Azure RTOS NetX Duo

User Manual

Published: February 2020

For the latest information, please see azure.com/rtos

Safety Certifications

IEC 61508 up to SIL 4
IEC 62304 up to SW safety Class C
ISO 26262 ASIL D
EN 50128 SW-SIL 4

UL/IEC 60730, UL/IEC 60335, UL 1998

Part Number: 000-1001
Revision 6.0

Contents

About This Guide

This guide contains comprehensive information about Azure RTOS NetX Duo, the Microsoft high-performance IPv4/IPv6 dual network stack.

It is intended for embedded real-time software developers familiar with basic networking concepts, Azure RTOS ThreadX, and the C programming language.

Organization

Chapter 1	Introduces NetX Duo
Chapter 2	Gives the basic steps to install and use NetX Duo with your ThreadX application.
Chapter 3	Provides a functional overview of the NetX Duo system and basic information about the TCP/IP networking standards.
Chapter 4	Details the application's interface to NetX Duo.
Chapter 5	Describes network drivers for NetX Duo.
Appendix A	NetX Duo Services
Appendix B	NetX Duo Constants
Appendix C	NetX Duo Data Types
Appendix D	BSD-Compatible Socket API

Appendix E ASCII Chart

Index Topic cross reference

Guide Conventions

Italics Typeface denotes book titles, emphasizes important words, and indicates variables.

Boldface Typeface denotes file names, key words, and further emphasizes important words and variables.

i Information symbols draw attention to important or additional information that could affect performance or function.

! Warning symbols draw attention to situations that developers should avoid because they could cause fatal errors.

NetX Duo Data Types

In addition to the custom NetX Duo control structure data types, there are several special data types that are used in NetX Duo service call interfaces. These special data types map directly to data types of the underlying C compiler. This is done to ensure portability between different C compilers. The exact implementation is inherited from ThreadX and can be found in the ***tx_port.h*** file included in the ThreadX distribution.

The following is a list of NetX Duo service call data types and their associated meanings:

UINT	Basic unsigned integer. This type must support 32-bit unsigned data; however, it is mapped to the most convenient unsigned data type.
ULONG	Unsigned long type. This type must support 32-bit unsigned data.
VOID	Almost always equivalent to the compiler's void type.
CHAR	Most often a standard 8-bit character type.

Additional data types are used within the NetX Duo source. They are located in either the ***tx_port.h*** or ***nx_port.h*** files.

Customer Support Center

Support email	azure-rtos support@microsoft.com
Web page	azure.com/rtos

Latest Product Information

Visit the Microsoft web site and select the “Support” menu option to find the latest online support information, including information about the latest NetX Duo product releases.

What We Need From You

To more efficiently resolve your support request, provide us with the following information in your email request:

1. A detailed description of the problem, including frequency of occurrence and whether it can be reliably reproduced.
2. A detailed description of any changes to the application and/or NetX Duo that preceded the problem.
3. The contents of the ***_tx_version_id*** and ***_nx_version_id*** strings found in the ***tx_port.h*** and ***nx_port.h*** files of your distribution. These strings will provide us valuable information regarding your run-time environment.
4. The contents in RAM of the following ULONG variables:

   _tx_build_options

   _nx_system_build_options1

   _nx_system_build_options2

   _nx_system_build_options3

   _nx_system_build_options4

   _nx_system_build_options5

These variables will give us information on how your ThreadX and NetX Duo libraries were built.

5. A trace buffer captured immediately after the problem was detected. This is accomplished by building the ThreadX and NetX Duo libraries with **TX_ENABLE_EVENT_TRACE** and calling ***tx_trace_enable*** with the trace buffer information. Refer to the *Azure RTOS TraceX User Guide* for details.

Where to Send Comments About This Guide

Email any comments and suggestions to the Customer Support Center at

azure-rtos-support@microsoft.com

Enter “NetX Duo User Guide” in the subject line

Chapter 1: Introduction to NetX Duo

Azure RTOS NetX Duo is a high-performance real-time implementation of the TCP/IP standards designed exclusively for embedded Azure RTOS ThreadX-based applications. This chapter contains an introduction to NetX Duo and a description of its applications and benefits.

NetX Duo Unique Features

Unlike other TCP/IP implementations, NetX Duo is designed to be versatile—easily scaling from small micro-controller-based applications to those that use powerful RISC and DSP processors. This is in sharp contrast to public domain or other commercial implementations originally intended for workstation environments but then squeezed into embedded designs.

Piconet™ Architecture

Underlying the superior scalability and performance of NetX Duo is *Piconet*, a software architecture especially designed for embedded systems. Piconet architecture maximizes scalability by implementing NetX Duo services as a C library. In this way, only those services actually used by the application are brought into the final runtime image. Hence, the actual size of NetX Duo is completely determined by the application. For most applications, the instruction image requirements of NetX Duo ranges between 5 KBytes and 30 KBytes in size. With IPv6 and ICMPv6 enabled for IPv6 address configuration and neighbor discovery protocols, NetX Duo ranges in size from 30kbytes to 45kbytes.

NetX Duo achieves superior network performance by layering internal component function calls only when it is absolutely necessary. In addition, much of NetX Duo processing is done directly in-line, resulting in outstanding performance advantages over the workstation network software used in embedded designs in the past.

Zero-copy Implementation

NetX Duo provides a packet-based, zero-copy implementation of TCP/IP. Zero copy means that data in the application's packet buffer are never copied inside NetX Duo. This greatly improves performance and frees up valuable processor cycles to the application, which is extremely important in embedded applications.

UDP Fast Path™ Technology

With *UDP Fast Path Technology*, NetX Duo provides the fastest possible UDP processing. On the sending side, UDP processing—including the optional UDP checksum—is completely contained within the ***nx_udp_socket_send*** service. No additional function calls are made until the packet is ready to be sent via the internal NetX Duo IP send routine. This routine is also flat (i.e., its function call nesting is minimal) so the packet is quickly dispatched to the application's network driver. When the UDP packet is received, the NetX Duo packet-receive processing places the packet directly on the appropriate UDP socket's receive queue or gives it to the first thread suspended waiting for a receive packet from the UDP socket's receive queue. No additional ThreadX context switches are necessary.

ANSI C Source Code

NetX Duo is written completely in ANSI C and is portable immediately to virtually any processor architecture that has an ANSI C compiler and ThreadX support.

Not A Black Box

Most distributions of NetX Duo include the complete C source code. This eliminates the "black-box" problems that occur with many commercial network stacks. By using NetX Duo, applications developers can see exactly what the network stack is doing—there are no mysteries!

Having the source code also allows for application-specific modifications. Although not recommended, it is certainly beneficial to have the ability to modify the network stack if it is required.

These features are especially comforting to developers accustomed to working with in-house or public domain network stacks. They expect to have source code and the ability to modify it. NetX Duo is the ultimate network software for such developers.

BSD-Compatible Socket API

For legacy applications, NetX Duo also provides a BSD-compatible socket interface that makes calls to the high-performance NetX Duo API underneath. This helps in migrating existing network application code to NetX Duo.

RFCs Supported by NetX Duo

NetX Duo support of RFCs describing basic network protocols includes but is not limited to the following network protocols. NetX Duo follows all general recommendations and basic requirements within the constraints of a real-time operating system with small memory footprint and efficient execution.

RFC	Description
RFC 1112	Host Extensions for IP Multicasting (IGMPv1)
RFC 1122	Requirements for Internet Hosts - Communication Layers
RFC 2236	Internet Group Management Protocol, Version 2
RFC 768	User Datagram Protocol (UDP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)

RFC	Description
RFC 826	Ethernet Address Resolution Protocol (ARP)
RFC 903	Reverse Address Resolution Protocol (RARP)
RFC 5681	TCP Congestion Control

Below are the IPv6-related RFCs supported by NetX Duo.

RFC	Description
RFC 1981	Path MTU Discovery for Internet Protocol v6 (IPv6)
RFC 2460	Internet Protocol v6 (IPv6) Specification
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 4291	Internet Protocol v6 (IPv6) Addressing Architecture
RFC 4443	Internet Control Message Protocol (ICMPv6) for Internet Protocol v6 (IPv6) Specification
RFC 4861	Neighbor Discovery for IP v6
RFC 4862	IPv6 Stateless Address Auto Configuration

Embedded Network Applications

Embedded network applications are applications that need network access and execute on microprocessors hidden inside products such as cellular phones, communication equipment, automotive engines, laser printers, medical devices, and so forth. Such applications almost always have some memory and performance constraints. Another distinction of embedded network applications is that their software and hardware have a dedicated purpose.

Real-time Network Software

Basically, network software that must perform its processing within an exact period of time is called *real-time network* software, and when time constraints are imposed on network applications, they are classified as real-time applications. Embedded network applications are almost always real-time because of their inherent interaction with the external world.

NetX Duo Benefits

The primary benefits of using NetX Duo for embedded applications are high-speed Internet connectivity and very small memory requirements. NetX Duo is also completely integrated with the high-performance, multitasking ThreadX real-time operating system.

Improved Responsiveness

The high-performance NetX Duo protocol stack enables embedded network applications to respond faster than ever before. This is especially important for embedded applications that either have a significant volume of network traffic or stringent processing requirements on a single packet.

Software Maintenance

Using NetX Duo allows developers to easily partition the network aspects of their embedded application. This partitioning makes the entire development process easy and significantly enhances future software maintenance.

Increased Throughput

NetX Duo provides the highest-performance networking available, which is achieved by minimal packet processing overhead. This also enables increased throughput.

Processor Isolation

NetX Duo provides a robust, processor-independent interface between the application and the underlying processor and network hardware. This allows developers to concentrate on the network aspects of the application rather than spending extra time dealing with hardware issues directly affecting networking.

Ease of Use

NetX Duo is designed with the application developer in mind. The NetX Duo architecture and service call interface are easy to understand. As a result, NetX Duo developers can quickly use its advanced features.

Improve Time to Market

The powerful features of NetX Duo accelerate the software development process. NetX Duo abstracts most processor and network hardware issues, thereby removing these concerns from a majority of application network-specific areas. This, coupled with the ease-of-use and advanced feature set, result in a faster time to market!

Protecting the Software Investment

NetX Duo is written exclusively in ANSI C and is fully integrated with the ThreadX real-time operating system. This means NetX Duo applications are instantly portable to all ThreadX supported processors. Better still, a completely new processor architecture can be supported with ThreadX in a matter of weeks. As a result, using NetX Duo ensures the application's migration path and protects the original development investment.

IPv6 Ready Logo Certification

NetX Duo "IPv6 Ready" certification was obtained through the "IPv6 Core Protocol (Phase 2) Self Test" package available from the IPv6 Ready Organization. Refer to the following IPv6-Ready project websites for more information on the test platform and test cases:

```
http://www.ipv6ready.org/
```

The Phase 2 IPv6 Core Protocol Self Test Suite validates that an IPv6 stack observes the requirements set forth in the following RFCs with extensive testing:

Section 1: RFC 2460
Section 2: RFC 4861
Section 3: RFC 4862
Section 4: RFC 1981
Section 5: RFC 4443

IxANVL Test

NetX Duo is tested with IxANVL from IXIA. IxANVL is the industry standard for automated network and protocol validation. More information about IxANVL can be found at:

```
http://www.ixiacom.com/products/ixanvl
```

In particular the following NetX Duo modules are tested with IxANVL:

Module	Standard
IP	RFC791 RFC1122 RFC894
ICMP	RFC792 RFC1122 RFC1812
UDP	RFC768 RFC1122
TCP-Core	RFC793 RFC1122 RFC2460
TCP-Advanced	RFC1191 RFC1981 RFC2001 RFC2385 RFC2463 RFC813 RFC896
TCP-Performance	RFC793 RFC1323 RFC2018

Safety Certifications

TÜV Certification

NetX Duo has been certified by SGS-TÜV Saar for use in safety-critical systems, according to IEC-61508 and IEC-62304. The certification confirms that NetX Duo can be used in the development of safety-related software for the highest safety integrity levels of the International Electrotechnical Commission (IEC) 61508 and IEC 62304, for the "Functional Safety of electrical, electronic, and programmable electronic safety-related systems." SGS-TÜV Saar, formed through a joint venture of Germany's SGS-Group and TÜV Saarland, has become the leading accredited, independent company for testing, auditing, verifying, and certifying embedded software for safety-related systems worldwide. The industrial safety standard IEC 61508, and all standards that are derived from it, including IEC 62304, are used to assure the functional safety of electrical, electronic, and programmable electronic safety-related medical devices, process control systems, industrial machinery, and railway control systems.

SGS-TÜV Saar has certified NetX Duo to be used in safety-critical automotive systems, according to the ISO 26262 standard. Furthermore NetX Duo is certified to Automotive Safety Integrity Level (ASIL) D, which represents the highest level of ISO 26262 certification.

In addition, SGS-TÜV Saar has certified NetX Duo to be used in safety-critical railway applications, meeting to the EN 50128 standard up to SW-SIL 4.

SGS TÜV SAAR FUNKTIONALE SICHERHEIT GEPRÜFT FUNCTIONAL SAFETY APPROVED

IEC 61508 up to SIL 4
IEC 62304 up to SW safety Class C
ISO 26262 ASIL D
EN 50128 SW-SIL 4

Please contact sales@expresslogic.com for more information on which version(s) of NetX Duo have been certified by TÜV or for the availability of test reports, certificates, and associated documentation.

UL Certification

NetX Duo has been certified by UL for compliance with UL 60730-1 Annex H, CSA E60730-1 Annex H, IEC 60730-1 Annex H, UL 60335-1 Annex R, IEC 60335-1 Annex R, and UL 1998 safety standards for software in programmable components. Along with IEC/UL 60730-1, which has requirements for “Controls Using Software” in its Annex H, the IEC 60335-1 standard describes the requirements for “Programmable Electronic Circuits” in its Annex R. IEC 60730 Annex H and IEC 60335-1 Annex R address the safety of MCU hardware and software used in appliances such as washing machines, dishwashers, dryers, refrigerators, freezers, and ovens.

UL/IEC 60730, UL/IEC 60335, UL 1998

Please contact azure-rtos support@microsoft.com *for more information on which version(s) of NetX Duo have been certified by UL or for the availability of test reports, certificates, and associated documentation.*

Chapter 2: Installation and Use of NetX Duo

This chapter contains a description of various issues related to installation, setup, and use of the high-performance network stack Azure RTOS NetX Duo, including the following:

Host Considerations

Embedded development is usually performed on Windows or Linux (Unix) host computers. After the application is compiled, linked, and the executable is generated on the host, it is downloaded to the target hardware for execution.

Usually the target download is done from within the development tool's debugger. After download, the debugger is responsible for providing target execution control (go, halt, breakpoint, etc.) as well as access to memory and processor registers.

Most development tool debuggers communicate with the target hardware via on-chip debug (OCD) connections such as JTAG (IEEE 1149.1) and Background Debug Mode (BDM). Debuggers also communicate with target hardware through In-Circuit Emulation (ICE) connections. Both OCD and ICE connections provide robust solutions with minimal intrusion on the target resident software.

As for resources used on the host, the source code for NetX Duo is delivered in ASCII format and requires approximately 1 Mbytes of space on the host computer's hard disk.

i *Review the supplied **readme_netx.txt** file for additional host system considerations and options.*

Target Considerations

NetX Duo requires between 5 KBytes and 45 KBytes of Read-Only Memory (ROM) on the target. Another 1 to 5KBytes of the target's Random Access Memory (RAM) are required for the NetX Duo thread stack and other global data structures.

In addition, NetX Duo requires the use of two ThreadX timer objects and one ThreadX mutex object. These facilities are used for periodic processing needs and thread protection inside the NetX Duo protocol stack.

Product Distribution

The exact content of the distribution disk depends on the target processor, development tools, and the NetX Duo package purchased. However, the following is a list of several important files that are common to most product distributions:

NetX_Duo_Express_Startup.pdf
PDF that provides a simple, four-step procedure to get NetX Duo running on a specific target processor/board and specific development tools.

readme_netx.txt Text file containing specific information about the NetX Duo port, including information about the target processor and the development tools.

nx_api.h C header file containing all system equates, data structures, and service prototypes.

nx_port.h	C header file containing all development-tool and target-specific data definitions and structures.
demo_netx.c	C file containing a small demo application.
nx.a (or nx.lib)	Binary version of the NetX C library that is distributed with the standard package.

