UNIVERSIDADE PORTUCALENSE

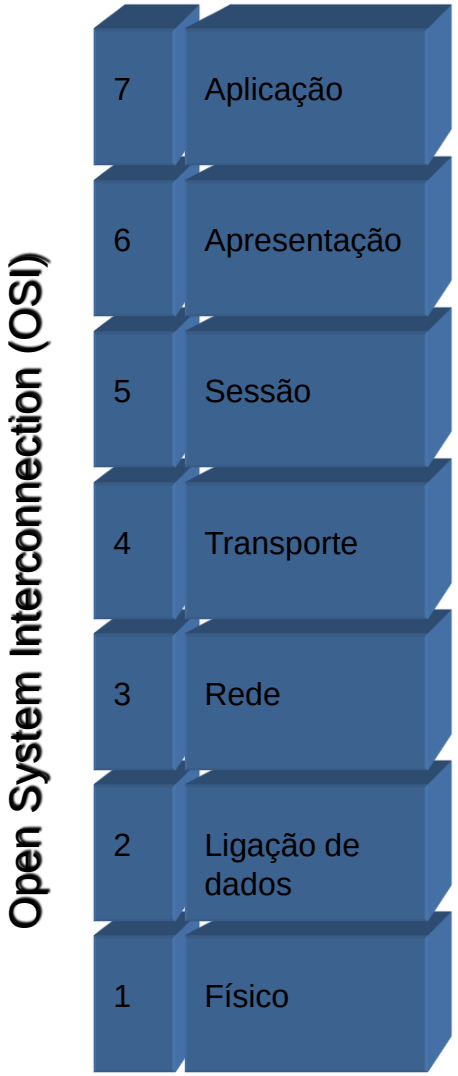
Segurança de rede

Camada 2

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

"The purpose of this Reference Model of Open Systems Interconnection is to provide a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model. "

http://www.acm.org/sigs/sigcomm/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-1.TXT

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- Porquê um modelo em camadas ?
  - Para se obter uma decomposição lógica de uma rede complexa em partes menores de fácil compreensão (as camadas).
  - Para se obterem interfaces standard entre os módulos de software.
  - Para haver uma linguagem standard de comunicação.

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- Cada camada ...
  - presta serviços para camada superior.
  - usa serviços da camada inferior.
  - apenas toma conhecimento da camada inferior.
  - Divisão de tarefas.
  - Facilita abstração.

DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- ***Camada da aplicação***
  (Application Layer)
  - Oferece acesso directo às aplicações para utilizar os recursos da rede.
  - Representada por API's de software.

- ***Camada da apresentação***
  (Presentation Layer)
  - Determina o formato de dados a ser utilizado nas trocas de informação entre computadores ligados em rede.
    - Algumas vezes chamado de "network's translator".
    - Transforma o formato de dados de uma camada de aplicação para um outro que ambos os computadores reconheçam.

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- ***Camada de sessão***

  (Session Layer)
  - Permite que duas aplicações em diferentes computadores estabeleçam, usem e terminem uma sessão.
  - Permite o reconhecimento de nomes e funções necessárias para comunicar através da rede.
  - Permite a sincronização entre as tarefas dos utilizadores.

- ***Camada de transporte***

  (Transport Layer)
  - Garante que as mensagens sejam transferidas sem erros, em sequência, sem perdas ou duplicação.
  - Divide as mensagens em pacotes e junta os pacotes no destino.
  - Envia mensagens de “acknowledgement “

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- ***Camada de rede***
  (Network Layer)
  - Responsavel pelos endereços.
  - Transforma os endereços lógicos em físicos e vice-versa.
  - Determina o caminho que a informação deve seguir na rede.
  - Gere problemas de tráfego na rede.
  - Se o destino não pode receber pacotes com o determinado tamanho divide os pacotes em outros mais pequenos que são depois enviados e no destino são juntos.

