

JULIANA C. MOURA CAMPOS  
MARCELLA MARIA. ROBERTO  
MARCELO AGUIAR STENICO  
SAMANTA CAMARGO POSSOBOM  
THIAGO RIBEIRO MENDES

## **SEGURANÇA DE REDES**

Pontifícia Universidade Católica de Campinas  
Faculdade de Engenharia de Computação  
Maio – 2005

Juliana C. Moura Campos	R.A: 01056811
Marcella Maria Roberto	R.A: 01041250
Marcelo Aguiar Stenico	R.A: 01006048
Samanta Camargo Possobom	R.A: 01034982
Thiago Ribeiro Mendes	R.A: 01030980

## **SEGURANÇA DE REDES**

*Trabalho apresentado como exigência da disciplina Tópicos em Engenharia Computação A, ministrada no Curso de Engenharia de Computação na PUC-Campinas, sob orientação do Prof. Ricardo Freitas.*

Pontifícia Universidade Católica de Campinas  
Faculdade de Engenharia de Computação

Maio – 2005



## SUMÁRIO

LISTA DE FIGURAS .....	IV
INTRODUÇÃO.....	1
1. TECNOLOGIAS DE IDENTIDADE .....	2
1.1 Senhas Seguras .....	2
1.1.1 Protocolo de Senhas S/Key .....	2
1.1.2 Esquemas De Autenticação De Senha Simbólicas .....	4
1.2 Protocolos de Autenticação PPP .....	5
1.2.1 O Protocolo PPP .....	5
1.2.2 Protocolo PAP .....	6
1.2.3 Protocolo SPAP .....	7
1.2.4 Protocolo CHAP .....	8
1.3 Protocolos que Usam Mecanismos de Autenticação .....	9
1.3.1 Protocolo RADIUS.....	10
1.3.2 Protocolo KERBEROS.....	11
2. TECNOLOGIAS DE SEGURANÇA PARA CAMADA DE REDE .....	14
2.1 IPsec .....	14
2.1.1 Protocolos do IPsec .....	14
2.2 Associação de Segurança.....	20
2.3 Banco de Dados de Segurança .....	21
2.4 Gerenciamento de Chaves .....	21
2.4.1 Primeira etapa de negociação ISAKMP .....	22
2.4.2 Segunda etapa da negociação ISAKMP .....	23
2.5 Geração de Chaves .....	24
3. TECNOLOGIAS DE SEGURANÇA PARA CONEXÕES DIAL-UP .....	25
3.1 O Protocolo de Tunelamento Ponto-a-Ponto.....	25
3.1.1 Conexão .....	26
3.1.2 Arquitetura PPTP.....	26
3.1.3 Mecanismos de Segurança do PPTP .....	27
3.2 The Layer 2 Forwarding (L2F) protocol .....	28
3.2.1 Negociação do Protocolo.....	28
3.2.2 Autenticação .....	29
3.2.3 Formato do Datagrama .....	29
3.3 Protocolo para Tunelamento na Camada de Enlace .....	30
3.3.1 Operação.....	30
3.3.2 Autenticação .....	31
3.3.3 Formato do Datagrama .....	31
3.3.4 Funcionamento .....	32
3.3.5 PPTP x L2TP .....	32
4. Tecnologias e Segurança para Redes Wireless e sistemas de comunicações móveis .....	34
4.1 WPAN (Wireless Personal Area Network) .....	35
4.2 WLAN (Wireless Local Area Network).....	36
4.3 WMAN (Wireless Metropolitan Area Network).....	39
4.4 WWAN (Wireless Wide Area Network).....	40
CONCLUSÃO.....	42
BIBLIOGRAFIA.....	43

## LISTA DE FIGURAS

Figura 1: Passos no processo da autenticação do protocolo Kerberos. ....	12
Figura 2: Campos do protocolo AH. ....	15
Figura 3: Modo transporte do protocolo AH. ....	16
Figura 4: Modo túnel do protocolo AH.....	17
Figura 5: Campos do protocolo ESP. ....	18
Figura 6: Modo transporte do protocolo ESP.....	19
Figura 7: Modo túnel do protocolo ESP. ....	20
Figura 8: Primeira Etapa: Modo principal da negociação. ....	23
Figura 9: Primeira Etapa: Modo agressivo da negociação. ....	23
Figura 10: Segunda Etapa: Modo rápido da negociação.....	24
Figura 11: Funcionamento do L2TP .....	32
Figura 12: PPTP x L2TP .....	33
Figura 13: Símbolos Warchalking .....	37

## INTRODUÇÃO

Existem muitas tecnologias de segurança que projetam soluções para acesso a rede e para mecanismos de transporte de dados dentro da infra-estrutura de rede corporativa. Muitas das tecnologias sobrepõem-se ao resolverem problemas que relacionam assegurar o usuário (identidade do dispositivo), integridade de dados, e confiabilidade de dados.

Autenticação é o processo de validar a identidade reivindicada de um usuário final ou um dispositivo (como clientes, servidores, switches, routers, firewalls, e assim por diante). Autorização é o processo de conceder acesso direto a um usuário, grupos de usuários, ou sistema específicos; controle de acesso limita o fluxo de informações dos recursos de um sistema para só as pessoas autorizadas ou sistemas na rede. Na maioria dos casos autorização e controle de acesso são subsequentes ao sucesso da autenticação.

Este documento descreve tecnologias de segurança geralmente utilizadas para estabelecer identidade (autenticação, autorização, e controle de acesso) como também por assegurar algum grau de integridade de dados e confidencialidade a uma rede. Integridade de dados assegura que o dado não foi alterado ou foi destruído exceto por pessoas explicitamente autorizadas a tal ato; confidencialidade de dados assegura que só as entidades permitidas a visualização dos dados os vejam em um formato utilizável.

A intenção é desenvolver uma compreensão básica de como estas tecnologias podem ser implementadas em redes e identificar suas forças e fraquezas. As categorias seguintes foram selecionadas em uma tentativa para se agrupar os protocolos de acordo com atributos compartilhados:

- Tecnologias de Identidade;
- Tecnologias de Segurança para Camada de Rede;
- Tecnologias de Segurança para Conexões Dial-Up;
- Tecnologias e Segurança para Redes Wireless e sistemas de comunicações móveis.

## 1. TECNOLOGIAS DE IDENTIDADE

Descreve as tecnologias primárias utilizadas para estabelecer identidade ao host, ao usuário final, ou ambos. Autenticação é um elemento extremamente crítico porque tudo está baseado em quem você é. Em muitas redes, você não concederia acesso autorizado a partes específicas da rede antes de estabelecer quem está tentando ganhar acesso a recursos restritos. O grau de simplicidade do método de autenticação depende da tecnologia utilizada.

Uma das fraquezas potenciais em alguns métodos de autenticação é em quem você confia, podemos categorizar métodos de autenticação como os de controle local e os que provêm verificação de autenticação por uma terceira parte confiável, que quando utilizada para autenticar um usuário final ou dispositivo há sempre a possibilidade de que essa autenticação tenha alguma falha.

### 1.1 *Senhas Seguras*

Embora senhas são freqüentemente utilizadas como prova na autenticação de um usuário ou dispositivo, elas podem ser facilmente comprometidas se forem fáceis de adivinhar, se não forem mudadas freqüentemente, e se forem transmitidas em texto aberto por uma rede. Para se ter senhas mais seguras, métodos mais robustos são oferecidos, codificando a senha ou modificando a criptografia de forma que o valor codificado mude de tempos em tempos, este é o caso utilizado pela maioria dos esquemas de senha, o mais comum é o protocolo S/Key e os esquemas de autenticação de senhas simbólicos.

#### 1.1.1 **Protocolo de Senhas S/Key**

O S/Key foi lançado pela Bellcore e está definida na RFC 1760, ele é um esquema de geração de senhas descartáveis, com isso, evita o ataque de captura ou adivinhação de senhas, porque a próxima conexão requererá uma senha diferente.

O protocolo de S/Key é projetado para se opor a um ataque de retomada quando um usuário estiver tentando se logar em um sistema. Um ataque de retomada no contexto de login é quando alguém escutar as escondidas uma conexão de rede para adquirir o login ID e senha de um usuário legítimo, utilizando então essas informações posteriormente para ganhar acesso à rede.

A operação do protocolo de S/Key é baseado em cliente/servidor: o cliente é tipicamente um PC, e o servidor é preferencialmente UNIX. Inicialmente, devem ser configurados o cliente e o servidor com a mesma frase como senha e um mesmo contador de repetição, este contador especifica quantas vezes uma determinada entrada será aplicada à função de hash.

O cliente inicia o S/Key enviando um pacote de inicialização; o servidor responde com um número de sucessão, o cliente computa a senha, processo que envolve três passos distintos, são eles: um passo preparatório, um passo de geração, e uma função de produção.

1. No passo preparatório, o cliente entra com uma frase secreta. Esta frase de passagem é concatenada com a mensagem que foi transmitida do servidor em texto aberto.
2. No passo de geração se aplica a função hash múltiplas vezes, produzindo um resultado final de 64-bit.
3. A função de produção pega a senha descartável de 64-bit e mostra em forma legível.

A última fase é para o cliente passar a senha descartável ao servidor onde poderá ser verificada.

O servidor tem um arquivo contendo, para cada usuário, a senha descartável do último login. Para verificar a tentativa de autenticação, o servidor de autenticação passa a senha descartável recebida uma vez pela função hash. Se o resultado desta operação combinar com a senha descartável prévia armazenada, a autenticação tem êxito e a senha descartável aceita é armazenada para uso futuro.

O número de aplicações da função hash executada pelo cliente diminui a cada vez, isto assegura uma sucessão de senhas diferentes geradas. Porém, depois de um tempo, o usuário deve reinicializar o sistema para evitar ser incapaz de logar novamente.

S/Key é uma alternativa simples e livre, implementações comerciais são amplamente encontradas.

### **1.1.2 Esquemas De Autenticação De Senha Simbólicas**

Sistemas de autenticação simbólicos geralmente requerem o uso de um cartão especial (chamado smart card ou cartão de símbolo), embora algumas implementações de software aliviam o problema de perder o cartão inteligente ou cartão de símbolo, os mecanismos de autenticação estão baseados no sistema desafio/resposta. Os passos seguintes mostram este esquema:

Passo 1: O usuário pede conexão em um servidor de autenticação que então emite um lembrete para um usuário ID.

Passo 2: O usuário provê o ID ao servidor que então emite um desafio, um número randômico que se aparece na tela do usuário.

Passo 3: O usuário entra com aquele número de desafio no cartão simbólico ou inteligente, o dispositivo então codifica o desafio com a chave de criptografia do usuário e exibe uma resposta.

Passo 4: O usuário digita esta resposta e envia isto ao servidor de autenticação. Enquanto o usuário estiver obtendo uma resposta do símbolo, o servidor de autenticação calcula o que a resposta apropriada deveria ser baseada em seu banco de dados de chaves de usuário.

Passo 5: Quando o servidor receber a resposta do usuário, compara aquela resposta com a que calculou. Se as duas respostas combinarem, é concedido acesso à rede ao usuário. Se elas não combinarem, acesso é negado.

Uso do esquema desafio-resposta exige que o usuário que leve um dispositivo que proveja credenciais de autenticação. Este pode ser um fardo a alguns usuários porque eles têm que se lembrar de levar o dispositivo, mas tem a flexibilidade para permitir acesso autenticado bastante seguro em qualquer lugar do mundo. É extremamente útil para usuários móveis que freqüentemente se conectam de locais remotos. Se os usuários móveis tiverem seu próprio laptop, o símbolo pode ser instalado como software que alivia o fardo de se lembrar de levar um dispositivo

adicional. Estes esquemas são muito robustos e escaláveis do ponto de vista de banco de dados centralizado.

## **1.2 Protocolos de Autenticação PPP**

A autenticação PPP é realizada por um processo na segunda fase da conexão. Durante a primeira fase, ambos, servidor e cliente, concordam em utilizar um único e específico canal de comunicação chamado Protocolo PPP (Point to Point Protocol - Protocolo de ponto a ponto).

