



Programa “Hackers do Bem”

Aula 01 – E-mail

Compreender Camada de Aplicação
Serviços de Rede.

- Primeiro e-mail enviado em 1971 pelo programador Ray Tomlinson (projeto ARPANET).
- Primeiro envio em massa de e-mails aconteceu em 1978 por Gary Thuerk.
- Chegada do FAX em 1989 acreditava-se que seria o fim do e-mail.
- Devido ao avanço da internet, o e-mail era usado em universidades e grandes empresas por conta do custo, em 1996 o Hotmail disponibilizou contas gratuitas para público em geral, tornando o e-mail mais popular.
- Segundo pesquisa feita em Outubro de 2022, existem cerca de 4,3 bilhões de contas de e-mail em todo mundo.



Introdução

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

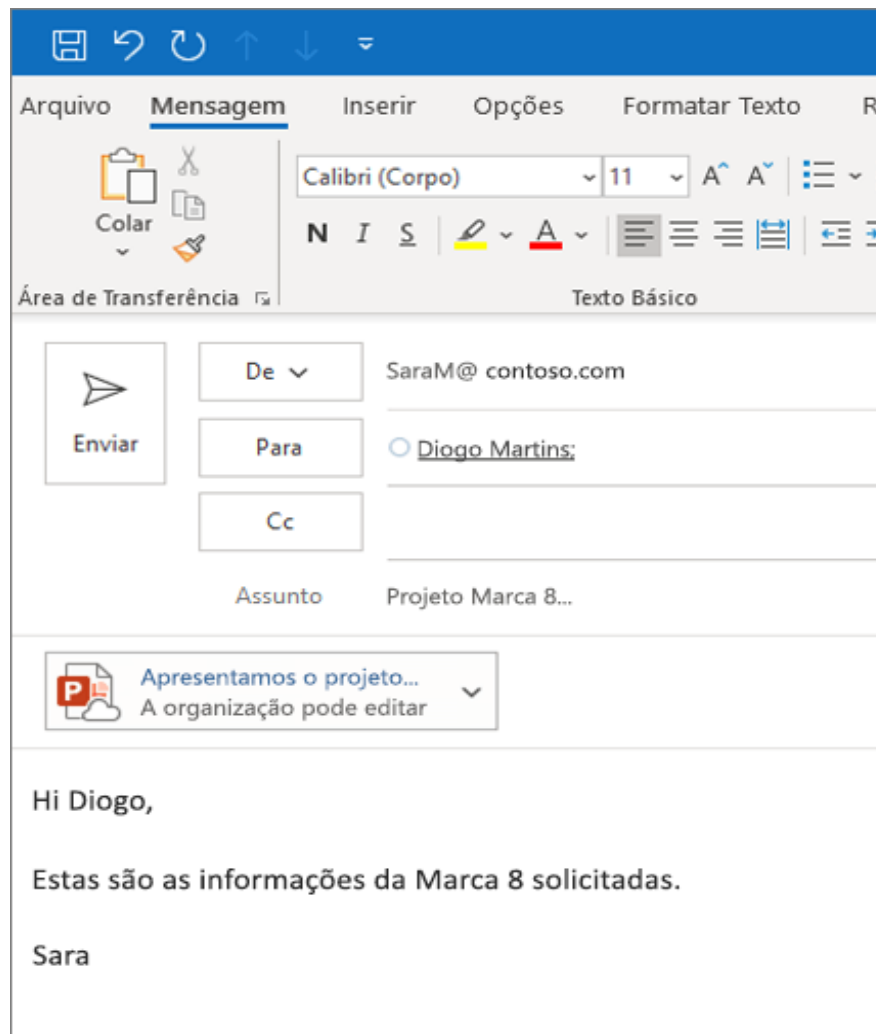
WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

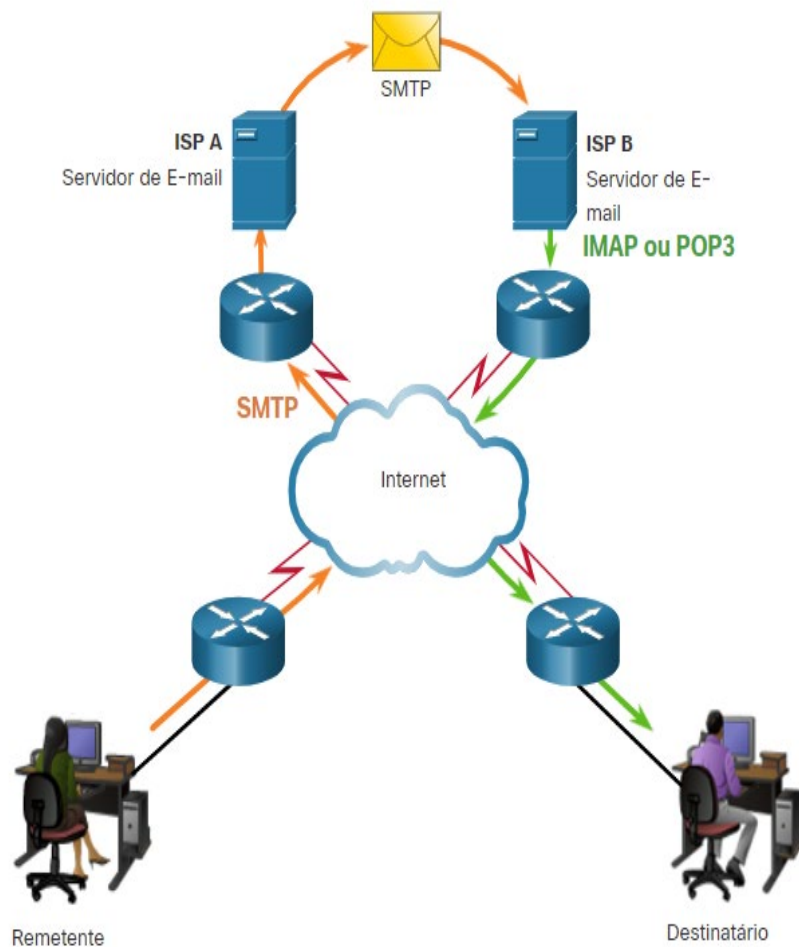
THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY

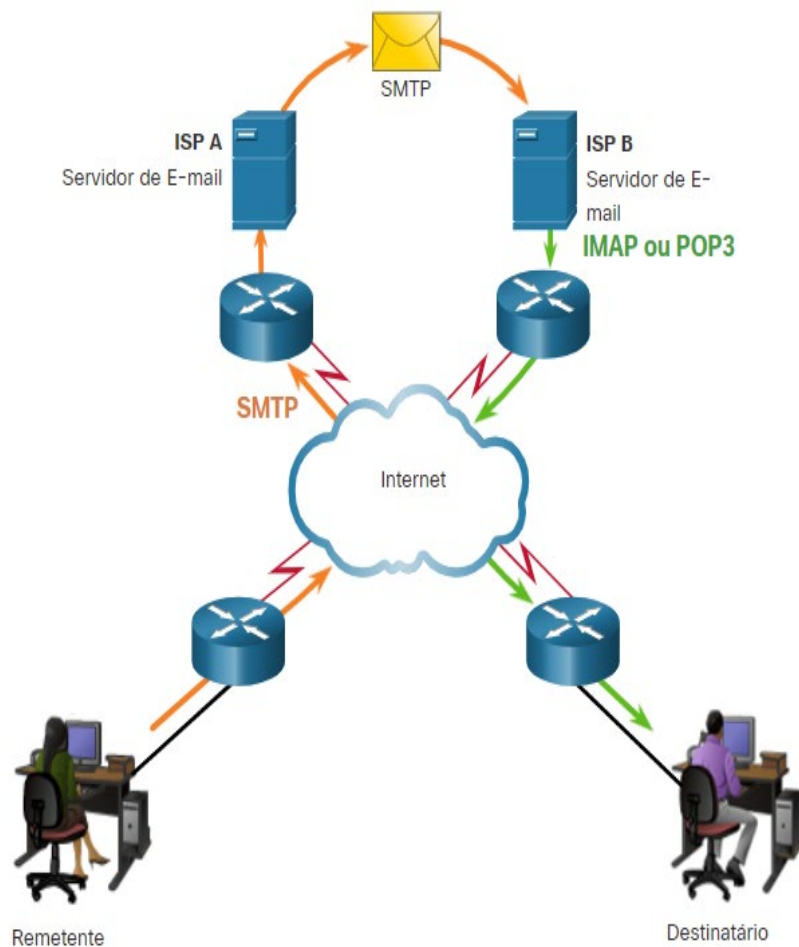
Fonte : https://www.researchgate.net/figure/The-First-Spam-Message-sent-by-a-Gary-Thuerk-a-DEC-marketing-representative-to-a-huge_fig1_242416368 acessada em 18/05/2023



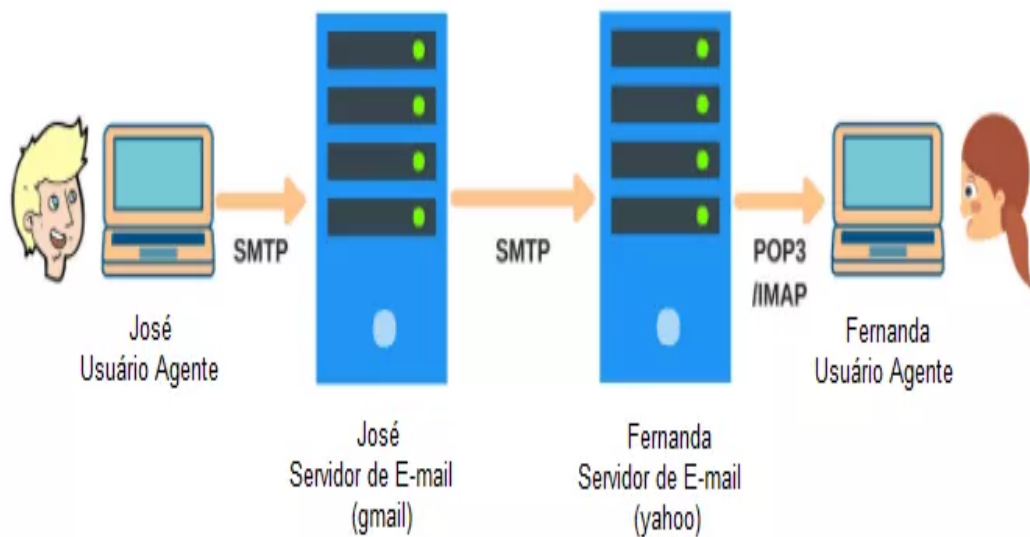
Fonte : <https://support.microsoft.com/pt-br/office/criar-e-enviar-emails-no-outlook-para-windows-a39afde4-0e07-4f0f-9076-ce97f1aabb03> acessada em 18/05/2023



