A REPORT ON CITRIX INDEPENDENT COMPUTING ARCHITECTURE (ICA) PROTOCOL

by

I V S K CHAITANYA 13026A0406

Jawaharlal Nehru Technological University Kakinada

A REPORT ON CITRIX INDEPENDENT COMPUTING ARCHITECTURE (ICA) PROTOCOL

INTRODUCTION:

- ICA stands for Independent Computing Architecture. It is a proprietary protocol for an application server system, designed by Citrix Systems.
- The aim of developing ICA was to streamline the data delivery process between a server and a client without binding it to a specific platform or transport protocol.
- ICA is designed to run on top of many operating systems including Windows, Linux, iOS.
- ICA is designed to run over industry-standard network protocols, such as TCP/IP, NetBEUI, IPX/SPX, and PPP and industry-standard transport protocols, such as async, ISDN, Frame Relay and ATM.

ICA PROTOCOL EVOLUTION:

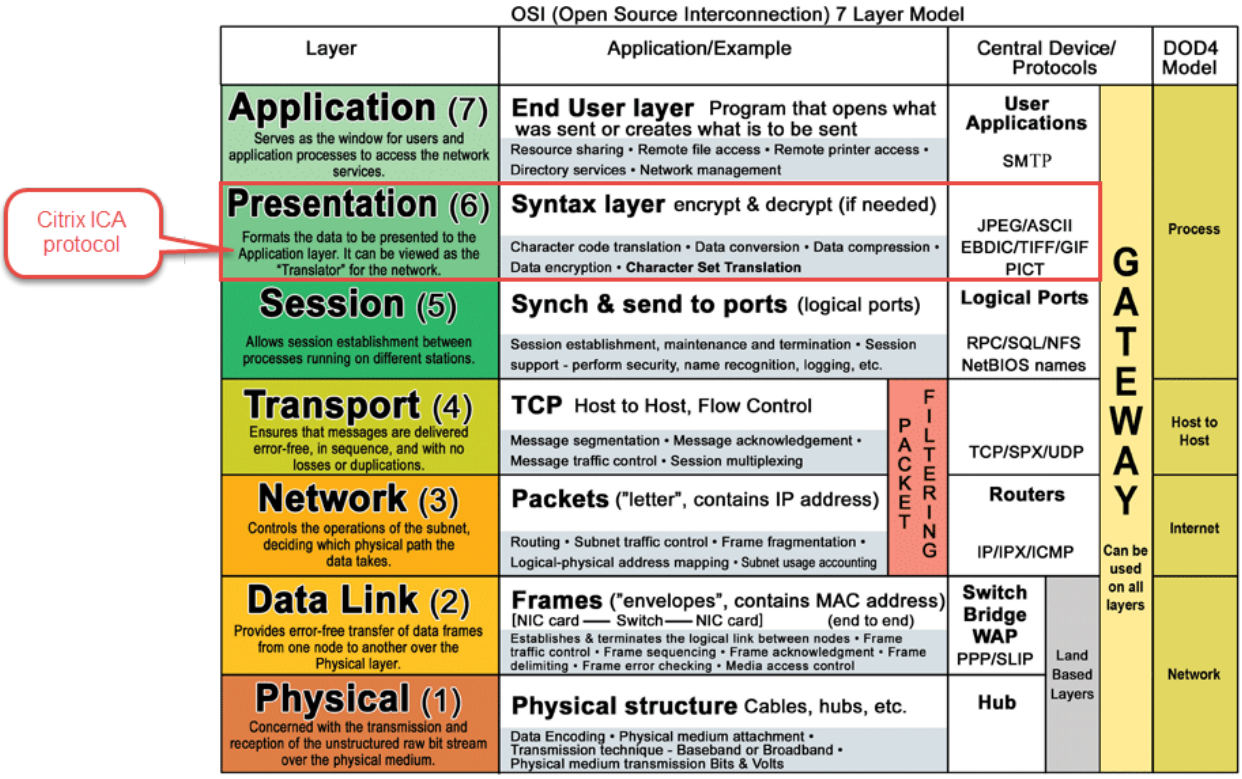
- First version of ICA protocol was developed in 1989-1990 and was used in Citrix Multiuser OS/2.
- In 1992 Citrix signed licensing agreement with Microsoft for NT Server which resulted in WinFrame
- WinFrame – a multi-user version of Windows NT 3.51 which was fully repackaged by Citrix.
- At this stage of the product development Citrix Systems licensed the Windows NT 3.51 base operating system from Microsoft.
- The core development that Citrix delivered was the Multi-Win engine. This allowed multiple users to logon and execute applications on a WinFrame server with use of ICA protocol.
- Citrix licensed the Multi-Win technology to Microsoft few years later, forming the basis of Microsoft's Terminal Services.
- This version of ICA is an ancestor of Microsoft RDP protocol.
- Citrix MetaFrame is widely used today to provide users with access to critical business applications via server-based computing and Terminal Server technologies.

