**PROTOCOLOS DE REDE**

Definição:

\*São linguagens que a RCDE. usa para comunicação.

\*Define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou recebimento de uma mensagem ou outro evento.

\*Cada serviço possui um protocolo associado

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Modelo TCP/IP | | | | |
| PROTOCOLO TCP/IP Protocolo padrão da Internet e também é uma família de protocolos | | | | |
| Aplicação | | Tranasporte | Rede | Física |
| HTTP | Porta 80 | TCP | ARP | SLIP |
| HTTPS | Porta 443 | UDP | IP | CSLIP |
| FTP | Portas 20/21 | RTP | RARP | PPP |
| TFTP | Porta 69 | DCCP | ICMP | Ethernet |
| SMTP | Porta 25 |  | IGMP |  |
| DNS | Porta 53 |  |  |  |
| TELNET | Porta 23 |  |  |  |
| POP3 | Porta 110 |  |  |  |
| IMAP4 | Porta 143 |  |  |  |
| DHCP |  |  |  |  |
| NTP | Porta 123 |  |  |  |

**ENDEREÇAMENTO IP**

AS **CLASSES** DO **IPV4**

|  |  |  |
| --- | --- | --- |
| **Classes** | **Intervalo** | **Quantidade total de hosts** |
| **A** | 0 a 127 | 16777216 |
| **B** | 128 a 191 | 65536 |
| **C** | 192 a 223 | 256 |
| **D** | 224 a 239 | Multicast |
| **E** | 240 a 255 | Teste |

**MASCARA DE REDES** (divide o endereço IPv4 em Rede e Host)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Classe** | Qnt Redes | Qnt Hosts válidos | **Mascara padrão** | **CIDR** |
| **A** | 126 (2^7-2) | 16777214 (2^24-2) | **255.0.0.0** | **/8** |
| **B** | 16384 (2^14) | 65534 (2^16-2) | **255.255.0.0** | **/16** |
| **C** | 2097152 (2^21) | 254 (2^8-2) | **255.255.255.0** | **/24** |

**PROTOCOLO TCP**

|  |  |
| --- | --- |
| Paradigma cliente-servidor | |
| Caracteristicas | Problemas tratados |
| Orientado a Conexão | Comunicação não confiavel: mensagens perdidas, diplicadas, corrompidas, em atraso ou fora de ordem |
| Comunicação ponto a ponto |
| Confiabilidade completa | Reinicialização de um ponto envolvido: Caso um dos pontos seja reiniciado por algum problema, não deve haver confusão |
| Full-duplex |
| Interface de Fluxo stream | Máquinas heterogêneas: Um computador mais potente pode gerar uma inundação ou transbordar uma aplicação em um computador mais lento |
| Inicio de comunicação confiável |
| Funalização de conexão suave | Congestionamento na internet: A transmissão de dados mauito rápida pode causar o abarrotamento de pacotes em computadores e roteadores intermediarios |
|  |

**Mecanismos de controle de erros no Protocolo TCP**

|  |  |
| --- | --- |
| Checksum (Soma de verificação) | Usado para detectar erros de bits em um pacote transmitido. |
| Temporizador | Controla a retransmissão de um pacote caso este ou seu ACK (acknowledge) seja perdido |
| Número Sequencia | Permite a detecção de pacotes perdidos ou duplicados para tratar o reenvio ou descarta-los |
| Números de reconhecimento | Habilita o bit AKW para confirmar o recebimento de um pacote, fortalecendo a integridade |
| Verificação de Paridade | Verifica a quantidade de bits 1, indicando se uma mensagem está correta em relação a sua paridade |

**AUTENTICAÇÃO E SEGURANÇA**

|  |  |
| --- | --- |
| **Autenticação por usuário** | **Autenticação por menságem** Processo em que as partes que se comunicam verificam se o conteúdo de uma mensagem recebida não foi alterado e se a origem é quem deveria ser, isto é, autêntica. |
| Algo que ele sabe: PIN, resposta secreta |
| Algo que ele possui: Chaves criptograficas, cartão de senha eletrônica, chave física, token, smart cards | **Mecaniasmos de defesa contra ataques** Senhas Fortes; Autenticação de dois fatores; Acesso a sites e download confiaveis; Restrição de acesso e firewall; Cuidado extra no preenchimento de formulários, envio de dados sensíveis e permissões de acesso |
| Algo que ele é: Biometria estatica, digital, retina, face |
| Algo que ele faz: Biometria dinâmica, padrão de voz, escrita manual, ritmo de digitação |

**PILARES DA SEGURANÇA DA INFORMAÇÃO**

* **Diponibilidade:** Manter um recurso sempre disponível para acesso
* **Integridade:** Garantir que os dados armazenados ou transmitidos permaneçam integros
* **Confidencialidade:** Garantir que os dados enviados não serão vistos por ninguém.

