

EAD
UNISANTA

REDES DE COMPUTADORES

Me. Claudio Souza Nunes

GUIA DA
DISCIPLINA
2022

Objetivo Geral

A disciplina de Redes de Computadores tem como objetivo geral capacitar o aluno para entender conceitualmente os protocolos usados em redes de computadores, tanto no âmbito de redes locais como na sua utilização na Internet. Ao final da disciplina o aluno deverá ter um conhecimento da estrutura e cenários de utilização dos principais protocolos de rede.

1. CONCEITOS BÁSICOS DE REDE - MODELO ISO/OSI

1.1. Redes de Computadores

O ser humano como espécie possui uma natureza gregária. Faz parte da nossa essência a necessidade de viver em grupos e partilhar nossas experiências. As redes de computadores que usamos diariamente são uma manifestação natural desta nossa necessidade social.

1.1.1. Modelos básicos de rede em relação a sua abrangência

Quando tentamos entender as redes usando uma combinação de abrangência e utilização típica podemos classificá-las da seguinte forma:

LAN	WAN	PAN
Abrange menores distâncias	Abrange maiores distâncias. Podem ser utilizadas para interconectar redes locais	Abrange distâncias muito curtas (geralmente 10m)
Links de comunicação mais rápidos	Links de comunicação mais lentos	Links de comunicação mais lentos (geralmente)
Voltada para compartilhamento de Recursos	Voltada para compartilhamento de Informações	Voltada para interligação de periféricos de uso pessoal
Peer ou servidores dedicados	Peer	Peer
Informações centralizadas	Informações distribuídas	Informações compartilhadas

1.1.2. Modelo ISO x OSI

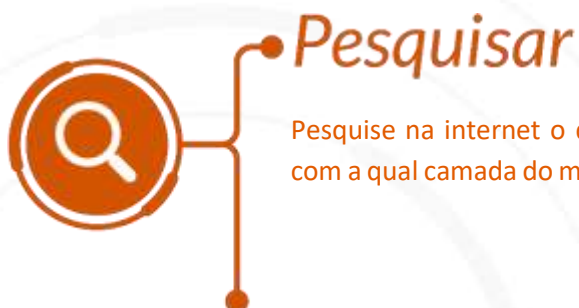
Conceitos complexos, como a forma como uma rede opera, podem ser difíceis de explicar e compreender. Em função desta complexidade é comum o uso de modelos de referência “em camadas” que nos ajudam a entender como as redes são estruturadas e como as operações são realizadas. Um dos modelos mais comuns para realizar esta função é o modelo OSI (Open System Interconnection) concebido pela ISO (International Organization for Standardization). Este modelo, popularmente conhecido como ISO x OSI possui as sete camadas como descrito abaixo:

Modelo OSI	Descrição
	A camada de aplicação contém protocolos usados para processo a processo comunicações.
	A camada de apresentação fornece uma representação comum dos dados transferidos entre serviços de camada de aplicativo.

Modelo OSI	Descrição
7 - Aplicação	A camada de sessão fornece serviços para a camada de apresentação para organizar seu diálogo e gerenciar o intercâmbio de dados.
6 - Apresentação	A camada de transporte define serviços para segmentar, transferir e remontar os dados para comunicações individuais entre o fim dispositivos.
5 - Sessão	A camada de rede fornece serviços para trocar as partes individuais de dados através da rede entre dispositivos finais identificados.
4 - Transporte	Os protocolos da camada de enlace descrevem métodos para troca de dados quadros entre dispositivos em uma mídia comum
3 - Rede	Os protocolos da camada física descrevem o mecânico, elétrico, meios funcionais e processuais para ativar, manter e desativar conexões físicas para uma transmissão de bits de e para uma rede dispositivo.
2 - Enlace	
1 - Física	

1.1.3. Topologia de Rede

A forma como é feita a interconexão entre os dispositivos de uma rede é conhecida como topologia da rede. Algumas das topologias mais comuns são Anel, Estrela e Barramento.



Pesquise na internet o que são equipamentos LAYER 3 e procure relacionar com a qual camada do modelo ISO X OSI estes equipamentos estão associados.



Entendendo

Para aprofundar o seu entendimento sobre o modelo ISO X OSI assista o vídeo disponível em <https://www.youtube.com/watch?v=iybbkP1c0kc>



Importante

No modelo ISO X OSI cada camada se comunica com a equivalente no dispositivo remoto e com as adjacentes no mesmo dispositivo. Exemplo: A camada de Rede presta serviços para a camada de transporte e usa serviços da camada de enlace. Em relação ao outro dispositivo a camada de rede “vê” apenas a camada de rede.

2. PROTOCOLOS DA CAMADA DE ENLACE E EQUIPAMENTOS DE REDE

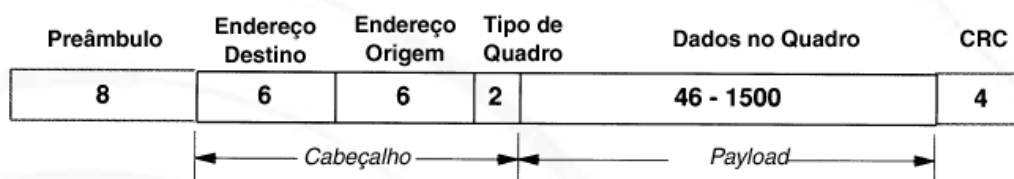
2.1. Camada de Enlace

A camada de enlace de dados do modelo OSI (Camada 2) prepara os dados da rede para a rede física. A camada de enlace de dados é responsável pela placa de interface de rede (NIC) para comunicações de placa de interface de rede. A camada de enlace de dados faz o seguinte:

- Permite que as camadas superiores acessem a mídia. O protocolo de camada superior não está completamente ciente do tipo de mídia que é usado para encaminhar os dados.
- Aceita dados, geralmente pacotes de Camada 3 (ou seja, IPv4 ou IPv6), e os encapsula em quadros da Camada 2.
- Controla como os dados são colocados e recebidos na mídia.
- Troca quadros entre pontos de extremidade através da mídia de rede.
- Recebe dados encapsulados, geralmente pacotes de Camada 3, e os direciona para o protocolo de camada superior apropriado.
- Executa a detecção de erros e rejeita qualquer quadro corrompido

