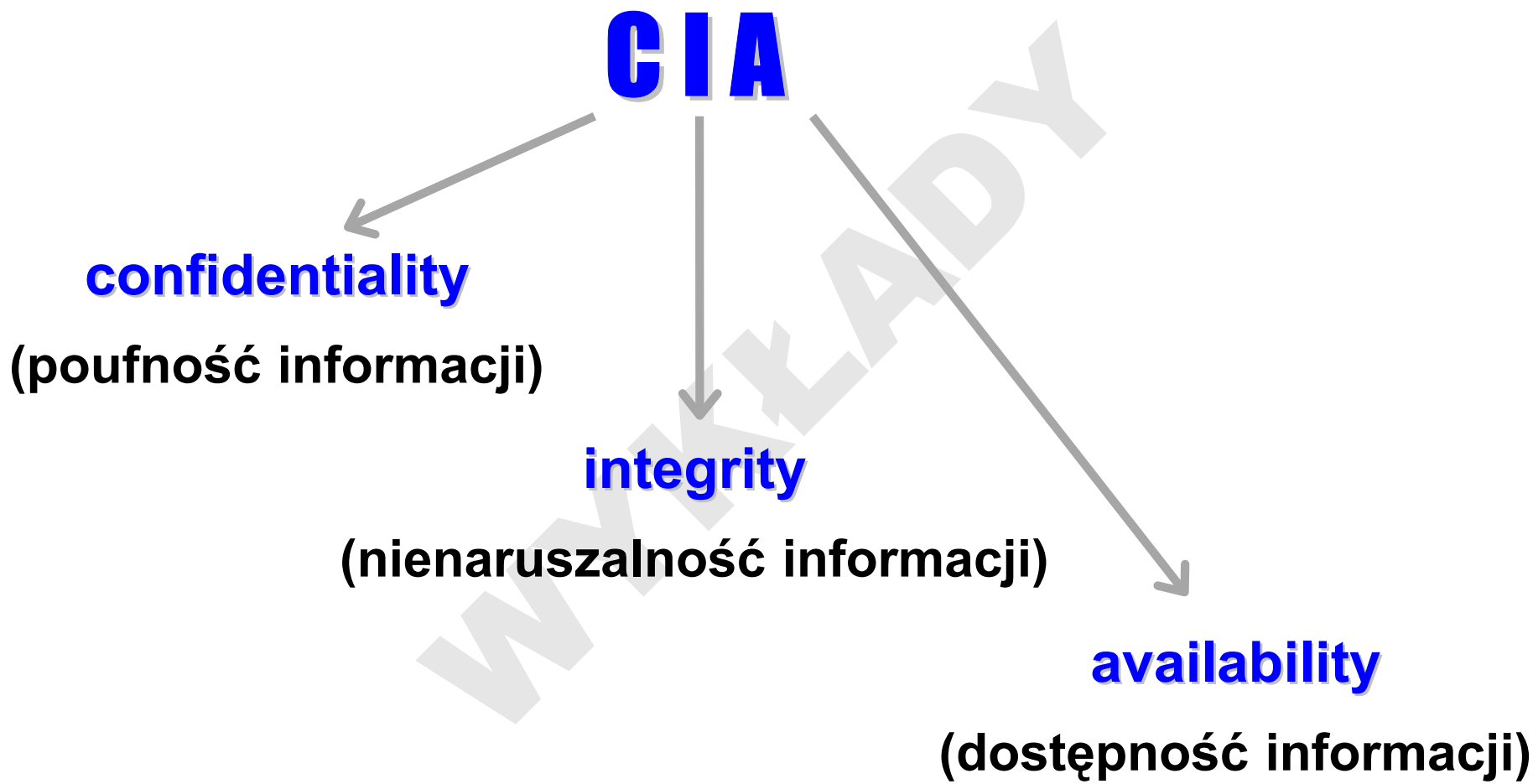
Podstawowe zagadnienia bezpieczeństwa systemów informatycznych

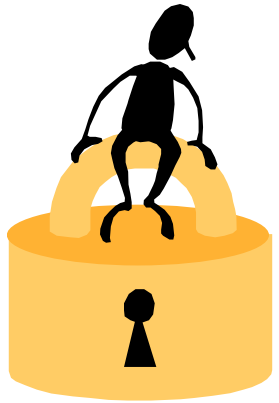
Zagadnienia

1. **Ogólne własności bezpieczeństwa informacji**
   - poufność
   - nienaruszalność
   - dostępność
2. **Wybrane mechanizmy zapewniania bezpieczeństwa**
   - uwierzytelnianie, autoryzacja
   - listy ACL
   - redundancja, archiwizacja

Ogólne własności bezpieczeństwa



Poufność informacji



Zagrożenia:

1. nieuprawniony dostęp do danych w miejscu składowania
2. nieuprawniony dostęp do danych w miejscu przetwarzania
3. podsłuchanie danych przesyłanych w sieci

podsłuch zdalny (receptory Van Ecka) – do 2. i 3.

Poufność informacji

Mechanizmy obrony:

- uwierzytelnianie użytkowników
- autoryzacja i kontrola dostępu do zasobów
- utrudnianie podsłuchu

Poufność informacji

Uwierzytelnianie (identyfikacja) użytkowników

- hasła ← problem złamania hasła (podsłuchanie, odgadnięcie, zdobycie)
- jednokrotne uwierzytelnianie (*single sign-on*)
- hasła jednorazowe
- karty identyfikacyjne (*security tokens*): smart cards, keys, USB tokens
- czytniki biometryczne (trafiają pod strzechy
  np. notebooki Acer Travel Mate z czytnikiem linii papilarnych)

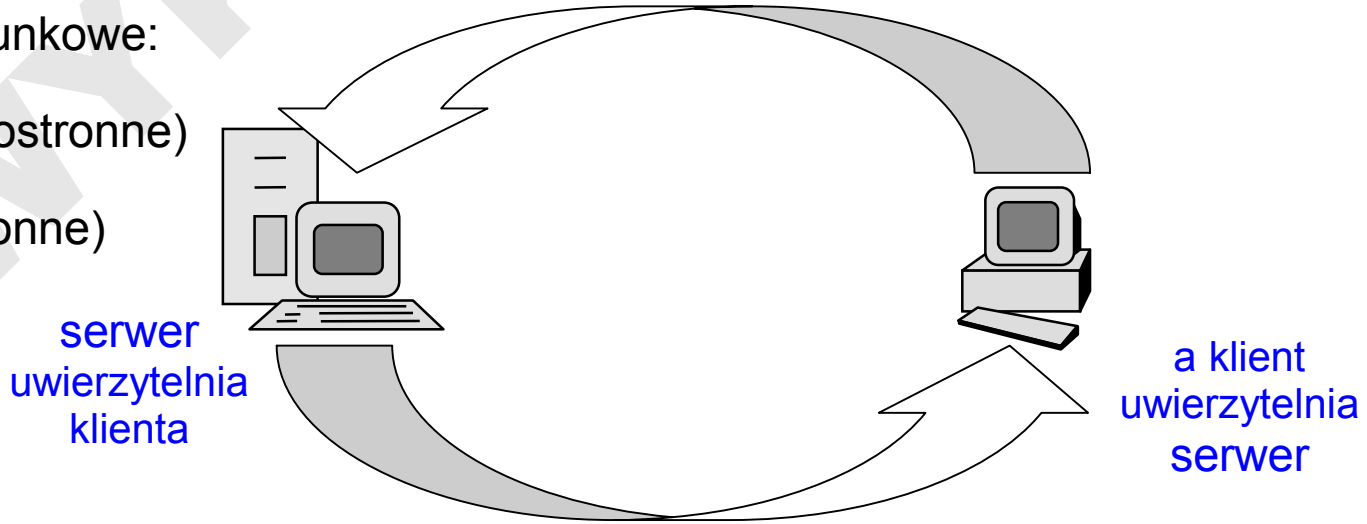
Uwaga: hasła domyślne (instalacyjne) !

Uwierzytelnianie

Rodzaje uwierzytelniania:

- uwierzytelnianie jednokierunkowe:

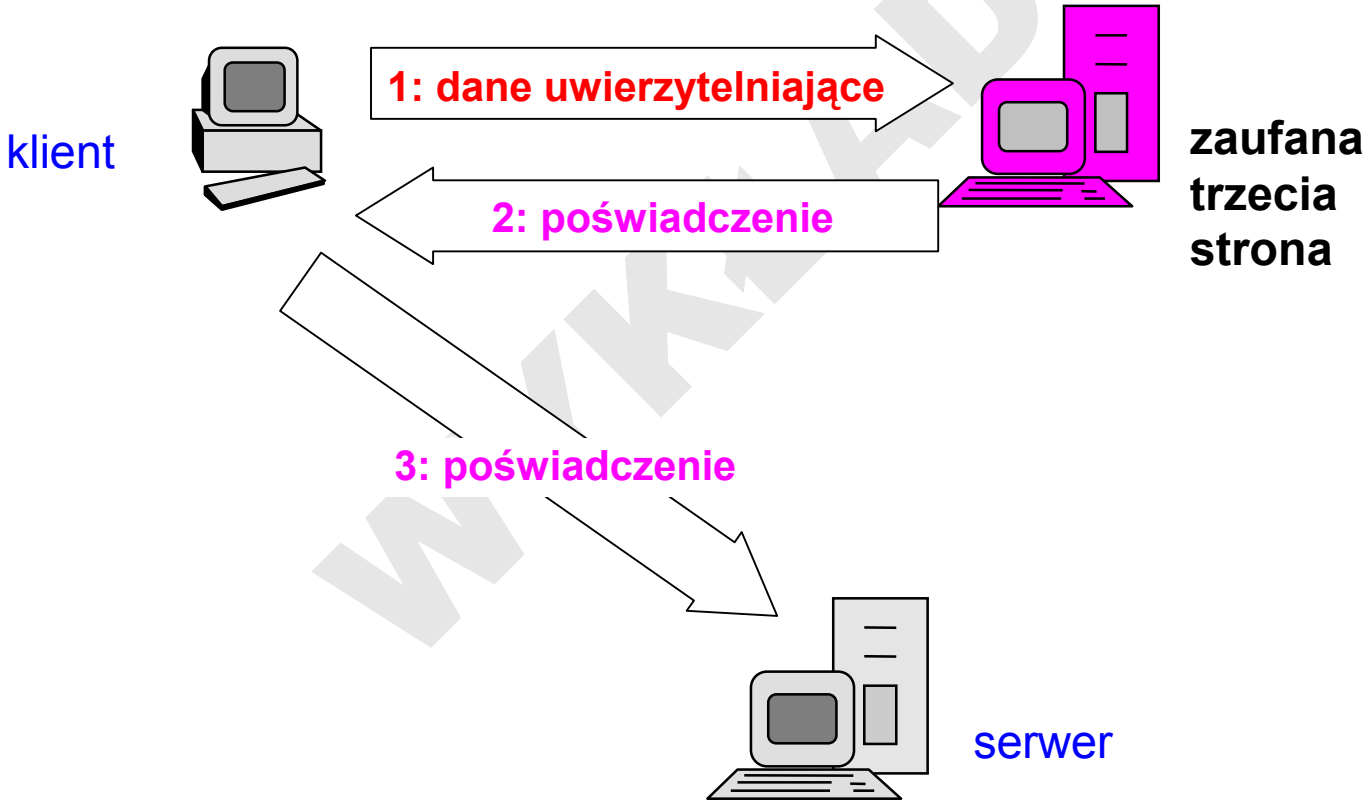
- uwierzytelnianie dwukierunkowe:
  - dwuetapowe (2 x jednostronne)
  - jednoetapowe (obustronne)



Uwierzytelnianie

Rodzaje uwierzytelniania:

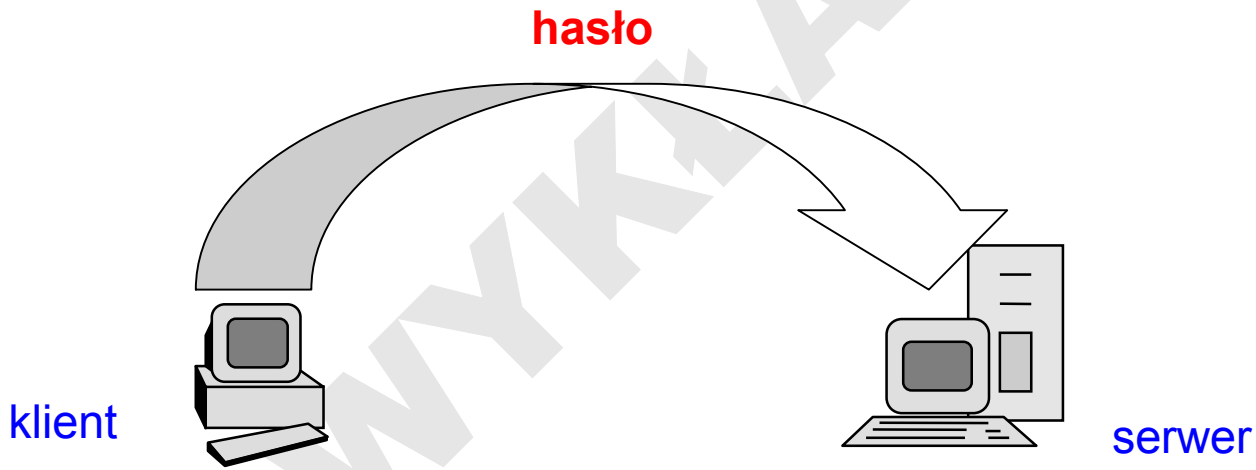
- uwierzytelnianie z udziałem zaufanej trzeciej strony



Uwierzytelnianie

Klasyczne uwierzytelnianie użytkownika:

- serwer pyta o nazwę użytkownika, a następnie o hasło i decyduje o dopuszczeniu do sieci



- nazwa użytkownika i hasło są przesyłane tekstem jawnym !

