ICT2203/ICT2203X

Network Security

SINGAPORE INSTITUTE OF TECHNOLOGY

Lab 2 Notes:

Attacks and Defense of Local Area Networks (LAN) with Switches Part 2

2021-2022 Trimester 3

Lab Exercise 3

SINGAPORE INSTITUTE OF TECHNOLOGY

3.1 Double tagging attack

3.2 Defenses:

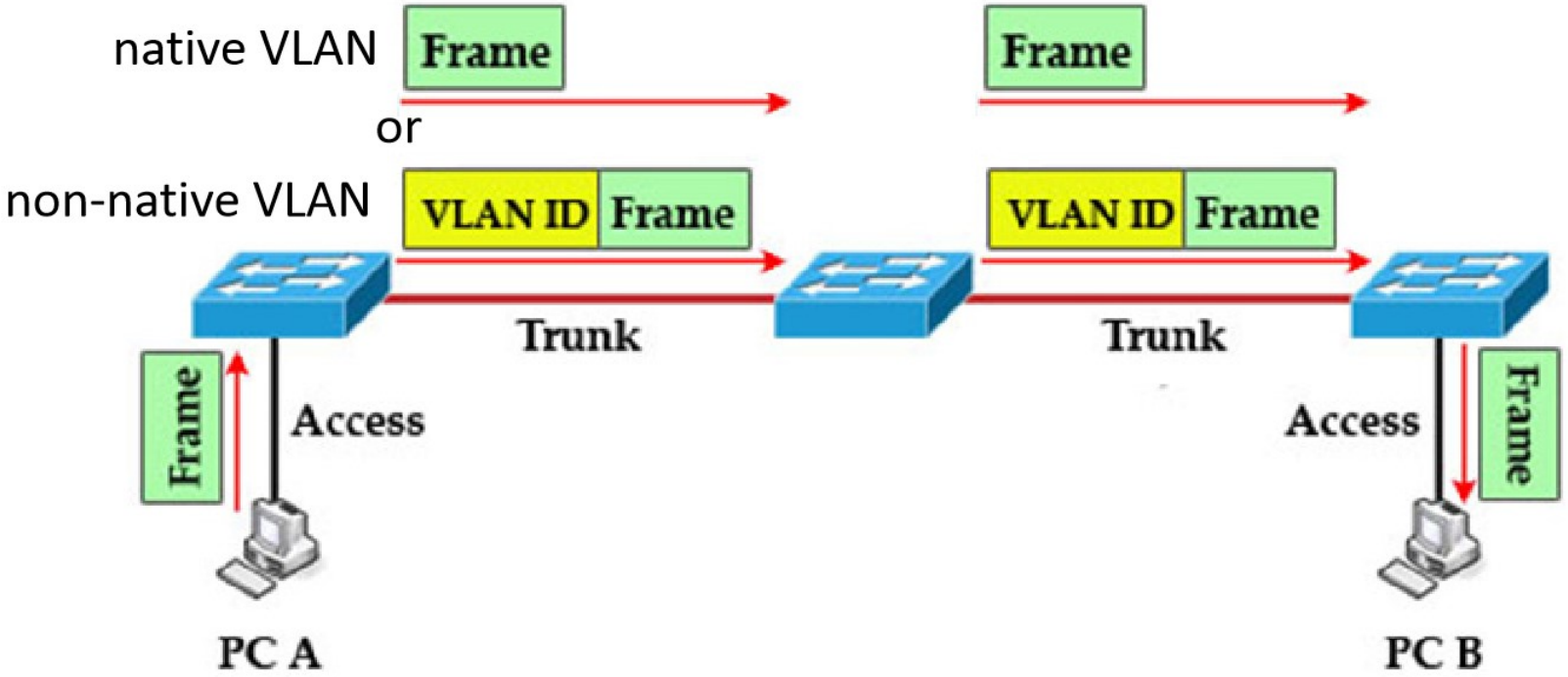
- Configure dedicated native VLAN ID for trunk which must not be used for access ports
- Enable tagging for native VLAN if applicable
- Good practice not to use default VLAN 1

Inside a trunk, the different VLAN traffic are distinguished using the IEEE 802.1Q tagging standard. (Refer ICT1010 lecture 3 for details.)

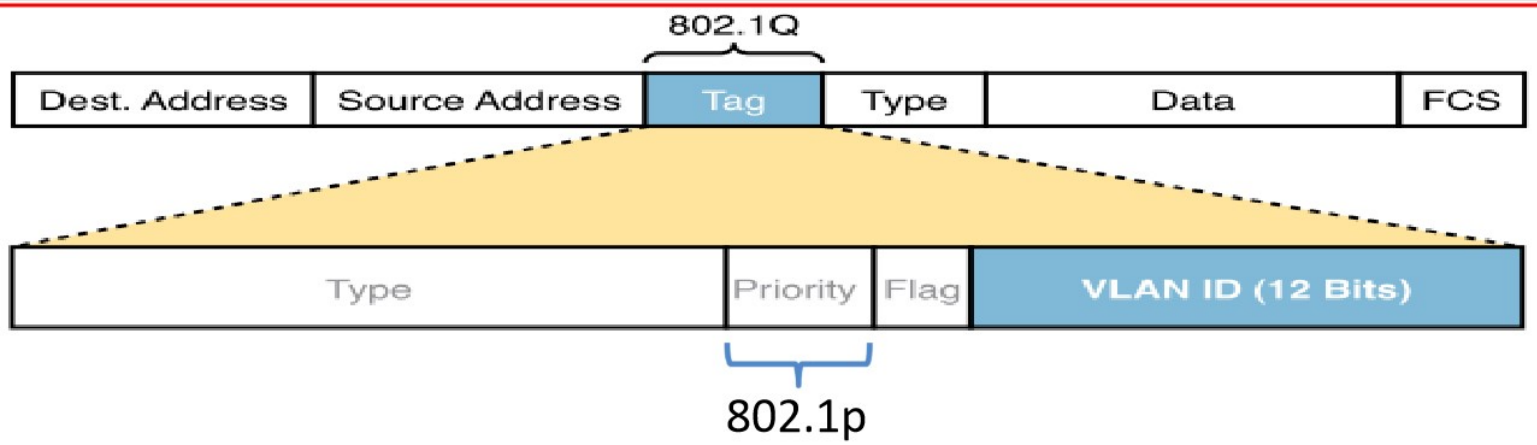
Specifically, IEEE 802.1Q supports two types of VLANs inside trunk:

(i) one native VLAN – frames are not tagged

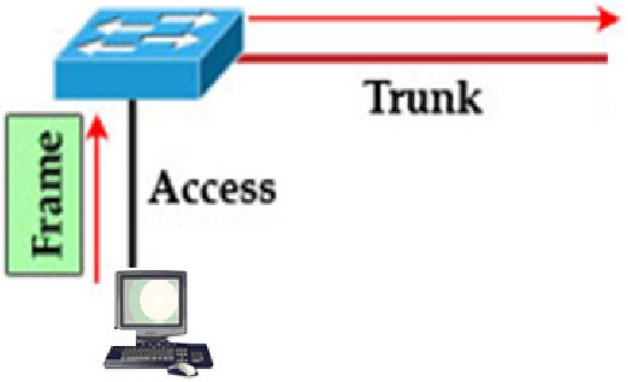
(ii) all other VLANs – frames are tagged with appropriate VLAN ID



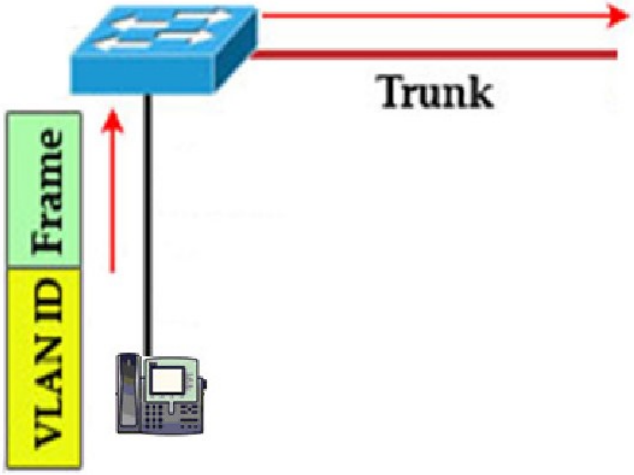
The 802.1Q tag is also being used to support voice over IP (VoIP), specifically the 3-bit priority field is used to specify class of service (CoS) according to IEEE 802.1p standard.