A família Windows suporta os seguintes protocolos de autenticação remota PPP: Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), Challenge Handshake Authentication Protocol (CHAP) e Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versões 1 e 2. Esses protocolos de autenticação visam prover, mas não garantem totalmente, proteção contra ataques de retomada, personificação de cliente remoto e do servidor de acesso remoto.

Senhas estão incorporadas em muitos protocolos que provêm serviços de autenticação. Para conexões dial-in, o protocolo PPP é freqüentemente utilizado.

### **1.2.1 O Protocolo PPP**

O protocolo PPP é utilizado para enviar datagramas através de uma conexão serial, e permite que ambos os lados da conexão negociem certas opções como endereços IP e o tamanho máximo dos datagramas, além de prover modos de autenticação do cliente.

PPP provê um Protocolo de Controle de Ligação extensível (LCP) e uma família de Protocolos de Controle de Rede (NCPs) para negociar parâmetros de configuração opcionais e instalações. Depois que a ligação foi estabelecida, PPP provê para uma fase de autenticação opcional antes de proceder à fase de protocolo da camada de rede.

Ele é implementado no Linux em duas partes: a primeira é implementada através de módulos do kernel e a segunda através do serviço pppd. Os módulos do kernel são carregados dinamicamente quando necessários, e são eles os

responsáveis pelas interfaces virtuais pppX (onde X é um número), utilizadas em conexões discadas. O serviço pppd auxilia o kernel executando as funções de inicialização e autenticação, que precedem o envio ou recebimento de informações através da conexão.

Ao se iniciar uma conexão, o pppd utilizará um dispositivo serial (um modem ligado a uma porta serial, como, por exemplo) ligando-o ao modo PPP e criando assim a interface ppp0, que a partir desse momento funcionará de maneira bastante semelhante a uma interface de rede comum (ethernet). O pppd procede então com a autenticação utilizando para isso a autenticação via PAP ou via CHAP. O pppd pode ser configurado também para alterar as rotas padrões do sistema de acordo com a nova conexão estabelecida.

As Negociações de PPP consistem em LCP e NCP. LCP é responsável para estabelecer a conexão com certas opções negociadas, mantendo a conexão, e provendo procedimentos para terminar a conexão. Para Executar estas funções, LCP é organizado nas quatro seguintes fases:

1. Estabelecimento da ligação e negociação de configuração;
2. Determinação de qualidade da ligação;
3. Negociação da configuração do protocolo da camada de rede;
4. Encerramento da ligação.

Para estabelecer comunicações ponto-a-ponto, cada fim da ligação tem que enviar primeiro pacotes LCP para configurar os dados. Depois que a ligação foi estabelecida, PPP provê uma fase de autenticação opcional antes de proceder à próxima etapa.

### **1.2.2 Protocolo PAP**

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

não oferece nenhuma proteção contra ataques de retomada, personificação de cliente ou do servidor de autenticação.

O uso do protocolo PAP é negociado durante a negociação do protocolo LCP. Uma vez que a negociação do protocolo LCP esteja estabelecida, mensagens do protocolo PAP vão usar o ID 0xC0-23 do protocolo PPP.

Funcionamento:

- O cliente de acesso remoto envia uma mensagem de pedido de autenticação PAP ao servidor de acesso remoto contendo o nome de usuário e senha do cliente em texto aberto;
- O servidor de acesso remoto então confere o nome de usuário e senha do cliente e envia de volta uma mensagem PAP Authenticate-Ack quando as credenciais do usuário estiverem corretas ou uma mensagem PAP Authenticate-Nak quando as credenciais do usuário estiverem incorretas.

Para fazer com que o servidor de acesso remoto seja seguro, basta desabilitar então o protocolo de autenticação PAP. Porém, clientes de acesso remoto mais antigos ou os que não apoiem protocolos de autenticação seguros estarão impossibilitados de se conectar ao servidor.

### **1.2.3 Protocolo SPAP**

O Shiva Password Authentication Protocol (SPAP) é um protocolo de mão dupla. Servidores de acesso remoto Shiva empregam mecanismo de criptografia reversível. Um cliente de acesso remoto Windows pode usar o protocolo SPAP para se autenticar em um servidor Shiva. Pode também usar o protocolo SPAP para se autenticar em um servidor de acesso remoto da família Windows. O protocolo SPAP é mais seguro do que o protocolo PAP, mas menos seguro que o protocolo CHAP ou MS-CHAP. Esse protocolo não oferece nenhuma proteção contra personificação do servidor de acesso remoto.

O uso do protocolo SPAP é negociado durante a negociação do protocolo LCP. Uma vez que a negociação do protocolo LCP esteja estabelecida, mensagens do protocolo SPAP vão usar o ID 0xC0-27 do protocolo PPP.

Assim como o PAP, o SPAP também é um protocolo simples de troca de mensagens:

- O cliente de acesso remoto envia um pedido de autenticação SPAP contendo o nome de usuário e senha codificada do cliente remoto;
- O servidor de acesso remoto decifra a senha e confere o nome de usuário e envia de volta uma mensagem SPAP Authenticate-Ack quando as credenciais do usuário estiverem corretas ou uma mensagem SPAP Authenticate-Nak com a razão pelo qual as credenciais do usuário estavam incorretas.

#### **1.2.4 Protocolo CHAP**

O Challenge Handshake Authentication Protocol (CHAP) é um protocolo de autenticação de desafio de resposta documentado na RFC 1994. Ele usa o protocolo de criptografia Message Digest 5 (MD5) de um só sentido para responder a um desafio de resposta hash emitido pelo servidor de acesso remoto.

O protocolo CHAP é usado por vários servidores e clientes Dial-up inclusive os da família Windows.

O protocolo CHAP é uma melhoria em cima do protocolo PAP, pois a senha, nunca é enviada em cima da primeira mensagem. Ao invés, a senha é usada para criar uma string hash de desafio de um só sentido. O servidor sabe a senha do cliente e duplica a operação para comparar o resultado das respostas do cliente.

O uso do protocolo CHAP é negociado durante a negociação do protocolo LCP e usa o algoritmo 0x05. Uma vez que a negociação do protocolo LCP esteja estabelecida, mensagens do protocolo CHAP vão usar o ID 0xC2-23 do protocolo PPP.

O CHAP é um protocolo de troca de mensagens que usa três mensagens:

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

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

O protocolo CHAP protege contra ataques de retomada usando uma string hash de desafio arbitrário por tentativa de autenticação. Porém, ele não protege contra personificação de servidor remoto.

### ***1.3 Protocolos que Usam Mecanismos de Autenticação***

A autenticação é importante quando uma corporação oferece acesso em sua rede privada, através de uma rede pública como a Internet a funcionários que estão em trânsito, e que, precisam acessar a rede para atualizar ou consultar informações vitais.

O usuário distante, com o cliente de autenticação instalado em seu computador, tenta uma conexão com um endereço dentro da rede protegida pelo mecanismo servidor de autenticação, esse, verifica que o computador remoto tem o cliente de autenticação e que possui uma regra válida na estratégia de segurança, subseqüentemente, o servidor fornece o acesso, entretanto, o acesso é válido para um período limitado de tempo, depois do qual o processo de autenticação será requerido novamente.

Muitos protocolos requerem verificação de autenticação antes de prover autorização e propriedade de acesso ao usuário ou dispositivo. RÁDIO e Kerberos são exemplos de tais protocolos. Eles são freqüentemente usados em ambientes dial-in para prover um banco de dados de autenticação escaláveis, podendo incorporar uma variedade de métodos de autenticação.

O protocolo RADIUS é adequado em sistemas de serviços remotos discados, enquanto o KERBEROS, pode ser utilizado através de qualquer tipo de conexão, a autenticação e um dos pontos forte na segurança de qualquer sistema, pois tem a finalidade de atravessar os mecanismos de segurança para autenticar o usuário, autorizando ou não a sua conexão.

### 1.3.1 Protocolo RADIUS

O RADIUS autentica através de uma série de comunicações entre o cliente e o servidor. Uma vez que o usuário é autenticado, o cliente proporciona a ele, o acesso aos serviços apropriados. Os passos envolvidos no processo do RADIUS estão descritos a baixo:

- O PortMaster cria um pacote de dados com as informações e o chama de “pedido de autenticação”. Este pacote inclui a informação que identifica o PortMaster específico que envia o pedido de autenticação, a porta que está sendo usada para a conexão de modem, identificação do usuário e a senha. Para proteger os dados de hackers que possam estar escutando a conexão, o PortMaster age como um cliente RADIUS e codifica a senha antes que seja enviada em sua jornada ao servidor RADIUS;
- Quando um pedido de autenticação é recebido, o servidor de autenticação valida o pedido e então decifra o pacote de dados para ter acesso a identificação do usuário e senha. Esta informação é passada para o sistema de segurança apropriado;
- Se o usuário e senha estiverem corretos, o servidor envia um reconhecimento de autenticação que inclui informação sobre o usuário e as exigências dos serviços. Por exemplo, o servidor RADIUS contará para o PortMaster que um usuário precisa do Protocolo PPP (ponto-a-ponto) para se conectar à rede. O reconhecimento pode também, conter filtros, com informações sobre os limites de acesso do usuário para os recursos específicos na rede. Se o usuário e a senha não estiverem corretos, o servidor RADIUS envia um sinal ao PortMaster e o usuário terá o acesso negado à rede.
- Uma vez que a informação é recebida pelo PortMaster, o servidor RADIUS envia uma chave de autenticação, ou assinatura, se identificando para o cliente RADIUS e permitindo então, a configuração necessária para que os serviços de envios e recepções personalizados, funcione para o usuário autenticado.

### 1.3.2 Protocolo KERBEROS

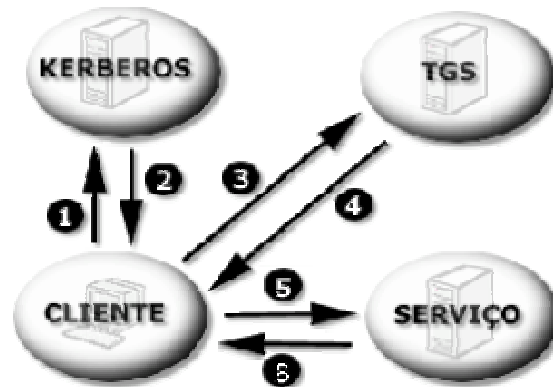
KERBEROS é um serviço de autenticação distribuído que permite que um cliente, através de um usuário, prove sua identidade a um servidor de autenticação, passando em seguida por um verificador de sessão, para que então, estabeleça a transferência das informações com o host destino, evitando assim, a violação da conexão estabelecida. Esse protocolo foi desenvolvido no meado dos anos Oitenta como parte do Projeto de MIT Athena. Hoje em dia, é uma das soluções aos problemas de segurança em rede, pois fornece ferramentas de autenticação e criptografia para trabalhos em redes públicas como a Internet.

Muitos dos protocolos usados na Internet não provêm segurança. Ferramentas que varrem senhas fora da rede são usadas em brechas de sistemas. Assim, aplicações que enviam senha sem criptografia pela rede Internet são extremamente vulneráveis. Contudo, em muitas aplicações cliente/servidor que são desenvolvidas e implementadas, não é dada a devida atenção sobre os aspectos aqui mencionados.

Alguns administradores tentam usar Firewalls para resolver os problemas de segurança de rede. Infelizmente, os Firewalls assumem que os acessos ruins estão todos do lado de fora, o que freqüentemente, é uma suposição muito ruim, pois usuários e colaboradores em trânsito, ficam restringidos de usar a rede interna, pois os mecanismos de segurança vão descartar suas tentativas de acesso.

