**Proiect susținut la Sisteme de Operare Avansate:**

**Sistemul DNS- Arhitectură și Securitate**

**Profesor coordonator:** Masterand:

**Conf. Dr. Ing. Ștefan Stăncescu** Deaconescu Claudia-Daniela

**Cuprins**

# Introducere ……………………………………………………………………….…….. 4

# Capitolul 1. DNS ………………………………………………………………………. 6

# Arhitectura DNS ………………………………………………………………… 6

# 1.2. Serviciu Domeniu Nume (DNS) ………………………………………………...… 6

# Servere DNS …………………………………………………….………………….. 9

## **Capitolul 2. Securitatea DNS … ………………………………………………. 13**

* 1. Securitatea extensiilor DNS ……………………….………………………………. 13

2.2 Asigurarea spațiului de nume DNS ………………….……………………………. 14

# Bibliografie ……………………………………………………………………………. 15

**Lista figurilor**

Figura 1.1 ……………………………………………………………………………….. 6

Figura 1.2 ……………………………………………………………………………….. 7

Figura 1.3 ……………………………………………………………………………… 11

# Introducere

Domain Name Server (DNS) se utilizează de fiecare dată când se trimite un email, sau atunci când se accesează o pagină web. Orice rețea funcționează prin alocarea unei adrese IP unice, care poate fi locală sau globală, către fiecare nod final (calculator, server, router, interfață etc.). În situația în care nu sunt asignate numele corespunzătoare pentru fiecare resursă, tot timpul când se dorește accesarea unei resurse disponibile, de exemplu un site web, va fi necesar să se cunoască adresa IP fizică. Numărul foarte mare de calculatoare și milioane de site-uri web va face imposibil asignarea acestor resurse.

În vederea rezolvării acestei probleme, conceptul de name server a apărut la mijlocul anilor 1970 pentru a asigura câteva atribute resurselor. În acest caz adresa IP a unui site, a putut fi păstrată într-o locație cunoscută, idea de bază a subliniat faptul că este mult mai ușor de reținut numele, în comparație cu o adresă numerică.

Când un name server este prezent într-o rețea, fiecare calculator are nevoie să cunoască adresa fizică a name server-ului și numele resurselor, un site web de exemplu, pentru a-l accesa. Folosind această informație, se poate găsi adresa resurselor prin interogarea name server-ului. Resursele pot fi adăugate, mutate, schimbate sau șterse dintr-o singură locație, name server, și informațiile noi pot fi imediat disponibile pentru fiecare calculator care utilizeaază acest name server. Cu alte cuvinte name server-ul este translatat intr-o adresă IP și invers. Prin utilizarea DNS-ului rețeaua devine mult mai dinamică

O primă soluție la problema disponibilității unui name server a fost aceea de a introduce name servere Primare si Secundare. Dacă name serverul Primar nu răspunde la o interogare, gazda va reîncerca utilizarea name server-ului Secundar. În prezent un name server poate vedea o listă de trei, patru, sau mai multe name servere. Termenul de name server Primar și Secundar și ulterior name server Terțiar va implica în continuare o prioritate de acces indiferent de disponibilitatea name server-lui.

Multiple software-uri pentru name servere sunt utilizate pentru acces aleatoriu, măsurarea timpului de răspuns sau accesul round-robin la lista de name server pentru a încerca și extinde solicitările și a micșora timpul de acces.

Pentru a se extinde rețeaua noastră vom începe să creăm un număr mare de nume în name servere-le noastre. Acest lucru va genera trei probleme:

1. Organizare: Găsirea oricărei intrări în bază de date a numelor va deveni tot mai lentă ca atunci când milioane de nume încearcă să se conecteze la cel pe care îl doresc. Vom avea nevoie de o metodă pentru a indexa și organiza numele.
2. Scalabilitate: Dacă fiecare gazdă este accestă de name servere, solicitarea devine foarte mare. Va fi necesară o metodă de a răspândi această solicitare de-a lungul unor name servere.
3. Management: Cu foarte multe nume înregistrate in baza noastră de date, problema administrării devine din ce în ce mai dificilă, ca multe încercări de administrare a acualizărilor înregistrate în același timp. Va fi nevoie de o metodă de separare (cunoscută sub denumirea de “delegare”), de administrare a acestor nume înregistrate (cunoscute general sub denumirea de resurse).

