

REDES DE COMPUTADORES

Aula 17 — Redes Corporativas e Segmentação (VLAN)

Como separar logicamente uma rede que compartilha a mesma infraestrutura física

Unidade 4 | 2 horas



Objetivos da aula



Por que segmentar

Entender por que uma rede corporativa precisa ser dividida em partes menores.



O que é VLAN

Compreender como um único switch físico pode hospedar redes logicamente separadas.



Aplicar na prática

Projetar a segmentação de VLANs de uma empresa com múltiplos setores.

Por que segmentar uma rede

Em uma empresa pequena, é comum que todos os dispositivos — computadores, impressoras, câmeras, Wi-Fi de visitantes — estejam na mesma rede, sem separação.

À medida que a empresa cresce, isso dificulta segurança, controle, organização e administração: um problema em qualquer parte da rede tem, potencialmente, acesso a tudo o mais.

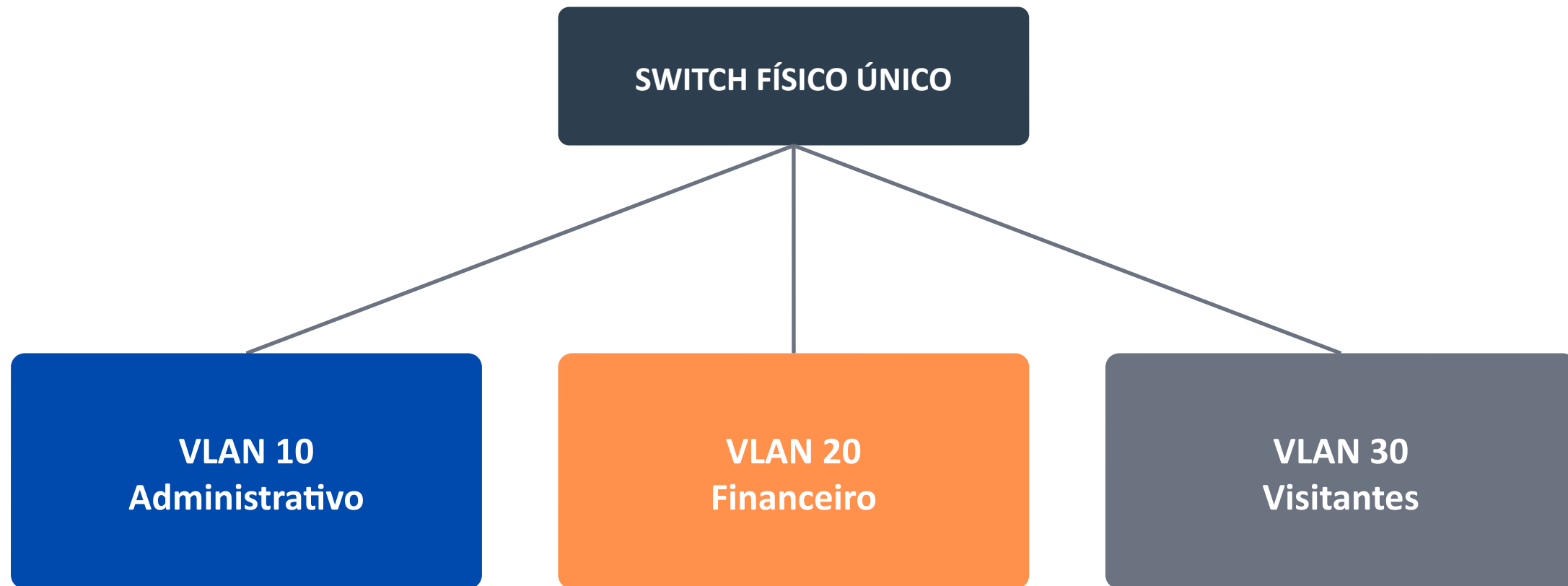


VLAN — Virtual LAN

VLAN é a tecnologia que permite separar logicamente grupos de dispositivos, mesmo que todos compartilhem a mesma infraestrutura física de switches.

- Fisicamente, pode existir um único switch conectando tudo.
- Logicamente, esse mesmo switch pode hospedar diferentes redes isoladas entre si.
- Cada VLAN se comporta como se fosse uma rede local independente.

Um switch físico, três redes lógicas



A separação é lógica: o cabeamento e o switch são os mesmos, mas cada VLAN funciona como uma rede isolada das demais.

IDEIA CENTRAL

Fisicamente, um switch. Logicamente, redes separadas.

É essa separação lógica — sem duplicar cabeamento ou equipamentos — que torna a VLAN uma das ferramentas mais usadas em redes corporativas.

Benefícios da segmentação por VLAN



Segurança

Um problema em uma VLAN não se propaga automaticamente para as demais.



Organização e controle

Permite aplicar políticas diferentes para grupos diferentes de dispositivos.



Menos tráfego de broadcast

Reduz o tráfego desnecessário espalhado pela rede inteira.



Regras por setor

Facilita aplicar regras específicas de acesso para cada setor da empresa.

A rede de visitantes deve ficar isolada

Um visitante conectado ao Wi-Fi de convidados deve conseguir acessar a Internet...

...mas não deve conseguir "enxergar" servidores, impressoras ou outros dispositivos da rede corporativa interna.



Câmeras e dispositivos IoT em VLAN própria

- Câmeras de segurança e outros dispositivos IoT costumam ter proteções mais fracas que computadores comuns.
- São um alvo relativamente comum de ataques na rede corporativa.
- Colocá-los em uma VLAN própria, separada da rede de usuários, reduz a superfície de ataque.
- Isolar esses dispositivos limita o estrago caso um deles seja comprometido.



Ideia prática: câmera comprometida na sua própria VLAN não vira porta de entrada para o resto da rede.

Projetando VLANs para uma empresa fictícia

Em grupos, projetem a segmentação de VLANs de uma empresa fictícia com 4 setores.

- Deem um nome e um número a cada VLAN (ex.: VLAN 10 Administrativo).
- Listem quais dispositivos entram em cada VLAN.
- Justifiquem, para cada VLAN, por que ela precisa (ou não) acessar as demais.

Sugestão de setores: Administrativo, TI/Servidores, Câmeras/IoT e Visitantes.

Resumo para levar da aula

- Redes sem segmentação ficam difíceis de administrar e proteger à medida que a empresa cresce.
- VLAN separa logicamente grupos de dispositivos dentro de um mesmo switch físico.
- Segmentar traz segurança, organização, menos broadcast e regras por setor.
- Visitantes e dispositivos IoT/câmeras devem ficar isolados em VLANs próprias.





Obrigado!

Próxima aula: Monitoramento, Manutenção e Diagnóstico