Vector

White Paper / TechNote

Secure Remote Control for conventional and virtual desktops

Key architecture and feature characteristics of Series 12 PC-Duo.

Background

Many organizations have a mix of conventional desktops, sessions virtualized with Citrix / Terminal Services, and fully virtualized desktops such as VMware.

A single remote control platform for user support is going to be key to providing an efficient helpdesk.

Users are spread across multiple LANs and mobile users connected over the internet.

High levels of security are mandated at all levels of IT. User support, with the ability to take control of a user's PC and view the screen, is a particularly demanding situation.

Protection of user privacy must be balanced by the need for privileged access, in accordance with compliance frameworks and legislation.

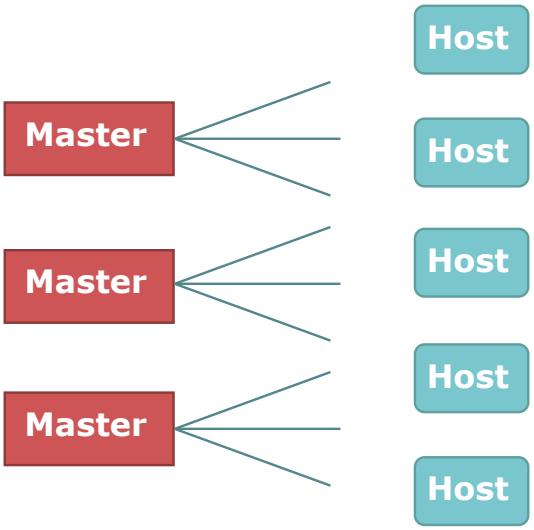
Contents

Foreword: Data Ownership

These notes detail some aspects of PC-Duo functionality but the topics should help provide a basic set of headings under which to evaluate any potential remote control choice.

There is however one fundamental characteristic to consider first: data ownership. PC-Duo belongs to a class of remote control product in which the customer retains full control over the way in which screen and keystroke data is transmitted. This is fundamentally differentiated from products and services in which your data is routed through third party servers. Depending on the strength of your security requirements, this area of choice could be more important than any other.

Host, Master and Gateway components with conventional desktops.



