PCoIP® Technology User Guide

EVGA Corporation
2900 SATURN ST. SUITE B, BREA, CA 92821, USA

p +1 714 528 4500 f +1 714 528 4501
www.evga.com

The information contained in this document represents the current view of EVGA Corporation as of the date of publication. Because EVGA must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EVGA, and EVGA cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EVGA MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Introduction

This user guide gives an overview of important features of EVGA's PC-over-IP® (PCoIP®) Technology. For more in-depth information, please refer to the reference documentation.

Configuration Examples

This document uses the Administrative Web Interface for configuration examples. Other tools, such as the Management Console, can provide similar functionality. For more details on configuring PCoIP, see the Administrative Interface User Manual [1] and other tool documentation.

Contents

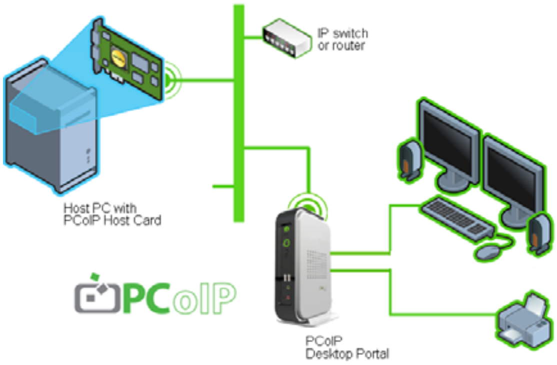
Introduction 2
Contents 2
1 PCoIP Technology Overview 3
2 PCoIP Technology Administration 5
3 Deployment Options 7
4 Discovery Mechanisms 12
5 Network Considerations 14
6 Bandwidth Considerations 16
7 Imaging Considerations 18
8 Network Characterization 19
9 Latency Considerations 22
10 USB Security 23
Definitions 25
References 26

1 PCoIP Technology Overview

PC-over-IP® (or PCoIP®) Technology is designed to deliver a user's desktop from a centralized host PC with an immaculate, uncompromised end-user experience across standard IP networks; including full DVI dual monitor video, complete USB compatibility, and high-definition audio.

PCoIP Technology makes it possible to locate the PC or workstation hardware in the datacenter while continuing to give users full desktop performance.

Figure 1-1: PCoIP System



PCoIP Technology uses networking and proprietary encoding/decoding technology to allow remoting of the host PC or Workstation. Using the desktop Portal, desktop peripherals can be used normally, as if they were connected directly to the host PC or Workstation.

PCoIP Host

The PCoIP PCIe Host card is installed in the remote host PC. The DVI output is connected to the Host card where the DVI output is compressed. The Host card PCIe bus connection provides transparent bridging of USB and HD audio using standard USB and audio drivers.

PCoIP Portal

At the desktop, the PCoIP Portal decompresses and distributes video, audio and USB data. The PCoIP Portal combines audio and USB peripheral data for transmission back to the Host.

To ensure desktop responsiveness, the process of compression, transmission, and rebuilding happens very quickly − typically in less than one display frame update.

A PCoIP Portal can be a standalone desktop device, or be integrated into a monitor.

OS and Application Compatibility

- Compatible with all operating systems
- Extensively tested with Microsoft Windows® XP® and Windows Vista®
- Uses standard USB and HD audio device drivers
- Compatible with all PC applications as no hardware or OS changes are required in the host PC

Display

- Perception-free experience with low latency, full frame rate video for the same user experience as a local PC
- Progressive build to deliver exact image of the rendered host display

Network

- Uses existing IP networks and coexists with existing IP data
- Optimizes user experience for a given bandwidth by adaptively controlling image data quality and update rate and optionally compressing the audio stream
- Adapts to changing network conditions and uses less bandwidth when the network is congested
- Can be optimized for minimal bandwidth usage for lower bandwidth situations (e.g. corporate WAN)

Input/Output

- Fully-bridged USB for all USB devices (including USB2.0 at USB1.1 data rates)
- Bi-directional, multi-channel digital audio

Security

- The PCoIP Portal is a stateless desktop device with no locally-stored host data or embedded Windows or Linux operating system to be compromised
- Host/Portal communication uses two secured streams. The control data stream is secured using digital certificates for mutual authentication. The media data stream is secured by an AES encryption algorithm
- USB access is fully configurable and may be authorized or blocked by Class or Vendor/Device ID. Any blocked USB devices are terminated at the Portal to ensure that security is not compromised

IT Support

- Neither Host nor Portal use an embedded Windows or Linux operating system allowing easier and less costly IT support
- The Portal does not need special drivers for peripheral support - all USB devices are transparently bridged to the host PC
- A PCoIP System provides the familiar PC user experience reducing end-user training requirements vs. other remoting technologies
- For users who do not need the rich experience of PCoIP Technology, the Portal can also be used as an RDP client

2 PCoIP Technology Administration

Administrators (admins) can use several tools to configure PCoIP Hosts and Portals:

- PCoIP Administrative Web Interface (Web Interface)
- PCoIP Management Console
- Connection broker
- Portal's On Screen Display (OSD) (Portal only)

These tools allow administrators to:

- Assign Host/Portal peering
- View and change network and security configuration settings and user permissions
- View session diagnostics and peripheral information

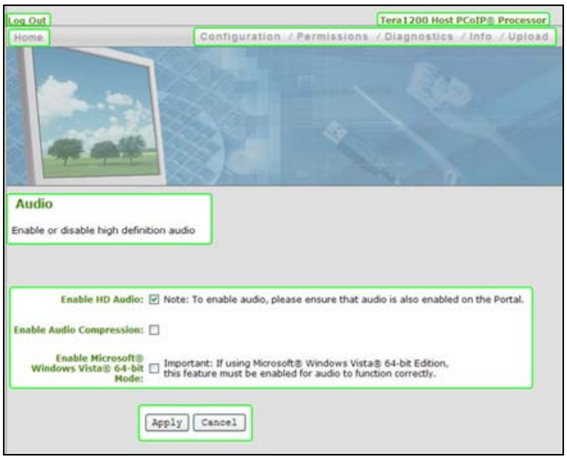
Each tool supports a different set of features. This document uses the Administration Web Interface for examples. For further information, see:

- PCoIP Administrative Interface User Manual [1]
- PCoIP Management Console Quick Start Guide [2]
- Connection broker documentation (provided by supplier)

Web Interface

The Web Interface allows admins to configure endpoints remotely via a Web browser.

Figure 2-1: Administration Web Interface


Log Out
Tera1200 Host PCoIP® Processor
Home
Configuration / Permissions / Diagnostics / Info / Upload
Apply
Cancel

Audio

Enable or disable high definition audio

Enable HD Audio: ☑ Note: To enable audio, please ensure that audio is also enabled on the Portal.

Enable Audio Compression: □

Enable Microsoft® Windows Vista® 64-bit Mode: □ Important: If using Microsoft® Windows Vista® 64-bit Edition, this feature must be enabled for audio to function correctly.

The figure above shows the Web Interface with seven regions highlighted:

- Log Out
- TERA1100 Portal PCoIP Processor or TERA1200 Host PCoIP Processor
- Home
- Drop-down menus: Configuration, Permissions, Diagnostics, Info, Upload
- Webpage summary information
- Data field (with inline help when appropriate)
- Apply/Cancel buttons (Apply stores parameters in flash memory; Cancel aborts the operation)

Supported Web Browsers

The Web Interface webpage server on PCoIP Hosts and Portals has been tested with:

- Firefox 1.5, 2.0 and 3.0
- Internet Explorer 6.0 and 7.0

Other browsers may also be compatible.

Accessing the Web Interface

1. Obtain the IP address of the Host or Portal endpoints:
   - If using a static IP Address, it is hard-coded and must be known.
   - If using a dynamic IP address, it is dynamically assigned by your DHCP (Dynamic Host Configuration Protocol) server. An admin can find the IP addresses

from the configuration settings or by querying the DHCP server.

2. In the browser's address bar, enter the IP address of the device to configure, for example:

    `https://192.168.1.123`.

Web Interface Security

The Web Interface uses HTTPS (HTTP over an SSL socket) and cannot be accessed without the administrative password. The HTTPS connection is secured by a self-signed certificate of Teradici, the provider of PCoIP processors.

