**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**
**ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE**

ANDRESON FERNANDO DOS SANTOS

# ESTUDO E IMPLEMENTAÇÃO DE SERVIÇOS DE ACESSO REMOTO

MONOGRAFIA

CURITIBA
2013

ANDRESON FERNANDO DOS SANTOS

# ESTUDO E IMPLEMENTAÇÃO DE SERVIÇOS DE ACESSO REMOTO

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR.
Orientador: Prof. Dr. Augusto Foronda.

CURITIBA
2013

## RESUMO

Santos, Andreson F.. **Estudo e Implementação de Acesso Remoto.** 2013. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

A presente monografia aborda o estudo para a implementação de técnicas de acesso remoto. Apresenta as vantagens para utilização de acesso remoto externo. O projeto inicializa-se utilizando método bibliográfico, seguido de estudo em campo, configuração de equipamentos *Modem Roteador* e análise dos resultados obtidos. O resultado mostrará a eficácia de uma rede com Acesso Remoto aplicado e funcionando de acordo com a necessidade de cada administrador da rede.



**Palavras-chave:** PROTOCOLOS DE REDE.  NAT. DNS. TCP/IP.

**LISTA DE SIGLAS**

AP – Access Point

ARPA - Advanced Research Projects Agency

BGP - Border Gateway Protocol

BSS - Basic Service Set

CIR - Commited Information Rate

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DNS - Domain Name System

DHCP - Dynamic Host Configuration Protocol

DSCP - Differentiated Services Code Point

DSSS - Direct Sequence Spread Spectrum

ESS - Extended Service Set

FHSS - Frequency Hopping Spread Spectrum

FTP – File Transfer Protocol

GHz – Giga Hertz

GIF - Graphics Interchange Format

GLP - General Public Licence

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Eletronics Engineers

IP – Internet Protocol

JPEG - Joint Photographic Experts Group

LAN – Local Area Network

LLC - Logical Link Control

MAC - Media Access Control

Mbps - Megabits por Segundo

MIMO - Multiple-Input Multiple-Output

MPEG - Motion Picture Experts Group

MPLS - Multi-Layer Protocol Label Switching

MPR - Multipoint Relays

NAT - Network Address Translation

OFDM - Orthogonal Frequency Division Multiplexing

OLSR - Optimized Link State Routing

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

PCI - Protocol Control Information

PDU - Protocol Data Unit

PHB - Per-Hop Behavior

TS – Terminal Service

RFC - Request for Comments

RIP - Routing Information Protocol

RSVP - Resource Reservation Protocol

SDU - Service Data Unit

SIP - Session Initiation Protocol

SLA - Service Level Agreement

SNMP - Simple Network Management Protocol

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

ToS – Type of Service

TTL – Time to Live

UDP - User Datagram Protocol

VoIP – Voice over Internet Protocol

WAN - Wide Area Network

WLAN – Wireless Local Area Network

## LISTA DE ILUSTRAÇÕES

Figura 1 Topologia de Distância de Rede.....13
Figura 2 Topologia de Rede.....14
Figura 3 Nat.....18
Figura 4 Topologia de Rede Estrela.....20
Figura 5 Configuração do Modem.....21
Figura 6 Registro de nome no Site www.noip.com.....22
Figura 7 Software de Registro de Nome Instalado no Servidor.....22
Figura 8 Tela de Usuários do WindowsServer2008.....23
Figura 9 Tela de Ativação de Licenças do Windows Server 2008 para TS....24
Figura 10 Area de Trabalho Remota do Windows.....25
Figura 11 Area de Trabalho Remota do Windows Autenticação.....26
Figura 12 Area de Trabalho Remota do Windows - Arquivos e Programas....26
Figura 13 Area de Trabalho Remota do Windows - Programa .....27

**SUMÁRIO**


**1 INTRODUÇÃO ..... 08**
1.1 TEMA ..... 08
1.2 OBJETIVOS ..... 08
1.2.1 OBJETIVO GERAL ..... 08
1.2.2 OBJETIVOS ESPECÍFICOS ..... 09
1.3 METODOLOGIA ..... 09
1.3.1 PROCEDIMENTOS METODOLÓGICOS ..... 09
1.4. JUSTIFICATIVA ..... 10
1.5 ESTRUTURA ..... 10
**2 REFERENCIAIS TEÓRICOS ..... 12**
2.1 MODELOS DE REFERÊNCIA ..... 12
2.1.3 NAT ..... 17
2.1.4 DNS ..... 18
2.2 TERMINAL SERVICE ..... 19
**3 ESTUDO DE CAMPO ..... 20**
3.1 CONFIGURANDO MODEM ROTEADOR E SERVIDOR ..... 21
3.2 TESTES E RESULTADOS ..... 25
**4 CONSIDERAÇÕES FINAIS ..... 28**
**REFERÊNCIAS ..... 29**

# 1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo e implementação de técnicas de Acesso Remoto.

## 1.1 TEMA

Acesso remoto é quando acessamos um computador ou outro aparelho eletrônico a distância, podendo este equipamento estar na nossa sala ao lado ou a milhares de quilômetros de distância. A Internet permite a usuários de computadores a conexão com outros computadores facilmente, mesmo estando em localidades distantes no mundo. Isto está encorajando novos meios de se trabalhar em casa, a colaboração e o compartilhamento de informações em muitas empresas. Um contador estando em casa pode auditar os livros-caixa de uma empresa baseada em outro país por meio de um servidor situado num terceiro país. Um executivo fora de seu local de trabalho, talvez no outro lado do mundo numa viagem a negócios ou de férias, pode abrir a sua sessão de desktop remoto em seu computador pessoal, através da Internet com serviço de Terminal Service de um Servidor. Isto dá ao trabalhador acesso completo de todo os seus dados e arquivos usuais, incluindo o e-mail e outras aplicações enquanto estiver fora de seu local de trabalho.

## 1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

### 1.2.1 Objetivo Geral

Desenvolver, implementar e apresentar os resultados de um modelo para acesso remoto com Terminal Service do Windows Server 2008.

### 1.2.2 Objetivos Específicos

- Instalar um Servidor Local.
- Habilitar o Serviço de Terminal Service.
- Liberar Acesso no Modem Roteador.
- Acessar programas, arquivos, e-mail do Servidor.

## 1.3 Metodologia

Será desenvolvida pesquisa bibliográfica para assimilar o que está ocorrendo dentro de uma conexão remota.

Será descrito no trabalho como liberar porta de acesso no Modem Roteador, configurar o Servidor Terminal Service. Descrever os passos e ao fim analisar a viabilidade técnica do modelo projetado.

### 1.3.1 PROCEDIMENTOS METODOLÓGICOS

Seguindo a linha de raciocínio de Gil (2002) sobre a classificação das pesquisas, levando em consideração os objetivos de cada uma, este trabalho de monografia estará seguindo os procedimentos técnicos de pesquisa bibliográfica e estudo de campo. Pesquisa bibliográfica, pois é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de um gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente (GIL, Antônio Carlos, 2002, p. 44-45). Já o estudo de campo é definido, pois procura muito mais o aprofundamento das questões propostas do que a distribuição das características da população segundo determinadas variáveis. Como consequência, o planejamento do estudo de campo apresenta muito maior flexibilidade, podendo ocorrer mesmo que seus objetivos sejam reformulados ao longo da pesquisa. Outra distinção é que no levantamento das informações procura-se identificar as características dos componentes do universo pesquisado, possibilitando a caracterização precisa de seus segmentos (GIL, Antônio Carlos, 2002, p. 53).

Referência Bibliográfica inicial:

http://technet.microsoft.com/pt-br/library/cc753844(v=WS.10).aspx

## 1.4 JUSTIFICATIVA

Os administradores de redes em geral apresentam ainda alguma dificuldade em compatibilizar sua arquitetura de redes já existente com novos serviços ofertados. Apesar de existirem tutoriais passo a passo mostrando como configurar equipamentos da maneira mais indicada, ainda encontram-se muitas redes subutilizadas devido ao projeto e dimensionamento errado da mesma.

