Laboratorio di Reti di Calcolatori

Lezione 2

Il livello applicazione

- I protocolli di **livello applicazione** si collocano al di **sopra** dello **stack TCP/IP**
  - immediatamente prima del **livello** di **trasporto**
  - rappresentano l'interfaccia utente al protocollo di rete
- Utilizzano **UDP** o **TCP** come meccanismo di trasporto
- Le applicazioni basate su UDP devono provvedere proprie routine
  - per il controllo del flusso
  - per la gestione di situazioni di errore
- UDP può garantire prestazioni migliori a causa del ridotto overhead

Il livello applicazione

• I protocolli che impiegano il livello di trasporto utilizzano la **nozione di porta** per l'individuazione di un **servizio**

• Le porte sono interi a 16 bit (da 0 a 65535, sia per TCP che UDP) che, abbinati agli indirizzi IP, sono utilizzati per stabilire una connessione tra le parti in comunicazione

• Alcuni servizi (FTP) usano una coppia di porte per la realizzazione della modalità duplex (ftp-data=20, ftp=21)
  • ma un'unica porta garantisce la modalità full-duplex

• **IANA** (Internet Assigned Numbers Authority) si occupa dell'attribuzione ufficiale di un servizio ad una porta
  • porte "ben note" (da 0 a 1023; servizi base o "storici");
  • porte registrate (da 1024 a 49151, servizi registrati);
  • porte dinamiche o private;

Il livello applicazione: C/S

- Molte applicazioni adottano il **modello client-server**:
  - gli utenti interagiscono con la parte **client**
    - costruire la richiesta per un particolare servizio
    - inviarla alla componente server utilizzando TCP/UDP
  - il **server** è un programma che
    - riceve una richiesta
    - esegue il servizio richiesto
    - invia i risultati al client
- La comunicazione è effettuata mediante opportune API
  - le socket API (stile BSD e derivate: Winsock)
  - le Remote Procedure Call (RPC) API

Il livello applicazione: P2P

- Il modello **peer-to-peer** (**P2P**) è un paradigma di progettazione per le **applicazioni distribuite** in cui le entità partecipanti condividono le proprie risorse per contribuire attivamente alla fornitura del servizio

- Ogni entità (**peer**) partecipa alla fornitura del servizio **agendo** contemporaneamente come **client** e come **server**

- Il servizio è fornito in modo **distribuito** e **decentralizzato**

- Nei sistemi P2P gli utenti accedono alle risorse in seguito ad una fase di **ricerca** di un **nodo** già **connesso**

- È necessario uno spazio di **indirizzamento** ed un algoritmo di **routing**

- I peer cooperano formando una **overlay network**

Servizi di rete

- I **servizi di rete** vengono attivati all'avvio del sistema operativo
  - attraverso la procedura di inizializzazione del sistema
  - dopo l'assegnazione degli indirizzi alle interfacce di rete
  - dopo la definizione degli instradamenti
- I processi che realizzano tali servizi si chiamano **demoni**
  - operano silentemente in background
- La **gestione** dei demoni può essere:
  - autonoma, detti **standalone**
  - gestiti da un processo **supervisore** (Internet service daemon)

Servizi di rete

- I **servizi standalone** sono
  - programmi avviati al boot del sistema
  - sempre in esecuzione
  - si occupano di ascoltare su una determinata porta di rete
  - provvedono da soli al controllo degli accessi al servizio
- I servizi gestiti dal **supervisore** sono
  - avviati dal supervisore in caso di richiesta del servizio
- Il supervisore si occupa di ascoltare su tutte le porte dei servizi che controlla
- **NFS** (Network File System) è un servizio standalone
- **FTP** (File Transfer Protocol) è un servizio gestito

Servizi di rete

- La configurazione di un servizio **standalone** si effettua attraverso **file di configurazione** del servizio

- La configurazione dei **servizi gestiti** si effettua tramite i **file di configurazione del supervisore** di rete

  - **inetd.conf** sui sistemi UNIX(-like) che utilizzano il supervisore inetd

  - **xinetd.d**/<service> sui sistemi UNIX(-like) che utilizzano il supervisore xinetd

- Sui sistemi windows si utilizza la funzionalità servizi della Microsoft Management Console (MMC);

Domain Name Service

- La gestione degli indirizzi IP in forma numerica è una pretesa inaccettabile dal lato utente
- Per tale ragione agli indirizzi IP sono di solito associati dei nomi
- La **trasformazione di un indirizzo in un nome** può avvenire in due modi
  - tramite un elenco indirizzo-nome contenuto nel file **/etc/hosts**
  - utilizzando il **servizio DNS**
- L'utilizzo del DNS impone l'utilizzo della convenzione dei **nomi di dominio**

Domain Name Service

- La convenzione per i nomi host usata dal servizio DNS è rappresentabile da una **struttura ad albero**

- La **radice dell'albero** è il dominio principale, rappresentato da un punto singolo (solitamente è sottinteso)