Nevoia de a satisfice aceste trei cerințe implică cunoașterea conceptului de Internet Domain Name System (DNS).

1.I Domeniul Internet pentru numele sistemului (The Internet Domain Name System)

Domeniul Internet pentru numele sistemului reprezintă o implementare specifică a conceptului de nume server optimizat pentru condițiile răspândite în Internet. Făcând referire la scurta istorie a numelui serverelor, se pot remarca trei concepte care au apărut:

1.a Necesitatea pentru o ierarhie a numelor

1.b Necesitatea de a extinde încercările operaționale la numele serverelor noastre

1.c Necesitatea de a desemna administrarea numelor serverelor noastre.

Internetul DNS rezolvă în mod elegant toate aceste trei concepte.

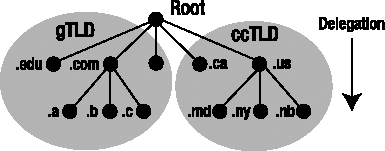
1.II Domenii și desemnări

Domeniul Nume Sistem utilizează structuri de nume ierarhizate (arborescente). În varful ierarhiei este nodul rădăcină urmat de către nodul TLD (Domeniul nivelului de sus), după de SDL (Domeniul celui de-al doilea nivel) și un număr de nivele de jos, fiecare separate cu un punct.

TLD este împărțit în două tipuri:

1. Domeniul Generic al Primului Nivel (gTLD), utilizat de exemplu pentru: .com, .edu, .net, .org, .mil, etc.
2. Domeniul Codului Tării al Primului Nivel (ccTLD), utizat de exemplu pentru: .us, .ca, .tv, .uk,etc.

Cele menționate anterior pot fi reprezentate și din punct de vedere grafic:



Un domeniu de nume este, de exemplu un site web, este în mod normal o combinație între un nume SDL și un nume TDL și este scris de la stânga la dreapta cu nivel de jos al ierarhiei din stânga și nivelul de sus din dreapta.

Termenul Domeniul de nivel Secundar este precis din punct de vedere tehnic și definește noduri de nivelul doi în ierarhia domeniului de nume, dar apare impedimentul cu privire la lungime. De asemenea Domeniul al Treilea impune o lungime mai mare, dar este relevant în cazul ccTLDs. General Domeniul de nume este utilizat în special pentru a descrie o entitate desemnată, de exemplu un site, care are în componență SLD și TLD

**Capitolul 1. DNS**

# *Arhitectura DNS*

Din punct de vedere arhitectural se ține cont de domeniu de aplicație (logica de transport) și domeniile tehnologice. EPC (Electronic Product Code)- Codul elctronic al produsului, este un identificator universal, bazat pe Identificatorii de Resurse Universali (URIs). EPC asigură tot timpul o identitate unică pentru fiecare obiect fizic.

Serviciul Nume Obiect (ONS) este un serviciu de rețea automat similar cu Serviciu Domeniu Nume (DNS). Când o interogare citește eticheta RFID a unui produs, EPC (Electronic Product Code) este blocat și interogările ONS la nivelul unei rețele locale din Internet găsesc informații unde este stocat produsul. Rezultatul acestor interogări este acel server unde un fisier legat de produs este stocat.

# *1.2 Serviciu Domeniu Nume (DNS)*

DNS este un serviciu cu un nivel vast în ceea ce privește infrastructura Internetului, utilizat pentru a descoperi informații despre numele domeniului și pentru a translate un nume gazdă într-o adresă IP. DNS pentru Internet utilizează anumite nume de domenii pentru a identifica gazda.

Figura următoare ilustrează conceptul de logică de transport:

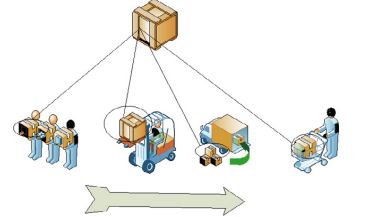


Figura 1.1

Echipamentul logistic este un alt tip de obiect logistic care este utilizat pentru a transporta alte obiecte logistice, incluzând alte obiecte ale echipamentelor logistice. De exempu, un container livrat este un obiect al echipamentului logistic, care poate transporta alte obiecte logistice precum cutii de carton. Figura 1.1 ilustrează câteva tipuri de pachete logistice în cutii (unități logistice), care sunt transportate de echipamente logistice precum camioane stivuitor și camioane de livrare.

