UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Conceitos Sobre Segurança em Redes Sem Fio

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

INTRODUÇÃO

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Base da segurança:
  - Confidencialidade
    - ✓ Controle de acesso
    - ✓ Não-repúdio
  - Integridade
  - Disponibilidade

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Confidencialidade:
  - A informação só deve ser acessada por quem for autorizado
  - Proteção de dados privados
  - Formas de obter confidencialidade
    - ✓Controle de acesso
    - ✓Controle das operações individuais de cada usuário (não-repúdio)

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Integridade:
  - A informação não pode ser corrompida
  - Em alguns casos, a integridade pode ser mais importante do que a confidencialidade (por exemplo, acessos e transações bancárias)
  - Pode haver alteração dos dados na fonte, no destino ou durante o trânsito.

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Disponibilidade:
  - – A informação deve estar sempre disponível para uso
  - – Uma ruptura do sistema não deve impedir o acesso aos dados
  - – Impedir a disponibilidade é uma forma de ataque à segurança, pois isso pode impedir a verificação se os dados continuam confidenciais e íntegros

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Critérios para a segurança:
  - Autenticação
    - ✓ Autenticação de Usuários
    - ✓ Certificação Digital (PKI)
  - Confidencialidade
    - ✓ Controle de acesso
      - Na Estação e na Rede
    - ✓ Criptografia de Dados
      - Na Estação e na Rede (VPN, Criptografia de e-mail)

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Critérios para a segurança:
  - Integridade
    - ✓ Criptografia dos dados
    - ✓ Anti-Virus / Anti-Trojan / Anti – Spyware
    - ✓ Controle de Conteúdo Ativo (ActiveX, Applets)
  - Monitoramento
    - ✓ Estático (análise/detecção de vulnerabilidades)
    - ✓ Dinâmico (Intrusion Detection / Intrusion Prevention)

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Critérios para a segurança:
  - Administração Centralizada
    - ✓ Auditoria / Reporting
    - ✓ Instalação / Manutenção
    - ✓ Backup
    - ✓ Política de Segurança

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Como se proteger:
  - Prevenção
  - Detecção
  - Resposta

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Planejamento e administração geral
    - ✓ Quais recursos devo proteger?
    - ✓ De quem/qual tipo de ameaça precisamos proteger?
    - ✓ Análise de custo e riscos
  - Segurança no dia-a-dia
    - ✓ Senhas, acessos, auditoria
  - Administração no dia-a-dia
    - ✓ Contas, manutenção, disponibilidade

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Deve conter
    - ✓ Diretrizes
    - ✓ Normas
    - ✓ Procedimentos

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Segurança Física
    - ✓ Relativo a aspectos físicos (ex: controle de acesso físico às instalações e CPD)
  - Segurança Lógica
    - ✓ Relativo a falhas voluntárias (ex: ataques e invasões)
  - Segurança Técnica
    - ✓ Relativo a falhas involuntárias (ex: pane em equipamentos)
  - Segurança Humana
    - ✓ Relativo ao despreparo de usuários e administradores

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Um exemplo
    - ✓ Usuários:
      - Tipos de contas
      - Finalidade de uso
      - Expiração / Renovação
      - Definir atitudes no caso de violação

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

INTRODUÇÃO

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

SEGURANÇA EM REDES WI-FI IEEE 802.11

SEGURANÇA EM REDES WI-FI IEEE 802.11

MOTIVAÇÃO

- Maior problema atualmente em redes sem fio.
- Muito suscetível a interceptações dos dados da rede
- Necessidade de protocolos de segurança para garantir a privacidade da rede

SEGURANÇA EM REDES WI-FI IEEE 802.11

WEP

- Segurança em redes sem fio no padrão IEEE 802.11 original
  - Autenticação
    - ✓ Sistema Aberto (Open System)
    - ✓ Chave Compartilhada (Shared key)
  - Criptografia
    - ✓ Wired Equivalent Privacy (WEP)
  - Integridade
    - ✓WEP-encrypted Integrity Check Value (ICV)
      - Cyclical Redundancy Check (CRC)-32 checksum calculation

