swisslog
healthcare

Technical Documents Library | 201935 | PN 9911622 Rev T | ECN 100188

SWISSLOG HEALTHCARE

Swisslog Pneumatic Tube System Network Communications Deployment Guide

The Swisslog Pneumatic Tube System is provided as-is, without any guarantees or warranty. In association with the product, Swisslog makes no warranties—either express or implied—of any kind, including but not limited to warranties of merchantability, fitness for a particular purpose, of title, or of non-infringement of third-party rights. Use of the product is at the user's risk.

Contents

CHAPTER 1

Network Integration

Requirements for integrating the tube system into a site network

This document provides IT administrators, network administrators and server administrators with the network and communications requirements and specifications required to implement a Swisslog Pneumatic Tube System (PTS) running Nexus™ Software on an established or planned site network.

The Pneumatic Tube System environment

The PTS consists of one System Control Center (SCC) computer/server, transmission devices, piping and optional remote client computers. The SCC software controls and monitors the various transmission devices in the tube system through the site's local area network or through dedicated serial communication lines in the case of legacy installations.

Client/server architecture

The SCC software uses a client-server architecture that communicates through a TCP/IP connection (socket). The client program is written in Java and runs in a Java virtual machine. This environment is installed entirely within the Swisslog folder structure and does not use or alter any other Java installations present on the host PC.

The server application is Windows®-based and runs in its own application window (hidden by default). The SCC primary computer hosts the server portion of the software and also typically hosts a single client.

Remote clients

Additional clients (remote clients) may connect to the server through the network. Remote clients must run a supported operating system as listed in "Remote client specifications" on page 16.

> Three remote client connections are supported and included with an initial Nexus license and three additional clients may be licensed for a total of six remote clients.

Communication protocols

Tube system devices communicate with the SCC via Ethernet lines, serial lines or a mixture of the two. Limitations apply to virtual machines, see "Virtual Server Specifications and Administration" on page 19.

> All systems upgrading to Nexus Software require communication line validation not limited to the following:
>
> - all communication line connection points are in good condition and fully seated,
> - junction boxes at tube system devices are in good condition and wired correctly,
> - Swisslog-approved wire and cabling is present throughout the system and
> - Communication Interface Assemblies are re-wired with fresh splices from lines at connectors.

User Datagram Protocol

Over Ethernet, the tube system uses UDP messaging; its low bandwidth requirements permit existing site networks to host the tube system with little or no impact to other network devices. UDP does not have its own error checking or require a communication handshake before transmitting messages. The SCC monitors whether each device is active on the network, so it does not need a protocol with error checking. The SCC pings each device, and once it receives a reply the SCC is assured that it is sending data to the correct device and proceeds with the actual data transmission.

Serial communication

Over serial lines, RS-422/485 signals are converted to RS-232 by a Communication Interface Assembly (CIA) at which point the DeviceMaster converts them to a User Datagram Protocol (UDP) signal to interface with the SCC.

The Pneumatic Tube System on the network

The diagrams in this section illustrate tube system connections to a network.

> Messaging between the server and the tube system devices must occur over a LAN. UDP messaging quality degrades when passed through a WAN or ISP and can cause tube system communication outages.
>
> **Off-site data centers are not currently supported. Hosts must be physically located in the hospital.**

100% Ethernet devices

A tube system consisting of devices communicating solely over Ethernet requires a primary SCC on the facility's network as shown in Figure 1.

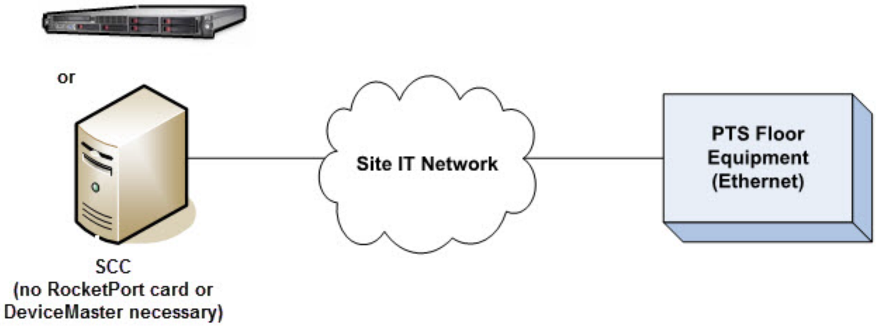


FIGURE 1. *100% Ethernet devices*

Mixed serial and Ethernet communications

A system with devices using a combination of serial and Ethernet is configured as shown in Figure 2.

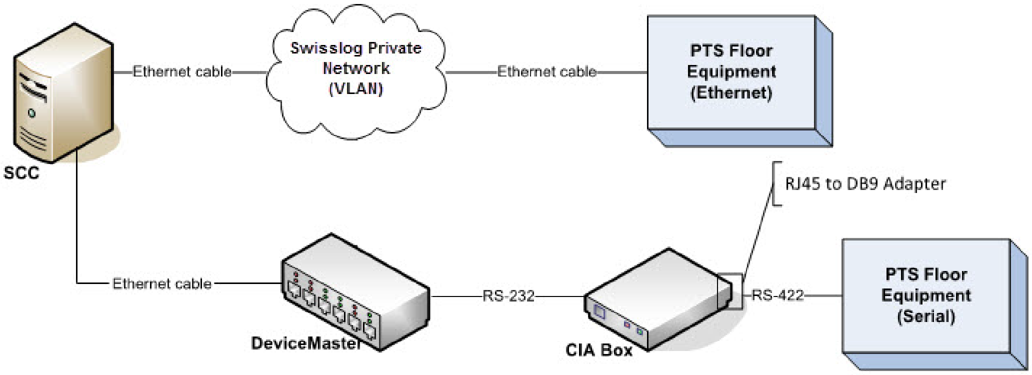


FIGURE 2. *Mixed serial and Ethernet devices*

100% serial devices

For new installations, a DeviceMaster is installed near the primary SCC and Communication Interface Assemblies (CIAs).

