dinamicidade na produção de bens ou serviços. As redes locais LAN (Local Area Network) é uma das soluções para que os funcionários de uma empresa possam de forma prática e eficiente acessar documentos, arquivos, impressoras, internet, intranet comunicar-se com outros funcionários, entre outras diversas possibilidades de serviços agregados a estas redes.

Uma LAN em sua concepção constitui de um grupo reduzido de terminais com acesso a rede e por isto são chamadas de redes locais. Seu objetivo é formar um ambiente integrado e que permita a comunicação veloz e segura entre terminais próximos. Assim como as LANs existem as MANs (Metropolitans Areas Networks) que consistem em um conjunto de redes menores, ou seja, aglomera várias redes locais e proporciona a interligação entre elas para um raio de abrangência maior que o da rede local (exemplo, uma cidade) e por fim as WANs (Wide Areas Networks) que são redes de longa distância também conhecidas como redes geograficamente distribuídas, responsáveis por interconectar as MANs espalhadas por diversas regiões.

O planejamento sério de uma rede local precisa anteriormente de um levantamento prévio sobre algumas características e necessidades da empresa, tais como: número de funcionários que devem ser atendidos com pontos de comunicação, quais tipos de tráfego percorrerão a rede a ser instalada, ou seja, os serviços que serão implementados juntos a ela, qual velocidade de conexão para os usuários finais (no caso, funcionários), nível de segurança dos dados, controle de acesso a rede e etc.

Esse estudo é de fundamental importância para a escolha dos equipamentos adequados e ferramentas a serem instaladas, permitindo que a elaboração do projeto atenda não somente a demanda de pontos de uma empresa, mas também forneça qualidade de

acesso, alta disponibilidade, confiabilidade e previsão de expansão para esta rede.

Este dossiê traz como objetivo mostrar de forma rápida e clara quais passos devem ser adotados para implementar uma rede LAN afim de usufruir as diversas funcionalidades de um ambiente com compartilhamento de serviços para aceleração dos processos eletrônicos de uma micro e pequenas empresas.

## 2. Redes de computadores

Alguns aspectos gerais sobre redes de computadores serão comentados ao longo do dossiê técnico para o entendimento de conceitos importantes e anteriores a implementação de uma rede local. Estas noções são úteis não só para o esclarecimento, como também para configuração da LAN de acordo com as necessidades da empresa.

### 2.1. Modelos de referência

Os modelos de referência organizam e agrupam de acordo com as funcionalidades em comum, os conjuntos de protocolos (procedimentos de comunicação rigorosamente padronizados) que são utilizados para interconectar as redes de computadores visando prover a interoperabilidade entre tecnologias e equipamentos de diversos fabricantes. Estes modelos consistem no pilar principal para que a redes de computadores, principalmente a Internet, abrangesse de forma tão acelerada e maciça todas as regiões do globo. Existem dois modelos mais comentados, sendo eles: o modelo OSI (Open Systems Interconnection) e o modelo TCP/IP (Transport Control Protocol / Internet Protocol)

#### 2.1.1. Modelo OSI

Modelo de referência criado pela ISO (International Organization for Standardization), pioneira em formalmente criar uma arquitetura universal para interconectar computadores.

Este modelo utiliza a idéia de sistemas abertos:

- Sistemas que suportam os padrões OSI na comunicação entre outros sistemas que também empregam tais padrões;

- Os sistemas não estão presos a particularidades de implementação ou tecnologias diferentes.

A estrutura deste modelo divide a rede de computadores em camadas de abstração que podem atuar independentemente uma das outras, ou seja, cada protocolo que exerce características em comum pertencerá a mesma camada e os serviços atendidos em cada uma delas serão levados para as N+1 camadas acima ou N-1 camadas abaixo dela, dependendo do sentido da comunicação. Cada nível ou camada de um determinado sistema aberto irá comunicar-se com a mesma camada de outro sistema mediante os protocolos que fazem parte.

O modelo OSI é composto basicamente por sete camadas, sendo elas:

- **Camada física:** define o tipo de meio físico usado para a conexão, tipo de cabos e conectores, níveis de sinal, velocidade de transmissão, método de codificação e etc.

- **Camada de enlace:** define as regras para estabelecer, manter e liberar conexões entre sistemas diretamente conectados. Define o formato de quadro a ser transmitido e procedimentos de controle e acesso ao meio físico.

- **Camada de rede:** responsável pelo endereçamento e roteamento das mensagens (pacotes) entre as diversas redes, controle de congestionamento, fragmentação e seqüenciamento de pacotes, tratamento de erros, entre outros.

- **Camada de transporte:** responsável pelos serviços orientados a conexão

(protocolo TCP), conferindo a integridade do pacote ou serviços não orientados à conexão (protocolo UDP – User Datagram Protocol) que não asseguram integridade do pacote, contudo, permite o envio deste em taxas maiores. Além dos itens citados a camada é responsável pelo controle de fluxo, reconhecimento e ordenação dos pacotes, correção de erros, dividi os dados oriundos da camada de sessão em pacotes.

- **Camada de sessão:** responsável por estabelecer, sincronizar, gerenciar e terminar os processos de comunicação entre as aplicações de usuários pela rede.

- **Camada de Apresentação:** conhecida como camada de Tradução, converte o formato dos dados recebidos pela camada de Aplicação em um formato comum a ser usado na transmissão desses dados, ou seja, um formato entendido pelo protocolo usado, por exemplo, converter um padrão de caracteres (texto) em um padrão no qual o dispositivo transmissor é capaz de interpretar (ASCII, dados em binários).

- **Camada de aplicação:** presta serviços básicos para os usuários finais (serviço web, correio eletrônico, troca de arquivos, entre outros), ou seja, faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através da rede.

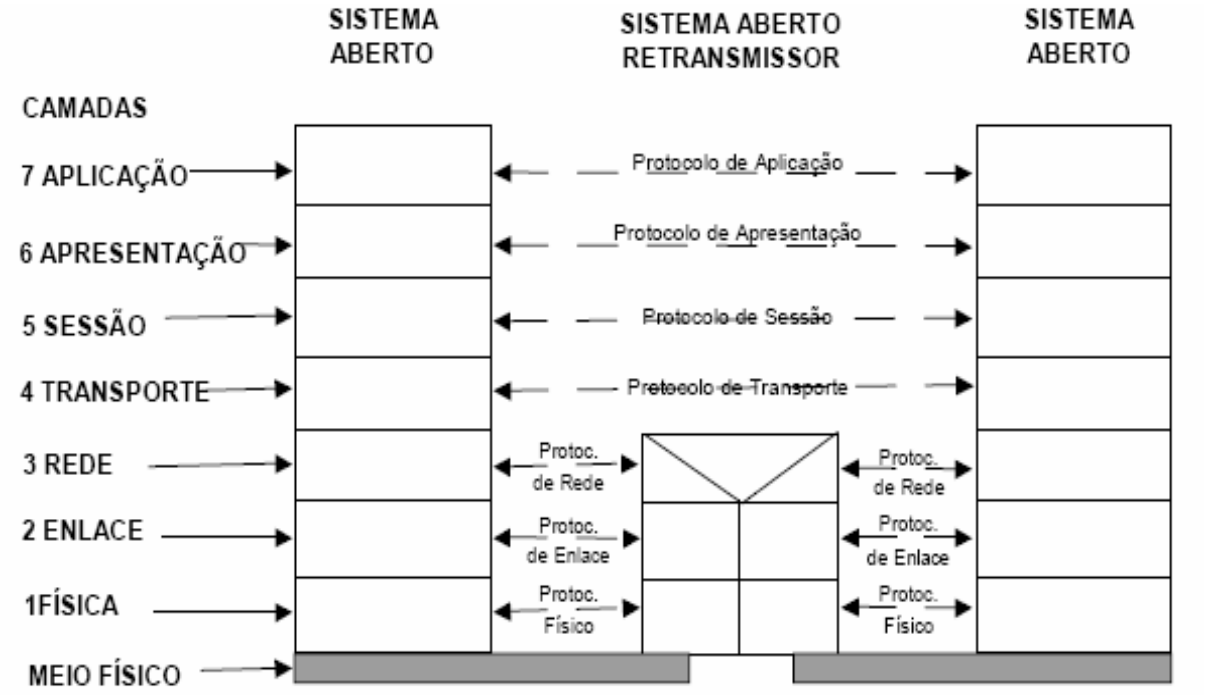



FIG. 1 – Camadas do Modelo OSI
Disponível em: Arquitetura de Redes de Comunicação, Prof. Ricardo Puttini. Junho/2001

### 2.1.2. Modelo TCP/IP

Chamada alternativamente de arquitetura internet, este consiste do agrupamento de camadas do modelo OSI que permite resolver alguns problemas referentes à transmissão de dados e fornecer um serviço bem definido para os protocolos nesses níveis. As camadas mais altas, deste modelo, estão mais próximas dos usuários (camada de aplicação) e lidam com dados mais abstratos, confiando nas camadas inferiores para traduzir eles em formatos que podem ser transmitidos.

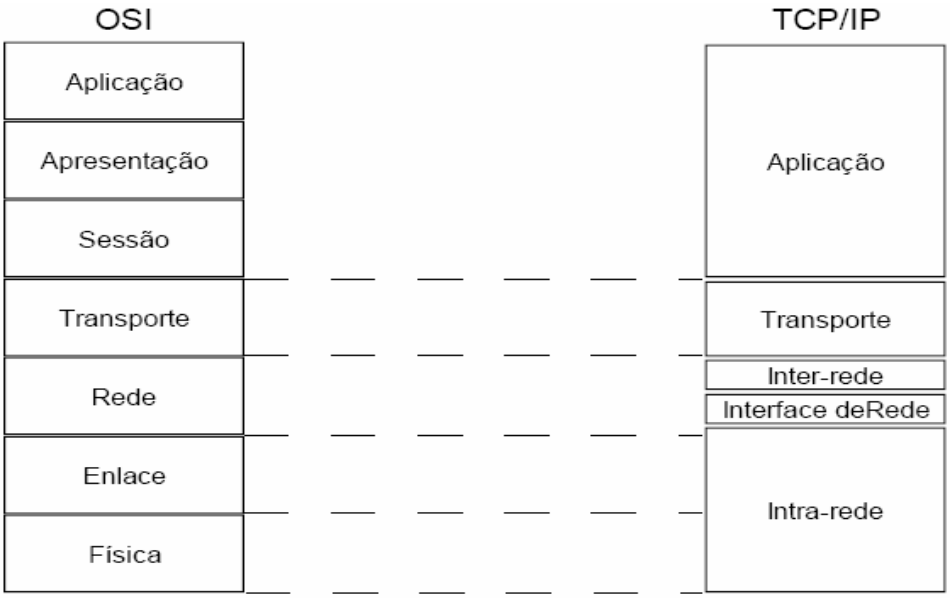



FIG. 2 – Comparativo de camadas entre Modelo OSI e TCP/IP
Disponível em: Arquitetura de Redes de Comunicação, Prof. Ricardo Puttini. Junho/2001