SEGURANÇA EM REDES WI-FI IEEE 802.11

WEP

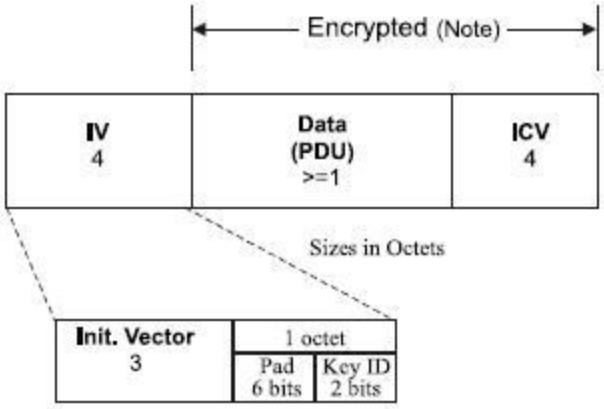
- WEP (Wired Equivalent Privacy):
  - Atua na camada de enlace entre estações e o Ponto de Acesso (AP)
  - Pode ser implementado em Software ou Hardware
  - Chaves de 40 bits ou 104 bits com IV de 24 bits que é passado em claro
  - Foi projetado para oferecer integridade, confidencialidade e autenticação

WEP

- Confidencialidade:
  - Utiliza o algoritmo RC4
    - ✓ Inventado por Ron Rivest em 1987
    - ✓ Simétrico: Chaves de criptografia e decriptografia iguais
    - ✓ Stream Cipher (cifra de fluxo): criptografia byte a byte
    - ✓ Simples de ser implementado e rápido: utiliza uma operação de XOR entre o texto a ser cifrado e a chave
    - ✓ Utilizado na maioria dos sites de comércio eletrônico, onde não oferece os mesmos problemas de segurança apresentados no WEP por conta da troca do IV

