Considerații generale:

Structura actuală a rețelei de date a fost proiectată în urmă cu 6 ani de zile. Din acel moment, rețeaua s-a mărit considerabil atât în dimensiune (prin adăugarea a circa 250 echipamente de rețea), cât si, inevitabil, în complexitate (a apărut nevoia unor servicii suplimentare de management de rețea – existența unui domeniu, centralizarea utilizatorilor şi resurselor din rețea, distribuția automată de update-uri, implementarea unei politici de securitate, monitorizarea accesului la resurse, etc).

Odată cu creşterea numărului de echipamente, au mai apărut următoarele probleme:

- Aglomerarea subnet-ului 192.168.1.0/24. În acest moment sunt disponibile maximum 10 ip-uri pentru acest subnet.
- Întârzieri foarte mari în accesarea serverelor. Pentru unii din utilizatorii rețelei (ex. serviciul Taxe si Impozite) traseul pachetelor IP traversează aproximativ 10 echipamente active de rețea, până când ajung la serverele de date.
- Nu există nici un port liber în nici unul din echipamentele active din dulapurile de comunicație din corpul A.
- Vulnerabilitatea rețelei în cazul în care se defectează anumite echipamente. Pentru ruterele de la Et 1 si Et 2, orice defecțiune atrage după sine pierderea conectivității cu serverul pentru mai mult de 200 utilizatori. Pentru ruterul de la etajul 1, corpul A, orice defecțiune înseamna pierderea conectivității pentru TOTI utilizatorii rețelei. Acelaşi lucru este valabil şi în cazul secționării vreunui dintre tronsoanele backbone-ului de 1 Gbps.
- Conexiunile unui procent de aproximativ 15% din echipamente se face pe 10 Mbps.
- Dulapurile de comunicații sunt pline de echipamente. Structura şi organizarea actuală face imposibilă adăugarea unor echipamente suplimentare, fără a modifica amplasarea şi dimensiunea lor.
- Dispunerea echipamentelor din Sala Serverelor nu întruneste condițiile de securitate, acces si ergonomie impuse de importanța acestor echipamente.
- Accesul dificil la resurse. Fie că e vorba de imprimante de rețea, acces la internet sau e-mail, fără o centralizare a tuturor resurselor nu se poate oferi o soluție viabilă la această problemă.
- Construirea suportului pentru controlul identității utilizatorilor, distribuirea de pachete software şi a sistemului de update-uri centralizate.
- Nu există definită o politică de securitate. Nu există un antivirus centralizat. Pentru calculatoarele care nu au acces la internet, actualizările sunt practic imposibile.
- Lipsa unei aplicații de gestiune şi administrare a echipamentelor.
- În unele birouri prizele şi cablurile de rețea s-au deteriorat, împiedicând accesul pentru diferite echipamente.

Măsuri recomandate:

Pentru a rezolva aceste probleme, considerăm necesară acoperirea următoarelor subiecte:

1) Reîmpărțirea rețelei pentru a susține situația existentă şi pentru a acomoda eventuale dezvoltări ulterioare. Accelerarea vitezei de lucru în LAN şi oferirea unui grad rezonabil de redundanță.
2) Reorganizarea elementelor active şi pasive din dulapurile de comunicații
3) Reorganizarea echipamentelor din camera serverelor
4) Consolidarea domeniului astfel încât să ofere o platformă stabilă pentru implementarea unor politici de securitate, servicii de File Server, Print Server, split DNS, etc.
5) Implementarea unei politici de securitate. Achiziționarea unui antivirus cu management centralizat.
6) Achiziția şi implementarea unei soluții de Asset Management care să permită administrare de la distanță.
7) Revizie pentru cablarea structurată – date.