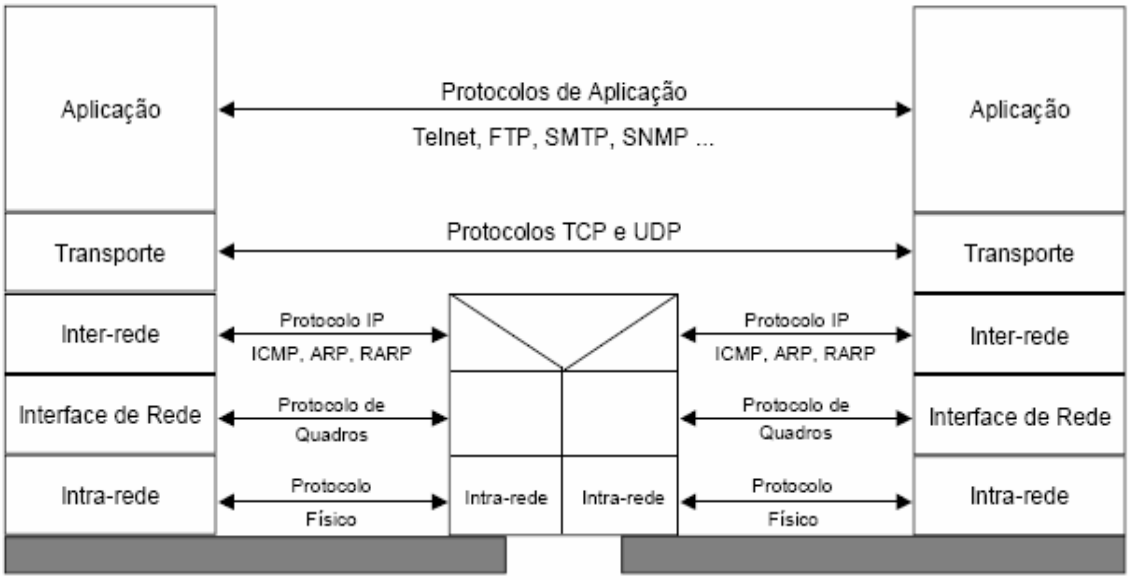



FIG. 3 – Camadas do Modelo TCP/IP
Disponível em: Arquitetura de Redes de Comunicação, Prof. Ricardo Puttini. Junho/2001

## 2.2. Tecnologias de rede local

### 2.2.1. IEEE 802.3 (Ethernet)

A tecnologia Ethernet foi concebida para interconectar redes locais, definindo o cabeamento, sinalização elétrica para camada física, formato de pacotes e protocolo de controle de acesso ao meio via camada MAC (Media Access Control) do modelo OSI (camada de enlace). A espinha dorsal desta tecnologia consiste na mais comum técnica de controle de acesso ao meio CSMA/CD (Carrier Sense Multiple Access/Collision Detection) especialmente para topologias em barramento estrela. Surgiu pioneiramente através de um projeto da Xerox PARC coordenado pelo pesquisador Robert Metcalfe que enxergou o grande potencial de aplicabilidade desta inovação para redes locais, posteriormente esta tecnologia veio a competir e ganhar espaço entre as já vigentes Token Ring, ARCNET e FDDI durante a década de 80.

O padrão IEEE 802.3 definindo universalmente todas as características técnicas da tecnologia Ethernet foi concretizado apenas na década de 80, no entanto, sua aplicação entre as redes locais já era significativamente difundida.

A Ethernet assemelha-se muito a um sistema de rádio onde vários terminais desejam transmitir utilizando os mesmos recursos físicos, ou seja, se uma estação deseja enviar alguma informação para outro dispositivo na rede em que se encontra, esta deve “escutar” o meio físico até que o mesmo fique ocioso para assim transmitir (técnica de acesso ao meio CSMA/CD). Anteriormente ao CSMA/CD existiam dois precursores: ALOHA e SLOTTED ALOHA que garantiam uma baixa eficiência na utilização do canal, em torno de 18% e 37 %, respectivamente. Nota-se então que a taxa de throughput (taxa de envio de pacotes pelos terminais na rede) e a perda de pacotes inviabilizavam o ALOHA e SLOTTED para tráfegos que demandavam elevadas taxas de transmissão.

### 2.2.2. IEEE 802.3u (Fast Ethernet)

O padrão 100BASE-T, batizado como Fast Ethernet, surgiu devido ao aumento do número de usuários e da grande demanda de tráfego pelas aplicações multimídias, exigindo das redes Ethernet um desempenho maior do que os seus 10 Mbps. Para resolver este problema foi criado o IEEE 802.3u que possui as principais características do padrão Ethernet, como: formato de frame, mecanismo de acesso ao meio CSMA/CD, tamanho do frame, diferenciando-se apenas com relação a velocidade de transmissão dos pacotes que passou de 10 Mbps para 100 Mbps, ou seja, um acréscimo de 10 vezes em relação ao padrão original.

Esta nova tecnologia possui uma relação custo/benefício bastante interessante para a tamanha velocidade que oferece, além de conseguir facilmente integrar-se as redes Ethernet proporcionando pouca ruptura. Isto tornou a aplicabilidade do Fast Ethernet cada vez mais comum em todo o mundo.

Suas principais vantagens além das citadas anteriormente são:

- Proporciona uma migração simples e flexível, através de adaptadores "autosense" de 10/100 Mbps;
- Não requer treinamento de pessoas, pois o Fast Ethernet praticamente não se difere do padrão Ethernet;
- Se o cabeamento não for muito antigo, por exemplo, cabo coaxial, esta tecnologia funciona perfeitamente, sem a necessidade de substituí-lo.

As desvantagens são:

- Utiliza o CSMA/CD que roda imprevisilvemente sob carga de tráfego pesada, ou seja, seu funcionamento não é ótimo com o aumento de tráfego nestas redes;

- Como conseqüência do item acima, a capacidade de throughput é reduzida.

Existem três diferentes variantes de implementação física do padrão Fast Ethernet e são elas:

- 100BASE-TX: é recomendável a utilização de 2 pares de cabo UTP categoria 5 ou 2 pares de cabo STP (cabos blindados eletromagneticamente), suportando transmissões half-duplex / full-duplex;
- 100BASE-T4: utiliza 4 pares de cabo UTP (cabos não blindados eletromagneticamente), categoria 3, 4 ou 5; suportando somente transmissões half-duplex;
- 100BASE-FX: utiliza fibra óptica, para transmissões half-duplex ou full-duplex.

Resumindo, o padrão Fast Ethernet oferece uma boa solução de atualização para redes Ethernet, no entanto, já existe o padrão Gigabit Ethernet – 1000BASE-TX (1Gbps de velocidade de transmissão) que vem como uma atualização do padrão 100BASE-TX.

### 2.2.3. IEEE 802.11 (Wi-Fi)

Este padrão define as redes conhecidas como Wi-Fi ou wireless devido a ausência de fios para conectar-se nelas. Esta característica revolucionou o mundo das LANs em termos de conectividade e praticidade, pois as velocidades de transmissão e a facilidade de instalação comparada a uma estrutura cabeada lhe conferem um grau de aceitação muito grande pelos consumidores, tanto que a maioria dos computadores portáteis fabricados atualmente suporta esta tecnologia.

A especificação do IEEE 802.11 é separada em varias partes levando em conta critérios como: velocidade de transmissão, freqüência de operação dos Access points - AP (Pontos de acesso, em português), tratamento de QoS (Quality of Service), segurança dos dados, alcançabilidade e etc. Cada parte agrega uma funcionalidade diferente ao padrão e são identificadas com letras do alfabeto seguida da numeração do padrão. Ex: 802.11a... 802.11v.

Os dois módulos mais empregados do padrão pelos fabricantes são:

**IEEE 802.11b**

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE e velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na freqüência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funciona na mesma freqüência de operação (2,4 GHz) que telefones móveis, fornos microondas e dispositivos Bluetooth. O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita, bem como a disponibilidade livre de uso em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

**IEEE 802.11g**

Baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 54 Mbps. Funciona também dentro da freqüência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). A vantagem é a velocidade. Usa autenticação WEP estática.

### 2.3. Elementos de rede

Os dispositivos de rede são classificados de acordo com sua forma de aplicação na rede, existindo duas categorias básicas:

- Elementos ativos de rede: são os responsáveis pela comunicação adequada e confiável entre estações de trabalho, servidores (maquinas dedicadas a um serviço de rede) ou Internet. Ex: roteadores, bridges, switches, access points.

- Elementos passivos de rede: são componentes responsáveis pelo transporte de dados a nível físico, ou seja, cabos, tomadas, tubulações e acessórios de cabeamento em geral.

#### 2.3.1. Roteador

Elemento de rede que atua na camada 3 do modelo OSI (Ver FIG. 1), responsável pelo encaminhamento dos pacotes para as rotas de destino alcançáveis, ou seja, escolhe a melhor rota para o pacote chegar ao seu destino proporcionando a interligação entre redes locais ou redes remotas (MAN's e WAN's). Além disto, este dispositivo pode realizar outras funcionalidades avançadas como: alertar congestionamento na rede, adotar políticas de QoS (Quality of Service), agregar função de NAT (Network Address Translation), Firewall, DHCP, interface e roteamento para diferentes tecnologias e protocolos de rede, entre outras tarefas.

FIG. 4 – Roteador
Disponível em: <http://www.msln.net/msln/curcust/1720_install.html>.

### 2.3.2. Bridges

Consistem em equipamentos que atuam na camada 1 e 2 do modelo OSI (Ver FIG. 1) com a funcionalidade de segmentar a rede local em várias sub-redes. Este filtra os pacotes de tal forma que os enviados em um determinado segmento, somente serão repassados para os demais segmentos (sub-redes) se o endereçamento estiver corretamente apontado para eles. Outras funcionalidades comuns aos bridges são: armazenar pacotes em caso de tráfego muito grande, filtrar pacotes com erros e evitar que sejam retransmitidos e atua como repetidores comuns dentro do mesmo segmento, ou seja, um pacote enviado com destino ao mesmo segmento em que se encontra será enviado a todos terminais nele presente.


FIG. 5 – Bridge
Disponível em: <http://www.ssos.com/networks.html>.

