**DHCP**

1. O que é DHCP?

DHCP (Dynamic Host Configuration Protocol) é um protocolo criado para facilitar a configuração de endereços IP em uma rede, pois permite um endereçamento automático de IP para máquinas em uma rede TCP/IP.

1. Como funciona a atribuição automática de IP em uma rede que utiliza o DHCP?

Se a rede possuir um DHCP ativo é possível receber configuração de IP automaticamente ao ligar a máquina. Evitando assim configuração adicional após tê-la (IP) recebido.

1. Como funciona o protocolo DHCP?

O Protocolo DHCP funciona em quatro etapas principais:

* DHCP DISCOVER: O cliente DHCP envia um pacote broadcast (DHCP DISCOVER) para descobrir servidores DHCP na rede.
* DHCP OFFER: Servidores DHCP respondem com um DHCP OFFER, que inclui uma oferta de configuração para o cliente.
* DHCP REQUEST: O cliente solicita a configuração oferecida por um servidor específico através de um DHCP REQUEST.
* DHCP ACK: O servidor confirma a configuração com um DHCP ACK, reservando o endereço IP para o cliente.

Além disso, o cliente deve renovar periodicamente sua configuração, e não há garantia de que receberá a mesma configuração novamente.

1. O que é o protocolo HTTP?

O Protocolo HTTP é um protocolo da camada de aplicação que usa TCP para transporte. É “stateless”, ou seja, cada requisição é independente das outras. É usado principalmente para transferir documentos de hipertexto e seus recursos de servidores remotos.

1. Quais as características gerais do HTTP?

* Protocolo da camada de aplicação: O HTTP é um protocolo da camada de aplicação que é enviado sobre o protocolo TCP.
* Funciona baseado na troca de requisição resposta: O HTTP é um protocolo cliente-servidor, o que significa que as requisições são iniciadas pelo destinatário, geralmente um navegador da Web.
* Cabeçalho das mensagens é texto puro: O HTTP usa uma estrutura de mensagem simples2.
* Não orientado a conexões: O HTTP é stateless, o que significa que cada requisição é considerada como uma nova requisição3.
* Transferência bidirecional: O HTTP permite a transferência de um navegador para um servidor.
* Suporte para uso de cache: O HTTP permite que o navegador interrogue o servidor para determinar se o conteúdo da página foi alterado desde que a cópia foi para o cache.

1. O que é o comando GET?

É um método que solicita ao servidor um recurso (página HTML, figura GIF, documento do word etc.). A URI do recurso pode conter dados separados por ‘? ‘como por exemplo: /index.html?dado1=valor1&dado2=valor2

1. O que é o comando POST?

Comando Usado para enviar dados para o servidor (p.e., upload de arquivo, dados de formulário HTML). Ao contrário do GET, os dados seguem após a linha em branco que separa cabeçalhos dos dados.

1. O que é URI, URL e URN?

* URI = Identificador Uniforme de Recursos
* URL = Localizador Uniforme de Recursos
* URN = Nome Uniforme de Recurso

1. Como é o formato de um formulário HTTP?

Formato de um formulário HTTP: Os dados são agrupados em pares nome=valor e não pode haver nenhum espaço em branco nos dados.

Resposta HTTP: Toda resposta HTTP deve ter um cabeçalho content-type que indica o tipo MIME do recurso enviado2. O protocolo HTTP é multimídia2.

Códigos de status da resposta3:

* 1xx: Mensagem de informação
* 2xx: Sucesso no atendimento à requisição
* 3xx: Redirecionamento para outro servidor/recurso
* 4xx: Erro no atendimento ao cliente
* 5xx: Erro do servidor Web
* 200 – OK: Requisição bem-sucedida e a informação é entregue com a resposta
* 301 – Moved Permanently: Objeto requisitado foi removido permanentemente; novo URL é especificado no cabeçalho
* 400 – Bad Request: Código genérico de erro que indica que a requisição não pode ser entendida pelo servidor
* 404 – Not Found: O documento requisitado não existe no servidor
* 505 – HTTP Version Not Supported: A versão do protocolo HTTP requisitada não é suportada pelo servidor.

1. O que é protocolo HTTPS?

HTTPs é a combinação do protocolo HTTP com o SSL (Secure Sockets Layer). É a maneira mais comum atualmente de trafegar documentos via HTTP de maneira segura. Provê encriptação de dados, autenticação de servidor, integridade de mensagem e autenticação de cliente.

1. O que é o SSL?

O SSL (Secure Sockets Layer) é um protocolo de segurança que cria um canal criptografado entre um servidor web e um navegador para garantir que todos os dados transmitidos sejam seguros e privados. Ele é usado para proteger transações sensíveis, como transações de cartão de crédito, transferências de arquivos e logins. O SSL faz isso autenticando os dois dispositivos que estão se comunicando e assinando digitalmente os dados para fornecer integridade de dados.

