Redes y comunicación de Datos 2

Sesión 15

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Dinámica: Lluvia de ideas sobre la Seguridad de Switch.
- Configuración de seguridad de Switch
- Mitigación de Ataques
- **Actividad:**
  - Configuración Seguridad Switch.

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la unidad, el estudiante explica los conceptos de seguridad y mitigación de ataques que ponen en riesgo la seguridad LAN., a través de ejemplos desarrollados en clase.

Buenas Prácticas

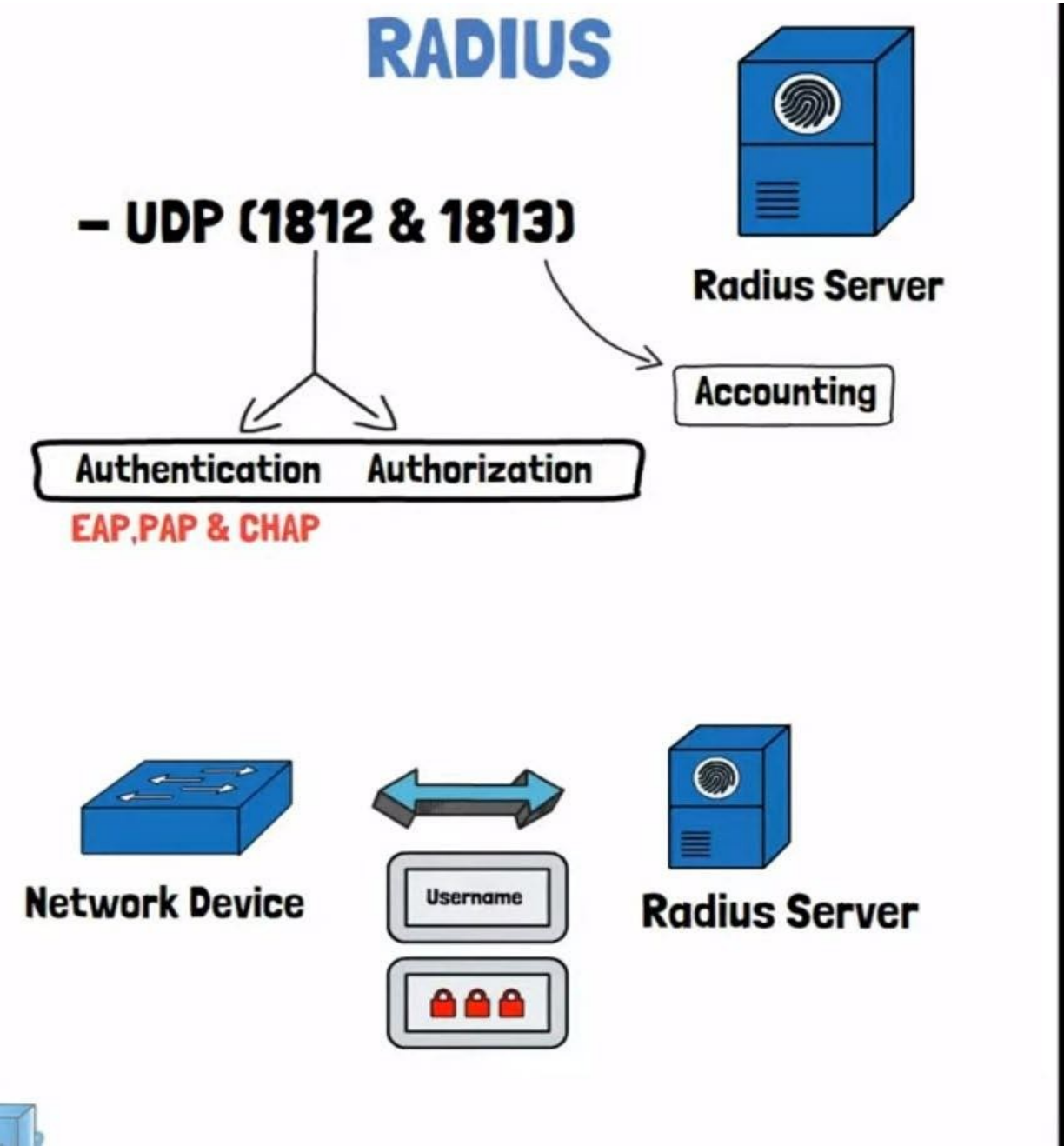
Buenas Prácticas

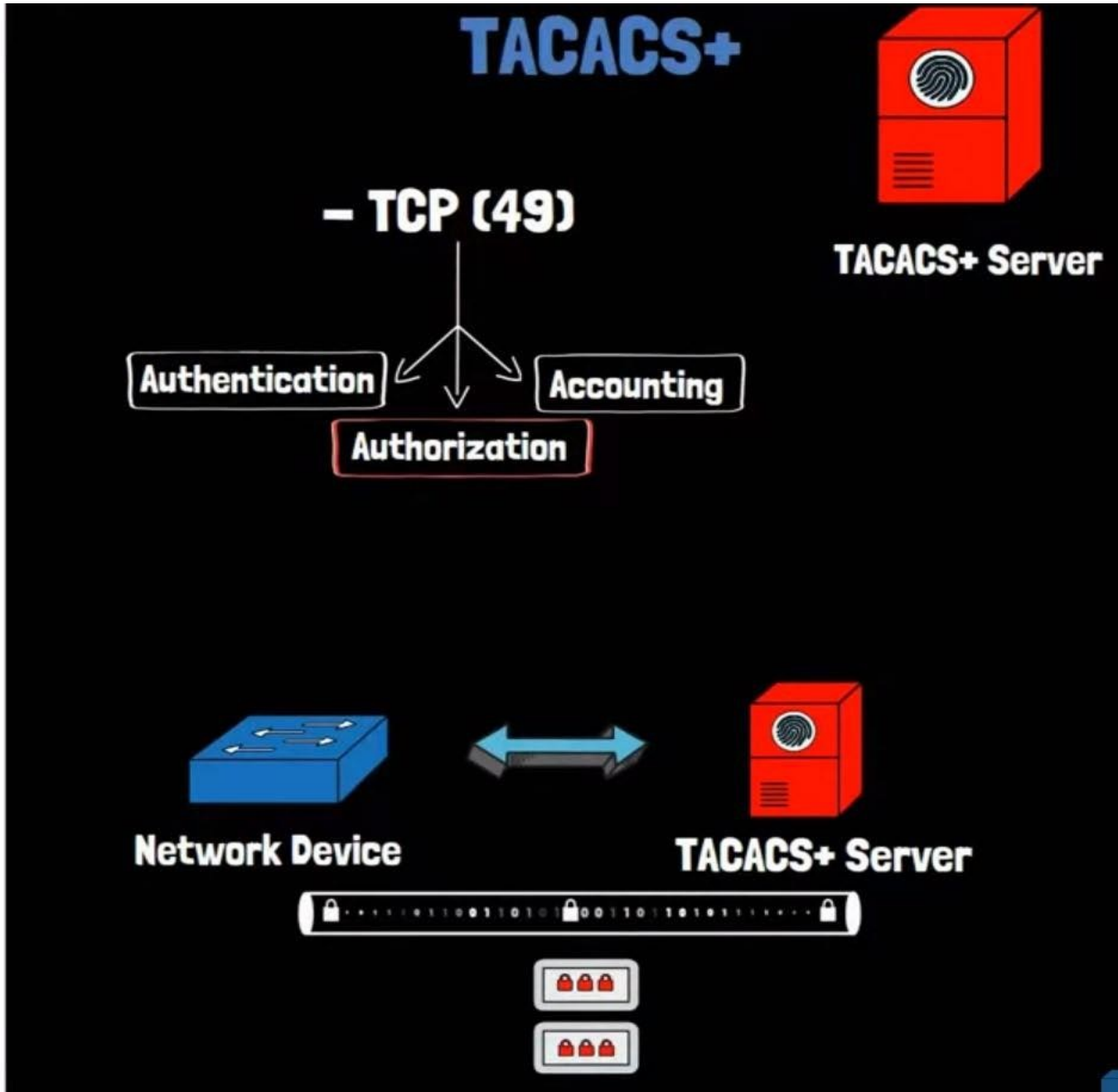
Con respecto a la Sesión 14

- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

Radius / Tacacs



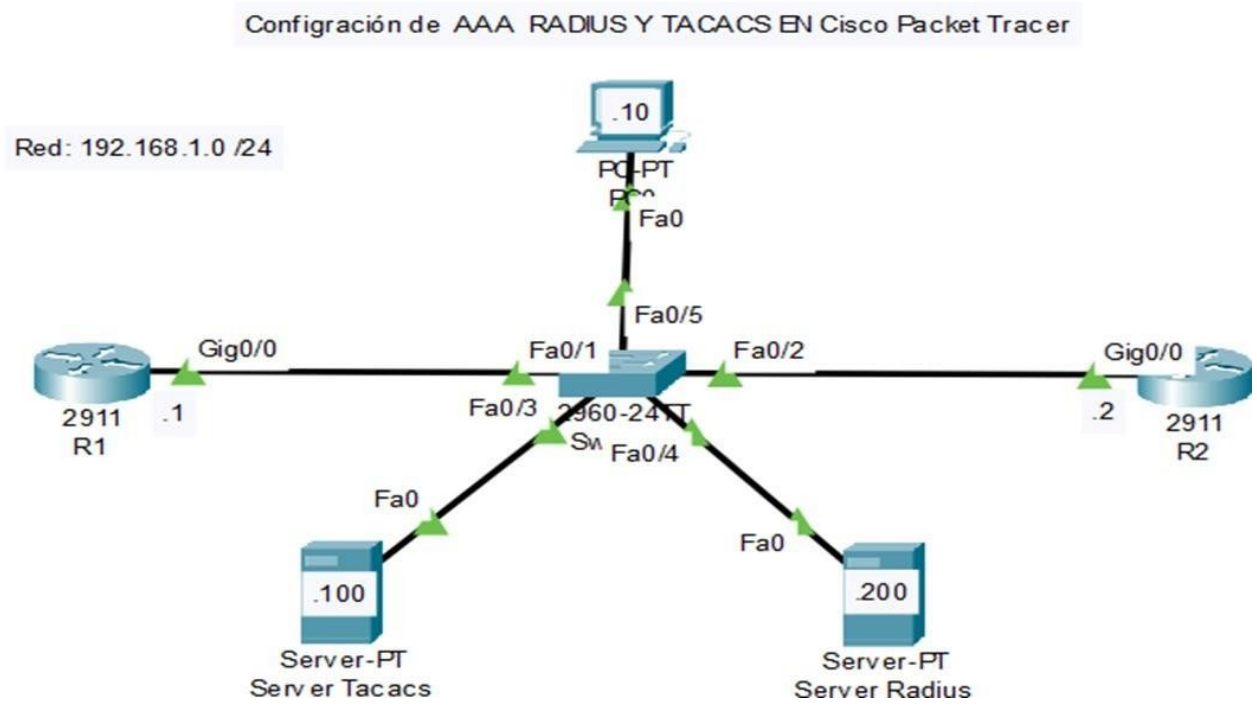


El protocolo AAA Radius/Tacacs

Información básica

- Los servidores AAA (Autorización, Autenticación y Accounting), se utilizan para una mayor seguridad en el acceso dentro de una red, centralizando y asegurando el acceso a dispositivos de red.

- Existen dos protocolos principales que son RADIUS y TACACS



Buenas Prácticas

Sesión 15

Lluvia de ideas sobre el port security

- ¿Qué es el port security?
- ¿Para que nos sirve el port security?