DIFFERENCE BETWEEN ICA PROTOCOL AND RDP PROTOCOL:

ICA PROTOCOL	RDP PROTOCOL
ICA is a proprietary protocol of Citrix, designed by Citrix Systems.	RDP is a proprietary protocol developed by Microsoft.
It is designed to transverse data between Server and Client.	It is used to access the server from client over the network.
ICA is not only restricted to one OS, it can be used to Linux, Unix, MAC and even on smart devices	It is used in only windows operating system
It works on all network layer and transport layer protocols	It works only on tcp/ip protocol
ICA Protocol compresses data between Server and Client and requires about 20 KBPS per connection.	RDA protocol not need compression technique
Encryption is possible In ICA.	Only 128-bit encryption, using the RC4 encryption algorithm, as of Version 6.
ICA ensures session reliability.	Session reliability is not ensured by RDP.
Low bandwidth is sufficient for ICA.	More bandwidth is required for RDP.
ICA uses port number 1494	RDP uses port number 3389

ICA Functionality:

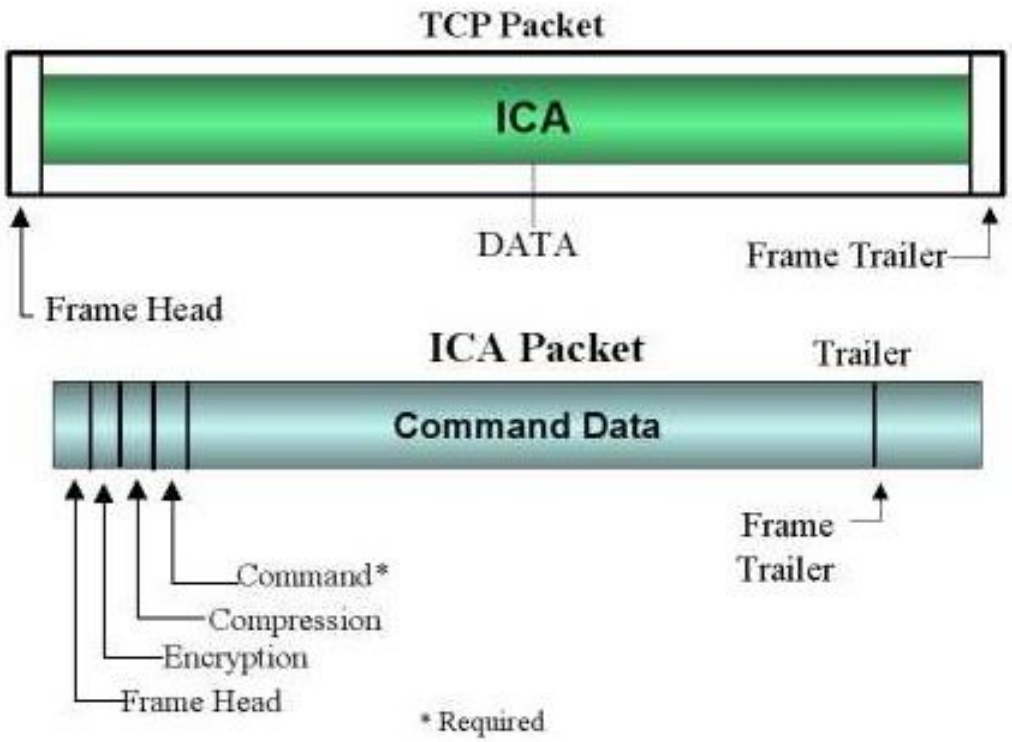
- ICA protocol operates at the Presentation layer of OSI Model, which prepares the received data to be presented in Application layer.
- Conceptually, ICA is similar to the UNIX X-Windows protocol.
- It also provides for the feedback of user input from the client to the server, and a variety of means for the server to send graphical output, as well as other media such as audio, from the running application to the client.



