Redes de Computadores

Conceitos Básicos de Redes de Computadores

O que é uma rede?

Conjunto de equipamentos e softwares que possibilitam o compartilhamento de recursos e comunicação.

Tipos de rede

Podem variar em tamanho, forma e uso. Possuem a seguintes categorias:

- Redes pessoais
- Redes locais
- Redes metropolitanas
- Redes de longa distância

Redes Pessoais: Personal Area Network – PAN. Conecta os dispositivos em curta distância, geralmente utilizando Bluetooth. Atuam em distâncias muito pequenas.

LAN (rede local): Local Area Network. Muito utilizadas em locais pequenos como casas e escritórios. Geralmente são de propriedade privada.

Redes Metropolitanas: Metropolitan Area Network, MAN. conectam os dispositivos em distâncias maiores, geralmente na mesma cidade ou bairro. Interliga

LANS

Redes de longa distância: conectam dispositivos em distâncias geográficas em diferentes locais no mundo. Uma matriz em um continente e uma filial em outro. A WAN engloba várias outras LANs.

Topologias de rede

A topologia descreve o desenho físico de uma rede, como os dispositivos estão conectados a rede.

Topologia de barramento

Em uma topologia de barramento, cada dispositivo de rede é conectado a um único cabo de rede. Simples e limitado, sendo que quanto mais longo o barramento (cabo) principal maior a possibilidade de falhas na transmissão do sinal. Os dispositivos devem estar próximos, numa mesma sala, por exemplo.

Topologia de anel

Os dispositivos são conectados lado a lado formando um círculo (anel).

Topologia de malha

Pode ser malha física ou malha lógica. Todos os dispositivos se conectam entre si, na malha física.

A topologia de malha é descrita como uma malha física ou uma malha lógica. A malha lógica diz respeito ao fato de que atualmente, praticamente todas as redes utilizam essa percepção de malha.

Topologia em estrela

Tipo de topologia mais comum, onde cada dispositivo se liga a um HUB ou comutador, centralizando as conexões. Esses equipamentos podem ser interligados e estender a capilaridade das redes.

Padrões de Rede de Computadores

Ethernet

É o padrão do setor de redes, utilizado por redes LAN, MAN e WAN. Utiliza cabeamento de cobre e fibra óptica. Esse padrão define toda a estrutura para transmissão, tratamento de erros e desempenho, estipulando as regras para configuração de uma rede. Possui taxas de até 400 Gbps (Gigabits por segundo).

Fast Ethernet

A Fast Ethernet (IEEE 802.3 u) foi desenvolvida para dar suporte a velocidades de transmissão de dados de até 100 Mbps. A Fast Ethernet também é conhecida como padrão 100BASE-TX.

Gigabit Ethernet

Desenvolvida para dar suporte a redes de comunicação mais rápidas que, por sua vez, podem dar suporte a serviços como streaming multimídia e VoIP (voz sobre IP). O padrão 1000BASE-T é executado 10 vezes mais rápido do que o padrão 100BASE-TX. A Gigabit Ethernet agora está incluída nos padrões 802.3 e é recomendada para redes empresariais. O novo padrão é compatível com versões anteriores do 100BASE-T e os padrões 10BASE-T mais antigos.

10 Gigabit Ethernet

Trabalha com velocidades de transferência de dados de até 10 Gbps, utilizando fibra óptica.

Terabit Ethernet

Próximo padrão de redes que oferece velocidades de transferência de dados de 200 Gbps e 400 Gbps podendo ainda chegar a 800 Gbps e 1,6 Tbps no futuro.

Padrões de Rede

Embora os protocolos de rede forneçam um método unificado para comunicação, os padrões de rede regem o hardware e ao software que os utiliza. Os padrões de rede fornecem uma estrutura que permite a interoperabilidade entre os dispositivos.

Facilitam a comunicação e interligação entre os mais diferentes dispositivos de rede. São controlados por órgãos como ITU (International Telecommunication Union), o ANSI (American National Standards Institute) e o IEEE (Institute of Electrical and Electronics Engineers).

O padrão 802 abrange todos os padrões de rede física para redes Ethernet e sem fio.

Infraestrutura da rede

Vários dispositivos em conformidade com os padrões de rede compõem a estrutura de suas redes. Dependendo do tamanho da rede, você pode usar vários desses dispositivos para criar o backbone de sua rede. São eles:

- Repetidores
- Hubs
- Pontes

- Comutadores
- Roteadores

Repetidor

Um repetidor é um dispositivo de duas portas que repete sinais de rede. Os repetidores são usados quando os dispositivos de rede estão a alguma distância uns dos outros. O repetidor não modifica nem interpreta pacotes de dados antes de reenviá-los e não amplifica o sinal. Em vez disso, ele regenera o pacote de dados com intensidade original, bit a bit.

Ponte

Uma ponte divide uma rede em segmentos de rede e pode filtrar e encaminhar pacotes de dados entre esses segmentos. As pontes usam o endereço MAC do dispositivo de rede para decidir o destino do pacote de dados. Normalmente, uma ponte é usada para melhorar o desempenho da rede reduzindo o tráfego de rede desnecessário em segmentos de rede.

Hub

Um hub atua como um repetidor multiporta em uma rede. Os hubs são usados para conectar mais de um dispositivo e estruturar o layout de uma rede. Um hub pode operar somente com uma velocidade, que é a velocidade do dispositivo de rede mais lento na rede. Ele não interpreta nem filtra pacotes de dados e envia cópias de cada pacote de dados para todos os dispositivos anexados.

Tipos de hubs

- **Fast Ethernet:** é usado para redes de 100 Mbps e é fornecido como hubs de Classe I e Classe II. A principal diferença entre eles é o atraso na transmissão de dados.

- **Velocidade dupla:** com uma rede de hub tradicional, a velocidade da rede era regida pelo dispositivo de rede mais lento conectado. Por exemplo, se você tivesse dispositivos de 10 Mbps e 100 Mbps conectados a uma rede, a velocidade da rede inteira seria de apenas 10 Mbps.

Comutador

Uma opção combina a funcionalidade de uma ponte e um hub. Ela segmenta redes e pode interpretar e filtrar dados de pacote para enviá-los diretamente a um dispositivo de rede anexado.

Recursos

Os comutadores modernos baseados em Ethernet oferecem mais funcionalidade e recursos do que um hub Ethernet.

- Um comutador Ethernet pode ajustar a velocidade de conexão de um pacote de entrada para corresponder à velocidade da conexão da rede de destino.

- Hoje, muitos comutadores possuem suporte a PoE (Power over Ethernet), sistema que permite que dispositivos de rede como telefones VoIP (voz sobre IP) obtenham energia do comutador sem a necessidade de uma fonte de alimentação separada.

- Outros módulos podem ser anexados ao comutador para habilitar funções como espelhamento de porta, farejadores de pacotes e sistemas de detecção de intrusões.

Tipos de comutador Ethernet

Os dois tipos diferentes de comutador são gerenciados e não gerenciados.