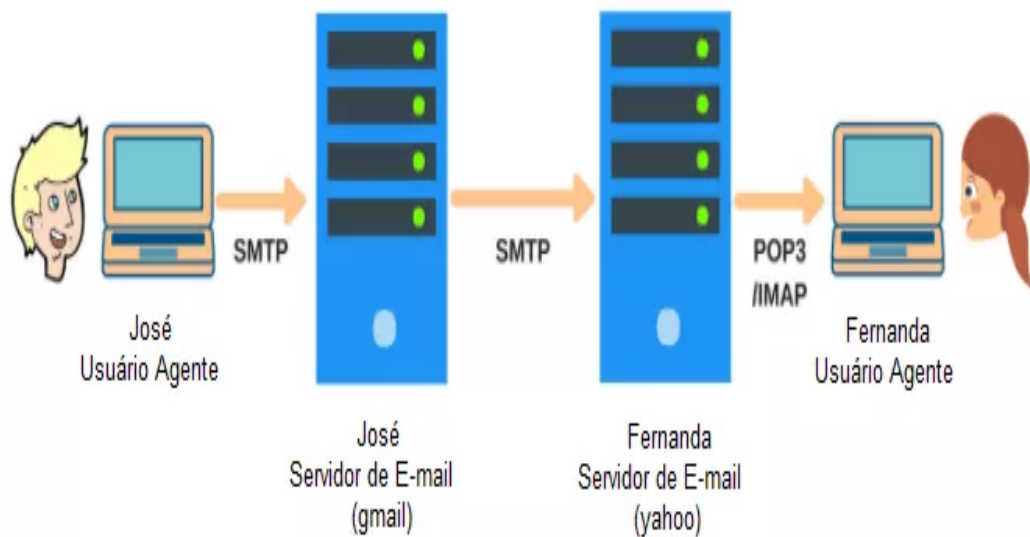
- Serviços de e-mail são oferecidos pelo provedor.
- E-mail armazena, encaminha, envia e recupera mensagens eletrônicas em uma rede.
- E-mail suporta 3 protocolos separados com diferentes propósitos: SMTP, POP3 e IMAP



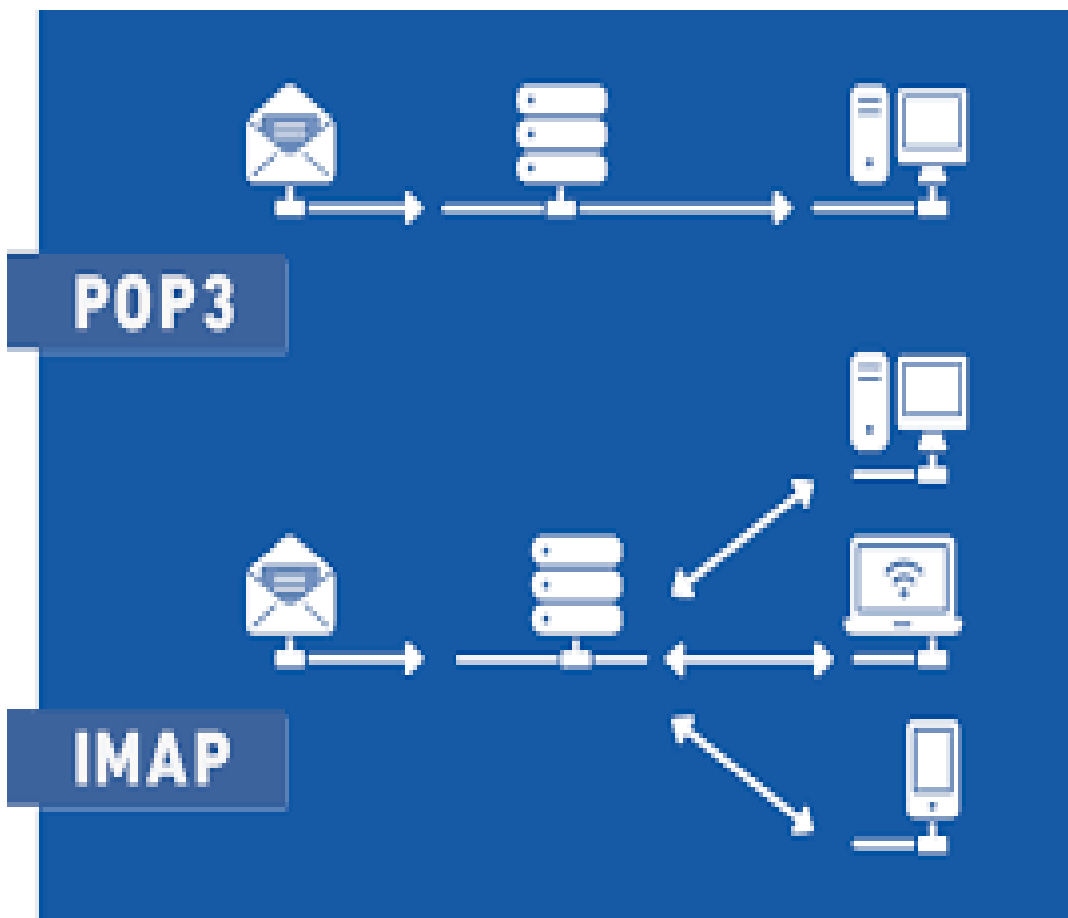
- SMTP – Simple Mail Transfer Protocol.
- Formato SMTP exige cabeçalho de mensagem e corpo de mensagem.
- Para envio da mensagem via SMTP, utiliza-se a porta 25.



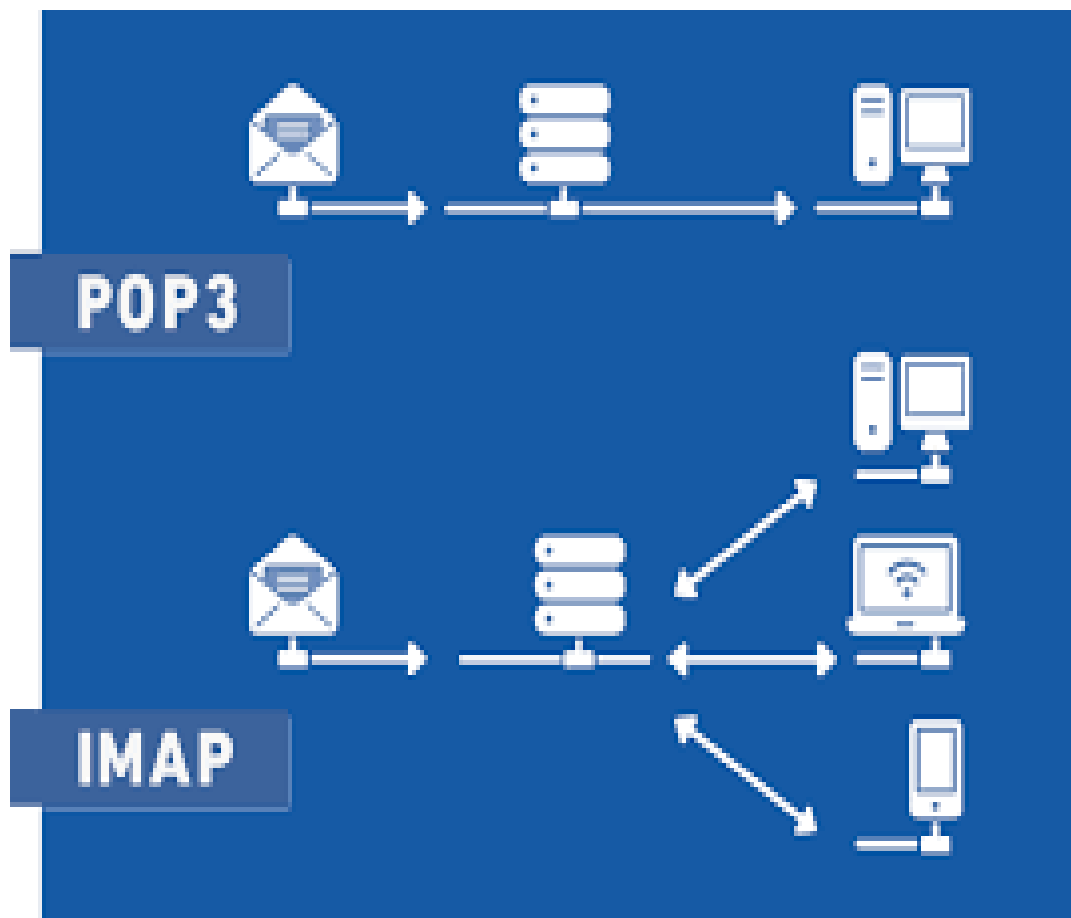
- Armazenamento do e-mail pode ser local ou encaminhado para outro servidor para entrega.
- Não há necessidade do servidor de destino estar online.
- SMTP armazena mensagens para serem enviadas posteriormente.



- POP3 é usado para recuperar e-mails de um servidor, é transferido para o cliente e excluído do servidor.
- POP3 porta padrão 110, insegura, sem criptografia.
- POP3 porta 995 segura e com criptografia.



- Outro protocolo além do POP3 para recuperação de mensagens de e-mail.
- Ao contrário do POP3 as mensagens originais são mantidas no servidor até serem excluídas.
- A estrutura de arquivos é duplicada, quando um usuário decide excluir uma mensagem, o servidor sincroniza a ação e exclui do servidor também.
- Pode verificar seu e-mail em diferentes dispositivos.



- Ambos são usados para recuperação de e-mail, enquanto o POP define apenas comandos simples para executar, o IMAP permite a sincronização entre dispositivos e acesso online (mais de 1).
- Vantagens e Desvantagens.

Após completar esta aula, saberá reconhecer e compreender os principais protocolos de e-mail, tais como o SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) e IMAP (Internet Message Access Protocol). Além disso, você saberá avaliar as características distintas de cada um desses protocolos, assim como suas aplicações práticas no contexto do envio, recebimento e gerenciamento de mensagens eletrônicas.

Aula 02 – Web (HTTP / HTTPS)

- O desenvolvimento do World Wide Web começou em 1980 por Tim Berners-Lee
- Em 1984 Berners-Lee se deparou com problemas de apresentação das informações.
- Em 1989 redigiu uma proposta para solucionar, através de um grande banco de dados e com hiperligações.
- Apenas em 1990 conseguiram recursos para levar a ideia para frente.
- No natal de 1990, Berners-Lee constrói a ferramenta HTTP e a linguagem HTML, o primeiro browser WWW, o primeiro servidor HTTP CERN httpd e o primeiro servidor web o `http://info.cern.ch`.
- No dia 6 de Agosto de 1991, Berners-Lee publicou um resumo do projeto World Wide Web no `alt.hypertext.newsgroup`, essa data marca o nascimento da Web.



