KRAMER

USER MANUAL

MODEL:

VIA IT Deployment Guide
for Firmware 2.0

P/N: 2900-300631 Rev 3

Contents

1 Introduction

The **VIA** products are powerful, multifunction collaboration tools for enhancing meeting productivity. **VIA** gateways combine wireless and wired network connectivity to accommodate multiple users running Windows, iOS™, Mac™, and Android™ platforms. Unique to **VIA** is a proprietary video streaming protocol for all users that ensures steady 60fps playback from PCs, laptops, and tablets.

As with any network-connected PC, you must configure **VIA** gateways to your particular IT requirements; specifically, network addresses, port addressing, firewalls, wired and wireless networks, and trusted/permitted users. To ensure you get the most out of your **VIA** gateway, we've prepared this deployment guide to assists you in connecting **VIA** gateway to the wired and wireless networks of your institution.

To help you estimate bandwidth requirements, we've included graphs in this guide that show typical bandwidth usage and demand for a variety of **VIA** gateway applications, including PowerPoint™ presentations, Web browsing, YouTube™ and other video streaming, file sharing, and collaboration/whiteboard operations. These graphs measure actual bandwidth used at the network switch for single and multiple users.

The **VIA** family consists of three products: **VIA Collage**, **VIA Campus** and **VIA Connect PRO**. The backend operating system of each of these devices differs and therefore integration into your network may be slightly different at times. Throughout this guide we point out any differences that you need to know.

VIA Collage – Windows 7
VIA Campus – Windows 10
VIA Connect PRO - Linux

1.1 User Experience

VIA gateways work with different PC and BYOD operating systems in two ways:

- For desktop and laptop computers, executable files must be loaded and run. These files are stored on the **VIA** gateway and are accessible to anyone who browses the home page of the **VIA** gateway. Windows and Mac OS are both supported.
- For tablets and smartphones, an app must first be downloaded. The app for iOS devices is available in the iTunes Store, while the app for Android devices can be found in Google Play. iOS mirroring is also available for Apple devices.

Once the executable file or app is downloaded and launched, each user is prompted for a user name and room code to access the **VIA** gateway. No further setup is required.

1.2 Pre-Deployment Planning

Prior to deploying **VIA** gateways, it is important to consider how the device integrates with your existing IT infrastructure. Depending on the complexity of your network and the level of integration you desire, there are several items to consider. This document provides you with the data you need so that you can deploy the **VIA** gateway in a way that best suits your existing IT environment.

1.3 Connectivity

This section describes all relevant network issues.

1.3.1 Network Addressing

An IP address is the logical address that identifies a device on a network. To connect and communicate properly with other devices on the network, the **VIA** gateway needs a properly configured IP address. Obtain this address information from the network administrator responsible for the network.

A subnet mask is a number that is used in combination with the IP address to define what network addresses are on the local network segment. If a network address is local, the **VIA** gateway can communicate with it directly. If a network address is not local, traffic from the **VIA** gateway is sent to the default gateway address.

The default gateway address is the network address of a device that is responsible for forwarding network traffic to other network segments. This may be a firewall, router, or Layer 3 network switch.

Domain Name System (DNS) servers translate names like www.KramerElectronics.com into IP addresses. For example, as of this writing, the DNS name www.KramerElectronics.com translates to IP address: 23.62.6.162.

To use a DNS name rather than an IP address for your room name, your network administrator must create one for your **VIA** gateway. For example, if you use an internal default domain name for all of your connected clients (such as domain.lan), you could configure a DNS map for Room1.domain.lan that points to the static IP address assigned to the **VIA** gateway.

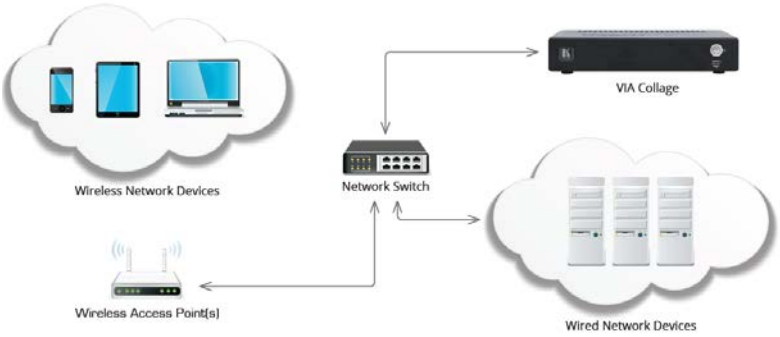
As long as connected clients are (1) able to resolve that DNS name by using the DNS map your network administrator configured and (2) the clients have the default domain name of domain.lan assigned to them, they can use the DNS name “Room1” to connect, rather than the static IP address assigned to the **VIA** Gateway.