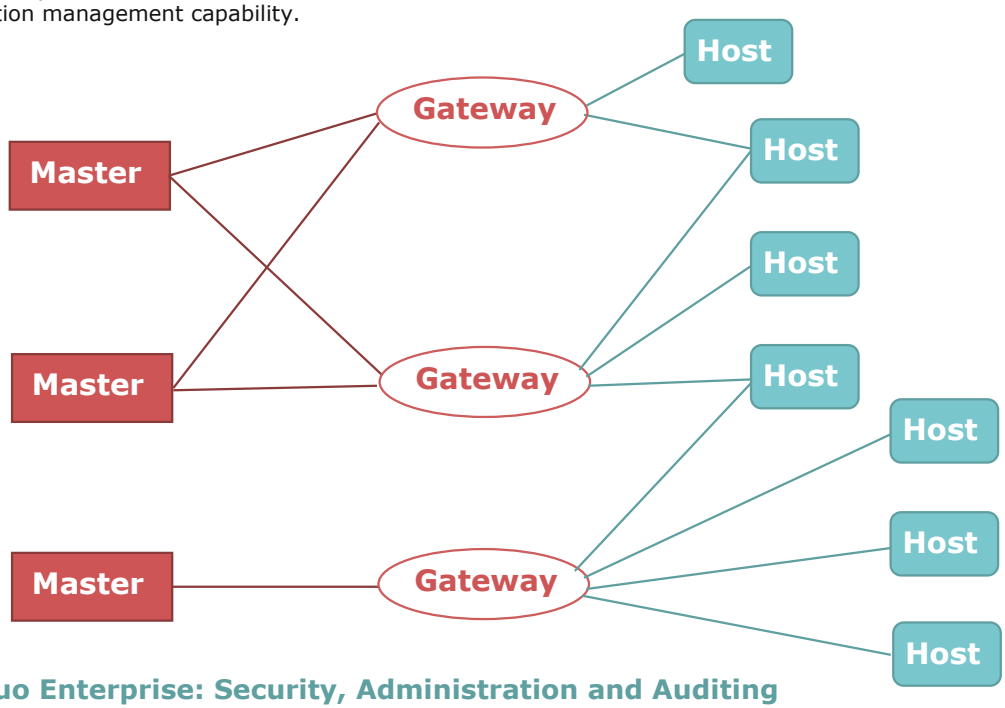
PC-Duo Express

- PC-Duo Express is the lowest cost option and is ideal for low numbers of PCs (typically less than 100, but with no fixed limits).
- A PC-Duo Express installation consists purely of PC-Duo Masters and Hosts.
- PC-Duo Express supports 1-to-1 connections. For Many-to-one connections, the PC-Duo Enterrpirse Gateway provides management of the multiple sessions to the Host.
- Where a number of Host systems are located behind firewalls, the Enterprise Gateway can be used with sufficient capacity in terms of numbers of registerred Hosts to provide the navigation through the firewall, without incurring the cost of implementing a full PC-Duo Enterprise installation. Our pre-sales advisors will ensure you implement the most cost-effective configuration.

PC-Duo Enterprise

The PC-Duo Enterprise Gateway functions as a virtual router for remote control connections, and can be installed at any location where you need to connect to Hosts that are behind a firewall.

For organizations with several populations of remote PCs that are only accessible over the internet, the Gateway therefore today provides a powerful combination of distributed session and connection management capability.



PC-Duo Enterprise: Security, Administration and Auditing

In addition to its role in providing secure firewall friendly connectivity, featuring SSL and AES encryption, the PC-Duo Enterprise Gateway also provides centralized connection, security and session recording management for the Hosts it serves.The Gateway supports the definition of Groups of supported Hosts, facilitating efficient configuration management.

Each Host can be registered with any number of Gateways, providing redundancy in the event of a Gateway hardware failure. Each Master can be defined as able to connect to specific Gateways, and hence to the Hosts registered with that Gateway.

In larger installations, Gateways are usually specified to have capacity to register all available Hosts, but direct Master-Host connection is still possible.

Vector

PC-Duo for Terminal Services: How it Works

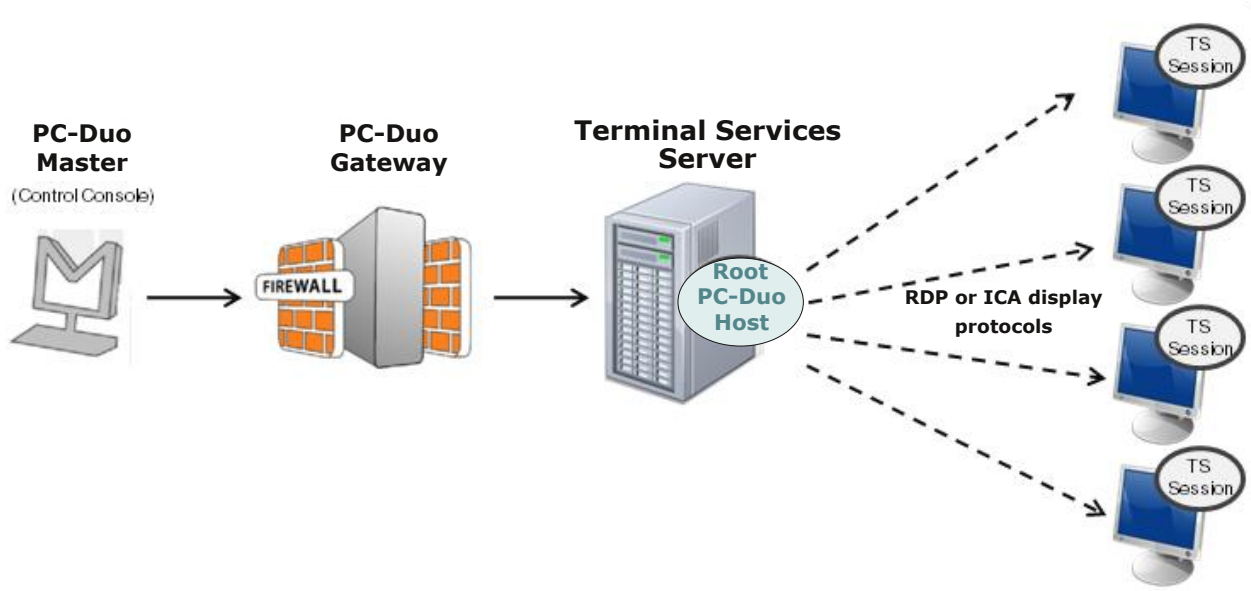
The Terminal Services Host

PC-Duo provides server-side support (screen capture, input control, screen recording) for session-based virtual desktops hosted by Terminal Services on Windows Server 2003, Window Server 2008 and 2012 (now called "Remote Desktop Services").

