VERSI 2.0

SEPTEMBER 2025

PRAKTIKUM JARINGAN KOMPUTER

MODUL 5 MATERI PRAKTIKUM - IMPLEMENTASI PORT SECURITY DAN KONFIGURASI SWITCH SECURITY

DISUSUN OLEH:

Ir. Mahar Faiqurahman, S.Kom., M.T.

Taufiq Ramadhan

Sutrisno Adit Pratama

TIM LABORATORIUM INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MALANG

PENDAHULUAN

TUJUAN

1. Mahasiswa mampu implementasi Port Security
2. Mahasiswa mampu memahami serangan Vlan
3. Mahasiswa mampu memahami serangan DHCP
4. Mahasiswa mampu memahami serangan ARP
5. Mahasiswa mampu memahami serangan STP

TARGET MODUL

1. Melakukan konfigurasi DTP dan Native VLAN untuk mitigasi serangan Vlan
2. Melakukan konfigurasi DHCP Snooping untuk mitigasi serangan DHCP
3. Melakukan konfigurasi inspeksi ARP untuk mitigasi serangan ARP
4. Melakukan konfigurasi PortFast dan BPDU Guard untuk mitigasi serangan STP

PERSIAPAN MATERI

1. Port Security
2. Vlan
3. DHCP
4. ARP
5. STP

PERSIAPAN SOFTWARE DAN HARDWARE

1. Komputer/Laptop
2. Sistem operasi Windows/ Linux/ MacOS
3. Simulator Packet Tracer - https://bit.ly/jarkom_2025_umm

KEYWORDS

Security, bpdu, vlan attack, stp, arp

DAFTAR ISI

MATERI POKOK

Mengimplementasikan Port Security

Mengamankan Port yang Tidak Digunakan

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 jalankan perintah shutdown pada IOS Cisco. Jika port harus diaktifkan kembali di lain waktu, port dapat diaktifkan dengan perintah no shutdown.

Untuk mengkonfigurasi 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)#
```

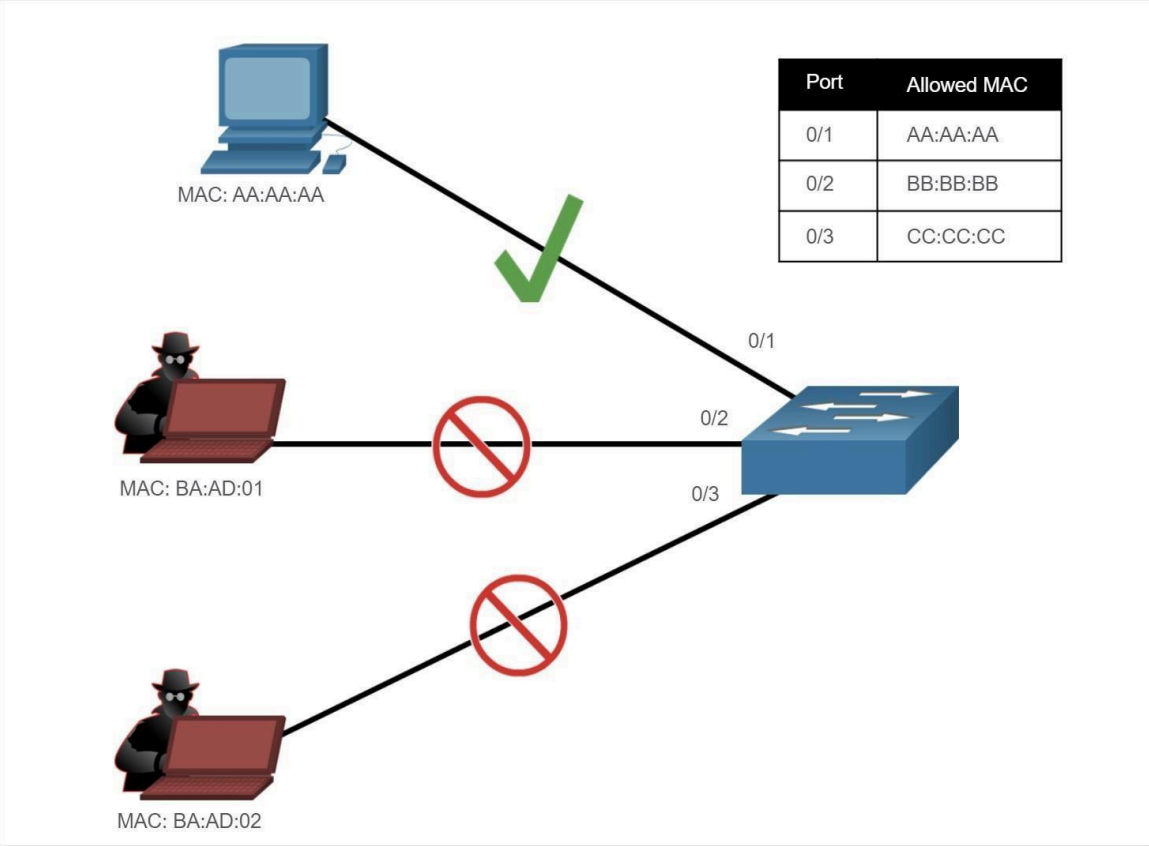
Mitigasi dari Serangan Mac Address

Metode paling sederhana dan efektif untuk mencegah MAC flooding attack adalah dengan mengaktifkan fitur keamanan port (port security) pada switch. Fitur ini bekerja dengan cara membatasi jumlah alamat MAC yang diizinkan pada sebuah port. Administrator dapat memilih salah satu dari dua cara:

- Statis: Mengkonfigurasi alamat MAC tertentu secara manual untuk setiap port.
- Dinamis: Mengizinkan switch untuk "mempelajari" satu atau beberapa alamat MAC pertama yang terhubung, lalu menolak sisanya.

Ketika sebuah port dengan keamanan aktif menerima data (frame), switch akan membandingkan alamat MAC sumber dari data tersebut dengan daftar alamat MAC yang sudah diizinkan. Jika alamat MAC tersebut tidak ada dalam daftar, switch akan segera mengambil tindakan pengamanan, seperti memblokir atau mematikan port tersebut.

Seperti yang ditunjukkan pada gambar, fitur keamanan port dapat mencegah akses tidak sah ke jaringan dengan membatasi setiap port agar hanya terhubung ke satu alamat MAC saja.



Port	Allowed MAC
0/1	AA:AA:AA
0/2	BB:BB:BB
0/3	CC:CC:CC

Mengaktifkan Port Security

Pada contoh berikut, perintah switchport port-security ditolak oleh sistem. Hal ini terjadi karena fitur keamanan port (port security) hanya bisa diaktifkan pada port yang modenya diatur secara manual, baik sebagai port access maupun port trunk. Secara default, port pada switch Layer 2 berada dalam mode dynamic auto. Untuk mengatasi masalah ini, port tersebut harus diubah modenya menjadi mode akses terlebih dahulu menggunakan perintah `switchport mode access`. Setelah itu, perintah `switchport port-security` akan dapat diterima.

Catatan: Pembahasan tentang keamanan port trunk berada di luar cakupan materi 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, misalnya untuk antarmuka FastEthernet 0/1. Seperti yang ditunjukkan pada contoh, perhatikan beberapa informasi penting berikut:

- Port Security: Statusnya `Enabled` (Aktif).
- Violation Mode: Mode pelanggaran diatur ke `Shutdown`. Artinya, port akan mati jika terjadi pelanggaran.
- Max MAC Addresses: Jumlah maksimum alamat MAC yang diizinkan adalah `1`.
- Port Status: Statusnya `Secure-down`. Ini menunjukkan bahwa port saat ini aman, tidak ada pelanggaran yang terjadi, dan belum ada perangkat yang terhubung.

Jika nanti ada perangkat yang terhubung, status port akan otomatis berubah menjadi `Secure-up`, dan switch akan "mempelajari" alamat MAC perangkat tersebut sebagai satu-satunya MAC yang sah.

