



Universidade do Minho
Escola de Engenharia

Serviços de suporte

DNS, DHCP, NAT

DNS - Domain Name System

Mecanismo de nomeação de recursos na rede:

- Máquinas, domínios, serviços, etc.

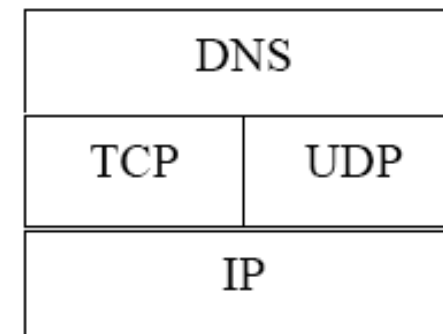


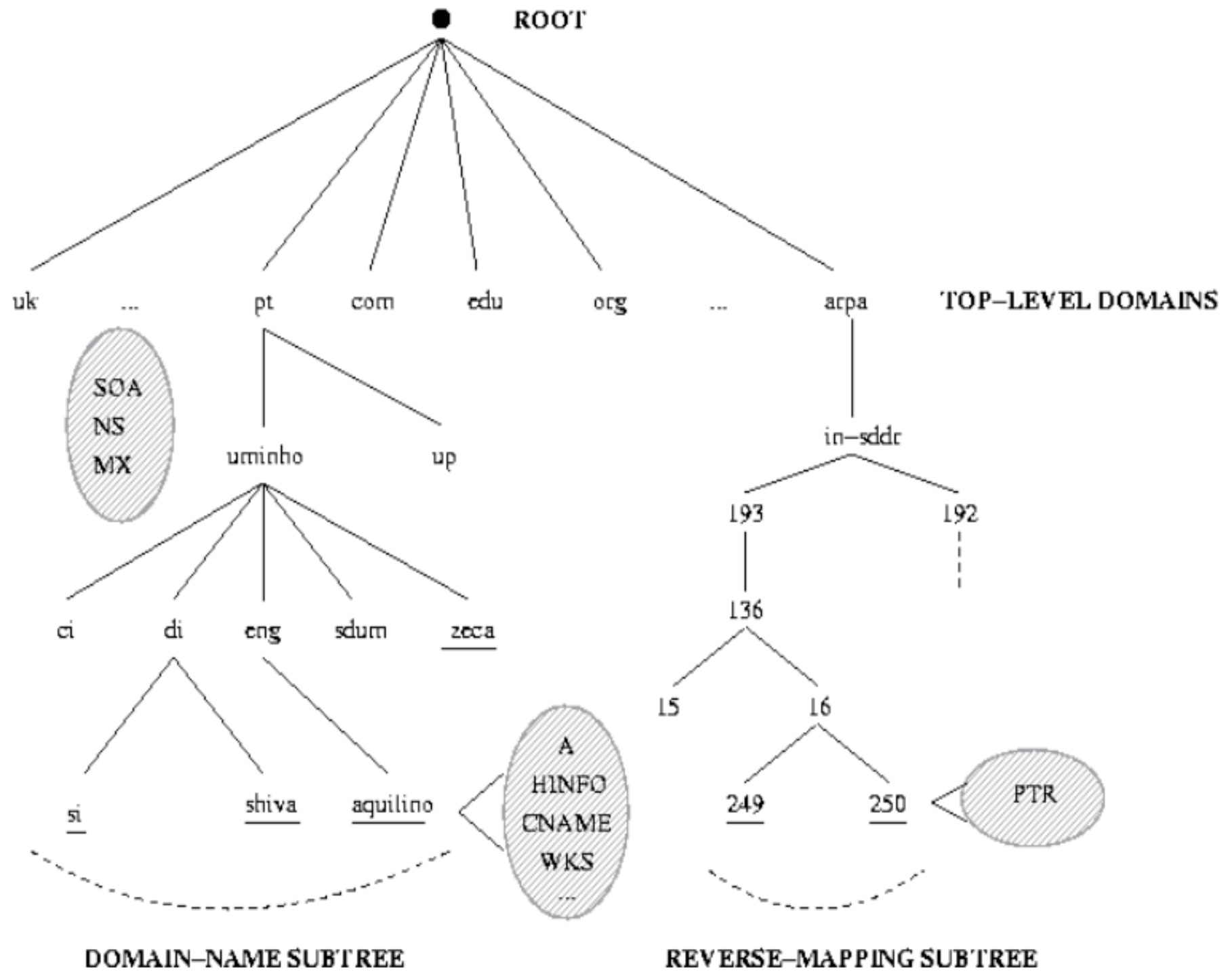
- Não mantém apenas nomes e endereços:
 - tipo de computador e sistema operativo (HINFO)
 - lista de serviços disponíveis (WKS)
 - aliases (CNAME)
 - servidores de mail (MX) e servidores de nomes (NS)
 - ...

Definido nos RFCs 1034 e 1035, vários RFCs subsequentes ...

DNS

- Base de dados distribuída, espaço de nomeação hierárquico:
 - cada servidor de nomes mantém base de dados de uma zona (parte da árvore)
- Serviço suportado pelo protocolo TCP ou UDP consoante a tarefa envolvida





DNS

- Os nomes absolutos (Fully Qualified Domain Names) terminam com "."
- Não há uma relação directa entre domínio de nomes e rede IP
 - ***dns.uminho.pt - 193.137.16.75***
 - ***marco.uminho.pt 193.136.9.240***
 - ***gw.sa.di.uminho.pt 193.136.19.11***
 - ***shiva.di.uminho.pt 193.136.19.19***
- Para uma correcta delegação de autoridades, os NS devem constar no domínio superior!



DNS

Ficheiro de configuração dos clientes:

/etc/resolv.conf

domain di.uminho.pt

nameserver 193.136.9.240

DNS

Existem três tipos de servidores de nomes:

- **primários:** carrega a sua BD de disco. Existe apenas um por cada zona. O primário para a raíz (".") da árvore chama-se root server.
- **secundários:** tal como o primário, detém autoridade sobre uma zona, mas obtém toda a informação directamente do primário por transferência de zona
- **caching-only:** não possuem dados autoritativos para nenhuma zona, mas respondem a *queries reenviando-as* a outros servidores e guardando as respostas obtidas em cache. Também se podem designar *forward-caching servers*.

Cada zona deve ter **pelo menos** um servidor primário e um servidor secundário acessíveis no interior e do exterior do domínio, de preferência em redes distintas.

DNS

Actualização dos secundários (transferência de zona):

- São os secundários que de tempos a tempos (*refresh*) *contactam os primários*:
 - Formulam uma query do tipo SOA e verificam o *serial number*
 - Se o n.º de série mudou, formulam um pedido AXFR (transferência total de zona)
- Todos parâmetros de transferência estão no SOA (responsabilidade do primário):

di.uminho.pt IN SOA dns.di.uminho.pt dnsadmin.di.uminho.pt (2011122201 28800 7200 604800 43200)

DNS – Resource Records

- Base de dados distribuída do DNS composta por *Resource Records (RRs)*
- Cada registo RR mapeia um nome num objecto segundo a estrutura geral

Name	TTL	Class	Type	RData
------	-----	-------	------	-------

- *Time To Live* – n^o de segundos que o RR pode ser mantido em cache como válido
- *Class* – define a classe (Internet=IN)
- *Type* – define o tipo de RR (SOA, NS, MX, etc.)
- *Rdata* - Dados dependentes do Type



Exemplos RR

- **SOA (Start of Authority)** - Define o início de uma zona todos os seus parâmetros
- **NS (Name Server)** - Define o(s) servidor(es) que detém autoridade numa zona
- **MX (Mail Exchanger)** - Define o(s) servidor(es) de mail para o domínio
- **A, AAAA (Address)** - Endereço IPv4, IPV6
- **HINFO (Hardware Info)** - Define o CPU e o SO de um sistema
- **PTR (Pointer)** - Apontador para o nome ... usado no *reverse-mapping*
- **CNAME (Canonical Name)** - Nome alternativo
- **WKS (Well Known Services)** - Define os serviços (portas) disponíveis num sistema

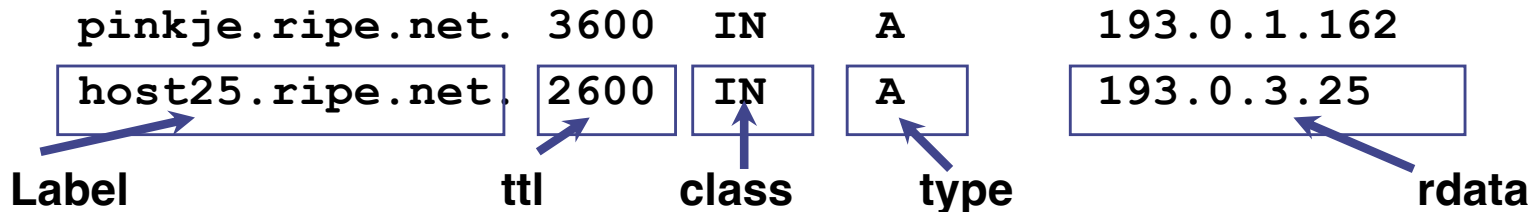
Exemplo: RR de uma zona

```
ripe.net. 7200 IN      SOA      ns.ripe.net.  olaf.ripe.net. (  
                2001061501      ; Serial  
                43200      ; Refresh 12 hours  
                14400      ; Retry 4 hours  
                345600      ; Expire 4 days  
                7200      ; Negative cache 2 hours  
                )
```

```
ripe.net. 7200 IN      NS      ns.ripe.net.  
ripe.net. 7200 IN      NS      ns.eu.net.
```

```
pinkje.ripe.net. 3600 IN      A      193.0.1.162  
host25.ripe.net. 2600 IN      A      193.0.3.25
```

