Dilemas do serviço de rede sem fios

Jornadas FCCN 2023

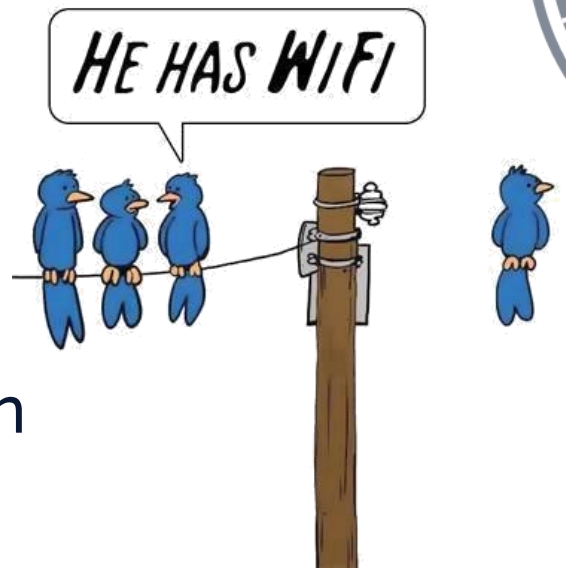
Utilizadores

Expectativas dos utilizadores

- Toda a conectividade é essencial

- Em todos os locais dos edifícios/campus
  - Equivalente a estar ligado por cabo a >100Mbit/s
  - Alto débito
  - Baixa latência
  - Sem interrupções

- Difícil corresponder mesmo com elevados r€cursos
  - Limitações da tecnologia (ex. canais)
  - Limitações dos dispositivos de utilizador

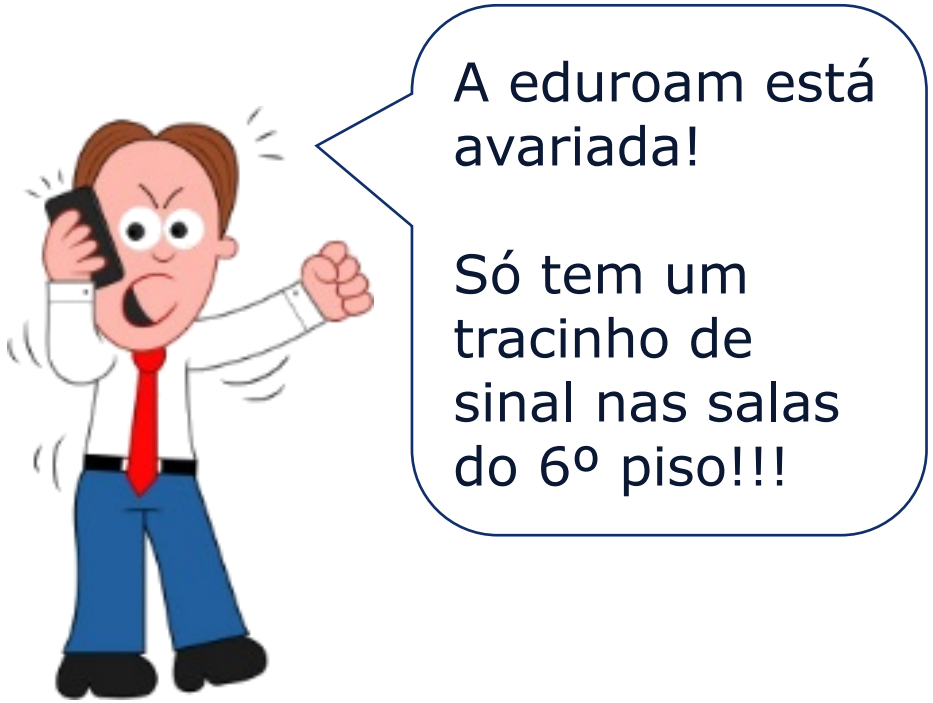


Desadaptação institucional

- Aulas de laboratório de “Química Orgânica” em anfiteatros? NÃO!
- Porquê remeter aulas de “Programação na Web” para um canto do edifício com conectividade marginal?
- Atribuição de salas tem de considerar a dependência que o uso terá da conectividade/WiFi!
  - Para Colibri/Zoom/Teams, existência de ligação Ethernet!