**Network Time Protocol NTP**

\*Utiliza o UTC – coordinated universal time.

\*Servidores garantem a sincronização da hora correta dos relógios dos dispositivos em rede.

**Importância:**

* Correto funcionamento de sistemas de redes
* Apoia processos de detecção e tratamento de incidentes de segurança
* Essencial para documentação em investigações de crimes digitais com a preservação das evidências

**Arquitetura:**

Topologia hierarquica em formato de cascata.

Dividida em camadas ou estratos, do 0 ao 16  
 estrato 0 – é o estrato raiz é o mais exato em tempo e não faz parte dos servidores NTP, é um receptor de GPS ou Relógio Atômico

estrato 16 – representa um servidor inoperante

Os demais estratos são uma cascata de requisição da hora, quanto mais perto do estrato 0, maior a precisão

**Relação de Associação:**

Permanentes: Criadas por um configuração ou comando e sempre mantidas

Priorizáveis: Pode ser desfeita depois de um tempo ou pela troca por um servidor melhor

Efêmeras ou Transitória: Criada pela solicitação de outro dispositivo NTP, pode ser desfeita depois de um tempo ou erro

**Network Time Protocol NTP**

**Possibilidades de Associação:**

Cliente-Servidor: (Confiabilidade, precisão e segurança) é a forma permanente mais comum, um dispositivo é o cliente e envia um pacote a outro dispositivo que é o servidor e aguarda a resposta ( *pull* )

Modo simétrico: (Confiabilidade, precisão e redundância) trabalha com redundência com um ou mais dispositivos NTP ( *peers* ) no mesmo estrato.  
 Ativo: Associação permantente entre um par de disitivos A e B, ambos configurando o outro como seu par.  
 Passivo: Um dos dispositivos atua como ativo e o outro cria uma associação transitória com o primeiro, mesmo sem te-lo em sua lista de pares.

Modo de operação, Broadcast ou Multicast: Utilizado para poucos servidores e muito clientes

**Segurança:**

A integridade e disponibilidade são garantidas com a configuração correta do sistema e número suficiente de fontes de tempo com referências primarias independentes.

A autenticidade é garantida por algoritmos de criptografia com metodos de chave simétrica ou pública

A confidencialidade não pe considerada pois o tempo é um informação pública

**Domain Name System DNS**

\*É um banco de dados distribuido, com tabelas de nomes de dominio e seu respectivo endereço IP. Atua no paradigma Cliente-Servidor.

|  |  |  |
| --- | --- | --- |
| **Classes Hierarquicas** de servidores DNS | | |
| **Raiz** | **Top Domain Level** | **Autoritativos** |
| São 13 desles no mais alto nível | gTDL: .com .org .net .info | O DNS autoritativo tem a autoridade final sobre o domínio, além de ser o responsável pela disponibilização de respostas para os servidores DNS recursivos com informações de endereço IP |

|  |  |  |  |
| --- | --- | --- | --- |
| **Classes Hierarquicas de servidores DNS** | | | |
| **Raiz** | **Top Domain Level** | **Autoritativos** | **Recursivos** |
| São 13 desles no mais alto nível | gTDL: .com .org .net .info | O DNS autoritativo tem a autoridade final sobre o domínio, além de ser o responsável pela disponibilização de respostas para os servidores DNS recursivos com informações de endereço IP | Um serviço DNS recursivo age como o concierge de um hotel: embora não tenha nenhum registro DNS, ele atua como um intermediário que pode obter informações de DNS por você. |
| São os pilares da internet mundial | sTDL: .aero .asia .edu .gov .mil |
|  | ccTDL: .br .uk .pt. .us .in |