O sistema KERBEROS usa ingressos eletrônicos para autenticar um usuário para um servidor. Um ingresso só é bom para um único servidor e um único usuário durante um certo período de tempo e para uma mensagem codificada que contém o nome do usuário, o seu servidor, o endereço da rede do servidor do usuário, um selo de tempo e uma chave de sessão. Uma vez que o usuário adquire este ingresso, ele pode usar isto para ter acesso ao servidor quantas vezes forem necessárias até que o ingresso se expire. O usuário não pode decifrar o ingresso, mas pode apresentá-lo ao servidor. Com isso, escutas clandestinas não podem violar o ingresso quando este estiver em curso na rede Internet.

O protocolo KERBEROS envolve dois servidores, um de autenticação e o outro (TGS) que concede os ingressos. Os passos envolvidos no processo do protocolo KERBEROS estão descritos a seguir:



**Figura 1: Passos no processo da autenticação do protocolo Kerberos.**

- Obter um ingresso para um servidor designado. O usuário primeiro pede ao servidor de autenticação KERBEROS um ingresso para o KERBEROS TGS. Este pedido leva a forma de uma mensagem que contém o nome do usuário e o nome do TGS (pode haver vários);
- O servidor de autenticação verifica o usuário em seu banco de dados e então gera uma chave de sessão para ser usada entre o usuário e o TGS. KERBEROS codifica esta chave de sessão que usa a chave de segredo do usuário (processo de uma só direção com senha do usuário). Então cria um TGT (ingresso que concede ingresso) para o usuário apresentar ao TGS e codifica o TGT usando a chave de segredo do TGS (que só é conhecido pelo servidor de autenticação e o servidor TGS). O Servidor de Autenticação envia de volta as mensagens codificadas ao usuário;
- O usuário decifra a primeira mensagem e recupera a chave de sessão. Logo, o usuário cria um autenticador que consiste em seu nome, seu endereço de rede e um selo de tempo, tudo codificado com a chave de sessão gerada pelo servidor de autenticação KERBEROS. O usuário envia o pedido então ao TGS para fazer ingresso a um servidor designado. Este pedido contém o nome do servidor, o TGT KERBEROS (que foi codificado com o a chave de segredo do TGS), e o autenticador codificado;
- O TGS decifra o TGT com sua chave secreta e então usa a chave de sessão incluída no TGT para decifrar o autenticador. Compara a informação do autenticador com a informação do ingresso, o endereço da rede do usuário com o endereço foi enviado no pedido e o tempo estampado com o tempo

atual. Se tudo se emparelhar, permite a continuação do pedido. O TGS cria uma chave de sessão nova para o usuário e o servidor final com esta chave em um ingresso válido para o usuário apresentar ao servidor. Este ingresso também contém o nome do usuário, endereço da rede, um selo de tempo, e um tempo de vencimento para o ingresso codificado com a chave de segredo do servidor designado e o seu nome. O TGS também codifica a nova chave de sessão designada que vai ser compartilhada entre o usuário e o TGS. Envia ambas as mensagens de volta ao usuário;

- O usuário decifra a mensagem e a chave de sessão para uso com o servidor designado. O usuário está agora pronto para se autenticar com o servidor. Ele cria um autenticador novo codificado com a chave de sessão de usuário e servidor final que o TGS gerou. Para pedir acesso ao servidor final, o usuário envia junto ao ingresso recebido de KERBEROS (que já é codificado com a chave de segredo do servidor designado) o autenticador codificado. O autenticador contém o texto plano codificado com a chave de sessão, prova que o remetente sabe a chave. Da mesma maneira que é importante, codificar o tempo para prevenir que intrometidos que venham registrar o ingresso e o autenticador, possam tentar usar as informações em futuras conexões;
- O servidor designado decifra e confere o ingresso e o autenticador e também confere o endereço do usuário e o selo de tempo. Se tudo confirmar, o servidor sabe agora que o usuário é que esta reivindicando o acesso é realmente ele, e podem usar a chave de criptografia para comunicação segura. (Como só o usuário e o servidor compartilham esta chave, eles podem assumir que uma recente mensagem codificou aquela chave originada com a outra chave anterior);
- Para aplicações que requerem autenticação mútua, o servidor envia para o usuário uma mensagem que consiste no selo de tempo mais 1, codificada com a chave de sessão. Isto serve como prova ao usuário que o servidor soube da sua chave secreta de fato e pôde decifrar o ingresso e o autenticador.

## **2. TECNOLOGIAS DE SEGURANÇA PARA CAMADA DE REDE**

### **2.1 IPsec**

A camada de rede tem como objetivo fornecer a camada de transporte independência quanto a questões de chaveamento e roteamento associadas à operação de uma conexão de rede, este nível da rede esta interligado ao roteamento e seus efeitos, como o controle de congestionamento. A Internet utiliza a arquitetura TCP/IP e especificamente o protocolo IP na camada de rede cujo serviço é de datagramas e não confiável. O IP não possui nenhum esquema de segurança, para solucionar esse problema foi desenvolvido um conjunto de protocolos, denominado IPsec, para prover serviços de segurança no protocolo IP utilizando protocolos de segurança de dados, de autenticação de cabeçalho, de encapsulamento seguro de dados e de procedimentos e protocolos de gerência de chaves.

O IPsec foi padronizado para garantir interoperabilidade e mecanismos de criptografia para o IPv4 e também IPv6. O IPsec oferece este serviço independentemente do algoritmo de criptografia utilizado, ou seja, é uma arquitetura aberta possibilitando o uso de outros algoritmos de autenticação e criptografia.

#### **2.1.1 Protocolos do IPsec**

Os serviços de segurança do IPsec são oferecidos através de dois protocolos, o Authentication Header (Autenticação de Cabeçalho – AH) e o Encapsulation Security Payload (Encapsulamento Seguro de Dados – ESP), estes dois protocolos fazem parte da arquitetura básica do IPsec e por questões de garantia de interoperabilidade, esses protocolos estabelecem que todas as implementações IPsec suportem alguns algoritmos predefinidos.

Ao longo do tempo vários algoritmos surgiram e como o IPsec é uma arquitetura aberta podemos utilizar diversos algoritmos conforme a necessidade. Temos como exemplo de criptografia os algoritmos DES, Blowfish, 3-DES, CAST, AES, SERPENT, TWOFISH, entre outros e como exemplo de autenticação os

algoritmos HMAC, MD5, SHA1, SHA2. Note que essa lista poderá ser modificada, alguns desses protocolos se tornarão obsoletos, seja por motivo de suspeitas de fragilidade ou até mesmo pela quebra e eficiência. Como IPsec possui uma arquitetura aberta não é problema a troca dos protocolos defasados por novos protocolos mais seguros.

### 2.1.1.1 Authentication Header (AH)

O protocolo AH adiciona autenticação e integridade, ou seja, garante autenticidade do pacote e também que este não foi alterado durante a transmissão. O AH previne ataques do tipo Replay onde um invasor captura os pacotes de uma conexão replica-os e os reenvia como se fosse a entidade que estava enviando primeiramente os pacotes. Também previne ataques do tipo Spoofing onde o invasor assume o papel de uma entidade confiável e ganha privilégios na comunicação. E por ultimo o Hijacking onde o invasor captura um pacote da conexão e passa a participar da comunicação. Para a autenticação é utilizada uma função de hash, utilizando as chaves negociadas durante o estabelecimento da Associação de Segurança (SA). O resultado da operação de hash é colocado dentro do campo de Dados de Autenticação. O receptor irá calcular novamente o hash e comparar com o resultado que está no campo de Dados de Autenticação, se forem iguais a autenticação é bem sucedida caso contrario houve alguma interferência na conexão. Embora a autenticação ocorra no cabeçalho IP, nem todos os campos podem ser autenticados, por que alguns dos campos do cabeçalho IP mudam de valor durante a transmissão do pacote IP ate seu destino. Campos do protocolo AH:

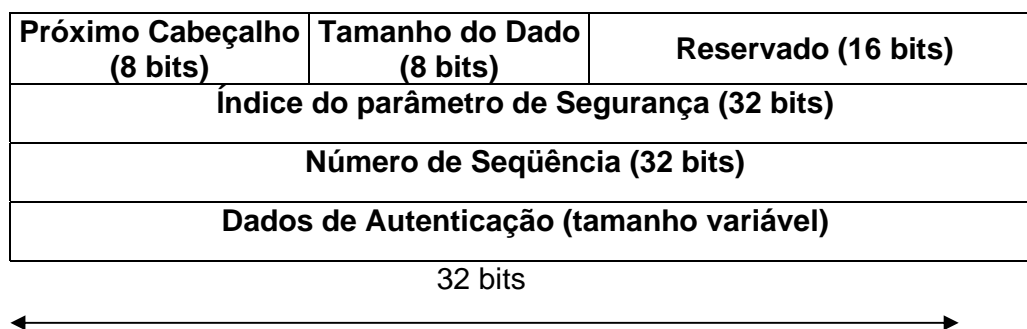
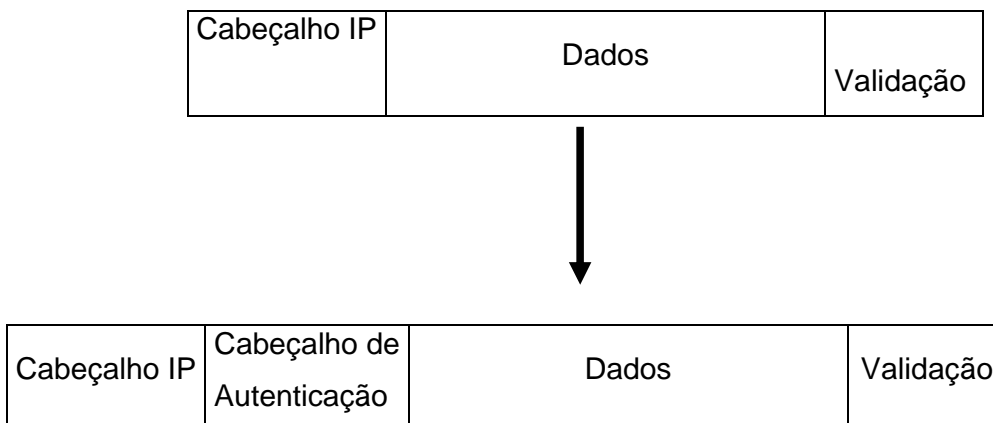


Figura 2: Campos do protocolo AH.

O cabeçalho de autenticação contém seis campos a saber:

- **Próximo Cabeçalho** – Contém o identificador do protocolo do próximo cabeçalho, é o mesmo valor atribuído ao campo Protocolo do cabeçalho IP;
- **Tamanho do Dado** – Comprimento do cabeçalho de autenticação e não o comprimento do dado;
- **Reservado** – 16 bits reservados para extensão do protocolo;
- **SPI** – Índice que identifica unicamente uma SA para um determinado pacote;
- **Número de Seqüência** – Contador que identifica os pacotes pertencentes a uma determinada AS;
- **Dados de Autenticação** – Campo de comprimento variável que contém o ICV (Integrity Check Valeu), este é calculado pela função de hash.

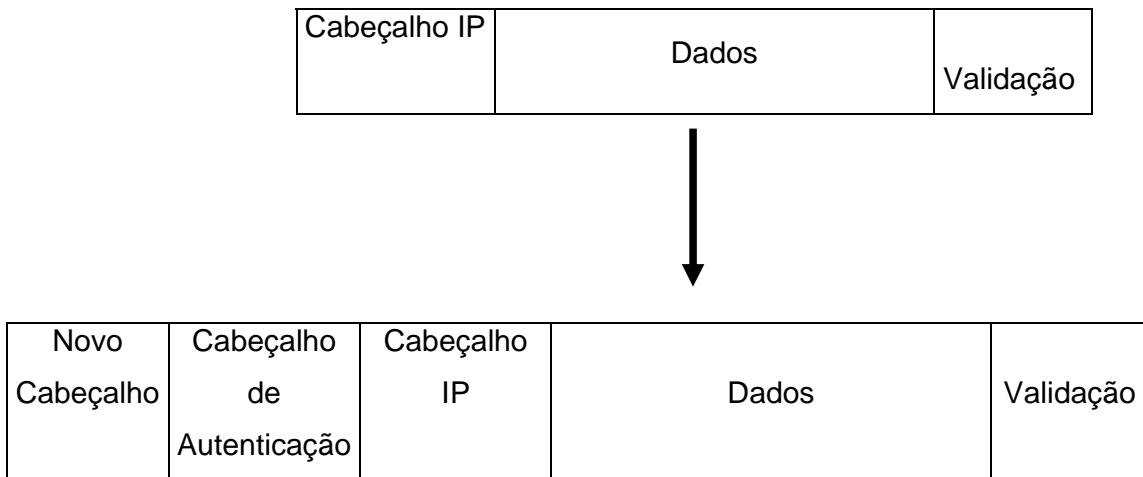
O protocolo AH pode ser utilizado no modo transporte e no modo túnel. No modo de transporte o cabeçalho original é mantido e um cabeçalho de autenticação é inserido. No cabeçalho original o valor do campo protocolo é alterado, o valor original é colocado dentro do cabeçalho de autenticação e no seu lugar é colocado o valor 51 correspondente ao protocolo AH.



