DNS

(con speciale attenzione all'implementazione DNS di Microsoft)

Concetti Generali (1)

- Risoluzione dei Nomi in Indirizzi e viceversa
- Gestione gerarchica del sistema di denominazione dei computer
- Database distribuito della mappatura dei nomi
- Nato nei primi anni di Internet – (BIND Berkeley Internet Name Domain)
- File Hosts (statico) vs DNS (dinamico)

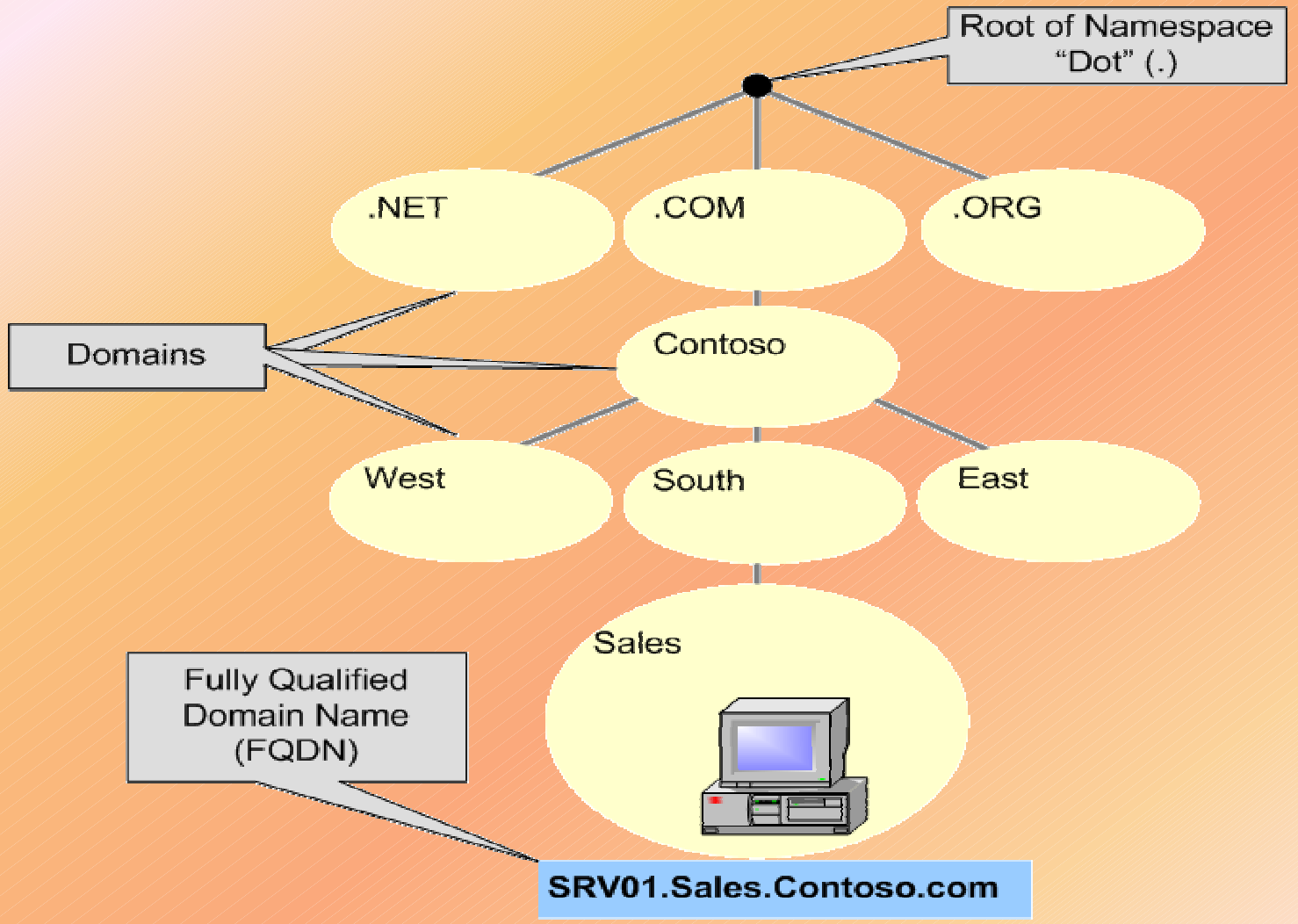
Concetti Generali (2)

- Host – un apparato di rete che utilizzi il protocollo TCP/IP e a cui sia assegnato un indirizzo IP (es. 147.90.10.12)
- Nome Host – un nome facilmente memorizzabile con cui riferirsi ad un host, in modo da non costringere l'utente o il client a ricordare direttamente l'indirizzo IP
  - Es. dc01.sales.contoso.com
    - dc01 → nome host
    - sales.contoso.com → nome dominio
- Risoluzione – traduzione del nome in indirizzo
- Dominio – partizione dell'intero *Domain Name Space,* inteso come albero gerarchico che si estende da una radice (root) verso i rami e i sotto-rami

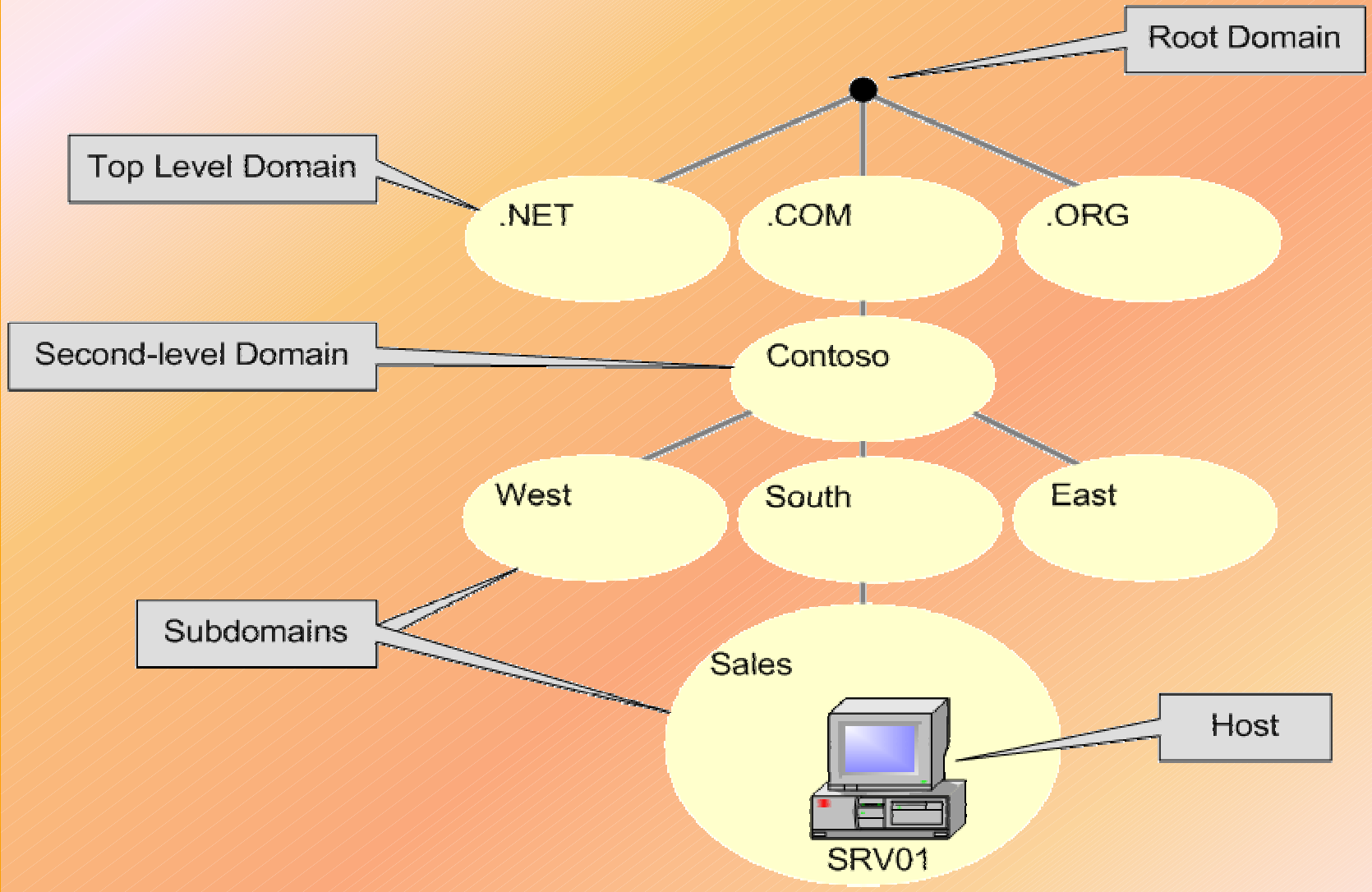
Concetti Generali (3)

- Server DNS
  - computer su cui è in esecuzione il servizio DNS
  - gestisce il *namespace* o una parte di esso
  - Hh autorità (*authoritative*) su uno specifico *namespace* o dominio
  - soddisfa le richieste di risoluzione inoltrate dal client Dns (resolver)
- FQDN (Fully Qualified Domain Name)
  - Combinazione del nome host e del nome di dominio che fornisce un completo riferimento relativo alla radice dell'albero gerarchico
    - Es. srv01.sales.south.newcomp.com
- Convenzioni di Denominazione
  - Set di caratteri accettati
    - A-Z. a-z, 0-9
    - - (trattino)
    - _ (underscore) → carattere riservato

Domain Name Space



Namespace (con Domini)

