Livro pagina 500 a 700

- DNS
    - Veio para substituir o arquivo hosts
    - Utiliza o UDP, pois manda um pacote e recebe outro
    - Função: traduzir nome para IP e vice versa
    - Domínios de nível superior se dividem em genéricos e de países
    - Registros de recursos formam o bando de dados DNS
    - Nomes de domínios são mapeados em registro de recursos
    - Registros de recursos possuem 5 campos:
        - Nome_dominio: informa o dominio que se aplica
        - Tempo de vida: indica a estabilidade do registro
        - Clase: sem um registro relacionado a internet
        - Tipo: SOA, A, AAAA, MX, NS, CNAME, PTR, SPF, SRV, TXT
        - Valor: depende do tipo de registro
    - Espaços de nome do DNS são divididos em zonas não sobrepostas
    - Cada zona está associada a um ou mais servidores de nomes
    - **A resolução de nomes** é o processo de pesquisa e localização de um endereço
    - A resolução de nomes pode retornar registros oficiais ou em cache
        - Pode ser feita por consulta interativa ou recursiva
    - Exemplo de consulta DNS
        - Originador consulta o servidor de nomes local
        - Servidor de nomes local consulta servidor de nomes raiz
        - Este retorna o domínio raiz que o endereço se encontra
        - Servidor de nomes local consulta cada sub domínio até encontrar o servidor de nomes onde se encontra o endereço pesquisado
        - Servidor de nomes local retorna para o originador
- Correio
    - A arquitetura do sistema consite em dois subsistemas
        - Agentes do usuário
        - Servidores de correio
            - Implementam fila de mensagens
            - Caixa postais
    - As mensagens de correio distinguem envelope do conteúdo
        - Conteúdo se divide em cabeçalho e corpo
    - MIME: pode ser utilizado para incluir vários tipos de conteúdo dentro de uma única mensagem
    - SMTP
        - Protocolo que o computador empurra o email para o servidor e o servidor empurra para o destinatario
        - Utiliza o padrão ASCII
        - TCP e porta de serviço 25

- POP/IMAP
  - Usado na entrega final do servidor para o agente do usuário
  - O IMAP é uma melhoria em relação ao POP3 que basicamente permitia ao usuário listar, baixar e apagar os seus emails

Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

Tabela comparativa IMAP x POP

- WWW
  - Serviço, publicação e distribuição de documentos
  - Arquitetura
    - Servidor
      - Passos seguidos pelo servidor em um loop principal
        - Aceitar conexão TCP do cliente
        - Obter caminho para a página ou arquivo requisitado
        - Obter o arquivo do disco
        - Enviar conteúdo do arquivo ao cliente
        - Encerrar conexão TCP
      - Como enfrentar o problema de atender a uma única solicitação por vez?
        - Um servidor web multithreaded com um front end e módulos de processamento
        - Etapas do modulo de processamento

                - Resolve o nome de uma pagina web solicitada
                - Controla o acesso à página web
                - Verifica o cache
                - Busca ou monta a página solicitada
                - Determina o restante da resposta
                - Retorna resposta ao cliente
                - Cria uma entrada no log do servidor
        - Navegador
            - Navegador é um interpretador de HTML
            - Outros formatos como mp3, pdf, jpeg, são processados por plugins no navegador ou por aplicações auxiliares
        - Protocolo HTTP
        - Linguagem HTML
        - Hipertexto
        - Hiperlinks
        - Páginas web
            - Estáticas
            - Dinâmicas
                - Necessário a execução de programas no servidor e no navegador para páginas web atuarem como aplicações
                - APIs
                - Scripts incorporados ao HTML
                - AJAX
            - CSS
        - Web (teia)
    - Passos que ocorrem ao acessar um link
        - O browser identifica a URL
        - O browser solicita ao DNS o endereço IP do servidor
        - Resposta DNS
        - O browser faz uma conexão TCP
        - Envia uma solicitação HTTP para aquela pagina
        - O servidor envia a página como resposta HTTP
        - O browser retorna outras URLs quando precisa
        - O browser apresenta a página
        - As conexões TCP são encerradas
    - COOKIE (rastro de conexão)
        - String que o servidor associa ao navegador
        - Conceito de sessão de login
        - Registro das ações do usuário
    - HTML
        - Linguagem de descrição e formatação de documentos
        - Cabeçalho e corpo
        - Comandos de formatação

