Paweł Pokrywka

Radar w Ethernecie

Lokalizowanie hostów w sieci LAN

Idea

- Traceroute w L3
  - dekrementacja pole TTL nagłówka IP
  - ICMP Time Exceeded, gdy TTL == 0
  - lokalizowanie hosta/routera
    - z dokładnością do routera
- Traceroute w L2?
  - odpowiednik routera – switch
  - nie ma odpowiednika TTL
  - przełączniki nie modyfikują ramek

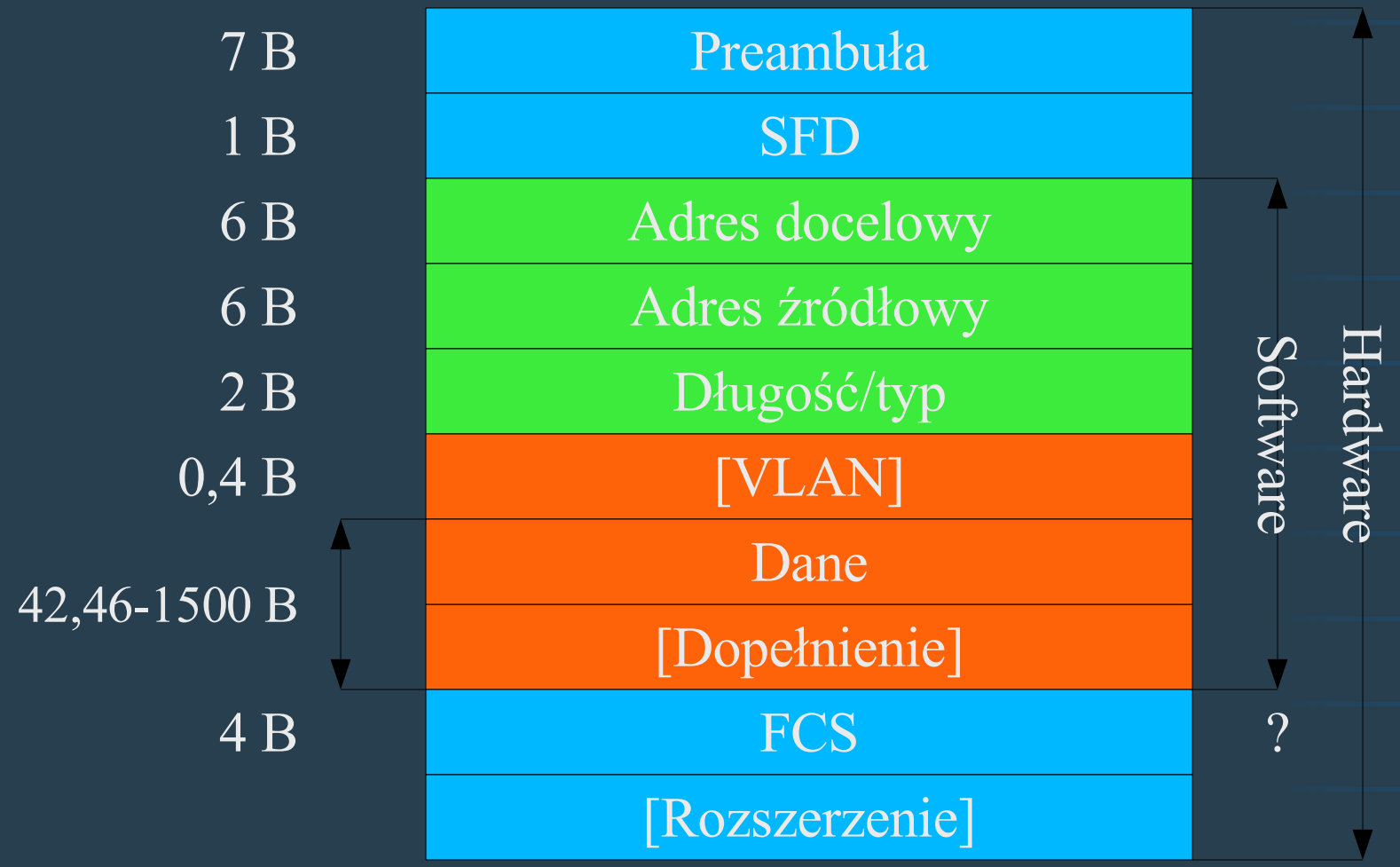
A gdyby się udało?

- Lokalizowanie
  - intruza
  - cennych zasobów
- Tworzenie mapy sieci LAN
  - dokumentacja sieci
  - audyt
  - przygotowania do ataku

Jak to osiągnąć?

- Zarządzalne przełączniki
  - admin – drogie
  - napastnik – trzeba uzyskać dostęp
- Ingerencja w fiz. strukturę sieci
  - kłopotliwe, szczególnie dla napastnika
- Badanie opóźnień
  - host A bliżej niż B gdy ping A < ping B?
- Obciążanie fragmentów sieci
- MAC Spoofing

Podstawy: ramka Ethernet

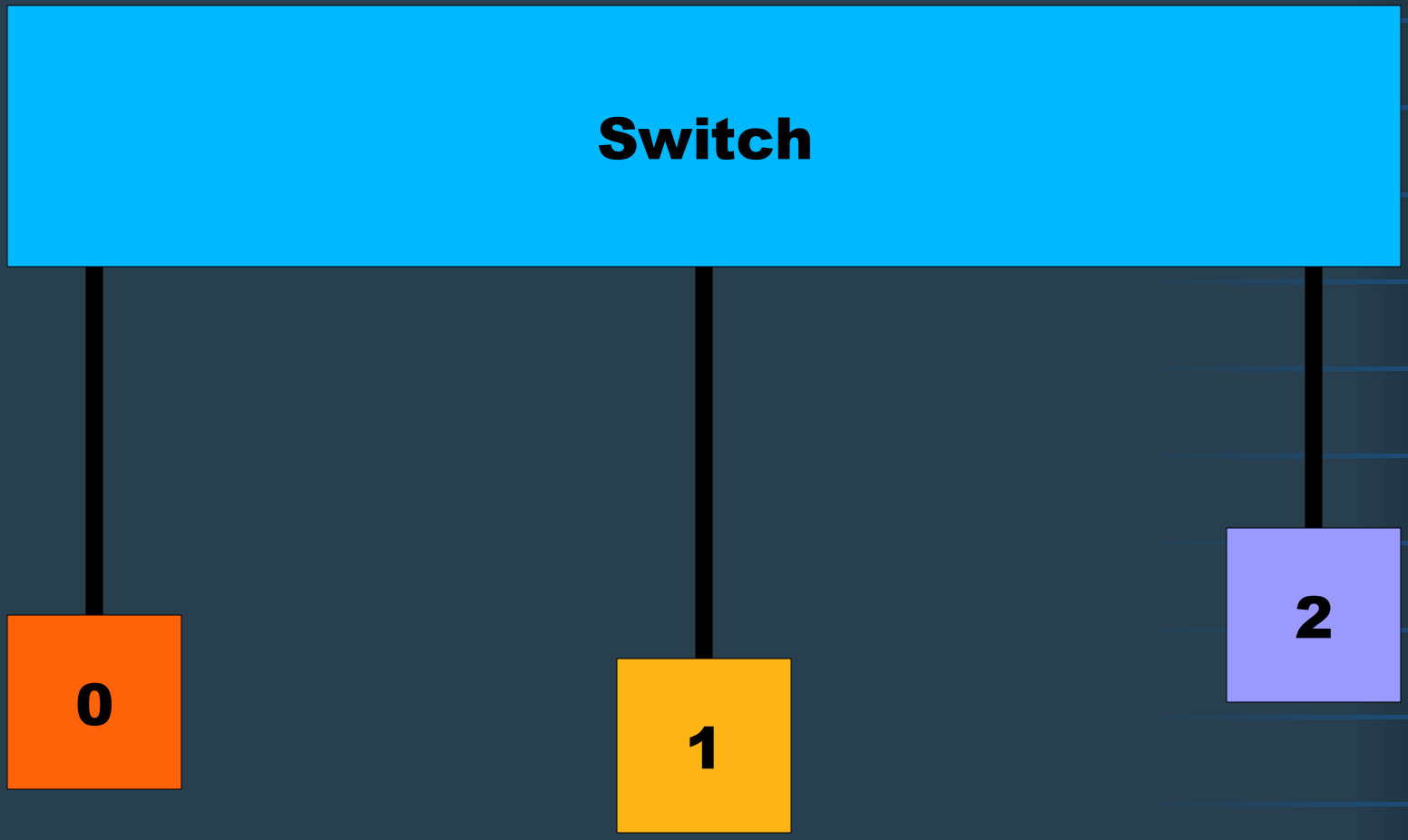


Jak rozpoznać koniec ramki?

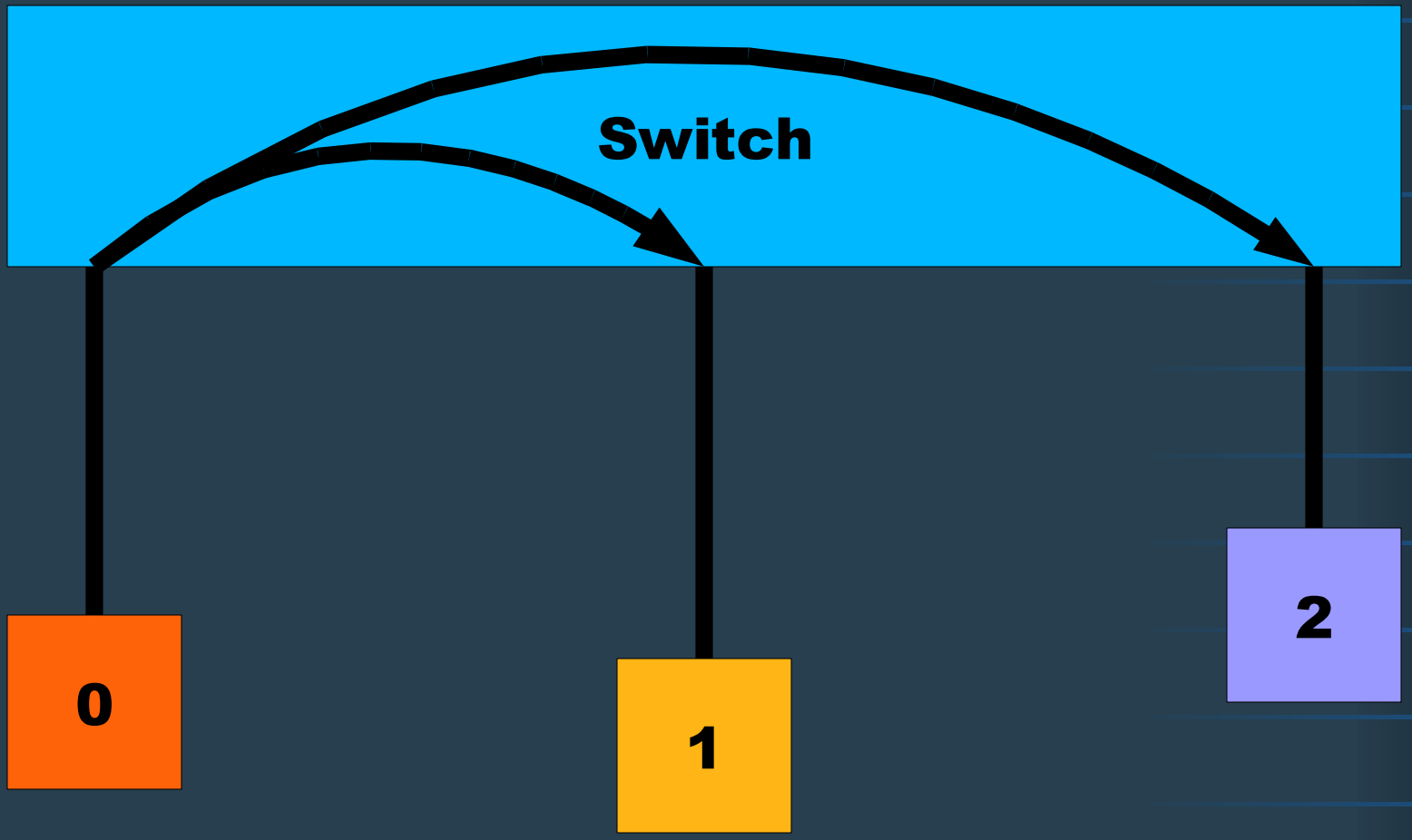
Podstawy: przełączanie 802.1d

- Procesy
  - przekazywanie (Forwarding Process)
  - uczenie (Learning Process)
- Tablica MAC (Filtering Database)
  - pamięć CAM
  - mac - port