When migrating an existing system from serial communications to Ethernet communications, devices can be configured as described above or in one of these options:

- Option 1: Leave the CIAs and serial communications lines in place, install the appropriate DeviceMaster at the existing CIAs and run a dedicated Ethernet line to the SCC.
- Option 2: Leave the CIAs and serial communications lines in place, install the appropriate DeviceMaster near the SCC. Install the appropriate length RS-232 cables between the CIAs and DeviceMaster.

Figure 3 shows a system with serial devices connected to the SCC.

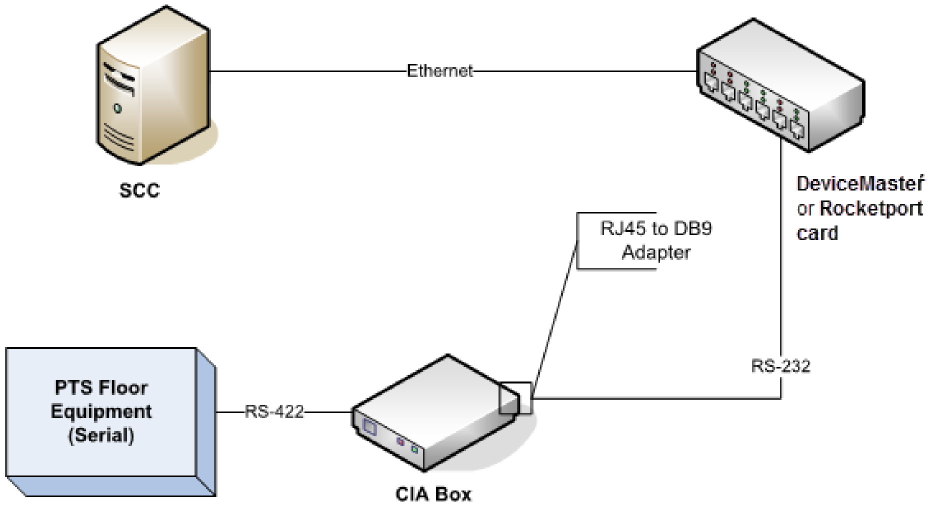


FIGURE 3. *100% serial devices*

100% serial devices with fiber optic lines

When there is a long distance from the SCC to the tube system, the CIAs and DeviceMaster are installed near the tube system floor devices. Fiber optic cable is routed from the Ethernet-to-Fiber Converter at the DeviceMaster to the SCC. The fiber optic cable is converted back to Ethernet for the connection to the SCC. See Figure 4.

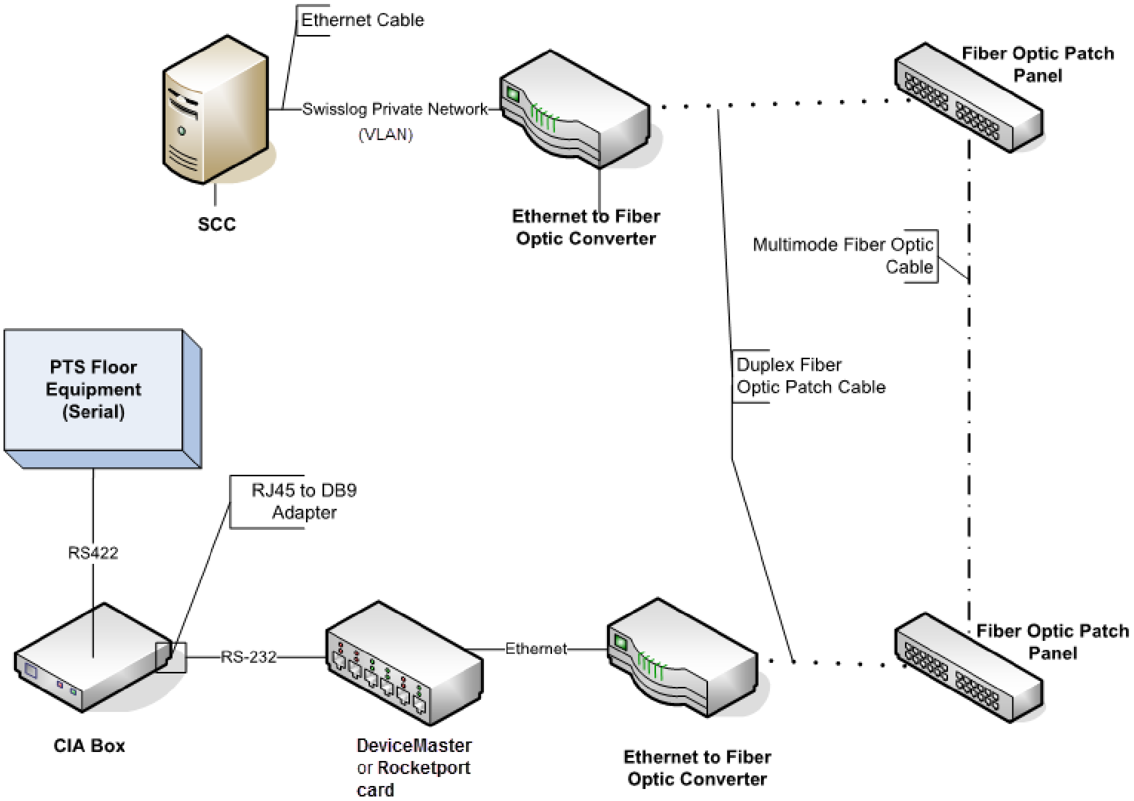

Ethernet Cable
Swisslog Private Network
(VLAN)
SCC
Ethernet to Fiber Optic Converter
Fiber Optic Patch Panel
Multimode Fiber Optic Cable
Duplex Fiber Optic Patch Cable
PTS Floor Equipment (Serial)
RJ45 to DB9 Adapter
RS422
RS-232
Ethernet
CIA Box
DeviceMaster or Rocketport card
Ethernet to Fiber Optic Converter
Fiber Optic Patch Panel

