



Reti di Calcolatori e Cybersecurity

CDN -Content Delivery Networks

Ing. Vincenzo Abate

DNS: chi fa cosa

Entità in gioco: Un'entità può coprire più modi

- **Resolver**
 - È il client da cui parte la richiesta di risoluzione al sistema DNS
 - È una funzionalità user-level del sistema operativo dell'end system
- **Registry**
 - È titolare della risoluzione di un determinato name space
 - È l'organizzazione abilitata a fare modifiche al database dei nomi di un determinato dominio
 - Mantiene in esercizio i server autoritativi per un determinato dominio
- **Registrar**
 - È l'agente che sottmette al registry le richieste di modifica di risoluzione per conto del registrant
- **Registrant**
 - È l'entità che “possiede” l’uso di un determinato dominio
Chi usa il dominio (non gli fa un server)

DNS: esempio

Esempio: azienda Network Utopia

Per prima cosa si vuole registrare il dominio **networkutopia.com** presso un ente di registrazione (registrar)

Un registrar è rappresentato da un'azienda che verifica l'unicità del nome di dominio, lo inserisce nel database DNS in cambio di denaro

Prima del 1999 un'azienda unica aveva il monopolio sulla registrazione dei nomi di dominio .com .net e .org

Adesso esistono molti registrar concorrenti accreditati dalla ICANN (Internet Corporation for Assigned Names and Numbers) (vedi lista www.internic.net)

In fase di registrazione occorre fornire al registrar gli indirizzi IP dei DNS server autoritativi

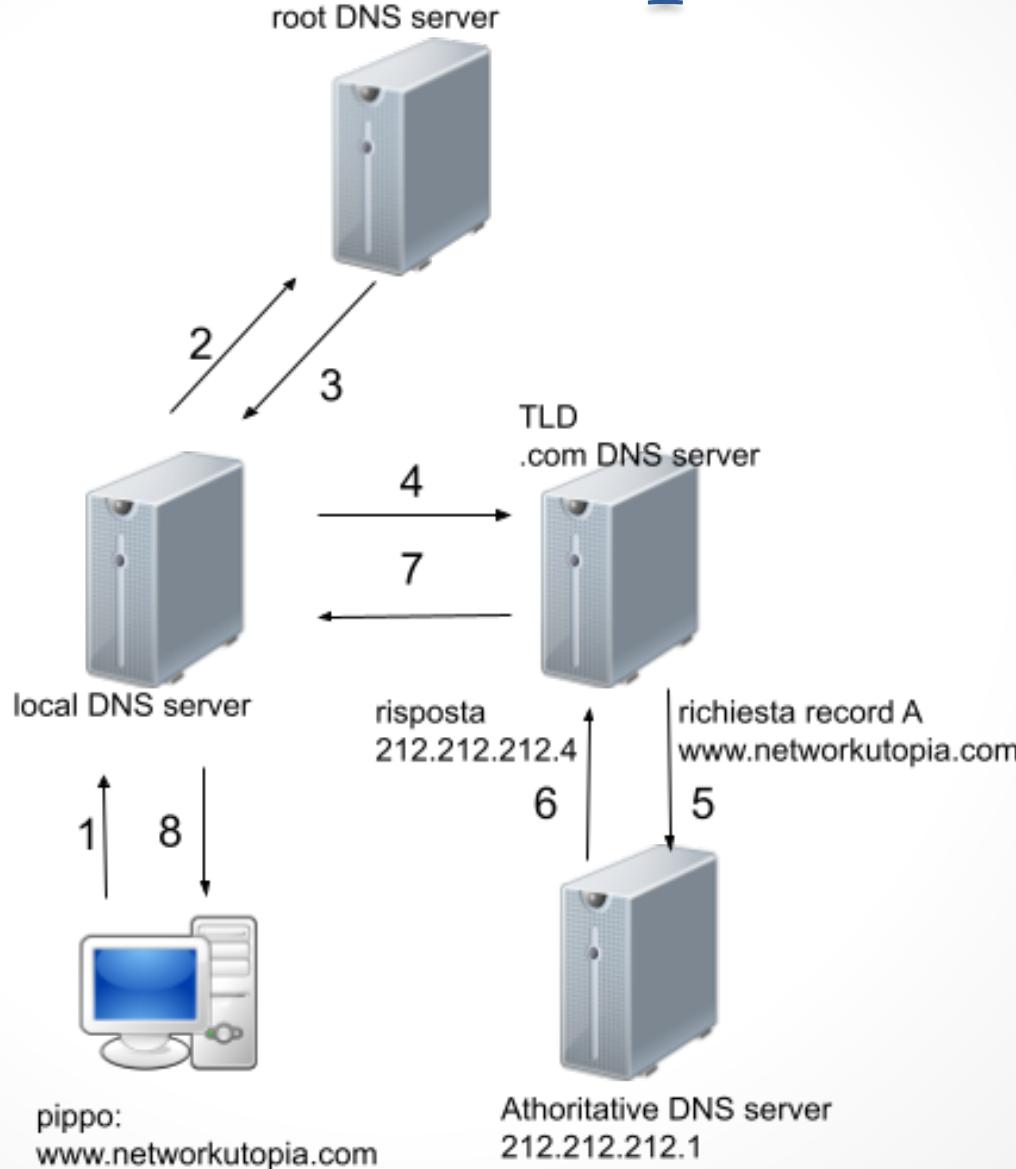
L'ente si accerterà dell'inserimento di un record NS e uno A nei TLD relativi al suffisso .com

networkutopia.com, dns1.networkutopia.com, NS

dns1.networkutopia.com, 212.212.212.1, A

• *Nel TLD ci devono essere queste* •

DNS: esempio



DNS: vulnerabilità

DNS è componente critico dell'infrastruttura di internet (servizi come web e posta elettronica non possono farne a meno)

E' possibile attaccare un DNS per metterlo fuori uso e di conseguenza bloccare tutti i servizi correlati?