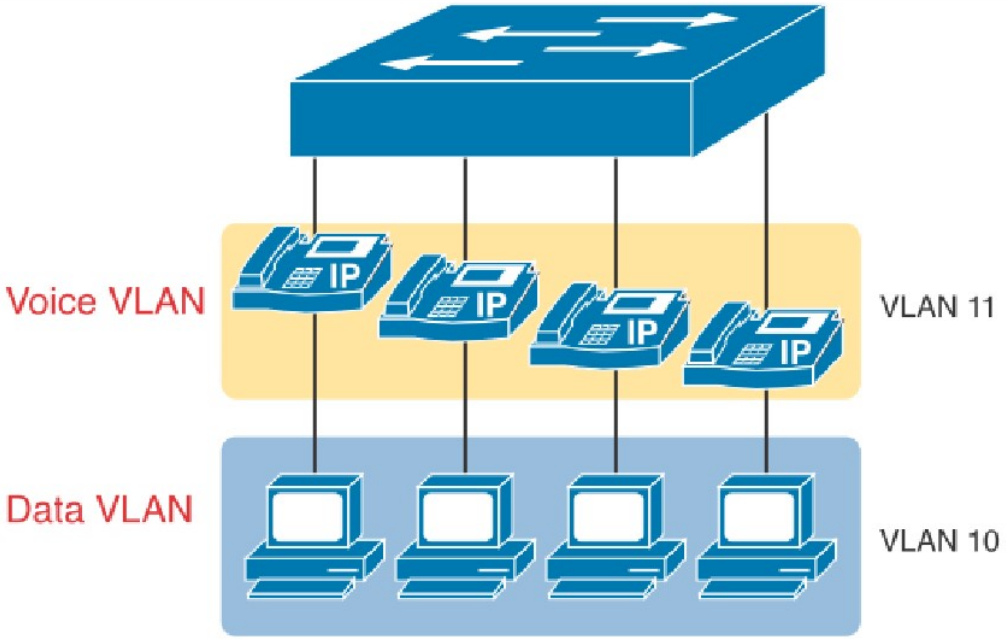
Frames carrying data:



Frames carrying voice:

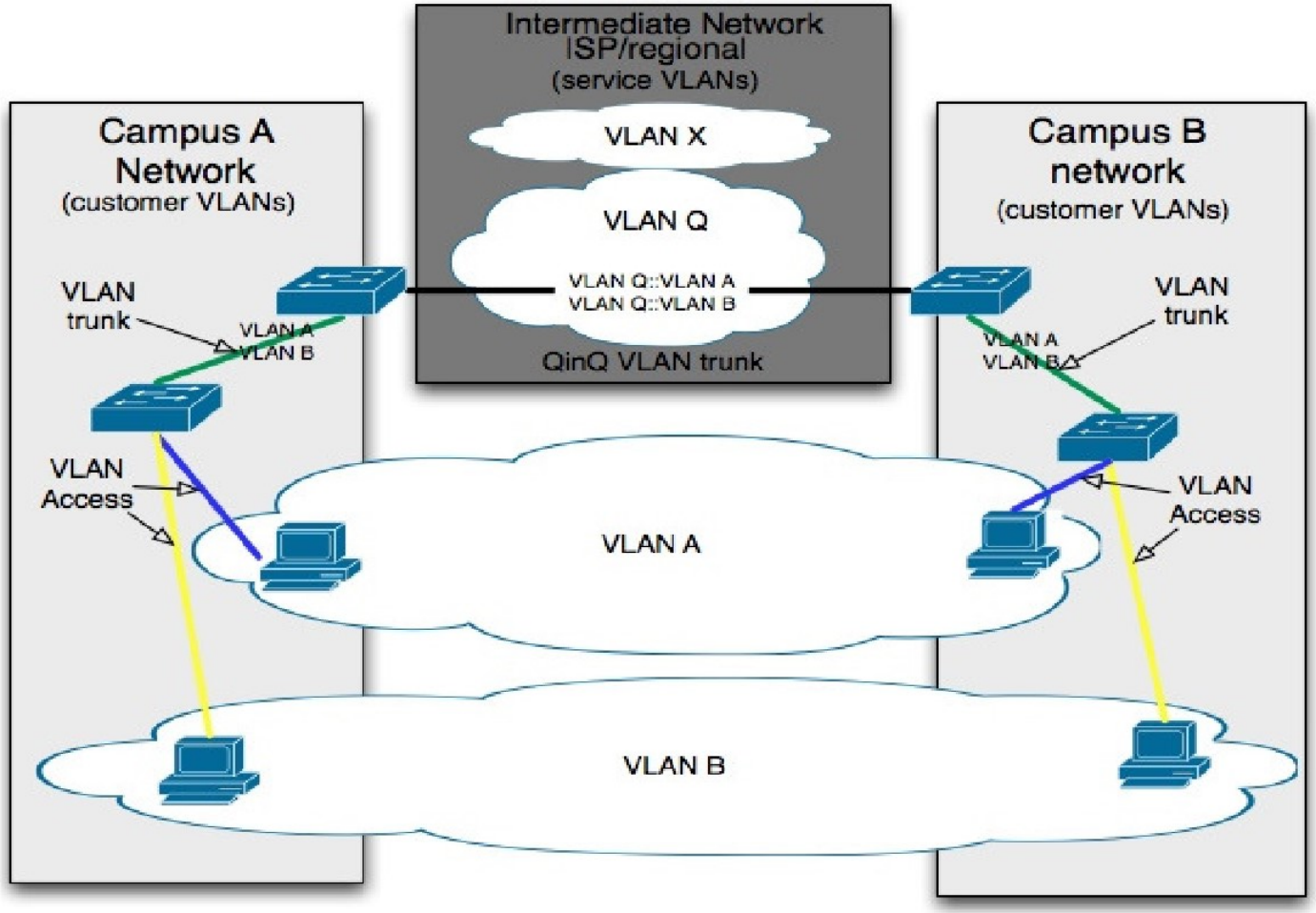


To support VoIP, the switch ports will also need to be configured with a data VLAN and an auxiliary voice VLAN to receive tagged frames.

