Paweł Pokrywka

Ethernet Radar

Suszarka. Ręczny radar do pomiaru prędkości.Taki pomiar policjanci nazywają fachowo kontrolą statyczną, bo suszarką można mierzyć tylko prędkość nadjeżdżających samochodów. Urządzenie ma wyświetlacz, na którym widać, jak szybko jechał kierowca. **Fotoradar.** To urządzenie, które samoczynnie rejestruje prędkość. Można je zamontować na stałe na maszcie, słupie bądź ustawić na trójnogach i przenosić w różne miejsca w zależności od po-

How to locate the host in the LAN

Idea

- Everybody knows Traceroute - L3
  - TTL (IP header field) decrementation
  - ICMP Time Exceeded if TTL == 0
  - allows to locate host/router
    - with router granularity
- Traceroute in L2?
  - switches in place of routers
  - no TTL equivalent
  - switches don't modify frames

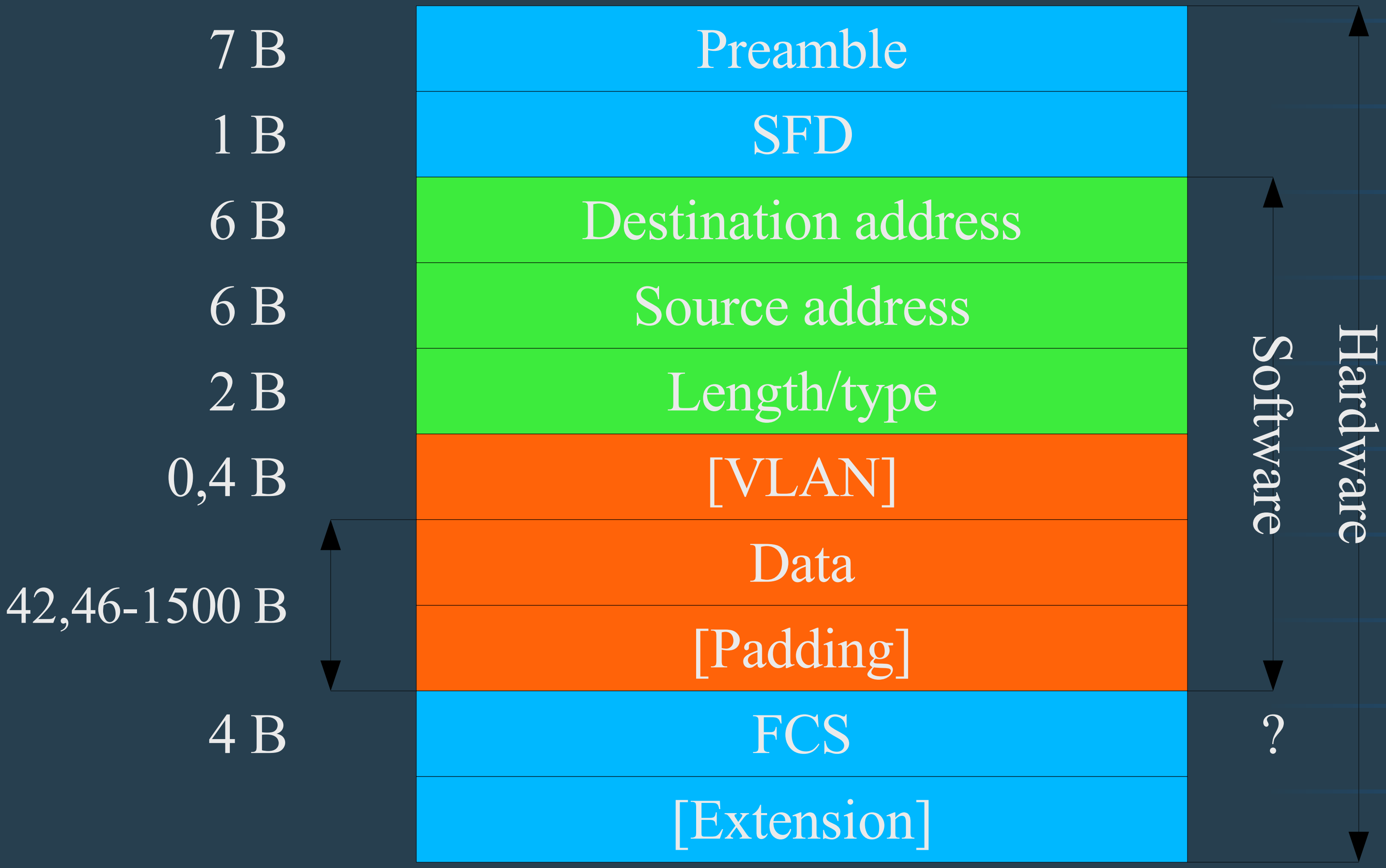
What if it would be possible?

- Get localization of
  - the intruder
  - valuable resources
- Generating LAN map
  - network documentation
  - audit
  - preparing for an attack

How to achieve that?

- Managable switches
  - admin – expensive
  - attacker – needs to get access
- Physical network structure changing
  - hard to do, especially for the attacker
- Latency analysis
  - host A closer than B if ping A < ping B?
- Overloading network fragments
- MAC Spoofing

Basics: Ethernet frame



7 B	Preamble
1 B	SFD
6 B	Destination address
6 B	Source address
2 B	Length/type
0,4 B	[VLAN]
42,46-1500 B	Data
	[Padding]
4 B	FCS
	[Extension]

Software

Hardware

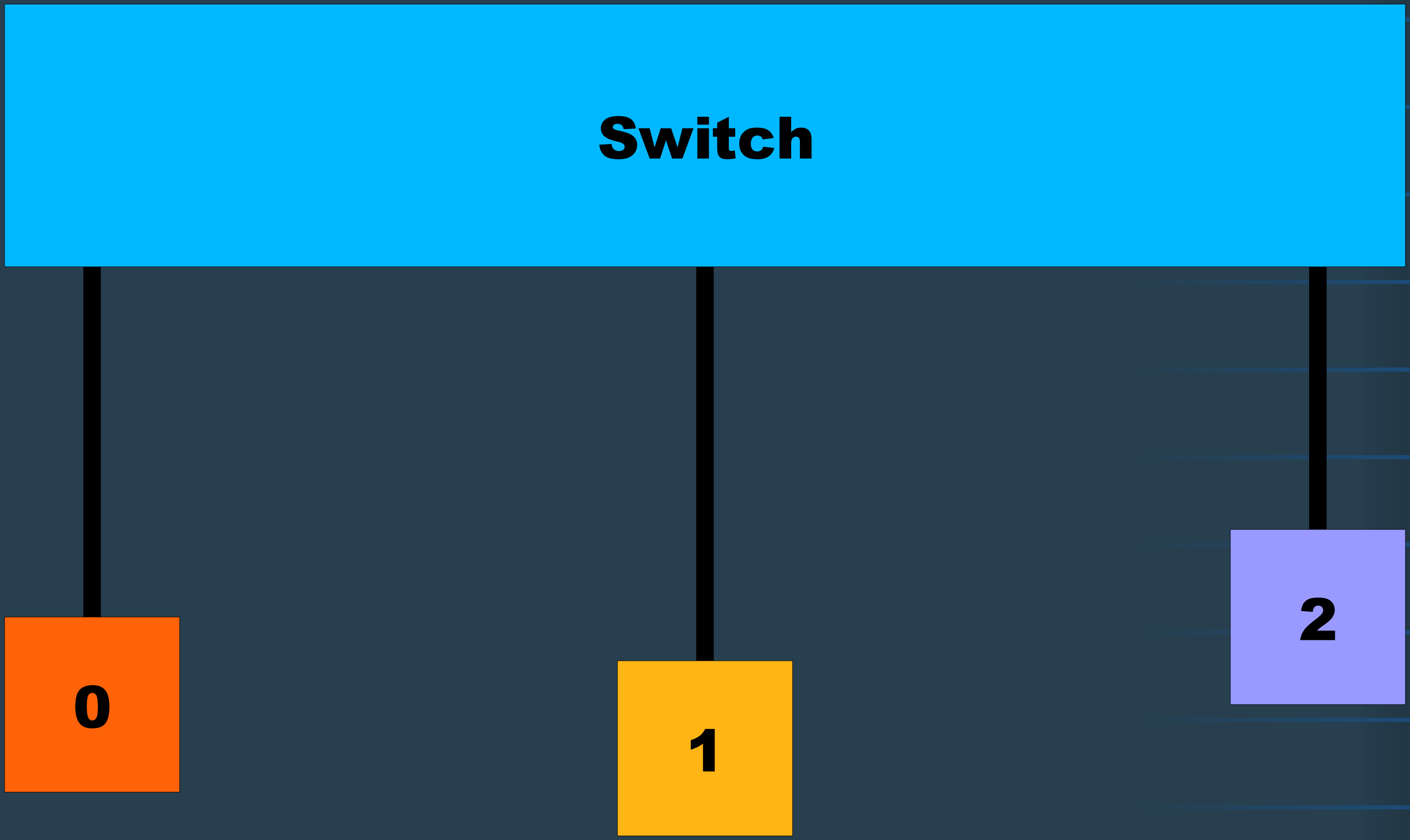
?

How to identify the end of frame if data part is variable length and there is no total length of frame?

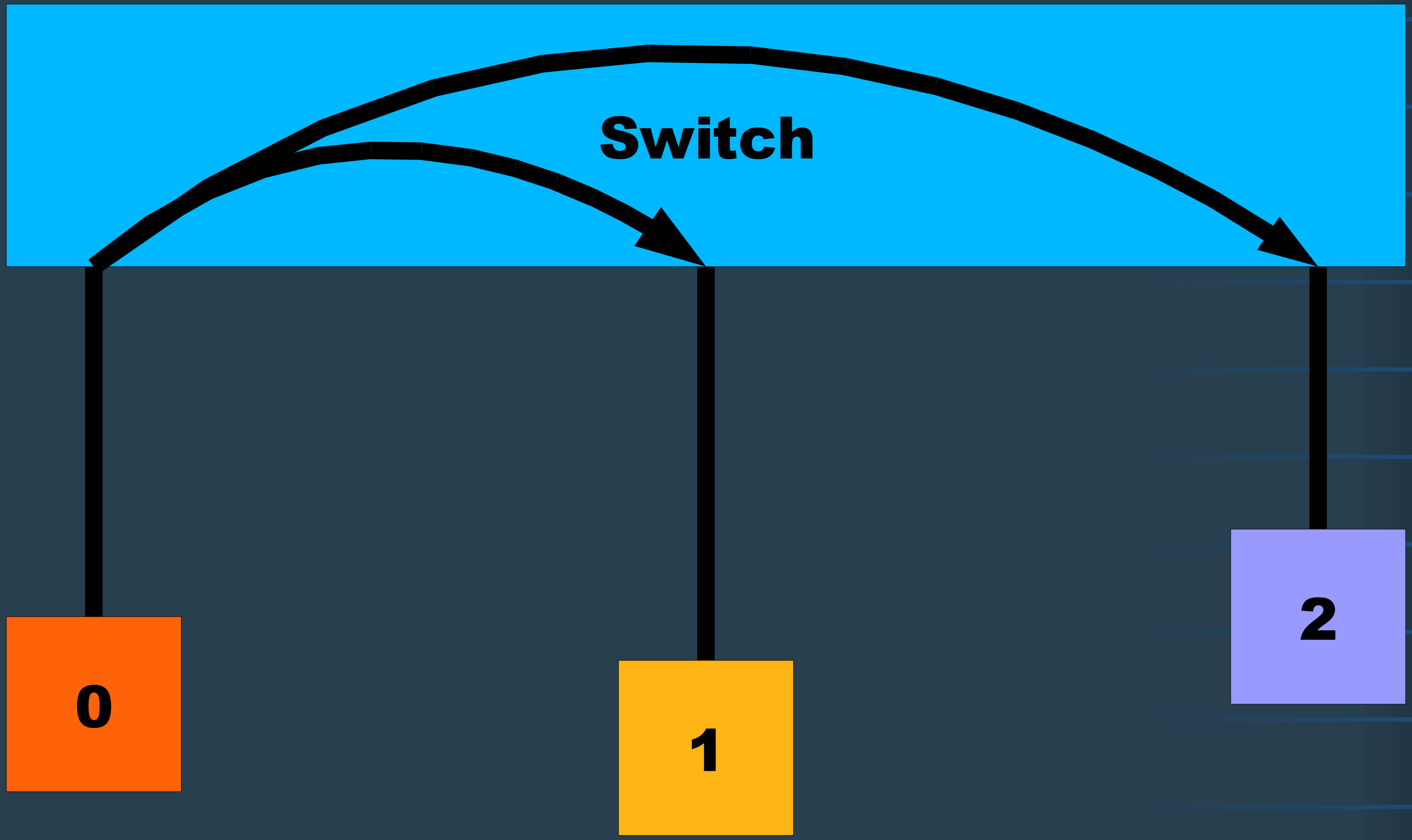
Basics: 802.1d switching

- Processes
  - Forwarding Process
  - Learning Process
- MAC table (Filtering Database)
  - CAM memory
  - MAC – port entries