Un possibile attacco è il DoS con flooding di banda:

Un attaccante può inondare di pacchetti tutti i root server lasciando senza risposta le richieste legittime

Caso 2002 messaggi ICMP mandati da botnet verso i 13 root server, fortunatamente molti server avevano sistemi di filtraggio dei pacchetti per bloccare pacchetti ICMP

Un'altra possibilità è un flooding di richieste DNS verso server di primo livello (TLD) (es 2016)

Altri possibili attacchi: man-in-the-middle e DNS poisoning

↓
Invecchiato, chi richiede con risposte filtrate

↳ nuovo record
inserito nelle cache DNS

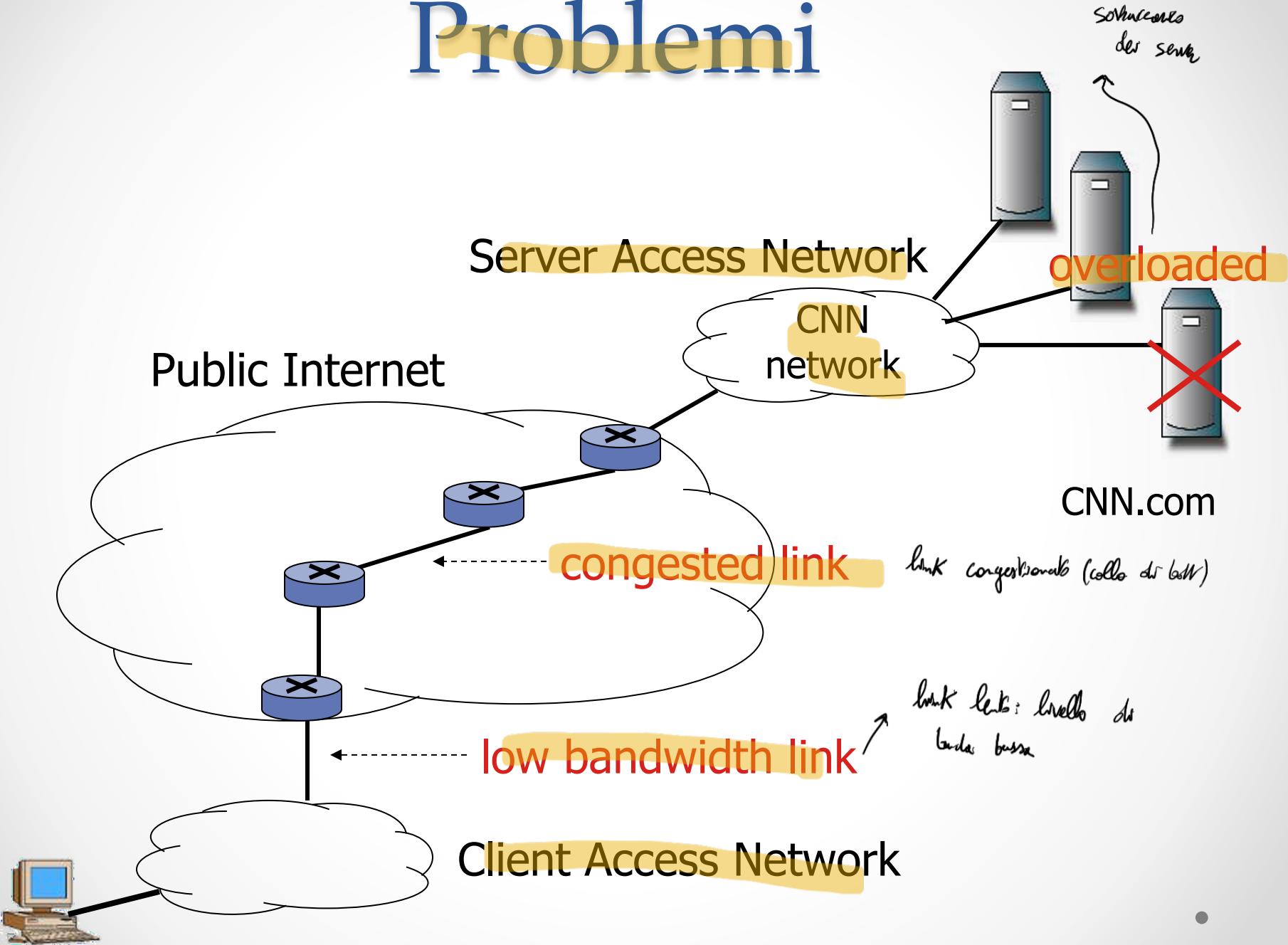
Web Timing

- Per un sito web una metrica importantissima è il **TTI** (time to interactive)
- **TTI** è il tempo che la pagina web impiega per rendere i suoi contenuti fruibili all'utente
- Una ricerca di Radware mostra che il 57% dei consumatori online abbandona una pagina web di un sito di e-commerce che richieda più di 3 secondi per caricarsi
- Se il tempo di caricamento di una pagina web supera i 10s, circa il 40% degli utenti rinuncia a proseguire la navigazione
- Il **tasso di conversione** (conversion rate) di un sito di e-commerce è la frazione percentuale di visite al sito che si traduce in una transazione commerciale (tipicamente, una vendita)