- **Não gerenciado:** não permite configuração e é utilizado em ambientes menores como casas e empresas pequenas>

- **Gerenciado**: dá maiores possibilidades ao usuário uma vez que pode ser configurado e ajustado.

O que pode ser configurado:

- Qualidade de Serviço: gerencie o tráfego de LAN para que os sistemas críticos tenham prioridade mais alta. Um exemplo são os pacotes de dados de voz, que precisam ser entregues rapidamente.

- LANs virtuais: crie grupos lógicos de dispositivos em sua LAN virtual. O tráfego em uma LAN virtual não atravessa para outra LAN virtual. Esse grupo lógico de dispositivos pode aprimorar a segurança e o desempenho da rede.

- STP (Spanning Tree Protocol): aumente a resiliência de sua rede definindo rotas de rede alternativas para o caso de falha de um cabo ou dispositivo.

- Espelhamento de porta: use com um analisador de rede para diagnosticar problemas e falhas de rede. Durante a configuração, o comutador exporta uma cópia do tráfego de rede para uma porta.

- Limitação da taxa de largura de banda: permite o controle fino da largura de banda usada por portas específicas, como largura de banda alta para portas que trabalham com banco de dados ou VoIP e larguras de banda menores para e-mail.

- Filtragem de endereço MAC: permite controlar quais dispositivos de rede podem ser usados ou ter acesso pelo comutador.

- Cliente SNMP: configure e ajuste o SNMP com suas ferramentas de monitoramento de rede.

Há dois subtipos de comutador gerenciado:

- **Inteligente**: opção intermediária entre um comutador não gerenciado e um gerenciado. Oferece uma interface baseada na Web para gerenciar a configuração. As opções disponíveis são LANs virtuais, espelhamento de porta e limitação de taxa de largura de banda.

- **Enterprise**: o serviço de comutador totalmente gerenciado descrito acima.

Roteador

Realizam a vinculação das redes de diferentes alcances. Interpretam e filtram os pacotes de dados, encaminhando-os para as redes corretas. Utilizam o IP do dispositivo para alcançar seu destino. Denominado também como Gateway. Possuem uma "tabela de roteamento" contendo uma lista com as rotas preferenciais entre as redes.

Tipos

A maioria dos roteadores usa o BGP para compartilhar informações de roteamento. O tipo das informações compartilhadas depende do uso do roteador e das funções usadas.

Há várias classificações ou tipos diferentes de roteadores disponíveis para atender a diferentes necessidades de rede.

- **Roteadores de acesso:** normalmente usados em ambientes residenciais ou em escritórios pequenos, esses roteadores tendem a ser dispositivos de baixo custo que atendem a necessidades de roteamento simples.

- **Roteadores de distribuição:** esses roteadores compilam dados de roteamento de tráfego de vários roteadores. Os roteadores de distribuição vêm com capacidade de processamento e memória mais significativa. Esse tipo de roteador tem a finalidade de manter enormes quantidades de informações de roteamento. Eles costumam ser usados para gerenciar e controlar a qualidade do serviço em uma WAN.

- **Roteadores de borda**: um roteador de borda opera no limite entre sua rede e outras redes. Eles atuam como gateways para filtrar o tráfego e roteá-lo internamente ou encaminhá-lo com base no cabeçalho do pacote. Um roteador de borda geralmente tem controle de acesso ou firewalls para aprimorar a segurança. Ele também pode manipular serviços DHCP e DNS.

- **Roteadores de núcleo**: são projetados para larguras de banda maiores. São usados para conectar diferentes prédios ou locais geográficos. Os roteadores de núcleo tendem a ter menos recursos do que os roteadores de borda, pois seu foco principal é minimizar a perda de pacotes e impedir congestionamentos. Eles tendem a fazer encaminhamento de pacotes para roteadores de borda.

Protocolos de Comunicação

Protocolos de rede

Conjunto de condições e regras que especificam como os dispositivos de rede se comunicam em uma determinada rede. Ele fornece a estrutura padrão para estabelecer e manter um canal de comunicação e tratar erros ou falhas, caso eles ocorram. Os protocolos de rede permitem a comunicação entre diferentes dispositivos habilitados para rede.

Endereço de rede

Identificador único que identifica um dispositivo em uma rede de computadores.

Tipos:

- Endereço MAC (controle de acesso à mídia), que identifica o adaptador de rede no nível do hardware.

- Endereço IP (Internet Protocol), que identifica o adaptador de rede no nível do software.

Pacote de dados

Unidade que descreve uma mensagem trocada entre dois dispositivos em uma rede. Um pacote de dados é composto por dados brutos, cabeçalhos e, potencialmente, um trailer.

Datagrama

Um datagrama é considerado o mesmo que um pacote de dados. Os datagramas normalmente se referem a pacotes de dados de um serviço não confiável, em que a entrega não pode ser garantida.

Roteamento

Mecanismo que realiza a verificação nos pacotes de dados assegurando que seguem o caminho de entrega correto entre os dispositivos de envio e de recebimento em redes diferentes.

Protocolos

Diversos aplicativos, dispositivos e serviços utilizam protocolos de rede específicos. Podemos ter três categorias de protocolos:

- Protocolos de comunicação de rede
- Protocolos de segurança de rede
- Protocolos de gerenciamento de rede

Protocolos de comunicação de rede

- Protocolo TCP: o TCP agrupa dados em pacotes de dados que podem ser enviados de maneira segura e rápida, minimizando a chance de perda de dados. Ele fornece um mecanismo estável e confiável para a entrega de pacotes de dados em uma rede baseada em IP. Embora o TCP seja um protocolo eficaz voltado à conexão, ele gera sobrecarga.

- Protocolo IP: o IP é responsável pelo endereçamento de um pacote de dados. Ele encapsula o pacote de dados a ser entregue e adiciona um cabeçalho de endereço. O cabeçalho contém informações sobre os endereços IP do remetente e do destinatário. Esse protocolo não está preocupado com a ordem na qual os pacotes são enviados ou recebidos. Ele também não garante que um pacote será entregue, apenas o endereço.

- Protocolo UDP: UDP é um protocolo sem conexão que oferece uma implementação de baixa latência e tolerante a perda. Ele é usado com processos que não precisam verificar se o dispositivo do destinatário recebeu um datagrama.

Protocolos de comunicação

- Protocolo HTTP: o protocolo HTTP usa TCP/IP para fornecer conteúdo de página da Web de um servidor para seu navegador. O HTTP também pode lidar com o download e o upload de arquivos de servidores remotos.

- Protocolo FTP: é usado para transferir arquivos entre computadores diferentes em uma rede. Normalmente, o FTP é usado para carregar arquivos em um servidor de uma localização remota. Embora você possa usar o FTP para baixar arquivos, os downloads baseados na Web normalmente são tratados pelo HTTP.

