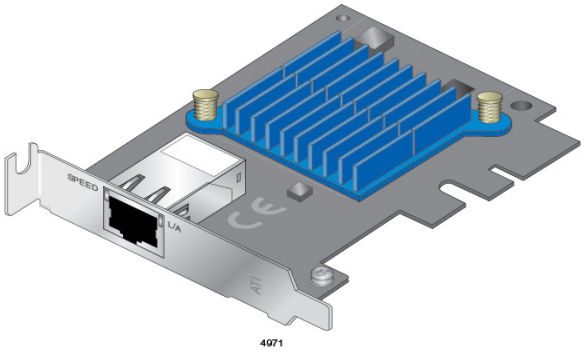
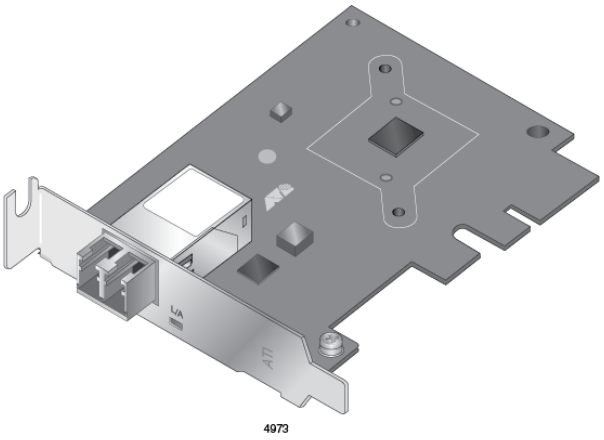
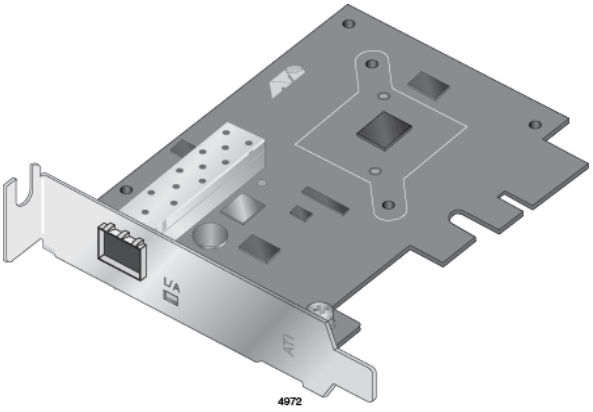
DNC10 Series

Single 10G Port Network Interface Cards with PCIe x4 Express Interface

- DNC10T
- DNC10LC
- DNC10SP







Installation and User's Guide

613-002857 Rev B

Electrical Safety and Emissions Standards

This product meets the following standards.

Federal Communications Commission Interference Statement

Declaration of Conformity

Manufacturer Name: Allied Telesis, Inc.

Declares that the product: **DNC10 Series 1 Port 10G Network Interface Card (w/PCI x4 Express Interface)**

Model Numbers: **DNC10LC, DNC10SP, and DNC10T**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device must not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

Industry Canada

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Restriction of the Use of Certain Hazardous Substances (RoHS) in Electrical and Electronic Equipment

This Allied Telesis RoHS-compliant product conforms to the European Union Restriction of the Use of Certain Hazardous Substances (RoHS) in Electrical and Electronic Equipment. Allied Telesis ensures RoHS conformance by requiring supplier Declarations of Conformity, monitoring incoming materials, and maintaining manufacturing process controls.

RFI Emissions	FCC Class B, EN55032 Class B, VCCI Class B, ICES-003 Issue 6
Immunity	EN55035
Electrical Safety	EN2368-1 (TUV), UL 62368-1 ($_{C}UL_{US}$)
 Laser Safety	EN60825

Translated Safety Statements

Important: Safety statements that have the ☞ symbol are translated into multiple languages in the *Translated Safety Statements* document at **www.alliedtelesis.com/library**.

Remarque: Les consignes de sécurité portant le symbole ☞ sont traduites dans plusieurs langues dans le document *Translated Safety Statements,* disponible à l'adresse **www.alliedtelesis.com/library**.

Contents

Tables

Figures

Preface

This guide contains instructions on how to install and configure the DNC10 Series adapters.

The Preface discusses the following topics:

This guide contains the installation instructions for the following single 10G port Network Interface Cards (NICs).

- ❒ DNC10SP
- ❒ DNC10LC
- ❒ DNC10T

Safety Symbols Used in this Document

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- Replacement Services - Submit an RMA request via our interactive support center.
- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, select your region and country, then go to **www.alliedtelesis.com/contact**.

Chapter 1
Introduction

This chapter provides an introduction to the DNC10 Series network interface cards (NICs) with Wake-on-LAN (WoL).

This chapter contains the following sections:

Functional Description

The DNC10 Series network adapters are 10 Gigabit Ethernet (10GbE) interface controllers that are based on the Aquantia AQC100 10GbE media access controller (MAC) with integrated serializer/deserializer (SerDes).

The Aquantia diagnostic tool can be used with the device to provide firmware programming and a first level of diagnostics and fault isolation.

These cards have Peripheral Component Interconnect Express (PCIe) bus connectors. The DNC10 Series network adapters support the PCIe x4 v3.0, 2.1 and 1.1a compliant interfaces.

The AT-DNC10 Series can perform accelerated Ethernet data networking and storage networking simultaneously for all popular protocols used in the data center, and includes features such as Data Center Bridging.

Enterprise networks that use multiple protocols and multiple network fabrics benefit from the ability of the network interface card (NIC) to combine data communications, storage, and clustering over a single Ethernet fabric and to boost server CPU performance and memory utilization while alleviating I/O bottlenecks.

Wake-on-LAN (WoL) is a protocol for remotely turning on a computer in a low power mode with a network message. A magic packet is a network message that a WoL-enabled computer receives and wakes up when the computer’s MAC address matches one in the magic packet.

As part of the company’s green range, the adapter is engineered to reduce power consumption. It incorporates centralized power management features that automatically place idle circuitry into a lower power mode to save energy.

The basic characteristics of the NICs are listed in Table 1.

Table 1. DNC10 Series Network Interface Cards

Adapter	Port	Speed	Cable Type	Maximum Distance	System Connection
DNC10SP	SFP+	10G/1G	Varies by SFP+ transceiver	Varies by SFP+ transceiver	PCIe x4 (Gen 3)
DNC10LC	Duplex LC	10G	OM1	33m	PCIe x4 (Gen 3)
			OM2	82m	
			OM3	300m	
			OM4	550m	
DNC10T	RJ45	10G	CAT6A	100m	PCIe x4 (Gen 3)
		5G/2.5G/ 1G/100M	CAT5e or CAT6A		

Note
The maximum operating distance of the SFP+ port on the DNC10SP adapter depends on the transceiver. Refer to the product's data sheet on the Allied Telesis web site for a list of supported transceivers.

After physically installing the DNC10 Series network adapter in your computer, install the driver software by referring to Chapter 3, "Installing the Driver Software" on page 41.

DNC10LC Fiber Optic Port

The DNC10LC adapter card has one 10Gbps fiber optic port with a duplex LC connector. The port has a maximum operating distance of 300m with OM3 fiber optic cable. The DNC10LC links at 10G only. It has one LED to show the networking state.

The DNC10LC has a PCIe x4 motherboard bus interface as shown in Figure 1.

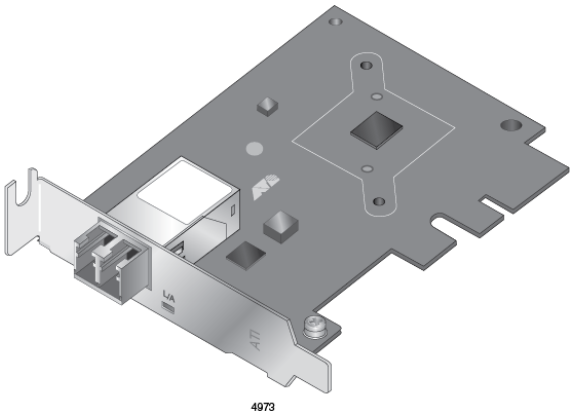


Figure 1. DNC10LC Adapter Card

The LC fiber optic adapter port is shown in Figure 2.

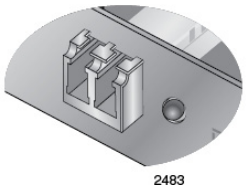


Figure 2. Duplex LC Connector on the DNC10LC Network Adapter

Table 2 describes the link states that the LED indicates.

Table 2. DNC10LC LED Status

Port LED	LED State	Description
L/A (Link/ Activity)	Solid Green	The port has established a link with a network device.
	Off	The port has not established a link with a network device.
	Flashing Green	The port is receiving or transmitting network packets.

DNC10SP SFP+ Port

The DNC10SP adapter has an SFP+ port where you can plug in an SFP+ transceiver to connect the adapter to a compatible link partner. The DNC10SP will detect whether a 10G SFP+ or 1G SFP has been inserted and will only operate at that speed. It has one LED to show the networking state.

You cannot change the speed or duplex mode of the transceiver port. The maximum operating distance of an SFP+ port will vary depending on the SFP+ transceiver and type of fiber optic cabling.

The port supports the following types of transceivers:

Note
See the Allied Telesis website for supported SFP models.

- 1Gbps SPSX and SPLX short and long distance SFP transceivers using multi-mode or single mode fiber optic cable.
- 10Gbps SP10SR and SP10LR SFP+ short and long distance SFP+ transceivers using multi-mode or single mode fiber optic cable.
- 10Gbps SP10BD series of bidirectional transceivers for single mode fiber optic cable with maximum operating distances of 10 to 40 kilometers.
- 10Gbps SP10TW series of direct connect twinax cables with SFP+ transceiver-style connectors, in lengths of 1, 3, and 7 meters.
- 10Gbps SP10T transceiver with RJ-45 connector for links up to 20 meters (depending on SFP) with Category 6a twisted pair cable, or 100 meters at 1Gbps.

Guidelines for the port are listed here:

- It does not support 100Mbps-FX transceivers.
- It supports full-duplex mode only.
- The adapter can set the speed automatically with Auto-Negotiation. The default is Auto-Negotiation.

The DNC10SP adapter has a PCIe x4 motherboard bus interface as shown in Figure 3.

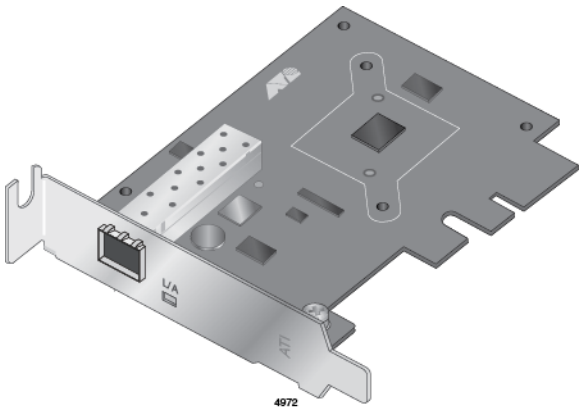


Figure 3. DNC10SP Adapter Card

Note
An SFP+ transceiver must be purchased separately. For a list of supported transceivers, refer to the product's data sheet on the Allied Telesis web site.

The SFP+ port is shown in Figure 4.

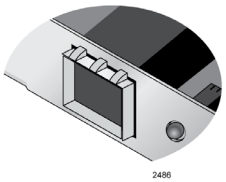


Figure 4. SFP+ Port on the DNC10SP Adapter

Table 2 describes the link states that the LED indicates.

Table 3. DNC10SP LED Status

Port LED	LED State	Description
L/A (Link/ Activity)	Solid Green	The port has established a link with a network device.
	Off	The port has not established a link with a network device.
	Flashing Green	The port is receiving or transmitting network packets.

DNC10T Twisted Pair Copper Port

The DNC10T adapter card has one copper port that can operate at 100Mbps or 1/2.5/5/10Gbps. The card uses Auto-Negotiation to automatically set port speed and supports full-duplex mode only. The port has two status LEDs.

The adapter has a PCIe x4 motherboard bus connector as shown in Figure 5.

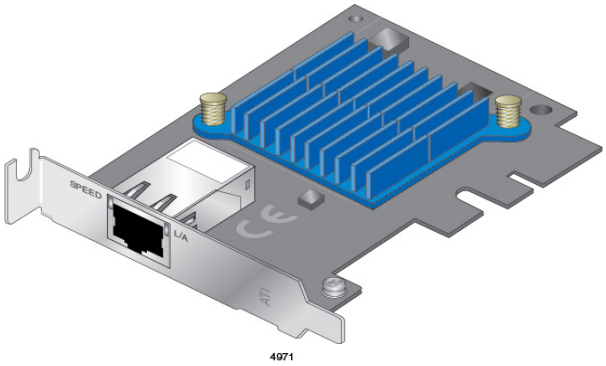


Figure 5. DNC10T Adapter Card

The twisted pair cable port is shown in Figure 6.

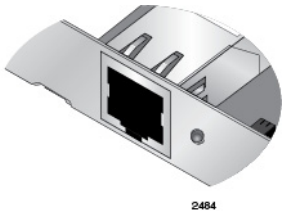


Figure 6. Twisted Pair Cable Port

The minimum cable requirements are listed here:

- 100Mbps - Standard TIA/EIA 568-A-compliant Category 5 twisted pair cabling
- 1/2.5/5Gbps - Standard TIA/EIA 568-B-compliant Category 5e twisted pair cabling
- 10Gbps - Standard TIA/EIA 568-C-compliant Category 6A twisted pair cabling

The port has a maximum operating distance of 100 meters (328 feet).

The LEDs for the twisted pair port are described in Table 4.

Table 4. DNC10T Link and Activity LEDs

Port LEDs	LED State	Network State
Left	Green Steady On	The transceiver has established a 10G link to a remote device.
	Amber Steady On	The transceiver has established a 100Mbps or 1/2.5/5G link to a remote device. The user will need to check connection properties in the OS to determine the actual link speed.
	Off	The port has not established a link.
Right	Green Steady On	The transceiver has established a link to a remote device.
	Green Blinking	The transceiver in the port is transmitting or receiving network traffic.
	Off	The port has not established a link.

Features

Here are the key features of the DNC10 Series network interface cards:

Hardware

- ❒ DNC10SP supports one SFP+ port
- ❒ DNC10LC supports one fiber optic port with a duplex LC connector port
- ❒ DNC10T supports one twisted pair port
- ❒ PCIe v3.0, 2.1, and 1.1a compliant
- ❒ TCP, IP, and UDP checksum
- ❒ Virtual LANs (VLANs) - 802.1q VLAN tagging
- ❒ Jumbo Frame support up to 16 KBytes
- ❒ Advanced Configuration and Power Interface (ACPI) power management compliant
- ❒ Low profile form factor
- ❒ RoHS compliant
- ❒ Preboot Execution Environment (PXE) v2.1
- ❒ Unified Extensible Firmware Interface (UEFI)
- ❒ Low profile and standard bracket
- ❒ Wake-on-LAN (WoL)
- ❒ Quality of Service (QoS) support up to eight traffic classes
- ❒ Data Center Bridging (DCB)

Software

- ❒ Windows 10, 64-bit
- ❒ Windows Server 2016
- ❒ Windows Server 2019
- ❒ Linux with kernel version 3.10 and higher

Chapter 2

Installing the Hardware

This chapter contains the following sections:

System Requirements

Before installing the DNC10 series network adapter, make sure your system meets the requirements listed below:

- Computer with one of the following operating systems installed:
  - Windows 10, 64-bit
  - Windows Server 2016
  - Windows Server 2019
  - Linux with kernel version 3.10 and higher
- One open PCIe x4 or larger slot

Reviewing Safety Precautions

Important: Safety statements that have the ✍ symbol are translated into multiple languages in the *Translated Safety Statements* document at **www.alliedtelesis.com/library**.

Remarque: Les consignes de sécurité portant le symbole ✍ sont traduites dans plusieurs langues dans le document *Translated Safety Statements,* disponible à l'adresse **www.alliedtelesis.com/library**.

