



NETWORKERS 2004

DNS DEPLOYMENT AND OPERATION

SESSION NMS-2101

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

1

Agenda

Cisco.com

- DNS Basics
- Zone Transfer
- Split DNS
- Moving DNS Servers
- Active Directory
- Dynamic Update

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

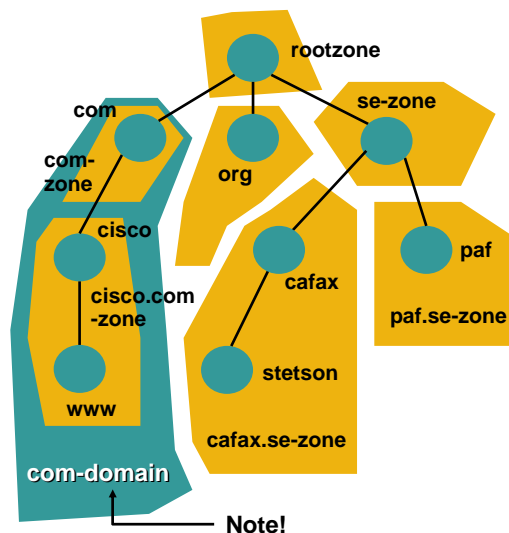
2

Agenda

- **DNS Basics**
- **Zone Transfer**
- **Split DNS**
- **Moving DNS Servers**
- **Active Directory**
- **Dynamic Update**

Domains and Zones

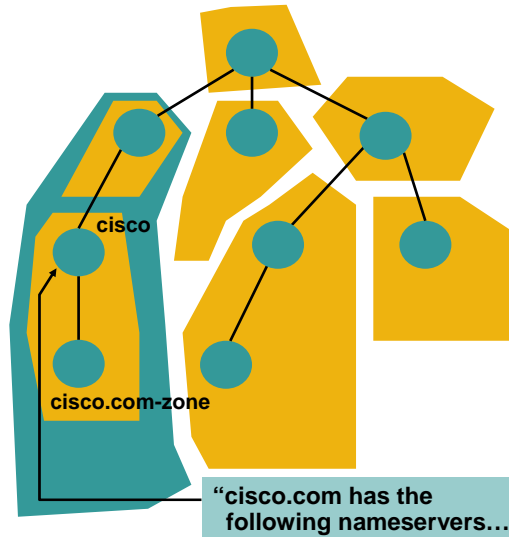
- **Nodes/tokens are grouped in “zones”**
 - Each zone is an administrative unit
 - Each node can be the start of a new zone, but it doesn't have to be
 - A node which is the start of a new zone is called a “delegation point”
- **All nodes below a node is included in the same “domain”**



Domains and Zones

Cisco.com

- “Zone” is a database term, while domain is a namespace term
- Each zone must have nameservers
 - Servers which run the service “respond to DNS queries for names in this zone”
- In the top node in a zone is (among other things) information about where the nameservers are



NMS-2101
9701_05_2004_c2

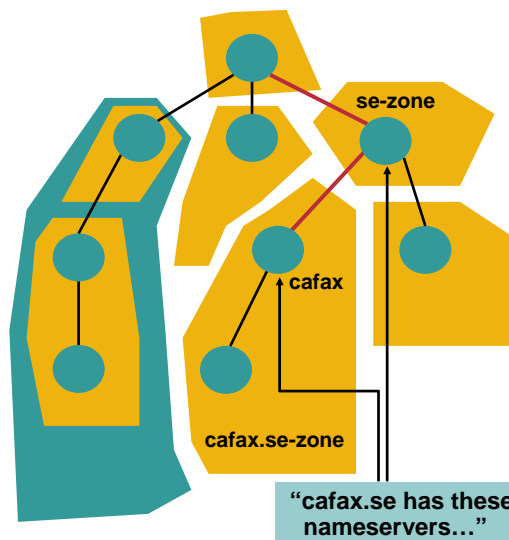
© 2004 Cisco Systems, Inc. All rights reserved.

5

Resolvers and Queries

Cisco.com

- We also have clients which issue queries to servers
 - Those are called “resolvers”
- Goal with DNS is to make sure resolvers find right server to send the query to
 - Information in “parent” zone on where nameservers are for “child” zone



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

6

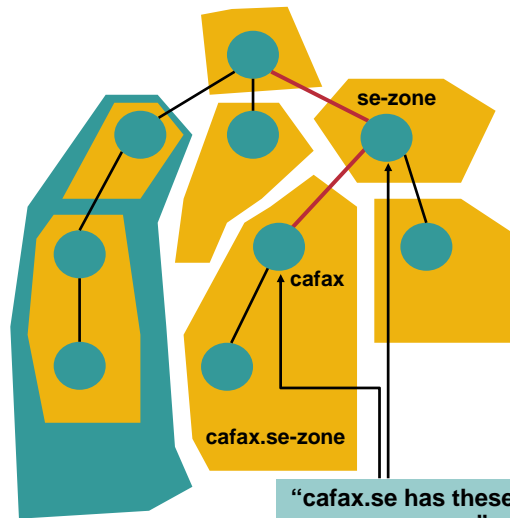
Resolvers and Queries

Cisco.com

- If the parent and child have different view on nameservers, there is something wrong

The information in parent zone has priority (child is authoritative)

Resolvers only find child via information at parent zone, so the parent still have control (resolver might not find any authoritative server for child zone)



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

7

Records

Cisco.com

- A record consists of a left- and right-hand side

Left hand side=name/owner (lookup key)

Right hand side=type of record and data

cisco.com.	4711	IN	A	198.133.219.25
------------	------	----	---	----------------

- The records have different names
- In many cases there are more than one record with the same name