Uwierzytelnianie

Hasła

- hasło można złamać:
  - odgadnąć, np. metodą słownikową (*brute-force dictionary attack*)
  - wykraść z systemowej bazy haseł użytkowników
  - pozyskać inną metodą (np. kupić)
- hasła się starzeją

Uwierzytelnianie

Hasła

Raport Klaina (1990,1995):

- wejściowy rozmiar słownika: ok. 1 500 haseł
- nazwy użytkowników w systemie, ich inicjały oraz inne dostępne informacje (np. daty urodzin)
- imiona i ich permutacje, nazwy miejsc, nazwiska sławnych ludzi, tytuły filmów i książek S-F oraz nazwiska postaci, dziedziny sportu i terminy sportowe
- przekształcenia: np. zmiana pierwszej litery na wielką, zastąpienie pierwszej litery znakiem sterującym, zamianę litery o na 0 czy l na 1, utworzenie liczby mnogiej, dodanie przed- i przyrostków
- kombinacje małych i wielkich liter
- łącznie ok. 1 000 000 słów

Uwierzytelnianie

Hasła

Raport Klaina – rezultaty:

- nazwa użytkownika: ponad 10%
- nazwy pospolite: ponad 16%
- imiona żeńskie: 4,8%
- imiona męskie: 4%
- mity i legendy: 2%
- sport: 0,8%
- …
- /usr/dict/words: blisko 30%

Uwierzytelnianie

Hasła

Raport Klaina – rezultaty:

- prawdopodobieństwo odgadnięcia hasła:

$$P = \frac{L \cdot R}{S}$$

gdzie L = czas obowiązywania hasła

R = współczynnik szybkości (ilość prób na jedn. czasu)

S = przestrzeń haseł

dla haseł o długości k z alfabetu N znaków: $S = N^k$

Uwierzytelnianie

Hasła

czego nie wolno:

- wybierać hasła o długości krótszej niż 6 znaków
- wybierać jako hasło znanego słowa, imienia, nazwiska, daty urodzenia, numeru telefonu, numeru rejestracyjnego
- zmieniać hasła tak, by nowe było zależne od starego
  (np. z 012345 na 123456)
- zapisywać hasła w widocznych lub łatwo dostępnych miejscach
  (jak np. fragment biurka zakryty klawiaturą, wnętrze szuflady
  czy dyskietka / płyta z danymi)
- informować nikogo o swoim haśle

Uwierzytelnianie

Hasła

co należy:

- wybierać długie i mało znane słowo lub frazę (kombinacja różnych znaków)
- wybrać hasło w sposób na tyle losowy na ile tylko możliwe
- zmieniać hasło możliwie często, lecz w nieprzewidywalny sposób
- zmienić hasło natychmiast, jak tylko rodzi się podejrzenie, że ktoś mógł je poznać

co można:

- zlecić systemowi wygenerowanie trudnego hasła

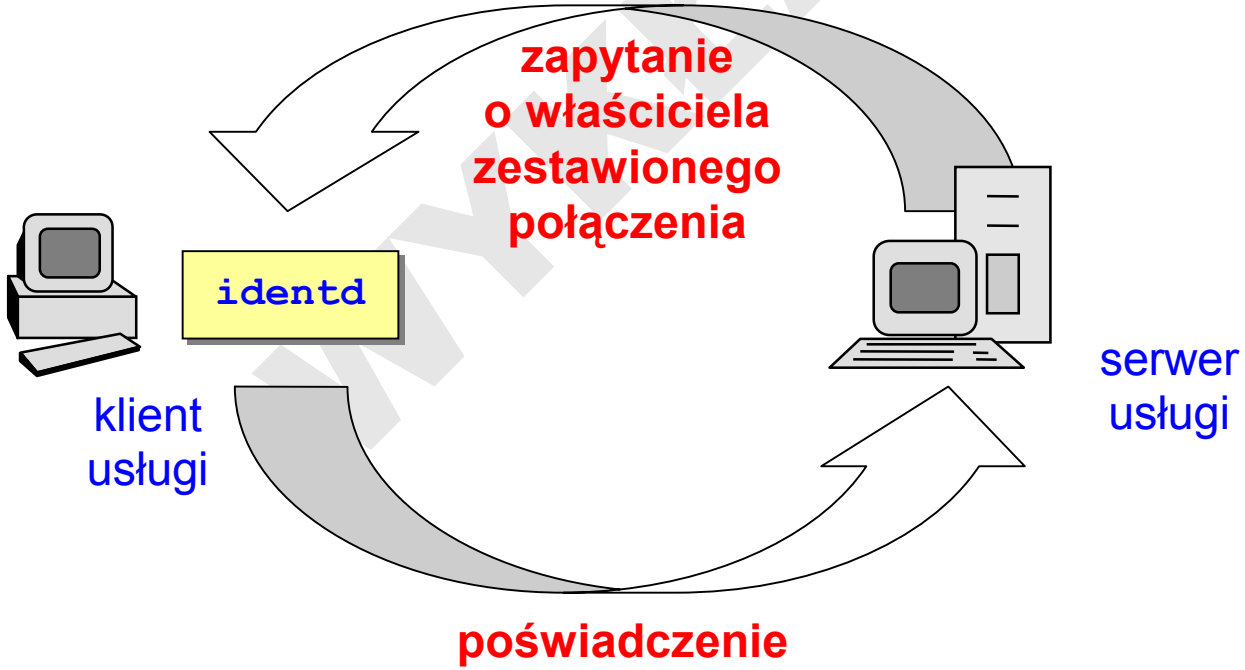
Przykładem trudnego do złamania hasła może być SzNsndJsAsz, *które powstało z fragmentu fraszki Jana Kochanowskiego pod tytułem „Na zdrowie”:*

„Ślachetne zdrowie, Nikt się nie dowie, Jako smakujesz, Aż się zepsujesz”

Uwierzytelnianie

Prosta weryfikacja tożsamości użytkownika (*ident*, RFC 1413):

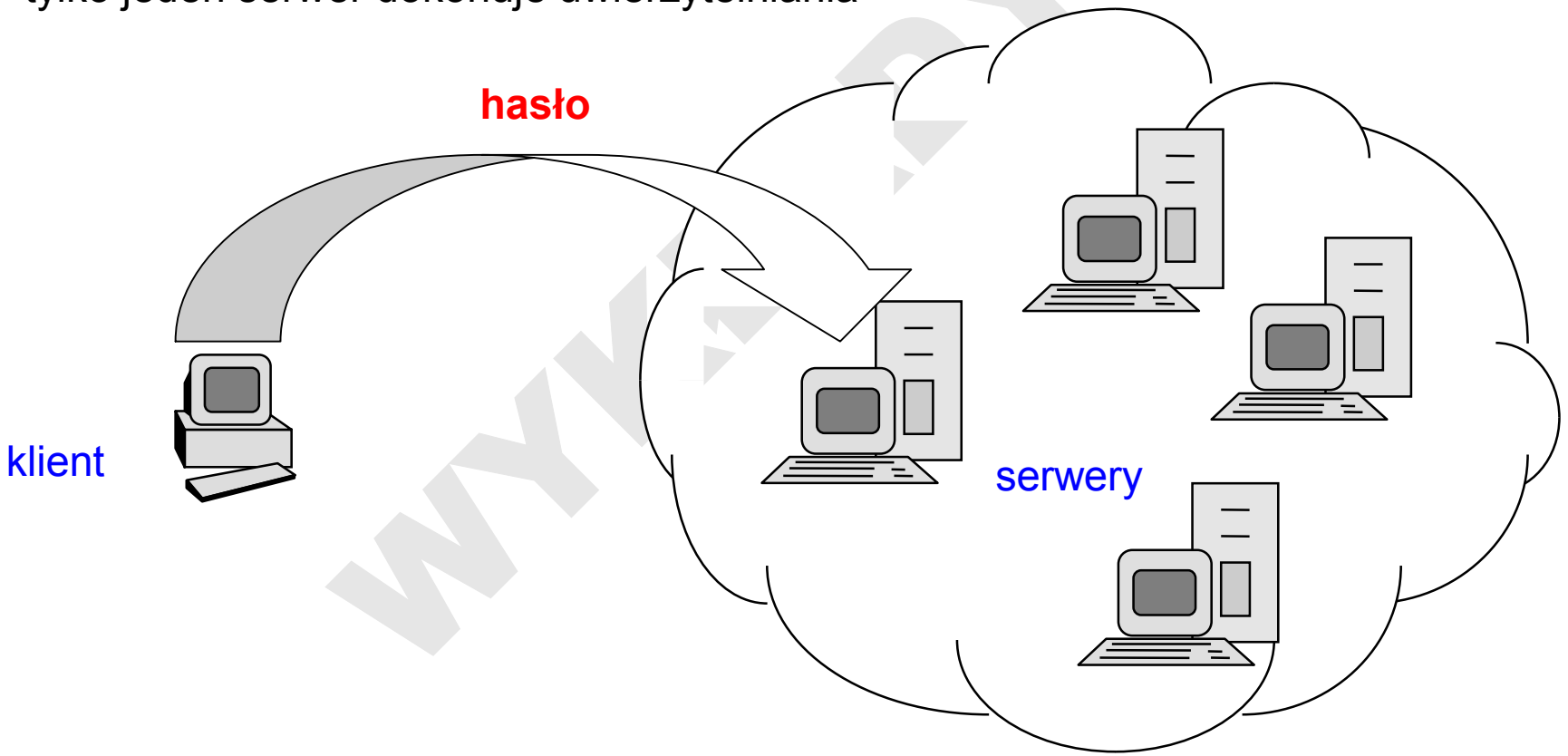
- użytkownik uruchamia klienta usługi i nawiązuje połączenie z serwerem
- serwer kontaktuje się z wydzielonym demonem – identd, pracującym na stacji klienta (113/tcp) w celu poświadczenia nazwy użytkownika (lub id) wykorzystującego usługę



Uwierzytelnianie

Uwierzytelnianie jednokrotne (SSO – *single sign-on*):

- tylko jeden serwer dokonuje uwierzytelniania



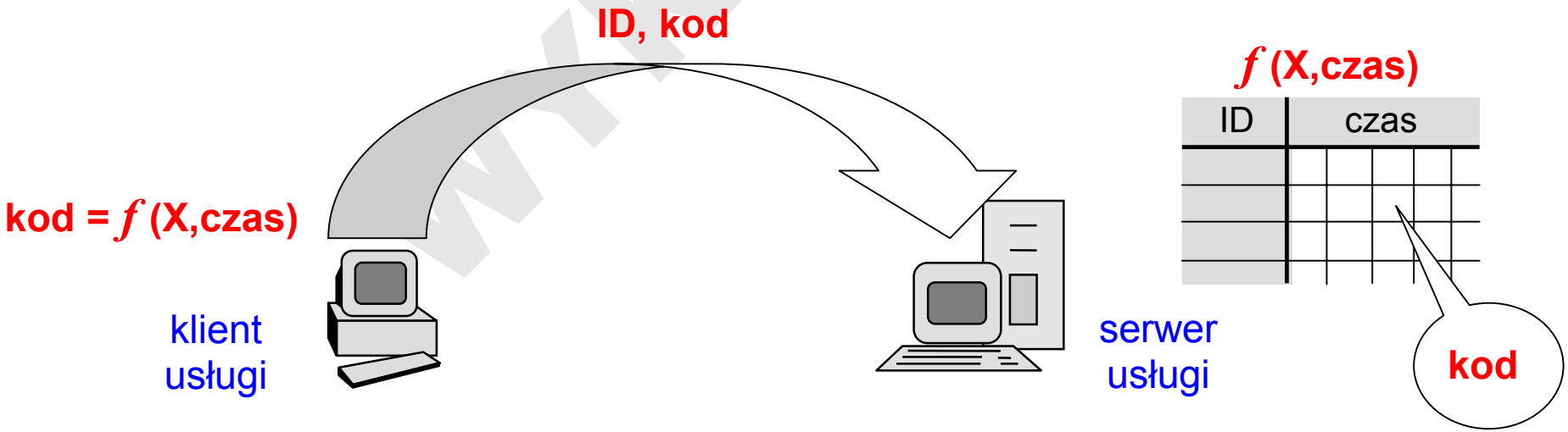
- NetWare (od 4.x), NIS, NIS+, Kerberos, MS Network

