# Prova 2 - Respostas Experimentos

| | |
|---|---|
| Created | @February 8, 2023 9:40 PM |
| Class | |
| Type | |
| Materials | |

## DHCP

1. Coloque um analisador de tráfego (Wireshark, tcpdump ou similar) de modo a identificar os tipos de diálogos existentes entre a estação de trabalho que está requisitando um endereço IP e o servidor DHCP. Anote a sequência de mensagens e apresente-as, associadas a uma pequena explicação sobre cada uma delas.

Os diálogos entre uma estação de trabalho e um servidor DHCP podem ser resumidos em quatro etapas:

1. Solicitação DHCPDISCOVER: a estação de trabalho envia uma mensagem de broadcast para todos os servidores DHCP na rede solicitando uma oferta de endereço IP.
2. Oferta DHCPOFFER: os servidores DHCP recebem a solicitação e enviam uma oferta de endereço IP para a estação de trabalho.
3. Solicitação DHCPREQUEST: a estação de trabalho escolhe a oferta de endereço IP que deseja e envia uma solicitação ao servidor DHCP para confirmar a atribuição do endereço IP.
4. Confirmação DHCPACK: o servidor DHCP confirma a atribuição do endereço IP e envia uma mensagem de confirmação para a estação de trabalho. A partir deste momento, a estação de trabalho tem o endereço IP atribuído e pode comunicar-se com outros dispositivos na rede.

Essas quatro etapas formam o diálogo básico entre uma estação de trabalho e um servidor DHCP para obtenção de um endereço IP.

2. Faça uma alteração no servidor DHCP de modo que ele ofereça endereços IP apenas para as estações de trabalho, cujo MAC Address esteja previamente reconhecido pelo servidor DHCP.

Para que um servidor DHCP forneça endereços IP com base em endereços MAC previamente conhecidos, você precisa configurar reservas de endereço no servidor DHCP. Isso significa associar um endereço MAC específico a um endereço IP específico, de modo que o servidor DHCP sempre atribua o mesmo endereço IP a um determinado dispositivo quando ele solicitar uma atribuição de endereço.

Aqui estão os passos gerais para configurar uma reserva de endereço em um servidor DHCP:

1. Identifique o endereço MAC e o endereço IP desejados para a reserva.
2. Acesse a interface de gerenciamento do servidor DHCP.
3. Navegue até a seção de configuração de reservas de endereço.
4. Adicione uma nova reserva, especificando o endereço MAC e o endereço IP desejados.
5. Salve as alterações e reinicie o servidor DHCP.

3. Se colocarmos mais de um servidor DHCP na rede, o que pode acontecer? Faça testes e mostre suas conclusões.

Ter mais de um servidor DHCP em uma rede pode causar problemas, pois pode haver conflitos entre os servidores quanto ao fornecimento de endereços IP. Alguns dos problemas mais comuns incluem:

1. Conflitos de endereços IP: se dois servidores atribuírem o mesmo endereço IP para dispositivos diferentes na mesma rede, ocorrerá um conflito de endereços IP e os dispositivos não conseguirão se comunicar corretamente.
2. Instabilidade de rede: se dispositivos na rede estiverem constantemente alternando entre diferentes servidores DHCP, isso pode causar interrupções na comunicação e instabilidade na rede.
3. Duplicidade de endereços IP: se dois servidores atribuírem o mesmo endereço IP para o mesmo dispositivo, o dispositivo poderá ter problemas para se comunicar corretamente com outros dispositivos na rede.

# DNS

1. Qual é o retorno do comando dnsdomainname? O que significa?

O comando "dnsdomainname" é um comando Unix/Linux que retorna o nome de domínio da máquina local. Ele exibe o nome de domínio da máquina, que é o sufixo usado para identificar o domínio da Internet em que a máquina está registrada.

O nome de domínio é composto por vários componentes, separados por pontos, que formam uma hierarquia de nomes de domínios. O componente mais a direita é o nome de topo de nível (TLD, na sigla em inglês), como .com, .org, .net, etc. Os componentes à esquerda representam subdomínios do TLD, cada um identificando uma parte específica da organização.

