INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

IMPLEMENTAÇÃO DO SERVIÇO RADIUS PARA A AUTENTICAÇÃO DE UTILIZADORES NO ACESSO À REDE WIRELESS DO ISUTC

Ted Nicolas António Fernandes

Projecto Final do Curso

Licenciatura em Engenharia Informática e de Telecomunicações

Supervisor:

Eng. Sete Matimele

Departamento de Tecnologia de Informação e Comunicação

Março, 2014

INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

IMPLEMENTAÇÃO DO SERVIÇO RADIUS PARA A AUTENTICAÇÃO DE UTILIZADORES NO ACESSO À REDE WIRELESS DO ISUTC

Ted Nicolas António Fernandes

Projecto Final do Curso

Licenciatura em Engenharia Informática e de Telecomunicações

Supervisor:

Eng. Sete Matimele

Departamento de Tecnologia de Informação e Comunicação

Março, 2014

Implementação do serviço RADIUS para a autenticação de utilizadores no acesso à rede wireless do ISUTC

Ted Fernandes

ÍNDICE

AGRADECIMENTOS

Aos meus pais, António Manuel Nicolau Fernandes e Haissa Abdul Remane Ismael, pelo amor, carinho, educação e principalmente pela persistência para o alcance dos objectivos desejados.

Aos meus irmãos, cunhadas e a família no geral, pelo apoio, companheirismo e amizade.

Ao meu supervisor, Eng. Sete Matimele, pelo incentivo, confiança, compreensão, paciência e acima de tudo pelas críticas.

Aos meus colegas de escola e professores no geral.

A todos que contribuíram directa ou indirectamente para a realização deste trabalho.

DEDICATÓRIA

Dedico este trabalho aos meus pais, António Manuel Nicolau Fernandes e Haissa Abdul Remane Ismael, que sempre acreditaram nas minhas capacidades e na concretização dos meus sonhos.

DECLARAÇÃO DE HONRA

Eu, Ted Nicolas António Fernandes declaro por minha honra que o presente Projecto Final do Curso é exclusivamente de minha autoria, não constituindo cópia de nenhum trabalho realizado anteriormente e as fontes usadas para a realização do trabalho encontram-se referidas na bibliografia.

Assinatura: _____

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DAS ABREVIATURAS UTILIZADAS

AAA	*Authentication, Authorization and Accounting*
ACL	*Access Control List*
ACS	*Access Control Server*
AES	*Advanced Encryption Standard*
AP	*Access Point*
ASA	*Adaptive Security Appliance*
CHAP	*Challenge Handshake Authentication Protocol*
EAP	*Extensible Authentication Protocol*
IAS	*Internet Authentication Service*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISUTC	Instituto Superior de Transportes e Comunicações
ITC	Instituto de Transportes e Comunicações
ITIL	*Information Technology Infrastructure Library*
LAN	*Local Area Network*
LCP	*Link Control Protocol*
LDAP	*Lightweight Directory Access Protocol*
LDIF	LDAP *Data Interchange Format*
LTS	*Long Time Server*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MD5	*Message-Digest algorithm 5*
MIC	*Message Integrity Code*
NAS	*Network Access Sever*
PAN	*Personal Area Network*
PAP	*Password Authentication Protocol*
PC	*Personal Computer*
PKI	*Public-Key Infrastructure*
PPP	*Password Authentication Protocol*
PSK	*Pre-Shared Key*

RADIUS	*Remote Authentication Dial-In-User Service*
RAM	*Random Access Memory*
RF	*Radio Frequency*
RFC	*Request for Comments*
SSID	*Service Set Identifier*
SSH	*Secure Shell*
TACACS+	*Terminal Access Controller Access-Control System Plus*
TCP	*Transmission Control Protocol*
TI	Tecnologia de Informação
TKIP	*Temporal Key Integrity Protocol*
UDP	*User Datagram Protocol*
VoIP	*Voice over Internet Protocol*
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WAP	*Wireless Application Protocol*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	Wi-Fi *Protected Access*
WPAN	*Wireless* PAN
WWW	*World Wide Web*

RESUMO

Nos dias de hoje, a segurança de redes é uma grande preocupação. A aplicação de uma política de segurança efectiva é o passo mais importante que uma organização pode dar para proteger a sua rede. Uma das habilidades mais importantes das quais um administrador de rede precisa, é identificar ameaças à segurança de redes corporativas e descrever métodos para atenuar essas ameaças. A importância da segurança da rede não pode ser subestimada, principalmente quando se trata de redes sem fio, pois estas, são mais vulneráveis. Sendo assim, o presente projecto demonstra a implementação de um serviço capaz de autorizar os utilizadores no acesso a rede sem fio do ISUTC (Instituto Superior de Transportes e Comunicações) para os diferentes tipos de serviços que esta fornece. Mediante entrevistas feitas aos funcionários do sector de informática, colectou-se vários dados referentes aos equipamentos que o ISUTC possui, ajudando assim no desenvolvimento do projecto. Dos estudos feitos, foi possível entender como encontra-se estruturada a rede do ISUTC, e qual o melhor método se adequa nesta estrutura para implementar o serviço RADIUS, sendo necessário para tal, identificar as possíveis vulnerabilidades da rede *wireless* com a presente implementação. Foram feitos testes depois da implementação do serviço, sendo estes realizados com sucesso. Um serviço destes na rede do ISUTC iria garantir uma melhor performance da rede, tanto como a segurança dos dados que trafegam pela mesma, pois somente pessoas autorizadas acederiam a rede após a autenticação.

Palavras-chave: Segurança em redes sem fio. RADIUS. Implementação do freeRADIUS.

CAPÍTULO 1 - INTRODUÇÃO

1.1 Justificação do tema

Actualmente o acesso a rede sem fio no Instituto Superior de Transportes e Comunicações (ISUTC) não é segura, possibilitando assim, o acesso de pessoas não autorizadas e/ou com más intenções pondo em causa a segurança da rede.

Sendo a segurança um ponto crítico, o projecto em questão é motivado pelos seguintes aspectos:

- A falta de controlo de acesso aprimorado pelo administrador de rede, com o intuito de proteger o ISUTC de ataques ou ameaças de segurança feito pelos invasores ou utilizadores de má-fé que acedem a rede. As informações conseguidas pelo administrador de rede sobre estes utilizadores, iria permitir responsabilizar o culpado de um determinado evento;
- Com o número de utilizadores crescendo no ISUTC, a segurança da rede torna-se mais vulnerável a ataques. Sendo assim, é indispensável o uso de um mecanismo de segurança baseado em um serviço responsável por autenticar e autorizar o acesso de quem pode fazer o uso da rede.

A implementação de um serviço seguro para autenticar os utilizadores no acesso a rede do ISUTC, iria proteger de possíveis ataques, pois esta, iria dificultar a entrada dos intrusos e dos malfeitores na rede.

1.2 Desenho teórico

1.2.1 Problemática

O ISUTC é uma instituição privada de ensino superior vocacionada para a formação de quadros superiores nas áreas ligadas aos Transportes e Comunicações e suas envolventes. O Sector de Informática desta instituição é responsável por garantir o acesso a rede em qualquer parte do edifício, de tal maneira que os utilizadores da rede sintam-se acomodados para realizar as suas tarefas.

Actualmente o ISUTC dispõe de uma rede de dados sem fio em algumas partes do edifício, pois esta, possui um baixo nível de protecção. O acesso a esta rede pode ser feita por computadores que não se encontram registados no domínio ISUTC, sendo estes: *laptops*, celulares, iPads e outros dispositivos com suporte a tecnologia *wireless*. O facto destes

dispositivos não se encontrarem no presente domínio, pode colocar em causa os seguintes pontos:

- O acesso de pessoas não autorizadas e/ou com más intenções;
- A manipulação da informação feita por pessoas não autorizadas;
- O mau funcionamento da rede causando um impacto no desempenho da mesma ou até mesmo um impacto destrutivo.

Sendo estes alguns dos pontos críticos, pode-se notar que não existe como responsabilizar estas pessoas por falta de controlo de acesso à rede *wireless* presente no ISUTC, pois o administrador teria dificuldades em identificar o dispositivo e a pessoa responsável por um determinado evento.

Sendo assim, surge a necessidade de implementar um serviço seguro que visa a autenticação, autorização e gestão de utilizadores para o acesso à rede sem fio através de *laptops*, celulares, iPads e outros dispositivos com suporte a tecnologia *wireless*. Este serviço será responsável por controlar, restringir e contabilizar o acesso dos utilizadores da rede ISUTC, melhorando assim o fluxo de dados e proporcionando segurança na comunicação.

1.2.2 Problema de investigação

Como implementar o serviço RADIUS (*Remote Authentication Dial-In-User Service*) de modo a garantir que apenas pessoas autorizadas possam aceder à rede *Wireless* do ISUTC?

1.2.3 Objecto de investigação

O objecto em estudo desta investigação é o serviço RADIUS.

1.2.4 Objectivo geral de investigação

Implementar o serviço RADIUS para a autenticação de utilizadores no acesso à rede *wireless* do ISUTC, garantindo que apenas pessoas autorizadas possam aceder os recursos da mesma.

1.2.5 Objectivos específicos de investigação

- Identificar as vulnerabilidades da rede *wireless* com a presente implementação;
- Analisar os métodos de implementação do Serviço RADIUS;
- Implementar o RADIUS no ISUTC;
- Testar a conexão de dispositivos de diferentes plataformas no serviço implementado.

1.2.6 Perguntas da investigação

- Quais os inconvenientes do actual modo de acesso à rede *wireless* do ISUTC?
- Como implementar o serviço RADIUS de forma a contornar esses inconvenientes?
- Que método melhor se adequa para autenticar os utilizadores no serviço RADIUS?
- Que melhorias verificar-se-ão com o uso do serviço implementado?

1.3 Metodologia

1.3.1 Abordagem da investigação

Dado que o presente estudo visa a implementação de um serviço que possibilita gerenciar diversos perfis para a autenticação de utilizadores, passando pela utilização e integração de tecnologias que possibilitam o alcance dos objectivos, será necessário um contacto directo entre o pesquisador e o ambiente onde a problemática reside.

Sendo assim, este trabalho terá como base de investigação uma abordagem qualitativa, de carácter descritivo, em que o tipo de informação a ser recolhida não pode ser quantificável. Este tipo de abordagem permitirá identificar os benefícios do objecto em estudo no contexto em que será aplicado.

1.3.2 Desenho da investigação

Das pesquisas feitas sobre os vários modelos de desenhos de investigação existentes, o modelo que se adequa a esta investigação é o não experimental, pois, para este estudo irá se observar os fenómenos tal como se produzem no seu contexto natural, para depois analisá-los.

1.3.3 Ideia a defender

A implementação de um serviço que possibilite gerir o acesso a diversos serviços de rede, fornecendo configurações que especifiquem quais as políticas e os tipos de serviços serão disponibilizados, pode garantir o uso apropriado dos recursos disponíveis na rede do ISUTC.

1.3.4 Métodos de investigação

Como método de investigação será usada a investigação empírica, pois esta baseia-se em fenómenos observáveis na realidade. As técnicas para a recolha e análise de dados serão essencialmente a realização de entrevistas formais que requerem documentos comprovativos com as respectivas assinaturas dos funcionário entrevistados do ISUTC, os quais vivem a problemática descrita.

1.3.5 Resultados esperados de investigação

Como resultado desta investigação, espera-se implementar um serviço capaz de autenticar, controlar, restringir e contabilizar o acesso dos utilizadores à rede *wireless* do ISUTC de forma a minimizar possíveis ataques, dificultando também o acesso de pessoas mal-intencionadas.

1.4 Resumo

Neste capítulo foram apresentados os aspectos relevantes para a escolha do tema, onde verificou-se qual serviço será oferecido e para que utilizadores. Foram feitas análises de forma a dar uma percepção do valor que será criado para o utilizador com o serviço implementado. Foi apresentado a metodologia de investigação, onde a abordagem de investigação será qualitativa de carácter descritivo.

CAPÍTULO 2 - MARCO TEÓRICO-CONCEPTUAL DA INVESTIGAÇÃO

2.1 Introdução

Este capítulo fornece fundamentos teóricos para uma melhor compreensão sobre os procedimentos seguidos na elaboração do projecto. Para tal, foi feita uma revisão bibliográfica sobre os principais conceitos e tecnologias que envolvem a segurança em rede de computadores, possibilitando assim entender a utilidade de implementação do serviço RADIUS.

Quando se fala da segurança em redes, um dos pontos cruciais é o acesso a informação não autorizada. Portanto, surge a necessidade de entender o conceito de informação. Para Rodrigues (2002), este conceito pode assumir várias definições dependendo do contexto a que ela se insere.

Na sua forma mais simples, a informação pode ser entendida como um conjunto de dados processados ou interpretados. Entretanto, e segundo Rezende D. (2005, pág. 26) "Informação é todo o dado trabalhado, útil, tratado, com valor significativo atribuído ou agregado a ele e com um sentido natural e lógico para quem usa a informação". Desta definição pode se concluir que os dados quando não são trabalhados ou processados não têm nenhum significado claro.

Tendo em consideração os conceitos tratados acima, será possível compreender melhor os assuntos abordados neste capítulo. Para dar continuidade ao presente projecto, será abordado primeiramente os conceitos chaves de uma rede de computadores.

2.2 Rede de computadores

Com a evolução tecnológica que se tem verificado de umas décadas para cá, a necessidade de comunicar com as pessoas tornou-se um processo indispensável nas organizações assim como nas famílias. A comunicação é o elemento fundamental para a realização das actividades do dia-a-dia. Os métodos usados para partilhar ideias e informações estão constantemente em evolução.

Para suportar o parágrafo acima, segundo Tittel E. (2002, pág. 36) "A comunicação entre pessoas e dispositivos é fundamental para o sucesso de muitas actividades comerciais da actualidade e, para facilitá-la usamos as redes ".

Uma rede de computadores pode ser definida de várias maneiras. Das definições existentes, Montico (2009) define uma rede de computadores como sendo um conjunto de computadores interconectados entre si, seja por meio de cabos, seja por meio de ondas de rádio (*wireless*).
Uma outra visão sobre a definição de rede de computadores é a do Cantu (2003), este diz que, uma rede de computadores é a conexão de dois ou mais computadores para permitir a partilha de recursos e a troca de informação entre as máquinas.
Baseando-se nessas definições, pode se dizer que uma rede de computadores não é nada mais que um conjunto de computadores interligados entre si, visando a partilha de informações e recursos como impressoras, disco duro, aplicações e outros, contribuindo economicamente para o sucesso de muitas actividades. Estes recursos podem ser classificados como de *Hardware ou de Software*. A diferença entre esses, segundo Chicole (2008), *Hardware* é toda a parte física do computador, esta envolve peças que podem ser apalpáveis, enquanto que o *Software* não existe no mundo físico, a estes podem se considerar os aplicativos do computador.
Ainda, dentro de uma rede de computadores, existem vários termos chave que a tornam operacional. Segundo Sousa (2009), dentre esses termos podem se destacar:

- **O administrador de rede -** Responsável pelo *software* e *hardware* que permite o funcionamento da rede, o que inclui funções relacionadas com:
    - Assegurar a máxima performance da rede;
    - Controlar a correcta comunicação de dados entre o servidor e os vários utilizadores;
    - Implementar sistemas de cópias de segurança e manutenção preventiva.
- **O servidor -** Computador responsável por partilhar informação, um conjunto de recursos de *hardware* e *software* com vários computadores. Existem diferentes categorias de servidores:
    - **Dedicado** – Computador utilizado como servidor dedica-se exclusivamente à gestão da rede.
    - **Não dedicado** - Computador servidor pode ser utilizado como servidor e estação de trabalho (situação praticamente inexistente na actualidade).
- **Topologias de rede** – Representam a forma como o servidor e as estações de trabalho estão conectadas.

Olhando para a abordagem de Ross (2008), ao falar-se da topologia de rede, é necessário distinguir uma topologia física duma topologia lógica. Os profissionais de rede utilizam o

termo de topologia física quando querem referir-se ao projecto físico da rede. Porém, a topologia lógica da rede, define como a informação vai se propagar na rede.

Já definidos os conceitos de topologia, surge a necessidade de classifica-las, podendo assim ser capaz de encontrar vantagens entre as demais topologias existentes.

2.2.1 Classificação das topologias de rede

Vários autores classificam as topologias de diversas maneiras. A figura 1, mostra o esquema das demais topologias existentes usadas em redes de computadores.

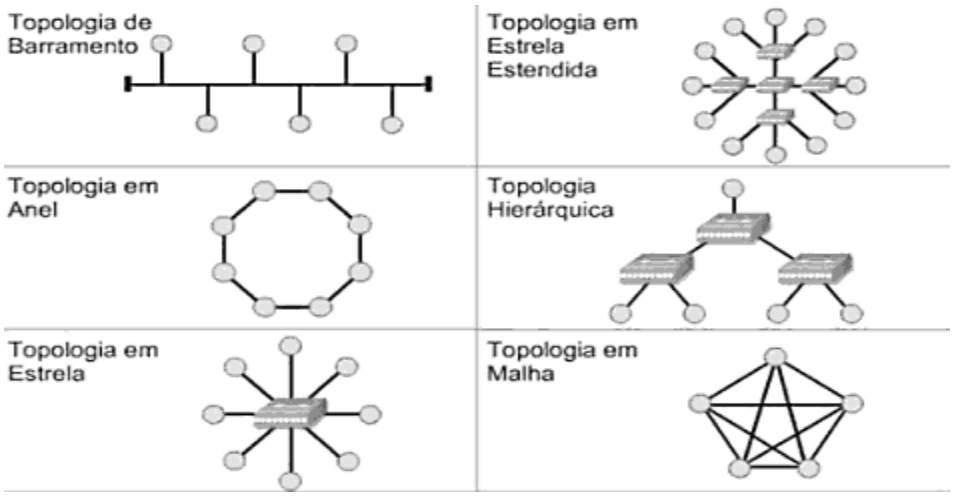

Figura 1: As demais topologias de rede existentes [ROSS, 2008]

Para Pinheiro (2006), existem três tipos básicos de topologias de rede descritas resumidamente na tabela 1.

Tabela 1: Comparação entre as topologias de rede [Pinheiro, 2006]

Topologia	Pontos Positivos	Pontos Negativos
Barramento	Estrutura simples; requer menos cabos para instalar.	A rede pode ficar lenta em momentos de uso mais intenso; as falhas são difíceis de localizar.
Anel	Instalação razoavelmente simples; apresenta desempenho uniforme sob condições diversas de tráfego.	Na falha de uma estação toda a rede para de funcionar.
Estrela	Mais tolerante a falhas, fácil de instalar e de monitorar	Custo de instalação mais elevado porque utiliza mais cabeamento.