- ***Camada de ligação de dados***
  (Data-Link Layer)
  - Dividida em duas sub-camadas
  - Media Access Control (MAC)
    - Media Access Protocols
    - Physical Addressing
  - Logical Link Control (LLC)
    - Frame Synchronization
    - Flow Control
    - Error Checking

UNIVERSIDADE PORTUCALENSE

O modelo de referência **OSI**

- ***Camada física***

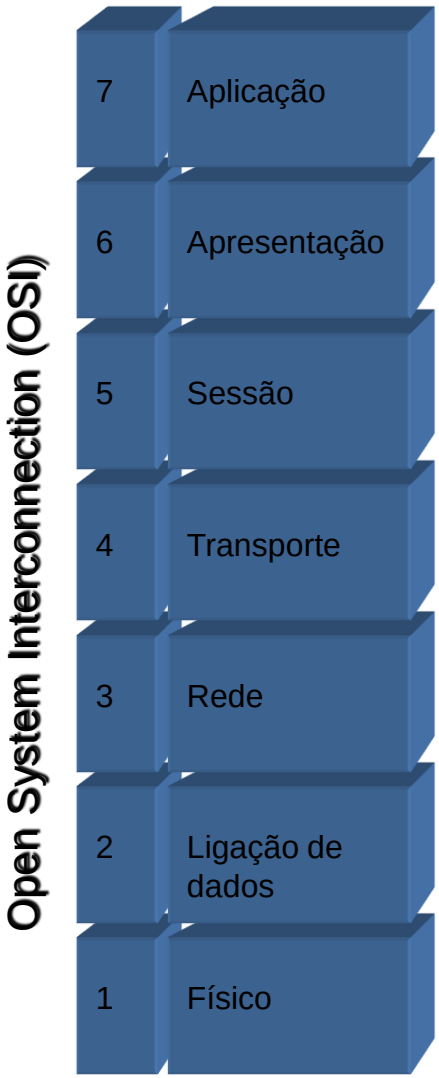
  (Physical Layer)

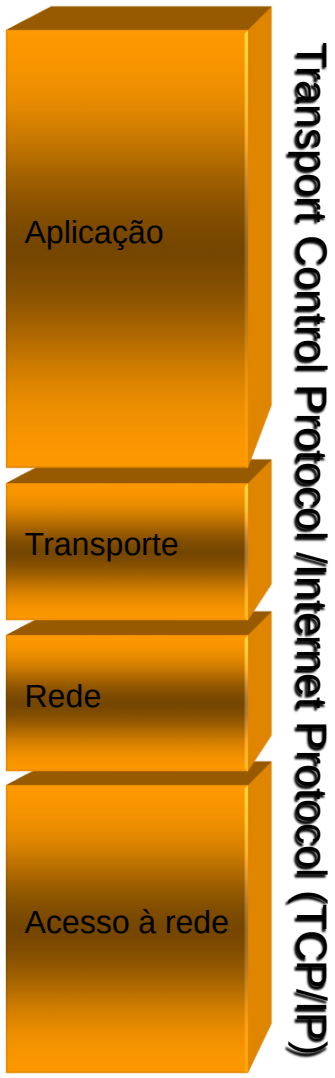
  – Define
    - Propriedades electricas
    - Meios de transmissão
    - Equipamentos de transmissão
    - Topologias fisicas
    - Sinalização de dados
    - Sincronização de dados
    - Largura de banda

O modelo de referência

UNIVERSIDADE PORTUCALENSE

OSI





DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Switches e segurança na camada 2

- A Segurança dos dispositivos da camada 2 (por exemplo switches) é importante, porque algumas ameaças são iniciadas nesta camada em vez de camadas superiores;

- Por exemplo um router não pode bloquear um servidor comprometido de contactar outros servidores na mesma rede porque a comunicação entre ambos ocorre na camada 2

UNIVERSIDADE PORTUCALENSE

Porquê a camada 2?

- Efeito de dominó.
  - Quando comprometida a camada 2 todas as camadas superiores estão em causa