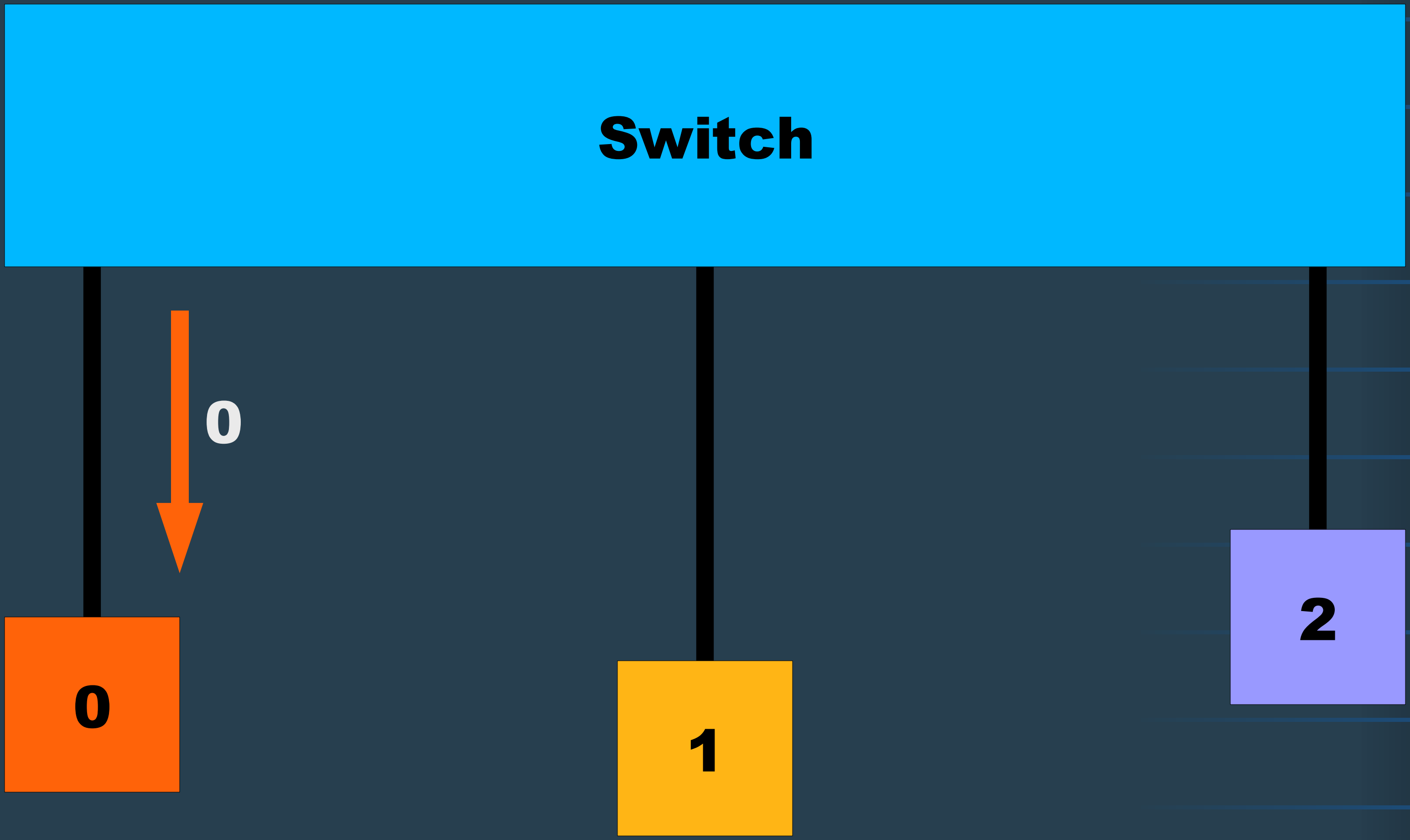
Basics: switch 1/5



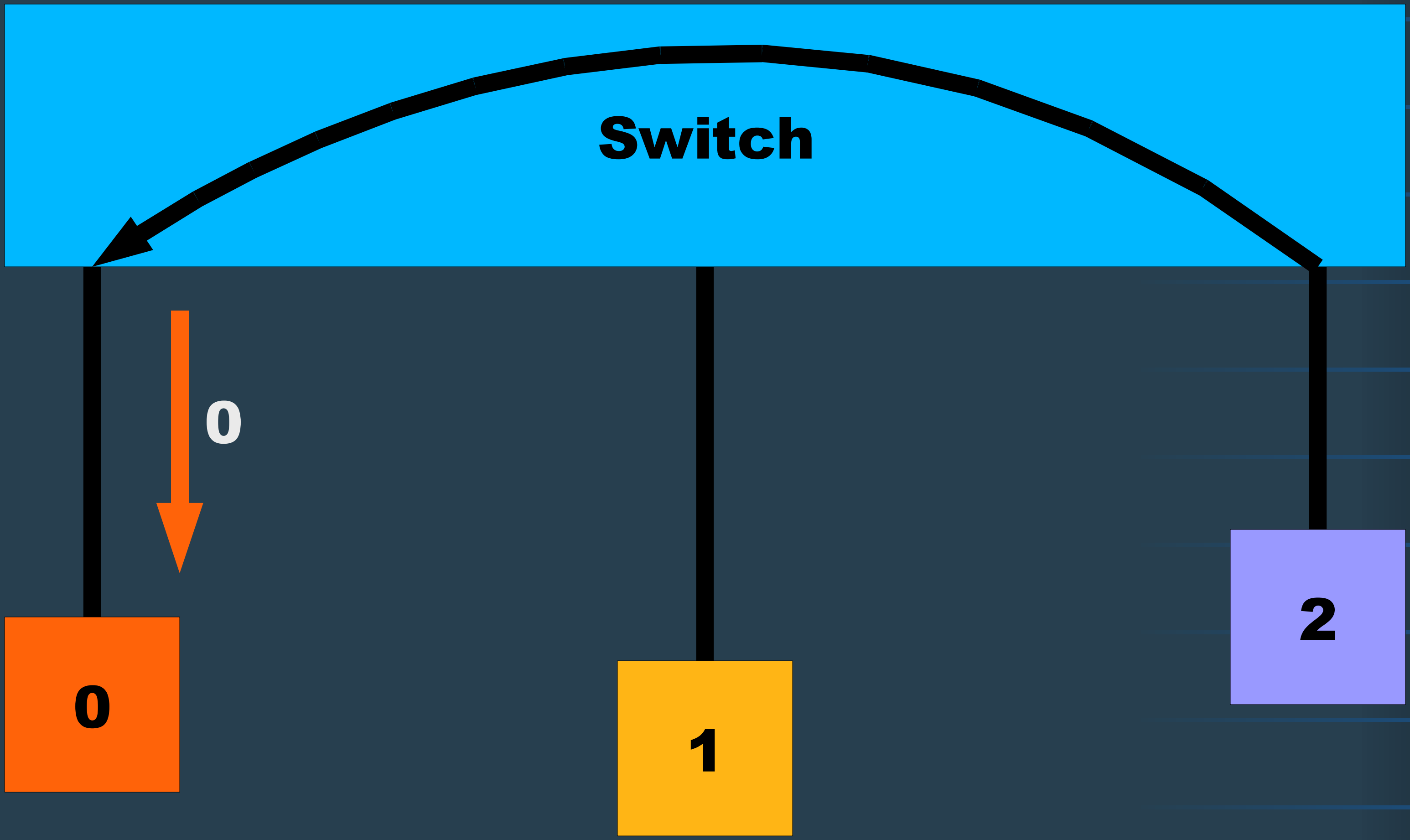
Basics: switch 2/5



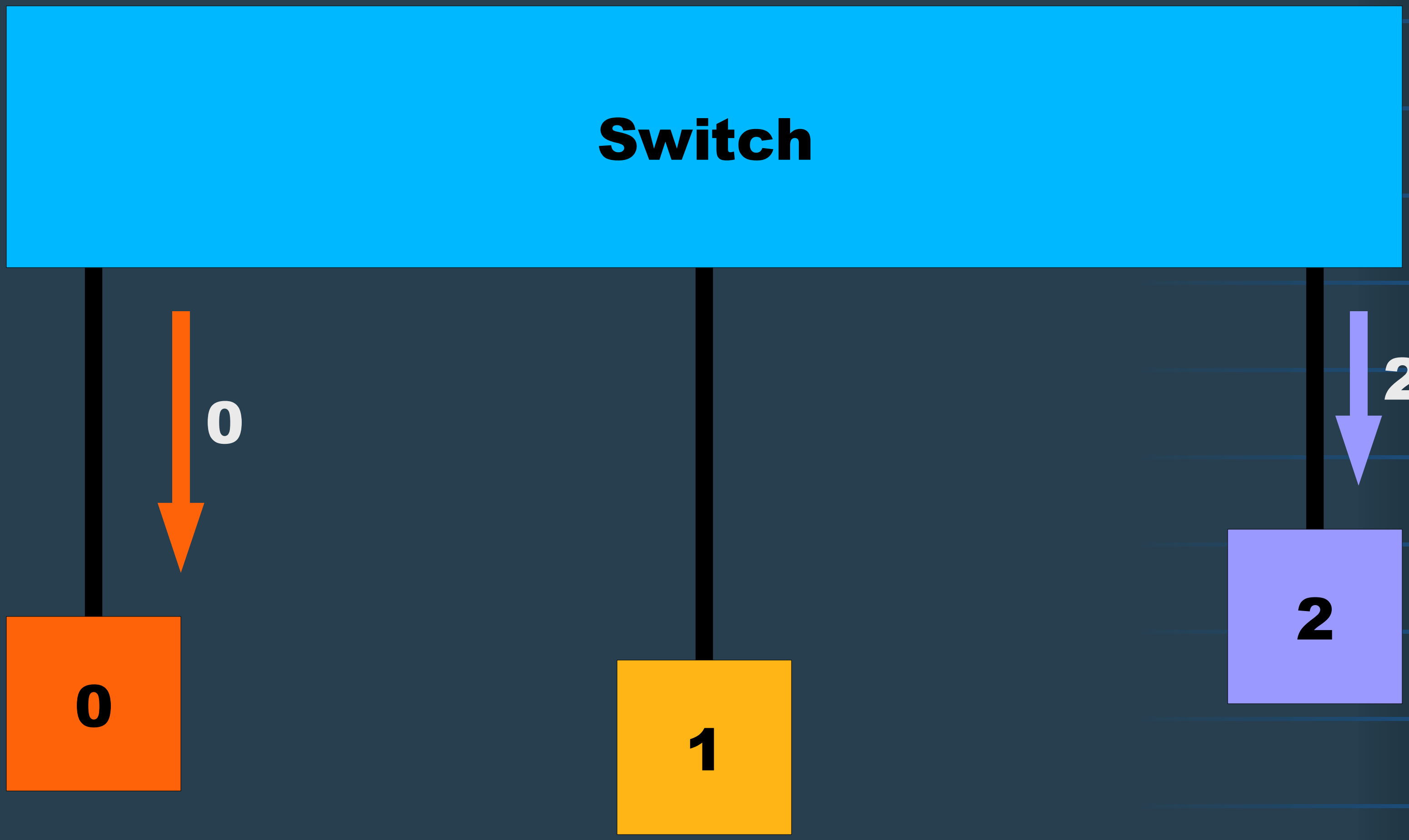
Basics: switch 3/5



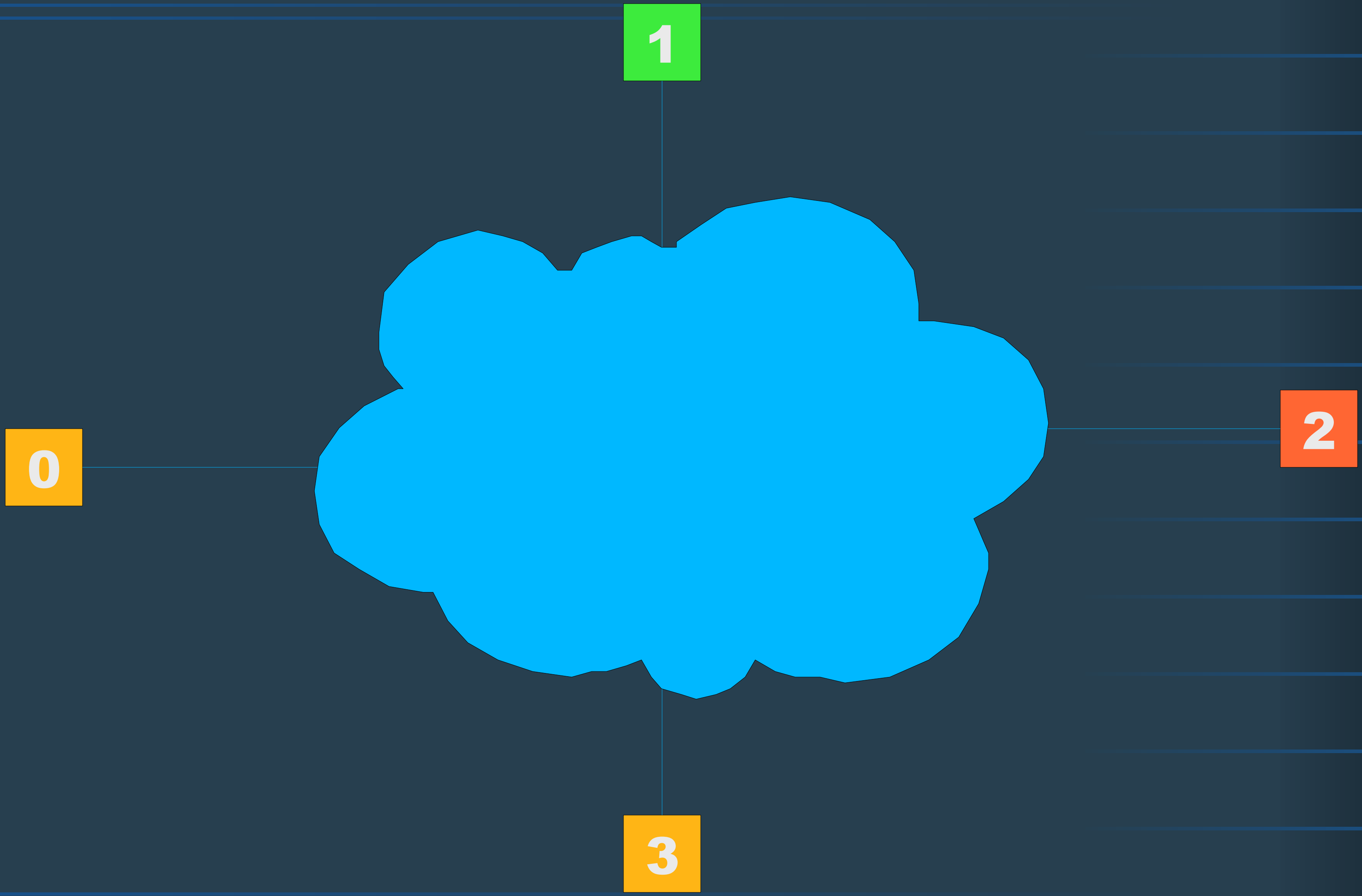
Basics: switch 4/5



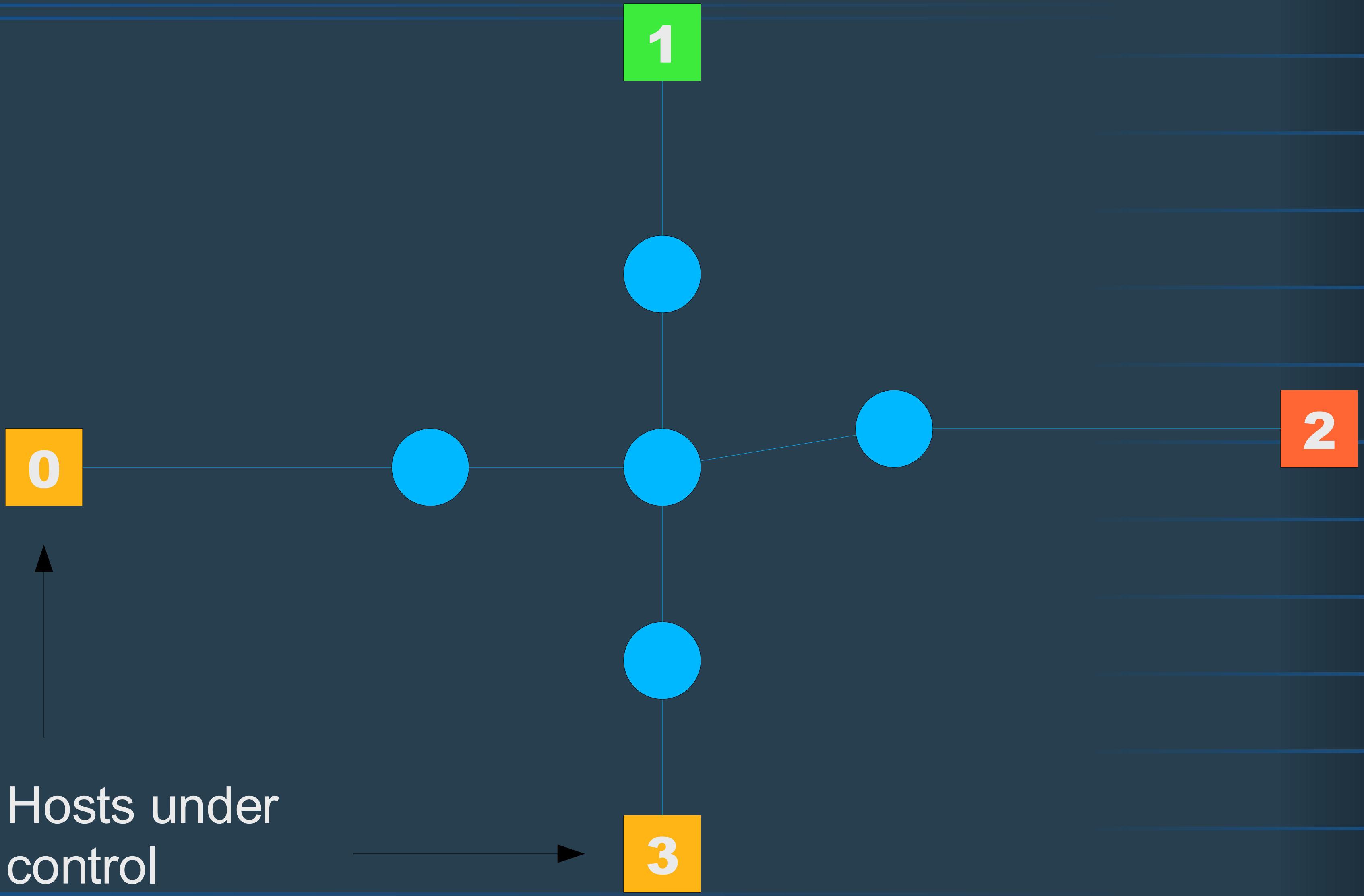
Basics: switch 5/5



Network structure identification

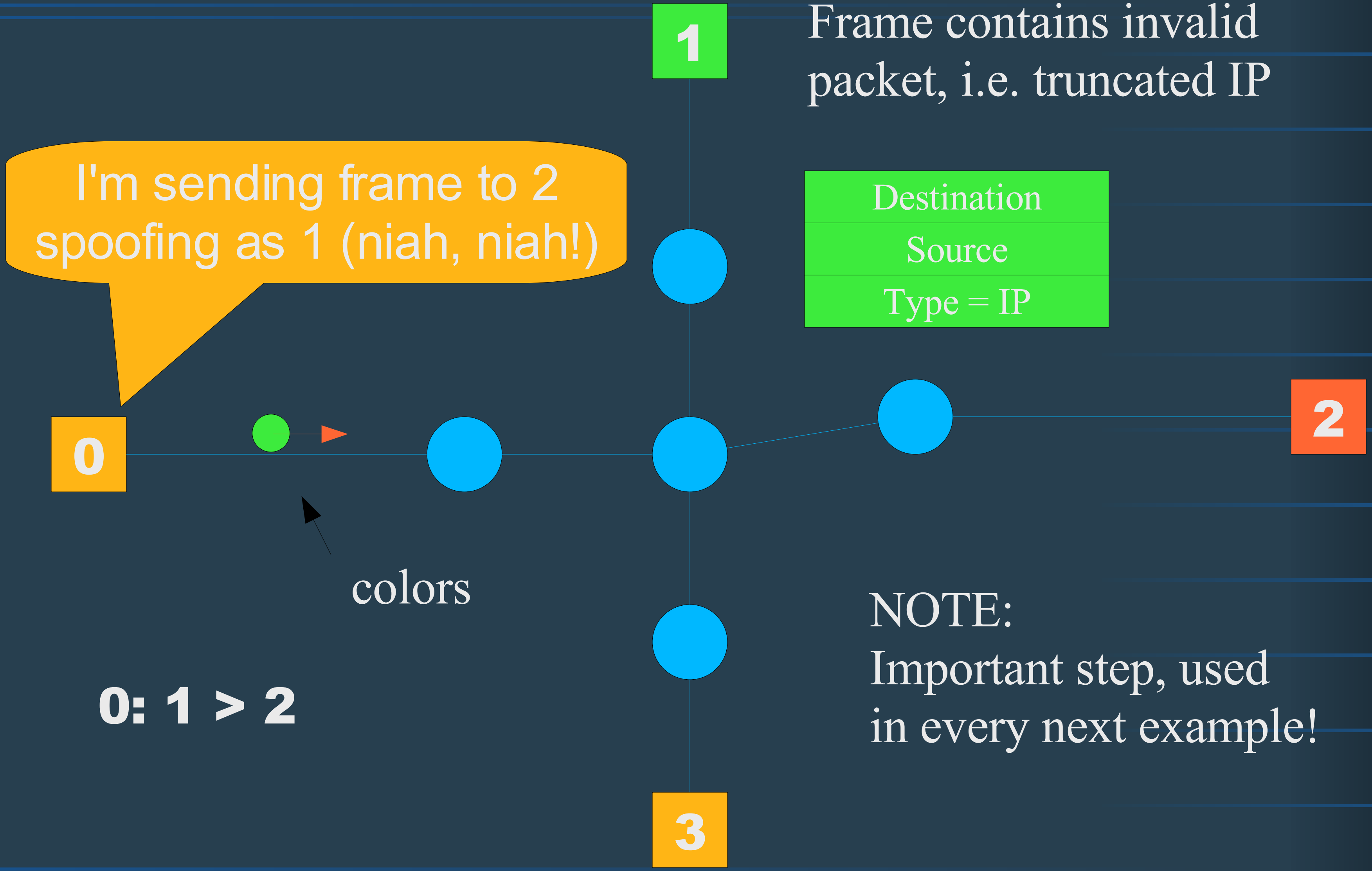


Network structure identification



Hosts under control

Network structure identification



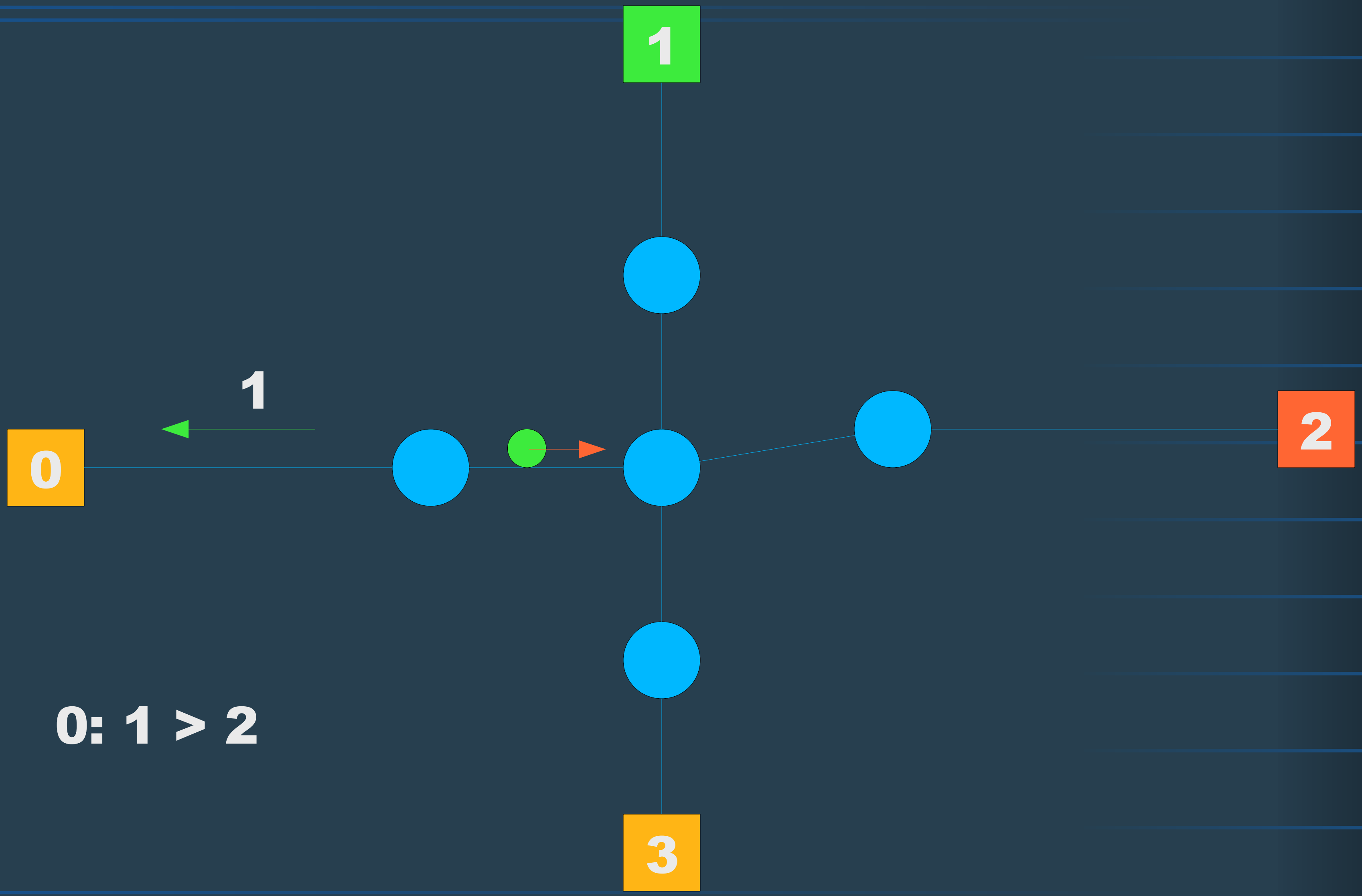
0: 1 > 2

Frame contains invalid packet, i.e. truncated IP

Destination
Source
Type = IP

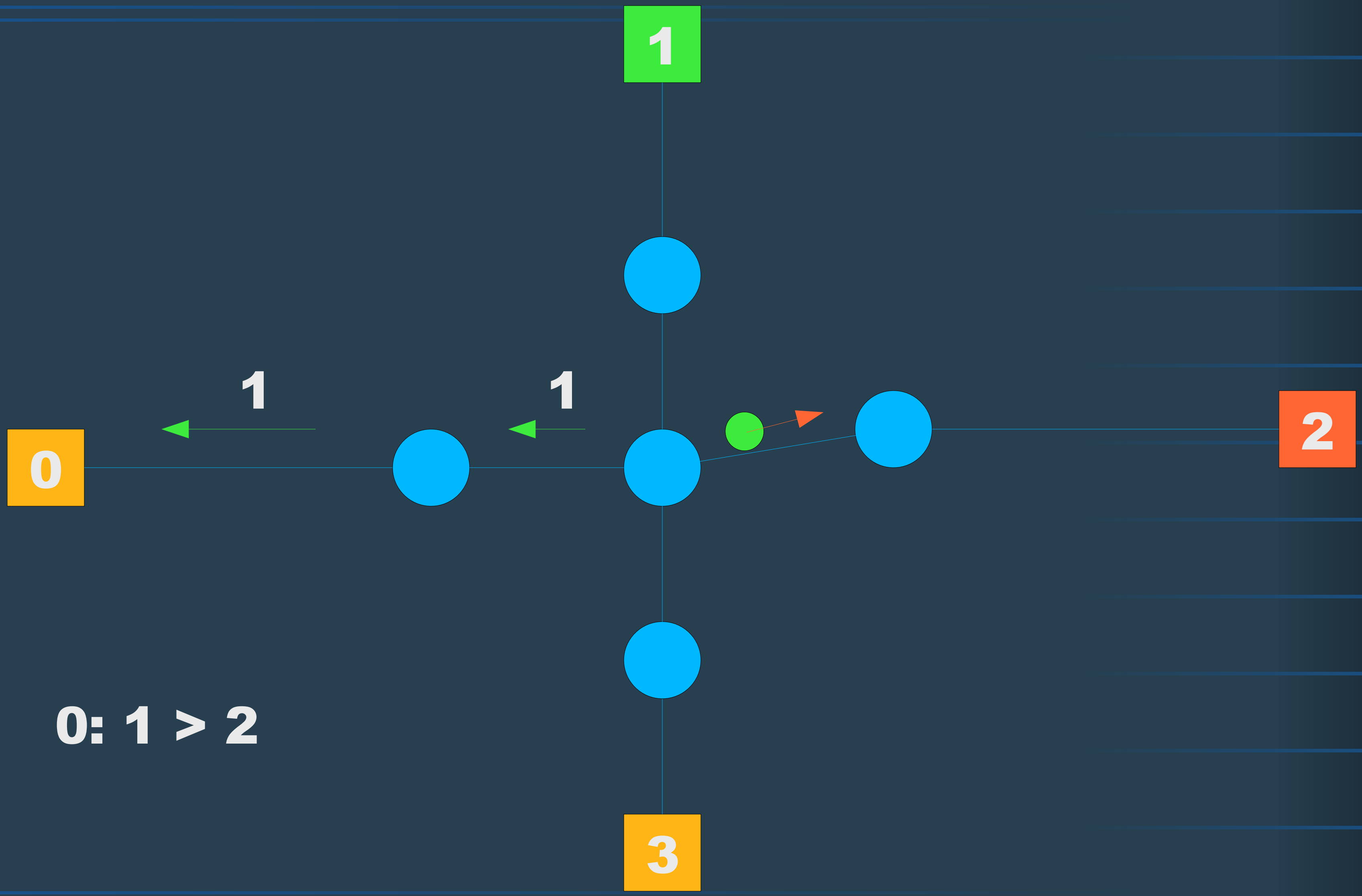
NOTE:
Important step, used
in every next example!