Implementar Seguridad de Puertos (Port Security)

Implementar Seguridad de Puertos (Port Security)

Asegure los puertos no utilizados

Los ataques de Capa 2 son de los más sencillos de desplegar para los hackers, pero estas amenazas también pueden ser mitigadas con algunas soluciones comunes de capa 2.

- Se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para la producción. ¿Cómo se asegura un puerto dependiendo de su función?.
- Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Navegue a cada puerto no utilizado y emita el comando de apagado **shutdown** de Cisco IOS. Si un puerto debe reactivarse más tarde, se puede habilitar con el comando **no shutdown**.
- Para configurar un rango de puertos, use el comando **interface range**.

```
Switch(config)# interface range type module/first-number - last-number
```

Implementar la seguridad de puertos (Port Security)

Mitigar los ataques de la tabla de direcciones MAC

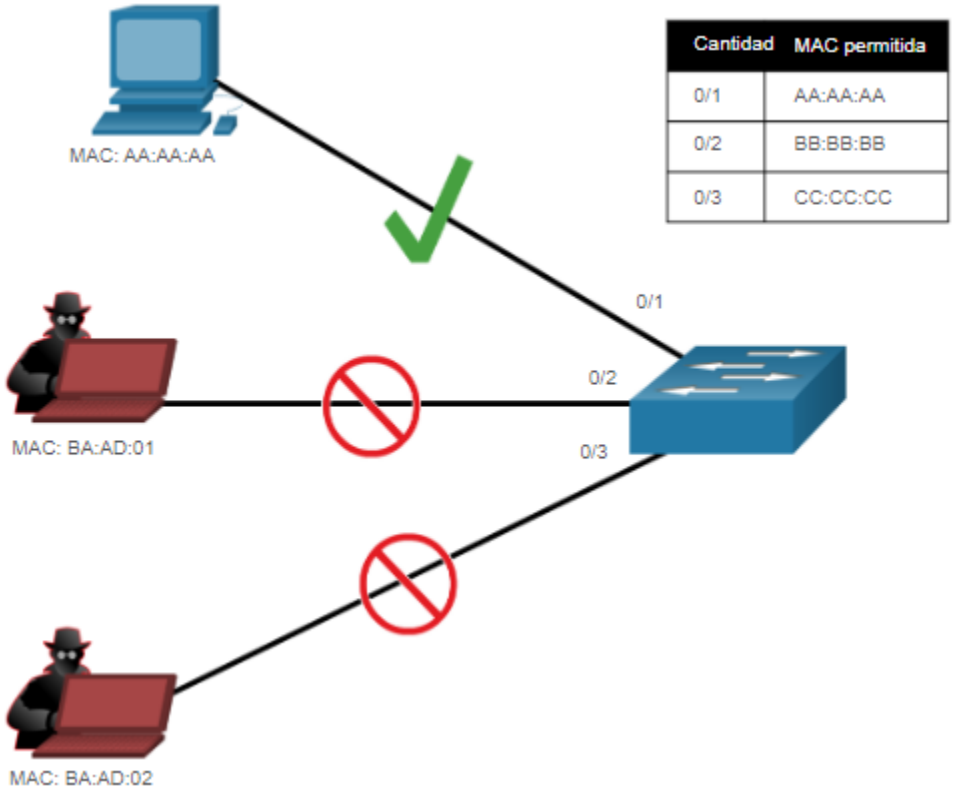
El método más simple y eficaz para evitar ataques por saturación de la tabla de direcciones MAC es habilitar el port security.

- La seguridad de puertos limita la cantidad de direcciones MAC válidas permitidas en el puerto. Permite a un administrador configurar manualmente las direcciones MAC para un puerto o permitir que el switch aprenda dinámicamente un número limitado de direcciones MAC. Cuando un puerto configurado con port security recibe un trama, la dirección MAC de origen del trama se compara con la lista de direcciones MAC de origen seguro que se configuraron manualmente o se aprendieron dinámicamente en el puerto.

