Universidade Estadual de Campinas

Orientações para implantação e uso de redes sem fio

Assunto: Redes sem fio
Identificação:
Data de publicação:
Datas das revisões:
Aplica-se a: Essas orientações se aplicam às redes de dados sem fio baseadas nos padrões IEEE 802.11 (Wi-Fi®), 802.15.1 (Bluetooth™) , 802.16 (WiMAX) e semelhantes, instaladas na Universidade. As orientações não se aplicam às redes de dados sem fio que não são de responsabilidade da Universidade, como por exemplo redes de dados através de operadoras de Telefonia Celular (EVDO, GPRS, EDGE, 1xRTT, etc).

I - Introdução

Este documento apresenta orientações para implantação e uso de redes sem fio visando:

- estabelecer requisitos mínimos de funcionalidade e segurança dos serviços disponíveis nas redes sem fio;
- proteger os dados da Universidade contra acessos indevidos;
- regularizar as instalações atuais de redes sem fio na Universidade, conforme os requisitos mínimos especificados.

Este documento não representa um projeto ou uma política corporativa de redes sem fio para a Universidade, mas consiste em um conjunto de orientações para a operação de redes sem fio nos diversos orgãos da Unicamp.

Uma rede local *wireless* (WLAN), ou sem fio, é um sistema de comunicação implementado como uma extensão ou uma alternativa à LANs cabeadas. Usando a tecnologia de rádio-freqüência, redes sem fio transmitem e recebem dados através de sinais de rádio, minimizando a utilização de cabos e permitindo mobilidade. Atualmente, a maioria das redes sem fio utiliza os padrões IEEE 802.11, conhecido como Wi-Fi®, popular em *notebooks*, *palms* e em alguns celulares.

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

- a rede é compartilhada e cada dispositivo pode ouvir o tráfego de qualquer outro dispositivo dentro da área de cobertura, tornando difícil manter a privacidade;
- o sinal de rádio-freqüência 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 freqüência 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 e 5 Ghz, que é limitado e potencialmente suscetível à interferência por outros equipamentos sem fio, fator que pode degradar drasticamente a performance da rede.

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

II - Definições

Redes Sem Fio – Redes de comunicação de dados que seguem os padrões da família IEEE 802.11 ou semelhantes.

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

WEP – *Wired Equivalent Privacy* . Padrão original de segurança em redes sem fio para encriptar o tráfego da rede.

WPA™ - Wi-Fi® *Protected Access* . Padrão de segurança, mais avançado que o WEP, que implementa a maioria das definições do padrão IEEE 802.11i.

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

Cliente – Usuário da rede sem fio.

Access Point (AP) - Equipamento que interconecta clientes de uma rede sem fio e possibilita sua comunicação com outras redes.

SSID - *Service Set IDentifier* . Identificador para acesso a uma determinada rede sem fio.

Canal – Faixa de rádio-freqüencia utilizada pelos dispositivos para que eles se comuniquem numa rede sem fio

NAT – *Network Address Translation*

EAP – *Extensible Authentication Protocol*

III - Orientações

1. Cobertura
   - Antes da implantação de uma rede sem fio, é necessário fazer um planejamento da solução, definindo as necessidades lógicas, os requisitos de serviço desejado, o posicionamento físico dos APs, a área de cobertura e a alocação de canais;

   - Se possível, a potência do sinal irradiado pelo AP deve ser 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 microondas, telefones sem fio 2.4Ghz e outros que utilizam a mesma faixa de freqüência, para que não haja interferência mútua.

2. Mecanismos de segurança

   - As redes sem fio devem utilizar mecanismos de autenticação, autorização e *accounting* para possibilitar a verificação e auditoria da identidade do usuário.

   - É recomendado o uso de IEEE 802.1x integrado com servidor RADIUS, para implementar autenticação, autorização e *accounting* de usuários da rede sem fio.

   - Se viável, deve-se configurar filtros por endereço MAC para restringir os dispositivos sem fio (*notebooks*, PDAs, etc) que podem acessar a rede sem fio.

   - Exige-se o uso de criptografia na camada de enlace da comunicação sem fio, a fim de evitar a exposição de quaisquer informações. Deve-se utilizar certificados de segurança, credenciais "usuário/senha" ou qualquer outro método de cifragem dinâmica, como WPA™, WPA2™, etc .

   - Nenhum AP pode ser instalado com a configuração de fábrica (*default*). É necessário alterar as senhas de administração/gerência do equipamento, os parâmetros de identificação do AP, o SSID da rede e as configurações de canal, além de restringir endereços IP que podem acessar a interface de gerenciamento, quando possível.

