Whitepaper Citrix over DVB-RCS

Version 1.2
22-oktober-2004

Created for ESA by BySky(www.bysky.nl),ing. Gert-Jan de Jonge (CTO),ing. Kasper Kombrink

Table of Contents

Foreword

Today there are many different ways to distribute applications from a server to a client. The best known way is to simply read the application software and data from the server by using a Networked file system like Novell network (ncp) or windows networking (smb/cifs). This is a good way to work when you have much bandwidth (ie. 100 Mbit up to 1 Gbit) to your server. Unfortunately this also means, that every desktop system (f.e. a PC) must have enough resource's to run the application. This makes the total cost of ownership (TCO) very high in a big network.

For these two problems there are solutions from different vendors. Al of these solutions are different in the way they are used, but share the same approach. Run the application on the server, show the application data on the screen of a terminal, much like the terminals on minicomputers of the past. This enables the use of so called "thin clients" as nearly no local resources are needed, and also the bandwidth requirement drop's down to speeds as existing infrastructure like PSTN/ISDN/xDSL and satellite.

There are many software solutions to create this functionality. If you need to take control of a remote machine, you might use PC-Anywhere, VNC or f.e. Windows XP remote desktop. If you need to run multiple users on the same hardware, you need to use other software to enable this. Examples of this software are: Terminal services for windows server family, Citrix metaframe for the windows server family or f.e. XWindows for Unix based servers. This way of working is also called Server based computing.

This document will focus on Citrix on the windows family OS used in conjunction with the DVB-RCS satellite network platform.

Trademarks

Microsoft ™
Windows ™, Windows2000 ™, Windows2003 ™, WindowsXP ™
Terminal Server ™, NT4.0 ™
Citrix ™,
Speedscreen ™,Metaframe ™, Winframe ™, NFuse ™
XWindows ™
VNC ™

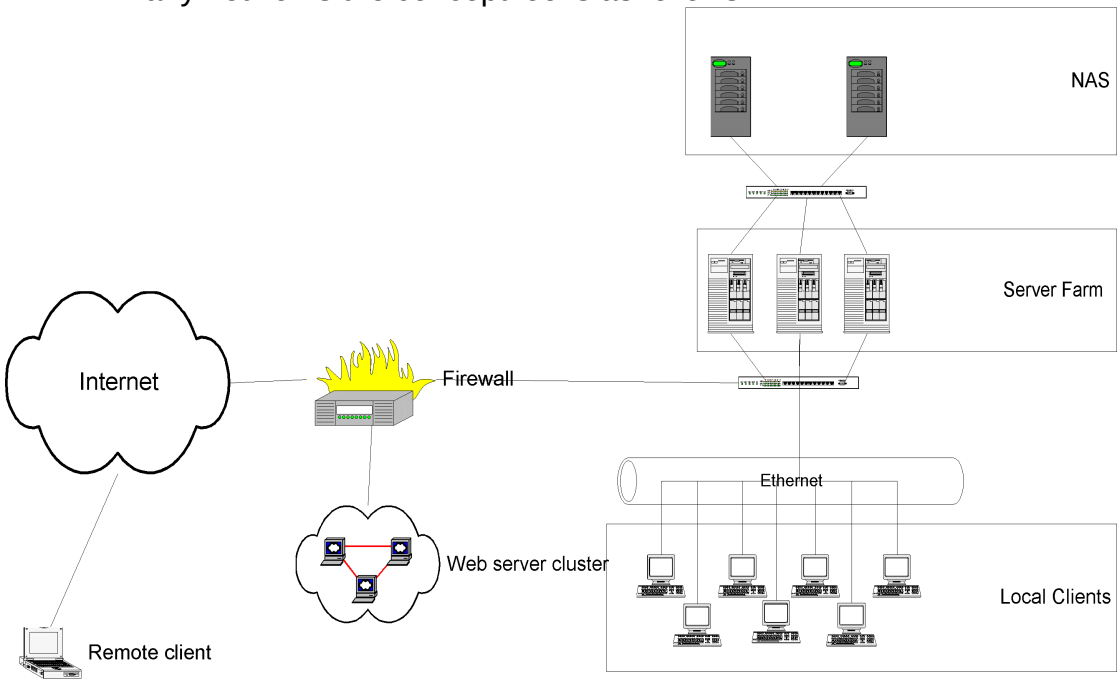
Server based computing

1.1. Server based computing concept

Server based computing is used by many different companies for as many different reasons. The most important reasons for choosing a server based computing concept can be divided as follows:

- Lower TCO
  - Centralization of skilled technical resources
  - Reduction in desktop costs
  - Simpler maintenance, help desk
  - Reduction in software license costs
- Possibility for remote office's and or home office's using low bandwidth connections.

In many networks the concept looks as follows:



What you see in this generalized setup is a server farm consisting of 3 servers, which deploy the applications. The data is saved on a NAS system. The servers deploy the applications to the local Ethernet network clients, but also through the firewall remote clients are supported. The web server cluster is mainly added for simpler access to internal data and/or applications. In many smaller networks you will not see the web cluster and the NAS system.

1.2. Overview of applications

The following products of Citrix are available:

- WinFrame
- MetaFrame
- NFuse

The following products of Windows Terminal services are available:

- NT4.0 Terminal services
- Windows 2000 Terminal services
- Windows 2003 Terminal services

The Citrix products are available on TCP/IP, but also on SPX,IPX, Netbeui. Windows Terminal services is only available on TCP/IP. Both product families can use RDP (Remote Desktop Protocol) and ICA (Independent Computing Architecture) as protocol (Terminal server needs Citrix metaframe add-on to use ICA).

Citrix provides some key features that Windows 2000 terminal has yet to offer, such as the ability to do automatic drive redirection and COM port redirection. Another big advantage of Citrix is that Citrix MetaFrame has the ability to run on virtually any client over virtually any connection. This is a very important consideration for organizations that are not running a homogenous Windows 9x or greater environment. The following figure shows the most important feature differences between the two solutions.

Citrix Metaframe features vs. Windows 2000 Terminal Services

Feature	Citrix Metaframe	Windows 2000 Terminal Services
Available client		
Windows NT	X	X
Windows 95/98	X	X
Windows 3.11 (Workgroups)	X	X
Windows 3.1	X	
Windows CE	X	X
DOS	X	
Macintosh (Motorola, PowerPC)	X	
UNIX (Solaris, Sparc, X386, DEC)	X	
UNIX (SunOS, SCO, DEC, HP)	X	
UNIX (SGI, SCO, Linux)	X	
RISC OS	X	
Client devices		
PCs (Windows 3.11 or greater)	X	X
PCs (DOS, UNIX, Linux)	X	
Macintosh (Motorola, PowerPC)	X	
Handheld PCs	X	
Windows-based terminals (CE)	X	X
Windows terminals (DOS, etc.)	X	X
Network terminals (Winterm, etc.)	X	
Set-top devices	X	
Mobile handheld devices	X	
Client features		
Manual drive redirection	X	X
Bitmap caching	X	
Automatic printer creation	X	X
Clipboard redirection	X	X
Automatic drive redirection	X	
Seamless windows	X	
Transport protocols		
TCP/IP	X	X
IPX	X	
SPX	X	
NetBeui	X	
Client multi-media		
System sounds (beep)	X	X
16-bit stereo (WAV, MIDI, AVI)	X	
Connections		
LAN	X	X
WAN	X	X
RAS dial-up	X	X
Direct serial connection (asynch)	X	
Direct dial-up	X	
Local device support		
Local printer (parallel port)	X	X
Local client printer spooler	X	X
COM port redirection	X	

1.3. Advantages of using Citrix in a satellite environment

As Citrix has been developing their application since 19xx they have noticed the problems that can arise when using networks which have a larger round trip time than desired. This happens on connections f.e. from Europe to Japan, or connection's which have inherent delays like a satellite connection.

Citrix has addressed different parts of this problem and incorporates this in the metaframe software. These advantages are not available in other products:

- Mouse and keyboard queuing.
- Caching of bitmaps (also in windows terminal services)
- Speedscreen latency reduction.

At the moment of this writing Citrix is the only software which has the functionality to type text in input fields without directly sending the information over satellite.

2. Setup and tuning of Citrix over DVB-RCS networks

2.1. Encountered problems and solutions

The main problem that can be encountered is that the TCP connection to the CITRIX server is not optimal in standard Windows configuration. The normal configuration for f.e. Windows 2000 is not to use Window Scaling, network send/receive buffers are not big enough.

First step for better performance is to alter these settings on the server and client side. This will ensure that when needed as much bandwidth as possible is used. Another solution is to use a satellite accelerator which is build for this functionality and which does not require reconfiguring Client and Server.