Conversion Rate = Number of Sales / Number of Visits

- Il **tasso di conversione** è fortemente influenzato dal tempo di caricamento delle pagine web del sito (particolarmente per l'accesso da terminali mobili)
- Amazon stima che un aumento della latenza media di 100 ms comporti una perdita di ricavi dell'1%

Problemi



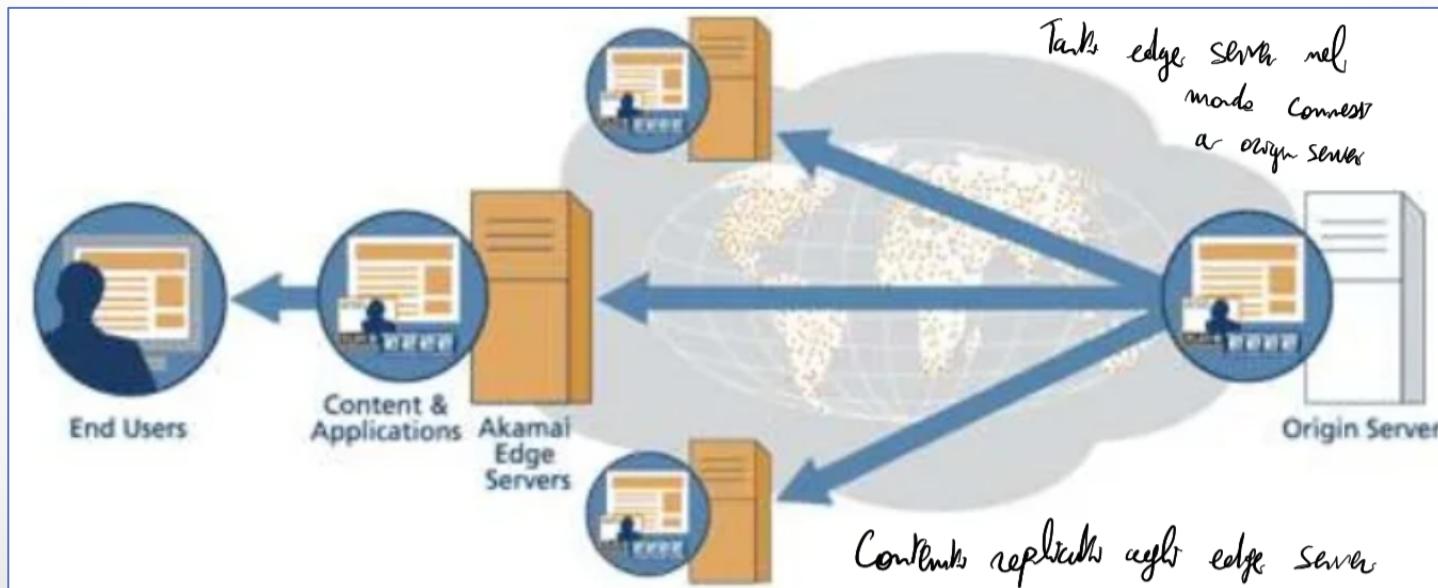
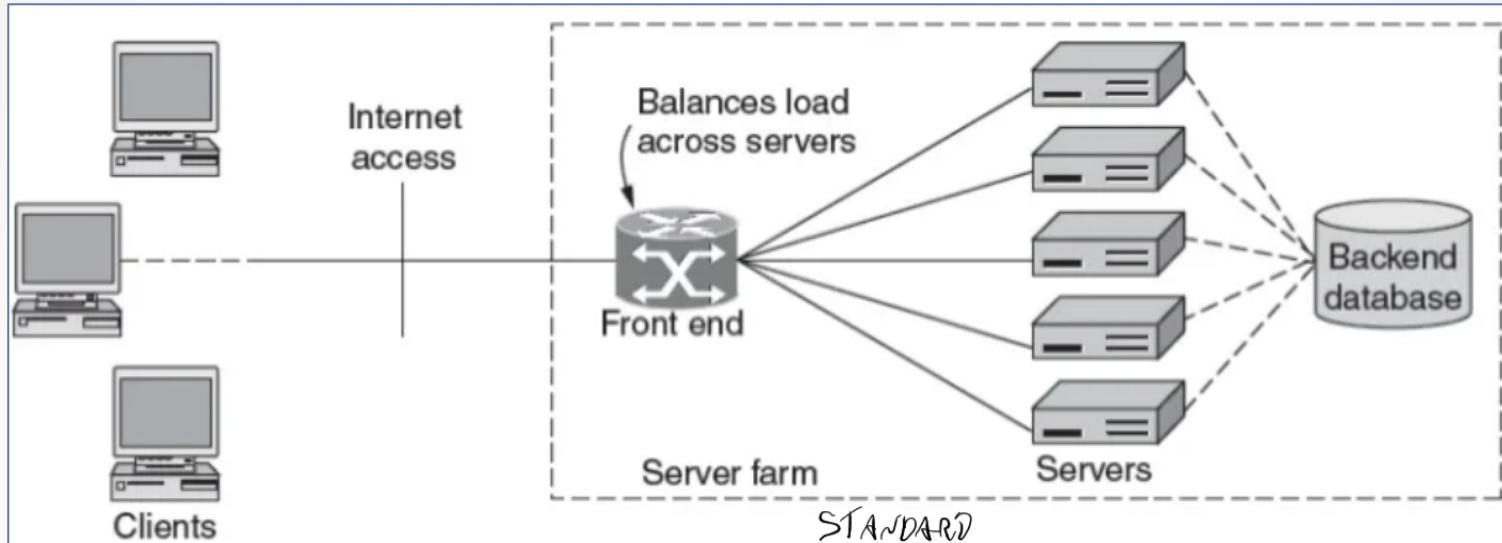
CDN