        - Parâmetros de formatação
        - Diretivas

Item	HTML 1.0	HTML 2.0	HTML 3.0	HTML 4.0	HTML 5.0
Hiperlinks	×	×	×	×	×
Imagens	×	×	×	×	×
Listas	×	×	×	×	×
Mapas e imagens ativas		×	×	×	×
Formulários		×	×	×	×
Equações			×	×	×
Barras de ferramentas			×	×	×
Tabelas			×	×	×
Recursos de acessibilidade				×	×
Objetos inseridos				×	×
Folhas de estilo				×	×
Scripting				×	×
Vídeo e áudio					×
Gráficos de vetores em linha					×
Representação XML					×
Threads em segundo plano					×
Armazenamento pelo navegador					×
Tela de desenho					×

    - HTTP
        - Protocolo da camada de aplicação que faz o transporte das paginas HTML
        - É fechado dentro do TCP na porta 80

        - Http 1.0
            - nova conexao a cada busca de arquivo
        - Http 1.1
            - Abre uma única conexão e pede tudo que precisa
        - Http 2.0
            - abre uma única conexão, pede o html e o servidor vai empurrando o restante mesmo sem o cliente ter pedido

        - Passos solicitação HTTP
            - Usuário solicita
            - Navegador verifica a validade da cache
            - Navegador consulta o servidor com um get condicional
                - Pode receber a resposta de não modificado
                - Pode receber a resposta da página solicitada

            - Navegador retorna página para o usuário
    - Web móvel
        - WAP
            - Pilhas de protocolo adaptada para dispositivos móveis com telas pequenas e baixa velocidade
        - XHTML
        - Transcodificação
            - Servidor intermediário
    - Entrega de conteudo
        - Parque de servidores
            - Utiliza o DNS para espalhar as solicitações
            - Front end para balancear a garga
        - PROXY
            - Compartilhar cache entre usuários
            - Servidor proxy passa a ser o gateway padrão da rede
            - Servidor proxy pode funcionar como filtro de conteúdo
            - Solicitações, sempre que possível, são atendidas pelo proxy
        - CDN - servidores que provêm conteúdo em escala global
            - Estrutura de árvore para garantir a escalabilidade, desempenho e balanço de carga
            - Redirecionamento de DNS - fornece IP do nó CDN mais próximo
    - P2P
        - No fundo não é p2p, são soluções híbridas, pois o servidor precisa gerenciar
        - Ao se conectar a um supernó, as máquinas informam o que possuem
        - Consulta feira no sub-conjunto dos dados locais e retornados ao nó
        - Segunda etapa, consulta a outros supernós
        - Arquitetura centralizada
        - Arquitetura descentralizada
        - BitTorrent
            - Tracker + chunk
            - Swarm: peers que fazem down/upload
            - Seeders: peer que armazenam todos os chunks de um conteúdo
            - Leechers: nós que usam recursos sem contribuir
            - Distribuição de forma anônima
            - Impossível a retirada completa do material da rede
            - Sem controle central
            - Busca direcionada e sem inundação
            - Download dividida
    - FTP
        - Estabelece duas conexões
        - Porta 20

- Multimidia
    - Codificação de voz
        - PCM - modulação por codificação de pulsos
            - 8000 amostras por segundo com 8 bits por amostra = 64kbps
        - CD - WAV - waveform audio file format
            - 44100 amostras por segundo com 16 bits por amostra= 1410kbps
    - Compressão de video
        - JPEG
            - Comprime na razão de 20:1
        - MPEG
            - 1
                - Qualidade de gravador de video - 1,5Mbps
            - 2
                - Qualidade de broadcast 3 a 6 Mbps
            - 3
                - Video interatico - blue ray

            - Saida MPEG
                - Intracodificado: imagens estáticas, autocontidas e comprimidas
                - Preditivo: diferença bloco a bloco em relação ao quadro anterior
                - Bidirecional: diferença b/b em relação a quadros futuros
    - Streaming de mídia armazenada
        - Servidor web
            - Navegador pede o arquivo por um get
            - Servidor web responde
            - Navegador utiliza de um plugin ou aplicação p/ reproduzir
        - Servidor web com metafile
            - Navegador web pede o metafile do arquivo para o servidor
            - Servidor web responde
            - Navegador passa o metafile para a aplicação que vai reproduzir
            - Aplicação pede ao servidor arquivo
            - Servidor responde
        - Media server
            - Navegador web pede o metafile do arquivo para o servidor
            - Servidor web responde
            - Navegador passa o metafile para a aplicação que vai reproduzir
            - Aplicação pede ao servidor de mídia o arquivo
            - Servidor de mídia responde
        - HTTP sobre QUIC
            - Quic faz o controle de congestionamento
            - Mantém a sessão com uso de um ID, mesmo alterando o IP