Warning
Do not stare into the laser beam. ✍ **L2**

Warning
The fiber optic ports contain a Class 1 laser device. When the ports are disconnected, always cover them with the provided plug. Exposed ports may cause skin or eye damage. ✍ **L4**

Warning
Do not look directly at the fiber optic cable ends or inspect the cable ends with an optical lens. ✍ **L6**

Warning
Do not work on this equipment or cables during periods of lightning activity. ✍ **E2**

Warning
Operating Temperature: This product is designed for a maximum ambient temperature of 40 degrees C. ✍ **E7**

Note
All Countries: Install this product in accordance with local and National Electric Codes. ✍ **E8**

Warning

The module is being installed in a system that operates with voltages that can be lethal. Before you remove the cover of your system, you must observe the following precautions to protect yourself and to prevent damage to the system components.

– Remove any metallic objects or jewelry from your hands and wrists.

– Make sure to use only insulated or nonconducting tools.

– Verify that the system is powered OFF and unplugged before accessing internal components.

– Installation or removal of modules must be performed in a static-free environment. The use of a properly grounded wrist strap or other personal antistatic devices and an antistatic mat is strongly recommended. **E39**

Caution

Do not use excessive force when seating the card, as the force may damage the system or the adapter card. If the card resists seating, remove it from the system, realign it, and try again. **E47**

Pre-Installation Checklist

Before installing the DNC10 series network adapter, check the following list:

1. Check that your computer has an appropriate open PCIe slot.
2. Verify that your system is using the latest BIOS.
3. When you download the driver software from the Allied Telesis website, record the path to where the driver file resides on your system.
4. If your system is active, shut it down.
5. When system shutdown is complete, unplug your system.
6. Holding the adapter card by the edges, remove it from its shipping package and place it on an antistatic surface.
7. Check the adapter for visible signs of damage, particularly on the card's edge connector.

Note
Do not attempt to install any damaged adapter card. If the adapter card is damaged, report it to Allied Telesis. See "Contacting Allied Telesis" on page 15.

Replacing the Bracket

The DNC10 series network adapter is shipped with the low-profile bracket attached to the adapter. Additionally, a standard bracket is supplied also. Depending on your system, you may need to replace the bracket attached to your adapter card.

The following procedure describes how to remove the low-profile bracket from the network adapter and replace it with the standard bracket. You can also use this procedure to remove the standard bracket and replace it with the low-profile bracket.

To replace the low-profile bracket with the standard bracket, perform the following procedure:

1. Remove the screws that attach the bracket to the network adapter. See Figure 7.

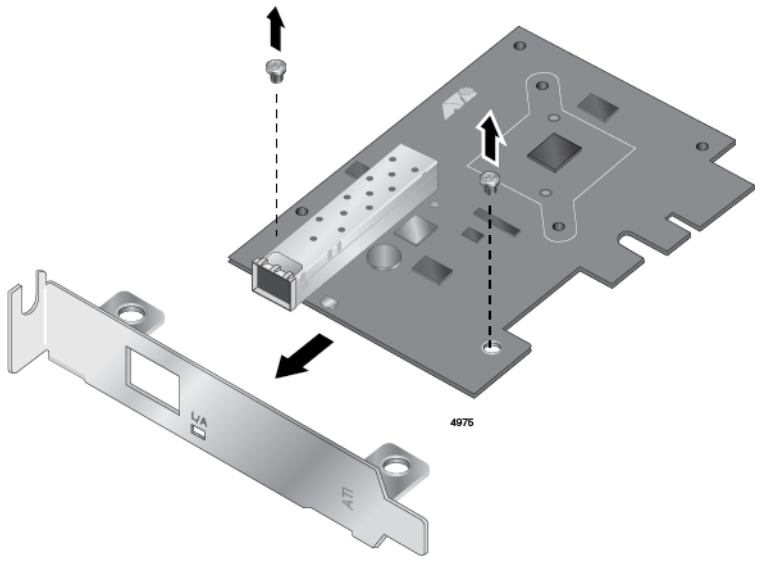


Figure 7. Removing the Low-Profile Bracket

2. Align the tabs of the standard bracket with the holes on the network adapter and fasten the screws onto the network adapter. See Figure 8 on page 33.

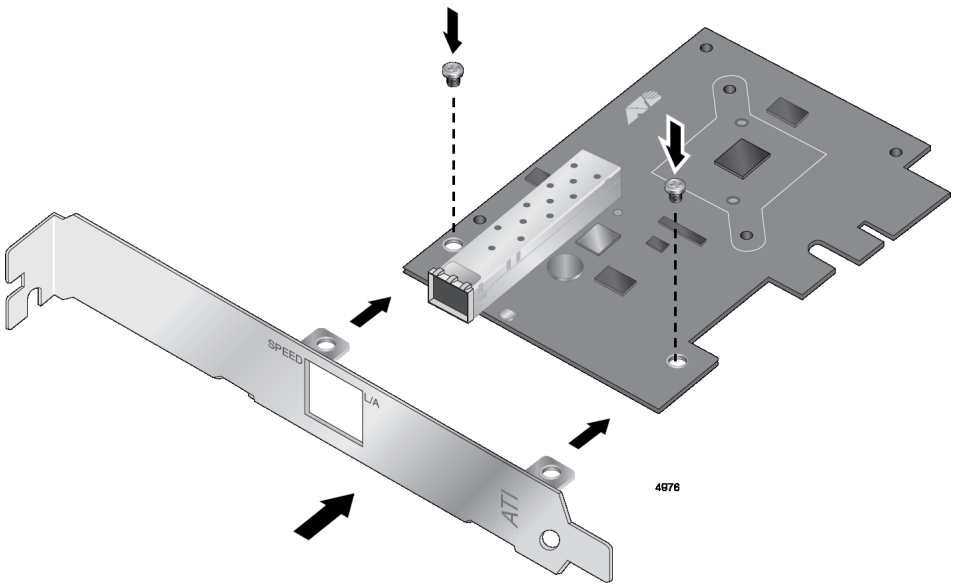


Figure 8. Fastening Screws onto Standard Bracket

Installing a Network Adapter

The following instructions apply to installing a DNC10 series network adapter in most systems. Refer to the manuals that were supplied with your system for details about performing these tasks on your particular system.

To install the network adapter, perform the following procedure:

1. Review the “Pre-Installation Checklist” on page 31 and “Reviewing Safety Precautions” on page 29.

   Before installing the network adapter, ensure the system power is OFF and unplugged from the power outlet, and that proper electrical grounding procedures have been followed.

   Warning
   The module is being installed in a system that operates with voltages that can be lethal. Before you remove the cover of your system, you must observe the following precautions to protect yourself and to prevent damage to the system components.

   – Remove any metallic objects or jewelry from your hands and wrists.

   – Make sure to use only insulated or nonconducting tools.

   – Verify that the system is powered OFF and unplugged before accessing internal components.

   – Installation or removal of modules must be performed in a static-free environment. The use of a properly grounded wrist strap or other personal antistatic devices and an antistatic mat is strongly recommended. E39

2. Remove the system cover and select any empty PCIe slot. See Figure 9 on page 35.

   If you do not know how to identify a PCIe x4 or larger slot, refer to your system documentation.

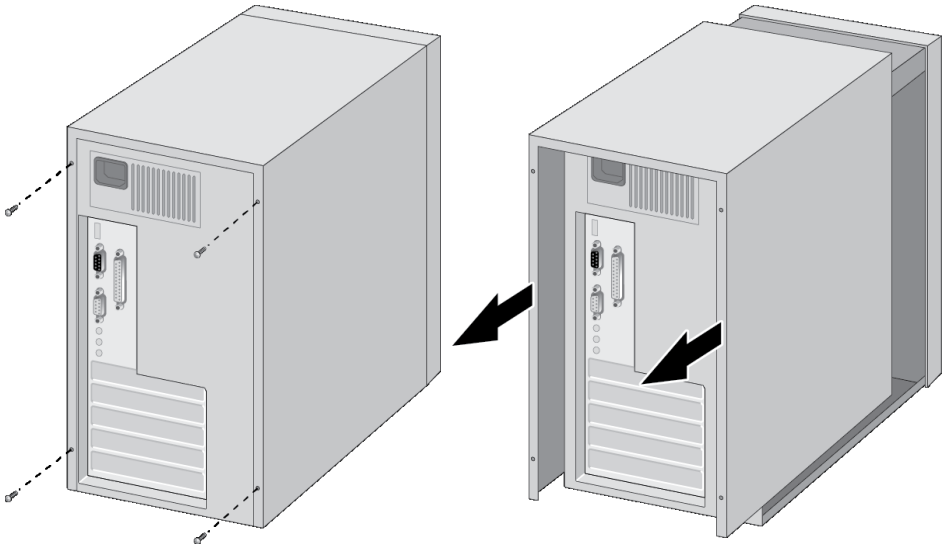


Figure 9. Removing the PC Cover

3. Select an empty, non-shared PCIe slot and remove the faceplate.

   Keep the faceplate in a safe place. You may need it for future use. See Figure 10.

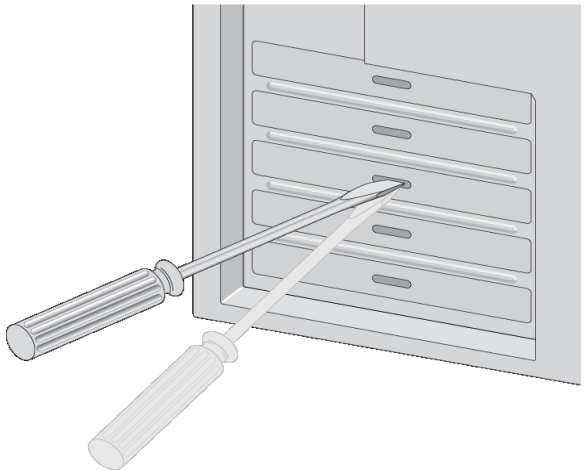


Figure 10. Removing the Faceplate From PCIe Slot

4. Remove the network adapter from the shipping package and store the packaging material in a safe location.

5. Applying even pressure at both corners of the network adapter, push the adapter until it is firmly seated in the PCIe slot.

   Make sure the adapter is securely seated. See Figure 11 on page 36.

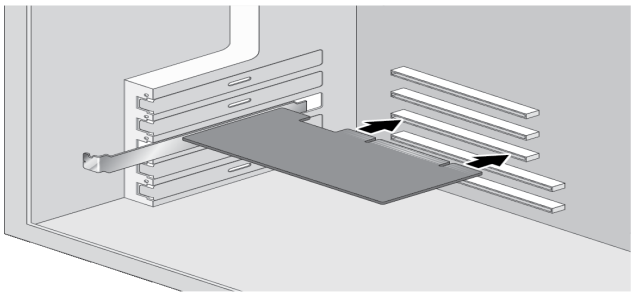


Figure 11. Inserting the Network Adapter

Caution

Do not use excessive force when seating the adapter, as the force may damage the system or the adapter. If the adapter resists seating, remove it from the system, realign it, and try again. E47

6. Secure the network adapter to the chassis with a Phillips-head screw (not provided) as shown in Figure 12.

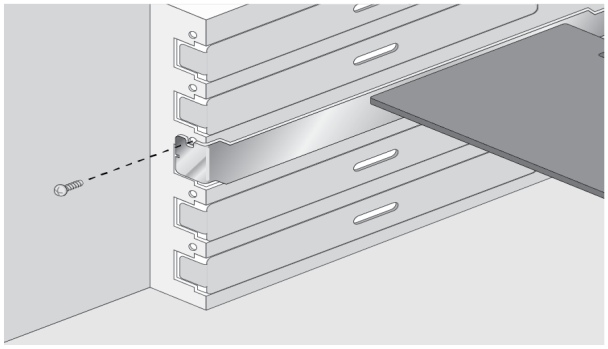


Figure 12. Securing the Network Adapter

7. Replace the system's cover and secure it with the screws removed in step 2.
8. Disconnect any personal antistatic devices.

9. Power the system on.

When the system returns to proper operation, the network adapter is fully installed. Next, connect the network cables. See "Connecting the Network Cable" on page 38.

Connecting the Network Cable

Depending on the type of DNC10 series network adapter installed, it is equipped with an SFP+, fiber optic, or copper RJ45 port. To connect the network adapter to the network, you must have a cable with the appropriate connector.

DNC10LC Fiber Optic Cable

To connect a fiber optic network cable to the duplex LC connector on the DNC10LC network adapter, perform the following procedure:

1. Prepare a fiber optic cable with an appropriate connector.

Warning
The fiber optic ports contain a Class 1 laser device. When the ports are disconnected, always cover them with the provided plug. Exposed ports may cause skin or eye damage. L4

2. Remove the dust cover from the duplex LC connector on the fiber optic port.
3. Connect one end of the cable to the network adapter.
4. Connect the other end of the cable to the fiber optic port on a remote network device.
5. Load the driver as described in Chapter 3, “Installing the Driver Software” on page 41.

DNC10SP SFP+ Transceiver

The network adapter requires an SFP+ transceiver and an appropriate cable to connect to the network.

1. Insert an SFP+ transceiver into the SFP+ port on the network adapter until the SFP+ transceiver snaps into place in the port.
2. Remove the dust cover from the SFP+ transceiver.
3. Connect one end of the cable to the SFP+ transceiver.
4. Connect the other end of the cable to the appropriate fiber optic port on a remote network device.
5. Load the driver as described in Chapter 3, “Installing the Driver Software” on page 41.

DNC10T Twisted-Pair Copper Cable

To connect a copper network cable to the network adapter, perform the following procedure.

1. Prepare a twisted-pair copper cable.
2. Connect one end of the cable to the network adapter.
3. Connect the other end of the cable to the appropriate port on a remote network device.
4. Load the driver as described in Chapter 3, "Installing the Driver Software" on page 41.

Chapter 3

Installing the Driver Software

This chapter describes how to install driver software for the DNC10 Series network adapter onto your operating system. It contains the following topics:

Overview

After you install the DNC10 Series network adapter on your computer, your next step is to install the driver software onto your Windows operating system. You can install the driver software using the Device Manager or the silent installation method.

When you install the driver software using the Device Manager, the dialog boxes guide you through the installation process. On the other hand, using the silent installation method, you can install software without constant interactions by suppressing dialog boxes.

Guidelines

Here are the guidelines for installing and updating the driver software on your operating system:

- ❒ To install or update the driver software, you must have administrative privileges.
- ❒ When you install the DNC10 Series network adapter on your computer and start the system, the system detects a new adapter and may install a default driver. In either case, you must update the driver software for the DNC10 Series network adapter. See “Installing the Driver Using the Device Manager”, or “Installing the Driver Using the Silent Installation Method”.

Installing the Driver Using the Device Manager

To install or update the driver software using the Device Manager, follow the steps below:

- ❒ “Downloading the Driver Software” on page 43
- ❒ “Accessing the Device Manager” on page 45
- ❒ “Installing the Driver Software” on page 47

  Or

- ❒ “Updating the Driver Software” on page 51

Installing the Driver Using the Silent Installation Method

To install or update the driver software using the silent installation, follow the steps below:

- ❒ “Downloading the Driver Software” on page 43
- ❒ “Performing the Silent Installation” on page 52

Downloading the Driver Software

The driver software for the adapters is available on the Allied Telesis website. The driver is the same for all DNC10 Series NICs.

To download the software:

1. Open a web browser, such as Internet Explorer or FireFox, on your computer and enter the following:

   http://www.alliedtelesis.com/support/software

   The Allied Telesis Software Download page is displayed as shown in Figure 13.

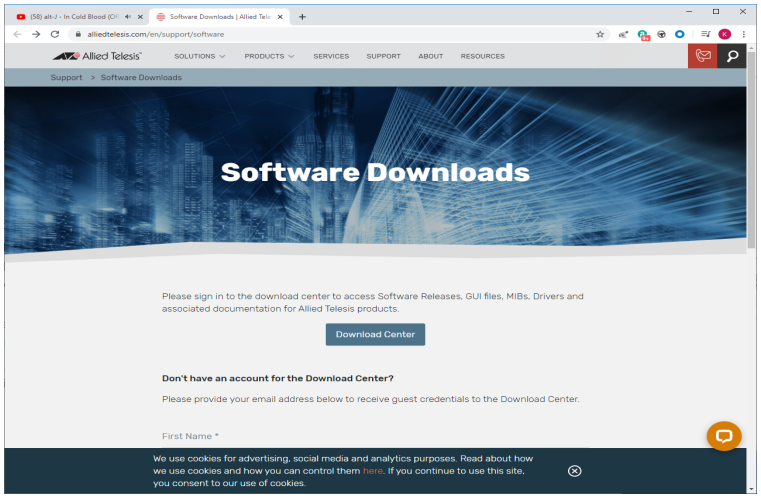


Figure 13. Software Downloads Search Result Example

2. Click Support.
3. Select Software Library.
4. Complete the form to gain access to the Download Center.
5. Check your email for the access Login ID and password.
6. Click Download Center.

