Protocolos STP e RSTP e Redes Sem Fio

Conceitos Gerais

1. Introdução

- É muito com

2. STP

- O STP é um protocolo usado para **evitar loops (ciclos)** em redes que utilizam mais de uma switche.

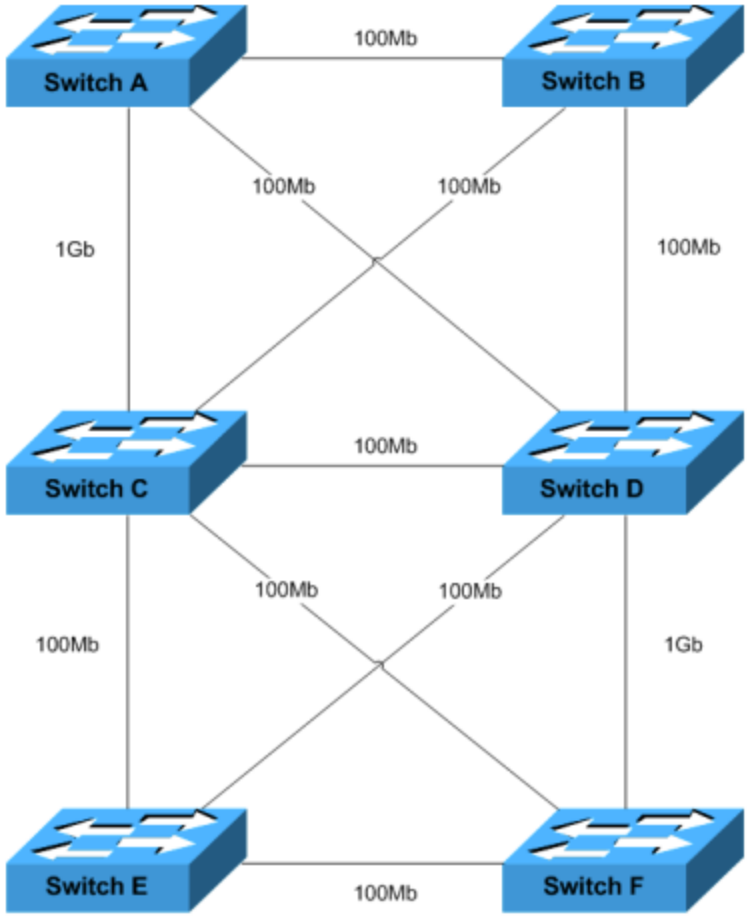
- Vamos pensar em uma rede que conecta conecta switches com **mais de um caminho** entre eles (para redundância). A princípio, a redundância de link é positiva, pois caso um dos links tenha problemas, a comunicação pode ser feita pelo outro link.

- Em contrapartida, mais de um caminho conectando switches pode gerar alguns problemas, como pacotes circulando infinitamente (em loop), fazendo que a rede fica lenta ou travada. Isso pode gerar um problema conhecido como **broadcast storm** (tempestade de pacotes).

- Para evitar esses “loops” ou caminhos cíclicos dentro da rede, foi criado o protocolo **STP (Spanning Tree Protocol)**, padronizado sob a identificação 802.1d. Ele faz o bloqueio de algumas portas dos switches que participam das interligações redundantes de forma que exista apenas um caminho operacional entre os dispositivos de rede.

2. STP

- Observe na imagem abaixo que existem diversos caminhos possíveis (com diferentes velocidades) para cada conexão entre os switches:



2. STP

- No STP os switches trocam informações entre a si a partir de **BPDU's (Bridge Protocol Data Unit)**. Chamaremos de Bridge o conjunto de informações do nó (switch), interface e enlace. Dessa forma, cada bridge possuirá uma Bridge ID, que serão fornecidas nas trocas de BPDU's.

- O primeiro passo do algoritmo STP é definir uma Bridge raiz (Root Bridge). Será definido como Bridge raiz aquele que possuir a menor Bridge ID. A partir de então o protocolo começará a mapear e montar a árvore (Tree) da rede.

- As demais bridges deverão definir entre suas interfaces aquela será considerada como porta raiz (Root Port). Essa interface será única por switch e apenas essa interface será utilizada para encaminhamento até a Root Bridge. Para essa definição, considera-se o melhor caminho possível.

- Após estas definições, as demais possibilidades de caminhos serão colocadas no modo "**blocking**".

3. RSTP

- O RSTP (Rapid Spanning Tree Protocol) é uma versão melhorada do STP. Ele detecta falhas muito rapidamente e já determina um caminho alternativo para conexão que eventualmente por perdida.

- O STP possui um tempo consideravelmente maior para identificar uma falha e determinar uma rota alternativa.