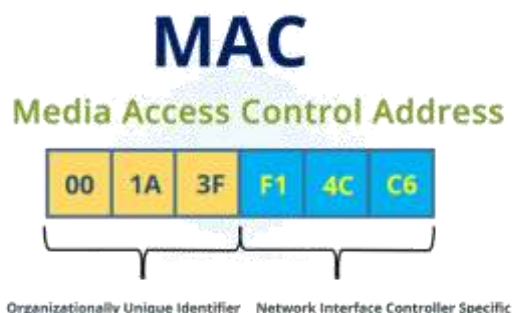
2.2. Formato de quadro camada de Enlace

Os quadros na camada de enlace seguem o padrão Ethernet que sofreu algumas variações ao longo do tempo, mas que na sua forma original tinha a seguinte composição:



2.3. Endereços da camada de Enlace (MAC Address)

Cada dispositivo de rede possui uma identificação de 6 bytes que é garantida ser única e permite ao dispositivo receber os dados que a ele são encaminhados. Para garantir esta unicidade o endereço MAC é composto de duas partes: uma correspondente ao fabricante e outro gerada pelo fabricante sem duplicidade.



2.4. Equipamentos de rede

Para a interconexão entre os dispositivos de rede são necessários vários tipos de equipamentos.

Equipamento	Função
Repetidores	São usadas para estender o tamanho físico da rede (distância entre os nós). Pertencem a camada física
Hubs	Equipamento atualmente considerado legado. Trata-se de um repetidor multiportas
Ponte (Bridge)	Permite dividir o tráfego da rede em dois grupos a partir da análise dos endereços MAC
Switches	Uma combinação de Hub + Bridge. Possuem várias portas e são capazes de fazer o encaminhamento dos pacotes diretamente para as portas que contêm o endereço MAC de destino.
Roteadores	Equipamentos para interconexão entre redes. Operam na camada de rede.

2.4.1. Como os switches funcionam?

Switches são equipamentos que podem otimizar a comunicação dentro de uma rede local encaminhando pacotes diretamente e somente para as portas participantes da

comunicação. Isso é possível porque cada switch mantém uma memória associando endereços MAC com suas portas. Switches possuem vários modos de operação:

MODO	AÇÃO
FLOODING	O pacote é encaminhado para todas as portas do switch.
FORWARDING	O pacote é encaminhado apenas para porta de destino.
BLOCKING	O pacote não é encaminhado para nenhuma porta.
AGING	Os endereços armazenados na tabela interna de encaminhamento são apagados após algum tempo sem envio de novos pacotes.

2.4.2. Tipo de switches

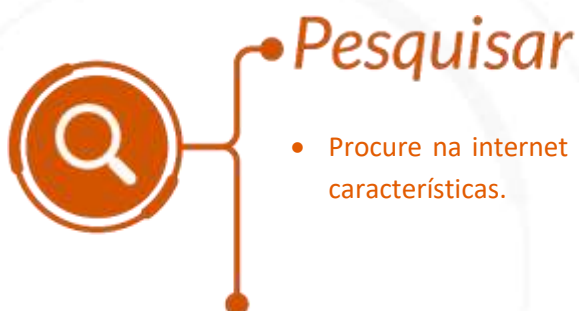
Switches podem ser classificados em função da sua estratégia para encaminhamento de pacotes ou camada do modelo ISO /OSI em que atuam.

Por estratégia:

- **store-and-forward**
Lê todo o pacote, armazena em buffer, testa integridade e envia se OK
- **cut-through**
Verifica apenas o endereço de destino e envia (sem verificação)

Por camada:

- **de camada 2**
Semelhante à uma bridge, usam os endereços MAC da camada 2
- **de camada 3:**
Semelhante à um roteador: observa as estruturas dos pacotes, e enviam por rotas baseadas nos endereços da camada 3: dependem de protocolo de rede



- Procure na internet os preços de switches de 24 portas e compare suas características.



Entendendo

Acesse o site macvendors.com e tente identificar qual o fabricante associado a um dos seus dispositivos de rede (computador, smartphone, etc.)



Saiba mais

Veja o vídeo disponível em <https://youtu.be/RMCYER3Q7Aw> para entender um pouco mais sobre o funcionamento de um switch.



Importante

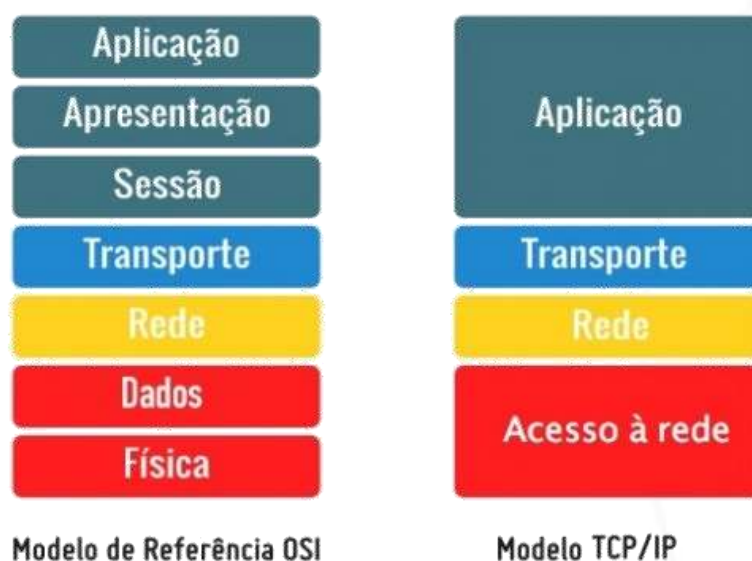
É comum que equipamentos de uso doméstico integrem as funções de switch e roteador. Desta forma um único equipamento pode gerenciar a comunicação com a rede local e a conexão com a internet.