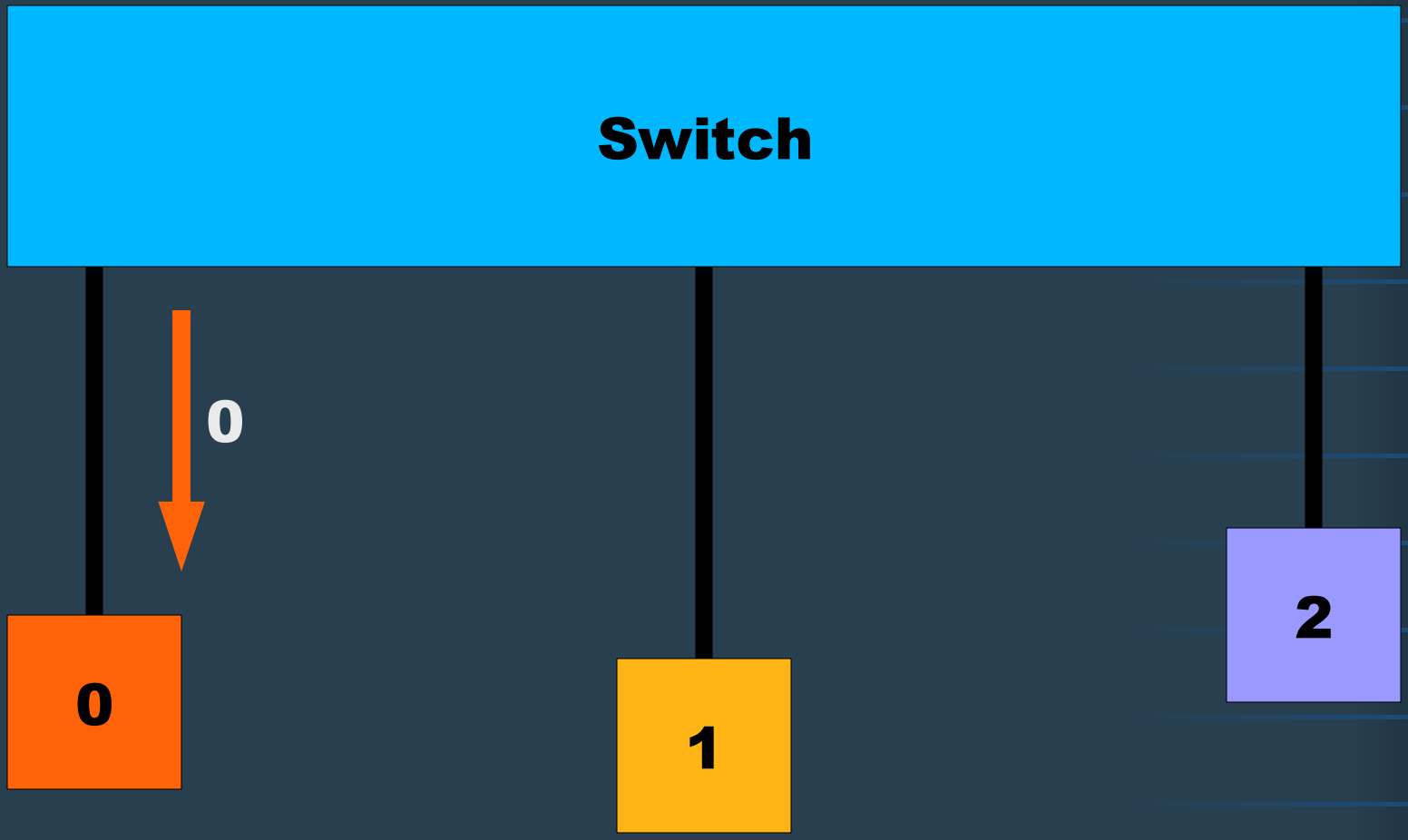
Podstawy: switch 1/5



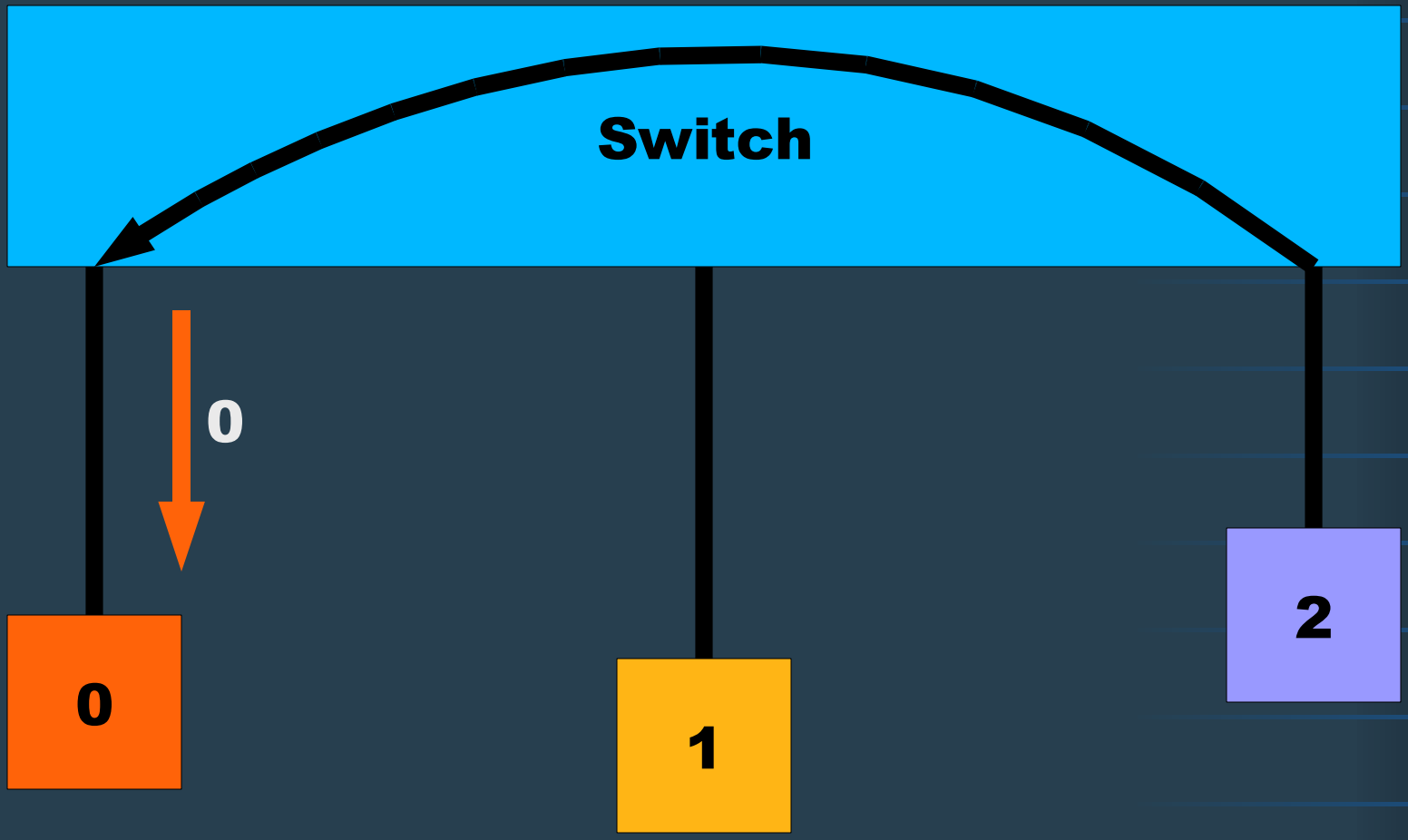
Podstawy: switch 2/5



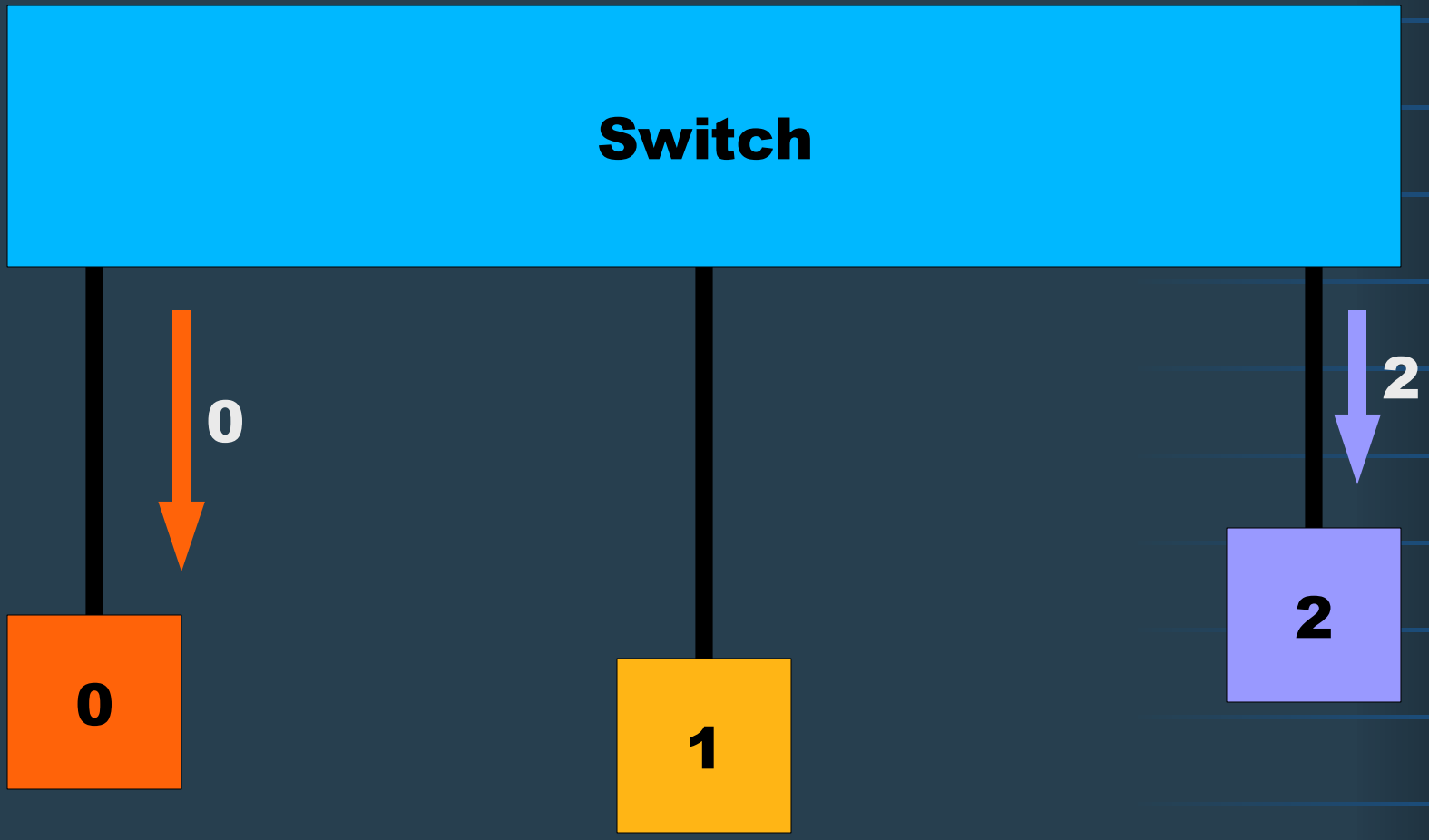
Podstawy: switch 3/5



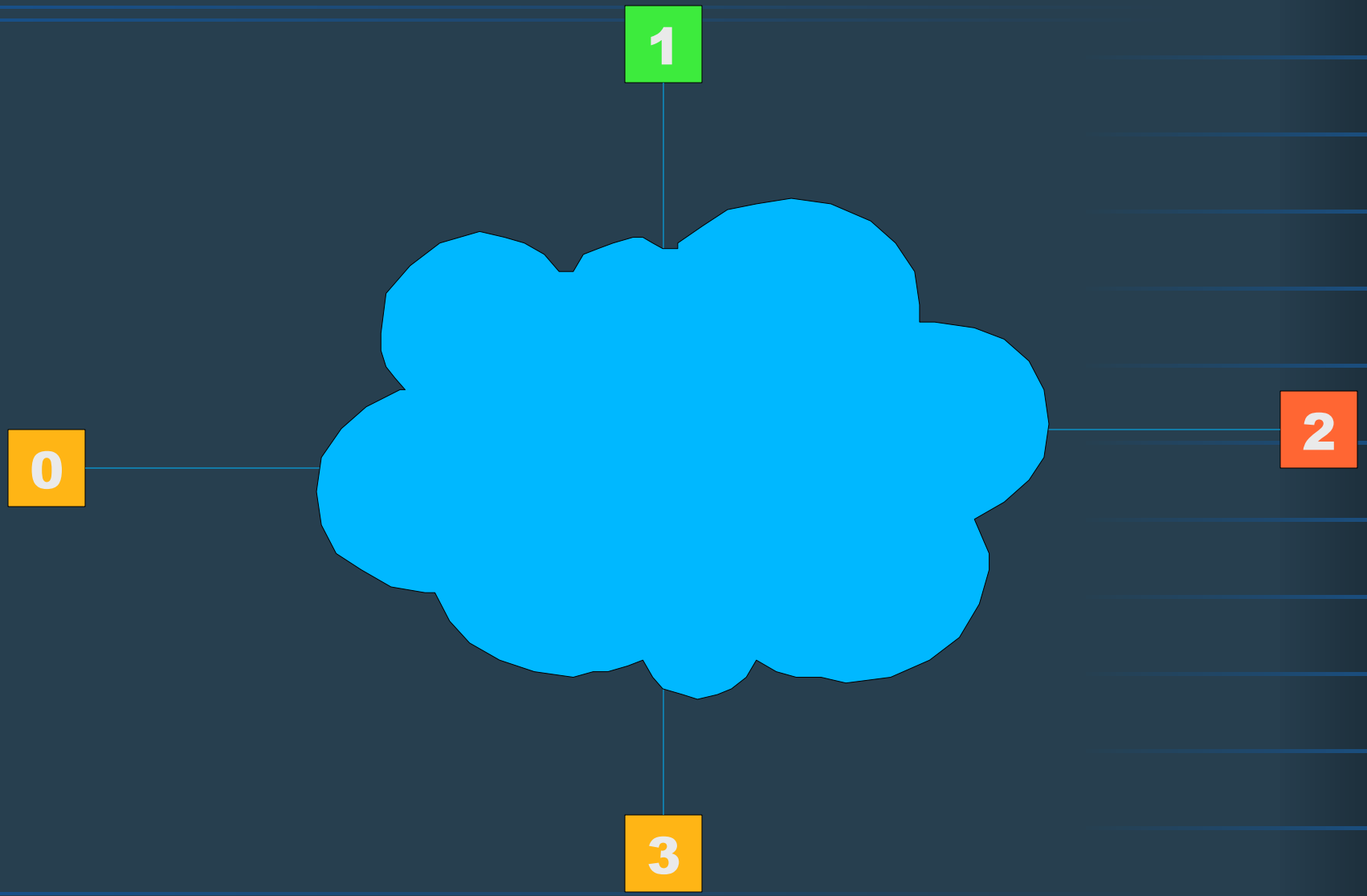
Podstawy: switch 4/5



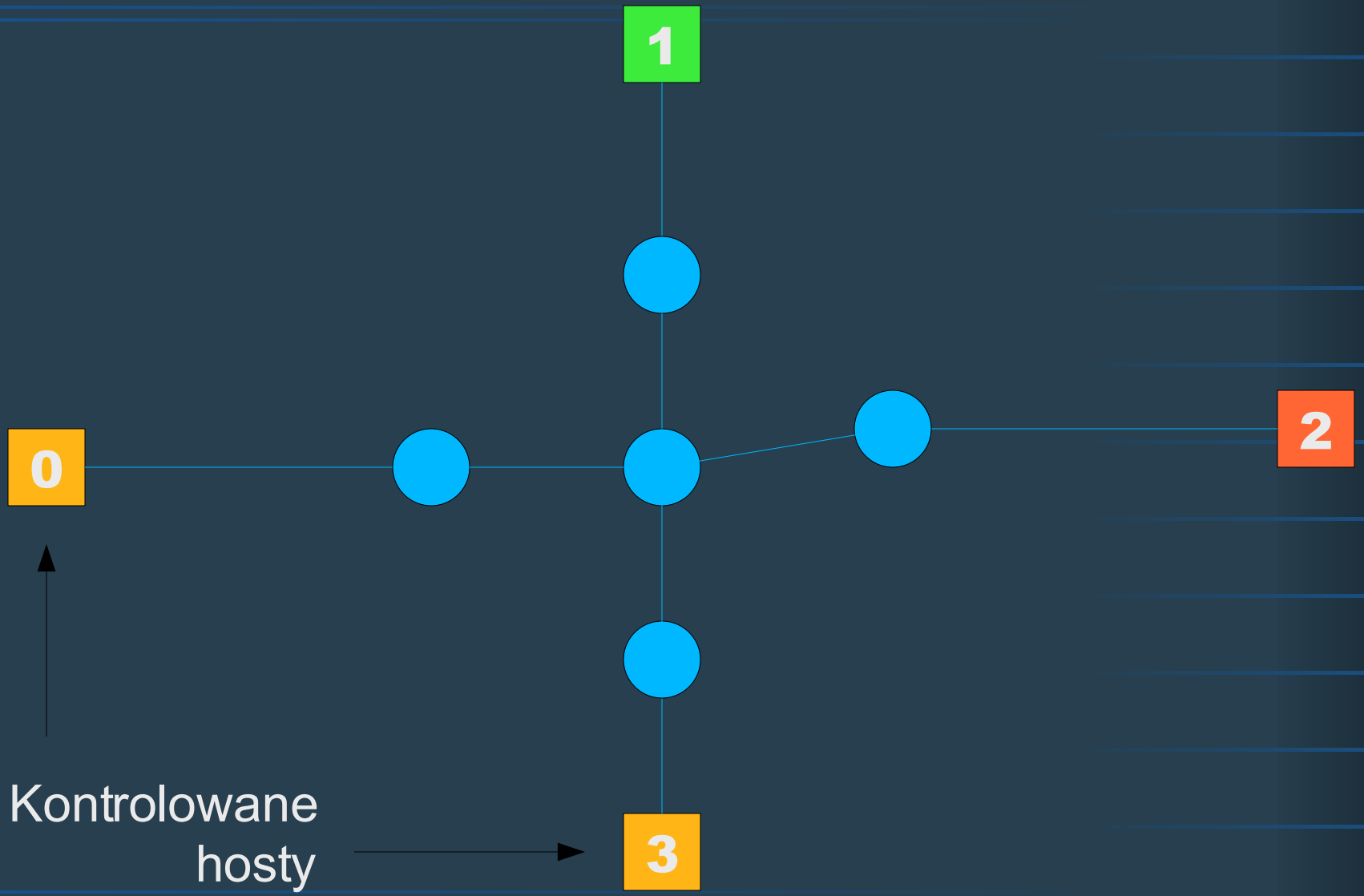
Podstawy: switch 5/5



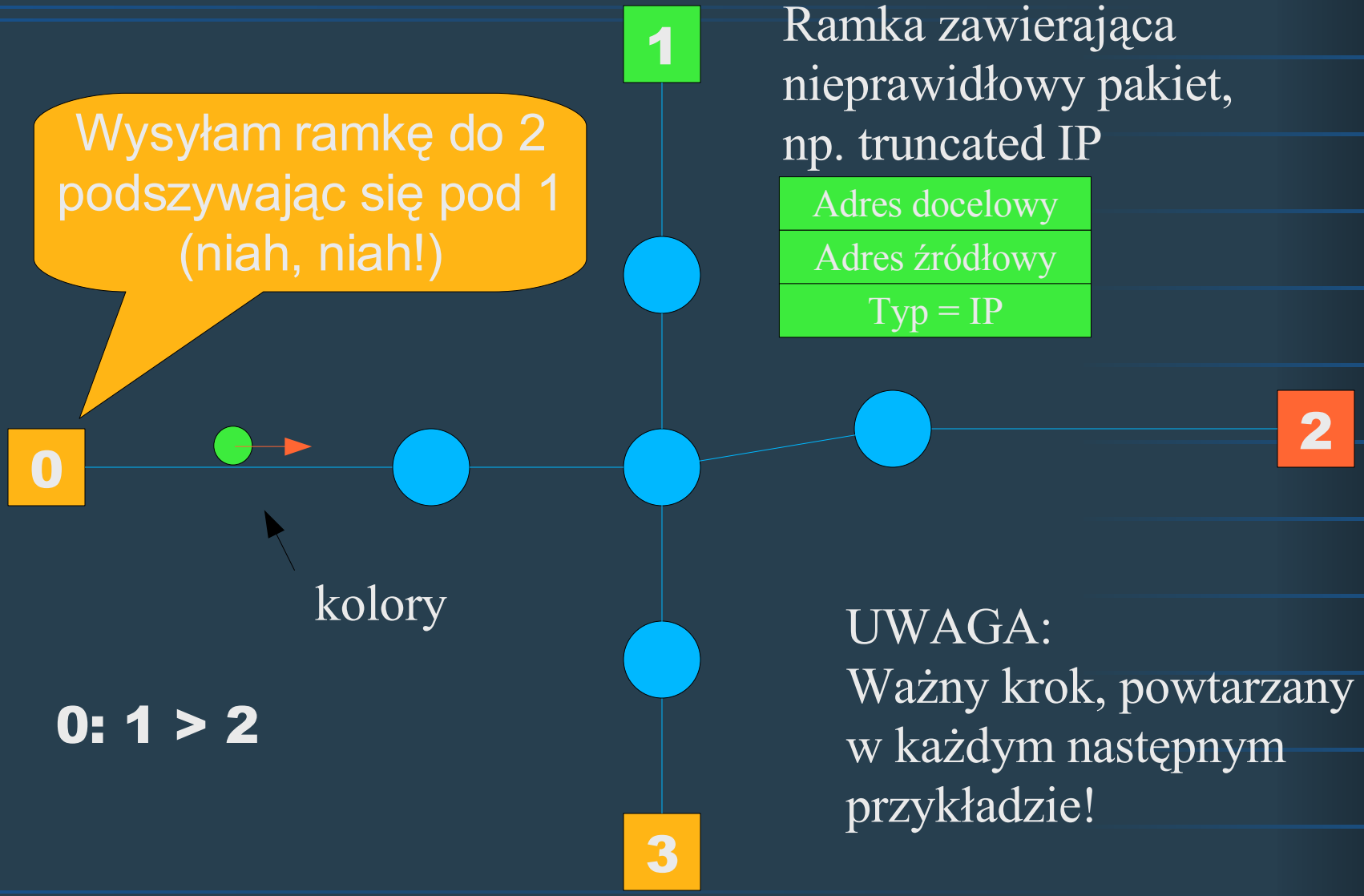