Por exemplo, se o comando "dnsdomainname" retornar "example.com", isso significa que a máquina está registrada no domínio "example.com" e pode ser acessada como "nome_da_maquina.example.com".

Nota: O comando "dnsdomainname" só funciona em sistemas que têm uma configuração de rede válida e acesso a um servidor DNS para resolver nomes de domínios.

2. O que é o nome localhost? E o endereço 127.0.0.1 dado a ele no arquivo /etc/hosts? Por que deve sempre existir este endereço e nome em sistemas UNIX/Linux?

"Localhost" é um nome especial usado para se referir à própria máquina em um sistema operacional Unix/Linux. O endereço IP "127.0.0.1" é atribuído a ele no arquivo de hosts "/etc/hosts" e é conhecido como o "endereço de loopback".

O endereço de loopback permite que um sistema envie pacotes de rede para si mesmo sem a necessidade de uma rede física. Isso é útil para testes de rede, aplicativos e serviços que precisam se comunicar com a própria máquina, ou para acessar serviços em execução na própria máquina sem precisar usar seu endereço IP real.

Por isso, é importante que o endereço de loopback e o nome "localhost" sempre estejam presentes no arquivo "/etc/hosts" em sistemas Unix/Linux. Isso garante que esses recursos sempre estarão disponíveis para os aplicativos e serviços que precisam usá-los, mesmo se a configuração de rede da máquina mudar ou se o acesso a um servidor DNS estiver indisponível.

3. O que é o FQDN?

FQDN significa Fully Qualified Domain Name (Nome de Domínio Totalmente Qualificado, em português).

O FQDN é uma forma de identificar uma máquina na Internet ou em uma rede privada, composta pelo nome da máquina e pelo nome de domínio completo. Ele fornece uma identificação única e completa de uma máquina na rede e permite que ela seja localizada e acessada por outros dispositivos.

Por exemplo, se uma máquina tem o nome "host1" e está registrada no domínio "example.com", seu FQDN seria "host1.example.com". Este nome pode ser usado para acessar a máquina em uma rede ou pela Internet, e permite que ela seja identificada de forma clara e unívoca.

O FQDN é importante para muitos aspectos da administração de redes, incluindo a configuração de serviços de rede, o acesso a serviços remotos, a resolução de nomes e a segurança. Por isso, é importante que cada máquina tenha um FQDN válido e único na rede.

4. Podemos ter 2 servidores DNS na mesma rede? Qual é a configuração mais adequada para esta situação?

Sim, é possível ter mais de um servidor DNS na mesma rede. A configuração mais adequada para esta situação depende das necessidades da rede e dos objetivos de segurança e disponibilidade.

Uma configuração comum é ter dois servidores DNS com configurações primário e secundário. O servidor primário é responsável por responder aos pedidos de resolução de nome e mantém uma cópia atualizada dos registros de nome da rede. O servidor secundário é responsável por replicar os registros do servidor primário e pode ser usado como backup em caso de falha do servidor primário. **-> rede menor**

Outra configuração possível é ter mais de um servidor DNS configurado como servidor primário. Isso é conhecido como configuração de cluster de servidores DNS. Nesta configuração, os servidores DNS trabalham em conjunto para responder aos pedidos de resolução de nome e compartilham a carga de trabalho. Isso pode melhorar a disponibilidade e a escalabilidade do serviço DNS. **-> rede maior**

5. O que é DNS reverso?

O DNS reverso (também conhecido como DNS inverso) é uma função do sistema de nomes de domínio (DNS) que permite a tradução de endereços IP em nomes de máquinas. Em contraposição ao DNS normal, que traduz nomes de máquinas em endereços IP, o DNS reverso realiza a tradução inversa.

O DNS reverso é utilizado principalmente para identificar de forma clara e precisa as máquinas em uma rede a partir de seus endereços IP. Ele é usado por outros serviços de rede, como serviços de correio eletrônico, para validar o endereço IP de uma máquina e verificar se ela é uma fonte confiável.

A configuração de um servidor de DNS reverso requer a criação de uma zona de pesquisa inversa que contém registros que associam endereços IP a nomes de máquinas. Essa zona é atualizada periodicamente para refletir as mudanças na rede e garantir a precisão das informações de resolução de nome.