```
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 sebuah port telah diaktifkan dengan perintah `switchport port-security` dan terdeteksi ada lebih dari satu perangkat yang terhubung, maka port tersebut akan beralih ke status error-disabled (dinonaktifkan karena ada kesalahan). Kondisi ini akan kita bahas lebih lanjut nanti.

Setelah fitur keamanan port diaktifkan, Anda dapat melanjutkan untuk mengkonfigurasi pengaturan yang lebih spesifik, seperti yang ditunjukkan pada 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
```

Mengatur Batas Maksimum Mac Address

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

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

Secara default, jumlah maksimum alamat MAC yang diizinkan untuk keamanan port adalah satu. Nilai maksimum ini dapat diubah dan bervariasi tergantung pada jenis switch dan versi IOS yang digunakan. Pada contoh ini, batas maksimalnya adalah 8.192 alamat MAC.

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

Sebuah switch dapat dikonfigurasi untuk mempelajari alamat MAC pada port aman melalui metode-metode berikut:

- **Dikonfigurasi secara manual**
  Untuk mengkonfigurasi alamat MAC secara statis pada sebuah port, administrator dapat menggunakan perintah berikut:

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

- **Dipelajari secara Dinamis (Dynamically Learned)**
  Saat perintah `switchport port-security` diaktifkan, switch akan secara otomatis mempelajari dan mengamankan alamat MAC dari perangkat yang sedang terhubung ke port. Namun, alamat MAC ini tidak disimpan ke dalam konfigurasi awal (startup configuration). Artinya, jika switch di-restart, port harus "mempelajari ulang" alamat MAC perangkat tersebut.
- **Dinamis dan tetap (Dynamically Learned-Sticky)**
  Administrator dapat mengaktifkan mode ini agar switch tidak hanya mempelajari alamat MAC secara dinamis, tetapi juga menyimpannya secara permanen ke dalam konfigurasi yang sedang berjalan (running configuration). Untuk melakukannya, gunakan perintah berikut:

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

  Alamat MAC yang dipelajari dengan mode "sticky" akan disimpan secara permanen ke NVRAM jika Anda menyimpan konfigurasi yang sedang berjalan (running configuration).

Contoh berikut menunjukkan konfigurasi keamanan port secara lengkap untuk interface FastEthernet 0/1. Dalam skenario ini, administrator ingin:

1. **Menetapkan batas maksimum dua alamat MAC pada port.**
2. **Mengonfigurasi satu alamat MAC secara manual (statis).**
3. **Mengizinkan port untuk mempelajari satu alamat MAC tambahan secara dinamis (mode sticky) hingga batas maksimal dua tercapai.**

Untuk memverifikasi konfigurasi tersebut, gunakan perintah `show port-security interface` dan `show port-security address`.