2.2. Tools required

TCP Optimizer

TCP Optimizer is a tool provided by speedguide.net which optimizes Internet-related settings on your end of the connection (your PC), allowing for faster throughput. It works with any internet connection. It's a free program that supports all current Windows versions. TCP Optimizer optimizes some networking related buffers for Internet connectivity, and allows for some educated custom tweaking of your Internet connection. Many network settings in Windows are configured for dialup (low speed) or Ethernet (low latency) devices. With today's high-speed Internet connections, this oversight hampers the performance of your Internet connection as much as 200%. The settings TCP optimizer edits, are described in annex A.

2.3. Used RDP/ICA/VPN port numbers

The following ports are used by RDP, ICA and VPN (all ports are outbound):

RDP:		3389	(TCP)
ICA:		1494	(TCP)
		1604	(UDP)
VPN:	PPTP:	1723	(TCP)
	L2TP:	1701 (win200), but also 500 is seen and after tunnel initiation a high port number will be used. (UDP)	
IPSEC:		own protocol	

2.4. Operating system dependencies

Citrix MetaFrame XP

Microsoft Windows 2000
Microsoft NT 4.0 Server Terminal Server Edition

MetaFrame XP requires approximately:

- 75MB of disk space on the server to store MetaFrame XP files and online documentation.
- 150MB of disk space to store all ICA Client software.
- 10MB of disk space for MetaFrame SNMP agent for HP Openview or Tivoli Netware.
- 20MB of disk space for the NFuse services on the MetaFrame XP server.
- 64MB of RAM for the IMA service and other MetaFrame XP services.
- 1.7MB of RAM for each idle session awaiting a connection. By default, two idle sessions exist per server.

Follow the sizing model for Microsoft's Windows 2000 Server or Microsoft's Windows NT Server 4.0, Terminal Server Edition, to ensure that your server's hardware meets the needs of these additional users.

Recommended Server Specifications

System Specifications

	10-20 Users	20-30 Users	For 30 or more
Operating System	Windows 2000	Windows 2000	Users
Processor	1 Pentium III 800 mhz	Dual Pentium III 800 mhz	we suggest Multiple
Free hard drive space	At least 1 GB	At least 1 GB	Servers
RAM	1 GB	At least 1 GB	

Minimum Client Specifications

System Specifications

Operating System	Windows 98, 2000 Professional, XP Professional, or NT Workstation 4.0 with Service Pack 6 or greater,
Processor	Pentium or AMD 100 MHz processor or greater
RAM	64 MB
Screen Resolution	800 x 600
Connection Speed	56 KBps, a broadband connection such as DSL, Cable, or ISDN is recommended

2.5. DVB-RCS recommendations

User experience in working with terminal based applications like CITRIX is mostly depending on interactivity. This means that the response times over satellite are the main issue for configuration. Satellite capacity in DVB-RCS is configured using one of the following categories:

- Continuous Rate Assignment (CRA)
- Rate Based Dynamic Capacity (RBDC)
- Volume Based Dynamic Capacity (VBDC)
- Absolute Volume Based Dynamic Capacity (AVBDC)
- Free Capacity Assignment (FCA)

When the needed bandwidth is known, most important part is the choice of the best category which fits the end user. To be sure of the best interactivity for

the end-user CRA should be used. In CRA the bit rate is warranted, the packet delay is minimal and there is low jitter. Downside of CRA is of course the used space segment, so it will have a higher price. RBDC could also be used, but the interactivity of working in Citrix will go down. Today, VBDC is a widely used configuration since it offers the most cost-effective solution.

2.6. Citrix Configuration

To get optimal performance from Citrix over a DVB-RCS link, you should configure speedscreen. Speedscreen is normally automatically enabled on the client side, but can also be forced to be always “on”.

Enable Speedscreen

Speedscreen consists of two components:

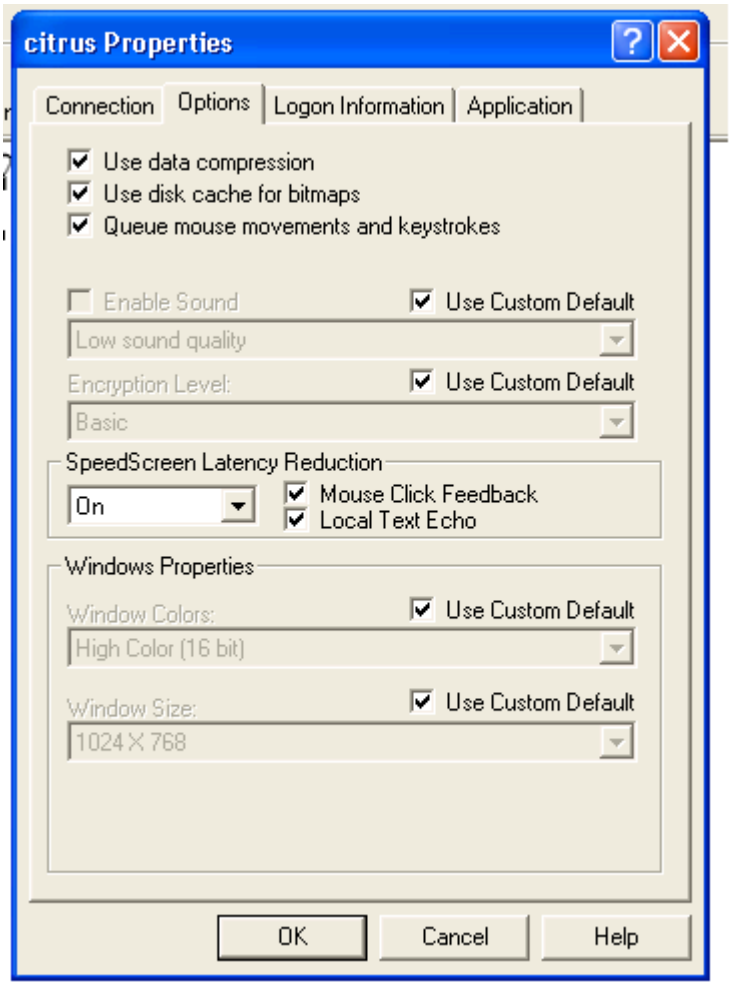
- Local text echo
- Mouse click feedback

Local text echo echoes keystrokes locally on the client as they are typed. The characters appear immediately and are later overwritten seamlessly by the server image as it becomes available. This eliminates the latency perceived when typing, because the user has instant visual feedback when typing.

Mouse click feedback changes the mouse cursor on the client to the “busy working” state when the user clicks a mouse button. When the server acknowledges the mouse click, the mouse cursor on the client reverts to the default pointer. The user is presented with instant feedback to the mouse click.

On the server, the speedscreen Latency Reduction Manager is used to set the options for both components. By default, mouse click feedback is enabled for the server, while local text echo is disabled.

For those applications that are published to DVB-RCS users, enable local text echo. Alternatively, the administrator may want to enable local text echo for the server as a whole.



Enable SpeedScreen Latency Reduction Channel Buffering

Channel buffering means that server data is buffered prior to being transmitted to the client. This has the effect of coalescing together many small packets into a larger packet, which on DVB-RCS connections reduces the number of radio transactions required for the same amount of data. This benefits the session latency.

The Server ! Client communication on the SpeedScreen Latency Reduction Channel typically consists of a large number of small packets, and is an ideal candidate for buffering. The small packets are typically ACK (acknowledge) packets for previously typed keystrokes.

Virtual Channel Buffering is controlled through the Buffering registry value located in the registry key HKLM\System\CurrentControlSet\Control\Terminal Server\WDs\icawd

