Unidade IV

4 O VPN E O RDSI

4.1 Gerenciamento de chaves

Para manter um gerenciamento das chaves é preciso realizar uma configuração prévia das chaves que serão tornadas secretas, no formato de redes virtuais privadas que não necessitam de automatização por *software* ou de grandes investimentos e nem de infraestrutura para mantê-las, porém as redes de grande porte podem se beneficiar desse tipo de implementação caso uma infraestrutura de chaves públicas PKI (*public key infrastructure*) seja usada para criar distribuir e emitir certificados digitais especificamente para cada usuário do sistema.

Os certificados digitais compreendem um conjunto de procedimentos que verificam a associação entre uma chave pública e a identidade de um determinado usuário do sistema, promovendo assim a incapacidade de falsificação de identidade de usuário. Podemos utilizar os serviços de autoridades certificadoras reconhecidas legalmente na internet, como serviços fornecidos por terceiros, ou ainda usar uma própria chave construída internamente. A grande vantagem de utilizar serviços de terceiros se dá justamente pela importância de grandes companhias em identificar e qualificar a quantidade de chaves por elas emitidas, o que serve tanto aos seus usuários quanto aos seus parceiros e clientes.

4.2 Autenticação

Quando falamos de mecanismos de autenticação, entendemos que o destinatário de um dado pode determinar se o emissor é realmente quem ele disse, baseando-se na autenticação do usuário ou do dispositivo ou apenas em se o dado foi redirecionado e corrompido ao longo do caminho por onde ele passou.

4.2.1 Autenticação de usuários ou dispositivos

Quando possuímos uma comunicação entre as entidades A e B, e ainda se A recebe uma mensagem assinada pela entidade B, a entidade A, então, escolhe o número aleatório e o encripta utilizando uma chave que somente a entidade B consiga responder – logo, esta será capaz de decodificar a informação. A entidade B ainda tem a capacidade de decriptar o número aleatório originado na mensagem e o reencripta aplicando uma chave que somente a entidade A seja capaz de decodificar. Quando a entidade A receber esse número de volta ela terá absoluta certeza de que a entidade B realmente está do outro lado da conexão.

4.2.2 Autenticação de dados

A fim de verificar se os pacotes de dados chegam com sua integridade assegurada e inalterada, os sistemas de rede virtual privada usualmente utilizam uma técnica que envolve funções de cabeçalho. Essa função cria um tipo de impressão digital ao dado original. Existe um cálculo de um número único para a mensagem em questão chamado de cabeçalho *hash*, construído por uma cadeia fixa ou variável de *bits*. O sistema emissor, então, acrescenta esse número ao pacote de dados antes do processo de encriptação. Assim que o destinatário recebe a mensagem, ele a decripta, e ainda pode calcular o cabeçalho *hash* da mensagem recebida de uma maneira independente. Para finalizar, o resultado é comparado com o valor anexado pelo mecanismo emissor e, obviamente, se os dois estiverem iguais, é entendido que os dados não foram alterados no caminho.

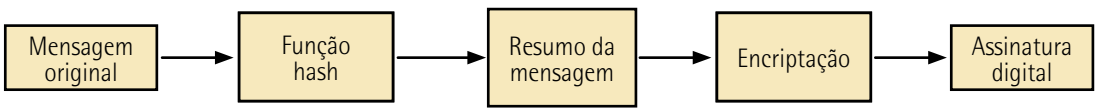

Figura 44 – Fases da aplicação da assinatura digital

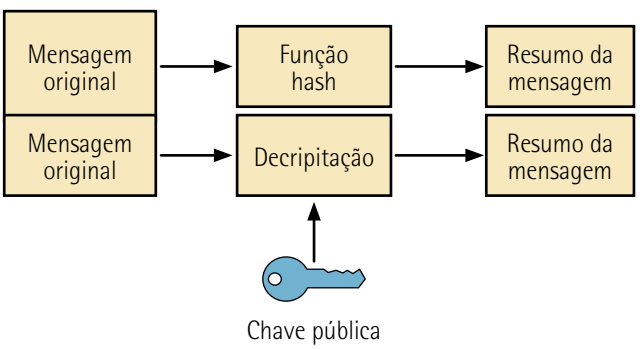

Figura 45 – Mecanismo de conferência da assinatura digital

4.3 Protocolos de tunelamento e encriptação

Inúmeros protocolos de encriptação são empregados para a construção de túneis de redes virtuais privadas na internet, porém o único protocolo que é reconhecido como padrão para a internet se chama IPsec. Ele foi projetado principalmente para proteger o tráfego da rede, observando os seguintes aspectos da informação por ele transportada: controle de acesso, integridade da conexão, autenticação da origem dos dados, proteção contra o reenvio de pacotes e privacidade no tráfego das informações.

Esse protocolo permite principalmente dois modos de operação: quando atribuímos o modo túnel, toda informação que estiver após o cabeçalho IP será protegida, ou ainda, além do modo túnel, todo e qualquer pacote enviado para o lado oposto será protegido, e um novo cabeçalho para cada pacote será gerado a partir de então.

Além do IPsec, observamos também o protocolo L2TP (*layer two transfer protocol*), também utilizado para construção de túneis de redes virtuais privadas. Porém, diferentemente do IPsec, todo e qualquer protocolo diferente do protocolo IP – por exemplo, IPX e SNA – será encapsulado em um datagrama

L2TP, ainda assim, com a prerrogativa clara de promover a segurança e a garantia dos dados através de um meio promíscuo (meio físico que não sofre controle por nenhuma entidade).

4.4 Políticas de segurança

A aplicação de políticas de segurança define os livros de privilégio e de acesso às informações que sejam aceitáveis, os quais ainda podem depender de diversos fatores, da posição hierárquica da empresa, dos projetos atuais em que o funcionário está trabalhando e da necessidade de informações ao nível de confiança. Essas políticas devem ainda ser suficientemente granulares a fim de permitir a diferenciação de seu propósito dentro da organização, ao nível de servidores e grupos de usuários até o nível de usuário. Também precisamos levar em consideração que estaremos traçando uma linha divisória entre o acesso limitado e os processos colaborativos dentro da corporação, ainda que as políticas tenham a obrigação de proteger os recursos de maior nível, desde que isso não prejudique a produtividade dos empregados da empresa.

Lembrete

As VPNs podem ser caracterizadas como um acesso remoto (conectando um computador a uma rede) ou rede a rede (conectando duas redes). Em uma configuração corporativa, as VPNs de acesso remoto permitem que os funcionários acessem a intranet de sua empresa a partir de casa ou enquanto viajam para fora do escritório. As VPNs do tipo rede a rede permitem ainda que os funcionários em escritórios geograficamente distantes compartilhem uma rede virtual consolidada. Uma VPN também pode ser usada para interconectar duas redes semelhantes em uma rede intermediária diferente – por exemplo, duas redes IPv6 em uma rede IPv4.

4.5 Aplicações VPN

4.5.1 Acesso remoto

Profissionais que viajam frequentemente ou que trabalham em casa utilizam VPN para acessar a rede interna da empresa e realizar suas tarefas. Não importa onde estejam, o acesso seguro à empresa está a apenas uma ligação telefônica para um ISP. Essa solução também é útil para os casos em que importantes funcionários da empresa precisam estar longe por um bom período de tempo.

4.5.2 Acesso remoto antes das VPNs

Em tempos passados, as conexões comutadas, como linhas discadas, eram a única opção disponível para realizar conexões entre os usuários e os seus pequenos escritórios, porém o advento da internet e as conexões virtuais privadas permitiram uma conectividade segura e assertiva para esse grupo de usuários.

É sabido que as tarifas de conexão de longa distância são as maiores responsáveis pelo crescente custo das operações de conectividade, associadas a outros custos, como investimento em servidores de acesso remoto e mecanismos de autenticação segura, que podem certamente alavancar o custo operacional das companhias.

4.5.3 Acesso remoto após as VPNs

Com esse novo paradigma, os usuários de redes remotas podem agora estabelecer conectividade segura com suas companhias através da internet. A vasta disponibilidade de conexões para a internet, como DSL ou conexão a cabo, permite que os usuários possam acessar seus recursos corporativos com velocidades superiores e segurança aplicada. Na maioria das vezes, a percepção é como se o funcionário estivesse sentado em sua mesa no escritório enquanto, na verdade, executa suas tarefas a uma longa distância.

Para essas aplicações, existem grandes benefícios associados às redes virtuais privadas. O principal fato de substituir as ligações de longa distância e os serviços 0800 – eliminando, sobretudo, a necessidade de servidores de acesso remoto e de *modems* de conexão e banindo substancialmente as linhas de escadas de acesso direto – permite que aplicativos e operações de transferência de arquivos possam ser executadas nativamente. A grande preocupação com as questões relativas à segurança e a permissões de acesso é que diversos estudos conduzidos demonstram que a economia gerada pelas ligações de longa distância paga, muitas vezes, os custos operacionais das redes virtuais privadas para as corporações, reduzindo substancialmente as despesas operacionais para esses fins.

4.5.4 Intranet

A globalização e o avanço dos pequenos negócios no plano comercial promovem, para o mercado de hoje, certas exigências quanto ao estabelecimento de escritórios de representação regional e internacional. As redes virtuais privadas vêm de encontro a esse novo momento permitindo uma infraestrutura fluída.