            - Ganho de 30% para youtube
            - Objetivo: aumentar desempenho
        - Media server e RTPS
            - Navegador web pede o metafile do arquivo para o servidor
            - Servidor web responde
            - Navegador passa o metafile para a aplicação que vai reproduzir
            - Aplicação pede ao servidor de mídia configuração do arquivo
            - Servidor de mídia responde
            - Aplicação pede ao servidor de mídia dados do arquivo e armazena-os em buffer
- Correção de erros
    - FCC
        - Provoca overhead e aumenta a latência da rede
    - Intercalação
        - Sem overhead, mas aumenta a latência
- Voz sobre IP
    - SIP
    - H.323
        - Modelo de referência
- Codec
    - Codec de voz
        - Precisa de pouco linx
    - Codec de video
        - Pelo menos 1Mb para atingir uma qualidade boa
- Protocolos de transmissão
    - Os protocolos fazem a função da camada de transporte, mas estão na camada de aplicação
    - RTP
        - protocolo usado em transmissão em tempo real
        - Intercalação
        - Interpolação
        - Micro buffer
        - Timbre de hora
        - Mixagem
        - Mudança de codec
    - RTCP
        - funciona junto com o RTP
        - Player controla o servidor
        - Controle de qualidade
        - Provém feedback do receptor para o tranmissor
    - RTSP
        - Não funciona em tempo real

                - O conteúdo está gravado do outro lado, mas vc recebe o dado e assiste
                - Mantém um buffer com os dados recebido, caso pare a conexão, o buffer para de ser enchido.
                - Pode usar o UDP ou TCP
            - GQuic
                - Não funciona em tempo real
                - Usa o UDP, pois ele mesmo gerencia as perdas de pacote
                - Mantém a seção mesmo que o cliente mude de IP

- Segurança
    - Índice de acidentes está só aumentando, pois envolve recursos financeiros de interesse de muitos
    - Objetivo
        - Confidencialidade: proteção da informação do clube
        - Autenticação: determinar identidade do usuário
        - Não repudio: impedir que seja negada o acesso a determinada informaçã
        - Integridade: impedir que determinado dado seja alterado/danifica
    - Tipos
        - Substituição
            - Mono alfabéticas
                - Cada letra eh substituida pela k-ésima letra consecutiva
            - Poli alfabéticas
                - Cada letra eh substituída por uma letra qualquer única
                - Playfair
                    - Letras repetidas no mesmo par sao separadas por X
                    - Letras na mesma linha, pega a próxima a direita
                    - Letras na mesma coluna, pega a próxima de baixo
                    - Se nao, pega pega a letra correspondente a linha da coluna examinada
        - Transposição
            - Usa uma cifra de transposição
        - Uso unico
            - Faz um XOR com uma chave do tamanho do texto, como manda a chave com segurança?
        - Quantico

    - Algoritmo
        - Simetrico
            - Rapido
            - Problema: transportar a chave para o outro lado
            - Mesma chave usada para criptografar e descriptografar

- Intruso com acesso a chave, toda a segurança é perdida
- DES
    - Criptográfa blocos de 64 bits usando uma chave de 56 bits
    - One way
    - 2^56 chaves possiveis
    - Muito fraco para usar agora
- 3DES
    - Criptografia tripla com o DES
    - Descriptografia inversa
    - Bom, mas está ficando ultrapassado
- AES
    - Algoritmo de cifra de bloco simétrico
        - Blocos de texto simples iguais dando saídas iguais
        - Permite acesso aleatório aos blocos
        - Como criptografar textos menores que o bloco de entrada?
        - Risco de inversão dos blocos cifrados ou padrões
    - Chaves de tamanho 128, 192 e 256 bits
    - Implementação em software e hardware
    - Melhor escolha
- Modos de cifra
    - ECB
    - Feedback ou realimentação de cifra
    - Fluxo de cifras
    - Control - usando contador
- Criptoanálise
    - Força bruta
    - Mensagem conhecida
    - Mensagem escolhida
    - Análise matemática e estatística
    - Engenharia social
    - Criptoanálise linear
        - Rompe o DES com 2^46 textos simples
    - Análise de consumo de energia

- Assimetrico
    - Usa o assimetrico para transportar o simetrico
    - Não pode ser decifrado por um ataque de texto
    - Algoritmo RSA
        - Escolha dois números primos grandes, p e q
        - Calcule n = p X q
        - Calcule z = (p-1)X(q-1)
        - Escolha d de forma que z e d sejam primos
        - Escola e de forma que e X d = 1 mod z

