WILSON JUNIOR DE BRITO AMADOR

ANÁLISE DE DESEMPENHO DO PADRÃO IEEE 802.1X EM REDES CABEADAS UTILIZANDO INFRA-ESTRUTURA DE CHAVE PÚBLICA

Brasília - DF
Julho de 2008

WILSON JUNIOR DE BRITO AMADOR

ANÁLISE DE DESEMPENHO DO PADRÃO IEEE 802.1X EM REDES CABEADAS UTILIZANDO INFRA-ESTRUTURA DE CHAVE PÚBLICA

Trabalho apresentado à banca examinadora da Faculdade de Tecnologia e Ciências Sociais Aplicadas (FATECS) - UniCEUB, como requisito parcial para obtenção do título de Engenheiro da Computação.
Professor Orientador: MsC Francisco Javier de Obaldía Díaz.

Brasília - DF
2008

WILSON JUNIOR DE BRITO AMADOR

ANÁLISE DE DESEMPENHO DO PADRÃO IEEE 802.1X EM REDES CABEADAS UTILIZANDO INFRA-ESTRUTURA DE CHAVE PÚBLICA

COMISSÃO EXAMINADORA

_____
Francisco Javier de Obaldía Díaz

_____
Cláudio Penedo de Albuquerque

_____
Maria Marony Souza Farias Nascimento

Brasília, Julho de 2008.

“Aos meus pais,
Pela dedicação, pelo incentivo e por sempre acreditarem em mim.

À minha namorada Karina,
Por todo carinho e paciência ao longo destes últimos meses.”

AGRADECIMENTOS

Agradeço a todos que colaboraram para a realização deste Projeto, em particular:

Ao professor e orientador Francisco Javier, pelo apoio, sugestões e incentivo.

Aos meus pais, que sempre estiveram ao meu lado, apoiando meu sucesso pessoal e profissional e incentivando para a conclusão do Projeto.

À Karina, por toda dedicação, cumplicidade e por estar ao meu lado nos momentos mais importantes da minha vida.

Aos grandes amigos “Pingüins” conquistados ao longo do Curso de Engenharia, em especial, Alessandro Nader e Rafael Gomes, pela disposição em auxiliar nos momentos críticos do desenvolvimento do Projeto.

À *True Access Consulting*, pela oportunidade de crescimento profissional e pela disponibilização de recursos (laboratório e equipamentos) utilizados neste Projeto.

Aos mestres e amigos Alexsander Bastos e Hebert Moura, pelo auxílio e esclarecimento de dúvidas.

A todos que, de uma forma ou outra, me incentivaram, apoiaram ou ajudaram na conclusão deste desafio, muito obrigado!

SUMÁRIO

RESUMO

A necessidade de eficiência nas redes de dados leva as empresas a buscarem soluções tecnológicas que tragam para a sua rede os melhores níveis de segurança e disponibilidade, tendo em vista as deficiências e vulnerabilidades através dos quais indivíduos não autorizados podem ter acesso às informações disponibilizadas pela rede. Para isso, um dos principais pontos a serem observados é o controle de admissão dos usuários à rede, visando redução na entrada de ameaças e de pessoas que possam porventura obter acesso a informações controladas.

A utilização do Padrão IEEE 802.1x visa solucionar problemas na precariedade de segurança na autenticação, proporcionando confidencialidade e integridade dos dados, uma vez que limita o acesso à rede fazendo o controle de portas no switch. No entanto, é possível que haja sobrecarga de pacotes, devido à inserção de tráfego extra para autenticação dos usuários podendo ocasionar comprometimento na *performance* da rede. Dessa forma, avaliou-se qual a efetiva degradação no desempenho das redes com o mecanismo de segurança 802.1x implementada, calculando a média do Tempo de Resposta, Latência e *Throughput*, utilizando os protocolos FTP (*File Transfer Protocol*) e HTTP (*Hypertext Transfer Protocol*).

Palavras-Chave:
IEEE 802.1x, EAP, RADIUS, autenticação, desempenho

ABSTRACT

The need for efficiency in data networks, leads companies to seek technological solutions that bring the network to its best levels of safety and availability. One of the main points to note is the control of user admission to the network, seeking reduction in the access of threats and people to controlled information.

The use of IEEE 802.1x standard, aims to solve problems of security during authentication. It provides confidentiality and integrity of data, as it limits access to the network, doing the port based access control in the switch. However, there is a possibility to overload the system due to the insertion of extra traffic for user authentication and messages encryption, what can cause impairment in the network performance. Therefore, was evaluated the effective degradation in the performance of networks due to the implementation of 802.1x security mechanism by assessing the average time of response, Latency and Throughput, using the protocols FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol).

Key-Words:
IEEE 802.1x, EAP, RADIUS, authentication, performance

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AAA – *Authentication, Authorization and Accounting* ou Autenticação, Autorização e Gestão de Contas

AC – Autoridade Certificadora

AD – *Active Directory*

CA – *Certification Authority* ou Autoridade Certificadora

CD – *Compact Disc* ou Disco Compacto

CHAP – *Challenge Handshake Authentication Protocol*

CRL – Certificate *Revocation List* ou Lista de Certificados Revogados

CSP – *Cryptographic Service Provider* ou Provedor de Serviço de Criptografia

DC – *Domain Controller* ou Controlador de Domínio

DHCP – *Dynamic Host Configuration Protocol* ou Protocolo de Configuração Dinâmica de Host

DNS – *Domain Name System* ou Sistema de Nomes de Domínios

EAP – *Extensible Authentication Protocol*

EAPOL – *Extensible Authentication Protocol over LAN*

FTP – *File Transfer Protocol* ou Protocolo de Transferência de Arquivos

GPO – *Group Policy Object* ou Política de Grupo

HD – *Hard Disc* ou Disco Rígido

HTML – *HyperText Markup Language* ou Linguagem de Marcação de Hipertexto

HTTP - *Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto

IAS – *Internet Authentication Service* ou Serviço de Autenticação da Internet

ICP – Infra-estrutura de Chave Pública

ID – *Identification* ou Identificação

IEEE - *Institute of Electrical and Electronics Engineers* ou Instituto de Engenharia Eletro-eletrônica

IETF – *Internet Engineering Task Force*

IIS – *Internet Information Service* ou Serviço de Informação da Internet

IP – *Internet Protocol* ou Protocolo da Internet

LAN – *Local Area Network* ou Redes Locais

MAC – *Media Access Control*

MS-CHAPv2 – *Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2*

NAS – *Network Access Server* ou Servidor de Acesso a Rede

OU – *Organization Unit* ou Unidade Organizacional

PAE – *Port Access Entity* ou Entidade de Porta de Acesso

PEAP – *Protected Extensible Authentication Protocol*

PPP – *Point-to-Point Protocol* ou Protocolo Ponto-a-Ponto

RADIUS – *Remote Authentication Dial-In User Service*

RFC – *Request for Comments*

TLS – *Transport Layer Security*

UDP – *User Datagram Protocol* ou Protocolo de Datagramas de Usuário

VLAN – *Virtual Local Área Network* ou Rede Local Virtual

WAN – *Wide Area Network*

CAPÍTULO 1. INTRODUÇÃO

1.1 MOTIVAÇÃO

Atualmente as empresas estão fortemente dependentes da eficiência das redes de dados, através da qual os seus colaboradores internos e externos acessam e prestam serviços. Toda essa interação que visa o compartilhamento dos mais diversos recursos esconde grandes ameaças para as corporações, já que a dificuldade de controlar individualmente a admissão de usuários na rede cresce na mesma medida que a extensão das suas LANs ou mesmo WANs.

Tal relevância e complexidade levam as empresas a buscarem soluções tecnológicas que tragam para a sua rede os melhores níveis de segurança e disponibilidade aplicadas no mercado. E nessa busca, os primeiros pontos a serem observados são os mecanismos de controle de admissão à rede, pois permite aos administradores reduzir a probabilidade da entrada de diversas ameaças, como vírus e *worms*[1], assim como a possibilidade de pessoas ou grupos não autorizados ganharem acesso a informações controladas ou confidenciais.

Uma tecnologia muito conhecida, que limita o acesso à rede, é a restrição porta a porta, em cada switch, a apenas um endereço físico. Essa abordagem traz grande dificuldade para o gerenciamento de redes grandes, onde qualquer alteração em um dos seus nós, seja troca de placas ou alteração de portas, implica em reconfigurações de portas, onerando sensivelmente os custos para seus administradores. Com o objetivo de facilitar o controle de admissão a rede e ao mesmo tempo ter garantias de acesso, o IEEE (*Institute of Electrical and Electronics Engineers*) criou um novo comitê denominado 802.1x, com a intenção de padronizar a segurança em portas de redes cabeadas e que agrega segurança à rede sem sobrecarregar os seus administradores. Essa padronização tornou-se também aplicável às redes sem-fio.

[1] Tipo de vírus que se dissemina criando cópias funcionais de si mesmo em outros sistemas. A propagação se dá por conexão de rede ou anexos de e-mail.

O padrão 802.1x proporciona confidencialidade, integridade, autenticidade e segurança para a rede interna de uma empresa, pois possibilita a autenticação mútua do cliente e do servidor Radius (*Remote Authentication Dial-In User Service*). Também faz o gerenciamento das chaves de criptografia de forma segura e confiável, além de fazer um controle de admissão, o que reduz os riscos de entrada de ameaças e grupo de pessoas não autorizadas a ganharem acesso à rede, devido à dificuldade em burlar o esquema de autenticação, e a conseguirem um certificado válido para acesso.

A autenticação é essencial para a segurança dos sistemas, ao validar a identificação dos usuários, concedendo-lhes a autorização para o acesso aos recursos. O processo de autenticação é responsável pela garantia de que o usuário é realmente quem ele declara ser e a autorização é a permissão dada direta ou indiretamente pelo sistema para a utilização do mesmo. O controle de acesso lógico, designado ao controle realizado sobre as informações referentes aos recursos computacionais, cuida do acesso aos diversos níveis existentes.

O controle de acesso lógico é responsável pela: (NAKAMURA, 2003)

- Proteção contra modificações ou manipulações não autorizadas de sistemas operacionais e outros sistemas (software), garantindo sua integridade e disponibilidade;

- Garantia da integridade e disponibilidade das informações, ao restringir o número de usuários e processos que acessam determinados tipos de informações;

- Sigilo das informações, que não podem chegar a usuários que não são autorizados.

1.2 OBJETIVOS

O projeto tem como objetivo avaliar o impacto que a utilização do 802.1x tem em uma rede cabeada, quando utilizado como mecanismo de

segurança no controle de acesso. Para isso, é necessário fazer uma validação de *performance* do padrão 802.1x para saber se há degradação e comprometimento no desempenho da rede. Será medido o tempo de resposta à requisição de serviços da rede com e sem a influência da infra-estrutura 802.1x, como por exemplo, o tempo médio para autenticação de um usuário e o desempenho de aplicações HTTP e FTP.

Quando se adota um mecanismo de segurança, há uma inserção de tráfego extra na rede. Esse tráfego pode gerar uma sobrecarga, comprometendo assim, o desempenho de uma rede corporativa. Isso significa que quanto mais robusto for o procedimento de segurança, maior o custo de desempenho, ou seja, quanto maior o processamento computacional do mecanismo de segurança adotado, maior o impacto no tráfego de dados.

Dessa forma, espera-se avaliar qual é a melhor solução para que seja viável a implementação do mecanismo de segurança para que não haja prejuízo no desempenho da rede, como, por exemplo, aumentando o link de conexão ou alterando a configuração dos equipamentos.

Para análise do desempenho, será realizada a simulação de uma LAN preparada com o padrão 802.1x e, com os resultados obtidos, avaliar:

a) Como o mecanismo de segurança 802.1x influencia no desempenho da rede;

b) O impacto da autenticação de um usuário com o mecanismo de segurança 802.1x.

1.3 ESTRUTURA DA MONOGRAFIA

Este trabalho é dividido em seis capítulos principais e estes se subdividirão em tópicos conforme a necessidade de descrição mais detalhada em cada capítulo.

O primeiro capítulo introduz o tema, especificando motivação, objetivos, resultados esperados e a estrutura da monografia.

No capítulo 2 são apresentados os conceitos e referencial teórico que darão base ao desenvolvimento do projeto.

O capítulo 3 mostra as especificações técnicas, o desenvolvimento do projeto e o ambiente a ser analisado.

No capítulo 4 é descrita a demonstração do processo de desenvolvimento, instalação, configuração e implementação do ambiente.

O capítulo 5 apresenta os testes realizados, resultados obtidos e dificuldades enfrentadas.

E no capítulo 6 são apresentadas as conclusões e sugestões de projetos futuros.

CAPÍTULO 2. O PADRÃO 802.1X E SUA UTILIZAÇÃO EM REDES

A transmissão de dados utiliza infra-estrutura de redes baseadas em modelos amplamente estudados, quer seja a transmissão de dados por redes em meios guiados (sinais confinados) ou por meios não guiados. Tanto nas redes cabeadas como nas redes sem fio utilizam-se protocolos para o controle de acesso. Neste capítulo iremos abordar brevemente uma comparação entre estas redes apenas com o intuito de delimitar o escopo do trabalho e o ambiente, em cada caso, no que tange às restrições e abrangência relacionadas ao acesso dos usuários a uma rede que utiliza alguma dessas tecnologias. Em especial, dar-se-á destaque ao padrão 802.1x em redes cabeadas.

As especificações do padrão 802.1x, objeto deste trabalho, são amplamente abordados, assim como os protocolos associados, as topologias, componentes e configurações utilizadas na autenticação de usuários e dispositivos, necessários para garantir a segurança em uma rede, utilizando o conceito de controle de portas.

2.1 REDES CABEADAS X REDES SEM FIO

As redes sem-fio trazem grandes benefícios paras as organizações e usuários, porém trazem também novas vulnerabilidades que podem colocar em risco os negócios da organização. Os dados trocados entre dispositivos sem fio (*Access Point* e notebook, por exemplo) podem ser facilmente interceptados por um intruso com o uso de interceptadores de tráfego de rede (*sniffers*). Se anteriormente um *hacker* tinha de ter pelo menos o acesso a um ponto de rede para ter acesso aos pacotes que trafegam por ela, com as redes sem fio isso não é necessário. As redes locais sem fio (WLAN – *Wireless Local Area Network*), por utilizarem o ar como meio de transmissão, permitem que informações e recursos possam ser acessados e utilizados em qualquer lugar e a qualquer momento. Basta que estejam dentro da área de cobertura para que os pacotes possam ser lidos, modificados ou inseridos novos pacotes.

A interceptação de dados em redes cabeadas é mais complexa, pois o

sinal está confinado no meio de transmissão (fibra ótica, cabo metálico ou cabo coaxial). A seguir, temos um breve comparativo entre redes cabeadas e redes sem fio.

- Redes sem fio:
  - Os limites físicos são amplos e difíceis de definir e restringir;
  - O meio é incontrolável;
  - Qualquer estação dentro da área de abrangência da rede pode ter acesso aos dados;
  - Há necessidade de mecanismos de autenticação, confidencialidade e integridade para tornar a rede equivalente a uma rede com fio.

- Redes cabeadas
  - Os limites físicos da rede estão bem estabelecidos;
  - O meio é controlável;
  - Apenas as estações fisicamente conectadas podem ter acesso à rede.

2.2 PADRÃO IEEE 802.1X

O padrão IEEE 802.1x (*Port-Based Network Access Control*) é uma extensão do pradrão IEEE 802 e é utilizado para proporcionar o controle de acesso a uma determinada rede corporativa, baseando-se em normas para autenticação de usuários e dispositivos de forma que possam ser autorizados a receber conectividade à rede interna e é baseado no controle de portas, podendo ser aplicado a redes com ou sem fio. O ponto fundamental do protocolo é a capacidade de controlar o acesso à rede, autenticando todos os usuários que acessam seus recursos.

Na introdução do documento do padrão IEEE 802.1x, disponível no *web site* do IEEE[2], com algumas omissões: “O controle de acesso a rede baseado

[2] Página oficial do IEEE: www.ieee.org/

em portas faz uso de características de acesso físico da infra-estrutura do padrão IEEE 802 *Local Area Network* (LAN) para fornecer um meio de autenticar e autorizar dispositivos ligados em uma porta LAN [...], e de prevenir acessos àquela porta nos casos em que a autenticação e autorização tenha falhado. [...] Exemplos de portas nas quais o uso de autenticação pode ser desejável incluem as Portas de *MAC Bridges*, [...], e associações entre estações e *Access Point* no IEEE 802.11 *Wireless* LANs." (IEEE Std 802.1x, 2001)

O padrão 802.1x requer um ou mais servidores dedicados e uma infra-estrutura de rede que ofereça suporte ao protocolo.

Para uma implementação efetiva do padrão 802.1x, são necessários alguns componentes como: Switch com suporte a 802.1x, que funcionará como autenticador e fará o controle de portas; Autoridade Certificadora (AC), responsável pela emissão e revogação dos certificados utilizados na validação do acesso a um determinado dispositivo na rede; Controlador de Domínio com base de contas (*Active Directory* – AD) para que as credenciais do usuário possam ser validadas. Faz-se necessário também o uso de um servidor de autenticação. Nas implementações comerciais do 802.1x comumente é utilizado o servidor RADIUS, pela facilidade de instalação e integração com outras soluções de mercado. A função fundamental do servidor RADIUS é autenticar o dispositivo para acesso a rede. Uma vez concedido o acesso, a máquina cliente passa a usufruir de seus recursos.

Conforme mencionado anteriormente o padrão 802.1x realiza controle de portas. Existem dois tipos de portas no 802.1x: as não-controladas e as controladas. As portas não-controladas são aquelas que permitem que o dispositivo conectado a ela se comunique com o restante da rede. Já as portas controladas são aquelas que limitam os endereços da rede que o dispositivo poderá se comunicar. Dessa forma, o 802.1x permite que todos os clientes se conectem nas portas controladas, porém essas portas apenas permitirão tráfego para o servidor de autenticação. Somente depois de autenticado, o cliente poderá ter acesso à porta não-controlada e dessa forma, ganhar o acesso a rede. No 802.1x, as portas não-controladas e controladas são entidades lógicas que podem

existir na mesma porta de rede física.

Em sua estrutura básica, de uma perspectiva física, o 802.1x consiste de três entidades, como pode ser observado na Figura 2.1: Suplicante, Autenticador e o Servidor de Autenticação. Suplicante é o dispositivo que solicita o acesso aos recursos da rede e que necessita ser autenticado (um notebook ou um usuário, por exemplo). O autenticador é o dispositivo que autentica o suplicante e decide se o acesso está liberado ou bloqueado (por exemplo, um Switch ou *Access Point*). O Servidor de Autenticação (RADIUS) fornece o serviço de autenticação ao autenticador e determina, a partir das credenciais apresentadas pelo suplicante, as características do acesso obtido.

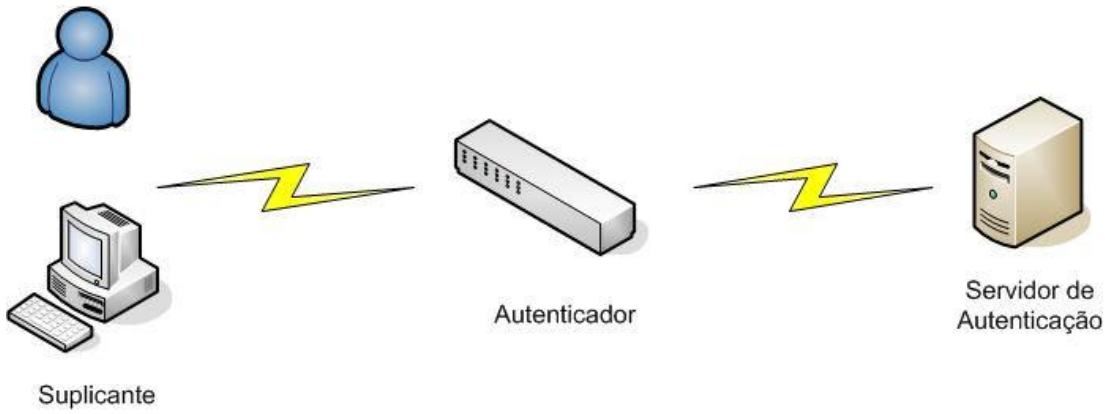

Figura 2.1 – Configuração básica no 802.1x

Essas três entidades executam três conversações diferentes para conduzir uma autenticação. Duas dessas conversações são físicas e podem ser vistas em captura de pacotes. A outra é inteiramente lógica e não pode ser capturada. O suplicante e o autenticador estabelecem uma comunicação física e as informações são transmitidas por meio do EAPOL. O autenticador e o servidor de autenticação também estabelecem uma comunicação física, transmitida por meio do protocolo RADIUS. As conversações físicas suportam de fato a troca de informações de credenciais entre o suplicante e o servidor de autenticação. Esta é a conversação inteiramente lógica e é transmitida pelo uso do EAP. O ponto chave aqui é que o suplicante apenas se comunica com o autenticador. Dessa forma, o autenticador atua como um tradutor entre o suplicante e o servidor de autenticação. Essas três conversações podem ser vistas na Figura 2.2.

A comunicação lógica para informação de autenticação entre o suplicante e o servidor de autenticação é realizada pela utilização do *Extensible Authentication Protocol* (EAP), um protocolo genérico que suporta múltiplos mecanismos de autenticação. O 802.1x define um formato de encapsulamento que permite as mensagens EAP serem transmitidas por um serviço LAN MAC. Este formato de encapsulamento é conhecido como EAP over LAN, ou EAPOL e é usado para todas as comunicações entre o suplicante e o autenticador. O autenticador, mais tarde, encapsula o pacote EAP para que seja submetido ao servidor de autenticação. (AHSON, 2005)

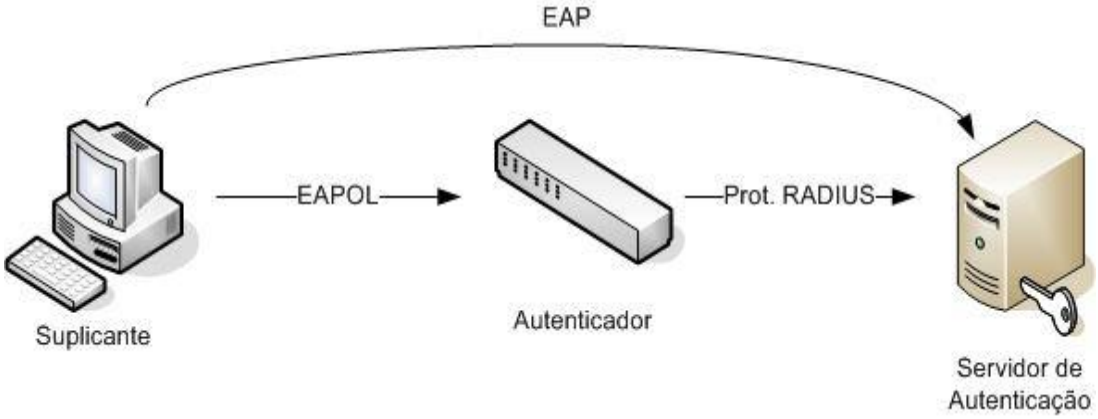

Figura 2.2 – Comunicação entre as entidades

O autenticador situa-se entre o suplicante e o servidor de autenticação. Não há comunicação direta entre as duas entidades. O autenticador será sempre o receptor de qualquer comunicação e sempre irá empacotar o conteúdo da comunicação antes de encaminhá-la. O autenticador normalmente não está apto a traduzir o conteúdo das trocas de credenciais, mas deve estar apto a re-empacotar o conteúdo enviado pelo suplicante ou pelo servidor de autenticação e repassá-lo para o devido receptor. Com isso, o autenticador pode garantir que o suplicante não se comunicará com nenhum outro dispositivo.

O funcionamento do padrão IEEE 802.1x segue a seguinte regra: quando é detectado um novo cliente (suplicante), a porta no switch (autenticador) será ativada e colocada no estado "não autorizado". Nessa situação, apenas o tráfego referente ao protocolo 802.1x é permitido. Outros pacotes, como DHCP ou HTTP, serão bloqueados. Então, o autenticador envia uma requisição de

identidade ao suplicante, que por sua vez, devolve um pacote de resposta contendo as suas credenciais que serão repassadas para o controle de acesso. Caso o usuário seja aceito (autenticado e autorizado), a porta em que está conectado passará ao modo "autorizado" e o tráfego de dados será liberado normalmente, mas se o processo de identificação falhar ou usuário não estiver autorizado, o estado anterior se manterá, limitando a comunicação através daquela porta. Na Figura 2.3 é ilustrado o processo para os casos de usuários autorizados e não autorizados.

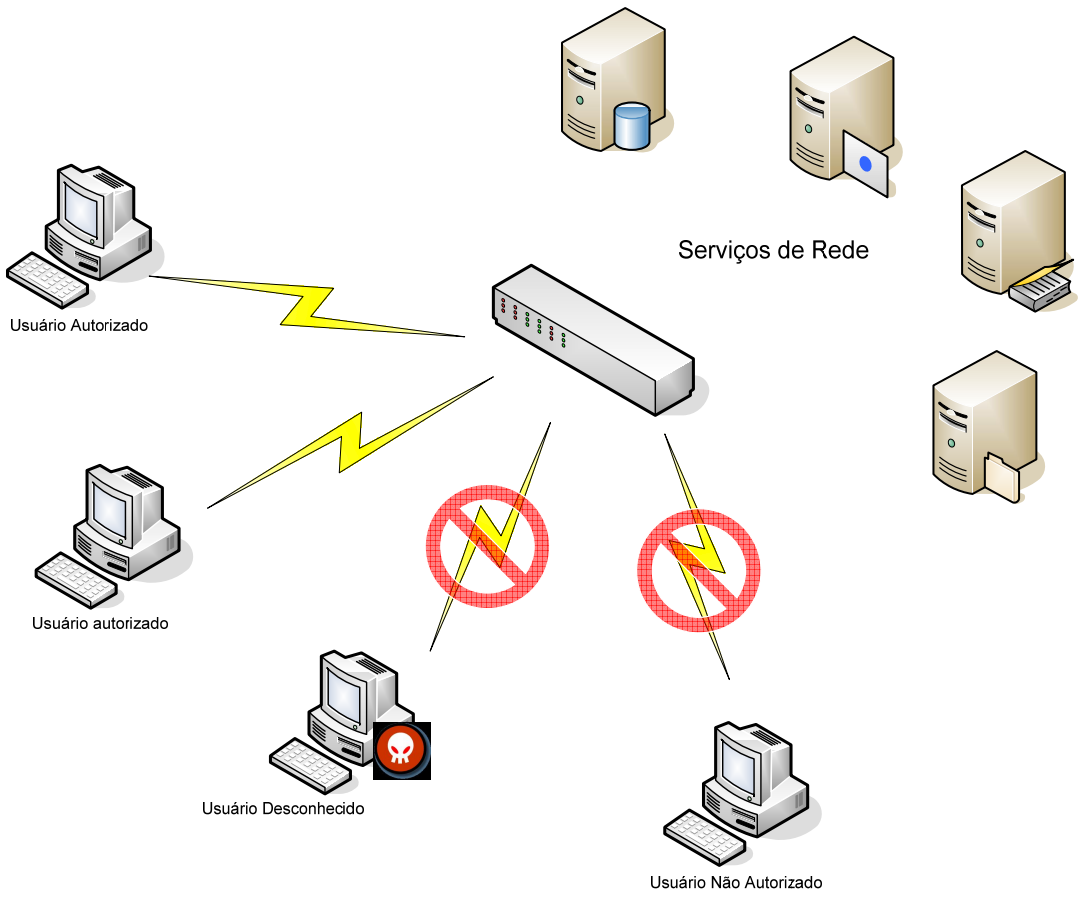

Figura 2.3 – 802.1x controle de acesso a rede

2.3 PROTOCOLOS UTILIZADOS PELO IEEE 802.1X

Conforme citado anteriormente, o 802.1x possui três conversações distintas durante o processo de autenticação. Cada um desses processos utiliza um ou mais protocolos.

Pelo menos cinco encapsulamentos distintos são utilizados em um

processo de autenticação completo. A informação de autenticação é encapsulada em um método EAP, que é encapsulado no EAP, que por sua vez é encapsulado no EAPOL, que, no retorno, é encapsulado em um protocolo 802 da camada 2, como a Ethernet.

Os métodos EAP fornecem uma estrutura em que o suplicante e o servidor de autenticação podem trocar informações. Portanto, o EAP é o protocolo que transporta os dados dos métodos EAP do suplicante para o servidor de autenticação e o encapsulamento EAPOL fornece funcionalidades específicas da LAN que não estão presentes no EAP, sem haver uma comunicação direta entre suplicante e servidor de autenticação. Tudo passa pelo autenticador.

