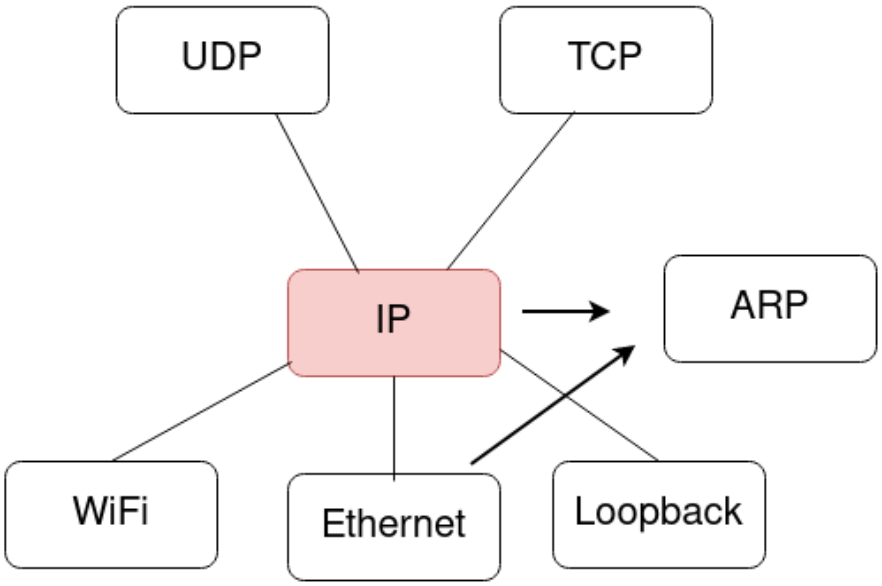
Apontamentos Práticos

Aula P 21/10/2021

- Temos de calcular a disponibilidade como sendo
  - Disponibilidade = Tempo de prestação efetiva do serviço / Tempo de prestação efetiva do serviço + downtime
- **Quando queremos alterar alguma coisa na rede temos sempre de pensar em alterar a rede em si de modo a nunca ter de fazer alterações nos terminais**

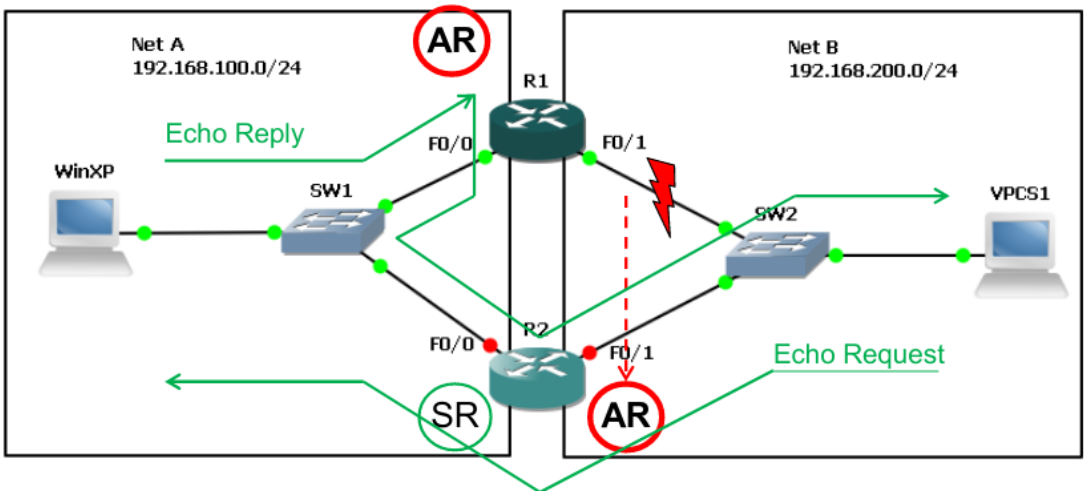
Pilha TCP/IP



Aula T 29/10/2021

- Nesta aula tivemos a ver o HSRP e a fazer algumas experimentações que estão no PowerPoint de Redundância
- Falamos tambem sobre o interface tracking

Interface Tracking



- Se a interface F0/1 do R1 for abaixo, não faz sentido o mesmo ser AR na Rede A, então o que vamos fazer é criar uma regra que diga ao HSRP "se por ventura este interface tiver problemas, não anuncias como AR na outra rede, nem se quer entras no grupo"

