**Sieci wirtualne (VLAN),**
**Algorytm budowy drzewa rozpinającego (STP)**

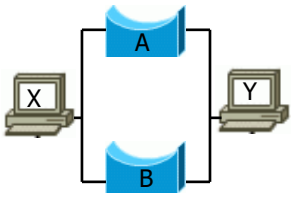
## Redundancja połączeń w sieci

- Czy dokładnie jedna ścieżka pomiędzy dowolnymi dwoma hostami w sieci jest wystarczająca?
- Dostępność
  - czy potrzebujemy dwóch (trzech) aut?
  - 99,999% – ile to jest w skali roku?
  - *single point of failure*
- Równoważenie obciążenia
- Co na to Ethernet?

**Problem**

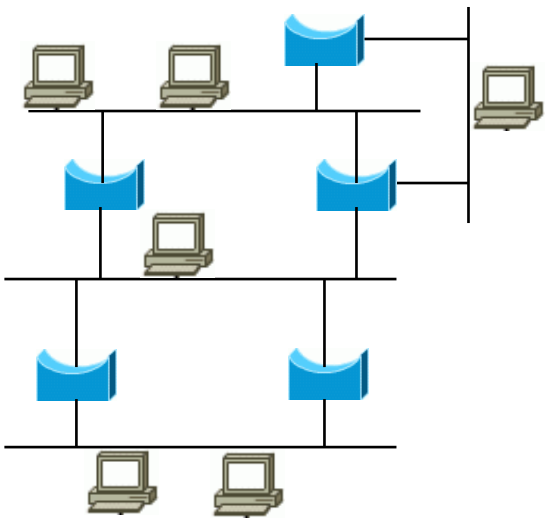
- Standard Ethernet nie pozwala na istnienie naraz więcej niż jednej ścieżki od punktu A do punktu B
- Dlaczego? Może wystąpić krążenie ramek w sieci

Komputer X wysyła ramkę do komputera Y. Tablice obu mostków nie zawierają wpisu dotyczącego Y. Oba zatem przesyłają ramki na drugą stronę, które jednak ponownie dotrą do mostków, które znów je przekażą na drugą stronę, itd....




- Rozwiązanie: dynamiczna adaptacja do warunków panujących w sieci, czasowa deaktywacja nadmiarowych połączeń

**Przykład**



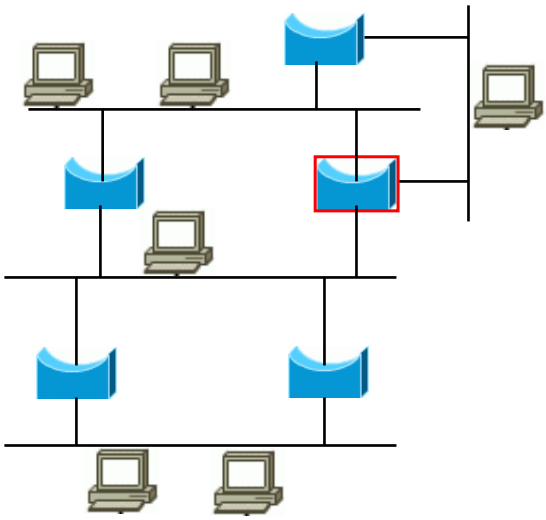
## Algorytm budowy drzewa rozpinającego

- ang. spanning-tree, określony w standardzie IEEE 802.1d
- Nie ma połączeń redundantnych mogących poprawić wydajność, ale istnieją połączenia zapasowe, które są aktywowane w przypadku awarii połączeń głównych
  - w sieci Ethernet aktywna może być tylko jedna ścieżka pomiędzy urządzeniami
- Działanie algorytmu jest przezroczyste dla urządzeń w sieci
- Drzewo rozpinające budowane jest dzięki komunikowaniu się mostków przez wymianę ramek BPDU (Bridge Protocol Data Unit)
- Do wymiany komunikatów BPDU używa się zarezerwowanego adresu grupowego MAC (01:80:c2:00:00:00)

## Algorytm spanning-tree

- Każdy mostek ma swój identyfikator (adres fizyczny) i ustalany administracyjnie priorytet
- Wyznaczany jest korzeń drzewa rozpinającego (*root bridge*) - zostaje nim mostek o najwyższym priorytecie
- Prawo do bycia korzeniem jest okresowo weryfikowane; nowo włączone mostki zakładają zawsze, że są korzeniem.