CA Root Certificate Installation

To avoid browser security warnings when using the Web Interface, an admin can install a CA (Certificate Authorities) root certificate.

Using Internet Explorer 7:

1. On the *Tools* menu, click *Internet Options.*
2. On the *Content* tab, click the *Certificates* button.
3. On the Trusted Root Certification Authorities tab, click the *Import* button.
4. Follow the directions to import the certificate (ensure to use the *Trusted Root Certification Authorities* certificate store).

Note: When browsing for the certificate, an admin may have to change the File Type setting to "All Files".

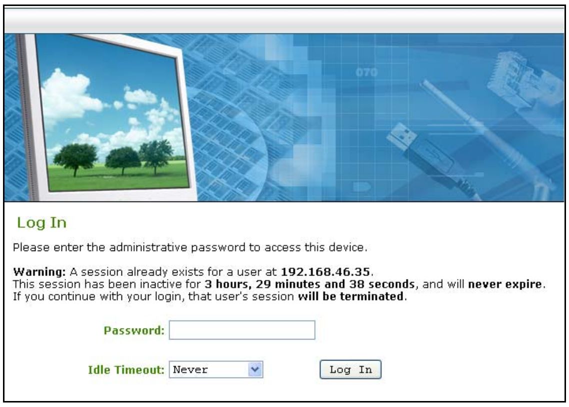
Using Firefox:

1. On the *Tools* menu, click *Options.*
2. At the top of the window, click the *Advanced* icon.
3. On the *Encryption* tab, click the *View Certificates* button.
4. On the *Authorities* tab, click the *Import* button
5. Follow the directions to import the certificate – ensure to check the option labeled *Trust this CA to identify web sites*

Log In Webpage

The *Log In* webpage lets the admin securely log in to the Web Interface.

Figure 2-2: Log In Webpage



Log In

Please enter the administrative password to access this device.

Warning: A session already exists for a user at **192.168.46.35**.
This session has been inactive for **3 hours, 29 minutes and 38 seconds**, and will **never expire**.
If you continue with your login, that user's session **will be terminated**.

Password:

Idle Timeout: Never

Figure 2-2 shows the *Log In* webpage with;

- Warning message displays pertinent information regarding the endpoint that the admin is logging in to
- Password - allows access to the admin webpage (default value is blank, i.e. "")
- Idle Timeout (1 minute, 5 minutes, 15 minutes, 30 minutes, Never) before automatically logged out

To log into a Host or Portal endpoint:

1. Browse to endpoint IP address
2. In the *Password* text box, enter the admin password
3. In the *Idle Timeout* list, select the amount of time the administration session can remain idle before automatically logged out
4. Click the Log In button

3 Deployment Options

DHCP vs. Static IP

PCoIP Hosts and Portals are configured with DHCP (Dynamic Host Configuration Protocol) enabled by default. When Hosts and Portals are connected to a DHCP server, their IP addresses are dynamically assigned and their address configuration information can be found on the Web Interface's *Network* webpage (see below).

When DHCP is used with default settings, the Host and Portal populate the DHCP server with names in this format:

```
pcoip-host-mac.domain
pcoip-portal-mac.domain
```

Where `mac` is the device's 6-octet MAC address and `domain` is the local domain.

If a DHCP server is not found after 120 seconds after power up, the endpoints use the following settings:

Host IP: `192.168.1.100`

Portal IP: `192.168.1.50`

Subnet Mask: `255.255.255.0`

Gateway: `192.168.1.0`

Although not recommended, static IP addresses may be used for small PCoIP System deployments. Recommendations when using static IP addresses:

- Reserve a range of static IP addresses for PCoIP deployments.
- Do not use IP addresses reserved for DHCP.

For larger deployments, DHCP is recommended to avoid having to manage large numbers of static addresses. With DHCP, it's recommended to use a discovery mechanism to avoid "losing" endpoints in the IP network (refer to Discovery Mechanisms).

Deployment Methods

There are four methods for deploying PCoIP Systems:

1. Basic 1:1 - uses default configuration settings to pair Host/Portal endpoints. Limited to one Host/Portal pair on a simple network.
2. Manual Configuration - allows manually entering Host/Portal pairings. This method is often most efficient for small deployments.
3. PCoIP Management Console - a simple tool for automating pairings and management. This is recommended for medium-size deployments.
4. Connection Broker - a third-party management tool often with extended configuration features. A Connection Broker is recommended for large deployments.

Deployment Method #1: Basic 1:1

In this scenario, the Host and Portal default settings allow a PCoIP Session without detailed configuration. This deployment allows a simple remoting experience with little or no endpoint management, including:

- Direct Host-Portal connection with single Ethernet cable (cross over cable not required)
- Host-Portal connection via IP switch(es)

When using a direct connection without an IP switch, the Host and Portal endpoints cannot be managed using the Administrative Web Interface.

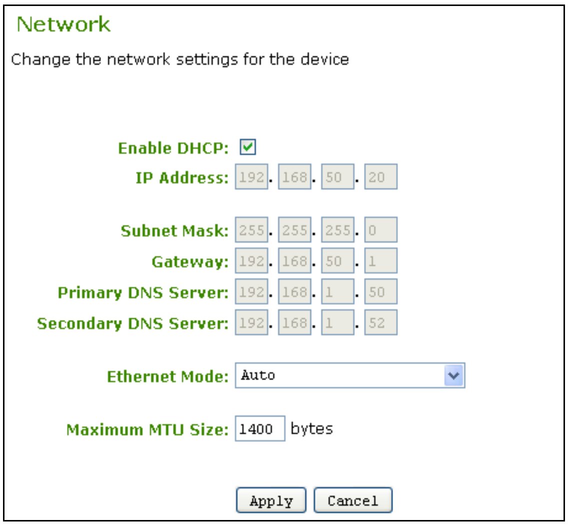
Note: Since all endpoints fall back to the default static IP addresses described above, no more than one Host/Portal pair can be used on a simple IP network. These static IP addresses may also conflict with other addresses if the network already uses them.

Deployment Method #2: Manual Configuration

For smaller deployments, manual pairing of Hosts and Portals is quick and easy and can be done using the PCoIP Administrative Web Interface.

To use Manual Configuration, log on to the Web Interface (see Accessing the Administrative Web Interface). Then use the Web Interface's *Network* and *Session* webpages as follows.

Figure 3-1: Network Webpage



Network

Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 50 . 20

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 50 . 1

Primary DNS Server: 192 . 168 . 1 . 50

Secondary DNS Server: 192 . 168 . 1 . 52

Ethernet Mode: Auto

Maximum MTU Size: 1400 bytes

The *Network* webpage has eight parameters:

Available IP addressing settings – allows network parameter configuration

- *Enable DHCP* (see DHCP vs. Static IP above)
- *IP Address*, *Subnet Mask*, *Gateway* (entered when using static IP addressing)
- *Primary DNS Server*, *Secondary DNS Server* (provided by DHCP server when using DHCP IP addressing – not used with static IP addressing)

Each endpoint must have a unique IP address that does not conflict with other devices on the network.

To simplify configuration, all endpoints can be on the same subnet, for example:

IP address: `192.168.1.x`

Subnet Mask: `255.255.255.0`.

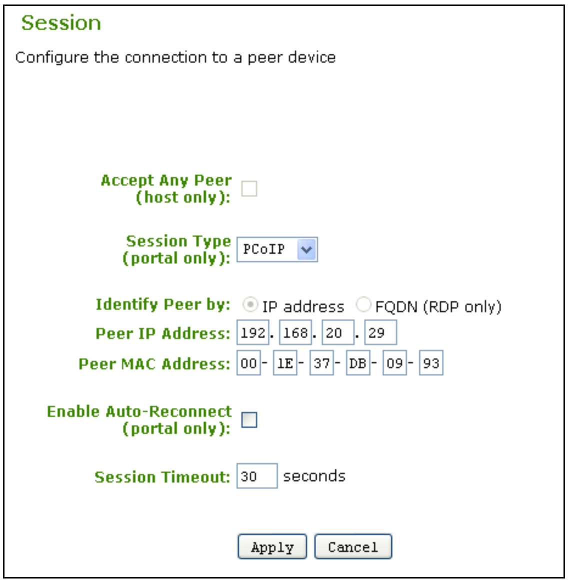
Ethernet Mode - sets the network data rate:

- *Auto* (recommended – will auto negotiate to proper network data rate)
- *10 Mbps Full-Duplex* – for use with legacy network equipment, such as an IP switch, that can only support 10Mbps
- *100 Mbps Full-Duplex* – for use with legacy network equipment, such as an IP switch that can only support 100Mbps

Note: An improper Ethernet setting may create a half-duplex connection. Since PCoIP Technology is not compatible with half-duplex network connections, a warning message is shown, and the session is eventually lost.