Rozpoznawanie struktury sieci



Rozpoznawanie struktury sieci



Rozpoznawanie struktury sieci

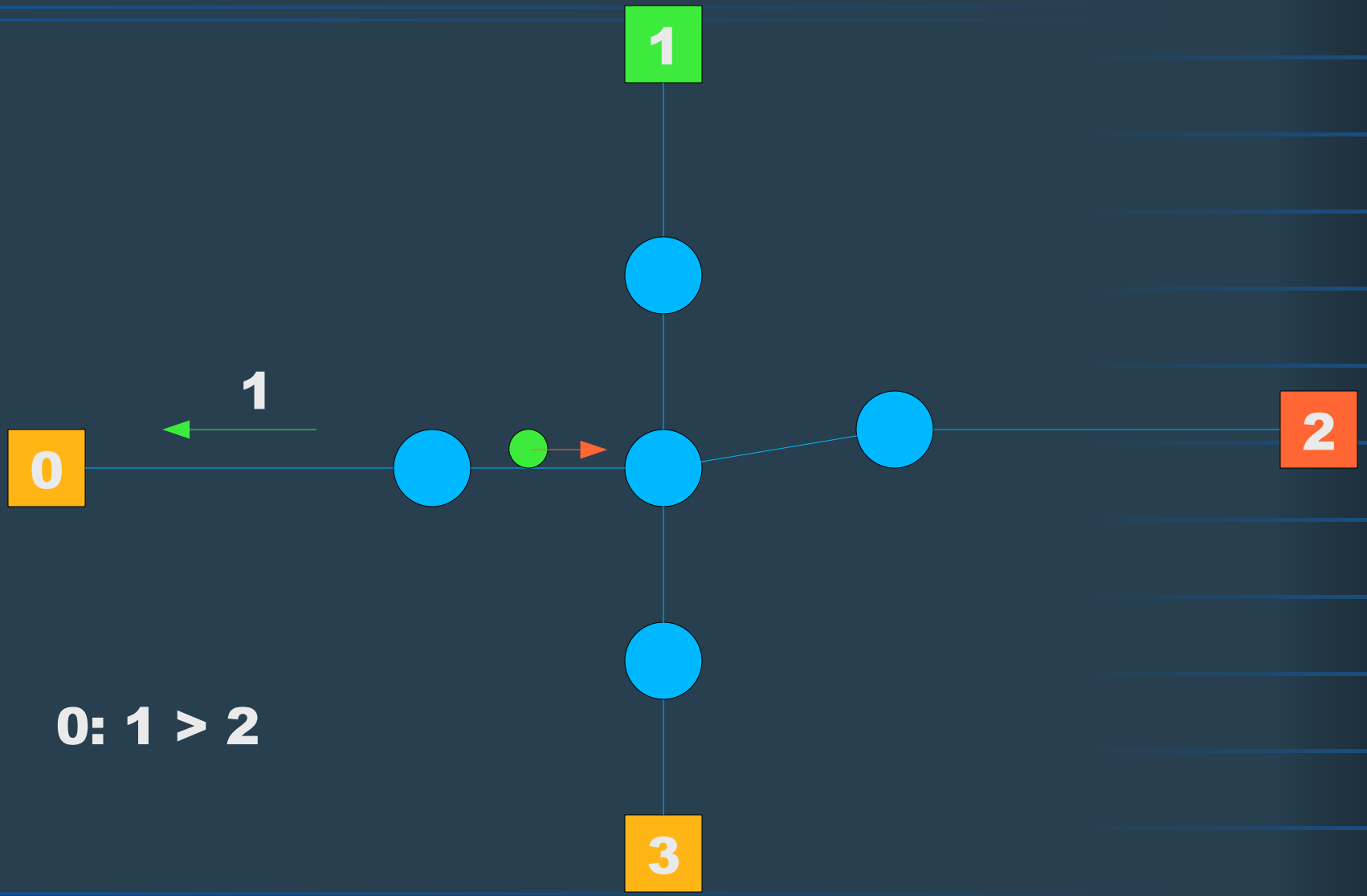


Ramka zawierająca nieprawidłowy pakiet, np. truncated IP

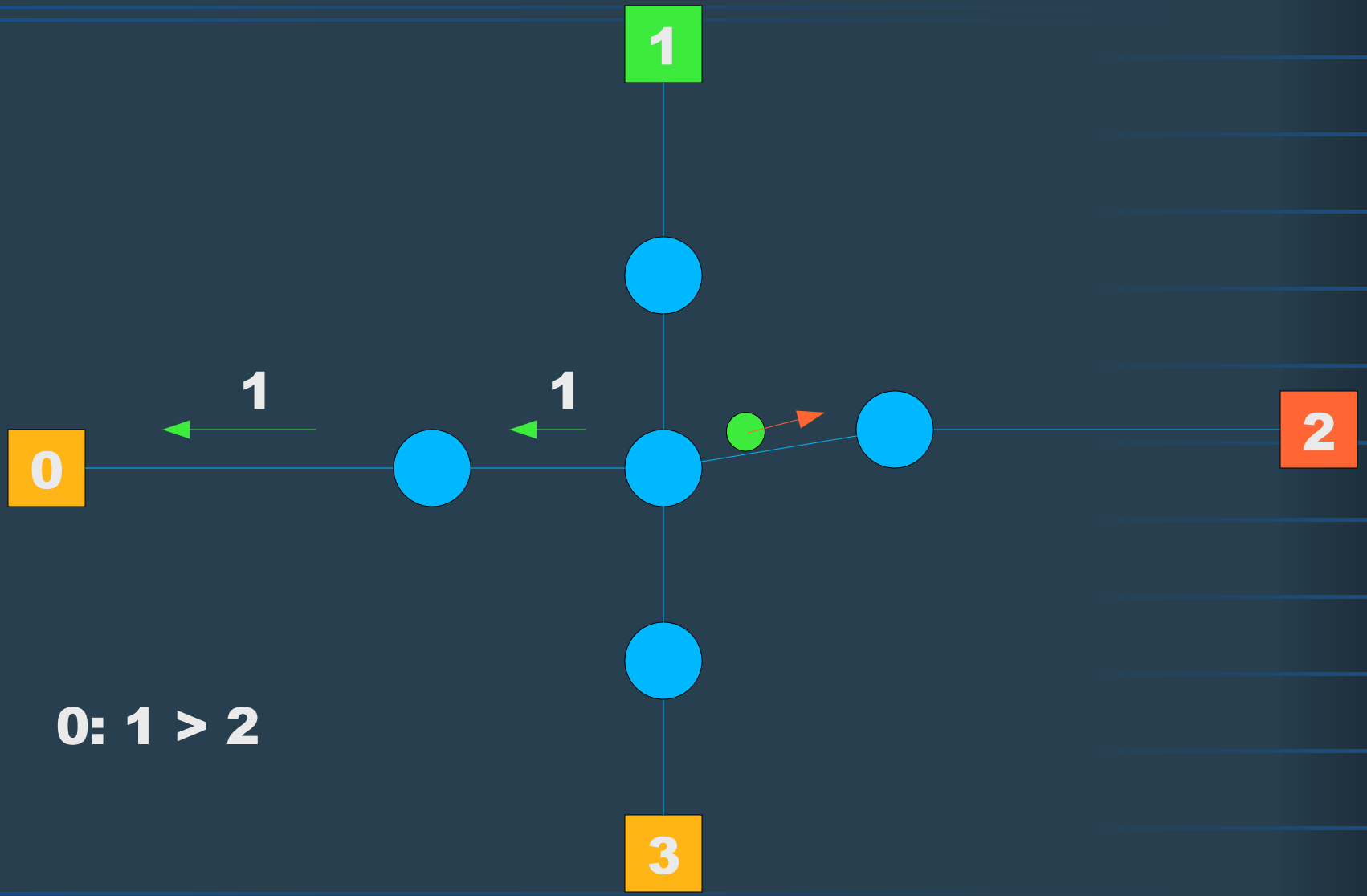
Adres docelowy
Adres źródłowy
Typ = IP

UWAGA:
Ważny krok, powtarzany w każdym następnym przykładzie!