**Figura 3: Modo transporte do protocolo AH.**

No modo túnel um novo cabeçalho é criado para o pacote IP e, também, é colocado o cabeçalho de autenticação. O pacote original fica intacto e é encapsulado dentro do novo pacote IP, desta forma a autenticação é feita em todo pacote IP original. A desvantagem desse modo é que necessita de mais

processamento para construir o pacote de depois voltar à condição original do pacote.

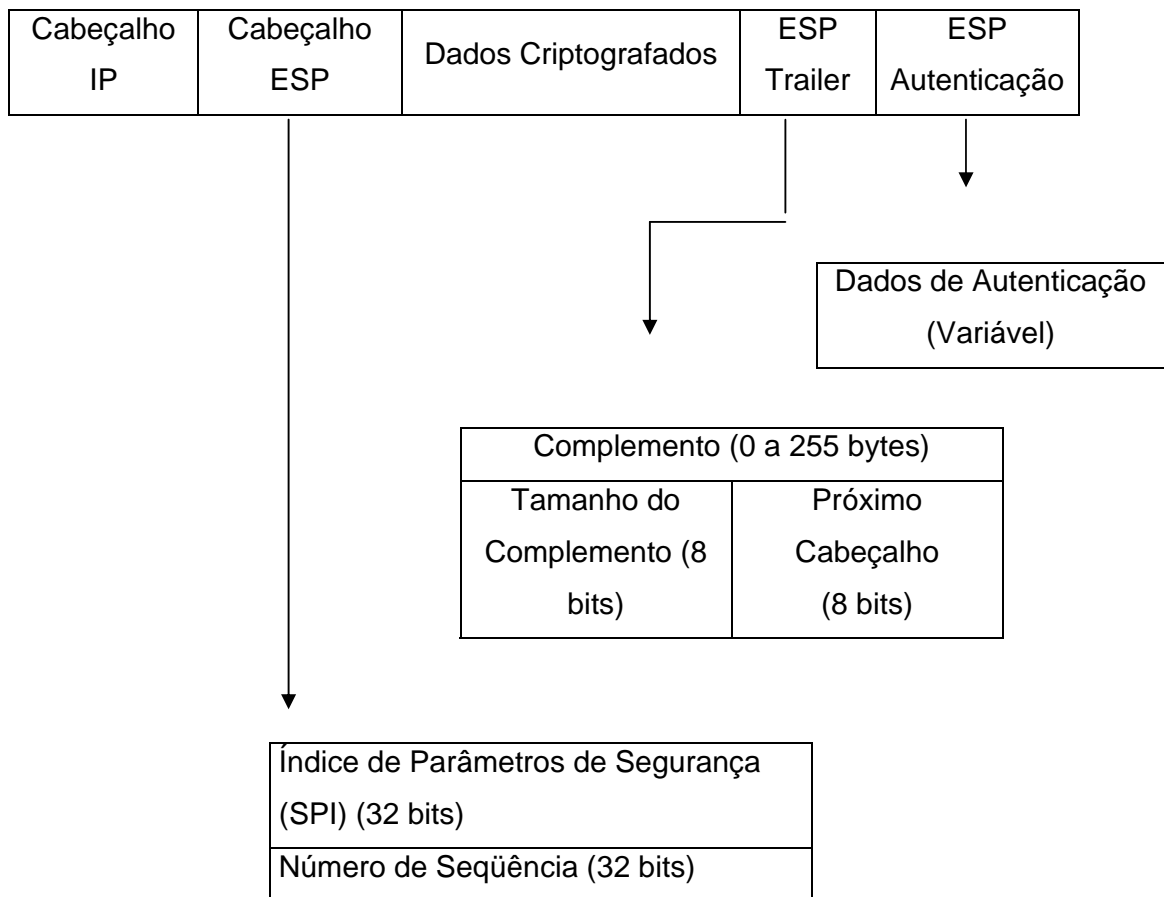


**Figura 4: Modo túnel do protocolo AH.**

Observa-se que em nenhum dos dois modos de utilização do protocolo AH a confidencialidade é tratada. Os dados trafegam na rede intactos e desprotegidos podem ser capturados por alguém mal intencionado e conseqüentemente ele poderá ter acesso aos dados que estão sendo carregados por este pacote.

### 2.1.1.2 Encapsulation Security Payload (ESP)

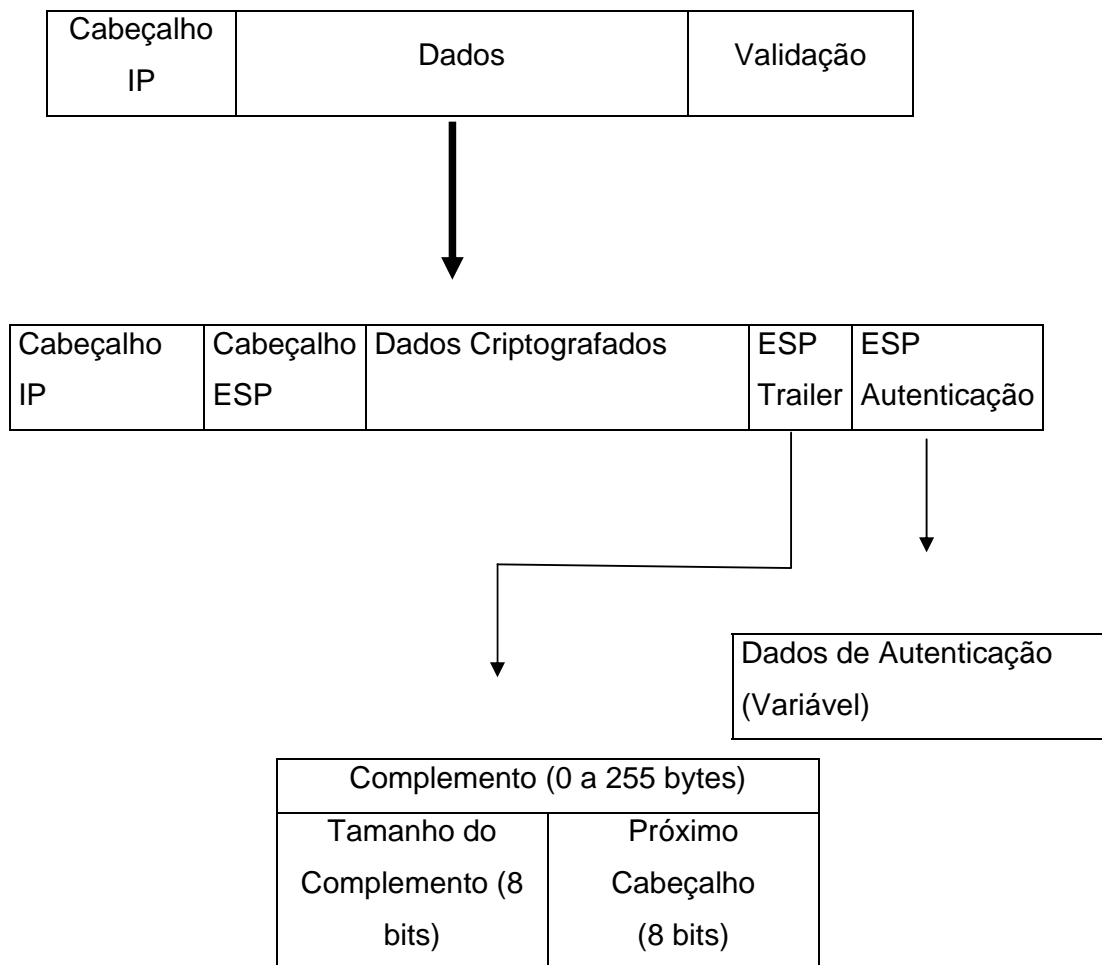
O protocolo de Encapsulamento de Dados (ESP) fornece autenticação e confidencialidade das informações através da criptografia e proteção contra replay. Assim como o AH alguns campos são inseridos no pacote, alguns destes campos têm o mesmo comportamento do AH. Estes campos estão contidos no cabeçalho ESP e também no segmento de autenticação que está localizado no final do pacote IP. Quando é utilizada criptografia o campo Dados contém informações de sincronismo da criptografia, permitindo que a descriptografia possa ocorrer na entidade de destino. Note que se nenhum algoritmo de criptografia for selecionado, o que é possível, o protocolo ESP apenas fornecerá autenticação como faz o protocolo AH.



**Figura 5: Campos do protocolo ESP.**

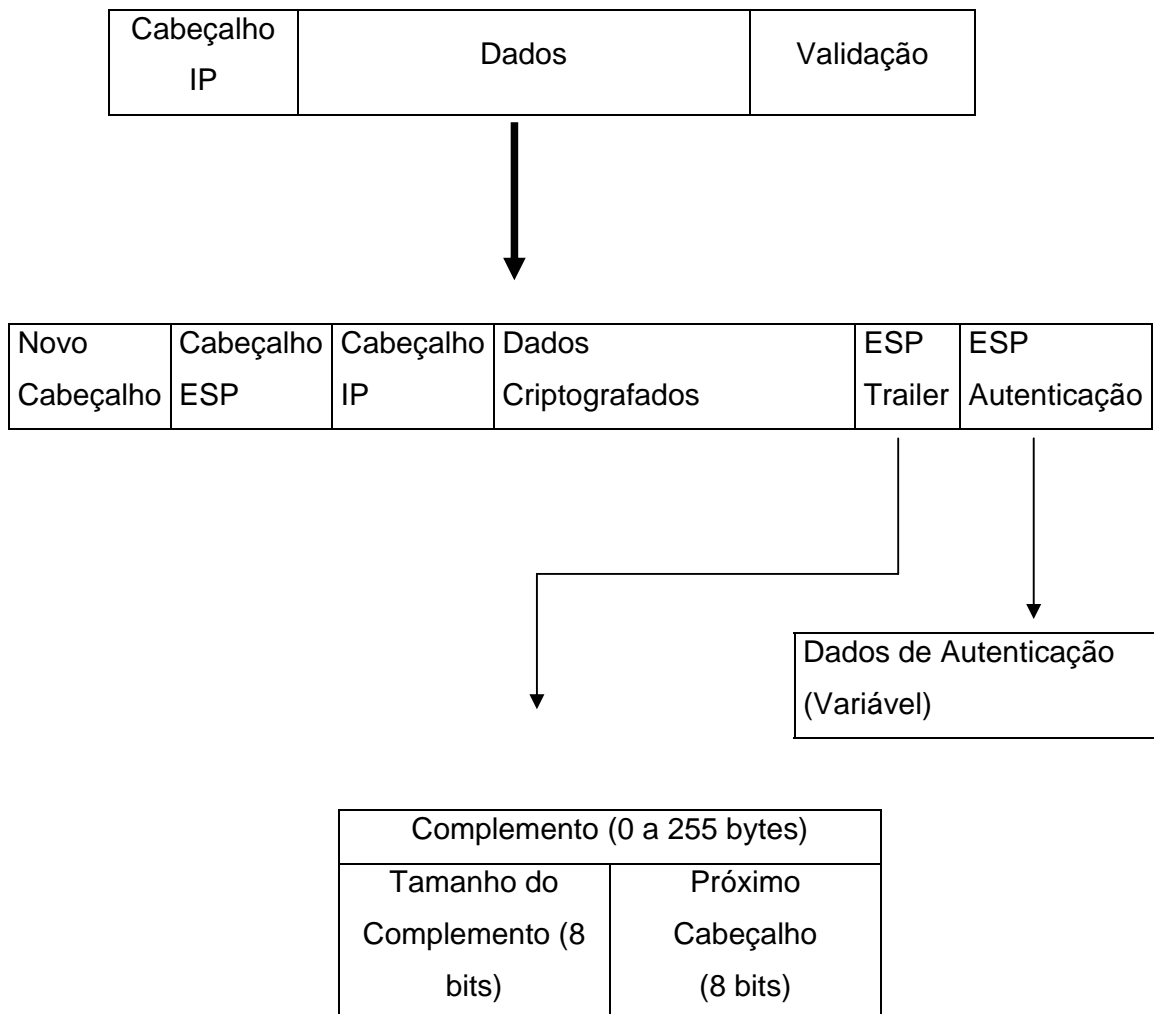
Como podemos perceber, o pacote resultante será maior que o pacote original e este acréscimo é um ponto importante a ser analisado já que o tamanho máximo do pacote normalmente é de 1500 bytes. Este valor é denominado MTU (Maximum Transmission Unit). Se o tamanho do pacote ultrapassar o valor do MTU irá ocorrer uma fragmentação. Neste caso, o processo ocorrerá somente no pacote não fragmentado, ou seja, caso o pacote original não comporte os dados adicionais, este deve ser fragmentado antes do processamento do ESP cabendo ao gateway que irá receber o pacote descriptografar as informações e remontá-las novamente.

