**VLAN**

"O padrão IEEE 802.1Q permite a criação de redes virtuais locais (VLAN) dentro de uma rede ethernet. A**ideia principal é a de adicionar rótulos de 32 bits (802.1Q tags) nos quadros etherne**t e instruir os elementos comutadores de camada de enlace (ex. switches, bridges) a trocarem entre si, apenas quadros contendo um mesmo identificado".

Segundo o livro Comunicação de Dados e Redes de Computadores do autor Forouzan, cada VLAN pode ser feita por:

* Números das portas;
* Endereços MAC;
* Endereços IP;
* Endereços IP multicast ou combinação de duas ou mais delas;

Campo VLAN, chamado de **TAG**, com tamanho de **32 bits (4 bytes)**é segmentado em 4 subcampos:

* **1º Type:** aqui é informado o tipo da VLAN empregada. Esse subcampo possui**16 bits (2 bytes);**
* **2º Priority:** aqui é onde ocorre a tratativa de QoS por meio do 802.1p. Esse subcampo possui **3 bits;**
* **3º Flag:** Também chamado de bit CFI, é usado para indicar que todos os endereços MAC presentes no campo de dados MAC (MAC data field) estão na forma canônica. Este campo é interpretado de forma diferente de acordo com a tecnologia utilizada (Ethernet, token ring, FDDI). Esse subcampo possui **1 bit.**
* **4º VID:** VLANID. É onde a VLAN recebe a sua identificação. Esse subcampo possui**12 bits.**

Como duas VLANs se comunicam:

* se forem duas VLANs com mesmo ID (vlan2 comunicando com vlan2): usa-se uma porta em modo trunk nos switches;
* **se forem duas VLANs com IDs diferentes (vlan1 comunicar com vlan3 - caso da questão): é necessário um roteador (gateway).**

Foram definidos vários tipos de VLAN, de acordo com o critério de comutação e o nível em que se efetua:

Uma VLAN de nível 1 (também chamada VLAN por porta, em inglês Port-Based VLAN) define uma rede virtual em função das portas de conexão no comutador;  
Uma VLAN de nível 2 (igualmente chamada VLAN MAC, em inglês MAC Address-Based VLAN) consiste em definir uma rede virtual em função dos endereços MAC das estações. Este tipo de VLAN é muito mais flexível que a VLAN por porta, porque a rede é independente da localização da estação;  
Uma VLAN de nível 3: distinguem-se vários tipos de VLAN de nível 3: A VLAN por subrede (em inglês Network Address-Based VLAN) associa subredes de acordo com o endereço IP  
fonte dos datagramas. Este tipo de solução confere uma grande flexibilidade, na medida em que a configuração dos comutadores se altera automaticamente no caso de deslocação de uma estação. Por outro lado, uma ligeira degradação de desempenhos pode fazer-se sentir, dado que as informações contidas nos pacotes devem ser analisadas mais finamente.

**Analista estabelece a criação de VLANs para otimizar o desempenho e aumentar a segurança da transmissão de dados entre os vários setores de atividade do TRE-SP.**

* 802.1D  é o spaning tree protocol;
* 802.1w é o rapid spanning tree protocol;
* 802.1Q é VLAN (Aumenta a segurança);
* **802.1p QoS(Quality of Service) ;**
* 802.1s Multiple Spanning Trees;

O **Link-Aggregation** permite  agregação de diversas interfaces Ethernet (portas físicas) para a criação de uma **única** porta lógica com o intuito de prover redundância e aumento de banda. As melhores práticas sugerem a negociação do protocolo **LACP (802.3ad)** entre os 2 equipamentos que desejam fechar a agregação de portas afim de evitar erros de cabeamento e certificar o meio físico em todo o tempo que o Link-Aggregation estiver ativo, além de agilizar a redundância em caso de falhas.

**802.3ad => Link Agregation -** 802.1q => VLAN

**Ethernet Automatic Protection Switching** (**EAPS**) é usado para criar uma topologia tolerante a falha configurando um caminho primário e um secundário para cada Virtual LAN.

Operação: Um anel é formado configurando um domínio (*Domain*). Cada domínio tem um único "nó principal"(*master node*) e vários nós de trânsito (*transit nodes*). Cada nó terá uma porta primária e uma porta secundária, ambos habilitados a enviar tráfego de controle ao nó mestre. Sob operação normal só a porta primária no nó mestre é usado para evitar *loops*(a porta secundária é bloqueada para todo trafego que não for de controle).

Quando há uma situação de queda de conexão, os dispositivos que detectam a falha enviam uma mensagem de controle ao master, e o *master* então desbloqueará a porta secundária e instrui os Transit a atualizar suas bases de dados. Os próximos pacotes enviados pela rede então podem ser direcionados para a porta secundária (agora habilitada) sem qualquer perturbação na rede.

Os tempos de falha (*fail-over*) são demonstravelmente em cerca de 50ms.

O mesmo *switch* pode pertencer a múltiplos domínios e assim múltiplos anéis. No entanto, estes agem como entidades independentes e pode ser controlado individualmente.

**"O Spanning Tree Protocol (STP)** é um protocolo de Camada 2 executado em pontes e switches. A especificação para o STP é chamada de **IEEE 802.1D.** O principal objetivo do STP é garantir que você não crie loops quando tiver caminhos redundantes na rede. Os loops estão inoperantes em uma rede."