Com base nos resultados dos testes que serão realizados, este trabalho apresentará alguns motivos para a utilização de Acesso Remoto em redes e também alguns cuidados que se deve ter em projetar endereços de redes.

Utilizando uma topologia de rede um pouco mais complexa, pretende-se demonstrar que um administrador pode ter o funcionamento adequado de sua rede apenas utilizando de recursos de configuração existentes nos próprios equipamentos e também a partir de pesquisas sobre NAT, AUTENTICAÇÃO DE PROTOCOLOS e DNS em rede de computadores.

## 1.5 ESTRUTURA

A monografia é composta por 4 capítulos. Primeiramente, o capítulo 1, tratará da parte introdutória, sendo apresentado o tema, os objetivos a serem atingidos, a justificativa da escolha e os problemas a serem resolvidos. Também nesta primeira parte, apresenta-se o procedimento metodológico e a estrutura da monografia.

O capítulo 2 trata do referencial teórico do projeto. Teoria sobre redes, Protocolos de Autenticação, NAT, DNS, e por fim a apresentação dos Serviços RDP. Este capítulo trará de forma clara e objetiva os conceitos de rede que qualquer administrador deve conhecer antes de aplicar RDP em sua estrutura ou até mesmo antes de promover qualquer mudança na arquitetura de sua

rede. Tratará também uma explicação sobre o funcionamento de RDP, como por exemplo, liberação de acesso de porta para comunicação remota.

Partindo para a parte prática do estudo, o capítulo 3 mostrará os passos seguidos para a configuração do Roteador Modem, bem como a aplicação dos serviços disponíveis por padrão neste equipamento. Com isso, associa-se a parte teórica (acesso a aplicações) com a parte prática (acessar remotamente). O estudo de campo será visto neste mesmo capitulo, onde equipamentos serão instalados e será analisado a eficácia dos serviços em rede pela internet. A partir dos resultados obtidos, poder-se-á afirmar que a configuração de Terminal Service é aplicável e benéfica.

Finalizando a monografia, o capítulo 4 traz as conclusões sobre o estudo como um todo.

# 2 REFERENCIAIS TEÓRICOS

A função de servidor dos Serviços de Terminal do Windows Server 2008 oferece tecnologias que permitem aos usuários acessar programas baseados no Windows e instalados em um servidor de terminal ou acessar a área de trabalho completa do Windows. Com os Serviços de Terminal, os usuários podem acessar um servidor de terminal estando em uma rede corporativa ou na Internet.

Os Serviços de Terminal permitem implantar e manter softwares de maneira eficaz em um ambiente corporativo. Você pode implantar os programas facilmente a partir de um local central. Como você instala os programas no servidor de terminal e não no computador cliente, fica mais fácil atualizar e manter os programas.

Quando um usuário acessa um programa em um servidor de terminal, a execução do programa ocorre no servidor. Somente informações de teclado, mouse e vídeo são transmitidos pela rede. Cada usuário vê apenas sua própria sessão. A sessão é gerenciada de maneira transparente pelo sistema operacional do servidor e é independente de qualquer outra sessão de cliente.

## 2.1 Modelos de Referência

***LAN* (Local Area *Network*)** - Pode-se caracterizá-la como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa “pequena região”, em geral distâncias entre 100m e 25 km.( Livro Gorki Starlin TCP/IP 5° Edição).

Características de *LANs*:

- Altas taxas de transmissão;
- Baixas taxas de erros;
- Propriedade privada;
- Geograficamente limitadas;
- Topologias mais utilizadas: estrela, anel e barramento.

***MAN* (*Metropolitan* Area *Network)*** - As Redes Metropolitanas são intermediárias às *LANs* e *WANs*, apresentando características semelhantes às redes locais e, em geral, cobrem distâncias maiores que as LANs. Um bom exemplo de *MAN* são as redes de TV a cabo.(Livro Gorki Starlin TCP/IP 5° Edição).

Características de *MANs*:

- Restrita a uma área metropolitana;
- Meios de transmissão: Cabos ópticos e coaxiais;
- Taxas de transmissão: 10mbps.

***WAN* (*Wide Area Network)*** - Redes Geograficamente Distribuídas. Surgiram da necessidade de se compartilhar recursos por uma comunidade de usuários geograficamente dispersos.(Livro Gorki Starlin TCP/IP 5° Edição).

Características de *WANs*:

- Custo de comunicação elevado devido a uso de meios como: linhas telefônicas, satélites e micro-ondas;
- Baixas velocidades de transmissão (dezenas de Kilobits, podendo chegar a Megabits/segundo);
- Geralmente são de propriedade pública;
- A escolha de um tipo particular de rede para suporte a aplicações é uma tarefa difícil. É necessário analisar atributos como: custo, confiabilidade, tempo de resposta, disponibilidade, facilidade de manutenção, prazos para atendimento de defeitos, velocidade, e outros.

A Tabela mostra os tipos de rede explicados, seguidos dos valores das distâncias entre os seus nós e a respectiva localização entre eles.

Tabela

| Distância Entre Módulos Processadores | Localização entre Módulos Processadores | Tipo de Rede |
|---|---|---|
| 10 m | Sala | Local |
| 100 m | Prédio | Local |
| 1 km | Campus | Local |
| 10 km | Cidade | Metropolitana |
| 100 km | País | Metropolitana |
| 1000 km | Continente | Geograficamente Distribuída |
| 10000 km | Planeta | Geograficamente Distribuída |

**Figura 1**

**Fonte: Autoria própria**

Topologias

Pode-se dizer que a estrutura de comunicação entre vários nós de rede é uma topologia ligada por um enlace físico e organizados por regras claras de comunicação, os protocolos. Esses enlaces são as linhas de comunicação. E a topologia física é muitas vezes confundida com a topologia lógica. Podemos ter topologia lógica em anel, mas ligados fisicamente em estrela. Isto é possível principalmente devido aos equipamentos que dispomos hoje no mercado. Livro

Principais tipos de topologias de rede

**Ponto-a-Ponto -** é comunicação entre dois ou mais processadores, não necessariamente conectados diretamente e, que pode usar outros nós como roteadores.

***Bus*** (barramento) - o canal é compartilhado entre todos os processadores, podendo o controle ser centralizado ou distribuído. É a mais comum, pois possui alto poder de expansão utilizando repetidores.

***Ring*** (anel) - utiliza em geral ligações ponto-a-ponto que operam em um único sentido de transmissão. O sinal circula no anel até chegar ao destino. É uma topologia confiável, mas com grande limitação quanto a sua expansão pelo aumento de “retardo de transmissão” (intervalo de tempo entre início e chegada do sinal ao nó destino).

**Estrela -** utiliza um nó central (comutador ou *switch*) para chavear e gerenciar a comunicação entre as máquinas. Provoca *overhead* localizado, já que uma máquina é acionada por vez, simulando um ponto-a-ponto. .(Livro Gorki Starlin TCP/IP 5° Edição).