A escolha de uma topologia, envolve decisões que referem aspectos tais como:

- Tamanho da rede;
- Custo;
- Facilidade de instalação;
- Facilidade de manutenção.

Para Ross (2008), em redes pequenas é comum utilizar-se topologias simples, tais como uma estrela, mas em redes maiores a combinação de várias topologias será necessária, pois cada pequena parte da rede utilizará uma topologia que serão combinadas para formar a rede completa.

A extensão da rede, leva a um outro conceito designado por classificação das redes de computador.

2.2.2 Classificação das redes

Vários autores classificam as redes de diferentes maneiras. Segundo Carissimi (2009), um critério muito utilizado para classificação de redes é a sua extensão geográfica. Tipicamente é utilizada a seguinte classificação:

- Redes pessoais ou PANs (*personal area networks*);
- Redes locais ou LANs (*local area networks*);
- Redes metropolitanas ou MANs (*metropolitan area networks*);
- Redes de longa distância ou WANs (*wide area networks*).

Mais para Montico M. (2009, pág. 9) “Existem dois tipos básicos de redes, definidas segundo sua localização: redes de área local (LAN) e redes de área extensa (WAN)”.

Estas redes no geral, podem ser caracterizadas da seguinte maneira:

- As redes do tipo PAN, são redes de curta distância que utilizam a comunicação sem fio, para interligar dispositivos numa área muito reduzida (GALLO & HANCOCK, 2002);
- As redes do tipo LAN, são usadas para interligar computadores numa área restrita, como por exemplo, computadores ligados numa mesma sala ou num mesmo edifício. Neste tipo de rede a comunicação é feita através de cabos que ligam as placas de rede inseridas nos computadores, (GOUVEIA & MAGALHÃES, 1999).
- As redes do tipo MAN, são redes que interconectam recursos computacionais ao longo de uma área metropolitana. Como por exemplo, organizações de negócio com prédios localizados ao longo de uma cidade, (CARISSIMI, 2009);

- As redes do tipo WAN, são usadas para interligar computadores localizados em diferentes cidades, países, continentes, ou simplesmente edifícios muito distantes dentro de uma mesma zona, (MONTICO, 2009).

Actualmente, fala-se de mobilidade, condições de trabalhar em qualquer local de trabalho sem estar necessariamente preso a uma estação local. Esta mobilidade traz consigo o conceito de redes sem fio, que por sua vez tem as suas características, topologias e classificações.

2.3 Redes sem fio

Nos dias de hoje, a gestão de uma infra-estrutura cabeada pode ser um desafio. As redes estão evoluindo com o objectivo de apoiar as pessoas na realização das suas tarefas. Alunos, docentes, a sociedade em geral, todos têm aparelhos móveis conectados uns aos outros. As redes sem fio oferecem mobilidade aos utilizadores.

Segundo Tanenbaum (2003), a comunicação digital sem fios não é uma ideia nova, pois, a produtividade já não se limita a um local de trabalho fixo ou a um período de tempo determinado. Agora, o que as pessoas querem é se manter conectadas a qualquer hora e em qualquer lugar. Estas redes, podem ser divididas em três categorias principais:

- **Interconexão de sistemas**: para interconectar componentes de um computador usando rádio de alcance limitado;
- **LANs sem fios (WLAN)**: sistema em que todo o computador tem um modem de rádio e uma antena por meio dos quais pode se comunicar com outros sistemas;
- **WANs sem fios**: sistemas geograficamente distribuídos, a rede de rádio utilizada para telefonia celular é um exemplo.

Além da flexibilidade que as WLANs oferecem, outro benefício importante é o custo reduzido. Um exemplo disso é a mudança de uma empresa para um novo prédio que não tem nenhuma infra-estrutura cabeada. Neste caso, a economia resultante do uso de WLANs pode ser ainda mais notável, pois assim, evita o custo de passar cabos por paredes.

Para Carissimi (2009), é muito comum hoje em dia encontrar em locais públicos, no local de trabalho, na universidade, em casa, acesso a Internet por intermédio de redes locais sem fio (*wireless* LAN) 802.11. Existem muitas tecnologias e padrões para as redes sem fio. Neste projecto, irá se focar apenas na tecnologia IEEE 802.11, também conhecida como *Wi-Fi*.

Na realidade, o IEEE 802.11 é composto por um conjunto de padrões, entre eles 802.11a, 802.11b e 802.11g, que possuem muitas características em comum as quais se destacam na tabela abaixo.

Tabela 2: Comparação entre os padrões WLAN [Ross, 2008]

Padrão	Frequência	Largura de banda	Alcance	Características
802.11a	5 GHz	54 Mbps	50 Metros	Altas taxas de comunicação
802.11b	2.4 GHz	11 Mbps	100 Metros	Mais amplamente utilizado no mercado
802.11g	2.4 GHz	54 Mbps	100 Metros	Novo padrão compatível com 802.11b.

Como mencionado anteriormente, essas redes também utilizam uma certa topologia. A comunicação numa topologia sem fio é feita computador a computador através do uso de uma frequência comum nos dispositivos em ambos computadores.

Para suportar o parágrafo acima, Ross (2008) afirma que, a implementação mais comum da topologia sem fio é a que utiliza RF, baseada no padrão IEEE 802.11b, que utiliza a faixa de 2.4 GHz do espectro de frequências.

Ainda, para Ross (2008), há basicamente dois tipos de implementação:

- **Redes RF *ad hoc*** – nesta rede, os computadores utilizando dispositivos RF (*transceivers*), se conectam mutuamente utilizando uma frequência comum de conexão. Quando um computador entra no raio de alcance do outro computador, cada um passa a enxergar o outro, permitindo assim a comunicação entre eles.
- **Redes RF multiponto** – nesta rede, existem pontos de conexão denominados *wireless access points* (WAP) que conectam computadores com dispositivos RF a uma rede convencional. Este sistema é o mais utilizado em escritórios e também no acesso a Internet em redes metropolitanas.

A principal vantagem desta topologia é exactamente o fato dela trabalhar sem fio, pois permite a mobilidade dos computadores principalmente em ambientes amplos e abertos como armazéns e pátios. A topologia sem fio está a ganhar mercado graças ao crescimento da utilização dos dispositivos móveis tais como *laptops*, celulares e *tablets*.

Para Ross (2008), o principal problema desta topologia é a segurança da comunicação. Pelo fato da comunicação sem fio poder ser capturada por qualquer receptor sintonizado na mesma frequência da comunicação, torna-se necessário que exista um mecanismo adicional de segurança na implementação desta topologia tal como a criptografia da comunicação que será visto neste projecto logo a posterior.

2.4 Segurança da informação

A segurança é um assunto abrangente e inclui diferentes tipos de problemas, pois esta preocupa-se em garantir que pessoas mal-intencionadas não interceptem mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que não estão autorizados a usar. A maior parte dos problemas é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou até mesmo prejudicar alguém, (TANENBAUM, 2003).

Vários autores definem segurança da informação, entretanto e segundo Oliveira (2001), a segurança da informação define-se como o processo de protecção de informações e activos digitais armazenados em computadores e redes de processamento de dados. A segurança da informação é um assunto complexo e pode abranger várias situações: erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, causas da natureza e outras.

Entretanto, a segurança não é uma questão técnica, mas sim uma questão estratégica e humana. Não adianta obter uma série de dispositivos de *hardware* e *software* sem formar e consciencializar o nível administrativo da empresa e seus funcionários.

Mais uma vez, para Oliveira (2001), os elementos básicos da segurança da informação são:

- **Confidencialidade**: proteger informações confidenciais contra revelação não autorizada ou captação compreensível.
- **Disponibilidade**: garantir que informações e serviços vitais estejam disponíveis quando requeridos;
- **Integridade**: manter informações e sistemas computadorizados, entre outros activos, exactos e completos.

Posto isso, com a segurança da informação obtêm-se a garantia de que a informação estará disponível para acesso no momento desejado, podendo garantir também o sigilo, autenticidade, controlo de acesso e não repúdio das informações.

Em geral, os profissionais na área afirmam que nenhum sistema é seguro na sua totalidade.

Quando se fala de segurança, é necessário considerar certos aspectos. Guimarães (2006), considera 3 aspectos de segurança da informação:

- **Ataques de Segurança** - quais queres acções que possam comprometer a disponibilidade, integridade, sigilo e autenticidade duma informação pertencente a uma organização;

- **Mecanismos de segurança** - mecanismos projectados para detectar, prevenir ou se recuperar de um ataque de segurança.
- **Serviços de Segurança** - funções que aumentam o nível de segurança dos sistemas de processamento de dados e das transmissões de informação em uma Organização. Estes serviços podem utilizar um ou mais mecanismos de segurança.

A segurança deve ser prioridade para qualquer um quando o assunto é administração e acesso a redes de telecomunicações. Portanto, surge necessidade de fazer um estudo em segurança de redes, sobretudo nas redes sem fio que é o foco do projecto.

2.5 Segurança nas redes sem fio

Se já é difícil manter a segurança em uma rede cabeada, torna-se ainda mais difícil no caso de uma rede sem fio. Estas redes usam ondas electromagnéticas como meio de acesso, o que torna difícil controlar a sua abrangência e, podendo facilmente ultrapassar os limites físicos dum determinado estabelecimento. Para Biersdorfer (2011), na maioria das vezes isso não é nenhum problema, a menos que alguém esteja oculto nas proximidades, e saiba roubar dados pelo ar.

A preocupação com a segurança é ainda mais preocupante quando se trata de redes empresariais. Para estes, falhas na segurança podem trazer consequências desastrosas, principalmente se estiverem envolvidas informações financeiras ou estratégias de marketing relacionadas a clientes.

Quando se fala de segurança nas redes sem fio, é necessário tomar em consideração diversos pontos chaves:

- As ameaças para a segurança;
- Os protocolos de segurança;
- A criptografia;
- O acesso WLAN;
- Os métodos de autenticação**.**

2.5.1 Ameaças para a segurança nas redes sem fio

De acordo com Costa D. (2008, pág. 134), "Uma ameaça de segurança é qualquer coisa que possa afectar a confidencialidade, a integridade, a autenticidade e a disponibilidade de um sistema", pode se assim concluir que, uma violação de segurança pode provocar danos irreparáveis a uma determinada rede.

Para Bueno (2005), dentre algumas ameaças, destaca-se o conceito de acesso não autorizado. Há três categorias principais de ameaças que levam ao acesso não autorizado:

- ***War drivers*** - Localizam redes "Abertas", usam-nas para obter acesso livre a Internet;
- ***Hacker* e *crackers*** - Exploram medidas frágeis de privacidade para ver informações confidenciais de WLAN e até mesmo invadir WLANs. Enquanto os *hackers* usam a sua inteligência para o bem, os *crackers* usam para o mal, prejudicando os outros;
- **Funcionários** - Conectam APs/*gateways* da classificação de consumidor em portas *Ethernet* da empresa para criarem as próprias WLANs.

Quando se fala de ameaças de segurança nas redes sem fio, um dos ataques muito mencionados é o ataque de interceptação. Para Guimarães (2006), estes ataques tem como objectivo capturar o que está sendo transmitido sem que o sistema perceba. Este ataque gera cópias de informações, arquivos ou programas não autorizados. Um dos principais tipos de ataques desta categoria é o *man-in-the-middle*, onde o invasor simula ser o parceiro de ambas as partes envolvidas na conexão, assumindo a identidade de um usuário válido.

Segundo Pellejero, Andreu e Lesta (2006), para levar a cabo este ataque é necessário que o dispositivo atacante tenha duas interfaces WLAN: uma para simular um ponto de acesso (AP) e outra para simular um usuário válido.

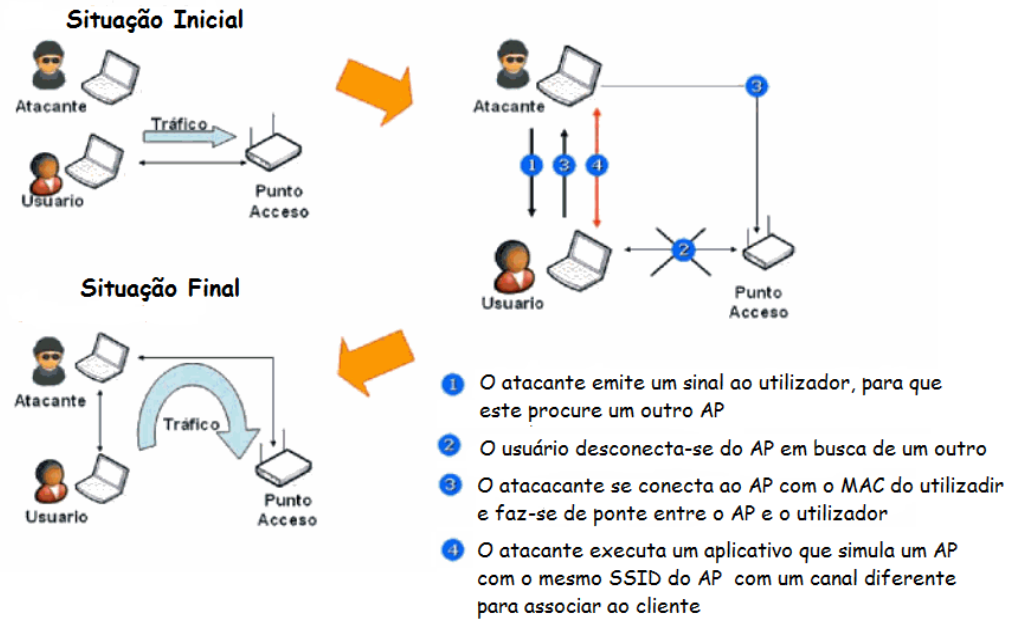

Figura 2: Ataque *Man In The Middle*. Adaptado de [PELLEJERO; ANDREU; LESTA, 2006]

Outra forma bastante usual de um ataque de interceptação, segundo Oliveira (2006), é a utilização de uma ferramenta *Sniffer*[1]. Desta forma, um invasor pode facilmente obter ou adulterar informações confidenciais de uma corporação, beneficiando-se das fragilidades encontradas em um ambiente de rede.

Em uma LAN, o invasor precisa conseguir aceder a rede local fisicamente para colocar de forma lógica um dispositivo na topologia. Com uma WLAN, as ondas de rádio emitidas por pontos de acesso permitem a conexão.

Das várias pesquisas feitas é possível concluir que, impedir um ataque como o de interceptação depende da sofisticação da infra-estrutura da WLAN e do monitoramento das actividades na rede. Este processo começa com a identificação de dispositivos legítimos na WLAN, pois, para isso é necessário autenticar os utilizadores na WLAN. Quando todos os utilizadores legítimos se tornam conhecidos, é possível monitorar a rede para detectar dispositivos e tráfego que não devem estar nela. Um PA mais ocupado que o normal, pode alertar o administrador de possível tráfego sem autorização.

2.5.2 Protocolos de segurança nas redes sem fio e criptografia

Segundo Montico (2009), depois de implementada uma rede sem fio, uma das decisões fundamentais é escolher se a rede será aberta ou fechada. Um dos primeiros padrões de encriptação a ser usado nessas redes, foi o WEP, este foi validado em 1999, sendo parte do padrão IEEE 802.11 e portanto usado por produtos desse padrão. Apesar de ser muito usado até aos dias de hoje, ele possui muitas vulnerabilidades e falhas, o que permite que *crackers* façam ataques bem-sucedidos à rede, desde captura de mensagens até autenticação na rede.

A primeira coisa feita pelas empresas para combater a fragilidade das chaves WEP compartilhadas foi tentar técnicas como disfarçar SSIDs e filtrar endereços MAC.

Para Jobstraibizer (2010), as falhas com a criptografia das chaves WEP compartilhadas foram duas:

- O algoritmo usado para criptografar os dados era descoberto facilmente;
- A escalabilidade era um problema. As chaves WEP de 32 *bits* foram gerenciadas manualmente, sendo acedidas manualmente pelos utilizadores, de maneira frequentemente incorrecta, criando chamadas aos serviços de suporte técnico.

---

[1] *Sniffer* - "programa ou dispositivo que controla o tráfego da rede e captura informações transmitidas por ela" (OLIVEIRA, 2006, pág. 131).

Ainda, para Jobstraibizer (2010), após as falhas na segurança baseada em WEP, houve um período intermediário de medidas de segurança. Enquanto isso, o algoritmo de criptografia TKIP foi criado e vinculado ao método de segurança *Wi-Fi Alliance Wi-Fi Protected Access* (WPA).

Actualmente, o padrão que deve ser seguido na maioria das redes empresariais é o 802.11i. Ele é como o padrão *Wi-Fi Alliance* WPA2. Para empresas, o WPA2 inclui uma conexão com uma base de dados RADIUS.

Dois mecanismos de criptografia de nível empresarial especificados pelo 802.11i são certificados como WPA e WPA2 pela *Wi-Fi Alliance*: o *Temporal Key Integrity Protocol* (TKIP) e a criptografia (AES).

TKIP é o método de criptografia certificado como WPA. Ele dá suporte para equipamentos de WLAN herdados direccionando-se as falhas originais associadas com o método de criptografia 802.11 WEP. Usa o algoritmo de criptografia original usado pelo WEP. Entretanto, para Lee e Choi (2008), o TKIP tem duas funções principais:

- Criptógrafa o *payload* da Camada 2;
- Executa uma verificação de integridade da mensagem (MIC) no pacote criptografado. Isso ajuda a impedir a adulteração de uma mensagem.

O AES tem as mesmas funções do TKIP, mas usa dados adicionais do cabeçalho MAC que permitem que *hosts* de destino verifiquem se os *bits* não criptografados foram adulterados. Além disso, ele adiciona um número de sequência ao cabeçalho dos dados criptografados.

Em alguns pontos de acesso, é possível não ver o WPA ou WPA2. Em vez disso, é possível ver as referências a algo chamado chave pré-compartilhada (PSK). Alguns tipos de PSK são:

- PSK ou PSK2 com TKIP é o mesmo que WPA;
- PSK ou PSK2 com AES é o mesmo que WPA2.

Tabela 3: Funções do TKIP e do AES. Adaptado de [Jobstraibizer, 2010]

TKIP - *Temporal Key Integrity Protocol*	**AES - *Advanced Encryption Standard***
• Criptógrafa acrescentando codificação de bit crescentemente complexa a cada pacote; • Baseado na mesma cifra (RC4 - Cifra de fluxo) como WEP.	• Nova cifra usada em 802.11i; • Baseado em TKIP com recursos adicionais que aprimoram o nível de segurança proporcionado.