Label ttl class type rdata



DNS - Modo de funcionamento

Face a uma query colocada ao nameserver por defeito:

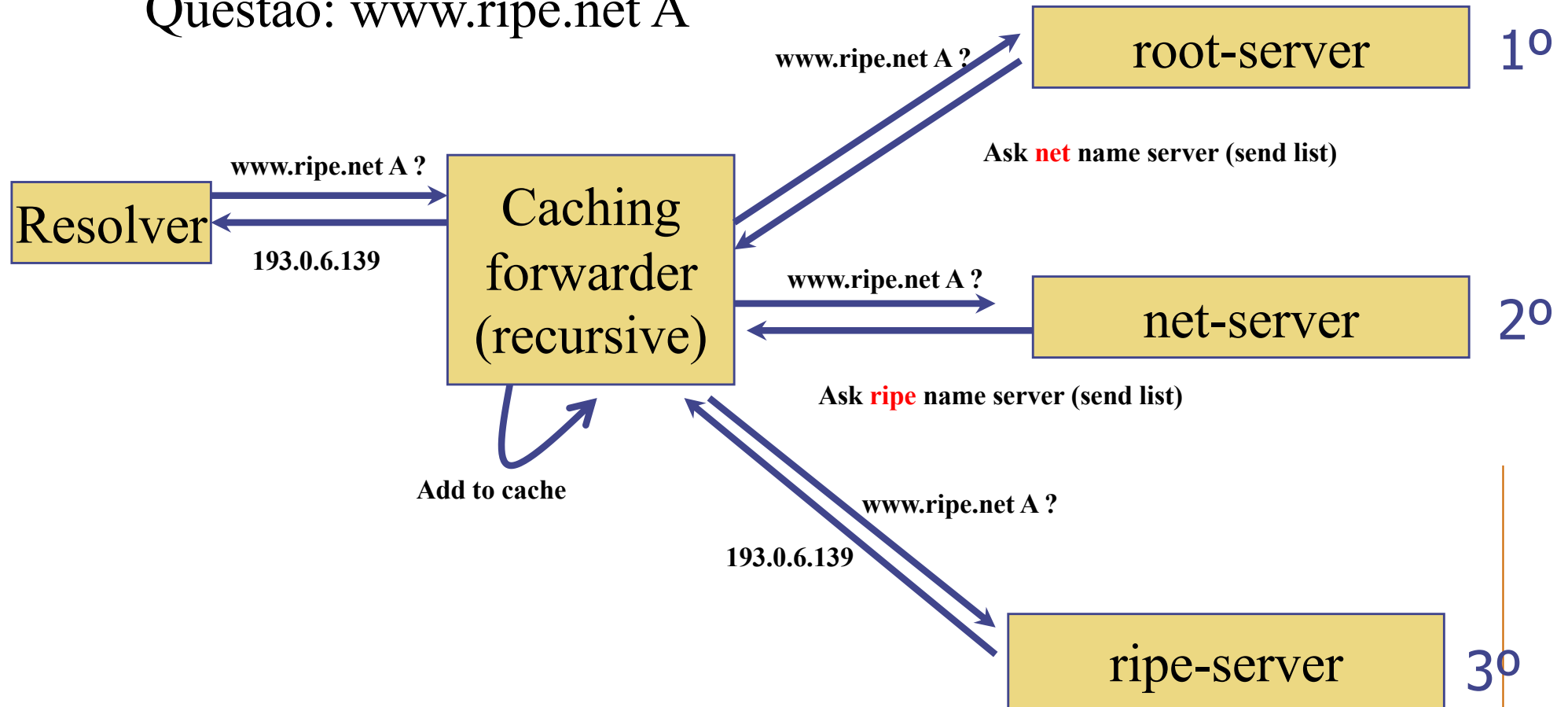
Se o nameserver não tem a resposta pode agir de duas formas:

- **modo recursivo:** o servidor contacta outros servidores de nomes, até obter uma resposta para devolver ao cliente
- **modo iterativo:** o servidor devolve ao cliente referências a servidores que podem responder (NS), e cabe ao resolver do cliente reformular a *query* a um destes servidores



Resolução de query e caching

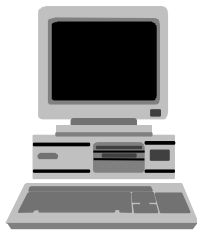
Questão: www.ripe.net A





The Resolution Process

- Let's look at the resolution process step-by-step:

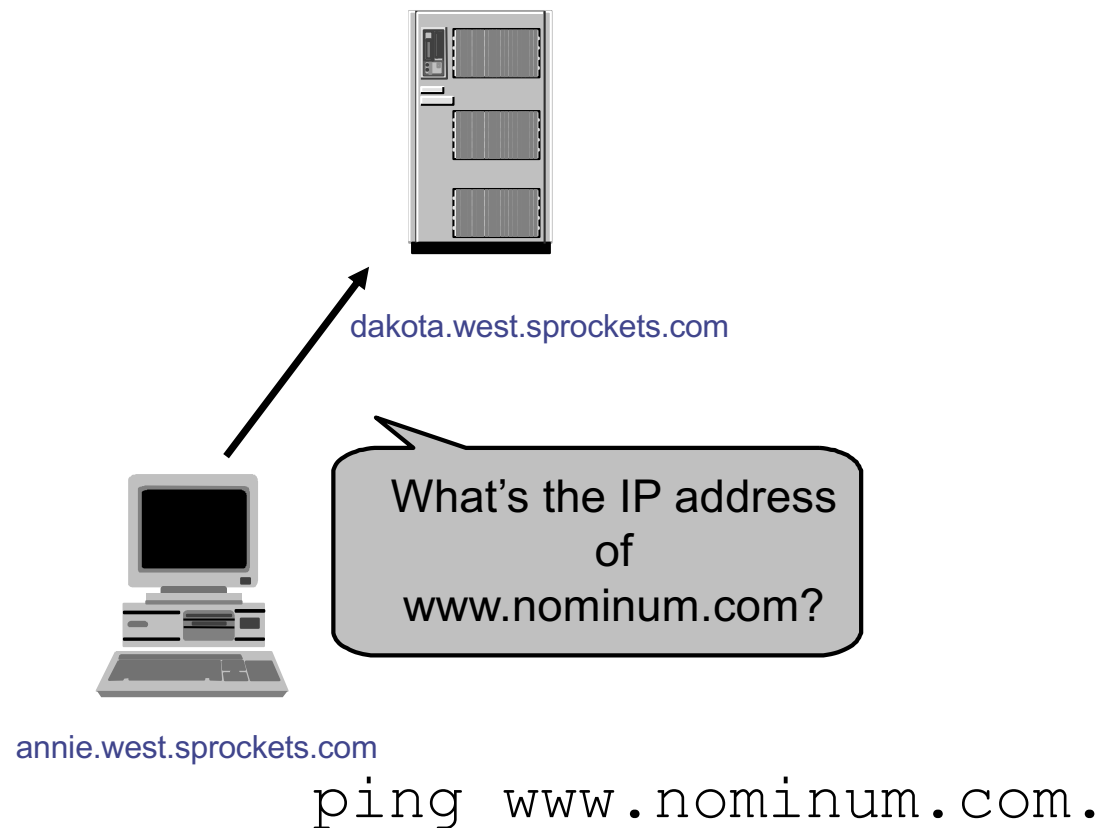


annie.west.sprockets.com

```
ping www.nominum.com.
```

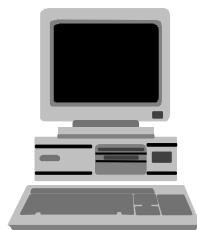
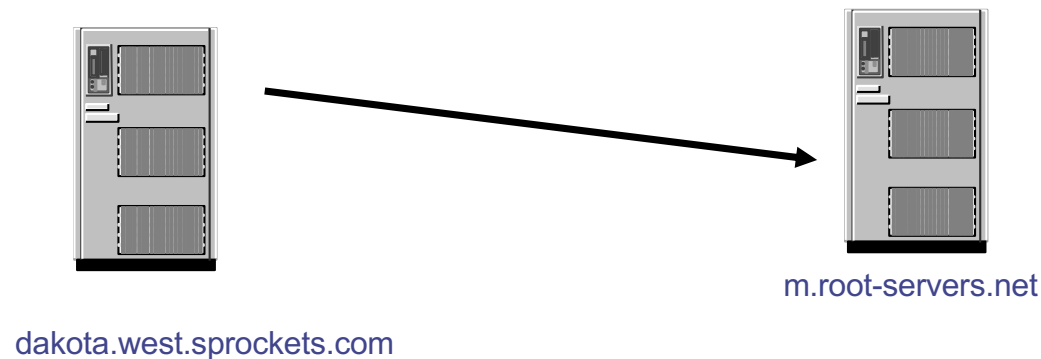
The Resolution Process

- The workstation *annie* asks its configured name server, *dakota*, for *www.nominum.com*'s address



The Resolution Process

- The name server *dakota* asks a root name server, *m*, for *www.nominum.com*'s address