- Protocolo POP3: o POP3 é um dos três protocolos de email. Ele é mais usado por um cliente de email para permitir o recebimento de emails. Esse protocolo usa TCP para o gerenciamento e a entrega de emails.

- Protocolo SMTP: o SMTP é outro dos três protocolos de email. Ele é mais usado para enviar emails de um cliente de email por meio de um servidor de email. Esse protocolo usa o TCP para gerenciamento e transmissão do email.

- Protocolo IMAP: o IMAP é o mais poderoso dos três protocolos de email. Com o IMAP e um cliente de email, você pode gerenciar uma caixa de correio em um servidor de email de sua organização.

Protocolos de segurança de rede

- Protocolo SSL: o SSL é um protocolo de criptografia e segurança padrão. Ele fornece uma conexão segura e criptografada entre seu computador e o servidor ou o dispositivo de destino que você acessou pela Internet.

- Protocolo TLS: o TLS é o sucessor do SSL e fornece um protocolo de criptografia de segurança mais forte e mais robusto. Com base no padrão IETF (Internet Engineering Task Force), ele foi projetado para impedir a falsificação e a adulteração de mensagens e a espionagem. Normalmente, ele é usado para proteger comunicações de navegador da Web, de email, de VoIP e de mensagens instantâneas. Embora o TLS seja usado atualmente, o protocolo de segurança substituto ainda costuma ser chamado de SSL.

- Protocolo HTTPS: o HTTPS fornece uma versão mais segura do protocolo HTTP padrão usando o padrão de criptografia TLS ou SSL. Essa combinação de protocolos garante que todos os dados transmitidos entre o servidor e o navegador da Web sejam criptografados e protegidos contra espionagem ou detecção de pacotes de dados. O mesmo princípio é aplicado aos protocolos POP, SMTP e IMAP listados anteriormente para criar versões seguras conhecidas como POPS, SMTPS e IMAPS.

- SSH (Secure Shell): o SSH é um protocolo de segurança de rede criptográfico que fornece uma conexão de dados segura em uma rede. O SSH tem a finalidade de dar suporte à execução de instruções de linha de comando, incluindo a autenticação remota para servidores. O FTP usa muitas das funções do SSH para fornecer um mecanismo de transferência de arquivos seguro.

- Kerberos: este protocolo de validação fornece uma autenticação robusta para aplicativos baseados em cliente e servidor por meio da criptografia de chave secreta. O Kerberos pressupõe que todos os pontos de extremidade na rede são desprotegidos. Ele impõe criptografia forte a todas as comunicações e dados a todo momento.

Protocolos de gerenciamento de rede

Dois protocolos de gerenciamento de rede estão disponíveis:

- Protocolo SNMP: o SNMP é um protocolo de Internet que permite coletar dados dos dispositivos em sua rede e gerenciar esses dispositivos. O dispositivo precisa dar suporte a SNMP para coletar informações.

- Protocolo ICMP: o ICMP é um dos protocolos incluídos no IPS (Pacote de Protocolos de Internet). Ele permite que os dispositivos conectados à rede enviem mensagens de aviso e de erro, bem como informações de operação sobre o êxito ou a falha de uma solicitação de conexão ou se um serviço não está disponível. Ao contrário de outros protocolos de transporte de rede, como UDP e TCP, o ICMP não é usado para enviar nem receber dados de dispositivos na rede.

Modelo TCP/IP

- Camada de aplicativo: a camada superior dessa pilha trata da comunicação do aplicativo ou do processo. A camada de aplicativo é responsável por determinar quais protocolos de comunicação são usados com base no tipo de mensagem transmitida. Por exemplo, a camada atribuirá os protocolos de email corretos, como POP, SMTP ou IMAP, se a mensagem for um conteúdo de email.

- Camada de transporte: essa camada é responsável pela comunicação de host para host na rede. Os protocolos associados a essa camada são TCP e UDP. O TCP é responsável pelo controle de fluxo. O UDP é responsável por fornecer um serviço de datagrama.

- Camada de Internet: essa camada é responsável pela troca de datagramas. Um datagrama contém os dados da camada de transporte e adiciona os endereços IP de origem e do destinatário. Os protocolos associados a essa camada são IP, ICMP e IPsec (Internet Protocol Security Suite).

- Camada de acesso à rede: a camada inferior dessa pilha é responsável por definir como os dados são enviados pela rede. Os protocolos associados a essa camada são ARP, MAC, Ethernet, DSL e ISDN.

Gerenciamento de Redes de Computadores

Gerenciar diz respeito a controlar as atividades e monitorar a utilização dos recursos em um ambiente de rede. As tarefas básicas são: obter informações da rede, tratar as informações obtidas e encaminhar soluções para os problemas encontrados.

O cumprimento dos objetivos exige que funções de gerência sejam embutidas nos vários componentes da rede, permitindo assim a detecção, prevenção e reação aos problemas que venham a ocorrer.

Um sistema de gerenciamento é formado por um conjunto de ferramentas para monitoramento e controle de rede atuando de forma integrada.

As aplicações que são utilizadas para realização do gerenciamento são residentes em computadores hospedeiros e nos processadores de comunicação, switches e roteadores, por exemplo.

Softwares de gerenciamento genéricos são compostos por elementos gerenciados, agentes, gerentes, bancos de dados, protocolos, interfaces para softwares e usuários.

Toda a arquitetura contida nos softwares de gerenciamento reside no software gerente e nos agentes, variando com a funcionalidade da plataforma adotada. O software pode ser classificado como apresentação, a interface, de gerenciamento (aplicação) e de suporte (BD e comunicação).

Pelo menos uma estação por rede gerenciada, atuará como gerente, sendo essa a responsável por monitorar e controlar os dispositivos gerenciáveis, os agentes. Um agente reside nos dispositivos gerenciáveis: switches, roteadores, estações de trabalho, por exemplo, e são responsáveis pelo controle dos dispositivos do ambiente em que estão instalados.

Os gerentes realizam as requisições aos agentes e estes respondem às requisições com o que foi solicitado, agindo em conjunto.

A gerência pode ser classificada como **centralizada**, com o controle sendo realizado por uma única estação e gerência **distribuída**, com o controle sendo realizado por diversas estações distribuídas pela rede.

No ambiente de gerência centralizada, apenas uma estação, o gerente, realiza todo o controle do gerenciamento, enviando as requisições aos agentes, que respondem a essas solicitações.

No modelo distribuído, o controle é descentralizado em domínio de gerência, que são bem definidos e controlados por um gerente. Cada gerente então gerencia as informações apenas em seu próprio domínio, repassando para o gerente dos gerentes as requisições globais.

A ISO definiu uma estrutura da informação de gerenciamento a ser armazenada em base de dados, podendo assim as operações serem tratadas em decorrência dessas operações.

A definição da estrutura da informação de gerenciamento que será gravada em um BD, é denominada de **SMI**, **Structure Management Information**, proposta pela ISO. Na definição desta estrutura, a ISO utilizou uma abordagem orientada a objetos, caracterizando os recursos do sistema como objetos gerenciados definidos através de seus atributos, das operações a que podem ser submetidos e das notificações que podem ser emitidas.

