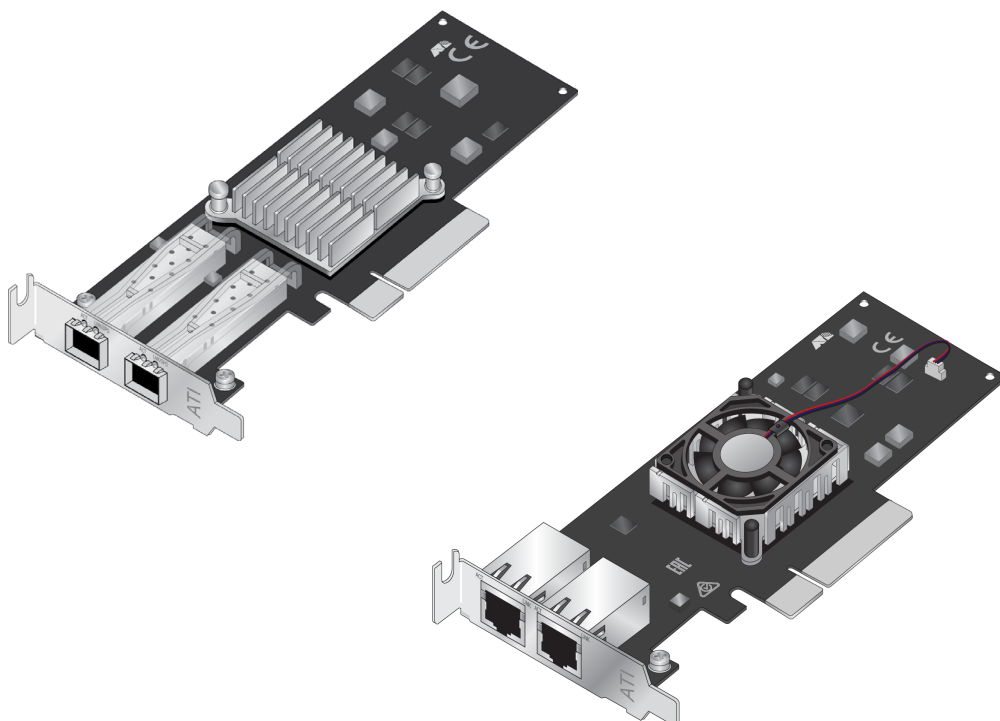


# ANCI0 Series

10 Gigabit Network Interface Cards

ANCI0Sa/2

ANCI0T/2



## Installation and User's Guide

Copyright © 2021 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

# 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: **ANC10Sa/2 and ANC10T/2 Adapters**

Model Numbers: **ANC10Sa/2 and ANC10T/2**

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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.


## 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 Part 15, EN55032 Class B, VCCI Class B, ICES-003
Immunity	EN55035, EN 61000-3-2, EN 61000-3-3
Electrical Safety	EN62368-1 (TUV), UL 62368-1 (cUL <sub>US</sub> ), CSA C22.2 No. 62368-1
Environmental	RoHS
 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](http://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](http://www.alliedtelesis.com/library).



# Contents

---

<b>Preface</b> .....	13
Safety Symbols Used in this Document .....	14
Contacting Allied Telesis .....	15
<b>Chapter 1: Introduction</b> .....	<b>17</b>
Functional Description .....	18
ANC10Sa/2 Network Interface Card SFP+ Ports .....	19
ANC10T/2 Network Interface Card Twisted Pair Copper Ports .....	22
Features .....	24
Software .....	25
<b>Chapter 2: Installing the Hardware</b> .....	<b>27</b>
Reviewing Safety Precautions .....	28
Pre-Installation Checklist .....	30
Installing the Standard Bracket on the Network Interface Card .....	31
Installing the Network Interface Card .....	33
Installing SFP+ Transceivers in the ANC10Sa/2 Network Interface Card .....	35
Connecting Twisted-Pair Copper Cables to the ANC10T/2 Network Interface Card .....	36
<b>Chapter 3: Installing the Windows Driver Software</b> .....	<b>37</b>
Overview .....	38
Guidelines .....	38
Installing the Driver Using the Device Manager .....	38
Installing the Driver Using the Silent Installation Method .....	38
Downloading the Driver Software .....	39
Accessing the Windows Device Manager .....	43
Installing the Driver Software .....	45
Updating the Driver Software .....	48
Performing the Silent Installation .....	49
Installing the Driver Silently .....	49
Viewing Supported DPLnst Options .....	50
<b>Chapter 4: Modifying Advanced Properties</b> .....	<b>51</b>
Overview .....	53
Guidelines .....	53
Accessing Advanced Properties .....	54
Encapsulated Task Offload .....	56
Encapsulation Overhead .....	57
Energy-Efficient Ethernet .....	58
Flow Control .....	60
Forward Error Correction .....	62
Interrupt Moderation .....	64
Interrupt Moderation Configuration .....	65
Jumbo Packet .....	66
Large Send Offload v2 (IPv4) .....	67
Large Send Offload v2 (IPv6) .....	68
Locally Administered Address .....	70
Maximum Number of MSI-X Messages .....	72

Maximum Number of RSS Processors .....	73
Maximum Number of RSS Queues .....	74
Maximum RSS Processor Number.....	75
Network Direct Functionality .....	76
Network Direct Technology .....	77
NVGRE Encapsulated Task Offload.....	78
Packet Direct .....	79
Preferred NUMA Node .....	80
Priority & VLAN.....	81
PTP Hardware Timestamp .....	83
Quality of Service .....	84
Receive Buffers (0=Auto) .....	85
Receive Side Scaling.....	86
Recv Segment Coalescing (IPv4).....	87
Recv Segment Coalescing (IPv6).....	89
RoCE MTU .....	91
RSS Base Processor Group .....	92
RSS Base Processor Number .....	93
RSS Load Balancing Profile .....	94
RSS Max Processor Group .....	96
Software Timestamp.....	97
Speed & Duplex.....	99
SR-IOV .....	101
TCP/UDP Checksum Offload (IPv4).....	102
TCP/UDP Checksum Offload (IPv6).....	104
Transmit Buffers (0=Auto) .....	106
UDP Segmentation Offload (IPv4).....	107
UDP Segmentation Offload (IPv6).....	108
VF Spoofing Protection.....	109
Virtual Machine Queues .....	110
Virtual Switch RSS .....	111
VLAN ID.....	112
VXLAN Encapsulated Task Offload.....	113
<b>Chapter 5: Uninstalling the Driver Software .....</b>	<b>115</b>
Overview.....	116
Guidelines .....	116
Uninstalling the Driver Software Using Device Manager .....	117
Uninstalling the Driver Software Silently.....	119
<b>Appendix A: Technical Specifications .....</b>	<b>121</b>
Physical Specifications .....	121
Environmental Specifications .....	122
Power Specifications .....	122
Performance Specification.....	122
Compliance Requirements .....	123



# Figures

---

Figure 1: ANC10Sa/2 Network Interface Card.....	20
Figure 2: ANC10Sa/2 Network Interface Card Faceplate.....	20
Figure 3: ANC10T/2 Network Interface Card.....	22
Figure 4: ANC10T/2 Network Interface Card Faceplate.....	22
Figure 5: Removing the Low-profile Bracket.....	31
Figure 6: Installing the Standard Bracket.....	32
Figure 7: Software Downloads Window.....	39
Figure 8: Login Window.....	39
Figure 9: Support Window.....	40
Figure 10: Support Portal Window.....	40
Figure 11: Register for an Account Window.....	41
Figure 12: Select a Destination and Extract.....	41
Figure 13: Windows Menu.....	43
Figure 14: Device Manager Window.....	44
Figure 15: Searching for Device Manager.....	44
Figure 16: Update Drivers Window.....	45
Figure 17: Selecting the Network Adapter in the Device Manager.....	46
Figure 18: Update Driver Software Window.....	47
Figure 19: Browse for Drivers on Your Computer.....	47
Figure 20: Device Manager Window.....	54
Figure 21: Device Manager Window - Network Adapters.....	55
Figure 22: Advanced Properties Window.....	55
Figure 23: Encapsulated Task Offload Window.....	56
Figure 24: Encapsulation Overhead Window.....	57
Figure 25: Energy-Efficient Ethernet Window.....	58
Figure 26: Flow Control Window.....	60
Figure 27: Forward Error Correction Window.....	62
Figure 28: Interrupt Moderation Window.....	64
Figure 29: Interrupt Moderation Configuration Window.....	65
Figure 30: Jumbo Packet Window.....	66
Figure 31: Large Send Offload v2 (IPv4) Window.....	67
Figure 32: Large Send Offload (IPv6) Window.....	68
Figure 33: Locally Administered Address Window.....	70
Figure 34: Maximum Number of MSI-X Messages Event Window.....	72
Figure 35: Maximum Number of RSS Processors Window.....	73
Figure 36: Maximum Number of RSS Queues Window.....	74
Figure 37: Maximum RSS Processor Number Window.....	75
Figure 38: Network Direct Functionality Window.....	76
Figure 39: Network Direct Technology Window.....	77
Figure 40: NVGRE Encapsulated Task Offload Window.....	78
Figure 41: Packet Direct Window.....	79
Figure 42: Preferred NUMA Node Window.....	80
Figure 43: Priority & VLAN Window.....	81
Figure 44: PTP Hardware Timestamp Window.....	83
Figure 45: Quality of Service Window.....	84
Figure 46: Receive Buffers Window.....	85
Figure 47: Receive Side Scaling Window.....	86
Figure 48: Receive Segment Coalescing (IPv4) Window.....	87
Figure 49: Receive Segment Coalescing (IPv6) Window.....	89

Figure 50: RoCE MTU Window.....	91
Figure 51: RSS Base Processor Group Window .....	92
Figure 52: RSS Base Processor Number Window .....	93
Figure 53: RSS Load Balancing Profile Window.....	94
Figure 54: RSS Max Processor Group Window.....	96
Figure 55: Software Timestamp Window .....	97
Figure 56: Speed & Duplex Window .....	99
Figure 57: SR-IOV Window.....	101
Figure 58: TCP/UDP Checksum Offload (IPv4) Window .....	102
Figure 59: TCP/UDP Checksum Offload (IPv6) Window .....	104
Figure 60: Transmit Buffers Window.....	106
Figure 61: UDP Segmentation Offload (IPv4) Window .....	107
Figure 62: UDP Segmentation Offload (IPv6) Window .....	108
Figure 63: VF Spoofing Protection Window .....	109
Figure 64: Virtual Machine Queues Window.....	110
Figure 65: Virtual Switch RSS Window.....	111
Figure 66: VLAN ID Window .....	112
Figure 67: VXLAN Encapsulated Task Offload Window .....	113
Figure 68: Device Manager Shortcut Menu .....	117
Figure 69: Deleting the Driver Software.....	118

# Tables

---

Table 1. ANC10 Network Interface Card Series .....	18
Table 2. ANC10Sa/2 LED Status .....	21
Table 3. ANC10T/2 Link and Activity LEDs .....	23
Table 4. Physical Specifications .....	121
Table 5. Environmental Specifications .....	122
Table 6. Operating Voltages and Maximum Power Consumption .....	122
Table 7. Compliance Requirements .....	123



# Preface

---

This guide contains instructions on how to install and configure the ANC10 Network Interface Card Series.

The Preface discusses the following topics:

- ❑ “Safety Symbols Used in this Document” on page 14
- ❑ “Contacting Allied Telesis” on page 15

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

- ❑ ANC10Sa/2
- ❑ ANC10T/2

## 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 Services & Support section of the Allied Telesis web site at **[www.alliedtelesis.com/support](http://www.alliedtelesis.com/support)**. You can find links for the following services on this page:

- ❑ Helpdesk (Support Portal) - Log onto Allied Telesis 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.
- ❑ Software Downloads - Download the latest software releases for your product.
- ❑ Licensing - Register and obtain your License key to activate your product.
- ❑ Product Documents - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- ❑ Warranty - View a list of products to see if Allied Telesis warranty applies to the product you purchased and register your warranty.
- ❑ Allied Telesis Helpdesk - Contact a support representative.

To contact a sales representative or find Allied Telesis office locations, go to **[www.alliedtelesis.com/contact](http://www.alliedtelesis.com/contact)**.





## Chapter 1

# Introduction

---

This chapter provides an introduction to the ANC10 Series network interface card and discusses the following topics:

- ❑ “Functional Description” on page 18
- ❑ “ANC10Sa/2 Network Interface Card SFP+ Ports” on page 19
- ❑ “ANC10T/2 Network Interface Card Twisted Pair Copper Ports” on page 22
- ❑ “Features” on page 24

## Functional Description

---

The ANC10 Network Interface Card Series features Ethernet with dual 1/10Gbps ports and x8 PCI-Express 3.0-compliant buses. The network interface cards provide standard Ethernet functionality along with features designed for virtualization environments, including VMware Direct Path and SR-IOV. The basic characteristics of the network interface cards are listed in Table 1.

Table 1. ANC10 Network Interface Card Series

Adapter	Ports	Speed	Cable Type	Maximum Distance	Bus Connector
ANC10Sa/2	2 SFP+	10G/1G	Varies by SFP+ transceiver	Varies by SFP+ transceiver	PCIe x8 (Gen 3)
ANC10T/2	2 RJ45	10G	CAT6A or better	100m	PCIe x8 (Gen 3)
		1G	CAT5e or CAT6A or better		

---

### Note

The maximum operating distance of the SFP+ ports on the ANC10Sa/2 network interface card depends on the transceivers. Refer to the product's data sheet on the Allied Telesis web site for a list of supported transceivers.

---

## ANC10Sa/2 Network Interface Card SFP+ Ports

---

The ANC10Sa/2 network interface card has two SFP+ ports for 1Gbps or 10Gbps SFP+ transceivers. The network interface card can set the speeds of the ports automatically or you can set them manually with Advanced Properties. Each SFP+ port has two LEDs that display link and activity states.

The maximum operating distance of an SFP+ port will vary depending on the SFP+ transceiver and type of fiber optic cabling.

The ports support the following types of transceivers:

---

**Note**

See the Allied Telesis website for supported SFP+ models.

---

- 1Gbps short and long distance SFP transceivers using multi-mode or single mode fiber optic cable.
- 10Gbps short and long distance SFP+ transceivers using multi-mode or single mode fiber optic cable.
- 10Gbps series of direct connect twinax cables.
- 10Gbps copper-based SFP+ with RJ-45 connector.

---

**Note**

ANC10Sa/2 does not support the use of two copper-based SFP+ modules at the same time. Customers who want dual RJ-45 ports should use the ANC10T/2 network interface card.

---

---

**Note**

The ANC10Sa/2 network interface card does not support the 7 meter SP10TW7 direct connect twinax cable.

---

Guidelines for the ports are listed here:

- They do not support 100Mbps-FX transceivers.
- They support full-duplex mode only.
- The network interface card can set the speed automatically with Auto-Negotiation or you can set it manually with Advanced Properties. The default is Auto-Negotiation.

The ANC10Sa/2 network interface card has a PCIe x8 motherboard bus interface as shown in Figure 1.

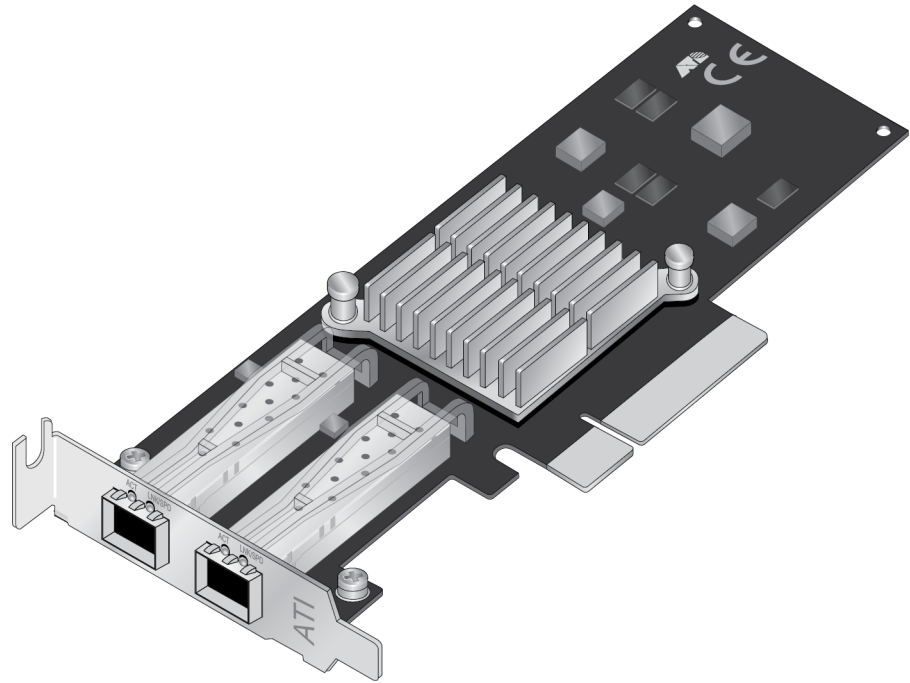


Figure 1. ANC10Sa/2 Network Interface Card

---

**Note**

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

---

The ANC10Sa/2 network interface card faceplate is shown in Figure 2.

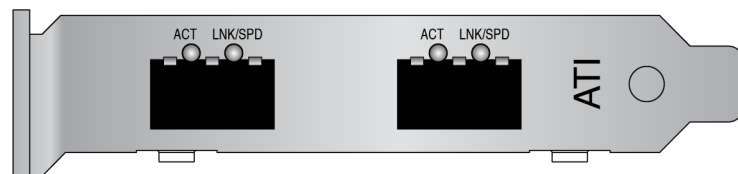


Figure 2. ANC10Sa/2 Network Interface Card Faceplate

Table 2 describes the LED states.