7. Enter the Login ID and Password and click Login.

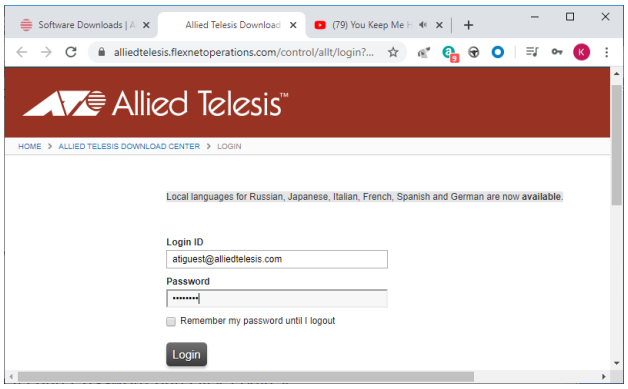


Figure 14. Login Window

8. Select the driver for the DNC10 Series network adapter and your operating system.

9. Save the zip folder onto your system.

10. Right-click the zip folder and select Extract All.

    A window appears and prompts you to specify the location of a folder where you want to place the unzipped files.

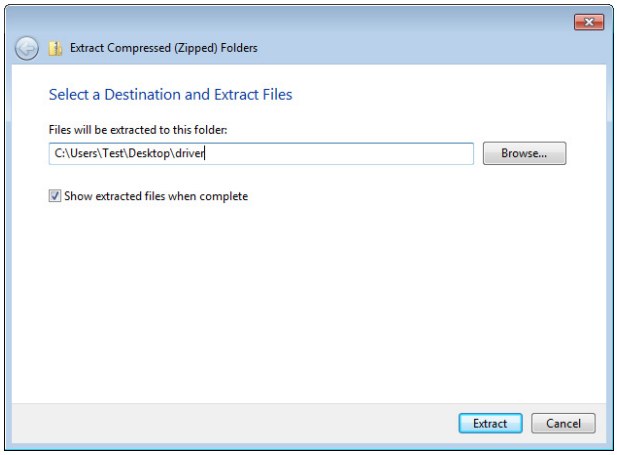


Figure 15. Select a Destination and Extract

11. Specify the location of the folder and click Extract.

12. Record the location of the folder.

Accessing the Device Manager

When you install or update the driver software for DNC10 Series network adapter, you must first access the Device Manager. The procedures for accessing the Device Manager are slightly different among Windows operating systems. To access the Device Manager on your operating system, follow one of the procedures below:

Option 1

To access the Device Manager on a Windows platform, do the following:

1. Right-click the start button at the bottom left corner.

   The Windows menu appears.

Figure 16. Windows Menu

2. Select **Device Manager** in the search box.

The Device Manager window appears.

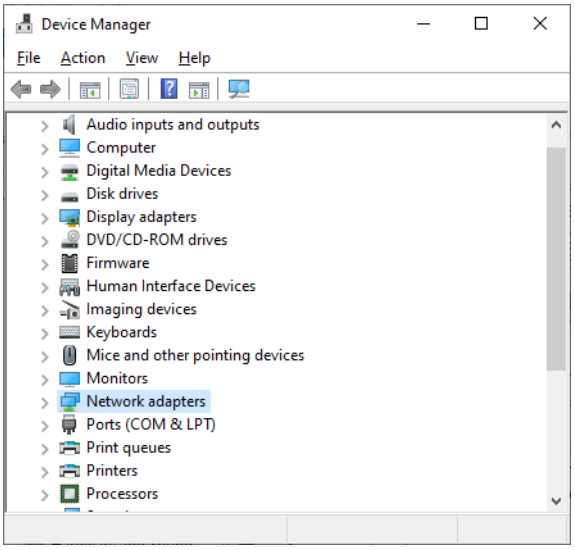


Figure 17. Device Manager Window

Option 2

Another option to accessing the Device Manager is:

1. Type **Device Manager** in the search field at the bottom left corner.

   The following screen appears.

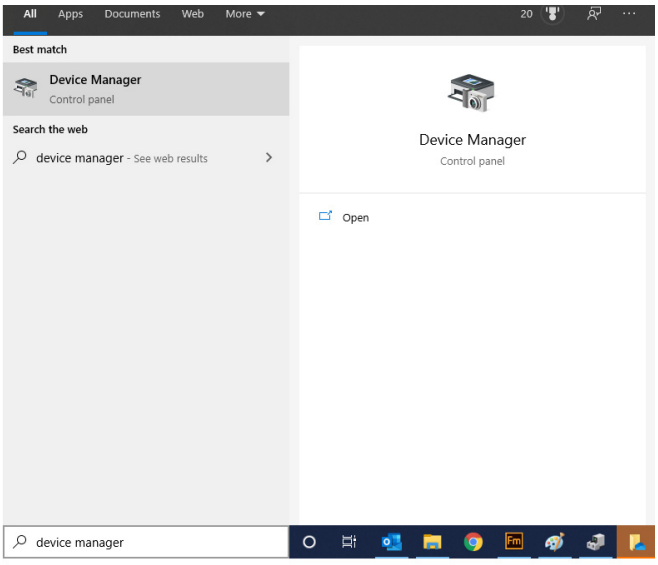


Figure 18. Searching for Device Manager

2. Click on the **Device Manager**.

   The Device Manager window appears as shown in Figure 17.

Installing the Driver Software

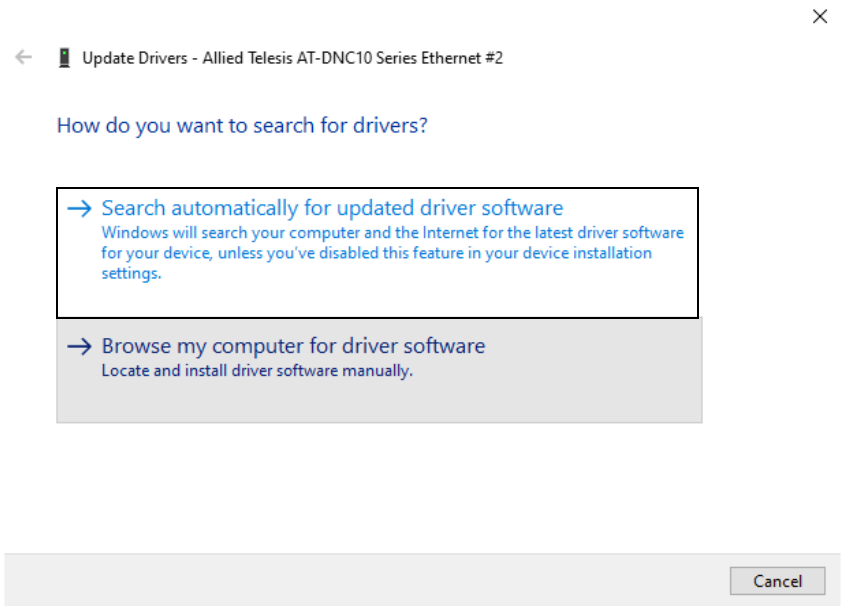
Once you physically install the DNC10 Series network card, the system detects the new hardware and creates an entry in the Device Manager when the Windows operating system first boots up. Shortly after you log in, you need to install the driver software for your adapter card.

> **Note**
> To install the driver software, you must have administrative privileges.

To install the driver software, do the following:

1. Access the Device Manager, see "Accessing the Device Manager" on page 45.
2. In the Device Manager window, double-click **Network Adapters** to expand the field.
3. **Option 1** - If the system has another network connection to provide Internet access:
   a. Right-click on **Aquantia device** or **Ethernet Controller** (if no driver was installed).
   b. Select **Update Driver Software**.

      The Update Driver Software window appears. See Figure 20 as an example.



c. Select **Search automatically for updated driver software**.

Windows will download the driver from Windows Update.

Option 2 - If the system does not have another network connection to provide Internet access:

a. Right-click on **Allied Telesis** DNC10 Series **Fiber Ethernet**.

Note
The Device Manager may identify the new DNC10 adapter as an Ethernet Controller, Aquantia device, or Allied Telesis device.

The shortcut menu appears. See Figure 19 as an example.

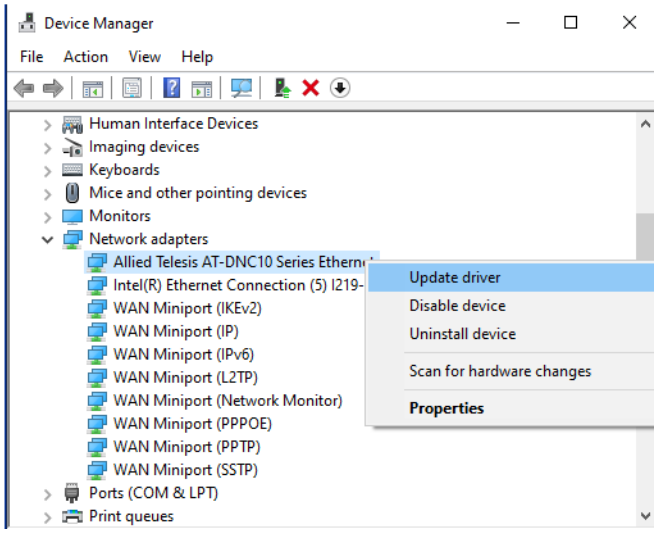


Figure 19. Selecting the DNC10 Series Adapter in the Device Manager

b. Select **Update Driver Software**.

The Update Driver Software window appears. See Figure 20 on page 49 as an example.

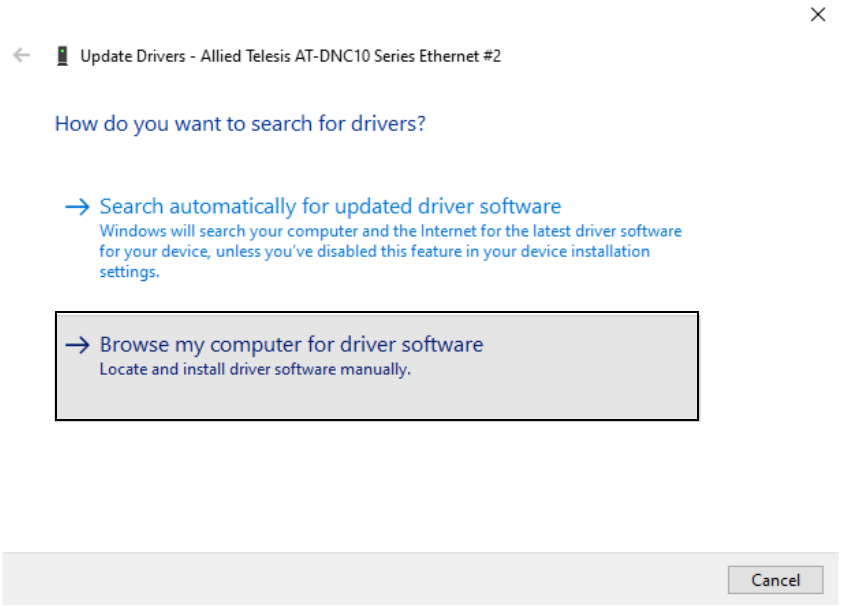


Figure 20. Update Driver Software Window

c. Select **Browse my computer for driver software**.

The Browse for Drivers on Your Computer window prompts you to enter the location of the driver folder. See Figure 21 as an example.

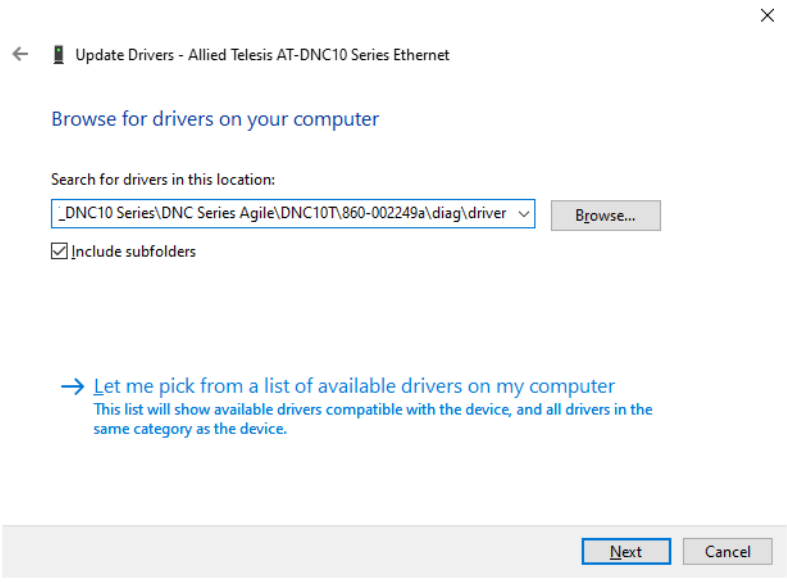


Figure 21. Browse for Drivers on Your Computer

4. Specify the location of the driver software. See "Downloading the Driver Software" on page 43 for details.

5. Click **Next**.

A confirmation message appears when the driver software is successfully updated.

6. Click **Close**.

Updating the Driver Software

If your operating system automatically installs a default driver or Aquantia driver, you need to update the driver software with the driver that you downloaded from the Allied Telesis website. To obtain the latest version of the DNC10 Series network adapter driver, see "Downloading the Driver Software" on page 43.

To update the driver software, you use the same procedure for installing the driver software for the first time. The only difference between updating and installing the driver software is the name of your adapter that the Device Manager detects and lists.

The Device Manager lists your adapter card entry as Allied Telesis DNC10 Series Fiber Ethernet once you installed the driver software. Before you installed the driver software, the Device Manager may list your adapter entry as an Ethernet Controller, Aquantia device, or Allied Telesis device.

To update the driver software for your DNC10 Series network adapter, see "Installing the Driver Software" on page 47.

Performing the Silent Installation

To simplify the driver installation process, you may perform a silent installation when installing driver software for the DNC10 Series network adapter card entries. The silent installation is a method of installing software in the silent mode without constant interactions by suppressing dialog boxes.

> **Note**
> You can apply the silent installation method only to Microsoft certified drivers. The drivers that Allied Telesis provides for the DNC10 Series network adapters are all Microsoft certified.

Use a command line utility called Driver Package Installer (DPInst) for the silent installation. DPInst is included in the Windows Developer Kit (WDK) provided by Microsoft. You can obtain the latest DPInst by downloading and installing the latest WDK from the Microsoft website.

Installing the Driver Silently

To install the driver silently, perform the following instructions:

1. Create a folder in your Windows system.
2. Download driver software for the DNC10 Series network adapter.

   See “Downloading the Driver Software” on page 43.
3. Place the driver files that you downloaded into the folder that you created in step 1.

   The folder should include the following driver files:

   - `.sys`
   - `.inf`
   - `.cat`
4. Download the latest WDK to obtain the `dpinst` utility.

   Consult Microsoft websites to download WDK.
5. Place the `dpinst.exe` and its supporting files in the same folder where you placed the driver files.

   You must place the 64-bit `dpinst` utility if your operating system is the 64-bit version. Place the 32-bit for `dpinst` utility for the 32-bit version operating system.
6. Open a command prompt window with administrator privileges.

7. Change the directory to the folder where the `dpinst` utility and the driver files reside.

8. Install the driver in the silent mode by entering the following command:

   ```
   > dpinst /S
   ```

   Note
   Adding the `/S` switch to the `dpinst` command suppresses the display of wizard pages, user dialog boxes, and other user intervention requests.

   The driver is installed silently.

Viewing Supported DPInst Options

You can display help information about the `dpinst` command-line options.

View all supported `dpinst` options by executing the following command:

1. Open a command prompt window with administrator privileges.

2. Change the directory to the folder where the `dpinst` utility and the driver files reside.

   ```
   > dpinst /?
   ```

   The command displays the help text.

Chapter 4

Modifying Advanced Properties

This chapter includes the following topics:

Overview

The DNC10 series network adapters allow you to modify advanced properties to meet your requirements. To access the advanced properties, access Device Manager, then go to each advanced property page.

