ESTT - Engenharia Informática

Projecto de redes 2013/2014

Aula 1 -3

Objectivos:

- Revisão das tecnologias da camada de ligação
  - Redes sem fios (802.11 a/b/g e HIPERLAN 2)
  - Planeamento de redes wireless

Planeamento de redes wireless (RF)

- Redes indoor
  - Planeamento complexo: modelos de propagação complexos devido às muitas variáveis a ter em conta
  - Devido à complexidade são normalmente utilizados programas
  - Distâncias curtas e grande concentração de dispositivos sem fios.
  - Modelo de conectividade: ponto multiponto (Um AP para vários clientes)
- Redes outdoor
  - Modelos de propagação mais simples: parte-se do princípio que há linha de vista
  - Distâncias da ordem das dezenas de metros
  - Modelos de conectividade:
    - Ponto a ponto
    - Ponto multiponto
    - Multiponto multiponto (pouco utilizado)

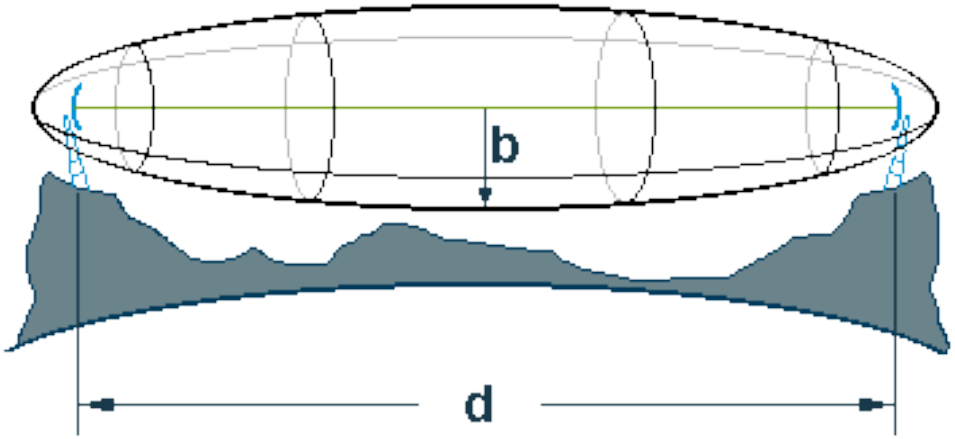
Planeamento de redes wireless (RF)

- Factores a ter em conta no planeamento de redes wireless:
  - Fontes de interferência.
  - Desvanecimento do sinal.
  - Propagação do sinal.
  - Número de nós que se pretendem ligar.
  - Tipo de topologia (ponto-a-ponto; ponto-multiponto; multiponto-multiponto)
  - Serviços a suportar (voz, dados, streaming de vídeo, etc..).
  - Distâncias.
  - Segurança.
  - Linha de vista

- O desvanecimento e a forma de propagação do sinal dependem fortemente do local de instalação.
- Durante a fase inicial do projecto deve ser feito um site survey para determinar a viabilidade do uso de tecnologias wireless.
  - Avaliação da distância; das interferências e da linha de vista; distância entre o AP e a antena externa, etc...

Planeamento de redes wireless (RF)

- Avaliação das condições de linha de vista
  - Elipsóide de Fresnel de primeira ordem desobstruído -> LoS
  - Elispóide de Fesnel parcialmente obstruído -> NoS



$$F_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

Fn = The nth Fresnel Zone radius in metres

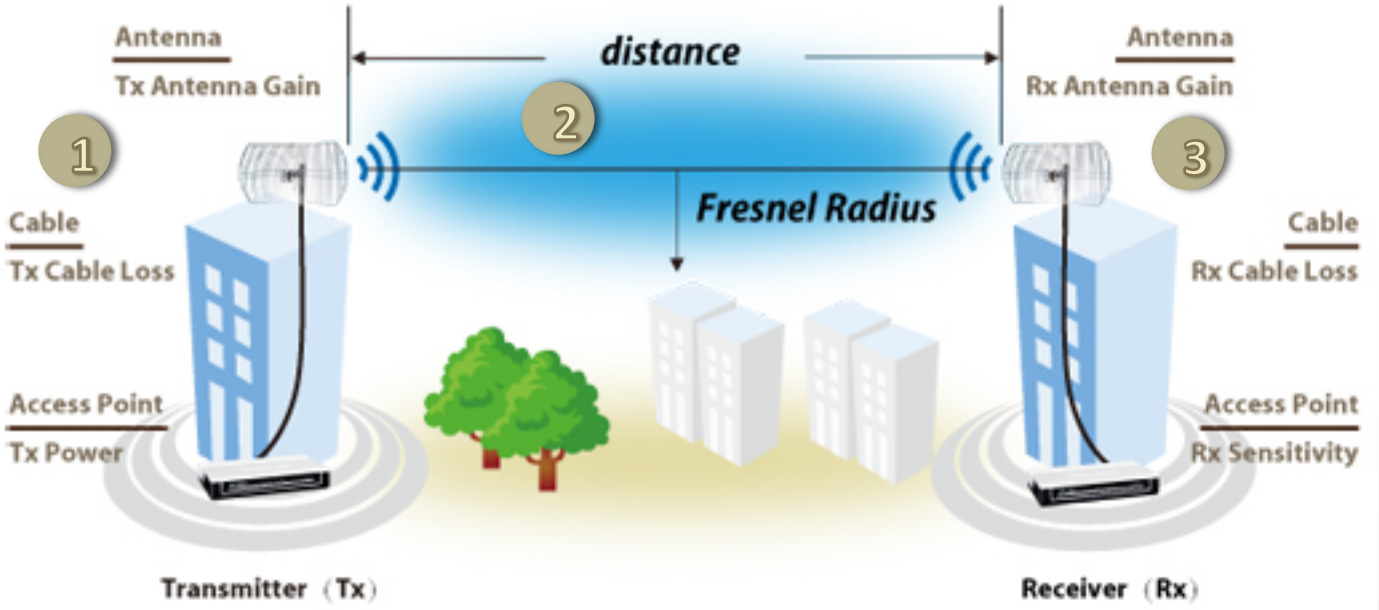
d1 = The distance of P from one end in metres

d2 = The distance of P from the other end in metres

λ = The wavelength of the transmitted signal in metres

Planeamento de redes wireless (RF)

- Estudo da viabilidade de um link wireless
  - Cálculo do link budget (balanço de potências)
    - É usado para dimensionar os vários componentes da rede de forma a assegurar a qualidade da ligação (e do cumprimento da lei).



Fonte: http://www.tp-link.com/en/support/calculator/

Planeamento de redes wireless (RF)

- Estudo da viabilidade de um link wireless
- Cálculo do link budget (balanço de potências)
  - Pode-se dividir o balanço de potência de uma ligação em 3 partes:
    - 1 - Potência transmitida efectiva: potência transmitida [dbm] + ganho antena [dBi] + perdas do cabo e conector [dB]
    - 2 - Perdas na propagação: perdas em espaço livre [dB]
    - 3 - Sensibilidade efectiva do receptor: ganho da antena [dbi] + perdas do cabo e conector [dB] + sensibilidade [dBm]
- O balanço de potência deverá estar compreendido entre 6 e 10dB.
- No caso em que a situação de transmissão não seja igual à de recepção, por exemplo utilizando antenas com ganhos diferentes, o balanço de potência terá de ser calculado em ambos os sentidos. (i.e. Do ponto A para o ponto B e do ponto B para o ponto A)

Planeamento de redes wireless (RF)

- Cálculo da potência em dBm (conversão entre W e dB):
  - Pot= 10*log10(P/ 0.001)
    (P [Watt])
- Cálculo das perdas nos cabos e nos conectores:
  - Existem tabelas com estes valores.
  - Dependem do tipo e do fabricante do cabo.
  - Valores tipo:
    - Cabo - 0.22dB/m.
    - Conectores - 0.1 e 0.5dB.
- Ganho da antena:
  - Depende do tipo da antena -> omnidireccional, Bi-quad, …
  - Depende do fabricante da antena.
  - Existem tabelas com estes valores.