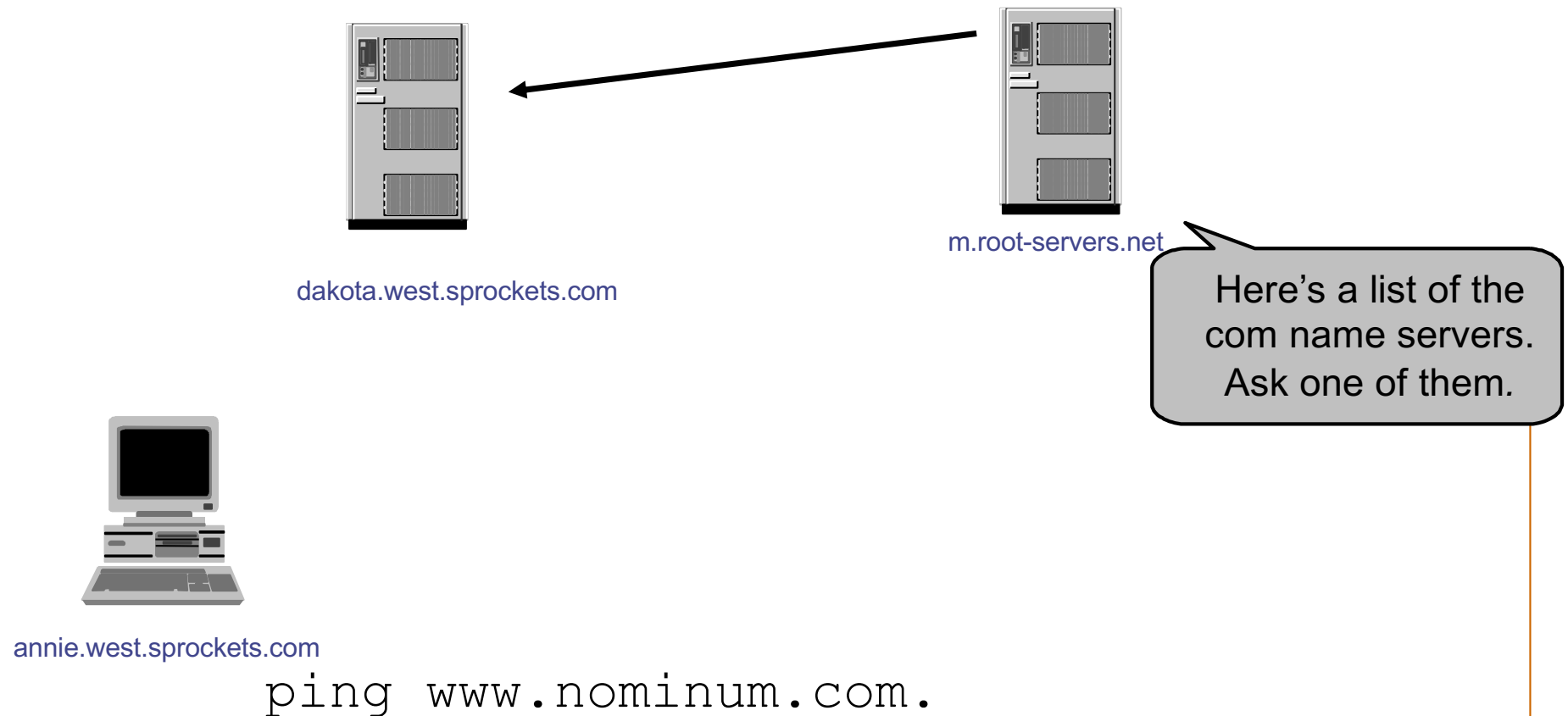
`annie.west.sprockets.com`

What's the IP address
of
`www.nominum.com`?

`ping www.nominum.com.`

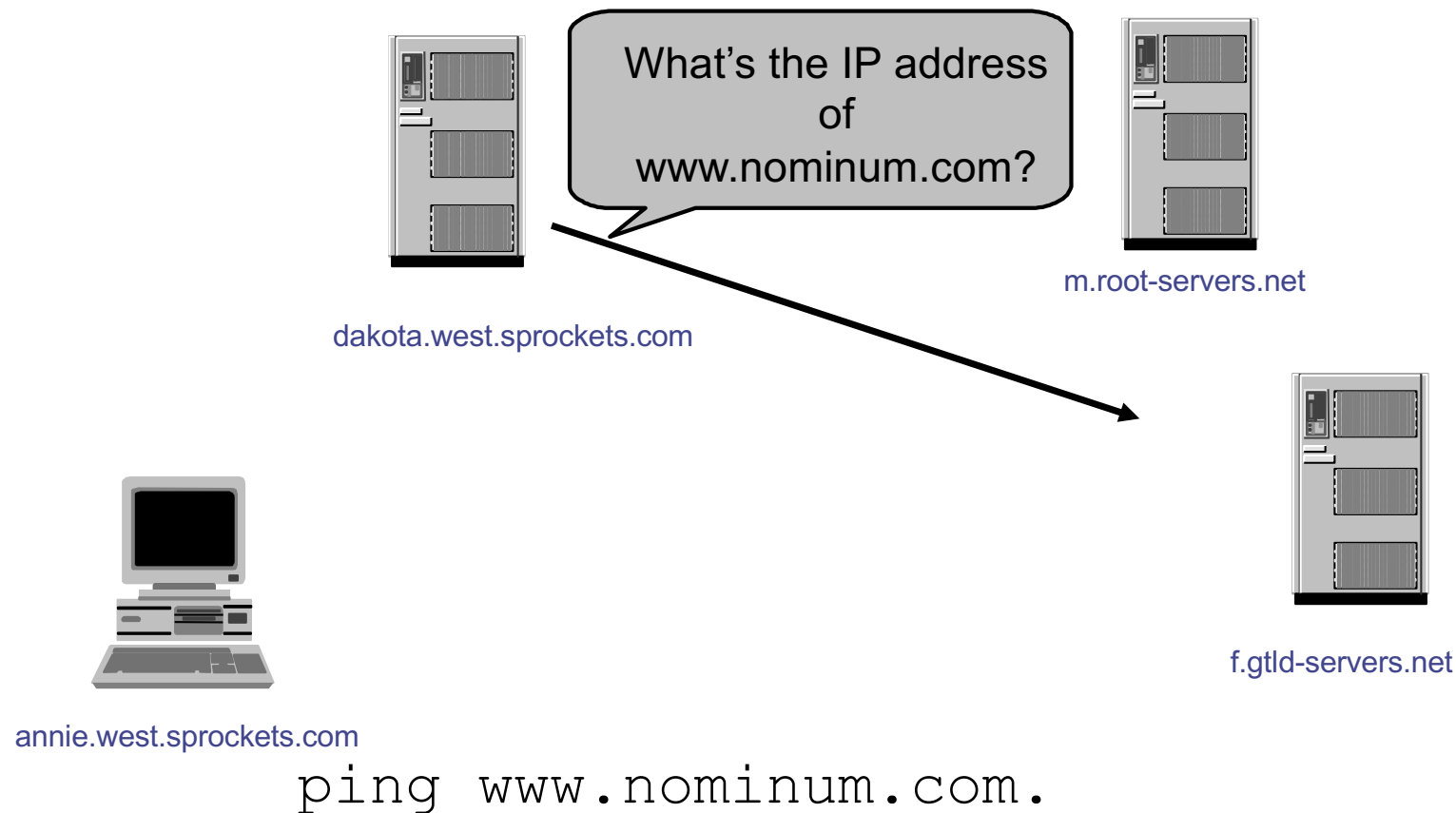
The Resolution Process

- The root server *m* refers *dakota* to the *com* name servers
- This type of response is called a “referral”