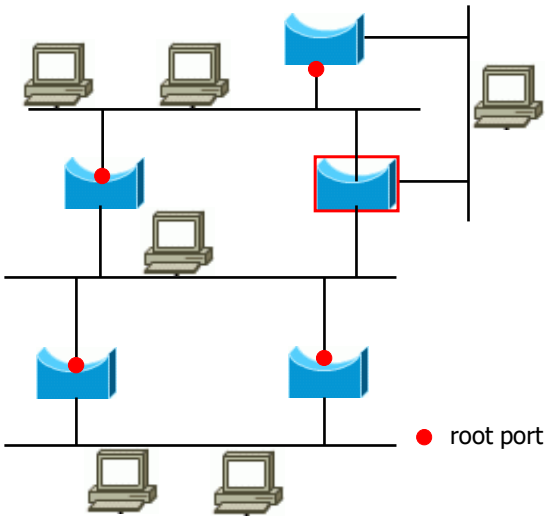
**Przykład, cd.**



**Algorytm spanning-tree, cd.**

- Każdy z mostków określa określa *root path cost* - najtańszą ze ścieżek wiodących od tego portu do korzenia. Port, który posiada najtańszą drogę to *root port*.
- Koszt wyznaczany jest w oparciu o tzw. *designated cost* - koszt przejścia przez dany segment sieci (wartość odwrotnie proporcjonalna do szybkości łącza).

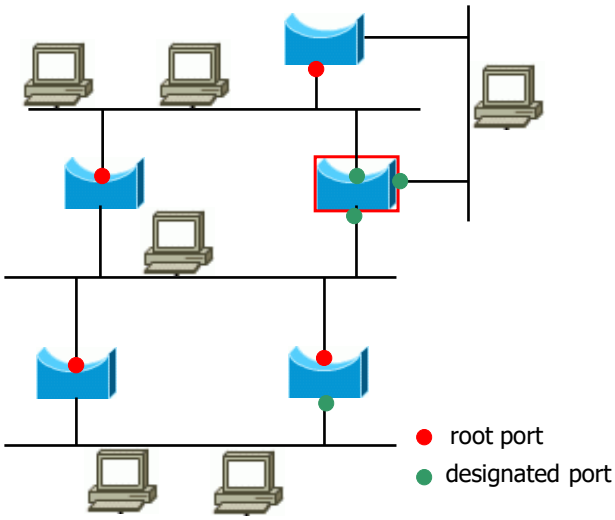
**Przykład, cd.**




**Algorytm spanning-tree, cd.**

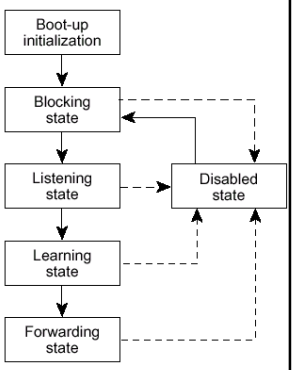
- Dla każdego segmentu sieci wybierany jest jeden mostek - *designated bridge*, który będzie stanowił drogę dojścia do korzenia. Port tego mostka to *designated port*. (Wszystkie porty korzenia są portami *designated*.)
- Wszystkie porty, które nie są ani *root* ani *designated* są zablokowane.