6. O que é a entrada MX inserida no domínio? Podem haver mais de uma?

A entrada MX (Mail Exchange) é um registro no sistema de nomes de domínio (DNS) que especifica o endereço IP de um ou mais servidores de correio eletrônico responsáveis por receber e entregar mensagens de e-mail para um domínio específico. O registro MX é importante para garantir que as mensagens de correio eletrônico sejam entregues corretamente às contas de e-mail associadas a um domínio.

Sim, é possível ter mais de uma entrada MX para um domínio. Isso é frequentemente usado para criar uma configuração de failover, onde um servidor de correio secundário é designado como backup caso o servidor principal falhe ou fique inacessível. Além disso, múltiplas entradas MX permitem a distribuição de carga entre vários servidores de correio eletrônico, o que pode melhorar a velocidade e a disponibilidade do correio eletrônico para os usuários do domínio.

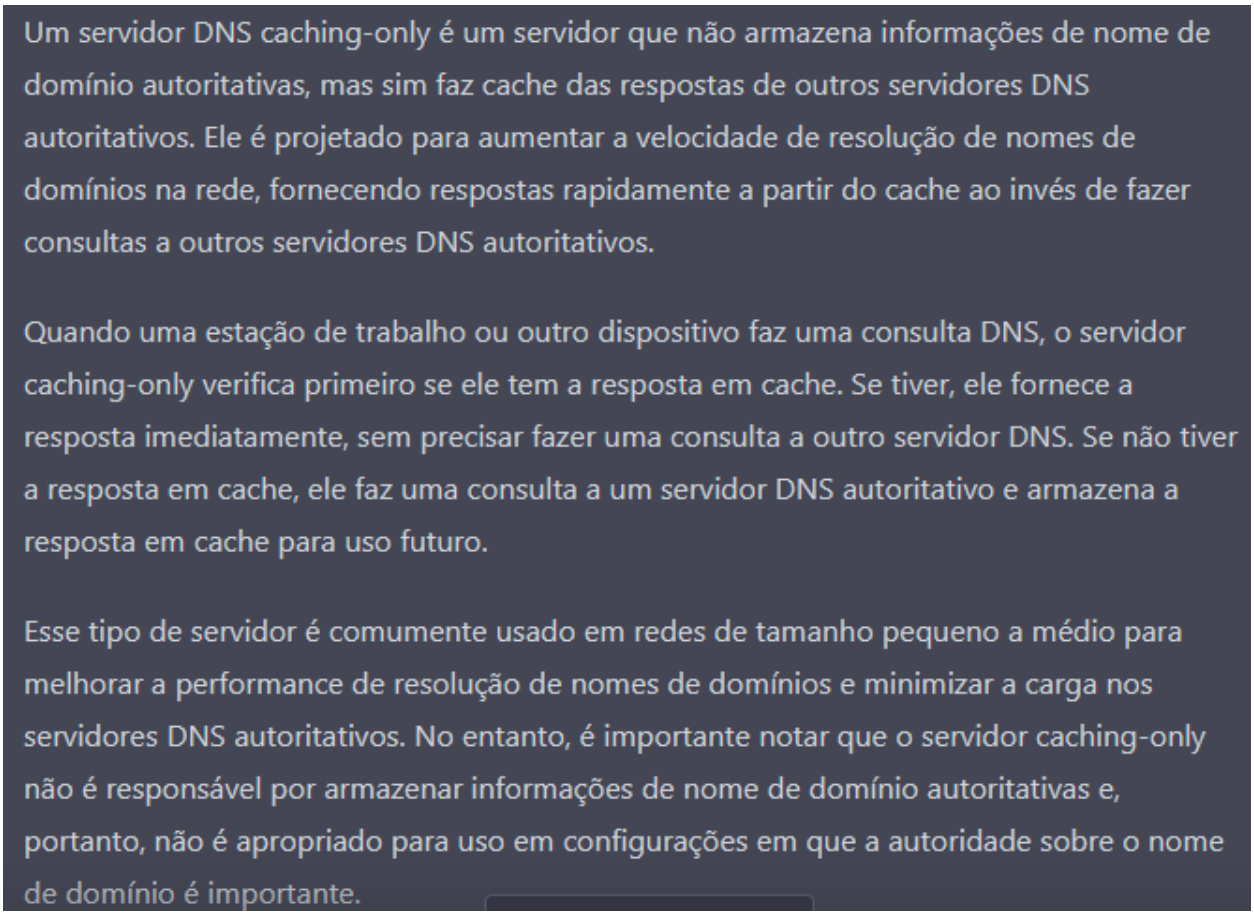
7. O que é resposta autoritativa dada por um servidor DNS?