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

8

Queries

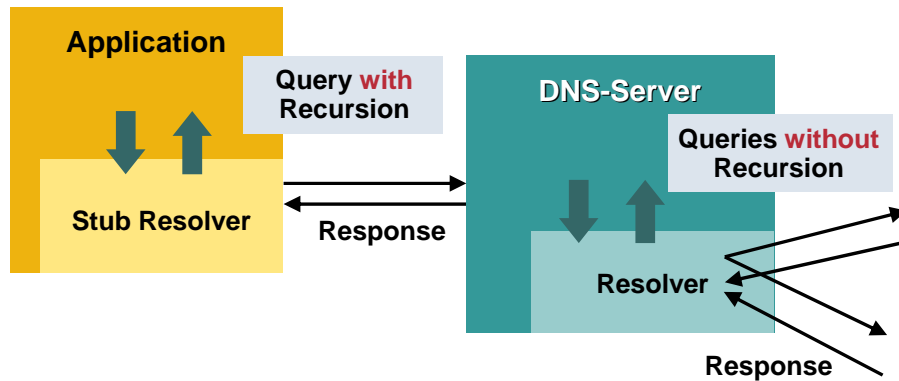
- Lookup is based on name, class and type
- Query for cisco.com:

cisco.com.	?	IN	A	?
------------	---	----	---	---

- Get back the answer 198.133.219.25:

cisco.com.	4711	IN	A	198.133.219.25
------------	------	----	---	----------------

Recursion



The Command “dig” 1(2)

Cisco.com

```
zx81>dig @a.gtld-servers.net. cisco.com. ns +norec

; <<> DiG 9.2.2 <<> @a.gtld-servers.net. cisco.com. ns +norec
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27753
;; flags: qr; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;cisco.com.                IN      NS
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

11

The Command “dig” 2(2)

Cisco.com

```
;; ANSWER SECTION:
cisco.com.          172800 IN      NS      ns1.cisco.com.
cisco.com.          172800 IN      NS      ns2.cisco.com.

;; ADDITIONAL SECTION:
ns1.cisco.com.     172800 IN      A       128.107.241.185
ns2.cisco.com.     172800 IN      A       192.135.250.69

;; Query time: 145 msec
;; SERVER: 192.5.6.30#53(a.gtld-servers.net.)
;; WHEN: Sun Apr 18 15:49:34 2004
;; MSG SIZE rcvd: 95
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

12

Agenda

Cisco.com

- DNS Basics
- **Zone Transfer**
- Split DNS
- Moving DNS Servers
- Active Directory
- Dynamic Update

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

13

Master, Slave, etc.

Cisco.com

- A **master server** is an authoritative server which allow outgoing zone transfers
- A **slave server** is an authoritative server which copy zone content from a master server
- A **primary master** is the master server which holds the zone content
- An **authoritative server** is a server which holds a zone directive for the zone
- A **stealth server** is an authoritative server which is not referred to from parent zone

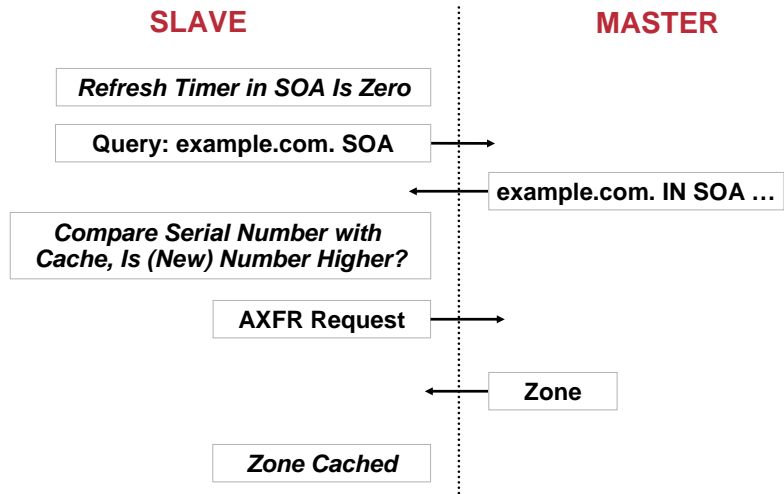
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

14

What Is a Zone Transfer?

Cisco.com



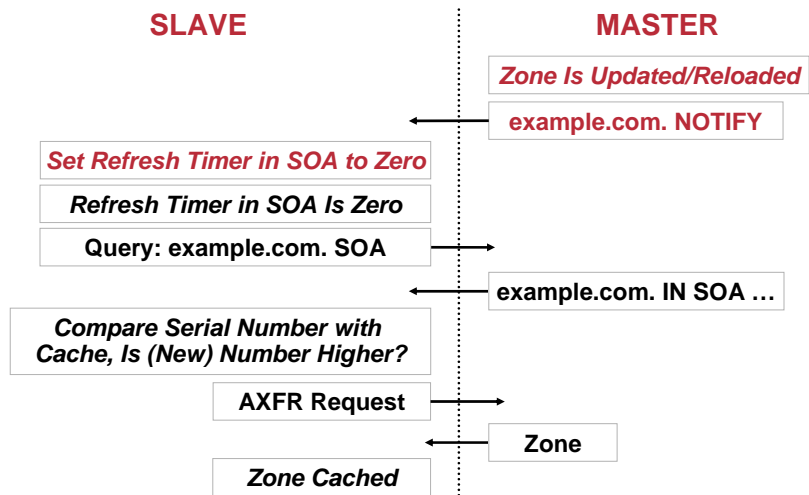
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

15

With DNS NOTIFY

Cisco.com



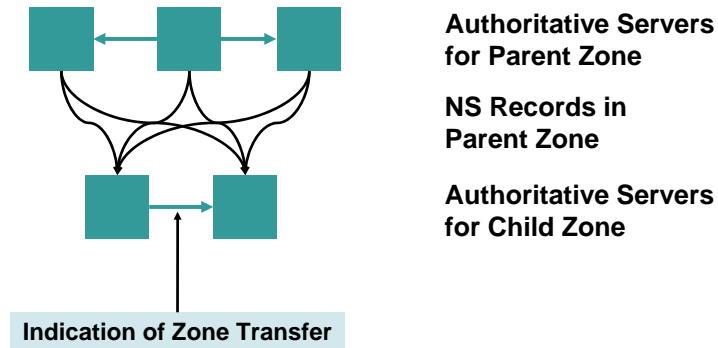
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

16

Master, Slave, etc.

Cisco.com



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

17

Master, Slave, etc.