NetX Duo Installation

Installation of NetX Duo is straightforward. Refer to the ***NetX_Duo_Express_Startup.pdf*** file and the ***readme_netx.txt*** file for specific information on installing NetX Duo for your specific environment.

Be sure to back up the NetX Duo distribution disk and store it in a safe location.

*Application software needs access to the NetX Duo library file (usually **nx.a** or **nx.lib**) and the C include files **nx_api.h, and nx_port.h**. This is accomplished either by setting the appropriate path for the development tools or by copying these files into the application development area.*

Using NetX Duo

Using NetX Duo is easy. Basically, the application code must include ***nx_api.h*** during compilation and link with the NetX Duo library ***nx.a*** (or ***nx.lib***).

The following are the four easy steps required to build a NetX Duo application:

Step 1: Include the ***nx_api.h*** file in all application files that use NetX Duo services or data structures.

Step 2: Initialize the NetX Duo system by calling ***nx_system_initialize*** from the ***tx_application_define*** function or an application thread.

Step 3: Create an IP instance, enable the Address Resolution Protocol (ARP), if necessary, and any sockets after ***nx_system_initialize*** is called.

Step 4: Compile application source and link with the NetX Duo runtime library ***nx.a*** (or ***nx.lib***). The resulting image can be downloaded to the target and executed!

Troubleshooting

Each NetX Duo port is delivered with one or more demonstrations that execute on an actual network or via a simulated network driver. It is always a good idea to get the demonstration system running first.

*See the **readme_netx.txt** file supplied with the distribution for more specific details regarding the demonstration system.*

If the demonstration system does not run properly, perform the following operations to narrow the problem:

1. Determine how much of the demonstration is running.
2. Increase stack sizes in any new application threads.

3. Recompile the NetX Duo library with the appropriate debug options listed in the configuration option section.
4. Examine the NX_IP structure to see if packets are being sent or received.
5. Examine the default packet pool to see if there are available packets.
6. Ensure the network driver is supplying ARP and IP packets with its headers on 4-byte boundaries for applications requiring IPv4 or IPv6 connectivity.
7. Temporarily bypass any recent changes to see if the problem disappears or changes. Such information should prove useful to Azure RTOS support engineers.

Follow the procedures outlined in the “What We Need From You” on page 10 to send the information gathered from the troubleshooting steps.

Configuration Options

There are several configuration options when building the NetX Duo library and the application using NetX Duo. The configuration options can be defined in the application source, on the command line, or within the ***nx_user.h*** include file, unless otherwise specified.

*Options defined in **nx_user.h** are applied only if the application and NetX Duo library are built with **NX_INCLUDE_USER_DEFINE_FILE** defined.*

Review the ***readme_netx_duo_generic.txt*** file for additional options for your specific version of NetX Duo. The following sections list the configuration options available in NetX Duo. General options applicable to both IPv4 and IPv6 are listed first, followed by IPv6-specific options.

System Configuration Options

NX_ASSERT_FAIL
Symbol that defines the debug statement to use when an assertion fails.

NX_DEBUG
Defined, enables the optional print debug information available from the RAM Ethernet network driver.

NX_DEBUG_PACKET
Defined, enables the optional debug packet dumping available in the RAM Ethernet network driver.

NX_DISABLE_ASSERT
Defined, disables ASSERT checks in the source code. By default this option is not defined.

NX_DISABLE_ERROR_CHECKING
Defined, removes the basic NetX Duo error checking API and improves performance. API return codes not affected by disabling error checking are listed in bold typeface in the API definition. This define is typically used after the application is debugged sufficiently and its use improves performance and decreases code size.

NX_DRIVER_DEFERRED_PROCESSING
Defined, enables deferred network driver packet handling. This allows the network driver to place a packet on the IP instance and have the real processing routine called from the NetX Duo internal IP helper thread.

NX_DUAL_PACKET_POOL_ENABLE
Renamed to ***NX_ENABLE_DUAL_PACKET_POOL***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_DUAL_PACKET_POOL***.

NX_ENABLE_DUAL_PACKET_POOL
Defined, allows the stack to use two packet pools, one with large payload size and one with smaller payload size. By default this option is not enabled.

NX_ENABLE_EXTENDED_NOTIFY_SUPPORT
Defined, enables more callback hooks in the stack. These callback functions are used by the BSD wrapper layer. By default this option is not defined.

NX_ENABLE_INTERFACE_CAPABILITY
Defined, allows the interface device driver to specify extra

capability information, such as checksum off-loading. By default this option is not defined.

NX_ENABLE_SOURCE_ADDRESS_CHECK
Defined, enables the source address of incoming packet to be checked. By default this option is disabled.

NX_IPSEC_ENABLE
Defined, enables the NetX Duo library to support IPsec operations. This feature requires the optional NetX Duo IPsec module. By default this feature is not enabled.

NX_LITTLE_ENDIAN
Defined, performs the necessary byte swapping on little endian environments to ensure the protocol headers are in proper big endian format. Note the default is typically setup in ***nx_port.h***.

NX_MAX_PHYSICAL_INTERFACES
Specifies the total number of physical network interfaces on the device. The default value is 1 and is defined in ***nx_api.h***; a device must have at least one physical interface. Note this does not include the loopback interface.

NX_NAT_ENABLE
Defined, NetX Duo is built with NAT process. By default this option is not defined.

NX_PHYSICAL_HEADER
Specifies the size in bytes of the physical header of the frame. The default value is 16 (based on a typical 14-byte Ethernet frame aligned to 32-bit boundary) and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included, such as in ***nx_user.h***.

NX_PHYSICAL_TRAILER
Specifies the size in bytes of the physical packet trailer and is typically used to reserve storage for things like Ethernet CRCs, etc. The default value is 4 and is defined in ***nx_api.h***.

ARP Configuration Options

NX_ARP_DEFEND_BY_REPLY
Defined, allows NetX Duo to defend its IP address by sending an ARP response.

NX_ARP_DEFEND_INTERVAL
Defines the interval, in seconds, the ARP module sends out the next defend packet in response to an incoming ARP message that indicates an address in conflict.

NX_ARP_DISABLE_AUTO_ARP_ENTRY
Renamed to ***NX_DISABLE_ARP_AUTO_ENTRY***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ARP_AUTO_ENTRY***.

NX_ARP_EXPIRATION_RATE
Specifies the number of seconds ARP entries remain valid. The default value of zero disables expiration or aging of ARP entries and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_ARP_MAC_CHANGE_NOTIFICATION_ENABLE
Renamed to ***NX_ENABLE_ARP_MAC_CHANGE_NOTIFICATION***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_ARP_MAC_CHANGE_NOTIFICATION***.

NX_ARP_MAX_QUEUE_DEPTH
Specifies the maximum number of packets that can be queued while waiting for an ARP response. The default value is 4 and is defined in ***nx_api.h***.

NX_ARP_MAXIMUM_RETRIES
Specifies the maximum number of ARP retries made without an ARP response. The default value is 18 and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_ARP_UPDATE_RATE
Specifies the number of seconds between ARP retries. The default value is 10, which represents 10 seconds, and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_DISABLE_ARP_AUTO_ENTRY
Defined, disables entering ARP request information in the ARP cache.

NX_DISABLE_ARP_INFO
Defined, disables ARP information gathering.

NX_ENABLE_ARP_MAC_CHANGE_NOTIFICATION
Defined, allows ARP to invoke a callback notify function on detecting the MAC address is updated.

ICMP Configuration Options

NX_DISABLE_ICMP_INFO
Defined, disables ICMP information gathering.

NX_DISABLE_ICMP_RX_CHECKSUM
Defined, disables both ICMPv4 and ICMPv6 checksum computation on received ICMP packets. This option is useful when the network interface driver is able to verify the ICMPv4 and ICMPv6 checksum, and the application does not use the IP fragmentation feature or the IPsec feature. By default this option is not defined.

NX_DISABLE_ICMP_TX_CHECKSUM
Defined, disables both ICMPv4 and ICMPv6 checksum computation on transmitted ICMP packets. This option is useful where the network interface driver is able to compute the ICMPv4 and ICMPv6 checksum, and the application does not use the IP fragmentation feature or IPsec feature. By default this option is not defined.

NX_DISABLE_ICMPV4_ERROR_MESSAGE
Defined, NetX Duo does not send ICMPv4 Error Messages in response to error conditions such as improperly formatted IPv4 header. By default this option is not defined.

NX_DISABLE_ICMPV4_RX_CHECKSUM
Defined, disables ICMPv4 checksum computation on received ICMP packets. This option is defined automatically if ***NX_DISABLE_ICMP_RX_CHECKSUM*** is defined. By default this option is not defined.

NX_DISABLE_ICMPv4_RX_CHECKSUM
Renamed to ***NX_DISABLE_ICMPV4_RX_CHECKSUM***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV4_RX_CHECKSUM***.

NX_DISABLE_ICMPV4_TX_CHECKSUM
Defined, disables ICMPv4 checksum computation on transmitted ICMP packets. This option is defined automatically if ***NX_DISABLE_ICMP_TX_CHECKSUM*** is defined. By default this option is not defined.

NX_DISABLE_ICMPv4_TX_CHECKSUM
Renamed to ***NX_DISABLE_ICMPV4_TX_CHECKSUM***.

Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV4_TX_CHECKSUM***.

NX_ENABLE_ICMP_ADDRESS_CHECK
Defined, the destination address of ICMP packet is checked. The default is disabled. An ICMP Echo Request destined to an IP broadcast or IP multicast address will be silently discarded.

IGMP Configuration Options

NX_DISABLE_IGMP_INFO
Defined, disables IGMP information gathering.

NX_DISABLE_IGMPV2
Defined, disables IGMPv2 support, and NetX Duo supports IGMPv1 only. By default this option is not set and is defined in ***nx_api.h***.

NX_MAX_MULTICAST_GROUPS
Specifies the maximum number of multicast groups that can be joined. The default value is 7 and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

IP Configuration Options

NX_DISABLE_FRAGMENTATION
Defined, disables both IPv4 and IPv6 fragmentation and reassembly logic.

NX_DISABLE_IPV4
Defined, disables IPv4 functionality. This option can be used to build NetX Duo to suupport IPv6 only. By default this option is not defined.

NX_DISABLE_IP_INFO
Defined, disables IP information gathering.

NX_DISABLE_IP_RX_CHECKSUM
Defined, disables checksum logic on received IPv4 packets. This is useful if the network device is able to verify the IPv4 checksum, and the application does not expect to use IP fragmentation or IPsec.

NX_DISABLE_IP_TX_CHECKSUM
Defined, disables checksum logic on IPv4 packets sent. This is useful in situations in which the underlying network device is capable of generating the IPv4 header checksum, and the application does not expect to use IP fragmentation or IPsec.

NX_DISABLE_LOOPBACK_INTERFACE
Defined, disables NetX Duo support for the loopback interface.

NX_DISABLE_RX_SIZE_CHECKING
Defined, disables the size checking on received packets.

NX_ENABLE_IP_RAW_PACKET_FILTER
Defined, enables the IP raw packet receive filter functionality. Applications requiring more control over the type of raw IP packets to be received can use this feature. The IP raw packet filter feature also supports the raw socket operation in the BSD compatibility layer. By default this option is not defined.

NX_ENABLE_IP_STATIC_ROUTING
Defined, enables IPv4 static routing in which a destination address can be assigned a specific next hop address. By default IPv4 static routing is disabled.

NX_FRAGMENT_IMMEDIATE_ASSEMBLY
Defined, allows IPv4 and IPv6 reassembly logic to execute right away after receiving an IP fragment. By default this option is not defined.

NX_IP_MAX_REASSEMBLY_TIME
Symbol that controls maximum time allowed to reassemble IPv4 fragment and IPv6 fragment. Note the value defined here overwrites both ***NX_IPV4_MAX_REASSEMBLY_TIME*** and ***NX_IPV6_MAX_REASSEMBLY_TIME***.

NX_IP_PERIODIC_RATE
Defined, specifies the number of ThreadX timer ticks in one second. The default value is derived from the ThreadX symbol ***TX_TIMER_TICKS_PER_SECOND,*** which by default is set to 100 (10ms timer). Applications shall exercise caution when modifying this value, as the rest of the NetX Duo modules derive timing information from ***NX_IP_PERIODIC_RATE.***

NX_IP_RAW_MAX_QUEUE_DEPTH
Symbol that controls the number of raw IP packets can be queued on the raw packet receive queue. By default value is set to 20.

NX_IP_ROUTING_TABLE_SIZE

Defined, sets the maximum number of entries in the IPv4 static routing table, which is a list of an outgoing interface and the next hop addresses for a given destination address. The default value is 8 and is defined in ***nx_api.h.*** This symbol is used only if ***NX_ENABLE_IP_STATIC_ROUTING*** is defined.

NX_IPV4_MAX_REASSEMBLY_TIME

Symbol that controls maximum time allowed to reassemble IPv4 fragment. Note the value defined in NX_IP_MAX_REASSEMBLY_TIME overwrites this value.

Packet Configuration Options

NX_DISABLE_PACKET_CHAIN

Defined, disables the packet chain logic. By default this is not defined.

NX_DISABLE_PACKET_INFO

Defined, disables packet pool information gathering.

NX_ENABLE_LOW_WATERMARK

Defined, enables NetX Duo packet pool low watermark feature. Application sets low watermark value. On receiving TCP packets, if the packet pool low watermark is reached, NetX Duo silently discards the packet by releasing it, preventing the packet pool from starvation. By default this feature is not enabled.

NX_ENABLE_PACKET_DEBUG_INFO

Defined, logs packet debug information.

NX_PACKET_ALIGNMENT

Defined, specifies the alignment requirement, in bytes, for starting address of the packet payload area. This option deprecates ***NX_PACKET_HEADER_PAD*** and ***NX_PACKET_HEADER_PAD_SIZE***. By default this option is defined to be 4, making the starting address of the payload area 4-byte aligned.

NX_PACKET_HEADER_PAD

Defined, enables padding towards the end of the NX_PACKET control block. The number of ULONG words to pad is defined by ***NX_PACKET_HEADER_PAD_SIZE***. Note this option is depreciated by ***NX_PACKET_ALIGNMENT***.

NX_PACKET_HEADER_PAD_SIZE
Sets the number of ULONG words to be padded to the NX_PACKET structure, allowing the packet payload area to start at the desired alignment. This feature is useful when receive buffer descriptors point directly into NX_PACKET payload area, and the network interface receive logic or the cache operation logic expects the buffer starting address to meet certain alignment requirements. This value becomes valid only when ***NX_PACKET_HEADER_PAD*** is defined. Note this option is deprecated by ***NX_PACKET_ALIGNMENT***.

RARP Configuration Options

NX_DISABLE_RARP_INFO Defined, disables RARP information gathering.

TCP Configuration Options

NX_DISABLE_RESET_DISCONNECT
Defined, disables the reset processing during disconnect when the timeout value supplied is specified as ***NX_NO_WAIT***.

NX_DISABLE_TCP_INFO Defined, disables TCP information gathering.

NX_DISABLE_TCP_RX_CHECKSUM
Defined, disables checksum logic on received TCP packets. This is only useful in situations in which the link-layer has reliable checksum or CRC processing, or the interface driver is able to verify the TCP checksum in hardware, and the application does not use IPsec.

NX_DISABLE_TCP_TX_CHECKSUM
Defined, disables checksum logic for sending TCP packets. This is only useful in situations in which the receiving network node has received TCP checksum logic disabled or the underlying network driver is capable of generating the TCP checksum, and the application does not use IPsec.

NX_ENABLE_TCP_KEEPALIVE

Defined, enables the optional TCP keepalive timer. The default settings is not enabled.

NX_ENABLE_TCP_MSS_CHECK

Defined, enables the verification of minimum peer MSS before accepting a TCP connection. To use this feature, the symbol ***NX_ENABLE_TCP_MSS_MINIMUM*** must be defined. By default, this option is not enabled.

NX_ENABLE_TCP_QUEUE_DEPTH_UPDATE_NOTIFY

Defined, allows the application to install a callback function that is invoked when the TCP transmit queue depth is no longer at maximum value. This callback serves as an indication that the TCP socket is ready to transmit more data. By default this option is not enabled.

NX_ENABLE_TCP_WINDOW_SCALING

Enables the window scaling option for TCP applications. If defined, window scaling option is negotiated during TCP connection phase, and the application is able to specify a window size larger than 64K. The default setting is not enabled (not defined).