Table 2. ANC10Sa/2 LED Status

<b>Ports</b>	<b>Port LED</b>	<b>LED State</b>	<b>Description</b>
SFP+	ACT	Flashing Green	The port is receiving or transmitting network packets.
		Off	The port is not receiving or transmitting any packets.
	LNK/SPD	Green Steady On	The transceiver has established a 10Gbps link to a remote device.
		Amber Steady On	The transceiver has established a 1Gbps link to a remote device.
		Off	The port has not established a link.

## ANC10T/2 Network Interface Card Twisted Pair Copper Ports

The ANC10T/2 network interface card has two 1/10Gbps copper ports. The card uses Auto-Negotiation to automatically set port speed and supports full-duplex mode only. Each port has two status LEDs.

The network interface card has a PCIe x8 motherboard bus connector as shown in Figure 3.

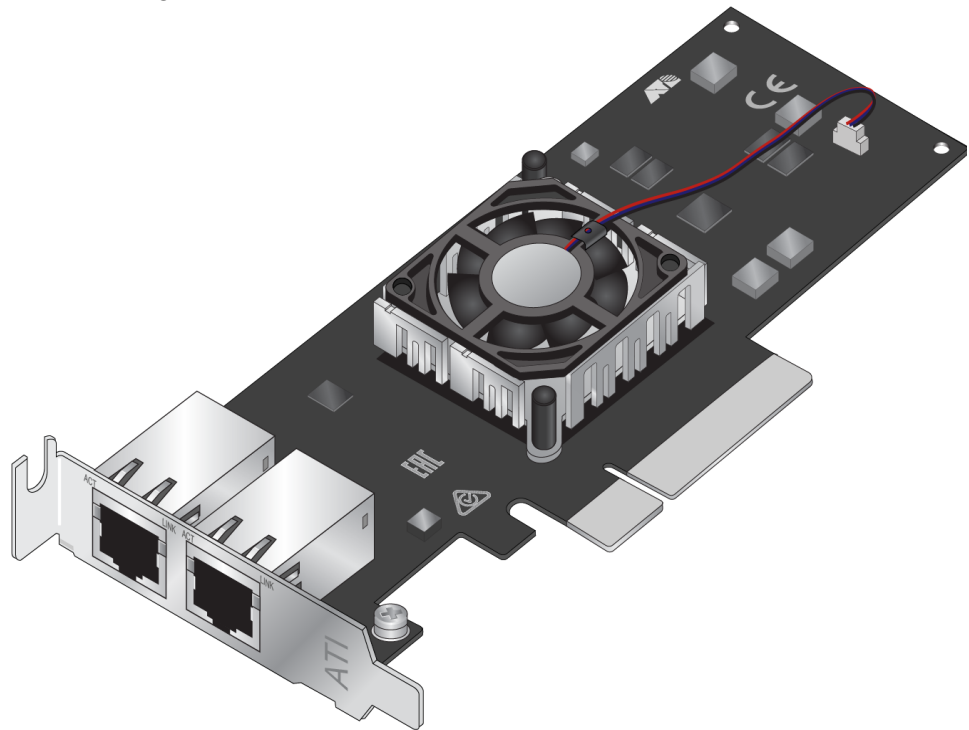


Figure 3. ANC10T/2 Network Interface Card

The ANC10T/2 network interface card front panel is shown in Figure 4.

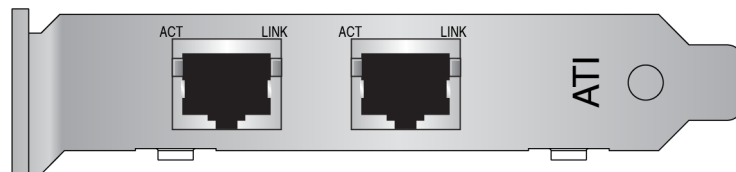


Figure 4. ANC10T/2 Network Interface Card Faceplate

The minimum cable requirements are listed here:

- 1Gbps - 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 ports are described in Table 3.

Table 3. ANC10T/2 Link and Activity LEDs

<b>Ports</b>	<b>Port LEDs</b>	<b>LED State</b>	<b>Network State</b>
Copper Port 1 & Port 2	ACT	Green Blinking	The port is transmitting or receiving network traffic.
		Off	The port is not receiving or transmitting any packets.
	LNK	Green Steady On	The port has established a 10Gbps link to a remote device.
		Amber Steady On	The port has established a 1Gbps link to a remote device.
		Off	The port has not established a link.

## Features

---

The following features apply to the ANC10 Network Interface Card Series:

- Encapsulated Task Offload
- Encapsulation Overhead
- Energy Efficient Ethernet
- Flow Control
- Forward Error Correction
- Interrupt Moderation (low/medium/high)
- Jumbo Frames (9174 bytes)
- Large Send Offload V2 (IPv4 and IPv6)
- Configurable Locally Administered Address
- MSI-X Messages (16 - 511)
- Receive Side Scaling
- Network Direct (RDMA) with RoCEv2
- NVGRE Encapsulated Task Offload
- Packet Direct
- NUMA Scaling (closest processor, closest processor static, conservative scaling, NUMA Scaling, NUMA Scaling Static)
- Priority and VLAN
- PTP Hardware Timestamp
- Quality of Service
- Receive buffers (up to 15000)
- Receive Segment Coalescing (IPv4 and IPv6)
- RoCE MTU up to 4096 Bytes
- Software Timestamp
- Speed and Duplex options (Auto/1.0 Gig Full Duplex/10.0 Gig Full Duplex)
- SR-IOV (up to 128 Virtual Functions)
- TCP/UDP Checksum Offload (IPv6 and IPv6)
- Transmit Buffers (Auto configured or up to 5000)
- UDP Segmentation Offload (IPv4 and IPv6)
- VF Spoofing Protection
- Virtual Machine Queues
- Virtual Switch Receive Side Scaling
- VLAN ID tagging



- ❑ VXLAN Encapsulated Task Offload
- ❑ Data Center Bridging
- ❑ PXE Boot (EFI and Legacy)
- ❑ iSCSI Boot (Legacy only)
- ❑ NIC Partitioning (up to 8 partitions per port)
- ❑ RDMA (remote direct memory access)

**Software** The ANC10 Network Interface Card Series supports the following operating systems:

- ❑ Linux®
  - RHEL7.x, RHEL6.x, OLE6.x UEK, SLES12, SLES11SP1 and newer
  - Most 3.x/4.x kernels and some 2.6 kernels starting from 2.6.32
- ❑ VMware®
  - ESX 6.0
  - ESX 6.5
  - ESX 6.7
  - ESX 7.0
- ❑ Windows®
  - Windows 2019
  - Windows 10



## Chapter 2

# Installing the Hardware

---

This chapter describes how to install the ANC10 Network Interface Card Series in a computer and discusses the following topics:

- ❑ “Reviewing Safety Precautions” on page 28
- ❑ “Pre-Installation Checklist” on page 30
- ❑ “Installing the Standard Bracket on the Network Interface Card” on page 31
- ❑ “Installing the Network Interface Card” on page 33
- ❑ “Installing SFP+ Transceivers in the ANC10Sa/2 Network Interface Card” on page 35

## 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](http://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](http://www.alliedtelesis.com/library).



**Warning**

This is a Class 1 Laser product. ⚡ L1

---



**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 stare into the laser beam. ⚡ L2

---



**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 35 degrees C. ⚡ E7

---

---

**Note**

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

---

**Warning**

The network interface card 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 network interface card, perform the following procedure:

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 the system shutdown is complete, unplug the power cord.
6. Holding the network interface card by the edges, remove it from its shipping package and place it on an antistatic surface.
7. Check the network interface card for visible signs of damage, particularly on the card's edge connector.

---

### **Note**

Do not attempt to install a damaged network interface card. If the card is damaged, report it to Allied Telesis. See "Contacting Allied Telesis" on page 15.

---

## Installing the Standard Bracket on the Network Interface Card

---

The network interface card is shipped with the low-profile bracket already installed. A standard bracket is included with the network interface card. Depending on your system, you may need to replace the bracket attached to your card.

The following procedure describes how to remove the low-profile bracket from the card 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 two screws that attach the bracket to the network interface card. See Figure 5.

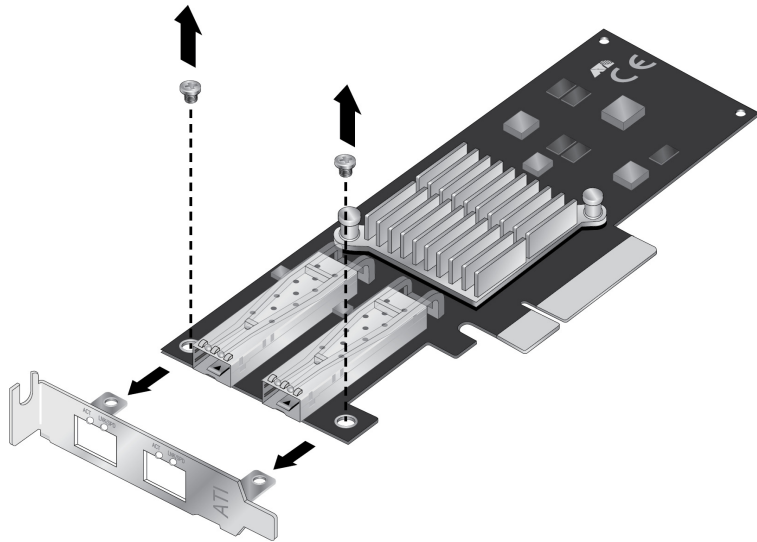


Figure 5. Removing the Low-profile Bracket

2. Align the tabs of the standard bracket with the holes on the network interface card and fasten the screws onto the card. See Figure 6 on page 32.

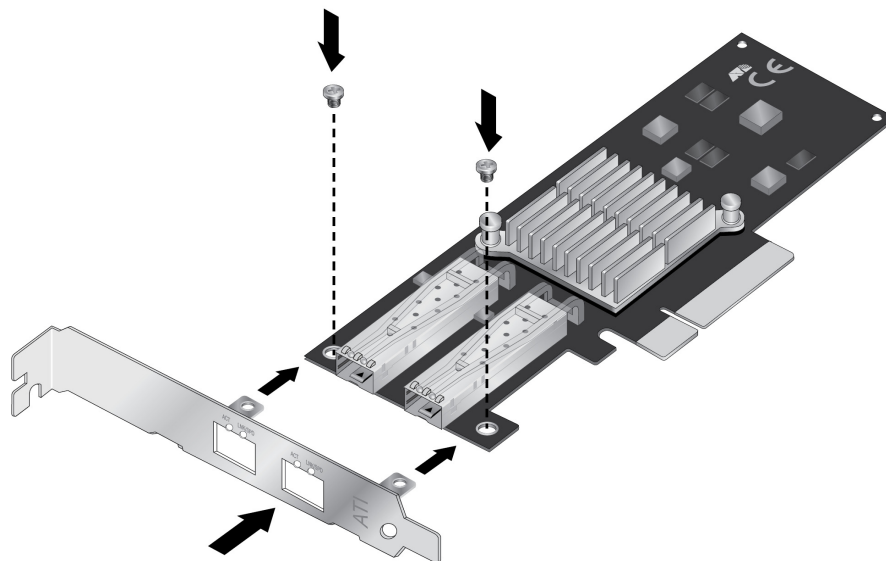


Figure 6. Installing the Standard Bracket



## Installing the Network Interface Card

---

The following installation instructions apply to most systems. For details about performing the tasks on your particular system, refer to the manuals that were supplied with your system.

---

### Note

The ANC10 Network Interface Card Series requires a system with an available PCIe x8 slot.

---



---

### Warning

The network interface card 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. *or* **E39**
- 

To install the network interface card, do the following:

1. Review the “Pre-Installation Checklist” on page 30 and “Reviewing Safety Precautions” on page 28.

Before installing the network interface card, verify that the computer is powered OFF and that the power cord is unplugged from the power outlet. You should also be sure to follow all proper electrical grounding procedures.

2. Remove the system cover.
3. Select an empty, non-shared PCIe port and remove the faceplate.

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

---

**Note**

If you cannot locate or do not know how to find an appropriate PCIe port, refer to the documentation that came with your system.

---

4. Remove the network interface card from the shipping package and store the packaging material in a safe location.
5. Applying even pressure at both corners of the card, push the network interface card until it is firmly seated in the appropriate PCIe port. Make sure the card is securely seated.

**Caution**

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

---

6. Secure the network interface card to the chassis with a Phillips-head screw (not provided) or the system's built-in latching mechanism.
7. Replace the system's cover.
8. Go to "Installing SFP+ Transceivers in the ANC10Sa/2 Network Interface Card" on page 35 or "Connecting Twisted-Pair Copper Cables to the ANC10T/2 Network Interface Card" on page 36.
9. Power on the system.

Download the driver from the Allied Telesis web site. For instructions on how to install the driver on Linux or VMware systems, refer to the README file included with the driver. For instructions on loading the driver on a Microsoft Windows system, refer to Chapter 3, "Installing the Windows Driver Software" on page 37

## Installing SFP+ Transceivers in the ANC10Sa/2 Network Interface Card


---

Here are the guidelines to installing and cabling SFP+ transceivers in the ANC10Sa/2 network interface card:

- ❑ SFP+ transceivers can be hot-swapped while the network interface card is powered on. However, you should always disconnect the fiber optic cables first before removing a transceiver.
- ❑ You should install a transceiver in the network interface card before connecting the fiber optic cable.
- ❑ Fiber optic transceivers are dust sensitive. Always keep the plug in the optical bores when a fiber optic cable is not installed, or when you store the transceiver. When you do remove the plug, keep it for future use.
- ❑ Unnecessary removal and insertion of a transceiver can lead to premature failure.
- ❑ The connector on the fiber optic cable should fit snugly into the port on the network interface card, and the tab should lock the connector into place.
- ❑ Do not remove the dust cover from a fiber optic port until you are ready to connect a fiber optic cable. Dust contamination can adversely affect the operation of a fiber optic port.




### Warning

A transceiver can be damaged by static electricity. Be sure to observe all standard electrostatic discharge (ESD) precautions, such as wearing an antistatic wrist strap, to avoid damaging the device.  E86

---



### 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

---

### Note

The cable specifications for the SFP+ transceivers are found in the installation guides that ship with the devices.

---

## Connecting Twisted-Pair Copper Cables to the ANC10T/2 Network Interface Card

---

The ANC10T/2 network interface card has two copper RJ45 ports. To connect the network interface card to the network, you must have a cable with the appropriate connector.

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

1. Prepare a twisted-pair copper cable.
2. Connect one end of the cable to the network interface card.
3. Connect the other end of the cable to the appropriate port on a remote network device.
4. Repeat steps 1 through 3 with the second cable and port.

Download the driver from the Allied Telesis web site. For instructions on how to install the driver on Linux or VMware systems, refer to the README file included with the driver. For instructions on loading the driver on a Microsoft Windows system, refer to Chapter 3, "Installing the Windows Driver Software" on page 37

## Chapter 3

# Installing the Windows Driver Software

---

This chapter describes how to install driver software for the ANC10 Network Interface Card Series onto your Windows operating system. It contains the following topics:

- “Overview” on page 38
- “Downloading the Driver Software” on page 39
- “Accessing the Windows Device Manager” on page 43
- “Installing the Driver Software” on page 45
- “Updating the Driver Software” on page 48
- “Performing the Silent Installation” on page 49

---

**Note**

For instructions on how to install the driver on Linux or VMware systems, refer to the README file included with the driver.

---

## Overview

---

After you install the ANC10Sa/2 or ANC10T/2 network interface card in 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. Otherwise, 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.
- ❑ If your computer installs a default driver for the network interface card, you must update it. 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 39
- ❑ “Accessing the Windows Device Manager” on page 43
- ❑ “Installing the Driver Software” on page 45

Or

- ❑ “Updating the Driver Software” on page 48

### 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 39
- ❑ “Performing the Silent Installation” on page 49

## Downloading the Driver Software

The driver software for the network interface cards is available on the Allied Telesis website. The driver is the same for both network interface cards ANC10 Series.

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 window is displayed as shown in Figure 7.



Figure 7. Software Downloads Window

2. Click **Download Center**.

The Login window appears.

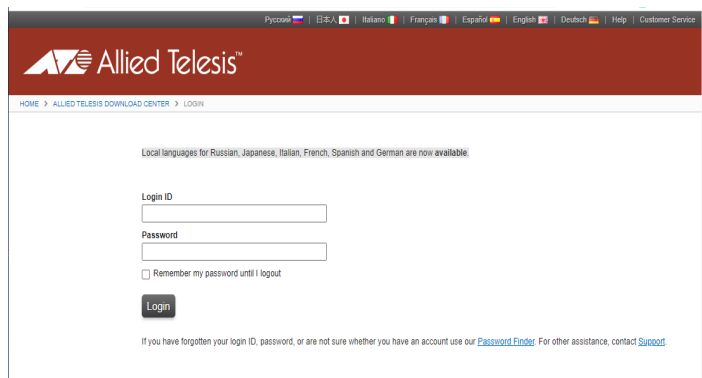


Figure 8. Login Window

3. Enter your Login ID and Password and click **Login**.

4. If you have not established a Login ID and Password, click **Support**.

The support window appears.

