

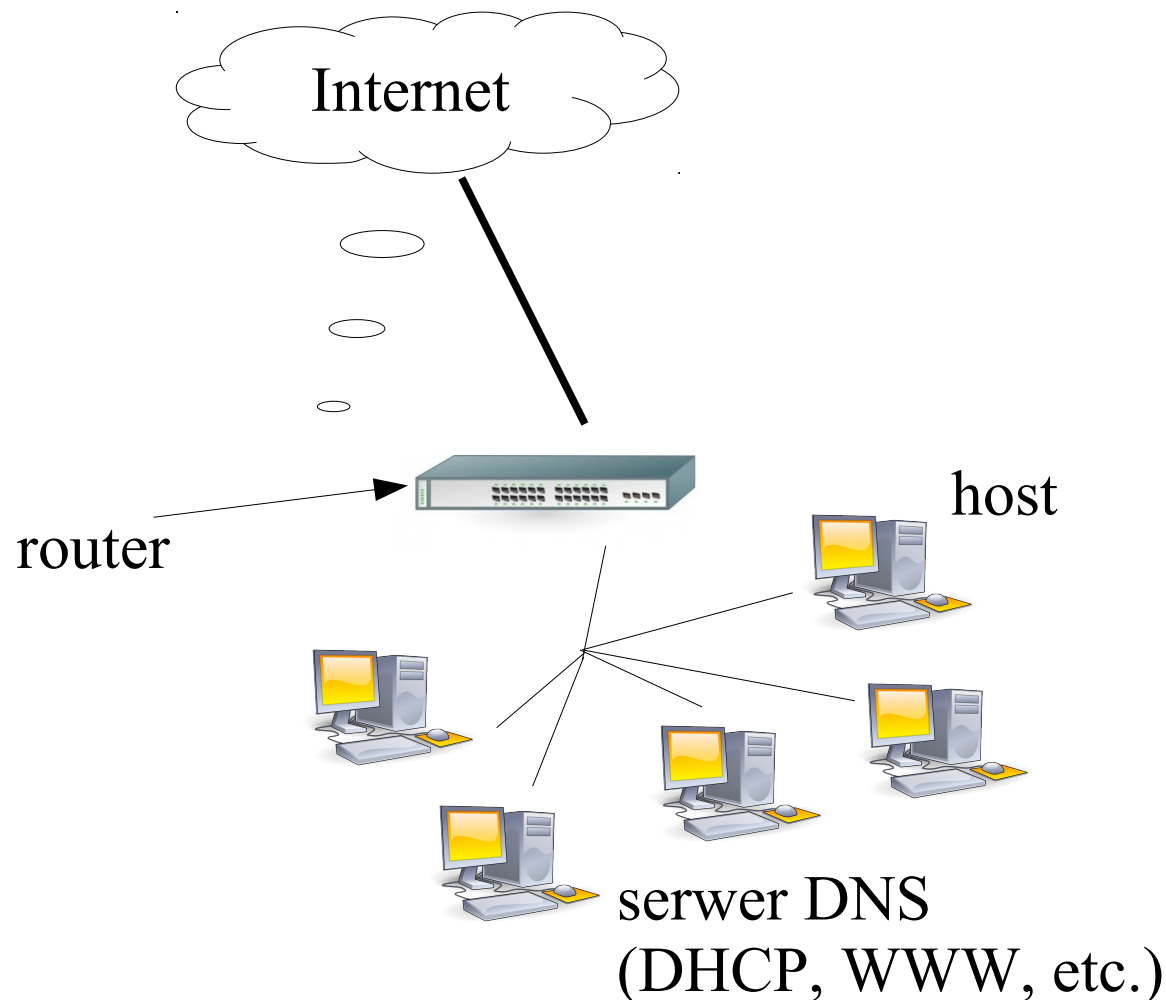


Wykład 2: Budowanie sieci lokalnych



Budowanie sieci lokalnych

- Technologie istotne z punktu widzenia konfiguracji i testowania poprawnego działania sieci lokalnej:
 - ◆ Protokół ICMP i narzędzia go wykorzystujące
 - ◆ Mapowanie adresów: DNS i ARP
- Funkcje i znaczenie routera w sieci lokalnej
- Technologia NAT
- Interfejs sieciowy i jego konfiguracja
- Automatyczna konfiguracja sieci: DHCP



- Sieć lokalna ma wspólny „adres IP sieci”
- Zwykle stanowi jeden zespół komputerów połączonych Ethernetem i/lub WiFi



- Protokół ICMP (Internet Control Message Protocol) działa w w. sieci, jest przekazywany w ramach IP
- ICMP kontroluje i modyfikuje działania urządzeń w w. sieci:
 - ◆ steruje przepływem danych
 - ◆ raportuje brak możliwości dostarczenia danych (z podaniem przyczyny)
 - ◆ umożliwia przekierowanie tras
 - ◆ testuje osiągalność zdalnego hosta
 - ◆ raportuje przekroczenie TTL protokołu IP (Time-To-Live), gdy pakiet jest zbyt wiele razy przekazywany pomiędzy kolejnymi hostami



Zastosowanie ICMP: ping i traceroute

- Polecenie ping wykorzystuje funkcjonalność ICMP *Echo*: host otrzymujący taki komunikat powinien odpowiedzieć
 - ♦ można sprawdzić dostępność hosta
 - ♦ można sprawdzić czas dostępu i jakość łącza
- Polecenie traceroute korzysta z funkcjonalności TTL protokołu IP i odpowiedzi ICMP do śledzenia drogi pakietów w sieci
 - ♦ pokazuje trasę, którą przebywają pakiety po drodze do zdalnego hosta
 - ♦ testuje, gdzie urywa się połączenie
 - ♦ pokazuje czas odpowiedzi w kolejnych etapach