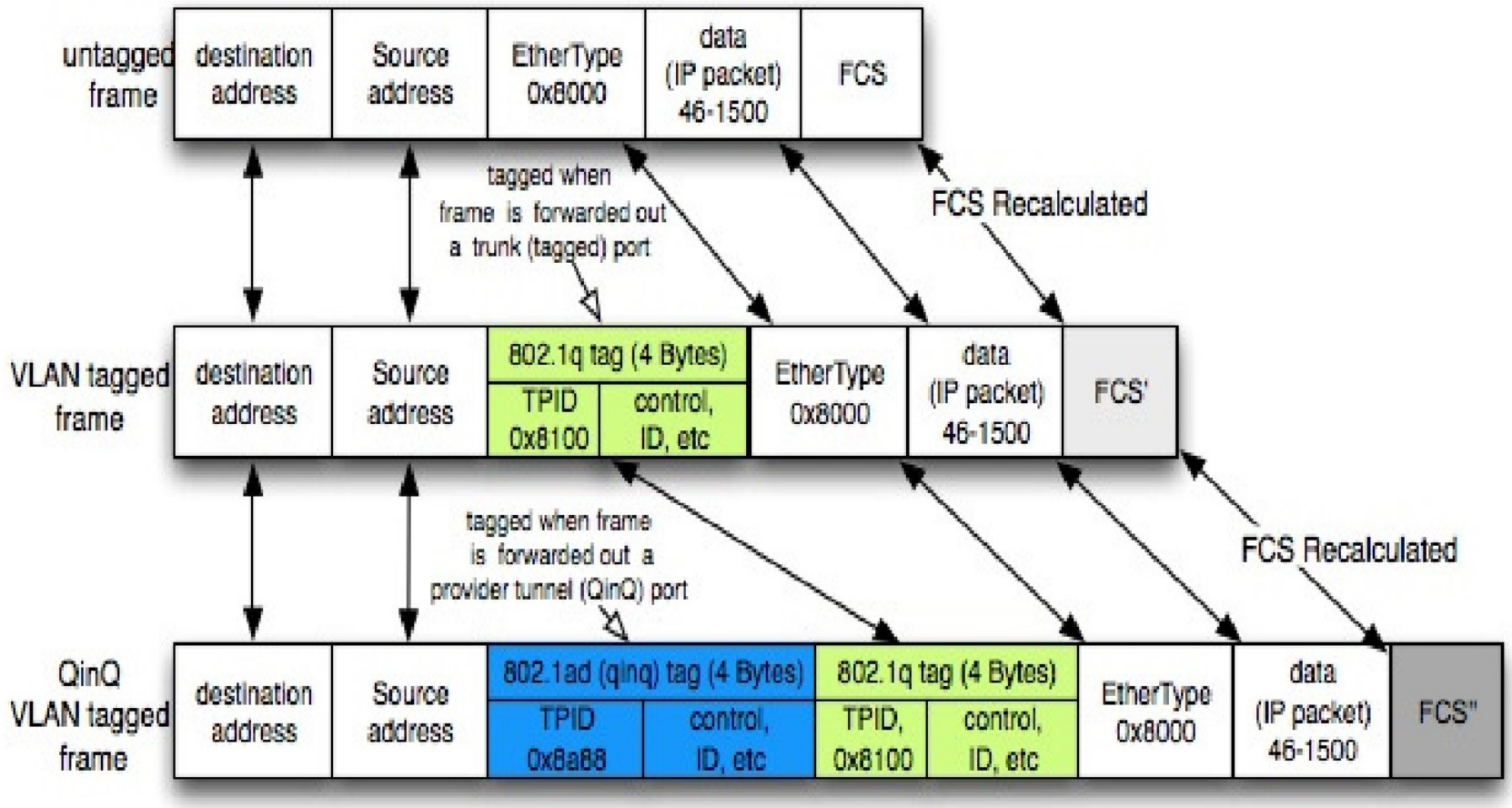



```
SW1(config-vlan)# interface range FastEthernet0/1 - 4
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# switchport voice vlan 11
```

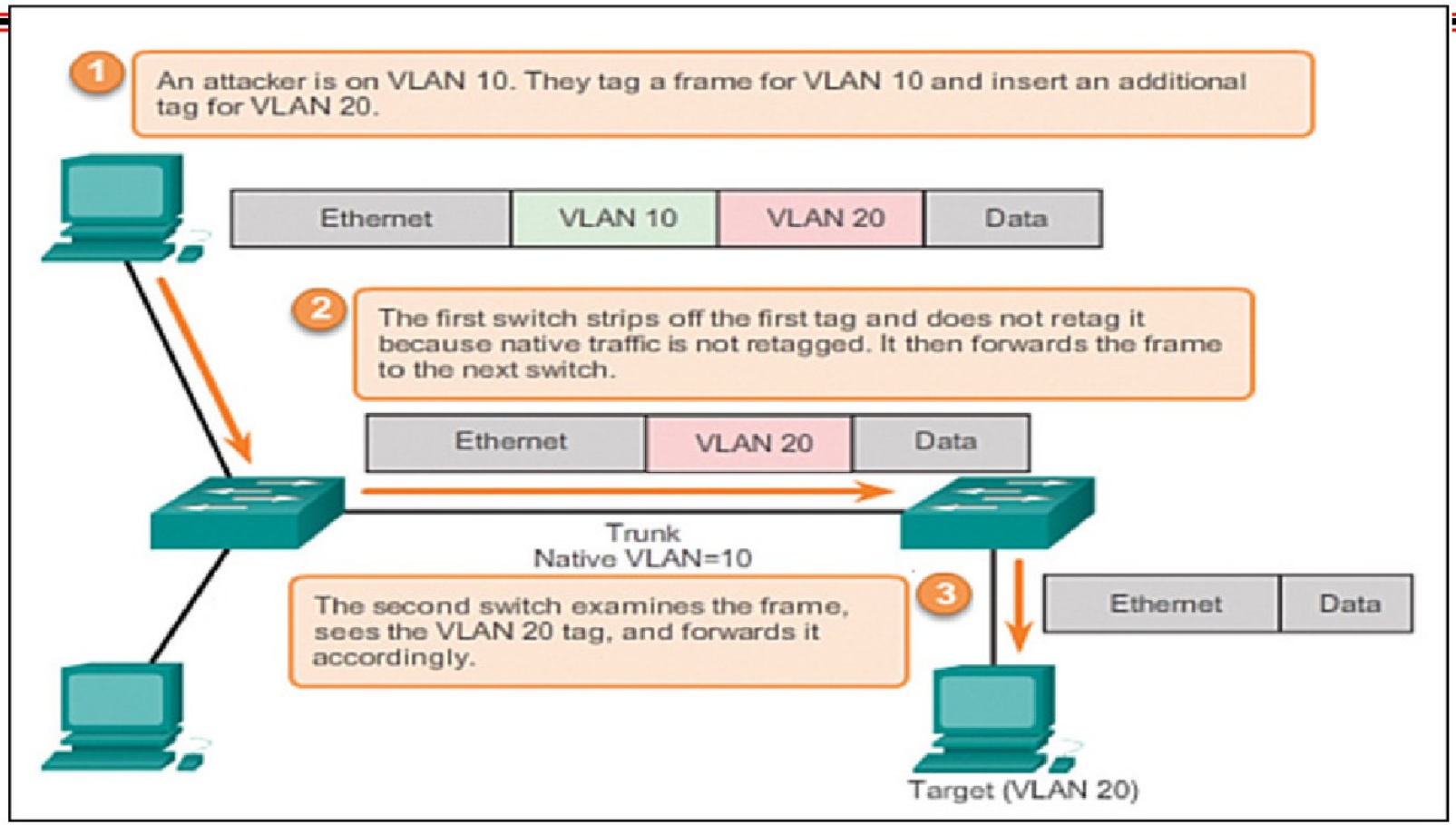
With the development of metropolitan-area Ethernet, double 802.1Q tags are also supported such as Q-in-Q (802.1Q in 802.1Q) where customers' VLANs can tunnel through ISP VLAN



Specifically, Q-in-Q is implemented by inserting an outer 802.1Q tag of the ISP besides the original inner 802.1Q tag of the customers as follows:

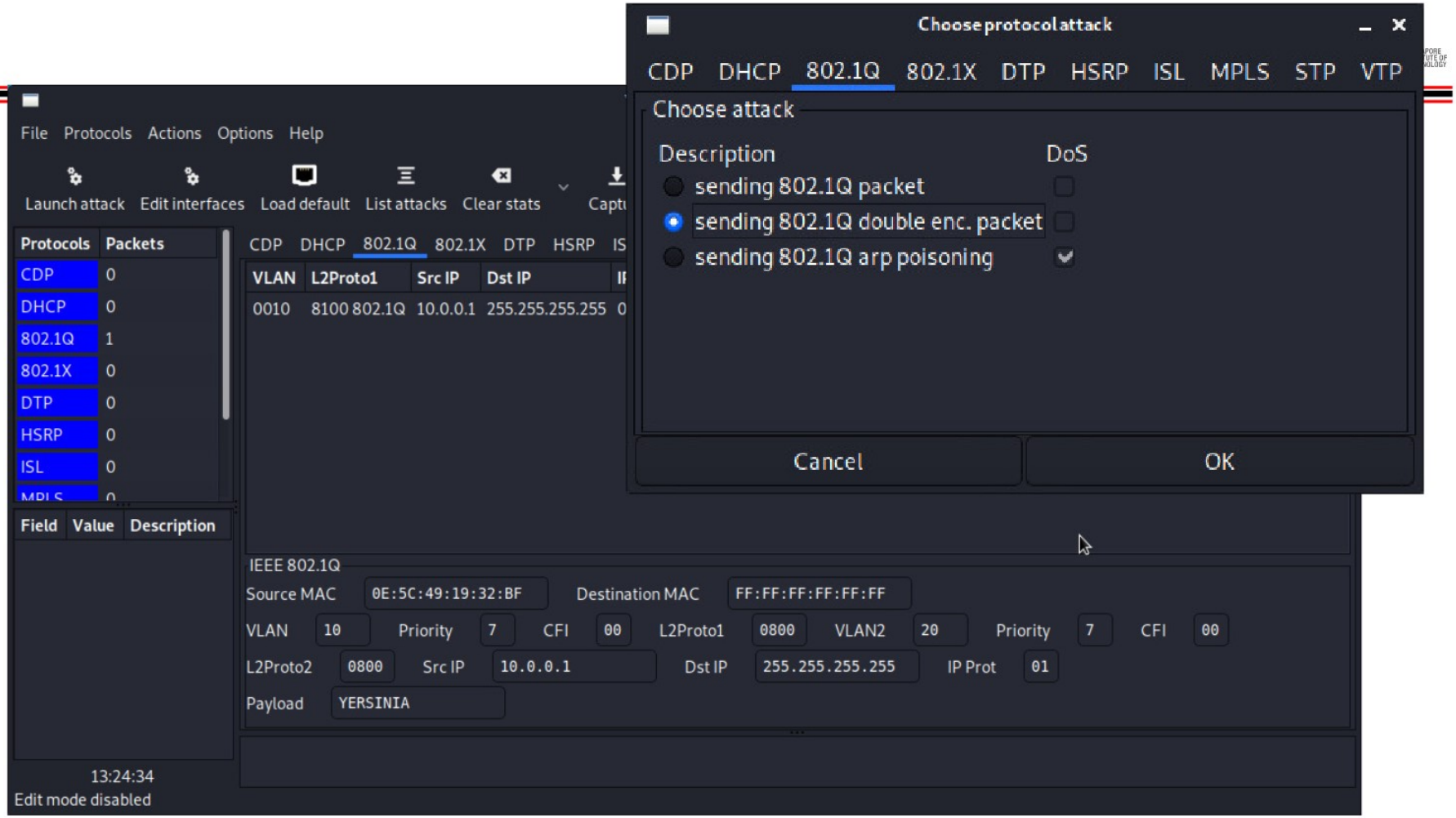


Double tagging attack – another form of VLAN hopping attack where an attacker can send frames to hop to other VLANs without going through a router or firewall.

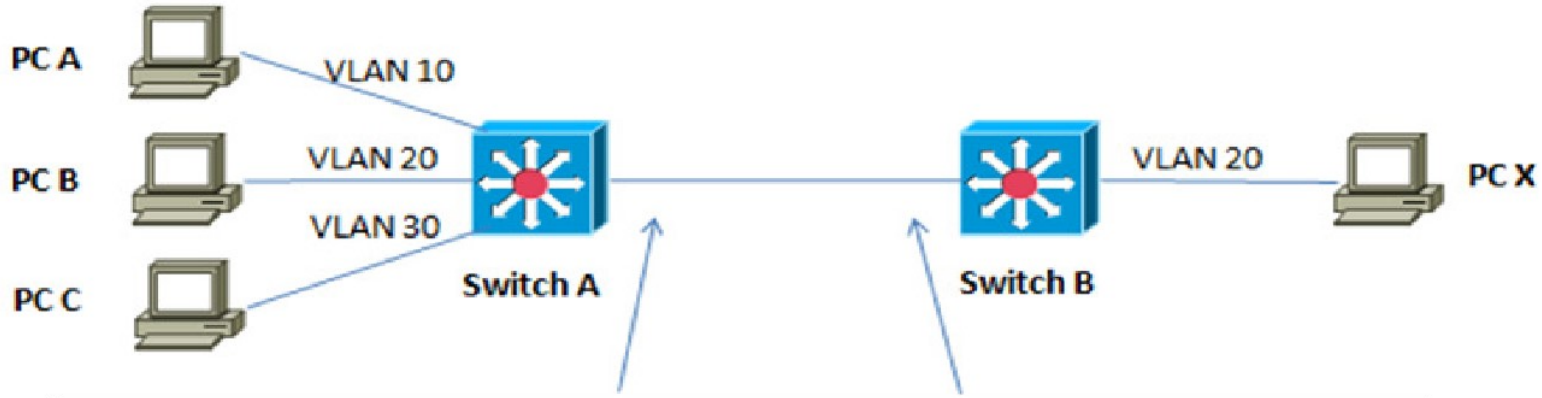


Note: double tagging attack works only if attacker's access port has the same VLAN ID as the native VLAN of the trunk, default is VLAN 1.

Similarly, Yersinia can be used to perform double tagging attack.



To prevent double tagging attack, configure dedicated native VLAN, e.g. VLAN 500, for all trunk ports which should not be assigned to any access ports.




```
CiscoSwitch(config-if)#switchport trunk native vlan 500
```

Alternatively, some switches like Catalyst 3650 switch in the lab have the feature of forcing all traffic on the trunk to be tagged, including native VLAN.

```
CiscoSwitch(config)#vlan dot1q tag native
```