The Resolution Process

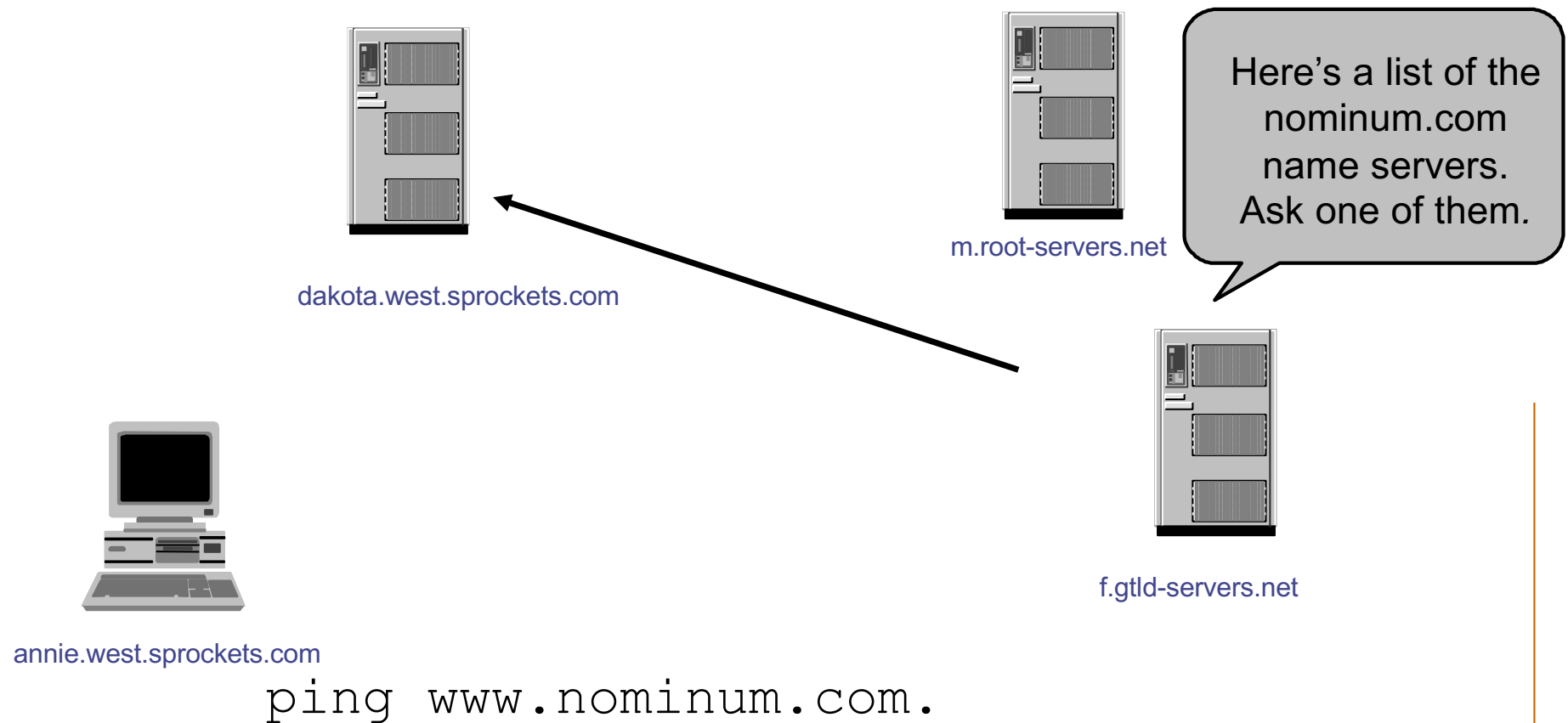
- The name server *dakota* asks a *com* name server, *f*, for *www.nominum.com*'s address





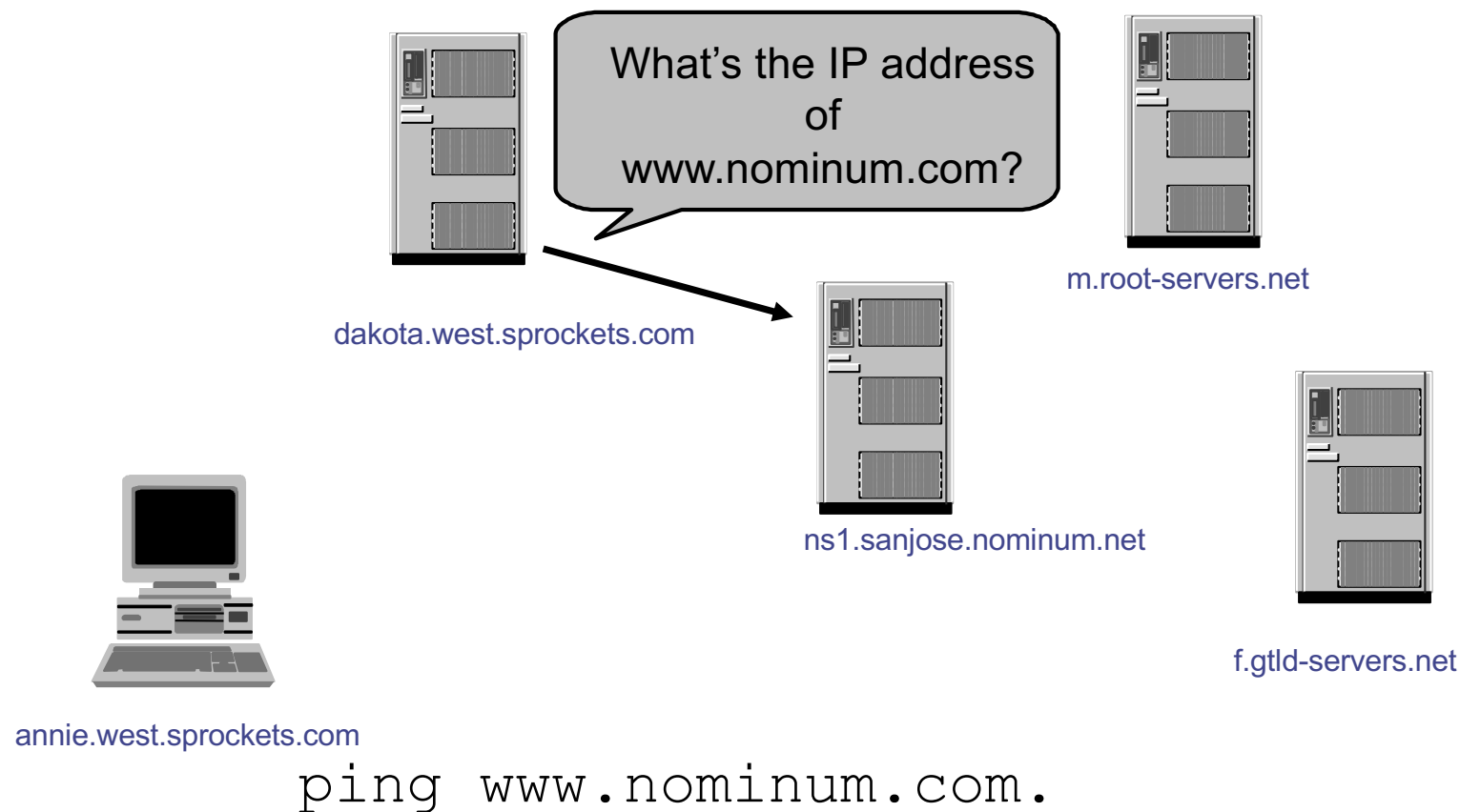
The Resolution Process

- The *com* name server *refers* *dakota* to the *nominum.com* name servers



The Resolution Process

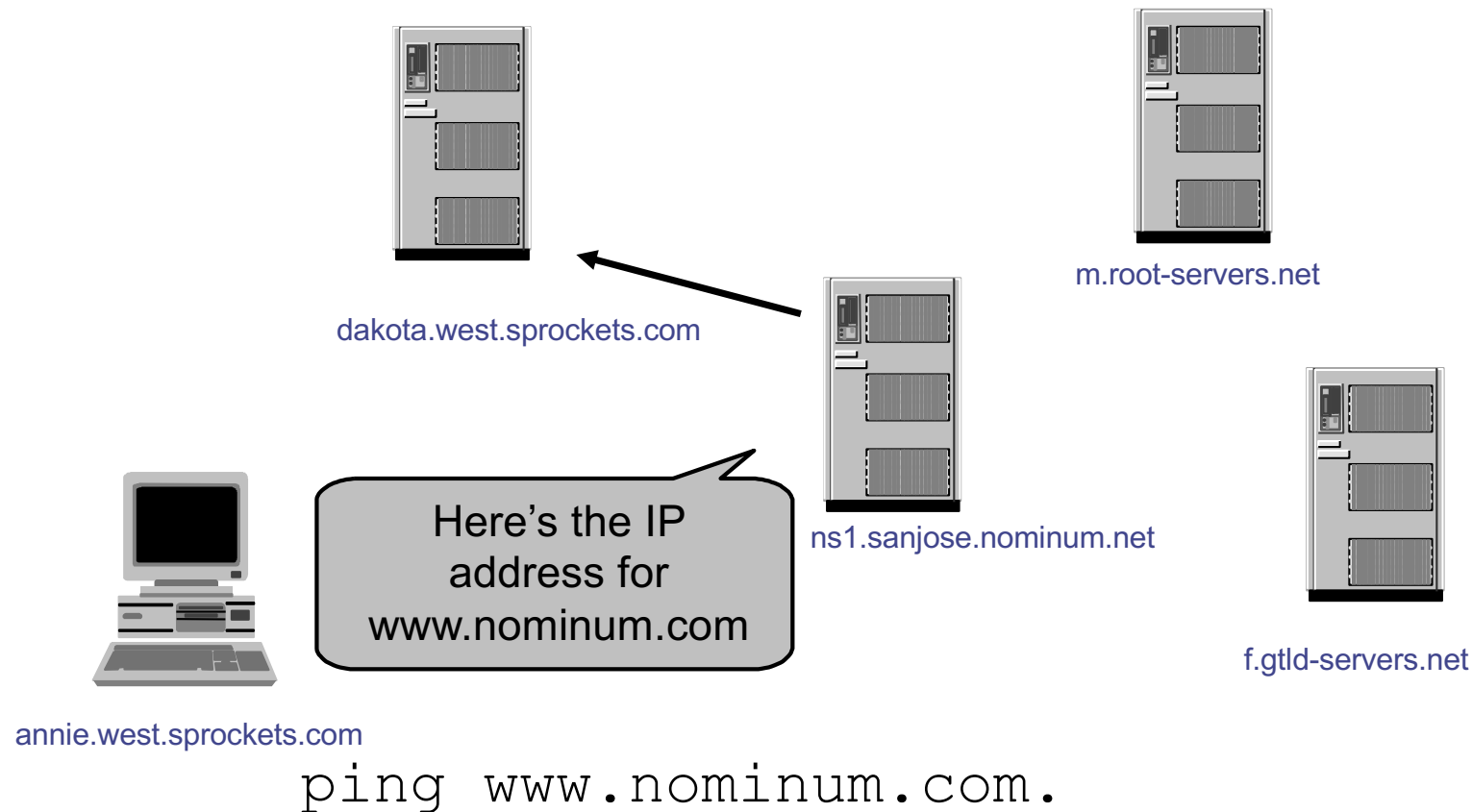
- The name server *dakota* asks an *nominum.com* name server, *ns1.sanjose*, for *www.nominum.com*'s address





