Conteúdos

0. Introdução a Fundamentos de Redes (10 horas)

Antes de explorarmos os serviços de rede, é fundamental entender a base: os endereços IP e a comunicação na rede.

- **Endereços IP e Máscaras de Rede** (4 horas)
  Explicação dos endereços IPv4 (Classes A, B, C) e IPv6, e como as máscaras de rede definem a sub-rede.

```
# Exemplo de IP e máscara
Endereço IP: 192.168.1.50
Máscara de Rede: 255.255.255.0  (ou /24)
```

- **Ferramentas de Diagnóstico de Rede** (3 horas)
  Apresentar ferramentas essenciais para testar a conectividade.

```
ping google.com          # Testar a conectividade com um host
traceroute google.com    # Seguir o caminho até um destino
ifconfig / ip addr       # Ver os detalhes das interfaces de rede
```

- **Exercício de Consolidação** (3 horas)
  1. Abra o terminal e use ‘ifconfig‘ ou ‘ip addr‘ para encontrar o endereço IP da sua máquina. 2. Use o comando ‘ping‘ para testar a conectividade com o router da rede (geralmente 192.168.1.1 ou 10.0.0.1). 3. Use o ‘traceroute‘ para seguir o caminho até um site conhecido e explique o que vê em cada "salto".

—

1. Serviços de rede (15 horas)

Nesta secção, vamos explorar como os serviços de rede são geridos no Linux, desde o seu início até ao encerramento, e os principais ficheiros e diretórios envolvidos neste processo.

- **O Gestor de Tarefas: O Papel do `systemd`** (3 horas)
  Pense no `systemd` como o "gerente de todas as tarefas"do seu computador. Ele garante que tudo comece a funcionar na ordem certa quando o sistema é ligado.
- **Controlar Serviços com `systemctl`** (5 horas)
  O comando `systemctl` é como a "lista de comandos"para o gestor de tarefas.

```
# Ver o estado de um serviço (Exemplo: SSH)
systemctl status sshd

# Ligar, desligar e reiniciar um serviço
systemctl start sshd
systemctl stop sshd
systemctl restart sshd
```

- **Tarefas Programadas e Serviços On-Demand** (5 horas)
  Aprofundar o uso do `systemd` para além da gestão básica de serviços.
  - **Systemd Timers**: Uma alternativa moderna ao ‘cron‘ para agendar tarefas.
  - **Systemd Sockets**: Iniciar serviços "on-demand"apenas quando há tráfego numa porta específica.
- **Exercício de Consolidação** (2 horas) 1. Crie uma unidade de serviço (‘.service‘) e uma unidade de temporizador (‘.timer‘) para um script simples que escreve a data e hora num ficheiro a cada minuto. 2. Verifique o estado do temporizador e do serviço com `systemctl list-timers`.

—

Figura 1: Exemplo da saída do comando `systemctl status sshd`. *Fonte: Imagem encontrada via Google Images.*

2. XINET.d (5 horas)

O `xinetd` é como um "rececionista"que só acorda um funcionário (serviço) quando alguém aparece para o ver.

- **Configuração e Gestão** (3 horas)
  As configurações do `xinetd` estão nos ficheiros do diretório `/etc/xinet.d/`. Cada serviço tem o seu próprio "cartão de identificação"com opções como `server`, `port` e `disable`.

- **Exercício de Consolidação** (2 horas)
  1. Encontre o ficheiro de configuração do serviço `ftp` no diretório `/etc/xinet.d/`. 2. Altere o valor da opção `disable` para habilitá-lo. 3. Crie uma nova configuração para um serviço simples, como um servidor de eco, e verifique o seu funcionamento.

—

3. TCPWrappers (5 horas)

Pense nos `TCPWrappers` como um porteiro. Ele decide quem pode entrar (permitir) e quem não pode (negar) num serviço, com base no endereço IP.

- **As Duas Listas: ‘hosts.allow‘ e ‘hosts.deny‘** (2 horas)
  - `hosts.allow`: A "lista de convidados". Se alguém estiver aqui, entra. - `hosts.deny`: A "lista negra". Se alguém não estiver na lista de convidados e estiver aqui, é barrado.

