UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Comunicação Sem Fio (Wireless)

Aula 10 – Segurança em Redes Sem-fio (continuação)

Prof. Fred Sauer

email: fsauer@gmail.com

http://www.fredsauer.com.br

IEEE 802.11i

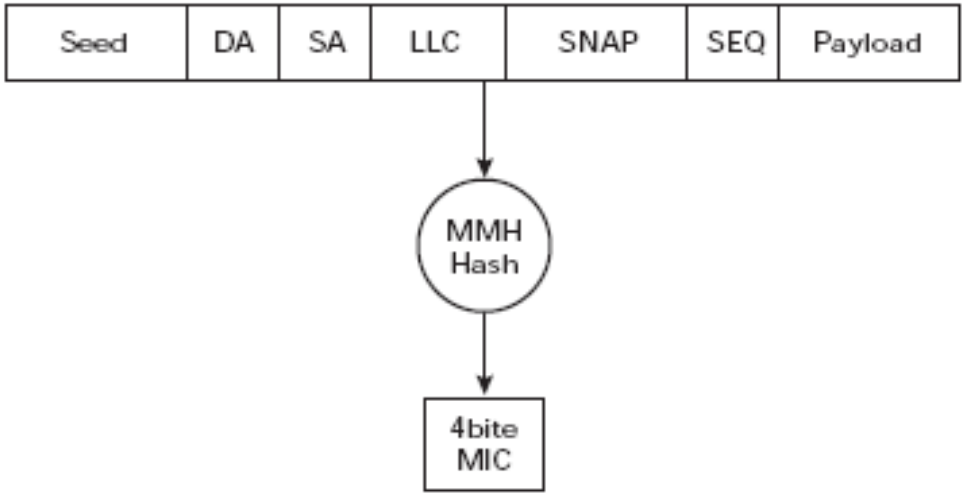
- Substituto do protocolo WEP:
  - Oferece dois esquemas de criptografia:
    - TKIP e CCMP que podem ser utilizados simultaneamente na mesma rede.

TKIP

- TKIP (Temporal Key Integrity Protocol), também chamado de WEP2
- Projetado para resolver os problemas apresentados pelo WEP, ao mesmo tempo que mantém a compatibilidade com a base instalada.
- Basta fazer um upgrade do firmware.

TKIP

- Integridade:
  - Controle através do MIC (Message Integrity Code)
  - MIC é um campo do frame 802.11i, calculado a partir de diversas informações contidas no próprio frame, como, por exemplo, os endereços MAC de origem e destino
  - MIC é calculado a partir de uma função de hashing, conhecida como Michael



TKIP

- Replay attacks Protection:
  - Implementa um campo de sequência para evitar ataques do tipo replay
  - O número de sequência é incrementado a cada frame enviado, sendo que o AP irá descartar frames que estejam fora de ordem

TKIP

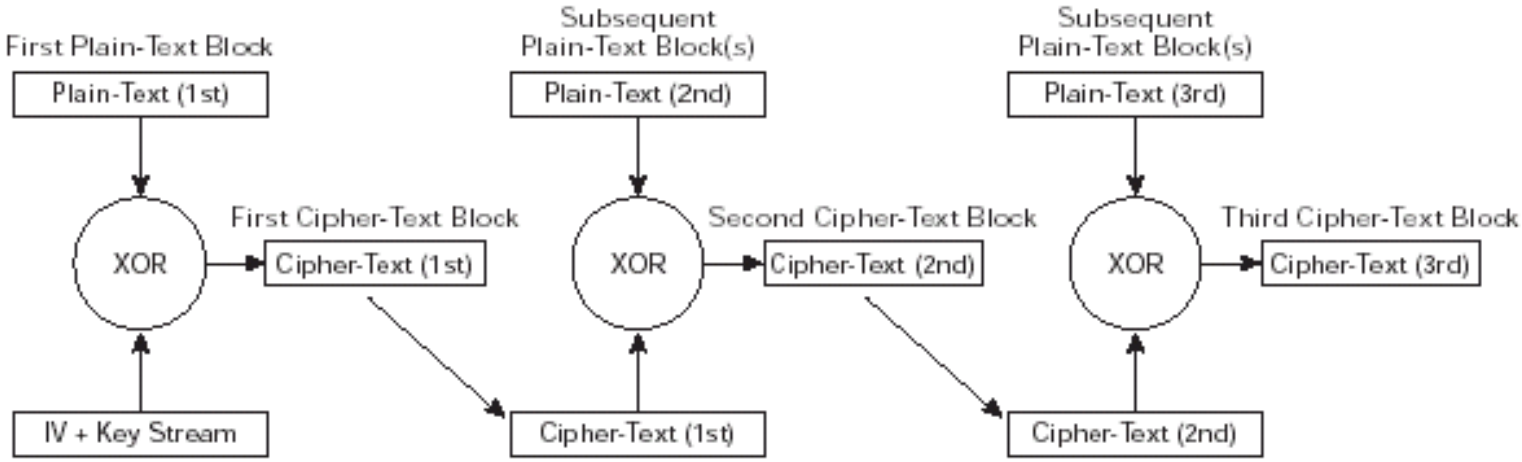
- Confidencialidade:
  - Utiliza um vetor de incialização (IV) de 48 bits, ao contrário dos 24 bits utilizados no WEP. Com 48 bits é possível enviar 2^{48} frames sem que o IV se repita, o que permite ampliar o tempo de vida da chave temporal, tornando desnecessária a geração de uma nova chave.