2.5.3 O acesso a rede local sem fio

Segundo Guimarães (2006), a segurança de acesso a rede é baseada em uma arquitectura modular denominada Arquitectura AAA por possuir três componentes básicos, a saber:

- ***Authentication*** **(Autenticação)** - requer que os utilizadores provem que são realmente quem dizem dizer;
- ***Authorization*** **(Autorização)** - após a autenticação do usuário, os serviços de autorização decidem quais recursos os utilizadores podem acessar e quais operações podem realizar;
- ***Accounting*** **(Contabilidade)** - regista o que o utilizador realmente faz, o que ele acedeu e por quanto tempo, para fins de contabilidade e auditoria, mantendo um registo de como os recursos de rede são utilizados. A contabilidade pode ser realizada também para controlar o acesso à rede e detectar intrusões.

Comummente, muitas referências bibliográficas sobre este assunto referenciam-se aos métodos AAA como sendo métodos de autenticação, isso porque praticamente todos os métodos AAA possuem suporte a autenticação, porém, nem sempre um método de autenticação possui métodos de autorização ou contabilidade. Seguindo este modelo, discorreremos sobre alguns métodos de autenticação importantes para um melhor entendimento dos processos que podem existir na implementação de um servidor RADIUS.

2.6 Métodos de autenticação

A informação de autenticação poderá estar sob o controle de duas ou três entidades. Quando o esquema de autenticação está sob o controle de duas entidades, a entidade que se está autenticado e a entidade autenticadora, o esquema é chamado *Two-Party Authentication*. Se for utilizada uma terceira entidade, que geralmente possui o papel de validar ou certificar a autenticidade das outras entidades, este esquema é chamado de *Trusted Third-Party Authentication* (SILVA, 2003 apud GUIMARÃES, 2006).

Para Guimarães (2006), a autenticação *Two-Party* ainda se subdivide em dois esquemas: o de uma via (*one-way*) e o de duas vias (*two-ways*). No primeiro esquema, uma entidade geralmente cliente, se autentica em um servidor, sem que este precise se autenticar no cliente. No esquema de duas vias, todas entidades devem se autenticar mutuamente. Em ambas situações, a informação ou parte da mesma que é compartilhada entre as duas entidades participantes da comunicação, é chamada *Shared Secret*. Os principais métodos de autenticação *Two-Party* conhecidos são: *Shared Secret* (Chave Secreta Compartilhada) e *Challenge/Response*. O *Shared Secret*, pela sua simplicidade, é um dos esquemas de

autenticação mais utilizados em redes onde o servidor lança um desafio a uma outra entidade, esperando uma resposta previamente acordada entre eles. Os principais protocolos de autenticação que sustentam estes métodos são:

- PAP (*Password Authentication Protocol*);
- CHAP (*Challenge Handshake Authentication Protocol*);
- EAP (*Extensible Authentication Protocol*), o TACACS+ e o RADIUS.

Como mencionado, a autenticação *Trusted Third-Party* utiliza uma terceira entidade que proverá um conjunto de credenciais. Este método é mais adequado à construção de redes VPNs mais robustas e com maior número de utilizadores. Os principais métodos de autenticação *Third-Party* conhecidos são: *Kerberos* e a infra-estrutura de Chave Pública X.509 (PKI), que não serão detalhadas neste projecto.

2.6.1 *Password Authentication Protocol* (PAP)

Estes foram um dos primeiros protocolos desenvolvidos para realizar autenticação. É um método que utiliza o protocolo PPP (protocolo ponto-a-ponto), geralmente adoptado em conexões discadas, para realizar a autenticação do cliente. Neste esquema, a senha é enviada a um NAS (*Network Authentication Service*) sob a forma de texto simples, que posteriormente passa por uma validação de informações. (GUIMARÃES, 2006)

A figura 3, ilustra os passos de trocas de mensagens no protocolo PAP:

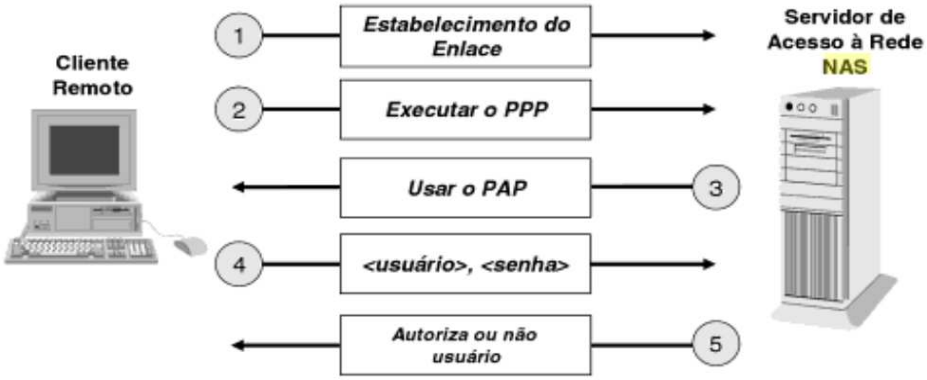

Figura 3: Etapas de autenticação do PAP sobre o PPP [WENSTROM, 2002 apud GUIMARÃES, 2006]

Ainda, para Guimarães (2006), as características principais do PAP são:

- Actua em nível de enlace;
- Não possui criptografia do envio do nome do usuário e da senha para o NAS;
- A autenticação é feita somente no início da conexão;

- Não possui controlo sobre o número de tentativas da conexão;
- Não oferece nenhuma protecção contra ataques de reprodução ou tentativas de erros repetidos.

2.6.2 *Challenge Handshake Authentication Protocol* (CHAP)

Simpson (1996), através da RFC 1994, define o CHAP (*Challenge Handshake Authentication Protocol*) como sendo um método utilizado pelo protocolo PPP, porém, mais complexo que o PAP, pois a senha real do utilizador não atravessa o canal de comunicação. Ele é um protocolo de autenticação bastante utilizado nos ambientes Linux.

O método de autenticação deste protocolo ocorre em três fases (*handshake* de três vias). O *handshake* de três vias ocorre após as etapas estabelecidas do *link*. A figura 4 ilustra as etapas de autenticação do protocolo CHAP sobre o PPP.

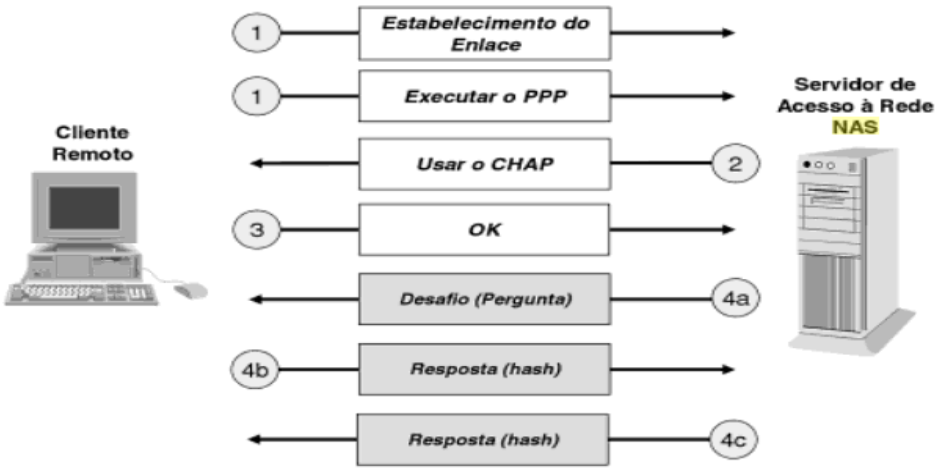

Figura 4: Fases do protocolo de Autenticação por Desafio (CHAP) [WENSTROM, 2002 apud GUIMARÃES, 2006]

Após as primeiras 3 etapas, ocorre o processo de *handshake* (etapa 4).

A primeira fase do *handshake* (4a), que ocorre após o estabelecimento do enlace (*link*), sempre iniciando do NAS, é o envio de um desafio por parte do autenticador (terminologia usada pela RFC 1994 para denominar o servidor de autenticação) para o cliente, seleccionando de forma aleatória dentro de um conjunto já preestabelecido de desafios e respostas.

Na segunda fase do *handshake* (4b), o cliente utiliza uma função *hash*[2] (normalmente o MD5[3]) calculado sobre o desafio proposto para posteriormente devolver a resposta ao servidor.

Na terceira fase do *handshake* (4c), o servidor valida a resposta (enviada pelo cliente), verificando-a contra seu próprio cálculo do valor *hash* esperado. Ele decifra a mensagem enviada através da senha do utilizador contida na sua base de dados, autorizando-o ou não.

É importante ressaltar que, em intervalos randômicos, o autenticador (servidor) pode enviar um novo desafio ao cliente, repetindo assim todas as fases mencionadas na etapa 4, e ao contrário do PAP, antes de enviar uma solicitação de conexão ao NAS, ele já faz a criptografia dos dados utilizando o MD5 (*Message Digest* 5).

Para Simpson (1996) apud Guimarães (2006), o protocolo CHAP possui as seguintes características:

- Depende de uma "senha/chave secreta" conhecida apenas pelo servidor e pelo cliente, porém, esta não é enviada através do *link*;
- É um método *one-way*, isto é, apenas um lado da comunicação se autentica. Este pode ser facilmente adaptado para uma autenticação mútua utilizando o mesmo "segredo".
- A autenticação pode ser repetida durante a conexão com o envio de diferentes desafios, escolhidos aleatoriamente, o que pode ser interessante para evitar ataques de *replay*, onde o invasor pode tentar se autenticar utilizando uma resposta de um desafio capturado anteriormente.
- As senhas dos utilizadores não são armazenadas de forma criptografada no servidor, pois ele necessita da senha em texto simples para descriptografar o *hash* recebido do cliente.
- Os dados enviados entre servidor e cliente são criptografados;
- Possui a finalidade apenas de permitir ou negar o acesso à rede e não possibilita definir níveis de permissões para determinados utilizadores.

---

[2] Uma função *hash* é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. (PISA, 2012)

[3] Segundo Flores (2004), o MD5 é um algoritmo para obter *hash* de mensagens. O algoritmo aceita como entrada uma mensagem de tamanho arbitrário e produz como saída 128 bits que representam um valor de *hash* da mensagem de entrada e que pode ser encarado como uma assinatura digital da mensagem.

2.6.3 *Extensible Authentication Protocol* (EAP)

Através da RFC 2284, Blunk e Vollbrecht (1998), descrevem o EAP (*Extensible Authentication Protocol*) como sendo um protocolo geral para autenticação PPP que suporta múltiplos mecanismos de autenticação. Ele funciona como um mecanismo de negociação de protocolos de autenticação. Os protocolos PAP e CHAP, vistos anteriormente, são mecanismos de autenticação simples, escolhidos na fase de *link* (protocolo LCP). No caso do EAP, ele não selecciona um mecanismo específico de autenticação. Na fase de controlo de *Link* (LCP) ele posterga a escolha até a fase de autenticação, o que permite que o servidor possa solicitar uma quantidade maior de informações ao cliente antes de determinar o mecanismo de autenticação específico.

Blunk e Vollbrecht (1998), definem várias formas de autenticação para o EAP, entre elas ressaltam-se as seguintes:

- ***MD5 Challenge*** - é análogo ao protocolo PPP CHAP, porém específica que os desafios e as respostas são construídos através de funções *hash* MD5;
- ***One-Time-Password*** - quando a senha é gerada uma única vez para cada sessão;
- ***Generic Token Card*** - gera-se uma combinação numérica aleatória para cada sessão.

A figura 5. apresenta um esquema de negociação e autenticação em um ambiente que utiliza EAP após a fase de controle do enlace (*link*).

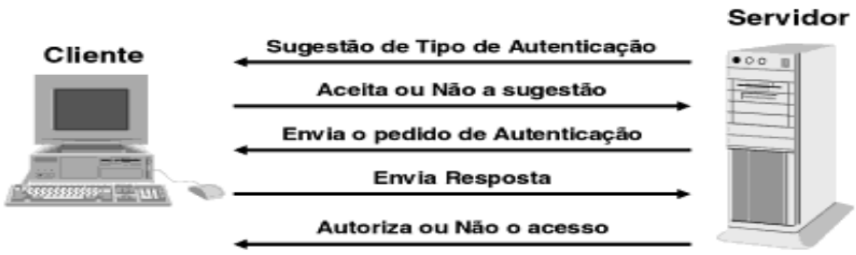

Figura 5: Protocolo de autenticação EAP [SILVA, 2003 apud GUIMARÃES, 2006]

Algumas observações quanto ao EAP são pertinentes. A primeira é que a autenticação pode ser feita *one-way* ou *two-ways*, porém não existe obrigação do mesmo método de autenticação ser aplicado em ambas as direcções, sendo aceitável o uso de diferentes protocolos em cada direcção. A segunda é que o EAP é vulnerável a ataques, pois é um mecanismo que permite vários métodos de autenticação. De acordo com Silva (2003) apud Guimarães (2006), este é o motivo pelo qual cada vez menos este protocolo é utilizado como padrão de autenticação entre duas entidades.

2.6.4 RADIUS e TACACS+

Diversos padrões de base de dados de segurança foram criadas para fornecer controlo de acesso uniforme para equipamentos e utilizadores de rede. Dos principais produtos desenvolvidos para este fim, destacam-se: RADIUS, TACACS+ e o *Kerberos*.

Segundo Guimarães (2006), o RADIUS foi desenvolvido primeiramente pela *Lucent Techonologies* como uma solução para prover autenticação e gestão de clientes remotos conectados através de linhas discadas. Em Janeiro de 1997, o RADIUS foi padronizado pela IETF através da RFC 2058. Posteriormente, o protocolo RADIUS teve dezenas de outras RFCs que o alteraram ao longo de sua existência, tornando a sua definição inicial totalmente obsoleta. Actualmente, ele é descrito pela RFC 2865, e pela RFC 2866 que define o serviço de contabilidade do RADIUS.

A solução RADIUS baseia-se em uma arquitectura cliente-servidor, que adiciona um elemento de rede chamado *Network Access Server* (NAS), ou Servidor de Acesso Remoto, que possui como principais funções: o estabelecimento da conexão remota via linha discada, a gestão dos pedidos de conexão e a liberação ou não dos pedidos.

Ainda, para Guimarães (2006), em vários ambientes o NAS está pré-configurado para realizar todo o processo de autenticação, pois pode conter a própria base de dados de utilizadores e senhas. Apesar dessa facilidade, esta configuração é um tanto incomum, pois nas corporações, em geral, existem servidores específicos de autenticação que centralizam todos os serviços de autenticação, não somente a autenticação dos clientes via linha discada mas também dos clientes internos da Intranet. Assim, é mais viável que se utilize um único servidor para autenticação.

Desta forma, o NAS pode e deve ser configurado para trabalhar como cliente de um servidor RADIUS. Entretanto, cada pedido de autenticação passa pelo NAS, que passa ao servidor RADIUS, que recebe um retorno do servidor e o encaminha ao cliente.

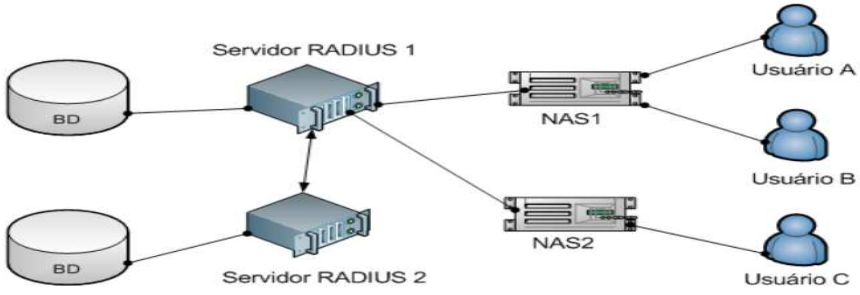

Figura 6: Possibilidade de requisição de acesso a um serviço - 1 [Macêdo, 2012]

O RADIUS está implementado em várias plataformas, inclusive no Linux.

O cliente RADIUS e o servidor de segurança RADIUS comunicam-se utilizando os seguintes pacotes: *Acces-Accept*, *Access-Request*, *Access-Accept*, *Access-Reject* e *Access-Challenge*. A seguir descrevemos os principais passos ocorridos quando um cliente tenta realizar *login* e autenticar-se em um NAS.

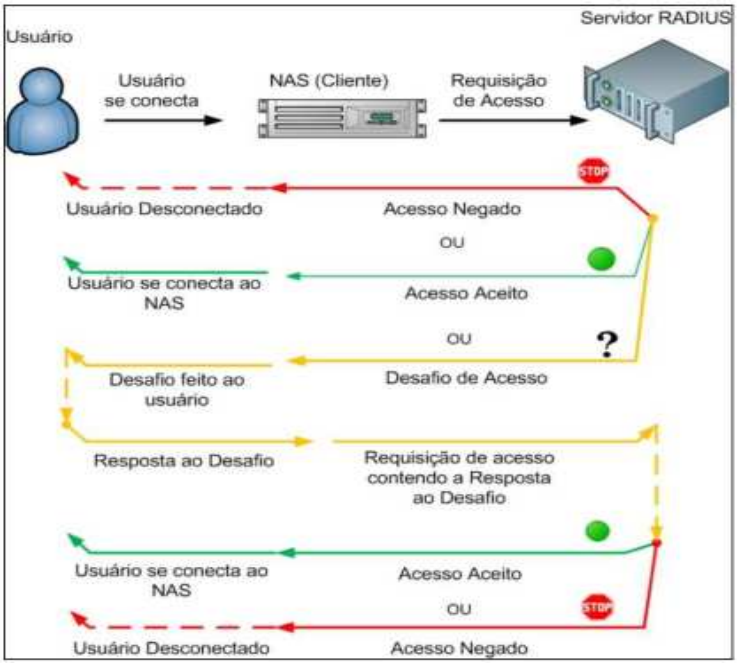

Figura 7: Possibilidade de requisição de acesso a um serviço - 2 [Carvalho, 2008]

Por outro lado, existe o TACACS+. Vários autores descrevem este de maneiras semelhantes. Para Carroll (2004), o TACACS+ é um protocolo recente fornecendo informações contabilísticas pormenorizadas e controle administrativo flexível sobre os processos de autenticação e autorização. Esta é uma implementação proprietária da Cisco.

Finseth (1993), através da RFC 1492, descreve o TACACS+ como sendo um aplicativo AAA para servidores de segurança e um protocolo que permite o controle central de utilizadores que tentam obter acesso através de um NAS, roteador ou outro equipamento de rede que suporte o TACACS+.

Sendo assim, pode se concluir que as funções do TACACS+ são muito semelhantes às do RADIUS, porém, para Guimarães (2006), eles apresentam algumas diferenças, das quais se destacam na tabela abaixo:

Tabela 4: Comparação entre TACACS+ e RADIUS. Adaptado de [GUIMARÃES, 2006]

Funcionalidade	**TACACS+**	**RADIUS**
Suporte AAA	Separa os três serviços AAA	Combina autenticação e autorização e separa a contabilidade
Protocolo de transporte	TCP	UDP (porta 1812 ou 1645)
Pergunta/Resposta	Bidireccional	Unidireccional (somente do Servidor RADIUS para o cliente)
Integridade de Dados	Todo o pacote TACACS+ é criptografado	Somente a senha do usuário é criptografada

Adiante, serão descritas as soluções RADIUS existentes no mercado e será escolhida numa fase posterior a melhor solução RADIUS que se enquadra no projecto em questão.