```
*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#
```

Hasil dari perintah `show port-security interface` memverifikasi beberapa hal berikut:

- Fitur keamanan port aktif (`Port Security: Enabled`).
- Ada perangkat yang terhubung ke port (`Port Status: Secure-up`).
- Batas maksimum alamat MAC yang diizinkan adalah dua.
- Switch S1 telah mempelajari satu alamat MAC secara statis dan satu alamat MAC secara dinamis (sticky).

Sementara itu, perintah `show port-security address` menampilkan daftar kedua alamat MAC yang telah dipelajari tersebut.

Port Security Aging

Fitur aging dalam keamanan port digunakan untuk mengatur batas waktu (kadaluarsa) bagi alamat MAC yang telah diamankan, baik yang dikonfigurasi secara statis maupun yang dipelajari secara dinamis. Terdapat dua jenis metode aging yang didukung:

- Absolute: Semua alamat MAC aman pada port akan dihapus secara otomatis setelah waktu yang ditentukan tercapai, tidak peduli aktif atau tidaknya alamat tersebut.
- Inactivity: Alamat MAC aman pada port hanya akan dihapus jika alamat tersebut tidak aktif (tidak mengirimkan data) selama waktu yang telah ditentukan.

Fitur ini berguna untuk menghapus alamat MAC lama secara otomatis tanpa perlu melakukannya secara manual. Anda bisa mengatur waktu aging agar alamat MAC yang jarang digunakan bisa dihapus, sehingga memberi ruang bagi perangkat baru untuk terhubung.
Untuk mengaktifkan, menonaktifkan, atau mengatur jenis dan waktu aging, gunakan perintah `switchport port-security aging`.

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

Parameter yang digunakan dalam perintah di atas dijelaskan dalam tabel berikut:

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: Untuk menyederhanakan contoh, alamat MAC hanya ditampilkan dalam format 24-bit.
Pada contoh berikut, administrator mengkonfigurasi fitur aging dengan metode inactivity selama 10 menit. Konfigurasi tersebut kemudian diverifikasi menggunakan perintah `show port-security interface`.

```
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#
```

Mode Violation pada Port Security

Pelanggaran keamanan port terjadi jika alamat MAC dari perangkat yang terhubung tidak cocok dengan daftar alamat MAC yang telah diamankan. Secara default, port yang mengalami pelanggaran akan langsung masuk ke status error-disabled. Untuk mengubah tindakan yang akan diambil saat terjadi pelanggaran, 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)	Ketika pelanggaran terjadi, port akan langsung masuk ke status **error-disabled**, yang ditandai dengan matinya lampu LED port dan dikirimkannya pesan notifikasi (syslog). Selain itu, penghitung jumlah pelanggaran juga akan bertambah. Untuk mengaktifkan kembali port yang berada dalam status ini, seorang administrator harus mengintervensi secara manual dengan

	mengeluarkan perintah `shutdown` diikuti oleh perintah `no shutdown`.
restrict	Dalam mode ini, port akan menjatuhkan (drop) semua paket dari alamat MAC yang tidak dikenal. Tindakan ini akan terus berlanjut sampai Anda menambah batas maksimum alamat MAC atau menghapus beberapa alamat yang sudah tersimpan. Selain itu, setiap paket yang dijatuhkan akan menambah penghitung pelanggaran dan memicu pengiriman pesan notifikasi (syslog).
protect	Ini merupakan mode pelanggaran yang paling tidak aman karena port akan menjatuhkan semua paket dari alamat MAC yang tidak dikenal secara diam-diam, tanpa mengirimkan notifikasi syslog apa pun. Port akan terus melakukan ini sampai Anda menambah batas maksimum alamat MAC atau menghapus beberapa alamat yang sudah ada.

Security Violation Mode Comparison

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

Contoh berikut menunjukkan administrator mengubah violation security menjadi “restrict". 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 Saat Mode Pelanggaran "Shutdown" Aktif? Ketika mode pelanggaran keamanan diatur ke shutdown dan terjadi pelanggaran, port tersebut akan:

1. Langsung masuk ke status error-disabled.
2. Dimatikan secara fisik (lampu LED port akan mati).
3. Berhenti mengirim dan menerima semua lalu lintas data.
4. Mencatat serangkaian pesan notifikasi di konsol.

Pada gambar berikut, mode pelanggaran untuk port Fa0/1 diatur kembali ke `shutdown` (default). Kemudian, skenario berikut terjadi:

```
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: Status protokol dan tautan port akan berubah menjadi `down`, yang secara fisik ditandai dengan matinya lampu LED port tersebut.
Untuk memverifikasi kondisi ini dapat dilakukan melalui beberapa perintah:

- Perintah `show interface` akan menampilkan status port sebagai error-disabled.
- Perintah `show port-security interface` akan menampilkan statusnya sebagai Secure-shutdown (bukan `Secure-up` seperti saat kondisi normal).
- Penghitung `Security Violation Count` akan bertambah 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 menyelidiki penyebab terjadinya pelanggaran keamanan. Jika port dimatikan karena terhubung dengan perangkat yang tidak sah, maka ancaman tersebut harus diatasi terlebih dahulu sebelum mengaktifkan kembali portnya.

Verifikasi Port Security

Setelah selesai mengonfigurasi, Anda harus selalu memverifikasi setiap antarmuka (interface) untuk memastikan keamanan port dan alamat MAC statis telah diatur dengan benar.