Rozpoznawanie struktury sieci



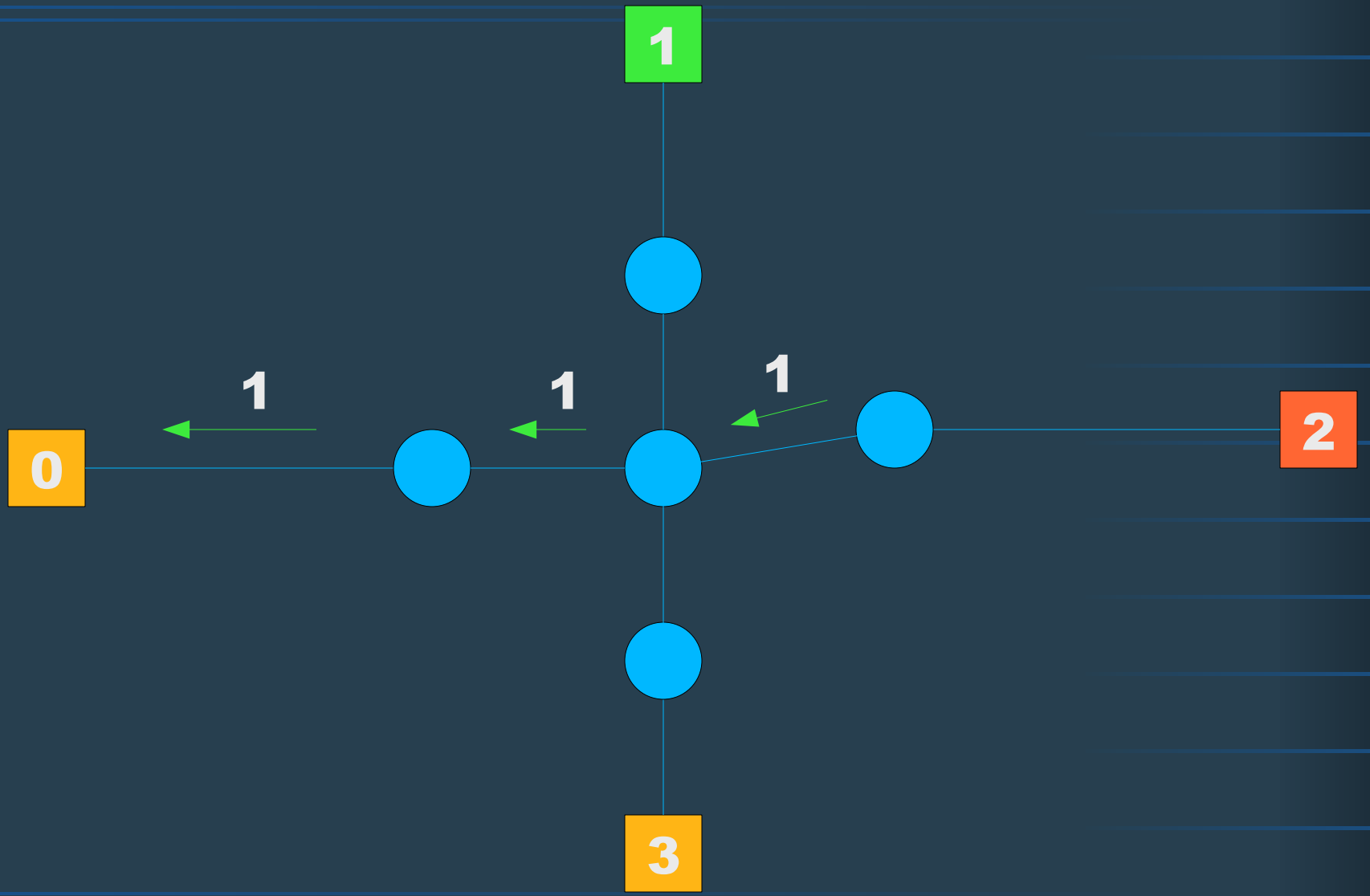
Rozpoznawanie struktury sieci



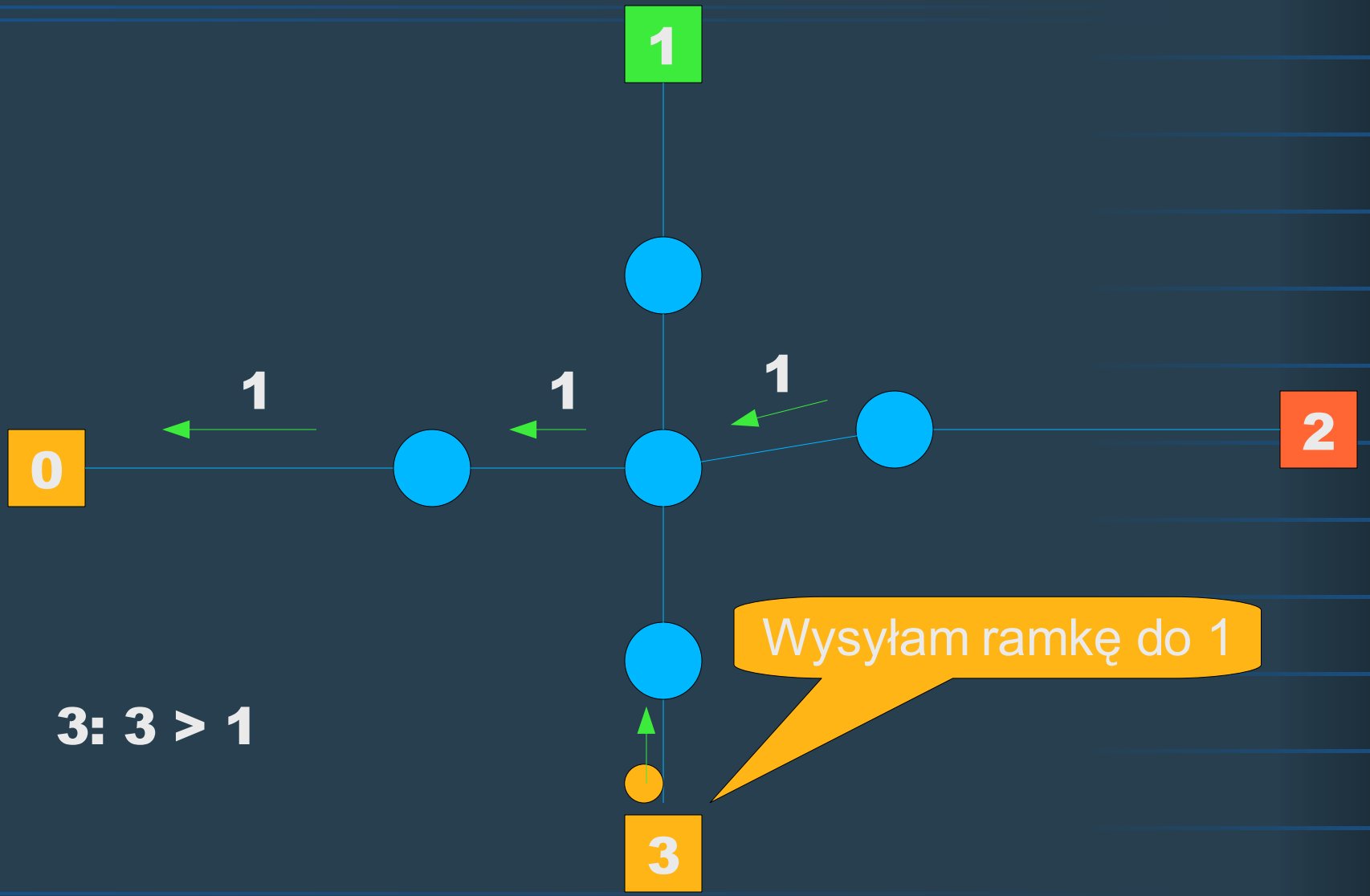
0: 1 > 2

Rozpoznawanie struktury sieci

Rozpoznawanie struktury sieci

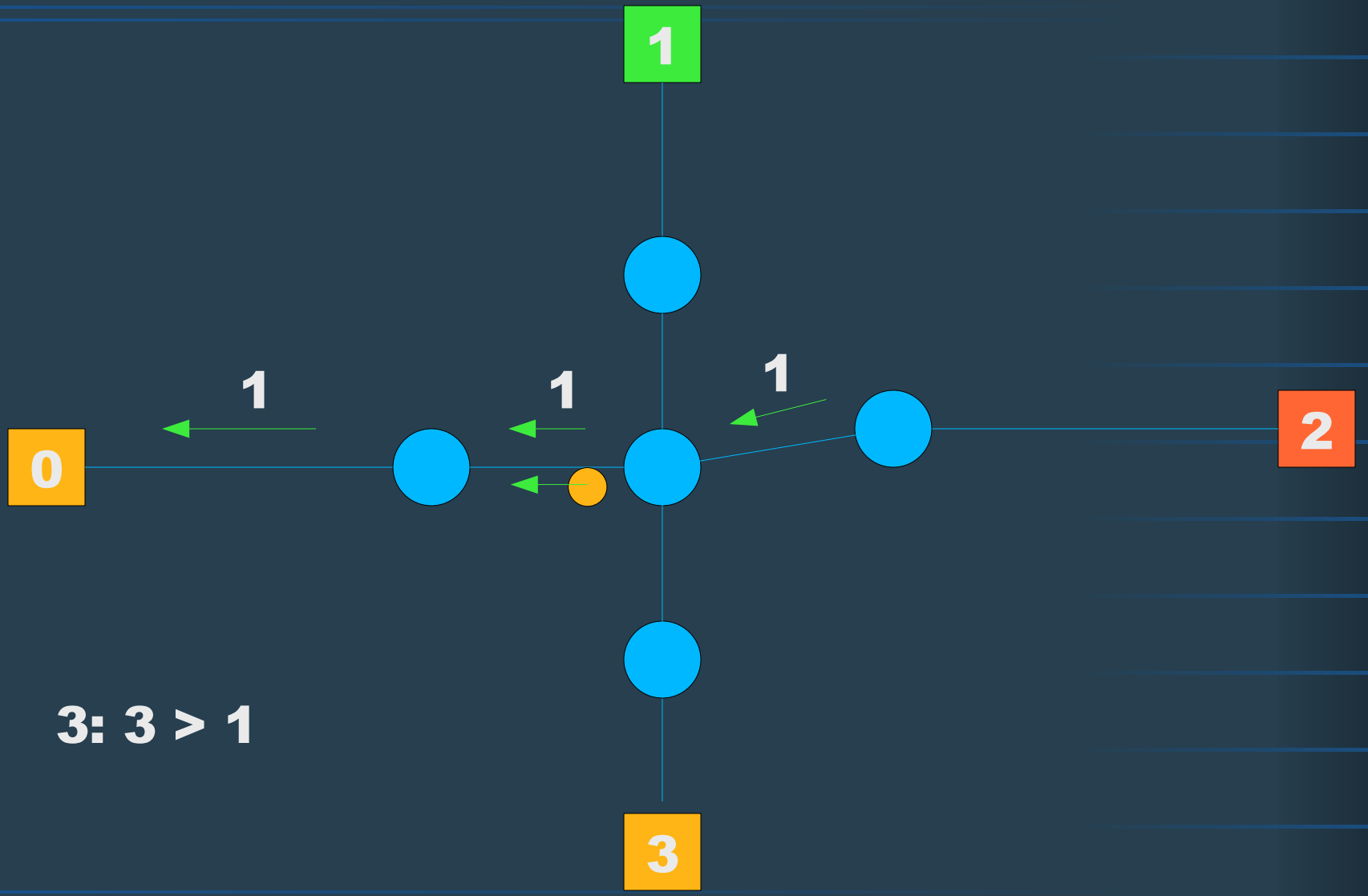


Rozpoznawanie struktury sieci

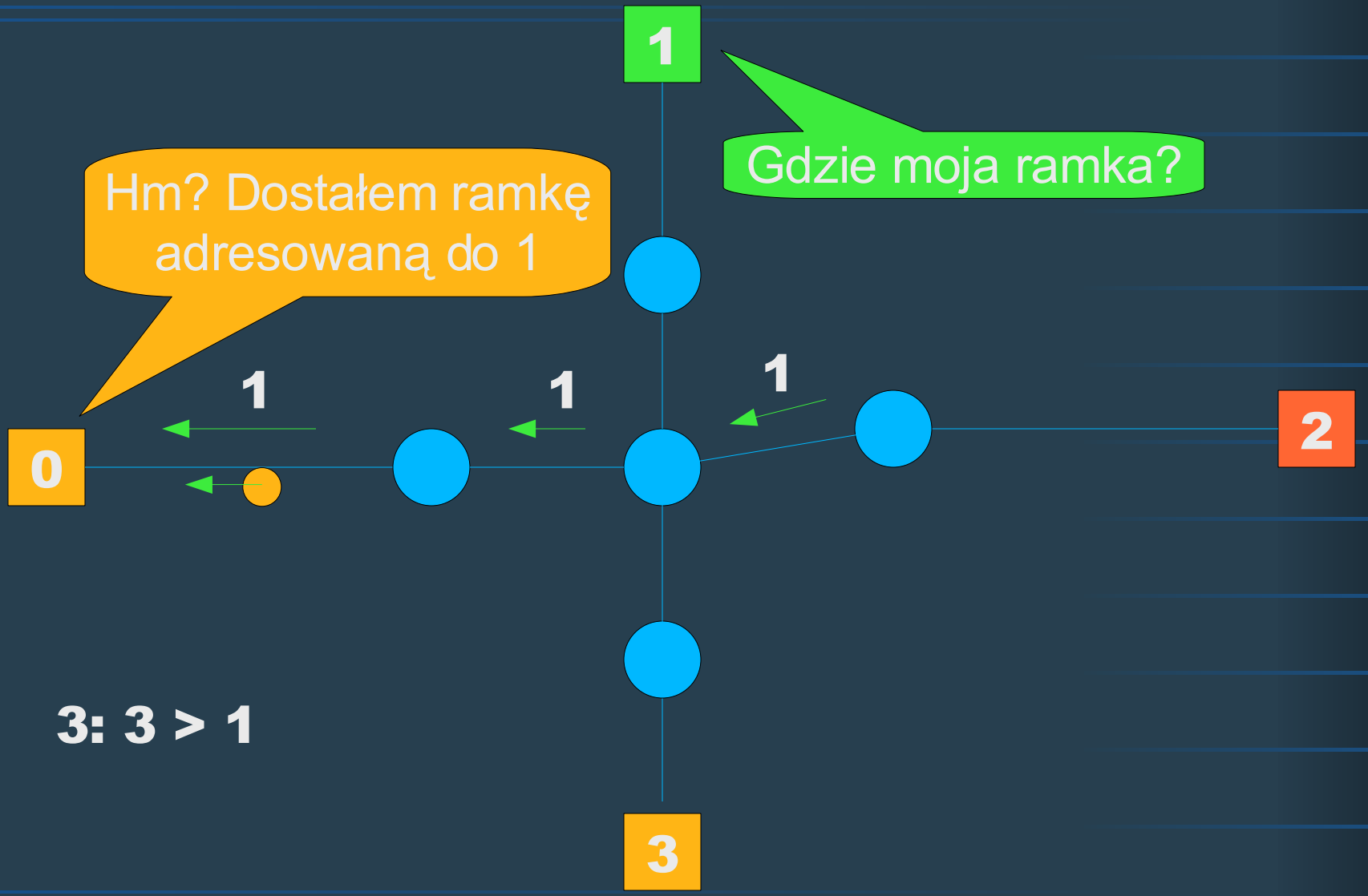


Rozpoznawanie struktury sieci

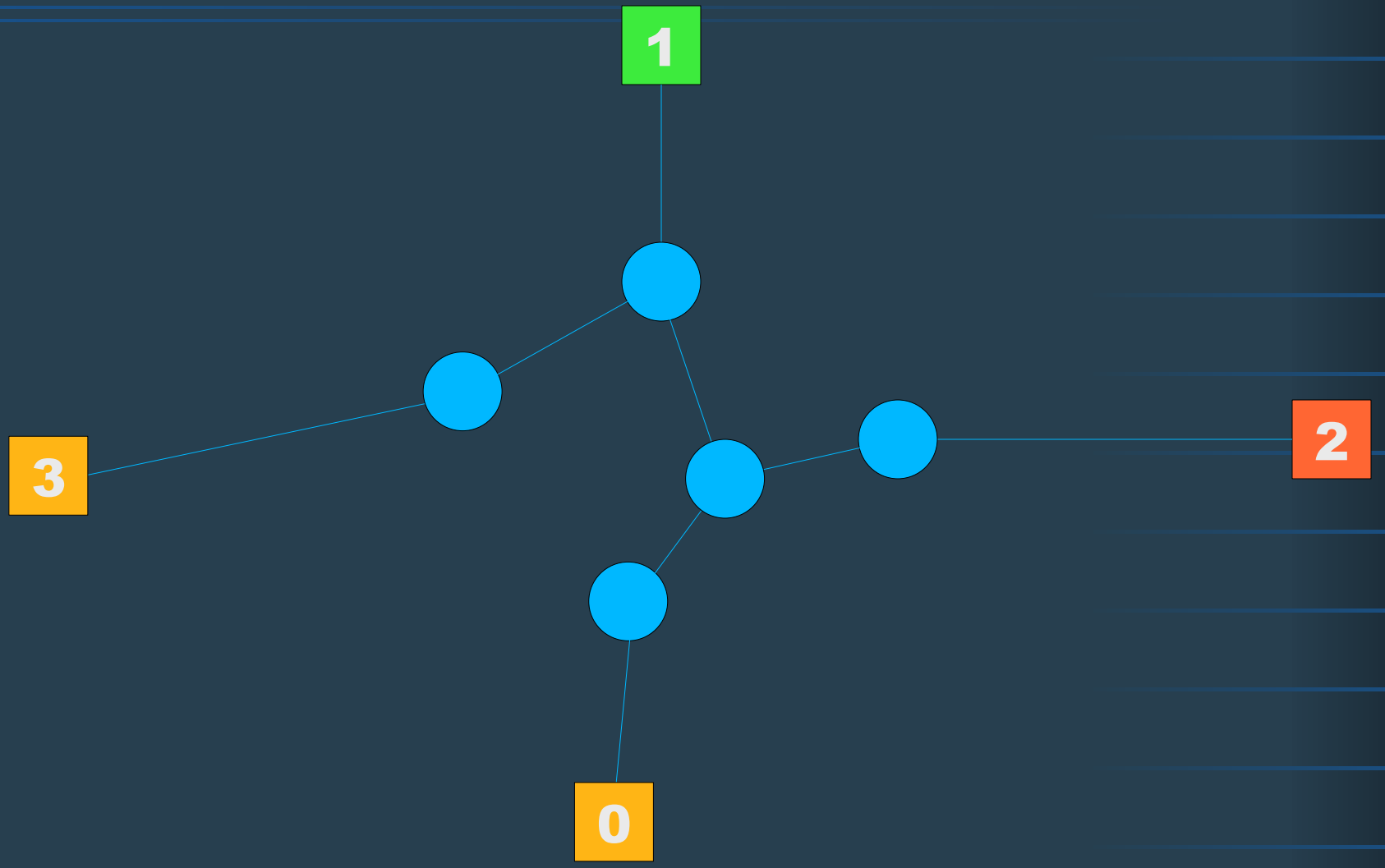
Rozpoznawanie struktury sieci



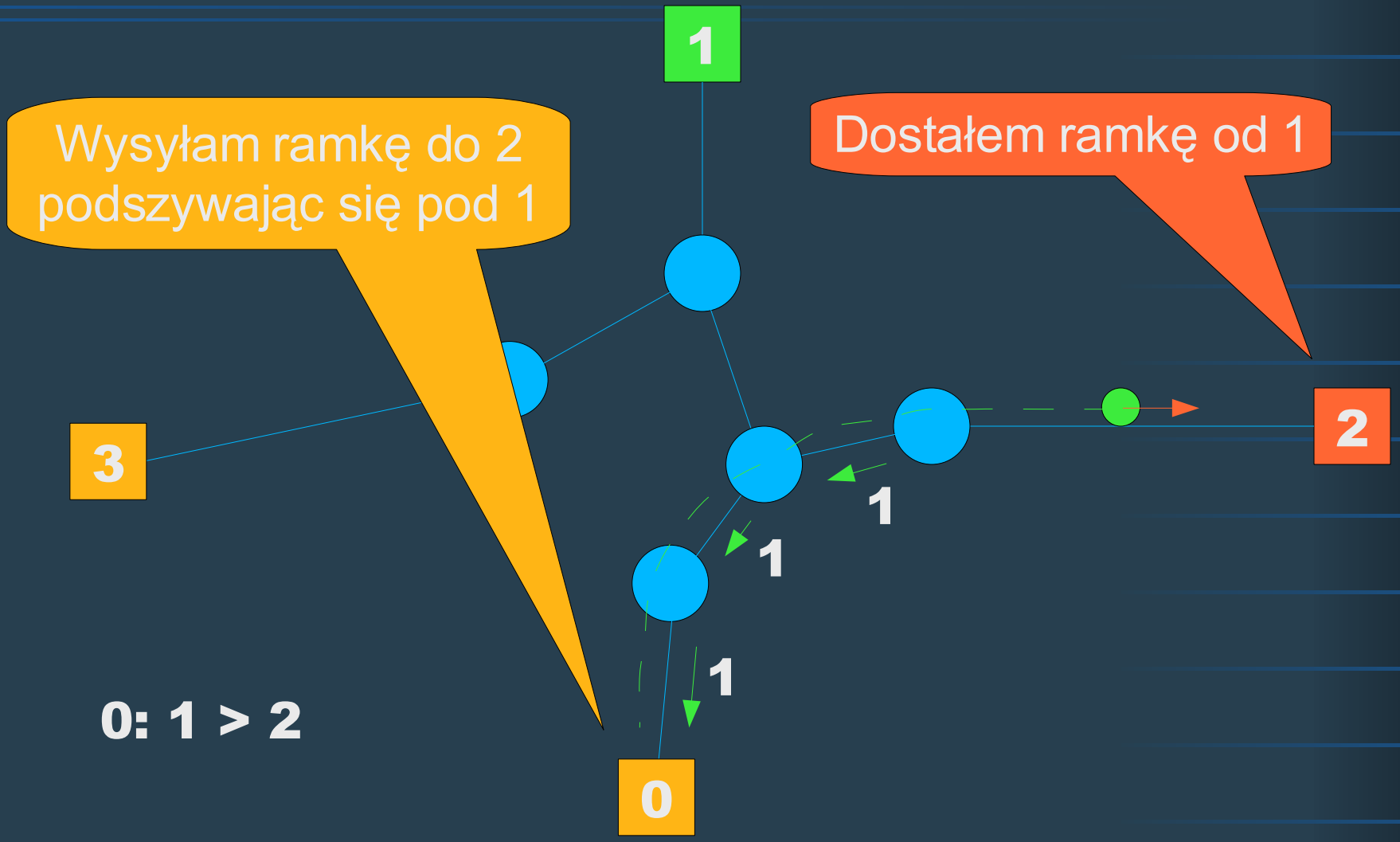
Rozpoznawanie struktury sieci



