Universidade do Porto

Faculdade de Engenharia

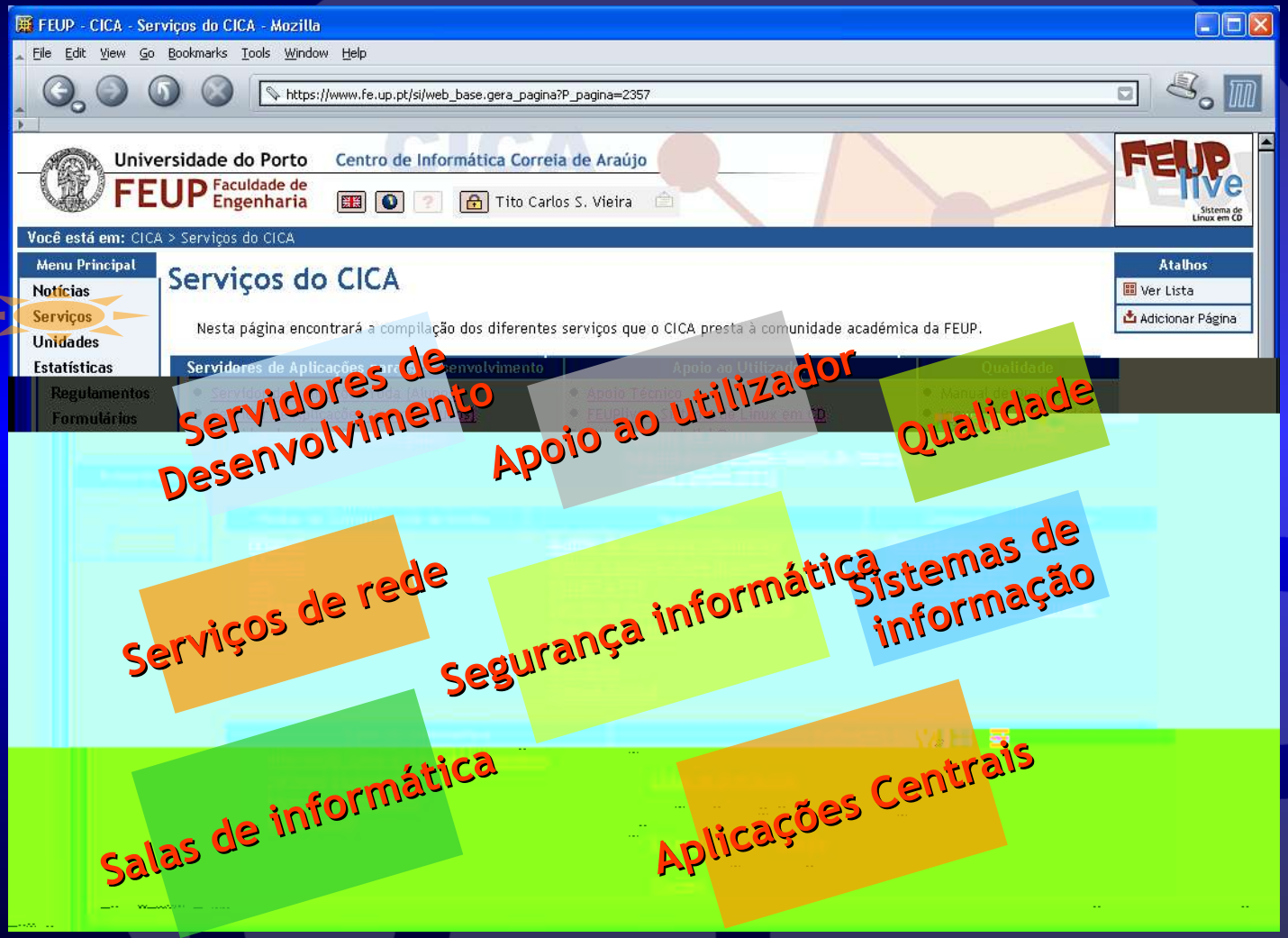
FEUP

Rede Wireless da FEUP

Fernando Romão

Universidade do Porto
Faculdade de Engenharia
FEUP

Serviços do CICA



Universidade do Porto
Faculdade de Engenharia
FEUP

CICA - Alguns nºs relativos a 2004

- Rede de dados
  - 6000 pontos de acesso
    - 3000 tomadas activas
    - 259 switches
    - 20 routers
  - Wi-Fi
    - 135 Access Points
    - Integração com e-U
- Sistemas
  - 100 servidores (Linux / Windows)
  - 22.082 – utilizadores nos sistemas
- 250.000 páginas/dia acesso ao SiFEUP

- 41 salas de informática
  - 654 PCs
  - 40 impressoras
  - 117.482 acessos aos sistemas em Nov 2004
  - 2.430.831 páginas impressas
- Apoio aos utilizadores
  - 8598 pedidos de apoio
  - 1975 e-mail recebidos
  - 10.128 carregamentos de quota impressão
  - 939 configurações DHCP
  - 1116 configurações WiFi
  - 262 PCs nos Serviços Centrais

Universidade do Porto
Faculdade de Engenharia
FEUP

CICA - UIRC

- IPv6 disponível em todas as tomadas de rede. (VLAN protocol based)
- Gestão de largura de banda
- Colaborou no projecto de video conferencia da FEUP
- Projecto VoIP (a decorrer)
- Desenvolvimento de aplicações de gestão de rede
- …

Universidade do Porto
Faculdade de Engenharia
FEUP

Projecto e-U

- Objectivo:
  - Incentivar e facilitar a produção, acesso e partilha de conhecimento
- Envolve serviços, conteúdos, aplicações e redes de comunicações móveis
- Financiado por fundos comunitários