Implementar la seguridad de puertos (Port Security)

Mitigar los ataques de la tabla de direcciones MAC

- Al limitar a uno el número de direcciones MAC permitidas en un puerto, port security se puede utilizar para controlar el acceso no autorizado a la red.



Cantidad	MAC permitida
0/1	AA:AA:AA
0/2	BB:BB:BB
0/3	CC:CC:CC

Implementar Seguridad de puertos (Port Security)

Activar Port Security

Port security se habilita con el comando **switchport port-security** de la interfaz de puerto

Observe que en el ejemplo, el comando **switchport port-security** fue rechazado. Esto se debe a que port security solo se puede configurar en puertos de acceso o trunks configurados manualmente. Los puertos capa 2 del switch están definidos como dynamic auto (troncal encendido), de manera predeterminada. Por lo tanto, en el ejemplo, el puerto se configura con el comando **switchport mode access** de la interfaz

Nota: La configuración de port security troncal va mas allá del alcance de este curso.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Implementar Seguridad de puertos (Port Security)

Activar Port Security (Cont.)

Use el **comando show port-security interface** para mostrar la configuración de seguridad del puerto actual para FastEthernet 0/1.

- Note que port security está habilitado, el modo de violación esta apagado, y que el número máximo de direcciones MAC permitidas es 1.
- Si un dispositivo está conectado al puerto, el switch automáticamente agregará la dirección MAC de este dispositivo como una dirección MAC segura. En este ejemplo, no existe ningún dispositivo conectado al puerto.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Nota: Si un puerto activo está configurado con el comando **switchport port-security** y hay más de un dispositivo conectado a ese puerto, el puerto pasará al estado de error desactivado.

Implemente Seguridad de puertos (Port Security)

Activar Port Security (Cont.)

Una vez que se activa port security, se pueden configurar otras funciones específicas de port security, como se muestra en el ejemplo.

```
S1(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
S1(config-if)# switchport port-security
```

Implementar Seguridad de Puertos (Port Security)

Limitar y aprender direcciones MAC

Para poner el número máximo de direcciones MAC permitidas en un puerto, utilice el siguiente comando

```
Switch(config-if)# switchport port-security maximum valor
```

- El valor predeterminado de port security es 1.
- El número máximo de direcciones MAC seguras que se puede configurar depende del switch y el IOS.
- En este ejemplo, el máximo es 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Implementar Seguridad de Puertos (Port Security)

Limitar y Aprender MAC Addresses (Cont.)

El switch se puede configurar para aprender direcciones MAC en un puerto seguro de tres maneras:

1. Configuración manual:el administrador configura manualmente una dirección MAC estática mediante el siguiente comando para cada dirección MAC segura en el puerto:

```
Switch(config-if)# switchport port-security mac-address dirección MAC
```

2.Aprendizaje dinámico: cuando se ingresa el comando **switchport port-security** la fuente MAC actual para el dispositivo conectado al puerto se asegura automáticamente pero no se agrega a la configuración en ejecución. Si el switch es reiniciado, el puerto tendrá que re-aprender la direccion MAC del dispositivo.

3.Aprendizaje dinámico: – Sticky: el administrador puede configurar el switch para aprender dinámicamente la dirección MAC y "adherirla" a la configuración en ejecución mediante el siguiente comando:

```
Switch(config-if)# switchport port-security mac-address sticky
```

Al guardar la configuración en ejecución la dirección MAC aprendida automáticamente se quedara en NVRAM.

Implementar Seguridad de Puertos (Port Security)

Limitar y Aprender direcciones MAC (Cont.)

El ejemplo muestra una configuración de seguridad de puerto completa para FastEthernet 0/1.

- El administrador especifica una cantidad máxima de 4 direcciones MAC, configura una direccion MAC segura, y luego configura el puerto para que aprenda mas direcciones MAC de manera automática hasta un máximo de 4 direcciones MAC.
- Use los comandos **show port-security interface** y el **show port-security address** para verificar la configuración.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

Implementar Seguridad de Puertos (Port Security)

activar Port Security

El vencimiento del port security puede usarse para poner el tiempo de vencimiento de las direcciones seguras estáticas y dinámicas en un puerto.