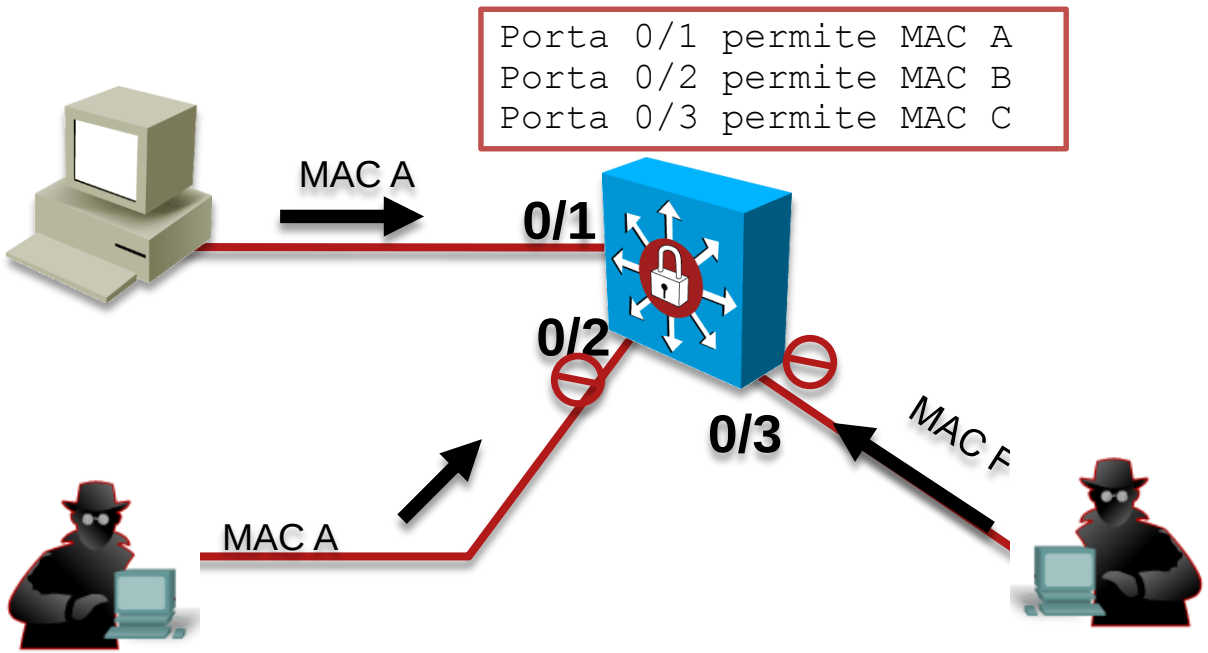
DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Port security

- Um mecanismo para restringir os endereços MAC que podem ligar-se a uma porta de um switch
  - Permite que seja definida uma gama de endereços que se podem ligar a uma porta determinada
  - Só as frames com o MAC correto podem comunicar através da porta
- Útil para prevenir ataques de flooding de MAC
  - CAM overflow (content-addressable memory)
  - A tabela de CAM guarda Informação tais como os endereços MAC e as respetivas associações com as portas e Informação sobre as VLANS associadas
  - A tabela de CAM tem um tamanho fixo
  - Quando a tabela está cheia o switch não consegue criar mais entradas
  - O switch envia então as frames recebidas para todas as portas …..