**PROTOCOLO HTTP/HTTPS**

\*Hyper Text Transfer Protocol  
\*Hyper Text Transfer Protocol / Secure Socket Layer (SSL)  
\*Utilizado na comunicação entre navegadores e servidores web

|  |  |
| --- | --- |
| Alguns metodos HTTP | |
| GET | Faz a solicitação de um arquivo ou script através do protocolo HTTP. Sendo o método mais comum, é conhecido por todos servidores. |
| HEAD | Faz o mesmo que o GET, no entanto, sem retorno de recurso. Útil para receber metainformações sem que seja necessário obter todo o conteúdo. |
| POST | Utilizado para enviar dados que precisam ser processados, como, por exemplo, dados de um formulário HTML. |
| PUT | Utilizado para atualizar determinado recurso. |
| DELETE | Utilizado para excluir determinado recurso. |
| TRACE | Ecoa a requisição por todo o caminho até chegar ao recurso de destino. É útil para realizar teste de loopback e para debug. |
| OPTIONS | Utilizado pelos clientes para descobrir quais são as opções de requisição permitidas para determinado recurso em um determinado servidor. |
| CONNECT | Utilizado para iniciar uma comunicação bidirecional com o recurso desejado. É útil para abrir um túnel. |
| LINK | Conecta dois recursos existentes. |
| UNLINK | Encerra uma conexão existente entre dois recursos. |

**PROTOCOLO HTTP/HTTPS**

|  |  |  |  |
| --- | --- | --- | --- |
| Códigos de Resposta padrão HTTP | | | |
| 2xx | Success | 200 | OK |
| 201 | Created |
| 202 | Accepted |
| 204 | No Content |
| 3xx | Redirect | 301 | Moved Permanently |
| 302 | Moved Temporarily |
| 304 | Not Modified |
| 4xx | Client **Error** | 400 | Bad Request |
| 401 | Unauthorized |
| 403 | Forbidden |
| 404 | Not Found |
| 5xx | Server **Error** | 500 | Internal Server Error |
| 501 | Not Implemented |
| 502 | Bad Gateway |
| 503 | Service Unavailable |

**File Transfer Protocol FTP**

\*Utilizado para transferir arquivos na internet entre computadores ou dispositivos

\* É chamado automaticamente pelo navegador quando o usuário

solicita uma transferência de arquivo.

\*Proporciona o controle da transferência e segurança do arquivo

\*TFTP trivial – é uma forma simples do FTP que usa UDP sem segurança nem controle para aquivos pequenos e configurações de equipamentos eletrônicos

**File Transfer Protocol FTP**

|  |  |
| --- | --- |
| Aspectos possibilitados pelo FTP | |
| Conteúdos arbitrários de arquivo | É possível transferir qualquer tipo de dados, tais como documentos, imagens, músicas ou vídeos. |
| Transferência bidirecional | Utilizada para baixar arquivos através da transferência do servidor para o cliente ou carregar (upload) arquivos, por meio da transferência do cliente para o servidor. |
| Suporte para autenticação e propriedade | Cada arquivo pode ser proprietário de alguém com direito à restrição de acesso. |
| Habilidade para navegar em pastas | O cliente pode navegar entre os conteúdos de um diretório. |
| Mensagens de controle textual | As mensagens de controle trocadas entre um cliente e um servidor FTP são enviadas como texto ASCII. |
| Acomodação de heterogeneidade | Detalhes dos sistemas operacionais dos computadores individuais são escondidos e é possível transferir uma cópia de um arquivo entre dois computadores quaisquer. |

\*Componentes do cliente:  
 interface com usuario  
 processo de controle cliente  
 processo transferencia de dados cliente

\*Componentes do servidor:  
 Processo de controle servidor  
 processo de trnsferencia de dados servidor

**A separação das conexões é responsável pela eficiência do funcionamento do protocolo FTP**

**File Transfer Protocol FTP**

|  |  |
| --- | --- |
| **Conexão de Controle** | **Conexão de Dados** |
| **porta 21** | **porta 20** |
| permanece aberta durante toda a interação | conexão de dados é aberta e fechada a cada atividade de transferência de arquivos |
| Depois de criar uma conexão de controle o cliente deve se conectar ao servidor com um login e senha | A conexão de dados é mais complexa por tratar das transferencias de arquivos com diversas variações de composição |
| um login anonimo com senha de convidade pe usado para arquivos públicos | FTP inverte o relacionamento cliente-servidor no momento da conexão de dados. Quando abre uma conexão de dados, o cliente age como se fosse um servidor (espera pela conexão de dados), enquanto o servidor age como se fosse um cliente (inicia a conexão de dados). Depois que a conexão foi utilizada para uma transferência, ela é fechada. |
| O servidor envia um status numério atravez da conexão de controle como resposta para cada pedido, para que o cliente saiba se o pedido era valido |
| A conexão de controle trabalha com regras de comunicação simples sendo uma linha de comando ou resposta transferida de cada vez |

