



Networking Fundamentals and Security

- Aula 09 -

Mauro Cesar Bernardes

São Paulo, 2022

Calendário 2º Sem

Agosto 2022							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
31	1	2	3	4	5	6	7
32	8	9	10	11	12	13	14
33	15	16	17	18	19	20	21
34	22	23	24	25	26	27	28
35	29	30	31				

Setembro 2022							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
35				1	2	3	4
36	5	6	7	8	9	10	11
37	12	13	14	15	16	17	18
38	19	20	21	22	23	24	25
39	26	27	28	29	30		

Outubro 2022							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
39						1	2
40	3	4	5	6	7	8	9
41	10	11	12	13	14	15	16
42	17	18	19	20	21	22	23
43	24	25	26	27	28	29	30
44	31						

Novembro 2022							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
44		1	2	3	4	5	6
45	7	8	9	10	11	12	13
46	14	15	16	17	18	19	20
47	21	22	23	24	25	26	27
48	28	29	30				

Programação Final:

Setembro

Semana 37: Atividade Prática: DNS e WiFi (Camada de Aplicação – CAP14 NetAcademy)

Semana 38: IPV6 (Camada de Rede – Capítulo 12 NetAcademy)

Semana 39: 2º Checkpoint

Outubro

Semana 40: NAT IPv4 e IPV6

Semana 41: Switching Ethernet (Camada de Aplicação – CAP07 NetAcademy)

Semana 42: Redes Wireless e Segurança

Semana 43: 3º Checkpoint

Calendário FIAP

8

AGOSTO

01

Início das aulas.

9

SETEMBRO

07

Independência do Brasil (feriado).

10

OUTUBRO

12

Nossa Senhora Aparecida (feriado).

22

NEXT.

31/10 a 11/11

Período de aplicação das Provas Semestrais.

11

NOVEMBRO

02

Finados (feriado).

31/10 a 11/11

Período de aplicação das Provas Semestrais.

14

Dia não letivo.

15

Proclamação da República (feriado).

16 a 18

Período de aplicação das Provas de DP.

20

Consciência Negra (feriado).

21 a 25

Provas Semestrais Substitutivas Regulares e de DP.

28/11 a 02/12

Período de vistas das Provas.

12

DEZEMBRO

28/11 a 02/12

Período de vistas das Provas.

05 a 09

Período de Aplicação dos Exames Finais.

14

Data máxima para divulgação dos resultados dos Exames Finais.

15

Data Limite para solicitação de revisão de notas e faltas de 2022.

16

Término do período letivo.

25

Natal (feriado).

Plano de Aula

- **Objetivo**

- Apresentar uma introdução a Roteamento
- Compreender o funcionamento do protocolo NAT com *Static NAT*
- Compreender o funcionamento do protocolo NAT com *Dynamic NAT*
- Compreender o funcionamento do protocolo NAT com *Port Address Translation*

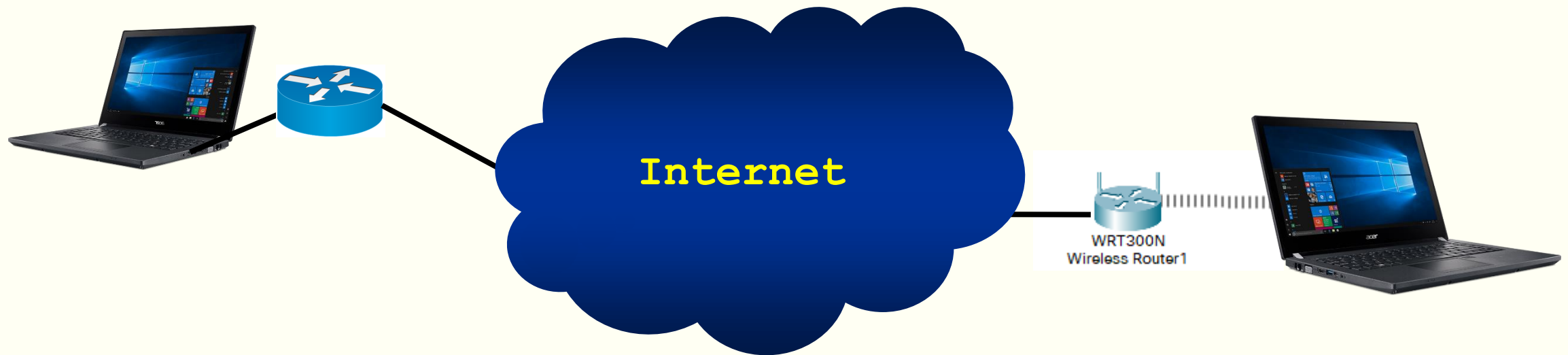
- **Conteúdo**

- NAT em simulador *Packet Tracer*

- **Metodologia**

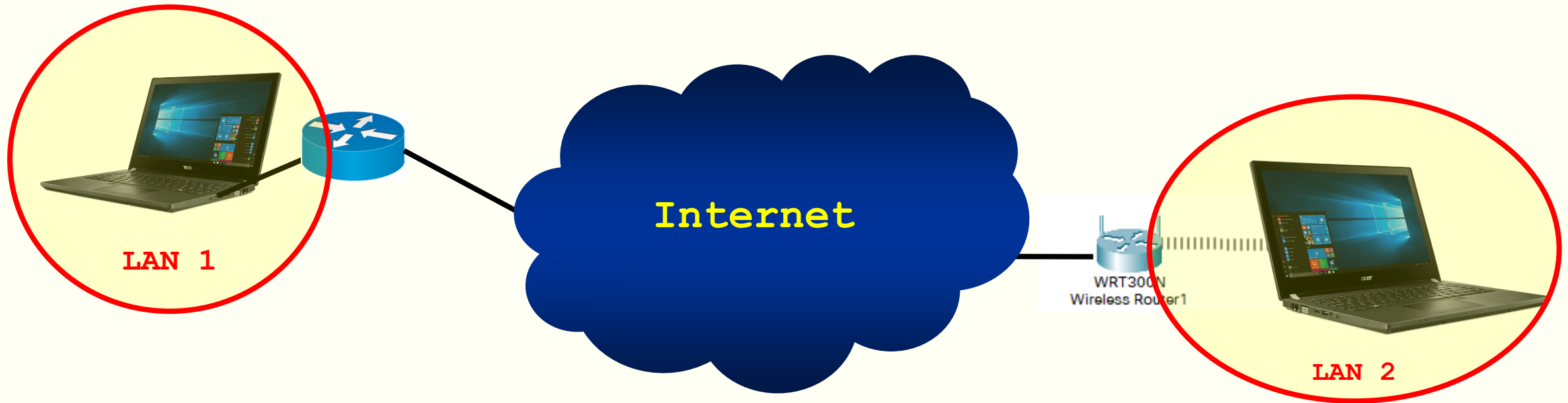
- Aula expositiva sobre os conceitos de NAT e desenvolvimento de atividade prática com configuração em simulador (*Packet Tracer*) de servidores HTTP.

Identificando usuários da rede



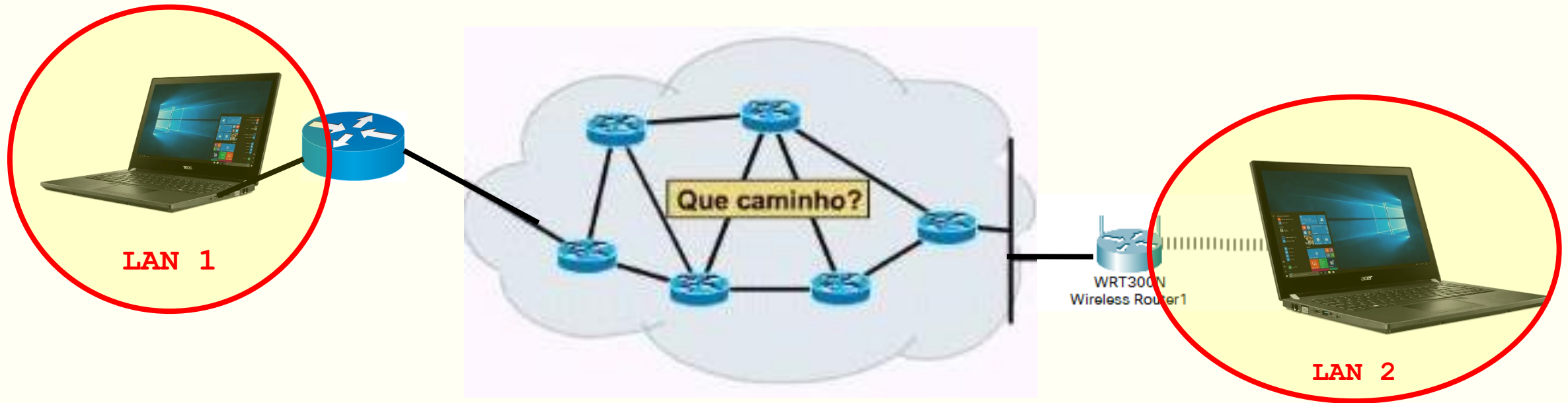
Para que um equipamento consiga efetuar uma comunicação com um outro equipamento em uma rede distante, é preciso uma **estrutura de endereçamento hierárquico**

Identificando usuários da rede



Para que um equipamento consiga efetuar uma comunicação com um outro equipamento em uma rede distante, é preciso uma **estrutura de endereçamento hierárquico**

Identificando usuários da rede



Para que um equipamento consiga efetuar uma comunicação com um outro equipamento em uma rede distante, é preciso uma **estrutura de endereçamento hierárquico**

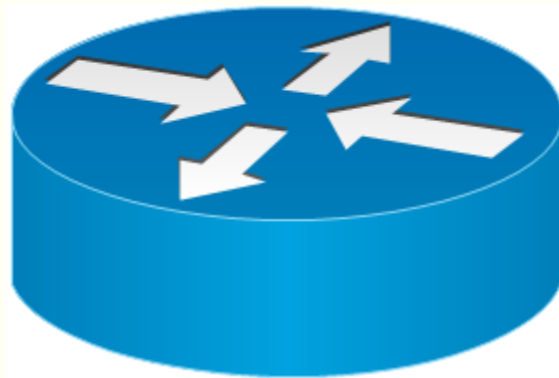
Roteador

(Equipamento da *camada de rede*)

Roteadores

Atividade Básica de um **Roteador**:

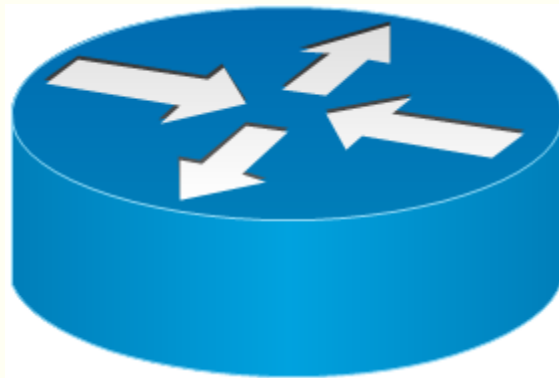
- Determinação das melhores rotas;
- Transporte de *pacotes de dados*.



Roteadores

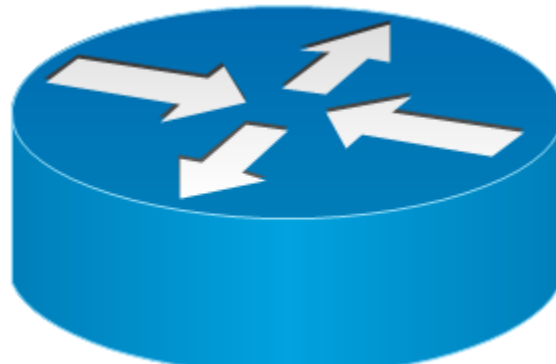
Determinação das **Melhores Rotas**

Métrica: padrão de medida que é usado pelos algoritmos de roteamento para determinar o melhor caminho para um destino

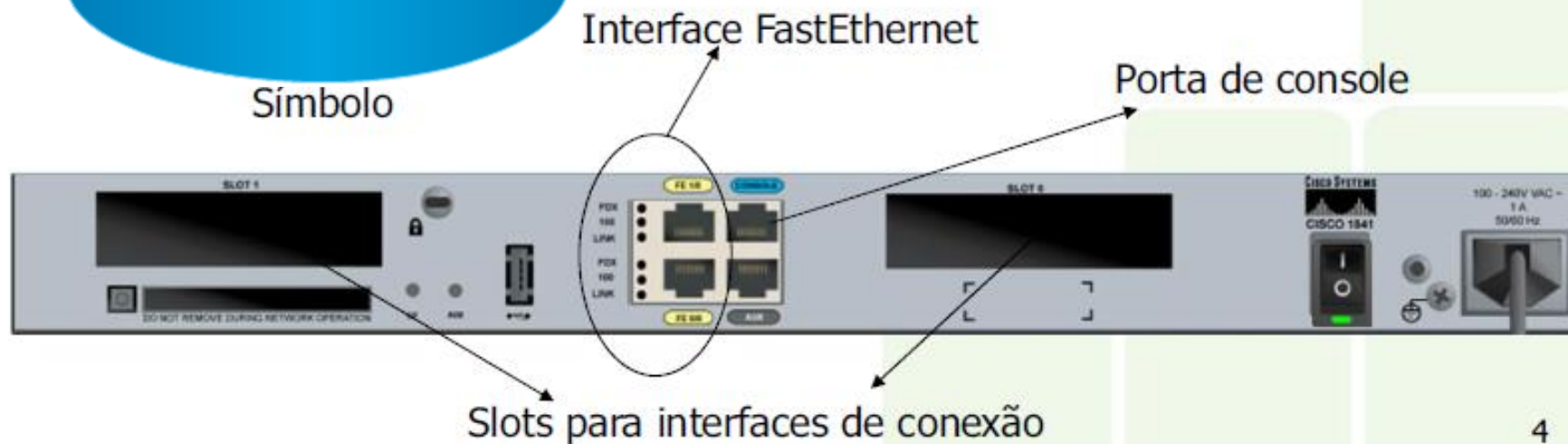


Roteadores

■ Roteador

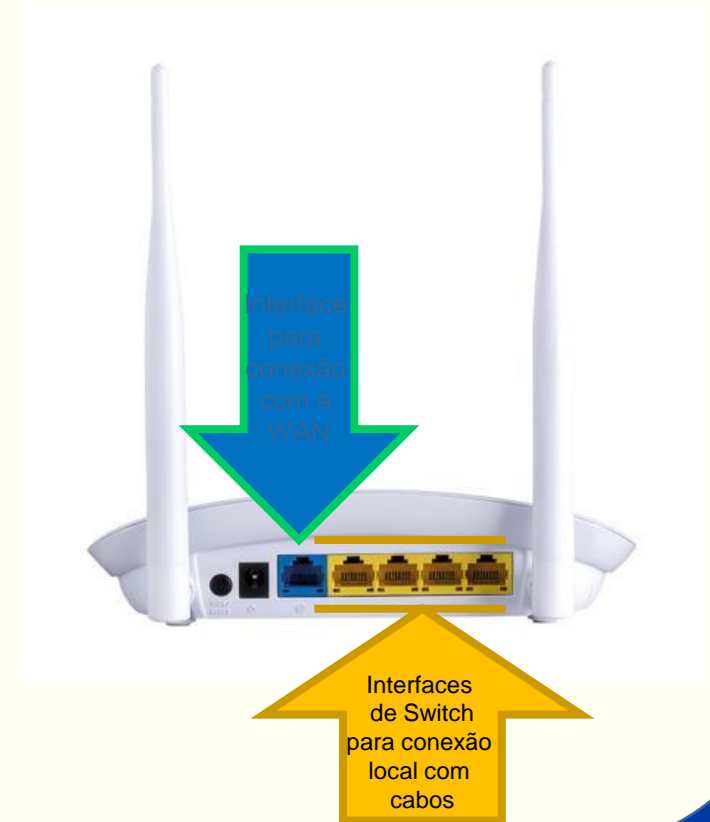


Símbolo

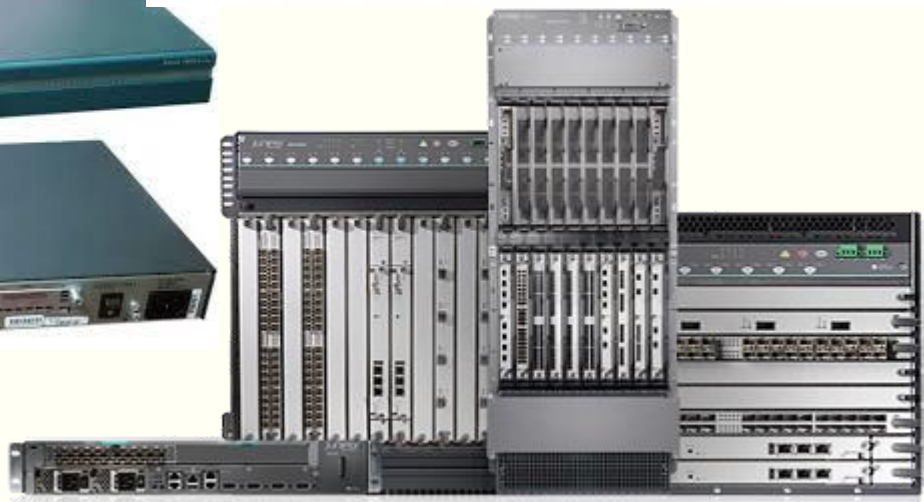
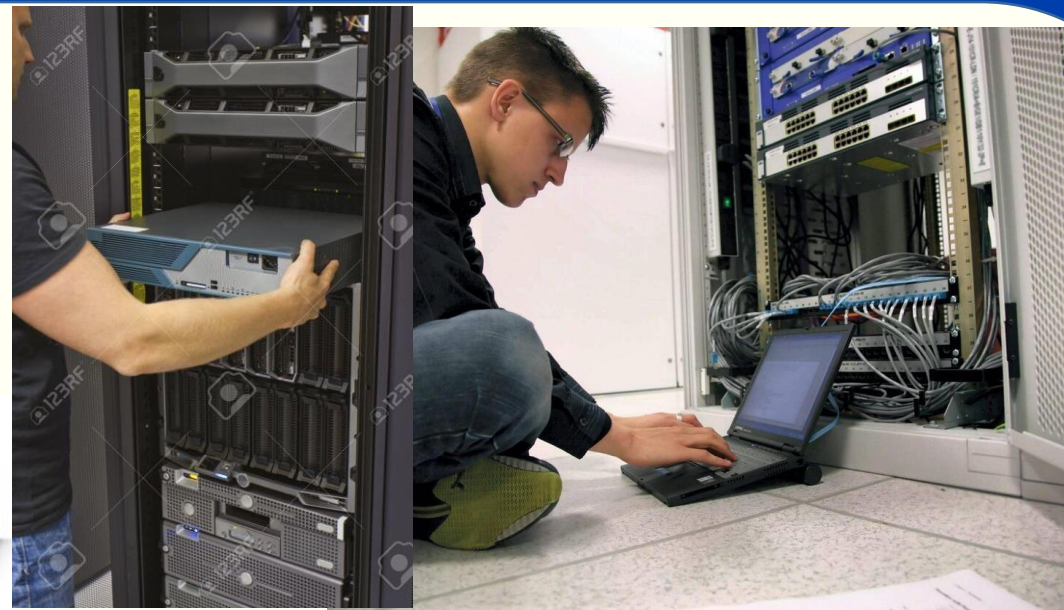


Roteadores

- Em redes locais de pequeno porte como, por exemplo as domésticas, é muito comum que um mesmo equipamento consolide várias funções da camada de rede IP (camada 3 do modelo OSI) e ainda incorpore funções de switch (camada 2 do modelo OSI).
- Dentre as funções de camada 3 podemos citar:
 - Roteamento;
 - Serviço DHCP (endereçoamento dinâmico);
 - NAT (*Network Address Translation*);



Roteadores



Roteadores

Em redes de médio e grande portes, dado o grande volume de tráfego de dados, é comum encontrar equipamentos específicos e exclusivos para a função de roteamento, enquanto em redes de pequeno porte esse papel pode ser exercido por um equipamento de menor porte (e.g. um home router ou até mesmo um PC configurado para atuar como roteador) executando um software que desempenha o papel de um roteador.



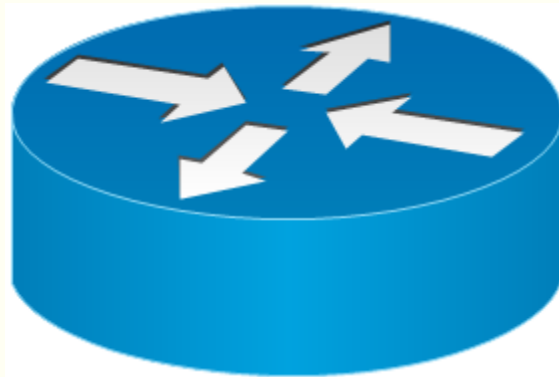
Roteador Doméstico



Roteador Backbone

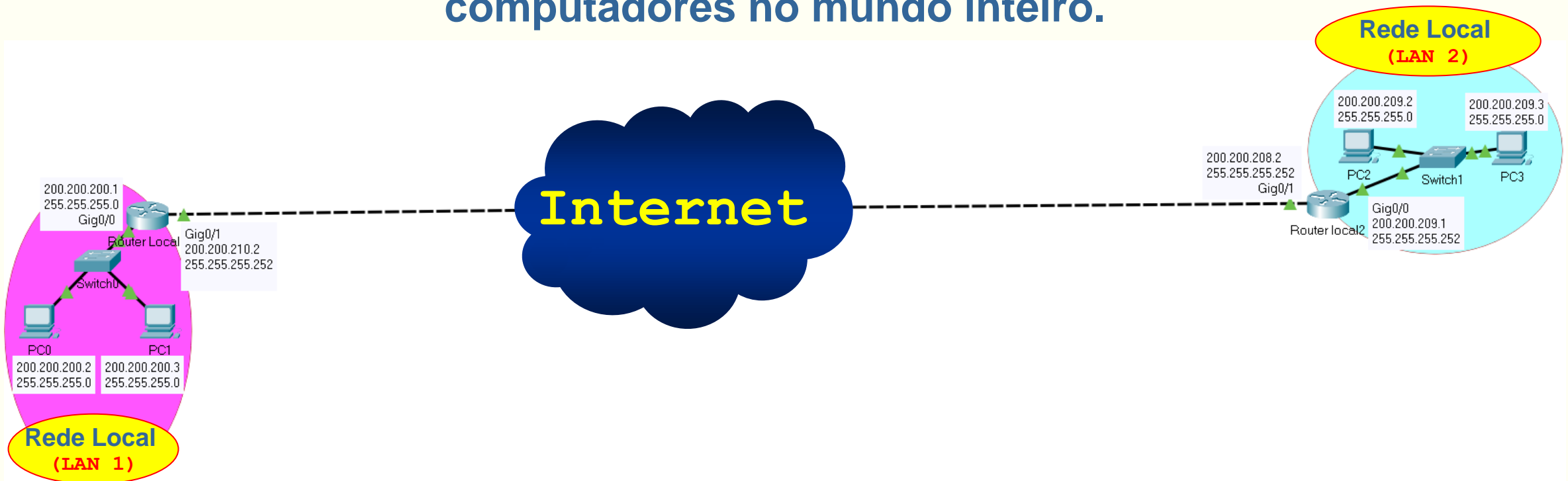
Premissas para o funcionamento de um roteador

- Conhecer a topologia da (sub)rede e **escolher os caminhos adequados** dentro dela;
- Cuidar para que algumas **rotas não sejam sobrecarregadas**, enquanto outras fiquem sem uso;
- Encontrar uma rota quando origem e destino **estão em redes diferentes**.



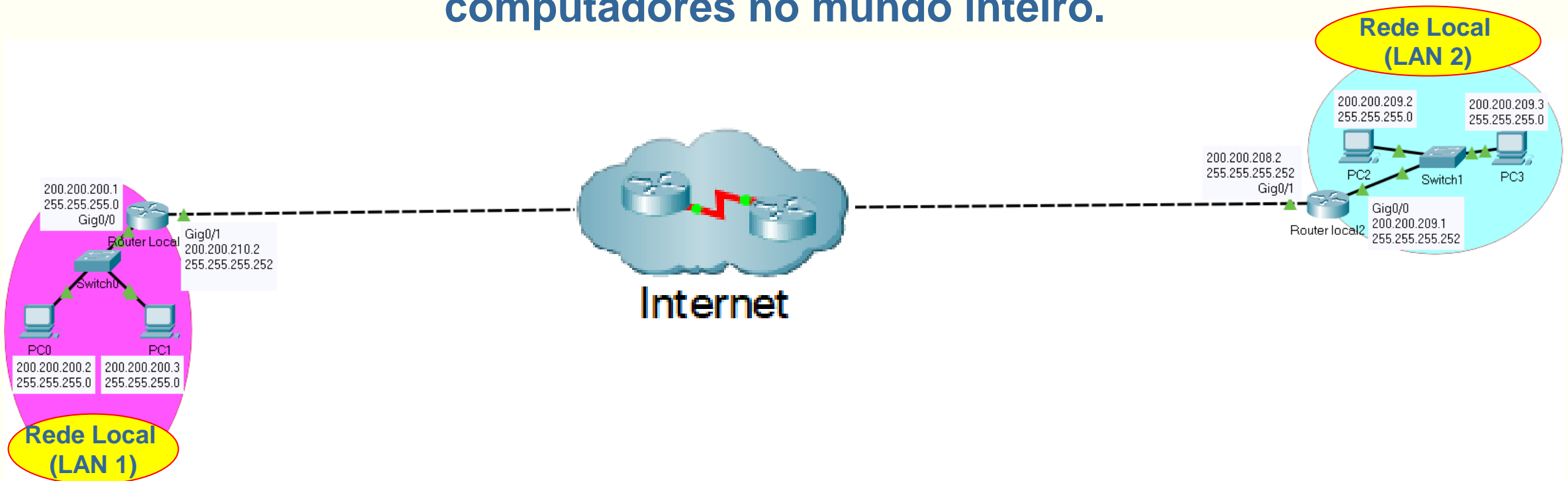
Roteadores

A rede mundial de computadores, conhecida como **Internet**, é uma interligação de várias redes locais via roteadores, ou seja, esse equipamento que é responsável por encaminhar todo o tráfego IP entre computadores no mundo inteiro.



Roteadores

A rede mundial de computadores, conhecida como **Internet**, é uma interligação de várias redes locais via roteadores, ou seja, esse equipamento que é responsável por encaminhar todo o tráfego IP entre computadores no mundo inteiro.



Roteadores

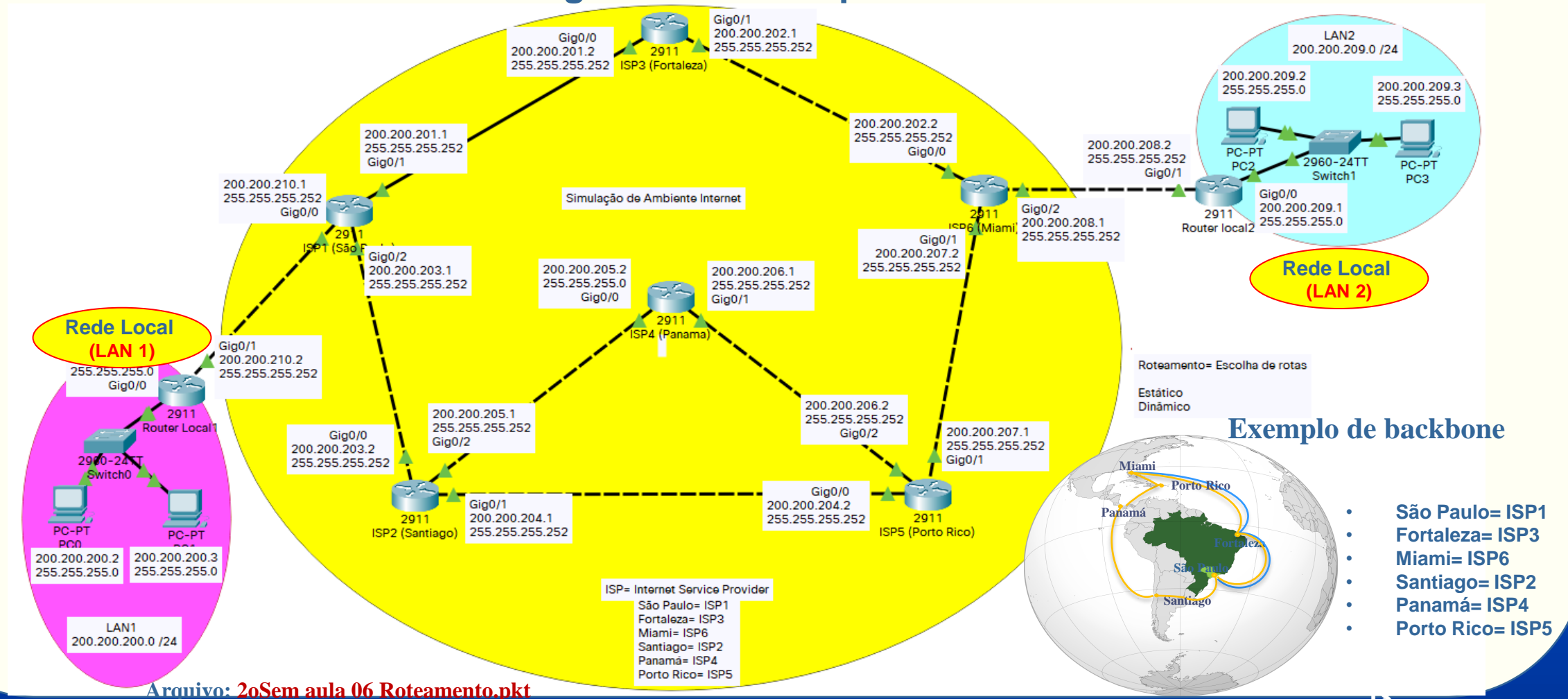


No exemplo apresentado na aula passada, uma rede acadêmica nacional realiza conexão com redes avançadas de pesquisa no continente americano por meio de links que conectam roteadores nas seguintes localidades:

- São Paulo
- Fortaleza
- Santiago
- Panamá
- Porto Rico
- Miami

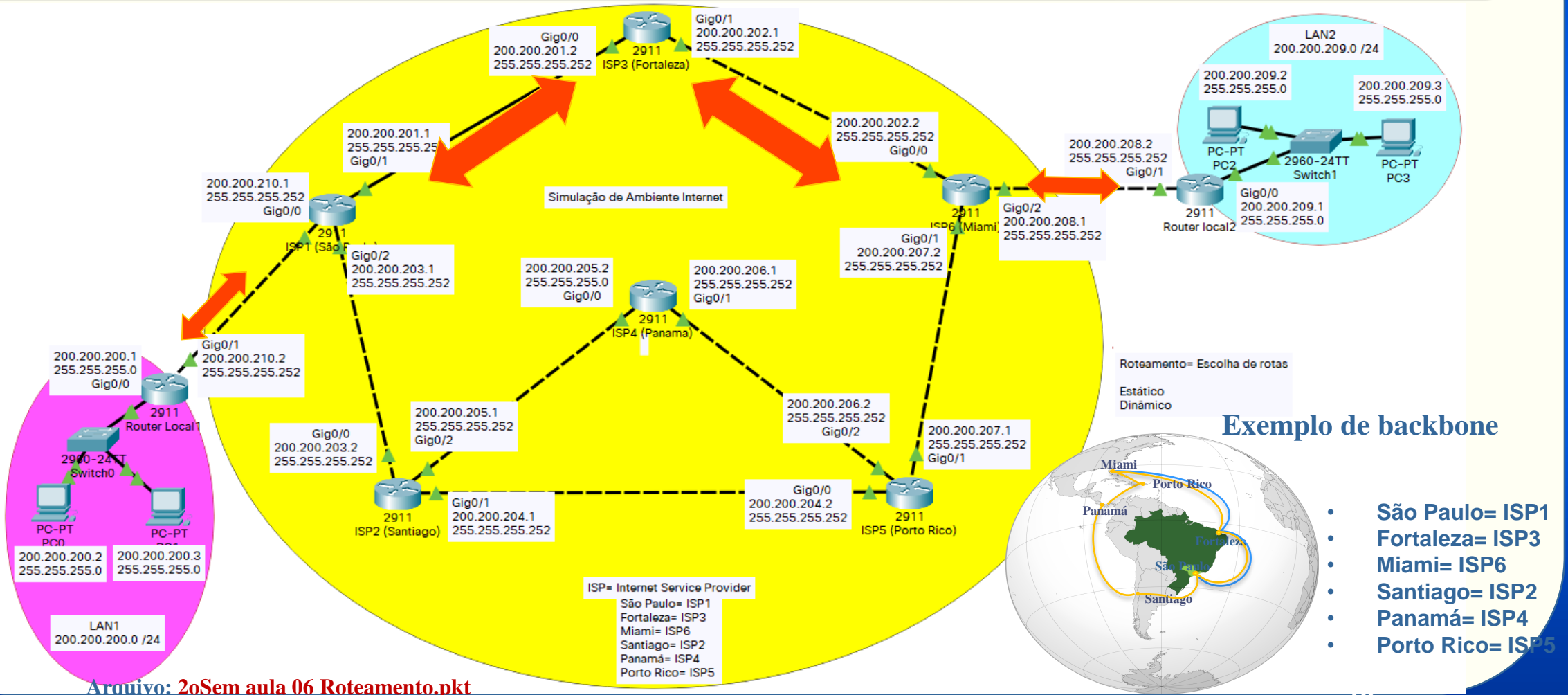
Roteadores

A rede mundial de computadores, conhecida como **Internet**, é uma interligação de várias redes locais via roteadores, ou seja, **o roteador** é responsável por encaminhar todo o tráfego IP entre computadores no mundo inteiro.



Roteamento

Roteamento é o processo de repassar um pacote de dados através de um caminho (rota) de forma que alcance seu destino com menor custo.