Cisco.com

- In Parent Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com.  IN A 192.168.1.1  
ns2.example.com.  IN A 192.168.1.2
```

- In Child Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com.  IN A 192.168.1.1  
ns2.example.com.  IN A 192.168.1.2
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

18

Nameserver Configuration

Cisco.com

- ns1.example.com

```
zone "example.com" {
    type master;
    file "example.com";
};
```

- ns2.example.com

```
zone "example.com" {
    type slave;
    file "slave/example.com";
    masters {192.168.1.1; };
};
```

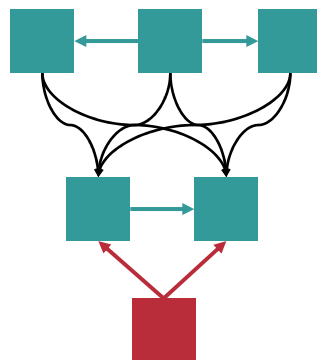
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

19

Add Separate Primary Master

Cisco.com



**Authoritative Servers
for Parent Zone**

**NS Records in
Parent Zone**

**Authoritative Servers
for Child Zone**

**Hidden Master, Not
Accessible from Internet**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

20

With Separate Hidden Master

Cisco.com

- In Parent Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com. IN A 192.168.1.1  
ns2.example.com. IN A 192.168.1.2
```

- In Child Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com. IN A 192.168.1.1  
ns2.example.com. IN A 192.168.1.2  
ns3.example.com. IN A 192.168.1.3
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

21

Nameserver Configuration

Cisco.com

- ns1.example.com

```
zone "example.com" {  
    type slave;  
    file "slave/example.com";  
    masters { 192.168.1.3; };  
};
```

- ns2.example.com

```
zone "example.com" {  
    type slave;  
    file "slave/example.com";  
    masters { 192.168.1.3; };  
};
```

- ns3.example.com

```
zone "example.com" {  
    type master;  
    file "example.com";  
};
```

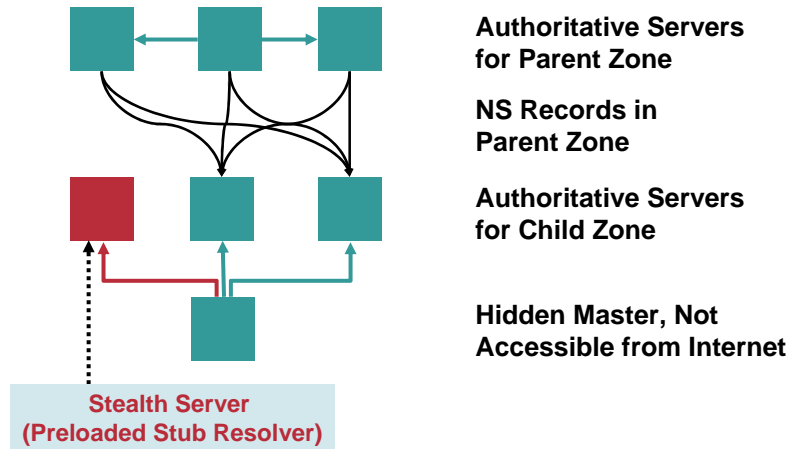
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

22

Add Internal Stealth Server

Cisco.com



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

23

With Internal Stealth

Cisco.com

- In Parent Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com. IN A 192.168.1.1  
ns2.example.com. IN A 192.168.1.2
```

- In Child Zone

```
example.com.      IN NS ns1.example.com.  
example.com.      IN NS ns2.example.com.  
ns1.example.com. IN A 192.168.1.1  
ns2.example.com. IN A 192.168.1.2  
ns3.example.com. IN A 192.168.1.3  
ns4.example.com. IN A 192.168.1.4
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

24

Nameserver Configuration 1(2)

Cisco.com

- ns1.example.com

```
zone "example.com" {  
    type slave;  
    file "slave/example.com";  
    masters { 192.168.1.3; };  
};
```

- ns2.example.com

```
zone "example.com" {  
    type slave;  
    file "slave/example.com";  
    masters { 192.168.1.3; };  
};
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

25

Nameserver Configuration 2(2)

Cisco.com

- ns3.example.com

```
zone "example.com" {  
    type master;  
    file "example.com";  
    also-notify { 192.168.1.4; };  
};
```

- ns4.example.com