Citrix ICA protocol in osi model

- ICA traffic flows from the client device to the XenApp Server over TCP port 1494 or 2598 when Session Reliability is configured.
- Each ICA session then creates and uses a dynamically allocated TCP port for communications from the server to the client device.
- Within the ICA protocol, virtual channels are used to designate the various functionalities, such as client drive mappings, video, keyboard strokes, etc.
- Layer 3 (IP) and Layer 4 (TCP) functionality of the ICA protocol can easily be viewed by using Microsoft Network Monitor or other network analysis tools such as Wireshark.

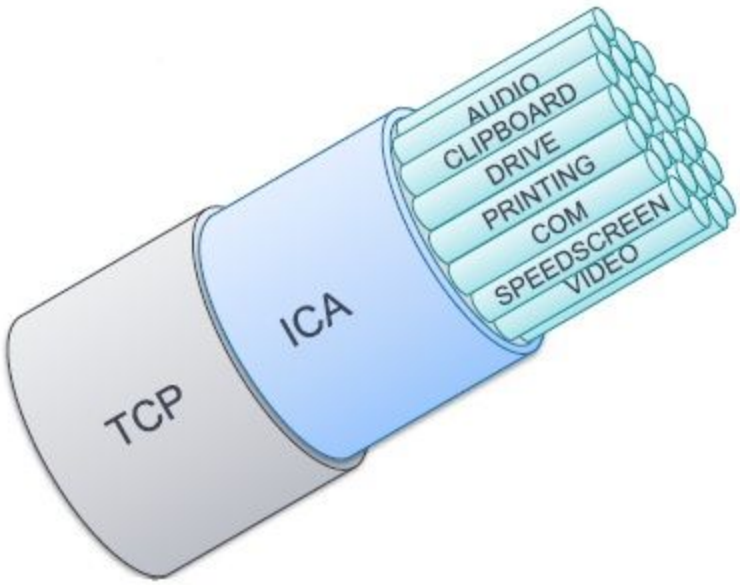
ICA Frame Format:



ICA Frame Format

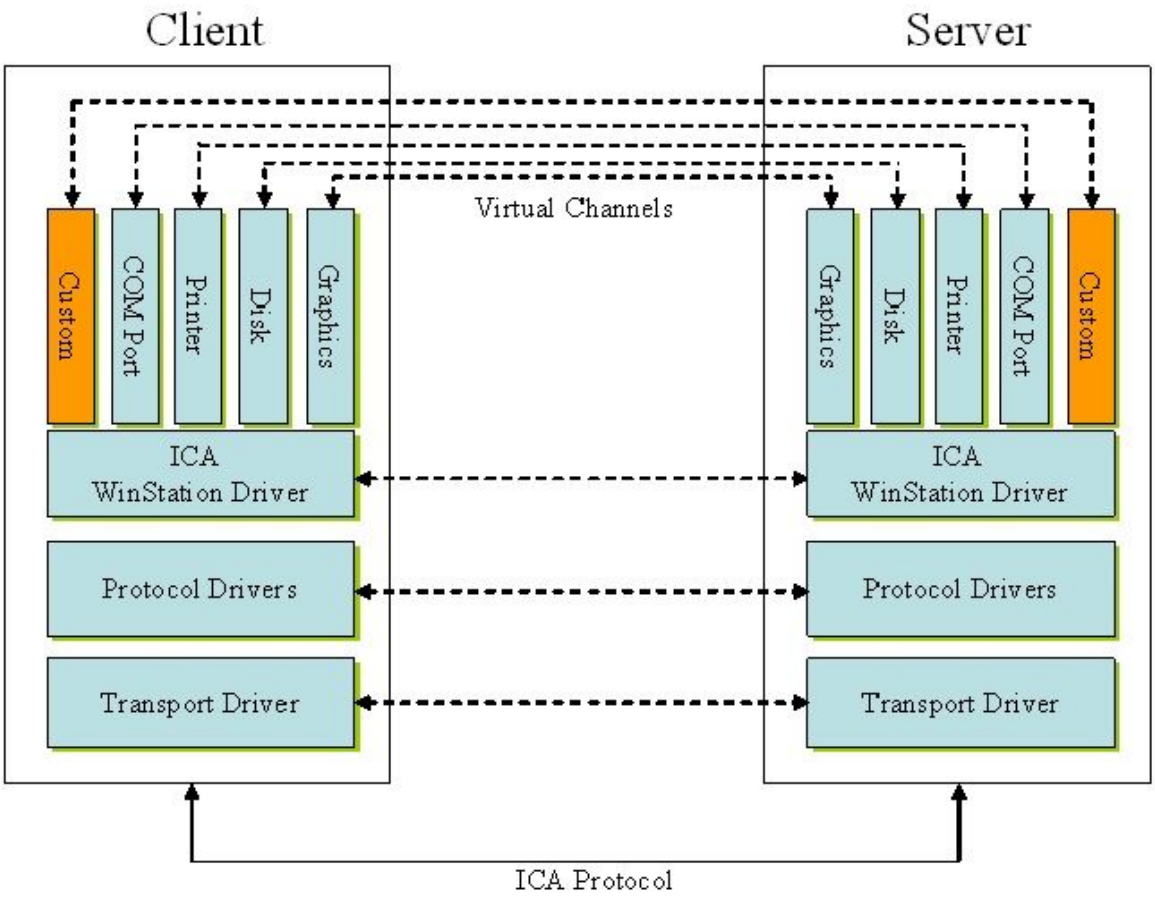
- Frame Head – Stream Oriented Transport data
- Reliable – Detection of errors and recovery
- Encryption – Managed data within encryption
- Compression – indicator of compression
- Command (required) – Starting point of the ICA protocol
- Command Data – Data bytes
- Frame Trailer – Asynchronous Transport Protocol Data

ICA Virtual Channels:



ICA Virtual Channels

- Within the ICA stream exist virtual channels, these virtual channels are for functions such as printing, audio, keyboard, mouse, video, drive mapping etc. on between the client and the XenApp server.
- There is a maximum of 32 channels that are available on each ICA stream.
- Each of the virtual channels above for both client and server would communicate with each other over the correct virtual channel. For example, the client Graphics channel would communicate with the Graphics channel of the server within the ICA stream.



ICA Protocol

- Virtual channels sit on top of the ICA Winstation Driver, on top of Protocol driver, on Transport Driver.
- Virtual drivers operate at the Presentation layer of OSI model.
- There can be a number of these protocols active at any given time by multiplexing channels that are provided by the WinStation protocol layer.

overview of client-server data exchange using a virtual channel:

1. The client connects to the XenApp Server. The client passes information about the virtual channels it supports to the server.
2. The server-side application starts, obtains a handle to the virtual channel, and optionally queries for additional information about the channel.
3. The client virtual driver and server-side application pass data using the following two methods:

1. If the server application has data to send to the client, the data is sent to the client immediately. When the data is received by the client, the WinStation driver de-multiplexes the virtual channel data from the ICA stream and immediately passes it to the client virtual driver.
2. If the client virtual driver has data to send to the server, the data is sent the next time the WinStation driver polls it. When the data is received by the server, it is queued until the virtual channel application reads it. There is no way to alert the server virtual channel application that data was received.

4. When the server virtual channel application is completed, it closes the virtual channel and frees any allocated resources.

Multi-Stream and Multi-Port ICA

Multi-Stream and Multi-Port ICA allow assigning a separate TCP Port for each of the four groups of ICA Channels. These TCP ports can then be assigned unique priorities on Network Devices.

To decide if it is required and to decide how to implement Multi-Stream and Multi-Port ICA in an environment, it is necessary to understand what the ICA Channels are, and how they are divided into the four priority groups.

Default ICA Virtual Channel Groups and Priorities:

The table in this article lists the default priorities for each ICA Virtual Channel in XenApp 6.5. The table includes both Single Stream ICA, and Multi-Stream ICA (with Multi-Stream Policy enabled).