NX_MAX_LISTEN_REQUESTS

Specifies the maximum number of server listen requests. The default value is 10 and is defined in ***nx_api.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_ACK_EVERY_N_PACKETS

Specifies the number of TCP packets to receive before sending an ACK. Note if ***NX_TCP_IMMEDIATE_ACK*** is enabled but ***NX_TCP_ACK_EVERY_N_PACKETS*** is not, this value is automatically set to 1 for backward compatibility.

NX_TCP_ACK_TIMER_RATE

Specifies how the number of system ticks (NX_IP_PERIODIC_RATE) is divided to calculate the timer rate for the TCP delayed ACK processing. The default value is 5, which represents 200ms, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_ENABLE_KEEPALIVE

Renamed to ***NX_ENABLE_TCP_KEEPALIVE***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_TCP_KEEPALIVE***.

NX_TCP_ENABLE_MSS_CHECK

Renamed to ***NX_ENABLE_TCP_MSS_CHECK***.Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_TCP_MSS_CHECK.***

NX_TCP_ENABLE_WINDOW_SCALING

Renamed to ***NX_ENABLE_TCP_WINDOW_SCALING***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_TCP_WINDOW_SCALING***.

NX_TCP_FAST_TIMER_RATE

Specifies how the number of NetX Duo internal ticks (NX_IP_PERIODIC_RATE) is divided to calculate the fast TCP timer rate. The fast TCP timer is used to drive the various TCP timers, including the delayed ACK timer. The default value is 10, which represents 100ms assuming the ThreadX timer is running at 10ms. This value is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_IMMEDIATE_ACK

Defined, enables the optional TCP immediate ACK response processing. Defining this symbol is equivalent to defining ***NX_TCP_ACK_EVERY_N_PACKETS*** to be 1.

NX_TCP_KEEPALIVE_INITIAL

Specifies the number of seconds of inactivity before the keepalive timer activates. The default value is 7200, which represents 2 hours, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_KEEPALIVE_RETRIES

Specifies how many keepalive retries are allowed before the connection is deemed broken. The default value is 10, which represents 10 retries, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_KEEPALIVE_RETRY

Specifies the number of seconds between retries of the keepalive timer assuming the other side of the connection is not responding. The default value is 75, which represents 75 seconds between retries, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_MAX_OUT_OF_ORDER_PACKETS
Symbol that defines the maximum number of out-of-order TCP packets can be kept in the TCP socket receive queue. This symbol can be used to limit the number of packets queued in the TCP receive socket, preventing the packet pool from being starved. By default this symbol is not defined, thus there is no limit on the number of out of order packets being queued in the TCP socket.

NX_TCP_MAXIMUM_RETRIES
Specifies how many data transmit retries are allowed before the connection is deemed broken. The default value is 10, which represents 10 retries, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_MAXIMUM_RX_QUEUE
Symbol that defines the maximum receive queue for TCP sockets. This feature is enabled by ***NX_ENABLE_LOW_WATERMARK***.

NX_TCP_MAXIMUM_TX_QUEUE
Specifies the maximum depth of the TCP transmit queue before TCP send requests are suspended or rejected. The default value is 20, which means that a maximum of 20 packets can be in the transmit queue at any given time. Note packets stay in the transmit queue until an ACK that covers some or all of the packet data is received from the other side of the connection. This constant is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_MSS_MINIMUM
Symbol that defines the minimal MSS value NetX Duo TCP module accepts. This feature is enabled by ***NX_ENABLE_TCP_MSS_CHECK***.

NX_TCP_QUEUE_DEPTH_UPDATE_NOTIFY_ENABLE
Renamed to ***NX_ENABLE_TCP_QUEUE_DEPTH_UPDATE_NOTIFY***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_TCP_QUEUE_DEPTH_UPDATE_NOTIFY***.

NX_TCP_RETRY_SHIFT
Specifies how the retransmit timeout period changes between retries. If this value is 0, the initial retransmit timeout is the same as subsequent retransmit timeouts. If this value is 1, each successive retransmit is twice as long. If this value is 2, each subsequent retransmit timeout is four times as long. The default value is 0 and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

NX_TCP_TRANSMIT_TIMER_RATE
Specifies how the number of system ticks (***NX_IP_PERIODIC_RATE***) is

divided to calculate the timer rate for the TCP transmit retry processing. The default value is 1, which represents 1 second, and is defined in ***nx_tcp.h***. The application can override the default by defining the value before ***nx_api.h*** is included.

UDP Configuration Options

NX_DISABLE_UDP_INFO
Defined, disables UDP information gathering.

NX_DISABLE_UDP_RX_CHECKSUM
Defined, disables the UDP checksum computation on incoming UDP packets. This is useful if the network interface driver is able to verify UDP header checksum in hardware, and the application does not enable IPsec or IP fragmentation logic.

NX_DISABLE_UDP_TX_CHECKSUM
Defined, disables the UDP checksum computation on outgoing UDP packets. This is useful if the network interface driver is able to compute UDP header checksum and insert the value in the IP head before transmitting the data, and the application does not enable IPsec or IP fragmentation logic.

IPv6 Options

NX_DISABLE_IPV6
Disables IPv6 functionality when the NetX Duo library is built. For applications that do not need IPv6, this avoids pulling in code and additional storage space needed to support IPv6.

NX_DISABLE_IPV6_PATH_MTU_DISCOVERY
Defined, disables path MTU discovery, which is used to determine the maximum MTU in the path to a target in the NetX Duo host destination table. This enables the NetX Duo host to send the largest possible packet that will not require fragmentation. By default, this option is defined (path MTU is disabled).

NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY
Defined, allows a callback function to be invoked when the IPv6 address is changed. By default this option is not enabled.

NX_ENABLE_IPV6_MULTICAST
Defined, enables IPv6 multicast join/leave function. By default this option is not enabled.

NX_ENABLE_IPV6_PATH_MTU_DISCOVERY

Defined, enables the IPv6 path MTU discovery feature. By default this option is not enabled.

NX_IPV6_ADDRESS_CHANGE_NOTIFY_ENABLE

Renamed to ***NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY***.

NX_IPV6_DEFAULT_ROUTER_TABLE_SIZE

Specifies the number of entries in the IPv6 routing table. At least onS entry is needed for the default router. Defined in ***nx_api.h***, the default value is 8.

NX_IPV6_DESTINATION_TABLE_SIZE

Specifies the number of entries in the IPv6 destination table. This stores information about next hop addresses for IPv6 addresses. Defined in ***nx_api.h***, the default value is 8.

NX_IPV6_MAX_REASSEMBLY_TIME

Symbol that controls the maximum time allowed to reassemble IPv6 fragment.

NX_IPV6_MULTICAST_ENABLE

Renamed to ***NX_ENABLE_IPV6_MULTICAST***. Although it is still being supported, new designs are encouraged to use ***NX_ENABLE_IPV6_MULTICAST***.

NX_IPV6_PREFIX_LIST_TABLE_SIZE

Specifies the size of the prefix table. Prefix information is obtained from router advertisements and is part of the IPv6 address configuration. Defined in ***nx_api.h***, the default value is 8.

NX_IPV6_STATELESS_AUTOCONFIG_CONTROL

Defined, allows NetX Duo to disable stateless address auto-configuration feature. By default this option is not enabled.

NX_MAX_IPV6_ADDRESSES

Specifies the number of entries in the IPv6 address pool. During interface configuration, NetX Duo uses IPv6 entries from the pool. It is defaulted to (NX_MAX_PHYSICAL_INTERFACES * 3) to allow each interface to have at least one link local address and two global addresses. Note that all interfaces share the IPv6 address pool.

NX_PATH_MTU_INCREASE_WAIT_INTERVAL
Specifies the wait interval in timer ticks to reset the path MTU for a specific target in the destination table. If ***NX_DISABLE_IPV6_PATH_MTU_DISCOVERY*** is defined, defining this symbol has no effect.

NX_PATH_MTU_INCREASE_WAIT_INTERVAL
Symbol that specifies the wait interval (in seconds) to reset the path MTU value for a destination table entry. It is valid only if ***NX_ENABLE_IPV6_PATH_MTU_DISCOVERY*** is defined. By default this value is set to 600 (seconds).

Neighbor Cache Configuration Options

NX_DELAY_FIRST_PROBE_TIME
Specifies the delay in seconds before the first solicitation is sent out for a cache entry in the STALE state. Defined in ***nx_nd_cache.h***, the default value is 5.

NX_DISABLE_IPV6_DAD
Defined, this option disables Duplicate Address Detection (DAD) during IPv6 address assignment. Addresses are set either by manual configuration or through Stateless Address Auto Configuration.

NX_DISABLE_IPV6_PURGE_UNUSED_CACHE_ENTRIES
Defined, this option prevents NetX Duo from removing older cache table entries before their timeout expires to make room for new entries when the table is full. Static and router entries are never purged.

NX_IPV6_DAD_TRANSMITS
Specifies the number of Neighbor Solicitation messages to be sent before NetX Duo marks an interface address as valid. If ***NX_DISABLE_IPV6_DAD*** is defined (DAD disabled), setting this option has no effect. Alternatively, a value of zero (0) turns off DAD but leaves the DAD functionality in NetX Duo. Defined in ***nx_api.h***, the default value is 3.

NX_IPV6_DISABLE_PURGE_UNUSED_CACHE_ENTRIES
Renamed to

NX_DISABLE_IPV6_PURGE_UNUSED_CACHE_ENTRIES. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_IPV6_PURGE_UNUSED_CACHE_ENTRIES***.

NX_IPV6_NEIGHBOR_CACHE_SIZE
Specifies the number of entries in the IPv6 Neighbor Cache table. Defined in ***nx_nd_cache.h***, the default value is 16.

NX_MAX_MULTICAST_SOLICIT
Specifies the number of Neighbor Solicitation messages NetX Duo transmits as part of the IPv6 Neighbor Discovery protocol when mapping between IPv6 address and MAC address is required. Defined in ***nx_nd_cache.h***, the default value is 3.

NX_MAX_UNICAST_SOLICIT
Specifies the number of Neighbor Solicitation messages NetX Duo transmits to determine a specific neighbor's reachability. Defined in ***nx_nd_cache.h***, the default value is 3.

NX_ND_MAX_QUEUE_DEPTH
Symbol that defines the maximum number of packets queued up for ND cache to be resolved. By default this symbol is set to 4.

NX_REACHABLE_TIME
Specifies the time out in seconds for a cache entry to exist in the REACHABLE state with no packets received from the cache destination IPv6 address. Defined in ***nx_nd_cache.h***, the default value is 30.

NX_RETRANS_TIMER
Specifies in milliseconds the length of delay between solicitation packets sent by NetX Duo. Defined in ***nx_nd_cache.h***, the default value is 1000.

NXDUO_DISABLE_DAD
Renamed to ***NX_DISABLE_IPV6_DAD***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_IPV6_DAD***.

NXDUO_DUP_ADDR_DETECT_TRANSMITS
Renamed to ***NX_IPV6_DAD_TRANSMITS***. Although it is still being supported, new designs are encouraged to use ***NX_IPV6_DAD_TRANSMITS***.

Miscellaneous ICMPv6 Configuration Options

NX_DISABLE_ICMPV6_ERROR_MESSAGE
Defined, disables NetX Duo from sending an ICMPv6 error message in response to a problem packet (e.g., improperly formatted header or packet header type is deprecated) received from another host.

NX_DISABLE_ICMPV6_REDIRECT_PROCESS
Defined, disables ICMPv6 redirect packet processing. NetX Duo by default processes redirect messages and updates the destination table with next hop IP address information.

NX_DISABLE_ICMPV6_ROUTER_ADVERTISEMENT_PROCESS
Defined, disables NetX Duo from processing information received in IPv6 router advertisement packets.

NX_DISABLE_ICMPV6_ROUTER_SOLICITATION
Defined, disables NetX Duo from sending IPv6 router solicitation messages at regular intervals to the router.

NX_DISABLE_ICMPV6_RX_CHECKSUM
Defined, disables ICMPv6 checksum computation on received ICMP packets.

NX_DISABLE_ICMPv6_RX_CHECKSUM
Renamed to ***NX_DISABLE_ICMPV6_RX_CHECKSUM***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_CMPV6_RX_CHECKSUM***.

NX_DISABLE_ICMPV6_TX_CHECKSUM
Defined, disables and ICMPv6 checksum computation on transmitted ICMP packets.

NX_DISABLE_ICMPV6_TX_CHECKSUM
Renamed to ***NX_DISABLE_ICMPV6_TX_CHECKSUM***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV6_TX_CHECKSUM***.

NX_ICMPV6_MAX_RTR_SOLICITATIONS
Define the max number of router solicitations a host sends until a router response is received. If no response is received, the host concludes no router is present. The default value is 3.

NX_ICMPV6_RTR_SOLICITATION_DELAY
Specifies the maximum delay for the initial router solicitation in seconds.

NX_ICMPV6_RTR_SOLICITATION_INTERVAL
Specifies the interval between two router solicitation messages. The default value is 4.

NXDUO_DESTINATION_TABLE_SIZE
Renamed to ***NX_IPV6_DESTINATION_TABLE_SIZE***. Although it is still being supported, new designs are encouraged to use ***NX_IPV6_DESTINATION_TABLE_SIZE***.

NXDUO_DISABLE_ICMPV6_ERROR_MESSAGE
Renamed to ***NX_DISABLE_ICMPV6_ERROR_MESSAGE***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV6_ERROR_MESSAGE***.

NXDUO_DISABLE_ICMPV6_REDIRECT_PROCESS
Renamed to ***NX_DISABLE_ICMPV6_REDIRECT_PROCESS***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV6_REDIRECT_PROCESS***

NXDUO_DISABLE_ICMPV6_ROUTER_ADVERTISEMENT_PROCESS
Renamed to ***NX_DISABLE_ICMPV6_ROUTER_ADVERTISEMENT_PROCESS***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV6_ROUTER_ADVERTISEMENT_PROCESS***.

NXDUO_DISABLE_ICMPV6_ROUTER_SOLICITATION
Renamed to ***NX_DISABLE_ICMPV6_ROUTER_SOLICITATION***. Although it is still being supported, new designs are encouraged to use ***NX_DISABLE_ICMPV6_ROUTER_SOLICITATION***.

NXDUO_ICMPV6_MAX_RTR_SOLICITATIONS
Renamed to ***NX_ICMPV6_MAX_RTR_SOLICITATIONS***. Although it is still being supported, new designs are encouraged to use ***NX_ICMPV6_MAX_RTR_SOLICITATIONS***.

NXDUO_ICMPV6_RTR_SOLICITATION_INTERVAL
Renamed to ***NX_ICMPV6_RTR_SOLICITATION_INTERVAL***. This symbol is being depreciated. Although it is still being supported, new designs are encouraged to use ***NX_ICMPV6_RTR_SOLICITATION_INTERVAL***

NetX Duo Version ID

The current version of NetX Duo is available to both the user and the application software during runtime. The programmer can find the NetX Duo version in the ***readme_netx_duo_generic.txt*** file. This file also contains a version history of the corresponding port. Application software can obtain the NetX Duo version by examining the global string ***_nx_version_id*** in ***nx_port.h***.

Application software can also obtain release information from the constants shown below defined in ***nx_api.h****.*

These constants identify the current product release by name and the product major and minor version.

```
#define EL_PRODUCT_NETXDUO
#define NETXDUO_MAJOR_VERSION
#define NETXDUO_MINOR_VERSION
```

Chapter 3: Functional Components of NetX Duo

This chapter contains a description of the high-performance Azure RTOS NetX Duo TCP/IP stack from a functional perspective.

Execution Overview

There are five types of program execution within a NetX Duo application: initialization, application interface calls, internal IP thread, IP periodic timers, and the network driver.

NetX Duo assumes the existence of ThreadX and depends on its thread execution, suspension, periodic timers, and mutual exclusion facilities.

Initialization

The service ***nx_system_initialize*** must be called before any other NetX Duo service is called. System initialization can be called either from the ThreadX ***tx_application_define*** routine or from application threads.

After ***nx_system_initialize*** returns, the system is ready to create packet pools and IP instances. Because creating an IP instance requires a default packet pool, at least one NetX Duo packet pool must exist prior to creating an IP instance. Creating packet pools and IP instances are allowed from the ThreadX initialization function ***tx_application_define*** and from application threads.

Internally, creating an IP instance is accomplished in two parts: The first part is done within the context of the caller, either from ***tx_application_define*** or from an application thread's context. This includes setting up the IP data structure and creating various IP resources, including the internal IP thread. The second part is performed during the initial execution from the internal IP thread. This is where the network driver, supplied during the first part of IP creation, is first called. Calling the network driver from the internal IP thread enables the driver to perform I/O and suspend during its initialization processing.

