PROTOCOLO TCP/IP

CAMADA DE APLICAÇÃO

- A camada de aplicação é responsável pela comunicação entre processos entre o remetente e o destinatário, permitindo a troca de dados das informações por meio da implementação de protocolos como http, ftp e smtp, sendo responsável pela implementação do protocolo cliente-servidor. Sendo assim, a camada de transporte (que já atua diretamente entre os dispositivos finais) é a responsável por transmitir os dados de forma integrada e sequencial para a camada de aplicação, direcionando o host através do IP e o processo através da porta
- Um processo é um programa que executa num hospedeiro (host); 2 processos no mesmo hospedeiro se comunicam usando comunicação entre processos definida pelo sistema operacional; 2 processos em hospedeiros distintos se comunicam usando um protocolo da camada de aplicação;
- Cada aplicação tem processos que se identificam pelo PID
- Protocolo é basicamente uma ordem de troca de informações
- Se eu mandar uma info A, irei receber A.
- Se eu mandar uma info do tipo CONNECT, ira conectar
- Os protocolos recebem infos da camada de transporte e conforme o conteúdo desses pacotes de dados ele vai implementar o respectivo protocolo com suas características. Se é transferência de arquivo, FTP porta 21, se é email, SMTP, se é WEB HTTP porta 80.
- Cookies armazenam informações sobre o usuário, senhas, etc..
- SMTP
    - agentes de usuário UA (o programa/navegador que mostra os emails)
    - servidores de correio MTA - message transfer agent (onde armazenam-se os emails)
    - SMTP simple mail transfer protocol (processa os emails, envia de um servidor ao outro, gmail -> outlook)
    - Caixa de correio> mensagens de chegada ainda não lidas
    - Filas de saída> contém mensagens de saída
    - geralmente porta 25
    - Formato: cabeçalho, linha em branco e corpo(caracteres ascii)
    - POP (o pop capta as infos do server e traz elas para o agente local. ler e apagar)E IMAP(Deixa as infos no servidor em cópia, ler a manter)
- DNS sobre o UDP e usa a porta 53
    - Servidor de resolução de nomes;

    - converte o nome do domínio para um IP;
    - PC aponta para o roteador que aponta para o modem que aponta para o servidor, caso o servidor não contenha o ip desejado ele vai enviando para secundários;
- Página WWW: consiste de “objetos” endereçada por uma URL
- Quase todas as páginas WWW consistem de: página base HTML, e vários objetos referenciados.
- Agente de usuário para WWW se chama de browser: MS Internet Explorer Mozilla Firefox**:**
- **HTTP: hypertext transfer protocol:**
    - serviço de transporte TCP:
    - cliente inicia conexão TCP (cria socket) ao servidor, porta 80 servidor aceita conexão TCP do cliente
    - mensagens HTTP (mensagens do protocolo da camada de aplicação) trocadas entre browser (cliente HTTP) e servidor e WWW (servidor HTTP)
    - encerra conexão TCP
    - HTTP é “sem estado” servidor não mantém informação sobre pedidos anteriores do cliente
    - Request e response
- HTTP: não persistente:
    - No máximo um objeto é enviado em uma conexão TCP
    - HTTP/1.0 usa conexões não persistentes
    - servidor analisa pedido, responde, e encerra conexão TCP
    - requer 2 RTTs para trazer cada objeto
    - mas os browsers geralmente abrem conexões TCP paralelas para trazer cada objeto
- HTTP: persistente
    - Múltiplos objetos podem ser enviados numa única conexão TCP entre o servidor e o cliente
    - HTTP/1.1 usa conexões persistentes no modo default
    - servidor mantém conexão aberta depois de enviar a resposta
    - mensagens HTTP subseqüentes entre o mesmo cliente/servidor são enviadas por esta conexão
    - na mesma conexão TCP: servidor analisa pedido, responde, analisa novo pedido e assim por diante
- FTP File Transfer protocol
    - SFTP - FTP Seguro - porta 22
    - Cliente FTP contacta servidor ftp na porta 21, especificando TCP como protocolo de transporte
    - Cliente obtém autorização através da conexão de controle
    - O cliente acessa o diretório remoto através do envio de comandos pela conexão de controle

    - Quando o servidor recebe um comando para transferência de arquivo, o servidor abre uma conexão TCP com o cliente, na porta 20
    - Códigos de retorno típicos: 331 Username OK, password required open; 125 data connection already, transfer starting; 425 Can't open data connection; 452 Error writing file

CAMADA DE TRANSPORTE

- Camada de transporte é o "coração" do modelo de redes
- Protocolos entregam dados de um processo (programa) em um dispositivo a outro processo (programa) em outro dispositivo
- Atua como intermediário entre protocolos de camada superior e os serviços fornecidos pelas camadas inferiores
- Camada de transporte fornece transparência sobre detalhes da rede física para as camadas superiores
- Serviços são similares aos da camada de enlace
- Provê uma comunicação lógica entre processos de aplicação executado em hosts diferentes
- Tipos de entrega de dados: transporte: processo a processo; rede: host a host; fisica: enlace a enlace;
- protocolos de transporte executam em sistemas terminais
    - emissor: fragmenta a mensagem da aplicação em **segmentos** e os envia para camada de rede
    - receptor: rearranja os segmentos em mensagens e os transmite para a camada de aplicação.
    - tcp verifica se rearranjou certo, é mais lento, udp não e é mais rápido,
    - Camada de rede trata pacotes como entidades separadas mas não como mensagens completas
    - A Camada de transporte garante que a mensagem completa chegue intacta, fim-a-fim.
    - A combinação de IP e número de porta é chamada endereço socket (socket address)
    - **Serviços sem conexão UDP (não confiável sem controle de erros e de fluxo) e orientados a conexão HTTP (confiável, tem controle de erros e de fluxo)+**
- Categorias de serviços: ▪ Entrega fim-a-fim ▪ Endereçamento ▪ Multiplexação ▪ Entrega confiável ▪ Controle de fluxo
- Números de portas universais, chamadas well-known port numbers, são usados para identificar certos processos em um servidor
- Endereço IP define o host; porta define o processo em um host particular
- A combinação Endereço IP e número da porta é chamada endereço socket (socket address)
- Sobre portas: Well known (conhecidas) – atribuídas e controladas pela IANA 0-1023; Registradas – não são atribuídas ou controladas pela IANA. Podem somente ser registradas por empresas comerciais junto a IANA para evitar

duplicação 1024-49151; Dinâmicas – portas temporárias que podem ser usadas por qualquer processo 49152-65525