FIGURE 4. *100% serial devices with fiber optic lines*

CHAPTER 2

Network Configuration Requirements

Specifications for the dedicated tube system network space

This chapter addresses specifications and requirements for the following:

- VLAN Specifications
- Network security
- Remote access requirements

VLAN Specifications

The site IT network hosts the services used by PTS equipment. Cable maintenance and network troubleshooting are owned by the site IT department.

Segmenting

A segregated virtual local area network (VLAN) dedicated to the tube system is required to isolate tube system traffic, allow for proper packet handling and provide reliable system operation.

> ! Multiple VLANs are acceptable, but must be segregated for Swisslog use only. There is no restriction on the subnets used, but routing must be configured to allow all devices to communicate with the SCC across the Swisslog VLAN.

Adhere to the setup requirements in Table 1 for VLANs hosting PTS components.

TABLE 1. VLAN Setup Requirements

Name	Setting
VLAN Interfaces	The VLAN interface must remain open. Shutdown must not be enabled.
Dynamic ARP Inspections	Exclude VLANs from dynamic ARP inspection.
Broadcast Suppression	Set broadcast suppression (if enabled) to 100%.
Spanning Tree	Enable PortFast to open ports used by the SCC and prevent latency issues.
Protected Ports	Ensure switch port protected mode is not active on any ports connected to the SCC or tube system equipment.
VLAN Pruning	Ensure no switches are pruning the VLAN of any PTS component.

IP addressing

Each device on the network requires a unique IP address provided by the site network administration team. The IT department may provide a range of IP addresses to be used by the Swisslog setup team to address devices or may provide a list of IP addresses assigned to specific ports/closets.

The IP Address range should consider future expansion and a minimum of two extra IP addresses for troubleshooting purposes. The site can choose to define which device is assigned to each IP address, but the decision should be made prior to tube system startup.

When a cold backup solution is established, routing rules must allow the backup computer to communicate with tube system floor equipment over a dedicated Swisslog VLAN.

> Domain Name System (DNS) is not currently supported for Swisslog floor devices.
>
> For networks with MAC address restrictions enabled, the network administrator will have to statically map each device’s MAC address to the Ethernet port.
>
> Static IP addressing is currently the only supported method of addressing for Swisslog devices.

Latency

Maximum round-trip network latency **cannot exceed 100 milliseconds at any time during system operation**. Interruptions in excess of this threshold, such as those caused by Spanning Tree Protocol without PortFast enabled are not tolerated.

Internet connection

A high-speed internet connection at the primary SCC is required for software licensing and remote technical support. See "Windows firewalls" and“White list sites” on page 10 for license server access requirements.

> The SCC is the only tube system device requiring direct internet access. Remote clients do not require an internet connection.

FTP service

File Transfer Protocol (FTP) is used only within the local area network and does not connect to the internet. FTP provides fast firmware downloads to Nexus Stations (it is not used for Nexus Control Panels installed on non-Nexus Stations). This feature requires access to the FTP service in Windows Internet Information Services. This requirement applies to all approved operating systems and physical servers. See “Windows firewalls” on page 10 for inbound and outbound port rules.

Network security

Most, if not all, site networks have access to the internet and/or outside networks that increase the possibility of a security breach or virus. Because the SCC has internet and network access, it should be provided with appropriate virus and security protection that falls within the requirements specified in this section. The rest of the system is not vulnerable to attacks because the equipment uses a language that only the SCC can understand, thereby eliminating any network security concerns for the other PTS devices.

Cisco® Identity Services Engine (ISE) is not currently supported by Swisslog Healthcare floor devices.

Antivirus and malware detection

In antivirus software programs, disable the option ‘Heuristic Check for suspicious files’.

For active virus scanning, exclude the following directories and their subdirectories:

- C:\Swisslog
- C:\Program Files\Swisslog
- C:\Program Files\PostgreSQL

For in-memory scanning, exclude the following processes:

- C:\Swisslog\CTS\Server\sl-ctssrvr.exe
- C:\Program Files\PostgreSQL\bin\
  - pg_ctl.exe
  - postgres.exe
- C:\Swisslog\RsmSender\RsmSender.exe
- C:\Swisslog\jre\bin\
  - sl-appmgrclient.exe
  - sl-applmgrsrvr.exe
  - sl-arbitrator.exe
  - sl-blowerUnitTest.exe
  - sl-client.exe
  - sl-cxupdate.exe
  - sl-datapak.exe
  - sl-esp.exe
  - sl-espserver.exe
  - sl-gci.exe
  - sl-gcicontrol.exe
  - sl-mediator.exe
  - sl-mm.exe
  - sl-monitor.exe
  - sl-overwatch.exe
  - sl-td.exe
  - sl-tm.exe
  - sl-upsclient.exe
  - sl-upsmediator.exe
  - sl-zm.exe

Windows firewalls

Firewalls are acceptable with the following inbound and outbound port rules set up to allow internal network connections from the ports listed below.