3. PROTOCOLOS CAMADA DE REDE

3.1. Modelo ISO/OSI e modelo TCP/IP

Embora o modelo de referência ISO/OSI possa ser usado para entender o funcionamento de qualquer estrutura de rede, no caso específico da Internet é comum usar o modelo TCP/IP. É importante entender que a camada de rede fornece serviços que permitem que os dispositivos finais troquem dados entre redes.

3.2. Comparação entre as camadas do modelo ISO/OSI e modelo TCP/IP



3.3. Principais características do protocolo IP

O protocolo IP possui as seguintes características:

- É a abreviatura para INTERNET Protocol
- Endereçamento lógico
- Camada de rede do modelo ISO x OSI
- Importância acentuada por conta da onipresença da INTERNET
- Faz parte da suíte TCP/IP
- Camada de rede (internet) do modelo TCP/IP.
- Não orientado à conexão
- Tem como função receber bits da camada anterior, montar pacotes menores, e selecionar rota para envio.
- Não garante entrega (melhor esforço).

3.4. Estrutura do Pacote IP

4	4	8	16	
Versão	Header	TOS	Tamanho (em bytes)	
16			3	13
Identificação			Flags	OffSet
8	TTL	8	16	Checksum
32		IP Origem		
32		IP Destino		
Opções (se existirem)				
DADOS				

Campos:

Versão (4 bits)

Indica a versão do Protocolo. Atualmente existem duas versões do IP em uso: IPv4 e IPV6.

Header (4 bits)

Tamanho do Header (incluindo opções).

TOS – Type of Service (8 bits)

É utilizado para diferenciar o tipo do pacote a ser transportado, classificando-o para que possa ter prioridade em sua transmissão.

Tamanho (16 bits)

Total de bytes do pacote (Header + dados).

Identificação (16 bits) / Flags (3 bits) / Offset (13 bits)

Usados para o controle de fragmentação dos pacotes quando necessário (camada inferior não tem “espaço” suficiente para acomodar o pacote).

TTL – Time To Live (8 bits)

Tempo de vida: contém o número máximo de vezes que o pacote pode ser roteado (hop count).

Protocolo (8 bits)

Contém a identificação do protocolo “transportado” pelo IP.

Checksum (16 bits)

Cálculo efetuado sobre os campos do cabeçalho para garantir a integridade do pacote.

IP Origem (32 bits) e IP Destino (32 bits)

Usados para indicar a origem/destino dos pacotes dentro da estrutura da internet.

3.4.1. Endereçamento IP (v4)

Os endereços IP possuem as seguintes características:

- Deve ser único para cada dispositivo participante da rede.
- Divido em Net Id e Host Id (endereço da rede e endereço do dispositivo dentro daquela rede).
- Poder ser público ou privado (privados: 10.x.x.x, 172.16.x.x, 192.168.x.x, 169.254.x.x).
- Cada IP está associado a um único dispositivo, MAS um dispositivo pode ter múltiplos IPs.

3.4.2. Classes de endereçamento do protocolo IP

Endereços IP possuem 32 bits mas sua notação é feita em 4 grupos de 8 bits (notação pontuada). A forma como os bits são divididos entre Net Id e Host determinam a classe de endereçamento a qual o IP pertence.

Veja a tabela abaixo:

Classe de Endereçamento	w	Net Id	Host Id	Nets	Hosts
A	1-126	w	x.y.z	126	16.777.214
B	128-191	w.x	y.z	16.384	65.534
C	192-223	w.x.y	z	2.097.151	254

O endereço 127.x.x.x tem uso especial: *loopback* ou auto retorno. Sempre indica o próprio dispositivo.

3.4.3. Atribuição do endereço IP

Endereços IP podem ser obtidos de duas formas diferentes:

- Estático: configurado manualmente

- Dinâmico: obtido através de um servidor DHCP (Dynamic Host Configuration Protocol) ou através de **APIPA** (Automatic Private IP Addressing)

Endereços IP públicos são obtidos através do ICANN (Internet Corporation for Assigned Names and Numbers) e FAPESP

Pesquisar

- As fases da aquisição de um endereço IP via DHCP são resumidas pelo acrônimo DORA. Através de pesquisa na internet identifique quais são estas fases.

Entendendo

Muitos confundem o campo de TTL do protocolo IP com uma unidade de tempo. Na verdade, ele configura o máximo de ‘saltos’ ou encaminhamentos que um pacote pode fazer até chegar ao destino. Cada roteador no caminho do pacote diminui “1” no valor do TTL. Quando este valor chega em zero o pacote é descartado.

Saiba mais

Veja o vídeo disponível em <https://youtu.be/RhI5NN-VxOY> para entender um pouco mais sobre o DHCP.

Importante

Um pacote IP só é fragmentado quando seu tamanho excede o MTU (Maximum Transmission Unit) da camada de enlace.