### 2.3.3. HUB

Elemento de rede que atua na camada 1 e 2 do modelo OSI (Ver FIG. 1) sendo responsável pela distribuição de pacotes aos terminais conectados a rede local. Funciona como um espelho ou repetidor, todo pacote que for enviado para algum outro computador dentro da rede local será encaminhado a todos os demais terminais conectados ao hub, isto o torna de certa forma ineficiente para uma rede LAN com número considerável de máquinas conectadas, pois esse mecanismo proporcionará aumento de tráfego, diminuindo a taxa de throughput da rede e conseqüentemente reduzindo o desempenho da mesma. Sua utilização geralmente é aconselhada para um número bem reduzido de estações.


FIG. 6 – HUB
Disponível em: <http://www.hw-group.com/products/sensors/HTemp-485_en.html>.

### 2.3.4. Switches

Este dispositivo assemelha-se ao hub na tarefa de centralizador de terminais locais, no entanto, este realiza a função de forma mais eficiente que o dispositivo anteriormente citado. Os switches criam um link de comunicação fim a fim com a estação que deseja enviar o pacote e o destinatário, não precisando o envio de várias cópias deste pacote para todos os terminais de uma rede local, reduzindo assim o tráfego desnecessário. Também chamados

de hub's inteligentes, alguns destes podem ser gerenciados de forma a aumentar ainda mais o desempenho de uma LAN, com a técnica chamada de Virtual LAN (padrão IEEE 802.1Q), configuração que divide as portas do switch da rede local em grupos específicos, exemplo, portas do switch que atende somente o setor do pessoal do marketing, da engenharia, entre outras áreas. Esta característica diminui algumas desvantagens do padrão Ethernet com relação a perda de pacotes por colisão de sinais.

FIG. 7 – Switch
Disponível em: <http://www.ldlc.com/photo/PB00046222/cisco-catalyst-2950-24.html>.

### 2.3.5. Access Points (APs)

Elementos de rede que trabalham na camada 1 e 2 do modelo OSI (Ver FIG. 1) e são responsáveis pela interface área entre terminais e a rede wireless local. Em geral trabalham com os padrões 802.11b e 802.11g para realizar sinalização, estabelecer níveis de potência para transmissão e recepção, alcance de cobertura, taxas e freqüências de operação, entre outras características.


FIG. 8 – Access Point
Disponível em: <http://www.amazon.com>.

### 2.3.6. Placas de rede ou adaptadores de LAN

Funcionam de interface entre o computador e o meio físico (cabeamento de rede), proporcionando a devida sinalização, transmissão e recepção dos sinais entre terminais e dispositivos ativos de rede. Aliado ao SO (Sistema Operacional), este contém *buffers* (armazenadores) que retêm dados por certo período de tempo até serem levados para a memória RAM do computador ou HD (Hard Disk) e assim ser tratado, isto se faz devido à diferença de velocidade de processamento entre o computador (bytes) e placa (bits). A escolha do tipo de conector de uma placa de rede dependerá de qual arquitetura de rede local está disponível ao computador. Entre alguns conectores existentes no mercado, temos:

- RJ (Cabos par trançado)
- BNC (Cabos coaxiais)
- ST
- RJ/BNC
- RJ/BNC/AUI
- RJ/ST
- MIC

O custo destas placas é cada vez mais baixo devido aos padrões na qual elas são construídas serem abertos, dentre eles o padrão mais comum de placa de rede é o que suporta o IEEE 802.3 (Padrão Ethernet) cujo conector é o RJ-45. Esta tecnologia como

citada anteriormente permite velocidades de rede que varia de 10Mbps, 100Mbps e 1Gbps, sendo que a compatibilidade entre equipamentos com estas diferentes taxas de transmissão já pode ser realizada automaticamente pelas placas atuais que possuem adaptadores “autosense” cujos quais providenciam a negociação de taxa da transmissão com os dispositivos ativos previamente.

FIG. 9 – Placa de rede Ethernet
Disponível em: <http://www.mercadolivre.com.br>.

### 2.3.7. Placas de rede wireless

Além das placas de redes convencionais para Ethernet, as placas de rede Wi-Fi são interfaces de rede que podem ser instaladas em computadores e laptops a fim de realizar a comunicação na rede wireless. Geralmente possuem um custo superior as placas de rede comuns devido à necessidade de antenas e componentes eletrônicos diferenciados na placa, no entanto, são fáceis e práticas de configurar permitindo mobilidade aos dispositivos com elas instaladas.

FIG. 10 – Placa de rede Wireless
Disponível em: <http://www.mercadolivre.com.br>.

### 2.3.8. Estações de trabalho

Consiste em maquinas clientes, como: computadores, laptops, PDAs e etc. Focam-se na realização de tarefas locais e podem acessar os serviços disponibilizados na rede através de servidores.

FIG. 11 – Notebook, laptop e PDA

### 2.3.9. Cabos coaxiais

Um dos primeiros tipos de cabos a serem utilizados para rede, no entanto, já em desuso. É formado por um núcleo de cobre com uma camada superficial de resina, seguida de uma camada de PVC (plástico), uma malha metálica que funciona de blindagem eletrostática e por fim uma capa de plástico para proteção externa. O cabo coaxial mais empregado é o 10Base2 fino que utiliza conectores do tipo BNC.

FIG. 12 – Camadas de um cabo coaxial
Disponível em: Curso de Montagem de Redes de Computadores, Vladimir Bezerra de Oliveira.

### 2.3.10. Cabos par trançado (Twisted Pair)

Cabo de rede mais utilizado atualmente cuja característica principal consiste do entrelaçamento em pares dos oito fios nele presente. Isto é realizado propositalmente para cancelar os campos eletromagnéticos que são gerados quando os sinais trafegam nesses fios, permitindo uma ótima proteção contra ruídos. Através destes cabos é possível realizar comunicações tanto half-duplex (um sentido de cada vez) quanto full-duplex (ambos sentidos simultaneamente) e o comprimento máximo deles para tráfego sem perdas consideráveis de sinal é de 100 metros.

Existem dois tipos principais de par trançado:

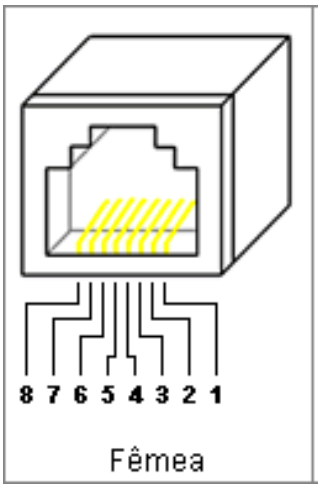
- **STP (Shielded Twisted Pair):** cabo com blindagem eletrostática geral (revestimento externo aos pares por fita metálica) e para cada par trançado. Extremamente recomendado para casos onde interferência eletromagnética é fator agravante na propagação do sinal.

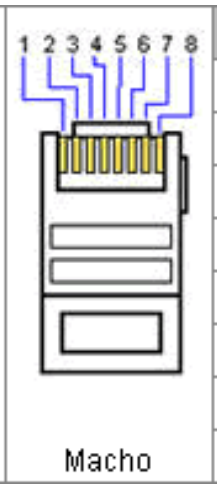
FIG. 13 – Cabo STP
Disponível em: Projetos de Cabeamento Estruturado –
Aulas 1 a 5, Departamento de Engenharia de Redes de Comunicação, UNB.

- **UTP (Unshielded Twisted Pair):** cabo sem blindagem eletrostática. É o mais popular entre os cabos par trançado e utiliza o conector RJ-45 em suas extremidades. Possui categorias que vão de 1 a 6, sendo o de categoria 6 o mais indicado atualmente para cabeamento em geral. Vale lembrar que quanto maior a categoria do cabo, maior é a capacidade de transmissão do cabo.

FIG. 14 – Cabo UTP
Disponível em: Projetos de Cabeamento Estruturado –
Aulas 1 a 5, Departamento de Engenharia de Redes de Comunicação, UNB.

**Sistema de cabeamento para Ethernet (10BASE-TX)**




| Pino | T-568A | T-568B |
|---|---|---|
| 1 | Branco / Verde | Branco / Laranja |
| 2 | Verde | Laranja |
| 3 | Branco / Laranja | Branco / Verde |
| 4 | Azul | Azul |
| 5 | Branco / Azul | Branco / Azul |
| 6 | Laranja | Verde |
| 7 | Branco / Marrom | Branco / Marrom |
| 8 | Marrom | Marrom |

FIG. 15 – Esquema de fiação para o padrão ethernet T-568A e T-568B
Disponível em: < http://www.catabits.com.br/artigos/conectividade>.

O primeiro esquema de fiação é derivado do padrão T-568A do TIA/EIA (Telecommunications Industry Association / Electronic Industries Alliance), que é o padrão preferido na ligação dos fios do cabo par trançado com conector RJ-45. Alternativamente a este padrão existe o T-568B, no entanto, é mais usual o T-568A.

Se houver a necessidade apenas de conectar dois computadores diretamente, existe uma forma barata e prática de interligá-los somente invertendo a pinagem de alguns fios do cabo par trançado, esta configuração é chamada de “cross-over”.

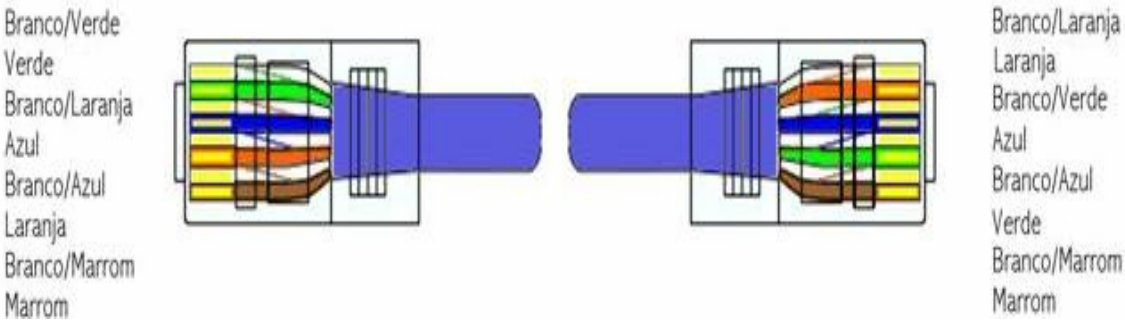



FIG. 16 – Esquema de fiação para cabo cross-over
Disponível em: <http://www.adrenaline.com.br/forum/showthread.php?t=77468>.

Ao lado esquerdo a pinagem padrão para ethernet (T-568A) e ao lado direito a pinagem que origina o cabo par trançado cross-over.