World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), November's [W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)

Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)

on the browser you are using

[Software Products](#)

A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#))

[Technical](#)

Details of protocols, formats, program internals etc

[Bibliography](#)

Paper documentation on W3 and references.

[People](#)

A list of some people involved in the project.

[History](#)

A summary of the history of the project.

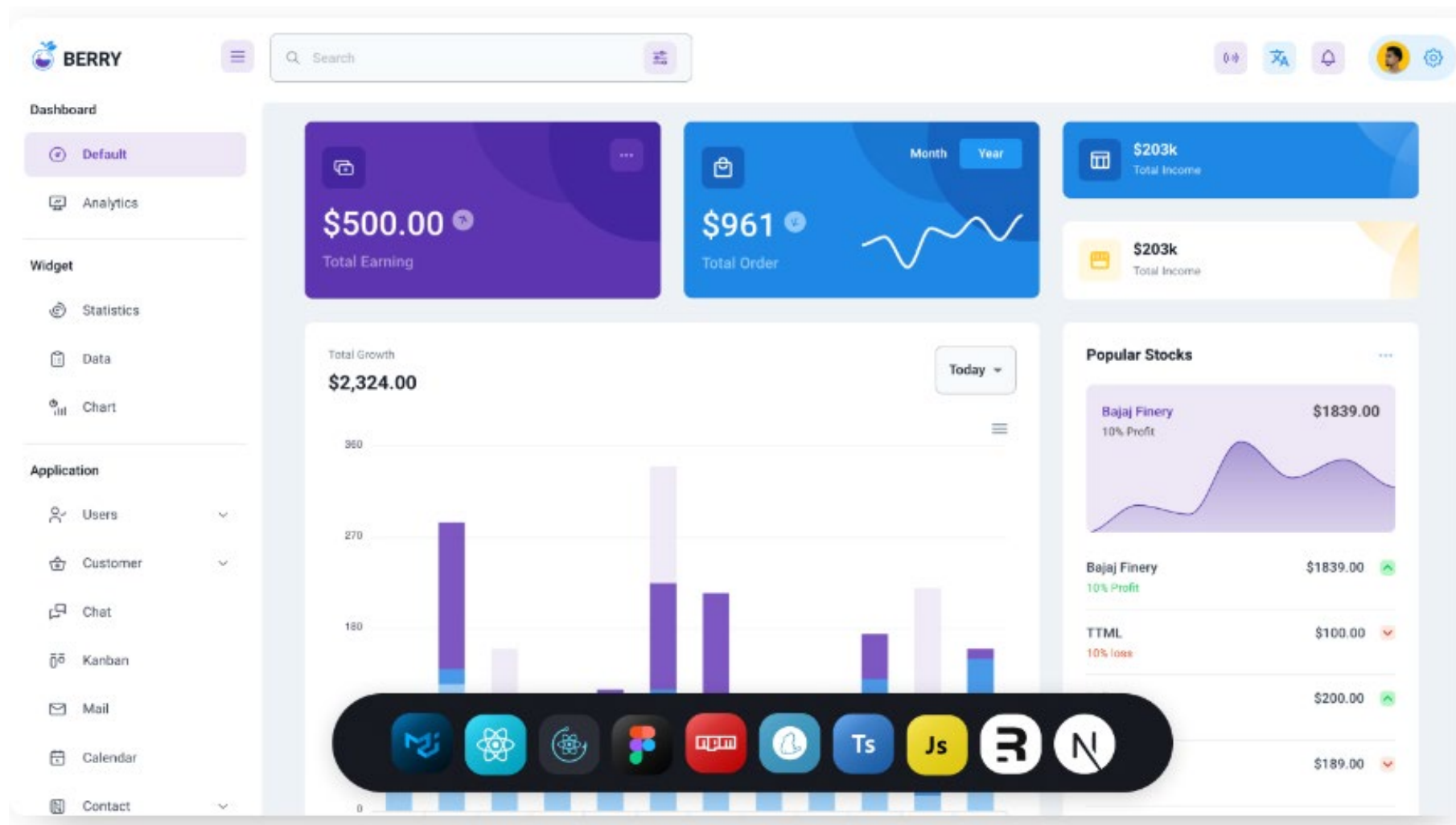
[How can I help ?](#)

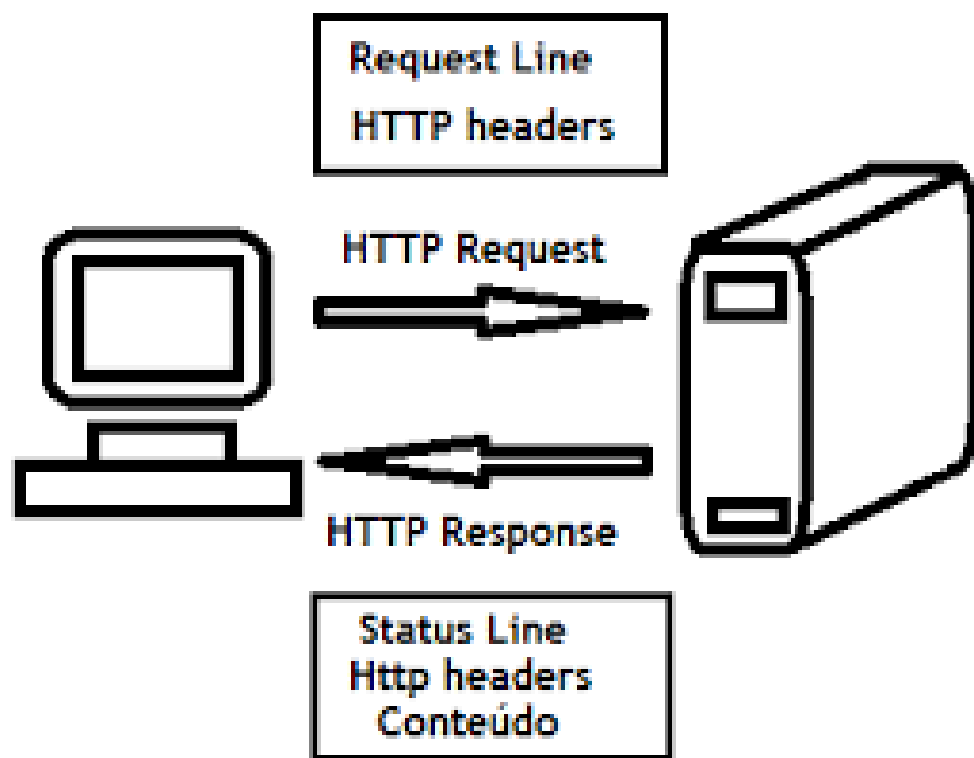
If you would like to support the web..

[Getting code](#)

Getting the code by [anonymous FTP](#), etc.

Introdução





- Etapas de uma estrutura Web:
- 1 – Navegador interpreta como 3 parte da URL:
 - http(protocolo)
 - www.abcde.com (nome do servidor)
 - Index.html(nome do arquivo solicitado)
- 2 – Navegador verifica em um servidor DNS para converter www.abcde.com em um endereço de IP válido.
- 3 – Em resposta à solicitação, o servidor envia um código HTML.
- 4 – O navegador decifra o código HTML e formata a página.

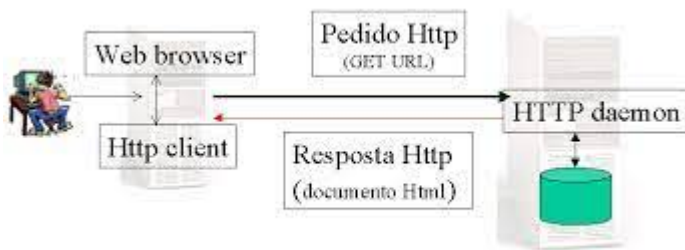
- GET – Solicitação de dados feita pelo cliente.
- POST – Carrega arquivos de dados de um servidor da web, como dados de formulário.
- PUT – Carrega recursos ou conteúdos, como imagem por exemplo.

PROTOCOLOS HTTP

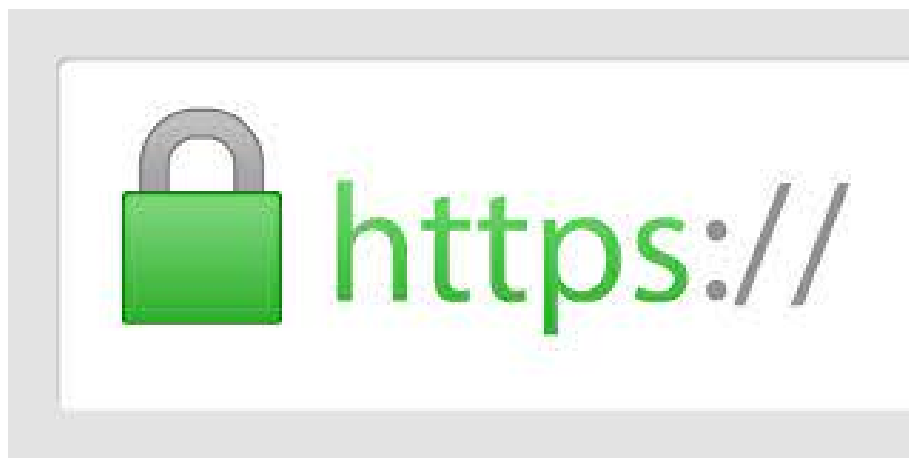
- GET
- POST
- PUT
- DELETE
- OPTIONS
- TRACE
- CONNECT
- HEAD

192.168.15.202	192.168.15.1	HTTP	210 GET /dyndev/uuid:a433d762-6921-2169-62d7-33a43362210000 HTTP/1.1
192.168.15.1	192.168.15.202	HTTP	184 HTTP/1.0 200 OK
192.168.15.202	192.168.15.1	HTTP/XML	660 POST /uuid:a433d762-6921-2169-62d7-33a43362210002/WANPPPConnection:1 HTTP/1.1
192.168.15.1	192.168.15.202	HTTP/XML	472 HTTP/1.1 200 OK

Fonte : O Autor feito em 18/05/2023

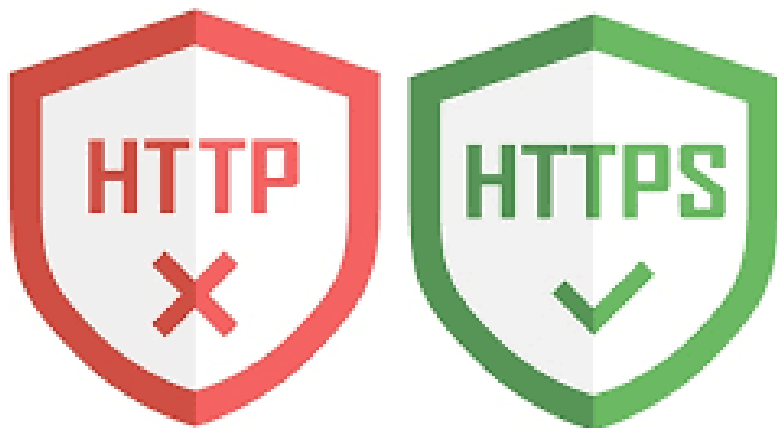


Fonte : <http://devfuria.com.br/php/como-funcionam-os-metodos-get-e-post/> acessado em 18/05/2023



- Utiliza autenticação e criptografia para proteção de dados.
- Processos e métodos são os mesmos do HTTP porem o fluxo é criptografado com SSL.
- Enquanto o HTTP utiliza das porta 80 ou 8080 o HTTPS utiliza das portas 443 ou 8443.

