Switch PortFast e Port Security

STP PortFast

O Portfast faz uma transição imediata da porta no modo de encaminhamento STP na criação do link. A porta ainda participa do STP. Sendo assim, se a porta for parte de um loop, ela poderá ser escolhida para entrar no modo de bloqueio STP.

Existem dois modos de ativação do portfast, por switch ou por interface individual.

Por Switch, todas as interfaces simultâneas:

Switch(config)# spanning-tree portfast default

Por Interface, ativa em uma porta somente:

Switch(config)#interface fastEthernet 0/1
Switch(config-if)# spanning-tree portfast

Port Security

Essa tecnologia serve para cadastrar os endereços físicos dos dispositivos conectados às suas interfaces de acesso e permitir que somente os dispositivos cadastrados em seu banco de endereços tenham acesso aos recursos da rede.

Este serviço que funciona nas portas de acesso dos switches e controla o tráfego da camada de enlace, é geralmente utilizado para impedir que pessoas não autorizadas se conectem a rede, restringindo a interface, de modo que apenas os dispositivos com seus endereços MAC devidamente cadastrados possam acessá-la.

Existem dois tipos de configuração, uma por inserção de endereços MAC manualmente e outra de forma automática – buscando os Mac atualmente conectados ao switch.

1) Configurar endereços permitidos manualmente

1.1) Interfaces de Acesso

Switch(config)#Interface fa 0/x
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security *(Habilitar Port Security)*
switch(config-if)#switchport port-security mac-address xxx.xxx.xxx
(Configurar endereços permitidos manualmente)

1.2) Interfaces TRUNK

Switch(config)#Interface fa 0/x
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport port-security *(Habilitar Port Security)*
Switch(config-if)#switchport port-security maximum NUN
(Habilitar Port Security para o NUN de mac-address definido, sempre inserir o número de VLANs mais a interface -> 3 VLANs(sub-interfaces) +1(interface real) = 4)
switch(config-if)#switchport port-security mac-address xxx.xxx.xxx
(Configurar endereços permitidos manualmente)

2) Configurar automaticamente para que todos os PCs conectados ao switch tenham acesso:

2.1) Interface de Acesso

Switch(config)#Interface fa 0/x
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security *(Habilitar Port Security)*
switch(config-if)# switchport port-security mac-address sticky
(Configurar endereços permitidos de forma automática)

2.2) Interface TRUNK

Switch(config)#Interface fa 0/x
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport port-security *(Habilitar Port Security)*
Switch(config-if)#switchport port-security maximum NUN
(Habilitar Port Security para o NUN de mac-address definido, sempre inserir o número de VLANs mais a interface -> 3 VLANs(sub-interfaces) +1(interface real) = 4)
switch(config-if)# switchport port-security mac-address sticky
(Configurar endereços permitidos de forma automática)

3) Definir o que fazer caso seja conectado um MAC fora da Lista

switch(config-if)#switchport port-security violation shutdown|restrict|protect

Shutdown - ação padrão, onde manda logs e SNMP de mac errado, descarta tráfego e desativa a interface

OBS: Caso uma interface esteja com a ação de violação shutdown e ocorra a violação de segurança naquela interface, a mesma será colocada em estado err-disable, e para que a mesma volte a operar normalmente, é necessário desabilita-la (shutdown) e habilitar novamente (no shutdown).

Restrict - Descarta todo o trafego e manda log e SNMP ao administrador

Protect - Protege descartando todo o trafego que vem daquela porta.

4) Analisar port-security

Para certificamos de que a configuração foi feita com sucesso, e verificarmos se a segurança de portas foi violada, podemos utilizar o seguinte comando:

Switch# show port-security