Assim como o AH o ESP pode, também, ser utilizado no modo de transporte ou no modo túnel. No modo de transporte o cabeçalho ESP é inserido entre o cabeçalho IP e os dados. Da mesma forma que o AH o cabeçalho original é mantido no novo pacote sendo assim o ESP no modo transporte só pode ser usado entre servidores ou hosts.



**Figura 6: Modo transporte do protocolo ESP.**

No modo túnel, todo o pacote original é colocado dentro de um novo pacote sendo gerado um novo cabeçalho IP e um cabeçalho ESP. Se o túnel for estabelecido entre dois servidores ou hosts, os endereços de destino e origem do novo cabeçalho serão os mesmos do cabeçalho original que está criptografado no pacote original. Se o túnel for estabelecido entre gateways, como roteadores ou firewall, os endereços de origem e destino do novo cabeçalho serão dos gateways e os endereços dentro do pacote original criptografado serão dos hosts ou servidores atrás dos gateways.



**Figura 7: Modo túnel do protocolo ESP.**

## **2.2 Associação de Segurança**

O conceito de Security Association (Associação de Segurança – SA) é muito importante, uma SA define os tipos de medidas de segurança aplicadas aos pacotes baseados em quem está enviando os pacotes, para onde eles estão indo e que tipo de dados estão conduzindo. As informações das SA podem ser trocadas dinamicamente entre as entidades que irão usar as informações da SA no momento que as entidades quiserem utilizar os serviços de segurança oferecidos pelo IPsec. Outra opção é o administrador da rede estabelecer SAs fixas para cada entidade.

Para identificar uma SA são necessários três parâmetros: IP destino, identificação do protocolo de segurança, e o índice do parâmetro de segurança

(Security Parameter Index – SPI). O SPI é um número que identifica uma AS, assim todos os membros de uma SA devem conhecer o SPI e usá-lo durante a comunicação. Uma SA é unidirecional, se duas entidades forem trocar informações será necessário negociar uma outra SA. Durante a negociação da SA serão definidas as chaves, os algoritmos de criptografia e autenticação e os parâmetros usados por estes algoritmos.

### **2.3 Banco de Dados de Segurança**

Dois bancos de dados são utilizados pelo Ipsec, o banco de dados de políticas de segurança (Security Policy Database – SPD) e o banco de dados de associações de segurança (Security Association Database – SAD). Um administrador define um conjunto de políticas de segurança para todos os tipos de tráfego IP de entrada e saída. As políticas de segurança são definidas e mantidas no SPD para serem utilizadas no processamento dos pacotes IPs e na construção de SAs quando for necessário. O SAD contém um conjunto de parâmetros associados a AS. Cada SA tem uma entrada nessa tabela especificando tudo que é necessário ao processamento do IPsec para cada pacote IP.

Quando um pacote IP chega ao host, a SA é localizada através do endereço IP de destino, do tipo de protocolo e do SPI. Se uma SA for localizada o pacote é processado de acordo com o serviço de segurança especificado. Depois disso, o processamento do pacote segue para o SPD. Quando um pacote está saindo, o SPD é processado primeiro, se o pacote atender as políticas especificadas no IPsec, o SAD tentará determinar se a SA já foi estabelecida, se a SA estiver estabelecida o processamento do pacote será de acordo com a SA, caso a SA não esteja estabelecida uma nova SA será negociada para o pacote.

### **2.4 Gerenciamento de Chaves**

Os serviços de segurança IPsec compartilham chaves secretas que são utilizadas para autenticação, integridade e criptografia. As especificações IPsec definem um mecanismo separado para o gerenciamento dessas chaves com suporte para distribuição manual ou automática das chaves. Para a distribuição das

chaves foram especificados procedimentos baseados em chaves públicas sendo possível utilizar o ISAKMP/OAKLEY (Internet Security Association and Key Management Protocol). O ISAKMP define o método de distribuição das chaves e o OAKLEY define como as chaves serão distribuídas.

Uma SA pode ser configurada manualmente por um administrador de segurança ou de forma dinâmica por meio de um protocolo de gerência de chaves como o IKE (Internet Key Exchange). Este mecanismo é muito interessante, pois não se sabe quando será preciso estabelecer uma conexão segura, uma SA não deve ter tempo de vida infinito é recomendável que a SA seja trocada de tempos em tempos e como consequência suas chaves de criptografia devem também ser trocadas. O IKE é baseado no ISAKMP, este define como duas entidades instituirão um canal de comunicação seguro entre elas para isso os participantes devem se autenticar trocando informações de chaves e negociando serviços de segurança. Entretanto não especifica como a autenticação é feita ou quais as chaves serão geradas, ou seja, é definido um caminho seguro deixando o conteúdo para que outro protocolo especifique.

O ISAKMP define duas fases de negociação da associação de segurança. A primeira fase é a negociação entre as duas entidades ISAKMP, ou seja, as duas entidades concordam em como proteger a comunicação entre elas estabelecendo uma associação de segurança, que não é uma SA do IPsec, a SA do ISAKMP é bidirecional e não se aplica ao tráfego IPsec.

A segunda fase que normalmente trata da negociação da associação de segurança entre outros protocolos, no caso o IPsec. Uma SA ISAKMP pode negociar várias SA do IPsec, reduzindo o tempo de negociação da SA entre as entidades participantes, pois como uma SA já foi estabelecida na fase um esta torna-se mais rápida.

#### **2.4.1 Primeira etapa de negociação ISAKMP**

Primeira etapa é subdividida em dois modos de negociação, modo principal (Main Mode) e modo agressivo (Aggressive Mode).





### **3. TECNOLOGIAS DE SEGURANÇA PARA CONEXÕES DIAL-UP**

As Virtual Private Dial-Up Networks (VPDNs), redes que proporcionam acesso à rede corporativa por usuários remotos, através de uma linha discada (provedor de acesso), permitem que as grandes corporações estendam suas redes privadas através das linhas dial-up. Ao invés de incorrer grandes custos para garantir a segurança ou diminuir a segurança da localidade para qualquer lugar do mundo, novas tecnologias habilitam usuários remotos a uma conexão segura à infraestrutura da corporação utilizando o acesso dial-up com a Internet.

A diferença principal entre uma Virtual Private Network (VPN) e uma VPDN é que a conexão na VPN entre o servidor e o cliente é feita via Internet, o que barateia os custos no caso de clientes geograficamente distantes do servidor, enquanto em uma VPDN o cliente disca diretamente para o servidor.

Atualmente existem três protocolos similares que realizam esse objetivo:

- The Point-to-Point Tunneling Protocol (PPTP) - Protocolo de Tunelamento Ponto-a-Ponto
- The Layer 2 Forwarding (L2F) protocol
- The Layer 2 Tunneling Protocol (L2TP) – Protocolo para Tunelamento na Camada de Enlace

#### ***3.1 O Protocolo de Tunelamento Ponto-a-Ponto***

O Protocolo de Tunelamento Ponto-a-Ponto (PPTP), desenvolvido por um fórum de empresas (Microsoft, Ascend Communications, 3Com, ECI Telematics e US Robotics), foi um dos primeiros protocolos de VPN a surgirem. Ele tem sido uma solução muito utilizada em VPDNs desde que a Microsoft incluiu suporte para Servidores Windows NT 4.0 e ofereceu um cliente PPTP em um service pack para Windows 95, o que praticamente assegura seu uso continuado nos próximos anos.

O protocolo mais difundido para acesso remoto na Internet é o PPP (Point-to-Point Protocol), o qual originou o PPTP. O PPTP agrega a funcionalidade do PPP

para que o acesso remoto seja tunelado através da Internet para um site de destino. O PPTP encapsula pacotes PPP usando uma versão modificada do protocolo de encapsulamento genérico de roteamento (GRE), que dá ao PPTP a flexibilidade de lidar com outros tipos de protocolos diferentes do IP, como o IPX e o NetBEUI.

Devido a sua dependência do PPP, o PPTP se baseia nos mecanismos de autenticação do PPP, os protocolos PAP e CHAP.

Entretanto, este protocolo apresenta algumas limitações, tais como não prover uma forte criptografia para proteção de dados e não suportar qualquer método de autenticação de usuário através de token.

### 3.1.1 Conexão

Em uma conexão PPTP, existem três elementos envolvidos: o Cliente PPTP, o Servidor de Acesso a Rede (NAS - Network Access Server) e o Servidor PPTP.

O cliente se conecta a um NAS, através de um PoP em um ISP local. Uma vez conectado, o cliente pode enviar e receber pacotes via Internet. O NAS utiliza TCP/IP para todo o tráfego de Internet.

Depois do cliente ter feito a conexão PPP inicial com o ISP, uma segunda chamada dial-up é realizada sobre a conexão PPP existente. Os dados desta segunda conexão são enviados na forma de datagramas IP que contém pacotes PPP encapsulados. É esta segunda conexão que cria o túnel com o servidor PPTP nas imediações da LAN corporativa privada.

### 3.1.2 Arquitetura PPTP

A comunicação segura criada pelo PPTP tipicamente envolve três processos, cada um deles exigindo que os anteriores sejam satisfeitos. Esses três processos são:

- **Conexão e Comunicação PPP:** o cliente PPTP usa o PPP para se conectar ao ISP utilizando uma linha telefônica ou ISDN padrão. O PPP é utilizado aqui para estabelecer a conexão e criptografar os dados;

- **Conexão de Controle PPTP:** Utilizando a conexão estabelecida pelo PPP, o PPTP cria um controle de conexão desde o cliente até o servidor PPTP na Internet. Esta conexão utiliza o TCP e é chamada de túnel PPTP;
- **Tunelamento de Dados PPTP:** O PPTP cria os datagramas IP contendo os pacotes PPP criptografados e os envia através do túnel até o servidor PPTP. Neste servidor, os datagramas são então desmontados e os pacotes PPP descriptografados para que finalmente sejam enviados até a rede privada corporativa.

No primeiro processo, o PPP, protocolo que permite enviar dados multi-protocolares encapsulados através de redes TCP/IP, é utilizado para desempenhar três funções: iniciar e terminar conexões físicas, autenticar usuários e criar datagramas PPP contendo pacotes criptografados.