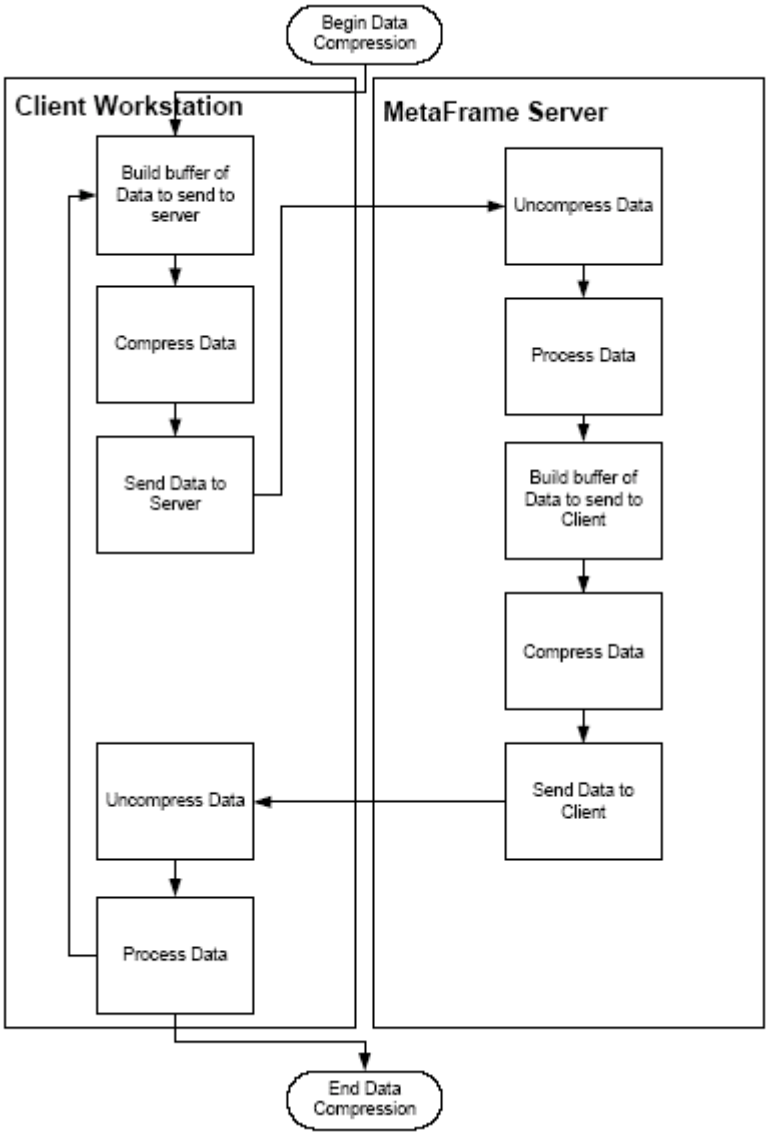
The format of this value is a multi string. Each entry in the multi string corresponds to a virtual channel name which shall be buffered. The regedt32.exe application should be used to edit multi strings (not regedit.exe), the name of the SpeedScreen Latency Reduction channel is "CTXZLC “. The trailing space must be added. Making this change will enable buffering for the channel. The ICA listener must be restarted prior to this taking effect.

ICA Data compression

The winstation driver can compress ICA data before sending it. Compression is enabled or disabled through the user interface, which directly modifies the .ICA file parameter shown in the following table.

ICA client Setting	ICA File Parameter	Description	Default Value
Use Data Compression	Compress	Enables (on) or Disables (off) data compression	Enabled (on)

By default, compression is enabled. If this setting is not modified, the Winstation driver receives data from the virtual channels and compresses it before sending the data to the encryption driver. Disabling the Use data compression setting allows the ICA packet to move from the Winstation driver to the Encryption driver without compression. If resources on the client device are limited, disabling compression allows for better usage of the system resources because compression and decompression require additional processor resources on both client device and server. In an environment where system and client resources are not a concern, data compression can be used to decrease the amount of data that must be sent across the network.

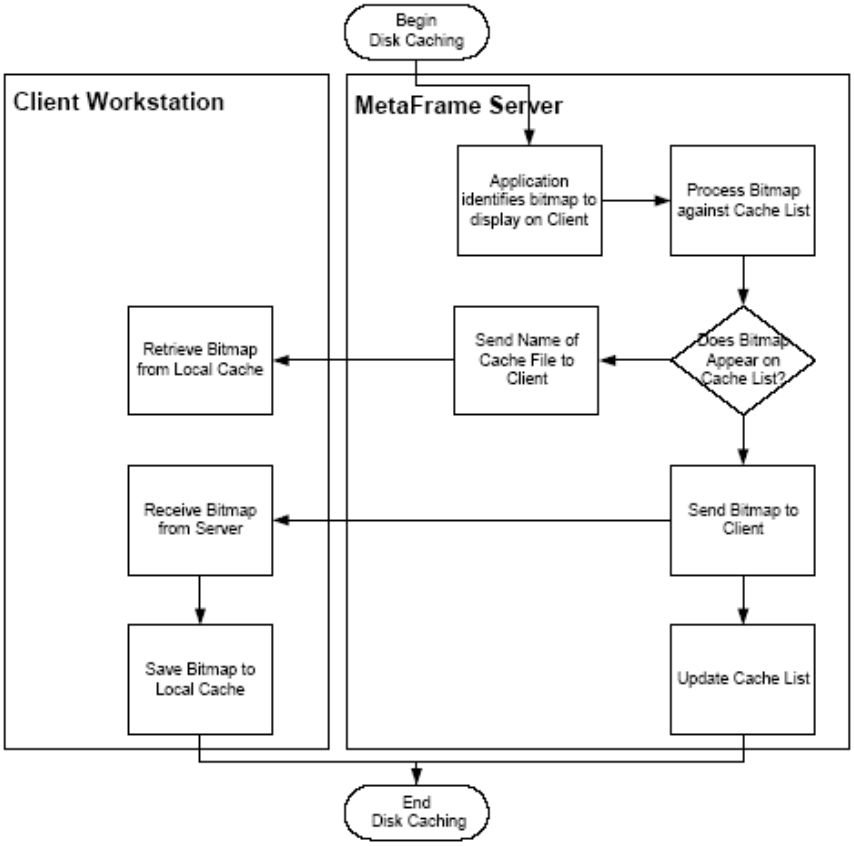


Disk cache for bitmaps

Use Disk Cache for Bitmaps utilizes local hard disk space to store commonly-used graphical objects such as bitmaps in a local disk cache on the client. When a server application identifies a bitmap to be displayed, the server sends the bitmap through the ICA session over the network to the ICA Client. The ICA Client then stores the bitmap locally for future use. When the ICA Client requires this same bitmap again, the locally cached bitmap is used, as shown in the diagram. Use disk cache for bitmaps can be enabled or disabled through the user interface on the client, which directly modifies the following .ICA file parameters.

ICA Client Setting	ICA File Parameter	Description	Default Value
Use disk cache for bitmaps	PersistantCacheEnabled	Enables (on) Disables (off) disk caching	Enabled (on) when connection type is WAN Disabled (off) when connection type is LAN

	PersistentCacheSize	Sets the maximumdiskspace in bytes allowed or caching bitmaps	10mb
	PersistentCacheMin Bitmap	Defines the minimum size in bytes a bitmap must be before it is cache	8kb
	PersistentCachePath	Specifies the directory path to the diskcache	%userprofile%\applicationdata\icaclient



Further citrix options/tuning enhancing user experience

From the client side, some options should also be considered. Caching should be enabled .The following can be disabled, to enhance login speed:

- Client drive mapping
- Client com port mapping
- Client printer mapping
- Use of print spooler
- Client audio
- Client update

On the server disable the wallpaper or use a very simple wallpaper to reduce bandwidth and memory requirements.

Virtual Channel Buffering is only available with Citrix MetaFrame XP Feature Release 1 and later.

2.7. Network sizing & Scalability

2.7.1 Bandwidth analysis

The bandwidth to be reserved for Citrix depends on the following parameters:

- The number of clients using the citrix-service at the same moment.
- The graphic mode the client is running.
- The graphical grade of the applications the client is running.
- Usage of Mouse Movement- and Keystroke-queuing.
    - Queuing causes the client to send mouse and keyboard updates less frequently to the Citrix server.
- Disk-caching on the client
- Bitmap caching to disk uses local hard disk space to store commonly used graphical objects such as bitmaps in a local disk cache on the client.
- Data-compression on the client
    - Data compression reduces the amount of data that needs to be transferred by utilizing additional processor resources to compress and decompress the data.
- Usage of Speedscreen latency reduction
    - Latency reduction is a collective term used to describe the functionality that helps enhance user experience on slower network connections.

ICA Client bandwidth analysis:

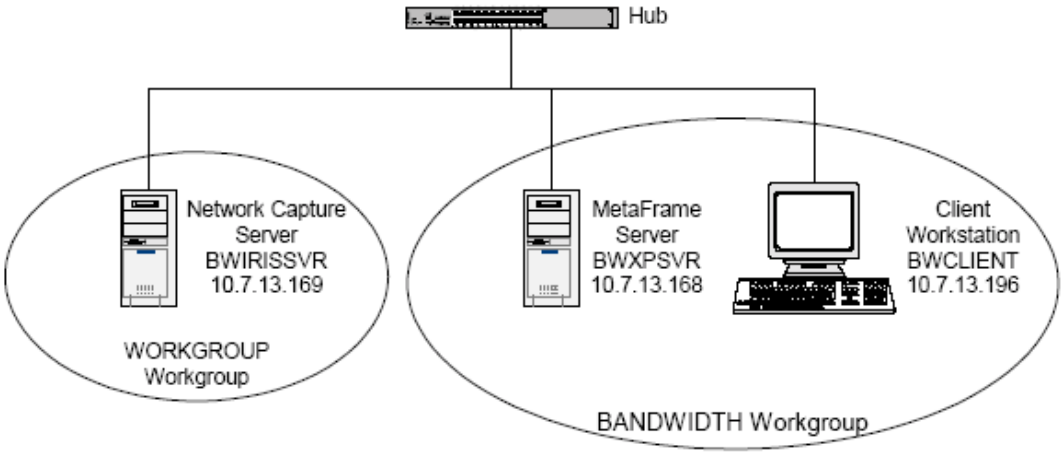
Two scripts were created to analyse the bandwidth usage in various cases. The first script is a script that analyses the bandwidth usage when a user is just typing some text. The second script analyses the bandwidth usage when a graphical application is used.