Uwierzytelnianie

Hasła jednorazowe (*one-time passwords*)

Metoda z synchronizacją czasu (*time synchronization*):

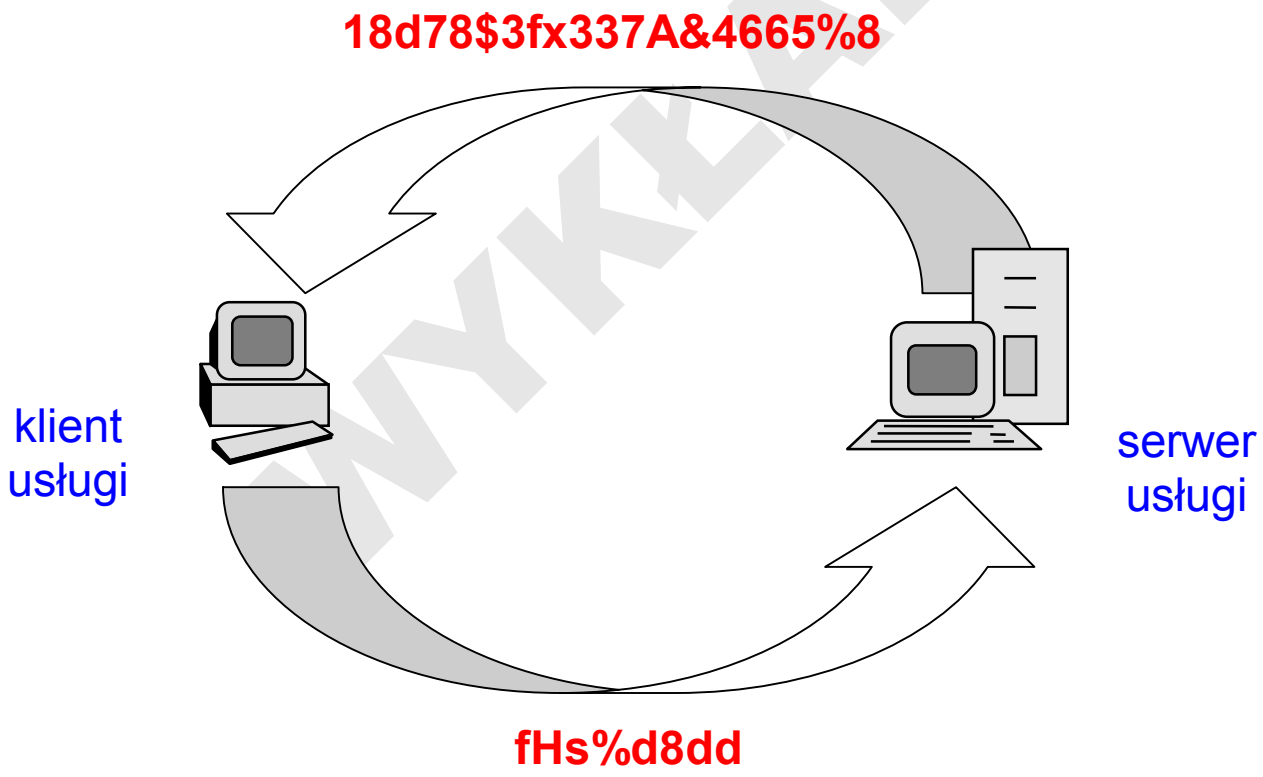
- klient generuje **unikalny kod** w funkcji pewnego parametru **X** użytkownika (identyfikatora, kodu PIN, hasła, numeru seryjnego karty identyfikacyjnej) oraz bieżącego **czasu**
- serwer weryfikuje otrzymany kod korzystając z identycznej funkcji (z odpowiednią tolerancją czasu)



Uwierzytelnianie

Metoda zawołanie-odzew (*challenge-response*):

- serwer pyta o nazwę użytkownika, a następnie przesyła unikalny ciąg („zawołanie”)
- klient koduje otrzymany ciąg swoim hasłem i odsyła jako „odzew”



Autoryzacja

Mechanizmy ochrony dostępu do danych

- weryfikacja praw dostępu legalnych użytkowników: ACL (Access Control List), ARL (Access Rights List), Trustees:

Poufność informacji

Utrudnianie podsłuchu

- topologia gwiazdy (okablowanie strukturalne)
- media transmisyjne: UTP → FTP → STP → SSTP → FO
- sztuczne generowanie ruchu (*traffic padding*)
- zamknięte grupy użytkowników (VLAN ACL, Wire-rate ACL, ...)
- kontrola dostępu do zasobów infrastruktury sieciowej (IEEE 802.1x)
- szyfrowanie

Ograniczanie emisji elektromagnetycznej

- atak przez przechwycenie promieniowania jest nadal tańszy od innego typu ataków (np. ataku kryptoanalitycznego)
- ... mimo że wymaga bardzo specjalistycznego sprzętu
- ekranujące materiały konstrukcyjne:
  - obudowy
- ekranujące materiały elastyczne:
  - tapety
  - wykładziny
- standard TEMPEST
  - stanowiska komputerowe zgodne z TEMPEST to wydatek rzędu kilku-kilkunastu tysięcy USD

Poufność informacji

Zagrożenia (c.d.):

Uwaga: przypadkowy dostęp do pozostawionej aplikacji !

Poufność informacji

Zagrożenia (c.d.):

Uwaga: Socjotechnika !

– Musimy uruchomić system.

Strażnik odchrząknął i rzucił tęsknym wzrokiem na swoją książkę.
– Uruchamianie systemu nie należy do moich obowiązków. Przyjdźcie jutro.

– Jeżeli nie uruchomimy teraz systemu, zrobi się gorąco. Przegrzeje się. *Muy caliente* i dużo pieniędzy.

Okrągła i pulchna twarz strażnika zmarszczyła się ze strachu, ale poruszył tylko ramionami.

– Ja tego nie potrafię zrobić, co miałbym zrobić?

– Wiem, że masz klucze. Wpuść nas, my to zrobimy.

Strażnik mrugnął urażony.
– Tego nie zrobię. – oświadczył – To jest zabronione.

– Czy widziałeś kiedyś rozbity komputer? – nalegał – To wygląda strasznie. Pełno go na całej podłodze!

Herbata z Czarnym Smokiem
R.A. MacAvoy

Poufność informacji

Zagrożenia (c.d.):

Uwaga: Socjotechnika !

„Mówi Ken Thompson. Ktoś dzwonił do mnie w sprawie problemu z poleceniem *ls*. Ta osoba chciała, żebym się tym zajął.”

„Taaak? Dobrze. Co mam zrobić?”

„Wystarczy zmienić hasło mojego logowania w twoim komputerze — nie używałem go od jakiegoś czasu.”

„Dobrze, nie ma problemu.”

```
From: smb@research.att.cotn
To: admin@research.att.com
Subject: Gość

W przyszłym tygodniu będziemy mieli gościa. Mógłbyś poprosić
administratora systemu o założenie dla niego konta w systemie?
Podaję Ci wiersz hasła, użyj tego samego zaszyfrowanego hasła.
pxf: 5bHD/k5k2mTTs:2403:147:Pat:/home/pat:/bin/sh
```

Nienaruszalność informacji (integralność)

Zagrożenia:

- nieuprawniona lub przypadkowa modyfikacja danych

Mechanizmy obrony:

- kontrola dostępu do danych: ACL, ARL, Trustees
- sumy kontrolne
- kryptograficzne sumy kontrolne = podpis elektroniczny
- rejestracja operacji na danych (*auditing*)
- kontrola antywirusowa

Nienaruszalność informacji (integralność)

Rejestracja operacji

- Rejestr zdarzeń systemowych
- Rejestr zdarzeń aplikacji

Dostępność informacji

Zagrożenia:

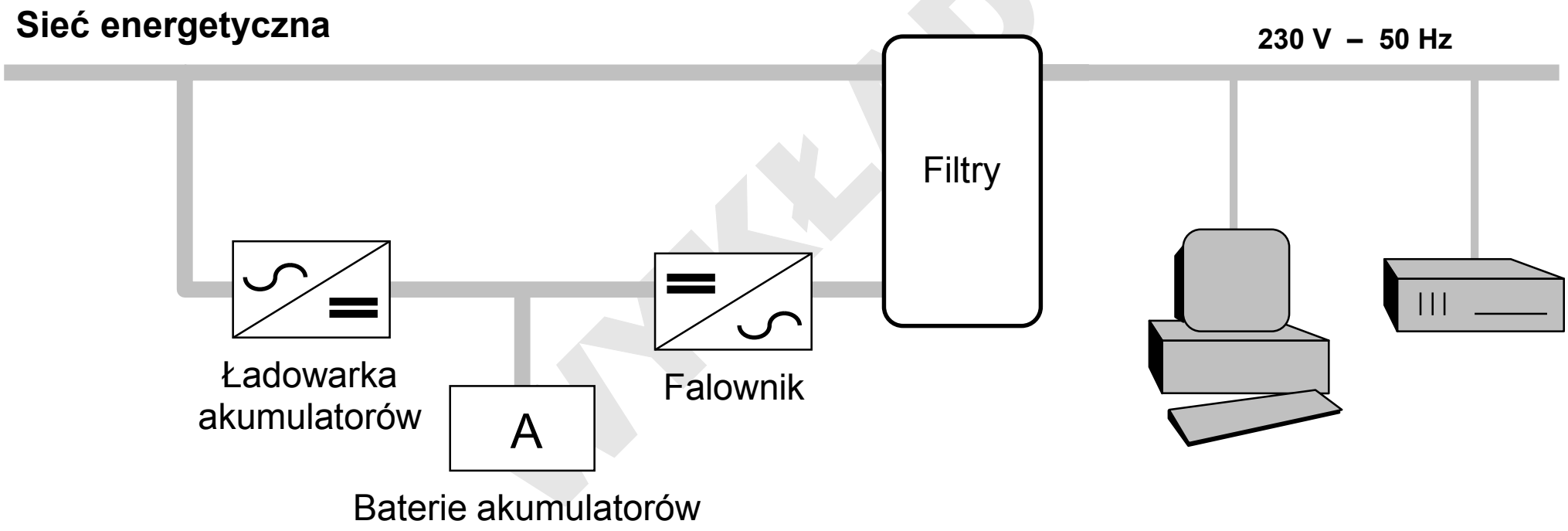
- awaria sprzętu i błędy oprogramowania, klęska żywiołu, celowy sabotaż

Mechanizmy obrony:

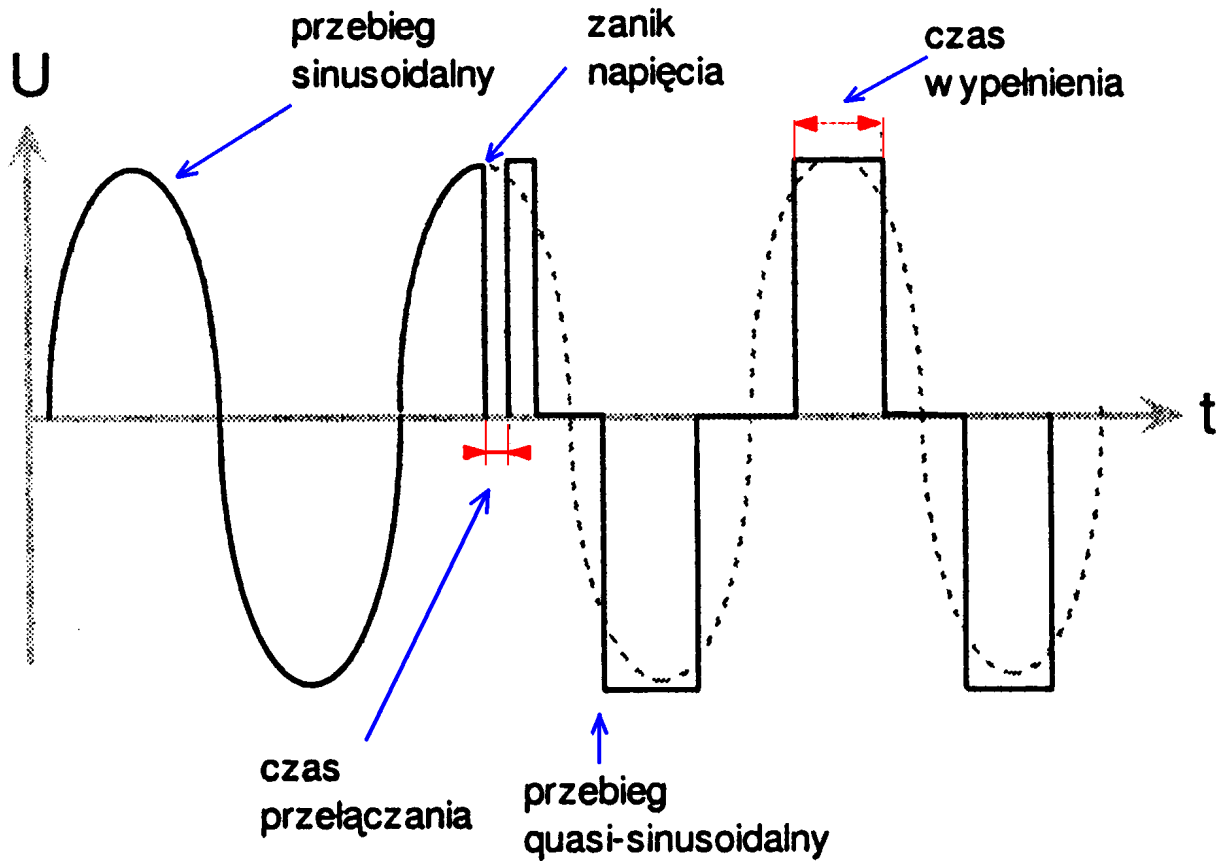
- ciągłość zasilania urządzeń sieciowych
- systemy redundantnych komponentów:
  - zasilanie awaryjne
  - macierze dyskowe RAID
- systemy redundantnych usług:
  - serwery lustrzane
  - grona serwerów (*clusters*)
- archiwizacja (*backup*) danych
- kontrola antywirusowa