Requisitos do e-U

- Cobrir áreas comuns, laboratórios, anfiteatros e salas de aula e de estudo
- SSID e-U (não anunciado)
- SSID guest-e-U (anunciado) para apenas identificar o hotspot
- Autenticação 802.1x, com PEAP e/ou TTLS
- Com roaming para os visitantes
- Rede com IP públicos para os visitantes
- Recolha de dados estatísticos

Universidade do Porto
Faculdade de Engenharia
FEUP

Requisitos da rede wireless

- Confidencialidade dos dados
- Controle de acesso
- Registo dos acessos
- Suporte aos vários modelos de placas
- Suporte aos vários SO
- Roaming Nacional
- Gestão da infra-estrutura
- Distinção de utilizadores (VLAN)

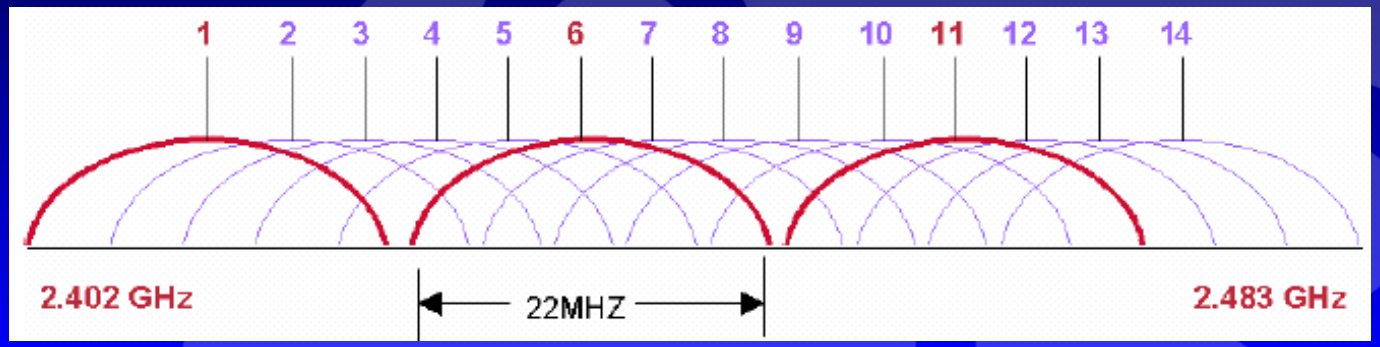
Dificuldades

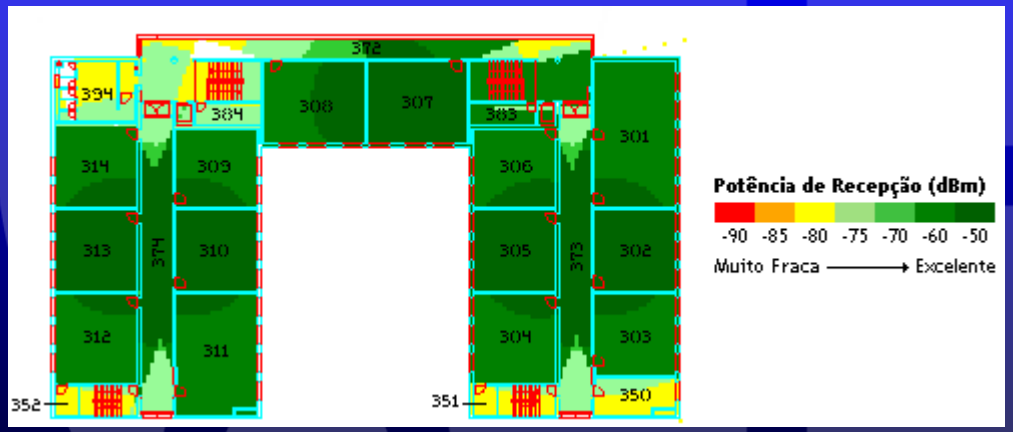
- Gestão Rádio
- Controle de Acesso
- Logs
- Segurança dos dados transmitidos
- IP Spoofing
- Gestão de equipamentos
- Rogue APs

Site Survey

- Estudo prévio do local a cobrir
- AP colocado no local previsto
- Leitura de medidas com Yellow Jacket
- Alterações do local do AP se necessário
- Canais 1,6,11

- Wireless Mapping
  - Criação dos mapas de cobertura


1
2
3
4
5
6
7
8
9
10
11
12
13
14
2.402 GHz
22MHZ
2.483 GHz


372
394
384
308
307
383
301
314
309
306
313
310
374
305
373
302
312
311
304
303
352
351
350
Potência de Recepção (dBm)
-90 -85 -80 -75 -70 -60 -50
Muito Fraca
Excelente

Controle de Acesso - Requisitos

- Compatível com actual sistema
- Seguro
- Distinção de tipos de utilizador
- Escalável
- Registo de acessos

- Opções
  - Registo MAC Address + WEP
  - Portal Web + RADIUS
  - VPN
  - 802.1x + TKIP +RADIUS
    - EAP-TLS
    - EAP-TTLS
    - PEAP
    - EAP-LEAP

MAC Address + WEP

- Necessidade de registo dos visitantes
- MAC spoofing
- Não identifica o tipo de utilizador
- Não é escalável
- WEP não é seguro, facilmente quebrável
- ...