Problema: oggi molte aziende distribuiscono video on demand in streaming a milioni di utenti.

- L'approccio più diretto potrebbe essere costruire un unico enorme datacenter e memorizzare tutti i contenuti. Questo approccio presenta 3 grandi problemi:
 1. Distanza utente – data center -> riduzione throughput per colli di bottiglia (alta probabilità link lenti)
 2. Spreco banda (stessi contenuti a molti utenti sullo stesso collegamento) maggiori costi verso l'ISP → *Mando contenuti sullo stesso collegamento ↪ Molto probabile*
 3. Single point of failure

Per tale motivo quasi tutte le maggiori aziende di streaming usano le **CDN (Content Delivery Network)**

Sist. Convenzionale vs CDN



Soluzione: CDN

- Una Content Delivery Network è un'infrastruttura creata per distribuire efficacemente agli utenti di Internet i contenuti dei siti web più popolari
- Una CDN si basa sulla distribuzione di repliche dei contenuti dal server principale del “Content Provider” ad una molteplicità di server disposti sulla rete da un “Content Delivery Operator”
- La CDN può essere:
 - Privata: ovvero di proprietà del fornitore di contenuti (es Google)
 - Di terze parti: distribuisce contenuti per molti fornitori (Akamai, Limelight, level-3). Si presenta come un servizio a pagamento del quale usufruiscono i gestori dei siti web commerciali più popolari
- Si usa per qualsiasi contenuto che ha necessità di performance

CDN: politiche di dislocazione

La CDN adottano due politiche di dislocazione dei server:

Enter Deep e Bring Home

Rete che sfrutta i link del provider

- Enter deep (entrare in profondità): filosofia seguita da Akamai, entrare in profondità nelle reti di accesso degli ISP installando gruppi di server, detti anche cluster, negli ISP di accesso sparsi in tutto il mondo. Akamai distribuisce server in migliaia di posti diversi con l'obiettivo di essere «vicino» all'utente finale. Diminuendo il numero di collegamenti tra l'utente e il cluster CDN si ha una migliore percezione del ritardo e del throughput. Questo approccio altamente distribuito richiede però grandi sforzi per la manutenzione e gestione dei cluster

Cluster all'interno delle reti del provider
Lo posizionano strategicamente nella rete del provider

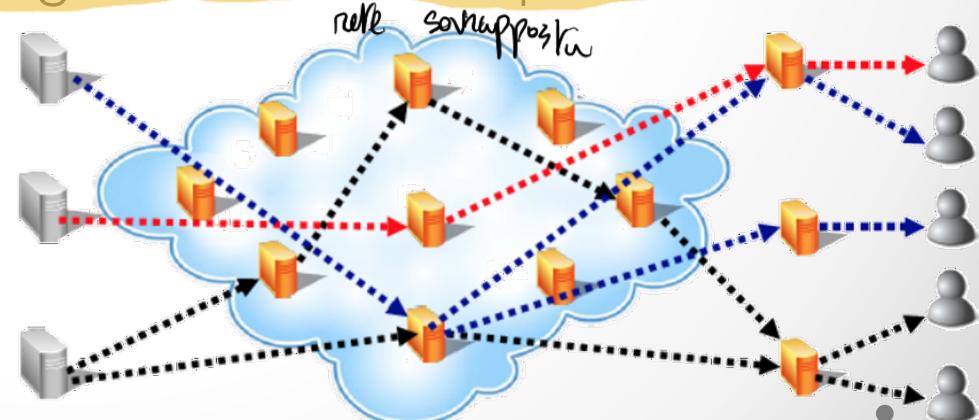
CDN: politiche di dislocazione

La CDN adottano due politiche di dislocazione dei server: Enter Deep e Bring Home

- Bring Home (portare a casa): seguito da Limelight e altri, ha come obiettivo portarsi in casa l'ISP costruendo grandi cluster in pochi punti chiave e interconnetterli con una rete privata ad alta velocità. Questo approccio presenta meno problemi di gestione e manutenzione ma spesso comporta una minore qualità del servizio. *Qaw s cluster sono estens.*