No segundo processo, o PPTP especifica uma série de mensagens de controle a serem trocadas entre o cliente PPTP e o servidor PPTP. Estas mensagens estabelecem, mantêm e terminam os túneis PPTP. Elas são enviadas em pacotes de controle dentro de um datagrama TCP através de uma conexão TCP especialmente criada para trocar mensagens de controle.

Após o túnel PPTP ter sido estabelecido, os dados do usuário são finalmente transmitidos entre o cliente PPTP e o servidor PPTP. É importante frisar que o cliente PPTP não necessariamente identifica o usuário numa extremidade da comunicação. Pode haver usuários utilizando máquinas sem suporte ao PPTP e nestes casos, a comunicação PPTP começa a partir do NAS.

### 3.1.3 Mecanismos de Segurança do PPTP

Para garantir a segurança na transmissão, o PPTP faz uso dos seguintes mecanismos:

- **Controle de acesso e autenticação:** a autenticação de usuários remotos é feita utilizando os mesmos métodos do PPP - através dos protocolos PAP, CHAP (Challenge Handshake Authentication Protocol) ou de uma versão da Microsoft, o MS-CHAP;

- **Criptografia de dados:** o PPTP utiliza os métodos de criptografia e compressão do PPP;
- **Filtragem de pacotes PPTP:** este recurso do PPTP permite que apenas os pacotes PPTP dos usuários autenticados entrem no servidor PPTP da rede privada;
- **Utilização de firewalls:** o PPTP também oferece recursos para trabalhar com firewalls, através do servidor PPTP.

### ***3.2 The Layer 2 Forwarding (L2F) protocol***

O Protocolo de Encaminhamento de Camada 2 (L2F), desenvolvido pela Cisco Systems, surgiu nos primeiros estágios da criação da tecnologia VPN. Assim como o PPTP, o L2F foi desenvolvido para criação de túneis em tráfegos de usuários para suas redes corporativas.

Uma grande diferença entre o PPTP e o L2F é a de que este último não possui tunelamento dependente do IP, sendo capaz de trabalhar diretamente com outros meios, como Frame Relay e ATM. Tal qual o PPTP, o L2F usa o PPP (Point-to-Point Protocol) para autenticação de usuários remotos, mas pode incluir também suporte para autenticação via TACACS e RADIUS. Outra grande diferença com o PPTP é a de que o L2F permite que os túneis possam dar conta de mais de uma conexão.

Há também dois níveis de autenticação do usuário, uma pelo ISP antes do estabelecimento do túnel e outra quando a conexão é efetuada no gateway da corporação. Pelo fato de ser um protocolo de camada 2, o L2F oferece aos usuários a mesma flexibilidade que o PPTP em lidar com outros protocolos diferentes do IP, tais como IPX e NetBEUI.

#### **3.2.1 Negociação do Protocolo**

Quando um usuário deseja se conectar ao gateway da intranet corporativa, ele primeiro estabelece uma conexão PPP com o NAS do ISP. A partir daí, o NAS

estabelece um túnel L2F com o gateway. Finalmente, o gateway autentica o nome de usuário e senha do cliente, e estabelece a conexão PPP com o cliente.

O NAS (Servidor de Acesso a Rede) do ISP local e o gateway da Intranet estabelecem um túnel L2F que o NAS utiliza para encaminhar os pacotes PPP até o gateway. A VPN de acesso se estende desde o cliente até o gateway.

### 3.2.2 Autenticação

Quando uma sessão VPN - L2F é estabelecida, o cliente, o NAS e o gateway da intranet usam um sistema triplo de autenticação via CHAP. O CHAP é um protocolo de autenticação por contestação/resposta na qual a senha é enviada como uma assinatura de 64 bits ao invés de texto simples. Isto possibilita a transmissão segura da senha do usuário entre a estação do cliente e o gateway de destino.

Primeiro, o NAS contesta o cliente e o cliente responde. Em seguida, o NAS encaminha esta informação de CHAP para o gateway, que verifica a resposta do cliente e devolve uma terceira mensagem de CHAP (sucesso ou fracasso na autorização) para o cliente.

### 3.2.3 Formato do Datagrama

O cabeçalho possui os seguintes campos:

- **Ver:** versão do L2F;
- **Protocol:** protocolo carregado dentro do pacote L2F;
- **Sequence Number:** quando o bit "S" (bit 3) for igual a 1, este campo identifica o número do pacote numa seqüência;
- **Multiplex ID:** identifica uma conexão dentro de um túnel;
- **Client ID:** campo utilizado para auxiliar a demultiplexação em túneis;
- **Length:** indica o tamanho do pacote em octetos, sem levar em conta o campo de checksum;
- **Offset:** quando o bit "F" (bit 0) for igual a 1, este campo identifica aonde começa a área de dados do pacote indicando o número de bytes após o cabeçalho;

- **Key:** o campo de chave está presente se o bit "K" (bit 1) for igual a 1. Serve como chave durante toda a sessão para resistir a ataques de "spoofing";
- **Checksum:** o campo de checksum está presente se o bit "C" (bit 12) for igual a 1.

### ***3.3 Protocolo para Tunelamento na Camada de Enlace***

O Protocolo de Tunelamento de Camada 2 (L2TP) vem sendo desenvolvido pela IETF como um substituto aparente para o PPTP e o L2F, corrigindo as deficiências destes antigos protocolos para se tornar um padrão oficial internet. Ele utiliza o PPP para prover acesso dial-up que pode ser tunelado através da Internet até um Site. Porém, o L2TP define seu próprio protocolo de tunelamento, baseado no que foi feito com o L2F. Seu transporte vem sendo definido para uma variedade de pacotes, incluindo X.25, Frame Relay e ATM. Para fortalecer a criptografia dos dados, são utilizados os métodos de criptografia do IPsec.

#### **3.3.1 Operação**

O L2TP opera de forma similar ao L2F. Um Concentrador de Acesso L2TP (LAC) localizado no PoP do ISP troca mensagens PPP com usuários remotos e se comunica por meio de requisições e respostas L2TP com o Servidor de Rede L2TP (LNS) para criação de túneis. O L2TP passa os pacotes através do túnel virtual entre as extremidades da conexão ponto-a-ponto. Os quadros enviados pelo usuário são aceitos pelo PoP do ISP, encapsulados em pacotes L2TP e encaminhados pelo túnel. No gateway de destino, os quadros L2TP são desencapsulados e os pacotes originais são processados para a interface apropriada.

O L2TP utiliza dois tipos de mensagem: mensagens de controle e mensagens de dados. As mensagens de controle são usadas para gerenciar, manter e excluir túneis e chamadas. As mensagens de dados são usadas para encapsular os pacotes PPP a serem transmitidos dentro do túnel. As mensagens de controle utilizam um confiável canal de controle para garantir entrega das mensagens.

### 3.3.2 Autenticação

Devido ao uso do PPP para links dial-up, o L2TP inclui mecanismos de autenticação dentro do PPP, os protocolos PAP e CHAP. Outros sistemas de autenticação também podem ser usados, como o RADIUS e o TACACS. Porém, O L2TP não inclui processos para gerenciamento de chaves criptográficas exigidas para a criptografia em suas especificações de protocolo. Para dar conta disso, o L2TP faz uso do IPsec para criptografia e gerenciamento de chaves em ambiente IP.

### 3.3.3 Formato do Datagrama

Os pacotes L2TP para canal de controle e canal de dados utilizam o mesmo formato de cabeçalho. O cabeçalho possui os seguintes campos:

- **Type (bit 0):** identifica o tipo de mensagem. Se o bit for igual a 1 é uma mensagem de controle, se for igual a 0 é uma mensagem de dados;
- **Ver:** identifica o número da versão do protocolo;
- **Length:** identifica o tamanho do pacote em octetos se o bit "L" (bit 1) for igual a 1;
- **Tunnel ID:** indica o identificador do Túnel para controle de conexão;
- **Session ID:** indica o identificador de uma sessão dentro de um túnel;
- **Ns:** indica o número de seqüência para o atual pacote (mensagem ou controle). Sua presença é definida pelo bit "S" (bit 4);
- **Nr:** indica o número de seqüência esperado para o próximo pacote de mensagem de controle. Sua presença também é definida pelo bit "S";
- **Offset Size:** especifica o tamanho do offset (espaço entre o cabeçalho e a área de dados). Sua presença é definida pelo bit "O" (bit 6);
- **Priority (bit 7):** se for igual a 1, o pacote deve receber tratamento preferencial com relação aos outros;
- **Bits X:** reservados para extensões futuras.

### 3.3.4 Funcionamento

Como mostrado na figura 1, os roteadores R1 e R2 fornecem o serviço L2TP. Estes roteadores comunicam-se por protocolo IP, através do caminho composto pela interface Int2, a rede IP e a interface Int3. Neste exemplo, os roteadores R3 e R4 comunicam-se utilizando um túnel L2TP. O túnel Tu1 é estabelecido entre as interfaces Int1 de R1 e Int4 de R2. Qualquer pacote que chegue à interface Int1 de R1 é encapsulado pelo L2TP e enviado pelo túnel Tu1 para R2. R2 então desencapsula o pacote e o transmite na interface Int4 para R4. Quando R4 precisa enviar um pacote para R3, o mesmo caminho, de forma inversa, é seguido.

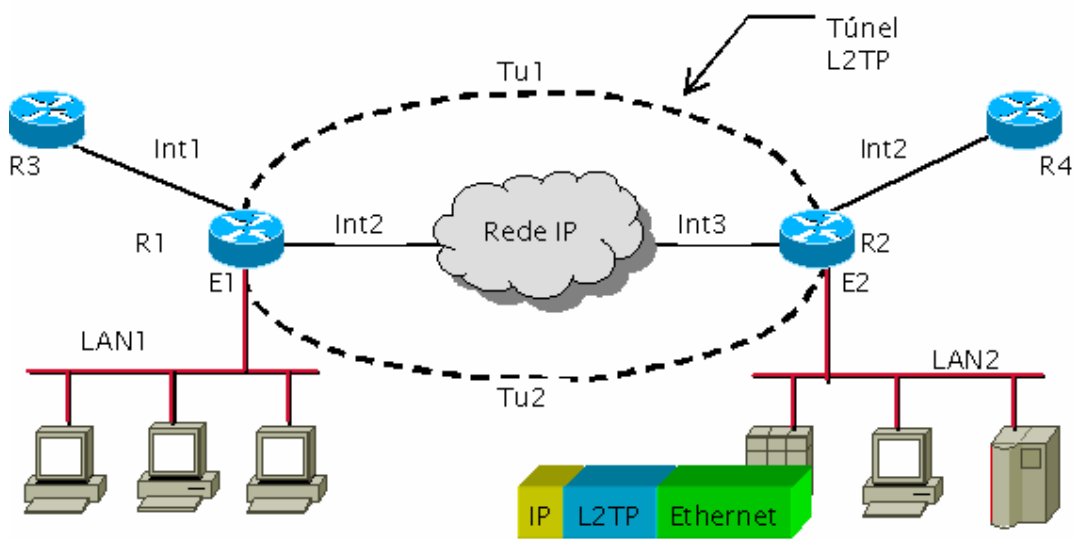


Figura 11: Funcionamento do L2TP

### 3.3.5 PPTP x L2TP

Apesar de parecidos, ambos os protocolos, L2TP ou PPTP, diferenciam-se quanto suas aplicações, ou melhor, a escolha do protocolo a ser utilizado é baseado na determinação da posse do controle sobre o túnel: controlado pelo usuário ou pelo provedor de acesso.

No protocolo PPTP, o usuário remoto tem a possibilidade de escolher o final do túnel, destino dos pacotes. Uma grande vantagem desta característica é que, quando os destinos mudam com muita frequência, nenhuma modificação

(configuração) nos equipamentos por onde o túnel passa se torna necessária. Além disso, os túneis PPTP são transparentes aos provedores de acesso e nenhuma outra ação, além de prover serviço de acesso à rede, se faz necessária. Usuários com perfis diferenciados em relação aos locais de acesso – diferentes cidades, estados e países – se utilizam deste protocolo com mais frequência pelo fato de se tornar desnecessária a intermediação do provedor no estabelecimento do túnel. Somente é necessário saber o número local para o acesso e o sistema do usuário, seu laptop, realizará o resto.