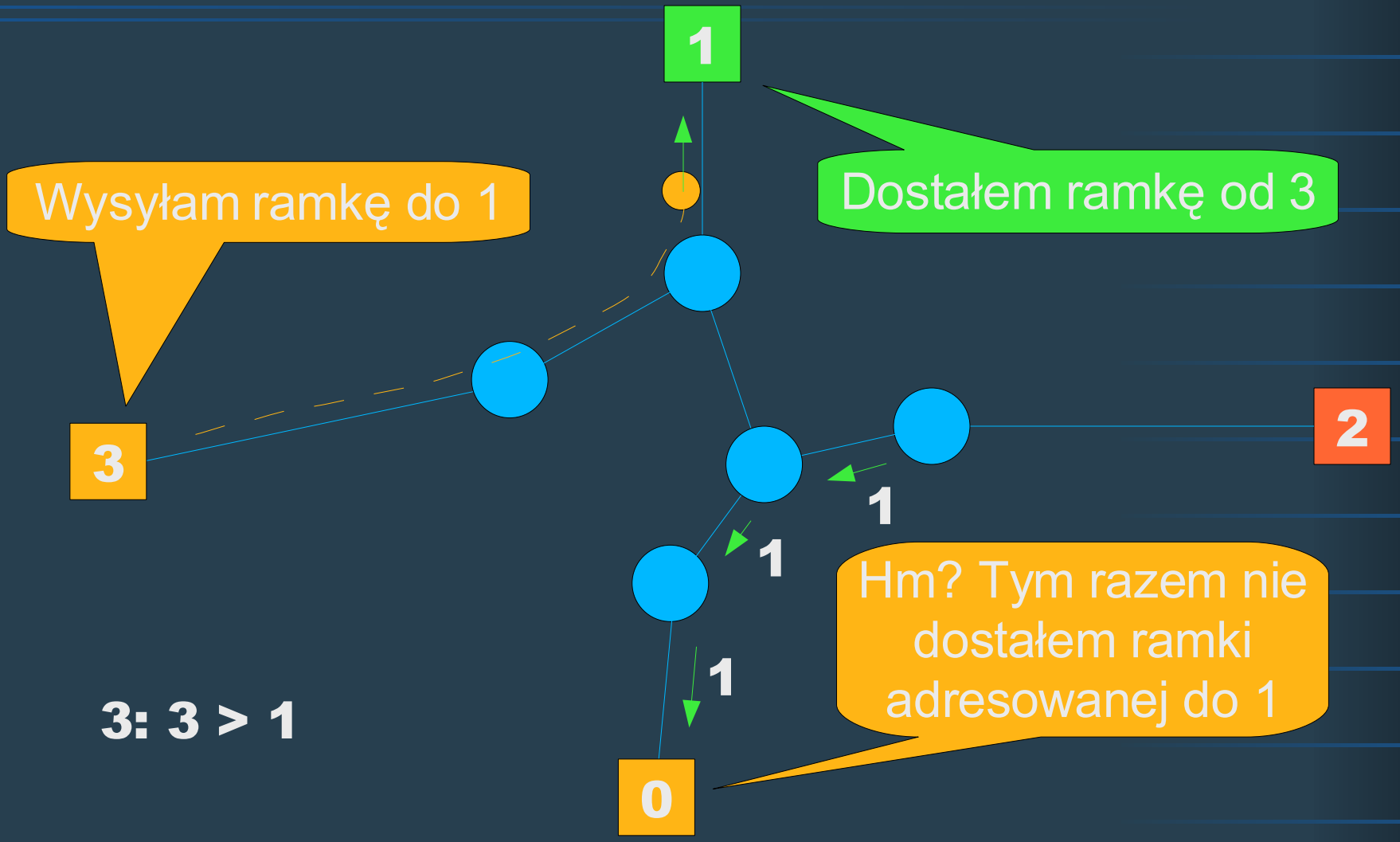
Rozpoznawanie struktury sieci 2



Rozpoznawanie struktury sieci 2

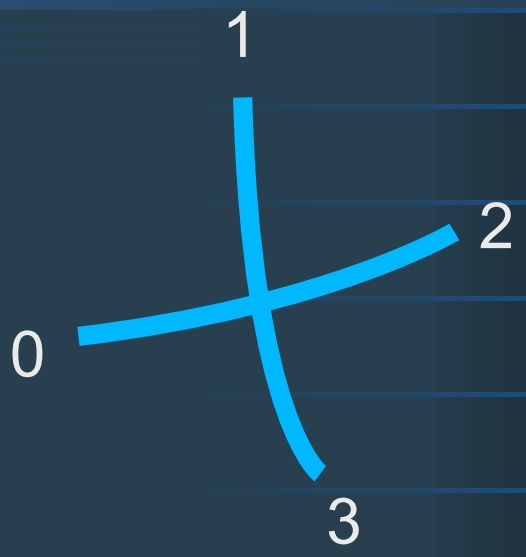


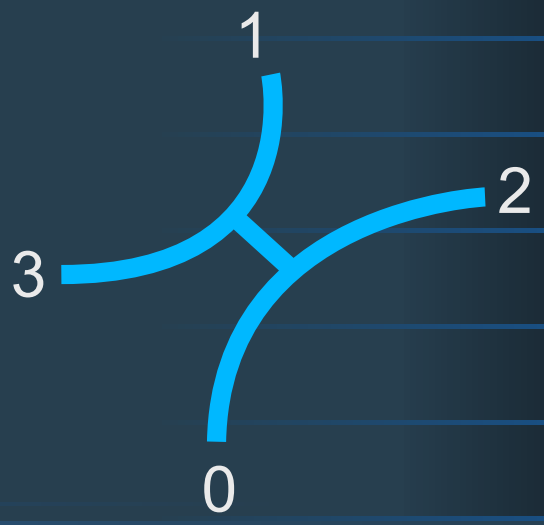
Rozpoznawanie struktury sieci 2



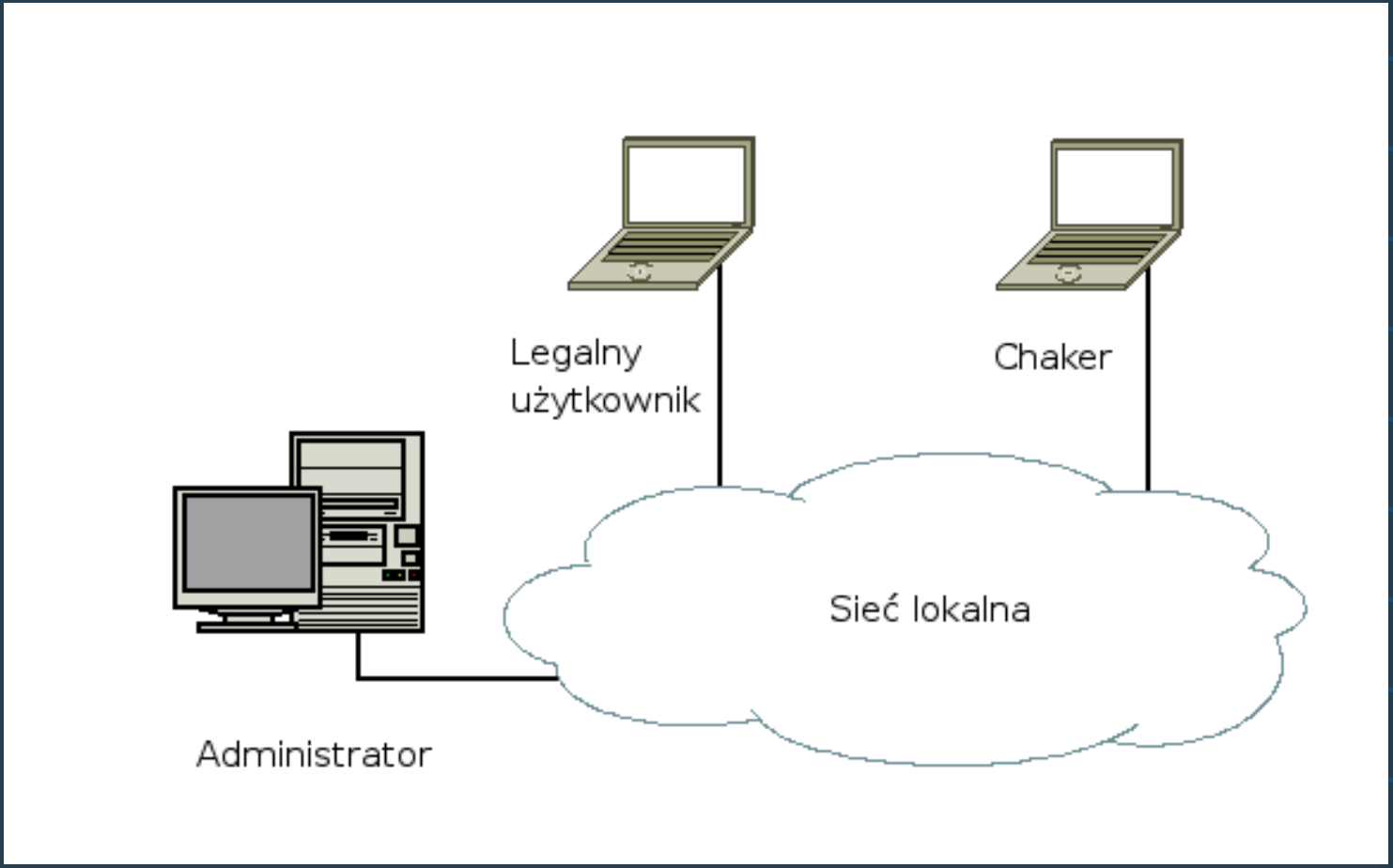
Interpretacja wyników

- Można rozróżnić dwa ułożenia
- Powtarzanie testów dla różnych kombinacji = mapa sieci
- Wady
  - trzeba kontrolować aż dwa hosty dla jednego testu
  - aby zmapować sieć trzeba kontrolować (prawie) wszystkie hosty!