The text based script opens Microsoft Word, and writes 10 paragraphs of six sentences each, typing 10 words each sentence. The script types 40-50 words per minute. After every 3 or 4 paragraphs the document is saved using keyboard shortcuts. During the creation of the document the font type is varied several times.

The graphical test script opens Microsoft Powerpoint and maximizes the window to take up the entire desktop. The script then opens the first Powerpoint presentation file from a directory on the hard disk. Then a slide show is started by pressing the F5 key. The mouse is used to click through each slide. When the slide show is over, the mouse is first used to close the presentation and then the Powerpoint application by clicking on the X in the top right corner.

Test setup

The following test setup was used to analyse the bandwidth usage of the two testscripts:



The test setup consists of a network capture server, a MetaFrame server and a client workstation all on the same network, connected by a Hub. A hub is used in this test to watch all ICA traffic between the client workstation and the MetaFrame server from the network capture server. A specification of the systems used in this test can be found in Annex B

Client configurations

Different combinations of ICA client configurations were tested:

ID	Use data compression	Use disk cache for bitmaps	Queue mouse movements and keystrokes	Speedscreen mouse click feedback	Speedscreen local text echo
data_01					
data_02	X				
data_03*	X	X			
data_04	X	X			
data_05	X		X		
data_06	X	X	X		
data_07**	X			X	X
data_08	X			X	X
data_09	X	X		X	X
data_10	X		X	X	X
data_11	X	X	X	X	X

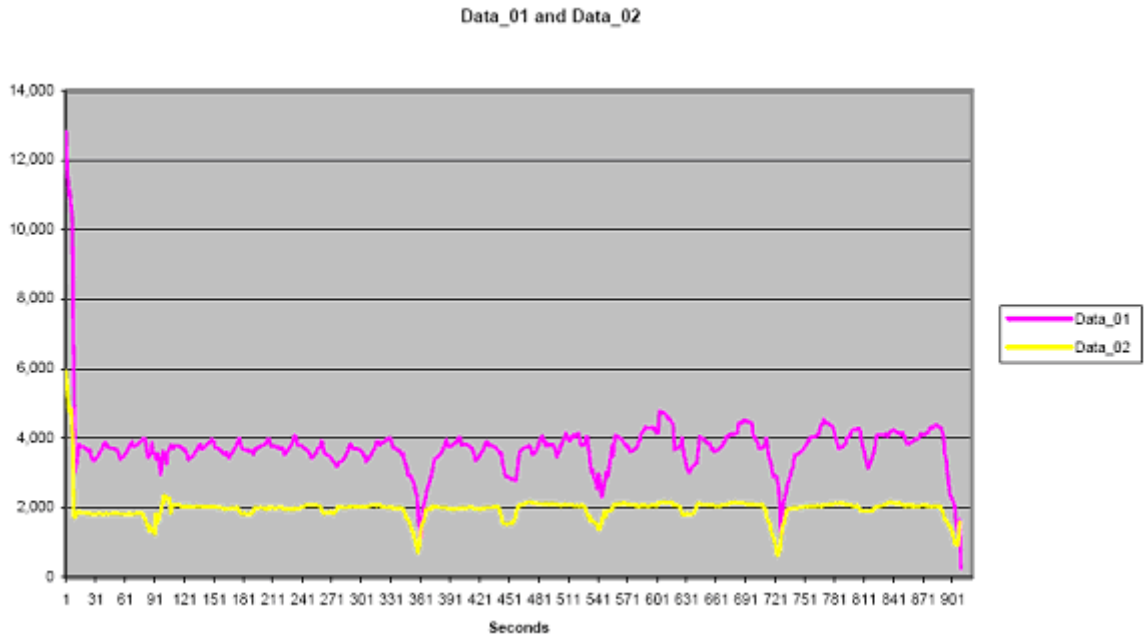
*Data_03 is a duplicate of Data_04, but it is executed without a baseline cache for only the PowerPoint test

** Data_07 is a duplicate of Data_08, but it is executed without a baseline cache for both the typing test and the PowerPoint test.

table 1 – the different ICA client settings

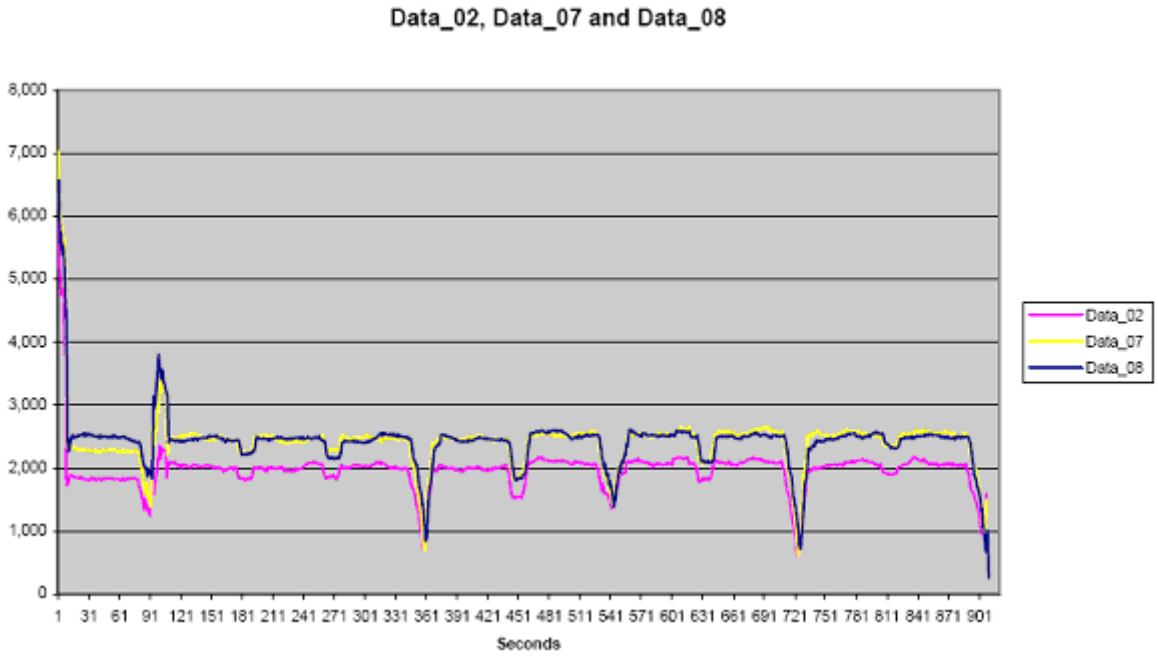
Observations Word script

The following observations were made about the different ICA Client settings shown in table 1 based on test results of the text-based test script using Microsoft Word. The time is placed on the X-axis, the bandwith (bytes / second, incoming) is placed on the Y-axis.



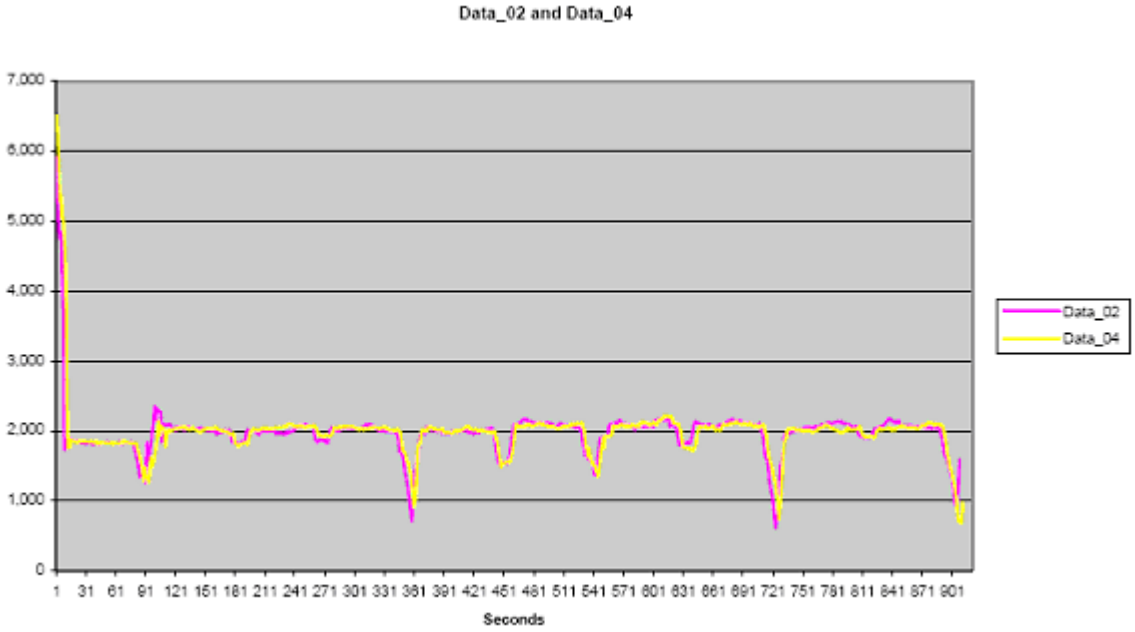
graph 1 - Bandwidth Usage for Data_01 and Data_02

- Data Compression reduces bandwidth by approximately 50% as shown in graph 1, but slightly increases processor usage on the client workstation by approximately 0.5%.



graph 2 - Bandwidth Usage for Data_02, Data_07 and Data_08

- SpeedScreen Latency Reduction settings do not show a significant difference in bandwidth, whether (Data_08) or not (Data_07) a baseline cache is present. SpeedScreen Latency Reduction settings increase bandwidth usage by approximately 17% when compared to the results of using Data Compression alone (Data_02) as shown in graph 2.