- WEP
  - Atribuição manual, não é escalável
  - Tamanho da chave é curto 40 bits ou 104.
  - Vector de inicialização enviado em claro

- TKIP
  - WEP “melhorado”
  - Surgiu para corrigir as fraquezas do WEP

Portal Web + RADIUS

- Confidencialidade das credenciais comprometida na hierarquia RADIUS
- Credibilidade dos certificados auto assinados do portal
- Não evita o IP spoofing e MAC Spoofing
- Não é escalável
- Não distingue utilizadores
- Dados não são encriptados no meio rádio
- Funciona com qualquer placa
- Solução específica por fabricante

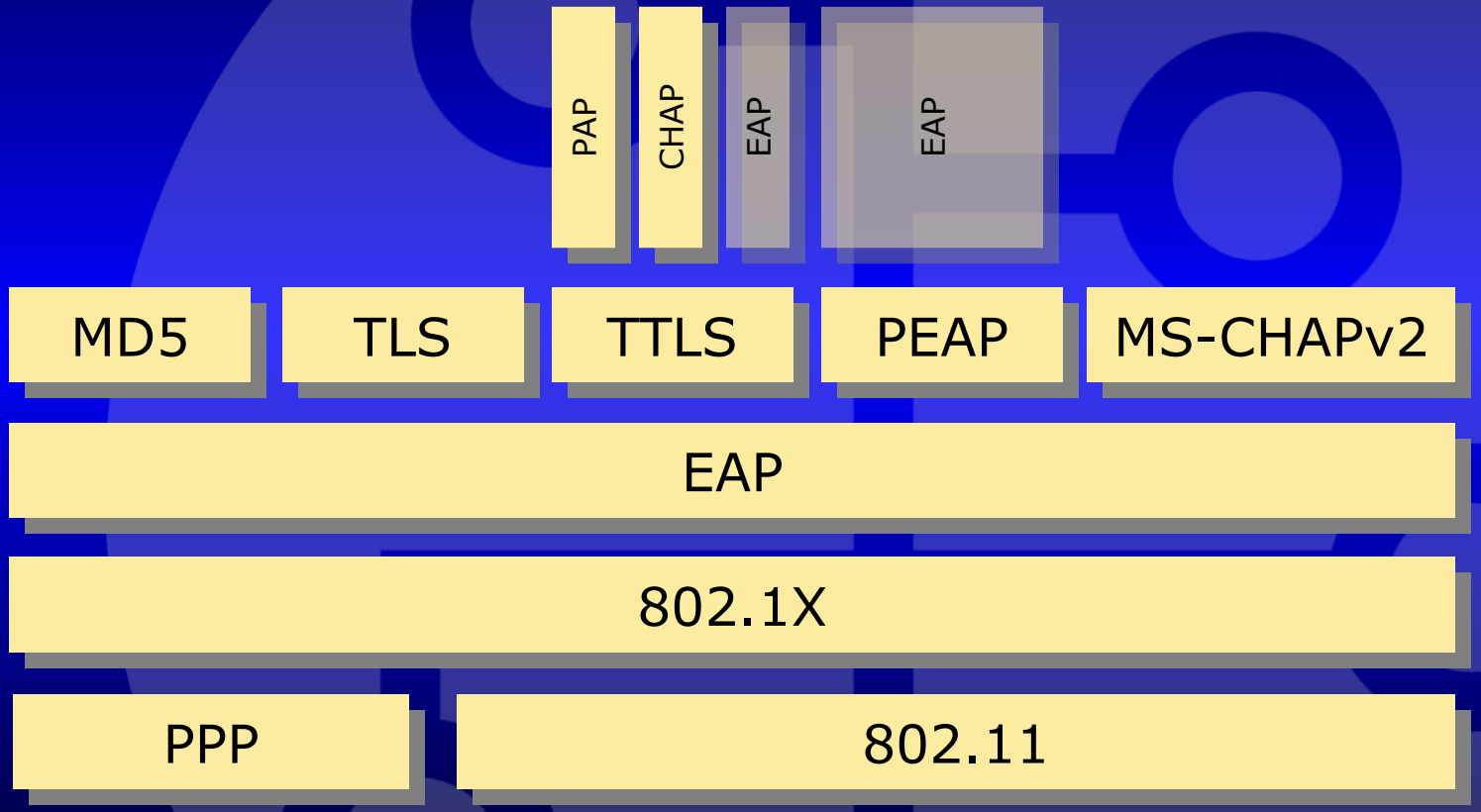
VPN

- Solução segura mas...
- Concentradores VPN são caros
- O cliente precisa de software
- Soluções específicas por fabricante
- Solução não é transparente para visitantes
- Pouco escalável