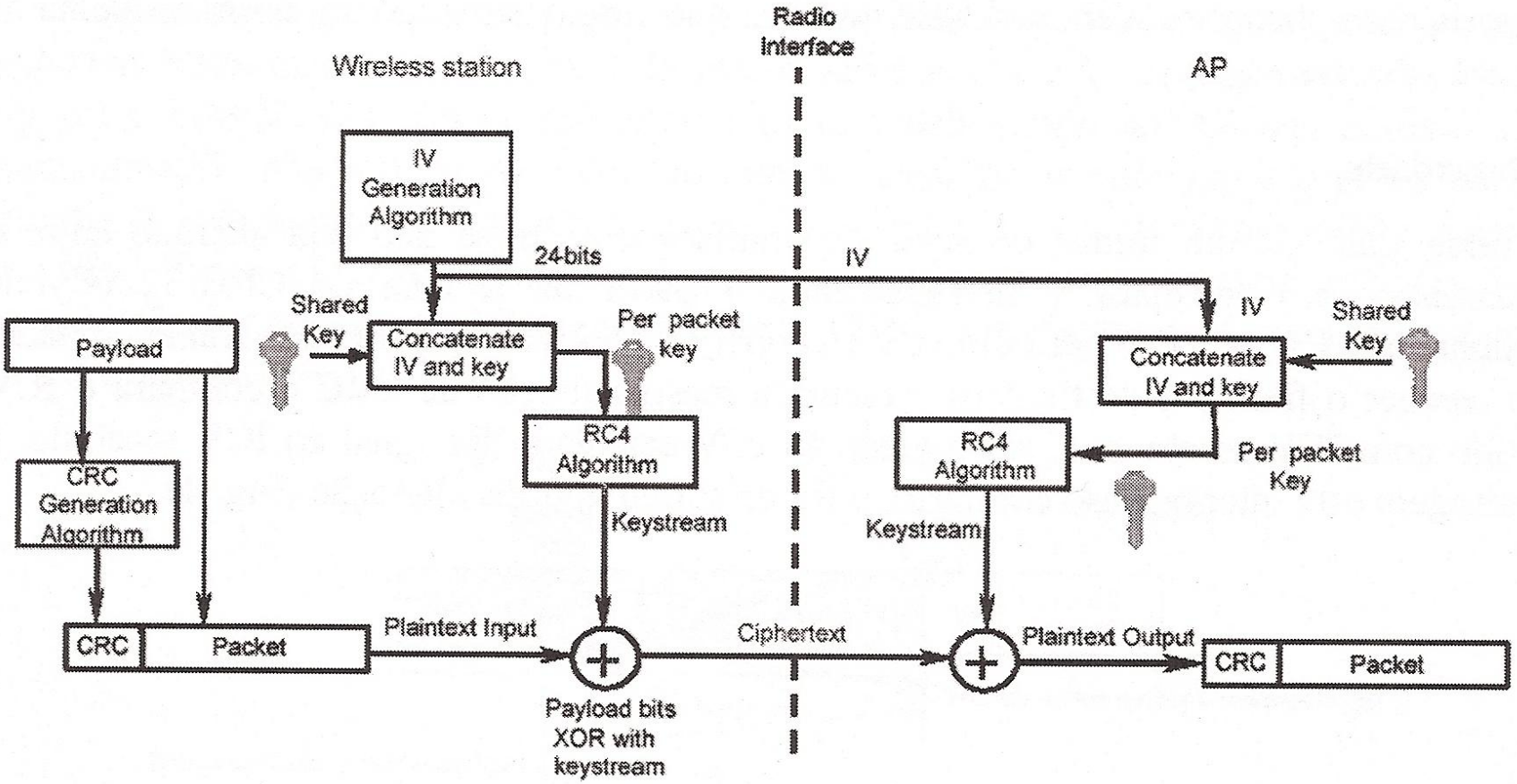
WEP

- Confidencialidade:
  - Cada frame é criptografado independentemente dos demais
  - Utiliza um vetor de inicialização (IV) para compor as chaves (de 40 para 64 bits e 104 para 128 bits)



WEP

- Confidencialidade - Processo:



WEP

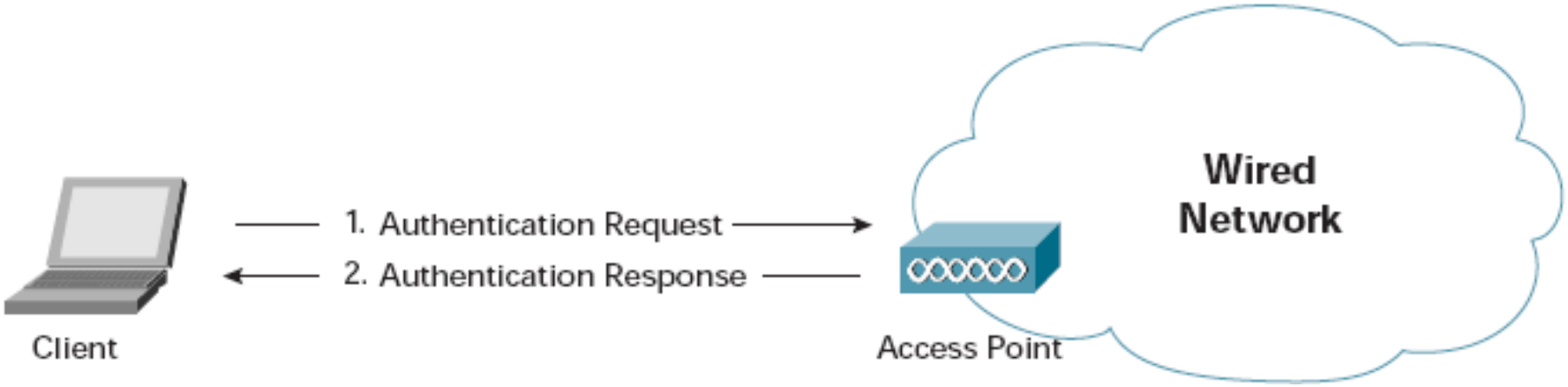
- Confidencialidade:
  - Problemas:
    - ✓ Não existe esquema de gerência de chaves. As estações e o AP compartilham a mesma chave
    - ✓ Existem diversos ataques que exploram o tamanho da chave de criptografia e a forma como é inicializada e incrementada.
    - ✓ O IV é transmitido em claro junto com a mensagem WEP
    - ✓ Após algum tempo monitorando o tráfego da rede é possível obter a chave de criptografia através de análise estatística dos textos cifrados
    - ✓ É possível obter-se a chave criptográfica a partir de uma mensagem conhecida e a respectiva mensagem criptografada