- Já o RSTP costuma identificar a determinar uma nova rota quase que instantaneamente.

4. VLAN (Virtual LAN)

- Antes de entender o conceito de VLAN, vamos imaginar o seguinte cenário: Uma empresa com 3 setores (RH, Financeiro e TI). Todos trabalham no mesmo prédio, e possuem seus computadores ligados fisicamente no mesmo switch.

- Como todo mundo na mesma rede, teremos problemas como falta de segurança (todo mundo acessa tudo) e muito tráfego desnecessário na rede.

- Os referidos problemas podem ser resolvidos com a técnica de LAN's virtuais, ou como são conhecidas, VLAN's. Essa tecnologia permite a criação de diversas redes locais virtuais em um único meio físico compartilhado.

- Desta forma, para resolver o problema anterior, poderíamos criar uma VLAN para cada departamento, de forma que seria possível isolar a comunicação, e impedir acesso não autorizado entre departamentos distintos.

4. VLAN (Virtual LAN)

- Para que haja a comunicação entre VLAN’s distintas, necessita-se de um roteador para fazer o roteamento entre elas.

- Desta forma, se um dispositivo na primeira porta de um switch estiver em uma VLAN 1 e um segundo dispositivo em outra porta do mesmo switch em uma VLAN 2, sem o uso de um roteador, esses dispositivos não conseguirão se comunicar.

- Cada VLAN possui um domínio de **BROADCAST** único, como uma rede de camada 3. Dessa forma, elimina-se o problema de falta de isolamento de tráfego apresentado anteriormente.

4. VLAN (Virtual LAN)

- A alocação dos dispositivos conectados aos switches em cada VLAN pode seguir três critérios:

- **Port-Based VLAN** – Também chamada de VLAN de nível 1 ou VLAN por porta. Nesse critério, não se considera o dispositivo a ser conectado, mas tão somente a porta utilizada do Switch.

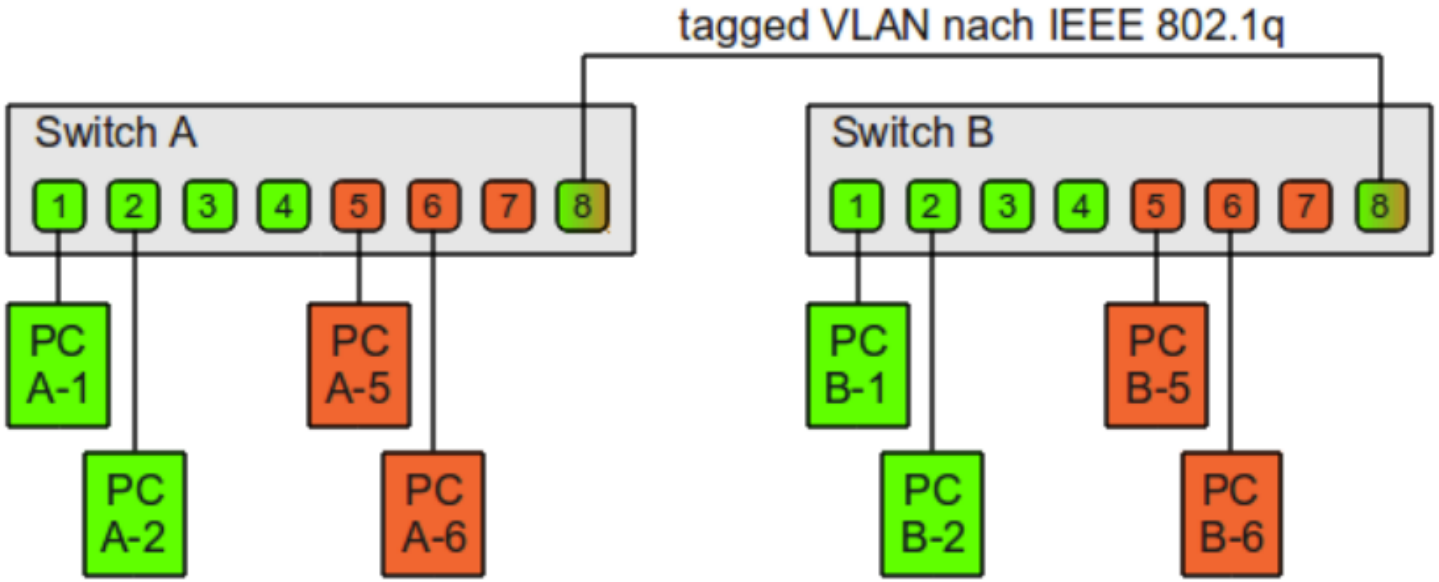
- **MAC Address-Based VLAN** – Também chamada de VLAN de nível 2 ou VLAN MAC. Neste critério, considera-se o endereço MAC do dispositivo e não mais a porta do switch. Mesmo trocando o computador de porta do switch, não mudará a VLAN.