```
zone "example.com" {  
    type slave;  
    file "slave/example.com";  
    masters { 192.168.1.3; };  
};
```

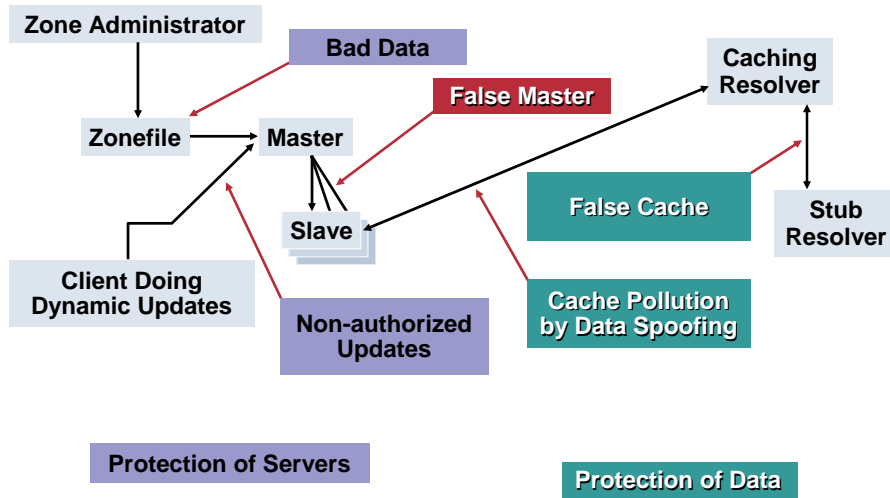
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

26

Security Issues with DNS

Cisco.com



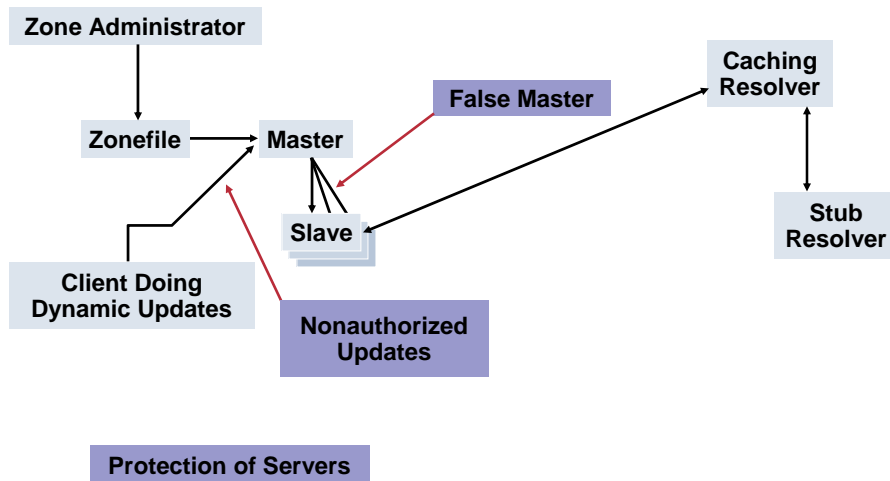
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

27

What TSIG Protects

Cisco.com



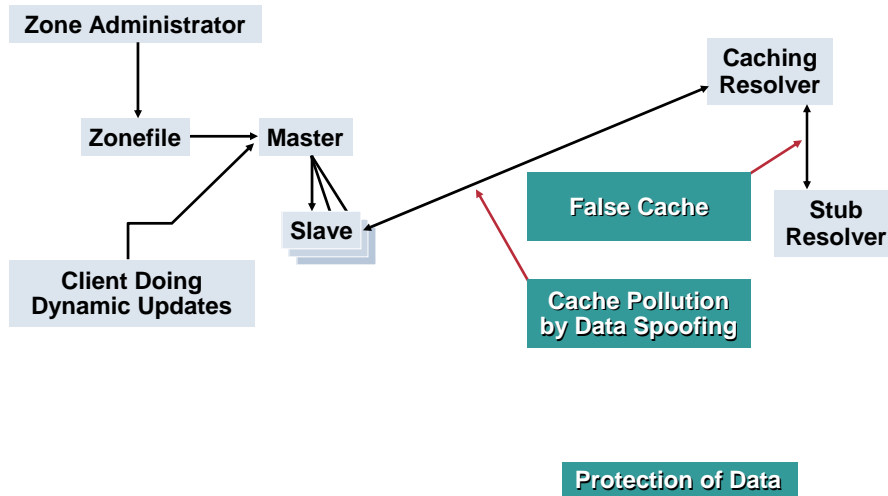
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

28

What DNSSEC Protects

Cisco.com



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

29

Symmetric and Asymmetric Encryption

Cisco.com

- **Symmetric encryption**
 - One key, shared between the parties
- **Asymmetric encryption**
 - One “public” key, distributed widely
 - One “private” key, kept secret
 - What one encrypt with one of the two keys can be decrypted with the other (in both directions)

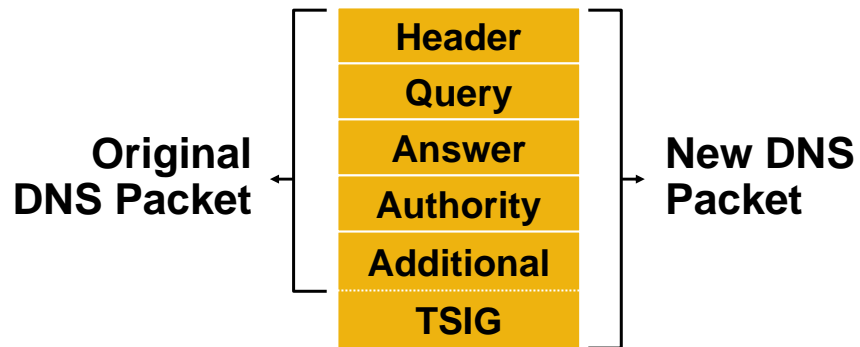
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

30

TSIG Packet

Cisco.com



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

31

TSIG

Cisco.com

- **Pseudo-RR which can not be cached (TTL=0)**
 - Still uses DNS for storage of data
 - For zone transfers (server-server)
 - For queries (resolver-server)
 - Secure the whole message, i.e. the whole DNS packet
 - Uses symmetric encryption, i.e. same key by all parties
- **Works only when one trust the other party**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

32

How to Use TSIG

Cisco.com

- **You have to:**

- Create a symmetric key**

- Configure the key on both servers using a “key” directive**

- Create a connection between the host and key using a “server” directive**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

33

Generate Symmetric Key

Cisco.com

- **Use dnssec-keygen:**

```
dnssec-keygen -a HMAC-MD5 -b 128 \  
-n HOST -r /dev/urandom ns1-ns3.
```

- **It's very important good entropy is used, and /dev/urandom might not be good enough**

- **Result is two files:**

```
Kns1-ns3.+157+24439.key  
Kns1-ns3.+157+24439.private
```

- **dnssec-keygen always generate two files, but when creating symmetric keys, content is same in both**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

34

Key-Statement in named.conf

Cisco.com

- In named.conf on both ns1.example.com and ns3.example.com (ns1-ns3 is a domain name):

```
key ns1-ns3 {  
    algorithm hmac-md5;  
    secret "V6iEJGBGfoo3bBTvY0fNOg==";  
};
```

- Fetch the key material (the secret string) from the files dnssec-keygen produced
- The name of the key is part of the validation process, so it must (also) be the same on both servers which communicate

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

35

Server Statement in named.conf

Cisco.com

- In named.conf on ns1.example.com:

```
server 192.168.1.3 {  
    keys { ns1-ns3; };  
};
```

- In named.conf on ns3.example.com:

```
server 192.168.1.1 {  
    keys { ns1-ns3; };  
};
```

- Result is that all DNS traffic is from now on signed with the given servers (using named keys)
Note: Signed, not encrypted
- Similar configuration on other pairs of host

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

36

Limit Zone Transfer to TSIG Transactions

Cisco.com

- One can add key names to acl's (on ns3.example.com):