Mapowanie adresów: DNS

- Usługa DNS (Domain Name Service) dokonuje zamiany (mapowania) nazwy literowej komputera na adres IP.
 - ♦ działa w warstwie aplikacji, t.j. w sieci musi być uruchomiona aplikacja serwera DNS na konkretnym komputerze. Jego adres musimy podać jako część konfiguracji sieci.
 - ♦ mapowanie nazwa-IP **nie** jest jednoznaczne, chociaż każde zapytanie o poprawną nazwę zawsze zwraca jeden numer IP
 - ♦ w lokalnej sieci jeden serwer DNS lub wcale
 - ♦ można użyć lokalnego pliku `/etc/hosts`



Mapowanie adresów: ARP

- Protokół ARP działa na połączeniu w. łączy danych i sieciowej. Dokonuje translacji adresów IP na adresy sprzętowe MAC
 - ♦ poprawne odpowiedzi ARP są przechowywane w lokalnej tablicy ARP (większa szybkość)
 - ♦ gdy adres IP jest poprawny, ale nie znajduje się w sieci lokalnej, ARP podaje adres urządzenia, które wie co dalej zrobić z pakietem
 - ♦ Adresy MAC są unikalne globalnie, ale nie da się ich użyć do adresowania w Internecie. Przy pomocy ARP poznajemy tylko adresy wewnątrz naszej sieci lokalnej (Ethernet)



Znaczenie i funkcje routera

- Router (gateway) jest urządzeniem łączącym sieć lokalną z inną siecią (w tym z Internetem)
 - ♦ działa w w. sieci – funkcjonuje na podstawie adresów IP
 - ♦ jego adres MAC jest granicą poza którą kończy się „sieć lokalna”
 - ♦ musi mieć połączenie z co najmniej dwoma sieciami i przekierowuje ruch pomiędzy nimi (w obie strony)
 - ♦ każdy komputer w sieci lokalnej, który chce połączyć się z Internetem musi znać jego adres (część konfiguracji komputera)



- Technologia NAT (Network Address Translation) mapuje jedne adresy IP/porty na inne
 - Powszechnie stosowane do podłączenia sieci prywatnych do Internetu
 - Taka sieć prywatna jest widoczna z zewnątrz jako jeden adres IP (adres routera), wewnątrz sieci komputery są rozróżniane przez ich adresy IP, na zewnątrz każda lokalna kombinacja IP+numer portu jest mapowane na inny port zewnętrzny routera.
 - Router musi obsługiwać NAT – gdy jakiś komputer z sieci lokalnej łączy się ze światem, połączenie jest mapowane na jeden z portów routera przypisanych do zewnętrznego adresu. Komunikacja zwrotna na ten port jest przekierowywana do hosta w sieci lokalnej.
 - Zalety i wady rozwiązania:
 - „Oszczędza” adresy IP
 - Utrudnia ataki na komputery w sieci lokalnej
 - Serwer postawiony na komputerze w sieci lokalnej nie będzie widoczny z zewnątrz (bez dodatkowych działań)



- Często stosowaną konfiguracją sieci lokalnej jest zmiana sposobu podłączenia do sieci Internet: zamiast routera używa się gateway
 - ♦ Router to urządzenie działające w w. sieci i w. transportowej, gateway działa w w. aplikacji
 - ♦ Aby dostać się do „wewnętrznej” sieci, należy najpierw zalogować się na gatewayu, dopiero z niego można połączyć się z komputerami w sieci lokalnej. Połączenia wychodzące zwykle nie mają tego ograniczenia.
 - ♦ Pozwala to na lepszą kontrolę bezpieczeństwa, dodatkowo sieć lokalna może być nierutowalna



- Interfejs sieciowy, to punkt dostępu przy pomocy którego komputer komunikuje się z siecią
 - ♦ zwykle jest związany z konkretnym urządzeniem fizycznym (kiedyś kartą sieciową, teraz zwykle wbudowaną w płytę główną), ale nie zawsze (np. interfejs loopback)
 - ♦ ma przypisany adres sieciowy (dla Internetu: adres IP)
 - ♦ jest obiektem używanym w konfiguracji bardziej zaawansowanych funkcjonalności sieciowych (routing, dzielenie łącza)



- „Skonfigurowanie sieci” polega na logicznym powiązaniu adresów z konkretnymi urządzeniami oraz wskazanie sposobów połączenia z najważniejszymi usługami
 - ♦ Musimy się upewnić, że mamy poprawnie uruchomione urządzenie fizyczne (zwykle: poprawnie zainstalowany sterownik)
 - ♦ Adres IP przypisujemy poleceniem `ifconfig`
 - ♦ Wskazujemy sposób kontaktu z adresami poza naszą siecią lokalną poleceniem `route`
 - ♦ Podajemy adres IP serwera DNS (plik `/etc/resolv.conf`)

- Protokół i usługa DHCP umożliwiają automatyczną konfigurację urządzeń w sieci lokalnej
 - ♦ działają w warstwie aplikacji
 - ♦ nowy komputer zgłasza się podając swój adres MAC (czyli tylko sieć lokalna!) i czeka na odpowiedź
 - ♦ w odpowiedzi dostaje np. numer IP(+maska), adres serwera DNS oraz sposób połączenia z Internetem (adres bramy – gateway)
 - ♦ adres przyznany przez DHCP ma okres ważności
 - ♦ poprawna konfiguracja serwera DHCP ułatwia instalację i zarządzanie siecią lokalną