4.6 Intranet antes das VPNs

As necessidades de conectividade entre escritórios e sedes das companhias é o primeiro passo para o estabelecimento de sistemas de roteamento e de *backbone* entre LANs e WANs. Os roteadores de acesso remoto possuíam capacidades de conectividade com outras localidades remotas, porém esses roteadores eram frequentemente conectados a uma rede com linhas privadas ou ainda a serviço *frame relay*.

O custo operacional desse serviço, associado aos custos de configuração do sindicato escritório, gerava tarifas de serviços de telecomunicação com custo significante devido a essas soluções de longa distância.

4.7 Intranet após as VPNs

Com aplicação das redes virtuais privadas, os *backbones* WAN, juntamente com *hardware* associado, são sistematicamente substituídos por soluções de internet. Cada novo escritório de uma corporação simplesmente associa o custo de conexão à internet do tipo DSL, à rede digital de serviços integrados e ainda à conexão a cabo, promovendo, sobretudo, a eliminação de necessidade dos roteadores de *backbone* e de todo o *software* e *hardware* necessário a administração, configuração e suporte. O retorno de investimento para essas aplicações promove também uma rápida absorção do retorno de investimento delas.

4.8 Produtos VPN

É necessário repassar as responsabilidades a um ISP. Nas questões observadas relativas à implementação das redes virtuais privadas e ao repasse das responsabilidades do gerenciamento a um provedor de soluções de internet, é observado que para as empresas que não possuem profissionais qualificados para as tarefas de estabelecimento de conexões seguras, a presença de um provedor de soluções de internet é necessária, bem como todo o aporte de *hardware* e *software* para a conclusão dessas tarefas.

4.9 Assumindo a responsabilidade na própria companhia

Ao implementar uma solução de redes virtuais privadas, devemos prever a existência de quatro áreas que devem ser levadas em consideração: o serviço de internet, o servidor com as políticas de segurança implementadas, o sistema PKI e o sistema de estabelecimento das redes virtuais privadas.

Esses dispositivos podem ser divididos em duas categorias: os independentes e os integrados.

Esses dispositivos são:

- O roteador: que adicionado ao suporte e às redes virtuais privadas diretamente pode associar os cursos de atualização e mantê-los em baixa. Suas funcionalidades podem ser adicionadas tanto por *software* de gerenciamento como por razões de expansão.

- O *firewall*: a sua utilização para criação de redes virtuais privadas é uma das mais aplicadas em redes de pequeno e médio portes que não possuem um volume de tráfego expressivo; porém, devido ao tipo de processamento realizado pelos equipamentos *firewall*, eles podem não ter uma representatividade relacionada à *performance*, se comparado a altos volumes de tráfego.

Os dispositivos independentes são projetados especificamente para construção de túneis, encriptação de pacotes e autenticação de usuários. Usualmente, são de simples instalação e manutenção, se comparados às implementações realizadas em roteadores e firewalls. Possuem ainda uma extensa variedade de dispositivos com diferentes capacidades de utilização e gerenciamento para conexões simultâneas.

Os *softwares* para criação e gerenciamento de túneis para redes virtuais privadas encontram-se disponíveis para serem aplicados entre os pares de dispositivos que utilizam esse tipo de serviço remoto ou ainda diretamente a dispositivos de VPN. Por serem soluções de baixo custo operacional e de implementação simples, possuem algumas desvantagens relacionadas ao volume de tráfego existente para as conexões remotas.

4.10 Qualidade de serviço (QoS)

Como sabemos, a internet é um ambiente altamente complexo, com uma grande mistura de dados e aplicações que são executadas em tempo real, que tem características de mobilidade para diferentes direções através de sua infraestrutura, a qual não conhecemos. Logo, a internet é um imenso desconhecido, em que encontramos gargalos e muitas condições de congestionamento. A implementação da qualidade de serviço, nessas condições, geralmente é aplicada à alocação de banda e à prioridade de pacotes.

No momento em que transmitimos informações, aquelas de missão crítica que devem chegar ao destinatário com o menor atraso possível, a aplicação da qualidade de serviço se torna imprescindível e acaba absorvendo uma parte importante das implementações das redes virtuais permanentes. Com o advento do protocolo internet versão 6 ipv6, que será a versão dominante do protocolo IP nos próximos anos, os aspectos da qualidade de serviço irão mudar de uma forma radical. Esse é o principal motivo de separar os motivos e os requisitos da qualidade de serviços em detrimento das redes virtuais permanentes, sempre observando, do ponto de vista da corporação, a avaliação da qualidade de serviço. Portanto, devemos escolher um provedor de serviço de internet que ofereça um nível de qualidade aceitável, e então escolher a melhor solução de redes virtuais privadas para aplicação.

4.11 L2TP (*layer 2 tunneling protocol*)

4.11.1 Protocolo para tunelamento na camada de enlace

O L2TP é uma das extensões do protocolo de conectividade ponto a ponto, absorvendo características de outros dois protocolos proprietários do modelo L2F (*layer 2 forwarding*), proveniente da Cisco, e do PPTP (*point-to-point tunneling protocol*), proveniente da Microsoft, por ser um padrão IETF (*internet engineering task force*), que conta com a participação da Cisco e da Microsoft em seu fórum, associado a outros líderes de mercado no segmento.

A versão 3 do L2TP é uma atualização da RFC 2661, que foi originalmente definida como um método para tunelamento de quadros ponto a ponto através de uma rede de comutação de pacotes. Apareceu, então, a necessidade de implementar o método para que ele incluísse todos os modelos de encapsulamento da camada 2 do modelo OSI que ainda necessitassem de tunelamento através das redes de comutação por pacotes. Observando essas mudanças para a versão 3, temos a retirada de todas as partes específicas do protocolo ponto a ponto e do cabeçalho L2TP originais, garantindo, assim, um formato genérico para outras aplicações e incluindo a mudança para um formato que possibilite o desencapsulamento de forma mais rápida.

O L2TP fornece a flexibilidade e a escalabilidade do IP com a privacidade do *frame relay* ou ATM, o que permite que o serviço de rede seja roteado através de redes IP. As tomadas de decisões nas terminações dos túneis ou nas redes virtuais privadas são colocadas sem nenhuma necessidade de processamento entre os nós intermediários.

Algumas das vantagens que são oferecidas pelo L2TP são: permitir o transporte de protocolos que não sejam origem IP, a exemplo do IPX e SNA; permitir outros protocolos dos terminais; e ter um mecanismo simples e tunelamento para implementação das funcionalidades para redes locais e protocolo IP de forma transparente, possibilitando também os serviços de redes virtuais privadas no formato IP nativo de forma simplificada, o que caracteriza a integração das redes cliente e provedor de serviços, sempre observando as facilidades de configuração por ambos os lados cliente-servidor.

4.11.2 Funcionamento

Sempre que os roteadores internos de uma rede IP tratam o volume de tráfego com qualquer outro segmento e estes não precisam das informações sobre as redes remotas, esse processo é chamado de tunelamento na camada 2.

Observe o exemplo a seguir, em que o roteador 1 e o roteador 2 fornecem um serviço L2TP. Esses roteadores se comunicam por um protocolo IP nativo através do caminho composto pelas interfaces internas 2 e a rede IP da interface interna 3. Os roteadores 3 e roteadores 4 comunicam-se por interfaces POS Sonet, que utilizam um túnel L2TP. A configuração do túnel TU1 é estabelecida entre as interfaces interna 1 do roteador 1 interfaces 4 do roteador 2. Qualquer pacote que chegue pela interface interna do roteador 1 é encapsulado automaticamente pelo túnel L2TP e, então, enviado pelo Tu1 diretamente para o roteador 2. Já o roteador 2 desencapsula o pacote e o transmite para a interface interna 4 do roteador 4.

Na operação do túnel L2TP, todos os pacotes recebidos pela interface 1 serão redirecionados para o roteador 4. O roteador 3 e o roteador 4 não vêem a rede que está entre eles. Do mesmo método utilizado para as interfaces ethernet, qualquer pacote recebido pela rede local 1 através do roteador 1 e na interface E1 será encapsulado automaticamente pelo L2TP e enviado pelo Tu2 até a interface E2 do roteador 2, o qual será transmitido pela rede local dois.

A mesma variação vale para o *frame relay*, em que qualquer pacote recebido pela rede local 1 através do roteador 1 operando uma subinterface será encapsulada pelo túnel L2TP e enviado até subir a interface do roteador 2, que subsequentemente será transmitido para a rede local 2.

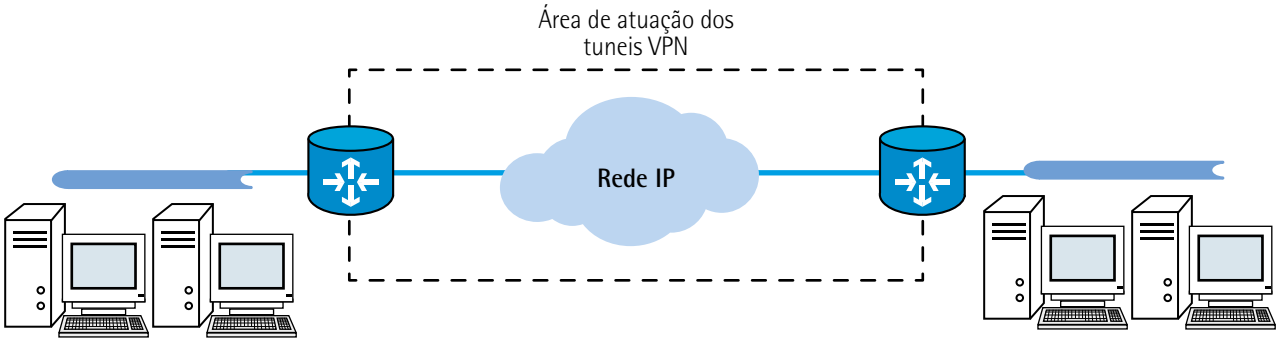

Figura 46 – Atuação da construção de tuneis VPN em uma rede IP

4.12 Cabeçalhos L2TP

Assim que as informações de um canal ingressam por uma interface de entrada de um túnel L2TP, elas são encapsuladas por um cabeçalho adicional L2TP, como mostrado na figura apresentada. O cabeçalho L2TP é composto pelos seguintes parâmetros:

- Cabeçalho para entrega (*delivery header*): necessário para transmitir os pacotes L2TP através da rede. Esse é um cabeçalho IPv4, com 20 octetos.

