Orientações para implantação e uso de redes sem fio

Define requisitos e orientações técnicas para implantação e uso de redes sem fio na Universidade Estadual de Campinas.

I. Introdução

Este documento apresenta um conjunto de orientações para a implantação e uso de redes sem fio na Universidade e, de acordo com a Instrução Normativa ConTIC-IN-02/2007, deve ser atendido em sua totalidade. Dentre os principais objetivos deste documento, citamos:

- estabelecer requisitos mínimos de funcionalidade e segurança das redes sem fio;
- regularizar as instalações existentes de redes sem fio, conforme os requisitos mínimos especificados;
- atualizar as especificações técnicas atendendo as novas demandas da Universidade.

As redes sem fio são inerentemente menos seguras que as redes cabeadas pois:

- o meio de comunicação é compartilhado por vários usuários, afetando o sigilo dos dados;
- o sinal de radiofrequência extrapola limites físicos (portas, janelas, etc), portanto não há segurança física, o que permite o acesso as redes sem fio por qualquer um que esteja sintonizado na frequência do rádio;
- o padrão original de segurança WEP é fraco e usa uma chave de acesso que é compartilhada entre todos os usuários, comprometendo a segurança e a privacidade;
- a eficiência de uma rede sem fio depende da alocação planejada do espectro disponível nas bandas de 2.4 Ghz e 5 Ghz, que é limitado e potencialmente suscetível à interferência por outros dispositivos sem fio e/ou eletrônicos, fator que pode degradar drasticamente a performance da rede.

Sem controle e segurança adequados, a conexão de uma rede sem fio à rede da Universidade pode comprometer a integridade dos equipamentos, dos serviços e dos dados corporativos.

II. Definições

AP (Access Point) – equipamento que possibilita a interconexão de clientes de uma rede sem fio com uma rede cabeada por meio de ondas de rádio.

Cliente – equipamento da rede sem fio que é operado pelo usuário final; é qualquer equipamento com interface de rádio apropriada para viabilizar a comunicação com um AP.

Redes sem fio – redes de comunicação de dados que fazem uso de ondas de rádio para estabelecer os enlaces de comunicação entre seus componentes.

IEEE 802.11 – conjunto de padrões de comunicação sem fio, também conhecidos como padrões , voltados para comunicações de média distância (dezenas de metros) entre um cliente e um AP ou entre clientes.

IEEE 802.15.1 – padrão de comunicação sem fio, também conhecido como Bluetooth, voltado para comunicações de curta distância (alguns metros) entre um equipamento principal (computador, telefone celular etc) e seus periféricos (teclado, fones, telefones etc).

IEEE 802.16 – padrão de comunicação sem fio, também conhecido como WiMAX, voltado para transmissão de dados em alta velocidade e longa distância (centenas de metros)

Wi-Fi – termo utilizado para descrever redes sem fio baseadas nos padrões IEEE 802.11 .

WPA2 – Mecanismo de segurança que implementa de forma completa o padrão IEEE 802.11i.

SSID (Service Set IDentifier) – Identificador para acesso a uma determinada rede sem fio.

Para que não existam dúvidas quanto a aplicação dessas orientações, alguns termos devem ser interpretados de acordo com as seguintes definições:

- DEVE, DEVEM, NÃO DEVE, NÃO DEVEM: significa que a orientação é mandatória e seu não atendimento será considerado um desrespeito as normas vigentes;
- OPCIONAL, RECOMENDADO: significa que a orientação não é mandatória, no entanto é importante que seu atendimento seja considerado.

III. Orientações técnicas

Cobertura

- Antes da implantação de uma rede sem fio, DEVE ser feito um planejamento da solução, definindo-se os requisitos de serviço desejados, o número de usuários, a quantidade e posicionamento dos APs e a área de cobertura;
- É RECOMENDADO que a potência do sinal irradiado pelo AP seja ajustada para evitar que o sinal se propague para locais indesejados (áreas de coberturas de outros APs e ambientes externos);
- Cuidados adicionais DEVEM ser tomados com equipamentos como fornos de micro-ondas, telefones sem fio 2.4Ghz e outros que utilizam a mesma faixa de frequência, para que não haja interferência mútua.

