VERSION 1

JULI , 2022

[PRAKTIKUM JARINGAN KOMPUTER]

IMPLEMENT PORT SECURITY DAN SWITCH SECURITY CONFIGURATION – MODUL 5

TIM PENYUSUN :

MAHAR FAIQURAHMAN, S.KOM, M.T

ALIF SYIFA ARSYILA

ARIEL BAGUS AR – RASYIID

PRESENTED BY: LAB - INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MALANG

[JARINGAN KOMPUTER]

PERSIAPAN MATERI

- Port Security
- VLAN
- DHCP
- ARP
- STP

TUJUAN

- Mahasiswa mampu implementasi Port Security.
- Mahasiswa mampu memahami serangan VLAN.
- Mahasiswa mampu memahami serangan DHCP.
- Mahasiswa mampu memahami serangan ARP.
- Mahasiswa mampu memahami serangan STP.

TARGET MODUL

- Melakukan konfigurasi DTP dan Native VLAN untuk mitigasi serangan VLAN.
- Melakukan konfigurasi DHCP Snooping untuk mitigasi serangan DHCP.
- Melakukan konfigurasi inspeksi ARP untuk mitigasi serangan ARP.
- Melakukan konfigurasi PortFast dan BPDU Guard untuk mitigasi serangan STP.

PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Latop
- Sistem operasi Windows/ Linux/ Mac OS
- Simulator Packet Tracer

MATERI POKOK

- **Implement Port Security**
  - **Secure Unused Ports**

    Perangkat Layer 2 dianggap sebagai tautan terlemah dalam infrastruktur keamanan perusahaan. Serangan Layer 2 adalah beberapa yang paling mudah digunakan oleh peretas tetapi ancaman ini juga dapat dimitigasi dengan beberapa solusi Layer 2 umum. Semua port switch (interface) harus diamankan sebelum switch digunakan untuk penggunaan produksi. Bagaimana port diamankan tergantung pada fungsinya.

    Metode sederhana yang digunakan banyak administrator untuk membantu mengamankan jaringan dari akses tidak sah adalah menonaktifkan semua port yang tidak digunakan pada switch. Misalnya, jika switch Catalyst 2960 memiliki 24 port dan ada tiga koneksi Fast Ethernet yang digunakan, ada baiknya untuk menonaktifkan 21 port yang tidak digunakan. Arahkan ke setiap port yang tidak digunakan dan terbitkan perintah shutdown IOS Cisco. Jika

port harus diaktifkan kembali di lain waktu, port dapat diaktifkan dengan perintah tanpa pematian.

Untuk mengonfigurasi rentang port, gunakan perintah **interface range**.

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

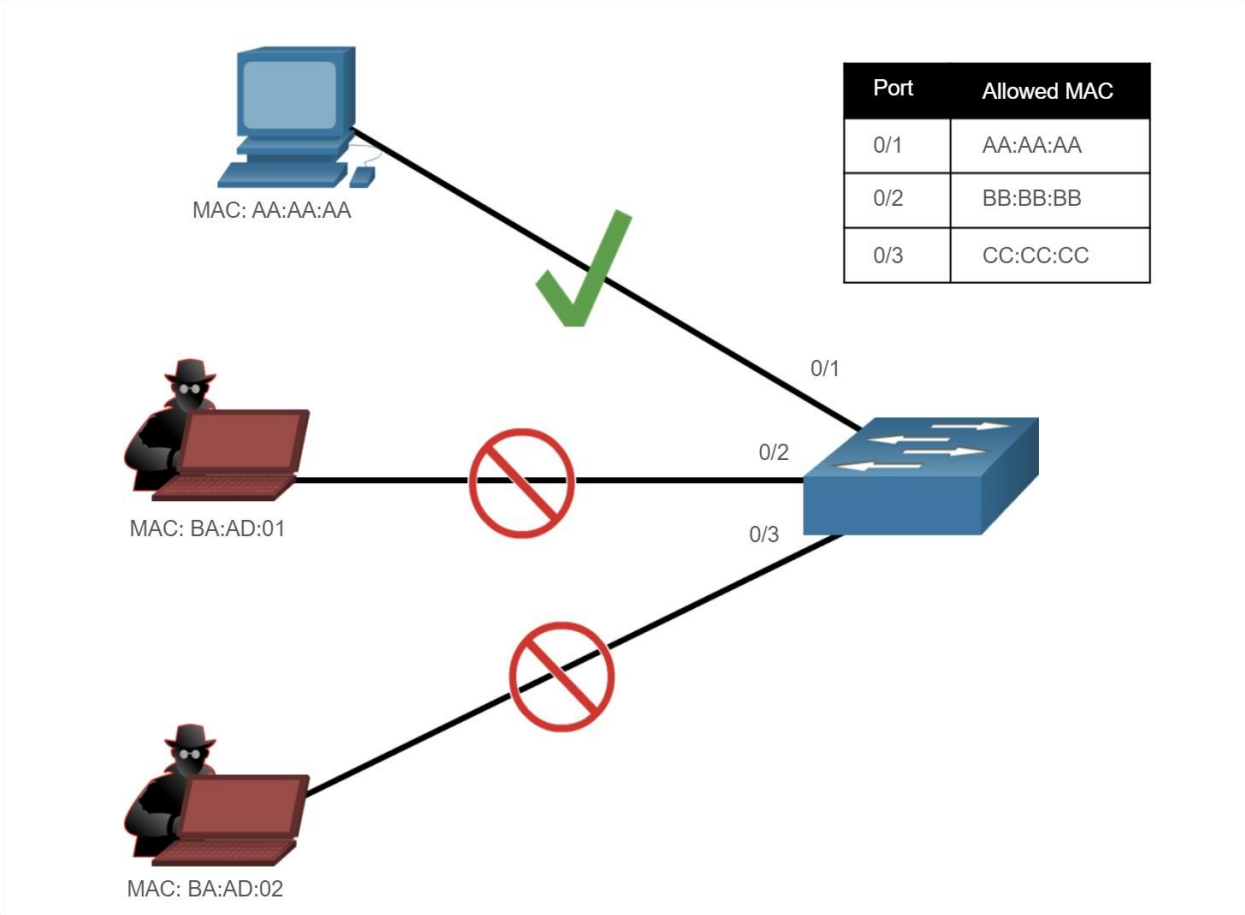
Misalnya, untuk mematikan port untuk Fa0/8 hingga Fa0/24 pada S1, Anda akan memasukkan perintah berikut.

```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
```