- **Network Address-Based VLAN** – Também chamada de VLAN de nível 3 ou VLAN por Subrede. Considera-se para a alocação da VLAN o endereço IP do dispositivo.

4. VLAN (Virtual LAN)

- Quando cada porta do switch estiver alocada para uma VLAN específica, os usuários que pertencem a uma mesma VLAN, porém em switches diferentes, precisarão se comunicar.

- Para isso, configura-se as portas em modo **TRUNK**. Essas portas são responsáveis por agregar todo o tráfego de todas as VLAN's e encaminhar a comutadores vizinhos.



4. VLAN (Virtual LAN)

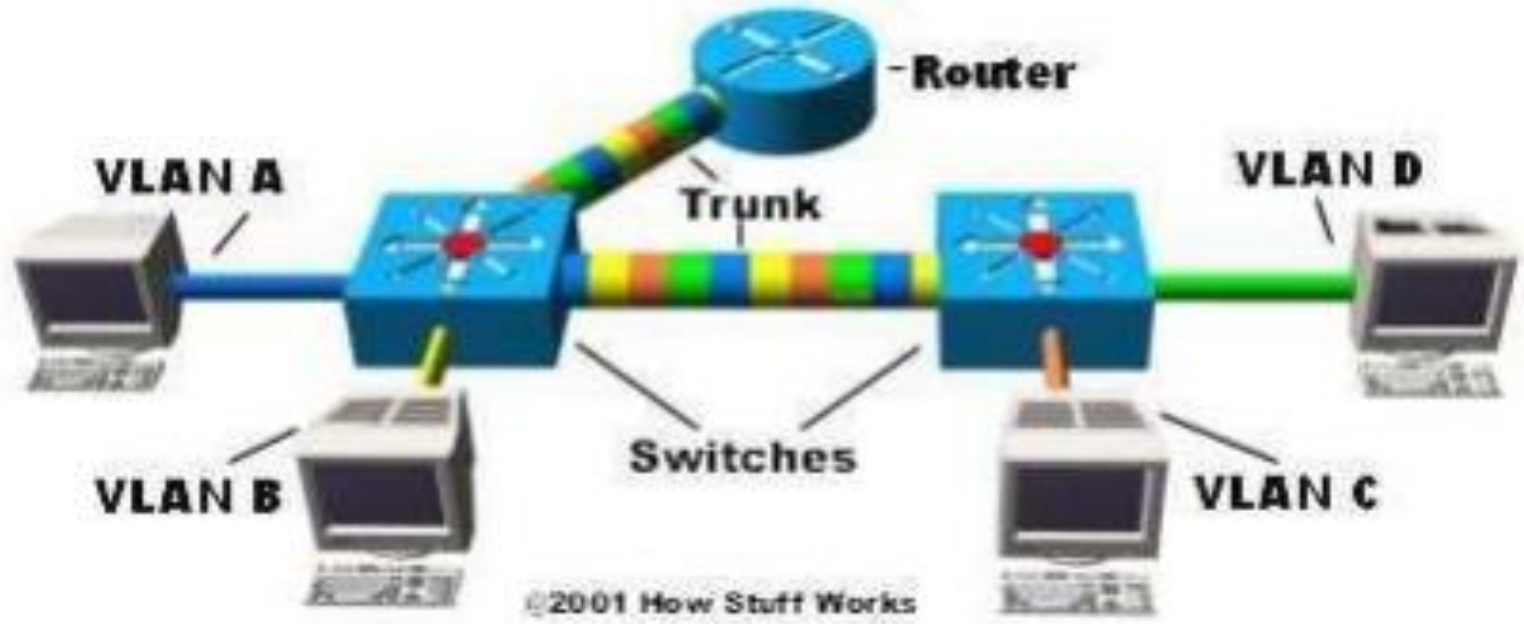
- Como podemos observar na imagem, existem 2 VLAN’s distintas (Verde e Laranja) e ambas configuradas nas respectivas portas (1 a 7) de ambos os switches.

- Já a porta número 8 de ambos está sendo utilizada no modo TRUNK para permitir a troca de dados entre as mesmas VLAN’s em switches diferentes. Ou seja, caso o “PC A-1” pretenda se comunicar com o “PC B-2”, ele utilizará a porta TRUNK para encaminhar os dados.

- Porém, a comunicação entre as VLAN’s não será possível devido à ausência de um roteador e o completo isolamento entre elas.

4. VLAN (Virtual LAN)

- Já na imagem a seguir, temos um ambiente com comunicação completa entre as VLAN’s. Podemos verificar a existência de 4 VLAN’s distintas e caso elas queiram se comunicar entre si, deve ser por intermédio do roteador e das portas TRUNK.