- Se isto for feito, tudo se passa como se a outra interface do R1 tivesse em baixo tambem tornando assim o R2 o AR em ambas as redes fazendo com que o encaminhamento passe de assimétrico para simétrico

  - Recorrendo à propriedade de *interface tracking*
  - Como funciona?
    - Os routers envolvidos (R1, R2) devem ser ambos configurados para actuar de forma preemptiva
    - Os routers envolvidos devem estar configurados para vigiar interfaces relevantes
    - Os routers envolvidos devem possuir preferências próximas dentro do grupo. Quando o protocolo associado à interface vigiada ficar *down* a prioridade do router é diminuída automaticamente

- **Atenção que isto só resulta se a preempeção estiver ativa**

Como fazer ?

No R1

```
R1(config)#track ?
  <1-500>     Tracked object
  resolution  Tracking resolution parameters
  timer       Polling interval timers

R1(config)#track 1 ?
  application  Application
  interface    Select an interface to track
  ip           IP protocol
  list         Group objects in a list
  rtr          Response Time Reporter (RTR) entry
  stub-object  Stub tracking object
```

```
R1(config)#track 1 interface f0/1 ?
  ip             IP parameters
  line-protocol  Track interface line-protocol
R1(config)#track 1 interface f0/1 line-protocol

R1(config-track)#?
Tracking instance configuration commands:
  carrier-delay  Report state change only after interface carrier-delay timer
                 expires
  default        Set a command to its defaults
  delay          Tracking delay
  exit           Exit from tracking configuration mode
  no             Negate a command or set its defaults

R1(config-track)#exit
```

- Depois fazemos tambem `track 2 interface f0/0 line-protocol` para vigiar tambem a outra interface do R1
- Depois vamos à f0/0 e fazemos o track à interface f0/1

```
standby 1 track 1
```

- Depois vamos à f0/1 e fazemos o track à interface f0/0

```
standby 1 track 2
```

No R2

- É fazer exatamente o mesmo que foi feito no R1

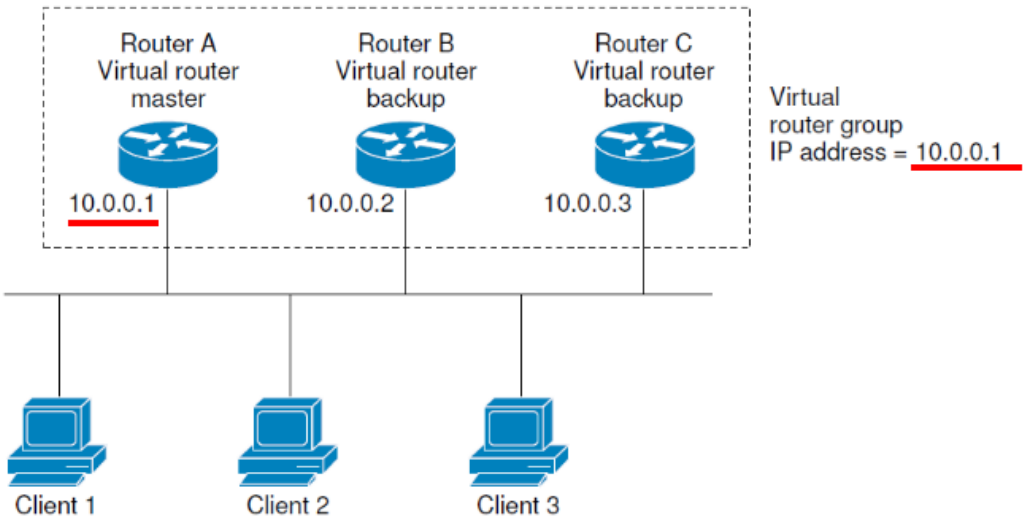
Aula P 04/11/2021

VRRP (Virtual Redundancy Protocol)