1. Como funciona o SSL?

O SSL (Secure Sockets Layer) é um protocolo de segurança que protege a comunicação na internet. Ele funciona através de um “handshake” (aperto de mão) que envolve as seguintes etapas:

**Início do Handshake:** O cliente inicia um handshake SSL ao tentar se conectar a um site seguro.

**Troca de Certificados:** O servidor envia seu certificado SSL ao cliente.

**Verificação do Certificado:** O cliente verifica o certificado e cria uma chave de sessão criptografada.

**Estabelecimento da Conexão Segura:** O servidor descriptografa a chave de sessão e confirma a conexão.

1. O que é o protocolo DNS?

O DNS (Domain Name System) é o serviço necessário para todos os computadores que utilizam a Internet ele é o Serviço que permite a resolução dos nomes de um domínio.

tradução: nome -> IP

tradução: IP -> nome

1. Como é o funcionamento do protocolo DNS?

**Resolver e Name Server:** Existem duas entidades principais no DNS - o Resolver (cliente) que faz requisições de resolução de nomes/endereços, e o Name Server (servidor) que responde a essas requisições.

**Tradução de Nome para IP e Vice-versa:** Os servidores DNS são capazes de traduzir nomes para endereços IP e vice-versa.

**Servidores por Domínio:** É necessário ter no mínimo dois servidores por domínio - um servidor primário e um ou mais servidores secundários.

**Fully Qualified Domain Name (FQDN):** FQDNs são rótulos separados por pontos que indicam uma hierarquia. Por exemplo, em www.univas.edu.br, “univas” está dentro do domínio “edu”, que está dentro do domínio “br”, que está dentro do domínio root ".".

**Domínio Root:** O domínio root pode ser omitido no final do nome. Por exemplo, www.univas.edu.br. é o mesmo que www.univas.edu.br.

**Nomes como Chave:** Nomes são usados como “chave” na busca de dados no DNS.

Essas características tornam o DNS uma parte essencial da Internet, permitindo que os usuários acessem sites usando nomes de domínio em vez de endereços IP.

1. O que são servidores DNS?

**Servidores DNS:** Existem milhares de servidores de nomes espalhados pelo mundo.

Root Name Servers: São os servidores responsáveis pelo domínio da raiz. Eles respondem a requisições sobre servidores de nomes do primeiro nível da árvore. Se todos falharem, todas as resoluções na Internet irão falhar.

Servidores de Zona: São os servidores dos outros domínios.

Servidores Primários e Secundários: Para cada domínio Internet são necessários ao menos 2 servidores: um servidor primário que contém o “mapa” do domínio, e um ou mais servidores secundários que buscam do servidor primário os “mapas” do domínio.

Time-to-Live (TTL): Define o tempo de vida de uma entrada no cache de nomes.

1. O que é uma VPN?

É uma rede de acesso restrito, onde duas partes são conectadas utilizando uma rede pública e assim substituindo a tecnologia de links dedicados para conexão de redes remotas

1. Quais as características da VPN?

* Privacidade dos dados: se houver interceptação dos dados durante sua transmissão, não poderão ser decodificados
* Integridade dos dados: não poderão sofrer mudanças durante a transmissão
* Autenticidade: garantir que o dispositivo remoto o qual o túnel foi estabelecido é um dispositivo autorizado e não um equipamento qualquer.

1. O que é o VPT Túnel?

É o canal criado para a comunicação entre o ponto origem e o destino.

1. O que é o Tunelamento?

É o processo de encapsular um tipo de pacote dentro de outro para facilitar algum o transporte de uma informação dentro da rede.

1. Quais os tipos de conexões VPN?

* Host-to-Host
* Host-to-Gateway
* Gateway-to-Gateway

1. O que é VPN-SSL?

Atua entre a camada de Aplicação e acamada de Transporte do protocolo TCP.

1. O que é o SSL Handshake?

É o processo de autenticação do cliente e do servidor. Fornece os parâmetros para o funcionamento do SSL Record. É constituído de duas fases:

1ª escolha da chave, autenticação do servidor e a troca da chave mestra;

2 ª é feita autenticação do cliente

1. O que é o SSL Record?

É o processo que encapsula protocolos de nível superior, provê serviços de autenticação, encriptação, fragmentação e compressão de dados.

1. O que é VPN – OPENVPN?

O openvpn é um software livre, utilizado para criar redes privadas virtuais sobre redes públicas.

O openvpn permite conexões ponto-a-ponto através de chaves secretas compartilhadas.

Possui entidade servidora para Linux/Unix e cliente para Linux/Unix/Windows/Mac