CCMP

- CCMP (CCM Protocol):
  - Utiliza o padrão para criptografia simétrica AES (Advanced Encryption Standard).
  - AES trabalha com blocos de 128 bits e, no caso do 802.11i, chaves de 128 bits

CCMP

- AES trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado
  - CCM utiliza o modo de operação conhecido como CBC (Cipher Block Chaining)
  - CBC-CTR (Cipher Block Chaining Counter Mode) oferece criptografia
  - CBC-MAC (Cipher Block Chaining Message Authenticity Check) Oferece controle de integridade



WPA

- Objetivos:
  - ✓ Exigir uma maior nível de segurança para as redes sem fio
  - ✓ Resolver os problemas encontrados no WEP através de upgrade de software
  - ✓ Prover uma solução de rede wireless segura para usuários de redes small office/home office (chave compartilhada)
  - ✓ Ser compatível com o padrão IEEE 802.11i

WPA

- Funcionalidades de segurança:
  - ✓ Autenticação
    - ✓ Combinação de autenticação open system e 802.1X (WPA Enterprise)
    - ✓ Autenticação com chave pré compartilhada (Pre-shared key), para ambientes sem infraestrutura de RADIUS (WPA Personal)
  - ✓ Criptografia
    - ✓ Temporal Key Integrity Protocol (TKIP)
    - ✓ Advanced Encryption Standard (AES) (optional)
  - ✓ Integridade dos dados
    - ✓ Michael

WPA

- Chaves:
  - ✓ Pairwise
    - ✓ Usada para tráfego entre o AP e cada cliente
  - ✓ De grupo
    - ✓ Chaves utilizadas para tráfego de multicast e broadcast enviado pelo AP

WPA

- Pairwise master Key:
  - ✓ Chave de 256-bits derivada da autenticação EAP-TLS ou PEAP
  - ✓ Pairwise master key (PMK) usada para derivar as chaves temporais (temporal keys):
    - ✓ Chave de criptografia (128 bits) (Data encryption key)
    - ✓ Chave de integridade de dados (128bits) Data integrity key
    - ✓ EAPOL-Key encryption key (128 bits)
    - ✓ EAPOL-Key integrity key (128 bits)