Planeamento de redes wireless (RF)

- Perdas de propagação
  - Por uma questão de facilidade é usada a fórmula de Friis que calcula as perdas em espaço aberto (este valor é o minorante).
  - As perdas de propagação em espaço aberto para uma ligação em 2.45GHz são dadas por:
    - $Lp(dB)= 92,45 + 20\log_{10} F+20 LOG_{10}d$
      Lp= Path loss
      F= frequência em GHz
      dB= decibels
      d= Distância em Km
    - Outros factores de atenuação: chuva 0.05dB/Km, nevoeiro 0.07dB/Km (f=2.4GHz)

Planeamento de redes wireless (RF)

- A potência emitida e a sensibilidade do receptor são dadas pelo fabricante.
  - Em relação à potência emitida, existem limites legais que devem ser cumpridos.
  - A sensibilidade depende das características do receptor (SenR) .
    - O valor da sensibilidade para um dado equipamento depende do débito pretendido.

Receive Sensitivity 802.11g (font: cisco aironet 802.11 a/b/g wireless card)

- -94 dBm @ 1 Mbps
- -93 dBm @ 2 Mbps
- -92 dBm @ 5.5 Mbps
- -86 dBm @ 6 Mbps
- -86 dBm @ 9 Mbps
- -90 dBm @ 11 Mbps
- -86 dBm @ 12 Mbps
- -86 dBm @ 18 Mbps
- -84 dBm @ 24 Mbps
- -80 dBm @ 36 Mbps
- -75 dBm @ 48 Mbps
- -71 dBm @ 54 Mbps

Planeamento de redes wireless (RF)

- Cálculo da Potência radiada (**Equivalent Isotropically Radiated Power**):

  $$Pr(dBm) = Pt(dBm) + PerdC + Ganho(dBi)$$

  - Pr – Potência radiada
  - Pt – Potência transmitida
  - PerdC – Perdas no Cabo
  - Ganho da Antena

  - Na Europa a potência emitida não pode exceder os 20 dBm (100mW) se for utilizada a norma IEEE802.11.
- Cálculo da potência máxima transmitida (Equivalent Isotropically Radiated Power - EIRP):

  $$EIRP(dBm) = Pr(dBm) + PerdC(dB) + Ganho(dBi)$$
- Sensibilidade efectiva do receptor:

  $$SefR(dB)=Ganho(dBi) + SensR+PerdC(dB)$$
- Balanço de potência:

  $$Balanço(dB)=EIRP(dBm) + Lp(dB)+SefR(dB)$$

802.11 - Planeamento de redes

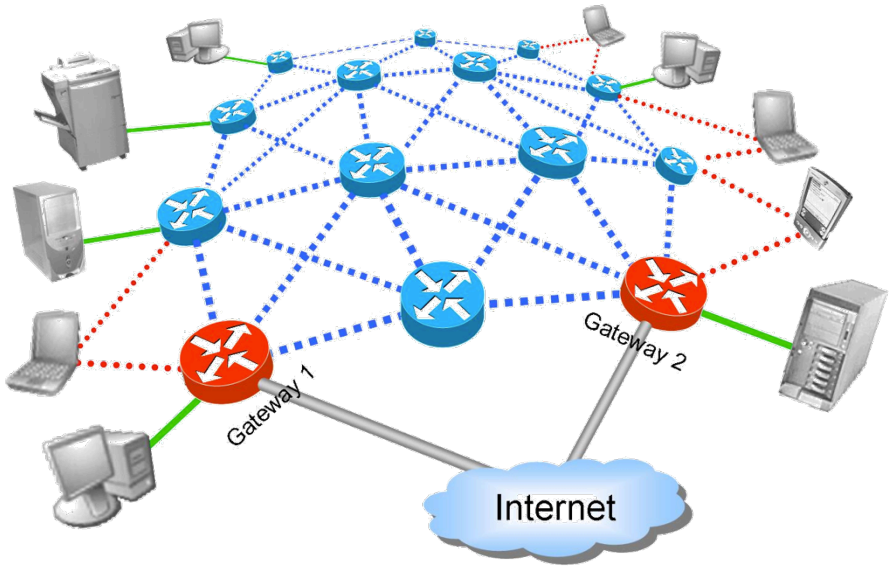
- Exemplo:
  - Considere uma rede wireless que usa um AP Cisco 350 que opera à potência de 20dBm na frequência 2.45GHz. A antena é omnidireccional e tem um ganho de 6dBi. A antena encontra-se ligada ao AP através de um cabo coaxial de 3m com atenuação de -0.63dB. À distância de 1Km, em campo aberto, encontra-se um portátil equipado com uma carta WLAN Cisco 350 com uma antena omnidireccional com o ganho de 2.2 dBi. A sensibilidade do receptor é de -80dBm.
    - Este sistema cumpre as normas legais?
    - Esta ligação é viável?
  - Trabalho para casa, encontrar uma solução que torne esta ligação legal e viável.

HIPERLAN 2

- Especificado pelo European Telecommunications Standards Institute (ETSI)
- Usa a banda 5,475 – 5.725 GHz
- Potência máxima radiada (PIRE) – 1W
- Usa 11 canais não sobrepostos
- Usa um mecanismo de DFS (Dynamic frequency selection)
- Só está normalizado para utilizações outdoor

Novas tecnologias wireless:

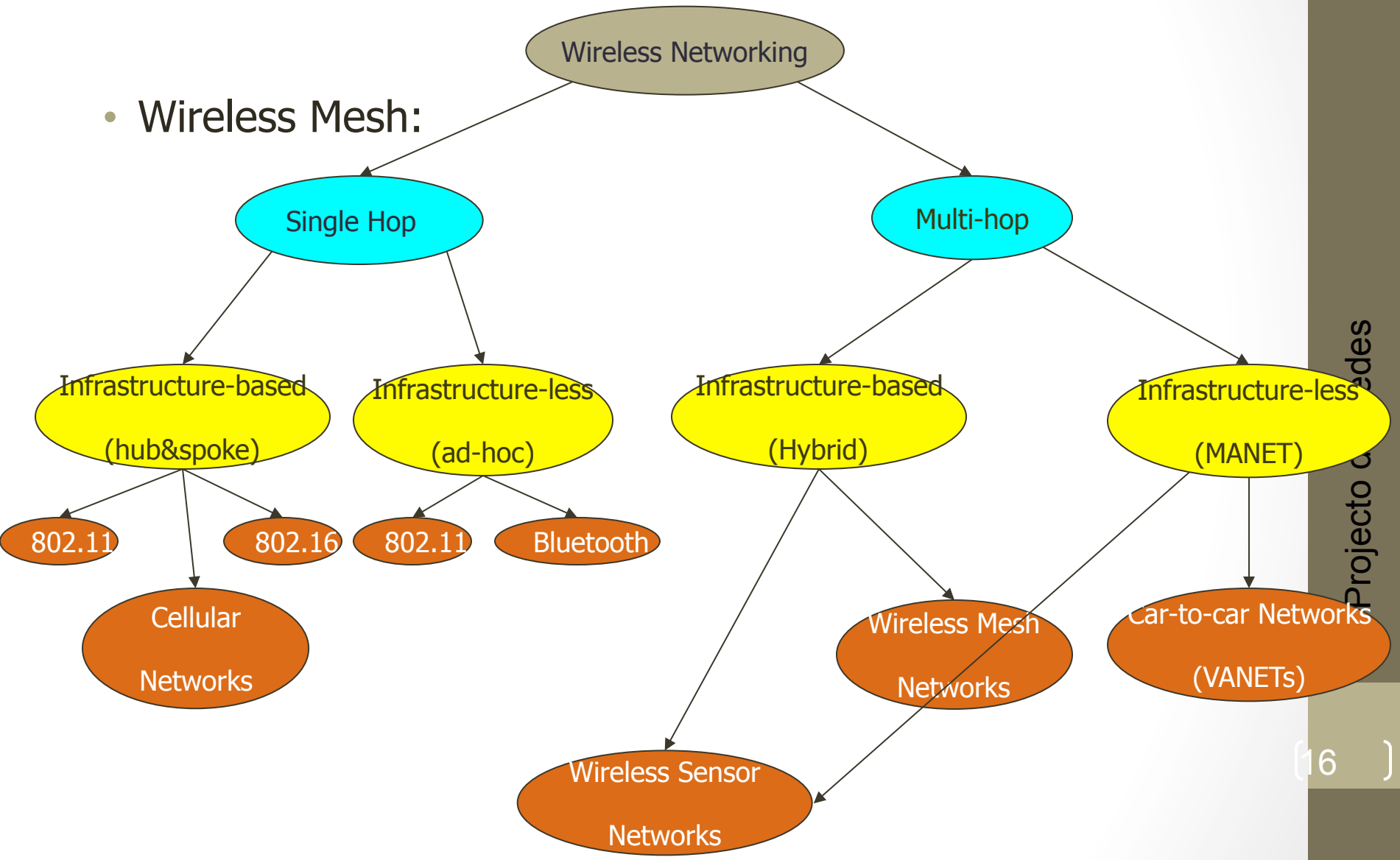
- Wireless Mesh



Novas tecnologias wireless:

- 802.11n:
- Baseia-se no uso de MIMO (multiple input multiple output).
  - Suporta até 4x4 MIMO.
- É compatível com as normas a/b/g.
  - No entanto podem surgir problemas porque os dispositivos compatíveis com a norma n podem não detectar a presença dos dispositivos a/b/g
- Operam nos 2.4 GHz e nos 5 GHz
- Usa 1 ou 2 canais não sobrepostos
- Velocidades de transmissão em ambiente indoor:
  - 100-200 Mbps
  - Máx. 600 Mbps
  - Suporta agregação de frames
    - Versão optimizada do protocolo IEEE 802.11e

- Wireless Mesh:



Fim

Objectivos:

- Segurança em redes 802.11

Introdução

- Ataques ao meio físico de transmissão
- O protocolo WEP
  - Objectivos
  - Funcionamento
- Ataques que se baseiam na reutilização da chave de cifra
  - O problema da cifras de verman
  - Ataques por dicionário
- Ataques que se baseiam no uso de mensagens de autenticação
  - Modificação de mensagens de autenticação
  - Injecção de mensagens
  - Spoofing de mensagens de autenticação
- Novos mecanismos de segurança
  - 802.11i
  - WPA
  - 802.1x

Ataques ao meio físico de transmissão

- Interferência no canal rádio.
  - Normalmente conduz a ataques de DoS.
  - Nos casos menos graves, conduz a perturbações na largura de banda da ligação.

Segurança em redes 802.11

- Introdução
  - As grandes questões de segurança que se colocam às redes sem fios.
    - Como impedir pessoas estranhas à minha rede de:
      - Terem acesso ao dados da minha rede.
      - Modificarem os dados da minha rede.
      - Usarem os recursos da minha rede.
  - Quando as redes 802.11 foram especificadas a resposta a estas perguntas baseava-se no uso do protocolo WEP(wired equivalence protocol).

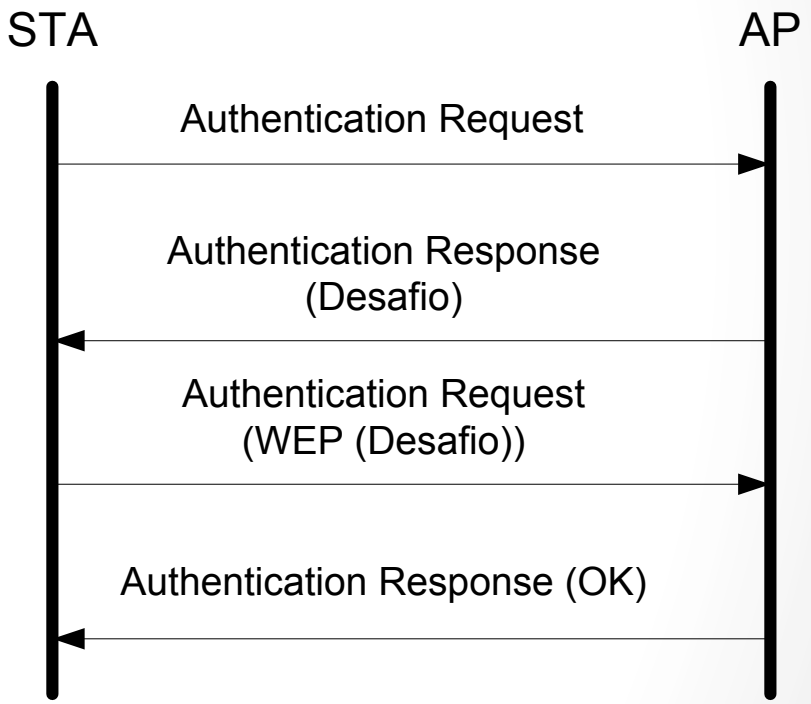
Segurança em redes 802.11

- Os objectivos de segurança do WEP:
  - Confidencialidade
  - Controlo de acessos
  - Integridade

- Infelizmente nenhum deles é garantido!

Segurança em redes 802.11

- Funcionamento:
  - Métodos de autenticação:
    - Open system Authentication (OSA): Não existe qualquer autenticação por parte das estações móveis. É usado em hotspots de acesso público.
    - Shared Key Authentication (SKA): Existe uma chave que é partilhada entre a estação móvel e o AP.