- Ogni **nodo** dell'albero è un **dominio**

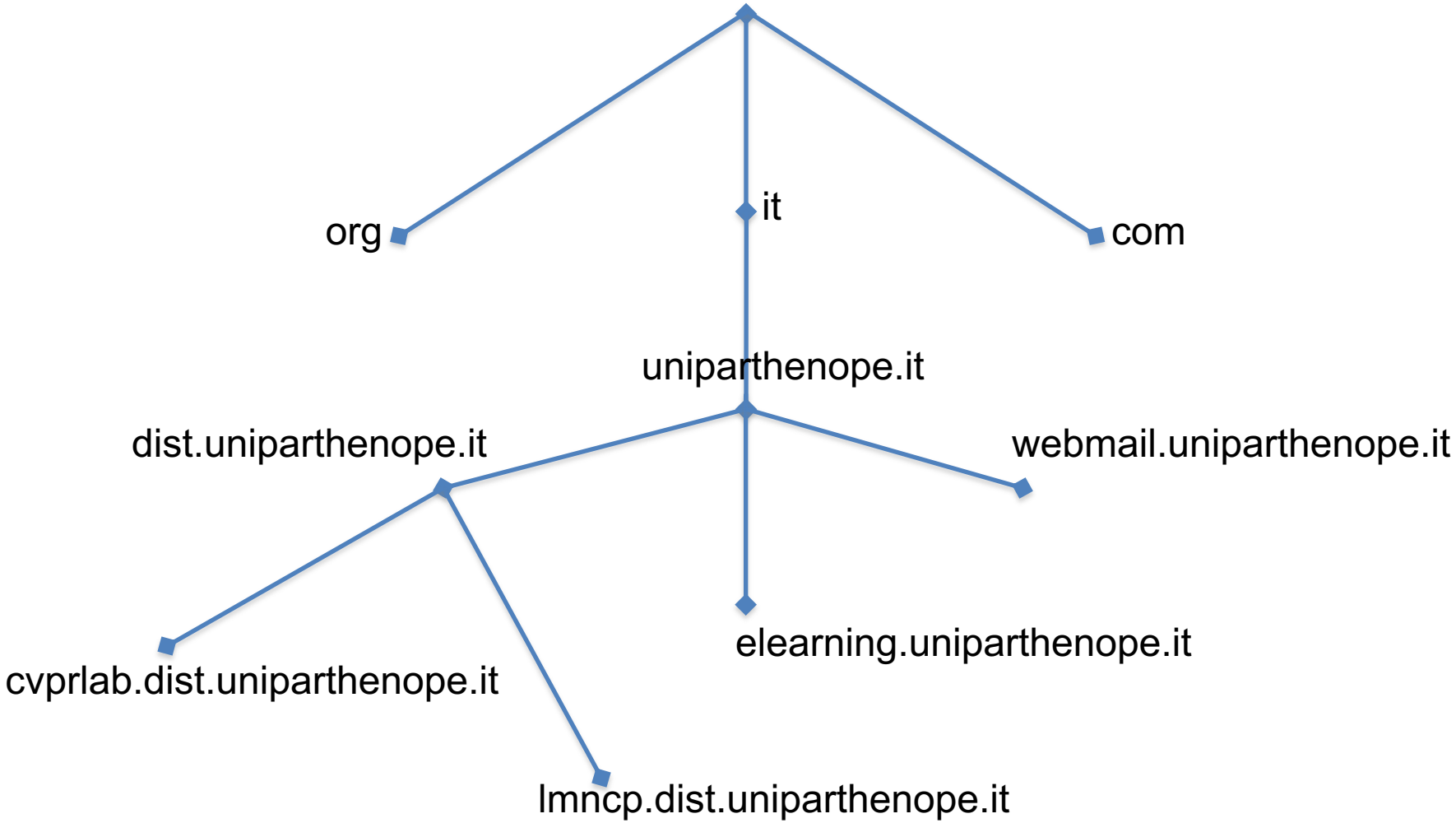
- Il **nome di un dominio** si ottiene

    - effettuando l'unione dei nomi dei nodi attraversati per giungere alla radice

    - separando tali nomi l'uno dall'altro con un punto

- I **nodi terminali** dell'albero corrispondono a degli **host** di rete

Domain Name Service



Autorità di registrazione

• I nomi di dominio utilizzati in Internet si ottengono attraverso una fase chiamata registrazione

• La registrazione avviene facendo una richiesta all'autorità competente per la zona a cui appartiene il nome

• Generalmente si registrano nomi di secondo livello, per cui ci si rivolge all'**autorità di registrazione (RA)** competente per il dominio di primo livello

ICANN

• La RA di gerarchia più alta di tutte è l'Internet Corporation For Assigned Names and Numbers (ICANN, www.icann.org):

• ICANN è un'organizzazione no-profit responsabile della gestione e del coordinamento del DNS a livello mondiale, che:

  • è competente per la zona relativa alla radice dell'albero dei domini

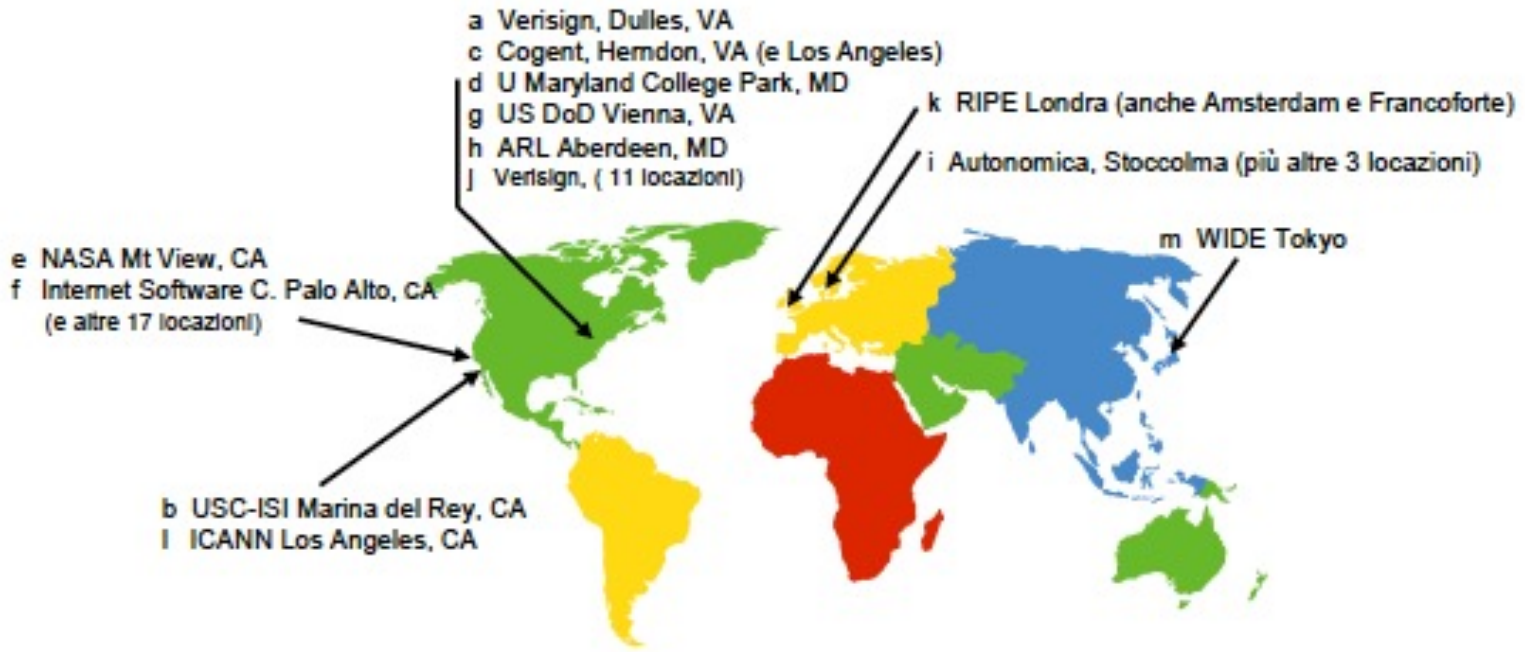
  • demandando la gestione dei domini di primo livello ad opportune RA, le Top Level Domain RA (**TLD RA**)

  • delega **13 named authorities** ubicate in diverse parti del mondo, con funzione di **root server**

  • ciascuno dei root server dell'ICANN contiene uno stesso database di informazioni nomi-indirizzi, relativo alle TLD RA

• ICANN gestisce un sito web (www.internic.com) per fornire informazioni sullo status delle registrazioni di domini Internet;

ICANN


a Verisign, Dulles, VA
c Cogent, Herndon, VA (e Los Angeles)
d U Maryland College Park, MD
g US DoD Vienna, VA
h ARL Aberdeen, MD
j Verisign, (11 locazioni)
k RIPE Londra (anche Amsterdam e Francoforte)
i Autonomica, Stoccolma (più altre 3 locazioni)
m WIDE Tokyo
e NASA Mt View, CA
f Internet Software C. Palo Alto, CA
(e altre 17 locazioni)
b USC-ISI Marina del Rey, CA
l ICANN Los Angeles, CA

Informazioni pubblicate dalle RA

• Le RA sono tenute a pubblicare un certo numero di **informazioni sui domini** di loro competenza

  • l'azienda od organizzazione a cui è intestato il dominio

  • il personale dell'azienda responsabile della gestione del dominio (ossia dei server autoritativi), con nome, indirizzo, etc.

  • il periodo di validità della registrazione

  • i nomi DNS e/o indirizzi IP degli host che fungono da server autoritativi

• Queste notizie sono accessibili attraverso il **protocollo NICNAME** (**WHOIS**);

Interrogazione WHOIS

• I database WHOIS sono interrogabili via WEB dai siti delle società che effettuano le registrazioni per conto dell'ICANN, oppure direttamente dai siti delle TLD RA

• Per il dominio .it il registro della TLD RA è disponibile all'indirizzo www.nic.it/RA/index.html

• Sono disponibili diversi client per l'interrogazione, che dipendono dal SO Utilizzato

  • i sistemi Unix/Linux dispongono di un **client WHOIS** il cui nome è **whois**

  • per i sistemi windows sono disponibili delle implementazioni freeware di terze parti (es.: win32whois)

Interrogazione WHOIS

```
ale@mbp ~# whois uniparthenope.it


*******************************************************************************
* Please note that the following result could be a subgroup of      *
* the data contained in the database.                               *
*                                                                   *
* Additional information can be visualized at:                      *
* http://www.nic.it/cgi-bin/Whois/whois.cgi                         *
*******************************************************************************
```

...