2.7 Soluções RADIUS existentes

Existem no mercado muitas soluções para servidores RADIUS. Segundo Hugo (2009), o freeRADIUS é o servidor RADIUS mais utilizado para sistemas Linux. Este é responsável pela autenticação de pelo menos um terço dos utilizadores na Internet. Os restantes utilizadores encontram-se divididos entre os restantes servidores, destacando-se entre eles o Cisco ACS (*Access Control Server*) e o Microsoft IAS (*Internet Authentication Service*).

2.7.1 freeRadius

De acordo com Walt (2011), pode-se dizer que o freeRadius, é uma implementação de RADIUS modular, *open source,* de alta *performance* e rica em opções e funcionalidades. Esta inclui servidor, cliente, bibliotecas de desenvolvimento e muitas outras utilidades.

Nesta implementação, cada cliente deverá ser correctamente configurado de modo a comunicar com o servidor instalado. Os clientes podem ser computadores ou APs.

Esta solução suporta à limitação do número máximo de acessos simultâneos, capacidade de inserir mais do que um valor por omissão e capacidade de funcionar como um servidor *proxy.*

O freeRADIUS pode ser implementado em servidores Linux.

2.7.2 Cisco Access Control Server

Para Hugo (2009), o ACS, é uma política de controlo de acesso que proporciona um ambiente centralizado de controle de autenticação, autorização e contabilização de acesso de utilizadores a recursos de rede. Este suporta simultaneamente múltiplos cenários que incluem:

- **Dispositivo de administração**: autentica administradores e comandos de autorização;
- **Acesso Remoto**: funciona com VPN e outros dispositivos de acesso a redes remotas para reforçar as políticas de acesso;
- ***Wireless***: Autentica e autoriza utilizadores e *hosts wireless* e reforça as políticas de segurança específicas de *wireless*;
- **Controlo de admissão na rede**: comunica com servidores de postura e auditoria para reforçar as políticas de controlo de admissão.

O Cisco *Secure* ACS possui uma interface WEB simples de usar para simplificar a gestão centralizada de AAA para dispositivos Cisco dentro da empresa. Este pode suportar grandes redes e é implementado em servidores *Windows.*

2.7.3 Microsoft Internet Authentication Service

O IAS, é a implementação da *Microsoft* de um servidor RADIUS, o que pode servir tanto como um servidor RADIUS e um *proxy* RADIUS.

Vários autores descrevem o IAS de maneira semelhante. Recorrendo para a descrição feita por Huntler e Dinerman (2006), ao configurar um IAS como um servidor RADIUS, este pode realizar a autenticação, autorização e contabilidade para diferentes tipos de acesso à rede. O IAS pode ser usado ainda para configurar e proteger WLANs, bem como uma VPN. Para além disso, é possível usar o IAS para criar uma zona de "quarentena", que vai impedir que clientes remotos acessem sua rede até que tenham passado por alguns diagnósticos, como verificação dos níveis de correcção e o *status* do antivírus. Funcionando como *proxy*, o IAS reencaminha as mensagens de autenticação e autorização para outros servidores RADIUS.

2.8 Resumo

Neste capítulo foram abordados os conceitos que apoiam o alcance dos objectivos propostos. Descreveu-se primeiramente os conceitos essenciais de uma rede de computadores até ao foco essencial do projecto, onde entram os conceitos relevantes a segurança de redes de computadores, sobretudo nas redes sem fio, dando conhecer as ameaças, os protocolos, criptografias usadas e os métodos de autenticação nessas redes.

CAPÍTULO 3 - MARCO CONTEXTUAL DA INVESTIGAÇÃO

3.1 Introdução

A segurança de rede consiste na política que o administrador de rede segue para poder prevenir assim como monitorar o acesso não autorizado, uso incorrecto, modificação e restrição ao acesso da rede de computadores e dos seus recursos.

Sendo assim, é fundamental que o desenvolvedor do projecto conheça o contexto a qual será implementado o serviço RADIUS, tendo total domínio dos processos actuais existentes, conhecendo os passos fundamentais para a execução dos mesmos e as suas limitações para possibilitar o melhoramento.

Neste capítulo é feita a descrição do actual modo de acesso à rede *wireless* do ISUTC, resultante de entrevistas feitas aos funcionários do Sector de Informática desta instituição. Para tal, é necessário conhecer a instituição, seus princípios, e limitações que os administradores enfrentam ao disponibilizarem o acesso a esta rede para os utilizadores.

3.2 O ISUTC

Segundo a Transcom (2014), o ISUTC é uma instituição de ensino superior privada e está em actividade desde 2000. É eminentemente uma escola de Engenharia que privilegia as temáticas do sector dos Transportes e Comunicações e suas envolventes. Por esse motivo, esta também dedica-se a gestão, uma área crucial com intervenção horizontal em todos os sectores de actividade.

3.2.1 Missão e visão

A sua missão é a criação e difusão da ciência, da cultura e da tecnologia, exercida nos domínios do estudo, da docência, da investigação e da prestação de serviços, em harmonia com os desígnios da identidade nacional e do desenvolvimento da comunidade nacional e internacional.

Sua visão é a de tornar-se uma instituição de ensino superior líder no país, nas áreas em que realiza formação e investigação e presta serviços, com particular destaque para as da engenharia e da gestão, ocupando a posição de melhor escola superior de engenharia no país.

O ISUTC foi instituído pela Transcom, SA (Transcom, Sociedade de Formação, Consultoria e Auditoria em Transportes e Comunicações, SA), um projecto multifacetado que abrange três áreas de actividade:

- ITC – Instituto de Transportes e Comunicações, instituto médio técnico-profissional privado (desde 1998);
- ISUTC – Instituto Superior de Transportes e Comunicações (desde 2000);
- Consultoria.

Como toda instituição, organização ou empresa, o ISUTC também é constituído por pessoas. Os utilizadores da rede de computadores do ISUTC actualmente encontram-se registados em um servidor de base de dados o qual está instalado o serviço de directórios LDAP, concretamente o OpenLDAP.

3.3 OpenLDAP

OpenLDAP é um *software* livre de código aberto que implementa o protocolo LDAP. O projecto de desenvolvimento do OpenLDAP teve início em 1998 por Kurt Zeilenga e posteriormente Howard Chu, juntou-se ao projecto. (BUTCHER, 2007)

A principal funcionalidade desta ferramenta, é possuir a capacidade de fornecer a autenticação aos utilizadores, fazendo o uso da sua base de dados. A autenticação de todos os serviços de rede se concentra em uma única árvore de informações.

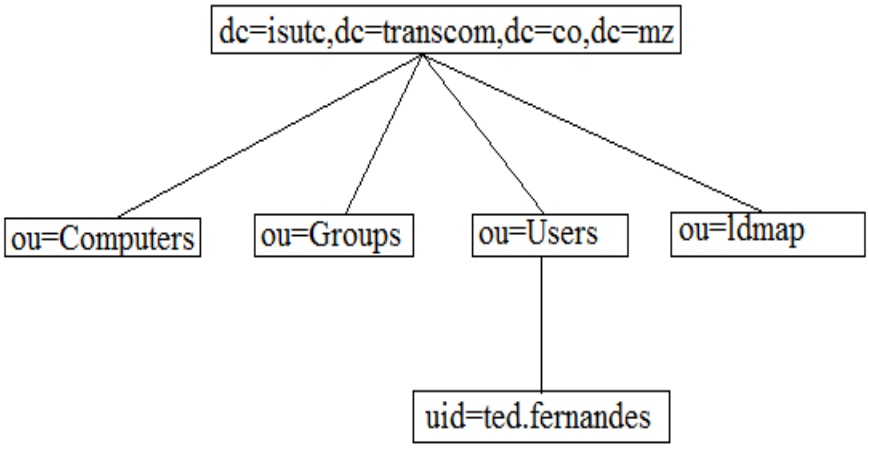

Figura 8: Directório de informação do LDAP no ISUTC [Fonte: Autor]

O atributo para identificar a entrada representada acima (DN), seria:
uid=ted.fernandes, ou Users, dc=isutc,dc=transcom,dc=co,dc=mz.

No ISUTC uma entrada de utilizador no LDAP é constituída pelos seguintes atributos:

Tabela 5: Atributos obrigatórios para a constituição de uma entrada no OpenLDAP do ISUTC [Fonte: Autor]

Atributo	**Descrição**
Uid	Id do utilizador, corresponde ao primeiro.ultimoNome no ISUTC (para alunos)
Cn	*CommonName*, corresponde ao nome do utilizador
Sn	*SurName*, corresponde ao último nome do utilizador
User name	Nome do utilizador usado para autenticação
userPassword	Senha do utilizador
departmentNumber	Corresponde a turma do estudante utilizador
displayNames	Nome visualizado
Email	Email do utilizador
gidNumber	Id do grupo que o utilizador esta incluso
sambaSID	Valor que possibilita verificar se o utilizador pode autenticar em um certo domínio

Uma conta de utilizador no ISUTC segundo os funcionários entrevistados é uma identificação atribuída ao utilizador, e que consiste numa entrada no LDAP. Esta conta tem a função de proporcionar o acesso aos serviços existentes no ISUTC, como o serviço de correio electrónico, o serviço de ftp, o acesso as estações de trabalho, o serviço de apoio e aprendizagem mais conhecido como *Moodle*, o *chat* interno, dentre outros serviços.

Para entender os processos que são tomados ao conectar-se a rede *wireless* do ISUTC, é necessário antes, perceber como encontra-se estruturada a rede no geral.

3.4 Estrutura da rede do ISUTC

Segundo os entrevistados do Sector de Informática, o ISUTC dispõe de uma rede local baseada no modelo hierárquico da Cisco como é apresentada na figura 9.

Para Wolkartt (2012), este modelo foi idealizado e desenvolvido para simplificar o planeamento de uma rede confiável, escalável e menos dispendiosa. Em cada uma de suas camadas, há funções específicas que ajudam a ter um fácil entendimento de uma rede e, consequentemente, definir uma maneira apropriada de aplicar uma configuração, visto que grandes redes podem ser extremamente complexas e incluir múltiplos protocolos e tecnologias.

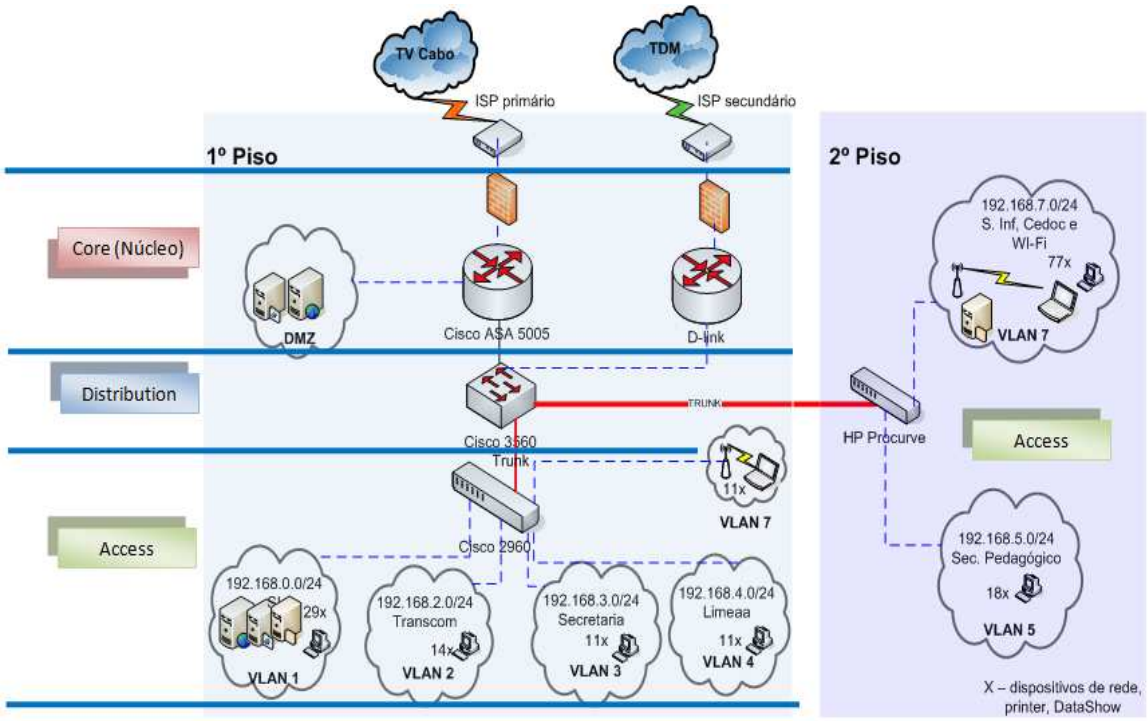

Figura 9: Rede de dados do ISUTC [Fonte: Sector de Informática do ISUTC]

Os entrevistados do sector de informática, afirmam que o ISUTC dispõe de equipamento Cisco e pessoas capacitadas para trabalhar com estes equipamentos até ao ponto de estruturar um modelo como o da figura acima apresentada.

Para entender o presente modelo implementado na rede de dados do ISUTC, simplesmente é necessário conhecer o papel que essas camadas desempenham na presente rede.

3.4.1 Camada de acesso

Na camada de acesso, dentro da rede de dados do ISUTC, é possível encontrar diferentes grupos de utilizadores com os seus correspondentes recursos:

- Funcionários (docentes a tempo inteiro, docentes a tempo parcial, estudantes trabalhadores, técnicos, pessoal da área administrativa e outros);
- Estudantes;
- Visitantes.

Não é possível proporcionar a esses diferentes tipos de utilizadores um acesso local a todos os serviços, como arquivos de *database*, armazenamento centralizado ou acesso à *Web* (WWW). Nestes casos, o tráfego de utilizadores que demandam estes serviços é desviado à próxima camada do modelo.

Segundo Wolkartt (2012), é na camada de acesso que os utilizadores se conectam à rede, assim como os recursos aos quais necessitam de aceder com mais frequência.

A camada de acesso, é ainda responsável por fazer interface com dispositivos finais como computadores, *laptops* e dispositivos móveis para poder fornecer acesso ao restante da rede. Na tabela abaixo, são referenciados alguns dispositivos da camada de acesso dentro da rede do ISUTC.

Tabela 6: Dispositivos de rede encontrados na camada de acesso na rede do ISUTC [Fonte: Autor]

ACCESS POINTS	
Modelo	**Localização**
D-Link Dir-615	Sector de Informática
LinkSys WAP54G	Cedoc
Cisco *Small Business* WAP4410N	2° Piso - Sector Pedagógico
SMC SMCWBR14S-N3	Sector de Informática
SWITCHES	
Modelo	**Localização**
Catalyst 2960	Cedoc
Dell PowerConnect 2324	Sector Pedagógico
Catalyst *express* 500	HelpDesk
Dell PowerConnect 2324	Limeaa

3.4.2 Camada de distribuição

É nesta camada onde é feita a filtragem de pacotes, ou seja, é feito o controlo para o acesso a determinados serviços de rede que o ISUTC oferece, pois é aqui onde determina-se que grupo de utilizadores ou que utilizador em específico pode ter ou não acesso a um determinado serviço, como por exemplo, o acesso directo à Internet, o FTP para a transferência de ficheiros e outros. Essa camada é responsável por controlar o fluxo do tráfego gerado na rede, usando políticas, e determinar domínios de *broadcast*, realizando funções de roteamento entre redes locais virtuais (VLANs) definidas na camada de acesso. As VLANs serão referenciadas em um ponto posterior neste capítulo para uma melhor compreensão.

Os s*witches* da camada de distribuição costumam ser dispositivos de alto desempenho que têm alta disponibilidade e redundância para assegurar a confiabilidade.

Tabela 7: Dispositivo de rede encontrado na camada de distribuição na rede do ISUTC [Fonte: Autor]

SWITCH Layer 3	
Modelo	**Localização**
Catalyst 3560	Sector de Informática

Para fortificar os parágrafos acima colocados, Wolkartt (2012) diz que, a camada de distribuição representa o ponto médio entre a camada de acesso e os serviços centrais da rede. A função primordial desta camada é realizar funções tais como roteamento, filtragem e acesso à WAN. Uma vez que a presente camada elege a rota, a requisição é enviada à camada *core*.

3.4.3 Camada core

A camada *core* é a que encarrega-se de desviar o tráfego o mais rápido possível, de forma confiável, aos serviços apropriados. Normalmente, o tráfego transportado se dirige ou provém de serviços comuns a todos os utilizadores. Estes serviços são conhecidos como globais ou corporativos, como o e-mail, o acesso à Internet e a videoconferência, (WOLKARTT, 2012).
Entretanto, pode se concluir que a presente camada na rede de dados do ISUTC é responsável por fornecer uma alta velocidade ao tráfego a ser transportado. Geralmente, nesta camada não é feito nenhum tipo de filtragem, pois, a filtragem exige que se cumprem certas condições e estas tais condições de um certo modo podem influenciar no atraso ao enviar um determinado pacote. A camada de núcleo deve ser altamente disponível e redundante, este agrega o tráfego de todos os dispositivos da camada de distribuição e deve ser capaz de encaminhar grandes quantidades de dados rapidamente. O dispositivo que pode ser encontrado nessa camada na rede de dados do ISUTC é apresentado na tabela abaixo:

Tabela 8: Dispositivo de rede encontrado na camada de núcleo no ISUTC [Fonte: Autor]

ROUTER	
Modelo	**Localização**
Cisco ASA 5505	Sector de Informática

3.5 VLAN (Virtual Local Network ou Virtual LAN)

A produtividade do utilizador e a capacidade de adaptação da rede são os principais responsáveis pelo crescimento e o sucesso dos negócios. Implementar a tecnologia VLAN permite a uma rede suportar metas comerciais com mais flexibilidade. Segundo Pillou (2013),

uma VLAN, é uma rede local que agrupa um conjunto de máquinas de maneira lógica e não física. A VLAN permite definir uma nova rede acima da rede física.