Recomandările noastre privind soluționarea acestor elemente constau în:

1) Reîmpărțirea rețelei pentru a susține situația existentă şi pentru a acomoda eventuale dezvoltări ulterioare. Accelerarea vitezei de lucru în LAN şi oferirea unui grad rezonabil de redundanță.

    a) Construirea a 7 VLAN-uri – unul pentru servere, iar 6 pentru echipamentele aferente fiecărui dulap de comunicație. Astfel se asigură posibilitățile de extindere viitoare (până la 1778 echipamente), fără a încărca traficul pe rețea de pachete tip „Broadcast”.
    b) Conectarea backbone-urilor de Gigabit în sistem „STAR”. Posibilitatea folosirii a 2 uplink-uri pentru fiecare traseu pentru un grad sporit de redundanță sau Aggregate pentru o viteză mărită (până la 2 Gbps).
    c) Înlocuirea hub-urilor sau a switch-urilor care funcționează la 10 Mbps cu unele care rulează la 100 Mbps

    Detaliere:

    a) VLAN-urile vor fi definite de către echipamentele Layer 3 aflate în acest moment în proprietatea Primăriei Municipiului Timişoara (5 switch-uri L3 Cisco Catalyst). Adițional, trebuie achiziționat si un al 6-lea echipament L3 pentru a menține o structură uniformă.
    Fiecare din ruterele L3 va avea interfețe din VLAN-ul desemnat pentru echipamentele din LAN, iar interfața Gigabit va fi alocată subnet-ului din care fac parte şi serverele. Rutarea va fi configurată astfel încât să permită propagarea pachetelor DHCP dinspre servere spre echipamentele din LAN.
    O propunere de numerotare pentru VLAN-uri este următoarea:
    192.168.1.0/24 pentru servere
    192.168.2.0/24 pentru echipamentele de la etajul2, corpul A

192.168.3.0/24 pentru echipamentele de la etajul2, corpul B
192.168.4.0/24 pentru echipamentele de la etajul1, corpul A
192.168.5.0/24 pentru echipamentele de la etajul1, corpul B
192.168.6.0/24 pentru echipamentele de la parter, corpul A
192.168.7.0/24 pentru echipamentele de la parter, corpul B

b) Fiecare dintre cele 6 rutere vor fi conectate de switch-ul central care deserveşte serverele prin uplink-uri de 1 Gbps. Se va evalua necesitatea suplimentării uplink-ului prin agregarea a încă un tronson de 1 Gbps. În cazul unor defecţiuni la echipamentele de rutare, topologia „STAR" permite izolarea tronsonului defect, şi continuarea operaţiunilor normale pentru restul echipamentelor.

c) Viteza disponibilă pe reţea este ingreunată şi de unele echipamente mai vechi care funcţionează pe 10 Mbps. Aceste hub-uri/switch-uri trebuie înlocuite datorită uzurii morale şi fizice.

2) Reorganizarea elementelor active şi pasive din dulapurile de comunicaţii

a) Schimbarea patch cord-urilor mai mari de 1 m.
b) Identificarea porturilor şi prizelor aferente şi întocmirea unui plan al reţelei în care să fie prezentată corespondenţa porturilor din Patch Panel-uri cu prizele de reţea.
c) Adaugarea unor echipamente active suplimentare acolo unde s-a atins limita capacităţii de conectare la reţea.
d) Evaluarea capacităţii dulapurilor de comunicaţii, iar acolo unde este nevoie suplimentarea rack-urilor sau înlocuirea dulapurilor cu altele mai mari.

Detaliere:

a) În fiecare din Dulapurile de Comunicaţii, intervenţiile la echipamente sunt îngreunate de organizarea defectuoasă a patch cord-urilor. Pentru a simplifica situaţia, propunem înlocuirea patch cord-urilor cu unele de lungime potrivită şi reorganizarea lor astfel încât toate echipamentele să fie uşor accesibile.

b) Datorită zugrăvelilor şi reparaţiilor efectuate în ultimii ani, numerotarea prizelor de reţea şi corespondenţa lor cu Patch Panel-urile s-a desincronizat. Pentru identificarea rapida a eventualelor probleme, se impune renumerotarea tuturor prizelor de reţea, verificarea corespondenţei cu Patch Panel-urile şi intocmirea unui plan al reţelei care să reflecte noua structură.

c) Pentru Dulapurile de Comunicaţii în care nu mai există porturi disponibile pentru echipamente suplimentare, se impune cascadarea unor switch-uri suplimentare. Cascadarea se va face respectând criteriile de viteză, adică fiecare switch suplimentar se va conecta direct în Ruterul VLAN-ului.

d) Dacă în conditiile în care îndeplinirea elementelor de la punctul C ar duce la suplimentarea capacității dulapurilor cu mai mult de 3U, se vor achiziționa Rack-uri suplimentare. Dacă această suplimentare va depăşi 12U, se va trece la înlocuirea în totalitate a Dulapurilor de Comunicații cu unele cu capacitate mai mare.