Zasilacze awaryjne – UPS

off-line, standby power supply

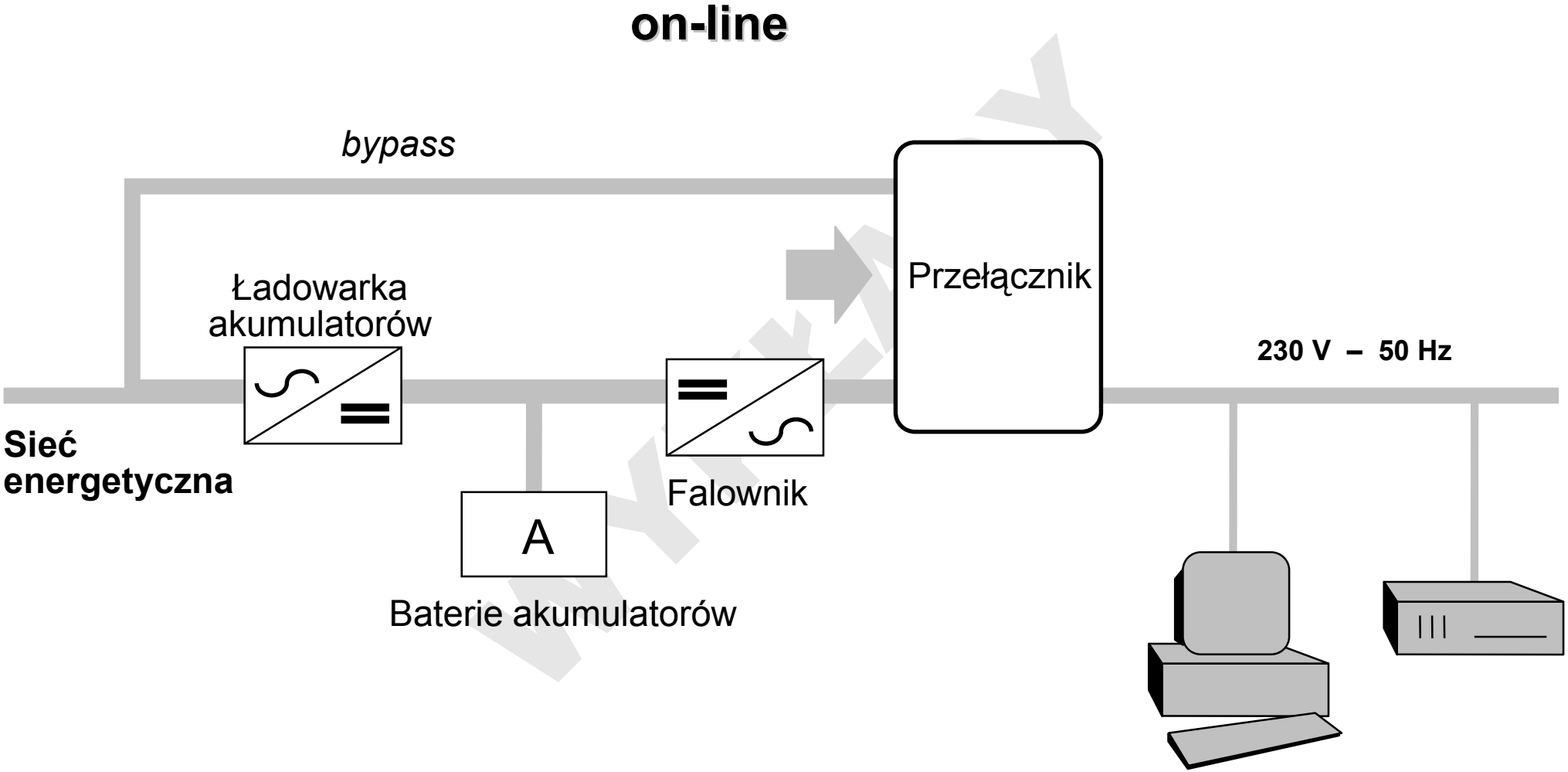


Zasilacze awaryjne – UPS



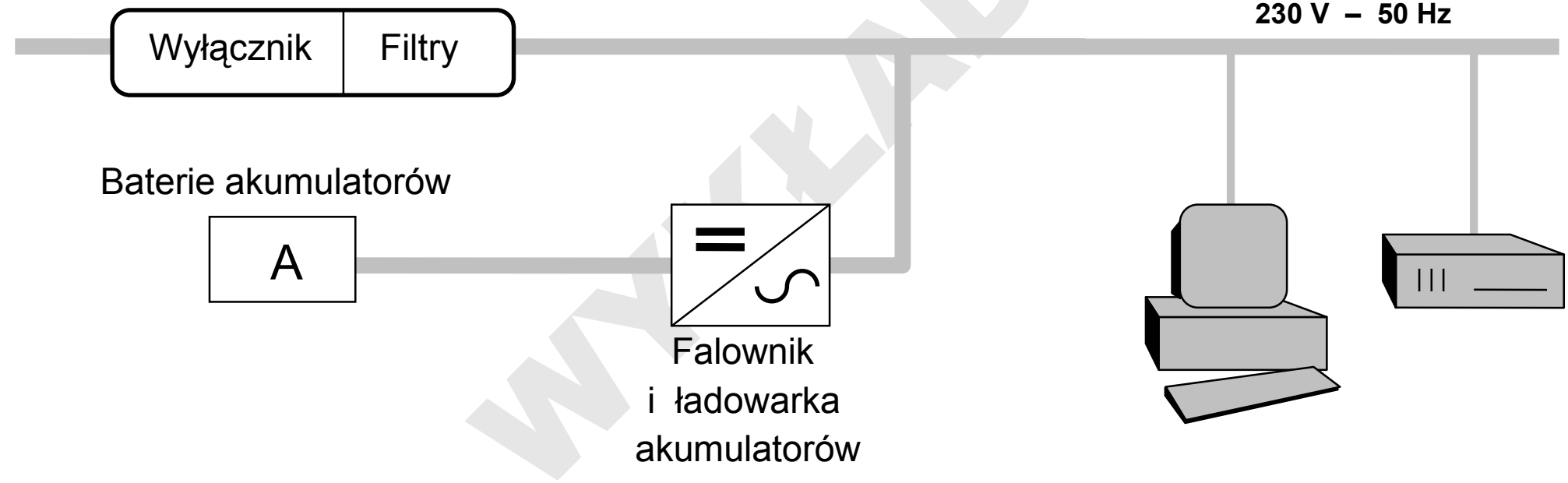
Kształt napięcia na wyjściu zasilacza awaryjnego *off-line*

Zasilacze awaryjne – UPS

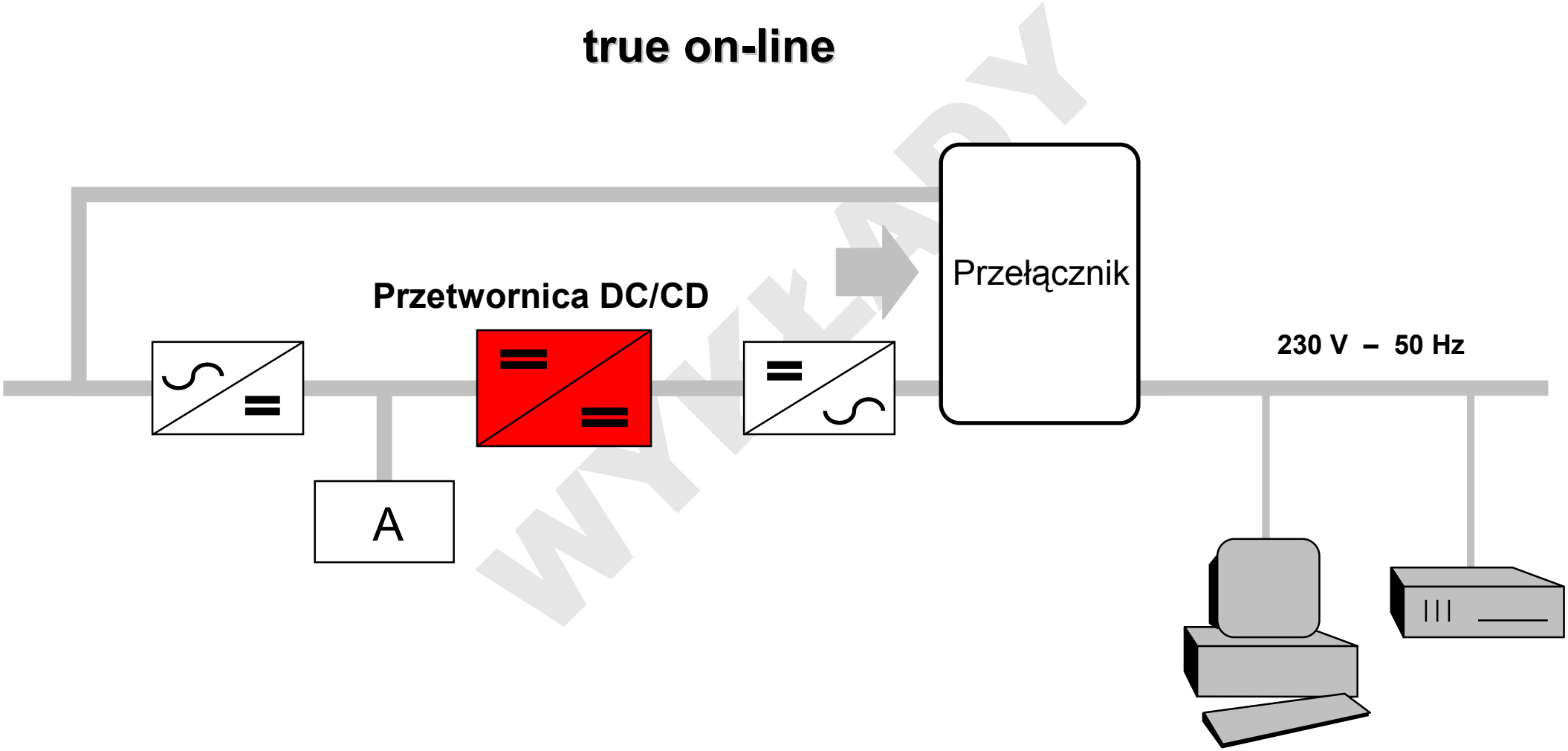


Zasilacze awaryjne – UPS

line-interactive, in-line



Zasilacze awaryjne – UPS

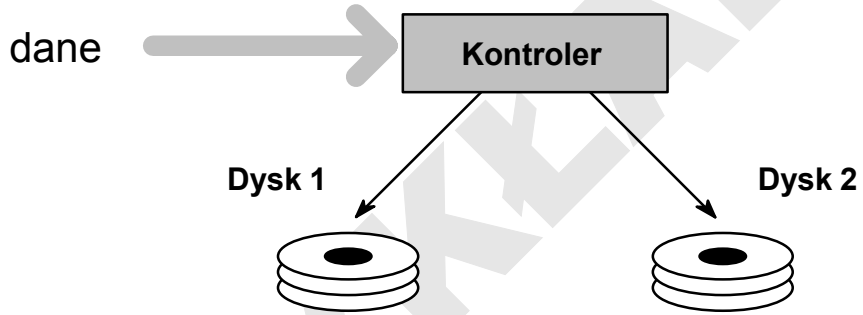


Macierze dyskowe RAID

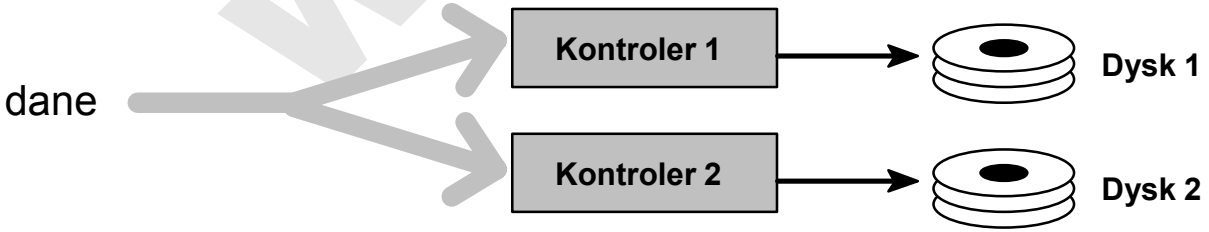
(*Redundant Array of Independent Disks*)

