

ICMP

(Camada Inter-rede)

Prof. Dr. Luiz Arthur Feitosa dos Santos



luiz.arthur.feitosa.santos@gmail.com

<https://luizsantos.github.io/>



ICMP

Modelo TCP/IP

5

Aplicação

4

Transporte

3

Inter-rede

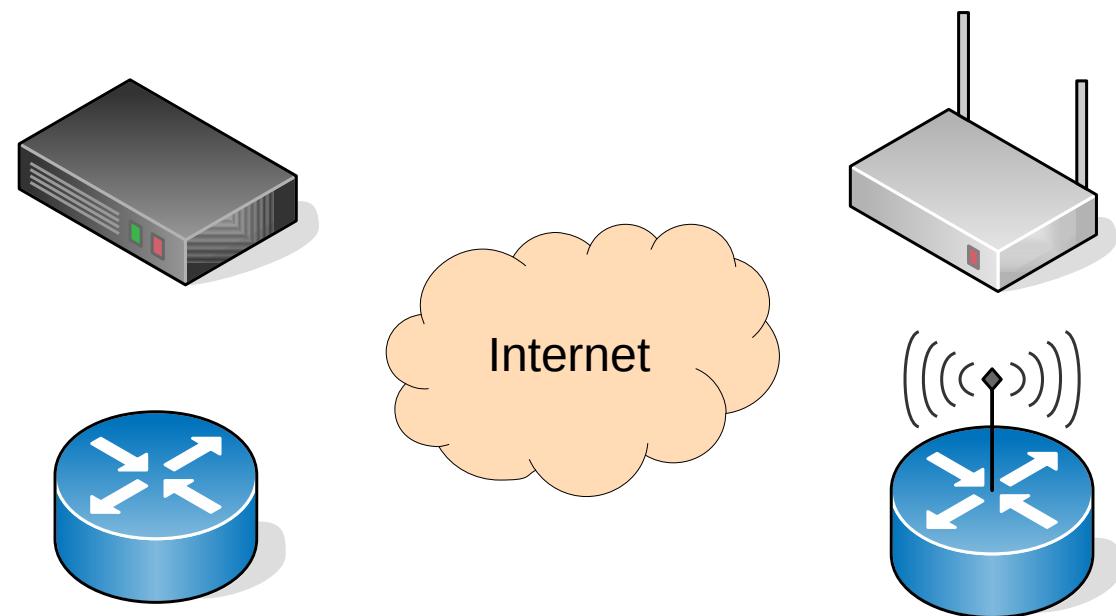
2

Enlace

1

Física

- Endereçamento e roteamento.



Camada de Inter-rede

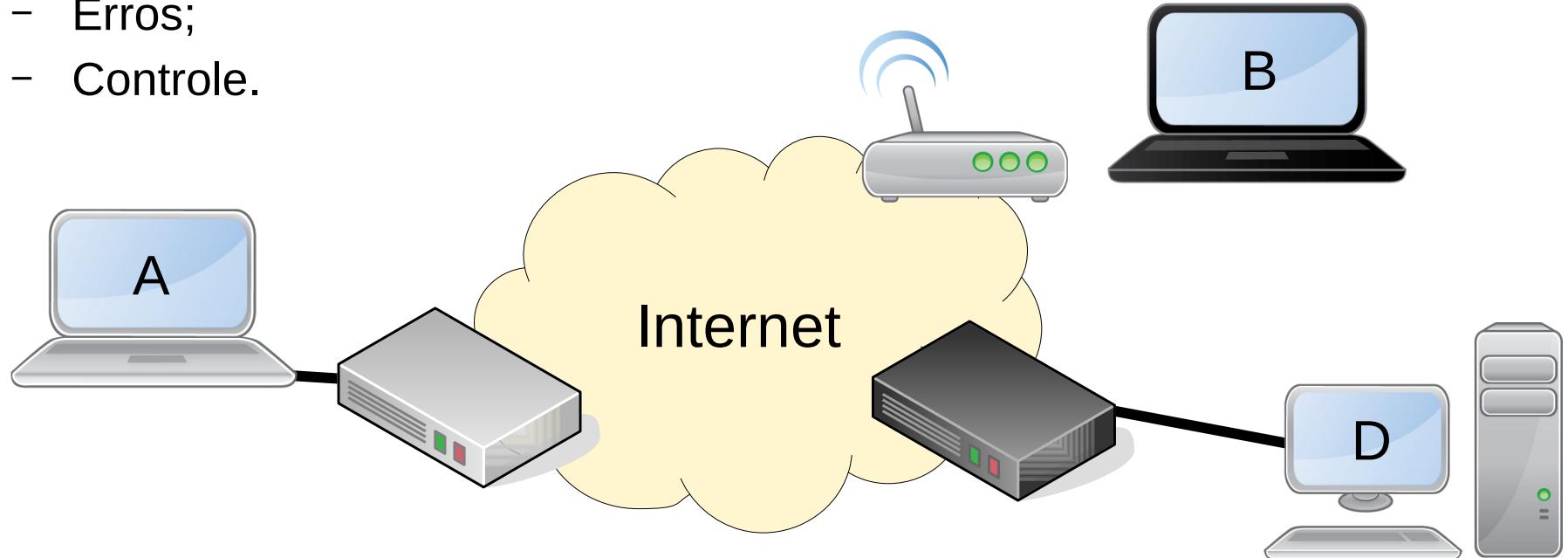
A tecnologia TCP/IP é foi criada para ser roteável e interligar vários *hosts* em uma rede tal como a Internet:

- IP (*Internet Protocol*);
 - Endereçamento IP (IPv4 e IPv6);
 - *Datagrama IP*.
- ARP (*Address Resolution Protocol*);
 - RARP (*Reverse Address Resolution Protocol*).
- ICMP (*Internet Control Message Protocol*).

ICMP

O ICMP, fornece informações a respeito da rede, tais informações podem ser algo como:

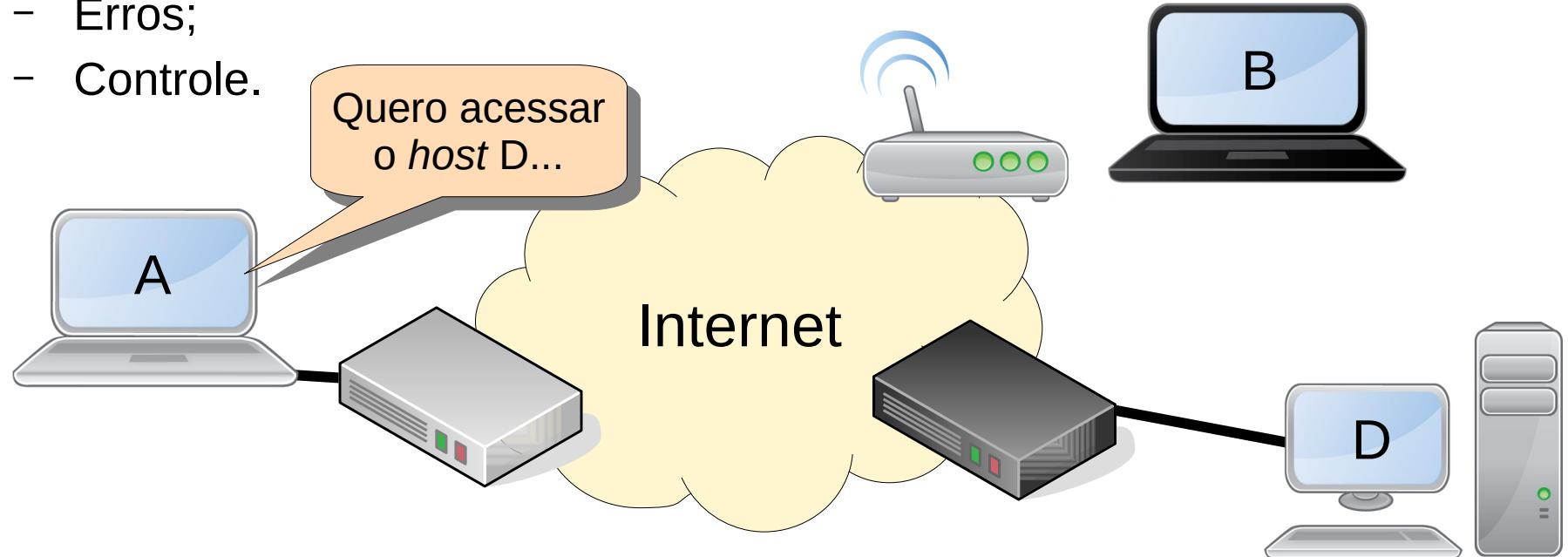
- Status da rede/*hosts*;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

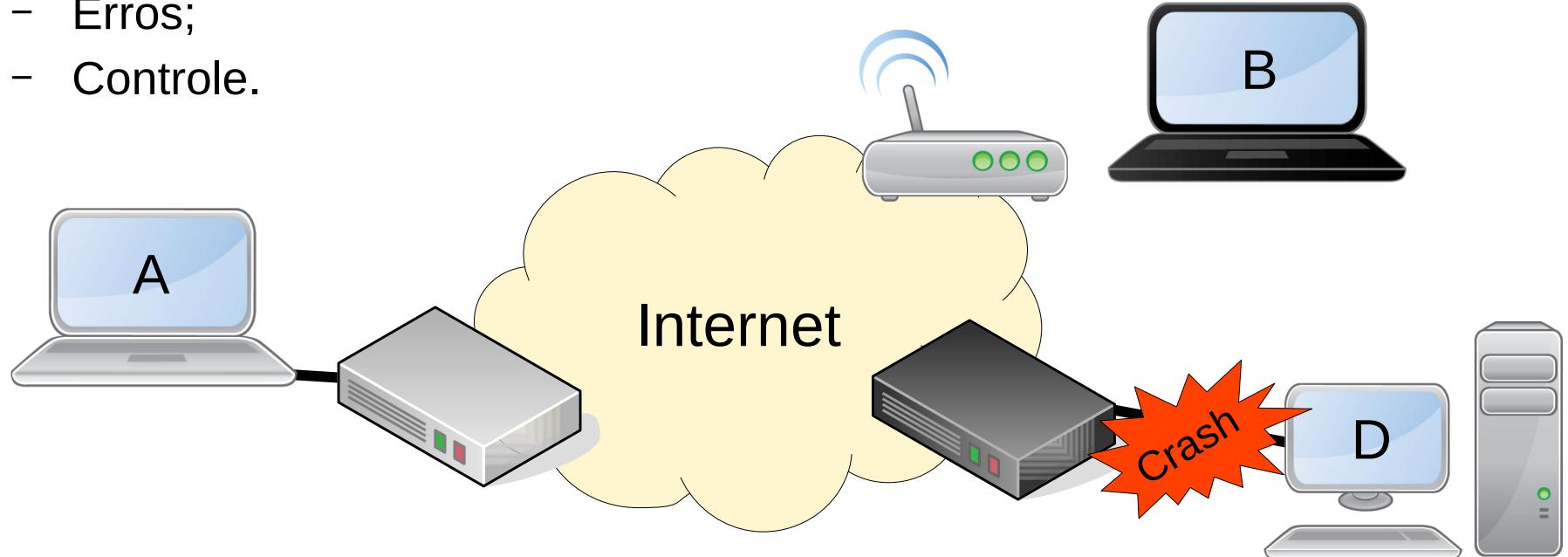
- Status da rede/hosts;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

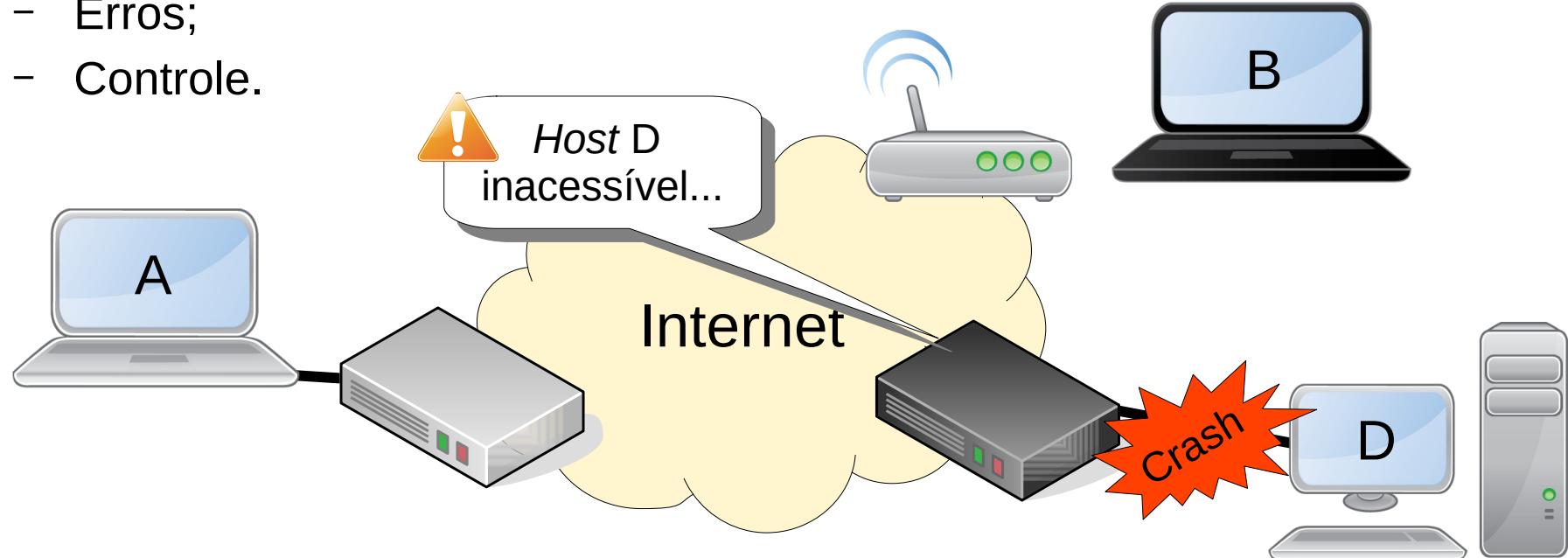
- Status da rede/*hosts*;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

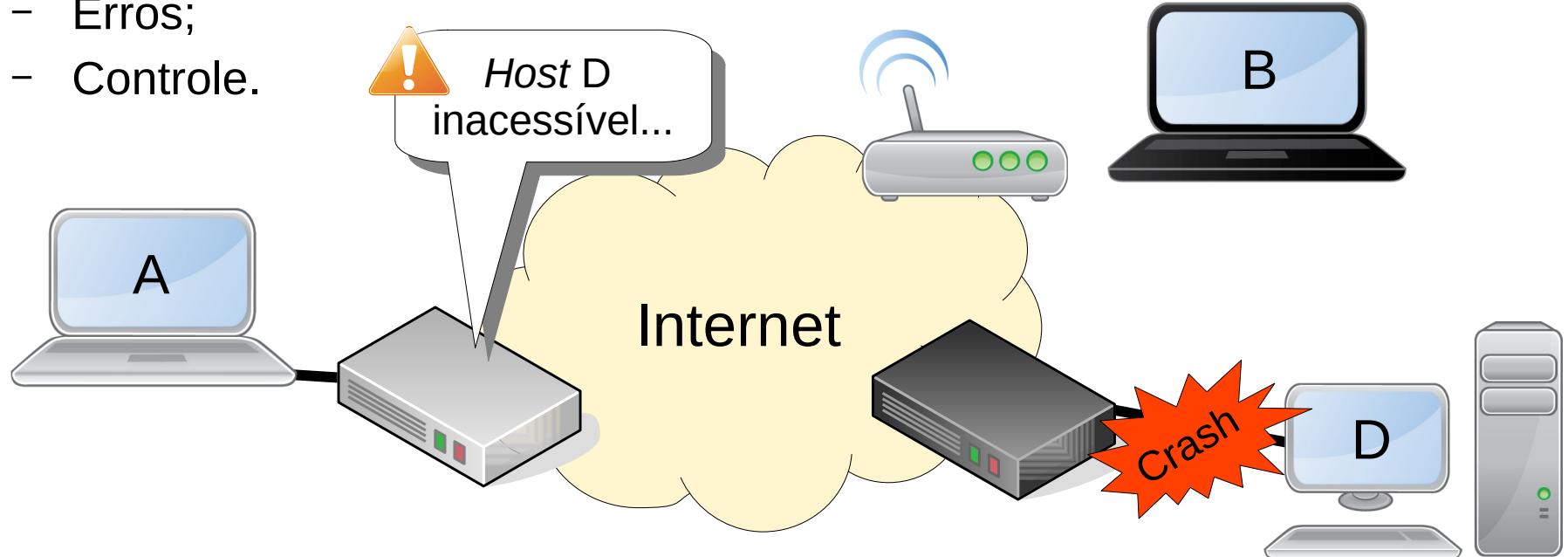
- Status da rede/hosts;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

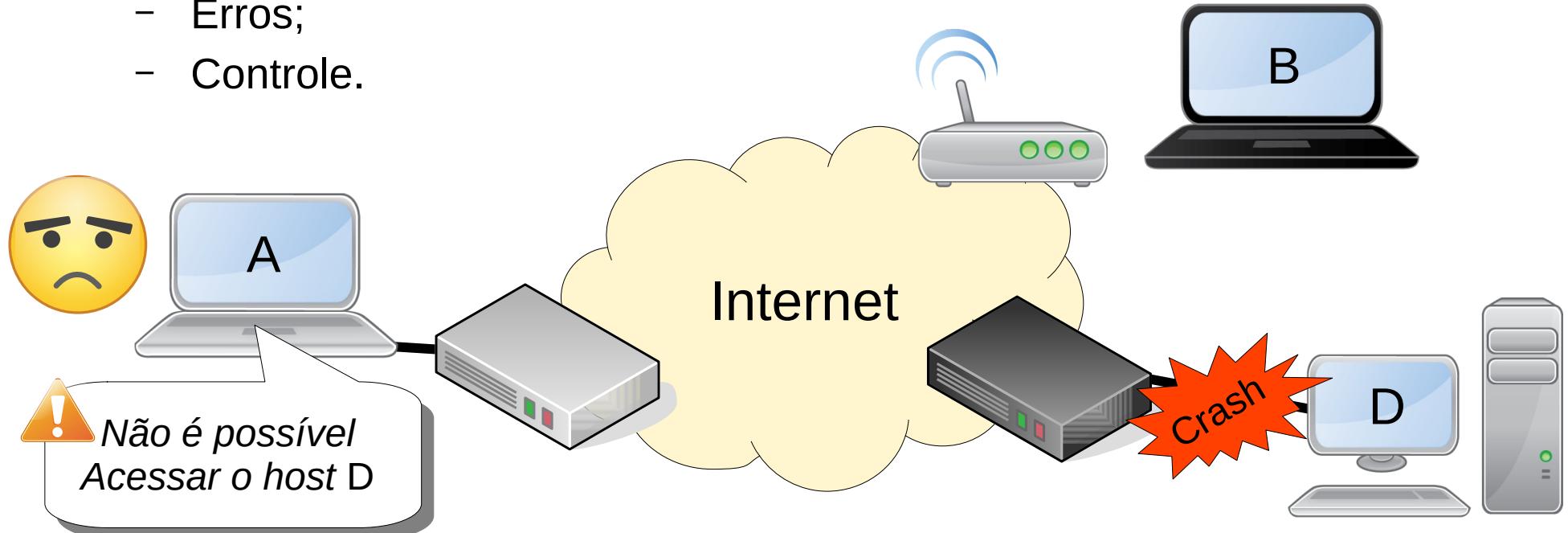
- Status da rede/hosts;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

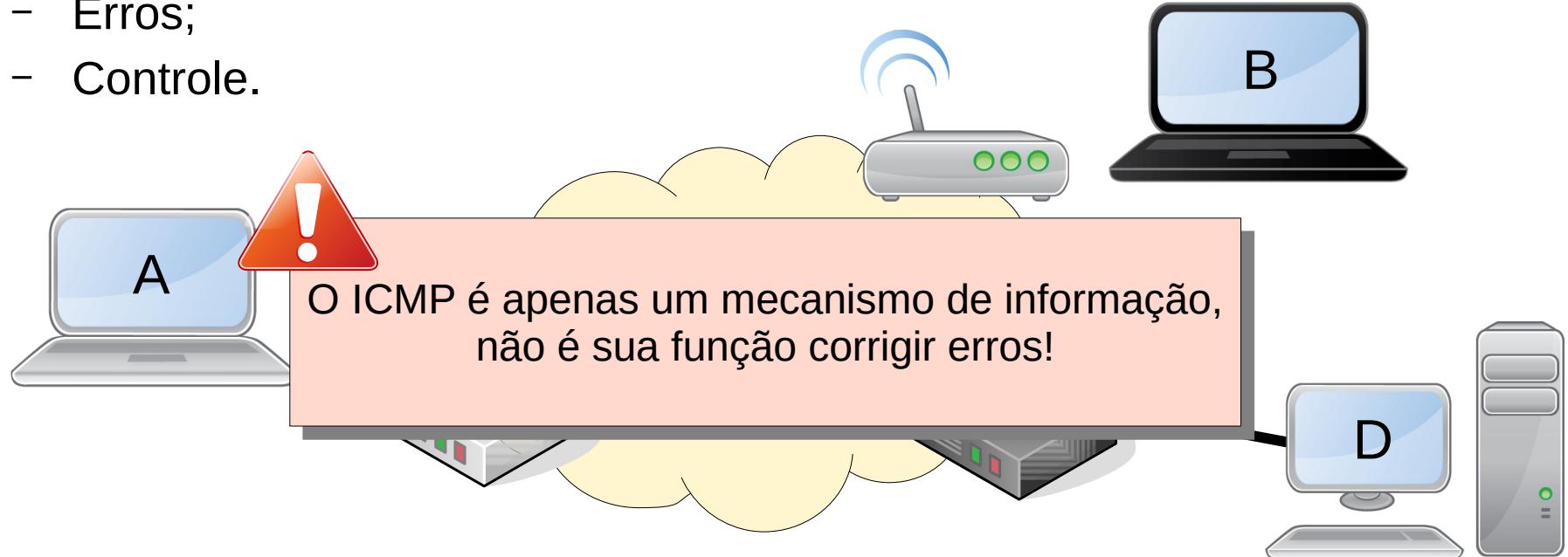
- Status da rede/hosts;
- Erros;
- Controle.