Guidelines

Here are the guidelines to modifying the advanced properties:

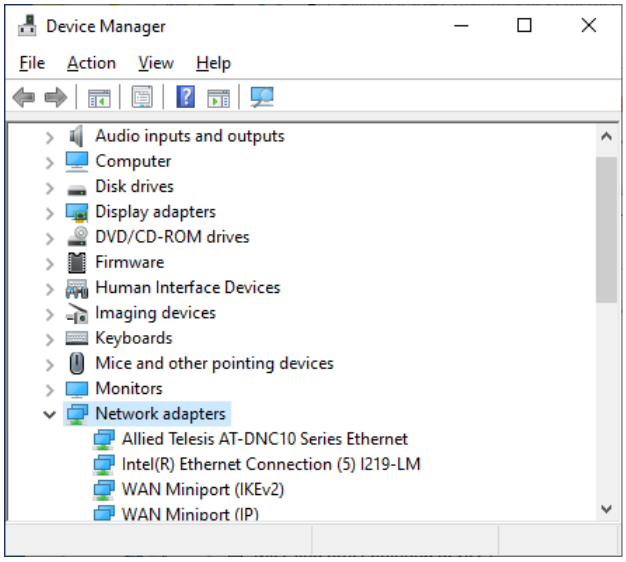
- To change the advanced property settings, you must have Administrator privileges.
- When you upgrade the driver software, the settings of the advanced properties may change. Verify the settings after upgrading the driver software.

Accessing Advanced Properties

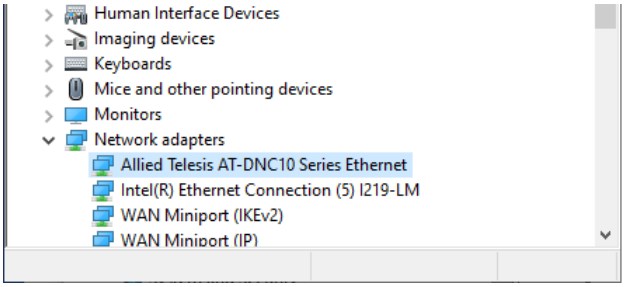
To modify advanced properties, first access Device Manager, open the properties of your adapter, and select a feature you want to change its setting.

1. Access the Device Manager. See “Accessing the Device Manager” on page 45.

2. In the Device Manager window, click **Network Adapters.**



3. Double-click **Allied Telesis AT-2911GP Series Ethernet**.



   The properties window pops up.

4. Click the **Advanced** tab.

   The Advanced Properties window opens as shown in Figure 22.

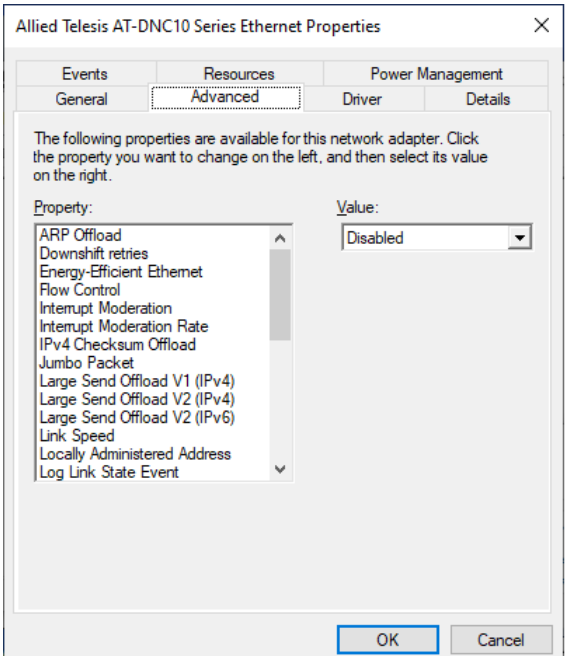


Figure 22. Advanced Properties Window

ARP Offload

The ARP Offload feature enables the adapter not to wake up when responding to an ARP request. ARP is used to verify whether a computer is still present on the network and resolve an IP address into a MAC address.

To enable or disable the ARP Offload feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **ARP Offload** in the Property box.

   The ARP Offload page is displayed as shown in Figure 23.

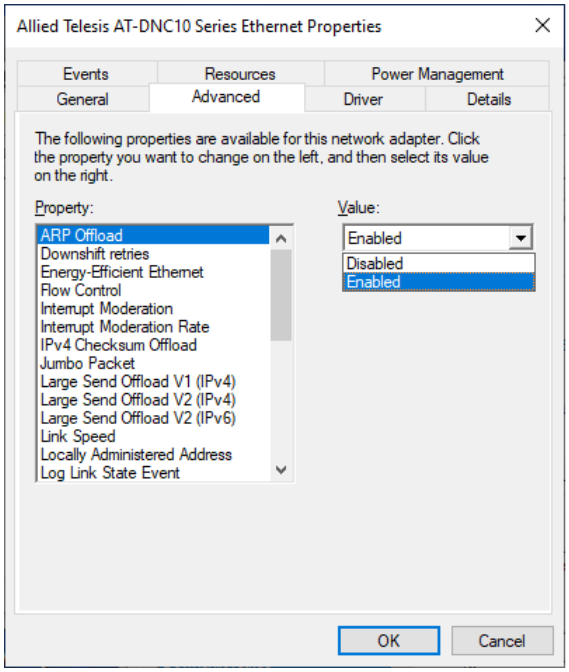


Figure 23. ARP Offload Page

3. Select one of the following options:

   - **Disabled —** This feature is disabled.
   - **Enabled —** The adapter does not wake up when responding to an ARP request. This is the default setting.

4. Click **OK**.

Downshift Retries

This feature offers a way for the network systems to reliably select the best speed that the cabling plant can support. When `on`, it enables a link speed downgrade in case the currently selected speed is constantly failing. This only applies to DNC10T.

To specify or change the Downshift Retries feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Downshift Retries** in the Property box.

   The Downshift Retries page is displayed as shown in Figure 24.

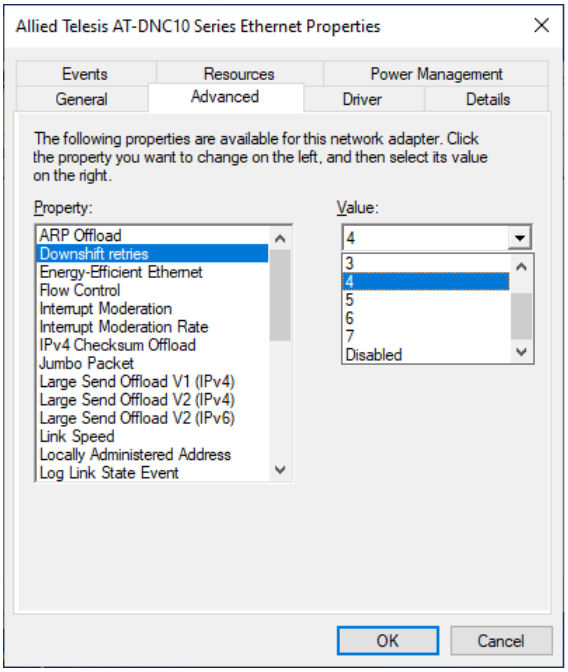


Figure 24. Downshift Retries Page

3. Select one of the following options:

   - **1 through 7 —** Enables the specified amount of tries before attempting to reduce the speed.
   - **Disable —** This feature is disabled.

4. Click **OK**.

Energy-Efficient Ethernet

The Energy-Efficient Ethernet property allows you to optimize the energy usage of the interface over Ethernet.

> **Note**
> This feature is valid only for copper ports.

To view the Energy-Efficient Ethernet feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Energy-Efficient Ethernet** in the Property box.

   The Energy-Efficient Ethernet page is displayed as shown in Figure 25.

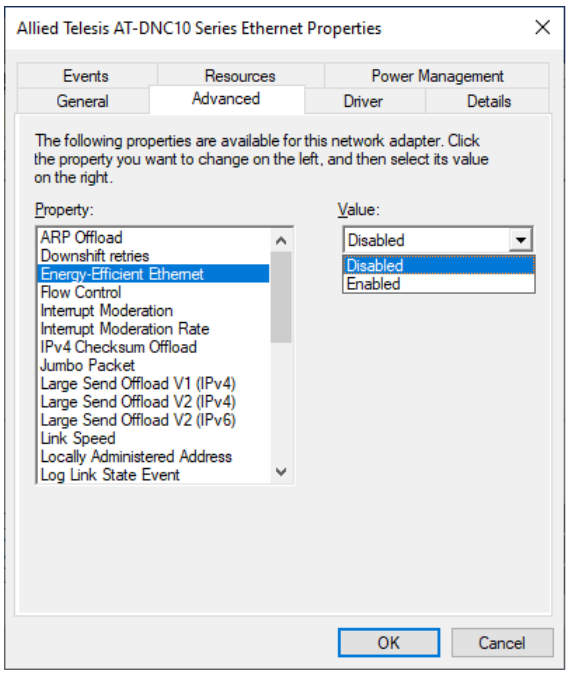


Figure 25. Energy-Efficient Ethernet Page

3. Select one of the following options:

   - **Disabled —** For the DNC10LC and DNC10SP network adapter ports are fiber connectors and the setting is always disabled.
   - **Enabled —** For the DNC10T network adapter has copper ports and can be set to Energy-Efficient Ethernet enabled.

4. Click **OK**.

Flow Control

The Flow Control feature allows you to control the flow between the DNC10 adapter port and its link partner. You can enable or disable the adapter port to process received PAUSE frames and transmit PAUSE frames.

To specify or change the Flow Control feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Flow Control** in the Property box.

   The Flow Control page is displayed as shown in Figure 26.

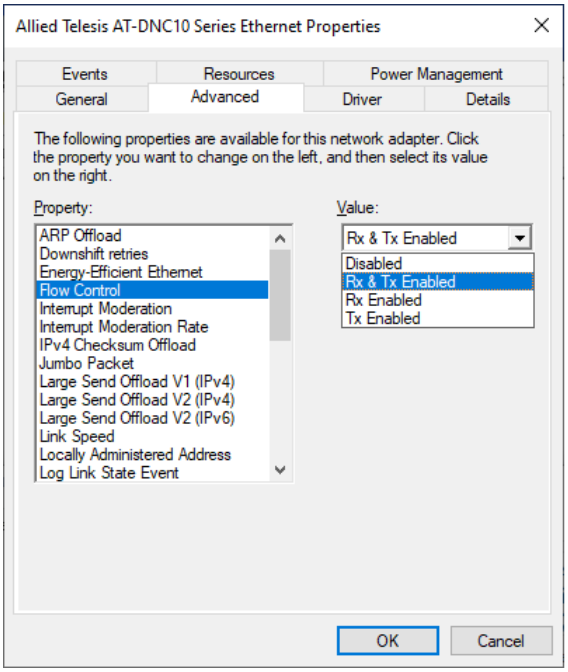


Figure 26. Flow Control Page

3. Select one of the following options if available:

   - **Disabled —** The adapter ignores PAUSE frames.
   - **Tx & Rx Enabled —** The adapter processes PAUSE frames when receiving and transmits PAUSE frames.
   - **Rx Enabled —** The adapter processes PAUSE frames when receiving, but does not transmit PAUSE frame.
   - **Tx Enabled —** The adapter transmits PAUSE frames, but ignores PAUSE frames when receiving.

4. Click **OK**.

Interrupt Moderation

The Interrupt Moderation feature allows you to limit the rate of interrupts to the CPU during packet transmission and packet reception. When this feature is enabled, interrupts are handled as a group so that the CPU utilization decreases; however, the latency may increase.

To enable or disable the Interrupt Moderation feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Interrupt Moderation** in the Property box.

   The Interrupt Moderation page is displayed as shown in Figure 27.

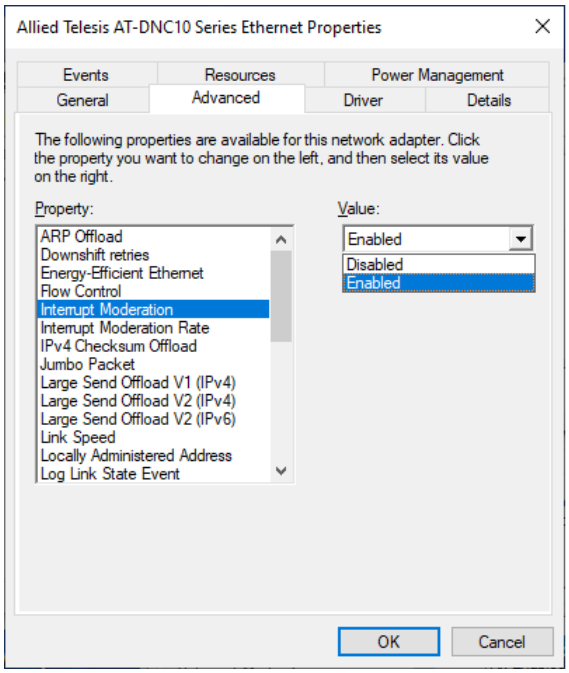


Figure 27. Interrupt Moderation Page

3. Select one of the following options:

   - **Disabled —** The Interrupt Moderation feature is disabled. The adapter generates one interrupt for every packet transmission and packet reception.
   - **Enabled —** The Interrupt Moderation feature is enabled. This is the default setting.

4. Click **OK**.

Interrupt Moderation Rate

To improve system performance, you can configure the interrupt moderation rate. This setting defines the maximum number of interrupts per second that the adapter is allowed to generate. Note that decreasing this value decreases the CPU usage.

To specify or change the Interrupt Moderation Rate feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Interrupt Moderation Rate** in the Property box.

   The Interrupt Moderation Rate page is displayed as shown in Figure 28.

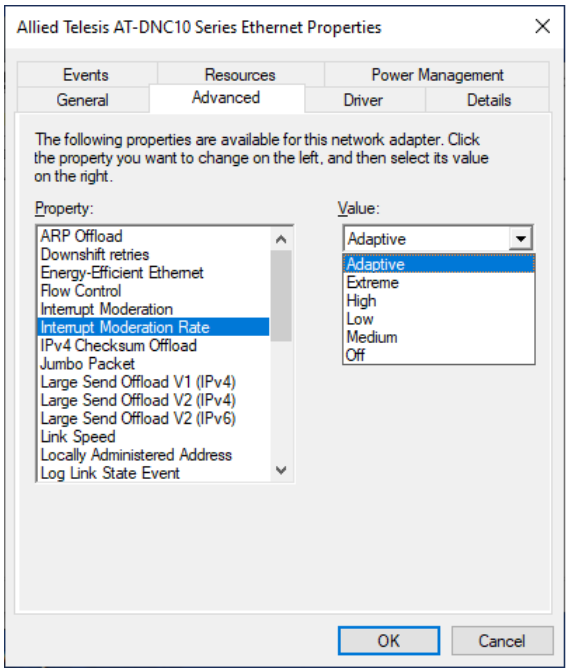


Figure 28. Interrupt Moderation Rate Page

3. Select one of the following options:

   - **Adaptive —** Interrupt throttle rate (ITR) = -1, no interrupts/sec, it is dynamically changed by the driver. This is the default setting.
   - **Extreme —** ITR = 3600.
   - **High —** ITR = 2000.

- **Medium —** ITR = 950.
- **Low —** ITR = 400.
- **Off —** ITR = 0, no limit.

4. Click **OK**.

IPv4 Checksum Offload

To specify or change the IPv4 Checksum Offload feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **IPv4 Checksum Offload** in the Property box.

   The IPv4 Checksum Offload page is displayed as shown in Figure 29.