O ISUTC possui várias VLANs de forma a acarretar determinados benefícios primários:

- **Segurança** - grupos com dados confidenciais são separados do restante da rede, o que diminui riscos de violações das informações confidenciais. Como trata-se duma instituição de ensino, onde existem alunos e docentes, é muito claro perceber que, estes precisam de ter as suas informações separadas para garantir a confidencialidade. O presente caso é válido para os demais grupos de utilizadores presentes no ISUTC;
- **Redução de custo -** Resultante da menor necessidade das actualizações de redes caras e do uso mais eficiente da largura de banda e dos *uplinks* existentes. Um exemplo disso seria a compra de um *switch.* Em um mesmo *switch*, é possível configurar diferentes VLANs. É o que acontece no ISUTC.;
- **Desempenho mais alto -** Dividir as redes em vários grupos de trabalho lógicos (domínios de *broadcast*) reduz um tráfego desnecessário na rede e aumenta o desempenho. No ISUTC, se um funcionário da secretaria desejar trocar informações com um outro funcionário do mesmo departamento, o desempenho será melhor, pois a informação encontra-se dentro de um determinado domínio de *broadcast* muito menor comparado com um domínio de *broadcast* em que a informação tem que percorrer toda a rede no geral;

Tabela 9: Disposição das VLANs dentro do ISUTC [Fonte: Autor]

VLAN	**Departamento**
1	Sector de Informática
2	Transcom
3	Secretaria
4	Limeaa
5	Sector Pedagógico
7	Salas de Informática, Laboratórios, Cedoc
10	Rede de visitantes

Para poder fazer possível o transporte de duas ou mais VLANs presentes em um *switch* para outro s*witch*, surge o conceito de *trunking*.

3.5.1 VLAN *trunking*

Prior (2012), define que tronco é um *link* ponto-a-ponto entre dois dispositivos de rede que transporta mais de uma VLAN. Um tronco de VLAN permite estender as VLANs através de uma rede inteira.

É possível verificar ainda na figura 9, que o ISUTC implementa o conceito de tronco para fazer possível a comunicação entre as diversas VLANs. Pois, o ISUTC é um edifício grande com dois pisos, onde os responsáveis por um determinado departamento podem encontrar-se uns no piso de baixo e os outros no piso de cima. Olhando para esse aspecto, pode se concluir que não implementar o conceito de *trunking*, poderia tornar a rede complexa. Pois, seria necessário desperdiçar portas e cabos para poder interligar várias VLANs entre a interligação de *switches*. A figura abaixo apresenta um caso com a interligação entre *switches* apenas com uma VLAN por porta.

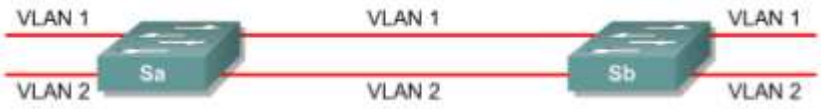

Figura 10: Interligação entre *switches* apenas com uma VLAN por porta [Prior, 2012]

Uma vez, implementado o conceito de *trunking*, seria possível observar o seguinte:

Figura 11: Interligação entre *switches* com portas em modo trunk [Prior, 2012]

Um caso prático no ISUTC são as salas de informática, onde os computadores encontram-se todos na mesma VLAN. A sala de informática 1 encontra-se no piso de baixo e a sala de informática 2 no piso de cima. Para poder transportar o tráfego do *switch* de baixo presente na sala de informática 1, para o *switch* de cima, presente na sala de informática 2, usa-se o conceito de *trunk.*

O *trunk* é configurado em uma determinada porta do *switch* para deixar passar pela respectiva porta todo o tráfego de diferentes VLAN's para um outro *switch.* Olhando ainda para o caso das salas de informática, é possível perceber ainda que, para reduzir os custos, em um mesmo *switch* podem estar configuradas várias VLAN's. No *switch* da sala de informática 1 podem estar configuradas as VLANs pertencentes ao sector pedagógico e de outros departamentos.

Fazendo transportar todas as VLANs para o *switch* de cima presente na sala de informática 2, poderia se aproveitar os recursos para ligar os computadores do sector pedagógico e dos demais departamentos no mesmo *switch*.

3.5.2 Encaminhamento entre diferentes VLAN

Mais uma vez, no presente contexto de estudo que apresenta a estrutura da rede de dados do ISUTC, existe uma necessidade de tornar possível a comunicação de diferentes VLAN's. Um exemplo prático e aplicável disso são os departamentos da secretária e do sector pedagógico ou então a secretaria do ISUTC com o departamento da Transcom. Estes departamentos em algum momento podem precisar de se comunicar. Como é sabido, para dois dispositivos se comunicarem, eles precisam de estar na mesma rede. Se estes estiverem em redes diferentes, não irão se comunicar. Uma VLAN é vista como uma única rede diferente da outra VLAN. Mais uma vez, como é sabido, para dois dispositivos em redes diferentes se comunicarem, precisam de um elemento intermediário para fazer o roteamento. O ISUTC não foge a regra, pois, existem equipamentos responsáveis por fazer esse roteamento que são os *switch layer 3* (um *switch* da camada 3 realiza funções de roteamento).

Para suportar o parágrafo acima, Prior (2012) afirma que diferentes VLANs comportam-se como redes independentes, não havendo possibilidade de comunicação entre elas nessa camada. A existir necessidade de comunicação entre máquinas em diferentes VLANs, ela terá que efectuar-se na camada de rede, ou seja, através de um *router*. Este pode ligar-se ao(s) *switches* através de múltiplas portas físicas ou através de uma única porta em modo *trunk*.

Ainda na figura que representa a estrutura LAN do ISUTC, é possível verificar que a VLAN 7 apresenta um dispositivo designado *Access Point* (Ponto de acesso), que representa como os portáteis se conectam à rede no Cedoc e nas salas de informática. Posto isso, é necessário estudar como esse processo ocorre para poder entender a necessidade de implementação de um serviço que vai ajudar a melhor a segurança da rede *wireless* do ISUTC.

3.6 Actual modo de acesso à rede *wireless* do ISUTC

Nenhuma rede é totalmente segura, seja ela cabeada ou então sem fios. Entretanto, há medidas que podem ser tomadas para reduzir os riscos de segurança sobretudo quando se trata de uma rede sem fio que é a mais sensível a aspectos de segurança.

Quando se conecta a uma rede sem fio não segura, é preciso ter noção que alguém capacitado, curioso e com as ferramentas necessárias pode invadir a rede invadir a rede e capturar os

dados que são trafegados nela, incluindo *sites* visitados, nomes de utilizadores e senhas usadas, pois, não existe nenhum tipo de criptografia nessas redes.

A falta de segurança influencia no desempenho da rede, pois, pessoas podem conectar-se a esta, tornando a conexão de Internet mais lenta.

Actualmente no ISUTC, a rede sem fio disponível não apresenta nenhum tipo de protecção. Entrar em uma rede sem fio desprotegida é simples, basta estar nas proximidades do ponto de acesso e pedir para o computador encontrar as redes disponíveis ao redor. Uma rede *wireless* sem segurança habilitada é identificada com um ícone de escudo amarelo (no Windows 7).

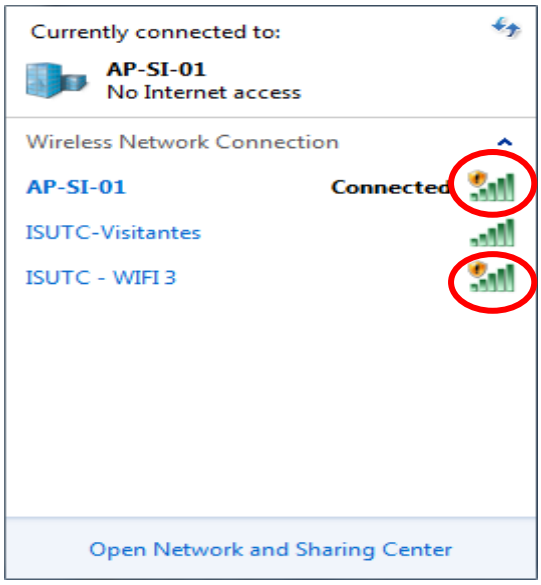

Figura 12: Conectar-se a uma rede não segura [Fonte: Autor]

pode ser feita ainda, uma análise mais rica sobre o actual modo de acesso à rede *wireless* do ISUTC usando a UML (*Unified Modeling Language*). Para Mucin (2011), esta, refere-se a uma linguagem de modelagem não proprietária de terceira geração. A UML não é uma metodologia de desenvolvimento, isto é, ela não diz o que fazer ou como projectar um sistema, mas auxilia na visualização de desenhos e a comunicação entre os objectos. Esta linguagem apresenta diversos diagramas, como por exemplo:

- Diagrama de caso de uso;
- Diagrama de classes;
- Diagrama de objectos;
- Diagrama de sequência;
- Diagrama de actividades;

A descrição dos diferentes tipos de diagramas não foi escopo deste trabalho. Somente foi feito o uso de alguns tipos de diagramas para ilustrar de forma mais perceptível alguns processos que ocorrem ao conectar-se à rede *wireless* do ISUTC.

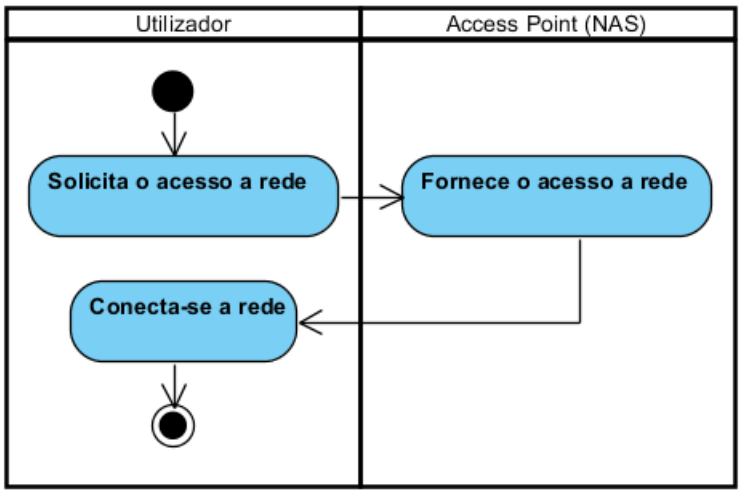

Figura 13: Diagrama de actividades do actual modo de acesso à rede wireless do ISUTC [Fonte: Autor]

3.6.1 Limitações com a configuração actual

Uma instalação com a configuração padrão coloca em causa a segurança da rede. Este tipo de instalação, são caracterizadas por terem as seguintes características:

- **Não tem controlo de acesso** - Apesar da existência ACL (lista de controlo de acesso) entre VLANs na rede ISUTC, este processo não possibilita o controlo lógico através de autenticação, desta forma, permite o acesso não autorizado e não identificado à rede do ISUTC. Este acesso possibilita que a mesma seja usada como base para ataques, podendo ter como alvo tanto a rede interna quanto redes externas;
- **Não usa comunicação criptografada** - Informações que trafegam por esta rede, podem ficar visíveis a outros utilizadores. Muitas vezes essas redes são instaladas em sectores administrativos, o que torna ainda mais grave o problema;

Há potenciais riscos que uma ligação *wireless* traz. Alguns destes riscos são:

- Um *cracker* pode interceptar quaisquer dados que envie ou receba;
- Um *cracker* pode obter acesso à sua rede sem fios;
- Outra pessoa pode roubar o seu acesso à Internet.

3.7 Resumo

Neste capítulo efectuou-se a contextualização do problema, descreveu-se o ISUTC, sua missão e visão. Fez-se um estudo profundo ao que diz respeito a estrutura da rede de dados presente no ISUTC, assim como os assuntos relacionados com os grupos de utilizadores existentes. Verificou-se que estes grupos encontram-se em diferentes VLANs de forma a garantir um melhor desempenho e um certo nível de segurança na rede. Descreveu-se também o actual modo de acesso à rede *wireless* de forma a dar mais ênfase na importância de um serviço que irá autenticar os utilizadores na rede *wireless* do ISUTC.

CAPÍTULO 4 – METODOLOGIA DE RESOLUÇÃO DO PROBLEMA E APRESENTAÇÃO DE RESULTADOS

4.1 Introdução

Após ter-se verificado as inconveniências do actual modo de acesso à rede *wireless* do ISUTC, todo o processo descrito para a implementação do serviço RADIUS será no sentido de minimizar estas inconveniências.

Sendo assim, este capítulo irá abordar os processos seguidos para a implementação do serviço RADIUS, mostrando posteriormente o resultado dos testes executados.

4.2 Metodologia de implementação

Para a implementação do serviço RADIUS, foram seguidas as melhores práticas para a gestão de serviços de TI usando o ITIL, pois este pode ser utilizado como apoio para melhorar processos de gestão que resultem na melhoria da qualidade dos serviços de TI.

4.2.1 ITIL (*Information Technology Infrastructure Library*)

ITIL é um *framework*[4] que reúne as boas práticas para a gestão de serviços de TI. Este desperta grande interesse no mercado. Actualmente, existe uma preocupação com a gestão de serviços de TI nas empresas. A grande dependência da TI para os negócios faz com que os gestores desses departamentos busquem a adopção das boas práticas com o objectivo de trazer resultados positivos, como redução de custos e agilidade em seus processos, (GASPAR; GOMES; MIRANDA, 2010).

O ITIL envolve factores como o tamanho e a maturidade da instituição, os serviços de TI que são executados e a maturidade da área de TI. Este é um dos *frameworks* mais utilizados para gestão de serviços de TI. A versão actual do *framework* possui 26 processo de gestão, que é dividida em 5 categorias. Para Fernandes A. (2008), estas categorias estão relacionadas ao ciclo de vida do serviço.

Na figura abaixo, verifica-se a relação de processos existentes em cada fase do ciclo de vida.

[4] Em gestão, um *framework*, segundo Cassão (2013), é uma estrutura conceitual que serve para incrementar a disciplina de gestão. Pode ser visto também como uma táctica bem definida para manipular com destreza ambientes organizacionais complexos e prover sugestões de solução para uma família de problemas semelhantes. Exemplos de *frameworks* para gestão: ISO 9.000, ISO 14.000, OHSAS 18.000, ITIL, COBIT, CMM, HACCP.

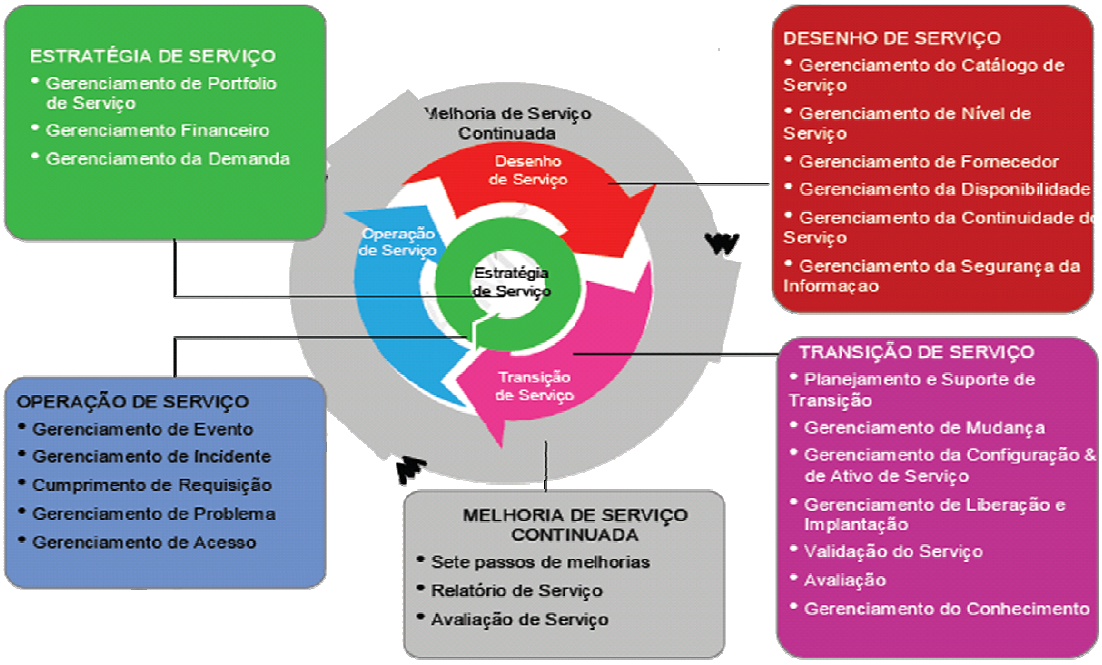

Figura 14: Processos existentes em cada uma das fases do ciclo de vida [Carvalho, 2012]

Estes processos propiciam o uso das boas práticas, fazendo com que o departamento de TI possa adoptá-las independentemente da estrutura da organização.

4.2.2 Fases do ciclo de vida do serviço

Fase 1 – Estratégia do serviço

Nesta primeira fase, e uma vez que o projecto tem o objectivo de implementar um serviço que possibilita autenticar os utilizadores no acesso à rede *wireless*, corresponde sobretudo a uma fase de identificação de requisitos e necessidades de negócio que sejam atendidos pelo serviço, de forma a poder entender ao fundo até que ponto este poderá ser útil dentro do ISUTC. Esta fase corresponde ao capítulo 1 do presente projecto.

Para suportar o parágrafo acima, segundo Fagury (2010), desenvolvimento de estratégias e modelos organizacionais baseados em serviços engloba questões como:

- Quais os serviços devem ser oferecidos e para quais clientes;
- Como criar valor para os clientes;
- Como fazer que percebam o valor criado;

Um dos tópicos abordados nesta fase é o catálogo de serviços no qual podem ser verificados todos os serviços que a rede do ISUTC fornece (Informação encontrada no anexo II).

Fase 2 – Desenho do serviço

Para Fagury (2010), a partir dos requisitos é concebida a solução de TI em forma de serviço. Esta fase desenha serviços de TI apropriados e inovadores, incluindo suas arquitecturas, processos, políticas e documentações, de modo a suprir actuais e futuros requisitos de negócio.

O principal objectivo dos processos da fase de Desenho de Serviço é o de projectar o serviço para que ele seja oferecido dentro das necessidades para as quais está sendo criado ou modificado (PEREIRA et al., 2013).

Sendo assim, pode se dizer que é nesta fase onde é projectado o RADIUS e também os processos ao longo do ciclo de vida que norteiam este serviço.

A solução RADIUS escolhida para ser implementada foi o freeRADIUS, descrito no capítulo 2 no ponto 2.7.1, por ser modular, *open source*, compatível com os sistemas Linux, e por permitir ainda a possibilidade de integração ao serviço LDAP.

Ainda nesta fase, foram feitos alguns diagramas para auxiliarem na percepção do serviço a ser implementado. Estes diagramas encontram-se ilustrados no anexo 3 do presente projecto.

Fase 3 – Transição do serviço

Foi nesta fase onde se implementou o serviço freeRADIUS com base nas especificações produzidas na fase de desenho. Esta implementação foi testada, acompanhada e validada. Importa referir que esta fase pode envolver a modificação do desenho e em alguns casos a reanálise das especificações, pois o principal foco desta, está em todos os aspectos do serviço, incluindo o suporte a falhas.