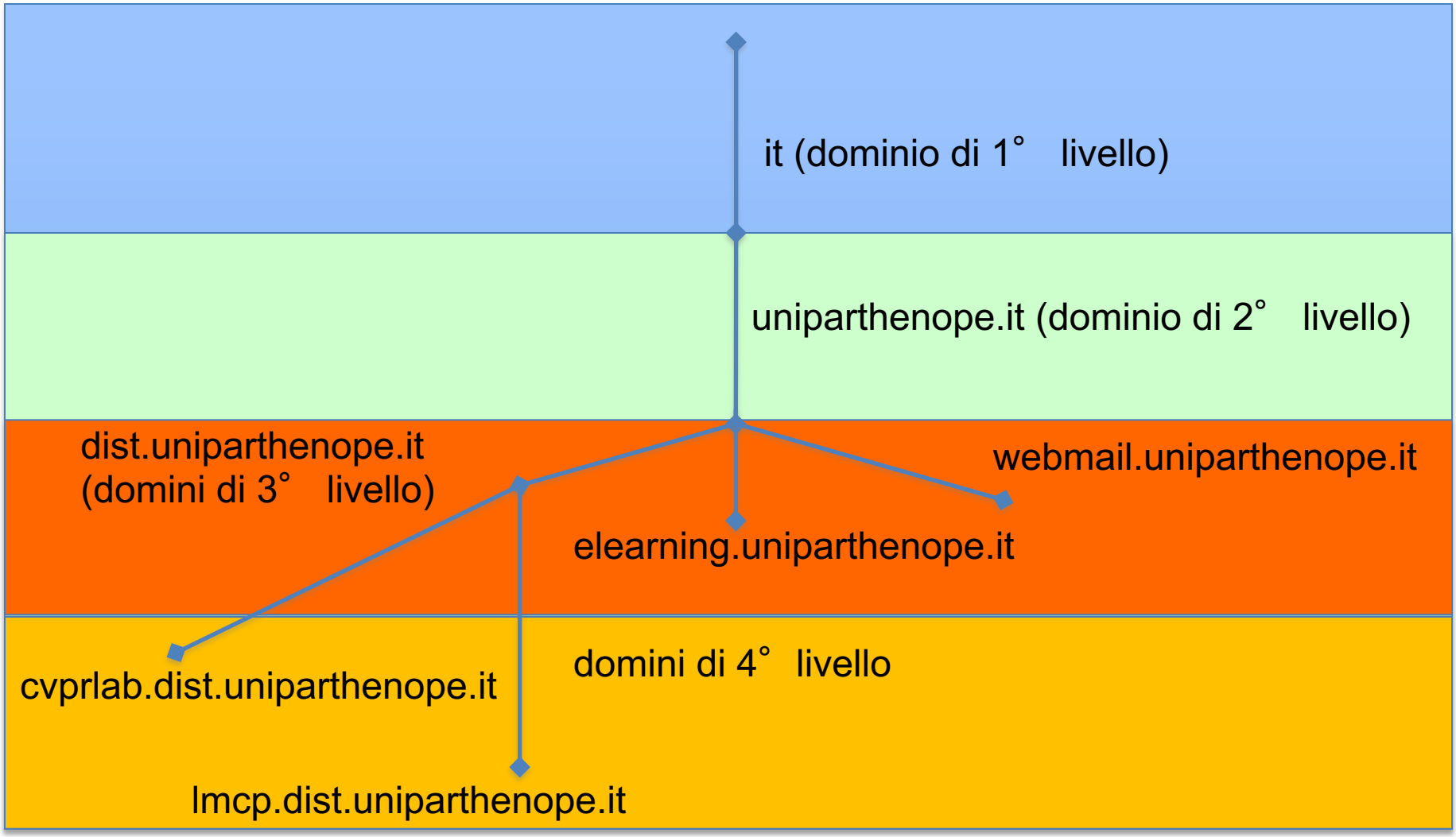
```
Nameservers
  nava1.uniparthenope.it
  parthenope.uniparthenope.it
  ns1.garr.net

ale@mbp ~#
```

Domain Name Service

- Il DNS è un **servizio distribuito**
  - un **insieme di server** di nomi (host su cui è in esecuzione il servizio)
  - ciascuno con una propria **zona di competenza**
- Una **richiesta di traduzione** nome-indirizzo è inviata al server di zona
  - se tale informazione non è disponibile
  - invia la richiesta e recupera l'informazione da un altro server DNS
- Le **zone di competenza si sovrappongono all'albero dei domini**
  - in modo da garantire che una qualsiasi richiesta possa essere soddisfatta
  - grazie all'interrogazione di una opportuna catena di server

Domain Name Service



Domain Name Service

• Ogni zona organizza le informazioni di sua competenza in **record di risorsa**

• I record di risorsa definiscono l'**associazione** tra un **nome** di dominio ed un'altra **informazione**, **in base al tipo di record**

• Es.:

  • Per cercare l'indirizzo IP associato ad un certo nome si consultano i record di tipo A (Address)

  • Per conoscere un servizio di risoluzione dei nomi competente (autoritativo) per una certa zona (individuata attraverso un nome di dominio) si consultano i record di tipo NS (Name Server)

Record risorsa

Nome	TTL	Classe	Tipo	Dati

- Nome: nome di dominio
  - stringhe alfanumeriche
  - iniziano con una lettera
  - hanno max 63 caratteri
  - separate da un punto
  - non vi è distinzione tra maiuscole e minuscole