TCP/IP	20	21 (Nexus Stations only)			80*	139	443
	1024	1433	1434	1527	3389	4606	4607
	5000	5432	5555	5556	5557	5559	6000
	6100	6975	6976	7777	9995	9999	25322
	35723	3426-3431					
UDP	21 (Nexus Stations only)			137	8000	12345	7000-7999

*Use of port 80 is limited to Nexus Version 6 for licensing purposes. Newer versions access the licensing servers through the secured port 443.

White list sites

Swisslog licensing and remote system monitoring sites must be permanently white listed to allow daily license verification (Nexus version 7 and newer) and to avoid service interruptions.

Purpose	License server address
Nexus Version 6 license server	http://swlnalicensing.swisslog.com
Nexus Version 7 license server	https://na01.swisslog.com
Remote access	https://d4sd.swisslog.com

Proxy Servers

If proxy servers are in place, the Administrator user must be authenticated for http transfers.

Encryption

Drive and disk encryption are not supported due to their tendency to increase network latency and cause system communication errors. This includes products such as McAfee® Endpoint Encryption (formerly Safeboot® Device Encryption).

Network access control

Appliances that monitor network security (such as ForeScout™ CounterACT™) are not supported. These products interfere with PTS system network traffic and processes.

When on site, Swisslog technicians will require access to the data closet and access to network analysis tools within the VLAN for troubleshooting. These tools may include Wireshark, Fluke Network Analyzer and others.

Network scanning utilities

Port scans tend to be resource-intensive and may create bandwidth issues which can cause communication failures within the tube system and SCC. Omit ping sweeps and NMAP scans of any VLANs or IP ranges that support the PTS.

SMTP server access

For sites enabling Alert Messaging, the SCC must be able to authenticate against the site SMTP server.

Remote access requirements

When a site requests technical support, Swisslog uses Bomgar™, a web-based, SSL remote application from the Swisslog domain to gain access to the SCC. Site staff must approve one-time access to Swisslog, and when Swisslog disconnects the connection is permanently closed. Bomgar activity is logged for each user and archived by Swisslog for 90 days.

Other means of remote access (such as VPN and SecureLink®) by Swisslog Technical Support are not supported.

During a Bomgar session, Swisslog does not have access to information governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Refer to the Bomgar technical documentation at http://www.bomgar.com for HIPAA regulatory compliance and details regarding secure access

See "Windows firewalls" and “White list sites” on page 10 for security exceptions.

CHAPTER 3

Physical Server Specifications and Administration

Settings, policies and configuration for workstations and servers

This chapter addresses the PTS specifications for applications and policies used by server administrators. These specifications apply to both physical and virtual machines.

> ⓘ See "Virtual Server Specifications and Administration" on page 19 for additional settings applicable to virtualized environments.

Group policies

Exclude the Swisslog PTS system from hospital IT group policies or create a new group policy that excludes the SCC from taking any downloads or updates. Do not override the SCC settings with the facility's domain policies.

Windows updates and patches

Swisslog does not perform compatibility testing on Microsoft patches or updates. The site IT group is responsible for implementing Windows security updates during a scheduled PTS shutdown period to avoid computer automatic shutdown; the SCC requires a manual restart to bring the system back to an operational state.

> ⓘ Turn off Windows automatic updates.

Disk memory management

These services, such as HP® Process Resource Manager, are not supported.

System Center Configuration Manager

Nexus Software cannot be distributed through Microsoft® System Center Configuration Manager (SCCM). SCCM can be used to manage Windows updates to the SCC with automatic reboots disabled. When a restart is required after an update the Nexus Software must be shut down, and then the computer can be manually restarted.

Server and software redundancy

High availability is not currently supported. Swisslog recommends a cold backup solution to minimize downtime in the event of a hardware failure.

PC and operating system configuration

This section addresses:

- User accounts and permissions
- Power management
- Windows indexing
- Fast user switching

User accounts and permissions

All SCC user accounts must have full read and write access to the C:\Swisslog folder for Nexus to run. This means a local administrator account or domain account with local administrator privileges must be set up and active on the SCC. Everything the PTS software executes must be run as the Administrator on the machine.

> Do not limit the read and write ability to the C:\ drive. Programs such as Datapak must have the ability to create and update files to the C:\ drive, even if those files are 'read only' by users accessing them.

Power management

In the Windows Control Panel, set the power plan for the computer running the SCC to:

- Never put the computer to sleep on all conditions
- Turn off all hibernate capability

Windows indexing

The Windows built-in indexing and search capabilities interfere with the CPU and Nexus software performance on the SCC. This issue affects Windows 7 operating systems. Disable the Windows search and indexing service(s) through the Services window.

Fast user switching

Disable this feature on the primary SCC and all remote computers.

Hardware specifications

This section provides the server-class machine and workstation requirements for Nexus software.

> Off-site data centers are not currently supported. Hosts must be physically located in the hospital.

Server-class machines and workstations

The following are minimum specifications.