        - Problema
            - muito lento
            - Autenticidade da chave,quem garante que a chave pública que eu peguei é realmente daquele cara
    - Sumario de msg
        - Função hash para criar um sumário do texto
- Ataque
    - Homem do meio
    - Aniversario
        - Dois textos diferente mesma saida que levariam a possibilidade de transmissão adulterada
    - Reflexão
        - Manda um desafio para a mesma pessoa que está perguntando para ela mesma responder
    - Repetição
        - Pega o mesmo pacote e manda varias vezes
            - Timbre de hora
- Serviços
    - Assinatura digital
        - Receptor pode verificar id do transmissor
        - Transmissor não pode repudiar o conteúdo da mensagem posteriormente
        - Receptor não tem a responsabilidade de criar a mensagem por si só
        - Tipos:
            - Assinatura de chave simétrica
                - Problema:
                    - Todos devem confiar em B
                    - Todas as mensagens assinadas devem ser lidas por B
        - Assinatura de chave pública
            - Supersecreto
            - Muito lento
            - Muito recente
            - Muito inseguro
        - Sumário de mensagens
            - Dado P, fácil calcular MD(P)
            - Dado MD(P), impossivel calcular P
            - Mudança de 1 bit produz uma saída muito diferente
            - SHA1/RSA
    - Certificado digital
        - Provo que determinada informação é verdadeira
        - Assinatura digital que eu reconheço e dou credito para ela

- Segurança na comunicação
    - Firewall/UTM
        - É uma combinação de Hardware e Software que isola a rede interna de uma organização da internet geral.
        - Permite que alguns pacotes passem e bloqueia outros.
        - Impedir ataques de negação de serviço
        - Impedir modificação ilegal de dados internos
        - Permite apenas acesso autorizado à rede interna
        - Técnicas gerais:
            - Controle de serviço
                - Tipos de serviços que podem ser acessados
            - Controle de direção
                - Direção na qual as requisições de serviços podem fluir
            - Controle de usuário
                - Controle o acesso aos serviços de acordo com permissões de usuários
            - Controle de comportamento
                - Controla a forma como os serviços são utilizados
        - Objetivos:
            - Facilita o gerenciamento e a execução de uma política de acesso pois todo o tráfego que entra e sai passa pelo firewall
            - Limita o acesso ao tráfego autorizado
            - O próprio fw é imune à penetração
        - Tipos:
            - Filtro de pacotes SEM estado
                - Todo pacote que entra e sai e filtrado pelo fw
                - Ferramenta pesada
                - Admite pacotes que não fazem sentido
            - Filtro de pacotes COM estado
                - Rastreia status de cada conexão
                - Time out de conexões inativas
            - Gateways de aplicação
                - Filtra pacotes nos dados da aplicação
                - Todos os usuário devem passar pelo gateway
                - Bloqueia tudo que não vem do gateway
    - VPN
        - Tunelamento voluntário ou compulsório

        - Segurança é garantida pelo tunelamento e criptografia mas não pode garantir tempo de resposta e taxa de transmissão
        - Autenticação de usuário
        - Gerenciamento de endereços
        - criptografia
        - Tunelamento na camada de enlace
            - PPTP
                - Trafégo criptografado e encapsulado
            - L2TP
                - Tráfego criptografado e mandado atraves de canais de comunicação
            - L2F
                - VPN discadas
            - CUPE
                - Empilha tudo dentro de um pacote UDP
        - Tunelamento na camada de rede (ipsec)
            - Confidencialidade
            - Autenticacao
            - Criptografa os dados
            - Usa a internet para mandar uma informação de um ponto A a um ponto B, de forma segura
        - Tunelamento na camada de transporte
            - SOCKS
                - Tráfego TCP atraves de proxy
            - SSL
            - SSH
                - Sessão remota a um computador que serve como proxy
- Redes sem fio
    - WEP
        - Uso chave default de fabrica
        - Criptografia RC4
        - Vetor de inicialização de 24 bits
    - WPA
        - Distribuição de chave de sessão
        - Vetor de inicialização de 48 bits
        - Criptografia RC4
        - Chaves quebradas por força brutas
    - WPA2
        - Criptografia AES
        - Chaves de 128 bits
    - EAP