1.3.2 Network Segmentation Requirements

A network segment is a logically-separated group of network devices with each group configured as sub-networks or subnets. For devices on one subnet to communicate with devices on another subnet, access control lists or firewall rules may need configuration.

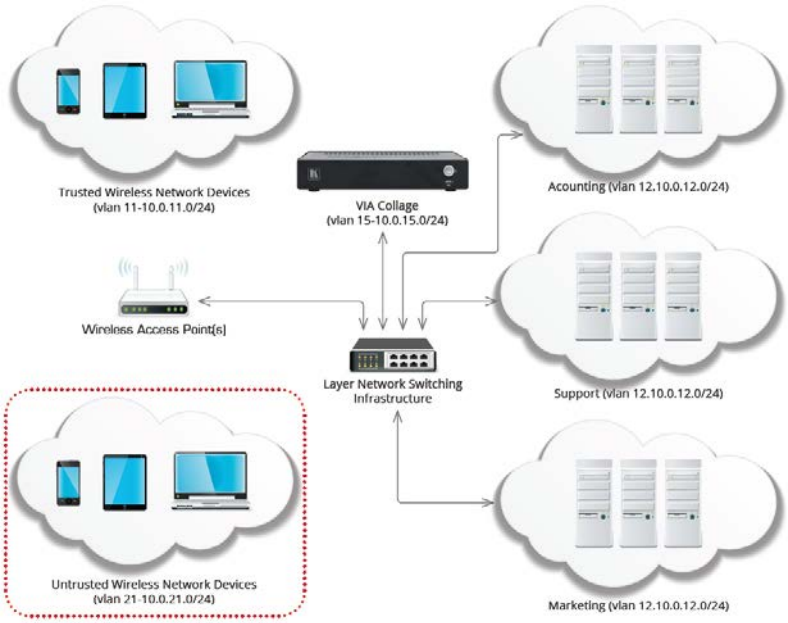
1.3.3 Flat (Non-Segmented) Networks

Smaller networks may not have network segmentation. In that case, connect the **VIA** gateway to your network and your other IP-connected devices on that network – wired or wireless – to see and interact with it, with little or no network configuration required.



1.3.4 Segmented Networks

Larger networks are usually segmented. For example, your network might have trusted network segments where devices owned and controlled by your organization are connected. However, you might also have an untrusted wireless network to which guests are allowed to connect their devices. Even basic segmentation of your network requires some planning to determine what network segment is best to connect to the **VIA** gateway. Connecting the **VIA** gateway to its own network segment may offer you the best ability to granularly control access to and from the **VIA** gateway from other segments on your network.



Note: VLANs and IP addresses listed in the above graphic are only examples.

You can connect the **VIA** gateway to any segment of your network as long as traffic to and from the **VIA** gateway can reach connected clients, along with any other resources that you want **VIA** gateway to access.

VIA gateway supports different VLANs and/or different IP subnets. However, all network segments must be connected to **VIA** routed subnets and may not have any devices translating network addresses (NAT) between the **VIA** gateway and connected clients. Clients connected to a network segment that makes use of network address translation between the client and the **VIA** gateway do not work properly and are unsupported.

For additional information regarding deploying **VIA** Gateways across multiple networks, see the supplemental guide that addresses dual network integration.

1.3.5 Wireless Networks

The **VIA** gateway fully supports clients that are connected by either wired or wireless networks. When dealing with clients connected by a wireless network, it is particularly important to make sure that these wireless clients have sufficient bandwidth through all wireless access points into the **VIA** gateway.