Lab Exercise 4

SINGAPORE INSTITUTE OF TECHNOLOGY

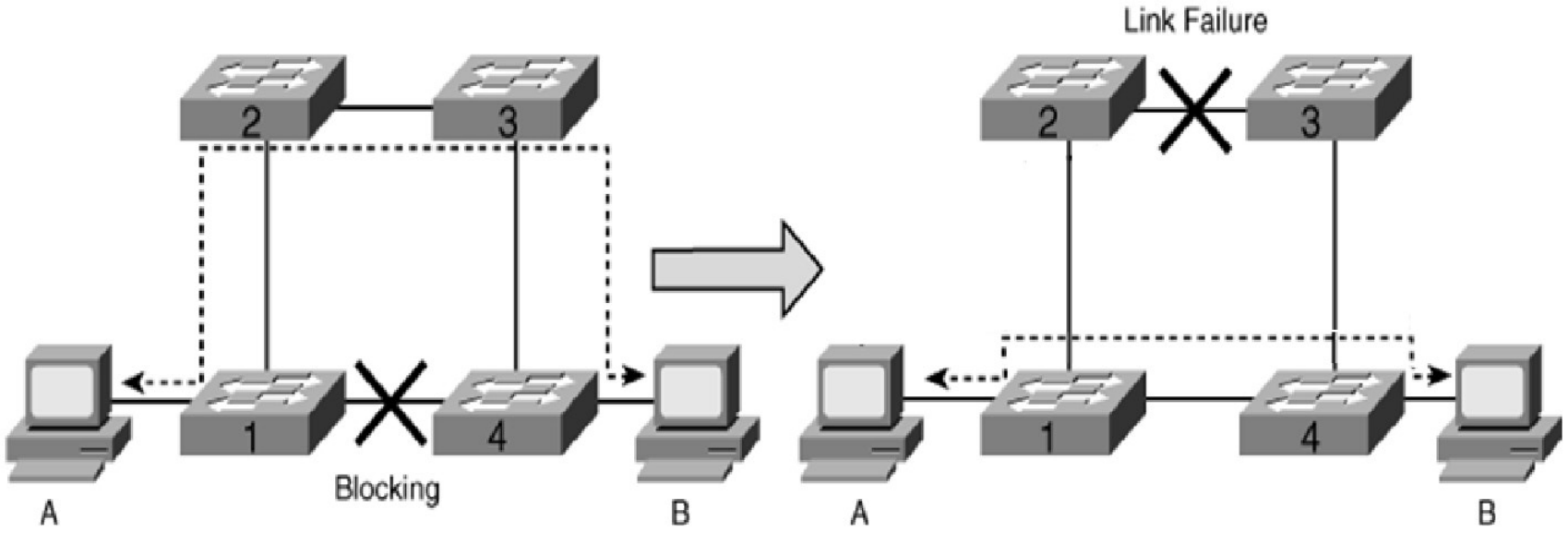
4.1 STP Attack

4.2 Defense:

- Implement PortFast, BPDU guard and root guard

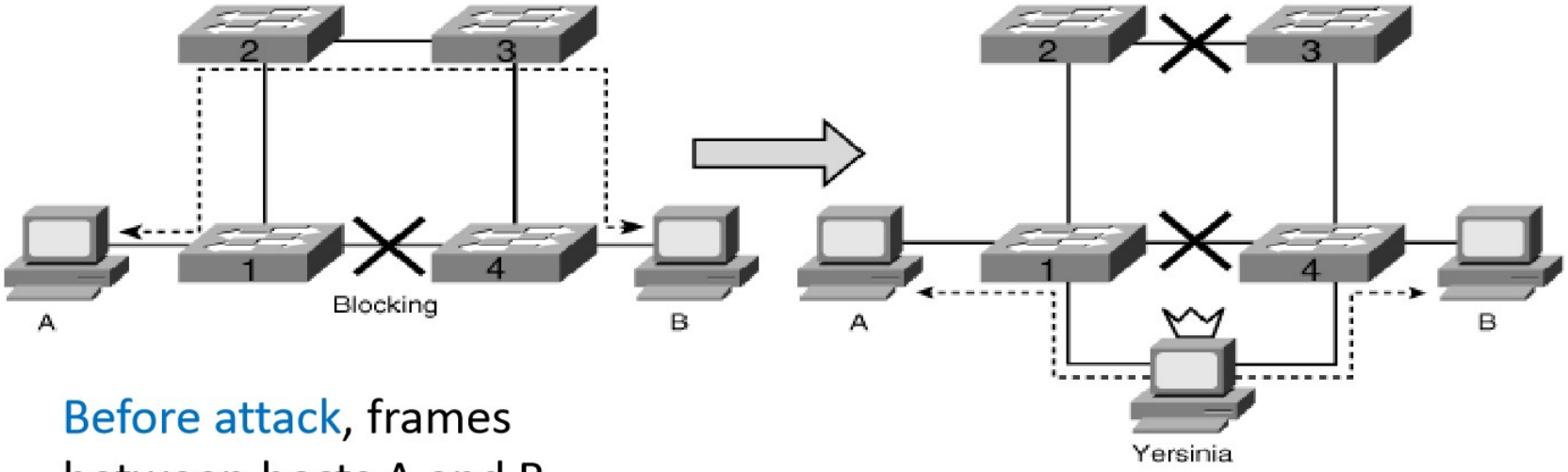
Recall from ICT1010 that to mitigate single point of failure, switches are commonly interconnected with redundancies and STP (802.1D) are run automatically to prevent loops.

With redundancies, the network can continue to work if a link fails as Spanning Tree Protocol (STP) is able to re-configure itself automatically.



However, STP has no security. An attacker can inject BPDU with lower bridge ID to take over root switch and capture frames that otherwise would not be accessible.

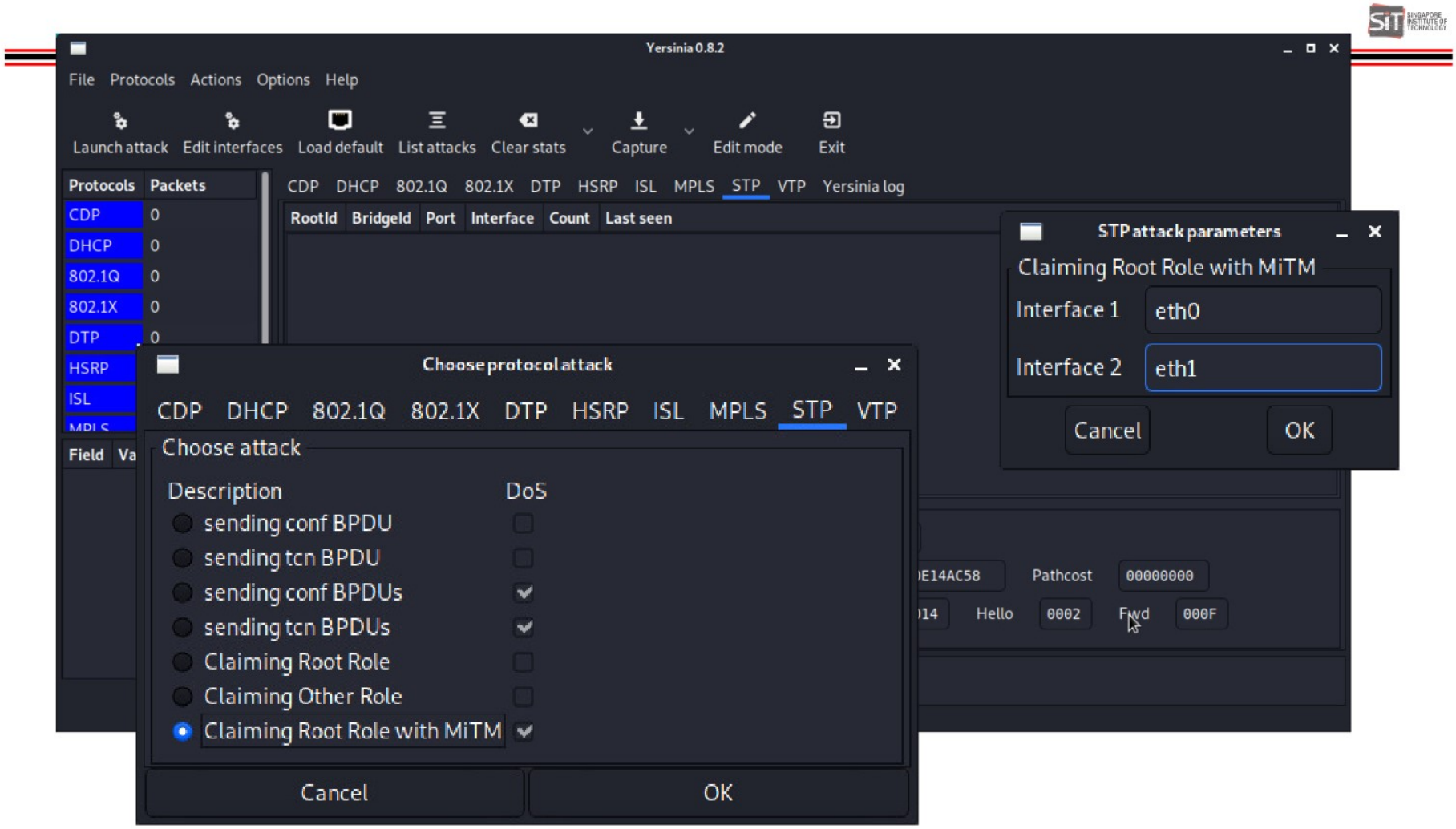
Connecting an attacker host with 2 Ethernet ports, one to each switch as shown:



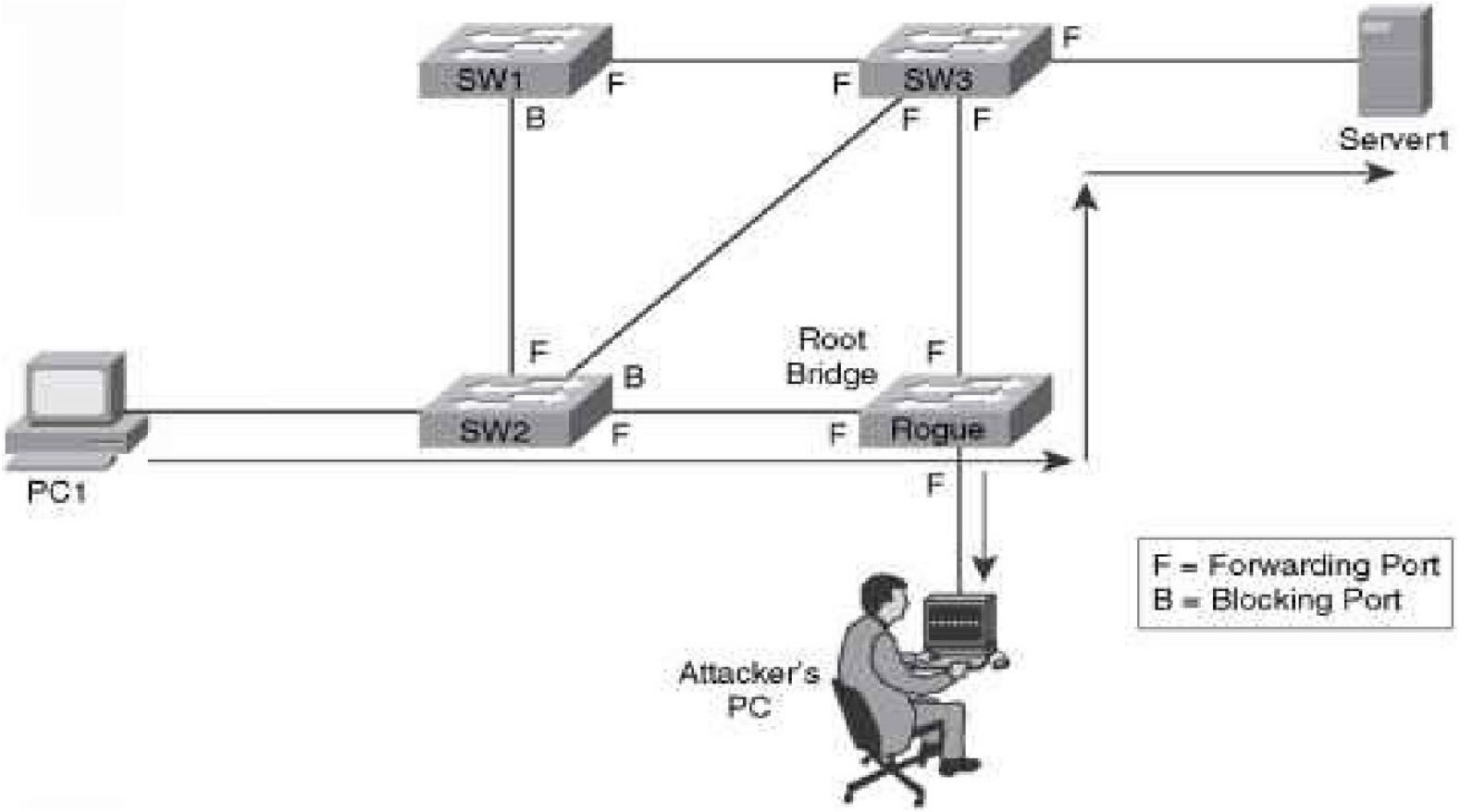
Before attack, frames between hosts A and B passes via switches 1-2-3-4 and are not seen by attacker.

After STP attack, link 2-3 becomes blocked. Frames between A and B are now passing via the attacker's host (new root bridge) and are captured by attacker.

Yersinia has an STP attack feature to claim root role with MiTM but unfortunately does not seem to work.

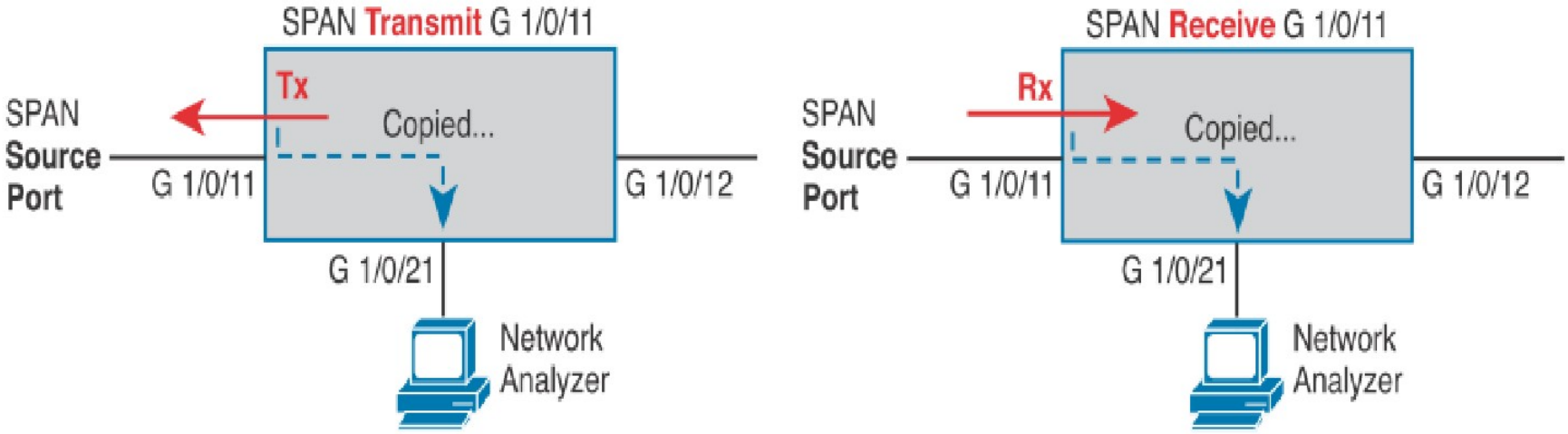


So for you to try STP attack in the lab, we will simulate an attacker bringing his own rogue switch to take over original root switch and capture frames.