Gerência de falhas

Falhas e erros não são a mesma coisa! Uma falha é uma condição anormal, causada por operações incorretas ou um grande número de erros. Certos erros como, por exemplo, um bit errado em uma linha de comunicação, podem ocorrer ocasionalmente e normalmente não são considerados falhas.

Cada um dos componentes essenciais deve ser monitorado individualmente, garantindo assim seu perfeito funcionamento. Quando houver uma falha deve-se rapidamente:

- Determinar o componente exato onde a falha ocorreu;
- Isolar a falha do resto da rede, para que ela continue a funcionar sem interferências;
- Reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou;
- Reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

Gerência de Configuração (Configuration)

O gerenciamento de configuração está relacionado à inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado às tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e da situação dos componentes durante a operação da rede.

O gerente da rede deve ser capaz de identificar os componentes da rede e definir a conectividade entre eles, além de modificar a configuração em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou para atender às necessidades dos usuários.

Gerência de Contabilização (Accounting)

Mesmo sem que haja cobrança pela utilização dos recursos de rede, é papel do administrador da rede controlar o uso dos recursos por usuários ou grupos de usuários, tendo como objetivos:

- Evitar que um usuário ou grupo abuse de seus privilégios de acesso e monopolize a rede, em detrimento de outros usuários;

- Evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e garantindo a desempenho da rede;

- Conhecer as atividades dos usuários com detalhes suficientes para planejar o crescimento da rede.

Gerência de desempenho (Performance)

O gerenciamento do desempenho consiste na monitoração das atividades e controle dos recursos através de ajustes e trocas, possibilitando a obtenção de informações para avaliar o comportamento dos recursos da rede através de

determinados parâmetros como: nível de utilização, perfil de tráfego, vazão (throughput), existência de gargalos, tempo de resposta, latência (atrasos), jitter, disponibilidade, níveis de QoS (em redes MPLS), perdas de pacotes, entre outros.

Gerência de Segurança (Security)

O gerenciamento da segurança provê facilidades para proteger recursos da rede e informações dos usuários, que devem estar disponíveis apenas para usuários autorizados. É necessário que a política de segurança seja robusta e efetiva e que o sistema de gerenciamento da segurança seja, ele próprio, seguro [6].

O gerenciamento de segurança trata de questões como:

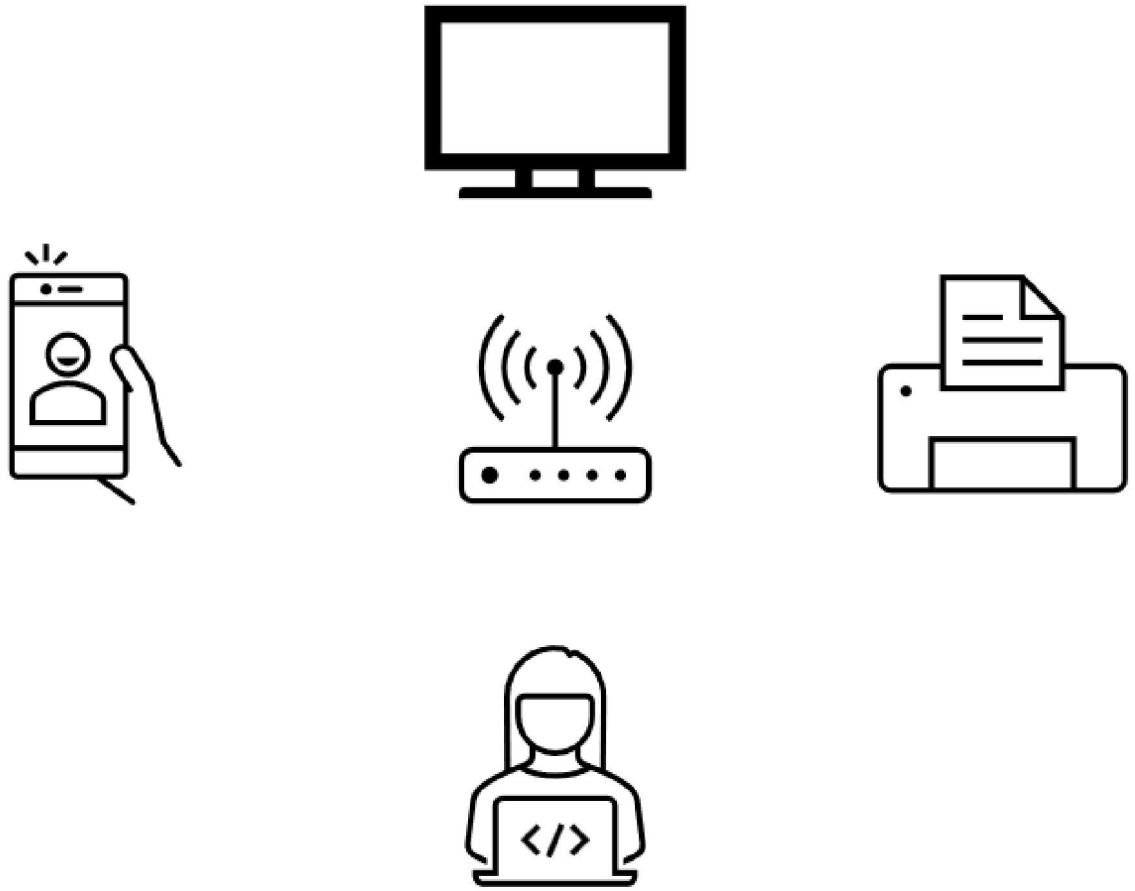
- Geração, distribuição e armazenamento de chaves de criptografia;
- Manutenção e distribuição de senhas e informações de controle de acesso;
- Monitoração e controle de acesso à rede ou parte dela e das informações obtidas dos nós da rede;
- Coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.

WiFi

Ao conectar seu dispositivo, notebook, ou smartphone em um restaurante ou hotel, ou instala o acesso a Internet em sua casa, você está utilizando uma rede sem fio WiFi. WiFi vem de Wireless Fidelity e quer dizer que o dispositivo conectado é compatível com o padrão 802.11, padrão determinado para redes sem fio.

Desde o ano de 1985 aproximadamente que a tecnologia 802.11 existe, sendo utilizada comercialmente apenas a partir dos anos 2000. Foi ainda nos anos 2000 que se iniciaram os testes WI-FI CERTIFIED em produtos 802.11b (trabalhando com 11 Mbps de dados brutos). Atualmente essas redes suportam velocidades, alcance e número de dispositivos conectados muito maiores.

As frequências de transmissão utilizadas pelas redes WiFi e seus dispositivos são de 2,4 GHz ou 5 GHz, sendo mais altas do que as frequências normalmente utilizadas para telefonia celular e rádio comunicadores do tipo "walkie-talkie", permitindo assim o transporte de uma maior quantidade de dados pelo sinal.