When the network driver returns from its initialization processing, the IP creation is complete.

Initialization of IPv6 in NetX Duo requires a few additional NetX Duo services. These are described in greater detail in the section ***IPv6 Protocol*** later in this chapter.

*The NetX Duo service **nx_ip_status_check** is available to obtain information on the IP instance and its primary interface status. Such status information includes whether or not the link is initialized, enabled and IP address is resolved. This information is used to synchronize application threads needing to use a newly created IP instance. For multihome systems, see "Multihome Support" on page 58. **nx_ip_interface_status_check** is available to obtain information on the specified interface.*

Application Interface Calls

Calls from the application are largely made from application threads running under the ThreadX RTOS. However, some initialization, create, and enable services may be called from ***tx_application_define***. The "Allowed From" sections in Chapter 4 indicate from which each NetX Duo service can be called.

For the most part, processing intensive activities such as computing checksums is done within the calling thread's context—without blocking access of other threads to the IP instance. For example, on transmission, the UDP checksum calculation is performed inside the ***nx_udp_socket_send*** service, prior to calling the underlying IP send function. On a received packet, the UDP checksum is calculated in the ***nx_udp_socket_receive*** service, executed in the context of the application thread. This helps prevent stalling network requests of higher-priority threads because of processing intensive checksum computation in lower-priority threads.

Values, such as IP addresses and port numbers, are passed to APIs in host byte order. Internally these values are stored in host byte order as well. This allows developers to easily view the values via a debugger. When these values are programmed into a frame for transmission, they are converted to network byte order.

Internal IP Thread

As mentioned, each IP instance in NetX Duo has its own thread. The priority and stack size of the internal IP thread is defined in the ***nx_ip_create*** service. The internal IP thread is created in a ready-to-execute mode. If the IP thread has a higher priority than the calling thread, preemption may occur inside the IP create call.

The entry point of the internal IP thread is at the internal function ***_nx_ip_thread_entry***. When started, the internal IP thread first completes network driver initialization, which consists of making three calls to the application-specific network driver. The first call is to attach the network driver to the IP instance, followed by an initialization call, which allows the network driver to go through the initialization process. After the network driver returns from initialization (it may suspend while waiting for the hardware to be properly set up), the internal IP thread calls the network driver again to enable the link. After the network driver returns from the link enable call, the internal IP thread enters a forever loop checking for various events that need processing for this IP instance. Events processed in this loop include deferred IP packet reception, IP packet fragment assembly, ICMP ping processing, IGMP processing, TCP packet queue processing, TCP periodic processing, IP fragment assembly timeouts, and IGMP periodic processing. Events also include address resolution activities; ARP packet processing and ARP periodic processing in IPv4, Duplicate Address Detection, Router Solicitation, and Neighbor Discovery in IPv6.

The NetX Duo callback functions, including listen and disconnect callbacks, are called from the internal IP thread—not the original calling thread. The application must take care not to suspend inside any NetX Duo callback function.

IP Periodic Timers

There are two ThreadX periodic timers used for each IP instance. The first one is a one-second timer for ARP, IGMP, TCP timeout, and it also drives IP fragment reassemble processing. The second timer is a 100ms timer to drive the TCP retransmission timeout and IPv6-related operations.

Network Driver

Each IP instance in NetX Duo has a primary interface, which is identified by its device driver specified in the ***nx_ip_create*** service. The network driver is responsible for handling various NetX Duo requests, including packet transmission, packet reception, and requests for status and control.

For a multi-home system, the IP instance has multiple interfaces, each with an associated network driver that performs these tasks for the respective interface.

The network driver must also handle asynchronous events occurring on the media. Asynchronous events from the media include packet reception, packet transmission completion, and status changes. NetX Duo provides the network driver with several access functions to handle various events. These functions are designed to be called from the interrupt service routine portion of the network driver. For IPv4 networks, the network driver should forward all ARP packets received to the ***_nx_arp_packet_deferred_receive*** internal function. All RARP packets should be forwarded to ***_nx_rarp_packet_deferred_receive*** internal function. There are two options for IP packets. If fast dispatch of IP packets is required, incoming IP packets should be forwarded to ***_nx_ip_packet_receive*** for immediate processing. This greatly improves NetX Duo performance in handling IP packets. Otherwise, forwarding IP packets to ***_nx_ip_packet_deferred_receive*** should be done. This service places the IP packet in the deferred processing queue where it is then handled by the internal IP thread, which results in the least amount of ISR processing time.

The network driver can also defer interrupt processing to run out of the context of the IP thread. In this mode, the ISR shall save the necessary information, call the internal function ***_nx_ip_driver_deferred_processing***, and acknowledge the interrupt controller. This service notifies IP thread to schedule a callback to the device driver to complete the process of the event that causes the interrupt.

Some network controllers are capable of performing TCP/IP header checksum computation and validation in hardware, without taking up valuable CPU resources. To take advantage of the hardware capability feature, NetX Duo provides options to enable or disable various software checksum computation at compilation time, as well as turning on or off checksum computation at run time, if the device driver is able to communicate with the IP layer about is hardware capabilities. See “Chapter 5: NetX Duo Network Drivers” on page 517 for more detailed information on writing NetX Duo network drivers.

Multihome Support

NetX Duo supports systems connected to multiple physical devices using a single IP instance. Each physical interface is assigned to an interface control block in the IP instance. Applications wishing to use a multihome system must define the value for ***NX_MAX_PHSYCIAL_INTERFACES*** to the number of physical devices attached to the system, and rebuild NetX Duo library. By default ***NX_MAX_PHYSICAL_INTERFACES*** is set to one, creating one interface control block in the IP instance.

The NetX Duo application creates a single IP instance for the primary device using the ***nx_ip_create*** service. For each additional network devices, the application attaches the device to the IP instance using the ***nx_ip_interface_attach*** service.

Each network interface structure contains a subset of network information about the network interface that is contained in the IP control block, including interface IPv4 address, subnet mask, IP MTU size, and MAC-layer address information.

NetX Duo with multihome support is backward compatible with earlier versions of NetX Duo. Services that do not take explicit interface information default to the primary network device.

The primary interface has index zero in the IP instance list. Each subsequent device attached to the IP instance is assigned the next index.

All upper layer protocol services for which the IP instance is enabled, including TCP, UDP, ICMP, and IGMP, are available to all the attached devices.

In most cases, NetX Duo can determine the best source address to use when transmitting a packet. The source address selection is based on the destination address. NetX Duo services are added to allow applications to specify a specific source address to use, in cases where the most suitable one cannot be determined by the destination address. An example would be in a multihome system, an application needs to send a packet to an IPv4 broadcast or multicast destination addresses.

Services specifically for developing multihome applications include the following:

nx_igmp_multicast_interface_join
nx_igmp_multicast_interface_leave
nx_ip_driver_interface_direct_command
nx_ip_interface_address_get
nx_ip_interface_address_mapping_configure
nx_ip_interface_address_set
nx_ip_interface_attach
nx_ip_interface_capability_get
nx_ip_interface_capability_set
nx_ip_interface_detach
nx_ip_interface_info_get
nx_ip_interface_mtu_set
nx_ip_interface_physical_address_get
nx_ip_interface_physical_address_set
nx_ip_interface_status_check
nx_ip_raw_packet_source_send
nx_ipv4_multicast_interface_join
nx_ipv4_multicast_interface_leave
nx_udp_socket_source_send
nxd_ipv6_multicast_interface_join
nxd_ipv6_multicast_interface_leave
nxd_udp_socket_source_send
nxd_icmp_source_ping
nxd_ip_raw_packet_source_send
nxd_udp_socket_source_send

These services are explained in greater detail in “Chapter 4: Description of NetX Duo Services” on page 149.

Loopback Interface

The loopback interface is a special network interface without an physical link attached to. The loopback interface allows applications to communicate using the IPv4 loopback address 127.0.0.1

To utilize a logical loopback interface, ensure the configurable option ***NX_DISABLE_LOOPBACK_INTERFACE*** is not set.

Interface Control Blocks

The number of interface control blocks in the IP instance is the number of physical interfaces (defined by ***NX_MAX_PHYSICAL_INTERFACES***) plus the loopback interface if it is enabled. The total number of interfaces is defined in ***NX_MAX_IP_INTERFACES***.

Protocol Layering

The TCP/IP implemented by NetX Duo is a layered protocol, which means more complex protocols are built on top of simpler underlying protocols. In TCP/IP, the lowest layer protocol is at the *link level* and is handled by the network driver. This level is typically targeted towards Ethernet, but it could also be fiber, serial, or virtually any physical media.

On top of the link layer is the *network layer*. In TCP/IP, this is the IP, which is basically responsible for sending and receiving simple packets—in a best-effort manner—across the network. Management-type protocols like ICMP and IGMP are typically also categorized as network layers, even though they rely on IP for sending and receiving.

The *transport layer* rests on top of the network layer. This layer is responsible for managing the flow of data between hosts on the network. There are two types of transport services supported by NetX Duo: UDP and

TCP. UDP services provide best-effort sending and receiving of data between two hosts in a connectionless manner, while TCP provides reliable connection-oriented service between two host entities.

This layering is reflected in the actual network data packets. Each layer in TCP/IP contains a block of information called a header. This technique of surrounding data (and possibly protocol information) with a header is typically called data encapsulation. Figure 1 shows an example of NetX Duo layering and Figure 2 shows the resulting data encapsulation for UDP data being sent.

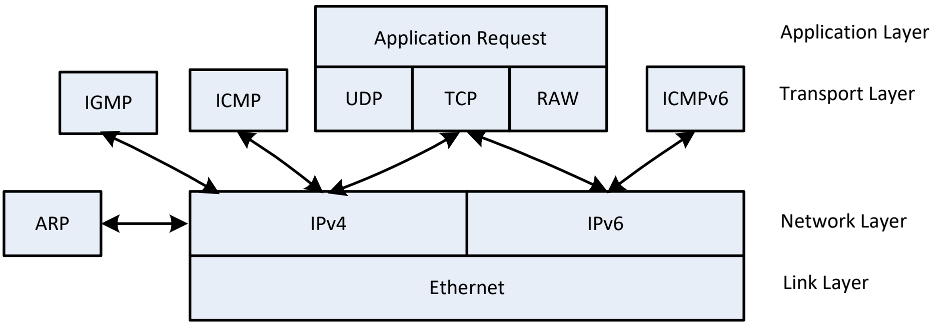


FIGURE 1. Protocol Layering

Packet Pools

Allocating packets in a fast and deterministic manner is always a challenge in real-time networking applications. With this in mind, NetX Duo provides the ability to create and manage multiple pools of fixed-size network packets.

Because NetX Duo packet pools consist of fixed-size memory blocks, there are never any internal fragmentation problems. Of course, fragmentation

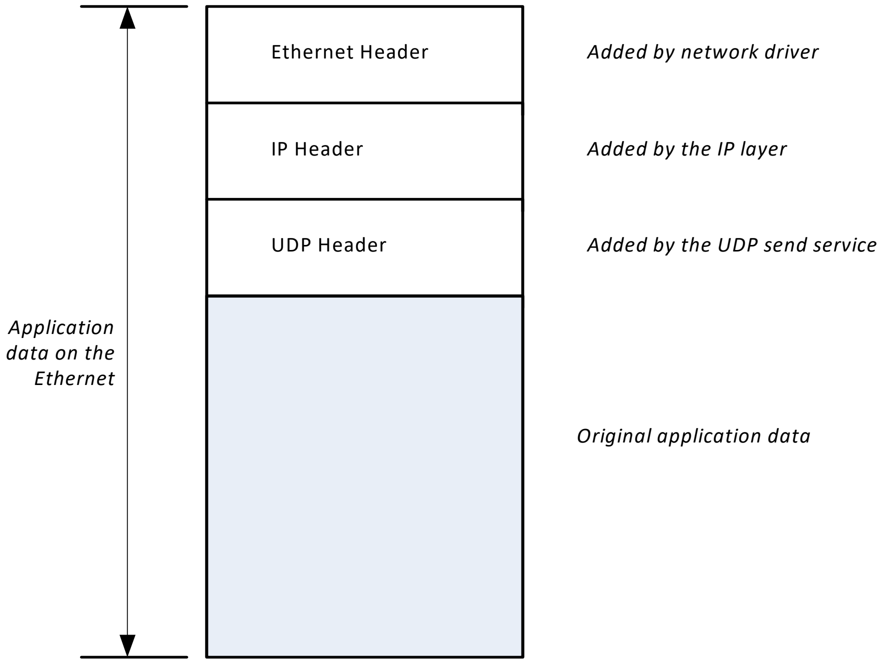


FIGURE 2. UDP Data Encapsulation

causes behavior that is inherently nondeterministic. In addition, the time required to allocate and free a NetX Duo packet amounts to simple linked-list manipulation. Furthermore, packet allocation and deallocation is done at the head of the available list. This provides the fastest possible linked list processing.

Lack of flexibility is typically the main drawback of fixed-size packet pools. Determining the optimal packet payload size that also handles the worst-case incoming packet is a difficult task. NetX Duo packets address this problem with an optional feature called packet chaining. An actual network packet can be made of one or more NetX Duo packets linked together. In addition, the packet header maintains a pointer to the top of the packet. As additional protocols are added, this pointer is simply moved backwards and the new header is written directly in front of the data. Without the flexible packet technology, the stack would have to allocate another buffer and copy the data into a new buffer with the new header, which is processing intensive.

Since each packet payload size is fixed for a given packet pool, application data larger than the payload size would require multiple packets chained together. When filling a packet with user data, the application shall use the service ***nx_packet_data_append***. This service moves application data into a packet. In situations where a packet is not enough to hold user data, additional packets are allocated to store user data. To use packet chaining, the driver must be able to receive into or transmit from chained packets.

For embedded systems that do not need to use the packet chaining feature, the NetX Duo library can be built with ***NX_DISABLE_PACKET_CHAIN*** to remove the packet chaining logic. Note that the IP fragmentation and reassembly feature may need to utilize the chained packet feature. Therefore defining ***NX_DISABLE_PACKET_CHAIN*** requires ***NX_DISABLE_FRAGMENTATION*** also be defined.

Each NetX Duo packet memory pool is a public resource. NetX Duo places no constraints on how packet pools are used.

Packet Pool Memory Area

The memory area for the packet pool is specified during creation. Like other memory areas for

ThreadX and NetX Duo objects, it can be located anywhere in the target's address space.

This is an important feature because of the considerable flexibility it gives the application. For example, suppose that a communication product has a high-speed memory area for network buffers. This memory area is easily utilized by making it into a NetX Duo packet memory pool.

Creating Packet Pools

Packet pools are created either during initialization or during runtime by application threads. There are no limits on the number of packet memory pools in a NetX Duo application.

Dual Packet Pool

Typically the payload size of the default IP packet pool is large enough to accommodate frame size up to the network interface MTU. During normal operation, the IP thread needs to send messages such as ARP, TCP control messages, IGMP messages, ICMPv6 messages. These messages use the packets allocated from the default packet pool in the IP instance. On a memory-constrained system where the amount of memory available for packet pool is limited, using a single packet pool (with the large payload size to match MTU size) may not be an optimal solution. NetX Duo allows application to install an auxiliary packet pool, where the payload size is smaller. Once the auxiliary packet pool is installed, the IP helper thread would allocate packets from either the default packet pool or the auxiliary pool, depending on the size of the message it transmits. For an auxiliary packet pool, a payload size of 200 bytes would work with most of the messages the IP helper thread transmits.

By default NetX Duo library is built without enabling dual packet pool. To enable the feature, build the library with ***NX_DUAL_PACKET_POOL_ENABLE*** defined. Then the auxiliary packet pool can be set by calling ***nx_ip_auxiliary_packet_pool_set***.

There is also the option of creating more than one packet pool. For example a transmit packet pool is created with optimal payload size for expected message sizes. A receive packet pool is created in the driver with a payload size set to the driver MTU, since one cannot predict the size of received packets.

Packet Header NX_PACKET

By default, NetX Duo places the packet header immediately before the packet payload area. The packet memory pool is basically a series of packets—headers followed immediately by the packet payload. The packet header (***NX_PACKET***) and the layout of the packet pool are pictured in Figure 3.