Camada de Inter-rede

O ICMP, fornece informações a respeito do da rede, tais informações podem ser algo como:

- Status da rede/hosts;
- Erros;
- Controle.

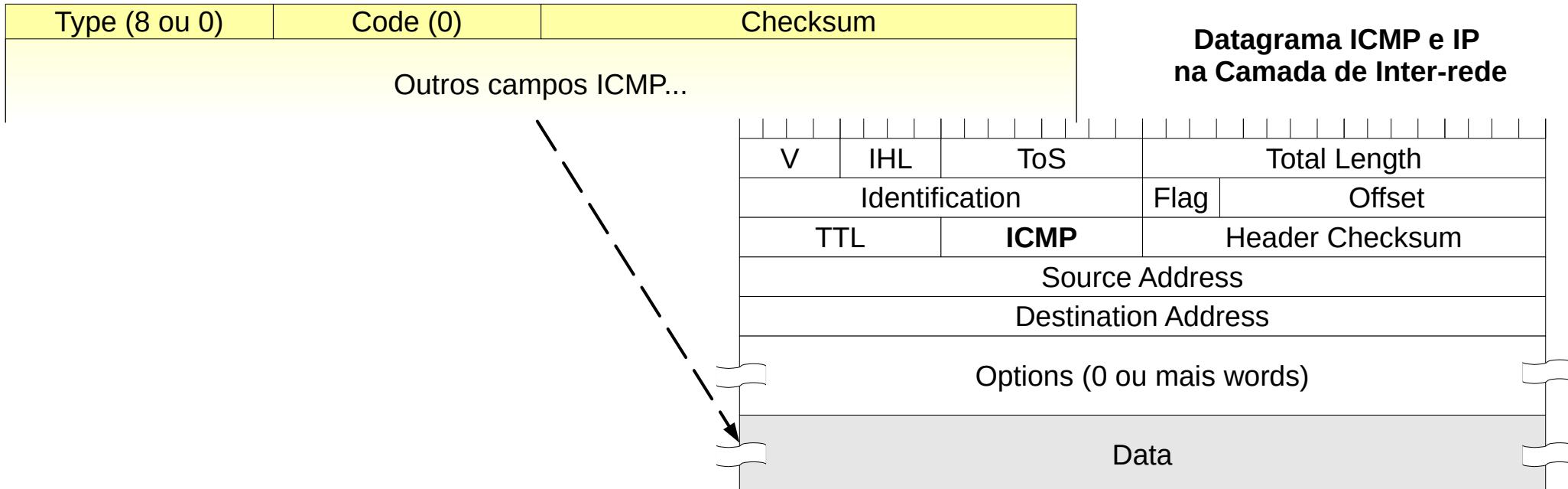


Camada de Inter-rede

Datagrama ICMP

| Type | Code | Checksum |
|-----------------------|------|----------|
| Outros campos ICMP... | | |

Camada de Inter-rede



| | | | | | |
|----------|-------------|--------|------------|------|----------|
| Preamble | Destination | Source | Type IP | Data | Checksum |
|----------|-------------|--------|------------|------|----------|

Quadro de Rede na camada de Enlace

ICMP

Mas o IP encapsula o ICMP que está na mesma Camada?

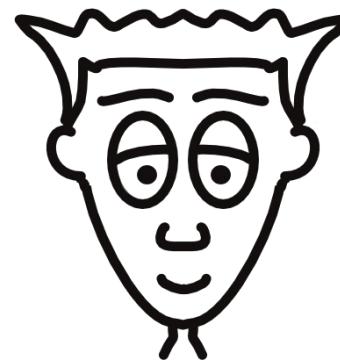
Não teria que ser uma informação da camada superior?



ICMP

Mas o IP encapsula o ICMP que está na mesma Camada?

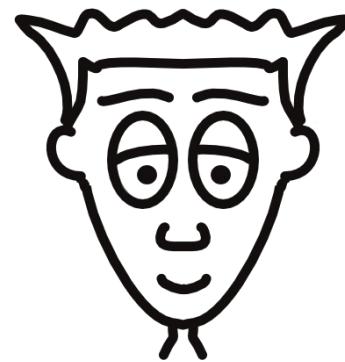
Não teria que ser uma informação da camada superior?



Na teoria sim,
mas na prática...

ICMP

Estou sabendo que o ICMP é o **ping**...



ICMP

Estou sabendo que o ICMP é o **ping**...

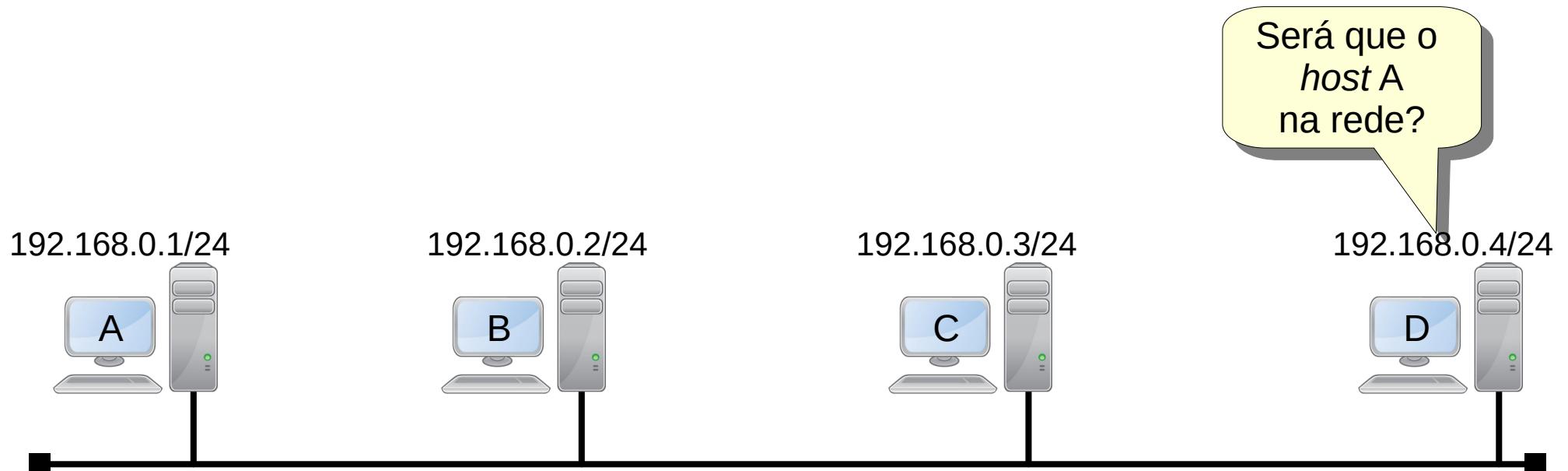


Mas o ping
é o mais
famoso!

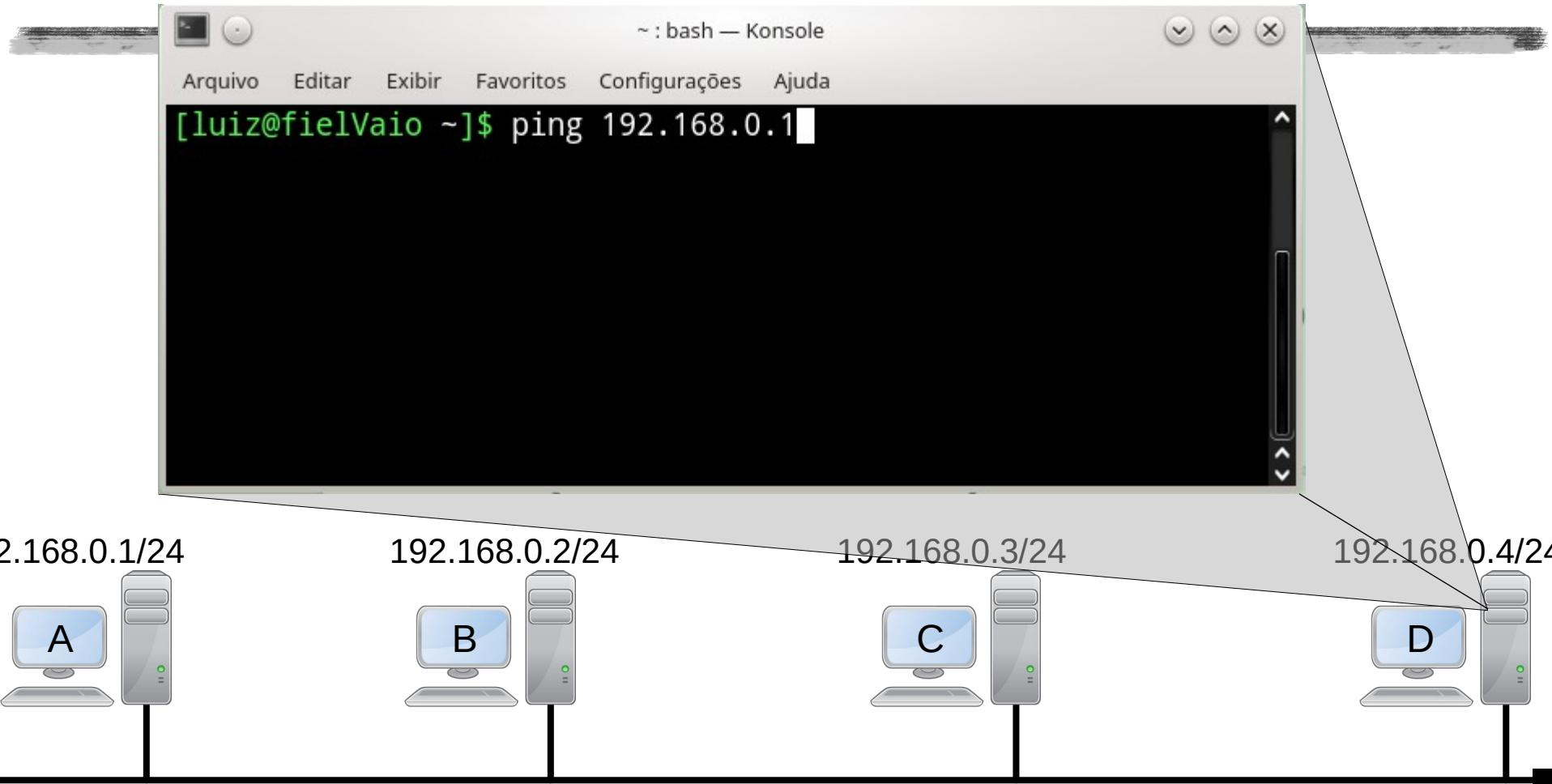
Não é bem
assim...

ICMP

ICMP – *echo request/echo reply (ping)*



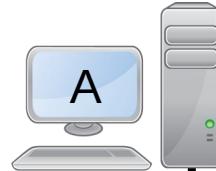
ICMP



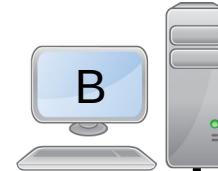
ICMP

| Type | Code | Checksum |
|------------|------|-----------------|
| Identifier | | Sequence Number |
| Data | | |

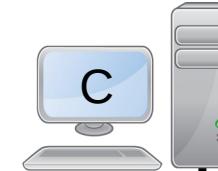
192.168.0.1/24



192.168.0.2/24



192.168.0.3/24



192.168.0.4/24



ICMP

| | | |
|--|----------|---------------------|
| Type (8) | Code (0) | Checksum (0xf91a) |
| Identifier (1) | | Sequence Number (1) |
| Data (oct 10, 2020 08:59:54.000000000 -03 – abcdefgh.....) | | |

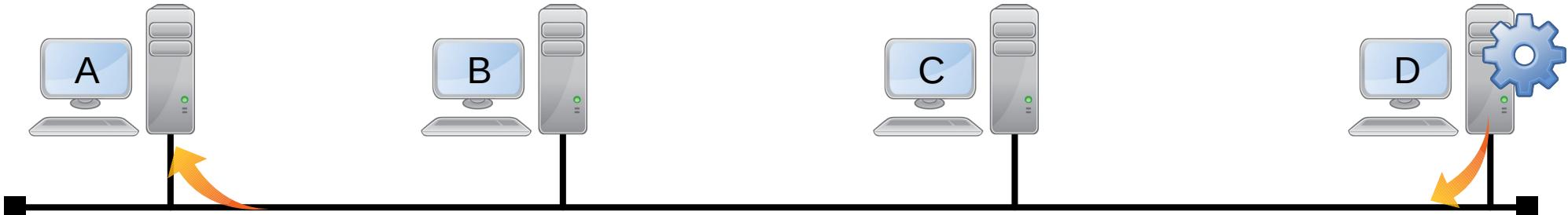


192.168.0.1/24

192.168.0.2/24

192.168.0.3/24

192.168.0.4/24

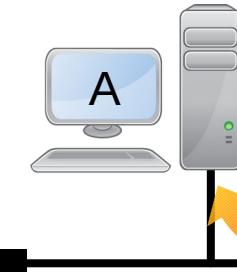


ICMP

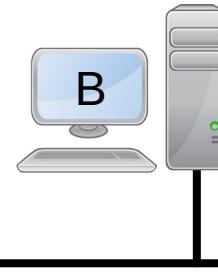
| | | |
|--|----------|---------------------|
| Type (8) | Code (0) | Checksum (0xf91a) |
| Identifier (1) | | Sequence Number (1) |
| Data (oct 10, 2020 08:59:54.000000000 -03 – abcdefgh.....) | | |



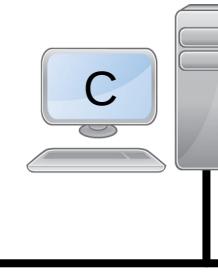
192.168.0.1/24



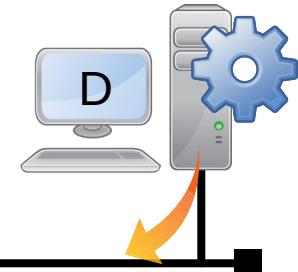
192.168.0.2/24



192.168.0.3/24

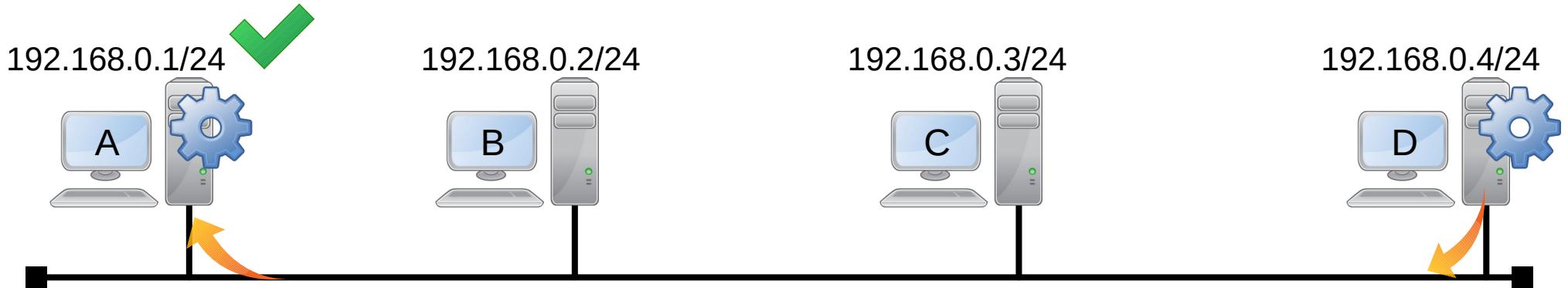


192.168.0.4/24

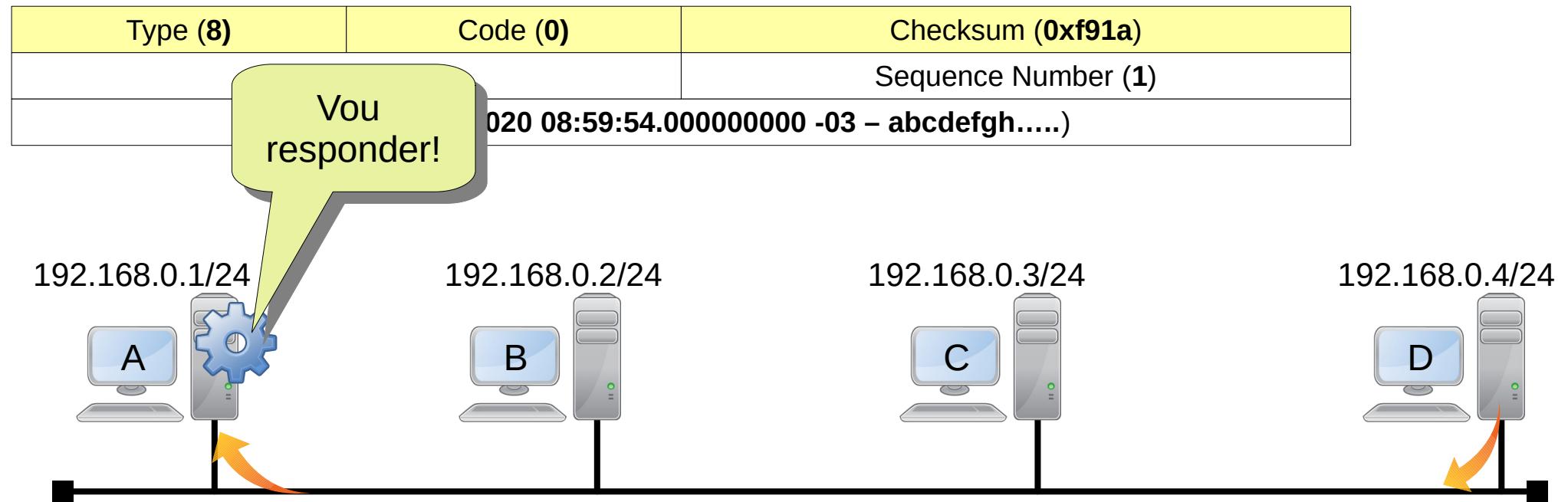


ICMP

| | | |
|--|----------|---------------------|
| Type (8) | Code (0) | Checksum (0xf91a) |
| Identifier (1) | | Sequence Number (1) |
| Data (oct 10, 2020 08:59:54.000000000 -03 – abcdefgh.....) | | |



ICMP

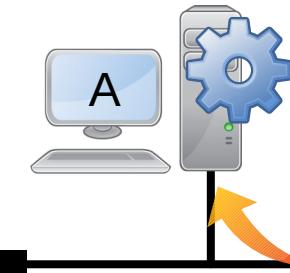


ICMP

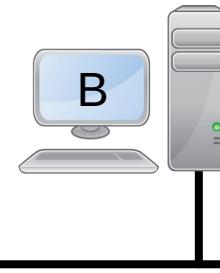
| | | |
|--|----------|---------------------|
| Type (0) | Code (0) | Checksum (0xf92b) |
| Identifier (1) | | Sequence Number (1) |
| Data (oct 10, 2020 08:59:54.000000000 -03 – abcdefgh.....) | | |