- Memeriksa untuk semua interface
  Untuk menampilkan ringkasan pengaturan keamanan port di semua antarmuka pada switch, gunakan perintah `show port-security`. Pada contoh berikut, output dari

perintah ini menunjukkan bahwa keamanan port hanya aktif pada satu antarmuka saja.

```
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#
```

- **Memeriksa pada interface tertentu**
  Untuk melihat detail konfigurasi pada satu interface tertentu, gunakan perintah `show port-security interface`.

```
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#
```

- **Verifikasi learned Mac Addresses**
  Untuk memverifikasi bahwa alamat MAC dalam mode "sticky" telah tersimpan ke dalam konfigurasi, gunakan perintah `show run interface fa0/1` seperti yang ditunjukkan pada contoh untuk antarmuka 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#
```

- **Verifikasi Semua Alamat MAC Aman**
  Untuk menampilkan semua alamat MAC yang telah diamankan—baik yang dikonfigurasi secara manual maupun yang dipelajari secara dinamis—di seluruh antarmuka switch, gunakan perintah `show port-security address` seperti yang ditunjukkan pada 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#
```

Mitigasi dari Vlan Attack

Vlan Attacks Review

VLAN hopping **adalah serangan yang memungkinkan penyerang mengirim lalu lintas dari satu VLAN ke VLAN lain tanpa melalui router. Serangan ini dapat dilancarkan dengan tiga metode utama:**

1. **DTP Spoofing**
   Penyerang mengirimkan pesan DTP (Dynamic Trunking Protocol) palsu untuk menipu switch agar mengubah port biasa menjadi port *trunk*. Setelah berhasil, penyerang dapat mengirimkan paket ke VLAN target mana pun, dan switch akan meneruskannya.
2. **Rogue Switch**

Penyerang menghubungkan switch miliknya ke jaringan dan mengaktifkan *trunking*. Dengan cara ini, switch penyerang dapat mengakses semua VLAN yang ada pada switch korban.

3. Double-Tagging
   Penyerang yang terhubung pada *native VLAN* menambahkan dua label VLAN pada paket. Switch pertama akan melepas label terluar (native VLAN) dan meneruskan paket. Switch kedua akan membaca label dalam dan mengirimkannya ke VLAN target, sehingga berhasil melompati batasan VLAN.

Langkah-langkah mitigasi serangan Vlan Hopping

Gunakan langkah-langkah berikut untuk mengamankan jaringan Anda dari serangan *VLAN hopping*:

1. Matikan DTP pada Port Akses: Nonaktifkan negosiasi *auto-trunking* (DTP) pada semua port yang tidak seharusnya menjadi *trunk*. (`switchport mode access`)
2. Amankan Port yang Tidak Digunakan: Matikan semua port yang tidak terpakai dan pindahkan ke VLAN "hitam" atau VLAN yang tidak digunakan.
   `shutdown`
   `switchport access vlan <vlan_tidak_terpakai>`
3. Konfigurasi Trunk secara Manual: Atur port yang memang berfungsi sebagai *trunk* secara manual. (`switchport mode trunk`)
4. Matikan DTP pada Port Trunk: Nonaktifkan negosiasi DTP bahkan pada port yang sudah diatur sebagai *trunk* untuk mencegah manipulasi. (`switchport nonegotiate`)
5. Ubah Native VLAN: Jangan gunakan VLAN 1 (default) sebagai *native VLAN*. Pindahkan ke VLAN lain yang tidak digunakan untuk data pengguna. (`switchport trunk native vlan <vlan_selain_1>`)

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.