- Tempo di vita: tempo di validità in minuti del record per un server caching-only
  - un unsigned int (32 bit) che esprime (di default 86400 = 1 giorno)

- Classe: individua il tipo di protocollo
  - l'unico valore previsto è IN (Internet)

- Tipo: tipo di informazione associata al nome di dominio

- Dati: informazione associata al nome di dominio

Tipi e dati di un record di risorsa

TIPO	VAL	SIGNIFICATO	DATI
A	1	L'indirizzo di un host	Un indirizzo IP
CNAME	5	Il nome canonico: specifica un alias per un host	Un nome di dominio
HINFO	13	La CPU ed il SO utilizzati dal computer host	Un commento
MX	15	Un server di mail per il dominio.	Un numero seguito da un nome di dominio
NS	2	Un server autoritativo per il dominio	Un nome host
PTR	12	Un puntatore a un'altra parte dello spazio dei nomi	
SOA	6	L'inizio di una zona di autorità	Parametri di config. relativi alla zona
WKS	11	Servizi di rete certamente in esecuzione su un dato host	Un indirizzo IP, il prot. trasp. ed i servizi

Domain Name Service

Per ciascuna zona ***Z***, si distinguono **tre tipi di server** di nomi:

- **Primario (autoritativo)**
  - dispone e gestisce in locale il database relativo a ***Z***
- **Secondario (autoritativo)**
  - riceve il database di ***Z*** da un server primario, tramite il processo di "**trasferimento di zona**"
  - per restare sincronizzato con un server primario, interroga quest'ultimo ad intervalli regolari (di default 3 ore), effettuando un trasferimento qualora esso sia stato aggiornato
- **Caching-only (non autoritativo)**
  - non dispone in locale del database di ***Z***
  - dispone di un **record di tipo NS** grazie al quale può ricevere le informazioni di zona di ***Z.***

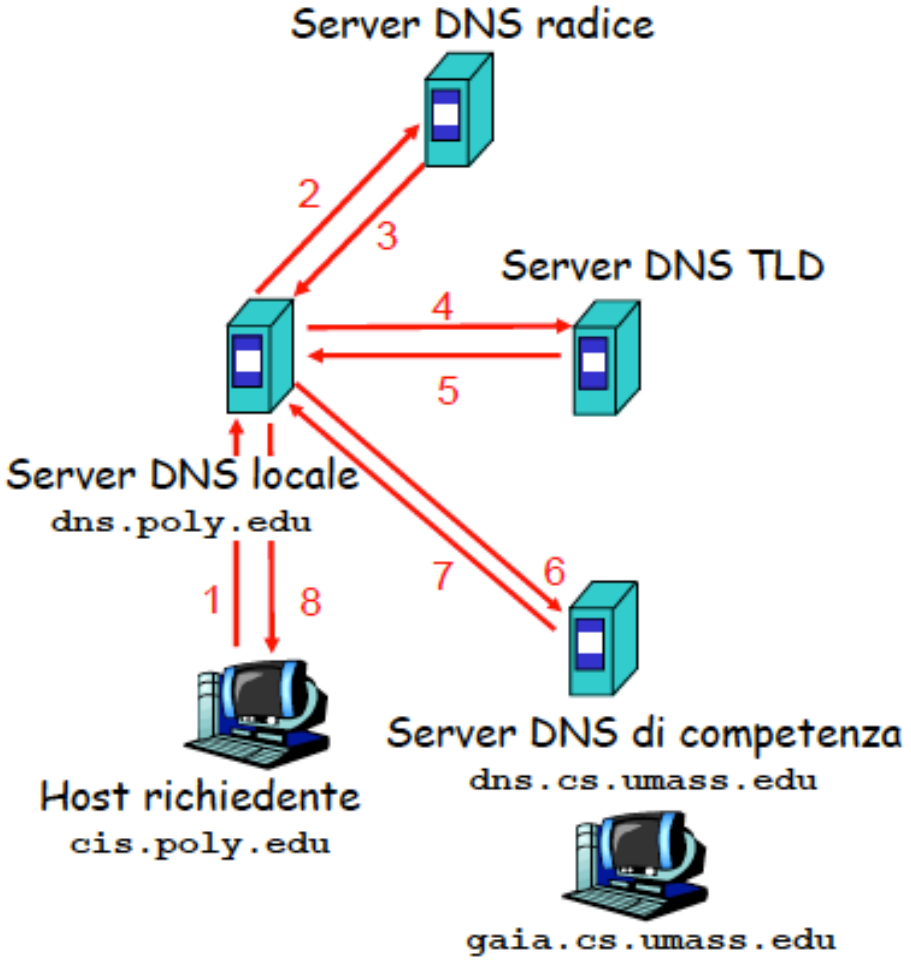
Risoluzione diretta: query iterativa

Esempio:

- L'host cis.poly.edu vuole l'indirizzo IP di gaia.cs.umass.edu
- Il server locale contatta un sever radice, o un server TLD
- Il server contattato risponde con il nome del server da contattare:

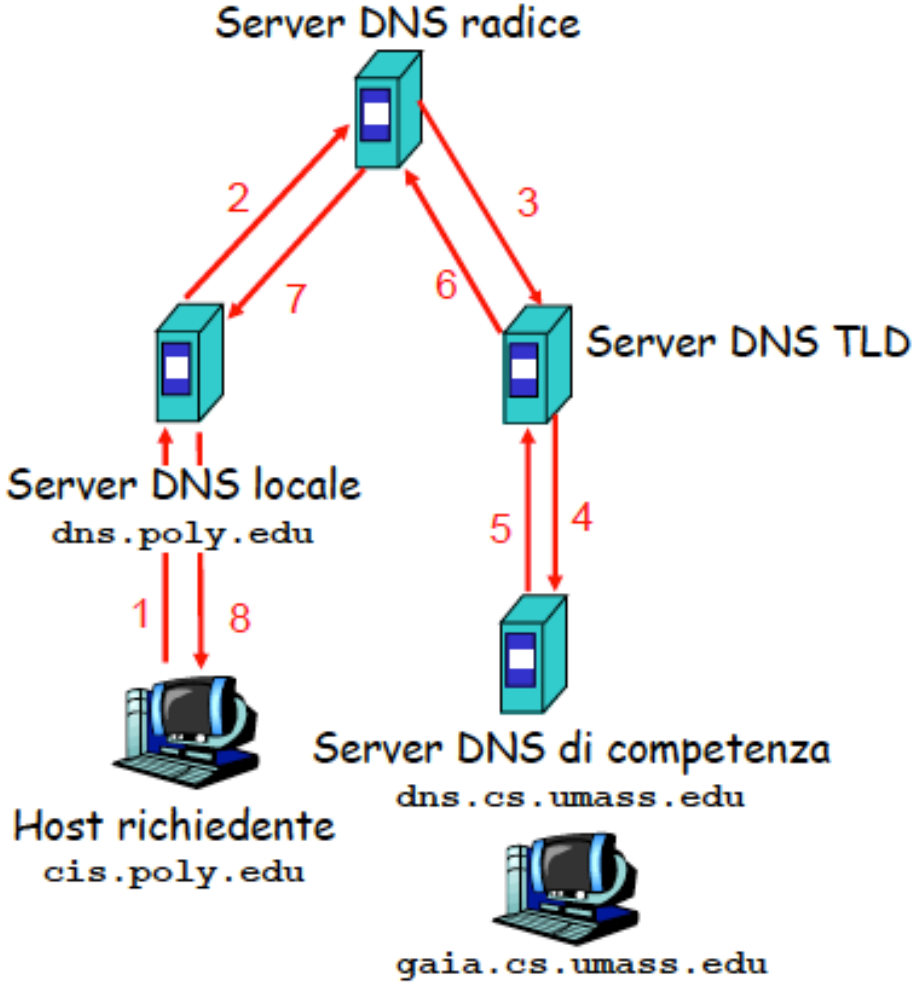
  "Io non conosco questo nome, ma puoi chiederlo a quest'altro server"

  e così via...



Risoluzione diretta: query ricorsiva

- Il server locale affida al server contattato il compito di tradurre il nome
- Ogni server che non è in grado di rispondere si rivolge esso stesso ad un altro server ed attende la risposta
- La risposta torna al server locale seguendo lo stesso percorso



Risoluzione inversa

• Il DNS fornisce anche un meccanismo per la **traduzione** di un **indirizzo IP** in un **nome di domino** (risoluzione inversa)

• Questo meccanismo, vista la natura degli indirizzi IP, non può sfruttare l'approccio gerarchico usato nella ricerca di un IP a partire da un nome di dominio

  • necessita di uno **spazio dei nomi specifico**

• Il dominio utilizzato è **in-addr.arpa**, per il quale gli indirizzi IP sono rappresentati al contrario (es: 192.168.1.5 diviene 5.1.168.192), per omogeneità con la codifica dei nomi di dominio.

Interrogazione DNS

- L'interrogazione di un servizio DNS corrisponde all'interrogazione di una base di dati distribuita, in cui il risultato è il record desiderato
- La base di dati del DNS ha due scopi
  - trovare l'indirizzo numerico associato ad un nome
  - trovare il nome a partire da un indirizzo numerico
- Esistono diverse modalità per interrogare il servizio direttamente

Interrogazione DNS

• Per interrogare direttamente un server DNS sono disponibili comandi specifici

• L'**interrogazione** andrebbe effettuata su un **server autoritativo** per il dominio in questione

  • tali host contengono tutte le informazioni col **massimo livello di aggiornamento**

• Se esiste più di un server autoritativo, è probabile che essi abbiano una diversa versione del servizio, oppure una diversa configurazione

  • alcune query possono essere rifiutate su dei server e abilitate su altri

Interrogazione diretta

• Il programma classico per l'interrogazione del DNS è **nslookup**, disponibile sia su sistemi di tipo Unix che Windows

• Su alcuni sistemi Linux, ad nslookup sono preferiti programmi quali **host** e **dig**, e l'implementazione di nslookup può essere solo parziale

• Nell'implementazione completa **nslookup** prevede il comando **ls**, che permette di ottenere l'elenco di tutti i record presenti sul server DNS

