E-fólio B | Instruções para a realização do E-fólio

SISTEMAS EM REDE | 21106

A preencher pelo estudante

UNIDADE CURRICULAR: Sistema de Rede

CÓDIGO: 21106

DOCENTE: Arnaldo Santos

NOME: Ivo Vieira Baptista

N.º DE ESTUDANTE: 2100927

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 04 de Janeiro de 2023

TRABALHO / RESOLUÇÃO:

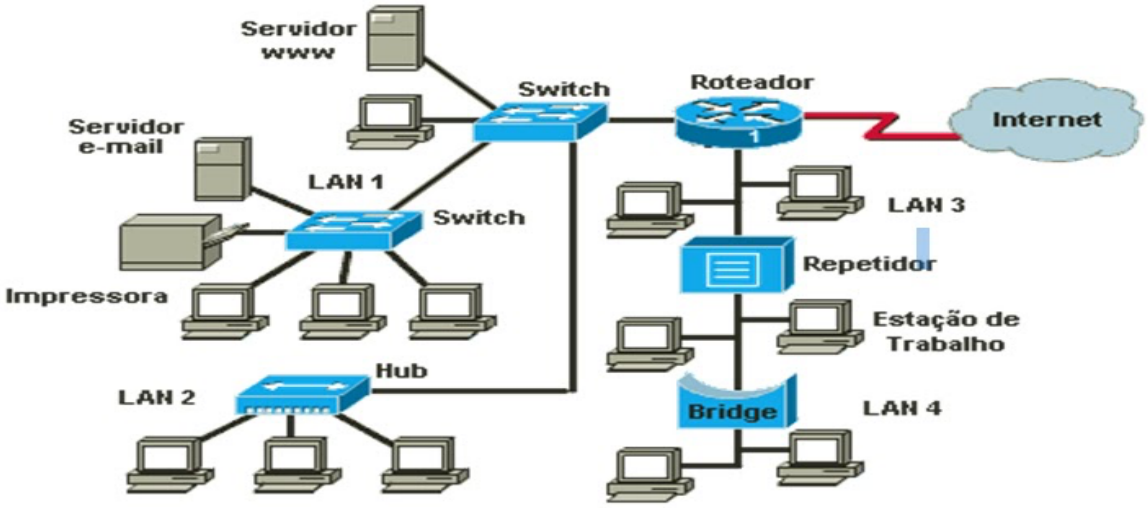
Resposta nª1)

LAN, abreviado significa "***Local Area Network***", e em português rede de área local ou simplesmente Rede Local. LAN é frequente em casa, em escritórios e empresas pequenas, por exemplo, é utilizada para conectar pequenas áreas ou localidades, como num edifício campos ou mesmo numa residência, salas de aula, etc. são o tipo de rede mais comuns. Uma LAN possui uma rede de baixa qualidade e com uma limitação pequena em relação ao seu alcance. A sua característica principal é ser uma rede privativa, isto quer dizer que (uma pessoa ou organização) controla essa rede e o acesso a ela, em uma área geográfica limitada.

Por outro lado:

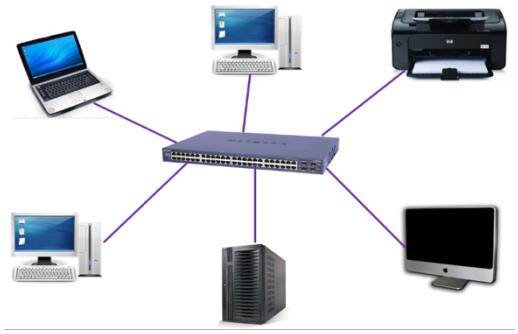
WAN, em abreviado significa "***Wide Area Network*** " que significa em português "***Área Longa de Contato*** " quer dizer que WAN conecta vários dispositivos e equipamentos eletrônicos como: Computador, Smart TV, Smartphones e Notebook. É essencial no nosso dia a dia.

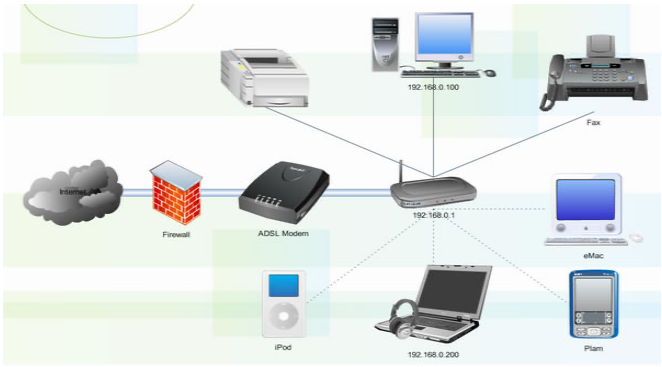
A Configuração de uma rede WAN é empregada para estabelecer conexão em longas localidades ou áreas, sendo comum encontrá-la em grandes empresas, universidades ou organizações. A WAN tem a características de possuir uma boa qualidade, maior rapidez, maior qualidade e mais segurança para os utilizadores.