Network structure identification



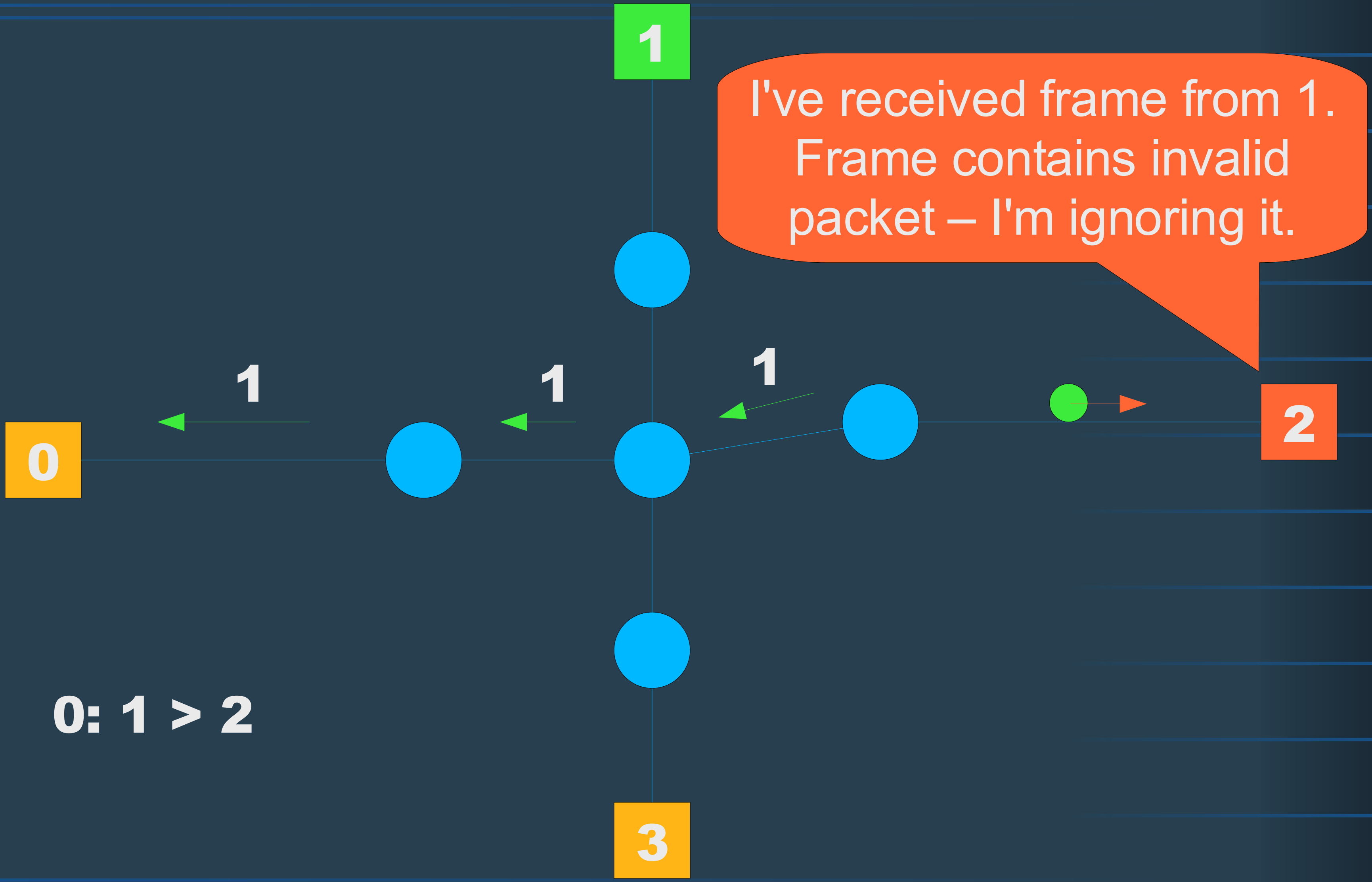
0: 1 > 2

Network structure identification



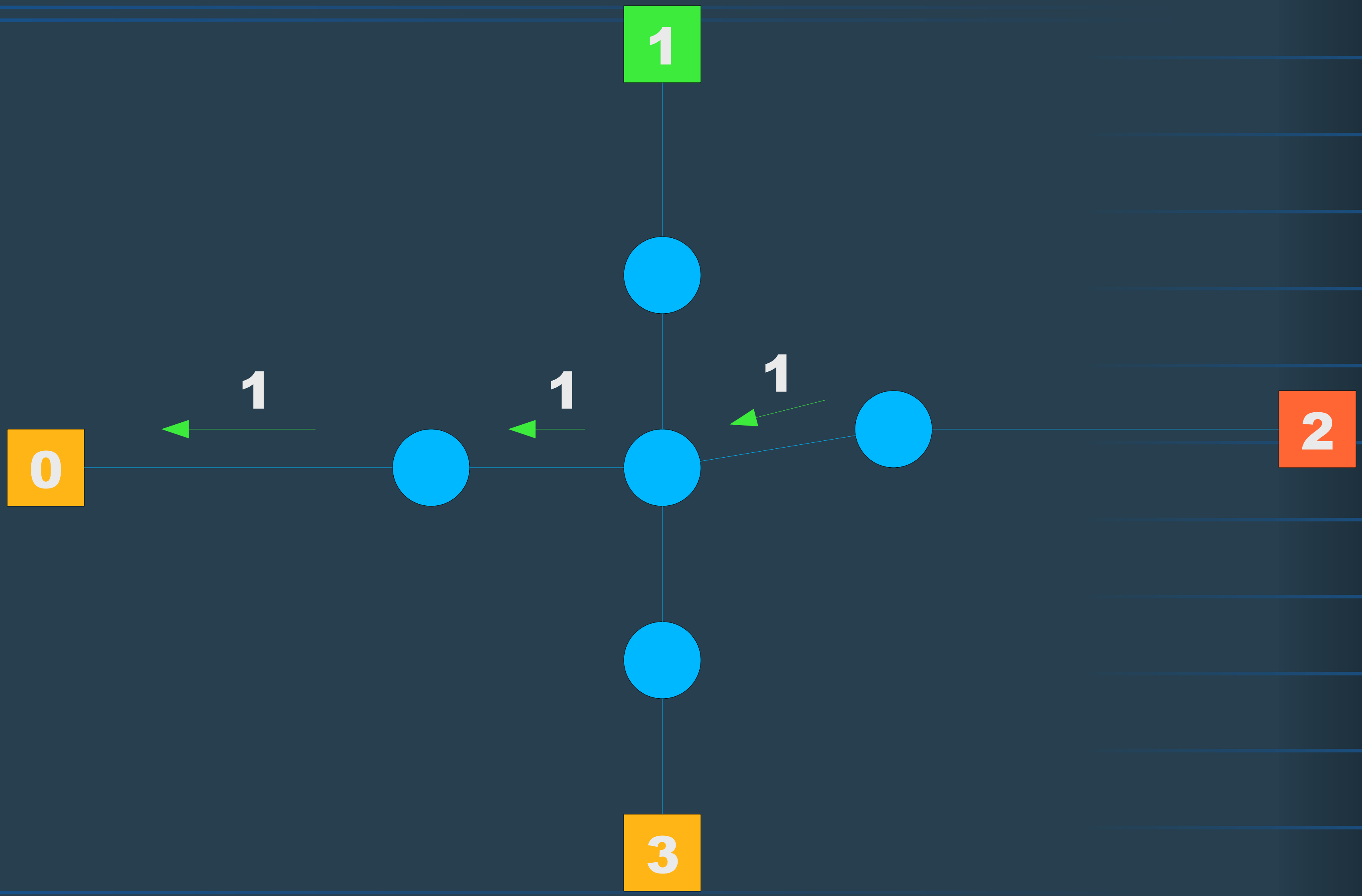
0: 1 > 2

Network structure identification

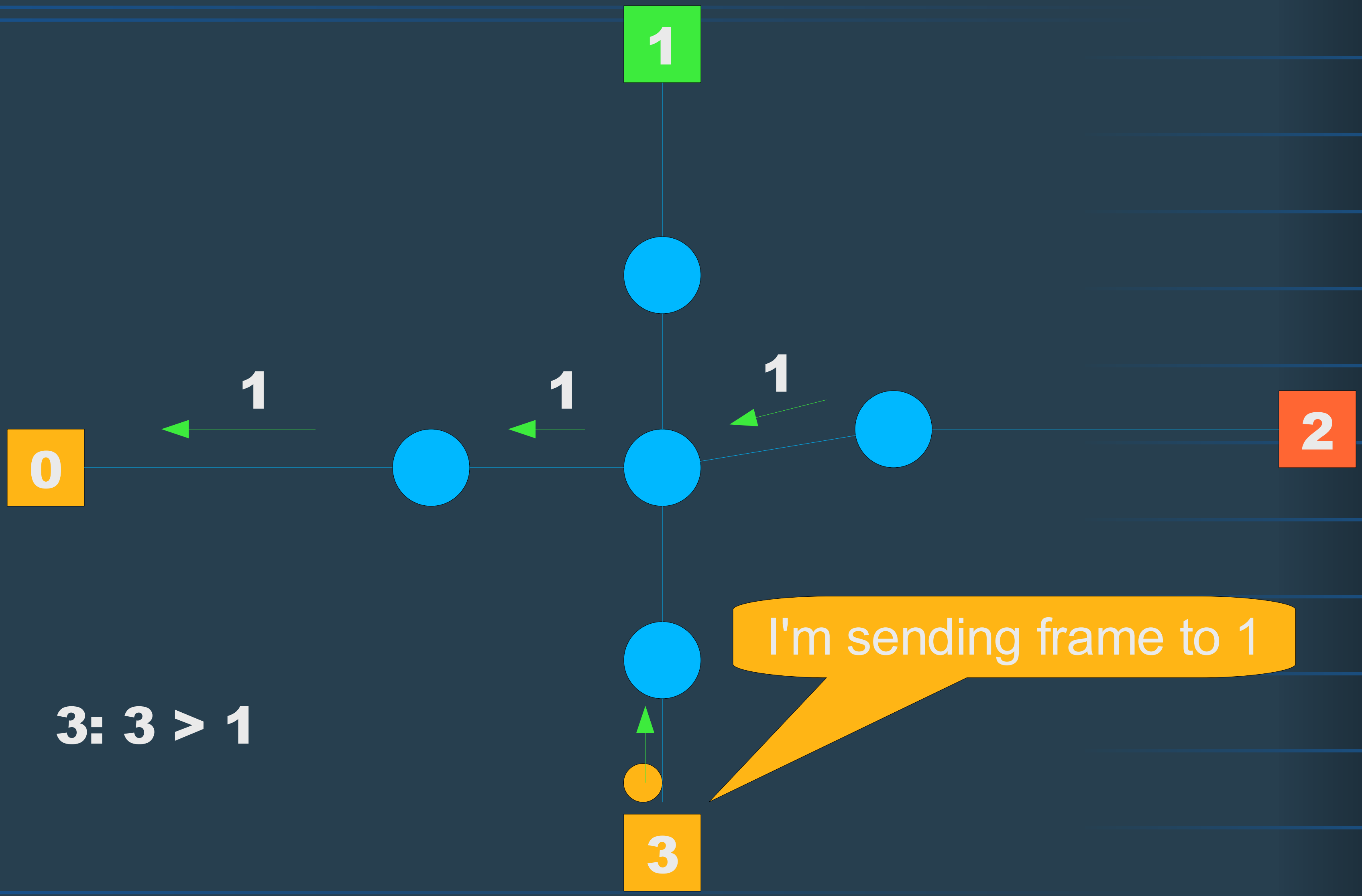


0: 1 > 2

Network structure identification

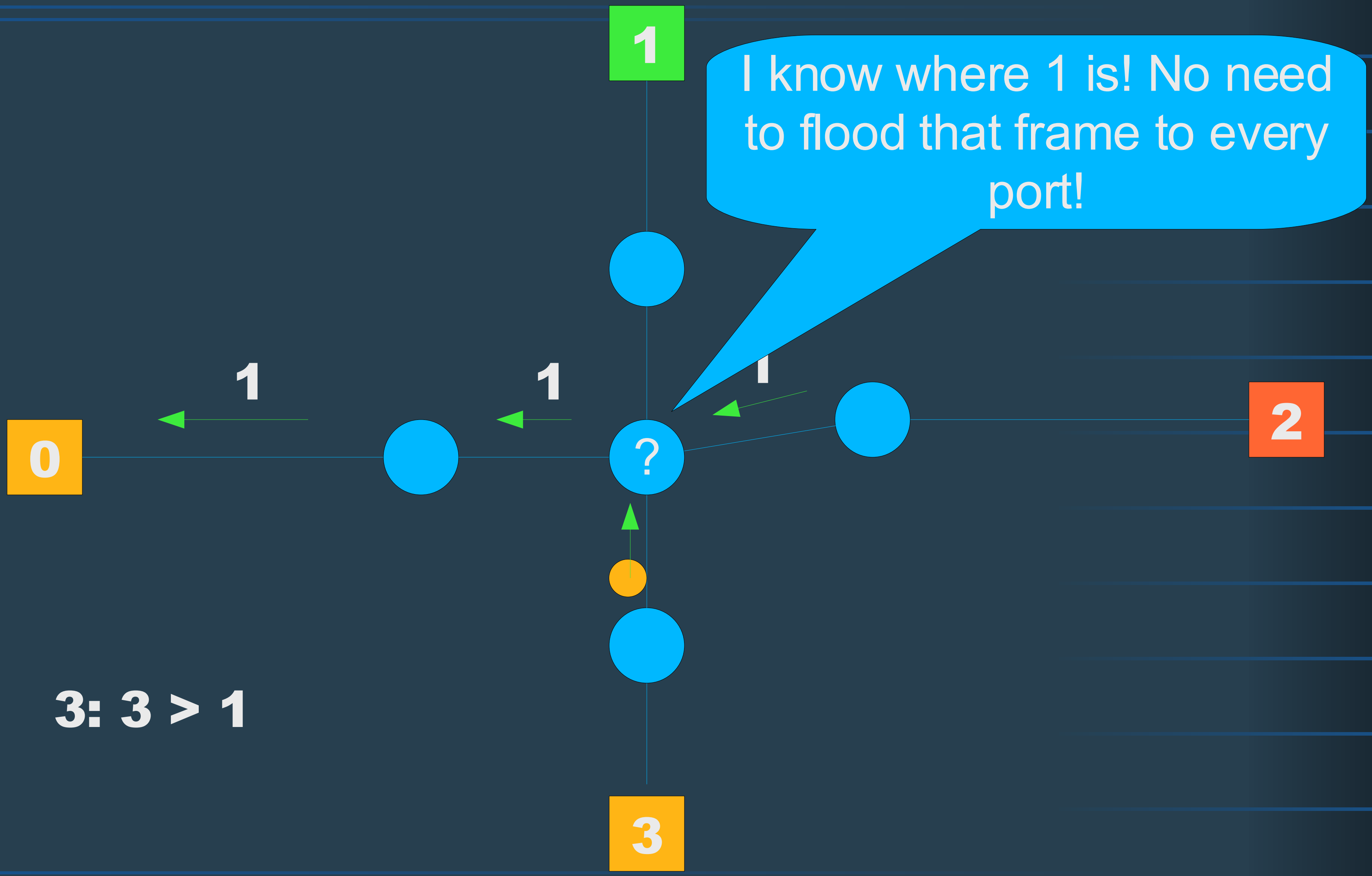


Network structure identification



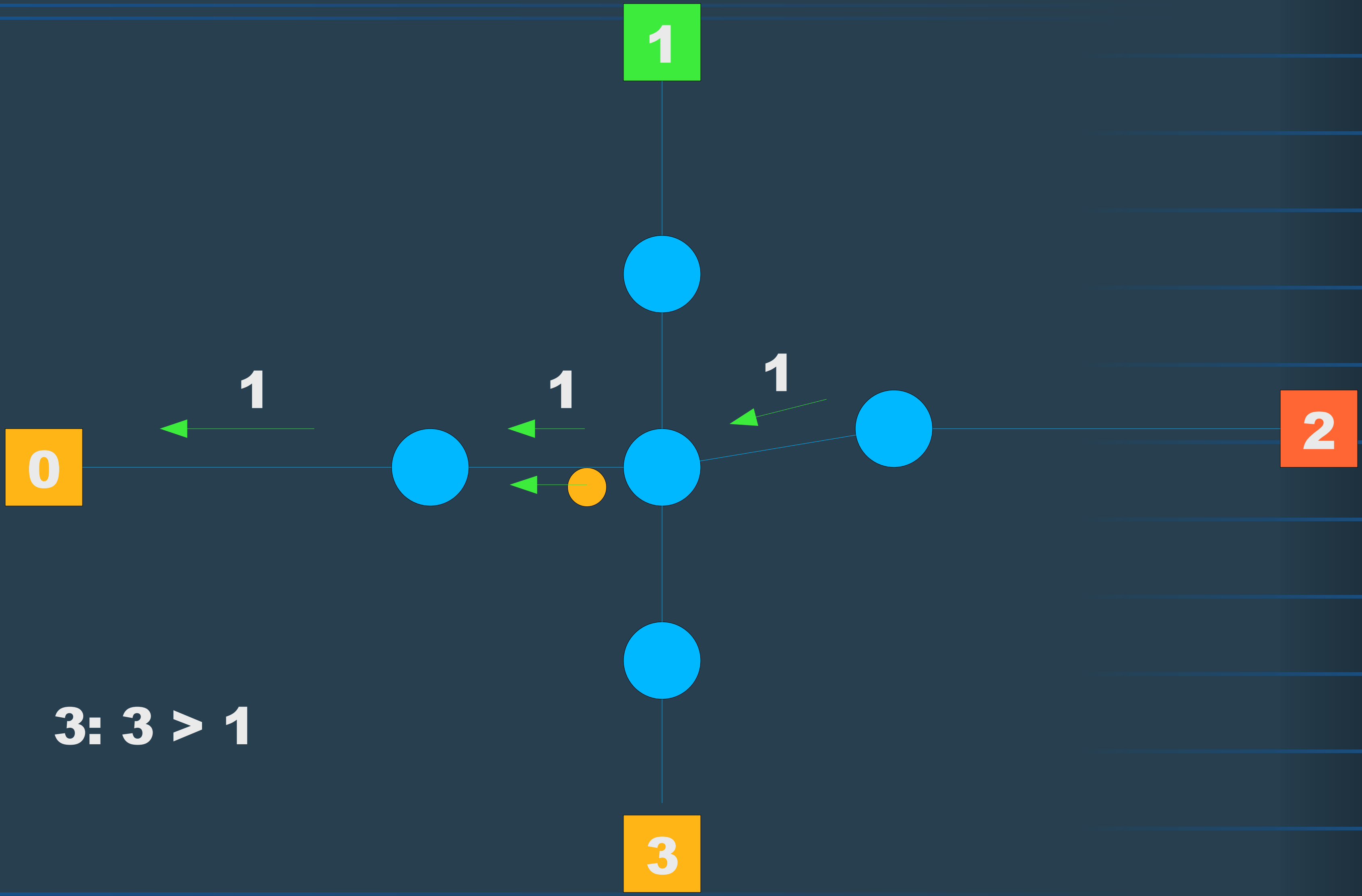