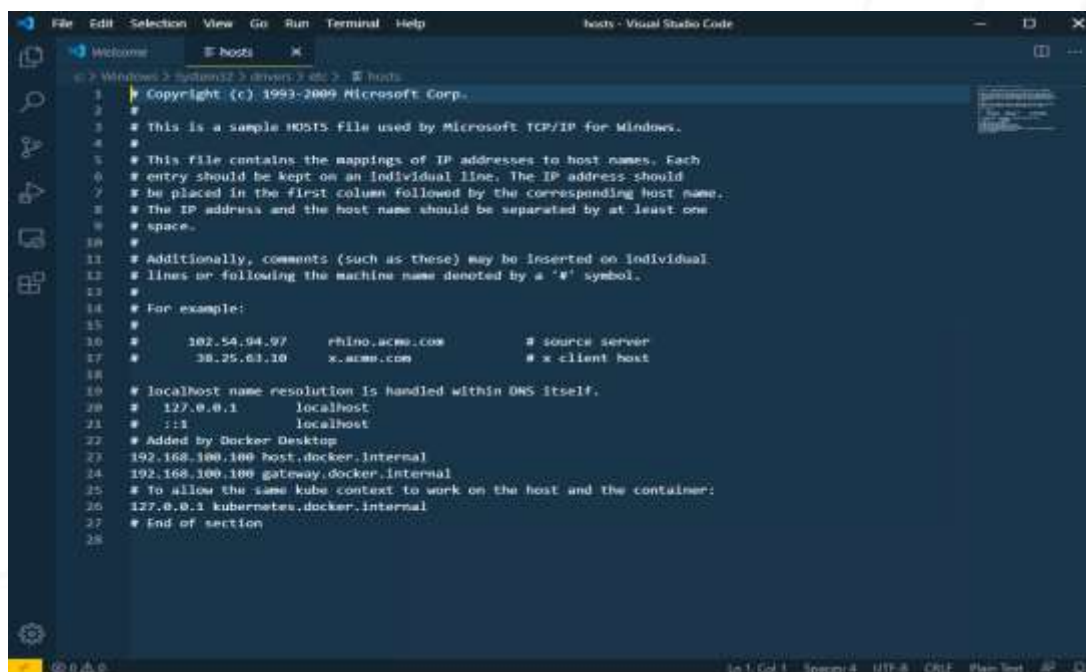
4. RESOLUÇÃO DE NOMES VIA DNS

4.1. Endereços IP x Nomes

Endereços IP são a forma de localizar dispositivos dentro da Internet. Cada nó (host) pode ser encontrado através do seu IP (4 bytes) expresso em notação decimal como no endereço 200.210.165.8 . No entanto achar os recursos através do IP não é uma forma intuitiva, pois é de difícil memorização. Para nós seres humanos “nomes” fazem muito mais sentido.

4.2. Resolução Nome – IP

Inicialmente a resolução de nomes para seus respectivos endereços IP era realizado através de arquivos texto como no caso do arquivo Hosts. Este arquivo possui uma linha para cada associação IP x nome como pode se ver na figura a seguir:



```
File Edit Selection View Go Run Terminal Help
hosts - Visual Studio Code

Welcome
hosts
> Windows > System32 > drivers > etc > hosts
1 Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97     rhino.acme.com   # source server
17 #       38.25.63.10    x.acme.com       # x client host
18 #
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1             localhost
21 # ::1                   localhost
22 #
23 # Added by Docker Desktop
24 192.168.100.100 host.docker.internal
25 192.168.100.100 gateway.docker.internal
26 # To allow the same kube context to work on the host and the container:
27 127.0.0.1 kubernetes.docker.internal
28 # End of section
```

4.3. DNS (Domain Name System)

Não seria possível resolver todos os nomes da internet a partir de arquivos texto nos dispositivos de cada usuário. Para o processo de resolução de nome para IP é usado um banco de dados distribuído (tipo de banco de dados onde os dados são particionados segundo algum critério lógico). O sistema de DNS é constituído de uma série de servidores que se comunicam entre si com o objetivo de localizar o endereço IP. Inicialmente a resolução de nomes para seus respectivos endereços IP.

4.3.1. Estrutura Hierárquica DNS

O banco de dados do DNS é constituído através de uma estrutura hierárquica em forma de árvore invertida.



Como não é possível a um único nó conter todas as associações nome-> IP esta estrutura hierárquica é composta de diversos servidores com as seguintes funções:

- Dispositivos fazer parte de “grupos” chamados domínios.
- Cada domínio possui um ou mais servidores.
- Cada servidor DNS passa a ser responsável somente pelo domínio a ele atribuído.
- Para resolver o endereço de dispositivos de outros domínios, é feita uma solicitação de resolução ao servidor de DNS do domínio correspondente.

4.3.2. Tipos de Solicitação DNS

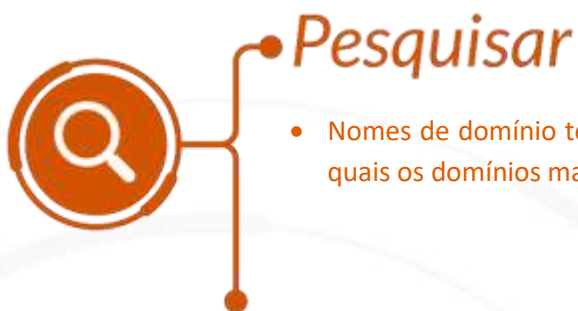
O processo de resolução de nomes pode envolver alguns tipos de solicitação:

- **Recursiva**
Cliente faz consulta a um servidor, passando o nome do host e o servidor responde com o IP (ou código de erro).
- **Iterativa**
Servidor DNS faz consulta a outro Servidor DNS quando não encontra em seu cadastro.
- **Reversa**
Retorna o nome de um host dado seu endereço IP.

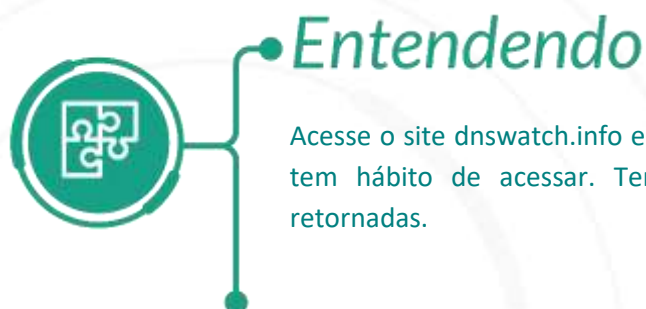
4.3.3. Tipos de registro DNS

Cada domínio é mantido em “zona DNS” que pode conter combinações de diversos tipos de registro:

- **Registros A:** basicamente, associam um ou mais endereços IP a um ou mais domínios. Pode-se utilizar AAAA para endereços IPv6;
- **Registros CNAME (Canonical Name):** servem para criar redirecionamentos para domínios ou subdomínios. Esta entrada é também conhecida como apelido, pois pode adicionar um segundo ou terceiro nome a um servidor ou equipamento host em uma rede;
- **Registros MX (Mail Exchanger):** são os parâmetros que devem ser configurados para contas de e-mail no domínio.
- **Registros NS (Name Server):** indicam quais servidores atuam como serviço de DNS dentro de uma rede ou de um site.
- **Registros PTR (Pointer):** informam quais domínios estão associados a determinados IPs, quase se fosse o reverso dos registros A.
- **Registros SRV (abreviação de Service):** indicam a localização de determinados serviços dentro do domínio.
- **Registros SOA (Start of Authority):** indicam o início de uma zona, isto é, de um conjunto de registros localizado dentro de um espaço de nomes de DNS. Cada zona deve ter um registro SOA.