- **Mitigate MAC Address Table Attacks**

  Metode paling sederhana dan paling efektif untuk mencegah serangan luapan tabel alamat MAC adalah dengan mengaktifkan keamanan port. Keamanan port membatasi jumlah alamat MAC yang valid yang diizinkan pada port. Ini memungkinkan administrator untuk mengkonfigurasi alamat MAC secara manual untuk port atau mengizinkan switch untuk secara dinamis mempelajari sejumlah alamat MAC yang terbatas. Ketika port yang dikonfigurasi dengan keamanan port menerima frame, alamat MAC sumber frame dibandingkan dengan daftar alamat MAC sumber aman yang dikonfigurasi secara manual atau dipelajari secara dinamis pada port.

  Dengan membatasi jumlah alamat MAC yang diizinkan pada port ke satu, keamanan port dapat digunakan untuk mengontrol akses tidak sah ke jaringan, seperti yang ditunjukkan pada gambar.



- **Enable Port Security**

  Pemberitahuan dalam contoh, perintah port-security switchport ditolak. Ini karena keamanan port hanya dapat dikonfigurasi pada port akses yang dikonfigurasi secara manual atau port trunk yang dikonfigurasi secara manual. Secara default, port switch Layer 2 diatur ke dynamic auto (trunking on). Oleh karena itu, dalam contoh, port dikonfigurasi dengan perintah konfigurasi interface akses mode switchport.

  Catatan: Keamanan port trunk berada di luar lingkup kursus ini.

```
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#
```

Gunakan perintah **show port-security interface** untuk menampilkan pengaturan keamanan port saat ini untuk FastEthernet 0/1, seperti yang ditunjukkan dalam contoh. Perhatikan

bagaimana keamanan port diaktifkan, status port secure-down yang berarti tidak ada perangkat yang terpasang dan tidak ada pelanggaran yang terjadi, mode pelanggaran adalah Shutdown, dan bagaimana jumlah maksimum alamat MAC adalah 1. Jika perangkat terhubung ke port, status port switch akan menampilkan Secure-up dan switch akan secara otomatis menambahkan alamat MAC perangkat sebagai MAC aman. Dalam contoh ini, tidak ada perangkat yang terhubung ke port.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
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#
```

Catatan: Jika port aktif dikonfigurasi dengan perintah port-security switchport dan lebih dari satu perangkat tersambung ke port tersebut, port akan beralih ke status error-disabled. Kondisi ini dibahas kemudian dalam topik ini.

Setelah keamanan port diaktifkan, spesifik keamanan port lainnya dapat dikonfigurasi, seperti yang ditunjukkan dalam contoh.

```
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
```

- **Limit and Learn MAC Addresses**

  Untuk mengatur jumlah maksimum alamat MAC yang diizinkan pada port, gunakan perintah berikut :

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

  Nilai keamanan port default adalah 1. Jumlah maksimum alamat MAC aman yang dapat dikonfigurasi tergantung pada switch dan IOS. Dalam contoh ini, maksimum adalah 8192.

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

Switch dapat dikonfigurasikan untuk mempelajari alamat MAC di port aman dengan beberapa cara :

- **Manually Configured**
  Administrator mengkonfigurasi alamat MAC statis secara manual dengan menggunakan perintah berikut untuk setiap alamat MAC aman pada port:

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

- **Dynamically Learned**
  Ketika perintah **switchport port-security** dimasukkan, MAC sumber saat ini untuk perangkat yang terhubung ke port secara otomatis diamankan tetapi tidak ditambahkan ke konfigurasi startup. Jika switch di-boot ulang, port harus mempelajari ulang alamat MAC perangkat.
- **Dynamically Learned-Sticky**
  Administrator dapat mengaktifkan pengalih untuk secara dinamis mempelajari alamat MAC dan "menempelkan" mereka ke konfigurasi yang sedang berjalan dengan menggunakan perintah berikut :

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

Menyimpan konfigurasi yang berjalan akan melakukan alamat MAC yang dipelajari secara dinamis ke NVRAM.
Contoh berikut menunjukkan konfigurasi keamanan port lengkap untuk FastEthernet 0/1 dengan host yang terhubung ke port Fa0/1. Administrator menentukan maksimum 2 alamat MAC, secara manual mengkonfigurasi satu alamat MAC aman, dan kemudian mengkonfigurasi port untuk secara dinamis mempelajari alamat MAC aman tambahan hingga maksimum 2 alamat MAC aman. Gunakan **show port-security interface** dan perintah **show port-security address** untuk memverifikasi konfigurasi.

```
*Mar  1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
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      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
1    a41f.7272.676a    SecureSticky                Fa0/1        -
1    aaaa.bbbb.1234    SecureConfigured            Fa0/1        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max  Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Output dari perintah **show port-security interface** menunjukkan memverifikasi bahwa keamanan port diaktifkan, terdapat host yang terhubung ke port (yaitu, Secure-up), total 2 alamat MAC akan diizinkan, dan S1 telah mempelajari satu alamat MAC secara statis dan satu alamat MAC secara dinamis (yaitu, lengket). Output dari perintah **show port-security address** mencantumkan dua alamat MAC yang dipelajari.