<https://www.divtec.com.br/artigos/20-o-que-e-o-certificado-ssl-e-porque-e-importante> - acessado em 18/05/2023



- Embora o HTTP seja flexível, não é seguro.
- Mensagens podem ser interceptadas e lidas.
- As páginas HTML não são criptografadas.
- HTTPS surge para corrigir esses problemas e agregar cibersegurança à WEB.

Após completar esta aula, saberá reconhecer e compreender o surgimento da web e seus protocolos, tais como o HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure). Além disso, você saberá avaliar as características distintas de cada um desses protocolos, assim como suas aplicações práticas no contexto da web e seus protocolos.

Aula 03 – DNS

- O DNS foi criado em 1983 pelo americano Paul Mockapetris.
- Objetivo de facilitar a escalabilidade da Internet.
- Popularizar e facilitar o acesso à Internet



Fonte : <https://blog.ingrammicro.com.br/seguranca-da-informacao/o-que-e-dns/> - acessada em 19/05/2023

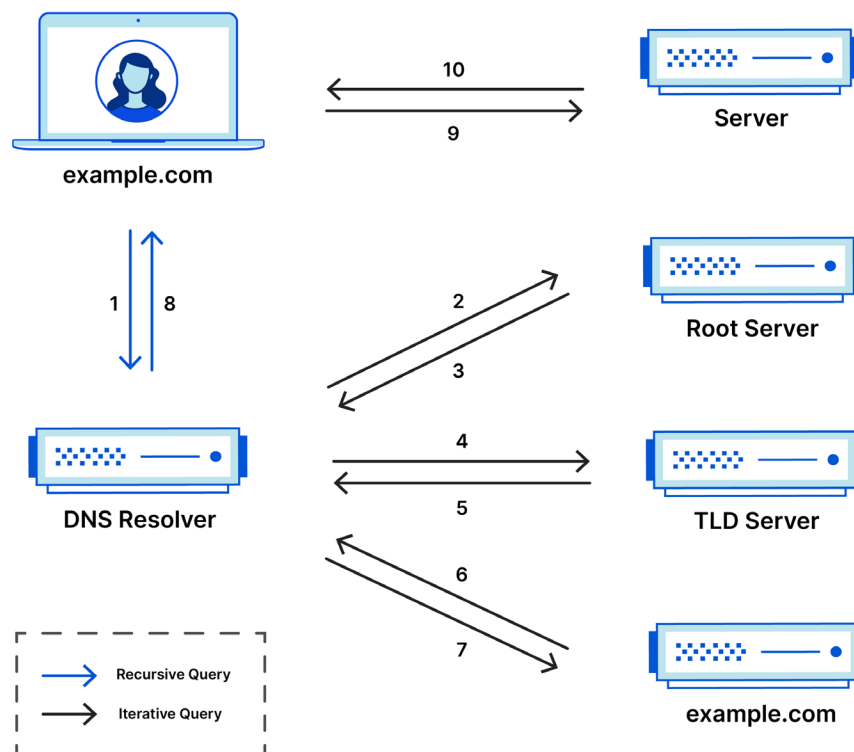
Camada de Aplicação – O que é DNS?



- DNS – Domain Name System (Sistema de Nomes de Domínio).
- Facilitador, é encarado como a “lista telefônica” da internet.
- O DNS converte os nomes de domínio como “google.com” em endereços IP.
- Os servidores DNS eliminam a necessidade de que humanos memorizem endereços IPv4 ou IPv6.

- O processo de resolução do DNS envolve a conversão de um hostname (google.com) em um endereço de IP fácil de ser entendido pelo computador(192.168.0.10).
- Existem 4 servidores de DNS envolvidos no carregamento de uma página de Internet:
 - Recursor de DNS;
 - Servidor Raiz;
 - Nameserver TLD;
 - Servidor de DNS autoritativo.

Complete DNS Lookup and Webpage Query



- O que é cache?
 - Armazenamento de dados
 - Aumento de desempenho.
 - Confiabilidade.
 - Redução de consumo de largura de banda.

Após completar esta aula, saberá reconhecer e compreender o surgimento do DNS, seu funcionamento bem como as etapas de uma consulta DNS. Além disso, você saberá avaliar as características distintas deste serviço, assim como suas aplicações práticas no contexto de redes.

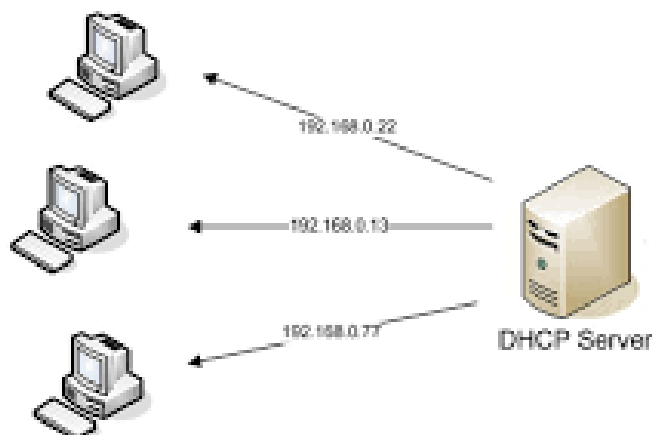
Aula 04 – DHCP

- O DHCP é uma evolução do protocolo BOOTP.
- Limitação do protocolo BOOTP em configurar redes muito grandes.
- IETF desenvolve o protocolo DHCP para prover escalabilidade para as redes.



Fonte : <https://redelan.wordpress.com/2020/02/10/como-funciona-o-dhcp/> - acessada em 19/05/2023

Camada de Aplicação – O que é DHCP?

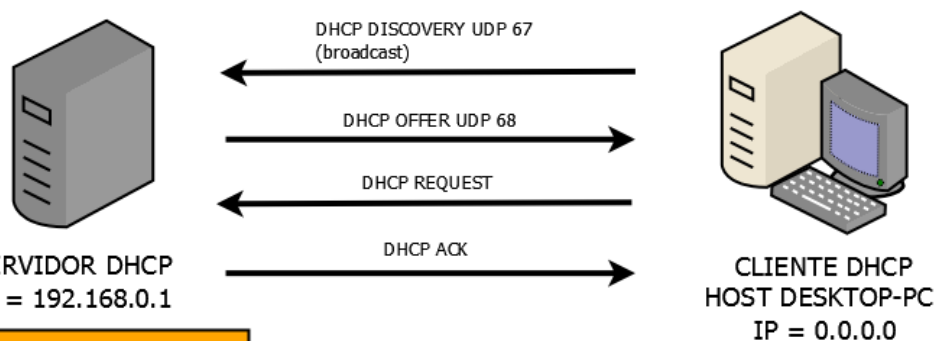


- DHCP – Dynamic Host Configuration Protocol.
- Protocolo do tipo cliente/servidor.
- Permite que os hosts obtenham as configurações TCP/IP de forma dinâmica.
- Elimina a necessidade de atribuição manual de endereço IPV4, muito vantajoso para grandes redes.

Fonte : <https://www.techtudo.com.br/noticias/2014/10/o-que-e-dhcp-entenda-tudo-sobre-o-protocolo.shtml> acessada em 19/05/2023

DHCP – Como funciona?

DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL



Endereço IP Inicial = 192.168.0.100
Endereço IP Final = 192.168.0.199
Tempo de Renovação = 120
Gateway Padrão = 192.168.0.1
DNS Primário = 208.67.222.222
DNS Secundário = 208.67.220.220

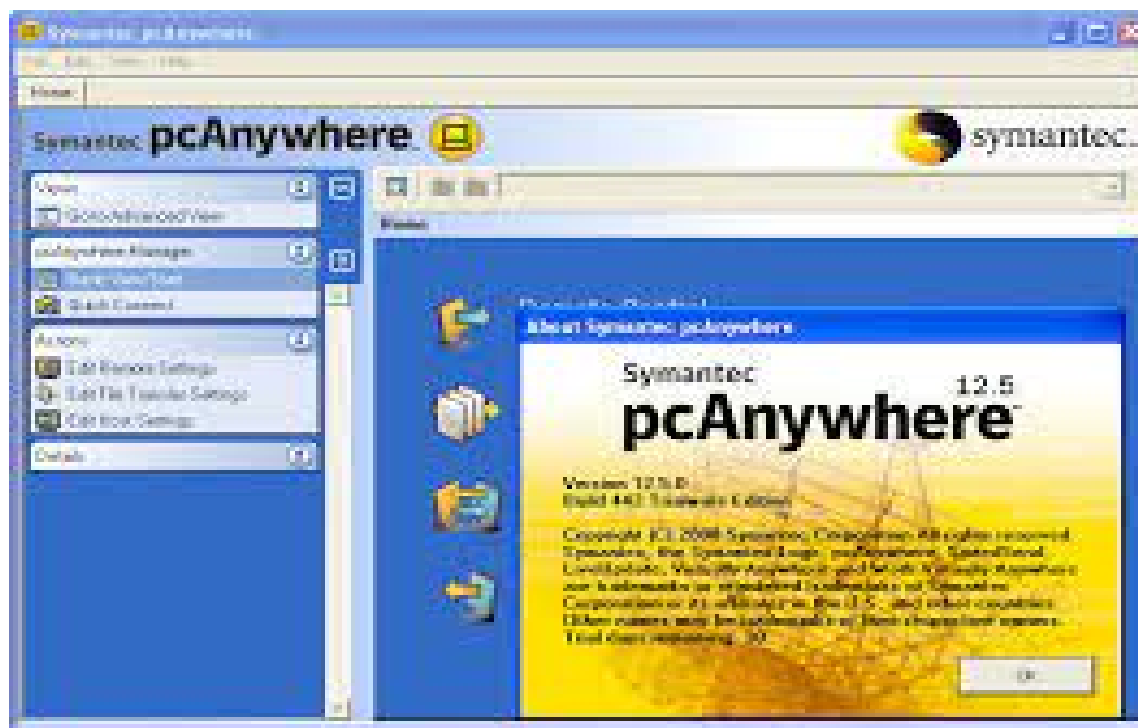
DHCP Ativado = Sim
Endereço IPv4 = 192.168.0.100
Mascara Sub-Rede = 255.255.255.0
Concessão Obtida = dd,mm,aa,h
Vencimento Concessão = dd,mm,aa,h
Gateway = 192.168.0.1
Servidor DHCP = 192.168.0.1
DNS Primário = 208.67.222.222
DNS Secundário = 208.67.220.220

- Servidor DHCP escolhe um endereço de uma “pool” disponível.
- Período de concessão de IP pelo DHCP.
- Servidor DHCP armazena as informações de configuração em um banco de dados.
- Portas de requisição e resposta 67 e 68.

