



UnISENAI

O FUTURO COMEÇA
POR VOCÊ!

Proposta para essa UC

Definir com será as atividades, temos 2 opções:

Opção A:

- Na última turma, frisamos o uso de laboratórios
- Demonstrações práticas dos serviços de rede
- Demonstrações práticas dos software ref. a UC
- Propostas de topologias e atividades práticas para exemplificar e demonstrar de forma visual o conteúdo da UC
- Tira duvidas no momentos sincronos.

Opção B:

- Professor palestrinha, não legal...
- Slides e tira duvidas.

Para opção A:

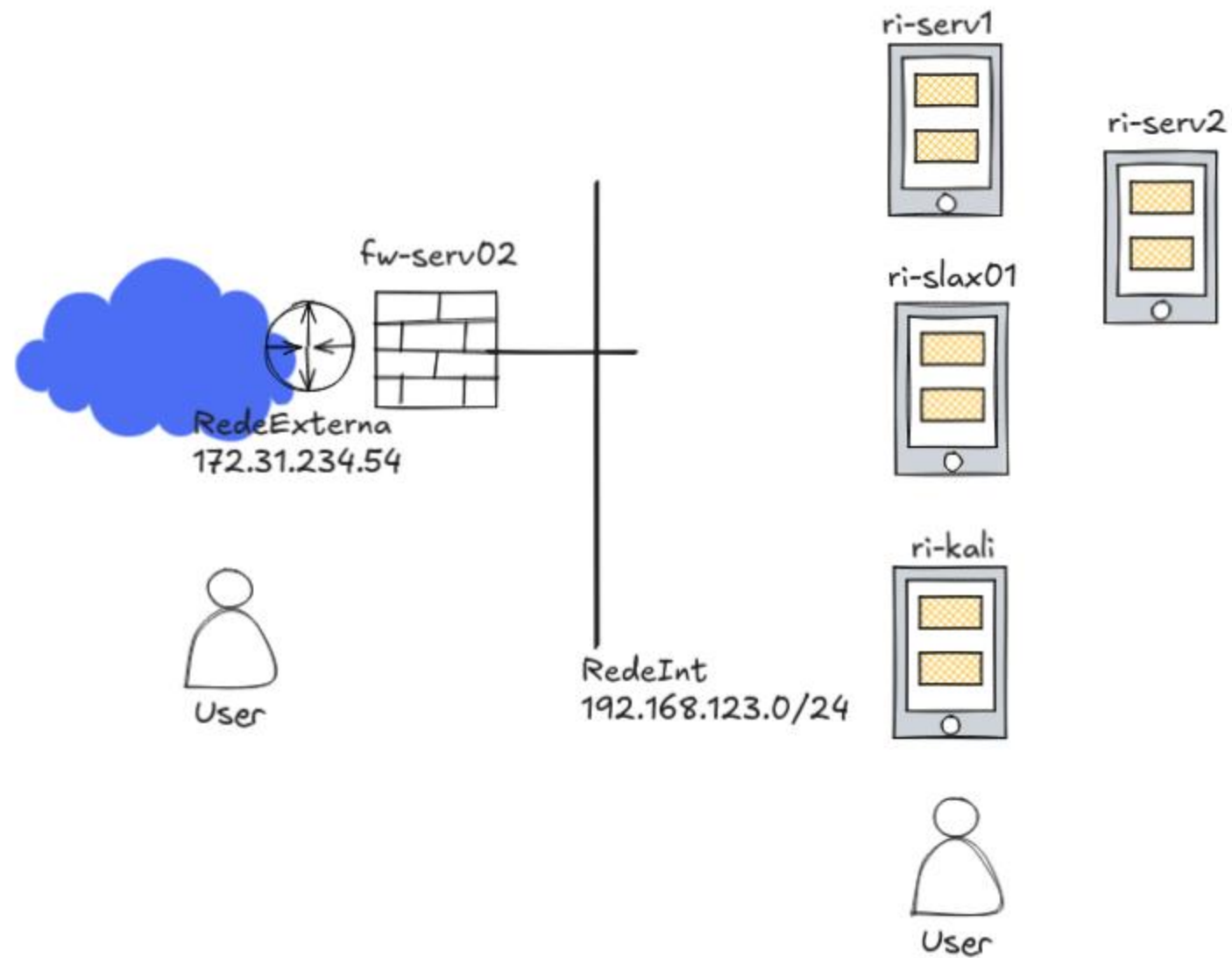
Montarei um github com as informações das aulas, e como será o laboratório. Junto com um cenário proposto condizente com o conteúdo e o que o mercado está solicitando.