```
acl my-slaveservers {
    key ns1-ns3;
    key ns2-ns3;
};
acl my-opsnetwork {
    !192.168.2.1;
    192.168.2.0/24;
};
allow-transfer {
    my-slaveservers;
    my-opsnetwork;
    key john-laptop;
};
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

37

Agenda

Cisco.com

- DNS Basics
- Zone Transfer
- **Split DNS**
- Moving DNS Servers
- Active Directory
- Dynamic Update

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

38

Split-DNS

Cisco.com

- Sometimes information in one zone have to be different on the inside and outside of a firewall
- This breaks the rule about coherence in DNS, and makes troubleshooting **very** difficult
- In Bind 9 views are introduced which makes it possible to give different responses back depending on a number of criteria

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

39

Split-DNS

Cisco.com

- With views one can on one server have different data on the same zone
- The selection is made by the server when a response is to be generated
- Selection can be made on things like
 - Who sends the query (client IP address)
 - Where the query was sent (IP-address, i.e. interface)

NMS-2101
9701_05_2004_c2

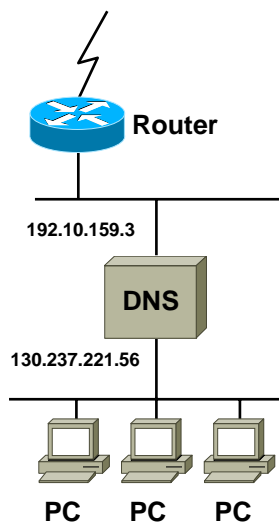
© 2004 Cisco Systems, Inc. All rights reserved.

40

Split-DNS: Example

Cisco.com

```
view "external" {
  match-destinations { 192.10.159.3; };
  zone "example.com" IN {
    type master;
    file "example.com.public";
  };
  ...
};
view "internal" {
  match-destinations { 130.237.221.56; };
  zone "example.com" IN {
    type master;
    file "example.com.private";
  };
  ...
};
```



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

41

Don't Make Mistakes!

Cisco.com

- **Note!**
 - Every query must match one view
 - ...or it will be thrown away
 - All zones must exist in all views
 - ...including root-zone etc
 - Matching is against "addr-match-list"
 - ...which might include TSIG keys

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

42

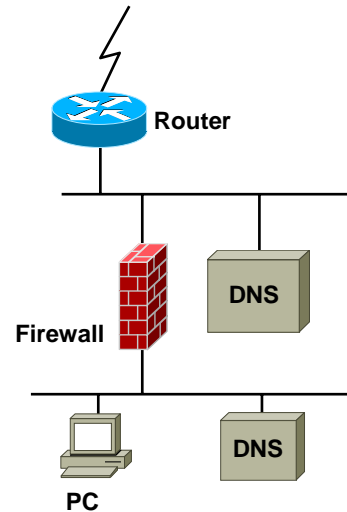
Firewall (DNS Server), Example 1

Cisco.com

- **Same zone content on inside and outside**

Very simple, easy to administer and easy to find errors

RECOMMENDED!



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

43

Firewall (DNS Server), Example 2

Cisco.com

- **Split DNS**

Different information on inside and outside

Pro: Simple to set up

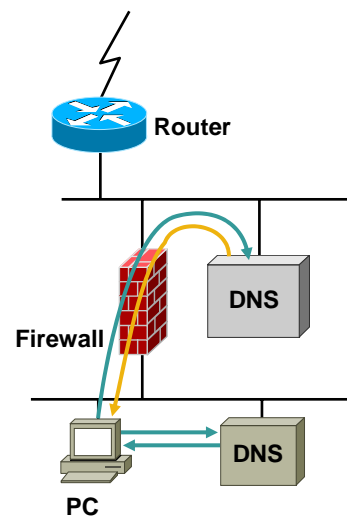
Cons: Inconsistency make debugging hard

- **Internal host send query:**

Q: A for db.example.com?
A: 192.168.1.1

- **External host send query:**

Q: A for db.example.com?
A: Hostname doesn't exist



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

44

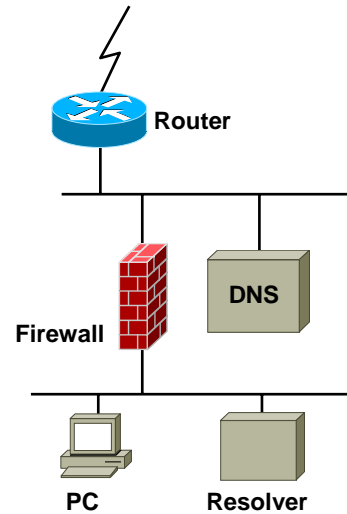
Firewall (Resolver), Example 3

Cisco.com

- DNS on outside which everyone can send queries to
- Resolver on inside which can (according to policy in FW) send queries to any host on the internet

Negative: Must have liberal rule in FW

Positive: Simple



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

45

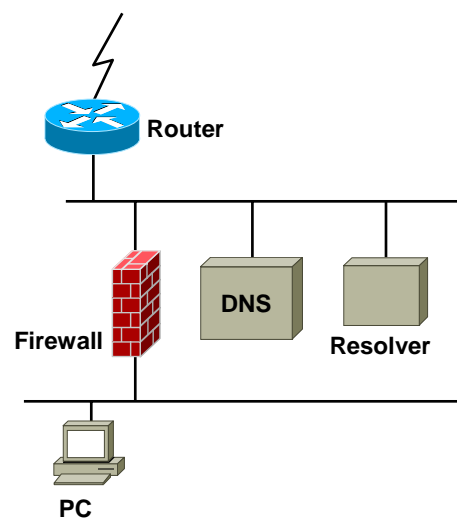
Firewall (Resolver), Example 4

Cisco.com

- DNS server on outside of FW
- Resolver on outside of FW

Negative: Resolver is not protected by FW

Positive: Simple



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

46

Firewall (Resolver), Example 5

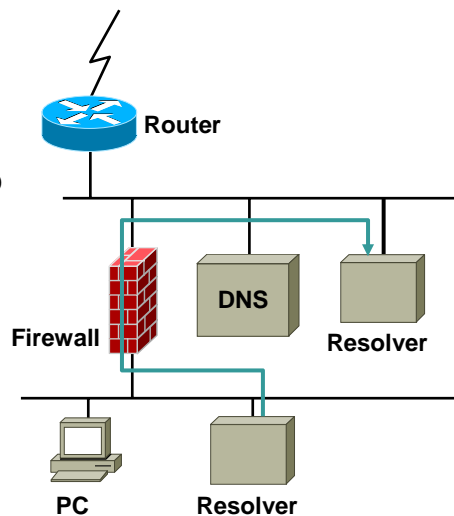
Cisco.com

- DNS server on outside of FW
- Resolver on inside send all queries to stub resolver on outside of FW (forwarding)

Negative: Complicated setup

Positive: Resolver on inside is protected

RECOMMENDED!