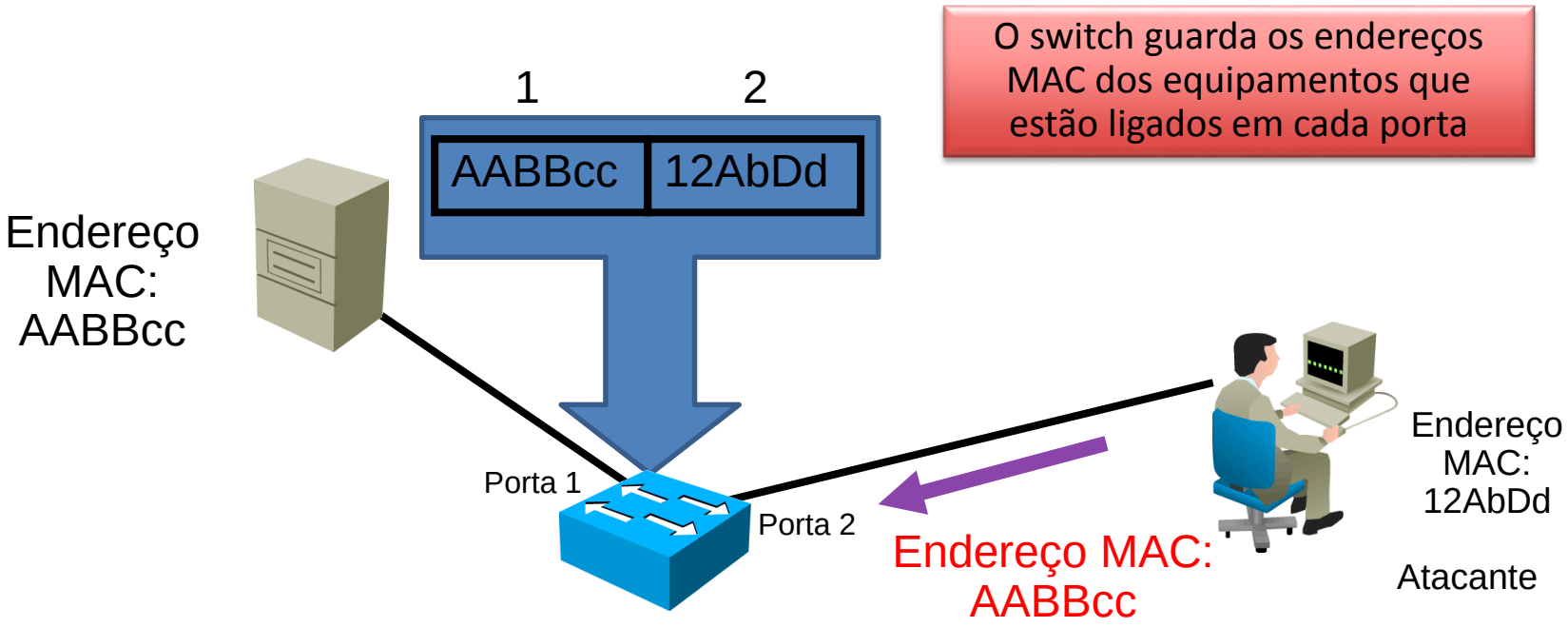
Port security



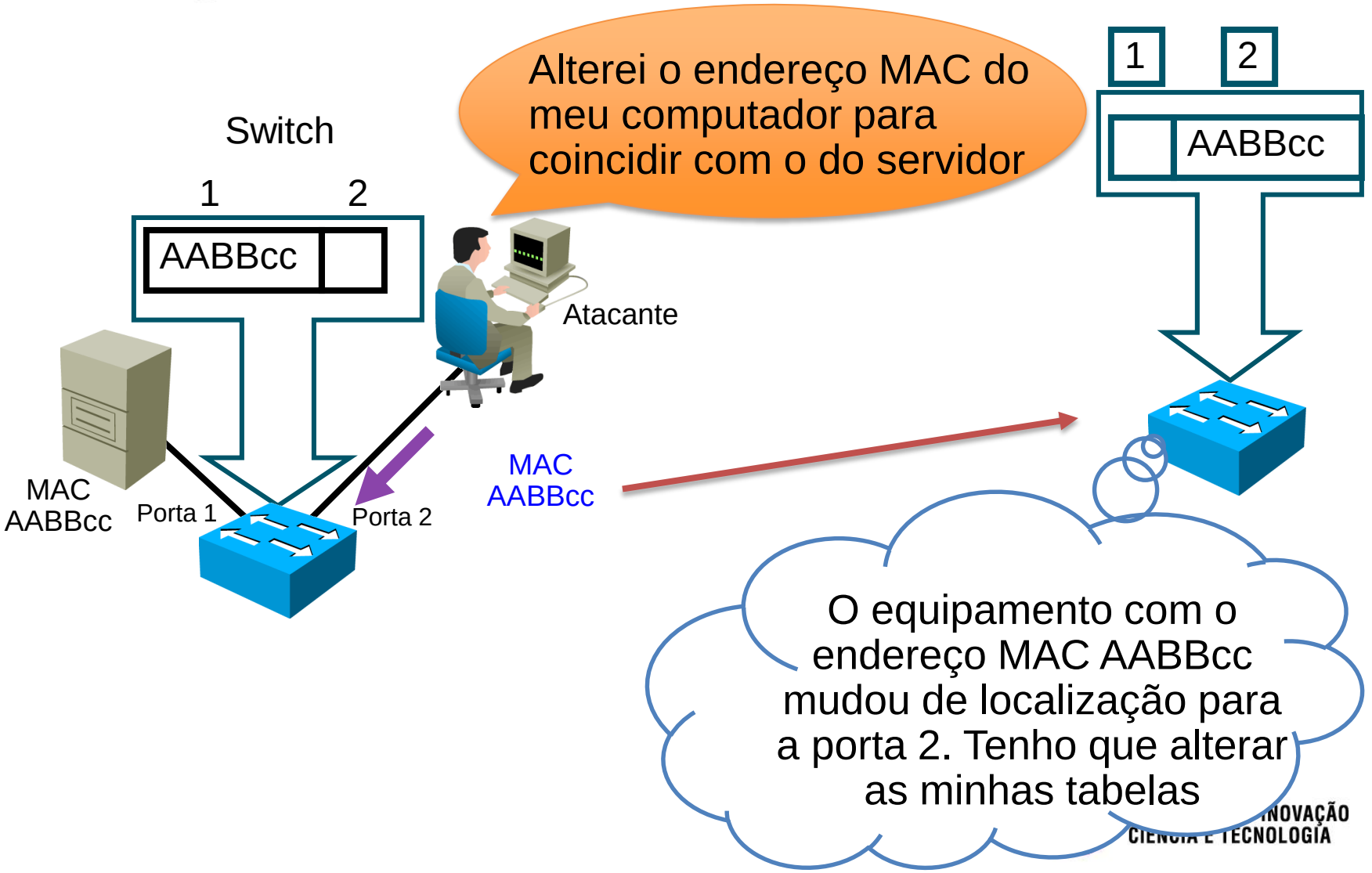
Atacante 1

Atacante 2

MAC Address Spoofing

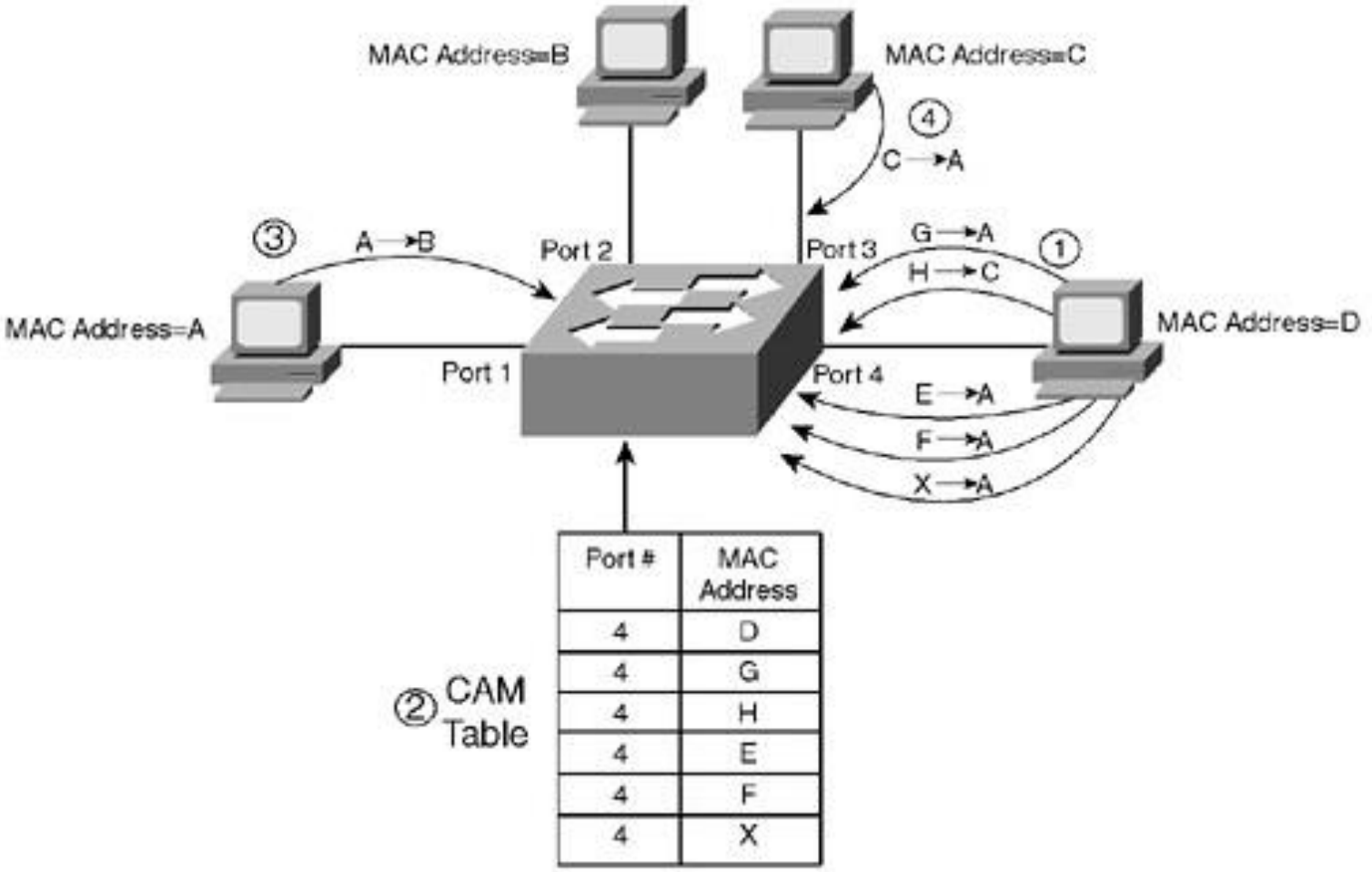


MAC Address Spoofing



UNIVERSIDADE PORTUCALENSE

MAC Address Flooding



Port #	MAC Address
4	D
4	G
4	H
4	E
4	F
4	X

MAC Address Flooding (cont.)

UNIVERSIDADE PORTUCALENSE

- Contra medidas:
  - Configurar manualmente os endereços que se podem ligar numa porta.
  - Limitar o número de máquinas que se podem ligar numa determinada porta

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Listas IP permit

- Restringir o tráfego que passa num switch:
  - Exemplo Permitir o tráfego telnet
  - Comandos CISCO:
    - ***set ip permit enable [telnet | snmp | ssh]***
    - ***set ip permit 172.16.0.0 255.255.0.0 telnet***

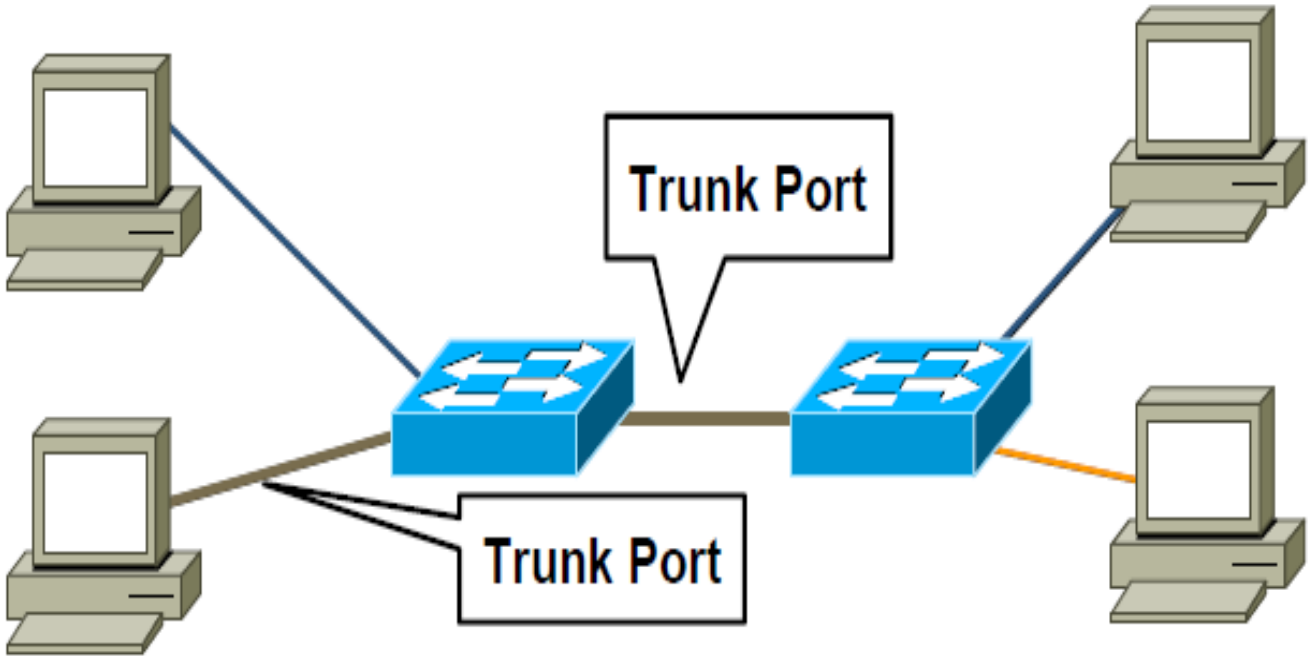
Controlo de LAN floods

- Os atacantes podem inundar a rede de frames (por exemplo CAM flooding) ou enviar broadcasts de modo a inundar a rede.
- Contra medidas:
  - Filtragem de protocolos
  - Definir os limites de tráfego broadcast/multicast permitido nas portas de um switch
    - Exemplo (CISCO) **set port broadcast 2/1-6 75%**