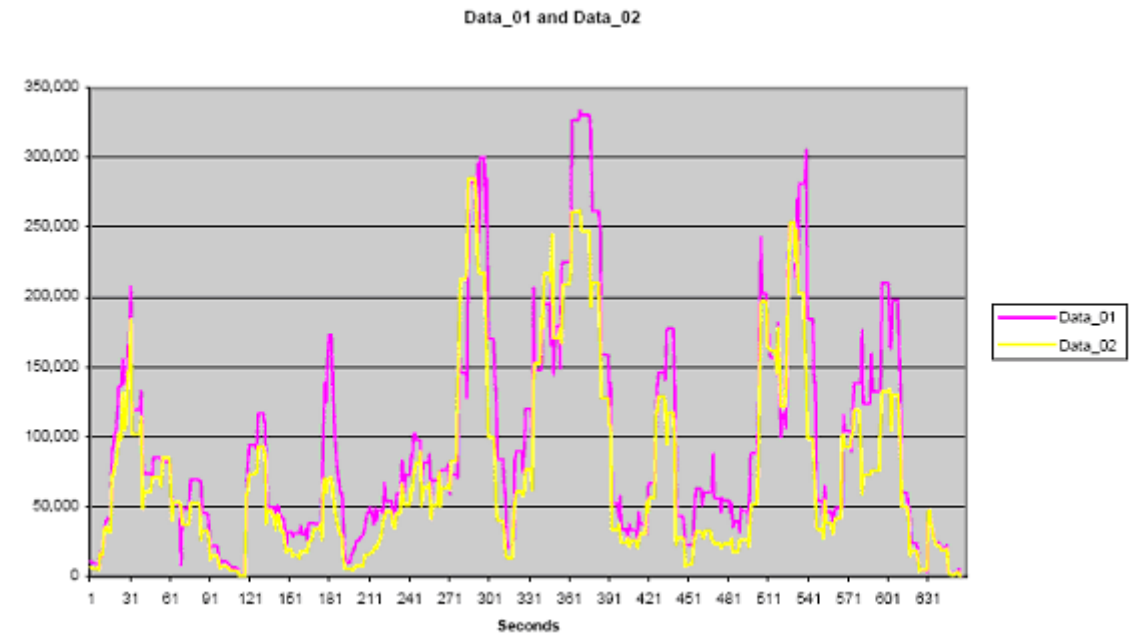


graph 3 - Bandwidth Usage for Data_02 and Data_04

- Use Disk Cache for Bitmaps (Data_04) does not have an impact on bandwidth usage when compared to Data Compression alone (Data_02) as shown in graph 3.

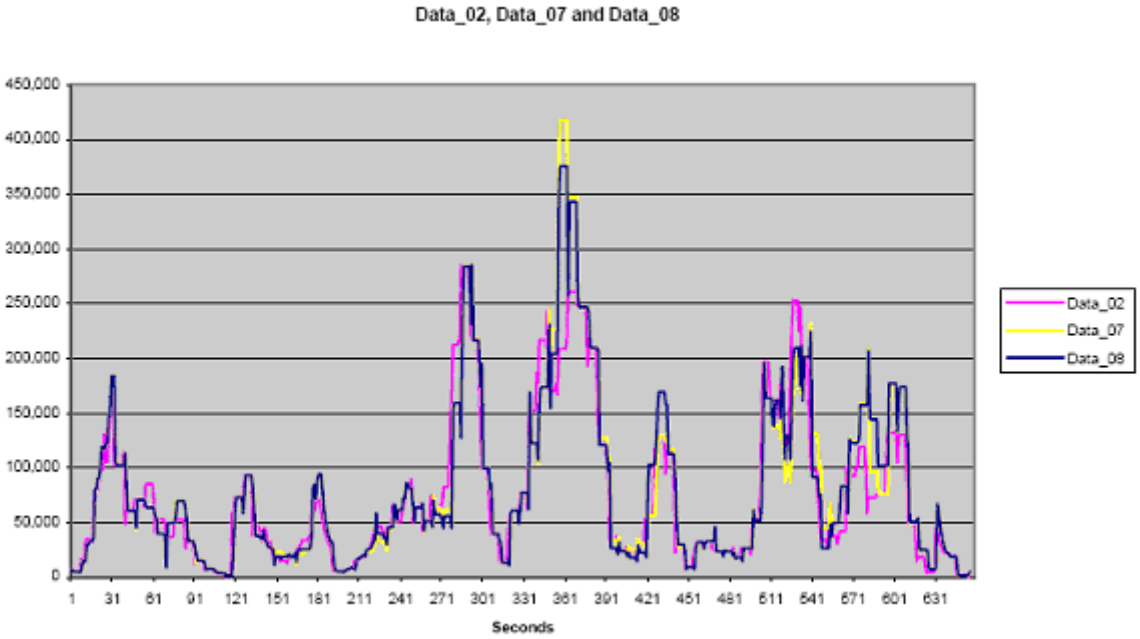
Observations Powerpoint script

The following observations were made about the different ICA Client settings as shown in table 1 based on test results of the graphic-rich test script using Microsoft PowerPoint. Again, the time is placed on the X-axis, the bandwith (bytes / second, incoming) is placed on the Y-axis.



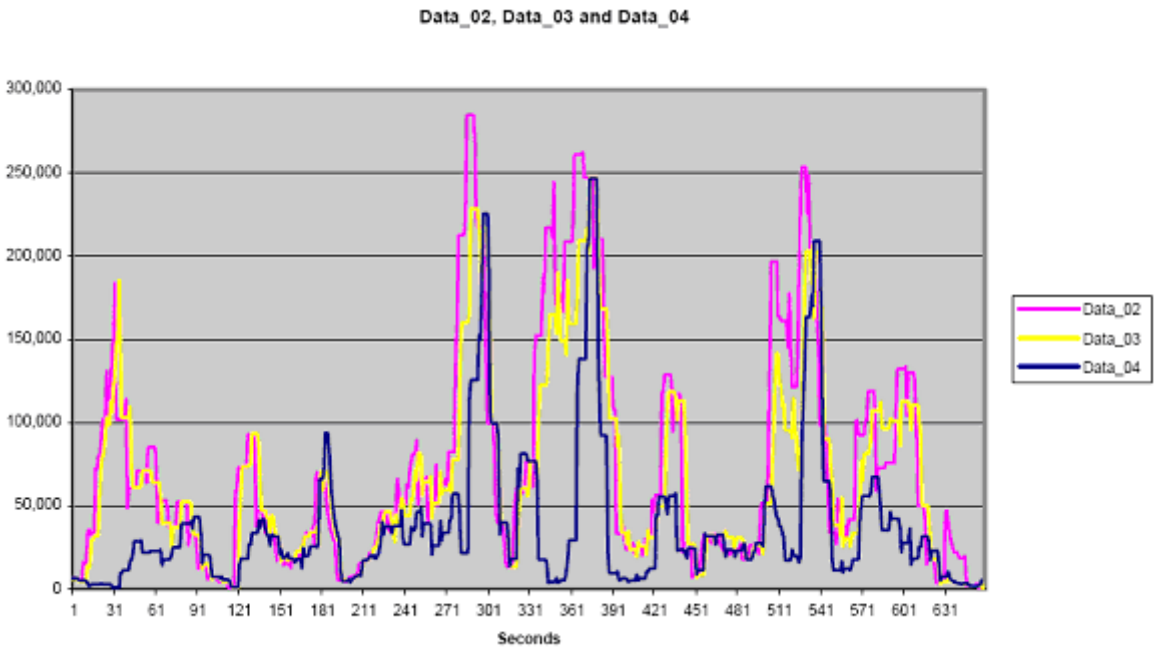
graph 4 - Bandwidth Usage for Data_01 and Data_02

- Data Compression reduces bandwidth by approximately 25% as shown in graph 4, but slightly increases processor usage on the client workstation by approximately 1.5%.



graph 5 - Bandwidth Usage for Data_02, Data_07 and Data_08

- SpeedScreen Latency Reduction settings do not show a significant difference in bandwidth, whether (Data_08) or not (Data_07) a baseline cache is present. There is a slight increase in bandwidth of approximately 0-4% when SpeedScreen Latency Reduction settings are compared to the results of using Data Compression alone (Data_02) as shown in graph 5.



graph 6 - Bandwidth Usage for Data_02, Data_03 and Data_04

- Use Disk Cache for Bitmaps without a baseline cache (Data_03) reduces bandwidth by approximately 4% as illustrated in graph 6, and with a baseline cache (Data_04) significantly reduces bandwidth by approximately 50% when compared to testing with Data Compression alone (Data_02).