Maximum MTU Size - see Maximum Transmission Unit in Section 5, Network Considerations.

Figure 3-2: Session Webpage



Session

Configure the connection to a peer device

Accept Any Peer (host only): □

Session Type (portal only): PCoIP

Identify Peer by: ● IP address ○ FQDN (RDP only)

Peer IP Address: 192 . 168 . 20 . 29

Peer MAC Address: 00 - 1E - 37 - DB - 09 - 93

Enable Auto-Reconnect (portal only): □

Session Timeout: 30 seconds

The *Session* webpage has seven parameters:

Session parameters – sets basic session settings

- *Accept Any Peer* - allows the Host to accept any Portal for a PCoIP Session.
- *Session Type* - PCoIP or RDP

Peer Identity parameters – sets how to identify the remote peer

- *Identify Peer by* - use IP address for PCoIP Sessions and FQDN for RDP sessions
- *Peer IP Address* – the other endpoint's IP address
- *Peer MAC Address* – the other endpoint's MAC address

Other session parameters

- *Enable Auto-Reconnect* - Portal reconnects automatically when a PCoIP Session is lost
- *Session Timeout* - time to wait before ending a session, when the network is lost or severely congested

Example: Manual Configuration

This example demonstrates manual peer-to-peer configuration of the Host and Portal pair, i.e. without the use of a management tool (Management Console, connection broker, etc).

This example uses the following IP and MAC addresses:

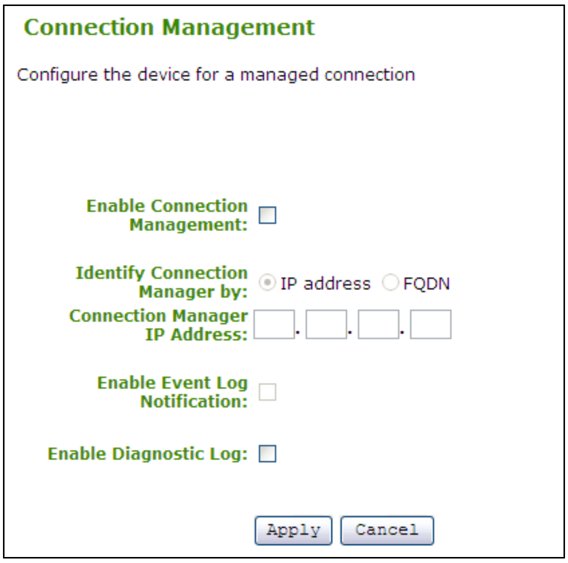
	IP	MAC
Host	`192.168.20.29`	`00-1E-37-DB-09-93`
Portal	`192.168.0.34`	`00-16-41-FF-5C-C0`

Note: For a manual peer-to-peer connection, the Host and Portal IP and MAC addresses must be known.

First configure the Portal:

1. In a browser, open the Portal's Web Administration Web Interface, for example: `https://192.168.0.34`.
2. Log in to the Web Interface by entering the admin password.
3. From the *Configuration* menu, select *Connection Management*.

Figure 3-3: Connection Management Webpage



Connection Management

Configure the device for a managed connection

Enable Connection Management: □

Identify Connection Manager by: ● IP address ○ FQDN

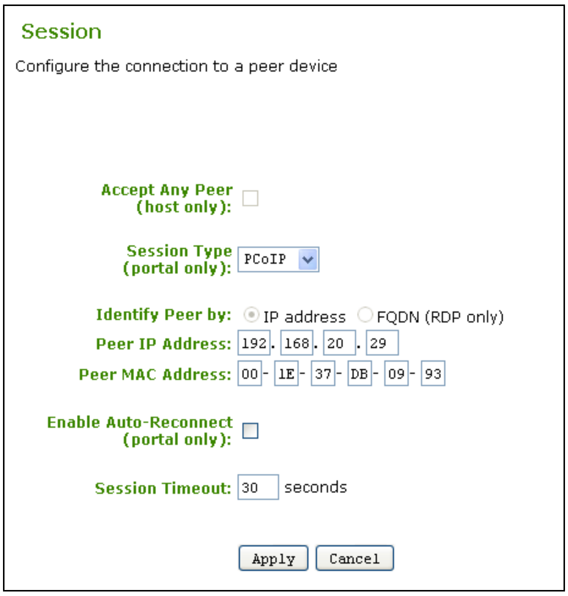
Connection Manager IP Address: ☐.☐.☐.☐

Enable Event Log Notification: □

Enable Diagnostic Log: □

4. Ensure that *Enable Connection Management* is not selected.
5. On the *Configuration* menu, select *Session* webpage from the *Configuration* menu.

Figure 3-4: Session Webpage (Portal)



Session

Configure the connection to a peer device

Accept Any Peer (host only): □

Session Type (portal only): PCoIP

Identify Peer by: ● IP address ○ FQDN (RDP only)

Peer IP Address: 192.168.20.29

Peer MAC Address: 00-1E-37-DB-09-93

Enable Auto-Reconnect (portal only): □

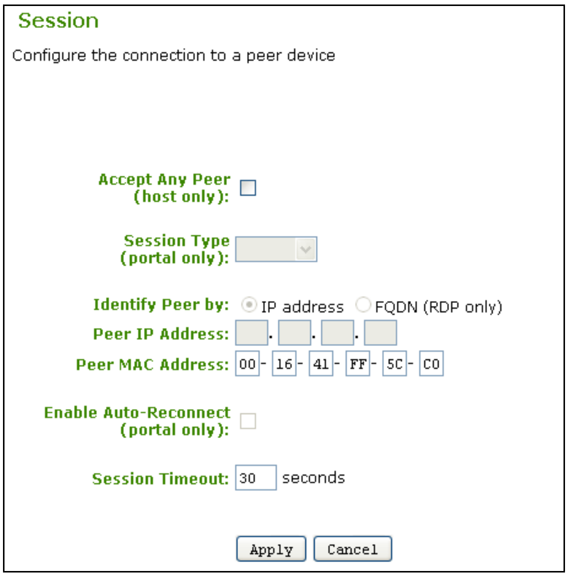
Session Timeout: 30 seconds

6. In the *Peer IP Address*, enter the Host's IP address, e.g. `192.168.20.29`.
7. In the *Peer MAC Address*, enter the Host's MAC address, e.g. `00-1E-37-DB-09-93`.
8. Click the *Apply* button to accept changes.

Now configure the Host:

1. In a browser, open the Host's Web Administration Web Interface by typing its address in the address box, for example, `https://192.168.20.29`.
2. Log in to the Web Interface by entering the admin password.
3. From the *Configuration* menu, select *Connection Management*.
4. Ensure *Enable Connection Management* is not selected.
5. On the *Configuration* menu, select *Session*. The *Session* webpage appears.

Figure 3-5: Session Webpage (Host)



Session

Configure the connection to a peer device

Accept Any Peer (host only): □

Session Type (portal only):

Identify Peer by: ● IP address ○ FQDN (RDP only)

Peer IP Address: . . .

Peer MAC Address: 00 - 16 - 41 - FF - 5C - C0

Enable Auto-Reconnect (portal only): □

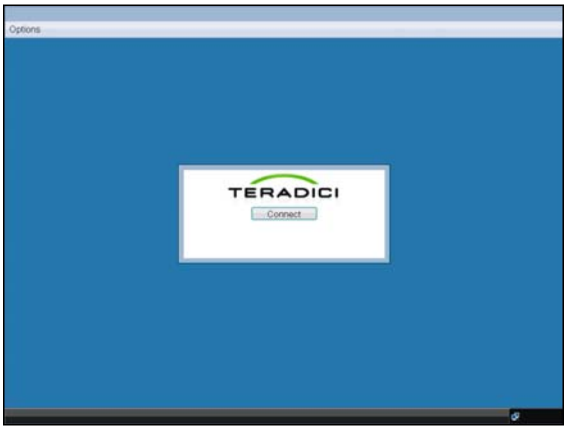
Session Timeout: 30 seconds

6. Ensure *Accept Any Peer* is not selected.
7. In the *Peer MAC Address*, enter the Portal's MAC address, e.g. `00-16-41-FF-5C-C0`.
8. Click the *Apply* button.