- **Port Security Aging**
  Aging pada Keamanan port dapat digunakan untuk mengatur waktu aging untuk alamat aman statis dan dinamis pada port. Dua jenis penuaan didukung per port:
  - **Absolute** – The secure addresses on the port are deleted after the specified aging time.
  - **Inactivity** - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

Gunakan Aging untuk menghapus alamat MAC aman di port aman tanpa menghapus alamat MAC aman yang ada secara manual. Batas waktu Aging juga dapat ditingkatkan untuk memastikan alamat MAC aman tetap ada, bahkan saat alamat MAC baru ditambahkan. Aging alamat aman yang dikonfigurasi secara statis dapat diaktifkan atau dinonaktifkan berdasarkan per-port.

Gunakan perintah **switchport port-security aging** untuk mengaktifkan atau menonaktifkan penuaan statis untuk port aman, atau untuk mengatur waktu atau jenis penuaan.

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

Parameter untuk perintah dijelaskan dalam tabel.

Parameter	Description
static	Enable aging for statically configured secure addresses on this port.
time *time*	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Catatan: Alamat MAC ditampilkan sebagai 24 bit untuk kesederhanaan.

Contoh menunjukkan administrator mengonfigurasi jenis aging hingga 10 menit tidak aktif dan dengan menggunakan perintah **show port-security interface** untuk memverifikasi konfigurasi.

```
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-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

- **Port Security Violation Modes**
  Jika alamat MAC perangkat yang dilampirkan ke port berbeda dari daftar alamat aman, maka pelanggaran pada port terjadi. Secara default, port memasuki status error-disabled.
  Untuk mengatur mode pelanggaran keamanan port, gunakan perintah berikut :

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

Tabel berikut menunjukkan bagaimana switch bereaksi berdasarkan mode pelanggaran yang dikonfigurasi.

Security Violation Mode Descriptions

Mode	Description
shutdown (default)	The port transitions to the error-disabled state immediately, turns off the port LED, and sends a syslog message. It increments the violation counter. When a secure port is in the error-disabled state, an administrator must re-enable it by entering the shutdown and no shutdown commands.
restrict	The port drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. This mode causes the Security Violation counter to increment and generates a syslog message.

protect	This is the least secure of the security violation modes. The port drops packets with unknown MAC source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. No syslog message is sent.

Security Violation Mode Comparison

Violation Mode	Discards Offending Traffic	Sends Syslog Message	Increase Violation Counter	Shuts Down Port
Protect	Yes	No	No	No
Restrict	Yes	Yes	Yes	No
Shutdown	Yes	Yes	Yes	Yes

Contoh berikut menunjukkan administrator mengubah pelanggaran keamanan menjadi "membatasi". Output dari perintah **show port-security interface** adalah untuk mengkonfirmasi bahwa perubahan telah dilakukan.

```
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-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

- **Port in error-disabled State**

Apa yang terjadi ketika pelanggaran keamanan port dimatikan dan terjadi pelanggaran port? Port dimatikan secara fisik dan ditempatkan dalam status cacat kesalahan, dan tidak ada lalu lintas yang dikirim atau diterima pada port tersebut.

Dalam gambar, pelanggaran keamanan port diubah kembali ke pengaturan pematian default. Kemudian host dengan alamat MAC a41f.7272.676a terputus dan host baru dicolokkan ke Fa0/1.

Perhatikan bagaimana serangkaian pesan terkait keamanan port dibuat di konsol.

```
S1(config)# int fa0/1
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# end
S1#
*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1#
*Mar  1 00:24:32.829: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 00:24:32.838: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port
FastEthernet0/1.
*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S1#
```

Catatan: Protokol port dan status tautan diubah ke bawah dan LED port dimatikan.

Pada contoh, perintah **show interface** mengidentifikasi status port sebagai **error-disabled** Output dari perintah **show port-security** adalah menunjukkan status port sebagai Secure-shutdown alih-alih Secure-up. Pelanggaran Keamanan mengalami kenaikan menjadi 1.

```
S1# show interface fa0/1 | include down
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 1
S1#
```

Administrator harus menentukan apa yang menyebabkan pelanggaran keamanan. Jika perangkat yang tidak sah terhubung ke port aman, ancaman keamanan dihilangkan sebelum mengaktifkan kembali port.

Dalam contoh berikutnya, host pertama terhubung kembali ke Fa0/1. Untuk mengaktifkan kembali ports, pertama-tama gunakan perintah shutdown, lalu, gunakan perintah no shutdown untuk membuat port beroperasi, seperti yang ditunjukkan dalam contoh.

- **Verify Port Security**

  Setelah mengonfigurasi keamanan port pada switch, periksalah setiap interface untuk memverifikasi bahwa keamanan port telah diatur dengan benar, dan periksalah untuk memastikan bahwa alamat MAC statis telah dikonfigurasi dengan benar.

  - **Port Security for All Interfaces**

    Untuk menampilkan setelan keamanan port untuk switch, gunakan perintah show **port-security**. Contoh menunjukkan bahwa hanya satu port yang dikonfigurasi dengan perintah port-security switchport.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-------------------------------------------------------------------------
      Fa0/1             2            2                  0         Shutdown
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

- **Port Security for a Specific Interface**
  Gunakan perintah show port-security interface untuk melihat detail interface tertentu, seperti yang ditunjukkan sebelumnya dan dalam contoh ini.

```
S1# show port-security interface fastethernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 0
S1#
```

- **Verify Learned MAC Addresses**
  Untuk memverifikasi bahwa alamat MAC "menempel" ke konfigurasi, gunakan perintah show run seperti yang ditunjukkan dalam contoh FastEthernet 0/19.

```
S1# show run interface fa0/1
Building configuration...

Current configuration : 365 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a41f.7272.676a
 switchport port-security mac-address aaaa.bbbb.1234
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 switchport port-security
end

S1#
```