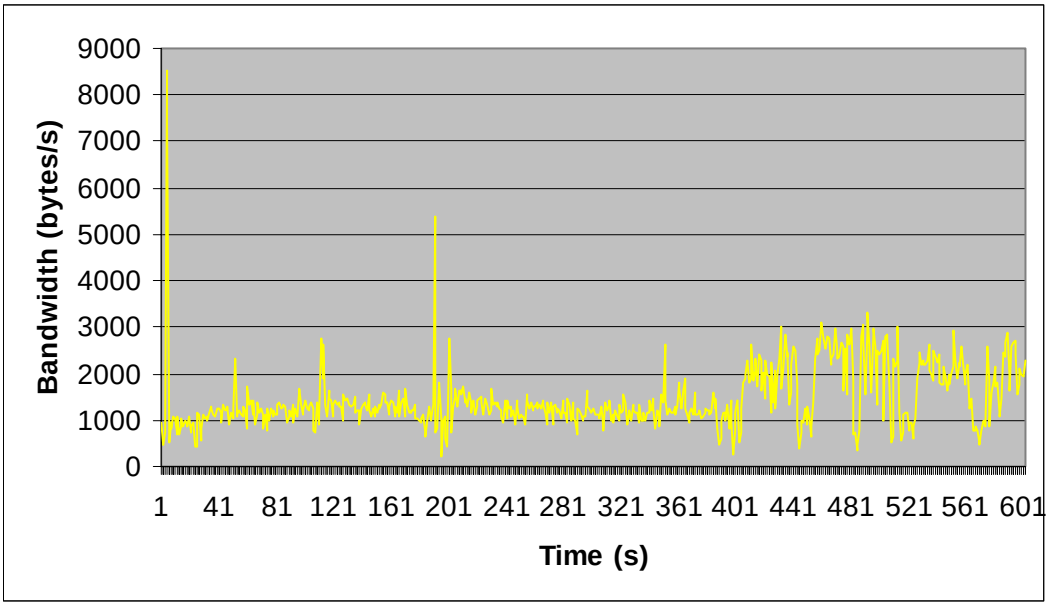
DVB-RCS test

The Word test and the powerpoint test have also been performed over a DVB-RCS network. The test with Microsoft word can be compared to the other tests. The Powerpoint test is a little different since another presentation was used, this presentation had more bitmaps at the start of the presentation and less bitmaps at the end of the presentation.

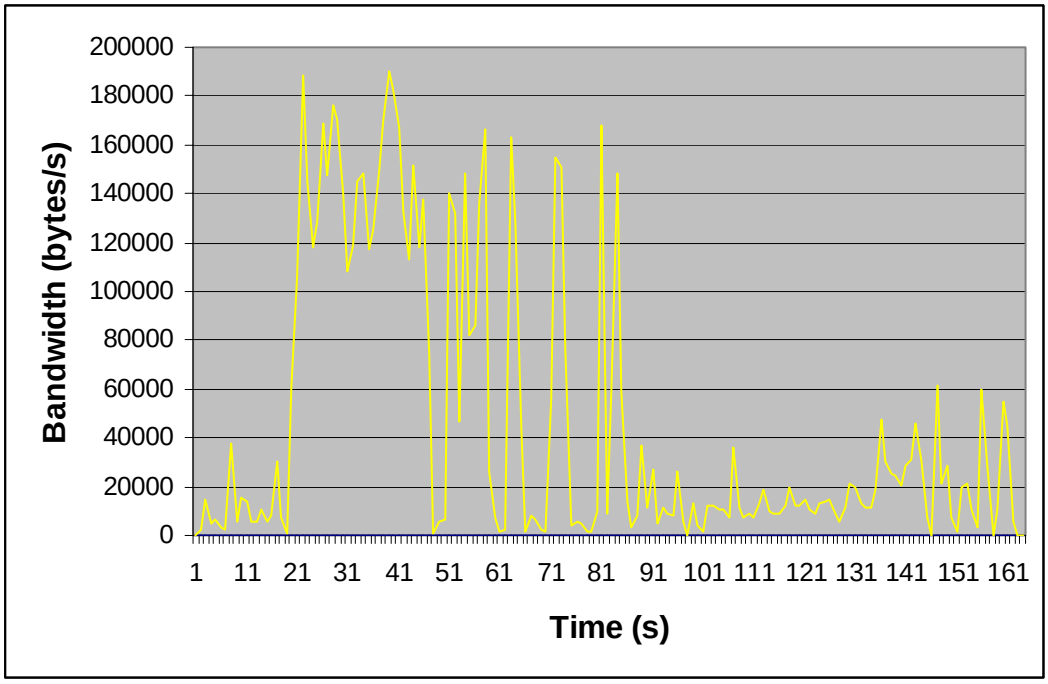
The following settings were enabled to get an optimal performance:

- Use data compression
- Use disk cache for bitmaps
- Queue mouse movements and keystrokes
- Speedscreen mouse click feedback
- Speedscreen local text echo

Results of the Word test



Results of the Powerpoint test



2.7.2 Minimizing broadcast traffic

IP addressing encompasses the IP identification of the server. To minimize cross-network broadcast traffic, two technologies are commonly used: subnetting and virtual LAN. If a bridged network solution is used, the problem of the cross-network broadcast traffic will arise. In that case subnetting and virtual LANs must be used to solve this problem. It is smarter to use a routed solution instead of a bridged solution. Subnetting and virtual LANs are discussed below.

Subnetting

In a standard networking environment, when a broadcast is received on a subnet, each host acknowledges the packet, although only the host(s) with the destination IP address and corresponding MAC address respond. Subnetting creates smaller broadcast domains. Subnetting the network wherein the MetaFrame servers are located is an excellent method of ensuring that both network broadcasts and network traffic are minimized. If the number of hosts within the network is minimized by subnetting, only the packets that are actually destined for the segmented group MetaFrame servers will reach that subnet.

Virtual LANs

A virtual LAN (VLAN) is a Layer 2 switching technology used to create segmented broadcast domains. Switch ports are configured so as to designate each port or MAC address as part of a specific VLAN. Either the physical switch port is statically assigned to the VLAN or the MAC address of the server can be dynamically assigned to the VLAN. Generally, a one-to-one ratio exists between a VLAN and a subnet. All configured devices in each VLAN are members of the same broadcast domain.

Instead of propagating multicasts and broadcasts to all other ports on one or more switches, only the port(s) logically defined as being within the same VLAN receive the multicasts or broadcasts. This is dictated by the source port and IP address. It is becoming more popular to use Layer 3 switches to support VLAN technology for separating smaller subnets, with reliance on more complex and expensive routers only for inter-LAN traffic.

MetaFrame servers can benefit greatly by being associated with the same subnet and VLAN. If MetaFrame servers are not physically co-located and plugged into the same switch, VLAN technology may provide the best solution since this technology allows the MetaFrame servers to logically reside on the same subnet. This may be particularly useful for a backup server farm or operations center that is located elsewhere.

2.7.3 Bandwidth

MetaFrame sessions should be estimated at an average minimum of 20 Kbps of bandwidth unless application-specific testing indicates otherwise. If sufficient bandwidth is not available, it is likely that the user experience will be poor, including dropped sessions.

Particularly as it relates to satellite connections and wireless wide-area networks, consistency of the connection is important; dropped frames are not conducive to consistent ICA connections. If a user connection is dropped, the Version 6.00 and higher ICA Clients will automatically attempt to reconnect the user connection.

When architecting or diagnosing network issues within a MetaFrame environment supporting a large number of users, not only should 20 Kbps per user be allocated, but also additional capacity must be allocated for ICA session printing, non-MetaFrame traffic, and general overhead, e.g., routing protocol broadcasts or multicasts, routing decisions, and ICMP traffic as applicable.