In deployments where the **VIA** gateway is used by a small number of connected clients, a single high-quality, commercial-grade wireless access point that supports the 802.11N or 802.11AC wireless standards is sufficient. In deployments where more than ten users are connecting to the **VIA** gateway wirelessly, check with wireless network administrators to ensure sufficient bandwidth is available.

1.3.6 Wireless USB Dongle Integration

The **VIA Connect PRO** gateway is capable of acting as an AccessPoint or Client within a wireless environment. A generic USB WiFi dongle is required to take advantage of these features. The USB WiFi adapter must first be connected to the **VIA Connect PRO** and then booted up. Once the **VIA Connect PRO** gateway is booted it can be configured as an AccessPoint to create its own WPA2 personal secured wireless network with open or closed internet ports. Alternatively, it can be configured as a Client device allowing it to join an existing WPA2 personal secured wireless network.

The maximum bandwidth available in either of these modes is 54MBps. To run the system at its best performance level, be sure to calculate the maximum number of users that connect simultaneously.

1.3.7 Wireless Bandwidth Scalability

When a **VIA** gateway is used by a large number of meeting participants, it is important that the network connecting the **VIA** gateway and participants has sufficient bandwidth.

One common problem is overloading wireless access points. For example, if a **VIA** gateway is used for a collaborative session where the stepped-in presenter is doing Web browsing while 50 connected clients use the “view main display” function (available only on **Collage** and **Campus**), the wireless network must support all 51 of the sessions (1 presenter + 50 clients). It must allow for approximately 5 Mbps of bandwidth between the **VIA** gateway and each connected client. In this scenario, up to 255 Mbps of bandwidth is used between the **VIA** and connected clients simultaneously.

In this case, you can use multiple commercial-grade wireless access points to spread the wireless bandwidth load over multiple access points. Check with your network administrators to be sure that sufficient wireless bandwidth is available for connecting **VIA** gateway.

1.3.8 TCP/IP Port Requirements

TCP/IP ports are numbers that are assigned to user sessions and server applications in a TCP/ IP network. The **VIA** gateway must be able to communicate with connected clients using TCP/IP traffic on the ports listed in the table below. If you have one or more network segmentation device(s) between the **VIA** gateway and connected clients, the following traffic must be considered for the **VIA** gateway to function properly.

Since network traffic can be blocked at multiple levels by (a) software firewalls running on client devices or (b) hardware devices that are part of the underlying network infrastructure, make sure that all firewalls or network segmentation devices between connected clients and the **VIA** gateway allow traffic on the following ports:

Traffic Client to VIA	Type	Function
5222	TCP	Communication data TLS/SSL
7001 - 7024	TCP	Audio
7777	TCP	File sharing
5555	TCP	File sharing
9955	TCP	Streaming video
9954	TCP	Streaming video
9985	TCP	Authentication

Traffic Client to VIA	Type	Function
9982	TCP	API commands
9986	TCP/TLS	API commands - TLS
9994	TCP	Android mirroring /Step-in
9987	TCP	Display mobile device
9989	TCP	Collaboration
9990	TCP	Step-in
9993	TCP	Step-in
80 / 8080	TCP	HTTP
443	TCP	HTTPS
9992	TCP	View main display
22	TCP	SSH
9984	TCP	Replaced with 9985 SSL-based
https://cb.wowvision.com:444	TCP	ChromeBook support
iOS to VIA	**Type**	**Function**
7000	TCP	Server port authentication
7100 – 7300*	TCP	Data
29053	TCP	Event port
2001 - 2201*	UDP	Timing
61875-62000	UDP	Audio data

* If the port is busy or not available, it jumps to next available port and tries to bind (maximum range, 200 ports).

VIA to iOS	Type	Function
5353	mDNS/UDP	mDNS Bonjour / Airplay broadcast
VIA to Client	**Type**	**Function**
9954	TCP	Streaming from OSX to a **VIA** static port at the client
3500-3599	TCP	Range of ports to send data from client
80	TCP	Android/ iOS app streaming
8080	TCP	Android/ iOS app streaming
12345	TCP	Streaming sync & ACK iOS only
https://cb.wowvision.com:444	TCP	ChromeBook support
VIA to Windows Server	**Type**	**Function**
389	TCP/UDP	AD/LDAP
53	TCP/UDP	DNS