Mitigasi dari DHCP attacks

DHCP attack review

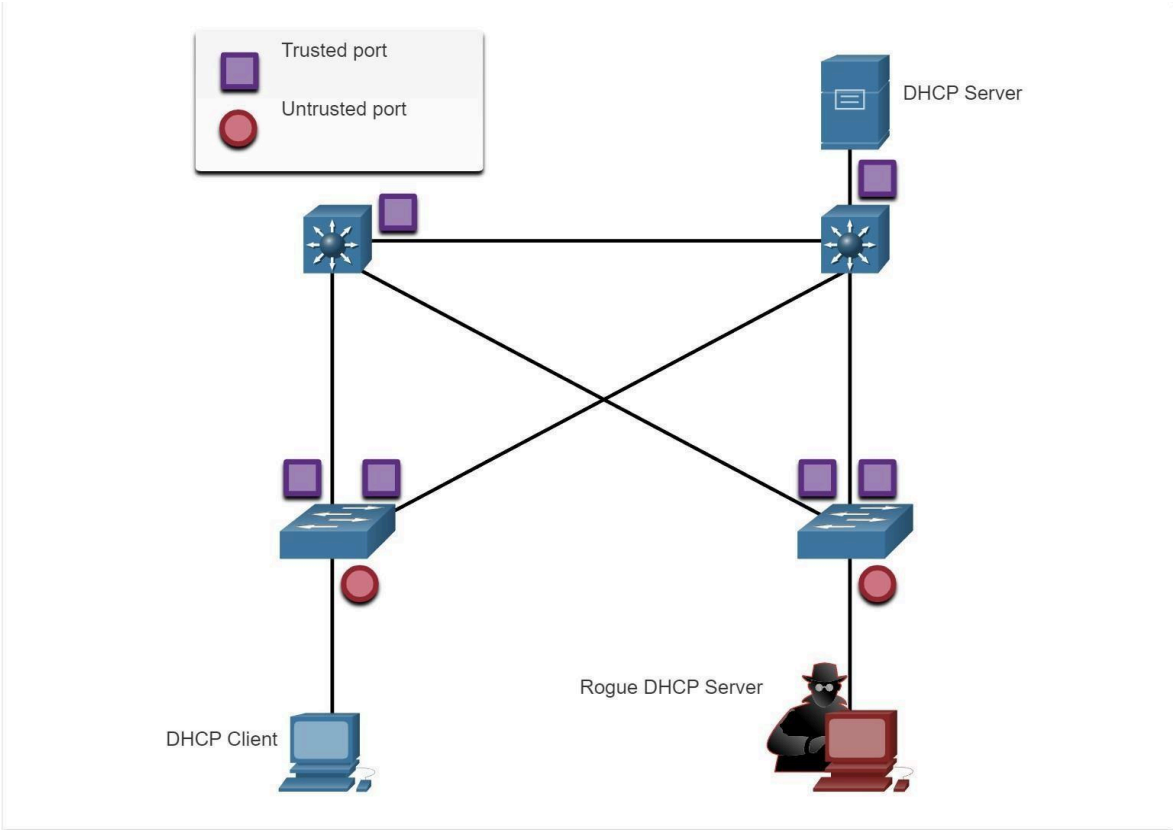
1. Serangan DHCP Starvation
   Tujuan utama dari serangan DHCP Starvation adalah menciptakan kondisi *Denial of Service* (DoS) yang menyebabkan klien baru tidak bisa mendapatkan alamat IP. Serangan ini biasanya menggunakan alat seperti Gobbler untuk membanjiri server DHCP dengan permintaan palsu.
   Serangan ini dapat dimitigasi secara efektif dengan fitur keamanan port (port security). Karena Gobbler menggunakan alamat MAC sumber yang unik untuk setiap permintaan, keamanan port akan segera memblokir port penyerang setelah batas alamat MAC terlampaui.
2. Serangan DHCP Spoofing
   Mitigasi untuk serangan DHCP Spoofing memerlukan perlindungan yang lebih canggih. Dalam serangan ini, penyerang bisa menggunakan alamat MAC aslinya (yang sah di mata keamanan port), tetapi menyisipkan alamat MAC palsu di dalam paket DHCP. Hal ini membuat keamanan port tidak efektif. Serangan DHCP Spoofing dapat dimitigasi dengan menggunakan fitur DHCP Snooping, yang akan memvalidasi pesan DHCP dan hanya mengizinkan pesan dari port yang terpercaya.

DHCP Snooping

Fitur ini tidak bergantung pada alamat MAC sumber. Sebaliknya, DHCP snooping bekerja dengan membedakan antara sumber yang terpercaya (trusted) dan tidak terpercaya (untrusted).

- Sumber Terpercaya: Perangkat di bawah kendali administratif, seperti switch, router, dan server DHCP resmi.
- Sumber Tidak Terpercaya: Semua perangkat lain di luar jaringan Anda, termasuk semua port akses yang terhubung ke pengguna akhir.

DHCP Snooping akan memfilter dan membatasi lalu lintas DHCP yang berasal dari sumber tidak terpercaya untuk mencegah serangan.



Setelah DHCP snooping diaktifkan, semua interface secara default dianggap tidak terpercaya (untrusted). Ini berarti server DHCP palsu (*rogue*) yang terhubung ke port akses biasa akan otomatis diblokir. Interface yang harus dikonfigurasi secara manual sebagai terpercaya (trusted) hanyalah port yang terhubung ke perangkat jaringan yang sah, seperti:

- **Link *trunk* yang menuju ke switch lain.**
- **Port yang terhubung langsung ke server DHCP resmi.**

DHCP snooping juga membuat sebuah tabel yang disebut binding table. Tabel ini mencatat dan mengikat alamat MAC dengan alamat IP yang diberikan oleh server DHCP resmi pada setiap port yang tidak terpercaya. Ini memastikan bahwa setiap perangkat hanya menggunakan alamat IP yang telah ditetapkan untuknya.

Langkah-langkah implementasi DHCP Snooping

Berikut adalah empat langkah untuk mengaktifkan DHCP Snooping pada switch:

1. **Langkah pertama adalah mengaktifkan fitur DHCP Snooping untuk seluruh switch. (`ip dhcp snooping`)**
2. **Tentukan port mana yang terhubung ke server DHCP resmi atau switch lain sebagai port yang terpercaya. (`ip dhcp snooping trust`)**
3. **Untuk mencegah serangan *starvation*, batasi jumlah pesan permintaan DHCP yang bisa diterima per detik pada port yang tidak terpercaya (port akses). (`ip dhcp snooping limit rate <jumlah_pesan_per_detik>`)**

4. Terakhir, tentukan pada VLAN mana saja fitur DHCP Snooping ini akan diberlakukan. (`ip dhcp snooping vlan <nomor_vlan>`)

Contoh konfigurasi DHCP Snooping

Topologi pada gambar di bawah ini digunakan sebagai referensi untuk contoh konfigurasi DHCP snooping. Port F0/5 dianggap tidak terpercaya (untrusted) karena terhubung ke PC pengguna. Port F0/1 dianggap terpercaya (trusted) karena terhubung langsung ke server DHCP.