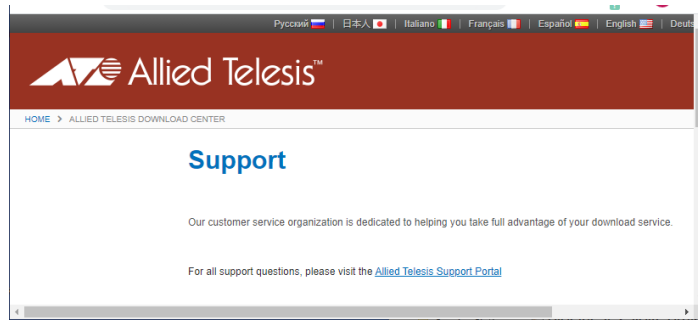


Figure 9. Support Window

5. Click **Allied Telesis Support Portal**.

The Support Portal window appears.

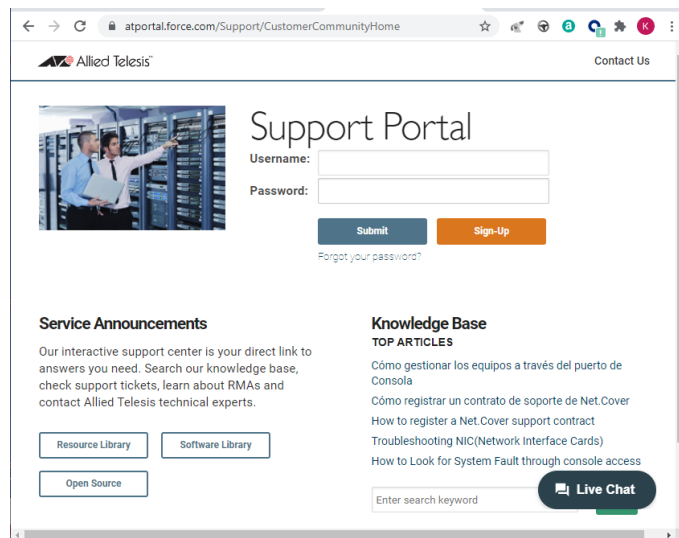


Figure 10. Support Portal Window

6. Click **Sign Up**.

The Register for an Account Window appears.



Register for an Account \* All the fields are required.

**Users Details**

First Name \*

Last Name \*

Company Name \*

Street \*

City \*

State/Province \*

Zip/Postal Code \*

Country \* - Select One -

Website \*

Nickname \*

Phone \* + ( ) - -

Email \*

Time Zone \* - Select One -

Submit Back

Figure 11. Register for an Account Window

7. Complete the form to gain access to the Download Center.
8. Check your email for the access Login ID and password. Allow up to 24 business hours.
9. Go back to the **Download Center**.
10. Select the driver for the ANC10 Series network interface card and your operating system.
11. Save the zip folder onto your system.
12. 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.

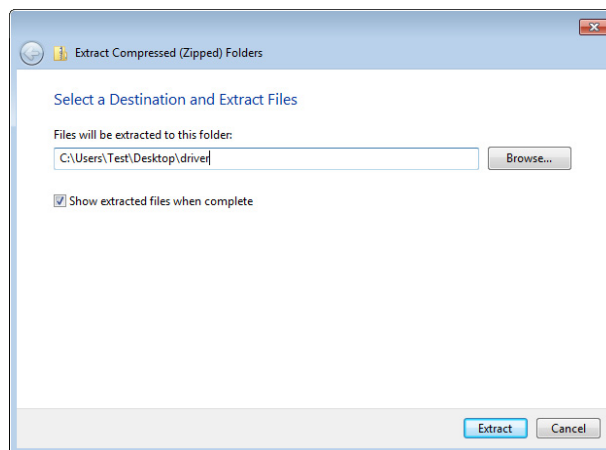


Figure 12. Select a Destination and Extract

13. Specify the location of the folder and click Extract.
14. Record the location of the folder.

## Accessing the Windows Device Manager

---

When you install or update the driver software for the ANC10 Network Interface Card Series on a Windows system, 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.

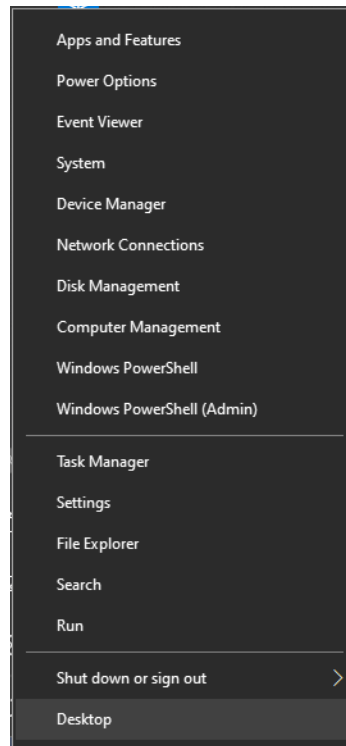


Figure 13. Windows Menu

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

The Device Manager window appears.

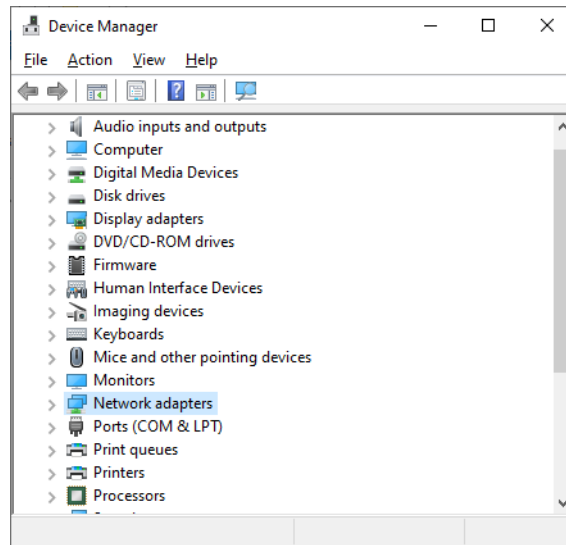


Figure 14. Device Manager Window

### 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.

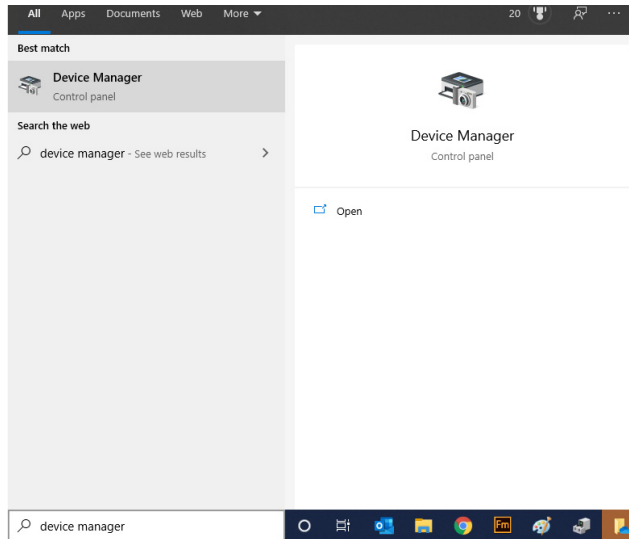


Figure 15. Searching for Device Manager

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

The Device Manager window appears as shown in Figure 14.

## Installing the Driver Software

---

Once you physically install the ANC10 Series network card, the system detects the new hardware and creates an entry in the Device Manager when the Windows operating system boots up. Shortly after you log in, you need to install the driver software for your network interface 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 Windows Device Manager” on page 43.
2. In the Device Manager window, double-click **Network Adapters** to expand the field.
3. **Option 1** - To have Windows search the computer for the driver, do the following:
  - a. Right-click on **AT- ANC10Sa/2 (or AT-ANC10T/2) 10G Dual Port 10BASE-T Adapter**.
  - b. Select **Update Driver**.

The Update Drivers window appears. See Figure 16 as an example.

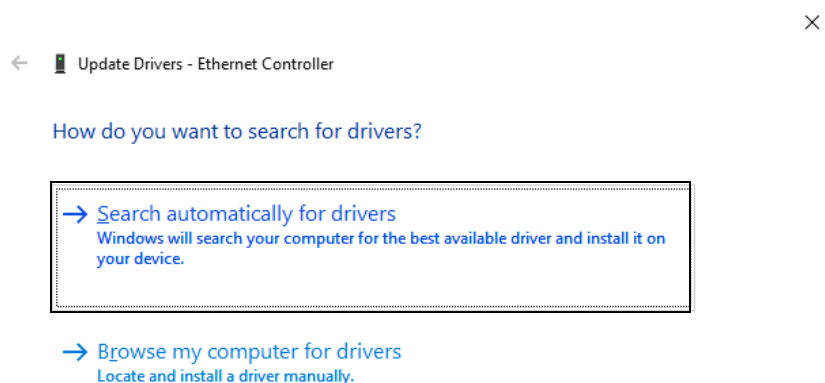


Figure 16. Update Drivers Window

- c. Select **Search automatically for updated drivers**.

Windows will search the computer for the driver. It displays a confirmation prompt after installing the driver.

**Option 2** - To manually identify the driver yourself, do the following:

- a. Right-click on **AT- ANC10Sa/2 (or AT-ANC10T/2) 10G Dual Port 10BASE-T Adapter**.

---

**Note**

The Device Manager may identify the new network interface card as an Ethernet Controller, Broadcom device, or Allied Telesis device.

---

The shortcut menu appears. See Figure 17 as an example.

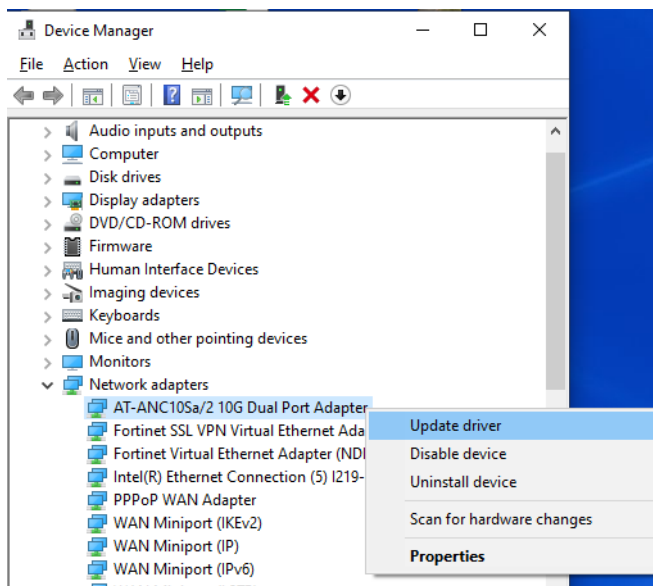


Figure 17. Selecting the Network Adapter in the Device Manager

- b. Select **Update Driver**.

The Update Driver window appears. See Figure 18 on page 47 as an example.

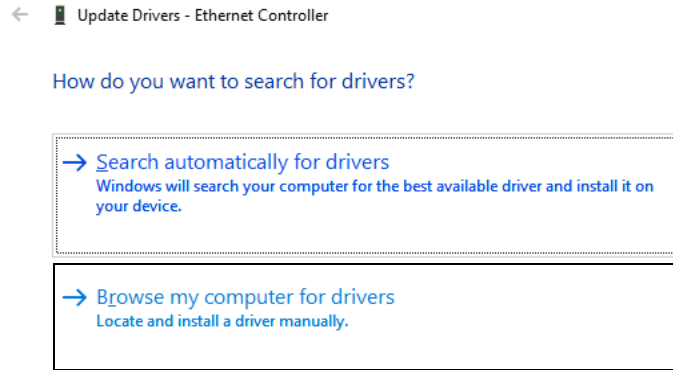


Figure 18. Update Driver Software Window

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 19 as an example.

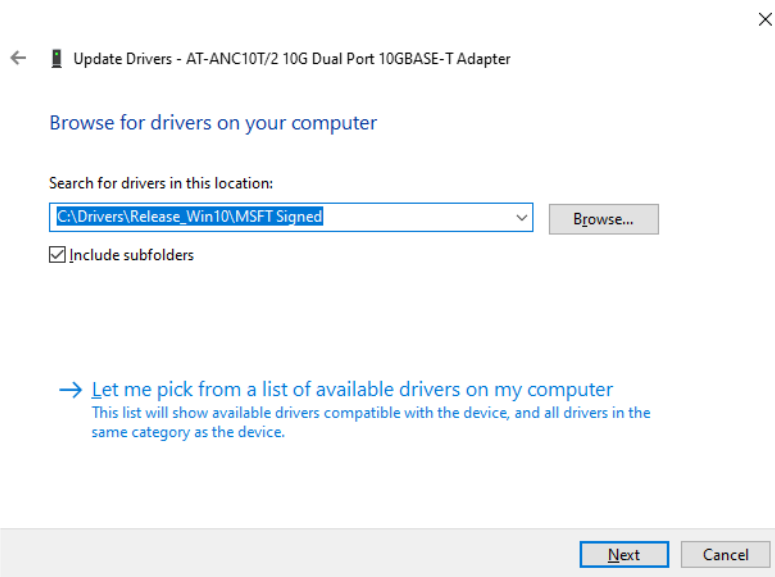


Figure 19. Browse for Drivers on Your Computer

4. Specify the folder where you stored the driver after downloading it from the Allied Telesis web site. See “Downloading the Driver Software” on page 39 for details.

5. Click **Next**.

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

6. Click **Close**.

## Updating the Driver Software

---

Allied Telesis may periodically post updates to the driver software for network interface cards on its web site. To obtain the latest version of the ANC10 Network Interface Card Series driver, see “Downloading the Driver Software” on page 39.

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 network interface card that the Device Manager detects and lists.

The Device Manager lists your network interface card entry as *AT-ANC10Sa/2 (or AT-ANC10T/2) 10G Dual Port 10BASE-T Adapter* once you installed the driver software. Before you installed the driver software, the Device Manager may list your network interface card entry as an Ethernet Controller, Broadcom device, or Allied Telesis device.

To update the driver software for your network interface card, see “Installing the Driver Software” on page 45.



## Performing the Silent Installation

---

To simplify the driver installation process, you may perform a silent installation of the driver software for the network interface card. 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 network interface cards are all Microsoft certified.

---

Use a command line utility called Driver Package Installer (DPIInst) for the silent installation. DPIInst is included in the Windows Developer Kit (WDK) provided by Microsoft. You can obtain the latest DPIInst 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 the driver software for the network interface card.

See "Downloading the Driver Software" on page 39.

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 `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” on page 53
- ❑ “Accessing Advanced Properties” on page 54
- ❑ “Encapsulated Task Offload” on page 56
- ❑ “Encapsulation Overhead” on page 57
- ❑ “Energy-Efficient Ethernet” on page 58
- ❑ “Flow Control” on page 60
- ❑ “Forward Error Correction” on page 62
- ❑ “Interrupt Moderation” on page 64
- ❑ “Interrupt Moderation Configuration” on page 65
- ❑ “Jumbo Packet” on page 66
- ❑ “Large Send Offload v2 (IPv4)” on page 67
- ❑ “Large Send Offload v2 (IPv6)” on page 68
- ❑ “Locally Administered Address” on page 70
- ❑ “Maximum Number of MSI-X Messages” on page 72
- ❑ “Maximum Number of RSS Processors” on page 73
- ❑ “Maximum Number of RSS Queues” on page 74
- ❑ “Maximum RSS Processor Number” on page 75
- ❑ “Network Direct Functionality” on page 76
- ❑ “Network Direct Technology” on page 77
- ❑ “NVGRE Encapsulated Task Offload” on page 78
- ❑ “Packet Direct” on page 79
- ❑ “Preferred NUMA Node” on page 80
- ❑ “Priority & VLAN” on page 81
- ❑ “PTP Hardware Timestamp” on page 83
- ❑ “Quality of Service” on page 84
- ❑ “Receive Buffers (0=Auto)” on page 85
- ❑ “Receive Side Scaling” on page 86
- ❑ “Recv Segment Coalescing (IPv4)” on page 87
- ❑ “Recv Segment Coalescing (IPv6)” on page 89

- ❑ “RoCE MTU” on page 91
- ❑ “RSS Base Processor Group” on page 92
- ❑ “RSS Base Processor Number” on page 93
- ❑ “RSS Load Balancing Profile” on page 94
- ❑ “RSS Max Processor Group” on page 96
- ❑ “Software Timestamp” on page 97
- ❑ “Speed & Duplex” on page 99
- ❑ “SR-IOV” on page 101
- ❑ “TCP/UDP Checksum Offload (IPv4)” on page 102
- ❑ “TCP/UDP Checksum Offload (IPv6)” on page 104
- ❑ “Transmit Buffers (0=Auto)” on page 106
- ❑ “UDP Segmentation Offload (IPv4)” on page 107
- ❑ “UDP Segmentation Offload (IPv6)” on page 108
- ❑ “VF Spoofing Protection” on page 109
- ❑ “Virtual Machine Queues” on page 110
- ❑ “Virtual Switch RSS” on page 111
- ❑ “VLAN ID” on page 112
- ❑ “VXLAN Encapsulated Task Offload” on page 113

## Overview

---

The ANC10 Series of network interface cards allow you to modify advanced properties to meet your requirements. To access the advanced properties, access Device Manager, then go to each advanced property window.

**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 network interface card, and select a feature.

1. Access the Device Manager. See “Accessing the Windows Device Manager” on page 43.
2. In the Device Manager window, click **Network Adapters**. Refer to Figure 20.