RAID 0 = brak redundancji (ew. *stripping*)

RAID 1 = mirroring :



duplexing :

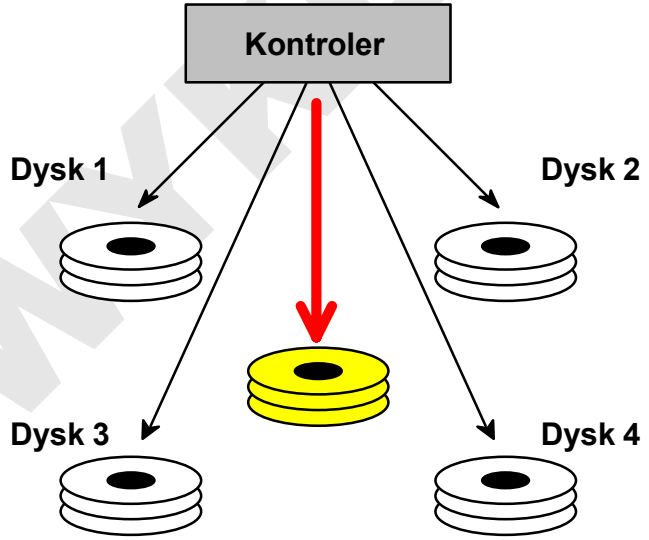


Macierze dyskowe RAID

RAID 2 = stripping

- równomierny podział bloków (na poziomie pojedynczych bitów) na wszystkie dyski
- opcjonalnie zapis sum kontrolnych ECC (kod Hamminga) w wydzielonym obszarze

RAID 3 = stripping + wydzielony dysk parzystości (zawierający ECC)



Macierze dyskowe RAID

RAID 4 = RAID 3 bez wzajemnej synchronizacji dysków
(w celu przyspieszenia operacji na dysku)

- podział bloków na poziomie pojedynczych sektorów
- wydzielony dysk kontrolny przechowuje różnice symetryczne sektorów

RAID 5 = stripping z rozproszoną parzystością

- kody korekcyjne zapisywane na każdym dysku macierzy jednocześnie
- wymiana i odtworzenie zawartości uszkodzonego dysku bez zatrzymywania systemu

RAID 6 = kodowanie Reeda-Solomona

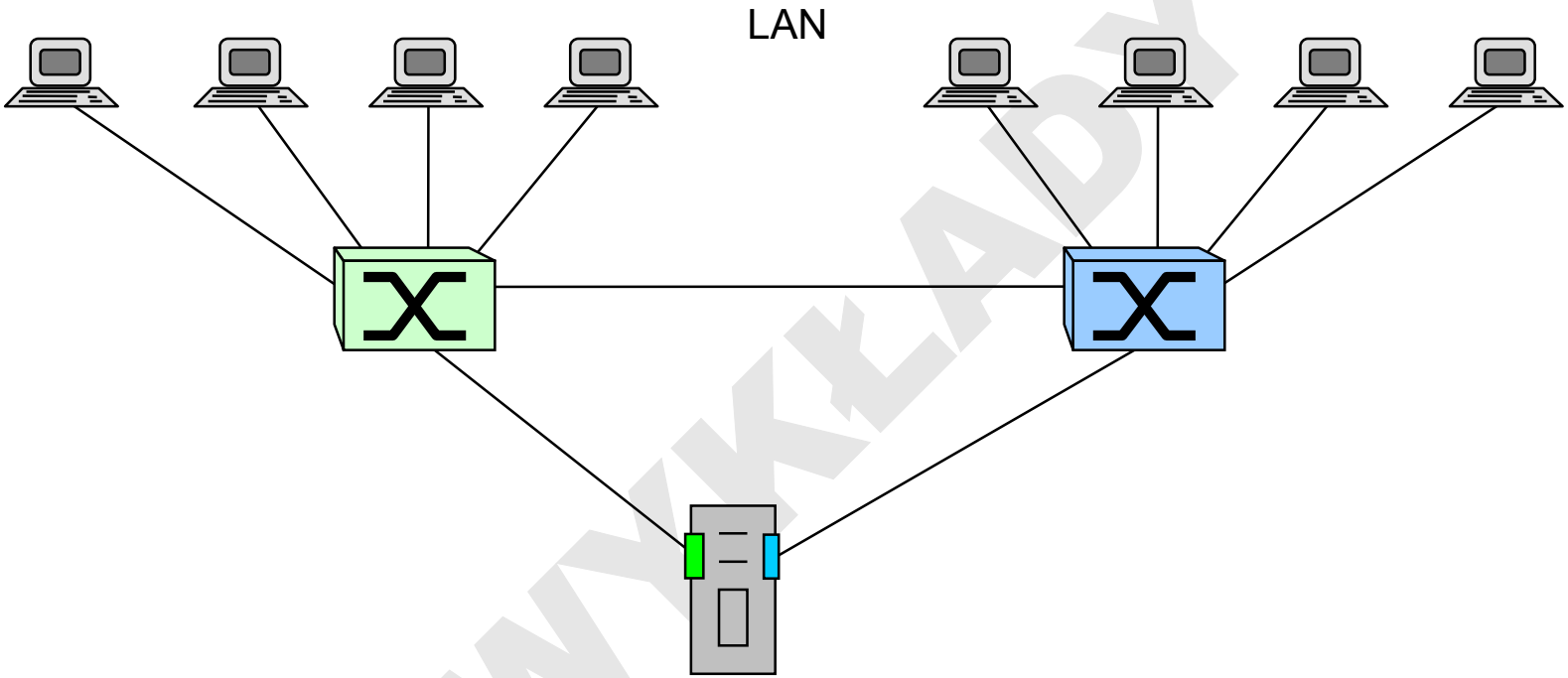
- odporność na awarie do 2 dysków jednocześnie

Redundancja interfejsu sieciowego

1. **Podwójne porty na karcie:**
   - bieżąco aktywny jeden port, drugi – rezerwowy
   - przykłady producentów: Adaptec, 3Com, Znyx
2. **Podwójne karty sieciowe:**
   - wspólny adres
   - przykład producenta: Intel

Redundancja połączeń

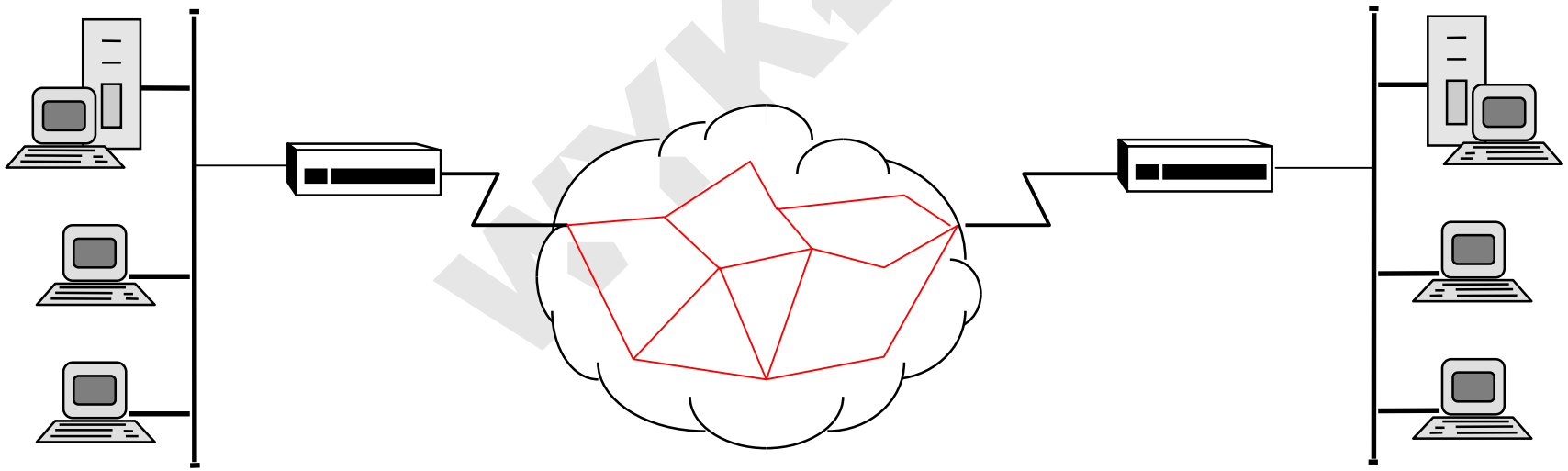
Olicom Clear Server – serwer dołączony do sieci lokalnej poprzez dwa interfejsy



jeden adres MAC – dwie karty sieciowe (np. RapidFire) – *load balancing*

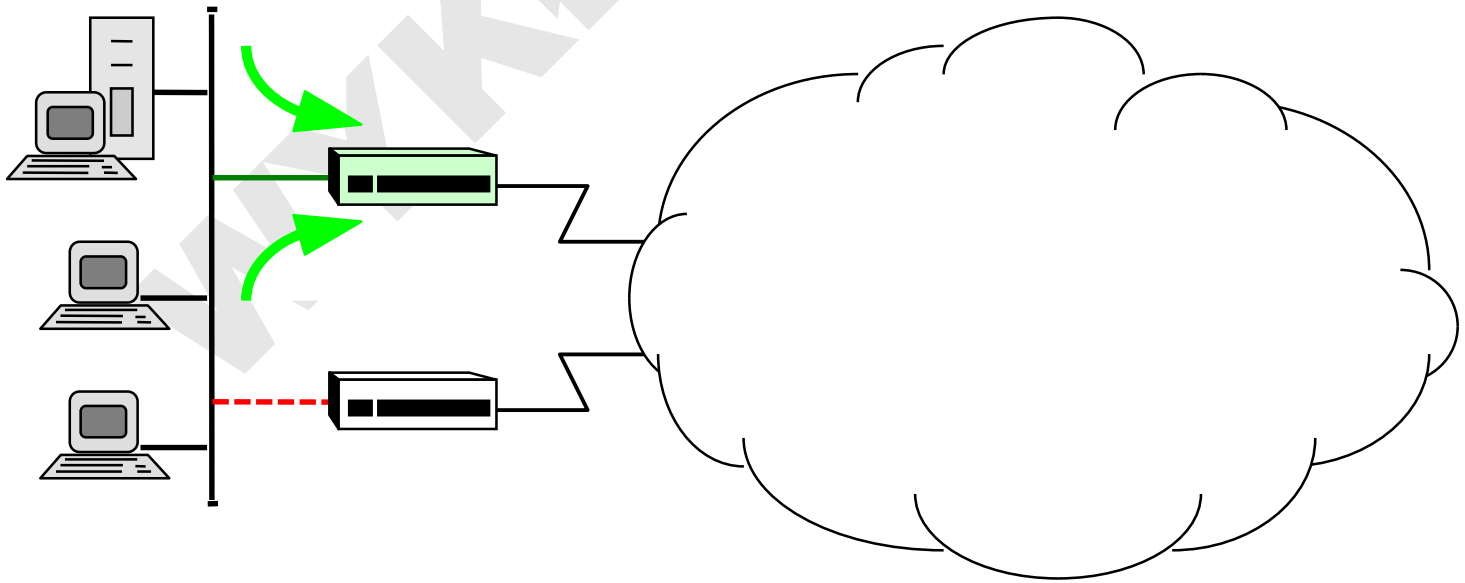
Redundancja łączy w sieci rozległej

- sieć prywatna, łącza prywatne lub dzierżawione – sami dbamy o nadmiarowość – dynamiczny routing (RIP, OSPF, EIGRP, BGP, IS-IS)
- sieć publiczna – istnieje już pewna nadmiarowość łączy operatora sieci, można wykorzystać kilku operatorów



Redundancja routerów

- **RDP** (Router Discovery Protocol) – routery mają różne IP i stacje sieciowe wybierają spośród nich jeden aktywny (zaangażowany software stacji sieciowych, wymagany ICMP)
- **HSRP** (Hot Standby Routing Protocol, RFC 2281), **VRRP** (Virtual Router Redundancy Protocol, RFC 2338), **GLBP** (Gateway Load Balancing Protocol, Cisco) – routery mają ten sam IP i dynamicznie wybierają spośród siebie jeden aktywny transparentnie dla stacji sieciowych