To copy frames from a switch to your laptop, you can configure Switch Port Analyzer (SPAN) in Cisco switch as follows:

SPAN may be configured to capture only transmitted frames, or only received frames, or both, from a source port.




```
SW11(config)# monitor session 1 source interface Gi1/0/11 both
SW11(config)# monitor session 1 destination interface Gi1/0/21
```

The monitor session number may be any valid number from 1 to 18.

If your capture does not appear to be working, you may verify the SPAN session with the following commands:

```
SW11# show monitor session all
Session 1
---------
Type                      : Local Session
Source Ports              :
    Both                  : Gi1/0/11
Destination Ports         : Gi1/0/21
    Encapsulation         : Native
          Ingress         : Disabled
```

```
SW11# show monitor detail
Session 1
---------
Type                        : Local Session
Description             : -
Source Ports                :
    RX Only                 : None
    TX Only                 : None
    Both                    : Gi1/0/11
Source VLANs                :
    RX Only                 : None
    TX Only                 : None
    Both                    : None
! Lines omitted for brevity
```

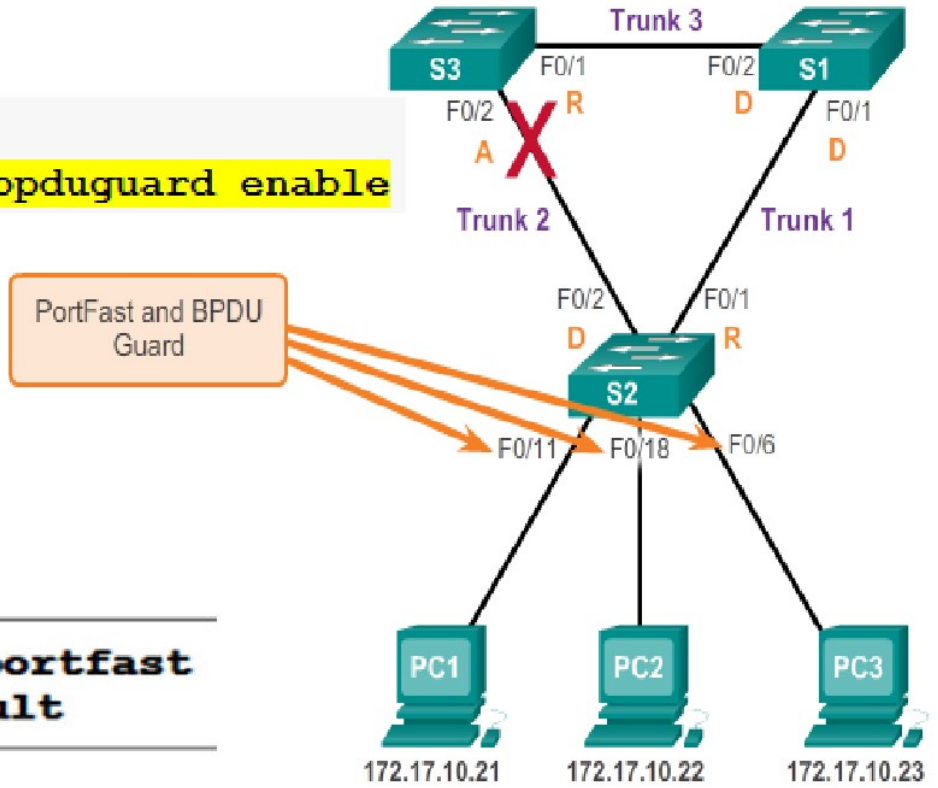
To prevent STP attack, apply BPDU guard feature available in Cisco switches.

BPDU guard may be enabled individually at each interface that is not supposed to receive BPDU, e.g.:

```
S2(config)# interface Fa0/11
S2(config-if)#  spanning-tree bpduguard enable
```

Alternatively, BPDU guard may simply be enabled globally on all PortFast-enabled ports since these ports should not receive BPDU.

```
S2(config)# spanning-tree portfast
            bpduguard default
```



If a BPDU guard-enabled port receives a BPDU, it will be put into error-disabled state. (The disabled port must then be re-enabled manually or configured with auto-recovery similar as port-security violation.)

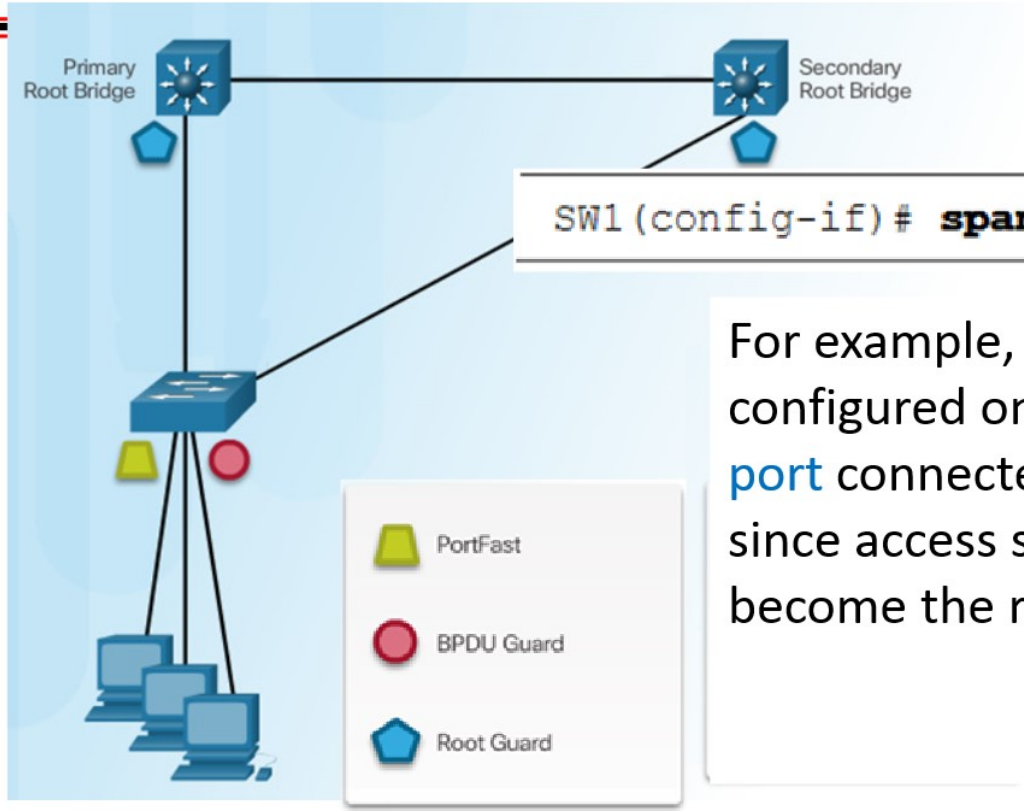
Recall ICT1010 a port will transit from listening to learning before finally being placed in forwarding or blocked state to prevent loops.

State	Forwards Data Frames?	Learns MACs Based on Received Frames?	Transitory or Stable State?
Disabled	No	No	Stable
Blocking	No	No	Stable
Listening	No	No	Transitory
Learning	No	Yes	Transitory
Forwarding	Yes	Yes	Stable

For ports connected to user hosts which will not create loops, you may speed up transiting to forwarding state immediately by configuring PortFast to bypass listening and learning states:

```
SW3(config)# interface fastEthernet 0/13
SW3(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
```

In addition, Cisco switches have a root guard feature to enforce the placement of root switches, preventing them from being taken over by rogue root switch.




```
SW1(config-if)# spanning-tree guard root
```

For example, root guard can be configured on distribution layer switch port connected to access layer switch since access switch should never become the root bridge.