For network devices driver that are able to perform zero copy operations, typically the starting address of the packet payload area is programmed into the DMA logic. Certain DMA engines have alignment requirement on the payload area. To make the starting address of the payload area align properly for the DMA engine, or the cache operation, the user can define the symbol ***NX_PACKET_ALIGNMENT***.

*It is important for the network driver to use the **nx_packet_transmit_release** function when transmission of a packet is complete. This function checks to make sure the packet is not part of a TCP output queue before it is actually placed back in the available pool.*

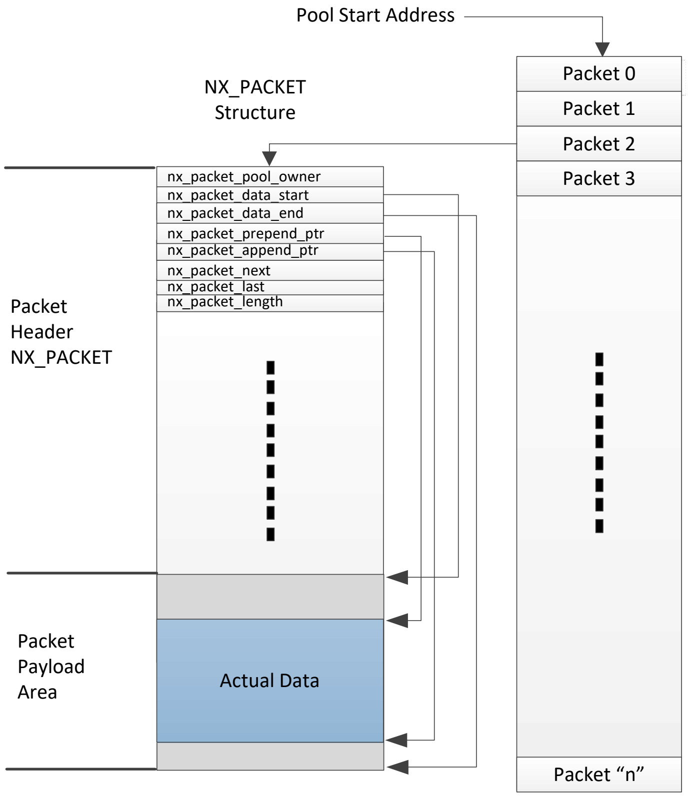


FIGURE 3. Packet Header and Packet Pool Layout

The fields of the packet header are defined as follows. Note that this table is not a comprehensive list of all the members in the *NX_PACKET* structure.

Packet header	Purpose
nx_packet_pool_owner	This field points to the packet pool that owns this particular packet. When the packet is released, it is released to this particular pool. With the pool ownership inside each packet, it is possible for a datagram to span multiple packets from multiple packet pools.
nx_packet_next	This field points to the next packet within the same frame. If NULL, there are no additional packets that are part of the frame. This field is also used to hold fragmented packets until the entire packet can be re-assembled. it is removed if ***NX_DISABLE_PACKET_CHAIN*** is defined.
nx_packet_last	This field points to the last packet within the same network packet. If NULL, this packet represents the entire network packet. This field is removed if ***NX_DISABLE_PACKET_CHAIN*** is defined.
nx_packet_length	This field contains the total number of bytes in the entire network packet, including the total of all bytes in all packets chained together by the *nx_packet_next* member.

Packet header	Purpose
nx_packet_ip_interface	This field is the interface control block which is assigned to the packet when it is received by the interface driver, and by NetX Duo for outgoing packets. An interface control block describes the interface e.g. network address, MAC address, IP address and interface status such as link enabled and physical mapping required.
nx_packet_data_start	This field points to the start of the physical payload area of this packet. It does not have to be immediately following the NX_PACKET header, but that is the default for the ***nx_packet_pool_create*** service.
nx_packet_data_end	This field points to the end of the physical payload area of this packet. The difference between this field and the *nx_packet_data_start* field represents the payload size.
nx_packet_prepend_ptr	This field points to the location of where packet data, either protocol header or actual data, is added in front of the existing packet data (if any) in the packet payload area. It must be greater than or equal to the *nx_packet_data_start* pointer location and less than or equal to the *nx_packet_append_ptr* pointer. *For performance reasons, NetX Duo assumes that when the packet is passed into NetX Duo services for transmission, the prepend pointer points to long word aligned address.*

Packet header	Purpose
nx_packet_append_ptr	This field points to the end of the data currently in the packet payload area. It must be in between the memory location pointed to by *nx_packet_prepend_ptr* and *nx_packet_data_end.* The difference between this field and the *nx_packet_prepend_ptr* field represents the amount of data in this packet.
nx_packet_packet_pad	This fields defines the length of padding in 4-byte words to achieve the desired alignment requirement. This field is removed if ***NX_PACKET_HEADER_PAD*** is not defined. Alternatively ***NX_PACKET_ALIGNMENT*** can be used instead of defining *nx_packet_header_pad.*

Packet Header Offsets

Packet header size is defined to allow enough room to accommodate the size of the header. The ***nx_packet_allocate*** service is used to allocate a packet and adjusts the prepend pointer in the packet according to the type of packet specified. The packet type tells NetX Duo the offset required for inserting the protocol header (such as UDP, TCP, or ICMP) in front of the protocol data.

The following types are defined in NetX Duo to take into account the IP header and physical layer (Ethernet) header in the packet. In the latter case, it is assumed to be 16 bytes taking the required 4-byte alignment into consideration. IPv4 packets are still defined in NetX Duo for applications to allocate packets for IPv4 networks. Note that if the NetX Duo library is built with IPv6 enabled, the generic packet types (such as NX_IP_PACKET) are mapped to the IPv6 version. If the NetX Duo Library is built without

IPv6 enabled, these generic packet types are mapped to the IPv4 version.

The following table shows symbols defined with IPv6 enabled:

Packet Type	Value
NX_IPv6_PACKET (NX_IP_PACKET)	0x38
NX_UDPv6_PACKET (NX_UDP_PACKET)	0x40
NX_TCPv6_PACKET (NX_TCP_PACKET)	0x4c
NX_IPv4_PACKET	0x24
NX_IPv4_UDP_PACKET	0x2c
NX_IPv4_TCP_PACKET	0x38

The following table shows symbols defined with IPv6 disabled:

Packet Type	Value
NX_IPv4_PACKET (NX_IP_PACKET)	0x24
NX_IPv4_UDP_PACKET (NX_UDP_PACKET)	0x2c
NX_IPv4_TCP_PACKET (NX_TCP_PACKET)	0x38

Note that these values will change if *NX_IPSEC_ENABLE* is defined. For application using IPsec, refer to NetX Duo IPsec User Guide for more information.

Pool Capacity

The number of packets in a packet pool is a function of the payload size and the total number of bytes in the memory area supplied to the packet pool create service. The capacity of the pool is calculated by dividing the packet size (including the size of the NX_PACKET header, the payload size, and proper alignment) into the total number of bytes in the supplied memory area.

Payload Area Alignment

Packet pool design in NetX Duo supports zero-copy. At the device driver level, the driver is able to assign the payload area directly into buffer descriptors for data reception. Sometimes the DMA engine or the cache synchronization mechanism requires the starting address of the payload area to have a certain alignment requirement.   This can be achieved by defining the desired alignment requirement (in bytes) in ***NX_PACKET_ALIGNMENT***. When creating a packet pool, the starting address of the payload area will aligned to this value. By default, starting address is 4-byte aligned.

Thread Suspension

Application threads can suspend while waiting for a packet from an empty pool. When a packet is returned to the pool, the suspended thread is given this packet and resumed.

If multiple threads are suspended on the same packet pool, they are resumed in the order they were suspended (FIFO).

Pool Statistics and Errors

If enabled, the NetX Duo packet management software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for packet pools:

Total Packets in Pool
Free Packets in Pool
Total Packet Allocations
Pool Empty Allocation Requests
Pool Empty Allocation Suspensions
Invalid Packet Releases

All of these statistics and error reports, except for total and free packet count in pool, are built into NetX Duo library unless ***NX_DISABLE_PACKET_INFO*** is defined. This data is available to the application with the ***nx_packet_pool_info_get*** service.

Packet Pool Control Block NX_PACKET_POOL

The characteristics of each packet memory pool are found in its control block. It contains useful information such as the linked list of free packets, the number of free packets, and the payload size for packets in this pool. This structure is defined in the ***nx_api.h*** file.

Packet pool control blocks can be located anywhere in memory, but it is most common to make the control block a global structure by defining it outside the scope of any function.

IPv4 Protocol

The Internet Protocol (IP) component of NetX Duo is responsible for sending and receiving IPv4 packets on the Internet. In NetX Duo, it is the component ultimately responsible for sending and receiving TCP, UDP, ICMP, and IGMP messages, utilizing the underlying network driver.

NetX Duo supports both IPv4 protocol (RFC 791) and IPv6 protocol (RFC 2460). This section discusses IPv4. IPv6 is discussed in the next section.

IPv4 Addresses

Each host on the Internet has a unique 32-bit identifier called an IP address. There are five classes of IPv4 addresses as described in Figure 4. The ranges of the five IPv4 address classes are as follows:

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

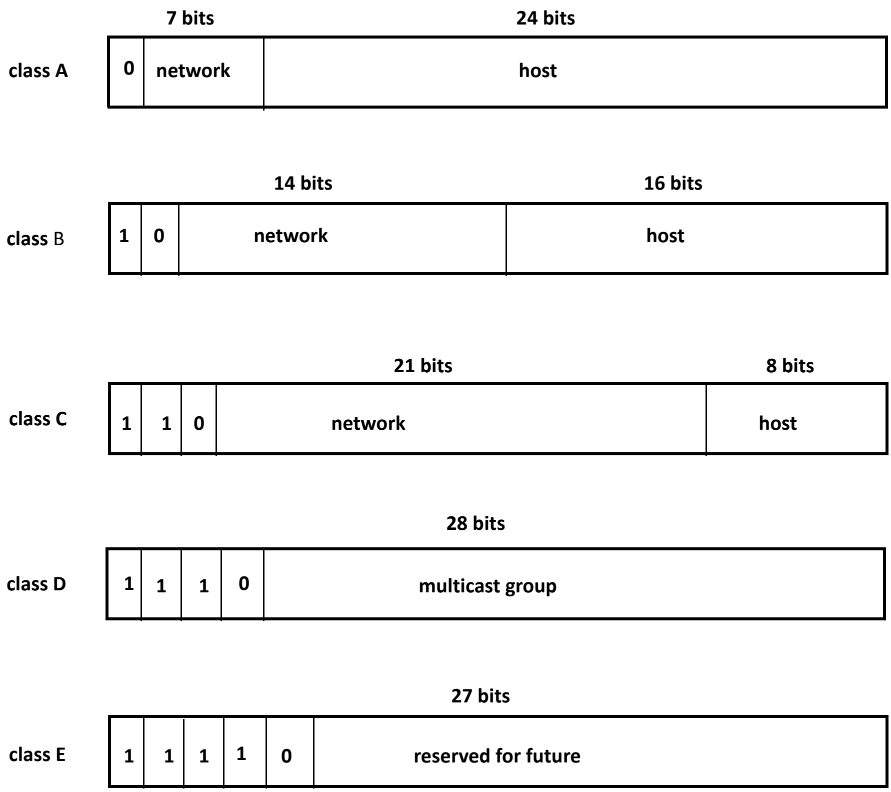


FIGURE 4. IPv4 Address Structure

There are also three types of address specifications: *unicast*, *broadcast*, and *multicast*. Unicast addresses are those IPv4 addresses that identify a specific host on the Internet. Unicast addresses can be either a source or a destination IPv4 address. A broadcast address identifies all hosts on a specific network or sub-network and can only be used as destination addresses. Broadcast addresses are specified by having the host ID portion of the address set to ones. Multicast addresses (Class D) specify a dynamic group of hosts on the Internet. Members of the multicast group may join and leave whenever they wish.

Only connectionless protocols like UDP over IPv4 can utilize broadcast and the limited broadcast capability of the multicast group.

The macro IP_ADDRESS *is defined in* **nx_api.h***. It allows easy specification of IPv4 addresses using commas instead of a periods. For example,* IP_ADDRESS(128,0,0,0) *specifies the first class B address shown in Figure 4.*

IPv4 Gateway Address

Network gateways assist hosts on their networks to relay packets destined to destinations outside the local domain. Each node has some knowledge of which next hop to send to, either the destination one of its neighbors, or through a pre-programmed static routing table. However if these approaches fail, the node should forward the packet to its default gateway which has better knowledge on how to route the packet to its destination. Note that the default gateway must be directly accessible through one of the physical interfaces attached to the IP instance. The application calls ***nx_ip_gateway_address_set*** to configure IPv4 default gateway address. Use the service ***nx_ip_gateway_address_get*** to retrieve the current IPv4 gateway settings. Application shall use the service ***nx_ip_gateway_address_clear*** to clear the gateway setting.

IPv4 Header

For any IPv4 packet to be sent on the Internet, it must have an IPv4 header. When higher-level protocols (UDP, TCP, ICMP, or IGMP) call the IP component to send a packet, the IPv4 transmit module places an IPv4 header in front of the data. Conversely, when IP packets are received from the network, the IP component removes the IPv4 header from the packet before delivery to the higher-level protocols. Figure 5 shows the format of the IP header.

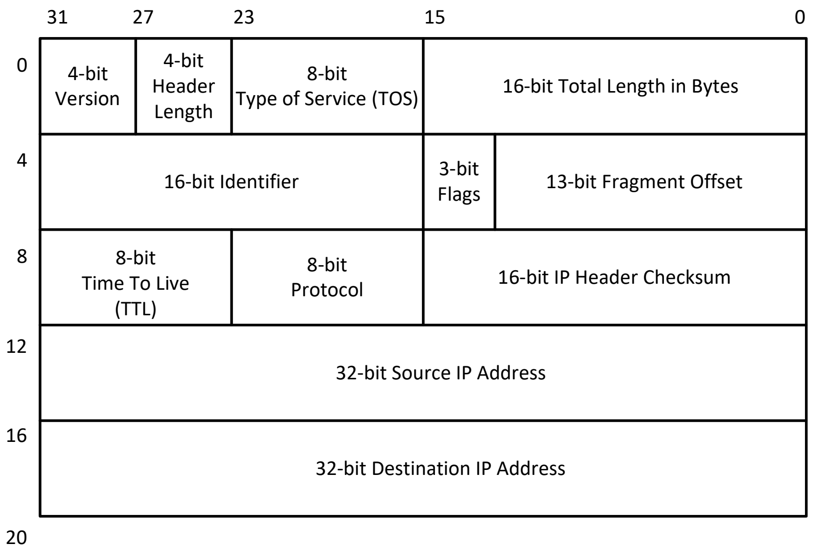


FIGURE 5. IPv4 Header Format

*All headers in the TCP/IP implementation are expected to be in **big endian** format. In this format, the most significant byte of the word resides at the lowest byte address. For example, the 4-bit version and the 4-bit header length of the IP header must be located on the first byte of the header.*

The fields of the IPv4 header are defined as follows:

IPv4 Header Field	Purpose
4-bit version	This field contains the version of IP this header represents. For IP version 4, which is what NetX Duo supports, the value of this field is 4.
4-bit header length	This field specifies the number of 32-bit words in the IP header. If no option words are present, the value for this field is 5.
8-bit type of service (TOS)	This field specifies the type of service requested for this IP packet. Valid requests are as follows:

TOS Request	Value
Normal	0x00
Minimum Delay	0x10
Maximum Data	0x08
Maximum Reliability	0x04
Minimum Cost	0x02

IPv4 Header Field	Purpose
16-bit total length	This field contains the total length of the IP datagram in bytes, including the IP header. An IP datagram is the basic unit of information found on a TCP/IP Internet. It contains a destination and source address in addition to data. Because it is a 16-bit field, the maximum size of an IP datagram is 65,535 bytes.
16-bit identification	The field is a number used to uniquely identify each IP datagram sent from a host. This number is typically incremented after an IP datagram is sent. It is especially useful in assembling received IP packet fragments.