- Cabeçalho L2TP: contém as informações necessárias para identificar de maneira única um túnel no local em que ele será desencapsulado, e contém 12 octetos.

- Informações (*payload*): o que será transportado pelo L2TP, podendo ser tanto um quadro da camada de enlace quanto um pacote da camada de rede. A parte do L2TP pode ser decomposta nos seguintes campos:

  – Identificador do túnel: identifica o túnel no sistema que desencapsula o pacote. O valor da identificação do túnel é escolhido de forma a otimizar a identificação do sistema que o desencapsulará. Esse sistema pode então escolher trabalhar com um número menor de *bits* nesse campo; trabalhando com 10 *bits*, por exemplo, serão possíveis 1.023 túneis, já que o identificador zero é reservado para uso pelo protocolo.

  – *Cookie*: uma assinatura contendo oito octetos, que é compartilhada entre as duas extremidades do túnel L2TP. O *cookie* reduz as chances de que dois tráfegos sejam misturados após o desencapsulamento devido a erros de configuração; as assinaturas nos roteadores de origem e destino devem coincidir ou os dados serão descartados.

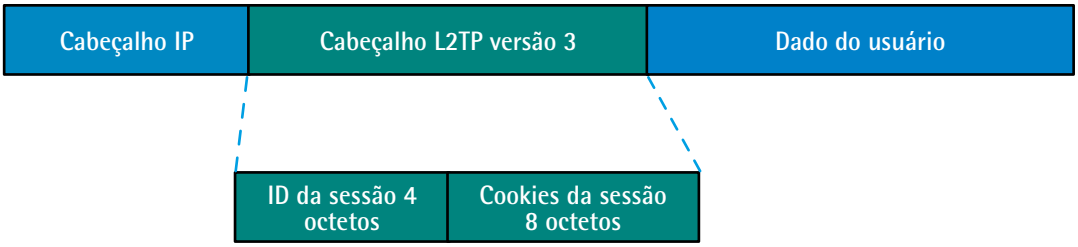

Figura 47 – Detalhamento do encapsulamento L2TP

A sinalização do L2TP é responsável por negociar os parâmetros da parte de controle, identificadores de sessão, *cookies*, autenticação e troca de parâmetros de configuração.

4.12.1 Ordenação dos quadros

De acordo com ordem de ingresso dos quadros da camada 2, eles passam a ser garantidos por qualquer tecnologia dessa camada (pela natureza do enlace, com uma linha serial) ou pelo próprio protocolo. Os quadros podem ser perdidos, duplicados ou reordenados enquanto passam como pacotes da rede IP. Se o protocolo da camada 2 não fornece um mecanismo de reordenamento de maneira explícita, o L2TP pode ser configurado para ordenar seus pacotes de acordo com um mecanismo descrito na RFC.

4.12.2 IPSec (protocolo de segurança IP)

O protocolo de segurança IP (IP *security protocol*, mais conhecido pela sua sigla IPSec) visa ser o método padrão para o fornecimento de privacidade, integridade e autenticidade das informações transferidas através de redes IP.

A internet atua com os avanços de como os novos negócios são feitos, mas até mesmo o rápido crescimento da internet tem sido atingido pela inerente falta de segurança. Algumas das principais ameaças a que ela está sujeita são:

- Perda de privacidade na troca de dados: os dados podem ser vistos por terceiros.
- Perda da integridade dos dados: em algum local no caminho entre a origem e o destino, os dados podem ser modificados por terceiros.
- Falsificação de identidade: a origem dos dados pode ser forjada, fazendo com que pessoas assumam o papel de outras.
- Ataques de negação de serviço (DoS – *denial of service*): muitas vezes, feitos através da união de diversas máquinas, que fazem requisições excessivas de um determinado serviço, tornando-o indisponível aos outros usuários.

O IPSec abrange o tratamento dessas ameaças na própria camada de rede (camada internet do modelo TCP/IP), principalmente para que não sejam necessárias modificações nos terminais (*hosts*) ou

aplicativos. Um dos meios para se conseguir isso é através da implementação de IPSec nos roteadores de borda, por onde passa todo o tráfego externo de uma empresa/instituição. Dessa forma, a segurança atuaria de forma transparente para o usuário.

O IPSec é orientado para a encriptação de camada IP e seu padrão define alguns formatos de pacote novos:

- A autenticação de cabeçalho (AH – *authentication header*) para fornecer a integridade dos pacotes entre origem e destino, e o encapsulamento seguro da informação (ESP – *encapsulating security payload*).

- O gerenciamento de chaves, as associações de segurança (SA – *security associations*) e os parâmetros para a comunicação IPSec entre dois dispositivos são negociados através do IKE (*internet key exchange*, anteriormente chamado de *internet security association key management protocol* ou ISAKMP/Oakley).

O IKE emprega as cadeias de certificados digitais (que garantem a identidade de uma pessoa, evitando a falsificação de identidades) para autenticação de dispositivos, permitindo a criação de grandes redes seguras. Sem o suporte dos certificados digitais, as soluções IPSec não seriam escaláveis para a internet.

Atualmente, o protocolo já é encontrado em roteadores, em *firewalls* e em sistemas operacionais Windows e UNIX.

4.12.3 Fundamentos das redes seguras

Uma rede, para ser considerada segura, deve se basear numa forte política de segurança, que defina a liberdade de acesso à informação para cada usuário, assim como a localização dos mecanismos de segurança na rede. Há várias soluções para se construir uma infraestrutura segura para a internet, a extranet, a intranet e as redes para acesso remoto, que oferecem autenticação do usuário, acompanhamento de suas ações e privacidade dos dados.

Privacidade, integridade e autenticidade são conseguidas através de encriptação na camada de rede, certificação digital e autenticação de dispositivos. São palavras-chave quando falamos de IPSec ou de mecanismos de segurança em redes públicas.

4.12.4 Mudança na comunicação das empresas

A internet está modificando rapidamente a forma como são feitos os negócios. Ao mesmo tempo em que a velocidade de comunicação aumenta, seu custo diminui. Há um grande espaço para o aumento de produtividade através das seguintes topologias:

- Extranet: as companhias podem facilmente estabelecer enlaces com seus fornecedores, clientes ou parceiros. Até pouco tempo atrás, isso era feito através de linhas privadas (dedicadas) ou de ligações telefônicas (de baixa velocidade). A internet permite uma comunicação instantânea, de alta velocidade e sempre disponível.

- Intranet: a maior parte das empresas utiliza WANs (*wide-area networks*) para conectar as redes de sua sede e filiais. Essa solução é cara, apesar de seu custo ter caído nos últimos anos.

- Usuários remotos: a internet fornece uma alternativa de baixo custo para a conexão desses usuários às redes corporativas. Em vez de a empresa ter que manter bancos de *modems* e arcar com os custos das ligações telefônicas (muitas vezes, interurbanas ou até internacionais), elas podem permitir que seus usuários acessem sua rede através da internet.

Com uma ligação local a um provedor de acesso à internet (ISP – *internet service provider*), um usuário pode ter acesso à rede corporativa. Essas e outras aplicações da internet estão mudando a forma como as empresas se comunicam. A internet fornece uma infraestrutura pública de comunicações que faz com que tudo isso se torne possível. No entanto, há fraquezas geradas por essa infraestrutura compartilhada: segurança, qualidade de serviço e confiabilidade. Nesse momento aparece o IPSec como peça-chave no fornecimento de segurança nas comunicações de rede.

4.13 Qual a função real do IPSec?

Sabemos que a internet apresenta grandes vantagens, mas também alguns riscos. Sem os mecanismos adequados de controle, os dados estão sujeitos a diversos tipos de ataques.

Estes ataques são:

Perda de privacidade

O atacante pode observar dados confidenciais enquanto eles atravessam a internet. Essa é uma das principais ameaças ao comércio pela internet hoje. Sem encriptação, todas as mensagens enviadas podem ser lidas por pessoas não autorizadas. Essas técnicas são chamadas de *sniffing*, e os programas utilizados para isso, de *sniffers*. Até usuários com pouco conhecimento já são capazes de bisbilhotar o conteúdo que trafega na rede.

Perda de integridade dos dados

Mesmo que os dados não sejam confidenciais, também devemos nos preocupar com a integridade deles. Por exemplo, uma pessoa pode não se importar que alguém veja suas mensagens do dia a dia, mas certamente se preocupará se os dados puderem ser alterados. Uma ordem para a promoção de um funcionário, geralmente, não precisa ser secreta, mas quem a enviou pode ficar realmente preocupado se ela puder ser trocada por outra indicando uma demissão. O mesmo vale para mensagens secretas, já que o emissor deseja que seus *bits* não sejam alterados no caminho, o que poderia causar uma alteração no significado dela. Mecanismos de integridade dos dados garantem que a mensagem chegue ao destino como saiu da origem.