Start the peer-to-peer session:

1. Click the *Connect* button.

Figure 3-6: Connect Screen



2. Once it is connected, the Host computer is ready to use over PCoIP Technology.

Deployment Method #3: Management Console

The PCoIP Management Console (PCoIPMC) is a tool to help configure Host and Portal endpoints for medium-size PCoIP Technology deployments.

The PCoIPMC is a HTML-based virtual appliance packaged with the minimum required OS.

The PCoIPMC can also be used in conjunction with a connection broker to manage the configuration of PCoIP Endpoints.

The recommended environments for the PCoIPMC are:

- Single subnet static IP addresses
- DHCP with DNS server deployments
- SLP for discovery (PCoIPMC discovers endpoints)
- DNS-SRV for discovery (endpoints discover PCoIPMC)

Note: The DNS-SRV Resource Record name for the PCoIPMC is `pcoip-tool`.

The PCoIP Management Console capabilities are summarized in the table below:

Table 3-1: PCoIPMC Capabilities

Devices	Add newly discovered Host and Portal endpoints (and give endpoints a descriptive name)
	Assign a endpoint to a group
	View endpoint info (firmware revision, attached devices, etc.)
Groups	Create/edit/delete group
	Assign profile(s) to group
Profiles	Create/edit/delete profiles
	Add configuration parameter to profile (USB authorization, bandwidth limits, etc)
Peering	Peer Portal with Host
Update	Update firmware to endpoint or endpoint group

For details on configuring the PCoIP Management Console, see the PCoIP Management Console Quick Start Guide [2].

Deployment Method #4: Connection Brokers

Connection brokers allow management of a large PCoIP Technology deployment by dynamically assigning Host/Portal pairs.

Compared to the Administrative Web Interface and PCoIP Management Console, connection brokers often offer more control over user and endpoint policies, for example:

- Host Pooling
- Defining user sessions
- Policies based on User ID and location

Connection brokers are server based to allow continuous monitoring of Host and Portal endpoints.

The PCoIP Management Console may be used simultaneously with a connection broker.

If using a connection broker, refer to documentation provided by the connection broker supplier.

4 Discovery Mechanisms

Before a PCoIP Session can begin, a Host and Portal must be paired (associated with each other).

The first step is to determine the network location of each Host and Portal endpoint. This can be done manually, but in larger PCoIP Technology deployments, it's often more convenient to discover the endpoints automatically.

In order for the management tool (PCoIP Management Console, connection broker, etc.) to discover the endpoints, the endpoints may use a combination of:

- DNS-SRV Resource Records discovery (DNS-SRV RR)
- SLP discovery

The discovery mechanisms available with PCoIP Technology may be used with each other or separately.

SLP discovery may be used by the Host and Portal without a management tool. See Service Location Protocol below for more detail.

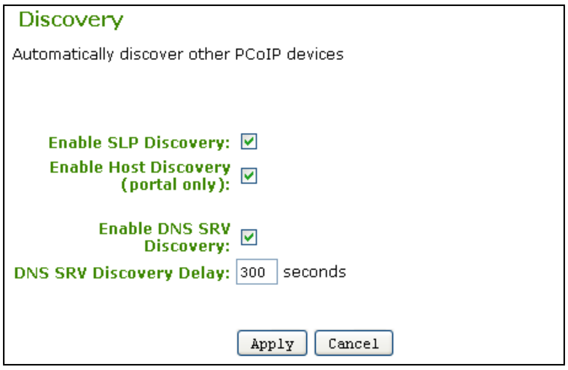
DNS-SRV is recommended for discovering Host and Portal endpoints. For more details, see the next section, Discovery using DNS-SRV Resource Records.

Note: A good understanding of networking is required before implementing discovery mechanisms.

Configuring Discovery

Use the Web Interface's *Discovery* webpage to enable discovery mechanisms.

Figure 4-1: Discovery Webpage



Discovery

Automatically discover other PCoIP devices

Enable SLP Discovery: ☑

Enable Host Discovery (portal only): ☑

Enable DNS SRV Discovery: ☑

DNS SRV Discovery Delay: 300 seconds

The *Discovery* webpage has four settings:

Enable SLP Discovery – see Discovery Using Service Location Protocol below

Enable Host Discovery – allows Portal to discover available hosts when establishing a PCoIP session

Enable DNS SRV Discovery – see Discovery Using DNS-SRV Resource Records, below

DNS SRV Discover Delay – amount of delay time in seconds between DNS SRV Discovery attempts. DNS SRV Discovery continues periodically until the device is successful in contacting a Connection Management Server

Discovery Using DNS-SRV Resource Records

Host and Portal endpoints can be configured to use discovery mechanisms that use DNS-SRV Resource Records (see RFC 2782). For details, see the PCoIP Management Console [2] or connection broker's documentation.

Like other discovery mechanisms, DNS-SRV discovery allows the management tool to discover the endpoint without prior configuration of the endpoint's Connection Manager IP Address or DNS Name parameter. (In other words, DNS-SRV discovery operates independently of the Connection Manager IP Address or DNS Name value.) If the value in the endpoint becomes stale, DNS-SRV discovery continues to work and the new CMS can discover the endpoint.

Benefits

DNS-SRV discovery has the ability to have redundant backup of CMS hosts. DNS-SRV Resource Records can have multiple CMS servers with different priorities and weights, so endpoints can advertise to the primary CMS first, and in the event of a transmit failure, advertise to a secondary CMS.

Unlike Service Location Protocol, DNS-SRV discovery does not use multicast IP traffic. As a result, it works across subnets. Routers are typically configured to block multicast IP traffic by default, so the CMS cannot use SLP to discover endpoints located on different subnets.

DNS-SRV provides a standardized approach for the endpoint to query the DNS server for a CMS service.

Requirements

DNS-SRV discovery requires that:

- DNS zone data must have a DNS-SRV RR in the format described by RFC 2782:

```
_Service._Proto.Name TTL Class
SRV Priority Weight Port Target
```

where:

```
_Service=_pcoip-broker,

_Proto=_tcp,

Name = hierarchical domain name
```

- Endpoints must have access to a DHCP server in order to get the domain name and hostname (to get DHCP options 15 and 12, respectively).
- The DHCP server must support either DHCP option 12 (hostname), 15 (domain name), or both. If the server supports only option 12, the hostname string must contain the domain name.

Discovery Using SLP (Service Location Protocol)

The endpoint can be configured to use SLP (Service Location Protocol) discovery. How the endpoint uses SLP discovery depends on whether the deployment is managed or unmanaged.

In unmanaged deployments:

- Host and Portal advertise services so that another network SLP-aware entity can discover the endpoint.
- When host discovery is enabled on a Portal, the Portal dynamically discovers Hosts.

In managed deployments:

- The Host and Portal advertise services so the CMS can discover the endpoint.

The endpoint uses the Service Location Protocol SLPv2 as defined in RFC2608. The endpoint advertises a service to either an SLP directory agent or an endpoint/CMS (if a Directory Agent is not present).

SLP over Multiple Subnets

When endpoints, CMS (if present), and Directory Agent (if present) are on the same subnet, SLP uses multicast/broadcast SLP messaging to register and discover service locations. However, when any endpoint or CMS is on a different subnet, routers must be configured to allow packets destined for the SLP multicast group 239.255.255.253 to pass.

Multicast reduces network congestion by directing SLP messages to endpoints registered with the standard SLP multicast group. The endpoint uses IGMP (Internet Group Management Protocol) to “join” the standard SLP multicast group. Packets sent to IP address 239.255.255.253 are multicast to the endpoints registered with the group.

A User Agent multicasts a service request (to the SLP multicast group) and a Service Agent responds via a unicast connection. If the PCoIP System is deployed over multiple subnets, the multicast-enabled routers must not filter packets destined for the SLP multicast group.