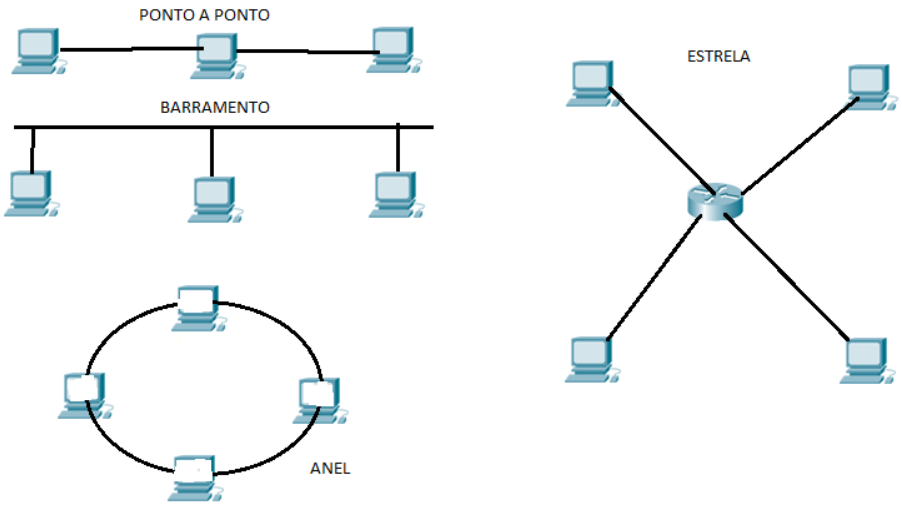


**Figura 2 – Topologia de Rede**

**Fonte: Autoria própria**

Protocolos de Autenticação PPP – *POINT TO POINT PROTOCOL*

O PPP fornece autenticação entre 2 pontos de qualquer sistema, pois sua finalidade é atravessar os mecanismos de segurança para autenticar o usuário, autorizando ou não sua conexão. A autenticação PPP é realizada por um processo na segunda fase da conexão. Durante a primeira fase, ambos - servidor e cliente concordam em utilizar um único e específico canal de comunicação. (Livro Gorki Starlin TCP/IP 5° Edição).

**PAP**

*O Password Authentication Protocol (PAP)* é um protocolo de autenticação de texto em formato simples. O nome do usuário e senha são esperados pelo servidor de acesso remoto e são enviados pelo cliente remoto em texto de formato simples. Porém, o protocolo PAP não é um protocolo de autenticação seguro. Um usuário remoto que capture pacotes de um segmento de rede aonde esta acontecendo uma conexão autenticada por esse protocolo, vai obter de maneira fácil e rápida o usuário e senha entre essa autenticação.

O PAP é um protocolo de troca de mensagens simples:

- O cliente de acesso remoto envia uma mensagem de pedido de autenticação PAP ao servidor de acesso remoto contendo o nome de usuário e senha do cliente em texto de formato simples;

- O servidor de acesso remoto então confere o nome de usuário e senha do cliente e envia de volta uma mensagem PAP Authenticate-Ack quando as credenciais do usuário estiverem corretas ou uma mensagem PAP Authenticate-Nak quando as credenciais do usuário estiverem incorretas.

O protocolo PAP esta incluído na família de servidores e clientes Windows. E possível então que clientes de acesso remoto Windows possam conectar os servidores de acesso remotos mais antigos. Para fazer com que o seu servidor de acesso remoto seja seguro, assegure-se que o protocolo de autenticação PAP esteja desabilitado. (TANENBAUM, ANDREW S., 2003, p.307).

**CHAP**

*O Challenge Handshake Authentication Protocol (CHAP)* é um protocolo de autenticação de desafio de resposta documentado na RFC 1994. Ele usa

protocolo de criptografia Message Digest 5 (MD5) de um só sentido para responder a um desafio de resposta hash emitido pelo servidor de acesso remoto.

O protocolo CHAP é uma melhoria em cima dos protocolos PAP e SPAP, pois a senha, nunca é enviada em cima da primeira mensagem. Ao invés, a senha é usada para criar uma string hash de desafio de um só sentido. O uso do protocolo CHAP é negociado durante a negociação do protocolo LCP (Link Control Protocol) e usa o algoritmo 0x05. O CHAP é um protocolo de troca de mensagens que usa três mensagens:

- O servidor de acesso remoto envia uma mensagem de desafio CHAP que contém uma chave de sessão e uma string hash de desafio arbitrário;

- O cliente de acesso remoto devolve uma mensagem de resposta CHAP que contém o nome de usuário em texto simples, uma string hash de desafio, a chave de sessão e a senha do cliente usando o algoritmo Message Digest 5 (MD5) de um só sentido;

- O servidor de acesso remoto duplica a string hash e compara com a string hash da resposta CHAP. Se as strings hashes são as mesmas, o servidor manda de volta uma mensagem de sucesso CHAP. Se as strings hashes são diferentes, uma mensagem de fracasso CHAP é enviada.

*O Challenge Handshake Authentication Protocol versão 1 (MS-CHAP v1)* é um protocolo de autenticação codificado bem parecido com o CHAP. Como no protocolo CHAP o servidor de acesso remoto envia um desafio ao cliente remoto que consiste em uma chave de sessão e um string hash de desafio arbitrário. O cliente remoto tem que devolver o nome de usuário e um string hash de desafio em Message Digest 4 (MD4), a chave sessão e a senha em MD4 também.

Uma diferença entre o CHAP e MS-CHAP v1 é que, no CHAP, a versão de texto simples da senha deve estar disponível para validar a resposta de desafio. No MS-CHAP v1, o servidor de acesso remoto exige só a string hash MD4 da senha para validar a resposta de desafio.

O uso do protocolo MS-CHAP v1 é negociado durante a negociação do protocolo LCP (Link Control Protocol) e usa o algoritmo 0x80. Uma vez que a negociação do protocolo LCP esteja estabelecida, mensagens do protocolo MS-CHAPv1 vão usar o ID 0xC2-23 do protocolo PPP.
O MS-CHAP v1 é um protocolo de troca de mensagens que usa três mensagens:

- O servidor de acesso remoto envia uma mensagem de desafio MS-CHAP que contém uma chave de sessão e um string hash de desafio arbitrário;

- O cliente remoto devolve uma mensagem de resposta MS-CHAP que contém o nome de usuário em texto de formato simples e um string hash de desafio, a chave de sessão e a string da senha em formato MD4 de um só sentido;

- O servidor duplica o string hash e compara com a string hash MS-CHAP resposta do cliente. (TANENBAUM, ANDREW S., 2003, p.307).

### 2.1.3 NAT

NAT é como a recepcionista de um grande escritório. Suponha que você deixou instruções com a recepcionista para que ela não encaminhe nenhuma ligação a menos que você peça. Mais tarde, você liga para um cliente potencial e deixa uma mensagem para que ele retorne a ligação.

Você diz à recepcionista que você está esperando uma ligação desse cliente e pede para que ela faça a transferência da chamada.

O cliente liga para o número principal para seu escritório, que é o único número que ele conhece. Quando o cliente disser à recepcionista quem ele procura, a recepcionista verificará uma tabela de pesquisa que corresponde seu nome ao seu ramal. A recepcionista sabe que você pediu essa chamada; portanto, ela encaminha a pessoa que efetuou a chamada para seu ramal.

Assim, enquanto o servidor DHCP designa os endereços IP dinâmicos para os dispositivos dentro da rede, os roteadores habilitados pela NAT retêm um ou muitos endereços IP de Internet válidos fora da rede. Quando o cliente enviar pacotes pela rede, a NAT traduzirá o endereço IP interno do cliente para um endereço externo. Para usuários externos, todo o tráfego destinado para a rede e proveniente dela possui o mesmo endereço IP ou vem do mesmo conjunto de endereços.

A NAT tem muitos usos, mas o principal é salvar os endereços IP, permitindo que as redes usem os endereços IP privados. A NAT traduz endereços privados, não roteáveis e internos em endereços públicos e externos. A NAT tem um benefício adicional de proporcionar um nível maior de privacidade e segurança para uma rede porque ela oculta endereços IP internos de redes externas.

Um dispositivo habilitado para NAT funciona normalmente na borda de uma rede stub. Em nosso exemplo, o R2 é o roteador de borda. Uma rede stub é uma rede que tem uma única conexão com sua rede vizinha. Como visto no ISP, o R2 forma uma rede stub.

Quando um host dentro da rede stub, por exemplo, PC1, PC2 ou PC 3, deseja transmitir um pacote para um host externo, esse pacote é encaminhado para R2, o roteador de gateway de borda. O R2 executa o processo de NAT,

traduzindo o endereço privado interno do host para um endereço público, roteável e externo.