Para Fagury (2010), os objectivos desta fase são:

- Planear e gerir os recursos de modo a estabelecer um novo serviço no ambiente de produção, com qualidade, custo previsível e dentro do prazo estimado;
- Assegurar o menor impacto possível nos serviços em produção quando o novo serviço for implantado;
- Aumentar a satisfação dos clientes, utilizadores e equipe de suporte com práticas de transição que resultem em menor impacto para organização;
- Fornecer plano compreensivo e claro para que o projecto de mudança esteja alinhado aos planos de transição de serviço.

O manual de instalação e configuração do freeRADIUS encontram-se no anexo IV.

É importante salientar que, os objectivos descritos acima, serão revistos de forma a garantir uma melhor credibilidade na implementação do serviço em toda a rede do ISUTC em geral.

Fase 4 – Operação do serviço

Esta fase corresponde na definição de actividades que devem ser seguidas de maneira periódica para garantir a operação do serviço.

Este é o único estágio em que os serviços efectivamente entregam valor ao cliente, uma vez que para o cliente o valor está no serviço de TI em produção (FAGURY, 2013).

Esta fase consiste então, no conjunto das seguintes actividades sendo as mesmas funções do Sector de Informática:

- Garantir a disponibilidade do serviço;
- Procedimentos de rotina de *backups* e de restauração;
- Monitorização do ficheiro de *logs*, para identificação prévia de problemas;
- Definição e actualização do manual de operações do serviço;
- Suporte sempre que necessário ao utilizador.

Fase 5 – Melhoria contínua do serviço

Para Fagury (2013), esta fase é responsável por identificar oportunidades de melhoria no serviço. Esta melhoria actua integrando todo o ciclo de vida, fazendo melhorias em cada fase ou no total delas. Importa referir que sempre a visão do negócio deverá nortear os serviços. São os objectivos desta fase:

- Aperfeiçoar a qualidade do serviço, da eficiência e da eficácia dos processos;
- Verificar se os objectivos do serviço estão sendo alcançados;
- Assegurar que os métodos de gestão de qualidade suportam as actividades de melhoria contínua.

Sendo assim, pode se dizer que esta melhoria pode ser feita com base em sugestões, opiniões e inquéritos de forma a medir o grau de satisfação do utilizador em relação ao serviço freeRadius. Com base nessa informação, é possível trazer algum tipo de melhoria no serviço de forma a satisfazer as necessidades da organização assim como a dos utilizadores.

4.2.3 Cronograma de actividades

Tabela 10: Cronograma de actividades [Fonte: Autor]

Fase	Actividade	Janeiro				Fevereiro				Março			
		Semanas				Semanas				Semanas			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Levantamento da informação necessária sobre o ISUTC referente a organização, gestão e processos.												
1	Levantamento da informação e recursos necessários para a implementação do RADIUS												
2	Montagem do ambiente para a implementação do serviço RADIUS (Análise de requisitos, avaliação de soluções alternativas, esboço da solução escolhida)												
3	Instalação e configuração do serviço RADIUS												
3	Testes dos clientes em diferentes plataformas e relatórios												
4	Elaboração do manual de instalação e de uso												

4.3 Implementação do projecto

4.3.1 Levantamento da informação necessária sobre o ISUTC

Esta fase consistiu na execução das seguintes actividades:

1. **Busca de informação relevante a documentação da rede do ISUTC, processos envolventes referente a gestão e da própria organização**

A maioria da informação sobre a instituição foi adquirida no *site* da Transcom. De seguida foram realizadas entrevistas de modo a entender como encontra-se estruturada a rede de dados do ISUTC e que inconveniências existem no actual modo de acesso à rede *wireless*. Foi feito um estudo de tal forma a entender que benefício esta rede teria se houvesse um serviço que visa a autenticação dos utilizadores no acesso a mesma, de forma a criar um valor no que diz respeito as informações dos utilizadores que trafegam por estas redes.

2. **Procura e leitura da documentação existente para o serviço RADIUS**

A documentação referente ao RADIUS foi obtida na página oficial do projecto freeRADIUS e em outros artigos como blogues e fóruns. Esta documentação ajudou em alguns pontos que são:

- Apresentação do serviço;
- Manual de instalação e configuração do serviço;
- Integração com o LDAP;
- Manual de configuração para os clientes em diferentes plataformas;
- *Troubleshooting.*

4.3.2 Montagem do ambiente para a implementação do serviço RADIUS

Esta fase consistiu em fazer uma análise de requisitos necessários para a implementação do RADIUS. Consistiu sobretudo em verificar que soluções RADIUS existem no mercado e qual a melhor solução se adequa ao presente caso de estudo. Das 3 soluções que foram descritas no capítulo 2, no ponto 2.7, foi escolhida o freeRADIUS para ser implementado no projecto em questão por razões óbvias e já descritas anteriormente. Esta é uma solução *open source*, modular, o que significa que pode ser integrado nela o LDAP, apresenta alta performance e bom desempenho e compatível com os servidores Linux, estes que são os fortes na infra-estrutura da rede ISUTC.

Para a solução escolhida, foi necessária a instalação e configuração das seguintes ferramentas:

- Preparação de uma máquina virtual com os requisitos mínimos para suportar o serviço;
- Sistema Operativo Ubuntu *Server* 10.04 LTS;
- Réplica do LDAP (LDAP *Slave*);
- Uso de um *router wireless* com suporte a tecnologia RADIUS (os *access points* que o ISUTC possui, suportam o serviço RADIUS. Sendo estes referenciados na tabela 6);

Os requisitos mínimos para a instalação do sistema operativo Ubuntu *Server* 10.04 LTS, são:

- Processador: 700MHz;
- Memória RAM: 512MB
- Disco: 4GB;
- Placa Gráfica: Sem requisito mínimo.

Para a instalação do freeRadius no servidor ubuntu 10.04 LTS, os requisitos mínimos são os mesmos.

No caso do ISUTC, os requisitos para a instalação do serviço freeRadius em um servidor ubuntu 10.04 lts, tendo em conta o número de utilizadores que este possui, os requisitos seriam:

- Processador: 1.2GHz ou superior
- Memória RAM: 1GB ou superior
- Disco: 20GB ou superior
- Placa Gráfica: Sem requisito mínimo.

Ainda no ambiente de preparação, importa referir que o serviço freeRADIUS suporta 1024 conexões simultâneas por padrão, porém esta configuração pode ser alterada dependendo das conexões simultâneas que os *access points* podem suportar. Não foi escopo deste projecto analisar quantas conexões simultâneas os *access points* presentes na rede de dados do ISUTC podem suportar, uma vez que a rede já encontra-se instalada e dimensionada, assume-se que esse estudo já foi feito.

4.3.3 Instalação, configuração e testes do serviço

Esta fase resume-se na implementação do projecto onde se verificou pequenas dificuldades. Esta fase foi sucedida passando pelas actividades descritas abaixo.

1. Instalação do serviço RADIUS

Esta primeira etapa consistiu primeiro na verificação de novos pacotes ou actualizações do sistema operativo encontrado no servidor. Só depois de actualizados os pacotes, foi possível a instalação do serviço freeRadius. Como foi referido anteriormente, o manual de instalação do freeRadius encontra-se no anexo IV.

2. Configuração do serviço RADIUS

Foi nesta etapa onde se integrou o serviço freeRadius com o LDAP, tendo sido necessário alterar as configurações de alguns ficheiros padrões. Esta alteração implicou em algumas ocasiões um efeito negativo, pois notava-se algumas falhas nos *logs* ao inicializar o serviço. Foi necessário rever as configurações de forma a eliminar as falhas verificadas nos *logs*. É nesta etapa onde cada passo dado foi documentado de forma a não cometer os mesmos erros posteriormente, tornando possível uma rápida configuração em um ambiente diferente. O manual referente a configuração também encontra-se no anexo IV.

3. Testes dos clientes de diferentes plataformas à solicitação do serviço RADIUS

Estes testes contaram com a participação de diferentes utilizadores, sendo alguns deles os funcionários do *HelpDesk*, Sector de Informática e do Limeaa.

É nesta fase que verificou-se também uma ligeira dificuldade na configuração dos clientes. Pois, para cada tipo de cliente era necessário uma diferente forma de configuração. Notou-se que seria necessário fazer configurações adicionais para determinados tipos de clientes.

No anexo V, é possível verificar que tipo de configuração adicional foi necessário fazer nos dispositivos clientes que iriam se conectar ao serviço RADIUS.

4. Resultado dos testes

Tabela 11: Resultado dos testes às funcionalidades [Fonte: Autor]

***Access Point* – LinkSys WAP54G**		
Plataforma usada (Cliente)	**Estado**	**Observação**
Windows XP	Funcional	É necessário fazer uma configuração adicional para que estes clientes se conectem ao servidor RADIUS. Esta configuração encontra-se explicada nos anexos.
Windows 7	Funcional	
Windows 8	Funcional	Nenhuma configuração adicional é feita.
Ubuntu Desktop 10.04	Funcional	
iOS	Funcional	
Android	Funcional	

4.3.4 Elaboração do manual de instalação e de uso

Esta fase resume-se essencialmente na elaboração do manual de instalação, mostrando passo à passo como instalar o serviço freeRADIUS e como configurar o mesmo para suportar a integração com o LDAP do ISUTC. Este manual encontra-se referido no anexo IV.

Foi ainda nesta fase onde se elaborou o manual do uso (anexo V). É ilustrado nesse manual como é que devem ser configurados os clientes para conectarem-se ao serviço implementado. Importa salientar mais uma vez que, a configuração é diferente para os diferentes tipos de sistemas operativos (XP, Ubuntu, Android, IOs).

4.4 Estimativa de custos

De seguida é efectuada uma estimativa dos custos do projecto, para possibilitar a implementação e estabilização em produção do serviço RADIUS.

Os custos foram elaborados segundo a tabela de salários dos funcionários do sector de informática, sendo estes, os estudantes trabalhadores cumprindo um mínimo de 12 horas de trabalho semanalmente.

Tabela 12: Estimativa de custos de implementação do serviço [Fonte: Autor]

Actividade	**Tempo [Horas]**	**Recursos**		
		Humanos	**Materiais**	**Financeiros [Meticais]**
Revisão de bibliografias e treinamento em tecnologias	48	1	Livros e Internet	$105\,{}^{Mt}/_{h} \times 48 = 5.040$
Implementação e configuração do Serviço	48	1	Livros e Internet	$105\,{}^{Mt}/_{h} \times 48 = 5.040$
Testes do serviço e modificações necessárias	48	3	Um servidor, um *router wireless* e computadores clientes (inclui celulares com diferentes sistemas operativos)	$105\,{}^{Mt}/_{h} \times 48 \times 3 = 15.120$
			TOTAL	25.200

Estima-se que o ISUTC possui o material necessário para a implementação do RADIUS.
A manutenção e melhorias necessárias do serviço pode ser feita semestralmente num período de 1 a 2 meses pelos funcionários do sector de informática.

4.5 Resumo

Foi neste capítulo onde se cumpriu com as necessidades do projecto. De acordo com as inconveniências do actual modo de acesso á rede *wireless*, implementou-se o RADIUS de forma a minimizar estas inconveniências. Este capítulo resume-se essencialmente por apresentar a metodologia usada para a implementação do serviço, desdobrando-se por cada fase que a metodologia apresenta de forma a conseguir assim o alcance do objectivo pretendido.

CAPÍTULO 5 – CONCLUSÕES E RECOMENDAÇÕES

5.1 Conclusões

O projecto teve como propósito implementar um serviço para a autenticar os utilizadores no acesso à rede sem fio do ISUTC. Numa primeira fase, foi feita a análise dos principais conceitos necessários para apoiar o alcance dos objectivos propostos.

Referente aos objectivos de investigação, foi feita a descrição dos actuais processos usados para o acesso a estas redes, informação conseguida a partir de entrevistas aos membros do Sector de Informática.

Durante o desenvolvimento do projecto, foi possível identificar as principais limitações que os administradores de rede do ISUTC enfrentam, pois estes não tem um controlo de acesso aprimorado sobre os dispositivos que se conectam a estas redes, podendo assim dificultar a identificação da causa de um determinado dano dentro da rede. Por sua vez, a informação dos utilizadores que são trafegados neste tipo de rede, podem ser facilmente capturados por alguém que percebe bem da matéria.

Foi possível ainda identificar quais as vulnerabilidades existentes no actual modo de acesso a estas redes. Verificou-se que não existe nenhum controlo feito para aceder a estas redes, o que designa-se em várias bibliografias “redes abertas, ou redes inseguras”.

Verificou-se o método de implementação do serviço RADIUS que melhor se adequa ao presente projecto, ajudando assim no melhoramento que pode ser atingido em todos os processos de trabalho após a implementação do serviço. Este resume-se essencialmente na autenticação dos utilizadores no acesso à rede *wireless* do ISUTC e consequentemente um ganho no que diz respeito a redução de ameaças que podem ocorrer dentro da rede, pois o acesso a mesma, teria deste modo um certo nível de segurança maior do que o actual.

Implementou-se o serviço freeRADIUS e de seguida os testes, onde neste ultimo verificou-se que a configuração é feita de maneira diferente para diferentes tipos de plataformas, sendo estas, Windows, Linux, Android e iOS.

5.2 Recomendações

Tendo em conta que esta solução introduz um melhoramento na segurança das redes sem fio no ISUTC, surge a necessidade de efectuar-se trabalhos e estudos futuros em cima desta solução.

Recomenda-se um estudo detalhado referente a custos de desenvolvimento, manutenção, implementação e a possibilidade de outras soluções RADIUS existentes.

No caso de desejo de introduzir este serviço em produção, é recomendável que sejam desenvolvidos planos de *backup* do serviço e planos de melhoria, executados por profissionais qualificáveis para tal, isto com vista a estabilização do serviço.

Recomenda-se que o desenvolvimento contínuo do serviço seja acompanhado por um profissional experiente na área de infra-estruturas e operações de serviços de rede.

Recomenda-se que o serviço RADIUS seja implementado em um ambiente completamente seguro, deste modo garantindo a segurança do próprio serviço.

REFERÊNCIAS BIBLIOGRÁFICAS

1. BIERSDORFER, J. D. *iPad : O Manual que faltava.* 1ª ed. São Paulo: Digerati Books, 2011.
2. BLUNK, L.; VOLLBRECHT, J. *Request For Comments: 2284, EAP*. Disponível em <https://tools.ietf.org/rfc/rfc2284.txt> Acesso em 23 de Janeiro de 2014.
3. Bueno, Maurício. *Informática fácil para concursos*. 1ª ed. Rio de Janeiro: Brasport, 2005.
4. BUTCHER, M. *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services*. 1ª ed. Birmingham: Packt, 2007.
5. CANTU, Evandro. *Redes de computadores e Internet*. 1ª ed. São José: CEFET/SC, 2003.
6. CARISSIMI, A.; ROCHOL, J.; GRANVILLE, Z. *Redes de Computadores*. 1ª ed. Porto Alegre: Bookman, 2009.
7. CARROLL, Brandon. *Cisco access control security: AAA Administration services.* 1ª ed. Indianapolis: Cisco Press, 2004.
8. CARVALHO, Hugo. *Estabelecimento de uma sessão.* Disponível em <http://www.gta.ufrj.br/grad/08_1/radius/EstabelecimentodeumaSesso.html> Acesso em 17 de Janeiro de 2014.
9. CARVALHO, Pedro. *Itil Foundation v3 – Governancia de TI.* Disponível em <http://www.pedrofcarvalho.com.br/itil.html> Acesso em 23 de Janeiro de 2014.
10. CASSÃO, Pedro. *Controle e administração de projectos.* Disponível em <http://www.cassao.eti.br/portal/controleAdministracaoProjetos> Acesso em 06 de Fevereiro de 2014.
11. CHICOLI, Milton. *Guia de Manutenção de PCs e notebooks*. 1ªed. São Paulo: Digerati Books, 2008.
12. COSTA, Daniel G. *Java em Rede: Recursos avançados de programação*. Rio de Janeiro : Brasport, 2008.
13. FAGURY, Thiago. *Concursos, TI e Gestão.* Disponível em <http://fagury.com.br/sys/wp-content/uploads/2010/09/apostila-itil-v3-3.pdf> Acesso em 20 de Dezembro de 2014.
14. FERNANDES, A.; ABREU, V. *Implantando a governança de TI – da Estratégia à gestão de processos e serviços*. 2ª ed. Rio de Janeiro: Brasport, 2008.

15. FINSETH, Craig. *Request For Comments: 1492, TACACS.* Disponível em <https://tools.ietf.org/html/rfc1492> Acesso em 9 de Fevereiro de 2014.
16. FLORES, Paulo. *Implementação em hardware do algoritmo MD5.* Disponível em <http://algos.inesc-id.pt/~pff/tfc04/node2.html> Acesso em 03 de Fevereiro de 2014.
17. GALLO, M.; HANCOCK, W. *Comunicação entre computadores e tecnologías de rede*. São Paulo: Thompson Learning, 2002.
18. GASPAR, Marcelo; GOMES, Thierry; MIRANDA, Zailton. *Mudar e Innovar: reoslvendo conflitos com ITIL® v3.* 1ª ed. Brasília: Senac DF, 2010.
19. GOUVEIA, J.; MAGALHÃES, A. *Hardware para PCs e Redes*. 3ª ed. Lisboa: FCA Editora, 1999.
20. GUIMARÃES, Alexandre. *Segurança em redes privadas virtuais – VPNs.* 1ª ed. São Paulo: Brasport Livros e Multimidia, 2006.
21. HUGO, Victor. F*rontend Web2.0 para gestão de RADIUS*. Disponível em <http://paginas.fe.up.pt/~ee04199/radius.html> Acesso em 23 de Janeiro de 2014.
22. HUNTLER, Robbie.; DINERMAN, Bradley. *Windows server 2003 Networking Recipes: A problem-Solution Approach*. 1ª ed. New York: Apress, 2006
23. JOBSTRAIBIZER, Flávia. *Desvendando as redes sem fio.* 1ª ed. São Paulo: Digerati Books, 2010.
24. LEE, Byeong.; CHOI, Sunghyum. *Broadband wireless access and local networks: Mobile WiMax and WiFi*. 1ª ed. Norwood: Artech House, 2008.
25. MACÊDO, Diego. *RADIUS.* Disponível em <http://www.diegomacedo.com.br/radius/> Acesso em 17 de Janeiro de 2014.
26. MONTICO, Matias. *Guia avançado de redes wireless*. 1ª ed. São Paulo: Digerati Books, 2009.
27. MUCIN, Samuel. *Astah Community, um software para trabalha com UMLs.* Dsiponível em <http://www.plantaonerd.com/blog/2011/04/18/astah-community-um-software-para-trabalha-com-umls/#more-411> Acesso em 03 de Fevereiro de 2014.
28. OLIVEIRA, Wilson. *Segurança da informação*. 1ª ed. Lisboa: Centro Atlântico, 2001.
29. OLIVEIRA, Wilson. *Dossiê Hacker*. 1ª ed. São Paulo: Digerati Books, 2006.
30. PELLEJERO, I.; ANDREU, F.; LESTA. *Fundamentos y aplicaciones de seguridade en redes WLAN*. 1ª ed. Barcelona: Marcombo, S.A. (ediciones técnicas), 2006.
31. PEREIRA, Henrique et al. *Gestão de serviços de TI com ITIL: resultados da implantação no CPD da UFSM.* Disponível em

<http://sites.multiweb.ufsm.br/sites/portalcpd/templates/meutemplate1.0b/images/artigos/2013/46997.pdf> Acesso em 07 de Janeiro de 2014.