• Generalmente la query di ls viene impedita

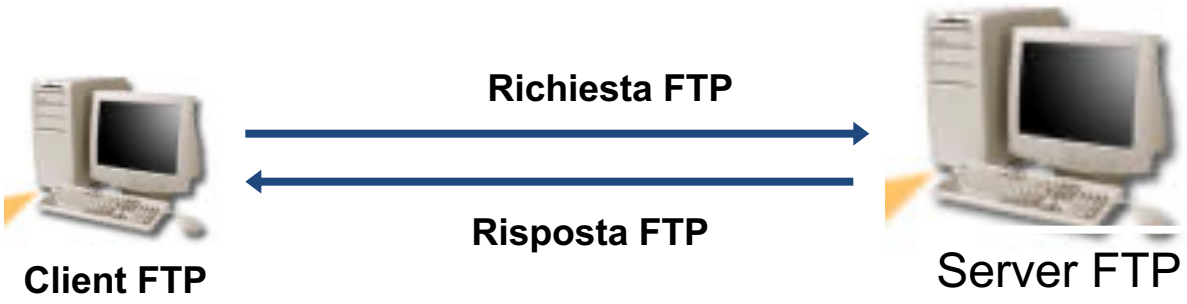
nslookup

- nslookup google.com [server dns]
- nslookup –type=mx google.com [server dns]
- nslookup –type=ns google.com [server dns]
- nslookup –type=any google.com [server dns]

File Transfer Protocol

- Il servizio FTP è l'acronimo di File Transfer Protocol, un protocollo che si utilizza per trasferire file (di testo o binari) tra computer collegati ad una rete.

- Mediante FTP è possibile
  - connettersi ad un sistema remoto ("server"),
  - visualizzare archivi di file
  - trasferire file dal proprio computer a quello remoto e viceversa.



Connessioni dati e controllo

- FTP utilizza due tipi di connessioni:
  - Connessione di controllo sulla **porta 21**
  - Connessione dati sulla **porta 20**

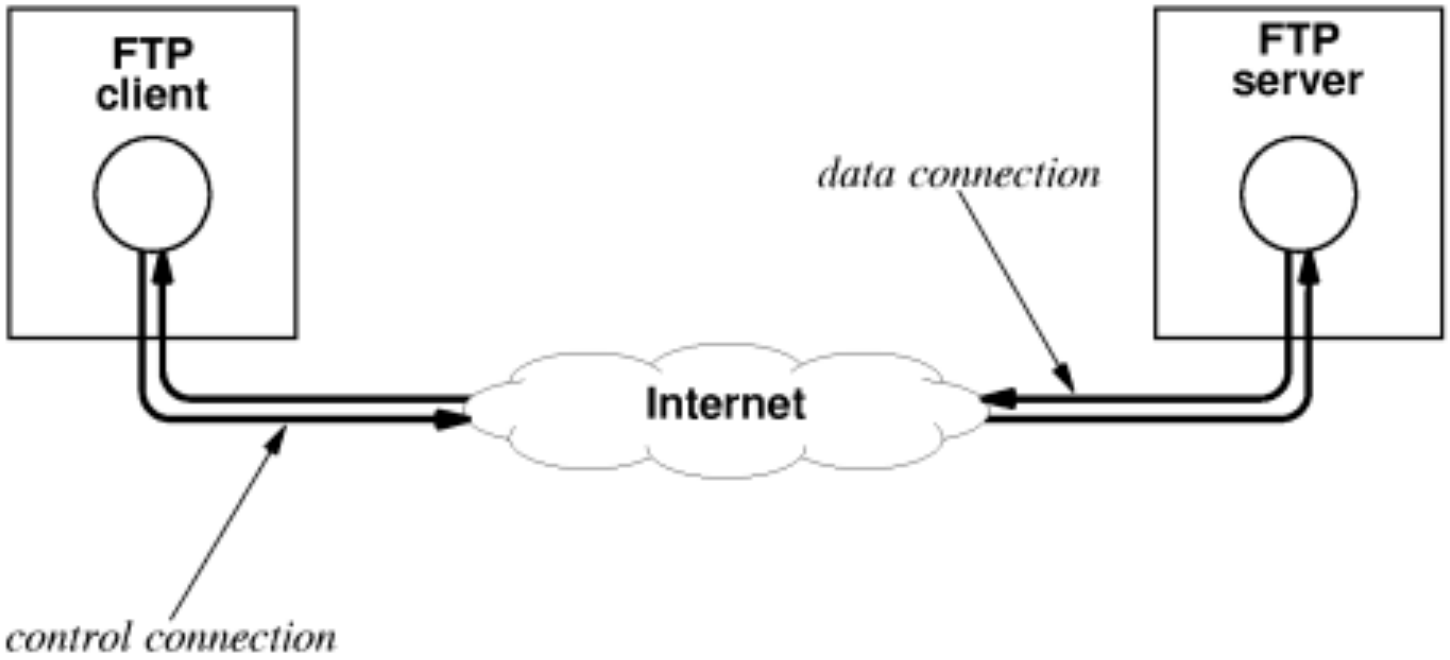
- La **connessione di controllo** è **richiesta** dal **client** ed è sempre aperta all'interno di una sessione.

- La **connessione dati** viene **richiesta** dal **server** (che si comporta quindi da client) ed è aperta solo durante gli effettivi trasferimenti di file.

- La separazione tra dati e controllo è utile sia per ragioni di semplicità (separare messaggi di natura diversa), sia per consentire il controllo "fuori banda" dei trasferimenti di file.