Segurança em redes 802.11

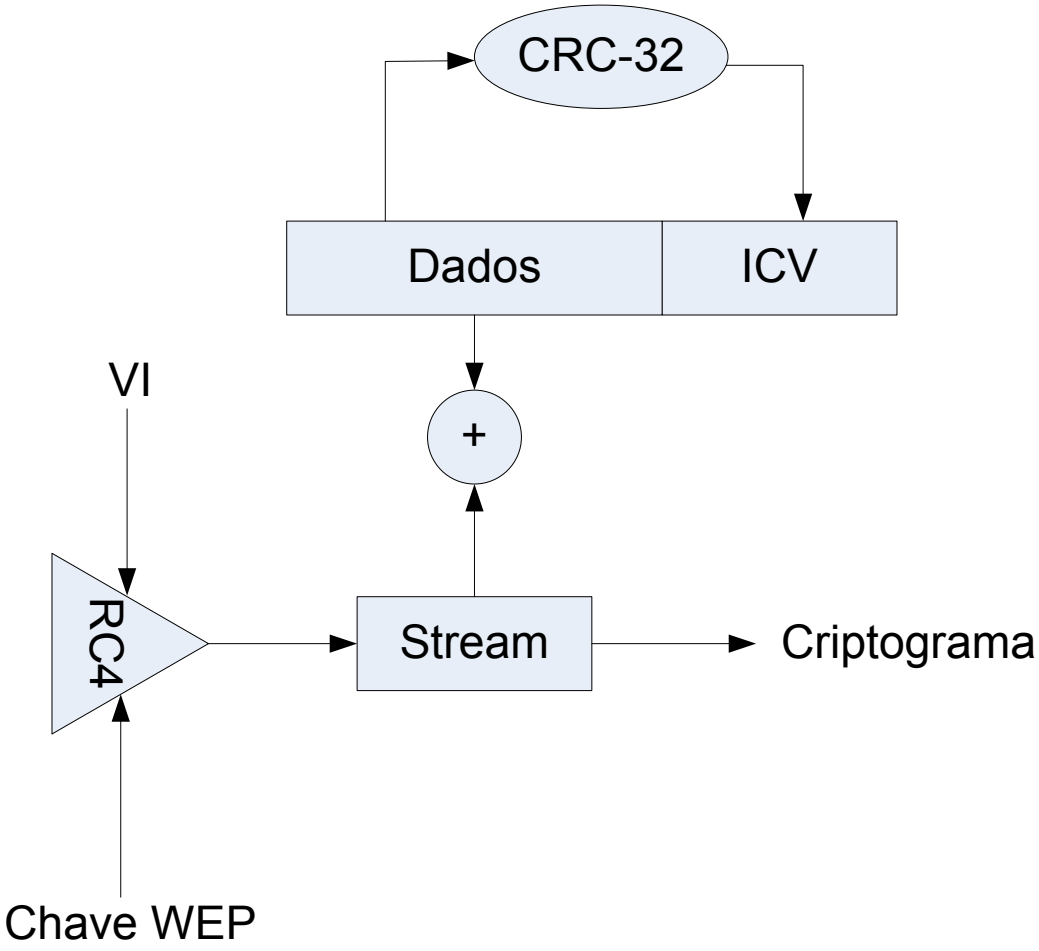
- Métodos de auntenticação:
  - Infelizmente a autenticação SKA é insegura
    - (SKA – Send Key to Attacker)
    - O atacante pode capturar as frames que transportam o desafio e a resposta ao desafio para mais tarde se autenticar.
    - Existem outras formas complementares para efectuar a autenticação:
      - Ocultar o SSID
      - Anunciar SSID falsos (cloacked SSID)
      - Listas de MAC address admitidos
    - Nenhuma resolve o problema!

Segurança em redes 802.11

- Confidencialidade e controlo de integridade
  - Os mecanismos que o WEP dispõe aplicam-se ao tráfego unicast.
  - Apenas as frames de dados e de Authentication Request são protegidas pelo WEP. (Rogue APs).
  - O WEP suporta-se num mecanismo criptográfico de chave simétrica de stream (RC4).
  - As chaves podem ter 40 ou 104 bits.
  - É usado um vector de inicialização (VI).
  - O WEP não dispõe de qualquer mecanismo para efectuar a distribuição das chaves.
  - É usado o CRC-32 no controlo de integridade.
  - O controlo de integridade do WEP é diferente do controlo de integridade do 801.11(campo FCS).

Segurança em redes 802.11

- WEP - Diagrama



Segurança em redes 802.11

- Problemas do WEP (parte 1):
  - As cifras de stream são difíceis de usar correctamente.
    - O problema “two-time pad”
    - Nunca se deve cifrar duas mensagens com a mesma chave. Porquê?

Segurança em redes 802.11

- Problemas do WEP (parte 1): (cont)
  - Nunca se deve cifrar duas mensagens com a mesma chave. Porquê?
    - Supondo que as mensagens P1 e P2 são cifradas com a mesma chave K, então:
      - C1=P1 xor K e C2=P2 xor K,
      - então C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2
    - Se conhecer parte de uma mensagem consegue determinar parte da outra.
    - Normalmente o conhecimento do XOR de duas mensagens é suficiente para determinar as duas mensagens.

Segurança em redes 802.11

- Problemas do WEP (parte 1): (cont)
  - O que o WEP faz:
    - A chave de stream depende do VI e da chave WEP.
    - A chave WEP, geralmente, não muda.
    - Assim, a qualidade da stream depende do VI.
    - O VI tem 24 bits (aproximadamente 16M de combinações).
      - Repete-se ao fim de algum tempo.
      - O atacante consegue determinar colisões porque o VI é transmitido em texto claro.
      - A grande maioria das cartas inicia o VI a zero em antes de cada associação.

Segurança em redes 802.11

- Problemas do WEP (parte 1): (cont)
  - Devido à repetição dos VI é possível a um atacante:
    - Construir um dicionário com todas as streams usadas, indexadas pelo valor do VI.
    - Descobrir qual a chave WEP usadas.
      - Airsnort, WEPcrack – 5 a 10 Milhões de pacotes.
        - » Modo passivo
        - » Modo activo

Segurança em redes 802.11

- Problemas do WEP (parte 2):
  - Mecanismo de controlo de integridade
    - O CRC-32 é usado para detectar erros introduzidos por deficiências do canal de tx.
    - O CRC-32 não pode ser usado para assegurar controlo de integridade criptográfico.
    - O CRC-32 é linear.

$$CRC32(x \oplus \Delta x) = CRC32(X) - CRC32(\Delta x)$$

  - Portanto se x for a mensagem original e Δx uma sua alteração, para efectuar a alteração correcta do ICV contido no criptograma é suficiente:

$$ICV_{NOVO} = ICV_{original} \oplus CRC32(\Delta x)$$

Segurança em redes 802.11

- Soluções:
  - Usar como chave RC4 a síntese do VI com a chave WEP, em vez da concatenação destes valores.
  - Vantagem: não se pode determinar quais os criptogramas fracos.
  - Desvantagem: continua a ser possível construir dicionários de chaves.

Segurança em redes 802.11

- Evolução:
  - Especificação do 802.11i
    - Mecanismo de cifra e de controlo de integridade AES.
    - Problema: O equipamento em uso é incompatível com a norma 802.11i
      - Necessidades de processamento
      - Problemas de consumo de energia
    - Especificação de uma solução de compromisso que:
      - Aumente a segurança
      - Garanta a compatibilidade com os equipamentos em uso
        - WPA – Wi-Fi Protected Access

Segurança em redes 802.11

- WPA – Wi-Fi Protected Access
  - Cada trama é cifrada com uma chave WEP diferente.
    - Não é possível construir dicionários de chaves, nem mesmo quando se usa a mesma PSK várias vezes.
    - O controlo de integridade do WEP é complementado com um mecanismo de controlo de integridade criptográfico mais abrangente.
    - O controlo de integridade deixa de ser por trama e contempla a ordem das tramas.
    - A autenticação também foi melhorada sendo possível a autenticação mútua.
  - O WPA assenta em dois pilares:
    - 802.1x – autenticação e confidencialidade das tramas.
    - TKIP – autenticação entre interlocutores e distribuição das chaves.