Falsificação de identidade (*identity spoofing*)

Além da proteção do dado, também devemos ter a garantia de que uma pessoa é realmente quem ela diz ser. Um atacante pode tentar se passar por outra pessoa, para ter acesso a informações confidenciais. Muitos sistemas ainda confiam no endereço IP para identificar um usuário de forma única; no entanto, esse sistema já é facilmente enganado.

Negação de serviço (DoS)

Ao migrar para a internet, uma organização deve tomar as medidas necessárias para garantir que seus sistemas estarão disponíveis aos usuários. Aproveitando brechas de segurança, atacantes fazem com que computadores da empresa sejam levados ao limite, até o ponto em que parem de oferecer o serviço que deveriam. Mesmo que o atacante não consiga acesso a informações privilegiadas, ele sem dúvida causará danos à empresa.

A figura a seguir mostra onde a encriptação atua nas diferentes camadas.

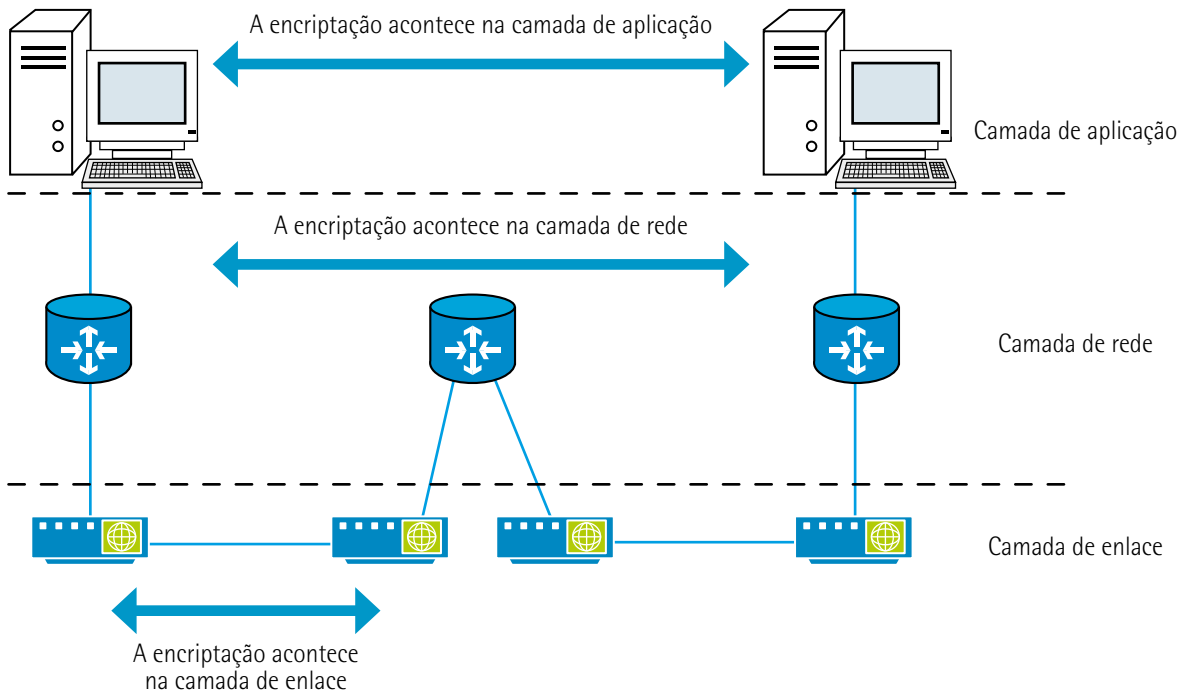

Figura 48 – A encriptação pode ser implementada nas camadas de enlace, rede e aplicação

4.13.1 Tecnologias envolvendo o IPsec

O IPSec combina diversas tecnologias diferentes de segurança em um sistema completo que provê confidencialidade, integridade e autenticidade, empregando atualmente:

- Mecanismo de troca de chaves de Diffie-Hellman.

- Criptografia de chave pública para assinar as trocas de chave de Diffie-Hellman, garantindo assim a identidade das duas partes e evitando ataques do tipo *man-in-the-middle* (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação).

- Algoritmos de encriptação para grandes volumes de dados, como o DES (*data encryption standard*).

- Algoritmos para cálculo de *hash* (resto de uma divisão, de tamanho fixo) com utilização de chaves, como o HMAC, combinado com os algoritmos de *hash* tradicionais, como o MD5 ou o SHA, para autenticar os pacotes.

- Certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

Detalhes do IPSec

Na realidade, além das tecnologias mencionadas no item anterior, o IPSec também se refere a diversos outros protocolos (mencionados nas RFCs 2401-2411 e 2451) para proteger datagramas IP.

Esses padrões são:

- Protocolo de segurança IP: define que informações adicionar ao pacote IP para permitir o controle da confidencialidade, autenticidade e integridade, assim como a forma em que os dados devem ser encriptados.

- *Internet key exchange* (IKE): negocia associações de segurança (SA –*security association*) entre duas entidades e realiza a troca de chaves. O uso da IKE não é obrigatório, mas a configuração manual de associações de segurança é difícil e trabalhosa, logo, torna-se impossível para comunicações seguras em larga escala.

Pacotes IPSec

É definido um novo conjunto de cabeçalhos a serem adicionados em datagramas IP. Os novos cabeçalhos são colocados após o cabeçalho IP e antes do cabeçalho da camada superior (como o dos protocolos de transporte TCP ou UDP). Esses novos cabeçalhos dão as informações para a proteção das informações (*payload*) do pacote IP:

- AH (*authentication header*): esse cabeçalho, ao ser adicionado a um datagrama IP, garante a integridade e a autenticidade dos dados, incluindo os campos do cabeçalho original que não são alterados entre a origem e o destino; no entanto, não fornece confidencialidade. É utilizada uma função *hash* com chave, em vez de assinatura digital, pois o mecanismo de assinatura digital é bem mais lento e poderia reduzir a capacidade da rede.

- ESP (*encapsulating security payload*): esse cabeçalho protege a confidencialidade, a integridade e a autenticidade da informação. Se o ESP for usado para validar a integridade, ele não inclui os

campos invariantes do cabeçalho IP. AH e ESP podem ser usados separadamente ou em conjunto, mas para a maioria das aplicações apenas um deles é suficiente. Para os dois cabeçalhos, o IPSec não especifica quais algoritmos de segurança devem ser utilizados, mas dá uma relação dos possíveis algoritmos, todos padronizados e muito difundidos. Inicialmente, quase todas as implementações trabalham com o MD5 (da RSA Data Security) e o SHA (Secure Hash Algorithm, do governo dos EUA) para integridade e autenticação. O DES é o algoritmo mais comumente usado para a encriptação dos dados, apesar de muitos outros estarem disponíveis, de acordo com as RFCs, como o IDEA, o Blowfish e o RC4.

4.13.2 Modos de operação

O IPSec fornece dois modos de operação:

- No modo de transporte, somente a informação (*payload*) é encriptada, enquanto o cabeçalho IP original não é alterado. Esse modo tem a vantagem de adicionar apenas alguns octetos a cada pacote, deixando que dispositivos da rede pública vejam a origem e o destino do pacote, o que permite processamentos especiais (como de QoS) baseados no cabeçalho do pacote IP. No entanto, o cabeçalho da camada 4 (transporte) estará encriptado, limitando a análise do pacote. Passando o cabeçalho sem segurança, o modo de transporte permite que um atacante faça algumas análises de tráfego, mesmo que ele não consiga decifrar o conteúdo das mensagens.

- No modo de tunelamento, todo o datagrama IP original é encriptado e passa a ser o *payload* de um novo pacote IP. Esse modo permite que um dispositivo de rede, como um roteador, aja como um *proxy* IPSec (o dispositivo realiza a encriptação em nome dos terminais). O roteador de origem encripta os pacotes e os envia ao longo do túnel IPSec, e o roteador de destino decripta o datagrama IP original e o envia ao sistema de destino. A grande vantagem do modo de tunelamento é que os sistemas finais não precisam ser modificados para aproveitarem os benefícios da segurança IP. Além disso, esse modo também protege contra a análise de tráfego, já que o atacante só poderá determinar o ponto de início e de fim dos túneis, e não a origem e o destino reais.

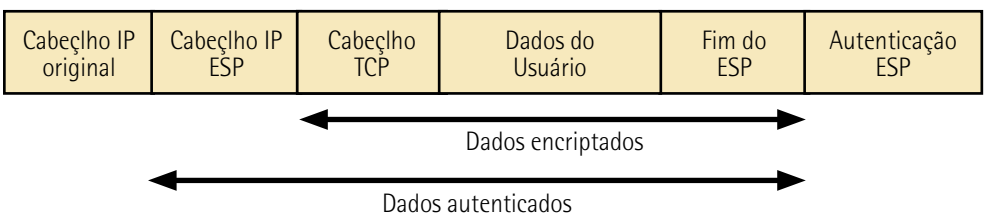

Figura 49 – Cabeçalho genérico encriptado no modo transporte

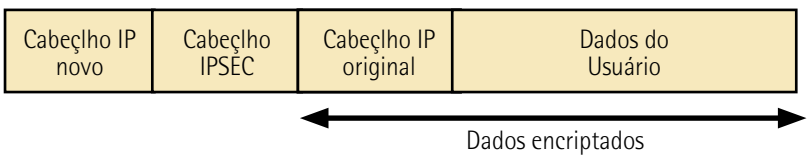

Figura 50 – Cabeçalho encriptado no modo túnel

Como definido pelo IETF, o modo de transporte só pode ser utilizado quando tanto a origem quanto o destino "entendem" IPSec. Na maior parte dos casos, é mais fácil trabalhar com o modo de tunelamento, o que permite a implementação do IPSec sem que sistemas operacionais ou aplicativos nos terminais e servidores precisem ser alterados.