4. VLAN (Virtual LAN)

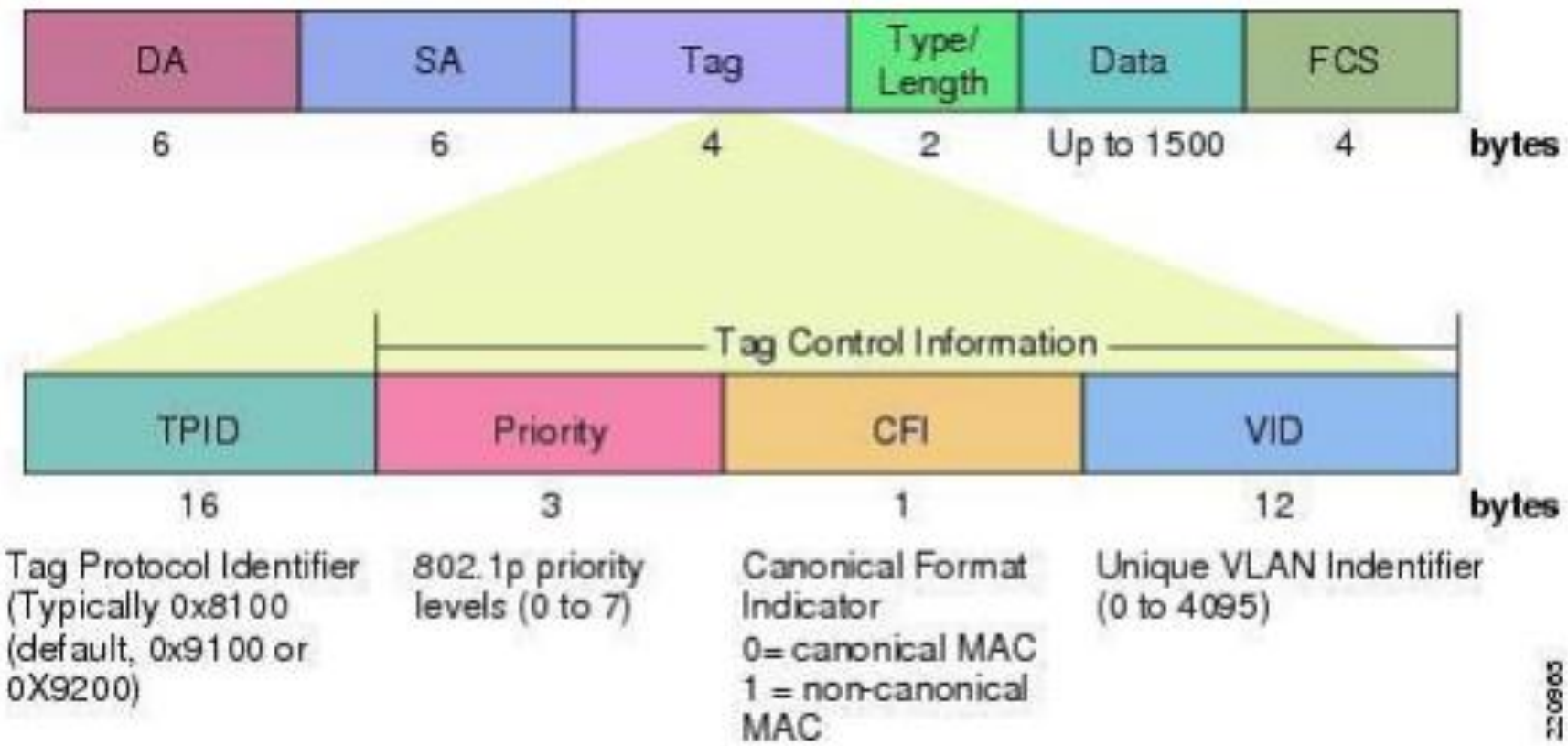
- Uma última questão a ser analisada é como os switches identificam a existência de VLAN's e como elas são diferenciadas nos frames.

- Para isso foi definido o protocolo 802.1q, que especifica o funcionamento da VLAN através da utilização de TAG's nos cabeçalhos dos frames na camada de enlace.

- No cabeçalho do frame, é criado uma TAG com os dados para identificação.

4. VLAN (Virtual LAN)

- A imagem abaixo mostra o cabeçalho do frame com a TAG para identificação de VLAN:



4. VLAN (Virtual LAN)

- Como podemos ver na figura anterior, a TAG é inserida no meio do cabeçalho do quadro, mais especificamente entre os campos “MAC de ORIGEM” e o campo “Length”.