Note: These priorities apply to XenApp 6.5

The following are the numerical priorities in the XenApp 6.5 ICA/GPO:

- Very High = 0
- High = 1
- Medium = 2
- Low = 3

Assuming that Branch Repeater is not in use in the environment, to implement Multi-Stream and Multi-Port ICA, complete the following tasks:

1. Enable Session Reliability, and CGP
2. Enable and configure the Multi-Stream and Multi-Port ICA/GPO Policies.
3. Configure Network Devices to assign QoS as desired to each configured port.

Channel Name	**Description**	**Single Stream (XenApp 6.5)**	**Multi-stream (XenApp 6.5)**
CTXCAM	Client audio mapping	0	0

CTXTWI	Seamless Windows screen update data (ThinWire)	0	1
CTXCTL	Citrix Control Virtual Channel	0*	1
CTXEUEM	End User Experience Monitoring	0*	1
CTXFLASH	Citrix Flash Redirection	0*	2
CTXGUSB	USB Redirection	0*	2
CTXSBR	No longer used. Previously: Citrix Browser Acceleration	0*	1

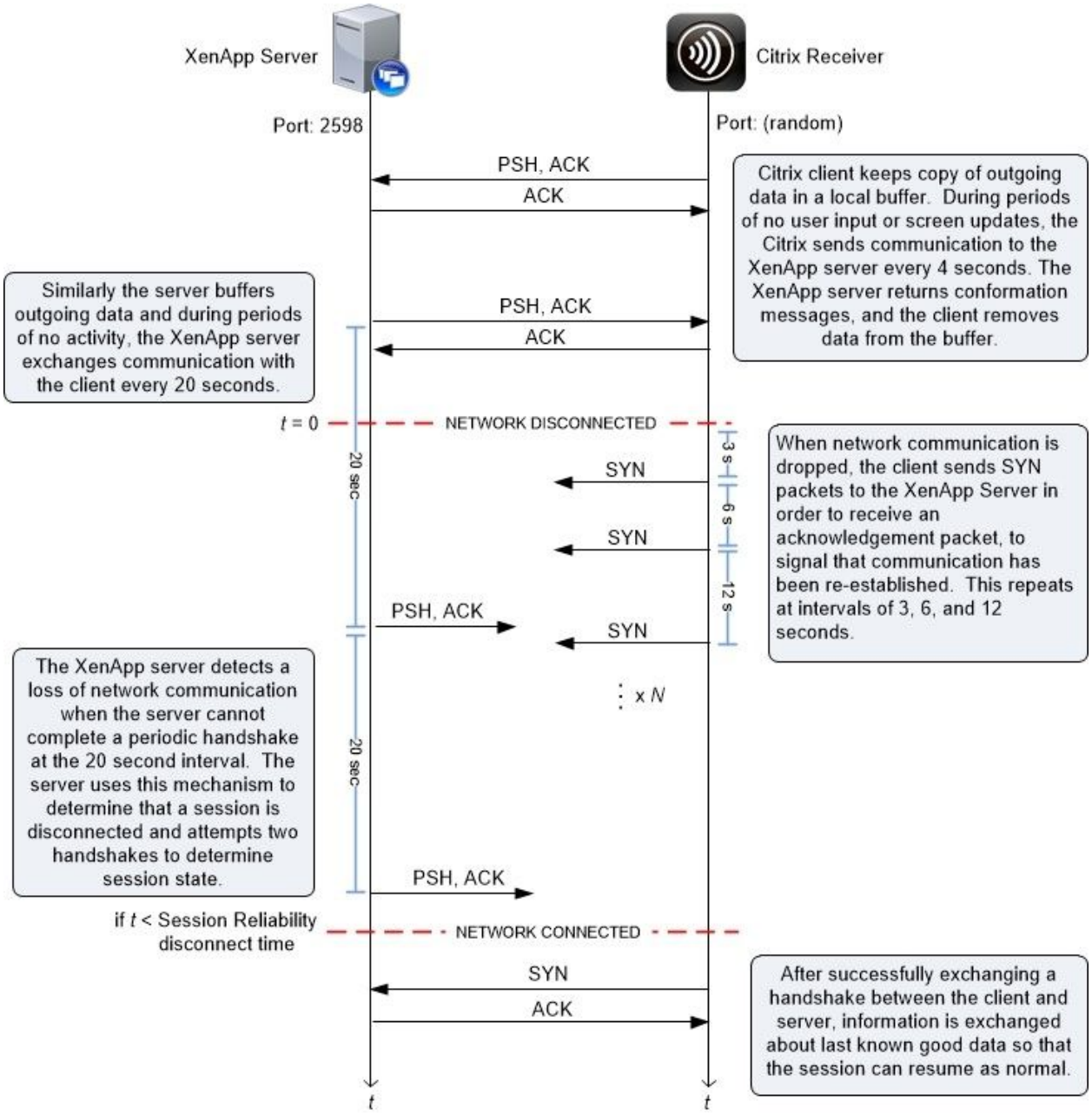
CTXSCRD	Smartcard	0*	1
CTXCLIP	Clipboard	1	2
CTXLIC	License management	1	1
CTXPN	Program Neighborhood	1	1
CTXTW	Remote Windows screen update data (ThinWire)	1	1
CTXVFM	Video server video (not ThinWire video)	1	1
CTXCCM	Client COM port mapping	2	3