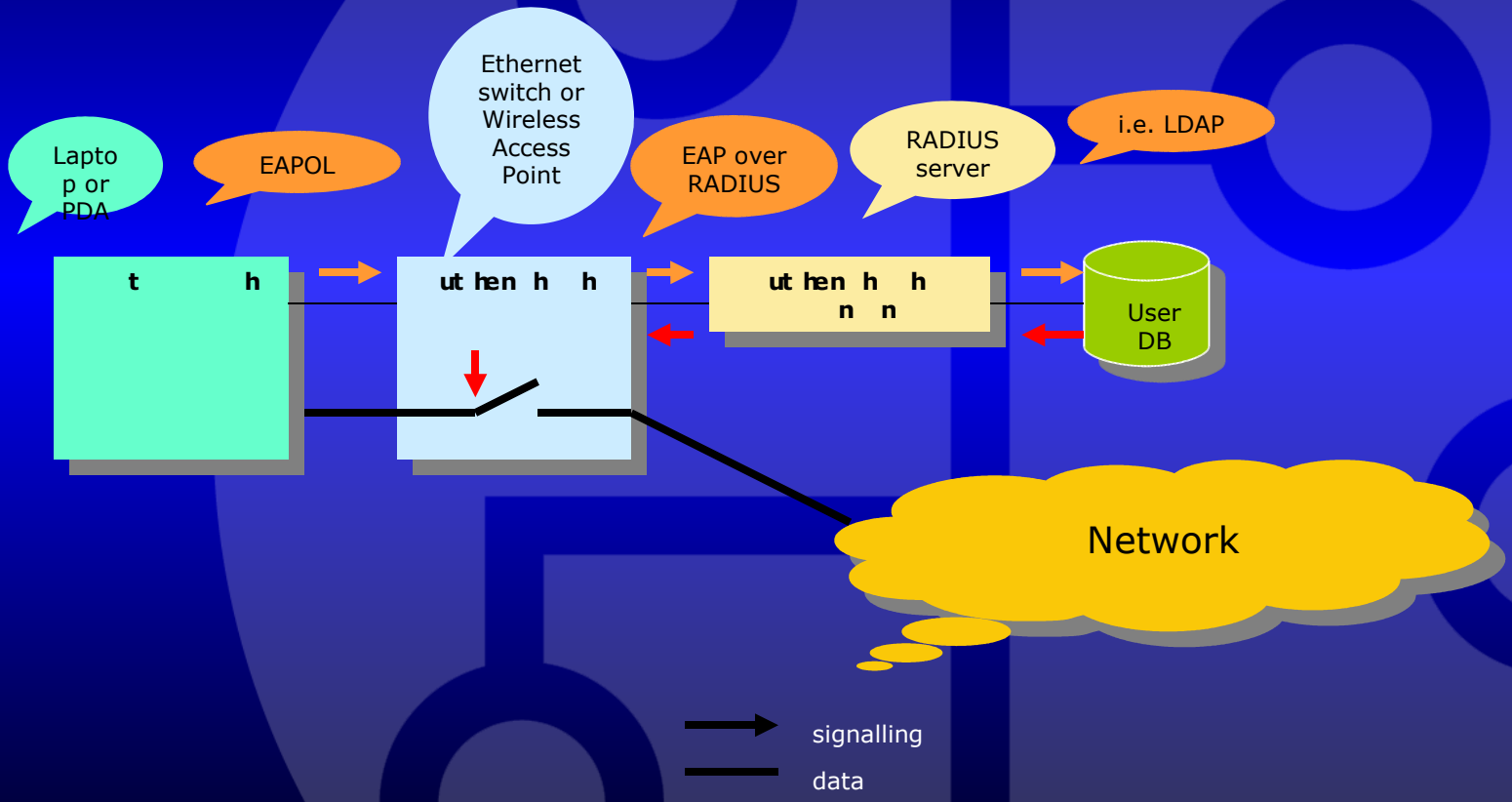
802.1x + TKIP

- EAP
- Autenticação RADIUS
  - Accounting
  - Escalável – Proxy RADIUS
  - Distinção de utilizadores
  - Integração no sistema de gestão de utilizadores
- Segurança das credenciais entre o cliente e o respectivo servidor RADIUS (depende do método de autenticação)
- Segurança dos dados na interface rádio (depende do método de autenticação)

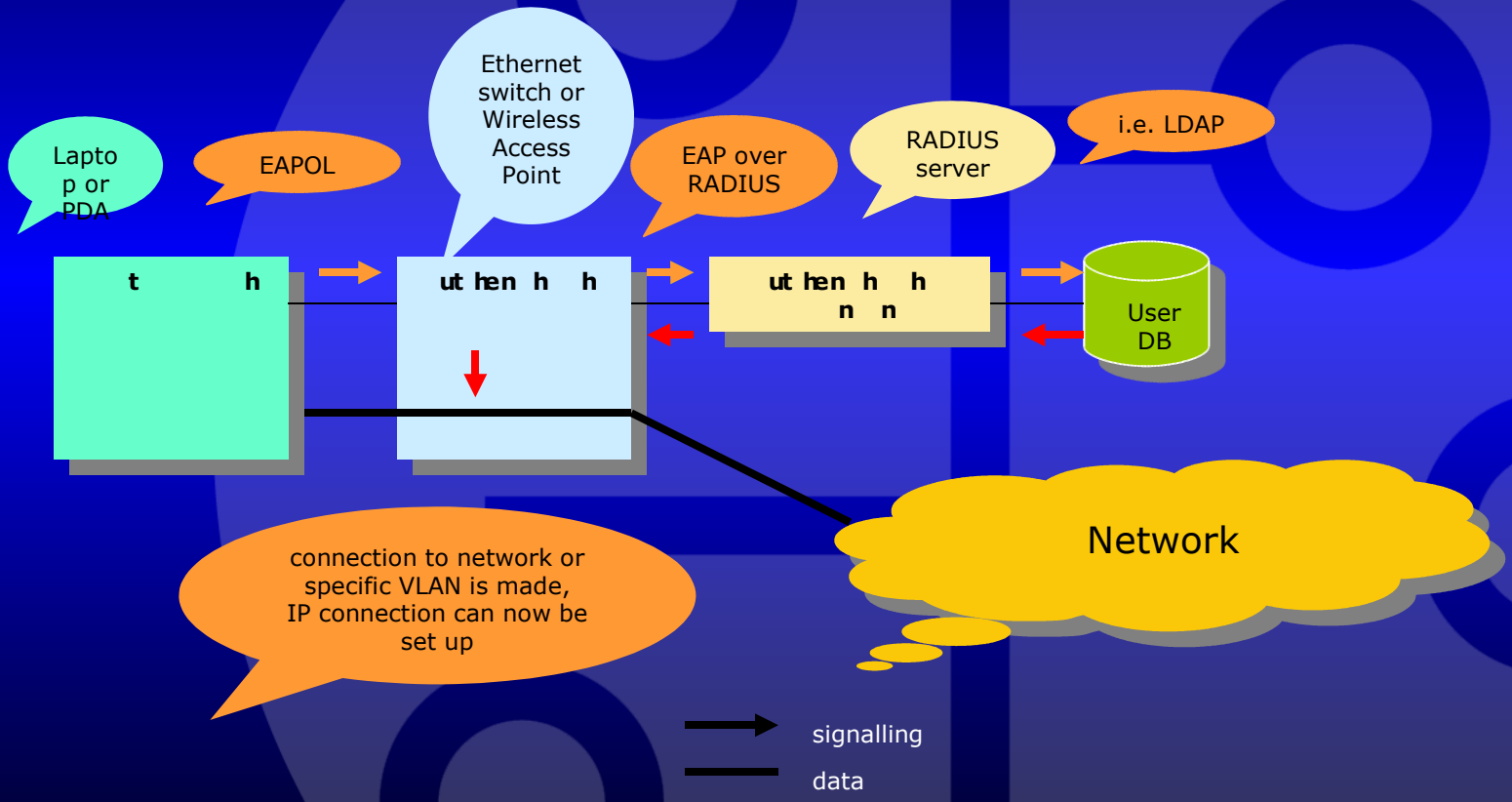
- EAP
  - Permite a troca de mensagens entre dispositivos que usam um determinado protocolo de autenticação
  - Usa a camada de ligação de dados, não necessita de endereço IP
  - Usado em redes com fios e sem fios (ex. 802.3 e 802.11)
  - Precisa de usar um protocolo de autenticação
  - Nível de segurança depende do método usado