## Przykład, cd.




## Stany portów

- Pięć stanów, w których może znajdować się mostek
  - *blocking*
  - *listening*
  - *learning*
  - *forwarding*
  - *disabled*
- Stany *blocking* i *forwarding* są trwałe, pozostałe są przejściowe
- Potrzeba stanów przejściowych
  - oczekiwanie na rozpropagowanie informacji o zmianie topologii po całej sieci
  - uniknięcie możliwości zaistnienia krótkotrwałych cykli



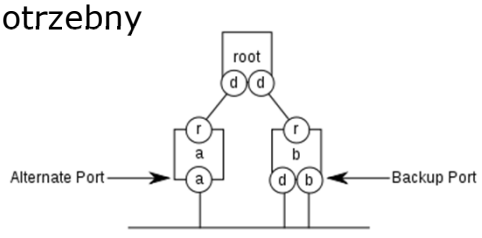

Grafika: www.cisco.com

## Ramki BPDU

- Korzeń co pewien czas (*hello time*) wysyła ramki BPDU
- Ramki BPDU są otrzymywane przez mostki nie będące korzeniem na porcie *root* i wysyłane do segmentu sieci poprzez port *designated*
- Jeśli przez pewien czas mostki nie otrzymują komunikatów BPDU przystępują do rekonfiguracji topologii, w przypadku awarii korzenia dokonuje się elekcja nowego

## Rapid Spanning Tree Protocol

- Rapid spanning-tree protocol (RSTP), określony został w standardzie IEEE 802.1w
- Rozszerza STP dodając „Alternate Port" i „Backup Port"
- RSTP jest znacznie szybszy niż STP
- Czas zbieżności (czas potrzebny na zbudowanie drzewa rozpinającego):
  - STP: 30 – 50 sekund
  - RSTP: 6 sekund




Grafika: wikipedia

**Rapid Spanning Tree Protocol**

- Połączenie stanów "blocking" i "listening" w jeden stan "discarding", gdzie port nasłuchuje ale nie może wysyłać ani odbierać ramek
- Tworzenie i rekonfiguracja (w przypadku awarii) drzewa jest szybsza niż w STP z powodu zmiany polegającej na tym że porty tras alternatywnych nie są w stanie "blocking" ale w stanie "discarding"
- Po wykryciu awarii port "discarding" ("Alternate Port" i "Backup Port") natychmiast przejmuje rolę "forwarding" (bez oczekiwania ok. 30 s jak w STP)
- Wykorzystuje nowy format ramki BPDU (inny niż STP)

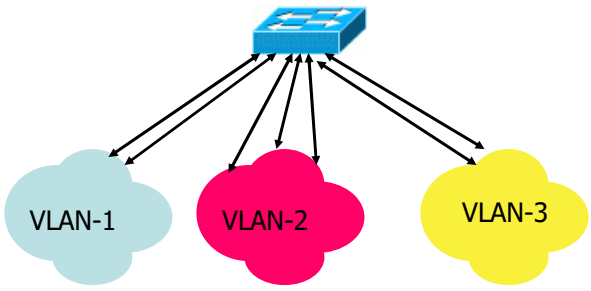
**Miejsce mostków w modelu OSI/ISO**

- Mostki pracują w warstwie łącza danych, rozumieją jedynie adresy MAC
- Łączą sieci o tych samych lub różnych standardach podwarstwy MAC, jednak warstwa LLC jest wspólna, zatem można połączyć np. sieć Ethernet i Token Ring

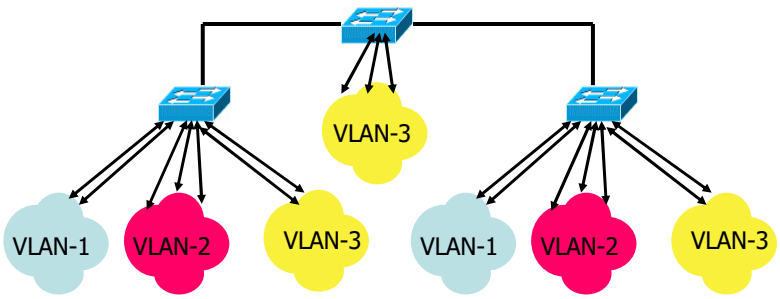
## Przełącznica (switch)

- Mostek wieloportowy – identyczna zasada działania
  - zmniejszenie domeny kolizyjnej
  - możliwość równoczesnej transmisji w różnych segmentach sieci
  - obsługa protokołu spanning-tree
- Mikrosegmentacja – tylko jeden host na jednym porcie
- Przełącznice asymetryczne - wiele portów wolnych (10/100 Mb/s) i jeden (kilka) szybkich (1000 Mb/s)
  - stacje robocze i serwery
  - problem z buforowaniem
- Szybsze niż mostki, zazwyczaj stosują mechanizm *cut-through*