Após completar esta aula, saberá reconhecer e compreender o surgimento do DHCP, seu funcionamento bem como as etapas de uma requisição DHCP. Além disso, você saberá avaliar as características distintas deste serviço, assim como suas aplicações práticas no contexto de redes.

Aula 05 – Acessos Remotos

- Ideias iniciais de acesso remoto começaram na década de 80.
- PC Anywhere



Fonte: <https://img.informer.com/pa/symantec-pcanywhere-v12.5-main-window-outlook.png> - acessada em 18/05/2023

Camada de Aplicação – O que é Acesso Remoto?



- Capacidade de acessar outro dispositivo à distância, ou outro dispositivo em uma mesma rede de computadores.
- Nem todo acesso remoto é igual ou realizado do mesmo jeito.
- Por que usamos acesso remoto?
- Intensificação por conta da pandemia COVID-19
- É seguro?



- Para um acesso remoto acontecer é necessário três elementos:
 - Software
 - Hardware
 - Conectividade de rede
- A partir da instalação de um programa de acesso é remoto, é possível, executar aplicações, abrir e editar arquivos, mudar configurações de dispositivos, etc.

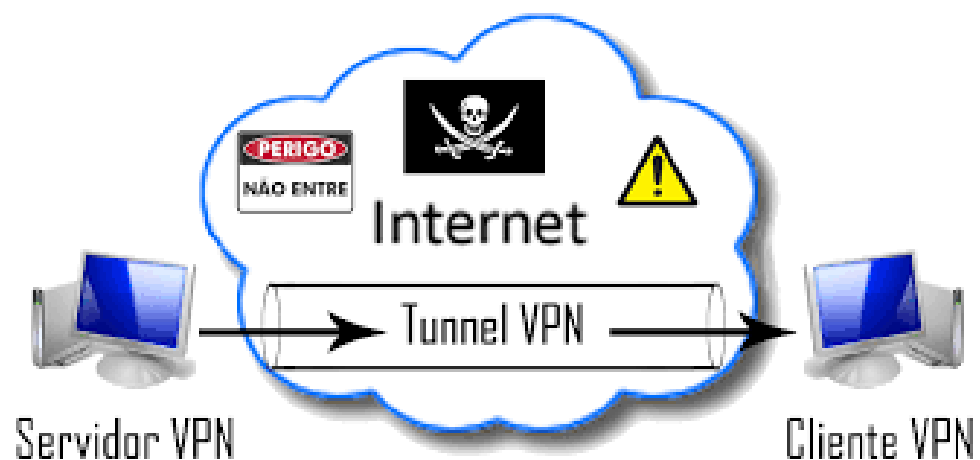


- Podemos encarar o acesso remoto como um “clone funcional” do servidor.
- Há basicamente duas formas de fazer com que a dinâmica aconteça:
 - Conexão de Área de Trabalho Remota
 - Conexão via Virtual Private Network - VPN

Tipos de Acesso Remoto – Conexão de Área de Trabalho Remota

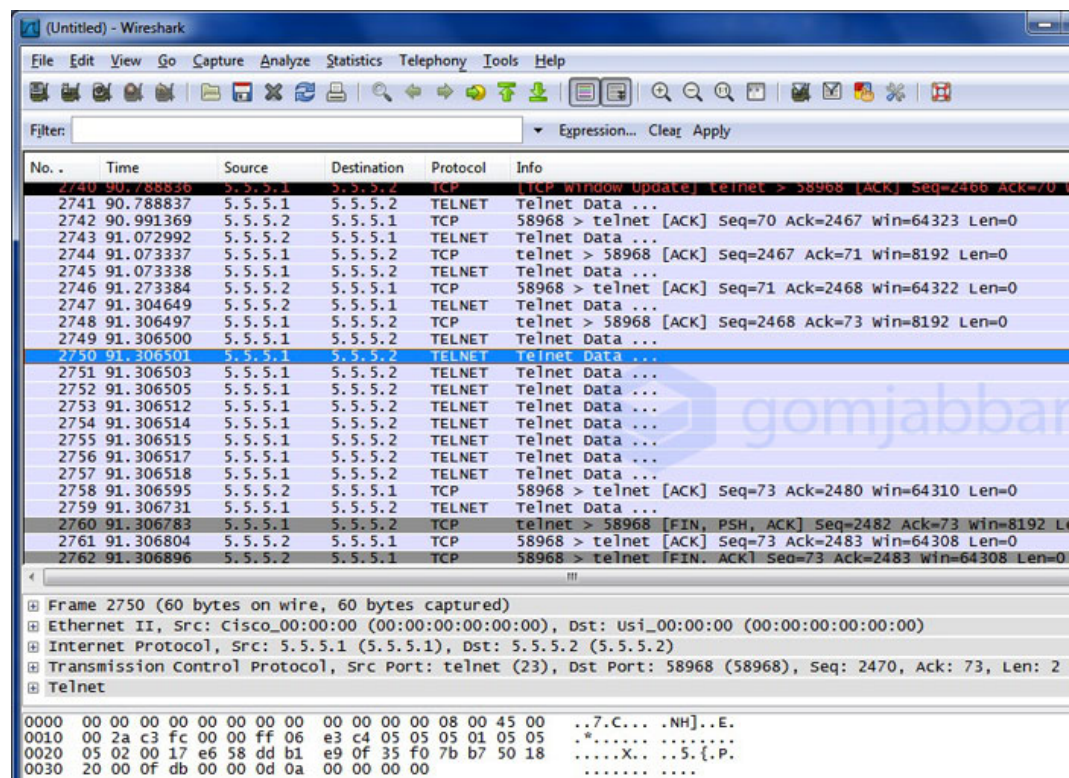


- Tem como base o protocolo Remote Desktop Protocol (RDP) – Microsoft Terminal Services (TS).
- Funciona em sistemas “Não Windows”.
- Porta mais comum utilizada 3389.
- Todos os recursos de hardware e software são compartilhados entre os dispositivos.
- Conexão não criptografada.



- Tipo de conexão por meio de tunelamento e criptografia.
- Diferente do RDP ou TS a VPN é mais segura
- Ponte entre diferentes redes e não entre diferentes dispositivos.
- Permite fazer um acesso para múltiplas conexões.

- Necessidade de muitos serviços a serem executados, para otimização de tempo e espaço o acesso remoto se torna fundamental.
- Configuração, atualização de segurança, instalações.
- Existem diversas ferramentas bem conhecidas para executar acesso remoto:
 - FTP
 - RCP
 - Telnet
 - Rlogin
 - RSH
 - SSH



The image shows a Wireshark packet capture of a Telnet session. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. Packets 2740 through 2762 are visible, showing a sequence of Telnet data and control frames. Packet 2750 is selected, and its details pane is expanded, showing the Ethernet II, Internet Protocol, and Transmission Control Protocol layers. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

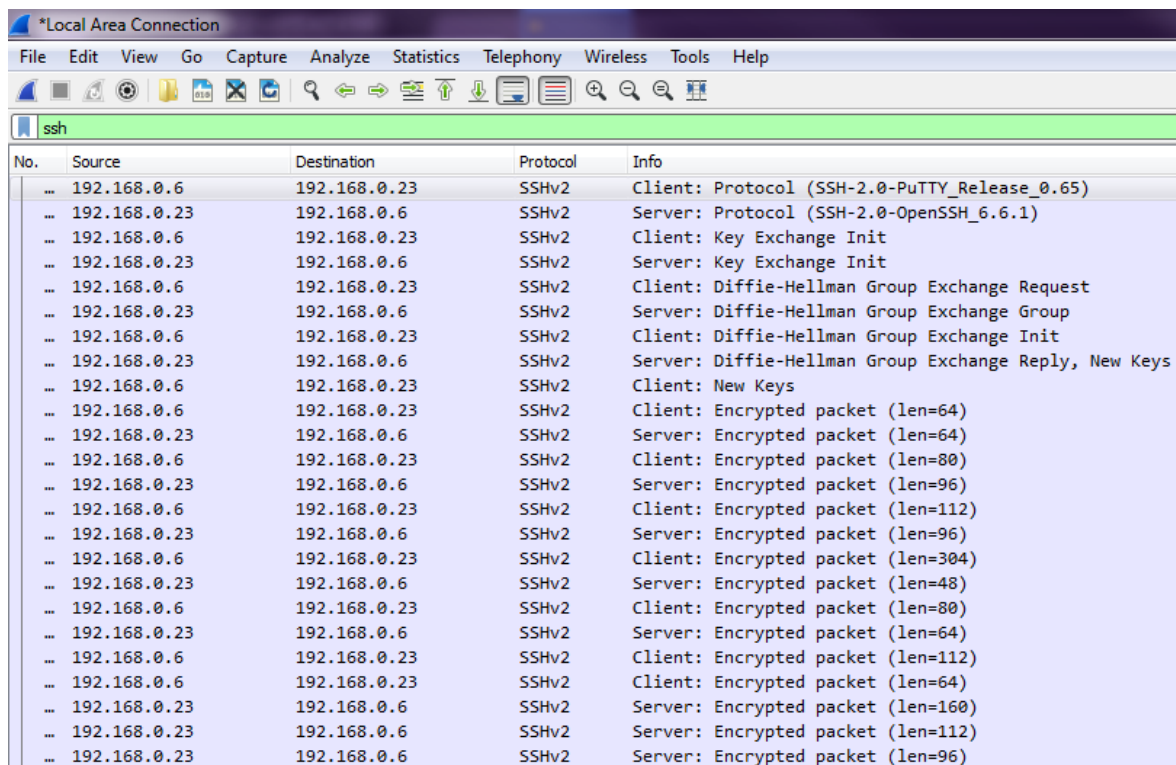
No.	Time	Source	Destination	Protocol	Info
2740	90.788837	5.5.5.1	5.5.5.2	TCP	TCP window update telnet > 58968 [ACK] Seq=2466 Ack=70
2741	90.788837	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2742	90.991369	5.5.5.2	5.5.5.1	TCP	58968 > telnet [ACK] Seq=70 Ack=2467 win=64323 Len=0
2743	91.072992	5.5.5.2	5.5.5.1	TELNET	Telnet Data ...
2744	91.073337	5.5.5.1	5.5.5.2	TCP	telnet > 58968 [ACK] Seq=2467 Ack=71 win=8192 Len=0
2745	91.073338	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2746	91.273384	5.5.5.2	5.5.5.1	TCP	58968 > telnet [ACK] Seq=71 Ack=2468 win=64322 Len=0
2747	91.304649	5.5.5.2	5.5.5.1	TELNET	Telnet Data ...
2748	91.306497	5.5.5.1	5.5.5.2	TCP	telnet > 58968 [ACK] Seq=2468 Ack=73 win=8192 Len=0
2749	91.306500	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2750	91.306501	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2751	91.306503	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2752	91.306505	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2753	91.306512	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2754	91.306514	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2755	91.306515	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2756	91.306517	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2757	91.306518	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2758	91.306595	5.5.5.2	5.5.5.1	TCP	58968 > telnet [ACK] Seq=73 Ack=2480 win=64310 Len=0
2759	91.306731	5.5.5.1	5.5.5.2	TELNET	Telnet Data ...
2760	91.306783	5.5.5.1	5.5.5.2	TCP	telnet > 58968 [FIN, PSH, ACK] Seq=2482 Ack=73 win=8192 Le
2761	91.306804	5.5.5.2	5.5.5.1	TCP	58968 > telnet [ACK] Seq=73 Ack=2483 win=64308 Len=0
2762	91.306896	5.5.5.2	5.5.5.1	TCP	58968 > telnet [FIN, ACK] Seq=73 Ack=2483 win=64308 Len=0