- **Sintaxe e Exemplos Avançados** (2 horas)
  Pode usar ‘ALL‘ para todos e ‘EXCEPT‘ para criar exceções.

  ```
  # No ficheiro /etc/hosts.allow
  sshd: 192.168.1.100 EXCEPT 192.168.1.101
  ```

- **Exercício de Consolidação** (1 hora)
  1. Configure o seu ficheiro `hosts.deny` para negar o acesso SSH a todos. 2. No ficheiro `hosts.allow`, adicione o IP do seu computador para poder aceder.

—

4. NIS (10 horas)

O NIS é como ter uma única "identidade"para toda uma rede de computadores. Em vez de ter uma conta de utilizador em cada máquina, você tem uma conta num servidor central que funciona em todas as máquinas NIS.

- **Arquitetura NIS (Servidor Mestre e Cliente)** (3 horas)
  - **Servidor Mestre**: Tem a lista principal de utilizadores e grupos. - **Cliente NIS**: Pede ao servidor as informações de utilizadores. O ‘ypbind‘ é o serviço que o cliente usa para encontrar o servidor.

- **Configuração de um Servidor NIS Mestre** (5 horas)
  Passos detalhados para instalar o ‘ypserv‘ e configurar os mapas NIS (‘/etc/passwd‘, ‘/etc/group‘, etc.) e exportá-los para os clientes.

- **Exercício de Consolidação** (2 horas)
  1. Numa máquina cliente, use o comando `ypwhich` para ver qual é o servidor NIS. 2. Use `ypcat passwd` para listar as contas de utilizador. 3. Crie uma nova conta no servidor NIS e verifique se consegue iniciar sessão com essa conta a partir do computador cliente.

—

5. DHCP (15 horas)

O DHCP é um protocolo que automaticamente dá um "endereço de rua"(o endereço IP) a cada dispositivo que se liga à sua rede.

- **O Processo DORA: Como funciona?** (4 horas)
  Pense no processo DORA como uma conversa entre um novo dispositivo e o servidor DHCP:

  1. **D**iscover: "Olá, estou aqui! Há algum servidor DHCP disponível?"
  2. **O**ffer: "Sim, eu sou um servidor! Aqui está um endereço IP que pode usar."
  3. **R**equest: "OK, obrigado! Quero usar este endereço."
  4. **A**cknowledge: "Certo, é todo seu! Divirta-se na rede!"

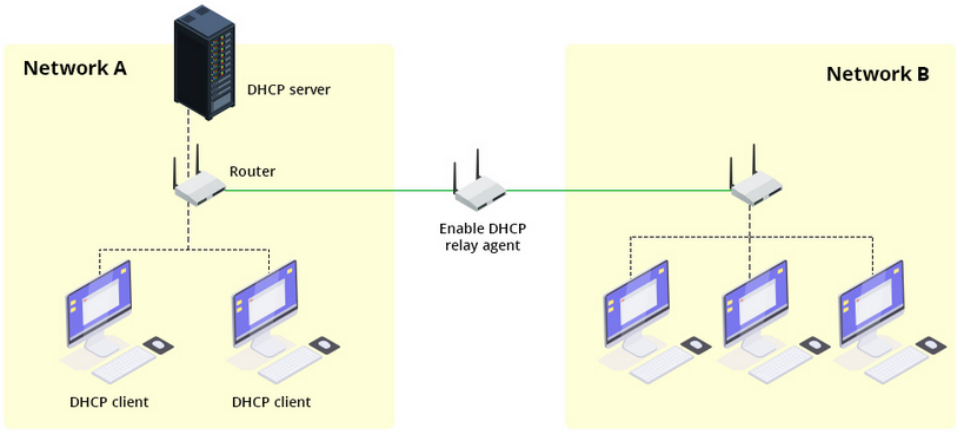

Figura 2: Diagrama do processo DORA. *Fonte: Imagem encontrada via Google Images.*

- **Configuração e Atribuição de Endereços** (7 horas)
  Aprofundar a configuração do servidor DHCP no ficheiro `dhcpd.conf`. - `subnet`: Define a rede que o servidor vai gerir. - `range`: A lista de IPs que serão atribuídos dinamicamente. - `option routers`: Define o endereço do router/gateway. - `host`: Para dar um IP fixo a um computador específico (com base no endereço MAC).

- **Conceitos Avançados: DHCP Relay Agent** (2 horas)
  Explicar como um **DHCP Relay Agent** pode ser usado para encaminhar pedidos de DHCP entre redes, eliminando a necessidade de ter um servidor DHCP em cada sub-rede.