Segurança em redes 802.11

- TKIP (Temporal Key Integrity Protocol)
  - Usa um VI de 48bits, designado por TSC que varia de forma bem definida e que permite o controlo de ordem na recepção.
  - Produz chaves WEP diferentes para cada trama e em cada sentido da comunicação.
  - Exclui as chaves fracas do RC4.
  - Usa um valor de controlo de integridade criptográfico (MIC), calculado para cada trama e abrangendo os cabeçalhos das tramas.
  - Permite o accionamento de contra-medidas caso seja detectado valores de MIC errados.

Segurança em redes 802.11

- TKIP (Temporal Key Integrity Protocol)
  - Usa 3 chaves:
    - Uma chave para garantir a confidencialidade (temporal Key) de 128bits
    - Duas de 64bits para o controlo de integridade (MIC)

Segurança em redes 802.11

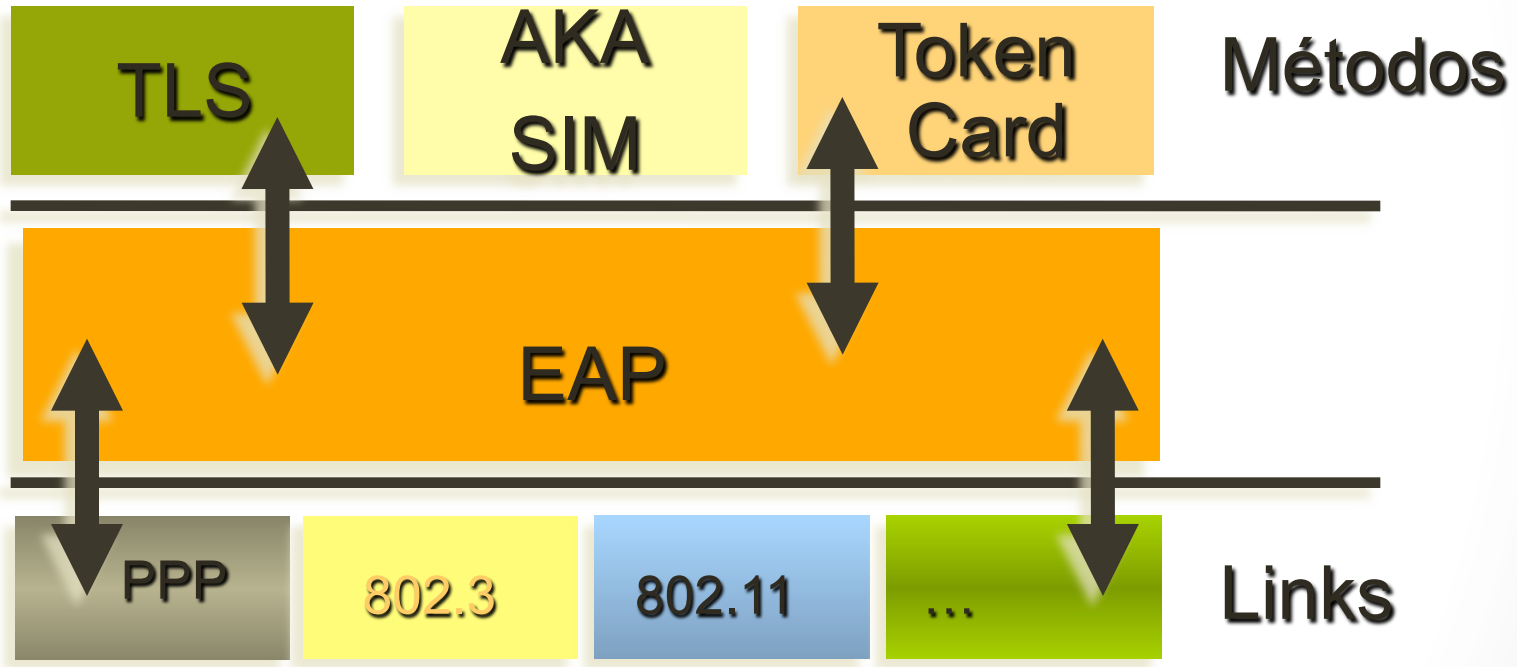
- WPA – Modos de funcionamento:
  - WPA: É usado 802.1x em conjunto com um servidor de autenticação.
  - WPA-PSK: São usadas chaves partilhadas e é dispensado o uso de servidores de autenticação.

Segurança em redes 802.11

- 802.1x
  - Objectivos:
    - Garantir a autenticação.
    - Distribuir as chaves de sessão.
  - Interlocutores:
    - Suplicant
    - Autenticador
    - Servidor de autenticação
  - Portos:
    - Cada porto 802.1x é constituído por dois portos:
      - Porto controlado
      - Porto não controlado