WEP

- Autenticidade:
  - Oferece dois mecanismos
    - ✓ Open authentication e Shared key authentication
    - ✓ Ambos não garantem autenticidade
  - Open authentication
    - ✓ Uma estação solicita acesso ao AP e o AP garante o acesso.
    - ✓ Funciona como autenticação nula

WEP

- Autenticidade:
  - Open authentication: Composto de duas mensagens

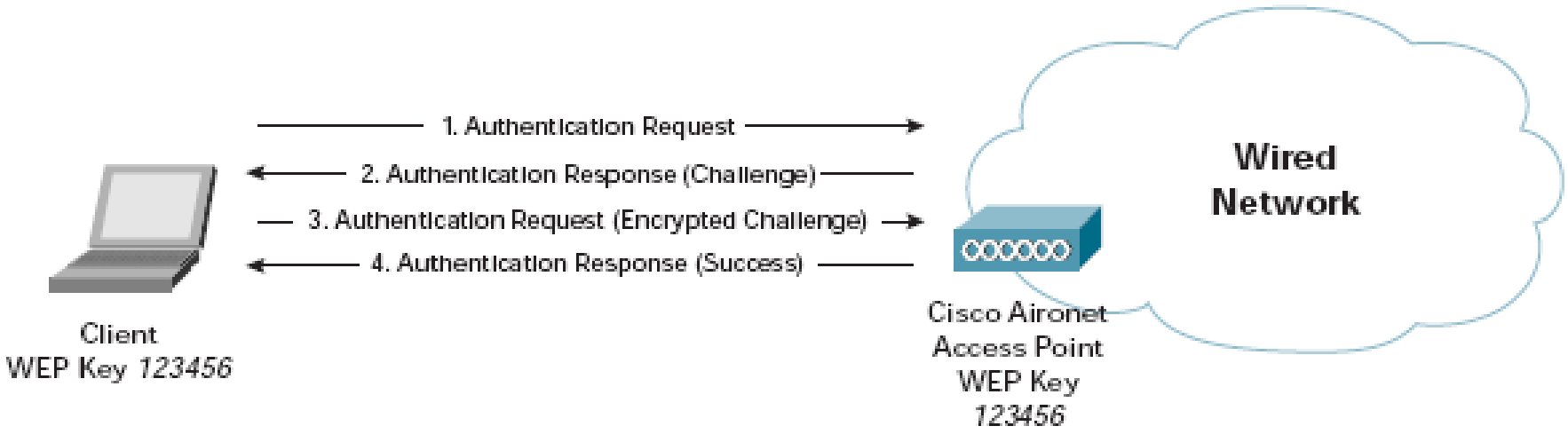


WEP

- Autenticidade:
  - Shared key authentication
    - ✓ Utiliza o esquema de challenge-response
    - ✓ Apenas garante que as chaves são as mesmas
    - ✓ Não deve ser utilizado por expor a chave de criptografia
  - Alguns fabricantes oferecem autenticação utilizando o MAC Address, porém este esquema pode ser forjado (spoofing)