Berikut adalah contoh langkah-langkah untuk mengonfigurasi DHCP snooping pada switch S1:

1. DHCP snooping diaktifkan secara global untuk seluruh switch.
2. Interface yang mengarah ke server DHCP, yaitu F0/1, secara eksplisit ditetapkan sebagai terpercaya (trusted).
3. Untuk semua port yang tidak terpercaya (F0/5 hingga F0/24), ditetapkan batas penerimaan paket DHCP sebanyak 6 paket per detik untuk mencegah serangan.
4. Terakhir, fitur DHCP snooping diterapkan pada VLAN 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#
```

Untuk memverifikasi konfigurasi DHCP snooping, gunakan dua perintah berikut:

1. `show ip dhcp snooping`
   Perintah ini digunakan untuk memverifikasi apakah DHCP snooping sudah aktif dan pada port mana saja fitur ini berjalan.
2. `show ip dhcp snooping binding`

Perintah ini digunakan untuk melihat tabel pengikat (binding table), yang berisi daftar klien beserta alamat IP dan MAC yang telah ditetapkan oleh server DHCP.

Catatan: Fitur DHCP Snooping merupakan prasyarat agar Dynamic ARP Inspection (DAI), topik kita berikutnya, dapat berfungsi.

```
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
```

Mitigasi dari ARP Attacks

Dynamic ARP Inspection (DAI)

Dalam serangan ARP, seorang penyerang bisa mengirimkan balasan ARP palsu untuk mengelabui host lain agar lalu lintasnya dialihkan melalui perangkat penyerang. Untuk mencegah serangan seperti ini (dikenal sebagai ARP spoofing atau ARP poisoning), switch harus bisa memastikan bahwa hanya paket ARP yang valid yang diteruskan. Fitur Dynamic ARP Inspection (DAI) adalah solusinya. Fitur ini bergantung pada binding table yang dibuat oleh DHCP Snooping untuk mencegah serangan ARP.

DAI membantu mengamankan jaringan dengan cara:

1. Tidak meneruskan balasan ARP yang mencurigakan ke port lain dalam VLAN yang sama.
2. Mencegat semua permintaan dan balasan ARP pada port yang tidak terpercaya (*untrusted*).
3. Memverifikasi setiap paket ARP yang dicegat dengan binding table DHCP Snooping untuk memastikan kecocokan antara alamat IP dan MAC.
4. Drop paket ARP yang berasal dari sumber tidak valid untuk mencegah *ARP poisoning*.

5. Mematikan interface jika jumlah paket ARP yang tidak valid melebihi batas yang telah dikonfigurasi.

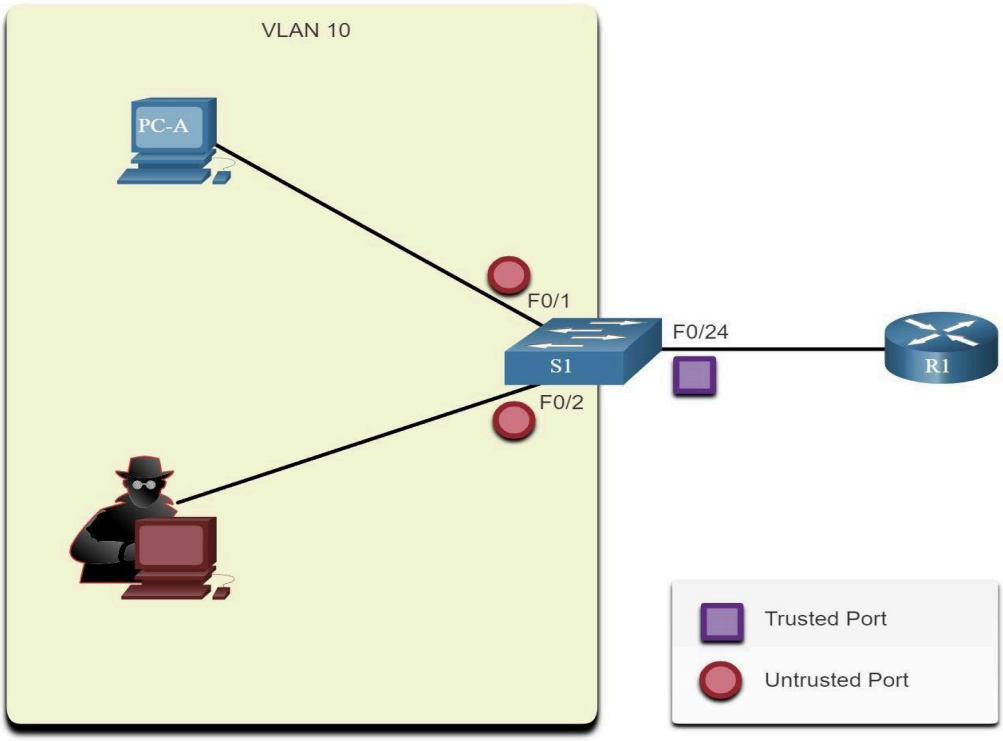
Panduan Implementasi DAI

Untuk mencegah serangan *ARP spoofing* dan *ARP poisoning*, ikuti panduan implementasi Dynamic ARP Inspection (DAI) berikut:

1. Aktifkan DHCP Snooping secara global.
2. Terapkan DHCP Snooping pada VLAN yang diinginkan.
3. Aktifkan DAI pada VLAN yang sama.
4. Konfigurasikan interface yang terpercaya (trusted) untuk DHCP Snooping dan DAI.

Umumnya, praktik terbaik yang disarankan adalah mengkonfigurasi semua port akses (yang terhubung ke pengguna) sebagai tidak terpercaya (untrusted) dan Konfigurasi semua port uplink (yang terhubung ke switch lain) sebagai terpercaya (trusted).

Topologi pada gambar di bawah menunjukkan contoh penerapan port terpercaya dan tidak terpercaya ini.



Contoh konfigurasi DAI

Berdasarkan topologi sebelumnya, switch S1 terhubung ke dua pengguna di VLAN 10. DAI akan dikonfigurasi untuk melindungi mereka dari serangan ARP. Berikut adalah langkah-langkah konfigurasinya:

1. DHCP Snooping diaktifkan terlebih dahulu, karena DAI memerlukan binding table yang dibuat oleh fitur ini.
2. Selanjutnya, DHCP Snooping dan DAI diaktifkan secara spesifik untuk VLAN 10.

3. Port uplink yang terhubung ke router (F0/1) ditetapkan sebagai port terpercaya (trusted) untuk DHCP Snooping dan DAI.