3) Reorganizarea echipamentelor din camera serverelor

a) Achiziționarea unor Rack-uri accesorizate pentru serverele existente.
b) Achiziționarea unor module de Rack-Mount pentru serverele Tower.
c) Achiziționarea unei console de comandă pentru toate echipamentele din rack.
d) Achiziționarea UPS-urilor pentru servere şi celelalte echipamente de rețea

Detaliere:

a) Pentru a îndeplini criteriile de securitate şi accesibilitate necesare pentru o infrastructură similară cu cea existentă în cadrul PMT, este necesară achiziționarea unor Rack-uri pentru amplasarea serverelor şi a echipamentelor conexe (ups-uri, consolă, switch, KVM, etc.). Ținând cont de numărul şi dimensiunea serverelor existente, se recomandă achiziționarea a 2 Rack-uri 42U, cu posibilitate de încuiere a uşii centrale. Fiecare dintre Rack-uri trebuie dotat cu 3 rafturi fixe (pentru UPS-uri, etc).

b) Toate serverele achiziționate de PMT până în prezent sunt în format Tower, ceea ce duce la imposibilitatea amplasării lor în rack-uri. Pentru a rezolva acest neajuns, se impune achiziționarea de module Tower-to-Rack pentru serverele existente.

c) Intervenția facilă la toate serverele din Rack-uri se face utilizând o consolă de comandă unică pentru toate echipamentele. Acest lucru permite folosirea unui punct unic de administrare pentru toate echipamentele din Rack-uri, eliminând astfel nevoia de a păstra câte un set format din Monitor, Tastatură şi Mouse.

d) Pentru a asigura funcționalitatea echipamentelor critice în timpul fluctuațiilor de curent, s-a adoptat ca măsură principală dotarea cu UPS-uri. Proiectul tehnic va evalua capacitatea de încărcare impusă de echipamentele prezente în momentul de față, şi va recomanda achiziționarea de UPS-uri pentru a oferi o autonomie de aproximativ 30 minute pentru servere şi switch-uri.
Toate UPS-urile vor fi tip „Rack-Mountable” şi vor fi amplasate în Rack-uri. Se vor furniza aplicații care vor monitoriza încărcarea UPS-urilor şi vor comanda oprirea serverelor în momentul în care acumulatorii vor ajunge sub un anumit prag critic, configurabil de către administrator.

4) Consolidarea domeniului astfel încât să ofere o platformă stabilă pentru implementarea unor politici de securitate, servicii de File Server, Print Server, split DNS, etc.

Pentru a face față numărului extins de calculatoare, aplicațiile existente trebuie să ruleze pe echipamente cu putere de calcul mărită. Noua structură a rețelei de date cu 7 VLAN-uri, necesită anumite servicii care să facă administrabil şi coerent portofoliul de conturi, drepturi şi politici.
Totodată dorim să oferim un suport necesar unei politici de securitate (din care face parte sistemul Antivirus, Firewall si aplicatia de Patch Management).
Am identificat un număr de 6 servicii principale care pot satisface noua structură organizațională şi funcțională a rețelei de date din cadrul Primariei Timişoara.