Soluzione: CDN

- Formata da una overlay network di edge server cooperativi
- Edge server distribuiti su una vasta area geografica per permettere la consegna dei contenuti da locazioni più vicine all'utente
- Content outsourcing: il content provider delega alla CDN il servizio del proprio contenuto (forniti dagli origin server)
- Gli edge server forniscono soltanto applicazioni/contenuti gestiti dalla CDN
- La CDN definisce un SLA con i suoi customer, impegnandosi a soddisfare determinati livelli di servizio
- Origin server - Insieme di server gestiti dal content provider



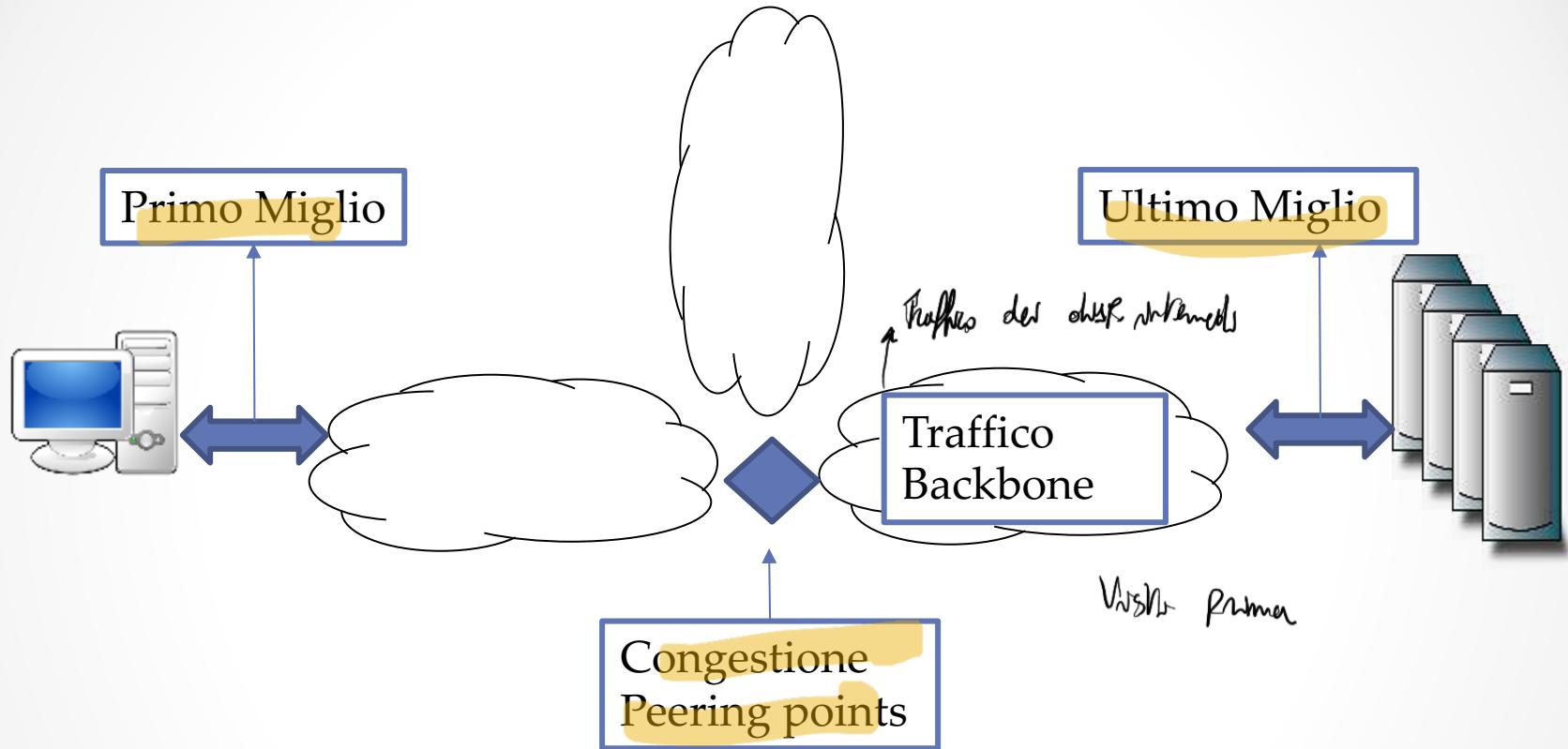
CDN o Web-cluster?