Frame 2750 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_00:00:00 (00:00:00:00:00:00), Dst: usi_00:00:00 (00:00:00:00:00:00)
Internet Protocol, Src: 5.5.5.1 (5.5.5.1), Dst: 5.5.5.2 (5.5.5.2)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 58968 (58968), Seq: 2470, Ack: 73, Len: 2
Telnet

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ..7.C... .NH)..E.
0010 00 2a c3 fc 00 00 ff 06 e3 c4 05 05 05 01 05 05 ..*.....
0020 05 02 00 17 e6 58 dd b1 e9 0f 35 f0 7b b7 50 18X.. .5.{.P.
0030 20 00 0f db 00 00 0d 0a 00 00 00 00

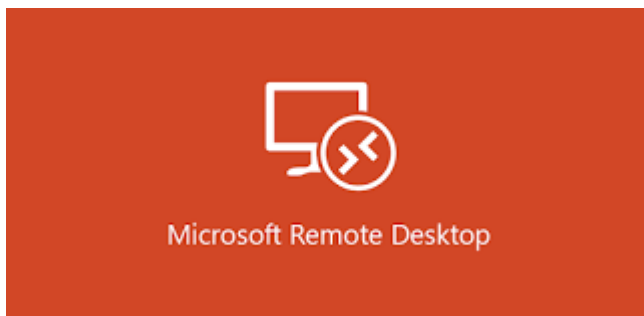
- Abreviação Teletype Network.
- Protocolo de rede na Internet ou rede local, proporciona facilidade de comunicação baseada em texto interativo usando conexão de terminal virtual.
- Porta 23.
- Protocolo de transferência de dados não seguro.

Protocolos de Acesso - SSH



No.	Source	Destination	Protocol	Info
...	192.168.0.6	192.168.0.23	SSHv2	Client: Protocol (SSH-2.0-PuTTY_Release_0.65)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Protocol (SSH-2.0-OpenSSH_6.6.1)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Key Exchange Init
...	192.168.0.23	192.168.0.6	SSHv2	Server: Key Exchange Init
...	192.168.0.6	192.168.0.23	SSHv2	Client: Diffie-Hellman Group Exchange Request
...	192.168.0.23	192.168.0.6	SSHv2	Server: Diffie-Hellman Group Exchange Group
...	192.168.0.6	192.168.0.23	SSHv2	Client: Diffie-Hellman Group Exchange Init
...	192.168.0.23	192.168.0.6	SSHv2	Server: Diffie-Hellman Group Exchange Reply, New Keys
...	192.168.0.6	192.168.0.23	SSHv2	Client: New Keys
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=64)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=64)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=80)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=96)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=112)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=96)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=304)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=48)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=80)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=64)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=112)
...	192.168.0.6	192.168.0.23	SSHv2	Client: Encrypted packet (len=64)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=160)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=112)
...	192.168.0.23	192.168.0.6	SSHv2	Server: Encrypted packet (len=96)

- Abreviação Secure Socket Shell.
- Ênfase em segurança.
- Porta 22.
- Utiliza um conjunto de criptografia de chaves assimétricas.



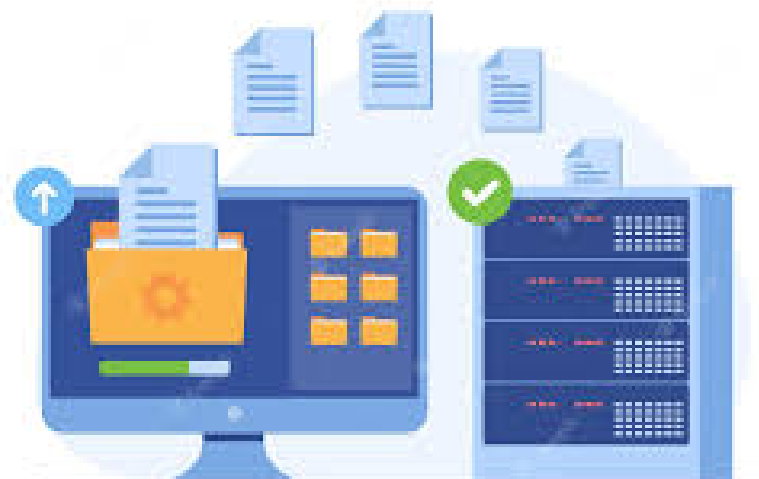
- Softwares de acesso remoto mais utilizados:

- AnyDesk
- KHelpDesk
- LogMeIn Pro
- TeamViewer
- Microsoft Remote Desktop
- Real VNC

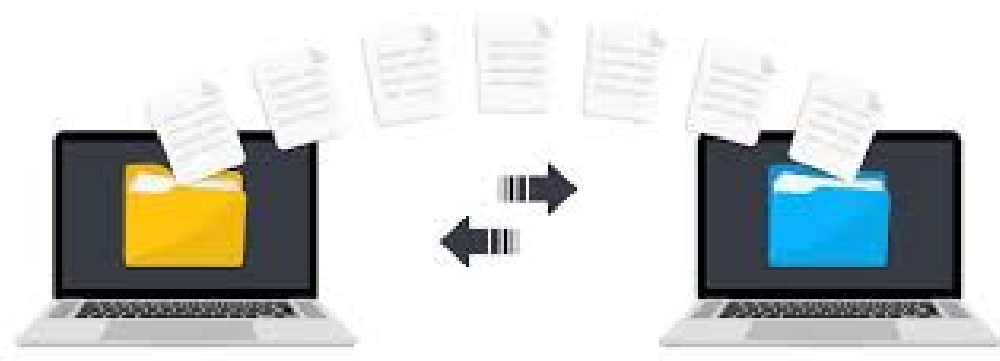
Após completar esta aula, saberá reconhecer e compreender o que é acesso remoto, seu funcionamento bem como algumas das formas de realizar o acesso. Além disso, você saberá identificar a diferença entre VPN e Acesso via Remote Desktop, bem como saberá identificar os principais protocolos de rede destinados a esses serviços.

Aula 06 – Transferência de Arquivos

- Protocolos:
 - SMB/CIFS
 - Torrent
 - FTP
- Servidores e NAS



https://www.valuehost.com.br/blog/wp-content/uploads/2023/05/valuesoftsistemas_valuehosthospedagem_image_760.jpeg.webp - acessada em 18/05/2023



Fonte: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRtwfT5VaPs_qxS8MK455soyUyPtgPCkyM4ljg-Say_TKBGB7MNaW3o7gFL628Z7iPjblU&usqp=CAU – acessada em 18/05/2023



- **Servidor:**
- Computador equipado com alto poder computacional e poder de processamento e armazenamento.
- São escaláveis.
- Podem atuar tanto em LAN quanto em WAN.
- Arquitetura cliente/servidor.
- Vários tipos de servidores.



- **NAS – Network Attached Storage:**
- Exclusiva para guardar e compartilhar arquivos através da rede.
- Backup de dados, executa aplicações, pode ser virtualizado, funciona como servidor de nuvem.
- Não foram inicialmente concebidos para tarefas computacionais.
- Pode suportar milhares de computadores.

Fonte: <https://www.controle.net/novo/assets/img/produtos/foto-nas-storage-com-capacidade-de-5-hds-ts-569-pro.jpg> -
acessada em 18/05/2023

Camada de Aplicação – Servidor ou NAS?



- Conceitualmente um NAS é um servidor.
- NAS possui sistema operacional embarcado e não precisa de um computador host para funcionar, basta estar conectado na LAN.
- Servidores NAS suportam diversos tipos de aplicações.
- Servidores NAS possuem sistemas de segurança como replicação de dados, arquivos podem ser gravados em mais de um destino diferente ao mesmo tempo.

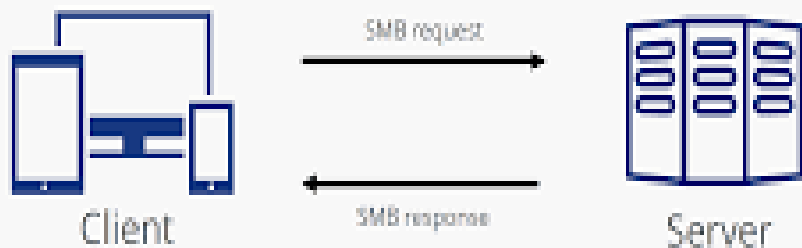
Fonte: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRm4Vu39cd_2Ey0V04rsiGft0QD_D0wFtb5xgrfkW7DTw&s – acessada 18/05/2023



- **SMB** – Server Message Block
- Protocolo que permite pessoas se comunicarem com computadores e servidores remotamente, para usar recursos destes dispositivos.
- Protocolo de compartilhamento de arquivos de rede.
- É utilizado em conjunto com protocolo TCP/IP.
- Protocolo servidor-cliente.
- Utilizava a porta 139, desde o Windows 200 utiliza a porta 445.