Nos primeiro 50% (aprox 15 dias), desenvolver todos os serviços SEM CRIPTOGRAFIA e analisar o "treco".

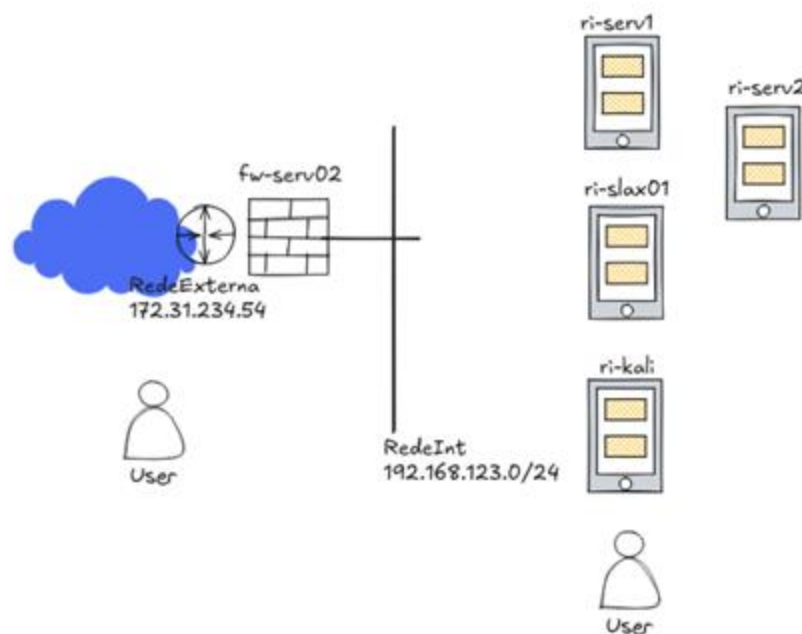
Nos ultimos 50% (aprox prox 15 dias), reconfigurar todos os serviços anteriores e ativar/configurar a criptografia.

E no fim, comparar e ver as diferenças entre eles. E quem

Exemplo:



E aqui começa a nossa conversa... WTF é esse desenho?

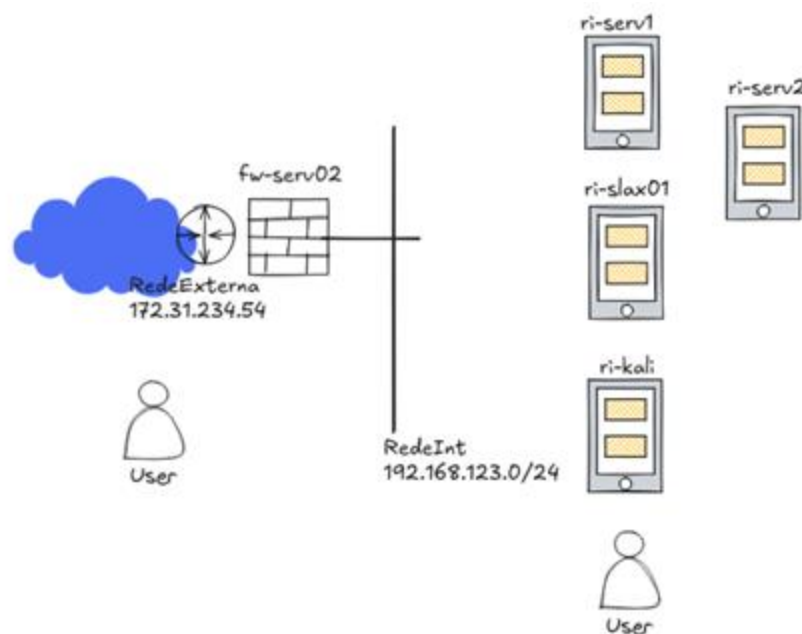


WTF é essa da bagaça?:

- 2x Servidores ri-serv1 e ri-serv2:
 - Utilizam Ubuntu Server.
 - Estão em modo DHCP e conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM e disco de até 10 GB (modo thin provision).
- 1x Servidor de Firewall fw-serv02-
 - Utiliza Debian Server.
 - Possui duas placas de rede: uma em modo bridge e outra conectada à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM e disco de até 5 GB (modo thin provision).
- 1x Servidores ri-slax01:
 - Utilizam uma distro live CD (Slax) e estão conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM, e disco de até 10 GB (modo thin provision).
 - Eles carregam uma imagem ISO do Slax como Live CD.
- 1x Servidores ri-kali:
 - Utilizam uma distro live CD (Kali) e estão conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM, e disco de até 10 GB (modo thin provision).
 - Eles carregam uma imagem ISO do Kali como Live CD.