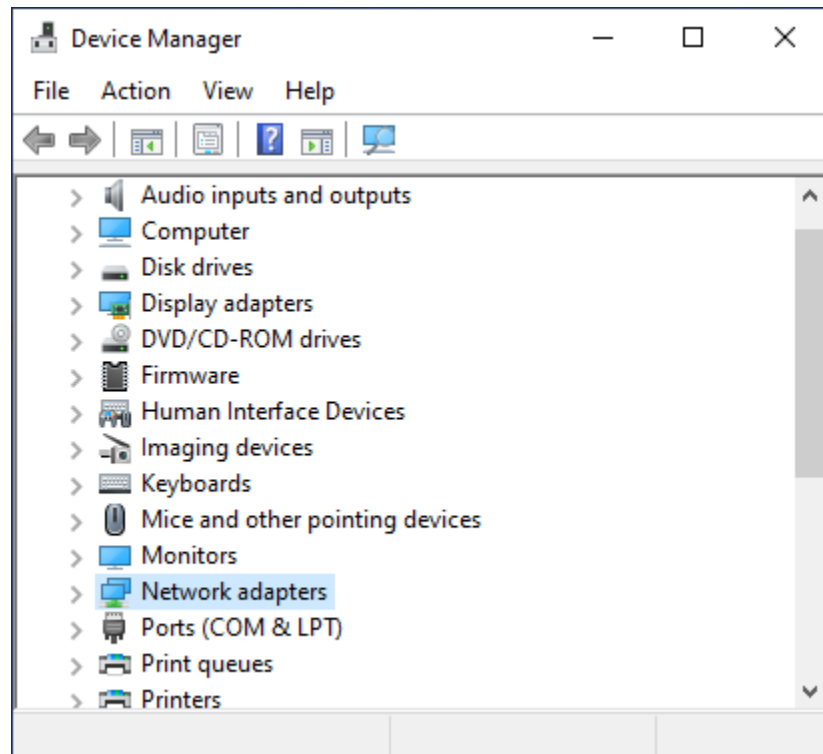


Figure 20. Device Manager Window

3. Double-click **AT-ANC10Sa/2 (or AT-ANC10T/2) 10G Dual Port Adapter**. Refer to Figure 21.

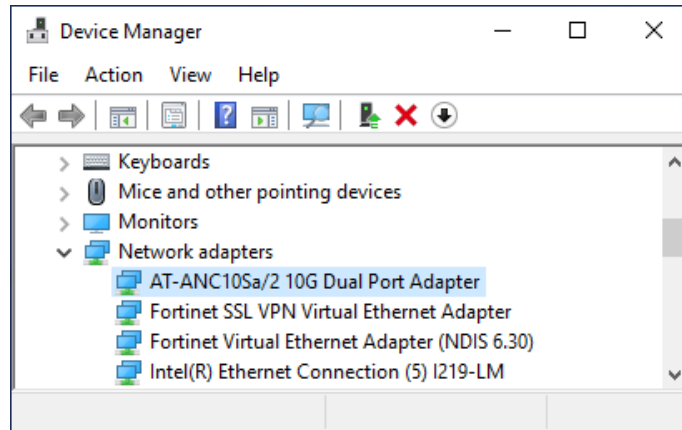


Figure 21. Device Manager Window - Network Adapters

The properties window pops up.

4. Click the **Advanced** tab.

The Advanced Properties window opens as shown in Figure 22.

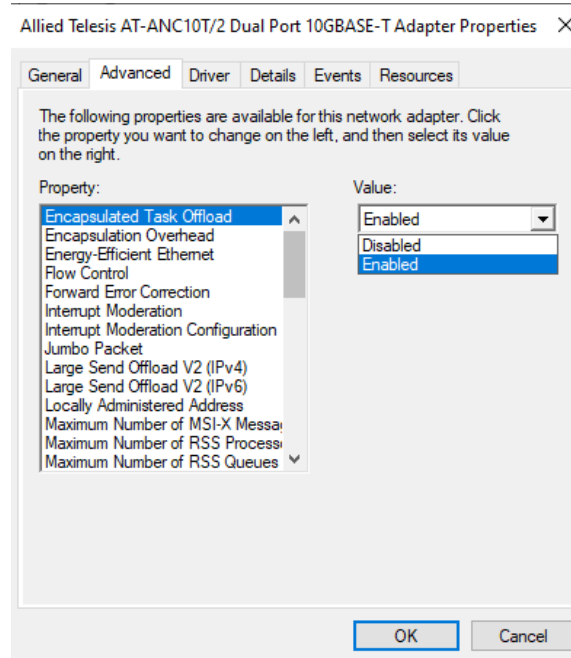


Figure 22. Advanced Properties Window

## Encapsulated Task Offload

The Encapsulated Task Offload property allows the network adapter to perform offload operations such as large send offload (LSO) and virtual machine queue (VMQ) on the inner header for encapsulated packets. Network performance may be degraded by running this cmdlet.

To view the Encapsulated Task Offload feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Encapsulated Task Offload** in the Property box.

The Encapsulated Task Offload window is displayed as shown in Figure 23.

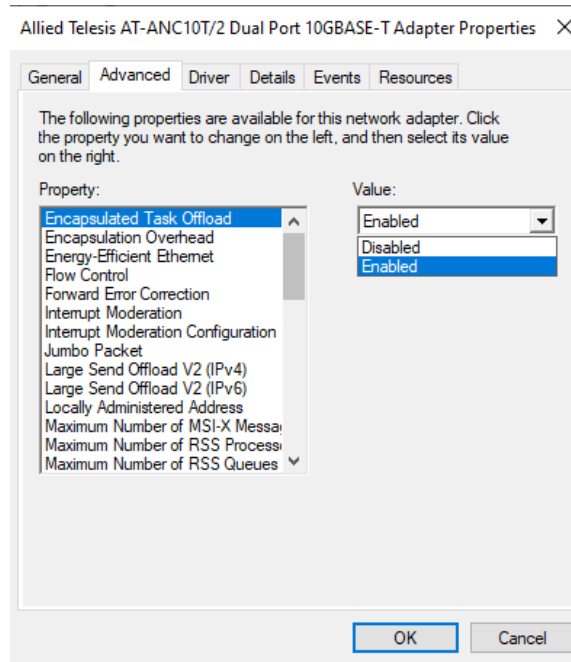


Figure 23. Encapsulated Task Offload Window

3. Select one of the following options:

- Disabled** — This setting disables the Encapsulated Task Offload.
- Enabled** — This setting enables Encapsulated Task Offload. This setting is the default.

4. Click **OK**.



## Encapsulation Overhead

---

The Encapsulation Overhead property defines the amount of overhead required in Ethernet frames due to virtual network overlay encapsulation such as VXLAN and NVGRE.

To view the Encapsulation Overhead feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Encapsulation Overhead** in the Property box.

The Encapsulation Overhead window is displayed as shown in Figure 24.

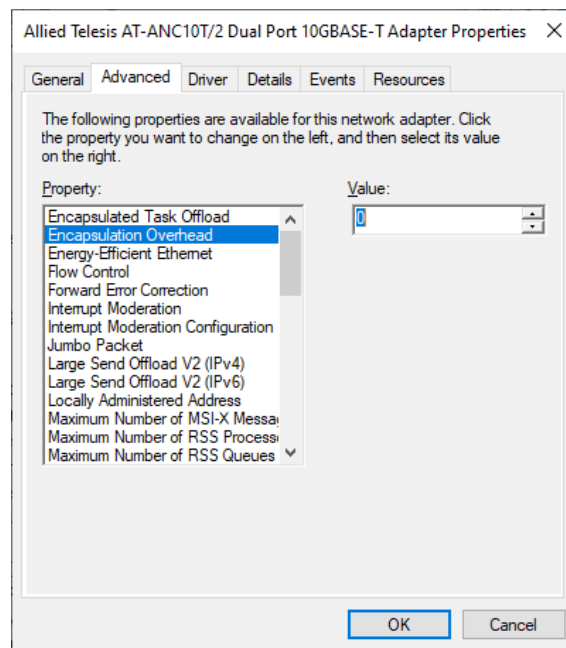


Figure 24. Encapsulation Overhead Window

3. Select a value. Valid range is 0 through 256 with step of 32. For example 0, 32, 64, 96, 128, etc. are valid values.
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 the copper ports on the ANC10T/2 network interface card.

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

1. Access the Advanced Properties.  
See “Accessing Advanced Properties” on page 54.
2. Select **Energy-Efficient Ethernet** in the Property box.

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

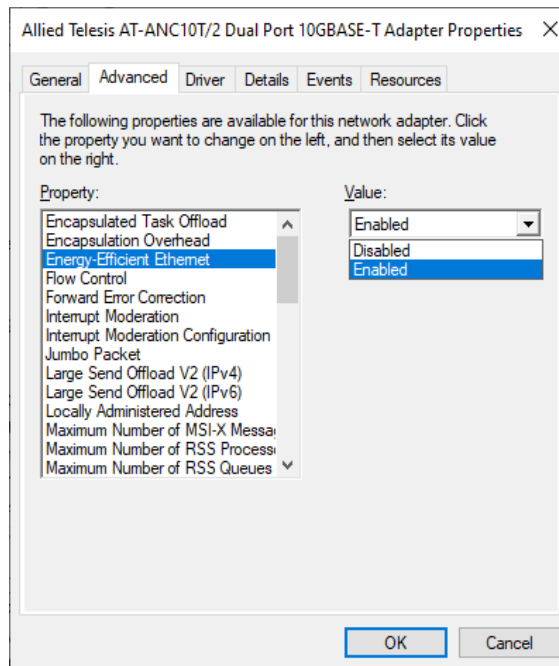


Figure 25. Energy-Efficient Ethernet Window

3. Select one of the following options:
  - Disabled** — This setting disables Energy-Efficient Ethernet on the ports of the ANC10T/2 network interface card.
  - Enabled** — This setting enables Energy-Efficient Ethernet on the ports of the ANC10T/2 network interface card.
4. Click **OK**.

## Flow Control

The Flow Control property allows you to control the flow between the ANC10 network interface card port and its link partner. You can enable or disable the network interface card 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 54.

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

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

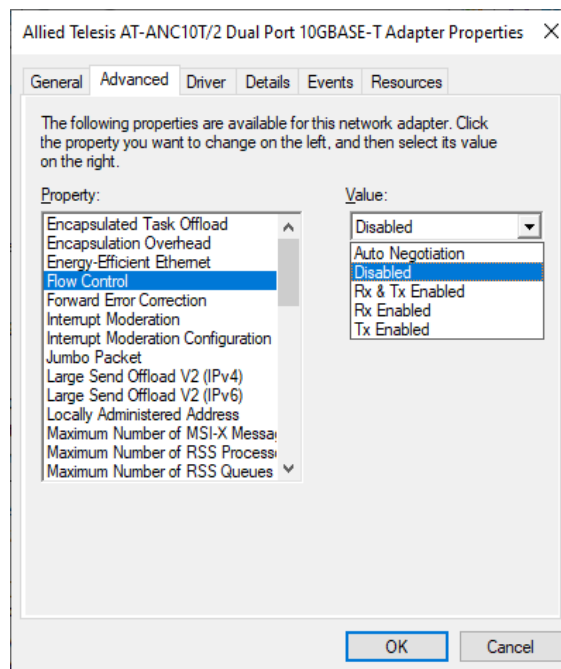


Figure 26. Flow Control Window

3. Select one of the following options if available:
  - Auto Negotiation** — The network interface card uses flow control if it receives PAUSE frames on its ports from its link partner. Otherwise, the network interface card does not use flow control. This is the default.
  - Disabled** — The network interface card ignores PAUSE frames.
  - Tx & Rx Enabled** — The network interface card processes ingress PAUSE frames and transmits PAUSE frames.

- ❑ **Rx Enabled** — The network interface card processes ingress PAUSE frames, but does not transmit PAUSE frames.
- ❑ **Tx Enabled** — The network interface card transmits PAUSE frames, but ignores ingress PAUSE frames.

4. Click **OK**.

## Forward Error Correction

The Forward Error Correction property allows for errors in the received packet to be corrected without the need for a packet re-transmission.

To specify or change the Forward Error Correction feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Forward Error Correction** in the Property box.

The Forward Error Correction window is displayed as shown in Figure 27.

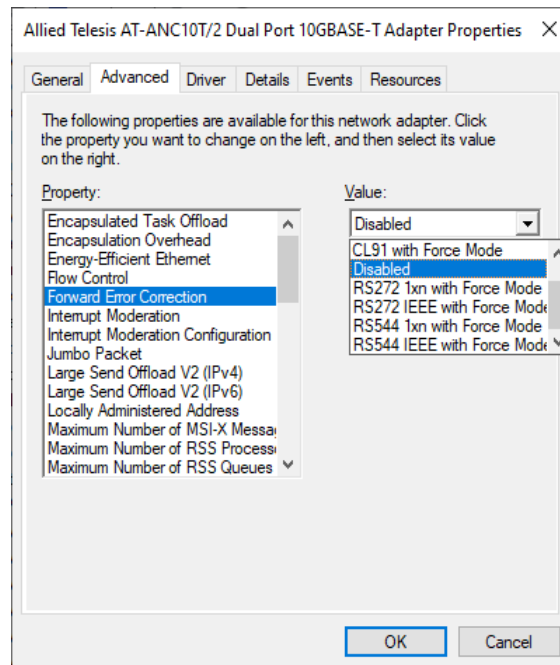


Figure 27. Forward Error Correction Window

3. Select one of the following options:

- Disabled** — This is the default.
- CL91 with Force Mode**
- RS272 1xn with Force Mode**
- RS272 IEEE with Force Mode**
- RS544 1xn with Force Mode**
- RS544 IEEE with Force Mode**

4. Click **OK**.

## Interrupt Moderation

The Interrupt Moderation property 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 54.
2. Select **Interrupt Moderation** in the Property box.

The Interrupt Moderation window is displayed as shown in Figure 28.

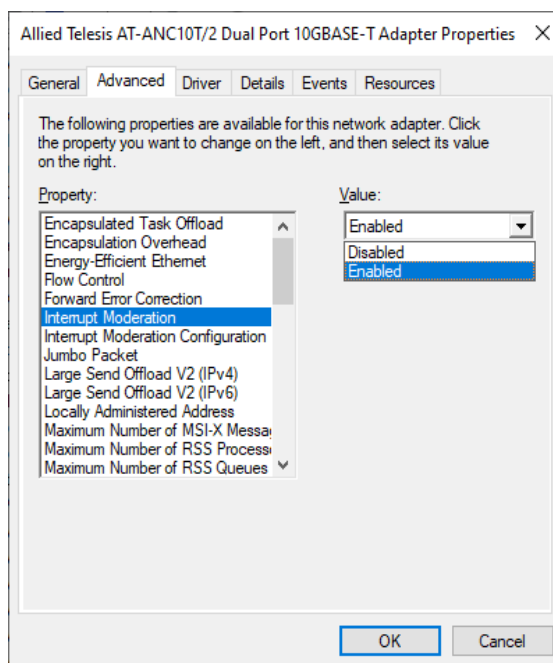


Figure 28. Interrupt Moderation Window

3. Select one of the following options:
  - Disabled** — The Interrupt Moderation feature is disabled. The network interface card 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 Configuration

The Interrupt Moderation Configuration property sets the level of interrupt moderation.

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

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

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

The Interrupt Moderation Rate window is displayed as shown in Figure 29.

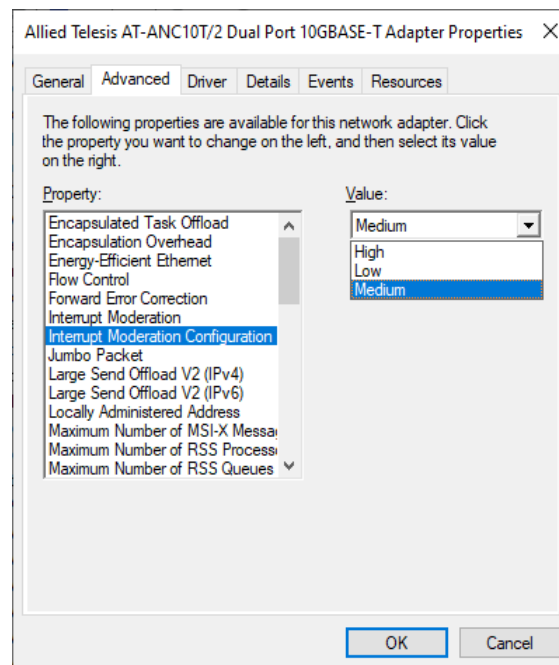


Figure 29. Interrupt Moderation Configuration Window

3. To set the level of interrupt moderation, select one of the following options:

- High**
- Low**
- Medium** — This is the default setting.

4. Click **OK**.

## Jumbo Packet

---

The Jumbo Packet property enables the network interface card to transmit and receive oversized Ethernet frames that are greater than 1500 bytes, but less than or equal to 9336 bytes in length. 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 54.
2. Select **Jumbo Packet** in the Property box.