IPv4 Header Field	Purpose
3-bit flags	This field contains IP fragmentation information. Bit 14 is the “don’t fragment” bit. If this bit is set, the outgoing IP datagram will not be fragmented. Bit 13 is the “more fragments” bit. If this bit is set, there are more fragments. If this bit is clear, this is the last fragment of the IP packet.
13-bit fragment offset	This field contains the upper 13-bits of the fragment offset. Because of this, fragment offsets are only allowed on 8-byte boundaries. The first fragment of a fragmented IP datagram will have the “more fragments” bit set and have an offset of 0.
8-bit time to live (TTL)	This field contains the number of routers this datagram can pass, which basically limits the lifetime of the datagram.
8-bit protocol	This field specifies which protocol is using the IP datagram. The following is a list of valid protocols and their values:

Protocol	Value
ICMP	0x01
IGMP	0x02
TCP	0X06
UDP	0X11

16-bit checksum	This field contains the 16-bit checksum that covers the IP header only. There are additional checksums in the higher level protocols that cover the IP payload.
32-bit source IP address	This field contains the IP address of the sender and is always a host address.
32-bit destination IP address	This field contains the IP address of the receiver or receivers if the address is a broadcast or multicast address.

Creating IP Instances

IP instances are created either during initialization or during runtime by application threads. The initial IPv4 address, network mask, default packet pool, media driver, and memory and priority of the internal IP thread are defined by the ***nx_ip_create*** service even if the application intends to use IPv6 networks only. If the application initializes the IP instance with its IPv4 address set to an invalid address(0.0.0.0), it is assumed that the interface address is going to resolved by manual configuration later, via RARP, or through DHCP or similar protocols.

For systems with multiple network interfaces, the primary interface is designated when calling ***nx_ip_create***. Each additional interface can be attached to the same IP instance by calling ***nx_ip_interface_attach***. This service stores information about the network interface (such as IP address, network mask) in the interface control block, and associates the driver instance with the interface control block in the IP instance. As the driver receives a data packet, it needs to store the interface information in the NX_PACKET structure before forwarding it to the IP receive logic. Note an IP instance must already be created before attaching any interfaces.

IPv6 services are not started after calling ***nx_ip_create***. Applications wishing to use IPv6 services must call the service ***nx_ipv6_enable*** to start IPv6.

On the IPv6 network, each interface in an IP instance may have multiple IPv6 global addresses. In addition to using DHCPv6 for IPv6 address assignment, a device may also use Stateless Address Auto-configuration. More information is available in the “IP Control Block” and “IPv6 Address Resolution” sections later in this chapter.

IP Send

The IP send processing in NetX Duo is very streamlined. The prepend pointer in the packet is moved backwards to accommodate the IP header. The IP header is completed (with all the options specified by the calling protocol layer), the IP checksum is computed in-line (for IPv4 packets only), and the packet is dispatched to the associated network driver. In addition, outgoing fragmentation is also coordinated from within the IP send processing.

For IPv4, NetX Duo initiates ARP requests if physical mapping is needed for the destination IP address. IPv6 uses Neighbor Discovery for IPv6-address-to-physical-address mapping.

For IPv4 connectivity, packets that require IP address resolution (i.e., physical mapping) are enqueued on the ARP queue until the number of packets queued exceeds the ARP queue depth (defined by the symbol ***NX_ARP_MAX_QUEUE_DEPTH****). If the queue depth is reached, NetX Duo will remove the oldest packet on the queue and continue waiting for address resolution for the remaining packets enqueued. On the other hand, if an ARP entry is not resolved, the pending packets on the ARP entry are released upon ARP entry timeout.*

For systems with multiple network interfaces, NetX Duo chooses an interface based on the destination IP address. The following procedure applies to the selection process:

1. If the sender specifies an outgoing interface and the interface is valid, use that interface.
2. If a destination address is IPv4 broadcast or multi-cast, the first enabled physical interface is used.
3. If the destination address is found in the static routing table, the interface associated with the gateway is used.
4. If the destination is on-link, the on-link interface is used.

5. If the destination address is a link-local address (169.254.0.0/16), the first valid interface is used.
6. If the default gateway is configured, use the interface associated with the default gateway to transmit the packet.
7. Finally, if one of the valid interface IP address is link-local address (169.254.0.0/16), this interface is used as source address for the transmission.
8. The output packet is dropped if all above fails.

IP Receive

The IP receive processing is either called from the network driver or the internal IP thread (for processing packets on the deferred received packet queue). The IP receive processing examines the protocol field and attempts to dispatch the packet to the proper protocol component. Before the packet is actually dispatched, the IP header is removed by advancing the prepend pointer past the IP header.

IP receive processing also detects fragmented IP packets and performs the necessary steps to reassemble them if fragmentation is enabled. If fragmentation is needed but not enabled, the packet is dropped.

NetX Duo determines the appropriate network interface based on the interface specified in the packet. If the packet interface is NULL, NetX Duo defaults to the primary interface. This is done to guarantee compatibility with legacy NetX Duo Ethernet drivers.

Raw IP Send

A raw IP packet is an IP frame that contains upper layer protocol payload not directly supported (and processed) by NetX Duo. A raw packet allows developers to define their own IP-based applications. An application may send raw IP packets directly using the ***nxd_ip_raw_packet_send*** service if raw IP packet processing has been enabled with the ***nx_ip_raw_packet_enabled*** service. When transmitting a unicast packet on an IPv6 network, NetX Duo automatically determines the best source IPv6 address to use to send the packets out on, based on the destination address. If the destination address is a multicast (or broadcast for IPv4) address, however, NetX Duo will default to the first (primary) interface. Therefore, to send such packets out on secondary interfaces, the application must use the ***nx_ip_raw_packet_source_send*** service to specify the source address to use for the outgoing packet.

Raw IP Receive

If raw IP packet processing is enabled, the application may receive raw IP packets through the ***nx_ip_raw_packet_receive*** service. All incoming packets are processed according to the protocol specified in the IP header. If the protocol specifies UDP, TCP, IGMP or ICMP, NetX Duo will process the packet using the appropriate handler for the packet protocol type. If the protocol is not one of these protocols, and raw IP receive is enabled, the incoming packet will be put into the raw packet queue waiting for the application to receive it via the ***nx_ip_raw_packet_receive*** service. In addition, application threads may suspend with an optional timeout while waiting for a raw IP packet. The number of packets that can be queued on the raw packet queue is limited. The maximum value is defined in ***NX_IP_RAW_MAX_QUEUE_DEPTH***, whose default value is 20. An application may change the maximum value by calling the ***nx_ip_raw_receive_queue_max_set*** service.

Alternatively, the NetX Duo library may be built with ***NX_ENABLE_IP_RAW_PACKET_FILTER*****.** In this mode of operation, the application provides a callback function that is invoked every time a packet with an unhandled protocol type is received. The IP receive logic forwards the packet to the user-defined raw packet receive filter routine. The filter routine decides whether or not to keep the raw packet for future process. The return value from the callback routine indicates whether the packet has been processed by the raw packet receive filter. If the packet is processed by the callback function, the packet should be released after the application is done with the packet. Otherwise, NetX Duo is responsible for releasing the packet. Refer to the ***nx_ip_raw_packet_filter_set*** for more information on how to use the raw packet filter function.

The BSD wrapper function for NetX Duo relies on the raw packet filter function to handle BSD raw sockets. Therefore, to support raw socket in the BSD wrapper, the NetX Duo library must be built with ***NX_ENABLE_IP_RAW_PACKET_FILTER*** *defined, and the application should not use the* ***nx_ip_raw_packet_filter_set*** *to install its own raw packet filter functions.*

Default Packet Pool

Each IP instance is given a default packet pool during creation. This packet pool is used to allocate packets for ARP, RARP, ICMP, IGMP, various TCP control packets (SYN, ACK, and so on), Neighbor Discovery, Router Discovery, and Duplicate Address Detection. If the default packet pool is empty when NetX Duo needs to allocate a packet, NetX Duo may have to abort the particular operation, and will return an error message if possible.

IP Helper Thread

Each IP instance has a helper thread. This thread is responsible for handling all deferred packet processing and all periodic processing. The IP helper thread is created in ***nx_ip_create.*** This is where the thread is given its stack and priority. Note that the first processing in the IP helper thread is to finish the network driver initialization associated with the IP create service. After the network driver initialization is complete, the helper thread starts an endless loop to process packet and periodic requests.

If unexplained behavior is seen within the IP helper thread, increasing its stack size during the IP create service is the first debugging step. If the stack is too small, the IP helper thread could possibly be overwriting memory, which may cause unusual problems.

Thread Suspension

Application threads can suspend while attempting to receive raw IP packets. After a raw packet is received, the new packet is given to the first thread suspended and that thread is resumed. NetX Duo services for receiving packets all have an optional suspension timeout. When a packet is received or the timeout expires, the application thread is resumed with the appropriate completion status.

IP Statistics and Errors

If enabled, the NetX Duo keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP instance:

Total IP Packets Sent
Total IP Bytes Sent
Total IP Packets Received
Total IP Bytes Received
Total IP Invalid Packets
Total IP Receive Packets Dropped
Total IP Receive Checksum Errors
Total IP Send Packets Dropped
Total IP Fragments Sent
Total IP Fragments Received

All of these statistics and error reports are available to the application with the ***nx_ip_info_get*** service.

IP Control Block NX_IP

The characteristics of each IP instance are found in its control block. It contains useful information such as the IP addresses and network masks of each network device, and a table of neighbor IP and physical hardware address mapping. This structure is defined in the ***nx_api.h*** file. If IPv6 is enabled, it also contains an array of IPv6 address, the number of which is specified by the user configurable option ***NX_MAX_IPV6_ADDRESSES***. The default value allows each physical network interface to have three IPv6 addresses.

IP instance control blocks can be located anywhere in memory, but it is most common to make the control block a global structure by defining it outside the scope of any function.

Static IPv4 Routing

The static routing feature allows an application to specify an IPv4 network and next hop address for specific out of network destination IP addresses. If static routing is enabled, NetX Duo searches through the static routing table for an entry matching the destination address of the packet to send. If no match is found, NetX Duo searches through the list of physical interfaces and chooses a source IP address and next hop address based on the destination IP address and the network mask. If the destination does not match any of the IP addresses of the network drivers attached to the IP instance, NetX Duo chooses an interface that is directly connected to the default gateway, and uses the IP address of the interface as source address, and the default gateway as the next hop.

Entries can be added and removed from the static routing table using the ***nx_ip_static_route_add*** and ***nx_ip_static_route_delete*** services, respectively. To use static routing, the host application must enable this feature by defining ***NX_ENABLE_IP_STATIC_ROUTING.***

When adding an entry to the static routing table, NetX Duo checks for a matching entry for the specified destination address already in the table. If one exists, it gives preference to the entry with the smaller network (longer prefix) in the network mask.

IPv4 Forwarding

If the incoming IPv4 packet is not destined for this node and IPv4 forwarding feature is enabled, NetX Duo attempts to forward the packet out via the other interfaces.

IP Fragmentation

The network device may have limits on the size of outgoing packets. This limit is called the maximum transmission unit (MTU). IP MTU is the largest IP frame size a link layer driver is able to transmit without fragmenting the IP packet. During a device driver initialization phase, the driver module must configure its IP MTU size via the service ***nx_ip_interface_mtu_set.***

Although not recommended, the application may generate datagrams larger than the underlying IP MTU supported by the device. Before transmitting such IP datagram, the IP layer must fragment these packets. On receiving fragmented IP frames, the receiving end must store all fragmented IP frames with the same fragmentation ID, and reassemble them in order. If the IP receive logic is unable to collect all the fragments to restore the original IP frame in time, all the fragments are released. It is up to the upper layer protocol to detect such packet loss and recover from it.

The IP fragmentation applies to both IPv4 and IPv6 packets.

In order to support IP fragmentation and reassembly operation, the system designer must enable the IP fragmentation feature in NetX Duo using the ***nx_ip_fragment_enable*** service. If this feature is not enabled, incoming fragmented IP packets are discarded, as well as packets that exceed the network driver's MTU.

i *The IP Fragmentation logic can be removed completely by defining* ***NX_DISABLE_FRAGMENTATION*** *when building the NetX Duo library. Doing so helps reduce the code size of NetX Duo. Note that in this situation, both the IPv4 and IPv6 fragmentation/reassembly functions are disabled.*

i *If* ***NX_DISABLE_CHAINED_PACKET*** *is defined, IP fragmentation must be disabled.*

i *In an IPv6 network, routers do not fragment a datagram if the size of the datagram exceeds its minimum MTU size. Therefore, it is up to the sending device to determine the minimum MTU between the source and the destination, and to ensure the IP datagram size does not exceed the path MTU. In NetX Duo, IPv6 PATH MTU discovery can be enabled by building NetX Duo library with the symbol* ***NX_ENABLE_IPV6_PATH_MTU_DISCOVERY*** *defined.*

Address Resolution Protocol (ARP) in IPv4

The Address Resolution Protocol (ARP) is responsible for dynamically mapping 32-bit IPv4 addresses to those of the underlying physical media (RFC 826). Ethernet is the most typical physical media, and it supports 48-bit addresses. The need for ARP is determined by the network driver supplied to the ***nx_ip_create*** service. If physical mapping is required, the network driver must use the ***nx_interface_address_mapping_needed*** service to configure the driver interface properly.

ARP Enable

For ARP to function properly, it must first be enabled by the application with the ***nx_arp_enable*** service. This service sets up various data structures for ARP processing, including the creation of an ARP cache area from the memory supplied to the ARP enable service.

ARP Cache

The ARP cache can be viewed as an array of internal ARP mapping data structures. Each internal structure is capable of maintaining the relationship between an IP address and a physical hardware address. In addition, each data structure has link pointers so it can be part of multiple linked lists.

Application can look up an IP address from the ARP cache by supplying hardware MAC address using the service ***nx_arp_ip_address_find*** if the mapping exists in the ARP table. Similarly, the service ***nx_arp_hardware_address_find*** returns the MAC address for a given IP address.

ARP Dynamic Entries

By default, the ARP enable service places all entries in the ARP cache on the list of available dynamic ARP entries. A dynamic ARP entry is allocated from this list by NetX Duo when a send request to an unmapped IP address is detected. After allocation, the ARP entry is set up and an ARP request is sent to the physical media.

A dynamic entry can also be created by the service ***nx_arp_dynamic_entry_set***.

If all dynamic ARP entries are in use, the least recently used ARP entry is replaced with a new mapping.

ARP Static Entries

The application can also set up static ARP mapping by using the ***nx_arp_static_entry_create*** service. This service allocates an ARP entry from the dynamic ARP entry list and places it on the static list with the mapping information supplied by the application. Static ARP entries are not subject to reuse or aging. The application can delete a static entry by using the service ***nx_arp_static_entry_delete***. To remove all static entries in the ARP table, the application may use the service ***nx_arp_static_entries_delete***.

Automatic ARP Entry

NetX Duo records the peer's IP/MAC mapping after the peer responses to the ARP request. NetX Duo also implements the automatic ARP entry feature where it records peer IP/MAC address mapping based on unsolicited ARP requests from the network. This feature allows the ARP table to be populated with peer information, reducing the delay needed to go through the ARP request/response cycle. However the downside with enabling automatic ARP is that the ARP table tend to fill up quickly on a busy network with many nodes on the local link, which would eventually lead to ARP entry replacement.

This feature is enabled by default. To disable it, the NetX Duo library must be compiled with the symbol ***NX_DISABLE_ARP_AUTO_ENTRY*** defined.

ARP Messages

As mentioned previously, an ARP request message is sent when the IP task detects that mapping is needed for an IP address. ARP requests are sent periodically (every ***NX_ARP_UPDATE_RATE*** seconds) until a corresponding ARP response is received. A total of ***NX_ARP_MAXIMUM_RETRIES*** ARP requests are made before the ARP attempt is abandoned. When an ARP response is received, the associated physical address information is stored in the ARP entry that is in the cache.

For multihome systems, NetX Duo determines which interface to send the ARP requests and responses based on destination address specified.

Outgoing IP packets are queued while NetX Duo waits for the ARP response. The number of outgoing IP packets queued is defined by the constant ***NX_ARP_MAX_QUEUE_DEPTH****.*

NetX Duo also responds to ARP requests from other nodes on the local IPv4 network. When an external ARP request is made that matches the current IP address of the interface that receives the ARP request, NetX Duo builds an ARP response message that contains the current physical address.

The formats of Ethernet ARP requests and responses are shown in Figure 6 and are described below .

