

## IP SLA

**Descrição:** É uma feature que permite o gerenciamento proativo das condições da rede monitorada. Basicamente, gera-se um tráfego específico de um dispositivo com destino a outro, que responde a este tráfego e medições são realizadas no decorrer do processo. Esta ferramenta torna muito mais simples tarefas como verificação do correto funcionamento das políticas de QoS, e também permite certificarmos-nos que estamos cumprindo os acordos de “uptime” assinados com o cliente, por exemplo.

Configuração:

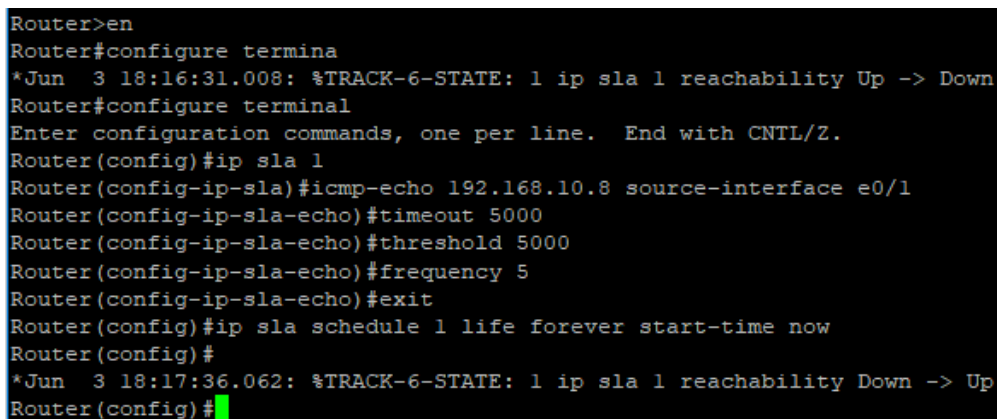
```
Router (config-if) # ip sla 1
Router (config-ip-sla)# icmp-echo 192.168.10.8 source-interface e0/1
Router (config-ip-sla)# timeout 5000
Router (config-ip-sla)# threshold 5000
Router (config-ip-sla)# frequency 5
Router (config-ip-sla)# exit
Router (config)# ip sla schedule 1 life forever start-time now
```

Breve explicação de cada seção dos comandos:

**ICMP Echo** envia um pacote ICMP Echo para 192.168.10.8 a cada 5 segundos, conforme definido no parâmetro “Frequency”.

**Timeout** define a quantidade de tempo que a operação IP SLA deve aguardar a resposta do pacote de requisição enviado. É recomendado configurar o mesmo tempo de Timeout para **trhwshold**.

E por último, é necessário agendar quando e por quanto tempo este IP SLA deve ser executado. Neste caso, ele teve seu “start-time”, ou início, imediatamente após configurado, e tem seu “life-time”, ou tempo de vida, marcado como “forever”, ou para sempre.



```
Router>en
Router#configure termina
*Jun  3 18:16:31.008: %TRACK-6-STATE: 1 ip sla 1 reachability Up -> Down
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip sla 1
Router(config-ip-sla)#icmp-echo 192.168.10.8 source-interface e0/1
Router(config-ip-sla-echo)#timeout 5000
Router(config-ip-sla-echo)#threshold 5000
Router(config-ip-sla-echo)#frequency 5
Router(config-ip-sla-echo)#exit
Router(config)#ip sla schedule 1 life forever start-time now
Router(config)#
*Jun  3 18:17:36.062: %TRACK-6-STATE: 1 ip sla 1 reachability Down -> Up
Router(config)#
```

O comando abaixo irá “rastrear” o status do IP SLA configurado. Caso não haja resposta no ping, o status será mudado para Down, e será alterado novamente para UP quando o endereço do ping voltar a responder.

```
Router(config)#track 1 ip sla 1 reachability
Router(config)#
```

O output abaixo mostra um track que está respondendo aos requests enviados pelo IP SLA.

```
Router#show track
Track 1
  IP SLA 1 reachability
  Reachability is Up
    7 changes, last change 00:08:08
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    Static IP Routing 0
Router#
```

```
Router#sho ip sla statistics 1
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
  Latest RTT: 1 milliseconds
Latest operation start time: 20:43:09 EET Mon Jun 3 2019
Latest operation return code: OK
Number of successes: 308
Number of failures: 0
Operation time to live: Forever

Router#
```

A última etapa é configurar as rotas estáticas e ajustá-las para utilizar o track.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.8 track 1
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.9 10
Router(config)#
```

O parâmetro Track no final da rota estática especifica que a rota será adicionada à tabela de roteamento somente quando o track estiver UP. Quando o track estiver down, a rota some da tabela, e a segunda rota, que agora será a única, assume o tráfego até que o link primário volte a ficar UP.

## SPAN (Switched Port Analyzer)

**Descrição:** O SPAN – Switched Port Analyzer, também conhecido como Port Mirroring ou Port Monitoring é a capacidade de espelhar o tráfego de uma porta (ou portas, ou VLAN) para outra. Entre outras aplicações, esta funcionalidade é muito utilizada em conjunto com equipamentos de análise de rede, que deve receber o tráfego espelhado.

Configuração:

**Switch(config)#monitor session 1 source interface e0/1** (interface origem)

**Switch (config)#monitor session 1 destination interface e0/0 0/5** (interface destino)

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session 1 source interface e0/1
Switch(config)#monitor session 1 destination interface e0/0
Switch(config)#
```