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

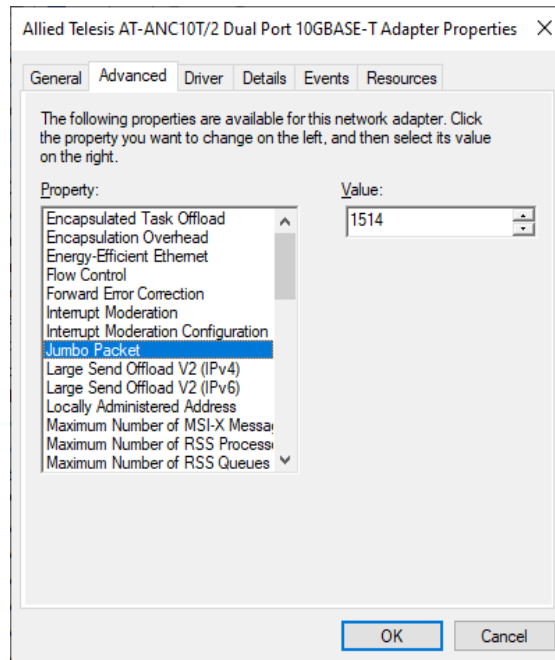


Figure 30. Jumbo Packet Window

3. Select the desired jumbo frame size from the list. The options are:
  - 1514 bytes. This is the default setting.
  - 4088 bytes.
  - 9014 bytes.
  - 9336 bytes.
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 interface card. 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 54.
2. Select **Large Send Offload v2 (IPv4)** in the Property box.

The Large Send Offload v2 (IPv4) window is displayed as shown in Figure 31.

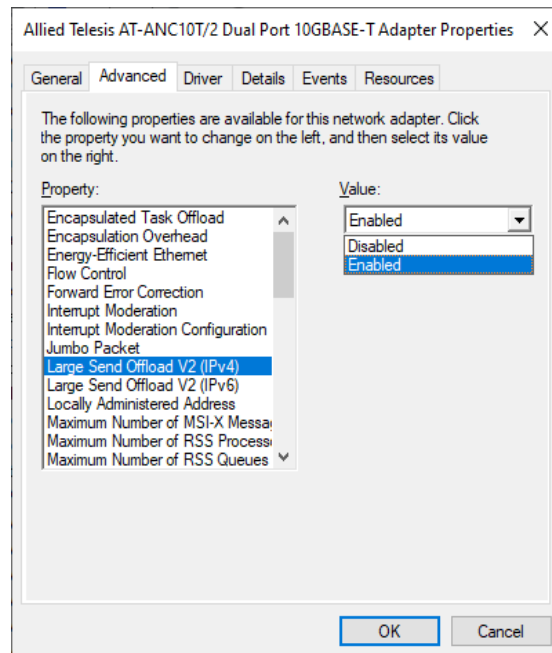


Figure 31. Large Send Offload v2 (IPv4) Window

3. Select one of the following options:
  - Disabled** — The feature is disabled.
  - Enabled** — The network interface card port segments large packets up to 256Kb for IPv4 traffic before sending them out. This is the default setting.
4. Click **OK**.

## Large Send Offload v2 (IPv6)

The Large Send Offload v2 (IPv6) property allows you to control the load of sending out large packets. When this feature is enabled, the network interface card 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 54.
2. Select **Large Send Offload v2 (IPv6)** in the Property box.

The Large Send Offload v2 (IPv6) window is displayed as shown in Figure 32.

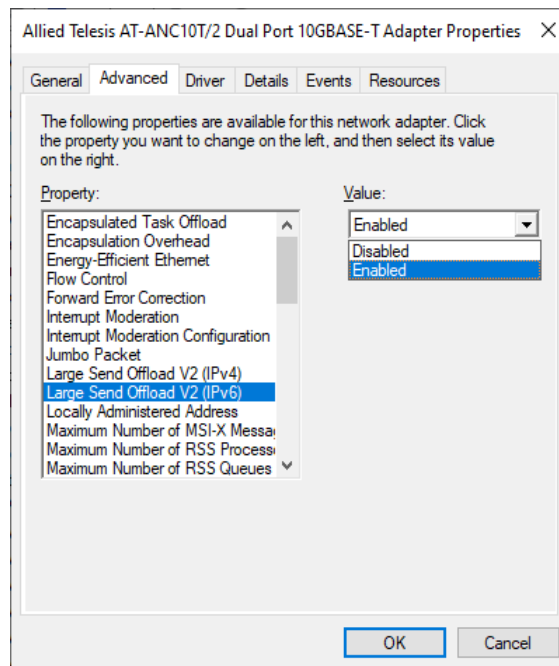


Figure 32. Large Send Offload (IPv6) Window

3. Select one of the following options:
  - Disabled** — The network interface card does not segment packets for IPv6 traffic.
  - Enabled** — The network interface card port segments large packets up to 256Kb for IPv6 traffic before sending them out. This is the default setting.

4. Click **OK**.

## Locally Administered Address

The Locally Administered Address property is a user-defined MAC address that is used in place of the MAC address originally assigned to the network interface card. Every network interface card 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 54.

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

The Locally Administered Address window is displayed as shown in Figure 33.

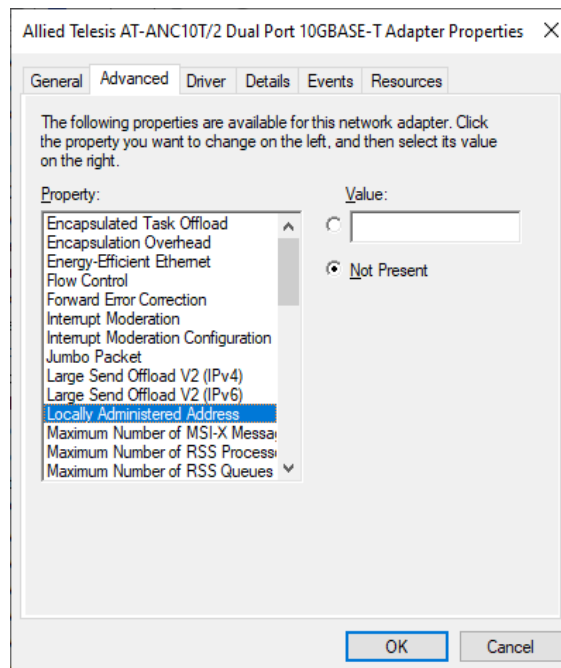


Figure 33. Locally Administered Address Window

3. Select one of the following options:

- Value** — Used to manually assign a MAC address to the network interface card.
- Not Present** — Uses the factory-assigned address on the network interface card. 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**.

## Maximum Number of MSI-X Messages

Message-signaled interrupts provide an in-band method of signaling interrupts to the host processor which can be used as an alternative to traditional out of band methods.

To enable or disable the Maximum Number of MSI-X Messages feature, do the following:

1. Access the Advanced Properties.  
See “Accessing Advanced Properties” on page 54.
2. Select **Maximum Number of MSI-X Messages** in the Property box.

The Maximum Number of MSI-X Messages window is displayed as shown in Figure 34.

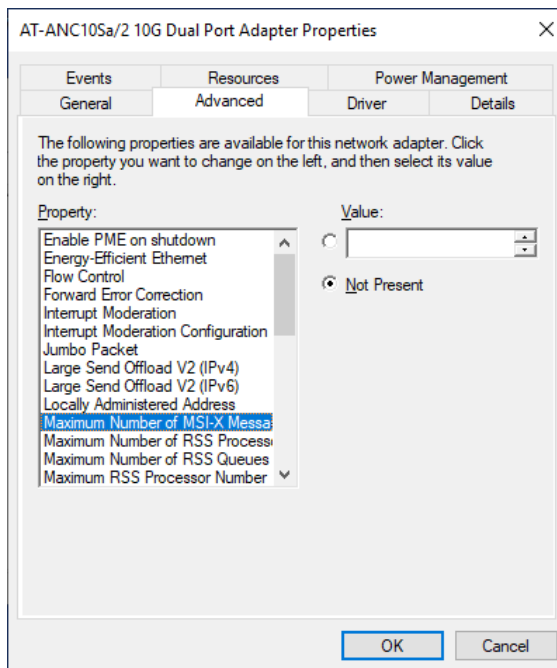


Figure 34. Maximum Number of MSI-X Messages Event Window

3. Select one of the following options:
  - Value** — Sets the number of interrupts that can be allocated (up to 2048).
  - Not Present** — This is the default.
4. Click **OK**.



## Maximum Number of RSS Processors

The Maximum Number of RSS Processors property sets the maximum number of processors that will be available for use with Receive Side Scaling.

To specify or change the Maximum Number of RSS Processors feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

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

The Maximum Number of RSS Processors window is displayed as shown in Figure 34.

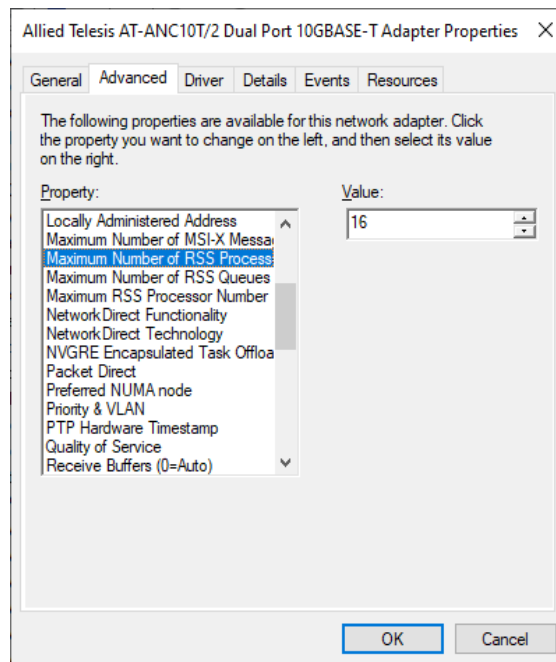


Figure 35. Maximum Number of RSS Processors Window

3. Select one of the following options:

- Value** — Sets the number of processors allocated for use.
- Not Present** — This is the default.

4. Click **OK**.

## Maximum Number of RSS Queues

---

The Maximum Number of RSS Queues property assigns data to queues associated with physical CPU cores. You can specify the maximum number of RSS queues that the network interface card 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 54.
2. Select **Maximum Number of RSS Queues** in the Property box.

The Maximum Number of RSS Queues window is displayed as shown in Figure 36.

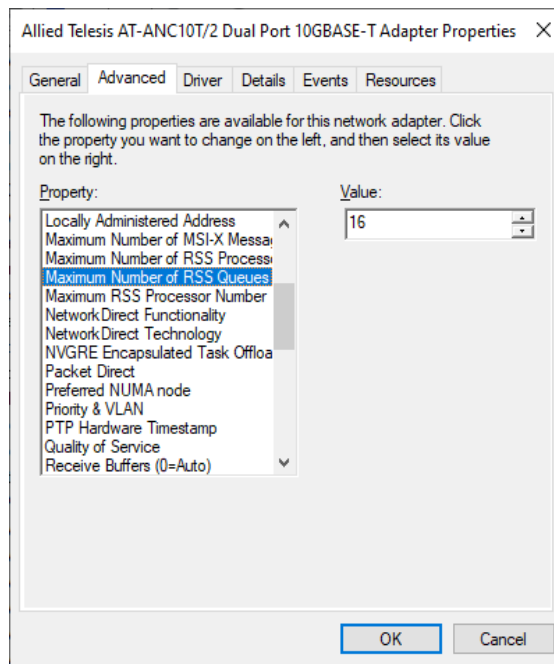


Figure 36. Maximum Number of RSS Queues Window

3. Select one of the following options:
  - Value** — The system allocates up to 16 RSS queues.
4. Click **OK**.

## Maximum RSS Processor Number

The Maximum RSS Processor Number property sets the highest processor number that will be available for use with Receive Side Scaling (RSS).

To specify or change the Maximum RSS Processor Number feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Maximum RSS Processor Number** in the Property box.

The Maximum RSS Processor Number window is displayed as shown in Figure 37.

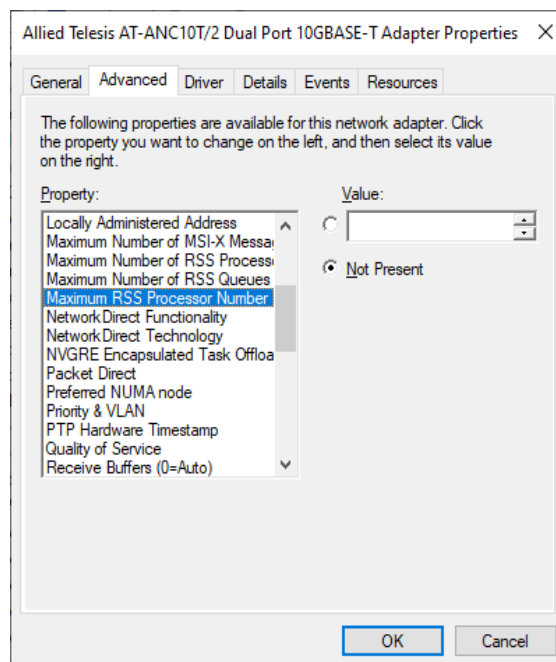


Figure 37. Maximum RSS Processor Number Window

3. Select one of the following options:

- Value** — The processor number of the highest processor to be made available.
- Not Present** — This is the default setting.

4. Click **OK**.

## Network Direct Functionality

---

The Network Direct Functionality property enables or disables the Remote Direct Memory Access (RDMA) feature.

To enable or disable the Network Direct Functionality feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Network Direct Functionality** in the Property box.

The Maximum Network Direct Functionality window is displayed as shown in Figure 38.

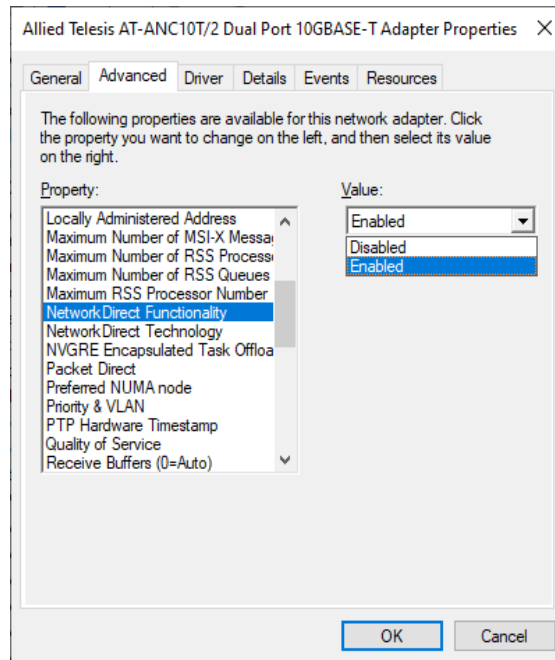


Figure 38. Network Direct Functionality Window

3. Select one of the following options:
  - Enabled** — Enables the RDMA feature.
  - Disabled** — Disables the RDMA feature. This is the default setting.
4. Click **OK**.

## Network Direct Technology

The Network Direct Technology property sets the RDMA type that will be used (RDMA over Converged Ethernet or RDMA over Converged Ethernet Version 2).

To specify or change the Network Direct Technology feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Network Direct Technology** in the Property box.

The Network Direct Technology window is displayed as shown in Figure 39.

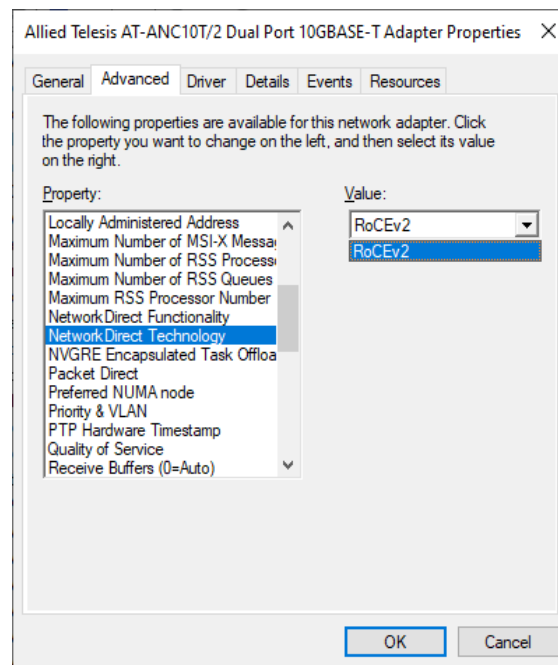


Figure 39. Network Direct Technology Window

3. Select one of the following options:

- RoCE** — Uses RDMA over Converged Ethernet.
- RoCEv2** — Uses RDMA over Converged Ethernet Version 2.

4. Click **OK**.

## NVGRE Encapsulated Task Offload

---

The NVGRE Encapsulated Task Offload property enables/disables task offloads for NVGRE encapsulated packets.

To specify or change the NVGRE Encapsulated Task Offload feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **NVGRE Encapsulated Task Offload** in the Property box.

The NVGRE Encapsulated Task Offload window is displayed as shown in Figure 40.

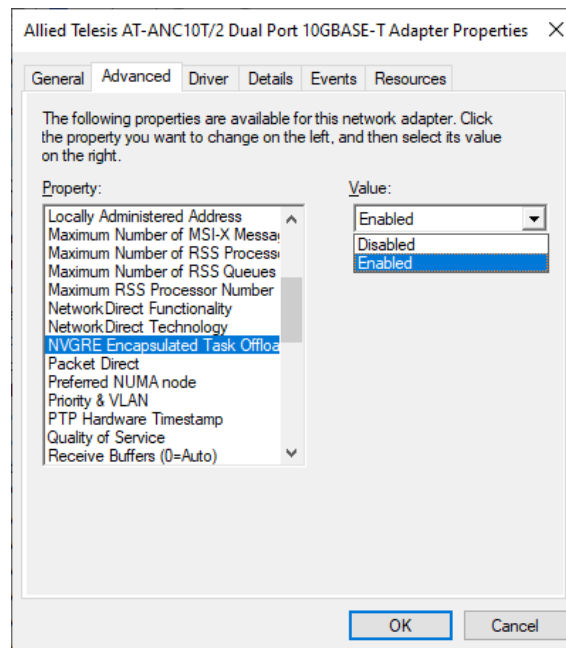


Figure 40. NVGRE Encapsulated Task Offload Window

3. Select one of the following options:
  - Disabled** — This setting disables task offloads for NVGRE encapsulated packets.
  - Enabled** — This setting enables task offloads for NVGRE encapsulated packets. This setting is the default.
4. Click **OK**.