- **Verify Secure MAC Addresses**
  Untuk menampilkan semua alamat MAC aman yang dikonfigurasikan secara manual atau dipelajari secara dinamis pada semua interface switch, gunakan perintah show port-security address seperti yang ditunjukkan dalam contoh.

```
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    a41f.7272.676a    SecureSticky                  Fa0/1       -
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1       -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

- **Mitigate VLAN Attacks**
  - **VLAN Attacks Review**

    Rangkuman, serangan VLAN hopping dapat diluncurkan dengan salah satu dari tiga cara:
    - Spoofing pesan DTP dari host yang menyerang agar menyebabkan tombol masuk ke mode trunking. Dari sini, penyerang dapat mengirim lalu lintas yang ditandai dengan target VLAN, dan switch kemudian mengirimkan paket ke tujuan.
    - Memperkenalkan switch ““nakal”” dan mengaktifkan trunking. Penyerang kemudian dapat mengakses semua VLAN pada switch korban dari switch ““nakal””.

    Jenis serangan VLAN hopping lainnya adalah serangan double-tagging (atau double-encapsulated). Serangan ini memanfaatkan perangkat keras pada Sebagian.

  - **Steps to Mitigate VLAN Hopping Attacks**

    Gunakan langkah-langkah berikut untuk mengurangi serangan melompat VLAN:

    Langkah 1: Nonaktifkan negosiasi DTP (auto trunking) pada port non-trunking dengan menggunakan perintah konfigurasi switch port access interface.

    Langkah 2: Nonaktifkan port yang tidak digunakan dan letakkan di VLAN yang tidak digunakan.

    Langkah 3: Aktifkan link trunking secara manual pada port trunk dengan menggunakan perintah switchport mode trunk.

    Langkah 4: Nonaktifkan negosiasi DTP (auto trunking) pada port trunk dengan menggunakan perintah switchport nonegotiate.

    Langkah 5: Atur VLAN asli ke VLAN selain VLAN 1 dengan menggunakan perintah switchport trunk native vlan vlan_number.

    Misalnya, asumsikan hal berikut:
    - Port FastEthernet 0/1 hingga fa0/16 adalah port akses aktif.
    - Port FastEthernet 0/17 hingga 0/20 saat ini tidak sedang digunakan.
    - Port FastEthernet 0/21 hingga 0/24 adalah port trunk.

    VLAN hopping dapat dimitigasi dengan mengimplementasikan konfigurasi berikut.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

- Port FastEthernet 0/1 hingga 0/16 adalah port akses dan oleh karena itu trunk dinonaktifkan dengan secara eksplisit menjadikannya port akses.
- Port FastEthernet 0/17 hingga 0/20 adalah port yang tidak digunakan dan dinonaktifkan dan ditugaskan ke VLAN yang tidak digunakan.
- Port FastEthernet 0/21 hingga 0/24 adalah tautan trunk dan diaktifkan secara manual sebagai batang dengan DTP dinonaktifkan. VLAN asli juga diubah dari VLAN default 1 menjadi VLAN 999 yang tidak digunakan.

- **Mitigate DHCP Attacks**
  - **DHCP Attack Review**

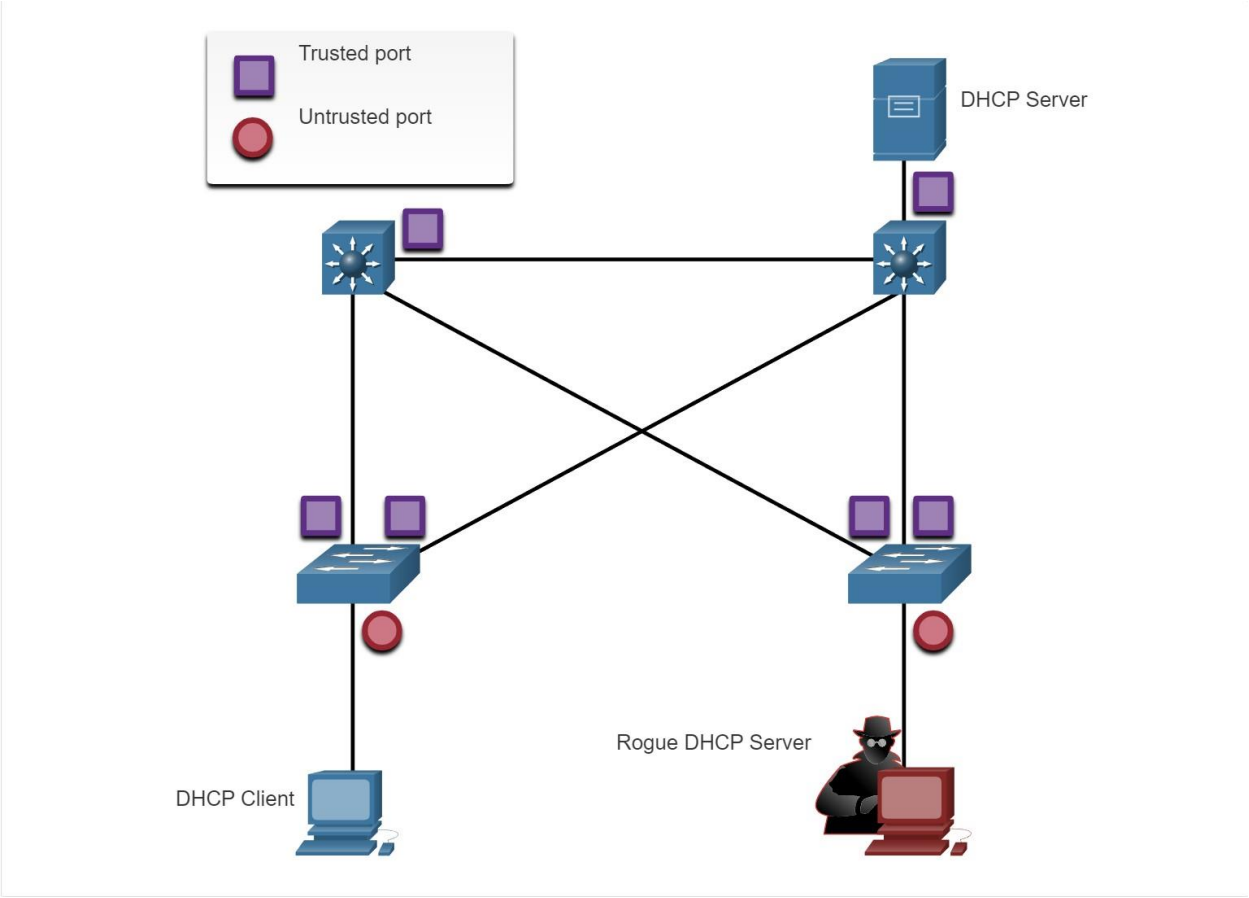
    Tujuan dari serangan starvation DHCP adalah untuk membuat Denial of Service (DoS) untuk menghubungkan klien. Serangan starvation DHCP membutuhkan alat serangan seperti Gobbler. Ingat bahwa serangan starvation DHCP dapat dimitigasi secara efektif dengan menggunakan keamanan port karena Gobbler menggunakan alamat MAC sumber unik untuk setiap permintaan DHCP yang dikirim.