Redundancja routerów

HSRP / VRRP / GLPB

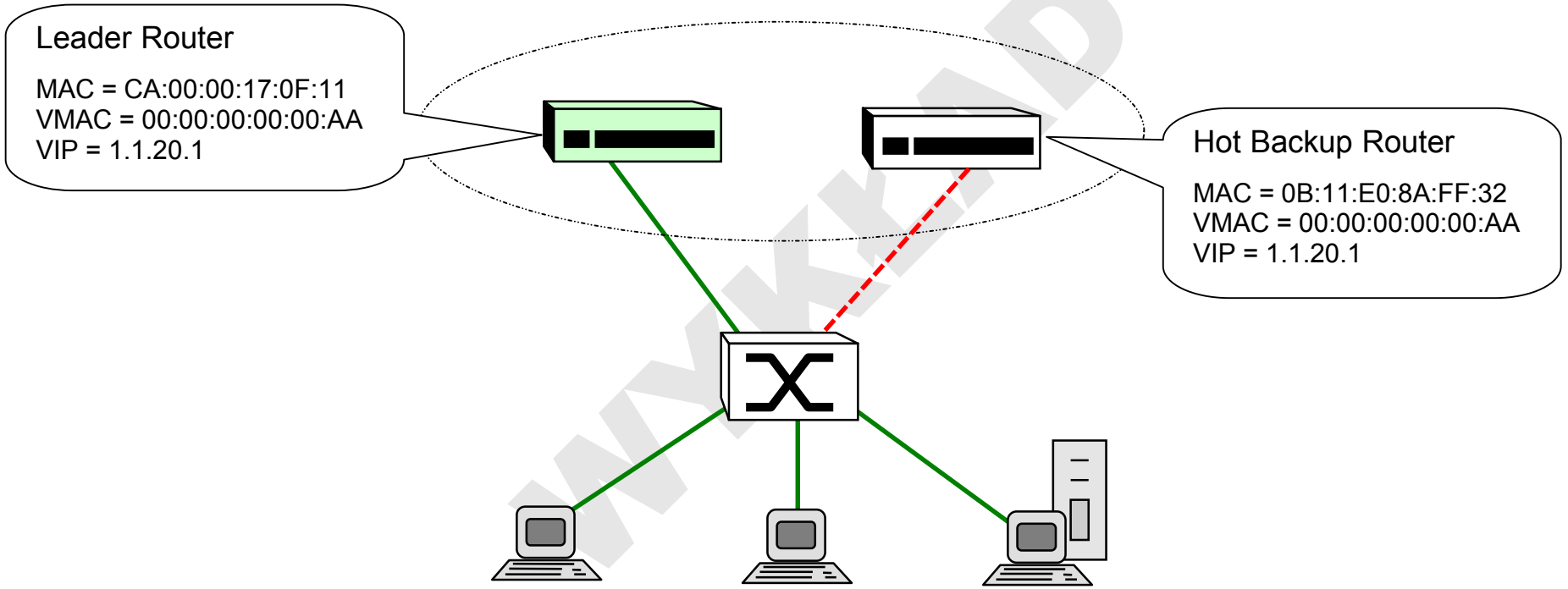
- HSR Group ("Phantom Router") – grupa routerów o wspólnym adresie IP (VIP) i MAC (VMAC)
- Leader Router – aktualnie obsługujący pakiety
- Hot Backup Routers – monitorują lidera
- awaria lidera – STP (Spanning Tree Protocol) wybiera nowego

Trasy równoległe (GLPB)

- połączenia redundantne nie stanowią tylko zabezpieczenia, lecz są wykorzystywane na bieżąco (równoważenie obciążenia tras – *load balancing*)

Redundancja routerów

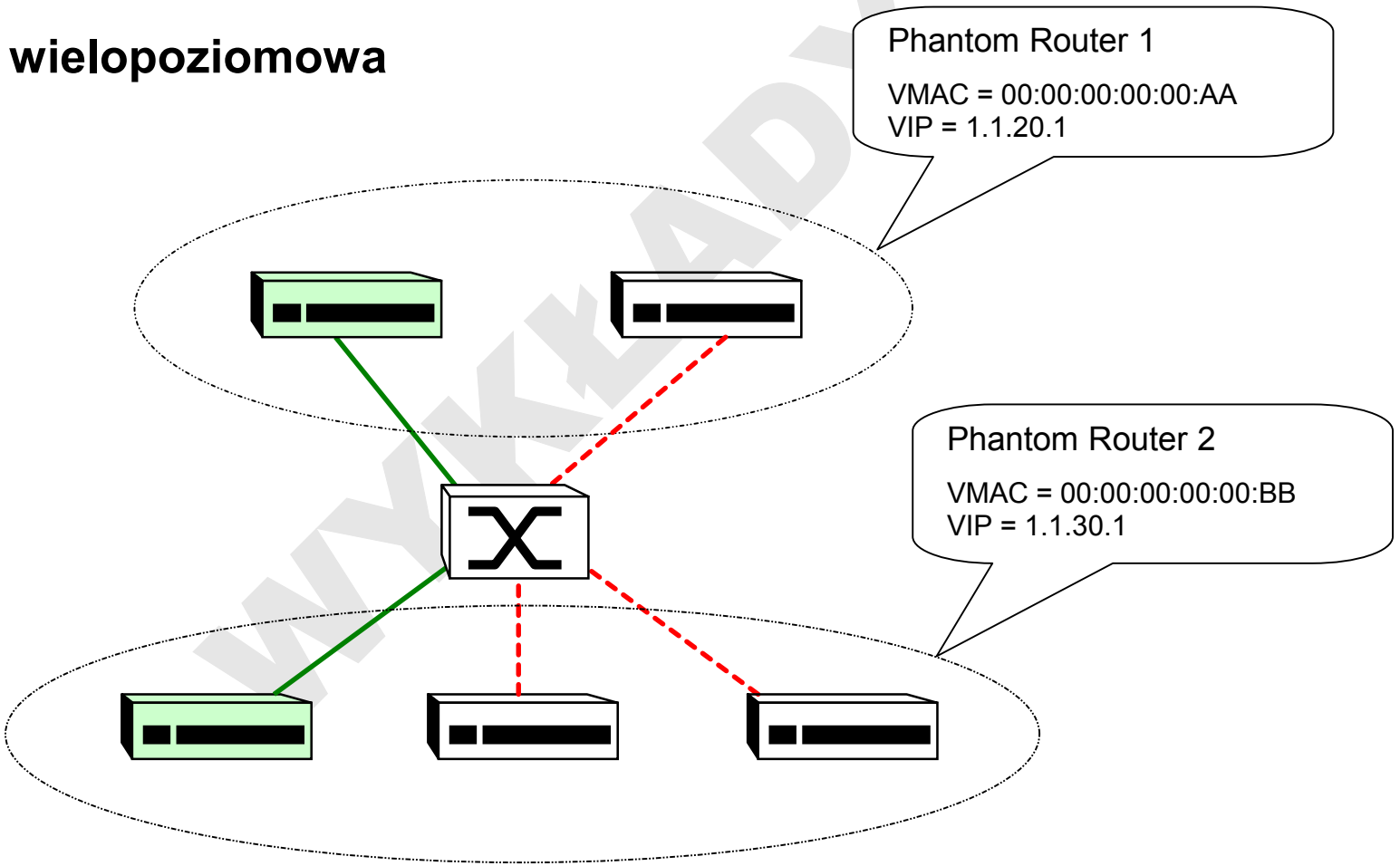
HSRP / VRRP / GLPB



Redundancja routerów

HSRP / VRRP / GLPB

Konfiguracja wielopoziomowa



Redundancja serwerów

Serwery wieloprocesorowe

- architektura równoległa: wiele procesorów – jedna wspólna pamięć (globalna)
- masywna równoległość – duża liczba procesorów
- NUMA: wiele procesorów, każdy z lokalną pamięcią
- przetwarzanie aplikacji równoległych

Serwery lustrzane

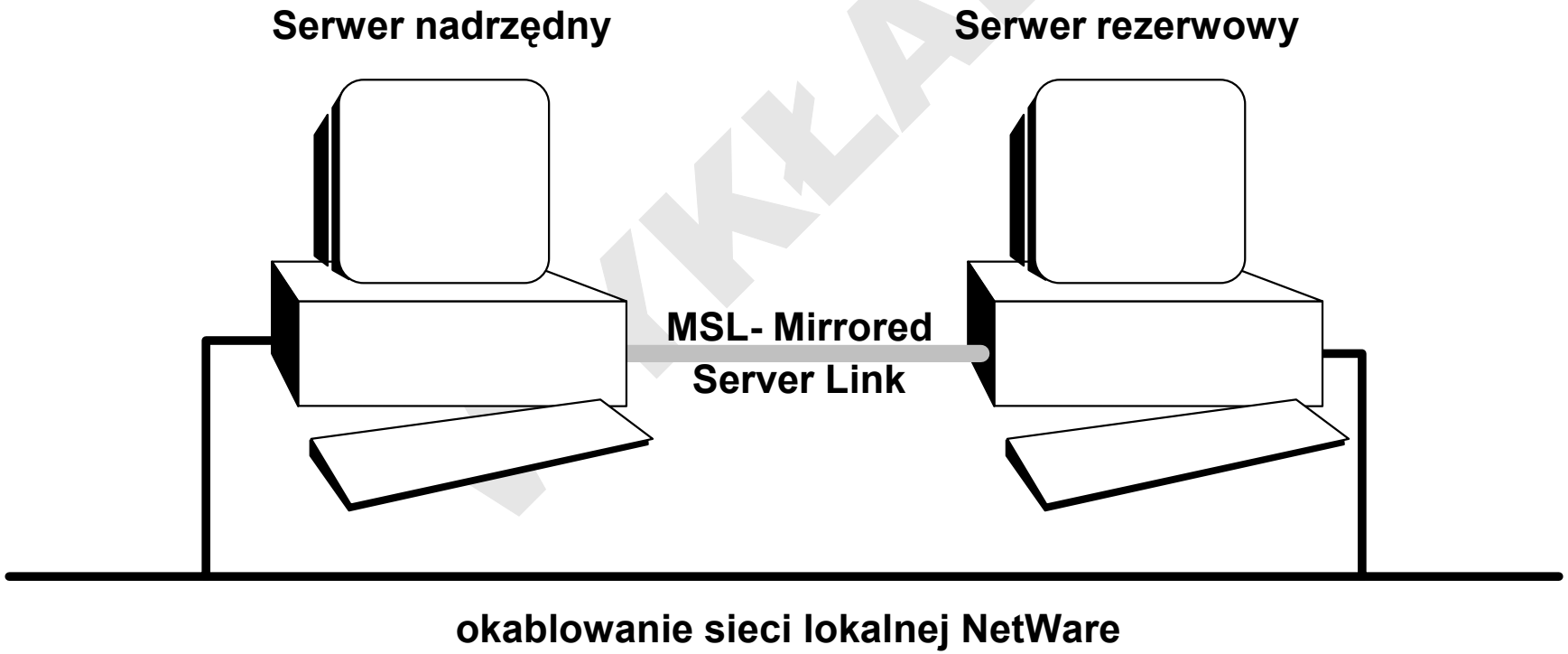
- serwer podstawowy + kopia lustrzana
- po awarii serwera podstawowego jego funkcje przejmuje kopia lustrzana (*fail-over*)

System Fault Tolerance
(Novell)

SFT I = kontrolny odczyt po zapisie + Hot Fix

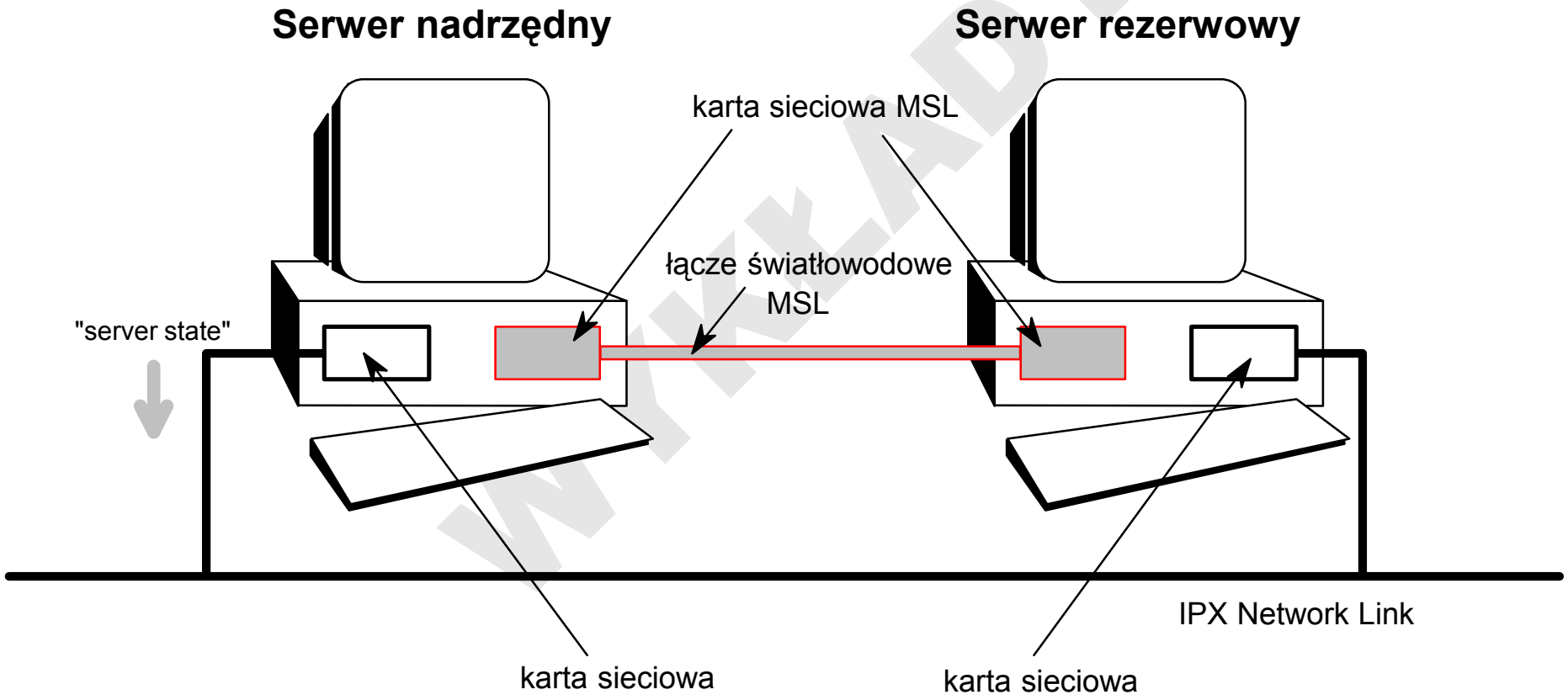
SFT II = mirroring / duplexing (RAID 1) + TTS