VSM to VIA	Type	Function
9988	TCP	API server used by **VIA** to VSM
5555	TCP	File server for updating firmware and wallpaper, etc.
80 / 8080	TCP	Web server HTTP
443	TCP	Web server (for future use with https)
PC to Mobile Devices	**Type**	**Function**
12345	TCP	Web browser data transfer
20000	TCP r	FTP data transfer

1.3.9 Ports to "Enable Internet" in Access Point Mode (Connect Pro)

Port	Type	Function
80	TCP	HTTP
443	TCP	HTTPS
25	TCP	SMTP
465	TCP	SMTP over SSL
587	TCP	SMTP message submission
53	TCP	DNS
53	UDP	DNS

1.3.10 Network Integration

VIA Collage & **VIA Campus** platforms run the Windows operating system on top of proprietary hardware, which means these **VIA** gateways can be easily integrated into your existing IT environment. Many of the technologies you already use to manage and protect your network can be leveraged to help you efficiently manage these **VIA** gateways.

1.3.11 Microsoft Active Directory

Microsoft Active Directory can be leveraged to populate the moderator and user databases when the **VIA** gateway is used in moderator mode. This mode establishes a moderator and user environment to ensure that meeting control is always maintained. Supplemental application note is available to aid in the integration of Active Directory.

1.3.12 Anti-Virus Software (Applies to VIA Collage & VIA Campus only)

Many organizations run organization-wide managed security software. Since the **VIA Collage** and **VIA Campus** run Windows, you can deploy your normal managed security software to **VIA** gateway. If your security software includes a software firewall, it is important for you to review the port requirements listed above and create any necessary exceptions.

It is important that antivirus software not use more than 5% of the **VIA** gateway CPU, to make sure that it performs properly. When running periodic, scheduled scans of **VIA** gateway, we suggest you schedule those scans to run during “off” hours when **VIA** gateway is not in use.

1.3.13 Patch Management (VIA Collage & VIA Campus only)

Patch management systems are often used by larger organizations to centrally manage the process of applying software patches to computers. These systems allow administrators to apply patches to groups of computers without dealing with each computer on an individual basis. These systems also have reporting functions that allow administrators to determine which machines on their network are missing important patches.

The **VIA** gateway does not require connection to a third party patch management system; however if your network already uses one, it can work with **VIA** gateway. The **VIA Collage** & **VIA Campus** ship with Windows update turned off by default, so that an update does not happen while a presentation is in progress. However, where **VIA Collage** or **VIA Campus** are not connected to a network-wide patch management system, enable Windows update and schedule it to run at a time when no one is using the **VIA** gateway.

1.3.14 Network Security - Surface Area

From a network security perspective, client computers (devices that access network services) and servers (devices that provide network services) are often treated differently. Servers, by design, run services that connect to other clients. Therefore, those services cannot be blocked at a network level if the server is to

perform its function. This makes keeping security patches updated on server devices all the more important.

VIA gateways run application server software that connects clients. From time to time, Kramer may release updates for **VIA** gateway application software to deal with underlying application level security issues with the **VIA** software itself.

1.3.15 Bandwidth Requirements

For a device to operate properly on a network, it must have sufficient bandwidth to communicate with the other devices on the network. The amount of bandwidth required depends heavily on how the device is used.

To help you properly plan your **VIA** gateway deployment, we have tested the **VIA** gateway in a variety of different scenarios and collected real-world bandwidth use data. After carefully reviewing this data, we have outlined some general bandwidth recommendations that help you properly size the bandwidth needs for your particular **VIA** deployment. These recommendations are suggested minimums for the amount of bandwidth needed between a connected client and the **VIA** gateway. These recommendations are given on a per-client basis:

- PowerPoint presentation display, document review, etc. – 1 Mbps per client
- Web browsing – 5 Mbps per client
- Video/multimedia streaming – 25 Mbps per client

Clients connected to the **VIA** gateway that are not actively stepped in, using the “view main display” function, or actively sharing files use a minimal amount of bandwidth.

All network traffic to and from the **VIA** gateway, including video streaming, is unicast traffic. The bandwidth requirements of the **VIA** gateway scale linearly based on the number of users stepped in or using the “view main display” function of the **VIA** client app. Therefore, two clients stepped in at the same time would require roughly double the bandwidth as one stepped-in client requires.