Na terminologia de NAT, a rede interna é o conjunto de redes que estão sujeitas à tradução. A rede externa se refere a todos os outros endereços. Os endereços IP possuem designações diferentes dependendo de estarem na rede privada ou na rede pública (Internet) e de o tráfego estar chegando ou saindo.( Modulo 4 CISCO)

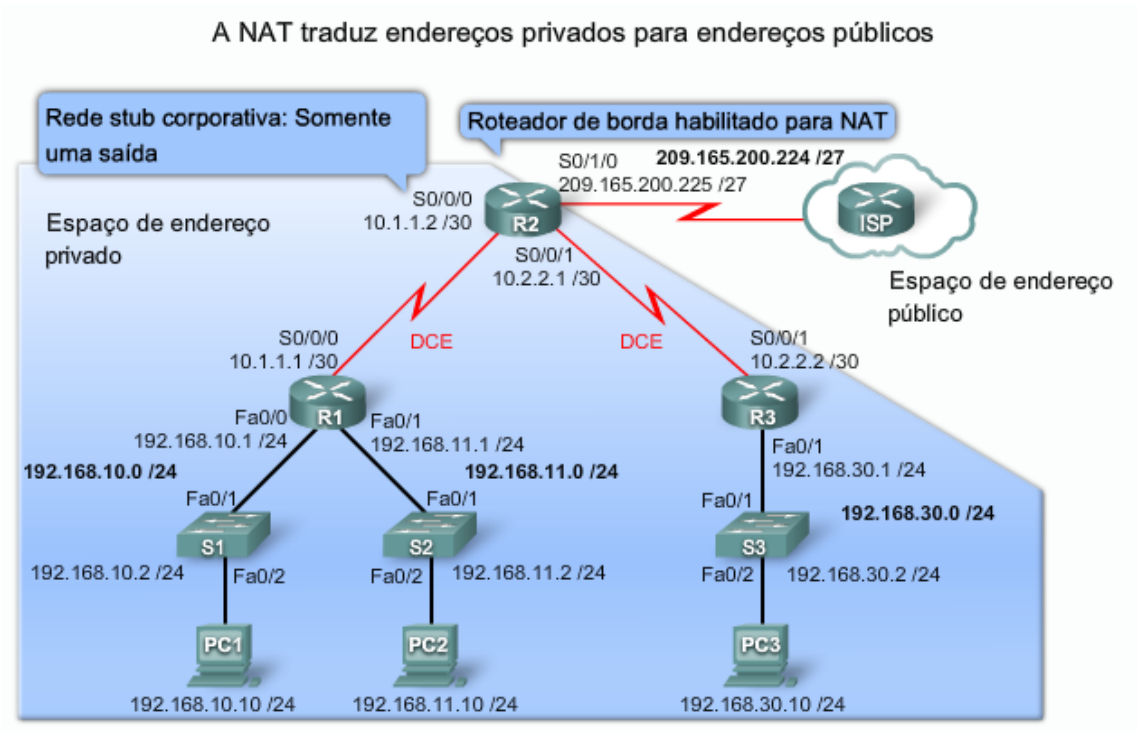


**Figura 3 - NAT**
**Fonte: Modulo 4 CISCO**

## 2.1.4 DNS

DNS é a sigla para Domain Name System (Sistema de Resolução de Nomes). Trata-se de um recurso usado em redes TCP/IP (o protocolo utilizado na internet e na grande maioria das redes) que permite acessar computadores sem que o usuário e computador não tenha conhecimento de seu endereço IP. O DNS (também conhecido como Sistema de Nomes de Domínios) é um sistema de gerenciamento de nomes hierárquico e distribuído operando em duas definições:

• Examinar e atualizar seu banco de dados.
• Resolver nomes de domínios em endereços de rede (IPs).

Cada site da internet é acessível por um endereço IP. O problema é que existe tantos que é praticamente impossível decorar o IP de cada um. O DNS é uma espécie de sistema para a tradução de endereços de IP para nomes de domínios. Assim, é possível atribuir nomes a um IP numérico, pois o DNS será responsável por efetuar a interpretação das palavras que foram utilizadas e transformá-las em números, de forma que o computador as compreenda e devolva o caminho correto por meio do acesso bem sucedido. Ou seja, é um recurso usado em redes TCP/IP que permite acessar computadores sem que o usuário saiba o endereço de IP ou sem que este precise ser informado para que o procedimento seja efetuado. É ele que permite o uso de nomes (também chamados de domínios) ao invés dos IPs no acesso aos sites. Basicamente, na internet, o DNS é um conjunto de grandes bancos de dados distribuídos em servidores de todo o mundo.

## 2.2 Terminal Service

Os Serviços de Terminal são uma função de servidor formada por vários subcomponentes, conhecida como “serviços de função”. No Windows Server 2008, os Serviços de Terminal consistem nos seguintes serviços de função: Terminal Server, Acesso via Web TS, Licenciamento TS, Gateway TS, Agente de Sessão TS. O Terminal Server permite que um servidor hospede programas baseados no Windows ou a área de trabalho completa do Windows. Acesso via Web TS habilita ferramenta para acesso Web. O Licenciamento do Terminal Services (Licenciamento do TS) gerencia as licenças de acesso para os clientes dos Serviços de Terminal (TS CALs) necessárias para que cada dispositivo ou usuário se conecte a um servidor de terminal.

O Gateway de Serviços de Terminal (Gateway TS) é um serviço de função que permite que os usuários remotos se conectem aos recursos em uma rede corporativa interna, a partir de qualquer dispositivo conectado à Internet que possa executar o cliente RDC (Conexão de Área de Trabalho Remota). O Agente de Sessão do Terminal Services (Agente de Sessão TS) dá suporte ao balanceamento de carga de sessão entre servidores de terminal de um farm e à reconexão a uma sessão existente em um farm de servidores de terminal com balanceamento de carga.

Para o bom funcionamento do acesso remoto é necessário ter essas funções habilitas, para não ocorrerem falhas de conexão por limite de licença e também mantem a boa conexão de acesso via Internet.( MICROSOFT, Technet. **Modelo TCP/IP.** Microsoft, Biblioteca., 2011.Disponível: <http://technet.microsoft.com/pt- br/library/cc786900%28WS.10%29.aspx> ).

## 3 ESTUDO DE CAMPO

Este capítulo apresentará a configuração do *Modem Roteador* para operar com a configuração de Acesso Remoto. Serão realizados testes e posteriormente mostrados os resultados a fim de demonstrar o funcionamento da aplicação.

Será instalados um Modem Roteador, um computador e um Servidor operando com o Windows. Primeiramente, será feito o registro DNS para que seja possível um nome fazer a resolução do IP WAN da Internet. Este registro pode ser feito no site http://www.noip.com/. Na configuração do Modem Roteador será direcionado um NAT para o IP do Servidor.

Na sequência, será habilitado o serviço de Terminal Server. Os resultados serão visualizados com acesso interno e externo.