The Resolution Process

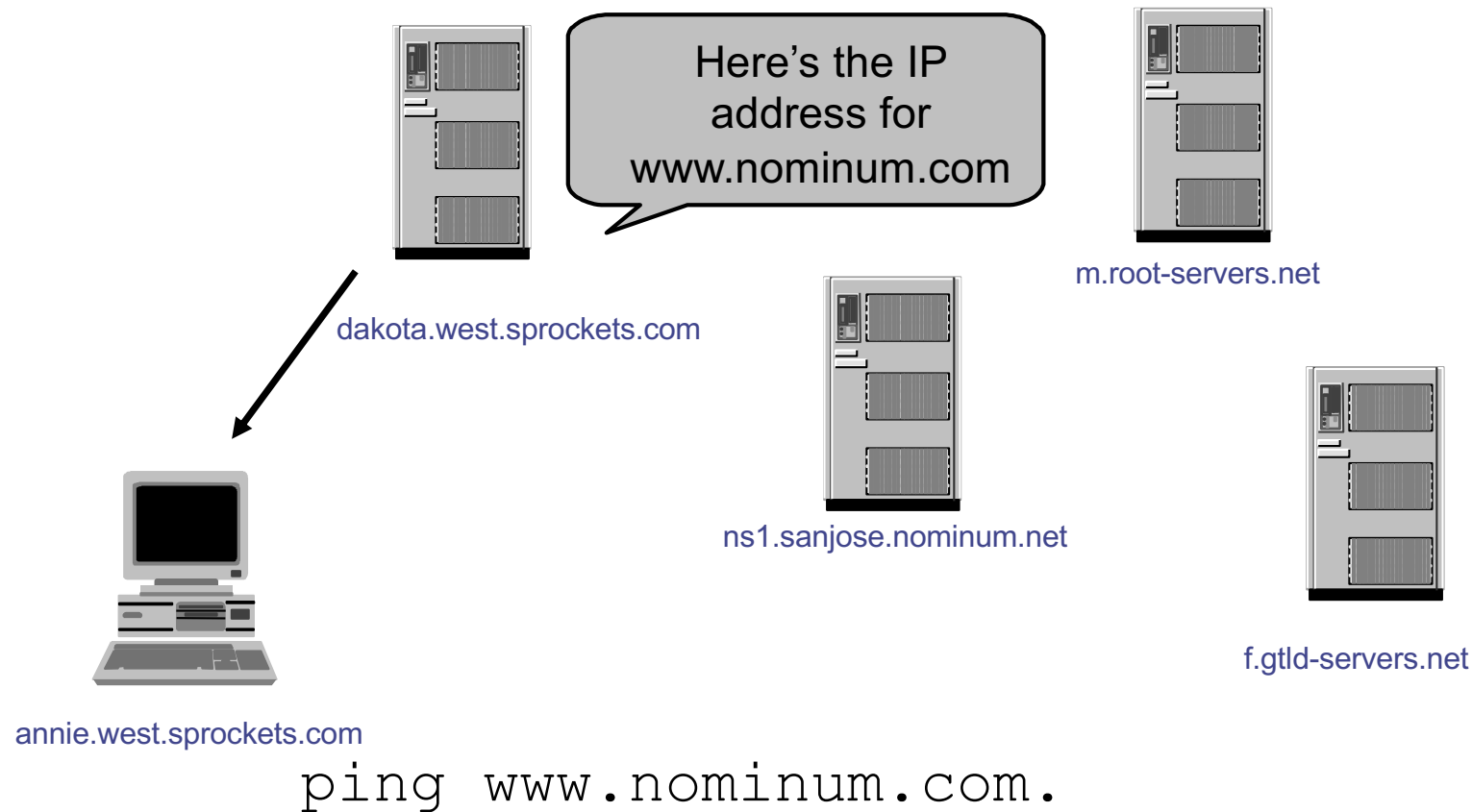
- The *nominum.com* name server *ns1.sanjose* responds with *www.nominum.com's* address





The Resolution Process

- The name server *dakota* responds to *annie* with *www.nominum.com's* address





Resolution Process (Caching)

- After the previous query, the name server *dakota* now knows:
 - The names and IP addresses of the *com* name servers
 - The names and IP addresses of the *nominum.com* name servers
 - The IP address of *www.nominum.com*
- Let's look at the resolution process again



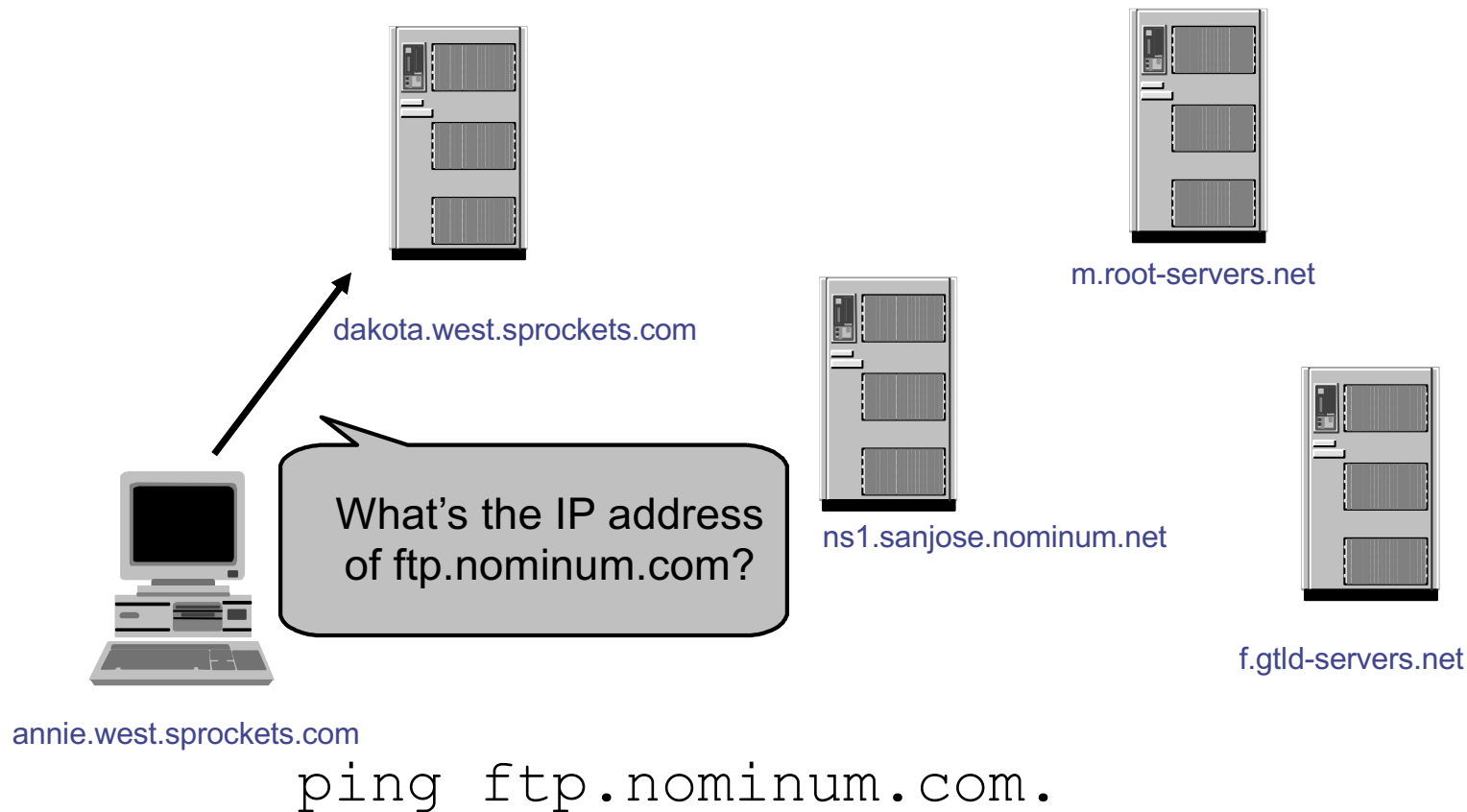
annie.west.sprockets.com

ping **ftp**.nominum.com.