1.3.16 Third-Party Applications (Via Collage & Via Campus Only)

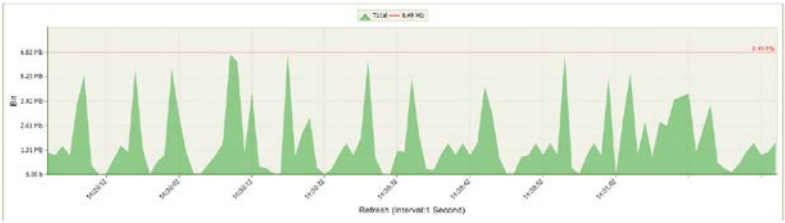
The **VIA Collage** and **VIA Campus** support third-party applications like Skype and WebEx. Review the specific requirements for these applications if you plan to use them with your **VIA** gateway.

- Skype
  https://support.skype.com/en/faq/FA1417/how-much-bandwidth-does-skype-need
- WebEx
  http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17161.htm

2 Bandwidth Measurement Data: Single Presenter

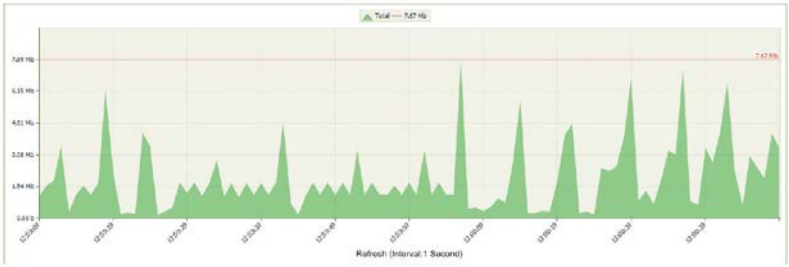
In addition to these summary suggestions, we provide you with the following detailed bandwidth graphs that show real-world **VIA** gateway bandwidth use in a variety of scenarios. Traffic was measured at the network switch port. For the purposes of these graphs, “traffic out” is defined as traffic being sent from the switch to **VIA**, and “traffic in” is defined as traffic sent from **VIA** to the network switch.

2.1 Typical PowerPoint Presentation



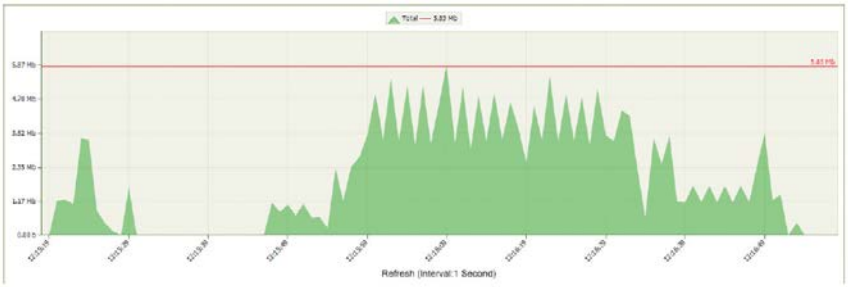
Slides with text and a few graphics are displayed on the **VIA** main display by a single connected client. Slides were advanced in irregular times to simulate real workflow.

2.2 Graphic Intensive PowerPoint Presentation



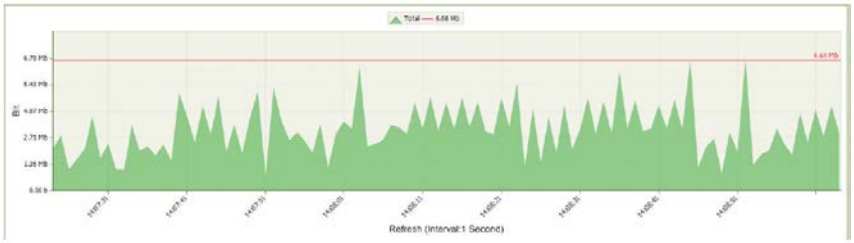
Slides consisting of heavy graphics and small animations are displayed on the **VIA** main display by a single connected client. Slides were advanced in irregular times to simulate real workflow.