Mecanismos de segurança

- As redes sem fio DEVEM utilizar mecanismos de autenticação, autorização e *accounting* (AAA) para possibilitar a verificação e auditoria da identidade do usuário;
- É RECOMENDADO o uso do padrão IEEE 802.1x , integrado com servidor RADIUS, para implementar autenticação, autorização e *accounting* de usuários da rede sem fio;
- A autenticação do usuário na rede sem fio DEVE ser protegida por um mecanismo de criptografia, como WPA2 ou portal web (HTTPS);
- É RECOMENDADO o uso de criptografia na camada de enlace da comunicação sem fio, para garantir o sigilo de dados. Para esse fim, é RECOMENDADO o uso de mecanismos de cifragem dinâmica, tal como o WPA2;
- As redes sem fio que atendem a eventos DEVEM solicitar a autenticação dos usuários. Para esse fim, é RECOMENDADO o uso de portal web (HTTPS). Após a autenticação, é RECOMENDADO que o acesso seja limitado à navegação web (HTTP/HTTPS), e-mail seguro e serviços de VPN;
- Equipamentos NÃO DEVEM ser instalados com a configuração de fábrica (*default*). Neste

caso, DEVEM ser alteradas configurações como senhas de administração/gerência do equipamento, parâmetros de identificação do AP e SSID da rede.

Gerência

- APs NÃO DEVEM ser conectados à *hubs,* por questões de performance da rede e segurança dos dados dos usuários, uma vez que esse tipo de equipamento replica todo o tráfego da rede para todas as portas;
- É RECOMENDADO que a rede de gerenciamento dos equipamentos sem fio seja isolada logicamente da rede local;
- No caso da aquisição de múltiplos APs, é RECOMENDADO buscar a padronização dos equipamentos, preferencialmente com uma solução de gerenciamento centralizado.

Configuração dos clientes

- Os equipamentos clientes DEVEM ter o modo *ad-hoc* de comunicação sem fio desabilitado;
- É RECOMENDADO o uso de criptografia nas aplicações, tais como SSL, SSH ou VPN;
- É RECOMENDADO evitar a comunicação de dados via Bluetooth, pois esta tecnologia não possui segurança adequada;
- É RECOMENDADO desabilitar a interface de rede sem fio após o uso. Em alguns computadores e *notebooks*, existem botões ou teclas específicos para este fim;
- Uma rede sem fio NÃO DEVE ser utilizada simultaneamente a uma rede cabeada;
- A fim de proporcionar um acesso seguro à rede sem fio, é RECOMENDADO aos usuários implementar as seguintes medidas adicionais de segurança:
  - instalar um *firewall* pessoal;
  - instalar e manter atualizado um programa antivírus reconhecidamente confiável;
  - atualizar as assinaturas do antivírus diariamente;
  - manter atualizado os *softwares* (sistema operacional, navegador *web*, etc);
  - desabilitar compartilhamento de disco, impressora, etc.

IV. Considerações finais

- Essas orientações se aplicam às redes sem fio baseadas nos padrões IEEE 802.11, 802.15.1, 802.16 e semelhantes sob responsabilidade da Universidade. As orientações não se aplicam às redes sem fio sob responsabilidade de terceiros, tais como redes de dados através de operadoras de Telefonia Celular (EVDO, GPRS, EDGE, 1xRTT, HSPDA, WCDMA, etc);
- Os equipamentos já instalados, quando da publicação dessas orientações, e que não atendam as mesmas, terão 120 dias para serem adequados ou substituídos por outros.

Após este prazo, as situações em não conformidade com este documento estarão infringindo a Instrução Normativa ConTIC-IN-02/2007, e serão tratadas pela Coordenadoria de Tecnologia da Informação e Comunicação da Unicamp (CTIC);

- Em nenhum momento estas orientações se sobrepõem às normas contidas na Resolução GR 05/2005.

V. Requisitos Mínimos

AP (Access Point)

Mínimo

- Compatível com o padrão IEEE 802.11g e/ou IEEE 802.11a e/ou IEEE 802.11n
- Certificação Wi-Fi Alliance
- Taxa de transmissão de dados mínima de 54Mbps
- Controle de acesso à rede por endereço MAC
- Controle de acesso à rede autenticado via servidor RADIUS
- Suporte a criptografia WPA2 Enterprise (por meio de credenciais individuais)
- Compatível com os padrões IEEE 802.1x e 802.11i
- Implementação de RADIUS Authentication e Accounting
- Gerenciamento via SNMP
- LEDS de indicação de energia e atividade
- 1 interface 100BaseTX ou superior com conector RJ45
- Controle de potência do sinal de rádio
- Suporte à atualização de *firmware*
- Certificado de homologação do equipamento junto à ANATEL

Desejável

- Suporte a VLAN IEEE 802.1q
- Suporte a 4 SSIDs simultâneos
- Suporte a *roaming* transparente de usuários
- Mecanismo de *polling* dinâmico
- Filtro de protocolos

- Porta RS-232 (conector DB9 ou RJ45)
- Suporte a alimentação *Power-over-Ethernet* (PoE) IEEE 802.3af ou IEE 802.3at (conforme necessidade)
- Gerenciamento via navegador web compatível com Windows Vista, 7 e Linux

VI. Referências

- Wi-Fi Alliance – http://www.wi-fi.org
- Cartilha de Segurança para a Internet – Cert.BR - http://cartilha.cert.br/