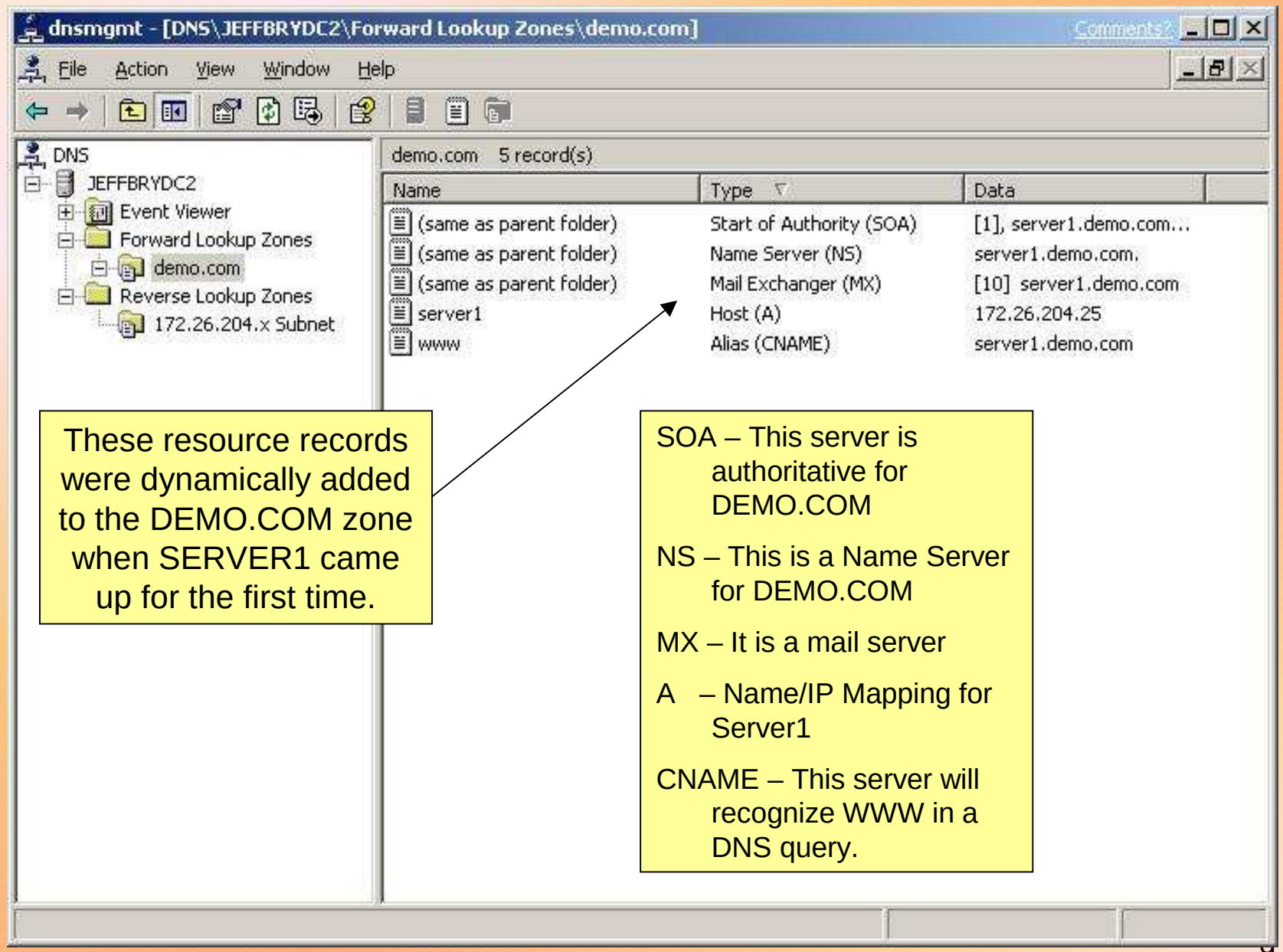


Concetti Generali (4)

- Zona – porzione del database DNS, o più dettagliatamente collezione di mappature nome/indirizzo per gli host appartenenti a porzioni **contigue** del *namespace*
  - Es. *support.contoso.com* non è contiguo a *marketing.contoso.com*, ma lo è rispetto a *partners.support.contoso.com*
- I dati della Zona sono conservati sul DNS server
- Un server è *authoritative* su una zona, se può risolvere nomi ed indirizzi richiesti dai *resolver*
- Di solito, una Zona corrisponde ad un dominio, ad un sotto-dominio o ad una serie contigua di domini e sotto-domini

Concetti Generali (5)

- Come tutti i database, anche il DNS è composto di tabelle e records
- RR (Resource Records) – voci del database DNS che specificano una particolare relazione di risoluzione
- Tipi di Records
  - A (Host)
    - Risolve un nome host in un indirizzo IP (forward lookup)
    - **Example:** Computer5.Microsoft.com -> 10.1.1.5
  - PTR (Pointer)
    - Risolve un indirizzo IP in un nome host (reverse lookup)
    - **Example:** 10.1.1.101 -> Computer1.Microsoft.com
  - NS (NameServer)
    - Identifica un nome host come server DNS per una certa Zona
    - **Example:** Microsoft.com -> NS2.Microsoft.com
  - SOA (Start of Authority)
    - Identifica il server DNS primario con *authority* su una certa Zona
    - **Example:** Microsoft.com -> NS1.Microsoft.com
  - SRV (Service Record)
    - Indica la disponibilità di un certo servizio su un certo host
    - **Example:** _TCP._LDAP.Microsoft.com -> DC01.Microsoft.com
  - CNAME (Alias)
    - Pone in relazione un nome ben noto (WWW) con un certo host
    - **Example:** www.Microsoft.com -> webserver12.Microsoft.com
  - MX (Mail Exchanger)
    - Identifica i server postali
    - **Example:** mail.Microsoft.com -> 10.1.1.8.


dnsmgmt - [DNS\JEFFBRYDC2\Forward Lookup Zones\demo.com]
File Action View Window Help
DNS
JEFFBRYDC2
Event Viewer
Forward Lookup Zones
demo.com
Reverse Lookup Zones
172.26.204.x Subnet
demo.com 5 record(s)
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[1], server1.demo.com...
(same as parent folder)
Name Server (NS)
server1.demo.com.
(same as parent folder)
Mail Exchanger (MX)
[10] server1.demo.com
server1
Host (A)
172.26.204.25
www
Alias (CNAME)
server1.demo.com
These resource records were dynamically added to the DEMO.COM zone when SERVER1 came up for the first time.
SOA – This server is authoritative for DEMO.COM
NS – This is a Name Server for DEMO.COM
MX – It is a mail server
A – Name/IP Mapping for Server1
CNAME – This server will recognize WWW in a DNS query.

Concetti Generali (6)

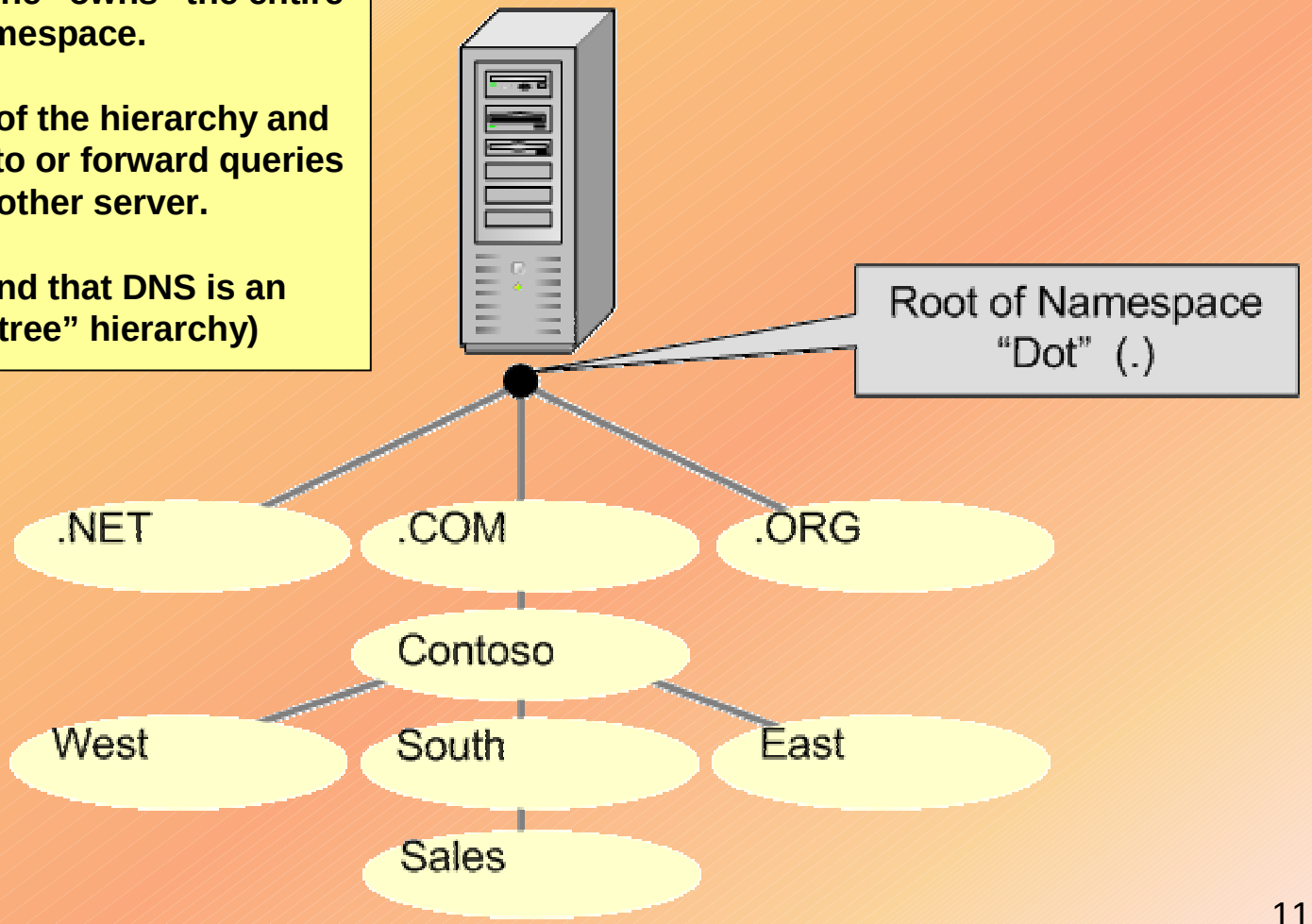
- Forward Lookup Zone
  - Risolve nomi in indirizzi
- Reverse Lookup Zone
  - Risolve indirizzi in nomi
- AD (Active Directory) Integrated Zone
  - Conservata nel database di AD
  - Sicurezza tramite ACL (Access Control List)
  - Possibili sia con *forward zones* che *reverse zones*
  - Supporto agli aggiornamenti dinamici (Dynamic Dns)
  - Modello di replica multi-master (FRS di Active Directory)
- Standard Primary Zone
  - Conservata in un file di testo sul *file system* del server DNS primario
    - \%systemroot%\system32\dns***domain***.dns
  - Ogni Zona DNS ha una sola copia di Primary Zone
  - Solitamente creata ed amministrata dall'amministratore
  - Aggoirnamenti dinamici delle Zone (Win2k o Win2k3)
- Standard Secondary Zone
  - Conservata su un server DNS secondario
    - \%systemroot%\system32\dns***domain***.dns
  - Copia in sola lettura (non può scrivere sul database)
  - Riceve gli aggiornamenti dal server DNS primario (Zone Transfer)

Root Zone

This DNS server that is authoritative for the Root Zone "owns" the entire namespace.

It is the "top" of the hierarchy and does not refer to or forward queries to any other server.