Existem várias soluções de segurança similar às que serão apresentadas neste projeto, como por exemplo o Cisco's Light EAP (LEAP) e o Funk Software's Tunneled Transport Layer Security (EAP-TTLS) que provêem segurança comparável ao PEAP e EAP-TLS, respectivamente. Entretanto, elas prendem a empresa para essas soluções específicas de cada fabricante. (KOMAR, 2004)

2.3.1 Protocolo EAP – Extensible Authentication Protocol

O padrão IEEE 802.1x utiliza o protocolo EAP (*Extensible Authentication Protocol*), definido pela RFC 3748, como uma ferramenta que permite uma grande variedade de mecanismos de autenticação com base em senhas, certificados de chaves públicas ou outras credenciais para fornecer uma autenticação segura das conexões e fazer o transporte das informações de credenciais entre o suplicante e o servidor de autenticação.

O EAP é uma tecnologia de autenticação genérica baseada no protocolo PPP, que foi adaptada para o uso em segmentos de redes locais Ponto-a-Ponto e, posteriormente, para redes convencionais cabeadas e sem-fio. As características das conexões ponto-a-ponto são fundamentais no conceito do EAP. Um simples suplicante conectando em uma porta no autenticador assemelha-se muito aos ambientes PPP.

O 802.1x depende de um servidor RADIUS, de uma autenticação de rede e de um serviço de autorização para verificar as credenciais do cliente na rede. O EAP é utilizado pelo 802.1x como meio de transmitir o pacote de conversação da autenticação entre o suplicante e o servidor de autenticação e gerar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso da rede.

O EAP possui quatro tipos de mensagens: EAP *Request*, EAP *Response*, EAP *Success* e EAP *Failure* e é basicamente um protocolo de autenticação desafio-resposta. A mensagem de *EAP Request* é enviada ao suplicante, indicando o desafio. O Suplicante responde usando a mensagem *EAP Response*. As mensagens EAP *Success* e EAP *Failure* são usadas para notificar ao suplicante o resultado da autenticação.

O EAP é extensível à medida que permite que qualquer mecanismo de autenticação seja encapsulado dentro de mensagens EAP *Request/Response*. Os melhores tipos de EAP normalmente utilizam a criptografia para proteger a conversação de autenticação e podem gerar, dinamicamente, as chaves usadas para a criptografia durante o processo.

O 802.1x usa o EAP para autenticar o cliente para a rede e a rede para o cliente e trocar mensagens durante o processo de autenticação, garantindo que ambos os lados se comuniquem com entidades reconhecidas. Para isso, o EAP utiliza métodos de condução de uma autenticação específica. Os métodos do EAP são definidos por várias maneiras de autenticar, como, por exemplo, por meio de certificados, usuário/senha e alguns métodos de trafegar informação entre o suplicante e o servidor de autenticação.

Existem vários métodos EAP que podem ser utilizados para a autenticação. Para este projeto, será utilizado o método de autenticação EAP-TLS, baseado em certificados digitais.

2.3.1.1 TLS (Transport Layer Security)

O protocolo TLS definido pela RFC 4346 tem como objetivo principal oferecer privacidade e integridade dos dados entre duas aplicações que estejam se comunicando, operando de forma transparente para as camadas superiores. Isso é possível através da autenticação das partes envolvidas e da criptografia dos dados transmitidos entre elas. Proporciona, assim, fácil portabilidade.

O protocolo é composto de duas camadas: a *TLS Record* e *TLS Handshake*. No nível mais baixo, disposto no topo de algum protocolo de transporte confiável, o TLS *Record* fornece conexões seguras que possuem duas propriedades básicas: (http://www.ietf.org/rfc/rfc4346.txt?number=4346)

- A conexão é privada. A criptografia simétrica é usada para encriptação dos dados e as chaves são geradas unicamente para cada conexão.

- A conexão é confiável. O transporte das mensagens inclui a checagem da integridade das mensagens usando um MAC chaveado.

O TLS *Record* é usado para encapsulamento de vários protocolos de níveis mais altos.

O *TLS Handshake*, semelhante ao *TLS Record*, permite que o servidor e o cliente se autentiquem e negociem um algoritmo encriptado e chaves criptografadas antes do protocolo de aplicação transmitir ou receber o primeiro byte de dados. O TLS *Handshake* fornece conexão segura e possui três propriedades básicas:

- A identidade do cliente pode ser autenticada usando criptografia assimétrica ou chave pública.

- A negociação do segredo compartilhado é segura, pois ela não está disponível para curiosos nem para qualquer conexão

autenticada em que o segredo não possa ser obtido.

- A negociação é confiável. Ninguém pode modificar a comunicação de negociação sem ser detectado por uma das partes da comunicação.

O protocolo TLS combina as criptografias simétrica e assimétrica para contornar o problema do segredo pré-estabelecido da simétrica, e o alto gasto computacional da assimétrica. Neste protocolo, a solução consiste em uma etapa inicial de negociação (*handshake*), na qual se utiliza a criptografia assimétrica para autenticar os nós, e combinar uma chave secreta para uso na criptografia simétrica. Terminada esta etapa, o algoritmo por chave pública garante que a negociação da chave secreta foi feita em um canal seguro, e que somente as duas partes a conhecem. Portanto, pode-se trabalhar durante todo o restante da conexão utilizando-se os algoritmos de chave simétrica, tornando a transmissão computacional viável.

A conexão baseada em protocolo TLS possui uma arquitetura do tipo cliente/servidor bem definida, já que a conexão delega papéis distintos às duas partes. O cliente é responsável por iniciar a conexão, e é ele quem propõe a configuração com a qual os nós trabalharão. Mesmo sendo o servidor quem determina os parâmetros que serão realmente utilizados, ele o faz baseado somente nos parâmetros propostos pelo cliente.

2.3.1.2 Protocolo EAP-TLS (EAP – Transport Layer Security)

O EAP-TLS, definido atualmente pela RFC 5216, é um protocolo baseado em certificado e depende da criptografia assimétrica usando o TLS *handshake* e requer tanto o suplicante quanto o autenticador para trocar seus certificados. Como certificados digitais são usados, uma infra-estrutura de chaves públicas, com Autoridade Certificadora e um serviço de diretório são necessários.

O protocolo EAP-TLS é um método robusto em que a troca de mensagens dentro do protocolo TLS fornece autenticação mútua, negociação de credenciais de forma segura, além de integrar determinação mútua de chaves de

criptografia e assinatura entre o cliente e o servidor de autenticação. Após a autenticação e autorização, o servidor de autenticação envia as chaves para o autenticador utilizando a mensagem “RADIUS *Access-Accept*”. Além disso, o EAP-TLS é recomendado para redes 802.1x devido às seguintes características:

- EAP-TLS não requer nenhuma dependência nas credenciais do cliente;
- A autenticação EAP-TLS ocorre de maneira automática, sem intervenção do cliente;
- O switch e a estação deverão possuir certificado emitido por CA (Autoridade Certificadora);
- Garante uma nova chave secreta a cada vez que a estação se associar ao switch;
- O EAP-TLS utiliza certificados e implementa autenticação mútua, provendo um esquema de autenticação mais seguro e proporcionando um forte controle de acesso.

O fluxo de transação com o EAP-TLS é similar aos outros métodos utilizados pelo EAP. O autenticador e o suplicante irão se identificar um ao outro e o autenticador assumirá a função de intermediador depois de estabelecida a sessão com o servidor de autenticação. Nesse ponto, o servidor de autenticação irá conduzir todas as conversações com o suplicante (através do autenticador) usando o protocolo EAP-TLS encapsulado. O primeiro pacote enviado pelo servidor será um “EAP-TLS-Start”. O suplicante irá responder com um pacote EAP-TLS contendo o número da versão TLS, o ID da sessão, um número randômico e uma lista de *cybersuites* suportadas. Esta informação será usada pelo servidor para assegurar que a sessão é correta e para suprir informações adicionais para o suplicante a ser usada durante o processo de autenticação. (BROWN, 2007)

Neste ponto, o suplicante irá validar que está conversando com um legítimo servidor de autenticação. O servidor pode autenticar o suplicante, mas não é absolutamente obrigatório fazê-lo. Uma vez a autenticação bem-sucedida, o servidor irá notificar o suplicante usando uma mensagem “EAP-TLS *Success*” e o suplicante deve reconhecer a mensagem. Quando o servidor recebe a confirmação, ele lança um “EAP-*Success*” que permitirá o autenticador a colocar a porta no estado autorizado. (BROWN, 2007)

A implementação do EAP-TLS requer a utilização de uma infra-estrutura de chaves públicas (ICP) para emitir certificados para clientes e servidores RADIUS. A Figura 2.4 mostra de forma básica o processo de troca de mensagens entre um suplicante e autenticador:

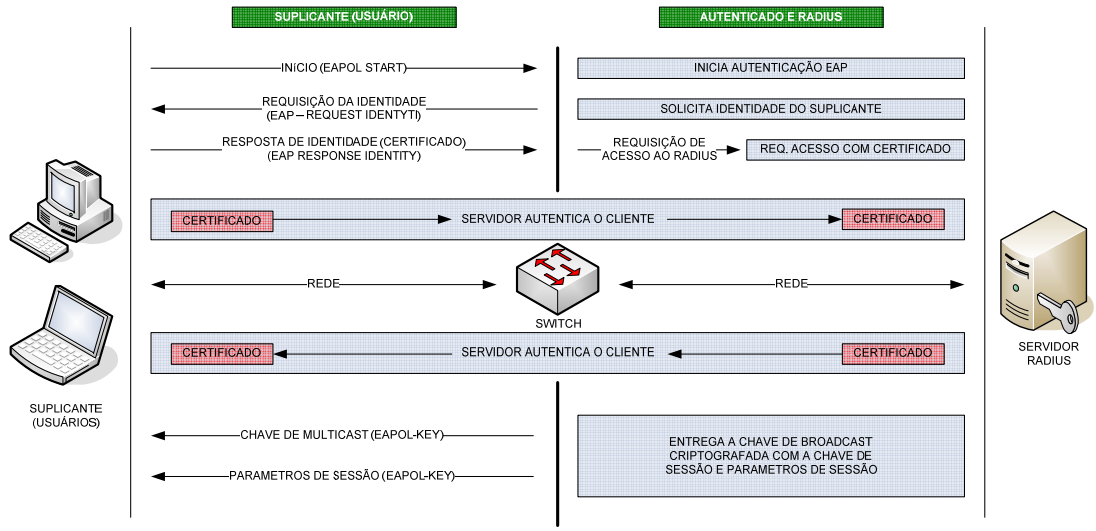

Figura 2.4 – Autenticação 802.1x EAP-TLS

No esquema mencionado, temos uma visão geral de como funciona a solicitação de acesso por parte de um suplicante e de como o autenticador trata esse fluxo com o servidor RADIUS. Temos um caso específico do processo de negociação em uma autorização bem sucedida.

O servidor de autenticação instala uma sessão de segurança da camada de transporte (*Transport Layer Security* - TLS) com o suplicante. O servidor envia seu certificado digital para o servidor de autenticação, que o valida. Dessa forma o cliente e a rede se autenticaram mutuamente, e desde que cada

lado confie no certificado, e que o certificado seja válido, a autenticação é bem sucedida.

Um ambiente implementado com autenticação baseada em certificados, apesar de ser mais robusto, se torna mais complexo e requer um aumento no nível de administração. O uso de certificados também aumenta o número de trocas exigidas entre o suplicante e o servidor de autenticação. Enquanto isso implica relativamente em pequeno impacto na rede, ela aumenta o tempo exigido para autenticação e pode conceber sensível impacto no tempo de aplicações.

Toda esta complexidade em um ambiente implementado com autenticação baseada em certificados será demonstrada neste projeto por meio da análise de desempenho com a utilização de ferramentas de medição de tráfego de redes. Também será verificado o impacto causado e os requisitos para esta implementação.

2.3.2 EAPOL (EAP Over LAN)

O IEEE 802.1x define um padrão criado para encapsular as mensagens *Extensible Authentication Protocol* (EAP) para que elas possam ser tratadas diretamente por um serviço LAN MAC. Esta forma de encapsulação da estrutura EAP é conhecida como EAPOL e é usado apenas em autenticações baseadas em portas entre um autenticador e um suplicante em redes 802.

A comunicação básica consiste em dois tipos de pacotes: o autenticador inicia a autenticação enviando um pacote *Request-Identity* (solicitação de identidade) para o suplicante, que responde com o pacote de resposta para o autenticador. Além de transmitir os pacotes EAP, o EAPOL também fornece funções de controle como *start, logoff* e distribuição de chaves.

O EAPOL possui cinco tipos de pacotes, como pode ser observado na tabela 2.1, abaixo. O mais comum é o Tipo 0, que é usado para transportar as mensagens EAP. Dois outros tipos podem ser usados pelo suplicante para iniciar e terminar uma sessão de autenticação. Os dois tipos restantes são usados para

transportar informações de chaves, normalmente usadas em wireless e alertas de suplicantes não autenticados.

Tabela 2.1 – Tipos de EAPOL (BROWN, 2007)

Tipo	Descrição
0	EAP Data
1	EAPOL-Start
2	EAPOL-Logoff
3	EAPOL-Key
4	EAPOL-Encapsulated-ASF-Alert

EAPOL Tipo 0 significa que o pacote é um frame EAP e não requer processo EAPOL, sendo transmitido simplesmente na camada EAP. Este tipo é normalmente visto nos pedidos de identificação do autenticador ou como resposta do suplicante.

O Tipo 1, EAPOL-*Start*, como pode ser visto na Figura 2.5, é usado para dizer ao autenticador que ele deve iniciar o processo de autenticação. Neste caso, o cliente estará iniciando o processo de autenticação. Isto é necessário porque normalmente o autenticador somente irá fazê-lo quando o estado do link da porta do switch mudar. Neste pacote, é interessante frisar que não há dados EAP encapsulados. Isso ocorre porque não há informação que possa ser enviada em um pacote EAP-*Start*. A intenção deste pacote é simplesmente notificar ao autenticador que existe um suplicante querendo estabelecer uma comunicação e que o processo de autenticação deve começar.

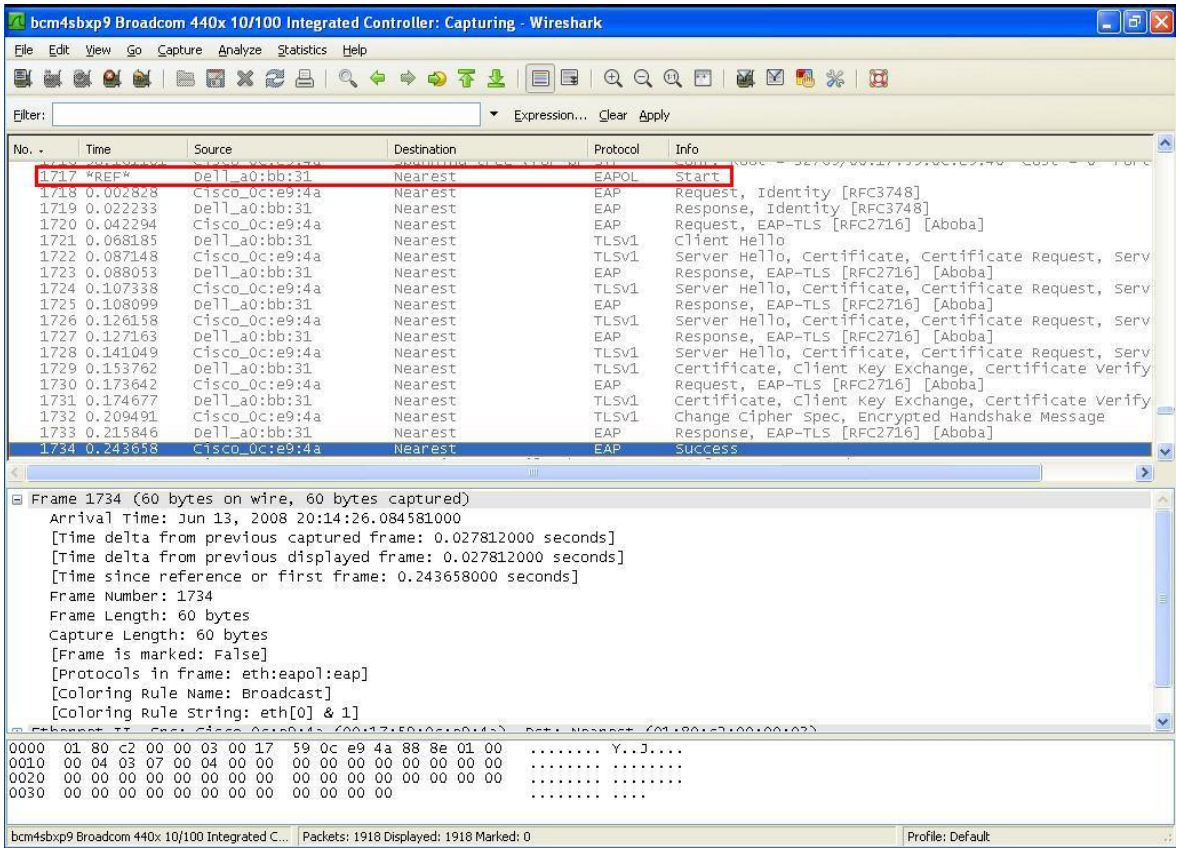

Figura 2.5 – EAPOL-Start

O EAPOL Tipo 2 tem uma função similar. Ele é usado para notificar o autenticador que o suplicante está saindo e retorna a porta para um estado não-autorizado.

O pacote Tipo 3 é usado para troca de informações de chave entre o autenticador e o suplicante para que a encriptação seja possível. Este pacote pode ser emitido tanto pelo suplicante quanto pelo autenticador e é usado para obter ou distribuir informações de chaves.

O pacote Tipo 4 é designado para permitir a ocorrência de alertas sem a exigência de autenticação. A exigência para que o dispositivo ligado participe do 802.1x permanece, mas é permitido declarar uma emergência sem exigir autenticação através do uso deste pacote. Este processo é parecido com a permissão de chamadas para hospitais, polícia e corpo de bombeiros de um telefone pago sem exigir o pagamento antes.

2.3.3 Protocolo PEAP (Protected EAP)

Como o próprio nome sugere, PEAP protege as permutas do EAP. A autenticação PEAP permite a transmissão de outros tipos de EAP em um canal de TLS seguro. Quando o PEAP é usado, o usuário é obrigado a entrar com as credenciais de conta de usuário e senha, que será enviado ao servidor RADIUS.

Este processo de autenticação ocorre em duas partes. A primeira parte é usada para estabelecer um túnel entre o suplicante e o servidor de autenticação, e a segunda parte é a atual autenticação por credenciais. A primeira parte do PEAP é o estabelecimento de um túnel TLS. Assim como o EAP-TLS, o PEAP pode utilizar um certificado para estabelecer o túnel, mas não é obrigado a fazê-lo. Uma vez estabelecido o túnel, um outro método EAP é utilizado para autenticação das credenciais do usuário. (BROWN, 2007)

Funciona basicamente da seguinte forma: o PEAP começa como a maioria dos métodos do 802.1x. O autenticador lança um pedido de identidade e o suplicante responde. O autenticador encaminha para o servidor de autenticação, que responde com um desafio especificando um *Start* PEAP. Neste ponto instala-se um túnel TLS entre o suplicante e o servidor de autenticação usado para o transporte de credenciais. Um método EAP inteiramente diferente é encapsulado dentro do túnel TLS. Um dos métodos mais populares é o MS-CHAPv2 (*Microsoft Challenge Handshake Authentication Protocol version 2*), que será brevemente comentado no tópico 2.3.3.1 a seguir. Pelo fato de estarem confinadas no túnel, as trocas de credenciais não podem ser visualizadas.

Este processo aumenta a complexidade de autenticação assim como a duração e o volume de tráfego exigido, por isso não é uma boa escolha para usuários móveis em ambiente wireless. Porém, é possível para o servidor RADIUS armazenar a sessão TLS criada como primeira parte do processo de autenticação depois que a segunda parte for bem-sucedida. Isto permite que o servidor RADIUS lance um EAP-*Success* imediatamente quando houver uma tentativa de reconexão.

2.3.3.1 Protocolo PEAP-MSCHAPv2

O protocolo PEAP-MSCHAPv2 (*Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2*) faz uso de credenciais com nome de usuário e senha para autenticação na rede e é um protocolo de autenticação mútua no formato desafio-resposta.

O servidor desafia o suplicante e o suplicante desafia o servidor de autenticação. Se uma das respostas ao desafio não for correta, a conexão é rejeitada. O suplicante lança a resposta e o autenticador a encaminha para o servidor de autenticação. O servidor então lança um desafio encriptado e o suplicante envia uma resposta encriptada derivada do uso de credenciais.

Neste ponto, a autenticação pode ter sido bem sucedida ou ter falhado. O servidor de autenticação envia uma falha por diversas razões. A tabela a seguir identifica os códigos de falha:

Tabela 2.2 – Códigos de falha do MS-CHAPv2 (BROWN, 2007)

Código de falha	Descrição
691	Falha de autenticação
646	Horas restritas de logon
647	Conta desabilitada
648	Senha expirada
649	Sem permissão Dial-in
709	Erro na troca de senha

2.4 SERVIDOR DE AUTENTICAÇÃO

Para a implementação do 802.1x no controle de acesso, faz-se necessário o uso de um servidor de autenticação que terá como função principal autenticar o dispositivo para acesso a rede. Existem vários servidores de autenticação, como, por exemplo, RADIUS (*Remote Authentication Dial-In User Service*), FreeRADIUS, DIAMETER ou Tacacs. Para este projeto, será utilizado o RADIUS da Microsoft, pela facilidade de instalação e integração com outras soluções de mercado, além de estar incluso no pacote Windows.

2.4.1 Servidor RADIUS

O IAS (*Internet Authentication Service*) é a implementação da Microsoft

para o servidor RADIUS. O IAS pode ser usado como um servidor RADIUS para qualquer dispositivo, tipicamente para o servidor de acesso a rede (NAS – *Network Access Server*). O RADIUS é um protocolo cliente-servidor que habilita o acesso remoto de equipamentos atuando como cliente Radius que submetem os pedidos de autenticação e conta para o servidor RADIUS. [http://technet.microsoft.com/pt-br/library/bb742380(en-us).aspx, 16/03/2008]

O serviço RADIUS está descrito nas especificações do IETF (*Internet Engineering Task Force*) e é um protocolo padrão usado há mais tempo que o 802.1x. Duas RFCs do IETF, 2865 e 3679, estendem as especificações para o 802.1x. Uma RFC adicional, 3780, identifica elementos particulares, conhecidos como atributos, que são úteis com o 802.1x.

O RADIUS opera no modelo cliente-servidor onde um dispositivo de acesso a rede (switch) passa a informação de autenticação entre um cliente e o servidor e é utilizado para fornecer serviços de AAA (*Authorization, Authentication and Accounting*). Um usuário (suplicante), por intermédio de um autenticador, envia suas credenciais em um pacote RADIUS a um servidor RADIUS que autentica e autoriza o pedido do usuário e devolve uma resposta em outro pacote RADIUS. As etapas de AAA são:

- **Autenticação**: é o processo de identificação. A autenticação é a responsável pela garantia de que o usuário é realmente quem ele declara ser. Compara as credenciais do usuário com as existentes no banco de dados local. Depois de confirmadas, o processo de autorização é iniciado;

- **Autorização**: é o processo que concede certo privilégio baseado nas credenciais e determina se a solicitação de acesso ao recurso será aceita ou não.

- **Gestão de contas**: coleta informações sobre o uso do recurso para análise de tendências, auditoria, cobrança por tempo da sessão ou alocação de custos.

A autenticação fornece a garantia de que a pessoa é quem ela diz ser, mas não diz nada sobre que acesso deve ser concedido. Dessa forma, o processo de garantia de que alguém é quem ele diz ser deve acontecer em uma “porta”. A porta em questão é uma conexão na camada 2 (link de dados). Em ambientes de redes cabeadas, ela é uma porta física em um switch. Em ambientes *wireless*, é uma associação com um *Access Point*.

O servidor RADIUS tem acesso as informações de conta do usuário e pode checar as credenciais de autenticação de acesso remoto. Se as credenciais são autênticas e a tentativa de conexão for autorizada, o servidor RADIUS autoriza o acesso do usuário baseado nas condições específicas e loga a conexão de acesso remoto em uma conta de logs.[http://technet.microsoft.com/pt-br/library/bb742380(en-us).aspx, 16/03/2008]

Os pacotes RADIUS são enviados como mensagens do protocolo UDP (*User Datagram Protocol*). A porta UDP 1812 é utilizada para mensagens de autenticação RADIUS e a porta UDP 1813 para mensagens de gestão de contas RADIUS. Alguns servidores de acesso à rede poderão utilizar a porta UDP 1645 para mensagens de autenticação RADIUS e a porta UDP 1646 para mensagens de gestão de contas RADIUS. Por predefinição, o IAS suporta receber mensagens RADIUS destinadas a ambos os conjuntos de portas UDP. [http://technet.microsoft.com/pt-br/library/bb742380(en-us).aspx#XSLTsection131121120120, 16/03/2008]

2.4.2 Processo e Fluxo de Autenticação do RADIUS

O processo de autenticação do RADIUS começa quando o usuário apresenta as informações de autenticação ao cliente RADIUS. Ao apresentar as credenciais usando o *Challenge Handshake Authentication Protocol* (CHAP), o cliente cria um pacote Radius de pedido de acesso contendo atributos como nome de usuário, senha, ID do cliente e ID da porta que fará o acesso. Este pacote é enviado ao servidor RADIUS e poderá ser reenviado várias vezes caso não haja resposta em um determinado período. Um servidor alternativo também poderá ser usado e priorizado como servidor de autenticação e dessa forma ter os pacotes encaminhados para ele caso o servidor primário falhe ou estiver

inalcançável. Se em um período de 3 segundos o servidor principal não responder, o pacote é automaticamente encaminhado para o servidor com o próximo nível de prioridade.

Após receber o pedido, o pacote é verificado para certificar-se de que foi enviado por um cliente RADIUS válido. Se confirmado e se as assinaturas digitais estiverem habilitadas para o cliente, o servidor RADIUS consulta um banco de dados de usuários para encontrar aquele que combina com o do pedido. A conta do usuário contém uma série de requisitos que devem ser conhecidas para que o acesso seja liberado como, por exemplo, verificação de senha, mas também pode especificar se ao usuário lhe é permitido a ter acesso. Se todas as condições forem aceitas, o servidor RADIUS envia de volta ao cliente um pacote de Acesso Aceito e o acesso é liberado.

Se nenhuma condição para autenticação e autorização for aceita, o servidor RADIUS responde enviando um pacote de Acesso Rejeitado, informando que o pedido é inválido.

Lembrando que o Autenticador estabelece uma comunicação física com o Servidor de Autenticação (RADIUS), enquanto o suplicante e o servidor de Autenticação estabelecem uma comunicação lógica. A Figura 2.6 demonstra esse fluxo.

O RADIUS possui seis tipos de mensagens que são pertinentes ao 802.1x. Quatro delas são usadas pelo servidor para transmissões para o autenticador e duas são usadas pelo autenticador para comunicação com o servidor. O autenticador lançará um pedido para o servidor de autenticação com um *Access-Request* ou um *Accounting-Request*. O servidor de autenticação poderá responder de várias formas, como, por exemplo, com um Accounting-Request, declarando o Sucesso ou Falha com um *Access-Accept* ou *Access-Reject*, ou pode solicitar informação adicional com um *Access-Challenge*. A comunicação mais comum consiste de um *Access-Request* do autenticador, seguido de um *Access-Challenge* do servidor RADIUS e, por fim, um *Access-Accept* ou *Access-Reject* do servidor RADIUS. As seis mensagens para os

códigos que são pertinentes a autenticação no 802.1x estão descritas na Tabela 2.3.