UNIVERSIDADE PORTUCALENSE

Ataque VLAN hopping

- Dynamic Trunk Protocol



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ataque VLAN hopping

- Um host “engana” (spoof) o switch disfarçando-se como um switch
- O link host/switch é colocado em modo trunk
- O host fica então membro de todas as vlans
- É necessário que a configuração do switch o permita

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ataque VLAN hopping

- Medidas de prevenção:
  - Identificar sempre as vlans de cada porta
  - Desativar as portas não utilizadas e coloca-las numa rede não ativa
  - Não utilize a VLAN 1 para nada
  - Coloque todas as portas em modo não trunking

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ataque GARP

- O que é o ARP (Adress resolution protocol) ?
- O que é o GARP (Gratuitous ARP) ?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

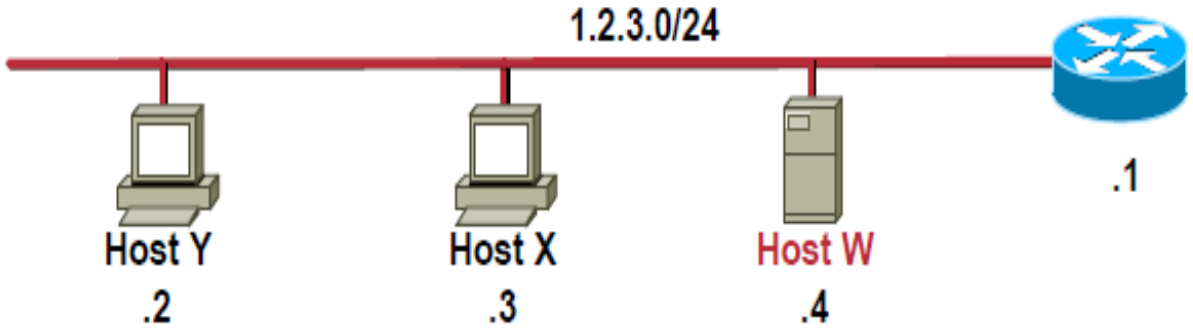
Ataque GARP

- GARP - Gratuitous ARP
  - É utilizado pelos hosts para anunciarem os seus endereços IP para evitar endereços IP duplicados
  - É um broadcast