Uma resposta autoritativa é uma resposta dada por um servidor de nomes de domínio (DNS) que tem autoridade para responder sobre um determinado domínio. O servidor autoritativo é responsável por armazenar e gerenciar as informações de nome e endereço IP para um domínio específico, como as entradas A, MX, CNAME, entre outras.

Quando uma estação de trabalho ou outro dispositivo faz uma consulta DNS para resolver um nome de domínio em um endereço IP, o servidor DNS inicia uma busca na hierarquia DNS, começando pelos servidores raiz e seguindo para os servidores TLD (Top Level Domain) e, finalmente, para os servidores autoritativos para o domínio específico.

Se a resposta for fornecida por um servidor autoritativo, ela é considerada autoritativa e é confiável. Isso significa que a resposta é a informação correta e atualizada sobre o nome de domínio e seu endereço IP associado. Caso contrário, se a resposta for fornecida por um servidor DNS não autoritativo, ela não é considerada confiável e pode não ser a informação correta ou atualizada.

8. O que é um servidor caching-only?




# SMTP

1. Qual a diferença entre o armazenamento de e-mails no formato mbox e maildir?

mbox é o formato de armazenamento de e-mails mais antigo e amplamente utilizado. Nele, todos os e-mails de uma caixa de correio são armazenados em um único arquivo, geralmente chamado de "mbox". Esse formato é simples e fácil de usar, mas tem algumas desvantagens:

- O arquivo mbox pode ficar muito grande, tornando-se lento e difícil de gerenciar.
- O arquivo mbox é um arquivo único, o que significa que todos os e-mails são bloqueados enquanto o arquivo é lido ou escrito. Isso pode causar problemas de performance em sistemas com muitos usuários ou com alta taxa de entrada de e-mails.

Maildir, por outro lado, é um formato de armazenamento de e-mails mais recente que resolve muitas das desvantagens do mbox. Em vez de armazenar todos os e-mails em um único arquivo, cada e-mail é armazenado em um arquivo separado na pasta "maildir". Isso permite que os e-mails sejam lidos e escritos independentemente uns dos outros, o que significa que o armazenamento de e-mails é mais rápido e escalável. Além disso, o tamanho da pasta maildir é mais fácil de gerenciar do que o tamanho de um arquivo mbox gigantesco.

2. Para que servem os esquemas de autenticação SASL/TLS?

SASL (Simple Authentication and Security Layer) e TLS (Transport Layer Security) são esquemas de autenticação que visam garantir a segurança das comunicações em redes.

O SASL é um protocolo que permite a autenticação de usuários em protocolos de rede como o SMTP (Simple Mail Transfer Protocol). Ele fornece uma camada de segurança adicional ao autenticar usuários antes de permitir que eles envie ou receba mensagens.

Já o TLS é um protocolo de camada de transporte que fornece criptografia e autenticação para comunicações na internet. Ele é amplamente utilizado para proteger as comunicações de e-mail, especialmente em servidores SMTP. O TLS criptografa todo o tráfego de rede entre dois pontos, garantindo que as informações transmitidas sejam protegidas contra interceptaç

3. O que é a diferença entre os formatos RFC822 e MIME types definido para e-mails?

RFC 822 é um padrão de formato de mensagem de correio eletrônico, publicado pela Internet Engineering Task Force (IETF) em 1982. Ele especifica o formato de uma mensagem de correio eletrônico, incluindo o cabeçalho e o corpo da mensagem. O formato é simples, com suporte para texto simples, endereços de remetente e destinatário, assunto, data e hora.