2.3 YouTube Video



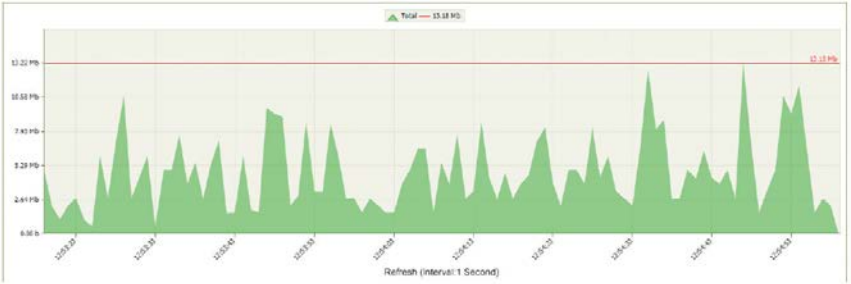
YouTube 720p video is displayed full screen on the **VIA** main display by a connected client.

2.4 Web Browsing



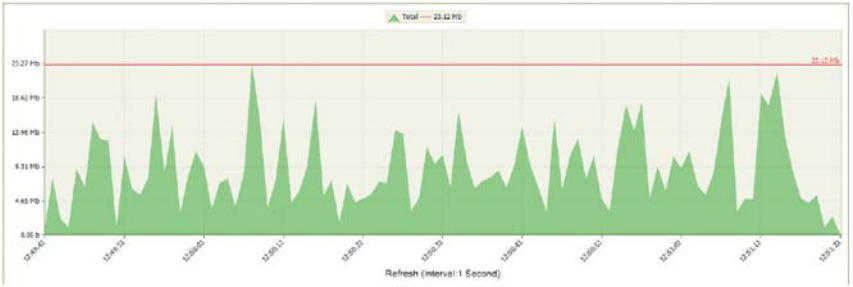
Random web browsing is displayed on the **VIA** main display by a connected client. Bandwidth spikes are generally attributable to animations or embedded video on the visited sites.

2.5 720p Multimedia Streaming



720p video is streamed and displayed on the **VIA** main display by a connected client.

2.6 1080p Multimedia Streaming



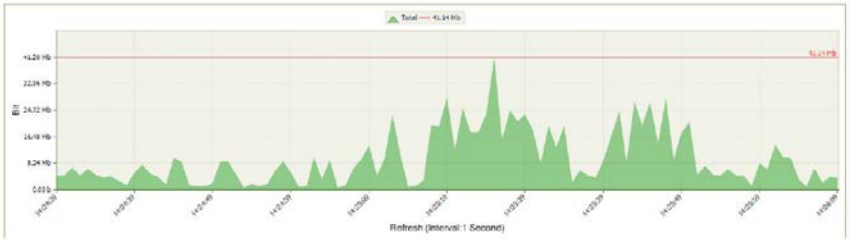
1080p video is streamed and displayed on the **VIA** main display by a connected client.

3 Bandwidth Measurement Data

Multiple presenters / Multiple Participants

3.1 Graphic Intensive PowerPoint Presentation

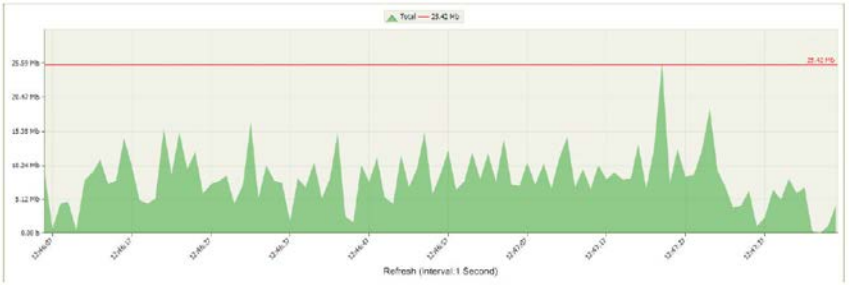
One Presenter / Three Participants Using “View Main Display”



Slides consisting of heavy graphics are displayed on the **VIA** main display by a single connected client and are viewed by three participants using the “View Main Display” function simultaneously.

