

Gold, Silver, Bronze

"Deploying a Samba/LDAP infrastructure in a SME business environment."

Georgatos Fotis <fotis@mikroskosmos.com>
Kanakis Isidoros <isikanak@otenet.gr>

15 April 2003

SambaXP 2003
14-15 April 2003, Göttingen, Germany

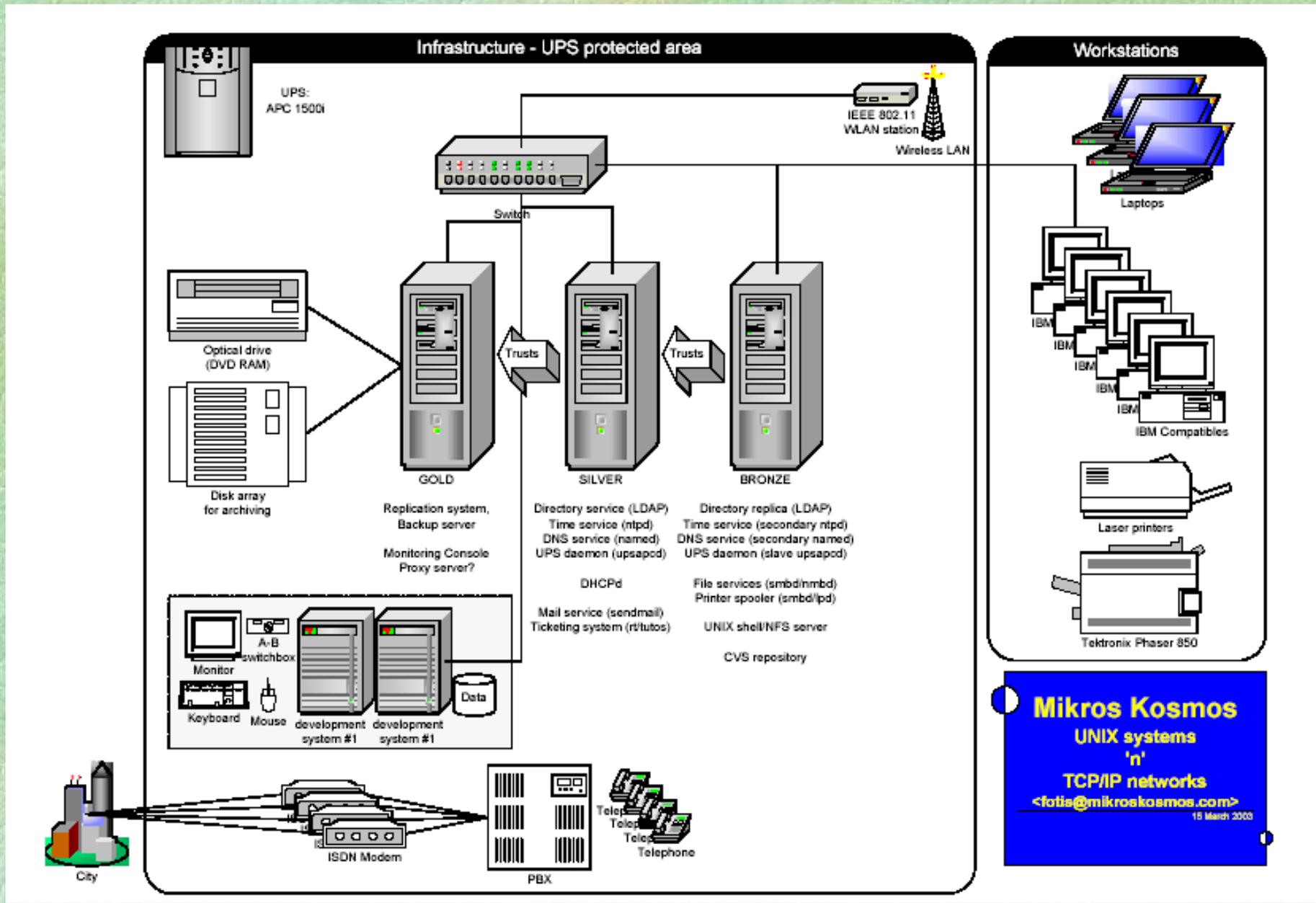
What triggered this presentation

- ♣ Most companies rarely have constant requirements for their network setups
- ♣ In fact, a healthy start-up **is** going to face exponential growth rate
- ♣ Planning ahead for growing up, minimizes growing pains :-)
- ♣ Never, EVER, think of redundancy and backing up as optional and ad-hoc!

What has all this to do with Samba?

- ♣ Steve Traugott and Joel Huddleston presented a paper at LISA '98, entitled "Bootstrapping an infrastructure"
- ♣ In this paper, concrete steps and a certain order are suggested for the aim of setting up a multi-user general purpose network.
- ♣ Gold, Silver, Bronze is a trio with ordered trust links, taking into account redundancy, backup schemes and disaster recovery

What it looks like



Mikros Kosmos
 UNIX systems
 'n'
 TCP/IP networks
 <fatia@mikroskosmos.com>
 15 March 2003

Gold server

This system has the same role as described by S. Traugott: "installation server" - possibly with CVS for /etc of other servers - plus, being a replication system for them. It holds the "state of the business"

- ♣ It holds on-line archives taken from disk contents of all the critical systems in the company's network
- ♣ It is not a daily production system, meaning that it can be taken offline for a few hours and no user should be able to notice
- ♣ External massive storage of 100GBytes or so (USB 2.0, nowadays) is appropriate . It is advisable that this external storage is only used for online backups. An offline backup scheme must also be planned here!