PAP
CHAP
EAP
EAP
MD5
TLS
TTLS
PEAP
MS-CHAPv2
EAP
802.1X
PPP
802.11

Como funciona o EAP



Como funciona o EAP



- Metodos de autenticação no EAP
  - EAP-MD5
  - LEAP (Lightweight EAP)
  - EAP-TLS (Transport Layer Security)
  - EAP-TTLS (Tunnelled TLS)
  - PEAP (Protected EAP)

- EAP-MD5
  - O MD5 não oferece segurança. É “leve“ e fácil de implementar mas apenas autentica o pacote, marcando-o univocamente.
  - Na hierarquia RADIUS as credenciais poderiam ficar comprometidas
  - Não suporta chaves dinâmicas
  - É usado em soluções *wired* porque o equipamento liga-se directamente á porta do equipamento

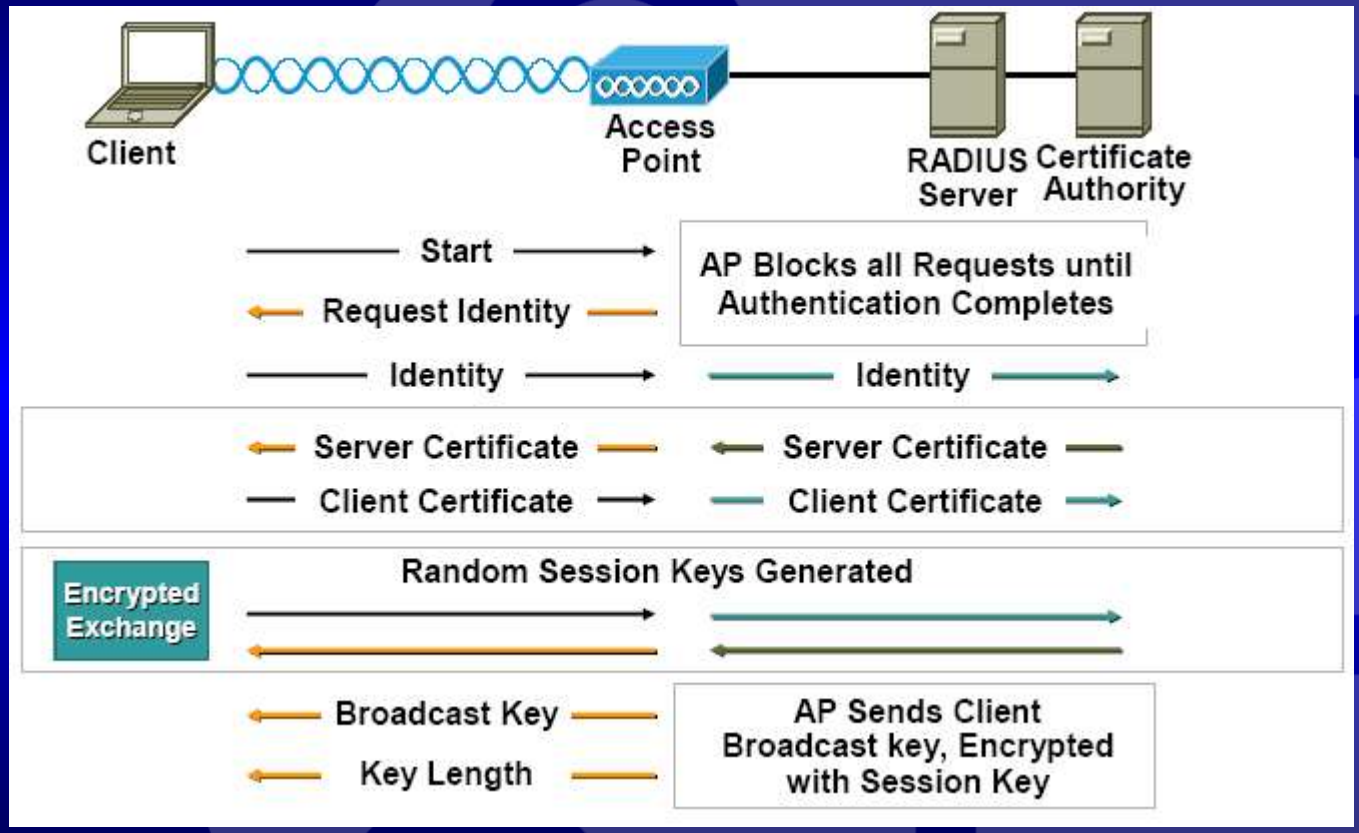
LEAP

- Não é considerado seguro
- É proprietário da Cisco.
- Nem todos os suplicantes suportam