If a root guard port receives superior BPDUs, it will transit to root inconsistent state, equivalent to listening state which stops forwarding traffic. It will recover automatically when superior BPDUs stop.

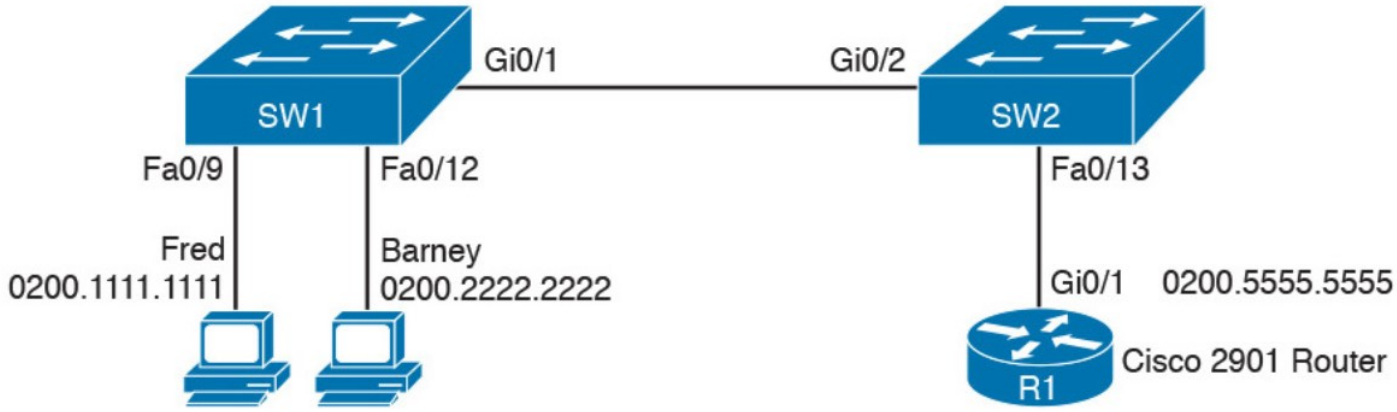
Lab Exercise 5

5.1 Network information leakage, e.g. CDP

5.2 Defense:

- Disable CDP on access ports not supporting VoIP

To facilitate network troubleshooting, Cisco has implemented proprietary CDP (Cisco Discovery Protocol) where a device will periodically send CDP frames to advertise itself.



CDP has no security, and by listening for CDP frames, neighbouring devices can be determined, e.g. on switch SW2 as follows:

```
SW2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW1              Gig 0/2           170           S I      WS-C2960- Gig 0/1
R1               Fas 0/13          136         R S I      CISCO2901 Gig 0/1
```

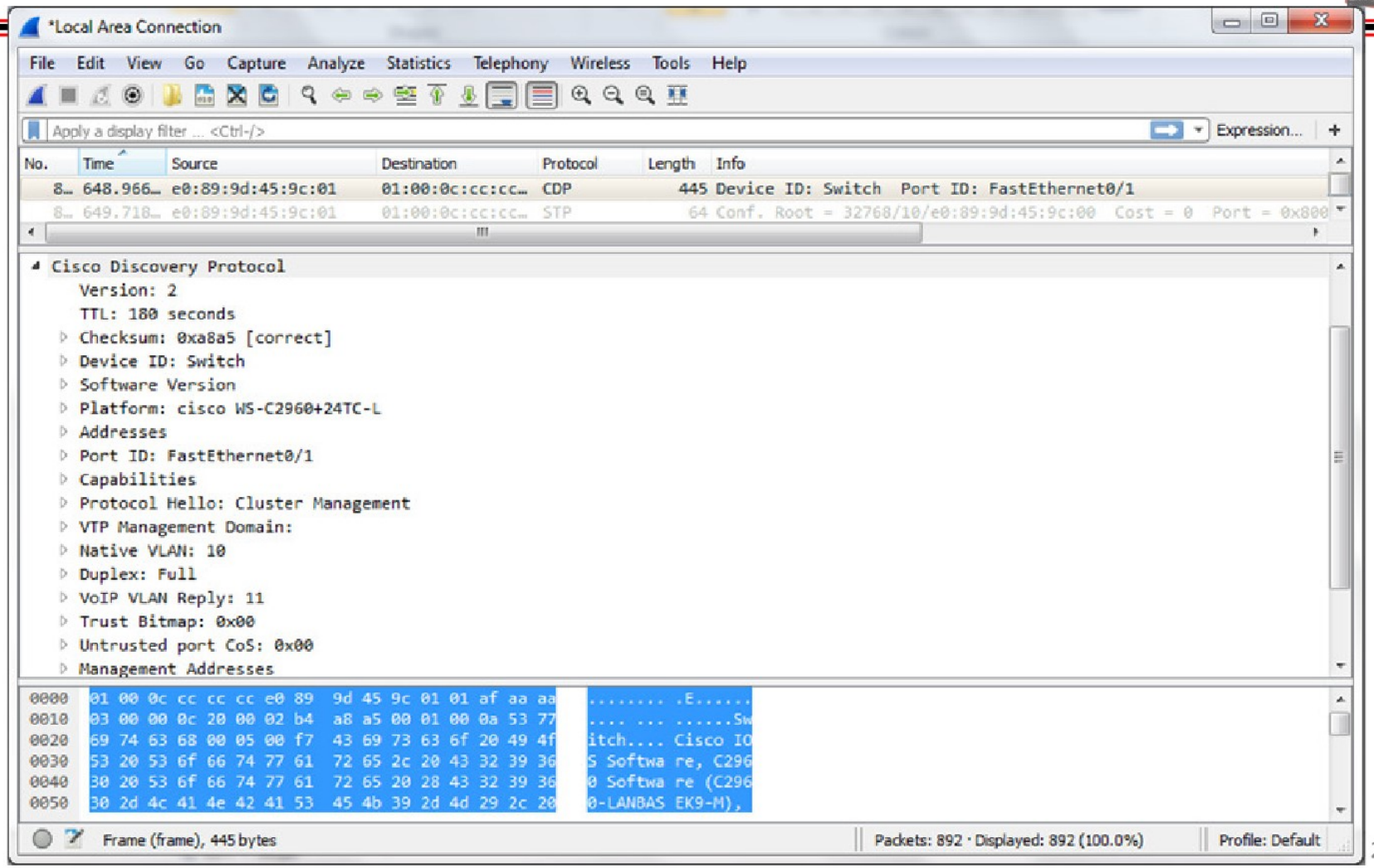
CDP runs on all Cisco network devices and reveals information which can be useful for attackers, e.g. IOS version, VLAN ID, auxiliary voice VLAN ID, IP address, etc., e.g. as follows:

```
SW2# show cdp neighbors detail
-------------------------
Device ID: SW1
Entry address(es):
  IP address: 172.16.1.1
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/2,  Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(1)SE3, RELEASE
  SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 30-May-12 14:26 by prod_rel_team

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
  value=00000000FFFFFFFF010221FF0000000000018339D7B0E80FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 172.16.1.1
```

By default CDP is multicast out all interfaces of the network devices, thus an attacker connected to an access switch can also capture CDP information, e.g. using Wireshark as shown:



To prevent information leakage, a recommended best practice is to disable CDP on all access ports, except ports supporting VoIP which require CDP to function.

CDP may be disabled individually on each interface:

```
! Disable CDP on Interface Fa1/0/24
sw2(config)# interface fa1/0/24
sw2(config-if)# no cdp enable
```

Or disabled globally on all interfaces of the device:

```
! Disable CDP Globally
sw2(config)# no cdp run
sw2(config)# exit
sw2#
! Verify CDP has been disabled
sw2# show cdp
% CDP is not enabled
```