SFT III = replikowany serwer:



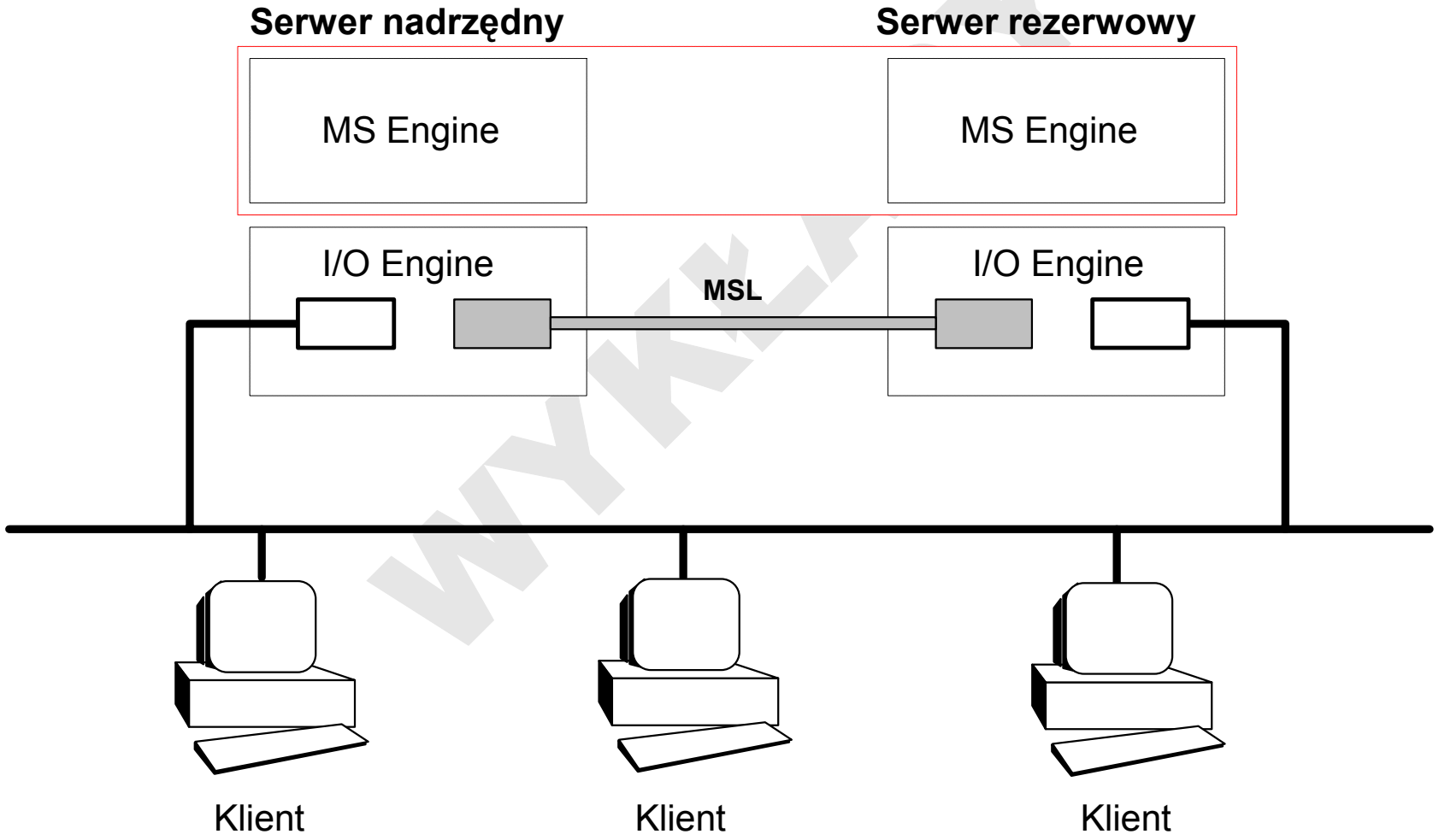
System Fault Tolerance

Architektura systemu SFT III

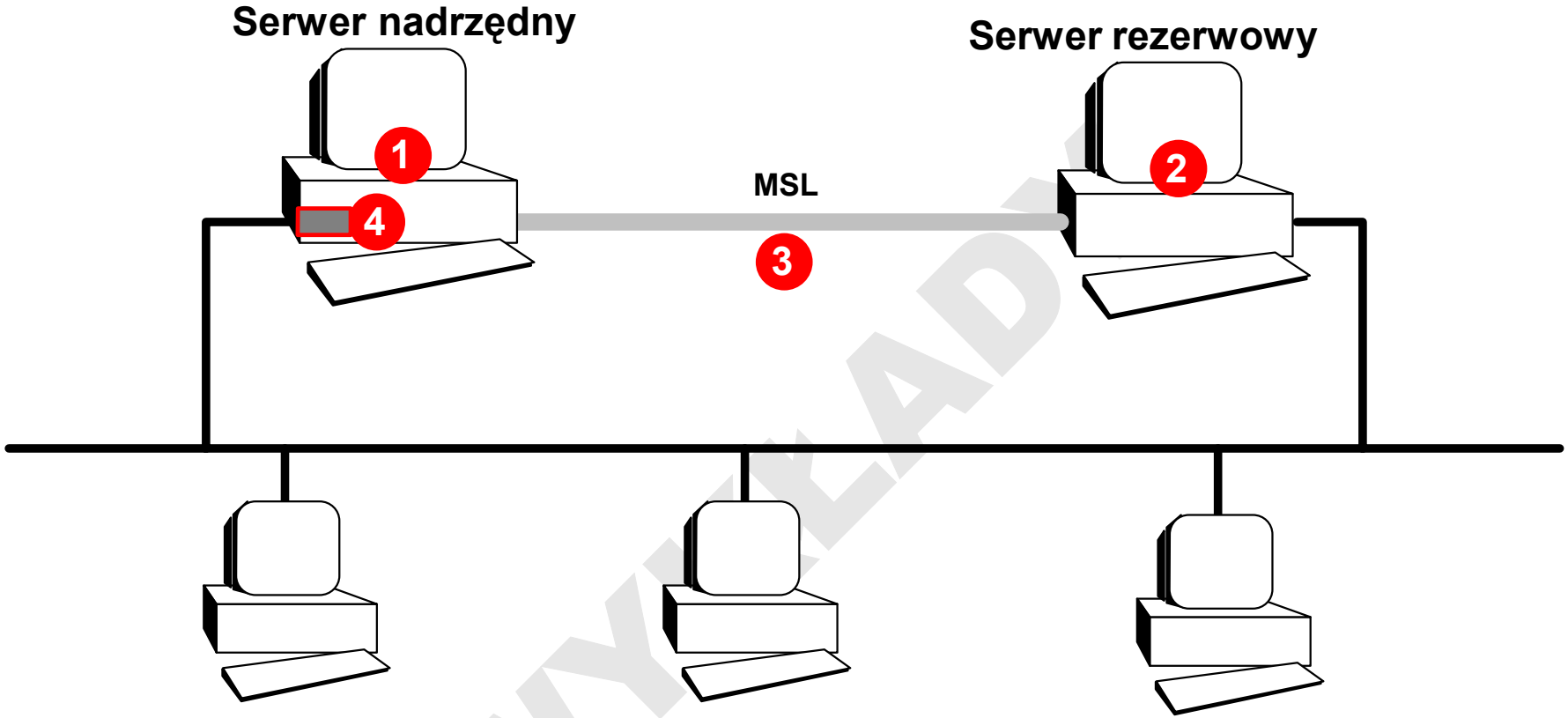


System Fault Tolerance

identyczne: pamięć operacyjna, pamięć dyskowa, karta graficzna



System Fault Tolerance



AWARIA:

1 - hardware serwera nadrzędnego

2 - hardware serwera rezerwowego

3 - łącze MSL

4 - karta sieciowa serwera nadrzędnego

Redundancja serwerów

Novell High Availability Server (NHAS)

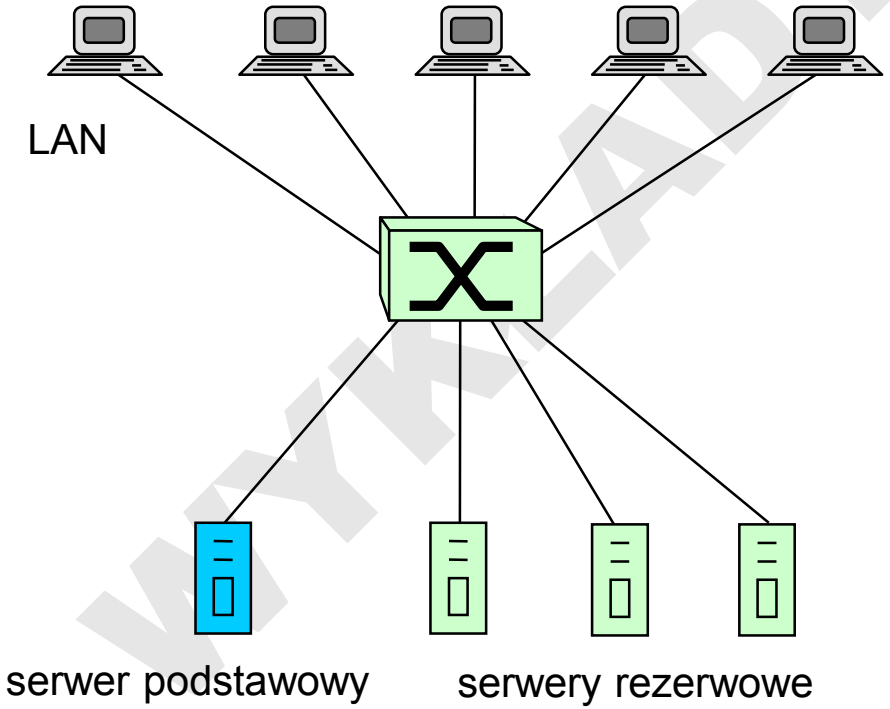
- odmiana serwera typu grono (*cluster*) w trybie *fail-over* (Orion Phase I)
- rozszerzenie SFT III dla NetWare $\geqslant$ 4.11
  - współdzielenie zasobów dyskowych

Novell Cluster Services (NCS)

- rozwinięcie w pełne grono dla NetWare 5 / 6
  - do 32 serwerów
  - połączonych przez Fibre Channel
  - z równoważeniem obciążenia
- czas przełączania zadań po awarii jednego z serwerów 15-30 s
- w NetWare 6 wsparcie dla serwerów SMP do 32 procesorów

Redundancja serwerów w sieci ATM

- *Primary-backup* – powielone przyłączenia serwerów do sieci lokalnej



każdy serwer ma ten sam adres IP

- SSRP = Simple Server Redundancy Protocol – dot. serwerów LES (LANE Server)

Grona

Grona niezależnych węzłów (*clusters*)

- system rozproszony w wąskim zakresie
  (rozproszony system operacyjny, specyficzne łącza)
- podniesienie stopnia niezawodności przetwarzania (dostępności danych)
  – po awarii jednego węzła jego funkcje przejmuje inny (*fail-over*)
- integralną funkcją systemu jest równoważenie obciążenia (*load balancing*)
- przetwarzania aplikacji rozproszonych dostosowanych do środowiska grona
- problemy w niekompatybilności architektur gron utrudniają przenośność aplikacji
- propozycja standaryzacji – specyfikacja VIA (Virtual Interface Architecture)