WAN:

Wide Area Network, ou Rede de Área Ampla. Numa WAN a comunicação dá-se numa distância relativamente (ou muito) longa. Geralmente podemos usar uma WAN para conectar uma LAN num local a outra LAN num outro local remoto, que pode estar localizada em um prédio vizinho ou do outro lado do planeta.





WAN (Wide Area Network) – Permitem a interligação de redes locais, metropolitanas e equipamentos de rede, numa grande área geográfica (ex. país, continente, etc).

Vantagens LAN

Mais rápidas e mais económicas por ter uma dimensão menor comparada com a WAN, o modelo LAN to LAN proporciona o grande benefício de redução de custos, com uma rede LAN podemos compartilhar recursos facilmente com outros computadores, economizando despesas, porque não precisamos comprar mais dispositivos, como impressoras, scanners, ou dispositivos de armazenamento para cada computador, basta comprar um e compartilhar para estes dispositivos serem acessados desde os outros computadores.

Resumindo podemos dizer que:

A LAN é mais rápida do que a WAN, pois os dispositivos estão fisicamente próximos um do outro.

A LAN é mais segura, pois os dados só viajam através de cabos físicos.

A LAN é mais barata de implementar e manter do que a WAN.

Desvantagens LAN

É a segurança mais vulnerável, problemas com um servidor central se falha ficam todos sem acesso aos dados que este tinha, como por exemplo uma aplicação de faturação.

Devido ao seu tamanho maior, as redes WAN são sempre mais lentas que uma LAN. Quanto maior a distância, mais lenta a rede, ter uma WAN privada é muito caro devido à tecnologia necessária para conectar dois locais remotos.

Resumindo podemos dizer que:

A LAN é limitada geograficamente e só pode conectar dispositivos em uma área local.

A LAN não fornece acesso à Internet para todos os dispositivos conectados.

Vantagens WAN

Abrange uma grande área geográfica de 1000 km ou mais. Se o escritório estiver em diferentes cidades ou países, podemos conectar as suas filiais através da WAN.

Dados centralizados:
Aqui a empresa não precisa comprar e-mails, arquivos e servidores de backup; todos podem residir na sede. Todas as filiais do escritório podem compartilhar os dados através do servidor da matriz. Podemos obter backup, suporte e outros dados úteis da matriz e todos os dados são sincronizados com todas as outras filiais.

Alta largura de banda:

Se tiver linhas alugadas para a empresa, ela oferece uma largura de banda alta do que a conexão de banda larga normal. Podemos obter uma alta taxa de transferência de dados que pode aumentar a produtividade da empresa.

Resumindo podemos dizer que:

A WAN é mais ampla em termos geográficos e pode conectar dispositivos em diferentes cidades, estados ou países.

A WAN fornece acesso à Internet para todos os dispositivos conectados.

A WAN é ideal para empresas que precisam conectar diferentes escritórios em diferentes locais.

Desvantagens WAN

Problemas de segurança:

Uma delas é a complexidade natural, devido à escala, o que torna a rede muito difícil de manter e controlar, o que pode gerar brechas de segurança e instabilidades na produtividade.

Exemplo disso é o fato das redes amplas tradicionais não se adaptaram bem à computação em nuvem e à revolução proposta pela cloud. Para isso, é preciso contar com novas soluções.

O custo altíssimo para manter e para garantir bons resultados. A rede de amplo acesso é extremamente grande e requer uma infraestrutura poderosa e robusta, com muito poder de computação.

Por ser grande demais, as redes e estruturas WAN podem sofrer com a falta de agilidade e tolerância a mudanças. No cenário de empresas que crescem e mudam muito rápido, isso pode se tornar custoso.

Precisa de software de firewall e antivírus.

Resumindo podemos dizer que:

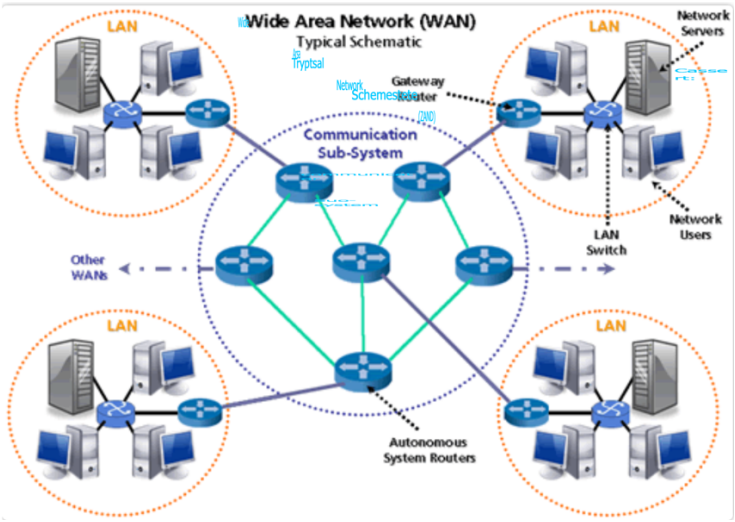
A WAN geralmente é mais cara de implementar e manter do que uma LAN.