(Keep in mind that DNS is an "inverted tree" hierarchy)



Concetti Generali (7)

- Delegation
  - Processo di assegnazione dell' *authority* su una porzione del *namespace* DNS ad un'altra entità amministrativa
  - Aggiunge due records al database
    - "Glue" Record - un A record che funge da raccordo tra le due porzioni
    - Delegation Record – un NS Record che identifica la zona delegata ed il Name Server con authority su di essa
  - Il NS *authoritative* per la Zona parent restituisce un *referral* al *resolver* con l'indirizzo del NS *authoritative* per la Zona *delegated child*

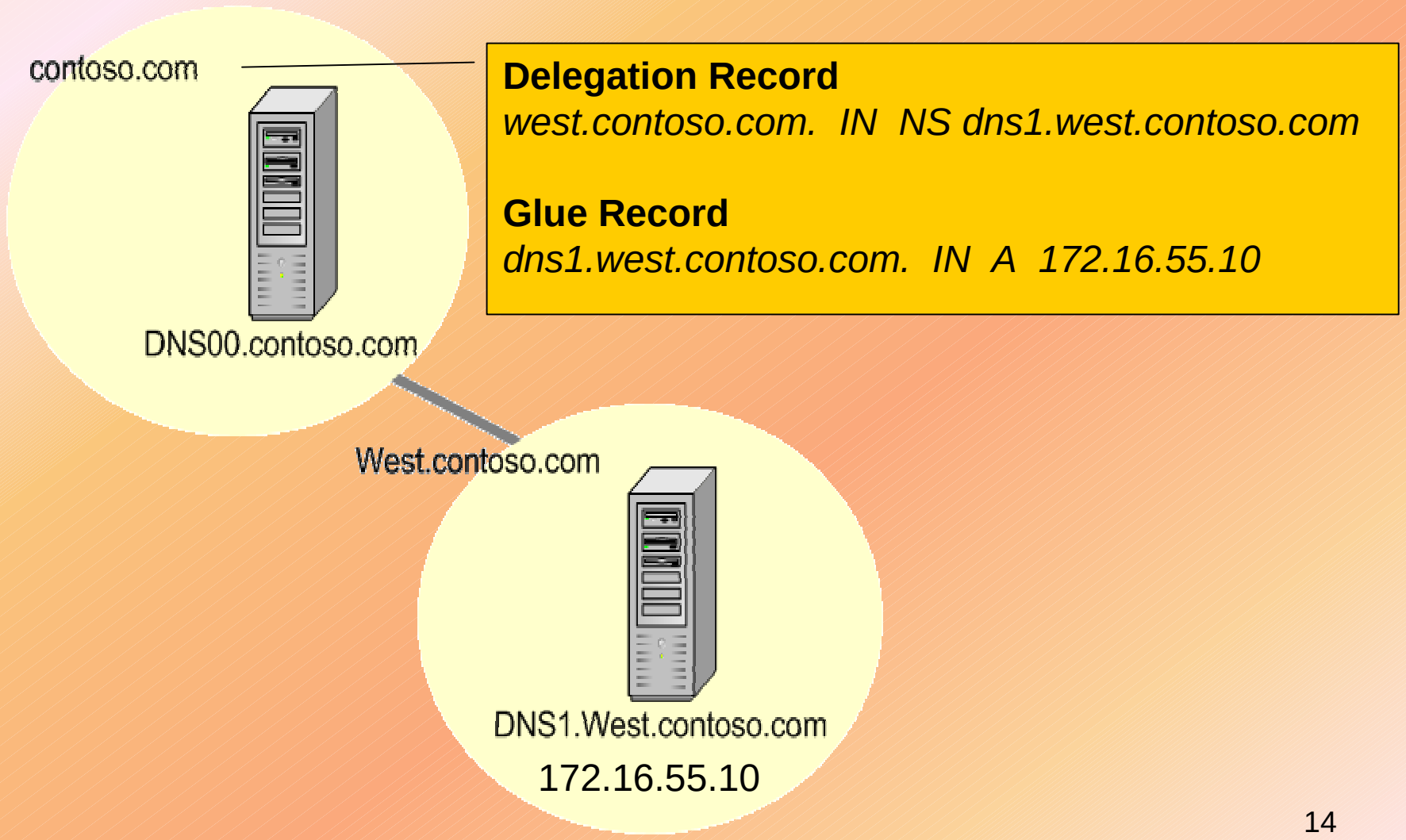
Delegation – Esempio (1)

Spazio delegato di west.contoso.com da parte del dominio *parent* contoso.com

West.Contoso.Com ha un'amministrazione separata ed è *authoritative* su una propria Zona

I record di *delegation* consentono al NS di contoso.com di localizzare il Name Server della zona delegata per le risoluzioni per le quali quest'ultimo ha *authority*

Delegation – Esempio (2)



Delegation Record

west.contoso.com. IN NS dns1.west.contoso.com

Glue Record

dns1.west.contoso.com. IN A 172.16.55.10

Concetti Generali (8)

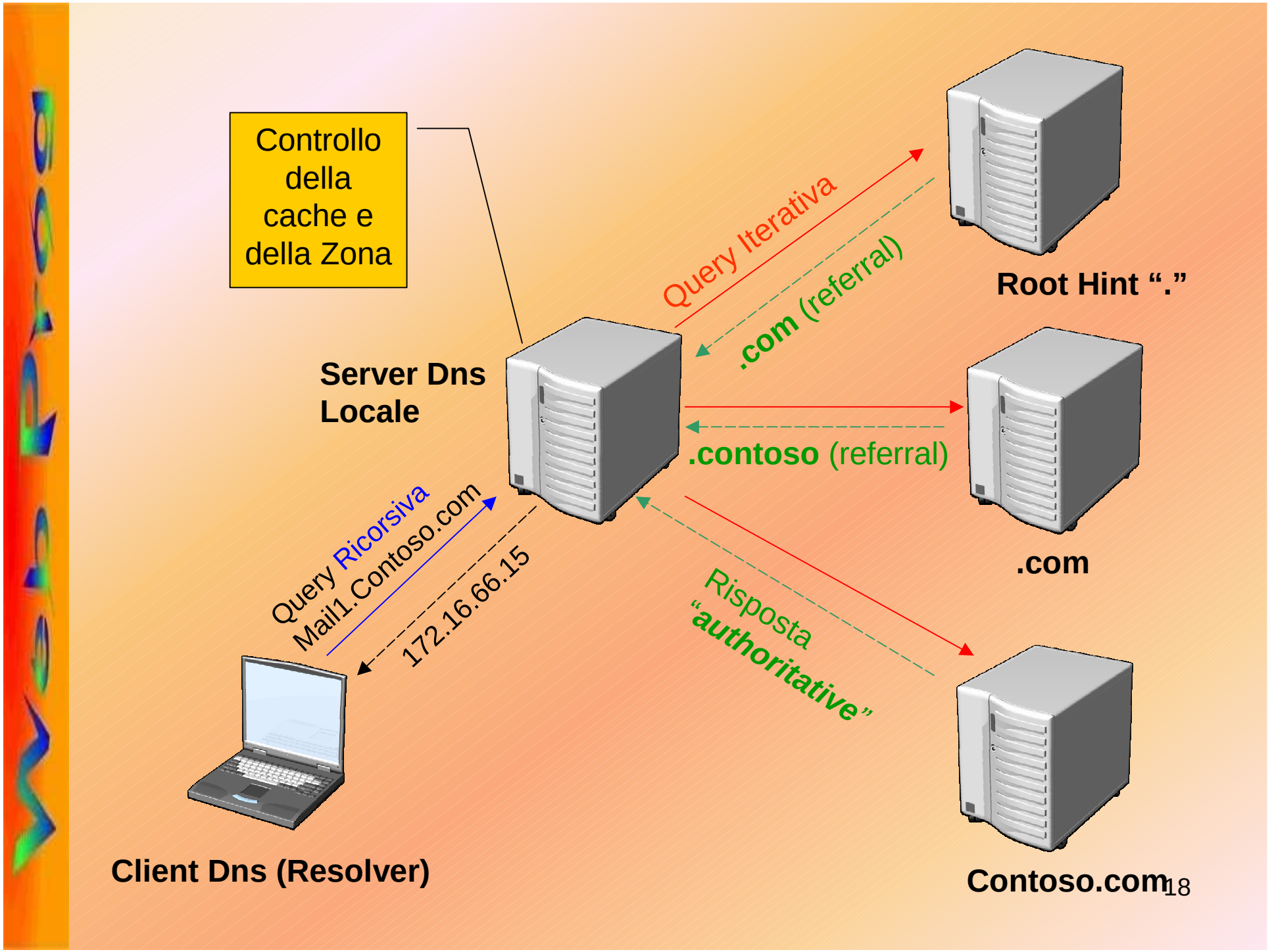
- Hosts File
  - File di testo mantenuto localmente sull' host e contenente mappature statiche tra nomi ed indirizzi
  - Utilizzabile in alternativa o in combinazione col DNS
  - Soggetto ad errori di risoluzione
    - Corrispondenze scadute dal punto di vista temporale
    - Corrispondenze non esatte o inesistenti
  - Posizionato nel seguente percorso %systemroot%\system32\drivers\etc\