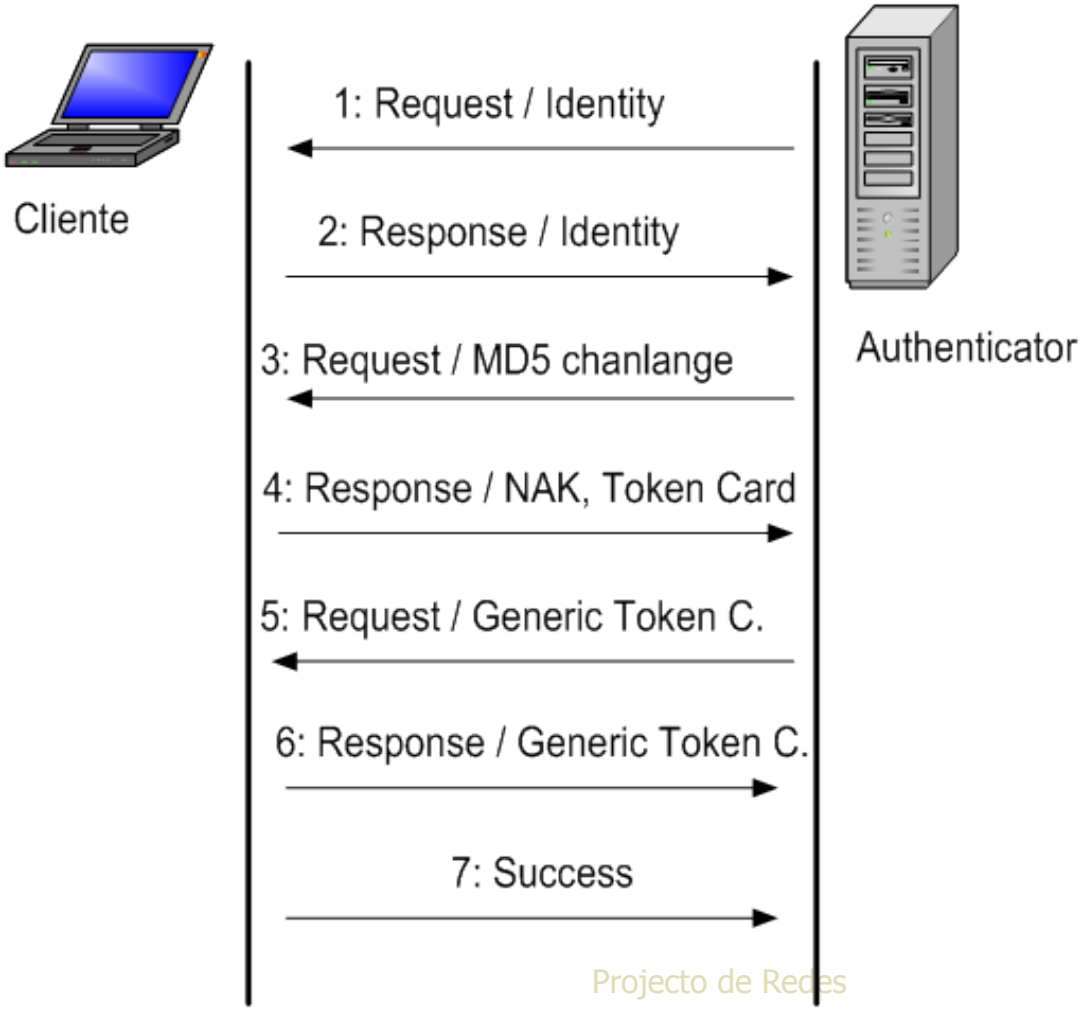
Segurança em redes 802.11

802.1x Aquitectura:



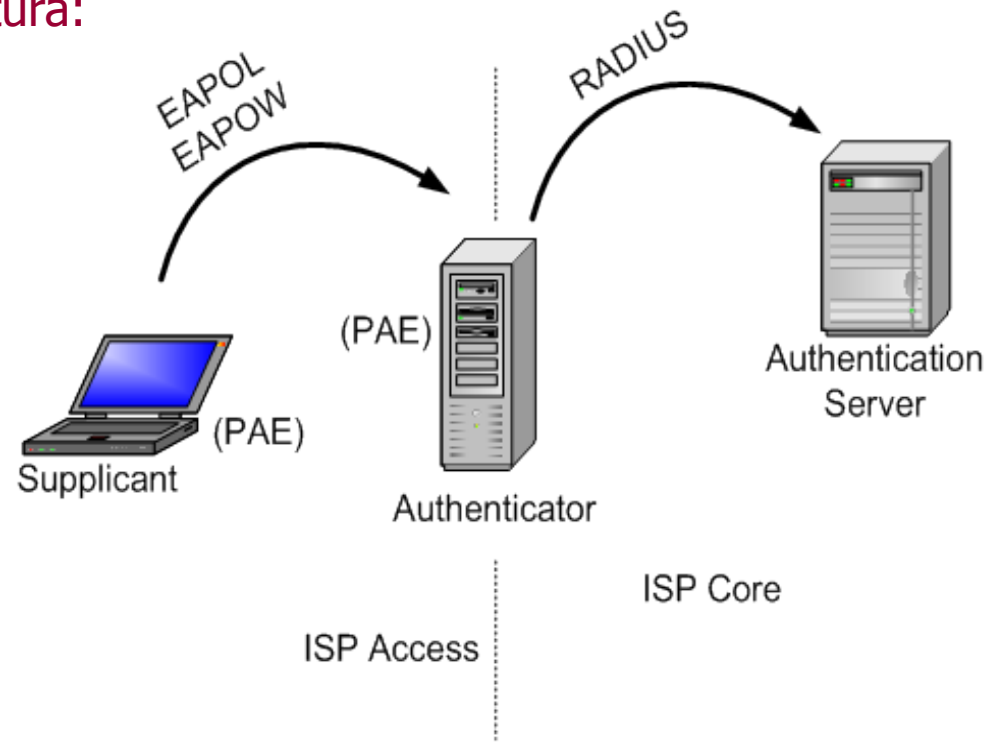
Segurança em redes 802.11

- 802.1x Troca de mensagens:



Segurança em redes 802.11

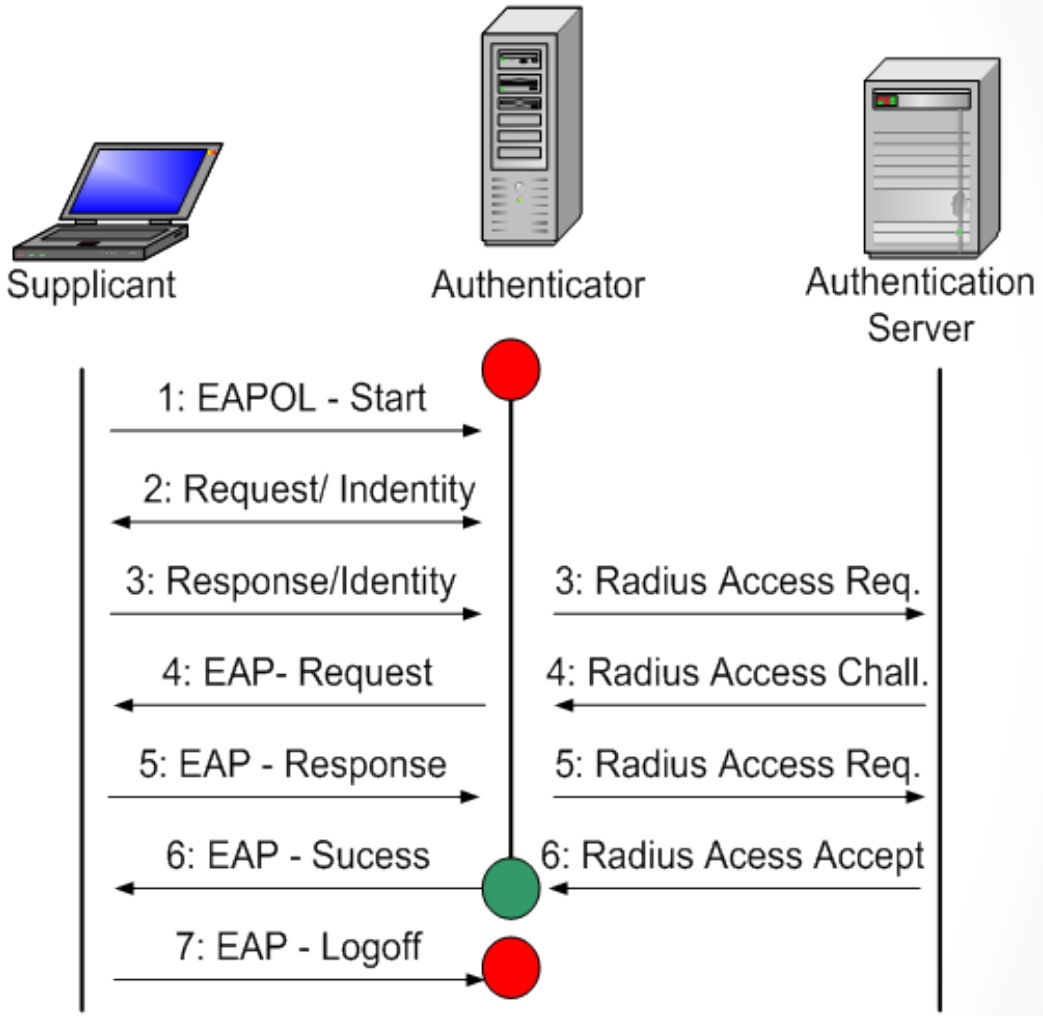
802.1x Arquitectura:



PAE - Port Athentication Authorities
EAPOL(W) – EAP over LAN (Wireless)

Segurança em redes 802.11

- 802.1x Arquitectura:



Segurança em redes 802.11

- RADIUS:
  - RADIUS – Remote Authentication Dial-In User Service
  - Protocolo usado para AAA de utilizadores remotos e de conexões Dial-In.
  - O RADIUS utiliza UDP para troca de mensagens entre o NAS (Cliente RADIUS) e o Servidor RADIUS.
  - O Servidor e o NAS possuem uma chave secreta partilhada que não é enviada pela rede e permite a codificação da password do utilizador, cifrada com MD5.