Vou precisar de um datacenter ?

E aqui começa a nossa conversa... WTF é esse desenho?



WTF é essa da bagaça?:

- 2x Servidores ri-serv1 e ri-serv2:
 - Utilizam Ubuntu Server.
 - Estão em modo DHCP e conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM e disco de até 10 GB (modo thin provision).
- 1x Servidor de Firewall fw-serv02-
 - Utiliza Debian Server.
 - Possui duas placas de rede: uma em modo bridge e outra conectada à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM e disco de até 5 GB (modo thin provision).
- 1x Servidores ri-slax01:
 - Utilizam uma distro live CD (Slax) e estão conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM, e disco de até 10 GB (modo thin provision).
 - Eles carregam uma imagem ISO do Slax como Live CD.
- 1x Servidores ri-kali:
 - Utilizam uma distro live CD (Kali) e estão conectados à "RedeInterna".
 - Configuração de 2 CPUs, 2048 MB de RAM, e disco de até 10 GB (modo thin provision).
 - Eles carregam uma imagem ISO do Kali como Live CD.

Não, vou compartilhar para usar
virtualbox com o min de ram necessária.
Posso fazer na
AWS/Vmware/Proxmox/OCI/Azure/ na
casa do chapéu? Sim, fique a vontade
desde que desenvolva as atividades.

Nuvem de tags:

Roteadores ?

Switches ?

HUB deve morrer ?

TCP/IP ?

DNS ?

FDP ?

FTP ?

HTTP ?

FIREWALL Camada 3/4/7 ? UTM ?

NGFW?

Nuvem ? OCI ? AWS ? Azure?

Ponto a ponto ?

Cliente - Servidor ?

Topologias ? Barramento ? Anel (lá ele)?

Estrela ? Malha?

Topologias físicas ?

Topologias lógicas ?

Por que utilizamos as camadas do modelo OSI e TCP ?

DHCP ? XYZ ?

Mais de 1 milhão de acrónimos...

Se quiser conversar sobre algum, é só perguntar.

Camada	Principais funções
Aplicação	Funções específicas para as aplicações dos usuários: transferência de páginas <i>web</i> ; transferência de arquivos pela rede; envio ou recebimento de correio eletrônico; terminal remoto; etc. Funções especializadas para o sistema: transferência de informações sobre caminhos entre roteadores; serviço de gerenciamento de equipamentos de rede; serviço de tradução de nomes; etc.
Apresentação	Conversão e formatação dos dados.
Sessão	Negociação e conexão entre as máquinas envolvidas.
Transporte	Transporte de dados fim a fim. Fornece um caminho virtual transparente entre um processo em uma máquina da rede com outro processo em alguma outra máquina.
Rede	Encaminhamento (roteamento) de pacotes pelas várias redes.
Enlace	Deteção e correção de erros do meio de transmissão.
Física	Transmissão e recepção dos <i>bits</i> brutos através do meio de transmissão.

<https://gsuite.tools/traceroute>

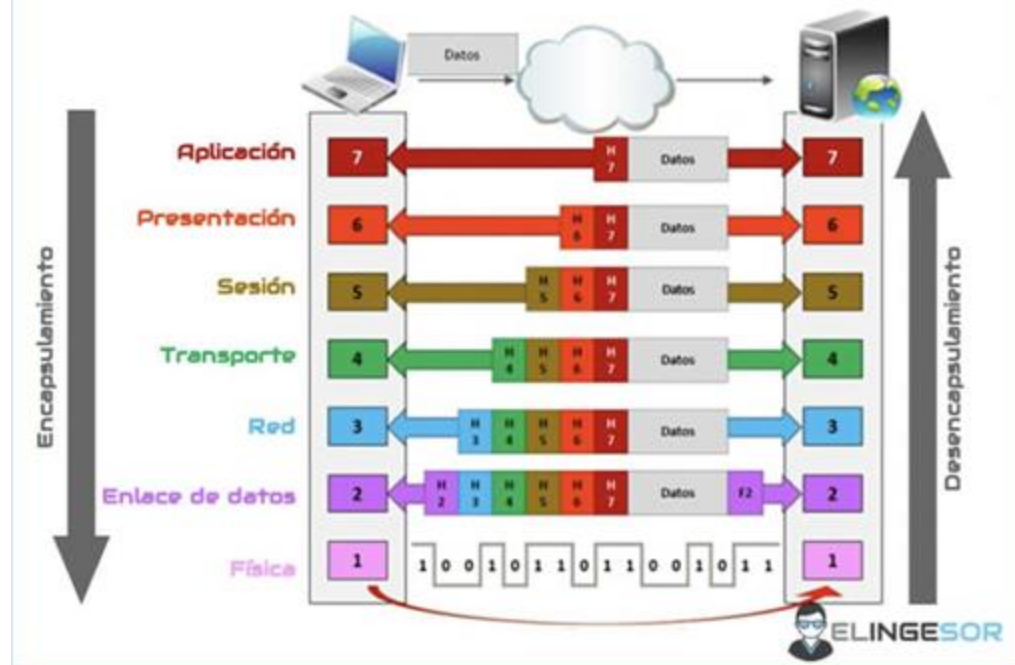
<https://www.ipvoid.com/ip-to-google-maps/>