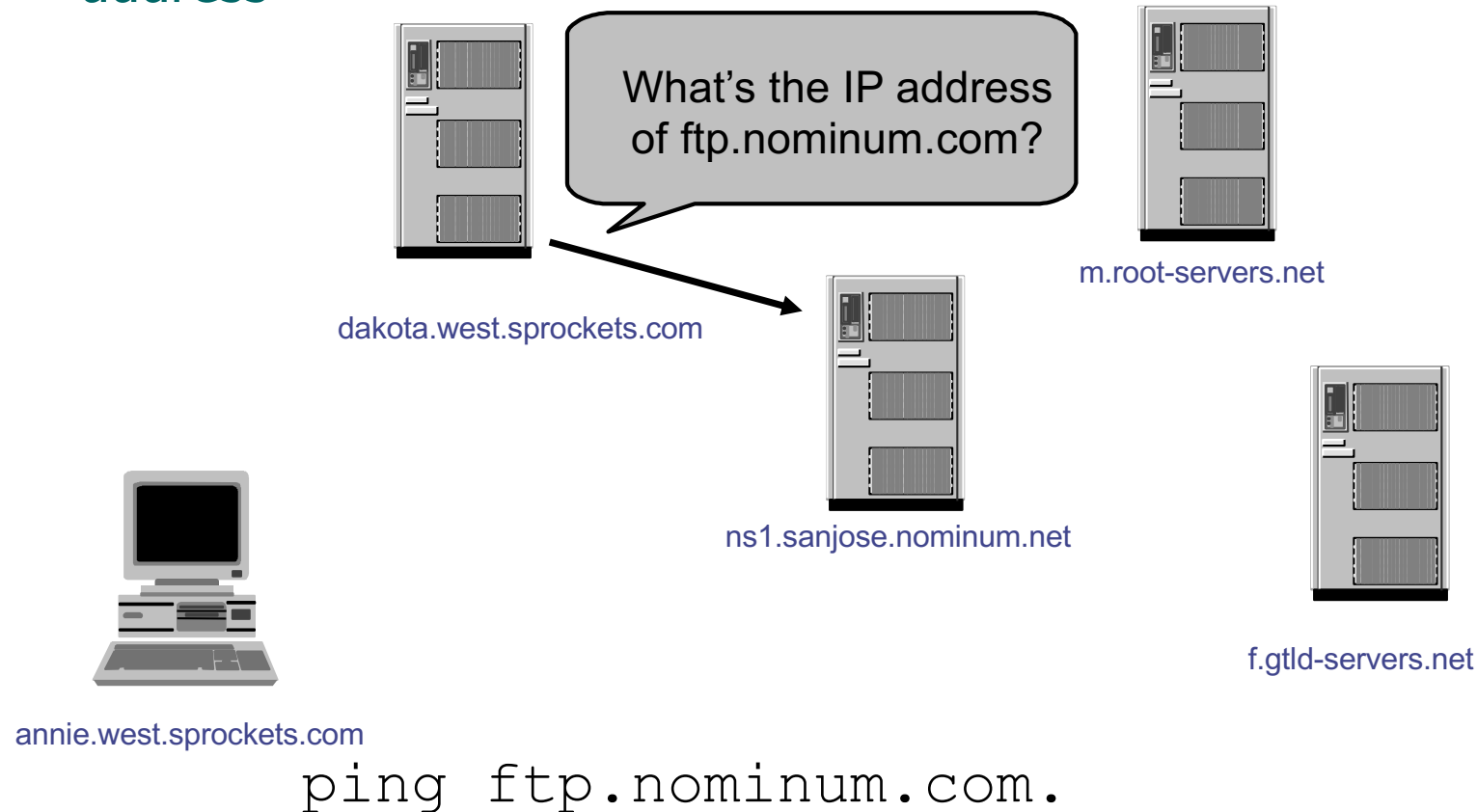
Resolution Process (Caching)

- The workstation *annie* asks its configured name server, *dakota*, for *ftp.nominum.com*'s address



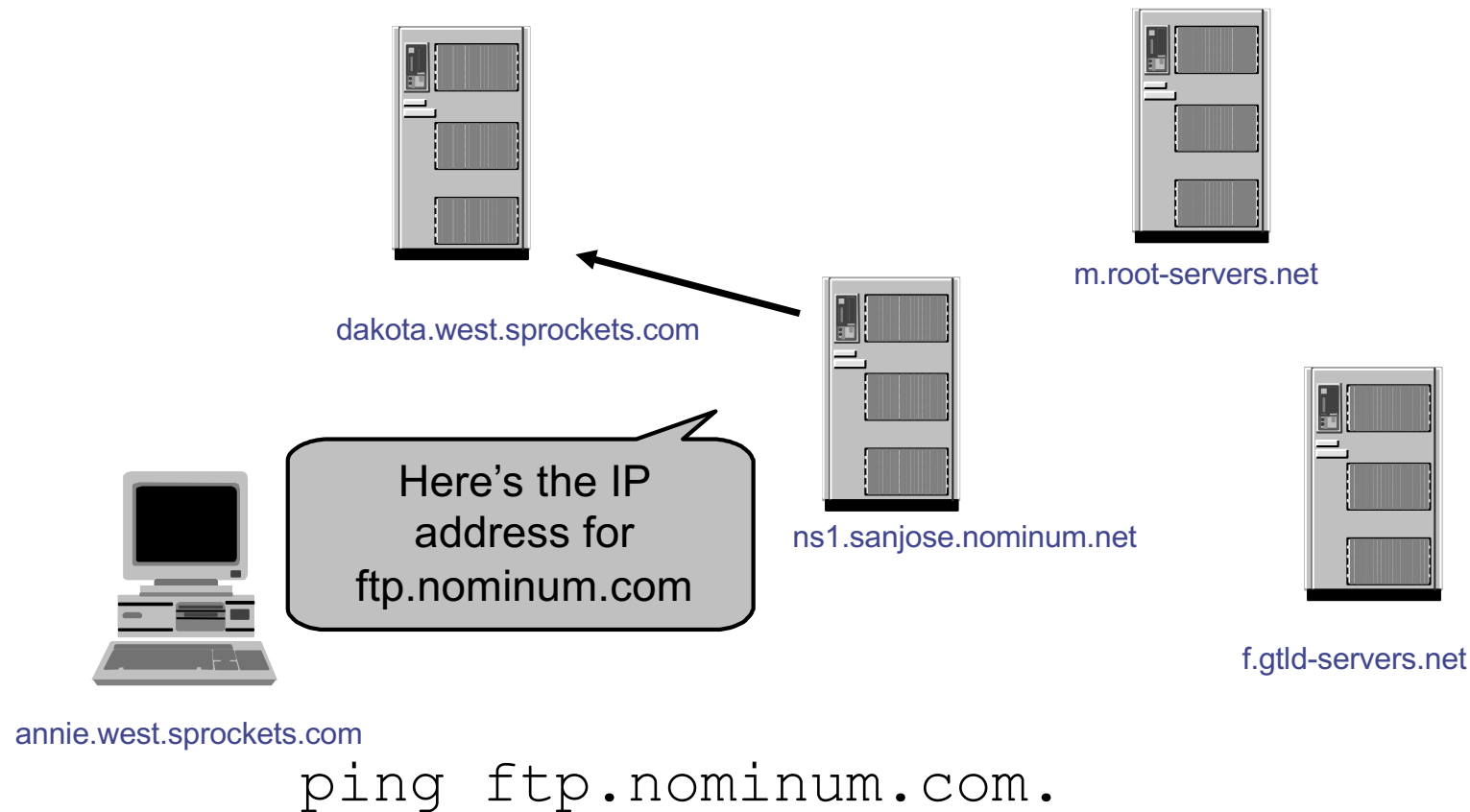
Resolution Process (Caching)

- dakota* has cached an NS record indicating *ns1.sanjose* is an *nominum.com* name server, so it asks it for *ftp.nominum.com*'s address



Resolution Process (Caching)

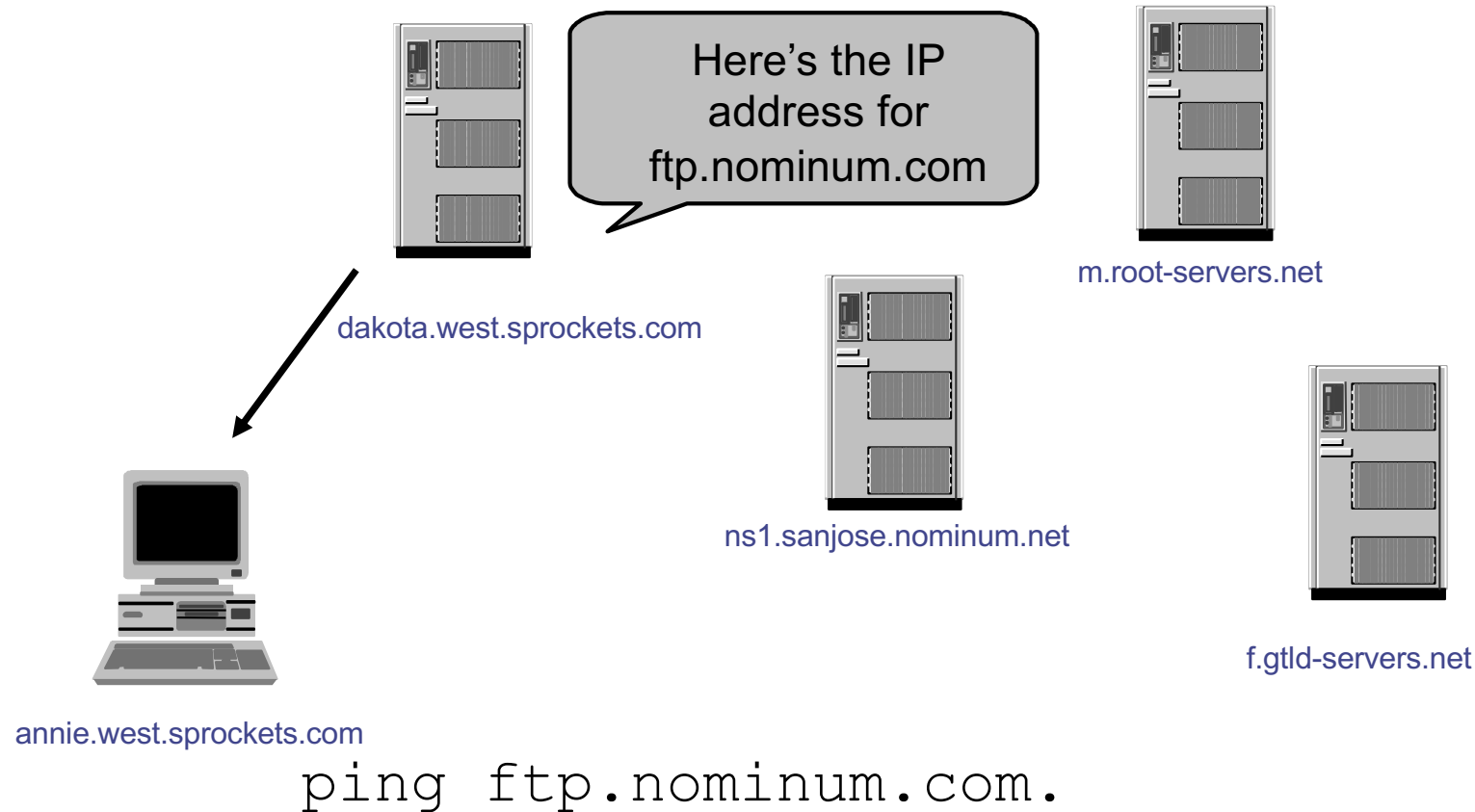
- The *nominum.com* name server *ns1.sanjose* responds with *ftp.nominum.com*'s address