Reorganização de espaços

- Mudanças funcionais ou estruturais sem considerar impacto na conectividade
- Problema coloca-se após a mudança e o IT é que tem de solucionar!



Jornadas FCCN 2023

Hardware

Infraestruturas WiFi

- Requisitos elevados de potência por porta
  - Renovação forçada dos *switch* de agregação
- Incompatibilidade entre componentes de diferentes fabricantes
  - Dependência das condições do fabricante ao longo do tempo
  - Manutenção de N ecossistemas WiFi distintos
- Incompatibilidade entre componentes de diferentes gerações do fabricante
  - Suporta novos equipamentos com atualização de software
  - Com a atualização deixa de suportar os AP mais antigos
- Custos incomportáveis (ex. 1300€/AP *refurbished!*)
  - Entrega em (talvez) 6 meses ...

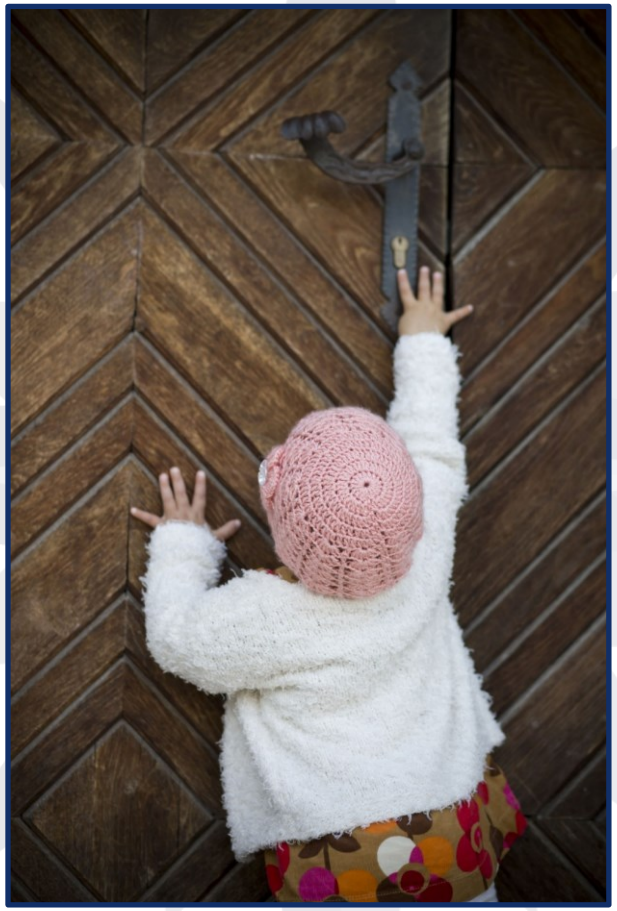
Dispositivos de utilizador

- Comportamentos inexplicáveis
  - Em condições idênticas um tem serviço o outro não
  - Um é instável e com baixo débito, o do lado consegue usar IPTV
  - Interferências com infraestrutura e outros (DHCP/Routing)

- Demasiado vocacionados para redes domésticas
  - Reiniciam DHCP no *handover* porque assumem que a rede IP poderá mudar
  - Noção de conectividade boa/má por validações nem sempre representativas
  - Abuso de comunicações de difusão inúteis na eduroam

