

Privacy Policy

- Everybody have to know the company e-mail policy (...and accept it...)
- For diagnostic reasons the SA may fumble among e-mails
- It can happen, that not only diag.....
- The higher management can announce that sending private mails from company's address is not supported
- Nevertheless,... The SA has to carry the privacy policy into execution

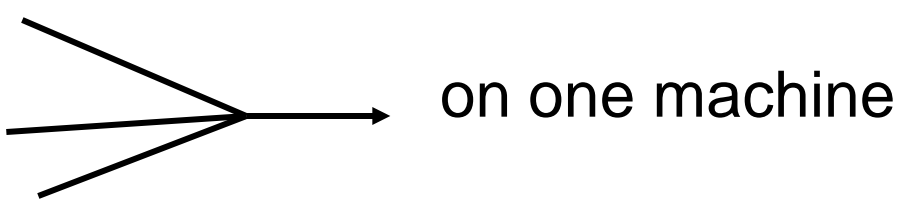
Namespaces

- The e-mail address is the most visible part of the companys' namespace
- Important to work properly
- The local and public e-mail address has to be the same (or translate to the same)
- The address format has to be standard
 - Eg. first.last
john.smith
 - Eg. Abbreviation or identifier
jsmith, pvarga, lkovacs, lakovacs

Reliability

- E-mail is a basic tool
- It has to work well all the time!
- The erroneous e-mail system is expensive.
 - Missing e-mail....-> Business panic
- Backup the whole system
 - If not possible („expensive”):
 - Standby plan, practiced steps to repair the fault

Simplicity

- Limit the number of required machines
 - Do not use desktop PC-s (only UA)
 - Small machine park:
 - message forwarding
 - delivery
 - list handling
- 
- on one machine
- Big park:
 - On separate machines / machine groups
 - SMTP port of the desktop PC's and non-email server's has to be prohibited
 - Do not use protocol-gateways

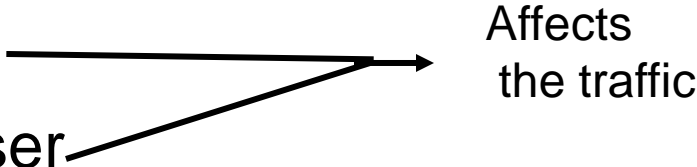
Automated

- The e-mail account creation has to be the part of general account-making procedure
- ...the removal as well
- Do not forward the leaving staff's e-mails: delete them from the lists
 - sensitive information!
 - ...notify in autoreply: „end” of this account
- Copy accounts between servers
- Administration of lists (create, delete, modify)

Monitoring

- Monitor all PC-s which participate in e-mail sending
- Network: **ping** (ICMP sends **echo** message)
- Storage field (disk out of space...)
- TCP 25 port accessible?
- Rebound messages – *diagnostic info*
- Logfiles (eg. message-quantity, forecast)

Scalability

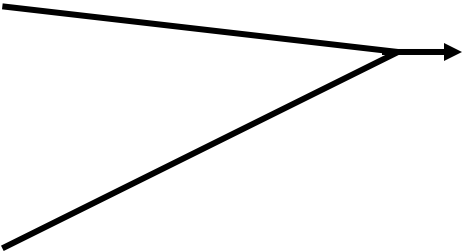
- Rising user basis
 - Has to handle great data traffic
 - Message size
 - Message number / user
 - Number of users
 - Handling traffic bursts
 - Storage of Huge, accumulated data quantity
 - Using a mail spool helps
 - Message size limitation can help (periodically)
- 
- A diagram consisting of two arrows. One arrow starts from the text 'Message size' and points to the right. The other arrow starts from the text 'Message number / user' and also points to the right, meeting the first arrow. Both arrows point towards the text 'Affects the traffic'.