- Nomes de domínio tem valor comercial. Pesquise na internet e descubra quais os domínios mais caros que já foram vendidos.



Acesse o site dnswatch.info e faça pesquisas de endereços de sites que você tem hábito de acessar. Tente entender o significado das informações retornadas.



Saiba mais

Para entender mais sobre como o sistema DNS é usado na internet assista o vídeo disponível em <https://youtu.be/ACGuo26MswI>



Importante

O arquivo Hosts, que em computadores com o sistema operacional Windows se encontra em C:\Windows\System32\Drivers\Etc, tem prioridade sobre todas as outras formas de resolução de nomes.

5. PROTOCOLOS CAMADA DE TRANSPORTE

5.1. Camada de Transporte

Os programas da camada de aplicação geram dados que devem ser trocados entre os hosts de origem e de destino. A camada de transporte é responsável pela comunicação lógica entre aplicativos executados em hosts diferentes. Isso pode incluir serviços como o estabelecimento de uma sessão temporária entre dois hosts e a transmissão confiável de informações para um aplicativo.

5.2. Protocolo TCP (Transmission Control Protocol)

O IP se preocupa apenas com a estrutura, o endereçamento e o roteamento de pacotes, do remetente original ao destino final. A IP não é responsável por garantir a entrega ou determinar se uma conexão entre o remetente e o destinatário precisa ser estabelecida.

O TCP é considerado um protocolo de camada de transporte confiável, completo, que garante que todos os dados cheguem ao destino. O TCP inclui campos que garantem a entrega dos dados do aplicativo. Esses campos exigem processamento adicional pelos hosts de envio e recebimento.

Nota: O TCP divide os dados em segmentos.

O transporte TCP é análogo a enviar pacotes que são rastreados da origem ao destino. Se um pedido pelo correio estiver dividido em vários pacotes, um cliente poderá verificar on-line a sequência de recebimento do pedido.

O TCP fornece confiabilidade e controle de fluxo usando estas operações básicas:

- Número e rastreamento de segmentos de dados transmitidos para um host específico a partir de um aplicativo específico;
- Confirmar dados recebidos;
- Retransmitir todos os dados não confirmados após um determinado período de tempo
- Dados de sequência que podem chegar em ordem errada
- Enviar dados a uma taxa eficiente que seja aceitável pelo receptor.

Para manter o estado de uma conversa e rastrear as informações, o TCP deve primeiro estabelecer uma conexão entre o remetente e o receptor. É por isso que o TCP é conhecido como um protocolo orientado a conexão.

5.3. Estrutura Básica do Pacote TCP



O IP se preocupa apenas com a estrutura, o endereçamento e o roteamento de pacotes, do remetente original ao destino. A IP não é responsável por garantir a entrega ou determinar se uma conexão entre o remetente e o destinatário precisa ser estabelecida.

5.4. Estabelecimento de conexão TCP

Cada conexão TCP é estabelecida através de um processo conhecido como handshaking:

- Estabelecimento de uma conexão antes da transmissão dos dados;
- Ao final da transmissão, a conexão é encerrada através do mesmo processo;



Objetivo: Sincronizar a transmissão e o recebimento de segmentos, configurar parâmetros de comunicação e criar uma conexão virtual.

5.5. Portas TCP

A “porta” TCP identifica qual aplicação no dispositivo está associada a conexão TCP:

- **16 Bits** com valor numérico entre 0 e 65.535.
- Função de identificar a **aplicação** e encaminhar o fluxo de dados para o local certo dentro do dispositivo.

- Uma aplicação da rede deve estar sempre associada à uma porta.



Pesquisar

- Através de pesquisa na internet identifique quais aplicações estão associadas as seguintes portas TCP: 80, 21, 443 e 1433.

Entendendo

Abra um prompt de comando no seu computador e digite o comando: “*netstat -a -n*”. Este comando mostrará quais conexões TCP estão estabelecidas no seu computador.

Saiba mais

Para entender mais sobre o protocolo TCP assista o vídeo disponível em <https://youtu.be/cy-ITN-ODDM>

Importante

O IP identifica o dispositivo e o TCP identifica a aplicação, por isso normalmente os dois são referenciados em conjunto. A este conjunto é dado o nome de SOCKET (Exemplo: 192.168.100.1:80)

6. CONTROLE DE FLUXO NOS PROTOCOLOS DA CAMADA DE TRANSPORTE

6.1. Confiabilidade do TCP

Não importa o quão bem projetada uma rede é, a perda de dados ocasionalmente ocorre. O TCP fornece métodos de gerenciamento dessas perdas de segmento. Entre esses métodos há um mecanismo que retransmite segmentos dos dados não confirmados.

O número de sequência (SEQ) e o número de confirmação (ACK) são usados juntamente para confirmar o recebimento dos bytes de dados contidos nos segmentos. O número SEQ identifica o primeiro byte de dados no segmento que está sendo transmitido. O TCP usa o número de confirmação (ACK) enviado de volta à origem para indicar o próximo byte que o destino espera receber. Isto é chamado de confirmação antecipatória.

6.1.1. Controle de Fluxo TCP

O protocolo TCP cria um serviço de **transferência confiável de dados** (sigla RDT em inglês) com as seguintes características:

- Transferência Confiável de Dados sob o serviço do protocolo IP que é um protocolo de “melhor” esforço, ou seja sozinho não garante a entrega dos dados;
- **Assegura fluxo de bytes** no lado receptor igual ao do lado remetente;
- **Segmentos em pipeline**;
- ACKs cumulativos;
- **Retransmissões podem ocorrer se:**
 - Der timeout;
 - Houver ACKs duplicados



A confirmação / retransmissão dos segmentos é assegurada com uso de dois “timers” que acompanham o tempo do envio dos pacotes:

Round-Trip time (RTT)

É o tempo necessário que o um pacote TCP seja enviado e a confirmação seja recebida.