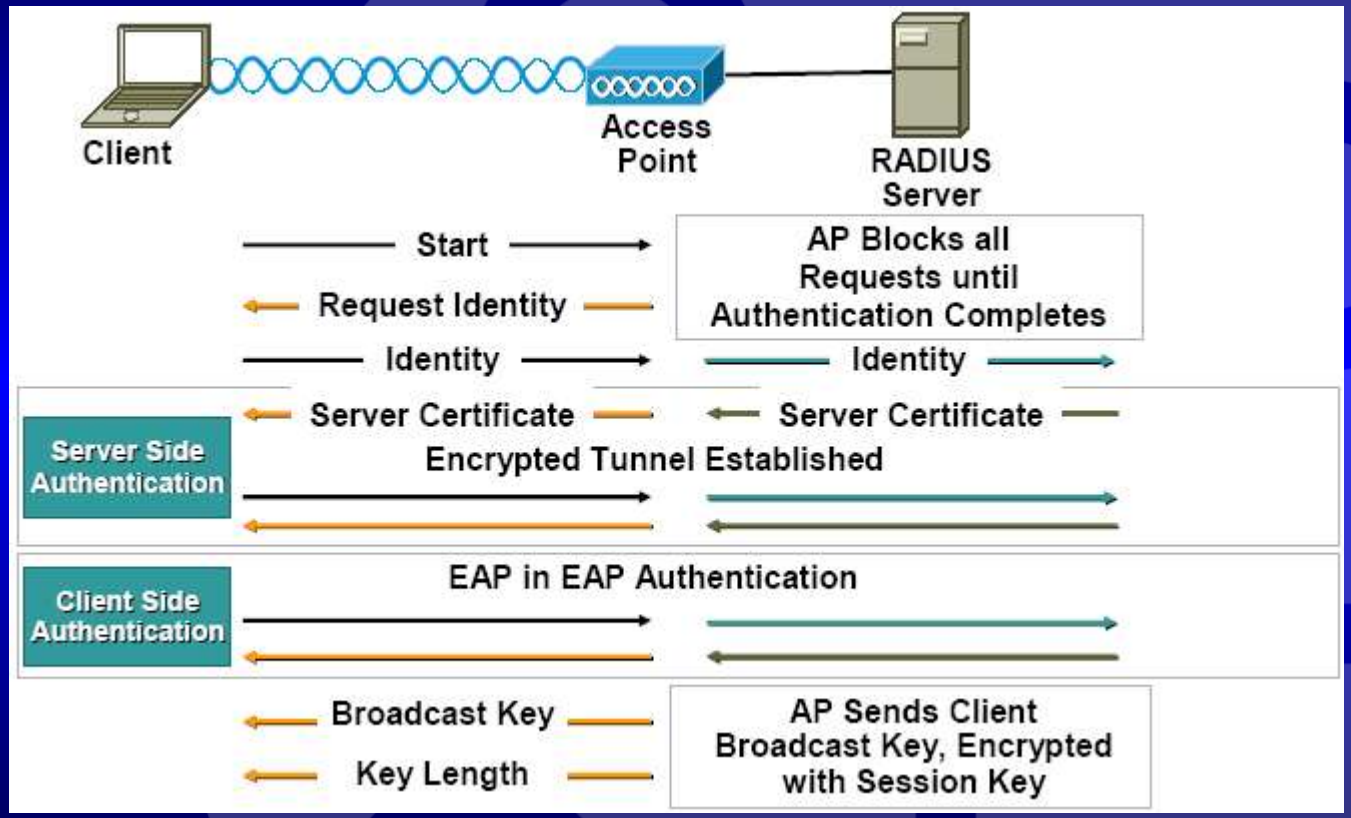
EAP-TLS

- Bom mecanismo de autenticação
- É necessário previamente ter uma infra-estrutura PKI.
- Faz atribuição dinâmica de chaves (WEP)
- Com base em certificados digitais é autenticado o servidor e o cliente

EAP-TLS


Client
Access Point
RADIUS Server
Certificate Authority
Start
Request Identity
Identity
AP Blocks all Requests until Authentication Completes
Identity
Server Certificate
Server Certificate
Client Certificate
Client Certificate
Encrypted Exchange
Random Session Keys Generated
Broadcast Key
Key Length
AP Sends Client Broadcast key, Encrypted with Session Key