Tabela 2.3 – Códigos e mensagens do RADIUS (BROWN, 2007)

Código	Descrição
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

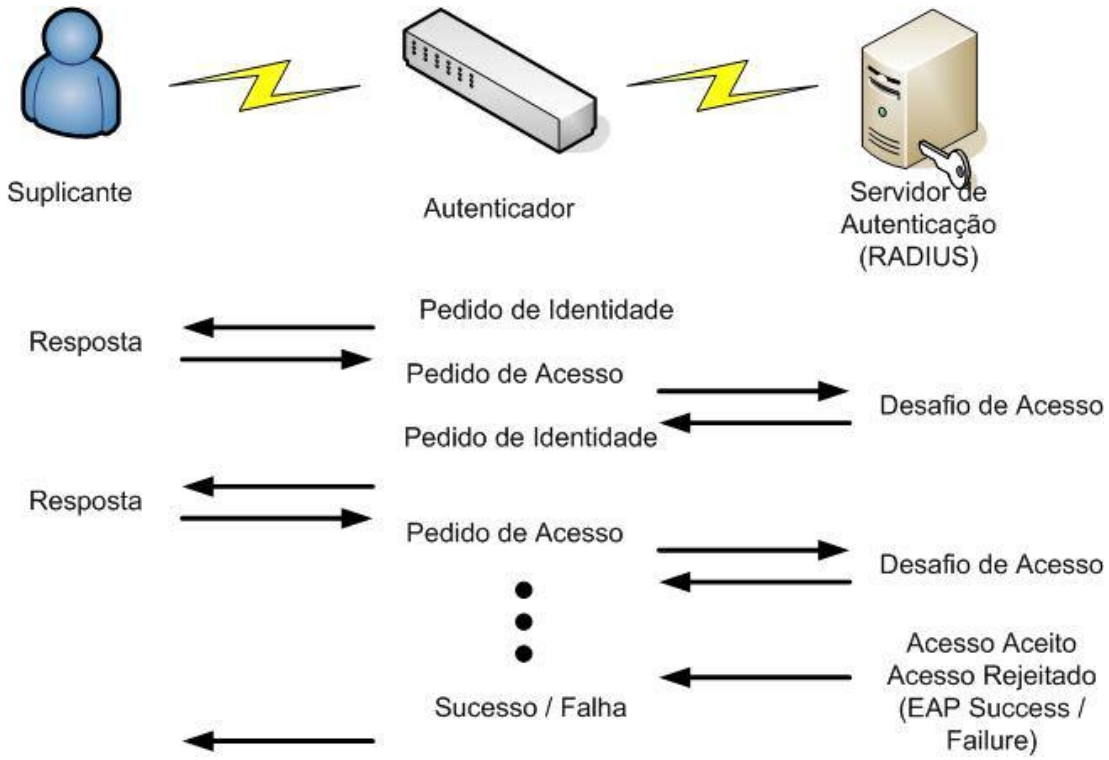

Figura 2.6 – Fluxo de comunicação do RADIUS

2.5 CONTROLE DE ACESSO NO SWITCH

O switch faz o controle do acesso físico à rede baseado no status da autenticação do cliente. Ele atua como intermediário entre um cliente e o servidor de autenticação, solicitando informação de identidade do cliente, verificando esta informação com o servidor de autenticação e transmitindo uma resposta ao cliente. O switch inclui um cliente RADIUS, que é responsável pelo encapsulamento e desencapsulamento do EAP e interage com o servidor de autenticação.

O switch ou o cliente podem iniciar a autenticação. O switch inicia a autenticação quando o link muda de “*down*” para “*up*”. O switch envia um pacote EAP-*request/identity* para o cliente requisitando sua identidade (credenciais). Após o recebimento do pacote, o cliente responde a solicitação com um pacote EAP-*response/identity* contendo suas credenciais. Entretanto, durante a inicialização do sistema, se o cliente não receber um pacote EAP-*request/identity* do switch, o mesmo poderá iniciar a conexão enviando um pacote EAPOL-*Start*, que faz com que o switch requisite a identidade do cliente como descrito acima.

Quando o switch recebe um EAPOL e o transmite ao servidor de autenticação, o cabeçalho Ethernet é retirado e o pacote EAP que fica é reencapsulado no formato RADIUS. O pacote EAP não é modificado ou examinado durante a encapsulação, e o servidor de autenticação deve suportar o EAP dentro do formato do pacote original. Quando o switch recebe o pacote do servidor de autenticação, o cabeçalho do pacote do servidor é removido, deixando o pacote EAP, que é em seguida encapsulado pela ethernet e enviado ao cliente.

2.5.1 Controle de Portas

O estado da porta do switch determina se o cliente terá ou não acesso à rede. A porta inicia no estado **não-autorizado** (também pode ser chamado de estado **controlado**). Enquanto estiver neste estado, a porta desabilita todo o tráfego de entrada e saída, exceto para os protocolos 802.1x. Quando o cliente for autenticado com sucesso, o estado da porta muda para **autorizado** (ou **não-controlado**) e o cliente ganha o acesso à rede. Nas Figuras 2.7 e 2.8 estão ilustrados esse processo.

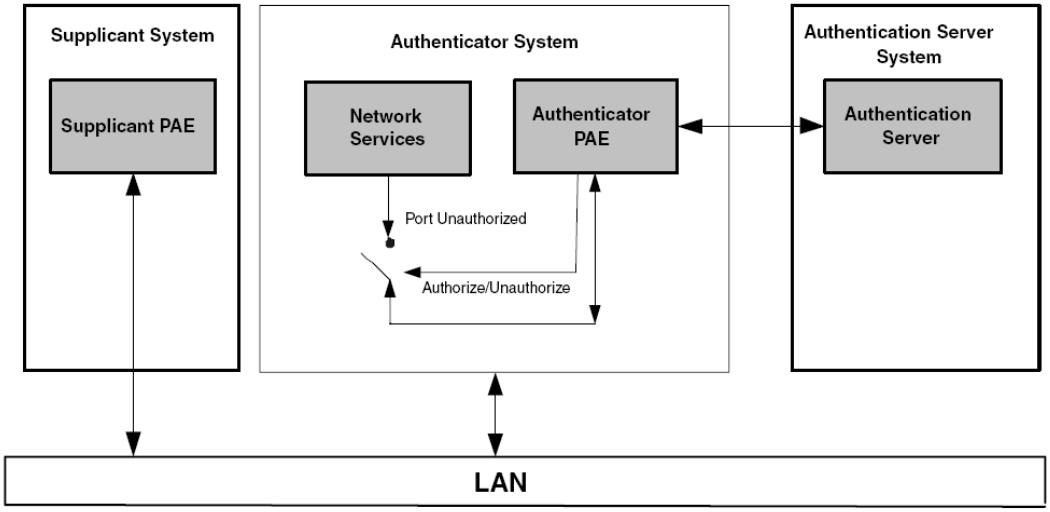

Figura 2.7 – Usuário não-autenticado (AHSON, 2005)

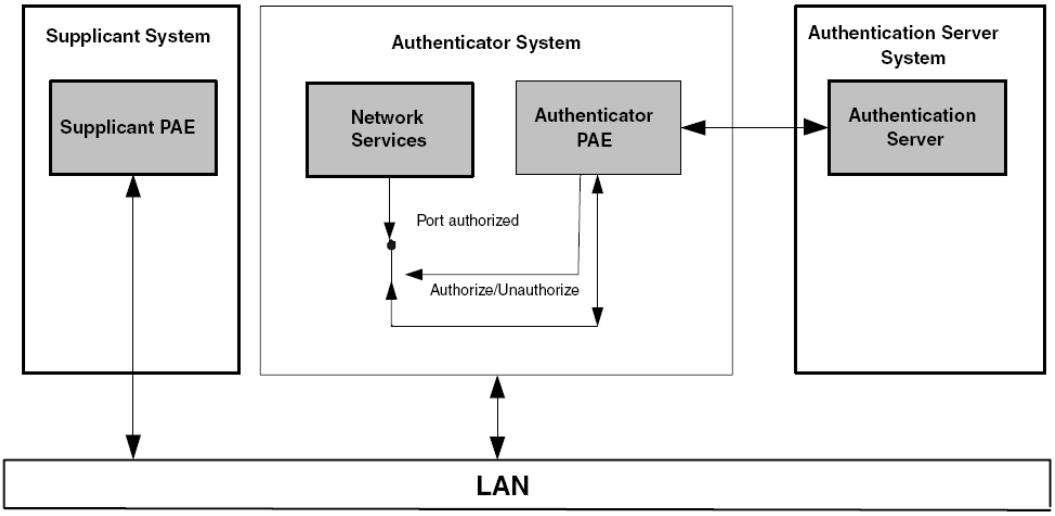

Figura 2.8 – Autenticação bem sucedida (AHSON, 2005)

Se um cliente que não suporta 802.1x estiver conectado em uma porta não-autorizada, o switch irá solicitar a identificação do cliente e, nesta situação, o cliente não irá responder ao pedido. Assim, a porta continuará no estado não-autorizado e o cliente não terá acesso à rede.

Quando um cliente habilitado com o 802.1x se conecta em uma porta que não está com o protocolo 802.1x rodando, o cliente inicia o processo de autenticação enviando o pacote EAPOL-Start. Quando não há resposta, o cliente envia o pedido em um número fixo de vezes. Pelo fato de não receber resposta, o cliente começa a enviar pacotes como se a porta estivesse no estado autorizado. Assim, o cliente poderá se conectar ou não, dependendo do estado da porta,

conforme mostrado abaixo.

O estado da porta pode ser controlado especificando o modo de operação, que pode ser:

- ***Force-authorized***: a autenticação 802.1x é desabilitada e a porta ficará sempre no estado *autorizado* sem que a autenticação seja requerida. A porta envia e recebe o fluxo de rede normalmente, sem autenticação 802.1x do cliente.

- ***Force-unauthorized***: neste caso, a porta permanecerá no estado não-autorizado, mesmo para clientes com credenciais válidas, e irá ignorar todas as tentativas de autenticação. O switch não poderá fornecer serviço de autenticação para o cliente através da interface.

- ***Auto***: a autenticação 802.1x é habilitada e a porta inicia no estado não-autorizado, permitindo apenas pacotes EAPOL enviados e recebidos através da porta. O processo de autenticação começa quando o estado do link da porta muda de "*down*" para "*u*p" ou quando o pacote EAPOL-*Start* é recebido. O switch solicita a identificação do cliente e começa a transmissão de mensagens de autenticação entre o cliente e o servidor de autenticação. Cada cliente tentando acessar a rede é identificado de modo único pelo switch pelo uso do endereço MAC do cliente.

Se o cliente for autenticado com sucesso (recebe um pacote *Accept* do servidor de autenticação), o estado da porta muda para *autorizado* e todos os pacotes do cliente autenticado são permitidos através da porta. Se a autenticação falhar, a porta permanece no estado *não-autorizado*, mas o cliente poderá tentar se autenticar novamente. Se o servidor de autenticação estiver inalcançável, o switch poderá reenviar o pedido. Se não houver resposta do servidor após algumas tentativas, a autenticação falha e o acesso à rede não será permitido.

A porta do switch retorna para o estado *não-autorizado* se o link da porta mudar de "*up*" para "*down*" ou quando o cliente sai do sistema e o switch recebe uma mensagem EAPOL-*Logoff*.

2.5.2 VLANS

Uma VLAN (*Virtual Local Área Network*) é um grupo de estações comunicando-se com uma série de requisitos comuns, independente de sua localização física. Funciona como uma rede logicamente independente dentro de um mesmo switch. Uma VLAN possui os mesmos atributos de uma rede física, mas permite agrupar estações mesmo que não estejam fisicamente situadas no mesmo segmento de rede.

As VLANs fornecem segmentação e flexibilidade organizacional. Elas podem ser projetadas para estabelecer estações que são logicamente segmentadas por funções e aplicações sem observar a localização física dos usuários.

Ao usar uma VLAN, é possível agrupar portas do switch e seus usuários conectados em comunidades logicamente definidas. Neste projeto, será utilizada uma VLAN de dados.

A VLAN de dados será utilizada para dar acesso aos clientes configurados com 802.1x. Todas as requisições que chegarem às portas do switch pedindo autenticação deverão apresentar suas credenciais (certificado ou usuário e senha, dependendo do tipo de autenticação configurada no cliente). Tais credenciais serão usadas para liberar a porta do switch ao qual o cliente está conectado. Esta VLAN somente permitirá acesso à rede mediante a validação das credenciais do usuário.

2.6 INFRA-ESTRUTURA DE CHAVES PÚBLICAS (ICP)

Infra-estrutura de Chave Pública (ICP) refere-se a um processo que utiliza chaves públicas e Certificados Digitais para garantir a segurança do sistema e confirmar a identidade de seus usuários.

Quando a criptografia de chave pública é utilizada, as chaves públicas de usuários ou sistemas podem estar assinadas digitalmente por uma autoridade certificadora (*Certification Authority* – CA) confiável, de modo que a utilização ou publicação falsa dessas chaves pode ser evitada. As chaves públicas assinadas digitalmente por uma autoridade certificadora confiável constituem, assim, os certificados digitais. A autoridade certificadora, os usuários, os sistemas e seus certificados digitais fazem parte de um modelo de confiança essencial em um ambiente cooperativo, necessário para a identificação, autenticação e acesso seguro aos sistemas críticos. (NAKAMURA, 2003)

Em um ambiente heterogêneo, o gerenciamento dos certificados digitais e de todas as suas funções (emissão, revogação e renovação, por exemplo) torna-se extremamente complexo, fazendo com que a infra-estrutura de chave pública seja importante dentro de uma arquitetura de segurança. De fato ela é essencial em um ambiente caracterizado pela complexidade das conexões e pelos diferentes níveis de usuários que têm de ser autenticados e controlados.

Uma ICP baseia-se em um sistema de confiança, no qual duas partes (pessoas ou computadores) confiam mutuamente em uma Autoridade Certificadora para verificar e confirmar a identidade de ambas as partes. Por exemplo, a maioria das pessoas e empresas confia na validade de uma carteira de habilitação de motorista ou em um passaporte. Isto ocorre porque elas confiam na forma pela qual o governo emite estes documentos. Entretanto, uma carteira de estudante é normalmente aceita como prova de sua identificação apenas para a instituição que a emite. O mesmo vale para os Certificados Digitais, ou seja, para que um certificado digital tenha validade no âmbito federal, este deverá ser emitido por uma entidade reconhecida pelos Estados da federação. Diferente disso, o certificado emitido por uma ICP própria, a exemplo de uma autoridade certificadora interna de uma empresa, terá validade somente para aquela empresa que o emitiu.

Com a infra-estrutura de Chave Pública, ambas as partes de uma transação concordam em confiar na autoridade certificadora (CA) que emite seus Certificados Digitais. Normalmente, o aplicativo de software que utiliza seu

Certificado Digital tem algum mecanismo para confiar nas CAs. Por exemplo, dentro da estrutura de ICP usada neste projeto temos o usuário (cliente) que contém uma lista das CAs em que confia. Quando é apresentado ao usuário um Certificado Digital (por exemplo, de um servidor de autenticação RADIUS), ele consulta em sua lista de CAs para aceitar a identidade do RADIUS, se a CA que emitiu o certificado do RADIUS estiver dentre as suas CAs confiáveis o usuário aceita a identificação do servidor RADIUS.

Caso a CA não estiver na lista de CAs confiáveis, o usuário rejeitará aquele servidor como sendo um servidor de autenticação RADIUS. O usuário tem o controle sobre em quais CAs deseja confiar, porém o gerenciamento da confiança é feito pelo componente de *software* (neste exemplo, pelo suplicante).

2.6.1 Autoridade Certificadora (CA)

A CA (*Certification Authority*) é um componente essencial em soluções de infra-estrutura de chaves públicas. É um computador na rede que emite certificados para usuários, computadores, serviços ou dispositivos de rede e que executa as seguintes tarefas (NAKAMURA 2003):

- Verifica a identidade de quem está solicitando um certificado. A CA deve validar a identidade do solicitante antes de emitir um certificado.

- Emitir certificados para os solicitantes. Depois que a identificação do solicitante é validada, a CA emite o certificado solicitado ao usuário, computador, dispositivo ou serviço.

- Gerencia os certificados revogados. A CA publica a CRL (*Certificate Revocation List* – Lista de Certificados Revogados) em intervalos agendados. A CRL contém uma lista com os números dos certificados que foram revogados e o código do motivo pelo qual foram revogados.

A autoridade certificadora tem o papel básico de garantir a correspondência entre a identidade e a chave pública de uma determinada entidade, sabendo que tal chave pública corresponde a uma chave privada que permanece sob guarda exclusiva dessa entidade.

O *Windows Server 2003* fornece duas classes de Autoridades Certificadoras (CA): a corporativa e a autônoma.

A CA corporativa deve, necessariamente, integrar-se com o *Active Directory* (AD). Ela aplica verificações de credenciais aos usuários durante o registro de certificados, ou seja, ela averigua se quem está solicitando o certificado está autorizado a receber o tipo de certificado solicitado.

Diferentemente de uma CA corporativa, uma autoridade de certificação autônoma não exige o uso do AD e, portanto, as credenciais do solicitador do certificado não são verificadas pela autoridade de certificação autônoma. Dessa forma, todas as solicitações de certificados enviadas para a AC autônoma são definidas como pendentes até que o administrador do serviço verifique a identidade do solicitante e aceite a solicitação.

Para este projeto, será utilizada a CA corporativa, isto é, ela será integrada com o AD do domínio e não haverá autoridades certificadoras subordinadas.

2.7 CONTROLADOR DE DOMÍNIO (DC)

O Controlador de Domínio é um servidor com o sistema *Windows Server* e que possui o serviço de diretório *Active Directory* instalado e responde a pedidos de autenticação de segurança.

2.7.1 Serviço de Diretório

O *Active Directory* (AD) é o serviço de diretório do Windows e é um dos principais componentes na implementação do projeto, pois realiza a partir de um controlador de domínio (DC) a identificação de todos os recursos disponíveis em

uma rede mantendo informações sobre gerência de usuários (clientes), grupos, computadores, políticas de grupos (GPO), unidades organizacionais (OU's) e scripts em um banco de dados e torna estes recursos disponíveis para usuários e aplicações.

Para que os usuários possam acessar os recursos disponíveis na rede, estes deverão efetuar o *logon*. Quando o usuário efetua *logon*, o AD verifica se as informações fornecidas pelos usuários são válidas e faz a autenticação, caso essas informações sejam válidas.

Grupos de usuários e máquinas definidos dentro do AD como usuários do Domínio (*Domain Users*) e Computadores do Domínio (*Domain Computer*) serão usados para atribuir permissões no uso da Política de Acesso (política definida dentro do servidor RADIUS para autenticação via PEAP ou EAP-TLS) e permissões na solicitação automática de certificados digitais.

2.7.1.1 GPO – Group Policy Object

A GPO (*Group Policy Object*) é capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede. As vantagens são muitas e podem ser aplicadas em sites, domínios e *organizational units* (OUs).

As políticas de grupo (GPO's) serão criadas com o objetivo de aplicar aos usuários (clientes) os certificados definidos anteriormente como modelo (certificados de usuários e máquinas), execução de um script que fará as modificações no registro das estações de trabalho e neste mesmo script haverá uma ferramenta que modifica as configurações do usuário (cliente) para que o mesmo suporte autenticação 802.1x.

Os aspectos teóricos abordados neste capítulo servirão como base para o desenvolvimento e implementação do projeto, em especial o protocolo EAP-TLS, mecanismo de autenticação que utiliza credenciais baseadas em certificados digitais para garantir o acesso do usuário.

O capítulo seguinte mostrará a topologia e as soluções de hardware e software utilizados para o desenvolvimento do Projeto.

CAPÍTULO 3. INFRA-ESTRUTURA DO PROJETO

Este capítulo trata das especificações e desenvolvimento do projeto.

Quando se adota um mecanismo de segurança, há uma inserção de tráfego extra na rede. Esse tráfego pode gerar uma sobrecarga, comprometendo assim, o desempenho de uma rede corporativa.

A concepção deste projeto está na implementação da transmissão de dados em redes cabeadas utilizando o padrão IEEE 802.1x, assim como na avaliação do impacto causado pela utilização da infra-estrutura de segurança em termos de desempenho e degradação quando comparado com uma rede sem esta infra-estrutura de segurança no controle de acesso baseado em portas.

A seguir serão apresentadas as topologias, especificações e soluções adotadas no desenvolvimento do projeto.

3.1 TOPOLOGIA

O projeto físico será dividido em dois cenários: um sem a infra-estrutura 802.1x implementada e o outro com a segurança que este protocolo confere, implementada.

3.1.1 Cenário I

A Figura 3.1 mostra a estrutura física montada para o Cenário I, onde não é utilizada a infra-estrutura 802.1x.

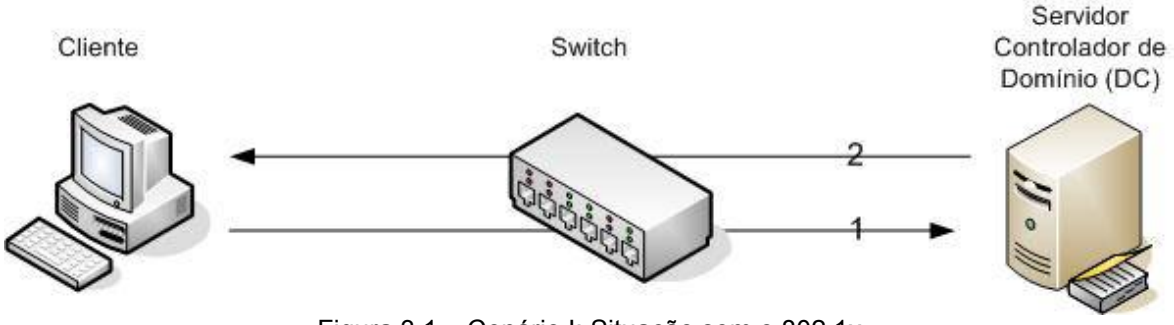

Figura 3.1 – Cenário I: Situação sem o 802.1x

Neste cenário (Figura 3.1), o cliente faz a autenticação no Controlador de Domínio (DC), utilizando credenciais de usuário e senha (1- Figura 3.1). O servidor verifica no *Active Directory* (AD) se as credenciais são válidas e responde ao cliente se foram aceitas ou não (2 – Figura 3.1). Uma vez aceitas, o cliente está apto a utilizar os serviços da rede. Neste caso, o switch não interfere no processo de autenticação.

3.1.2 Cenário II

A Figura 3.2 mostra a estrutura física montada para o Cenário II, com a infra-estrutura 802.1x implementada.

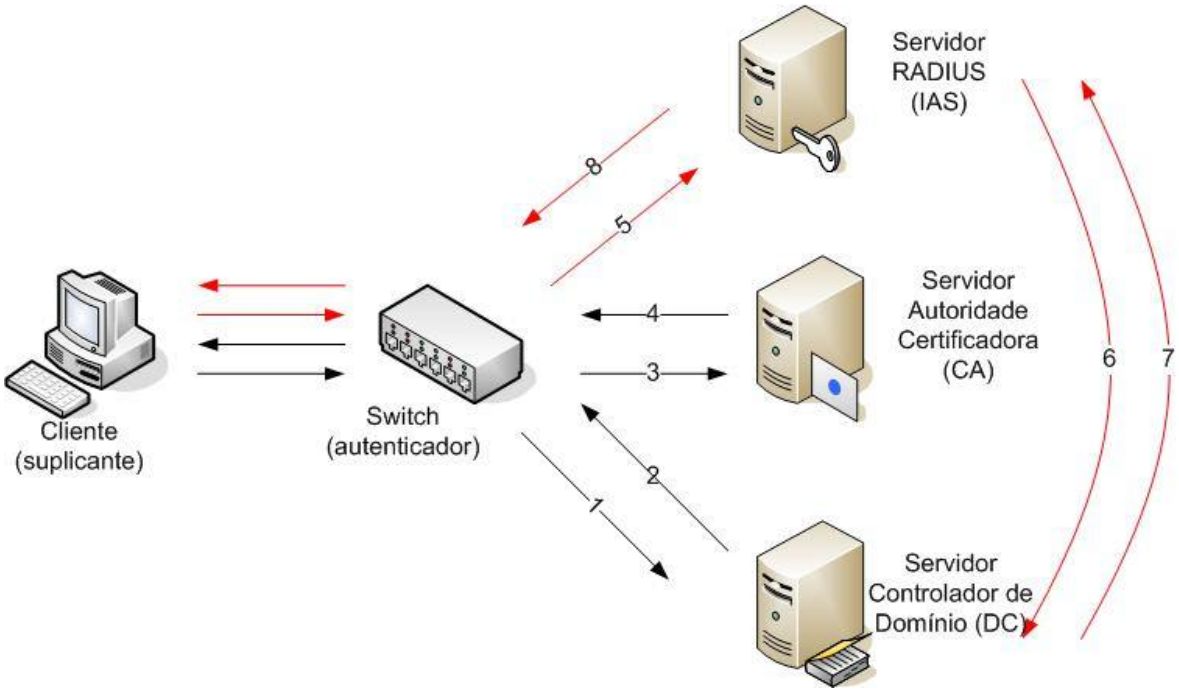

Figura 3.2 – Cenário II: Infra-estrutura 802.1x implementada

Neste cenário (Figura 3.2), um cliente sem as configurações 802.1x fornece suas credenciais (1 - Figura 3.2) com nome de usuário e senha e é autenticado pelo DC. Essa comunicação é realizada em uma porta não-controlada (de acordo com a figura, representada pelas linhas pretas). Uma vez que suas credenciais são aceitas, o cliente recebe uma GPO (*Group Policy*) do servidor DC (2 - Figura 3.2) que fará a solicitação dos certificados de usuário e máquina no servidor Autoridade Certificadora (3 – Figura 3.2). Os certificados digitais são instalados no cliente automaticamente (4 – Figura 3.2) através das configurações de permissionamento e registro automático (*autoenroll*) definidos na CA. De

posse do certificado, o cliente é configurado para realizar autenticação 802.1x (se tornando doravante suplicante). Ao se conectar em uma porta controlada (de acordo com a figura, representada pelas linhas vermelhas), o suplicante envia um pacote EAPOL para o switch que o repassa para o servidor RADIUS (5 - Figura 3.2). O servidor RADIUS confirma a autenticação do usuário no *Active Directory* do DC (6 - Figura 3.2) que o retorna com uma confirmação positiva das credenciais do usuário (7 - Figura 3.2). O RADIUS, por sua vez, verifica as políticas de acesso para aquele cliente. Caso o suplicante atenda todos os requisitos definidos na política, o RADIUS responde ao switch (8 - Figura 3.2) com as informações de liberação e finalmente o cliente obterá acesso a rede.

3.2 HARDWARE

Para a execução dos testes deste projeto, foram utilizados os seguintes *hardwares*:

3.2.1 Solução usuário

Nome do Computador: wilson-note
Endereço IP: 172.16.3.107
Tipo: Notebook Dell Latitude D520
CPU: Intel® Core™2 CPU T5500 1.66GHz
Memória: 2Gb
Disco Rígido: 120Gb
Placa de Rede: Broadcom 440x 10/100 Integrated Controller
Sistema Operacional: Windows XP Professional Edition Service Pack 3

3.2.2 Solução Switch

Para este projeto será utilizado o switch *Cisco Catalyst 2950* (Figura 3.3) que possui as seguintes características:

- 24 portas 10/100 Mbps
- Processadores ASICS PowerPC 403C
- Backplane de 4.8Gbps
- Taxas de transferência baseadas em pacotes de 64 bytes

- Performance de 3.6 mpps
- 16mb DRAM
- 8mb flash
- 8000 endereços MAC
- Suporte a VLAN
- Suporte a 802.1x

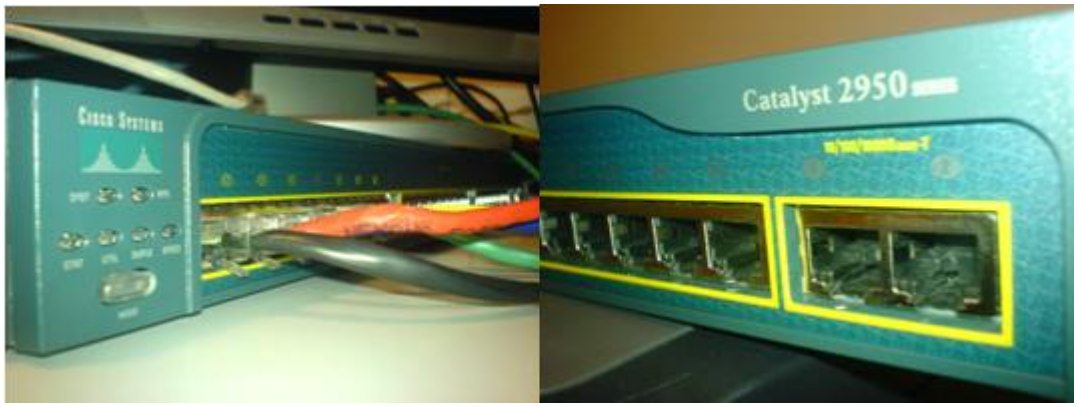

Figura 3.3 – Switch *Cisco Catalyst 2950* utilizado para o Projeto

3.2.3 Solução Servidor Controlador de Domínio

Nome do Computador: SRV-DC

Endereço IP: 172.16.3.236

Tipo: Appliance

CPU: Intel® Xeon™ CPU 2.00GHz

Memória: 1.0Gb

Disco Rígido: 120Gb

Placa de Rede: Intel 8255x-based PCI Ethernet Adapter

Sistema Operacional: Microsoft Windows Server 2003 Enterprise Edition Service Pack 2

3.2.4 Solução Servidor Autoridade Certificadora

Nome do Computador: SRV-CA

Endereço IP: 172.16.3.235

Tipo: Appliance

CPU: Intel® Xeon™ CPU 2.40GHz

Memória: 1Gb

Disco Rígido: 160Gb

Placa de Rede: 3Com Etherlink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)

Sistema Operacional: Microsoft Windows Server 2003 Enterprise Edition Service Pack 2

3.2.5 Solução Servidor Radius

Nome do Computador: SRV-RADIUS

Endereço IP: 172.16.3.234

Tipo: Torre

CPU: Intel® Pentium® 4 2.00GHz

Memória: 2Gb

Disco Rígido: 250Gb

Placa de Rede: Intel® PRO/1000 MT Network Connection

Sistema Operacional: Microsoft Windows Server 2003 Enterprise Edition Service Pack 2

3.3 SOFTWARES E FERRAMENTAS UTILIZADAS

Nesta seção serão apresentados os principais *softwares* aplicados nas soluções: usuário, Servidor Controlador de Domínio, Servidor Autoridade Certificadora e Servidor RADIUS IAS.