→ replica contenuti su N server e faew Load Balancing

- I Web cluster possono essere lontani dagli utenti e fallire a causa di congestioni di rete Edge server parla solo per loro
- L'application/content provider deve possedere l'infrastruttura di servizio (o affittarla da un data center o Cloud provider)
- Le CDN possono avere una migliore reattività a picchi di traffico improvvisi ed inattesi (flash crowd)

La scelta dipende anche dalla durata del servizio e dal tipo di applicazione

Limiti Approccio Centralizzato



Contenuti

- **Contenuti non streaming** - Contenuti statici, in particolare immagini - Contenuti volatili, dinamici (in modo parziale) - Contenuti con autenticazione - Contenuti sicuri
- **Contenuti streaming on-demand** – Contenuto digitalizzato e memorizzato come media file su media server (video-on-demand, clip musicali)
- **Contenuti streaming live** - Contenuto distribuito quasi istantaneamente come media file (eventi sportivi e musicali)

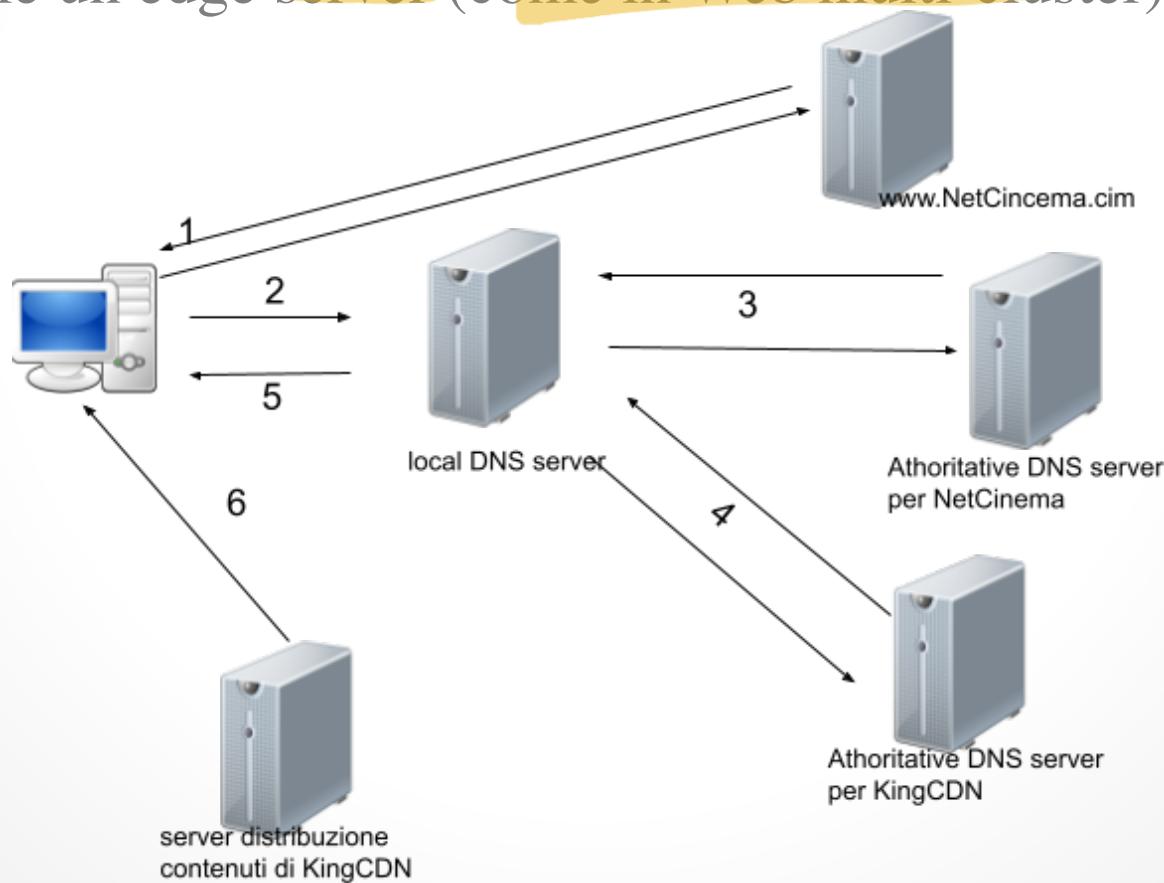
Meccanismi Request Routing

- Meccanismi più usati:
per direct all'edge server più vicino
 - Redirezione DNS
 - IP anycast (usato ad es. da CloudFlare, KeyCDN e CacheFly)
- Altri meccanismi
 - Redirezione mediante protocollo HTTP/RTSP
 - URL rewriting: riscrittura dell'hostname nell'URL con altro hostname
 - IP tunneling

Redirect DNS

Il DNS autoritativo del sito Web delega la risoluzione dell'hostname ad un DNS autoritativo gestito dalla CDN

Nell'effettuare il mapping da hostname ad indirizzo IP, il DNS della CDN sceglie un edge server (come in Web multi-cluster)



Redirect DNS

Osservazioni:

- Limitando il caching nei name server locali e intermedi, il DNS della CDN aumenta il controllo sul mapping tra hostname e indirizzo IP *Dal momento che cambiano velocemente. Non voglio dubbi falso.*
- Per evitare che il DNS autoritativo della CDN sia il collo di bottiglia, la CDN deve possedere un'infrastruttura DNS scalabile (es. Akamai)
- Ci sono comunque DNS server (locali e intermedi) non cooperativi (circa 17%), che violano il TTL stabilito dal DNS della CDN e continuano ad usare il mapping in cache sebbene scaduto *Sono passati almeno 24 ore da autorizzare a edge*

Redirect DNS

Due tipologie di CDN che usano la redirezione DNS:

Full-content delivery (o first hit at CDN)

L'origin server è nascosto a tutti, eccetto che alla CDN

Il DNS autoritativo dell'origin server delega le richieste di risoluzione al DNS server autoritativo della CDN (DNS outsourcing): resource record di tipo CNAME