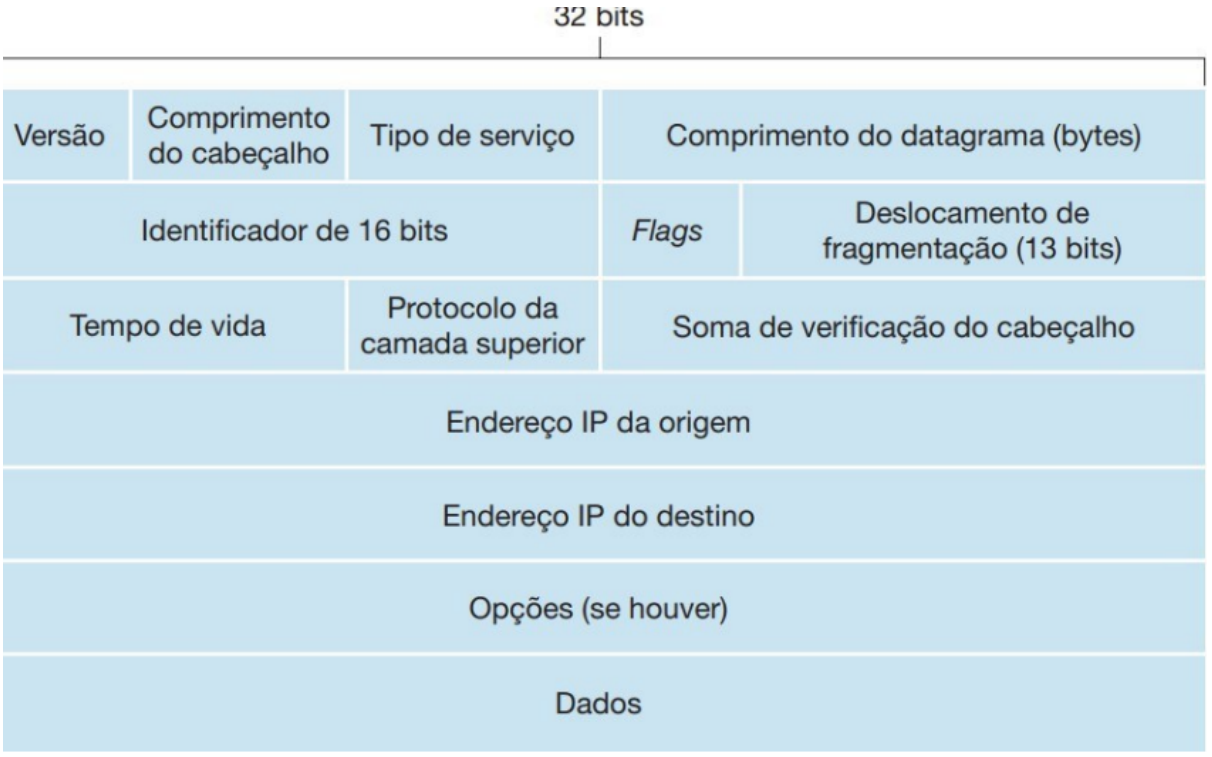
- **Multiplexação:** camada de transporte aceita mensagens de processos diferentes, diferenciados pelos seus números de porta; Adiciona cabeçalhos e passa o pacote para a camada de rede; **Demultiplexação** – recebe datagramas da camada de rede, verifica erros, remove cabeçalho e entrega a mensagem ao processo apropriado baseado no número da porta
- **Protocolos sem conexão** (sem estabelecimento ou término de conexão, pacotes não numerados) UDP - Connectionless, protocolo de transporte não confiável. Overhead mínimo; NÃO TEM controles de erro e fluxo; Usa números de porta para multiplexar dados da camada de aplicação; Freqüentemente usado por aplicações multimídia e multicast, FTP, e protocolos de roteamento como o RIP. **Com conexão:** estabelece e termina conexão, confiável e com controle de fluxo TCP - Protocolo de transporte confiável e orientado a conexão de fluxos; Adiciona características de confiabilidade e de orientação a conexão ao IP; Usa números de porta como endereços da camada de transporte;
- **Serviços TCP** - Serviços de entrega de fluxos – permite que o processo emissor envie dados como um fluxo de bytes; Buffers de emissão e recepção – controla o processo de envio e recebimento já que processos podem produzir e consumir dados em velocidades diferentes; Bytes e segmentos – agrupa bytes em segmentos, adiciona um cabeçalho e entrega ao IP para transmissão; Suporte a ambas as direções; Cria uma conexão virtual para criar um ambiente orientado a fluxos; Confiabilidade é alcançada pelo uso de ACKs
- **Estabelecimento da Conexão** handshake triplo manda SYN, recebe SYN+ACK, envia ACK
- **Controle de Erros**: Baseado na detecção de erros e retransmissão; Checksum, ACK e time-out; Verificações da camada de enlace acontecem conforme os pacotes são enviados de um nó para outro nó; Controle de erros de transporte verifica para ter certeza de que erros não foram introduzidos nos pacotes quando processados pelos roteadores;
- **Controle de Perdas**; Garante que todas as partes da transmissão chegaram ao destino; Números de seqüência permitem à camada de transporte no receptor identificar os segmentos faltantes e pedir o reenvio Controle de Duplicação; Garante que nenhum pedaço chegou duplicado; Segmentos duplicados são identificados pelo números de seqüência