```
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 melakukan validasi tambahan pada paket ARP dengan memeriksa alamat tujuan, sumber MAC, dan sumber IP.

- Validasi MAC Tujuan: Memeriksa kecocokan antara alamat MAC tujuan di *header* Ethernet dengan alamat MAC target di dalam paket ARP.
- Validasi MAC Sumber: Memeriksa kecocokan antara alamat MAC sumber di *header* Ethernet dengan alamat MAC pengirim di dalam paket ARP.
- Validasi Alamat IP: Memeriksa isi paket ARP untuk alamat IP yang tidak valid, seperti `0.0.0.0`, `255.255.255.255`, dan semua alamat *multicast*.

Untuk mengkonfigurasi validasi tambahan pada DAI, gunakan perintah global `ip arp inspection validate {[src-mac] [dst-mac] [ip]}`. Perintah ini akan membuang paket ARP jika alamat MAC atau IP di dalam paket tidak cocok dengan alamat di *header* Ethernet. Penting untuk diperhatikan: Saat mengkonfigurasi, Anda harus memasukkan semua metode validasi yang diinginkan dalam satu baris perintah. Jika Anda memasukkan perintah ini beberapa kali, setiap perintah baru akan menimpa perintah sebelumnya.

- Cara yang salah

  `ip arp inspection validate src-mac`

  `ip arp inspection validate dst-mac` (perintah ini akan menimpa perintah src-mac)
- Cara yang benar

  `ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Contoh berikut menunjukkan bagaimana ketiga metode validasi tersebut dikonfigurasi dan diverifikasi dalam satu perintah.

```
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)#
```

Mitigasi dari STP Attacks

PortFast dan BPDU Guard

Seorang penyerang dapat memanipulasi Spanning Tree Protocol (STP) untuk mengubah topologi jaringan dengan cara menyamar sebagai *root bridge*. Untuk mencegah serangan semacam ini, gunakan kombinasi fitur PortFast dan BPDU Guard.

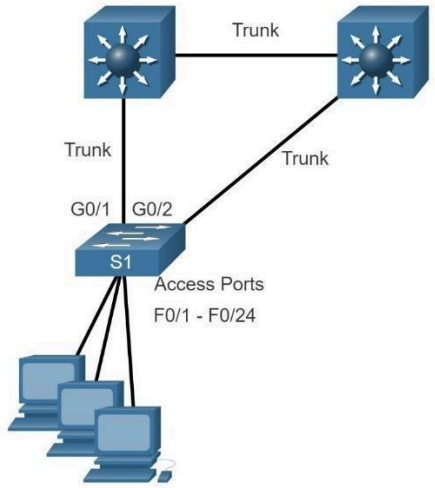
PortFast

Fitur ini mempercepat proses *convergence* STP pada sebuah port. Port yang diaktifkan dengan PortFast akan langsung beralih ke status *forwarding*, tanpa harus melalui status *listening* dan *learning* yang memakan waktu. PortFast hanya boleh diaktifkan pada port akses yang terhubung langsung ke perangkat pengguna akhir (seperti PC, printer, atau server), bukan ke switch lain.

BPDU Guard

Fitur ini berfungsi sebagai pengaman untuk PortFast. BPDU Guard akan secara otomatis mematikan (masuk ke status *error-disabled*) sebuah port jika port tersebut menerima paket BPDU. Karena paket BPDU seharusnya hanya dikirim antar-switch, fitur ini efektif mencegah koneksi switch liar (*rogue switch*) ke jaringan. Sama seperti PortFast, BPDU Guard hanya boleh diaktifkan pada port akses yang terhubung ke perangkat pengguna akhir.

Berdasarkan gambar di bawah ini, semua port akses pada switch S1 seharusnya dikonfigurasi dengan PortFast dan BPDU Guard untuk keamanan optimal.