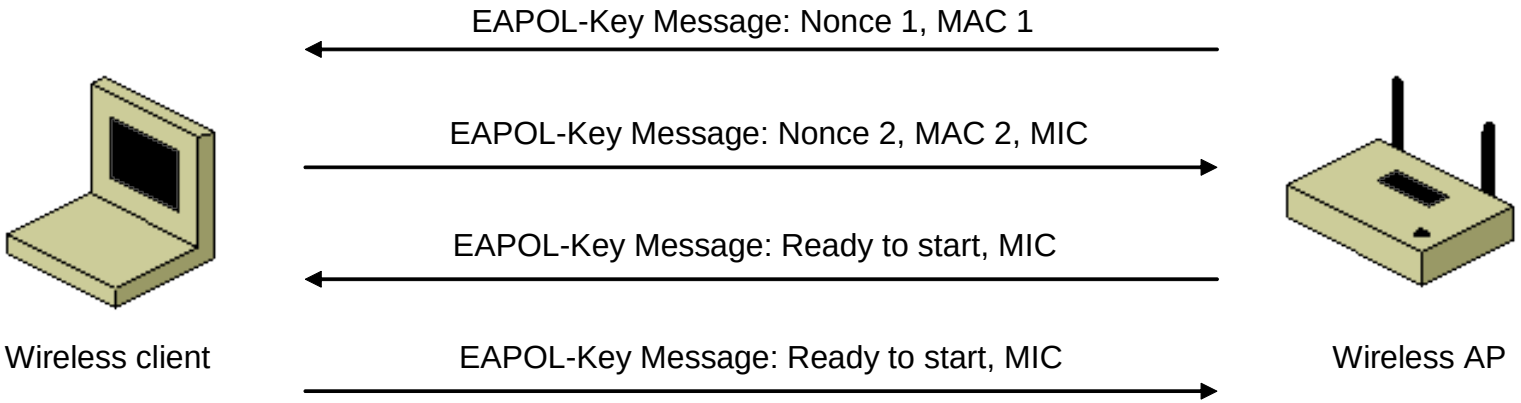
WPA

- Elementos para a computação da chave temporal:
  - PMK
  - Nonce 1
    - Criado pelo AP wireless
  - MAC 1
    - MAC address do AP wireless
  - Nonce 2
    - Criado pelo cliente wireless
  - MAC 2
    - MAC address do cliente wireless

Troca de mensagem da chave temporal (Temporal key)

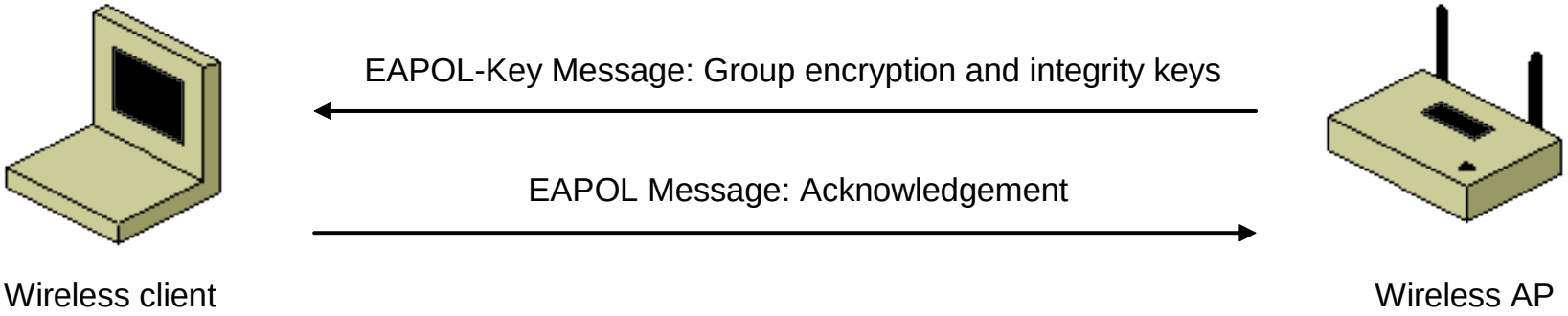
WPA

- Troca de quatro mensagens
  - Confirma que cada cliente possui o conhecimento da PMK
  - Permite cada cliente saber as chaves temporais (temporal keys)