Retransmission Timeout (RTO)

É o tempo até que se inicie a retransmissão dos pacotes. A cada nova tentativa o tempo de espera dobra até que seja atingido o número limite de tentativas.

6.2. Protocolo UDP

O UDP é um protocolo de camada de transporte mais simples do que o TCP. Ele não fornece confiabilidade e controle de fluxo, o que significa que requer menos campos de cabeçalho. Como o remetente e os processos UDP receptor não precisam gerenciar confiabilidade e controle de fluxo, isso significa que datagramas UDP podem ser processados mais rápido do que segmentos TCP. O UDP fornece as funções básicas para fornecer datagramas entre os aplicativos apropriados, com muita pouca sobrecarga e verificação de dados.

UDP é um protocolo sem conexão. Como o UDP não fornece confiabilidade ou controle de fluxo, ele não requer uma conexão estabelecida. Como o UDP não controla informações enviadas ou recebidas entre o cliente e o servidor, o UDP também é conhecido como um protocolo sem estado.

UDP também é conhecido como um protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino. Com o UDP, não há processo de camada de transporte que informe ao remetente se a entrega foi bem-sucedida.



Pesquisar

- Através de pesquisa na internet identifique ao menos um serviço ou aplicação que faça uso do protocolo UDP



Entendendo

Embora não possua controle de fluxo como o TCP o protocolo UDP também faz uso do número de porta para identificar o serviço/aplicação. Consultas de DNS (que utilizam UDP para melhorar o desempenho) utilizam a porta 53.



Saiba mais

Para entender mais sobre o protocolo TCP x UDP assista o vídeo disponível em <https://youtu.be/cy-ITN-ODDM>



Importante

Como o protocolo UDP não tem controle de fluxo, ele deve ser preferencialmente adotado por aplicações com tolerância à falhas. Para os casos em que é necessário garantia de entrega deve ser usado o protocolo TCP

7. PROTOCOLO HTTP

7.1. História do Protocolo HTTP (HyperText Transfer Protocol)

O protocolo HTTP é provavelmente um dos maiores responsáveis pela popularização da Internet. Ele é usado toda vez que alguém abre um navegador para acessar um site, usar uma rede social ou fazer uma pesquisa.

Desenvolvido inicialmente em 1990 por **Tim Bernes Lee** no Laboratório de Física de partículas em CERN na Suíça;

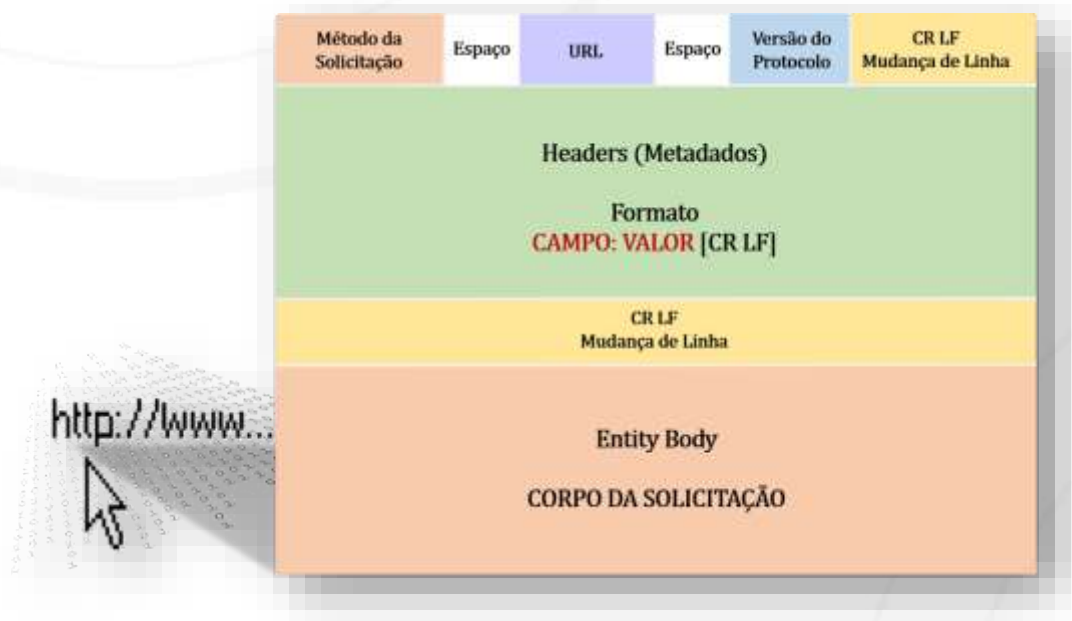


Permite recuperar documentos através de um sistema de navegação conhecido como hipertexto.

7.2. Características do protocolo HTTP

- O Protocolo da **Camada de Aplicação**.
- Modelo **cliente/servidor**.
- **Cliente:** Browser que pede, recebe, visualiza objetos www.
- **Servidor:** Servidor www envia respostas.
- Duas versões **HTTP/1.0 e HTTP/1.1**
- Usa serviço de **transporte TCP**;
- **Cliente:** Estabelece conexão TCP ao servidor na porta 80;
- **Servidor:** Escuta porta 80;
- **Mensagens HTTP:** Mensagens do protocolo da camada de aplicação são trocadas entre browser (cliente HTTP) e servidor Web (servidor HTTP);
- Cada troca **encerra conexão TCP**;
- **Não mantém/conserva estado**;
- Protocolo **Response – Request**