\*Para cada comando exite uma resposta numerica do servidor para o cliente pela conexão de controle

**File Transfer Protocol FTP**

|  |  |
| --- | --- |
| **Principais comandos FTP** | |
| **USER** | username - identificação do usuario para o servidor |
| **PASS** | password - senha do usuario para o servidor |
| **LIST** | lista com todos arquivos existentes no diretorio atual remoto |
| **RETR** | filename -obter um arquivo do diretorio atual do host remoto |
| **STOR** | filename - inserir um arquivo no diretorio atual do host remoto |
| **STRU** | define a organização dos dados (F para arquivo, R para registro, P para página) |
| **PORT** | identificador de porta, o cliente escolhe uma porta |
| **TYPE** | tipo padrão do arquivo (A para ASCII, E para EBCDIC e I para imagem) |
| **QUIT** | sai do sistema |

|  |  |
| --- | --- |
| **Resposta do servidor, conesão de controle** | |
| **331** | Nome de usuário OK, senha requisitada |
| **125** | Conexão de dados já aberta, iniciando transferência |
| **425** | Não é possível abrir a conexão de dados |
| **452** | Erro ao escrever o arquivo |
| **226** | Fechando conexão de dados |
| **221** | Serviço fechando |
| **220** | Serviço pronto |
| **200** | Comando OK |
| **250** | Solicitação de ação em arquivo OK |

**CORREIO ELETRÔNICO**

\*Paradigma cliente-servidor  
\*Envio e resposta de mão única

|  |  |  |
| --- | --- | --- |
| **Tipos de normas amplas de protocolos** | | |
| Transferência | Acesso | Representação |
| um protocolo utilizado para mover a copia de uma msg de um pc para o outro | um protocolo que permite ao usuario ter acesso a sua caixa de correio eletronico para ler ou enviar mensagens | um protocolo que especifica o formato da mensagem quando armazenada no disco |

|  |  |
| --- | --- |
| **Um software de de e-mail pode ser dividido em duas partes** | |
| uma aplicação de interface de mensagem | uma aplicação de trnasferencia de mensagem |

**Simple Mail Transfer Protocol SMTP**

Caracteristicas:

• Segue o paradigma stream

• Usa mensagem de controle textual

• Transfere somente mensagem de texto

• Permite a um remetente especificar os nomes dos destinatários e checar cada um deles

• Envia uma cópia de uma dada mensagem

Portas:

587 – transmissão segura via TLS  
2525 – quando a 587 está bloqueada

465 – Entrando em desuso

25 – Antiga usa para relay SMTP

**Simple Mail Transfer Protocol SMTP**

Processos de transferência de arquivos:

1. Estabelecimento de conexão
2. Transferência de menságens
3. Encerramento de conexão7

Respostas SMTP:



**Simple Mail Transfer Protocol SMTP**

Comandos SMTP:



**IMAP4** é mais completo e complexo  
\*um usuário pode verificar o cabeçalho do e-mail antes de recuperá-lo do servidor;

\*permite que o usuário procure por uma sequência específica de caracteres no conteúdo dos e-mails antes de recuperá-los;

\*possibilita a obtenção do e-mail de forma parcial, quando a largura de banda é limitada e o e-mail inclui conteúdo multimidia que exija um elevado consumo da capacidade de sua internet;

\*possibilita a criação, remoção e renomeação nas caixas de correio no servidor;

\*um usuário pode criar uma hierarquia e organização de caixas de correio em uma pasta para armazenamento de e-mails.

**CORREIO ELETRÔNICO**

**POP3** é simples, sendo um software cliente instalado no compoutador do destinatario e um servidor no servidor de e-mail Em configuração padrão, realiza-se a leitura das mensagens disponíveis e logo depois há a remoção do servidor dessa mensagem. Não é possivel organizar os emails no servidor nem verificar parcialment o conteudo

**MIME multipurpose internet extensions**

É possivel enviar dados que não seja apenas ASCII, transforma os dados não ASCII do lado do remetente em dados NVT ASCIIe entrega ao cliente que reconverte os dados.