- A TAG é composta por 4 bytes, sendo que os dois primeiros bytes (16 bits), é utilizado para a identificação da existência de uma TAG no quadro (TPID). Os 2 últimos bytes são utilizados pelos protocolos 802.1q e 802.1p.

- Os 3 primeiros bits (cor rosa na figura) são utilizados para definir oito classes diferentes de tráfego. Os 12 últimos bits são utilizados para a identificação da VLAN (cor azul).

- Como existe a possibilidade de uso de 12 bits para identificação, pode-se criar até 4096 VLAN’s diferentes (0 a 4095). Entretanto, as VLAN’s 0 e 4095 são reservadas, restando 4094 VLAN’s para utilização efetiva.

4. VLAN (Virtual LAN)

- Como exemplo de aplicação prática, vamos pensar na seguinte situação: Imagine uma empresa com 3 setores: Financeiro, Recursos Humanos (RH) e TI.

- Sem VLAN, todos os computadores estariam na **mesma rede**, o que causa problemas de segurança e organização. Com uma VLAN nós configuramos um switch gerenciável da seguinte forma:

- VLAN 10 → Financeiro
- VLAN 20 → RH
- VLAN 30 → TI

4. VLAN (Virtual LAN)

- Um funcionário do RH conecta seu computador na rede. Como a porta do switch está configurada para VLAN 20, ele só consegue se comunicar com dispositivos do RH.

- O Financeiro NÃO consegue acessar máquinas do RH diretamente. Desta forma, dados sensíveis (salários, contas) ficam isolados, mesmo estando no **mesmo switch físico.**

- Também é possível isolar serviços de rede. Por exemplo, se o RH tiver um servidor de banco de dados, apenas computadores da VLAN poderão utilizar.

4. VLAN (Virtual LAN)

- Apesar das VLAN's serem uma técnica muito usada atualmente, ela também apresenta algumas desvantagens.

- Maior complexidade de configuração: Precisa de switch gerenciável, configuração exige conhecimento (VLAN ID, trunk, access, etc.)

- Dificuldade de manutenção: Erros de configuração podem derrubar comunicação. Exemplo: Porta na VLAN errada → usuário sem acesso à rede

- Necessidade de roteamento entre VLANs: Se uma VLAN precisar falar com outra, é necessário um roteador ou switch camada 3 (mais caro e mais latência).

- Diagnosticar problemas fica mais difícil, pois pode ser VLAN errada, trunk ou switch mal configurado, etc.

4. VLAN (Virtual LAN)

- E por fim, a segurança não é absoluta. A VLAN **aumenta a segurança**, mas não substitui o uso do firewall e de controle de controle de acesso. Ataques como VLAN hopping podem ocorrer (se mal configurado).

- **VLAN Hopping** é uma técnica de ataque cibernético que permite a um invasor contornar a segmentação de rede e acessar dados em uma VLAN (Virtual Local Area Network) para a qual não tem permissão. Geralmente, o atacante explora configurações incorretas em switches.

- Para proteger uma VLAN, devemos:

1 - Desativar DTP: Desabilite a negociação automática (DTP) em portas de acesso.

2 - Configurar Portas Trunk: Desative o modo automático e configure as portas trunk manualmente.

3 - VLAN Nativa: Nunca utilize a VLAN 1 (padrão) para tráfego nativo e altere a VLAN nativa dos troncos para um número não utilizado.

4 - Desativar Portas Inativas: Desative todas as portas não utilizadas do switch.

4.1 Riscos de uma Rede

- Considerando a era da Informação em que nos encontramos atualmente, aspectos de Segurança digital são fundamentais em qualquer ambiente.

- Existem muitas empresas que possuem basicamente o centro dos seus negócios centrado em dados e informações (Google, Amazon). Alguns especialistas dizem que dados são o novo petróleo.

- Assim como o uso da computação e das redes de comunicação cresceram, também aumentaram de forma exponencial os golpes e ataques virtuais.

- A área de segurança da informação tem como objetivo identificar e elaborar técnicas que possam proteger servidores e sistemas destes ataques.

4.1. Varredura de SO em Redes (Scan)

- A varredura em redes é uma técnica que geralmente antecede ataques. Essa técnica visa a obtenção de informações que subsidiarão as ações dos atacantes, como a busca de vulnerabilidades.
- Fazer a varredura fora da rede é mais complexo, pois o firewall costuma identificar e bloquear.
- Por isso, os hackers costuma infectar um computador interno da rede com um software de varredura para obter informações.
- Geralmente, a varredura é o primeiro passo para uma invasão mais agressiva.

4.2 Tipos de Ataques

- **Spoofing**: Se passar por alguma pessoa, instituição ou dispositivo que possua certo grau de confiabilidade para dar confiança à informação enviada. Por exemplo, posso enviar e-mails em nome da Receita Federal.