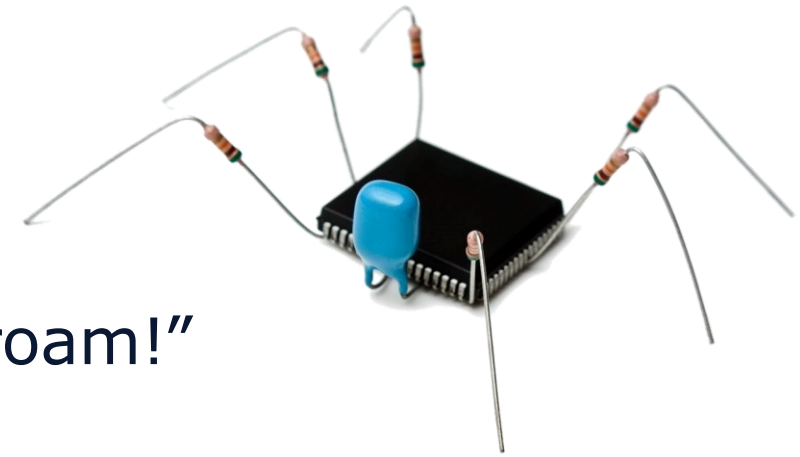
Jornadas FCCN 2023

Acesso



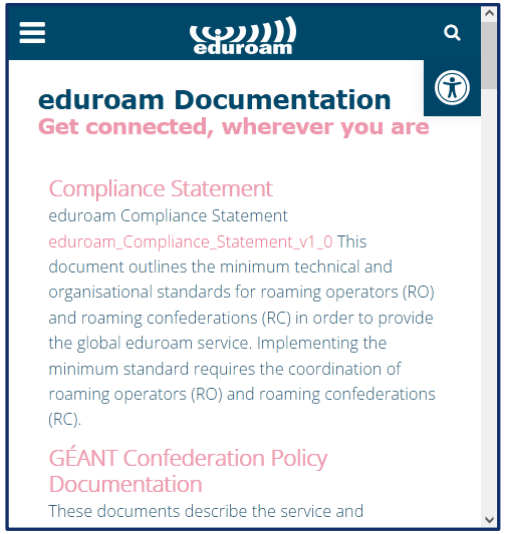
IoT sensores, atuadores e similares

- Adoção não informada de dispositivos incompatíveis
  - Projetos de I&D, iluminação, controlos de acesso, ecrãs interativos ...
- Dispositivos com implementações IP incompletas e com *bugs*
- Pressão para a criação de redes virtuais (SSID) extra caso-a-caso
  - Ingerível, sem qualquer controlo ou segurança
    - Chaves partilhadas e imutáveis
  - Degradação do serviço eduroam base
- "Funciona em casa, o problema é da eduroam!"



Garantia de serviço roaming

- Processo de validação continua tipícamente a circular em claro na Internet
  - Acabar com o RADIUS/UDP nos proxys nacionais ASAP!
- O *accounting* é para enviar ou não?
  - Origem da autenticação sem noção das contas em uso
  - Face ao RGPD em que condições se deve suprimir? (extra EU?)
- Atributos
  - Autenticação falha se alguns estiverem em falta
  - Os nossos utilizadores em roaming serão os prejudicados!
- Inaceitável a incerteza de serviço que ainda ocorre
  - Algum sistema deverá monitorizar simulando em todos os participantes o acesso de todos os restantes
- Há que auditar e excluir entidades que não cumprem o acordo!



Escalabilidade e partilha do recurso

- Todos os dispositivos na mesma rede L2?
  - Tráfego "ruído de fundo", tipicamente *multicast* consome imenso tempo de canal e baterias
- Alguns pólos com utilização corrente reduzida
  - Em picos de atividade necessitam milhares de acessos
  - Dedicar grandes blocos IP é ineficiente
- Partilha de segmentos L2 entre pólos
  - Propaga problemas locais
  - Propaga o "ruído de fundo"

Eventos e convidados

- Frequente aparecimento de contas de eventos de terceiros ligando-se localmente em *roaming*
  - Filtro atual:

    /^(visitante|digitalis|convidado|user|eduroam|microbiologia|guest.*|aluno|wireless|formacao.*|teste[^_e].*)@/i
- Usamos contas @IPL.LOCAL
  - Garantidamente inválidas para uso em roaming
  - Rede IP isolada
  - Serviços locais das escolas podem gerir
    - Criação, renovação, eliminação
    - Com limite de acessos simultâneos e validade
- Ponderamos usar o eVA.eduroam.pt !