Silver server

- ♣ This is the "maestro" of the network, as far as user services and security policy are concerned
- ♣ It runs the primary DNS, DHCP, NTP services as well as a UPS-aware daemon which is handy for coordinated shutdowns
- ♣ Company's directory server must be placed here. OpenLDAP has been our choice as the directory and authentication server
- ♣ Although this system holds the information regarding user accounts, it is not intended for user logins or running user processes. "Admin only"

Silver server, part II

- ♣ This system is a good place to put auditing tools or software for monitoring network activity
- ♣ We chose to add to this machine a mail server for relaying mail to the outside world, tightly bound with a ticketing system (rt). Other sysadmins may find this poor choice depending on their budget
- ♣ Availability concerns dictate a RAID-1 setup for this system. The CPU/memory/disk needs of this machine should remain relatively constant over long periods of time.

Bronze server

- ♣ This is the file server. The place where users are allowed to bite each other with their tasks...
- ♣ First, we setup the secondary DNS, DHCP, NTP servers and a UPS-aware daemon in client mode
- ♣ A replica LDAP service must run here (read-only) with referral to the master server (Silver)
- ♣ Your guide is the document by Olivier Lemaire: "The SAMBA-2.2.4/LDAP PDC HOWTO"
- ♣ The file services can include not only Samba for the Windows clients, but also NFS, Coda, DFS etc.

Bronze server, part II

- ♣ This is the place to setup a printer server with its spooling queues, CVS tree for developers and so on
- ♣ A UNIX shell may be given here, when it is a requested service within the network
- ♣ Any service which is highly user-controlled load should fit on Bronze server.
- ♣ Dual CPU is advisable.
- ♣ Performance and capacity concerns dictate a RAID-0/5/10 for this system

Setup your UPS correctly!

Get a UPS that can talk with your master server. Put on the UPS *anything* which is part of the infrastructure and only that:

- ♣ Gold, Silver, Bronze servers
- ♣ Hubs, Switches, Wireless LAN devices, Firewall
- ♣ Development systems and other critical machinery
- ♣ Your PBX and ISDN terminals (if needed/possible)

Put exactly one monitor on the UPS, so that you still have a monitoring console. We hooked it on the Gold server for reasons that have to do with trust order.

Generic network tips

- ♣ Having a couple of laptops with WLAN in the network, may prove handy as well during power-cuts
 - ♣ Consider every user system in the network as "disposable" and let users know this
 - ♣ Make sure you monitor your RAID disks. There's not much reason to have RAID if you don't monitor it.
- There is only a single system that will require maintenance over time, the Bronze server. Give it the CPU, memory and disk capacity it asks from you. Follow the capacity upgrades on the Gold server for proper replication.

Troubleshooting Gold server

If the Gold server dies, you run out of two things:
backup server and installation server

♣ You have to go to the nearby shop for replacing its hardware, but you can still walk slowly

♣ During this time, your network runs in "degraded mode"

♣ Not a problem for a period less than a day, but then, you start losing on your backup scheme.

♣ If its disk subsystem breaks, you **SHOULD** have had a proper backup scheme anyway.

Troubleshooting Silver 'n' Bronze

If Silver or Bronze servers die, you will try to “push” the problem on Gold by using spare parts from it in order to recover within half an hour or so

♣ This is appropriate for CPU or memory errors, but not hard disks

♣ If the hard disks of Silver or Bronze server have problems, yes, you are in trouble, but...

♣ Even so, you do have an online backup of last day on Gold and that should give you enough time and efficiency to repair the damage with no painful outcomes (a reasonable downtime for a disk failure).

Troubleshooting, other

- ♣ If a user runs on you claiming he has lost his files, you can recover a recent version from the Gold server. Depending on your backup schemes you may be able to do more
- ♣ In case of severe physical damage on the site of installation (fire, flood, earthquake), you may pick your Gold server's off-site backup (you have one, don't you?) and proceed in a luckier place...
- ♣ The latter is a way to bootstrap the infrastructure in a different location, too (eg. in another city).

Unresolved issues (open problems)

- ♣ How to implement redundancy in authentication? (PDC/BDC? pGina? Or what?)
- ♣ What kind of Windows clients should we consider as "the only supported"? 9x/Me/NT/200x/XP?
- ♣ Is it possible to autcreate home directories on first login or authentication of a user? (just like what is possible already with pam modules for unix logins)
- ♣ How far can we stretch the rule of compartmentalization? (think of the ticketing system or a mail server)

Unresolved issues (open problems)

- ♣ We may reexport the Gold server's filesystem with Samba serving “yesterday” image. If so, then we break the "not-for-production" initial specification
- ♣ Because Gold is sitting idle most of the time, it could be recycled by running on it a service like a transparent http proxy. How to circumvent this in case of Gold server failing?
- ♣ Should we think of IPP/CUPS instead of LprNG for Samba Printing Services? What's best?
- ♣ Is there a place for High Availability in this setup? What is the rule for preferring a HA solution?

Coffee time

♣ Did you know that Linux can make coffee?



♣ Read the Coffee-HOWTO! <http://www.tldp.org>