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

47

Internal Root Server

Cisco.com

- Sometimes the internal network can not contact the root servers in any way
- One have to have a root server internally
- One will never get responses to external zones

```
zone "." IN {  
    type master;  
    file "db.root";  
};
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

48

Internal Root Zone File (db.root)

Cisco.com

```
. IN SOA x.example.com. hostmaster.example.com. (  
  4711; serial  
  3600; refresh  
  300; retry  
  18600; expire  
  3600; ttl  
)  
. IN NS ns1.example.com.  
. IN NS ns2.example.com.  
. IN NS ns2b.example.com.  
example.com. IN NS ns1.example.com.  
example.com. IN NS ns2.example.com.  
1.168.192.in-addr.arpa. IN NS ns1.example.com.  
1.168.192.in-addr.arpa. IN NS ns2.example.com.  
ns1.example.com. IN A 192.168.1.1  
ns2.example.com. IN A 192.168.1.2  
ns2b.example.com. IN A 192.168.1.2
```

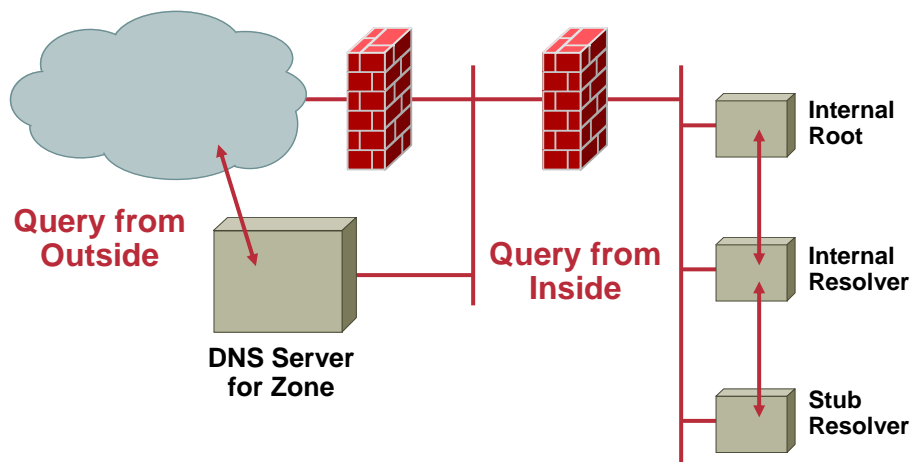
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

49

Internal Root: Example

Cisco.com



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

50

Agenda

Cisco.com

- DNS Basics
- Zone Transfer
- Split DNS
- **Moving DNS Servers**
- Active Directory
- Dynamic Update

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

51

Setting Up a Zone

Cisco.com

- **What is important?**
 1. Your own hosts must be able to issue DNS queries
 2. External hosts must be able to issue DNS queries about zones you administer
- **Two different problems, which should not be mixed up**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

52

Selecting Full-Service Resolvers

Cisco.com

- **Configure them using DHCP**
Even statically assigned IP addresses can be assigned using DHCP (mac address matching)
- **Make sure they have good connectivity**
And good uptime
- **If the host have IPv6 configured, make sure it has IPv6 connectivity**
- **It does not have to be authoritative for any zones**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

53

Selecting Authoritative Servers

Cisco.com

- **Use a hidden primary master**
It will make authorization of changes easier
- **All other authoritative servers will be selected as “slave servers”**
 - One close to your own hosts
 - On your own network
 - Other (two is recommended) distributed on the Internet
 - One at your upstream ISP (if you loose connectivity with your ISP)
 - One at some other ISP (if your ISP looses connectivity)

NMS-2101
9701_05_2004_c2

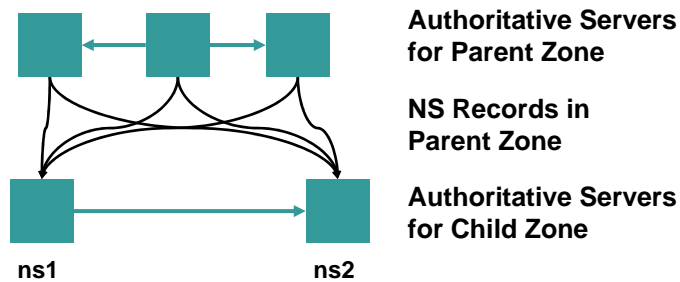
© 2004 Cisco Systems, Inc. All rights reserved.

54

Moving Authoritative Server

Cisco.com

- This is the scenario we will work with
- One of the authoritative servers in child zone will move from one host to another



NMS-2101
9701_05_2004_c2

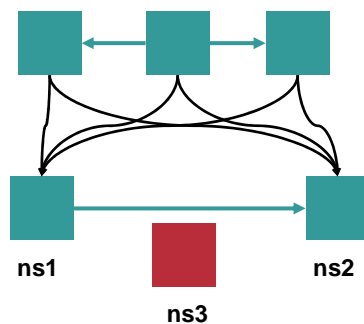
© 2004 Cisco Systems, Inc. All rights reserved.

55

Moving Master, ns1: Step 1

Cisco.com

- Decrease TTL and refresh in SOA
- Set up new master, so both old and new are up at the same time



NMS-2101
9701_05_2004_c2

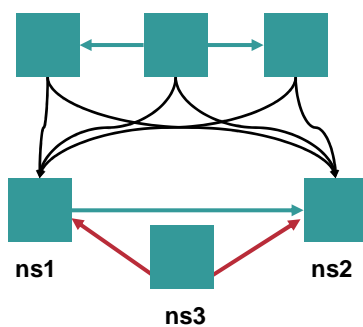
© 2004 Cisco Systems, Inc. All rights reserved.

56

Moving Master, ns1: Step 2

Cisco.com

- Change so old master is slave
- Inform all slave servers



NMS-2101
9701_05_2004_c2

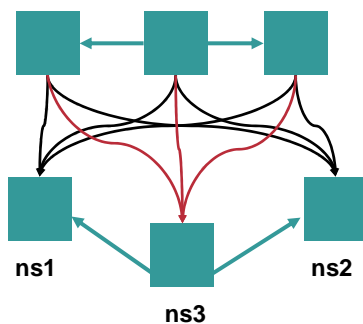
© 2004 Cisco Systems, Inc. All rights reserved.

57

Moving Master, ns1: Step 3

Cisco.com

- Change NS records in your zone
- Inform parent zone
- Pull the plug



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

58

Moving Slave

Cisco.com

- Set up new slave server
- Inform master (access control adjusted?)
- Make sure zone transfer works
- Wait for “ok” from zone owner
 - Master is to update it's zone content plus talk with parent zone
- Wait and log queries
- Wait until queries decrease...pull plug

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

59

Agenda

Cisco.com

- DNS Basics
- Zone Transfer
- Split DNS
- Moving DNS Servers
- **Active Directory**
- Dynamic Update

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

60

DNS and Active Directory

Cisco.com

- **AD is a distributed LDAP database designed to be used as infrastructure for different services in a microsoft environment**
- **AD is completely dependent on DNS because it uses SRV records to find the services and functions**
- **AD offer ability to only use AD (and not DNS) by publishing DNS data directly from AD**
i.e. DNS ends up being an “AD service”

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

61

Active Directory and Dynamic Updates

Cisco.com

- **AD is normally dependent on Windows implementation of dynamic updates in DNS**
 - Windows uses authentication mechanism “GSS-TSIG” (based on Kerberos 5)
 - This is not interoperable with any free open implementation (like for example Bind)
 - This imply it is difficult to integrate “AD zones” with traditional “DNS zones”
 - This is not only bad, because one have different requirements on different kind of zones