Já o MIME (Multipurpose Internet Mail Extensions) é uma extensão do formato de mensagem de correio eletrônico que permite o envio de tipos de conteúdo além de texto simples, como imagens, arquivos de som, vídeo e documentos. O MIME define tipos de conteúdo (conhecidos como "MIME types") que identificam o tipo de conteúdo em uma mensagem de correio eletrônico, como "text/plain" para texto simples ou "image/jpeg" para imagem JPEG.

Em resumo, o formato RFC 822 é uma especificação básica de formato de mensagem de correio eletrônico, enquanto o MIME é uma extensão que permite o envio de tipos de conteúdo mais avançados.

# WEB

1. O que são Server Side Includes (SSI)?

Server Side Includes (SSI) são uma tecnologia usada em servidores web para incluir dinamicamente conteúdo em uma página HTML. Com SSI, você pode incluir o conteúdo de um arquivo em uma página HTML antes de enviá-la ao navegador.

Ao usar SSI, você pode incluir arquivos comuns em várias páginas, o que significa que, se você precisar fazer uma alteração no conteúdo incluído, você só precisará modificar um arquivo, em vez de vários. Além disso, você pode usar SSI para exibir informações dinâmicas, como a data e hora atual, ou a contagem de visitas de uma página.

Para usar SSI, você precisa colocar código especial em sua página HTML, que informa ao servidor web para incluir o conteúdo de um arquivo específico. Normalmente, as extensões de arquivo SSI são .shtml, .stm ou .shtm. O servidor web precisa estar configurado para reconhecer e processar essas extensões de arquivo como SSI.

2. Quais são os mecanismos implementados por um servidor Web para conseguir atender tantas conexões simultaneamente?

1. Modelo de processamento: O Apache usa um modelo de processamento baseado em processos e threads para atender a várias solicitações ao mesmo tempo. Cada processo é responsável por lidar com várias solicitações, e cada thread é responsável por lidar com uma solicitação específica.
2. Pool de processos: O Apache mantém um pool de processos prontos para lidar com novas solicitações. Quando uma nova solicitação é recebida, ela é atribuída a um processo livre no pool.
3. Balanceamento de carga: O Apache pode usar vários métodos de balanceamento de carga, como Round Robin e Least Connections, para equilibrar a carga entre os processos e garantir que nenhum deles seja sobrecarregado.
4. Reaproveitamento de processos: O Apache tem uma opção de reaproveitamento de processos que permite que processos antigos sejam reutilizados para lidar com novas solicitações, em vez de criar novos processos. Isso é mais eficiente em termos de recursos do sistema.
5. Timeout de conexão: O Apache tem uma configuração de timeout de conexão que determina o tempo máximo que uma conexão pode ficar aberta sem atividade. Se a atividade for inativa por mais tempo do que o timeout de conexão, a conexão é fechada.

3. Explique qual é a utilidade e como funciona um proxy server no caso do protocolo HTTP.

Um servidor proxy é uma entidade que atua como intermediário entre um cliente (como um navegador web) e um servidor remoto. Quando um cliente envia uma solicitação a um servidor, ele a envia primeiro ao servidor proxy. O servidor proxy, em seguida, faz a solicitação em nome do cliente e retorna a resposta ao cliente.

4. Qual é a relação entre o protocolo MIME e o serviço WEB?

O protocolo MIME (Multipurpose Internet Mail Extensions) é um padrão usado para especificar a formatação de dados ao serem transmitidos por meio da Internet, incluindo serviços web. Ele é usado para especificar o tipo de conteúdo que está sendo transmitido (por exemplo, texto, imagem, vídeo, etc.), bem como o seu formato (por exemplo, HTML, JPEG, PNG, etc.).

O serviço web utiliza o protocolo HTTP (Hypertext Transfer Protocol) para enviar e receber dados da Internet, e o protocolo MIME é usado para especificar o formato dos dados que são transmitidos. Por exemplo, quando um navegador solicita uma página web, o servidor envia uma resposta HTTP que inclui um cabeçalho MIME, que especifica o tipo de conteúdo que está sendo enviado (por exemplo, text/html para HTML).

Em resumo, o protocolo MIME é um dos padrões importantes que estão por trás do funcionamento do serviço web, permitindo que os dados sejam transmitidos de forma eficiente e corretamente interpretados pelos clientes.