<https://www.geolocation.com/>

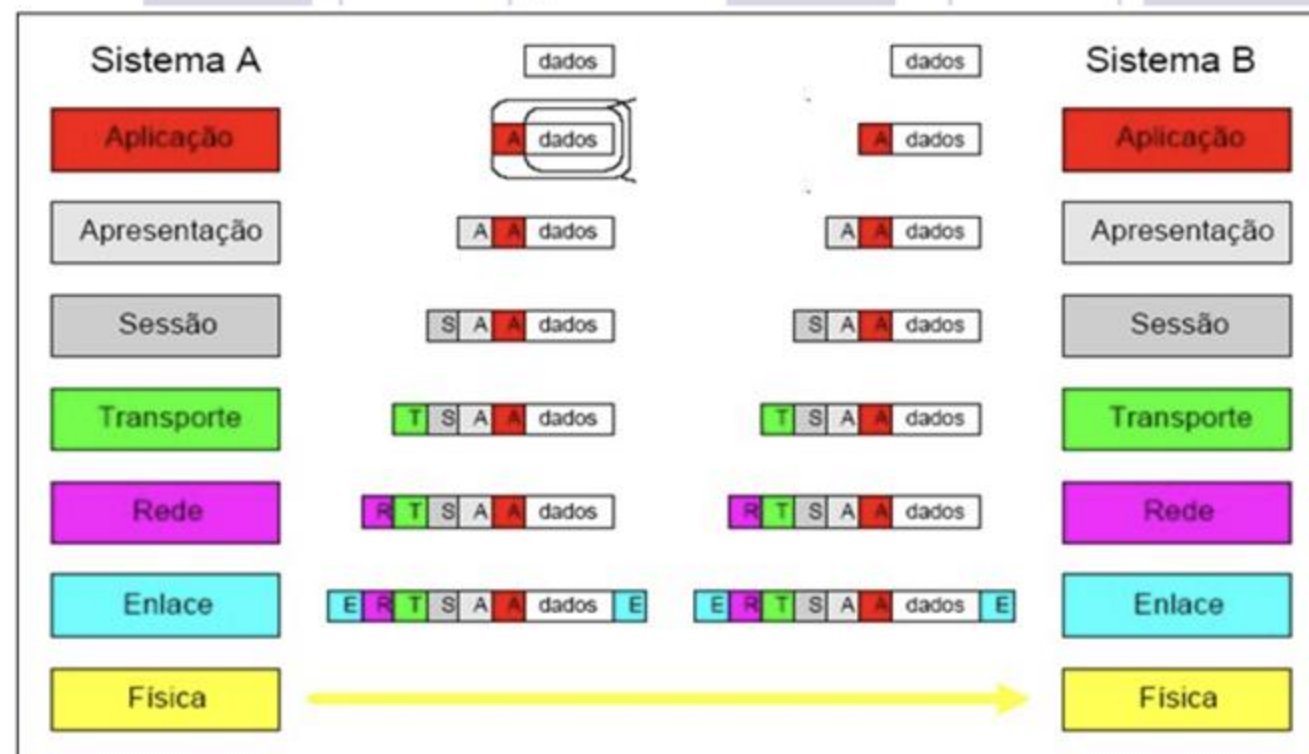
<https://www.ip-tracker.org/>