Resolution Process (Caching)

- The name server *dakota* responds to *annie* with *ftp.nominum.com*'s address



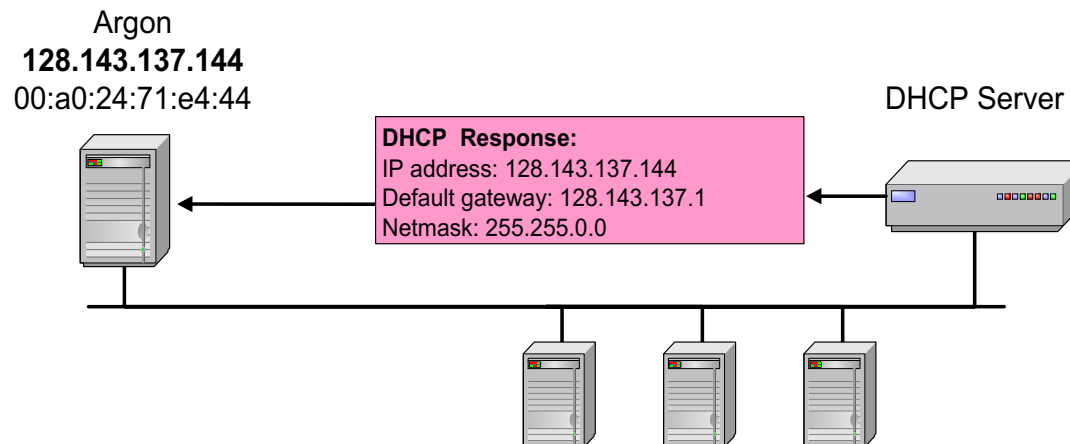
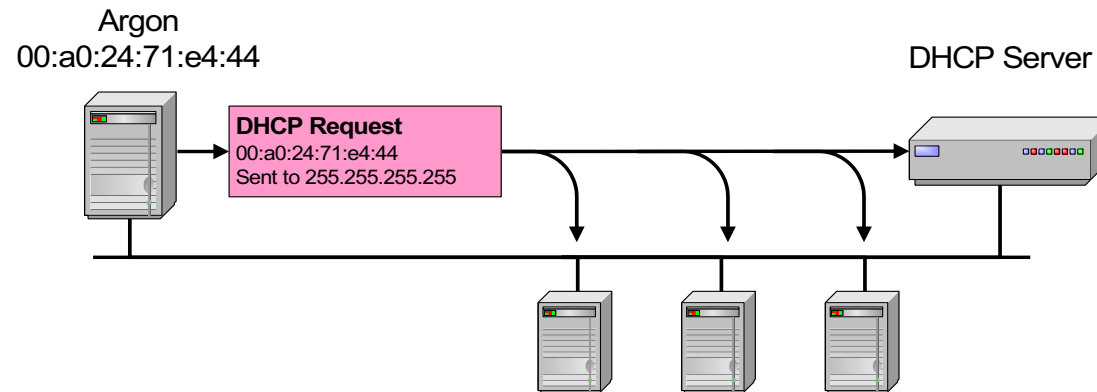
DHCP

- Dynamic Host Configuration Protocol
 - Definido nos RFCs 2131, 2132 e 1534
 - Implementado com base no BOOTP (formato idêntico das mensagens; compatibilidade entre servidores DHCP e clientes BOOTP)
- Atribuição automática de endereços IP a dispositivos (hosts, ...) na rede
 - Atribuição de endereços IP consoante necessário
 - Evita configuração manual
 - Favorece a mobilidade dos dispositivos

DHCP

- DHCP permite que um servidor realize duas funções:
 - Alocar temporária ou permanentemente endereços aos hosts
 - Entregar parâmetros de configuração aos hosts
- Se não tiver endereço IP atribuído, o cliente usa EndDest = 255.255.255.255 (broadcast limitado à própria rede) e EndSrc = 0.0.0.0
- Se já tiver endereço IP atribuído, o cliente usa endereço do servidor como destino e o seu endereço como origem (unicast)

Interação DHCP (simplificada)



DHCP

Suporta três mecanismos de alocação de endereços IP:

- **Alocação manual** – servidor pré configurado para atribuir sempre o mesmo endereço (definido pelo administrador) a um host (MAC-IP)
- **Alocação dinâmica** – servidor escolhe e atribui (da pool de endereços) um endereço durante um período de tempo limitado – *Lease*
 - único mecanismo que permite reutilizar automaticamente endereços libertados
- **Alocação automática** – servidor escolhe e atribui um endereço (da pool de endereços) permanente a um host
- Alguns servidores DHCP podem interagir com servidores DDNS (Dynamic DNS) para registar dinamicamente os nomes dos seus clientes

DHCP

- *Lease*
 - É o intervalo de tempo durante o qual um cliente utiliza um endereço
 - O cliente, caso necessite, deve pedir ao servidor o prolongamento do *lease*, senão este é expirado
 - Um servidor só reutilizará um endereço libertado quando esgotar sequencialmente todos os restantes endereços da *pool*

DHCP Tipo de mensagens

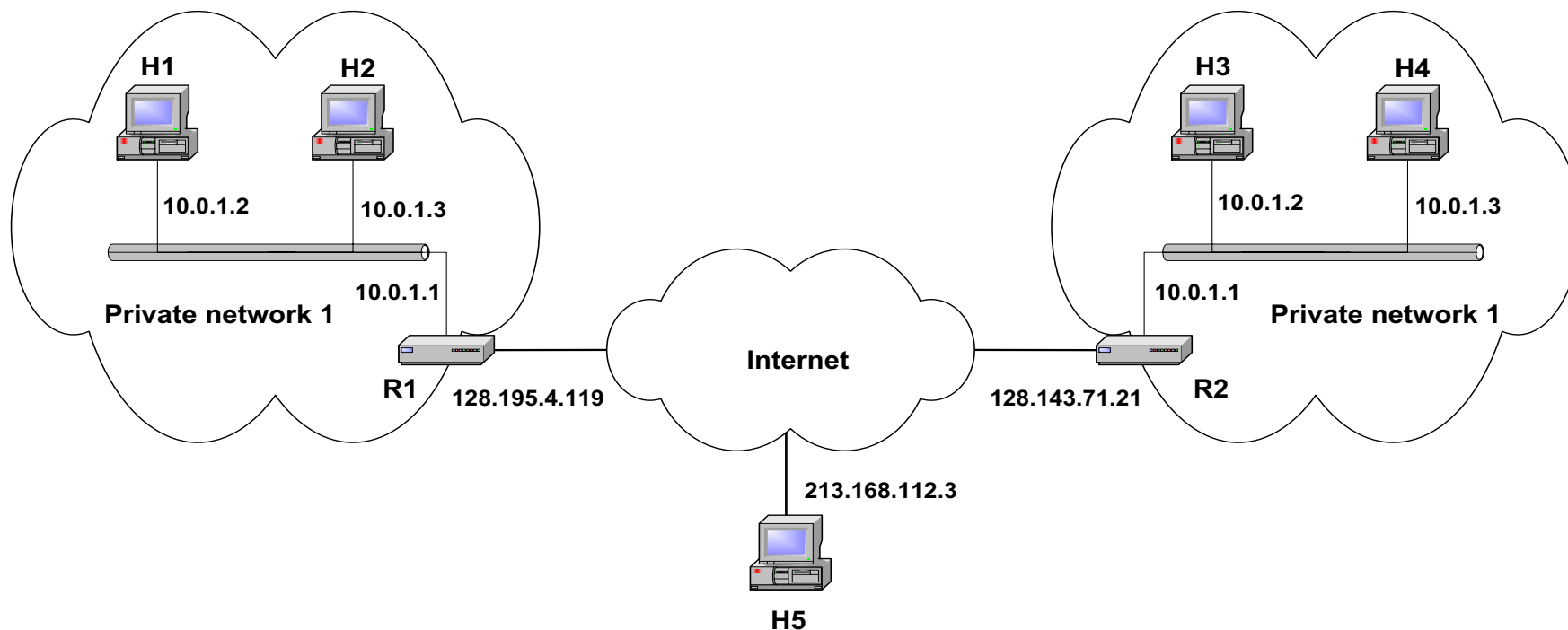
- Oito mensagens usadas na interacção cliente-servidor