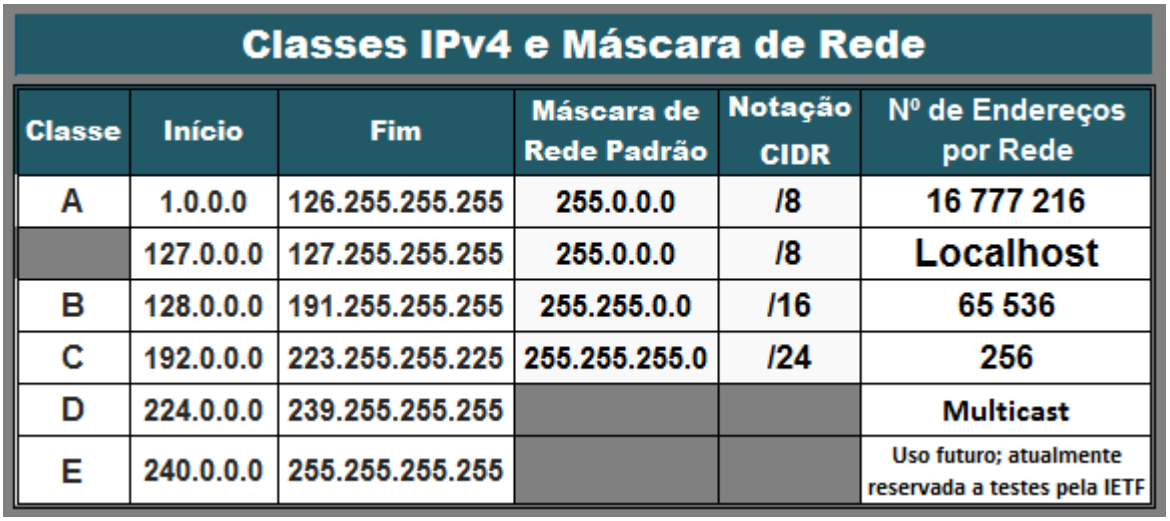
CAMADA DE REDE

- Propósito: comunicação entre hosts
- **Repasse:** Repassar a informação de uma rede para outra rede, passar a informação de dois pcs em uma mesma rede. Quando um pacote chega ao enlace de entrada, o roteador deve levar ele até o pacote de saída.
- **Roteamento:** Repassar informações entre redes diferentes. determina a rota que os pacotes devem tomar de um remetente até um destinatário

- Circuitos virtuais: serviço orientado a conexão, Estabelece um caminho antes de trocar os pacotes
    - A tabela de repasse associa um número para cada pacote em cada enlace
    - Consiste em:
        - Um caminho, uma séries de enlaces e roteadores entre hospedeiro de origem e destino
        - Número de CV(circuito virtual): Um número que associa cada pacote a um enlace para cada roteador ao longo do caminho
- EM UMA REDE DE DATAGRAMAS,
    - QUANDO UM pacote é enviado: informa-se o endereço de destino e enviar-o para dentro da rede
    - é serviço utilizado na internet IP
    - Cada pacote atravessa indefinidos roteadores
    - Como um roteador funciona:
        - Portas de entrada: LAN(interna), WAN(externa)
        - Elemento de comutação: Gerencia as rotas de entrada e saída (fazer o melhor roteamento)
        - Porta de entrada: Terminação de linha(espeta-se o cabo nela. Realiza o processo de desencapsulamento) e faz o repasse para uma fila a ser utilizada pelo elemento de comutação
        - Do elemento de comutação ele vai para o gerenciamento de buffer, passa pelo encapsulamento e vai para a terminação da linha

- Cabeçalho da Rede IPV4



- Sobre o endereço IPV4
    - Deve identificar unicamente e universalmente cada dispositivo
    - Endereço internet ou endereço IP
    - O endereço é escrito em notação decimal separado por ponto
    - Endereço binário de 32 bits
    - Chega a 4 bilhões de máquinas 2^32
    - Endereço define dois campos:
        - NetID Identifica a sub-rede da internet
        - Host ID: Identifica a máquina numa sub-rede
        - Notação binária: 32 bits
        - Notação decimal com pontos: mais compacto e a fácil de ler: cada número entre 0 e 255
    - Definido por classes em ranges de IPs, ver tabela:
- 

Classes IPv4 e Máscara de Rede

Classe	Início	Fim	Máscara de Rede Padrão	Notação CIDR	Nº de Endereços por Rede
A	1.0.0.0	126.255.255.255	255.0.0.0	/8	16 777 216
	127.0.0.0	127.255.255.255	255.0.0.0	/8	Localhost
B	128.0.0.0	191.255.255.255	255.255.0.0	/16	65 536
C	192.0.0.0	223.255.255.225	255.255.255.0	/24	256
D	224.0.0.0	239.255.255.255			Multicast
E	240.0.0.0	255.255.255.255			Uso futuro; atualmente reservada a testes pela IETF

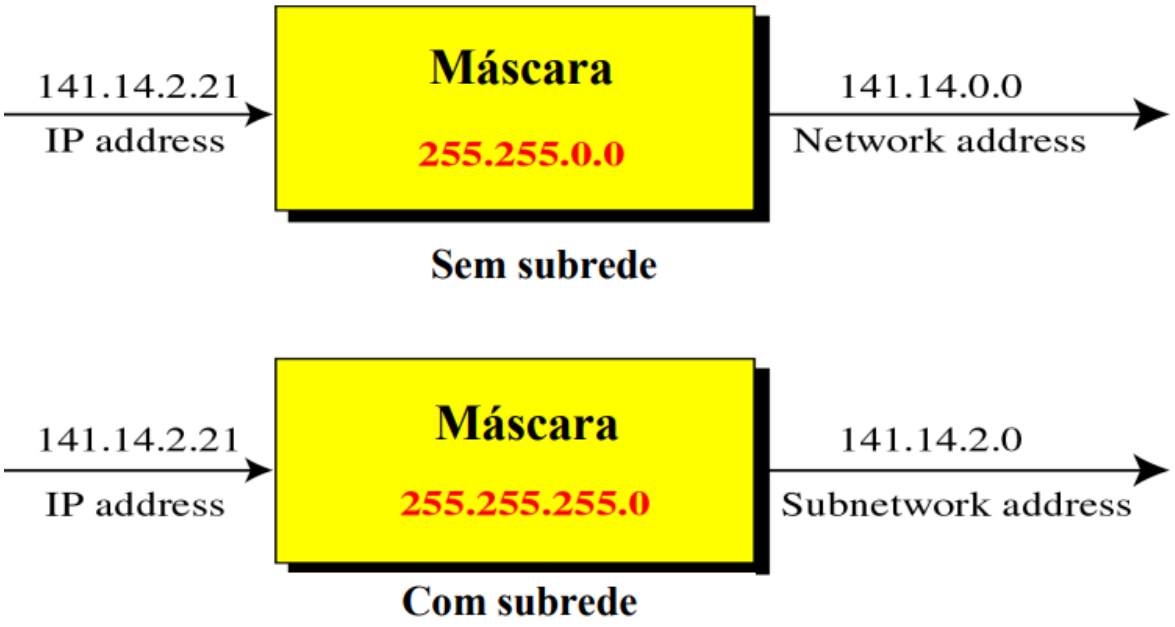
- Unicast: Sai de um e vai para um. Switch
- BroadCast: Sai de um e vai para todos da rede. HUB
- Multicast: Sai de um e vai para muitos específicos. Switch gerenciável
- **Tabelas de endereços privados, especiais e reservados**