Windows Server creates and hosts the Terminal Services (TS) sessions like virtual machines. A presentation technology using a display protocol such as RDP from Microsoft or ICA from Citrix is typically used to remote the session display, as well as the keyboard and mouse input, to and from an end user device (such as a thin client computer like a Wyse terminal).

PC-Duo allows administrators to capture (and optionally record) the session presentation information at the Windows Server before it is remoted to the end user device over the RDP or ICA display protocol.

PC-Duo does this by injecting a Host instance into each server-side TS session, which in turn captures and sends presentation information directly to PC-Duo Enterprise Gateway for recording and/or further transmission to a PC-Duo Master.



Because Terminal Services sessions are captured by the PC Duo Host at the Windows Server level (and not at the end user device), the PC Duo Host effectively bonds a new instance of itself to every TS session created by the Windows Server.

With this architecture, PC Duo Remote Control is compatible with Microsoft Terminal Services clients as well as Citrix Presentation Server (XenApp) clients.

Note: PC-Duo only supports TS sessions created on server-class Windows operating systems such as Windows Server 2003, Windows Server 2008 and 2012.

Managing Host Transience

Each TS instance of the Host will have its own unique workstationID and must be configured to report to a Gateway. When it first reports to the Gateway Server, it will be automatically managed and added to the "All Hosts" group. The TS Hosts are considered transient, since they go away when the TS user logs out of his/her session.

To keep track of transient TS Hosts, the PC-Duo Enterprise Gateway will create a new Group called "Terminal Services on <Servername>", and automatically insert transient Hosts into this Group. They are automatically deleted from the Gateway when the TS session ends. The main purpose of this Group is to allow security to be assigned to the Hosts and TS sessions that belong to this Group, and to provide the correct and appropriate access to the TS-based Host instances.

Note: PC-Duo Host for Terminal Services works on Server 2003, Server 2008 and 2012, and requires a Gateway Server v11.6 or later.

Limitations of Terminal Services Hosts

Due to technical limitations and the nature of Terminal Services sessions, the following Host features are NOT supported.

- Remote printing.
- Keyboard and mouse suppression (requires kernel-based input stack intercept).
- Screen blanking (requires kernel-based support and physical display to blink).
- Peer-to-peer connections: all protocols are disabled, and the only connections that can be made are through a configured Gateway Server.
- Kernel-mode screen capture (even on Windows Server 2003, requires kernel-mode display support).

PC-Duo for VMware images: How it Works

Setting up PC-Duo in the VMware Image

We saw how with Terminal Services a Host process is inserted into each desktop session as it is created on the server, and the Terminal Services Host registers with the PC-Duo Gateway with the session identify. In a VMware environment, the PC-Duo Host is pre-installed into the VMWare image, and in this process it will adopt the machine identity present at the time of installation.

However, the Host needs to be configured, after installation into the image, to behave differently. To achieve this, a program is run after installation and before the image is frozen. 'HostPrep.exe' stops the PC-Duo Host Service and deletes the existing Host GUID from the registry. When the image snapshot is taken in this state, this allows the resulting machines to generate unique GUIDs the moment their PC-Duo Host Service(s) start up for the first time.

Managing VDI Hosts in the PC-Duo Gateway and Web Console

Once an end-user logs into Windows to effectively launch their VDI machine (or simply when the PC-Duo Host Service starts, whichever comes first) you will notice that machine appearing in your PC-Duo Gateway Administrator and/or PC-Duo Web Console's "All Hosts" group as well as a group labeled "Transient VDI Hosts", a group that is automatically created the first time a VDI Host reports in.

Additionally, if you've created custom grouping rules within the Gateway Administrator or PC-Duo Web Console that apply to your VDI Hosts, they will also enter and leave those groups as well. The moment a VDI Host stops reporting into your Gateway, it will be removed from all groups. And due to the transient nature of VDI Hosts, PC-Duo lists only the active VDI Hosts at any given time.

Multiple LANs, Mobile Users, Firewalls: Topology Challenges

With more and more employees working from remote locations, whether it's on the go for business trips via a laptop, or employees that regularly work from home, it becomes increasingly difficult to connect securely with these remote computers when a remote session is needed. In an attempt to deliver an attractive, easy fix for this problem, many solutions require the remote computer to connect to a third party server. This may function well, but having another company handling all the details for the connection and the confidential traffic presents an unnecessary risk and may compromise compliance.