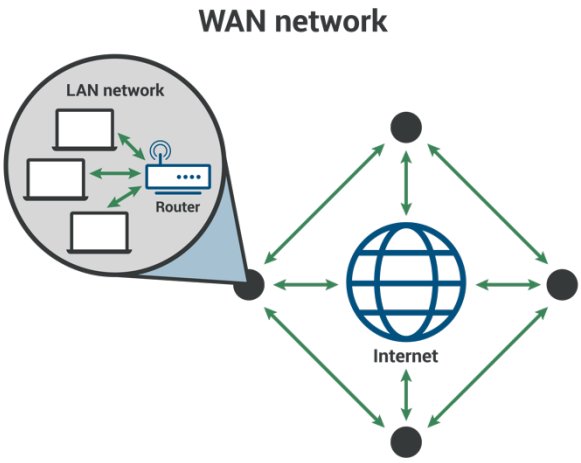
A WAN pode ser menos segura, pois os dados viajam através de linhas telefônicas ou satélite, o que os torna mais suscetíveis a ataques cibernéticos.

A WAN pode ter latência (atraso) maior do que uma LAN, pois os dados precisam viajar através de grandes distâncias.

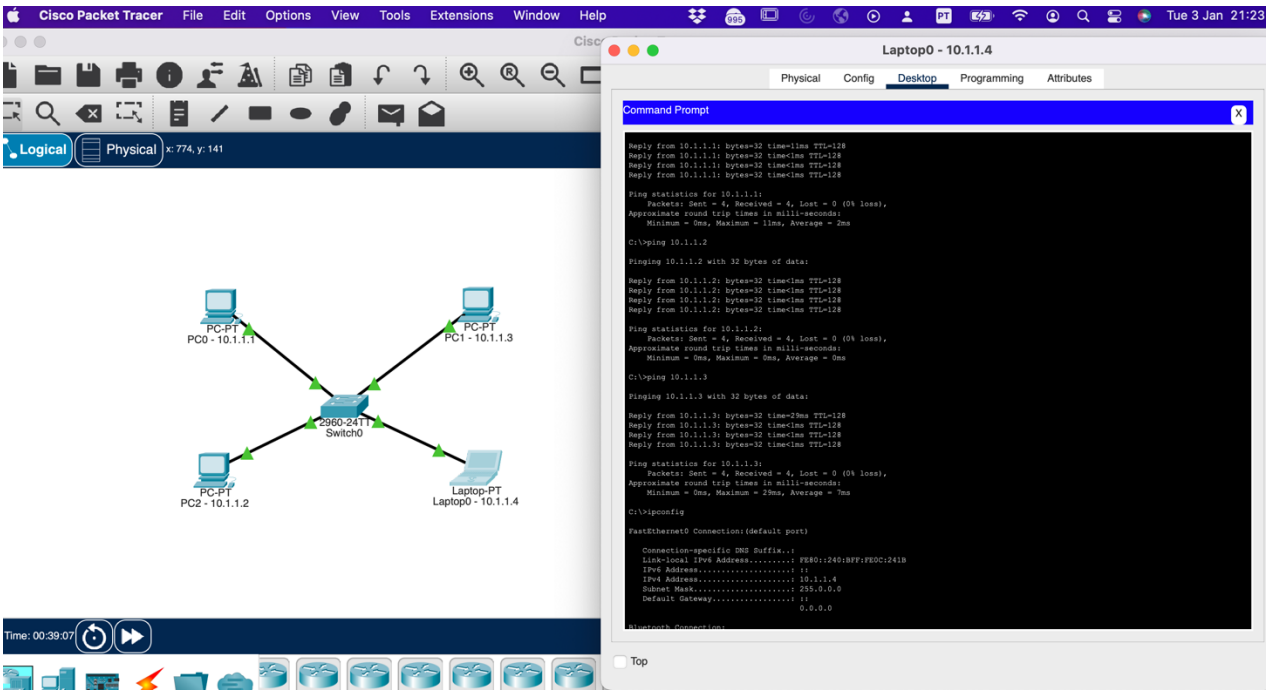
Para mostrar o diagrama de LAN e WAN:

O diagrama seria LAN ------- **Router** -------WAN:





Também aproveitei e fiz no *Cisco Packet Tracer* uma simulação de uma rede LAN, com uma gama de IPs, como podemos ver no terminal do laptop, que esta a fazer ping a todas as máquinas que estão ligadas entre si, através de um **Switch**, para o WAN basta ligar internet a esta rede e já tínhamos o exemplo de WAN:



Resposta nª2)

ARP (Address Resolution Protocol) é um protocolo de rede utilizado para mapear endereços IP para endereços MAC (Media Access Control) em redes LAN. Ele é utilizado para descobrir o endereço MAC de um host em uma rede, a partir do seu endereço IP.

Recentemente um leitor enviou-me um e-mail com a seguinte questão: "**Numa rede ethernet, como é que os PC's se descobrem uns aos outros?".** Quem trabalha com redes a resposta seria directa: o protocolo ARP (*Address Resolution Protocol* – RFC 826) permite que um PC obtenha o endereço físico de uma máquina(mac address), usando o endereço IP (da máquina de destino).

RARP (Reverse Address Resolution Protocol) tambem é um protocolo de camada de rede. O RARP é um protocolo TCP / IP que permite que qualquer host obtenha seu endereço IP do servidor. O RARP é adaptado do protocolo ARP e é apenas reverso do ARP.