Case	● Rack mount ● Tower chassis (workstation)
Memory	32 GB RAM
Available space	250 GB available hard drive space residing on a single partition
Processor	● 2.6 GHz Intel®-compatible 2-4 core processor (server-class)* ● 2.6 GHz Intel Core™ i7 processor (workstation)* *Celeron® models not acceptable, Xeon® models recommended
Operating systems	● Windows 7 Professional, Enterprise and Ultimate (all 64-bit) ● Windows Server 2012 and 2012 R2 (Standard and Datacenter) ● Windows Server 2016 (Standard and Datacenter)
Software frameworks requirements	.Net 3.5.1 and .Net 4.5 installed and enabled
Network adapters	Two (10/100 mbps)
Communication equipment	A DeviceMaster or a RocketPort multi-serial port card is required when PTS devices use serial communication.
PCI slots	● Systems with PTS devices that use serial communication and RocketPort multi-serial port cards will need one available PCIe slot per RocketPort card. ● A 16-channel PCI slot is required for the graphics card if the card is not already on board.
Video card	128 MB RAM, 1024 x 768, 256 colors, DVI capable, non-integrated

Sound card	Required for workstation
Power requirements	Backup power supply (UPS) recommended.
Browser requirements	• Firefox, Chrome or Internet Explorer version 8 and newer (for Webhelp) • Adobe FlashPlayer is required for Webhelp.
Ports	Two USB ports
Miscellaneous hardware	• Keyboard • Optical Mouse • External speakers • UL Listed
Peripherals	Any additional peripherals must be UL Listed.

Remote client specifications

The following are minimum specifications.

Memory	2 GB RAM	
Drives	10 GB available hard drive space	
CPU	2.0 GHz Intel-compatible dual-core processor (Celeron models not acceptable)	
Operating systems	• Windows 7 Professional, Enterprise and Ultimate (all 64-bit) • Windows 10 Professional and Enterprise (all 64-bit) supported by Nexus Software version 7.2.0.6 and newer. • Windows Server 2008 and 2008 R2 (Standard, Datacenter and Enterprise) • Windows Server 2012 and 2012 R2 (Standard and Datacenter) • Windows Server 2016 (Standard and Datacenter)	
Video card	64 MB RAM, 1024 x 768, 256 colors, non-integrated	
Sound card	Required	
Miscellaneous hardware (UL listed)	• Keyboard, optical mouse • External speakers	• Cat 5 cable • 10/100 mbps

Remote clients are not supported in Citrix environments.

Monitor specifications

- 19 in. to 27 in. flat panel LCD
- DVI interface
- 16.7 million color display
- UL listed

Network devices

The network device requirements are listed in this section.

USB networking devices

USB network adapters, modems, routers and wireless devices are not permitted.

Network interface cards

Network Interface Cards (NICs) at the SCC (or ports of any hubs or switches that PTS equipment goes through) must be configured as follows:

- Full-duplex 10/100 mbps
- Auto negotiate
- Disable any power management options on the NIC, including the option to "Allow the computer to turn off this device to save power".
- Disable any auto-sleep/auto-power-save features

> ⓘ Set all access device ports to auto-negotiate speed and use full-duplex transmission.

Switches

Switches are used to connect remote client computers to the primary SCC; or to connect several Xpress Traffic Control Unit (TCU) controllers, stations, Transfer Units (TUs), manifolds, and blowers to a single Ethernet connection.

> ⓘ Set all access device ports to auto-negotiate speed and use full-duplex transmission.

Concealing network devices

Although rated for extreme conditions, switches, DeviceMasters and converters (extenders) should not be concealed as it may lead to inadequate airflow.

Cable requirements and specifications

Ethernet Cable must be installed following the IEEE Standard 802.3 for good cabling practices.

> Power over Ethernet (PoE) is not supported and may damage PTS equipment firmware. PoE must be turned off at the switch port.

TABLE 1. Ethernet Cable Specifications

Standard	100Base-T
Cable Type	5e or better
Cable Connector	RJ-45 using either T568A or T568B termination standard
Jack	• 10/100 RJ-45 jack • Connected to the switch • Location: inside station control panels and inside Transfer Units, Blowers and MTU/TCU Control Enclosures as shown in product data submittals. • Ethernet lines must be affixed with a label at the switch and at the jack. • Each jack must be active and tested for continuity
Combined Cable Length	Maximum 328 ft (100 m) from the System Control Center (or switch) to the last device (including connections). The communication data rate slows with longer cable lengths. Repeaters may be used to extended the cable length by an additional 328 ft (100 m). No more than two repeaters may be used on a single network.
Minimum Cable Length	Between devices is 8.2 ft (2.5 m)

Fiber optic cable

Fiber Optic Multiplexer (MUX) applications are not supported for new site implementation or configuration. However, if the site has an existing Fiber MUX configuration, a certified replacement solution is available. Contact Technical Support for details.

> The maximum fiber optic cable distance is 1.19 miles (1.9 km).

CHAPTER 4

Virtual Server Specifications and Administration

System configuration settings to support Nexus Installations on a virtual machine (VM)

Nexus Software version 7.x can be installed on virtual machines for sites that meet the requirements and specifications listed in this section provided that the response time, I/O latency, and similar performance considerations are met by the virtual host on a level at, or exceeding, the equivalent performance of a dedicated, physical hardware server (as specified in this document).

VM requirements and specifications

This section provides the minimum requirements a pneumatic tube system must meet to qualify for installation on a VM and VM specifications.

Requirements for VM installations

Software	• Nexus Software Version 7.x only • VMWare® virtualization software only • Remote System monitoring (RSM) is highly recommended, but not required. RSM minimizes risk in virtualized environments.
Communications protocol	Approved for systems that communicate over 100% Ethernet*. *A one-port DeviceMaster is required at each MTU and Exit TCU. Air-powered TCUs must communicate over Ethernet. Belt-driven TCUs are not supported on VMs.
File preservation	Incremental server backups that only copy data changed since the last backup are run during periods of low tube system usage to preserve system performance.
Server location	Off-site data centers are not currently supported. Hosts must be physically located in the hospital.
VM and network configuration	The site IT group adheres to the requirements, specifications and configuration procedures documented in this guide.
Remote support	Bomgar™ connectivity by Swisslog is required.