4.13.3 Associações de segurança (SA – *security association*)

Como visto, o IPSec fornece diversas opções para executar a encriptação e autenticação na camada de rede. Quando dois nós desejam se comunicar com segurança, eles devem determinar quais algoritmos serão usados (se DES ou IDEA, MD5 ou SHA). Após escolher os algoritmos, as chaves de sessão devem ser trocadas. Como vemos, há certa quantidade de informações que precisam ser negociadas. A associação de segurança é o método utilizado pelo IPSec para lidar com todos esses detalhes de uma determinada sessão de comunicação. Uma SA representa o relacionamento entre duas ou mais entidades que descreve como estas utilizarão os serviços de segurança para se comunicarem. As SAs também podem ser utilizadas por outras entidades, como IKEs, para descrever os parâmetros de segurança entre dois dispositivos IKE.

As SAs são unidirecionais, o que significa que para cada par de sistemas que se comunicam, devemos ter pelo menos duas conexões seguras, uma de A para B e outra de B para A. As SAs são identificadas de forma única pela associação entre um número aleatório chamado SPI (*security parameter index*) e o endereço IP de destino. Quando um sistema envia um pacote que requer proteção IPSec, ele olha as SAs armazenadas em seus bancos de dados, processa as informações e adiciona o SPI da SA no cabeçalho IPSec. Quando o destino IPSec recebe o pacote, ele procura a SA em seus bancos de dados de acordo com o endereço de destino de SPI e então processa o pacote da forma necessária. As SAs são simplesmente o relatório das políticas de segurança que serão usadas entre dois dispositivos.

4.13.4 Protocolo de gerenciamento de chaves (IKMP – *internet key management protocol*)

O IPSec assume que as SAs já existem para serem utilizadas, mas não especifica como elas serão criadas.

O IETF decidiu dividir o processo em duas partes: o IPSec fornece o processamento dos pacotes, enquanto o IKMP negocia as associações de segurança. Após analisar as alternativas disponíveis, o IETF escolheu o IKE como o método padrão para configuração das SAs para o IPSec.

O IKE cria um túnel seguro e autenticado entre duas entidades, para depois negociar SAs para o IPSec. Esse processo requer que duas entidades se autentiquem entre si e estabeleçam chaves compartilhadas.

4.14 Autenticação

As duas partes devem ser autenticadas entre si. O IKE é bastante flexível e suporta diversos tipos de autenticação. As duas entidades devem escolher o protocolo de autenticação que será utilizado através de negociação. Nesse momento, os seguintes mecanismos são implementados:

- Chaves compartilhadas já existentes: a mesma chave é instalada em cada entidade. Os dois IKEs autenticam-se enviando ao outro um *hash* com chave de um conjunto de dados que inclui a

chave compartilhada existente. Se o receptor conseguir criar o mesmo *hash* usando sua chave já existente, ele sabe que os dois IKE possuem a mesma chave, autenticando assim a outra parte.

- Criptografia de chave pública: cada parte gera um número aleatório e encripta esse número com a chave pública da outra parte. A capacidade de cada parte computar um *hash* com chave contendo o número aleatório da outra parte, decriptado com a chave privada local, assim como outras informações disponíveis pública e privadamente, autentica as duas partes entre si. Esse método permite que as transações sejam negadas, ou seja, uma das partes da troca pode, plausivelmente, negar que tenha feito parte da troca. Somente o algoritmo de chave pública RSA é suportado atualmente.

- Assinatura digital: cada dispositivo assina digitalmente um conjunto de dados e o envia para a outra parte. Esse método é similar ao anterior, mas ele não permite que uma entidade repudie a participação na troca. Tanto o algoritmo de chave pública RSA quanto o DSS (*digital signature standard*) são suportados atualmente.

Tanto a assinatura digital quanto a criptografia de chave pública necessitam do uso de certificados digitais para validar o mapeamento entre a chave pública e a chave privada. O IKE permite que certificados sejam acessados independentemente (por exemplo, através do DNSSEC) ou que dois dispositivos troquem explicitamente os certificados como parte do IKE.

4.15 Troca de chaves

As duas partes devem possuir uma chave de sessão compartilhada para poderem encriptar o túnel IKE. O protocolo de Diffie-Hellman é usado para que as entidades concordem em uma chave de sessão. A troca é autenticada como descrito anteriormente para prevenir contra-ataques do tipo *man-in-the-middle*.

4.16 Utilizando o IKE com o IPSec

A autenticação e a troca de chaves criam a SA entre os IKEs, um túnel seguro entre os dois dispositivos. Um dos lados do túnel oferece um conjunto de algoritmos e o outro deve aceitar uma das ofertas ou rejeitar a conexão. Quando os dois lados concordam com os algoritmos que serão utilizados, eles devem produzir as chaves que serão utilizadas pelo IPSec no AH, no ESP ou nos dois. A chave compartilhada pelo IPSec é diferente da compartilhada pelos IKEs; ela pode ser obtida pelo método de Diffie-Hellman novamente, para garantir o sigilo, ou atualizando a criada pela troca original para gerar a SA IKE, fazendo o *hash* com outro número aleatório. O primeiro método, apesar de fornecer maior segurança, é mais lento. Após esses passos, a SA IPSec é estabelecida.

Sabemos que o IPSec usa o IKE para iniciar uma SA. O primeiro pacote de A para B que deve ser encriptado inicia o processo. O processo IKE monta um túnel seguro entre B e A, onde a SA IPSec será negociada. A então pode usar esta SA para enviar dados de forma segura para B.

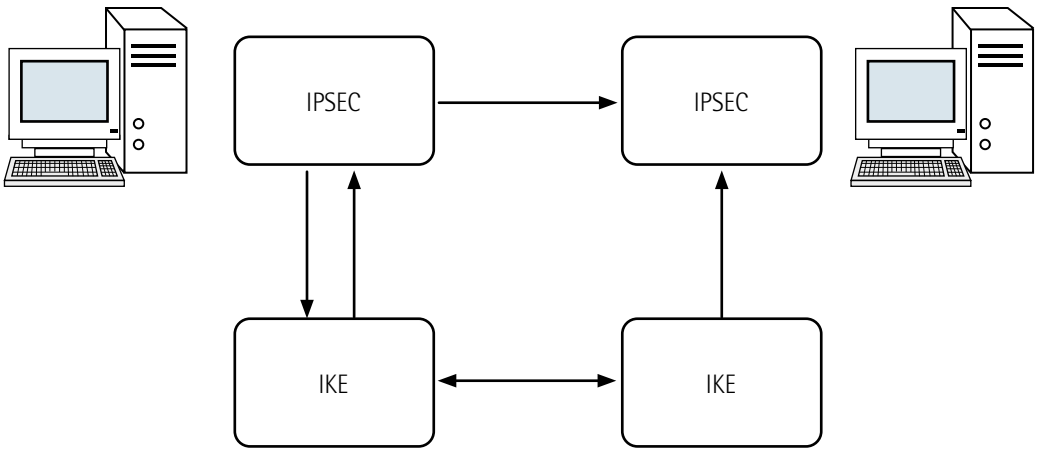

Figura 51 – Aplicação do IPSEC com algoritmo IKE

Juntando todos os passos descritos anteriormente, temos o seguinte exemplo: B quer iniciar uma comunicação segura com A, enviando o primeiro pacote de dados. Quando o roteador de B recebe esse pacote, ele olha suas políticas de segurança e vê se esse pacote deve ser encriptado; a política de segurança, que deve ser configurada anteriormente, também diz que o outro ponto do túnel IPSec será o roteador de A. O roteador de B procura se já há alguma SA IPSec com o roteador. Se ainda não existe, ele pede uma para o IKE; se os dois roteadores já compartilham uma SA IKE, a SA IPSec pode ser rapidamente gerada. Se ainda não compartilham uma SA IKE, ela deve ser criada antes que possa ser negociada uma SA IPSec. Como parte desse processo, os dois roteadores trocam certificados digitais, que estão assinados por alguma autoridade certificadora que os roteadores de A e B confiam. Quando a sessão IKE é ativada, os dois roteadores podem então negociar a SA IPSec; quando esta última é ativada, significa que os dois roteadores concordaram num algoritmo de encriptação (por exemplo, o DES) e um de autenticação (como o MD5), e agora compartilham de uma chave de sessão. Agora o roteador de B pode encriptar o pacote IP que B quer enviar a A, colocá-lo em um novo pacote IPSec e enviá-lo ao roteador de A. Quando o roteador de A recebe o pacote IPSec, ele faz uma busca na SA IPSec, e então processa o pacote e envia o datagrama original para A. Note que todos os passos são feitos pelos roteadores de A e B, deixando o processo transparente aos usuários.