Tipo	Início do Endereço IP	Fim do Endereço IP
This Host	0.0.0.0/8	
LAN Classe A	10.0.0.0/8	10.255.255.255
Local Host "loopback"	127.0.0.0/8	127.255.255.255
Link Local "APIPA"	169.254.0.0/16	169.254.254.255
LAN Classe B	172.16.0.0/12	172.31.255.255
LAN Classe C	192.168.0.0/16	192.168.255.255
Multicast Classe D	224.0.0.0/4	239.255.255.255
Reservado Classe E	240.0.0.0/4	254.255.255.255
Broadcast	255.255.255.255	

- Endereços reservados a redes privadas:

Nome	Número de IPs	*classful* Descrição	Faixa de endereços IP	Maior bloco CIDR	Referência
8-bit block	16,777,216	Uma classe A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	RFC 1597 (obsoleto), RFC 1918
12-bit block	1,048,576	16 classes B	172.16.0.0 – 172.31.255.255	172.16.0.0/12	
16-bit block	65,536	256 classes C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	
16-bit block	65,536	Uma classe B	169.254.0.0 – 169.254.255.255	169.254.0.0/16	RFC 3330, RFC 3927

- Máscara:
  - Extrai o endereço físico da rede a partir do endereço IP
  - Usada pelos roteadores dentro da organização

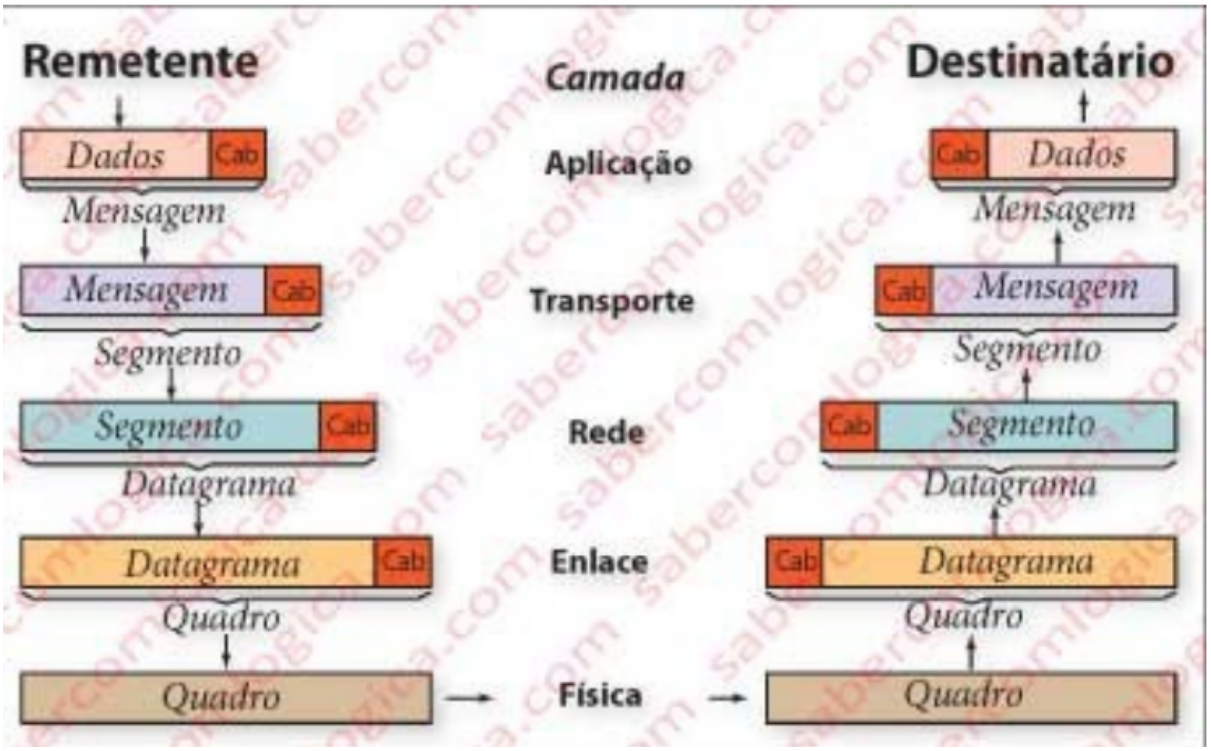


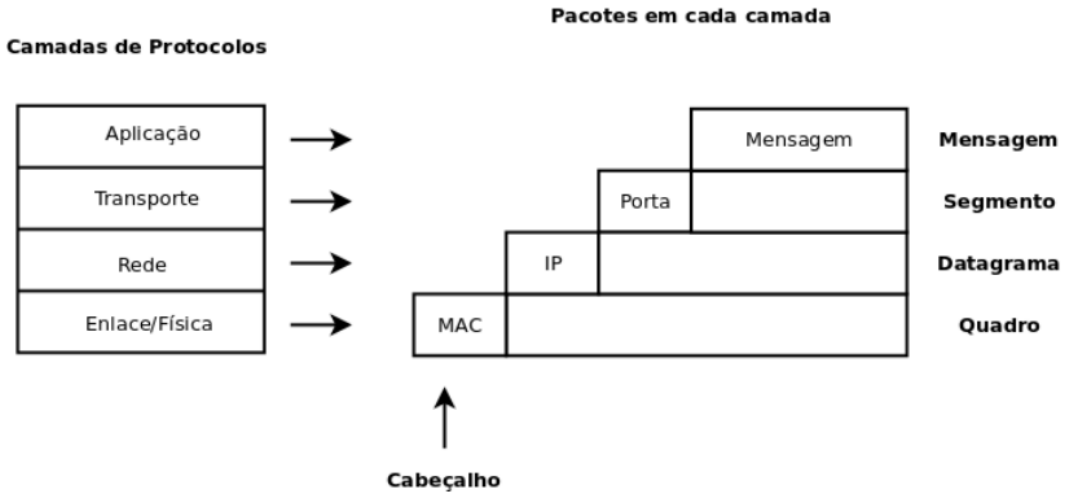
- Exemplos de máscara de sub-rede para uma rede de Classe C:

Subredes	Hosts	Máscara de Subrede
2	126	255.255.255.128
4	62	255.255.255.192
8	30	255.255.255.224
16	14	255.255.255.240
32	6	255.255.255.248
64	2	255.255.255.252

- Na falta de endereços IP para todos os dispositivos que conectam um roteador, é preciso usar a técnica do NAT O roteador toma o papel de um equipamento único, com um IP para o mundo externo, e associa a cada dispositivo um número de porta. Para a rede local ele associa um IP local para cada máquina e uma tabela que relaciona o número de porta com o IP associado.
-
- Um roteador está ligado a um DHCP que está ligado a um repetidor, que está ligado a um computador. Um repetidor não tem um DHCP, que é responsável por fornecer um ip ao computador
- WAN é quando há um DHCP ligado, se comunica com a rede externa, LAN é a rede interna;

CAMADA DE ACESSO A REDE ENLACE+FÍSICA





- Responsável pela transferência de quadros (frames) de um nó para o seguinte;
- Deve transformar a camada física em uma linha confiável e livre de erros;
- Faz o enquadramento: divide fluxos recebidos da camada de rede em quadros, adicionando header e trailer ;
- Colocar endereços físicos de origem e destino no cabeçalho. Na LAN Ethernet é o endereço MAC (Media Access Control);
- Controle de erros: (Como erros são tratados?) detecta e retransmite frames danificados ou perdidos;

- Controle de acesso: (Quem envia e quando?) determina qual dispositivo assume o controle do link quando dois ou mais dispositivos estiverem conectados ao mesmo link
- Controle de fluxo: (Quanto deve ser enviado?) coordenar a quantidade de dados enviados antes de receber o reconhecimento para que o emissor não “inunde” o receptor
- Tecnologias específicas da camada de enlace: Ethernet, pontes, switches, IEEE 802.11 LANs, PPP, ATM
- Camada de enlace tem a responsabilidade de transferir datagramas de um nó para o nó adjacente sobre um enlace
- Terminologias:
    - hosts e roteadores são nós (pontes e comutadores também)
    - Enlaces são canais de comunicação que conectam nós adjacentes ao longo dos caminhos de comunicação
        - Enlaces cabeados
        - Enlaces sem fios
        - LANs
    - 2-PDU é um quadro, que encapsula um datagrama

Implementação de Protocolo da Camada de Enlace

- Combina software, hardware e firmware
- Protocolo da camada de enlace é implementado totalmente no adaptador em todo e cada host
- Adaptador tipicamente inclui:
    - RAM, circuitos de processamento digital de sinais, interface do barramento do computador, e interface do enlace
    - Adaptador é semi-autônomo, conectado ao barramento do computador
- **transmissão do adaptador:**
    - **encapsula (coloca número de seqüência, info de realimentação, etc.)**
    - **inclui bits de detecção de erros**
    - **implementa acesso ao canal para meios compartilhados**
    - **coloca no enlace**
- **recepção do adaptador:**
    - **verificação e correção de erros**
    - **interrompe computador para enviar quadro para a camada superior**
    - **atualiza info de estado a respeito de realimentação para o remetente, número de sequência, etc.**

Controle de Fluxo (e Erro)

- Coordena a quantidade de dados enviados antes de receber o reconhecimento (ACK – acknowledgement)
- Objetivo: impedir que o receptor seja “inundado”: Buffer overflow
- Receptor informa emissor de frames perdidos ou corrompidos e coordena a retransmissão de tais frames pelo emissor: Número de frames será determinado pelo protocolo

- Usualmente tratado através de retransmissão chamada ARQ (“automatic repeat request”) ao invés de usar a correção
- Stop-and-Wait ARQ: Algoritmo de Bit Alternado
- Go-back-N ARQ
- Janela n com retransmissão integral; Selective-Repeat ARQ
- Janela n com retransmissão seletiva
- Erros isolados: um único bit. Mais comum em transmissão paralela
- Erros em rajadas (Burst error)
    - Dois ou mais bits nos dados, não necessariamente em ordem consecutiva
    - Mais comum em transmissão serial
    - Depende da taxa de dados e duração do ruído
- Detecção
    - Precisa ser detectado antes de processar a mensagem
    - Redundância pode ser usada para adicionar bits à mensagem para controle de erros
    - Processamento deve ser feito pelo receptor

Redes Locais LAN – Local Area Network

- **É uma rede: Computadores autônomos e interconectados por um sistema de comunicação para troca de informações e compartilhamento de recursos**
- Contida em área geograficamente limitada (sala, prédio, campus) - possível comunicação entre quaisquer dois equipamentos da rede
- Alta velocidade de transmissão
- facilidade de inserção de novos equipamentos
- simplicidade do meio físico
- Equipamentos interconectados porém independentes
- Alto grau de interconexão entre equipamentos
- Interface com a rede e meios de transmissão baratos
- Rede Local
    - Conjunto de PCs ou estações de trabalho interligados
    - Softwares e dados armazenados em servidores
    - Usuários executam suas tarefas a partir de seus PCs
- Módulos de uma Rede Local
    - servidores
    - estações de trabalho
    - recursos de comunicação

Endereçamento - Endereços físicos e ARP

- Endereços IP de 32-bit: endereços da camada de rede usados para levar o datagrama até a rede de destino
- Endereço de LAN (ou MAC ou físico):
    - Usado para levar o datagrama de uma interface física a outra fisicamente conectada com a primeira (isto é, na mesma rede)

    - A maioria das LANs usam um endereço físico de 48-bits (6- bytes) escrito com 12 dígitos hexadecimais; cada byte (2 dígitos hexadecimais) separado por dois pontos **07:01:02:01:2C:4B**
    - Endereços MAC são gravados na memória fixa (ROM) do adaptador de rede, são administrados pelo IEEE

Address Resolution Protocol (ARP)