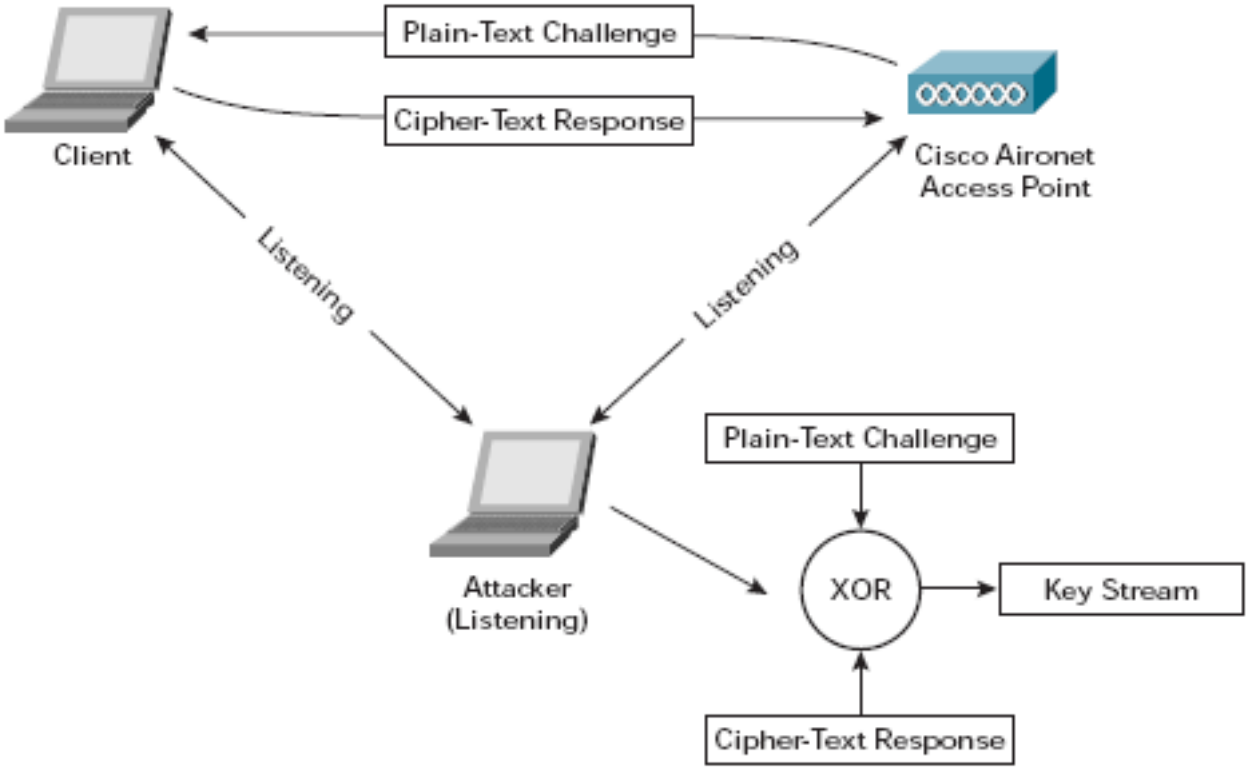
WEP

- Autenticidade:
  - Shared key authentication:



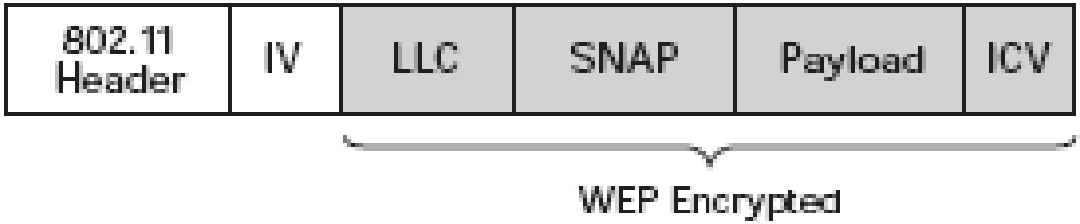
WEP

- Autenticidade:
  - Problema:



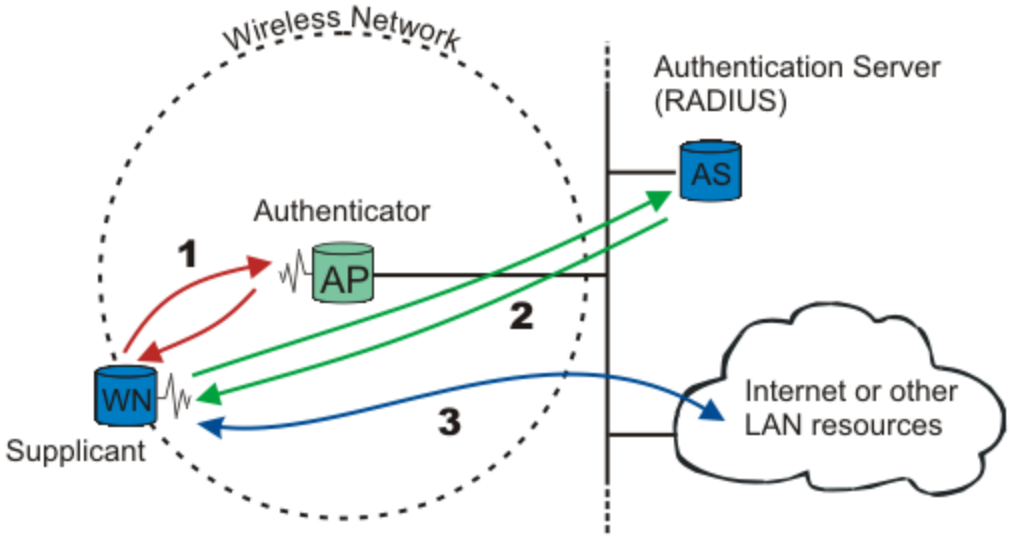
WEP

- Integridade:
  - – Permite que o destinatário verifique se o frame foi alterado
  - – Adiciona um campo (Integrity Check Value – ICV) ao frame antes de ser criptografado
  - – O ICV é calculado a partir do frame a ser transmitido
  - –Semelhante ao CRC, porém o CRC não é enviado criptografado e pode ser recalculado



IEEE 802.1X

- Controle de acesso baseado no conceito de porta
  - Foi definido originalmente para Switches Ethernet
- Formado por três entidades
  - O suplicante, que solicita a conexão
  - Autenticador, que controla o acesso
  - Servidor de autenticação, que processa os pedidos de conexão



IEEE 802.1X

- Utiliza o EAP (Extensible Authentication Protocol), RFC 2284, para interligar os protocolos de autenticação da camada de aplicação com os da camada de enlace.
  - O EAPOL (EAP Over LAN) extensão para ser utilizada em redes 802.*
- Geralmente utiliza o RADIUS como protocolo e servidor de autenticação
- É normal que o AP faça o papel de autenticador e servidor de autenticação