3.3.1 Solução Usuário

- Sistema Operacional: *Microsoft Windows XP Professional*
- *Service Pack:* SP3
- Linguagem: Inglês
- Software adicional: *Wireshark*

3.3.1.1 Ferramenta para captura de pacotes

Para a análise de desempenho proposto neste projeto, foi necessária a utilização de uma ferramenta de captura de pacotes, o *Wireshark*[3] (antigo *Ethereal*).

[3] Página oficial: http://www.wireshark.org/

O *Wireshark* é um programa que verifica os pacotes transmitidos pelo dispositivo de comunicação do computador e faz a análise do tráfego de redes e o organiza por protocolos. Ele permite ao usuário monitorar todos os pacotes de informações que estão trafegando pela rede. Este tipo de software também é conhecido como *Sniffer*.

3.3.2 Solução Servidor Controlador de Domínio

Os pré-requisitos de *software* utilizados para estabelecer a infra-estrutura do servidor Controlador de Domínio, definido na seção 2.7 deste projeto, foram os seguintes:

- Sistema Operacional: *Windows Server 2003 Enterprise Edition*
- *Service Pack*: SP2
- Linguagem: Inglês
- Software adicional: *Active Directory*, incluso no próprio pacote do *Windows Server 2003*.
- Software adicional: *Wireshark*

O procedimento de instalação da solução Controlador de Domínio poderá ser visto na seção 4.1 do capítulo de implementação deste projeto.

3.3.3 Solução Servidor Autoridade Certificadora

Os pré-requisitos de *software* utilizados para estabelecer a infra-estrutura da Autoridade Certificadora, definida na seção 2.6.1 deste projeto, foram os seguintes:

- Sistema Operacional: *Windows Server 2003 Enterprise Edition*
- *Service Pack*: SP2
- Linguagem: Inglês
- Software adicional: *Certificate Services*, incluso no próprio pacote do *Windows Server 2003*.

O procedimento de instalação da solução Autoridade Certificadora

poderá ser visto na seção 4.2 do capítulo de implementação deste projeto.

3.3.4 Solução Servidor RADIUS IAS

Os pré-requisitos de *software* utilizados para estabelecer a infra-estrutura de autenticação baseada no RADIUS IAS, definido na seção 2.4.1 deste projeto, são os seguintes:

- Sistema Operacional: *Windows Server 2003 Enterprise Edition*
- *Service Pack*: SP2
- Linguagem: Inglês
- Software adicional: *Internet Authentication Service* (IAS), incluso no próprio pacote do *Windows Server 2003*.
- Software adicional: *Wireshark*

O procedimento de instalação do servidor de autenticação RADIUS IAS poderá ser visto na seção 4.3 do capítulo de implementação deste projeto.

3.4 MEDIDAS DE DESEMPENHO

O tempo de resposta, latência e vazão (*throughput*) foram escolhidos como parâmetros por serem importantes para avaliação e medição do desempenho e por representarem a análise na maioria das aplicações em rede. Eles são definidos assim:

a) **Tempo de resposta**: é o tempo total de transmissão da mensagem entre dois pontos. O tempo de resposta total inclui o tempo de negociação entre o cliente e o servidor, o tempo de efetiva transferência dos dados e o tempo de desconexão, como pode ser visto na Figura 3.4.

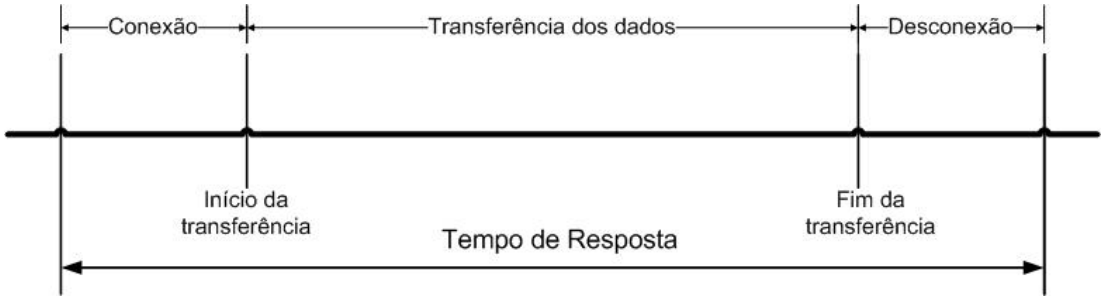

Figura 3.4 – Medição do Tempo de Resposta

b) **Latência**: é a diferença de tempo entre o início de um evento e o momento em que seus efeitos tornam-se perceptíveis, ou seja, é a medida do tempo decorrido entre o início de uma atividade e a sua conclusão, como pode ser visto na Figura 3.5. A latência corresponde ao tempo gasto para uma mensagem atravessar de uma ponta da rede até a outra.

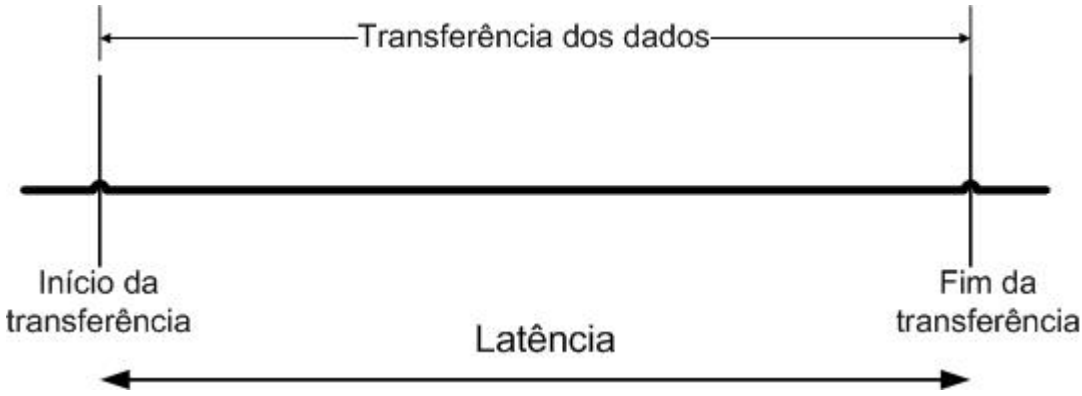

Figura 3.5 – Medição da Latência

c) **Vazão (*throughput*)**: é a taxa de pacotes (bits ou bytes) que podem ser transmitidos na rede em um dado período de tempo. É inversamente proporcional a latência.

3.5 PROCEDIMENTOS PARA MEDIÇÃO

Para cada cenário proposto neste projeto, o experimento será repetido seis vezes, sendo que o primeiro resultado será descartado de forma a evitar a influência de fatores dos sistemas operacionais e de máquinas, como, por exemplo, o processo de armazenamento de dados das páginas em memória

cache[4].

Serão utilizados os protocolos de aplicação FTP (*File Transfer Protocol*) e HTTP (*Hipertext Transfer Protocol*), tendo em vista serem os mais amplamente utilizados. Optou-se pelos protocolos FTP e HTTP, pois representam com mais fidelidade a maioria das aplicações em rede e facilitam a avaliação da sobrecarga inserida pelos mecanismos de segurança no desempenho dos serviços proporcionados pelos referidos protocolos (por exemplo, transmissão de arquivos e acesso a internet).

Para facilitar a medição do tempo de resposta, foi desenvolvido um *script* de forma a automatizar e eliminar a influência do operador na transação FTP. Sem esse *script* o operador poderia inserir um retardo aleatório no início e fim da transação. O texto do *script* encontra-se no Apêndice A deste projeto. O comando para inicializar o script via *prompt* é: *ftp –s:<nome_do_arquivo>*.

Para as requisições HTTP, foi desenvolvida uma página em *html* com os *links* para *download* dos arquivos e armazenada em um servidor *web*.

Os itens acima abordados representam as especificações utilizadas para o desenvolvimento e implementação do Projeto, descrita no capítulo a seguir.

[4] Bloco de memória para o armazenamento temporário de dados que possuem uma grande probabilidade de serem utilizados novamente.

CAPÍTULO 4. IMPLEMENTAÇÃO

Este capítulo descreverá os processos de montagem, instalação e configuração dos Servidores Controlador de Domínio (DC), Autoridade Certificadora (CA) e RADIUS IAS e seus respectivos serviços, bem como do Switch *Cisco Catalyst 2950* e suas conexões, necessárias na implementação da solução tratada neste trabalho.

4.1 MONTAGEM E INSTALAÇÃO DO AMBIENTE

4.1.1 Ambiente sem a infra-estrutura de segurança

De acordo com o exposto no tópico 3.1.1 deste projeto, a montagem do ambiente inicia-se com a instalação do servidor Controlador de Domínio (seção 4.2). Uma vez com o domínio configurado, uma conta de usuário será criada no AD para autenticação do cliente.

Neste cenário, o switch não possuirá nenhuma configuração referente ao 802.1x e não fará o controle de portas. A autenticação funcionará pela utilização de credenciais de usuário e senha definidos no AD, e a solicitação será direta entre cliente e servidor, sem intervenção do switch.

O cliente, um notebook com *Windows XP SP3*, será configurado como membro do domínio "**projetofinal.net**" (seção 4.3.2) e não estará configurado para autenticação 802.1x.

A Figura 4.1 ilustra a montagem básica deste ambiente:

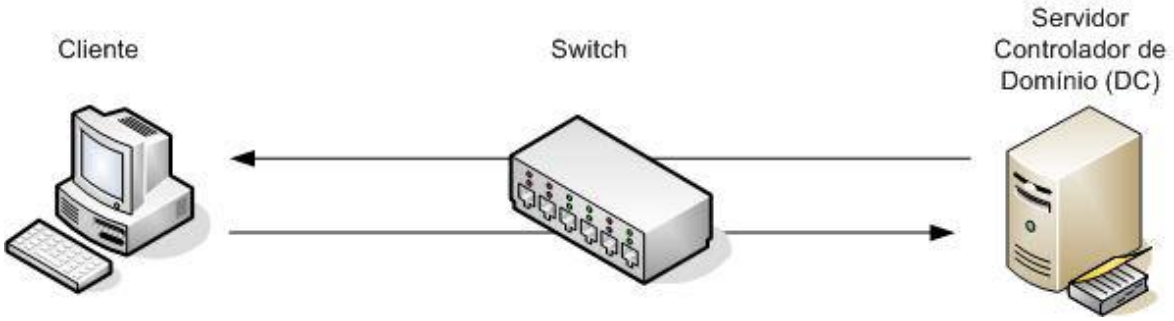

Figura 4.1 – Montagem do ambiente sem a infra-estrutura de segurança

4.1.2 Ambiente com a infra-estrutura de segurança

A montagem do ambiente com a infra-estrutura de segurança, de acordo com o exposto no tópico 3.1.2 deste projeto, inicia-se com a instalação e configuração do servidor Autoridade Certificadora (seção 4.3), onde serão criados os certificados de autenticação.

Em seguida, será feita a instalação e configuração do servidor de autenticação RADIUS IAS (seção 4.4), com a criação das políticas de acesso.

Nesta etapa, o switch *Cisco Catalyst 2950* será configurado para autenticação 802.1x, realizando o controle de portas de acesso a rede. O procedimento de configuração encontra-se no tópico 4.5 deste capítulo. Com a configuração implementada, o switch funcionará como autenticador e fará o intermédio nas comunicações entre suplicante e servidor de autenticação.

Neste ambiente, todos os servidores serão configurados como membro do domínio "**projetofinal.net**". O servidor Controlador de Domínio é o mesmo utilizado no primeiro cenário proposto no projeto.

A Figura 4.2 abaixo ilustra a montagem deste ambiente:

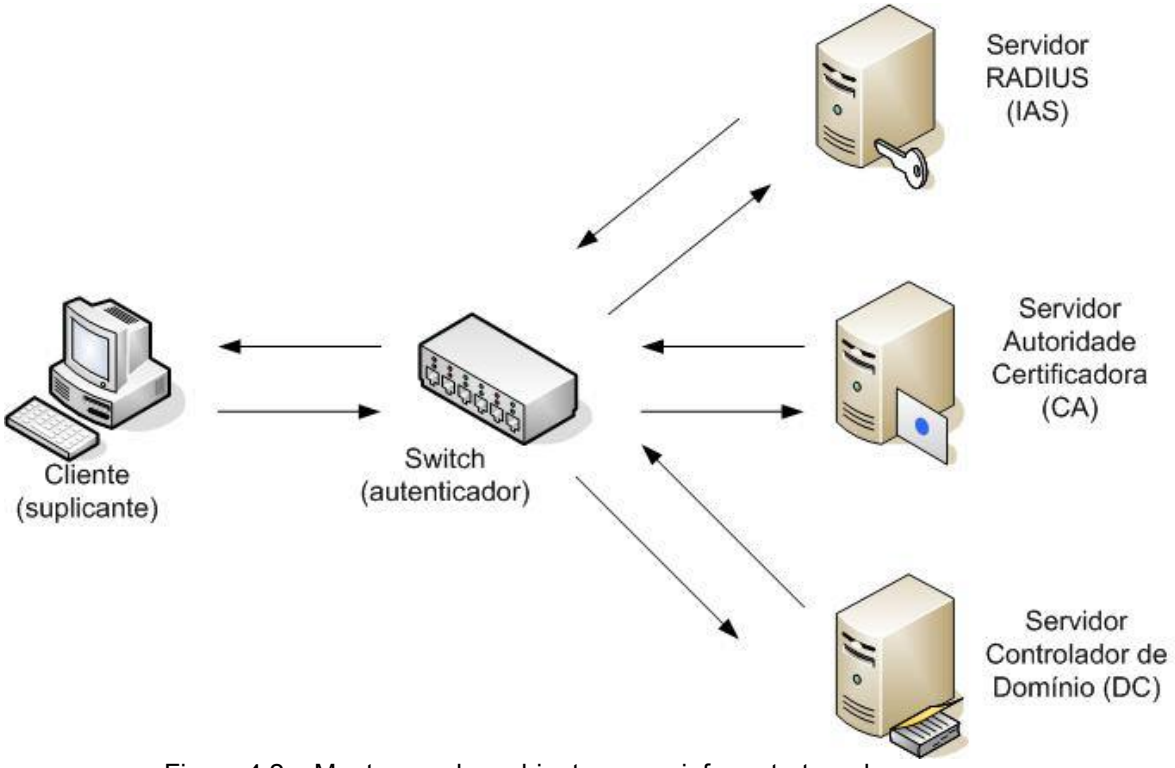

Figura 4.2 – Montagem do ambiente com a infra-estrutura de segurança

Em ambos os cenários descritos acima, os equipamentos estão conectados com cabos de rede direto, com conectores RJ-45.

A seguir, serão apresentados os procedimentos de instalação e configuração dos dispositivos supra citados.

4.2 INSTALAÇÃO DO SERVIDOR CONTROLADOR DE DOMÍNIO (DC)

A seguir serão descritos os procedimentos de instalação do servidor Controlador de Domínio.

O procedimento de instalação do *Microsoft Windows Server 2003*, descrito na subseção 4.2.1 abaixo, será o mesmo para os servidores Autoridade Certificadora (SRV-CA) e RADIUS IAS (SRV-RADIUS).

4.2.1 Instalação do Windows Server 2003

Os passos a seguir fazem parte da recomendação do fabricante do software para se chegar a uma instalação com sucesso. Para a instalação do *Windows Server 2003 Enterprise Edition*, foram escolhidas as seguintes opções:

- Após o boot do sistema no CD Windows Server 2003 Enterprise Edition, escolher a opção "*Set up Windos Now*". Com esta opção, o Windows começará a ser instalado;

- F8 para aceitar os termos da licença;

- O HD de 120b foi particionado, sendo a partição C: de 40Gb e a partição D: de 80Gb; Dessa forma, tem-se a possibilidade de armazenar logs e registros em uma partição diferente da partição em que os arquivos do *Windows* estarão instalados;

- Configuração do teclado ABNT2;

- Para personalizar o software, foi necessário inserir as informações pessoais: nome e organização;

- Inserir a licença do software;

- Em "*Licensing Modes*", a forma de licença escolhida foi a opção padrão "*Per Server* - 5";

- Nome do computador e definição de senha de *Administrator*;

- Horário do sistema definido foi GMT-03:00 – Brasília, com opção para auto-ajustar o horário de verão;

- Em *Networking Settings*, foi escolhida a opção *Custom Settings*. Com isso, foi possível configurar o IP estático, máscara de rede, *gateway*, DNS e Domínio. Os servidores devem ser configurados com IP estático para que não haja alteração no endereço, caso necessitem ser reiniciados, e assim ter que reconfigurar serviços dependentes desses IPs;

Depois disso, o *Windows* finalmente foi instalado e está pronto para ser

utilizado.

4.2.2 Instalação do DC

Para a instalação do Controlador de Domínio, foram necessários seguir os passos descritos abaixo. Este procedimento permite a instalação do serviço de diretório *Active Directory* (AD) e servidor de DNS.

- Clicar no botão "*Start*", clicar em "*Run*", digitar "DCPROMO" e em seguida "OK";

- Surgirá a tela "*Active Directory Installation Wizard*". Clicar em "*Next*" para iniciar a instalação;

- Após revisar a compatibilidade do Sistema Operacional em "*Operating System Compatibility*", clicar em "*Next*";

- Conforme a Figura 4.3, em "*Domain Controller Type*" foi escolhida a opção "*Domain controller for a new domain*". Com esta opção selecionada, será possível a criação de um novo domínio, de acordo com o exposto na seção 2.7 deste Projeto. O servidor será o primeiro controlador de domínio do novo domínio;

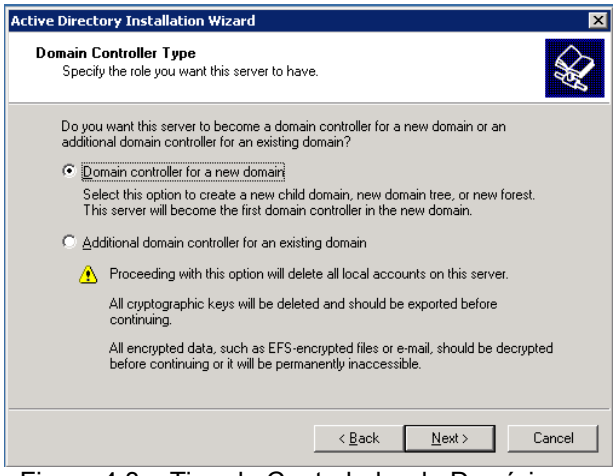

Figura 4.3 – Tipo de Controlador de Domínio

- Na janela mostrada na Figura 4.4, "*Create a New Domain*", foi selecionada a opção "*Domain in a new forest*" pois, como não há outro domínio

configurado, esta opção é selecionada para instalação de um primeiro domínio;

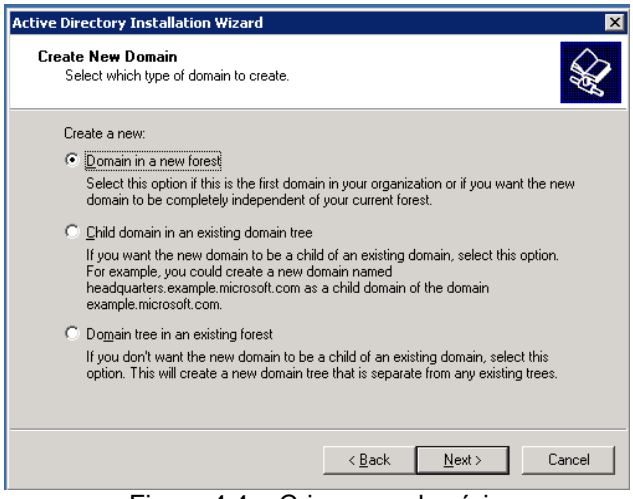

Figura 4.4 – Criar novo domínio

- Na tela "*New Domain Name*" mostrada na Figura 4.5, foi solicitado o nome DNS completo para o novo domínio. O nome escolhido foi "**projetofinal.net**". Essa é a opção mais importante na criação do AD pois, como todo sistema é baseado no DNS, a criação do nome de domínio irá afetar toda a operação da rede;

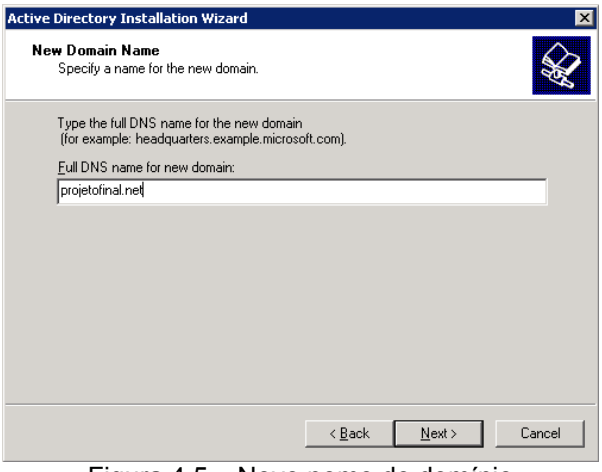

Figura 4.5 – Novo nome de domínio

- Na tela mostrada na Figura 4.6, clicar em "*Next*" para aceitar o "*NetBIOS Domain Name*" **PROJETOFINAL**. Os nomes NetBIOS fornecem compatibilidade para usuários de versões mais antigas do Windows;

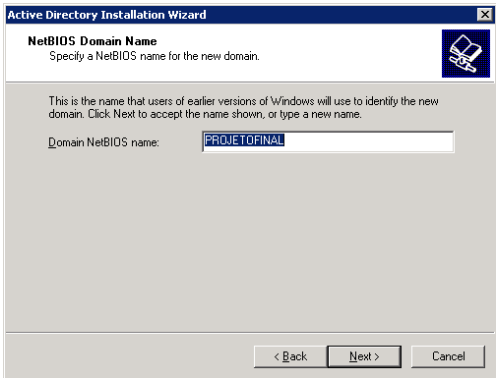

Figura 4.6 – Nome do domínio NetBIOS

- Na tela "*Database and Log Folders*" mostrada na Figura 4.7, devem ser especificados os diretórios para armazenamento do banco de dados e dos logs do *Active Directory*. O banco de dados será armazenado em **C:\WINDOWS\NTDS**, diretório padrão. Os logs do AD serão armazenados na outra partição do HD, em **D:\WINDOWS\NTDS**;

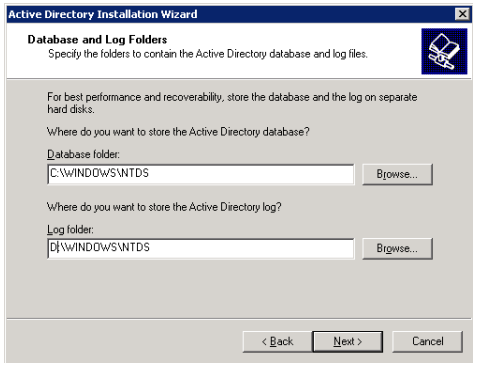

Figura 4.7 – Pastas do banco de dados e log

- Em seguida, na janela "*Shared System Volume*", deve ser especificado o diretório que será compartilhado como volume do sistema. O diretório SYSVOL armazena a cópia do dos arquivos públicos do domínio do servidor, como GPOs e scripts do AD. O conteúdo desta pasta é replicado para todos os controladores de domínio dentro do domínio, caso venham a existir, mas que para a implementação deste projeto não será necessário. Foi mantido o diretório padrão da pasta SYSVOL, **C:\WINDOWS\SYSVOL**;

- A tela seguinte (Figura 4.8), "*DNS Registration Diagnostics*", verifica o suporte DNS ou faz a instalação do DNS no computador. Como não há DNS instalado no computador, foi escolhida a opção "*Install and configure*

the DNS server on this computer", para instalação e configuração do servidor de DNS no computador. Com isso, o computador passará a usar este servidor de DNS como servidor DNS primário;

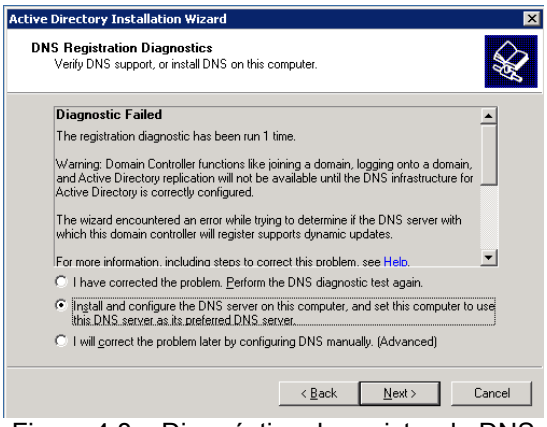

Figura 4.8 – Diagnóstico de registro de DNS

- A tela "*Permissions*" mostrada na Figura 4.9 define as permissões padrões para usuários e grupos. Foi escolhida a opção padrão, "*Permissions compatible only with Windows 2000 or Windows Server 2003*", que permite apenas usuários autenticados a lerem informações no domínio;

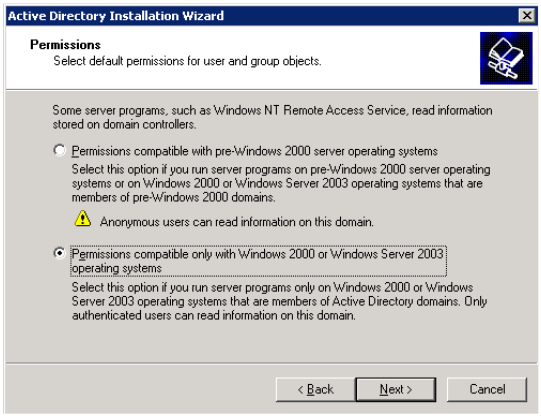

Figura 4.9 – Permissões

- Em seguida, conforme Figura 4.10 abaixo, a tela "*Directory Services Restore Mode Administrator Password*" solicita que seja criada uma senha para ser usada quando o computador for iniciado no modo de restauração dos serviços de diretório. Essa senha não é a mesma do administrador do DC e deve ser usada quando houver problemas no DC ou quando o DC for removido do computador;

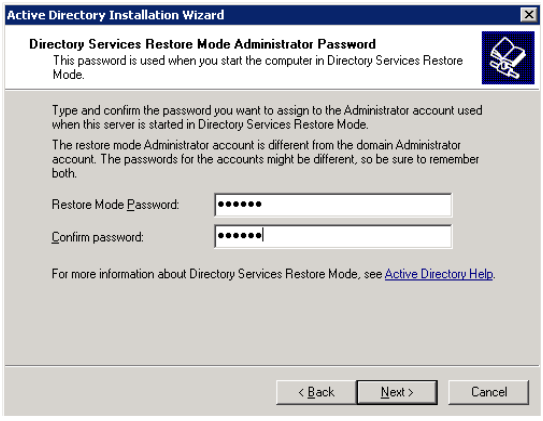

Figura 4.10 – Senha do administrador do modo de restauração dos serviços de diretório

- Em seguida será apresentada uma tela com o resumo das opções de instalação do *Active Directory*, conforme Figura 4.11. Clicar em "*Next*" para iniciar a instalação do AD. Caso seja solicitado, apontar o caminho do CD de instalação do *Windows Server 2003*.

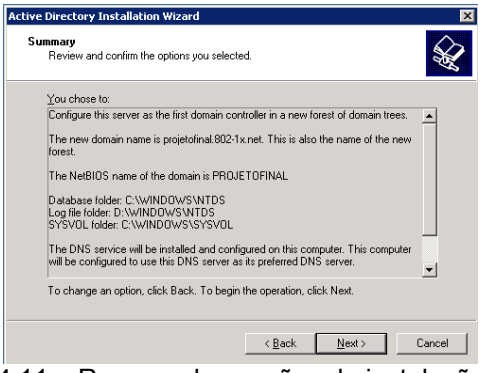

Figura 4.11 – Resumo das opções de instalação do AD

- Finalmente a instalação do servidor Controlador de Domínio, com o serviço de diretório *Active Directory* e *DNS Server* está completa, como pode ser visto na Figura 4.12 abaixo.

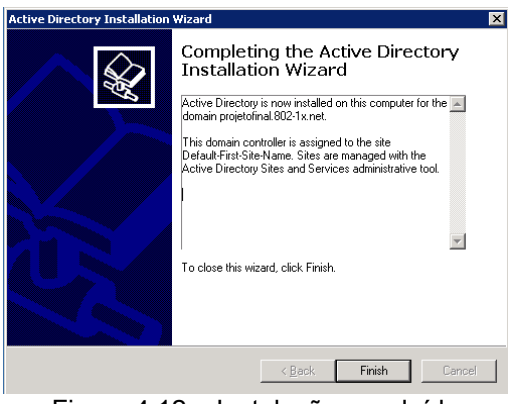

Figura 4.12 – Instalação concluída

4.2.2.1 Configuração da GPO (*Group Policy Object*)

Este procedimento permite a configuração da GPO que fará a emissão automática dos certificados de computador e de usuário.