5 Network Considerations

PCoIP Technology uses routable IPv4 network packets. By default, endpoints are configured for use in an enterprise network with minimal setup. This section describes factors that may affect some IP networks.

The bulk of network traffic between the PCoIP Host and Portal consists of video, USB, and audio data, and is carried in IPsec-ESP packets. Other network protocols are used for configuration and control (see port numbers below).

Full-Duplex Networks

PCoIP Technology requires full-duplex Ethernet links. Older communication equipment, including hubs and half-duplex switches, are not appropriate for PCoIP Technology deployments due to their limited effective bandwidth.

PCoIP Technology TCP/UDP Ports

Table 5-1 summarizes the TCP and UDP ports used in PCoIP Systems. For networks with firewalls between the Host and Portal, these ports must be open.

Table 5-1: PCoIP Technology TCP/UDP Ports

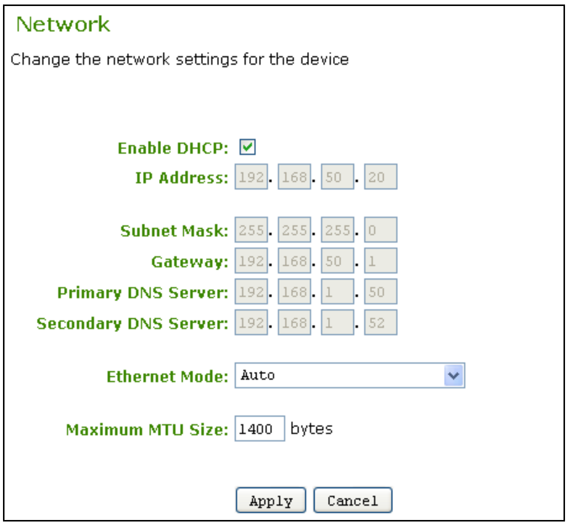
Port	Port Number
TCP ports	21, 51, 80, 427, 443, 8000, 50000, 50001
UDP ports	53, 67, 68, 427

Maximum Transmission Unit (MTU)

The PCoIP Technology firmware allows configuration of the Maximum Transmission Unit (MTU) of data packets. This allows customization of MTU size for the network equipment used (see Packet Fragmentation, below).

The *Maximum MTU Size* can be set using the Administrative Web Interface's *Network* webpage:

Figure 5-1: Network Webpage (MTU configuration)



Network

Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 50 . 20

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 50 . 1

Primary DNS Server: 192 . 168 . 1 . 50

Secondary DNS Server: 192 . 168 . 1 . 52

Ethernet Mode: Auto

Maximum MTU Size: 1400 bytes

Maximum MTU Size configuration:

- Default *Maximum MTU Size* is 1400 bytes, and can be set from 500 to 1500 bytes

NAT Traversal

PCoIP Technology data packets are IPSec encrypted and do not have any port numbers external to encryption. As a result, the packets are not compatible with networking equipment (e.g. routers) that implements Network Address Translation (NAT).

NAT networking gear can be used when PCoIP Technology network traffic is encapsulated in a tunneling protocol as well. This tunneling can be achieved using a hardware VPN link (see Virtual Private Networks section, below).

Packet Loss and Ordering

PCoIP Technology is resilient to packet loss; however, performance degrades as a function of the loss rate. For good user experience, packet loss should be limited to less than 0.1%.

Packets reordered by network equipment are treated as lost.

PCoIP Technology transfer and loss statistics are available in the Administration Web Interface, management tools (PCoIP Management Console, connection broker, etc.), and are also provided via an SNMP MIB.

Packet Fragmentation

PCoIP Technology data packets must not be fragmented by network equipment.

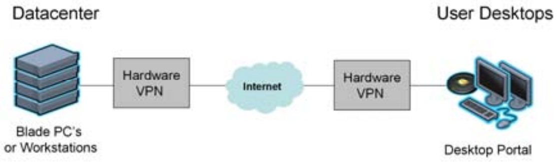
To avoid fragmentation, the MTU can be set to the largest MTU supported by all the equipment across the network path. See Maximum Transmission Unit (MTU) above for configuration information.

Virtual Private Networks (VPN)

A Virtual Private Network (VPN) tunnel can allow PCoIP Technology traffic to traverse firewalls and network equipment that is performing NAT. PCoIP Technology is compatible with hardware VPNs.

For port and MTU configuration, refer to the PCoIP TCP/UDP Ports and Maximum Transmission Unit sections above.

Figure 5-2: Example VPN



6 Bandwidth Considerations

Bandwidth requirements in PCoIP Systems depend on users' applications and the kind of experience they require. This section describes some considerations for bandwidth configuration.

Bandwidth Usage

PCoIP Systems have four general sources of bandwidth usage:

- Host to Portal imaging data – dominates bandwidth
- HD Audio streams – typically use significantly less bandwidth than imaging data
- USB bridging – typically uses significantly lower bandwidth than imaging data
- System management – uses relatively negligible bandwidth

Imaging Bandwidth

As PCoIP Technology's imaging data dominates PCoIP System network bandwidth use, it's important to understand these characteristics:

- Only changing screen areas generate imaging related network traffic
- Because lower-resolution displays have fewer possible pixel changes, they usually require less bandwidth than high-resolution displays
- The most demanding imaging is high-resolution, high-contrast, full-screen moving images (e.g. video games, real-time 3D rendering)
- If desired, PCoIP Technology can be configured to use less bandwidth (with a possible reduction in user experience)
- Long periods with no pixel changes result in low average network traffic

Audio and USB Bandwidth

Audio and USB considerations:

- Audio compression can be enabled to reduce bandwidth during network congestion
- USB data is not compressed

Bandwidth Priorities

PCoIP System bandwidth priorities are:

1. USB and audio (highest)

2. Imaging (uses remaining available bandwidth)

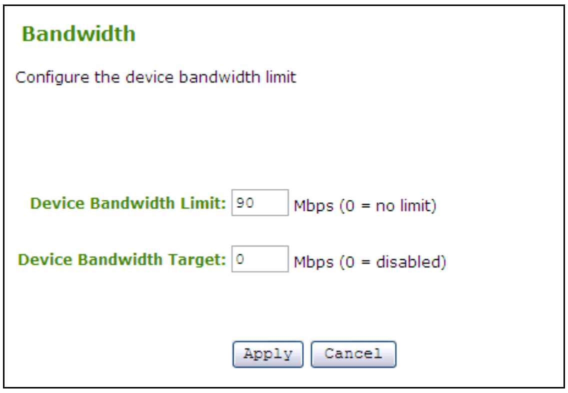
Bandwidth Configuration

The Administrative Web Interface's *Bandwidth* webpage has two bandwidth parameters

- The Portal webpage defines Portal → Host bandwidth.
- The Host webpage defines Host → Portal bandwidth.

Bandwidth paramaters can be set from 3 to 220 Mbps.

Figure 6-1: *Bandwidth* Webpage



Bandwidth

Configure the device bandwidth limit

Device Bandwidth Limit: 90 Mbps (0 = no limit)

Device Bandwidth Target: 0 Mbps (0 = disabled)

The *Bandwidth* webpage has two parameters:

Device Bandwidth Limit - limits maximum peak bandwidth use

- A value of 0 (zero) allows PCoIP Technology to adjust for congestion (no congestion, no limit)
- Recommended setting: link limit (minus 10% headroom) of network connected to Host and Portal

Note: Device Bandwidth Limit is applied immediately after clicking Apply.

Device Bandwidth Target - a soft bandwidth limit during congestion

- Allows more even distribution of user bandwidth on congested trunks
- A value of 0 (zero) sets no target

- A good understanding of network topology is required before setting Device Bandwidth Target to a non-zero value

Note: Device Bandwidth Target is applied on next PCoIP Session after selecting Apply.

7 Imaging Considerations

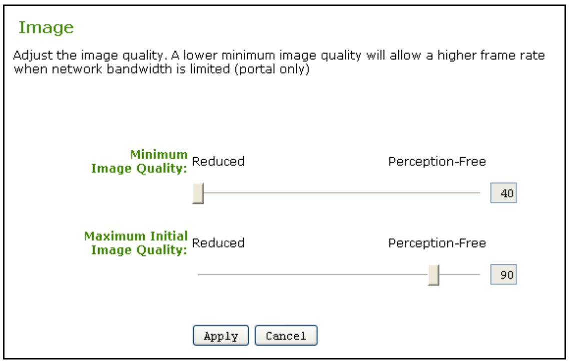
PCoIP Technology's imaging parameter settings have a large impact on user experience and bandwidth use.