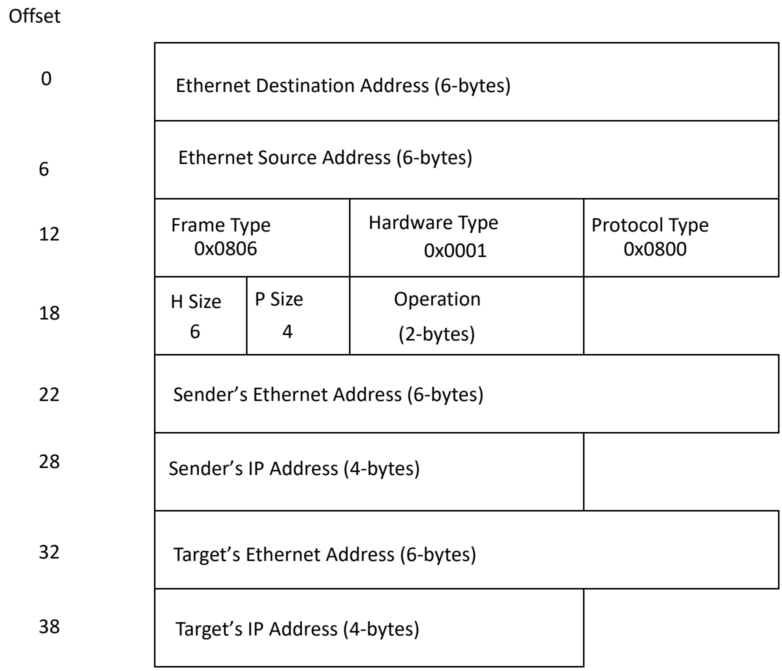


FIGURE 6. ARP Packet Format

Request/Response Field	**Purpose**
Ethernet Destination Address	This 6-byte field contains the destination address for the ARP response and is a broadcast (all ones) for ARP requests. This field is setup by the network driver.
Ethernet Source Address	This 6-byte field contains the address of the sender of the ARP request or response and is set up by the network driver.

Request/Response Field	Purpose
Frame Type	This 2-byte field contains the type of Ethernet frame present and, for ARP requests and responses, this is equal to 0x0806. This is the last field the network driver is responsible for setting up.
Hardware Type	This 2-byte field contains the hardware type, which is 0x0001 for Ethernet.
Protocol Type	This 2-byte field contains the protocol type, which is 0x0800 for IP addresses.
Hardware Size	This 1-byte field contains the hardware address size, which is 6 for Ethernet addresses.
Protocol Size	This 1-byte field contains the IP address size, which is 4 for IP addresses.
Operation Code	This 2-byte field contains the operation for this ARP packet. An ARP request is specified with the value of 0x0001, while an ARP response is represented by a value of 0x0002.
Sender Ethernet Address	This 6-byte field contains the sender's Ethernet address.
Sender IP Address	This 4-byte field contains the sender's IP address.
Target Ethernet Address	This 6-byte field contains the target's Ethernet address.
Target IP Address	This 4-byte field contains the target's IP address.

i

ARP requests and responses are Ethernet-level packets. All other TCP/IP packets are encapsulated by an IP packet header.

i

*All ARP messages in the TCP/IP implementation are expected to be in **big endian** format. In this format, the most significant byte of the word resides at the lowest byte address.*

ARP Aging

NetX supports automatic dynamic ARP entry invalidation. ***NX_ARP_EXPIRATION_RATE*** specifies the number of seconds an established IP address to physical mapping stays valid. After expiration, the ARP entry is removed from the ARP cache. The next attempt to send to the corresponding IP address will result in a new ARP request. Setting ***NX_ARP_EXPIRATION_RATE*** to zero disables ARP aging, which is the default configuration.

ARP Defend

When an ARP request or ARP response packet is received and the sender has the same IP address, which conflicts with the IP address of this node, NetX Duo sends an ARP request for that address as a defense. If the conflict ARP packet is received more than once in 10 seconds, NetX Duo does not send more defend packets. The default interval 10 seconds can be redefined by ***NX_ARP_DEFEND_INTERVAL***. This behavior follows the policy specified in 2.4(c) of RFC5227. Since Windows XP ignores ARP announcement as a response for its ARP probe, user can define ***NX_ARP_DEFEND_BY_REPLY*** to send ARP response as additional defence.

ARP Statistics and Errors

If enabled, the NetX Duo ARP software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP's ARP processing:

Total ARP Requests Sent
Total ARP Requests Received
Total ARP Responses Sent
Total ARP Responses Received
Total ARP Dynamic Entries
Total ARP Static Entries

Total ARP Aged Entries
Total ARP Invalid Messages

All these statistics and error reports are available to the application with the ***nx_arp_info_get*** service.

Reverse Address Resolution Protocol (RARP) in IPv4

The Reverse Address Resolution Protocol (RARP) is the protocol for requesting network assignment of the host's 32-bit IP addresses (RFC 903). This is done through an RARP request and continues periodically until a network member assigns an IP address to the host network interface in an RARP response. The application creates an IP instance by the service ***nx_ip_create*** with a zero IP address. If RARP is enabled by the application, it can use the RARP protocol to request an IP address from the network server accessible through the interface that has a zero IP address.

RARP Enable

To use RARP, the application must create the IP instance with an IP address of zero, then enable RARP using the service ***nx_rarp_enable***. For multihome systems, at least one network device associated with the IP instance must have an IP address of zero. The RARP processing periodically sends RARP request messages for the NetX Duo system requiring an IP address until a valid RARP reply with the network designated IP address is received. At this point, RARP processing is complete.

After RARP has been enabled, it is disabled automatically after all interface addresses are resolved. The application may force RARP to terminate by using the service ***nx_rarp_disable***.

RARP Request

The format of an RARP request packet is almost identical to the ARP packet shown in Figure 6 on page 90.The only difference is the frame type field is 0x8035 and the *Operation Code* field is 3, designating an RARP request. As mentioned previously, RARP requests will be sent periodically (every ***NX_RARP_UPDATE_RATE*** seconds) until a RARP reply with the network assigned IP address is received.

*All RARP messages in the TCP/IP implementation are expected to be in **big endian** format. In this format, the most significant byte of the word resides at the lowest byte address.*

RARP Reply

RARP reply messages are received from the network and contain the network assigned IP address for this host. The format of an RARP reply packet is almost identical to the ARP packet shown in Figure 6. The only difference is the frame type field is 0x8035 and the *Operation Code* field is 4, which designates an RARP reply. After received, the IP address is setup in the IP instance, the periodic RARP request is disabled, and the IP instance is now ready for normal network operation.

For multihome hosts, the IP address is applied to the requesting network interface. If there are other network interfaces still requesting an IP address assignment, the periodic RARP service continues until all interface IP address requests are resolved.

*The application should not use the IP instance until the RARP processing is complete. The **nx_ip_status_check** may be used by applications to wait for the RARP completion. For multihome systems, the application should not use the requesting interface until the RARP processing is complete on that interface. Status of the IP address* *on the secondary device can be checked with the **nx_ip_interface_status_check** service.*

RARP Statistics and Errors

If enabled, the NetX Duo RARP software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP's RARP processing:

Total RARP Requests Sent
Total RARP Responses Received
Total RARP Invalid Messages

All these statistics and error reports are available to the application with the ***nx_rarp_info_get*** service.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol for IPv4 (ICMP) is limited to passing error and control information between IP network members. Internet Control Message Protocol for IPv6 (ICMPv6) also handles error and control information and is required for address resolution protocols such as Duplicate Address Detection (DAD) and stateless address autoconfiguration.

Like most other application layer (e.g., TCP/IP) messages, ICMP and ICMPv6 messages are encapsulated by an IP header with the ICMP (or ICMPv6) protocol designation.

ICMP Statistics and Errors

If enabled, NetX Duo keeps track of several ICMP statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP's ICMP processing:

Total ICMP Pings Sent
Total ICMP Ping Timeouts
Total ICMP Ping Threads Suspended
Total ICMP Ping Responses Received
Total ICMP Checksum Errors
Total ICMP Unhandled Messages

All these statistics and error reports are available to the application with the ***nx_icmp_info_get*** service.

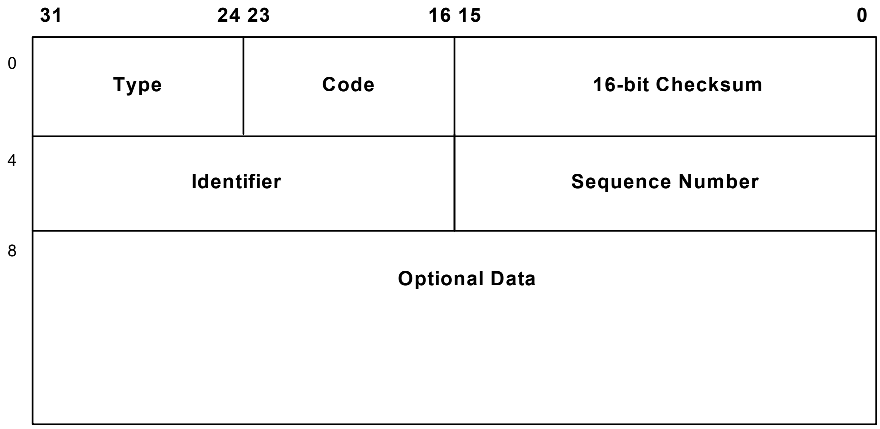
ICMPv4 Services in NetX Duo

ICMPv4 Enable

Before ICMPv4 messages can be processed by NetX Duo, the application must call the ***nx_icmp_enable*** service to enable ICMPv4 processing. After this is done, the application can issue ping requests and field incoming ping packets.

ICMPv4 Echo Request

An echo request is one type of ICMPv4 message that is typically used to check for the existence of a specific node on the network, as identified by its host IP address. The popular ping command is implemented using ICMP echo request/echo reply messages. If the specific host is present, its network stack processes the ping request and responses with a ping response. Figure 7 details the ICMPv4 ping message format.



(Note: IP header is prepended)

FIGURE 7. ICMPv4 Ping Message

*All ICMPv4 messages in the TCP/IP implementation are expected to be in **big endian** format. In this format, the most significant byte of the word resides at the lowest byte address.*

The following describes the ICMPv4 header format:

Header Field	***Purpose***
Type	This field specifies the ICMPv4 message (bits 31-24). The most common are: 0 Echo Reply 3 Destination Unreachable 8 Echo Request 11 Time Exceeded 12 Parameter Problem
Code	This field is context specific on the type field (bits 23-16). For an echo request or reply the code is set to zero.

Checksum	This field contains the 16-bit checksum of the one's complement sum of the ICMPv4 message including the entire the ICMPv4 header starting with the Type field. Before generating the checksum, the checksum field is cleared.
Identification	This field contains an ID value identifying the host; a host should use the ID extracted from an ECHO request in the ECHO REPLY (bits 31-16).
Sequence number	This field contains an ID value; a host should use the ID extracted from an ECHO request in the ECHO REPLY (bits 31-16). Unlike the identifier field, this value will change in a subsequent Echo request from the same host (bits 15-0).

ICMPv4 Echo Response

A ping response is another type of ICMP message that is generated internally by the ICMP component in response to an external ping request. In addition to acknowledgement, the ping response also contains a copy of the user data supplied in the ping request.

ICMPv4 Error Messages

The following ICMPv4 error messages are supported in NetX Duo:

Destination Unreachable
Time Exceed
Parameter Problem

Internet Group Management Protocol (IGMP)

The Internet Group Management Protocol (IGMP) provides a device to communicate with its neighbors and its routers that it intends to receive, or join, an IPv4 multicast group (RFC 1112 and RFC 2236). A multicast group is basically a dynamic collection of network members and is represented by a Class D IP address. Members of the multicast group may leave at any time, and new members may join at any time. The coordination involved in joining and leaving the group is the responsibility of IGMP.

IGMP is designed only for IPv4 multicast groups. It cannot be used on the IPv6 network.

IGMP Enable

Before any multicasting activity can take place in NetX Duo, the application must call the ***nx_igmp_enable*** service. This service performs basic IGMP initialization in preparation for multicast requests.

Multicast IPv4 Addressing

As mentioned previously, multicast addresses are actually Class D IP addresses as shown in Figure 4 on page 73. The lower 28-bits of the Class D address correspond to the multicast group ID. There are a series of pre-defined multicast addresses; however, the *all hosts address* (244.0.0.1) is particularly important to IGMP processing. The *all hosts address* is used by routers to query all multicast members to report on which multicast groups they belong to.

Physical Address Mapping in IPv4

Class D multicast addresses map directly to physical Ethernet addresses ranging from 01.00.5e.00.00.00 through 01.00.5e.7f.ff.ff. The lower 23 bits of the IP multicast address map directly to the lower 23 bits of the Ethernet address.

Multicast Group Join

Applications that need to join a particular multicast group may do so by calling the ***nx_igmp_multicast_join*** service. This service keeps track of the number of requests to join this multicast group. If this is the first application request to join the multicast group, an IGMP report is sent out on the primary network indicating this host's intention to join the group. Next, the network driver is called to set up for listening for packets with the Ethernet address for this multicast group.

In a multihome system, if the multicast group is accessible via a specific interface, application shall use the service ***nx_igmp_multicast_interface_join*** instead of ***nx_igmp_multicast_join**,* which is limited to multicast groups on the primary network.

Multicast Group Leave

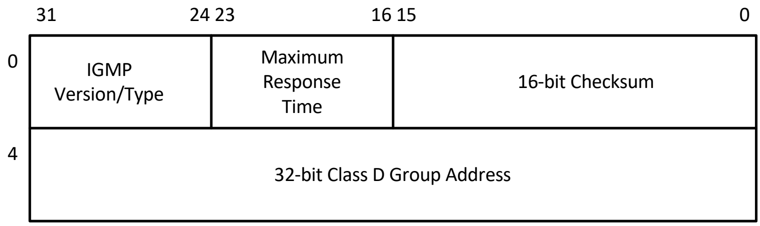
Applications that need to leave a previously joined multicast group may do so by calling the ***nx_igmp_multicast_leave*** service. This service reduces the internal count associated with how many times the group was joined. If there are no outstanding join requests for a group, the network driver is called to disable listening for packets with this multicast group's Ethernet address.

Multicast Loopback

An application may wish to receive multicast traffic originated from one of the sources on the same node. This requires the IP multicast component to have loopback enabled by using the service ***nx_igmp_loopback_enable***.

IGMP Report Message

When the application joins a multicast group, an IGMP report message is sent via the network to indicate the host's intention to join a particular multicast group. The format of the IGMP report message is shown in Figure 8. The multicast group address is used for both the group message in the IGMP report message and the destination IP address.



(Note: IP header is prepended)

FIGURE 8. IGMP Report Message

In the figure above (Figure 8), the IGMP header contains a version/type field, maximum response time, a checksum field, and a multicast group address field. For IGMPv1 messages, the Maximum Response Time field is always set to zero, as this is not part of the IGMPv1 protocol. The Maximum Response Time field is set when the host receives a Query type IGMP message and cleared when a host receives another host's Report type message as defined by the IGMPv2 protocol.

The following describes the IGMP header format:

Header Field	***Purpose***
Version	This field specifies the IGMP version (bits 31- 28).
Type	This field specifies the type of IGMP message (bits 27 -24).

Maximum Response Time	Not used in IGMP v1. In IGMP v2 this field serves as the maximum response time.
Checksum	This field contains the 16-bit checksum of the one's complement sum of the IGMP message starting with the IGMP version (bits 0-15)
Group Address	32-bit class D group IP address

IGMP report messages are also sent in response to IGMP query messages sent by a multicast router. Multicast routers periodically send query messages out to see which hosts still require group membership. Query messages have the same format as the IGMP Report message shown in Figure 8. The only differences are the IGMP type is equal to 1 and the group address field is set to 0. IGMP Query messages are sent to the *all hosts* IP address by the multicast router. A host that still wishes to maintain group membership responds by sending another IGMP Report message.

i

All messages in the TCP/IP implementation are expected to be in ***big endian*** *format. In this format, the most significant byte of the word resides at the lowest byte address.*

IGMP Statistics and Errors

If enabled, the NetX Duo IGMP software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP’s IGMP processing:

Total IGMP Reports Sent
Total IGMP Queries Received
Total IGMP Checksum Errors
Total IGMP Current Groups Joined

All these statistics and error reports are available to the application with the ***nx_igmp_info_get*** service.

Multicast without IGMP

Application expecting IPv4 multicast traffic can join a multicast group address without invoking IGMP messages by using the service ***nx_ipv4_multicast_interface_join***. This service instructs the IPv4 layer and the underlying interface driver to accept packets from the designated IPv4 multicast address. However there is no IGMP group management messages being sent or processed for this group.