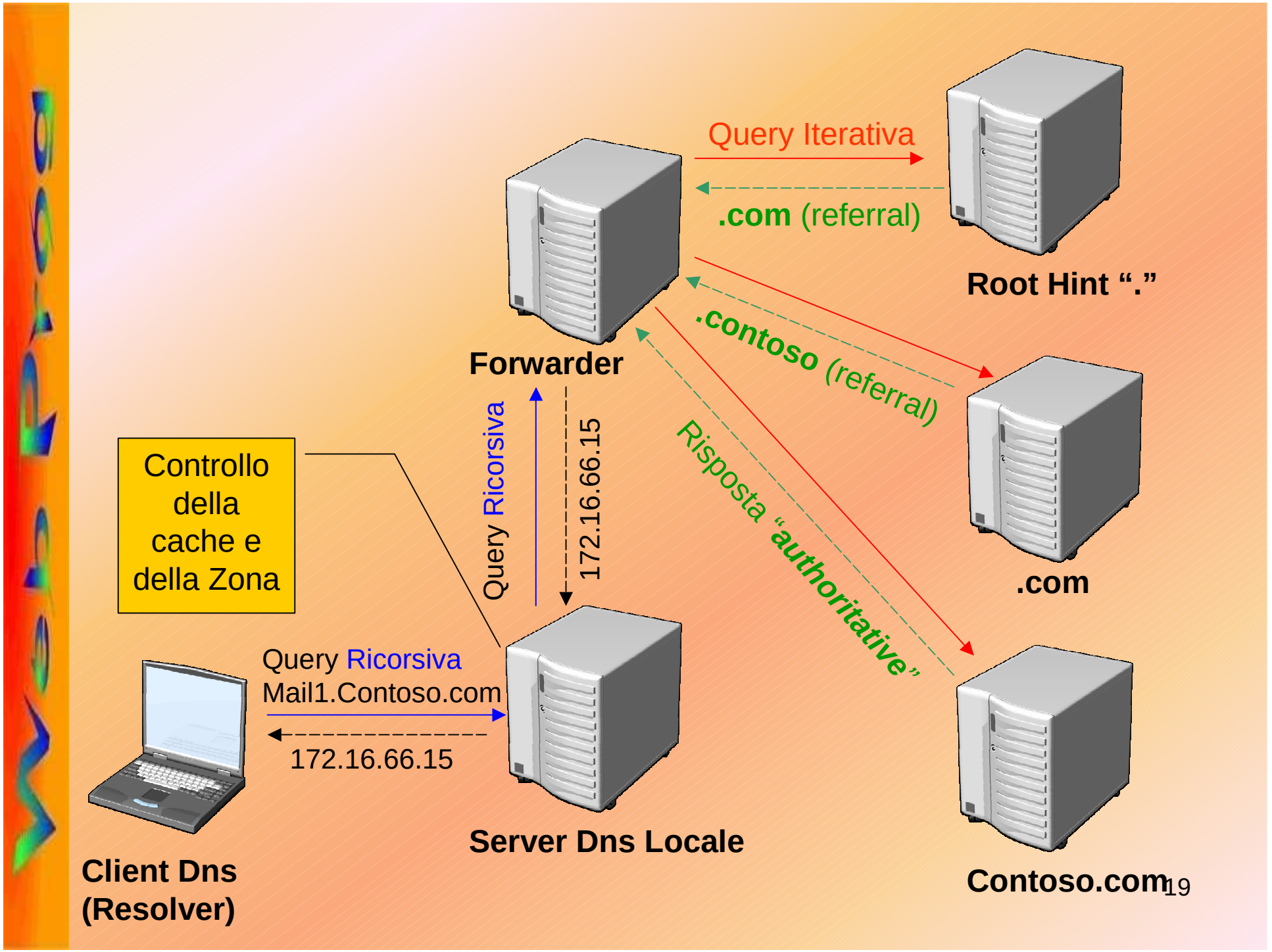
Query (1)

- Richiesta di risoluzione rivolta ad un Name Server
- Sia i client Dns che i server Dns possono rivolgere una query ad un Name Server
- Il Name Server interrogato controlla
  - la propria cache Dns
  - L'eventuale *authority* sul nome da risolvere
    - Se non è *authoritative* per la risoluzione, si rivolge a
      - Forwarders
        - » Gestiscono le query non locali
        - » **Modalità Esclusiva** – in caso di mancata risoluzione da parte del forwarder, il server DNS si rivolge ai Root Hints secondo la procedura iterativa
        - » **Modalità Non-Esclusiva** - in caso di mancata risoluzione da parte del forwarder, non si procede oltre
      - Root Hints o Cache Hints (Name Server di livello *root*)
        - » Usato da DNS locali o da Forwarders per raggiungere Name Servers esterni al *namespace* locale partendo dal *namespace* radice
        - » Se non è richiesta la risoluzione del *namespace* esterno, è possibile sostituire i *root hints* di default con altri che puntino ai Root NS del *namespace* interno
        - » Sui sistemi Microsoft il file che contiene la lista dei root hints si chiama **cache.dns** (%systemroot%\system32\drivers\etc\)
        - » Sui sistemi Unix il file che contiene la lista dei root hints si chiama **db.cache**

Query (2)

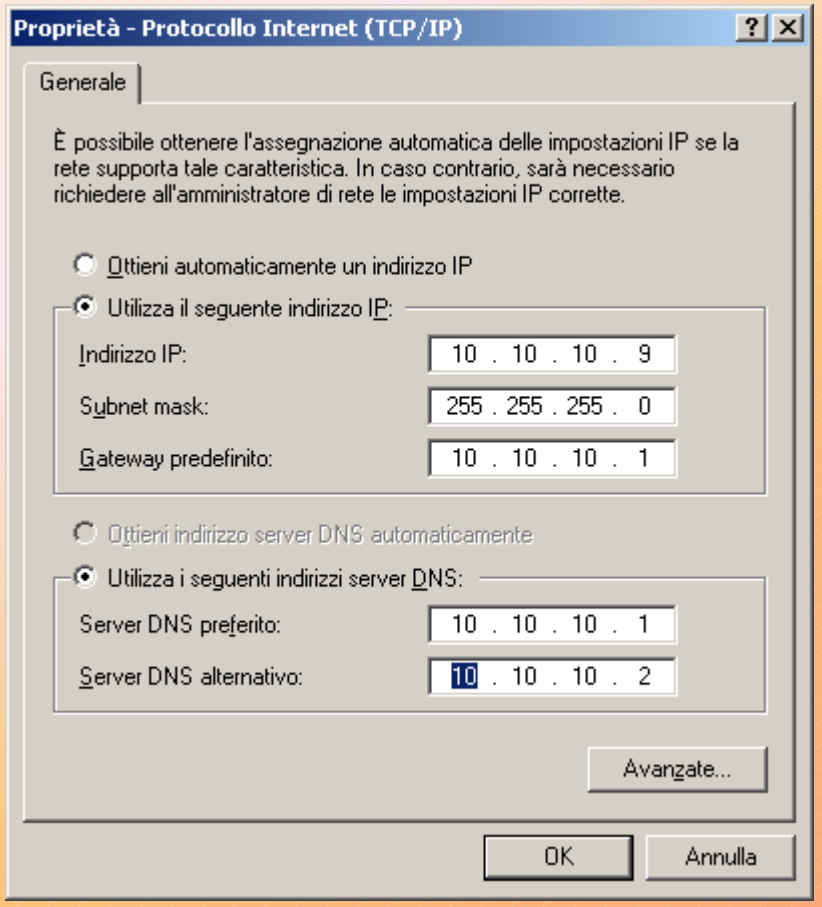
- Query Ricorsiva
  - Il Name Server interrogato deve rispondere direttamente al resolver restituendogli
    - una risoluzione
    - una risposta negativa
    - in nessun caso un riferimento ad altro Name Server (*referral*)
  - Per fare questo, il Name Server può interrogare altri Name Server alla ricerca di riferimenti (*referral*) per il Server authoritative rispetto alla risoluzione richiesta dal resolver
  - Il Name Server che inoltra le richieste ad un Forwarder utilizza la *recursion,* ovvero si comportano nei confronti di questo, come dei client Dns
- Query Iterativa
  - Usata generalmente dai Name Server per interrogare altri Name Server durante il processo di risoluzione di una richiesta proveniente da un resolver. La risposta ad una query iterativa puiò essere
    - L'indirizzo ricercato
    - Una risposta negativa authoritative
    - Un referral

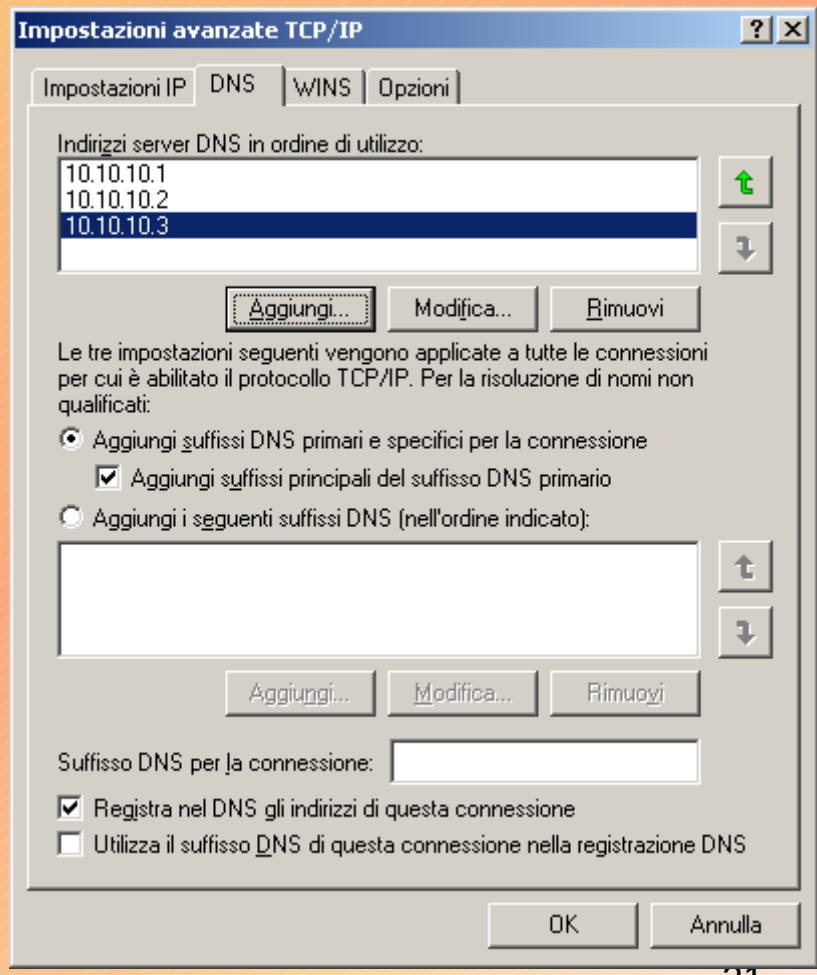

Controllo della cache e della Zona
Server Dns Locale
Query Iterativa
.com (referral)
Root Hint "."
.contoso (referral)
.com
Query Ricorsiva Mail1.Contoso.com
172.16.66.15
Risposta "authoritative"
Client Dns (Resolver)
Contoso.com


Query Iterativa
.com (referral)
Root Hint "."
Forwarder
.contoso (referral)
Risposta "authoritative"
Query Ricorsiva
172.16.66.15
.com
Controllo della cache e della Zona
Query Ricorsiva
Mail1.Contoso.com
172.16.66.15
Server Dns Locale
Client Dns (Resolver)
Contoso.com

Query (3)

- Durante il processo di risoluzione, il resolver segue la seguente procedura:
  - Controlla la cache locale
  - Se la cache non fornisce la risoluzione richiesta, interroga i server Dns elencati nelle Proprietà del TCP/IP per ogni NIC (Network Interface Card) disponibile