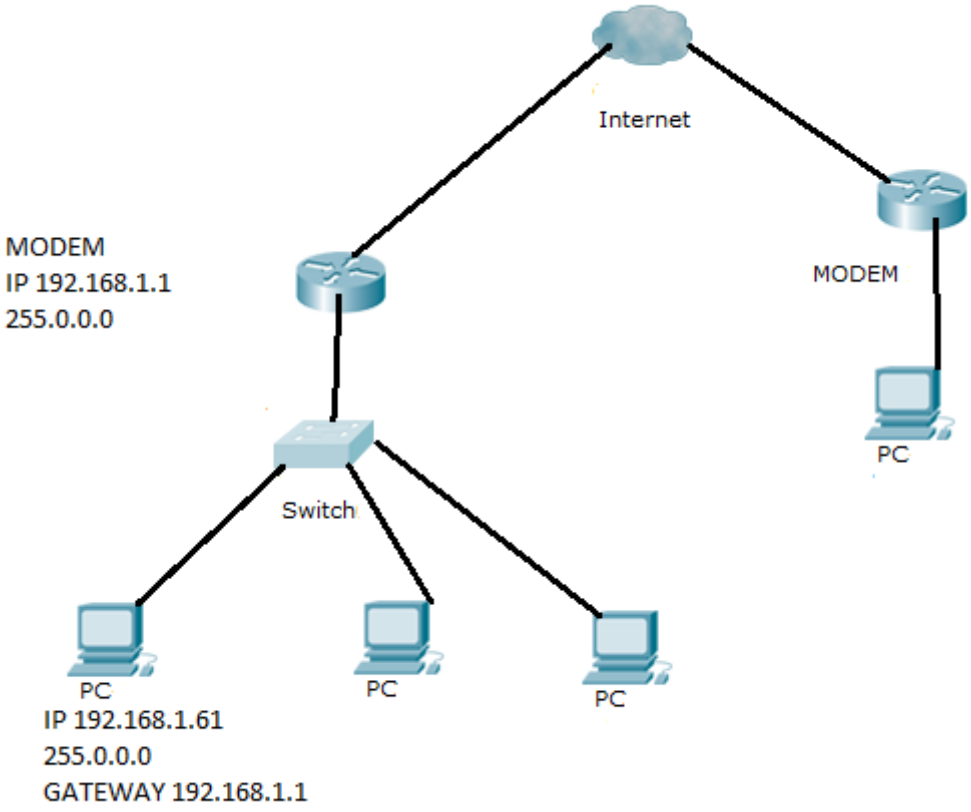


**Figura 4– Topologia de Rede - Estrela**
**Fonte: Autoria Própria.**

Na figura 4 apresenta a topologia Estrela. O acesso remoto será configurado no PC de IP 192.168.1.61 o modem de com IP 192.168.1.1.

## 3.1 CONFIGURANDO MODEM ROTEADOR E SERVIDOR WINDOWS SERVER 2008

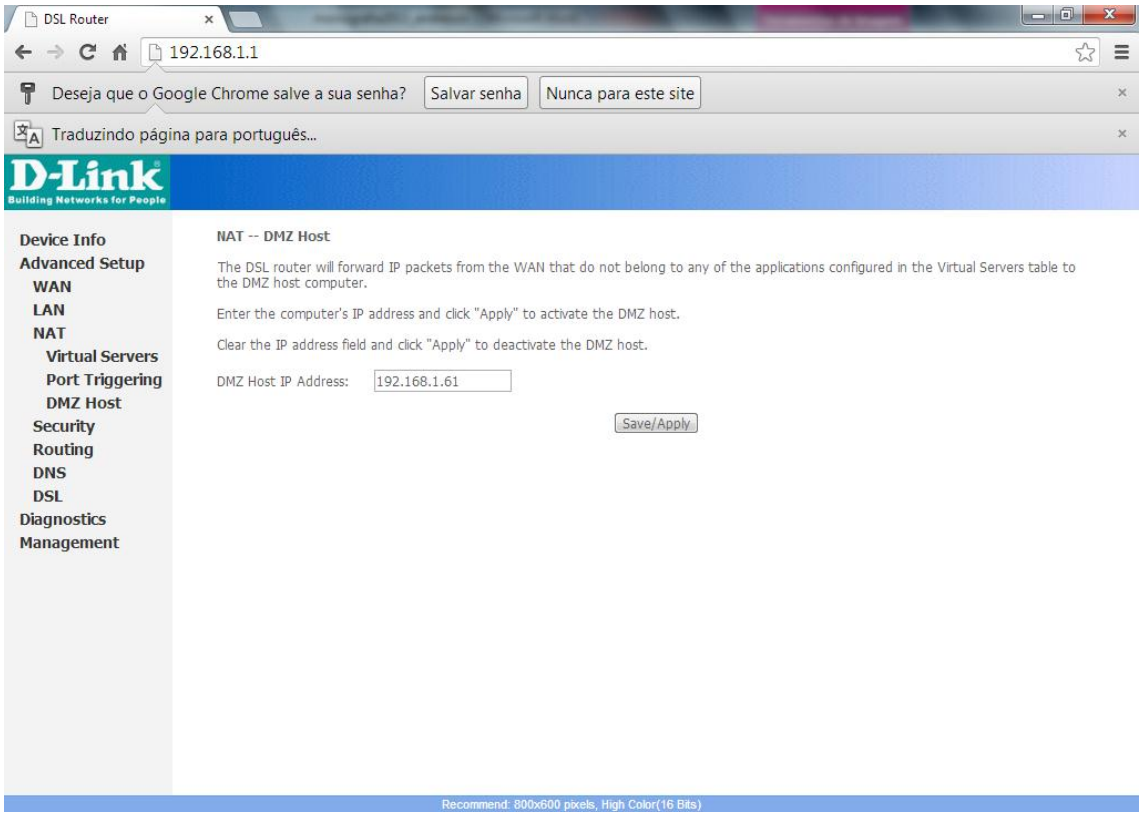


**Figura 5 – Configuração do Modem DLINK DSL 500B**
**Fonte: Autoria Própria.**

Para a configuração do modem DLINK DSL 500B, devem-se escolher as opções - ir até as abas *NAT>DMZ HOST)*, inserir o IP que é 192.168.1.61 o qual foi escolhido para ser configurado no Servidor conforme mostrado na figura 5.

O IP 192.168.1.61 é o IP do computador que receberá o acesso remoto. O DMZ fará com que este ip seja escondido e acessado com o IP *WAN* ou nome do host fornecido no site www.noip.com como neste caso.

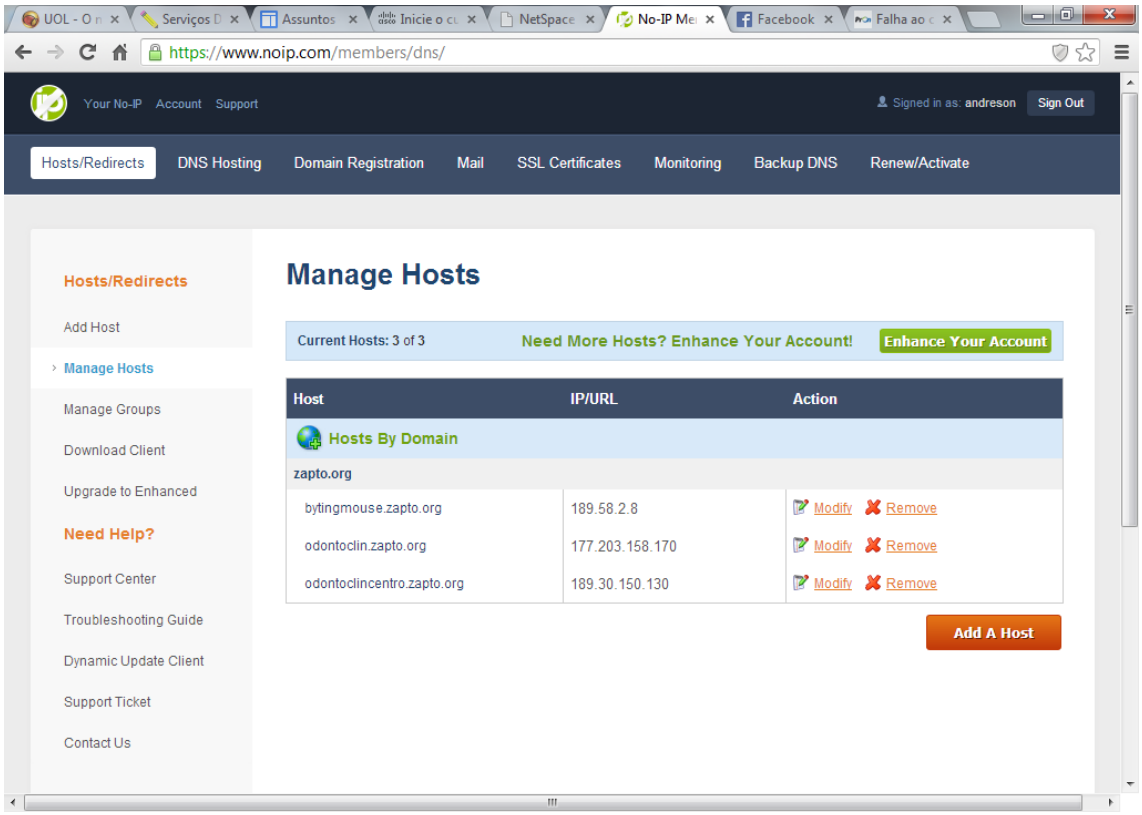


**Figura 6 – Registro de Nome no site http://www.noip.com**
**Fonte: Autoria Própria.**

Na figura 6 apresenta o registro de um nome odontoclin.zapto.org para ser resolvido o numero IP dinâmico de *WAN* da Internet. Também tem a opção de contratar com o Provedor de Internet um IP fixo, dando possibilidades de fazer o acesso remoto com o mesmo número de IP fornecido pela Operadora de Internet que não é neste caso.