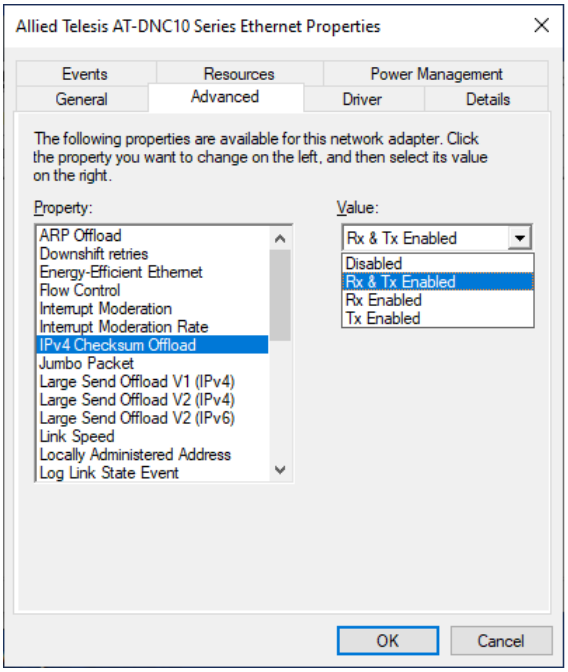


Figure 29. IPv4 Checksum Offload Page

3. Select one of the following options:

   - **Disabled —** Disables the IPv4 Checksum Offload function for both receiving and transmitting.
   - **Rx & Tx Enabled —** Enables the IPv4 Checksum Offload function for both receiving and transmitting IPv4 packets. This is the default setting.
   - **Rx Enabled —** Enables the IPv4 Checksum Offload function only for receiving IPv4 packets.
   - **Tx Enabled —** Enables the IPv4 Checksum Offload function only for transmitting IPv4 packets.

4. Click **OK**.

Jumbo Packet

Enables the network adapter to transmit and receive oversized Ethernet frames that are greater than 1500 bytes, but less than or equal to 16348 bytes in length. This property requires the presence of a switch that is able to process jumbo frames. Maximum frame size is set at 1500 bytes by default (Jumbo Packet disabled). To increase the maximum frame size, choose one of the values from the drop-down list.

To change the Jumbo Packet setting, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Jumbo Packet** in the Property box.

   The Jumbo Packet page is displayed as shown in Figure 30.

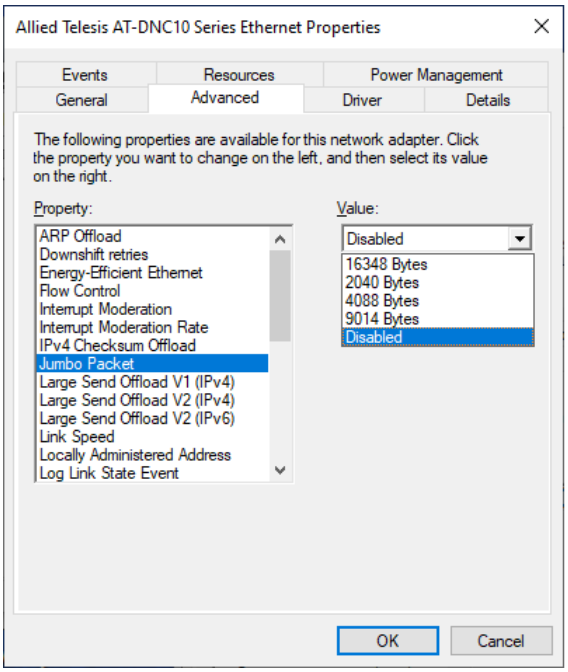


Figure 30. Jumbo Packet Page

3. Select the desired jumbo frame size from the list. The options are:

   - 2040 bytes
   - 4088 bytes
   - 9014 bytes
   - 16348 bytes

- Disabled — The adapter does not handle jumbo frames.

4. Click **OK**.

Large Send Offload v1 (IPv4)

Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property, the TCP segmentation can be done by the network adapter. The default setting for this property is Enabled.

To enable or disable the Large Send Offload v1 (IPv4) feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Large Send Offload v1 (IPv4)** in the Property box.

   The Large Send Offload v1 (IPv4) page is displayed as shown in Figure 31.

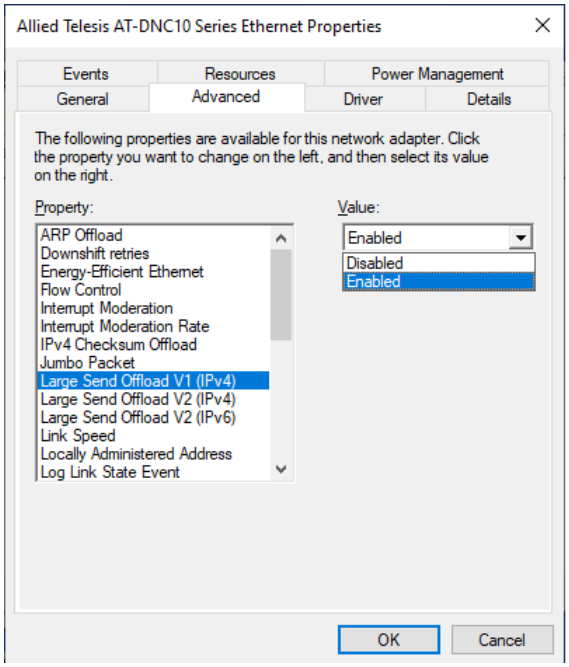


Figure 31. Large Send Offload v1 (IPv4) Page

3. Select one of the following options:

   - **Disabled —** The Large Send Offload v1 (IPv4) feature is disabled
   - **Enabled —** The Large Send Offload v1 (IPv4) feature is enabled. This is the default setting.

4. Click **OK**.

Large Send Offload v2 (IPv4)

Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property, the TCP segmentation can be done by the network adapter. The default setting for this property is Enabled.

To enable or disable the Large Send Offload v2 (IPv4) feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Large Send Offload v2 (IPv4)** in the Property box.

   The Large Send Offload v2 (IPv4) page is displayed as shown in Figure 32.

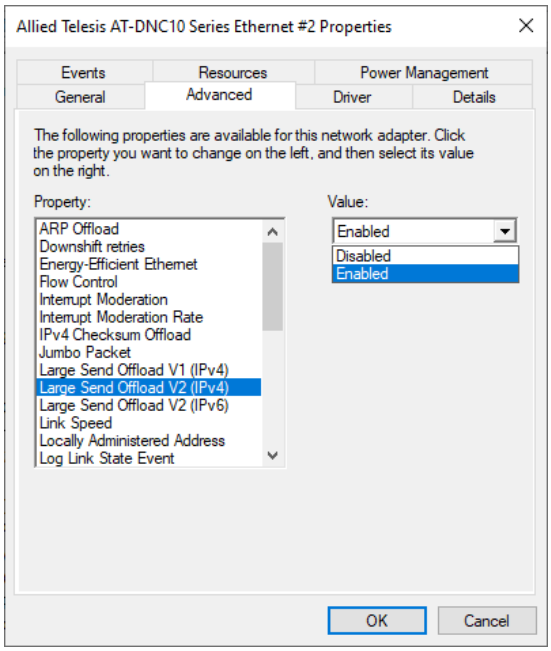


Figure 32. Large Send Offload v2 (IPv4) Page

   Select one of the following options:

   - **Disabled —** The feature is disabled.
   - **Enabled —** The adapter port segments large packets up to 256Kb for IPv4 traffic before sending them out. This is the default setting.

3. Click **OK**.

Large Send Offload v2 (IPv6)

The Large Send Offload v2 (IPv6) feature allows you to control the load of sending out large packets. When this feature is enabled, the adapter port segments large packets for IPv6 traffic and reduces the CPU load.

To enable or disable the Large Send Offload v2 (IPv6) feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Large Send Offload v2 (IPv6)** in the Property box.

   The Large Send Offload v2 (IPv6) page is displayed as shown in Figure 33.

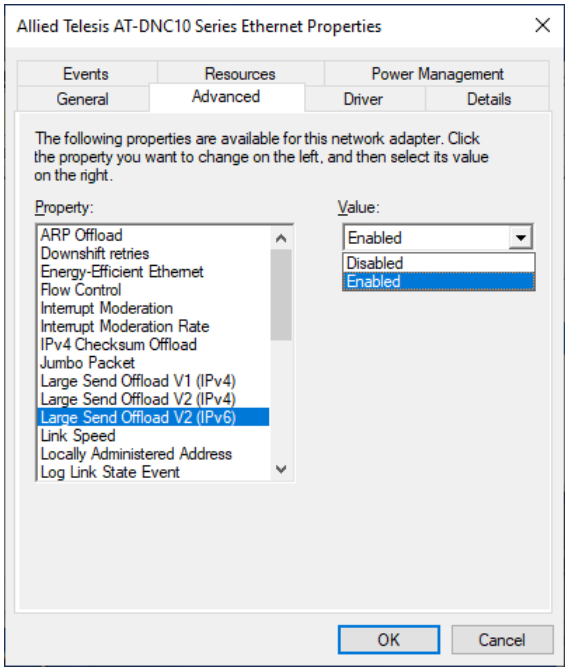


Figure 33. Large Send Offload (IPv6) Page

3. Select one of the following options:

   - **Disabled —** The adapter does not segment packets for IPv6 traffic.
   - **Enabled —** The adapter port segments large packets up to 256Kb for IPv6 traffic before sending them out. This is the default setting.

4. Click **OK**.

Link Speed

To specify or change the port speed, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Link Speed** in the Property box.

   The Link Speed page is displayed as shown in Figure 34.

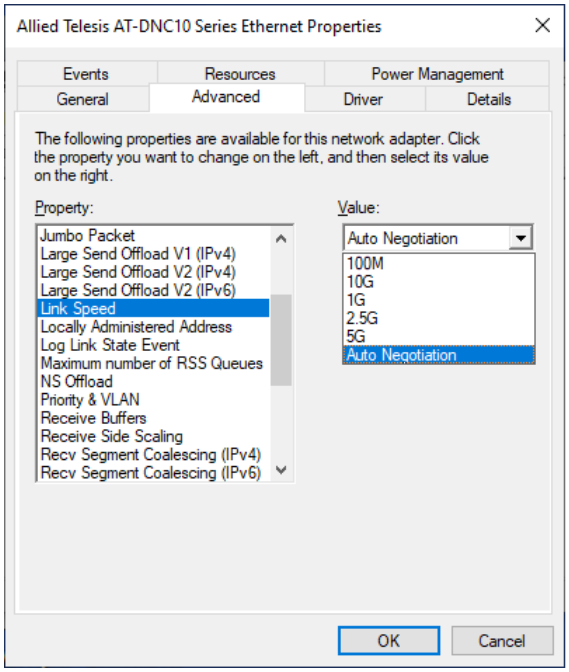


Figure 34. Link Speed Page

3. Select one of the following options:

> **Note**
> Allied Telesis recommends leaving this value set to the default Auto Negotiation. For the fiber versions of the DNC10, auto-negotiation does not refer to traditional speed and duplex auto-negotiation that is commonly used on copper-based NIC products. It simply means that the NIC will automatically detect the speed of the fiber module and set the controller's speed to match.

DNC10LC

- Auto Negotiation - Link speed will be set to 10G
- 10G - Link speed is 10G per second

All other settings are invalid.

DNC10SP

- Auto Negotiation - The NIC will auto-detect the SFP speed and link speed will be set to 10G or 1G accordingly
- 10G - Link speed is 10G per second
- 1G - Link speed is 1G per second

All other settings are invalid.

> **Note**
> The DNC10T uses standard auto-negotiation to determine link speed in all cases. Forced speed is disallowed by IEEE 802.3 for any speed of 1Gbps and above. When choosing a single speed from the drop-down list, only that speed will be advertised by the NIC; if the link partner does not also advertise the chosen speed, no link will be established.

DNC10T

- Auto Negotiation - The NIC will advertise all supported speeds and negotiate the highest common speed with the link partner.
- 10G - Only 10Gbps speed will be advertised.
- 5G - Only 5Gbps speed will be advertised.
- 2.5G - Only 2.5Gbps speed will be advertised.
- 1G - Only 1Gbps speed will be advertised.
- 100M - Only 100Mbps speed will be advertised.

4. Click **OK**.

Locally Administered Address

The Locally Administered Address is a user-defined MAC address that is used in place of the MAC address originally assigned to the network adapter. Every adapter in the network must have its own unique MAC address. This locally administered address consists of a 12-digit hexadecimal number.

To specify or change the Locally Administered Address, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Locally Administered Address** in the Property box.

   The Locally Administered Address page is displayed as shown in Figure 35.

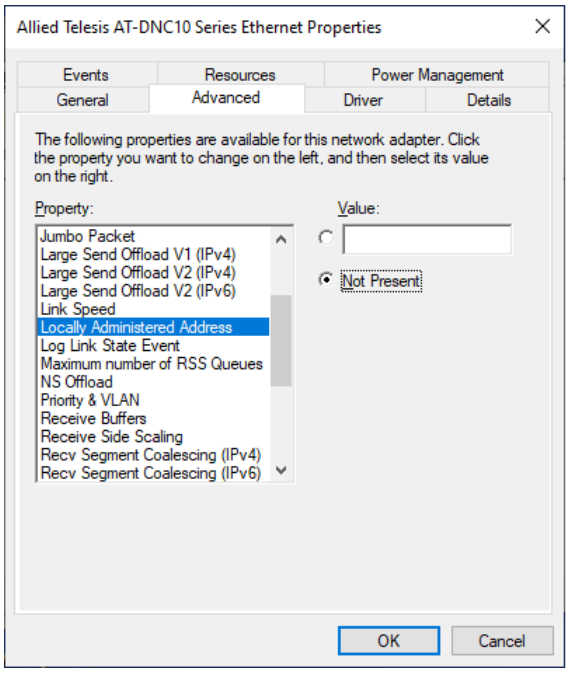


Figure 35. Locally Administered Address Page

3. Select one of the following options:

   - **Value —** Used to manually assign a MAC address to the adapter.
   - **Not Present —** Uses the factory-assigned address on the adapter. This is the default.

Note
The appropriate assigned ranges and exceptions for the locally administered address include the following:

The range is 00:00:00:00:00:01 to FF:FF:FF:FF:FF:FD.

Do not use a multicast address (least significant bit of the high byte = 1).

Do not use all 0s or all Fs.

4. Click **OK**.

Log Link State Event

This feature allows you to enable or disable logging of the adapter's link state changes (such as changes to the port link state or duplex mode mismatch) in the system logs.

To enable or disable the Log Link State Event feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Log Link State Event** in the Property box.

   The Log Link State Event page is displayed as shown in Figure 36.

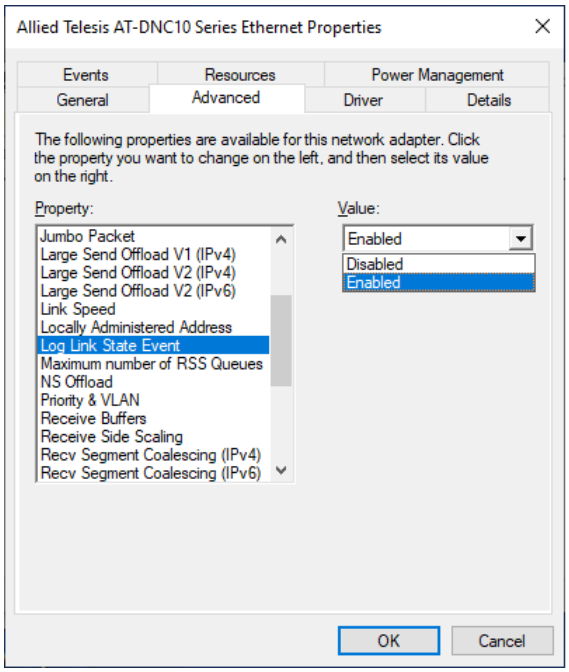


Figure 36. Log Link State Event Page

3. Select one of the following options:

   - **Disabled —** This feature is disabled.
   - **Enabled —** The adapter generates link state events. This is the default setting.

4. Click **OK**.

Maximum Number of RSS Queues

The RSS Queues feature assigns data to queues associated with physical CPU cores. You can specify the maximum number of RSS queues that the network adapter assigns receiving data to.

To specify or change the maximum number of RSS Queues, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Maximum Number of RSS Queues** in the Property box.

   The Maximum Number of RSS Queues page is displayed as shown in Figure 37.