A desvantagem do protocolo L2TP é que, como o controle está na mão do provedor, o mesmo está fornecendo um serviço extra que poderá ser cobrado.

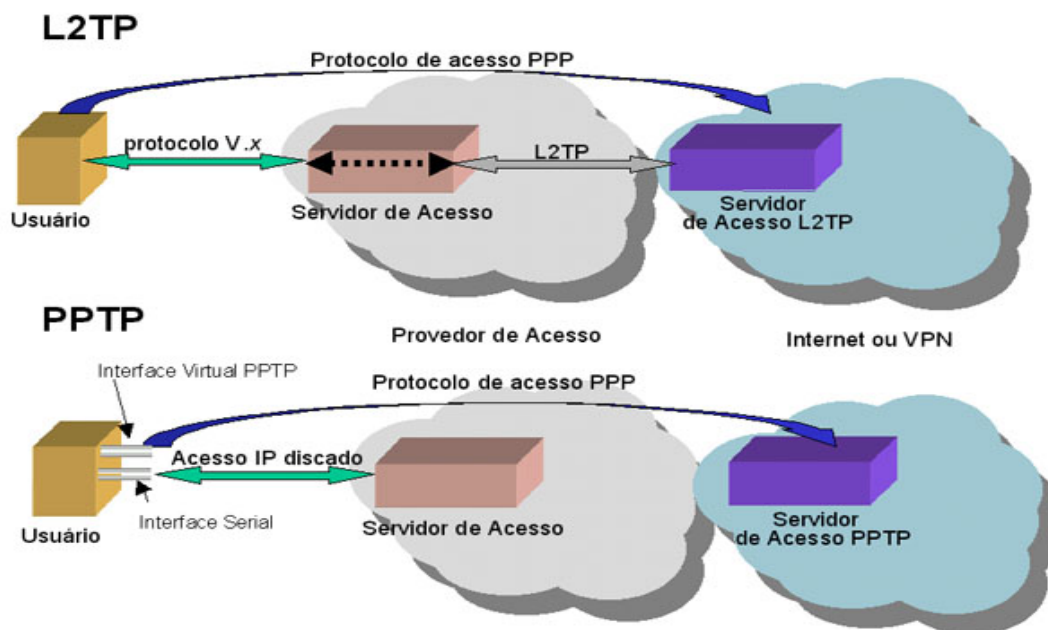


Figura 12: PPTP x L2TP

## 4. Tecnologias e Segurança para Redes Wireless e sistemas de comunicações móveis

A palavra wireless provém do língua inglesa e significa sem fio, ou seja, wire (fio, cabo) e less (sem). Assim, wireless caracteriza o tipo de conexão para transmissão de informações sem a utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio e transmitidos através do ar, ou seja, a rede estabelece a comunicação de dados entre os pontos da rede e os dados são modulados na portadora de rádio e transmitidos no ar através de ondas eletromagnéticas.

Uma tecnologia como esta, que oferece mobilidade, flexibilidade, promove a interligação e economia em infra-estrutura de cabeamento, tem sido muito utilizada e difundida.

Apesar de amplamente utilizada, redes sem fio oferecem diversas vulnerabilidades que colocam em risco a confidencialidade, integridade, autenticidade e disponibilidade da comunicação. Como conseqüência, preocupações com a segurança são inerentes, fazendo com que mecanismos de defesa para combater a vulnerabilidade e ataques sejam indispensáveis.

A tecnologia de comunicação wireless é composta de padrões estabelecidos pelo IEEE - Institute of Electrical and Electronics Engineers. Dentro deste modelo de comunicação, enquadram-se várias tecnologias como: Padrões 802.11, Wi-Fi, InfraRed (infravermelho), bluetooth e WiMax. Tais tecnologias, podem ser aplicadas cada qual no tipo de rede mais adequado.

Os tipos de redes podem ser:

- WPAN (Wireless Personal Area Network) – rede com um alcance pequeno que efetua a comunicação entre dispositivos pessoais. Por exemplo, celulares ou PDAs (Personal Digital Assistats);
- WLAN (Wireless Local Area Network) – rede local, entre equipamentos que se encontram em um mesmo ambiente. Por exemplo, residências ou empresas;
- WMAN (Wireless Metropolitan Area Network) – rede que oferece uma cobertura geográfica maior que as WLAN e altas taxas de transmissão.

Essa conexão é utilizada na prática entre os provedores de acesso e seus pontos de distribuição;

- WWAN (Wireless Wide Area Network) – rede com grandes dispersões geográficas, voltadas para aplicações móveis que utilizem telefones celulares.

#### **4.1 WPAN (*Wireless Personal Area Network*)**

Infrared e bluetooth se aplicam às WPANs, realizando a interoperabilidade entre dispositivos próximos.

A comunicação InfraRed é a mais comum conexão sem fio e está presente há mais tempo no nosso cotidiano. Esta conexão utiliza raios infravermelhos para a transmissão de dados. Apesar de barata, é uma conexão bem lenta e necessita do alinhamento dos dispositivos, o que cria uma certa dificuldade para locomoção. Encontra-se em controles remotos, PDAs ,etc.

Foi então desenvolvida a tecnologia conhecida como bluetooth. Esta, fornece uma maneira fácil de comunicação entre dispositivos e com a Internet. Trata-se de uma tecnologia que segue o padrão IEEE 802.15, via rádio frequência de 2.4 GHz – 2.48 GHz com alcance de 10m e com uma velocidade maior que o Infrared. Com bluetooth, o sinal se propaga em todas as direções, não necessitando de alinhamento e torna a locomoção mais fácil. Utilizada principalmente em celulares e PDAs.

Esta tecnologia já vem sendo difundida também para os automóveis. A exemplo disso, a Fiat, em parceria com a TIM e a Nokia, lançou um modelo do Stilo, o Stilo Connect, que vem equipado com a tecnologia bluetooth na qual é possível fazer ligações por meio de comando de voz e atender chamadas apertando um botão localizado no console central.

Sinais de rádio podem ser facilmente interceptados, por isso é importante que os dispositivos bluetooth disponíveis sejam seguros para prevenir mensagens de origem não autorizada, acesso a dados importantes ou que suas conversas sejam ouvidas sem autorização.

O padrão bluetooth possui mecanismos de segurança, que abrangem autenticação, autorização, criptografia e QoS (Quality of Service).

Autenticação e autorização: evita o recebimento de mensagens de origem duvidosa e acesso não desejado a dados e funções importantes.

Criptografia: evita escutas não autorizadas, mantendo assim a privacidade do canal. O fato do alcance de transmissão dos dispositivos bluetooth estar limitada a 10 m, ajuda na prevenção de escutas.

Outro mecanismo mais conhecido e mais básico da segurança de bluetooth é a habilidade do usuário escolher se um dispositivo está na modalidade de "discoverable" (visível a outros dispositivos) ou na modalidade "non-discoverable".

Quando um dispositivo de bluetooth está no modo visível, é muito fácil de fazer sua varredura e conseguir obter dados confidenciais.

Na teoria, permitir a modalidade oculta em um dispositivo de bluetooth deve proteger usuários das conexões desautorizadas, contudo na prática é ainda completamente possível encontrar estes dispositivos.

## **4.2 WLAN (*Wireless Local Area Network*)**

Tecnologia que permite a conexão entre dispositivos sem fio, com a rede ethernet corporativa e internet através da transmissão e recepção de ondas de rádio. É uma rede local sem fio padronizada pelo IEEE 802.11. É conhecida também pelo nome de Wi-Fi, abreviatura de wireless fidelity (fidelidade sem fios) e marca registrada pertencente a Wireless Ethernet Compatibility Alliance (WECA).

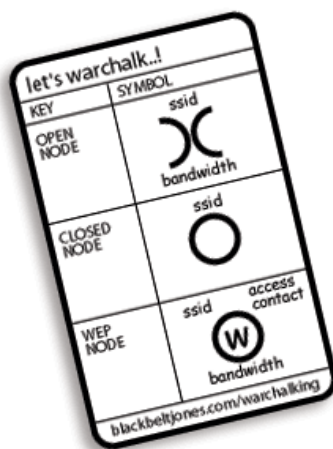
Estas redes sem fio são implementadas com dois tipos básicos de componentes. São eles, os adaptadores de redes, que são interfaces eletrônicas nos computadores dos clientes e os access points, que provêem os serviços às estações associadas. Os access points são dispositivos que fazem o gerenciamento da rede sem fio. Eles podem atuar ainda como uma ponte entre a rede sem fio e a rede guiada.

As modificações encontradas entre as redes ethernet e sem fio estão localizadas na camada física e na metade inferior da camada de enlace. Estas modificações são inseridas por causa da mudança do meio físico da rede e também para suportar a autenticação, associação e privacidade de estações.

O principal problema da ausência de um meio de transmissão ligado é a grande exposição a ataques, que comprometem a confidencialidade da comunicação. Com

software e hardware apropriados, é possível capturar facilmente logins, senhas, endereços de servidores e estações de usuários. Além do problema de confidencialidade, existe o risco de perda de integridade e autenticidade. Mensagens podem ser alteradas e reencaminhadas comprometendo as informações.

Para provar tamanha vulnerabilidade e chamar a atenção para a enorme falta de preocupações com a segurança em algumas redes sem fio, grupos saem à procura de redes sem fio abertas, passíveis de invasão. Para efetuar a prática são usados: um computador, uma placa ethernet configurada no modo "promísco" (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa), e um tipo de antena, (uma lata de batatas fritas "pringles" costuma ser utilizada para a construção das antenas). Quando há a detecção da existência de redes wireless símbolos usualmente feitos em giz são escritos em calçadas. Esta prática é conhecida como warchalking e tais símbolos são descritos na figura abaixo:



**Figura 13: Símbolos Warchalking**

- Open Node: significa que a rede é vulnerável;
- Closed Node: serve para uma rede fechada;
- A letra W dentro do círculo informa que a rede wireless utiliza o padrão de segurança WEP (Wireless Equivalent Privacy), com presença de criptografia;
- Em cima de cada símbolo, temos o SSID (Service Set Identifier), que funciona como uma senha para o login na rede, obtidos através de softwares próprios conhecidos como sniffers.

Como podemos perceber, redes sem fio podem ser facilmente acessadas por pessoas não autorizadas se não houver a preocupação e a procura de mecanismos de segurança adequados.

As soluções disponíveis no mercado utilizam em sua maioria o padrão WEP para garantia de sigilo das informações. O WEP (Wired Equivalent Privacy), utiliza a implementação do protocolo RC4 para realizar criptografia das ondas de rádio enquanto os dados são transmitidos de um ponto de extremidade a outro, procurando assegurar-se de que os pacotes não sejam modificados no trânsito.

Entretanto, sinais de falhas já foram encontrados. Como o WEP é usado nas duas camadas mais baixas do modelo de OSI (Open systems interconnection) - a ligação de dados e as camadas físicas; conseqüentemente não oferece a segurança end-to-end e é possível se ter acesso à chave utilizada na criptografia provocando o surgimento de diversas ferramentas para quebra do WEP.

Além do WEP, não se devem confiar nas demais características de segurança disponíveis em access points e interfaces de rede. Controle de acesso por endereços MAC (Medium Access Control) e comunidades SNMP (Simple Network Management Protocol) são alguns exemplos de funcionalidades que podem ser burladas.

Para se obter um nível de segurança satisfatório é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte, autorização e monitoração dos acessos da rede sem fio são imprescindíveis.