PEAP

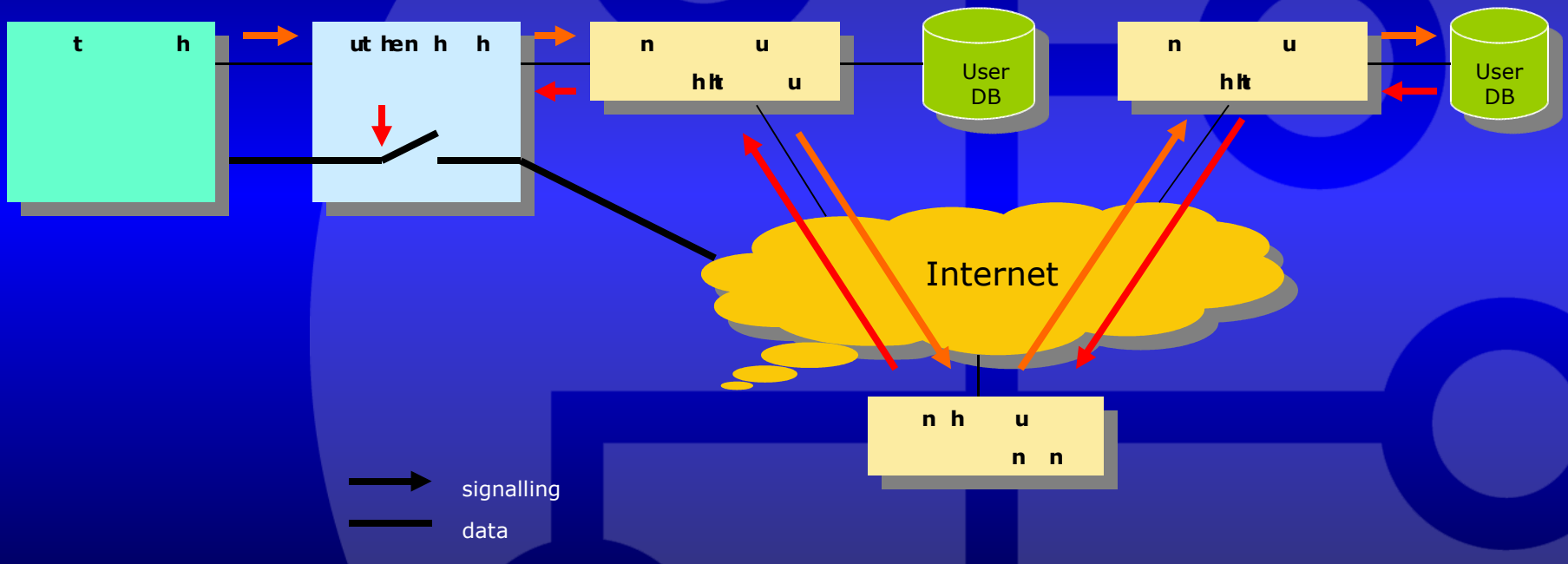

Client
Access Point
RADIUS Server
Start
AP Blocks all Requests until Authentication Completes
Request Identity
Identity
Identity
Server Certificate
Server Certificate
Server Side Authentication
Encrypted Tunnel Established
Client Side Authentication
EAP in EAP Authentication
Broadcast Key
AP Sends Client Broadcast Key, Encrypted with Session Key
Key Length

Universidade do Porto
Faculdade de Engenharia
FEUP

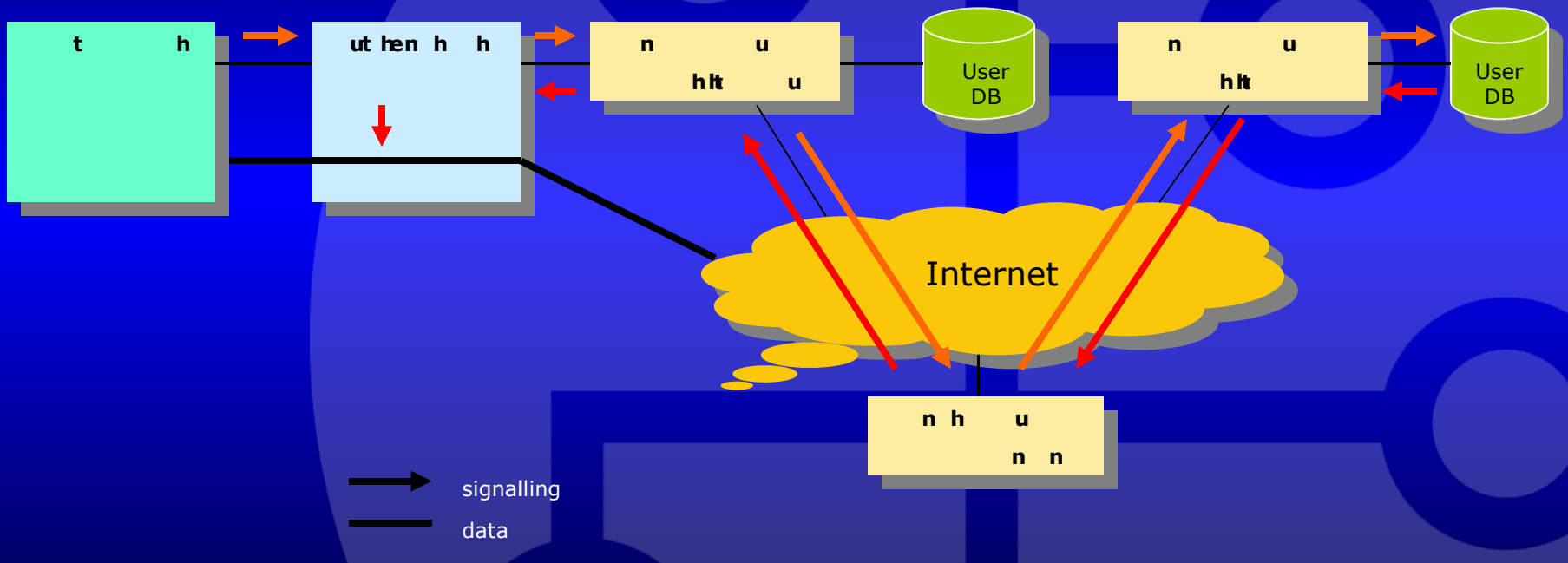
Distinção de utilizadores

- RADIUS
  - Atributos RADIUS
  - Proxy
  - Realm @fe.up.pt
- VLAN assigment
- 4 Redes Virtuais
  - utilizadores da FEUP- rede interna
  - utilizadores em roaming - DMZ
  - rede guest, sem gateway
  - gestão do equipamento