            - Informa como cliente e servidor de autenticação devem agir
        - WPA-psk
            - Troca de chaves pelo AP
        - WPA-enterprise
            - Troca de chaves pelo servidor de autenticação
        - WPA3
            - Criptografia com AES
            - Chaves de 192 bits
            - Maior segurança com criptografia individualizada
            - Maior proteção contra ataques de força bruta
- Protocolos de autenticação
    - Chave secreta compartilhada
        - Pode sofrer ataque de reflexão
        - Transissor deve provar quem é antes de o receptor responder
        - Transmissor e receptor utilizam chaves especifícas
        - Estrair os desafios de conjuntos distintos
        - Tornar o protocolo resistente a ataques por segunda sessão em paralelo
    - Troca de chaves Diffie-Hellman
        - G^xy mod n
        - G^xy mod n
    - Sumário de mensagem
    - KDC
        - Centro de distribuição de chaves
        - Pode sofrer ataque de repetição
- Segurança na WEB
    - DNS spooting
        - Ataca um servidor de DNS e coloca a tradução errada
            - Faz assinaturas nos registros
            - URL
        - DNS sec
            - Prova onde os dados são originados
            - Distribuição de chave publica
            - Autenticação de transação e solicitação
        - URL auto certificados contendo um hash do nome e da chave pública do servidor
    - SSL
        - Camada de soquetes seguros
        - Conexão segura inclui
            - Negociação de parâmetro entre cliente e servidor
            - Autenticação do servidor pelo cliente

            - Comunicação secreta
            - Proteção da integridade dos dados
        - PGP
            - Assino o email
                - Sumário de mensagem fechado com a chave privada
        - Esteganografia
            - Fotos da zebra
            - Forma de transmitir alguma coisa de forma oculta, sem necessariamente criptografar
- **Gerencia de redes**
    - Disponibilização, integração e coordenação de elementos de hardware, software e humanos
    - Garantir tudo funcionando
    - Necessidade de monitoração e controle dos dispositivos da rede
    - Precisa de uma equipe para gerenciar
        - Equipe de GRC
            - Prevenir e solucionar problemas na rede
            - Vários níveis de profissionais

            - Helpdesk
                - Atende chamadas telefonicas
                - Certo grau de conhecimento
                - Problemas ja reportados
                - Pessoal pouco especializado
                - Auxiliados por aplicaçoes para gerenciar problemas ja relatados
                - Incluir novo problema
                - Ver estado de problemas de usuarios
                - Criticidade
                    - Grau de importância que um requisito, módulo ou erro possui no sistema
            - Operador
                - Acompanhar alarmes disparados pela estação de gerência
                - Perceber alarmes disparados, email, celular, mudança de cor no mapa de redes
                - Tentar resolver os problemas percibidos, ou encaminhar ao suporte
            - Suporte tecnico
                - Põe a mão na massa
                - Soluciona problemas que nao foram solucionados ainda
                - Responsável pela configuração, operação e manutenção dos equipamentos da rede

        - Alto nível de conhecimento
    - Gerente da equipe
        - Não necessariamente um expert técnico em redes
        - Conhecimento não tão profundo com o suporte
        - Avalia a equipe
            - Tempo médio entre falhas
            - Tempos médio para correção de falhas
            - Percentual de problemas resolvidos em menos de 1h
        - Solicita compra de equipamentos e aplicações
        - Providencia treinamento
        - Encaminha problemas para outros membros da equipe
- Áreas funcionais de gerenciamento (FCAPS)
    - Gerência de falhas
        - Detecção, diagnóstico e correção de falhas na rede
        - Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento
        - Cada componente essencial deve ser monitorado individualmente
        - Tolerância a falhas
            - Componentes redundantes
            - Rotas de comunicação alternativas
        - Ao ocorrer uma falha:
            - Determinar onde ocorreu
            - Isolar o resto da rede da falha para a mesma funcionar sem interferências
            - Reconfigurar ou modificar a rede para cobrir a falha
            - Reparar ou trocar o componente com problema
    - Gerência de configuração
        - Configuração inicial da rede
        - Inicialização
        - Topologia
        - Manutenção e monitoramento
        - Adição e atualização de componentes
        - Identificar componentes e suas conectividades
        - Modificar a rede para atender a demanda
        - Controlar inventário
        - Alterar a configuração
        - Gerar relatórios de configuração
    - Gerência de contabilização
        - Contabilizar e verificar a utilização dos recursos da rede
        - Evitar que determinado usuário abuse e monopolize a rede
        - Garantir o desempenho da rede
        - Conhecer as atividades dos usuários