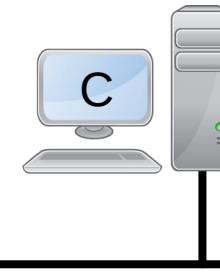
192.168.0.1/24



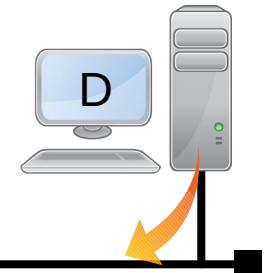
192.168.0.2/24



192.168.0.3/24

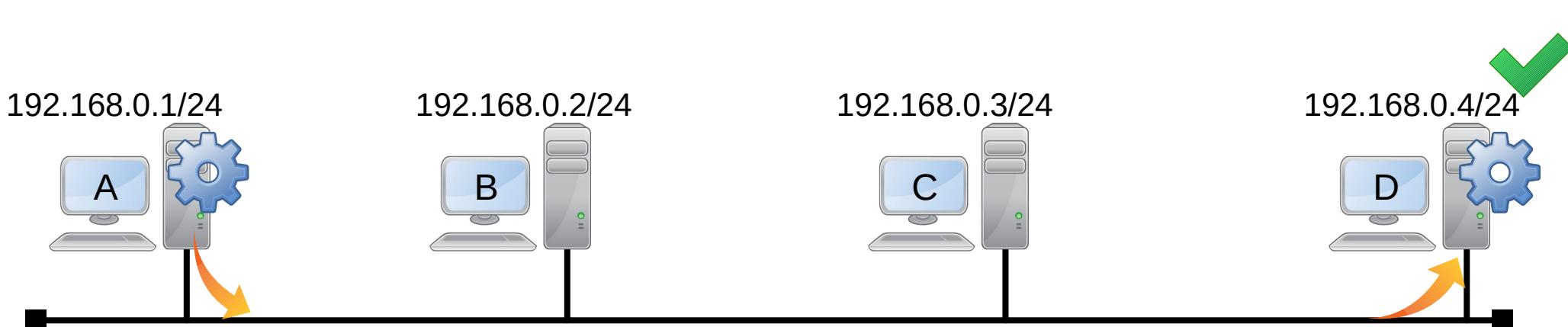


192.168.0.4/24



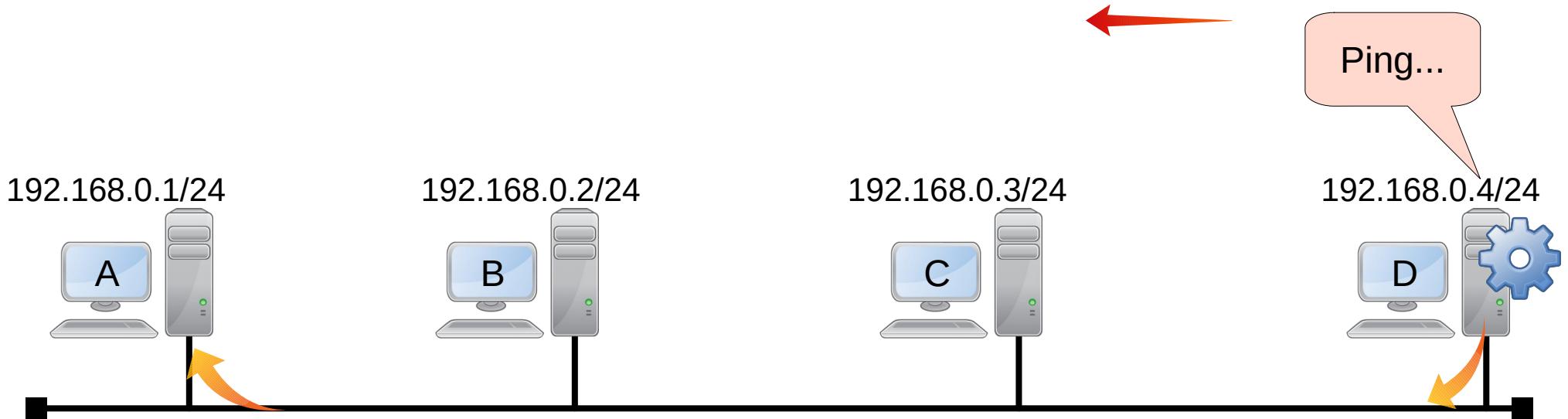
ICMP

| | | |
|--|----------|---------------------|
| Type (0) | Code (0) | Checksum (0xf92b) |
| Identifier (1) | | Sequence Number (1) |
| Data (oct 10, 2020 08:59:54.000000000 -03 – abcdefgh.....) | | |

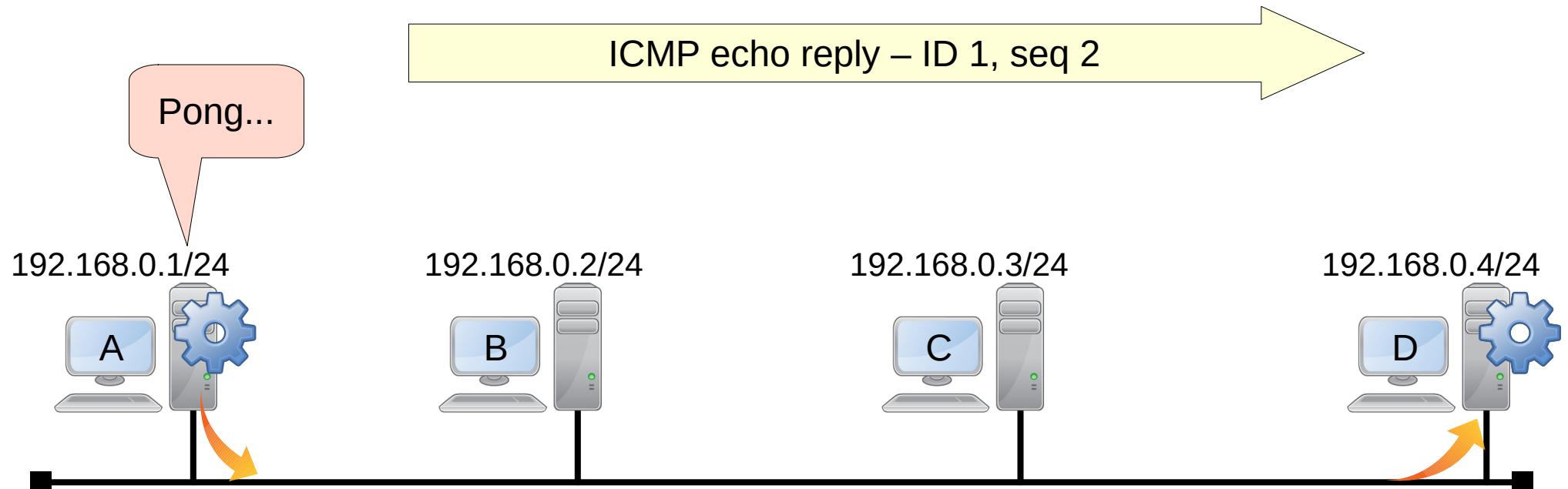


ICMP

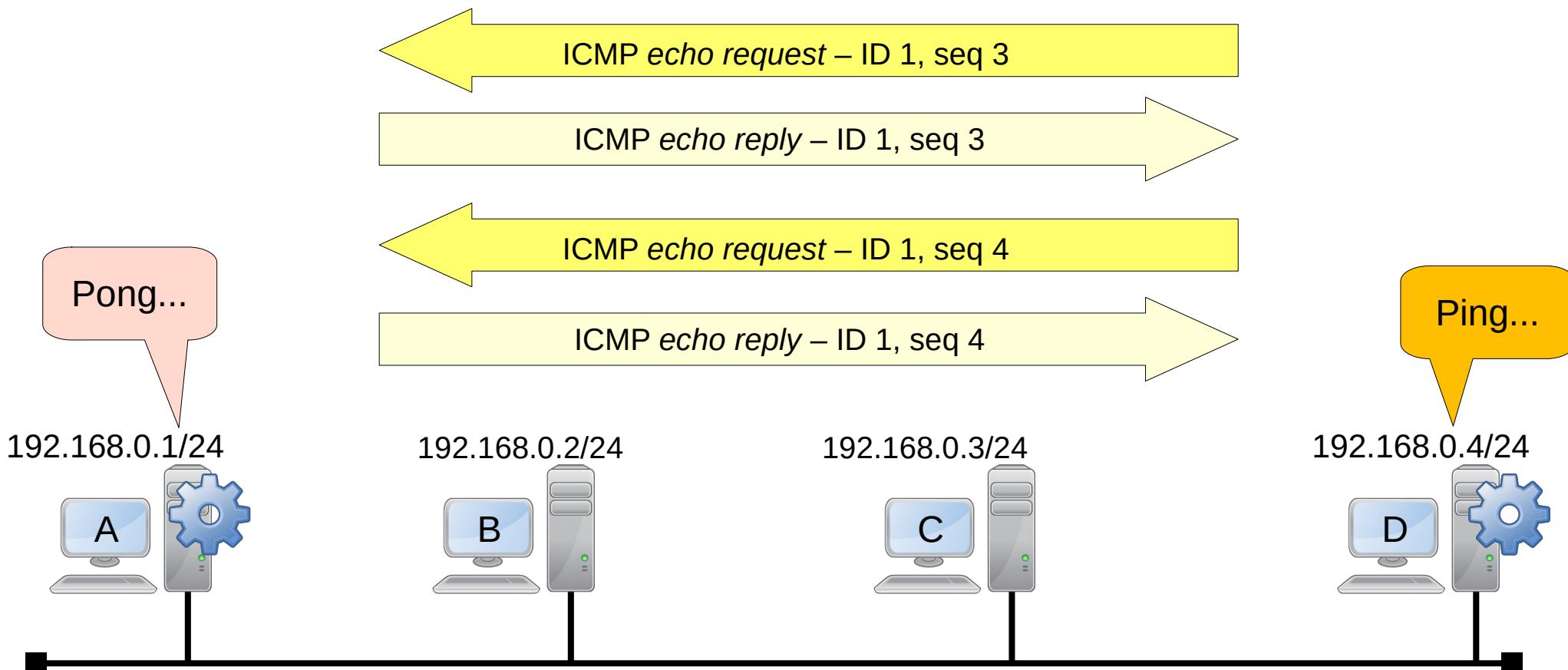
| | | |
|--|----------|---------------------|
| Type (8) | Code (0) | Checksum (0xf91a) |
| Identifier (1) | | Sequence Number (2) |
| Data (oct 10, 2020 08:59:55.000000000 -03 – abcdefgh.....) | | |



ICMP

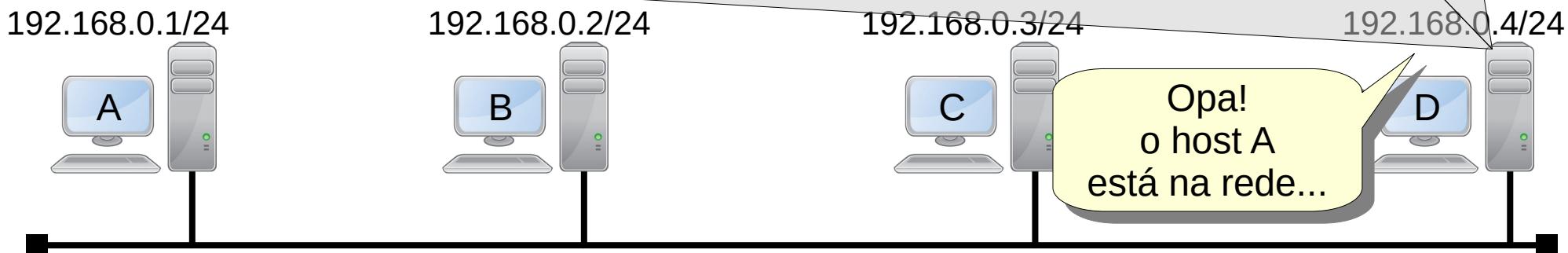


ICMP



ICMP – e

```
[luiz@fielVaio ~]$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes de dados.
64 bytes de 192.168.0.1: icmp_seq=1 ttl=64 tempo=5.32 ms
64 bytes de 192.168.0.1: icmp_seq=2 ttl=64 tempo=3.32 ms
64 bytes de 192.168.0.1: icmp_seq=3 ttl=64 tempo=8.57 ms
64 bytes de 192.168.0.1: icmp_seq=4 ttl=64 tempo=5.62 ms
64 bytes de 192.168.0.1: icmp_seq=5 ttl=64 tempo=8.52 ms
^C
--- 192.168.0.1 estatísticas de ping ---
5 pacotes transmitidos, 5 recebidos, 0% packet loss, time 4007ms
```



ICMP

Legal então sempre posso utilizar o ping (ICMP echo request/reply), para saber se um *host* está ou não na rede...



ICMP

Legal então sempre posso utilizar o ping (ICMP echo request/reply), para saber se um *host* está ou não na rede...



Sim, mas ele não
é 100% confiável...

ICMP



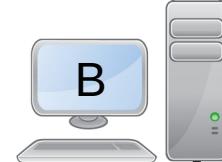
Alguns administradores desabilitam a resposta do ping para impedir que *hackers* mapeiem a rede ou executem algum tipo de ataque...



192.168.0.1/24



192.168.0.2/24



192.168.0.3/24

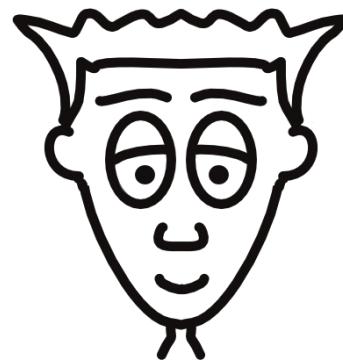


192.168.0.4/24



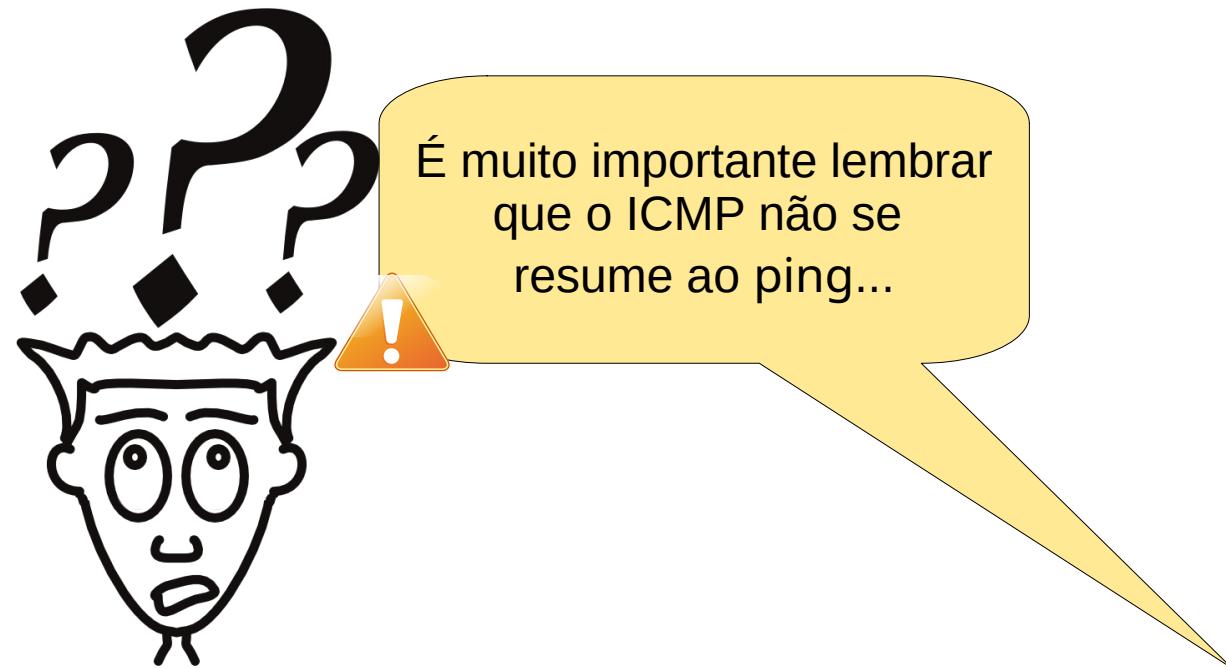
ICMP

Entendi, então caso o ping não responda, não significa que o *host* não está na rede!



ICMP

Entendi, então caso o ping não responda, não significa que o *host* não está na rede!



ICMP

| Campo de tipo | Tipo de mensagem ICMP |
|---------------|---|
| 0 | Resposta de eco (echo) |
| 3 | Destino inalcançável (host unreachable) |
| 4 | Source quench |
| 5 | Redirecionamento (mudar uma rota) |
| 6 | Endereço de host alternativo |
| 8 | Requisição de echo (echo) |
| 9 | Anúncio de roteador |
| 10 | Solicitação de roteador |
| 11 | Tempo excedido para um datagrama |
| 12 | Problemas de parâmetro em um datagrama |
| 13 | Requisição de estampa de tempo |
| 14 | Resposta de estampa de tempo |
| 15 | Requisição de informações |
| 16 | Resposta de informações |
| 17 | Requisição de máscara de endereço |
| 18 | Resposta de máscara de endereço |
| 30 | Tracecoute |
| 31 | Erro de conversão de datagrama |
| 32 | Redirecionar host móvel |
| 33 | “Onde está você” do Ipv6 |
| 34 | “Eu estou aqui” do Ipv6 |
| 35 | Requisição de registro móvel |
| 36 | Resposta de registro móvel |
| 37 | Requisição de nome de domínio |
| 38 | Resposta de nome de domínio |
| 39 | SKIP |

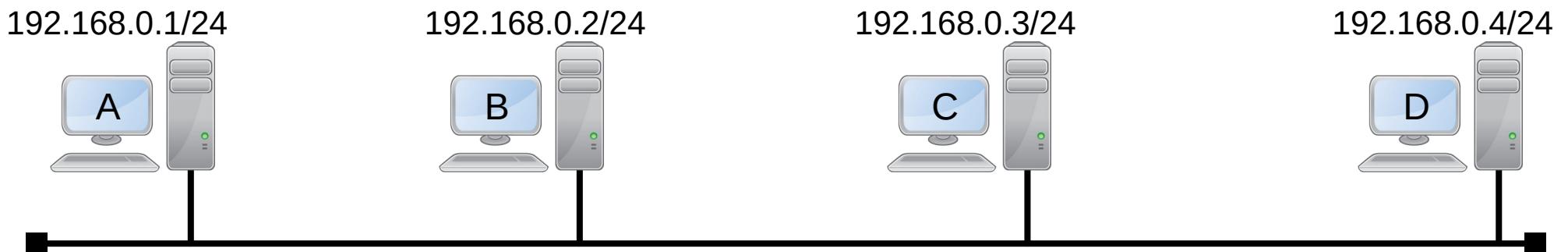
ICMP

| Campo de tipo | Tipo de mensagem ICMP |
|---------------|---|
| 0 | Resposta de eco (echo) |
| 3 | Destino inalcançável (host unreachable) |
| 4 | Source quench |
| 5 | Redirecionamento (mudar uma rota) |
| 6 | Endereço de host alternativo |
| 8 | Requisição de echo (echo) |
| 9 | Anúncio de roteador |
| 10 | Solicitação de roteador |
| 11 | Tempo excedido para um datagrama |
| 12 | Problemas de parâmetro em um datagrama |
| 13 | Requisição de estampa de tempo |
| 14 | Resposta de estampa de tempo |
| 15 | Requisição de informações |
| 16 | Resposta de informações |
| 17 | Requisição de máscara de endereço |
| 18 | Resposta de máscara de endereço |
| 30 | Traceoute |
| 31 | Erro de conversão de datagrama |
| 32 | Redirecionar host móvel |
| 33 | “Onde está você” do Ipv6 |
| 34 | “Eu estou aqui” do Ipv6 |
| 35 | Requisição de registro móvel |
| 36 | Resposta de registro móvel |
| 37 | Requisição de nome de domínio |
| 38 | Resposta de nome de domínio |
| 39 | SKIP |

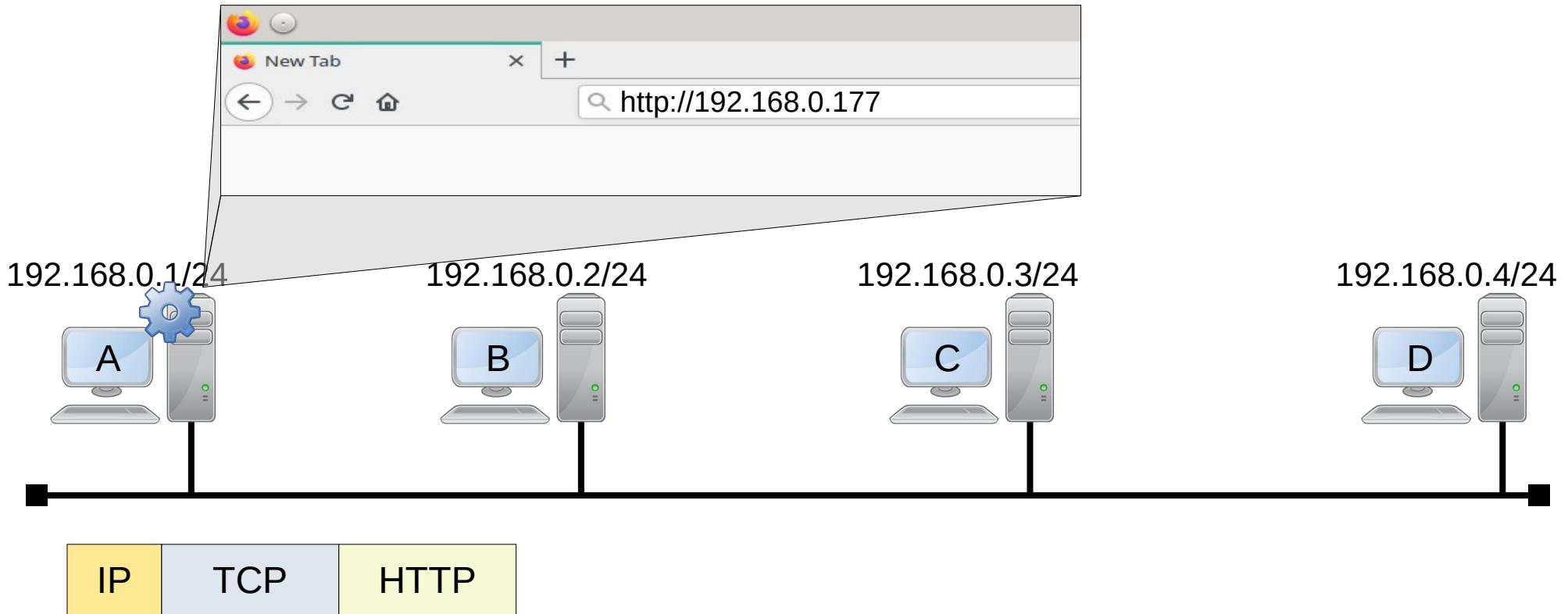
Vamos ver alguns tipos de mensagens ICMP...

