## ext

| *EXT-2* | *EXT-3* | *EXT-4* |
|---|---|---|
| Ext2 does not have journaling feature. | The main benefit of ext3 is that it allows journaling. | Supports huge individual file size and overall file system size. |
| Maximum individual file size can be from 16 GB to 2 TB | Maximum individual file size can be from 16 GB to 2 TB | Maximum individual file size can be from 16 GB to 16 TB |

## Netstat

mostra informações sobre as conexões de rede, tabelas de roteamento e estatísticas da utilização da interface na rede.
Algumas opções do comando
−−tcp : mostra conexões TCP.
−−numeric : exibe apenas o endereço IP.
−−programs : indica qual processo está ouvindo a porta especificada.
−−all : mostra portas com conexões e portas que estão sendo ouvidas.
−−route : mostra a tabela de encaminhamento.
−−statistics : mostra as estatísticas da rede.
−−help : lista as opções do aplicativo.
−−version : mostra informações sobre o aplicativo.

## Microsoft Baseline Security Analyser (MBSA)

O Microsoft Baseline Security Analyzer (MBSA) é uma ferramenta fácil de usar que ajuda empresas de pequeno e médio porte a determinar o estado de sua segurança de acordo com as recomendações de segurança da Microsoft e oferece diretrizes de correção específicas. Aprimore o processo de gerenciamento da segurança usando o MBSA para detectar erros comuns de configuração relacionados à segurança e atualizações de segurança que estão faltando nos seus sistemas de computador.

## Microsoft Baseline Security Analyser (MBSA) (cont)

Criado a partir do Windows Update Agent e da infra-estrutura do Microsoft Update, o MBSA assegura a consistência com os demais produtos de gerenciamento Microsoft, inclusive MU (Microsoft Update), WSUS (Windows Server Update Services), SMS (Systems Management Server), SCCM (System Center Configuration Manager) 2007 e SBS (Small Business Server).
Usado por muitos dos principais auditores de segurança e fornecedores de segurança de terceiros, o MBSA examina, em média, mais de três milhões de computadores semanalmente. Junte-se a milhares de usuários que contam com o MBSA para análise do estado de segurança.
O Microsoft Baseline Security Analyzer (MBSA) também pode ser executado através de linha de comando usando o “mbsacli.exe”, com isso você pode montar um script .BAT, .VBS e automatizar sua verificação gerando os relatórios.

## Classe de Fogos

| Classe | Descrição |
|---|---|
| A | Ocorre em materiais como papel, tecido, algodão, borracha, madeira e outros que queimam em profundidade e extensão e deixam resíduos. Nesse caso, o extintor que deve ser usado para combater as chamas é o à base de água. |
| B | É o incêndio que acontece em óleo, gasolina, álcool, tinta e outros líquidos inflamáveis. Para combater esse tipo de fogo, é preciso utilizar o extintor à base de pó químico ABC, para abafar e interromper a combustão imediatamente. |

## Classe de Fogos (cont)

| | |
|---|---|
| C | Quando o incêndio ocorre em máquinas elétricas, transformadores, geradores, quadros de força, equipamentos de informática e outros equipamentos ligados à energia ou energizados, acontece o incêndio de Classe C. |
| D | Entre as classes de incêndio, essa é uma das menos comuns. Zircônio, zinco, titânio, lítio e urânio são alguns exemplos de metais que podem dar origem a esse tipo de incêndio, já que são propensos a ter combustão instantânea. |
| K | Normalmente, o incêndio classe K acontece em cozinhas. Trata-se da ocorrência em óleos vegetais ou gordura animal. Nesse caso, o extintor que deve ser utilizado é específico para esse fim, já que resfria o meio de cozimento e abaixa a temperatura. |

## Rainbow Series

| Color | Meaning |
|---|---|
| Green | Password |
| Red | Integridade e Disponibilidade |
| Orange | Confidentiality |

## mkfs

O comando mkfs no Linux formata a partição criada pelo fdisk / gdisk / parted com o sistema de arquivos.
O tipo de sistema de arquivos é definido pela opção –t e são os formatos nativos ext2, ext3, ext4, fat, vfat, minix, msdos e xfs
Os comandos mke2fs e mkdosfs são variações do mkfs.
mkfs.ext3, mkfs.ext4

By **xoulea**
cheatography.com/xoulea/

Published 8th January, 2024.
Last updated 8th January, 2024.


Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## mkfs (cont)

-t: Informa qual o tipo de formatação a partição deverá ser
-c: Verifica a existência de bad blocks (defeitos) no dispositivo;
-L: nome Configura o nome do dispositivo;
-n: nome Configura o nome do dispositivo para o formato msdos;
-q: Faz com que o mkfs trabalhe com o mínimo de saída no vídeo possível;
-v: Faz com que o mkfs trabalhe com o máximo de saída no vídeo possível;
-m: Percentual de disco reservado

## Registros DNS

| Registro | Significado |
|---|---|
| A | registro que contém o endereço IP de um domínio |
| AAAA | Registro que contém o endereço IPv6 para um domínio (ao contrário dos registros A, que listam o endereço IPv4) |
| CNAME | encaminha um domínio ou subdomínio para um outro domínio; NÃO fornece um endereço IP. |
| MX | direciona o e-mail para um servidor de e-mails. |
| TXT | Permite que um administrador armazene notas de texto no registro. Esses registros são frequentemente usados para segurança de e-mail. |
| NS | armazena o nameserver de uma entrada de DNS. |
| SOA | armazena informações de administrador sobre um domínio. |
| SRV | especifica uma porta para serviços específicos |

## Registros DNS (cont)

| | |
|---|---|
| PTR | ornece um nome de domínio em pesquisas inversas |
| CAA | trata-se do registro de "autorização da autoridade certificadora"; permite que os proprietários do domínio indiquem quais autoridades certificadoras podem emitir certificados para esse domínio. Quando não existe nenhum registro CAA, qualquer pessoa pode emitir um certificado para o domínio. Esses registros também são herdados pelos subdomínios. |
| APL | a "lista de prefixos de endereços" é um registro experimental que especifica listas de intervalos de endereços. |

## PAP VS CHAP VS EAP

Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point-to-Point Protocol (PPP) to validate users.PAP is also used to describe password authentication in other protocols such as RADIUS and Diameter. However, those protocols provide for transport or network layer security, and therefore that usage of PAP does not have the security issues seen when PAP is used with PPP.
In computing, the Challenge-Handshake Authentication Protocol (CHAP) is an authentication protocol originally used by Point-to-Point Protocol (PPP) to validate users. CHAP is also carried in other authentication protocols such as RADIUS and Diameter. Almost all network operating systems support PPP with CHAP, as do most network access servers. CHAP is also used in PPPoE, for authenticating DSL users.

## PAP VS CHAP VS EAP (cont)

PAP (Password Authentication Protocol) que é um protocolo de controle de acesso utilizado para autenticar a senha do usuário no servidor de acesso à rede. O servidor de acesso à rede pede uma senha a partir da máquina cliente e envia a senha recuperada de um servidor de autenticação para verificação. Como um protocolo de autenticação, PAP é considerado o menos seguro, porque a senha não é criptografada na transmissão.
CHAP (Challenge Handshake Authentication Protocol) que é semelhante ao PAP com várias características únicas. Em vez de pedir uma senha, o servidor de acesso à rede envia uma mensagem de desafio para a máquina cliente. A mensagem de desafio é um valor aleatório. A máquina cliente criptografa a mensagem de desafio com a senha do usuário e envia a combinação de volta para o servidor de acesso. Os atacantes servidor de acesso a combinação usuário / senha para o servidor de autenticação. O servidor de autenticação criptografa o desafio com a senha do usuário armazenados no banco de dados de autenticação. Se a resposta do usuário é um jogo, a senha é considerada autêntica. CHAP usa o modelo de um segredo compartilhado (a senha do usuário) para autenticar o usuário. O uso de CHAP é considerado um método moderadamente seguro de autenticação.. EAP (Extensible Authentication Protocol) que é considerado um quadro de autenticação usado por uma série de protocolos de autenticação seguros. EAP mais comumente usado para autenticação em redes sem fio.



Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## IMAP x POP3

IMAP - manipular um arquivo remotamente sem baixar para a maquina
POP3 - manipular um arquivo porém realizando download para a máquina

## IEEE 802.11

| Standard | Max Bit Rate | Frequency | Generation |
|---|---|---|---|
| 802.11 | 1–2 | 2.4 | Wi-Fi 0 |
| 802.11b | 1–11 | 2.4 | Wi-Fi 1 |
| 802.11a | 6–54 | 5 | Wi-Fi 2 |
| 802.11g | 6–54 | 2.4 | Wi-Fi 3 |
| 802.11n | 72–600 | 2.4, 5 | Wi-Fi 4 |
| 802.11ac | 433–6933 | 5 | Wi-Fi 5 |
| 802.11ax | 574–9608 | 2.4, 5, 6 | Wi-Fi 6, Wi-Fi 6E |
| 802.11be | 1376–46120 | 2.4, 5, 6 | Wi-Fi 7 |

## DSL

xDSL, a term that encompasses the broad range of digital subscriber line (DSL) services, offers a low-cost, high-speed data transport option for both individuals and businesses, particularly in areas without access to cable internet.
*HDSL (High-Bit-Rate DSL)*
Standardized in 1994, HDSL uses two pairs of 24 AWG copper wires to provide symmetric E1/T1 data rates to distances up to 3657 meters. Its successors are HDSL2 and HDSL4, the latter using four pairs of wire instead of two.
*SDSL (Symmetric DSL)*

## DSL (cont)

SDSL succeeded HDSL as the two-wire (single-pair) type of symmetric DSL. SDSL is also known within ANSI as HDSL2. Essentially offering the same capabilities as HDSL, SDSL offers T1 rates (1.544 Mbps) at ranges up to 10,000 feet and is primarily designed for business applications.
*ADSL: Asymmetric DSL*
ADSL provides transmission speeds ranging from downstream/upstream rates of 9 Mbps/640 kbps over a relatively short distance to 1.544 Mbps/16 kbps as far as 18,000 feet. The former speeds are more suited to a business, the latter more to the computing needs of a residential customer. ADSL's substantial bandwidth accommodates large downstream transmissions, such as receiving data from a host computer or downloading multimedia files.
*SHDSL: Single-Pair, High-Speed Digital Subscriber Line*
Also known as G.SHDSL, this type of DSL transmits data at much higher speeds than older types of DSL. It enables faster transmission and connections to the internet over regular copper telephone lines than traditional voice modems can provide. Support of symmetrical data rates makes SHDSL a popular choice for businesses using PBXs, private networks, web hosting and other services.
SHDSL can be used effectively in enterprise LAN applications. When interconnecting sites on a corporate campus, buildings and network devices are often beyond the reach of a standard Ethernet segment. Now you can use existing copper network infrastructure to connect remote LANs across longer distances and at higher speeds than previously thought possible. Ratified as a standard in 2001, SHDSL combines ADSL and SDSL features for communications over two or four (multiplexed) copper wires.