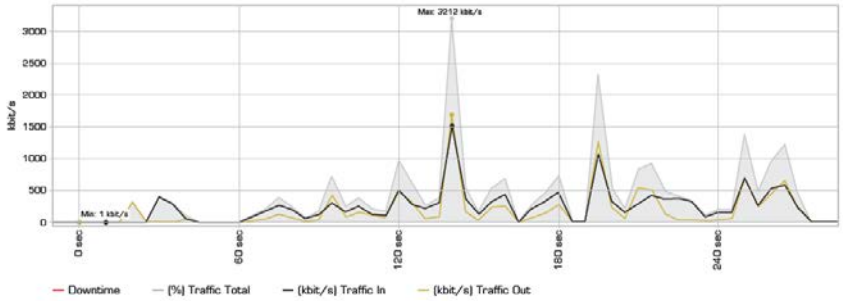
3.2 YouTube 720p Video

One Presenter / Three Participants Using “View Main Display”



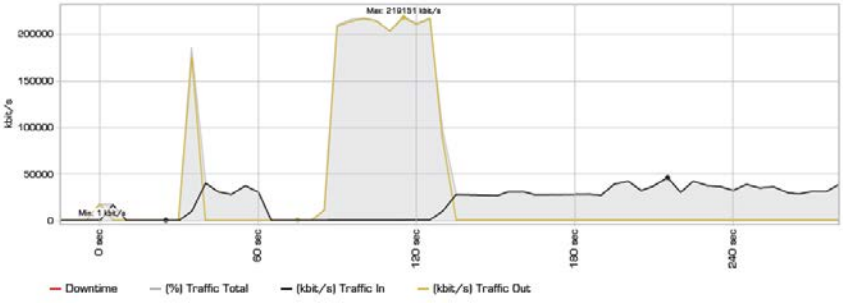
YouTube 720p video is displayed full screen on the **VIA** main display by a connected client and are viewed by three connected participants using the “View Main Display” function simultaneously.

3.3 Bandwidth Patterns – Collaboration / Whiteboard / Enable Control

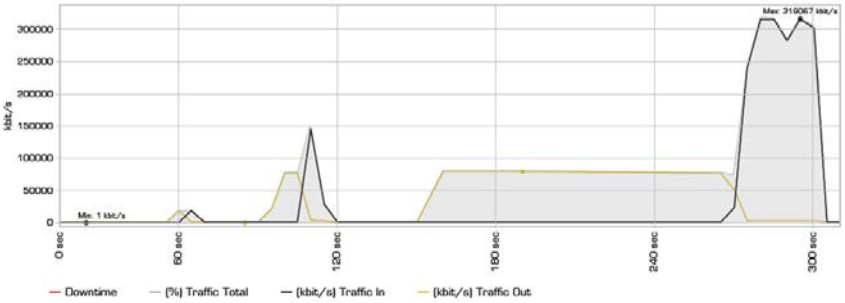


The **VIA** gateway allows multiple participants to whiteboard and share control of a stepped-in member's device. The bandwidth graph below shows a session where one user was stepped-in and allowed the other users to remotely control his machine and whiteboard collaboratively.

3.4 Bandwidth Patterns – During File Sharing Sessions



VIA gateway can be used to easily transfer files between participants. From a network perspective, the speed of the transfers is limited by the amount of available bandwidth between **VIA** gateway and connected client devices.



The graph below shows a series of files (10MB, then 100MB, then 1,024MB) uploaded by a computer with a gigabit Ethernet connection and then downloaded by a computer with a 100 Mbps connection.

The graph below shows the same series of files (10MB, then 100MB, then 1,024MB) uploaded by a computer with a 100 Mbps network connection and downloaded by a computer with a gigabit Ethernet connection.

As seen in these graphs, the available bandwidth between the **VIA** gateway and the devices is the major constraint on the speed of the file transfers. The **VIA** gateway platform does not affect bandwidth until data speeds of 200 Mbps are reached. This constraint only becomes an issue during the transfer of very large files or during the transfer of files to a very large number of participants.

4 Conclusion

We hope this deployment guide has been helpful in installing and configuring your **VIA** gateway. Once installed, your **VIA** gateway operates like any other computing platform on your network. If you have further questions or require assistance with network configuration, contact your local Kramer sales support engineer or Kramer technical support.