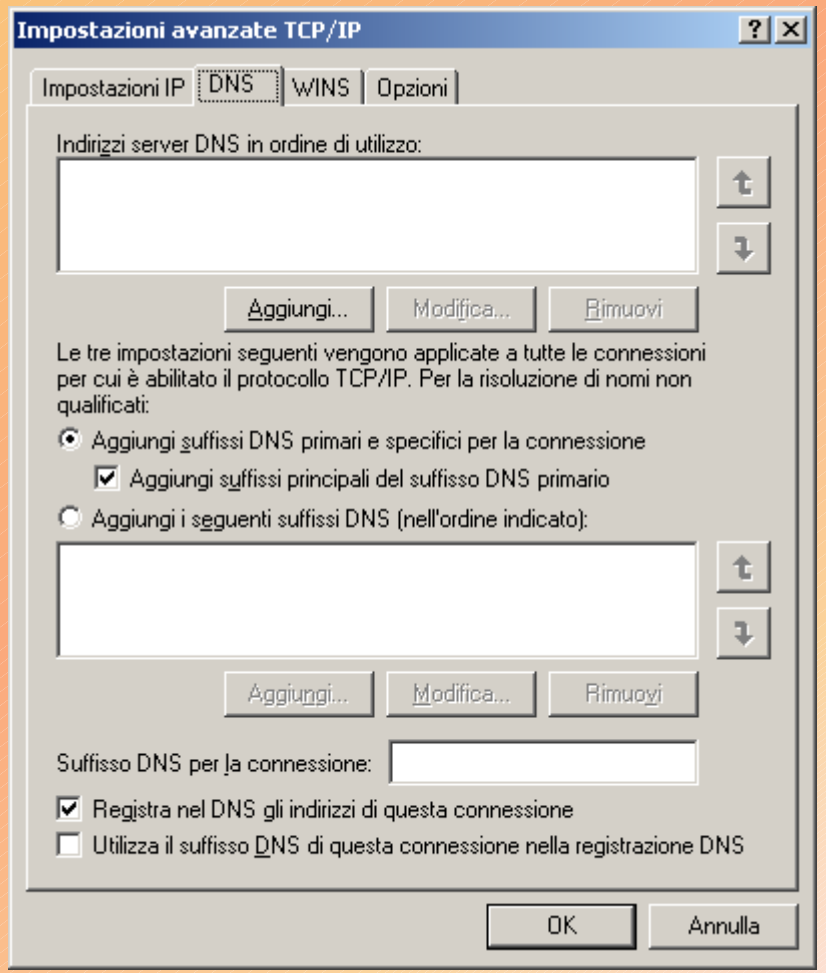

Proprietà - Protocollo Internet (TCP/IP)
Generale
È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.
Ottieni automaticamente un indirizzo IP
Utilizza il seguente indirizzo IP:
Indirizzo IP: 10 . 10 . 10 . 9
Subnet mask: 255 . 255 . 255 . 0
Gateway predefinito: 10 . 10 . 10 . 1
Ottieni indirizzo server DNS automaticamente
Utilizza i seguenti indirizzi server DNS:
Server DNS preferito: 10 . 10 . 10 . 1
Server DNS alternativo: 10 . 10 . 10 . 2
Avanzate...
OK
Annulla


Impostazioni avanzate TCP/IP
Impostazioni IP
DNS
WINS
Opzioni
Indirizzi server DNS in ordine di utilizzo:
10.10.10.1
10.10.10.2
10.10.10.3
Aggiungi...
Modifica...
Rimuovi
Le tre impostazioni seguenti vengono applicate a tutte le connessioni per cui è abilitato il protocollo TCP/IP. Per la risoluzione di nomi non qualificati:
Aggiungi suffissi DNS primari e specifici per la connessione
Aggiungi suffissi principali del suffisso DNS primario
Aggiungi i seguenti suffissi DNS (nell'ordine indicato):
Aggiungi...
Modifica...
Rimuovi
Suffisso DNS per la connessione:
Registra nel DNS gli indirizzi di questa connessione
Utilizza il suffisso DNS di questa connessione nella registrazione DNS
OK
Annulla

I Suffissi DNS (1)

- Esiste la possibilià di specificare i suffissi che verranno utilizzati nel caso di una richiesta di risoluzione "*non qualificata*"
  - Suffissi DNS Primari
  - Suffissi DNS per Connessione

    o in alternativa
  - Suffissi DNS elencati in una Lista

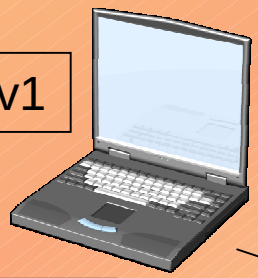


I Suffissi DNS (2)

- FQDN (Fully Qualified Domain Name)
  - srv1.sales.contoso.com**.**
  - Notare il punto finale !!!
    - Il resolver utilizza il FQDN
- Unqualified Multi-label Name
  - srv1.sales.contoso.com
  - Notare l'assenza del punto finale !!!
    - Il resolver aggiunge il punto finale ed usa il nome
- Single-label Unqualified Name
  - Srv1
  - Assenza del suffisso di dominio
  - Assenza delle informazioni che qualifichino il nome indicandone l'appartenenza ad uno specifico *namespace*
    - Il resolver aggiunge i suffissi specificati, aggiunge il punto

I Suffissi DNS (3)

- Il resolver prova tutti i suffissi specificati (Primario e per Connessione oppure elencati nella Lista)
- Nel caso tutti i suffissi falliscano nel fornire una risoluzione, il resolver
  - Aggiunge alla nome proposto, il *Primary Domain Name* impostato per il computer (Pannello di Conrollo/Sistema)
  - Risale il nome ottenuto di nodo in nodo e da sinistra verso destra



Nome Richiesto = srv1

Dominio Primario = south.sales.contoso.com

srv1.south.sales.contoso.com

srv1.sales.contoso.com

srv1.contoso.com

Cache – Server DNS

- Il server Dns pone in una cache le risoluzioni effettuate, memorizzando
  - I nomi host risolti tramite iterazione
  - I Name Server con *authority* su altri domini
- Ottimizzazione del tempo di risposta per le risoluzioni future
- TTL (Time-To-Live) – periodo di tempo per cui le risoluzioni avvenute rimangono in cache
- *Negative Caching* – riduce il tempo di risposta per risoluzioni successive di un host che si è rivelato
  - Non valido
  - Inesistente

Cache – Client DNS

- Anche il client Dns, memorizza le risoluzioni avvenute in una cache, che controlla successivamente prima di contattare i Name Server (valido anche per il N*egative Caching*)
- Il file *Hosts*, viene precaricato nella cache Dns del client
- TTL (Time-To-Live) – periodo di validità della cache<

Server DNS (Only Caching)

- Configurati solo per interrogare e memorizzare in cache
- Non hanno *authority* su alcun Dominio
- Nessun file di Zona, ma solo dati in cache
- I sistemi Microsoft individuano come *Only Caching Servers,* i DNS Servers per cui non è stata configurata nessuna Zona
- Usano i Root HInts per interrogazioni esterne

Server DNS – Funzioni

- I Server Dns possono essere configurati con varie tipologie di Zona
  - Standard Primary
    - *Authoritative* sulla propria zona
    - Ospita la copia *master* (in scrittura) del file di Zona
    - L'implementazione di Microsoft supporta gli aggiornamenti dinamici dei file di Zona
  - Standard Secondary
    - Riceve i dati di Zona ed i relativi aggiornamenti dal Name Server (Master Server) con autorità sulla Zona in questione (Zone Transfer)
    - A sua volta può agire da Master Server per un altro Secondary
  - Active Directory Integrated (solo Domini Microsoft)
    - I dati di Zona sono conservati nel database di Active Directory (i Domain Controllers divengono i NS *authoritative* per le Zone)
    - File Master di Zona replicati in più copie
    - La replica dei file di Zona segue la replica di Active Directory (modello multi-master)
    - Collisioni nella replica (modifiche simultanee o quasi su diversi Domain Controllers)
      - risolte confrontando le versioni ed il timestamp delle modifiche Active Directory
  - Caching Only (nessuna Zona)
    - Configurati solo per interrogare e memorizzare in cache
    - Non hanno *authority* su alcun Dominio
    - Nessun file di Zona, ma solo dati in cache
    - I sistemi Microsoft individuano come *Only Caching Servers,* i DNS Servers per cui non è stata configurata nessuna Zona
    - Usano i Root HInts per interrogazioni esterne

Zone Transfer

- Trasferimento dei record del database Dns ad un Secondary Name Server all'interno di una Zona
- Metodologia di funzionamento basata sul principio del *notify-and-pull*
  - il Primary avverte delle eventuali modifiche i Secondary presenti nella *notify list*
  - il Secondary avvertito esplicita la richiesta di trasferimento, solo se il dato notificato è più aggiornato di quello attuale
    - Viene controllato il Serial Number presente nel record SOA
    - Tale Serial Number è increntato dal Primary ad ogni aggiornamento dei dati
- Due tipologie
  - Full Zone Transfer (AXFR)
  - Incremental Zone Transfer (IXFR)
- Tre parametri presenti nel SOA sono determinanti
  - Refresh → periodo che il Secondary attende prima di richiedere un trasferimento
  - Retry → periodo durante il quale il Secondary ritenta la richiesta di trasferimento, nel caso in cui il Master non risponda
  - Expire → periodo trascorso il quale il Secondary rimuove i dati dalla Zona, in quanto non più aggiornati

Round Robin (1)

- Si utilizza un algoritmo Round Robin quando ci sono più Record per uno stesso nome (differenti IP ma un solo hostname)
  - Può essere una scelta dovuta a necessità di ridondanza o di *load-balancing*
  - Il NS risponde ruotando l'ordine dei record A
- Esempio

srv1.contoso.com.	IN	A	172.16.64.15
srv1.contoso.com.	IN	A	172.16.64.25
srv1.contoso.com.	IN	A	172.16.64.35

  - Il primo client richiede la risoluzione per srv1.contoso.com ed ottiene in risposta 172.16.64.15
  - Il secondo client richiede la risoluzione per srv1.contoso.com ed ottiene in risposta 172.16.64.25
  - Il terzo client richiede la risoluzione per srv1.contoso.com ed ottiene in risposta 172.16.64.35
  - Il successivo client richiede la risoluzione per srv1.contoso.com ed ottiene in risposta 172.16.64.15, ovvero il primo record A in ordine di rotazione

Round Robin (2)

- Subnet Prioritization
  - L'ordine delle risoluzioni fornite in risposta si basa sull'appartenza di subnet del resolver
- Esempio

client1.contoso.com.	IN	A	10.4.3.2
srv1.contoso.com.	IN	A	192.168.1.27
srv1.contoso.com.	IN	A	10.0.0.14
srv1.contoso.com.	IN	A	172.16.20.4