    Namun, memitigasi serangan spoofing DHCP membutuhkan perlindungan lebih. Gobbler dapat dikonfigurasi untuk menggunakan alamat MAC interface aktual sebagai alamat Ethernet sumber, tetapi tentukan alamat Ethernet yang berbeda dalam muatan DHCP. Ini akan membuat keamanan port tidak efektif karena alamat MAC sumber akan sah. Serangan spoofing DHCP dapat dimitigasi dengan menggunakan DHCP snooping port yang tepercaya.

  - **DHCP Snooping**

    Snooping DHCP tidak bergantung pada alamat MAC sumber. Sebaliknya, snooping DHCP menentukan apakah pesan DHCP berasal dari sumber tepercaya atau tidak tepercaya yang dikonfigurasi secara administratif. Kemudian memfilter pesan DHCP dan membatasi tingkat lalu lintas DHCP dari sumber yang tidak tepercaya.

Perangkat di bawah kontrol administratif Anda, seperti switch, router, dan server, adalah sumber tepercaya. Perangkat apa pun di luar tembok api atau di luar jaringan Anda adalah sumber yang tidak tepercaya. Selain itu, semua port akses umumnya diperlakukan sebagai sumber yang tidak tepercaya. Angka tersebut menunjukkan contoh port terpercaya dan tidak tepercaya.



Perhatikan bahwa server DHCP “nakal” akan berada di port yang tidak tepercaya setelah memungkinkan snooping DHCP. Semua interface diperlakukan sebagai tidak tepercaya secara default. Interface tepercaya biasanya merupakan link trunk dan port yang terhubung langsung ke server DHCP yang sah. Interface ini harus dikonfigurasi secara eksplisit sebagai tepercaya.

Tabel DHCP dibuat yang menyertakan alamat MAC sumber perangkat pada port yang tidak tepercaya dan alamat IP yang ditetapkan oleh server DHCP ke perangkat tersebut. Alamat MAC dan alamat IP terikat bersama- sama. Oleh karena itu, tabel ini disebut tabel pengikatan snooping DHCP.

- **Steps to Implement DHCP Snooping**

  Gunakan langkah-langkah berikut untuk mengaktifkan snooping DHCP:

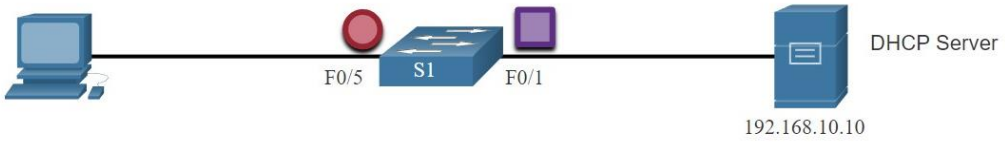
Langkah 1. Aktifkan snooping DHCP dengan menggunakan perintah konfigurasi global ip **dhcp snooping**.

Langkah 2. Pada port terpercaya, gunakan perintah konfigurasi ip dhcp snooping trust.

Langkah 3. Batasi jumlah pesan penemuan DHCP yang dapat diterima per detik pada port yang tidak tepercaya dengan menggunakan perintah konfigurasi **ip dhcp snooping limit rate**.

Langkah 4. Aktifkan snooping DHCP oleh VLAN, atau oleh berbagai VLAN, dengan menggunakan perintah konfigurasi global vlan **ip dhcp snooping**.

- **DHCP Snooping Configuration Example**
  Topologi referensi untuk contoh snooping DHCP ini ditunjukkan pada gambar. Perhatikan bahwa F0/5 adalah port yang tidak tepercaya karena terhubung ke PC. F0/1 adalah porta terpercaya karena tersambung ke peladen DHCP.



Berikut ini adalah contoh cara mengonfigurasi snooping DHCP pada S1. Perhatikan bagaimana snooping DHCP pertama kali diaktifkan. Kemudian interface hulu ke server DHCP secara eksplisit dipercaya. Selanjutnya, kisaran port FastEthernet dari F0/5 hingga F0/24 tidak dipercaya secara default, sehingga batas tarif diatur ke enam paket per detik. Akhirnya, snooping DHCP diaktifkan pada VLANS, 5,10,51, dan, 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Gunakan perintah exec istimewa show ip dhcp snooping untuk memverifikasi snooping DHCP dan show ip dhcp snooping binding untuk melihat klien yang telah menerima informasi DHCP, seperti yang ditunjukkan dalam contoh.

Catatan: Snooping DHCP juga diperlukan oleh Dynamic ARP Inspection (DAI), yang merupakan topik berikutnya.

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5    FastEthernet0/5
```