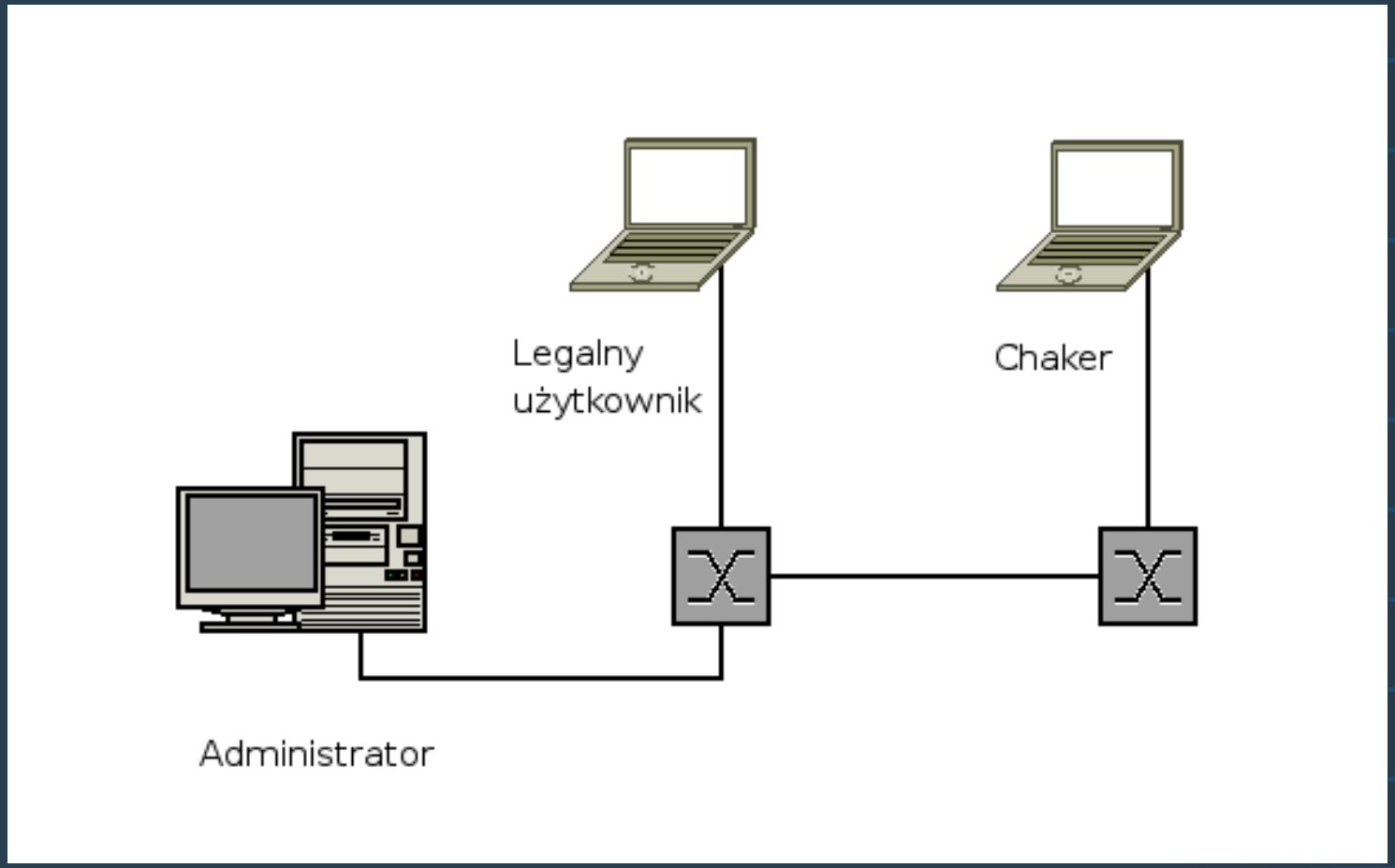


Demonstracja: Etherbat



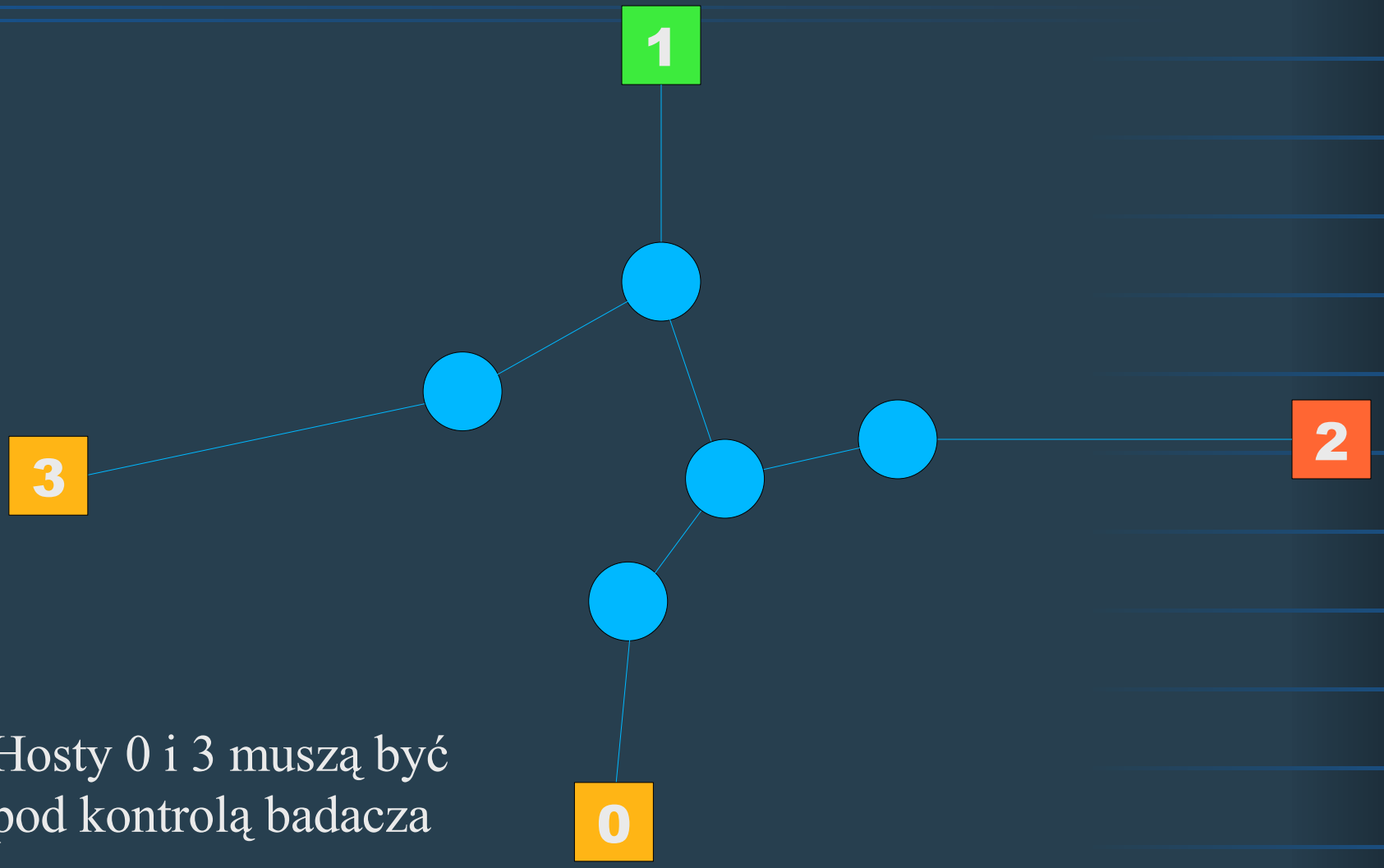
Administrator zna układ przełączników ale nie wie do którego podłączony jest “chaker”

Demonstracja: Etherbat



Administrator zna układ przełączników ale nie wie do którego podłączony jest “chaker”

Przypomnienie sieci z przykładu



Hosty 0 i 3 muszą być pod kontrolą badacza

Pomysł

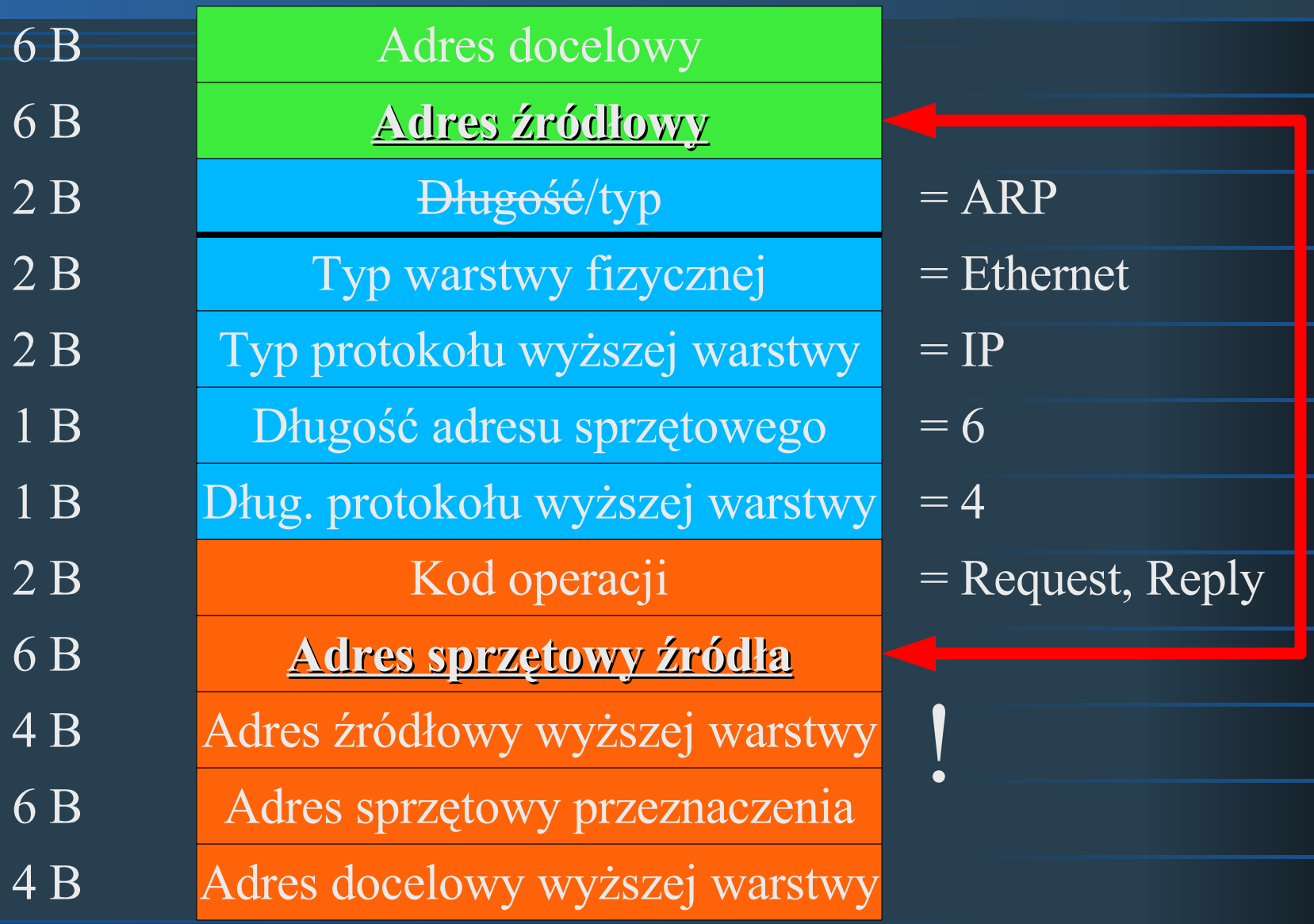
- Czy można poprosić 3 o wysłanie ramki do 1
  - MAC spoofing, SA=3?
    - niweluje skuteczność testu
  - jeśli jest to możliwe bez MAC spoofingu to nie trzeba kontrolować 3
    - test się upraszcza!

Pakiet ARP

Komunikat do wszystkich: Kto ma adres IP=X?
Odpowiedź hosta X: Ja mam ten adres, mój MAC to xx:xx:xx

2 B	Typ warstwy fizycznej	= Ethernet
2 B	Typ protokołu wyższej warstwy	= IP
1 B	Długość adresu sprzętowego	= 6
1 B	Dług. protokołu wyższej warstwy	= 4
2 B	Kod operacji	= Request, Reply
6 B	Adres sprzętowy źródła	(adres MAC)
4 B	Adres źródłowy wyższej warstwy	(adres IP)
6 B	Adres sprzętowy przeznaczenia	(adres MAC)
4 B	Adres docelowy wyższej warstwy	(adres IP)

