1. VLANs

LAN : Conjunto de redes locais. Define um domínio de broadcast e todos os terminais a si ligados podem comunicar de forma direta.

Ethernet (802.3): tecnologia lan com mais sucesso.

Usa CSMA/CD):

- **Carrier Sense:** o host vê primeiro se o canal de comunicação está a ser usado (se existe transmissão de dados corrente);
- **Multiple Access:** vários hosts têm acesso ao mesmo tempo;
- **Collision Detect:** o host "ouve" o canal de comunicação enquanto transmite para detetar colisões;

Curiosidade:Não há colisões nas Ethernets modernas

Qual é a necessidade das Virtual LANs?

Os endereços IPv4 e IPv4 encontram-se em redes relativamente pequenas, isto começa logo em Layer 2, porque se "pegarmos" num grupo de máquinas ou utilizadores e juntá-los numa rede de switching específica, essa rede vai isolar os broadcasts e no limite do Layer 2, isola também todo o outro tráfico (o tráfico dos outros não interfere no tráfico da determinada vlan.
Também se houver algum problema numa vlan, é muito mais fácil localizar a máquina.
Virtual LAN (VLAN) : Grupo de terminais/utilizadores com um conjunto de características ou requisitos comuns no mesmo domínio de broadcast (independente da sua localização física.

Normalmente uma VLAN pode partir por vários critérios:

- localização
- tipo de utilizador

As VLANs resolver o problema de escabilidade de grandes redes

- Subdividindo um único domínio de broadcast, em vários mais pequenos;
- Permite uma administração e implementação de segurança da rede, de forma mais simples e correta

Os terminais em VLANs diferentes não comunicam em Layer 2, mas sim em Layer 3. Complica um bocadinho mais o routing, pois vão ter mais redes IP pois se dois terminais de diferentes VLANs quiser se comunicar irão ter que ir a um router (layer 3) mas isso até é uma vantagem nas redes modernas, pois tanto estamos a falar de routers com firewall e sem firewall, e é uma maneira de restringir a propagação do tráfico dentro da rede.

Definindo terminais na VLAN

Nota: no PC que se liga ao switch, não se configura nada

As VLANs configuram-se nos próprios switches, define-se um conjunto de portas que correspondem às vlans.

A VLAN a que o terminal pertence, depende apenas do porto do switch a que está conectado.

Por default, todas as portas pertencem à vlan1. Esta vlan é geralmente reservada para administração da rede.

Ligação de switches com diferentes vlans

Numa empresa existem vários switches, pois os switches têm um número de portas limitado.

Existem duas maneiras de ligação das vlans entre os switches:

1- Através de uma ligação física que liga as vlans onde o broadcast passa. Tem que haver uma ligação para cada pares de vlans

Exemplo: Vlan1 ---- Vlan1 ; Vlan2 ---- Vlan2

Esta solução não é viável, pois as empresas possuem inumeras vlans, e devido à limitação de portas dos switches

2- Através de uma única ligação fisica, usando um InterSwitch/Trunk port(s), isto é, no switch define-se uma porta especial por onde passam todos os pacotes de todas as VLANs.

Isto requer um mecanismo que seja capaz de diferenciar os pacotes de diferentes VLANs
Cada pacote deve estar identificado:

- Adicionar o identificador quando este é direcionado para uma porta trunk
- Lendo e removendo o identificador quando se recebe o pacote de uma porta trunk

Curiosidade: Interswitch é o nome antigo, que é uma porta entre switches. Trunk é "molho", praticamente, tudo ao molho e fé em Deus :)

O protocolo usado nas portas trunk é o IEEE802.1Q, que para identificar a vlan que representa, apenas adiciona o campo TAG
O campo TAG tem:

- A prioridade relativa ao tráfego
- CFI que é usado para garantir compatibilidade com tecnologias mais velhas
- VLAN ID para identificar a vlan

Ligações Trunk

Ligação física entre dois portos trunk
As ligações trunk podem transportar todas as VLANs ou só algumas

Conexões IP entre VLANs

Para comunicar entre VLANs é necessário usar Layer3 (IP routing).

É preciso um router ou um switch L3 (que faz routing)

ROUTER

- A interface do router que liga ao switch tem que suportar também o protocolo 802.1Q, para conseguir identificar as vlans
- O router tem que ter um IP para cada vlans (A interface física do router é sub-dividida em sub-interfaces)

- O gateway de IP para um terminal na VLAN é o endereço IP da respetiva sub-interface do Router

SWITCH com LAYER 3
-Conectar os switches (L2 e L3) usando portas trunk
-Cada VLAN é mapeada a um interface virtual da Layer 3
-O gateway IP para um terminal na VLAN é o endereço IP da respetiva interface virtual do switch L3

Diferenças fundamentais entre o router e o switch L3

No router temos uma interface fisica com sub-interfaces e os IPs estão nas sub-interfacess
No swL3, por cada VLAN que existe no switch já temos uma interface virtual do L3, vlan1, vlan2 e vlan3 (exemplo), e nesses é que temos os IPs

Redundância

As redes têm que ter redundância, pois permite que a rede recupere dinamicamente de falhas na rede.

O problema é que a redundância de ligações, cria loops de Layer 2. Isto causa o colapso de comunicações quando
um pacote de MAC com um endereço de broadcast são enviados, devido a um flood infinito.

Modelos

Nesta matéria falamos de 2 modelos de vlan

End-to-End VLAN : As vlans estão associadas com portos do switch vastamente distribuídos pela rede
O tráfego entre estas vlans devem possuir switches nas camadas de distribuição (usando truncamento)

Local VLAN: A vlans locais estão, usualmente, confinadas a uma rack de conexão

O tráfego entre estas vlans devem ser routeados em camadas de distribuição (usando routing ou links layer3)

Segmentação VLAN

Os objetivos da segmentação passam por juntar, na mesma rede lógica, serviços, terminais e utilizadores, que partilhem tráfego, políticas de QoS e de segurança
Cada VLAN têm de possuir um IP único de (sub)-rede e pode possuir mais que uma sub-rede (incluindo IPv4 privado e público, e também IPv6)

Redes locais VLAN vizinhas, com tráfego, políticas de QoS e de segurança similares, devem possuir (sub-)redes de IP que possam ser sumarizadas / agregadas.
Exemplo: VLAN de telefones VoIP no edifício X (VLAN 21: 200.0.0.0/24).
VLAN de telefones VoIP no edifício Y (VLAN 22: 200.0.1.0/24).
Sumarização / agregação de endereços da VLAN 21 + VLAN 22 : 200.0.0.0/23

Agregação de ligações de Ethernet

A velocidade de uma única conexão pode não ser suficiente para sastifazer as exigências.
Múltiplas ligações de Ethernet podem ser agregadas, fornecendo uma conexão trunk imperceptível com N vezes a velocidade de uma ligação
Pacotes de Ethernet são load-balanced entre todas as ligações físicas disponíveis.