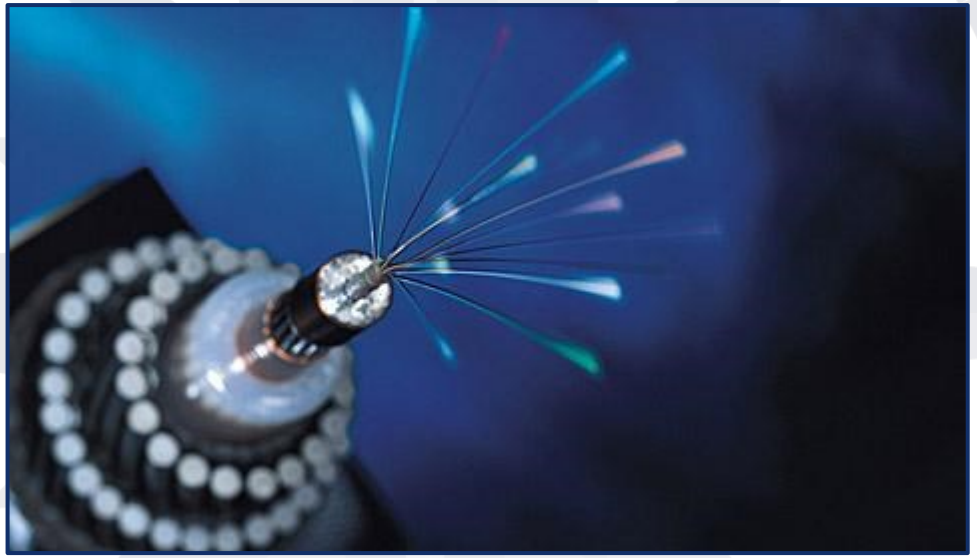
Garantia de serviço

- Interferências
  - entre sistemas oficiais distintos
  - utilizações exteriores aos pólos
  - de equipamentos não WiFi que partilham a banda
    - Bluetooth
    - Transmissão A/V (Drones, câmaras, etc.)
- Dispositivos “mal comportados”
- Sabotagem intencional (ex. “Deauther”)

- Que fique claro, o funcionamento sem licenciamento do WiFi não permite assumir quaisquer garantias de serviço!