Proxy-RADIUS



Proxy-RADIUS



Universidade do Porto
Faculdade de Engenharia
FEUP

Equipamento

135 APs

- 107 Cisco 1100
- 24 Cisco 1200
- 4 Cisco 1130 (brevemente)

Router Cisco 3845

HP (serviço RADIUS)

IP Spoofing

```
ip dhcp pool RedeInterna
   network 172.30.0.0 255.255.0.0
   netbios-name-server 193.136.28.44 193.136.28.43
   dns-server 193.136.28.10 193.136.28.9
   domain-name wireless-int.fe.up.pt
   default-router 172.30.255.253
   lease 0 1
   update arp
   accounting ACCT-GROUP
!
ip dhcp pool RedeWIFIExterna
   network 193.137.154.0 255.255.255.0
   dns-server 193.137.55.20 193.137.55.21
   domain-name wireless-ext.fe.up.pt
   default-router 193.137.154.254
   lease 0 0 10
   update arp
   accounting ACCT-GROUP
```

Web Login

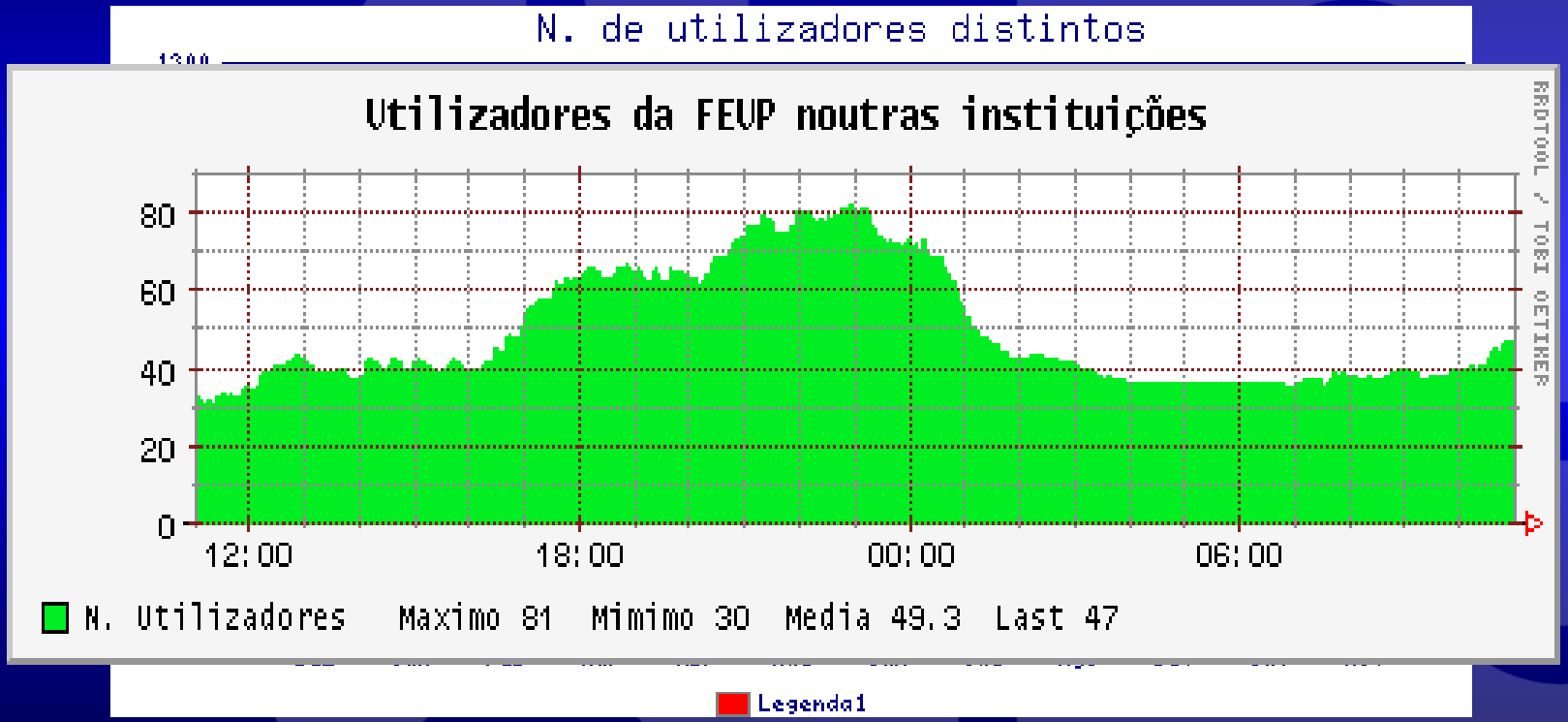
- Portal Web
- Apenas para conferências
- Não existe segurança na transmissão dos dados
- http e https

Estatísticas

- Base de dados
- Daemon recolhe dados da BD periodicamente e produz os gráficos
- Gráficos

Universidade do Porto
Faculdade de Engenharia
FEUP

Estatísticas



802.11i

- Concluído em Junho de 2004
- TKIP
- *Counter Mode with CBC-MAC Protocol (CCMP) –AES como algoritmo de encriptação*
- 802.1x
- Gestão e distribuição de chaves

Universidade do Porto
Faculdade de Engenharia
FEUP

www.fe.up.pt/wireless