ICMP

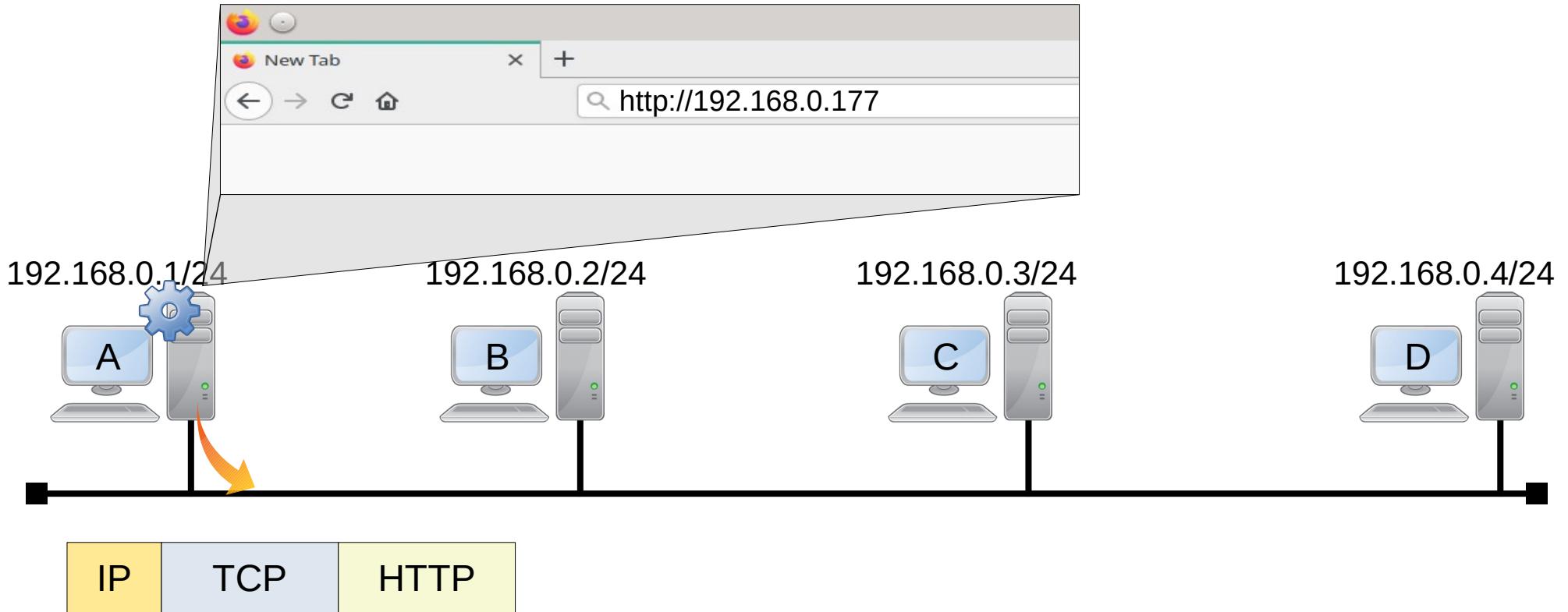
ICMP – Destino inalcançável (*host/rede/porta*)



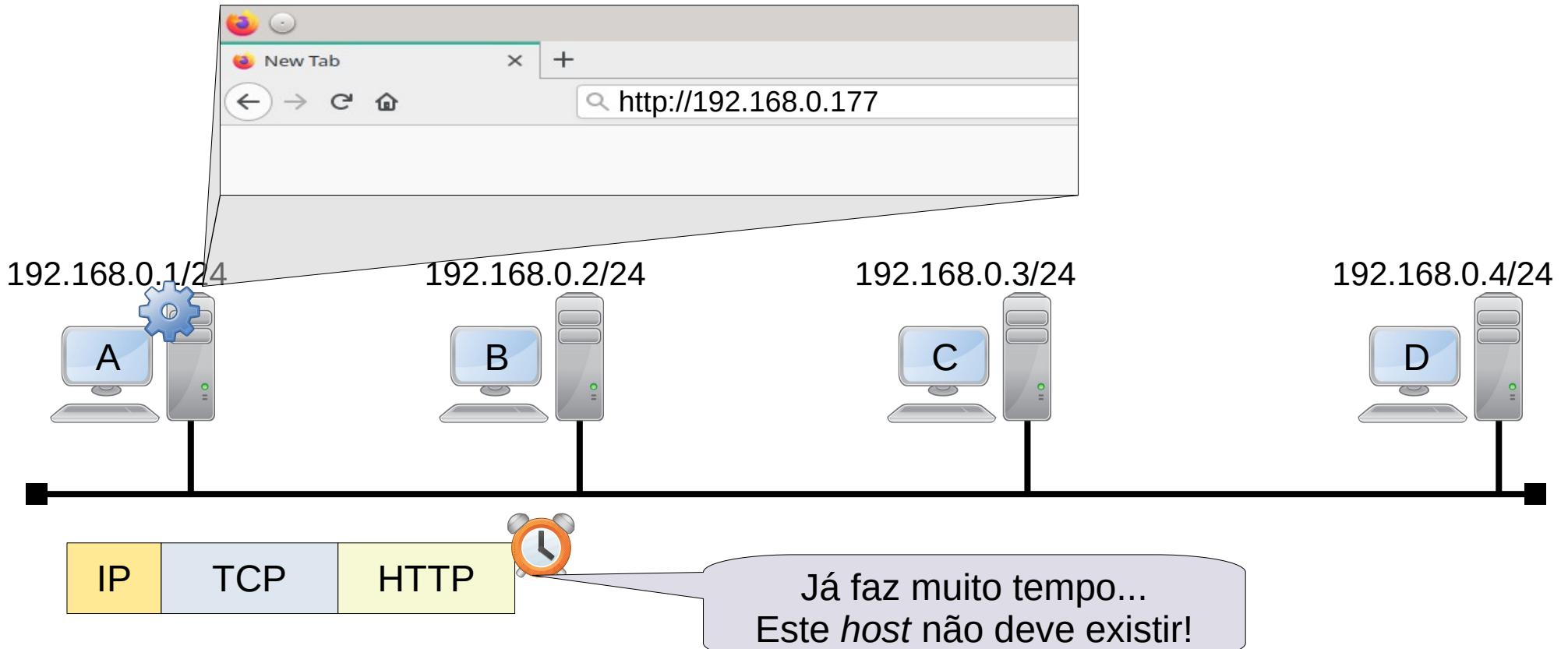
ICMP



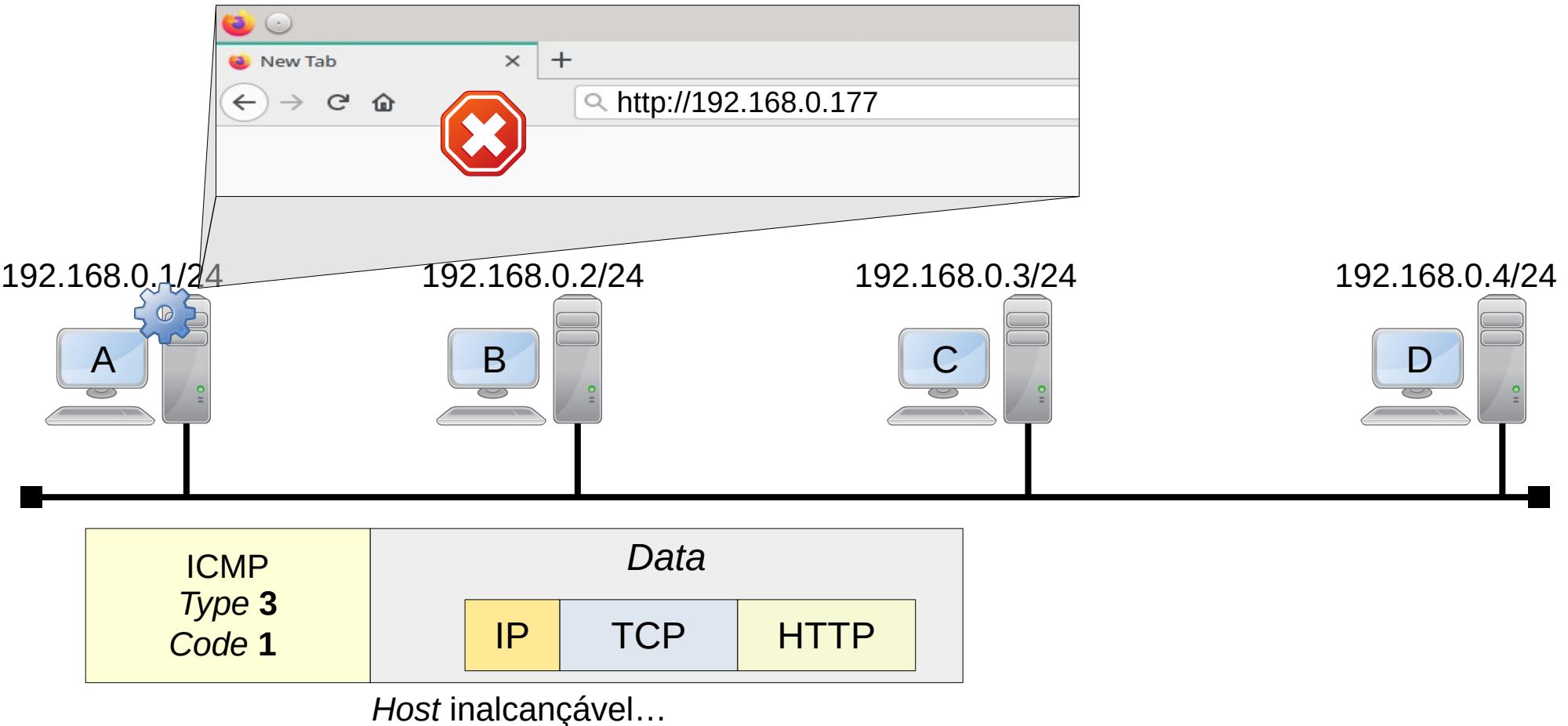
ICMP



ICMP

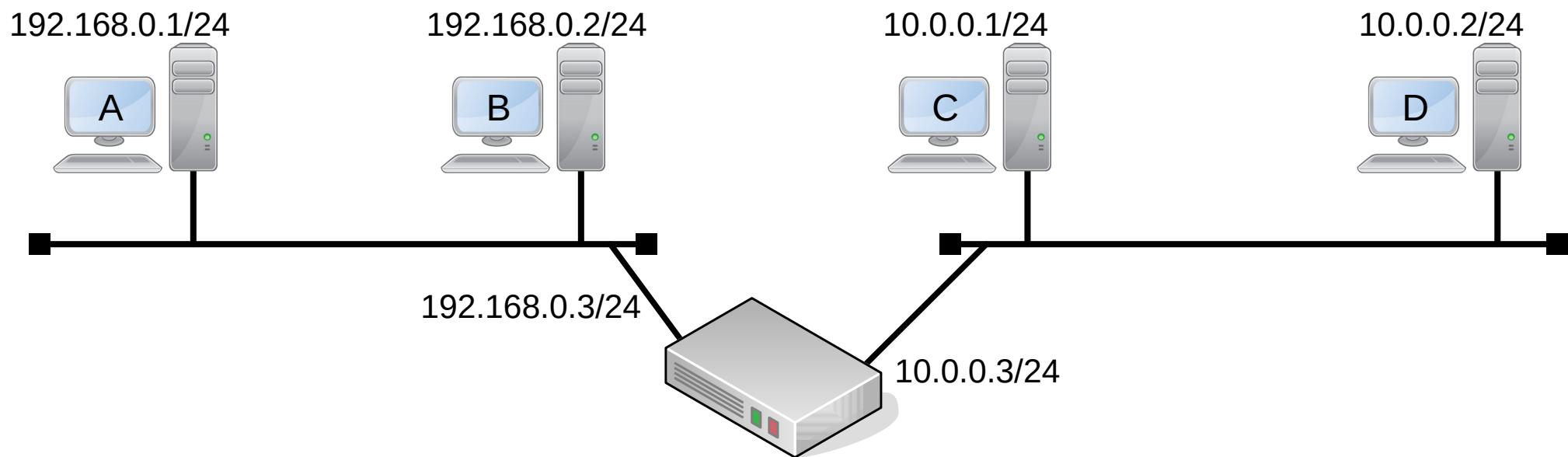


ICMP



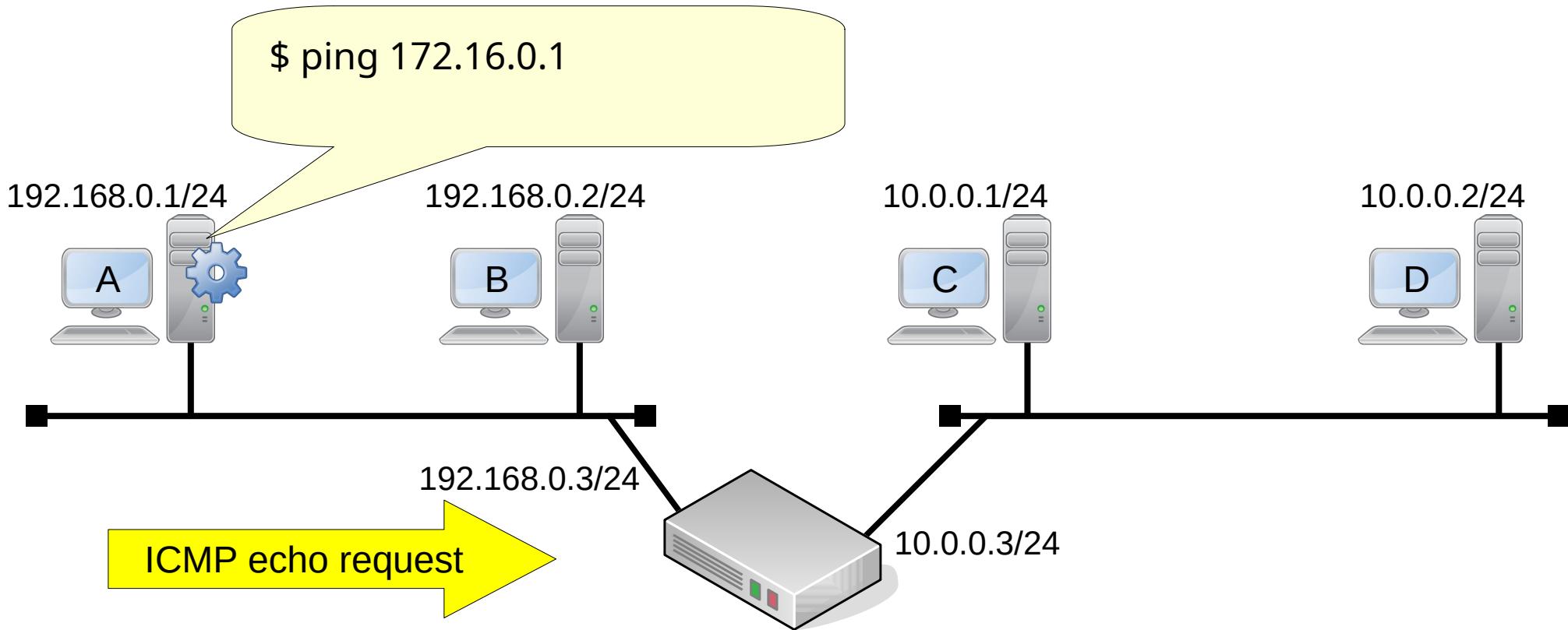
ICMP

ICMP – Destino inalcançável (*host/rede/porta*)



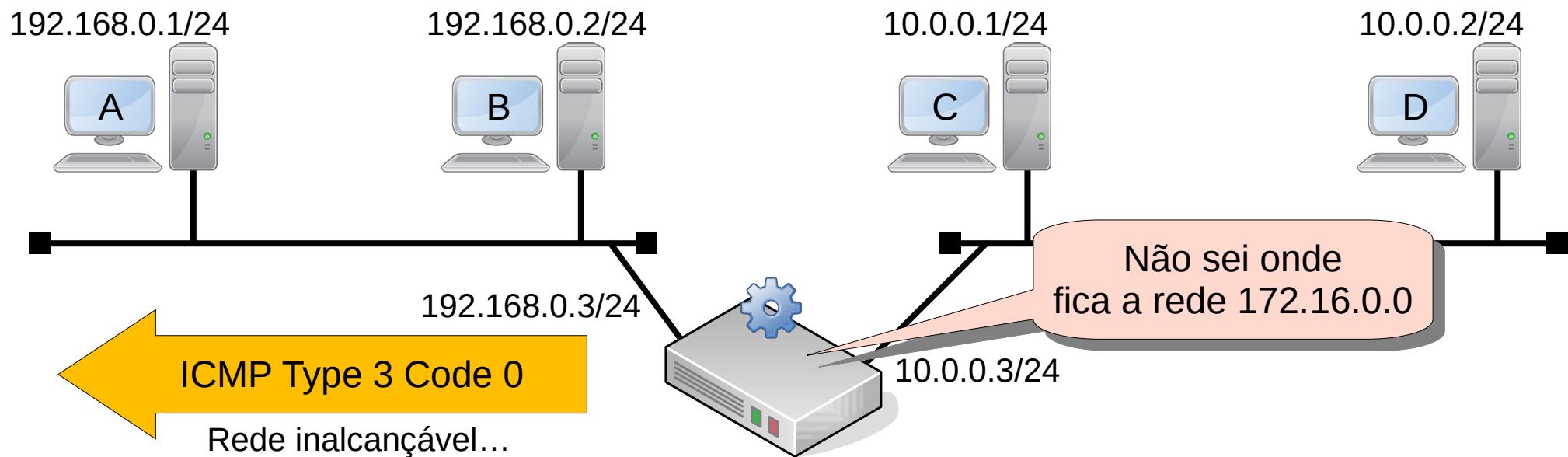
ICMP

ICMP – Destino inalcançável (host/rede/porta)



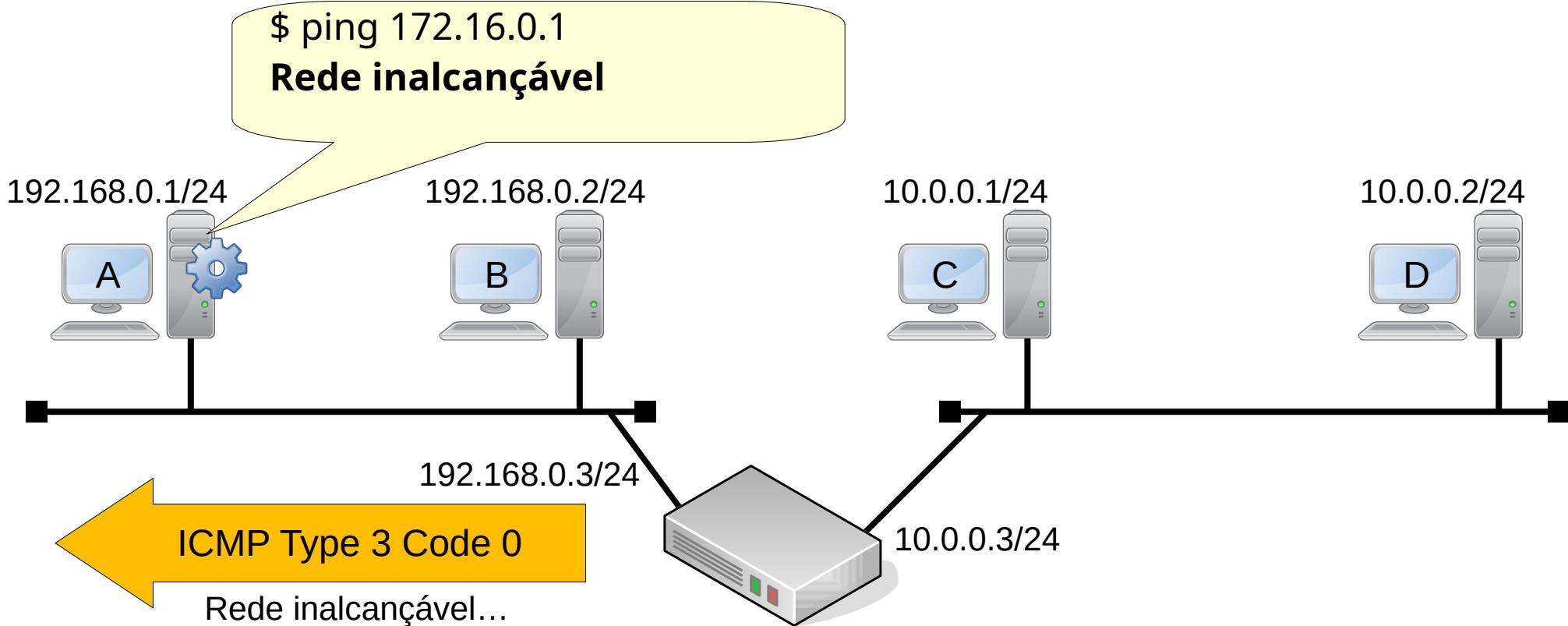
ICMP

ICMP – Destino inalcançável (*host/rede/porta*)



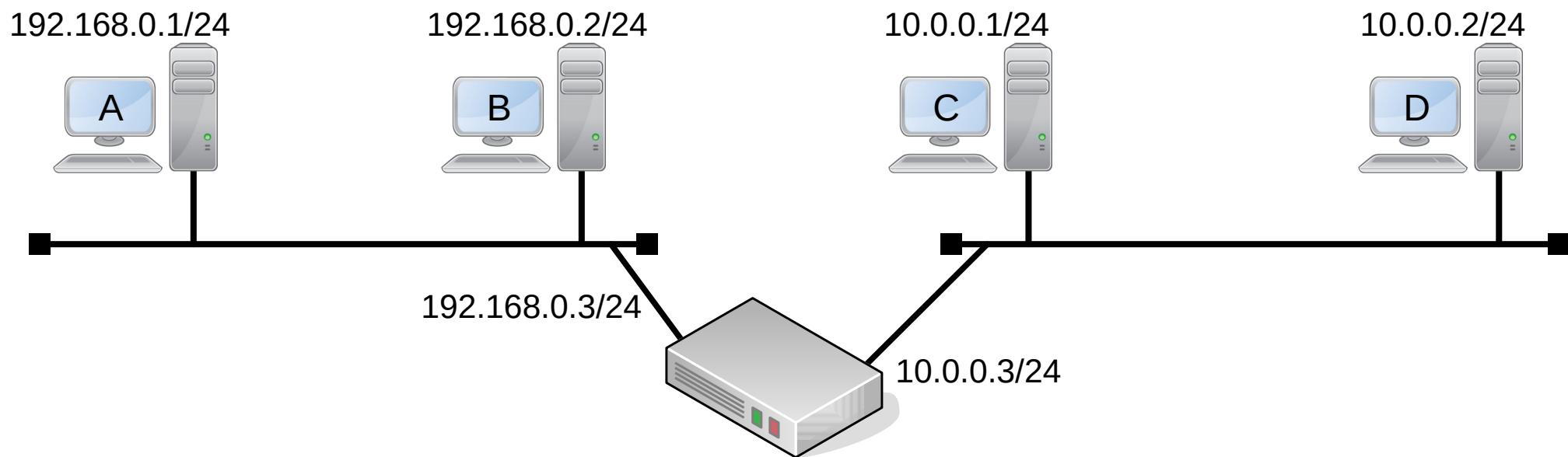
ICMP

ICMP – Destino inalcançável (*host/rede/porta*)