            - Relatórios de informação de contabilização
        - Gerência de desempenho
            - Monitora o desempenho para identificar problemas e planejar a capacidade
            - Calcula índices de desempenho como utilização de tempo e de resposta em vários pontos de rede.
            - Monitorar a rede em questões como capacidade de utilização, tráfego, gargalos, tempo de resposta
            - Monitoramento de um conjunto de recursos
            - Gerar estatísticas de desempenho
            - Executar ações corretivas como redirecionamento de fluxo
        - Gerência de segurança
            - Protege os elementos da rede
            - Monitorando e detectando violação da política de segurança estabelecida
            - Provê facilidade para proteger os recursos da rede e informações dos usuários
            - Gerência de chaves de criptografia
            - Gerência de controle de acesso
            - Gerência de acesso à rede e dados
            - Auditoria e logs
            - Controle de serviçoes
    - Funções de gerenciamento
        - Monitoramento
            - Observação de componente, leitura
                - Estática
                    - Caracteriza a configuração e os elementos atuais, localização e responsável
                - Dinâmica
                    - Relaciona os eventos na rede como transmissão de pacotes, estado de uma interface de rede
                - Estatística
                    - Derivado de informações dinâmicas como média de pacotes por unidade de tempo
            - Coleta de informações por comunicação entre agente e gerente
                - Polling
                    - Interação request/response
                - Event-reporting
                    - Iniciativa do agente de mandar um relatório com informações
                    - Relatório com evento significativo ou não usual
                    - Gerente fica na escuta
        - Controle

- Alteração de valores de parâmetros e execução de determinadas ações, escrita
- Definição da informação de configuração
- Modificação de relacionamentos
- Inicialização de operações
- Relatorio de status de configuração
- Controle de segurança
    - Objetivo: garantir a confidencialidade, integridade e disponibilidade
    - Ameaças: interrupção, interceptação, modificação e mascaramento;

- SNMP
    - Simple network management protocol
    - Protocolo de gerência de dispositivos que atuam na camada de aplicação TCP/IP
    - Usa UDP
        - Porta 161 para envio e recebimento de informações
        - Porta 162 para recebimento de traps de dispositivos gerenciados
    - MIB - base de dados de objetos gerenciados que o agente tem acesso
    - SMI - structure of manegemente information
        - Regras para se definir objetos gerenciados e respectivos comportamentos
        - Definição do nome do objeto - OID em forma de árvore
        - Definição do tipo do objeto
        - Codifica em BER
    - SNMP v1 e v2 utiliza o conceito de comunidade, que eh uma string que configura o agente com 3 possibilidade
        - Porem essa string traféga na rede e pode ser interceptada
            - SNMP v3 trata isso
        - Operações:
            - • get
            - • get-next
            - • get-bulk (SNMPv2 e SNMPv3)
            - • set
            - • get-response
            - • trap
            - • notification (SNMPv2 e SNMPv3)
            - • inform (SNMPv2 e SNMPv3)
            - • report (SNMPv2 e SNMPv3)
    - Taxa de erros
    - Estado operacional de enlaces e equipamentos
    - Utilização de enlace, etc
    - Estabelecimento de limites de uso, THREASHOLDS

        - SNMP v3
            - Criptografia
            - Autenticação
            - Visões na MIB
            - Proteção contra playback
            - Controle de acesso baseado em visões
    - RMOM
        - Instala em alguns equipaento para fazer o monitoramento de toso os pacotes que passam naquela determinada parte da rede
        - V1
            - Atua na camada 1 e 2 (fisica e enlace
        - V2
            - Atua a partir da camada de rede
    - SFLOW
        - Instalado nos switchs/roteadores para monitorar o fluxo e o tráfego
        - Usa de estatística (não pega todos os pacotes) para ter uma visão sobre o que acontece na rede
    - Softwares de gerencia de redes
        - Redes são vitais
        - Dificuldade do gerenciamento de grandes redes
        - Atribuir e controlar recursos
        - Sistema deve garantir a disponibilidade

- **Comp movel**
    - Arquitetura
        - Redes sem fio com infra
            - Parte cabeada e o acesso final sem fio
        - Redes sem fio sem infra
            - Tipo adhoc
                - Sem estações base
                - Nós só podem transmitir a outros nós dentro da cobertura do enlace
    - Computação parvarsiva
        - Dispositivos executam tarefas mesmo sem intervenção do usuário
    - Computação móvel
        - Capacidade do dispositivo ser móvel
    - Computação ubíqua
        - Capacidade de acessar informações a qualquer momento e em qualquer lugar, mesmo que o usuário não saiba que existe toda uma infraestrutura por trás
    - DESAFIOS:
        - Conectividade
        - Mobilidade