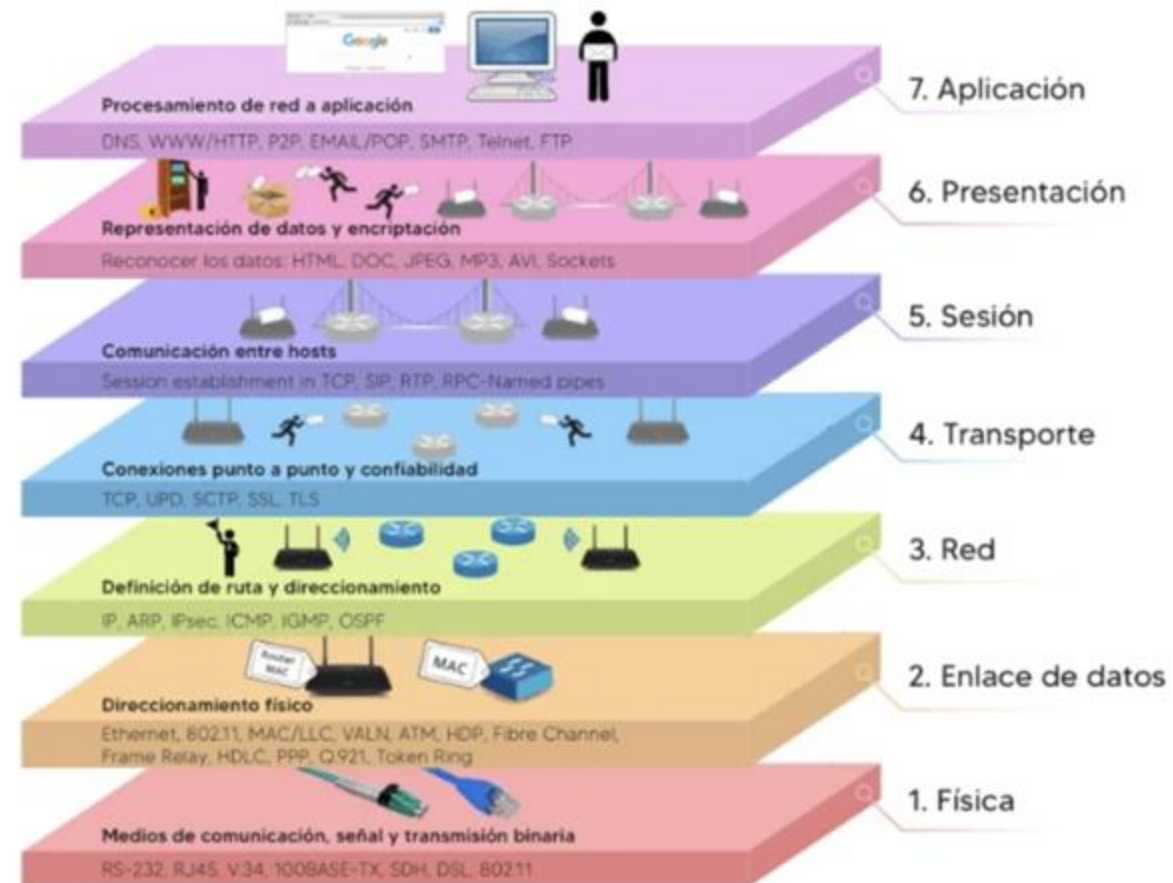
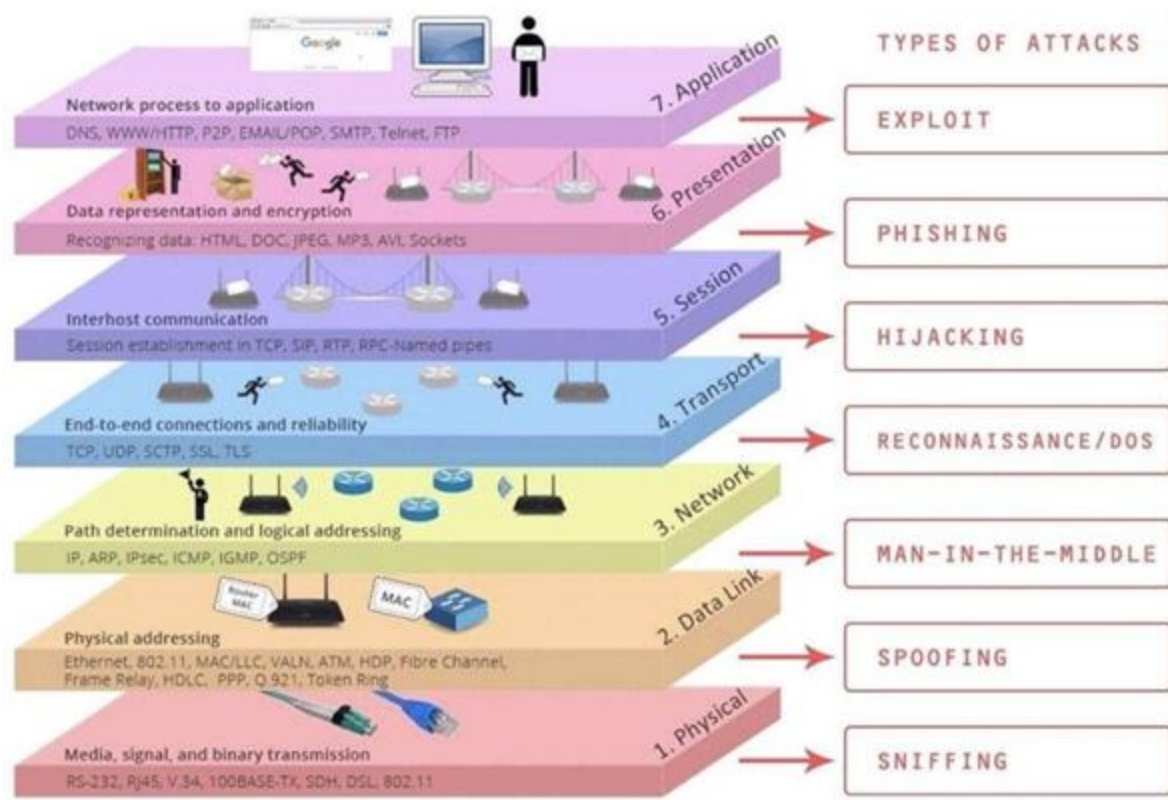