- A partir do menu Executar, digitar "***dsa.msc***" e em seguida "OK". Surgirá a console de gerenciamento do "*Active Directory Users And Computers*". Sobre o domínio **projetofinal.net**, clicar com o botão direito do mouse e, em seguida, em propriedades;

- Na guia "*Group Policy*" clicar sobre o botão "*New*". O nome dado a política foi **Emissao de Certificados**. A opção "*No Override*" foi marcada, conforme Figura 4.13 abaixo. Em seguida clicar em "*Edit*";

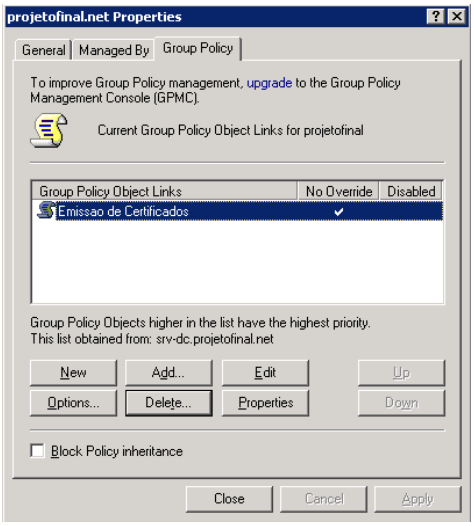

Figura 4.13 – Criação da GPO

- Surgirá a console "*Group Policy Object Editor*". Para emissão do certificado de computador, deve-se expandir o caminho "*Computer Configuration / Windows Settings / Security Settings / Public Key Policies*". Clicar com o botão direito do mouse sobre "*Automatic Certificate Request Settings*", clicar em "*New / Automatic Certificate Request...*", como mostra a Figura 4.14;

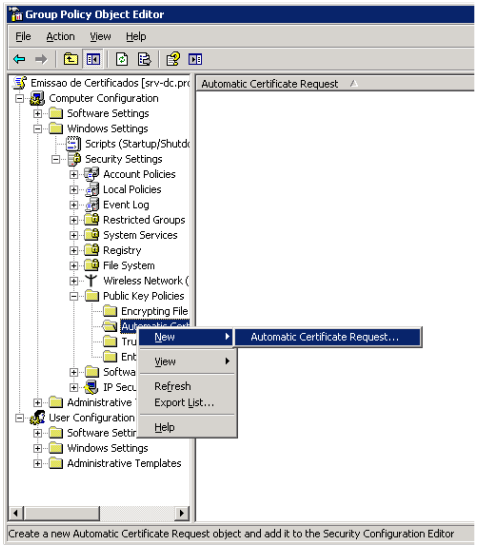

Figura 4.14 – Solicitação de Certificado Automático

- Surgirá o "*Wizard*" para a solicitação automática de certificado. Clicar em "*Next*";

- Na janela "*Certificate Template*" que aparecerá, a opção de modelo de certificado "*Computer*" deve ser marcada, como mostra a Figura 4.15;

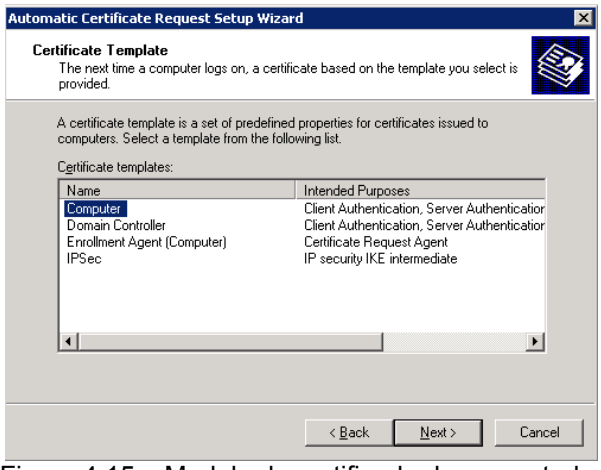

Figura 4.15 – Modelo de certificado de computador

- Clicar em "*Finish*" para concluir a solicitação de certificado de computador. Após finalizar o *Wizard*, verificar que o certificado de computador foi importado com sucesso, como mostra a Figura 4.16.

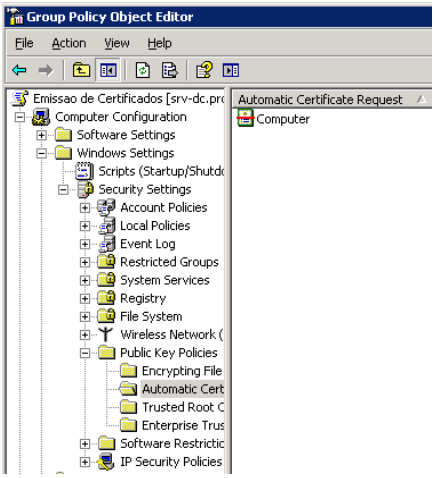

Figura 4.16 – Certificado importado

- Após confirmado, expandir a guia "*User Configuration / Windows Settings / Security Settings*" para inserir a solicitação de certificado de usuário. Clicar em "*Public Key Policy*" e, em seguida, duplo clique sobre a opção "*Autoenrollment Settings*". As opções "*Enroll certificates automatically*","*Renew expired certificates, update...*" e "*Update certificates that use certificate templates*" deverão ser marcadas, como mostra a Figura 4.17. Clicar em "OK" para concluir a GPO.

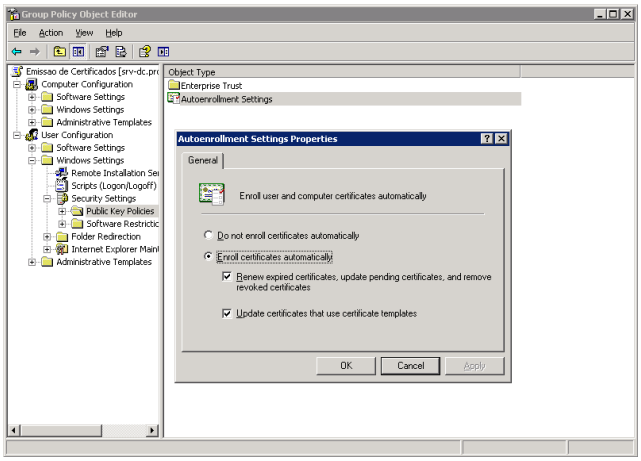

Figura 4.17 – Solicitação de certificado de usuário

4.3 INSTALAÇÃO DO SERVIDOR AUTORIDADE CERTIFICADORA (CA)

Para a instalação e configuração do servidor Autoridade Certificadora (SRV-CA), foram necessários, além da instalação do *Windows Server 2003*, seguir os seguintes passos:

4.3.1 Procedimento de Instalação do IIS (*Internet Information Services*)

Ter o Serviço de Informação da Internet (IIS) instalado é requisito para o sucesso na instalação da Autoridade Certificadora (CA) e do servidor RADIUS IAS.

O IIS é um servidor *Web* que fornece alta confiabilidade, gerenciamento e infra-estrutura de aplicações web para todas as versões do *Windows Server 2003*, ajudando a aumentar a organização de web sites e disponibilidade de aplicações com baixo custo de administração de sistemas.

Para a instalação do IIS do Windows, tanto no servidor Autoridade Certificadora (CA) quanto no RADIUS IAS, foram seguidos os seguintes procedimentos:

- No Painel de Controles, duplo clique em “Adicionar ou Remover Programas”;

- Clicar em “Adicionar/Remover Componentes do *Windows*”. Com este assistente, é possível adicionar componentes do *Windows* que não foram instalados durante a instalação original ou remover componentes que não sejam mais necessários;

- Na lista de componentes, clicar em “*Application Server*” e, em seguida, clicar em “detalhes”;

- Na lista de subcomponentes de *Application Server*, clicar em “*Internet Information Service*”;

- Clicar em “OK” e em seguida, “*Next*” para iniciar a instalação do IIS;

- Durante a instalação, poderá ser solicitado o CD do *Windows Server 2003* caso o sistema não encontre no HD os arquivos necessários para a instalação de novos componentes. Apontar o caminho para finalizar a

instalação.

4.3.2 Procedimento de Instalação da CA

Este procedimento permite a instalação da Autoridade Certificadora da *Microsoft*. As informações preliminares fornecidas durante a instalação, como o nome da CA, não poderão ser alteradas depois que a instalação da autoridade de certificação for concluída.

- A instalação desta parte inicia-se com a escolha em Painel de Controle, da opção "*Add or Remove Programs*" e, em seguida, a opção "*Add/Remove Windows Components*;

- Na janela assistente de componentes do *Windows*, selecionar "*Certificates Services"* (serviços de certificado) e clicar em "*Next"*, conforme Figura 4.18 abaixo;

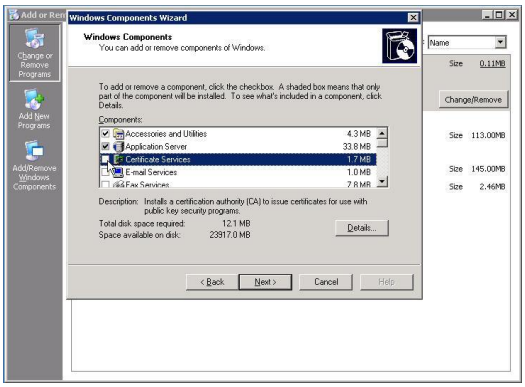

Figura 4.18 – Componentes do *Windows*

- Aparecerá uma caixa de diálogo dizendo que o computador não deve ser renomeado uma vez que o *Windows Certificate Services* estiver instalado, pois as informações referentes a CA que está sendo implementada dependem dessa informação. Caso a informação seja alterada, o certificado emitido por esta CA perderá a validade. Clicar em *Yes* para fechar o aviso e em seguida em "*Next*" para prosseguir;

- Nesta etapa, conforme Figura 4.19, deve ser informado o tipo de CA que será criada. De acordo com a seção 2.6.1 deste projeto, a CA utilizada será

a corporativa (*enterprise*). No campo *CA Type*, clicar em “Enterprise root CA” e marcar a opção “*Use custom settings to generate the key pair and CA certificate*”. Clicar em “*Next*” para prosseguir;

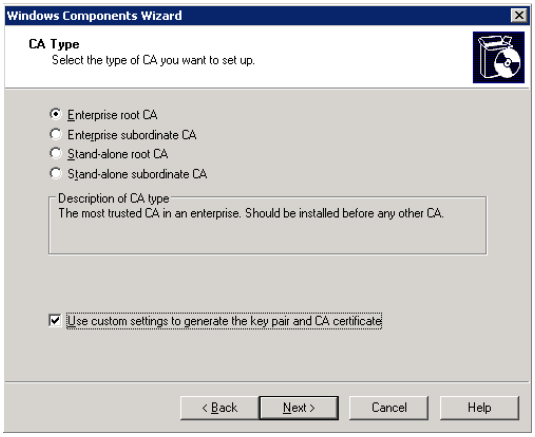

Figura 4.19 – Tipo de CA

- Neste ponto, serão definidas as configurações para a geração do par de chaves para a CA. Na janela “*Public and Private Key Pair*”, as opções padrão foram mantidas. O Provedor de Serviço de Criptografia (CSP – *Cryptographic Service Provider*) é o “***Microsoft Strong Cryptographic Provider***”. O algoritmo *hash* é **SHA-**1 e o tamanho do par de chaves mantido em **2048**, conforme mostrado na Figura 4.20. Clicar em “*Next*” para prosseguir;

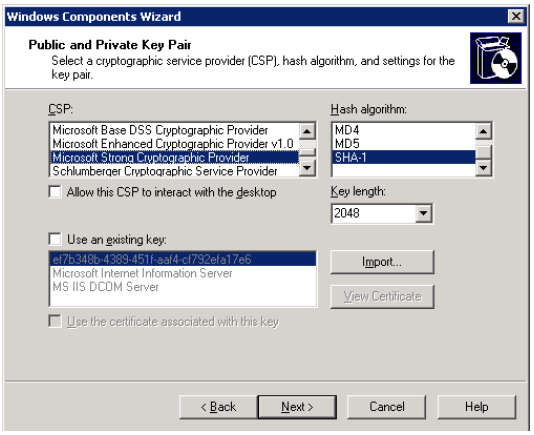

Figura 4.20 – Pares de chaves públicas e privadas

- Na janela que segue abaixo (Figura 4.21), em “*common name for this CA*”, foi escolhido o nome **CA Projeto**. Este nome será registrado no AD. O período de validade foi mantido em 5 anos. O período de validade

escolhido para a CA determinará quando ela perderá a validade e, portanto, quando deverá ser renovada. Clicar em "*Next"* para prosseguir;

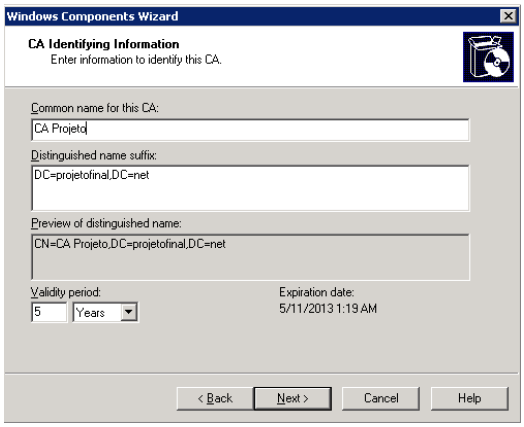

Figura 4.21 – Informações de identificação de autoridade de certificação

- Nesta etapa, deve ser informado o caminho da pasta onde será armazenada a base de dados de certificados e os logs de transações. Foi criada uma pasta chamada CA no disco D:\ para armazenar as informações "*Certificate Database*" e "*Certificate Database Log*". Ficarão gravadas em D:\CA\CertLog. Aparecerá uma caixa de diálogo, como na Figura 4.22, informando que o diretório D:\CA\CertLog será criado. Clicar em "*Yes*" e, em seguida, em "*Next*"**;**

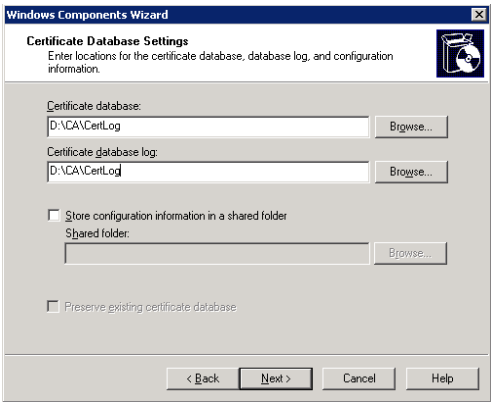

Figura 4.22 – Configurações de banco de dados de certificados

- Neste momento aparece uma mensagem informando que para completar a instalação, o IIS deverá ser parado temporariamente. Clicar em "*Yes*". Durante a instalação, poderá ser solicitado o CD do *Windows Server 2003*. Apontar o caminho para finalizar a instalação.

4.3.2.1 Procedimento de configuração da CA

Os passos descritos a seguir permitem a configuração da Autoridade Certificadora para que os certificados sejam emitidos de forma adequada.

Primeiramente, após a instalação da CA, é necessário fazer a publicação dos certificados revogados. A lista de certificados revogados é um elemento fundamental para o funcionamento da estrutura de Chaves Públicas. Com base na LCR é realizada a verificação dos certificados emitidos e já revogados.

- Para isso, clicar em *Start - Programs - Administrative tools - Certificate Authority*. Expandir a Autoridade Certificadora **CA Projeto** e clicar com o botão direito em "*Revoked Certificates*". Clicar em "*All Tasks - Publish*" para que os certificados revogados sejam publicados, conforme Figura 4.23;

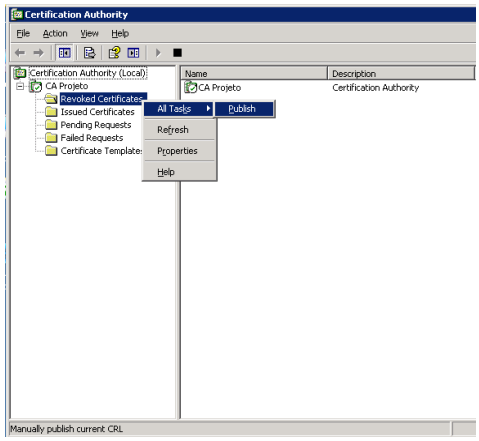

Figura 4.23 – Publicação dos certificados revogados

- Para que uma nova lista de certificados revogados seja emitida, selecionar "*New CRL*" e clicar em OK para finalizar, conforme Figura 4.24;

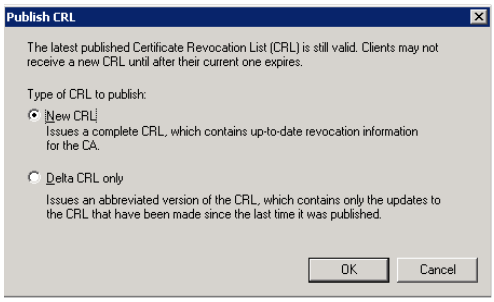

Figura 4.24 – Tipo de CRL a ser publicada

A partir deste ponto, será iniciada a criação dos modelos de certificados que serão utilizados para autenticação. Os modelos de certificado permitem a personalização dos certificados emitidos pelos serviços de certificado, incluindo como os certificados são emitidos e o que eles contêm. Um modelo de certificado é o conjunto de regras e configurações aplicado mediante as solicitações de certificado recebidas.

- Clicar em *Start - Programs - Administrative Tools - Certification Authority*. Em seguida, expandir a Autoridade Certificadora **CA Projeto**, clicar em *Certificate Templates* com o botão direito e clicar em *Manage*, como mostra a Figura 4.25. Também pode ser digitado **certtmplt** em "Executar" no menu "Iniciar";

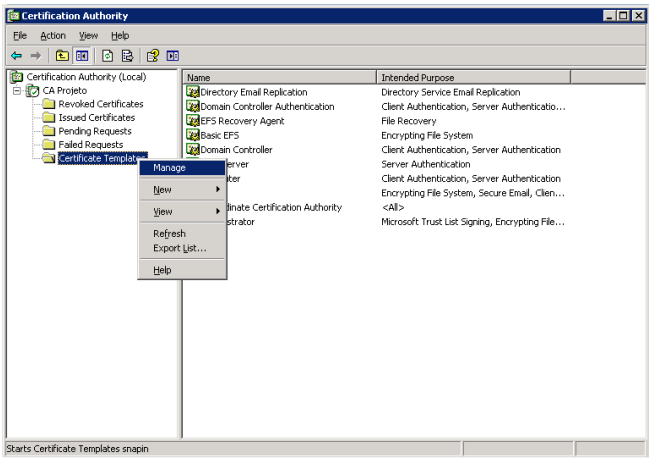

Figura 4.25 – Gerenciando os certificados

É possível criar novos modelos (*templates*) de certificados copiando um modelo existente e usando suas propriedades como padrão para o novo modelo. Para isso, basta copiar o modelo de certificado existente mais próximo da configuração pretendida para o novo modelo para reduzir o trabalho necessário.

- A janela "**certtmpl**" surgirá. Para criar um certificado de usuário, clicar com o botão direito em "*user*", dentro de "*Template Display Name*" e escolher a opção "*Duplicate Template*", conforme Figura 4.26. Esse procedimento foi repetido na criação do **certificado de Computador** e **certificado RADIUS**;

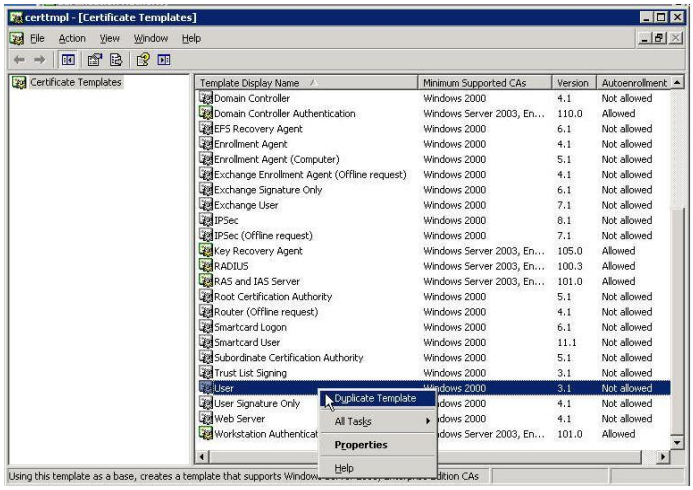

Figura 4.26 – Criação de um novo t*emplate*

- Surgirá a tela "*Properties of new template*" mostrada na Figura 4.27. Na aba "*General*", em *Template Display name*, foi escolhido o nome **usuario** para o novo modelo, pois esse será o certificado emitido a um usuário. O "*Validity Period*" (período de validade) foi alterado para 5 anos e a opção "*Publish certificate in Active Directory*" foi marcada para que o certificado seja publicado no AD;

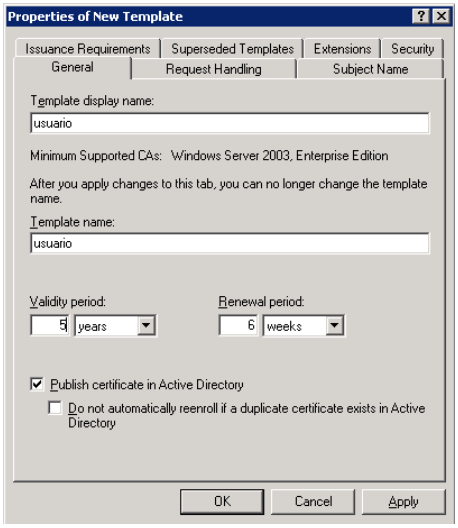

Figura 4.27 – Configuração do *template* de usuário

- Na guia "*Request Handling*", foi desmarcada a opção "*Allow private key to be exported*" para que a chave privada não seja exportada, como mostrado na Figura 4.28;

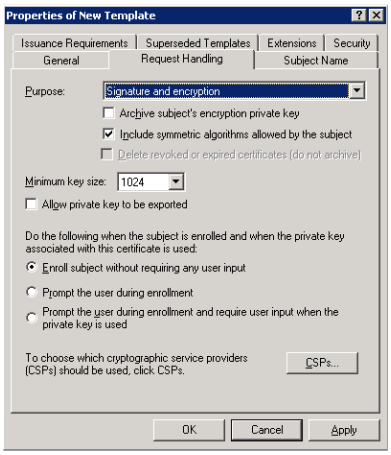

Figura 4.28 – Configuração do *template* de usuário

- A guia "*Subject Name*" permite que sejam adicionados informações no AD e simplifica a administração de certificados. O "*Subject name format*" foi alterado para "***common name***" e a opção "*User principal name (UPN)"* foi marcada, como mostra a Figura 4.29;

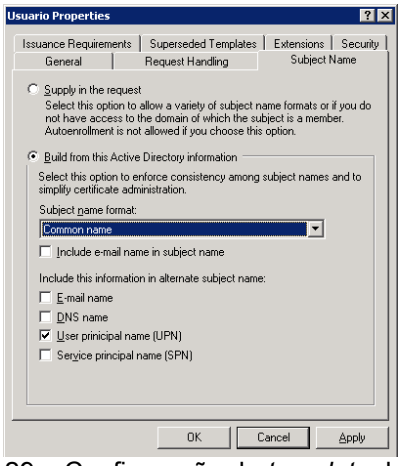

Figura 4.29 – Configuração do *template* de usuário

Nesta etapa, o modelo de certificado será configurado para registro automático do cliente (*autoenroll*). O registro automático é um recurso útil dos serviços de certificado no *Windows XP* e no *Windows Server 2003 Enterprise Edition*. Ele permite que os clientes sejam configurados para registrarem-se automaticamente para certificados, recuperar certificados emitidos e renovar certificados que estão expirando sem precisar de interação do cliente. O cliente não precisa conhecer qualquer operação de certificado, a menos que o modelo de certificado seja configurado para interagir com o cliente. Aqui, será demonstrada a

maneira de modificar o modelo de certificado para que o cliente se registre automaticamente.

- Na guia "*Security*" mostrada na Figura 4.30, será configurado o permissionamento de registro automático do certificado. Os grupos "*Domain users*" e "*Domain Admins*" ficarão com as linhas "*Read*", "*Write*" e "*Enroll*" e "*Autoenroll*" marcadas como *Allow*. Isso permitirá o registro automático do certificado dos usuários que se logarem no domínio. Em seguida, clicar em "OK" para finalizar a configuração do *template* **usuario**;

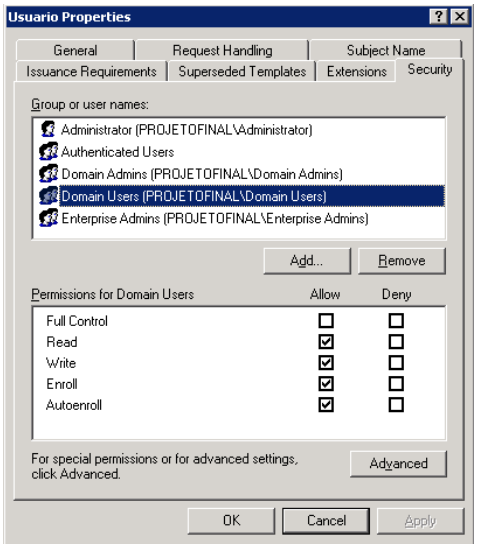

Figura 4.30 – Registro automático do cliente

- Retornará para a janela "certtmpl". Será iniciada criação do modelo de certificado de computador e para isso o modelo "*Workstation Authentication*" foi duplicado;

- Na guia "*General*", em "*Template Display name*", foi escolhido o nome **Certificado de Maquina** para o novo modelo, pois esse será o certificado emitido a um computador. O "*Validity Period*" (período de validade) foi alterado para 5 anos e a opção "*Publish certificate in Active Directory*" foi marcada para que o certificado seja publicado no AD, como pode ser verificado na Figura 4.31;

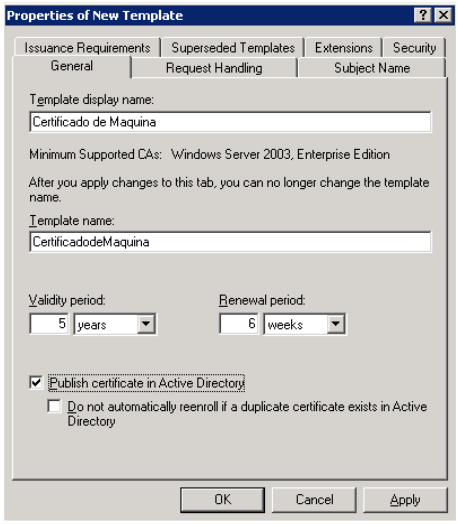

Figura 4.31 – Configuração do *template* de computador

- Na guia "*Subject Name*", o "*Subject name format*" foi alterado para ***common name*** e a opção "*DNS name*" foi marcada, como mostra a Figura 4.32;

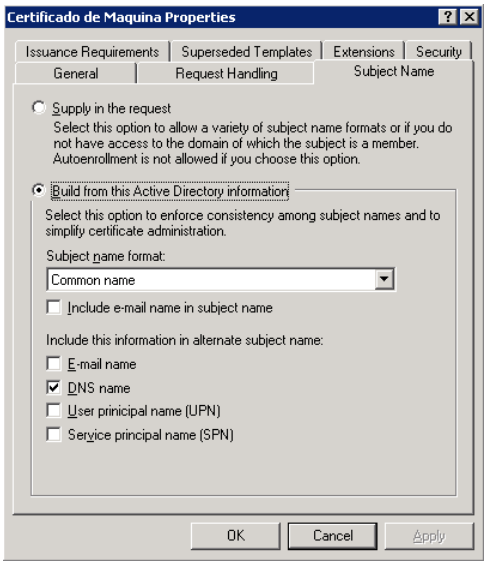

Figura 4.32 – Configuração do *template* de computador

- Na guia "*Security*" mostrada na Figura 4.33, o grupo "*Domain Computers*" ficará com as linhas "*Read*", "*Write*", "*Enroll*" e "*Autoenroll*" marcadas em "*Allow*". Dessa forma, o computador poderá fazer o registro automático do certificado. Em seguida, clicar em "OK" para finalizar a criação do *template* **Certificado de Maquina**;

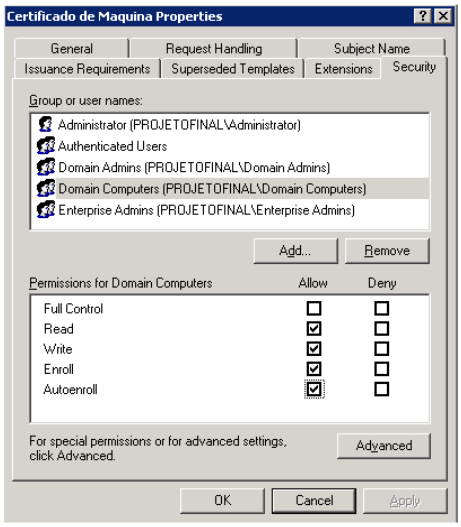

Figura 4.33 – Configuração do *template* de computador

- Retornará para a janela "certtmpl". Será iniciada criação do modelo de certificado RADIUS e para isso o modelo "*RAS and IAS Server*" foi duplicado;

- Na guia "*General*", em "*Template Display name*", foi escolhido o nome **RADIUS** para o novo modelo, pois esse será o certificado emitido ao RADIUS. O "*Validity Period*" (período de validade) foi alterado para 5 anos e a opção "*Publish certificate in Active Directory*" foi marcada para que o certificado seja publicado no AD, como pode ser verificado na Figura 4.34;

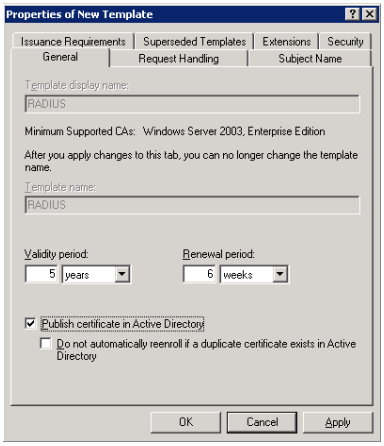

Figura 4.34 – Configuração do *template* RADIUS

- Na guia "*Subject Name*", o "*Subject name format*" foi alterado para ***common name*** e a opção "*DNS name*" foi marcada, como mostra a Figura 4.35;

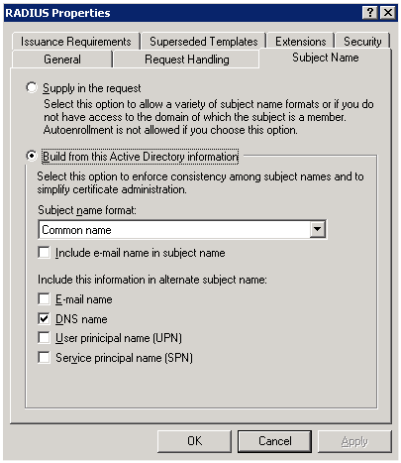

Figura 4.35 – Configuração do *template* RADIUS

- Na guia "*Security*" mostrada na Figura 4.36, o grupo "*Domain Computers*" ficará com as linhas "*Read*" e "*Enroll* marcadas como "*Allow*". Clicar em "OK" para finalizar a criação do *template* de certificado **RADIUS**.