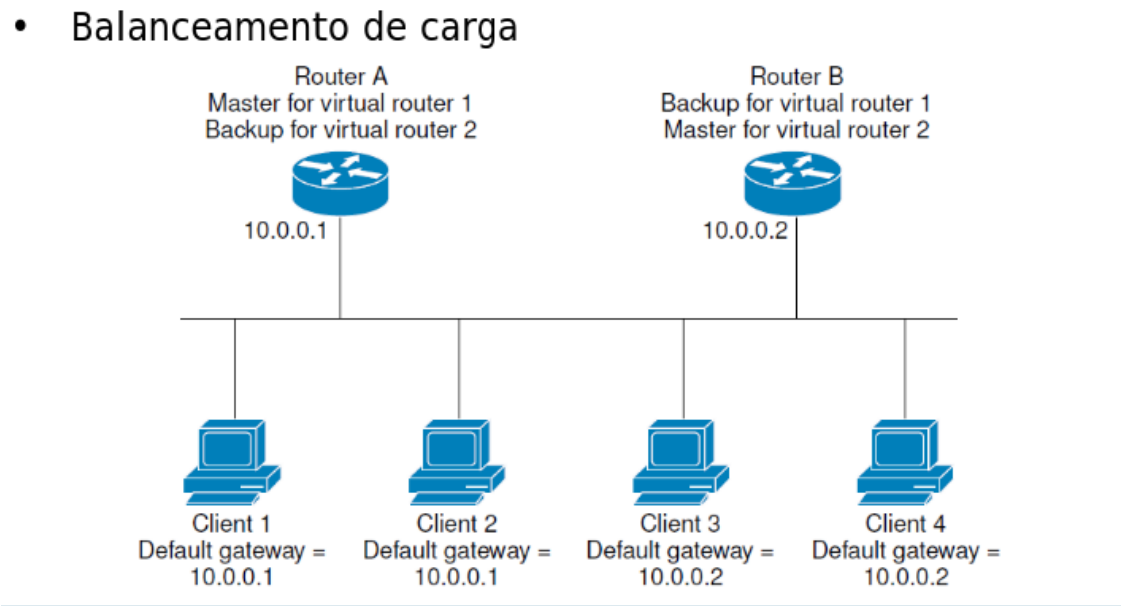
- É um protocolo normalizado pelo IETF que resolve alguns problemas do HSRP
- No VRRP é possível usar um IP atribuido a uma interface
  - A prioridade do router torna-se máxima no grupo
  - No entanto não é possível, neste caso especifico, mudar de forma dinâmica a prioridade do router no grupo com o mecanismo sofisticado de *object tracking*
- No VRRP, tal como no HSRP, é possível diminuir e forma dinâmica a prioridade em resposta à mudança de estado de uma rota ou interface (*object tracking*)

	VRRP	HSRP
Terminologia	Master Router - apenas um Backup Router - restantes	Active router - Apenas um Standby router - Apenas um Listening routers - Restantes
Grupos possíveis	0 a 254	0 a 255
Prioridade	1 a 254 (def. 100) (255 Virtual IP==IP) 0: serve para o master avisar que já não pertence ao grupo	0 a 255 (default 100)
Virtual MAC	0000.5e00.01***xx*** (***xx*** = group)	0000.0c07.ac***xx*** (***xx*** = group)
Virtual IP	Poder ser usado o IP da interface física	Obrigatório
Avisos periódicos	1 segundo (só o Master)	3 segundos (AR e SR)
Preempção	Activo por omissão	Activo se configurado
Object tracking	Interfaces e rotas	Interfaces e rotas
Grupo multicast	224.0.0.18 Protocolo IP 112	224.0.0.2 “all routers” Recorre ao UDP
Autenticação	None, Clear text, IP Authentication Header, MD5	None, Clear text, MD5
Timers	Milisegundo	Segundo (IOS Milisegundo)
IPv6	Não (v1, v2) Sim (v3)	Sim