Imaging Configuration

The Administrative Web Interface's *Image* webpage allows setting the preference during network congestion:

- Lower-quality images at a higher frame rate
- Higher-quality images at a lower frame rate

Figure 7-1: *Image* Webpage



Image

Adjust the image quality. A lower minimum image quality will allow a higher frame rate when network bandwidth is limited (portal only)

Minimum Image Quality: 40

Maximum Initial Image Quality: 90

The *Image* webpage has two parameters:

Minimum Image Quality – allows balancing between image quality and frame rate for limited-bandwidth scenarios:

- Selecting towards *Reduced* allows higher frame rates (and lower quality display) when network bandwidth is constrained
- Selecting towards *Perception-Free* allows higher image quality (and lower frame rates) when network bandwidth is constrained

Note: When network bandwidth is not constrained, PCoIP System maintains maximum image quality regardless of this setting.

Note: *Minimum Image Quality* must be set less than or equal to *Maximum Initial Image Quality* (see below).

It is recommended to set *Minimum Image Quality* to 40 to fully utilize PCoIP to balance quality and frame rate.

Maximum Initial Image Quality - changes the network bandwidth peaks a PCoIP Session requires by limiting initial quality on the changed regions of the image:

- Selecting towards *Reduced* reduces image quality of content changes and reduces peak bandwidth requirements
- Selecting towards *Perception-Free* increases image quality of content changes and increases peak bandwidth requirements

Note: The unchanged regions of the image progressively build to lossless state regardless of this setting.

Note: *Maximum Initial Image Quality* must be set greater than or equal to *Minimum Image Quality*.

It is recommended to set *Maximum Initial Image Quality* to 90 or lower to best utilize the available network bandwidth.

8 Network Characterization

This section describes the basic network impact of PCoIP Technology implementations.

Note: This base analysis is conservative and weighted towards a perception free user experience. Administrators must study usage cases typical for their deployment, and adjust network requirements accordingly.

User Categories

Understanding the user category and user experience desired are important to determine the network footprint required for PCoIP Technology deployments.

The generalized user categories below are arranged from lowest to highest bandwidth needs.

- Task Worker – primarily text entry into forms
- Knowledge Worker – standard office applications such as word processing, spreadsheets, presentation tools; Internet, email, etc.
- Performance User/Basic CAD – similar to Knowledge Worker, plus occasional use of high-end visual applications; may perform analysis on static images
- Video Editor – requires consistent high-quality multimedia playback
- Extreme User – Critical high-end visual applications such as 3D CAD, video editing, and animation; higher-resolution content; dynamically-manipulated images (CAD design, healthcare MRI/CAT scan analysis, etc.)

Bandwidth Planning

Bandwidth planning requires understanding the desired user experience to provide. The following are some guidelines:

- For conservative planning, plan according to the bandwidth a user needs during a worst-case congestion period
- A conservative, worst-case scenario is continuously changing full-screen video
- Plan for worst-case network congestion during simultaneous worst-case users
- The *Minimum Image Quality* and *Maximum Initial Image Quality* settings define user experience during instances of congestion (see Section 7 Imaging Considerations)
- For most users, minimum acceptable frame rate is 10 to 30 fps

Planning Basics

The following are provided as starting points for planning PCoIP System network requirements:

- More graphically-demanding applications command higher bandwidth than less graphically-demanding ones
- User applications and scenarios vary
- It's unlikely that all users will need peak bandwidth at the same time
- Some users are more critical then others. Acceptable performance is subjective.
- If network is rarely congested, no one will experience performance degradation

Conservative Planning

The following are some conservative recommendations to ensure a perception free experience:

- Provision network bandwidth with 10% "extra" bandwidth beyond the planning bandwidth
- Several Task Workers/Knowledge Workers could share a 100 Mbps connection
- More demanding users (e.g. Extreme Users) may benefit from the available bandwidth of 1 Gbps connections depending applications used

Once a baseline is established, there are more application characteristics to consider:

- Few applications produce full screen changes all the time
- Video has periods of low bandwidth
- Graphic screensavers consume bandwidth

Addressing Fairness

An important issue in network usage is fairness − the even sharing of network resources. Without fairness control, some users may get more bandwidth than others.

The administrator can improve fairness by using the Administrative Web Interface to set the *Device Bandwidth Target*.

Example: Target Bandwidth Example

Here's a simplified example of how the *Device Bandwidth Target* setting works. The example uses this scenario:

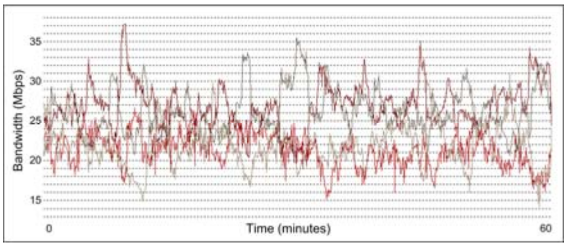
- Four users sharing a 100 Mbps link
- All users constantly active, using graphically-intensive applications (approximately 60% of display continually changing)
- *Device Bandwidth Limit* set to 0 Mbps (PCoIP Technology adjusts bandwidth use depending on congestion, to let users take advantage of unused bandwidth)
- Bandwidth measured over 60 minutes at 5 second intervals

The examples below show what happens when different *Device Bandwidth Target* setting are used: 0 Mbps (no Target), 20 Mbps, 25 Mbps, and 30 Mbps.

Device Bandwidth Target: 0 Mbps (no Target)

The figure below shows 4 users sharing a 100 Mbps link. Each user has Device Bandwidth Target set to 0 Mbps (no Target).

Figure 8-1: Device Bandwidth Target: 0 (no Target)



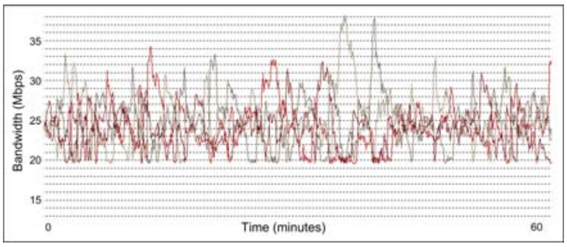
In the figure above, we can see:

- Many dips below 17 Mbps
- Obviously "unfair" network bandwidth use (some users left with lower bandwidths)

Device Bandwidth Target: 20 Mbps

Now users have the *Device Bandwidth Target* set to 20 Mbps.

Figure 8-2: Device Bandwidth Target: 20 Mbps



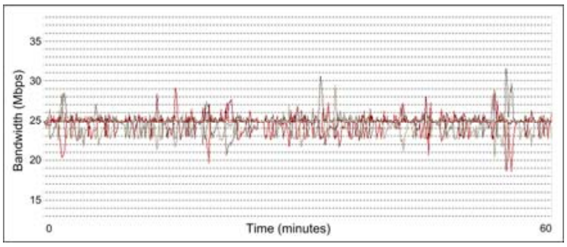
We now see:

- Bandwidth use clamps at 20 Mbps
- No user below "fair" bandwidth more than 20% of the time

25 Mbps Device Bandwidth Target

The bandwidth parameters are now updated so each user has the *Device Bandwidth Target* of 25 Mbps.

Figure 8-3: Device Bandwidth Target: 25 Mbps



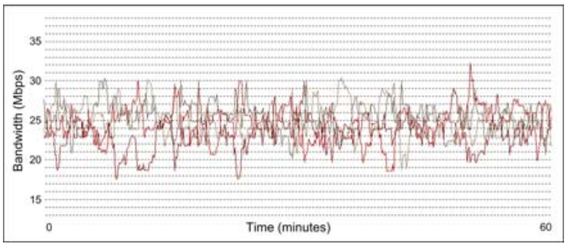
We now see:

- 25 Mbps per connection is the network capacity (100 Mbps / 4 users)
- Congestion management keeps bandwidth tight around 25 Mbps
- Some dips down to 19 Mbps

Device Bandwidth Target: 30 Mbps

Finally, each user has the *Device Bandwidth Target* configured to 30 Mbps.