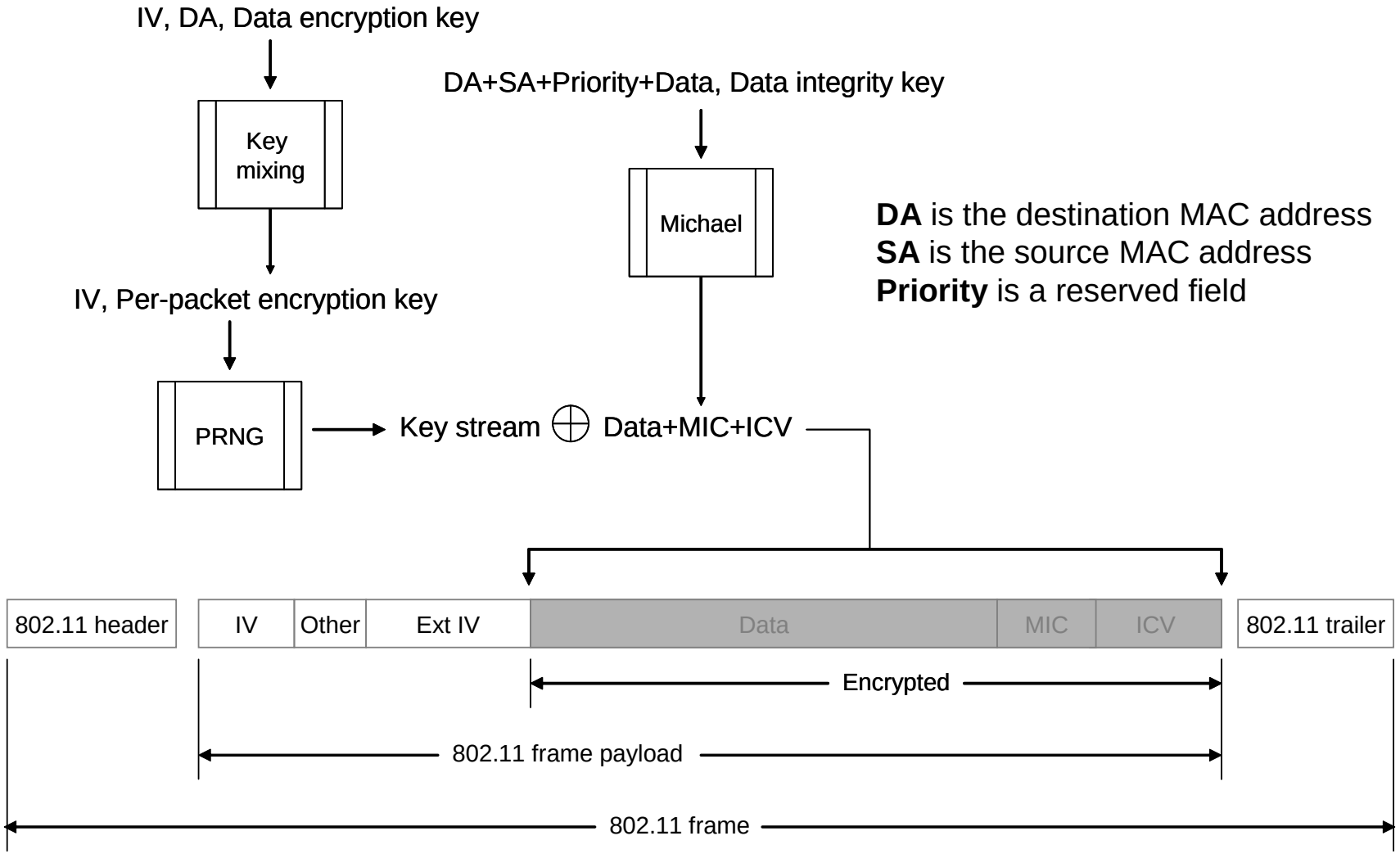
Chaves de Grupo

- O AP Wireless gera:
  - Group encryption key (128 bits)
  - Group integrity key (128 bits)
- O AP Wireless distribui as chaves de grupo para cada cliente wireless