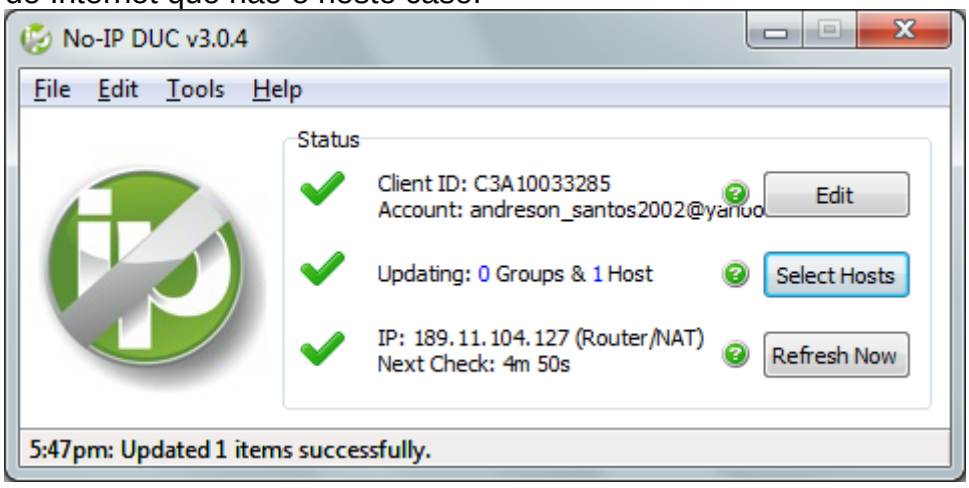


**Figura 7 – Software de Registro de Nome Instalado no Servidor**
**Fonte: Autoria Própria**

A Figura 7 representa o Software instalado no servidor que tem a função de fazer a leitura e gravação do IP *WAN* e resolver o nome escolhido. Este

software pode ser baixado da internet no site www.noip.com e instalado no Servidor que receberá o acesso remoto.
O IP dinâmico *WAN* é alterado com o desligamento do Modem, porém o nome ODONTOCLIN.ZAPTO.ORG não vai ser alterado pois esta tendo um DNS do nome para resolver qualquer IP *WAN* deste acesso.

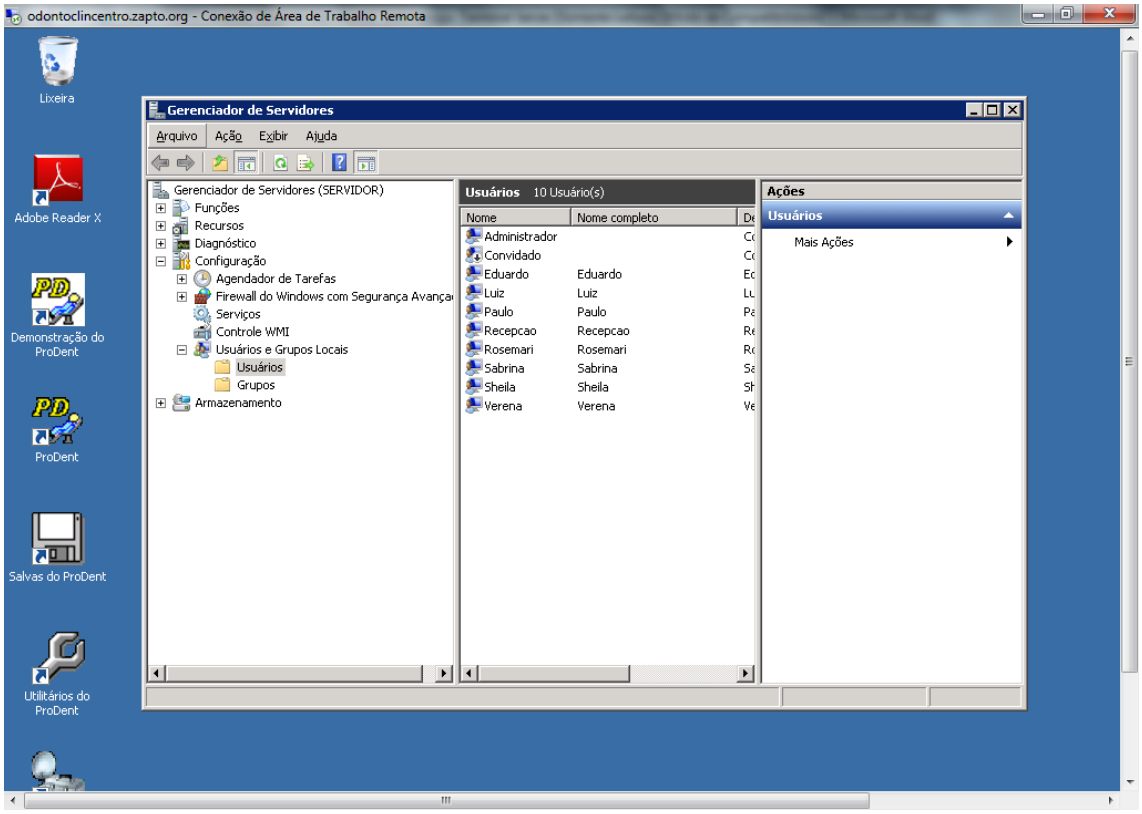


**Figura 8 – Tela de Usuários do Windows Server 2008**
**Fonte: Autoria Própria.**

No Servidor foi criado usuários para acesso remoto. O usuário administrador foi inserido a senha qwe123@. Foi habilitado o serviço de Terminal Server com suas licenças respectivamente. O Terminal Service pode ser acessado por mais de um *login* de usuário conforme licenças adquiridas.