Structura experimentală a arhitecturii DNS:

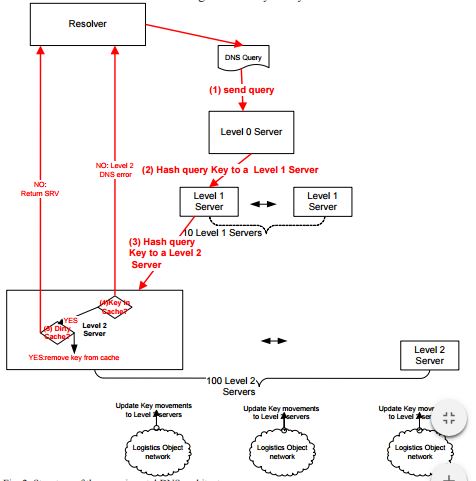


Figura 1.2

Pentru a întelege comportamnetul DNS ca un subdomeniu este necesară extrapolarea comportamentului întregului sistem DNS. În acest caz au fost adoptate trei nivele în arhitectura DNS, dupa cum se observă și în figura 1.2. Nivelul de sus al serverului (Server Level 0), responsabil pentru tratarea interogărilor DNS în vederea rezolvării acestora. În cazurile reale acestea trebuie să fie implementate ca niște clustere de servere. Totodată mai avem nevoie de zece servere autorizate de nivele 1, care corespund cu majoritatea subdomeniilor în interiorul unui domeniu principal. În schema mai sunt 100 de servere autorizate de nivel 2, responsabile pentru a menține direcția rețelei de la gazdă către obiectele logistice. Fiecare dintre serverele de nivel 2 mențin serviciul înregistrat (SRV) la câteva obiecte logistice. Un SVR înregistrat conține informații despre TTL (time to live), nume gazdă, numărul portului etc, dacă serverul obiectului este asociat cu cu un serviciu asigurat de către obiect pentru o locație fizică, și alte informații relevante de acest gen.

# *1.3 Servere DNS*

# Specificațiile DNS definesc două tipuri de nume servere (nameservers): primul diresctor și al doilea director. Primul director al numelui de server pentru o zonă este cel care citește datele dintr-un fișier al gazdei. Cel de-al doilea director al numelui server este cel care primește o zonă de date de la un alt nume server autorizat pentru zona respectivă, numit server director. Destul de des, serverul director este în zona primului director, dar nu este necesar acest lucru, de aceea va exista un al doilea director care încarcă o zonă de date cu alta secundară. Când această zonă secundară iși începe procesul de pornire va contacta numele server director și dacă este necesar va extinde zona de date. Acest lucru se referă la o zonă de transfer.

# În prezent, termenul preferat pentru un director secundar al numelui server apare sub denumirea de “slave”, cu toate acestea multe persoane (și anumite software-uri, incluzând consola DNS Microsoft) utilizează în continuare vechiul termen. Amândoua, atât directorul primar cât și numele server slave pentru o zonă sunt autorizate pentru zona respective. De notat este faptul că directorul secundar al numelui server (slave) copiază datele de la un calculator la un alt calculator pentru a crea noi nume servere pentru zona respective. Trebuie în mod normal să fie setat numele server slave pentru a încărca datele lor de la directorul primar din zona respective. “Sclavii” (slaves) sunt setați să transfere noi zone de date atunci când este necesar. Nume servere sclavi (slave nameserver) sunt importante deoarece este este o idee foarte bună de a seta mai mult de un nume server autorizat pentru fiecare zonă primită. Este nevoie de mai mult de un server setat pentru redundanță, pentru a extinde solicitările și a face posibil faptul că toate calculatoarele din zonă va avea un nume server închis. Utilizând nume servere secundare se va crea un spațiu de lucru administrativ.