  - Il client richiede la risoluzione per srv1.contoso.com
  - Il NS verifica la subnet del richiedente
    - Se una delle possibili risoluzioni presenta la medesima subnet del resolver viene posta in cima all'ordine di risposta
      - Nel nostro caso client1.contoso.com = 10.4.3.2 / 8 quindi la risoluzione prioritaria (la prima fornita in risposta) sarà srv1.contoso.com = 10.0.0.14
    - Altrimenti, la lista non subiisce nessun riordino

DDNS - Intro

- Il DDNS (Dynamic DNS)
  - Definito nel RFC 2136
  - Una delle componenti fondamentali del DNS implementato da Microsoft
  - Si occupa della registrazione e dell'aggiornamento dei RR
  - Esistono diversi scenari di aggiornamento che dipendono principalmente dal tipo di client e server dhcp e dal modello di assegnazione dello spazio di indirizzamento IP
  - I RR interessati dal DDNS sono:
    - A e PTR
      - DHCP client (Win2k o superiore)
      - DHCP Server (per i legacy client)
    - SRV (solo per i Domain Controllers)
      - Servizio Netlogon
  - I RR vengono registrati nella zona corrispondente al "Suffisso DNS Primario"

DDNS – Client

- Client configurato in modo statico
  - Necessita sia avviato il servizio DHCP Client
  - Registra A e PTR ad ogni
    - Avvio
    - Cambio di indirizzo IP
    - Cambio di nome-dominio associato ad una particolare connessione (vedi Proprietà Avanzate del TCP/IP sotto la scheda DNS)
- Client DHCP di tipo legacy
  - Non sono in grado di gestire autonomamente l'aggiornamento dei RR
  - Il processo viene quindi controllato dal DHCP Server
    - Il client DHCP ottiene un lease DHCP
    - Il server DCHP genera il FQDN per il client (nome client + nome dominio)
    - Il server DHCP aggiorna i record A e PTR comunicandoli al server DNS
- Client DHCP Win2k o superiore
  - Il processo è gestitio in modo combinato da client e server DHCP
    - Il client DHCP ottiene un lease DHCP
    - Il server DHCP aggiorna il record PTR comunicandolo al server DNS
    - Il client DHCP aggiorna il record A comunicandolo al server DNS (opzione 81 della DHCPRequest)
- Client RAS
  - Come nel caso statico, il client aggiorna sia il record A che il PTR
  - Prima di chiudere la connessione di Accesso Remoto, il client tenta di eliminare i RR
    - Se ciò non riesce, il server RAS tenta di eliminare il record ormai vecchio (*stale record*)

DDNS – DC (1)

- Il servizio Netlogon registra
  - I record SRV (LDAP)
  - I record SRV (Kerberos v5)
  - Un singolo record A per il nome di dominio (DnsDomainName) in cui esiste il Domain Controller e l'ip del DC stesso. In questo modo, anche i client che non riconoscono il record SRV, possono contattare il DC grazie ad un normale *host lookup*
- Ogni DC regitra records SRV che permettono ai server di essere localizzati a partire dal tipo di servizio (es. LDAP) o dal protocollo utilizzato (es. TCP)
- Esempi
  - _ldap._tcp.esempio.com -
  - _ladp._tcp.nord._sites.esempio.com
  - _ldap._tcp.dc._msdcs.esempio.com
  - _ldap._tcp.NomeSito._sites.dc._msdcs.esempio.com
  - _ldap._tcp.pdc._msdcs.esempio.com
  - _ldap._tcp.gc._msdcs.esempio.com
  - _ldap._tcp.NomeSito._sites.gc._msdcs.esempio.com
  - _gc._tcp.contoso.com

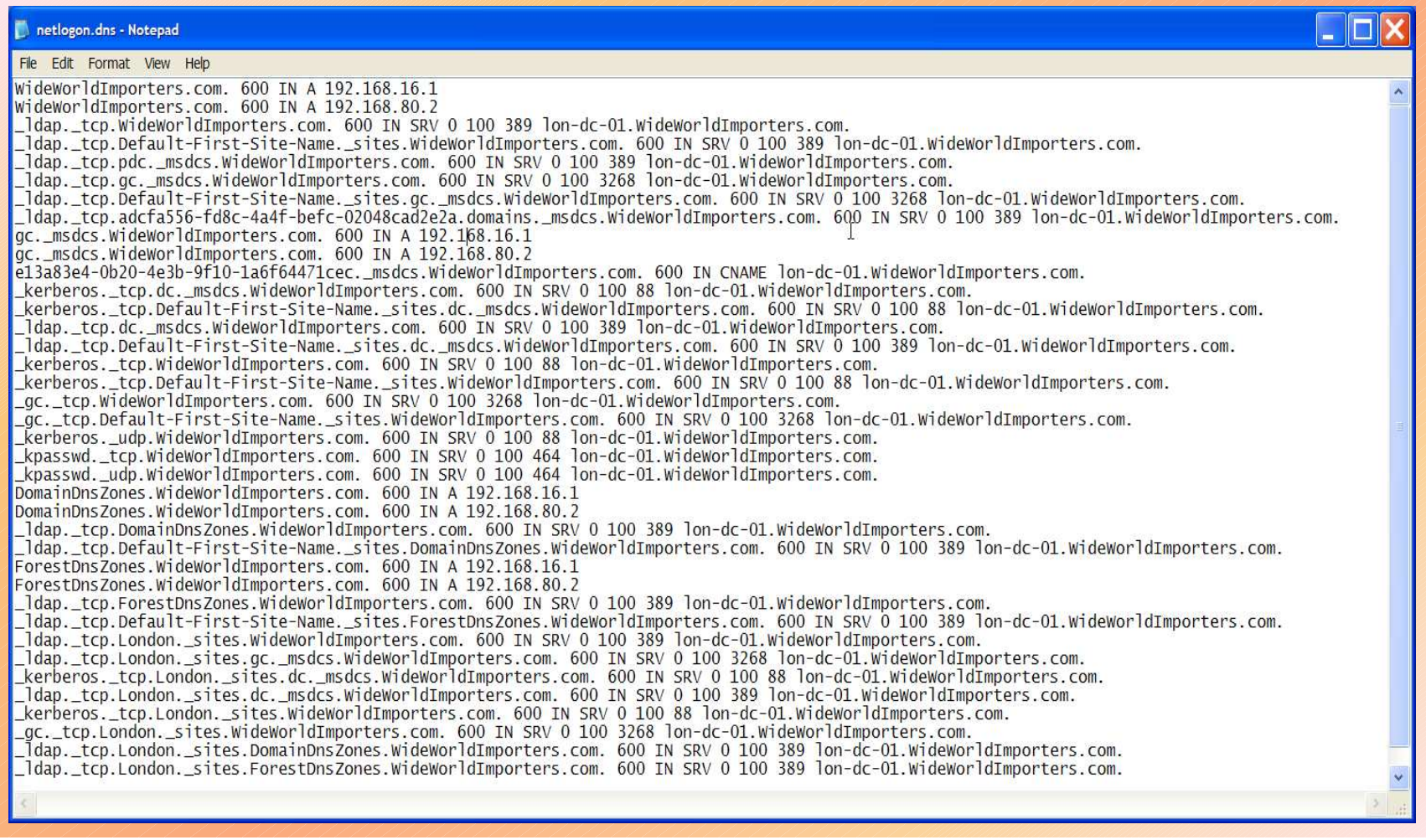
DDNS – DC (2)

- Proprietà dei record SRV

Service Protocol Site	TTL		Priority	Weight	Port	Host
_ldap._tcp	600	SRV	0	100	389	NY-DC-01.esempio.com.
_kerberos._tcp	600	SRV	0	100	88	NY-DC-01.esempio.com.
_kpasswd._tcp	600	SRV	0	100	464	NY-DC-01.esempio.com.
_gc._tcp	600	SRV	0	100	3268	NY-DC-01.esempio.com.

DDNS – DC (3)

- Il file Netlogon.dns elenca i record SRV



DDNS – Conflitto di Nomi

- Problema: cosa accade se una un client registra un nome già registrato per un altro indirizzo ip ?
  - ES. il client ottiene un nuovo lease dhcp e vuole registrare il nuovo ip ma ovviamente con lo stesso nome host
  - Per default (modificabile tramite registro di configurazione), il client:
    - Elimina la registrazione precedente
    - Registra il proprio record corrente
  - Nasce però un altro problema legato alla sicurezza dei record, in modo che un client qualunque non possa modificare il record appartenente ad un secondo client (vedi slides successive)

DDNS - Sicurezza

- Un controllo sull'autenticazione di chi è autorizzato ad effettuare una registrazione dinamica dei RR, si può configurare utilizzando due accorgimenti, purchè si utilizzi un modello di *Active Directory (AD) Integrated Zones*:
  - Stabilire Security Context grazie al transito di security Tokens
  - Impostare ACL specifiche per gli accounts abilitati ad aggiornare i RR

Secure Dynamic Update – AD

- Il client chiede al server DNS locale di localizzare un server *authoritative*
- A quest'ultimo, il client chiede conferma
- Il client tenta un aggiornamento non-sicuro (default), che viene rifiutato dal server
- Usando il record TKEY, avviene la negoziazione di un Security Context per verificare la reciproca identità
- Dopo che è stato stabilito un Security Context, client e server possono creare e verificare le firme di identità sui messaggi seguenti
- il client invia una richiesta di aggiornamento firmata con TSIG
- Il server procede nell'aggiornamento del record in AD
  - L'esito della registrazione dipende dai permessi attribuiti al client
  - In caso favorevole, il server invia al client una risposta di conferma
  - In caso sfavorevole, il server invia al client un rifiuto

Secure Dynamic Update – ACL

- Le ACL (Access Control List) possono essere specificate per:
  - Zona
  - Specifico nome
- Per default
  - L'utente può creare i record A e PTR
  - Una volta che il nome è stato creato
    - Solo chi abbia nell'ACL un permesso in scrittura può modificare/eliminare/creare records per il nome
    - Il creatore ha permesso in scrittura
    - Si applica a qualunque tipo di record
- Altro problema: per i client il cui processo di registrazione (A e PTR) viene svolto dai server DHCP, come si impostano i permessi sui record ?
  - Si aggiungono i server DHCP al gruppo ***DNSUpdateProxy***
  - Ciò assicura che i record creati dai server DHCP possano essere modificati/eliminati da qualunque server DHCP (purchè precedentemente autorizzato in Active Directory)

DDNS – Tempi di Rilascio

- La registrazione viene rinnovata periodicamente
- Il client
  - Per default, riregistra i record ogni 24 ore
  - La frequenza del rinnovo può essere configurata tramite registro di configurazione
- Il server DHCP
  - Riregistra i record al momento del rinnovo del lease DHCP da parte del clent