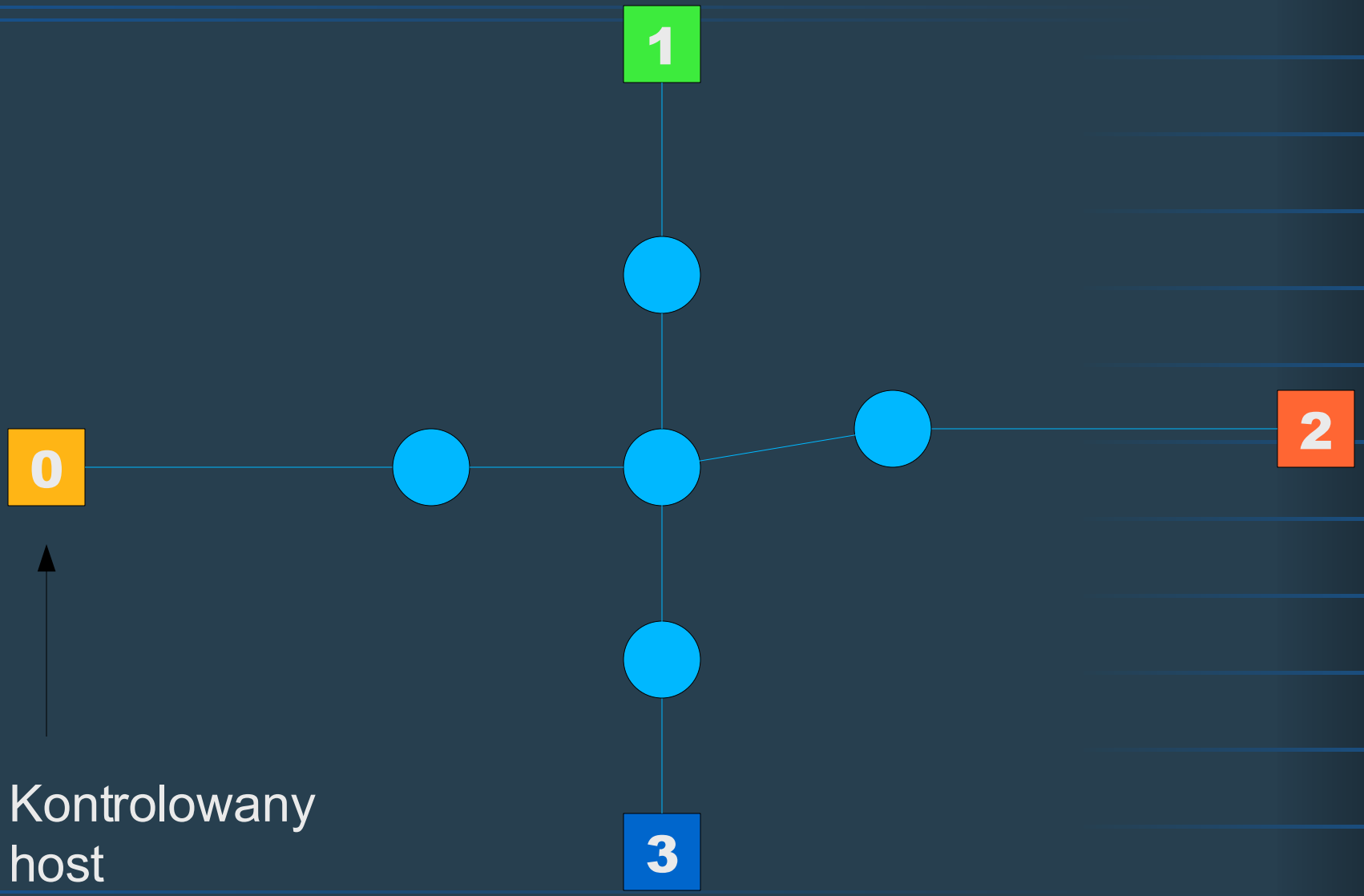
Ramka z pakietem ARP



Asymetryczny ARP Request

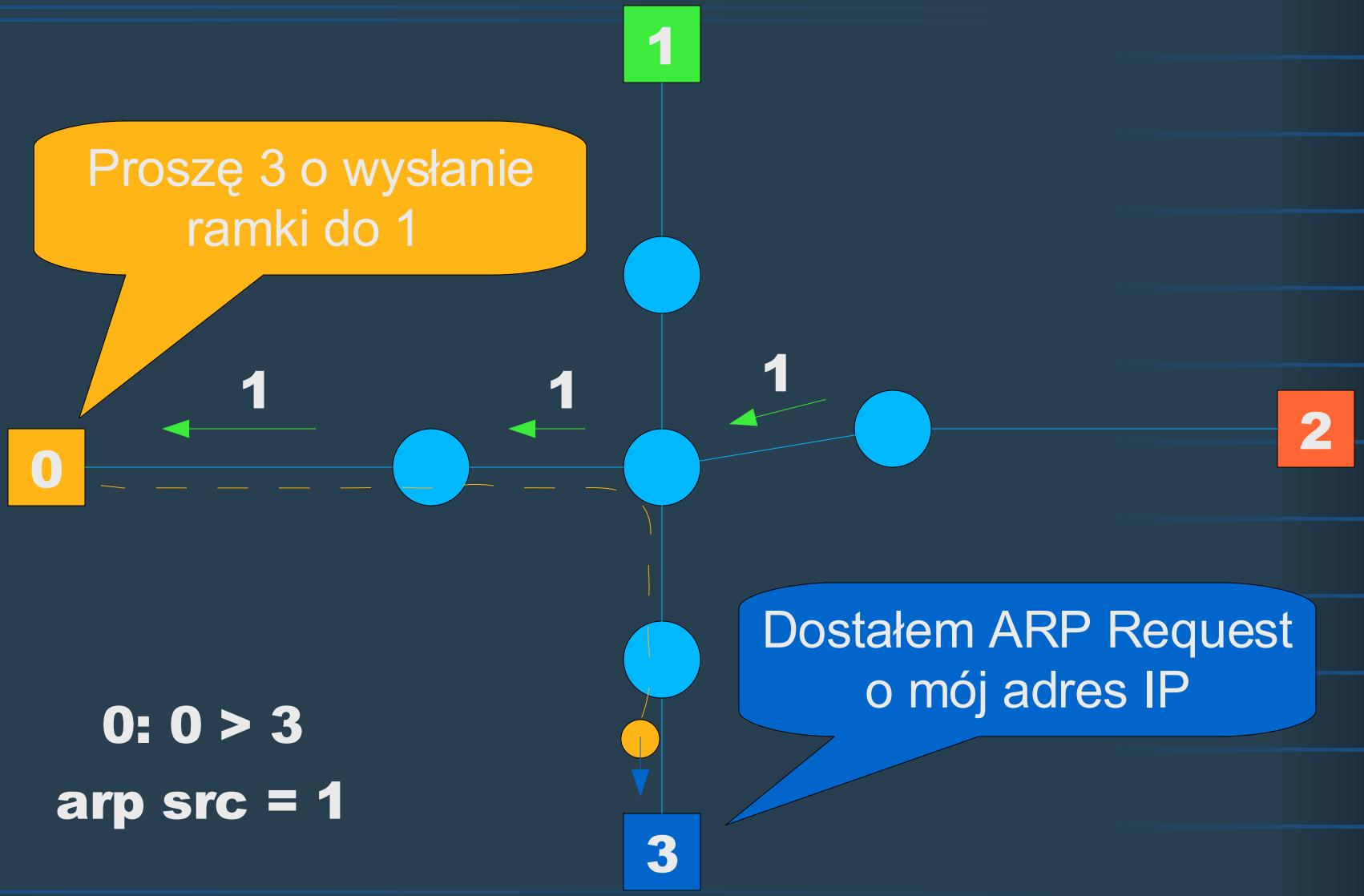
- Adres źródłowy ramki != adres źródłowy podany w nagłówku ARP
- Odpowiedź jest wysyłana na adres z nagłówka ARP, a nie na adres źródłowy ramki!
- “DoS” ze zrzuceniem odpowiedzialności na inny host