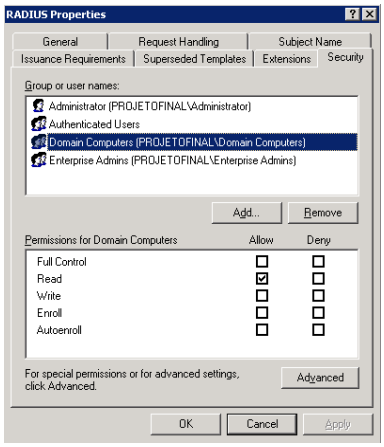

Figura 4.36 – Configuração do *template* RADIUS

- Fechar a janela "certtmpl" para finalizar a criação dos modelos de certificados.

Nesta etapa, a Autoridade Certificadora será configurada para emitir os certificados com base nos modelos criados (**usuário, certificado de máquina e RADIUS**). Para isso, foram seguidos os seguintes passos:

- Dentro da Autoridade de Certificação, clicar com o botão direito sobre "*Certificate Templates*", escolher a opção "*New*" e clicar em "*Certificate*

Template to Issue" conforme Figura 4.37. Isso permitirá que os *templates* de certificados criados possam ser emitidos;

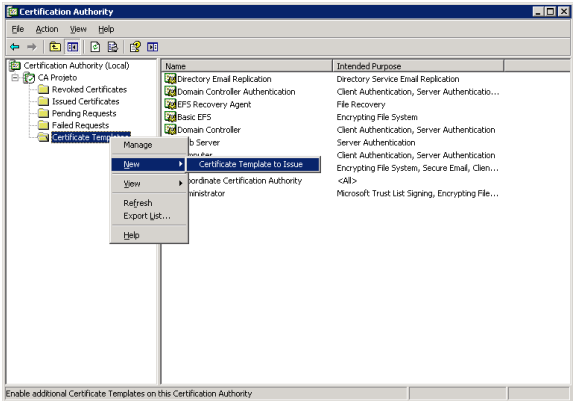

Figura 4.37 – Emissão dos *templates* de certificados

- Na caixa de diálogo "*Enable Certificate Templates*" selecionar os certificados criados "**usuario**", "**Certificado de Maquina**" e "**RADIUS**" para que sejam disponibilizados. Clicar em "OK". No final da criação dos *templates*, os três modelos de certificados selecionados estarão disponíveis no recipiente, como mostra a Figura 4.38.

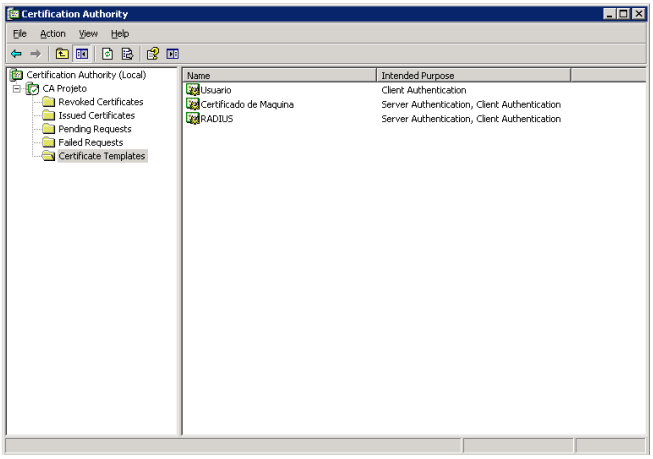

Figura 4.38 – Certificados disponíveis

Nesta etapa, serão configuradas as propriedades da lista de certificados revogados e de auditoria:

- Em "**CA Projeto**", na pasta "*Revoked Certificates*", clicar com o botão direito e selecionar a opção "*Properties*". As configurações de distribuição da lista de certificados revogados (CRL) serão distribuídas de forma

completa a cada 8 dias e de forma parcial (delta) a cada 4 horas, como mostra a Figura 4.39;

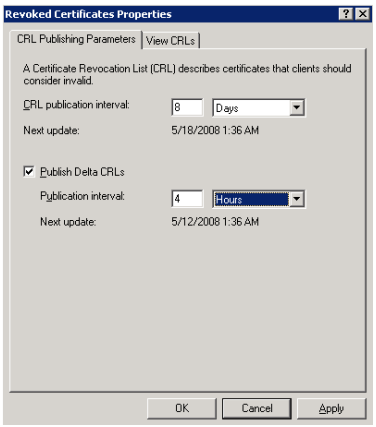

Figura 4.39 – Configuração da CRL

- Na Autoridade Certificadora “CA Projeto”, clicar com o botão direito e selecionar a opção “*Properties*”;

- Na janela seguinte, selecionar a guia “*Auditing*”. Nessa guia foram selecionadas as opções listadas de acordo com a Figura 4.40 abaixo. Esses eventos serão registrados no “*Event Viewer*” como eventos de segurança e devem ser marcadas de acordo com a necessidade de cada ambiente:

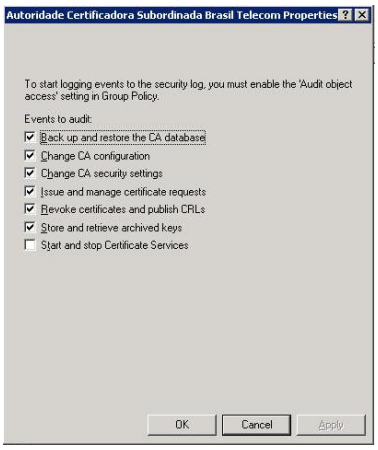

Figura 4.40 – Eventos de segurança para auditoria

4.4 INSTALAÇÃO DO SERVIDOR RADIUS IAS

Para a instalação do servidor RADIUS IAS da Microsoft, foi necessário seguir os seguintes passos:

4.4.1 Procedimento de Instalação do RADIUS IAS (*Internet Authentication Service*)

- A instalação inicia com a escolha no Painel de Controle da opção "*Add or Remove Programs*" e em seguida, com a escolha da opção "*Add/Remove Windows Components*;

- Marcar a opção "*Networking Services*", em seguida clicar no botão "*Details*", conforme Figura 4.41;

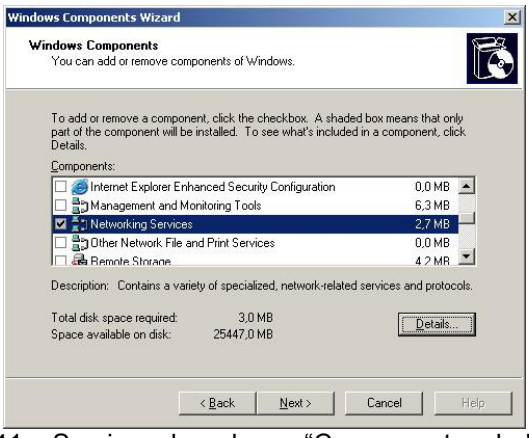

Figura 4.41 – Serviços de rede em "Componentes do *Windows*"

- Marcar a opção "*Internet Authentication Service*" como mostra a Figura 4.42 e a seguir clicar em "OK". Clicar em "*Next*" para prosseguir;

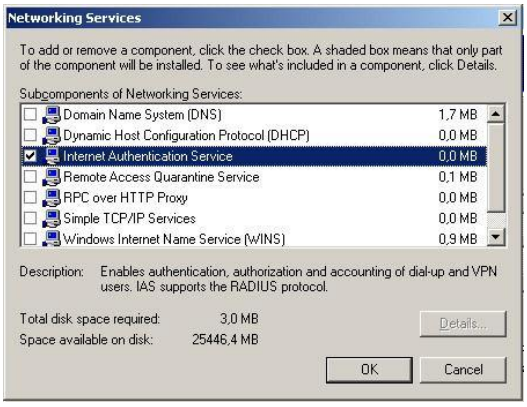

Figura 4.42 – Opção de instalação do IAS

- O processo de instalação poderá pedir o CD do *Windows Server 2003*. Apontar o caminho e clicar em "OK" para finalizar a instalação.

4.4.1.1 Instalação do Certificado Digital do RADIUS IAS

Este procedimento permite instalar o certificado digital do RADIUS IAS, para que a autenticação mútua entre o servidor e o cliente possa ser realizada, conforme descrito na seção 2.4.1. Para isso, foram seguidos os seguintes passos:

- Abrir o menu executar e digitar “mmc”. Na console aberta, clicar em “*File*” e em seguida em “*Add/Remove Snap-in*”, conforme Figura 4.43;

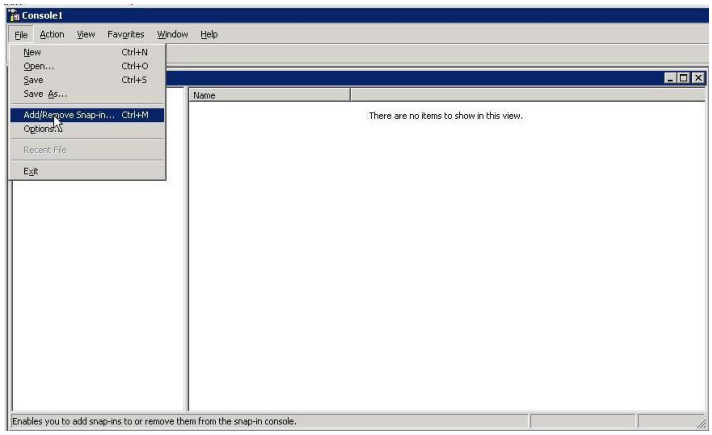

Figura 4.43 – Console para requisição do certificado

- Na guia “*Standalone*”, clicar em “*Add*” para adicionar um certificado. Selecionar “*Certificates”* e clicar em “*Add*”, conforme Figura 4.39;

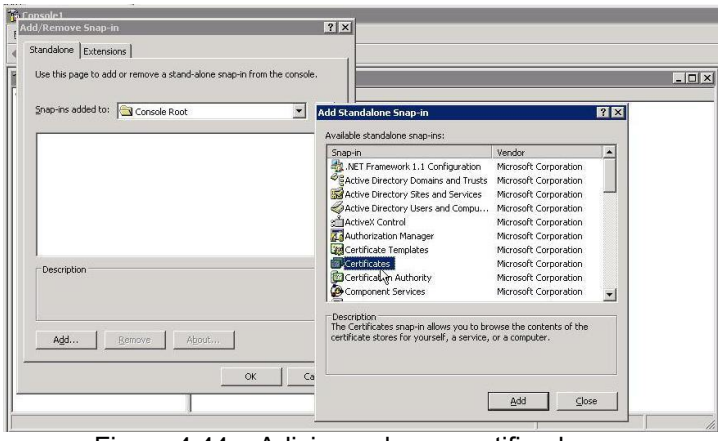

Figura 4.44 – Adicionando um certificado

- Surgirá a janela “*Certificates snap-in*”. Em “*This snap-in will always manage certificates for*” selecionar ***Computer account*** para que o certificado gerencie contas de computador como mostra a Figura 4.45 e, em seguida, clicar em “*Next*” para prosseguir;

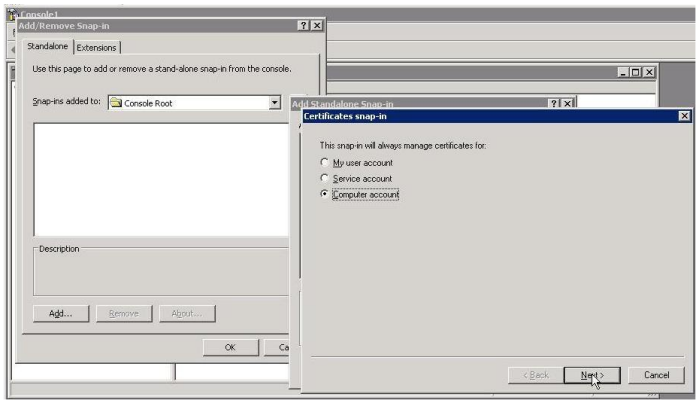

Figura 4.45 – Opção de gerenciamento de certificados de computador

- Em "*Select the computer you want this snap-in to manage*", escolher a opção ***Local computer*** para que a máquina local seja gerenciada pelo certificado, como pode ser visto na Figura 4.46. Em seguida, clicar em "*Finish*" e fechar as janelas;

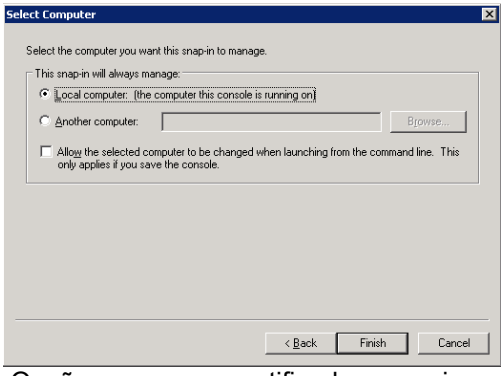

Figura 4.46 – Opção para que o certificado gerencie a máquina local

- Expandir "*Certificates (Local Computer)*" e clicar com o botão direito sobre "*Personal*". Selecionar "*All Tasks*" e clicar na opção "*Request New Certificate*", conforme Figura 4.47;

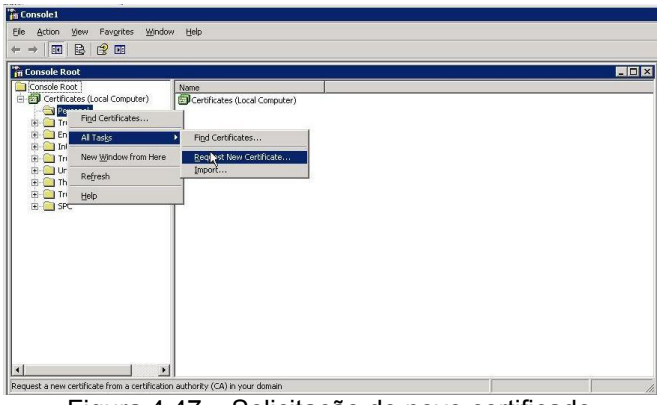

Figura 4.47 – Solicitação de novo certificado

- Surgirá a tela "*Certifcate Request Wizard*" mostrada na Figura 4.48 para que o certificado possa ser solicitado. Clicar em "*Next*" para prosseguir;

Figura 4.48 – "*Wizard*" para solicitação do novo certificado

- Na tela "*Certifcate Types*", selecionar **RADIUS** e marcar a opção "*Advanced*", conforme Figura 4.49. Esse certificado foi criado e configurado na subseção 4.2.3.1 (Procedimento de configuração da CA). Clicar "*Next*" para prosseguir;

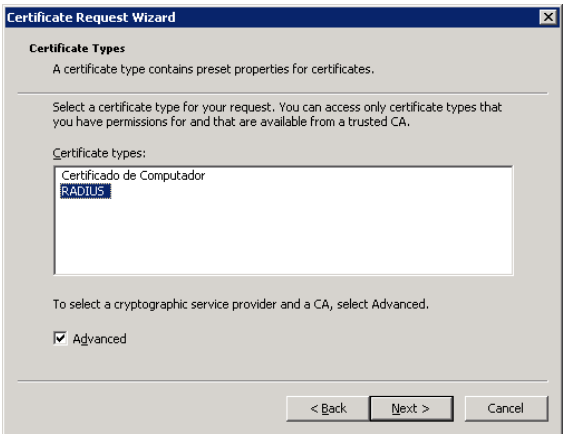

Figura 4.49 – Tipo de certificado

- Em "*Criptographic Service Provider*" (CSP), mostrado na Figura 4.50, as opções padrão ***Microsoft RSA Schannel Criptographic Provider*** e **1024** para "*Key Length*" foram mantidas;

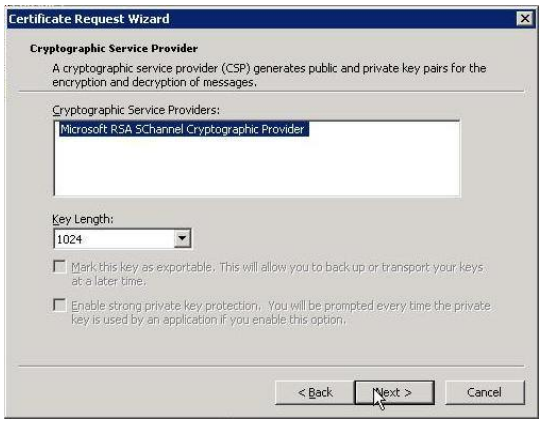

Figura 4.50 – Provedor de serviço de criptografia

- Na tela "*Certification Authority*", o campo "CA" deverá conter o nome da Autoridade Certificadora criada na subseção 4.2.3 (Procedimento de instalação da CA) **CA Projeto** e o campo "*Computer*" deverá conter o nome do servidor **SRV-CA.projetofinal.net**, conforme mostrado na Figura 4.51. Clicar em "*Next*" para prosseguir;

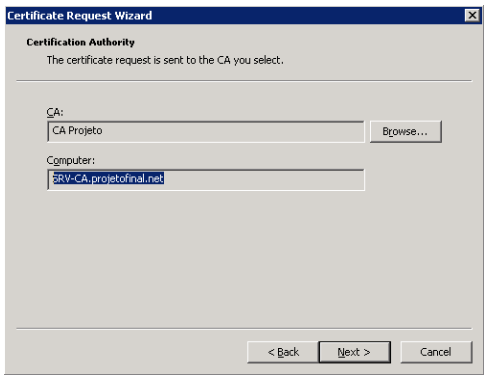

Figura 4.51 – Autoridade Certificadora

- Na tela seguinte, em "*Friendly name*", foi escolhido o nome **certCA**, como pode ser visto na Figura 4.52. Clicar em "*Next*" para prosseguir;

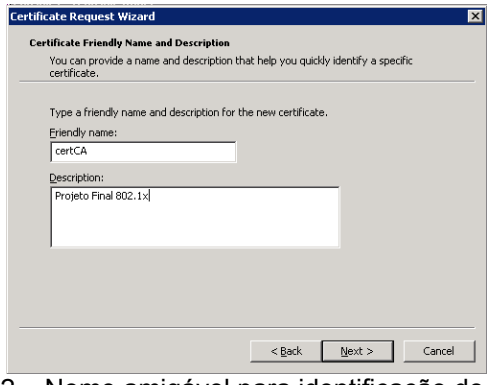

Figura 4.52 – Nome amigável para identificação do certificado

- Clicar em “*Finish*” para finalizar o processo de criação do certificado, como mostrado na Figura 4.53.

Figura 4.53 – Resumo da criação do certificado

4.4.1.2 Procedimento de configuração das políticas do RADIUS IAS

Este procedimento, referenciado na seção 2.7.1 deste projeto, fará a configuração das políticas de acesso do RADIUS IAS para autenticação do cliente.

- Após a instalação, é necessário fazer o registro do RADIUS no servidor do AD. Para isso, deve-se abrir o menu executar e digitar “**ias.msc**”. Clicar com o botão da direita sobre *Internet Authentication Services* e em seguida fazer o registro do servidor no AD, clicando na opção “*Register Server in Active Directory*”, conforme Figura 4.54;

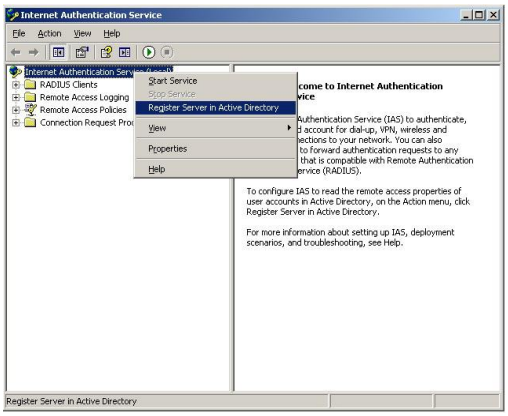

Figura 4.54 – Registrando o IAS no AD

- Durante o processo de registro do IAS, será solicitado que seja concedida a permissão de leitura da base “*dial-in*”. Clicar em “OK” e em seguida será

retornada uma mensagem informando sucesso (ou falha) ao habilitar a opção. Clicar em “OK”;

- No menu executar, digitar “**dsa.msc**”. Abrirá uma janela com o “*Snap-In”* do *Active Directory Users and Computers*. É necessário se conectar ao domínio “**projetofinal.net**”. Expandir o nome do domínio “**projetofinal.net**” e clicar em “*Users*”. Clicar com o botão da direita sobre o grupo “*RAS and IAS Servers*” e selecionar a opção “Properties”, conforme Figura 4.55;

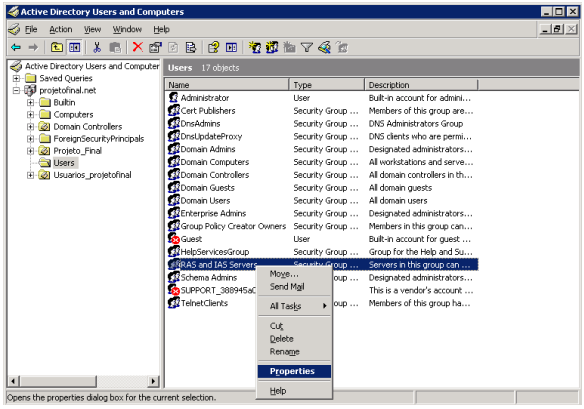

Figura 4.55 – *Snap-in* do AD

- Certificar-se dentro da janela “*RAS and IAS Servers Properties*”, na aba “*Members*”, que o servidor do IAS é um dos membros deste grupo, como na Figura 4.56. Caso não seja, deve-se repetir o procedimento de registro do IAS no AD. Em seguida, fechar todas as janelas;

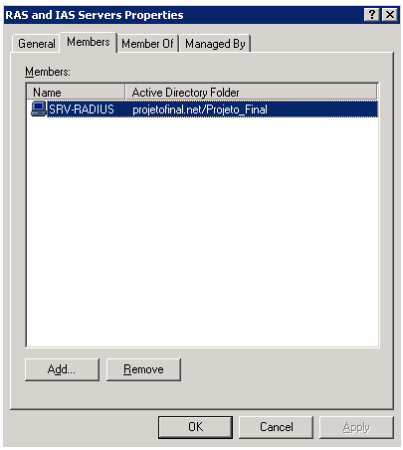

Figura 4.56 – Propriedades dos servidores IAS

A partir desse ponto, será iniciado o procedimento de configuração das políticas de acesso do RADIUS IAS.

- No menu executar, digitar “ias.msc”. Clicar em “*Remote Access Policies*”, conforme Figura 4.57;

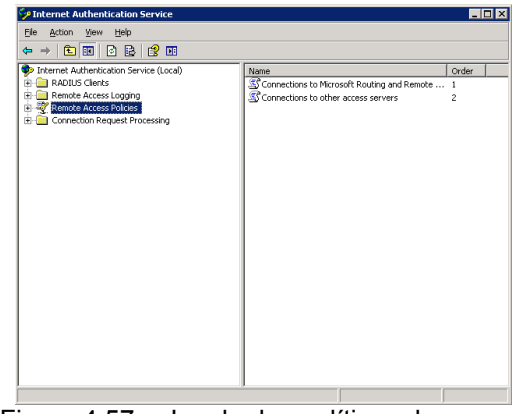

Figura 4.57 – Janela das políticas de acesso

- É necessário deletar as políticas padrões para que uma nova seja configurada. Ao deletar a última política, aparecerá uma caixa de diálogo informando que os usuários serão rejeitados. Isso ocorre porque neste momento não haverá política de acesso configurada no IAS. Clicar em “*Yes*”;

- Clicar com o botão direito sobre “*Remote Access Policies*”. Selecionar “*New*” e clicar em “*Remote Access Policy*”, conforme Figura 4.58. Assim, será possível criar uma política de acesso remoto customizada;

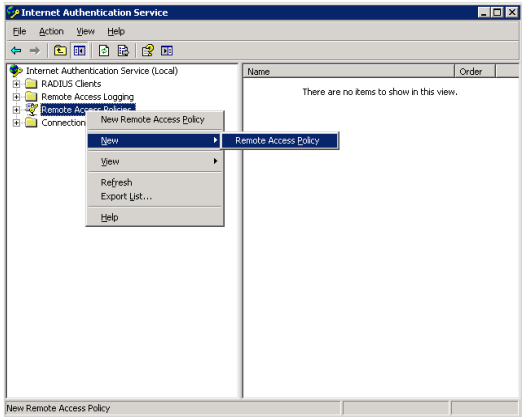

Figura 4.58 – Criação de uma nova política

- Surgirá a janela para criação de uma nova política “*New Remote Access Police Wizard*”. Clicar em “*Next*” para prosseguir;

- Surgirá a janela "*Policy Configuration Method*". Em "*How do you want to set up this policy?*", selecionar a primeira opção "*Use the wizard to set up a typical policy for a commom scenario*". Para a "*Policy name*", foi escolhido o nome **EAP-802.1x** para a nova política, como pode ser observado na Figura 4.59. Clicar em "*Next*" para prosseguir;

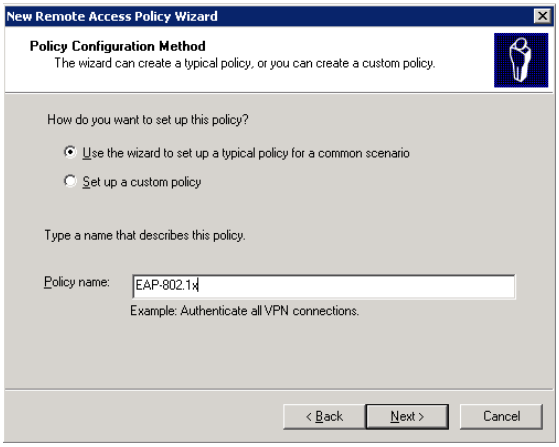

Figura 4.59 – Método de configuração da política

- Na janela "*Access Method*" mostrada na Figura 4.60, selecionar a opção "*ethernet*". Clicar em "*Next*" para prosseguir;

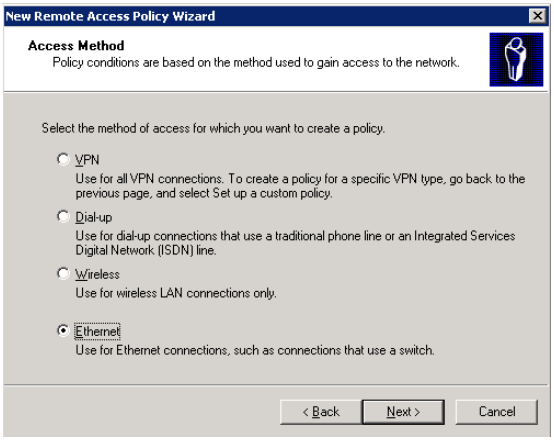

Figura 4.60 – Método de acesso

- Na janela "*User or Group Access*", selecionar a opção "*Group*" e em seguida clicar em "*Add*", como mostra a Figura 4.61;

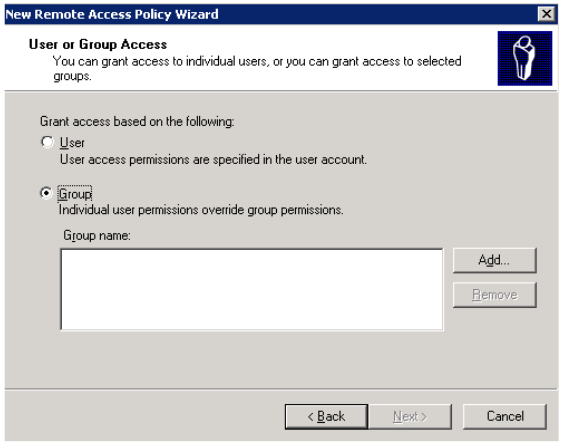

Figura 4.61 – Acesso de grupos ou usuários

- Clicar em "*Locations*" e selecionar o domínio **projetofinal.net**. Em seguida, em "*Enter the object names to select*", selecionar os grupos "*Domain Admins*", "*Domain Users*" e "*Domain Computers*", como mostra a Figura 4.62. Esses grupos terão garantia de acesso a rede. Clicar em "OK" e, em seguida, em "*Next*" para prosseguir;

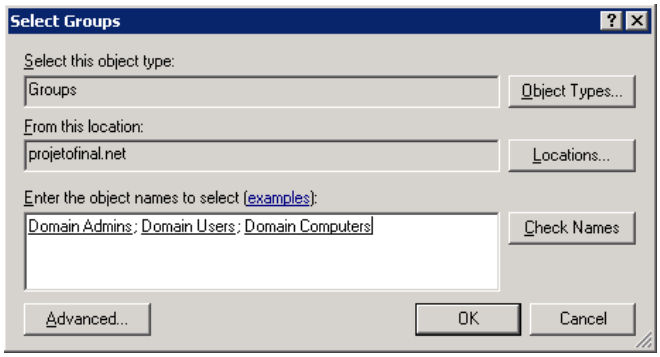

Figura 4.62 – Selecionando os grupos

- Na janela seguinte, "*Authentication Methods*", mostrada na Figura 4.63, selecionar a opção ***Smart Card or other certificate*** como método de autenticação, tendo em vista que este projeto focará na autenticação baseada na troca de certificados, utilizando o protocolo EAP-TLS, conforme descrito na subseção 2.3.1.2 do projeto. Clicar em "*Next*" para prosseguir;

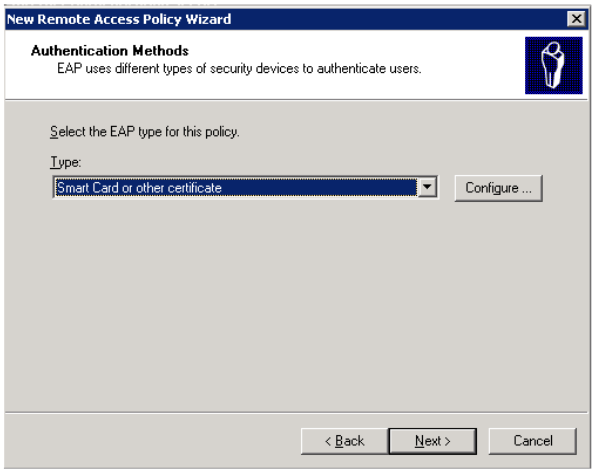

Figura 4.63 – Método de autenticação

- O processo de criação da política de acesso remoto estará concluído. Clicar em "*Finish*" para concluir, como mostra a Figura 4.64.