2.7.4 Conclusion

The network environment scenario as we will use it describes a network where latency is high and bandwidth constraints exist that requires the most efficient bandwidth usage possible, in order to achieve the fastest response time for the user. In this environment, the Data Compression, Use Disk Cache for Bitmaps, and SpeedScreen Latency Reduction settings should be used. This recommendation provides the following benefits:

- Enhanced user experience – SpeedScreen Latency Reduction provides additional user experience benefits, including instant mouse click feedback and keystrokes that are displayed based on cached data instead of waiting for a server response.
- Reduced bandwidth usage – The Use Disk Cache for Bitmaps and Use Data Compression settings reduce the amount of network bandwidth required for each ICA session.
- Faster response due to disk caching – Cached files are used to render images on the client workstation, eliminating the time it takes to request and receive an image.

The following potential drawbacks must be considered:

- Client workstation processor resources - While Data Compression requires some additional processor usage on the client workstation, the impact is minimal. However, if client resources are a priority, this should be monitored closely.
- Client workstation hard disk resources – The Use Disk Cache for Bitmaps and SpeedScreen Latency Reduction settings require hard disk space on the client workstation. Test results indicate that the Use Disk Cache for Bitmaps setting requires approximately 10MB of hard disk space for the graphic-rich tests (no hard disk space was used for the text-based tests), and the SpeedScreen Latency Reduction settings required approximately 10KB of hard disk space for both types of tests. The client workstation must have suitable hard disk space available before enabling these settings.
- Bandwidth increase due to SpeedScreen Latency Reduction - The SpeedScreen Latency Reduction settings slightly increase bandwidth. However, the benefits to the user experience outweigh the minimal impact of the bandwidth increase.

To minimize broadcast traffic, Subnetting and Virtual LANs must be used to avoid the cross-network broadcast traffic problem.

MetaFrame sessions should be estimated at an average minimum of 20 Kbps of bandwidth unless application-specific testing indicates otherwise. Consistency of the connection is important; because of this prioritising is important when a DVB/RCS connection is used for multiple purposes. If the DVB/RCS connection is used for only Citrix, there is nothing to prioritise. If the DVB/RCS connection is used for more than just Citrix, Citrix should be given QOS in the firewall for example.

3. Satellite specific security issues for Citrix Clients

3.1. Types of VPN's

VPN solutions can be roughly devided in 3 different groups:

- PPTP (layer 3 tunneling)
- L2TP (layer 2 tunneling)
- IPSEC (transport level)

For the 3 different groups all different kinds of encryption can be used, from DES to 3DES, blowfish or any other. IPSEC is the only protocol which also defines the end parties of the connection and not only the encryption of the data.

As the satellite is an open network, and anybody with the correct knowledge can intercept all sent and received data, it is important to use encryption over satellite. Considering this it is also smart to use an encryption which is more difficult in being deciphered.

3.2. Combinations of VPN's with Citrix & DVB-RCS

For security of Citrix you can use build in SSL functionality of Citrix or you can rely on the security delivered by a VPN. On choosing a correct security model you should look at the complete setup of the satellite solution.

Depending on the used satellite hardware some VPN solutions might have problems in the connection over the satellite. Especially the packet delay may have problems in certain implementation's of VPN hardware which require low latency or else the VPN hardware will drop a connection, or even refuse to make a connection.

Second problem that can be encountered is in terminal hardware which incorporates satellite enhancements like TCP PEP & TCP spoofing. There are VPN solutions which are very strict in allowing 3rd party products in altering IP header or TCP header information. When the hardware detects altered packets it will also refuse to make a connection. In this case the TCP enhancements can be disabled, but this also means, the average throughput of the satellite system will drop, and optimisation will have to be done on another place of the network.

There are many different implementations of VPN solutions, it is beyond the scope of this document to list good and bad working VPN hardware.

At the moment of this writing there is special VPN IPSEC hardware for VSAT terminals which is fully optimized for satellite networks (UDCAST, www.udcast.com)

Depending on the type of application you plan to provide over the satellite you may need such an accelerator. When you use mostly text, like database application's there is no need for an accelerator. When your application also sends photos or other large blocks of data, an accelerator is desired.

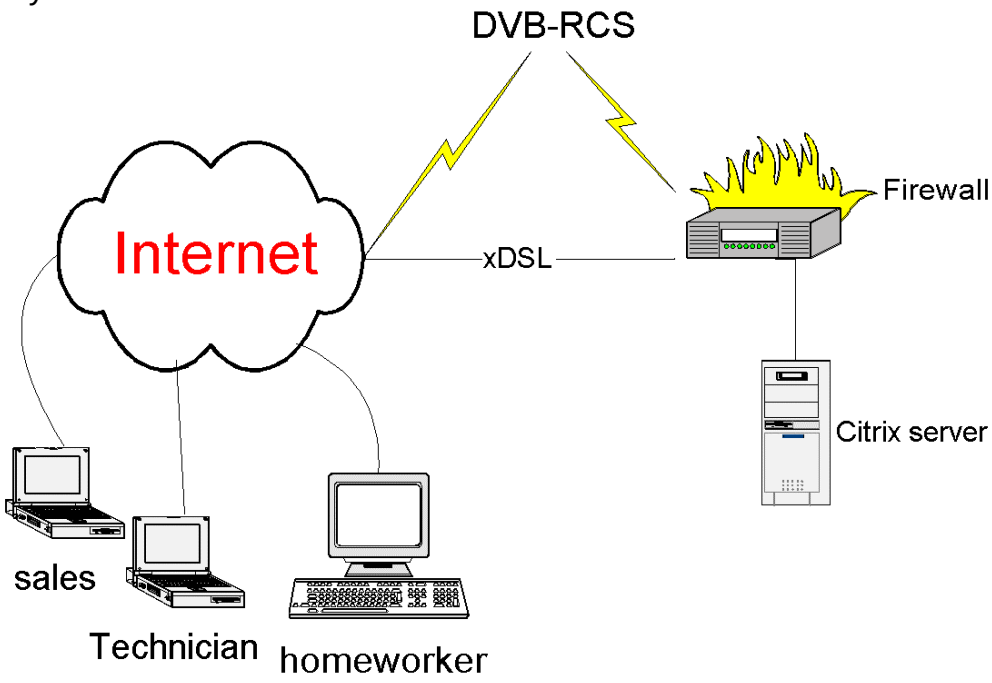
USE Cases

4. De Kooi Groep

De Kooi Groep is a combination of different companies. For their work internet connectivity is trivial, so they are connected to the internet using a xDSL solution. To be sure of connectivity they have a backup-line using a BySky DVB-RCS system on the Satlynx platform.

The main connectivity consists of E-Mail and Web traffic. Additional functionality was introduced using CITRIX. With CITRIX it became possible to enable remote network support, and remote workplaces for helpdesk, secretarial work and sales/technicians access who are at a client or in a hotel.

The main reason for the choice of CITRIX was the ability to provide a good working environment when for some reason the network is using the DVB-RCS system.



Netwerk structuur Citrix De Kooi Groep 1

Using routers to do the fail safe routing, this way only specific issues of the satellite have to be addressed. Standard email and web traffic will work fine over the DVB-RCS connection.

Settings

CITRIX
The Citrix server is configured to use speedscreen when higher latency is discovered. Speedscreen in this case of De Kooi Groep is enabled for Microsoft Word, Notepad, Excel, Access. Without Speedscreen these applications would not be workable. Speedscreen has been configured with the Latency buffer see chapter 2.6

Considerations
When looking for “De Kooi”, different scenario’s have been considered. In the end a solution without PEP’s is chosen. A PEP is only used in cases where much bandwith is needed in short time intervals. In our case we do not need PEP since they only use applications like Word, Access, etcetera. These applications have no high bandwidth needs, so no PEP is implemented.

Client configuration
The different CITRIX clients have a simple configuration. The following optimisations are enabled: Speedscreen, Keyboard & mouse queueing, Caching.

Firewall
The firewall is configured as a traditional firewall. This means it is not doing Port or Adress translation. It will only block or accept traffic according to it’s ruleset. Regarding the CITRIX server, the firewall blocks all traffic except VPN’s from specific predefined IP numbers and Standard CITRIX SSL connection’s from specific IP numbers.

5. Summary

When you are planning to use a remote desktop environment, there are many different products available. For this purpose, Microsoft Windows 2000 terminal and Citrix MetaFrame are the best options. Citrix provides some features that Windows 2000 terminal does not offer, features such as the ability to do automatic drive redirection and com port redirection. Another advantage of Citrix over Windows 2000 terminal is that Citrix MetaFrame has the ability to run on virtually any client over virtually any connection.

Using Citrix in a satellite environment offers some additional advantages which are not available in other products. These advantages are:

- Mouse and keyboard queueing
- Caching of bitmaps
- Speedscreen latency reduction

The advantages mentioned above make Citrix the best product to use in a remote desktop environment, especially when using a satellite environment. The purpose of this document is to describe the functionality and network setup of Citrix over DVB-RCS.

Using Citrix in a satellite environment can accomplish good results. The only problem will be the TCP connection to the Citrix server. This TCP connection is not optimal in a standard Windows configuration. Configuring the TCP settings on the client and the server side can solve this problem. Another option is to use a satellite accelerator. To get an optimal performance from Citrix over a DVB-RCS link, speedscreen should be enabled, channel buffering should be used and in many cases ICA data compression provides good results. Another option to get a faster response time is to use disk cache for bitmaps.