## Packet Direct

---

The Packet Direct property enables a low-latency data path between the NIC and packet direct enabled virtual switch.

To specify or change the Packet Direct feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

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

The Packet Direct window is displayed as shown in Figure 41.

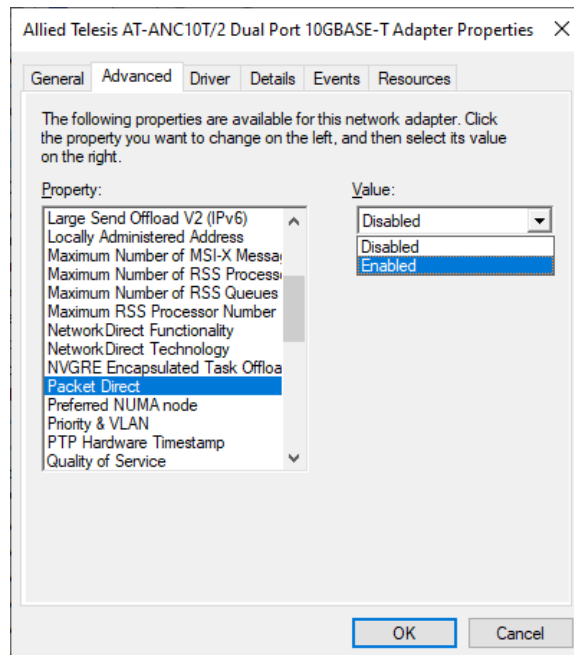


Figure 41. Packet Direct Window

3. Select one of the following options:

- Disabled** — This setting disables Packet Direct.
- Enabled** — This setting enables Packet Direct. This setting is the default.

4. Click **OK**.

## Preferred NUMA Node

The Preferred NUMA Node property sets the processor bus number that will be used for the NIC to access host memory.

To specify or change the Preferred NUMA Node feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Preferred NUMA Node** in the Property box.

The Preferred NUMA Node window is displayed as shown in Figure 43.

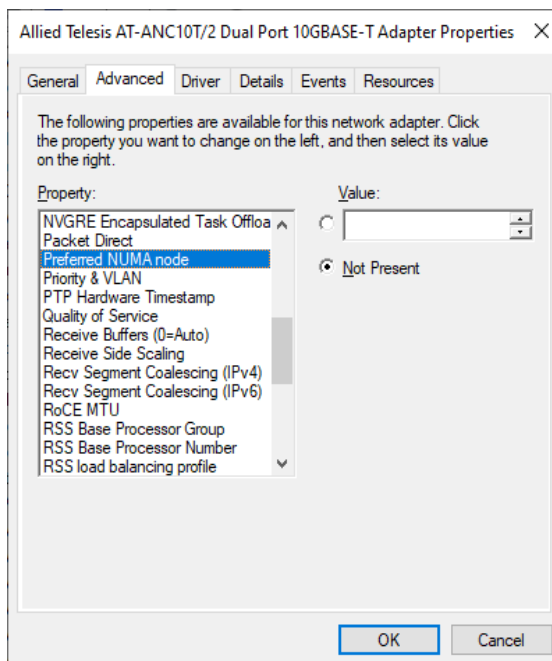


Figure 42. Preferred NUMA Node Window

3. Select one of the following options:
  - Value** — Host bus number.
  - Not Present** — This is the default setting.
4. Click **OK**.



## Priority & VLAN

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

When the property is set to Priority & VLAN Enabled, the network interface card sends and receives QoS and VLAN tagged frames; with Priority Enabled, the network interface card sends and receives QoS tagged frames; with VLAN Enabled, the network interface card sends and receives VLAN tagged frames. To assign a VLAN ID to the network interface card, see “VLAN ID” on page 112.

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

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

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

The Priority & VLAN window is displayed as shown in Figure 43.

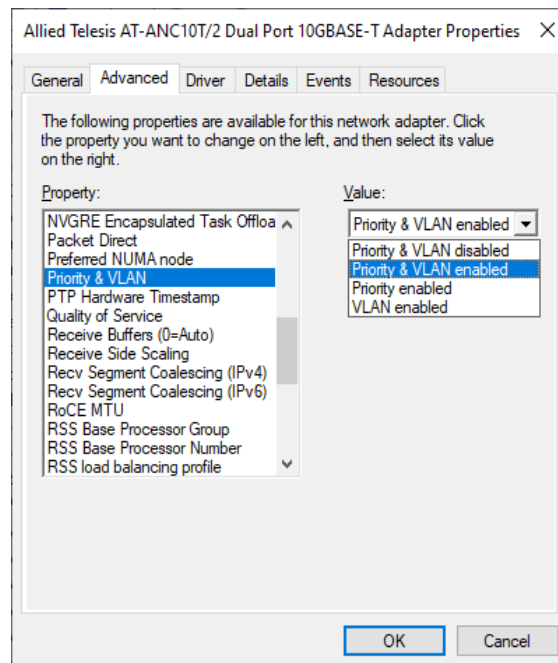


Figure 43. Priority & VLAN Window

3. Select one of the following options:

- Priority & VLAN Disabled** — Prevents packet prioritization and VLAN tagging.

- Priority & VLAN Enabled** — Allows for packet prioritization and VLAN tagging. This is the default setting.
  - Packet Enabled** — Allows packet prioritization only.
  - VLAN Enabled** — Allows VLAN tagging only.
4. Click **OK**.

## PTP Hardware Timestamp

The PTP Hardware Timestamp property generates timestamps using the network interface card's own hardware clock. This feature is used in particular by the Precision Time Protocol (PTP), which is a time synchronization protocol. Those calculations can then be used by PTP to improve the accuracy of time synchronization.

To specify or change the PTP Hardware Timestamp feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **PTP Hardware Timestamp** in the Property box.

The PTP Hardware Timestamp window is displayed as shown in Figure 44.

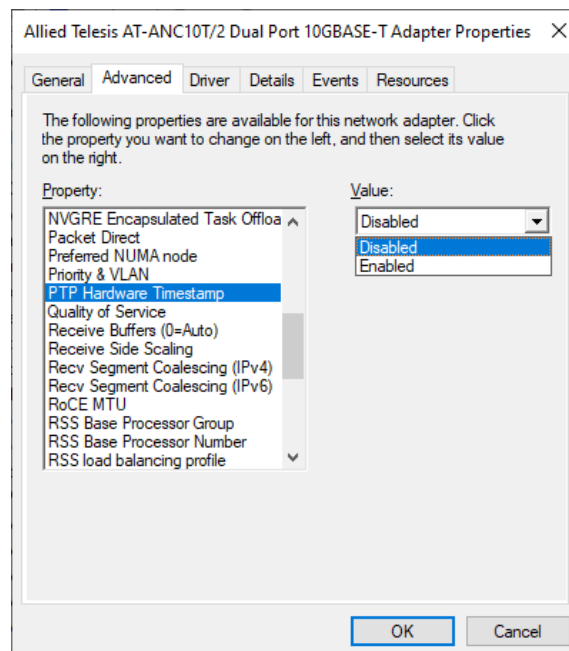


Figure 44. PTP Hardware Timestamp Window

3. Select one of the following options:

- Disabled** — This setting disables PTP hardware generation. This setting is the default.
- Enabled** — This setting enables PTP hardware generation.

4. Click **OK**.

## Quality of Service

---

The Quality of Service property enables the processing of QoS-enabled frames.

To enable or disable the Quality of Service feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Quality of Service** in the Property box.

The Quality of Service window is displayed as shown in Figure 43.

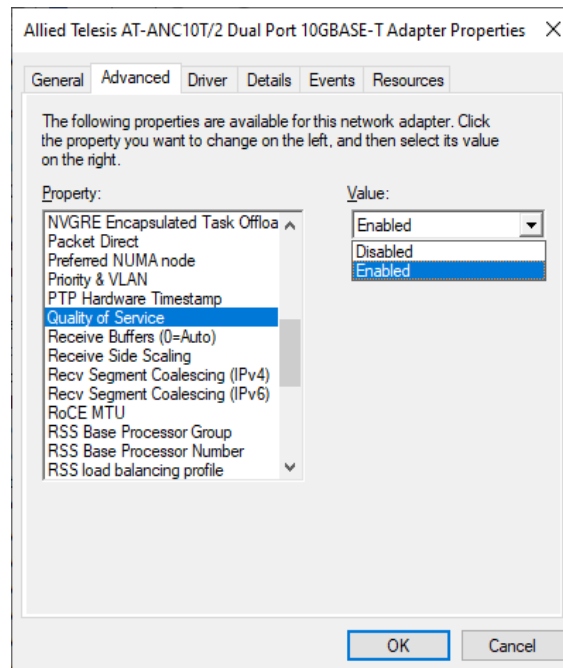


Figure 45. Quality of Service Window

3. Select one of the following options:
  - Enabled** — Enables QoS processing. This is the default setting.
  - Disabled** — Disables QoS processing.
4. Click **OK**.

## Receive Buffers (0=Auto)

The Receive Buffers are data segments that allow the network interface card 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 54.

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

The Receive Buffers window is displayed as shown in Figure 46.

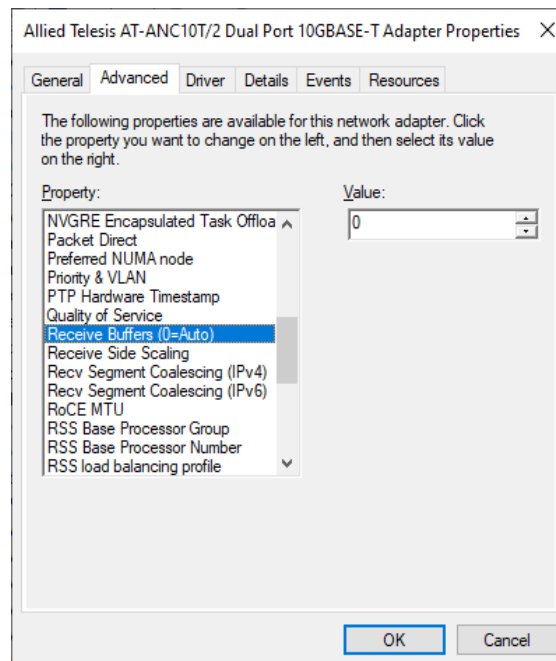


Figure 46. Receive Buffers Window

3. Specify the buffer size in the Value box.

The range of valid receive buffers is 0 (auto) to 15000 in increments of 500 with 500 receive buffers as the default value.

4. Click **OK**.

## Receive Side Scaling

The Receive Side Scaling (RSS) property allows the network interface card 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 54.
2. Select **Receive Side Scaling** in the Property box.

The Receive Side Scaling window is displayed as shown in Figure 47.

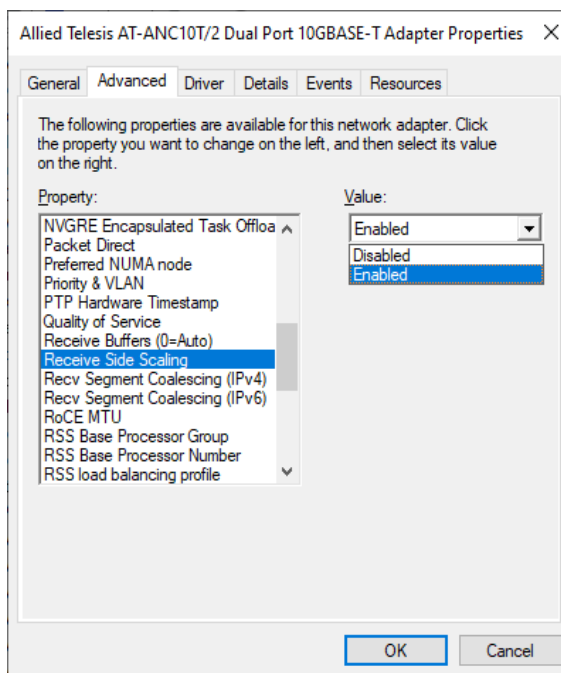


Figure 47. Receive Side Scaling Window

3. Select one of the following options:
  - Enabled** — Processes receiving data by multiple CPUs. This is the default setting.
  - Disabled** — Processes receiving data 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 54.

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

The Receive Segment Coalescing (IPv4) window is displayed as shown in Figure 48.

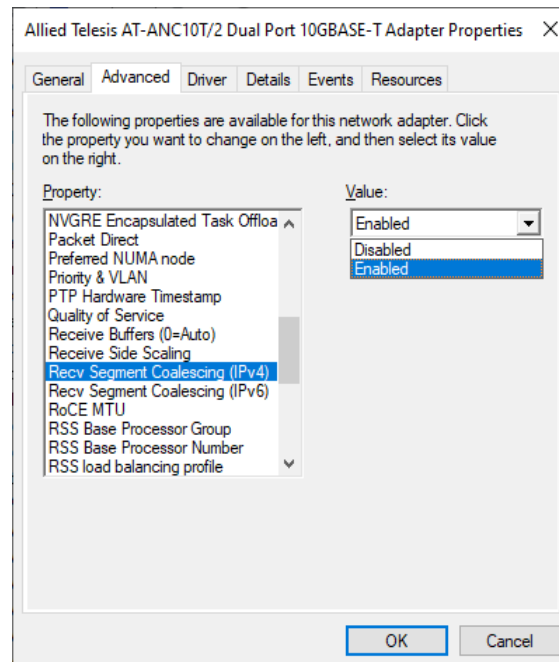


Figure 48. Receive Segment Coalescing (IPv4) Window

3. Select one of the following options:

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

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 54.

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

The Receive Segment Coalescing (IPv6) window is displayed as shown in Figure 49.

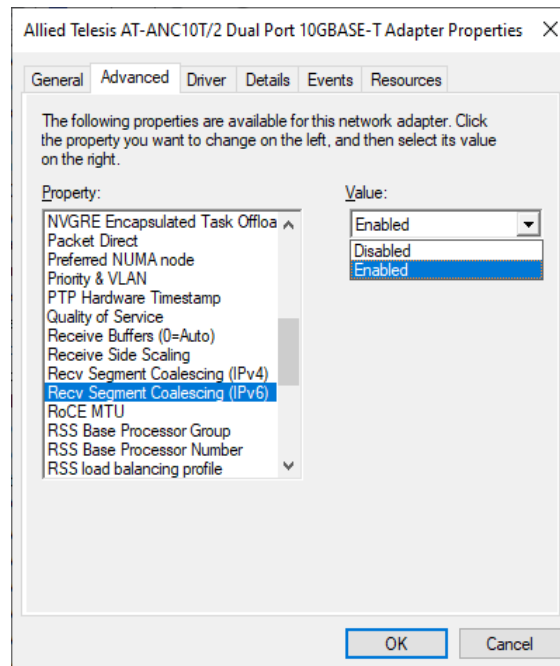


Figure 49. Receive Segment Coalescing (IPv6) Window

3. Select one of the following options:

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

4. Click **OK**.

## RoCE MTU

---

The RDMA over Converged Ethernet (RoCE) Maximum Transmission Unit (MTU) property sets the maximum packet size for RDMA packets.

To specify or change the RoCE MTU feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **RoCE MTU** in the Property box.

The RoCE MTU window is displayed as shown in Figure 50.

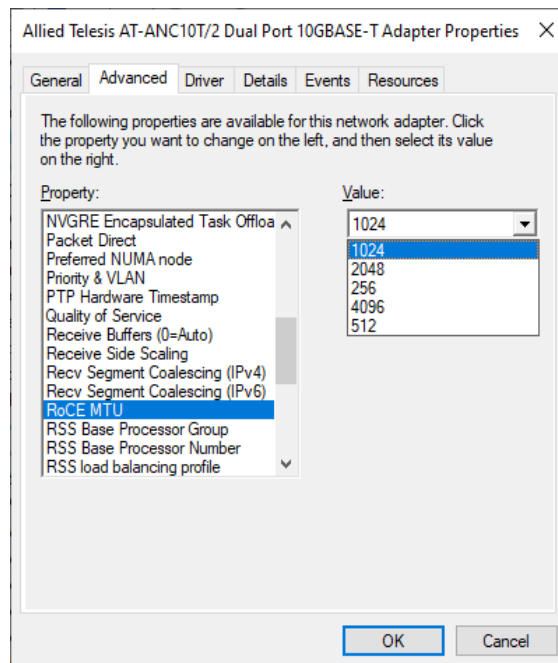


Figure 50. RoCE MTU Window

3. Select one of the following node options:
  - 1024** — This is the default setting.
  - 2048**
  - 256**
  - 4096**
  - 512**
4. Click **OK**.

## RSS Base Processor Group

The RSS Base Processor Group property defines the base processor group for the RSS queues on the network adapter.

To specify or change the RSS Base Processor Group feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **RSS Base Processor Group** in the Property box.

The RSS Base Processor Group window is displayed as shown in Figure 51.