- Protocolo ARP:
    - Mapeamento dinâmico de endereço lógico (IP) para físico (MAC)
    - Solicitação ARP é transmitida em broadcast
    - Resposta ARP é transmitida em unicast
- Hosts e roteadores usam endereços IP a nível de camada de rede
- Redes físicas usam endereços locais (MAC)
- Dois níveis de endereços: IP e MAC
- Address Resolution Protocol (ARP) 29
- Quando a camada Ethernet recebe um pacote com um endereço IP para ser transmitido, é necessário traduzir este endereço IP para endereço físico
- Para descobrir o endereço físico associado a um endereço IP é enviado um pacote de broadcast ARP
- Todos os equipamentos que possuírem a informação devem enviar a resposta
- Assim que tiver uma resposta (uma tradução) é possível realizar o envio do pacote Ethernet
- A tabela ARP mantém entradas estáticas e dinâmicas
    - Entradas dinâmicas são adicionadas e apagadas automaticamente
    - Entradas estáticas permanecem na tabela até que o computador seja reiniciado
- **A tabela ARP sempre mantém o endereço de hardware (FF FF FF FF FF FF) para a subrede local como uma entrada permanente. Esta entrada permite a uma máquina aceitar uma mensagem broadcast do ARP. Este endereço não é mostrado quando visualizamos a tabela.**
- A descoberta de endereços na camada de enlace é utilizada para determinar o endereço mac dos vizinhos do mesmo enlace. O host envia uma mensagem neighbor solicitation informando no campo de dado seu endereço mac e solicitando o max do vizinho. Ao receber a mensagem o bizinha responde utilizando um neighbor advertisement informando seu mac

Padrões IEEE

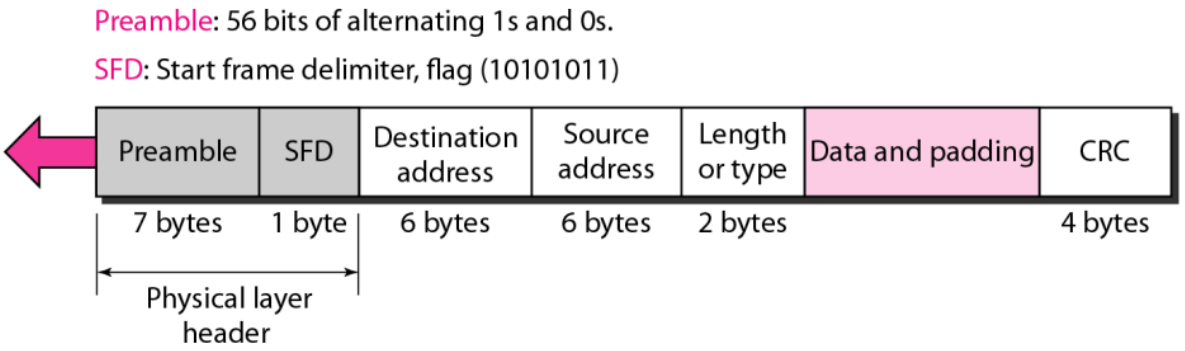
- Camada de Enlace subdividida em duas subcamadas:
    - LLC (Logical Link Control)-Controle de fluxo, controle de erros, parte do enquadramento
    - **MAC (Medium Access Control)-Controle de acesso ao meio e formato do enquadramento específico para a LAN**
    - 802.1 : gerenciamento de redes e generalidades
    - 802.2 : subcamada LLC da camada de Enlace

- **802.3 : Ethernet - subcamada MAC e camada Física para redes em barramento e método de acesso ao meio CSMA/CD**
- 802.4 : subcamada MAC e camada Física para as redes em barramento e método de acesso ao meio "tokenpassing" (Token-Bus)
- 802.5 : subcamada MAC e camada Física para as redes em anel e método de acesso ao meio "token-passing" (Token-Ring)
- 802.11: LANs Sem fio (wireless)

Ethernet

- Tecnologia de rede com fio “dominante”
- Uma placa de rede é barata
- Primeira tecnologia de LAN amplamente usada
- Mais simples que LANs de token e ATM
- Foi aumentando a velocidade: 10 Mbps – 10 Gbps

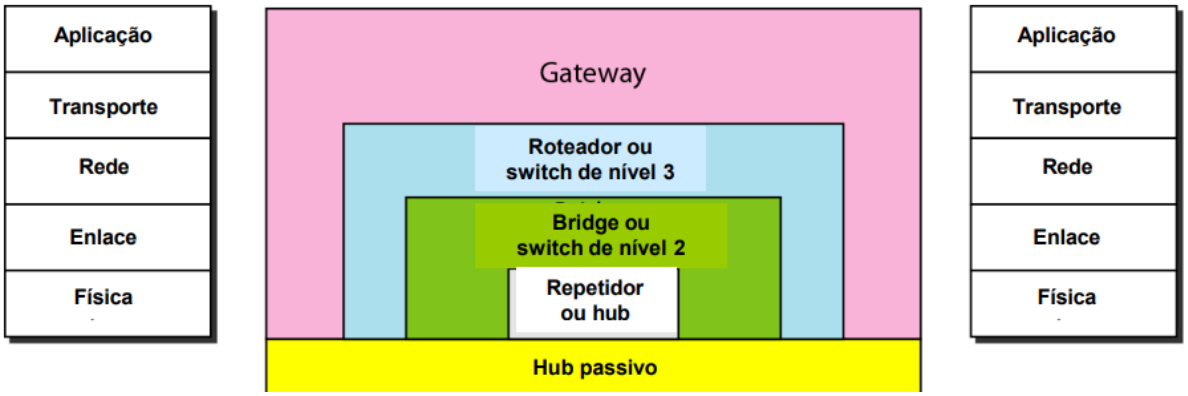
Ethernet – formato do frame



- Preâmbulo (preamble): primeiro campo do frame MAC 802.3 contém 7 bytes (56 bits) composto por 0s e 1s alternados que alertam o receptor sobre o frame que está chegando e o habilita a sincronizar seu clock de entrada
- SFD (Start Frame Delimiter): anuncia início do frame (1 byte:10101011)
- Endereço de destino (DA-Destination Address): endereço físico da estação (ou estações) de destino
- Endereço fonte (SA-Source Address): endereço físico do emissor do pacote
- Comprimento ou tipo (Length or type): campo de tipo ou de comprimento
- Dados (Data and padding): transporta dados encapsulados das camadas superiores. Tem um comprimento mínimo de 46 bytes e um tamanho máximo de 1500 bytes
- CRC: CRC-32 para detecção de erros.
- Endereço MAC: 6 bytes = 12 dígitos hexa = 48 bits
- O primeiro bit menos significativo do primeiro byte define o tipo de endereço. Se o bit é 0, o endereço é unicast, senão é multicast.
- O endereço de destino broadcast é um caso especial do endereço multicast no qual todos os bits são 1s.