 - For example, there is an administrative collision between dynamic updates from clients and requirements on static configuration of server information with requirement on version control

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

62

Active Directory and DNS

Cisco.com

- **If one want to start use AD, there are several possible paths forward:**
 - Stop using traditional DNS, and use only AD**
 - This is recommended by Microsoft (it requires all authoritative servers for all zones to be Microsoft servers)
 - Keep traditional DNS for old zones, and have AD zones in a separate delegated tree**
 - Separate tree can be a subdomain in your existing naming hierarchy, like a new domain name (example2.com) or a subdomain (ad.example.com) when having the main domain example.com
 - Integrate AD in DNS in the same naming structure**
 - More on this follows

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

63

Integrate AD and DNS

Cisco.com

- **Integration of AD and DNS in the same namespace is possible because**
 - A technical detail in on how SRV records work
 - Microsoft implementation of AD
- **All you need are delegations in “example.com” of four subdomains to the AD server(s):**
 - _msdcs.example.com.**
 - _sites.example.com.**
 - _tcp.example.com.**
 - _udp.example.com.**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

64

Agenda

Cisco.com

- DNS Basics
- Zone transfer
- Split DNS
- Moving DNS servers
- Active Directory
- **Dynamic Update**

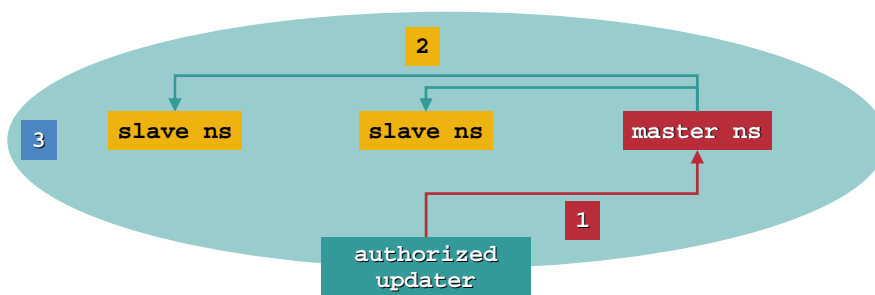
NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

65

Dynamic Update

Cisco.com



- 1** An Update Request Is Sent to the Primary Master
- 2** The Master Send Out a NOTIFY About the Zone Change
- 3** The Slave Servers Update their Zone Content, and Respond to Queries Using the New Data

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

66

Impact of Dynamic DNS Updates

Cisco.com

- **The largest changes from “normal” updates are:**

The zone is always “correct” as the update is in running version instead of a “zonefile” which is reloaded now and then

Security model for “who can change zone data” is changed

From

The people which can edit the zonefile on the computer which is primary master

To

An authentication and authorization (comparison with policy) when update request is received at primary master

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

67

Why Use Dynamic Update?

Cisco.com

- **Mobility is easier**
 - Laptops are not the only devices which uses IP addresses and need domain names
- **Example1: Two laptops want to communicate with each other, even though they use DHCP; they know each others domain names, but have no idea what IP address the other peer have at the moment**
- **Example2: A network of nodes spread over the Internet have the need for use IPSec VPN tunnels between themselves; the domain names are known, but not IP addresses**
- **Conclusion: One need fast, secure updates of the DNS**
- **Platform and proprietary solutions have always exists (DynDNS.org and others), but a standardized version was missing for a long time**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

68

What Is “Secure”

Cisco.com

- The update is both “Authenticated” and “Authorized”

Authentication imply a crypto key is used, either symmetric (TSIG) or assymetric (SIG0)

Authorization imply rules for who can do what, i.e. implementation of policies

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

69

Packet Format #1

Cisco.com

- Dynamic Updates
- RFC 2136 allow updates of any record in the DNS, except information of zone cuts, i.e. data in the delegation point itself
- DNS packet format is not dependent on opcode (QUERY, UPDATE, NOTIFY, etc.)

Because of this the same format is used, but the sections in the packet have different meaning

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

70

Packet Format #2

Cisco.com

- Structure of an Update-message is the same as for any DNS message (header + 4 sections of records)

Section	Size (Octets)	Contains
Header	12	Details
Zone	(name+4)*1	Target
Prerequisite	(name+10+data)*N	Requirements
Update	(name+10+data)*N	Changes
Additional	(name+10+data)*N	Clues

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

71

Packet Format #3

Cisco.com

- “Zone section” tell what zone the update is to take part in
- “Prerequisite section”—requirements for the update
- “Update section”—the new records (can be more than one)
- “Additional section”—proof needed for authentication
- The update is “best effort” (the server can refuse) and “atomic”

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

72

TSIG and SIG(0)

Cisco.com

- **TSIG uses symmetric keys, and used when you trust your DNS operator**
- **SIG(0) uses asymmetric keys, with private key only at client**
- **Both supported by Bind 9 and later**
Not all <9.3.x versions support SIG(0)

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

73

Policies #1

Cisco.com

- **Update-policy define what key have what rights**
What record types can be updated?
Can they key update only one name, or a whole tree?