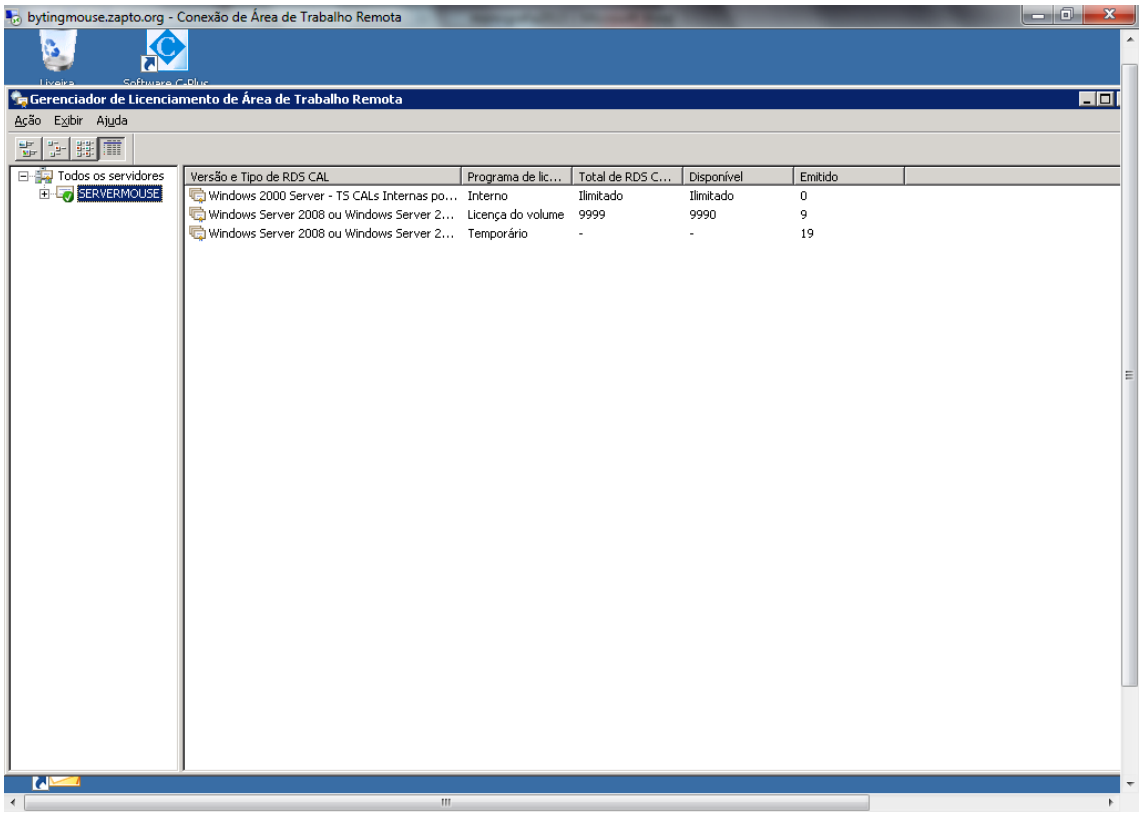


**Figura 9 – Tela de Ativação de Licenças do Windows Server 2008 para TS**
**Fonte: Autoria Própria.**

Na figura 9 é mostrada a ativação das licenças do Windows Server 2008. O tempo para fazer a ativação é de 21 dias, sendo que se passar o período, o acesso a área de trabalho remota não estará acessível até a efetivação das licenças.

## 3.2 TESTES E RESULTADOS

Os testes para chegar-se ao objetivo da presente pesquisa, iniciaram-se em um computador com Sistema Operacional Windows, utilizando o aplicativo de Conexão da Área de Trabalho Remota. O nome do Computador é o DNS que foi elaborado no Site http://www.noip.com/ para o Servidor de Destino.

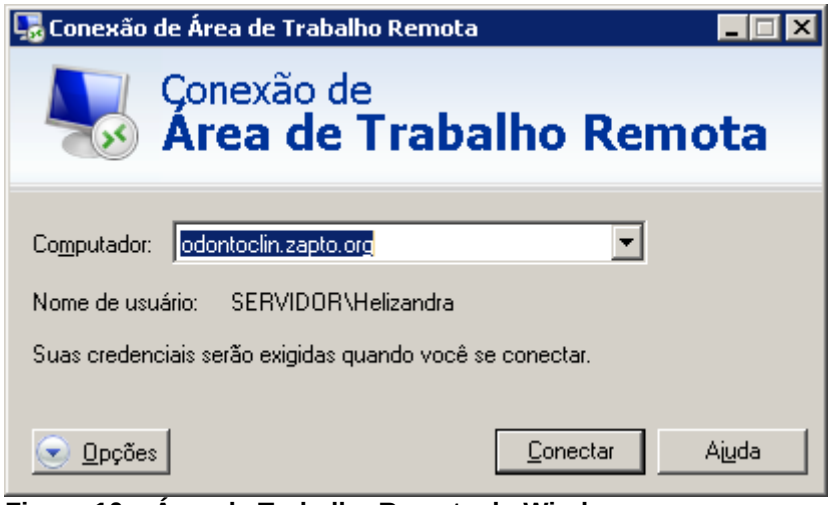


**Figura 10 – Área de Trabalho Remota do Windows**
**Fonte: Autoria Própria.**

Para iniciar o acesso remoto é utilizada a conexão de área de trabalho do Windows conforme mostrado na figura 10. Esta conexão pode ser feita para rede *Lan ou Wan*. Também pode ser executado no *prompt* do *Msdos* com o comando MSTSC.

Na área de trabalho remota foi inserido o nome do Computador de Destino em seguida o login e senha do usuário para autenticação no Servidor conforme figura 11.

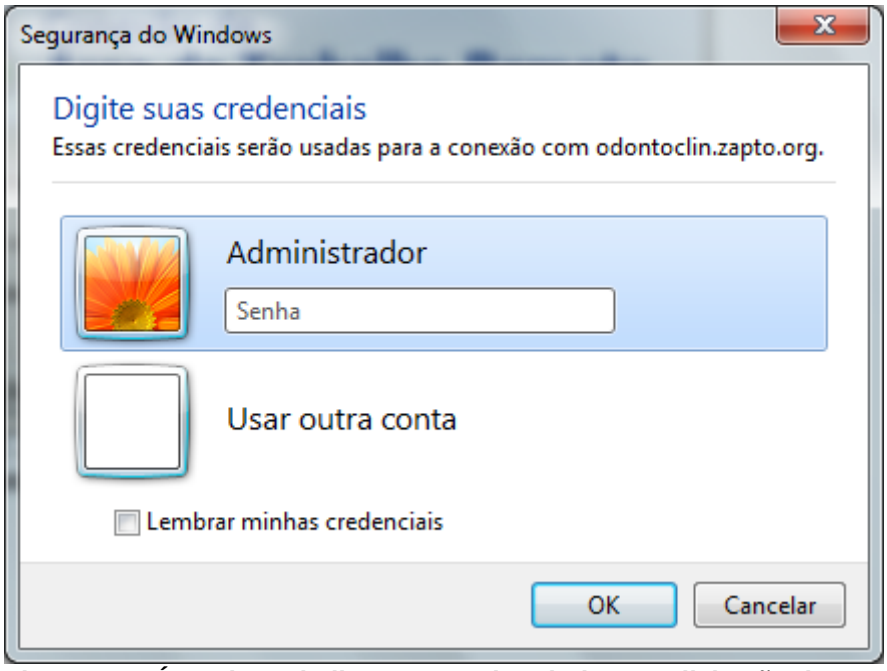


**Figura 11 – Área de Trabalho Remota do Windows Solicitação de Autenticação**
**Fonte: Autoria Própria.**

Depois de autenticado será aberto a área de trabalho remota com acesso direto a arquivos e programas do Servidor acessado conforme figura 12 e 13. Pode ser feito alterações, inclusões, acesso a dados etc.