### 2.3.11. Fibra óptica

Este meio de comunicação tornou-se fundamental tanto para redes de telefonia tradicionais quanto para redes de dados devido ao seu alto desempenho e ao elevado volume de dados que esta suporta. Grandes taxas de transmissão podem ser alcançadas com presença de ruído insignificante em relação ao comprimento dos cabos que esta atinge (Km) sem a perda considerável de sinal que se propaga através de luz. Em aspecto construtivo, se

assemelha aos cabos coaxiais sendo que o núcleo e a casca são feitos de sílica dopada (uma espécie de vidro) ou até mesmo de plástico, sua espessura é de um fio de cabelo, no entanto, permitem pouca flexibilidade, i.e, não podem ser dobrados com a mesma intensidade que os cabos par trançado.O custo dos equipamentos, conectores e até da própria fibra são muito elevado e geralmente é empregada para conectar redes locais geograficamente separadas.

FIG. 17 – Fibra óptica
Disponível em: <http://www.blackbox.com.br>.

### 2.4. Cabeamento estruturado (CE)

O primeiro passo para instalação de uma rede local através de cabeamento é realizar o planejamento da infra-estrutura abordando alguns critérios importantes, como [14]:

- Avaliar infra-estrutura de edificação/arquitetura do lugar e espaços disponíveis para passagem de cabos;
- Analisar a capacidade atual e futura para serviços de voz, vídeo e dados, i.e, quantidades de pontos de rede que atenderá a demanda atual e a possibilidade de expansão desses para atender novos terminais;
- Dimensionar adequadamente a distribuição dos pontos levando em consideração as atividades desenvolvidas pelas pessoas no espaço disponível.
- Determinar o nível de integração e interdependência para os serviços de comunicação (voz, vídeo e dados);
- Definir parâmetros de qualidade a serem atingidos pela rede: disponibilidade, segurança, confiabilidade e desempenho;
- Construir políticas de acesso a infra-estrutura da rede;
- Avaliar custo e benefício das possíveis tecnologias a serem adotadas.

Todo esse planejamento é relevante na hora de promover a ampliação dos serviços de rede, reduzindo os custos que seriam necessários, por exemplo, de quebrar paredes para passagem de fiação, redução de custos para deslocamento de estações de trabalho, rápida manutenção, aumento da vida útil do cabeamento, entre outras vantagens implícitas.

Existem várias normas e padrões técnicos que definem como deve ser realizado o cabeamento estruturado, logo abaixo encontram-se uma lista delas (internacionais e nacionais):

| ***Normas*** | ***Especificações*** |
|---|---|
| ANSI/TIA/EIA-568-B.1 | Requerimentos gerais de CE |
| ANSI/TIA/EIA-568-B.2 | Componentes UTP de CE |
| ANSI/TIA/EIA-568-B.2-1 | Componentes UTP Categoria 6 |
| ANSI/TIA/EIA-568-B.3 | Componentes Ópticos de CE |

| | |
|---|---|
| ANSI/TIA/EIA-569A | Caminhos e Espaços de CE |
| ANSI/TIA/EIA-606A | Administração e Identificação de CE |
| ANSI/TIA/EIA-607 | Aterramento de CE |
| ANSI/TIA/EIA-854 | 1000BASE-TX sobre UTP Categoria 6 |
| ANSI/TIA/EIA-862 | Sistemas de automação sobre CE |
| Cobei/ABNT – NBR 14565 | Norma Brasileira equivalente a 568A |
| Cobei/ABNT – Projeto 03:046.05-14 | Norma Brasileira equivalente a 569A |

TAB. 1 – Normas internacionais e nacionais para cabeamento estruturado
Disponível em: Projetos de Cabeamento Estruturado –
Aulas 1 a 5, Departamento de Engenharia de Redes de Comunicação, UNB.

### 2.5. Endereçamento IP

Além de montar a estrutura física de uma rede local através de cabos e equipamentos, os hosts como são chamados os terminais que compõem a rede (computadores, impressoras, scanners, laptops) precisam de um identificador padrão e fixo no qual permite que os mesmos se localizem e troquem informações de forma rápida e correta. Por esta razão cada um deles recebe este identificador de seus fabricantes, que é mais comumente conhecido como endereço MAC.

Estes endereços MAC permitem que os dispositivos se comuniquem a nível físico, ou seja, o endereçamento IP que utiliza o protocolo IP (Internet Protocol) é encapsulado com esses endereços para navegarem na rede, sendo os endereços IP facilitadores na localização de um host na rede, uma vez que, os roteadores de pacotes trabalham basicamente na camada 3 (camada de rede do modelo OSI). Dois outros protocolos da camada 2 do modelo OSI auxiliam nessa localização: ARP (Address Resolution Protocol) e o RARP (Reverse-ARP). O primeiro é responsável por buscar e traduzir o endereço IP para o endereço MAC, enquanto que o segundo realiza exatamente o contrário, utiliza o endereço MAC para obter o endereço IP.

Para representação de um endereço TCP/IP são utilizados quatro bytes (32 bits), no qual cada byte representa um número decimal e é separado por um ponto, como exemplificado abaixo:

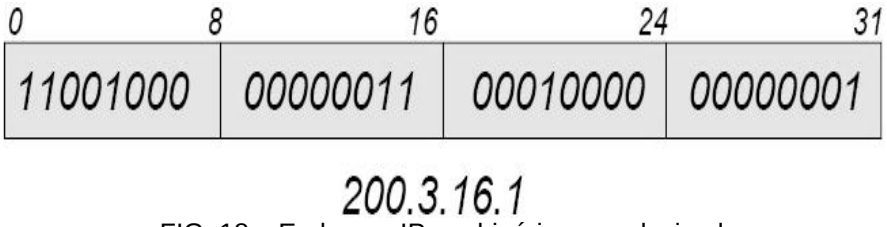



FIG. 18 – Endereço IP em binário e em decimal
Disponível em: TCP/IP e Internet, Prof. Ricardo Puttini, UNB.

#### 2.5.1. Classes de endereço IP

Junto ao surgimento do endereçamento IP durante a adoção do IPv4 (Protocolo IP versão 4), surgiram as classes de endereço IP cuja função é definir quantos octetos (bytes) serão utilizados para identificação de uma rede e quantos serão alocados para a identificação dos hosts.

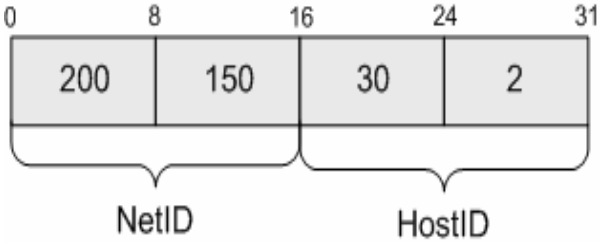



FIG. 19 – Partes do endereço IP

No caso acima temos, 2 octetos (16 bits ou 2 bytes) destinados ao endereçamento de rede (NetID) e 2 octetos destinados ao endereçamento de hosts (HostID), permitindo assim um n° de 65536 endereços de rede possíveis. O calculo é relativamente simples:

Sabendo o n° de bits pertencentes à parte do endereçamento desejado, por exemplo, os 16 bits mencionados acima referentes ao NetID, este entrará como expoente de uma potência de base 2 (conversão de binário para decimal) e assim obtêm-se o resultado que é de 65536. O cálculo do nº de endereços de hosts segue procedimento semelhante, no entanto, deve-se subtrair 2 endereços de hosts do valor total, pois estes possuem funcionalidades específicas para a rede.

Por padrão o primeiro deles (endereços IP de rede) é terminado com o último byte representando o n° decimal zero. Ex: Endereço IP de rede, 200.101.20.0.

O segundo host específico consiste no endereço IP de “broadcast”, isto é, endereço IP terminado em 255, no qual o todo pacote encaminhado para este endereço será redistribuído para todos os hosts pertencentes a mesma rede. Ex: Endereço IP de broadcast, 200.101.20.255.

As classes de endereço IP em si proporcionam um contra-balanço entre o n° de identificadores de rede e a quantidade de endereços de host possíveis, sendo que existem três classes principais de IP's (A, B e C) e duas classes restantes (D e E) que são utilizadas para implementações especificas.

Classe A: Primeiro bit mais significativo é 0.
Classe B: Primeiros dois bits mais significativos são 10.
Classe C: Primeiros três bits mais significativos são 110.
Classe D: (endereço multicast): Primeiros quatro bits mais significativos são: 1110.
Classe E: (endereço especial reservado): Primeiros quatro bits são mais significativos 1111.

Obs.: Os bits mais significativos de um byte consistem dos localizados mais a esquerda do byte, ou seja, os primeiros da esquerda para direita.

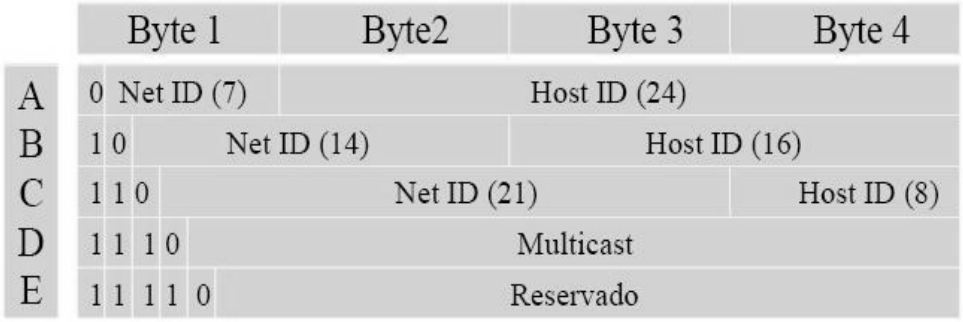



FIG. 20 – Classes de endereços IP
Disponível em: TCP/IP e Internet, Prof. Ricardo Puttini, UNB.

A tabela seguinte contém o intervalo de IP das classes de endereços.

| ***Classe*** | ***Intervalo de Endereços*** | ***N.º Endereços por Rede*** |
|---|---|---|
| **A** | 1.0.0.0 até 126.0.0.0 | 16777216 |
| **B** | 128.0.0.0 até 191.255.0.0 | 65536 |
| **C** | 192.0.0.0 até 223.255.255.254 | 256 |
| **D** | 224.0.0.0 até 239.255.255.255 | multicast |
| **E** | 240.0.0.0 até 255.255.255.255 | reservado |

TAB. 2 – Intervalo de IPs e quantidade de endereços de rede por classe
Disponível em: < http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>.