```
update-policy {  
    grant <keyname> name <domainname> A TXT;  
};
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

74

Policies #2

Cisco.com

- **Example of update-policy**

h1 and h2 can update A and TXT records with the same name as the key

master can update any record in the ex.com domain

```
update-policy {  
  grant h1.ex.com. name h1.ex.com. A TXT;  
  grant h2.ex.com. name h2.ex.com. A TXT;  
  grant master.ex.com. subdomain ex.com. ANY;  
};
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

75

Policies #3

Cisco.com

- **Another example of update-policy**

In this example any key can update A and TXT records which have the same name as the key:

```
update-policy {  
  grant * self * A TXT;  
};
```

- **Note that it is important to use “self” here**
- **update-policy is described further in 6.2.22.4 in BIND ARM**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

76

Configuration: Define Keys

Cisco.com

- **TSIG-key**
(see previous example regarding zone transfer)
Key is stored in `/etc/named.conf`
- **SIG(0)-nyckeln**
The key is stored in the zone file in a **KEY** record
No changes needed in `/etc/named.conf`

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

77

Configuration: SIG(0) KEY

Cisco.com

- **SIG(0)-key**

```
snout.example.net. IN A 192.71.80.82
```

```
snout.example.net. IN KEY 512 3 1 (
```

```
AQPvUTDsgm6QpUMquohFihBVggiKdlVfB9UnO1  
YR24kRZ7N2Ij89bRRHZdBd7zdpmdWlrZu5uIEK  
xcZI3LM6DVszTxAOx6Nte+ZOeV8oCG/jIS4NJa  
Q4GgNkgA+WAIH71lvfG7PsygdTx8OmH83z39ft  
69Kuodmbj091cqQ==) ; key id = 14684
```

- **Used by the nameserver to verify the SIG(0) signature on the update request**

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

78

Configuration: Define Policy

Cisco.com

- **Server side: named.conf**

```
zone "example.net" {  
  type master;  
  file "...";  
  update-policy {  
    grant key.laptop.example.net.  
      name laptop.autonomica.net. A TXT;};  
};
```

Key

Only This Name

Record Types

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

79

Updating the Records: nsupdate

Cisco.com

- **Tool to generate dynamic update requests**
- **Support both TSIG- och SIG(0)-based dynamic updates**
- **It is important to think about**
 - How the keys are stored which nsupdate uses
 - How nsupdate is triggered, and by what

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

80

nsupdate with TSIG

Cisco.com

```
% nsupdate -k Ktwo.dyn.cafax.se.+157+57806.  
> zone dyn.cafax.se.  
> server 192.71.228.192  
> update add two.dyn.cafax.se. 900 TXT "New stuff"  
> send  
% dig @192.71.228.192 two.dyn.cafax.se. txt
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

81

nsupdate with SIG(0)

Cisco.com

```
% nsupdate -k Kone.dyn.cafax.se.+001+50281.  
> server 192.71.228.192  
> zone dyn.cafax.se.  
> update add one.dyn.cafax.se. 900 txt "adding this"  
> show  
Outgoing update query:  
;; ->HEADER<<- opcode: UPDATE, status: NOERROR, id: 0  
;; flags: ; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0  
;; UPDATE SECTION:  
one.dyn.cafax.se. 900 IN TXT "adding this"  
> send
```

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

82

Summary

Cisco.com

- **We have talked about a number of things**
 - DNS basics
 - Zone transfer
 - Split DNS
 - Moving DNS servers
 - Active directory
 - Dynamic update
- **But, some things have not been covered**
 - IPv6
 - DNSSEC

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

83

Q AND A



NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

84

Complete Your Online Session Evaluation!

Cisco.com

- WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing
- WHY:** Win fabulous prizes! Give us your feedback!
- WHERE:** Go to the Internet stations located throughout the Convention Center
- HOW:** Winners will be posted on the onsite Networkers Website; four winners per day

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

85

Other Network Management Sessions

Cisco.com

- NMS-1N01—Introduction to Network Management—Networkers Online
- NMS-1N02—Introduction to SNMP and MIBs—Networkers Online
- NMS-1N03—Accurate Time Synchronization—Networkers Online
- NMS-1N04—Introduction to Service Assurance Agent—Networkers Online
- NMS-1N41—Introduction to Performance Management—Networkers Online
- NMS-1011—Principles of Fault Management
- NMS-1101—Understanding DNS and DHCP
- NMS-2001—Network Troubleshooting Tools and Techniques
- NMS-2021—Large Scale Deployments of CiscoWorks
- NMS-2031—Traffic Accounting Scenarios
- NMS-2032—NetFlow for Accounting, Analysis and Attack
- NMS-2042—Performance Measurement with Cisco IOS
- NMS-2051—Securely Managing Your Network
- NMS-2102—Deploying and Troubleshooting NAT
- NMS-3011—Getting the Right Fault Events from Network Elements
- NMS-4012—MPLS Embedded Management Tools
- NMS-4043—Advanced Service Assurance Agent
- NMS-2T00—Network Management Best Practices—Techtorial

NMS-2101
9701_05_2004_c2

© 2004 Cisco Systems, Inc. All rights reserved.

86

CISCO SYSTEMS