Fonte: https://play-lh.googleusercontent.com/iUUVcmJE6gWKe-YISiReNiLeedXOUVaFtqxKZ1eqye5MU3LoQBj_0WK4vzgGRa6EvWY - acessada em 18/05/2023

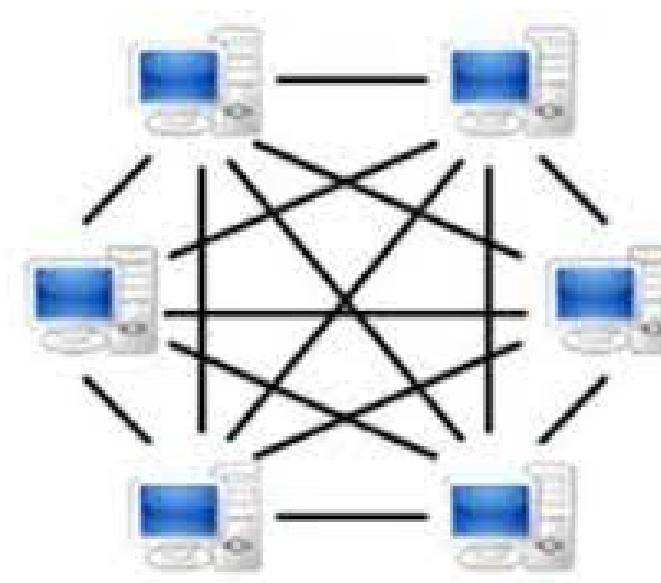
Server Message Block (SMB)



- Conexão entre servidor e cliente.
- SMB permite aos membros utilizar os arquivos compartilhados como se estivessem nos próprios dispositivos.
- Exige um nome de usuário e senha para permitir acesso ao servidor.

- Histórico e variações do SMB:
 - SMBv1
 - CIFS
 - SMBv2
 - SMBv2.1
 - SMBv3
 - SMBv3.02
 - SMBv3.1.1

- Torrent é uma extensão de arquivo, no entanto é apenas compatível com protocolo BitTorrent.
- BitTorrent é responsável por uma grande fatia do tráfego da internet.
- Antes do surgimento do BitTorrent havia apenas o modelo baseado em servidor.
- No modelo P2P todos os computadores são servidores.
- Modelo descentralizado de compartilhamento de arquivos.



Fonte: https://3.bp.blogspot.com/-MikFMAWDZ8s/TcEfyKnAXWI/AAAAAAAAABk/9ddo6AToWJI/s1600/P2P_peer-to_peer.png - acessada 18/05/2023

Transferência de arquivos – Como funciona o Torrent?

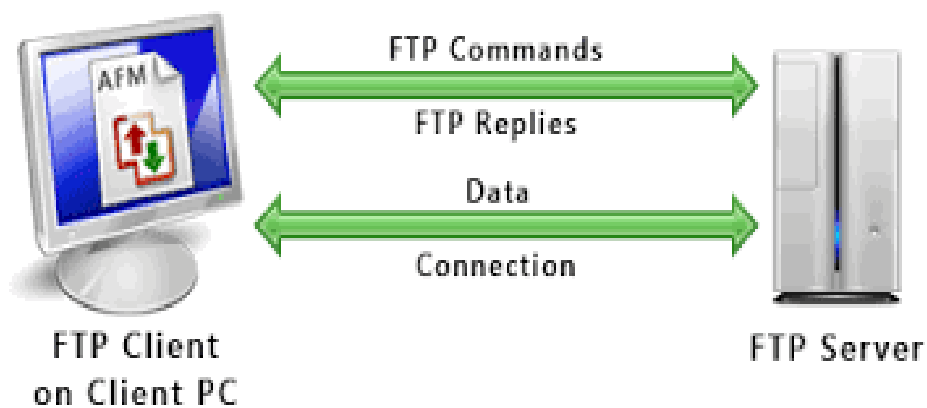
Size	Done	Status	Seeds	Peers	↓ Speed	↑ Speed
339.3...	<div><div></div></div> 61%	Downloading	2 (2)	1 (4)	395.4 k...	0.2 kB/s
9.8 MB	<div><div></div></div>	Seeding	0 (48)	1 (22)		
135.5...	<div><div></div></div>	Seeding	0 (24)	3 (12)		
135.6...	<div><div></div></div> 81%	Stopped	0 (47)	0 (20)		
47.5 MB	<div><div></div></div>	Seeding	0 (116)	5 (15)		
32.7 MB	<div><div></div></div>	Seeding	0 (8)	0 (5)		
41.0 MB	<div><div></div></div> 87%	Stopped	0 (162)	0 (50)		
194.2...	<div><div></div></div>	Seeding	0 (4)	0 (2)		
2.6 GB	<div><div></div></div> 9%	Downloading	20 (54)	0 (12)	1.4 MB/s	1.4 kB/s
636.4...	<div><div></div></div>	Seeding	0 (43)	0 (18)		
95.7 MB	<div><div></div></div> 45%	Stopped	0 (22)	0 (4)		
77.9 MB	<div><div></div></div>	Seeding	0 (176)	0 (48)		
9.8 MB	<div><div></div></div>	Seeding	0 (48)	0 (15)		
500.0	<div><div></div></div> 34%	Downloading	10 (10)	0 (0)	1.0 MB/s	1.0 kB/s

- Ficar atento a 2 termos: seed e peer.
- Seed é todo usuário que está compartilhando um arquivo.
- Peer é todo usuário que está baixando um arquivo.
- No BitTorrent, o usuário pode ser seed e peer ao mesmo tempo.
- Quanto mais mais seeds um download tiver, mais rápido e estável será o download do arquivo.



- FTP – File Transfer Protocol.
- Utiliza canais individuais para comunicação de dados tipo cliente-servidor.
- Porta 21.
- Servidores públicos e privados.

Transferência de arquivos – Como funciona o FTP?

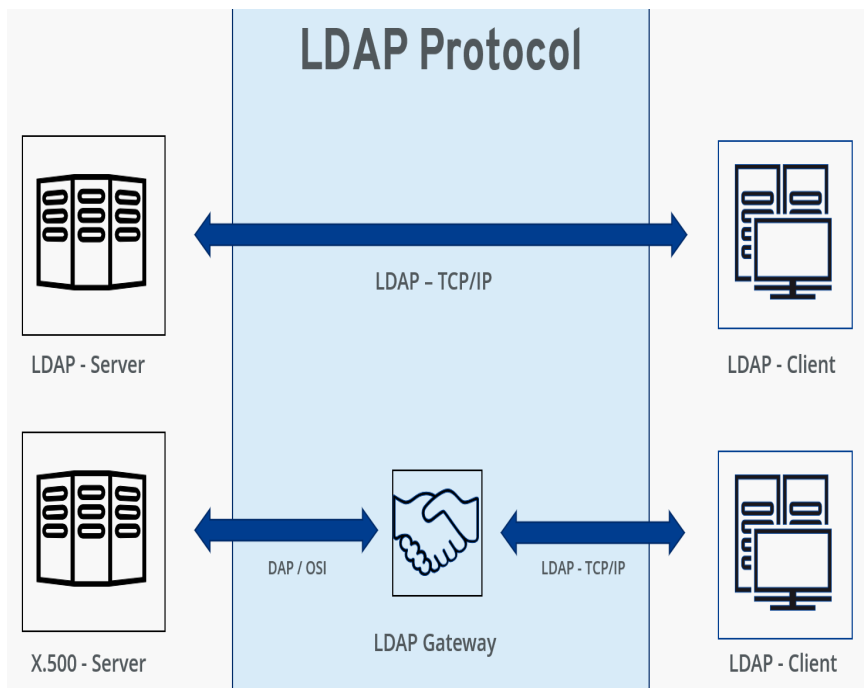


- FTP tradicional é necessário fornecer credencias.
- FTP anônimo não é necessário.
- Dois canais distintos de comunicação para estabelecer conexão:
 - Canal de comando;
 - Canal de dados;
- Modos ativo e passivo.

Após completar esta aula, saberá reconhecer e compreender o que é servidor e transferência de arquivos, e seu funcionamento. Além disso, você saberá identificar os principais protocolos de rede destinados a esses serviços.

Aula 07 – Controle de Usuários

- Primeiras redes locais:
 - Baixo custo, “peer-to-peer”.
 - Conectavam poucos computadores.
 - Não possuíam escalabilidade.
- Com a incorporação do protocolo TCP/IP às redes locais, as redes passaram a “conversar” muito mais entre si.
- Com esse expressivo aumento do uso das redes, exigiu-se que fossem criadas ferramentas para organizar e controlar acesso dos usuários.
- Toda essa demanda levou à criação dos serviços de diretório.
- O que são serviços de diretório?
 - LDAP



- **LDAP:**

- Lightweight Directory Access Protocol
- Versão mais “leve” do Directory Access Protocol(DAP).

- **Onde usamos o LDAP?.**

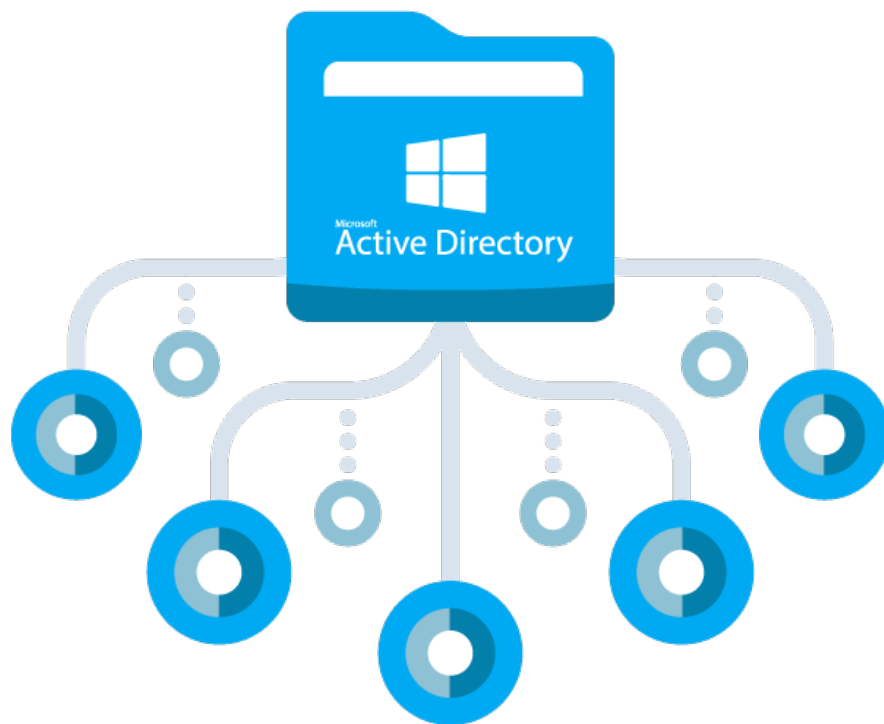
- Centralização de autenticação de usuários de uma rede.
- Usado principalmente no Active Directory da Microsoft.