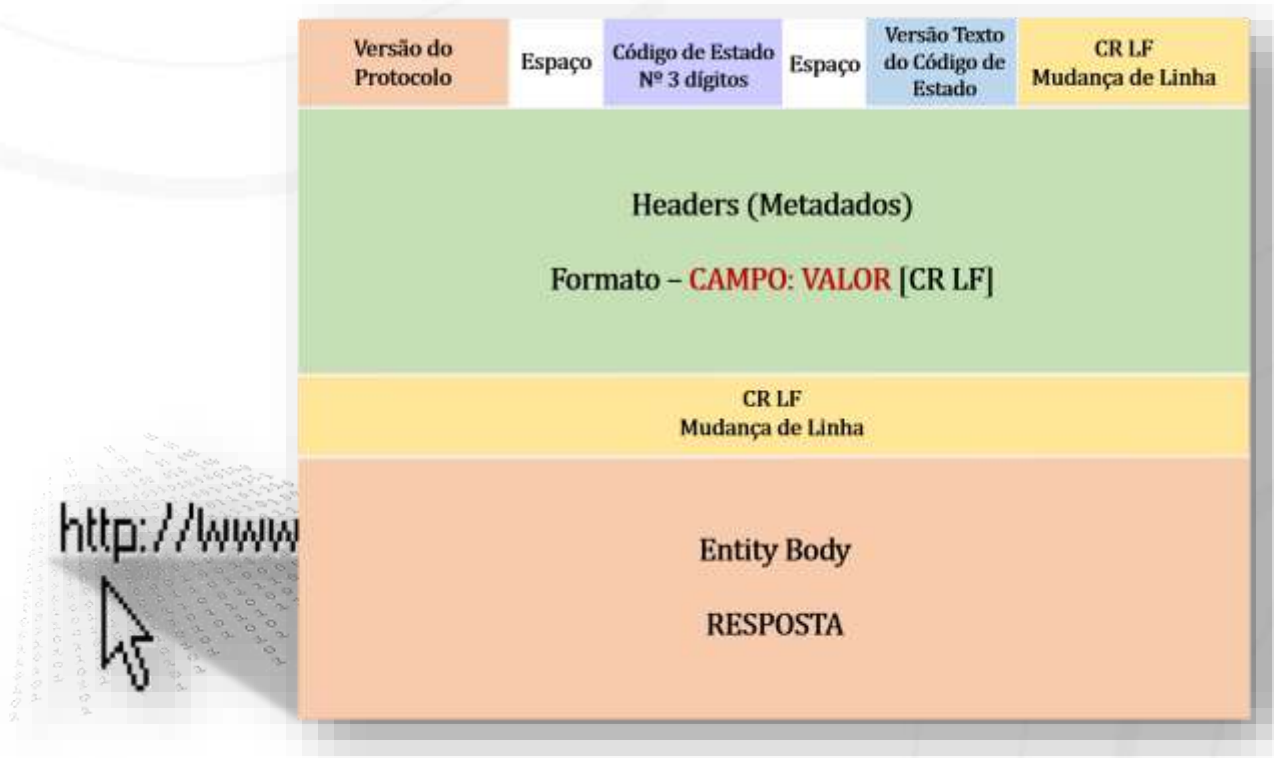
7.3. Formato Solicitação HTTP



7.3.1. Métodos mais comuns em uma solicitação HTTP

		GET /default.htm HTTP/1.1 Host: www.redes4.net Connection: close User-agent: Mozilla/4.0
GET	Recupera um recurso .	
HEAD	Recupera informações sobre um recurso.	
POST	Envia informações ("valores") usando os campos de cabeçalho.	
PUT	Faz "upload" de um recurso.	
DELETE	Exclui um recurso.	

7.4. Formato Resposta HTTP



7.4.1. Códigos de Resposta HTTP

Retorno	Descrição	HTTP/1.1 200 OK Connection: close Date: Thu, 06 Aug 1998 12:00:15 GMT Server: Apache/1.3.0 (Unix) Last-Modified: Mon, 22 Jun 1998 Content-Length: 6821 Content-Type: text/html (DADOS - RESPOSTA)
1YZ	Informação apenas 100 Continue	
2YZ	Resposta Positiva 200 OK	
3YZ	Redirecionamento para outra URL ou cache 301 Moved Permanently *	
4YZ	Erros do Cliente 404 Not Found	
5YZ	Erros do Servidor 500 Server Error	



Pesquisar

- Acesse <http://info.cern.ch/> - primeiro site da internet



Entendendo

Embora o protocolo HTTP seja inegavelmente um grande sucesso, isso não poderia ser concluído em seus primeiros anos de uso. Em 1993 com cerca de três anos da criação do protocolo existiam pouco mais de 130 sites no mundo.



Saiba mais

Para entender mais sobre o protocolo HTTP assista o vídeo disponível em <https://youtu.be/fhAXgcD21iE>



Importante

Os browsers (navegadores) são prontamente associados ao protocolo HTTP, mas é importante ressaltar que atualmente este protocolo é usado como mecanismo de comunicação entre processos, sendo usados desde aplicativos de celular a “smart TVs”

8. PROTOCOLOS PARA COMPARTILHAMENTO DE INTERNET (NAT X PROXY)

8.1. Network Address Translation (NAT)

Um dispositivo dotado de NAT (Network Address Translation) pode ser usado para compartilhar um único ip público entre vários dispositivos de rede que possuam apenas IPs privados. Um dispositivo NAT tem as seguintes características:

- Pode ser implementado por um serviço rodando em um computador multihomed (2 placas de rede) ou um hardware especializado;
- Basicamente “troca” os IPs privados por IPs públicos (normalmente);
- Dois tipos: Estático e Dinâmico.
- Estático: Associa IPs e Portas Internas com IPs e Portas Externas com uma relação permanente de 1 para 1. Serve para quando quer que um serviço seja acessível pela rede. Ex.: câmeras de vigilância.
- Dinâmico: Associa IPs e Portas Internas com IPs e Portas Externas sem relação permanente. NAT seleciona portas aleatórias, as que estiverem livres/disponíveis.