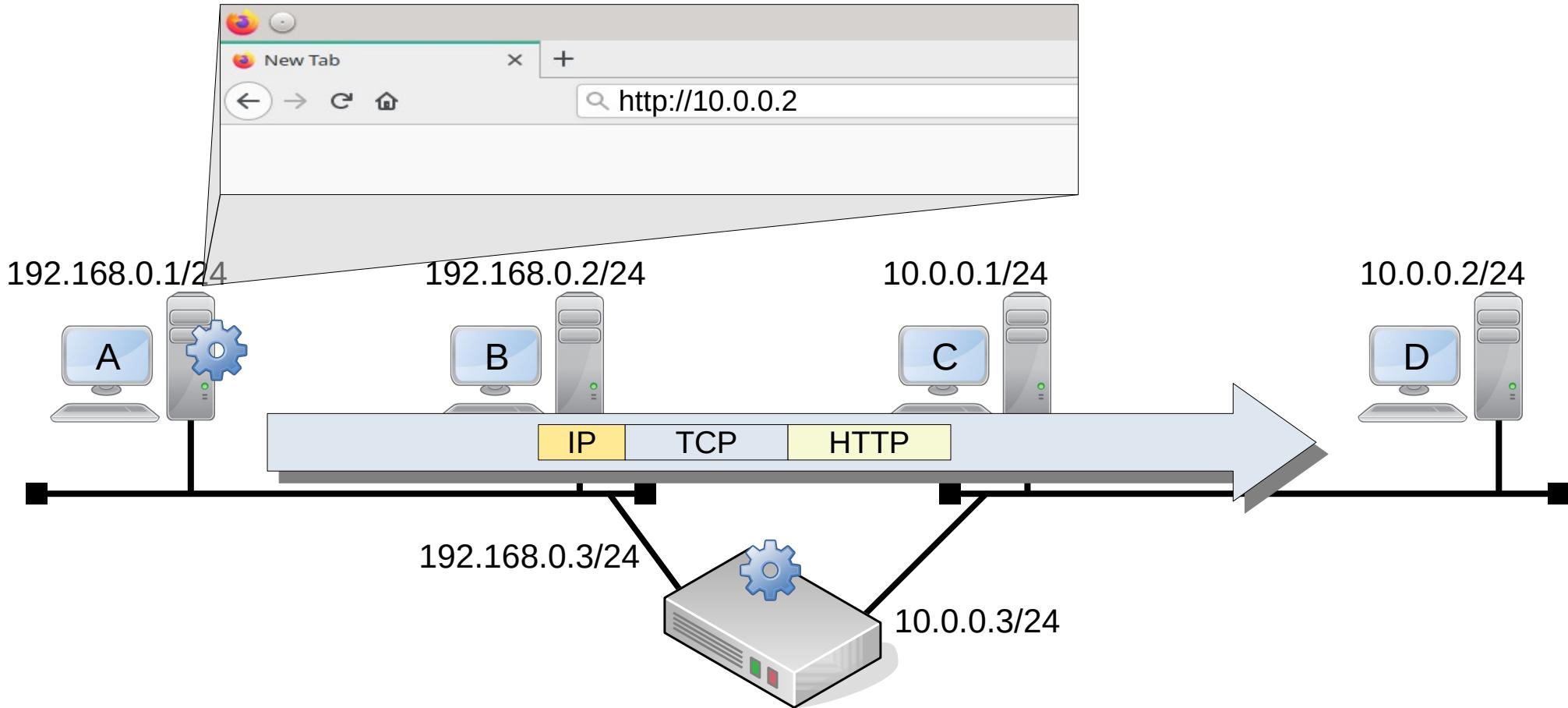


ICMP

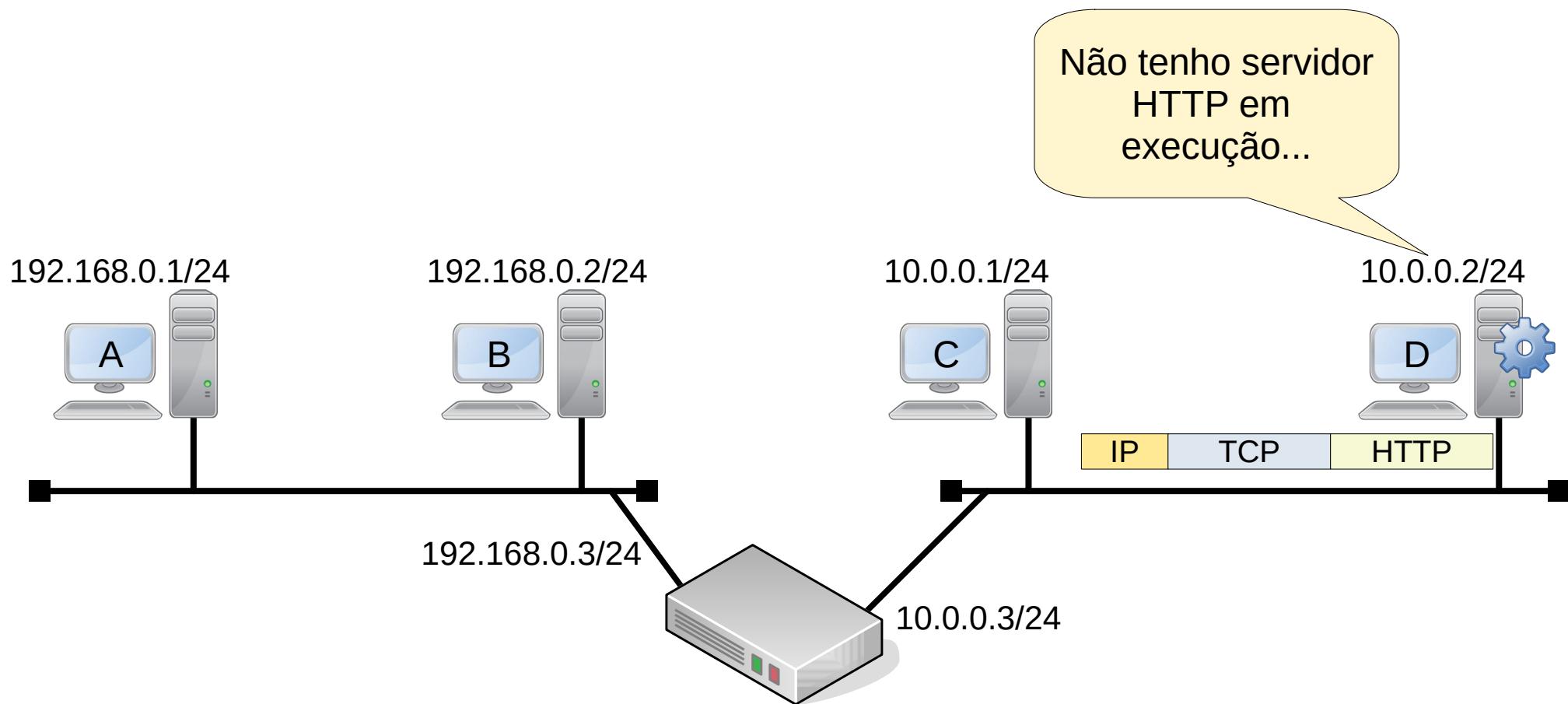
ICMP – Destino inalcançável (*host/rede/porta*)



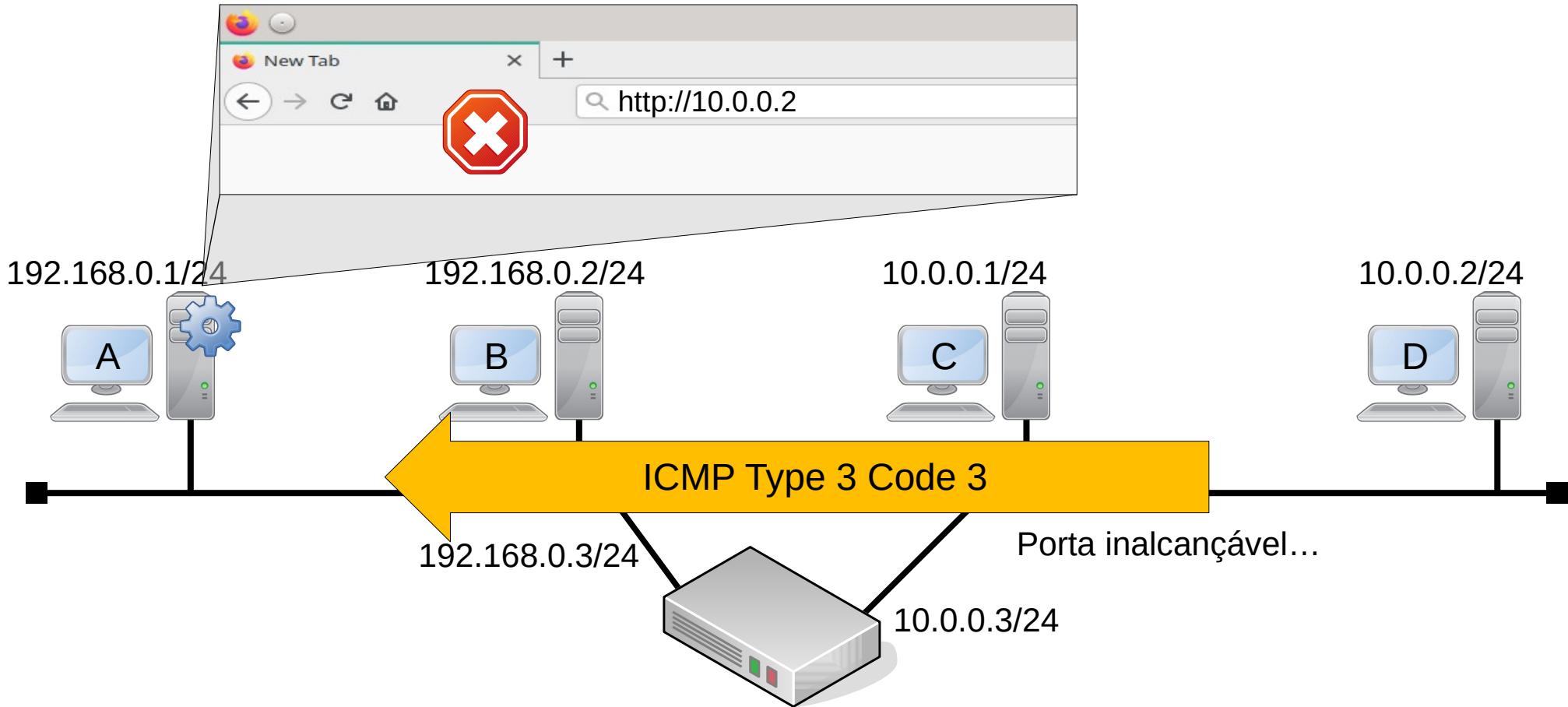
ICMP



ICMP



ICMP



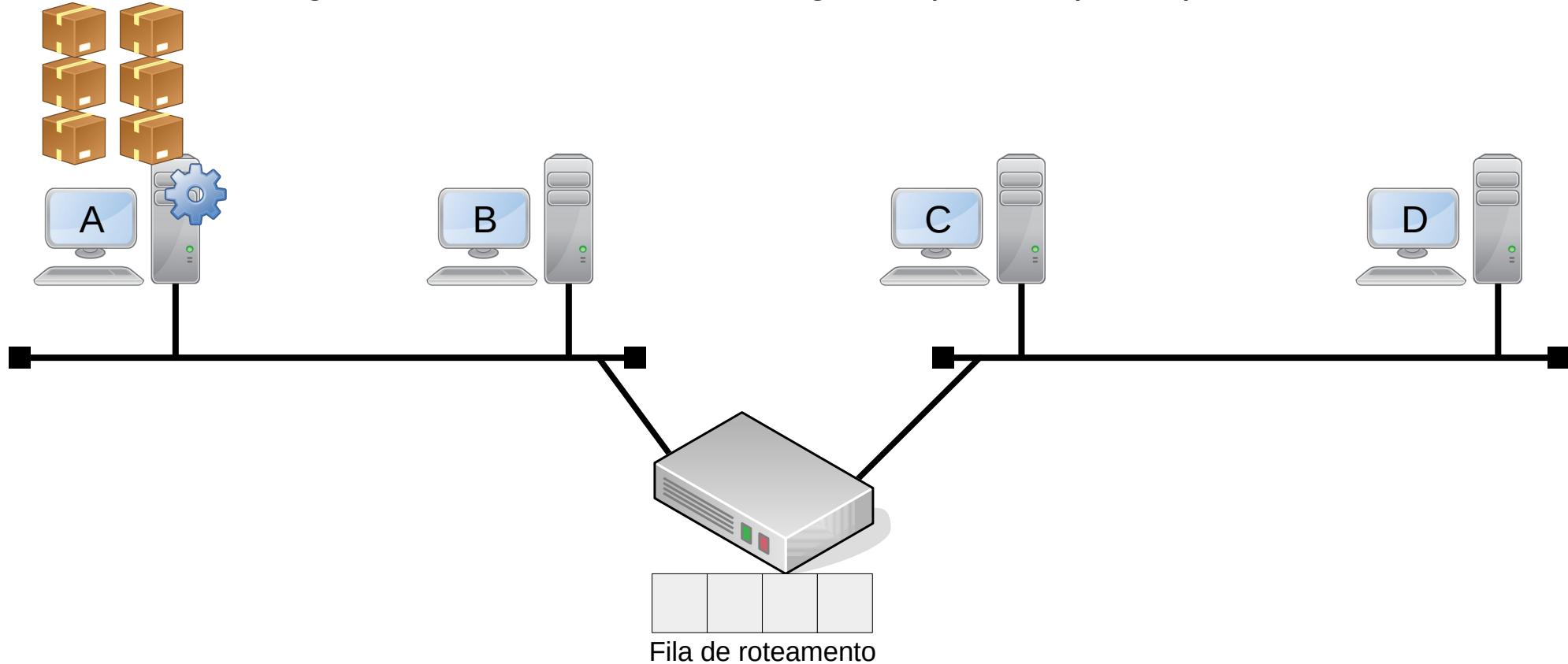
ICMP

Valor do código Significado

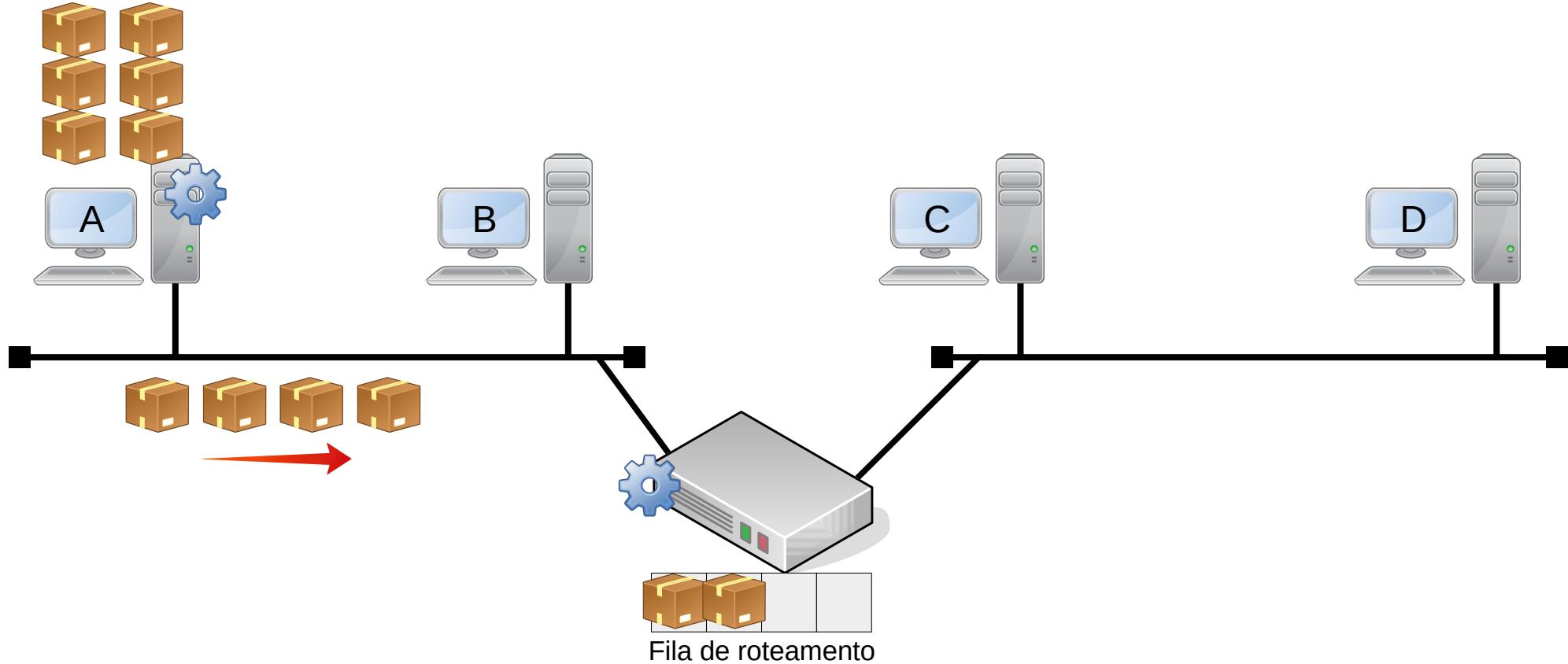
| | |
|----|--|
| 0 | Rede inalcançável |
| 1 | Host inalcançável |
| 2 | Protocolo inalcançável |
| 3 | Porta inalcançável |
| 4 | Fragmentação necessária e DF marcado |
| 5 | Rota de origem falhou |
| 6 | Rota de destino desconhecida |
| 7 | Host de destino desconhecido |
| 8 | Host de origem isolado |
| 9 | Comunicação com rede de destino proibida |
| 10 | Comunicação com host de destino proibida |
| 11 | Rede inalcançável para o tipo de serviço |
| 12 | Host inalcançável par o tipo de serviço |
| 13 | Comunicação proibida administrativamente |
| 14 | Violação de precedência de host |
| 15 | Corte de precedência em vigor |

ICMP

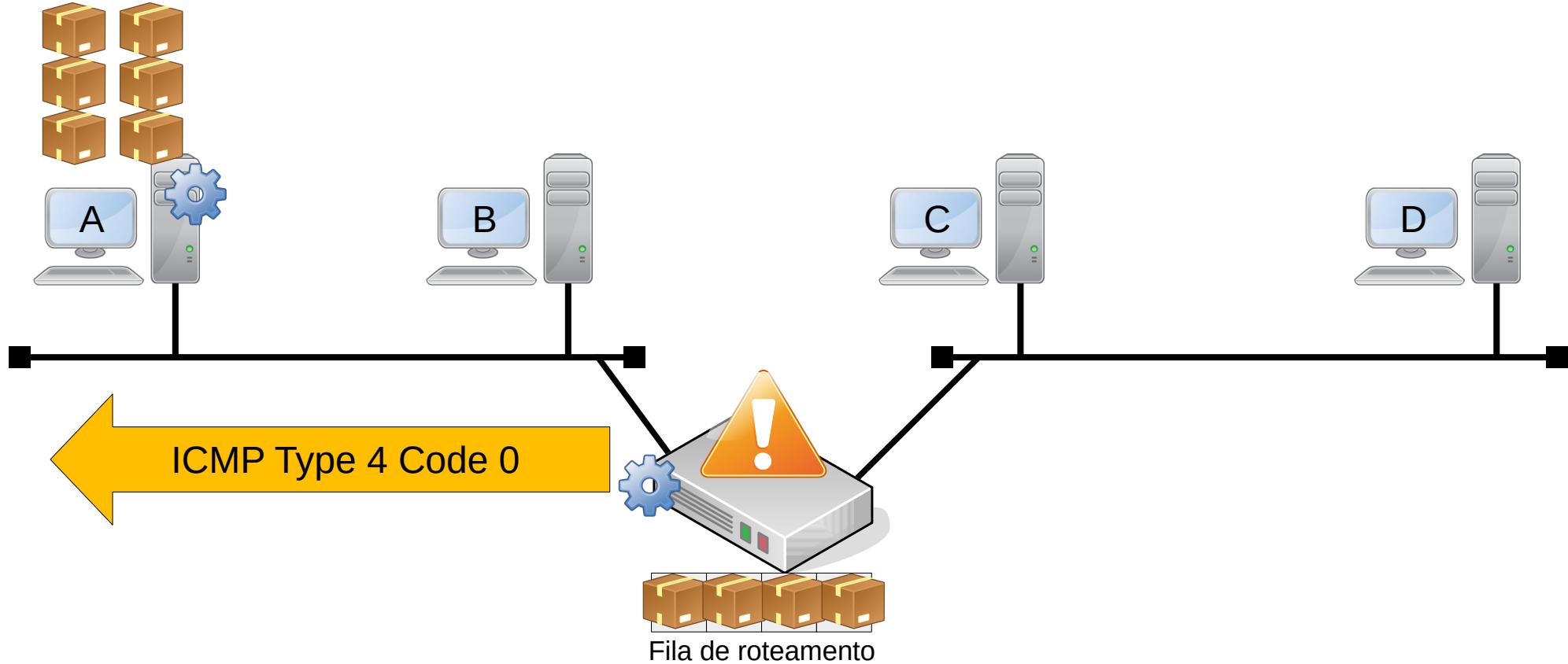
Controle de congestionamento e fluxo de datagrama (*source quench*)