- Configuração dos Equipamentos: durante as configurações devem ser incluídas as características de segurança disponíveis nos equipamentos e podem também ser incluídas características de segurança personalizadas. Pois, mesmo não sendo confiáveis se utilizadas isoladamente, constituem mais uma barreira a ser vencida quando utilizada em conjunto com os demais itens;
- Criptografia: É fundamental o uso de criptografia confiável uma vez que não é possível contar apenas com o WEP. Durante esta etapa, uma implementação de uma VPN (Virtual Private Network) na rede sem fio pode ser realizada, utilizando recursos já existentes ou utilizando soluções de mercado;
- Autenticação e autorização: Autenticação é o processo pelo qual se verifica a identidade de um indivíduo. Em redes de computadores confidenciais e

públicas, a autenticação geralmente é baseada em um usuário e uma senha. Outros meios de se demonstrar a identidade também podem incluir métodos como um cartão, uma varredura da retina, um reconhecimento de voz ou impressões digitais. Em sistemas de segurança, a autenticação é distinto da autorização. A autenticação assegura que o indivíduo seja quem ele reivindica ser, mas não diz nada sobre seus direitos de acesso. O processo de conceder ou negar acesso a um recurso da rede baseado em sua identidade é a autorização. Em um primeiro estágio é feita a autenticação, que assegura um usuário ser quem ele reivindica ser; e o segundo estágio é a autorização, que define os acessos e privilégios desse usuário;

- **Monitoração dos acessos:** os Access points instalados e a rede propriamente dita devem ser monitorados. A monitoração é seguida do envio de alertas, previamente configurados em casos que se julgarem suspeitos.

### **4.3 WMAN (Wireless Metropolitan Area Network)**

Muito semelhante às redes WLAN, difere-se por abranger um alcance territorial maior e destaca-se por suas altas taxas de transmissão. Com para criar uma rede de área metropolitana é preciso ter um alcance de cobertura de algumas dezenas de Kms o raio de cobertura dos pontos sem fio, conhecidos como hotspots, foram ampliados.

A recente tecnologia WiMax (Worldwide Interoperability for Microwave Access) encontra-se nesse conceito de redes metropolitanas. O WiMax é capaz de comportar milhares de usuários por setor e de cobrir áreas de até 50 quilômetros. A tecnologia usa o padrão IEEE 802.16e e possibilita taxas de transferência de até 70Mbps.

O WiMax é a tecnologia mais indicada para ambientes urbanos. Porém isso traz algumas dificuldades para uma rede sem fio. Por exemplo, o sinal refletido em edifícios deve ser o suficiente para que o receptor recupere o sinal transmitido. Mesmo assim, os custos de infra-estrutura e implantação do WiMax são menores do que os da tecnologia celular e irá facilitar o desenvolvimento de uma série de aplicações de Wireless Broadband.

Características de privacidade e criptografia estão previstos no padrão 802.16, permitindo transmissões seguras incluindo os procedimentos de autenticação. Porém outras práticas de seguranças devem ser aplicadas. Opções são a criptografia de dados utilizando DES (Data Encryption Standard), protocolo podendo transportar tanto IPv4 quanto IPv6 e utilizar QoS.

#### **4.4 WWAN (*Wireless Wide Area Network*)**

As redes WWAN permitem aos usuários estabelecerem conexões sem fio com redes remotas privadas ou públicas a qualquer momento e em qualquer lugar com cobertura celular. A proposta desta tecnologia agrega valores mais abrangentes que os sistemas Wi-Fi ou Bluetooth, pois oferecem serviços em uma área de cobertura de proporções bem maiores de acesso à Internet, Intranet e serviços diferenciados relacionados aos terminais móveis e sua mobilidade.

Inicialmente esta tecnologia foi desenvolvida para suportar comunicação de voz. Mas a convergência da mídia e de dados gerou o desenvolvimento de adaptações para suportar esses novos serviços. Assim, as redes de celulares estão caminhando rapidamente para tornarem-se a maior aplicação de WWAN. Com o crescente uso de conexões de banda larga, celulares estão transmitindo e-mails, textos, imagens, som e vídeo. Trata-se de um fluxo de informações em tempo real entre o dispositivo onde ocorre a atividade e o sistema host remoto.

Essa tecnologia é dividida nos seguintes tipos:

- 1G (primeira geração) – apenas voz. AMPS (Advanced Mobile Phone Services) – Analógico;
- 2G (segunda geração) – circuito compartilhado entre voz e dados, velocidades de até 14,4 Kbps. CDPD (Cellular Digital Packet Data) – Digital, GSM (originalmente Groupe Speciale Mobile, mas depois mudou para o inglês Global System for Mobile Communications), TDMA (Time Division Multiple Access) e CDMA (Code Divison Multiple Access).
- 2.5G – HSCSD (High Speed Circuit Switched Data), trouxe melhorias na comunicação de dados nas redes 2G, que passaram a ter velocidades superiores (144 Kbps), GPRS (General Packet Radio Service – para

transmissão de dados utilizando os canais e frequências GSM para localização e rastreamento) e CDMA2000 (1xRTT);

- 3G (terceira geração) – sistema re-desenvolvido para aumentar a capacidade, velocidade (2 Mbps) e eficiência para ambos, voz e dados. EDGE (Enhanced Data rates for Global Evolution) / WCDMA (Wideband CDMA) e CDMA 1xEV-DO/1xEV-DV (Podem aumentar em 3 vezes a taxa de transmissão pela utilização de um novo esquema de modulação);
- 4G (quarta geração) – ainda em desenvolvimento, visa o aumento da qualidade e velocidade (planejadas para atingir de 20 Mbps a 100 Mbps), exigência devido ao aumento do uso de imagens e sons. Aplicações tais como: videoconferências e serviços multimídia.

A idéia de ter acesso às informações podendo estar em qualquer lugar e apenas usando dispositivos portáteis por meio de comunicação sem fio, tornou-se muito atrativa e indispensável nessa nova era da informação. Porém, esse acesso não pode se tornar crítico e tem que oferecer garantia de segurança proporcionando integridade e confiabilidade.

Três modelos oferecem segurança avançada e que procuram garantir aos usuários proteção do conteúdo crítico armazenado e de sua transferência pelas conexões sem fio. São os softwares VPN (Virtual Private Network), WEP (Wired Equivalent Privacy) e LEAP (Lightweight Extensible Authentication Protocol).

Além destas técnicas existe também o Spread Spectrum, uma técnica de rádio frequência desenvolvida pelo exército americano e utilizada em sistemas de comunicação de missão crítica, garantindo segurança e rentabilidade. O Spread Spectrum é o mais utilizado atualmente. Utiliza a técnica de espalhamento espectral com sinais de rádio frequência de banda larga, foi desenvolvida para dar segurança, integridade e confiabilidade.

As utilizações destas técnicas e não se esquecendo é claro das outras práticas já citadas anteriormente, como configuração adequada, criptografia, autenticação, autorização e monitoração dos acessos da rede sem fio, são essenciais para a segurança das redes e a garantia da confidencialidade, integridade, autenticidade e disponibilidade da comunicação.

## CONCLUSÃO

Os recursos e investimentos em segurança estão, obviamente, relacionados à importância da informação e ao risco que a mesma está exposta. O processo é semelhante ao da própria defesa do patrimônio físico, com o agravante que a recuperação da informação pode ser muito mais onerosa do que do equipamento físico e que na maioria dos casos sua mensuração é extremamente difícil.

No caso de rede de computadores a vulnerabilidade fica aumentada devido à fragilidade apresentada por cada nó da rede. As informações estratégicas podem estar em qualquer lugar a todo instante.

Em função destes relatos podemos assumir que mais importante que escolhermos produtos e ferramentas que prometem níveis de segurança “X” ou “Y” é termos políticas aplicáveis a todos ambientes operacionais multiplataformas e que estes mesmos ambientes nos permitam ter programas segmentados que auxiliem na aplicação e fácil operacionalização destas políticas.

Compete então ao administrador de rede combinar múltiplas tecnologias para prover segurança em profundidade.

## BIBLIOGRAFIA

- NORTEL NETWORKS, *Virtual Private Networks (VPNs)*, Tutorial, IEC Webproforum Tutorials: <http://www.webproforum.com> , Internet.
- PSINET, *Intranets and Virtual Private Networks (VPNs)*, Tutorial, IEC Webproforum Tutorials: <http://www.webproforum.com/> , Internet
- CISCO SYSTEMS, *PACKET - Cisco Systems Users Magazine*, Vol.12, N°1, Primeiro Trimestre/2000
- CISCO SYSTEMS, *Overview of Access VPNs and Tunneling Technologies*, <http://www.cisco.com/> , Internet.
- CISCO SYSTEMS, *Layer Two Tunnel Protocol*, <http://www.cisco.com> , Internet.
- ASCEND COMMUNICATIONS, *Virtual Private Networks Resource Guide*, Arquivo PDF: <http://www.lucent.com/ins/library/pdf/techdocs/vpnrg.pdf> , Internet.
- MICROSOFT CORPORATION, *Understanding Point-to-Point Tunneling Protocol (PPTP)*, Janeiro de 1997, [http://msdn.microsoft.com/library/backgrnd/html/understanding\\_pptp.htm](http://msdn.microsoft.com/library/backgrnd/html/understanding_pptp.htm) , Internet.
- CHIN, Liou Kuo; *Rede Privada Virtual - VPN*, RNP – NewsGeneration , 13 de novembro de 1998, volume 2, número 8: <http://www.rnp.br/newsgen/9811/vpn.shtml> , Internet.
- VALENCIA, Andy; LITTLEWOOD, Morgan; e KOLAR, Tim; *Cisco Layer Two Forwarding (Protocol) - L2F*, RFC 2341, Maio de 1998, <http://www.ietf.org/rfc/rfc2341.txt> , Internet.
- CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. *Firewalls and Internet Security – Reppelin the Wily Hacker*. 2<sup>nd</sup> Ed.
- MILLER, S. S. *Wi-Fi Security – Enhance security and maintain privacy of mission-critical data, even when going wireless*. 2<sup>nd</sup> Ed.

### Sites Consultados:

- <http://apostilando.com>
- [http://carroonline.terra.com.br/serverpage\\_new/?tipo=1&cod=2&info=8103](http://carroonline.terra.com.br/serverpage_new/?tipo=1&cod=2&info=8103)
- [http://csrc.nist.gov/publications/nistpubs/800-48/NIST\\_SP\\_800-48.pdf](http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf)
- <http://httpd.apache.org/docs/howto/auth.html>
- <http://wimax.com>
- <http://www.bluetooth.com>
- <http://www.dlnet.vt.edu/Search.jsp?Keyword=network+security&Offset=0&DLselect1=DLNET>
- <http://www.iec.org/online/tutorials/index.html>

- <http://www.las.ic.unicamp.br/~edmar/>
- <http://www.nokia.com.br/nokia/0,8764,64378,00.html>
- [http://www.portaldaautomacao.com.br/artigo\\_014.asp](http://www.portaldaautomacao.com.br/artigo_014.asp)
- <http://www.protocols.com/hot.htm>
- <http://www.securityfocus.com/infocus/1830>
- <http://www.teleco.com.br>
- [http://www.telepac.pt/suporte/wifi/acesso\\_wifi.html](http://www.telepac.pt/suporte/wifi/acesso_wifi.html)
- <http://www.timbrasil.com.br/portaltim/homebusiness/0,1618,2400019032001105,00.html>
- [www.cbpf.br/cat/download/seminarios/XSIC/Bruno.pdf](http://www.cbpf.br/cat/download/seminarios/XSIC/Bruno.pdf)
- [www.cin.ufpe.br/~lrcs/arquivos/Apresentacao%20Final.ppt](http://www.cin.ufpe.br/~lrcs/arquivos/Apresentacao%20Final.ppt)
- [www.warchalking.org](http://www.warchalking.org)

**Cursos eletrônicos:**

- Motorola University

- Bluetooth Technology and Applications
- Evolution of GSM - (Security in Wireless Networks)

- Manpower Global Learning Center

- Designing Cisco Enterprise Wireless Networks,  
<http://www.manpowerglc.com/manpowernet/techtrack.nsf/0/9CAD4081207DCABA86256E660060BED1?OpenDocument>