Figure 8-4: Device Bandwidth Target: 30 Mbps



We now see:

- *Device Bandwidth Target* is set too high
- PCoIP Technology congestion management still operates, but is not optimized
- Fairness is better than with no Target (0)
- Some dips down to 18 Mbps

Bandwidth Optimization

The simplified example above shows that PCoIP System is optimized when the *Device Bandwidth Target* is set to ensure fairness for all users. Here the network link is 100 Mbps for four users, so the fair *Device Bandwidth Target* is 25 Mbps (100 Mbps / 4 users).

In the example, all four users were continually active. This is not a realistic scenario, as even extremely active users do not have constantly changing displays (e.g. pause to study detail). In actual use, it’s reasonable to assume that each user has periods of low bandwidth usage.

Also, this example is a bit backward, as it started with network capacity (100 Mbps) and then found fair-usage settings. A better strategy is to determine the bandwidth required to meet users’ expectations, and then work towards the network capacity it requires.

Device Bandwidth Limit Considerations

The example above has the *Device Bandwidth Limit* set to 0 (none) to let the PCoIP Processors manage bandwidth throttling. This is recommended for most networks, unless the administrator must limit bandwidth usage, for example if:

- Legacy network equipment is unreliable when fully utilized
- It is desired to put a cap on user bandwidth usage

Constrained Network Effects

PCoIP Technology is designed to adjust gracefully when there is not optimal bandwidth available. However, during high network congestion, some artifacts may become noticeable, including:

- Image smearing/blocking
- Less-responsive user interface (e.g. slower mouse and window movements)

It is recommended to set the *Device Bandwidth Limit* at or below the limiting network link the PCoIP Session data traverses. For example, if the PCoIP Session data traverses a 100 Mbps link (e.g. switch link to the desktop), the limit should not exceed 100 Mbps.

9 Latency Considerations

Every network has latency effects that may require attention. Latency effects keyboard, mouse and display response. These effects are user subjective with some users noticing effects more than others.

Some latency considerations:

- Latency due to length of physical medium (i.e. speed of light of copper/fiber) and switch hops
- Additional latency due to OS overhead (e.g. 40-50 ms for Windows)

The table below describes latency effects based on critical user evaluation.

Table 9-1: Latency Observations

Network Latency	Approximate Distance[1]	User Observations
0-30 ms	Campus/metro/ inter-city (0-1500km)	Perception free to average user
40-60 ms	Inter-city/intra-country (1500-2500km)	Minimal latency perceived, e.g. 'heavy' mouse and window movement, but very usable
60-100 ms	Intra-country/ inter-continent (2500-5000km)	Sluggish mouse and windows; some audio dropouts
> 100 ms	Inter-continent/ overseas (> 5000km)	Slow mouse and windows; audio dropouts

[1] High bandwidth, low-error network

Note: As with bandwidth considerations, these latency observations are subjective and biased towards a perception free experience. Administrators must study use case(s) typical for their deployment and adjust user expectations accordingly.

USB Latency Performance

Latency effects observed for USB performance depend on the type of data transfer.

- Isochronous - may notice delay or loss of data (e.g. video data lost when using a webcam)
- Interrupt - may delay device response (e.g. slow keyboard keystrokes)
- Bulk - may notice slower data transfer (e.g. slower USB flash drives)

Desired Network Attributes

Latency effects can be minimized by using a network with these attributes:

- High bandwidth
- Low error rate
- Minimized data path/network hops

Minimizing Latency Effects

Often latency effects can not be avoided due to extreme long distances, non-optimal networks, etc. Administrators can minimize bandwidth use and therefore reduce latency effects by:

- Using less graphically-demanding applications (and setting user expectations accordingly)
- Using *Device Bandwidth Target* and *Device Bandwidth Limit* settings to limit bandwidth usage to minimum requirements (see Section 6, Bandwidth Considerations)
- Configuring image settings to minimum image quality requirements (see Section 7, Imaging Considerations)

10 USB Security

PCoIP Technology provides granular security over USB devices. This allows authorizing or deauthorizing (blocking) USB devices.

USB security is applied in the following priority order:

1. Unauthorized Vendor ID/Product ID (highest priority)
2. Authorized Vendor ID/Product ID
3. Unauthorized Device Class/Sub Class/ Protocol
4. Authorized Device Class/Sub Class/Protocol (lowest priority)

The sections below show three USB security examples:

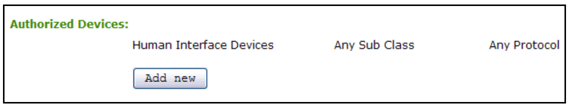
- Authorizing USB device by Class
- Authorizing USB device by Vendor ID and Product ID
- Deauthorizing (Blocking) a USB device by Class

Example: Authorizing USB Device by Class

This example shows authorizing a class of devices: printers.

1. In the Administrative Web Interface's *USB* menu choose the *Authorization* webpage, and select the *Add new* button.

Figure 10-1: Add New Button



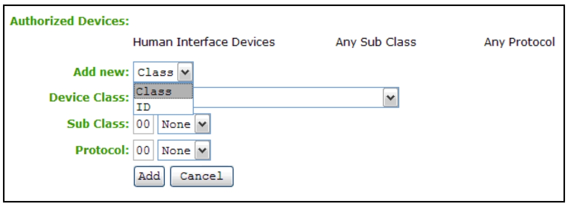
Authorized Devices:

Human Interface Devices | Any Sub Class | Any Protocol

Add new

2. In the drop-down list that appears, select *Class*.

Figure 10-2: Selecting Class



Authorized Devices:

Human Interface Devices | Any Sub Class | Any Protocol

Add new: Class

Device Class: Class / ID

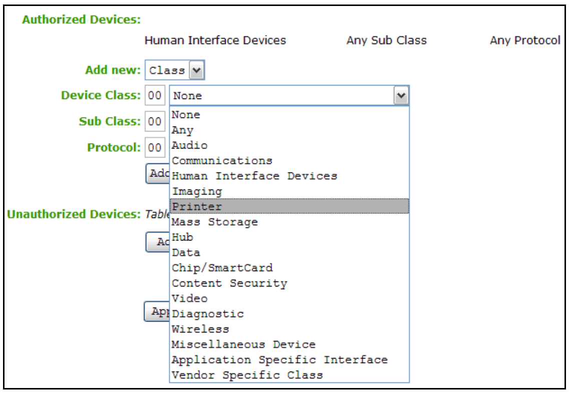
Sub Class: 00 None

Protocol: 00 None

Add | Cancel

3. Next the *Device Class* must be selected; select *Printer*.

Figure 10-3: Selecting Printer



Authorized Devices:

Human Interface Devices | Any Sub Class | Any Protocol

Add new: Class

Device Class: 00 None

Sub Class: 00

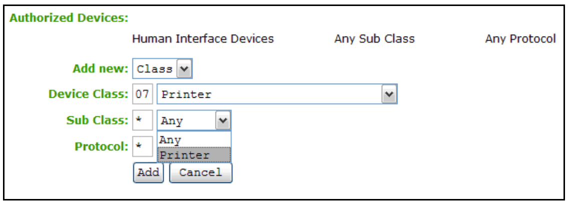
Protocol: 00

Unauthorized Devices: Table

None
Any
Audio
Communications
Human Interface Devices
Imaging
Printer
Mass Storage
Hub
Data
Chip/SmartCard
Content Security
Video
Diagnostic
Wireless
Miscellaneous Device
Application Specific Interface
Vendor Specific Class

4. To authorize all USB printers, leave the *Sub Class* and *Protocol* settings at *Any*. But in this example, only printers that support a specific protocol are authorized, so under *Sub Class*, select *Printer*.