### 2.5.2. Classes especiais

Além das classes de endereço IP usuais também existem as classes de IP que são

consideradas especiais pelo fato de não serem públicas, isto é, essas classes aglomeram faixas de IP que não são roteáveis ou endereçáveis pelas redes públicas, são reservados para uma comunicação através de uma rede privada ou no próprio computador local (localhost).

| ***Bloco de Endereços*** | ***Descrição*** | ***Referência*** |
|---|---|---|
| **0.0.0.0/8** | Rede corrente (só funciona como endereço de origem) | RFC 1700 |
| **10.0.0.0/8** | Rede Privada | RFC 1918 |
| **14.0.0.0/8** | Rede Pública | RFC 1700 |
| **39.0.0.0/8** | Reservado | RFC 1797 |
| **127.0.0.0/8** | Localhost | RFC 3330 |
| **128.0.0.0/16** | Reservado (IANA) | RFC 3330 |
| **169.254.0.0/16** | Zeroconf | RFC 3927 |
| **172.16.0.0/12** | Rede Privada | RFC 1918 |
| **191.255.0.0/16** | Reservado (IANA) | RFC 3330 |
| **192.0.0.0/2** | | |
| **192.0.2.0/24** | Documentação | RFC 3330 |
| **192.88.99.0/24** | IPv6 para IPv4 | RFC 3068 |
| **192.168.0.0/16** | Rede Privada | RFC 1918 |
| **198.18.0.0/15** | Teste de benchmark de redes | RFC 2544 |
| **223.255.255.0/24** | Reservado | RFC 3330 |
| **224.0.0.0/4** | Multicasts (antiga rede Classe D) | RFC 3171 |
| **240.0.0.0/4** | Reservado (antiga rede Classe E) | RFC 1700 |
| **255.255.255.255** | Broadcast | |

TAB. 3 – Endereços disponíveis nas classes especiais de IP
Disponível em:< http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>.

### 2.5.3. Máscara de Rede

Conhecida também como *subnet mask* ou *netmask*, consiste de um número de 32 bits cuja função é separar através de um endereço IP, a parte referente ao endereço de rede (NetID) ou endereço de sub-rede (SubnetID) e hosts (HostID).

Essas máscaras de bits indicam onde começa e termina a numeração para identificação dos hosts, assim como informa o endereço de rede. São formadas de binários 1 e 0, onde os binários iguais a 1 revelarão a parte referente ao endereço de rede, enquanto os binários iguais 0 revelarão a parte que pertencem aos hosts.

Da mesma forma como o endereçamento IP, as máscaras de sub-rede são representadas por quatro blocos de números decimais que variam de 0 a 255, contudo para melhor entendimento de como funcionam as máscaras neste dossiê, a notação em binário foi adotada, uma vez que para determinar-se a porção do endereço de rede é necessário realizar a operação lógica AND com o endereço IP, ou seja,

Exemplo:

| | ***Endereço decimal*** | ***Binário*** |
|---|---|---|
| Endereço completo (host) | 192.168.5.10 | 11000000.10101000.00000101.00001010 |
| Máscara da sub-rede | 255.255.255.0 | 11111111.11111111.11111111.00000000 |
| Porção da rede | 192.168.5.0 | 11000000.10101000.00000101.00000000 |

TAB. 4 – Obtendo a porção de rede (NetID)
Disponível em: <http://pt.wikipedia.org/wkii/M%C3%A1scara_de_rede>.

Além da notação convencional em decimais ou em binário paras as máscaras, estas

podem ser representadas pela notação CIDR (Classless Inter-Domain Routing). Esta notação consiste em informar quantos bits 1 estão presentes nos 32 bits da máscara, retirando a necessidade de escrever todos os números decimais ou binários referentes a ela. Ex: (host) 192.168.67.72 / 24 (máscara), anteriormente era escrito por (host) 192.168.67.72 / 255.255.255.0 (máscara).

Para as três classes principais IPv4 ( A, B e C ), as máscara de rede mais comuns são:

| ***Classe*** | ***Bits iniciais*** | ***Início*** | ***Fim*** | ***Máscara de sub-rede padrão*** | ***Notação CIDR*** |
|---|---|---|---|---|---|
| **A** | 0 | 0.0.0.1 | 126.255.255.255 | 255.0.0.0 | /8 |
| **B** | 10 | 128.0.0.0 | 191.255.255.255 | 255.255.0.0 | /16 |
| **C** | 110 | 192.0.0.1 | 223.255.255.254 | 255.255.255.0 | /24 |

TAB. 5 – Máscaras de sub-rede
Disponível em: <http://pt.wikipedia.org/wkii/M%C3%A1scara_de_rede>.

### 2.5.4. Sub-redes

É a subdivisão de redes grandes em redes menores proporcionando assim a redução do tráfego, uma administração simplificada e melhor desempenho da rede como um todo. Estas subdivisões são realizadas pelas máscaras de sub-redes cujas quais se apoderam de alguns bits destinados a identificação dos hosts para criar novas sub-redes.

Exemplo:

| | ***Endereço Decimal*** | ***Binário*** |
|---|---|---|
| Endereço host | 192.168.5.130 | 1000000.10101000.00000101.**10**000010 |
| Máscara de sub-rede | 255.255.255.192 | 1111111.11111111.11111111.**11**000000 |
| Porção da sub-rede | 192.168.5.128 | 1000000.10101000.00000101.**10**000000 |

TAB. 6 – Obtendo a porção de sub-rede (SubnetID)
Disponível em: <http://pt.wikipedia.org/wkii/M%C3%A1scara_de_rede>.

No caso acima os dois bits mais significativos da porção destinada aos hosts (parte em negrito) foram cedidos para a identificação da sub-rede.

### 2.6. Serviços essenciais para uma rede local

Explicação de alguns serviços que oferecem dinamicidade e segurança a rede.

### 2.6.1 DNS (Domain Name System)

Sistema hierárquico e distribuído de gerenciamento de nomes (RFCs 1034 e 1035) que possui as seguintes funcionalidades:

- Resolver nomes de servidores em endereços IP de rede;
- Examinar e atualizar seu banco de dados.

Como o sistema é distribuído, isto permite que os bancos de dados DNS possam ter tamanho ilimitado e um desempenho que não decai facilmente com a adição de novos servidores ao banco. Este mecanismo é bastante útil, uma vez que, é mais fácil decorar nomes para identificar uma maquina na rede, ao invés de um endereço IP.

O servidor DNS traduz tanto nomes para os endereços IP quanto endereços IP para os respectivos nomes, permitindo a localização de hosts em um domínio determinado. Esse serviço geralmente se encontra localizado no servidor DNS primário.

O servidor DNS secundário ou alternativo é uma espécie de cópia de segurança do servidor DNS primário. Quando não é possível encontrar um domínio através do servidor primário o sistema tenta resolver o nome através do servidor secundário.

### 2.6.2 DHCP (Dynamic Host Configuration Protocol)

Com o aumento do número de terminais conectados a uma rede local, a configuração manual de cada um deles com endereços IP, máscaras de sub-rede, gateway padrão e DNS se torna um exercício muito desgastante e demorado. Para isso surgiu em 1993 de forma oficial o protocolo DHCP (sendo a RFC 2131 mais atual), que permiti aos dispositivos pedir e obter dinamicamente parâmetros de configuração da interface de rede junto ao servidor DHCP que contêm uma lista de endereços disponíveis para atribuição (faixa de IPs disponíveis). Vale lembrar que além de endereços IP, este mecanismo também pode fornecer outros parâmetros de configuração, como os citados no inicio do parágrafo.

O protocolo DHCP usa um modelo cliente-servidor de tal forma que o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede e o clientes é responsável por novas requisições.

### 2.6.3 NAT (Network Address Translation)

Técnica também conhecida como “masquerading”, esta reescreve os endereços IP de origem de um pacote que passam sobre um roteador ou firewall de maneira que um computador de uma rede interna (rede privada) tenha acesso à rede externa (rede pública). Esta técnica foi elaborada para amenizar a futura escassez de endereços IP válidos da rede pública, alem de permitir a construção de topologias de rede mais seguras, pois todo o tráfego de entrada e saída de uma rede privada pode passar através de um único endereço IP válido, isto favorece a implantação de sistemas de segurança.

### 2.6.4 Firewall

Consiste no elemento de rede que possui a função de regular o tráfego entre redes distintas (rede local e MAN, por exemplo), negando a transmissão e recepção de dados nocivos, autorizando ou barrando tráfegos específicos, em resumo, este é o guardião da rede. Os firewalls podem ser implementados através de hardware ou software e o nível de complexidade na configuração vai depender do tamanho da rede envolvida e o volume de regras para controle do tráfego de entrada e saída.

Os sistemas de firewall podem ser classificados em:

- **Filtro de Pacotes:** Estes sistemas de firewall analisam individualmente os pacotes à medida que estes são transmitidos da camada de enlace (camada 2 do modelo OSI) para a camada de rede (camada 3 do modelo OSI). As regras podem ser formadas estabelecendo os endereços de rede (origem e destino) e as portas (TCP/IP envolvidas na conexão. As principais desvantagens deste tipo de tecnologia é a falta de controle de estado do pacote, o que permite que agentes maliciosos possam produzir pacotes simulados.

- **Proxy Firewall:** Os conhecidos "bastion hosts" foram introduzidos por Marcus Ranum em 1995. Trabalhando como uma espécie de eclusa, os firewalls de proxy trabalham recebendo o fluxo de conexão e originando um novo pedido sob a responsabilidade do firewall (non-transparent proxy). A resposta para o pedido é analisada antes de ser entregue para o solicitante original.

- **Stateful Firewall:** esse firewall inspeciona o tráfego para evitar pacotes ilegítimos, guardando o estado de todas as últimas transações efetuadas.

- **Firewall de Aplicação:** Com a explosão do comércio eletrônico percebeu-se que mesmo a última tecnologia em filtragem de pacotes TCP/IP poderia não ser tão

efetiva quanto se esperava. Com todos os investimentos despendidos em tecnologia de stateful firewalls, as estatísticas demonstravam que os ataques continuavam a prosperar de forma agressiva. Percebeu-se que havia a necessidade de desenvolver uma tecnologia que pudesse analisar as particularidades de cada protocolo e tomar decisões que pudessem evitar ataques maliciosos. A idéia então é analisar o protocolo específico da aplicação e tomar decisões dentro das particularidades da aplicação, criando uma complexidade infinitamente maior do que configurar regras de fluxo de tráfego TCP/IP.

## 3. Passos para implementação de uma rede local com compartilhamento de recursos

Exemplo básico de topologia LAN com serviços, segurança e compartilhamento de internet.