        - Tecnologías heterogéneas
        - Restrições dos dispositivos
        - Segurança
    - Classificação das redes sem fio
        - Infraestruturada
            - Possui pontos de acesso
            - Célula de cobertura (necessita-se frequências diferente em células vizinhas pois precisa haver uma comunicação entre elas, usa-se algoritmos de coloração de grafos para isso
                - WWAN: celular
                - WMANs: wimax (wifi metropolitano)
                - WLANs: wifi
        - Ad hoc
            - Todo nó é potencial fonte de destino e origem
            - Todo nó é roteador de pacotes
            - Interferências em transmissões simultaneas
            - Energia limitada
            - Liberdade de locomoção
                - WLANs
                - WPANs: bluetooth
                - REDES DE SENSORES
        - Redes de satélites
            - Ampla cobertura
            - Taxas de tranmissão podendo atingir centenas de Mbps
            - Custo elevado
            - Alta latência
    - Transmissao sem fio
        - Atenuação do sinal quando se propaga pela matéria
        - Interferencia de outras fontes
        - Propagação miltivias (reflexo do sinal em paredes e chão)
        - Transmissão por frequências eletromagnéticas
        - Existem bandas que não requerem licenciamento da transmissão
            - ISM - instrumentation, scientific and medical
                - 902Mhz a 928Mhz
                - 2400Mhz a 2483,5Mhz
                - 5725Mhz a 5850Mhz
            - U-NII unlicensed national information
                - 5150Mhz a 5825Mhz
        - Padrões de propagação
            - Omnidirecional: todas as direções
            - Direcional: em apenas uma direção ou ângulo
            - Setorizada: em algumas direções
        - Problemas

            - Espalhamento: ondas ao se chocarem com objetos, são decompostas em várias ondas difusas de intensidade menos
            - Multi_path: reflexão em diferentes objetos pode causar recebimentos defasados
            - Atenuação: perda de sinal como ondas chegando fora de fase, ângulos e amplitudes diferentes
    - 802 sem fio
        - 802.20 - WAN
        - 802.16 - Wimax
            - Full duplex
            - Classes de serviços
                - Serviço com taxa de bits constante
                - Tempo real com taxa de bits variável
                - Modo offline com taxa de bits variável
                -
        - 802.15 - PAN
        - 802.11 - wifi/LAN
            - BSSID - basic service set identify
                - Mac adress da ap
                - Número aleatório de 46 bits
            - SSID - service set ID
                - Conhecido como nome da rede
                - 2 a 32 Bytes
            - Modos de operação
                - Access point
                - Bridge
                    - Mutuamente exclusivo com o ap
                    - Dois tipos
                        - Ponto a ponto
                        - Ponto a multiplo
                - Repetidor
                    - Ap nao se conecta a rede cabeada
                    - Retransmite o sinal de outro ap
                    - Mesmo SSID, cala e sobreposição de sinal
            - Site survey
                - Assegurar que o número, localização e configuração da nova instalação de rede forneçam as funcionalidades requeridas e propiciem um desempenho compatível com o investimento proposto no projeto
                - Análise de necessidade do negócio
                    - Nível de segurança
                    - Usuários por área média

            - Haverá aplicações com necessidades de tempo real?
        - Redes e dispositivos existente
            - Número de usuários
            - Sistemas operacionais
        - Qual a largura da banda requerida?
        - Obstrução por obstaculos
        - Fontes de interferência
        - Comportamento de ondas
            - Atenuação
            - Reflexão
            - Refração
            - Difração
            - Absorção
        - Segurança de WLAN
            - Defesa dos equipamentos da rede e dos clientes
            - Filtros por endereço MAC
            - Autenticação
            - WEP
            - WAP
            - WPA2
            - VPN
- Bluetooth
    - FHSS na banda de 2.4Ghz
    - WLAN 802.11
    - Suporta criptografia
    - Sugurançã definida em 3 modos
        - Sem segurançã
        - Estabelecida por serviço
        - Estabelecida por conexão
- ZigBee
    - Redes de sensores
    - 802.15.4
    - Opera em bandas não licenciadas
- Wifi
    - 802.11
    - Hospedeiro sem fio se conecta a estação base pelo AP (access point)
    - 802.11a
        - 5 a 6 Ghz
        - Até 54Mbps
        - OFDM (orthogonal frequency division multiplexing)
    - 802.11b