- A possibilidade de utilizar um endereço IP existente



Balanciamento de carga



- Fizemos experiências com o VRRP

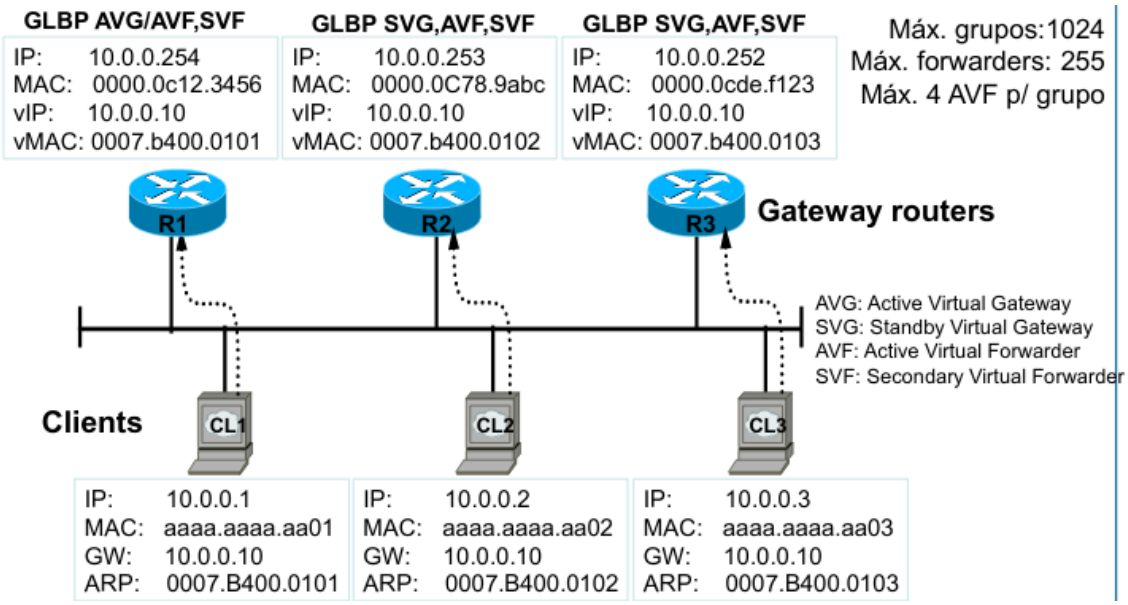
GLBP (Gateway Load Balancing Protocol)

- Representa uma versão HSRP melhorada
  - Suporta explicitamente load balancing sem a necessidade (e complexidade) de configurar múltiplos grupos e múltiplos DGs em clientes distintos
  - Em vez de um, podem ser usados simultaneamente até quatro routers a desempenhar a tarefa de DG
  - Todos partilham o mesmo endereço IP Virtual
  - Todos recorrem a um endereço MAC virtual distinto
  - O protocolo suporta o failover dos membros como o HSRP

Funcionamento

- Os membros de um grupo GLBP elegem um elemento como **Active Virtual Gateway(AVG)**
  - O AVG atribui um Virtual MAC a cada membro do grupo
  - Estes tornam-se **Active Virtual Forwarders(AVFs)**
    - São no máximo 4 e passam a ter a responsabilidade de encaminhar tráfego endereçado para o seu Virtual MAC
  - O AVG responde aos ARP Request dirigidos ao Virtual IP
    - O balanceamento é conseguido através de diferentes respostas
  - Os AVFs estão sempre disponíveis como backup do AVG

- Em caso de falha de um **AVF**
  - Um dos **Secondary Virtual Forwarders (SVF)** toma temporariamente a responsabilidade de PVF daquele MAC Virtual
- Durante *Redirect Time* o AVG continua a enviar *ARP Replies* para o MAC Virtual perdido
- Após esse *timer* expirar o AVG cessa a utilização do MAC Virtual mas o AVF substituido continua a encaminhar trafego que lhe é remetido com o "MAC Virtual perdido"
- Quando o *holdtime timer* expirar o "MAC Virtual perdido" volta a estar disponível para o AVG atribuir



Prioridade

- A prioridade configurada em cada router determina
  - Quem substitui o AVG em caso de falha daquele
  - Quem suporta temporariamente os MAC Virtuais perdidos
  - Na retoma do papel de AVG o modo preempetivo encontra-se inativo por omissão
  - Na retoma do papel de AVF o modo preempetivo encontra-se ativo mas a retoma é atrasada em 30 segundos

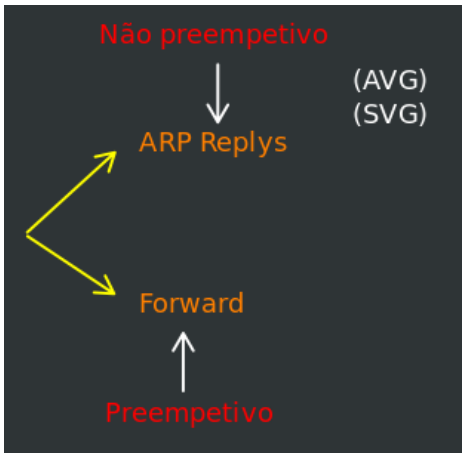
Como é feito o balanceamento de carga?