Value	Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

NAT

- Network Address Translation
 - Definido no RFC 1631
- Mapeia os endereços IP de redes privadas em endereços IP da internet
 - Permite que os hosts da rede privada partilhem a ligação internet
 - Permite abrandar o esgotamento dos endereços IPv4
- RFC 1597 especifica a gama de endereços reservados para redes privadas
 - Classe A: 10.0.0.0 – 10.255.255.255
 - Classe B: 172.16.0.0 – 172.31.255.255
 - Classe C: 192.168.0.0 – 192.168.255.255

Endereços privados

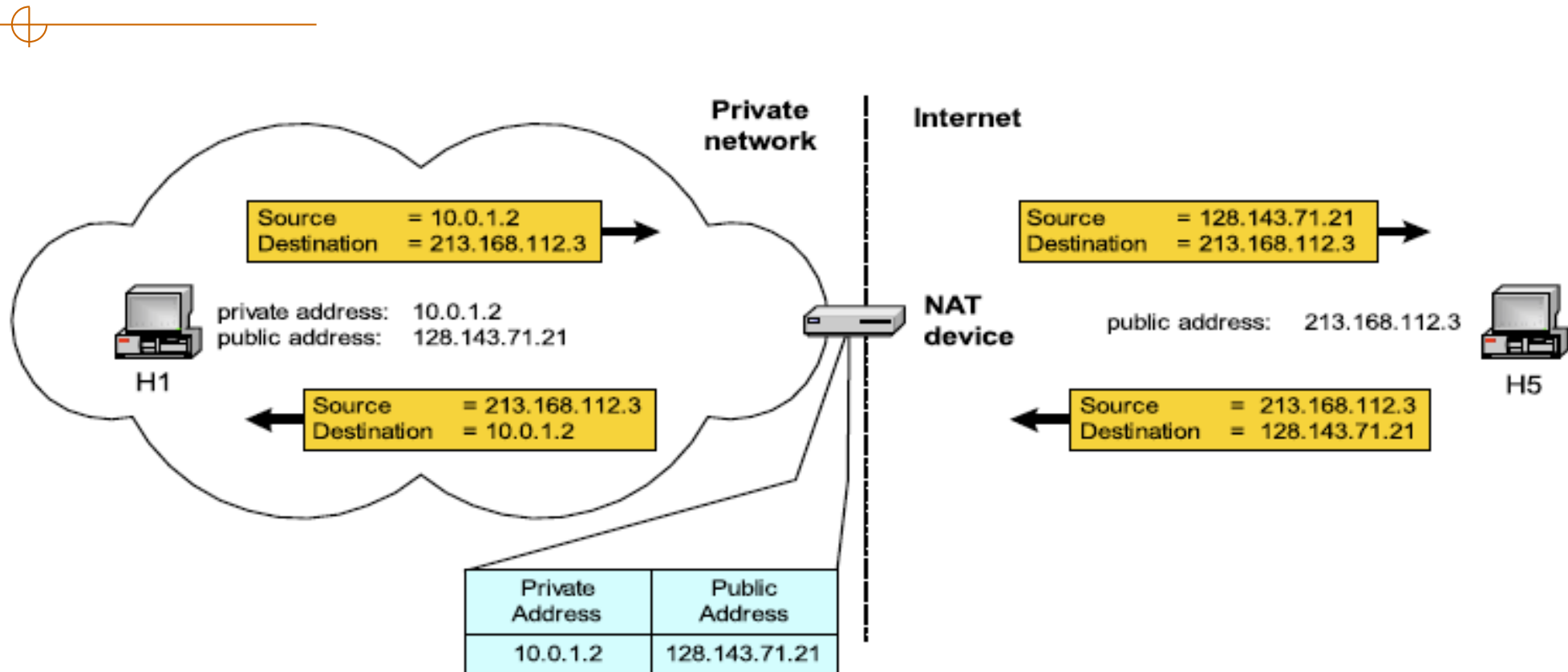




NAT

- NAT corre nos routers fronteira que conectam as redes privadas à internet, substituindo o endereço IP (e eventualmente a porta) de um pacote IP por outro usável na rede pública.
- Permite que os hosts da rede privada comuniquem com hosts da internet

Operação básica do NAT



- O dispositivo NAT possui uma tabela de conversão de endereços



Pooling de endereços IP

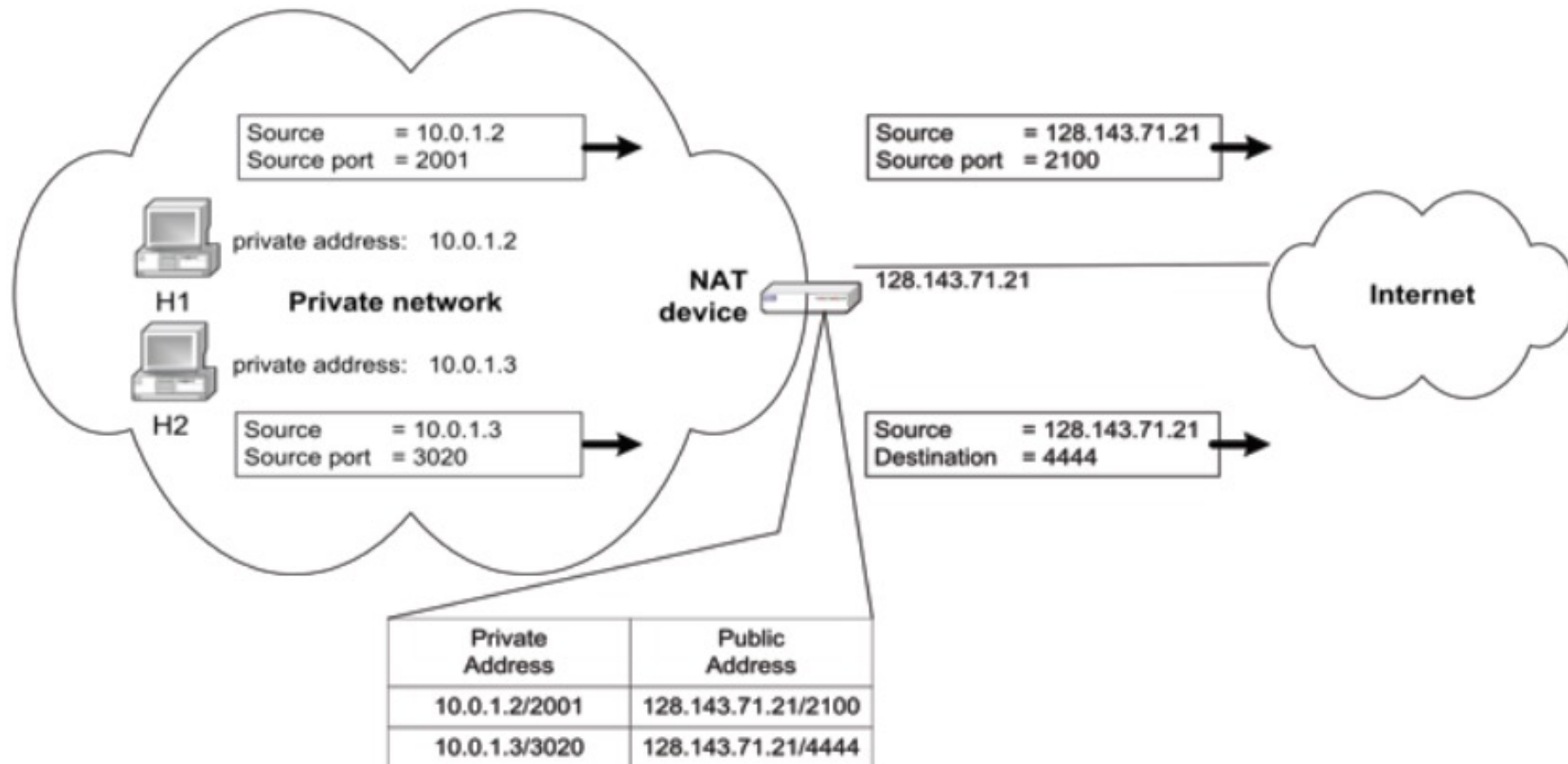
- O dispositivo NAT, localizado na fronteira entre a rede privada e a internet pública, gere uma *pool* de endereços públicos IP
- Quando um hosts da rede privada envia um datagrama a um host da rede pública, o dispositivo NAT escolhe um endereço IP público e associa-o a esse host da rede privada
- Se esse endereço público não é usado por um tempo pré-definido é devolvido à *pool*



IP masquerading

- Também chamado: Network address and port translation (NAPT), port address translation (PAT).
- Permite que um único endereço IP público seja mapeado para múltiplos hosts da rede privada
- O dispositivo NAT modifica o número de porta do tráfego de saída

IP masquerading





Considerações

- **Desempenho:**
 - Modificar o cabeçalho IP pela mudança do endereço IP, envolve que o dispositivo NAT recalcule o campo checksum do cabeçalho IP
 - Modificar o número de porta envolve recalcular o checksum TCP