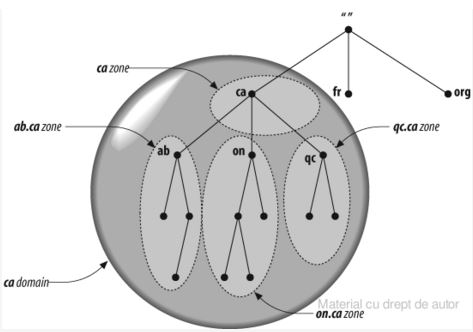
# Se poate menționa faptul că un nume server poate fi autorizat pentru mai multe zone. Similar un nume server poate fi un director primar (primary master) pentru o zonă și un director sclav (slave) pentru alta. Mai multe nume servere sunt primare sau secundare pentru mai mute zone pe care le solicit. Dacă se utilizează un nume server particular care este primar sau sclav, acest lucru înseamnă că acesta este primar sau slave pentru mai multe zone la care este autorizat.

# În continuare am atașat o figură care corespunde cu modul în care un domeniu se împarte în zonele corespunzătoare:

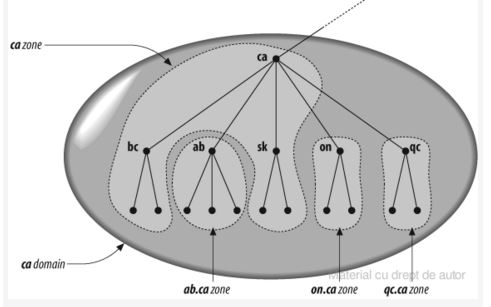
# C:\Users\Serj\Desktop\clauss capuri\Capture 5.JPG

# O zonă care conține toate numele de domenii cu același nume de domeniu, este împărțit în subdomenii. De exempu, nivelul de sus al domeniului este împărțit în subdomenii precum: cc., ce. , cs. , me. Autoritatea în fiecare din aceste subdomenii este delegate de un nume server în fiecare dintre acestea.

În continuare (în figura următoare) se poate observa că domeniul ca. conține toate datele în ab.ca, on.ca și qc.ca. Cu toate acestea, zona ca. conține doar date de aceea majoritatea pointerilor sunt delegați în subdomeniile ab.ca, on.ca și qc.ca sunt zone separate față de zona ca.



Zona conține de asemenea nume de domenii și date in fiecare subdomeniu care nu sunt delegate în afară. De exemplu, subdomeniile care aparțin domeniului și anume bc.ca și sk.ca pot exista însănu pot fi delegate. În acest caz zona ca. are un buton pe margine care conține subdomeniile bc.ca și sk.ca dar nu conțin alte subdomenii ca. acest lucru fiid ilustrat în figura următoare:



▶ Subdomeniu delegate

Deși nu este nevoie să fie delegate anumite părți din domeniul utilizat , însă este important de înțeles cum funcționează procesul de delegare al unui subdomeniu. Acest process implică responsabilități de asignare a unei anumite părți a subdomeniului spre o altă organizare. Ceea ce se întâmplă în realitate este de asignare a autorității unui subdomeniu la diferite nume servere. Zona de date, conține în schimb informații în subdomeniul pe care îl delegăm, incluzând pointeri pentru nume server ce sunt autoritare pentru acel subdomeniu.

▶ Zona cu fișiere de date

Fișierele pentru fiecare director primar de nume server încarcă zonele de date pentru care este solicitat cu zone ce conțin fișiere de date. Acestea poartă denumirea de datafiles. Numele server Slave poate de asemenea să încarce zonele sale de la aceste fișiere de date. Sclavii (Slaves) sunt configurați de obicei ca zonă de date de back-up și transferă de la un nume server Master către fișierul de date. Dacă serverul Slave este ulterior restartat, va citi prima dată fișierul de date de back-up și după va verifica să vadă dacă zona de date este cea curentă. Aceste două particularități înlătură necesitatea de a transfera zona de date dacă nu se produc anumite modificări și dacă asigură datele atunci când serverul Master nu funcționează. Fișierul de date conține resurse stocate care descriu zona. Resursele stocate descriu toate calculatoarele din zona respective și relaizează delegăriile de subdomenii.

▶ Nume server rădăcină

Nume server rădăcină este un nume server autoritar pentru fiecare zonă de la nivelul cel mai de sus. (De fapt, anumite nume servere rădăcină sunt autoritare pentru anumite zone generice pentru nivelul de sus). Atunci când se primește o interogare despre oricare nume de domeniu, numele server rădăcină poate să asigure numele și adresa ale numelor server pentru care sunt autoritare pentru zona cu nivelul cel mai de sus pe care il conține numele de domeniu respectiv.