DDNS – Rilascio

- I record vengono rimossi da computer che li ha registrati
  - Client
  - Server DHCP
    - Rimuove il record PTR al momento del *lease expiration*
    - Rimuove il record A se è stato configurata l'opzione "Discard forward lookups when leases expire" (presente nelle proprietà del server DHCP sotto la scheda DNS)

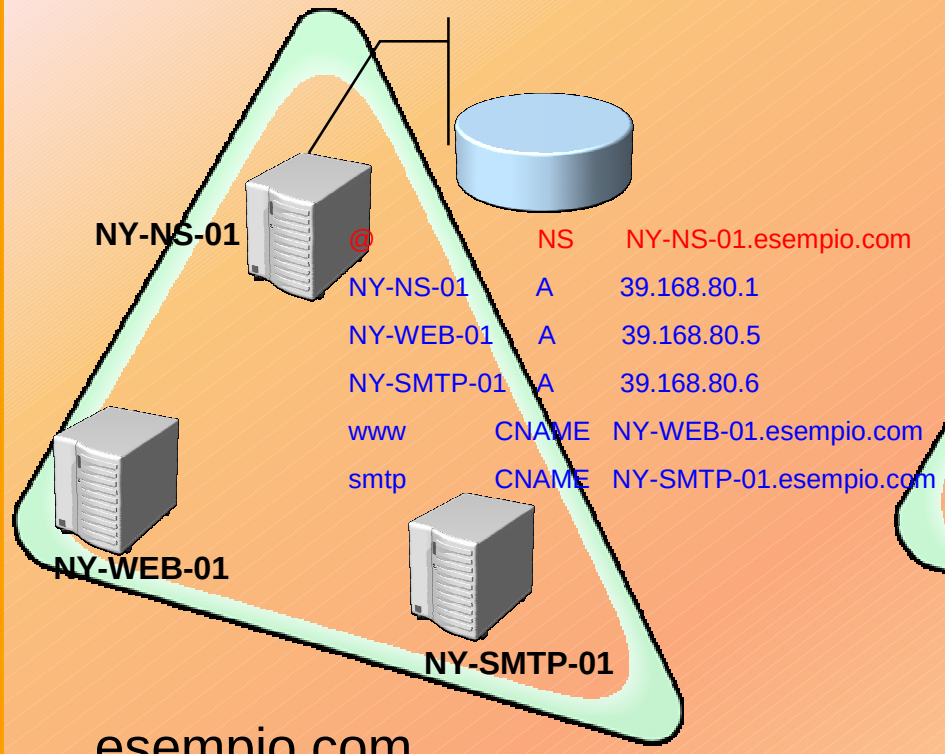
Aging & Scavenging

- Si applica ai record invecchiati e quindi resi inutili (Stale Records)
- Lo scavenging cerca nel database DNS i record riconosciuti come *stale* e li elimina
- Per default, l'opzione è disabilitata
  - Una volta abilitata, si applica solo ai record registrati successivamente
  - Può essere abilitata per
    - Server
    - Zona
    - Record

DNS – Architetture (1)

- Spazio dei Nomi Unico

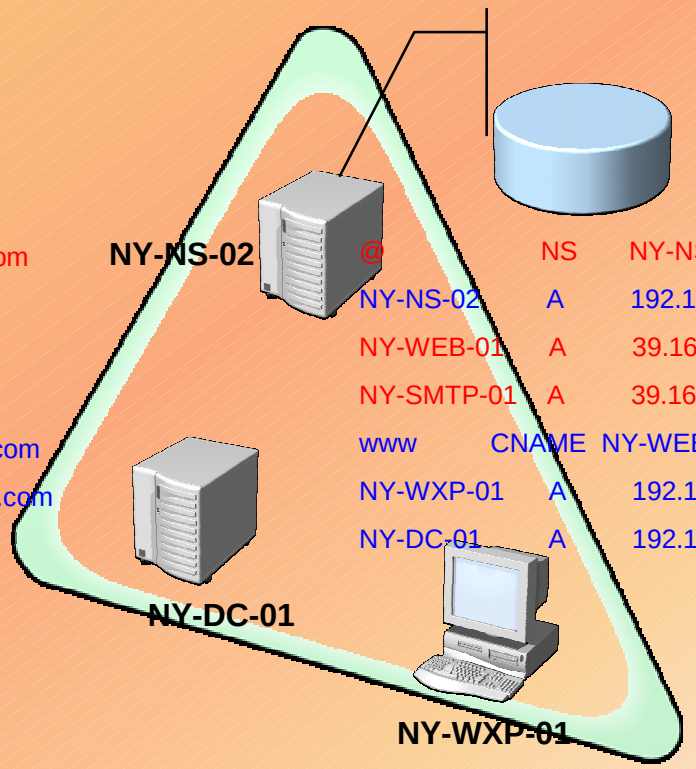
Internet



@	NS	NY-NS-01.esempio.com
NY-NS-01	A	39.168.80.1
NY-WEB-01	A	39.168.80.5
NY-SMTP-01	A	39.168.80.6
www	CNAME	NY-WEB-01.esempio.com
smtp	CNAME	NY-SMTP-01.esempio.com

esempio.com

Rete Interna

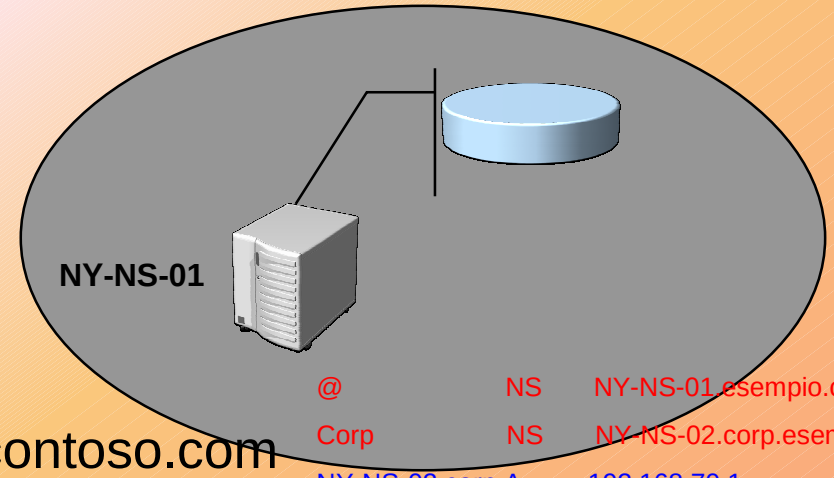


@	NS	NY-NS-02.esempio.com
NY-NS-02	A	192.168.80.1
NY-WEB-01	A	39.168.80.5
NY-SMTP-01	A	39.168.80.6
www	CNAME	NY-WEB-01.esempio.com
NY-WXP-01	A	192.168.80.6
NY-DC-01	A	192.168.80.200

esempio.com

DNS – Architetture (2)

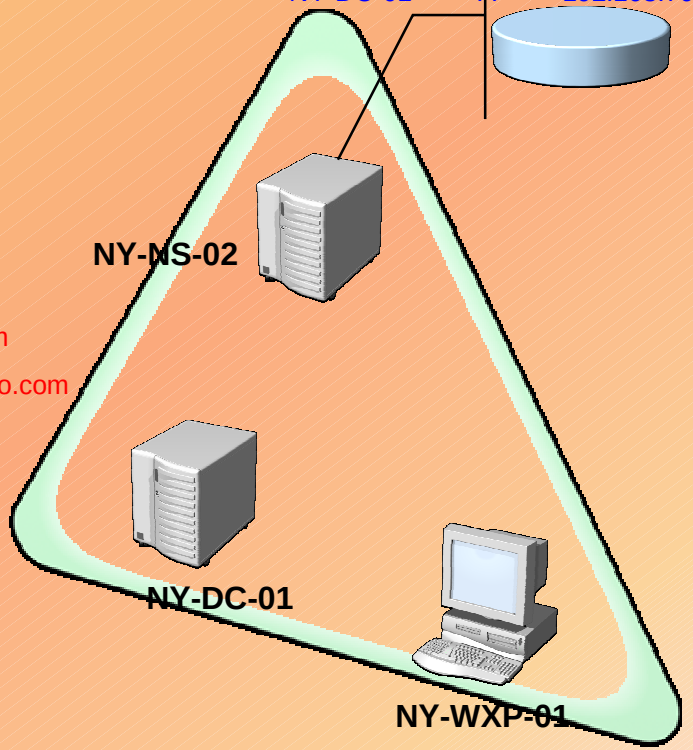
- Spazio dei Nomi Delegato (1)



contoso.com

```
@          NS    NY-NS-01.esempio.com
Corp       NS    NY-NS-02.corp.esempio.com
NY-NS-02.corp A  192.168.70.1
NY-NS-01   A     192.168.80.1
NY-WEB-01  A     192.168.80.5
NY-SMTP-01 A     192.168.80.6
www CNAME  NY-WEB-01.esempio.com
smtp CNAME NY-SMTP-01.esempio.com
```