**Princípios do STP:**  
  
\*Somente um caminho ativo pode existir entre 2 estações na rede.  
\*Bloquear as portas que impliquem em loops fechados.

Já o PVSTP (per-vlan spanning tree) é uma variação do STP criado pela Cisco. Esse protocolo mantém uma instância do STP para cada VLAN da rede. Ademais, como a questão afirma, "de modo que as VLans possam utilizar enlaces diferentes na rede."

"**O STP é considerado muito lento, especialmente para rede atuais e que exigem alta disponibilidade. Um protocolo mais rápido, portanto, precisou ser desenvolvido e, para satisfazer essa demanda, em 1982 foi introduzido pela primeira vez o Rapid Spanning Tree (IEEE 802.1w). No ano de 2004, o RSTP foi incorporado pela IEEE no padrão 802.1D, com identificação 802.1D-2004.**"

<http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/st/index.php?file=protocolos/rstA>

Ademais, **RSTP não é um protocolo totalmente novo, mas sim uma evolução do STP** que preserva conceitos básicos, como por exemplo, a maneira que o**algoritmo Spanning Tree elege uma bridge raiz.** Incorpora, no entanto,**novas características:**

* Novo estado e novas funções das portas;
* Conceito de tipo de segmento;
* Sistema de proposta e de acordo veiculado pelas **BPDUs**, fazendo com que a transição para o estado de encaminhamento dispense um temporizador, utilizado no STP (IEEE 802.1D).

**Vantagem do RSTP:**

* Graças aos**caminhos alternativos calculados previamente, q**uando um enlace falha, os switches são capazes de excluí-lo da topologia imediatamente sem ter que calcular uma nova árvore, o que**aumenta a velocidade de convergência do algoritmo**significativamente.
* **Possui 3 estados**:**descarte, desativado e encaminhament**o; ao contrário do**STP que possui 5 estados**: bloqueio, escuta, aprendizado, encaminhamento e desativado.

As portas de um switch ou bridge rodando STP podem variar entre

* Blocking: Todas as portas de um switch encontra-se em modo blocking quando ele é ligado;
* Listening: Recebe e analisa BPDUs para certificar-se de que não ocorrerão loops;
* Learning: Registra os endereços dos hardwares conectados às interfaces e forma a tabela MAC.
* Forwarding: Envia e recebe frames.
* Disabled.

**CSMA-CD**  
  
1 - Dispositivo escuta o meio;  
2 - Se o meio estiver livre, a informação é transmitida;  
3 - Se outro dispositivo, também escutou e transmitiu ocorre a colisão e isso vai gerar um sinal de colisão chamado **jam**;  
4 - Caso ocorra a colisão, as maquinas param de transmitir por um tempo aleatório antes de tentarem novamente;  
5 - O ator principal no processo de detecção de colisão é o meio;

**CSMA-CA**  
  
1 - Emissor pergunta em unicast para o receptor se ele está livre para receber mensagens. Isso é feito enviando um RTS (Request to send);  
2 - Receptor responde em broadcast se está livre ou não. Dessa forma todos na rede são notificados da resposta;  
3 - Se estiver disponível o receptor envia em broadcast um CTS (Clear to send). Aqui o receptor informa para todos que estará ocupado, por um determinado intervalo de tempo, se comunicando com o emissor;  
4 - Se o receptor não estiver livre ocorre o backoff (espera um tempo aleatório para tentar novamente);  
5 - Todo o quadro recebido pelo receptor deve ser confirmado com um ACK. A premissa básica das redes de computadores "Confirmação positiva e retransmissão por timeout".  
6 - Aqui não ocorre a detecção da colisão como no CSMA-CD, e sim a prevenção.  
7 - O ator principal no processo de prevenção de colisão é o receptor.

O padrão **IEEE 802.3af** descreve a tecnologia Power over Ethernet - PoE - que permite transmissão de energia elétrica juntamente com os dados para um dispositivo remoto, através do cabo de par trançado padrão em uma rede Ethernet.

**Switch** é um equipamento que atua nas redes locais ou intranets, compartilhando o sinal entre os dispositivos (retransmitindo o sinal e ampliando a rede). O resultado é um **maior desempenho na comunicação entre as máquinas**. Usando Switch, os dados do computador de origem são recebidos APENAS pelo computador destino. O Switch pode gerar 3 tipos de tráfego:**unicast** (1 origem para 1 destino), **broadcast** (1 origem para todos os destinos possíveis) e **multicast**(1 origem para um grupo específico de destinos).

Originalmente o Switch atua na camada 2 (enlace) do modelo OSI, entretanto **os mais modernos** podem acumular funções e atuar como ROTEADORES. Assim atuando também na camada 3 (rede). Assim, os switches de camada 3 **SUPORTAM ROTEAMENTO e criação de redes virtuais (VLANs).**

**Proxy Transparente : o** proxy transparente é uma arquitetura que permite que o navegador cliente não saiba da existência do proxy. Ele acha que está solicitando o recurso diretamente ao servidor original; o Proxy encarrega-se de capturar e processar a solicitação. A principal vantagem nesta arquitetura é que não é necessária a configuração de proxy nos navegadores cliente. Outra (incorretamente) alegada vantagem é que o proxy não transparente não impede a conexão direta à Internet.