32. PILLOU, Jean-François. *VLAN – Redes virtuais.* Disponível em <http://pt.kioskea.net/contents/289-vlan-redes-virtuais> Acesso em 20 de Fevereiro de 2014.
33. PINHEIRO, José. *Topologias de redes de comunicação*. Disponível em <http://www.projetoderedes.com.br/artigos/artigo_topologias_de_rede.php> Acesso em 22 de Dezembro de 2013.
34. PISA, Pedro. *O que é hash*. Disponível em <http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html> Acesso em 03 de Fevereiro de 2014.
35. PRIOR, Rui. *Laboratório de redes.* Disponível em <http://www.dcc.fc.up.pt/~rprior/1112/LabRedes/VLAN.pdf> Acesso em: 20 de Fevereiro de 2014.
36. REZENDE, Denis A. *Engenharia de software e sistemas de informação*. 3ª ed. Rio de Janeiro: Brasport Livros e Multimedia, 2005.
37. RODRIGUES, L. Silva. *Arquitecturas dos sistemas de informação*. 1ª ed. Lisboa: FCA Editora, 2002.
38. ROSS, Júlio. *Redes de computadores*. 1ª ed. São Paulo: Editora Antena, 2008.
39. SIMPSON, William. *Request For Comments: 1994, CHAP*. Disponível em <http://tools.ietf.org/rfc/rfc1994.txt> Acesso em 9 de Fevereiro de 2014.
40. SOUSA, Sérgio. *Tecnologias de informação.* 1ª ed. Lisboa: FCA Editora, 1999.
41. TANENBAUM, Andrew S. *Redes de computadores.* 3ª ed. Rio de Janeiro: Elsevier, 2003.
42. TITTEL, Ed. *Rede de computadores*. 1ª ed. Porto Alegre: Artmed Editora, 2002.
43. Transcom. Sociedade de Formação, Consultoria e Auditoria em Transportes e Comunicações. *Catálogos de Universidade.* Apresenta historial e missão do ISTC. Disponível em: <http://www.transcom.co.mz/isutc/Home-ISUTC/A-Instituicao/Historial-e-Missao> Acesso em 14 de Fevereiro de 2014.
44. WALT, Dirk. *FreeRADIUS beginner's guide.* 1ªa ed. Mumbai: Packt Publishing, 2011.
45. WOLKARTT, Carlos. *O modelo hierárquico da cisco.* Disponível em <http://blog.wolkartt.com/2012/10/o-modelo-hierarquico-da-cisco.html#.Uw85_FPLHYc> Acesso em 22 de Dezembro de 2013.

BIBLIOGRAFIA

1. BRASIL, Cyclades. *Guia Internet de conectividade.* 14ª ed. São Paulo: Editora Senac, 2009.
2. CARUSO, C,; STEFFEN, F. *Segurança em informática e de informações*. 2ª ed. São Paulo: Editora Senac, 1999.
3. COMER, Douglas. *Redes de computadores*. 4ª ed. Porto Alegre: Artmed Editora, 2007.
4. DAVIDSON, J. et al. *Fundamentos de VoIP*. 2ª ed. Porto Alegre: Artmed Editora, 2007.
5. KHAN, Ryaz. *LDAP e FreeRADIUS no ubuntu 10.04 LTS.* Disponível em <http://ryazkhan.blogspot.com/2011/05/ldap-freeradius-on-ubuntu-1004-lts.html> Acesso em 13 de Fevereiro de 2014.
6. LOUREIRO, Paulo. *TCP/IP em Redes Microsoft*. 8ª ed. Lisboa: FCA Editora, 2003.
7. SCHEWEBEL, Samuel. *Semelhanças e diferenças entre ITIL e CMMI para serviços.* Disponível em <http://www.teclogica.com.br/blog/?p=508> Acesso em 07 de Janeiro de 2014.
8. The FreeRADIUS Project. *Catálogos da organização*. Apresenta a documentação do freeRADIUS. Disponível em <http://freeradius.org/> Acesso em 15 de Fevereiro de 2014.

ANEXOS

ANEXO I - ENTREVISTAS AOS FUNCIONÁRIOS DO ISUTC

Foram realizadas algumas entrevistas aos funcionários do ISUTC, sendo estes concretamente, os funcionários do *HelpDesk*, Sector de Informática, Limeaa e do Sector Pedagógico.

Entrevista 1

No dia 5 de Fevereiro de 2014, no período entre 10:00 – 11:00 Horas, foi feita uma entrevista estruturada com perguntas abertas a Eng. Vanessa Mabunda do sector de informática.

Participantes:

- Eng. Vanessa Mabunda;
- Ted Fernandes.

Resultados:

1. Quais são os grupos de utilizadores que existem no ISUTC?

R: São vários os grupos de utilizadores que existem aqui no ISUTC. Alguns deles são:

- Funcionários, aqui na verdade encontra-se dividido em vários outros grupos, pois cada funcionário tem as suas categorias. Alguns destes grupos são: recursos humanos, secretaria académica, marketing, consultoria, sector pedagógico, estudantes funcionários e outros;
- Estudantes;
- Visitantes.

2. Como é feito o controlo dos dispositivos que se conectam à rede *wireless* do ISUTC?

R: Infelizmente não é feito nenhum tipo de controlo para estes dispositivos.

3. Um serviço que visa a autenticação dos utilizadores no acesso à rede *wireless* do ISUTC ajudaria na administração da rede? Porquê?

R: Claro. Pois assim teríamos como limitar o acesso para os diferentes grupos de utilizadores existentes aqui no ISUTC. Teríamos também um melhor controlo sobre quem de facto esta usando a nossa rede.

Assinatura

_____

Entrevista 2

No dia 07 de Fevereiro de 2014, no período entre 15:00 – 16:00 Horas, foi feita uma entrevista estruturada com perguntas abertas ao técnico Amamo Mathola do *HelpDesk*.

Participantes:

- Amamo Mathola;
- Ted Fernandes.

Resultados:

1. Quais são os principais problemas que a rede *wireless* do ISUTC costuma apresentar?

R: Um dos problemas que costuma haver nas redes sem fio, é quando os laptops não conseguem se conectar a rede, pois costuma ser lhe atribuído um IP inválido. Para solucionar este caso, costumamos fazer um *restart* do *access point*.

2. Como classifica o desempenho da rede *wireless* do ISUTC? Bom? Médio? ou Mau?

R: O desempenho é bom, visto que os problemas que mencionei antes são muito raros de acontecerem.

3. Que grupo de utilizadores mais se conecta a estas redes?

R: A maioria são estudantes. Os professores que usam são os residentes e os mais jovens.

Assinatura

_____

Entrevista 3

No dia 20 de Fevereiro de 2014, no período entre 11:00 – 11:30 Horas, foi feita uma entrevista estruturada com perguntas abertas ao Eng. Micas Rafael do Sector de Informática, mas, actualmente presente no Limeaa.

Participantes:

- Eng. Micas Rafael;
- Ted Fernandes.

Resultados:

1. Um serviço que visa a autenticação dos utilizadores no acesso à rede *wireless* do ISUTC ajudaria na administração da rede? Porquê?

R: Ajudaria sim. Pois teríamos um melhor controlo sobre quem esta usando a nossa rede. Dependendo dos dados que o serviço colecta, poderíamos ter a informação de quem esta conectado a rede, o tipo de dispositivo que encontra-se conectado, o sistema operativo usado pelo dispositivo, o endereço IP atribuído ao dispositivo conectado e outras informações relevantes.

Poderia ainda ajudar-nos a fazer uma estatística, informando em qual período do dia é que temos um maior número de utilizadores conectados à rede, informando também em que período do mes é que verifica-se um maior tráfego na rede.

Assinatura

_____

Entrevista 4

No dia 11 de Março de 2014, no período entre 12:00 – 12:30 Horas, foi feita uma entrevista estruturada com perguntas abertas ao Eng. Radek Baduro do Sector Pedagógico.

Participantes:

- Eng. Radek Baduro;
- Ted Fernandes.

Resultados:

1. Qual é o grau de satisfação que o Eng. Radek Baduro tem com o actual modo de acesso à rede *wireless* do ISUTC?

R: Não muito feliz. Em algumas vezes, a velocidade de transmissão é baixa, a rede costuma apresentar um fraco desempenho. As oscilações de energia também contribuem para o mau desempenho da mesma.

2. Até que ponto o Eng. Radek Baduro acha que os seus dados estão seguros quando conectado à rede *wireless* do ISUTC?

R: Não estou seguro. Pois não existe nenhum método de encriptação nas redes abertas que o ISUTC disponibiliza. Eu costumo trocar e-mails importantes, e se por acaso aparecer um utilizador com conhecimentos em capturar dados que trafegam pela rede, este pode muito bem capturar os meus dados e fazer o uso dela de forma a prejudicar o meu trabalho e quem sabe a minha reputação.

3. Um serviço que visa a autenticação dos utilizadores no acesso à rede *wireless* do ISUTC ajudaria na administração da rede? Porquê?

R: Ajudaria ate um certo ponto. Pois teríamos como saber quem acedeu a rede. Mas ai surge um problema, a politica de segurança do ISUTC não é conhecida, sendo assim, é possível eu ter a senha de um determinado utilizador e começar a fazer o uso da conta dele para ataques maliciosos.

Assinatura

_____

ANEXO II - LISTA DE SERVIÇOS INSTALADOS NOS SERVIDORES DO ISUTC

Servidor	Serviços
Licungo	• Samba PDC • DHCP • File Server • DNS Slave • Web Server • LDAP Master • Chat • FTP (Interno) • Moodle
Zambeze	• DNS Master • Zimbra ZCS • Nagios • LDAP Slave • Backup Transcom
Limpopo	• Proxy • File Server • Apt-proxy • LDAP Slave • MRTG • Jira
Incomati	• FTP (Externo) • LDAP Slave • ISUPAC3 (Externo) • Web Server • Moodle
Save	• DHCP Slave • LDAP Slave • Proxy Slave
Rovuma	• Zimbra ZCS Slave • DNS Slave • LDAP Slave • OpenVPN AS
PC-00-02	• Anti-Virus • Backup dos Serviços

ANEXO III - DIAGRAMAS QUE ILUSTRAM O MODO DE ACESSO À REDE *WIRELESS* DEPOIS DE IMPLEMENTADO O RADIUS

Foram desenvolvidos alguns diagramas que ilustram o modo de acesso à rede *wireless* do ISUTC depois de implementado o serviço RADIUS. Estes desenhos ajudam a ter uma percepção melhor sobre os processos que estão em causa ao conectar-se a rede sem fio do ISUTC.

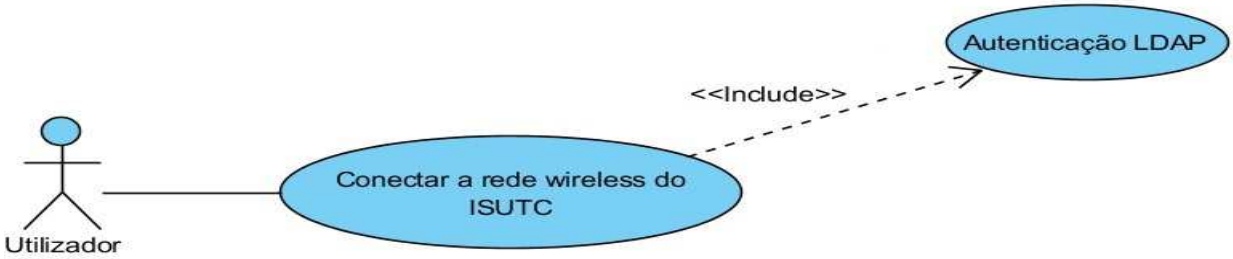

Figura 15: Diagrama de caso de uso referente ao modo de acesso à rede *wireless* do ISUTC depois de implementado o serviço RADIUS [Fonte: Autor]

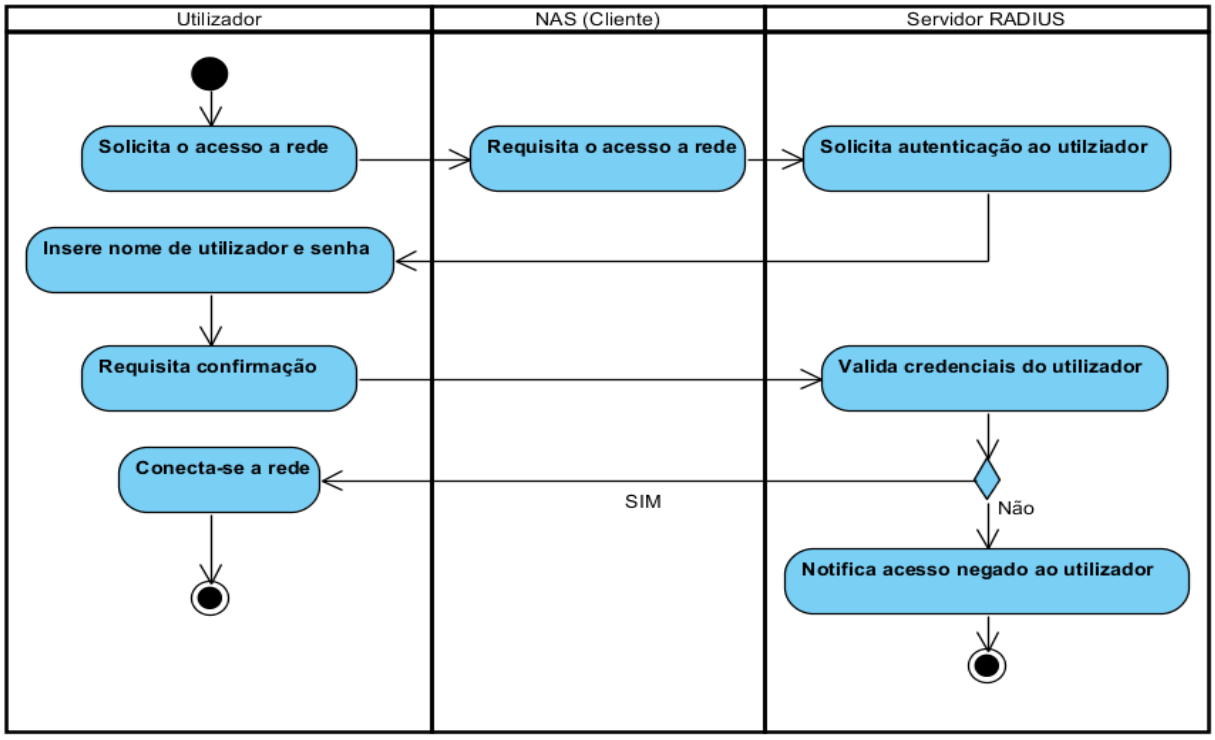

Figura 16: Diagrama de actividades referente ao modo de acesso à rede *wireless* do ISUTC depois de implementado o serviço RADIUS [Fonte: Autor]

ANEXO IV - MANUAL DE INSTALAÇÀO E CONFIGURAÇÃO DO RADIUS COM CONEXÃO LDAP

Neste manual assume-se que:

- O Ubuntu *server* 10.04 LTS já encontra-se instalado e funcionando com o serviço ssh;
- O IP já foi configurado como estático;
- A réplica do LDAP já encontra-se disponível no servidor.