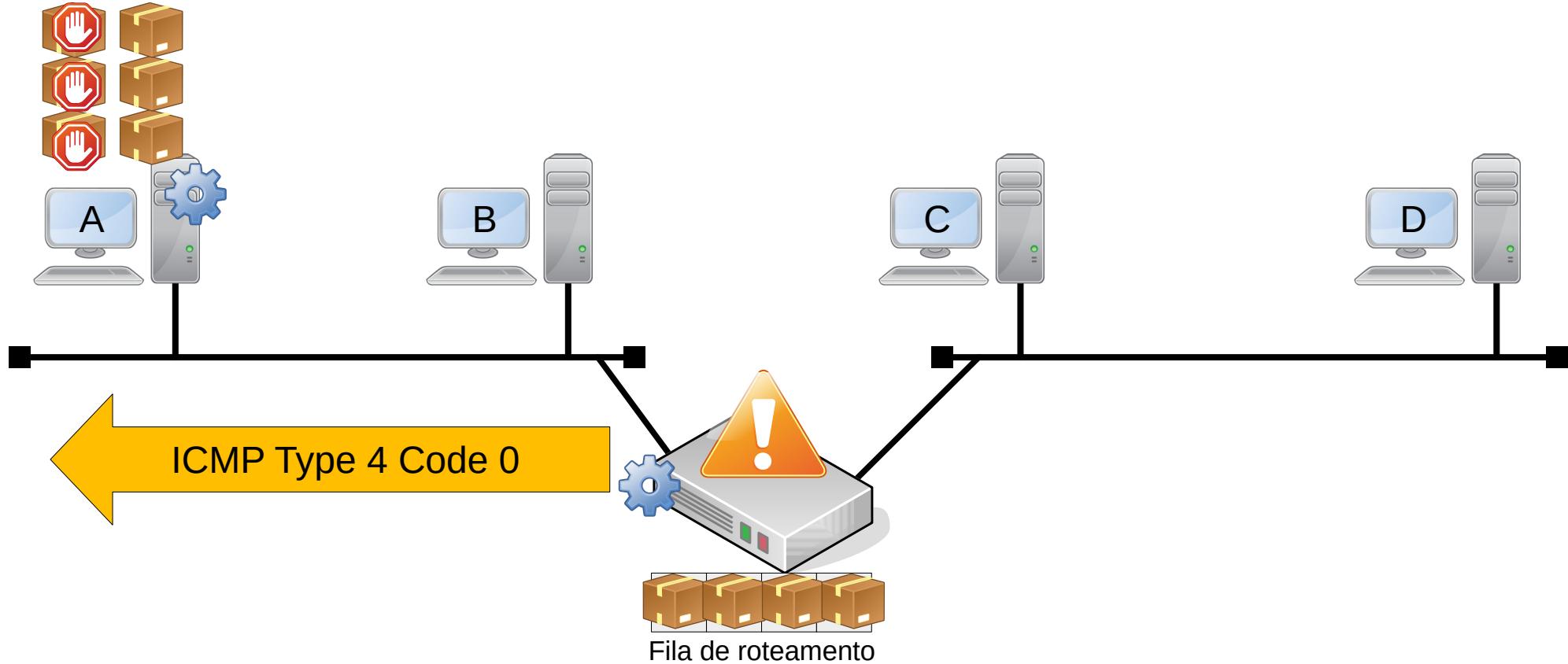
ICMP



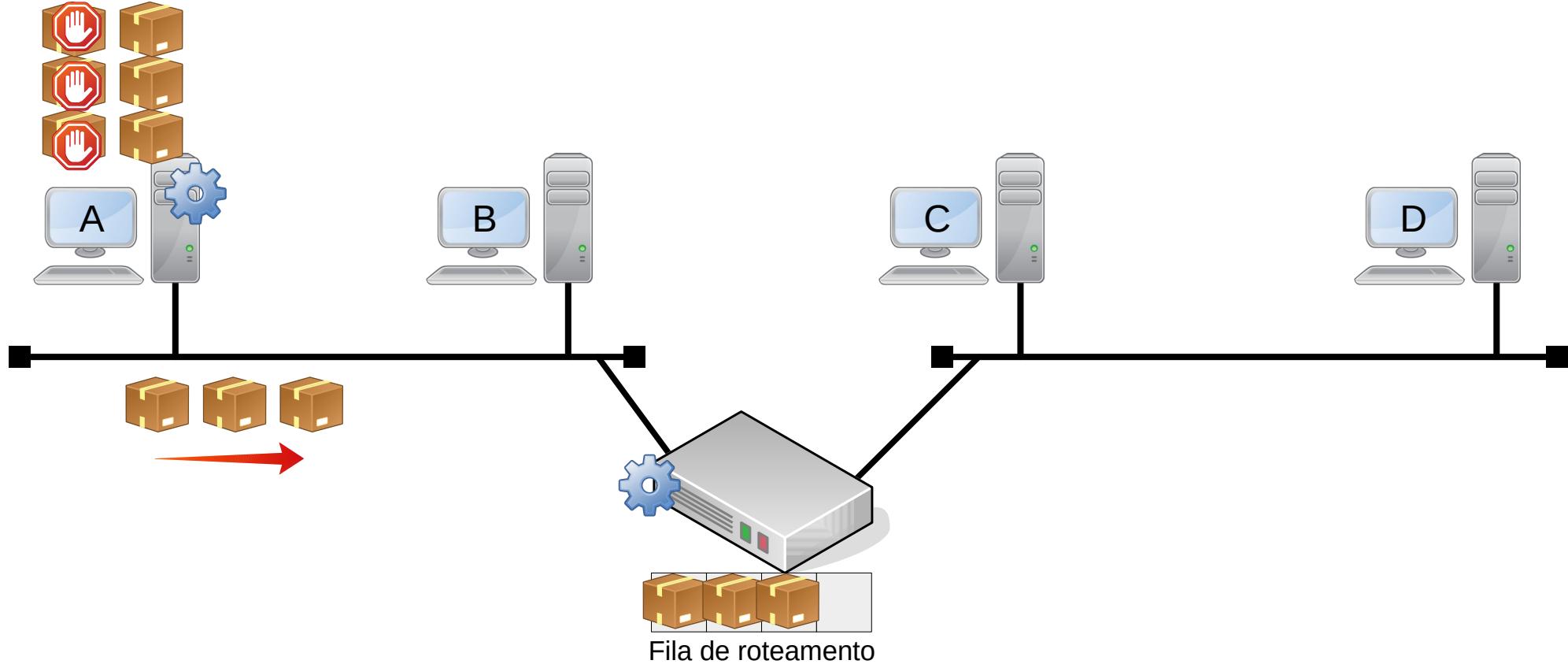
ICMP



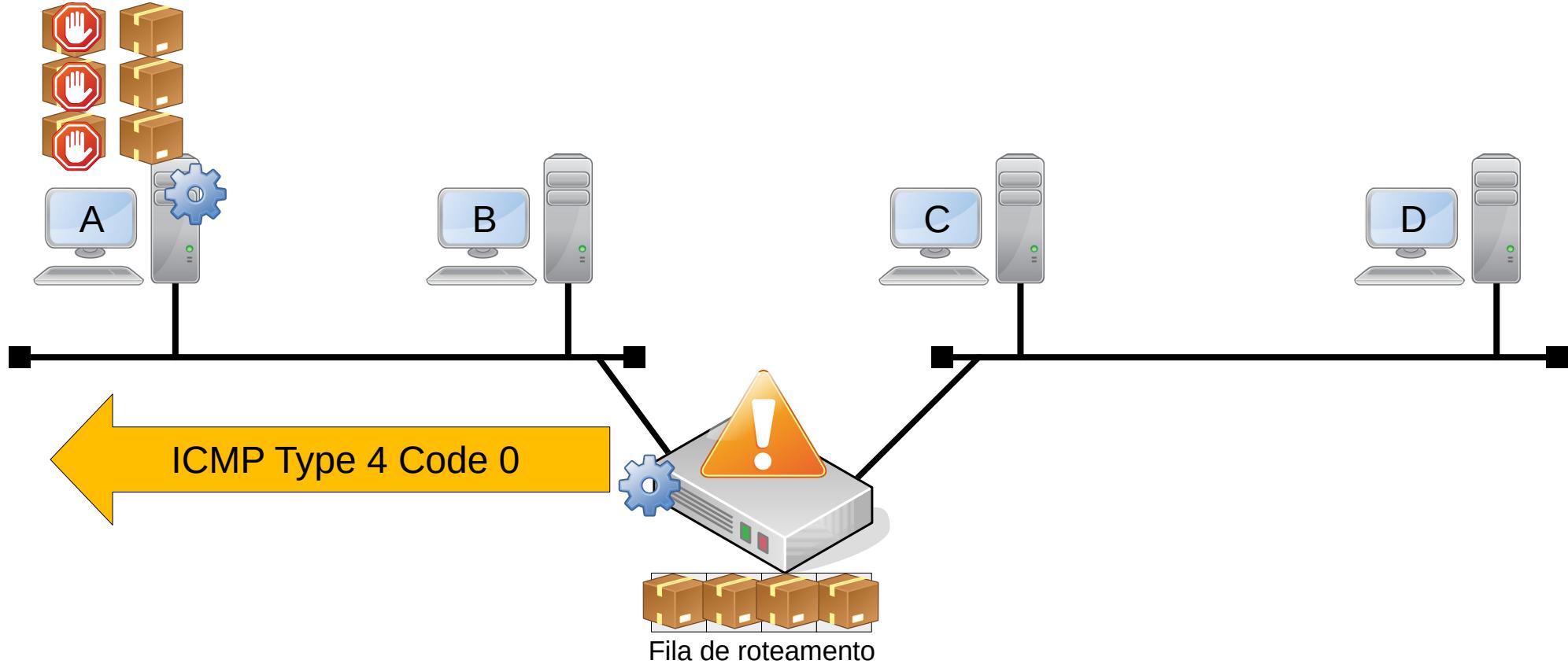
ICMP



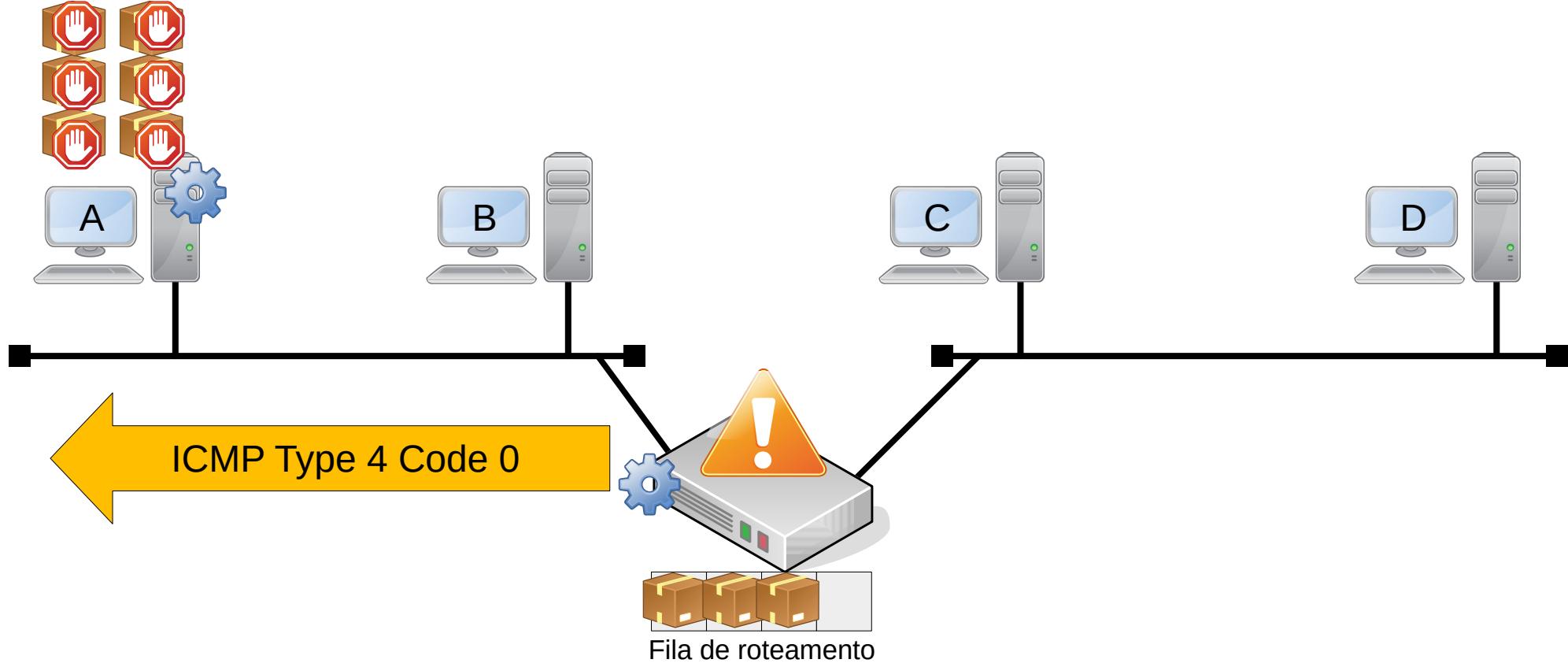
ICMP



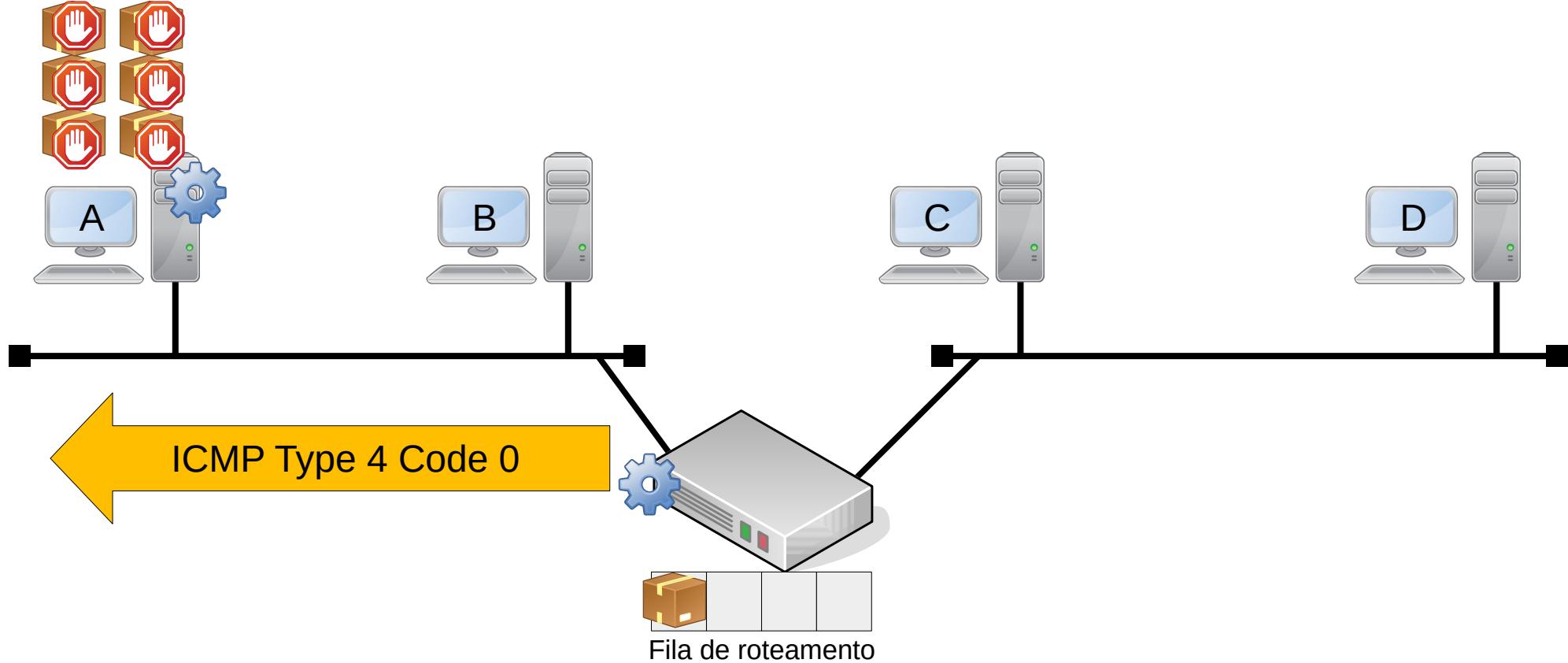
ICMP



ICMP



ICMP



ICMP

Quando é que o roteador envia um ICMP *source quench* para voltar a transmitir?



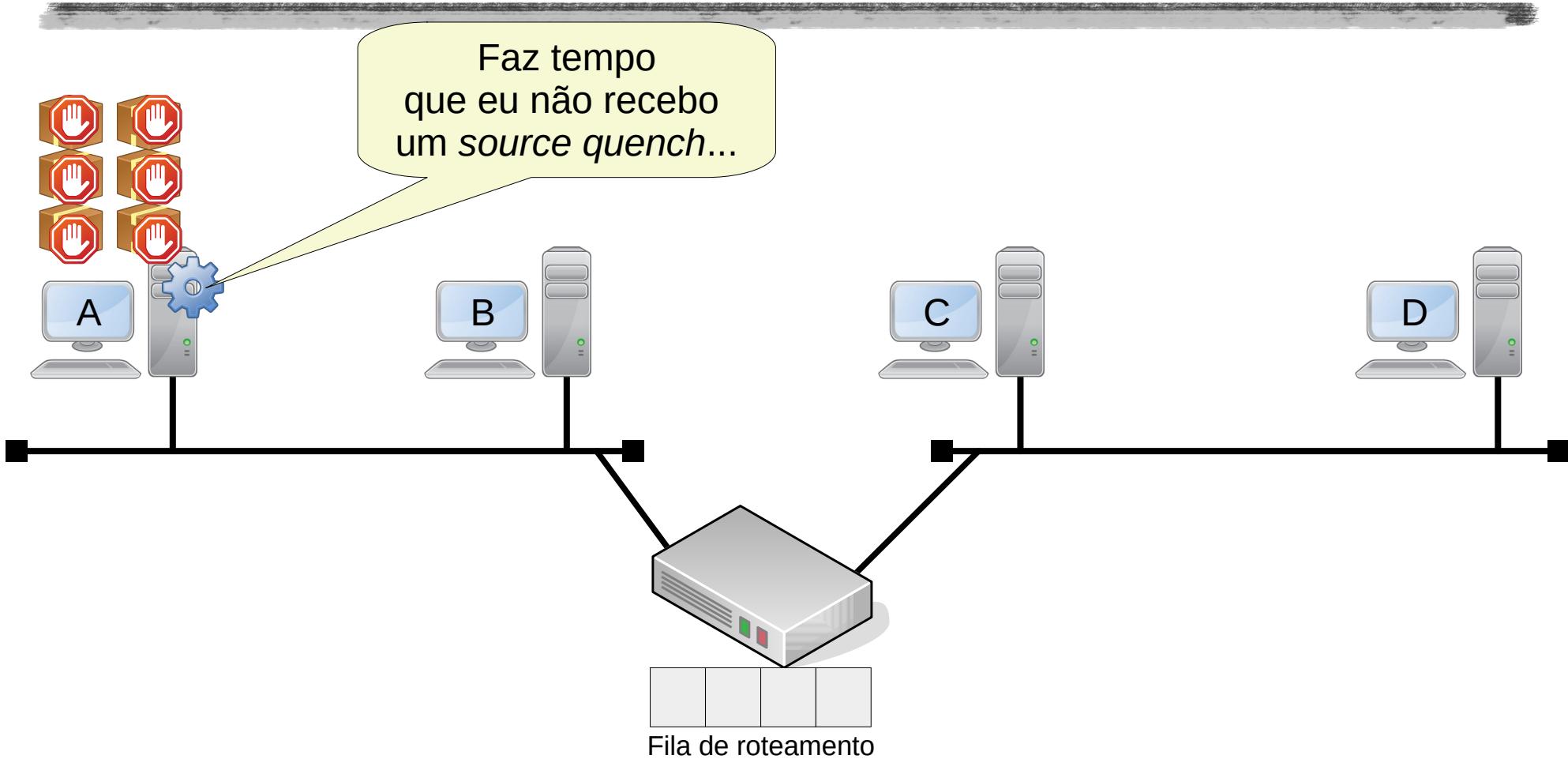
ICMP

Quando é que o roteador envia um ICMP *source quench* para voltar a transmitir?