- Protocollo Out Of Band (OOB)

Connessioni dati e controllo



File Transfer Protocol

- **FTP** utilizza **due processi** distinti
  - **PI** (Protocol Interpreter) attraverso cui il client invia i comandi e riceve le risposte dal server;
  - **DTP** (Data Transfer Process) attraverso il quale il client ed il server si scambiano i dati;
- Il Data Transfer Process può essere di due tipi
- **Active MODE:** il client contatta il server il quale da inizio alla connessione (sulla porta 20) per trasmettere i dati con il client.
- **Passive MODE**: il client avvia anche la connessione per il trasferimento dei dati.

File Transfer Protocol

- Ad **ogni comando** inserito il server risponde inviando un **codice** che identifica la riuscita o meno dell'operazione richiesta.
- I **codici sono numerici** e composti da tre caratteri **xyz**, ognuno dei quali identifica in modo sempre più dettagliato lo stato delle operazioni. In particolare avremo in x il valore più significativo in y un maggiore dettaglio in relazione a x così di seguito per z.
- Per quanto riguarda il codice di risposta più significativo, ovvero il primo dei tre caratteri abbiamo:
  - 1yz: **Risposta preliminare positiva**. Indica che il comando è stato accettato e che si avrà un'ulteriore risposta prima del comando successivo;
  - 2yz: **Comando terminato con successo**;
  - 3yz: **Risposta intermedia positiva**. Comando eseguito correttamente e in attesa di ulteriori informazioni per completare l'operazione;
  - 4yz: **Il comando non è stato eseguito correttamente**;
  - 5yz: **Comando che il server non ha potuto eseguire**;

File Transfer Protocol

- Per trasferire un file con FTP è necessario installare sul proprio computer un programma ad-hoc (FTP client) che dialoga con un programma analogo, ma più sofisticato (FTP server)

- Per usare FTP sono disponibili numerosi programmi (quasi sempre forniti dai sistemi operativi che supportano il protocollo TCP/IP).
  - Windows e Linux, ad esempio, includono un client FTP.

- In rete sono disponibili molti client FTP ed alcuni sono disponibili gratuitamente.

Upload e download

- Con FTP è possibile copiare file
  - dal proprio PC al computer remoto (operazione denominata upload)
  - dal computer remoto al proprio PC (operazione denominata download).
- Quando si stabilisce una connessione con un sito FTP vengono richiesti un **login** e una **password**, perché si suppone che l'utente disponga di un accesso personale a quel server.

FTP anonimo

- Per poter creare archivi di software aperti al pubblico, si usa il cosiddetto FTP anonimo.

- E' un accesso che chiunque può utilizzare, e mediante il quale si accede ad una parte del file system del server in cui sono contenuti file "pubblici".

- Quando si parla di "FTP" e di "siti FTP", si sottintende normalmente una connessione di tipo anonimo, ed i programmi di FTP effettuano come default connessioni di questo tipo.

FTP anonimo

- La modalità anonima viene normalmente attivata indicando, all'atto del collegamento,
  - come login "**`anonymous`**" - è un nome convenzionale
  - e come password il proprio indirizzo di E-mail.

- Si avrà accesso nella directory radice del sito FTP, nella quale viene solitamente posta una sottodirectory denominata pub (pubblica) che contiene i file che è possibile trasferire.

FTP

- >ftp
  - open 192.168.0.1
    - login: root
    - password: toor
  - open 192.168.0.1
    - login: anonymous
    - password: anon@anon.com
- >ncftp –u root 192.168.0.1
- >ncftp
  - open 192.168.0.1

FTP

- >ftp ftp.uniparthenope.it
  - login: anonymous
  - password: anon@anon.com

Comandi FTP

ftp> open sito
login:
Password: Si collega con il sito indicato, fornendo login e password.

cd pippo	Entra nella directory `pippo` sul computer remoto.
pwd	Scrive il nome completo della directory remota in cui vi trovate.
ls	Mostra i file contenuti nella directory corrente.
lcd pippo	Entra nella directory `pippo` sul vostro computer.
binary (o bin)	Setta la modalità di trasferimento binaria.
ascii (o asc)	Setta la modalità di trasferimento ASCII.
get nomefile	Preleva il file `nomefile` e lo salva nella directory corrente sul vostro computer.
prompt	Esclude la modalità interattiva, utile per trasferimenti multipli
mget nomefile	Come get, ma permette l'uso di asterischi nel `nomefile`.
put nomefile	Copia il file `nomefile` dal vostro computer a quello remoto.
mput nomefile	Come put, ma permette l'uso di asterischi nel `nomefile`
Hash	Stampa un # per ogni blocco di 1 KB trasferito con successo
help	Mostra l'elenco dei comandi supportati.
quit	Si scollega dal sito a cui si è collegati.
bye	Si scollega dal sito a cui si è collegati ed esce dal programma
CTRL-C	Per interrompere un trasferimento

Comandi utili

- Per creare files da trasferire
  - dd if=/dev/zero of=/media/sda1/testfile bs=16k count=16384
  - crea un file di 256M (16384 blocchi da 16k)

- Per modificare la configurazione di ncftpd (su pc1)
  - /usr/local/etc/ncftpd/general.cf
  - /usr/local/etc/ncftpd/domain.cf

Per riavviare il server ncftpd

  - /usr/local/sbin/restart_ncftpd