What if the support team could connect to the remote sites and computers just as easily, while not giving up control over the traffic of the organization's confidential data? The PC-Duo Gateway provides a fully secure, Windows-authenticated access point to reach any remote computer in the world, with all computer availability monitored in real time.

With the PC-Duo Gateway running on a server under the organization's control, administrators can configure any remote computer to stay in secure contact with that Gateway at all times, whether that remote computer is in an office down the hall on a different network, or is a roaming laptop in another country. The PC-Duo Gateway offers a list of available computers that are constantly updated, where the Gateway can display every available machine from around the world.

Through the pre-configuration of the PC-Duo Host onto any computer outside your network, administrators can instruct those remote computers to report on their availability through any network connection that could reach the Gateway. Even from behind a firewall, as long as the PC-Duo Host can reach the open Gateway port on the other side, it will negotiate a connection, and ensure that a remote connection can still be made. Remote users won't even need to click on a link.

Encryption

To ensure privacy of communications between PC-Duo applications across the network, PC-Duo provides advanced encryption using Advanced Encryption Standard (AES) block ciphers and Secure Hashing Algorithm (SHA-1). This protection will be automatic and transparent every time two PC-Duo v12.1 components or later are communicating with each other.

By default, PC-Duo uses AES 256-bit encryption, however other encryption options can be set, including:

- AES encryption (256-bit key) with SHA1 hash
- AES encryption (192-bit key) with SHA1 hash
- AES encryption (128-bit key) with SHA1 hash
- Triple-DES (3DES) encryption (192-bit key) with SHA1 hash
- RC4-compatible encryption (128-bit key) with MD5 hash

NOTE: PC-Duo 11.2 applications and older support only RC4 encryption; thus, this would be the encrpytion option negotiated between a PC-Duo 11.2 or later application (e.g. PC-Duo Master) and PC-Duo 11.2 application (e.g. PC-Duo Host).

Order of precedence

When two PC-Duo components have different encryption options set, the first encryption choice in common between the two is used (going down the list in order), with preference set as follows:

- Preference set by the Host, when the Gateway requests connection to the Host
- Preference set by the Gateway, when the Master requests connection to a Host through the Gateway

Authentication

In the PC-Duo model, PC-Duo applications that request information and services are considered "clients" and those that provide information and services are considered "servers". For example, the PC-Duo Master is considered a client when it connects to and requests a list of Hosts from a PC-Duo Gateway. In turn, the PC-Duo Gateway is considered a client when it connects to and requests information from a PC-Duo Host in the same domain.

When PC-Duo Host is not in the same domain as the Gateway, the relationship is automatically reversed: The Host is programmed to be the client and will reach out to the Gateway (see "Firewall-friendly connections" for more information about PC-Duo firewall-friendly connections).

To guarantee security in the PC-Duo environment, it is critical that PC-Duo components acting as servers validate the credentials of users of PC-Duo components acting as clients before they provide access or data. The burden is placed on the client to authenticate itself to the server.

PC-Duo implements two types of authentication to support this:

- **Identity Authentication**
- **Endpoint Authentication**

Identity Authentication

In general, this operation answers the following security question: How does the server know who the client is? A PC-Duo application acting as a server will not provide access or information to any PC-Duo application acting as a client until it can validate that client"s identity. PC-Duo provides the server three different methods of authenticating the identity of the PC-Duo client:

Windows Authentication

By default, a PC-Duo application acting as a server uses Windows authentication to check the Windows credentials of the client application.

Simple password

Prior to making a connection, a custom password can be created on the Security tab of the Host and shared with PC-Duo Master user. This feature permits the PC-Duo Master user to connect to a Host without regard to PC-Duo Master user"s Windows credentials.

NOTE: Simple password applies only to peer-to-peer connections.

Shared secret password

In the case that the Host does not share a domain relationship with the PC-Duo Gateway, or if the Host is outside of the network and cannot contact its domain controller, Windows authentication will not usually be available. Behind the scenes, the PC-Duo Gateway and the Host will exchange a 16-byte secret password that only they will know. As a result, in all subsequent connections, the PC-Duo Gateway and Host will have some measure of authentication when they are not in the same domain. If the Host belongs to the same domain as the PC-Duo Gateway, and the Host is able to reach a domain controller, the Host will prefer to do Windows authentication instead of shared secret password.

Endpoint Authentication

In general, this operation answers the following security question: How does the client know it is connected to the right server? Identity authentication doesn't prohibit the client from being fooled into connecting to a different server. In order to guarantee that information and services are coming from the expected server, PC-Duo supports endpoint authentication using Secure Sockets Layer (SSL).