Na prática, a política de segurança pode ser bastante flexível: os roteadores podem decidir quais pacotes devem ser encriptados ou autenticados, de acordo com alguma combinação entre os endereços de origem e destino, portas e protocolo de transporte. Cada um dos tipos de comunicação pode ser autenticado e encriptado separadamente, com chaves diferentes.

4.17 Conclusões

Antes do surgimento de VPN, as comunicações dentro de uma empresa e entre empresas eram feitas através de serviços de *frame relay*, linhas privadas, servidores de acesso remoto e *modems*.

Apesar de serem seguras e apresentarem grande disponibilidade, essas tecnologias são caras e pouco escaláveis. A cada nova filial a ser conectada à rede interna da empresa ou um novo fornecedor que deva acessar um servidor interno, uma nova conexão dedicada deveria ser acionada.

Com as VPN, toda a infraestrutura dedicada foi trocada por uma rede pública e compartilhada, a internet. A conexão permanente com a internet é barata, e para usuários remotos será necessária apenas uma ligação local para acessar a rede interna da empresa.

Apesar da economia de recursos e escalabilidade, a internet apresenta problemas inerentes às redes públicas: não é garantida a privacidade. Para isso, são usados mecanismos de encriptação que garantem o sigilo, a autenticação e a integridade dos dados, formando túneis seguros em meio à rede pública.

Começamos este trabalho com uma visão geral de VPN, sua motivação e as aplicações em que elas são implementadas. Falamos também dos equipamentos e dos mecanismos de segurança. Dois protocolos foram abordados mais profundamente: o L2TP, responsável pela criação de túneis na camada de enlace, e o IPSec, que aparece como o futuro padrão de segurança em redes IP. Com todos esses fatores, conseguimos uma redução acentuada nos custos de comunicação entre a rede da empresa, filiais e fornecedores/consumidores, pelo uso de uma rede pública e compartilhada, associada à privacidade equivalente de conexões dedicadas.

Segue a representação da tecnologia ISDN (*integrated services digital network*), também conhecida por RDSI (rede digital de serviços integrados).

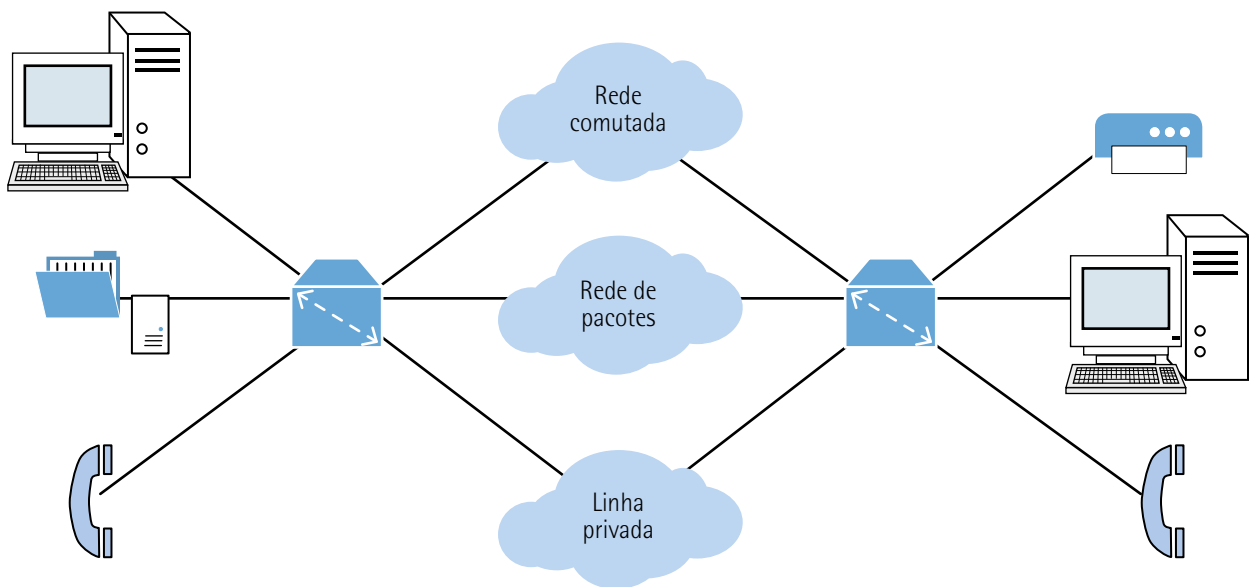

Figura 52 – Exemplo da topologia da rede digital de serviços integrados

Os usuários remotos podem utilizar diversos tipos de tecnologias para solucionar simples problemas de conectividade. Uma dessas tecnologias que vem de encontro a essas necessidades é a da rede digital de serviços integrados, conhecida como ISDN – ou RDSI, em português. A rede digital de serviços integrados foi projetada com os princípios de solucionar o problema de largura de banda para pequenos e médios escritórios ou para aqueles usuários que utilizam tecnologia de rede discada baseada em serviço telefônico tradicional.

As empresas de telefonia então se dedicaram a resolver e desenvolver uma nova tecnologia totalmente digital. A rede digital de serviços integrados surgiu a partir de um sistema de cabeamento telefônico e tem seus princípios muito próximos aos da telefonia tradicional. Quando se inicia uma transferência de dados a partir da rede digital de serviços integrados, o *link one* dessa rede é ativado durante o procedimento de transferência de dados, e quando a chamada é concluída, ele é desarmado. Isso é bem parecido com o que acontece quando se usa o telefone tradicional e se faz uma chamada de voz.

A rede digital de serviços integrados nessas condições permite que sinais digitais possam ser transferidos através de um cabeamento telefônico pré-existente. Tudo isso é fruto da implementação de *switches* pelas companhias telefônicas que foram atualizados para suportar a sinalização digital. A rede digital de serviços integrados é entendida como uma alternativa para a série de dados com linhas privadas e pode ser usada tanto por usuários de conexões móveis quanto por usuários de redes de escritórios pequenos e suporte a redes remotas.

As companhias operadoras de telefonia desenvolveram a rede digital de serviços integrados como parte de um esforço de padronização dos serviços a seus assinantes. Isso inclui a interface de usuário de rede, que é a forma como o usuário se conecta à rede, e apresenta a esses seus recursos a padronização dos serviços assinantes, aumentando a possibilidade de garantia e compatibilidade a padrões internacionais. Os padrões de rede digital de serviços integrados definem os esquemas de hardware, de configuração de chamada e de conectividade global do formato digital para redes ponto a ponto. Esses princípios ajudam a chegar aos objetivos de conectividade mundial e garantem que as redes digitais de serviços integrados se comuniquem de forma facilitada. Podemos encarar essa iniciativa como uma função de digitalização que é realizada dentro das instalações do usuário em vez de ser realizada pela companhia telefônica.

Podemos observar as principais vantagens da rede digital de serviços integrados ao propiciar a conectividade digital para as estações locais:

- A rede digital de serviços integrados pode transportar diversos tipos de sinalização de tráfego para usuário. Ela ainda fornece o acesso ao serviço de rede de telefonia de dados comutados por pacotes e vídeo digital.

  – A rede digital de serviços integrados ainda oferece a configuração por chamada mais rápida do que as conexões por *modem* porque ela usa sinalização para a configuração da chamada de forma muito mais ágil. Por exemplo, algumas chamadas de redes digitais e serviços integrados podem ser configurados em menos de um segundo.

  – A rede digital de serviços integrados ainda fornece uma taxa de transferência de dados expressivamente maior do que os *modems* utilizados em conexões assíncronas. Ela oferece aos seus usuários uma maior largura de banda para as sinalizações que muitas linhas privadas existentes. A aplicação de múltiplos circuitos canalizados em um único circuito é uma das suas características interessantes.

  – A rede digital de serviços integrados ainda pode fornecer um caminho de dados no formato *live* em que são feitas as negociações para lentes do tipo ponto a ponto.

- A construção de projetos com redes digitais de serviços integrados exige um conjunto de recursos que sejam apropriados a toda a flexibilidade do serviço, trazendo questões de projeto ideais para sua implementação:

  – As questões de segurança que envolvem os dispositivos da rede nesse instante podem ser conectadas através de uma rede de telefonia tradicional. Modelos de segurança mais robustos são exigidos para a proteção extensiva dessa rede.

  – As questões de custo e contenção possuem como principal objetivo selecionar equipamentos para redes digitais e serviços integrados evitarem o custo excessivo do serviço de dados em tempo integral, como as linhas privadas e o *frame relay*; portanto, é importante avaliar o perfil de tráfego de dados, as mecânicas e o monitoramento junto aos padrões de redes digitais e serviços integrados para garantir que os custos do *link* sejam controlados.

4.18 A tecnologia da ISDN

4.18.1 Componentes básicos da ISDN

Os componentes utilizados na rede digital de serviços integrados incluem os terminais, os adaptadores e terminais, os dispositivos terminadores de rede, os equipamentos determinadores de linha e ainda os equipamentos determinação da troca.

Existem dois tipos de terminais de rede digital de serviços integrados: o tipo 1 e o tipo 2.

Os terminais de rede digital de serviços integrados especializados são chamados de *terminal equipment type* 1 (TE1 – equipamento de terminal tipo 1). Terminais que não são de rede digital de serviços integrados, como o *data terminal equipment* (DTE), que precedem os padrões da ISDN, são chamados de *terminal equipment type* 2 (TE2 – equipamento de terminal tipo 2).