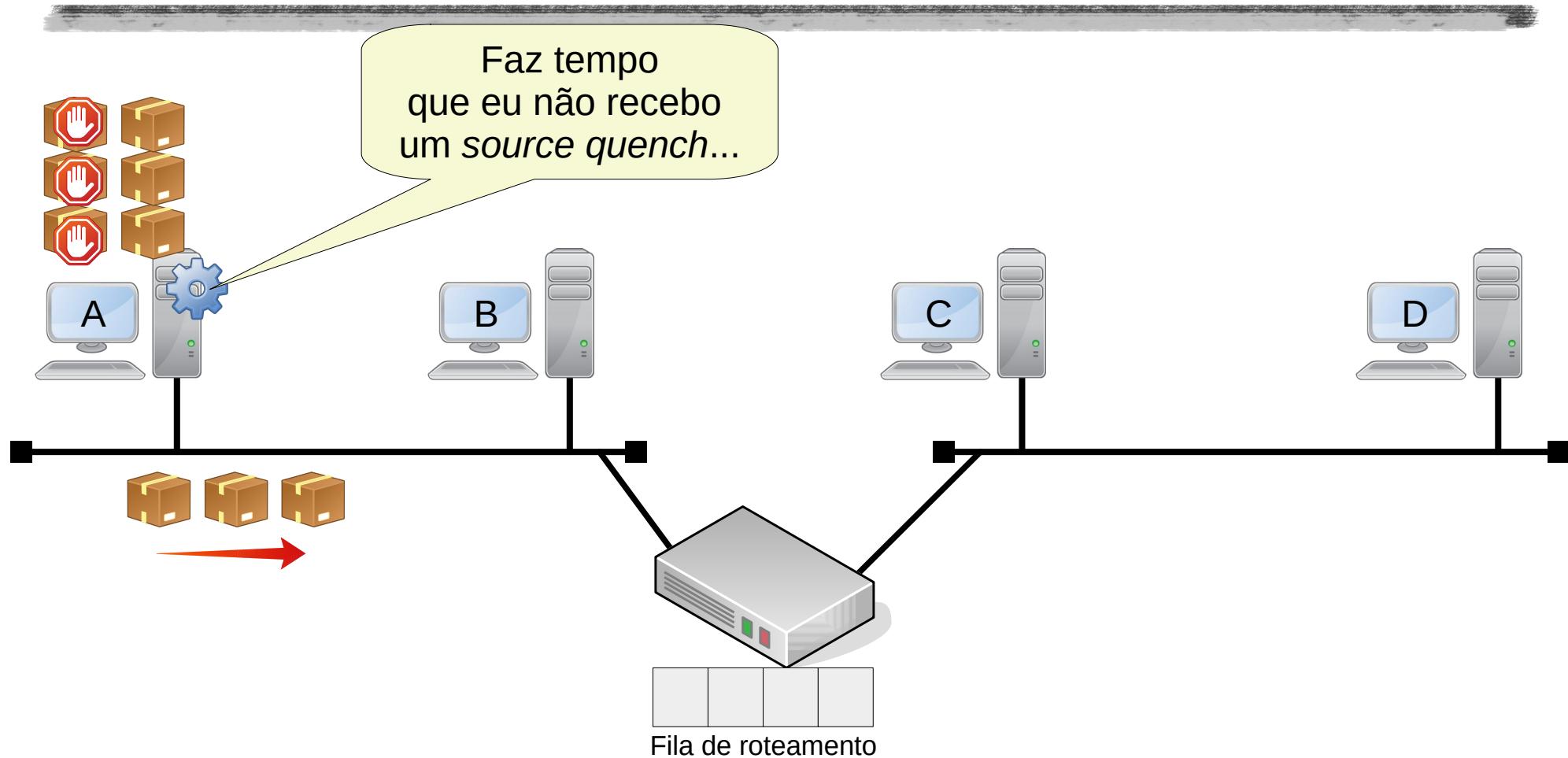


Não existe este tipo
de mensagem...

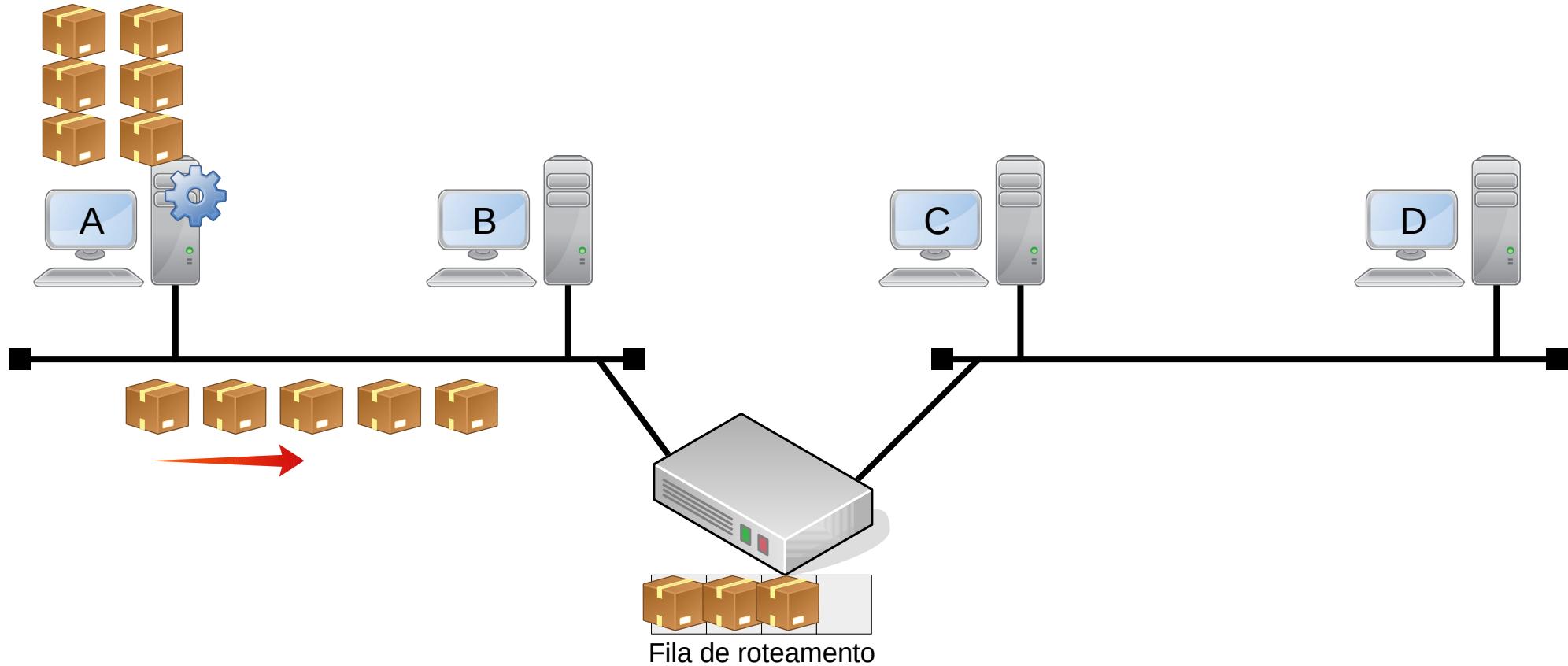
ICMP



ICMP



ICMP



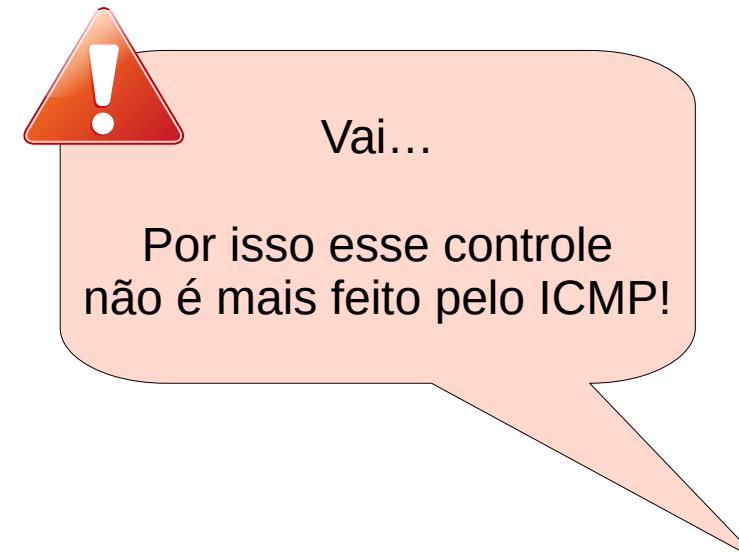
ICMP

Mais vai sobrecarregar o roteador novamente...



ICMP

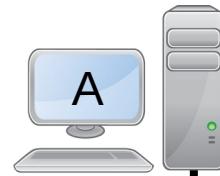
Mais vai sobrecarregar o roteador novamente...



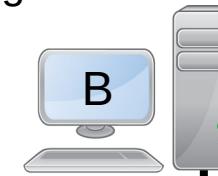
ICMP

Mudança de rota por roteadores

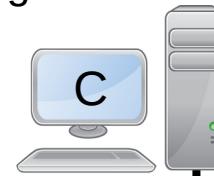
192.168.0.1/24
gw 192.168.0.3



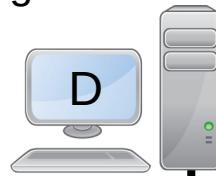
192.168.0.2/24
gw 192.168.0.1



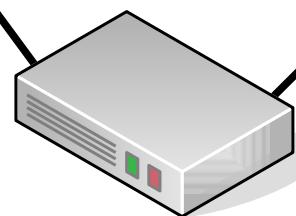
10.0.0.1/24
gw 10.0.0.3



10.0.0.2/24
gw 10.0.0.3

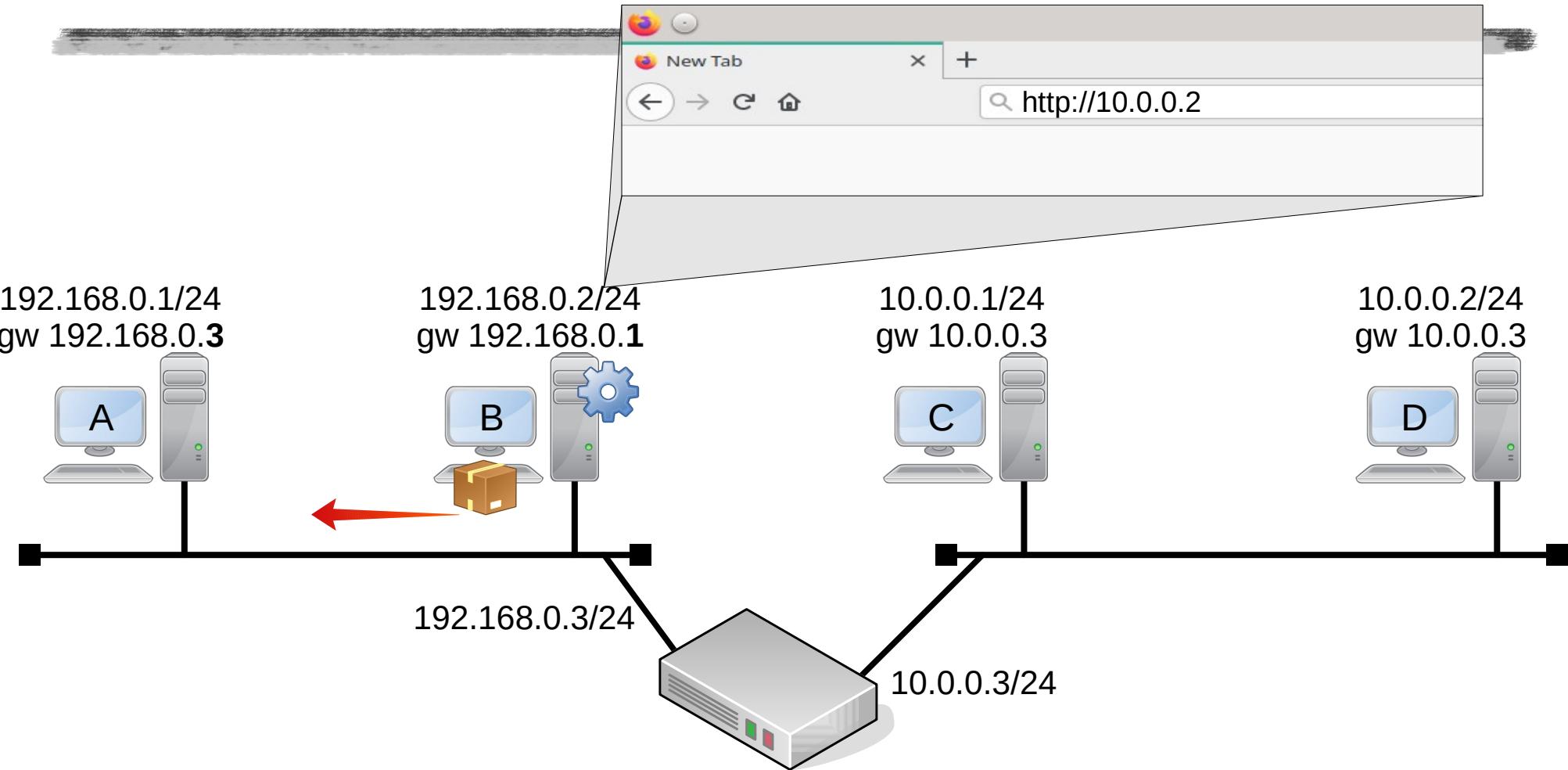


192.168.0.3/24

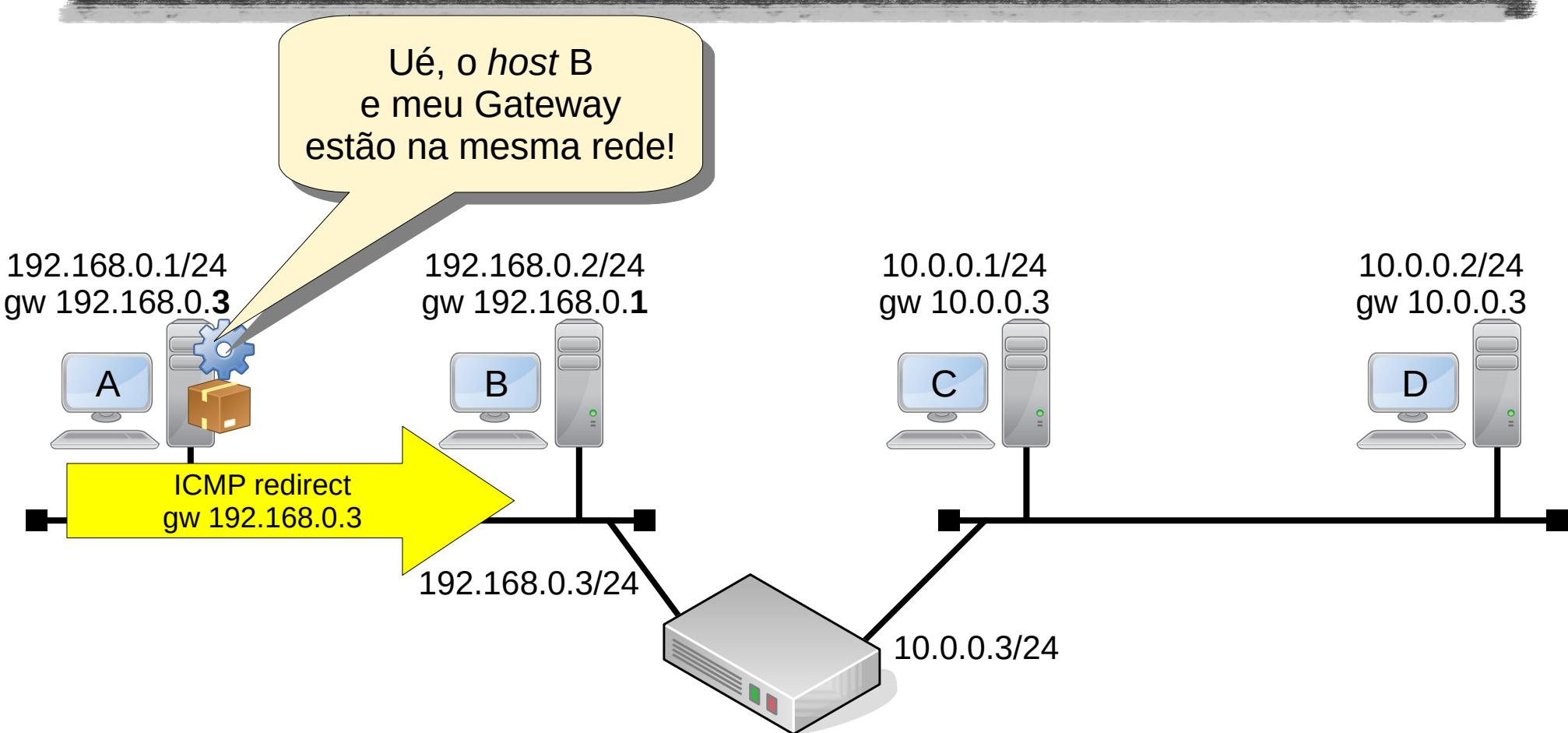


10.0.0.3/24

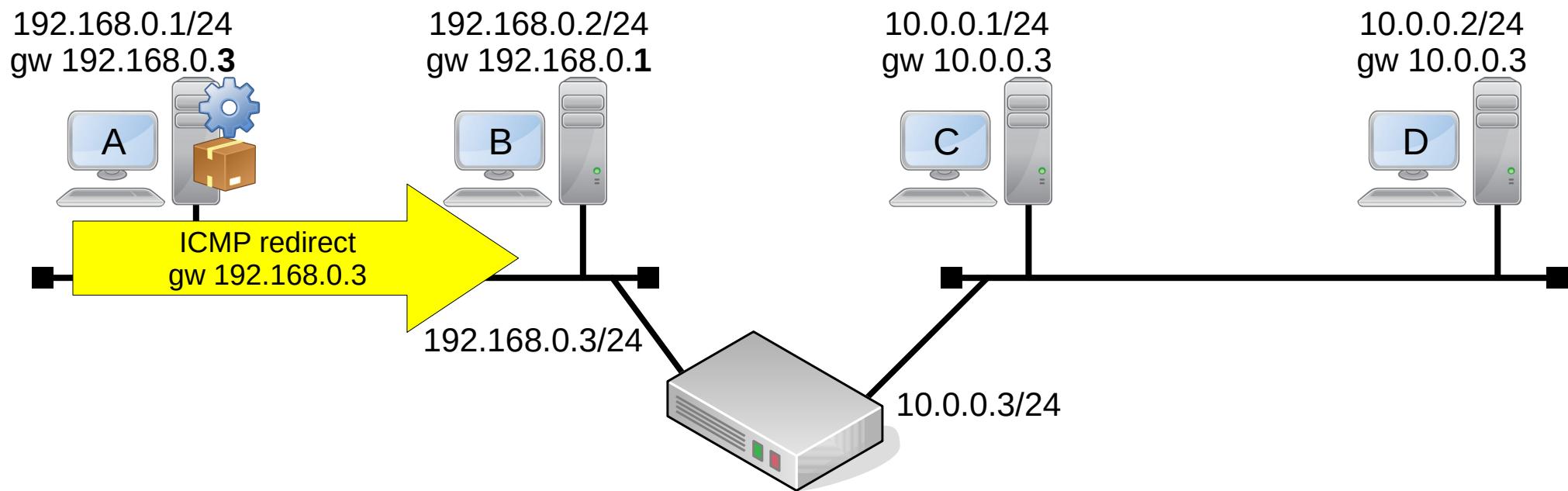
ICMP



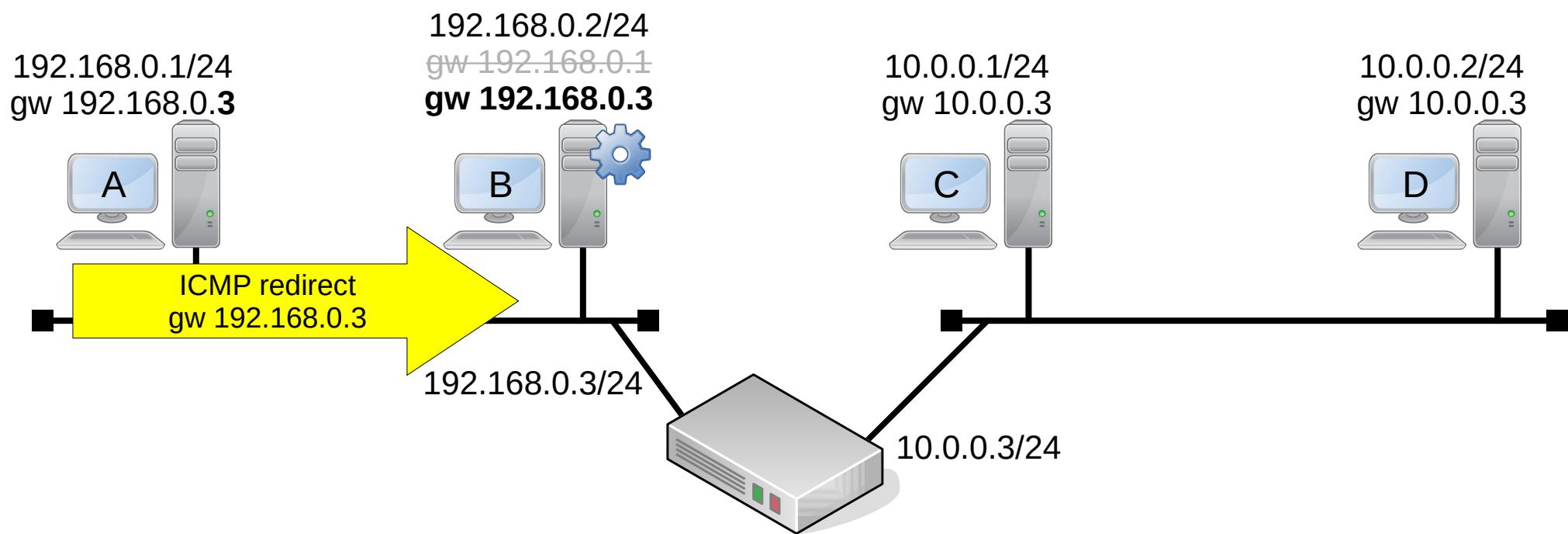
ICMP



ICMP



ICMP



ICMP

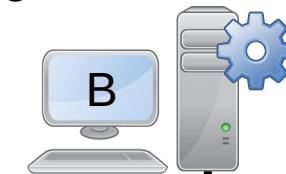


É claro que sistema operacional
tem que aceitar essa troca!