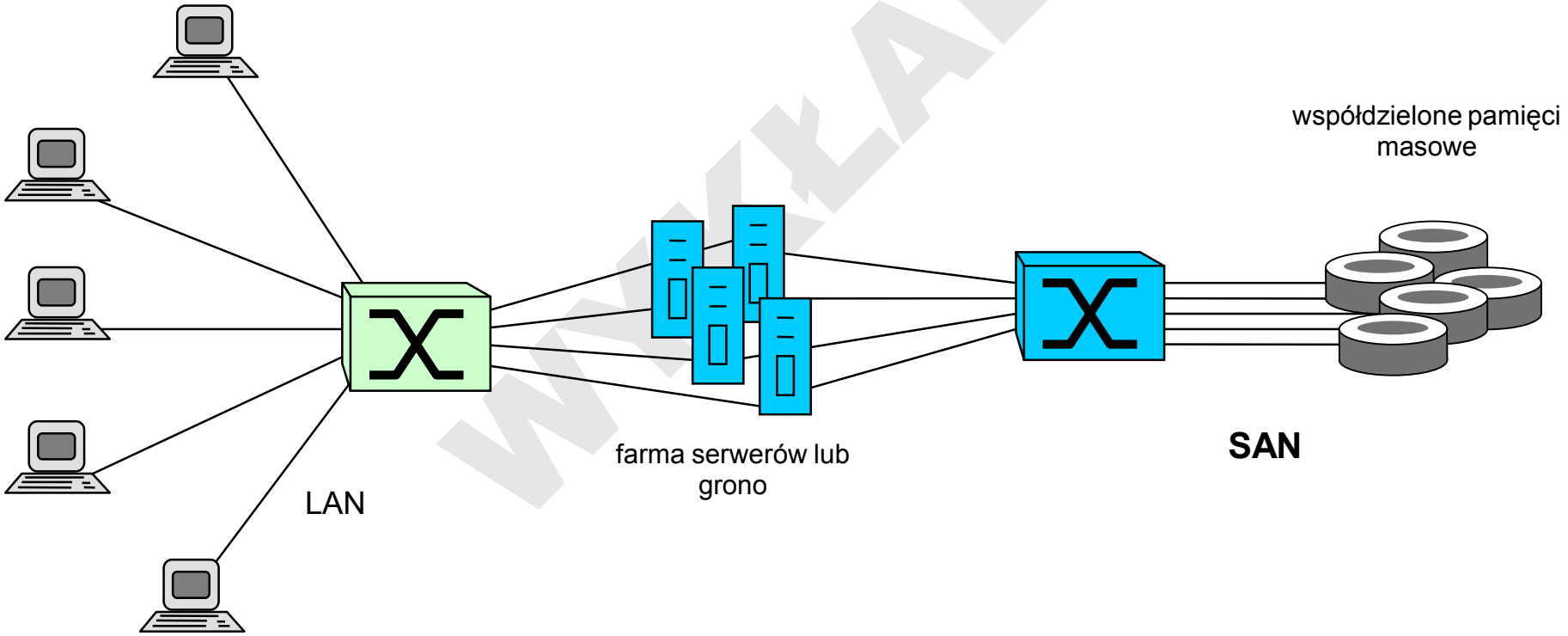
Grona

Przykłady:

- NonStop Clusters – dla SCO UnixWare 7
- FullMoon – dla SUN Solaris 8
  - do 8 węzłów
  - cluster file system
  - pojedynczy obraz systemu operacyjnego
- MS Cluster Server – począwszy od Windows NT Server Enterprise Edition
  - 2 węzły
- Compaq ProLiant Cluster HA/F500 + MS Cluster Server
  - macierz dyskowa StorageWorks dołączona do obu serwerów poprzez Fibre Channel
  - możliwa redundancja koncentratorów Fibre Channel i macierzy
- Dell PowerEdge 6300 Cluster (16 Win2000 + IBM DB2) – zgodny z VIA

Storage Area Network (SAN)

- separacja zasobów dyskowych
- zasoby dyskowe są współdzielone na równych prawach przez wszystkie serwery (NFS = Network File System, CIFS = Common Internet File System)

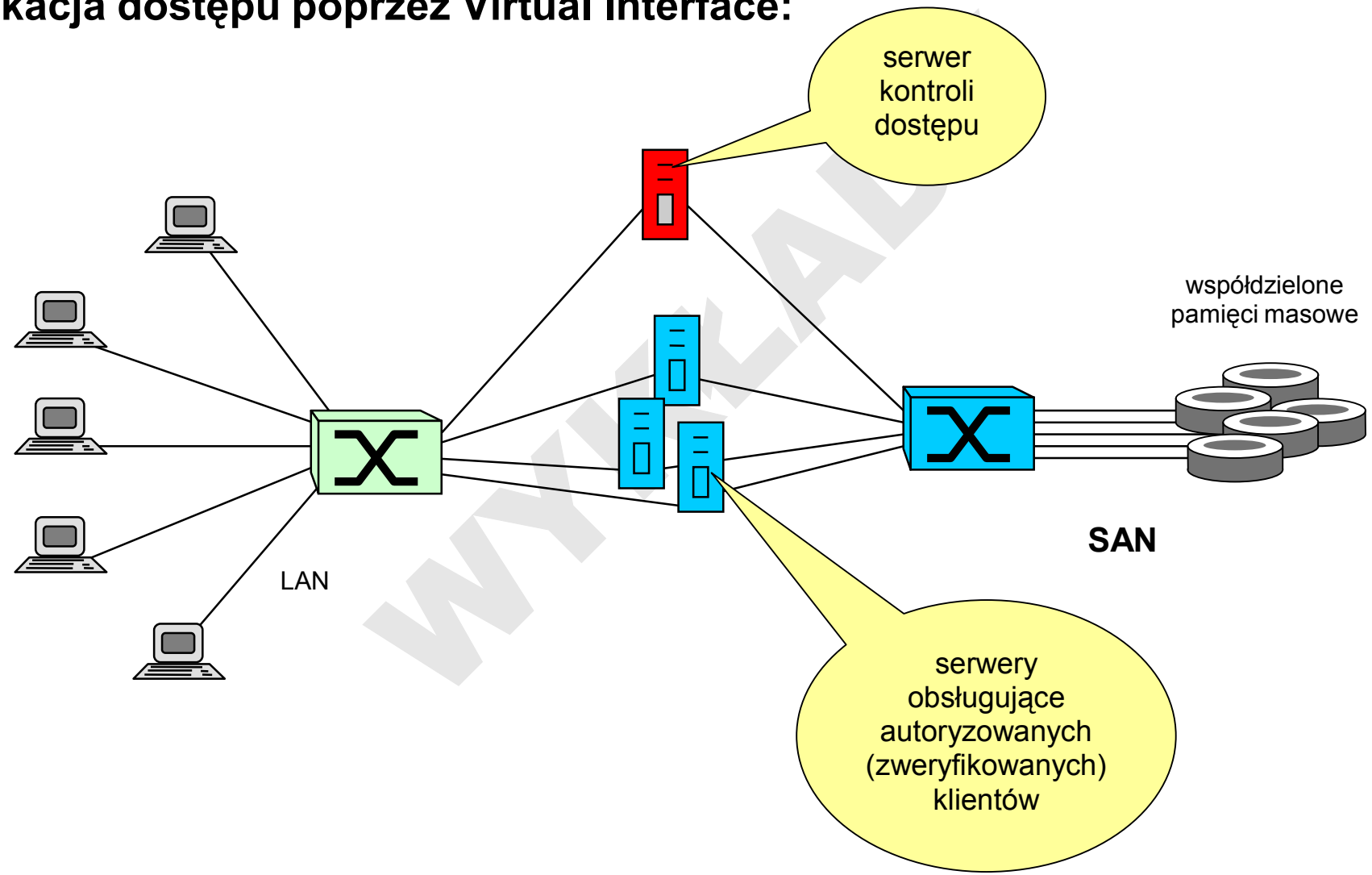


Storage Area Network (SAN)

- łatwiejsze zarządzanie
- awarie poszczególnych serwerów bez wpływu na dostępność dysków
- wskazana dedykowana sieć SAN
- problem kontroli dostępu i bezpieczeństwa przesyłanych informacji

Virtual Interface Architecture (VIA)

Weryfikacja dostępu poprzez Virtual Interface:



Archiwizacja danych i kopie zapasowe (backup)

Podstawowe modele archiwizacji:

- **bezpośrednio z serwera (*server-based backup*)**
  - bezpośrednio do serwera sieciowego dołączone są dodatkowe urządzenia archiwizujące (napędy pamięci masowej) i software
  - zapewniona spójna ochrona archiwizowanych danych
  - duża szybkość procesu archiwizacji
  - obciążenie serwera
  - błędy systemu archiwizacji mogą zawiesić podatny system operacyjny serwera (szczególnie NT)

Archiwizacja danych i kopie zapasowe (backup)

- **dedykowany serwer archiwizacji (*backup-server*)**
  - bezpieczne, ale drogie
- **ze stacji sieciowej (*workstation-based backup*)**
  - dodatkowe urządzenia archiwizujące dołączone są do stacji sieciowej i na niej pracuje program archiwizujący
  - możliwość archiwizowania danych z kilku serwerów, również zdalnych (a nawet innych stacji sieciowych)
  - konieczność zapewnienia stacji archiwizującej odpowiednich przywilejów
  - mniejsza szybkość procesu archiwizacji przy współdzielonych ruchu sieciowym (ograniczona przepustowością sieci)
  - obciążenie sieci

Archiwizacja danych i kopie zapasowe (backup)

Przykładowe nośniki archiwizacji:

Klasyczne (dostęp sekwencyjny):

- streamery Ditto
- taśmy Travan (do 10 GB)
- taśmy DAT (std. DDS-3)

niezawodność: kody ECC

- CRC-64 daje prawdopodobieństwo błędnej korekcji 1 : 18 446 744 070

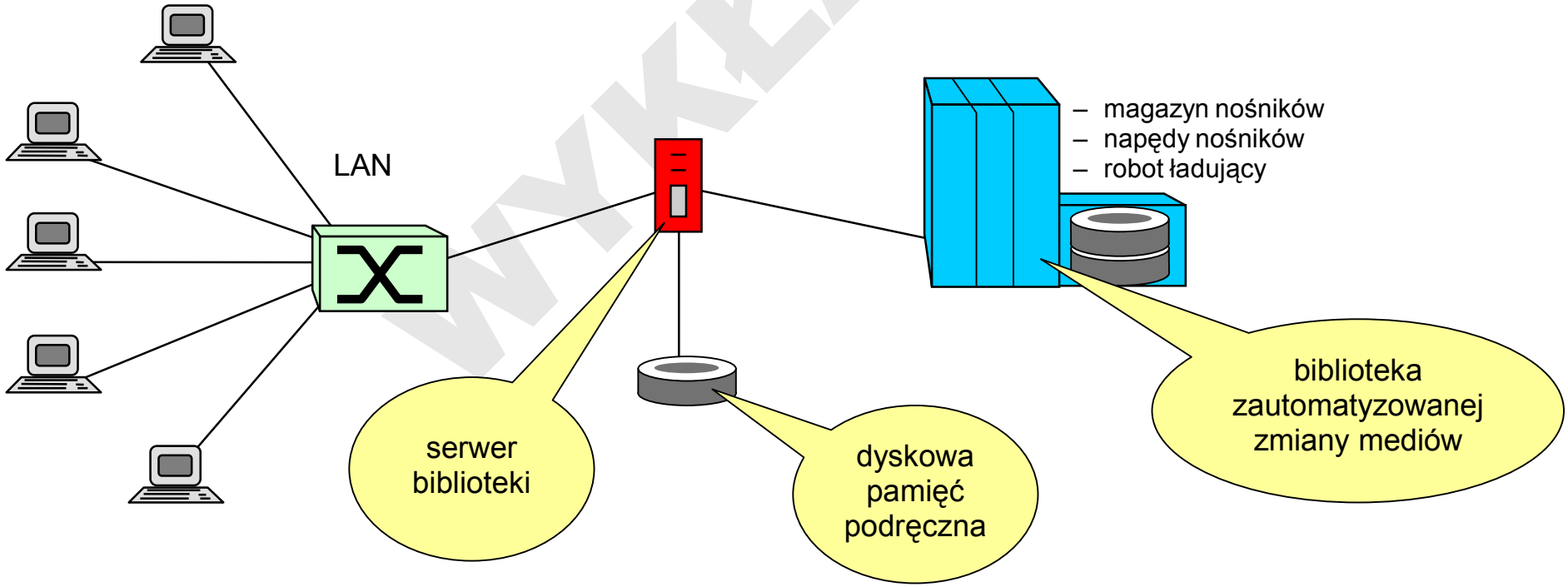
Szybkie (dostęp bezpośredni):

- dyski optyczne i magnetooptyczne
  (CD-R/RW 700MB/800MB; WORM 2.6GB; DVD 4.7GB, DVD DL 9GB)
- przenośne napędy dysków magnetycznych JAZ

Archiwizacja danych i kopie zapasowe (backup)

Hierarchiczne systemy archiwizacji (HSM – *Hierarchical Storage Management*):

- wybór klasy nośnika w funkcji częstotliwości wykorzystania (lub ważności) danych
- pojemność zakumulowana często powyżej 10 TB i przepustowość ponad 200 GB/h



Archiwizacja danych i kopie zapasowe (backup)

Najczęstsze błędy w procesie archiwizacji:

- brak weryfikacji poprawności sporządzanych kopii archiwalnych / zapasowych
- przechowywanie kopii w tym samym miejscu co archiwizowane dane (system)