Oricare interogare de nume server primește informații de interogare despre cât de aproape se află de răspunsul căutat sau asigură el însuți răspunsul căutat. Numele server rădăcină este important ca rezoluție. Deoarece acesta este atăt de important, DNS asigură mecanisme precum “caching”, pentru a ajuta la eliminarea numelui server rădăcină. Dar în absența altei informații, rezoluția incepe la nivelul nemelui server rădăcină. Acest lucru face ca numele server rădăcină să fie crucial în operația DNS, dacă tot Internetul numelui server rădăcină este inaccesibil pentru o perioadă extinsă de timp, toată rezoluția a Internetului va eșua. Pentru a Evita acest aspect, Internetul are 13 nume server rădăcină extinse de-a lungul diferitelor părți ale rețelei. Una dintre acestea este PSINet, o rețea “backbone” Internet comercială, o alta este NASA Science Internet, două sunt în Europa și una în Japonia. Fiind punctul central pentru foarte multe interogări ține rădăcinile ocupate, chiar și cu 13 rădăcini, traficul la nivelul fiecărui nume server rădăcină este foarte ridicat. Figura următoare arată procesul de rezoluție pentru o adresă la un calculator real într-un domeniu real, incluzând procesul de corespondență prin care se traversează ierarhia domeniului namespace.

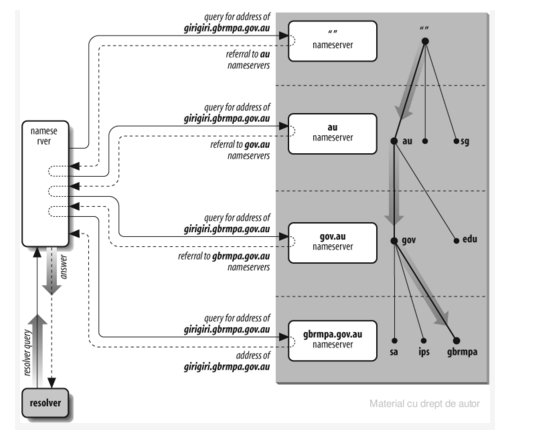


Figura 1.3

Numele server local interoghează numle server rădăcină pentru adresa “girigiri.gbrmpa.gov.au” și se referă la numele server “au”. Numele server local interoghează un nume server “au” și se referă la numele server “gov.au”. Numele server “gov.au” se referă la numele server local “gbrmpa.gov.au”. În cele din urmă, nemele server local interoghează numele server “gbrmpa.gov.au” pentru adresă și primește răspunsul.

▶ Translatarea adreselor în nume

Unul din elementele fundamentale care lipsesc din procesul de rezoluție poate fi explicat prin faptul că adresele pot fi translatate în nume de domenii. Adresa nume translatează informația de ieșire într-o forma mai ușoară pentru utilizator pentru a o putea citi și interpreta (în logfile de exemplu). Este de asemenea utilizată în anumite verificări autorizate. Calculatoarele UNIX mapează adresele în nume de domenii pentru a le compara cu intrările .rhosts și hosts.equiv files de exemplu.

Datele, incluzând adresele, într-un domeniu namespace este indexat prin nume. Atunci când se primește un nume de domeniu, se găsește o adresă relativ ușor. Dar a găsi un nume de domeniu pentru a oferi o adresă este o muncă mai dificilă care necesită anexarea fiecărei date la fiecare nume de domniu din ierarhie.

Adresa IP poate fi reprezentată opus în nume server, cu primul octet din adresa IP la sfârsit în cazul numelui domeniu. Adresa IP este ierarhică la fel ca și numle de domeniu.

## **Capitolul 2. Securitatea DNS**

*2.1 Securitatea extensiilor DNS*

▶ De ce este importantă securitatea DNS.

Întotdeauna când se conectează calculatoarele la nivelul rețelei locale este mai sigur să fie trimisă parola într-un mesaj clar, astfel încât în afara rețelei locale nu va exista o altă rețea privată. Dacă numele server este capabil să primească pachete UDP pe portul 53 din afara rețelei locale, atunci utilizatorul este conștient că securitatea nu este la un nivel ridicat.