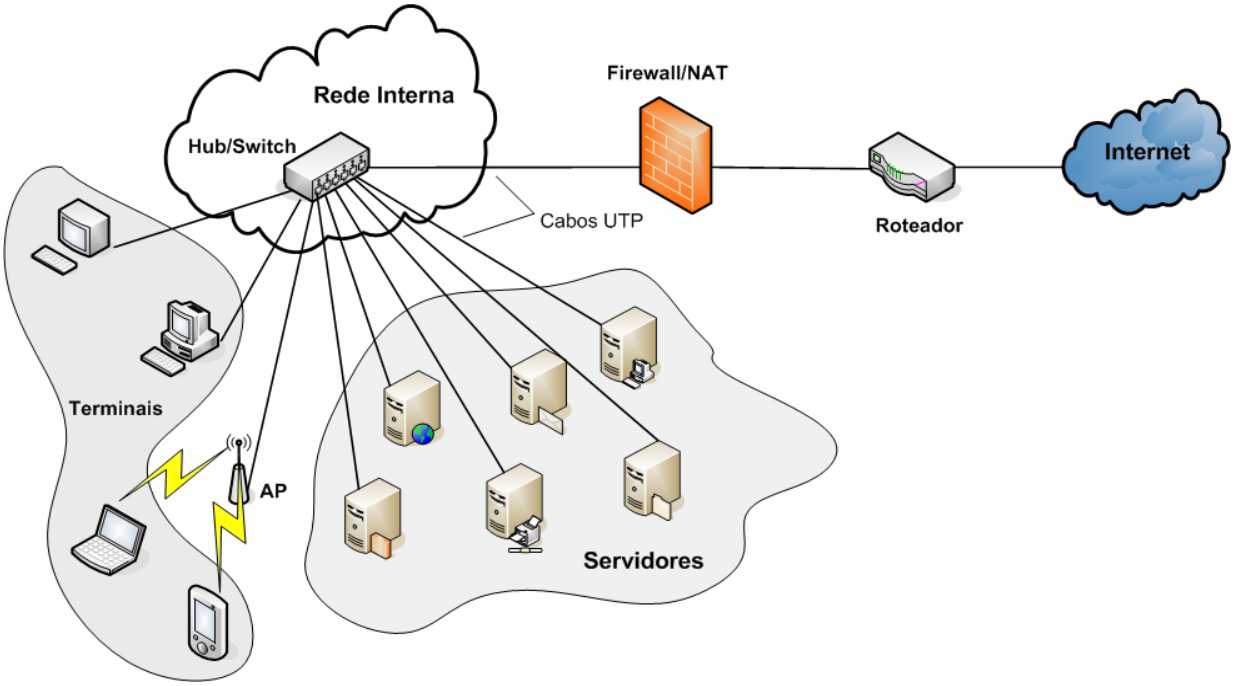



FIG. 21 – Topologia da rede local

A figura acima mostra a infra-estrutura básica de uma LAN que proporciona além de acesso a internet, recursos de rede como: compartilhamento de arquivos, impressoras e serviços de rede (Web, Mail, Proxy, DNS/DHCP, Impressão e etc).

### 3.1. Conexão com a internet

Os meios mais comuns de conexão com a rede mundial oferecida pelos provedores de Internet são:

| ***Tecnologia*** | ***Velocidade de conexão*** |
|---|---|
| ADSL | a partir de 128 Kbps |
| CABO | a partir de 128 Kbps |
| FIBRA ÓPTICA | Muito superiores a 1Mbps |

TAB. 7 – Relação Tecnologia x Velocidade de conexão

A escolha da velocidade de conexão e tecnologia vai depender do volume de tráfego que a empresa demanda. Em geral se faz necessário para as tecnologias a cabo ou ADSL, a compra ou aluguel de um modem com entrada para rede pública (WAN ou MAN) e saída Ethernet devido as diferentes características de transmissão e recepção entre eles, o mesmo ocorre para a fibra óptica que necessita de um conversor de Fibra para Ethernet,

ou vice e versa. A presença de um roteador antes do firewall como mostra a FIG. 21 é opcional se o provedor de Internet já disponibiliza um endereço IP válido (endereço roteável). Isto já é suficiente para que os pacotes oriundos da rede interna possam ser encaminhados para a rede externo (WAN), uma vez configurado adequadamente o NAT.

Existem no mercado, diversos modens/roteadores ADSL ou a cabo que aglomera várias funcionalidades ao mesmo tempo, como: interface para WAN e Ethernet, Firewall, NAT, servidor DHCP, entre outros. Este tipo de solução é bastante utilizada em residências, escritórios e pequenas empresas que demandam poucos terminais de rede e volume reduzido de tráfego.

### 3.2. Infra-Estrutura da rede interna

#### 3.2.1. Firewall / NAT

Será o ponto efetivo de interface entre a rede externa e a rede interna, junto ao firewall temos a função NAT para conversão de endereços. Geralmente a máquina destinada para exercer tais funções precisa ter: processador razoavelmente potente e memória RAM com capacidade média para realizar as conversões de endereços da função NAT e aplicar as regras do Firewall simultaneamente, além disso, duas placas de rede são necessárias: uma destinada para receber a conexão vinda da rede externa com IP válido e a outra placa voltada para as conexões internas à rede. É aconselhável configurar a interface interna manualmente com os parâmetros da rede interna (endereço IP, máscara, gateway padrão e DNS interno), isto evita que os terminais internos percam conectividade com a rede externa devido a divergência do parâmetro “gateway padrão” entre as máquinas internas e o Firewall/NAT, pois todo o tráfego para internet originada de dentro da rede interna passará pela interface interna do Firewall/NAT.

#### 3.2.2. HUB ou Switch

Será o responsável por distribuir todo o tráfego interno e o acesso a Internet para os terminais da rede privada. O acesso externo é garantido para todos conectando-se um cabo Ethernet que deve sair da interface interna do Firewall/NAT a uma das portas do HUB ou Switch.

#### 3.2.3. Servidor DNS / DHCP

Mesmo se tratando de dois serviços distintos, estes podem ser colocados na mesma máquina, pois a capacidade de processamento exigida por cada um é relativamente baixa. Na topologia acima, o servidor DNS pode ser utilizado para identificar servidores e terminais internos através de nomes, ao invés de IPs. Ao mesmo tempo em que o servidor DHCP deve ser configurado com a faixa de IPs Privados (Ex: 192.168.10.2 a 192.168.10.200) junto com os parâmetros adicionais (máscara, gateway padrão e DNS interno). Isto permitirá que os terminais internos que possuem o cliente DHCP ativado, carreguem as configurações de rede automaticamente. Em caso de falha do cliente, a placa de rede pode ser configurada manualmente da seguinte forma:

Entre no menu Iniciar do Windows, Painel de Controle, em seguida Conexões de Rede.

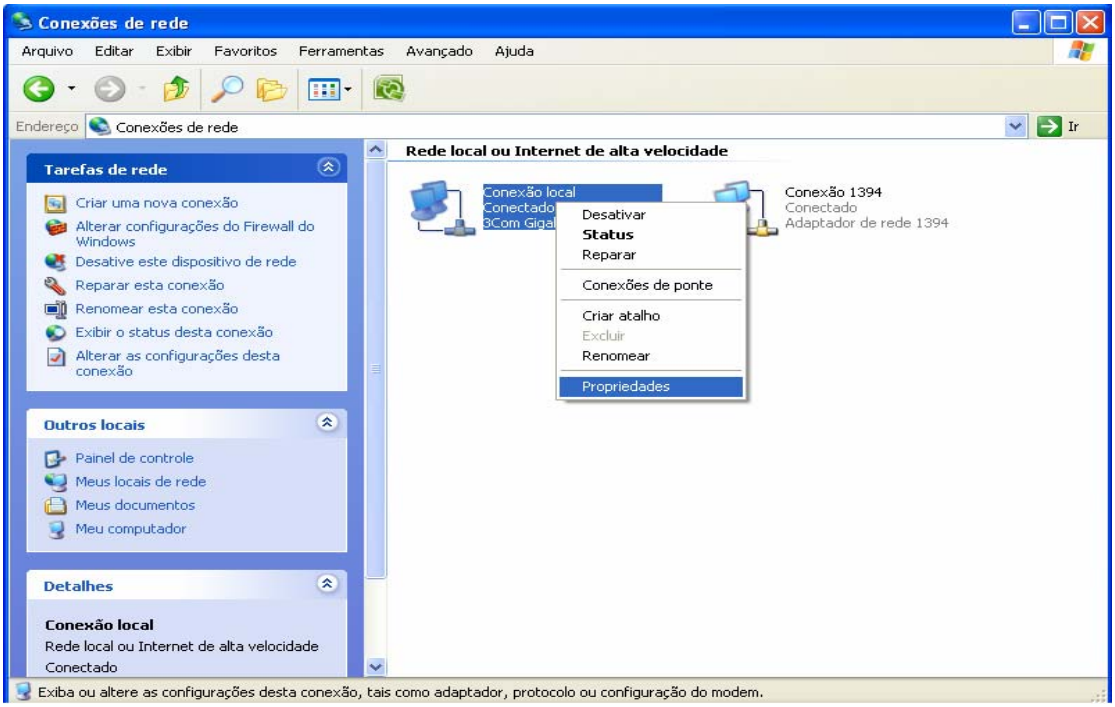



FIG. 22 – Tela de Conexões de Rede

Clique sobre o ícone Conexão Local com o botão direito do mouse, em seguida selecione a opção Propriedades (Ver FIG. 22). Na guia Geral da tela aberta, marque a opção Protocolo TCP/IP e em seguida Propriedades.

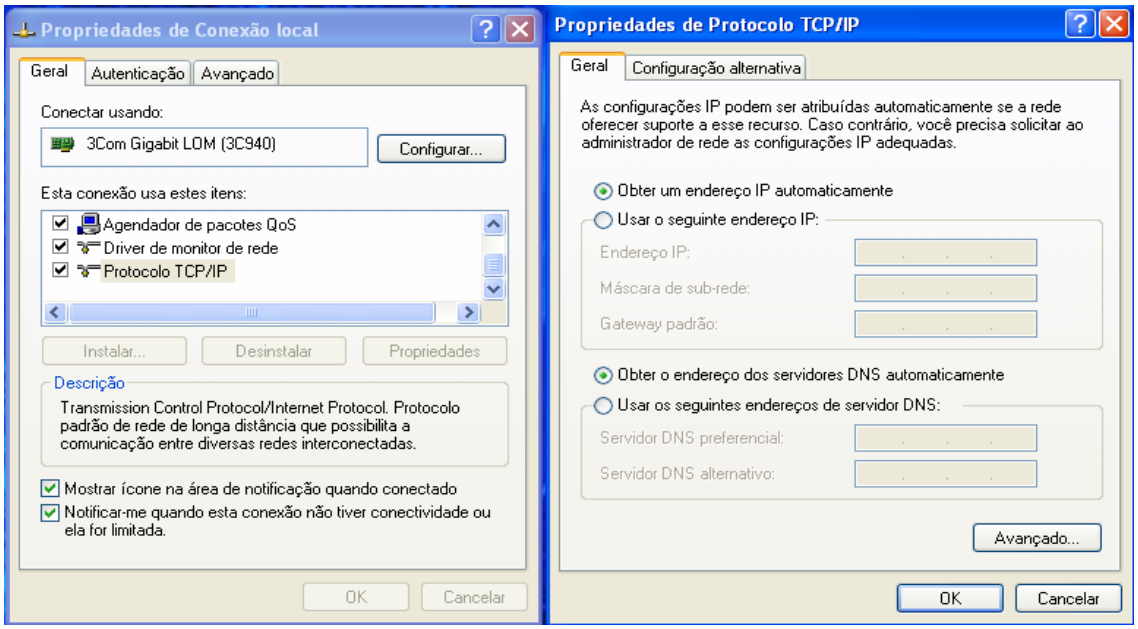



FIG. 23 – Telas de Propriedades: Conexão Local e Protocolo TCP/IP

Na janela Propriedades do Protocolo TCP/IP (Ver FIG. 23), já estão pré-selecionados as opções que ativam o cliente DHCP “Obter em endereço IP automaticamente e Obter endereço dos servidores DNS automaticamente”, para configurar manualmente a placa de rede basta selecionar as opções “Usar o seguinte endereço IP e Usar os seguintes endereços de servidor DNS” que abrirão os campos referentes ao Endereço IP, Máscara de sub-rede, Gateway padrão, Servidor DNS primário e Servidor DNS alternativo, ao fim do preenchimento, basta confirmar com OK as janelas e esperar que o dispositivo se conecte na rede.