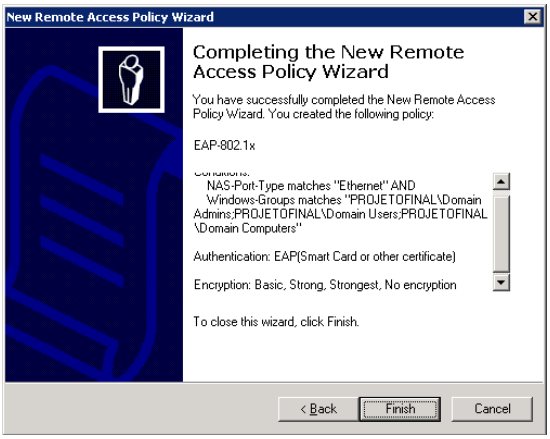

Figura 4.64 – Criação da política finalizada

4.4.1.3 Procedimento de configuração dos clientes RADIUS IAS

Para que o switch de acesso possa se autenticar no IAS, deve-se criar e configurar um cliente RADIUS. Para isso, foram seguidos os seguintes passos:

- Clicar com o botão direito sobre "*Radius Client*" e em seguida na opção "*New Radius Client*", conforme Figura 4.65;

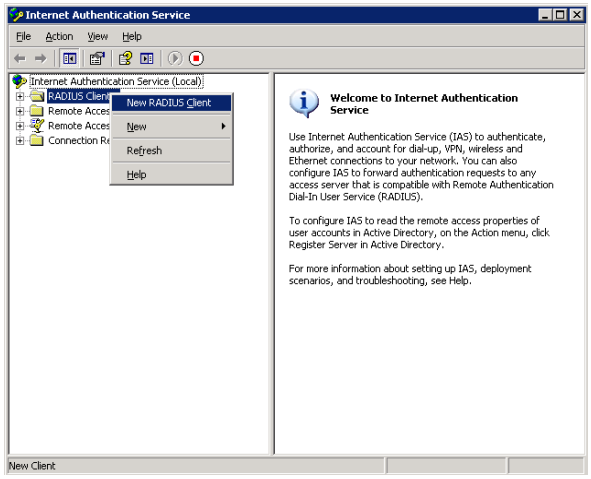

Figura 4.65 – Criação de um novo cliente RADIUS

- Na janela que surgirá, deve-se especificar um nome que identifique o cliente RADIUS e o endereço IP. Foi escolhido o nome **Catalyst 2950** e o IP **172.16.3.237**, como pode ser visto na Figura 4.66;

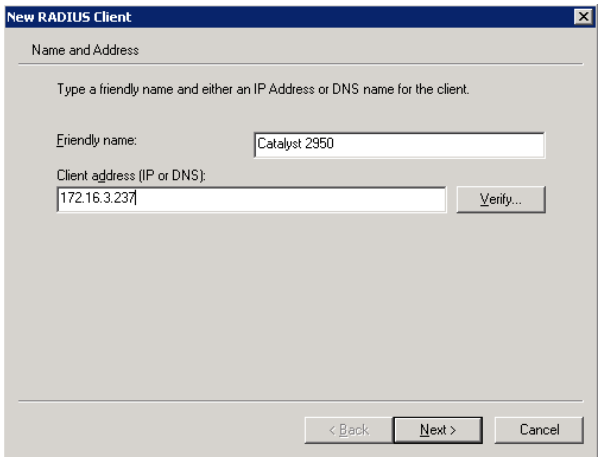

Figura 4.66 – Nome e IP do cliente

- Em seguida, serão solicitadas informações adicionais sobre o cliente RADIUS. Em "*client-vendor*" foi mantido o padrão ***RADIUS Standard***, como pode ser visto na Figura 4.67. A "*Shared secret*" (chave compartilhada) é uma senha de autenticação que será compartilhada entre o servidor RADIUS e o switch para que a comunicação entre eles seja estabelecida. Essa mesma senha será configurada no switch. Clicar em "*Next*" para finalizar a configuração do cliente.

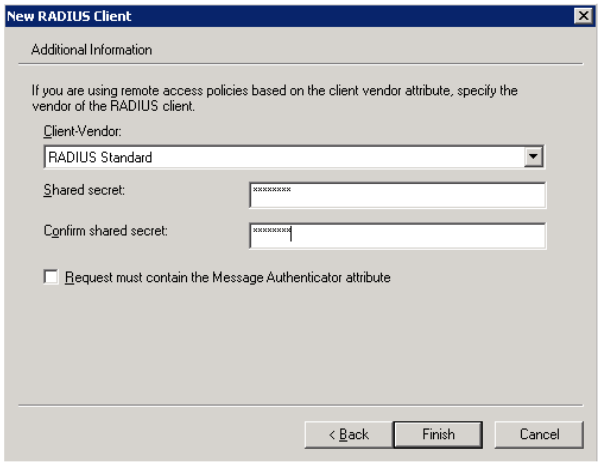

Figura 4.67 – Informações adicionais

4.5 PROCEDIMENTO DE CONFIGURAÇÃO DO SWITCH

Os procedimentos apresentados abaixo mostram como configurar o Switch *Cisco Catalyst 2950 Series* para funcionar com autenticação 802.1x. A programação completa do switch utilizada no desenvolvimento do Projeto encontra-se no Apêndice B.

Para acessar as configurações do switch, primeiramente foi necessário conectá-lo com um cabo console na porta **COM 1**[5] do computador e em seguida acessar o *Hyper Terminal*[6] do Windows para estabelecer a sessão, encontrado em "*Iniciar / Programas / Acessórios / Comunicações / Hyper Terminal*". As configurações de acesso, conforme Figura 4.68, são:

- *Bits per second:* ***9600***
- *Data bits:* ***8***
- *Parity:* ***None***
- *Stop bits:* ***1***
- *Flow control:* ***None***

[5] Porta de comunicação

[6] *Hyper Terminal* é um *software* de comunicação usado para se conectar com outros computadores ou dispositivos e está incluso em todas as versões do *Microsoft Windows.*

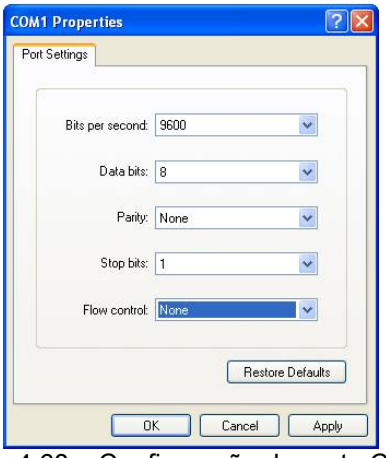

Figura 4.68 – Configuração da porta COM1

4.5.1 Configuração das Interfaces

A seguir serão apresentados os procedimentos de configuração das portas no switch *Cisco Catalyst 2950* adotados para a implementação deste projeto. A programação utilizada encontra-se no Apêndice B.

- Comando para criar VLAN:

  Switch#configure terminal
  Switch(config)#vlan <ID VLAN>

- Nomear VLAN 2:

  Switch(config-vlan)#name <nome VLAN>

- Adicionar interfaces do switch em uma VLAN:

  Switch#configure terminal
  Switch(config)#interface fastEthernet 0/<PORTA>
  Switch(config-if)#switchport access vlan <ID VLAN>

- Configuração do 802.1x no switch:

  Switch#configure terminal
  Switch(config)#aaa new-model

Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface fastethernet 0/<PORTA>
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end

- Configurar a comunicação entre o switch e o servidor RADIUS

Switch#configure terminal
Switch(config)#radius-server host <IP SERVIDOR RADIUS> auth-port 1812 key <SENHA>

- Configurar endereço IP e máscara de rede do switch:

Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address <IP> <MÁSCARA>
Switch(config-if)#no shutdown

4.6 CONFIGURAÇÃO DO CLIENTE

Para habilitar a autenticação do 802.1x utilizando um certificado digital (EAP-TLS) no cliente, basta seguir os seguintes passos:

- Clicar com o botão direito sobre "*My Network Places*" ou "Meus Locais de Rede" e clicar em "Propriedades";

- Em seguida, clicar com o botão direito sobre a conexão local de rede cabeada e clicar em "Propriedades";

- Na guia "*Authentication*" ou "Autenticação", habilitar a opção "*Enable IEEE 802.1x authentication*", como mostra a Figura 4.69. Em seguida deve-se escolher o método de autenticação. Foi escolhida a opção ***Smart Card or***

other Certificate. Com essa opção, o método de autenticação será por meio de certificado digital. Após isso, clicar em "*Settings*" para configuração;

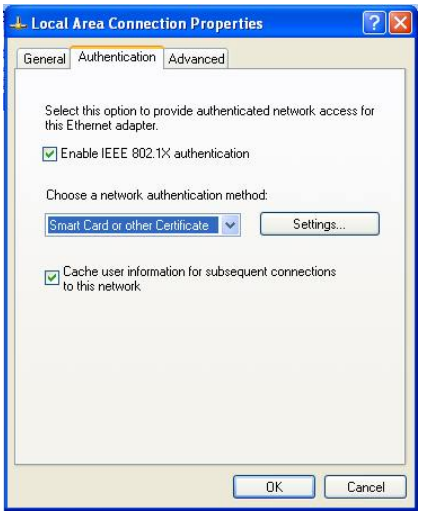

Figura 4.69 – Habilitando o 802.1x no cliente

- Na janela que surgirá, mostrada na Figura 4.70, em "*When connecting*" foram marcadas as opções "*Use a certificate on this computer*" e "*Use simple cerificate selection*", para que o certificado armazenado no computador seja utilizado e "*Validate server certificate*" para verificar se o certificado do servidor que está presente na máquina ainda é válido. No campo "*Trusted Root Certification Authorities"*, a Autoridade de Certificação criada **CA Projeto** foi selecionada por ser a Autoridade de Certificação raiz confiável. Em seguida, clicar em "OK" para fechar as janelas.

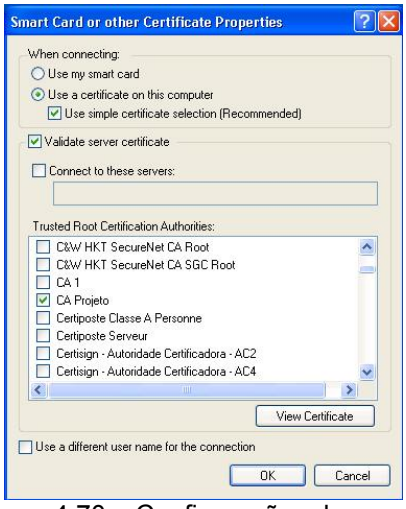

Figura 4.70 – Configurações de acesso

Uma observação importante que deve ser ressaltada é que no sistema operacional *Windows XP* com *Service Pack 3* (SP3), o serviço 802.1x deverá ser iniciado manualmente. Sem esse procedimento, a aba "*Authentication*" não aparecerá nas propriedades de conexão. Portanto, deve-se clicar no menu **Iniciar** / **Executar** e digitar "*services.msc*". O serviço "*Wired AutoConfig*" deve ser colocado para iniciar automaticamente, como mostra a Figura 4.71. Para isso, basta clicar com o botão da direita sobre ele e clicar em "Propriedades". Em seguida, no tipo de inicialização, escolher "Automático".

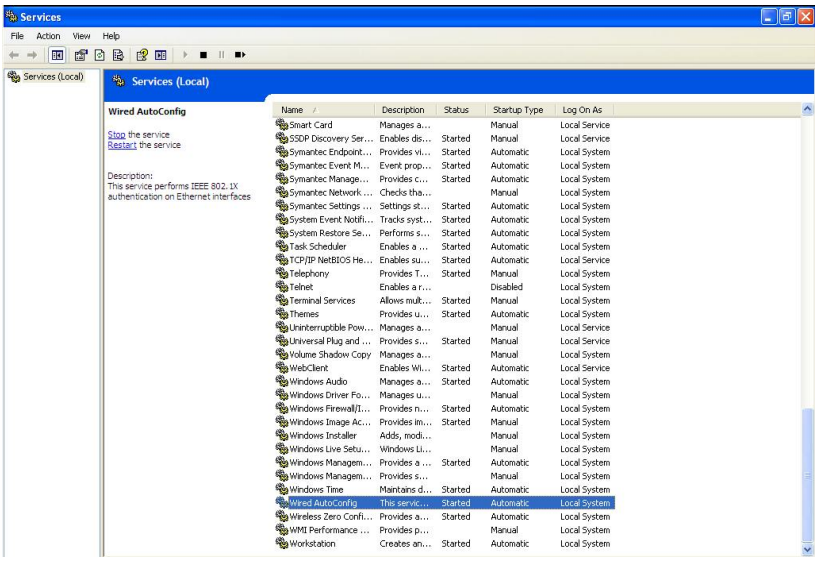

Figura 4.71 – Iniciando o serviço 802.1x no *Windows XP SP3*

Com isso, finalmente chega-se a instalação e configuração completa dos ambientes propostos para o desenvolvimento deste projeto. A seguir serão mostrados os resultados das simulações realizadas nestes ambientes para análise de desempenho do padrão IEEE 802.1x.

CAPÍTULO 5. ANÁLISE DE RESULTADOS

Neste capítulo são apresentados os resultados que foram obtidos nos testes e simulações dos cenários propostos no projeto. Em seguida, os resultados de cada ambiente serão confrontados para análise comparativa de desempenho e validar se há ou não degradação na rede com a infra-estrutura de segurança 802.1x implementada.

Também serão citados os problemas que ocorreram durante o desenvolvimento deste projeto.

5.1 PROCEDIMENTO PADRÃO PARA MEDIÇÕES

Para este projeto, foram analisados os seguintes aspectos em cada um dos dois cenários propostos:

1. Medição dos parâmetros de **Tempo de Resposta**, **Latência** e ***Throughput***, tomando como base a realização de *downloads* de arquivos de tamanhos variados, sendo um arquivo de 20 MB, outro de 50 MB e outro de 100 MB, com requisições HTTP e FTP e com auxílio da ferramenta *Wireshark* para captura dos pacotes e medição dos parâmetros.

Para cada arquivo, o *download* foi repetido cinco vezes, limpando os *caches* e tirando uma média do tempo de *download*, para cada arquivo em cada situação. As repetições do procedimento se faz necessária pois os sistemas operacionais possuem rotinas e aplicativos que funcionam em *background*, efetuando tarefas paralelas com a utilização normal, podendo causar variações no tempo de *download.* Uma média do tempo dará um resultado mais próximo do real.

2. Tempo de autenticação em cada ambiente.

Um importante parâmetro a ser analisado nos cenários propostos é o tempo de autenticação de um usuário. No primeiro cenário, o usuário informa

suas credenciais e se autentica direto no servidor Controlador de Domínio. Já no segundo cenário, a permissão de acesso a rede é concedida pelo servidor RADIUS. Com auxílio do *Wireshark* instalado nestes servidores, pode-se verificar o tempo médio de autenticação em cada ambiente. Para isso, a autenticação do usuário foi repetida cinco vezes e, em seguida, calculada a média do tempo dessas autenticações.

O tempo de autenticação foi calculado pela subtração do tempo de fim e início do processo de autenticação, conforme descrito abaixo:

$T_{Início}$: *Tempo de início do processo de autenticação*
T_{Fim}: *Tempo de fim do processo de autenticação*
$T_{Aut}: T_{Fim} – T_{Início}$

5.2 RESULTADOS OBTIDOS

De acordo com os testes descritos na seção 5.1 deste capítulo, os seguintes resultados foram obtidos:

5.2.1 Medição dos Parâmetros de Desempenho

5.2.1.1 Requisição FTP

Para os resultados dos parâmetros de desempenho com requisição FTP medidos em ambos os cenários, calculou-se o valor médio do Tempo de Resposta, Latência e *Throughput* da rede, cujos resultados estão consolidados na Tabela 5.1. Todos os valores calculados nos testes encontram-se no Apêndice C deste projeto.

Tabela 5.1 – Média dos parâmetros de desempenho calculados com requisição FTP

	FTP					
	Cenário 1			**Cenário 2**		
Arquivo	**T.Resposta (seg)**	**Latência (seg)**	***Throughput* (Mbps)**	**T.Resposta (seg)**	**Latência (seg)**	***Throughput* (Mbps)**
Tamanho (MB)	Valor médio	Valor médio	Valor médio	Valor médio	Valor médio	Valor médio
20,71	2,49	1,98	10,49	2,55	2,07	10,18
52,5	5,63	5,48	9,60	5,97	5,36	9,79
100	10,70	10,39	9,70	10,73	10,20	9,85

Pelos valores calculados, observa-se um acréscimo máximo de 0,34 segundo no tempo de resposta para o arquivo de 50 MB, o que representa 6,03% de aumento em relação ao primeiro cenário. Em contrapartida, a latência para o mesmo arquivo diminuiu em 2,23% quando requisitado no ambiente com 802.1x. Já o tempo de resposta para o arquivo de 100 MB sofreu um aumento de 0,03 segundo, representando 0,28% de acréscimo. Quanto ao *throughput*, houve uma queda máxima de 3,04% em relação ao primeiro cenário na requisição do arquivo de 20 MB.

Os gráficos a seguir ilustram a comparação entre a média dos parâmetros de desempenho nos dois cenários implementados neste projeto. Em ambos os casos foram utilizadas requisições do protocolo de aplicação FTP. A Figura 5.1 ilustra a comparação entre a média do Tempo de Resposta e da Latência, calculados em segundos, e a Figura 5.2 ilustra a diferença de *Throughput*, calculado em Mbps (Megabytes por segundo).

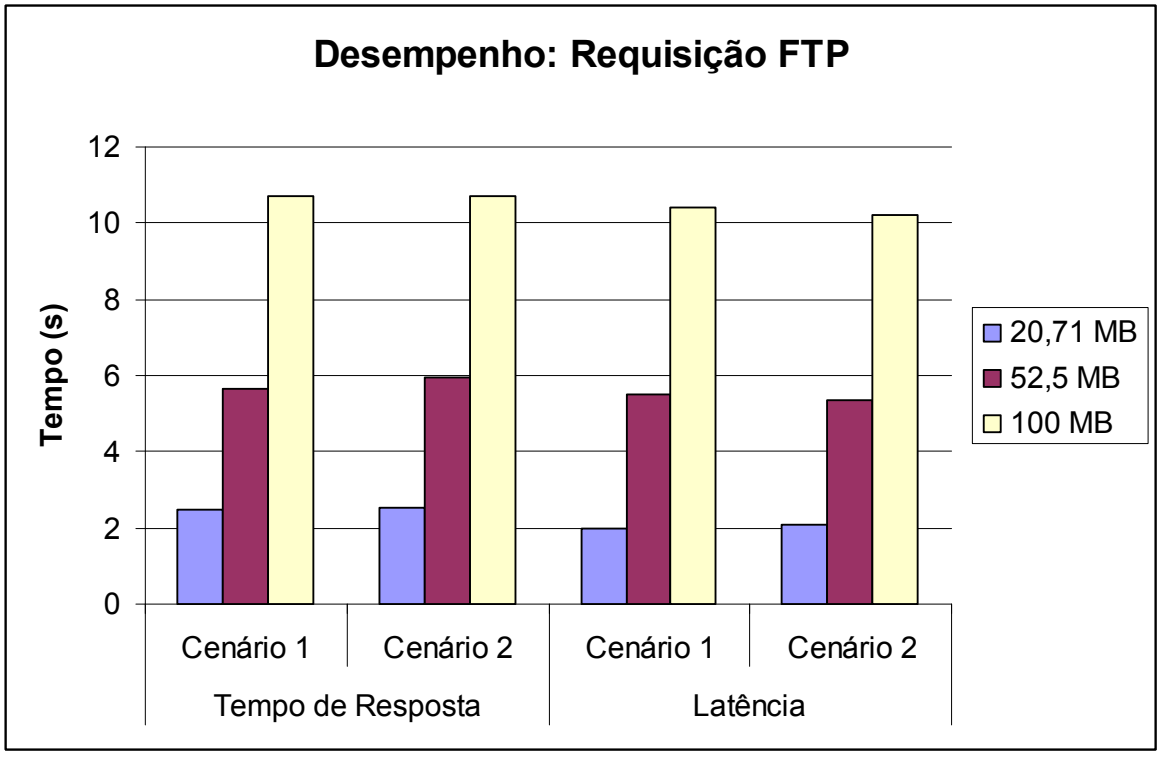

Figura 5.1 – Comparação de Tempo de Resposta e Latência entre os dois cenários para requisição FTP

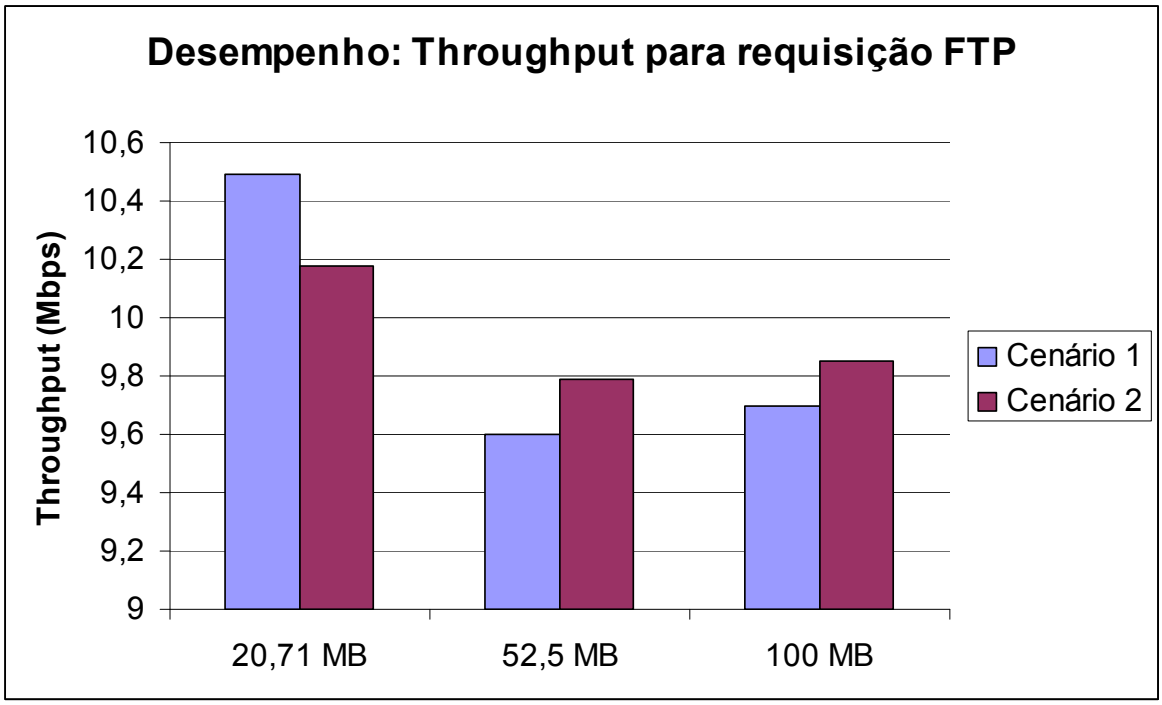

Figura 5.2 – Diferença de *Throughput* entre os dois cenários para requisição FTP

Observa-se que o comprometimento no desempenho da rede devido a implementação do mecanismo de segurança é praticamente desprezível, sendo que os piores casos ocorreram com o download dos arquivos de menor tamanho. A utilização do IEEE 802.1x ocasiona impacto mínimo na *performance* da rede quando o protocolo de aplicação FTP é utilizado.

5.2.1.2 Requisição HTTP

Para os resultados dos parâmetros de desempenho com requisição HTTP medidos em ambos os cenários, calculou-se o valor médio do Tempo de Resposta, Latência e *Throughput* da rede, cujos resultados estão consolidados na Tabela 5.2 abaixo. Todos os valores calculados nos testes encontram-se no Apêndice C deste projeto.

Tabela 5.2 – Média dos parâmetros de desempenho calculados com requisição HTTP

	HTTP					
	Cenário 1			**Cenário 2**		
Arquivo	**T.Resposta (seg)**	**Latência (seg)**	***Throughput* (Mbps)**	**T.Resposta (seg)**	**Latência (seg)**	***Throughput* (Mbps)**
Tamanho (MB)	Valor médio	Valor médio	Valor médio	Valor médio	Valor médio	Valor médio
20,71	2,47	2,25	9,30	2,48	2,24	9,38
52,5	6,05	5,87	9,00	6,21	5,98	8,79
100	10,74	10,57	9,53	10,99	10,86	9,24

Pelos valores calculados, observa-se um acréscimo da ordem de 0,01 segundo no tempo de resposta para o arquivo de 20 MB, o que representa um aumento de 0,4% em relação ao primeiro cenário. Da mesma forma, a latência para o arquivo de 50 MB apresentou um acréscimo de 0,11 segundo, representando 1,87% de aumento. Quanto ao *throughput*, houve uma queda máxima de 3,13% em relação ao primeiro cenário na requisição do arquivo de 100 MB.

Nos gráficos a seguir estão ilustrados a comparação entre a média dos parâmetros de desempenho nos dois cenários implementados neste projeto. Em ambos os casos foram utilizadas requisições do protocolo de aplicação HTTP. A Figura 5.3 ilustra a comparação entre a média do Tempo de Resposta e da Latência, calculados em segundos, e a Figura 5.4 ilustra a diferença de *Throughput*, calculado em Mbps (Megabytes por segundo).