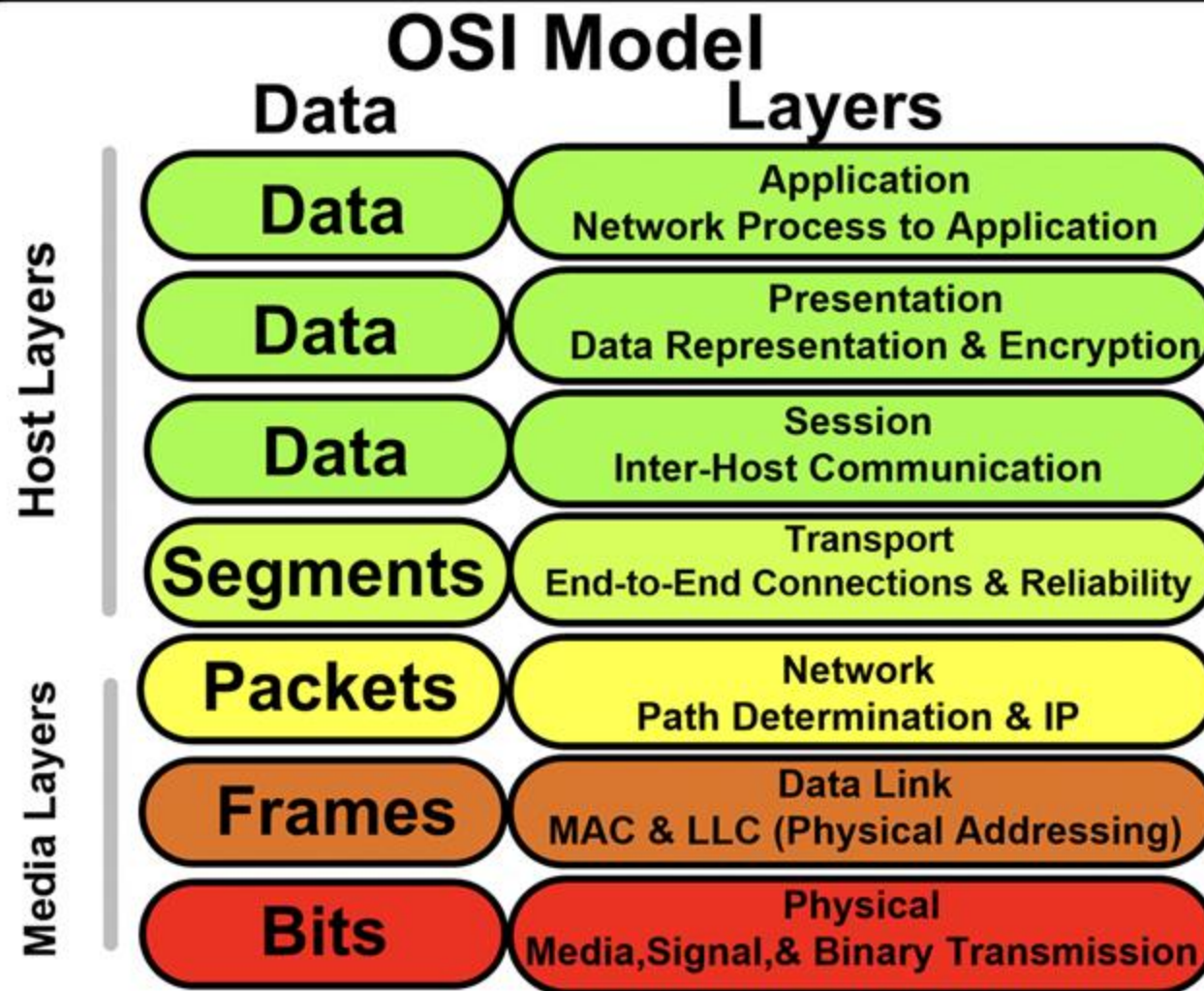
Encapsulamiento OSI



Encapsulamiento de Datos







E temos que também falar da história da criptografia...

Início da Civilização (3000 a.C.)

Nossa jornada começa no Egito Antigo, onde os faraós precisavam proteger suas mensagens secretas. Eles desenvolveram uma das primeiras formas de criptografia, conhecida como "substituição de letras". Eles substituíam letras por símbolos ou hieróglifos para criar mensagens codificadas. Além disso, os egípcios também usavam a "cifra de transposição", que consistia em reorganizar as letras de uma mensagem para criar um código.

- Exemplos:

- A "cifra de substituição" foi usada para proteger mensagens secretas entre os faraós e seus generais.
- A "cifra de transposição" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

E temos que também falar da história da criptografia...

Grécia Antiga (500 a.C.)

À medida que a civilização grega crescia, a criptografia se tornou mais sofisticada. Os gregos desenvolveram a "cifra de César", que consistia em substituir cada letra por uma letra três posições à frente no alfabeto. Essa técnica foi usada por Júlio César para enviar mensagens secretas aos seus generais. Além disso, os gregos também usavam a "cifra de substituição polialfabética", que consistia em usar múltiplos alfabetos para criar um código mais seguro.

- Exemplos:

- A "cifra de César" foi usada por Júlio César para enviar mensagens secretas aos seus generais.

- A "cifra de substituição polialfabética" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

E temos que também falar da história da criptografia...

Idade Média (500 d.C.)

Durante a Idade Média, a criptografia se tornou mais complexa. Os alquimistas e os monges desenvolveram técnicas de criptografia baseadas em símbolos e códigos. A "cifra de Vigenère" foi desenvolvida nesse período, usando uma série de letras para criar um código mais seguro. Além disso, os monges também usavam a "cifra de substituição monográfica", que consistia em substituir cada letra por um símbolo ou imagem.

- Exemplos:

- A "cifra de Vigenère" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