### 3.2.4. Access Point (AP)

Permite a conexão sem fio dos dispositivos que suporta a tecnologia. Isto viabiliza uma futura expansão de acesso à rede interna em caso de escassez de pontos de rede, além de permitir mobilidade e acesso rápido para os equipamentos já existentes.

Os terminais automaticamente receberão as configurações de rede se o Access Point estiver corretamente configurado, i.e, recebendo os parâmetros do servidor DHCP da rede, pois vale lembrar que alguns APs possuem a função de servidor DHCP e se ativado pode causar conflito de IP nas máquinas, ou seja, dois terminais com o mesmo endereço IP na rede interna, por isto é recomendável apenas um servidor DHCP na rede. Outra característica importante a ser configurada nos APs é a restrição de acesso a rede wireless através do uso de chave para cifragem do tráfego interno.

### 3.2.5. Servidores de rede

A utilização dos servidores listados a seguir é opcional, no entanto, oferecem recursos adicionais a rede e considerável melhoria dos processos eletrônicos da empresa.

**Controlador de Domínio:** Para montar uma rede com controle centralizado de acesso dos usuários a computadores conectados em rede é necessário instalar este serviço. A ferramenta vem por padrão nos Windows NT e 2003 Server, permitindo definir grupos e permissões de usuários para manipular pastas, arquivos, instalar aplicativos nos computadores em que estão autenticados e etc. Isto é importante para definir políticas de utilização dos computadores, acesso remoto a determinadas pastas ou arquivos compartilhados na rede entre outras características.

**Arquivos:** Aliado ao controlador de domínio, este permite fornecer um espaço centralizado de arquivos digitais da empresa através da rede, além de definir cotas de espaço por grupo ou usuários, permissões de segurança para os arquivos, proteção dos dados contra falhas mecânicas ou erros de gravação nos HD (hard disks) através de técnicas de espelhamento, permitindo alta disponibilidade do serviço, ou seja, o funcionamento ininterrupto. Outra característica destes servidores são as ferramentas de backup em outras mídias (fita magnética e etc).

**Impressão:** fornece e gerencia o acesso aos drivers e impressoras conectadas na rede.

**Web e Banco de Dados:** Podem ser utilizados para mostrar o Web site da empresa na Internet ou uma Intranet para os funcionários divulgarem assuntos internos, instalar ferramentas on-line para administração, gerência e etc.

**Proxy – Cache:** Consiste em uma alternativa para acelerar a navegação dos funcionários na Internet e controlar de conteúdo Web. Este servidor destina-se a realizar o “cache” (armazenamento temporário) de paginas Web e arquivos, sendo que, ao funcionário entrar em uma mesma pagina Web ou realizar um download de arquivo pela segunda vez, este fará diretamente do Proxy, ao invés de consumir largura de banda disponível para Internet em outros fins. O controle de conteúdo Web também é possível e permite autorizar ou bloquear domínios específicos, de acordo com a política de acesso da empresa.

## 3.3. Compartilhamento simples de arquivos ou pastas

Para realizar o compartilhamento simples de arquivos ou pastas, sem a necessidade de um servidor para tal função, primeiramente se necessita verificar quais computadores da rede interna conseguem “enxergar” uns aos outros, ou seja, se um computador consegue visualizar o outro através do sistema de diretórios do sistema operacional (neste caso, o Windows XP). Para isto seguem-se os seguintes procedimentos:

Entre no menu Iniciar do Windows, Meus locais de Rede, em seguida no menu lateral “Outros Locais” existe a opção “Toda a Rede”, selecione esta opção e então aparecerá um ícone chamado de “Rede Microsoft Windows”, clique-o para automaticamente aparecer o domínio ou grupo(s) de trabalho em que os computadores da rede interna estão inseridos.

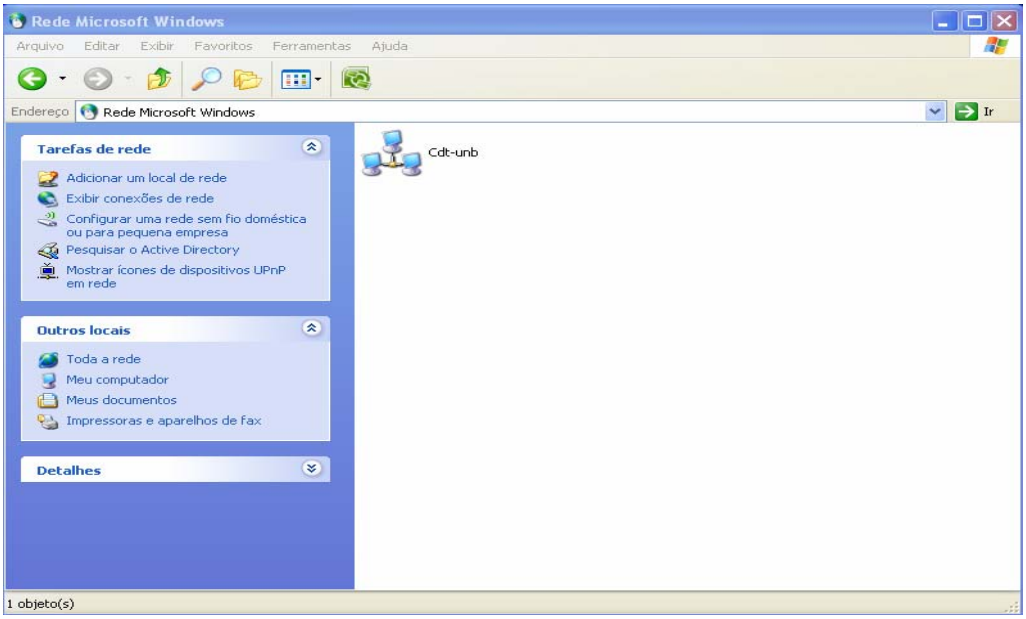



FIG. 24 – Tela de Meus Locais de rede, domínio ou grupo de trabalho encontrado.

Ao clicar-se sobre o ícone referente ao domínio ou grupo de trabalho, aparecerá uma lista de nomes de computadores em cada um deles, basta agora verificar se o computador que se deseja compartilhar arquivos está presente.

O nome do computador e domínio/grupo de trabalho no qual ele faz parte pode ser configurado em Painel de Controle, Sistema, Aba ”Nome do Computador”.

Uma vez os computadores estando visíveis no domínio/grupo de trabalho para compartilhar uma pasta ou arquivo, basta selecionar a pasta ou arquivo a ser compartilhado com o botão direito do mouse, clicar em Propriedades, em seguida abrirá uma janela com uma Aba “Compartilhamento”.

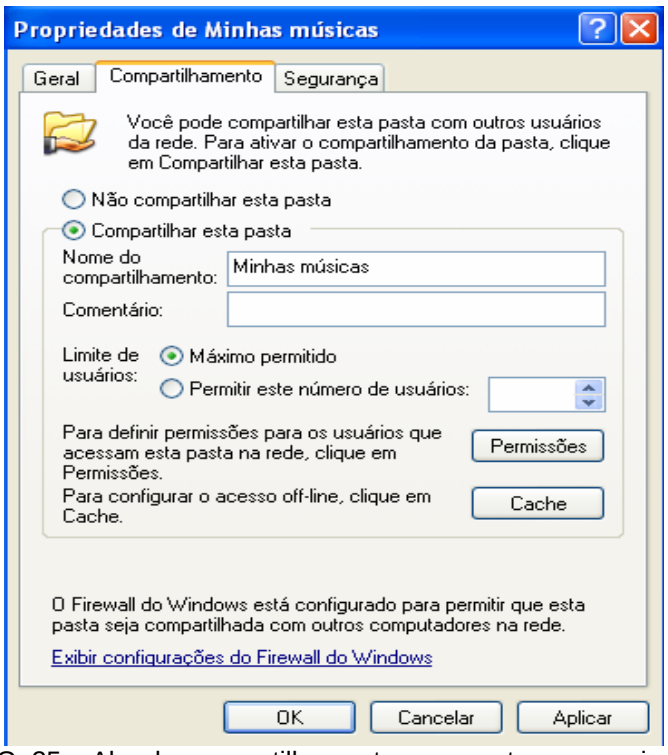



FIG. 25 – Aba de compartilhamento para pastas ou arquivos.

Nesta Aba o usuário define a quantidade de usuários que podem compartilhar a pasta/arquivo, as permissões de manipulação dos arquivos para usuários específicos, entre outras características. Ao fim, basta confirmar todas as alterações e acessar a pasta/arquivo de outro computador, para isto entre em Meus locais de Rede, menu lateral “Outros Locais” , “Toda a Rede”, “Rede Microsoft Windows”, domínio ou grupo de Trabalho visível, nome

do computador que está compartilhando a pasta/arquivo. Nessa ação aparecerá a pasta ou arquivo compartilhado no respectivo computador.

Outra forma de acesso mais rápido é através do menu Iniciar do Windows, “Executar”. Abrirá uma tela pequena de procura, nela coloca-se \\ Endereço IP ou nome da máquina que está compartilhando. Ao final aparecerá a(s) pasta(s)/arquivo(s) compartilhadas desse computador.