Camada de Rede

Network Address Translation (NAT)

Endereços IP não roteáveis (privados)

RFC 1918, February 1996

<http://www.rfcsearch.org/rfcview/RFC/1918.html>

Os endereços IP privados, não roteáveis,
correspondem aos seguintes intervalos de endereços:

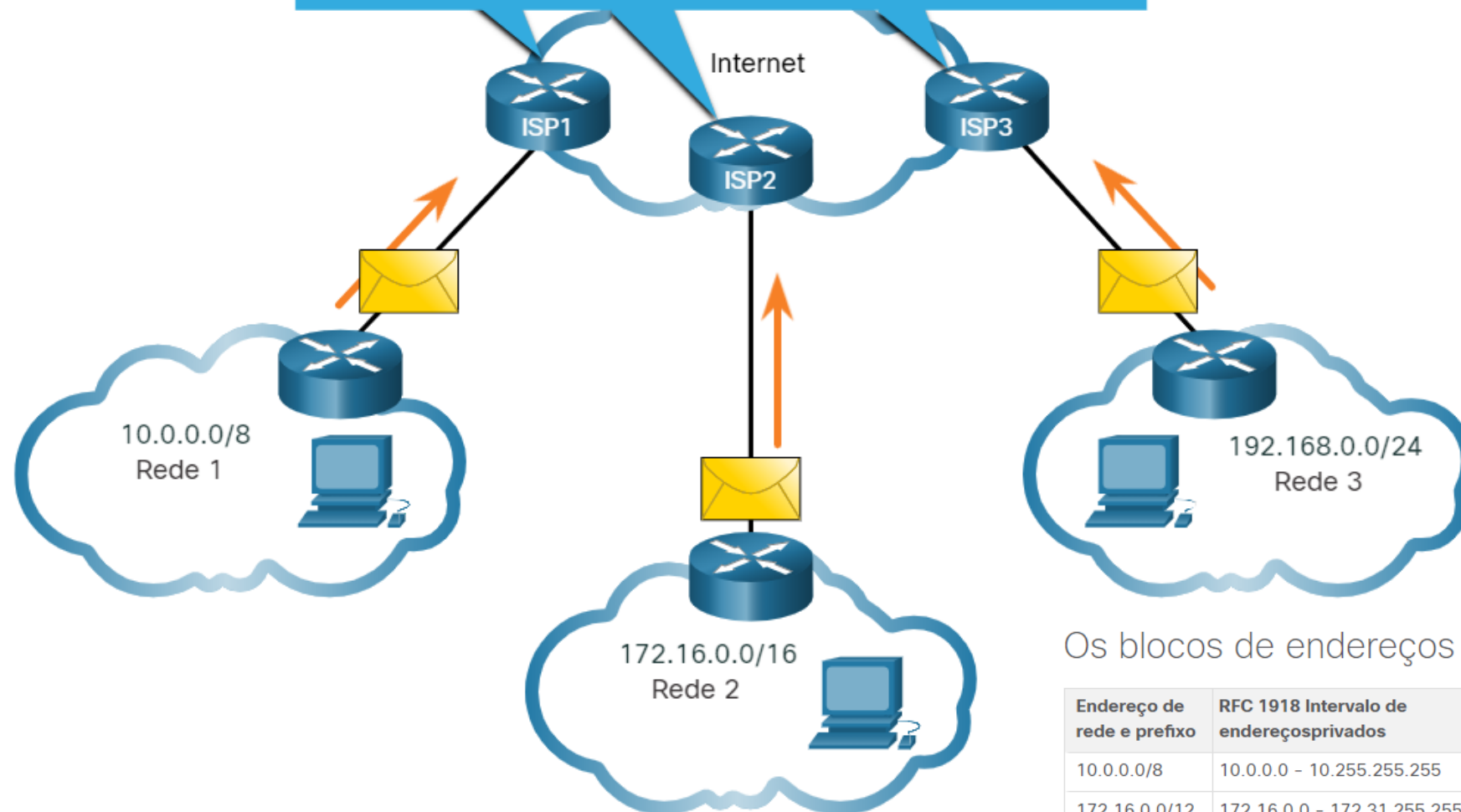
Classe A: intervalo de **10.0.0.0** a **10.255.255.255**

Classe B: intervalo de **172.16.0.0** a **172.31.255.255**

Classe C: intervalo de **192.168.0.0** a **192.168.255.255**

Roteamento para a Internet

Este pacote tem um endereço IPv4 de origem que é um endereço privado. Vou traduzi-lo para um endereço IPv4 público usando NAT

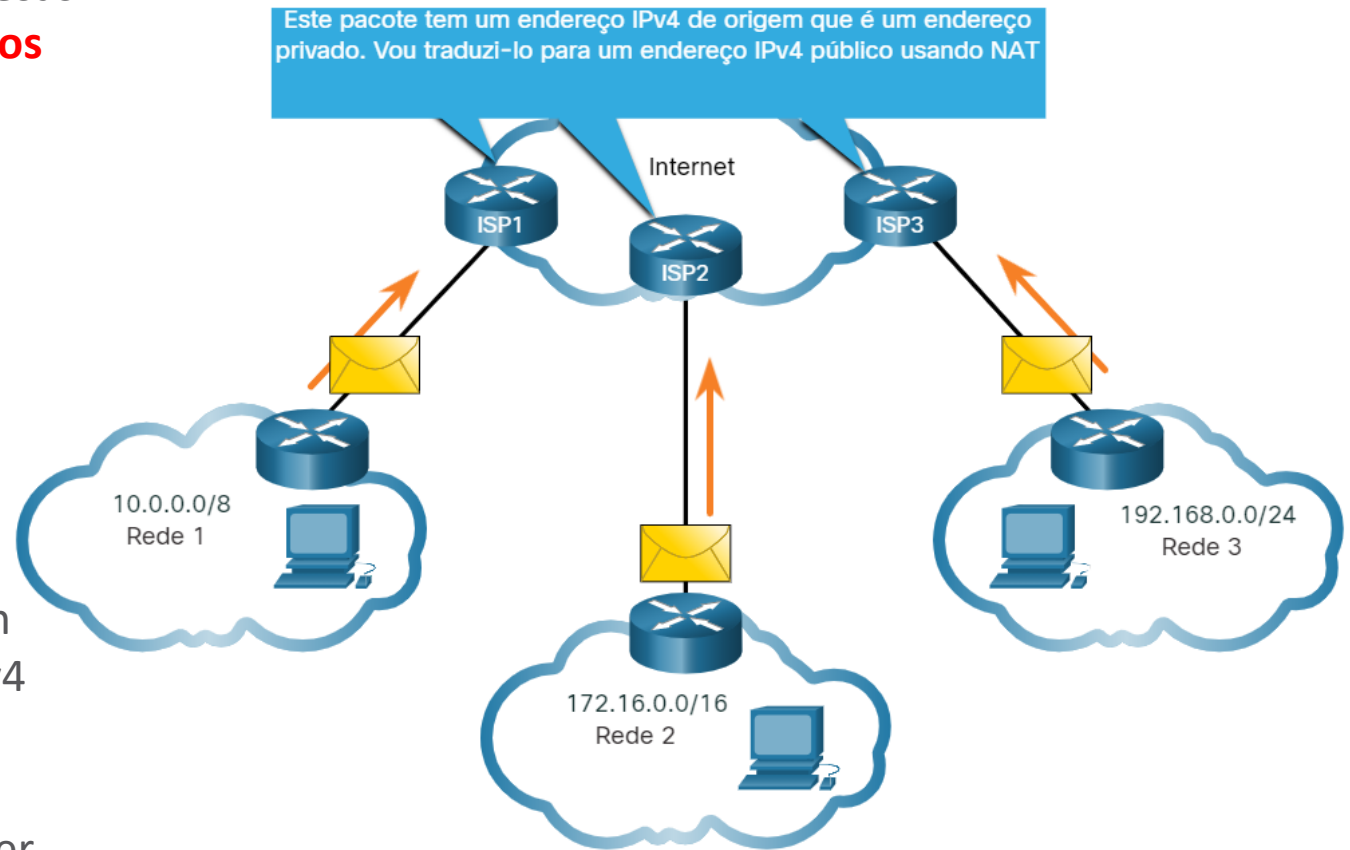


Os blocos de endereços privados

Endereço de rede e prefixo	RFC 1918 Intervalo de endereços privados
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

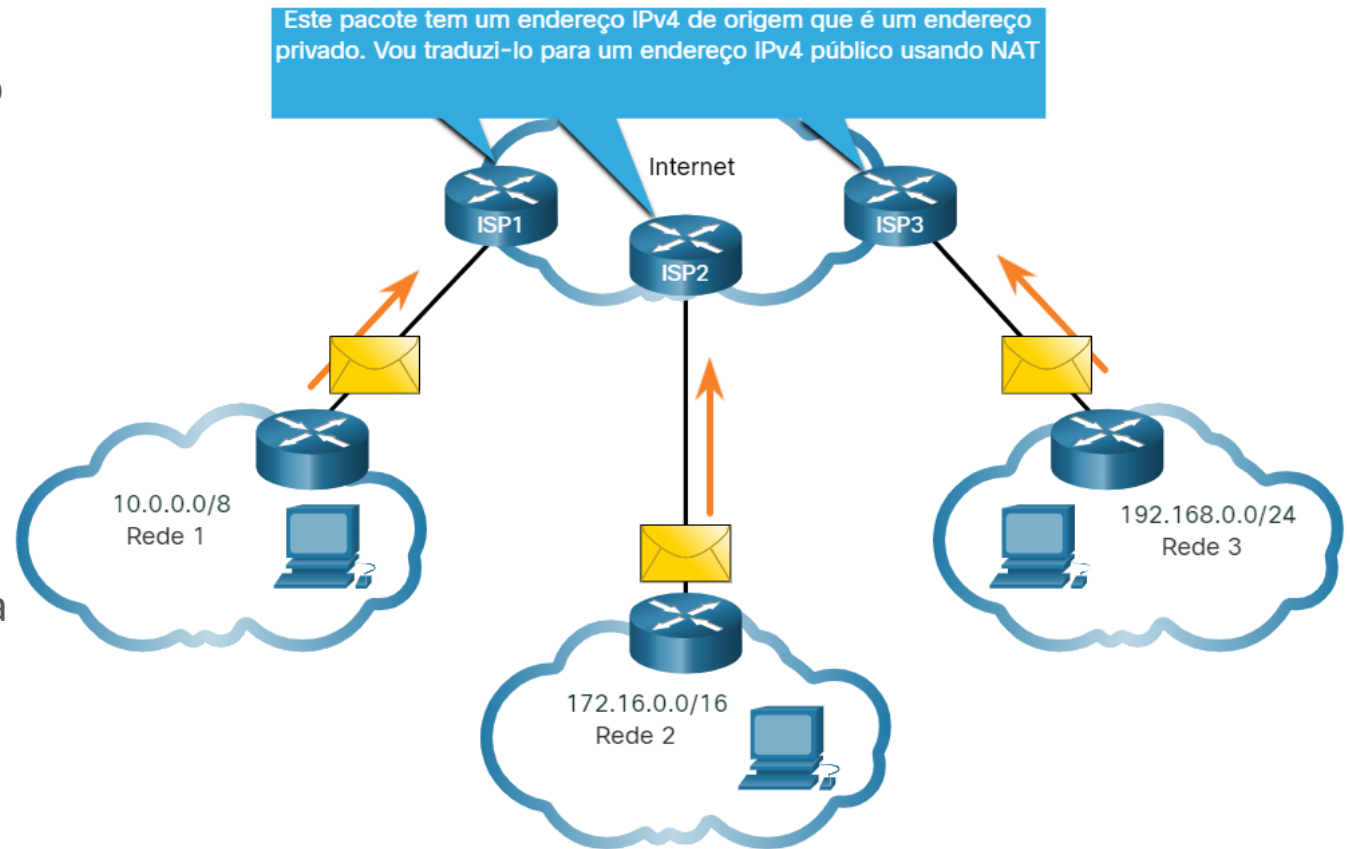
Roteamento para a Internet

- A maioria das redes internas, de grandes empresas a redes domésticas, **usa endereços IPv4 privados** para endereçar todos os dispositivos internos (intranet), incluindo hosts e roteadores.
- No entanto, **os endereços privados não são globalmente roteáveis**.
- Na figura, as redes de clientes 1, 2 e 3 estão enviando pacotes fora de suas redes internas.
- Esses pacotes têm um endereço IPv4 de origem que é um **endereço privado** e um endereço IPv4 de destino público (globalmente roteável).
- Os pacotes com um endereço privado devem ser filtrados (descartados) **ou traduzidos para um endereço público** antes de encaminhar o pacote para um ISP.



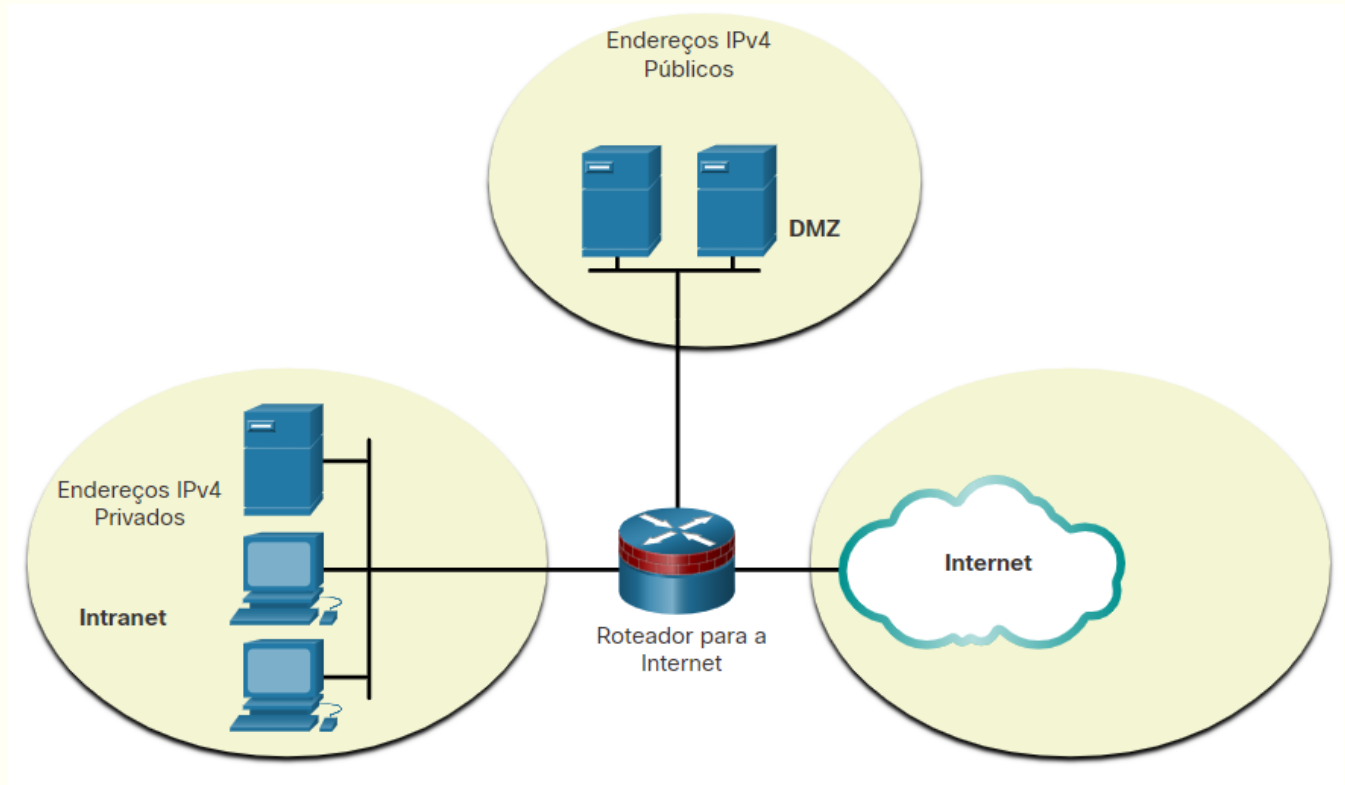
Roteamento para a Internet

- Antes que o ISP possa encaminhar esse pacote, ele deve traduzir o endereço IPv4 de origem, que é um endereço privado, para um endereço IPv4 público usando a Conversão de Endereços de Rede (NAT).
- O NAT é usado para converter entre endereços IPv4 privados e IPv4 públicos.
- Isso geralmente é feito no roteador que conecta a rede interna à rede ISP.
- Os endereços IPv4 privados na intranet da organização serão traduzidos para endereços IPv4 públicos antes do encaminhamento para a Internet.
- **Observação:** Embora um dispositivo com um endereço IPv4 privado **não seja diretamente acessível** a partir de outro dispositivo através da Internet, o IETF não considera endereços IPv4 privados ou NAT como medidas de segurança eficazes.



Roteamento para a Internet

- As organizações que têm recursos disponíveis para a Internet, como um servidor Web, também terão dispositivos com endereços IPv4 públicos.
- Como mostrado na figura, esta parte da rede é conhecida como a DMZ (zona desmilitarizada).
- O roteador na figura não só executa roteamento, mas também executa NAT e atua como um firewall para segurança.
- **Observação:** Endereços IPv4 privados são comumente usados para fins educacionais em vez de usar um endereço IPv4 público que provavelmente pertence a uma organização.



NAT (*Network Address Translation*)

Tradução de Endereços de Rede

- O RFC 1918 define um espaço de endereçamento privado permitindo a qualquer organização atribuir endereços IP aos computadores da sua rede interna sem correr o risco de provocar um conflito com um endereço IP público atribuído pelo IANA (*Internet Assigned Number Authority*).
 - *IANA*: órgão responsável pela coordenação global dos endereços da Internet (endereços IP roteáveis).
- Os endereços IP privados, não roteáveis, correspondem aos seguintes intervalos de endereços:

Classe A:	intervalo de	10.0.0.0	a	10.255.255.255
Classe B:	intervalo de	172.16.0.0	a	172.31.255.255
Classe C:	intervalo de	192.168.0.0	a	192.168.255.255
- Para as pequenas redes domésticas, a gama de endereços de rede de 192.168.0.0 a 192.168.255.0 é geralmente a mais utilizada.

NAT (*Network Address Translation*)

Tradução de Endereços de Rede

- Com o surgimento das redes privadas (que utilizam endereçamento IP privado) conectadas à Internet (que demanda endereçamento IP público), surgiu o problema de como os computadores pertencentes a esta rede privada poderiam receber as respostas aos seus pedidos feitos para fora da rede.
- Por se tratar de uma rede privada, os números de IP interno da rede (como **10.0.0.0/8**, **172.16.0.0/12** e **192.168.0.0/16**) nunca poderiam ser passados para a Internet pois não são roteados nela e o roteador que recebesse um pedido com um desses números não saberia para onde enviar a resposta. Sendo assim, os pedidos teriam de ser gerados com um IP global do roteador. Mas quando a resposta chegasse ao roteador, seria preciso saber a qual dos computadores presentes na LAN pertencia aquela resposta.
- A solução encontrada foi fazer um mapeamento baseado no IP interno (IP privado) com um endereço IP externo (IP público). A esse mecanismo deu-se o nome de NAT (*Network Address Translation*).

NAT (*Network Address Translation*)

Tradução de Endereços de Rede

- Como a Internet cresceu muito nos últimos anos de forma que os endereços IPv4 se tornaram escassos, o IANA já não possui mais endereços IPv4 para alocação, restando somente os estoques dos RIRs (*Regional Internet Registry*).
- Com a finalidade de reduzir a distribuição de endereços IPs públicos, foram desenvolvidas diversas soluções e o NAT é uma delas. Dispositivos configurados com NAT geralmente operam na borda de uma rede *stub* (rede que tem uma única conexão para a rede externa).
- Quando um pacote é roteado através de um dispositivo de rede, geralmente um firewall ou um roteador de borda, o endereço IP interno (privado) é traduzido para um endereço IP externo (público). Isso permite que o pacote seja transportado por redes públicas como a Internet. Em seguida, o endereço IP externo de resposta é retraduzido para o endereço IP interno que originou o pacote, para ser entregue dentro da rede interna.
- Assim, o NAT é um mecanismo que visa economizar endereços IP públicos e simplificar as tarefas de gerenciamento do endereçamento IP.

NAT (*Network Address Translation*)

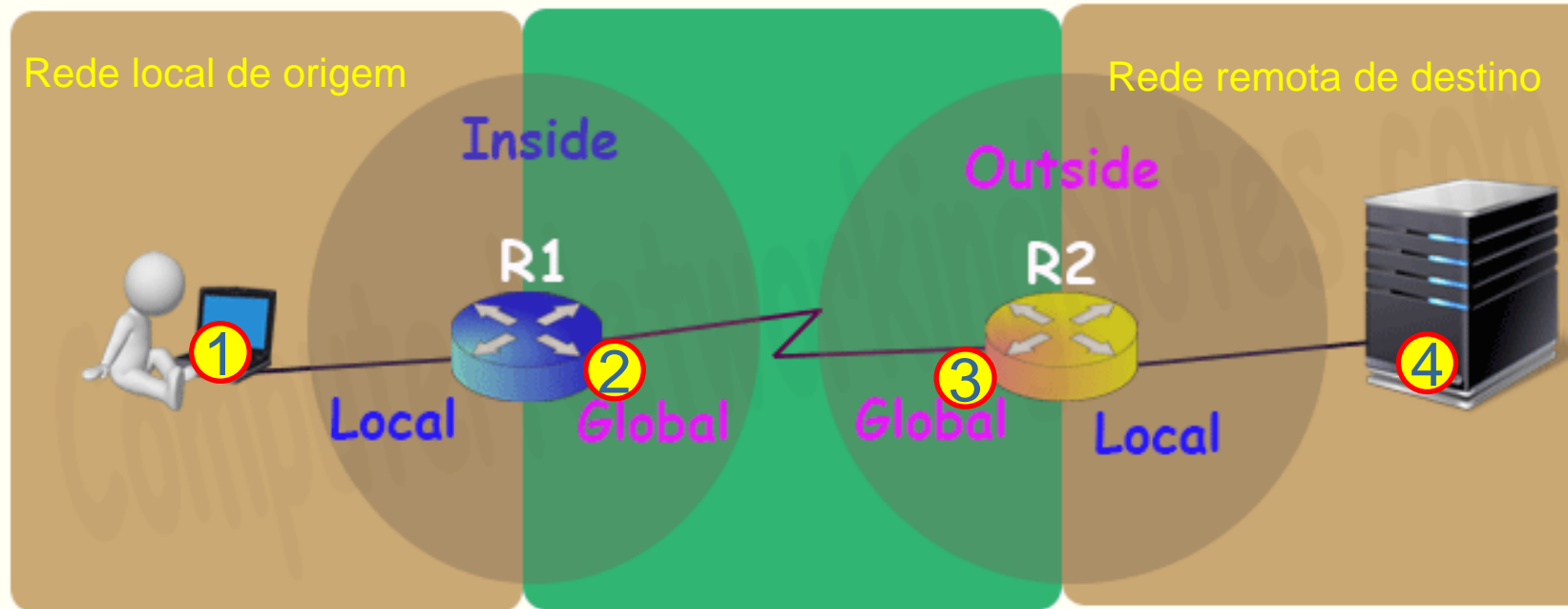
NAT foi criado com o objetivo principal de economizar endereços IPv4, uma vez que toda uma rede com endereços privados da RFC 1918 (**10.0.0.0 /8**, **172.16.0.0 /12** e **192.168.0.0 /16**) pode ter acesso à Internet através de apenas um (ou poucos) endereço(s) público(s).

NAT (*Network Address Translation*)

Tradução de Endereços de Rede

- A maioria dos NATs mapeiam vários hospedeiros privados para um endereço IP exposto publicamente. Em uma configuração típica, uma rede local usa uma das sub-redes de endereços IP "privados" (RFC 1918).
- Um roteador desta rede tem um endereço privado naquele espaço de endereços. O roteador também está conectado à Internet com um endereço "público" atribuído por um provedor de serviços de Internet.
- Quando o tráfego passa da rede local para a Internet, o endereço de origem em cada pacote é traduzido em tempo real de um endereço privado para o endereço público.
- O roteador rastreia dados básicos sobre cada conexão ativa (em particular o endereço de destino e porta). Quando uma resposta retorna ao roteador, ele usa os dados de rastreamento de conexões que armazenou durante a fase de saída para determinar o endereço privado na rede interna para encaminhar a resposta.

NAT (*Network Address Translation*)



Considerando o usuário do notebook, à esquerda da figura, temos:

	Termos	Descrição
1	Inside Local IP Address	Antes da tradução de um endereço IP de origem localizado dentro da rede local de origem
2	Inside Global IP Address	Depois da tradução do endereço IP de origem , fora da rede local do usuário
3	Outside Global IP Address	Antes da tradução do IP de destino, localizado fora da rede remota.
4	Outside Local IP Address	Depois da tradução do IP de destino, localizado dentro da rede remota

NAT (*Network Address Translation*)

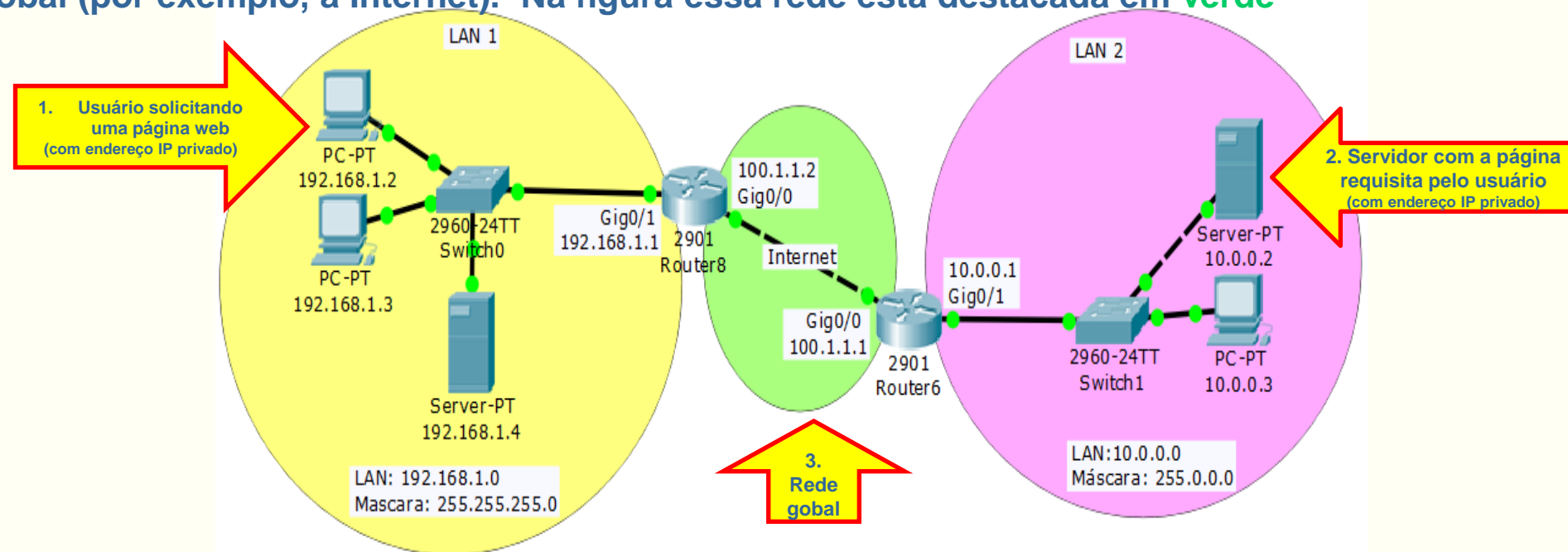
Tradução de Endereços de Rede

Os endereços IPs internos e externos são definidos por algumas nomenclaturas:

- **Endereço local interno:** Endereço IP atribuído a um host da rede interna. Definido pelo administrador da rede local e provavelmente um dos endereços privados especificados na RFC 1918.
- **Endereço global interno:** Endereço IP público atribuído pelo provedor de serviço. Este endereço pode representar um ou mais endereços IP locais internos para o mundo exterior.
- **Endereço global externo:** Endereço IP público atribuído a um host da rede externa pelo NAT dessa rede externa.
- **Endereço local externo:** Endereço IP privado de um host na rede externa, atribuído localmente e conhecido pelos hosts que estão na sua rede local.

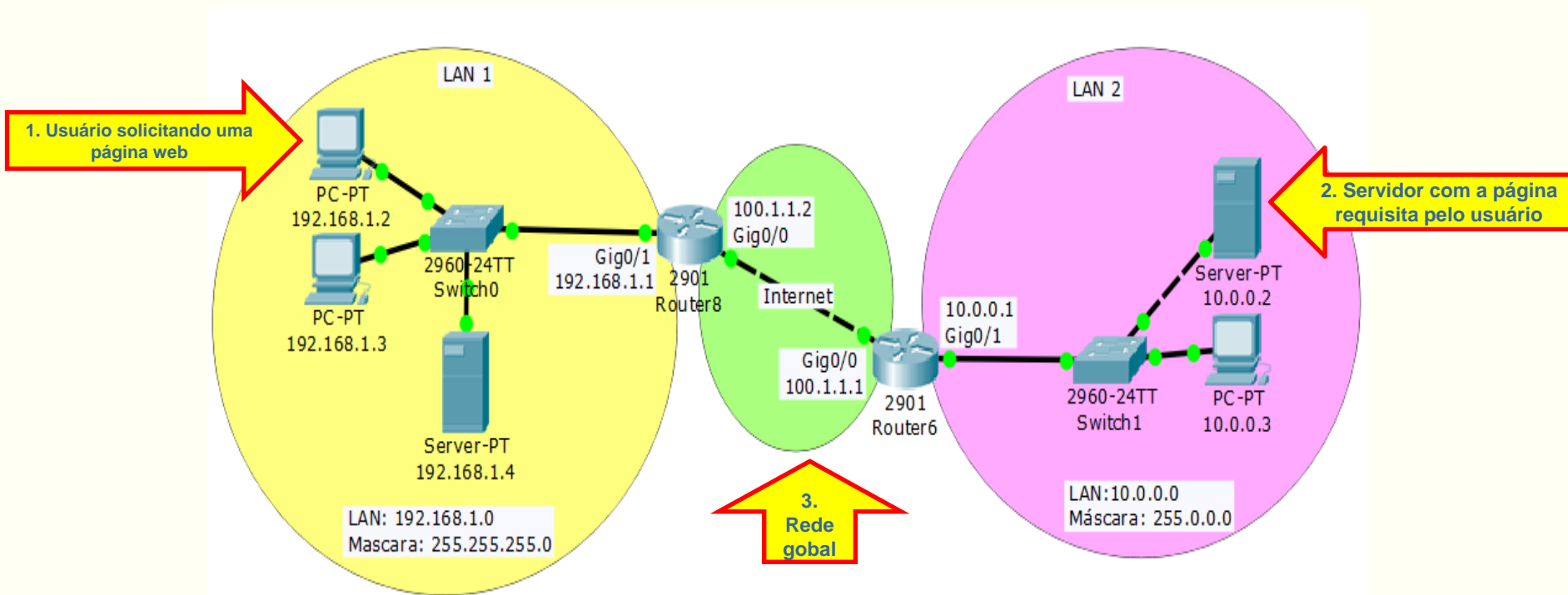
Um exemplo:

1. Suponha um usuário solicitando uma página WEB na Internet a partir de seu computador em sua empresa. A rede no qual ele está conectado é considerada uma rede interna (LAN) para ele. Na figura esta rede está destacada em **amarelo**.
2. Em nosso exemplo o servidor no qual ele busca a página está em uma rede externa. Entretanto, a rede onde está este servidor é uma outra rede local (LAN), diferente da rede do usuário. A rede onde está o servidor WEB é considerada a rede local daquele servidor WEB. Na figura essa segunda rede está destacado em **roxo**.
3. A rede que conecta os dois equipamentos (computador do usuário e o servidor remoto) pode ser uma rede Global (por exemplo, a Internet). Na figura essa rede está destacada em **verde**



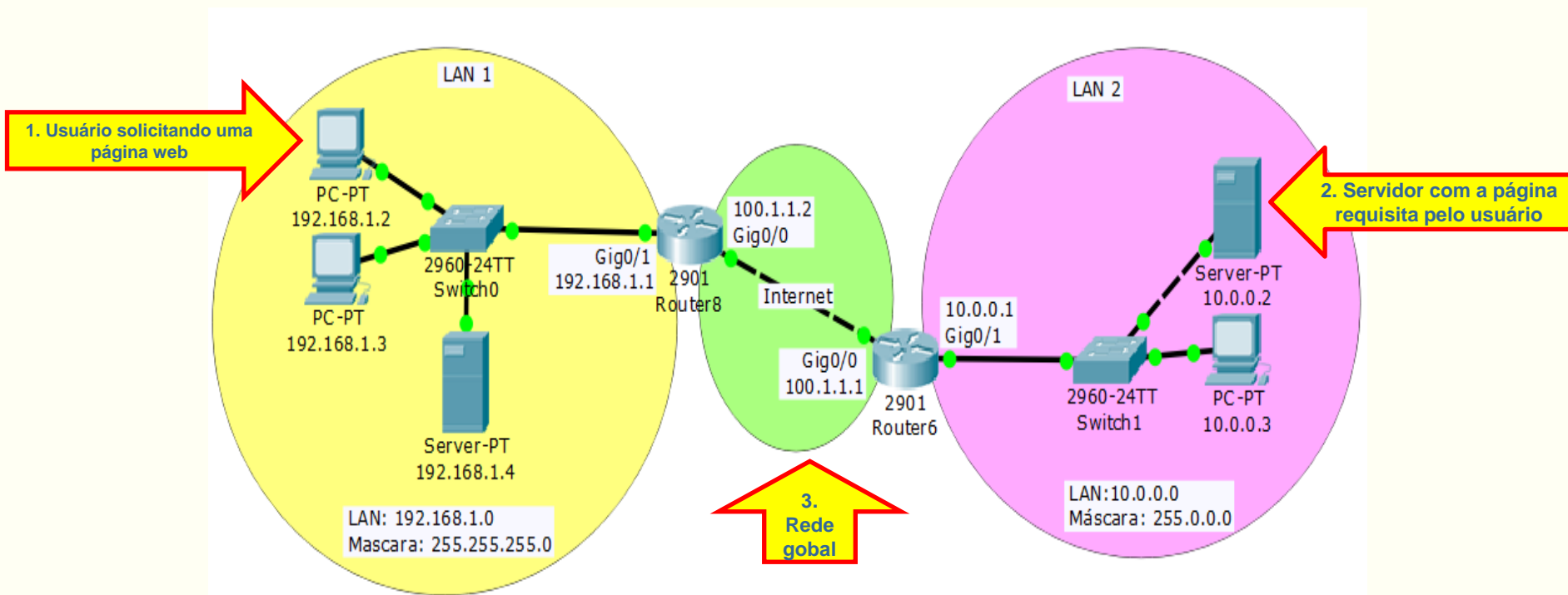
Definições NAT

- Do ponto de vista do usuário que utiliza o PC na rede LAN1, temos:
 - a interface do roteador ao qual se conecta a rede do usuário (o *gateway* para os equipamentos da rede local do usuário) será configurada com um inside local IP address.
 - a interface do roteador que se conecta à rede Global será configurada como inside global IP address.
 - assim, inside e outside depende de onde o usuário se encontra. No exemplo abaixo o usuário da LAN1, conecta-se ao router 8, que é inside. Desse ponto de vista, para o usuário o router6 é outside.



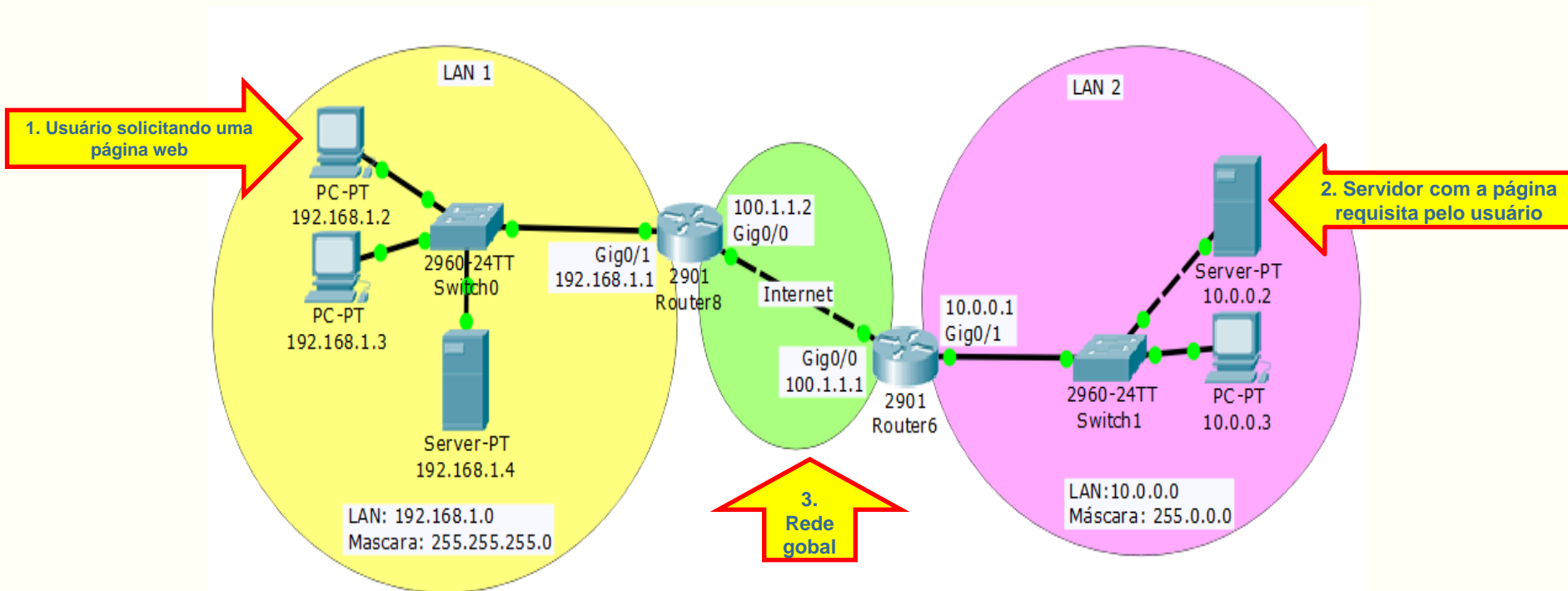
Definições NAT

Para o usuário no PC com IP 192.168.1.2, o Roteador **Router8** é **inside** e o Roteador **Router6** é **outside**;
Para o Webserver no IP 10.0.0.2, o Roteador **Router6** é **inside** e o Roteador **Router8** é **outside**.

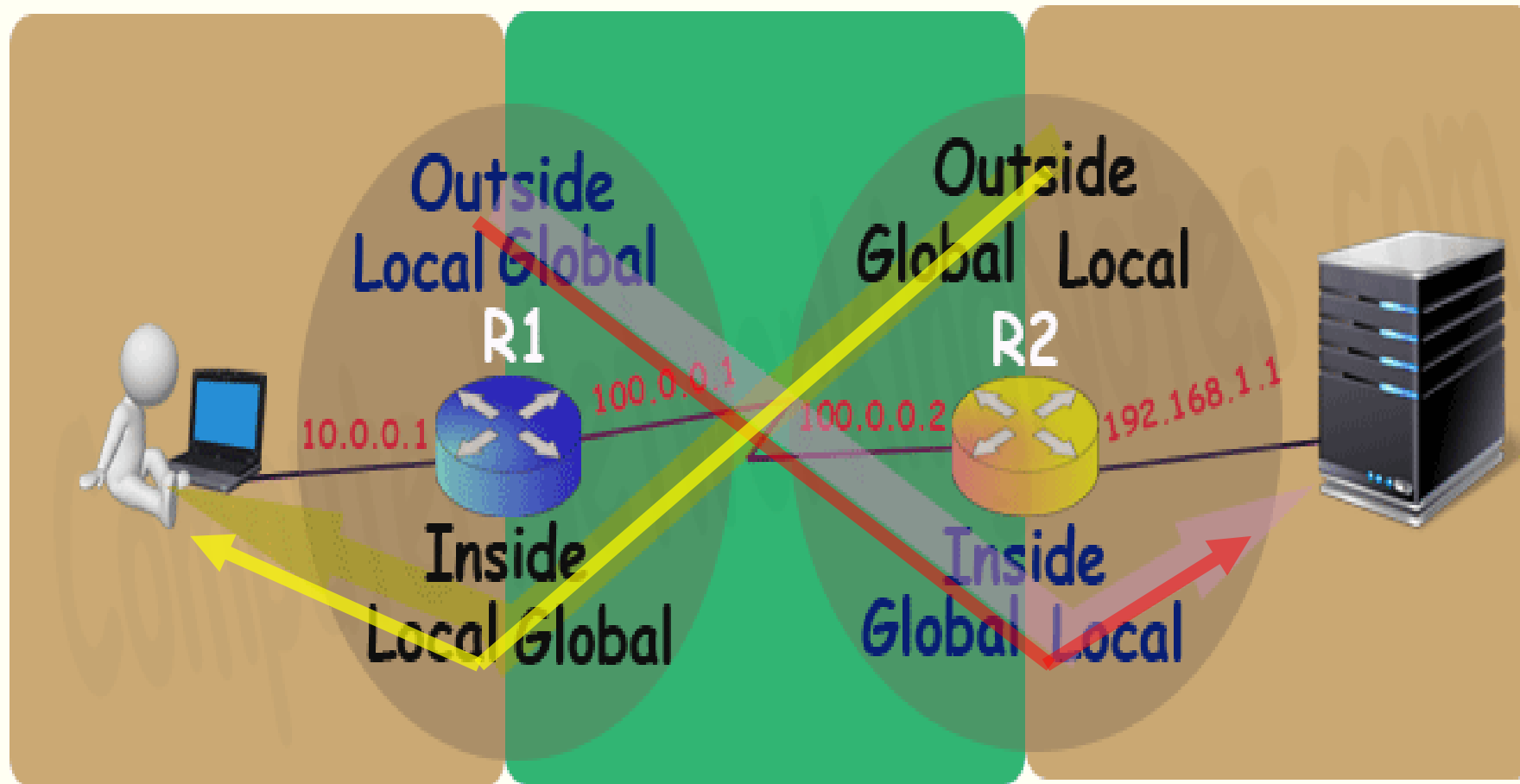


Definições NAT

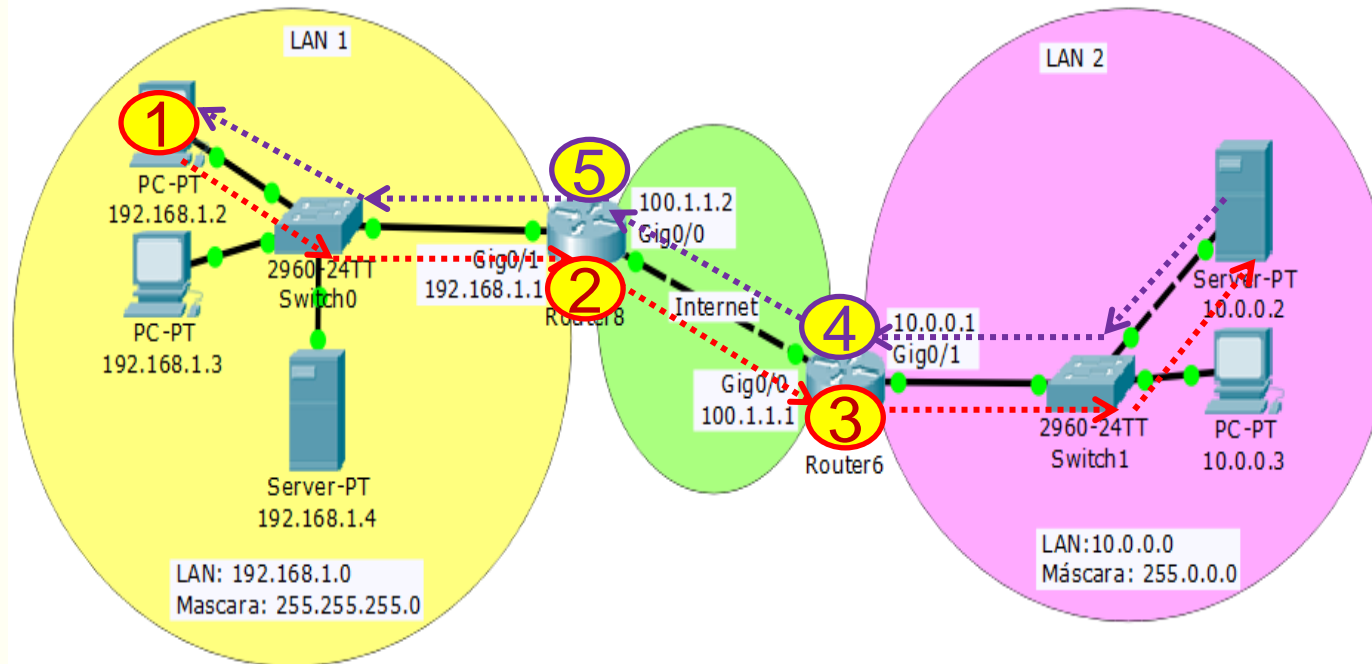
- No Router8 iremos configurar **inside local address** (192.168.1.1) e **inside global address** (100.1.1.2) o qual se tornará **outside local address** (192.168.1.1) and **outside global address** (100.1.1.2) para o Router6.
- Da mesma forma, no Router6 iremos configurar **inside local address** (10.0.0.1) e **inside global address** (100.1.1.1) o qual se tornará **outside local address** (10.0.0.1) e **outside global address** (100.1.1.1) para o Router8.
- Então, praticamente somente configuramos **inside local** e **inside global**. O que for **inside** para uma rede, será **outside** para a outra rede.