Konfigurasi PortFast

Fitur PortFast membuat port akses bisa langsung aktif tanpa harus menunggu proses STP *convergence* (status *listening* dan *learning*). Hal ini meminimalkan waktu tunggu bagi perangkat pengguna seperti PC untuk terhubung ke jaringan. Mengaktifkan PortFast pada port yang terhubung ke switch lain sangat berisiko karena dapat menciptakan *spanning-tree loop*.
Anda bisa mengaktifkan PortFast dengan dua cara:

1. **Pada satu interface spesifik**
   `spanning-tree portfast`
2. **Secara global untuk semua port akses**
   `spanning-tree portfast default`

Setelah diaktifkan, sebuah pesan peringatan akan ditampilkan untuk mengingatkan Anda tentang risikonya. Untuk memverifikasi apakah PortFast sudah aktif, gunakan perintah berikut:

- **Verifikasi Global:** `show spanning-tree summary`
- **Verifikasi per interface:** `show running-config interface <nama_interface>` **atau** `show spanning-tree interface <nama_interface> detail`

```
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#
```

Konfigurasi BPDU Guard

Meskipun PortFast diaktifkan, sebuah port akan tetap listening paket BPDU. Penerimaan BPDU pada port akses bisa terjadi karena kesalahan konfigurasi atau upaya penyerang untuk menyambungkan switch liar (*rogue switch*) ke jaringan. Fitur BPDU Guard berfungsi untuk mencegah hal ini. Jika sebuah port yang dilindungi BPDU Guard menerima paket BPDU, port tersebut akan langsung masuk ke status error-disabled, yang berarti port akan dimatikan.
Untuk mengaktifkannya kembali, administrator harus melakukannya secara manual atau mengkonfigurasi pemulihan otomatis.
Anda bisa mengaktifkan BPDU Guard dengan dua cara:

1. **Pada satu interface spesifik: `spanning-tree bpduguard enable`**
2. **Secara global untuk semua port yang memiliki PortFast: `spanning-tree portfast bpduguard default`**

Untuk melihat status global PortFast dan BPDU Guard, gunakan perintah `show spanning-tree summary`. Pada contoh di bawah ini, output dari perintah tersebut menunjukkan bahwa PortFast dan BPDU Guard telah diaktifkan secara default untuk semua port yang berada dalam 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
```

CODELAB

Tugas yang dilakukan yaitu mengerjakan aktivitas Implement port security menggunakan packet tracer yang sudah disediakan di tautan berikut ini:
https://bit.ly/modul-5_jarkom_2025_umm

1. **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".**
2. **Kemudian buatlah laporan tertulis sebagai bukti pemahaman kalian terhadap pekerjaan yang kalian kerjakan. Laporan ini akan di cek, apabila ada kesamaan kata-kata, penjelasan dan atau hasil Ai, maka akan codelab tidak akan dinilai alias nilai 0. Format laporan "Tugas-Nama-NIM.pdf".**
3. **Tugas dikumpulkan di infotech.umm.ac.id pada bagian attachment sebelum berlangsungnya kegiatan praktikum demo.**

Tabel Alamat

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

Tujuan

Bagian 1: Konfigurasi Port Security
Bagian 2: Verifikasi Port Security

Latar Belakang

Pada aktivitas ini, Anda akan mengkonfigurasi dan memverifikasi keamanan port (port security) pada sebuah switch. Fitur keamanan port memungkinkan Anda untuk membatasi lalu lintas yang masuk ke sebuah port dengan cara menyaring alamat MAC mana saja yang diizinkan untuk mengirim data.

Bagian 1: Konfigurasi Port Security

a. **Akses baris perintah (command line) pada switch S1 dan aktifkan fitur keamanan port pada antarmuka FastEthernet 0/1 dan 0/2.**

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

b. Atur agar hanya satu perangkat saja yang bisa mengakses port FastEthernet 0/1 dan 0/2.

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

c. Amankan port agar alamat MAC perangkat dipelajari secara dinamis dan langsung ditambahkan ke dalam konfigurasi yang sedang berjalan (running configuration).

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

d. Atur mode pelanggaran agar saat terjadi pelanggaran, port FastEthernet 0/1 dan 0/2 tidak mati (not disabled). Sebagai gantinya, sebuah notifikasi akan dikirim dan paket dari sumber yang tidak dikenal akan dijatuhkan (dropped).

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

e. Matikan semua port lain yang tidak digunakan. Gunakan kata kunci `range` untuk menerapkan konfigurasi ini ke semua port secara bersamaan.

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

Bagian 2: Verifikasi Port Security

a. Dari PC1, lakukan ping ke PC2.

b. Verifikasi bahwa keamanan port sudah aktif dan alamat MAC dari PC1 dan PC2 telah ditambahkan ke dalam konfigurasi yang berjalan.

```
S1# show running-config | begin interface
```

c. Gunakan perintah `show port-security` untuk menampilkan informasi konfigurasi.

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

d. Hubungkan Rogue Laptop ke port switch lain yang tidak digunakan dan perhatikan bahwa lampu indikatornya berwarna merah (mati).

e. Aktifkan port tersebut dan verifikasi bahwa Rogue Laptop bisa melakukan ping ke PC1 dan PC2. Setelah verifikasi selesai, matikan kembali port yang terhubung ke Rogue Laptop.

f. Cabut koneksi PC2 dan hubungkan Rogue Laptop ke port F0/2 (port yang tadinya digunakan oleh PC2). Verifikasi bahwa Rogue Laptop tidak dapat melakukan ping ke PC1.

g. Tampilkan data pelanggaran keamanan port untuk port yang terhubung dengan Rogue Laptop.

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

Pertanyaan: Berapa banyak pelanggaran yang telah terjadi?

h. Cabut koneksi Rogue Laptop dan hubungkan kembali PC2. Verifikasi bahwa PC2 bisa melakukan ping ke PC1.

Pertanyaan: Mengapa PC2 bisa melakukan ping ke PC1, sedangkan Rogue Laptop tidak bisa?

RUBRIK PENILAIAN

Pemahaman Materi	**30%**
Codelab	**20%**
Demo	**50%**