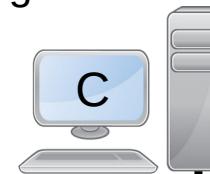
192.168.0.1/24
gw 192.168.0.3



192.168.0.2/24
~~gw 192.168.0.1~~
gw 192.168.0.3



10.0.0.1/24
gw 10.0.0.3



10.0.0.2/24
gw 10.0.0.3

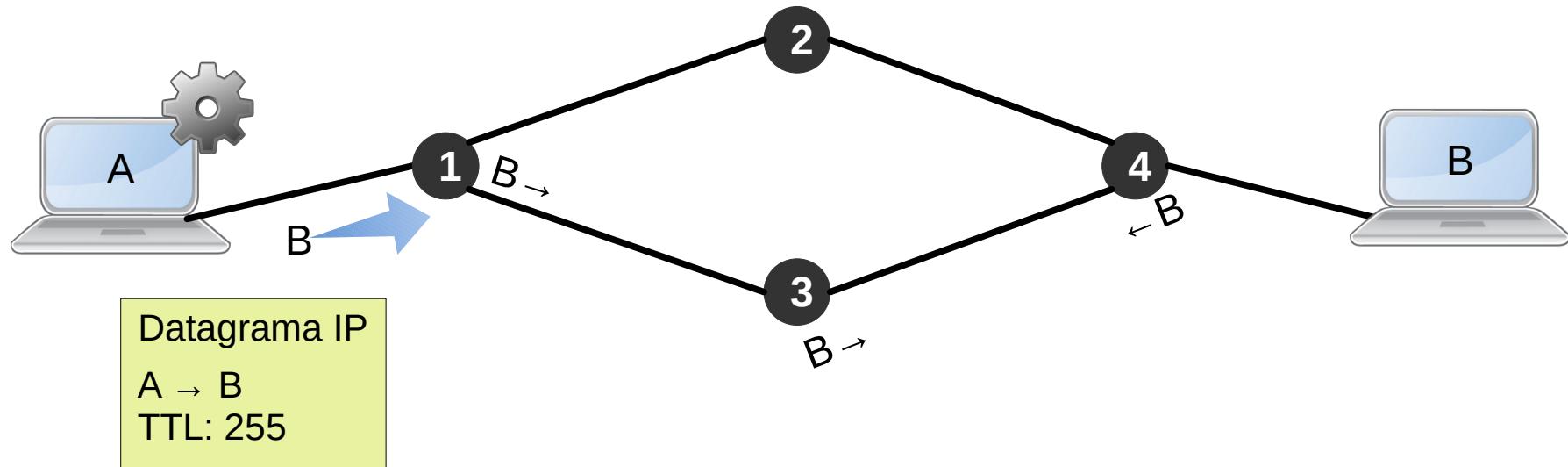


192.168.0.3/24



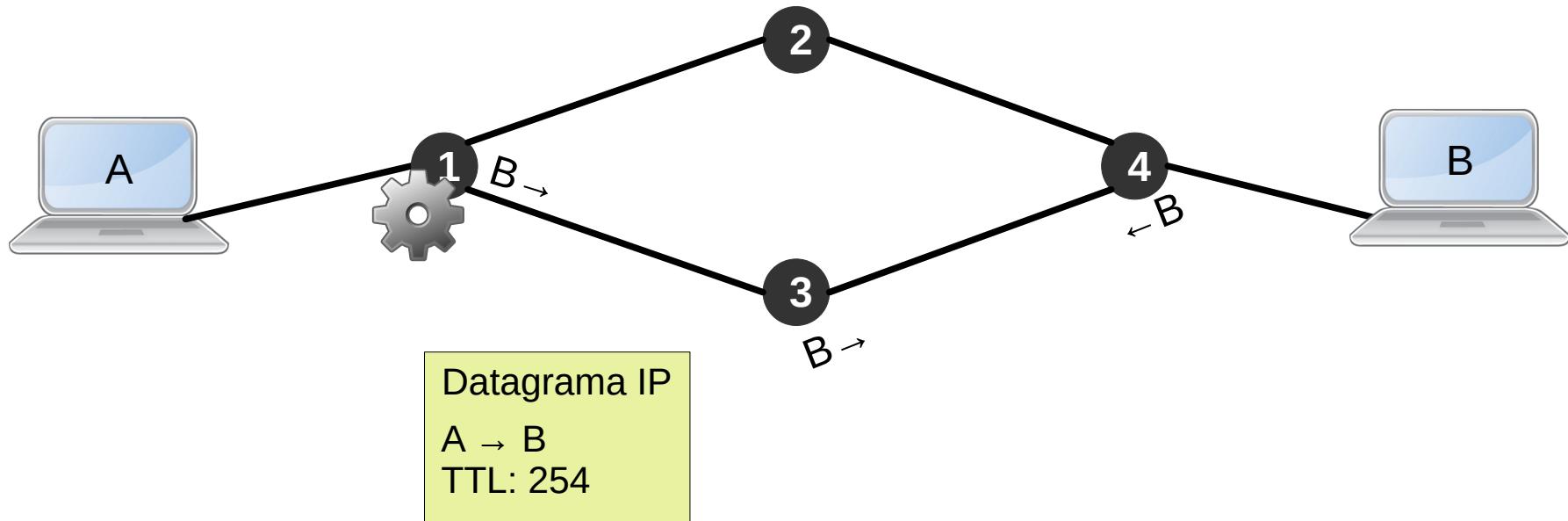
ICMP

Detectando rotas circulares ou excessivamente longas



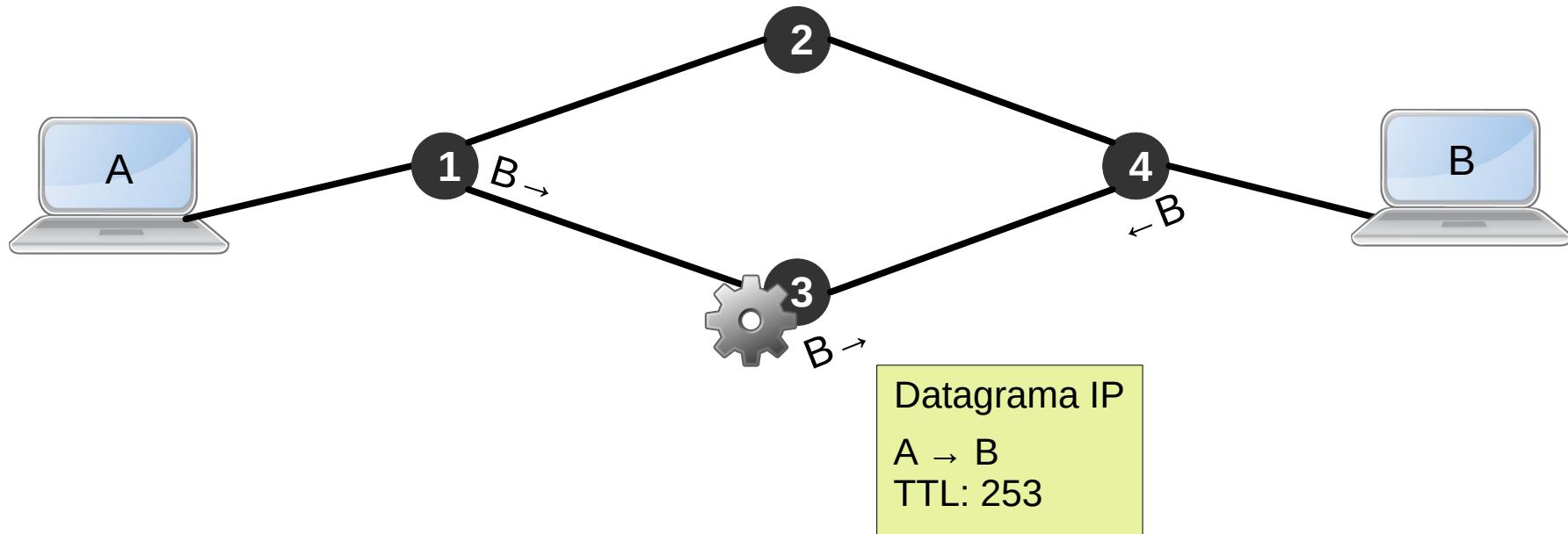
ICMP

Detectando rotas circulares ou excessivamente longas



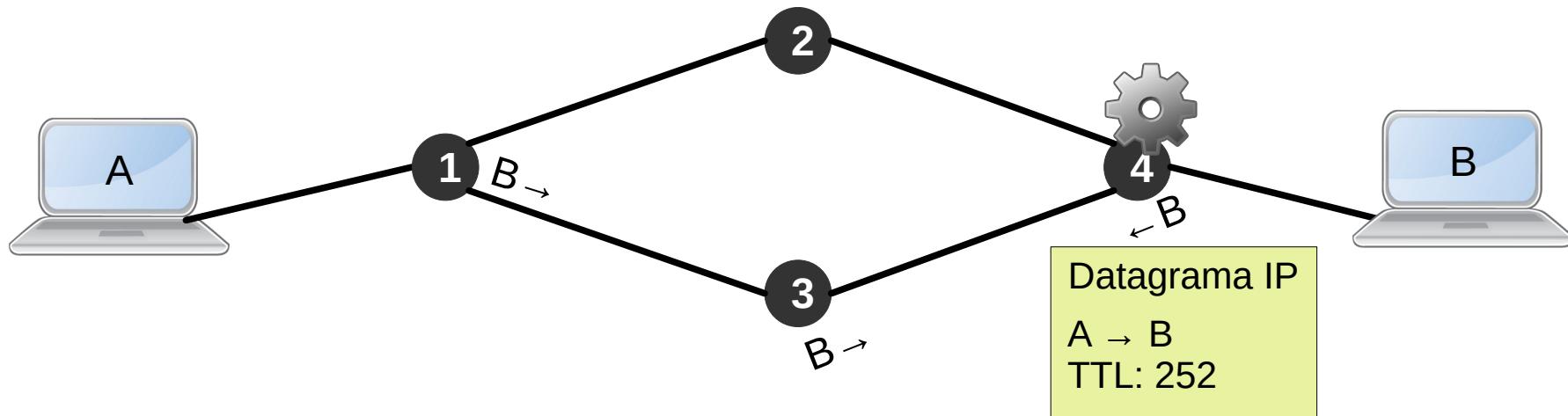
ICMP

Detectando rotas circulares ou excessivamente longas



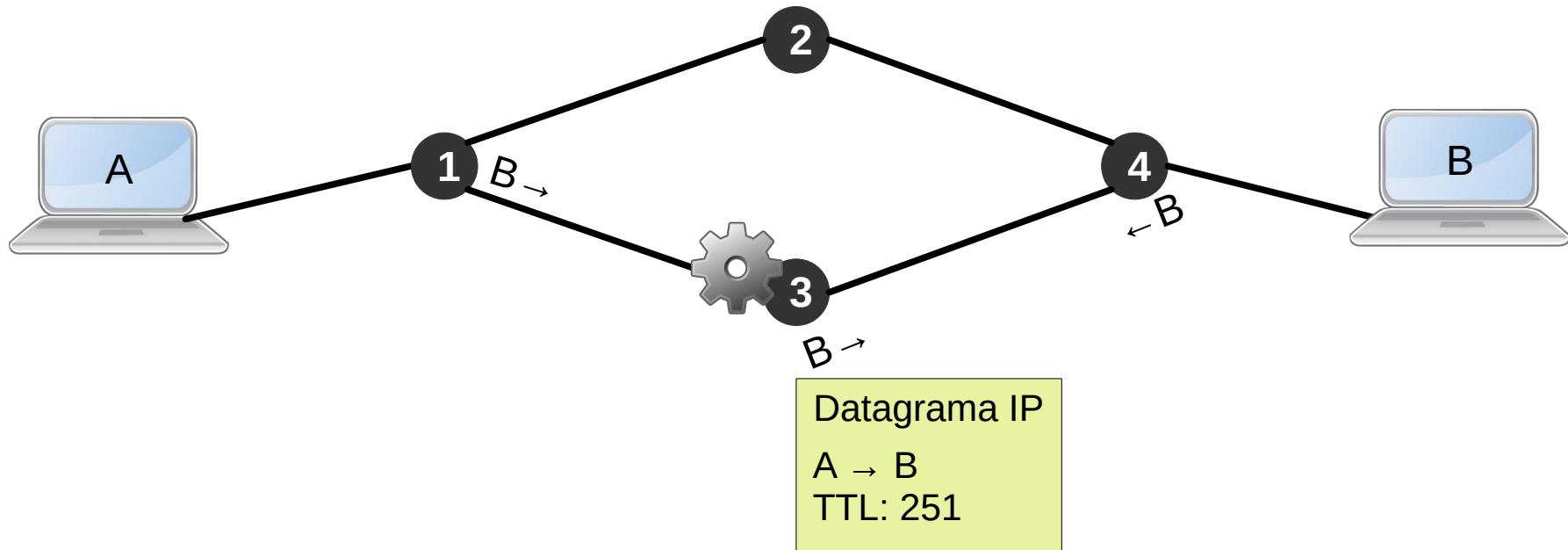
ICMP

Detectando rotas circulares ou excessivamente longas



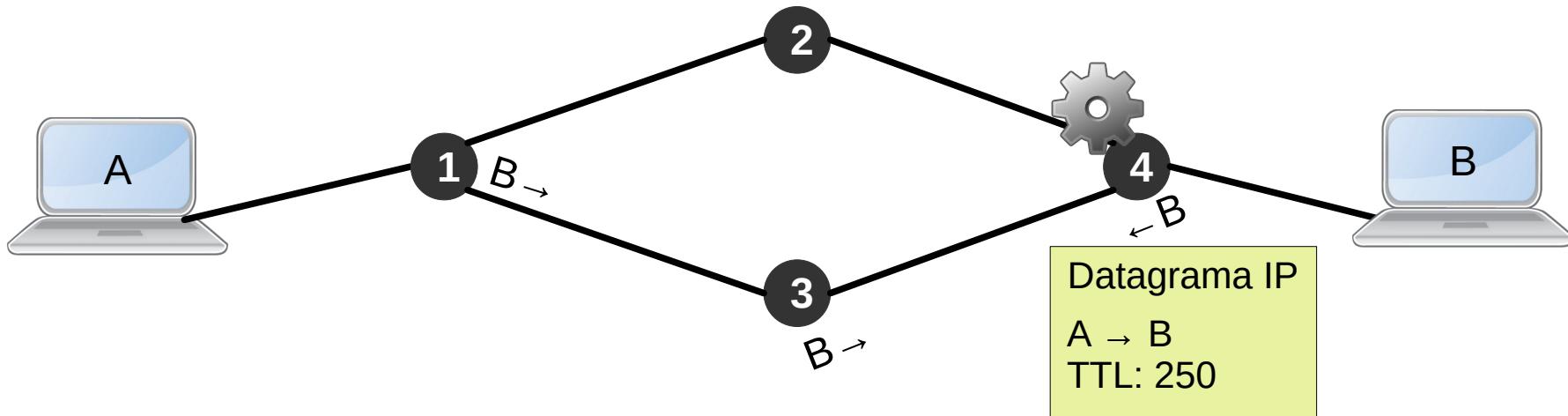
ICMP

Detectando rotas circulares ou excessivamente longas



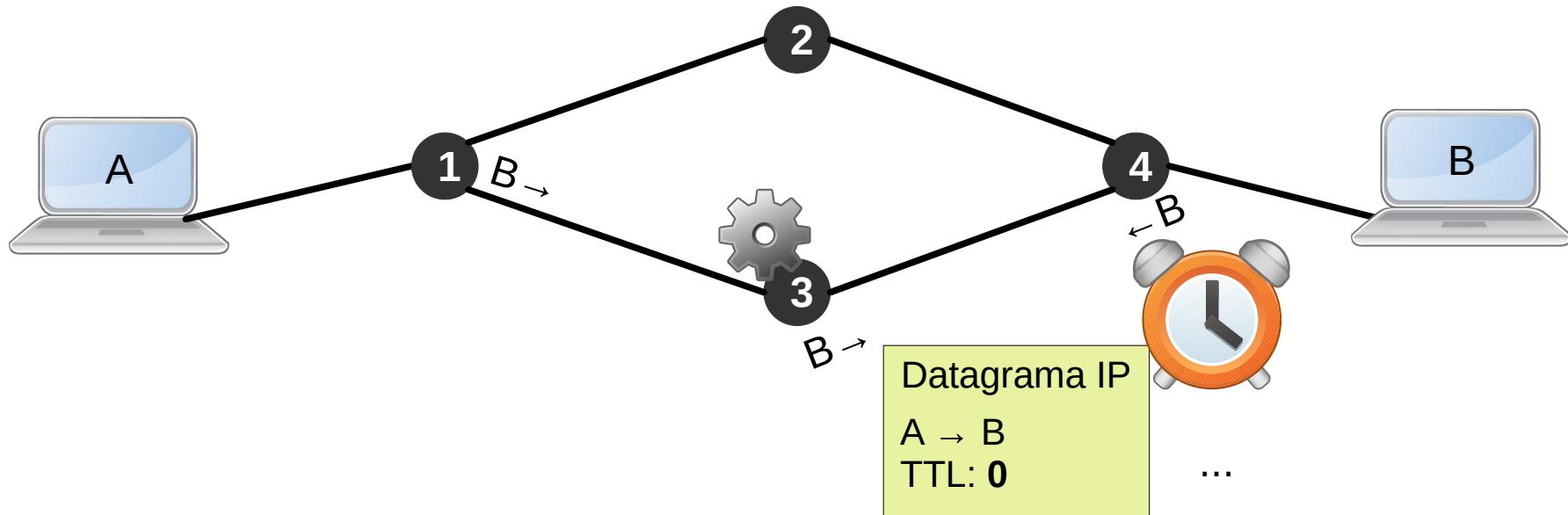
ICMP

Detectando rotas circulares ou excessivamente longas



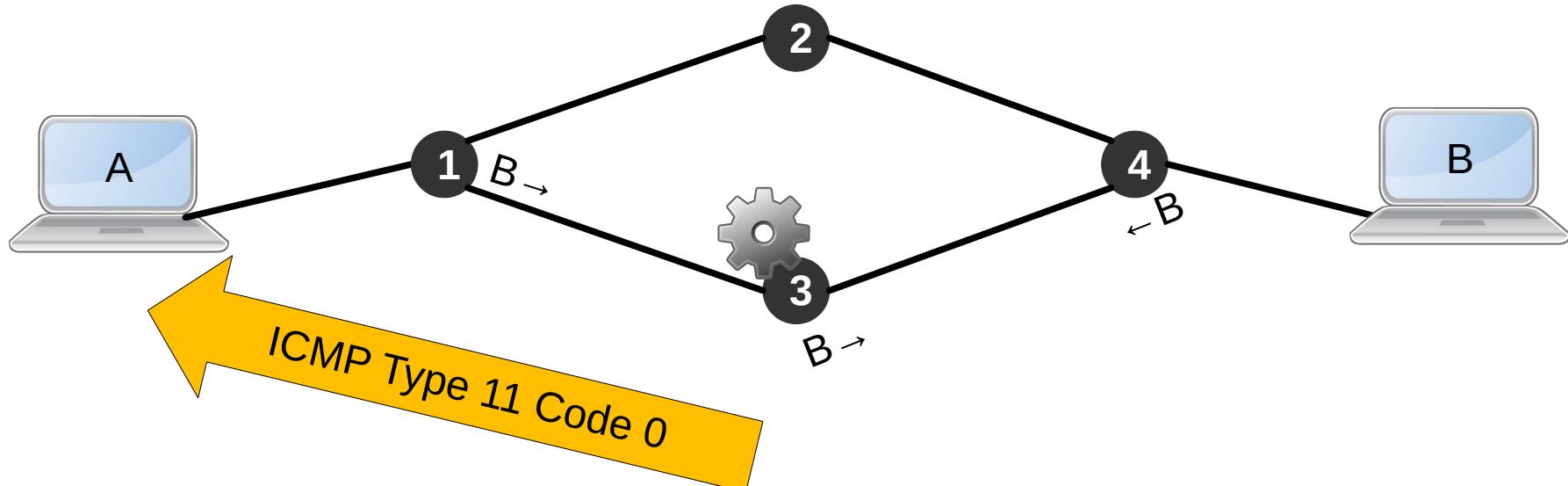
ICMP

Detectando rotas circulares ou excessivamente longas



ICMP

Detectando rotas circulares ou excessivamente longas



ICMP

Nossa quanto tipo de mensagem ICMP...



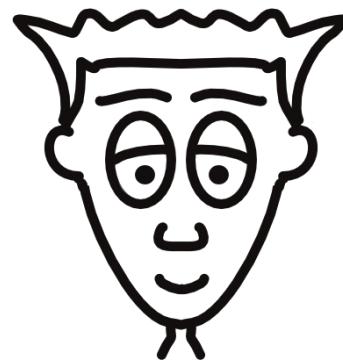
Sim, vamos parar
por aqui, mas há
muito mais...

ICMP

Conclusão:

O ICMP fornece principalmente informações a respeito do que está ocorrendo da rede.

Um dos usos mais conhecidos do ICMP é com o comando ping, mas há vários tipos de mensagens ICMP, fora *echo request* e *reply*.



Obrigado!!!

Prof. Dr. Luiz Arthur Feitosa dos Santos



luiz.arthur.feitosa.santos@gmail.com

<https://luizsantos.github.io/>

Links e referencias na descrição do vídeo