   - Deve-se desabilitar no AP a difusão do SSID da rede, dificultando que a mesma seja detectada por usuários que não sabem de sua existência.

   - As configurações de segurança devem ser feitas antes da instalação do equipamento, a fim de evitar riscos quando utilizado na configuração *default*.

3. Gerência

- APs não devem ser ligados em *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.

- A rede de gerenciamento do AP deve, sempre que possível, ser isolada logicamente da rede local.

- No caso da aquisição de múltiplos APs, recomenda-se buscar a padronização dos equipamentos, preferencialmente com uma solução de gerenciamento centralizado.

- Recomenda-se a utilização de endereços reservados para as redes sem fio, com o uso de NAT para acesso à Internet e a outros sistemas da Universidade.

4. Configuração dos clientes

- configurar mecanismos de segurança no seu computador:

    - instalar um *firewall* pessoal;
    - instalar e manter atualizado um bom programa antivírus;
    - manter atualizado os *softwares* (sistema operacional, navegador *web*, etc);
    - desligar compartilhamento de disco, impressora, etc.

- desabilitar o modo *ad-hoc* de comunicação sem fio;
- optar pelo uso de criptografia também nas aplicações, como por exemplo, o uso de SSH para conexões remotas ou ainda o uso de VPNs;
- evitar a comunicação de dados através de Bluetooth™, pois esta tecnologia não possui segurança adequada;
- desabilitar a interface de rede sem fio após o uso. Em alguns computadores e *notebooks*, existem botões ou teclas específicos para isso. No caso de cartões PCMCIA, recomenda-se retirar o cartão do *notebook* quando não estiver usando a rede sem fio;
- não utilizar uma rede sem fio simultaneamente ao uso de uma rede cabeada.

IV - Considerações finais

- Os usuários devem estar cientes das limitações de performance e segurança das redes sem fio;

- Os equipamentos já instalados, quando da publicação dessas orientações, e que não atendam as mesmas, terão 180 dias para serem adequados ou substituídos por outros;

- Em nenhum momento estas orientações se sobrepõem às normas contidas nas GR 05/05.

V - Requisitos Mínimos

Devem ser observados os seguintes requisitos mínimos para aquisição de APs e clientes de acesso (placas ou cartões) para redes sem fio:

AP (*Access Point*)

Mínimo
Compatível com os padrões IEEE 802.11g e/ou IEEE 802.11a
Certificação Wi-Fi®
Taxa de transmissão de dados mínima de 54Mbps
Compatível com o padrão IEEE 802.1D
Sistema de criptografia WPA™ / EAP (*Pre-shared key* e certificado)
Tabela de controle de acesso MAC
Tabela de controle de acesso utilizando servidor RADIUS
Compatível com o padrão IEEE 802.1x
Gerenciamento através de SNMP
LEDS de indicação de energia e atividade

Certificado de homologação do equipamento junto a ANATEL
Controle de potência do sinal
Suporte à atualização de *firmware*

Desejável
Suporte a VLAN 802.1Q
Software de gerenciamento compatível com Windows® 2000 / XP e Linux
Sistema de alertas através de *traps* SNMP
Suporte a *Roaming*
Mecanismo de *polling* dinâmico
Filtro de protocolos
Porta RS-232 (conector DB9)
Suporte a alimentação via *Ethernet* (*Power over Ethernet*)

Clientes de Acesso

Mínimo
Interface padrão (uma entre PCI, PCMCIA, USB, mini-PCI, *ethernet-wireless* ou integrada).
Compatível com os padrões IEEE 802.11g e/ou IEEE 802.11a (compatível com os APs existentes).
Certificação Wi-Fi®
Taxa de transmissão de dados mínima de 54MBps
Driver de instalação para Windows® 2000, 2003, XP e CE/Mobile quando aplicável.
Suporte aos sistemas operacionais Unix-like.
Sistema de criptografia de WPA™ com os respectivos *drivers* para o sistema operacional.
Suporte ao modo *ad-hoc* e ao modo infraestrutura
Certificado de homologação do equipamento junto a ANATEL

VI - Referências

- http://www.wi-fi.org
- http://en.wikipedia.org
- Wireless Network Station Connection Policy – The University of Sheffield
- Segurança em Redes sem Fio – Nelson Murilo de O. Rufino – Ed. Novatec
- Cartilha de Segurança para a Internet – Cert.BR - http://cartilha.cert.br/