Evolução do Wi-Fi

Desde seu lançamento para os consumidores em 1997, os padrões de Wi-Fi têm evoluído continuamente – normalmente resultando em velocidades mais rápidas e maior cobertura. Com cada novo recurso vem uma mudança de nome para

diferenciar os padrões. À medida que os recursos são adicionados ao padrão IEEE 802.11 original, eles se tornam conhecidos por sua emenda (802.11b, 802.11g, etc.).

Padrões Wi-Fi

Veja a seguir uma lista com os padrões mais comuns do Wi-Fi. As letras indicam uma variação da tecnologia original e representam velocidades, frequência de rádio e outras especificações diferentes entre cada uma delas:

- **802.11a** transmite a 5 GHz e pode atingir velocidades sem fio de até 54 Mbps. A banda de 5 GHz é menos congestionada que a popular de 2,4 GHz; isso significa que há menos interferência – o que se traduz em melhor desempenho para atividades como voz e vídeo HD. O rádio necessário para o equipamento sem fio 802.11a é mais caro; por esse motivo, não é compatível com a maioria dos dispositivos domésticos.

- **802.11b** é o padrão Wi-Fi mais lento e mais barato. Ele transmite na banda de frequência de 2,4 GHz e pode lidar com velocidades de até 11 Mbps. Por algum tempo, o baixo custo do 802.11b o tornou a escolha popular para redes domésticas, mas desde então foi substituído pelas tecnologias 802.11g e 802.11n.

- **802.11g** também transmite na banda de 2,4 GHz como o 802.11b, mas em velocidades muito mais rápidas. O 802.11g é capaz de velocidades de até 54 Mbps (embora as velocidades do mundo real normalmente registrem em torno de 24 Mbps).

- **802.11n** é como o padrão Wi-Fi predominante no mercado hoje. Aumenta significativamente a velocidade e o alcance em comparação com 802.11ge 802.11b. O 802.11n pode teoricamente atingir velocidades de até 140 Mbps.

- **802.11ac** é basicamente uma versão atualizada do 802.11n. Sua velocidade máxima teórica é de apenas 7 Gbps. No entanto, as velocidades máximas da vida real estão mais próximas de 1,3, que ainda é duas vezes mais rápida que uma rede Wi-Fi hoje. Os primeiros roteadores 802.11ac surgiram em janeiro de 2012, e o padrão ainda está surgindo.

Características de cada padrão:

802.11b

O 802.11b usou a mesma frequência de 2,4 GHz que o padrão 802.11 original. Ele suportava uma taxa teórica máxima de 11 Mbps e tinha um alcance de até 45,72 metros.

Os componentes 802.11b eram baratos, mas o padrão tinha a velocidade máxima mais lenta de todos os padrões 802.11. E como o 802.11b operava em 2,4 GHz, eletrodomésticos ou outras redes Wi-Fi de 2,4 GHz podem causar interferência.

Eventualmente, o padrão 802.11n (o que se tornaria o Wi-Fi 4) veio para substituir o 802.11a, 802.11be 802.11g como o novo padrão de rede local (WLAN). (Mais sobre Wi-Fi 4 posteriormente.) Roteadores que suportam apenas 802.11n não são mais fabricados.

802.11a

Por que o 802.11b veio antes do 802.11a?

A emenda 'a' ao padrão foi lançada ao mesmo tempo que o 802.11b. Mas introduziu uma técnica mais complexa, conhecida como OFDM (multiplexação por divisão de frequência ortogonal) para gerar o sinal sem fio. Em outras palavras, o 802.11a oferecia algumas vantagens sobre o 802.11b:

- Operou na banda de frequência de 5 GHz menos lotada, tornando-a menos propensa a interferências.

- Sua largura de banda era muito maior que 802.11b, com um máximo teórico de 54 Mbps.

Você provavelmente não encontrou muitos dispositivos ou roteadores 802.11a. Isso porque os dispositivos 802.11b eram mais baratos e se tornaram mais populares no mercado consumidor. O 802.11a foi usado principalmente em aplicações de negócios.

802.11g

O padrão 802.11g usou a mesma tecnologia OFDM introduzida com o 802.11a. Assim como o 802.11a, ele suportava uma taxa teórica máxima de 54 Mbps. Mas, como o 802.11b, ele operava na frequência lotada de 2,4 GHz (e, portanto, estava sujeito aos mesmos problemas de interferência do 802.11b). 802.11g era compatível com dispositivos 802.11b: um dispositivo 802.11b poderia se conectar a um ponto de acesso 802.11g (mas em velocidades 802.11b).

Com o 802.11g, os consumidores desfrutaram de um avanço significativo nas velocidades e cobertura do Wi-Fi. Ao mesmo tempo, os roteadores sem fio de consumo estavam ficando melhores, com maior potência e melhor cobertura do que as gerações anteriores.

802.11n (Wi-Fi 4)

Com o padrão 802.11n, o Wi-Fi ficou ainda mais rápido e confiável. Ele suportava uma taxa de transferência máxima teórica de 300 Mbps (e poderia atingir até 450 Mbps ao usar três antenas).

O 802.11n usava MIMO (*Multiple Input Multiple Output*) onde vários transmissores/receptores podiam operar simultaneamente em uma ou ambas as extremidades do link para um único dispositivo. Isso proporcionou um aumento

significativo nos dados sem precisar de uma largura de banda ou potência de transmissão mais alta. 802.11n operado nas bandas de 2,4 GHz e 5 GHz

802.11ac (Wi-Fi 5)

Wi-Fi superalimentado 802.11ac, com velocidades que variam de 433 Mbps até vários Gigabits por segundo. Para obter esse tipo de desempenho, o 802.11ac:

- Trabalhou exclusivamente na banda de 5 GHz
- Suporta até oito fluxos espaciais (em comparação com os quatro fluxos do 802.11n)
- Dobrou a largura do canal até 80 MHz
- Usou uma tecnologia chamada beamforming

Com o beamforming, as antenas basicamente transmitem os sinais de rádio, então eles são direcionados para um dispositivo específico.

Outro avanço significativo com o 802.11ac foi o MIMO multiusuário (MU-MIMO). Enquanto o MIMO direciona vários fluxos para um único cliente, o MU-MIMO pode direcionar os fluxos espaciais para vários dispositivos simultaneamente.

Embora o MU-MIMO não aumente a velocidade para um único cliente, ele pode aumentar a taxa de transferência geral de dados de toda a rede.

O Wi-Fi 5 foi um grande passo para a evolução do Wi-Fi. Agora, o Wi-Fi está dando outro grande salto de 5 para 6.

Wi-Fi 6 (802.11ax)

O padrão Wi-Fi de última geração é o Wi-Fi 6. Estávamos acostumados com o Wi-Fi 5 sendo sobrecarregado com as mudanças, e agora o Wi-Fi 6 oferece ainda mais.