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ataque GARP



- O Que acontece se:
  - Host W anuncia sou 1.2.3.1 com o MAC 12:34:54:12:5D:11

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

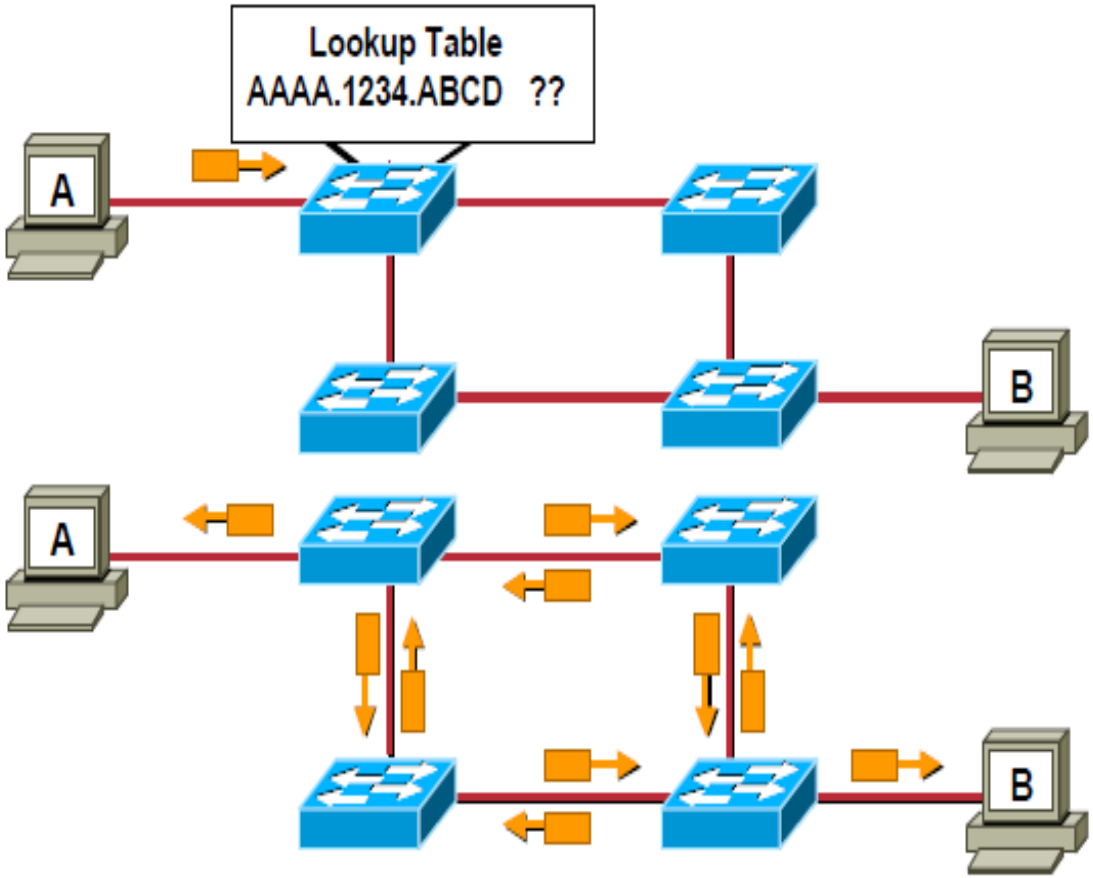
UNIVERSIDADE PORTUCALENSE

Ataque Spanning Tree

- Para que é utilizado o spanning tree ?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Ataque Spanning Tree



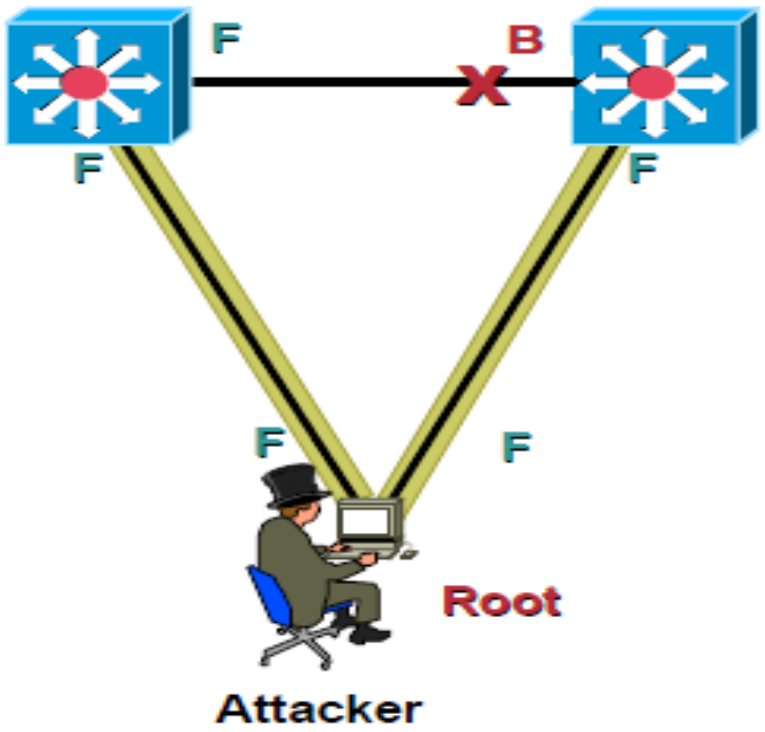
UNIVERSIDADE PORTUCALENSE

Ataque Spanning Tree

- O atacante envia mensagens para o switch de modo a que este recalcule a árvore de spanning tree.
- Envia mensagens de modo a que se possa tornar o root bridge
- Indica qual a ligação que é cancelada

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Ataque Spanning Tree



UNIVERSIDADE PORTUCALENSE

Ataque Spanning Tree

- Medidas de prevenção
  - Desative o STP (não é necessário em redes que não tenham loops)
  - Utilizar BPDU Guard
    - Desativa as portas utilizando o portfast depois da deteção de uma mensagem de BPDU recebida