## Idea sieci wirtualnych (VLAN)



## VLAN na wielu przełącznicach




## Sieci wirtualne: ogólnie

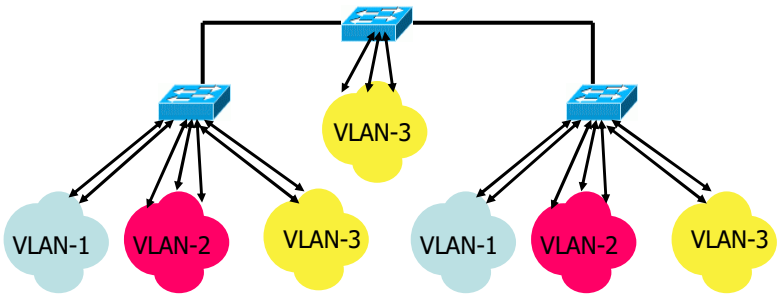
- Logiczne (nie: fizyczne) grupowanie użytkowników
- Są to zadania routerów, wykonywane jednak szybciej
- Reguła 80/20
- Zalety sieci wirtualnych
  - ograniczenie domeny rozgłoszeniowej
  - lepsza skalowalność sieci
  - większe bezpieczeństwo sieci
  - (re)konfiguracja VLAN jest programowa: nie trzeba zmieniać fizycznych połączeń w sieci

## Przynależność do VLAN

- Statyczna (*port-based*, *port-centric*)
  - w oparciu o numer portu
  - konfigurowana administracyjnie
  - pełna kontrola i największe bezpieczeństwo
- Dynamiczna
  - w oparciu a adres MAC lub warstwę trzecią
  - mechanizm konfigurowany administracyjnie
  - działanie automatyczne
  - np. mechanizm VMPS zarządzający odwzorowaniem MAC-VLAN

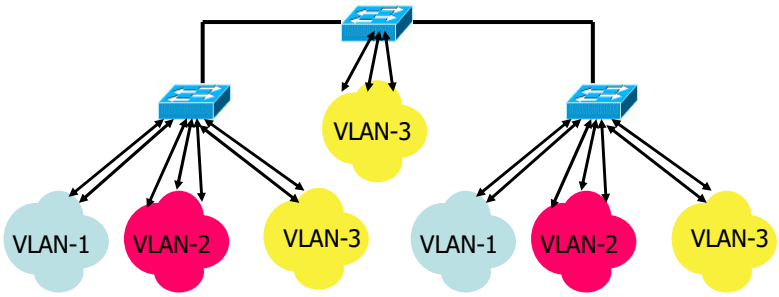
## Sieci wirtualne na wielu przełącznicach

- Na czym polega problem?
- Jakieś pomysły rozwiązania?



## Sieci wirtualne na wielu przełącznicach

- Zadanie niezbyt proste
- Realizowane w różny sposób
  - standard: IEEE 802.1q
  - rozwiązanie Cisco: ISL (InterSwitch Link)




## *Trunk* – co to?

- Pojedyncze łącze na którym ruch z wielu urządzeń jest multipleksowany
- Łącze (zazwyczaj) o dużej przepustowości
- Łącze punkt-punkt
- Szkielet sieci (*backbone*)

**Sposoby tagowania**

- 802.1q – standard IEEE
  - dodatkowe czerobajtowe pole między adresami a polem typ/długość
  - zwiększenie maksymalnej długości ramki z 1518 B do 1522 B
- ISL – opracowany przez Cisco, obecnie wycofywany
  - enkapsulacja oryginalnej ramki (tunelowanie)
  - 26 B nagłówka i 4 bajty zakończenia ramki

**Ethernet – podsumowanie**

- Początek
  - Medium dzielone
  - Kabel koncentryczny
  - 10 Mb/s
- Obecnie
  - Medium dedykowane
  - Segmentacja sieci
  - Skrętka, światłowód
  - Przepustowości ≥ 1000 Mb/s