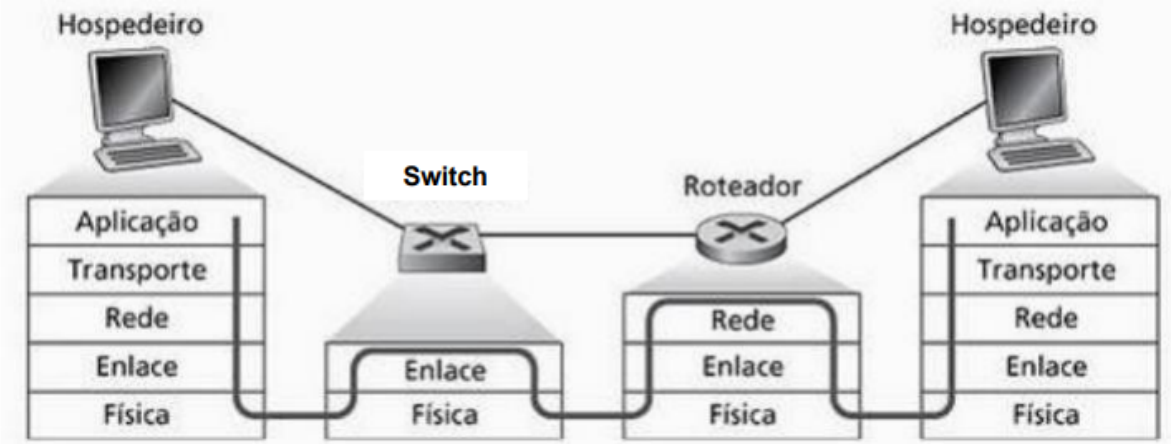
Interconexão de Redes via Switches e Hubs

- LANs são conectadas entre si ou à Internet
- Para interligar LANs ou segmentos de LANs usam-se dispositivos de conexão que podem operar em diferentes camadas/níveis da arquitetura TCP/IP

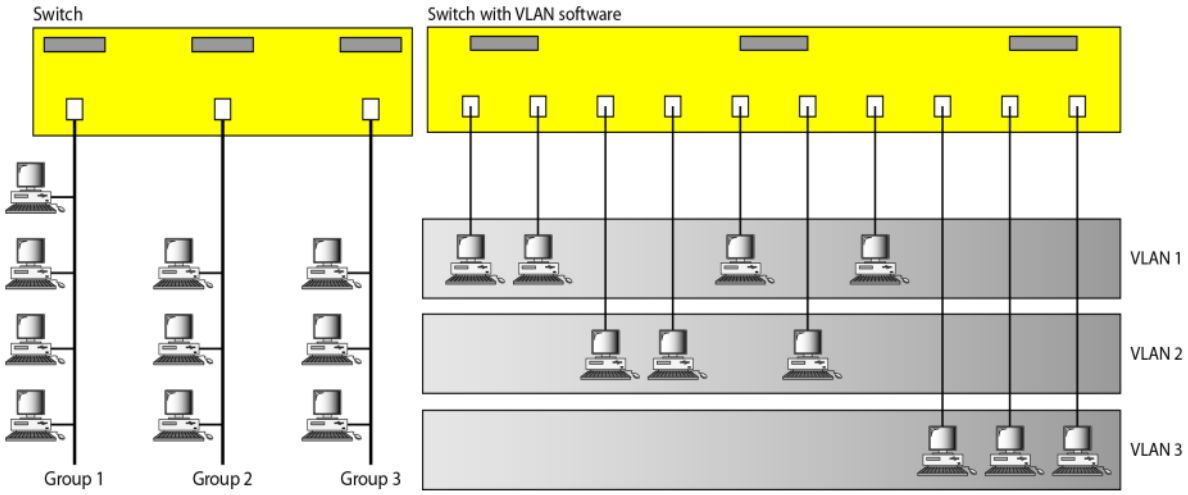


- Hub passivo
  - simplesmente um conector de cabos provenientes de diferentes ramificações
  - na LAN Ethernet com topologia estrela um hub passivo é o ponto de colisão
- Repetidor
  - Conecta segmentos de uma LAN. Segmentos: partes de uma mesma rede conectadas por repetidores
  - Encaminha todos os frames; não tem capacidade de filtragem
  - É um regenerador, não um amplificador
  - Supera restrição de comprimento de redes 10Base5 (500m): divide-se o cabo em segmentos e instala-se repetidores entre os segmentos
  - Repetidor atua como um nó de duas portas: recebe o sinal em uma porta, regenera o sinal e o encaminha para a outra porta
- Switches
  - Switch de camada 2 = bridge com muitas portas
  - Pode conectar LANs entre si
  - Tem filtragem, algoritmos de aprendizado para preencher as tabelas, são “plug-and-play”
  - Pode ser mais sofisticado: pode ter buffers para reter os frames para processamento ou um encaminhamento mais rápido (cut-through)
  - Eliminam colisões no modo full-duplex
  - Enlaces heterogêneos: 10 Mbps, 100 Mbps, ...
  - Facilita o gerenciamento da rede: tem facilidades para coleta de informações como uso da largura de banda, atrasos, ...
  - É possível conectar switches entre si
- Roteadores (camada de rede)
  - Direciona pacotes com base nos endereços lógicos (host-host), escolhendo a rota

- Geralmente interliga LANs e WANs na Internet
- Dispositivo armazena e envia
- Switches de camada 3 funcionam como roteadores (às vezes são mais sofisticados e rápidos)



- Uma VLAN (Virtual Area Network) é uma rede local configurada por software, não por cabos físicos



- VLANs criam domínios de broadcast
- A tecnologia VLAN permite agrupar estações conectadas a switches distintos em uma VLAN
- Configuração pode ser manual, automática (usando critérios como ser membro de um grupo/projetos) ou semi-automática
- Considerando que a reconfiguração física é dispendiosa, as VLANs reduzem o custo de migração de estações de um grupo para outro já que a migração é via software

Dados Analógicos e Digitais

- Dispositivos Analógicos:
    - Utilizam representação contínua (amplitude contínua)
    - Medindo quantitativamente fenômenos da natureza e grandezas analógicas ou contínuas.
    - Temperatura, pressão, distância e som.
- Dispositivos Digitais:
    - Utilizam representação dígitos (amplitude discreta)
    - Medindo quantitativamente fenômenos da natureza e grandezas analógicas ou contínuas.