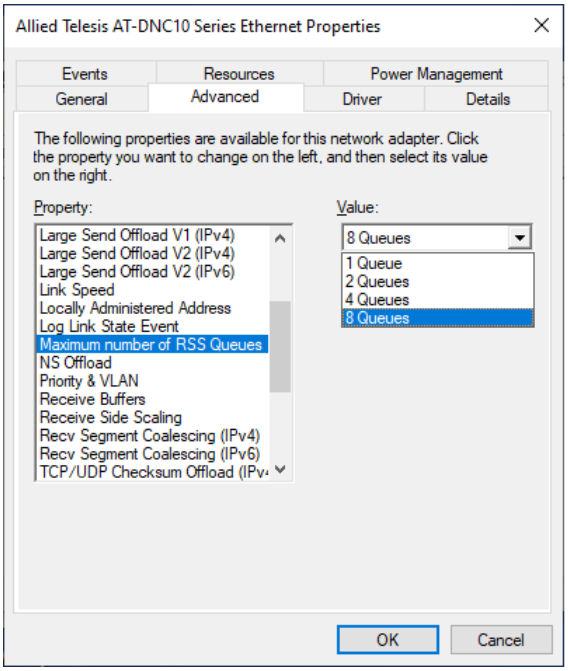


Figure 37. Maximum Number of RSS Queues Page

3. Select one of the following options:

   - **1 Queue —** The system allocates up to one RSS queue.
   - **2 Queues —** The system allocates up to two RSS queues.
   - **4 Queues —** The system allocates up to four RSS queues.
   - **8 Queues —** The system allocates up to eight RSS queues.

4. Click **OK**.

NS Offload

The NS (Neighbor Solicitation) Offload feature enables the adapter not to wake up when responding to an NS request.

To enable or disable the NS Offload feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **NS Offload** in the Property box.

   The NS Offload page is displayed as shown in Figure 38.

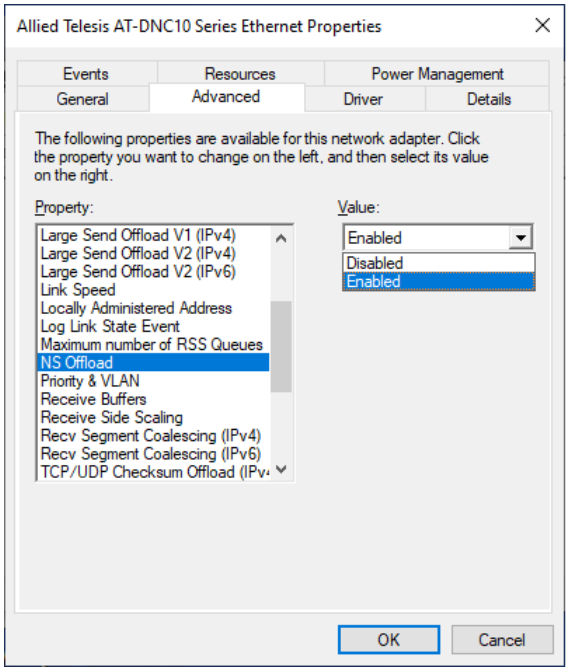


Figure 38. NS Offload Page

3. Select one of the following options:

   - **Disabled —** This feature is disabled.
   - **Enabled —** The adapter does not wake up when responding to an NS request. This is the default setting.

4. Click **OK**.

Priority & VLAN

The Priority & VLAN feature allows you to control sending and receiving tagged frames of QoS and VLAN.

When the property is set to Priority & VLAN Enabled, the adapter sends and receives QoS and VLAN tagged frames; with Priority Enabled, the adapter sends and receives QoS tagged frames; with VLAN Enabled, the adapter sends and receives VLAN tagged frames. To assign a VLAN ID to the adapter, see "VLAN ID" on page 94.

To enable or disable the Priority & VLAN feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Priority & VLAN** in the Property box.

   The Priority & VLAN page is displayed as shown in Figure 39.

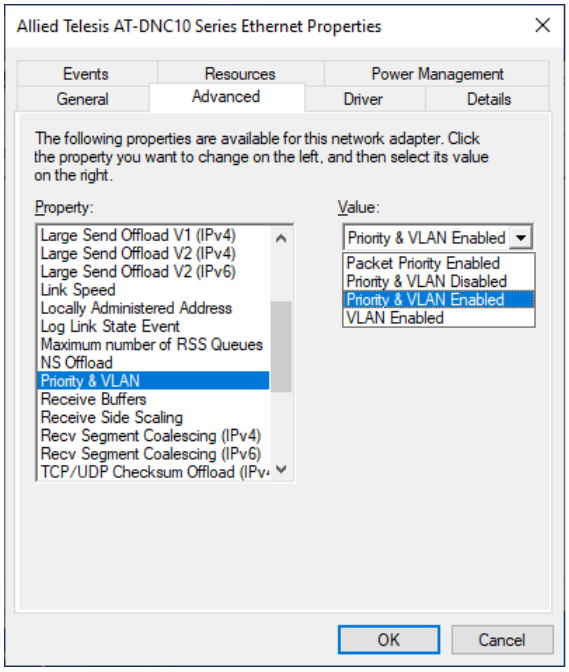


Figure 39. Priority & VLAN Page

3. Select one of the following options:

   - **Priority & VLAN Enabled —** Allows for packet prioritization and VLAN tagging. This is the default setting.

- **Priority & VLAN Disabled —** Prevents packet prioritization and VLAN tagging.
- **Packet Priority Enabled —** Allows packet prioritization only.
- **VLAN Enabled —** Allows VLAN tagging only.

4. Click **OK**.

Receive Buffers

Receive buffers are data segments that allow the network adapter to allocate receive packets to memory.

To specify or change the Receive Buffers feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Receive Buffers** in the Property box.

   The Receive Buffers page is displayed as shown in Figure 40.

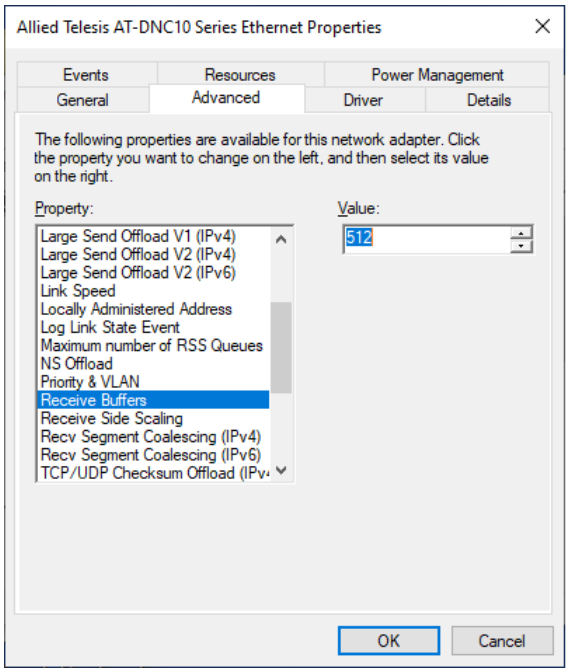


Figure 40. Receive Buffers Page

3. Specify the buffer size in the Value box.

   The range of valid receive buffers is 128 to 4096 in increments of 8 with 512 receive buffers as the default value.

4. Click **OK**.

Receive Side Scaling

The Receive Side Scaling (RSS) feature allows the adapter to efficiently distribute receive processing across multiple CPU's so as to prevent overloading a single CPU. To make this feature effective, the computer must have multiple CPU's in a multiprocessor system.

To enable or disable the Receive Side Scaling feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Receive Side Scaling** in the Property box.

   The Receive Side Scaling page is displayed as shown in Figure 41.

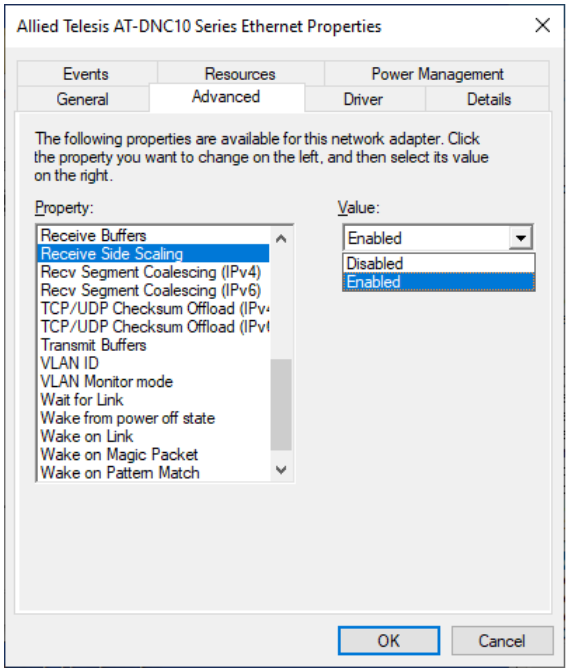


Figure 41. Receive Side Scaling Page

3. Select one of the following options:

   - **Enabled —** Receiving data is processed by multiple CPU's. This is the default setting.
   - **Disabled —** Receiving data is processed by a single CPU.

4. Click **OK**.

Recv Segment Coalescing (IPv4)

When receiving data, the miniport driver, NDIS, and TCP/IP must all look at each segment's header information separately. When large amounts of data are being received, this creates a large amount of overhead. Receive segment coalescing (RSC) reduces this overhead by coalescing a sequence of received segments and passing them to the host TCP/IP stack in one operation, so that NDIS and TCP/IP need only look at one header for the entire sequence.

To enable or disable the Receive Segment Coalescing (IPv4) feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Receive Segment Coalescing (IPv4)** in the Property box.

   The Receive Segment Coalescing (IPv4) page is displayed as shown in Figure 42.

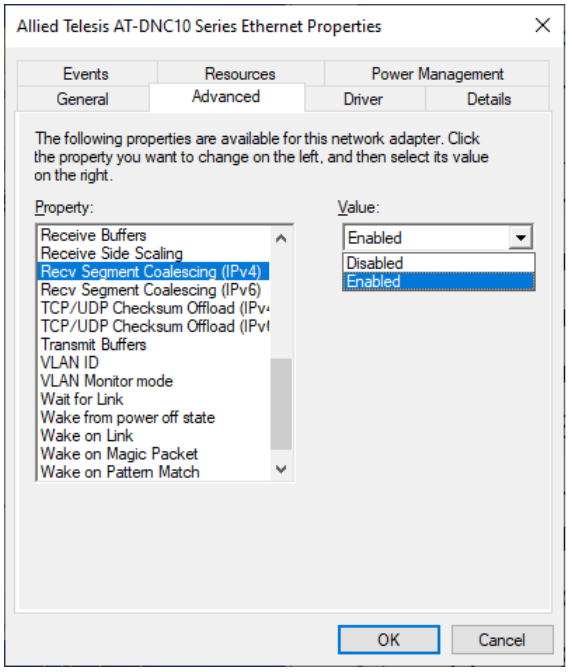


Figure 42. Receive Segment Coalescing (IPv4) Page

3. Select one of the following options:

   - **Enabled —** RSC is enabled. This is the default setting.
   - **Disabled —** RSC is disabled.

4. Click **OK**.

Recv Segment Coalescing (IPv6)

When receiving data, the miniport driver, NDIS, and TCP/IP must all look at each segment's header information separately. When large amounts of data are being received, this creates a large amount of overhead. Receive segment coalescing (RSC) reduces this overhead by coalescing a sequence of received segments and passing them to the host TCP/IP stack in one operation, so that NDIS and TCP/IP need only look at one header for the entire sequence.

To enable or disable the Receive Segment Coalescing (IPv6) feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Receive Segment Coalescing (IPv6)** in the Property box.

   The Receive Segment Coalescing (IPv6) page is displayed as shown in Figure 43.

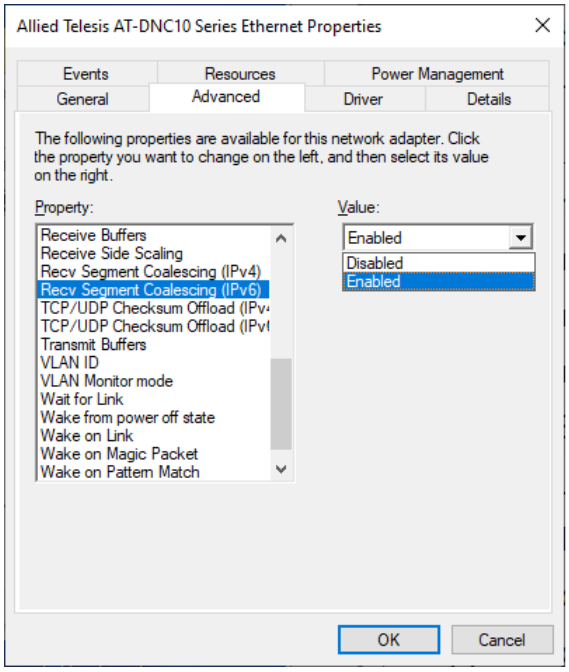


Figure 43. Receive Segment Coalescing (IPv6) Page

3. Select one of the following options:

   - **Enabled —** RSC is enabled. This is the default setting.
   - **Disabled —** RSC is disabled.

4. Click **OK**.

TCP/UDP Checksum Offload (IPv4)

The TCP/UDP Checksum Offload (IPv4) function enables the adapter port to compute the checksum of transmitting IPv4 packets and verify the checksum of receiving IPv4 packets, taking load off from the CPU.

To modify the TCP/UDP Checksum Offload (IPv4) setting, do the following:

1. Access the Device Manager on your operating system.

   See "Accessing Advanced Properties" on page 58.

2. Select **TCP/UDP Checksum Offload (IPv4)** in the Property box.

   The TCP/UDP Checksum Offload (IPv4) page is displayed as shown in Figure 44.

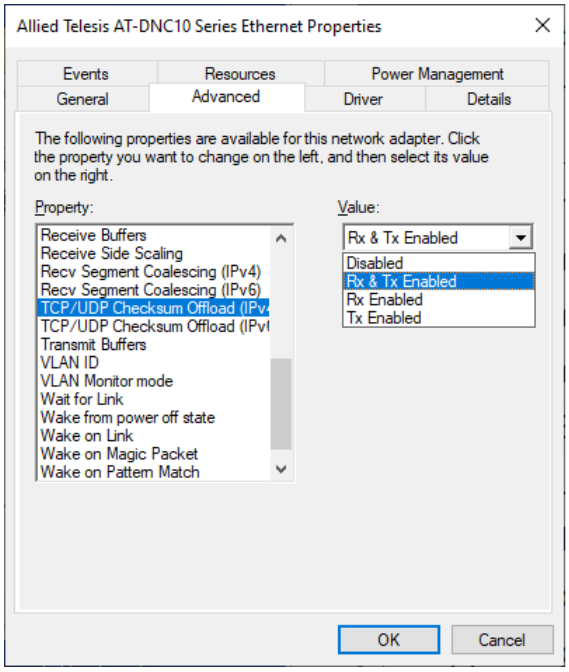


Figure 44. TCP/UDP Checksum Offload (IPv4) Page

3. Select one of the following options:

   - **Rx & Tx Enabled —** Enables the TCP/UDP Checksum Offload (IPv4) function for both receiving and transmitting IPv4 packets. This is the default setting.
   - **Disabled —** Disables the TCP/UDP Checksum Offload (IPv4) function for both receiving and transmitting.
   - **Rx Enabled —** Enables the TCP/UDP Checksum

Offload (IPv4) function only for receiving IPv4 packets.

- **Tx Enabled —** Enables the TCP/UDP Checksum Offload (IPv4) function only for transmitting IPv4 packets.

4. Click **OK**.

TCP/UDP Checksum Offload (IPv6)

The TCP/UDP Checksum Offload (IPv6) function enables the adapter port to compute the checksum of transmitting IPv6 packets and verify the checksum of receiving IPv6 packets, taking load off from the CPU.

To enable or disable the TCP/UDP Checksum Offload (IPv6) feature, do the following:

1. Access the Device Manager on your operating system.

   See "Accessing Advanced Properties" on page 58.

2. Select **TCP/UDP Checksum Offload (IPv6)** in the Property box.

   The TCP/UDP Checksum Offload (IPv6) page is displayed as shown in Figure 45.