ARP (Protocolo de resolução de endereço) e RARP (Protocolo de resolução reversa de endereço) são dois dos protocolos de rede de computador usados para resolver a camada de link e os endereços de protocolo IP. O ARP resolve um endereço IP, dado o endereço de hardware. O RARP resolve um endereço de hardware quando o endereço IP correspondente é fornecido. Na realidade, o RARP faz o oposto ou o reverso do ARP, daí o nome Reverse ARP. Mas O RARP não é mais usado (foi substituído por protocolos melhores.)

O funcionamento do ARP é o seguinte:

Quando um host precisa enviar um pacote para outro host em uma rede LAN, ele verifica se possui o endereço MAC do destinatário em sua tabela ARP.

Se o endereço MAC não estiver na tabela, o host envia um broadcast para todos os outros hosts da rede solicitando o endereço MAC do destinatário.

Os outros hosts da rede recebem o broadcast e verificam se possuem o endereço MAC solicitado. Se possuírem, eles enviam uma resposta de volta ao host solicitante com o endereço MAC do destinatário.

O host solicitante recebe a resposta e adiciona o endereço MAC do destinatário à sua tabela ARP. Ele então pode enviar o pacote para o destinatário utilizando o endereço MAC obtido.

RARP é um protocolo de rede usado em redes de computadores. O RARP é descrito no RFC 903 publicado pela IETF. Este é um protocolo obsoleto e não é mais usado. Um computador host costumava usar este protocolo para solicitar o endereço IP (Protocolo de Internet, mais especificamente IPv4) de outro host, quando o endereço de hardware (camada de link) estivesse disponível para ele.

Exemplo de endereço de hardware usado foi o endereço MAC (Media Access Control) do host. O RARP tornou-se obsoleto devido às introduções dos protocolos BOOTP (Bootstrap Protocol) e DHCP (Dynamic Host Configuration Protocol) mais recentes, porque ambos oferecem muito mais recursos do que o RARP.

O funcionamento do RARP é o seguinte:

Quando um host precisa obter um endereço IP, ele envia um broadcast para todos os outros hosts da rede solicitando um endereço IP.

Os outros hosts da rede recebem o broadcast e verificam se possuem um endereço IP disponível para atribuir ao host solicitante. Se possuírem, eles enviam uma resposta de volta ao host solicitante com um endereço IP disponível.

O host solicitante recebe a resposta e adiciona o endereço IP atribuído à sua configuração de rede. Ele então pode se comunicar com outros hosts da rede utilizando o endereço IP atribuído.

Resposta nª3)

a)

O algoritmo de Flooding é um método de disseminação de informação em uma rede, no qual uma mensagem é enviada para todos os nós da rede. Ele é utilizado principalmente em redes de computadores que não possuem um esquema de endereçamento pré-estabelecido ou em que há falhas frequentes na comunicação entre os nós.

A seguir, explicarei como o algoritmo de Flooding funciona e darei um exemplo de sua aplicação:

O nó de origem (que deseja disseminar a mensagem) envia a mensagem para todos os seus vizinhos diretos.

Cada nó que recebe a mensagem verifica se já a possui. Se já possuir, descarta a mensagem. Caso contrário, adiciona a mensagem à sua tabela de mensagens e envia a mensagem para todos os seus vizinhos diretos.

Esse processo se repete até que todos os nós da rede tenham recebido a mensagem ou até que a mensagem alcance um nó que já a possui.

Exemplo de aplicação:

Imagine que existe uma rede de computadores composta por cinco nós: A, B, C, D e E. O nó A deseja disseminar a mensagem "Olá" para todos os outros nós da rede. Ele envia a mensagem para os nós B, C e D. O nó B envia a mensagem para os nós C e E. O nó C envia a mensagem para o nó D. O nó D envia a mensagem para o nó E. Dessa forma, todos os nós da rede (A, B, C, D e E) acabam recebendo a mensagem "Olá" do nó A.

Vantagens do algoritmo de Flooding:

Fácil de implementar: o algoritmo de Flooding é simples de ser implementado, pois não exige um esquema de endereçamento pré-estabelecido.

Robusto: o algoritmo de Flooding é robusto, pois mesmo em caso de falhas na comunicação entre os nós, a mensagem ainda será disseminada para todos os nós da rede.

Desvantagens do algoritmo de Flooding:

Consome muita largura de banda: isto porque o algoritmo de Flooding envia a mensagem para todos os nós da rede, o que pode consumir muita largura de banda.

Pode levar ao congestionamento da rede: se houver muitas mensagens sendo disseminadas pela rede ao mesmo tempo, pode haver congestionamento e atraso.