        - Espectro não licenciado
        - 2.4 a 2.5 Ghz
        - Todos os hospedeiros usam o mesmo código de chipping
        - Muda automaticamente a velocidade em casos de problemas na transmissão
        - DSSS (direct sequence spread spectrum)
    - 802.11g
        - 2.400 a 2.483Ghz
        - Até 54Mbps
        - OFDM e DSSS
    - 802.11n
        - 2400 a 2500Ghz
        - 600Mbps
        - OFDM
        - Múltiplas antenas
        - Objetivos:
            - Melhorar consideravelmente em relação a versões anteriores
            - Manter a compatibilidade
    - Problema da estação oculta e exposta
        - DCF
            - Não utiliza controle central
            - Dois tipos
                - CSMA/CA puro
                    - Função de distribuição coordenada
                    - Acesso multiplo com detecção da portadora
                    - Tenta prevenir colisões com intervalos
                    - Se houver colisão, as estações esperam um pouco para retransmitir
                - CSMA/CA com MACAW
                    - Utilisação do RTS e CTS
                        - RTS - request to send
                        - CTS - clear to send
            - Implementação obrigatória
        - PCF
            - O controle é feito por APs ou BS (estações base)
            - Polling
            - Sem colisões
            - Implementação opcional
- Celular

- Antenas próximas devem ter frequências diferentes para poder se comunicarem (problema de coloração de grafo)
- 1.0G
    - AMPS
    - Canais para transmissão e canais para recepção
    - Cliente se registra à celula a cada 15 min
    - Sinal analógico
    - Não criptografa
    - 868 a 900 Mhz
- 2.0G
    - TDMA/GSM - Divide o espectro em canais de frequência e divide cada canal em intervalos de tempo
    - Voz digital aplicando codex
    - TDMA
        - Cada canal agora, o pacote é dividido em 3 ou 6 pessoas transmitindo no mesmo pacote e canal
    - GSM
        - Aumentou a largura do canal para 200Ghz e consegue dividir em 8 pessoas usando o TDM
    - CDMA
        - Code division multiple access
        - Taxa de dados de ate 144Kbps
- 2.5G
    - Canais de dados e voz
    - GPRS
        - Evolução do GSM
        - Dados enviados em multiplos canais, se possível
        - Taxa de dados 115.2Kbps
    - EDGE
        - Evolução do GSM
        - Usa modulação avançada
        - Taxa de dados de até 384Kbps se pegar os 8 canais
- 3.0G
    - Voz digital
    - UMTS
        - 3Mbps
    - HSDPA
        - 14Mbps
- 3.5G
    - HSDPAT
- 3.99G
    - Não atingiu a velocidade esperada do 4G
    - Tranmitia tudo em dados 4G, mas quando ligava caia para digital

            - LTE
        - 4.0G
            - Baseada totalmente em IP
            - Velocidade de acesso entre 100Mbps em movimento e 5Gbps parado
            - Qualidade de serviço ponto a ponto a qualquer momento e em qualquer lugar
        - 4.5G
            - LTE+
        - 5.0G
            - LTE+
        - Mobilidade
            - Roteamento cuida da mobilidade
                - Tabelas de roteamento indica onde cada nó móvel está localizado
                - Sem mudança nos sistemas finais
            - Sistemas finais cuidam da mobilidade
                - Roteamento indireto
                    - comunicação do corresponden passa por agente nativo, depois encaminhada ao remoto
                    - Nó móvel usa dois endereços
                        - Endereço permanente
                            - Usado pelo correspondente
                        - Endereço aos cuidados
                            - Usado para repassar datagramas ao nó móvel
                    - Roteamento triangular
                    - Suponha que usuário móvel mude de rede
                        - Registra com novo agente externo
                        - Novo agente externo registra com agente natico
                        - Pacotes continuam sendo encaminhados ao nó móvel
                    - Mudança de rede transparente ao usuário
                - Roteamento direto: correspondente recebe endereço externo do nó móvel e envia diretamente a ele
                    - Contorna problema de roteamento triangular
                    - Não transparente ao correspondente
                    - Dados sempre roteados primeiramente para agente externo âncora
- IP móvel
    - RFC 3344
    - Agentes nativos, externos

- registro de agentes externos
- endereços aos cuidados
- Encapsulamento
- Componentes do padrao
    - Roteamento indireto de datagramas
    - Descoberta de agente
    - Registro com agente nativo
- rede nativa: rede do provedor de celular que você assina
    - Home Location Register (HLR): banco de dados na rede nativa contendo # de telefone celular permanente, informação de perfil (serviços, preferências, cobrança), informações sobre local atual (poderia estar em outra rede)
- Rede visitada: rede em que nó móvel reside no momento
    - Visitor Location Register (VLR): banco de dados com entrada para cada usuário atualmente na rede
    - poderia ser a rede nativa