## DSL (cont)

SHDSL provides symmetrical upstream and downstream transmission with rates ranging from 192 kbps to 2.3 Mbps. As a departure from older DSL services designed to provide higher downstream speeds, SHDSL specified higher upstream rates, too. Higher transmission rates of 384 kbps to 4.6 Mbps can be achieved using two to four copper pairs. The distance varies according to the loop rate and noise conditions.. *VDSL: Very-High-Bit-Rate DSL*
Also approved in 2001, VDSL as a DSL service enables downstream/upstream rates up to 52 Mbps/16 Mbps. Extenders for local networks boast 100-Mbps/60-Mbps speeds when communicating at distances up to 500 feet (152.4 m) over a single voice-grade twisted pair. As a broadband solution, VDSL enables the simultaneous transmission of voice, data, and video, including HDTV, video on demand and high-quality video conferencing. Depending on the application, you can set VDSL to run symmetrically or asymmetrically.. *VDSL2: Very-High-Bit-Rate DSL 2*
Standardized in 2006, VDSL2 provides higher bandwidth (up to 100 Mbps) and higher symmetrical speeds than VDSL, enabling its use for Triple Play services (data, video, voice) at longer distances. While VDSL2 supports upstream/downstream rates similar to VDSL, at longer distances, the speeds don't deteriorate as much as those transmitted with ordinary VDSL equipment.

## Rainbow Table

A rainbow table is a precomputed table for caching the outputs of a cryptographic hash function, usually for cracking password hashes. Passwords are typically stored not in plain text form, but as hash values.

By **xoulea**
cheatography.com/xoulea/

Published 8th January, 2024.
Last updated 8th January, 2024.


Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## Rainbow Table (cont)

If such a database of hashed passwords falls into the hands of an attacker, they can use a precomputed rainbow table to recover the plaintext passwords. A common defense against this attack is to compute the hashes using a key derivation function that adds a "salt" to each password before hashing it, with different passwords receiving different salts, which are stored in plain text along with the hash.. Rainbow tables are a practical example of a space–time tradeoff: they use less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple table that stores the hash of every possible password.

## ACL - Access Control List

A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access.

There are two basic kinds of ACLs:

- Filesystem ACLs: These work as filters, managing access to directories or files. A filesystem ACL gives the operating system instructions as to the users that are allowed to access the system, as well as the privileges they are entitled to once they are inside.
- Networking ACLs: Networking ACLs manage access to a network. To do this, they provide instructions to switches and routers as to the kinds of traffic that are allowed to interface with the network. They also dictate what each user or device can do once they are inside.

## ACL - Access Control List (cont)

When ACLs were first conceived, they worked like firewalls, blocking access to unwanted entities. While many firewalls have network access control functions, some organizations still use ACLs with technologies such as virtual private networks (VPNs). In this way, an administrator can dictate which kinds of traffic get encrypted and then sent through the secure tunnel of the VPN.

NACL

An access control list on a router consists of a table that stipulates which kinds of traffic are allowed to access the system. The router is placed between the incoming traffic and the rest of the network or a specific segment of the network, such as the demilitarized zone (DMZ). The ACL examines the information held within data packets flowing into or out of the network to determine where it came from and where it is going. The ACL on the router then decides whether the data packet should be allowed to pass to the other side..

## Agentes Extintores

| Tipo | Descrição |
|---|---|
| Agua | Age por resfriamento. São utilizados em incêndios Classe A, ou seja, em materiais sólidos como madeira, tecidos, papel, borracha e plástico. Em hipótese alguma deve ser usado em líquidos e gases inflamáveis e em equipamentos elétricos. |

## Agentes Extintores (cont)

| | |
|---|---|
| CO2 | O gás age por abafamento, extinguindo o oxigênio do local, impossibilitando assim, que a reação do fogo ocorra. São indicados para incêndios classe B e C. E estes são exatamente os casos em que a água não surte efeito, líquidos e gases inflamáveis e em equipamentos elétricos. |
| Pó Quimico BC | São utilizados para as mesmas classes de incêndio (B e C) que o extintor de CO2. Mas ao invés de agir por abafamento, age por meio de reações químicas do bicarbonato de sódio. |
| Pó Quimico ABC | Este é o agente químico mais completo. Pode ser utilizado em qualquer classe de incêndio. Ele extingue o fogo através do abafamento por fosfato monoamônico. |
| Espuma Mecanica | Combatem as classes de incêndio A e B. São muito utilizados em locais que possuem armazenagem de líquidos e gases inflamáveis. A espuma age por resfriamento e abafamento. |