Security

- The machines of e-mail system get most of the attack (extranet, Internet)
- Worms, viruses, ...
 - Contain filtering!
 - Privacy Policy
 - Adjusting applications – updating
- Monitoring on servers AND on user PC
- Together with the firewall: company's security strategy

Remote Access Service

Company's Internet-access

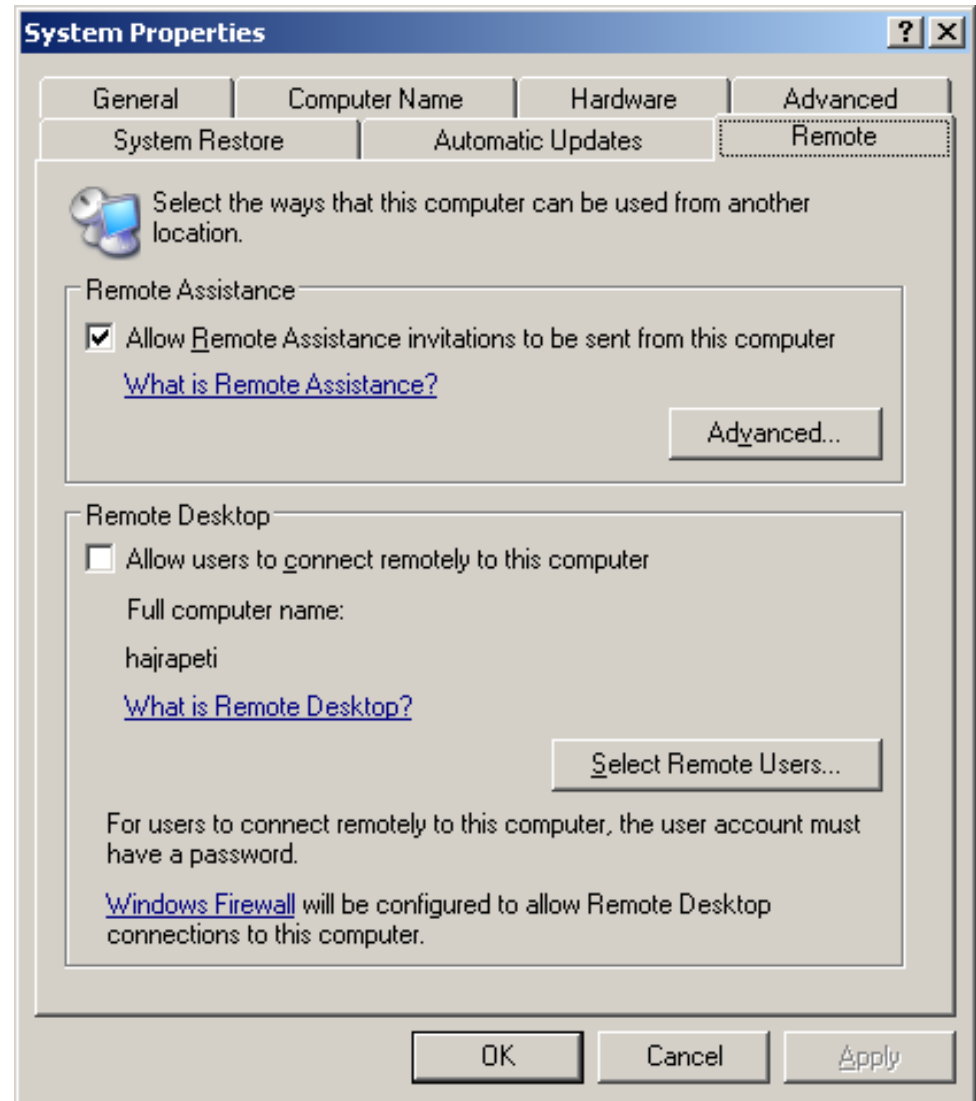
- Security
 - Security
 - Security
- 
- Firewall,
firewall-configuration
- Internet-access regulation
 - all prohibit given domains
 - Private-Internet access limitations
 - Bandwidth-limit
 - Requirement: Staff remote log in

Example: „Remote Desktop”

- Windows based (reachable by MS Win XP)
- The whole remote display is visible, mouse+keyboard control
- Login is possible with the (remote desktop) Windows password
 - Be very complex!!