Tutte le richieste di risorse arrivano agli edge server

Partial-content delivery (o first hit at origin)

L'origin server modifica nella pagina HTML l'URL delle risorse incluse nella pagina (immagini, video, audio, ...) applicando l'URL rewriting

Esempio: <http://www.foo.com/bar.gif> viene modificato in <http://cdn-foo.net/www.foo.com/bar.gif>

L'hostname nell'URL modificato è risolto in un indirizzo IP dal DNS server autoritativo della CDN

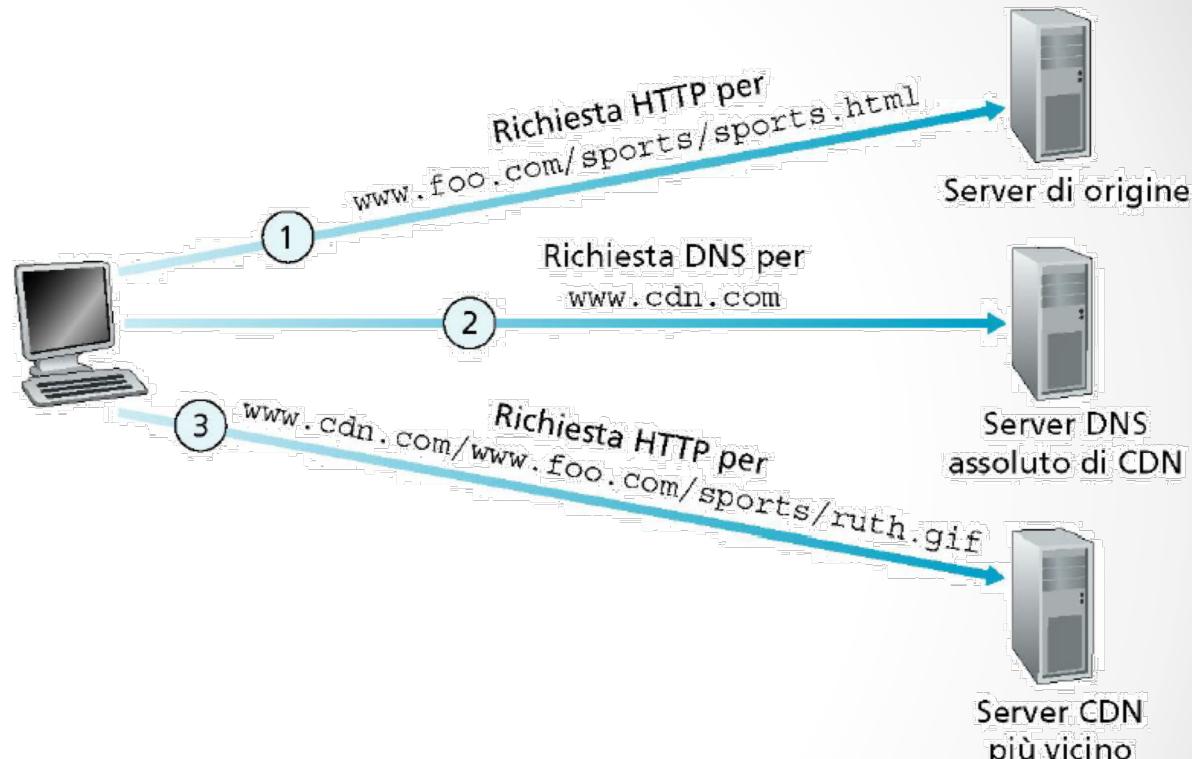
Prelievo da parte del Client

Dal server origine al nodo CDN: routing delle richieste

La CDN crea una mappa che indica le distanze tra i vari ISP e i nodi CDN

Quando arriva una query al DNS aut. si determina l'ISP che ha originato la query

Si usa la mappa per la scelta del server CDN più vicino



Akamai

- Azienda leader nel settore CDN, fondata nel 1998 da docenti e studenti del MIT
- Delivery del 15-30% del traffico Web (più di 30 Tbps)
- Akamai Intelligent Platform composta da oltre 240000 edge server localizzati in oltre 130 paesi e 1700 AS
- Un solo “network hop” dall’85% degli utenti di Internet (network hop = AS hop)
- Alcuni clienti di Akamai: Adobe, Apple, Fox Sports, Microsoft, NASA.gov, Sky, Salesforce

“When Akamai goes down, it takes the Internet with it”
- Possiede numerosi domini usati per il content delivery – akamai.net, akamaiedge.net, akadns.net, edgekey.net
- Usa la redirezione DNS, sia per full-content delivery sia per partial-content delivery

Akamai: redirezione DNS

- Nel caso di full-content e partial-content delivery – Il prefisso include un hostname, ad es. a799.g.akamai.net – Il prefisso a799 identifica il customer di Akamai
- La risoluzione dell'hostname nell'indirizzo IP di un edge server di Akamai è gestita dall'infrastruttura scalabile di name server che compongono il DNS autoritativo di Akamai