Segurança em redes 802.11

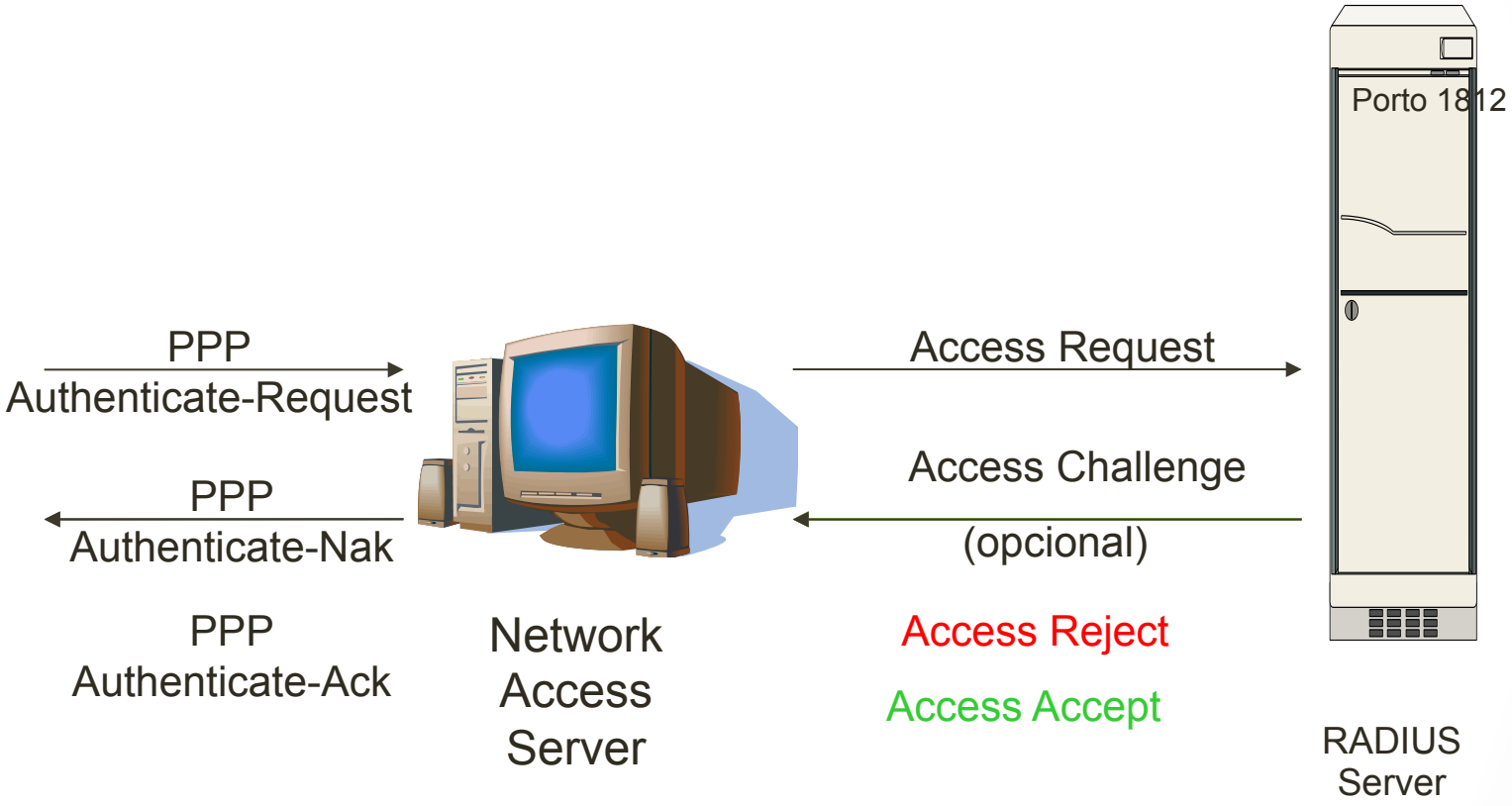
- RADIUS:

  - O RADIUS é bastante usado em redes que necessitem aplicar: Authentication, Autorization and Accounting.
  - Desvantagens:
    - Não suporta roaming de forma eficiente;
    - Os campos dos pacotes não são codificados
    - Os vários clientes Radius poderem ter a mesma chave
    - O Radius permite PAP, protocolo essencialmente académico pois o grau de segurança é nulo.
    - Não suporta serviços com qualidade de serviço de forma eficiente.

  - Devido a estes factores o protocolo RADIUS deixou de ser desenvolvido a partir de 1998, para se canalizarem todos os recursos no desenvolvimento de um melhor protocolo de AAA, o DIAMETER.