## NBTSTAT

Exibe as estatísticas de protocolo NetBIOS sobre TCP/IP (NetBT), as tabelas de nomes NetBIOS dos computadores local e remoto e o cache de nomes NetBIOS. Nbtstat permite uma atualização do cache de nomes NetBIOS e dos nomes registrados com o serviço de cadastramento na Internet do Windows (WINS). Quando usado sem parâmetros, nbtstat exibe a ajuda.



Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## NBTSTAT (cont)

Sintaxe
nbtstat [-a nome_remoto] [-A endereço_IP] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [intervalo]
Parâmetros
-a nome_remoto
Exibe a tabela de nomes NetBIOS de um computador remoto, onde nome_remoto é o nome de computador NetBIOS do computador remoto. A tabela de nomes NetBIOS é a lista de nomes NetBIOS que correspondem aos aplicativos em execução no computador.
-A endereço_IP
Exibe a tabela de nomes NetBIOS de um computador remoto, especificado pelo seu endereço IP (com notação de ponto decimal).
-c
Exibe o conteúdo do cache de nomes NetBIOS, a tabela de nomes NetBIOS e seus endereços IP resolvidos.
-n
Exibe a tabela de nomes NetBIOS do computador local. O status Registrado indica que o nome foi registrado por difusão ou em um servidor WINS.
-r
Exibe as estatísticas de resolução de nomes NetBIOS. Em um computador com o Windows XP configurado para usar WINS, esse parâmetro retorna o número de nomes resolvidos e registrados via difusão ou via WINS.
-R
Limpa o conteúdo do cache de nomes NetBIOS e recarrega as entradas marcadas com #PRE do arquivo Lmhosts.
-RR
Libera e atualiza nomes NetBIOS para o computador local registrado em servidores WINS.
-s

## NBTSTAT (cont)

Exibe sessões de cliente e servidor NetBIOS, tentando converter o endereço IP de destino em um nome.
-S
Exibe as sessões de cliente e de servidor NetBIOS, listando os computadores remotos somente por endereço IP de destino.
intervalo

## Kerberos

Kerberos é um protocolo de autenticação usado para verificar a identidade de um usuário ou host.
Kerberos é um Protocolo de rede, que permite comunicações individuais seguras e identificadas, em uma rede insegura.
O protocolo Kerberos previne Eavesdropping e Replay attack, e ainda garante a integridade dos dados. Seus projetistas inicialmente o modelaram na arquitetura cliente-servidor, e é possível a autenticação mutua entre o cliente e o servidor, permitindo assim que ambos se autentiquem.
Kerberos utiliza Criptografia simétrica e necessita de um sistema de confiança tripla.
Kerberos é um protocolo desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor, onde ele funciona como a terceira parte neste processo, oferendo autenticação ao usuário.
Para garantir a segurança, ele usa criptografia de chave simétrica, com o DES.

## Sistemas de Arquivos

NTFS é o sistema de arquivos padrão do Windows, mais moderno e indicado para dispositivos de armazenamento não removíveis, como disco rígido (HD) e disco de estado sólido (SSD).

