

## Voz em ambiente Wireless

Mobilidade, acesso sem fio e convergência são temas do momento no atual mercado das redes de comunicação. É uma tendência irreversível, que vem se tornando realidade e incorporando-se ao dia-a-dia dos indivíduos, principalmente para aqueles interessados nas facilidades tecnológicas que agregam valor à sua rotina, seja no trabalho, em casa ou no lazer. A possibilidade da utilização de tecnologias de voz em redes sem fio, por exemplo, torna-se cada vez mais um argumento forte para impulsionar o mercado das redes de computadores e, de quebra, torna-se uma preocupação a mais para os profissionais incumbidos pela administração dos recursos da rede.

### A voz como uma informação

A transmissão de voz em redes sem fio pode não ser uma coisa nova em termos tecnológicos, mas, sem dúvida, é algo novo em termos de serviço. Até pouco tempo atrás limitado às redes tradicionais de telefonia, o serviço de transmissão de voz vem se tornando uma solução viável no ambiente das redes sem fio das empresas e mesmo nas residências.

Para que a voz seja transmitida através de uma rede de computadores, ela deve ser transformada para o formato digital (bits) e enviada na forma de pacotes. Logo passa a ser vista como "informação" e não mais como "voz". Esse conceito, adaptado à realidade das redes sem fio, herda todas as vantagens e problemas que qualquer transmissão de dados teria, uma vez que não existe qualquer distinção entre ambos os tráfegos (pacotes de voz ou de dados).

Quando essa técnica de transmissão é introduzida sobre uma solução sem fio, os aspectos tecnológicos observados são basicamente os mesmos que já existem para a rede antes destinada ao tráfego exclusivo de dados, uma vez que, na prática, o que estamos implementando é o transporte da voz (no formato digital) utilizando um protocolo específico (neste caso, o protocolo IP) e apresentando os mesmos mecanismos e funcionalidades quando são transportados apenas dados.

### Um novo cenário

"À medida que a utilização de voz cresce em uma rede, também crescerá a exposição dessa rede às ameaças de segurança". Por se tratar de uma tecnologia que utiliza a infra-estrutura de uma rede sem fio, é natural pressupor que esta afirmativa seja fundamentada e que o tráfego de voz implique realmente em novos riscos quando abordamos os aspectos de segurança para uma rede de computadores.

Todavia, devemos observar que, se uma rede sem fio segue regras de segurança eficientes para a transmissão das informações, o tráfego de dados é seguro e o de voz também o será, pois, como os canais de comunicação são os mesmos, a voz herda a segurança que a rede sem fio oferece para os dados. Entretanto, se a rede sem fio não oferece nenhum meio de proteção para a informação digital, as transmissões de sinais de voz também não terão qualquer tipo de segurança.

Por exemplo, no caso dos hotspots que oferecem acesso sem fio à internet livremente e sem oferecer qualquer nível de segurança, tanto dados quanto voz estarão sujeitos aos vários tipos de riscos e ataques encontrados nesse ambiente inseguro. Cabe ao usuário do serviço providenciar garantias quanto à privacidade de suas comunicações, estabelecendo políticas de acesso capazes de oferecer segurança para a informação que deseja transmitir.

Na verdade, a união entre voz e redes sem fio não traz ameaças novas ou que não possam ser combatidas com políticas de segurança eficientes, embora essa associação possa, certamente, aumentar os efeitos das vulnerabilidades da rede por várias razões.

Por exemplo, é comum um administrador de rede buscar formas alternativas de prover aos seus usuários funcionalidades de rede adicionais (telefonia, por exemplo). Neste aspecto, a segurança deve tornar-se um dos fatores e característica mais importante dos serviços disponibilizados, sendo que as funcionalidades oferecidas devem considerar a aplicação de políticas de segurança que sejam integradas e capazes de abranger a totalidade da rede.

Por esse motivo, é extremamente importante que as empresas adotem políticas de segurança adequadas para protegerem seus ativos de rede, tanto para a comunicação de dados, quanto para a comunicação de voz.

As formas disponíveis para reduzir os riscos na transmissão de voz em redes sem fio são as mesmas que se aplicam às redes antes destinadas ao tráfego exclusivo de dados, são elas: a autenticação por endereço MAC e a criptografia.

Tanto a autenticação por endereço MAC como algumas chaves de criptografia (WEP, por exemplo), são consideradas como de nível de segurança fraco, estando mais vulneráveis a ataques. Outras especificações mais recentes (série IEEE 802.1x, WPA e WPA2, por exemplo) são consideradas mais seguras, permitindo a autenticação e encriptação do tráfego de dados com maior eficiência.

## **Preocupações nos projetos de Voz em WLAN**

Os projetos que envolvem a transmissão de voz sobre redes locais sem fio – WLAN's - devem buscar funcionalidades cujas principais preocupações devem girar em torno de implementações quanto à mobilidade, segurança e à qualidade de serviço oferecido. A autenticação dos usuários e dos dispositivos de rede, assim como a introdução de protocolos de criptografia mais evoluídos, torna-se igualmente uma necessidade que não pode ser relegada a um plano secundário.

### **Mobilidade**

Em termos de mobilidade, é claramente uma vantagem essa integração entre voz e redes sem fio, pois já temos uma infra-estrutura pronta e vamos tirar partido dessa mesma infra-estrutura. A preocupação adicional fica por conta do alcance, da forma de cobertura e da forma de proteção do sistema de rádio escolhido.