- Round-Robin
  - Modo de operação por omissão
  - Por cada pedido é fornecido o Virtual MAC do próximo AVF do grupo GLBP, sendo a operação rotativa.
- Host-Dependent
  - Por cada pedido é fornecido o Virtual MAC do próximo AVF do grupo GLBP se o pedido vier de um novo nó (i.e., de um MAC ainda não servido). Caso contrário é atribuído o mesmo Virtual MAC.
- Weighted
  - A distribuição é feita de forma balanceada de acordo com o peso (*weight*) com que *router* está configurado. Opera em histerese: desliga/liga acima/abaixo de determinado nível crítico.

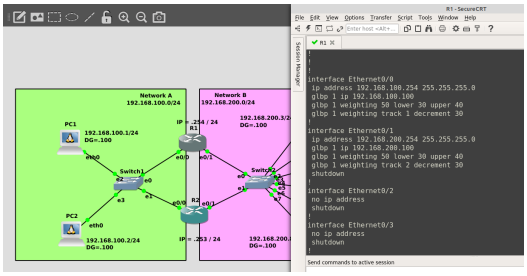
Aula 11/11/2021

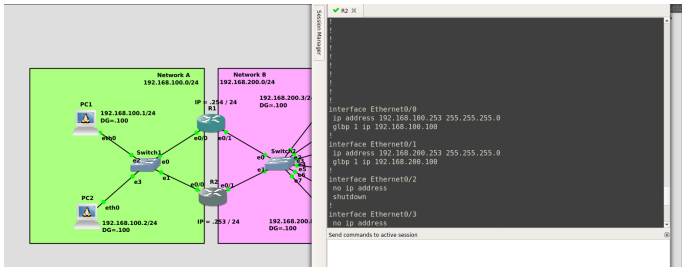
GLBP

- Foi feito um ping do PC1 para o PC3 e o PC3 ficou com um mac virtual, e depois foi feito outro ping do PC1 para o PC4 e o PC4 ficou com um mac virtual diferente do que o PC3 tem no entanto com o mesmo IP virtual e é assim que é feito o loadbalancing



- O GLBP nao permite alterar dinamicamente a priority por *object tracking*
- O *priority* no GLBP apenas server para saber quem faz de *Arp Replier* ou seja quem é o **AVG**
- **Num mecanismo de loadbalancing, o peso serve para saber que router vai ter mais trabalho, ou seja, se tivermos 2 routers com pesos diferentes, o router que tiver maior peso terá mais trabalho**
- Os tracking objects funcionam de maneira diferente no GLBP
- Os tracking objects aqui mexem no peso (`weight`) dos routers para dizermos com que peso é que o router deixa de encaminhar por exemplo
  - "Se o peso descer abaixo de 8 já não encaminhas (**deixa de ser AVF**), se subir acima de 10 passas a encaminhar (**passa a ser AVF**)"





Referências

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-glbp.html#GUID-FFA459B3-479D-4749-8BB6-C2D64EF7E6B7

Aula 02/12/2021

Experiência da aula

- Colocamos uma ACL no R2 para deixarmos apenas sairem IPs públicos permitidos na empresa

```
conf t
ip access-list standard PUBLIC_ADDR_SPACE
permit 194.65.52.0 0.0.0.7 log
deny any log

int e0/1
ip access-group PUBLIC_ADDR_SPACE out
```

- Instalamos uma *discard route* no R2 para o espaço de endereçamento da empresa para que caso o R2 receba trafego de fora para aquela rede, ele envia para null0

```
conf t
ip route 194.65.52.0 255.255.255.248 null0
```

- No R2 criamos uma ACL para depois configurarmos o PAT

```
ip access-list 1 permit 192.168.100.0 255.255.255.0
ip access-list 2 permit 192.168.200.0 255.255.255.0

ip nat inside source list 1 pool NATPOOL_NETA overload
ip nat inside source list 2 pool NATPOOL_NETA overload

int e0/0
ip nat inside
```

- https://moodle.isec.pt/moodle/pluginfile.php/333633/mod_resource/content/6/04_DD_Multihoming_1.12.pdf