In a bridged network solution subnetting and virtual LAN are used to minimize the cross network broadcast traffic. Subnetting creates smaller broadcast domains, so that only the packets that are actually destined for the segmented group MetaFrame servers will reach that subnet. A VLAN is a technology used to create segmented broadcast domains. Either the physical switch port is statically assigned to the VLAN or the MAC address of the server can be dynamically assigned to the VLAN. All configured devices in a VLAN are members of the same broadcast domain. MetaFrame servers can benefit greatly by being associated with the same subnet and VLAN.

MetaFrame sessions should be estimated at an average minimum of 20 Kbps of bandwidth unless application-specific testing indicates otherwise. Consistency of the connection is important; because of this prioritising is important when a DVB/RCS connection is used for multiple purposes. If the DVB/RCS connection is used for only Citrix, there is nothing to prioritise. If the DVB/RCS connection is used for more than just Citrix, Citrix should be given QOS in the firewall for example.

For security of Citrix you can use built in SSL functionality of Citrix or you can rely on the security delivered by a VPN.

Abbreviations

ACK	Acknowledge
(A)VBDC	(Absolute) Volume Based Dynamic Capacity
CIFS	Common Internet File System
CRA	Continuous Rate Assignment
DES	Data Encryption Standard
DVB-RCS	Digital Video Broadcast-Return Channel System
DSL(xDSL)	Digital Subscriber Line
FCA	Free Capacity Assignment
ICA	Independent Computing Architecture
ICMP	Internet Core Message Protocol
IP	Internet Protocol
IPSEC	IP Security
IPX	Internetwork Packet eXchange
ISDN	Integrated Services Digital Network
L2TP	Layer 2 Tunneling Protocol
MAC	Medium Access Control
MTU	Maximum Transfer Unit
NAS	Network Attached Storage
NCP	Netware Core Protocol
Netbeui	NetBios Extended User Interface
PC	Personal Computer
PPTP	Point to Point Tunneling Protocol
PSTN	Public Switched Telephone Network
RBDC	Rate Based Dynamic Capacity
RDP	Remote Desktop Protocol
SACK	Selective Acknowledgement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet eXchange
SSL	Secure Sockets Layer
TCO	Total Cost of Ownership
TCP	Transport Control Protocol
TCP-PEP	Transport Control Protocol – Performance Enhancing Protocol
TTL	Time To Live
Proxy	A server that sits between a client application and a real server
(V)LAN	Virtual Local Area Network
VPN	Virtual Private Network

6. References

[1] *Harder, J., 2003. Networking Issues Affecting Citrix® MetaFrame Environments Whitepaper.*

[2] *Citrix Consulting Services for Citrix Systems Inc., 2001. ICA Client Bandwidth Analysis.*

[3] *Smith, D., 2001. When does Citrix provide value over Win2K Terminal Services?*

[4] *www.speedguide.net., 2003. Optimization tools FAQ.*

[5] *Citrix Consulting Services for Citrix Systems Inc., 2001. ICA Client Bandwidth Analysis Test Environment.*

[6] *Systems Inc., 2001. Citrix® MetaFrame XP Security Standards and Deployment Scenarios*

[7] *Citrix Systems, 2002. Optimising Citrix Technology for Operation over 1xRTT Networks*

[8] *Citrix Systems, Optimizing Citrix technology for operation over wireless Wide Area Networks*

[9] *Nera Broadband Satellite AS (NBS),2002. Digital Video Broadcasting, Return Channel via Satellite (DVB-RCS) Background Book*

[10] *Satlabs 2003, SatLabs System Recommendations*

Annex A

TCP optimizer edits the following TCP settings on your client:

- MTU discovery
    - MTU means Maximum Transmission Unit and describes, in bytes, the largest possible TCP packet size. The default MTU size is 1500 bytes for Ethernet, on the Internet, however, the default MTU size is 576 bytes.
- TCP receive window size
    - The TCP receive window size is a TCP setting that dictates how much data is received before the receiving computer sends back an ACK packet. If the TCP Window Size is enlarged, the computer doesn't have to send quite as many ACK packets for the data received, and therefore can have that much more latency and bandwidth off the connection.
- Black hole detection
    - Black Hole Detection attempts to find out if there are routers out there that don't forward a key piece of packet information -- specifically, the "Don't Fragment" bit. If the Don't Fragment bit is set, then packets are sent through in sequence, and the MTU is decreased to allow faster transmission. Routers that don't forward this information will allow the TCP stack to increase the number of retransmission tries to compensate.
- Selective ACKs (SACK)
    - TCP may experience poor performance when multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can only learn about a single lost packet per round trip time. An aggressive sender could choose to retransmit packets early, but such retransmitted segments may have already been successfully received. Selective Acknowledgment (SACK) is a strategy which corrects this behaviour in the face of multiple dropped segments. With selective acknowledgments, the data receiver can inform the sender about all segments that have arrived successfully, so the sender needs to retransmit only the segments that have actually been lost. The selective acknowledgment extension uses two TCP options. The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which may be sent over an established connection once permission has been given by SACK-permitted. The SACK option is to be included in a segment sent from a TCP that is receiving data to the TCP that is sending that data; we will refer to these TCPs as the data receiver and the data sender, respectively. We will consider a particular simplex data flow; any data flowing in the reverse direction over the same connection can be treated independently.
- Maximum number of duplicate ACKs
    - This allows for faster retransmission of packets (information), when packet loss is encountered.
- Maximum number of connections per server

    - One setting which can pay off for web browsing is MaxConnectionsPerServer. The HTTP 1.1 spec states that a client can only open up to two connections to a web server at a given time. If you change this setting, you can enlarge this number (the recommended upper limit for this is 4).
- TTL
    - The Time To Live, or TTL, is a value that indicates how many hops a packet can traverse before it is considered lost or misrouted. The upper bound for this is 32 by default, and many routers will force a packet that comes in with a TTL higher than 32 to be dropped back to 32.

Annex B

Hub Specifications

- 3Com OfficeConnect Hub 8/TPO (Product #: 3C16700)
- 8 ports
- 10Mb Ethernet

Network Capture Server Specifications (BWIRISSVR)

- Compaq Proliant DL360
- Dual Intel Pentium III 800Mhz processors
- 1GB RAM
- 2 mirrored 9.1 GB hard drives
    - Hidden System Partition – 36MB
    - C: Drive – 4GB
    - D: Drive – 4.5GB
- Network
    - 2 Compaq NC3163 Fast Ethernet NIC adapters, only the first is enabled (supports promiscuous mode)
    - No DHCP
    - IP Address: 10.7.13.169
    - Subnet Mask: 255.255.255.0
- Software
    - Windows 2000 Server, SP2
    - Eeye Iris 3.60 Build 3 (latest evaluation version from www.eeye.com)
- Display Configuration
    - 1024x768
    - True Color (24 bit)

MetaFrame Server Specifications (BWXPSVR)

- Compaq Proliant DL360
- Dual Intel Pentium III 800Mhz processors
- 1GB RAM
- 2 mirrored 9.1 GB hard drives
    - Hidden System Partition – 36MB
    - C: Drive – 4GB
    - D: Drive – 4.5GB
- Network
    - 2 Compaq NC3163 Fast Ethernet NIC adapters, only the first is enabled
    - No DHCP
    - IP Address: 10.7.13.168
    - Subnet Mask: 255.255.255.0
- Software
    - Windows 2000 Server, SP2

    - MetaFrame XP 1.0, FR1 (local MS Access Data Store, farm name - BWTEST)
    - Citrix Resource Management Services (RMS) 1.0b
    - Microsoft Office 2000
    - Adobe Acrobat Reader 5.0.1
    - WinZip 8.0
- Display Configuration
    - 1024x768
    - True Color (24 bit)
- Published Applications: “MS Word”, “MS PowerPoint”
    - 1024X768
    - True Color (24 bit)
    - Maximize application at startup
    - Audio On
    - Basic Encryption
    - Normal CPU Priority
    - Local Administrators and Local Users are permitted access
- User Configuration
    - Local username: bwuser, Password: password

Client Workstation Specifications (BWCLIENT)

- Dell Optiplex G1 (Service Tag 3PI2B)
- Intel Celeron 433 Mhz processor
- 128MB RAM
- 6GB hard drive
    - C: Drive – 4GB
    - D: Drive – 2GB
- Network
    - 3Com 3C918 Integrated Fast Ethernet Controller (3C905B-TX Compatible)
    - No DHCP
    - IP Address: 10.7.13.196
    - Subnet Mask: 255.255.255.0
- Software
    - Windows 2000 Professional, SP2
    - ICA Client V 6.20.985
    - WinBatch 2001N (latest evaluation version from www.winbatch.com)