3: 3 > 1

Network structure identification


1
I know where 1 is! No need to flood that frame to every port!
1
1
1
0
?
2
3

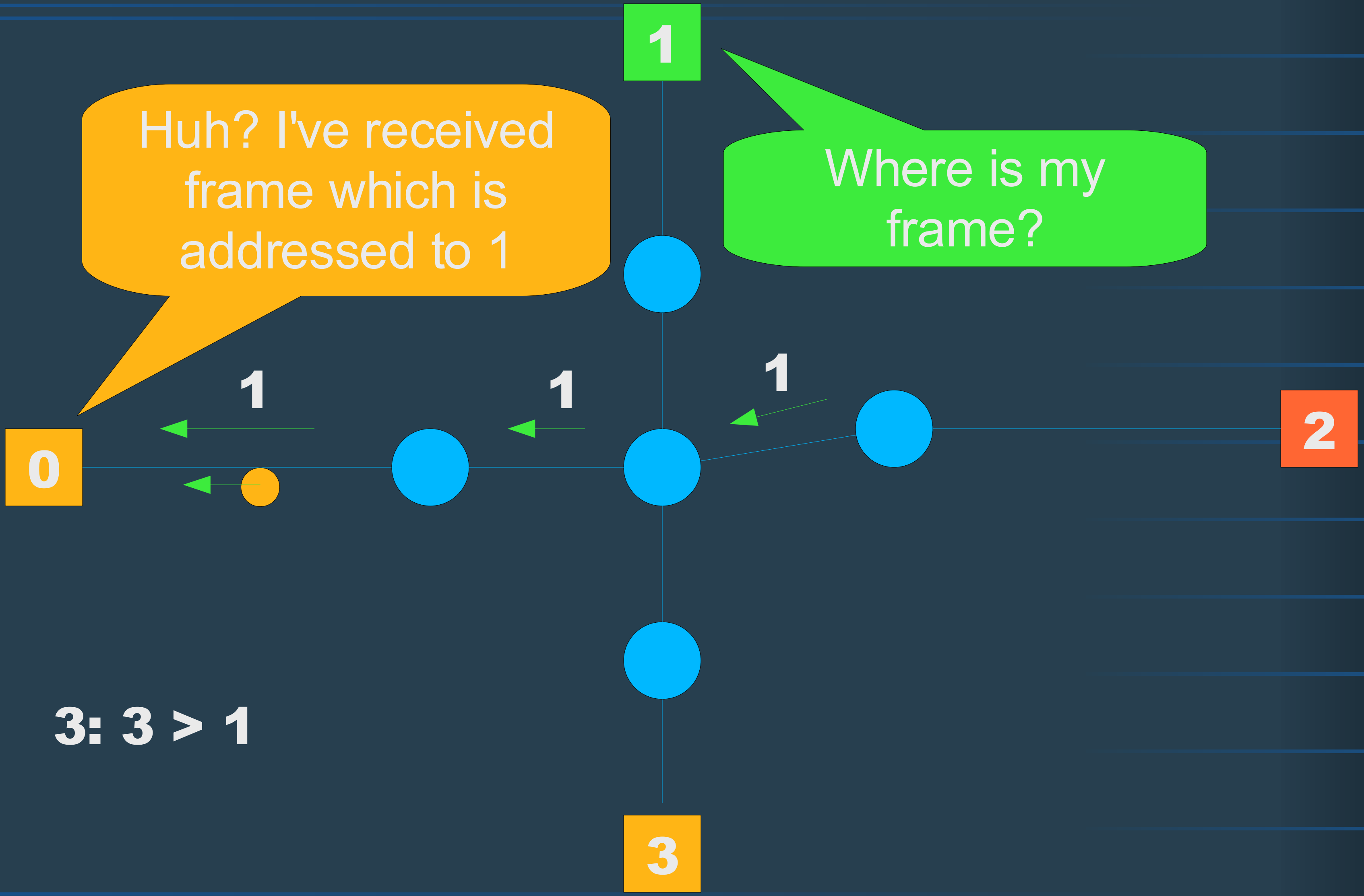
3: 3 > 1

Network structure identification



3: 3 > 1

Network structure identification

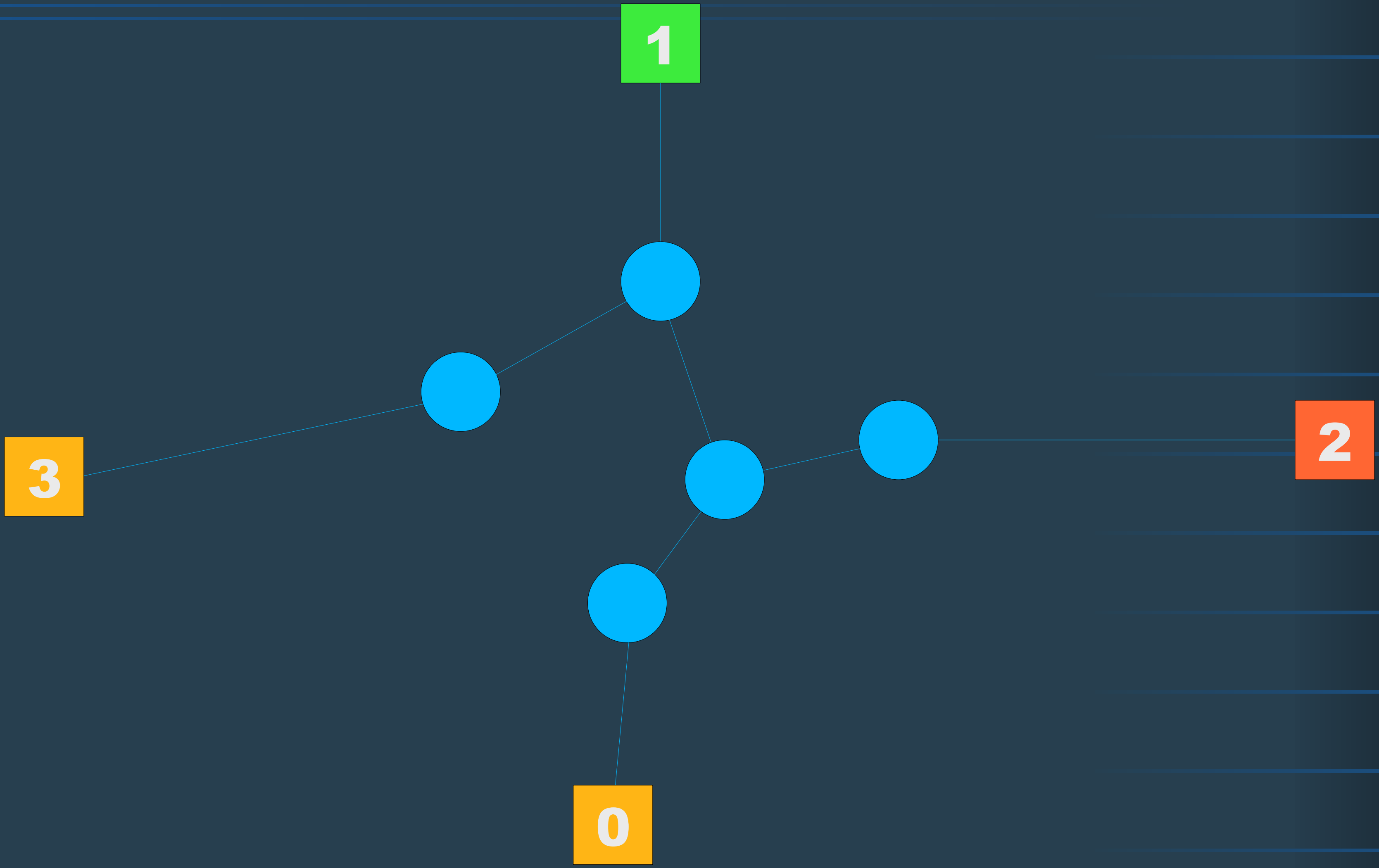


Huh? I've received frame which is addressed to 1

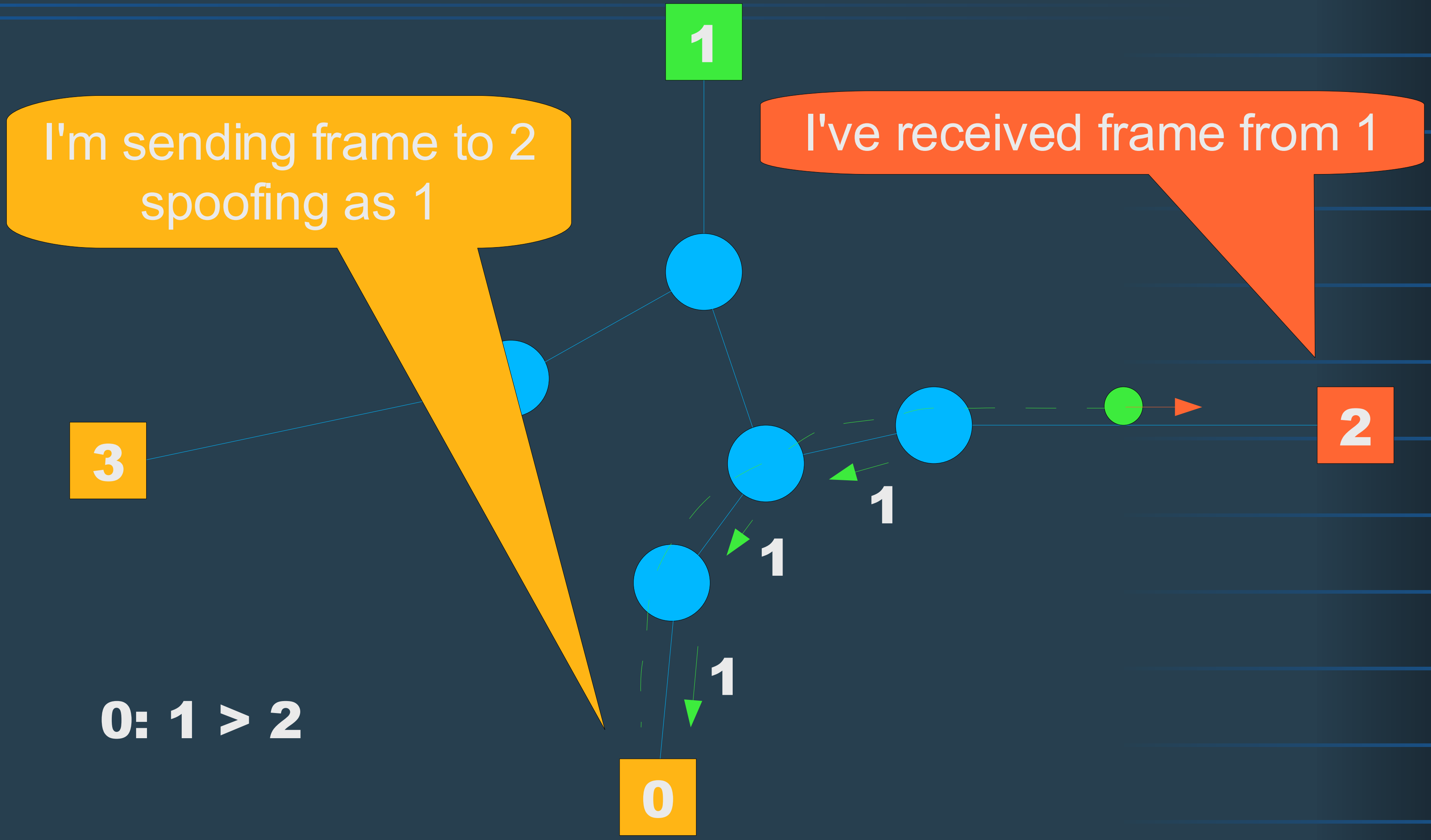
Where is my frame?