- **Mitigate ARP Attacks**
  - **Dynamic ARP Inspection**

    Dalam serangan ARP yang khas, aktor ancaman dapat mengirim permintaan ARP yang tidak diminta ke host lain di subnet dengan Alamat MAC aktor ancaman dan alamat IP gateway

default. Untuk mencegah spoofing ARP dan keracunan ARP yang dihasilkan, switch harus memastikan bahwa hanya Permintaan dan Balasan ARP yang valid yang disampaikan.
Inspeksi ARP Dinamis (DAI) memerlukan snooping DHCP dan membantu mencegah serangan ARP dengan :

- Tidak menyampaikan Permintaan ARP yang tidak valid atau gratifikasi ke port lain di VLAN yang sama.
- Mencegat semua Permintaan dan Balasan ARP pada port yang tidak tepercaya.
- Memverifikasi setiap paket yang disadap untuk pengikatan IP-ke-MAC yang valid.
- Menjatuhkan dan mencatat Permintaan ARP berasal dari sumber yang tidak valid untuk mencegah keracunan ARP.
- Menonaktifkan interface jika jumlah dai paket ARP yang dikonfigurasi terlampaui.

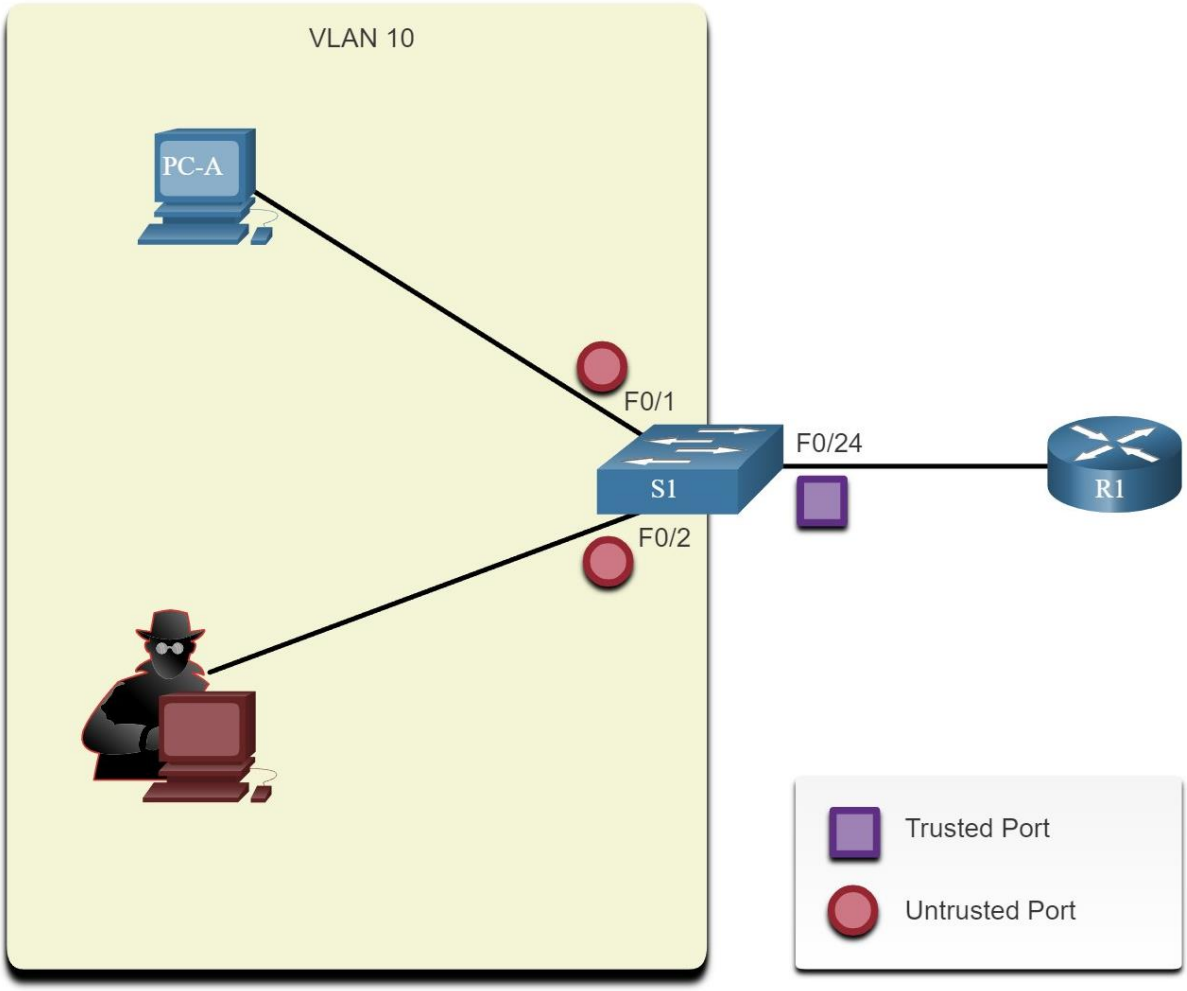
- **DAI Implementation Guidelines**

  Untuk mengurangi kemungkinan spoofing ARP dan keracunan ARP, ikuti pedoman implementasi DAI berikut:

  - Aktifkan snooping DHCP secara global.
  - Aktifkan snooping DHCP pada VLAN tertentu.
  - Aktifkan DAI pada VLAN terpilih.
  - Mengonfigurasi interface tepercaya untuk snooping DHCP dan inspeksi ARP.

  Umumnya disarankan untuk mengkonfigurasi semua port switch akses sebagai tidak tepercaya dan untuk mengkonfigurasi semua port uplink yang terhubung ke switch lain sebagai tepercaya.

  Contoh topologi dalam gambar mengidentifikasi port tepercaya dan tidak tepercaya.



- **DAI Configuration Example**

  Dalam topologi sebelumnya, S1 menghubungkan dua pengguna di VLAN 10. DAI akan dikonfigurasi untuk mengurangi serangan spoofing ARP dan keracunan ARP.