- **Absoluta**- Las direcciones seguras en el puerto se eliminan después del tiempo de caducidad especificado.
- **Inactiva**- Las direcciones seguras en el puerto se eliminan si están inactivas durante un tiempo específico.

Utilice el vencimiento para remover las direcciones MAC seguras en un puerto seguro sin necesidad de eliminar manualmente las direcciones MAC existentes.

- El vencimiento de direcciones seguras configuradas estáticamente puede ser habilitado o des-habilitado por puerto.

Use el comando**switchport port-security aging** para habilitar o deshabilitar el vencimiento estático para el puerto seguro, o para establecer el tiempo o el tipo de vencimiento.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

Implementar Seguridad de Puertos (Port Security)

Vencimiento de Port Security (Cont.)

El ejemplo muestra a un administrador configurando el tipo de vencimiento a 10 minutos de inactividad.

El comando **show port-security** confirma los cambios.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

Modos de violación de Port Security

Si la dirección MAC de un dispositivo conectado a un puerto difiere de la lista de direcciones seguras, se produce una violación del puerto y el puerto entra en estado de error desactivado.

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

La siguiente tabla muestra cómo reacciona un switch en función del modo de infracción configurado.

Modo	Descripción
shutdown (predeterminados)	El puerto pasa al estado de error desactivado de inmediato, apaga el LED del puerto y envía un mensaje de registro del sistema. Aumenta el contador de violaciones. Cuando un puerto seguro se encuentra en estado de error desactivado, un administrador debe volver a habilitarlo ingresando los comandos **shutdown** y **no shutdown**.
restrict (Restricción)	El puerto descarta paquetes con direcciones de origen desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para caer por debajo del valor máximo o aumentar el valor máximo. Este modo hace que el contador de Infracción de seguridad se incremente y genera un mensaje de syslog.
protect (protección)	Este modo es el menos seguro de los modos de violaciones de seguridad. El puerto descarta paquetes con direcciones de origen MAC desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para colocar por debajo del valor máximo o aumentar el valor máximo. No se envía ningún mensaje syslog.

Implementar Seguridad de Puertos (Port Security)

Modos de violación de Security (Cont.)

El ejemplo muestra a un administrador cambiando la violación de seguridad a "Restrict"

El resultado del comando **show port-security interface** confirma que se ha realizado el cambio.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
S1#
```

Implementar Seguridad de Puertos (Port Security)

Puertos en estado de error-disabled

Cuando un puerto está apagado y puesto en modo error-desabilitado, no se envía ni se recibe tráfico a través de ese puerto.

En la consola, se muestra una serie de mensajes relacionados con la seguridad del puerto.

Nota: **El protocolo del puerto y el estado del enlace se cambian a inactivo y el LED del puerto se apaga.**

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in
err-disable state
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000c.292b.4c75 on port FastEthernet0/18.
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state
to down
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Implementar Seguridad de Puertos (Port Security)

Puertos en estado error-disabled (Cont.)

- En el ejemplo, el comando **show interface** identifica el estado del puerto como **err-disabled**. La salida del comando **show port-security interface** ahora muestra el estado del puerto como **secure-shutdown**. El contador de violación incrementa en uno.
- El administrador debe determinar que causó la violación de seguridad, si un dispositivo no autorizado está conectado a un puerto seguro, la amenazas de seguridad es eliminada antes de restablecer el puerto.
- Para volver a habilitar el puerto, primero use el **shutdown** luego, use el comando **no shutdown**.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

Implementar Seguridad de Puertos (Port Security)

Verificar Port Security

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Para mostrar la configuración de seguridad del puerto para el conmutador, use el comando **show port-security**.

- El ejemplo indica que las 24 interfaces están configuradas con el comando **switchport port-security** porque el máximo permitido es 1 y el modo de violación está apagado.
- No hay dispositivos conectados, por lo tanto, el CurrentAddr (Count) es 0 para cada interfaz.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
-----------------------------------------------------------------------------
      Fa0/1            1            0                  0         Shutdown
      Fa0/2            1            0                  0         Shutdown
      Fa0/3            1            0                  0         Shutdown
(output omitted)
     Fa0/24            1            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Implementar Seguridad de Puertos (Port Security)

Verificar Port Security (Cont.)

Use el comando **show port-security interface** para ver detalles de una interfaz específica, como se mostró anteriormente y en este ejemplo.

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
S1#
```