3: 3 > 1

Network structure identification 2

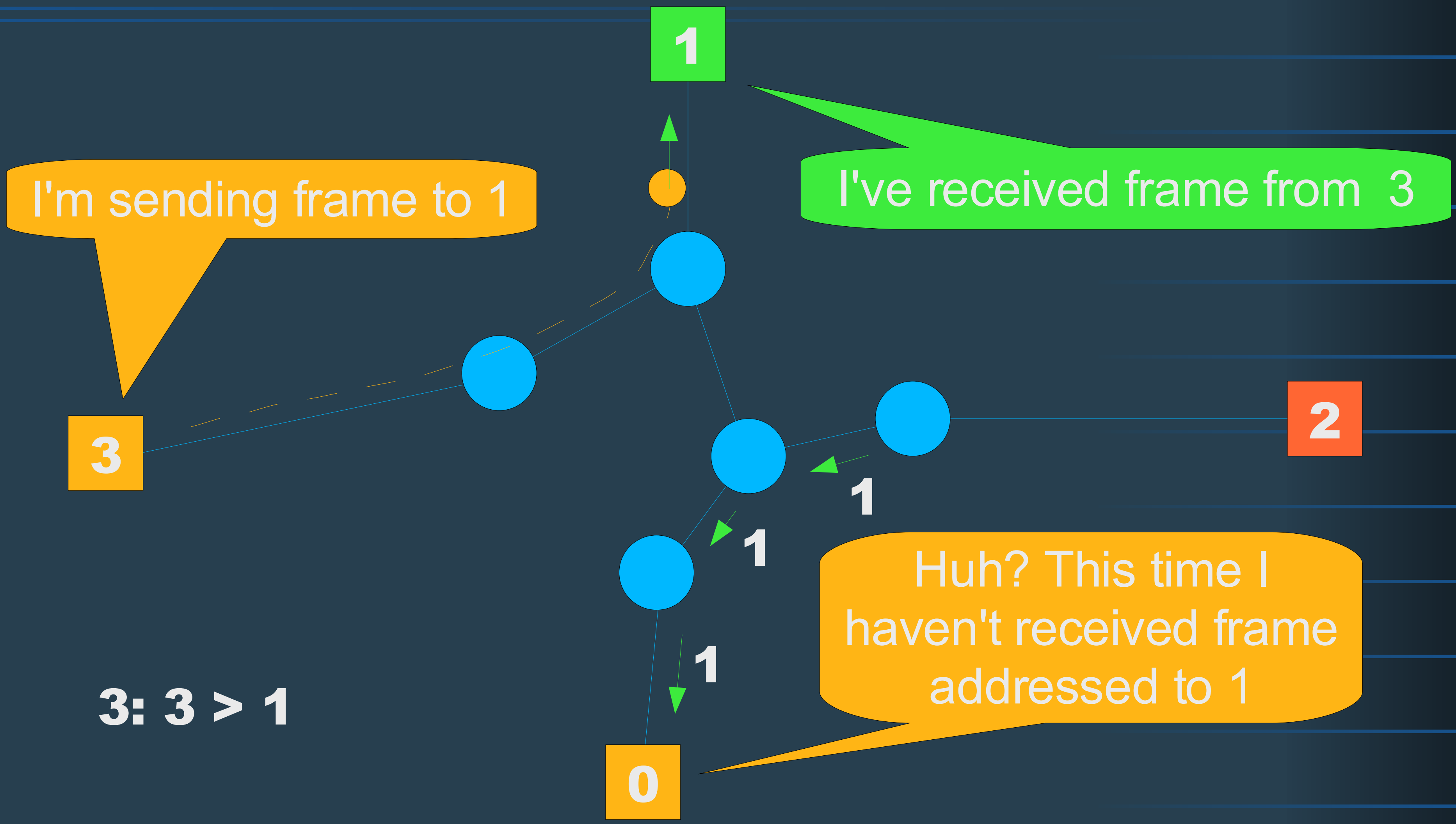


Network structure identification 2


1
I'm sending frame to 2 spoofing as 1
I've received frame from 1
2
3
1
1
1
0

0: 1 > 2

Network structure identification 2

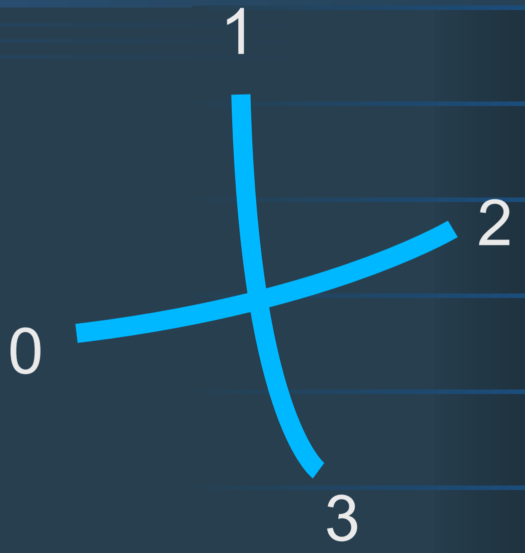


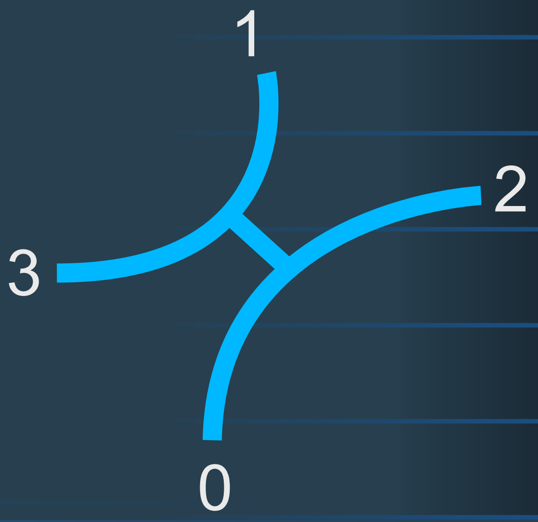
1
I'm sending frame to 1
I've received frame from 3
3
2
1
1
1
Huh? This time I haven't received frame addressed to 1
0

3: 3 > 1

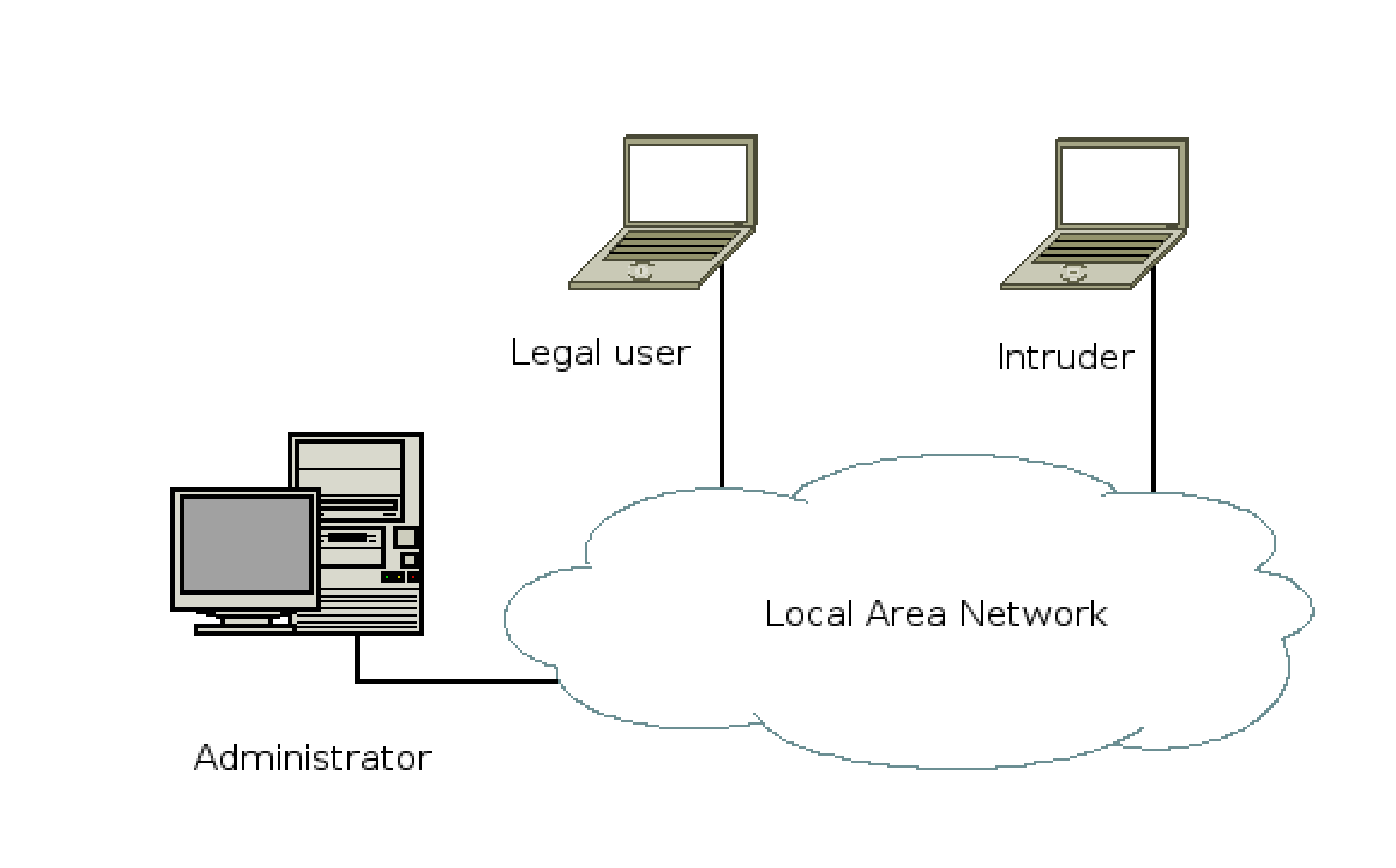
Results interpretation

- It's possible to distinguish between two layouts
- Repeating test with different hosts = network map
- Shortcomings
  - need to control 2 hosts
  - need to control every or almost every host to create network map



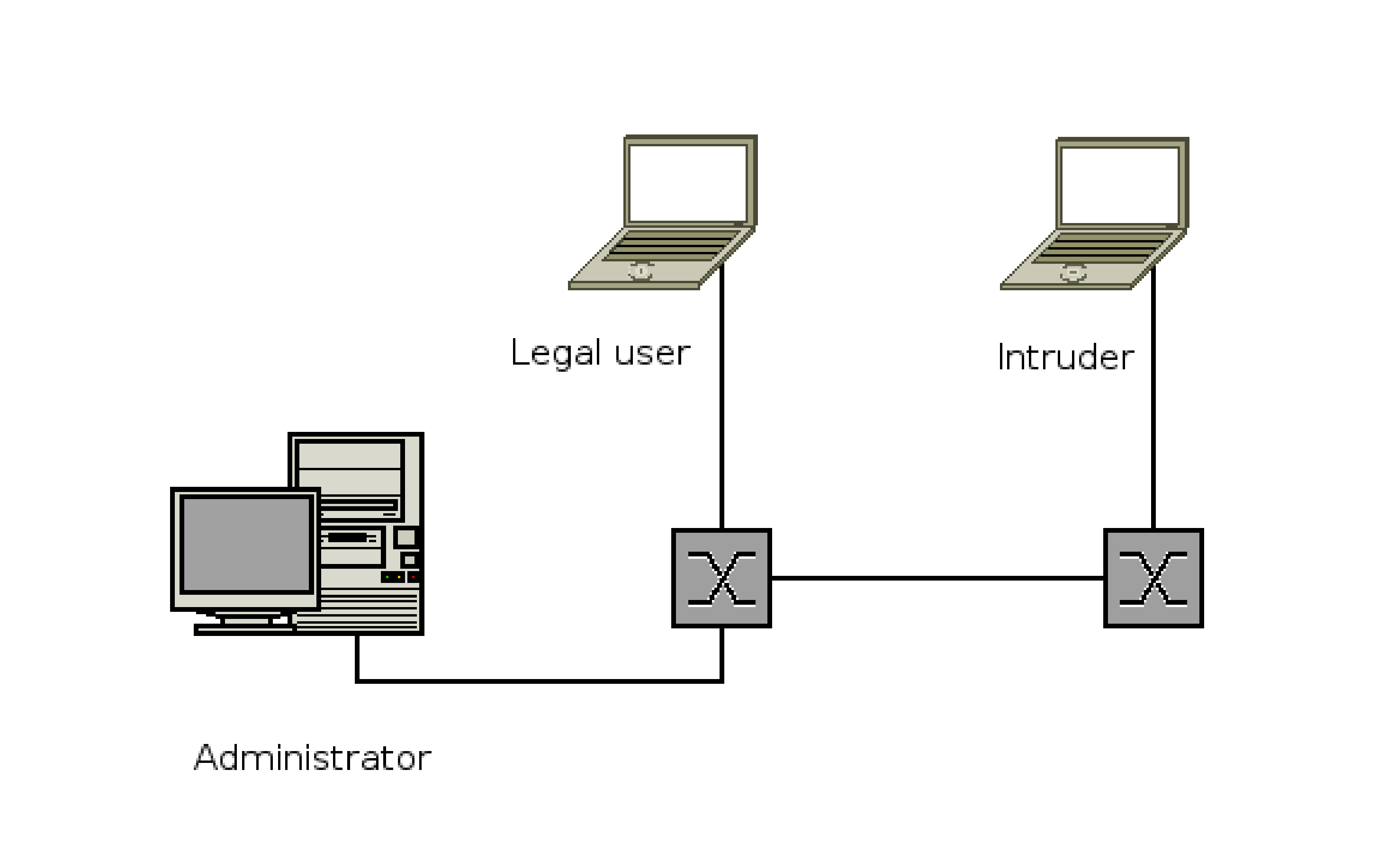


Demonstration: Etherbat



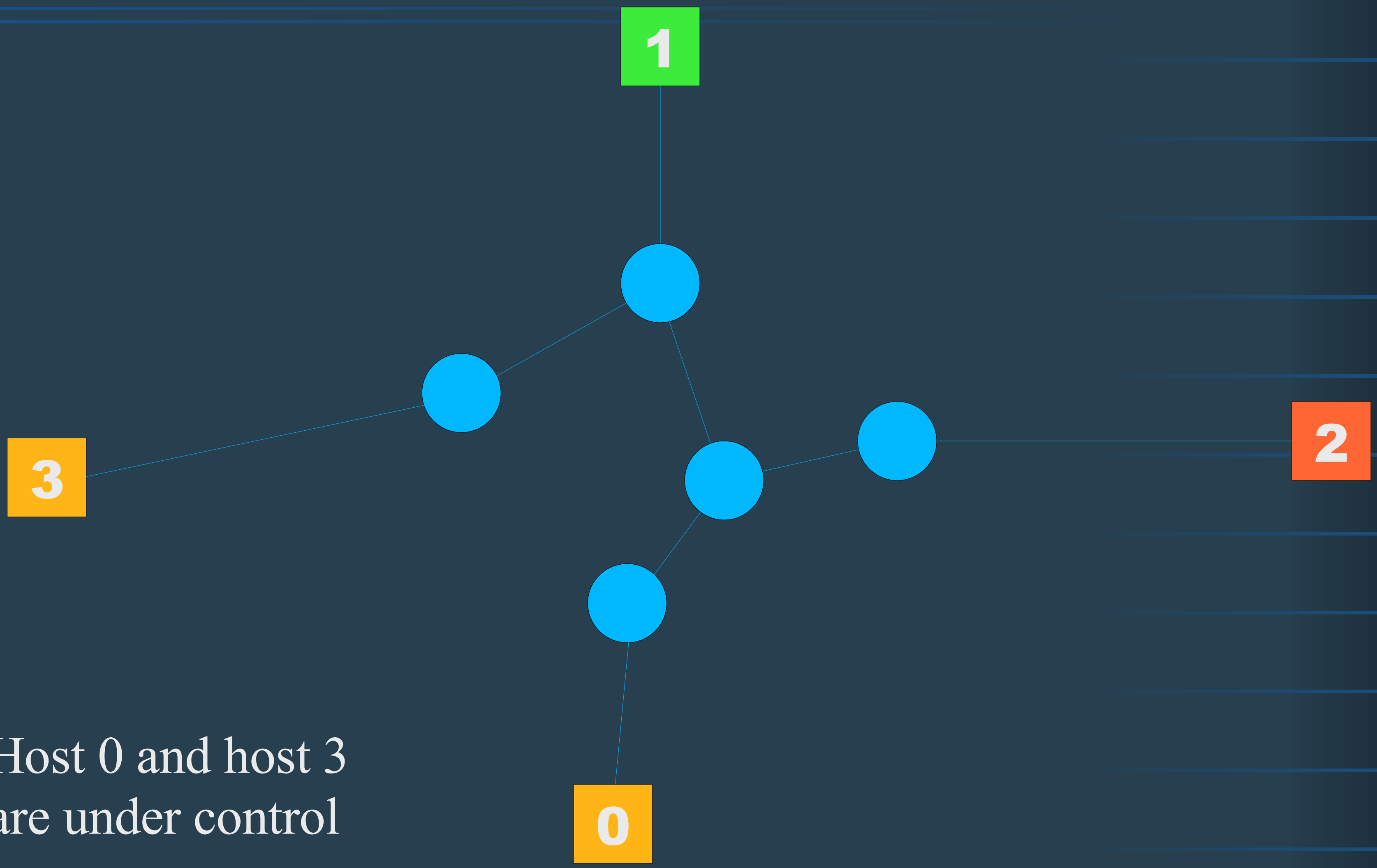
Administrator knows how switches are interconnected, but he doesn't know to which one intruder is connected.

Demonstration: Etherbat



Administrator knows how switches are interconnected, but he doesn't know to which one intruder is connected.