Sendo assim siga com os seguintes procedimentos na consola do ubuntu *server*:

1 - Ser *root* usando o comando:

```
sudo su
```

2 - Verificar se existem novas actualizações e instalar, caso for necessário:

```
apt-get update
apt-get upgrade
```

3 - Instalar o freeradius:

```
apt-get install freeradius freeradius-ldap
```

4 - Copiar o ficheiro “openldap.schema” para o freeradius trabalhar com ldap:

```
cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/
```

4.1 - Converter o .schema que acabou-se de copiar para um ficheiro .ldif para que possa ser adicionado à base de dados ldap:

```
nano /tmp/schema_convert.ldif
```

4.2 - Colar as seguintes linhas, e apagar todas as entradas existentes a partir do arquivo, se existirem:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
```

4.3 - Criar LDIF:

```
slapcat -f /tmp/schema_convert.ldif -F ~ -n0 –s
"cn={7}openldap,cn=schema,cn=config" > /tmp/cn=openldap.ldif
```

4.4 – Apagar alguns detalhes do LDIF:

```
nano /tmp/cn\=openldap.ldif
```

4.5 - Retirar o número e {} das primeiras linhas para torná-lo parecido com o seguinte:

```
dn: cn=openldap,cn=schema,cn=config
...
cn: openldap
```

4.6 - Livrar-se das linhas seguintes, não há nenhuma utilização destes, eles estão localizados na extremidade de openldap.ldif:

```
structuralObjectClass: olcSchemaConfig
entryUUID: c69d2a24-1274-1030-8c56-69db9ca637cf
creatorsName: cn=config
createTimestamp: 20110514125231Z
entryCSN: 20110514125231.473294Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20110514125231Z
```

4.7 - Agora é só adicionar o ficheiro acima à base de dados ldap:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/cn\=openldap.ldif
```

*** Mais uma vez não deve haver qualquer erro.**

4.8 - Para certificar se os .schemas que foram adicionados até agora estão no lugar, emita o seguinte:

```
sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
```

5 - Agora o servidor ldap esta pronto com o esquema FRAD, é hora de configurá-lo. Reiniciar o LDAP e o freeradius:

```
service slapd restart
service freeradius restart
```

6 - Voltando as configurações

```
nano /etc/freeradius/modules/ldap
```

6.1 - Verificar as seguintes linhas e editar conforme o seguinte:

```
server = "localhost"
```

```
identity = "cn=admin,dc=isutc,dc=transcom,dc=co,dc=mz"
password = "******"
basedn = "ou=Users,dc=isutc,dc=transcom,dc=co,dc=mz"
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
base_filter = "(objectclass=posixAccount)"
password_attribute = userPassword
```

7 - Dizer ao freeradius para usar o LDAP para autenticação editando o seguinte arquivo:

```
nano /etc/freeradius/sites-enabled/default
```

7.1 - Descomentar "ldap", localizado nas linhas 170, 181 e 182 e alterar as seguintes linhas que dizem respeito ao Auth-Type para que fiquem de acordo como:

```
Auth-Type PAP {
   ldap
}
```

7.2 - Informar também o freeradius para usar o LDAP dentro do túnel:

```
nano /etc/freeradius/sites-enabled/inner-tunnel
```

7.3 - Descomentar a linha 129 (ldap) e alterar as seguintes linhas que dizem respeito ao Auth-Type para que fiquem de acordo como:

```
Auth-Type PAP {
   ldap
}
```

8 - Reiniciar o ldap e o freeradius

```
service slapd restart
service freeradius restart
```

9 - Emitir o seguinte comando para ver que o mapeamento ldap está funcionando correctamente:

```
freeradius –XXX
```

9.1 - Se as seguintes linhas forem apresentadas, tudo está funcionando do jeito projectado:

```
Debug: rlm_ldap: Registering ldap_groupcmp for Ldap-Group
Debug: rlm_ldap: Registering ldap_xlat with xlat_name ldap
Debug: rlm_ldap: LDAP radiusCheckItem mapped to RADIUS $GENERIC$
```

```
Debug: rlm_ldap: LDAP radiusReplyItem mapped to RADIUS $GENERIC$
Debug: rlm_ldap: LDAP radiusAuthType mapped to RADIUS Auth-Type
Debug: rlm_ldap: LDAP lmPassword mapped to RADIUS LM-Password
Debug: rlm_ldap: LDAP ntPassword mapped to RADIUS NT-Password
Debug: rlm_ldap: LDAP sambaLmPassword mapped to RADIUS LM-Password
Debug: rlm_ldap: LDAP sambaNtPassword mapped to RADIUS NT-Password
Debug: rlm_ldap: LDAP dBCSPwd mapped to RADIUS LM-Password
Debug: rlm_ldap: LDAP acctFlags mapped to RADIUS SMB-Account-CTRL-TEXT
Debug: rlm_ldap: LDAP radiusExpiration mapped to RADIUS Expiration
Debug: rlm_ldap: LDAP radiusNASIpAddress mapped to RADIUS NAS-IP-Address
Debug: rlm_ldap: LDAP radiusServiceType mapped to RADIUS Service-Type
Debug: rlm_ldap: LDAP radiusFramedProtocol mapped to RADIUS Framed-Protocol
Debug: rlm_ldap: LDAP radiusFramedRoute mapped to RADIUS Framed-Route
Debug: rlm_ldap: LDAP radiusFramedRouting mapped to RADIUS Framed-Routing
Debug: rlm_ldap: LDAP radiusFilterId mapped to RADIUS Filter-Id
Debug: rlm_ldap: LDAP radiusFramedMTU mapped to RADIUS Framed-MTU
Debug: rlm_ldap: LDAP radiusLoginIPHost mapped to RADIUS Login-IP-Host
Debug: rlm_ldap: LDAP radiusLoginService mapped to RADIUS Login-Service
Debug: rlm_ldap: LDAP radiusLoginTCPPort mapped to RADIUS Login-TCP-Port
Debug: rlm_ldap: LDAP radiusCallbackNumber mapped to RADIUS Callback-Number
Debug: rlm_ldap: LDAP radiusCallbackId mapped to RADIUS Callback-Id
Debug: rlm_ldap: LDAP radiusClass mapped to RADIUS Class
Debug: rlm_ldap: LDAP radiusSessionTimeout mapped to RADIUS Session-Timeout
Debug: rlm_ldap: LDAP radiusIdleTimeout mapped to RADIUS Idle-Timeout
Debug: rlm_ldap: LDAP radiusLoginLATNode mapped to RADIUS Login-LAT-Node
Debug: rlm_ldap: LDAP radiusLoginLATGroup mapped to RADIUS Login-LAT-Group
Debug: rlm_ldap: LDAP radiusPortLimit mapped to RADIUS Port-Limit
Debug: rlm_ldap: LDAP radiusLoginLATPort mapped to RADIUS Login-LAT-Port
Debug: rlm_ldap: LDAP radiusReplyMessage mapped to RADIUS Reply-Message
Debug: rlm_ldap: LDAP radiusTunnelType mapped to RADIUS Tunnel-Type
```

10 - Neste ponto o freeradius já está configurado para fazer a autenticação com o ldap, para permitir que o cliente, *localhost* seja permitido por padrão:

```
nano /etc/freeradius/clients.conf
```

10.1 – Analisar o ficheiro e fazer as alterações necessárias:

É neste arquivo onde define-se quais os *access points* são clientes. Um exemplo disso são as seguintes linhas:

```
client private-network-1 {
        ipaddr          = 192.168.0.0
        netmask         = 24
        secret          = testing123
        shortname       = private-network-1
}
```

Nota: Para fazer testes de serviço existem aplicativos como o NTRadPing compatível com o Windows e de fácil utilização.

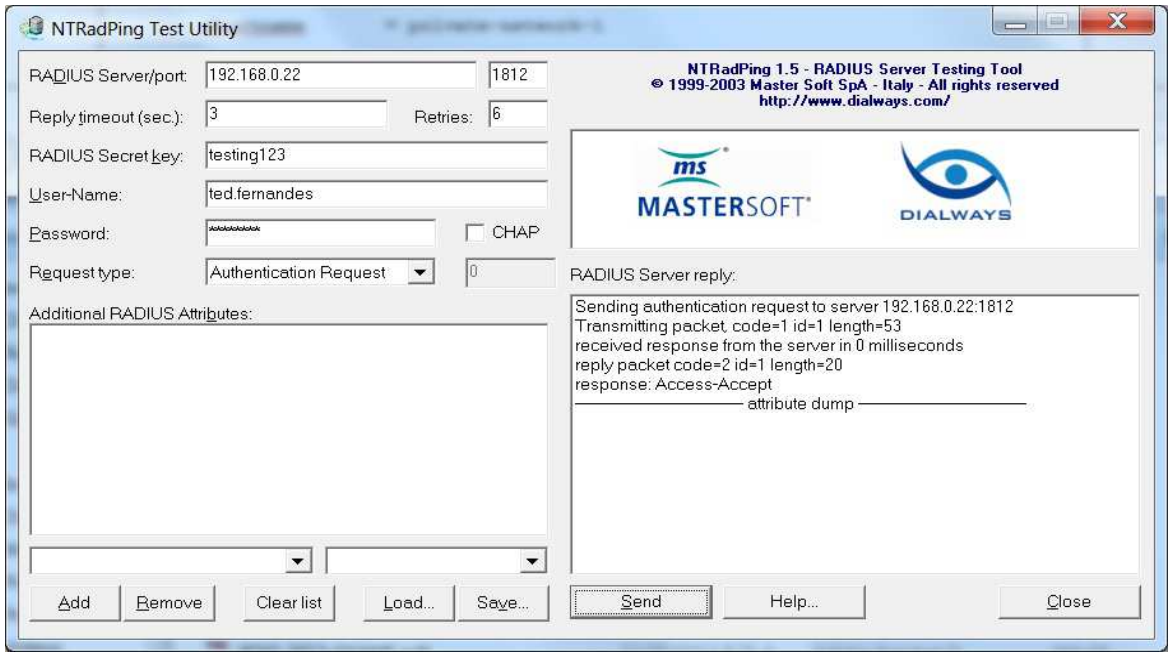

Figura 17: Teste de conectividade ao servidor RADIUS de um utilizador através da aplicação NTRadPing [Fonte: Autor]

Também existe o comando "radtest" que funciona da seguinte maneira por exemplo:

```
radtest ted.fernandes "*******" 192.168.0.244 0 testing123
```

"testing123" é a chave secreta definida no ficheiro clients.conf, conforme é mostrado no passo 10.

ANEXO V - CONFIGURAÇÃO DO *ACCESS POINT*

Aceder ao *Access Point* através do *browser* seguido das suas credenciais.

1 - Deixar as configurações de acordo como mostra a imagem abaixo para este caso:

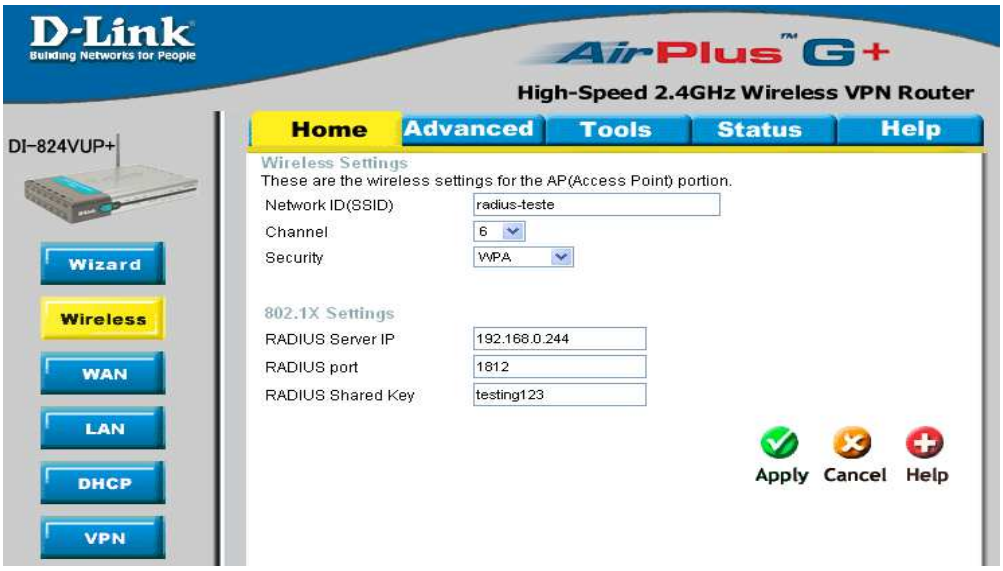

Figura 18: Configuracação do *access point* para o suporte ao RADIUS [Fonte: Autor]

2 - Configurar a rede no ambiente Windows XP:

- Primeiro é criada a conexão com o AP-RADIUS, depois que ela falhar, é necessário ir em "alterar configurações avançadas":

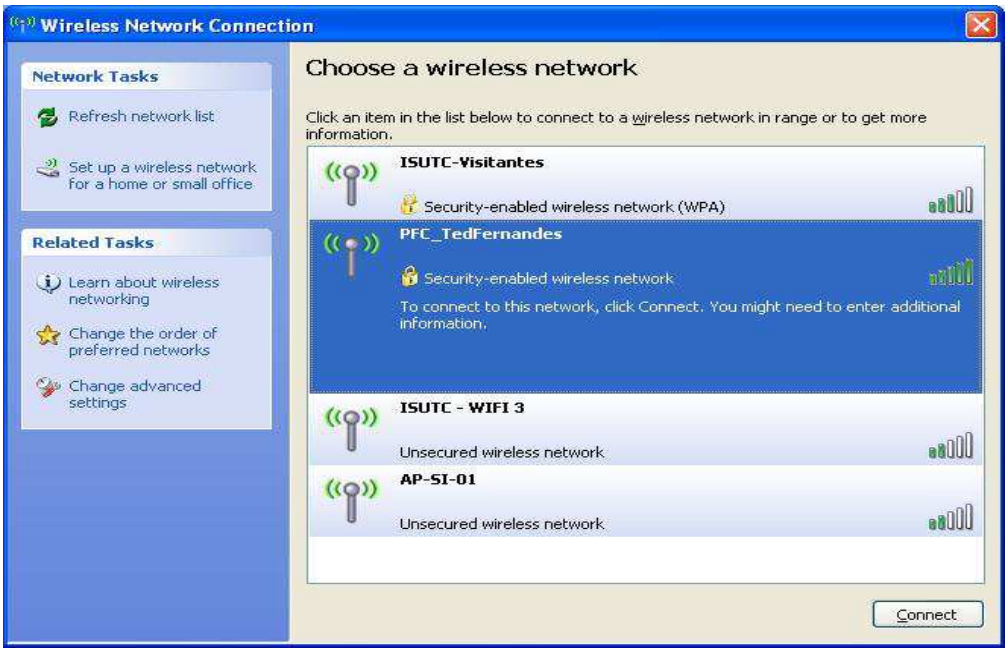

Figura 19: *Access Points* disponíveis ao redor [Fonte: Autor]

- Editar as conexões de rede sem fio:

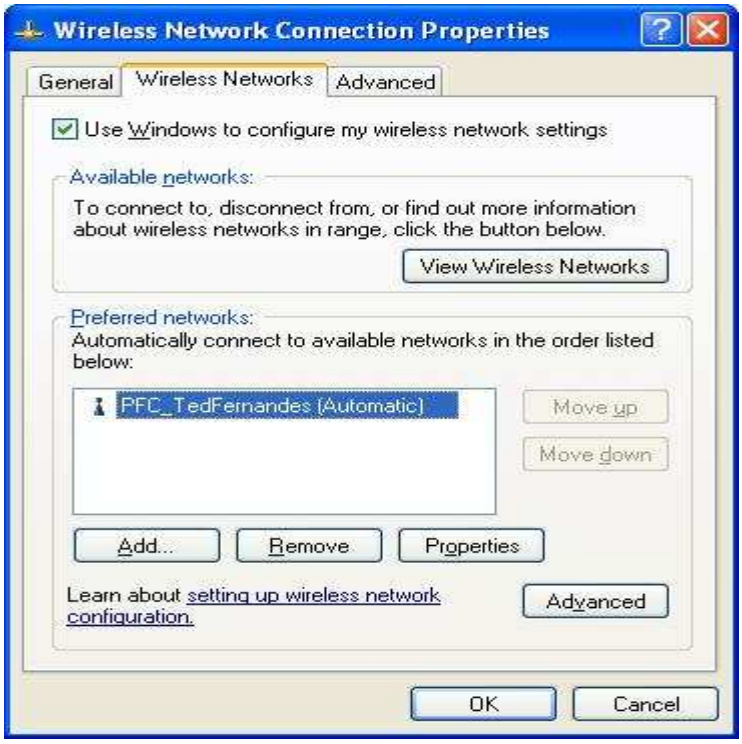

Figura 20: Propriedades da conexão local da rede [Fonte: autor]

- Clicando em proriedades, devemos definir o método de autenticação para *Protected EAP (PEAP)*:

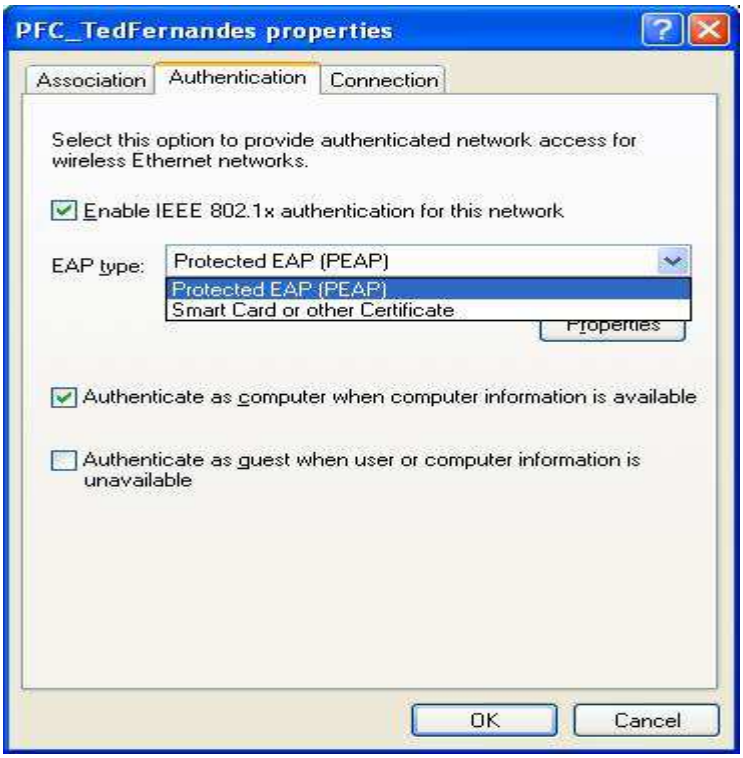

Figura 21: Propriedades do *Access Point* em questão [Fonte: Autor]

- Depois volte e edite as configurações avançadas, agora deve-se desmarcar "Validar certificado do servidor":

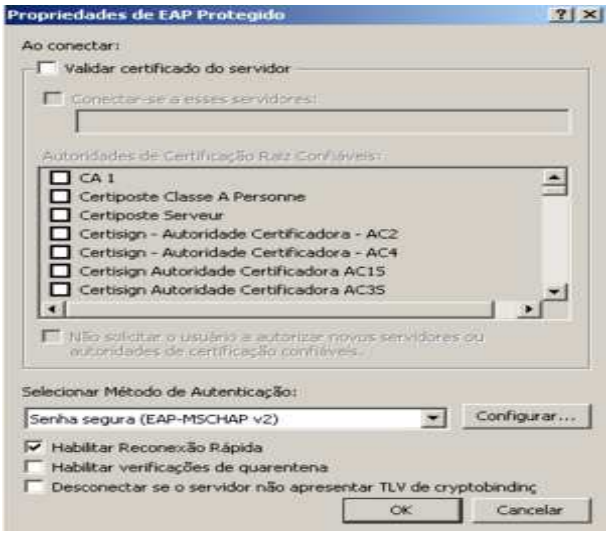

Figura 22: Propriedades do método de autenticação usado [Fonte: Autor]

- Depois configurar o MSCHAPv2, desmarcando o *logon* automático de rede:

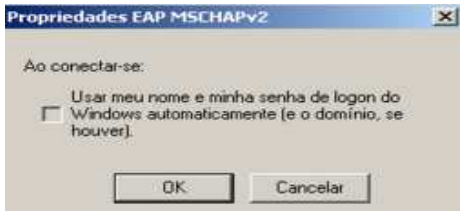

Figura 23: Desmarcação do *logon* automático [Fonte: Autor]

- Com isso, ao tentar conectar ao AP-RADIUS, será questionado pela sua autenticação:

Figura 24: Janela para a digitação das credenciais [Fonte: Autor]

- A partir daí o Windows XP deve autenticar e conectar normalmente:

3 - Configurando a rede no ambiente Windows 7

Para configurar a rede no Windows 7, é só seguir os mesmos passos que o do Windows XP, bastando primeiro, criar manualmente uma conexão wireless com um SSID igual ao do *access point*.

Nota: Para o caso do Windows 8 (Tanto para PC como para o Nokia Lumia), Ubuntu 10.04 Desktop, Android (Versão 2.33 para cima) e iOS (versão 4 para cima), já não há necessidades dessas configurações adicionais para o lado do cliente, bastando simplesmente conectar a rede. Esses foram os sistemas operativos usados para a realização de testes.