Jornadas FCCN 2023

Conectividade



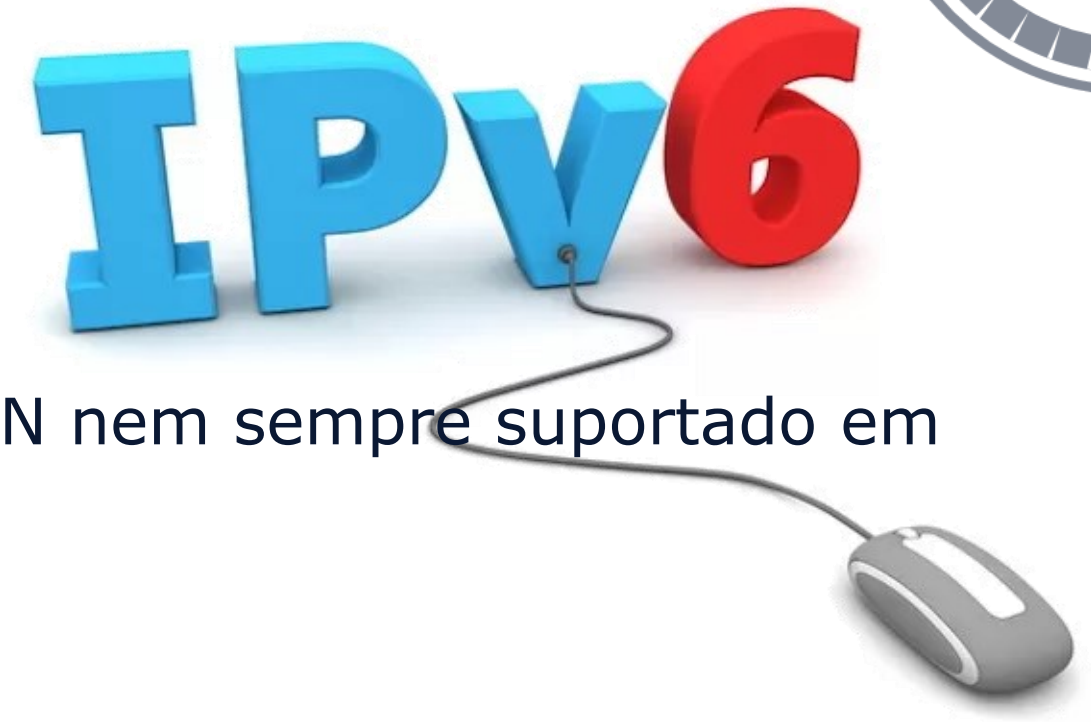
Tráfego centralizado

- Comunicações passam pelo controlador?
  - Trajeto ineficiente
  - Adequação de perfil e filtragem de "lixo"
  - Necessidade de garantir capacidade no trajeto entre APs e controlador
  - Controlador tem de ter a capacidade adequada
  - Latência acrescida
  - Complicações de fragmentação IP/MTU
- Tráfego comutado junto aos AP
  - Eficiente
  - Necessidade de replicar as redes IP usadas ou transportar as N VLAN até cada pólo/AP
  - As redes L2 a atravessar terão de conseguir lidar com os milhares de endereços MAC

NAT

- É a conectividade “normal” para utilizadores e dispositivos
- Contam com isso nas redes domésticas (e todas)
- Aplicações e protocolos de uso corrente já não contam com conectividade do exterior para dispositivos
  - É tudo iniciado do dispositivo para a *cloud*
- Manutenção de registos mínimos de conectividade
  - Necessidade do uso de formas de NAT “NETMAP” com registo de correspondências IP externo/interno
- Justifica a preferência do fornecimento de IP público?

IPv6 ou não?



- IPv6 depende muito de *multicast*
- WiFi com múltiplas redes SSID/VLAN nem sempre suportado em combinação com IPv6
- IPv6 perdeu a credibilidade!
  - O serviço "normal" de Internet continua a ser IPv4
  - IPv6 é visto pelos utilizadores como motivo para sub-desempenho
  - Para o IT é uma duplicação de sistemas e recursos a manter
- Justifica o esforço?

Partilha do serviço

- Partilha de credenciais
  - Comunidade não tem a noção que é equivalente a partilhar um cartão de identificação
  - Chegam a pedir suporte estando a usar credenciais de terceiros!

- Repetidores
  - Identificadas situações de utilizadores que introduzem dispositivos específicos para partilhar o serviço com terceiros
  - Versões recentes de Android realizam a partilha WiFi
    - Anteriormente só era suportada a partilha do LTE para o WiFi
  - Há técnicas que podem limitar estes abusos
    - Forçar a 1 o TTL do tráfego (todo ou parte) para os dispositivos
    - Podem limitar a conectividade do uso legítimo de WSL2

Anonimizações de rede (excessivas?)

- Paranoia da anonimização complica o serviço
  - Quase totalidade dos S.O. atuais acede por omissão com MACs aleatórios
- Alteração de MAC a cada religar consome recursos de rede
- Inviabiliza análise de problemas reportados
- No Bluetooth continuam a usar sempre o mesmo MAC
  - Quem quer e tem recursos para fazer negócio do *profiling* continuará!

Jornadas FCCN 2023

Que futuro para os serviços WiFi?