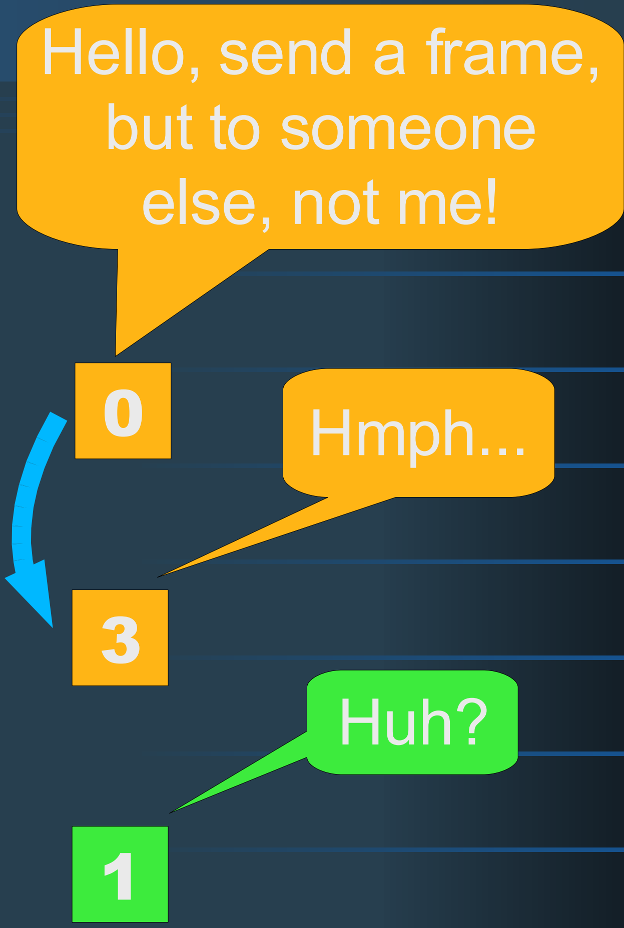
Remember: the network looks like this



Host 0 and host 3
are under control

Idea

- Is it possible to ask 3 to send frame to 1?
  - MAC spoofing, SA=3?
    - does not make sense when path to 1 is faked
  - if it would then there is no need to control 3
    - test would be simpler!



Hello, send a frame, but to someone else, not me!

0

Hmph...

3

Huh?

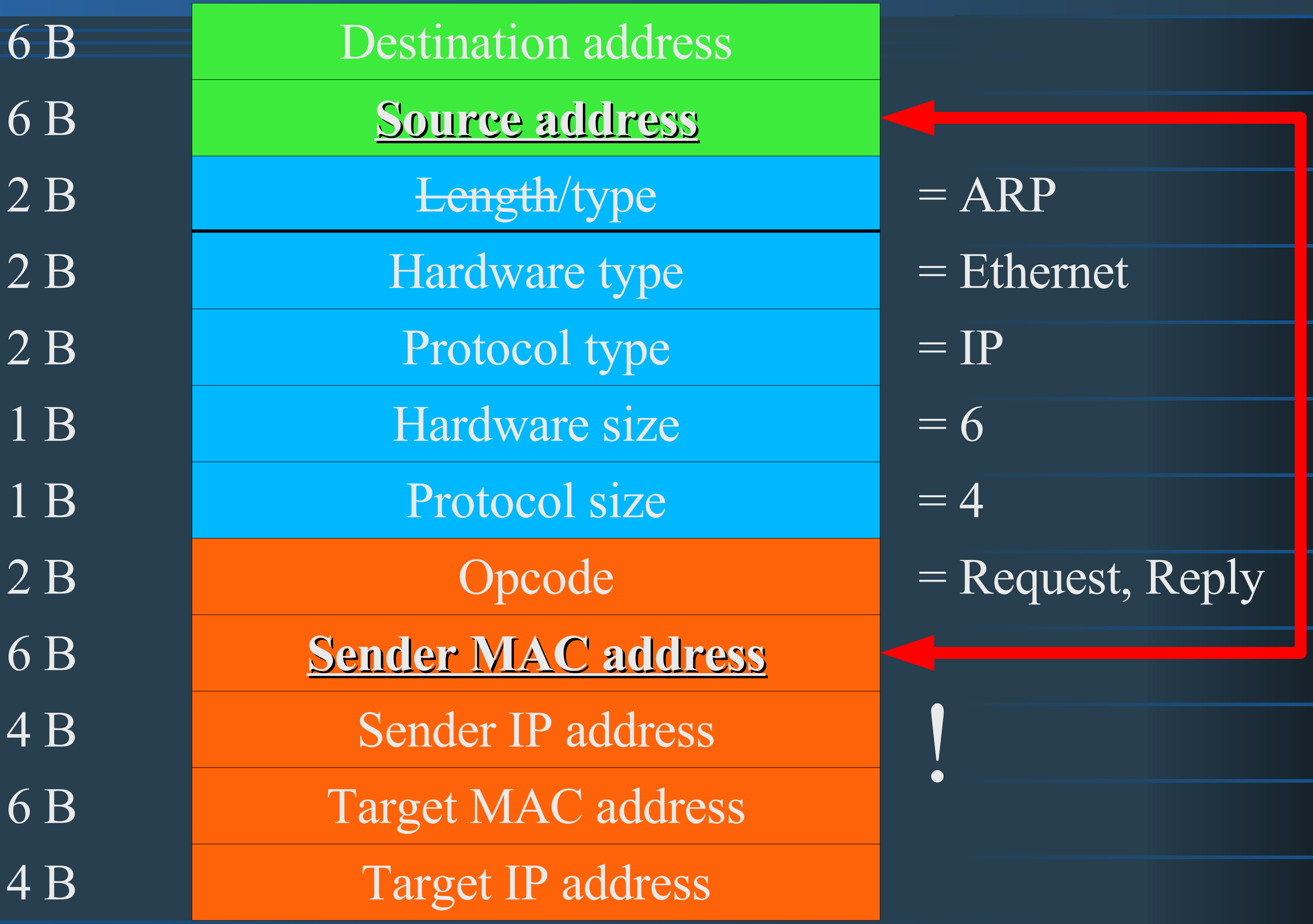
1

ARP packet

To all: Who has IP=X?
X replies: I have this address, my MAC is xx:xx:xx

2 B	Hardware type	= Ethernet
2 B	Protocol type	= IP
1 B	Hardware size	= 6
1 B	Protocol size	= 4
2 B	Opcode	= Request, Reply
6 B	Sender MAC address	
4 B	Sender IP address	
6 B	Target MAC address	
4 B	Target IP address	

Frame with ARP packet

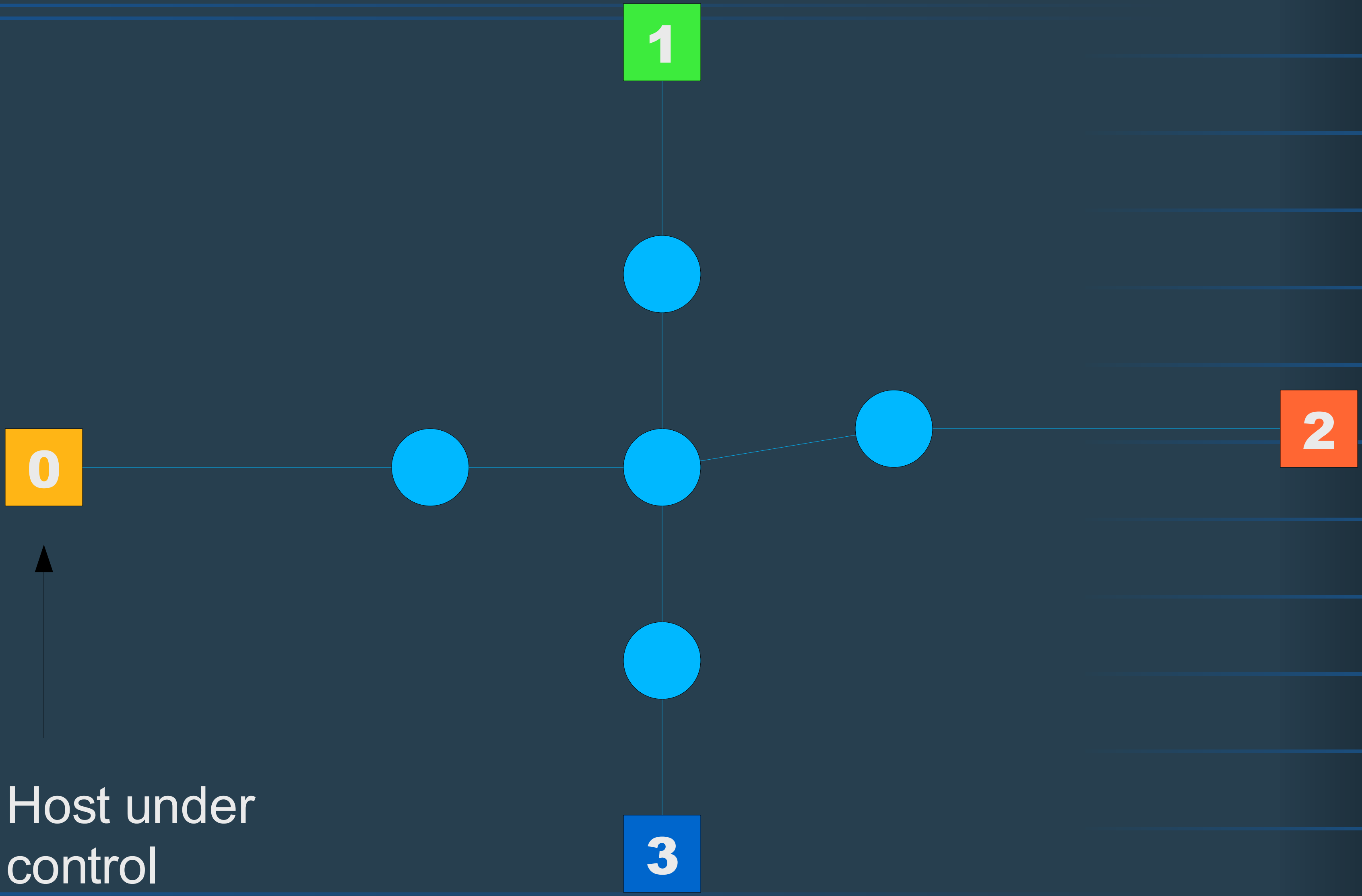


6 B	Destination address	
6 B	**Source address**	
2 B	~~Length~~/type	= ARP
2 B	Hardware type	= Ethernet
2 B	Protocol type	= IP
1 B	Hardware size	= 6
1 B	Protocol size	= 4
2 B	Opcode	= Request, Reply
6 B	**Sender MAC address**	
4 B	Sender IP address	!
6 B	Target MAC address	
4 B	Target IP address	

“Asymetric” ARP Request

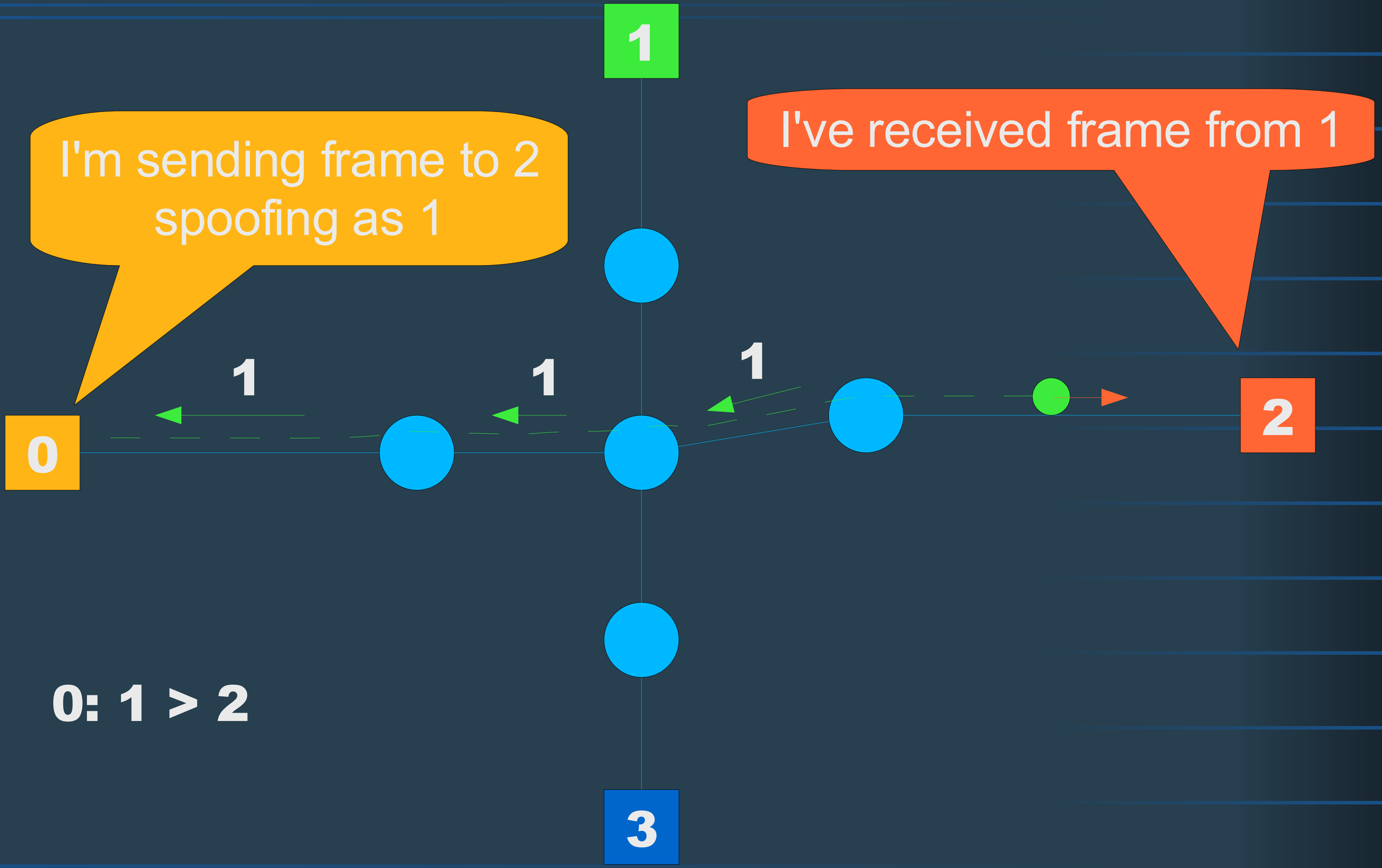
- Source address in frame != source address in ARP Packet
- Reply will be send to address from ARP Packet, not the one specified in frame!
- Ask someone to do a “DoS”