Definições NAT



NAT (Network Address Translation)



- Analisando o fluxo de dados da figura acima, percebe-se que o pacote no momento "1" sai da estação de trabalho com o endereço local interno "192.168.1.2" (um endereço IP privado) e em seguida, no momento "2", é traduzido para o endereço IP global interno "100.1.1.2" (um endereço público), isto permite que o pacote que saiu da estação de trabalho seja roteado através de uma rede pública e alcance seu destino, o endereço ip global externo "100.1.1.1".
- O endereço global externo será traduzido no momento "3" para o endereço ip local externo do servidor WEB "10.0.0.2".
- Quando o pacote retorna do servidor WEB, com o endereço IP de origem "10.0.0.2" (um endereço ip privado) , precisará ser traduzido, no momento "4", para um endereço IP público ("100.1.1.1"), levando o endereço IP de destino "100.1.1.2".
- No momento 5 o endereço IP de destino ("100.1.1.2") será retraduzido pelo roteador para a rede interna com o endereço IP local interno "192.168.1.2".
- O NAT permitiu que o pacote que foi originado na rede interna retornasse corretamente pois o endereço de origem "100.1.1.2", atribuído pelo processo de NAT no momento "2", é conhecido na rede pública, possibilitando o seu retorno. (Se o pacote levasse o endereço 192.168.1.0, não haveria retorno, pois sendo um endereço privado, a rede pública não o reconhece).

NAT (*Network Address Translation*)

- O NAT Tradicional é o método mais comum de utilização de tradução de endereços. Seu principal uso é traduzir endereços locais internos (privados) em endereços globais internos (públicos) para serem utilizados em uma rede externa.
- Em um NAT Tradicional as sessões são unidirecionais, somente no sentido de saída da rede privada, as sessões na direção oposta só podem ser realizadas utilizando mapeamento estático de endereço, direcionando o tráfego para os endereços locais internos selecionados ou métodos como o NAT Bidirecional.
- O NAT Tradicional é dividido em dois tipos: Basic NAT e o NATPT,
- Quando um dispositivo está utilizando o Basic NAT este fica limitado somente à tradução por meio de endereços IP, que podem ser realizados de maneira estática ou dinâmica, já com NATPT a sua operação é estendida para utilizar endereços IPs e portas (como o TCP / UDP ou ICMP query ID).

NAT (*Network Address Translation*)

- A tradução de um endereço privado num endereço público é então definido como NAT e está definido no [RFC 1631](#).
- Existem 3 tipos de NAT principais:
 - **NAT Estático** – Um endereço privado é traduzido num endereço público.
 - **NAT Dinâmico** – Existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
 - **NAT Overload (PAT)** – Esta é certamente a técnica mais usada. Um exemplo de PAT é quando temos 1 único endereço público e por ele conseguimos fazer sair várias máquinas (1:N). Este processo é conseguido, uma vez que o equipamento que faz PAT utiliza portas que identificam univocamente cada pedido das máquinas locais (ex: 217.1.10.1:53221 ou 217.1.10.1:53220) para o exterior.

NAT (*Network Address Translation*)

- **Basic NAT (Estático):** O NAT Básico Estático realiza o mapeamento de endereços IPs locais internos para endereços IPs globais internos, um endereço IP local interno sempre vai ter o mesmo endereço global interno (regra: um pra um). Este tipo de NAT é muito útil quando dispositivos da rede local interna precisam ser acessados pela Internet com um endereço consistente.
- **Basic NAT (Dinâmico):** O NAT Básico Dinâmico realiza o mapeamento de endereços IPs locais internos para endereços IPs globais internos de forma dinâmica. Qualquer endereço local interno pode ser traduzido para um range de endereços globais internos de forma dinâmica, diferentemente do Basic NAT (Estático) onde os endereços locais internos possuem sempre o mesmo endereço global externo. Este tipo de NAT também pode ser aplicado em conjunto com o NAT.

NAT (*Network Address Translation*)

- **PAT (*Port Address Translation*)**, NAT Overload ou NAPT (*Network Address Port Translation*) : realiza o mapeamento utilizando números de portas (como o TCP / UDP ou ICMP query ID) de origem dos endereços locais internos, para distinguir cada uma das traduções.
- Esse método tenta preservar a porta de origem, se essa porta de origem já estiver em uso, o NAT atribui o primeiro número de porta disponível a partir do início do grupo de portas apropriadas:
 - 0-511, 512-1023 ou 1024-65535.
- Quando não há mais portas disponíveis e há mais de um endereço global interno configurado, passa-se para o próximo endereço IP, para tentar alocar novamente a porta de origem, esse processo continua até que não haja mais portas disponíveis nem endereços globais internos.
- O método permite que vários endereços locais internos sejam traduzidos usando um único endereço global interno, permitindo assim que se tenham diversos dispositivos em uma rede interna utilizando um único global interno.

NAT (*Network Address Translation*)

- Também é possível localizar outros tipos de NAT como o *Bi-Directional NAT*, *Twice NAT* e o *NAT-PT*.
 - **Twice NAT (2x NAT):** Este tipo de NAT permite que você decida qual endereço IP global interno será utilizado no processo de tradução, baseado no endereço IP de destino ou pelo número da porta de destino do pacote.
 - Você pode criar regras para determinar que um endereço IP de origem deverá ser traduzido para o endereço IP “A” quando for para o destino “1”, ou traduzido para o endereço IP “B” quando for para o destino “2”.
 - No caso de portas, você pode determinar que um endereço IP de origem com uma porta de destino “80” deverá ser traduzido para o endereço “A” ou traduzido para o endereço “B” quando tiver a porta de destino “23”.

NAT (*Network Address Translation*)

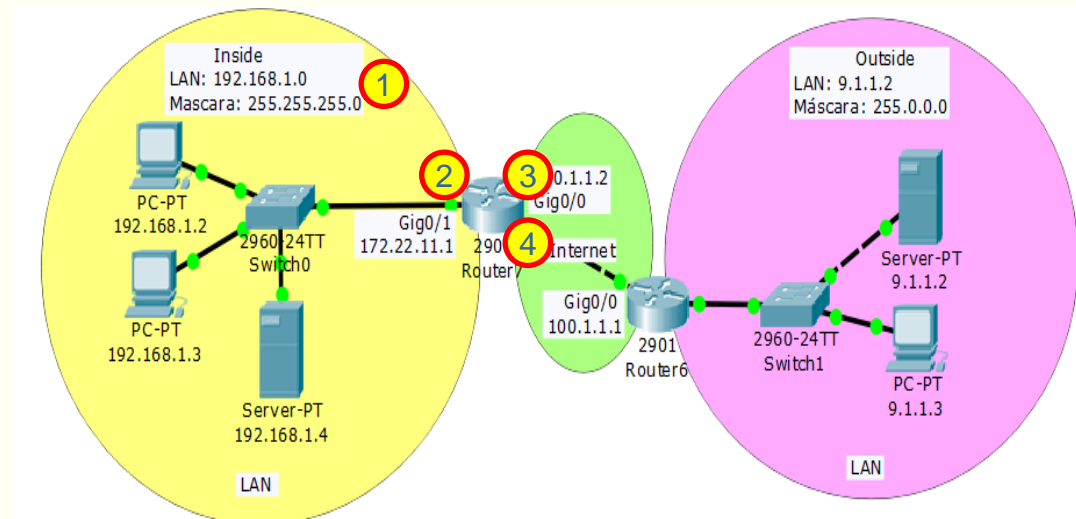
- **Bi-Directional NAT (ou two-way):** Com o NAT bidirecional as sessões podem ser iniciadas a partir de hosts na rede pública. Esta característica foi incorporada no NAT Básico para adicionar capacidades mais avançadas. Quando o NAT é somente de saída, as transações se tornam mais difíceis, hosts da rede interna (endereço local interno) geralmente sabem os endereços IPs de hosts da rede externa (endereço global externo), porque estes são públicos. Entretanto, os hosts das redes externas não sabem o endereço IP de hosts da rede interna, então se um host estiver na rede externa, ele não vai poder especificar um endereço IP de um servidor ou dispositivo que esteja em uma rede interna para enviar um pacote. O endereço IP do host interno não é roteável em redes públicas.
- Como exemplos de NAT bidirecional podemos citar os túneis IPv6 e a utilização de serviços DNS (*Domain Name System*) em redes internas.
- Em túneis IPv6 (será abordado em outra sessão deste site), o mesmos poderão ser estabelecidos mesmo quando não houver tráfego interno sendo gerado para a extremidade do túnel.
- Para os serviços de DNS, os servidores em redes internas podem responder requisições para hosts na rede pública. Quando um host externo tenta resolver o nome de um host onde o servidor de DNS está dentro de uma rede interna, o roteador NAT intercepta a solicitação de DNS e instala uma tradução de endereços para permitir que o host externo possa alcançar o servidor de DNS utilizando um endereço IP global interno (público).
- O mapeamento dinâmico citado acima, depende a utilização de DNS-ALG (*Application Level Gateway*).

NAT (*Network Address Translation*)

- **NAT-PT: O NAT-PT** (*Network Address Translation - Protocol Translation*) é uma técnica de tradução de endereços entre redes IPv6 e IPv4, onde pacotes IPv6 são traduzidos em pacotes IPv4 e vice-versa.
- Este método pode ser utilizado quando equipamentos legados não permitirem o upgrade para utilização de endereços IPv6. Esta técnica de tradução nada mais é do que uma extensão das técnicas de NAT já citadas acima.

NAT (*Network Address Translation*)

- A maioria dos NATs mapeiam vários hospedeiros privados para um endereço IP exposto publicamente.
- Em uma configuração típica:
 1. uma rede local usa uma das sub-redes de endereços IP "privados" (RFC 1918).
 2. um roteador desta rede tem um endereço privado naquele espaço de endereços.
 3. o roteador também está conectado à Internet com um endereço "público" atribuído por um provedor de serviços de Internet.
 4. quando o tráfego passa da rede local para a Internet, o endereço de origem em cada pacote é traduzido em tempo real de um endereço privado para o endereço público.
 5. o roteador rastreia dados básicos sobre cada conexão ativa (em particular o endereço de destino e porta).
 6. quando uma resposta retorna ao roteador, ele usa os dados de rastreamento de conexões que armazenou durante a fase de saída para determinar o endereço privado na rede interna para encaminhar a resposta.

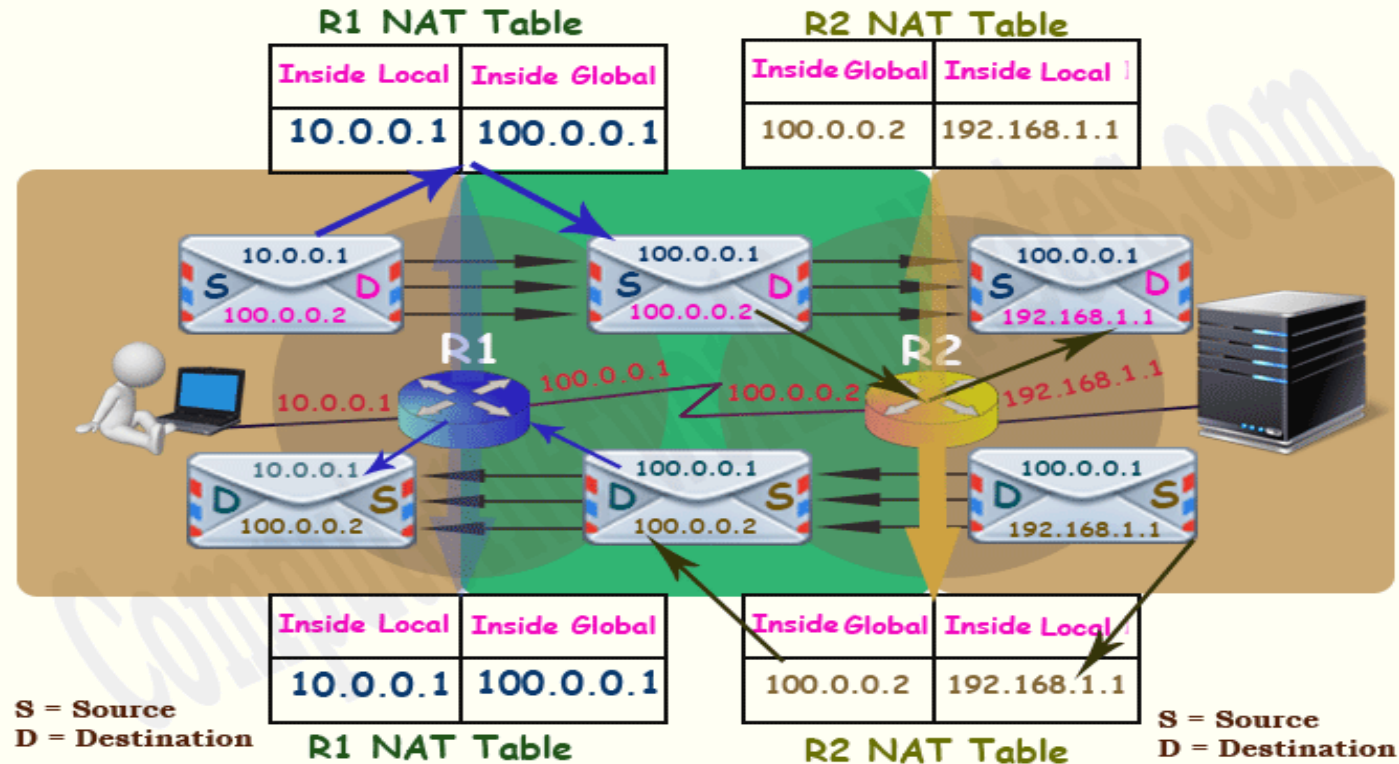


Exemplos de situações para uso de NAT

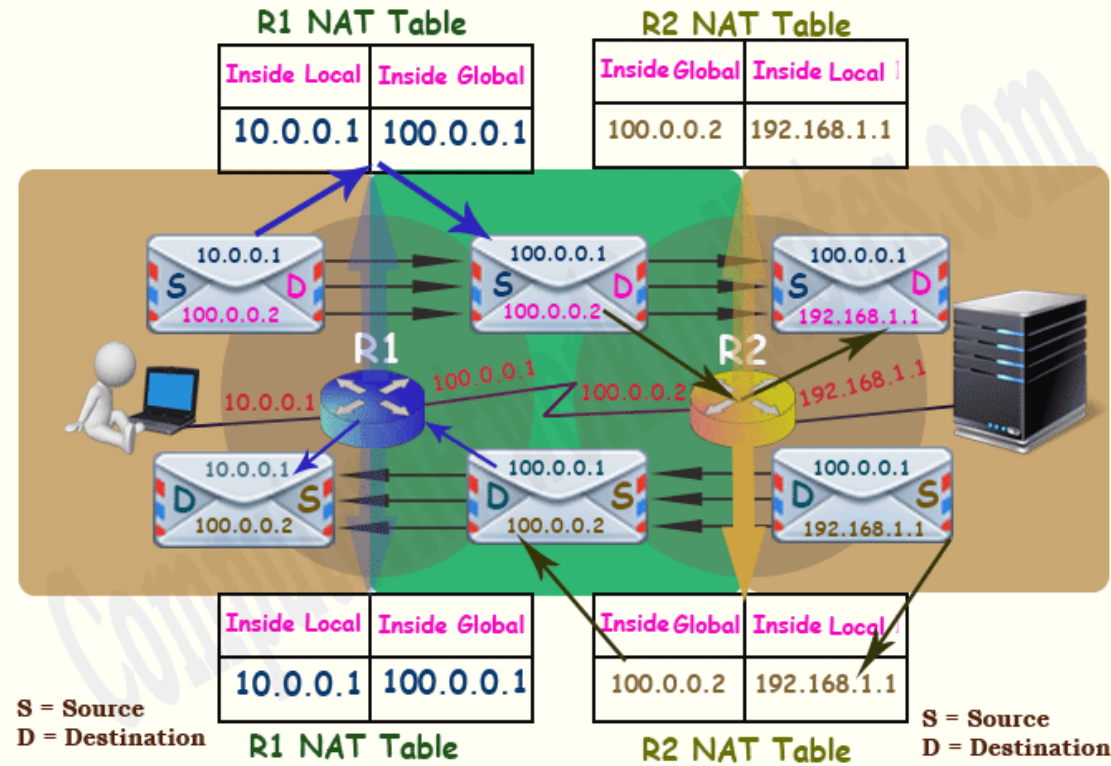
- Não há uma regra rígida sobre quando deve-se utilizar ou não o NAT. Os requerimentos de uma rede para o uso de NAT são as seguintes situações:
 - Os equipamentos de uma rede interna configurados para utilizar endereço IP privado precisam-se conectar à internet.
 - Para conectar-se à internet estes equipamentos precisarão de um endereço IP público. Nesta situação pode-se utilizar o NAT para traduzir endereços IP privados em endereços IP públicos (e o processo inverso quando chegar uma resposta).
 - Duas redes utilizando endereço IP serão unificadas.
 - Nesta situação o NAT pode ser utilizado para evitar sobreposição (repetição) de endereçamento IP.
 - Na necessidade de conexão de diversos equipamentos com a internet por meio de um único (ou um número menor) de endereços públicos.
 - Nesta situação o NAT é utilizado para traduzir múltiplos endereços IP privados em um único (ou um número menor) de endereço IP privado.

Como o NAT funciona 1/5

- Para entender como NAT funciona, observe o exemplo a seguir.
 - Neste exemplo um usuário está acessando um servidor WEB
 - O usuário e o servidor WEB estão utilizando endereços IPs privados que não são roteáveis na Internet.
 - O usuário e o servidor WEB estão conectados à Internet utilizando NAT.
- A figura ilustra o funcionamento de NAT neste exemplo:

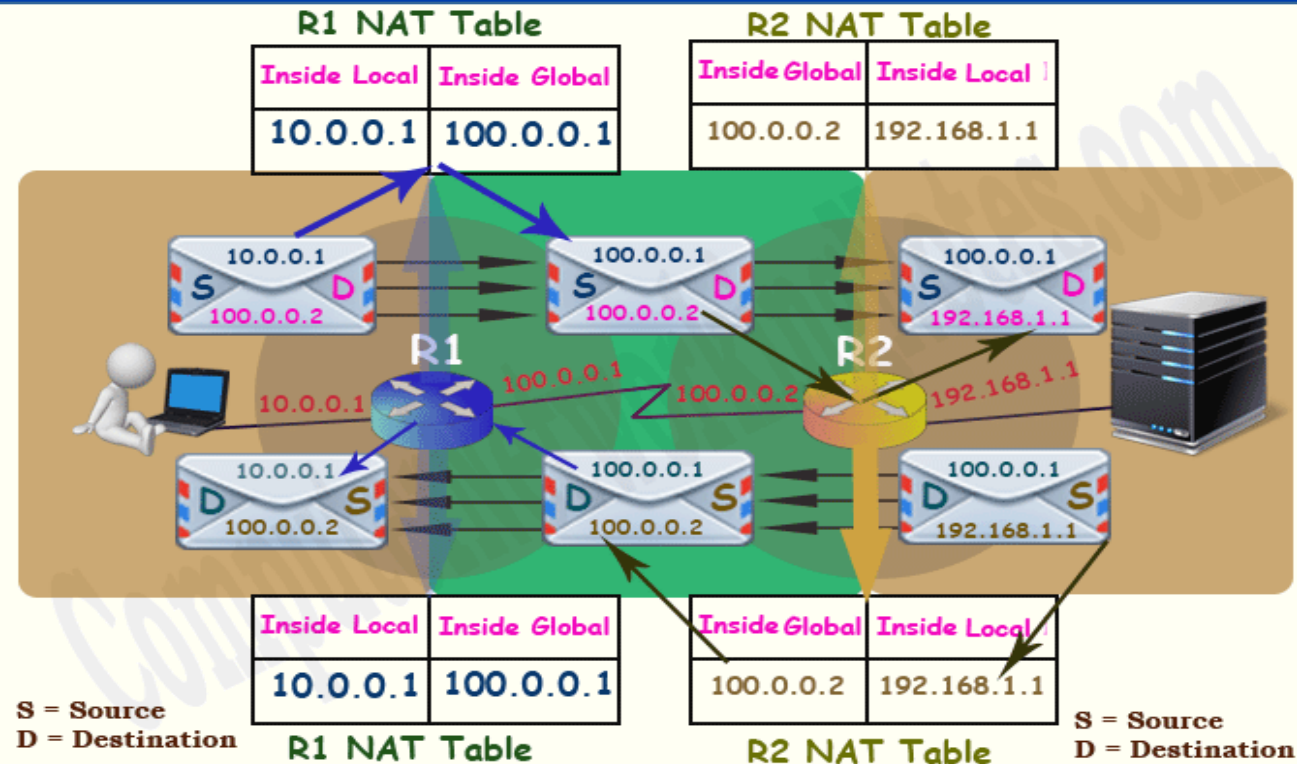


Como o NAT funciona 2/5



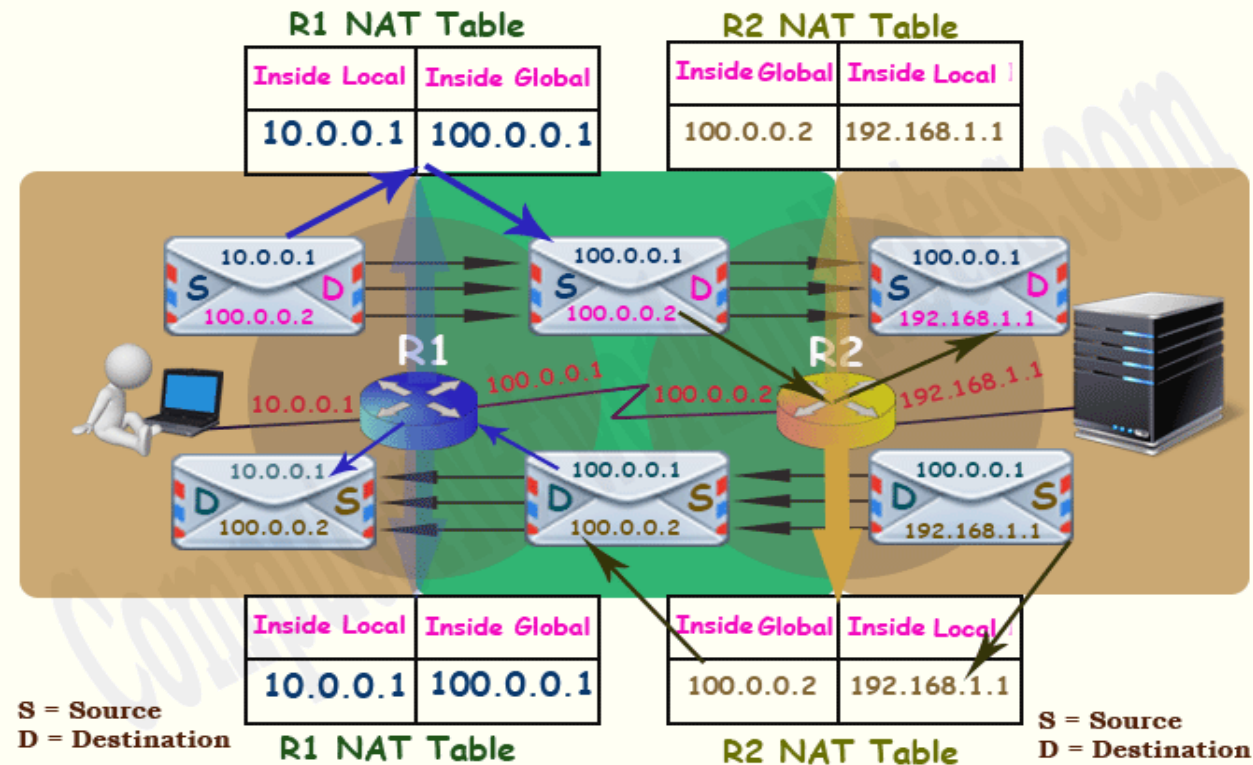
- O equipamento do usuário possui endereço IP 10.0.0.1 e o WebServer IP 192.168.1.1, ambos endereços IP privados.
- O usuário gera pacotes de dados com requisição ao Webserver, mas endereçados à interface do roteador da rede de destino (100.0.0.2), que possui um endereço privado. Estes pacotes possuem endereço de origem 10.0.0.1 e endereço de destino 100.0.0.2 (a porta do roteador da rede de destino)
- Isso ocorreu porque quando o equipamento do usuário precisou se conectar ao Webserver o DNS informou que o endereço IP do Webserver é a porta do roteador, que possui endereço público e está configurado para realizar NAT.
- Uma vez que o Webserver possui endereço privado, usuários externos à rede desse Webserver só poderão se conectar a ele por meio do endereço IP informado pelo DNS (que é um IP público): a porta do roteador que irá realizar NAT para o endereço IP privado do Webserver.
- Por esta razão o pacote de destino possui o endereço IP 100.0.0.2 ao invés de 192.168.1.1.

Como o NAT funciona 3/5



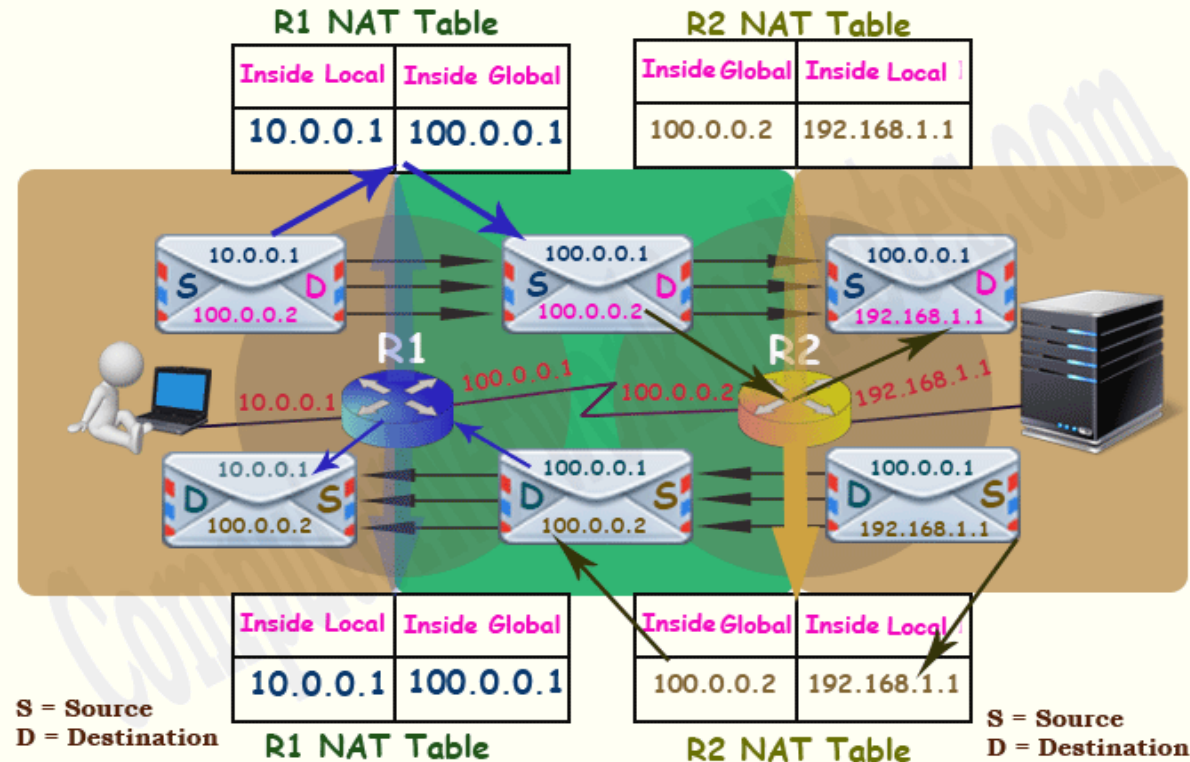
- A requisição irá alcançar o roteador R1. Uma vez que os pacotes contém um endereço IP privado como origem, que não é roteável na Internet, R1 precisará traduzi-lo (NAT) para um endereço IP público, roteável na Internet, antes de encaminhar este pacote à Internet.
- R1 verifica a tabela NAT à procura de um endereço IP público. Dependendo do tipo de NAT (*Static, Dynamic ou PAT*) será realizada uma troca do endereço IP de origem (privado) para um endereço IP público que consta nessa tabela.
- No exemplo, 100.0.0.1 é o endereço IP privado escolhido. R1 irá trocar 10.0.0.1 por 100.0.0.1 e encaminhar o pacote ao roteador R2.

Como o NAT funciona 4/5



- R2 receberá o pacote e irá ler o endereço IP de destino.
- R2 verificará a tabela NAT para encontrar o endereço IP privado correspondente ao destino. Uma vez que a tabela NAT de R2 tem o mapeamento do endereço 100.0.0.2 (público) para 192.168.1.1 (privado), R2 irá trocar o endereço de destino de 100.0.0.2 para 192.168.1.1 e encaminhar o pacote para a rede interna.
- O Webserver irá processar o pacote e irá responder com outros pacotes. Os pacotes agora possuirão endereço de origem 192.168.1.1 e endereço de destino 100.0.0.1.
- *Uma vez que o Webserver recebeu os pacotes de 100.0.0.1 ele irá responder a este endereço ao invés de responder a 10.0.0.1.*

Como o NAT funciona 5/5



- R2 recebe o pacote e antes de encaminhá-lo à Internet R2 irá trocar o endereço IP de origem por um endereço em sua tabela NAT. No exemplo 192.168.1.1 será trocado por 100.0.0.2.
- R1 receberá o pacote e verifica o endereço de destino. R1 irá fazer uma consulta em sua tabela NAT e descobrir que o endereço IP de destino está associado a 10.0.0.1. Uma vez que o endereço IP de destino 100.0.0.1 está mapeado para 10.0.0.1, R1 irá trocar o endereço 100.0.0.1 para 10.0.0.1 e encaminhar o pacote para rede interna.
- Do ponto de vista do usuário, o endereço IP do Webserver é 100.0.0.2. Enquanto que do ponto de vista do Webserver o o endereço IP do usuário é 100.0.0.1. Dessa forma, nenhum equipamento conhece exatamente com qual equipamento final esta trocando informações.

Vantagens e Desvantagens do uso de NAT

- **Vantagens:**

- NAT resolve questões de sobreposição de endereço IP.
- NAT oculta a estrutura interna de endereçamento IP do mundo externo.
- NAT permite a conexão com qualquer rede com a troca automática de IP privado para IP público
- NAT permite a conexão de múltiplos computadores com a Internet utilizando um único endereço IP privado.

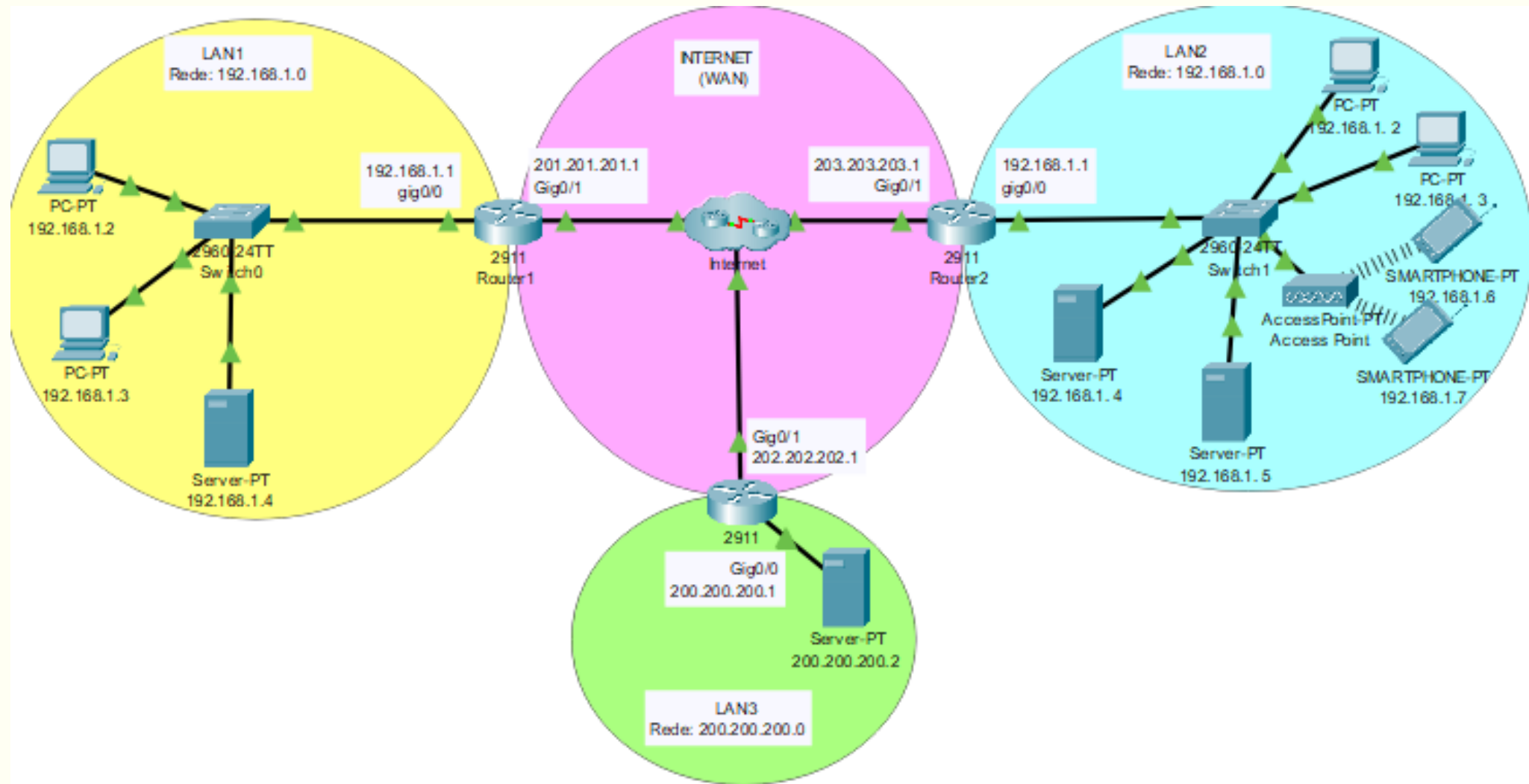
- **Desvantagens:**

- NAT adicionará um atraso (*delay*) na rede;
- Algumas aplicações não são compatíveis com NAT
- O rastreamento fim-a-fim com endereçamento IP não será possível com o
- NAT ocultará o endereço do dispositivo final.