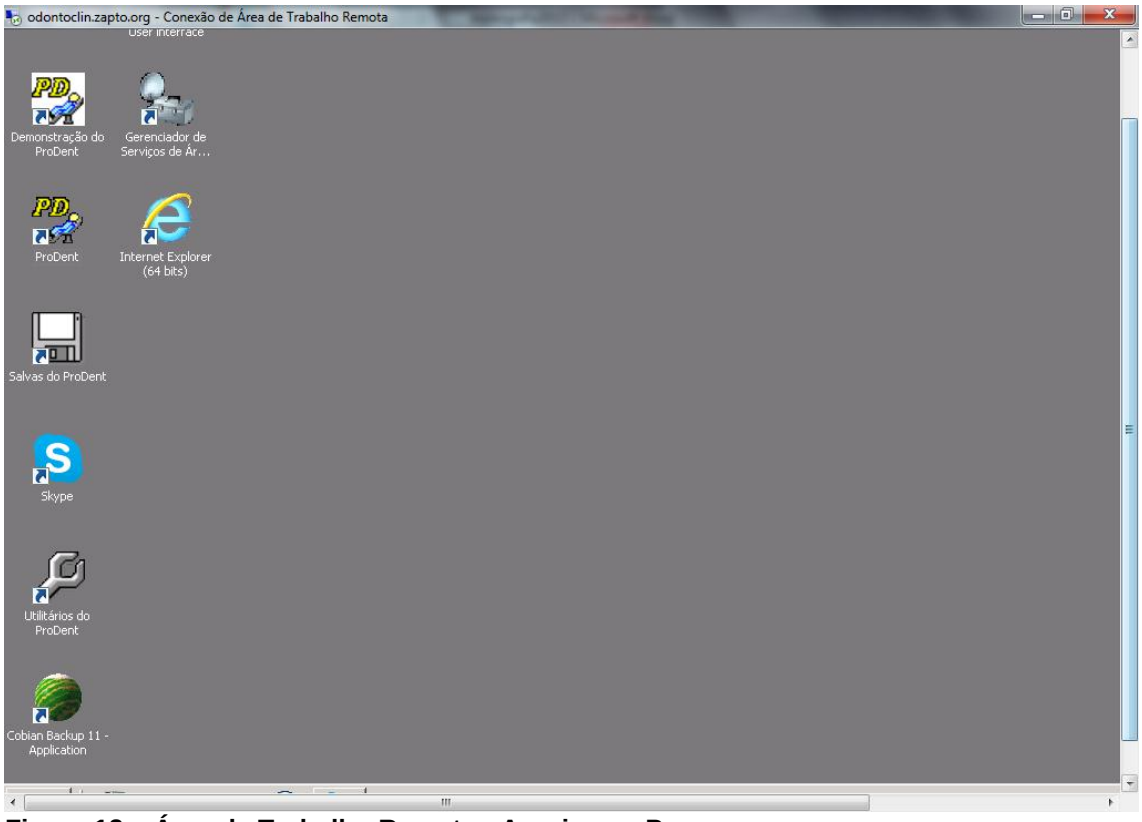


**Figura 12 – Área de Trabalho Remota - Arquivos e Programas**
**Fonte: Autoria Própria.**

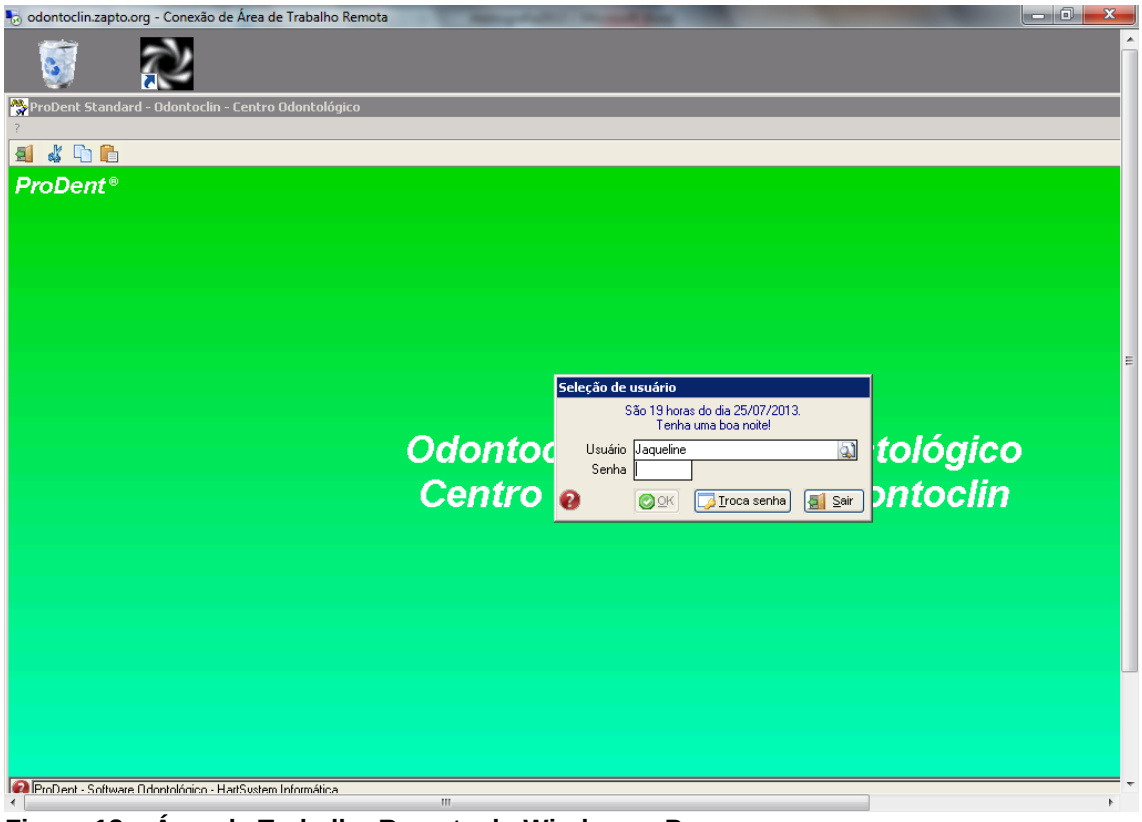


**Figura 13 – Área de Trabalho Remota do Windows - Programa**
**Fonte: Autoria Própria.**

## 4 CONSIDERAÇÕES FINAIS

As redes estão em constante crescimento e as empresas tendem a acompanhar tal fato, onde praticamente tudo gira em torno da TI de uma empresa, como transações bancárias, telefonia, sistemas internos de controle, contabilidade e muitas outras funções. Com a pesquisa bibliográfica e o estudo de casos concluídos, pode-se afirmar que o uso de Acesso Remoto realmente é eficaz nas redes das corporações. Recomenda-se a utilização do Acesso Remoto, principalmente em programas de informação que tende a ser atualizado durante 24 horas com novas informações e pesquisas de trabalho, tendo o usuário total acesso a essas informações a hora que precisar.

## REFERÊNCIAS

http://technet.microsoft.com/pt-br/library/cc753844(v=WS.10).aspx Acesso em 22/07/2013, 20:00.

Livro Gorki Starlin TCP/IP 5° Edição. Acesso em 22/07/2013, 20:30

Modulo 4 – CISCO - Acesso em 22/07/2013, 23:20.

CASTRO, Jaime J. de. **Como nasceu a ideia de rede entre computadores.** Disponível <http://www.apostilando.com/download.php?cod=2963&categoria= > Acesso em 24/07/2013, 15:00.

CISCO, Networking Academy. **CCNA Exploration – Fundamentos de Rede.** Cisco Systems, Inc., 2007-2009. Acesso em 25/07/2013, 13:15.

TANENBAUM, ANDREW S., 2003, p.307 Acesso em 22/07/2013, 20:15.

FILIPPETTI, Marco Aurélio. **CCNA 4.1 – Guia Completo de Estudos.** Florianópolis: Editora Visual Books, 2008. Acesso em 27/07/2013, 20:00.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4ª. ed. São Paulo: Atlas, 2002. Acesso em 15/07/2013, 13:00.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 791 – *Internet Protocol – Protocol Specification***. Acesso em 16/07/2013, 19:00.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 3626 – OLSR Protocol**. Disponível em <http://www.ietf.org/rfc/rfc3626.txt> Acesso em 01/08/2013, 21:00.

LIMA, Carlos Eduardo Parag; HOLLICK Matthias; STEINMETZ Ralf. **Diferenciação de Serviços na Internet - DiffServ.** Universidade Federal do Rio de Janeiro – Rio de Janero, 2001. Disponível em < http://www.gta.ufrj.br/grad/01_2/diffserv/index.html> Acesso em 22/07/2013, 22:00.

MOGRE, Parag; HOLLICK Matthias; STEINMETZ Ralf. **QoS in Wireless Mesh Networks: Challenges, Pitfalls and Roadmap to its Realization.** Department of Electrical Engineering and Information Technology. Darmstadt University. Darmstadt – Germany, 2007. Acesso em 12/082013, 22:00.

MICROSOFT, Technet. **Modelo TCP/IP.** Microsoft, Biblioteca., 2011.Disponível: <http://technet.microsoft.com/pt- br/library/cc786900%28WS.10%29.aspx> Acesso em 15/08/2013, 20:00.