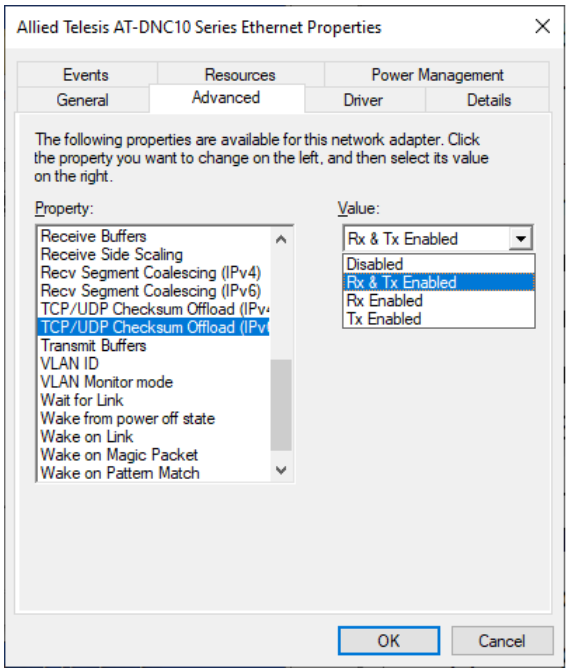


Figure 45. TCP/UDP Checksum Offload (IPv6) Page

3. Select one of the following options:

   - **Rx & Tx Enabled —** Enables the TCP/UDP Checksum Offload (IPv6) function for both receiving and transmitting IPv6 packets. This is the default setting.
   - **Disabled —** Disables the TCP/UDP Checksum Offload (IPv6) function for both receiving and transmitting.
   - **Rx Enabled —** Enables the TCP/UDP Checksum

Offload (IPv6) function only for receiving IPv6 packets.

- **Tx Enabled —** Enables the TCP/UDP Checksum Offload (IPv6) function only for transmitting IPv6 packets.

4. Click **OK**.

Transmit Buffers

The number of transmit buffers. Transmit buffers are data segments that allow the network adapter to monitor transmit packets in the system memory.

To specify or change the Transmit Buffers feature, do the following:

1. Access the Device Manager on your operating system.

   See "Accessing Advanced Properties" on page 58.

2. Select **Transmit Buffers** in the Property box.

   The Transmit Buffers page is displayed as shown in Figure 46.

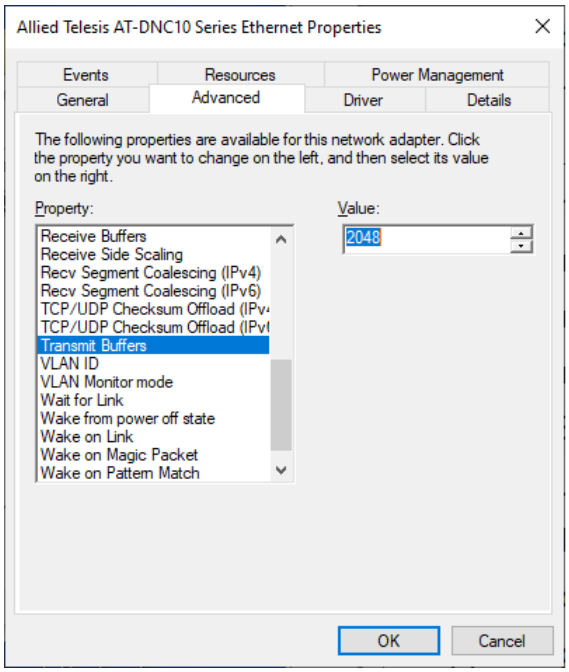


Figure 46. Transmit Buffers Page

3. Specify the buffer size in the Value box. The valid range is 256 to 8184 in increments of 8. The default value is 2048

4. Click **OK**.

VLAN ID

The VLAN ID property allows you to specify a VLAN ID on your network to the adapter port. The adapter port adds the value of the VLAN ID to a frame in the VLAN tag before transmitting the frame.

To change the VLAN ID value, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **VLAN ID** in the Property box.

   The VLAN ID page is displayed as shown in Figure 47.

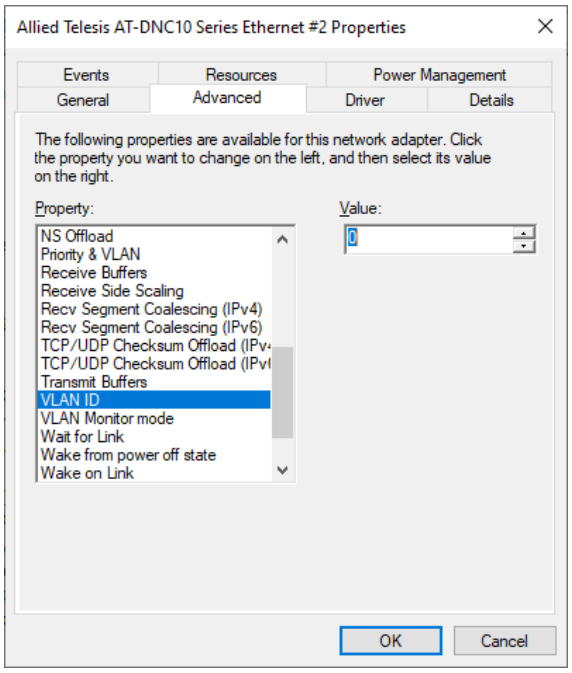


Figure 47. VLAN ID Page

3. Specify a VLAN ID in the Value box.

   The range of the value is from 0 to 4094. The default value is 0. Leaving the VLAN ID set to 0 will result in no VLAN tag being added to egress packets, even if VLAN is enabled. This field must be set to the desired VLAN ID if VLAN headers are desired.

4. Click **OK**.

VLAN Monitor Mode

The VLAN Monitor Mode controls VLAN stripping.

Note
Allied Telesis recommends setting this feature as Disabled. This property will be removed in future driver versions.

To change the VLAN Monitor Mode feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **VLAN Monitor Mode** in the Property box.

   The VLAN Monitor Mode page is displayed as shown in Figure 48.

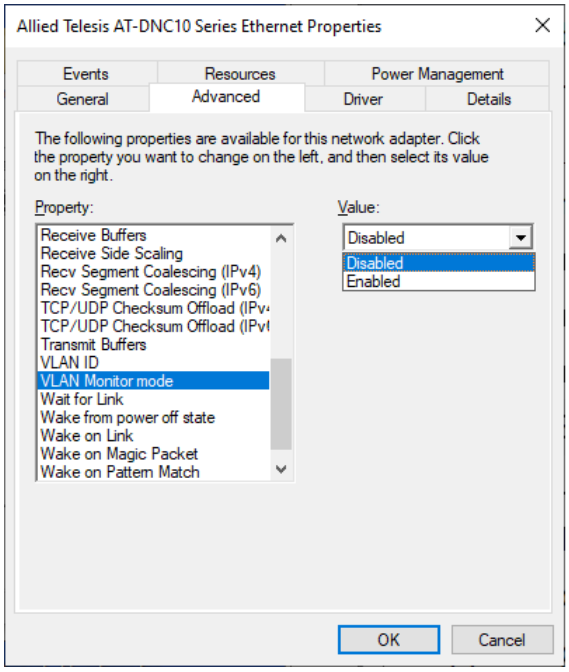


Figure 48. VLAN Monitor Mode Page

3. Select one of the following options:

   - **Enabled — If set to enabled, the VLAN tags may be stripped.**
   - **Disabled —** If set to disabled, the VLAN tags will not be stripped and packets will be passes to OS as is. This is the default setting.

4. Click **OK**.

Wait for Link

Decides if the driver waits for the link status of the interface before reporting the link state to the OS.

> **Note**
> Allied Telesis recommends setting this feature as Auto or On. This property will be removed in future driver versions.

To change the Wait for Link feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Wait for Link** in the Property box.

   The Wait for Link page is displayed as shown in Figure 49.

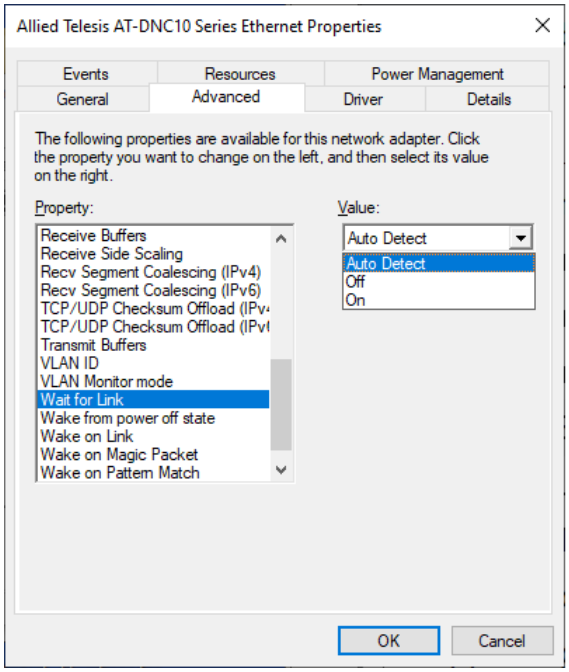


Figure 49. Wait for Link Page

3. Select one of the following options:

   - **Auto Detect —** If set to Auto Detect, it is the same as on. This is the default setting.
   - **Off —** If set to Off, driver will not wait for link negotiation on copper side and will report link state as

connected to OS.

- **On —** If set to On, driver will report only actual link state of the network interface.

4. Click **OK**.

Wake from Power Off State

When enabled this feature directs the NIC to wake the computer from sleep/power off for Wake on LAN support.

To enable or disable the Wake from Power Off State feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Wake from Power Off State** in the Property box.

   The Wake from Power Off State page is displayed as shown in Figure 50.

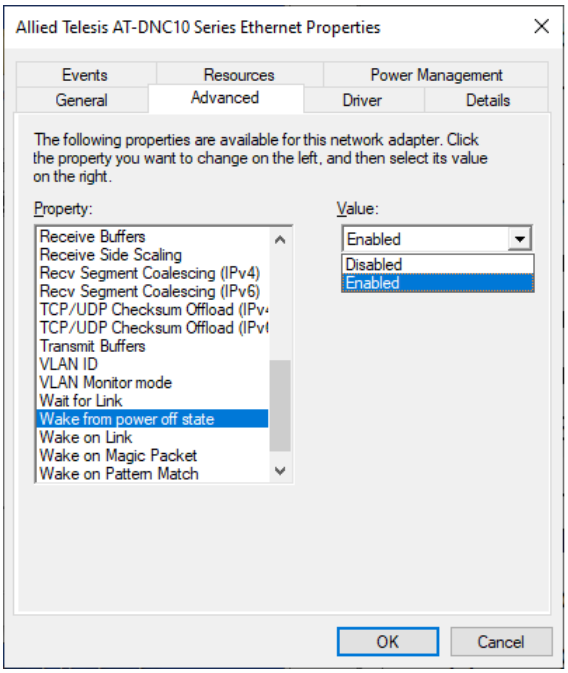


Figure 50. Wake from Power Off State Page

3. Select one of the following options:

   - **Enabled —** Wakes the computer from sleep/power off for Wake on LAN support. This is the default setting.
   - **Disabled —** The feature is disabled.

4. Click **OK**.

Note
This feature may require addition settings in the OS and/or BIOS.

Wake on Link

This is part of the Wake on LAN feature. The adapter wakes the computer from a low-power mode when the link state on the adapter's port changes from no link to link.

To enable or disable the Wake on Link feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Wake on Link** in the Property box.

   The Wake on Link page is displayed as shown in Figure 51.

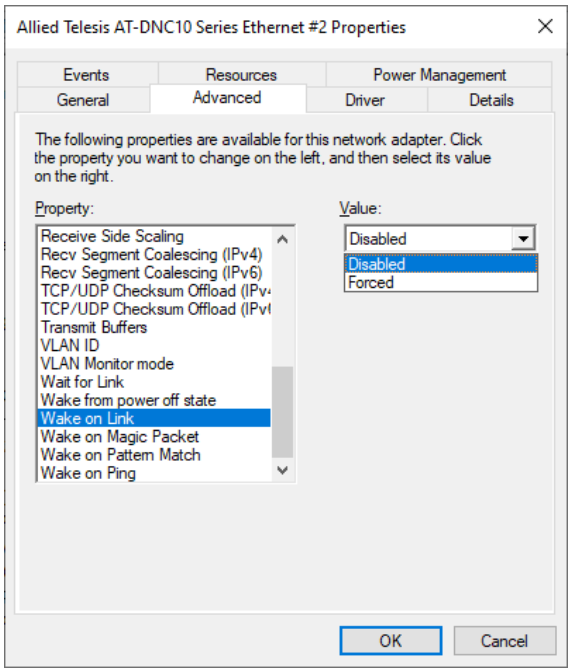


Figure 51. Wake on Link Page

3. Select one of the following options:

   - **Disable —** This feature is disabled. This is the default setting.
   - **Forced —** The adapter wakes the computer when the status of the port changes from no link to link.

4. Click **OK**.

Wake on Magic Packet

The Wake on Magic Packet feature enables the adapter to wake up from a low-power mode when the adapter port receives a Magic packet.

To enable or disable the Wake on Magic Packet feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Wake on Magic Packet** in the Property box.

   The Wake on Magic Packet page is displayed as shown in Figure 52.

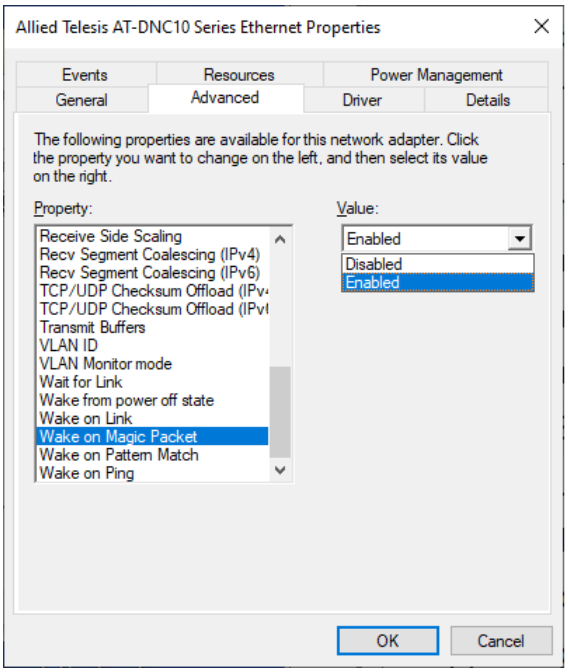


Figure 52. Wake on Magic Packet Page

3. Select one of the following options:

   - **Enabled —** The adapter wakes up from a low-power mode when receiving a Magic Packet. This is the default setting.
   - **Disabled —** The adapter stays in a low-power mode when receiving a Magic Packet.

4. Click **OK**.

Wake on Pattern Match

The Wake on Pattern Match feature enables the network adapter to wake up the computer from a low-power mode when it receives a packet that matches the wake patterns specified in the operating system.

To enable of disable the Wake on Pattern Match feature, do the following:

1. Access the Advanced Properties.

   See "Accessing Advanced Properties" on page 58.

2. Select **Wake on Pattern Match** in the Property box.

   The Wake on Pattern Match page is displayed as shown in Figure 53.

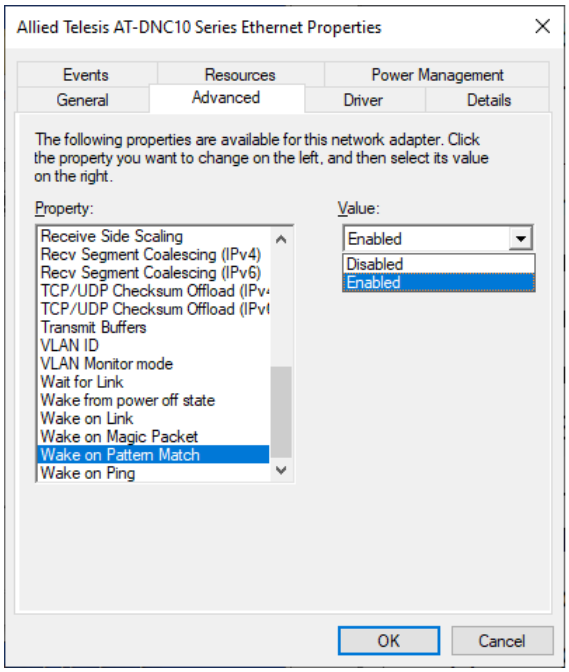


Figure 53. Wake on Pattern Match Page

3. Select one of the following options:

   - **Enabled —** The adapter wakes up from a low-power mode when receiving a packet that matches one of the patterns specified in the operating system.
   - **Disabled —** The adapter stays in a low-power mode.

4. Click **OK**.

Wake on Ping

This is part of the Wake on LAN feature. The adapter wakes the computer from a low-power mode when it receives a Ping packet on its port.