Implementar Seguridad de Puertos (Port Security)

Verificar Port Security (Cont.)

Para verificar que las direcciones MAC están configuradas “sticking” (pegadas) a la configuración, use el comando **show run** como se muestra en el ejemplo de FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

Implementar Seguridad de Puertos (Port Security)

Verificar Port Security (Cont.)

Para mostrar todas las direcciones MAC seguras que son configuradas manualmente o aprendidas dinámicamente en todas las interfaces del switch use el comando **show port-security address** como se muestra en el ejemplo.

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type            Ports     Remaining Age
                                                        (mins)
----    -----------       ----            -----     -------------
1       0025.83e6.4b01    SecureDynamic   Fa0/18            -
1       0025.83e6.4b02    SecureSticky    Fa0/19            -
------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Actividad

Práctica de laboratorio

Packet Tracer

Actividades

- ¿Cómo podría la seguridad del puerto causar problemas a los usuarios legítimos?
- ¿Qué modo de violación de la seguridad del puerto parece ser el más eficaz para la implementación general y por qué?
- ¿Hay alguna desventaja en configurar puertos como acceso estático o troncal estático?
- ¿Qué beneficio cree que se obtiene al designar una VLAN nativa para toda la organización?
- ¿Cómo podría afectar negativamente DHCP Snooping a un usuario autorizado para conectarse a la LAN?
- ¿Qué tienen los datos que recopila DHCP Snooping que son tan fundamentales para otros mecanismos de seguridad de LAN?
- ¿Qué pasa si otro dispositivo pretende ser la puerta de enlace predeterminada en una LAN?
- ¿Por qué cree que los puertos que miran hacia arriba normalmente se configuran como confiables para la inspección ARP dinámica?

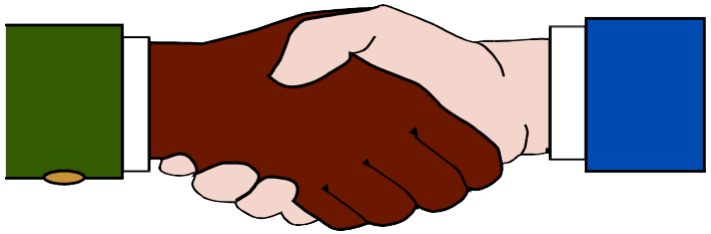
Conclusiones

¿Qué aprendí en esta sesión?

¿Qué aprendí en está sesión?

- Se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para la producción.
- Los puertos capa 2 del switch están definidos como dynamic auto (troncal encendido), de manera predeterminada.
- El método más simple y eficaz de evitar ataques por saturación de la tabla de direcciones MAC es habilitar la seguridad de los puertos (port security).
- El switch se puede configurar para obtener información sobre las direcciones MAC en un puerto seguro de una de las siguientes tres maneras: configurado manualmente, aprendido dinámicamente y aprendido dinámicamente-fijo.
- Si la dirección MAC de un dispositivo conectado a el puerto difiere de la lista de direcciones seguras, entonces ocurre una violación de puerto. El puerto entra en el estado de error-disabled de manera predeterminada. Cuando un puerto esta apagado y puesto en modo error-deshabilitado, no se envía ni se recibe tráfico a través de ese puerto.

Gracias



Universidad
Tecnológica
del Perú