  Seperti yang ditunjukkan dalam contoh, snooping DHCP diaktifkan karena DAI memerlukan tabel pengikatan snooping DHCP untuk beroperasi. Selanjutnya, snooping DHCP dan inspeksi ARP diaktifkan untuk PC pada VLAN10. Port uplink ke router tepercaya, dan oleh karena itu, dikonfigurasi sebagai tepercaya untuk snooping DHCP dan inspeksi ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

DAI juga dapat dikonfigurasi untuk memeriksa tujuan atau alamat MAC dan IP sumber:

- MAC Destination - Memeriksa alamat MAC tujuan di header Ethernet terhadap alamat MAC target di isi ARP.
- MAC Source - Memeriksa alamat MAC sumber di header Ethernet terhadap alamat MAC pengirim di isi ARP.
- Alamat IP - Memeriksa isi ARP untuk alamat IP yang tidak valid dan tidak terduga termasuk alamat, dan semua alamat multicast IP.

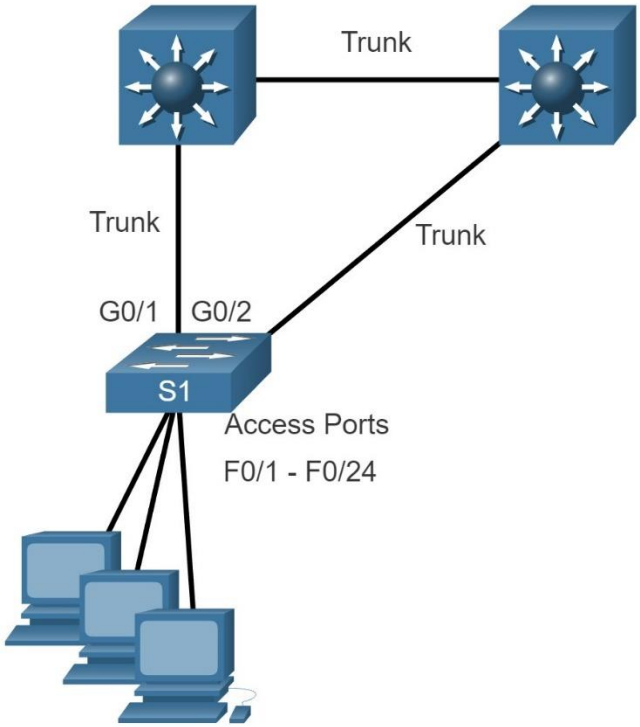
Perintah **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** global digunakan untuk mengonfigurasi DAI untuk membuang paket ARP saat alamat IP tidak valid. Ini dapat digunakan ketika alamat MAC di isi paket ARP tidak cocok dengan alamat yang ditentukan di header Ethernet. Perhatikan dalam contoh berikut bagaimana hanya satu perintah yang dapat dikonfigurasi. Oleh karena itu, memasukkan beberapa **ip arp inspection validate** perintah menimpa perintah sebelumnya. Untuk menyertakan lebih dari satu metode validasi, masukkan metode tersebut pada baris perintah yang sama seperti yang diperlihatkan dan diverifikasi dalam output berikut.

```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

- **Mitigate STP Attacks**
  - **PortFast and BPDU Guard**

    Ingat bahwa penyerang jaringan dapat memanipulasi Spanning Tree Protocol (STP) untuk melakukan serangan dengan spoofing root bridge dan mengubah topologi jaringan. Untuk mengurangi serangan manipulasi Spanning Tree Protocol (STP), gunakan PortFast and Bridge Protocol Data Unit (BPDU) Guard:
    - **PortFast** - PortFast segera membawa interface yang dikonfigurasi sebagai port akses ke status penerusan dari keadaan pemblokiran, melewati negara-negara mendengarkan dan belajar. Terapkan ke semua porta pengguna akhir. PortFast hanya boleh dikonfigurasi pada port yang terpasang pada perangkat akhir.
    - **BPDU Guard**- Penjaga BPDU segera melakukan kesalahan menonaktifkan pelabuhan yang menerima BPDU. Seperti PortFast, penjaga BPDU hanya boleh dikonfigurasi pada interface yang terpasang ke perangkat akhir.

    Dalam gambar, port akses untuk S1 harus dikonfigurasi dengan PortFast dan BPDU Guard.



- **Configure PortFast**
  PortFast melewati beberapa listening dan learning STP untuk meminimalkan waktu bahwa port akses harus menunggu STP bertemu. Jika PortFast diaktifkan pada port yang menghubungkan ke switch lain, ada risiko membuat loop pohon spanning.

  PortFast dapat diaktifkan pada interface dengan menggunakan perintah konfigurasi interface **spanning-tree portfast**. Atau, Portfast dapat dikonfigurasi secara global pada semua port akses dengan menggunakan perintah konfigurasi global **spanning-tree portfast default**.

  Untuk memverifikasi apakah PortFast diaktifkan secara global, Anda dapat menggunakan **show running-config | begin span** atau perintah **show spanning-tree summary**. Untuk memverifikasi apakah interface PortFast diaktifkan, gunakan perintah **show running-config interface**, seperti yang ditunjukkan dalam contoh berikut. Perintah **show spanning-tree** type/number **detail** juga dapat digunakan untuk verifikasi.

  Perhatikan bahwa ketika PortFast diaktifkan, pesan peringatan ditampilkan.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

- **Configure BPDU Guard**
  Meskipun PortFast diaktifkan, interface akan tetap mendengarkan BPDUs. BPDUs yang tidak terduga mungkin tidak disengaja, atau bagian dari upaya tidak real untuk menambahkan switch ke jaringan.

  Jika ada BPDUs yang diterima pada port yang diaktifkan BPDU Guard, port tersebut dimasukkan ke dalam status cacat kesalahan. Ini berarti port dimatikan dan harus diaktifkan kembali secara manual atau secara otomatis dipulihkan melalui perintah global BPDUGUARD **errdisable recovery cause bpduguard**.

  BPDU Guard dapat diaktifkan pada port dengan menggunakan perintah **spanning-tree bpduguard enable**. Atau, Gunakan perintah **spanning-tree portfast bpduguard default** untuk mengaktifkan penjaga BPDU secara global pada semua port yang mendukung PortFast.

Untuk menampilkan informasi tentang status spanning tree, gunakan perintah **show spanning-tree summary**. Dalam contoh, default PortFast dan BPDU Guard keduanya diaktifkan sebagai status default untuk port yang dikonfigurasi sebagai mode akses.

Catatan: Selalu aktifkan BPDU Guard di semua port yang mendukung PortFast.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

PRE-PRAKTIKUM

Tugas yang dilakukan yaitu mengerjakan aktivitas implementasi port security menggunakan paket tracer yang sudah di sediakan di tautan berikut ini :

https://bit.ly/jarkom2022UMM

Konfigurasi harus dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Setelah selesai melakukan konfigurasi pada File Packet Tracer, simpan hasil konfigurasi tersebut, kemudian ganti nama file Packet Tracer tersebut mengikuti format **Tugas-nama-nim.pka**.

Kemudian buatlah laporan tertulis sebagai bukti pemahaman kalian terhadap pekerjaan yang kalian kerjakan. Laporan ini akan di cek, apabila ada kesamaan kata-kata dan penjelasan, maka akan dilakukan pengurangan nilai (menghindari CTRL+C dan CTRL+V). Format laporan **Tugas-nama-nim.pdf**.

Tugas dikumpulkan di infotech.umm.ac.id pada bagian attachment **sebelum** berlangsungnya kegiatan praktikum.

Implement Port Security

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

INSTRUCTIONS

STEP 1: CONFIGURE PORT SECURITY

a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)# switchport port-security
```