DNSSEC (Domain Name System Security Extensions) asigură originea de autentificare a datei și integritatea datei pentru numele sistem al domeniului (Domain Name System). Acest lucru include mecanisme pentru existența autentificărilor din DNS. Aceste mecanisme sunt descrise în continuare. Mecanismele de care am amintit necesită schimbări ale protocolului DNS. DNSSEC adaugă patru tipuri de resurse înregistrate: RRSIG ( Resource Record Signature), DNSKEY (DNS Public Key), Delegation Signer (DS), și NSEC (Next Secure). De asemenea sunt adăugate două noi mesaje de început: Checking Disabled (CD) și Authenticated Data (AD). Cu toate acestea, pentru a suporta mesaje DNS de mărime mai mare este necesar adăgarea DNSSEC OK (DO) ENDS header bit [RFC3225] care va asigura securitatea ce indică acele interogări ce sunt așteptate să fie primite de la DNSSEC RRs în mesajul de răspuns. Aceste servicii protejează împotriva amenințărilor către Domain Name System descrise în [RFC3833].

Originea de autentificare a datei și integritatea datei.

DNSSEC asigură autentificarea prin asocierea criptografică a semnăturii digitale cu DNS RRsets. Aceste semnături digitale sunt stocate într-o nouă resursă înregistrată. În mod normal, trebuie să existe o singură cheie privată care să semneze o zonă de date, dar sunt posibile și mai multe chei. De exemplu, pot exista chei pentru fiecare semnătură digitală ce corespunde diferitor algoritmi. Un concept DNSSEC important este acela ca o cheie de autentificare să indice că o zonă de date este asociată cu însăși acea zonă și nu cu o zonă autoritară cu un nume server. Cheile asociate cu o Securitate înregistrată pot fi stocate în diferite tipuri RR. De notat că acele chei private utilizate pentru a indica o zonă de date trebuie ținute în siguranță și deconectate în practică. Pentru a descoperi o cheie publică fiabilă cu rezoluția DNS această cheie trebuie să fie semnată de o cheie de autentificare configurată sau o cheie care a fost autentificată în prealabil. Asigurarea securității de autentificare a unei zone se realizează prin formarea unui lanț de autentificare de la o cheie publică recent învățată la cheia publică anterioară care a fost autentificată, care la rândul ei a fost configurată sau ar trebui să fi fost învățată și verificată în prealabil.

* 1. *Asigurarea spațiului de nume DNS*

Autentificarea numelor și tipurilor non-existente

Problema de a oferi răspunsuri negative la același nivel de autentificare și integritate necesită utilizarea unui nou tip de înregistrare a resurselor, și anume înregistrarea NSEC. Înregistrarea NSEC permite securitatea printr-un resolver care este apt să autentifice un răspuns negativ, pentru fiecare nume sau tip non-existent cu aceleași mecanisme utilizate pentru autentificarea altor răspunsuri DNS.

Utilizarea înregistrărilor NSEC necesită o reprezentare canonică și ordonarea zonelor din domeniul de nume. Lanțurile de înregistrări NSEC descriu în mod explicit lacunele, sau “spațiul gol” între domeniile de nume dintr-o zonă și lista tipurilor RRsets prezente în cazul numelor existente. Fiecare înregistrare NSEC este indicate și autentificată utilizând aceste mecanisme care au fost menționate.

Sevicii care nu sunt asigurate de Securitatea DNS

DNS a fost initial conceput în idea că va returna același răspuns la oricare interogare primită, indiferent de numărul de interogări emise și că toate datele din DNS sunt astfel vizibile. În consecință, DNSSEC nu este conceput pentru a oferi confidențialitate, controlul de acces la liste sau diferite modalități de diferențiere între cerințe. DNSSEC nu asigură protecție împotriva respingerii atacului asupra serviciului. Securitatea resolvers și securitatea name servers este vulnerabilă la o clasă adițională de respingere a atacurilor serviciului bazată pe operații criptografice. Extensiile de securitate DNS furnizează date și autentificarea originii datelor DNS. Mecanismele descries mai sus nu sunt concepute pentru a proteja operații precum zone de transfer și actualizări dinamice. (RFC2136), (RFC3007).

**Bibliografie**

<http://www.amazon.com/DNS-BIND-5th-Edition-Cricket/dp/0596100574> [DNS and BIND, 5th Edition - O'Reilly Media](http://shop.oreilly.com/product/9780596100575.do)

<http://tools.ietf.org/html/rfc2535>

<http://tools.ietf.org/html/rfc2136?christopljw_session=437ceh84un2a0jq2j2d48m1os4>