**Dynamic Host Configuration Protocol DHCP**

Seu antecessor foi o BOOTP - bootstrap protocol onde o administrador da rede deveria configurar o servidor BOOTP para conhecer o IP d computador

Permite a obtenção de um ip de forma automática, sem necessidade de configuação manual do servidor, pode ser conhecido como plug and play networking

O dhcp trata de configuração para que um dispositivo esteja conectado em uma rede TCP-IP

O dipositivo precisa estar configurado com pelo menos 4 parametros de rede  
 Endereço IP  
 Mascara de rede  
 Endereço do primeiro roteador da rede(gateway default)  
 Endereço do DNS

O Administrador da rede pode configurar o DHCP para que um host tenha sempre o memo IP ou que obtenha um endereço diferente sempre que se conectar

**Dynamic Host Configuration Protocol DHCP**

Cada atribuição de endereço ip é limitada a tempo fixo definido pelo administrador de rede, a isto se da o nome de lease ou locação. Isso possibilita a recuperação de endereços já atribuidos, o host pode abandonar ou renegociar a extenção de tempo com o DHCP

Paradigma cliente-servidor

Cada sub-rede pode ter um servidorDHCP ou ele pode não existir, assim o agente DHCP (roteador) sabe o endereço de um servidor DHCP para essa sub-rede

|  |  |
| --- | --- |
| **Etapas do funcionamento do processo DHCP** | |
| DHCP discover | o cliente envia uma mensagem de descoberta em modo broadcast 255.255.255.255 e um endereço de IP destinatário 0.0.0.0 dentro de um pacote UDP envolvido em um datagrama IP para a porta 67. essa transmissão vai para a camada de enlace que transmite para todos os nós da sub-rede |
| DHCP offer | um servidor DHCP recebe a mensagem do cliente e responde com uma oferta também em broadcast. Cada oferta contem o ID da mensagem de descoberta, o IP proposto para o cliente, a mascara de rede e o tempo de lease |
| DHCP request | a resposta de solicitação do cliente deve repetir os parametros de configuração |
| DHCP ack | O servidor responde de volta com uma mensagem de confirmação dos parametros solicitados |

**Dynamic Host Configuration Protocol DHCP**

|  |  |
| --- | --- |
| **Mensagens para conexão de rede** | |
| DHCPDISCOVER | broadcast enviado pelo cliente para encontrar o servidor |
| DHCPOFFER | mensagem enviada pelo servidor oferecendo seus serviços para o cliente |
| DHCPREQUEST | mensagem enviada pelo cliente para o servidor, solicitando, confirmando ou renovando um empréstimo dos parâmetros |
| DHCPACK | mensagem do servidor com as configurações DHCP |
| DHCPRELEASE | mensagem do cliente liberando os parâmetros emprestados |
| DHCPINFORM | mensagem do cliente requisitando informações de configuração de rede |

O agente relay fica configurado com o endereço do servidor DHCP caso este não esteja na rede e é encarregado de encaminhar as mensagens entre cliente e servidor DHCP

Administradores de rede preferente um servidor DHCP e vários agentes relay, centralizando a administração em um único dispositivo

lém dos 4 parametros citados, outros elementos podem ser distribuidos atravéz do DHCP

Endereço do servidor de logs

Servidor NTP

Servidor proxy

**Servidor PROXY ( procuração ou pro curador )**

Opera na camada de aplicaão do TCP-IP. é um software de SO assim como HTTP e DNS

Elemento de filtragem de conteudo para praticas de segurança

Proxy-cache armazenador temporário de arquivos de acesso a páginas web

Pode-se administrar a autenticação de usuarios, registros de acesso a rede e relatórios gerenciais sobre a utilização da rede de internet pelos usuários

O firewall nesse contexto possibilita controlar o acesso externo a rede interna

Proxy transparente definido pelo RCF 3040 possibilita impor regras para utilização da rede

Proxy reverso - é util para dividir tarefas entre servidores, sendo o reverso responsável por tarefas simples, além de fornecer segurança a tentativas de invasão aos servidores da intranet

**PROXY HTTP**

Tipo mais comum de proxy conhecido como proxy web

Fornece um cache de objetos para todos os dispositivos da rede minimizando o trafego

Repassa a URL solicitada pelo cliente, se conecta com o servidor web e faz a requisição do objeto, depois de recebido repassa o objeto para o navegador

Existem algoritmos responsáveis pela remoção de arquivos de acordo com o tempo que foram acessados:

Algoritmo **LRU least recently used** extrai os arquivos que estão amais temp sem serem usados

Algoritmo **LFU least frequently used** extrai os domunets que são usados com menos frequencia