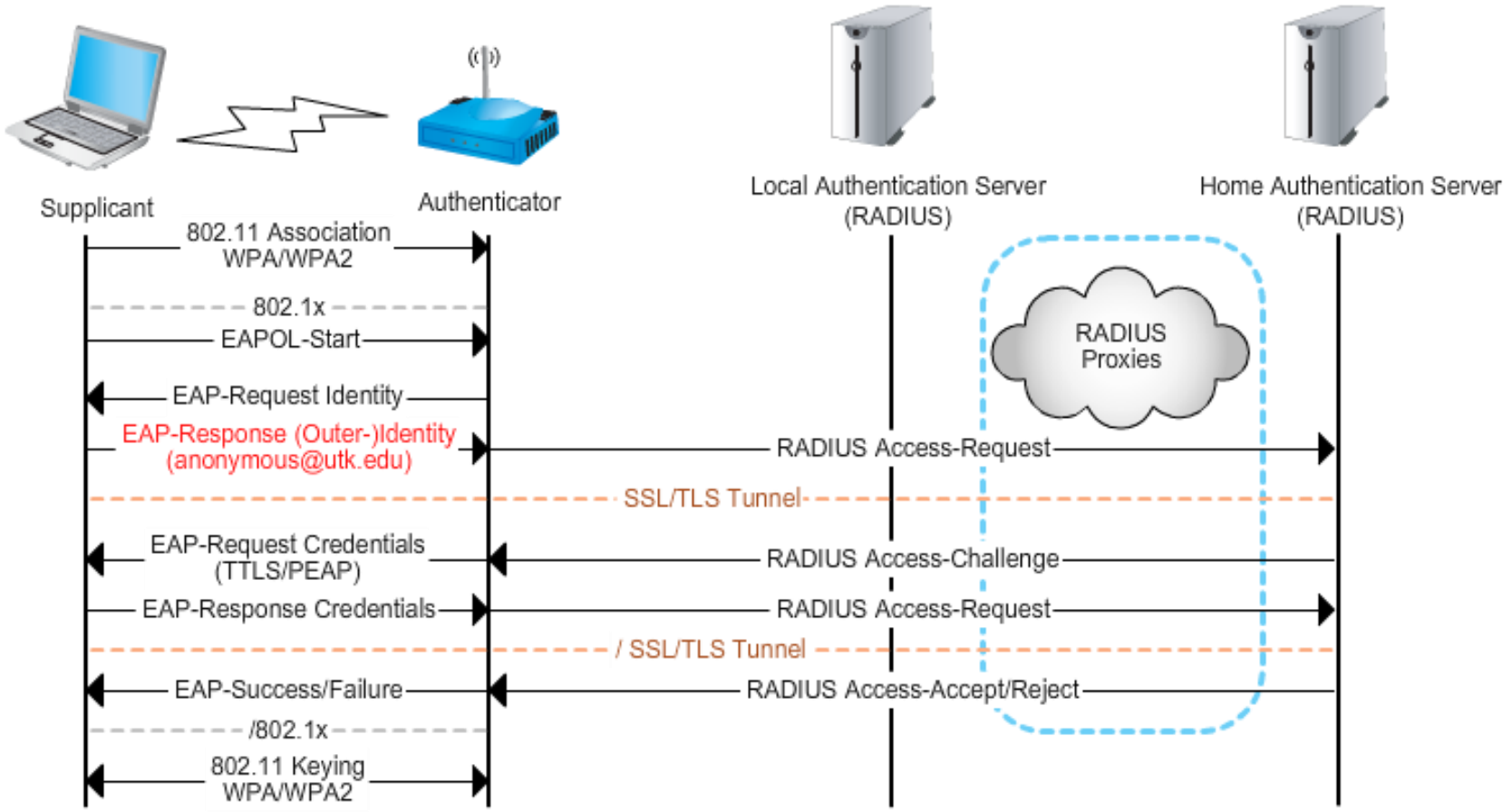
IEEE 802.1X

- Processo de autenticação (resumo):

1) A estação envia uma mensagem do tipo EAP-start, que inicia o processo de autenticação;
2) O AP responde com mensagem EAP-request, solicitando ao cliente sua identificação;
3) A estação envia uma mensagem EAP-response com sua identificação para o AP;
4) O AP envia a mensagem para o servidor de autenticação;
5) O servidor de autenticação verifica as credenciais do cliente e envia uma mensagem para o AP indicando se o cliente está ou não autorizado;
6) O AP envia uma mensagem EAP-success ou EAP-reject para o cliente;
7) Caso o cliente seja autorizado, o AP altera o estado da porta para autorizada.

IEEE 802.1X

- Processo de autenticação



IEEE 802.11i

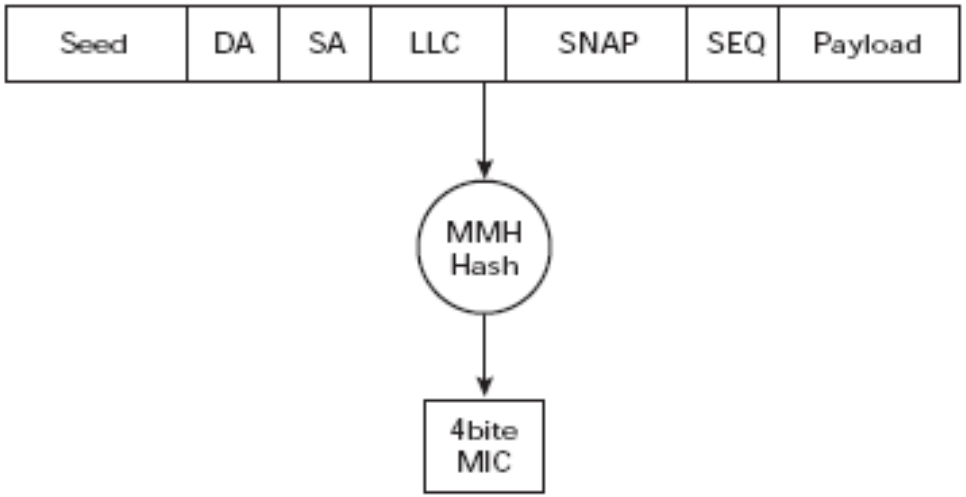
- Substituto oficial (IEEE) do protocolo WEP:
  - Oferece dois esquemas de criptografia:
    - TKIP e CCMP que podem ser utilizados simultaneamente na mesma rede.