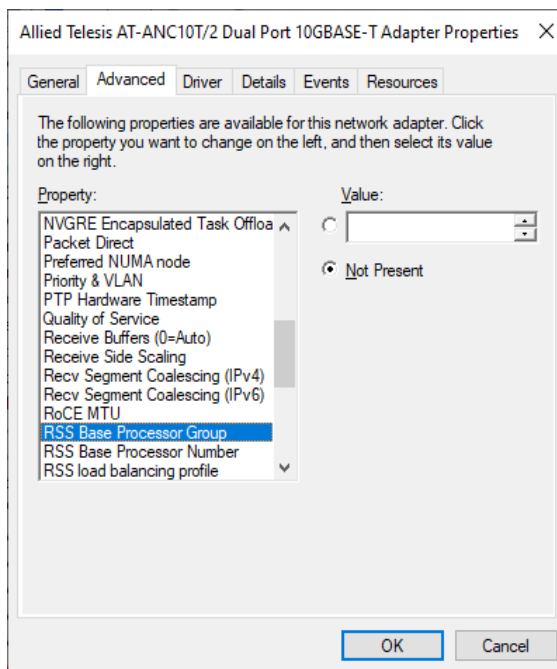


Figure 51. RSS Base Processor Group Window

3. Select one of the following options:
  - Value** — Base processor group number.
  - Not Present** — This is the default setting.
4. Click **OK**.

## RSS Base Processor Number

The RSS Base Processor Number property may be set to explicitly define the CPU affinity for the RSS queues of this device. It is the CPU number of the lowest RSS queue for this device.

To specify or change the RSS Base Processor Number feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **RSS Base Processor Number** in the Property box.

The RSS Base Processor Number window is displayed as shown in Figure 52.

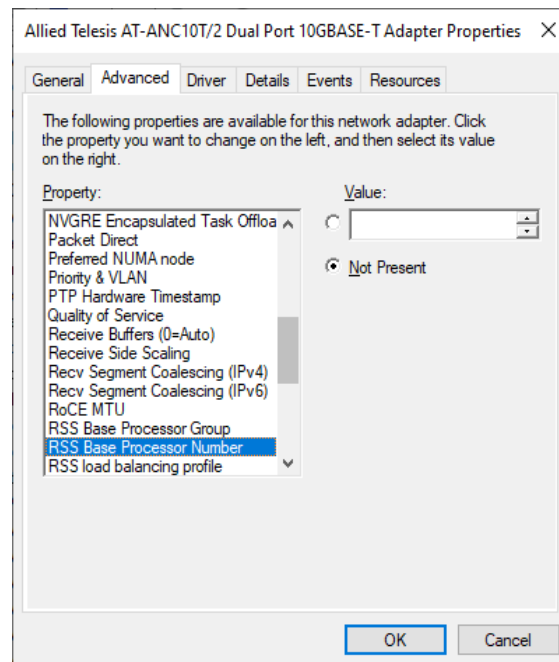


Figure 52. RSS Base Processor Number Window

3. Select one of the following options:

- Value** — The base processor number.
- Not Present** — This is the default setting.

4. Click **OK**.

## RSS Load Balancing Profile

The RSS Load Balancing Profile property sets the profile that RSS will use to determine how to scale receive functions across CPUs.

To specify or change the RSS Load Balancing Profile feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **RSS Load Balancing Profile** in the Property box.

The RSS Load Balancing Profile window is displayed as shown in Figure 53.

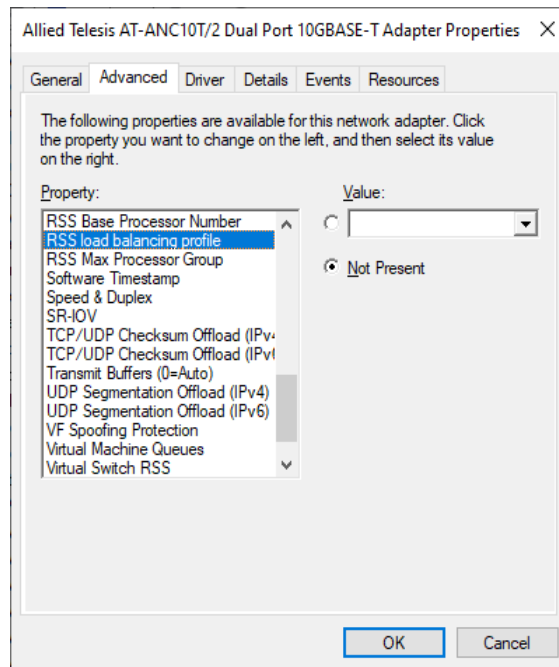


Figure 53. RSS Load Balancing Profile Window

3. Select one of the following options:

- **Value** —
  - **NUMA scaling static:** RSS processor selection is the same as for NUMA scalability without dynamic load balancing.
  - **Closest processor:** Behavior is consistent with the behavior of Windows Server® 2008 R2.

- **Closest processor static:** No dynamic load balancing, such as distributing but not load balancing at runtime.
  - **Conservative scaling:** RSS uses as few processors as possible to sustain the load. This option helps reduce the number of interrupts.
  - **NUMA scaling:** Assigns RSS processors in a round robin basis across every NUMA node to enable applications that are running on NUMA servers to scale well.
- Not Present** — This is the default setting.
4. Click **OK**.

## RSS Max Processor Group

The RSS Max Processor Group property value defines the maximum number of processor groups for the RSS CPUs in use.

To specify or change the RSS Max Processor Group feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **RSS Max Processor Group** in the Property box.

The RSS Max Processor Group window is displayed as shown in Figure 54.

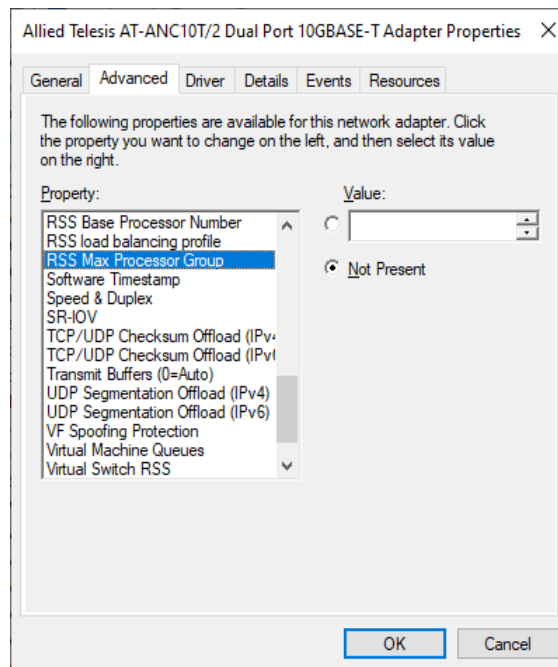


Figure 54. RSS Max Processor Group Window

3. Select one of the following options:
  - Value** — The maximum processor group.
  - Not Present** — This is the default setting.
4. Click **OK**.



## Software Timestamp

The Software Timestamp property allow for the generation of network timestamps to be done at the software level.

To specify or change the Software Timestamp feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Software Timestamp** in the Property box.

The Software Timestamp window is displayed as shown in Figure 55.

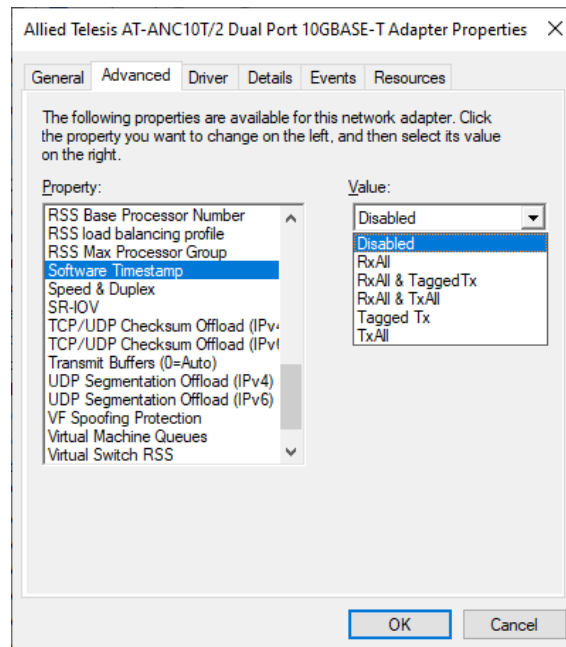


Figure 55. Software Timestamp Window

3. Select one of the following options:

- Disabled** — This setting disables software timestamping. This setting is the default.
- Rx All** — Enables all Rx timestamping.
- Rx All and Tagged Tx** — Enables all Rx and tagged Tx timestamping.
- Rx All and Tx All** — Enables all Rx and all Tx timestamping.
- Tagged Tx** — Enables tagged Tx timestamping.
- Tx All** — Enables all Tx timestamping.

- Click **OK**.

## Speed & Duplex

The Speed & Duplex property sets the connection speed and mode to that of the network. Note that Full-Duplex mode allows the network interface card to transmit and receive network data simultaneously.

To specify or change the Speed & Duplex feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Speed & Duplex** in the Property box.

The Speed & Duplex window is displayed as shown in Figure 56.

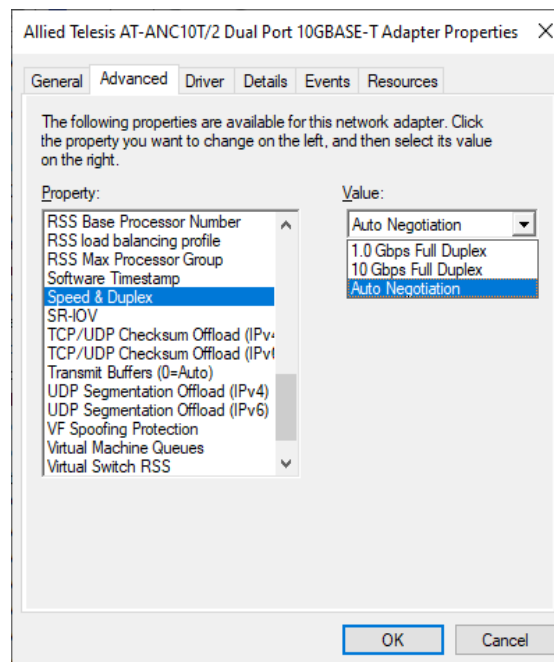


Figure 56. Speed & Duplex Window

3. Select one of the following options:

- 1.0Gbps Full Duplex** — Use this setting when connecting to a gigabit link partner that is configured for 1000 Mbps Full Duplex operation. ANC10 Network Interface Card Series will only connect to a 1Gbps link partner.
- 10Gbps Full Duplex** — Use this setting when connecting to a 10 gigabit link partner that is configured for 10000 Mbps Full Duplex operation. ANC10 Network Interface Card Series will only connect to a 10Gbps link partner.

- ❑ **Auto Negotiation** — Use this setting when connecting to a 1 or 10 Gbps link partner that is configured for Auto-Negotiation. ANC10 Network Interface Card Series will attempt to detect the maximum speed supported by the installed SFP module, and will set the port speed to match. This is the default setting.

4. Click **OK**.

## SR-IOV

The Single Root I/O Visualization (SR-IOV) property allows guest operating systems in a virtualized environment direct access to the NICs PCIe bus and physical functions as opposed to being virtualized by the hypervisor.

To specify or change the SR-IOV feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **SR-IOV** in the Property box.

The SR-IOV window is displayed as shown in Figure 57.

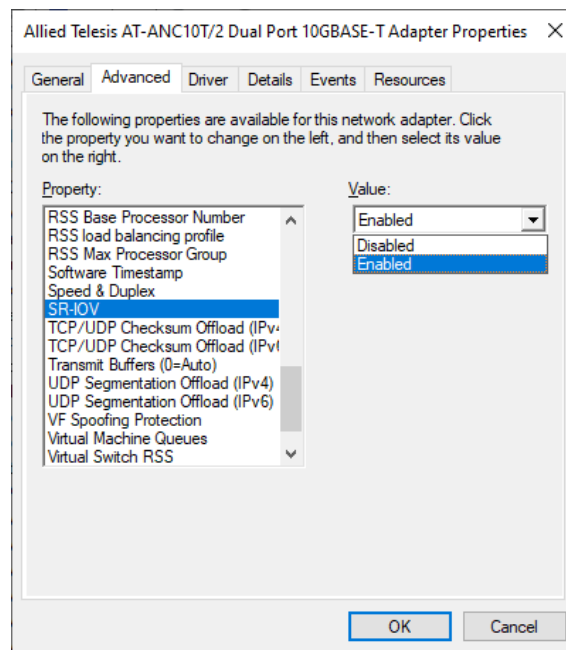


Figure 57. SR-IOV Window

3. Select one of the following options:

- Enabled** — Enables SR-IOV. NIC physical function access is available to guest operating systems. This is the default setting.
- Disabled** — Disables SR-IOV. No physical function access is available.

4. Click **OK**.

## TCP/UDP Checksum Offload (IPv4)

The TCP/UDP Checksum Offload (IPv4) property enables the network interface card 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 54.
2. Select **TCP/UDP Checksum Offload (IPv4)** in the Property box.

The TCP/UDP Checksum Offload (IPv4) window is displayed as shown in Figure 58.

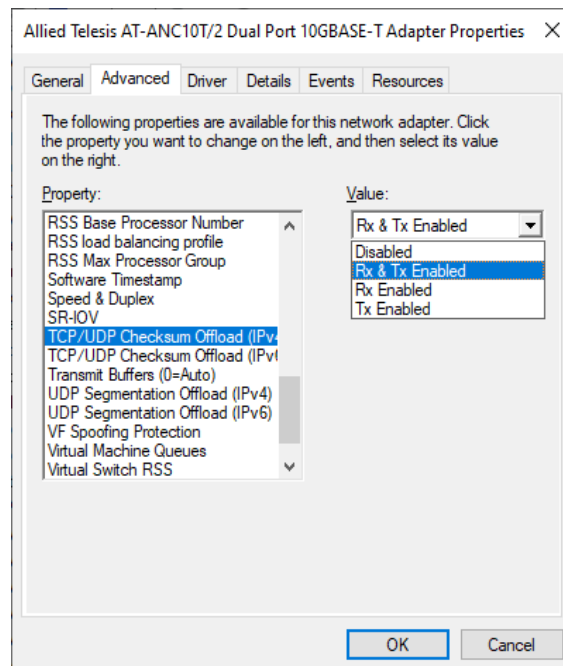


Figure 58. TCP/UDP Checksum Offload (IPv4) Window

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) property enables the network interface card 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 54.
2. Select **TCP/UDP Checksum Offload (IPv6)** in the Property box.

The TCP/UDP Checksum Offload (IPv6) window is displayed as shown in Figure 59.

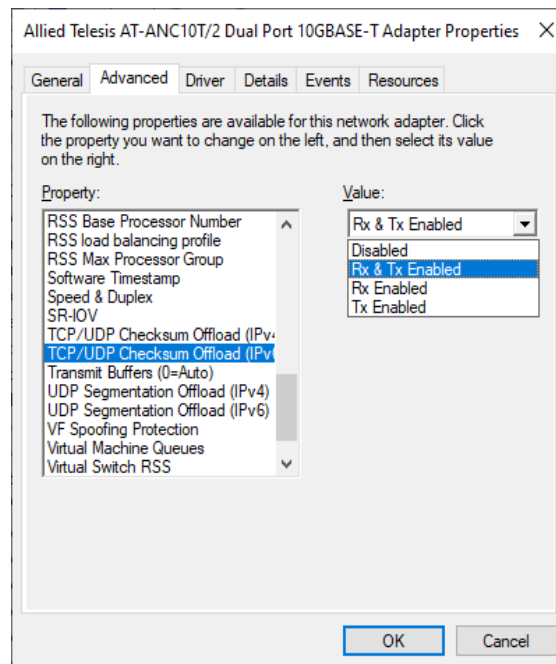


Figure 59. TCP/UDP Checksum Offload (IPv6) Window

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 (0=Auto)

---

The Transmit Buffers property value is the number of transmit buffers allowed. Transmit buffers are segments of system memory allocated to processing transmit packets.

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 54.

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

The Transmit Buffers window is displayed as shown in Figure 60.

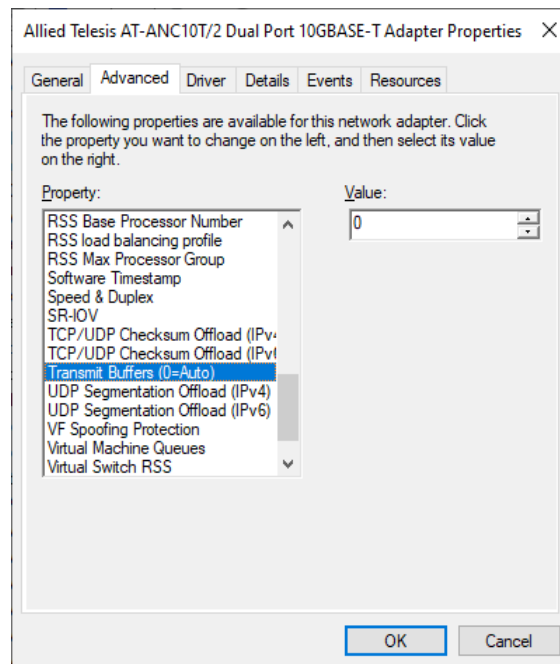


Figure 60. Transmit Buffers Window

3. Specify the buffer size in the Value box. The valid range is 0 to 5000 in increments of 50. The default value is 0.
4. Click **OK**.

## UDP Segmentation Offload (IPv4)

The UDP Segmentation Offload (USO) property allows the NIC to perform the segmentation of UDP datagrams that are larger than the maximum transmission unit (MTU) of the network medium. By doing so, Windows reduces CPU utilization associated with per-packet TCP/IP processing.