Dispositivos do tipo NAT são muitos comuns em redes domésticas para possibilitar o acesso a internet. Veja algumas vantagens/desvantagem do uso de NAT:

Vantagens	Desvantagem
<ul style="list-style-type: none"> • NAT não precisa ser configurado: Não precisa de nenhum programa para funcionar. • Pode deixar um serviço acessível pela rede, associando IPs/Portas internas com as externas. • ADM Centralizada: Controle de acesso e conteúdo. • NAT aceita todos os protocolos. 	<ul style="list-style-type: none"> • NAT trabalha de forma transparente para o Protocolo TCP: Não examina o conteúdo. <p>Ex.: Se 30 computadores forem acessar o mesmo conteúdo, NAT fará as 30 conexões. Trafego da rede sobrecarregado!</p>

8.2. Servidor Proxy

Uma outra estratégia muito usada para compartilhamento de internet é o uso de servidores Proxy. Um proxy tem as seguintes características:

- **Proxy** é um computador ou roteador que intermedia a conexão entre cliente e servidor, estando entre a LAN e a Internet.
- **Normalmente é dual-homed:** Duas placas de rede.

- **Previne contra invasões à rede interna**, saída de dados confidenciais e restrição a conteúdo não permitido;
- **Possui Cache.**

Entre as vantagens do uso servidores proxy estão:

- **Proxy está mais próximo do cliente:** Tempo de resposta menor;
- **Diminui tráfego aos servidores distantes;**
- **Get Condicional:** Retorna conteúdo somente se não foi modificado;
- **Túnel:** Ao usar a porta 443, conexão segura, o proxy cria um túnel e não analisa a informação que estiver passando (CONNECT), o que garante;
- **ADM Centralizada:** Controle de acesso e conteúdo;

A principal desvantagem de um servidor proxy é que, ao contrário do que acontece com o NAT, ele exige a configuração no dispositivo.



- Pesquise na internet e verifique se consegue achar servidores proxy gratuitos



Para saber mais sobre NAT assiste o vídeo disponível em <https://youtu.be/BSe7EgvDB6Q>.



Servidores Proxy são comumente usadas para “mascarar” a origem do acesso, uma vez que para o servidor que está recebendo as conexões os acessos partiram do IP do Proxy.

9. CONCEITOS BÁSICOS DE SEGURANÇA DE REDES.

9.1. Propriedades (atributos) relativas à segurança

Quando se trata de segurança de informação é comum que sejam levados em conta três atributos da informação:

- **Confidencialidade**

A informação **não deve nem ficar acessível**, nem ser divulgada para um usuário, uma entidade ou um processo não autorizado.

- **Integridade**

A informação **não deve ser alterada** ou destruída de maneira não autorizada.

- **Disponibilidade**

O **acesso** aos serviços oferecidos pelo sistema deve ser **sempre possível** para um usuário, entidade ou processo autorizado

9.2. Ameaças

Quando algum atributo de segurança é comprometido estamos lidando com a concretização de uma ameaça:



9.3. Exemplo de ataques

Veja alguns dos ataques mais comuns:

- **Vírus x Worms x Trojans**
- **Packet Sniffing** - Visualização pacotes.
- **Spoofing** - Falsificação IP/Mac.
- **Session Hijacking** – Interceptação.
- **DoS (Denial of Service)** – Interrupção de acesso.

- **DDoS (Distributed Denial of Service).**
- **Ransomware** – “Sequestro” de dados.

9.4. Proteção contra “hackers” e outros ataques

Quando se trata de proteção contra a exploração de vulnerabilidades de rede, duas das soluções mais usadas são uso de Firewall e sistemas de detecção de intrusão (sigla IDS em inglês).

9.4.1. Firewall

Características de um “Firewal”:

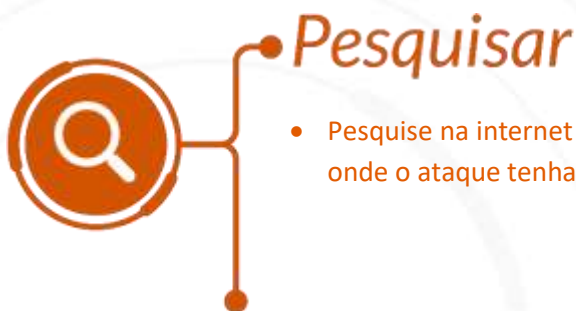
- **Sistema que restringe o acesso entre duas redes.**
- Isola a rede interna da rede externa.
- Regras pré-programadas e estabelecidas.
- **Componentes:** Filtro de Pacotes, Proxy, NAT, VPN



9.4.2. IDS

Como os ataques podem usar variação de técnicas ou novas vulnerabilidades para quais o firewall não tem uma “regra” programada em alguns cenários é necessário a adoção de soluções “inteligentes”. Os sistemas de detecção de intrusão são a principal estratégia usada nestes casos. Suas características:

- Sistema que restringe o acesso entre duas redes, porém **examina padrões de comportamento/cenário.**
- **Aprendem** e são capazes de mudar as **regras dinamicamente.**
- **Desvantagem:** Falso-Positivo (Comportamento não esperado, porém válido, IDS não detecta).



- Pesquise na internet algum comprometimento de segurança a informação onde o ataque tenha sido feito através de um “ransomware”.



Entendendo

Embora os termos “Vírus” e “Worms” sejam usados por muitos como “sinônimos”, há uma diferença importante entre eles: Worms não necessitam de uma ação do usuário podendo se espalhar pela rede usando vulnerabilidades do sistema operacional ou da infraestrutura de redes.



Saiba mais

Para saber mais sobre o que é ransomware assista o vídeo disponível em <https://youtu.be/x9PgxTSbo0o>



Importante

A maioria dos ataques bem-sucedidos não exploram apenas vulnerabilidades técnicas, mas falhas humanas através de estratégias conhecidas como “engenharia social”



Referências

KUROSE, JAMES F ; ROSS KEITH W. Redes de computadores e a Internet: uma abordagem top-down. São Paulo: Pearson Education do Brasil, 2013
TANENBAUM, ANDREW S. Redes de computadores. São Paulo: Pearson Prentice Hall, 2011
RIBEIRO, MARCELLO P. Redes de telecomunicações e teleinformática: um exercício conceitual com ênfase em modelagem. Rio de Janeiro: Interciência, 2012



Concluindo

Após assistir as aulas online, participar de fóruns e fazer uma série de atividades complementares, você deve ter ampliado o seu conhecimento sobre redes de computadores em geral. Aliado a esta nova gama de informações estruturais o seu conhecimento sobre o funcionamento da Internet também deve ter sido ampliado.