Figure 10-4: Selecting Sub Class



Authorized Devices:

Human Interface Devices | Any Sub Class | Any Protocol

Add new: Class

Device Class: 07 Printer

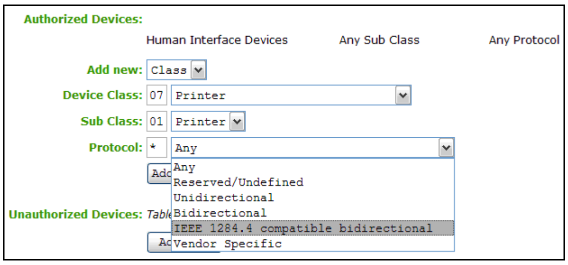
Sub Class: * Any

Protocol: * Any / Printer

Add | Cancel

5. Select the protocol: *IEEE 1284.4 compatible bidirectional.*

Figure 10-5: Selecting the Protocol



Authorized Devices:

Human Interface Devices | Any Sub Class | Any Protocol

Add new: Class

Device Class: 07 Printer

Sub Class: 01 Printer

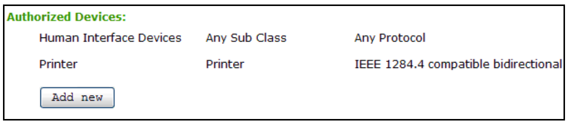
Protocol: * Any

Unauthorized Devices: Table

Any
Reserved/Undefined
Unidirectional
Bidirectional
IEEE 1284.4 compatible bidirectional
Vendor Specific

6. Click the *Add* button, and then click the *Apply* button to save changes.

Figure 10-6: Printer Class Authorized



Authorized Devices:

Human Interface Devices	Any Sub Class	Any Protocol
Printer	Printer	IEEE 1284.4 compatible bidirectional

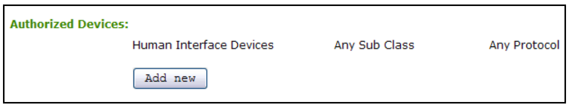
Add new

Example: Authorizing USB Device by Vendor ID and Product ID

This example demonstrates authorizing USB mass-storage devices with a particular Vendor and Product ID.

1. In the *Authorization* section, click the *Add New* button.

Figure 10-7: Add New Button

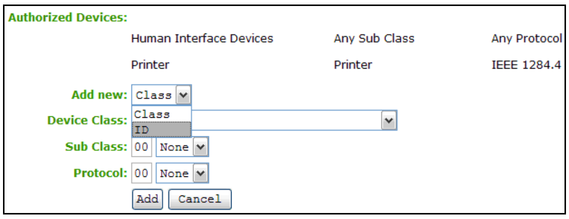


Authorized Devices:

Human Interface Devices	Any Sub Class	Any Protocol

2. In the drop-down list that appears, select *ID*.

Figure 10-8: Selecting ID



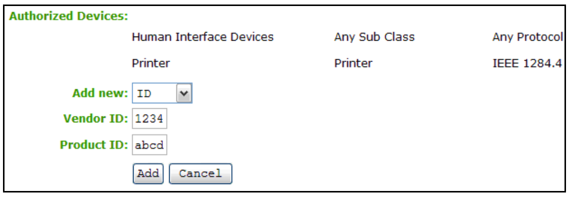
Authorized Devices:

Human Interface Devices	Any Sub Class	Any Protocol
Printer	Printer	IEEE 1284.4

Add new: Class
Device Class:
Sub Class: 00 None
Protocol: 00 None

3. In the text boxes, enter the USB device's Vendor ID and Product ID.

Figure 10-9: Entering Vendor and Product IDs



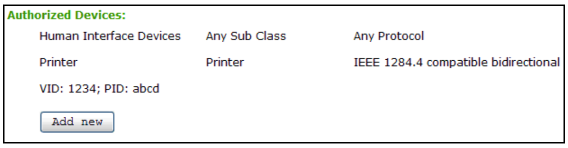
Authorized Devices:

Human Interface Devices	Any Sub Class	Any Protocol
Printer	Printer	IEEE 1284.4

Add new: ID
Vendor ID: 1234
Product ID: abcd

4. Click the *Add* button to add the changes, then the *Apply* button to save changes.

Figure 10-10: Vendor ID and Product ID Authorized



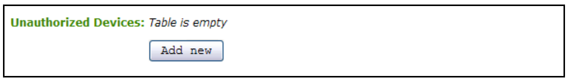
Authorized Devices:

Human Interface Devices	Any Sub Class	Any Protocol
Printer	Printer	IEEE 1284.4 compatible bidirectional
VID: 1234; PID: abcd		

Example: Deauthorizing (Blocking) a USB Device by Class

1. In the *Deauthorization* section, click the *Add New* button.

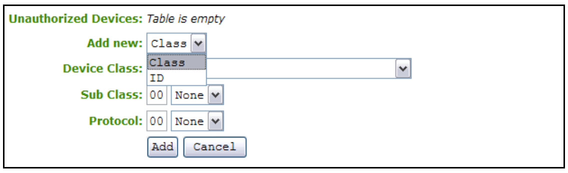
Figure 10-11: Add New Button



Unauthorized Devices: *Table is empty*

2. In the drop-down list that appears, select *Class*.

Figure 10-12: Selecting Class

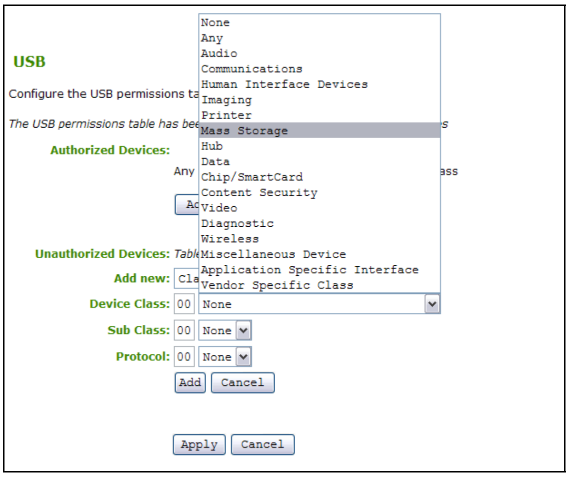


Unauthorized Devices: *Table is empty*

Add new: Class
Device Class:
Sub Class: 00 None
Protocol: 00 None

3. In *Device Class*, select *Mass Storage*.

Figure 10-13: Selecting Mass Storage



USB

Configure the USB permissions ta

The USB permissions table has bee *s*

Authorized Devices:

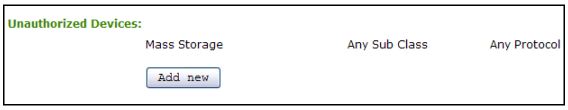
Any ass

Unauthorized Devices: *Tabl*

Add new: Cla
Device Class: 00 None
Sub Class: 00 None
Protocol: 00 None

4. Click the *Add* button to add the changes, then the *Apply* button to save changes.

Figure 10-14: Mass Storage Deauthorized



Unauthorized Devices:

Mass Storage	Any Sub Class	Any Protocol

Definitions

3D	Three-dimensional
CAD	Computer Aided Design
CMS	Connection Management Server − an external third-party management tool that used to manage PCoIP Hosts and Portals
DA	Directory Agent
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS-SRV	Domain Name System Service Record
fps	Frames Per Second − the display update rate
FQDN	Fully Qualified Domain Name
HTML	HyperText Markup Language
IPsec-ESP	Internet Protocol security-Encapsulated Security Payload
IP	Internet Protocol
IPv4	Internet Protocol version 4 − the most common protocol on the Internet
MAC	Media Access Control, i.e. MAC address − a unique hardware ID number
MIB	Management Information Base (used by SNMP)
MTU	Maximum Transmission Unit
NAT	Network Address Translation
OS	Operating System
OSD	On-Screen Display – Portal screen interface (when not in a PCoIP Session)
PC-over-IP®	Personal Computer over Internet Protocol Technology
PCoIP®	An abbreviation of “PC-over-IP”
PCoIP Host	Host side of a PCoIP System
PCoIP Portal	Portal (client) side of a PCoIP System
PCoIPMC	PCoIP Management Console
RDP	Remote Desktop Protocol
RFC	Request for Comments − Internet standards documents
SA	Service Agent
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol − used to monitor network devices
SSL	Secure Socket Layer − a security protocol
Teradici	Teradici Corporation, the provider of PCoIP processors
TERA1100	Teradici PCoIP Portal (client) processor
TERA1200	Teradici PCoIP Host processor
UA	User Agent
VPN	Virtual Private Network
WAN	Wide Area Network − an extended corporate network

References

1. TER0606004, PC-over-IP Administrative Interface User Manual Issue 3, May 2008
2. TER0806011, PCoIP Management Console Quick Start Guide Issue 1, July 2008