Concluimos que:

O algoritmo de inundação (Flooding) é um algoritmo de roteamento estático que é utlizado em redes de computadores para encontrar o caminho mais curto entre dois dispositivos. Ele funciona enviando copias de um pacote par a todos os dispositivos da rede, incluído o dispositivo de origem e o dispositivo de destino. Quando um pacote é recebido por um dispositivo, ele é encaminhado par a todos os dispositivos vizinhos, exempto o dispositivo de origem. Dessa forma, o pacote é propagado por toda a rede até chegar ao destino. O algoritmo de inundação é simples e fácil de implementar, mas pode ser ineficiente em redes grandes, pois gera muito tráfego na rede. Alem disso ele não leva em consideração o caminho mais curto para o destino, o que pode resultar em atrasos na entrega de pacotes. O algoritmo de inundação é mais adequado para redes pequenas e em situações em que a precisão na entrega de pacotes não é tao critica, como em redes de mensagens ou em redes de sensores. Em redes maiores ou em que a entrega precisa ser mais rápida e

confiável, é melhor utilizar algoritmos de roteamento dinâmicos, como o protocolo de roteamento do estado de ligação (Link-State Routing Protocol) ou o algoritmo de roteamento com vetor de distancia (Distance-Vector Routing).

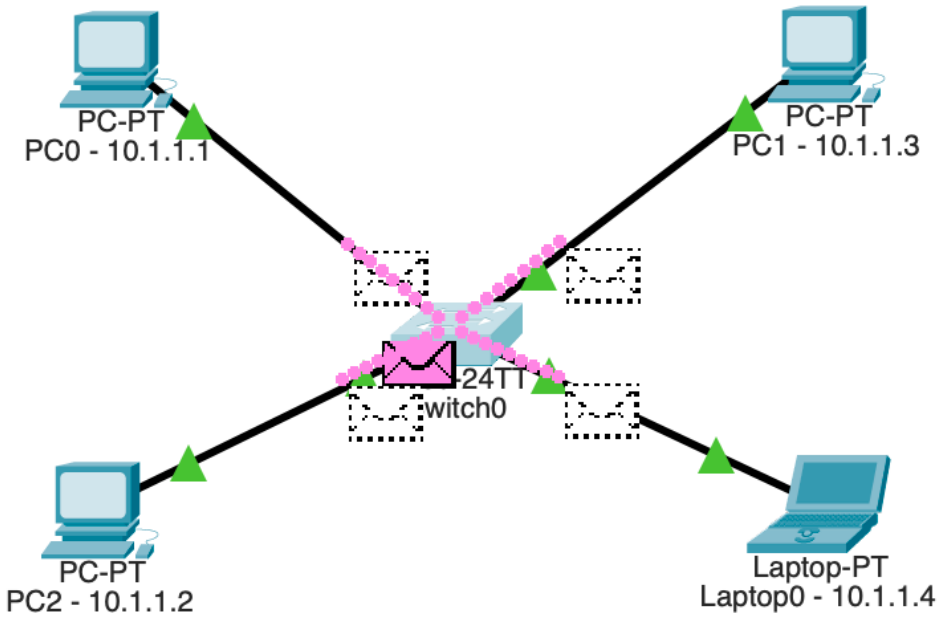
Lembrando-me de vírus e ataques hacker:

Existem ataques **DDoS** com flooding desenvolvido para sobrecarregar um servidor visado com solicitações HTTP **ataques de volumetria:** Inclui flood UDP, flood ICMP e outros floods de pacotes falsos. O objetivo do ataque é saturar a largura de banda do site atacado e a magnitude é medida em bits por segundo (Bps), existem vírus para enviar massivamente mails para uma caixa de correio causando sua saturação.

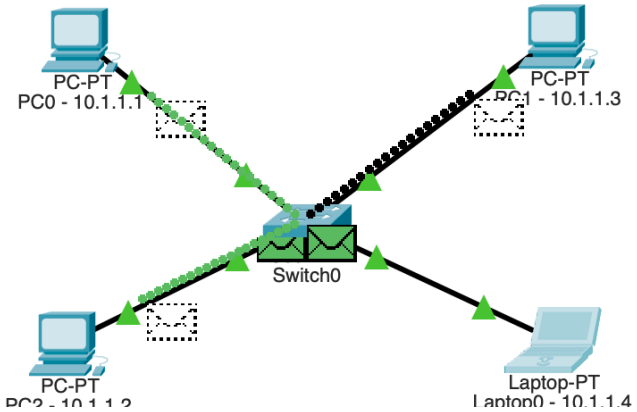
Fiz uma simulação no Cisco Packet Tracer para mostrar o Flooding:

Enquanto os switch não sabe o mac address de um pc para outro, ele vai fazer o envio de pack para todas as máquinas és isto que chamamos o Flooding:

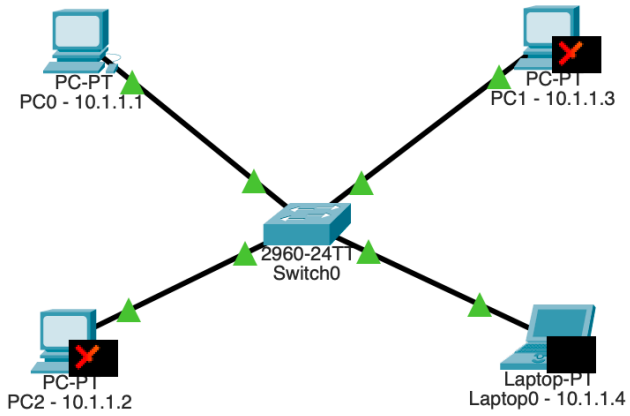
Vemos aqui no passo 1 ele envia para todos:

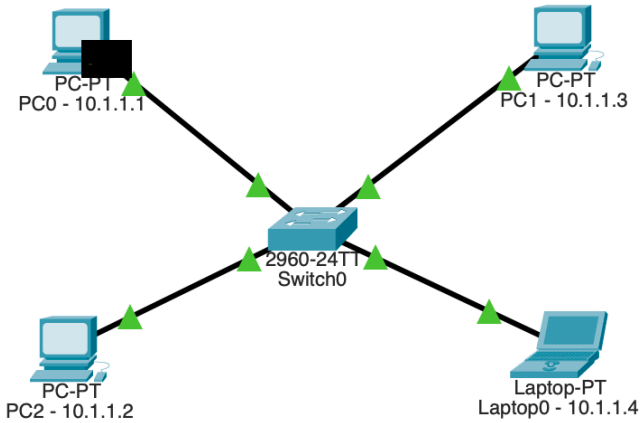


Agora note que ao fazer ping do laptop 10.1.1.4 para o pc 10.1.1.1 ele vai conhecer o mac address deste e vice-versa, ao fazer ping no pc 10.1.1.1 ele vai conhecer o mac address do laptop 10.1.1.4, no envio de pack ele faz o Flooding para todas as máquinas porque não conhece o mac address das outras duas:

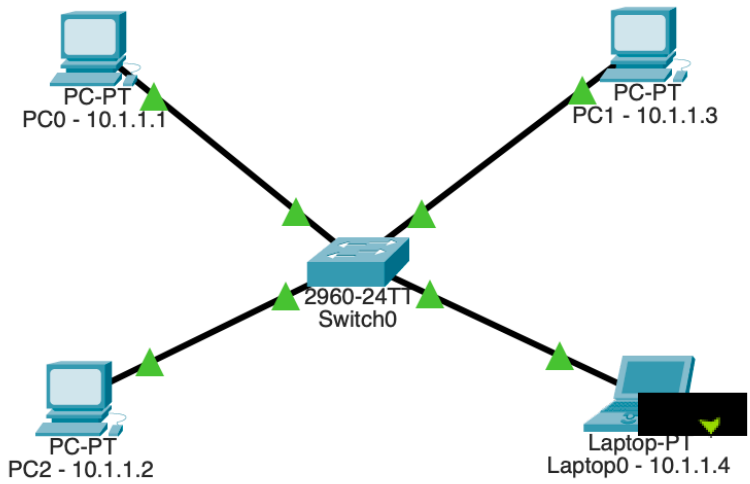


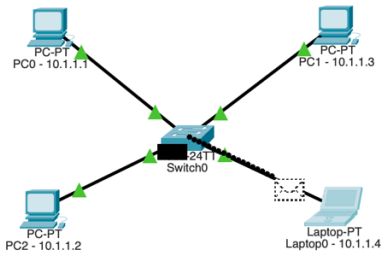
Depois quando encontra o pc 10.1.1.1 que conhece o mac address do laptop 10.1.1.4, regressa ao laptop validado o mac address encontrado:

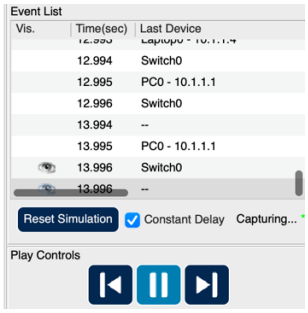




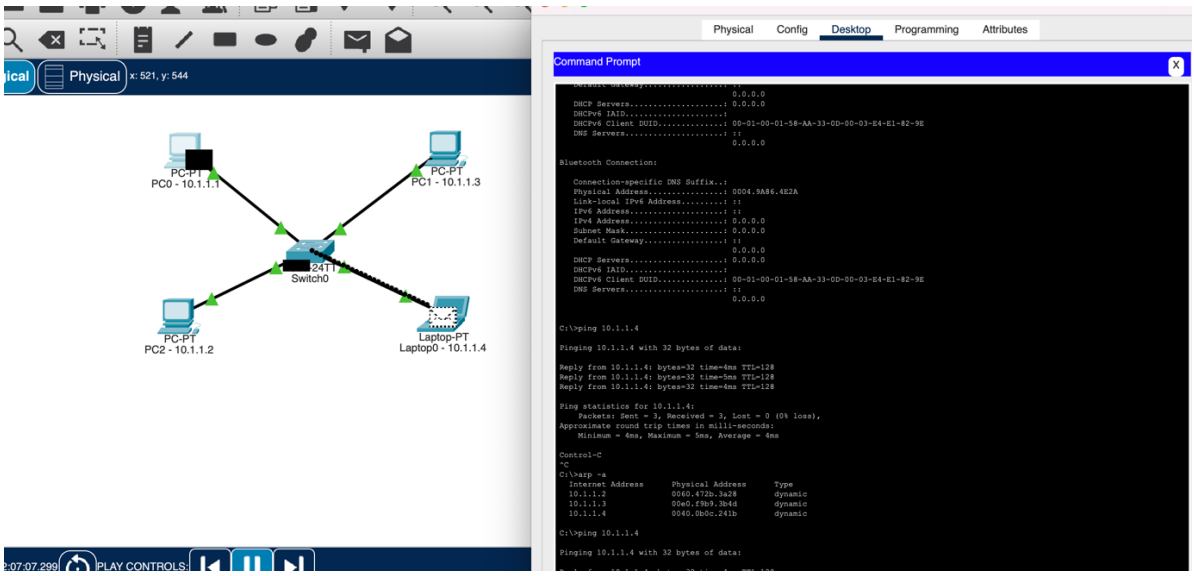
Já fica o regresso do pack só para o laptop 10.1.1.4:







Desta forma vemos os packs, só a ser enviados entre estas duas máquinas:



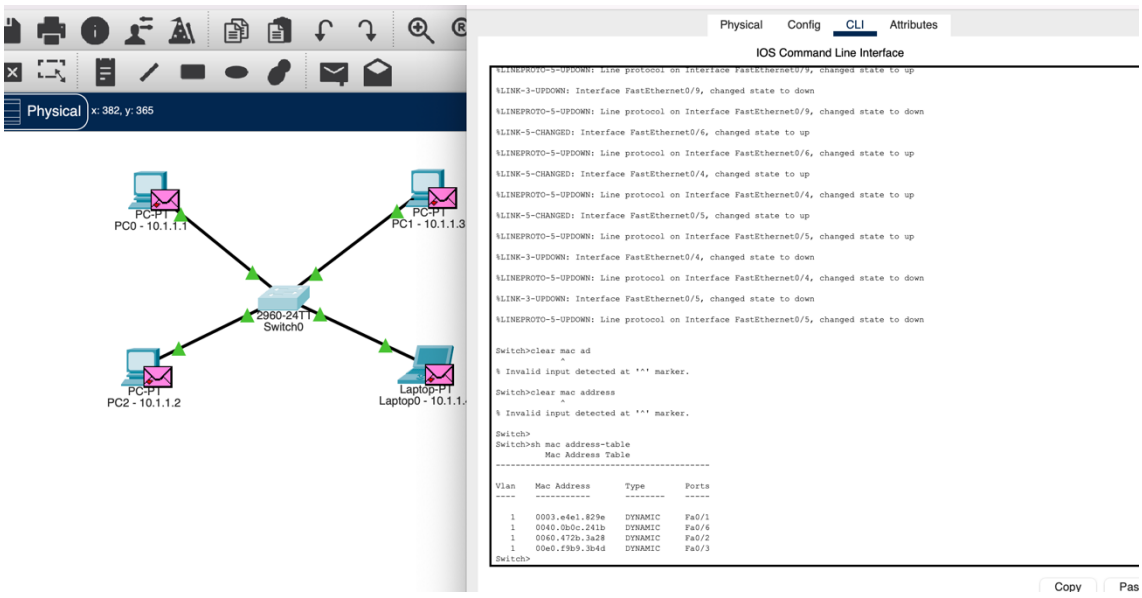
Aqui vemos um exemplo com o comando ARP, que mostra o protocolo, como são capturados os mac address ao fazer o ping entre as duas máquinas 10.1.1.1 e o laptop que é a 10.1.1.4, enquanto conhecer os mac address no switch esta irá fazer a comunicação entre estas duas máquinas, se não conhecer o mac address, ira fazer o Flooding para todas as máquinas até obter o mac address:

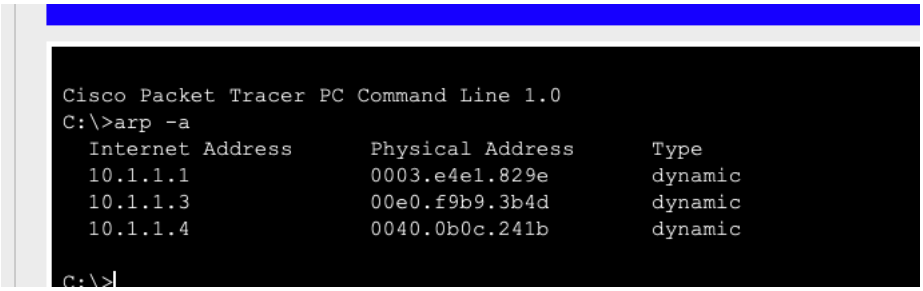
```
C:\>arp -a
  Internet Address      Physical Address      Type
  10.1.1.1              0003.e4e1.829e        dynamic
  10.1.1.4              0040.0b0c.241b        dynamic

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:
```

Para saber o mac address da máquina 10.1.1.2, por exemplo, basta fazer um ping e ele passa a conhecer também o mac address da máquina 2, até não saber o mac address faz o flooding para a rede toda e assim vai capturando os mac address na cache do switch como vemos na imagem seguinte:





Tem na biografia o link do vídeo em HD da demostração que fiz.

b) As rotas possíveis que seguirá o pacote enviado de A até I, que tem uma contagem máxima de hops igual a 4, são:

ADFHI

ADGI

ABDGI

ADGHI

Resposta 4)

a)