Network structure identification 3



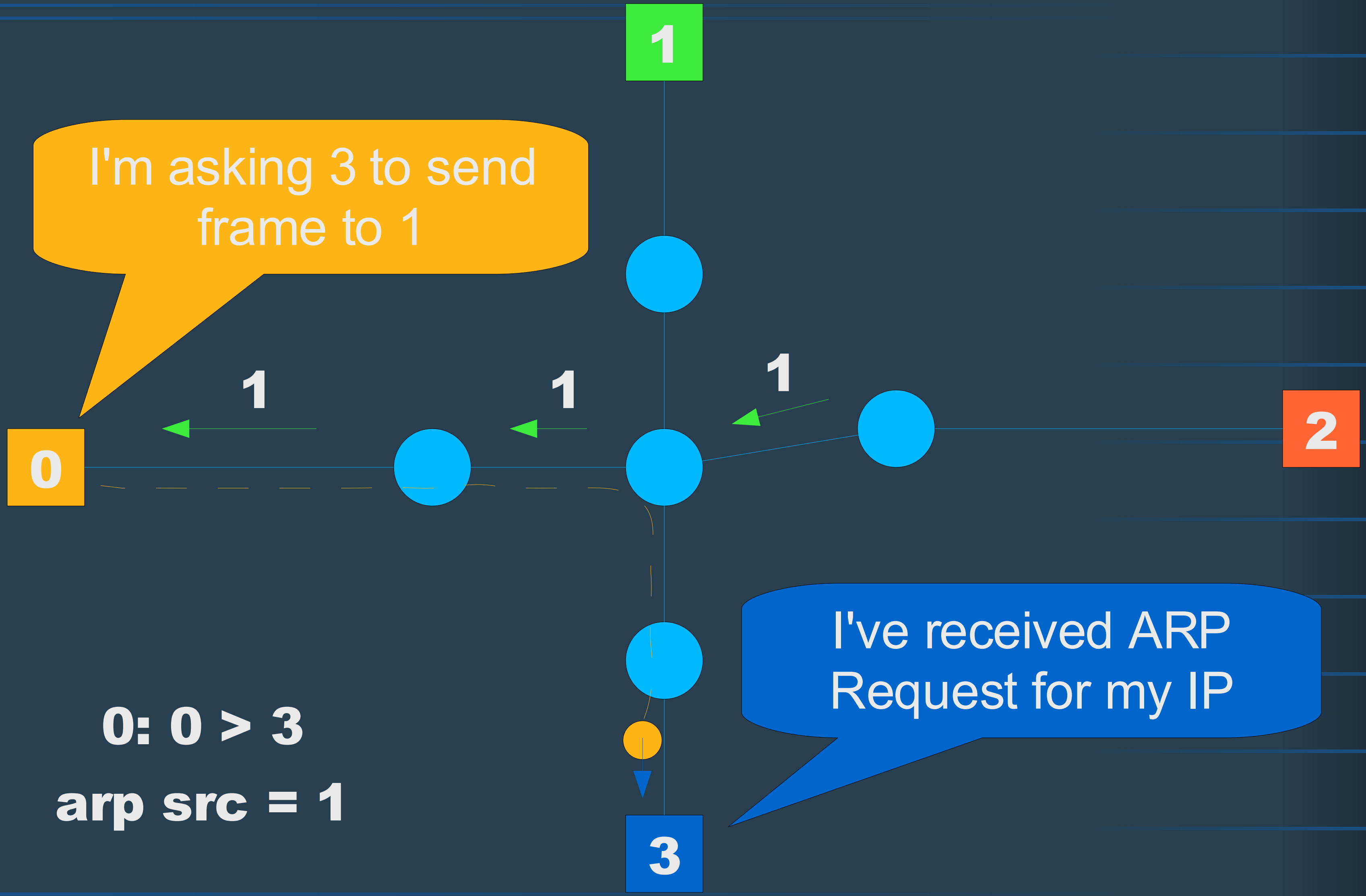
Host under control

Network structure identification 3


1
I've received frame from 1
I'm sending frame to 2 spoofing as 1
1
1
1
0
2
3

0: 1 > 2

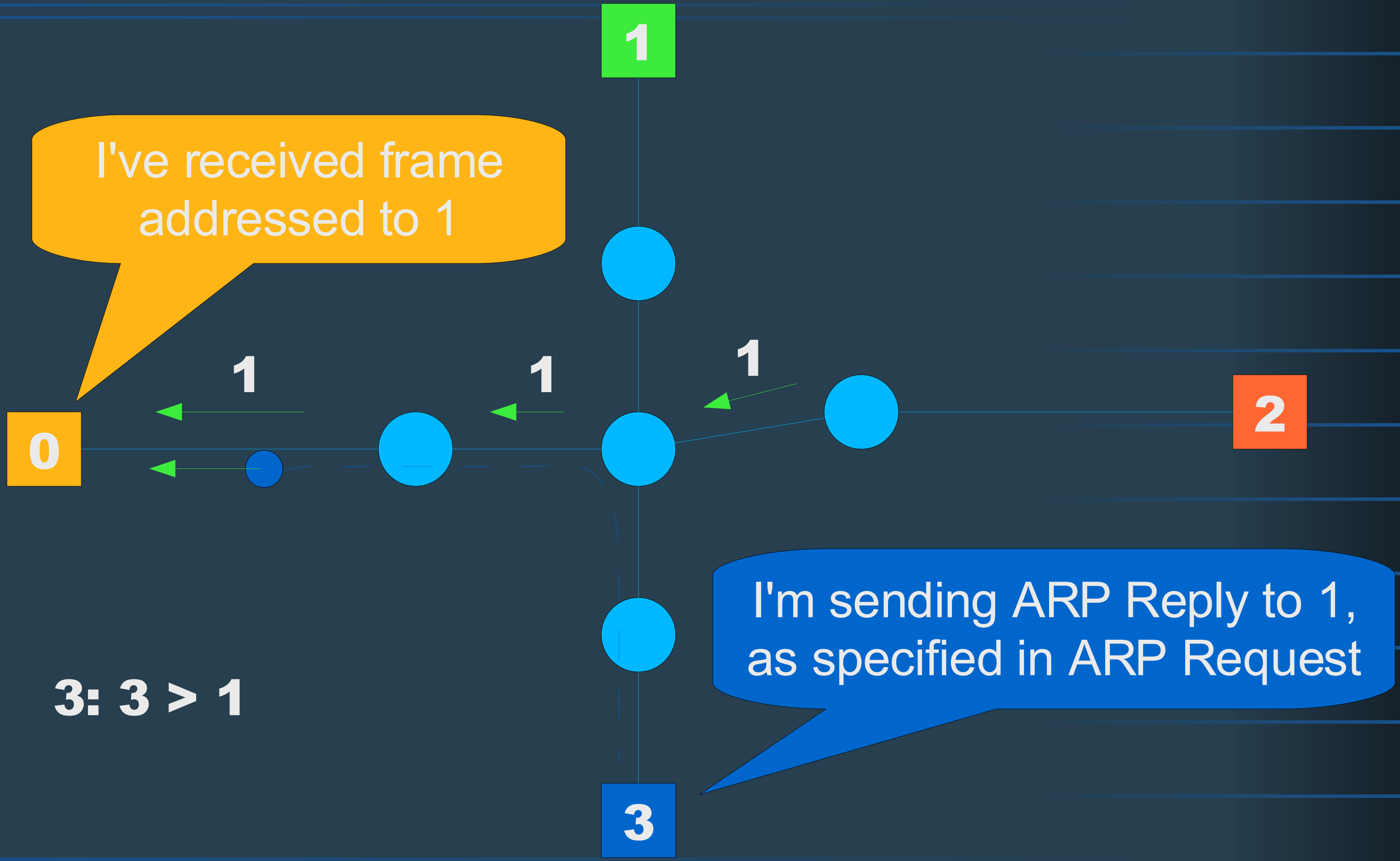
Network structure identification 3


1
I'm asking 3 to send frame to 1
1
1
1
0
2
I've received ARP Request for my IP
3

0: 0 > 3

arp src = 1

Network structure identification 3


1
I've received frame addressed to 1
1
1
1
0
2
I'm sending ARP Reply to 1, as specified in ARP Request
3

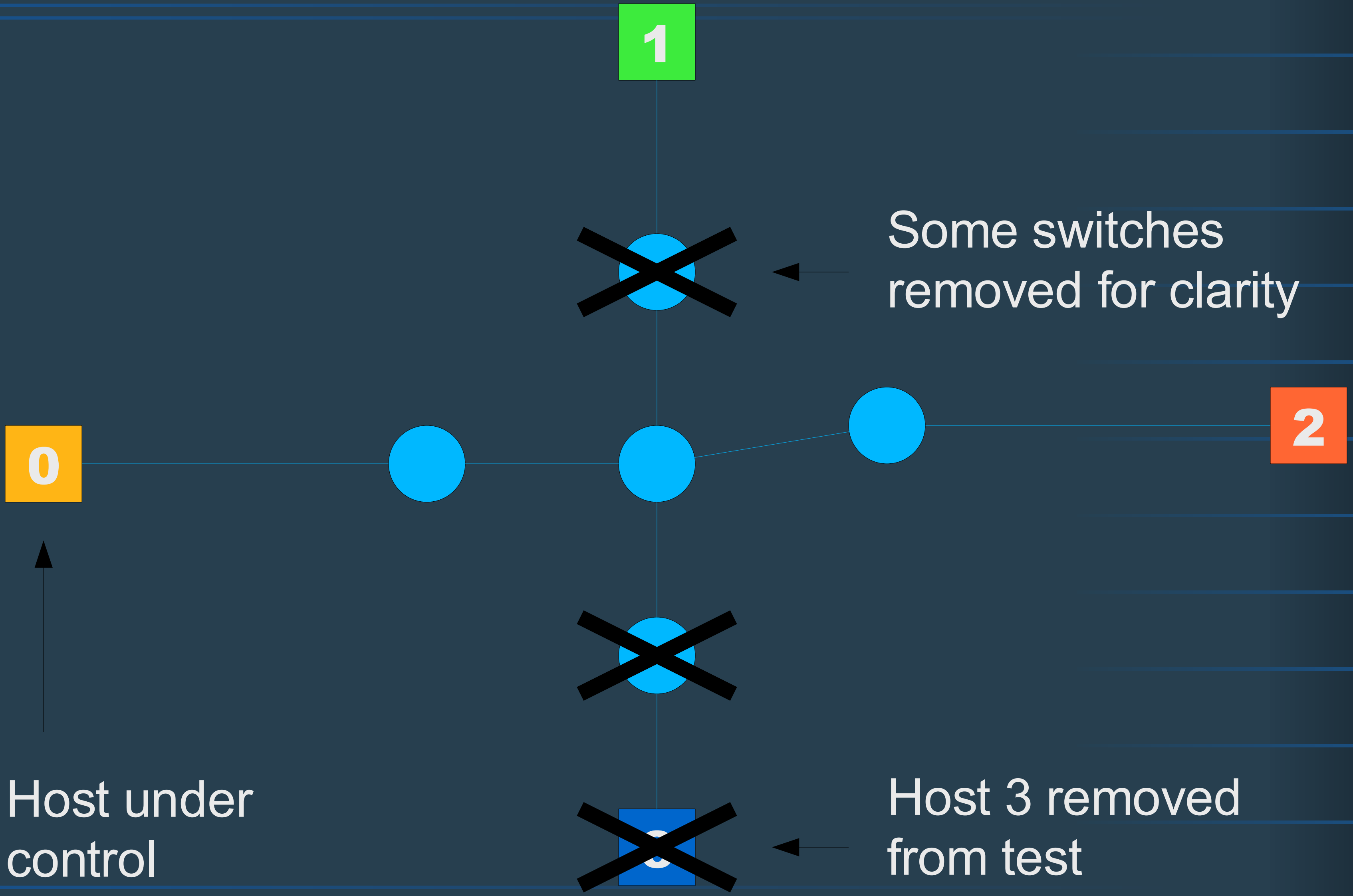
3: 3 > 1

Problem

Tree external hosts required

– too much

Network structure identification 4

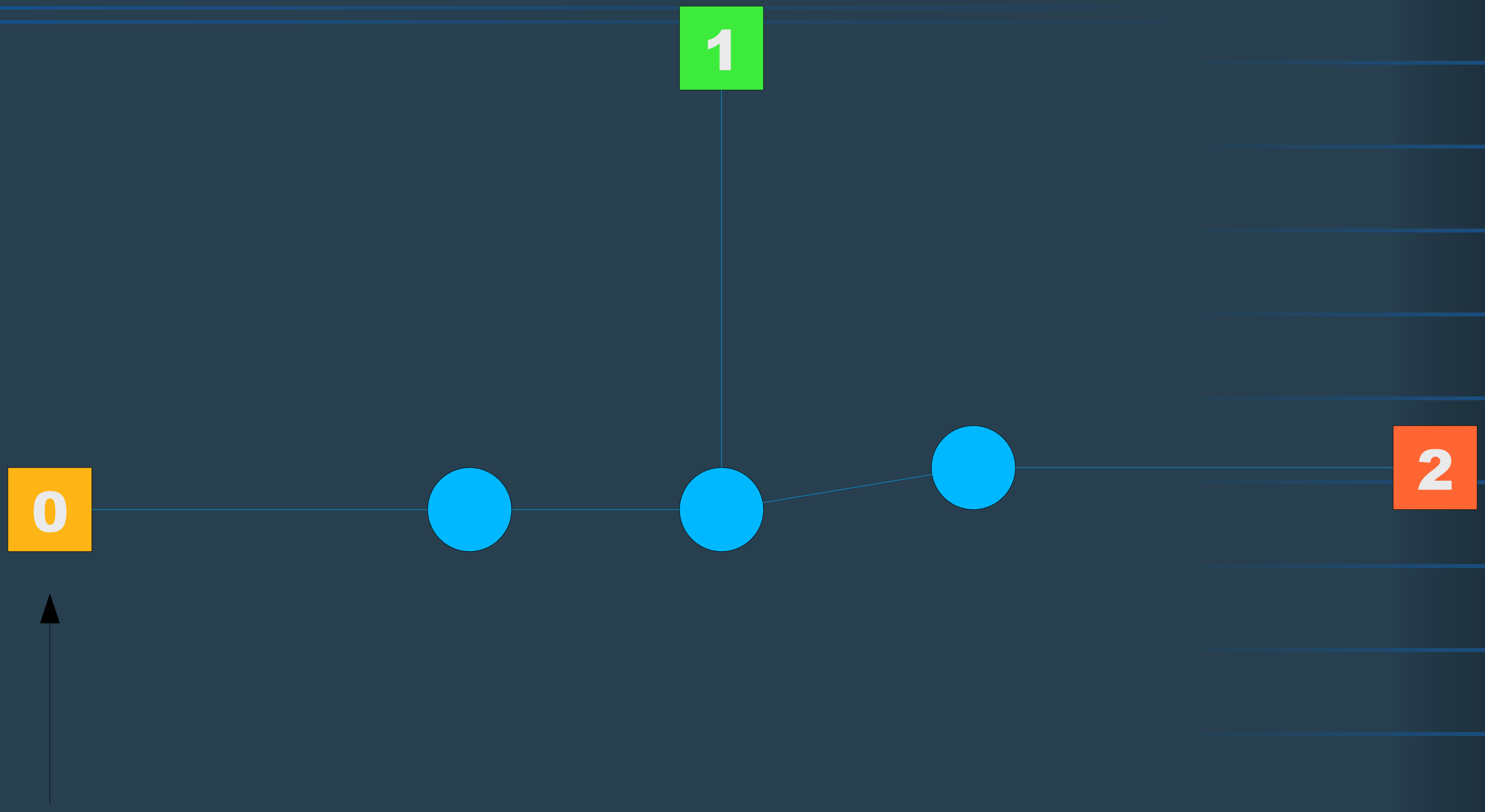


Some switches removed for clarity

Host under control

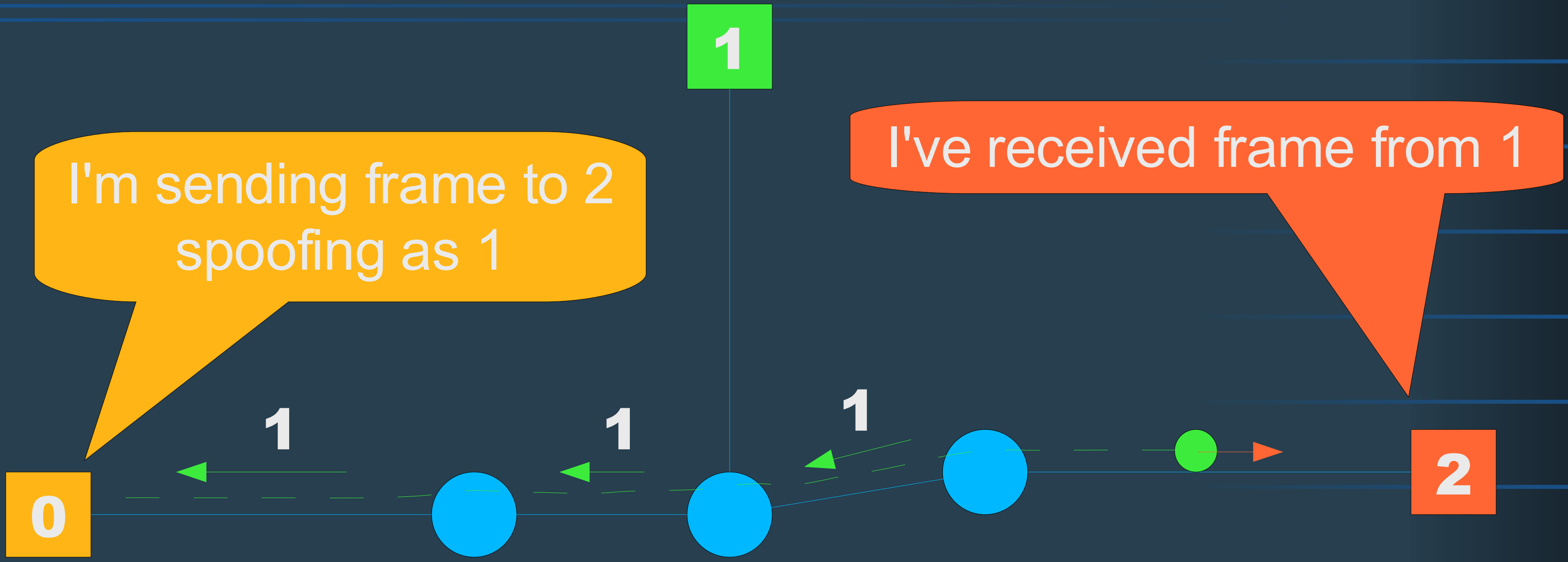
Host 3 removed from test

Network structure identification 4



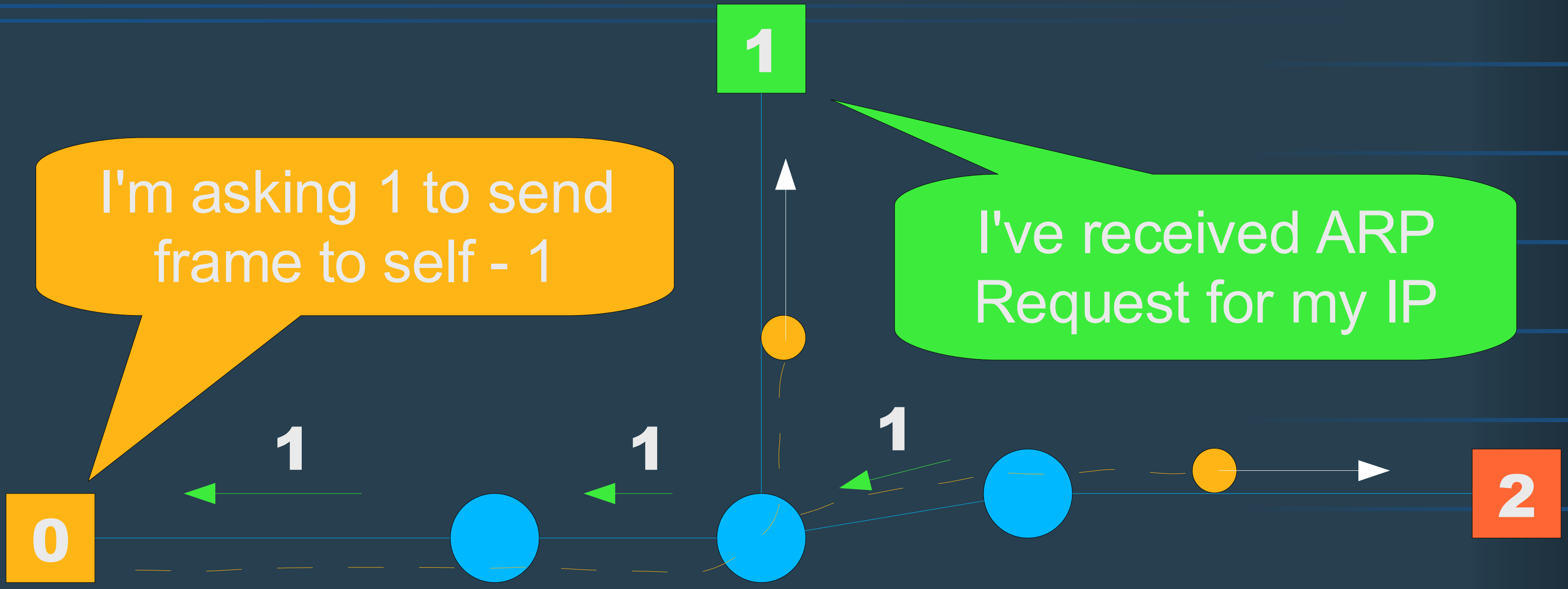
Host under control

Network structure identification 4


I'm sending frame to 2 spoofing as 1
1
I've received frame from 1
1
1
1
0
2

0: 1 > 2

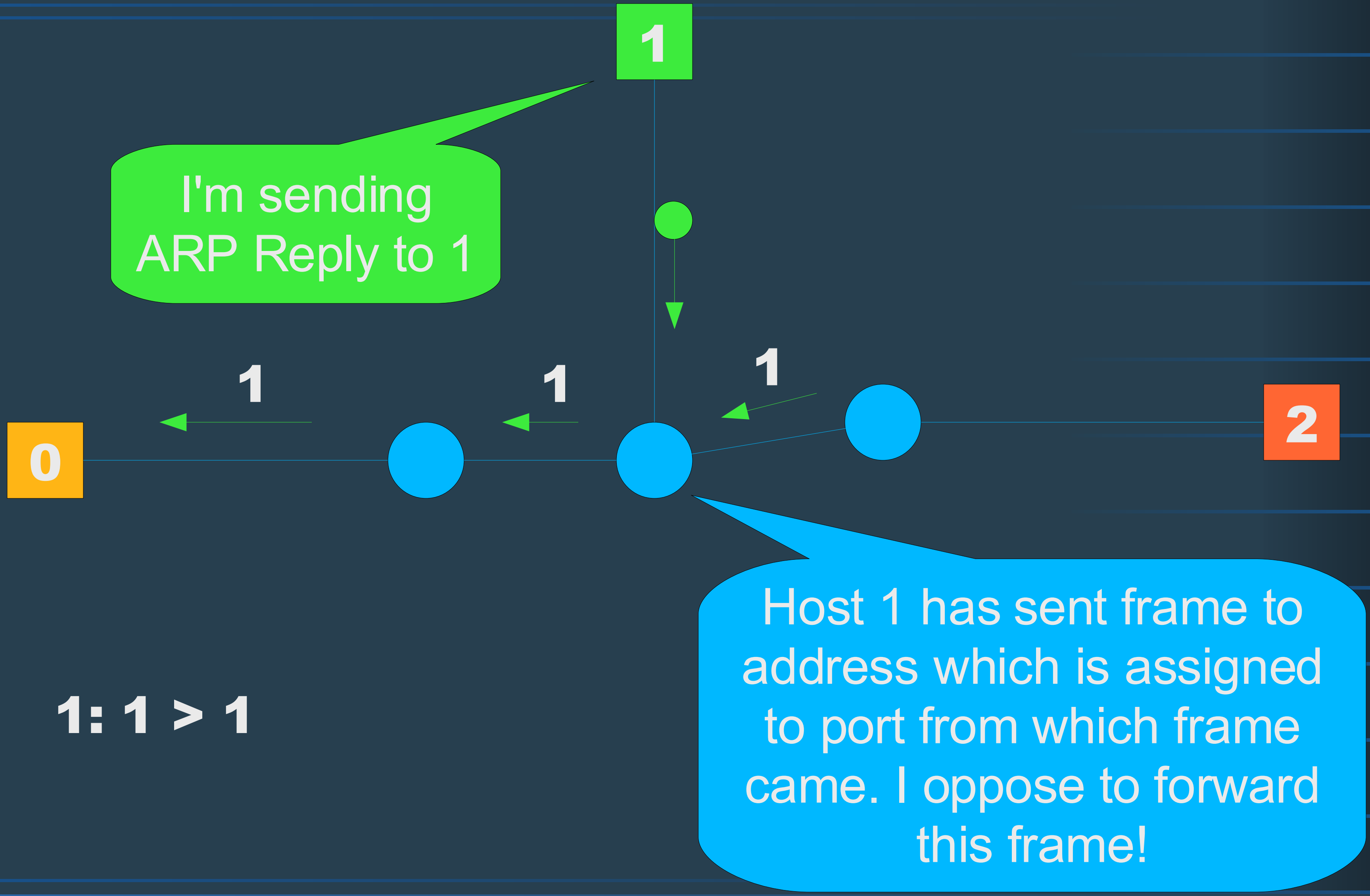
Network structure identification 4


1
I've received ARP Request for my IP
I'm asking 1 to send frame to self - 1
1
1
1
0
2

0: 0 > broadcast

arp src = 1 !

Network structure identification 4

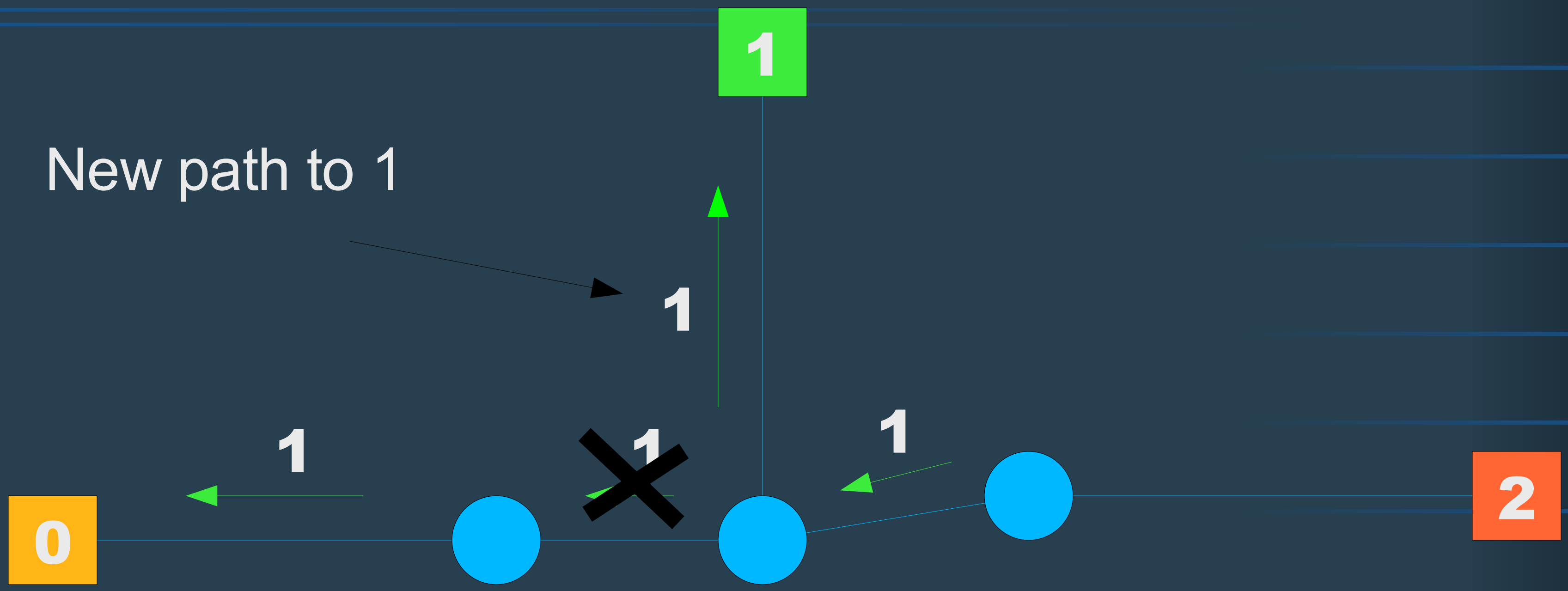


I'm sending ARP Reply to 1

Host 1 has sent frame to address which is assigned to port from which frame came. I oppose to forward this frame!

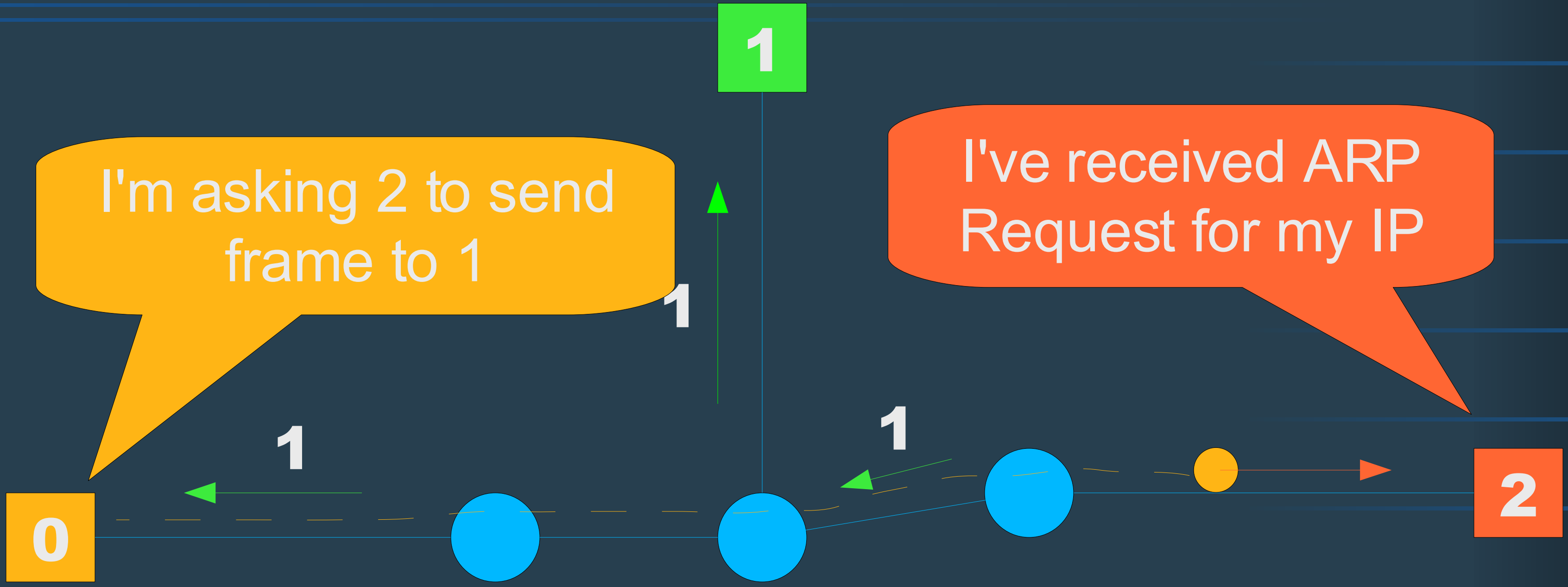
1: 1 > 1

Network structure identification 4



New path to 1

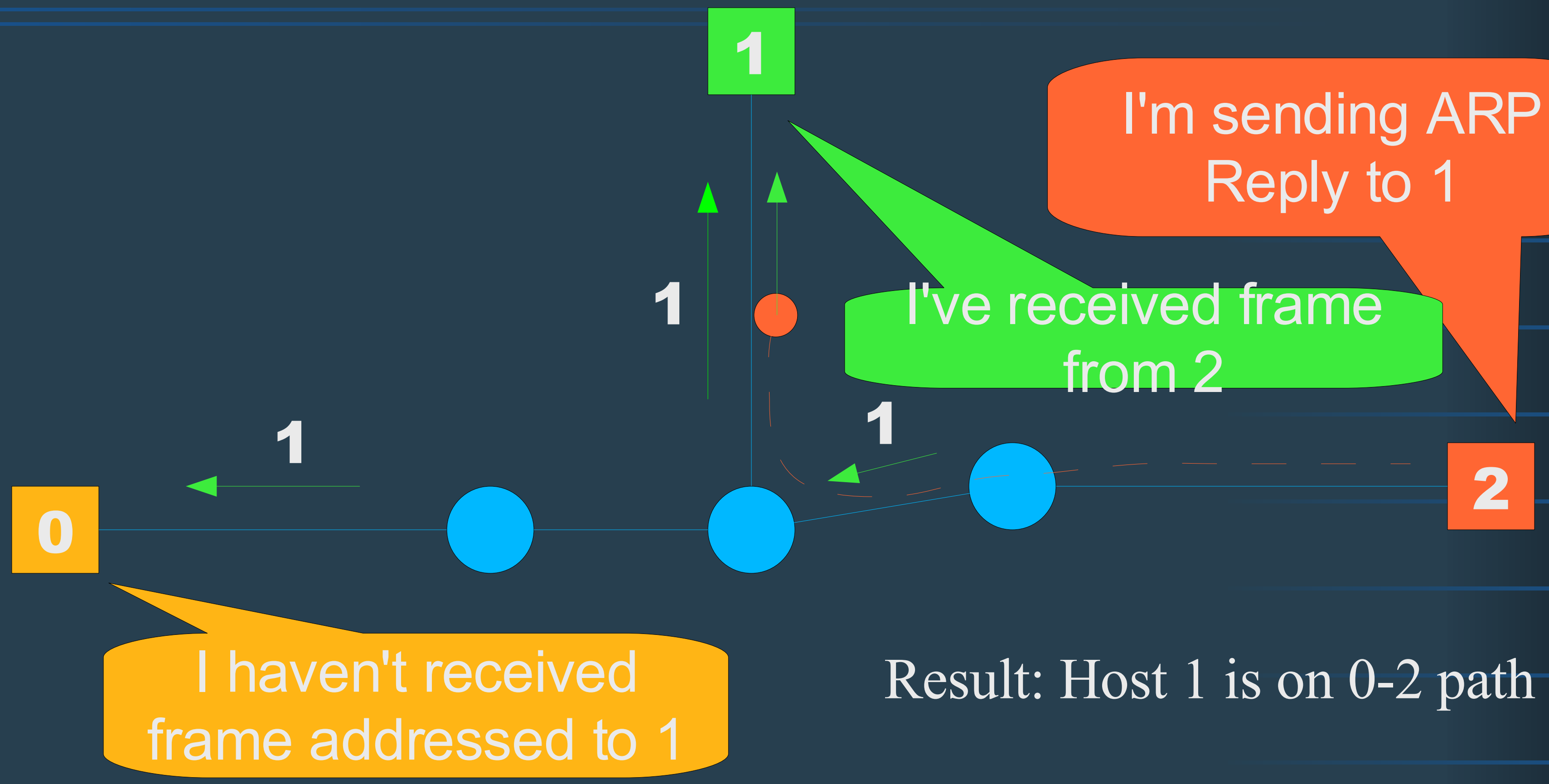
Network structure identification 4


1
I'm asking 2 to send frame to 1
I've received ARP Request for my IP
1
1
1
0
2

0: 0 > 2

arp src = 1

Network structure identification 4

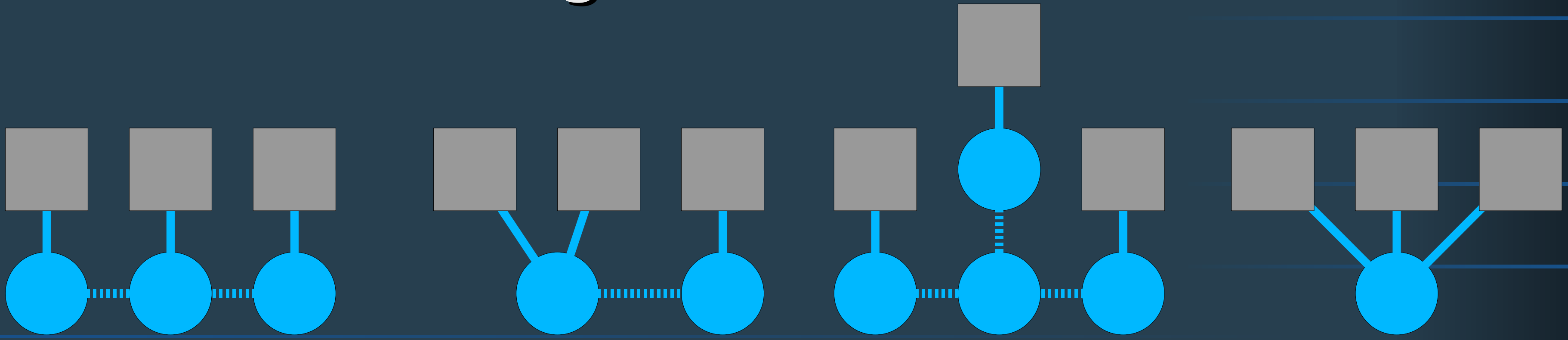

1
I'm sending ARP Reply to 1
1
I've received frame from 2
1
1
0
2
I haven't received frame addressed to 1

Result: Host 1 is on 0-2 path

2: 2 > 1

Etherbat

- 3 basic tests
  - A1, A2 – difference in host order
  - B1
- Additional test
  - B2 – error detection
- 2^3 = 8 configurations



Problems: when result is invalid?

- Symetric ARP?
- “Silent host” (in examples host 2) generates traffic
  - some transmissions detected by sniffing
  - test repeating
  - “jabber” message -> more than one possible configurations
  - test B guarantees jabber detection