VM specifications

All the requirements of a physical server apply to virtual machines along with the items listed here.

Virtual server software	VMware vSphere® 6.x and newer with complete installation of the VMware Tools™ package.
Operating system	• Windows Server 2012, 2012 R2 and 2012 Datacenter* • Windows Server 2016 (Standard and Datacenter) *The latest Windows updates are required for all operating systems
Processor	2.8GHz Intel Xeon Dual Core
RAM	16GB (minimum)
Capacity	150GB (minimum)
Disk provisioning	Thick provision eager zeroed
Device drivers	Paravirtual SCSI controller
Adapter type	VMXNET3 Special configuration settings are required, see "Configure the network adapter" on page 22.
NTP server	Network Time Protocol servers must be identical to that of the switches on which Swisslog equipment resides.
Validation	Validate networking between the VM and known ICMP, such as gateway IP.
File preservation	Incremental server backups that only copy data changed since the last backup are run during periods of low tube system usage to preserve system performance.

Clients in a VM environment

Remote clients are compatible with VMs when they meet the requirements listed in “Remote client specifications” on page 16.

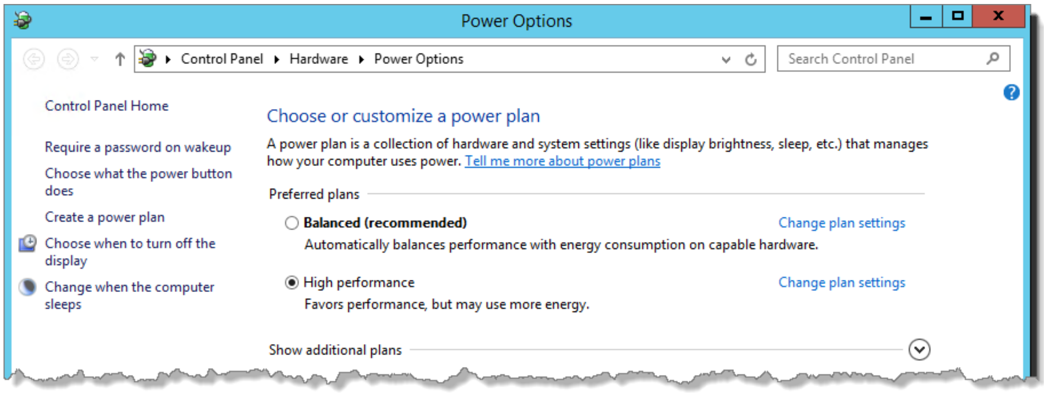
VM Administration

In addition to the network configuration and server administration requirements previously stated, the procedures provided in this chapter are required for VMs to ensure proper data flow and resolve incompatibilities between Windows NIC options and VMXNET3 drivers.

> Limitations apply. See “VM requirements and specifications” on page 19.

Configure power system settings

1. Click Windows Start and type `powercfg.cpl`.
2. Press **Enter**.
3. Select **High performance** on the Power Options window.


Power Options
Control Panel ▸ Hardware ▸ Power Options
Search Control Panel
Control Panel Home
Require a password on wakeup
Choose what the power button does
Create a power plan
Choose when to turn off the display
Change when the computer sleeps
Change plan settings
Change plan settings
Show additional plans

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

Preferred plans

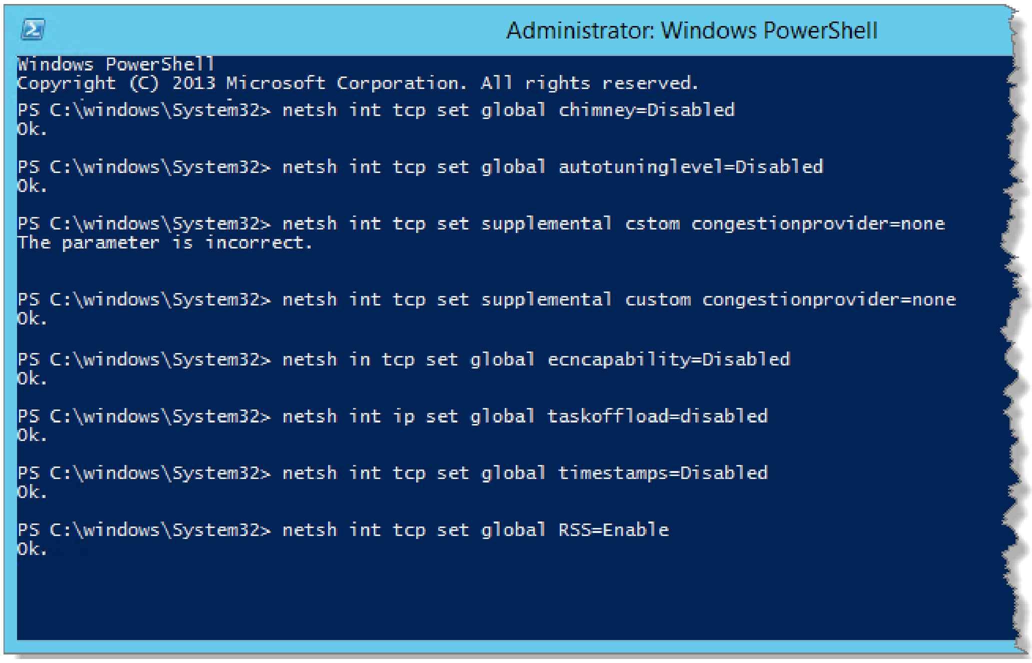
○ **Balanced (recommended)**
Automatically balances performance with energy consumption on capable hardware.