- **Man in the Middle**: Se inserir no meio da comunicação entre dois nós e capturar/modificar a informação trocada.

- **Sniffing**: É uma técnica que consiste em inspecionar os dados trafegados em toda a rede por meio do uso de programas chamados de sniffers (Ex. Wireshark).

- **Brute Force**: Tentar descobrir uma senha ou alguma outra informação através do método de tentativa e erro de forma exaustiva. Senha simples são quebradas facilmente.

- **Desfiguração (defacement)**: Técnica que consiste em alterar o conteúdo de uma página Web. Possui um caráter unicamente de vandalismo. Para isso explora vulnerabilidades na página ou no servidor.

4.2 Tipos de Ataques

- **Phishing**: Geralmente usado junto com o spoofing. O Spoofing induz o usuário a clicar em um link que irá direcionar para um site falso ou instalar um software malicioso.
- **Pharming**: Este tipo de ataque ocorre quando um tráfego que originalmente deveria ir para um site legítimo é redirecionado para outro. Geralmente um software malicioso altera este trafego em algum lugar da rede.
- **Ddos** (Negação de serviço): Gerar artificialmente um grande tráfego em determinado sistema/servidor e derrubar o serviço.
- **Engenharia Social:** Enganar usuários para que os demais ataques possam ser realizados.
- **Spyware**: Este tipo de malware foca na obtenção de informações de um host através do monitoramento de suas atividades. Em seguida envia para terceiros. Ex: keyloggers.
- **Botnet**: São programas que permitem a comunicação e controle do invasor sobre o sistema da vítima por intermédio de acessos remotos.

4.2 Tipos de Ataques

- **Ransomware**: Sequestro dos dados. O atacante criptografa os dados do computador, e libera a chave apenas mediante pagamento.

4.3 Tipos de Malwares (vírus)

- Os principais tipos de vírus são:

Vírus de Boot: Infecta a área de inicialização dos sistemas operacionais, também conhecido como MBR (Master Boot Record) do disco rígido. Esse tipo de vírus não corrompe arquivos específicos, mas sim, todo o disco. Os antivírus comuns de sistemas operacionais não são capazes de detectar esse tipo vírus, sendo necessário uma varredura antes da inicialização do sistema para sua detecção.

Vírus de Arquivo: Infecta arquivos de programas executáveis, geralmente, nas extensões .EXE e .COM. Ao se executar o referido programa, ativa-se o vírus.

Vírus Residente: Este é carregado diretamente na memória RAM do SO toda vez que o SO é iniciado. Este tipo de vírus pode ser extremamente danoso, bloqueando acessos à memória RAM, interromper determinados processos e funções a serem executadas e inclusive, alterar tais funções para fins maliciosos.

Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Vírus de script: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou também por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

5. Redes Sem Fio

- As redes sem fio fazem parte de um dos padrões de implementação definidos pelo IEEE derivados das redes com fio. O padrão traz dois conceitos base, chamados de tipos de serviços, quais sejam:

1. BSS – Basic Service Set
2. ESS – Extended Service Set.

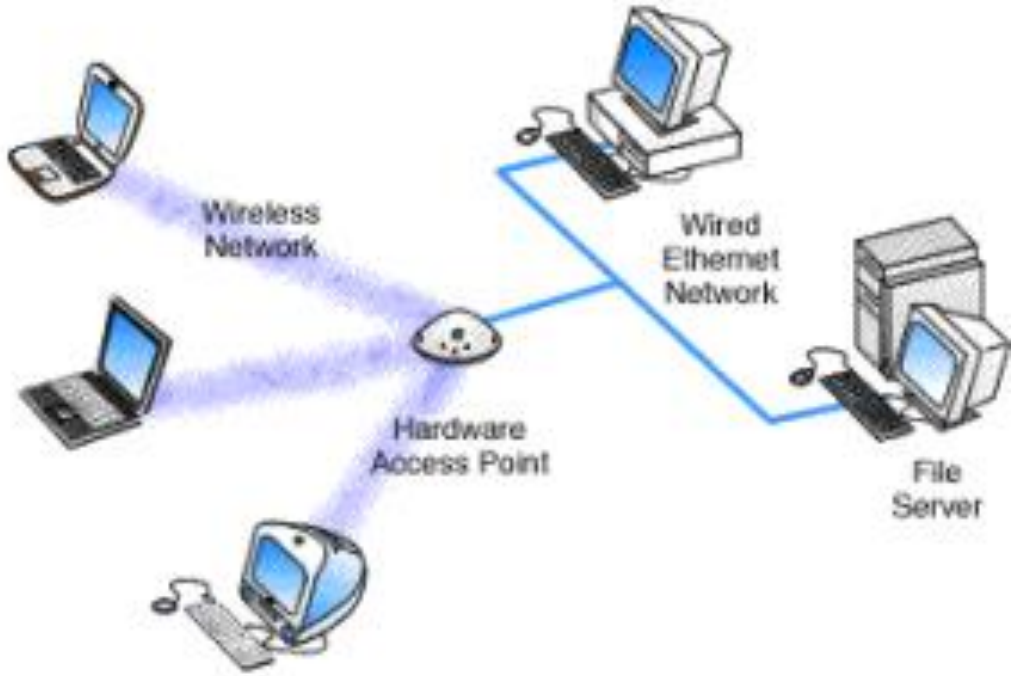
- Define-se como BSS a base de uma rede local sem fio, sendo formada por estações fixas ou móveis, e, opcionalmente, por uma estação-base central.