Introdução ao NAT

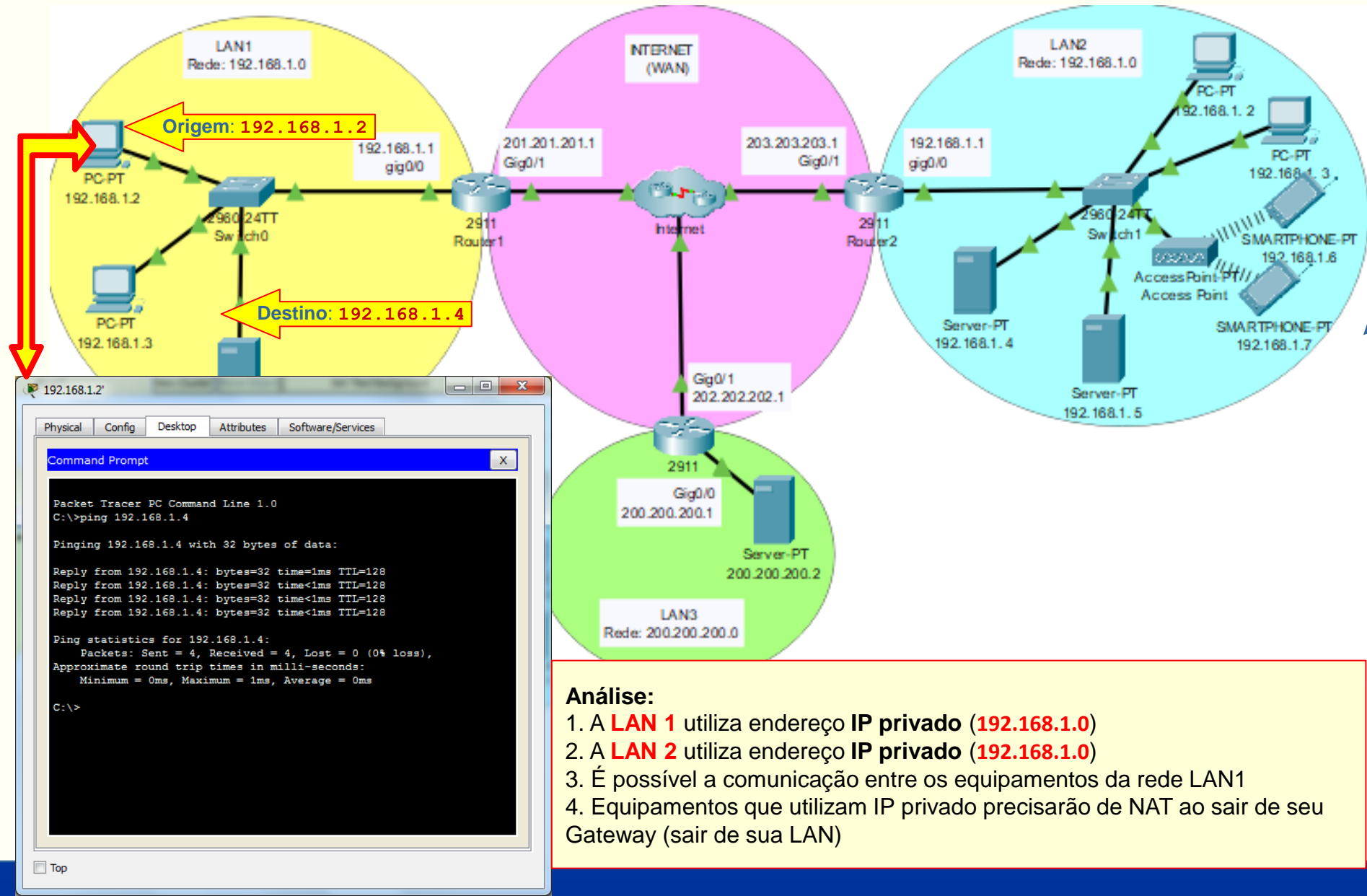
(Network Address Translation)

Analise a topologia a seguir



Arquivo: 2oSEM Aula 09 2022 - NAT.pkt

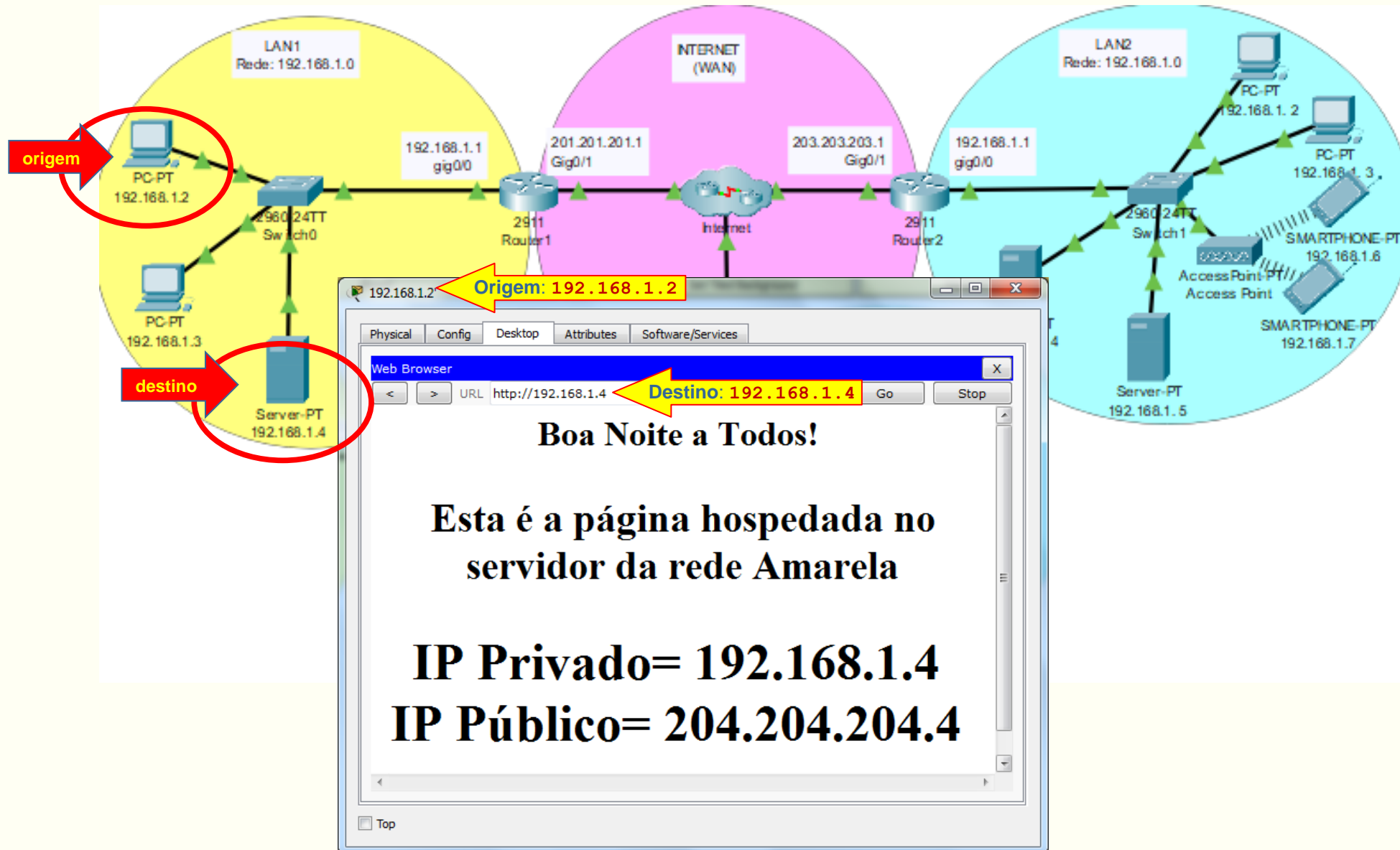
Analise a topologia a seguir:



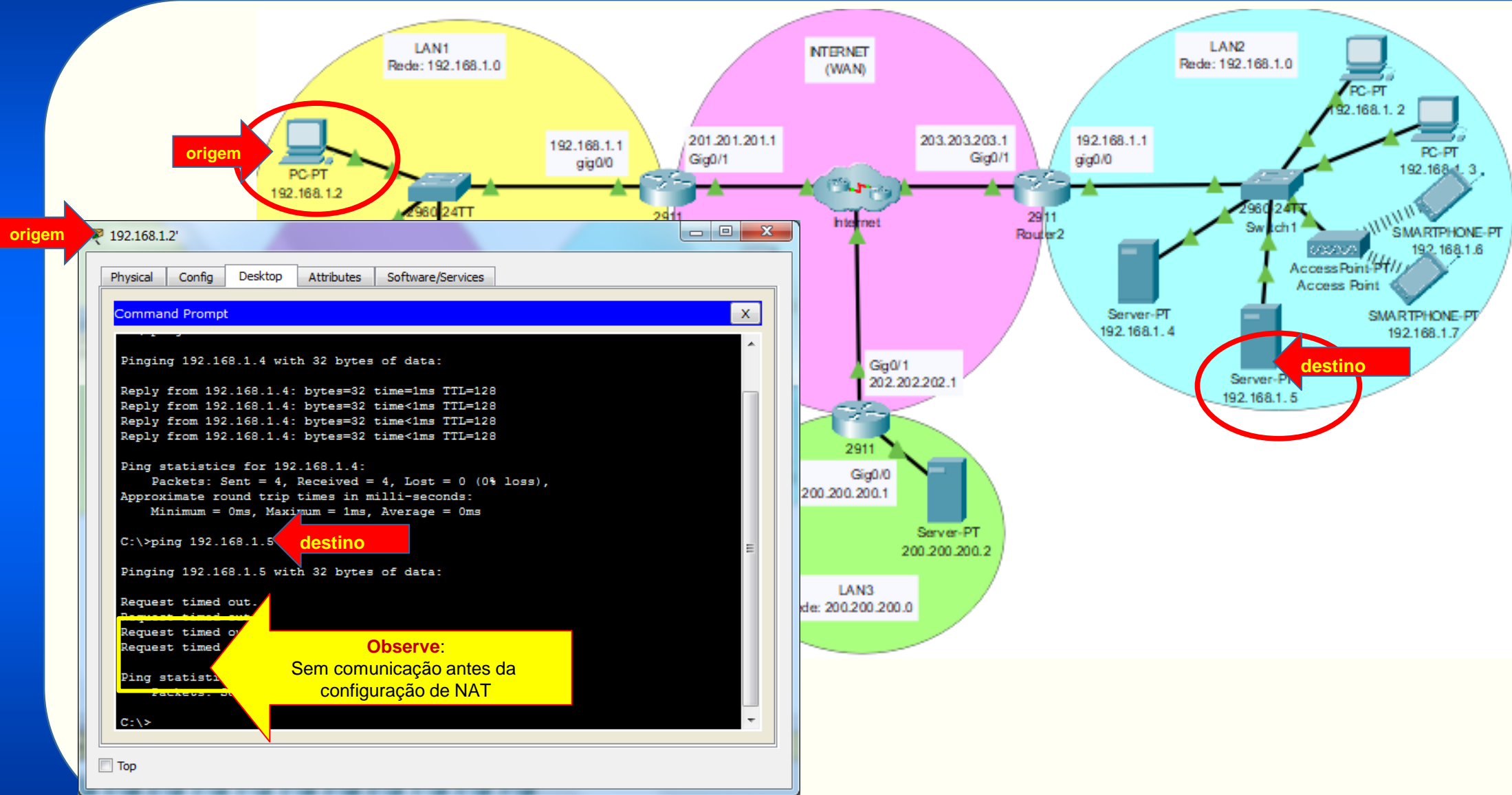
Análise:

1. A **LAN 1** utiliza endereço IP privado (**192.168.1.0**)
2. A **LAN 2** utiliza endereço IP privado (**192.168.1.0**)
3. É possível a comunicação entre os equipamentos da rede LAN1
4. Equipamentos que utilizam IP privado precisarão de NAT ao sair de seu Gateway (sair de sua LAN)

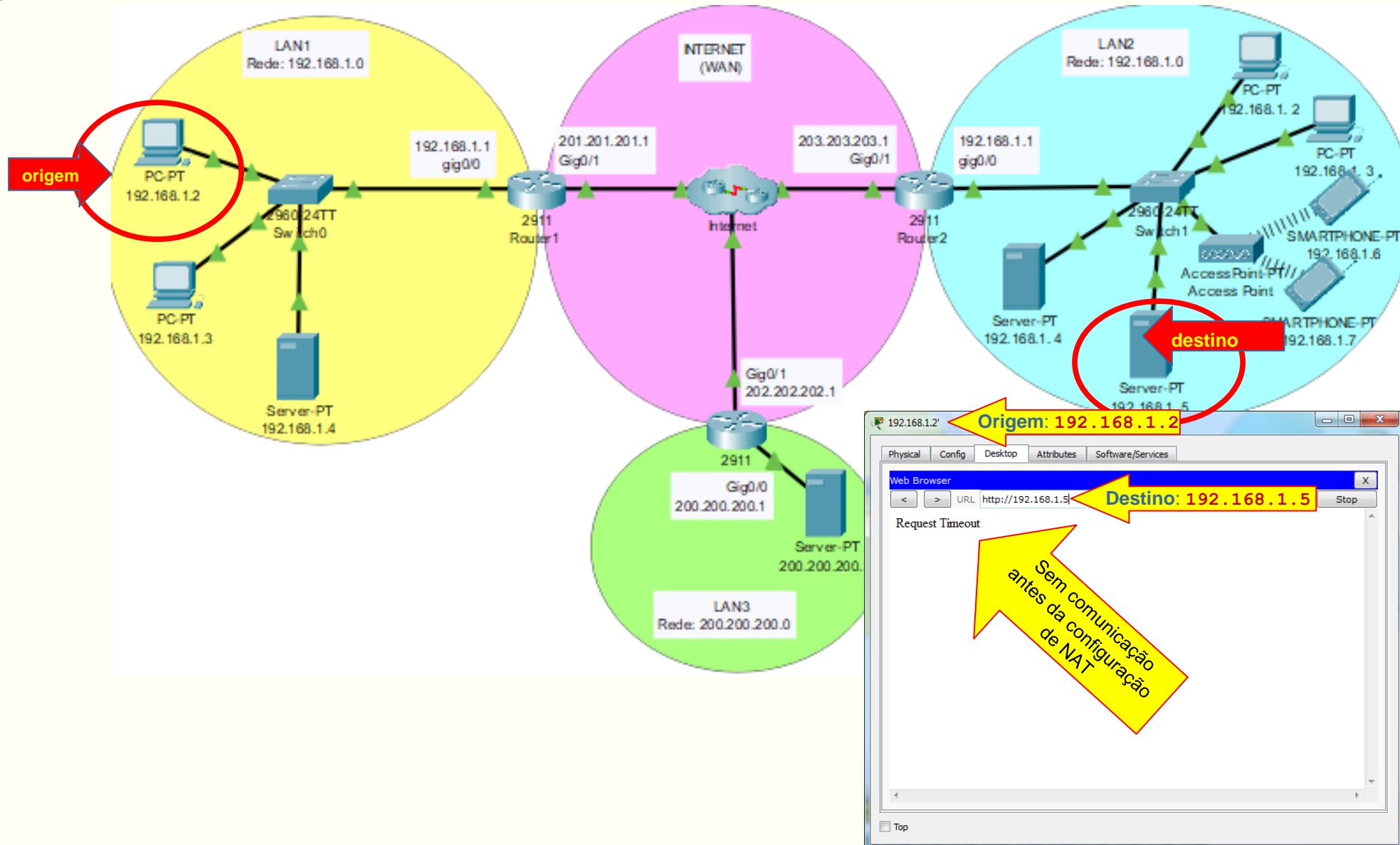
Analise a topologia a seguir



Analise a topologia a seguir



Analise a topologia a seguir



Camada de Rede

Network Address Translation (NAT)

Configuração *Static NAT*

Configuração de *Static NAT*

Uma vez que static NAT utiliza “tradução manual” (definida em configuração direta no roteador, teremos que fazer um mapeamento de cada inside local IP address (endereço IP interno, geralmente um endereço IP privado) que precisa de tradução para um inside global IP address (que será sempre um endereço IP público)

O seguinte comando é usado para mapear um **inside local IP address** para um **inside global IP address**:

```
Router(config)#ip nat inside source static [inside local ip address] [inside global IP address]
```

Por exemplo, para configurar a tradução no roteador do endereço IP privado 192.168.1.2, configurado no PC da rede local para um endereço IP público, 200.200.200.2, será necessário o comando:

```
Router(config)#ip nat inside source static 192.168.1.2 200.200.200.2
```

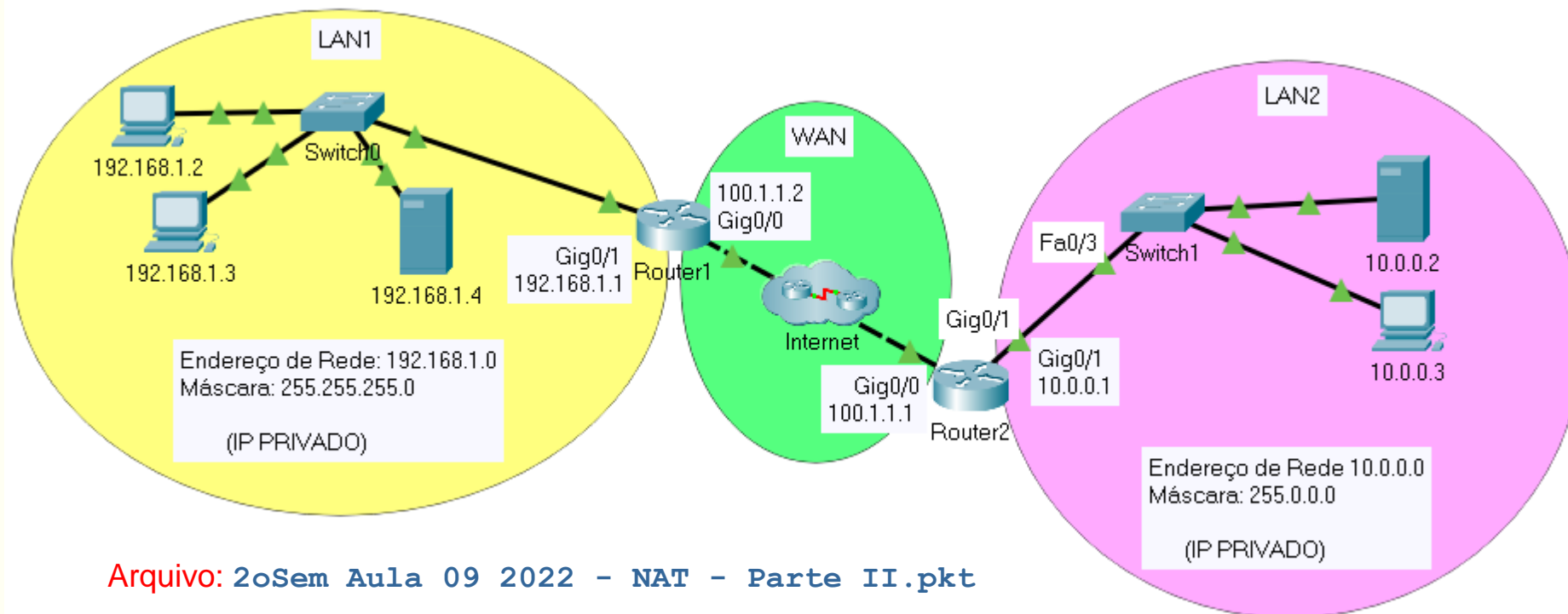
Como um segundo passo será necessário definir qual interface é conectada com a rede local como sendo a interface inside. O comando a seguir defini a interface Fa0/0 como inside local.

```
Router(config-if)#ip nat inside
```

Em um terceiro passo será necessário definir qual interface é conectada como a rede global, configurando-a como uma **inside global**.

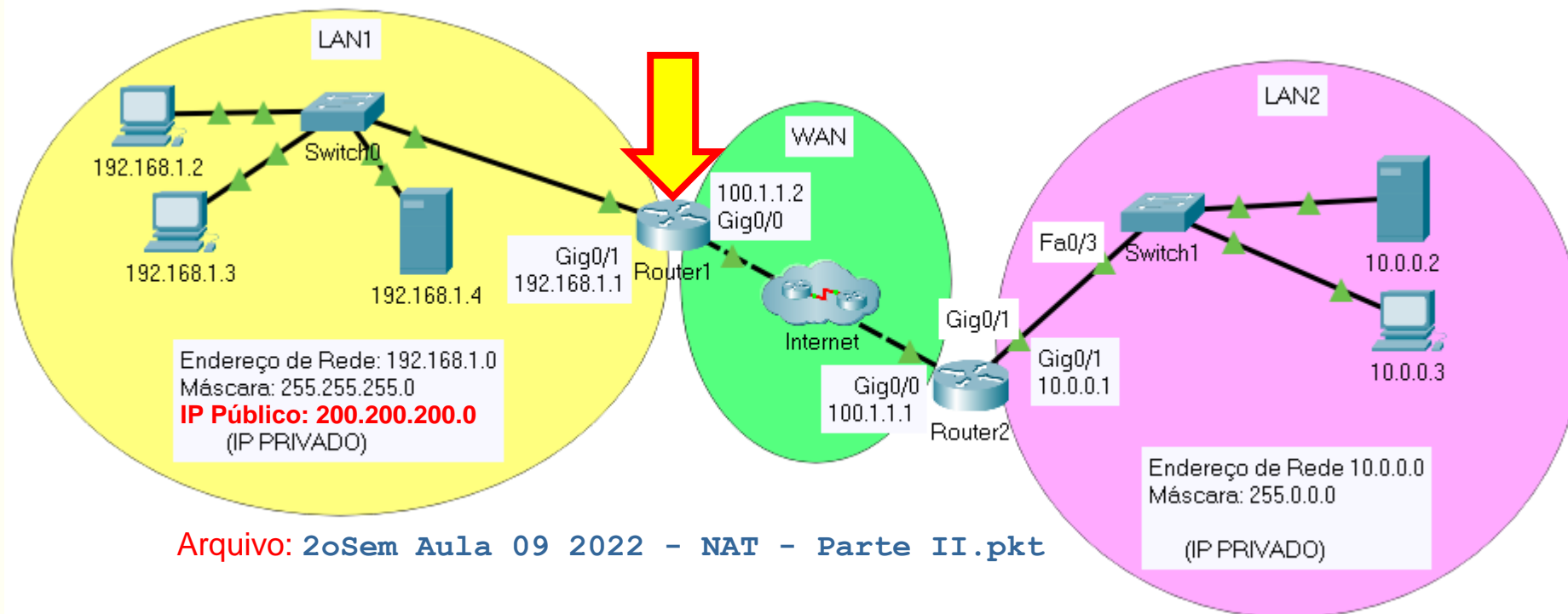
```
Router(config-if)#ip nat outside
```

Configuração de *Static NAT*: LAN1



- Para a configuração de NAT na LAN1 (rede amarela) foi solicitado (como exemplo!) ao Provedor Internet (ISP) um range de **IPs públicos**, sendo fornecido o endereço de rede **200.200.200.0 255.255.255.0**
- Cada IP privado na rede LAN1 será traduzido para um IP público (um-para-um).

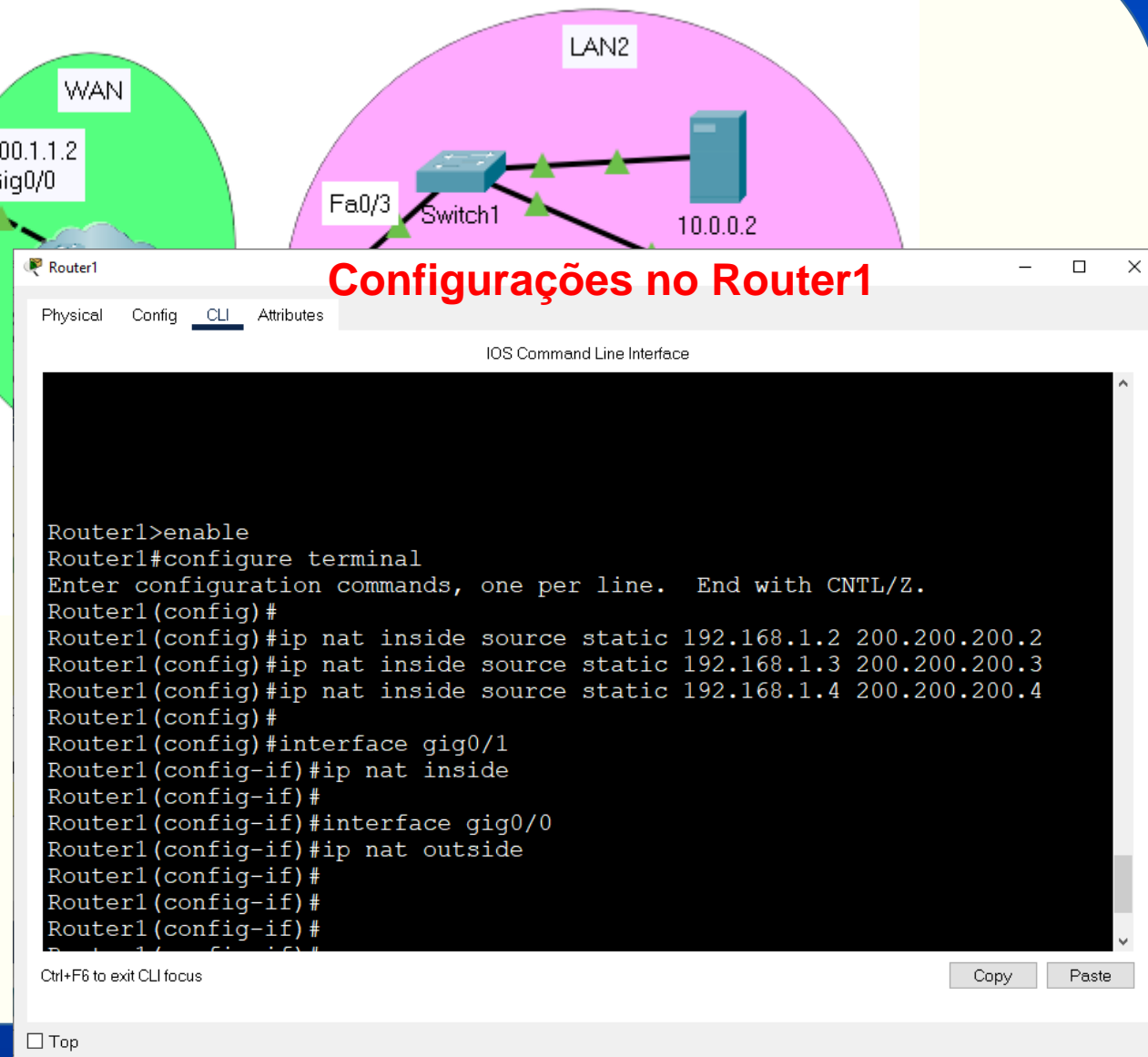
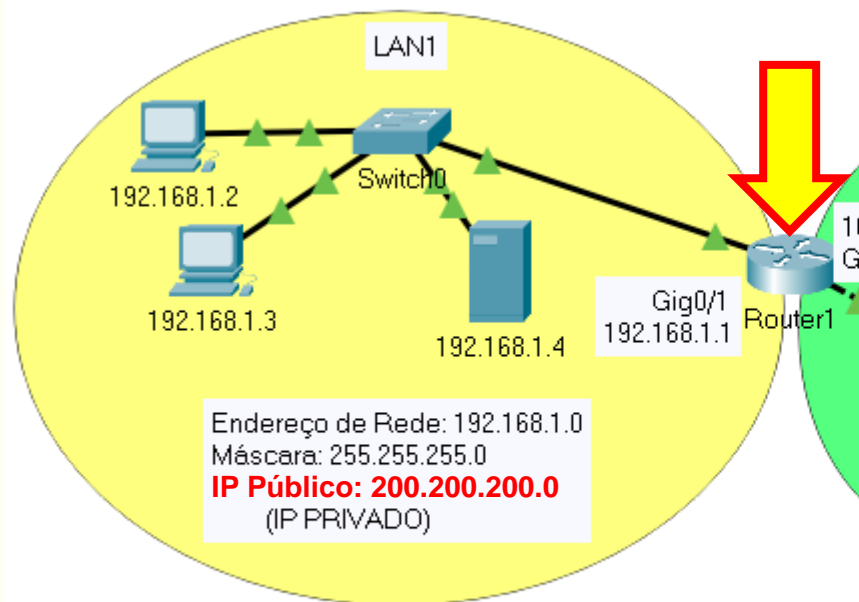
Configuração de *Static NAT*: LAN1



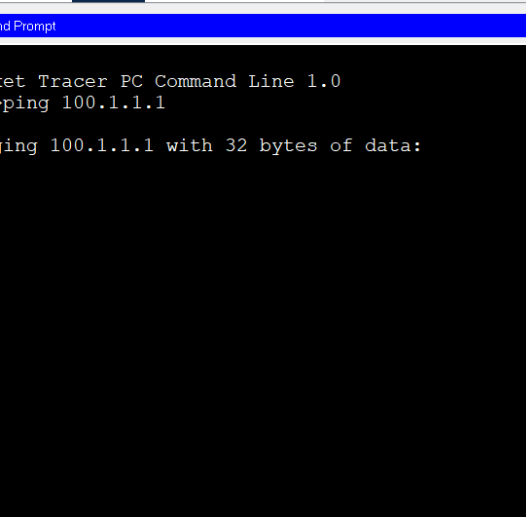
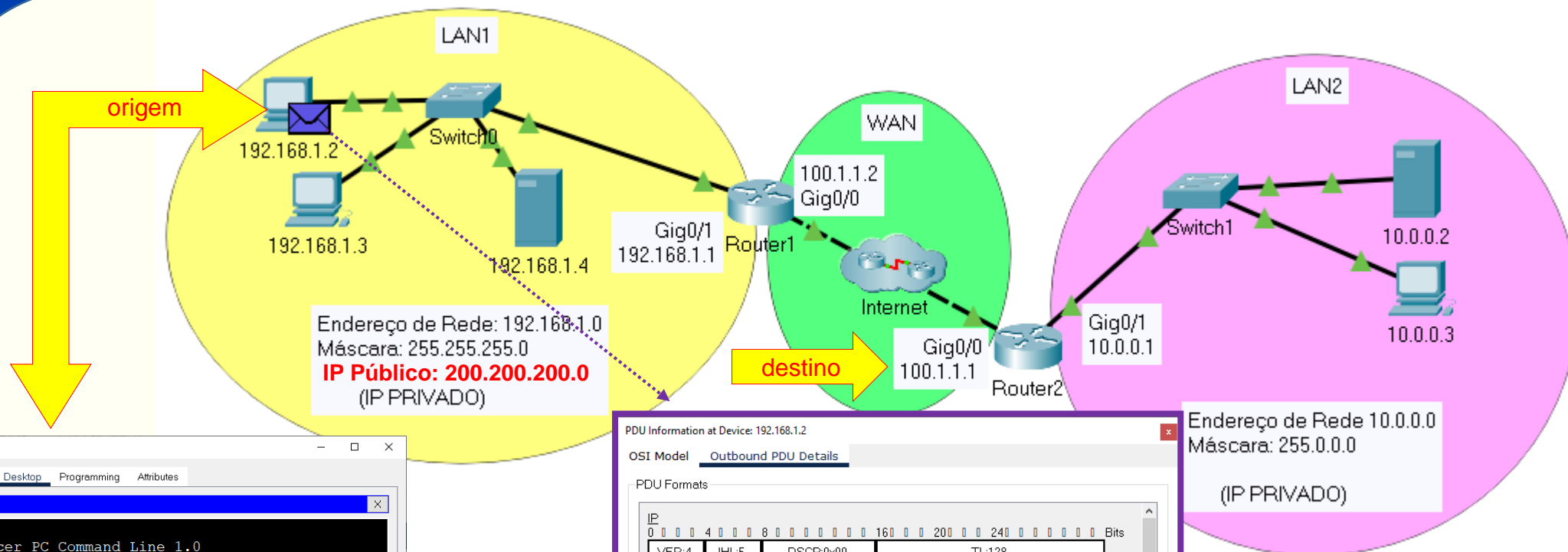
Configurações no Router1

```
Router0 (config) #ip nat inside source static 192.168.1.2 200.200.200.2
Router0 (config) #ip nat inside source static 192.168.1.3 200.200.200.3
Router0 (config) #ip nat inside source static 192.168.1.4 200.200.200.4
Router0 (config) #interface gig0/1
Router0 (config-if) #ip nat inside
Router0 (config-if) #interface gig0/0
Router0 (config-if) #ip nat outside
```

Configuração de *Static NAT*: LAN1



Simulação de *Static NAT*: LAN1



The screenshot shows a Packet Tracer PC Command Line window. The title bar reads "192.168.1.2". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The main area is a black terminal window titled "Command Prompt" with a blue header bar. The text in the terminal is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:

|
```

At the bottom left of the image, there is a checkbox labeled "Top".

PDU Information at Device: 192.168.1.2

OSI Model Outbound PDU Details

PDU Formats

IP

0 Bits

VER:4	IHL:5	DSCP:0x00	TL:128
ID:0x0001		FLAGS:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x01	CHKSUM	
SRC IP:192.168.1.2			
DST IP:100.1.1.1			
DATA (VARIABLE LENGTH)			

ICMP

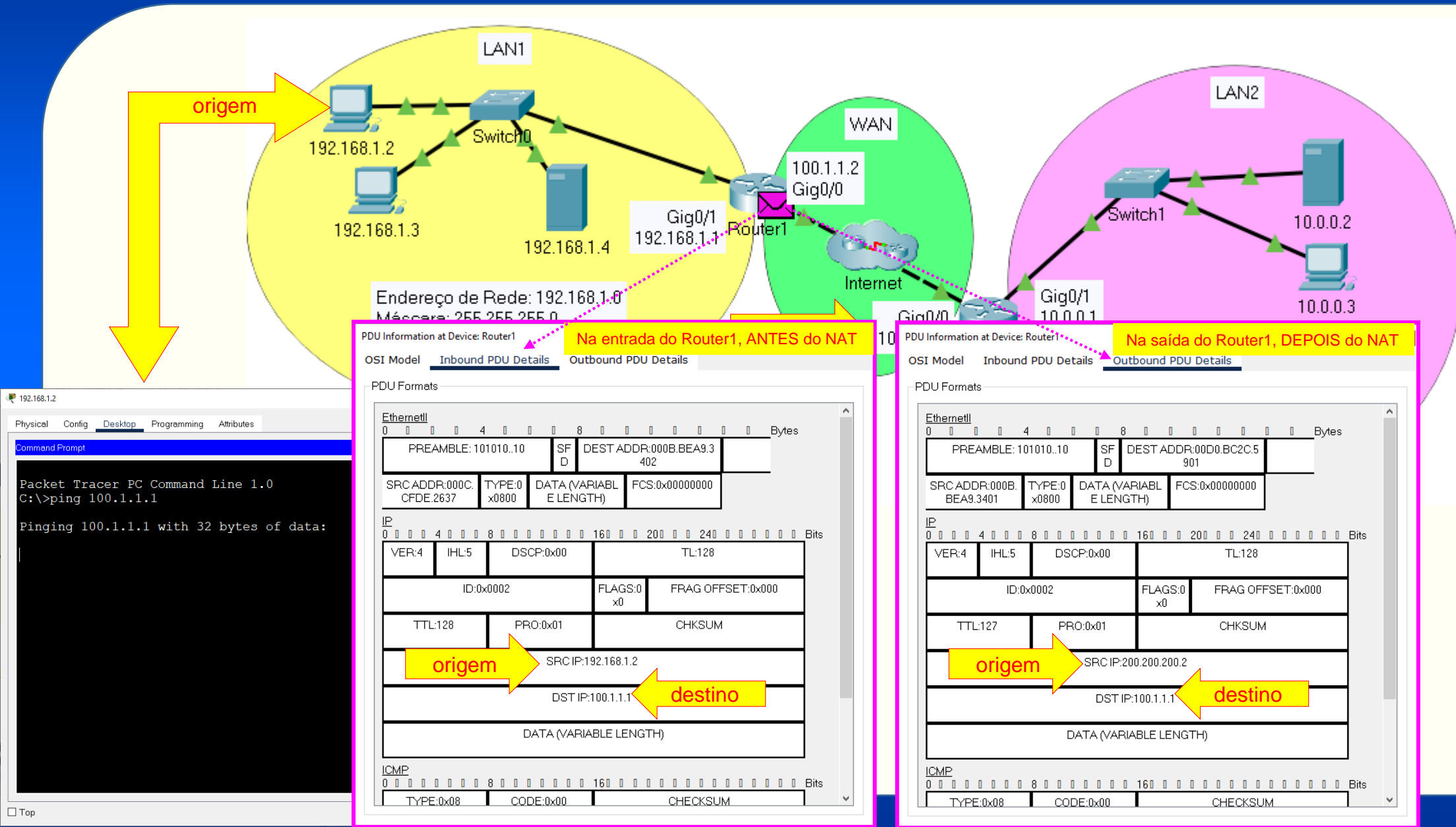
0 Bits

TYPE:0x08	CODE:0x00	CHECKSUM
ID:0x0002	SEQ NUMBER:1	

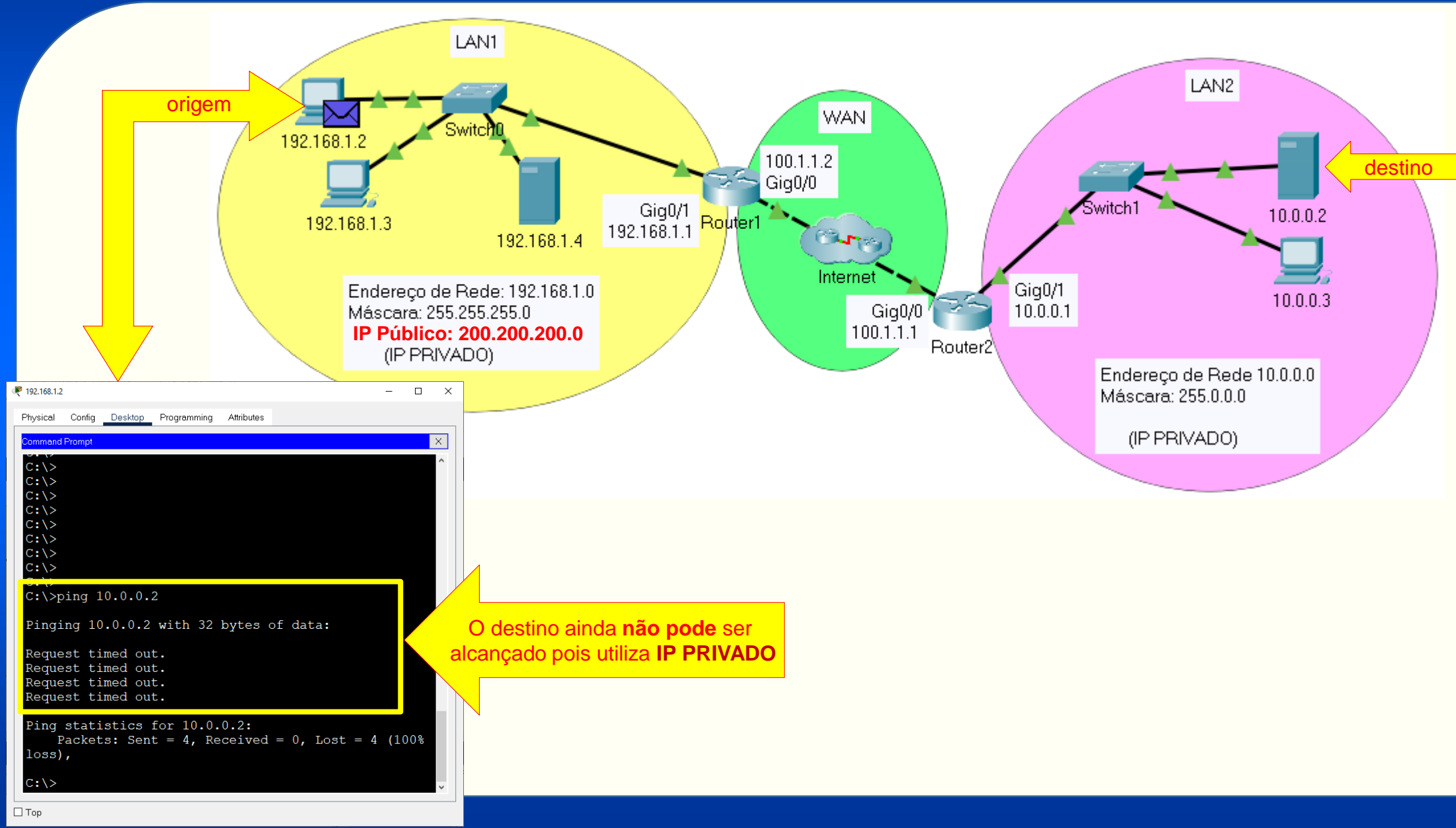
Variable Size PDU

0 Bytes

Simulação de *Static NAT*: LAN1



Simulação de *Static NAT*: LAN1

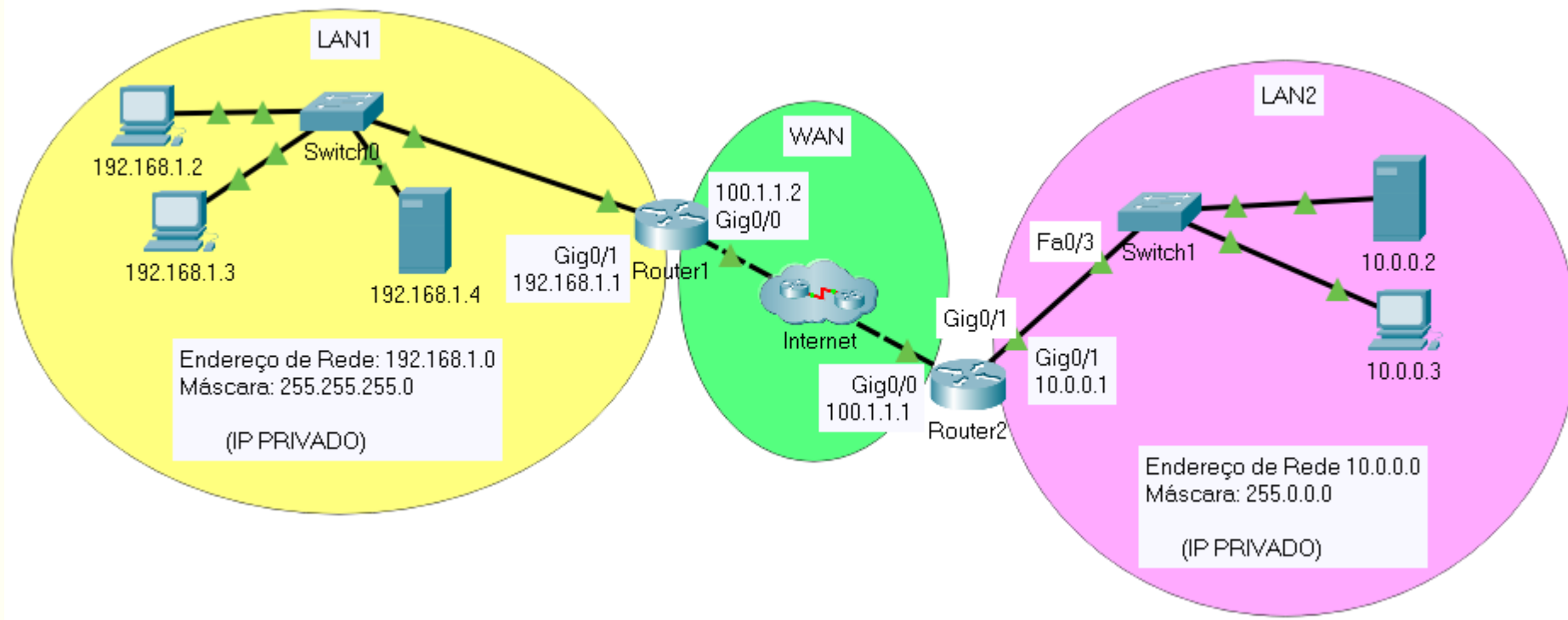


Camada de Rede

Network Address Translation (NAT)

Configuração *Dynamic NAT*

Configuração de *Static NAT*: LAN1

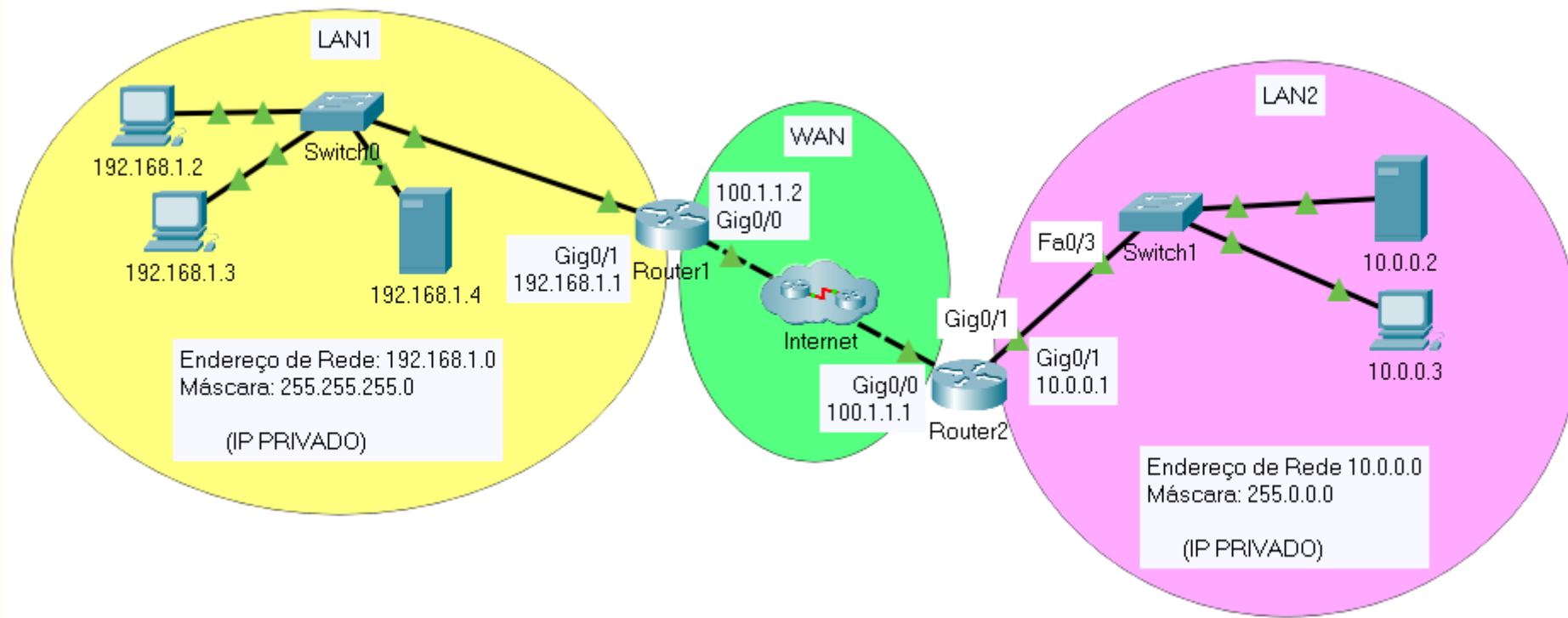


- Para a configuração de NAT na rede **LAN2** (roxa) foi solicitado (como exemplo!) ao Provedor Internet (ISP) um range de **IPs públicos**, sendo fornecido o endereço de rede **202.202.202.0 255.255.255.0**
- Um pacote de dados partindo de um equipamento com IP Privado, na rede **LAN2**, terá seu endereço traduzido pelo roteador para um endereço IP público (não necessariamente em uma relação um-para-um, uma vez que mais de um IP privado poderá compartilhar um mesmo IP Público).

Configuração de *Dynamic NAT*

A configuração do *Dynamic NAT* requer as 4 etapas abaixo:

1. Criação de uma *Access-list* dos endereços IPs privados que serão traduzidos para IP público;
2. Criação de um *pool* de todos os endereços IP privados que serão utilizados na tradução;
3. Associar a *Access-list* ao *Pool* de endereços;
4. Definir as interfaces *inside* e *outside*.



Configuração de *Dynamic NAT* (1)

No primeiro passo será criado uma lista de acesso (*access-list*) padrão no qual definirá quais endereços locais internos (IPs privados) serão permitidos serem traduzidos para endereços IP internos globais (IPs públicos)

Para criar uma lista de acesso padrão no modo de configuração global utilize o seguinte comando:

```
Router(config)# access-list ACL_Identifier_number permit/deny matching-parameters
```

Router(config)# This command prompt indicates that we are in global configuration mode.

access-list : Through this parameter we tell router that we are creating or accessing an access list.

ACL_Identifier_number

With this parameter we specify the type of access list. We have two types of access list; standard and extended. Both lists have their own unique identifier numbers. Standard ACL uses numbers range 1 to 99 and 1300 to 1999. We can pick any number from this range to tell the router that we are working with standard ACL. This number is used in grouping the conditions under a single ACL. This number is also a unique identifier for this ACL in router.

permit/deny

An ACL condition has two actions; permit and deny. If we use permit keyword, ACL will allow all packets from the source address specified in next parameter. If we use deny keyword, ACL will drop all packets from the source address specified in next parameter.

matching-parameters

This parameter allows us to specify the contents of packet that we want to match. In a standard ACL condition it could be a single source address or a range of addresses. We have three options to specify the source address: Any; host; A.B.C.D

Any: Any keyword is used to match all sources. Every packet compared against this condition would be matched.

Host: Host keyword is used to match a specific host. To match a particular host, type the keyword host and then the IP address of host.

A.B.C.D

Through this option we can match a single address or a range of addresses. To match a single address, simply type its address. To match a range of addresses, we need to use wildcard mask.

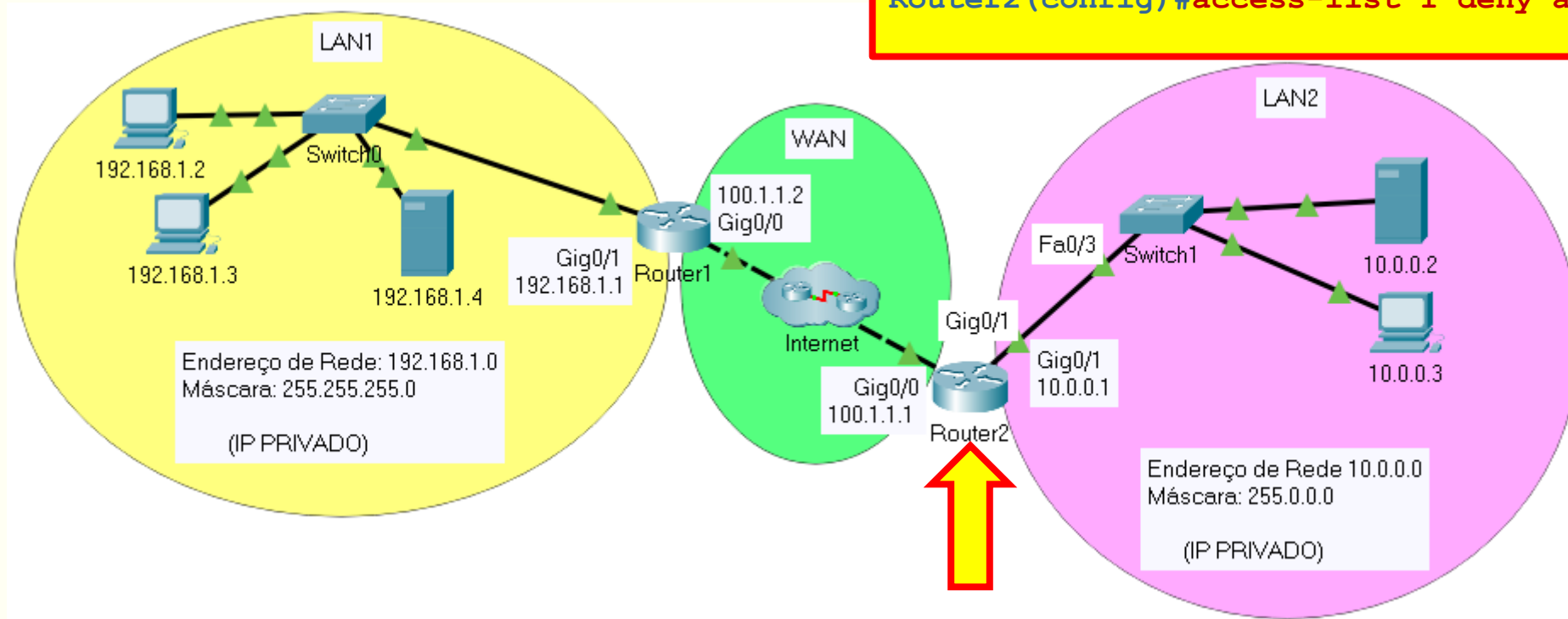
Wildcard mask

Just like subnet mask, wildcard mask is also used to draw a boundary in IP address. Where subnet mask is used to separate network address from host address, wildcard mask is used to distinguish the matching portion from the rest. Wildcard mask is the invert of Subnet mask. Wildcard can be calculated in decimal or in binary from subnet mask.

Configuração de *Dynamic NAT* (etapa1)

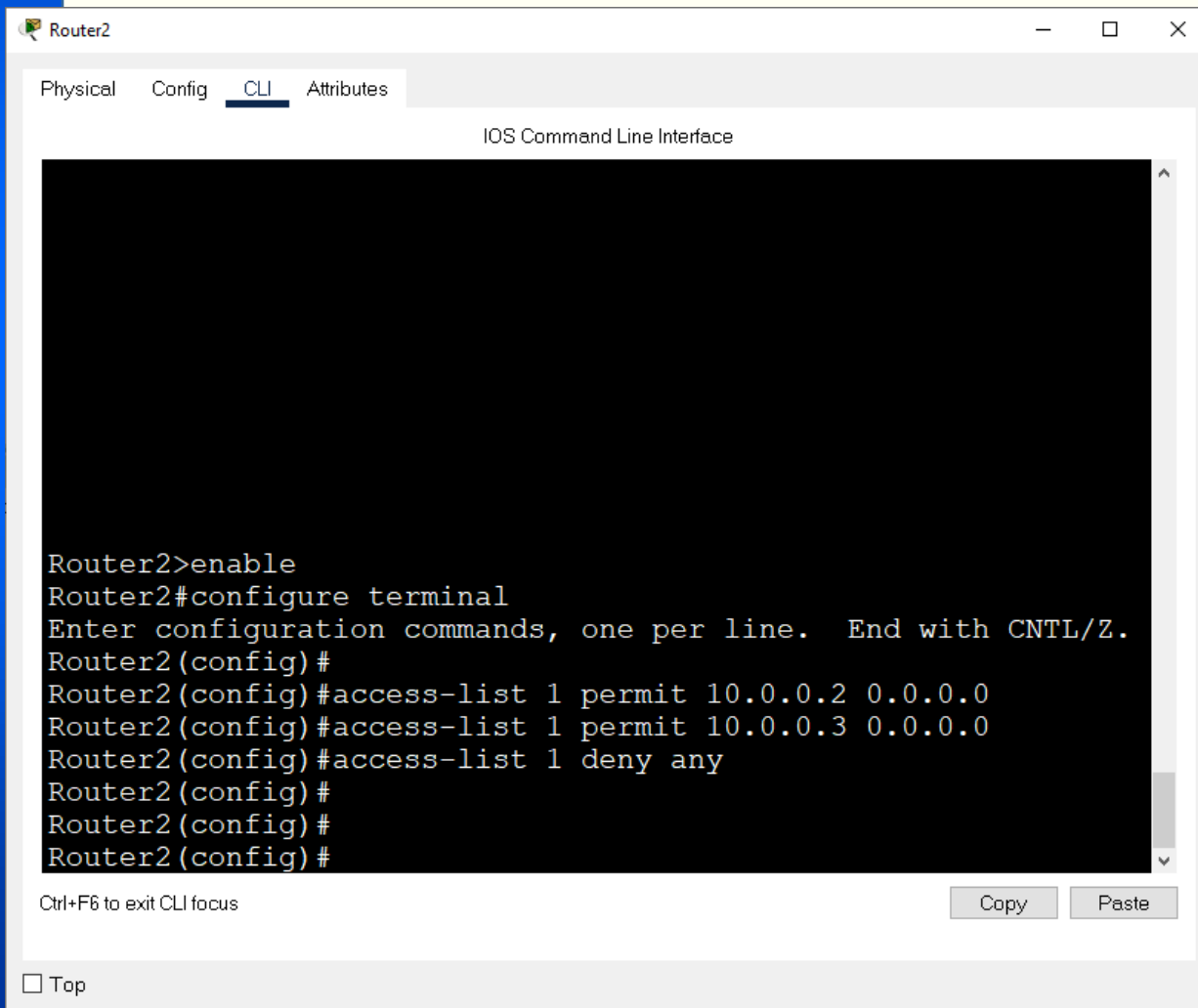
Para o cenário a seguir, que possui três hosts na LAN1, utilize a seguinte lista de acesso para permitir que os três hosts existentes utilizem o NAT a ser configurado no **Router2**.

```
Router2(config)#access-list 1 permit 10.0.0.2 0.0.0.0  
Router2(config)#access-list 1 permit 10.0.0.3 0.0.0.0  
Router2(config)#access-list 1 deny any
```



Configuração de *Dynamic NAT* (etapa1)

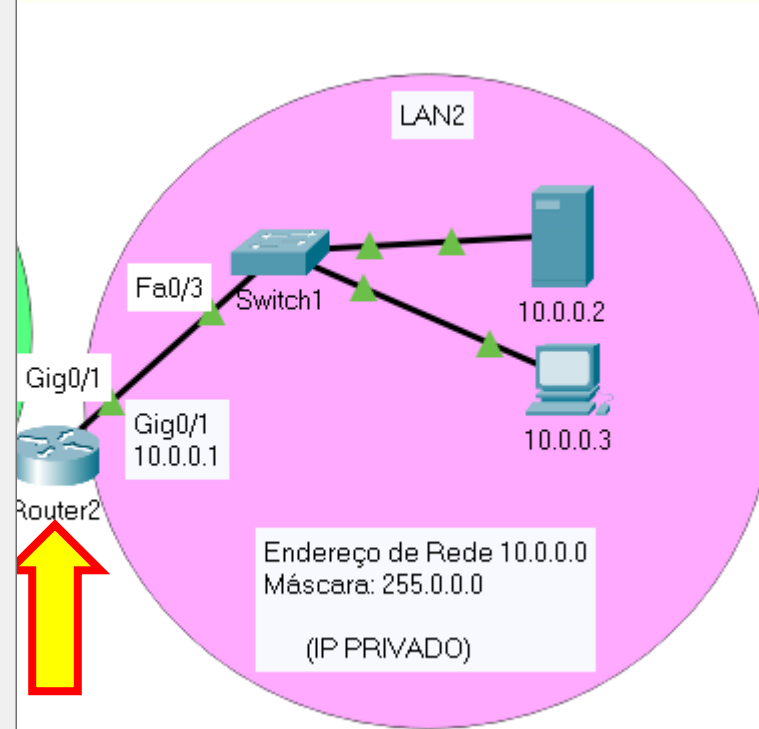
Para o cenário a seguir, que possui três hosts na LAN1, utilize a seguinte lista de acesso para permitir que os três hosts existentes utilizem o NAT a ser configurado no **Router2**.



```
Router2>enable
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#
Router2(config)#access-list 1 permit 10.0.0.2 0.0.0.0
Router2(config)#access-list 1 permit 10.0.0.3 0.0.0.0
Router2(config)#access-list 1 deny any
Router2(config)#
Router2(config)#
Router2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste



Configuração de *Dynamic NAT* *(etapa2)*

O segundo passo será definir o pool de endereços IP globais internos (*inside global addresses*) que serão utilizados para a tradução.

Para isso será utilizado o seguinte comando:

```
Router(config)#ip nat pool [Pool Name] [Start IP address] [End IP address] netmask [Subnet mask]
```

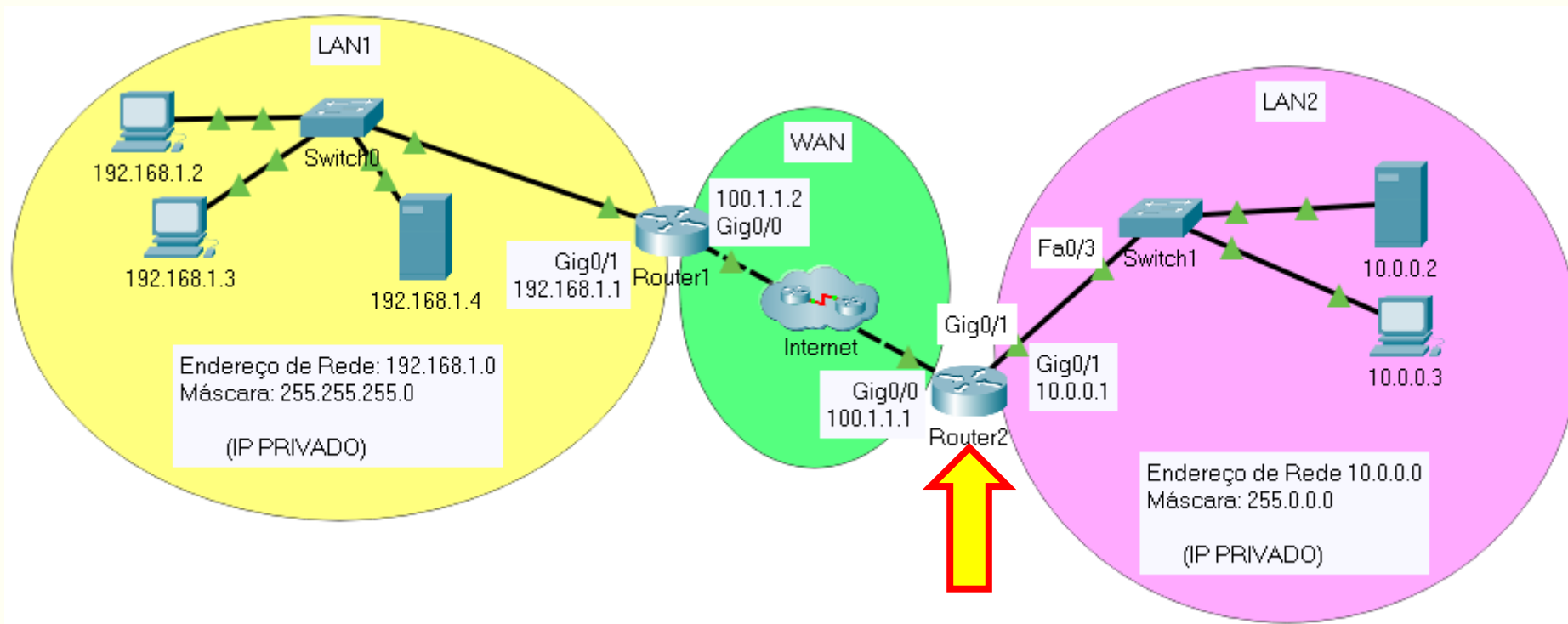
Este comando aceita quatro parâmetros:

1. **Pool Name:** - This is the name of pool. We can choose any descriptive name here.
2. **Start IP Address:** First IP address from the IP range which is available for translation.
3. **End IP Address:** Last IP address from the IP range which is available for translation. There is no minimum or maximum criteria for IP range for example we can have a range of single IP address or we can have a range of all IP address from a subnet.
4. **Subnet Mask:** Subnet mask of IP range.

Configuração de *Dynamic NAT* (etapa2)

Para o cenário a seguir, pode-se utilizar o seguinte comando no roteador **Router1**:

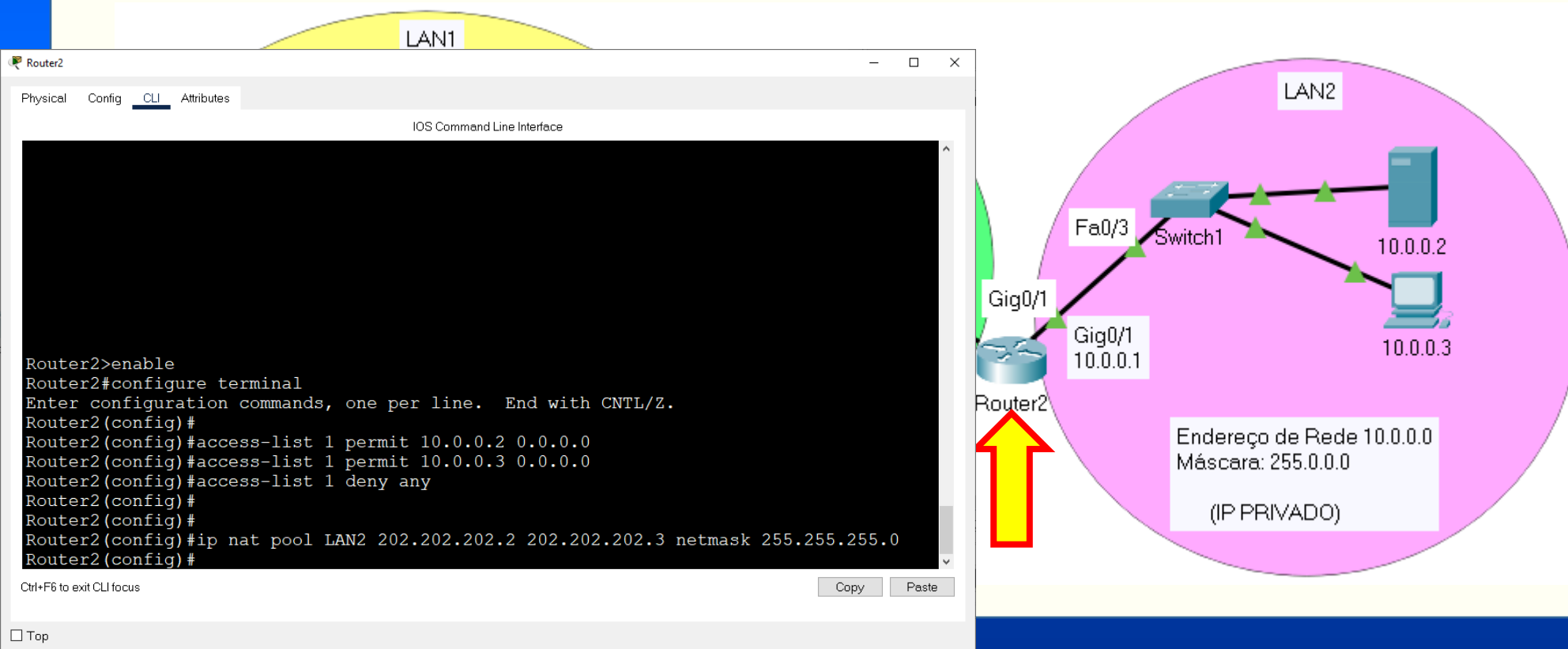
```
Router2(config)#ip nat pool LAN2 202.202.202.2 202.202.202.3 netmask 255.255.255.0
```



Configuração de *Dynamic NAT* (etapa2)

Para o cenário a seguir, pode-se utilizar o seguinte comando no roteador **Router1**:

```
Router2(config)#ip nat pool LAN2 202.202.202.2 202.202.202.3 netmask 255.255.255.0
```



Configuração de *Dynamic NAT* *(etapa3)*

No terceiro passo será necessário associar a lista de acesso com o pool criado.

O seguinte comando será utilizado:

```
Router(config)#ip nat inside source list [access list name or number] pool [pool name]
```

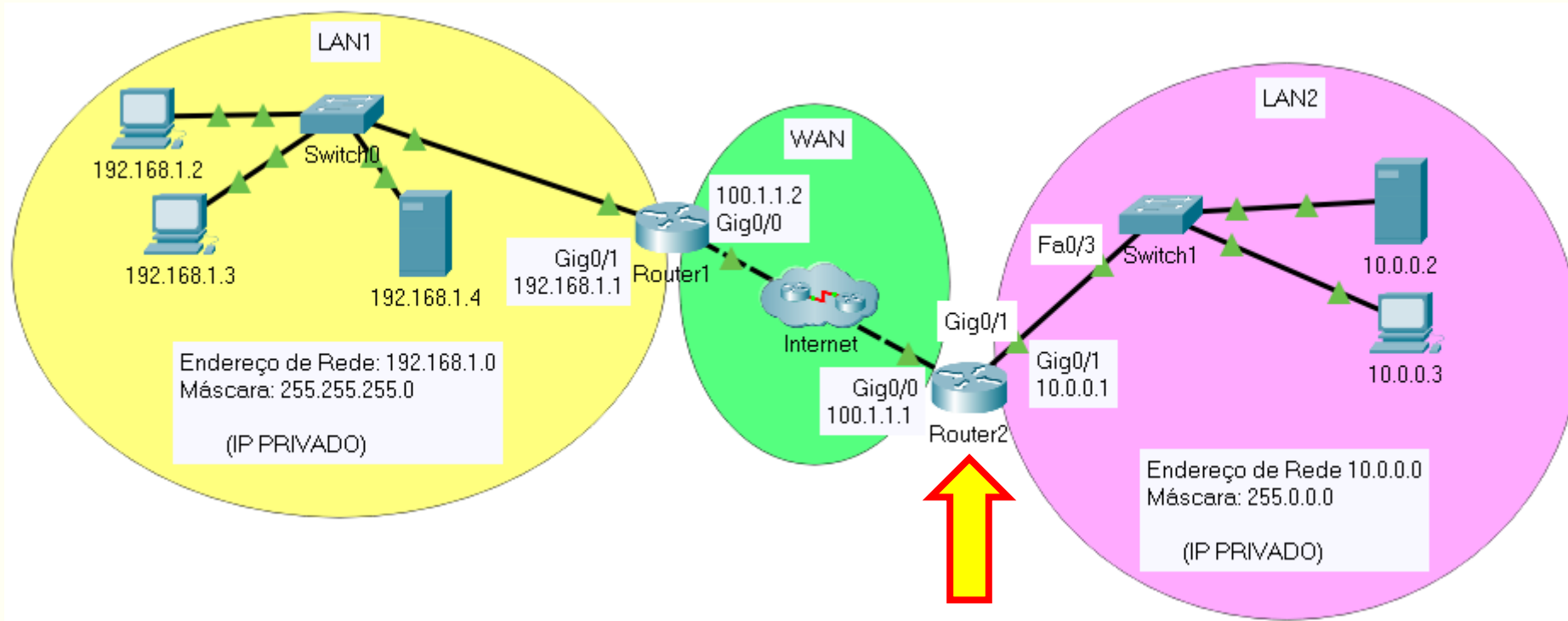
Este comando aceita dois parâmetros:

1. Access list name or number: Name or number the access list which we created in first step.
2. Pool Name: Name of pool which we created in second step.

Configuração de *Dynamic NAT* (etapa3)

Para o cenário a seguir, pode-se utilizar o seguinte comando:

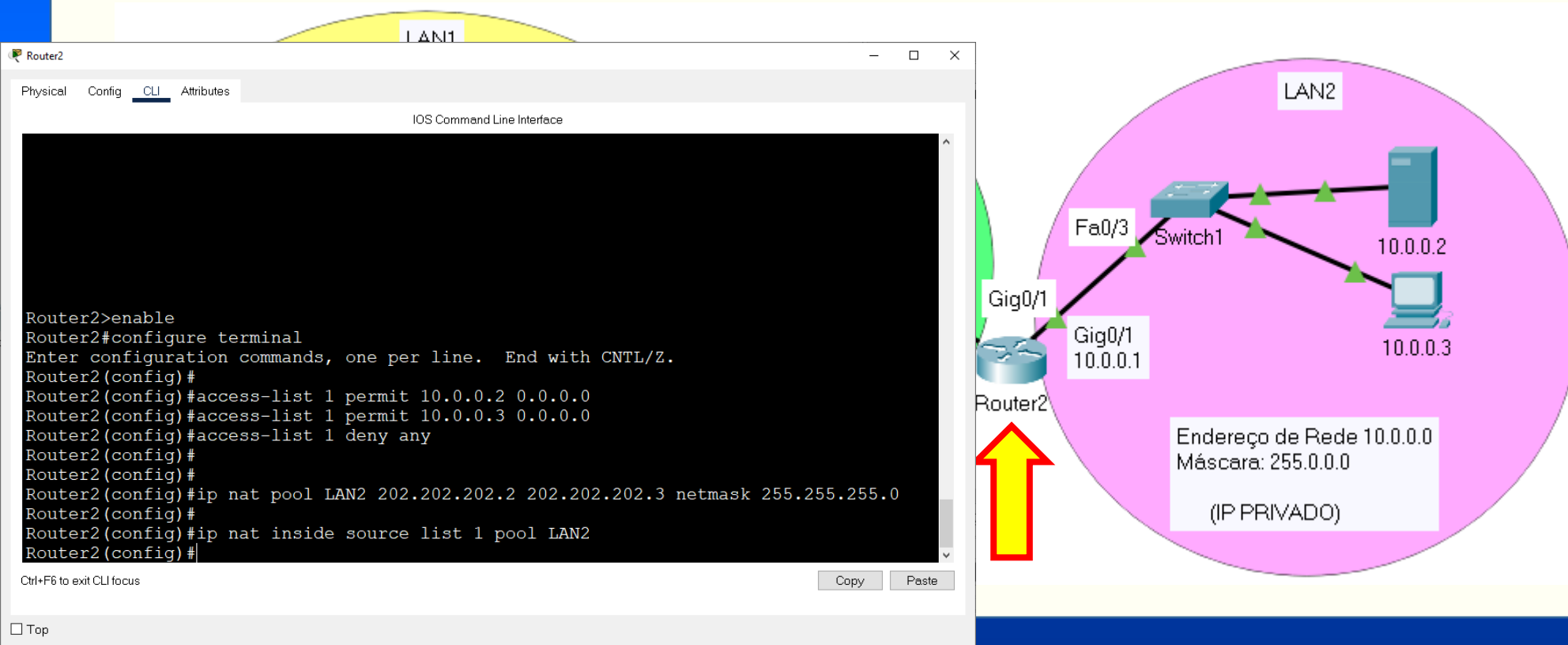
```
Router2(config)#ip nat inside source list 1 pool LAN2
```



Configuração de *Dynamic NAT* (etapa3)

Para o cenário a seguir, pode-se utilizar o seguinte comando:

```
Router2(config)#ip nat inside source list 1 pool LAN2
```

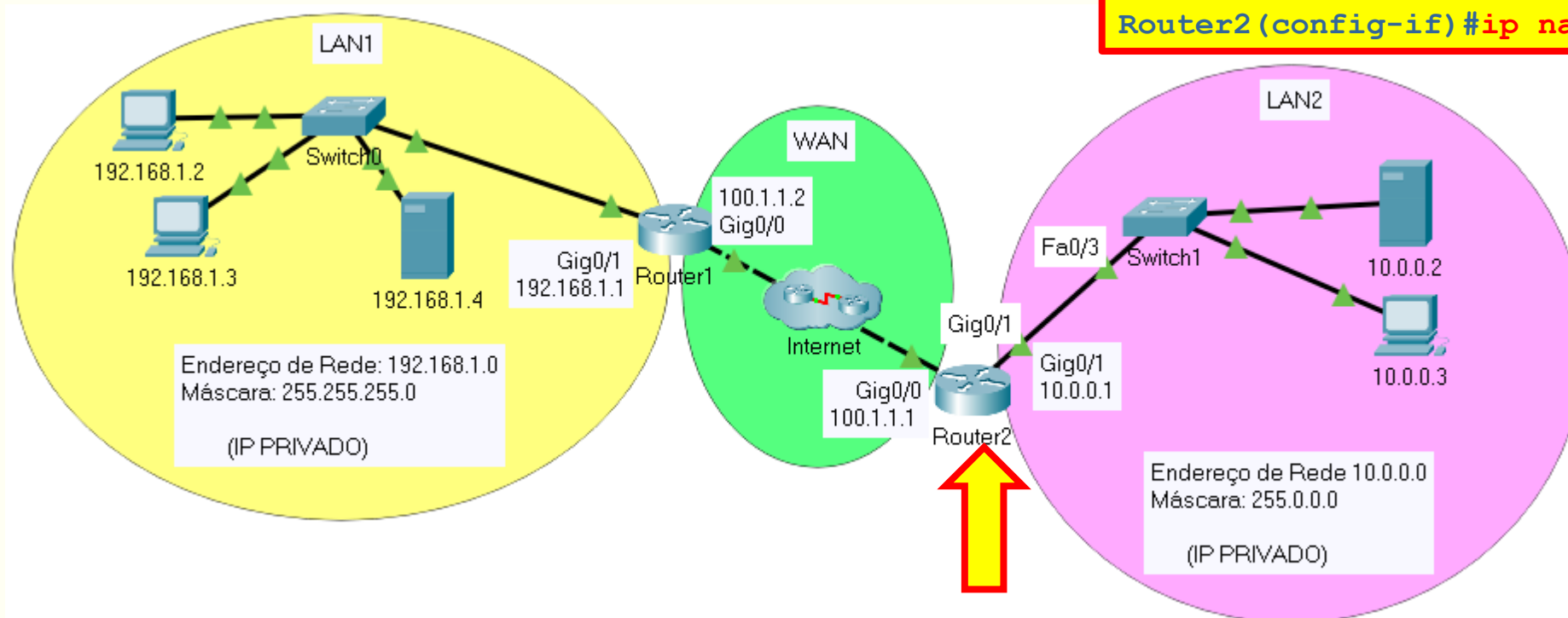


Configuração de *Dynamic NAT* (etapa4)

No quarto passo será necessário identificar as interfaces *inside* e *outside*.