Os TE1s se conectam à rede digital de serviços integrados através de um *link* digital de par trançado de quatro cabos. Os TE2s se conectam à rede digital de serviços integrados através de um TA.

O TA de rede digital de serviços integrados pode ser um dispositivo *standalone* ou uma placa dentro do TE2. Se o TE2 for implementado como um dispositivo *standalone*, ele se conectará ao TA através de uma interface padrão da camada física.

Além dos dispositivos TE1 e TE2, o próximo ponto de conexão na rede digital de serviços integrados é o dispositivo *network termination type* 1 (NT1 – terminação de rede tipo 1) ou *network termination type* 2 (NT2 – terminação de rede tipo 2). Esses são dispositivos de terminação de rede que conectam o cabeamento em quatro cabos do assinante ao *loop* local de dois cabos convencionais. Na América do Norte, o NT1 é um dispositivo CPE (*customer premises equipment*). Na maioria dos lugares além da América do Norte, o NT1 faz parte da rede fornecida pela operadora. O NT2 é um dispositivo mais complicado, geralmente encontrado em PBXs (*private branch exchanges*) digitais, que executa os serviços de protocolo das camadas 2 e 3. Há também um dispositivo NT1/2, que é um dispositivo único e combina as funções de um NT1 e de um NT2.

Lembrete

O ISDN é empregado como rede, enlace de dados e camadas físicas no contexto do modelo OSI ou pode ser considerado um conjunto de serviços digitais existentes em camadas 1, 2 e 3 do modelo OSI. Em uso comum, o ISDN é, muitas vezes, limitado ao uso do protocolo Q.931 e a outros protocolos relacionados, que são um conjunto de protocolos de sinalização, a fim de estabelecer e quebrar conexões de comutação de circuitos para subsidiar recursos avançados de chamada para o usuário. Ele foi introduzido em 1986.

4.18.2 Pontos de referência do ISDN

Como o CPE (*customer premise equipment*) abrange uma ampla gama de recursos e exige vários serviços e interfaces, os padrões se referem a interconexões através de pontos de referência em vez de requisitos específicos de *hardware*. Os pontos de referência são uma série de especificações que definem a conexão entre determinados dispositivos, dependendo da função desses dispositivos na conexão ponto a ponto. É importante conhecer esses tipos de interfaces, pois um dispositivo CPE, como um roteador, pode suportar diferentes tipos de referências. Os pontos de referência suportados determinam que equipamentos específicos devem ser adquiridos.

Os SPIDs e o *switches* ISDN

Para se ter uma operação funcional da rede digital de serviços integrados, é importante que o tipo de *switch* correto esteja configurado no dispositivo de rede digital de serviços integrados. Os tipos mais comuns nos Estados Unidos são o 5ESS da AT&T e o DMS-100 da Nortel. O tipo mais comum no Japão é o NTT. Os tipos mais comuns no Reino Unido são o Net3 e o Net5. Os provedores de serviços de rede digital de serviços integrados usam vários tipos de *switches* para os serviços de rede digital. Os serviços oferecidos pelas operadoras variam consideravelmente de país para país e de região para região. Assim como os *modems*, cada tipo de *switch* opera de forma distinta e tem um conjunto específico de requisitos de configuração de chamada. Como resultado, antes de conectar um roteador a um serviço de rede digital de serviços integrados, você deve saber os tipos de *switches* usados no escritório central. Identifique essas informações durante a configuração do roteador para que o roteador possa fazer chamadas do nível da rede digital de serviços integrados e enviar dados.

Além de aprender sobre o tipo de *switch* usado pelo provedor de serviços, você também precisa saber os SPIDs (*service profile identifiers*) que estão atribuídos a sua conexão. A operadora da ISDN fornece um SPID para identificar a configuração de linha do serviço da ISDN. Os SPIDs são uma série de caracteres (que podem se assemelhar aos números telefônicos) que fazem a sua identificação com o *switch* no escritório central. Após a sua identificação, o *switch* vincula os serviços que você solicitou à conexão.

4.18.3 As diferenças entre os protocolos de ISDN E, I e Q

O desenvolvimento dos padrões de redes digitais de serviços integrados se iniciou na década de 1960. Surgiu então um conjunto completo de recomendações destinados à rede digital de serviços integrados, o qual foi originalmente publicado em 1984. Ele ainda é continuamente atualizado pelo Comité Consultatif International Téléphonique et Télégraphique e pela ITU-T (União Internacional de Telecomunicações) para estandardização do setor de telecomunicações, órgão que atualmente organiza os protocolos de redes digitais de serviços integrados.

O protocolo Q.921 trabalha essas recomendações do processo de enlace de dados para o canal de redes digitais de serviços integrados D, então o padrão Q.931 controla as funcionalidades da camada de rede entre os nós de extremidades dos terminais e *switch* RDSI correspondente local. Não existe nenhuma recomendação para esse protocolo nas segmentações ponto a ponto. Para os diversos fornecedores do serviço de redes digitais de serviços integrados e ainda contando com diversos modelos de *switches*, pode-se implementar uma variedade imensa de configurações para o protocolo Q.931, apesar de vários outros modelos de *switches* terem sido desenvolvidos antes do desenvolvimento dos padrões pelos comitês.

Apesar de esses novos *switches* não serem padronizados, no momento da configuração da porta de roteamento, você deverá especificar o encaminhador de redes digitais e serviços integrados ao qual esteja se conectando. Os roteadores Cisco têm comandos para identificar falhas e monitoramento dos processos do protocolo Q.931 e Q.921 quando uma conexão de redes digitais de serviços integrados estiver sendo iniciada ou encerrada.

4.18.4 A rede digital de serviços integrados comparados ao modelo OSI

A rede digital de serviços integrados usa um conjunto dos padrões ITU-T, que são comparados às camadas física, de enlace e de rede do modelo de referência OSI.

- Camada física: a especificação da camada física da BRI (*basic rate interface*) da ISDN é definida no ITU-T I.430. A especificação da camada física da PRI (*primary rate interface*) da ISDN é definida no ITU-T I.431.

- Camada de enlace: a especificação da camada de enlace da ISDN é baseada no LAPD e formalmente especificada no ITU-T Q.920, no ITU-T Q.921, no ITU-TQ.922 e no ITU-T Q.923.

- Camada de rede da ISDN: a camada de rede da ISDN está definida no ITU-T Q.930 (também conhecido como I.450) e no ITU-T Q.931 (também conhecido como I.451). Juntos, esses dois padrões especificam conexões comutadas por circuito, comutadas por pacotes e de usuário com usuário.

A camada física do ISDN

A formatação dos quadros da camada física da rede digital de serviços integrados (camada 1) difere dependendo se o quadro é de saída (do terminal para a rede, o formato de quadro NT) ou de chegada (da rede para o terminal, o formato de quadro TE). Ambos os quadros têm tamanho de 48 *bits*, dos quais

36 *bits* representam os dados. Na verdade, são dois quadros de 24 *bits* em sequência que consistem em dois canais B de 8 *bits*, um canal D de 2 *bits* e 6 *bits* de informações de enquadramento (2 * (2 * 8B + 2D + 6F) = 32B + 4D + 12F = 36BD + 12F = 48BDF). Ambos os formatos de quadro da camada física são exibidos. Os *bits* de um quadro da camada física da rede digital de serviços integrados são usados da seguinte maneira:

- *Bit* de enquadramento: fornece a sincronização.
- *Bit* de balanceamento de carga: ajusta o valor médio de *bits*.
- Eco dos *bits* anteriores do canal D: usado para a resolução de disputa quando vários terminais em um barramento passivo disputam um canal.
- *Bit* de ativação: ativa os dispositivos.
- *Bit* reserva: não atribuído.
- *Bits* do canal B1.
- *Bits* do canal B2.
- 8 *bits* adicionais de contagem de *bits* de canal.
- *Bits* do canal D usados para os dados do usuário.

Cada um dos quadros da BRI da ISDN deve ser enviado a uma taxa de 8000 por segundo. Existem ainda 24 *bits* em cada quadro (2 * 8B + 2D + 6F = 24) para uma taxa de *bits* de 8000 * 24 = 192 Kbps. A taxa eficiente é de 8000 * (2 * 8B + 2D) = 8000 * 18 = 144 Kbps.

Muitos dispositivos de usuários de rede digital de serviços integrados podem ser fisicamente conectados a um circuito. Nesse tipo de configuração, poderão ocorrer colisões se dois terminais transmitirem simultaneamente. A rede digital de serviços integrados, portanto, fornece recursos para determinar a disputa de *link*. Esses recursos fazem parte do canal D da rede digital de serviços integrados.

Observe a camada de enlace do ISDN:

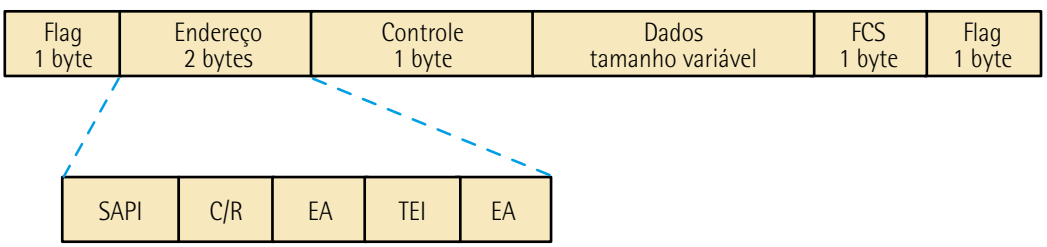

Figura 53 – Detalhes do *trailer* da camada de enlace do ISDN

Detalhe dos campos da camada de enlace da tecnologia das redes digitais de serviços integrados:

- Sapi: são os *bits* de controle do ponto de acesso ao serviço – tamanho: 6 *bits*.
- C/R: *bit* de comando e resposta.
- EA: *bits* do endereçamento estendido.
- TEI: identificador do nó da extremidade do terminal.