Aula 06/01/2022

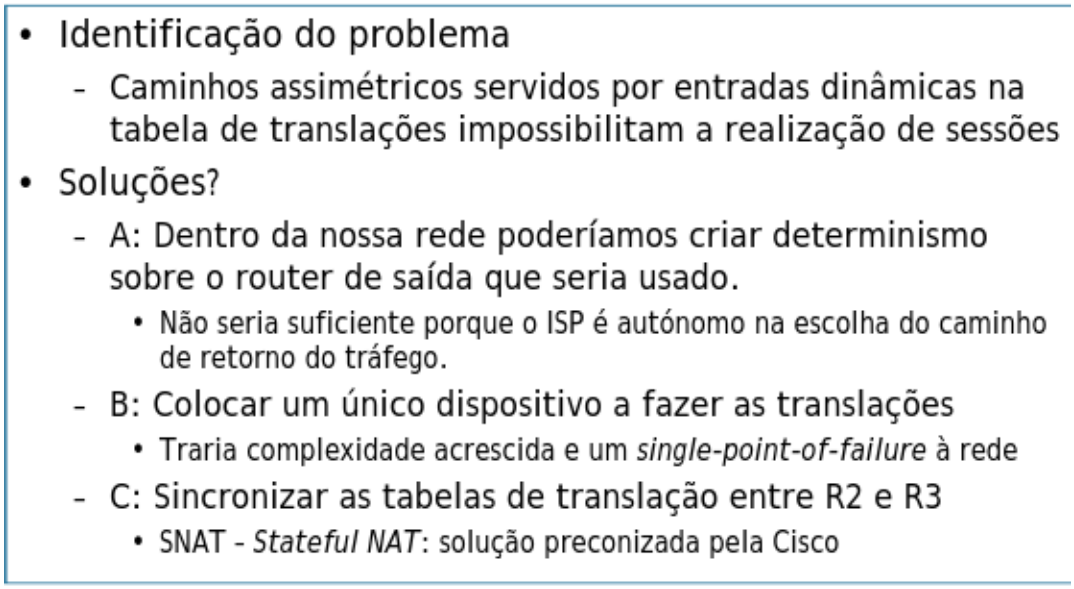
Topologia MultiAttachment

- O comando *redistribute static* redistribui tudo o que são rotas estáticas

Problema 1

- No inicio temos um serviço stateful por isso é que se pingassemos de dentro da empresa para fora funcionava, mas quando voltava ia para o R2 e o R2 nao tem a entrada NAT para receber o Reply (pag.113)
    - As coisas falham porque o caminho é assimétrico (a saida é um caminho e a entrada é outro caminho)
- Se estamos a usar um serviço com estado e queremos aumentar a redundância do mesmo temos de sincronizar os estados

Solução do problema 1



- Na pagina 120 tem uma experiencia com o HSRP mas isso nao funciona porque o RIP nao trabalha com o Virtual IP

Problema 2

- Se quisermos chegar à Internet pelo R2 mas a interface do RISP esteja em baixo, nós queremos que o R2 saiba que nao pode anunciar a sua rota 0.0.0.0 e isso pode ser feito com o object tracking

Solução do problema 2

- Criamos uma sonda no R2 para confirmarmos que o caminho para o exterior a partir do R2 é ou não operacional
    - Temos de usar o *source-interface* sendo este a interface que liga diretamente ao ISP

    - Depois criamos um tracking object que é o element que vai viajar a sonda
    - Depois reescrevemos a rota estatica com o tracking object criado
- No R2

```
conf t
sla 1
icmp-echo 1.1.1.1 source-interface e0/1
frequency 10
timeout 5000
exit
exit
ip sla schedule 1 life forever start-time now
track 3 ip sla 1 reachability
ip route 0.0.0.0 0.0.0.0 194.65.52.9 track 3
```

- *sh ip sla statistics* Mostra as estatisticas da sonda criada
- Mas depois de fazer isto, **temos um problema de dependencia circular** em que a sonda precisa do 0.0.0.0 e o 0.0.0.0 precisa da sonda
- Então eu posso criar no router uma rota especial para o destino **e0/1** e esta entrada vai sempre ser usada antes da entrada dos 0.0.0.0
- No R2(corrigindo a dependencia circular)

```
conf t
ip route 1.1.1.1 255.255.255.255 194.65.52.9
```

- A partir deste momento fico com o pequeno problema na mesma em que o 1.1.1.1 não está protegido pelo tracking object
- **Foi feita a mesma configuração mas no R3**

Stateful NAT

- Protocolo usado para sincronizar tabelas de NAT