- **Exercício de Consolidação** (2 horas)
  1. Configure um servidor DHCP para a sua rede de treino com um ‘range‘ de IPs dinâmicos. 2. Adicione uma entrada estática para o computador do instrutor. 3. Configure um cliente Linux para obter o IP do servidor e verifique se as configurações (IP, gateway, DNS) estão corretas.

—

6. DNS (20 horas)

O DNS é como a "lista telefónica"da internet. Ele traduz nomes fáceis de lembrar (como ‘google.com‘) em endereços IP que os computadores entendem.

- **Como a Lista Telefónica Funciona: A Hierarquia** (6 horas)
  A consulta de DNS é um processo de "perguntas e respostas"entre o cliente, o servidor DNS local e a hierarquia de servidores de raiz, TLD e autoritativos.

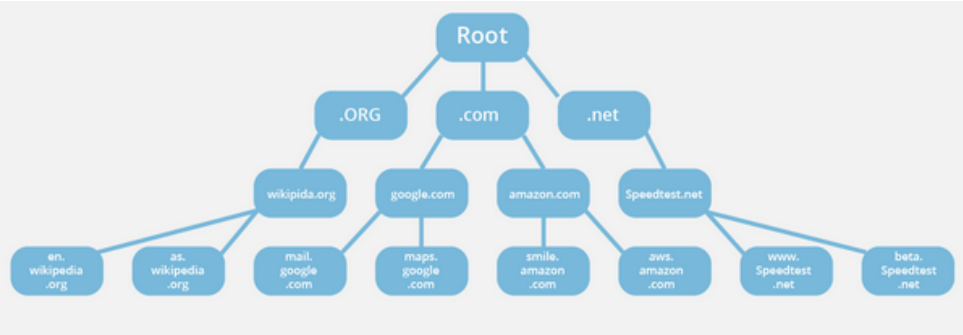

Figura 3: Fluxo de uma consulta DNS típica, mostrando a hierarquia de servidores. *Fonte: Imagem encontrada via Google Images.*

- **Tipos de Registos DNS (A, AAAA, CNAME, MX, PTR)** (4 horas)
  - `A`: Mapeia um nome de domínio para um endereço IPv4. - `CNAME`: Cria um "apelido"para outro nome de domínio. - `MX`: Especifica o servidor de correio para um domínio. - `PTR`: Usado para a pesquisa inversa, mapeando um IP para um nome de domínio.
- **Configuração de um Servidor DNS com BIND** (8 horas)
  Instalar o ‘BIND‘ (servidor DNS mais popular) e configurar um servidor DNS primário (autoritativo) para um domínio. - Configurar o ficheiro de zona de **‘forward lookup‘** para traduzir nomes para IPs. - Configurar o ficheiro de zona de **‘reverse lookup‘** para traduzir IPs para nomes.
- **Exercício de Consolidação** (2 horas)
  1. Crie um servidor DNS com o BIND e configure-o para ser autoritativo para um domínio fictício (‘meu-curso.com‘). 2. Adicione vários registos (A, CNAME) para máquinas na sua rede. 3. Configure uma máquina cliente para usar este novo servidor DNS e use o ‘dig‘ para testar se as consultas estão a funcionar.

—

7. LOGS (10 horas)

Os logs são como um "diário de bordo"do seu computador. Eles registam tudo o que acontece e são essenciais para encontrar erros e problemas.

- **Onde Encontrar o Diário** (2 horas)
  A maioria dos logs está em `/var/log`. Os ficheiros mais importantes são: - `syslog` ou `messages`: Mensagens gerais do sistema. - `auth.log`: Registos de login e autenticação.
- **Como Ler o Diário: Comandos Úteis** (3 horas)
  - `tail -f /var/log/syslog`: Mostra as últimas linhas do ficheiro e acompanha as novas linhas em tempo real. - `grep "erro"/var/log/syslog`: Procura por uma palavra-chave como "erro".
- **Gerir o Diário: Rotação de Logs (‘logrotate‘)** (3 horas)
  Explicar o conceito de rotação de logs para evitar que os ficheiros fiquem demasiado grandes, e como configurar o ‘logrotate‘.
- **Logging Centralizado** (2 horas)
  Introdução ao conceito de enviar logs de várias máquinas para um servidor central, o que facilita a gestão e a monitorização de redes maiores, usando ferramentas como o ‘syslog-ng‘ ou ‘rsyslog‘.