Processo de criptografia do WPA

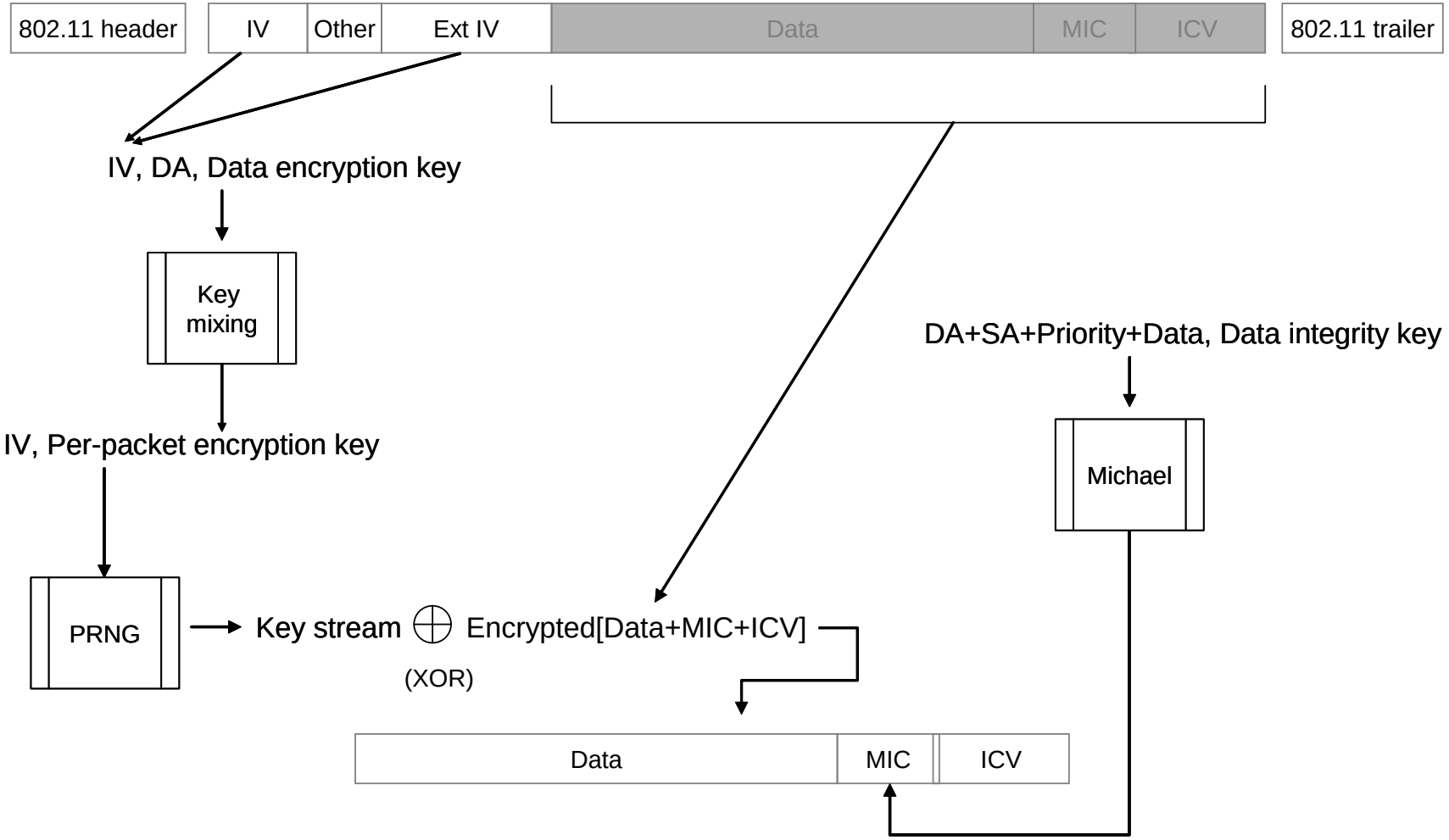
WPA



DA is the destination MAC address
SA is the source MAC address
Priority is a reserved field

Processo de decriptografia do WPA

WPA



Visão geral do WPA2

WPA2

- Padrão de criptografia definido pelo NIST (National Institute of Standards and Technology) para substituir o DES
- Certificado da Indústria por ser compatível com o padrão IEEE 802.11i
- WPA2 Corporativo (Enterprise)
  - Usa o 802.1X e EAP para autenticação
- WPA2 Pessoal (Personal)
  - Usa chave pré-compartilhada (preshared key) para autenticação
- Métodos de criptografia:
  - TKIP
  - AES

WPA2

- Bloco de criptografia AES
  - 128, 192, ou 256 bits

- São definidos vários modos de operação

WPA2

- Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)
  - Usa blocos e chaves de 128-bits
- Criptografia com AES/Counter mode
  - Usa o número do pacote (IV) e o endereço MAC de origem para gerar um contador usado durante o processo de criptografia/descriptografia
- Autenticação dos dados e integridade dos dados com CBC-MAC

Comparativo WPA x WPA2

	WPA	WPA2
Enterprise Mode **(Business, Education, Government)**	**Authentication:** IEEE 802.1X/EAP **Encryption:** TKIP/MIC	**Authentication:** IEEE 802.1X/EAP **Encryption:** AES-CCMP
Personal Mode **(SOHO, Home/Personal)**	**Authentication:** PSK **Encryption:** TKIP/MIC	**Authentication:** PSK **Encryption:** AES-CCMP

WPA2

- Quando utilizar autenticação 802.1X:
  - WPA2/AES e EAP-TLS
  - WPA2/AES e PEAP-MS-CHAP v2
  - WPA/TKIP e EAP-TLS
  - WPA/TKIP e PEAP-MS-CHAP v2
- Small office/home office sem autenticação 802.1X:
  - WPA2/AES com uma preshared key
  - WPA/TKIP com uma preshared key

Recomendações de Segurança

- Verificar o alcance do sinal utilizando algum scanner de rede
- Utilizar autenticação por endereço MAC se for possível.
- Configurar a chave secreta de acesso aos dispositivos de rede diferente da default
- Habilitar o melhor protocolo de segurança com a maior chave possível
- Utilizar firewall pessoal nas estações
- Colocar o AP na DMZ do seu firewall corporativo.