● High performance
Favors performance, but may use more energy.

Configure TCP/IP and UDP settings

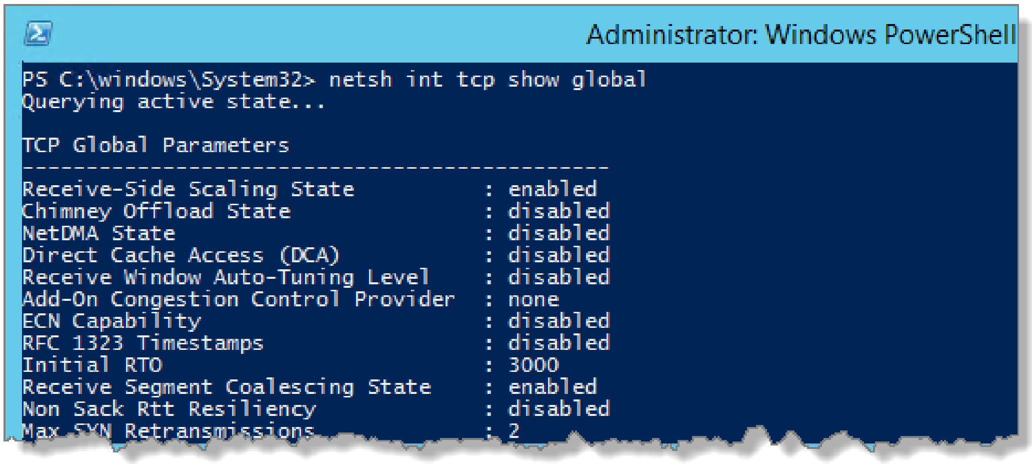
1. Open PowerShell.
2. Navigate to the system32 directory.
3. Enter the following commands to disable the specified settings:
   - `netsh int tcp set global chimney=Disabled`
   - `netsh int tcp set global autotuninglevel=Disabled`
   - `netsh int tcp set supplemental custom congestionprovider=none`
   - `netsh int tcp set global ecncapability=Disabled`
   - `netsh int ip set global taskoffload=disabled`
   - `netsh int tcp set global timestamps=Disabled`

4 Enable receive-side scaling with the command `netsh int tcp set global RSS=Enable`



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\windows\System32> netsh int tcp set global chimney=Disabled
Ok.

PS C:\windows\System32> netsh int tcp set global autotuninglevel=Disabled
Ok.

PS C:\windows\System32> netsh int tcp set supplemental cstom congestionprovider=none
The parameter is incorrect.


PS C:\windows\System32> netsh int tcp set supplemental custom congestionprovider=none
Ok.

PS C:\windows\System32> netsh in tcp set global ecncapability=Disabled
Ok.

PS C:\windows\System32> netsh int ip set global taskoffload=disabled
Ok.

PS C:\windows\System32> netsh int tcp set global timestamps=Disabled
Ok.

PS C:\windows\System32> netsh int tcp set global RSS=Enable
Ok.
```

5 Validate the settings with the command `netsh int tcp show global`



```
PS C:\windows\System32> netsh int tcp show global
Querying active state...