As características a saber sobre o mais novo padrão é que o Wi-Fi 6:

- Tem melhorias semelhantes ao 5G.
- Evita o congestionamento do tráfego em espaços públicos.
- Oferece taxas de dados e capacidade mais altas, até 9,6 Gbps.
- Oferece melhor suporte ao espectro de 2,4 GHz e 5 GHz.
- Oferece aumento de multiusuário, entrada múltipla, saída múltipla (MU-MIMO) de 4 x 4 para 8 x 8.
- No geral, promete um desempenho melhor e mais rápido.
- Permite conectar ainda mais dispositivos em sua casa.

Ao contrário dos padrões anteriores, o Wi-Fi 6 permite que um roteador lide com mais antenas. O que significa que um roteador pode se conectar a mais dispositivos. O Wi-Fi 6 foi projetado para tornar a internet sem fio melhor em residências e em público.

Taxas de Transferência

Todos os padrões 802.11 tem suas medições de taxas de transferência máximas alcançáveis realizadas em condições ideais ou em taxas de dados da camada de enlace. Porém, em configurações típicas onde os dados são normalmente transferidos entre dois dispositivos, onde um está conectado a uma infraestrutura com fio e outro em uma sem fio.

Sendo assim, os quadros trafegam por um meio 802.11 (WLAN) e são convertidos para 802.3 (ETHERNET) e vice-versa. Por causa da diferença existente nos

comprimentos dos quadros dessas duas mídias, a velocidade de transferência será definida pelo tamanho do pacote do aplicativo. Assim sendo, aplicativos cujos pacotes são menores criam fluxo de dados de alta sobrecarga (baixo *goodput*). Velocidade de transmissão dos pacotes pelo aplicativo, potência de sinal (saída e recepção) e distância são outros fatores que contribuem para a taxa de dados geral.

As frequências dos canais 802.11

Canais	Espectro
802.11b, 802.11g e 802.11n-2.4	2.400–2.500 GHz
802.11a, 802.11ne 802.11ac	2,4 GHz e 5 GHz

Datagramas

Chamamos de quadros os datagramas da rede. Nos padrões atuais do 802.11 os tipos de quadros que serão utilizados na transmissão de dados e para o gerenciamento e controle de links sem fio são especificados pelo próprio padrão.

Cada quadro é dividido em seções específicas, consistindo em um cabeçalho MAC, carga útil e sequência de verificação de quadro (FCS). Veja a representação de um quadro abaixo:

Campo	Controle de quadro	Duração	Endereço 1	Endereço 2	Endereço 3	Controle de sequência	Endereço 4	Controle de QoS	Controle de HT	Corpo da moldura	Seq. de verific. do quadro
Comprimento (bytes)	2	2	6	6	6	0 ou 2	4	0 ou 2	0 ou 4	Variável	4

Os primeiros dois bytes do cabeçalho MAC formam um campo de controle de quadro especificando a forma e a função do quadro. Este campo de controle de quadro é subdividido nos seguintes subcampos:

- Versão do protocolo: dois bits que representam a versão do protocolo. A versão do protocolo usado atualmente é zero. Outros valores são reservados para uso futuro.

- Tipo: Dois bits que identificam o tipo de quadro WLAN. Controle, dados e gerenciamento são vários tipos de quadro definidos no IEEE 802.11.

- Subtipo: quatro bits que fornecem discriminação adicional entre os quadros. Tipo e Subtipo são usados juntos para identificar o quadro exato.

- ToDS e FromDS: Cada um tem um bit de tamanho. Eles indicam se um quadro de dados se dirige a um sistema de distribuição. Os quadros de controle e gerenciamento definem esses valores como zero. Todos os quadros de dados terão um desses bits definido. No entanto, a comunicação dentro de uma rede de conjunto de serviço básico independente (IBSS) sempre define esses bits como zero.

- More Fragments: O bit More Fragments é definido quando um pacote é dividido em vários quadros para transmissão. Cada quadro, exceto o último quadro de um pacote, terá esse conjunto de bits.

- Repetir: Às vezes, os quadros exigem retransmissão e, para isso, há um bit de Repetição que é definido como um quando um quadro é reenviado. Isso ajuda na eliminação de quadros duplicados.

- Gerenciamento de energia: Este bit indica o estado de gerenciamento de energia do remetente após a conclusão de uma troca de quadros. Os pontos de acesso são necessários para gerenciar a conexão e nunca definirão o bit de economia de energia.

- More Data: O bit More Data é usado para buffer de frames recebidos em um sistema distribuído. O ponto de acesso usa esse bit para facilitar as estações no

modo de economia de energia. Indica que pelo menos um quadro está disponível e endereça todas as estações conectadas.

- Quadro protegido: O bit do Quadro protegido é definido como um se o corpo do quadro for criptografado por um mecanismo de proteção como Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) ou Wi-Fi Protected Access II (WPA2).

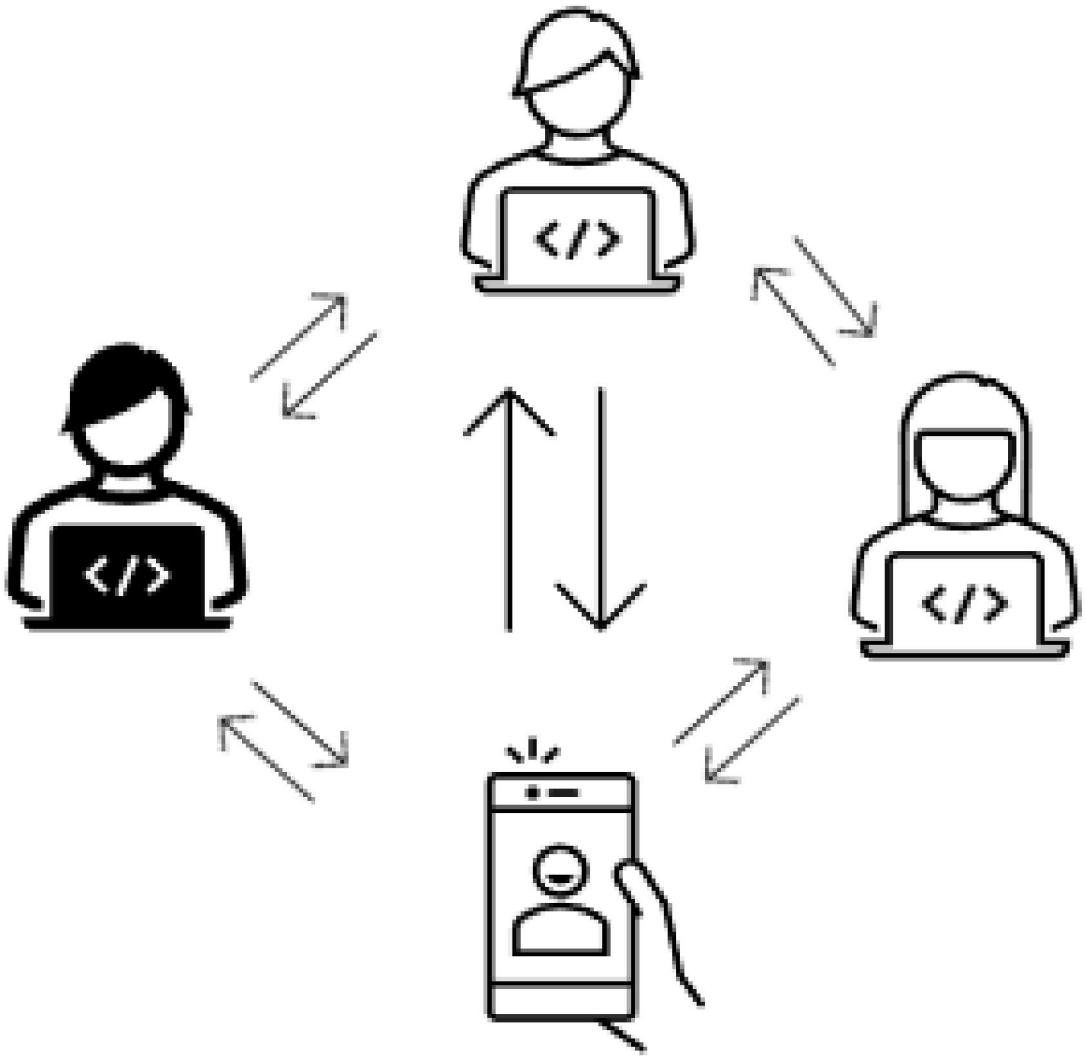
- Pedido: Este bit é definido apenas quando o método de entrega "pedido estrito" é empregado. Quadros e fragmentos nem sempre são enviados em ordem, pois isso causa uma penalidade no desempenho de transmissão.