### **Segurança**

Ao nível da segurança, os vários mecanismos disponíveis nos dispositivos sem fio devem ser estendidos aos demais dispositivos associados com a transmissão de voz. É fundamental que os administradores da rede se lembrem que é importante (e necessário) configurar as funcionalidades de segurança (tais como criptografia e firewall) para proteger a rede de possíveis ataques.

A segurança deve partir de uma filosofia centrada na necessidade de implementar políticas de acesso aos principais recursos da rede com o objetivo de deter os ataques antes que estes afetem os servidores ou outros dispositivos. Por exemplo, temos freewares e sharewares cujo tráfego de pacotes ou a transferência de arquivos não é detectada pelo tradicional firewall. Usar um aplicativo destes como solução corporativa caracteriza-se, seguramente, como uma falha na segurança.

Sempre é bom lembrar também que os pacotes de voz pode ser um alvo de ataques de spam, DoS, spoofing e phishing, resultando em danos graves como perda de confidencialidade, indisponibilidade dos serviços de comunicação, entre outros.

A utilização de sistemas modulares que permitam lidar com problemas de segurança em qualquer ponto da rede (e não apenas nos pontos de acesso) pode oferecer um maior grau de segurança nesse caso. No entanto, devido à especificidade de algumas soluções e as novas tecnologias emergentes, as soluções devem se preocupar em trabalhar na segurança das redes sem fio, principalmente ao nível da intrusão. Uma vez garantido o nível de segurança no que diz respeito à infra-estrutura, as questões de segurança podem ser tratadas no nível de aplicação e não mais em relação ao meio utilizado.

### **Qualidade de Serviço**

A voz é um tipo de serviço em tempo real que não admite latência na rede, ou seja, o tempo de envio do pacote de voz é o ponto chave para a transmissão em redes onde trafegam pacotes de dados. Os pacotes de voz, ao contrário da maioria dos pacotes de dados, necessitam de uma rede estável que ofereça baixa latência e um mínimo atraso (delay), ou seja, necessitam de redes que ofereçam uma Qualidade de Serviço - QoS (Quality of Service). É através do QoS que os fluxos de dados das aplicações podem ser categorizados em classes de serviço e assim passam a receber um tratamento diferenciado, de acordo com a importância de cada pacote. Este tratamento se dá normalmente por mecanismos de controle e de priorização de fluxo.

Por exemplo, temos a seguinte situação: uma rede com link de Internet, por onde trafegam vários pacotes de diferentes serviços como: FTP, HTTP, SMTP, etc. Uma estação de trabalho conectada nesta rede consome uma determinada banda de transmissão para enviar e receber informações. Se houver uma conexão de voz ativa nesta mesma máquina, a banda consumida tende a aumentar mesmo que seja usado algum tipo de compressão para os dados.

Se, nesta mesma rede, passamos a ter outras máquinas realizando as mesmas funcionalidades da primeira, mas realizando ainda downloads ou uploads de arquivos de forma simultânea, nesta condição teríamos a possibilidade de um link saturado, com a toda a banda praticamente consumida e, neste caso, a conexão de voz seria certamente prejudicada porque não haveria prioridade para os pacotes de voz.

Isso acontece porque os pacotes de voz precisam sair em tempo real e sem atraso (ou com o mínimo de atraso possível), mas se a rede não oferece uma forma de priorizar os pacotes de voz, simplesmente qualquer pacote que chegar primeiro terá a preferência para ser transmitido. Assim, os pacotes de voz esperariam outros pacotes que estivessem na sua frente disputando a

banda disponível e teriam sua saída retardada.

O que se faz na prática é colocar todos os pacotes de voz na frente dos outros pacotes ou disponibilizar uma quantidade específica de banda para que esses pacotes tenham prioridade de transmissão na rede. Neste caso, os pacotes sem prioridade ficam aguardando a sua vez para serem transmitidos, enquanto os prioritários utilizam toda a banda ou uma parte predefinida dela. As outras aplicações ou pacotes, ou aguardam a sua vez, ou recebem uma porcentagem menor da banda. Assim, se um usuário da rede tentar fazer um download ao mesmo tempo em que outro estiver fazendo uma conexão de voz na mesma rede, o QoS dará preferência para a ligação de voz.

### **Resumo, prós e contras**

A utilização de voz em redes sem fio é realmente importante pelos benefícios que oferece, seja pela comodidade que traz ao usuário, seja por causa da redução de custos com telecomunicações que possibilita.

A transmissão de voz está sujeita aos mesmos problemas de segurança que uma rede sem fio oferece para a transmissão de dados, estando susceptível aos mesmos tipos de ataques, ou seja, se não for corretamente protegida, a voz (digitalizada sob a forma de pacotes) pode ser igualmente capturada, permitindo aos intrusos a utilização indevida das informações.

Essa preocupação com a transmissão de voz é tão importante em termos de segurança como em termos da transmissão de qualquer outro tipo de informação sobre o mesmo ambiente.

Por fim, além dos habituais cuidados com o acesso à informação em uma infra-estrutura sem fio, com a voz temos uma preocupação adicional: os problemas ocasionados pela introdução de atrasos nos pacotes de voz, que podem reduzir a qualidade percebida em termos de conversação e até interromper a própria comunicação.