Remote Desktop setting - 1

- Remote:
Complex psw!
- My Computer –
"right click"
– Properties,
Remote tag



Remote Desktop setting - 2

- Router:
Complex psw!
(10-16
character)
- Port forwarding
set up
(router -> „remote pc”)

- Startup:

<http://portforward.com/>

PortForward.com - Free Help Setting up Your Router or Firewall - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://portforward.com/englis

Getting Started Latest Headlines Hajrá Peti | 2007 myipaddress.com

Your external IP address is 152.66.247.164.

	Longshine	SMC
00V	• LCS-883-DSL-4F	• 1244TX
00G		• 2404WBR
0E	Loopcomm	• 2804WBR
0		• 2804WBRP-G
0V	• LP-AL2011	• 2804WBRV2
0WE	• LP-AL2014P	• 2804WBRv3
	• LP-AL5011P	• 7004ABR
Smith Elec		• 7004ABRv2
		• 7004AWBR
REL10v2	Lucent Technologies	• 7004BR
Rel9P-B1		• 7004BRV2
REL10v2	• CELL-22A-FX-CZ	• 7004FW
Rel9P-B1		• 7004VBR
REL10v2	MacSense	• 7004VBRv2
REL10v2		• 7004VBRv2EU
REL10v2		• 7004VWBR
REL10v2	• MTH-130 A	• 7004WBR

http://portforward.com/english/routers/port_forwarding/SMC/7004BR/7004BRindex.htm

Remote Desktop setting - 3

- Router:
 - Application
 - Portlist
 - *Authority*

Port Range Forwarding

Application	Start	End	Protocol	IP Address	Enable
FTP1	21	To 21	Both	192.168.1.	<input checked="" type="checkbox"/>
	0	to 0	Both	192.168.1.	<input type="checkbox"/>

Port Range Forwarding:
Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request comes in from the Internet, the router will route the request to the computer you want to limit only those and the checkbox.

Save Settings Cancel Changes

Remote Desktop setting - 4

Enhanced security:

RDP port modification
(primary: 3389)

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure of the registry, with the path `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp` selected. The right pane shows a list of registry values:

Name	Type	Data
OutBufLength	REG_DWORD	0x00000212 (530)
Password	REG_SZ	
PdClass	REG_DWORD	0x00000002 (2)
PdDLL	REG_SZ	tdtcp
PdFlag	REG_DWORD	0x0000004e (78)
PdName	REG_SZ	tcp
PortNumber	REG_DWORD	0x00000d3d (3389)
WsxDLL	REG_SZ	rdpwsx

An "Edit DWORD Value" dialog box is open over the "PortNumber" entry. It shows the "Value name" as "PortNumber" and the "Value data" as "3389". The "Base" is set to "Decimal".

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

Firewall-hack

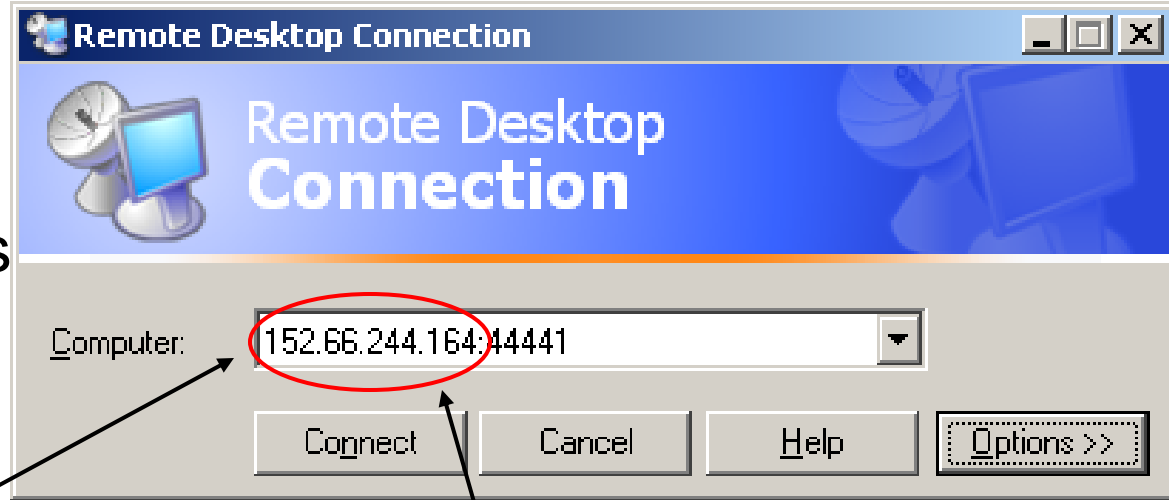
- For remote access (eg. Remote Desktop)
 - On the company's firewall
 - On the local machines' firewall