Comando **show monitor session 1** para verificar a configuração

```
Switch#show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
    Both             : Et0/1
Destination Ports   : Et0/0
Encapsulation       : Native

Switch#
```

## Syslog

**Descrição:** O Syslog é um protocolo utilizado pelos sistemas operacionais, processos e aplicativos que permite o envio mensagens de atividades e erros para uma estação de gerenciamento. Existem 08 (oito) níveis de log que variam de 0 (zero) a 7 (sete) com um certo nível de gravidade que indica a natureza crítica da uma certa mensagem.

O Nível 0 é o mais crítico e o Nível 7 é o menos crítico:

- 0 – Emergências
- 1 – Alertas
- 2 – Crítico
- 3 – Erros
- 4 – Avisos
- 5 – Notificações
- 6 – Informações
- 7 – Depuração

Nos equipamentos Cisco o registro syslog baseia-se no utilitário syslog da UNIX. Os eventos do sistema são normalmente registrados no console do sistema a menos que este esteja desativado. Todas as mensagens do log registradas são associadas a uma mensagem de timestamp, de instalação, de gravidade e de registro e às vezes são o único meio para obter informações sobre o comportamento de algum dispositivo.

## Configuração:

Router>enable

Router#configure terminal

Router(config)# logging on (habilita os logs no roteador)

Router (config)# logging 192.168.20.9 (ip da estação que receberá os logs)

Router (config)# logging trap informational (defini o nível de gravidade como 6 "Informativo")

Router (config)#service timestamps log datetime (inclui timestamp com mensagem syslog)

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging on
Router(config)#
*Error opening tftp://255.255.255.255/ciscortr.cfg (Timed out)
*Jun  3 20:33:47.369: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (t
ftp://255.255.255.255/ciscortr.cfg) failed
Router(config)#logging 192.168.20.9
Router(config)#loggi
*Jun  3 20:34:15.913: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.20.9
port 514 started - CLI initiated
Router(config)#logging trap informational
Router(config)#service timestamps log datetime
Router(config)#
```

Comando de verificação da configuração do Syslog

Router (config)#show logging

```
Router#show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes,
 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 43 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 44 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

## SNMP v2c V3 (Simple Network Management Protocol)

**Descrição:** O protocolo SNMP (*Network Management Protocol* – Protocolo Simples de Gerência de Rede) é um protocolo de gerência típica de redes UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (*switches*). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão, dentre outras.

**SNMPv1:** Utiliza o protocolo UDP para transmissão dos dados

- \* Agente escuta a porta 161
- \* Gerente escuta a porta 162 para receber traps
- Segurança fraca, baseada em comunidade (community string) Cada agente possui 3 comunidades: read-only, read-write e trap Por padrão os equipamentos usam “public” e “private” para Community

### Configuração:

**Switch(config)# snmp-server community Una** (habilita o SNMP com a comunidade "Una")

**Switch (config)# snmp-server location Una, Belo Horizonte MG** (opcional: Configura a localidade)

**Switch (config)# snmp-server contact Reristen souza, reristen@una.com.br** (opcional: Configura o contato da localidade)

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#snmp-server community Una
Switch(config)#snmp-server location Una, Belo Horizonte MG
Switch(config)#snmp-server contact Reristen souza, reristen@una.com.br
Switch(config)#
```

**SNMPv2:** Desenvolvido como uma solução intermediária

\* Melhorias: Operação com outros protocolos além de UDP, suporte a comunicação gerente-gerente, novo formato de trap.

Foram criadas versões:

SNMPv2p – baseado em parties (Complexo)

SNMPv2c – baseado em comunidade (Padrão)

SNMPv2u – baseado em usuários

### Configuração:

**Switch(config)# snmp-server community Una**

**Switch(config)# snmp-server host 192.168.40.120 version 2c Una**

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#snmp-server community Una
Switch(config)#snmp-server host 192.168.40.120 version 2c Una
Switch(config)#
```

**SNMPv3:** Desenvolvido a partir de 1998

- \* Requisitos: Manter compatibilidade com versões anteriores, resolver limitações das versões anteriores, arquitetura modular, manter o SNMP o mais simples possível

- \* USM (User-based Security Model)

  - DES, MD5 e SHA1

- \* VACM (View-based Access Control Model)

  - Controla quem pode e o que pode acessar

  - Views – Grupos/Objetos que podem ser acessa

**Configuração:** snmp-server gourp Una v3 priv

**Switch(config)#** snmp-server user Reristen Una v3 auth sha 0123456789 priv aes 128 9876543210

**Switch(config)#** snmp-server contact Reristen

**Switch(config)#** snmp-server location Una, Belo Horizonte MG

```
Switch>
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sten Una v3 auth sha 0123456789 priv aes 128 9876543210
Switch(config)#snmp-server contact Reristen
Switch(config)#snmp-server location Una, Belo Horizonte MG
Switch(config)#
```