Rozpoznawanie struktury sieci 3



Rozpoznawanie struktury sieci 3

Rozpoznawanie struktury sieci 3

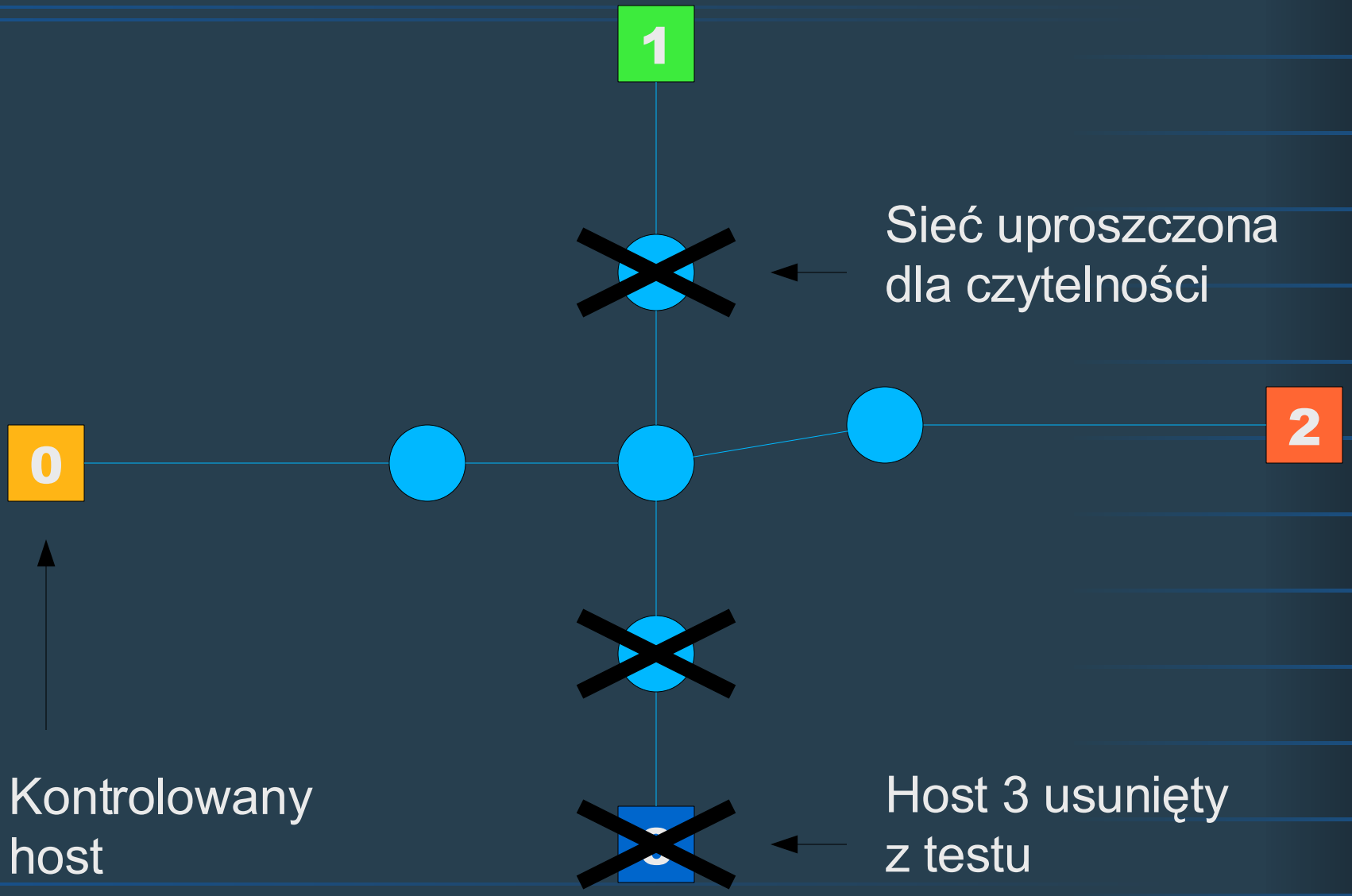


Rozpoznawanie struktury sieci 3

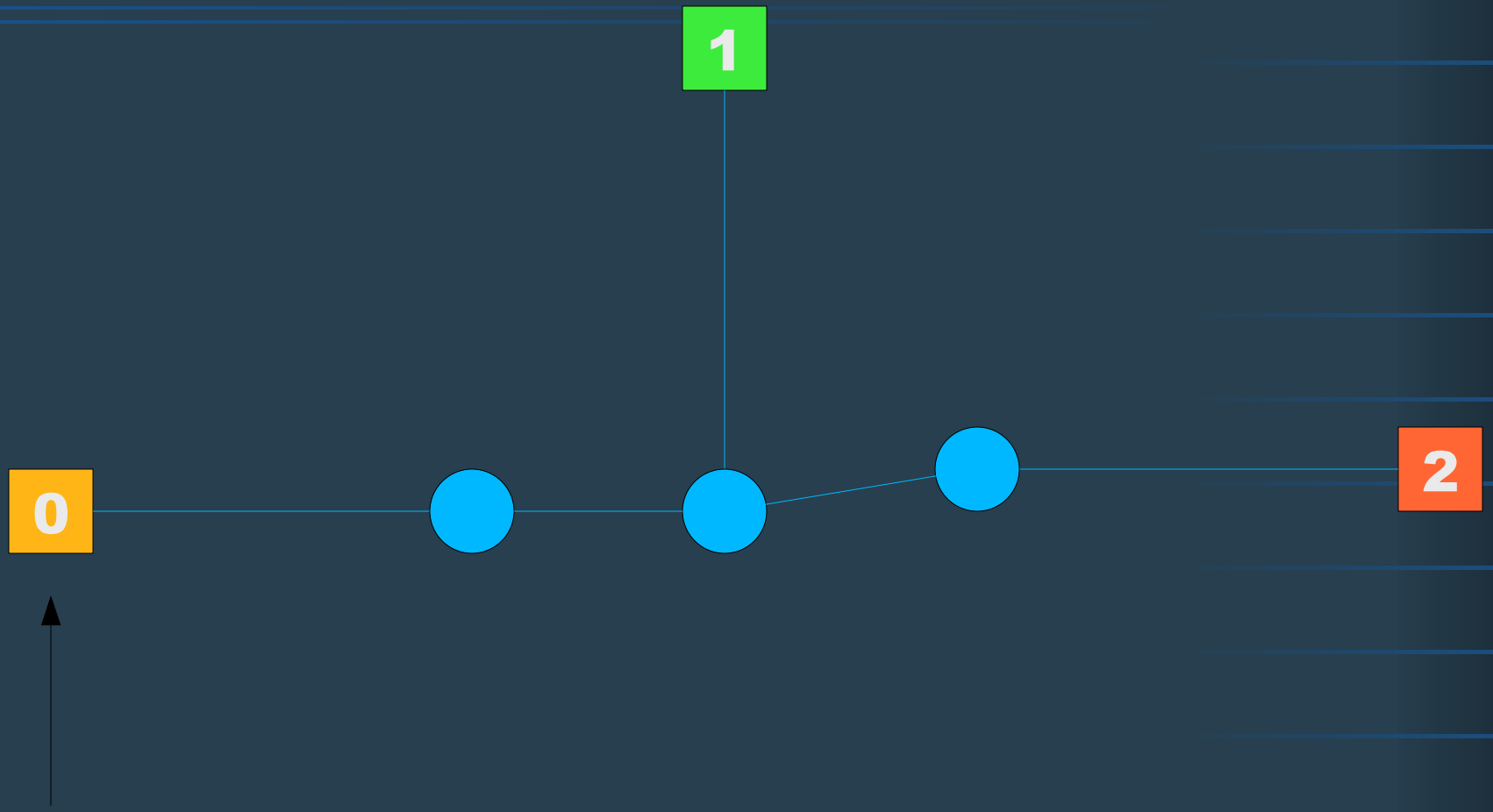
Problem

Ciągle pozostaje wymaganie aż trzech hostów

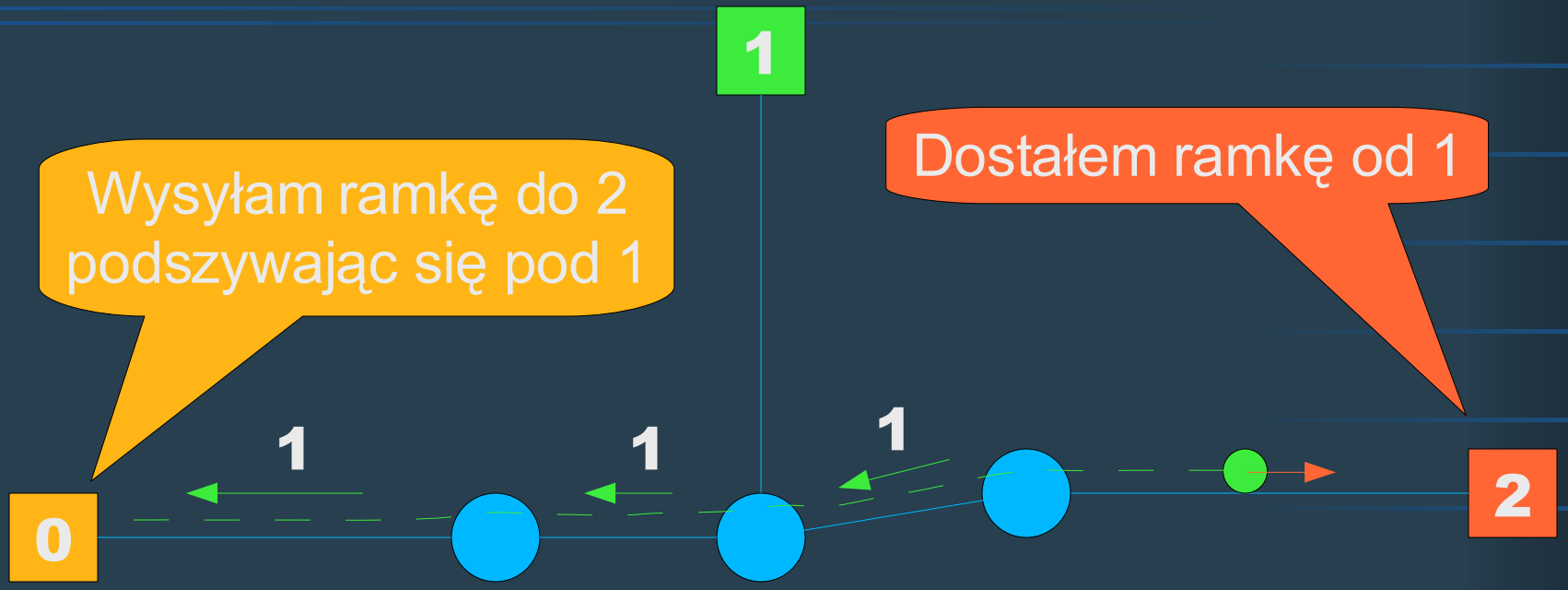
Rozpoznawanie struktury sieci 4



Rozpoznawanie struktury sieci 4

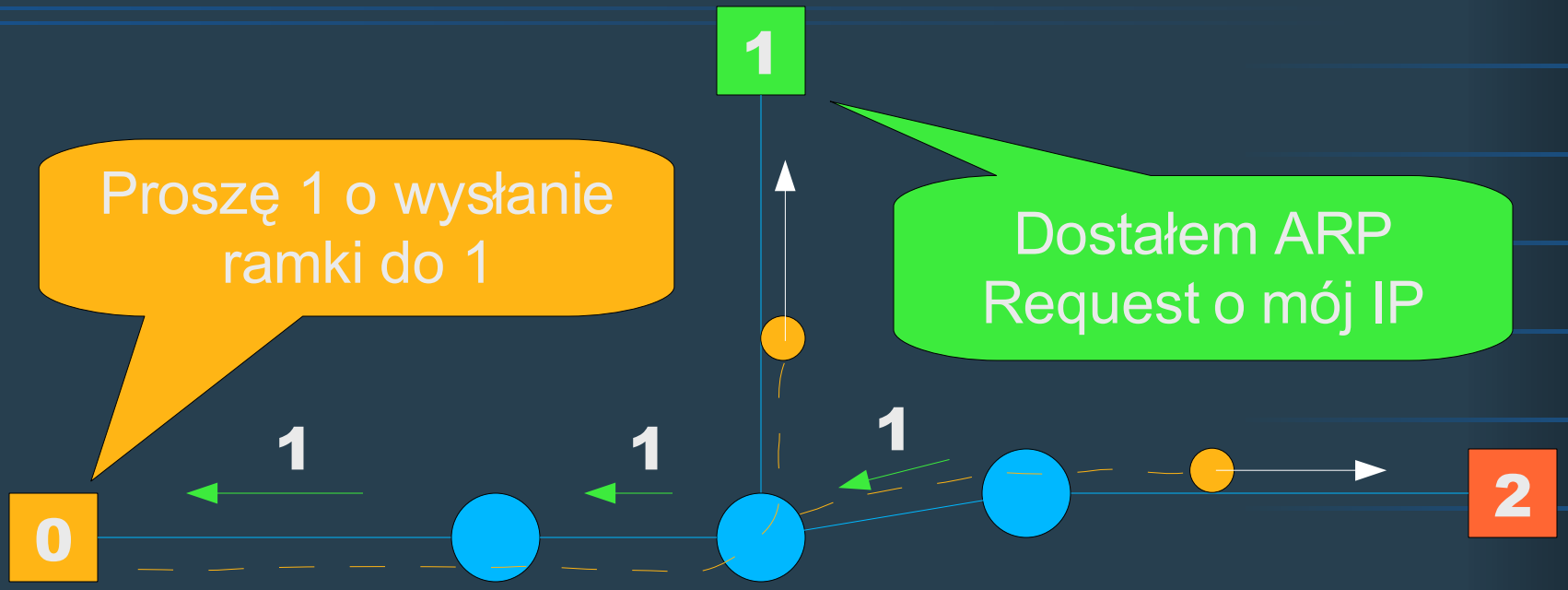


Rozpoznawanie struktury sieci 4



0: 1 > 2

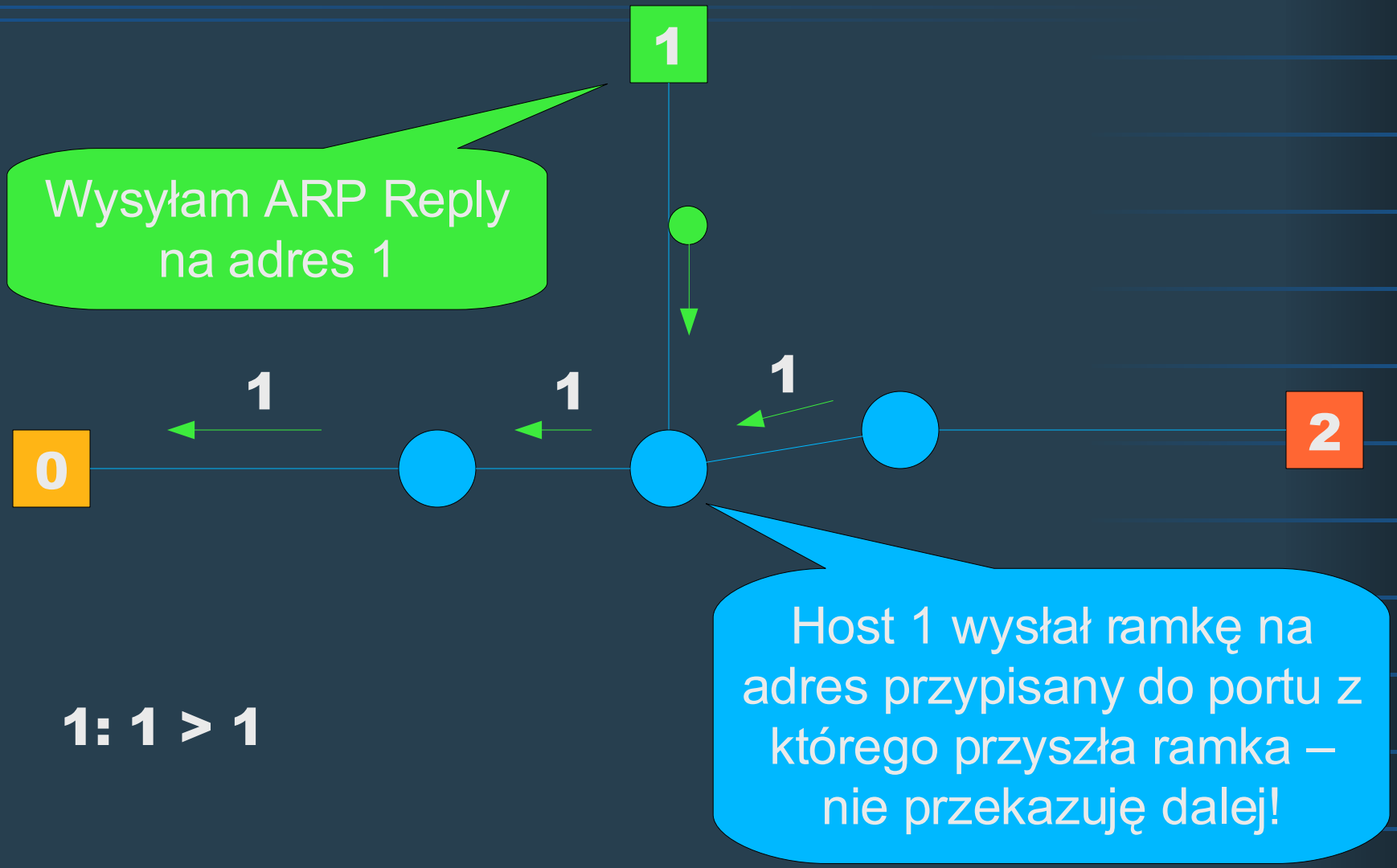
Rozpoznawanie struktury sieci 4



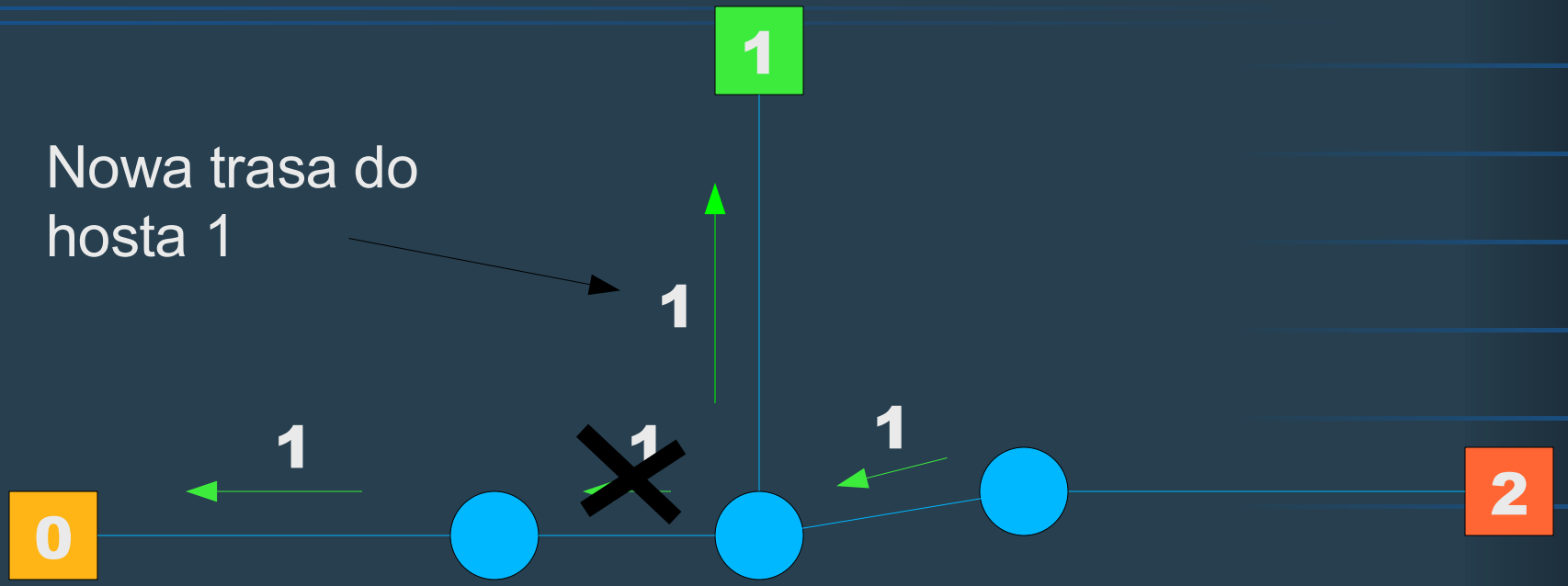
0: 0 > broadcast

arp src = 1 **!**

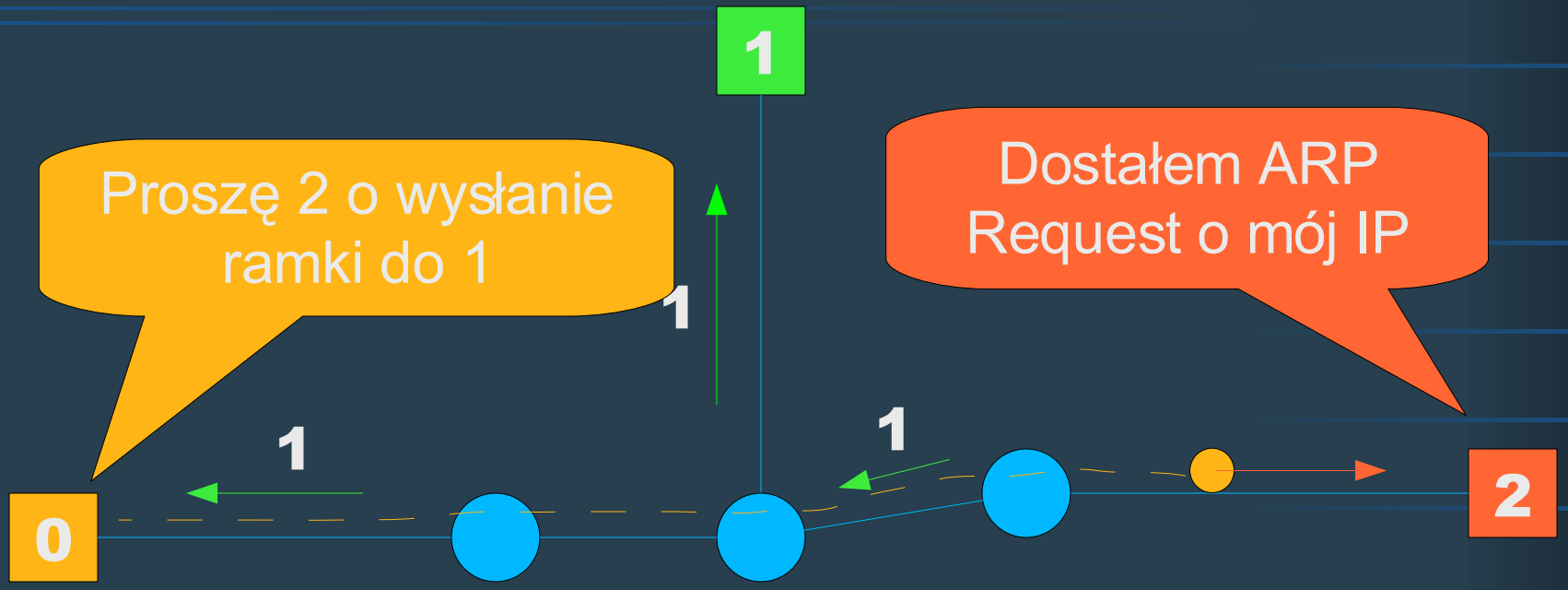
Rozpoznawanie struktury sieci 4



Rozpoznawanie struktury sieci 4



Rozpoznawanie struktury sieci 4



0: 0 > 2

arp src = 1

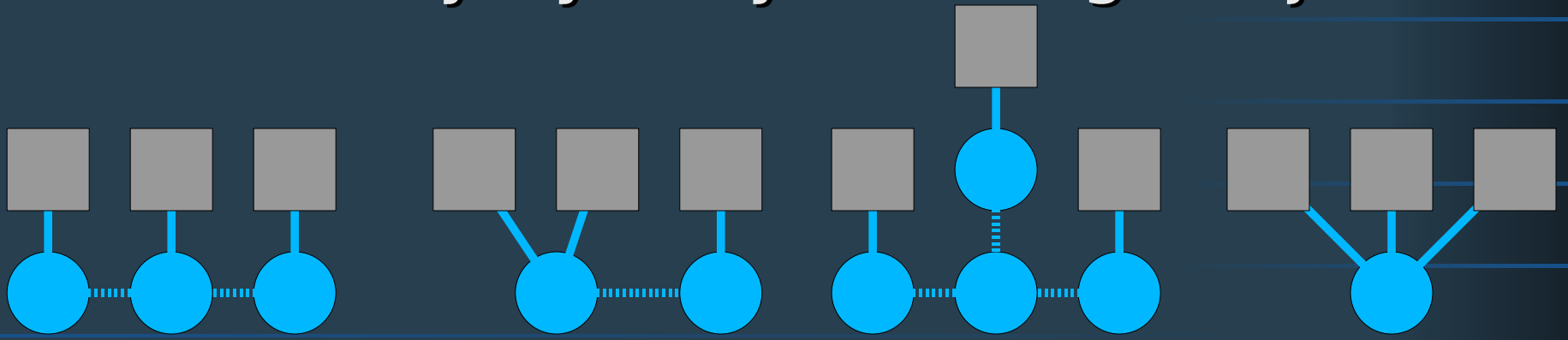
Rozpoznawanie struktury sieci 4

Czyli host 1 znajduje się na trasie 0-2

2: 2 > 1

Etherbat

- 3 testy podstawowe
  - A1, A2 – różnica w kolejności hostów
  - B1
- Test pomocniczy
  - B2 – wykrywanie błędów
- $2^3 = 8$ wykrywanych konfiguracji



Problemy: kiedy wynik jest fałszywy?

- Symetryczny ARP?
- “Cichy host” (w przykładach host 2) transmituje dane
  - niektóre transmisje wykrywane przed podsłuch
  - powtarzanie testów
  - komunikat “jabber” -> kilka konfiguracji hostów
  - testy B gwarantują wykrycie jabberu
- Filtrowanie (port-security itp.)
  - większość przypadków wykrywana
- Duplikaty
  - część można wykryć (nie w tej wersji)
- Straty w sieci – ginące ramki
  - Praktycznie nie do wykrycia
- Switche i “switche”

Switche i “switche”

- Pierwsza ramka SA=DA
  - kolejność procesów uczenia i przekazywania
- Ramki DA=PAUSE
  - zapamiętywanie adresu SA
  - przekazywanie
- Odporność Etherbata

Switche i “switche”

- Specyfikacje układów stosowanych w switchach informują o spełnianiu standardu 802.3
- Te same układy nie zapamiętują adresu źródłowego ramek PAUSE
- 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?
- Wynik:
  - urządzenie które nie zapamiętuje adresu źródłowego ramek PAUSE nie jest switchem w rozumieniu standardu 802.3

Tryb optimistic

- Czasami wykrywane jest wiele konfiguracji
- **`etherbat -o`**
  - Wybór najbardziej prawdopodobnej

Jak nie dać się zlokalizować?

- Zabezpieczenie sieci przed MAC spoofingiem
- Generowanie ruchu
  - najlepiej broadcasty, propagują się wszędzie, uczą wszystkie switche
  - małe ramki, często
  - Blaster na wszystkich komputerach
    - niestety dostepny tylko pod Windows ;-)
- Modyfikować/filtrować ARP
  - arptables

Etherbat: dalsze pomysły

- Tryb batch
  - aplikacja GUI do wizualizacji
- Tryby pracy
  - jeden host - dokładny fingerprinting trasy od A do B
  - trzy hosty (może lepsze wyniki przy dziwnych switchach)
- Wydajność przy dużym pps
  - możliwość uruchamiania etherbata na gateway'u
- Optymalizacja testów
  - teraz – dokładność wyników
  - jak najmniej ramek

Etherbat: dalsze pomysły

- Rozszerzenie narzędzia o inne protokoły
- Każdy “asymetryczny” protokół da się wykorzystać!
  - IPv6
  - IPX
  - ARP+L3/4 (np. IP/ICMP, IP/TCP syn/rst)
  - inne?

Reklama: Ispara Storm Guard

- Eliminacja negatywnych zjawisk w sieci LAN
  - ataki DoS/DDoS
  - wirusy
  - spam
- Kwarantanna zainfekowanych hostów
  - ruch komputera nie dostaje się do Ethernetu!
  - nie wymaga zarządzalnych urządzeń
- Sprzętowa akceleracja przetwarzania pakietów
  - 100mbit, 144800 pps, opóźnienia ~ 0

Więcej informacji:

http://stormguard.ispara.pl

Dziękuję za uwagę.

Paweł Pokrywka

http://www.cryptonix.org

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