SSL certificate authentication (PC-Duo Gateway only)

PC-Duo has implemented server endpoint authentication using SSL, which means the client will request and validate a certificate from the server before providing requested information or services. This ensures the client has connected to the right server. The following list describes where SSL authentication can and cannot be used:

SSL certificate authentication (PC-Duo Gateway only)

PC-Duo has implemented server endpoint authentication using SSL, which means the client will request and validate a certificate from the server before providing requested information or services. This ensures the client has connected to the right server. The following list describes where SSL authentication can and cannot be used:

Peer-to-peer connections

SSL authentication is not available for peer-to-peer connections. This would require each Host (acting as server) to carry its own certificate, which would be unwieldy and costly to manage.

Gateway-managed connections (Host is in same domain as Gateway)

SSL authentication is available between Master (acting as client) and Gateway (acting as server). Before connecting, the Master will request and validate a certificate from the Gateway. In general, SSL between Master and Gateway would be most useful when the Master is outside the LAN and/or coming in through a corporate firewall to access the Gateway.

NOTE: SSL authentication is not available between the Gateway (acting as client) and the Host (acting as server). As in peer-to-peer connections, this would require each Host to carry its own certificate. SSL connections to the Host are generally not required because the Host can be configured to use a reverse connection to the Gateway, which can use SSL.

Gateway-managed connections (Host is not in same domain as Gateway)

When the Host is outside the LAN and/or behind a firewall or NAT-device, the Host is the client and has responsibility to contact the Gateway. SSL authentication is supported and would be appropriate to ensure that the Host is connecting to the right Gateway. The Host will validate the Gateway Server certificate before accepting the connection, ensuring that the Host is communicating with the correct Gateway Server.

In summary, SSL can be used by the Master to authenticate a Gateway, and by a Host to authenticate a Gateway when the Host is outside the domain.

Vector

Secure Remote Control for conventional and virtual desktops

Authorization Controls for Connection and for Access

One of the strongest features of PC-Duo remote support solutions is the fine-grained access control. For example, to perform remote support, you must have the following:

- Proper credentials with which to connect to the Host computer
- Authorization to view the Host computer remotely
- Authorization to control the Host computer remotely

Your credentials are established when you connect to a Host computer (or to a PC-Duo Gateway), and persist until the connection breaks. You can configure access and other rights directly on the Host computer for peer-to-peer connections. Alternatively, you can use the PC-Duo Gateway to enforce custom access rights policies on PC-Duo Master users, roles, or groups for Gateway-managed connections.

For a full listing of all the connection and access control provisions for Series 12 PC-Duo, please see the documentation available online at www.vector-networks.com, under the Resources \ Documentation section.

Accessing Locked Desktops

Over time we have been required to provide a broad spectrum of behaviour when dealing with locked desktops. In many situations the helpdesk is already working in a position of trust and after a short timeout access is granted and support can logon. For a minority of desktops or virtual desktop sessions, the remote user's security profile will dictate that remote control has to be explicitly granted on every occasion. In turn this prompted the ability for a customer to create a super-administrator user with ability to override the restriction. Session Audit, with Record and Replay, is normally enforced in this scenario.

Recent applications of PC-Duo's support for Terminal Services and VMware include -

- **IT user support in a hospital in the Netherlands.**
- **Gas pipeline monitoring in Canada.**
- **IT user support in local government in the Netherlands.**
- **IT user support in a manufacturing installation in Portugal.**
- **Biochemical process monitoring in Belgium.**

About the author:

Colin Bartram's background in IT Asset and Service Management runs uninterrupted from the 1980s, and includes specifying, writing, selling and supporting software solutions. Today he contributes to product strategy and marketing for the Vector Networks group of companies.

Acknowledgements:

Thanks are due to our great customers for talking to us about the challenges they face, and to our PC-Duo product specialists for highlighting the security functions that provide the solutions.

More at:

http://www.vector-networks.com/it-asset-and-service-management/ITIL-ITSM-products/PC-Duo-remote-control.html

Americas and AsiaPacific

Vector Networks Inc
Atlanta, Georgia, USA
www.vector-networks.com
sales@vector-networks.com
Sales: 770 622 2850
Support: 800 330 5035

EMEA

Vector Networks Europe Ltd
Sheffield, South Yorkshire, UK
www.vector-networks.eu
sales@vector-networks.eu
support@vector-networks.eu
Sales: +44 (0)203 286 7500

Your local supplier