Tipos de Rede

Veja a seguir, os tipos de rede do padrão 802.11.

Independent Basic Service Set (IBSS ou Ad hoc)

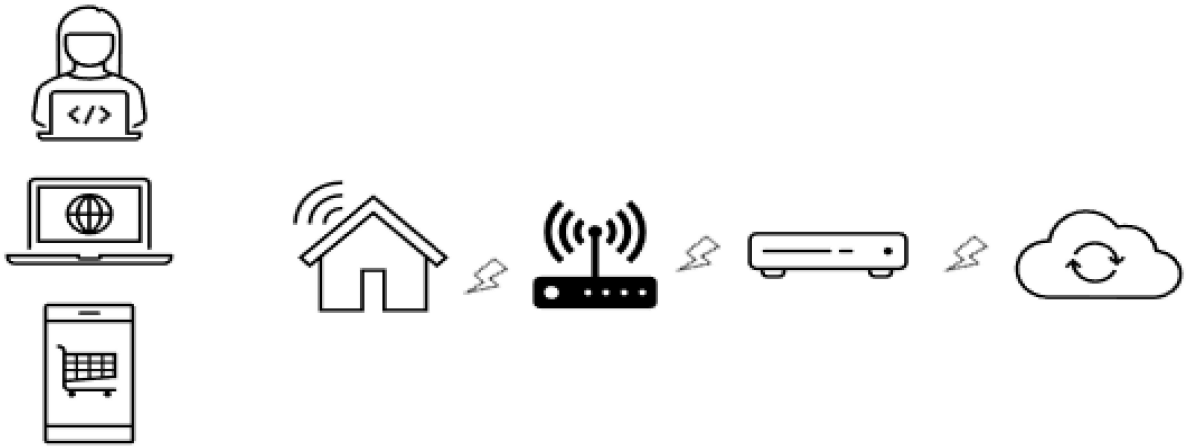
Uma rede IBSS consiste em pelo menos duas estações, onde não há ponto de acesso que conecte a rede a um sistema de distribuição. Essa rede também é conhecida como uma rede sem fio Ad-hoc.



Basic Service Set (BSS)

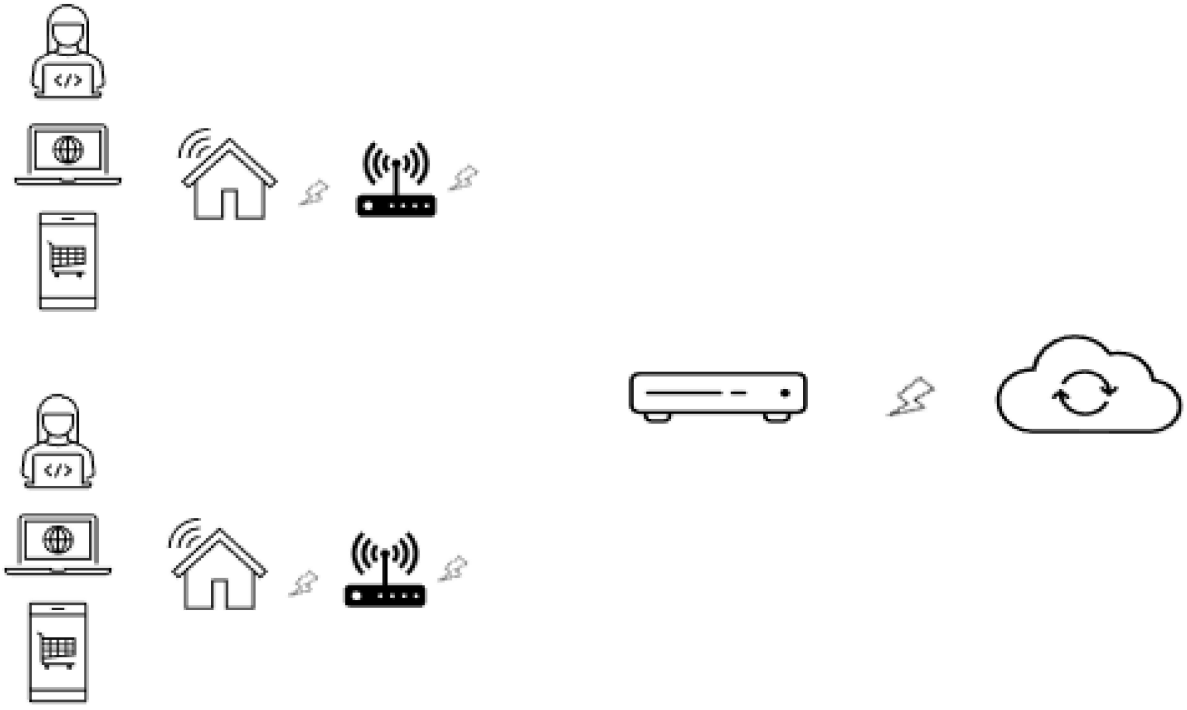
Uma rede BSS consiste em um simples Access Point (AP) que suporta um ou mais clientes sem fio. Essa rede é também conhecida como Infrastructure Wireless Network (Rede Infra-estrutura). Nessa rede todas as estações se comunicam entre si através de um AP. Esse tipo de rede tem o inconveniente de consumir o dobro da banda, mas um dos grandes benefícios é o armazenamento dos dados enquanto as estações estão em modo de economia de energia (Power Save).