- A "cifra de substituição monográfica" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

E temos que também falar da história da criptografia...

Renascimento (1500 d.C.)

Com o Renascimento, a criptografia se tornou mais científica. Matemáticos como Girolamo Cardano e Blaise de Vigenère desenvolveram novas técnicas de criptografia. A "cifra de Vigenère" se tornou uma das mais populares e foi usada por séculos. Além disso, os matemáticos também desenvolveram a "cifra de substituição polinomial", que consistia em usar polinômios para criar um código mais seguro.

- Exemplos:

- A "cifra de Vigenère" foi usada por séculos para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

- A "cifra de substituição polinomial" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

E temos que também falar da história da criptografia...

Era Moderna (1900 d.C.)

No século XX, a criptografia se tornou mais complexa e sofisticada. A invenção do computador permitiu a criação de algoritmos de criptografia mais avançados. A "cifra de Enigma" foi desenvolvida pelos alemães durante a Segunda Guerra Mundial e foi considerada inquebrável. Além disso, os cientistas também desenvolveram a "cifra de bloco", que consistia em dividir a mensagem em blocos e criptografar cada bloco separadamente.

- Exemplos:

- A "cifra de Enigma" foi usada pelos alemães durante a Segunda Guerra Mundial para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.
- A "cifra de bloco" foi usada para criar mensagens codificadas que só podiam ser decifradas por aqueles que conheciam a chave.

E temos que também falar da história da criptografia...

Era Digital (1970 d.C.)

Com a chegada da era digital, a criptografia se tornou mais acessível e amplamente usada. A invenção da criptografia de chave pública, como o RSA, permitiu que as pessoas criptografassem mensagens sem precisar compartilhar a chave secreta. Além disso, os cientistas também desenvolveram a "cifra de fluxo", que consistia em criptografar a mensagem em tempo real, à medida que ela era transmitida.

- Exemplos:

- O RSA foi usado para criar sistemas de criptografia de chave pública que permitiam que as pessoas criptografassem mensagens sem precisar compartilhar a chave secreta.