To enable or disable the Wake on Ping feature, do the following:

1. Access the Advanced Properties.

   See “Accessing Advanced Properties” on page 58.

2. Select **Wake on Ping** in the Property box.

   The Wake on Ping page is displayed as shown in Figure 48.

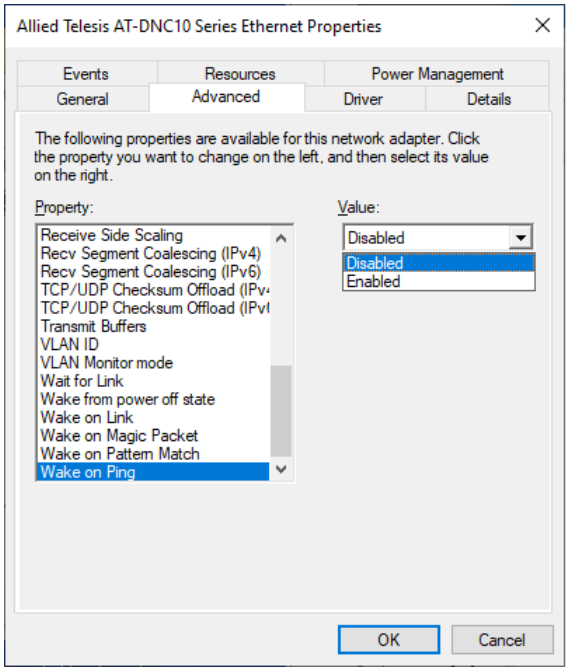


Figure 54. Wake on Ping Page

3. Select one of the following options:

   - **Disabled —** This feature is disabled. This is the default setting.
   - **Enabled —** The adapter wakes the computer when it receives a Ping packet.

4. Click **OK**.

Chapter 5

Uninstalling the Driver Software

This chapter describes how to uninstall the driver software for the DNC10 Series network adapter.

This chapter contains the following topics:

Overview

When you no longer use the DNC10 Series network adapter for your computer, you can uninstall the driver software from your operating system.

As you can install driver software for the DNC10 Series network adapter using Device Manager or the silent installation method, you can also uninstall driver software in two ways:

- ❒ “Uninstalling the Driver Software Using Device Manager” on page 107
- ❒ “Uninstalling the Driver Software Silently” on page 108

Guidelines

Here are the guidelines for uninstalling the driver software from your system:

- ❒ You must have Administrator privileges to remove the driver software.
- ❒ Before uninstalling the network adapter, capture all of the Advanced Property settings for later use. The properties are lost during the uninstall process.

Uninstalling the Driver Software Using Device Manager

To uninstall the driver software from your operating system, do the following:

1. Start your Windows operating system and log in.
2. Access the Device Manager.

   See "Accessing the Device Manager" on page 45.
3. In the Device Manager window, expand the Network Adapters folder.
4. Right-click the **Allied Telesis AT-DNC10 Series Series Ethernet**.

   The shortcut menu appears as shown in Figure 55.

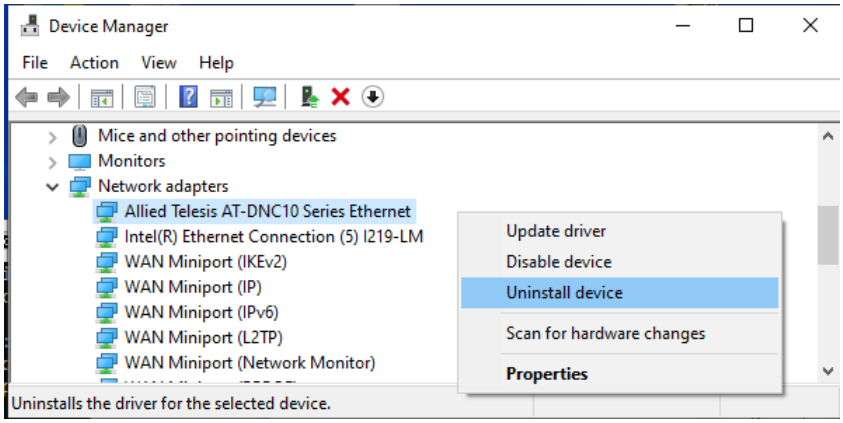


Figure 55. Device Manager Shortcut Menu

5. Select **Uninstall device**.

   The Confirm Device Uninstall window pops up.
6. Check the check box if you want to remove the driver software for your adapter.
7. Click **OK** to complete the uninstall.

Uninstalling the Driver Software Silently

You can apply the silent installation method to uninstall the driver.

To uninstall the driver without user-intervention, perform the following steps:

1. Open a command prompt window with administrator privileges.
2. Change the directory to the folder where the `dpinst` utility and the driver files reside.
3. Uninstall the driver silently by executing the following command:

   ```
   > dpinst /U inf_file_name.inf /S
   ```

   Note
   Replace *inf_file_name* with the name of `.inf` file.

   The driver is uninstalled without user-intervention.

Chapter 6

Troubleshooting

This chapter describes troubleshooting procedures. It contains the following sections:

Troubleshooting Checklist

The following checklist provides recommended actions to take to resolve problems installing the DNC10 series adapter card or running it in your system.

Note
Before opening the cabinet of your system to remove or install the adapter card, review all precautions outlined under “Reviewing Safety Precautions” on page 29.

General Troubleshooting

Here are general troubleshooting suggestions:

- ❒ Inspect all cables and connections. Verify that the cable connections on the network adapter and network device are attached securely.
- ❒ Verify that the fiber strand connected to TX of the port is connected to the RX of the link partner and vice versa.
- ❒ Verify that the remote network device is powered on and operating properly.
- ❒ Try connecting the adapter to another network device.
- ❒ Repeat the procedure for installing the adapter driver. Refer to “Installing the Driver Software” on page 47.
- ❒ If the remote device is a management device, use its management software to confirm that the port connected to the adapter is enabled.
- ❒ Verify that the computer with the adapter has the latest BIOS.

Note
The following items require removing the cover from the computer.

- ❒ Inspect the adapter for damage.
- ❒ Verify that the adapter is completely inserted in the PCIe connector in the system.
- ❒ Try installing the adapter in a different PCIe slot in the system.
- ❒ Try installing the adapter in a different system.

DNC10LC Adapter

Here are troubleshooting suggestions for the DNC10LC adapter:

- ❒ Verify that the fiber optic cable is securely connected to the duplex LC ports on the DNC10LC adapter and remote network device.

- ❒ Verify that you are using the correct type of fiber optic cable and that the cable length does not exceed the maximum length. Refer to Table 9 on page 117.
- ❒ Verify that the duplex LC ports on the DNC10LC adapter and the remote network device have the same operating properties, such as wavelength, fiber optic cable type, and maximum operating distance. Refer to Table 1 on page 19.
- ❒ Test the attenuation of both directions on the fiber optic cable with a fiber optic tester to determine whether the optical signal is too weak (sensitivity) or too strong (maximum input power). Table 9 on page 117. If there is no link, try creating a loopback between the TX port and the RX port of the fiber connector. A successful link may indicate an incompatibility or fault with the connected cables or equipment.

DNC10SP Adapter

Here are troubleshooting suggestions for the DNC10SP adapter:

- ❒ Verify that the SFP+ transceiver is fully inserted in the port in the adapter.
- ❒ Verify that the fiber optic ports on the fiber optic transceiver and remote network device have the same operating properties, including wavelength, fiber optic cable type, and maximum operating distance. Refer to the specifications included with the transceiver.
- ❒ Verify that the SFP or SFP+ module is of a supported type.
- ❒ If the problem is with two BiDi (bi-directional) transceivers, refer to their data sheets to verify that their transmission and reception frequencies are opposite each other. For instance, a BiDi transceiver that transmits and receives at 1310nm and 1550nm, respectively, has to be connected to a transceiver that transmits and receives at 1550nm and 1310nm, respectively. Two BiDi transceivers will not establish a link if they transmit and receive at the same frequencies.
- ❒ Test the attenuation of both directions on the fiber optic cable with a fiber optic tester to determine whether the optical signal is too weak (sensitivity) or too strong (maximum input power). If there is no link, try creating a loopback between the TX port and the RX port of the fiber connector. A successful link may indicate an incompatibility or fault with the connected cables or equipment.

DNC10T Adapter

Here are troubleshooting suggestions for the DNC10T adapter:

- Verify that the Ethernet cable is securely connected to the ports on the network adapter and network device.
- Verify that the cable is correct for the link speed. Refer to “DNC10T Twisted Pair Copper Port” on page 23.
- Verify that the cable does not exceed 100 meters (328 feet).

Testing Network Connectivity

This section describes how to test the network connectivity of the new adapter with the operating system TCP/IP Ping command. This test assumes the following:

- ❒ The adapter is connected to your network.
- ❒ The computer has an IP address. The address can be a static address that you manually assigned it or a dynamic address from a DHCP server.
- ❒ You know the IP address of another network device.
- ❒ If the new DNC10 adapter is the only network adapter in the computer, you may test it either by having it ping another device or by having another device ping the adapter. However, if there is more than one network adapter in the computer, you should test the new adapter by having another device ping it.

To test the network connectivity, perform the following procedure.

1. Click the Start icon in the left bottom corner of the computer screen.
2. In the search box, type **cmd** and click **OK**.
3. If you are performing the ping command at the system with the new network adapter, type **ipconfig /all** to display its IP address configuration.

An example of the command output is shown in Figure 56.

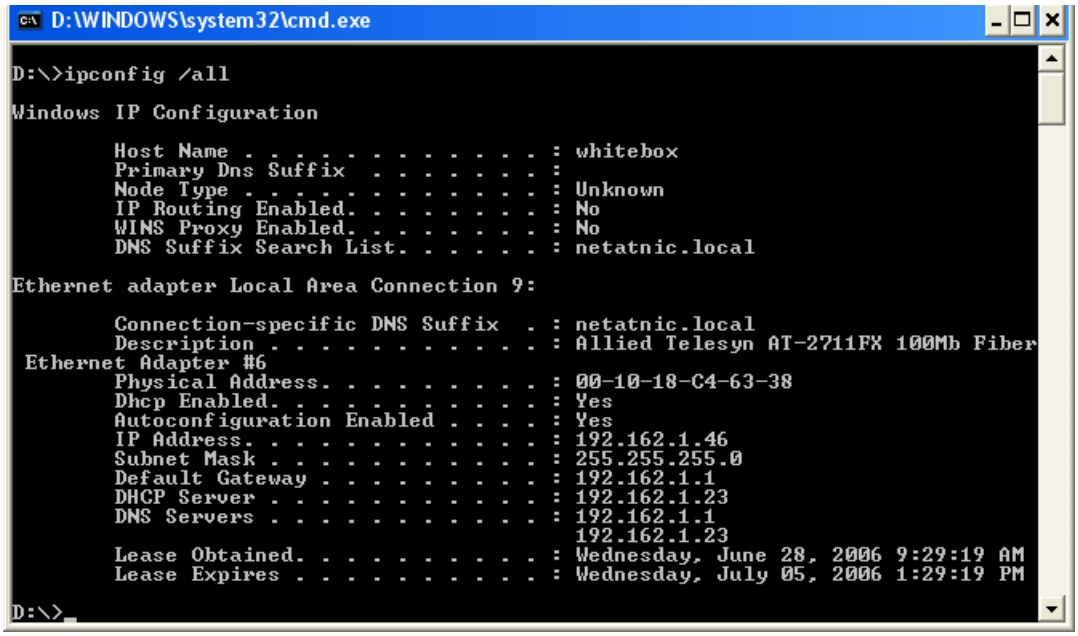


Figure 56. IPCONFIG Command

4. Type **ping** and the IP address of another network device from the command line, then press **Enter**. If you are performing the ping command at the system with the new adapter, specify the IP address of a remote device the adapter should ping. If you are performing the command at another system, enter the IP address of the new adapter.

   The results of the Ping command are displayed, as shown in Figure 57. The output should indicate that the system received a reply to its ping from the destination system.

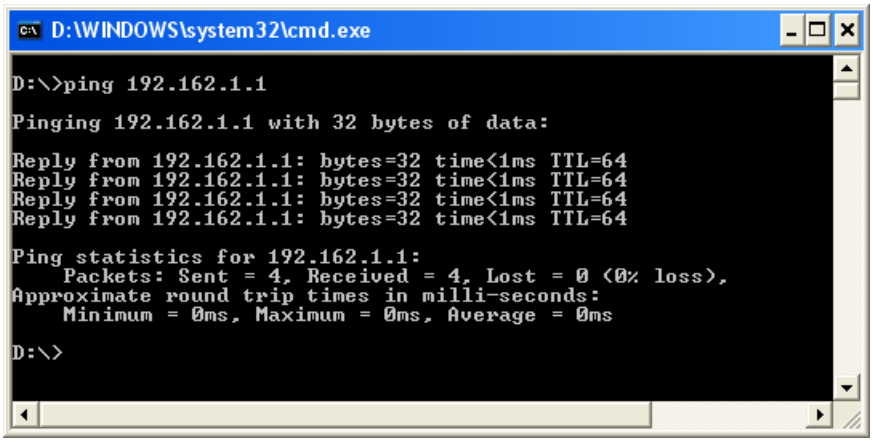


Figure 57. Ping Command

Appendix A
Technical Specifications

This appendix contains the following sections:

Physical Specifications

Table 5 contains the weights of the adapter cards.

Table 5. Weights

Network Interface Card	Weight
DNC10LC	4.25 g (0.15 oz)
DNC10SP	2.83 g (0.10 oz)
DNC10T	2.83 g (0.10 oz)

Table 6 contains the dimensions of the adapter cards.

Table 6. Dimensions

Network Interface Card	Dimension (H x D x W)
DNC10LC	82.55 mm x 101.6 mm x 9.05 mm (3.25 in x 4.0 in x 0.75 in)
DNC10SP	82.55 mm x 101.6 mm x 9.05 mm (3.25 in x 4.0 in x 0.75 in)
DNC10T	82.55 mm x 101.6 mm x 9.05 mm (3.25 in x 4.0 in x 0.75 in)

Environmental Specifications

Table 7 contains the environmental specifications of the adapter cards.

Table 7. Environmental Specifications

Environmental Specification	Value
Operating Temperature	DNC10LC: 0° C to 50° C (32° F to 122° F) DNC10SP: 0° C to 50° C (32° F to 122° F) DNC10T: 0° C to 40° C (32° F to 104° F)
Storage Temperature	-25° C to 70° C (-13° F to 158° F)
Operating Humidity	5% to 95% non-condensing
Storage Humidity	5% to 95% non-condensing
Maximum Operating Altitude	Up to 3,048 m (10,000 ft)
Maximum Storage Altitude	Up to 3,048 m (10,000 ft)

Power Specifications

Table 8 contains the power specifications of the adapter cards:

Table 8. Operating Voltages and Maximum Power Consumption

Operating Voltage	3.3V
Maximum Power Consumption	DNC10SP Typical: 2W (with SP10SR) Maximum: 4.5W (with SP10ZR80/I) DNC10LC Typical: 1.75W Maximum: 3W DNC10T Typical: 4W Maximum:7W

RJ-45 Twisted Pair Port Pinouts

Figure 58 illustrates the pin layout of the RJ-45 connector on the DNC10T adapter.

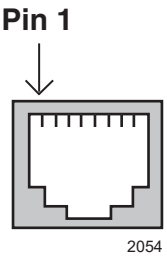


Figure 58. Pin Layout (Front View) of the Twisted Pair Port on the DNC10T Adapter

Table 9 lists the pin signals at 100Mbps.

Table 9. Pin Signals on the RJ-45 Twisted Pair Port at 100Mbps

Pin	MDI Signal	MDI-X Signal
1	TX+	RX+
2	TX-	RX-
3	RX+	TX+
4	Not used	Not used
5	Not used	Not used
6	RX-	TX-
7	Not used	Not used
8	Not used	Not used

Table 10 lists the pin signals at 1/2.5/5/10Gbps.

Table 10. Pin Signals on the Twisted Pair Port at 1/2.5/5/10Gbps

Pin	Pair	Signal
1	1 +	TX and RX+
2	1 -	TX and RX-
3	2 +	TX and RX+
4	3 +	TX and RX+
5	3 -	TX and RX-
6	2 -	TX and RX-
7	4 +	TX and RX+
8	4 -	TX and RX-