a) Domain Controller (Active Directory)
   Toate informațiile cu privire la numele utilizatorilor, parolele, drepturile şi politicile implementate pe fiecare stație în parte se regăsesc, centralizat, pe Domain Controller. Active Directory este componenta care permite instalare automată de software, management de la distanță, utilizarea unor soluții performante de antivirus şi patch management.
b) File Server
   O componentă esențiala a politicii de backup este File Server-ul. Aceasta este locația în care sunt salvate de către utilizatori toate datele pentru care se asigură disponibilitatea. Documentele salvate local, pe fiecare stație de lucru în parte, nu vor face obiectul vreunor salvări periodice, şi sunt vulnerabile în eventualitatea defectelor hardware.
   Va fi asigurată o locație securizată pentru fiecare utilizator din rețea, în care poate să-şi păstreze datele în condiții de siguranță.
c) Print Server
   Centralizarea accesului la toate imprimantele de rețea din cadrul PMT. Astfel se va asigura accesul facil din orice punct al rețelei la oricare din imprimantele de rețea, rezultând astfel o mai bună gestionare a consumabilelor şi downtime cauzat de defecțiuni la aceste periferice mult micşorat.
d) DNS
   Serviciul de DNS este responsabil pentru translatarea numelor calculatoarelor sau a locațiilor internet (URL-uri) în adrese de ip, pentru a se putea asigura o comunicație facilă între calculatoare. DNS-ul este o componentă esențială a Domain Controller-ului, şi o implementare corectă şi completă a acestui serviciu duce la broadcast-uri mai puține în rețeaua locală, implicit mărind disponibilitatea lățimii de bandă pentru aplicații esențiale. Totodată, returnează din cache ip-urile de la URL-urile folosite anterior, pentru a mări viteza de acces la aceste site-uri.
e) WINS
   Pentru calculatoarele cu sisteme de operare Windows NT, 95 sau 98, rolul serviciului DNS este preluat de WINS. Pentru compatibilitate cu sistemele de operare mai vechi, este recomandată implementarea acestui serviciu.
f) DHCP
   O problemă majoră pentru orice rețea cu mai mult de 20-30 de calculatoare este alocarea adreselor de IP. Orice echipament care încearcă să obțină aceeaşi adresă de ip ca şi un alt echipament, duce la încetarea comunicației în rețea a celor două echipamente. În cazul în care pentru o stație este alocată aceeaşi

adresă de ip ca şi a unui server, problema apărută este majoră, iar în cazul unor rețele cu multe echipamente, rezolvarea sa poate dura mult timp. DHCP-ul este serviciul responsabil cu alocarea adreselor de IP pentru toate VLAN-urile existente. Funcționarea acestui serviciu asigură excluderea conflictelor de ip-uri, şi permite configurarea automată a celorlaltor parametrii de rețea (DNS, WINS, Gateway, Subnet Mask, etc.).

5) Implementarea unei politici de securitate. Achiziționarea unui antivirus cu management centralizat şi implementarea unui sistem de distribuție automată a update-urilor.

   a) Pentru a proteja datele de pe calculatoarele din rețea (inclusiv servere) este recomandată implementarea unei soluții antivirus. Rolurile pe care această soluție trebuie să le îndeplinească sunt scanarea în timp real a fişierelor copiate sau modificate, actualizări centralizate, rapoarte cu privire la activitatea antivirusul în toată rețeaua, etc.
      Principalele caracteristici pe care aplicația antivirus trebuie să le permită sunt:
      i. Management centralizat. Posibilitatea de a implementa politici în funcție de grupuri şi calculatoare.
      ii. Rapoarte integrate cu privire la starea antivirusului de pe stațiile de lucru.
      iii. Alertarea administratorului în cazul infectării vreunui sistem.
      iv. Posibilitatea de a actualiza de pe server definițiile si motorul de cautare pentru modulul client al antivirusului.
      v. Posibilitatea de a instala de la distanță modulul client pe sisteme care rulează Windows NT, 2000 si XP

   b) sistem de distribuție a update-urilor
      Majoritatea viruşilor de astăzi exploatează diferite breşe de securitate în sistemele de operare Microsoft Windows – mai ales Windows 2000 şi XP pentru a se distribui (vezi Sasser, Netsky, Sobig, Zotob, Bugbear, etc.). Pentru acest tip de viruşi, un antivirus actualizat nu reprezintă un impediment, singura piedică în calea lor fiind fixurile şi patchurile de la Microsoft. Soluția de patch management ar putea oferi o variantă de eliminare a acestor riscuri. Cu ajutorul acestui utilitar se pot programa, instala şi urmări actualizările sistemelor de operare de pe stațiile de lucru. De obicei, Microsoft publică fix-urile de securitate pentru sistemele de operare cu cateva zile/saptamani înainte de răspândirea la scară largă a viruşilor, ceea ce face instalarea manuală pe stațiile de lucru imposibilă.

6) Achiziția şi implementarea unei soluții de Asset Management care să permită şi administrare de la distanță.

   a) Componenta de inventariere a echipamentelor din punct de vedere Hardware şi Software

b) Software Deployment – posibilitatea de a crea şi instala pachete software în funcție de rezultatele inventarierii ale componentei de Asset Management.
c) Managementul personalității utilizatorilor de pe stațiile de domeniu. Include migrarea sistemelor de operare cu păstrarea identității, transferul identității şi migrarea personalității utilizatorilor între calculatoare.
d) Crearea de fişiere-imagine pentru fiecare stație de lucru, şi instalarea acestei imagini remote, în cazul coruperii sistemului de operare.