- A "cifra de fluxo" foi usada para criar sistemas de criptografia em tempo real que permitiam que as mensagens fossem criptografadas à medida que eram transmitidas.

E temos que também falar da história da criptografia...

Desenvolvimentos Recentes (2000 d.C.)

Nos últimos anos, a criptografia continuou a evoluir e se adaptar às novas tecnologias e ameaças. A invenção da criptografia quântica permitiu que as pessoas criptografassem mensagens de forma mais segura e eficiente. Além disso, os cientistas também desenvolveram a "cifra de homomorfismo", que permitia que as operações fossem realizadas em dados criptografados sem precisar decifrar a mensagem.

- Exemplos:

- A criptografia quântica foi usada para criar sistemas de criptografia mais seguros e eficientes que permitiam que as mensagens fossem criptografadas de forma mais segura.
- A "cifra de homomorfismo" foi usada para criar sistemas de criptografia que permitiam que as operações fossem realizadas em dados criptografados sem precisar decifrar a mensagem.

E temos que também falar da historia da criptografia...

Aplicações Atuais (2023 d.C.)

Hoje em dia, a criptografia é usada em todos os aspectos da vida digital. Desde a segurança online até as transações financeiras, a criptografia é fundamental para proteger a privacidade e a segurança dos dados. Além disso, a criptografia também é usada em aplicações como:

- Criptomoedas: A criptografia é usada para criar sistemas de criptomoedas que permitam que as transações sejam realizadas de forma segura e eficiente.
- Segurança de rede: A criptografia é usada para criar sistemas de segurança de rede que protejam as comunicações online.
- Proteção de dados: A criptografia é usada para proteger os dados armazenados em dispositivos e servidores.
- Exemplos:
 - A criptografia é usada em sistemas de criptomoedas como o Bitcoin para proteger as transações.
 - A criptografia é usada em sistemas de segurança de rede como o SSL/TLS para proteger as comunicações online.
 - A criptografia é usada em sistemas de proteção de dados como o AES para proteger os dados armazenados em dispositivos e servidores.

Unit	Gigabit Interfaces																							
1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
Unit	Gigabit Interfaces																							
2	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

Vlan ID	Descrição	IP	Classe de IP	Range DHCP	Port Channel	Interfaces	
447	VlanCorporativa	172.18.254.141	172.18.41.0/22	172.18.41.50-250			
446	VlanDiretoria		192.168.230.0/24	192.168.230.50-250			
445	VlanVisitante		192.168.231.0/24	192.168.231.50-250			
254	Gerencia Equipamentos	172.18.254.1					
250	Servidores	10.0.0.28					
122	Farmacia Manipulação		172.18.22.0/22	172.18.22.10-200	22	Gi1/0/22	Gi2/0/22
121	Farmacia XV		172.18.21.0/22	172.18.21.10-200	21	Gi1/0/21	Gi2/0/21
120	Varejo Matriz		172.18.20.0/22	172.18.20.10-200	20	Gi1/0/20	Gi2/0/20
119	Switch Cobranca	172.18.254.119	172.18.19.0/22	172.18.19.10-200	19	Gi1/0/19	Gi2/0/19
118	Switch Contabilidade	172.18.254.118	172.18.18.0/22	172.18.18.10-200	18	Gi1/0/18	Gi2/0/18
117	Switch Desenvolvimento Sistemas	172.18.254.117	172.18.17.0/22	172.18.17.10-200	17	Gi1/0/17	Gi2/0/17
116	Switch Diretoria	172.18.254.116	172.18.16.0/22	172.18.16.10-200	16	Gi1/0/16	Gi2/0/16
115	Switch RH	172.18.254.115	172.18.15.0/24	172.18.15.10-200	15	Gi1/0/15	Gi2/0/15
114	Compras Terreo	172.18.254.114	172.18.14.0/24	172.18.14.10-200	14	Gi1/0/14	Gi2/0/14
113	Compras 1o. Andar	172.18.254.113	172.18.13.0/24	172.18.13.10-200	13	Gi1/0/13	Gi2/0/13
112	Patrimônio	172.18.254.112	172.18.12.0/24	172.18.12.10-200	12	Gi1/0/12	Gi2/0/12
111	Vlan Corporativa WIFI		172.18.11.0/24	172.18.11.10-200	11	Gi1/0/11	Gi2/0/11
110	TI	172.18.254.110	172.18.10.0/24	172.18.10.10-200	10	Gi1/0/10	Gi2/0/10
	Sem configuração definida						