Os algoritmos de roteamento por vetor de distância operam fazendo cada roteador manter uma tabela (isto é, um vetor) que fornece a melhor distância conhecida até cada destino e determina qual enlace deve ser utilizado para chegar lá. Essas tabelas são atualizadas por meio da troca de informações com os vizinhos. No fim, cada roteador saberá o melhor enlace para alcançar cada destino. No roteamento por vetor de distância, cada roteador mantém uma tabela de roteamento indexada para cada roteador da rede e que contém uma entrada para cada um deles. Essa entrada contém duas partes: a interface de saída preferencial a ser utilizada para o destino e uma estimativa da distância até esse destino. A métrica utilizada pode ser o número de hops ou outra medida, conforme discutimos para o cálculo do caminho mais curto. O roteamento com vetor de distância ou em inglês "**Distance Vector Routing**", foi o algoritmo de roteamento original da ARPNET. É conhecido por diversos nomes, sendo o mais comum o algoritmo de roteamento distribuído de **Bellman-Ford**. Em termos comparativos, para entendimento deste processo, temos o exemplo do sistema de navegação por GPS quando estamos em um local (origem) e pretendemos ir para um destino pelo caminho mais rápido calculando todas as possíveis estradas que irão dar ao destino considerando tráfego, outros, etc.

b)

Vetores que entram no Routeador C:

Vetor desde B (5,0,8,12,6,2)

Vetor desde D (16,12,6,0,9,10)

Vetor desde E (7,6,3,9,0,4)

Os retardos medidos de C para B=6; D=3; E=5

Calculamos o retardo esperado que é a soma do vetor mais a retardo vindo de cada routeador:

Roteadores	**Vetores B**	**Vetores + retardo B**	**Vetores D**	**Vetores + retardo D**	**Vetores E**	**Vetores + retardo E**
A	5	**5+6 = 11**	16	16+3=19	7	7+5=12
B	0	**0+6 = 6**	12	12+3=15	6	6+5=11
C	8	8+6 = 14	6	6+3 = 9	3	3+5=8
D	12	12+6 =18	0	**0+3 = 3**	9	9+5=14
E	6	6+6 = 12	9	9+3 =12	0	**0+5=5**
F	2	**2+6 = 8**	10	10+3=13	4	4+5=9

Em cada linha/roteador podemos verificar qual é o caminho mais curto (valores realçados em azul) e desta forma obtemos a linha de saída e o retardo esperado:

Roteador	Saida	Retardo
A	B	11
B	B	6
C	-	-
D	D	3
E	E	5
F	B	8

Como podemos ver de acordo com o calculo/tabela o vetor transmitido é C: (11,6,-,3,5,8).

Também vi outra maneira de obter estes valores de retardo, mas vi que era um processo mais longo, só fiz para o primeiro e último.

11 e o 8 do vetor C (11,6,-,3,5,8):

	A	B	C	D	E	F
B	5	0	8	12	6	2
D	16	12	6	0	9	10
E	7	6	3	9	0	4
C	11	6	0	3	5	8
Interface	$\underline{B}$	B	-	D	E	$\underline{B}$

CA = CEA; CBA

CEA = 5+7 = 12

CBA = 6+5 = 11

A linha de saída mais curta é CBA com 11ms de retardo.

CF = CDF; CEF; CBF; CBAEF;

CDF = 3+10 = 13

CEF = 5+4 = 9

CBF = 6+2=8

CBAEF = 6+5+7+4=22

A linha de saída mais curta é CBF com 8ms de retardo.

BIBLIOGRAFIA

Tanenbaum, A. S., Wetherall, D.J. (2013).Computer Networks, Fifth Edition. Pearson International Editions, ISBN-10: 1292024224

WEBGRAFIA

1) https://tudotecnologia.net/o-que-e-lan-e-wan-quais-as-diferencas/
2) https://sit13.wordpress.com/disciplinas/bases-da-internet/definicoes-complementares/lan-man-e-wan/
3) http://sistemasaplicativoseaengenharia.blogspot.com/2011/11/uma-redelan-e-as-empresas-de-engenharia.html
4) https://blog.algartelecom.com.br/gestao/lan-to-lan-quais-sao-as-vantagens-em-adotar-a-solucao/
5) https://altitudetvm.com/pt/jaringan/1200-pengertian-jaringan-lan-beserta-kelebihan-dan-kekurangannya.html#Kelebihan_Jaringan_LAN
6) https://www.desterroeletricidade.com.br/blog/telefonia/o-que-e-rede-wan-e-lan-tipos-e-vantagens-para-empresas/
7) https://internetempresarial139116546.wordpress.com/2020/05/01/vantagens-e-desvantagens-da-rede-de-longa-distancia-wan/
8) https://pt.gadget-info.com/difference-between-arp
9) https://pplware.sapo.pt/microsoft/windows/redes-sabe-para-que-serve-o-protocolo-arp/
10) https://pt.strephonsays.com/arp-and-vs-rarp-12033
11) https://efagundes.com/networking/algoritmos-de-roteamento/inundacao-flooding/
12) https://www.tutorialspoint.com/flooding-in-computer-network
13) https://www.packettracernetwork.com/download/download-packet-tracer.html
14) (vídeo eu a mostrar o flooding numa rede LAN) https://youtu.be/tjqsrqrpI9U