CTXCDM	Client drive mapping	2	2
CTXMM	Citrix Windows Multimedia Redirection	2	2
CTXCM	Client management (Auto Client Update)	3	3
CTXCOM1	Printer mapping for non-spooling client (Thin client devices)	3	3
CTXCOM2	Printer mapping for non-spooling client (Thin client devices)	3	3

CTXCPM	Printer mapping for spooling clients	3	3
CTXLPT1	Printer mapping for non-spooling client (Thin client devices)	3	3
CTXLPT2	Printer mapping for non-spooling client (Thin client devices)	3	3
OEMOEM	Used by Original Equipment Manufacturers (OEMs)	3	3
OEMOEM2	Used by Original Equipment Manufacturers (OEMs)	3	3

Session Reliability:

- Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted.
- Users continue to see the application they are using until network connectivity resumes.
- This feature is especially useful for mobile users with wireless connections. Take, for example, a user with a wireless connection who enters a railroad tunnel and momentarily loses connectivity.
- Ordinarily, the session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session.
- With Session Reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel.
- The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored.
- Session Reliability reconnects users without reauthentication prompts. If it is enabled Session Reliability encapsulates ICA traffic through TCP port 2598.
- Session Reliability relies on Common Gateway Protocol (CGP).



Graphical explanation of Session Reliability

ICA bandwidth requirements

- ICA protocol will work properly on any network connection that will have at least 14 kb/s.
- The ICA protocol is optimized for Wide Area Networks or WANs with high latency links.

- This shouldn't be a surprise as ICA was developed when in everyday use where data-link connections via modems.
- The available bandwidth had only 56 kbps and ICA protocol had to be optimized enough to allow work on such a connection.
- ICA protocol supports also Quality-Of-Service (QoS) and other bandwidth optimization features.
- Key challenges of such an architecture are network latency and performance—a graphically intensive application (as most are when presented using a GUI) being served over a slow or bandwidth-restricted network connection requires considerable compression and optimization to render the application usable by the client.
- The client machine may be a different platform, and may not have the same GUI routines available locally—in this case the server may need to send the actual bitmap data over the connection.
- Depending on the client's capabilities, servers may also off-load part of the graphical processing to the client, e.g. to render multimedia content. All that put some requirements on the bandwidth allocation for ICA protocol. It may depend also on:

  Use of video or audio applications

  Number of users

  User behavior

  Printing

  Other network traffic

  Aero redirection/desktop composition redirection

Number of factors that may affect bandwidth requirements is long. Don't be surprised then when some of the users will be able to connect to Citrix published desktop or VDI machine and work normally while others will send a mass of tickets to support team with complaints about performance. For the first group the bandwidth tens of Kbps will be enough while the second group may require few Mbps bandwidth to stream their graphics or video.
In case of insufficient bandwidth ICA session may be dropped or users may experience choppy typing or screen paints. A possible workaround/fix for that might be configuration of Session Reliability.