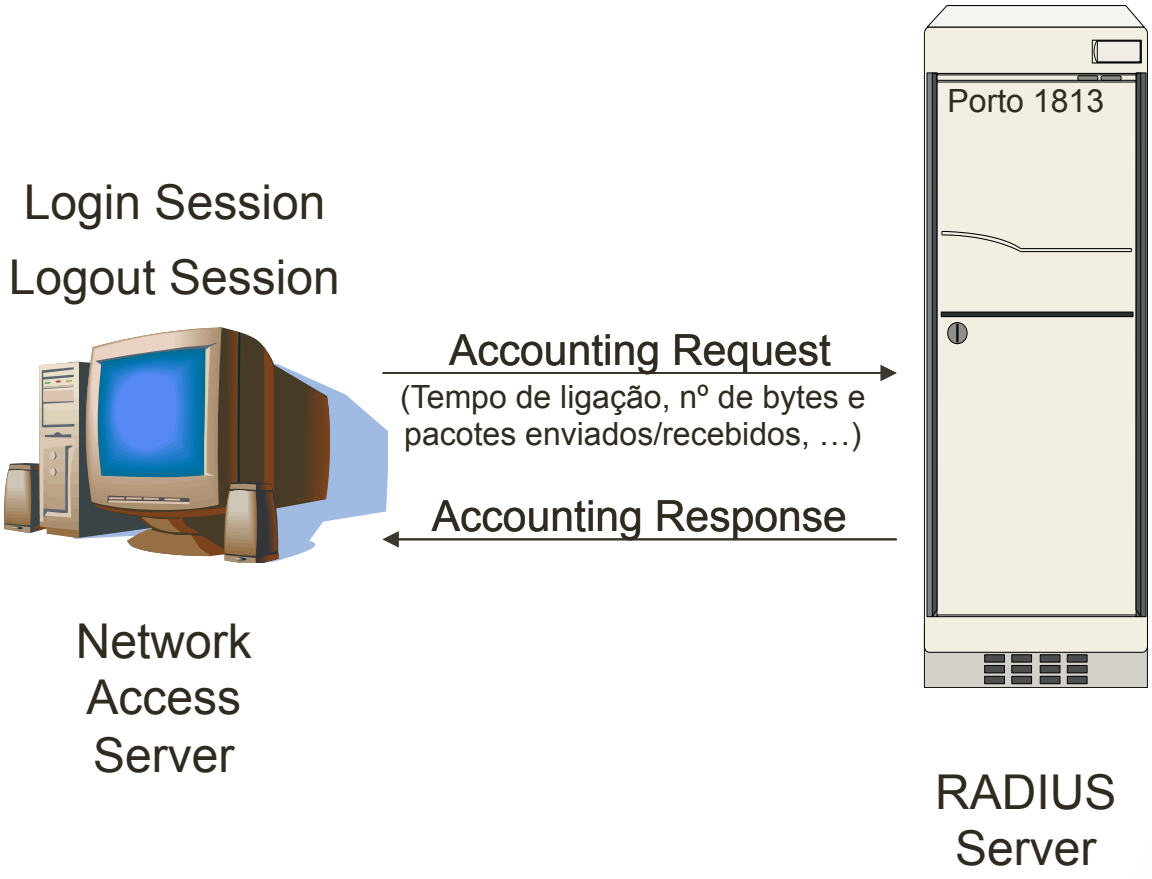
Segurança em redes 802.11

RADIUS:



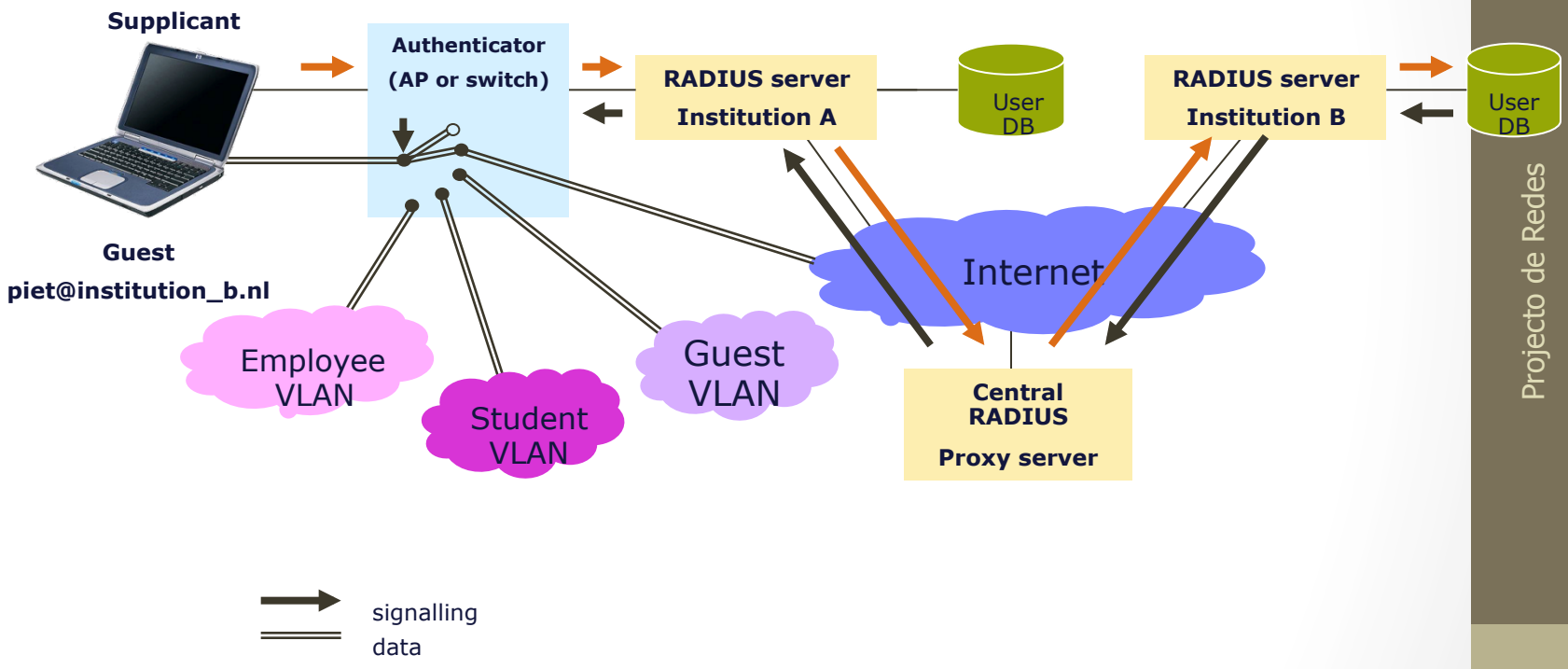
Segurança em redes 802.11

- RADIUS Accounting:



Segurança em redes 802.11

RADIUS - exemplo:



Segurança em redes 802.11

- 802.1x
- Métodos Standard
  - EAP-MD5
  - EAP-TLS
  - Protected EAP
    - PEAP
    - EAP-TTLS
- Métodos proprietários
  - LEAP
  - ...

Segurança em redes 802.11

- EAP-MD5:
  - Os clientes são autenticados através do HASH MD5 da password.
  - Simples de implementar
  - Inseguro:
    - É fácil determinar a identidade e o HASH MD5 dos clientes.
    - Não valida a identidade do ponto autenticador.

Segurança em redes 802.11

- LEAP (cisco):
  - Os clientes e o autenticador são autenticados através do HASH MD5 da password.
  - Evita ataques do tipo Man-in-de-middle.
  - Simples de implementar quando os clientes e o autenticador são cisco.
  - Inseguro:
  - As identidade e a HASH da password continuam vulneráveis a ataques de sniffing + ataque de dicionário.

Segurança em redes 802.11

- EAP-TLS:
  - Usa um servidor RADIUS.
  - A identidade dos clientes e dos autenticadores é assegurada através do uso de certificados.
  - A comunicação entre os clientes e o autenticador é transportada por um túnel TLS.
  - Muito resistente a ataques do tipo Man-in-the –middle.
  - A identidade do cliente continua exposta.
  - Fácil de implementar em ambientes Windows.

Segurança em redes 802.11

- EAP Tunneled TLS (EAP-TTLS) e Protected EAP (PEAP):
  - Os servidores de autenticação são autenticados através de certificados.
  - Os clientes podem usar vários métodos de autenticação.
  - Tão seguro como o anterior no entanto o uso incorrecto de passwords pode comprometer estes mecanismos.

Segurança em redes 802.11

EAP – Tipos de autenticação (resumo)

Topic	EAP MD5	LEAP	EAP TLS	PEAP	EAP TTLS
Security Solution	Standards-based	Proprietary (CISCO)	Standards-based	Standards-based	Standards-based
Certificates – Client	No	n/a	Yes	No	No
Certificates – Server	No	n/a	Yes	Yes	Yes
Credential Security	None	Weak	Strong	Strong	Strong
Supported Authentication Databases	Requires clear-text database	Active Directory, NT Domains	Active Directory, LDAP etc.	Active Directory, NT Domain, Token Systems, SQL, LDAP etc.	Active Directory, LDAP, SQL, plain password files, Token Systems etc.
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes	Yes