## Sistemas de Arquivos (cont)

O FAT32 é similar ao NTFS, sendo mais antigo e menos eficiente, porém é o que tem maior compatibilidade com dispositivos removíveis, como pen drives e cartões SD. Já o exFAT é o “meio termo” entre eles: tem recursos avançados como o NTFS e também é utilizado em dispositivos portáteis, mas não é tão popular quanto o FAT32.
*NTFS* é o sistema de arquivos padrão do Windows. Foi criado pela Microsoft para resolver as limitações do FAT32, até então o sistema mais utilizado. É mais seguro, tem recursos avançados de recuperação (backup) de arquivos, suporte para discos rígidos maiores, configurações de controle e acesso a arquivos, suporte a criptografia, entre outras vantagens.
A maior desvantagem do NTFS é a falta de compatibilidade com outros sistemas operacionais. O macOS lê arquivos do NTFS, mas não consegue gravar na partição. A compatibilidade com Linux varia de acordo com a distribuição.
*FAT32* é o sistema de arquivos mais antigo dos três. Sua maior vantagem é a compatibilidade: pode ser lido e gravado por qualquer sistema operacional e quase todo dispositivo com uma porta USB; por isso, é considerado como o formato “padrão” para dispositivos de armazenamento móveis, como pen drives e cartões de memória.
Ele é prático, mas possui limitações consideráveis: não suporta partições maiores do que 8TB, não aceita arquivos maiores do que 4GB, não possui regras de acesso e segurança como o NTFS, e geralmente é mais lento para ler e gravar arquivos do que os outros sistemas.



Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## Sistemas de Arquivos (cont)

O *exFAT* foi criado para resolver os problemas do FAT32, porém mantendo a alta compatibilidade entre dispositivos. Oferece suporte a arquivos grandes (bem maiores do que 4GB), é mais rápido do que o FAT32, e pode ser lido e gravado nativamente pelo sistema operacional da Apple, enquanto que no Linux basta instalar as extensões corretas.
O exFAT foi pensado para dispositivos flash (pen drives, cartões de memória, SSD, celulares, etc), mas apesar de ser mais compatível do que o NTFS, alguns equipamentos mais antigos podem não reconhecer ou aceitar o formato.

## Job Control Signal

| Signal | Description |
|---|---|
| SIGCHLD | This signal is sent to a parent process whenever one of its child processes terminates or stops. |
| SIGCONT | You can send a SIGCONT signal to a process to make it continue. This signal is special—it always makes the process continue if it is stopped, before the signal is delivered. The default behavior is to do nothing else. You cannot block this signal. You can set a handler, but SIGCONT always makes the process continue regardless. |
| SIGSTOP | The SIGSTOP signal stops the process. It cannot be handled, ignored, or blocked. |
| SIGTSTP | The SIGTSTP signal is an interactive stop signal. Unlike SIGSTOP, this signal can be handled and ignored. |

## Job Control Signal (cont)

| | |
|---|---|
| SIGTTIN | A process cannot read from the user's terminal while it is running as a background job. When any process in a background job tries to read from the terminal, all of the processes in the job are sent a SIGTTIN signal. The default action for this signal is to stop the process. |
| SIGTTOU | This is similar to SIGTTIN, but is generated when a process in a background job attempts to write to the terminal or set its modes. Again, the default action is to stop the process. |

## RAID

Tipos de configurações de RAID
Existem, também, diferentes tipos de configuração RAID, que estão presentes nos diferentes níveis desse recurso, como veremos mais à frente. Abaixo, você confere os três tipos de configuração e como funcionam. Continue acompanhando!
Divisão de dados (striping):
Esse tipo permite a leitura e gravação de dados em tempo real, aumentando a performance. O ponto negativo dessa abordagem é que se houver falha em um dos HDs, todos os dados serão comprometidos.
Espelhamento (mirroring):
Grava os mesmos dados em ambos os discos, fornecendo maior segurança dos dados. Com isso, se um dos HDs falhar, as informações estarão salvas no outro.
Paridade (parity):
Armazena informações de forma que se houver perda de dados em um dos discos, os mesmos serão restaurados. Assim, garantindo ótima redundância dos dados.
RAID 0:

## RAID (cont)

Striping ou matriz de distribuição, neste RAID são necessários no mínimo 2 discos. Nele, todos os HDs trabalham simultaneamente no processo de leitura e gravação dos dados. Assim, as informações ficam fragmentadas, com um "pedaço" gravado em cada disco.
Tolerância a falha: nenhuma
Ganho de velocidade de leitura: 2x
Ganho de velocidade de gravação: 2x
RAID 1:
Com configuração Mirroring, este RAID espelha os dados. Ou seja, cria uma cópia de todas as informações em tempo real, produzindo basicamente uma cópia de segurança. Em outras palavras, as informações de um HD são gravadas também no outro.
Tolerância a falha: 1 disco em falha
Ganho de velocidade de leitura: 2x
Ganho de velocidade de gravação: nenhuma
RAID 5:
Esse nível de RAID é indicado para quem precisa de alta capacidade e segurança das informações e são necessários, no mínimo, 3 discos para sua execução. Nele, só é considerado o espaço equivalente a 1 dos HDs para manter a redundância, independente de quantos discos há.
Tolerância a falha: 1 disco em falha
Ganho de velocidade de leitura: 3x em caso de quatro discos (para mais discos: número de discos – 1)
Ganho de velocidade de gravação: nenhuma
RAID 10 ou 1+0:
Este RAID é a junção do espelhamento do RAID 1 mais a performance do RAID 0. Ele utiliza Divisão de Dados e Espelhamento, só podendo ser executado por no mínimo 4 HDs. E, nele, os dados são divididos em blocos que são escritos em todos os HDs, de forma simultânea.
olerância a falha: pelo menos 1 disco em falha



Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

## RAID (cont)

Ganho de velocidade de leitura: 4x em caso de 4 discos (para mais discos: número total de discos)
Ganho de velocidade de gravação: 2x em caso de 4 discos (para mais discos: número total de discos / 2)

## HALON

O halon consiste num composto químico orgânico constituído por um ou dois átomos de carbono, ligados a um átomo de bromo e a outro halogéneo. Os mais utilizados são o Halon 1211 (bromoclorodifluormetano) e o Halon 1301 (bromotrifluormetano). Os halons são gases muito utilizados em extintores de incêndios. São até dez vezes mais perigosos do que os clorofluorocarbonetos (CFC), aos quais se encontram quimicamente relacionados, na destruição da camada de ozônio. Os níveis de halon na atmosfera aumentam cerca de 25% ao ano, principalmente devido aos testes de equipamento de combate a incêndios.. - Halon 1211 is used only in portable extinguishers and is a streaming agent
- Halon 1301 is used only in fixed extinguisher installations typically cargo holds or engines and is a total flooding agent.

## IGMP

O Protocolo de Gerenciamento de Grupos da Internet (IGMP) é um protocolo que permite que vários dispositivos compartilhem um endereço de IP para que todos possam receber os mesmos dados. O IGMP é um protocolo de camada de rede usado para configurar multicast em redes que usam o protocolo de internet versão 4 (IPv4). Especificamente, o IGMP permite que os dispositivos se juntem a um grupo de multicast.

## IGMP (cont)

Computadores e outros dispositivos conectados a uma rede usam IGMP quando desejam ingressar em um grupo multicast. Um roteador que suporta IGMP escuta transmissões IGMP de dispositivos para descobrir quais dispositivos pertencem a quais grupos multicast.
O IGMP usa endereços de IP que são reservados para multicast. Os endereços de IP multicast estão no intervalo entre 224.0.0.0 e 239.255.255.255. (Em contraste, as redes anycast podem usar qualquer endereço de IP normal.) Cada grupo multicast compartilha um desses endereços de IP. Quando um roteador recebe uma série de pacotes direcionados ao endereço de IP compartilhado, ele duplica esses pacotes, enviando cópias para todos os membros do grupo multicast. Os grupos multicast IGMP podem mudar a qualquer momento. Um dispositivo pode enviar uma mensagem IGMP "ingressar no grupo" ou "sair do grupo" a qualquer momento.



Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com