make the application's protocol port transparent

- At a good company: long authorization procedure

Remote Desktop - login

- Programs
 - Accessories
 - Communications
 - Remote Desktop Connection



- IP address : port
- Username / password

Our remote PC's IP-address
(eg. from www.myipaddress.com)

VNC – Virtual Network Computing

- „Whatever OS machine” environment displays on any other machines
- Two components:
 - VNC server: runs on the present PC
 - (eg. remote server)
 - VNC client: the present PC
 - (eg. IT-staff’s laptop)
 - **vncviewer** application – or
 - Java application runs on Web-Browser
 - Example: Linux server, WinXP client

VNC – Server side (eg. Linux)

- <http://www.realvnc.com/>
- Install
 - If ‘vnc’ the home
 - vnc/bin – binary logs (include binary search path..)
 - vnc/classes – further classes
 - **\$vncClasses** be the **\$HOME/vnc/classes**
 - `$vncClasses = ((-d "/home/pvarga/VNC/classes") && "/home/pvarga/VNC/classes");`
- Run: ‘vncserver :n’
 - n: session number
 - used port: 5800+n
- End: ‘vncserver –kill :n’

VNC – Client side (eg. WinXP)

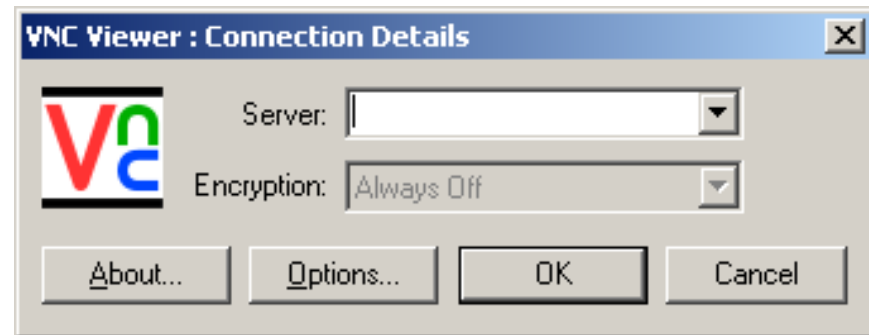
- ‘vncviewer a.b.c.d:port’
 - a.b.c.d – server’s IP-address
 - port: 5800+n

Or:

‘server:session’

Or:

- Web-browser, Java application
 - <http://server:port/>
 - eg.: <http://foszerver.ceg.hu/5801/>



Log in (RAS)

- Authorised users can log in to the company's network
 - from home,
 - from outside,
 - from any point of the world
- User's requirements
 - „only to see the e-mail”
 - Working any time
- Require careful planning

Service level

- Clarify with users
 - possibilities
 - regulations (policy), security as well
 - responsibilities
 - paying construction
- If possible outsource the RAS-service
- **Never outsource security tasks...**
 - Authentication (username/password)
 - Authorization
 - Network protection

Requirements (RAS)

- Everybody **has to have** a simple, cheap, pleasant remote access
- If haven't: build to himself... *Not secure!*
- Short time login: small bandwidth requirement
- Longer work (eg. at home)
 - Interrupts
 - Big bandwidth requirement
 - Other cost model
 - Data coding (username/psw)
- Login from another company
 - Has to harmonize the two company's policy
 - Not applicable the „always-on” system
 - Firewall hack
 - Application used protocols (-> port)