O AP provê conectividade entre as estações e a rede cabeada e fornece também funcionalidade de bridge quando uma estação inicia a comunicação com outra estação ou com um nó do sistema de distribuição (Distribution System - DS).



Extended Service Set (ESS)

Uma rede ESS é constituída por dois ou mais AP's conectados na mesma rede cabeada que pertencem ao mesmo segmento lógico (subnet), separado por um roteador.



Distribution Systems (DS)

Os AP's de múltiplos BSS's são interconectados através do DS. Isso provê mobilidade, pois as estações podem mover-se de um BSS para outro BSS. Os AP's podem ser interconectados através da rede cabeada ou não. O DS é o componente

lógico usado para interconectar BSS's. O DS provê serviços que permitem o roaming entre as estações e os BSS's.

Modos de rede Wi-Fi

Rede ad hoc

Uma rede ad hoc sem fio (WANET) é um tipo de rede local (LAN) que é construída espontaneamente para permitir que dois ou mais dispositivos sem fio sejam conectados uns aos outros sem exigir equipamentos típicos de infraestrutura de rede, como um roteador sem fio ou ponto de acesso. Quando as redes Wi-Fi estão no modo ad hoc, cada dispositivo na rede encaminha dados que não se destinam a si mesmo para os outros dispositivos.

Os dispositivos na rede ad hoc requerem um adaptador ou chip de rede sem fio e precisam ser capazes de funcionar como um roteador sem fio quando conectados. Ao configurar uma rede sem fio ad hoc, cada adaptador sem fio deve ser configurado para o modo ad hoc em vez do modo de infraestrutura. Todos os adaptadores sem fio precisam usar o mesmo identificador de conjunto de serviços (SSID) e número de canais de frequência sem fio.

Rede Infraestrutura

Esse tipo de rede funciona assim:

Uma estação faz a identificação da rede sem fio e seus AP's disponíveis em sua área de cobertura. Utiliza-se a monitoração de quadros "anúncio" enviados dos AP's, ou também através do uso de "probe frames", quadros de sondagem vindos de uma rede WI-Fi privada.

A estação seleciona uma rede disponível e se autentica no AP. Realizada a autenticação, inicia-se processo de associação.

No processo de associação, o AP e a estação trocam informações e funcionalidades, podem essas informações ser compartilhadas com outros AP's na rede, disseminando a localização atual da estação na rede.

Apenas quando se completa a associação é que a estação poderá transmitir e receber dados na rede. Nesse modo, infraestrutura, passa pelo AP todo o tráfego das estações.

O gerenciamento do acesso a rede é realizado através do protocolo CSMA/CA (Carrier Sense Multiple Access - Collision Avoidance).

Quando no modo infraestrutura, o AP funciona sempre como receptor e transmissor. Como algumas estações podem não ser capazes de detectar as demais, deve-se tomar alguns cuidados para evitar colisões. Isso inclui um tipo de reconhecimento (reservation exchange) que pode ocorrer antes de um pacote de dados ser transmitido.

Normalmente utiliza-se o RTS (Request to Send) para a função de reconhecimento, além do NAV (Network Allocation Vector – Vetor Alocação de Rede) mantido para cada estação na rede sem fio. Assim, caso uma estação não consiga "escutar" a transmissão de outra, ela escutará o CTS emitido pelo próprio AP.

Protocolos para WLAN de Alta Velocidade

Estrutura de Camadas

É nas camadas físicas (PHY) de enlace (subcamada MAC) que as atividades do padrão 802.11 são realizadas, ficando ao encardo das camadas superiores controlar endereçamento, roteamento, integridade de dados, formato e sintaxe dos dados de cada pacote, sem diferenciar o meio em que eles estão sendo transportados.

Todas as atividades especificadas pelo padrão 802.11 acontecem nas camadas físicas (PHY) e de enlace (na subcamada MAC, especificamente), pois as camadas superiores controlam aspectos como endereçamento e roteamento, integridade de dados, sintaxe e formato dos dados contidos dentro de cada pacote, não fazendo diferença se elas estão transportando pacotes através de fios, de fibra óptica ou de sinais de rádio.

Camadas Física

Responsável pelo envio dos quadros no canal de comunicação. Existem três técnicas para transmissão de dados para as redes sem fio:

- Uma Infravermelho
- E duas radiofrequências (RF):
  - FHSS (Frequency Hopping Spread Spectrum)
  - DSSS (Direct Sequence Spread Spectrum).

Infravermelho

Utiliza-se como meio de transmissão raios próximos à luz visível. Essa técnica é restrita a ambientes fechados devido aos sinais infravermelhos não ultrapassarem paredes, e por estarem sujeitos a interferências.

Nesta técnica, são utilizados como. Pelo fato de os, esta técnica de transmissão é restringida a ambientes fechados, operando a 1Mbps ou 2 Mbps. Existem duas formas de realização das comunicações infravermelhas: reflexão (difusão) ou linha direta (direta).

FHSS (Frequency Hopping Spread Spectrum)

Utiliza como meio transmissão o rádio de alcance limitado, operando na banda ISM (Industrial Scientific and Medical) de 2,4 GHz. A banda de frequência é dividida em 79 canais de frequência com 1 MHz de largura, sendo que é gerada uma sequência pseudorrandômica destes canais, por onde o sinal é difundido.

Nessa técnica fez-se necessário o garantir o sincronismo de todas as estações, para que elas mudem para as mesmas frequências de forma simultânea, utilizando igualmente os canais da sequência.

DSSS (Direct Sequence Spread Spectrum)

Essa técnica também utiliza a radiofrequência como meio de transmissão, operando na banda ISM de 2,4 GHz. Nela, cada tempo de bit é dividido em "n" intervalos denominados de chips. Cada estação possui uma sequência pseudorrandômica de "n" bits, chamada sequência de chips. Para enviar o bit 1, uma estação envia uma sequência de chips. Para enviar o bit 0, é enviado o complemento de sua sequência de chips.

A PHY DSSS, segundo o padrão 802.11, usa uma sequência de 11 bits para espalhar os dados antes de transmiti–los. Cada bit transmitido é modulado por esta sequência. Este processo espalha a energia de radiofrequência em torno de uma banda de faixa larga que pode ser necessária para transmitir o dado. O receptor concentra o sinal de radiofrequência recebido para recuperar o dado original.

Como técnica de modulação esta camada utiliza para provimento em operações de 1Mbps a técnica DBPSK (Differential Binary Phase Shift Keying), enquanto que para operações em 2 Mbps a técnica usada é a DQPSK (Differential Quadrature Phase Shift Keying).

Bibliografia

KUROSE, J. F. e ROSS, K. **Redes de Computadores e a Internet** - 8ª Ed., Pearson, 2015.

Ir para exercício