- Filtering (port-security etc.)
  - most filtering cases detected
- Duplicates
  - some could be detected (not in this version)
- Frame loss
  - Practically not detectable
- Switches and “switches”

Switches & “switches”

- First SA=DA frame
  - Learning and forwarding processes order
- DA=PAUSE frame
  - SA learning
  - forwarding
- Etherbat resistance

Switches & “switches”

- Almost every switch chip specyfications mentions about 802.3 standard compilance
- Some chips don't learn SA of DA=PAUSE frames
- 802.3-2005, section 1, 1.4 Definitions:
  - (...) switch: A layer 2 interconnection device that conforms to the (...) 802.1D-1998. Syn: bridge.
- 802.1D-1998, Annex A, A.6 Relay and filtering of frames:
  - Mandatory: Are correctly received frames submitted to the Learning Process?
- Result:
  - Device which doesn't learn SA od DA=PAUSE frames is not compilant with 802.3

Optimistic mode

- Sometimes Etherbat recognizes more than one possible configuration
- **`etherbat -o`**
  - this option makes Etherbat choose the most probable one

How to defend host locating?

- Protect network againt MAC Spoofing
- Generate traffic
  - broadcasts are the best, they propagate everywhere and learn every switch
  - small frames, frequently
  - Blaster on all computers
    - sorry *nix users, it's a Windows app ;-)
- Modify/filter ARP
  - arptables

Etherbat: more ideas

- Batch mode
  - GUI app to visualize entire network
- More modes
  - one host – fingerprint path from A to B
  - three hosts (maybe better results in networks with strange switches)
- Performance under high pps
  - possibility to run Etherbat on gateway machine
- Tests optimization
  - now – optimized for exact results
  - should generate less frames

Etherbat: more ideas

- Extend tool to include other protocols
- Every “asymetric” protocol could be used!
  - IPv6
  - IPX
  - ARP+L3/4 (i.e. IP/ICMP, IP/TCP syn/rst)
  - other?

Commerial: Ispara Storm Guard

- Eliminates LAN problems
  - DoS/DDoS attacks
  - virus scanning
  - spam sending
- Infected hosts are put in quarantine
  - host traffic doesn't reach Ethernet!
  - manageable switches don't required
- Hardware accelerated packets processing
  - 100mbit, 144800 pps, latency ~ 0

More info:

http://stormguard.ispara.pl

Thank you for your attention.

Paweł Pokrywka

http://www.cryptonix.org

Ispara
Storm Guard
http://stormguard.ispara.pl