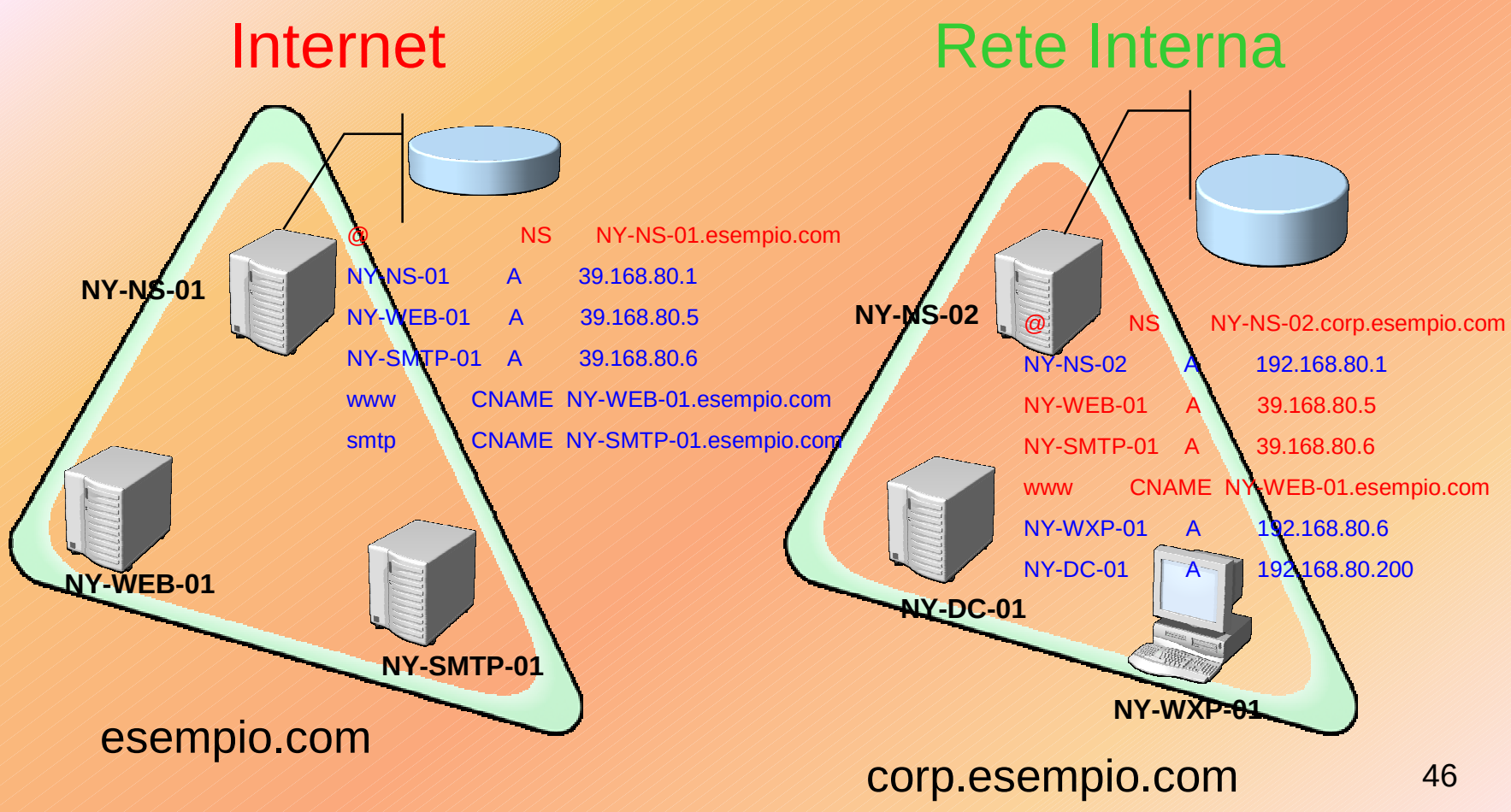
```
@          NS    NY-NS-02.corp.esempio.com
NY-NS-02   A     192.168.70.1
NY-WXP-01  A     192.168.70.6
NY-DC-01   A     192.168.70.200
```



corp.esempio.com

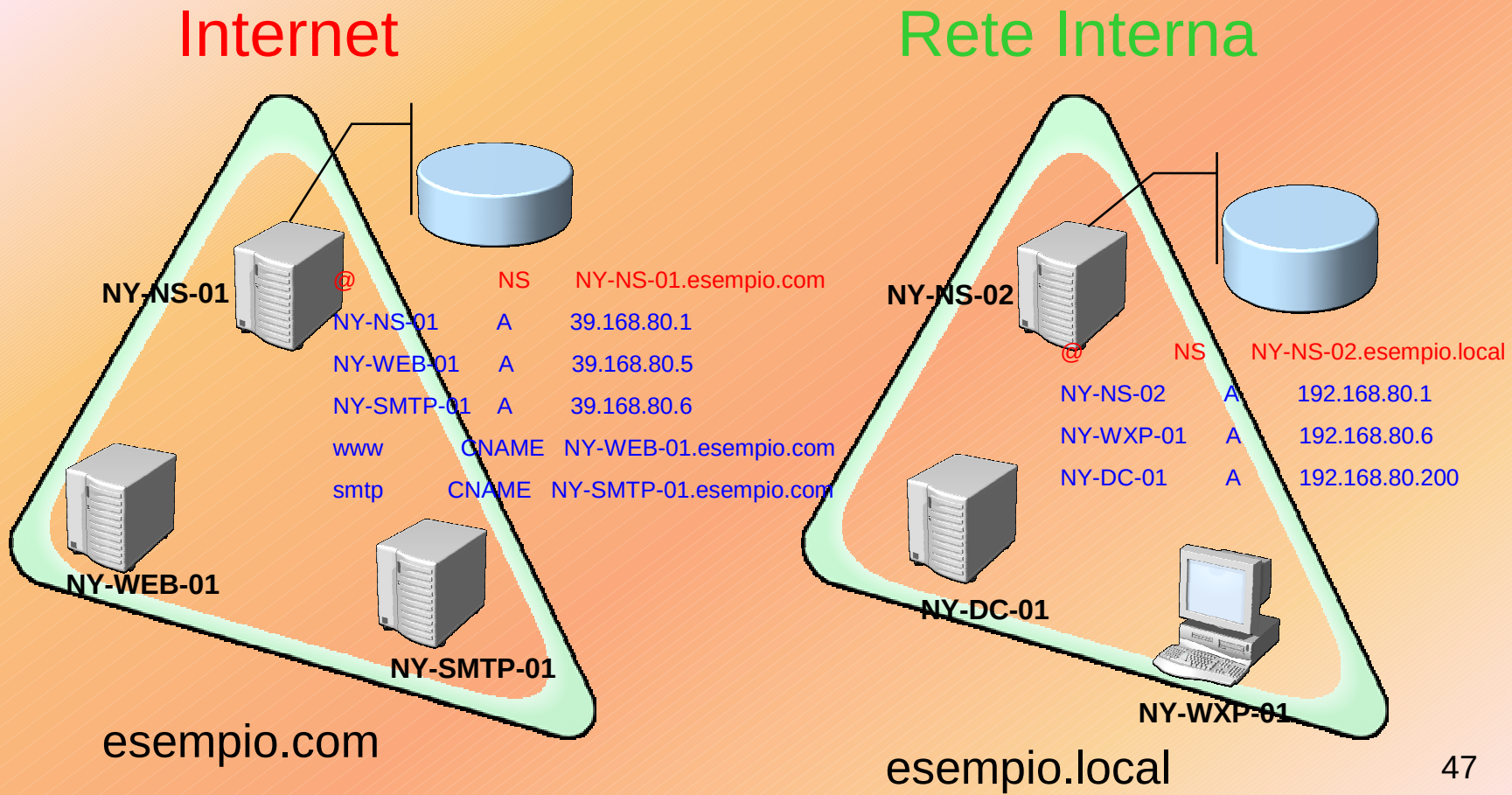
DNS – Architetture (3)

- Spazio dei Nomi Delegato (2)



DNS – Architetture (4)

- Spazio dei Nomi Univoco



Interoperabilità con BIND

- Nel caso di coesistenza tra NS Microsoft e NS BIND, si può ricorrere ad uno dei seguenti approcci:
  - Usare BIND per Internet e MS DNS per la rete interna
  - Usare BIND sia per Internet che per la Intranet
  - Usare BIND sia per Internet sia per Intranet, ma porre i domini AD in zone delegate su MS DNS
  - Usare MS DNS sia per Internet che per Intranet
- E’ possibile usare per AD anche dei server DNS non-Microsoft
  - Devono supportare i record SRV
  - Preferibilmente dovrebbero supportare anche l’aggiornamento dinamico dei record

Esempio di Named.conf

```
//BIND Configuration File
options {
   directory "/usr/local/named";
   notify yes;
};
zone "corp.contoso.com" in {
   type master;
   file "db.corp.contoso";
   check-names ignore;
   allow-transfer { 192.168.80.7; };
   allow-update { 192.168.80.5; 192.168.80.6; 192.168.80.100;};
};
zone "80.168.192.in-addr.arpa" in {
   type master;
   file "db.192.168.80";
   allow-transfer { 192.168.80.7; };
   allow-update { 192.168.80.5; 192.168.80.6; 192.168.80.100;};
};
zone "0.0.127.in-addr.arpa" in {
   type master;
   file "db.127.0.0";
zone "." in  {
   type hint;
   file "db.cache";
};
```

Opzioni in Named.conf

- **notify yes** - Istruisce il DNS Primario a mandare modifiche immediatamente ai DNS Secondari quando ci sono delle modifiche alla Zona
- **check-names ignore** - Per default, BIND controlla tutti i record per verificare che siano usati solo nomi di host standard per evitare problemi di interoperabilità.. Windows 2000 usa una sub-zone chiamata "_msdcs" per mantenere i dati di Active Directory. Questa zona non può entrare in conflitto con un nome di host (_ non ammesso per questi), ma rende anche impossibile mettere nomi di host in questa zona (BIND li vede come illegali). Active Directory cerca di inserire i GC in _msdcs, ma questa operazione viene vietata per default da BIND. Per evitare questi problemi, Microsoft raccomanda che AD sia piazzata in una sub-zone per la quale disabilitare il controllo dei nomi host.
- **allow transfer** - Indica quali host (NS) possono iniziare un trasferimento di zona.
- **allow update** - Per motivi di sicurezza è meglio consentire solo ai DC e ai DHCP la modifica dei record in DNS.

DNS – Sicurezza

- Esporre solo la parte pubblica del namespace
- Limitare il numero dei record nel DNS esterno
- Usare pochi record alias (CNAME)
- Integrare le zone in AD
- Considerare la possibilità di usare zone secondarie
- Usare i *Forwarder* o ancora meglio dei proxy/gateway (firewall) per le zone su Internet
- Filtrare il traffico DNS sui firewall
- Restringere il traffico DNS in base agli IP
- Usare la ricorsione quando possibile
- Cancellare i R*oot Hint* sui server che non devoo comunicare con i server DNS che hanno autorità sui domini radice
- Modificare i *Root Hint* se il dominio radice è interno
- Consentire la replica solo per i NS specificati
- Mettere in sicurezza il servizio DNS usando le ACL
- Per le Zone Standard modificare i permessi sui file di zona
  - <%systemroot%>\System32\DNS
- Mettere in sicurezza le chiavi del registro di configurazione relative al DNS
  - HKLM\System\CurrentControlSet\Services\DNS

DNS – Scenari

- Scenario 1 – Ambiente Intranet
  - Hardening del Sistema Operativo e del servizio DNS
  - Il firewall dovrebbe bloccare qualunque traffico DNS in entrata sulla porta 53 tcp ed udp
  - Le zone dovrebbero essere integrate in AD
  - I trasferimenti di zona dovrebbero essere consentiti solo a specifici server
- Scenario 2 – Ambiente Internet
  - Separare il DNS esterno da quello interno
  - Usare all'interno zone integrate in AD
  - Trasferimenti di zona consentiti sui server interni
  - Trasferimenti di zona verso l'esterno solo in modalità *sicura* e ai soli server previsti
  - Hardening del Sistema Operativo
  - Hardening del Registry
  - Disabilitare tutti i servizi non utilizzati sul server DNS esterno
  - Disabilitare il Dynamic DNS sui server DNS esterni