Para o cenário a seguir, pode-se utilizar os seguintes comandos:

```
Router2(config)#interface gig0/0
Router2(config-if)#ip nat outside
Router2(config-if)#exit
Router2(config)#interface gig0/1
Router2(config-if)#ip nat inside
```

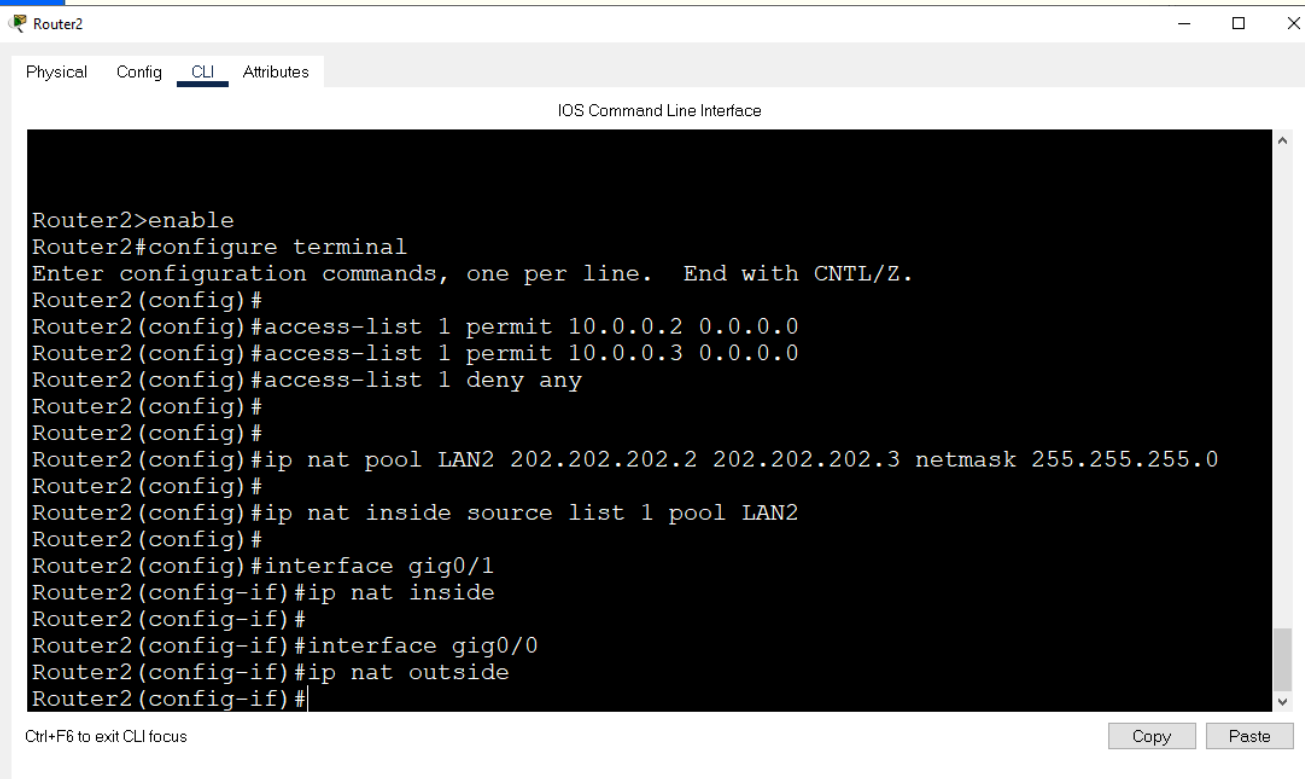


Configuração de *Dynamic NAT* (etapa4)

No quarto passo será necessário identificar as interfaces *inside* e *outside*.

Para o cenário a seguir, pode-se utilizar os seguintes comandos:

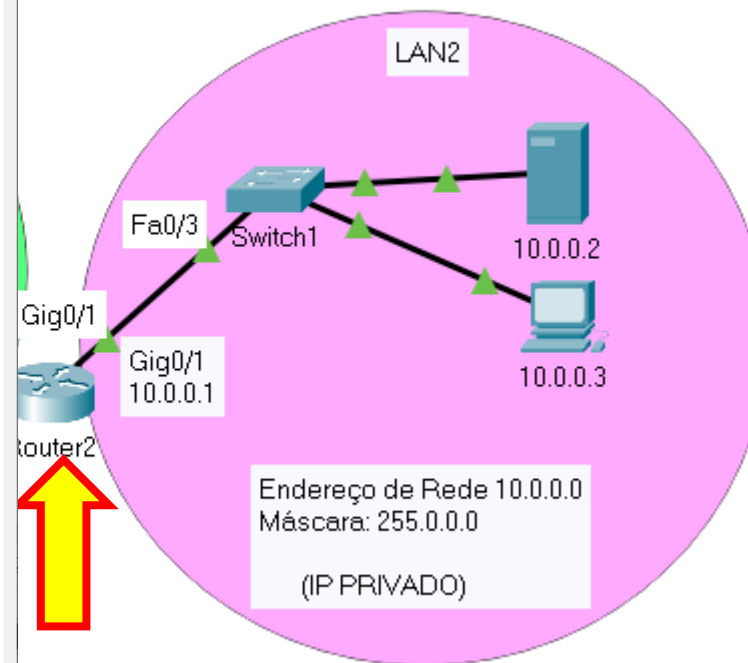
```
Router2(config)#interface gig0/0
Router2(config-if)#ip nat outside
Router2(config-if)#exit
Router2(config)#interface gig0/1
Router2(config-if)#ip nat inside
```



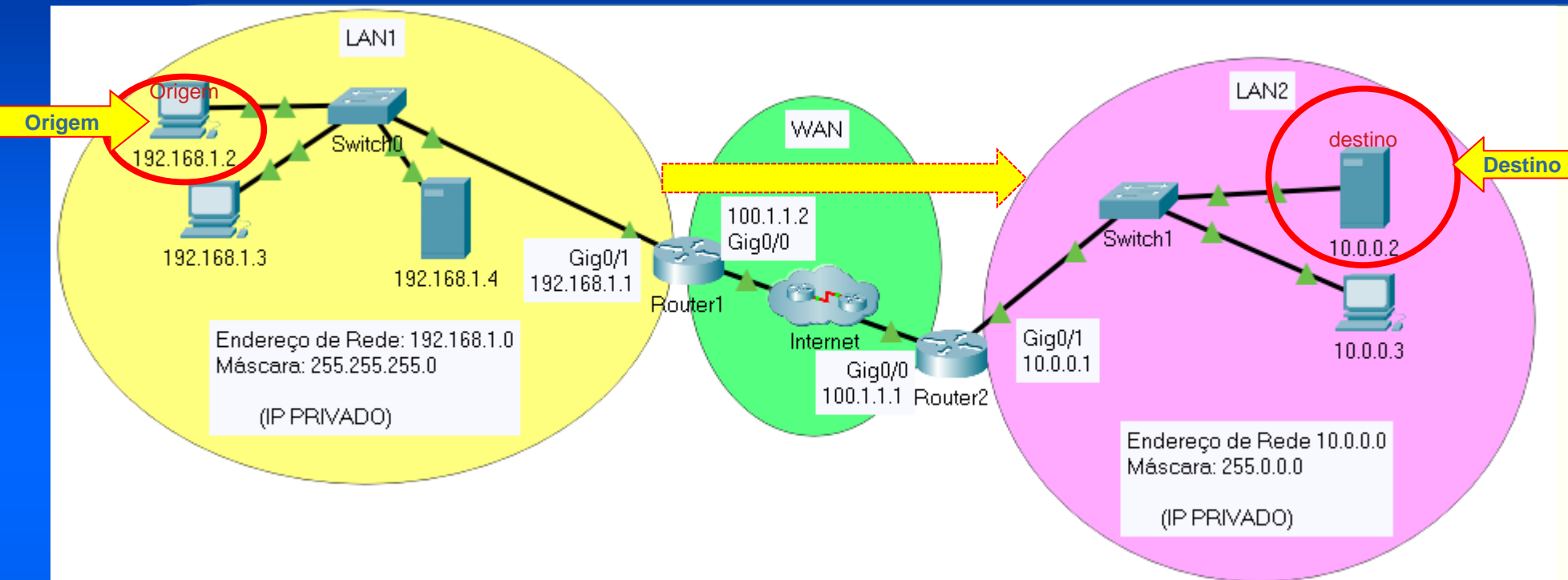
```
Router2>enable
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#
Router2(config)#access-list 1 permit 10.0.0.2 0.0.0.0
Router2(config)#access-list 1 permit 10.0.0.3 0.0.0.0
Router2(config)#access-list 1 deny any
Router2(config)#
Router2(config)#ip nat pool LAN2 202.202.202.2 202.202.202.3 netmask 255.255.255.0
Router2(config)#
Router2(config)#ip nat inside source list 1 pool LAN2
Router2(config)#
Router2(config)#interface gig0/1
Router2(config-if)#ip nat inside
Router2(config-if)#
Router2(config-if)#interface gig0/0
Router2(config-if)#ip nat outside
Router2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

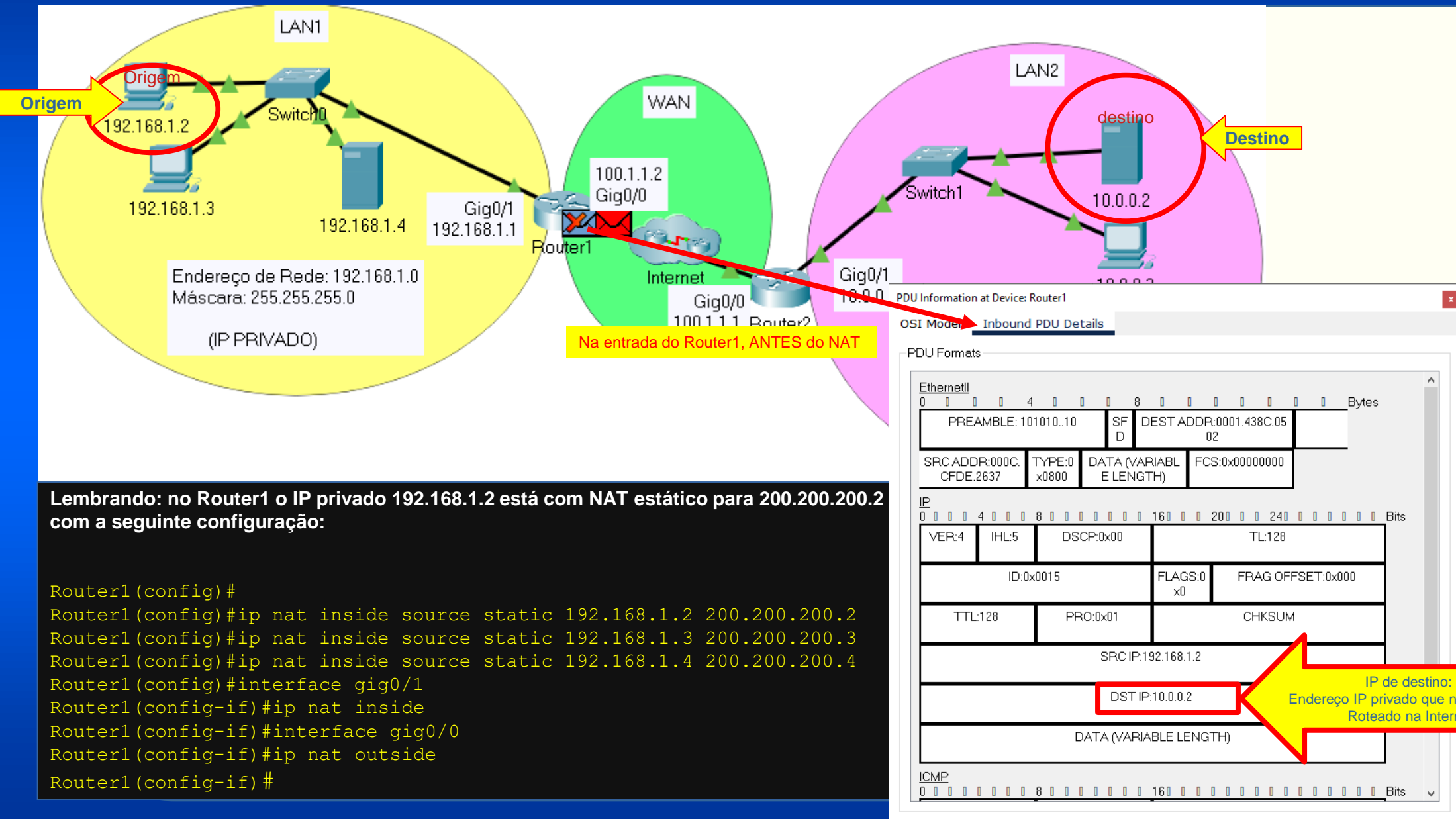


Simulação do uso de *Dynamic NAT*

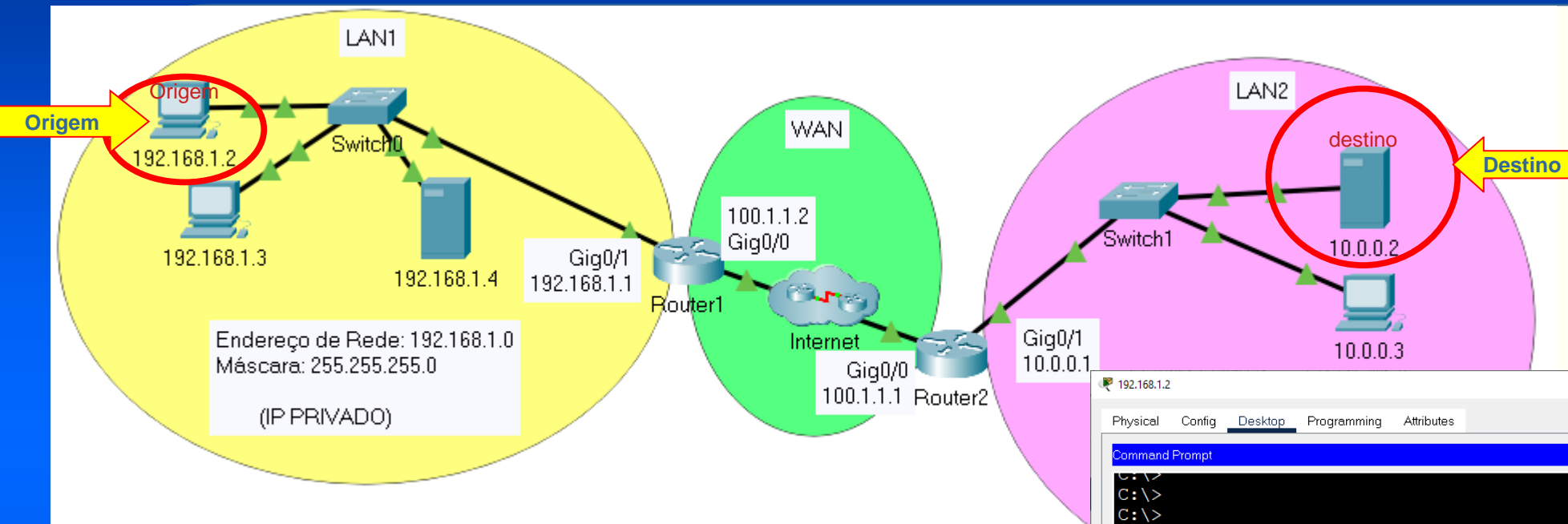


Simulação de comunicação **partindo da LAN1** com **destino à LAN2**

Simulação do uso de *Dynamic NAT*

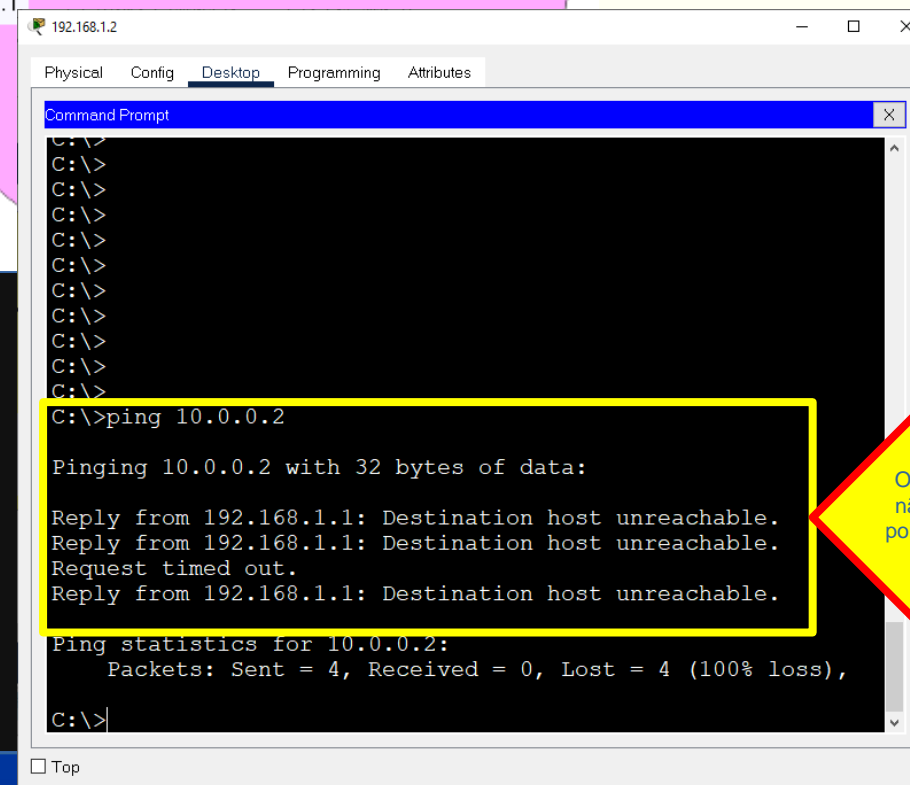


Simulação do uso de *Dynamic NAT*



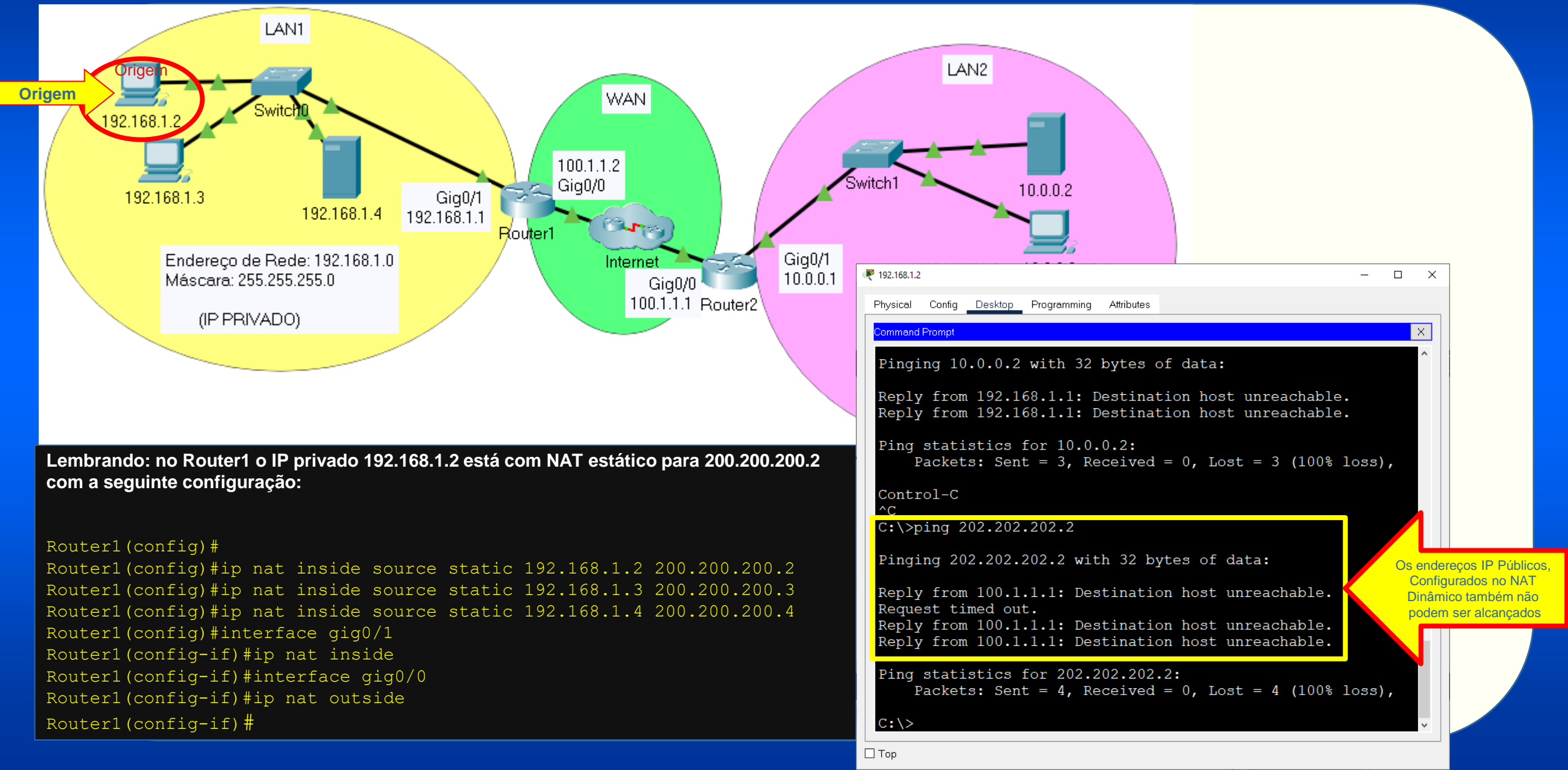
Lembrando: no Router1 o IP privado 192.168.1.2 está com NAT estático para 200.200.200.2 com a seguinte configuração:

```
Router1(config)#
Router1(config)#ip nat inside source static 192.168.1.2 200.200.200.2
Router1(config)#ip nat inside source static 192.168.1.3 200.200.200.3
Router1(config)#ip nat inside source static 192.168.1.4 200.200.200.4
Router1(config)#interface gig0/1
Router1(config-if)#ip nat inside
Router1(config-if)#interface gig0/0
Router1(config-if)#ip nat outside
Router1(config-if)#
```

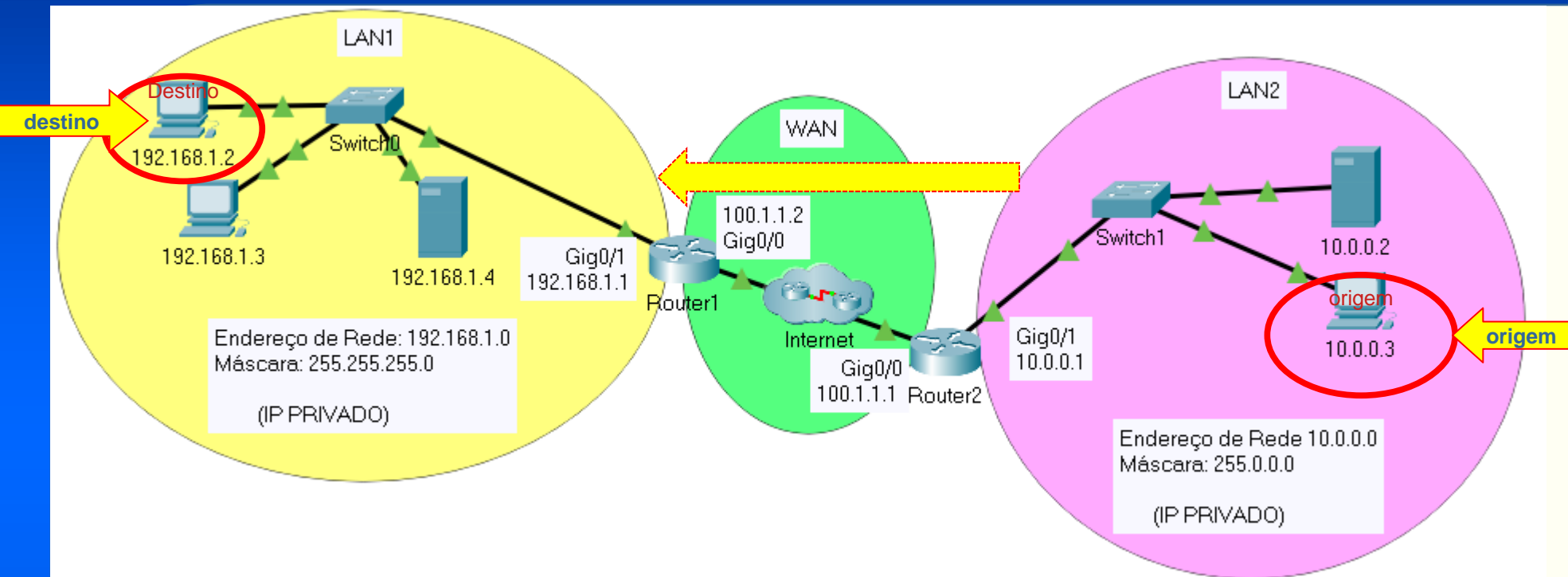


Os endereços IP privados, não podem ser alcançados pois não podem ser roteados na Internet

Simulação do uso de *Dynamic NAT*

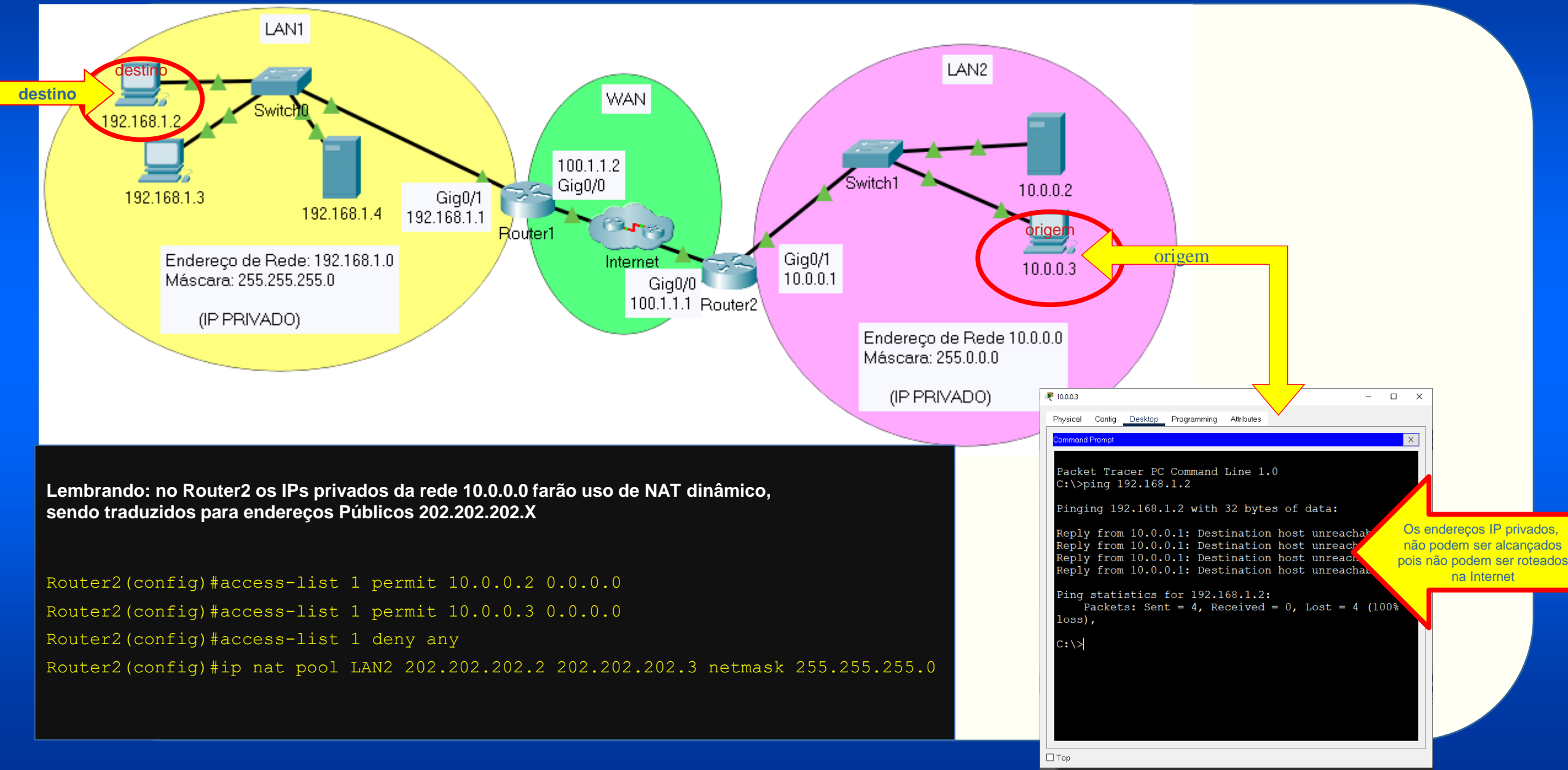


Simulação do uso de *Dynamic NAT*

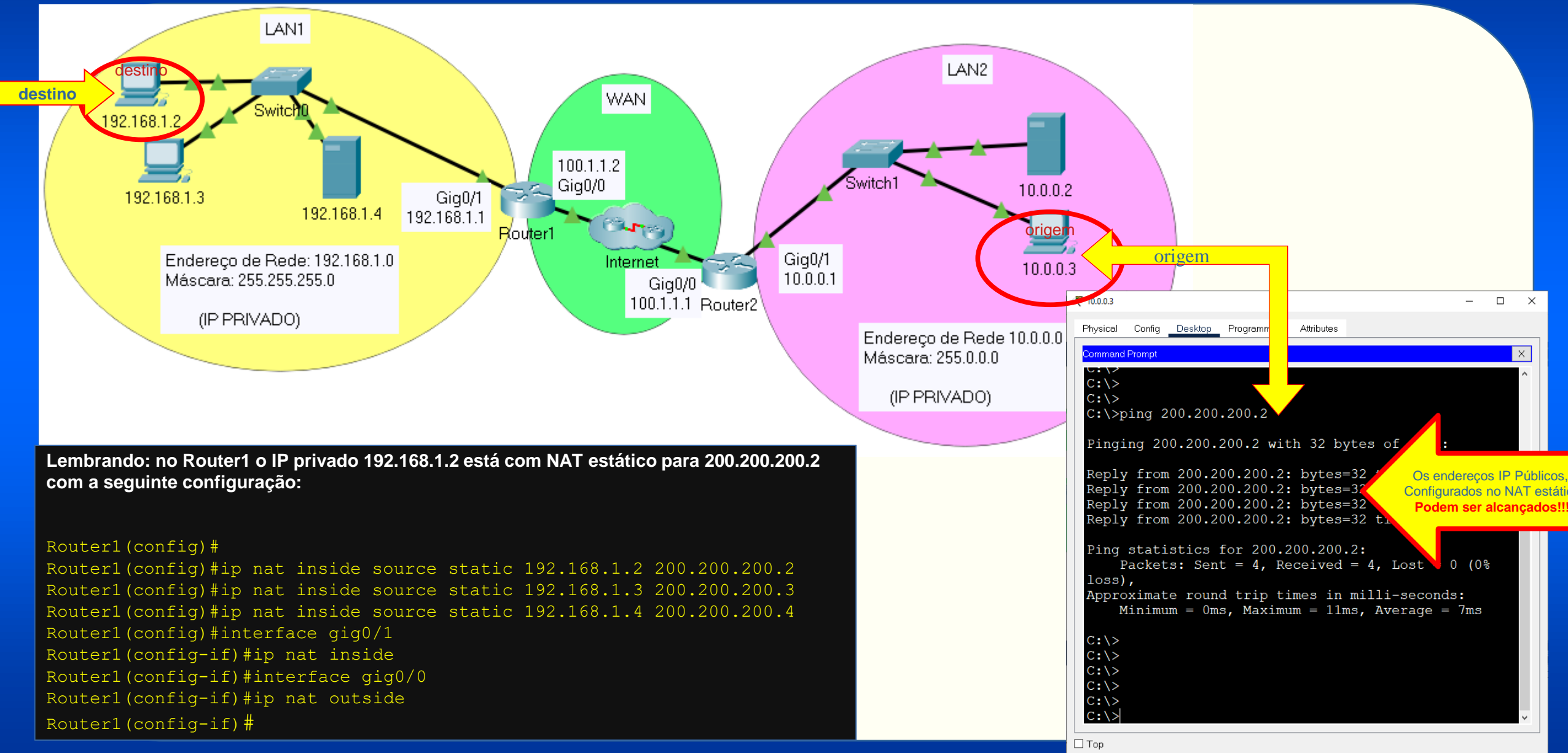


Simulação de comunicação partindo da LAN2 com destino à LAN1

Simulação do uso de *Dynamic NAT*



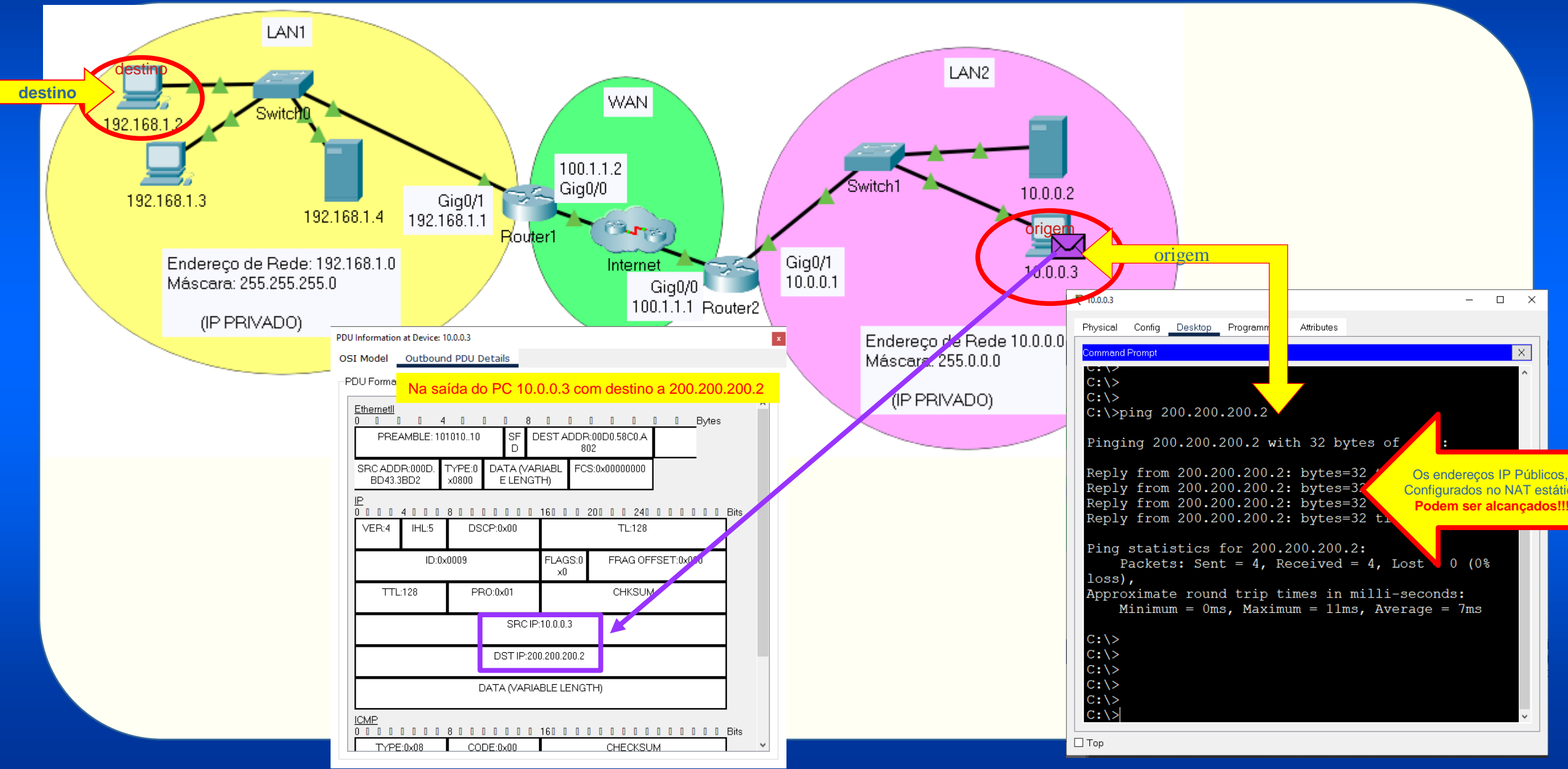
Simulação do uso de *Dynamic NAT*



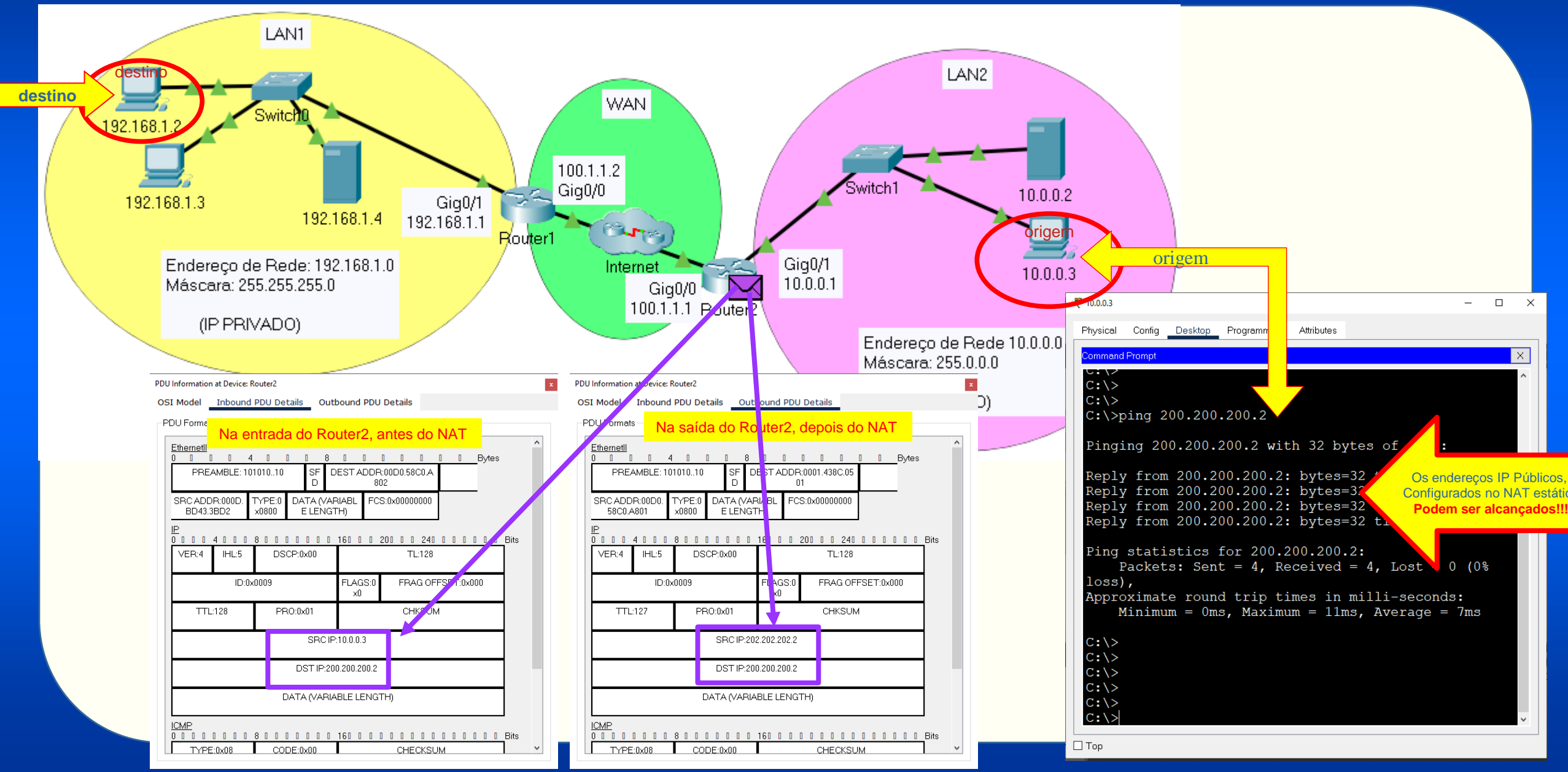
Lembrando: no Router1 o IP privado 192.168.1.2 está com NAT estático para 200.200.200.2 com a seguinte configuração:

```
Router1(config)#
Router1(config)#ip nat inside source static 192.168.1.2 200.200.200.2
Router1(config)#ip nat inside source static 192.168.1.3 200.200.200.3
Router1(config)#ip nat inside source static 192.168.1.4 200.200.200.4
Router1(config)#interface gig0/1
Router1(config-if)#ip nat inside
Router1(config-if)#interface gig0/0
Router1(config-if)#ip nat outside
Router1(config-if)#
```

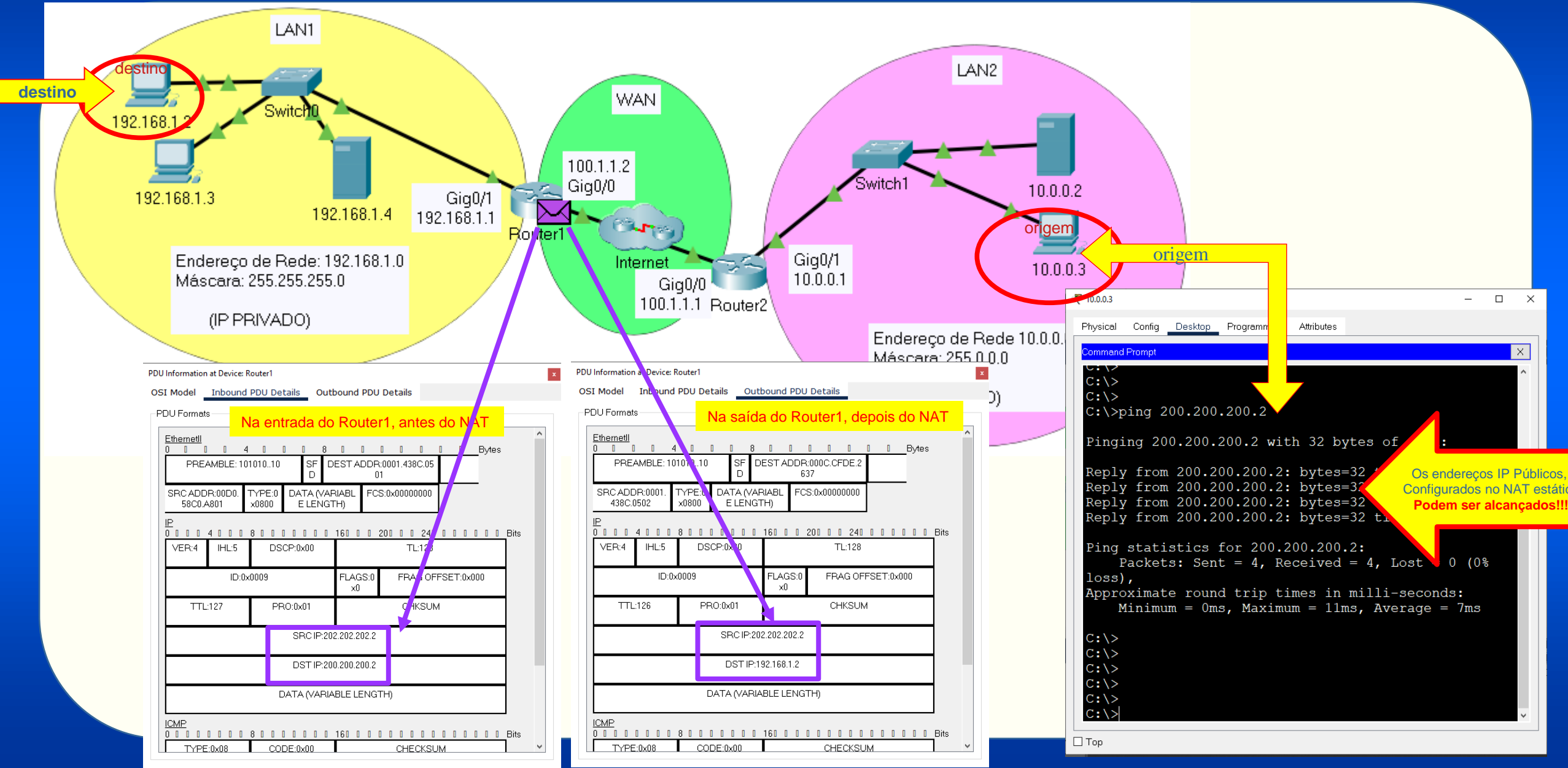

Simulação do uso de *Dynamic NAT*



Simulação do uso de *Dynamic NAT*



Simulação do uso de *Dynamic NAT*



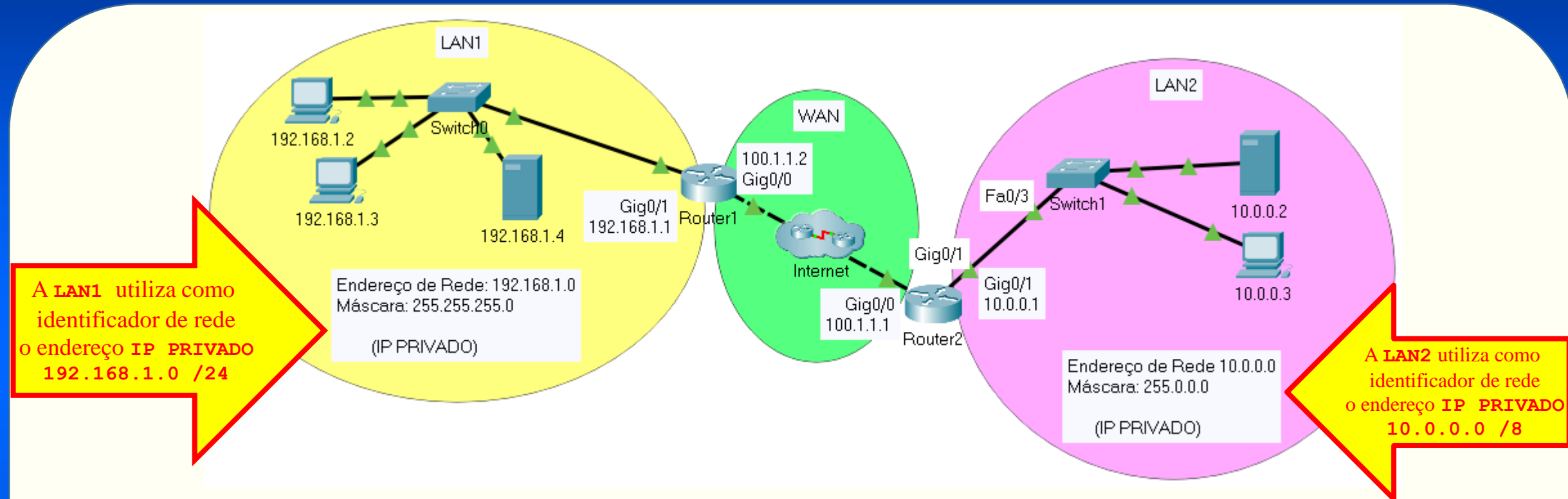
PAT

(Port Address Translation)

PAT (*Port Address Translation*)

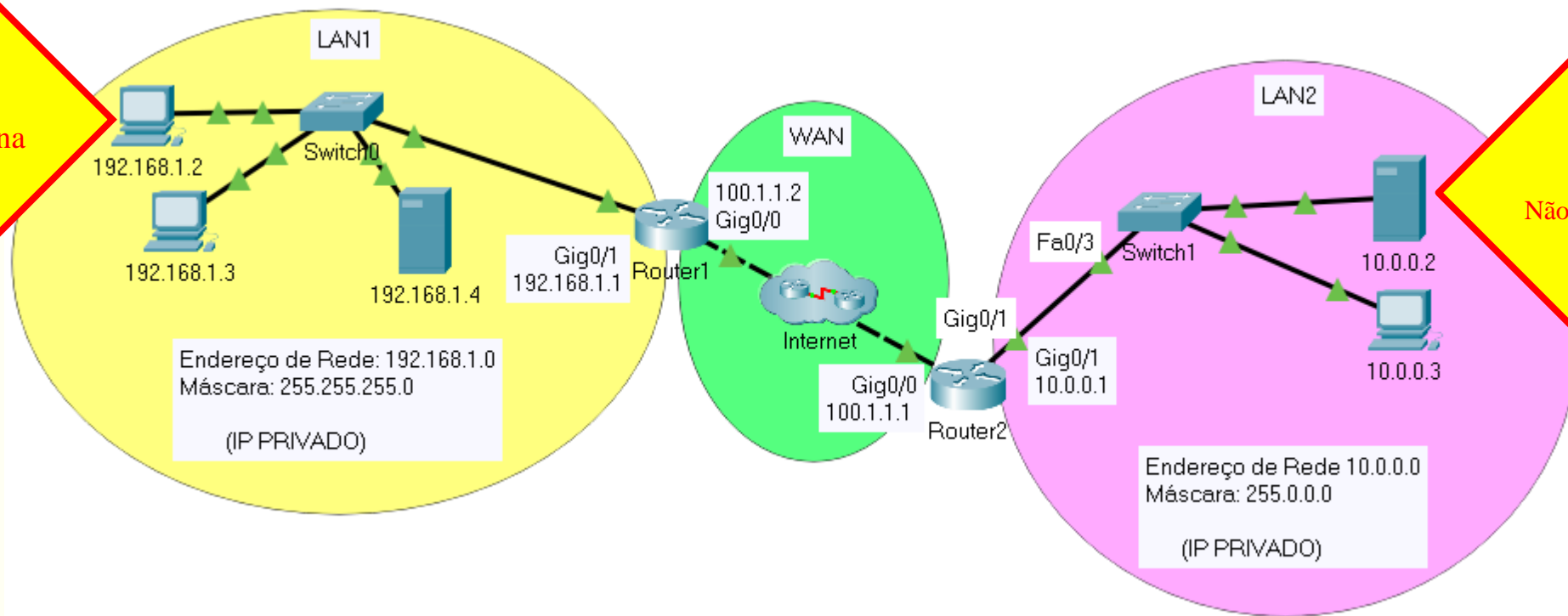
- **Port Address Translation (PAT)** é uma extensão de **Network Address Translation** (NAT) que permite diversos dispositivos em uma LAN serem mapeados para um único endereço IP público, conservando seus endereços internos (privados).
- Assim, no PAT (*Port Address Translation*) é possível associar todos os equipamentos de uma rede privada a um (1) único endereço IP público para a Internet.
- Pode-se dizer que o **PAT** é um "**NAT Overload**"
- PAT é similar a *port forwarding* exceto que um pacote que chega à rede, com uma porta de destino (*external port*) é traduzido para uma porta de destino diferente (*internal port*).
- **Cenário comum em redes domésticas.**

Configuração de *Static NAT*: LAN1



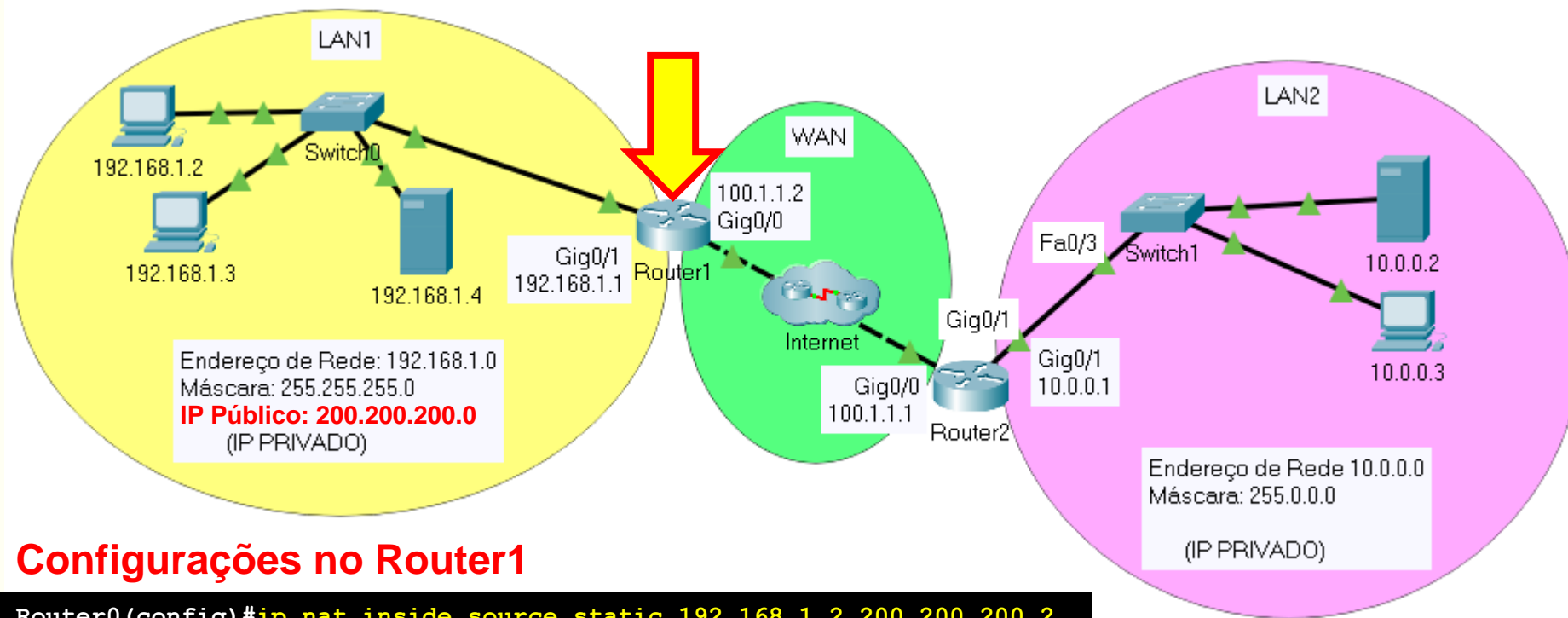
Configuração de *Static NAT*: LAN1

O endereço IP
192.168.1.2
Não pode ser roteado na
Internet



O endereço IP
10.0.0.2
Não pode ser roteado na
Internet

Configuração de *Static NAT*: LAN1



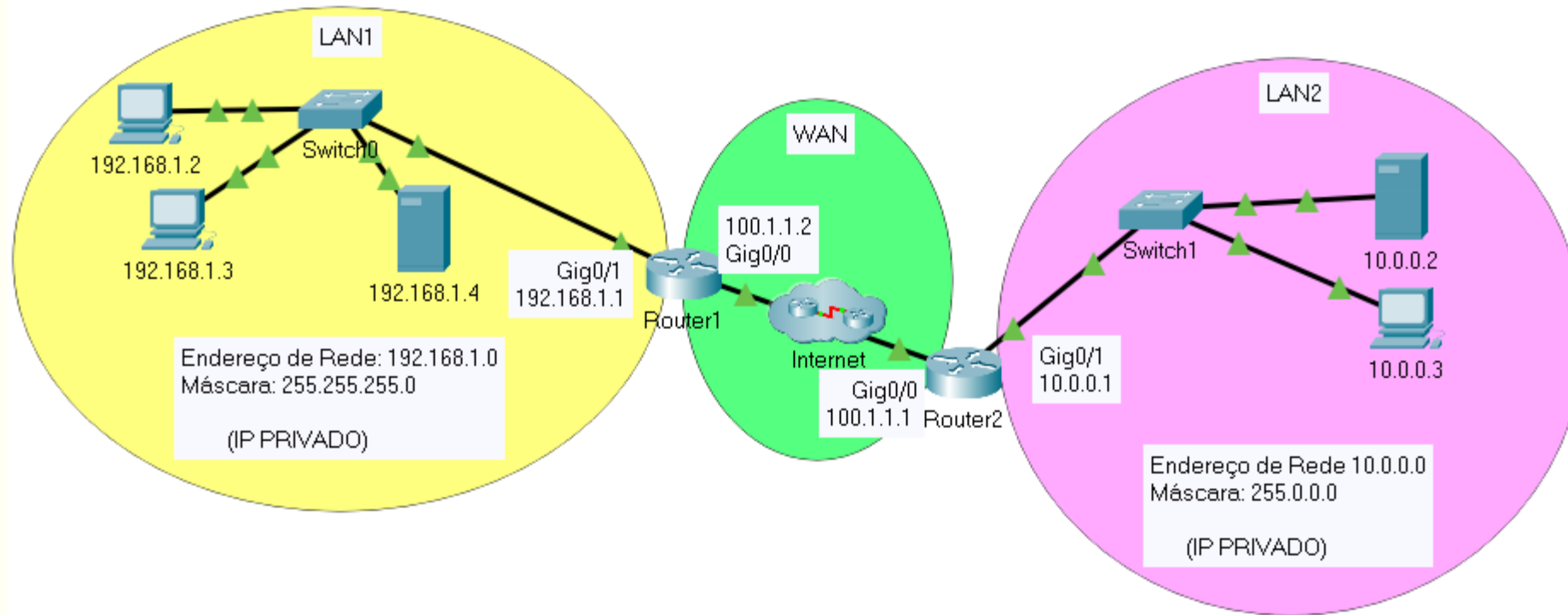
Configurações no Router1

```
Router0 (config) #ip nat inside source static 192.168.1.2 200.200.200.2
Router0 (config) #ip nat inside source static 192.168.1.3 200.200.200.3
Router0 (config) #ip nat inside source static 192.168.1.4 200.200.200.4
Router0 (config) #interface gig0/1
Router0 (config-if) #ip nat inside
Router0 (config-if) #interface gig0/0
Router0 (config-if) #ip nat outside
```

Configuração NAT estático no Router 1.
Poderia ser NAT dinâmico ou PAT.

DNAT (*Destination Network Address Translation*)

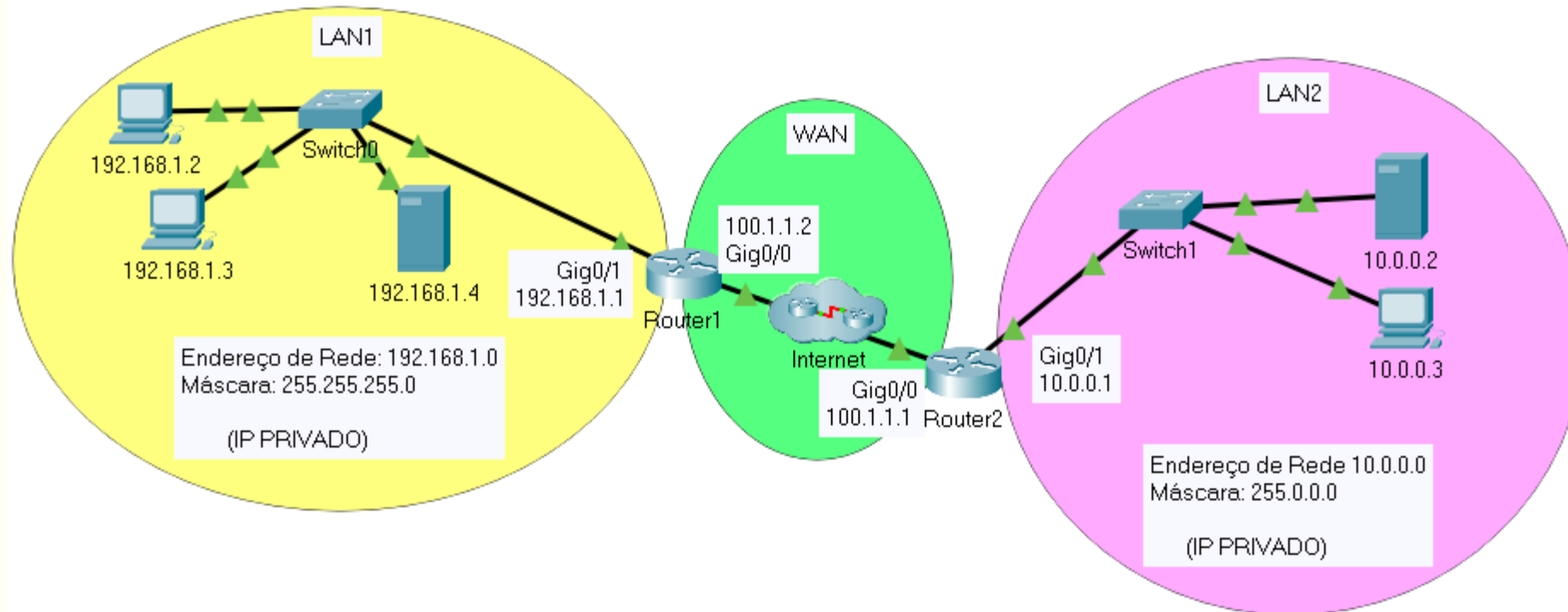
PAT (*Port Address Translation*)



No cenário acima o NAT pode ser configurado para realizar o redirecionamento de endereços e portas de forma que um dado serviço na rede local **LAN2**, em execução no servidor configurado com IP privado **10.0.0.2**, possa ser acessado por equipamentos em outra rede na Internet (por exemplo, pelos funcionários da empresa em suas casas).

DNAT (*Destination Network Address Translation*)

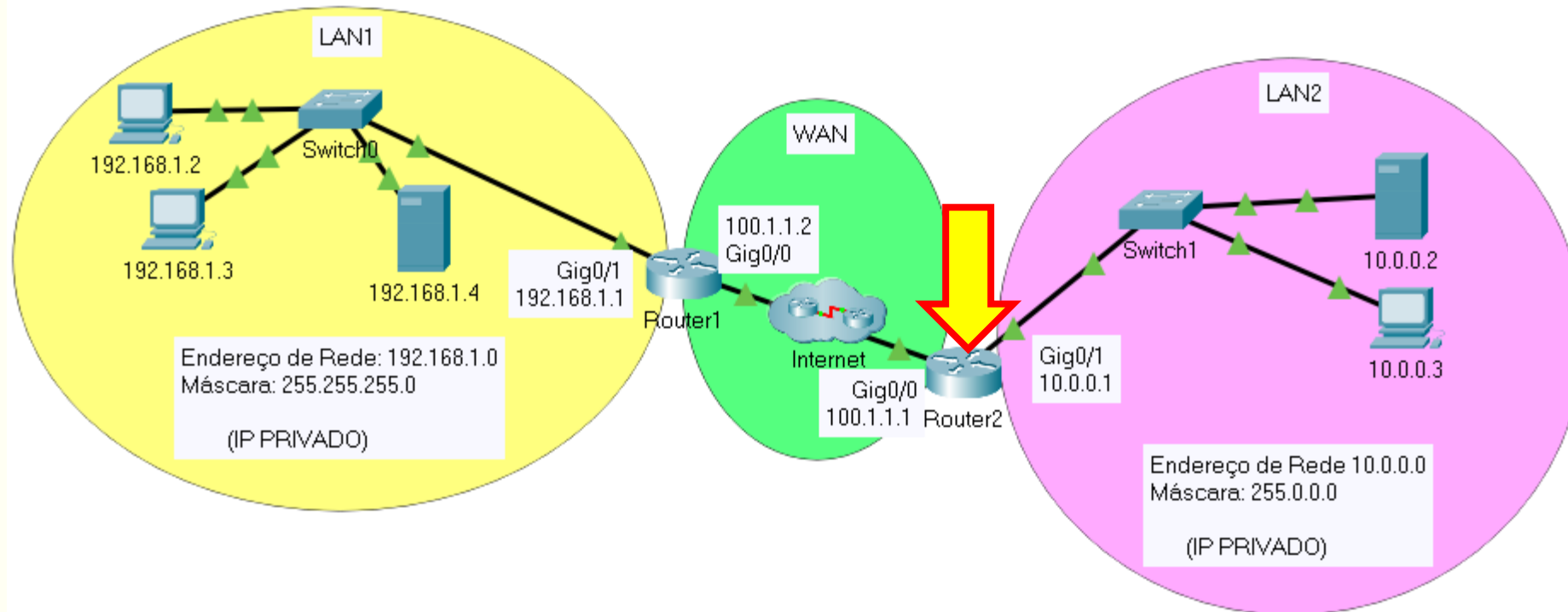
PAT (*Port Address Translation*)



- A rede local **LAN2** utiliza o endereço de rede privado **10.0.0.0** (endereço **IP privado** descrito na RFC 1918), então o serviço WEB em execução no servidor (**10.0.0.2**) **NÃO** pode ser acessado a partir de equipamentos na Internet, uma vez que esses endereços **não são roteáveis publicamente**.
- O primeiro ponto da empresa que tem acesso à Internet é seu roteador de borda (Router2) que possui o endereço público **100.1.1.1**, provido pelo Provedor Internet (ISP).

DNAT (*Destination Network Address Translation*)

PAT (*Port Address Translation*)



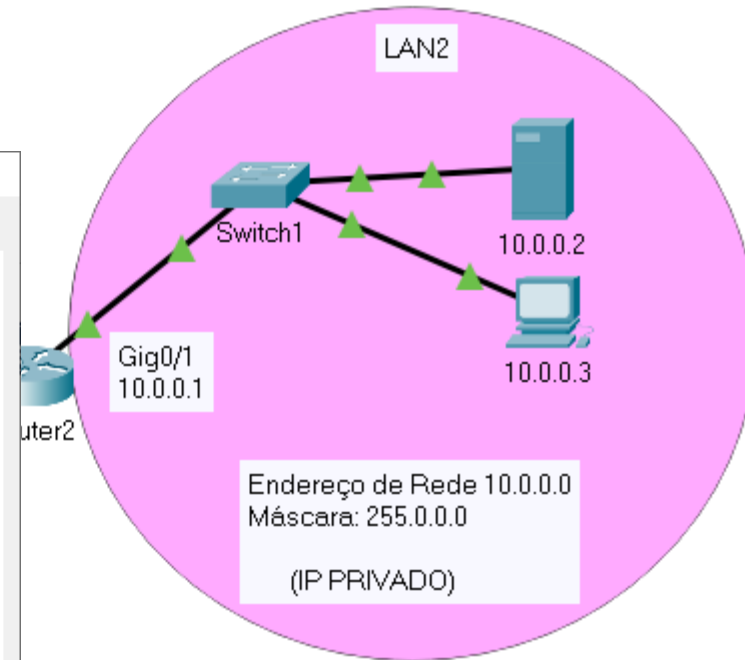
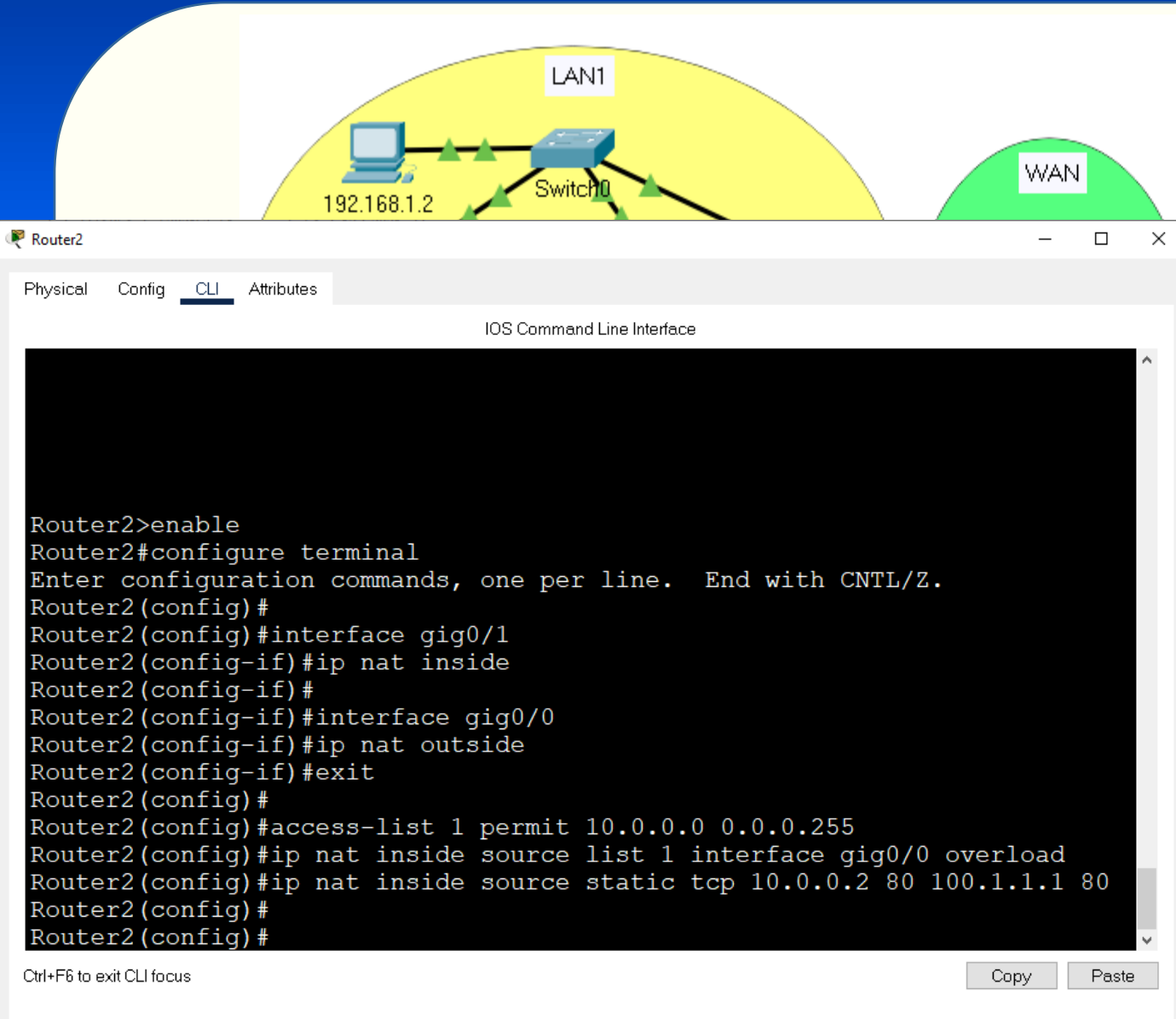
A configuração para habilitar o NAT na modalidade DNAT (*Destination Network Address Translation*), permitindo que todo acesso destinado ao endereço público do roteador de borda (**100.1.1.1**) na porta 80 seja redirecionado para o endereço privado **10.0.0.2** na porta 80 é:

```
Router2(config)# int gig0/1
Router2(config-if)# ip nat inside
Router2(config-if)# int gig0/0
Router2(config-if)# ip nat outside
Router2(config-if)# exit
Router2(config)# access-list 1 permit 10.0.0.0 0.0.0.255
Router2(config)# ip nat inside source list 1 interface gig0/0 overload
Router2(config)# ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80
```

Configuração NAT do tipo PAT no router2.
. Poderia ser NAT dinâmico ou estático

DNAT (*Destination Network Address Translation*)

PAT (*Port Address Translation*)

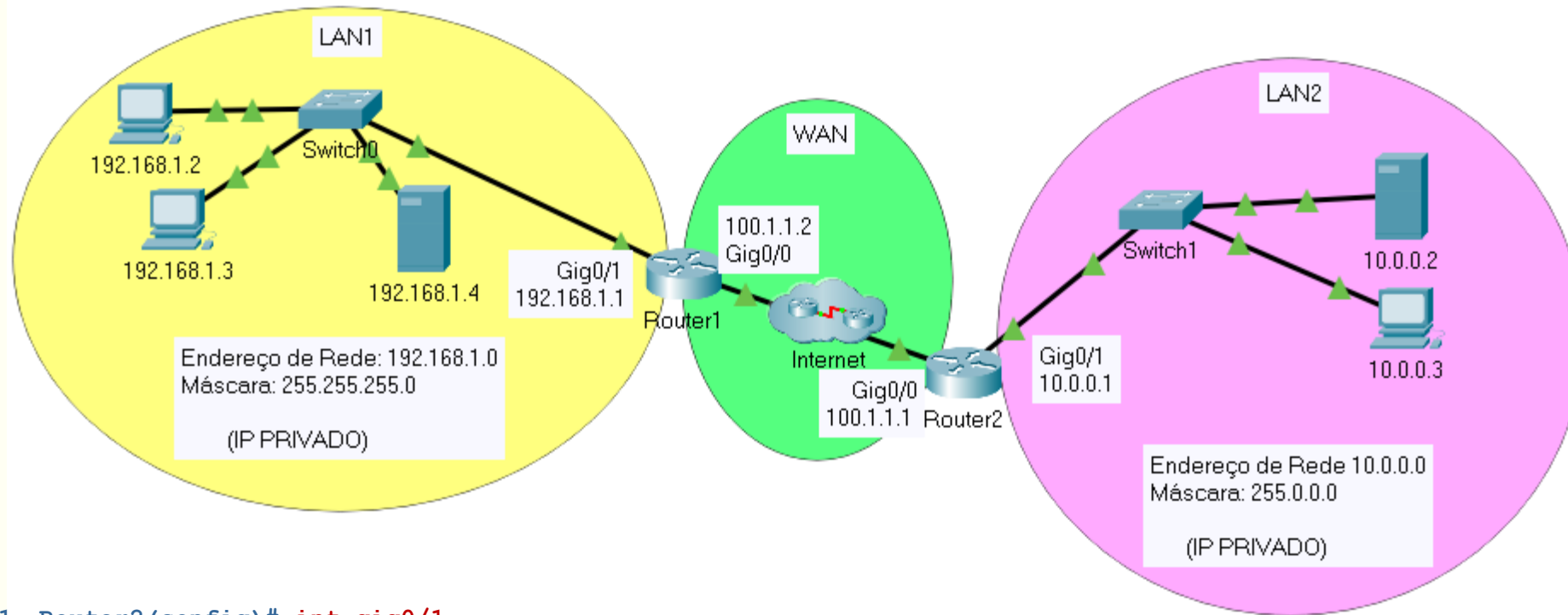


A configuração para habilitar o NAT na modalidade DNAT (*Destination Network Address Translation*), permitindo que todo acesso destinado ao endereço público do roteador de borda (100.1.1.1) na porta 80 seja redirecionado para o endereço privado 10.0.0.2 na porta 80 (http) é:

```
Router2(config)# int gig0/1
Router2(config-if)# ip nat inside
Router2(config-if)# int gig0/0
Router2(config-if)# ip nat outside
Router2(config-if)# exit
Router2(config)# access-list 1 permit 10.0.0.0 0.0.0.255
Router2(config)# ip nat inside source list 1 interface gig0/0 overload
Router2(config)# ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80
```

DNAT (*Destination Network Address Translation*)

PAT (*Port Address Translation*)

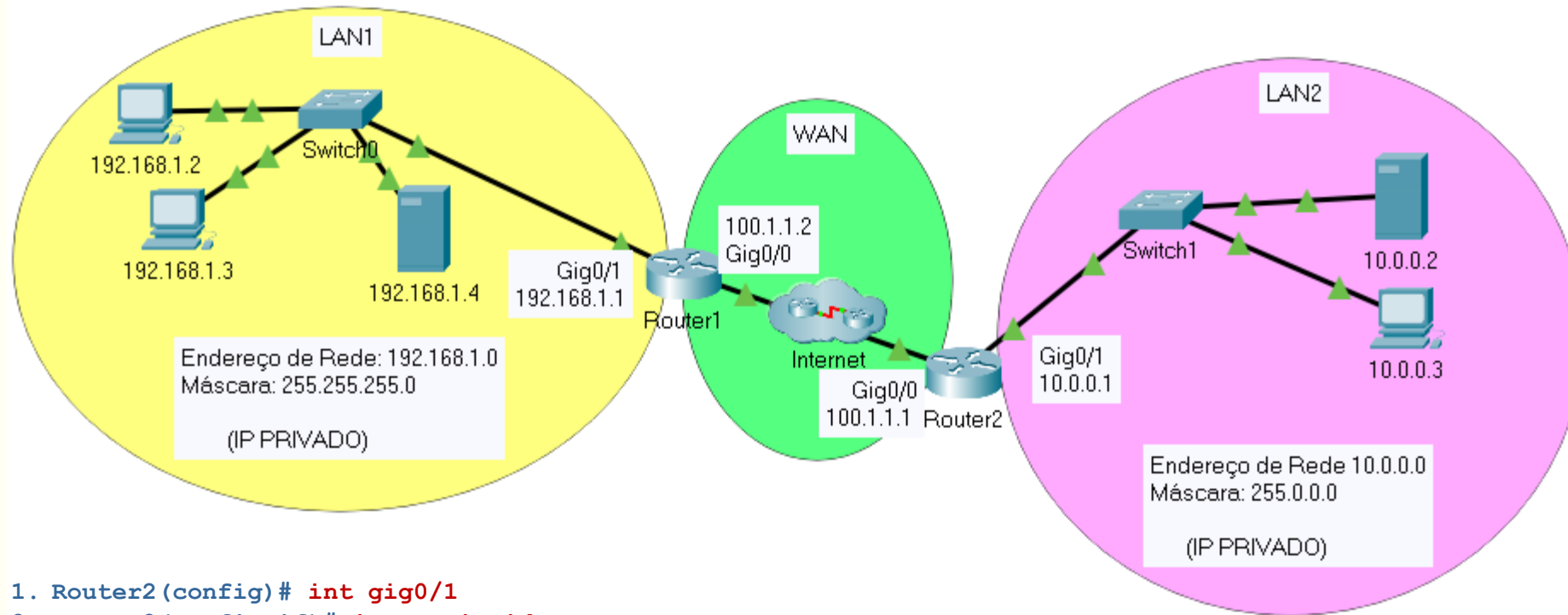


1. Router2(config)# **int gig0/1**
2. Router2(config-if)# **ip nat inside**
3. Router2(config-if)# **int gig0/0**
4. Router2(config-if)# **ip nat outside**
5. Router2(config-if)# **exit**
6. Router2(config)# **access-list 1 permit 10.0.0.0 0.0.0.255**
7. Router2(config)# **ip nat inside source list 1 interface gig0/0 overload**
8. Router2(config)# **ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80**

As configurações apresentadas nas linhas de 01 a 05 foram utilizadas para definir as **zonas inside** (rede interna privada) e **outside** (zona externa pública). Nas linhas 06 e 07 são realizadas as **configurações** para realizar a tradução dos endereços de origem para compartilhamento da Internet

DNAT (Destination Network Address Translation)

PAT (Port Address Translation)

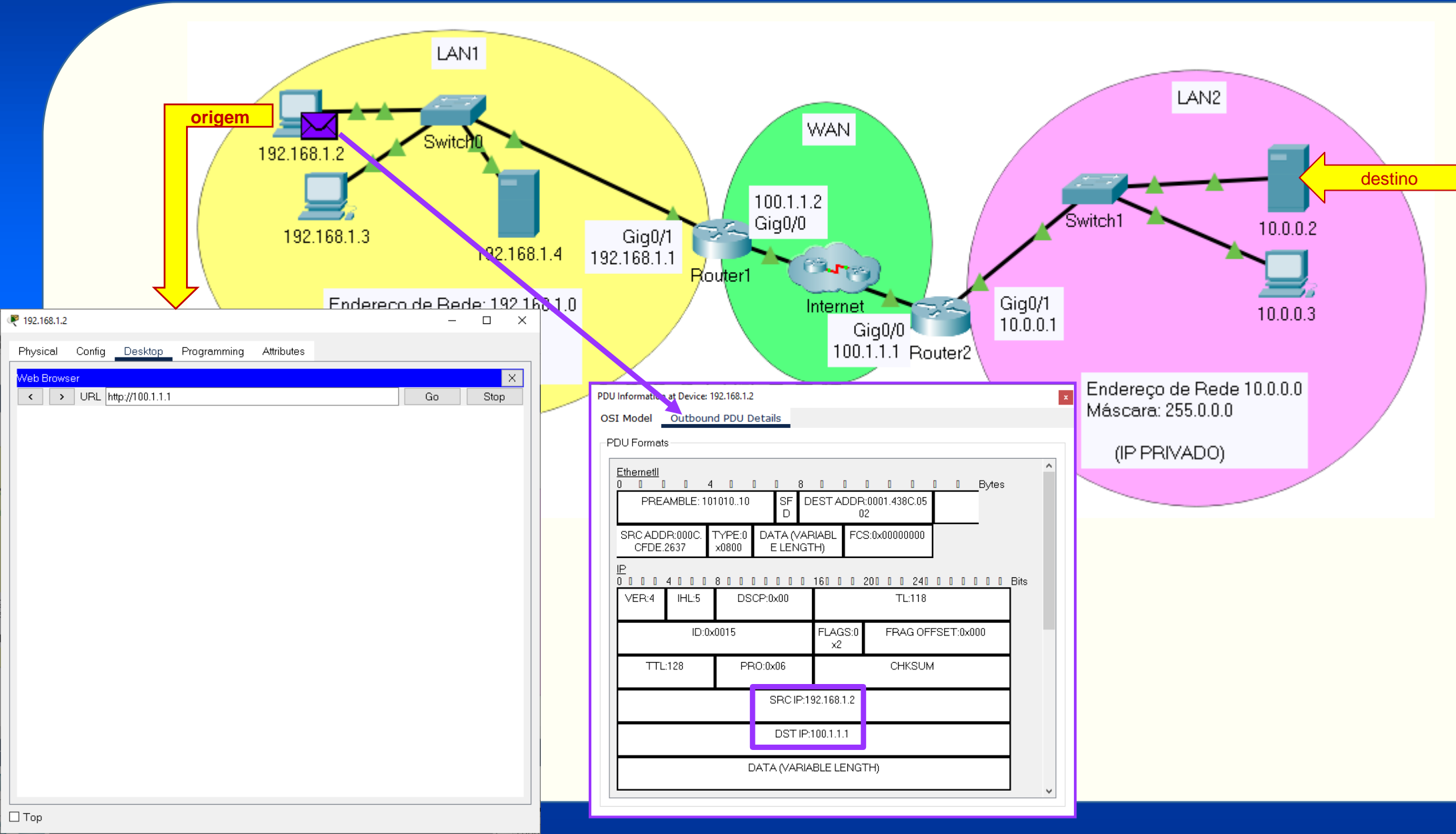


1. Router2(config)# **int gig0/1**
2. Router2(config-if)# **ip nat inside**
3. Router2(config-if)# **int gig0/0**
4. Router2(config-if)# **ip nat outside**
5. Router2(config-if)# **exit**
6. Router2(config)# **access-list 1 permit 10.0.0.0 0.0.0.255**
7. Router2(config)# **ip nat inside source list 1 interface gig0/0 overload**
8. Router2(config)# **ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80**

A configuração do NAT para fazer o redirecionamento de portas/endereços é exibida na linha 8 (destacada em **verde**), onde é realizado o mapeamento estático entre um endereço **inside** e outro **outside** (e suas respectivas portas TCP). Portanto, é "informado" ao roteador que todos os pacotes destinados ao seu endereço público na porta 80 (**100.1.1.1:80**) devem ser encaminhados para o endereço privado do servidor na porta padrão (**10.0.0.2:80**).

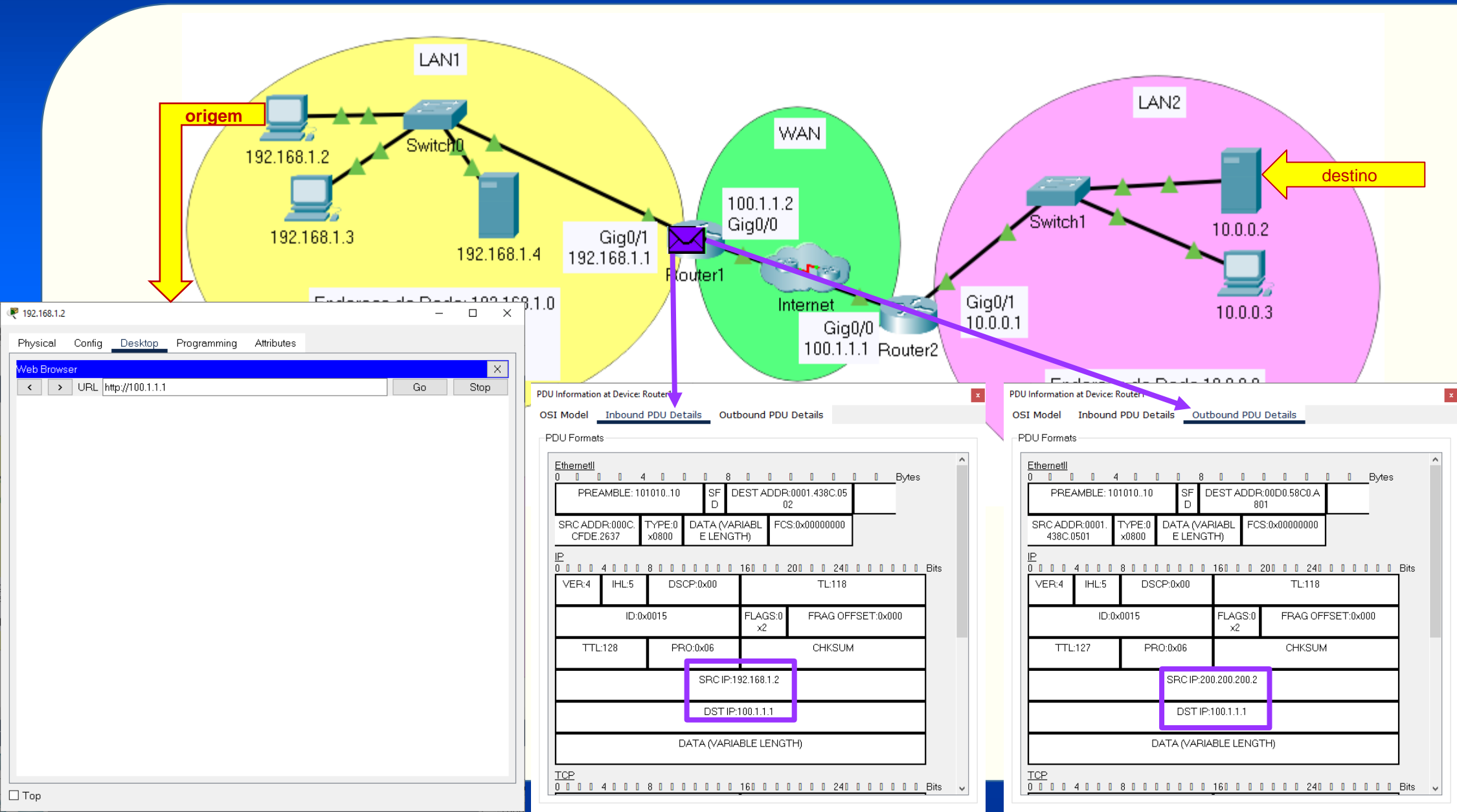
DNAT (Destination Network Address Translation)

PAT (Port Address Translation)



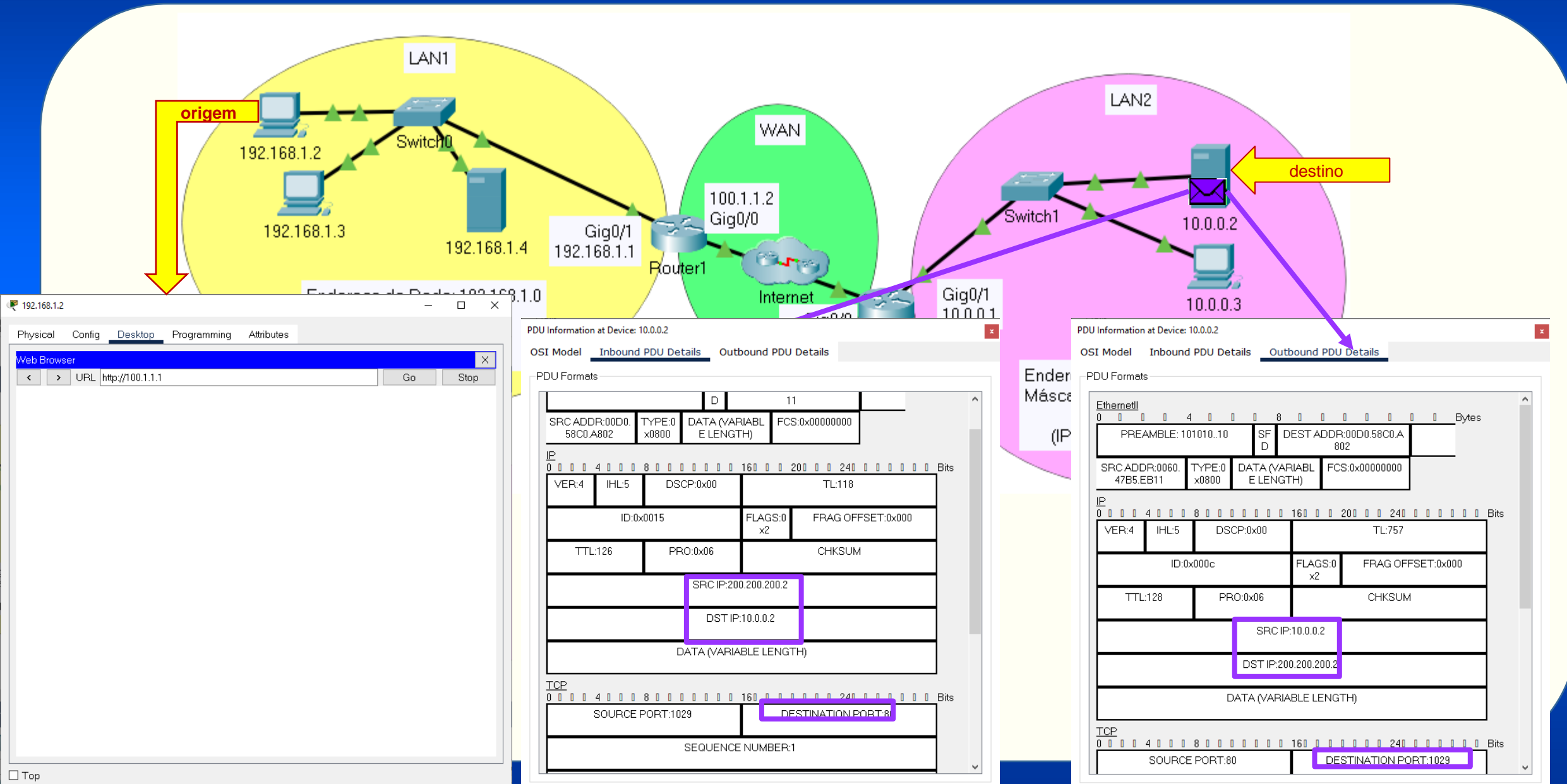
DNAT (Destination Network Address Translation)

PAT (Port Address Translation)



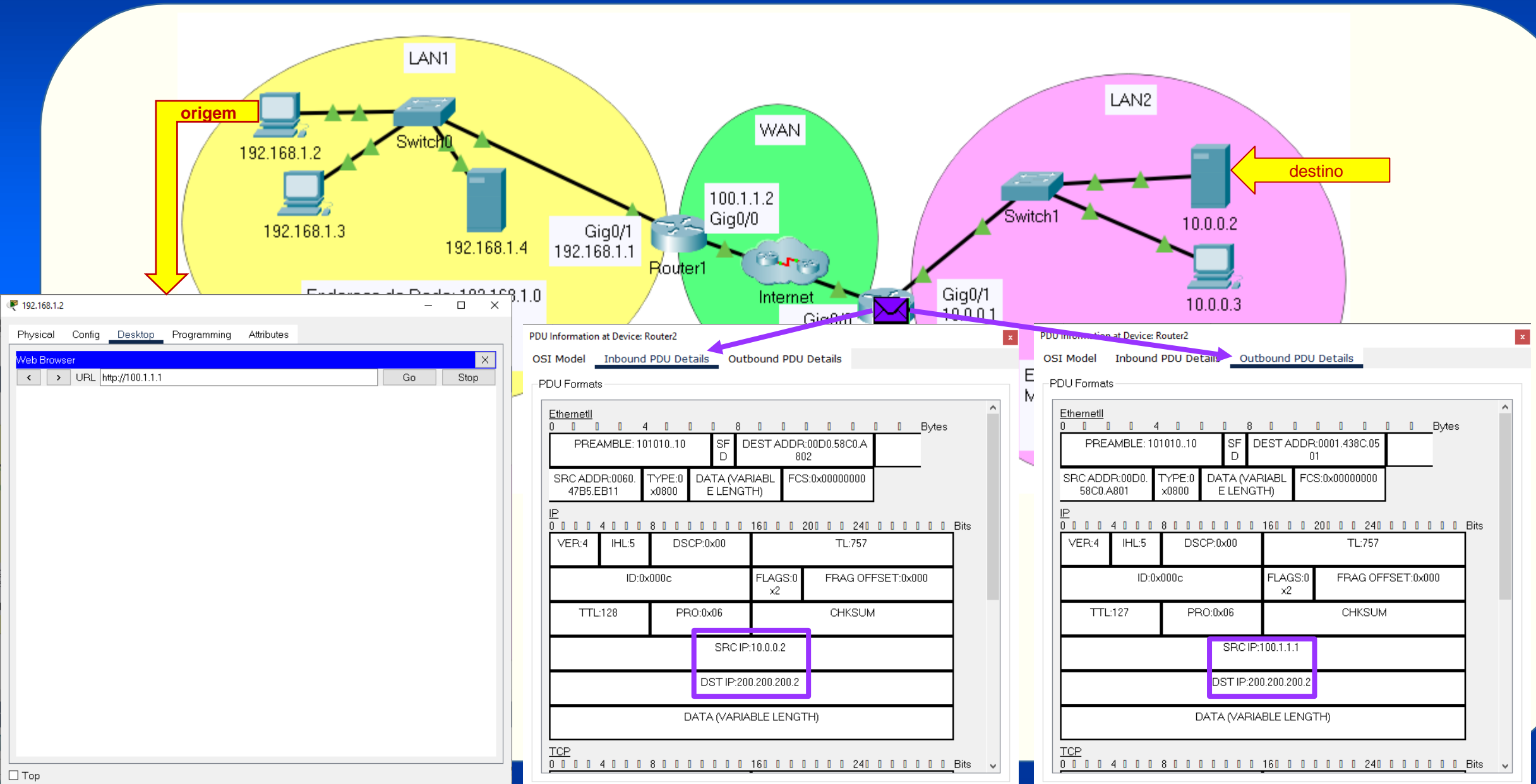
DNAT (Destination Network Address Translation)

PAT (Port Address Translation)



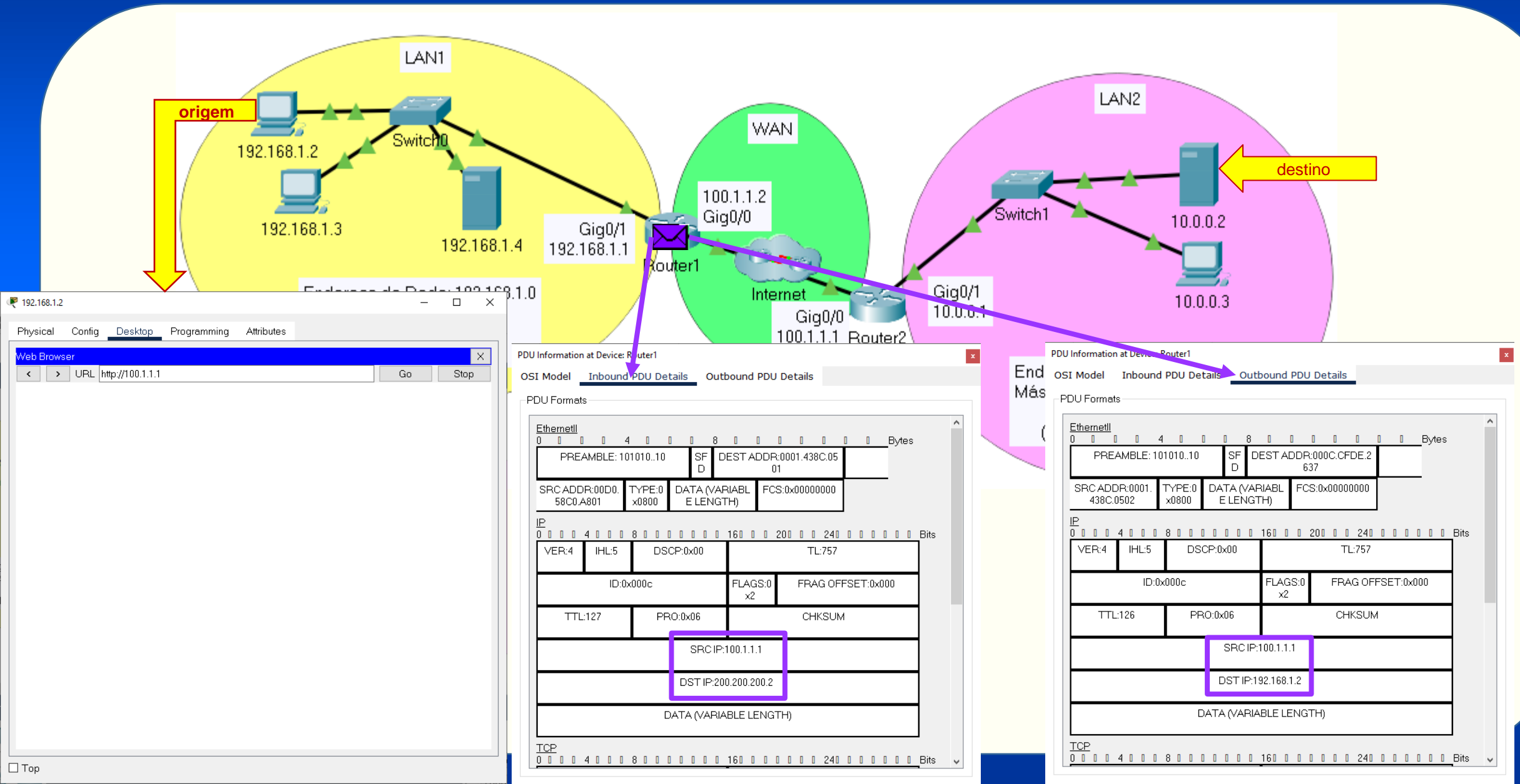
DNAT (Destination Network Address Translation)

PAT (Port Address Translation)



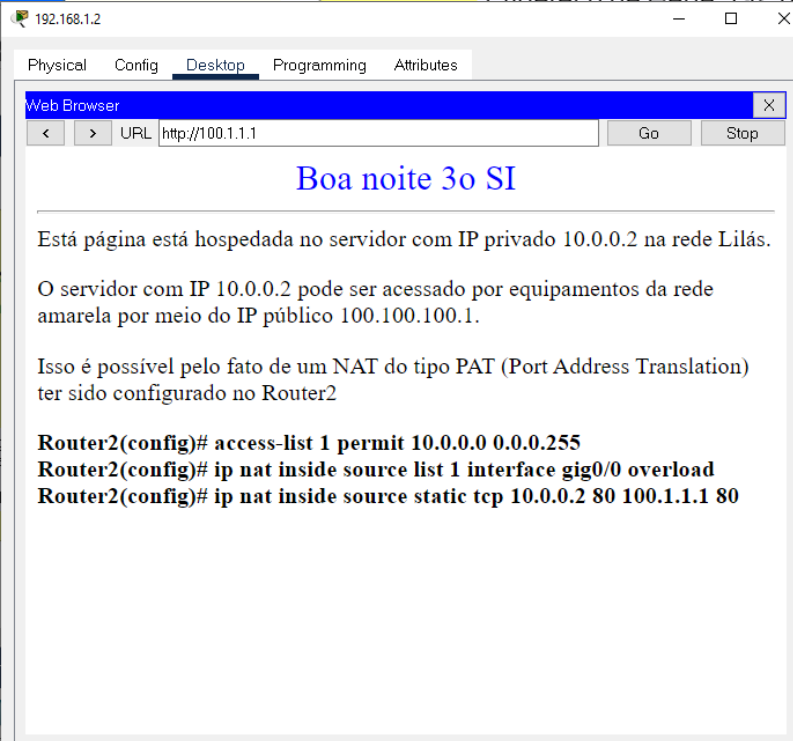
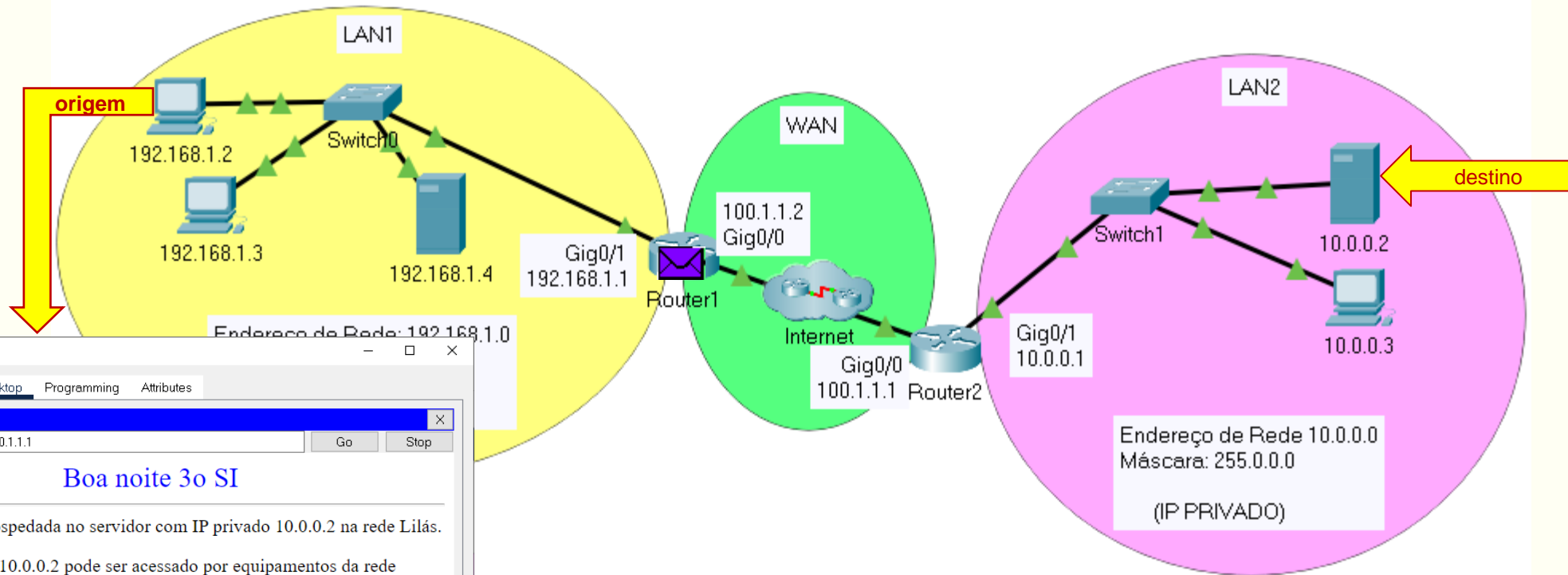
DNAT (Destination Network Address Translation)

PAT (Port Address Translation)



DNAT (*Destination Network Address Translation*)

PAT (*Port Address Translation*)



Limitações do NAT

- Os hosts por trás dos roteadores com o NAT habilitado não possuem conectividade fim-a-fim e não podem participar em alguns protocolos da Internet.
- Por reconhecer apenas os protocolos **TCP** e **UDP**, não é possível estabelecer uma conexão que não utilize um desses protocolos.
- Serviços que exigem o início de conexões **TCP** do lado externo da rede, ou protocolos *stateless*, como aqueles que utilizam o **UDP**, podem ser comprometidos.
- A menos que o roteador com NAT faça um esforço específico para suportar tais protocolos, os pacotes recebidos não podem alcançar seu destino.

Limitações do NAT

- O uso de NAT também complica os protocolos de tunelamento, como o IPSec porque o NAT modifica valores nos cabeçalhos que interferem nas verificações de integridade feitas pelo IPSec e por outros protocolos de tunelamento.
- A conectividade fim-a-fim tem sido um princípio fundamental da Internet, apoiado, por exemplo, pelo *Internet Architecture Board*.
- Os documentos arquiteturais atuais da Internet observam que o NAT é uma violação do princípio fim-a-fim, mas o NAT tem um papel valioso nas redes de comunicação.
- Há consideravelmente mais preocupação com o uso do NAT no IPv6, e muitos arquitetos do IPv6 acreditam que o IPv6 foi projetado para remover a necessidade do NAT.

Limitações do NAT

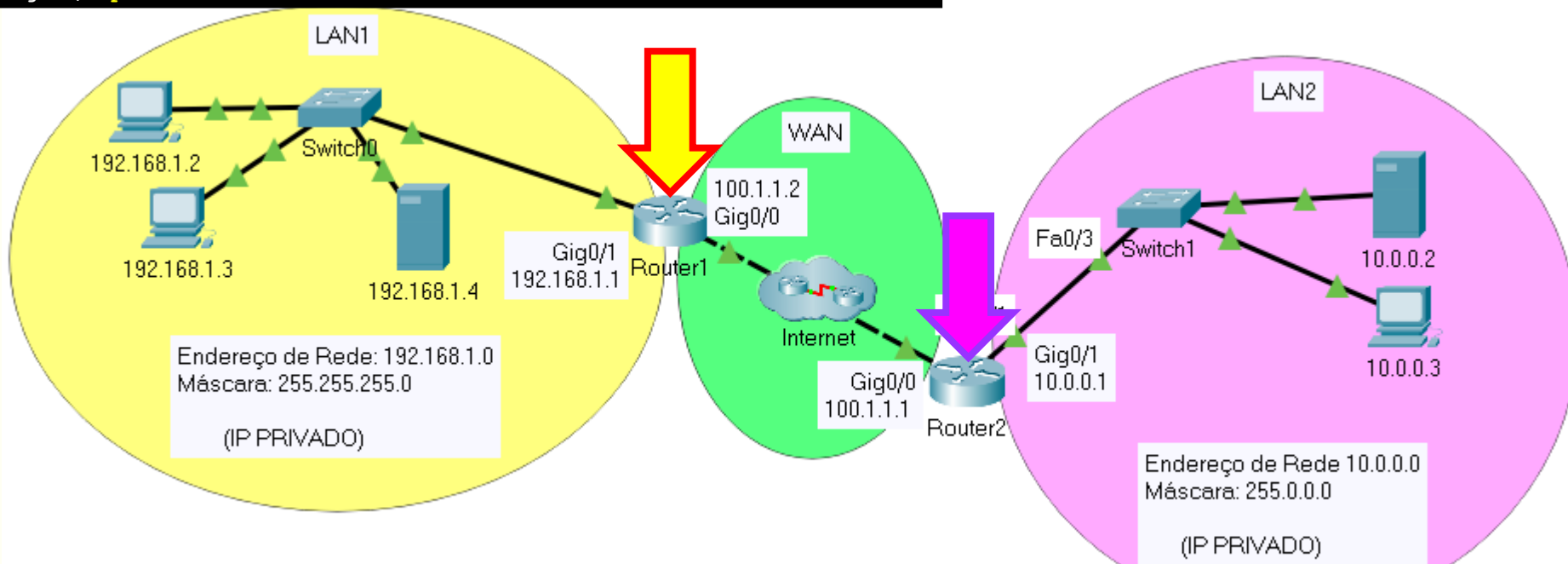
- Aplicativos como VOIP, videoconferência e outras aplicações *peer-to-peer* devem usar as técnicas de NAT transversal para funcionar.

Atividade

Atividade: analise as configurações a seguir

```
Router1>enable
Router1#configure terminal
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router1(config)#ip nat inside source list 1 interface gig0/0 overload
Router1(config)#
Router1(config)#interface gig0/1
Router1(config-if)#ip nat inside
Router1(config-if)#interface gig0/0
Router1(config-if)#ip nat outside
```

Configuração NAT overload
no Router 1



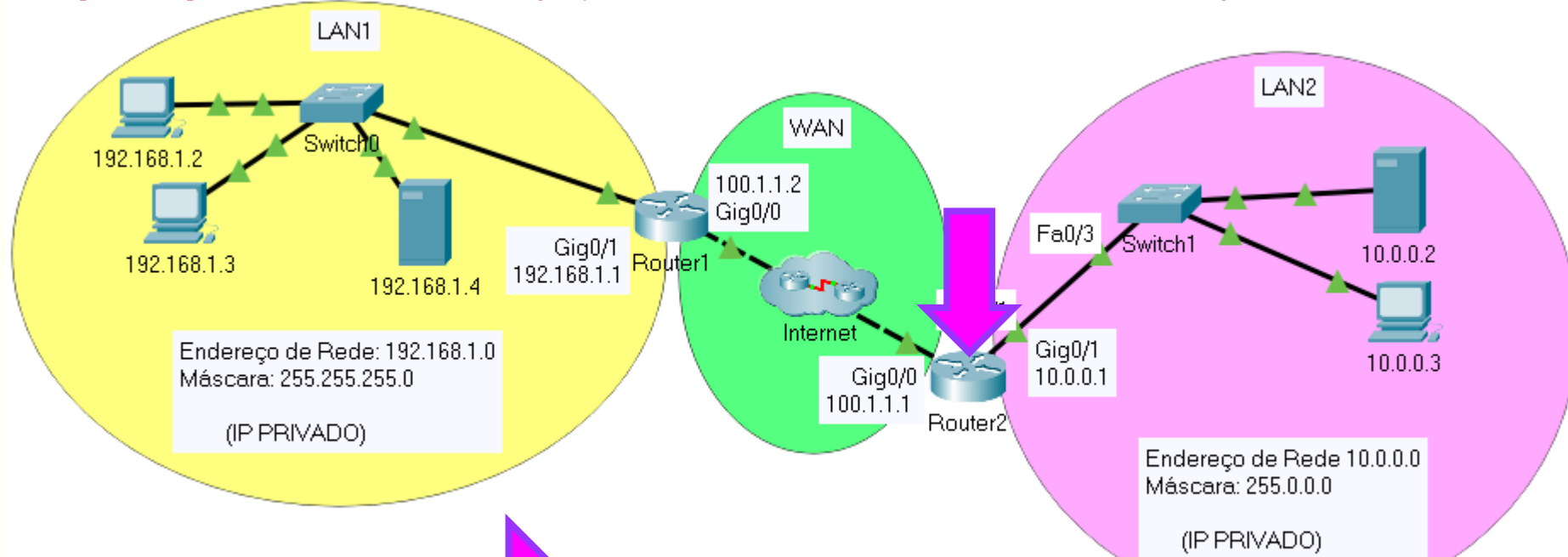
Configuração NAT overload com PAT no Router 2.

```
Router2(config)# int gig0/1
Router2(config-if)# ip nat inside
Router2(config-if)# int gig0/0
Router2(config-if)# ip nat outside
Router2(config-if)# exit
Router2(config)# access-list 1 permit 10.0.0.0 0.0.0.255
Router2(config)# ip nat inside source list 1 interface gig0/0 overload
Router2(config)# ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80
```

Atividade 1 : realize os passos descritos a seguir

Passos a serem seguidos para a Atividade 2 do 2º Checkpoint:

1. Utilize o arquivo 2oSem Aula 09 2022 - NAT - Parte II.pkt
2. Altere os endereços **IP PRIVADOS** dos equipamentos (**Servidor, PC e interface GIG0/1 do roteador**) da LAN2 (que atualmente utilizam endereços **PRIVADOS** da Classe A 10.0.0.0) para endereços **IP PRIVADOS** em uma faixa de rede Classe C **à sua escolha**;
3. Baseado no quadro abaixo, que apresenta as configurações realizadas em aula para o router2, altere a configuração (do **Router2**) para refletir a nova configuração de endereço IP.
4. Faça *upload* de um arquivo no formato .pdf (ATENÇÃO PARA A NECESSIDADE DE ENTREGA NO FORMATO .PDF) com seu nome e nova configuração realizada no **Router2** (**apenas o que foi alterado no quadro cinza abaixo**) e faça upload na área de trabalhos do portal da FIAP.
5. **ENTREGÁVEL:** apenas o arquivo no formato .PDF com a configuração realizada no **Router2** e o seu nome. (APENAS ISSO! Entregas em outros formatos não serão avaliadas!)



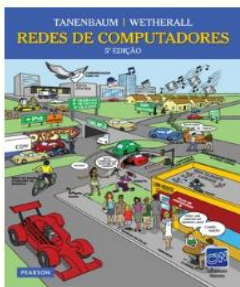
Configuração a ser alterada no roteador Router2 e que deverá ser entregue em um arquivo no formato .pdf (apenas a configuração ao lado após a alteração deverá ser entregue)

```
Router2(config)# int gig0/1
Router2(config-if)# ip nat inside
Router2(config-if)# int gig0/0
Router2(config-if)# ip nat outside
Router2(config-if)# exit
Router2(config)# access-list 1 permit 10.0.0.0 0.0.0.255
Router2(config)# ip nat inside source list 1 interface gig0/0 overload
Router2(config)# ip nat inside source static tcp 10.0.0.2 80 100.1.1.1 80
```

Referências Bibliográficas



Kurose, James F. Redes de computadores e a Internet: uma abordagem top-down/James F. Kurose e Keith W. Ross; 6ª edição, São Paulo: Addison Wesley, 2013. ISBN 978-85-8143-677-7. *FTP*. Página Inicial: 85– Página Final: 87. *VPN*: Página Inicial: 528– Página Final: 530



Tanenbaum, Andrew S; Wetherall, David. Redes de Computadores. São Paulo: Pearson Prentice Hall, 2011. 5ª edição americana. ISBN 978-85-7605-924-0. *Redes privadas*: Página Inicial: 515– Página Final: 516

Referência Complementar

- Comer, Douglas E., Interligação de Redes Com TCP/IP.
- Internet
 - <http://www.juliobattisti.com.br/tutoriais/gersonkonnus/iis6004.asp>