- **Para que serve o LDAP?**

- Permite que organizações armazenem, enderecem, gerenciem e protejam informações.
- Serve como um local central para armazenar informações de autenticação, como nomes de usuários, privilégios e senhas.



- **Estrutura organizada como se fosse uma “árvore”:**
 - Um diretório raiz;
 - Países;
 - Organizações;
 - Unidades organizacionais;
 - Indivíduos
- Um diretório LDAP pode ser distribuído entre vários servidores.



- Microsoft Active Directory – serviço de diretório para gerenciamento de domínios, usuários e recursos distribuídos.
- Contém informações sobre cada conta de usuário de toda a rede.
- O LDAP pode armazenar e extrair objetos, como nomes de usuário e senhas no AD.

2600	18.328594	10.83.131.35	10.190.240.3	CLDAP	189 searchRequest(87) "<ROOT>" baseObject
2601	18.337558	10.190.240.3	10.83.131.35	CLDAP	218 searchResEntry(87) "<ROOT>" searchResDone(87) success [1 result]

Fonte: do autor – 18/05/2023

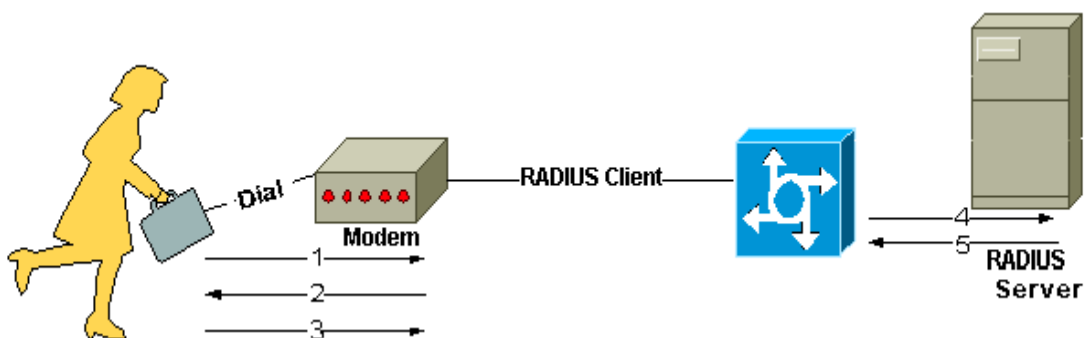
- 1 – O usuário(10.83.131.35) tenta conectar-se à rede.
- 2 – É realizada uma requisição de autenticação ao servidor (10.190.240.3).
- 3 – O servidor então requisita dados de login e senha para que sejam consultados no banco de dados e ai poder ser autenticado o acesso e suas permissões.
- 4 – Após realizada a autenticação o servidor(10.190.240.3) responde para o usuário(10.83.131.35) com uma “entrada” e um sucesso na realização de autenticação.
- 5 – O usuário pode normalmente acessar à rede com suas respectivas permissões.



Fonte: <https://www.shutterstock.com/image-photo/radius-protocol-implementing-authentication-260nw-1912844740.jpg> - acessada em 18/05/2023

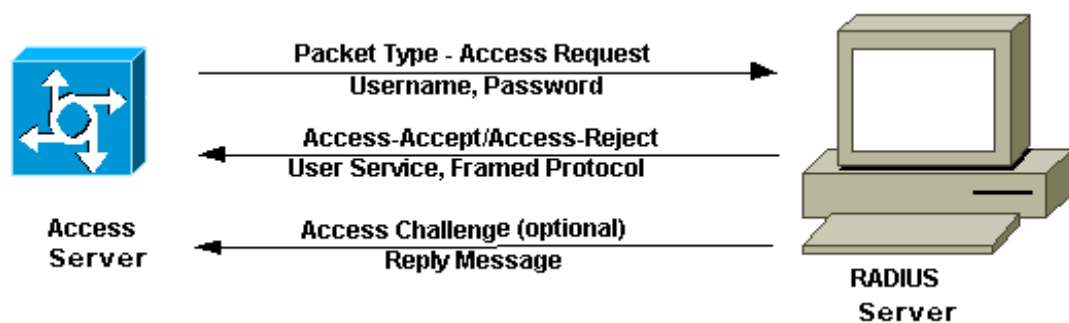
- **Remote Authentication Dial in User Service (RADIUS).**
- Desenvolvido pela Livingston Enterprises Inc em 1991.
- Protocolo que fornece gerenciamento centralizado de AAA (Autenticação, Autorização e Contabilização(Accounting)).
- Incorporado em outros protocolos como acesso wireless, VPN, servidores web entre outros.

Controle de Usuários – Como funciona o RADIUS?



<https://www.cisco.com/c/dam/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32-00.png> - acessada em 18/05/2023

- Protocolo do tipo cliente/servidor.
- Normalmente é um processo de background.
- Servidor RADIUS possui 3 funções básicas:
 - Autenticação
 - Autorização
 - Contabilização



Fonte: <https://www.cisco.com/c/dam/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32-01.png> - acessada em 18/05/2023

- Servidor RADIUS pode suportar vários métodos de autenticação do usuário.
- Normalmente o processo consiste em:
 - Consulta do NAS ao servidor RADIUS (Access-Request);
 - Resposta do servidor (Access-Accept ou Reject);
- Em sua concepção a porta UDP do RADIUS era a 1645, depois atualizada para porta 1812

Após completar esta aula, saberá reconhecer e compreender o que é o controle de usuários, seu surgimento e seu funcionamento. Além disso, você saberá identificar os principais protocolos de rede e funcionamento como LDAP e RADIUS destinados a esse serviço.

Aula 08 – Gerenciamento e Monitoramento de dispositivos

- Gerenciamento e monitoramento de dispositivos, surgiram nas décadas de 1960 e 1970.
- Surgimento de protocolos como SNMP, NTP e SYSLOG.
- Os protocolos de gerenciamento e monitoramento desempenham papel estratégico no mundo da tecnologia da informação.

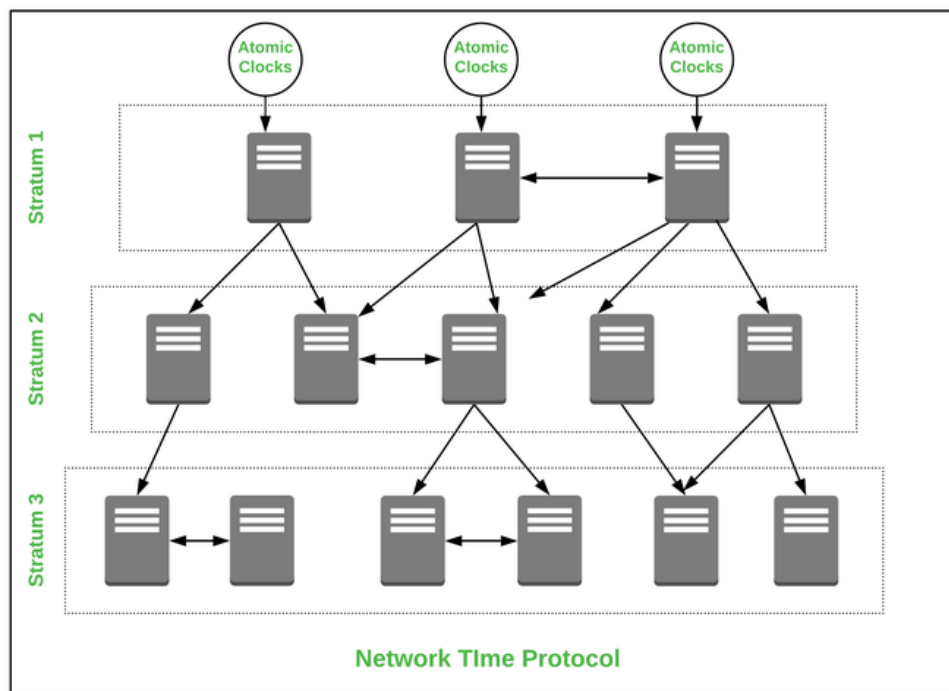


- **SNMP:**
 - Simple Network Management Protocol
 - Coleta, organiza e envia dados de elementos de uma rede IP.
 - Possui 3 versões, onde a V3 é a mais atual.
- **Onde usamos o SNMP e qual sua função?**
 - Monitoramento e desempenho.
 - Detecção e resolução de problemas.
 - Configuração de dispositivos.
 - Notificação de eventos.



Fonte: <https://vinasupport.com/uploads/2022/05/NTP.png> - acessada em 18/05/2023

- **NTP:**
 - Network Time Protocol
 - Sincronização de relógios dos dispositivos da rede.
 - Sensibilidade de softwares e aplicações ao sincronismo de relógios.
- **Onde usamos o NTP e qual sua função?**
 - Obter informações de tempo de um determinado servidor.
 - Disciplinar o relógio local.
 - Escolher dentre vários servidores qual oferece o tempo correto.
 - Topologia simples e confiável.



- Formam uma topologia hierárquica dividida em camadas/estratos.
- Possui diferentes tipos de associações.
- Cliente-Servidor.
- Modo Simétrico.
- Broadcast ou Multicast.

Fonte: <https://media.geeksforgeeks.org/wp-content/uploads/20210111195037/NTP-660x480.png>
acessada em 18/05/2023



Fonte: <https://hassets.paessler.com/common/files/graphics/glossary/syslog.png> - acessada em 18/05/2023

- **SYSLOG:**
 - System Logging Protocol.
 - Armazenar mensagens de eventos do sistema.
- **Onde usamos o SYSLOG e qual sua função?**
 - Monitoramento
 - Solução de Problemas.
 - Segurança.
 - Conformidade.
 - Análise e Planejamento.



- Geração de Eventos
- Envio para o Servidor SYSLOG.
- Formato de Mensagem.
- Armazenamento e Análise.

Fonte: <https://hassets.paessler.com/common/files/graphics/glossary/syslog.png> - acessada em 18/05/2023

Após completar esta aula, saberá reconhecer e compreender o que é o gerenciamento e monitoramento de dispositivos, seu surgimento e seu funcionamento. Além disso, você saberá identificar os principais protocolos de rede e funcionamento como SNMP, NTP e SYSLOG destinados a esse serviço.