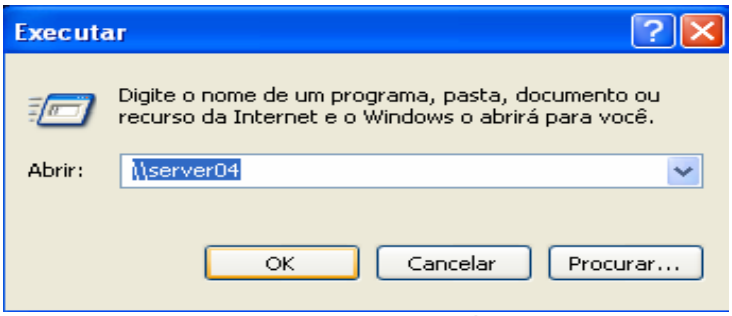



FIG. 26 – Acessando pasta ou arquivo através da ferramenta Executar.

### 3.4. Compartilhamento de impressoras

Geralmente dentro de uma empresa, as impressoras encontram-se diretamente conectadas a algumas estações de trabalho estratégicas, que por sua vez estão conectadas a rede, isto a faz uma espécie de servidor semi-dedicado a impressão. Para compartilhar estas impressoras na rede, primeiramente entre em menu Iniciar do Windows do computador no qual o dispositivo de impressão está instalado, “Impressoras e Aparelhos de Fax”, abrirá então uma tela contendo o ícone da impressora instalada, a seguir clica-se com o botão direito do mouse aparecendo a opção de compartilhamento e a partir daí o procedimento de configuração é similar ao feito para pasta(s)/arquivo(s), não esquecendo de marcar a opção “Listar em Diretório” para visualizar o compartilhamento através dos “Meus Locais de Rede” e facilitar a instalação desta em outros computadores.

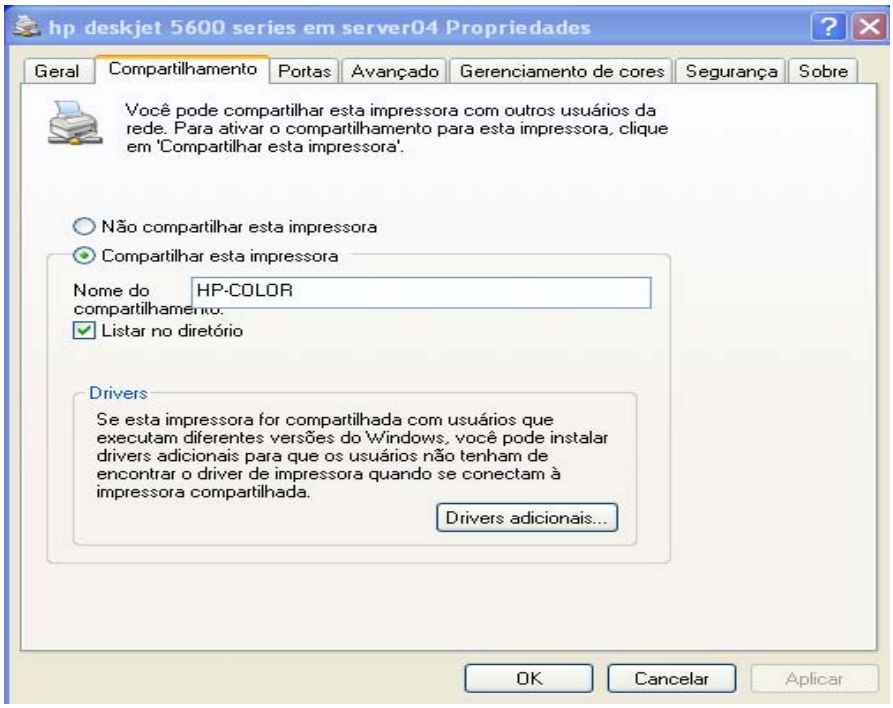



FIG. 27 – Compartilhando impressora na rede

A instalação de uma impressora compartilhada na rede em outros computadores é feita acessando o menu Iniciar do Windows, “Impressoras e Aparelhos de Fax”, menu lateral “Tarefas de Impressora ” , opção “Adicionar uma Impressora”. Após esta ação abrirá um tela do “Assistente para adicionar Impressora”, clique em Avançar e em seguida marque a opção “Uma impressora de rede ou conectada a outro computador”, avance e aparecerá uma nova tela mostrando três formas diferentes de acessar a impressora na rede.

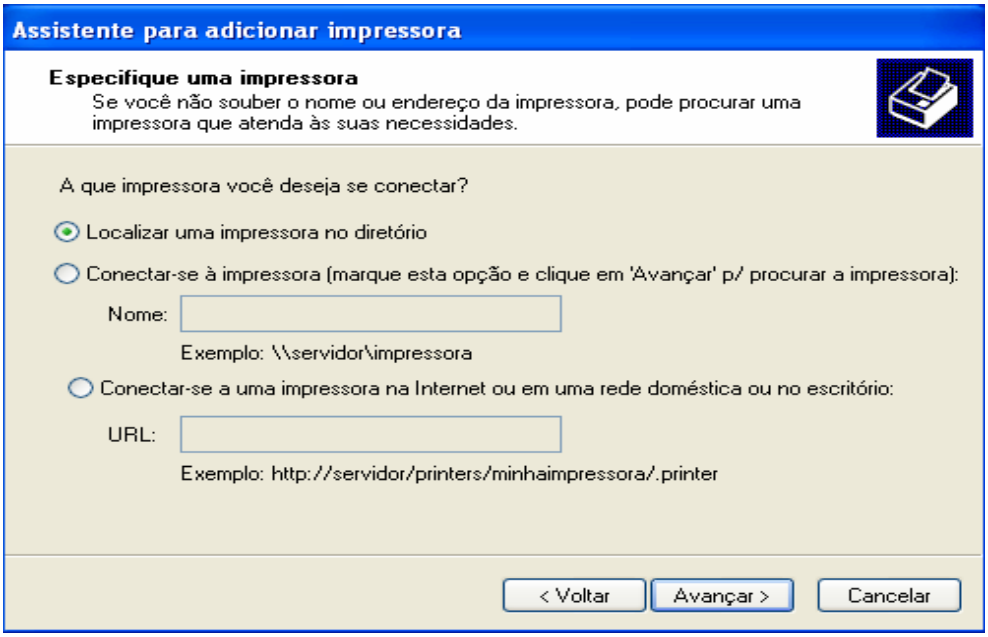


FIG. 28 – Configurando computadores com a impressora de rede.

Deixe a opção que está marcada e clique em avançar, na tela a seguir clique em “Localizar agora” para visualizar as impressoras que estão instaladas e compartilhadas na rede, escolha uma delas, confirme com OK e pronto já está configurada a impressora de rede na máquina. Para torná-la impressora padrão basta entrar no menu Iniciar do Windows, “Impressoras e Aparelhos de Fax” , verificar o ícone da impressora de rede, clicar com o botão direito do mouse e assinalar a opção “Definir como impressora padrão”, isto permitirá que todos os documentos que forem impressos seja feito por esta impressora.

## Conclusões e recomendações

As redes de comunicação, em particular as redes locais, foram o princípio de uma grande revolução no que se trata de disseminação de informação e dinamicidade aos processos produtivos (intelectual-científico, institucional, governamental e etc) tanto nas grandes corporações empresariais com nas médias, pequenas e micro empresas.

A tendência mundial é que este tipo de infra-estrutura se expanda pelos mais diversos ramos do empreendedorismo em geral, pois a rapidez da geração e troca de informações, redução de custos em relação aos processos produtivos tradicionais, confere a utilização de uma rede local, um grau de relevância para prosperidade de um negócio.

## Referências

WIKIPÉDIA. **Rede de longa distância**. Disponível em: <http://pt.wikipedia.org/wiki/Rede_de_longa_dist%C3%A2ncia>. Acesso em: 01 out. 2007.

WIKIPÉDIA. **Modelo OSI**. Disponível em: <http://pt.wikipedia.org/wiki/Modelo_OSI>. Acesso em: 01 out. 2007.

PUTTINI, RICARDO S. “Arquitetura de Redes de Comunicação” Departamento de Engenharia Elétrica - UNB, Junho / 2001.

WIKIPÉDIA, **TCP/IP**. Disponível em: <http://pt.wikipedia.org/wiki/TCP/IP>. Acesso em: 01 out. 2007.

SOARES, LUIZ F. G.; LEMOS, GUIDO; COLCHER, SÉRGIO “Redes de Computadores, Das LANs, MANs e WANs às Redes ATM” 2ª edição ed. Campus, 1995 pp 210 – 221.

WIKIPÉDIA. **Fast Ethernet**. Disponível em: <http://pt.wikipedia.org/wiki/Fast_Ethernet>. Acesso em: 02 out. 2007.

WIKIPÉDIA, **IEEE 802.11**. Disponível em: <http://pt.wikipedia.org/wiki/IEEE_802.11>. Acesso em: 03 out. 2007.

DN CONECTIVIDADE. **Rede Local (LAN)**. Disponível em: <http://www.dnconectividade.com.br/lan.html>. Acesso em: 02 out. 2007.

PROJETO DE REDES. **Equipamento para Redes – 2ª Parte**. Disponível em: <http://www.projetoderedes.com.br/tutoriais/tutorial_equipamentos_de_redes_02.php>. Acesso em: 03 out. 2007.

SAMPAIO, LUIZ P. M. "Projetos de cabeamento Estruturado – Aulas 1 a 5" Departamento de Engenharia de Redes de Comunicação – UNB, Março / 2005.

OLIVEIRA, VLADIMIR B. "Curso de Montagem de Redes de Computadores", Abril / 2006.

WIKIPÉDIA. **Endereço IP**. Disponível em: <http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>. Acesso em: 03 out. 2007.

PUTTINI, RICARDO S. "TCP/IP e Internet" Departamento de Engenharia Elétrica – UNB, 2001.

WIKIPÉDIA. **Máscara de Rede**. Disponível em: <http://pt.wikipedia.org/wkii/M%C3%A1scara_de_rede>. Acesso em: 03 out. 2007.

WIKIPÉDIA. **Domain Name System**. Disponível em: <http://pt.wikipedia.org/wiki/Domain_Name_System>. Acesso em: 04 out. 2007.

WIKIPÉDIA. **DHCP**. Disponível em: <http://pt.wikipedia.org/wiki/DHCP>. Acesso em: 04 out. 2007.

ADRENALINE. **Redes de Computadores**. Disponível em: <http://www.adrenaline.com.br/forum/showthread.php?t=77468>. Acesso: 05 out. 2007.

**Nome do técnico responsável**

Arley Pinheiro Mendes

**Nome da Instituição do SBRT responsável**

Centro de Apoio ao Desenvolvimento Tecnológico – CDT/UnB

**Data de finalização**

09 out. 2007