To specify or change the UDP Segmentation Offload (IPv4) feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **UDP Segmentation Offload (IPv4)** in the Property box.

The UDP Segmentation Offload (IPv4) window is displayed as shown in Figure 61.

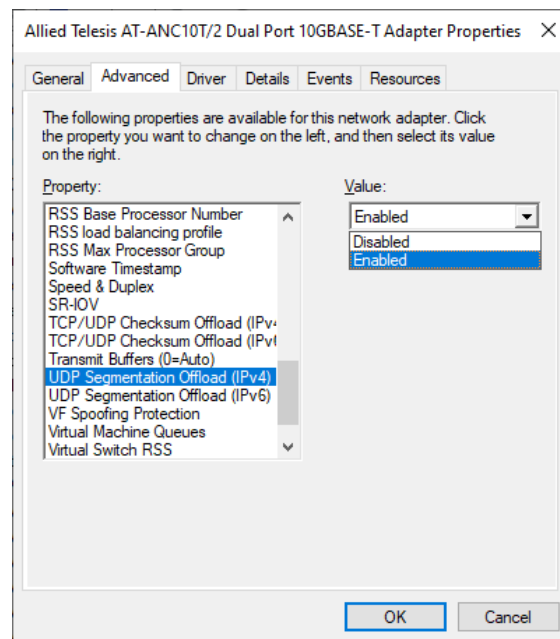


Figure 61. UDP Segmentation Offload (IPv4) Window

3. Select one of the following options:

- Enabled** — Enables UDP Segmentation Offload (IPv4). This is the default setting.
- Disabled** — Disables UDP Segmentation Offload (IPv4).

4. Click **OK**.

## UDP Segmentation Offload (IPv6)

O) property allows the NIC to perform the segmentation of UDP datagrams that are larger than the maximum transmission unit (MTU) of the network medium. By doing so, Windows reduces CPU utilization associated with per-packet TCP/IP processing.

To specify or change the UDP Segmentation Offload (IPv6) feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **UDP Segmentation Offload (IPv6)** in the Property box.

The UDP Segmentation Offload (IPv6) window is displayed as shown in Figure 62.

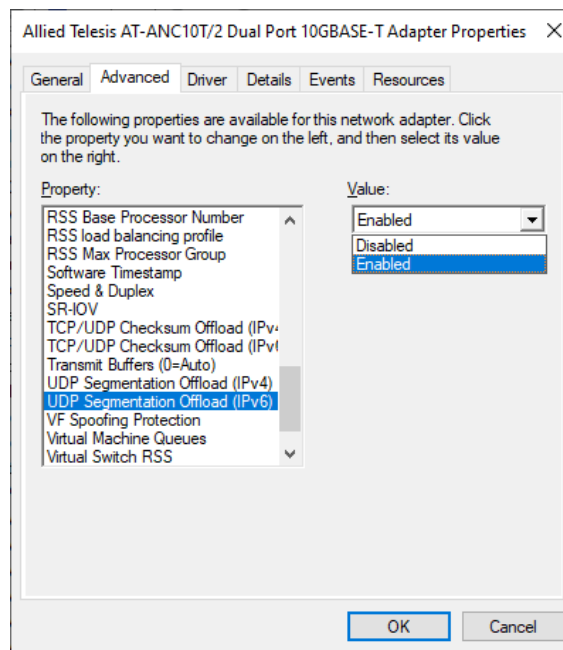


Figure 62. UDP Segmentation Offload (IPv6) Window

3. Select one of the following options:

- Enabled** — Enables UDP Segmentation Offload (IPv6). This is the default setting.
- Disabled** — Disables UDP Segmentation Offload (IPv6).

4. Click **OK**.

## VF Spoofing Protection

The Virtual Function (VF) Spoofing Protection property prevents malicious intent under the guise of legitimate behavior.

To specify or change the VF Spoofing Protection feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **VF Spoofing Protection** in the Property box.

The VF Spoofing Protection window is displayed as shown in Figure 63.

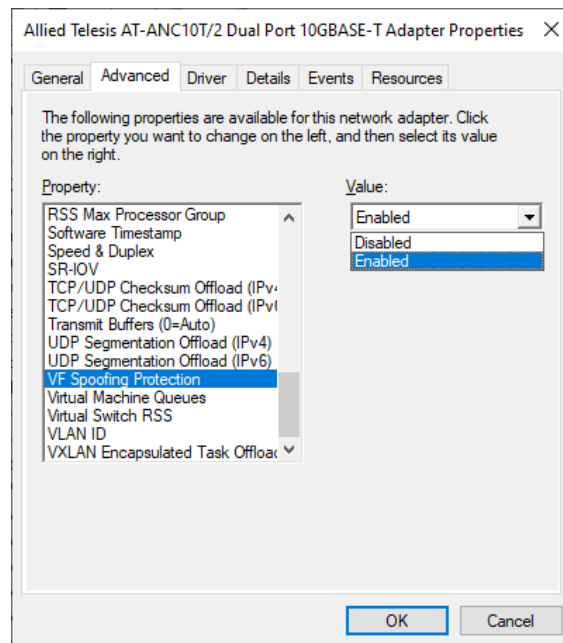


Figure 63. VF Spoofing Protection Window

3. Select one of the following options:
  - Enabled** — Enables VF Spoofing Protection. This is the default setting.
  - Disabled** — Disables VF Spoofing Protection.
4. Click **OK**.

## Virtual Machine Queues

The Virtual Machine Queues property allows the NIC to cache external network traffic to dedicated storage areas on the NIC to be accessed by individual virtual machines.

To enable or disable the Virtual Machine Queues feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Virtual Machine Queues** in the Property box.

The Virtual Machine Queues window is displayed as shown in Figure 64.

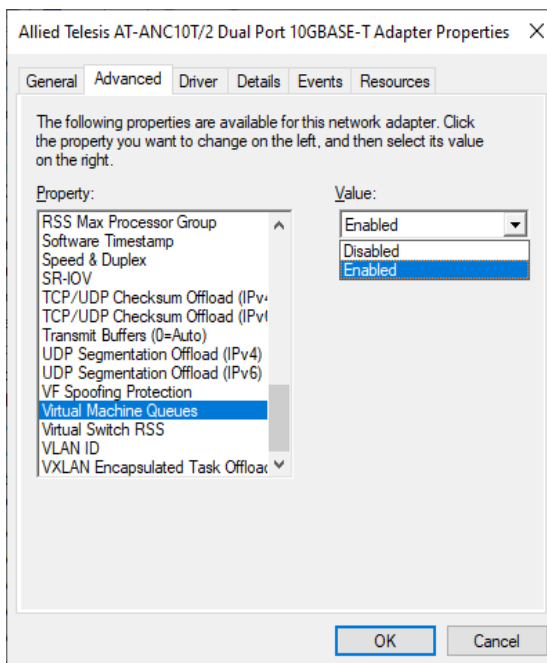


Figure 64. Virtual Machine Queues Window

3. Select one of the following options:
  - Enabled** — Enables virtual machine queues. This is the default setting.
  - Disabled** — Disables virtual machine queues.
4. Click **OK**.

## Virtual Switch RSS

The Virtual Switch RSS property enables network traffic processing to be scaled over multiple host CPUs for virtual machines.

To specify or change the Virtual Switch RSS feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **Virtual Switch RSS** in the Property box.

The Virtual Switch RSS window is displayed as shown in Figure 57.

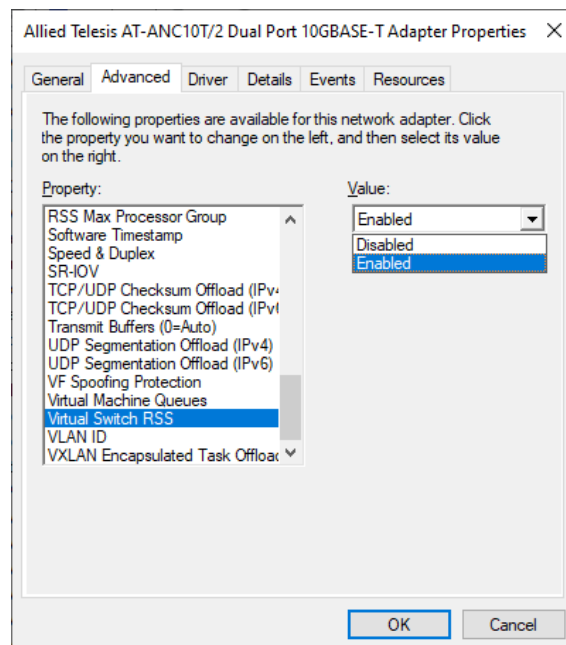


Figure 65. Virtual Switch RSS Window

3. Select one of the following options:

- Enabled** — Enables Virtual Switch RSS. This is the default setting.
- Disabled** — Disables Virtual Switch RSS.

4. Click **OK**.

## VLAN ID

---

The VLAN ID property allows you to specify a VLAN ID on your network to the network interface card port. The network interface card 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 54.

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

The VLAN ID window is displayed as shown in Figure 66.

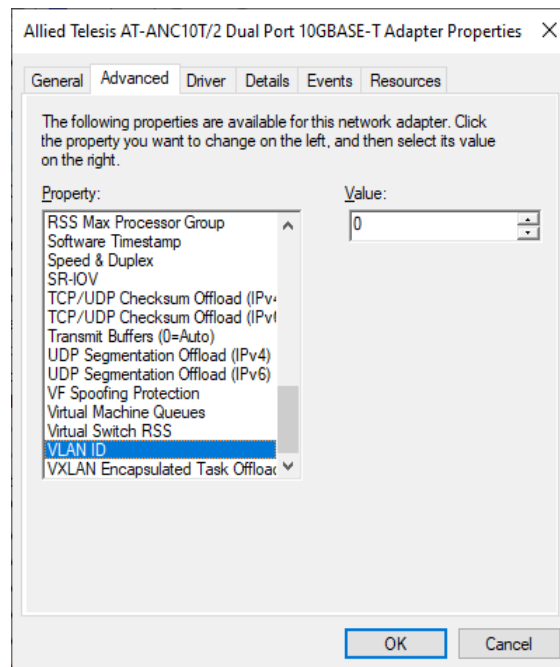


Figure 66. VLAN ID Window

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**.



## VXLAN Encapsulated Task Offload

The VXLAN Encapsulated Task Offload property allows for the use of Encapsulated Task offload functions in a VXLAN environment

To specify or change the VXLAN Encapsulated Task Offload feature, do the following:

1. Access the Advanced Properties.

See “Accessing Advanced Properties” on page 54.

2. Select **VXLAN Encapsulated Task Offload** in the Property box.

The VXLAN Encapsulated Task Offload window is displayed as shown in Figure 67.

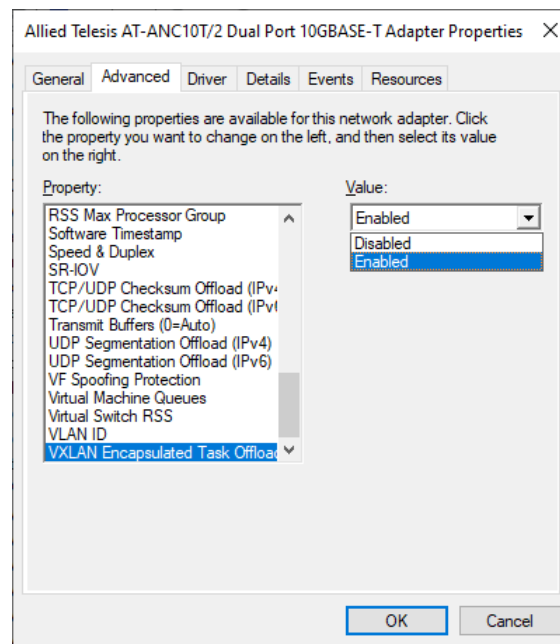


Figure 67. VXLAN Encapsulated Task Offload Window

3. Select one of the following options:

- Enabled** — Enables VXLAN Encapsulated Task Offload. This is the default setting.
- Disabled** — Disables VXLAN Encapsulated Task Offload.

4. Click **OK**.



## Chapter 5

# Uninstalling the Driver Software

---

This chapter describes how to uninstall driver software for the ANC10 Network Interface Card Series onto your Windows operating system. It contains the following topics:

- ❑ “Overview” on page 116
- ❑ “Uninstalling the Driver Software Using Device Manager” on page 117
- ❑ “Uninstalling the Driver Software Silently” on page 119

## Overview

---

When you no longer use the ANC10Sa/2 or ANC10T/2 for your computer, you can uninstall the driver software from your operating system.

As you can install driver software for the network interface card 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 117
- ❑ “Uninstalling the Driver Software Silently” on page 119

### 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 interface card, 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 Windows Device Manager” on page 43.
3. In the Device Manager window, expand the Network Adapters folder.
4. Right-click the **Allied Telesis AT-ANC10Sa/2 (or AT-ANC10T/2) 10G Dual Port Adapter**.

The shortcut menu appears as shown in Figure 68.

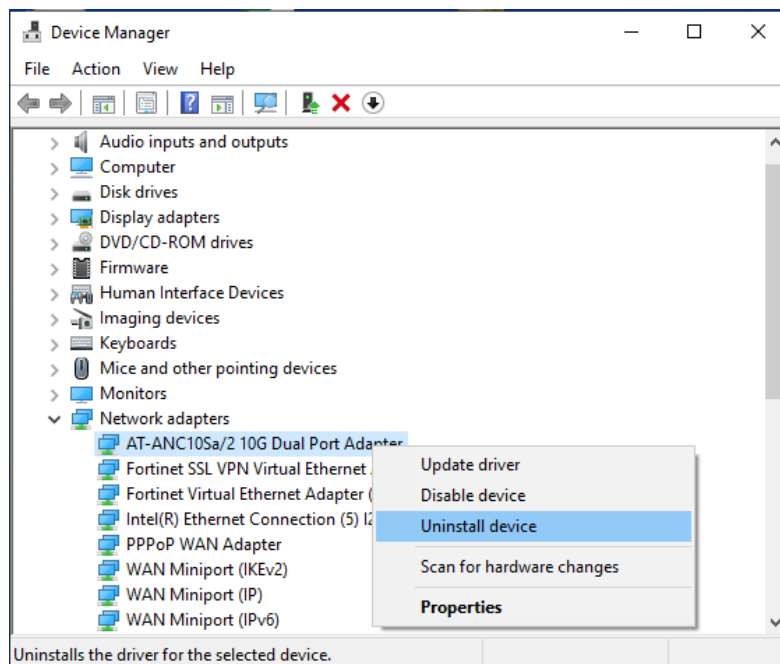


Figure 68. Device Manager Shortcut Menu

5. Select **Uninstall device**.

The Confirm Device Uninstall window pops up.

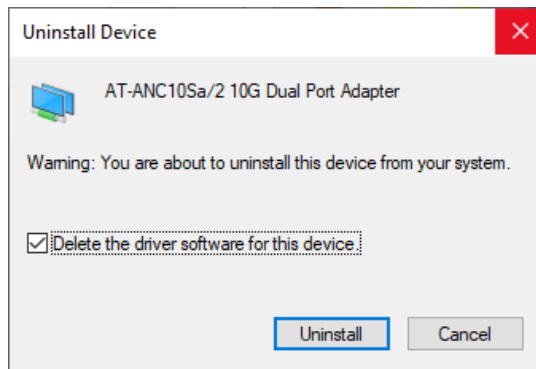


Figure 69. Deleting the Driver Software

6. Check the check box if you want to remove the driver software for your network interface card.
7. Click **Uninstall** 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.





## Appendix A

# Technical Specifications

---

This appendix contains the following sections:

- ❑ “Physical Specifications” on page 121
- ❑ “Environmental Specifications” on page 122
- ❑ “Power Specifications” on page 122
- ❑ “Performance Specification” on page 122
- ❑ “Compliance Requirements” on page 123

## Physical Specifications

---

Table 4 contains the dimensions and weight of the network interface card.

Table 4. Physical Specifications

<b>Network Interface Card</b>	<b>Dimensions (L X W)</b>	<b>Weight</b>
ANC10Sa/2	160.0 mm (6.3 in) x 68.9 mm (2.7 in)	79.37 grams
ANC10T/2	160.0 mm (6.3 in) x 68.9 mm (2.7 in)	90.71 grams

## Environmental Specifications

---

Table 5 contains the environmental specifications of the network interface card.

Table 5. Environmental Specifications

Environmental Specification	Value
Operating Temperature	0° C to 35° C (32° F to 95° F)
Storage Temperature	-30° C to 70° C (-22° 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 6 contains the power specifications of the network interface card.

Table 6. Operating Voltages and Maximum Power Consumption

Operating Voltage	12V	
Maximum Power Consumption	ANC10Sa/2	15W @ 35° C (95° F)
	ANC10T/2	25W @ 35° C (95° F)
Typical Power Consumption	ANC10Sa/2	8W <sup>a</sup>
	ANC10T/2	12W

a. Power consumption with two AT-SP10SR SFP+ modules installed. Refer to the SFP data sheet for power figures.

## Performance Specification

---

The network interface card is x8 PCIe 3.0 compliant.

## Compliance Requirements

---

Table 7 contains the specifications of the compliance requirements.

Table 7. Compliance Requirements

Item	Specification
Safety	UL62368-1 (CUL <sub>US</sub> )
	CSA C22.2 No. 62368-1
	EN62368-1 (TUV)
Emissions (EMI)	FCC Part 15
	EN55032 Class B
	VCCI, Class B
	ICES-003
Immunity	EN55035
	EN 61000-3-2
	EN 61000-3-3
Environmental	RoHS