A camada enlace do protocolo de sinalização da rede digital de serviços integrados é o LAPD (*link access procedure on the D channel*). O LAPD é similar ao HDLC (*high-level data link control*) e ao LAPB (*link access procedure, balanced*). O LAPD é usado no canal D para garantir que as informações de sinalização e de controle trafeguem e sejam recebidas corretamente. Como indica o significado da abreviação LAPD (procedimento de acesso ao *link* no canal D), ele é usado no canal D para garantir que as informações de sinalização e de controle trafeguem e sejam recebidas corretamente.

Os campos de controle e do *flag* do LAPD são idênticos aos do HDLC. O campo de endereço do LAPD pode ter o tamanho de 1 ou 2 *bytes*. Se o *bit* do endereço estendido do primeiro *byte* estiver definido, o endereço será de 1 *byte*; se não estiver definido, o endereço será de 2 *bytes*. O primeiro *byte* do campo de endereço contém o Sapi (*service access point identifier* ou identificador de ponto de acesso aos serviços), que identifica o portal no qual os serviços LAPD são fornecidos para a camada 3. O *bit* de comando/resposta (C/R) indica se o quadro contém um comando ou uma resposta. O campo do TEI (*terminal endpoint identifier* ou identificador do nó de extremidade do terminal) identifica um único terminal ou vários terminais. Todos os valores 1 no campo TEI indicam um *broadcast*.

4.18.5 A camada de rede do ISDN

Existem duas especificações da camada de rede que são usadas para a sinalização da rede digital de serviços integrados: ITU-T I.450 (também conhecida como ITU-T Q.930) e ITU-T I.451 (também conhecida como ITU-T Q.931). Juntos, esses protocolos suportam conexões comutadas por circuito, comutadas por pacotes e de usuário com usuário. É composta de diversas mensagens para o estabelecimento da chamada, de encerramento da chamada e de informações. Mensagens variadas são especificadas, incluindo configuração, conexão, versão, informações dos usuários, cancelamento, *status* e desconexão.

4.18.6 O encapsulamento do protocolo rede digital de serviços integrados

Quando implementamos as soluções de acesso remoto, uma gama diversa de opções de encapsulamento estará disponível. Os dois tipos de encapsulamento mais comuns são o ponto a ponto e o HDLC. O padrão das redes digitais de serviços integrados é HDLC, porém o ponto a ponto oferece níveis de robustez mais expressivos do que o HDLC, porque fornece um mecanismo de autenticação de negociação das configurações dos *links* associado a protocolos compatíveis. Outro modelo de encapsulamento para rede digital de serviços integrados às conexões ponto a ponto é o LAPB (*link access procedure balanced*).

As interfaces de rede digital de serviços integrados só permitem um único tipo de encapsulamento, aplicado, claro, depois do estabelecimento de uma chamada para RDSI.

As interfaces de redes digitais e serviços integrados são aplicados à maioria dos projetos que utilizam o ponto a ponto para o encapsulamento. O ponto a ponto é um mecanismo que permite conexão modular e eficiente, sendo utilizado especificamente para estabelecer enlace de dados, além de fornecer segurança e encapsulamento protegido no tráfego dos dados. Assim que uma conexão ponto a ponto é negociada entre os dois dispositivos, ela pode encapsular sistematicamente diversos tipos de protocolo, como o IP e o IPX, a fim de estabelecer conectividade à camada de rede.

O ponto a ponto é um protocolo de padrão aberto especificado pela RFC 1661. Ele foi projetado com diversos recursos que o tornam peculiarmente útil nas aplicações de acesso remoto e ainda utiliza o LCP (*logical control protocol*) para, de início, estabelecer os *links* e fazer o acerto da configuração, prerrogativas da camada de enlace. Existem recursos de segurança que foram embutidos dentro desse protocolo, o PAP e o Chap, que auxiliam no projeto de segurança robusta. Para se ter uma ideia, o Chap é um dos protocolos de autenticação mais populares para a filtragem das chamadas.

Resumo

As redes digitais de serviços integrados surgiram para agregar recursos de tecnologia da forma mais próxima das pessoas, sobretudo pela utilização dos serviços de telecomunicações ligados à tecnologia de redes digitais de serviços integrados, o que trouxe um novo momento na comunicação de dados, de voz e de vídeo corporativo.

Na década de 1980, a indústria de telecomunicações esperava que os serviços digitais seguissem o mesmo padrão que os serviços de voz na rede telefônica pública comutada e concebeu um circuito fim a fim de serviços comutados conhecido como B-ISDN (*Rede Digital de Serviços Integrados*).

Antes do B-ISDN, o ISDN original tentou substituir o sistema telefônico analógico por um sistema digital que era apropriado para o tráfego de voz e não voz. A obtenção de acordo mundial sobre a taxa básica padrão de interface era esperada para levar uma grande demanda do usuário para o equipamento ISDN, o que levou à produção em massa de *hardware* ISDN de baixo custo.

No entanto, o processo de padronização levou anos, enquanto a tecnologia de rede informática evoluía rapidamente. Uma vez que o padrão ISDN foi finalmente acordado e os produtos estavam disponíveis, ele já estava obsoleto. Seu emprego foi substancialmente voltado para uso doméstico, então, a maior demanda por novos serviços foi a transferência de vídeo e voz, mas a taxa básica ISDN carece da capacidade de canal necessária.

Isso levou à introdução do B-ISDN, adicionando o termo banda larga, que, embora tivesse um significado em Física e Engenharia (semelhante à banda larga), foi definido pelo CCITT como "qualificar um serviço ou sistema que exija canais de transmissão capazes de suportar taxas superiores à taxa primária", referindo-se à taxa primária que variou de aproximadamente 1,5 a 2 Mbit/s. Os serviços provisionados incluíram o telefone vídeo e a conferência vídeo. Os documentos técnicos foram publicados pelo CCITT no início de 1988. Os padrões foram emitidos pelo Comité Consultatif International Téléphonique et Télégraphique (CCITT, agora conhecido como ITU-T) e chamados de "recomendações". Incluíram os protocolos G.707, G.709 e I.121, que definiram os principais aspectos da B-ISDN, com muitos outros na sequência da década de 1990. A tecnologia designada para B-ISDN foi o modo de transferência assíncrona (ATM), que pretendia transportar ambos os serviços de dados síncronos de voz e assíncrono no mesmo transporte.

A visão B-ISDN foi sobrelevada por outras tecnologias disruptivas utilizadas na internet. A tecnologia ATM sobreviveu como uma camada de baixo nível na maioria das tecnologias de linha de assinante digital (DSL) e como um tipo de carga em algumas tecnologias sem fio, como WiMAX. O termo banda larga tornou-se um termo de *marketing* para qualquer serviço de acesso à internet digital.

Surgida da engenhosidade da engenharia de telecomunicação, a rede digital de serviços integrados não esqueceu os elementos de qualidade de serviço e nem os elementos de segurança para comunicação dos dados e de outras coisas, e até os dias atuais se faz presente em grandes mercados pelo mundo, com uma nova roupagem que acaba para muitas pessoas descaracterizando suas qualidades. As redes digitais de serviços integrados são a base das aplicações digitais e de uma gama imensa de serviços que chegam até a casa das pessoas todos os dias.

Exercícios

Questão 1. (ESAF, 2009) O protocolo que fornece autenticação e criptografia de dados entre hospedeiros e um ponto de acesso em redes sem fio, num esquema baseado em chaves simétricas compartilhadas, é o(a):

A) IKE (algoritmo de troca de chaves na internet).

B) WEP (privacidade equivalente sem fio).

C) AH (protocolo de autenticação de cabeçalho).

D) ESP (protocolo de segurança de encapsulamento de carga útil).

E) EAP (protocolo extensível de autenticação).

Resposta correta: alternativa B.

Análise das alternativas

A) Alternativa incorreta.

Justificativa: faz parte do IPSec e é usado para a troca de chaves.

B) Alternativa correta.

Justificativa: veio antes do WPA e serve para criptografar o tráfego entre o *host* e seu AP.

C) Alternativa incorreta.

Justificativa: faz parte do IPSec e é para criptografia de *payload* em modo transporte.

D) Alternativa incorreta.

Justificativa: faz parte do IPSec e é para criptografia de todo o pacote em modo túnel.

E) Alternativa incorreta.

Justificativa: serve para a autenticação de usuário em nível 2. Depois da autenticação, outra ferramenta fornece criptografia. Parte superior do formulário.

Questão 2. (Funcab, 2010) Em relação a uma interface telefônica RDSI 2B + D, podemos afirmar que:

A) Sua taxa de transmissão máxima é de 164 Kbps.

B) Segue o protocolo 2B + D, de acordo com o modelo europeu.

C) A interface 2B +D também é chamada interface primária.

D) Mesmo sendo uma interface digital, permite a conexão direta de telefones analógicos.

E) Permite a conexão de até 10 equipamentos.

Resolução desta questão na plataforma.