- Existem dois modos principais de operação das BSS's: Com ou sem estação base (ponto central).

- Nas redes com ponto central, segue a mesma analogia de uma topologia em estrela, em que toda a comunicação deve passar pelo nó central. Nesse caso, um destaque é que o nó central é obrigatório no contexto da autenticação e acesso à rede.

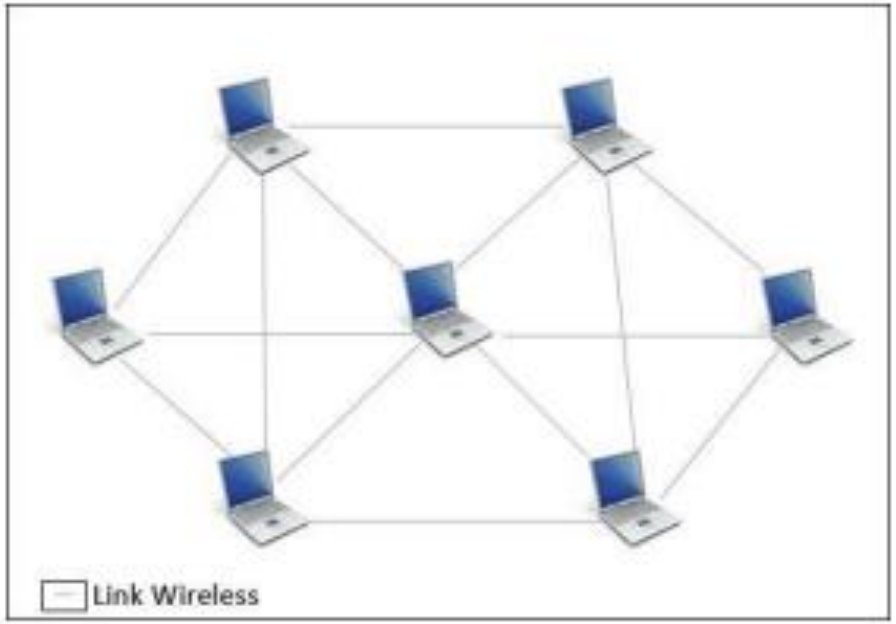
5. Redes Sem Fio

- Após a autenticação, os dispositivos dentro de uma mesma BSS podem se comunicar entre si diretamente. Geralmente, esse ponto é chamado de ponto de acesso (Access Point – AP ou Hotspot). A imagem abaixo mostra a representação de uma rede:



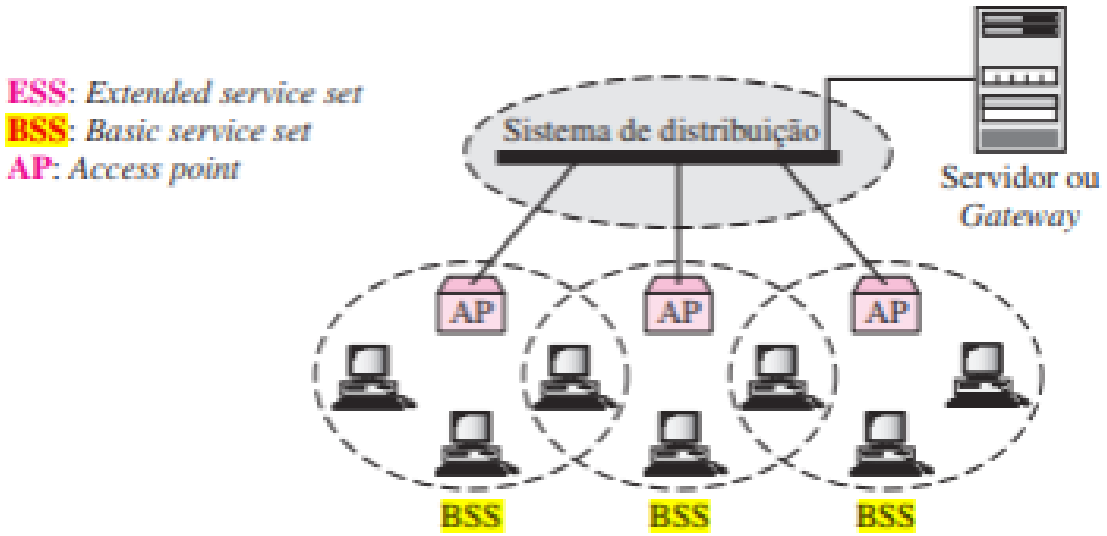
5. Redes Sem Fio

- Já nas redes que não utilizam um ponto de acesso, os dispositivos são capazes de se comunicarem diretamente entre si e de repassar a informação para outros dispositivos, fazendo o papel de roteadores de uma rede sem fio. Geralmente são chamados de redes ad hoc.



5. Redes Sem Fio

- Já as redes ESS são formadas por duas ou mais BSS's, necessariamente com pontos centrais ou AP's. A conexão entre as BSS's se dá justamente por um sistema de distribuição, que geralmente é uma rede local cabeada, entre os AP's. A imagem abaixo mostra um exemplo:



5. Redes Sem Fio

- Conforme já analisado, dentro de uma mesma BSS's, ainda que haja o ponto central, os dispositivos conversam entre si diretamente.

- Agora com múltiplas BSS's, no contexto de uma ESS, podemos ter equipamentos que estão em uma zona de alcance de duas BSS's, como os dispositivos da figura anterior.

- Nesse contexto, o IEEE 802.11 define três tipos de estação, dependendo da sua capacidade de mobilidade em uma rede WLAN:
- 1. **Sem transição** - Uma estação do tipo sem transição é fixa (não pode se movimentar) ou pode se movimentar apenas dentro da BSS.
- 2. **Transição inter-BSS** - Uma estação com mobilidade de transição inter-BSS pode se movimentar de uma BSS a outra, mas essa movimentação fica confinada ao interior de um mesmo ESS.
- 3. **Transição inter-ESS** - Uma estação com mobilidade de transição inter-ESS pode se movimentar de um ESS para outro. O protocolo não garante 100% segurança entre ESS diferentes.

6. Frequência de Redes Sem Fio

- Frequência é **quantas vezes uma onda se repete por segundo**. É medida em **Hertz (Hz).** Exemplo: 2.4 GHz = 2,4 bilhões de oscilações por segundo ou 5 GHz = 5 bilhões de oscilações por segundo.

- A tabela abaixo mostra as principais frequências utilizadas na maioria das redes sem fio:

Frequência	Característica
2.4 GHz	Mais alcance, mais interferência
5 GHz	Menor alcance, mais velocidade
6 GHz	Muito rápido, alcance ainda menor

6. Frequência de Redes Sem Fio

- A frequência baixa (2.4 GHz) tem MAIS alcance porque:

- **Maior Comprimento de Onda**: Ondas de baixa frequência têm ondas mais longas e espaçadas. Isso permite que elas contornem obstáculos como paredes, móveis e pessoas com mais facilidade (fenômeno de difração).

- **Menor Atenuação**: Ondas de baixa frequência perdem menos energia ao atravessar barreiras físicas. Ondas curtas (altas frequências) são mais facilmente absorvidas por paredes e sólidos.

6. Frequência de Redes Sem Fio

- A frequência baixa (2.4 GHz) tem MAIS Interferência porque:

- **Uso Saturado**: A frequência de 2.4 GHz é a "via única" para quase tudo. A maioria dos roteadores antigos, dispositivos de casa inteligente (IoT), micro-ondas, babás eletrônicas e dispositivos Bluetooth opera nesta faixa.

- **Poucos Canais Disponíveis:** A faixa de 2.4 GHz tem apenas 3 canais que não se sobrepõem (1, 6 e 11), o que causa congestionamento quando múltiplos roteadores próximos tentam usar o mesmo canal.

- **Interferência de Eletrodomésticos**: Fornos de micro-ondas operam em frequências muito próximas de 2.4 GHz, podendo gerar interferência direta quando estão em funcionamento.

6. Frequência de Redes Sem Fio

- Canal é uma parte (divisão) dentro da frequência, ou seja: Frequência é “faixa geral” e o Canal é a “subdivisão dentro dela”.

- Imagine uma rodovia, frequência é a estrada inteira e o canal são as faixas da estrada. Com isso, se muita gente usa a mesma faixa, gera trânsito (interferência).

- A banda 2.4 GHz tem canais variando de 1 até 11. Mas alguns deles se sobrepõe (gerando interferência). Por isso, o ideal é usar os canais: **1, 6 e 11 (esses canais não se sobrepõe)**