TKIP

- TKIP (Temporal Key Integrity Protocol)
- Projetado para resolver os problemas apresentados pelo WEP relacionados com a sua chave estática
- Ao mesmo tempo mantém a compatibilidade com a base instalada.
- Basta fazer um upgrade do firmware.

TKIP

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

TKIP

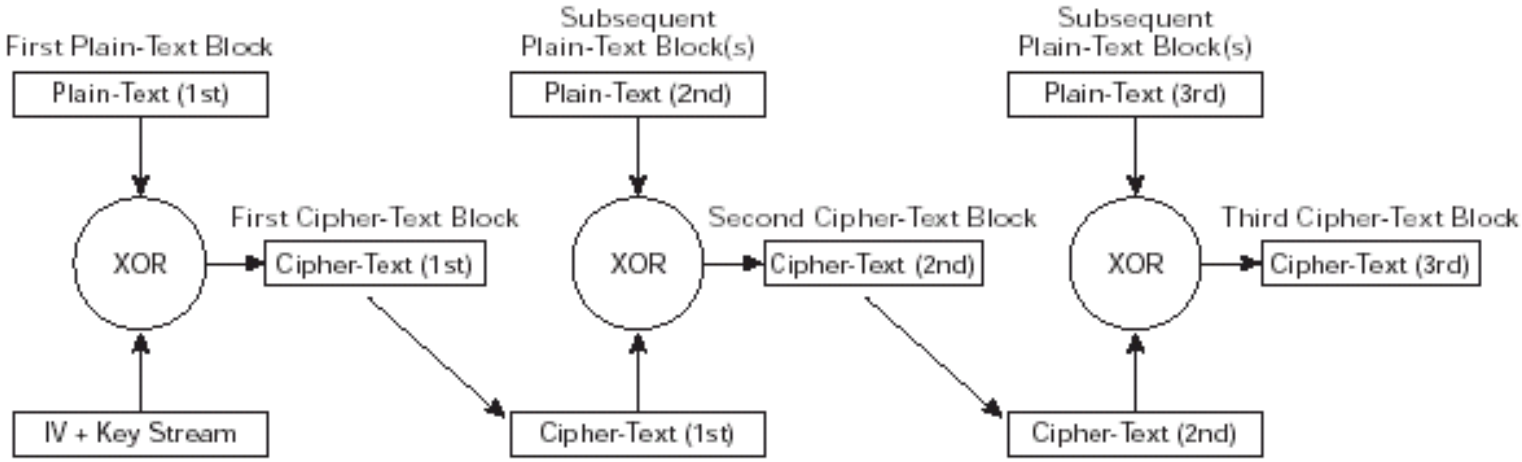
- Confidencialidade:
  - Utiliza um vetor de incialização (IV) de 48 bits, ao contrário dos 24 bits utilizados no WEP.
  - Com 48 bits é possível enviar 2^{48} frames sem que o IV se repita, o que permite ampliar o tempo de vida da chave temporal, tornando desnecessária a geração de uma nova chave.

CCMP

- CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol):
  - Utiliza o padrão para criptografia simétrica AES (Advanced Encryption Standard).
  - Usa o modo de operação CBC (Cipher Block Chaining) e a autenticação baseada no conhecimento da chave simétrica (MAC)
  - O AES trabalha com blocos de 128 bits e, no caso do 802.11i, chaves de 128 bits

CCMP

- O CCMP trabalha com o modo de operação CBC e com o AES, que altera 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 através do AES com chave de 128 bits
  - CBC-MAC (Cipher Block Chaining Message Authenticity Check)



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)

WPA

- Funcionalidades de segurança:
  - ✓ Autenticação
    - ✓ Combinação de autenticação open system e 802.1X (WPA Enterprise); ou
    - ✓ 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

Visão geral do WPA2

WPA2

- 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

- 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:**	**Authentication:** IEEE 802.1X/EAP **Encryption:**