b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

```
S1(config-if-range)# switchport port-security maximum 1
```

c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

```
S1(config-if-range)# switchport port-security mac-address sticky
```

d. Set the violation mode so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but anotification of the security violation is generated and packets from the unknown source are dropped.

```
S1(config-if-range)# switchport port-security violation restrict
```

e. Disable all the remaining unused ports. Use the **range** keyword to apply this configuration to all the portssimultaneously.

```
S1(config-if-range)# interface range f0/3 - 24 , g0/1 - 2
S1(config-if-range)# shutdown
```

Step 2: Verify Port Security

a. From **PC1**, ping **PC2**.

b. Verify that port security is enabled and the MAC addresses of **PC1** and **PC2** were

added to the runningconfiguration.

```
S1# show run | begin interface
```

c. Use port-security show commands to display configuration information.

```
S1# show port-security
S1# show port-security address
```

d. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

e. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the portconnected to **Rogue Laptop.**

f. Disconnect **PC2** and connect **Rogue Laptop** to F0/2, which is the port to which PC2 was originally connected.Verify that **Rogue Laptop** is unable to ping **PC1**.

g. Display the port security violations for the port to which **Rogue Laptop** is connected.

```
S1# show port-security interface f0/2
```

How many violations have occurred?

h. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.

Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?

PRAKTIKUM

Download file Packet Tracer pada link di bawah ini :

https://bit.ly/jarkom2022UMM

Praktikum dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Praktikum akan dilaksanakan secara **live configuration**, yang akan dilakukan secara **real time** pada saat jam praktikum dilaksanakan. Jadi tolong dipersiapkan dan dipelajari dengan sungguh-sungguh agar tidak menghambat kelancaran jalannya praktikum. Terimakasih.

Switch Security Configuration

VLAN Table

Switch	VLAN Number	VLAN Name	Port Membership	Network
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	None
	999	BlackHole	All unused	None

SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	None	None
	999	BlackHole	All unused	None

Objectives

Part 1 : Create a Secure Trunk

Part 2 : Secure Unused Trunk

Part 3 : Implement Port Security

Part 4 : Enable DHCP Snooping

Part 5 : Conifigure Rapid PVST PortFast and BPDU Guard

Background

You are enhancing security on two access switches in a partially configured network. You will implement the range ofsecurity measures that were covered in this module according to the requirements below. Note that routing has beenconfigured on this network, so connectivity between hosts on different VLANs should function when completed.

INSTRUCTIONS

STEP 1: Create a Secure Trunk.

a. Connect the G0/2 ports of the two access layer switches.

b. Configure ports G0/1 and G0/2 as static trunks on both switches.

c. Disable DTP negotiation on both sides of the link.

d. Create VLAN 100 and give it the name Native on both switches.

e. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

STEP 2: SECURE UNUSED SWITCHPORTS.

a. Shutdown all unused switch ports on SW-1.

b. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.

c. Move all unused switch ports to the BlackHole VLAN.

STEP 3: IMPLEMENT PORT SECURITY.

a. Activate port security on all the active access ports on switch SW-1.

b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.

c. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.

d. Configure each active access port so that it will automatically add the MAC addresses learned on the port to therunning configuration.

e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum,generate a Syslog entry, but not disable the ports.

STEP 4: CONFIGURE DHCP SNOOPING.

a. Configure the trunk ports on SW-1 as trusted ports.

b. Limit the untrusted ports on SW-1 to five DHCP packets per second.

c. On SW-2, enable DHCP snooping globally and for VLANs 10, 20 and 99.

Note: The DHCP snooping configuration may not score properly in Packet Tracer.

STEP 5: CONFIGURE PORTFAST, AND BPDU GUARD.

a. Enable PortFast on all the access ports that are in use on SW-1.

b. Enable BPDU Guard on all the access ports that are in use on SW-1.

c. Configure SW-2 so that all access ports will use PortFast by default.

RUBRIK PENILAIAN

Pemahaman Materi	10%
Pre-praktikum	20%
Praktikum	70%