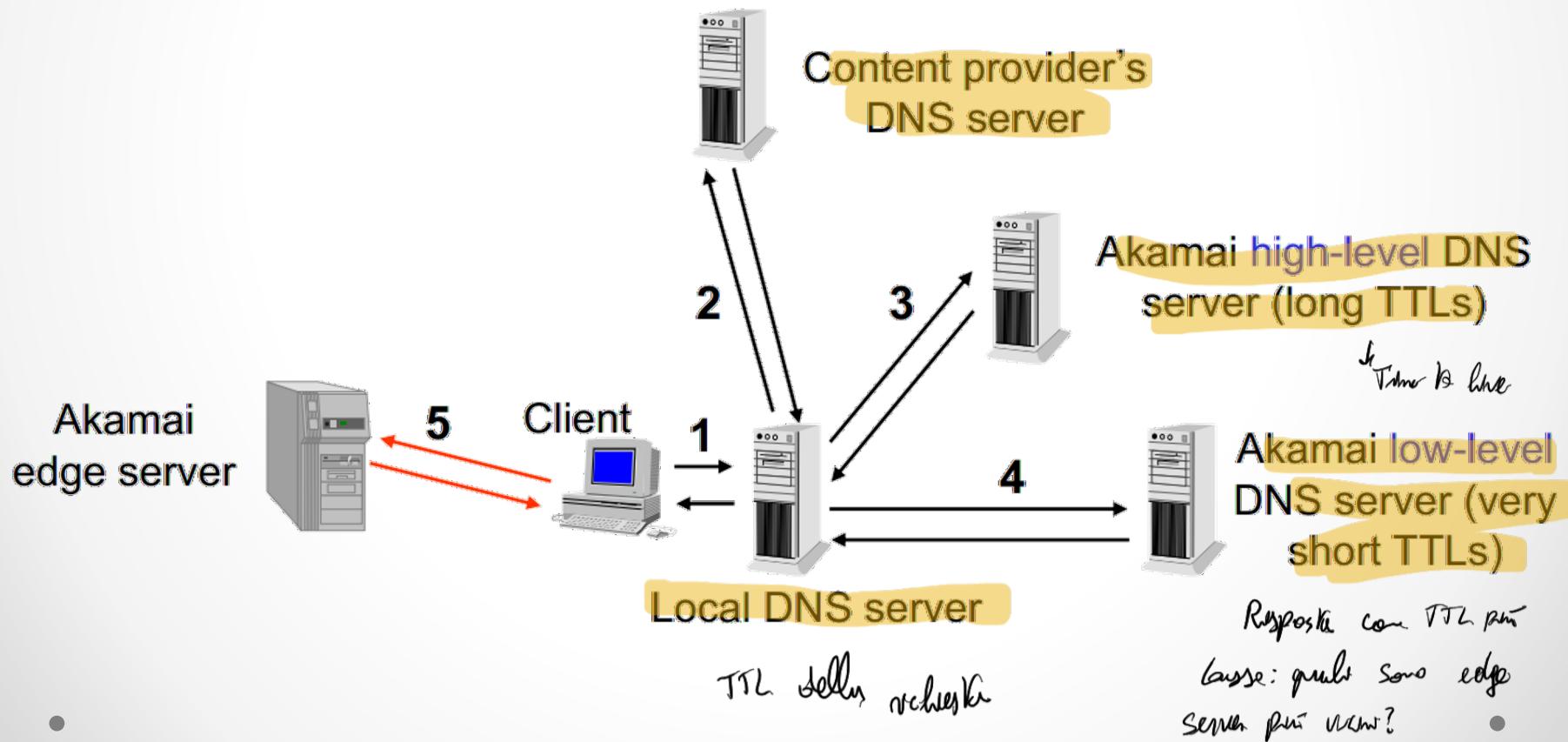
Come viene scelto l'edge server? Vicino al client e non sovraccarico

- Obiettivo: prestazioni e disponibilità
- Edge server: non singolo server fisico, ma cluster di server
- Algoritmo di selezione dell'edge server: combina informazioni su topologia di rete (tramite BGP), prossimità (numero di hop o round trip time) e carico degli edge server

Quanto step deve fare?

Akamai: redirezione DNS

Akamai utilizza una gerarchia di DNS server (almeno due livelli) per risolvere l'hostname nell'indirizzo IP di un edge server – Esempio di full-content delivery



Akamai: Esempio

- Il sito Web di Apple è gestito da Akamai
- Come trovarlo? Risolviamo www.apple.com usando dig – Nota i molteplici livelli dell'infrastruttura DNS vendibile di Akamai (record di risorse CNAME)

```
; <>> DiG 9.10.6 <>> www.apple.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50497
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;www.apple.com.           IN      A
;;
;; ANSWER SECTION:
www.apple.com.        311     IN      CNAME   www.apple.com.edgekey.net.
www.apple.com.edgekey.net. 18158 IN      CNAME   www.apple.com.edgekey.net.globalredir.akadns.net.
www.apple.com.edgekey.net.globalredir.akadns.net. 2985 IN CNAME e6858.dscx.akamaiedge.net.
e6858.dscx.akamaiedge.net. 5      IN      A       2.22.33.2
;;
;; Query time: 11 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Oct 11 01:56:00 CEST 2022
;; MSG SIZE  rcvd: 192

```

iMac-di-iMac:~ imac\$