7) Revizie pentru cablarea structurată – date.

Datorită deteriorării infrastructurii de rețea din ultimii ani, se impune o revizie generală care să permită rezolvarea problemelor de conectică (instalarea prizelor smulse de pe pereți, aranjarea cablurilor, etc.) din diferite birouri. În proiectul tehnic se vor menționa birourile în care aceste lucrări vor trebui efectuate.

NOTĂ:

Odată cu implementarea acestei soluții se impune Monitorizarea şi Administrarea ei pentru a asigura un ciclu de viață îndelungat. Având în vedere complexitatea structurală şi tehnicitatea soluțiilor folosite, recomandăm achiziționarea serviciului de "Monitorizare şi Administrare pentru infrastructura de rețea" (Servere de infrastructură, Echipamente active de rețea – rutere, switch-uri, echipamente conexe – UPS-uri, consolă, etc).

Devizul General al Investiției

Deviz General

Privind cheltuielile necesare implementării extinderii de rețea din cadrul PMT

TIMIŞOARA

Nr. Crt	Denumirea capitolelor şi subcapitolelor de cheltuieli	Total (EURO, inclusiv TVA)	Din care supusă procedurii de achiziție publică
1	Echipamente Hardware – materiale	36183	36183
2	Aplicații software – licențe	43000	43000
3	Manopera implementare	10000	10000
4	Asistența tehnică – Consultanță	1750	1750

CAPITOLUL I
ECHIPAMENTE HARDWARE - MATERIALE

1.1	SAN (inclusiv 3 HDD 143 Gb)	6144	6144
1.2	Switch 24 port 10/100, 2xGBIC – 8 buc	3984	3984
1.3	Switch 24 port 10/100/1000	703	703
1.4	Switch L3, 24 port 10/100, 2xGigabyte, Ruter	5300	5300
1.5	Server + Tape	7200	7200
1.6	UPS 2200 VA RM – 2 buc	3152	3152
1.7	RACK 42U + tavi fixe si mobile – 2 buc	2200	2200
1.8	RM kit 4 srv – 8 buc	2000	2000
1.9	KVM + Monitor	2000	2000
1.10	Materiale rețelistica	3500	3500

CAPITOLUL II
APLICAȚII SOFTWARE – LICENȚE

2.1	Antivirus	14000	14000
2.2	Win 2k3 Srv OEM – 3 buc	2100	2100
2.3	100 CAL Windows 2003	5000	5000
2.4	Asset Management – 300 buc	21900	21900

CAPITOLUL III
MANOPERA IMPLEMENTARE

3.1	Antivirus	1500	1500
3.2	Manopera dulapuri şi uplink-uri	2500	2500
3.3	Manopera implementare	6000	6000

CAPITOLUL IV
ASISTENTA TEHNICA – CONSULTANTA

4.1	Asistența tehnică privind verificarea şi recepția etapelor lucrării	1000	1000
4.2	Consultanța privind eşalonarea etapelor pentru a menține serviciile disponibile pe rețea	750	750

PRINCIPALII INDICATORI TEHNICO-ECONOMICI AI INVESTITIEI:

- Valoarea totală a investiției: 90.933 EURO (TVA inclus)
- Eşalonarea investiției: 2005-2006
- Durata de realizare: 3 luni de la semnarea contractului

FINANȚAREA INVESTIȚIEI:

- 90.933 EURO din fondurile bugetului local

AVIZE ŞI ACORDURI:

- Aviz privind oportunitatea investiției.

OPORTUNITATEA INVESTIȚIEI

Necesitatea extinderii rețelei si a implementării unei soluții pentru infrastructura software de rețea derivă din dorința asigurării tuturor utilizatorilor rețelei de calculatoare din cadrul PMT de accesul la resursele disponibile, în mod securizat şi pe baza unor politici valabile în întreaga rețea. De asemenea se are în vedere o soluție care să permită includerea în rețea a 1518 echipamente (stații de lucru şi imprimante de rețea) fără o modificare majoră de infrastructură.