TCP Global Parameters
----------------------------------------------
Receive-Side Scaling State          : enabled
Chimney Offload State               : disabled
NetDMA State                        : disabled
Direct Cache Access (DCA)           : disabled
Receive Window Auto-Tuning Level    : disabled
Add-On Congestion Control Provider  : none
ECN Capability                      : disabled
RFC 1323 Timestamps                 : disabled
Initial RTO                         : 3000
Receive Segment Coalescing State    : enabled
Non Sack Rtt Resiliency             : disabled
Max SYN Retransmissions             : 2
```

6 Review the output to verify the settings were successfully applied.

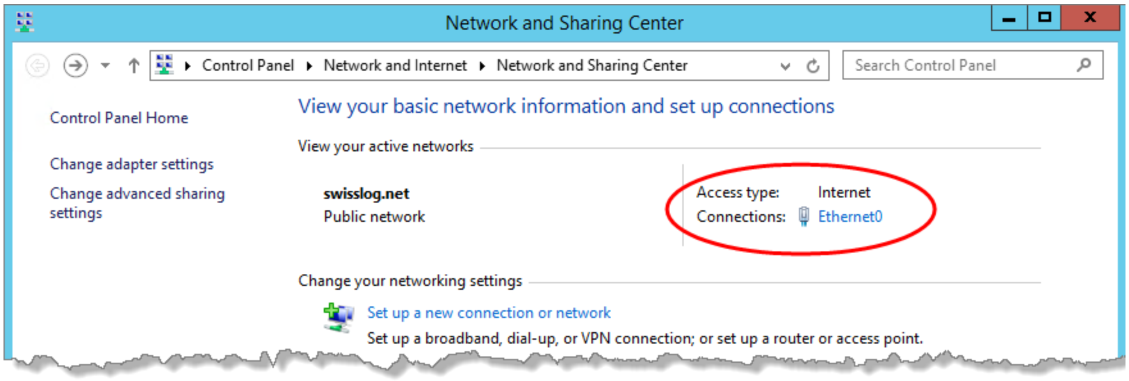
Configure the network adapter

Follow the procedures listed here to disable Internet Protocol version 6, power management and advanced properties for the network adapter.

Disable Internet Protocol version 6

1 Open the Network and Sharing Center.

2 Click the Ethernet connection.

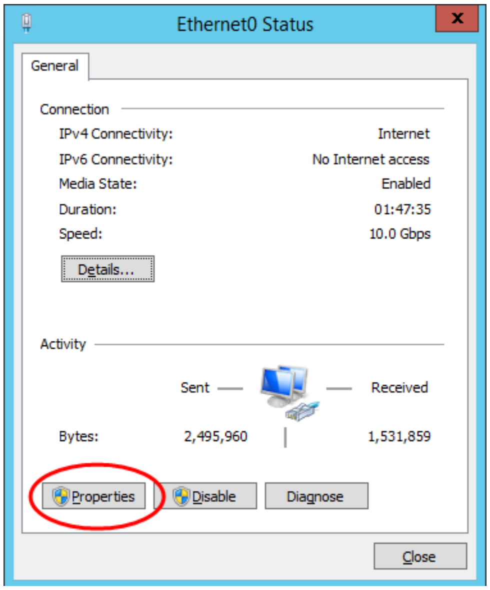

Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

swisslog.net
Public network

Access type: Internet
Connections: Ethernet0

The Ethernet Status window opens.

3 Click **Properties** on the Ethernet Status window.



Connection

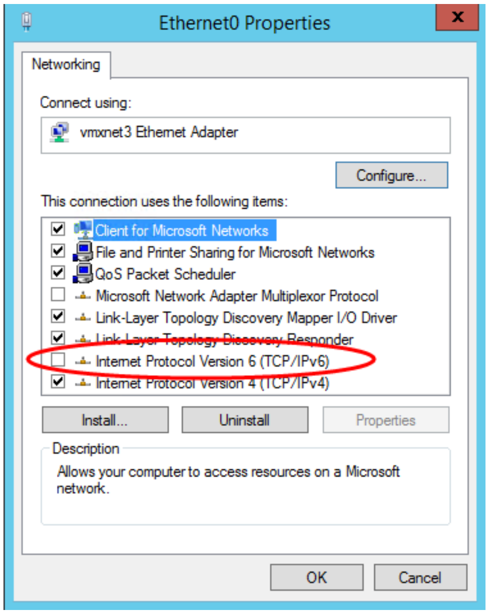
IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	01:47:35
Speed:	10.0 Gbps

Activity

	Sent	Received
Bytes:	2,495,960	1,531,859

The Ethernet Properties window opens.

4 Clear the **Internet Protocol Version 6 (TCP/IPv6)** option, and click **OK**.



Connect using:

vmxnet3 Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Allows your computer to access resources on a Microsoft network.

The Ethernet Properties window closes.

Disable power management

1 Click **Properties** on the Ethernet Status window.

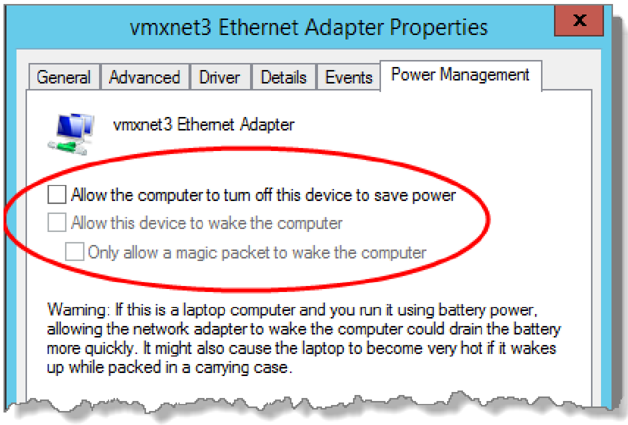
The Ethernet Properties window opens.

2 Click **Configure**.

The vmxnet3 Ethernet Adapter Properties window displays.

3 Click the **Power Management** tab.

4 Clear (de-select) all power options.



vmxnet3 Ethernet Adapter

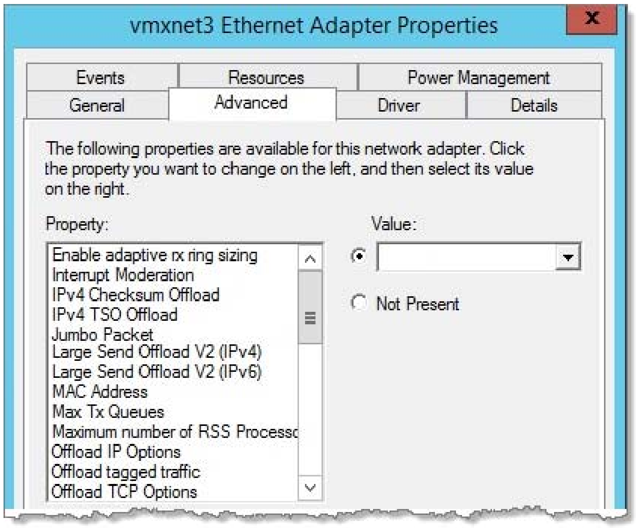
- ☐ Allow the computer to turn off this device to save power
- ☐ Allow this device to wake the computer
  - ☐ Only allow a magic packet to wake the computer

Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.

5 Click **OK**.

Modify the advanced settings

1 Click the **Advanced** tab on the vmxnet3 Ethernet Adapter Properties window.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

2 Individually select each property listed below, and change its value to **Disabled**.

- IPv4 Checksum Offload
- IPv4 TSO Offload
- Large Send Offload V2 (IPV4)
- Large Send Offload V2 (IPV6)
- Offload IP Options
- Offload tagged traffic
- Offload TCP Options
- Recv Segment Coalescing (IPV4)
- Recv Segment Coalescing (IPV6)
- TCP Checksum Offload (IPv4)
- TCP Checksum Offload (IPv6)
- UDP Checksum Offload (IPv4)
- UDP Checksum Offload (IPv6)

3 Click **OK**.

The Properties window closes.