IPLNet POLITÉCNICO DE LISBOA fct Fundação para a Ciência e a Tecnologia FCCN

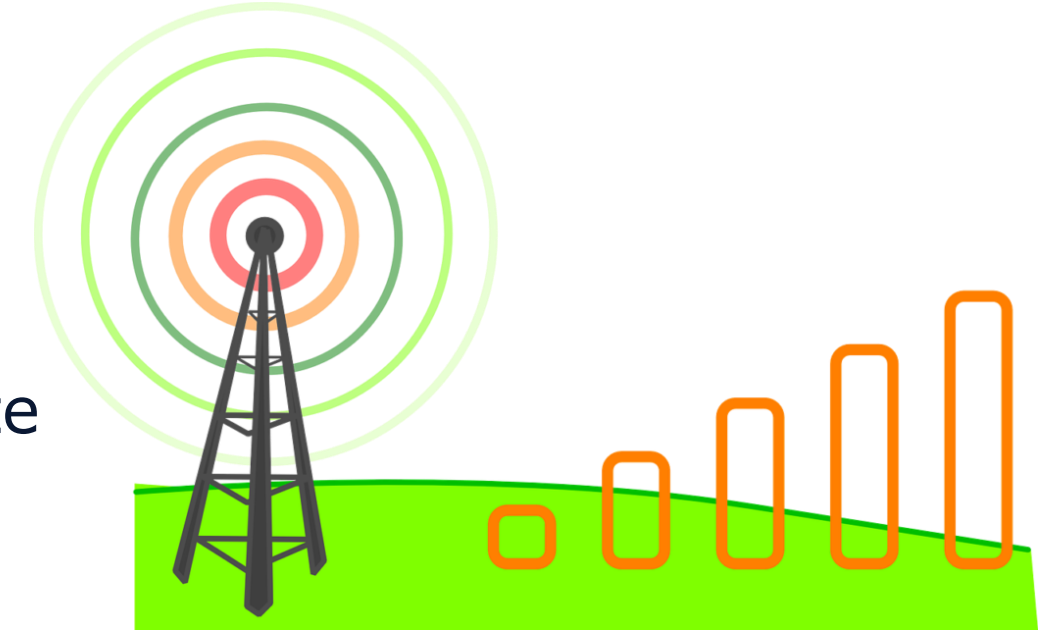
Evolução de continuidade

- Evolução para células por sala
  - Serviço primário em 5/6GHz
  - 2GHz para cobertura exterior e retro-compatibilidade

- Custos elevadíssimos
  - APs
  - Passagem de cablagens
  - Concentração de APs (switch/PoE)
  - Sistemas controladores
  - Instalação e manutenção

Talvez 5G (parece ser solução para tudo!)

- Haverá possibilidade de implementação de serviços privados?
  - 2 torres por campus!
- Infraestrutura e operação radicalmente distinta da atual
  - Atribuição de eSIM por utilizador/dispositivo?
- Dispositivos de utilizador necessitam suportar



Espaço a servir no IPL

- 6 pólos nos concelhos de Lisboa e Amadora
- Pólos de ESTC, ESTeSL, ISCAL e Presidência isolados
- O pólo Marvila/ISEL aloja o ISEL, ESD e Residência com um total de 13 edifícios
- No pólo de Benfica estão ESCS, ESELx, ESML e diversos serviços comuns e de ação social

POLITÉCNICO DE LISBOA

Infraestrutura hardware atual

- Equipamentos WiFi de 2 fabricantes distintos
- Usados 2 controladores de cada fabricante
  - Todo o tráfego vai aos controladores (centralizado)
- Ativos 293 pontos de acesso eduroam de geração WiFi5
- Um dos fabricantes permite a funcionalidade de controlador em qualquer dos seus routers físicos ou virtuais
  - O licenciamento de router virtual é perpétuo e de custo inferior a 1 AP
- A diferença média de custo por AP entre os dois fabricantes é de 15 vezes
  - Atribuímos ao mais barato o valor de produto (características/operação) de ¾ do mais caro

Infraestrutura RADIUS atual

- 7 servidores virtualizados sob Debian/VMWare
  - 2 Radsecproxy para RADSEC e proxy's nacionais
  - 4 FreeRADIUS para validação de acessos e registos
    - Repositório de credenciais e autorização em SQL
  - 1 FreeRADIUS para desenvolvimento e testes

- 8 VLANs atribuídas em função do perfil
  - Para escalabilidade e segurança
  - Roamers e visitantes no exterior do firewall
  - 4k endereços IP por VLAN
  - 2 usam endereços privados e NAT

Jornadas FCCN 2023

Obrigado!

Pedro Ribeiro
pribeiro@net.ipl.pt