BLOCKCHAIN

- O que é BlockChain?
    - Colocar um timestamp em um documento digital
    - Evolução para cadeias de timestamps (carimbo de data), (listas contínuas)
    - Lista crescente de registros chamados de blocos
    - Uma cadeia de blocos - BlockChain
    - Utiliza função hash para criptografar as conexões sobre blockchain

- Características
    - Não pode ser corrompida
    - Descentralizada - várias cópias em diversos locais
    - Registros Distribuídos, registros mantidos por diversos usuários
    - Consenso, algoritmo de consenso que serve para validar a aceitação de registros na blockchain, esse registro é válido?
    - Acordos mais rápidos - em comparação a TED por exemplo

- O que é:
    - Desejo inserir na blockChain dados: “Max”
    - Além do dado, o **bloco atual** tem o hash do bloco anterior e o hash do bloco atual.
    - Se for o primeiro bloco (bloco gênesis) o hash anterior será 0000000.
    - Assim e forma a cadeia de blocos, com referências aos blocos anteriores

- Entendendo hash
    - Cada arquivo tem um hash único
    - Hash sem retorno, somente conversão para o hash.
    - Determinístico, para a mesma informação sempre se gera o mesmo hash.
    - Processamento rápido
    - Efeito avalanche - qualquer mínima alteração do arquivo deve gerar um hash completamente diferente.
    - Deve suportar colisões
    - EX. Hash SHA256 - 64 Caracteres

- Registros imutáveis
    - Verificação através do hashing do bloco anterior torna imutável
    - Ao inserir o bloco na blockchain, ele não é mais modificável, afinal, caso mude um bloco no meio, perde o registro de todos os blocos anteriores, afinal, irá modificar o hash

- Rede p2p distribuída
    - No mundo comum as informações estão centralizadas, em um hd, em um contrato de papel e é perdida em caso de algum incidente sobre essa central
    - A rede é descentralizada, múltiplas partes interessadas contém cópias, informações sobre toda a rede.
    - Caso alguma parte seja perdida, a informação não é perdida
    - A informação armazenada é a cadeia de blocos
    - Caso algum computador (interessado) sofra algum ataque, modificando o conteúdo de algum bloco, esse computador verifica que os seus dados estão diferentes de todos os demais.
    - Ao verificar isso ele descarta sua informação e recopia a cadeia dos demais computadores para garantir a integridade
    - Os dados modificados anteriormente pelo ataque foram descartados

- Mineração
    - Gerar um hash válido com os dados do bloco
    - Existem dados em um bloco, transações monetárias por exemplo.
    - Existe o hash atual e do bloco anterior
    - Número do bloco
    - Nonce - valor variável. Esse valor é alterado para conseguir achar um hash que comece com quarto 0s (0000)
    - A mineração vai alterando as informações, o nonce até achar um hash válido
    - quando achar, enviar para rede e esse bloco é válido
    - A rede vai validar se o conteúdo do bloco está na fila de transações (no caso do bitcoin ele valida se o conteúdo do bloco, as transações, estão na fila. Garantido que a única informação modificada é o nonce)

- Protocolos de consenso
    - Proof of Work - Pow - Há um objetivo a ser alcançado (em bitcoin, achar os 4 primeiros dígitos com 0) - ao cumpri-lo você ganha uma porcentagem de bitcoin
    - Proof of Stake - Pos - É validado com base na quantidade de moedas que um minerador possui. - usado no ethereum
    - Byzantine fault tolerance - BTF - usado pelo hyperledger - Não pode ter mais que ⅓ de nós atacantes. Rede permissionada, você controla quais nós fazem parte da rede

CONTAINERS

- Essencialmente os containers servem para que possamos isolar processos em um sistema operacional.

- Temos duas técnicas de virtualização bem características são elas a para-virt e a full-virt. Na virtualização clássica temos o que chamamos de HOSPEDEIRO (host) e CONVIDADO (guest). O sistema hospedeiro (host) é quem executa do software de virtualização, também chamado de "hypervisor". O sistema convidado (guest) é o sistema operacional que será executado dentro do hospedeiro (host).
- Na para-virtualização (para-virt) o sistema operacional virtualizado usa um kernel modificado que consegue se comunicar de forma mais livre com o hypervisor, podendo até acessar alguns componentes do hardware diretamente. Na virtualização completa (full-virt) o sistema operacional convidado (guest) utiliza um kernel normal que se comunica apenas com um hardware emulado pelo hypervisor, ele não fala diretamente com nenhum componente do hardware do hospedeiro (host)
- No uso de containers não temos um Hypervisor, o kernel linux se encarrega de isolar o processo utilizando recursos nativos.
- Os containers no linux são compostos por: Namespaces CGROUPS SecComp SELinux ou AppArmour
- Os Namespaces atuam no isolamento do container, eles dão ao container uma visão de um filesystem. Isso vai limitar o que um processo pode ver e os recursos que ele pode ou deve acessar. Dentro dos namespaces podemos trabalhar com: Users Filesystem/Mount Hostname Processes Network
- O CGROUPS vai nos ajudar a definir os limites para os recursos utilizados por um containers: CPU Memória Network I/O;
- O SECCOMP vai limitar as chamadas de sistema (syscalls) que um container pode fazer. No sistema operacional linux existem centenas de chamadas de sistemas que podem ser feitas, temos mais de 300 tipos de syscals. O SECCOMP vai filtrar quais chamadas de sistemas o container pode fazer e liberar apenas aquelas necessárias para que ele funcione. O SECCOMP funciona com conjuntos de configurações que se chamam profiles, cada tecnologia de containers tem seu próprio profile e syscalls liberados
- Camada de segurança: SELINUX é nativo em ambiente RedHat Like e o APPArmour de ambientes Debian-Like como ubuntu por exemplo. Essa camada de segurança protege o sistema operacional host em caso do comprometimento do mesmo através de uma aplicação em execução. Isso significa que caso um APP seja comprometida, ainda assim ela não irá conseguir alterar ou modificar partes sensíveis do sistema operacional.