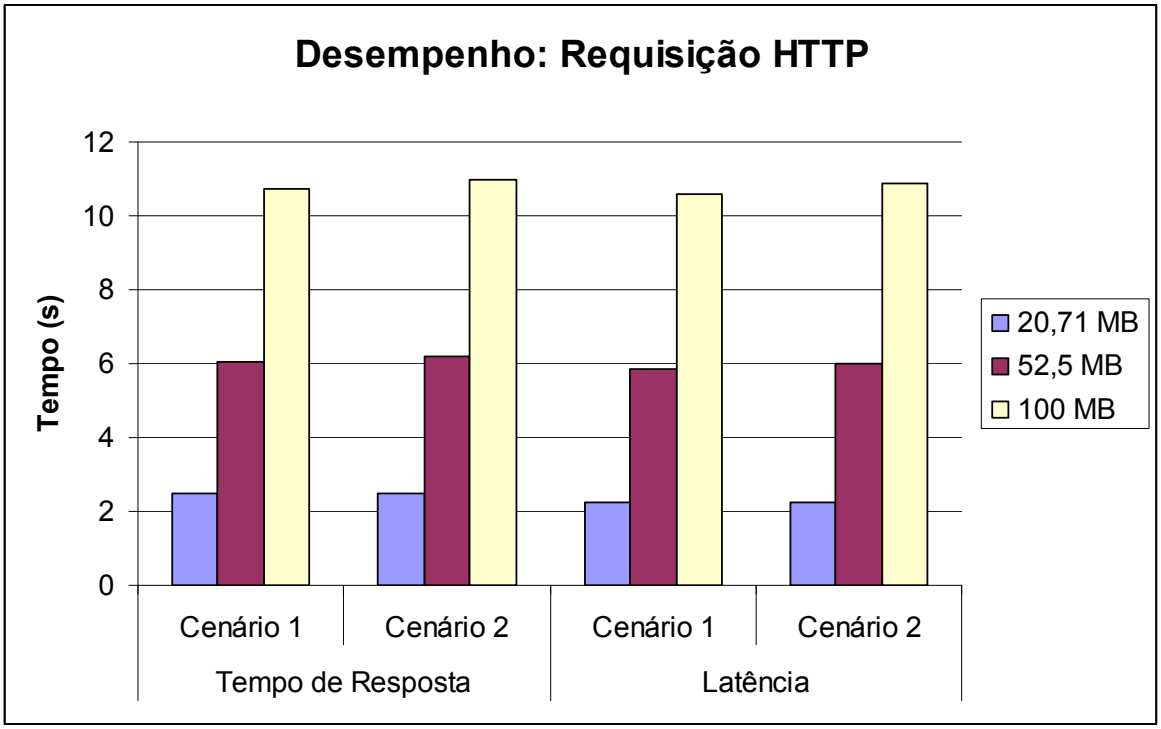

Figura 5.3 – Comparação de Tempo de Resposta e Latência entre os dois cenários para requisição HTTP

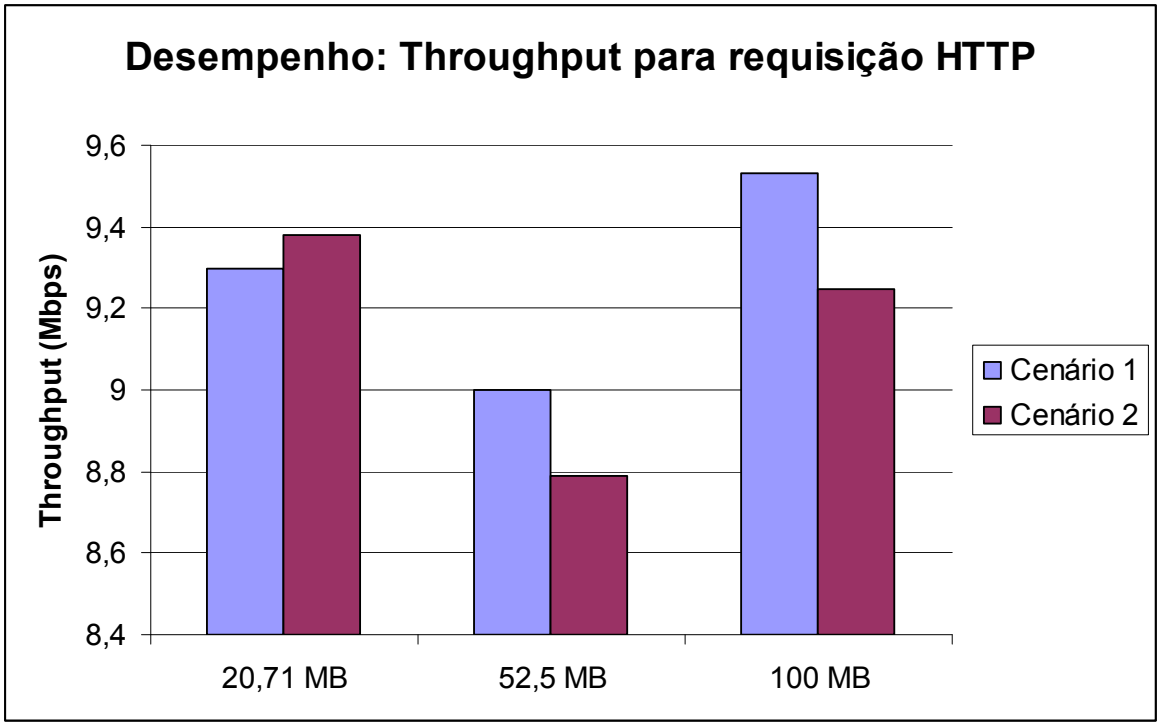

Figura 5.4 – Diferença de *Throughput* entre os dois cenários para requisição HTTP

Assim como na requisição FTP, pode-se observar que a degradação no desempenho da rede causada pela utilização do mecanismo de segurança 802.1x com o protocolo de aplicação HTTP é mínima e praticamente desprezível, sendo o pior caso observado no *download* do arquivo de maior tamanho.

5.2.2 Tempo de Autenticação

Conforme procedimento descrito no item 3 da seção 5.1 deste capítulo, foi calculada a média no tempo de autenticação do usuário em cada ambiente. A Tabela 5.3 mostra a média do tempo de autenticação em cada um dos cenários implementados. Todos os valores calculados nos testes encontram-se no Apêndice C deste projeto.

Tabela 5.3 – Consolidação do tempo médio de autenticação em cada ambiente

	Tempo de autenticação
Ambiente	Valor médio (seg)
Cenário 1	0,022
Cenário 2	0,378

Pelos valores obtidos, percebe-se uma grande diferença no tempo de autenticação do usuário quando é utilizado o mecanismo de segurança 802.1x.

No segundo cenário, temos um tempo de autenticação 17 vezes superior ao primeiro cenário.

O gráfico mostrado na Figura 5.5 ilustra a diferença no tempo de autenticação do Cenário 1 sem a infra-estrutura de segurança, quando comparado com o Cenário 2, com o 802.1x implementado.

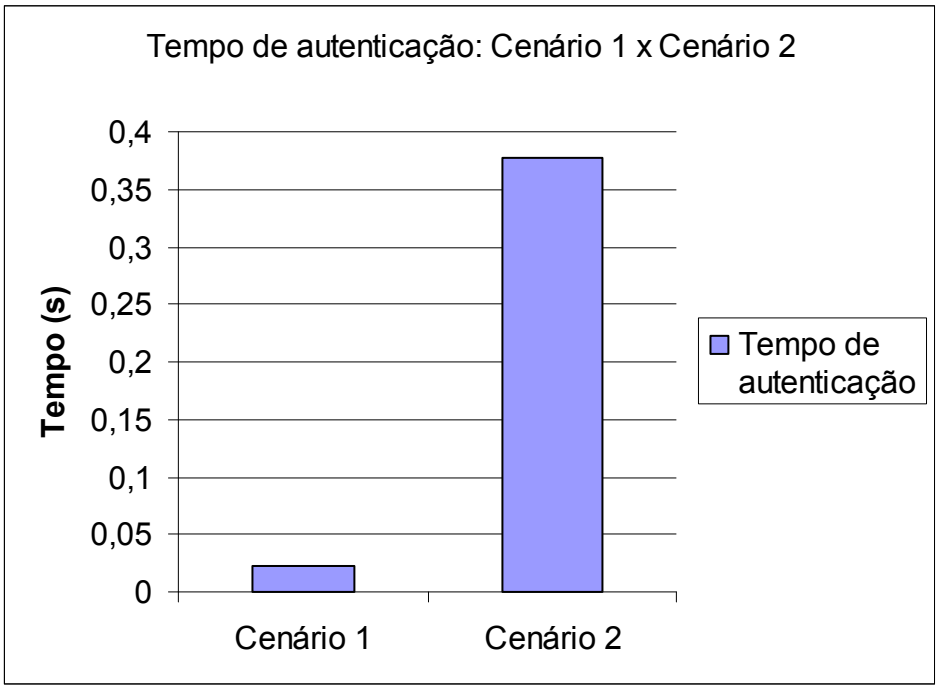

Figura 5.5 – Tempo de autenticação Cenário 1 x Cenário 2

5.3 ANÁLISE DE RESULTADOS

Na análise dos resultados obtidos, pôde-se observar que há pouca influência sobre a *performance* da rede quando se implementa o mecanismo de segurança intrínseco do padrão IEEE 802.1x. Uma vez que os certificados digitais foram conferidos e a autenticação bem sucedida, o switch coloca o usuário na porta não-controlada e lhe permite o acesso a rede. A pequena diferença de resultados entre os cenários deve-se basicamente às oscilações de tempo de *download*, influenciado pelas condições e configurações da rede e dos equipamentos utilizados, sendo, portanto, desprezível e imperceptível para o usuário.

Na análise do tempo de autenticação do usuário, percebe-se uma

grande diferença entre os dois ambientes. Este, de fato, é o efetivo impacto da utilização da infra-estrutura de segurança 802.1x, utilizando o método de autenticação EAP-TLS.

O tempo de autenticação no segundo cenário é maior devido ao fluxo de mensagens trocadas entre Suplicante, Autenticador, Servidor de Autenticação e Servidor Controlador de Domínio. Como o método de autenticação utilizado no Projeto é o EAP-TLS, ainda há o tempo gasto para verificação e validação do certificado digital do suplicante. A Figura 5.6, obtida por meio do *software Wireshark* instalado no servidor RADIUS, mostra a troca de pacotes entre o switch, IAS e Controlador de Domínio. Na figura, observa-se o momento em que o switch (172.16.3.237) envia um pedido de acesso ao servidor de autenticação (172.16.3.234) até o momento em que o switch recebe o pacote com a informação de acesso aceito. Tomando como referência o primeiro pacote com a solicitação de acesso, pode-se calcular o tempo que levou para o cliente ser autenticado.

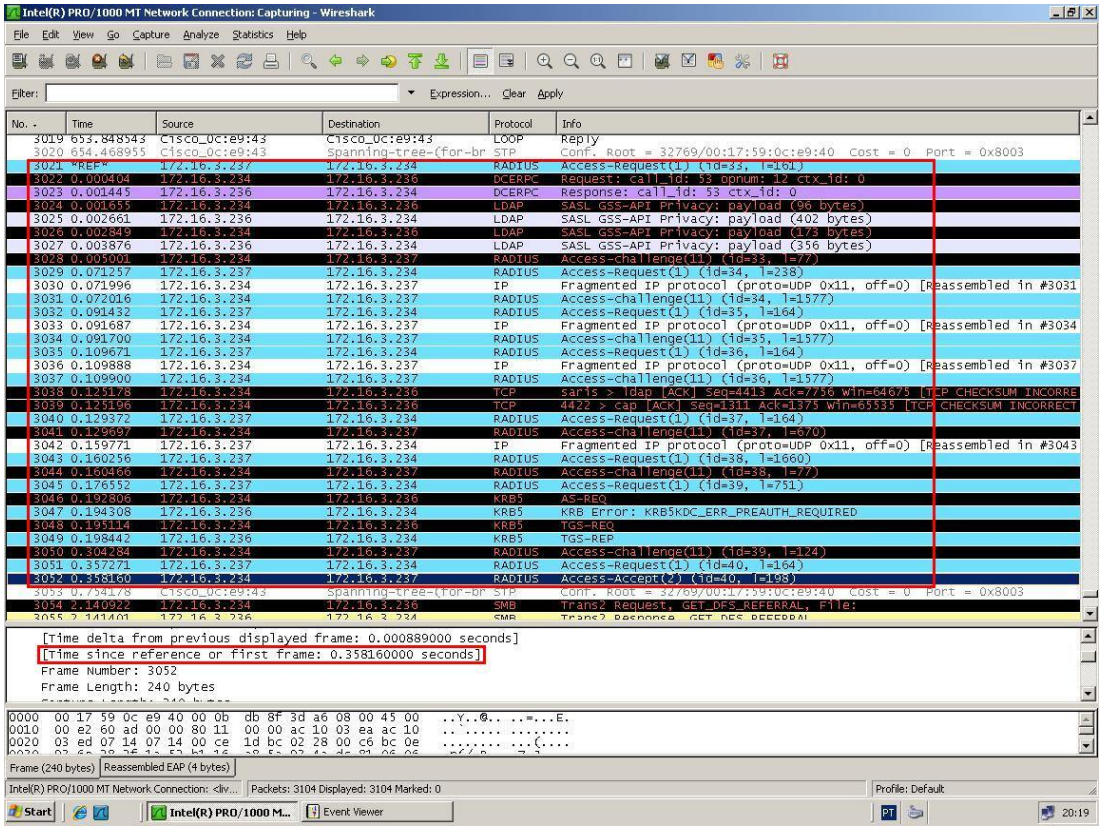

Figura 5.6 – Tempo de autenticação RADIUS

Já a Figura 5.7 mostra a autenticação de um usuário (172.16.3.109) por meio de credenciais de usuário e senha no servidor Controlador de Domínio (172.16.3.236). O tempo de autenticação foi calculado tomando-se como referência o primeiro pacote enviado pelo cliente, até o momento em que o DC envia um pacote com uma resposta positiva ao cliente.

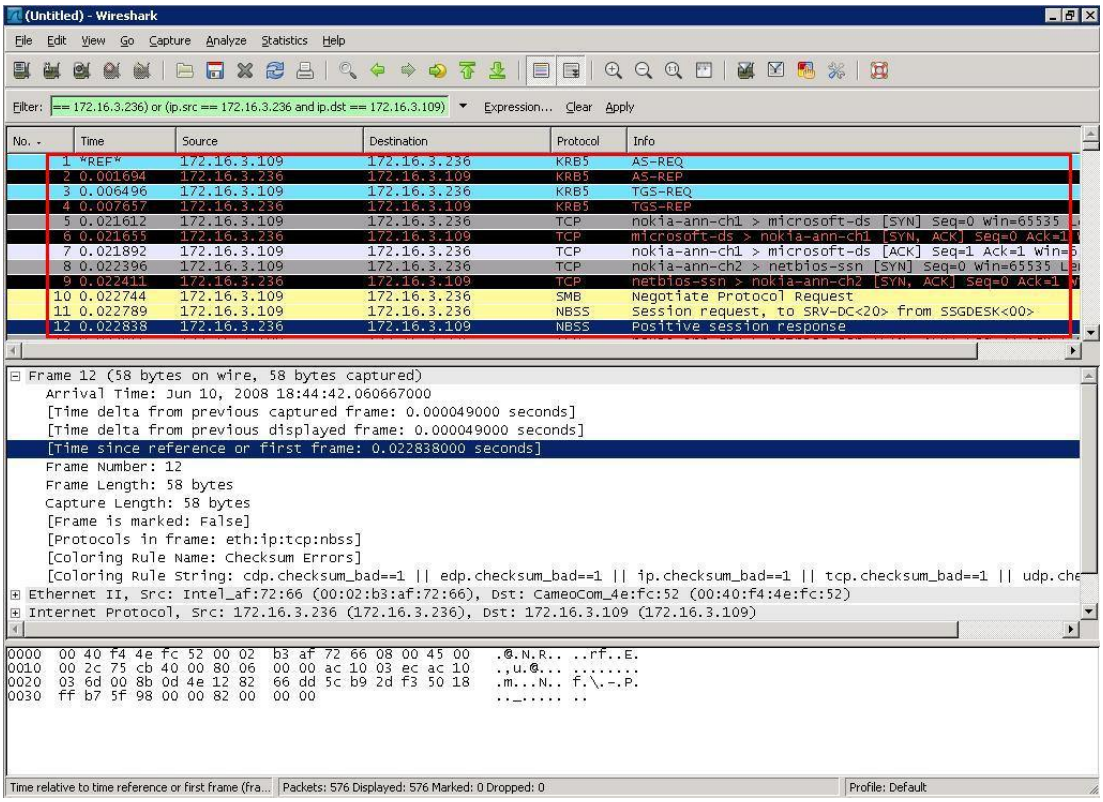

Figura 5.7 – Tempo de autenticação no DC

Apesar da grande discrepância no tempo de autenticação dos dois cenários, essa diferença é praticamente imperceptível para o usuário, devido ao tempo que o *Windows* leva até carregar toda a configuração inicial do sistema. Isso ocorre apenas no instante da validação e autenticação do usuário. Depois que o acesso com o 802.1x foi permitido e o usuário autenticado, a conectividade na rede será normal, respeitando as políticas de acesso definidas no servidor RADIUS.

Portanto, percebe-se que a utilização do 802.1x com o EAP-TLS como mecanismo de segurança de redes é válida e viável por fornecer um controle de acesso rígido e confiável, praticamente sem causar degradação no desempenho

da rede.

5.4 PROBLEMAS OCORRIDOS

Durante a fase de implementação, foram encontradas algumas dificuldades na configuração e utilização correta do ambiente, devido à grande dificuldade em encontrar documentação disponível para configuração do 802.1x, principalmente quando a autenticação é por meio de certificados.

Percebeu-se que existe uma limitação para o funcionamento do mecanismo de segurança quando são utilizadas máquinas virtuais. Por exemplo, um servidor RADIUS em uma máquina virtual não recebe os pacotes com a solicitação de acesso enviada pelo switch. Dessa forma, o usuário não consegue ter acesso às portas não-controladas. Por isso, todos os equipamentos utilizados no projeto tiveram que ser físicos.

Após a instalação e configuração dos equipamentos, surgiram alguns problemas como dificuldade para emissão automática de certificados e erros durante a autenticação, como pode ser visto na Figura 5.8. A solução encontrada foi desinstalar e reinstalar o serviço IAS.

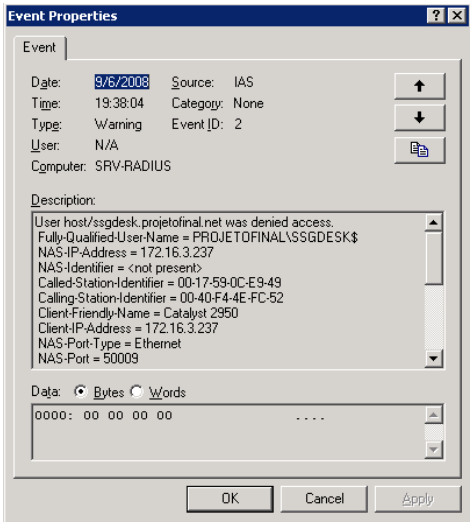

Figura 5.8 – Erro durante a autenticação

Durante a execução dos testes, verificou-se a dificuldade em encontrar aplicações que mensurassem de forma precisa os valores desejados. Após

algumas pesquisas sobre ferramentas para a realização das medições, optou-se pela utilização do *Wireshark*, apesar da dificuldade inicial encontrada no entendimento e análise dos pacotes capturados pela ferramenta.

CAPÍTULO 6. CONCLUSÃO

A dependência da eficiência nas redes de dados faz com que as empresas busquem soluções de segurança, principalmente no que tange ao controle de acesso de seus usuários. As redes possuem diversas vulnerabilidades decorrentes da fragilidade dos mecanismos de segurança no que diz respeito a autenticação, confidencialidade e integridade dos dados.

A fragilidade na segurança da rede põe em risco as informações confidenciais de uma instituição, podendo causar transtornos às atividades administrativas e comerciais de uma empresa, além de prejuízos financeiros, quando há a possibilidade de interceptação e adulteração dos dados através de acesso de pessoas não autorizadas em um ambiente corporativo.

A solução de segurança que visa o controle de acesso por meio de portas, IEEE 802.1x, com a utilização de servidores RADIUS e o mecanismo de autenticação EAP-TLS que utiliza certificação digital para autenticar os usuários, proporciona maior rigidez e maiores níveis de segurança na autenticação uma vez que limita o acesso do usuário na rede.

Contudo, esperava-se que a utilização deste mecanismo de segurança gerasse uma sobrecarga na rede pela inserção de tráfego extra para autenticação dos usuários, ocasionando uma degradação e comprometimento no desempenho da rede. Porém, após a implementação deste projeto foi verificado, por meio de testes em laboratório, utilizando protocolos de aplicação FTP e HTTP, com requisições de *download* de arquivos de tamanhos variados, que o impacto em termos de tempo de resposta, latência e *throughput* é mínimo e, em alguns casos, imperceptível.

Com os resultados obtidos, pode-se concluir que praticamente não há a influência sobre a *performance* da rede quando se implementa o mecanismo de segurança, pois as variações dos resultados entre um ambiente sem a infra-estrutura de segurança e o outro com essa infra-estrutura implementada é desprezível.

O maior impacto da utilização do 802.1x observado nas simulações realizadas foi no tempo de autenticação dos usuários. Essa diferença, apesar de imperceptível, deve ser levada em consideração quando a solução de segurança é aplicada em ambientes maiores, onde vários usuários poderão estar se autenticando ao mesmo tempo. Dessa forma, uma solução poderia ser a utilização de outros servidores RADIUS, funcionando com balanceamento de carga.

Por fim, embora o processo de autenticação do usuário quando se está utilizando o 802.1x como mecanismo de segurança tenha apresentado uma diferença considerável em relação a um ambiente sem segurança implementada, o uso do 802.1x com o servidor RADIUS e autenticação baseada em certificação digital é uma excelente alternativa para empresas que desejam melhorar o nível de segurança e buscam confidencialidade e integridade dos dados, por implementar um controle de acesso robusto e limitar o acesso à rede, reduzindo os riscos de pessoas não autorizadas receberem conectividade ao ambiente.

Sugere-se para desenvolvimento de projetos futuros, a análise e implementação do 802.1x nas seguintes condições:

- Tempo de autenticação em uma rede com vários usuários, implementando o mecanismo de segurança e avaliando o impacto das autenticações simultâneas;

- Análise comparativa de eficiência e tempo de autenticação do protocolo 802.1x com outros dos muitos mecanismos de autenticação disponíveis como, por exemplo, PEAP, LEAP e EAP-TTLS;

- Análise do IEEE 802.1x quando utilizado em ambientes *wireless* e comparação da segurança implementada pelo padrão IEEE 802.11.

REFERÊNCIAS BIBLIOGRÁFICAS

AHSON, Syed. ILYAS, Mohammad. **Handbook of Wireless Local Area Networks**. *Applications, Technology, Security, and Standards*, 2005.

BROWN, Edwin L. **802.1x Port-Based Network Access Authentication**. 1ª Ed. New York : Auerbach Publications, 2007 – 238 pág.

HAHN, Genebeck. KWON, Taekyoung. **A Comparative Analysis of Extensible Authentication Protocols**.

KOMAR, Brian. **Microsoft Windows Server 2003 PKI and Certificate Security**. Microsoft Press, 2004.

MARTINS, Alessandro. **Autoridade Certificadora para Acesso Seguro**. 2001.

NAKAMURA, E. GEUS, P. L. ***Segurança de Redes em Ambientes Cooperativos***. 2ª Ed. Futura, 2003.

PETERSON, LARRY L. **Redes de Computadores: Uma Abordagem de Sistemas.** 3ª Ed. São Paulo : Elsevier Editora LTDA, 2004 – 587 pág.

Sites

1. http://www.microsoft.com/brasil/technet/seguranca/colunas/sm0805.mspx - Mar.2008
2. http://standards.ieee.org/getieee802/download/802.1X-2001.pdf - Fev.2008
3. ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt - Mar.2008
4. http://www.ietf.org/rfc/rfc2865.txt?number=2865 – Mar.2008
5. http://www.ietf.org/rfc/rfc4346.txt?number=4346 – Mar.2008
6. http://www.microsoft.com/technet/archive/community/columns/security/5min/5min-303.mspx?mfr=true – Fev.2008
7. http://msdn2.microsoft.com/en-us/library/ms889599.aspx - Fev.2008
8. http://www.microsoft.com/downloads/details.aspx?familyid=8A0925EE-EE06-4DFB-BBA2-07605EFF0608&displaylang=en – Fev.2008
9. http://technet.microsoft.com/pt-br/library/bb742380(en-us).aspx – Fev. 2008
10. http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/intwork/inbc_ias_elfq.mspx?mfr=true – Fev.2008
11. http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technolo

gies/directory/activedirectory/stepbystep/domcntrl.mspx - Mar.2008

12. http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22_ea5/configuration/guide/sw8021x.html - Mai.2008

13. http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22_ea5/configuration/guide/2950scg.html - Mai.2008

APÊNDICE A – SCRIPT DE REQUISIÇÃO FTP

O *ScriptFTP.txt* é o arquivo responsável pelo processo de requisição dos arquivos no serviço de FTP.

Texto do *script*:

1. Arquivo de 20 MB (*teste20Mb.exe*):

```
open 172.16.3.109
anonymous
123
cd Projeto
get teste20Mb.exe
quit
```

2. Arquivo de 50 MB (teste50Mb.exe):

```
open 172.16.3.109
anonymous
123
cd Projeto
get teste50Mb.exe
quit
```

3. Arquivo de 100 MB (teste100Mb.zip):

```
open 172.16.3.109
anonymous
123
cd Projeto
get teste100Mb.zip
quit
```

APÊNDICE B – PROGRAMAÇÃO DO SWITCH

```
Current configuration : 2064 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname projeto
!
aaa new-model
aaa authentication dot1x default group radius
enable secret 5 $1$UNCj$FIPlzk/iYo.qSpOalUFty/
enable password wilson
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/10
```

```
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
```

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.3.237 255.255.255.0
 no ip route-cache
!
ip http server
radius-server host 172.16.3.234 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 3
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password wilsonjr
line vty 5 15
 password wilsonjr
!
!
end
```

APÊNDICE C – TABELAS COM AS MEDIDAS REALIZADAS

1. Requisições FTP

	FTP					
	Medições sem o 802.1x			Medições com o 802.1x		
	20 MB			20 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	2,9	2,14	9,677	2,18	1,83	11,316
2	2,06	1,95	10,62	2,95	1,92	10,786
3	1,96	1,83	11,316	2,74	2,71	7,642
4	3,02	2,08	9,956	1,96	1,84	11,25
5	2,53	1,9	10,9	2,96	2,09	9,909
M	2,494	1,98	10,4938	2,558	2,078	10,1806

	50 MB			50 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	5,17	5,01	10,479	5,95	5,38	9,758
2	5,78	5,48	9,58	6,13	5,27	9,962
3	5,71	5,68	9,242	5,95	5,38	9,757
4	5,56	5,35	9,813	5,74	5,14	10,214
5	5,93	5,89	8,913	6,08	5,67	9,259
M	5,63	5,482	9,6054	5,97	5,368	9,79

	100 MB			100 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	10,4	10,36	9,699	10,14	10,11	9,939
2	11,42	10,75	9,347	10,98	10,06	9,989
3	10,37	9,82	10,233	11,06	10,32	9,737
4	11,65	11,37	8,838	10,12	9,9	10,15
5	9,69	9,67	10,391	11,38	10,65	9,435
M	10,706	10,394	9,7016	10,736	10,208	9,85

2. Requisições HTTP

	HTTP					
	Medições sem o 802.1x			Medições com o 802.1x		
	20 MB			20 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	2,25	2,08	9,956	3,05	2,82	7,343
2	2,45	2,06	10,053	2,31	2,14	9,677
3	2,26	2,1	9,861	2,65	2,34	8,85
4	2,42	2,24	9,245	2,27	1,98	10,459
5	2,98	2,79	7,422	2,12	1,96	10,566
M	2,472	2,254	9,3074	2,48	2,248	9,379

	50 MB			50 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	5,07	4,91	10,692	6,37	6,2	8,467
2	6,19	6,05	8,677	5,7	5,53	9,493
3	6,4	6,12	8,578	5,86	5,69	9,226
4	6,16	6	8,75	6,3	6,02	8,72
5	6,46	6,3	8,333	6,86	6,5	8,076
M	6,056	5,876	9,006	6,218	5,988	8,7964

	100 MB			100 MB		
	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*	T. Resposta (seg)	Latência (seg)	*Throughput (Mbps)*
1	10,88	10,7	9,391	10,98	10,63	9,453
2	10,39	10,25	9,803	11,44	11,09	9,061
3	10,84	10,68	9,409	10,85	10,79	9,312
4	9,84	9,66	10,4	11,64	11,18	8,988
5	11,76	11,6	8,662	10,04	10,65	9,435
M	10,742	10,578	9,533	10,99	10,869	9,249

3. Tempo de autenticação

	Tempo de autenticação (seg)	
	Medições sem o 802.1x	**Medições com o 802.1x**
	Controlador de Domínio	**RADIUS IAS**
1	0,023	0,39
2	0,023	0,32
3	0,025	0,40
4	0,022	0,34
5	0,019	0,44
M	0,022	0,378