Application no longer wish to receive traffic from the group can use the service ***nx_ipv4_multicast_interface_leave.***

IPv6 in NetX Duo

IPv6 Addresses

IPv6 addresses are 128 bits. The architecture of IPv6 address is described in RFC 4291. The address is divided into a prefix containing the most significant bits and a host address containing the lower bits. The prefix indicates the type of address and is roughly the equivalent of the network address in IPv4 network.

IPv6 has three types of address specifications: unicast, anycast (not supported in NetX Duo), and multicast. Unicast addresses are those IP addresses that identify a specific host on the Internet. Unicast addresses can be either a source or a destination IP address. Multicast addresses specify a dynamic group of hosts on the Internet. Members of the multicast group may join and leave whenever they wish.

IPv6 does not have the equivalent of the IPv4 broadcast mechanism. The ability to send a packet to all hosts can be achieved by sending a packet to the link-local all hosts multicast group, which is described on page102.

IPv6 utilizes multicast addresses to perform Neighbor Discovery, Router Discovery, and Stateless Address Auto Configuration procedures.

There are two types of IPv6 unicast addresses: link local addresses, typically constructed by combining the well-known link local prefix with the interface MAC address, and global IP addresses, which also has the prefix portion and the host ID portion. A global address may be configured manually, or through the Stateless Address Autoconfiguration or DHCPv6. NetX Duo supports both link local address and global address.

To accommodate both IPv4 and IPv6 formats, NetX Duo provides a new data type, NXD_ADDRESS, for holding IPv4 and IPv6 addresses. The definition of this structure is shown below. The address field is a union of IPv4 and IPv6 addresses.

```
typedef struct NXD_ADDRESS_STRUCT
{
    ULONG     nxd_ip_version;
    union
    {
        ULONG v4;
        ULONG v6[4];
    } nxd_ip_address;
} NXD_ADDRESS;
```

In the NXD_ADDRESS structure, the first element, *nxd_ip_version*, indicates IPv4 or IPv6 version. Supported values are either NX_IP_VERSION_V4 or NX_IP_VERSION_V6. *nxd_ip_version* indicates which field in the *nxd_ip_address* union to use as the IP address. NetX Duo API services typically take a pointer to NXD_ADDRESS structure as input argument in lieu of the ULONG (32 bit) IP address.

Link Local Addresses

A link-local address is only valid on the local network. A device can send and receive packets to another device on the same network after a valid link local address is assigned to it. An application assigns a link-local address by calling the NetX Duo service ***nxd_ipv6_address_set***, with the prefix length parameter set to 10. The application may supply a link-local address to the service, or it may simply use NX_NULL as the link-local address and allow NetX Duo to construct a link-local address based on the device's MAC address.

The following example instructs NetX Duo to configure the link-local address with a prefix length of 10 on the primary device (index 0) using its MAC address:

```
nxd_ipv6_address_set(ip_ptr, 0, NX_NULL, 10,
                     NX_NULL);
```

In the example above, if the MAC address of the interface is 54:32:10:1A:BC:67, the corresponding link-local address would be:

```
FE80::5632:10FF:FE1A:BC67
```

Note that the host ID portion of the IPv6 address (`5632:10FF:FE1A:BC67`) is made up of the 6-byte MAC address, with the following modifications:

- `0xFFFE` inserted between byte 3 and byte 4 of the MAC address
- Second lowest bit of the first byte of the MAC address (U/L bit) is set to 1

Refer to RFC 2464 (Transmission of IPv6 Packets over Ethernet Network) for more information on how to construct the host portion of an IPv6 address from its interface MAC address.

There are a few special multicast addresses for sending multicast messages to one or more hosts in IPv6:

All nodes group	`FF02::1`	All hosts on the local network
All routers group	`FF02::2`	All routers on the local network
Solicited-node	`FF02::1:FF00:0/104`	Explained below

A solicited-node multicast address targets specific hosts on the local link rather than all the IPv6 hosts. It consists of the prefix `FF02::1:FF00:0/104`, which is 104 bits and the last 24-bits of the target IPv6 address. For example, an IPv6 address `205B:209D:D028::F058:D1C8:1024` has a solicited-node multicast address of address `FF02::1:FFC8:1024`.

The double colon notation indicates the intervening bits are all zeroes. `FF02::1:FF00:0/104` *fully expanded looks like* `FF02:0000:0000:0000:0000:0001:FF00:0000`

Global Addresses

An example of an IPv6 global address is

`2001:0123:4567:89AB:CDEF::1`

NetX Duo stores IPv6 addresses in the NXD_ADDRESS structure. In the example below, the NXD_ADDRESS variable `global_ipv6_address` contains a unicast IPv6 address. The following example demonstrates a NetX Duo device creating a specific IPv6 global address for its primary device:

```
NXD_ADDRESS global_ipv6_address;
UINT        primary_interface_index = 0;

global_ipv6_address.nxd_ip_version  = NX_IP_VERSION_V6;
global_ipv6_address.nxd_ip_address.v6[0]  = 0x20010123;
global_ipv6_address.nxd_ip_address.v6[1]  = 0x456789AB;
global_ipv6_address.nxd_ip_address.v6[2]  = 0xCDEF0000;
global_ipv6_address.nxd_ip_address.v6[3]  = 0x00000001;

status = nxd_ipv6_address_set(&ip_0,
                              primary_interface_index,
                              &global_ipv6_address,
                              64, NX_NULL);
```

Note that the prefix of this IPv6 address is `2001:0123:4567:89AB`, which is 64 bits long and is a common prefix length for global unicast IPv6 addresses on Ethernet.

The NXD_ADDRESS structure also holds IPv4 addresses. An IP address of `192.1.168.10` `(0xC001A80A)` stored in `global_ipv4_address` would have the following memory layout:

Field	Value
`global_ipv4_address.nxd_ip_version`	`NX_IP_VERSION_V4`
`global_ipv4_address.nxd_ip_address.v4`	`0xC001A80A`

When an application passes an address to NetX Duo services, the *nxd_ip_version* field must specify the correct IP version for proper packet handling.

To be backward compatible with existing NetX applications, NetX Duo supports all NetX services. Internally, NetX Duo converts the IPv4 address type ULONG to an NXD_ADDRESS data type before forwarding it to the actual NetX Duo service.

The following example illustrates the similarity and the differences between services in NetX and NetX Duo.

```
NXD_ADDRESS   global_ipv4_address;
NX_TCP_SOCKET tcp_socket;
UINT          port_number = 80;

/* Make a connection to the destination IPv4
address
   192.1.168.12 through an already created TCP
socket bound
   to the well known HTTP port number 80. */

global_ipv4_address.nxd_ip_version =
NX_IP_VERSION_V4;
global_ipv4_address.nxd_ip_address.v4 =
0xC001A80C;

nxd_tcp_client_socket_connect(&tcp_socket,

&global_ipv4_address,
                              port_number,
                              NX_WAIT_FOREVER);
```

The following is the equivalent NetX API:

```
ULONG         server_ip = 0xC001A80C;
NX_TCP_SOCKET tcp_socket;
UINT          port_number = 80;

nx_tcp_client_socket_connect(&tcp_socket,
                             server_ip,
                             port_number,
                             NX_WAIT_FOREVER);
```

Application developers are encouraged to use the nxd version of these APIs.

IPv6 Default Routers

IPv6 uses a default router to forward packets to off-link destinations. The NetX Duo service ***nxd_ipv6_default_router_add*** enables an application to add an IPv6 router to the default router table. See Chapter 4 “Description of Services” for more default router services offered by NetX Duo.

When forwarding IPv6 packets, NetX Duo first checks if the packet destination is on-link. If not, NetX Duo checks the default routing table for a valid router to forward the off-link packet to.

To remove a router from the IPv6 default router table, application shall use the service ***nxd_ipv6_default_router_delete***. To obtain entries of the IPv6 default router table, use the service ***nxd_ipv6_default_router_entry_get***.

IPv6 Header

The IPv6 header has been modified from the IPv4 header. When allocating a packet, the caller specifies the application protocol (e.g., UDP, TCP), buffer size in bytes, and hop limit.

Figure 9 shows the format of the IPv6 header and the table lists the header components.

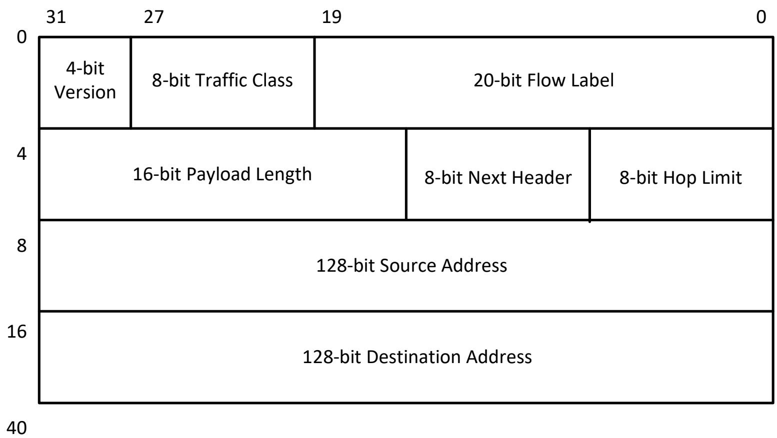


FIGURE 9. IPv6 Header Format

IP header	Purpose
Version	4-bit field for IP version. For IPv6 networks, the value in this field must be 6; For IPv4 networks it must be 4.
Traffic Class	8-bit field that stores the traffic class information. This field is not used by NetX Duo.
Flow Label	20-bit field to uniquely identify the flow, if any, that a packet is associated with. A value of zero indicates the packet does not belong to a particular flow. This field replaces the *TOS* field in IPv4.
Payload Length	16-bit field indicating the amount of data in bytes of the IPv6 packet following the IPv6 base header. This includes all encapsulated protocol header and data.
Next Header	8-bit field indicating the type of the extension header that follows the IPv6 base header. This field replaces the *Protocol* field in IPv4.
Hop Limit	8-bit field that limits the number of routers the packet is allowed to go through. This field replaces the *TTL* field in IPv4.
Source Address	128-bit field that stores the IPv6 address of the sender.
Destination Address	128-bit field that sores the IPv6 address of the destination.

Enabling IPv6 in NetX Duo

By default IPv6 is enabled in NetX Duo. IPv6 services are enabled in NetX Duo if the configurable option ***NX_DISABLE_IPV6*** in *nx_user.h* is not defined. If ***NX_DISABLE_IPV6*** is defined, NetX Duo will only offer IPv4 services, and all the IPv6-related modules and services are not built into NetX Duo library.

The following service is provided for applications to configure the device IPv6 address:

nxd_ipv6_address_set

In addition to manually setting the device's IPv6 addresses, the system may also use Stateless Address Autoconfiguration. To use this option, the application must call ***nxd_ipv6_enable*** to start IPv6 services on the device. In addition, ICMPv6 services must be started by calling ***nxd_icmp_enable***, which enables NetX Duo to perform services such as Router Solicitation, Neighbor Discovery, and Duplicate Address Detection. Note that ***nx_icmp_enable*** only starts ICMP for IPv4 services. ***nxd_icmp_enable*** starts ICMP services for both IPv4 and IPv6. If the system does not need ICMPv6 services, then ***nx_icmp_enable*** can be used so the ICMPv6 module is not linked into the system.

The following example shows a typical NetX Duo IPv6 initialization procedure.

```
/* Assume ip_0 has been created and IPv4 services (such as ARP,
   ICMP, have been enabled. */
#define SECONDARY_INTERFACE 1

/* Enable IPv6 */
status = nxd_ipv6_enable(&ip_0);

if(status != NX_SUCCESS)
{
    /* nxd_ipv6_enable failed. */
}

/* Enable ICMPv6 */
status = nxd_icmp_enable(&ip_0);
if(status != NX_SUCCESS)
{
    /* nxd_icmp_enable failed. */
}

/* Configure the link local address on the primary interface. */
status = nxd_ipv6_address_set(&ip_0, 0, NX_NULL, 10, NX_NULL);

/* Configure ip_0 primary interface global address. */
ip_address.nxd_ip_version = NX_IP_VERSION_V6
ip_address.nxd_ip_address.v6[0] = 0x20010db8;
ip_address.nxd_ip_address.v6[1] = 0x0000f101;
ip_address.nxd_ip_address.v6[2] = 0;
ip_address.nxd_ip_address.v6[3] = 0x202;

/* Configure global address of the primary interface. */
status = nxd_ipv6_address_set(&ip_0, SECONDARY_INTERFACE,
                              &ip_address, 64, NX_NULL);
```

Upper layer protocols (such as TCP and UDP) can be enabled either before or after IPv6 starts.

IPv6 services are available only after IP thread is initialized and the device is enabled.

After the interface is enabled (i.e.,the interface device driver is ready to send and receive data, and a valid link local address has been obtained), the device may obtain global IPv6 addresses by one of the these methods:

- Stateless Address Auto Configuration;
- Manual IPv6 address configuration;
- Address configuration via DHCPv6 (with optional DHCPv6 package)

The first two methods are described below. The 3rd method (DHCPv6) is described in the DHCP package.

Stateless Address Autoconfiguration Using Router Solicitation

NetX Duo devices can configure their interfaces automatically when connected to an IPv6 network with a router that supplies prefix information. Devices that require Stateless Address Autoconfiguration send out router solicitation (RS) messages. Routers on the network respond with solicited router advertisement (RA) messages. RA messages advertise prefixes that identify the network addresses associated with a link. Devices then generate a unique identifier for the network the device is attached to. The address is formed by combining the prefix and its unique identifier. In this manner on receiving the RA messages, hosts generate their IP address. Routers may also send periodic unsolicited RA messages.

NetX Duo allows an application to enable or disable Stateless Address Autoconfiguration at run time. To enable this feature, NetX Duo library must be compiled with ***NX_IPV6_STATELESS_AUTOCONFIG_CONTROL*** *defined. Once this feature is enabled, applications may use* ***nxd_ipv6_stateless_address_autoconfigure_enable*** *and* ***nxd_ipv6_stateless_address_autocofigure_disable*** *to enable or disable IPv6 stateless address autoconfiguration.*

Manual IPv6 Address Configuration

If a specific IPv6 address is needed, the application may use ***nxd_ipv6_address_set*** to manually configure an IPv6 address. A network interface may have multiple IPv6 addresses. However keep in mind that the total number of IPv6 addresses in a system, either obtained through Stateless Address Autoconfiguration, or through the Manual Configuration, cannot exceed ***NX_MAX_IPV6_ADDRESSES***.

The following example illustrates how to manually configure a global address on the primary interface (device 0) in ip_0:

```
NXD_ADDRESS global_address;
global_address.nxd_ip_version = NX_IP_VERSION_V6;
global_address.nxd_ip_address.v6[0] = 0x20010000;
global_address.nxd_ip_address.v6[1] = 0x00000000;
global_address.nxd_ip_address.v6[2] = 0x00000000;
global_address.nxd_ip_address.v6[3] = 0x0000ABCD;
```

The host then calls the following NetX Duo service to assign this address as its global IP address:

```
status = nxd_ipv6_address_set(&ip_0, 0,
                                  &global_address, 64
                                  NX_NULL);
```

Duplicate Address Detection (DAD)

After a system configures its IPv6 address, the address is marked as *TENTATIVE*. If Duplicate Address Detection (DAD), described in RFC 4862, is enabled, NetX Duo automatically sends neighbor solicitation (NS) messages with this tentative address as the destination. If no hosts on the network respond to these NS messages within a given period of time, the address is assumed to be unique on the local link, and its state transits to the

VALID state. At this point the application may start using this IP address for communication.

The DAD functionality is part of the ICMPv6 module. Therefore, the application must enable ICMPv6 services before a newly configured address can go through the DAD process. Alternatively, the DAD process may be turned off by defining ***NX_DISABLE_IPV6_DAD*** option in the NetX Duo library build environment (defined as ***nx_user.h***). During the DAD process, the ***NX_IPV6_DAD_TRANSMITS*** parameter determines the number of NS messages sent by NetX Duo without receiving a response to determine that the address is unique. By default and recommended by RFC 4862, ***NX_IPV6_DAD_TRANSMITS*** is set at 3. Setting this symbol to zero effectively disables DAD.

If ICMPv6 or DAD is not enabled at the time the application assigns an IPv6 address, DAD is not performed and NetX Duo sets the state of the IPv6 address to VALID immediately.

NetX Duo cannot communicate on the IPv6 network until its link local and/or global address is valid. After a valid address is obtained, NetX Duo attempts to match the destination address of an incoming packet against one of its configured IPv6 address or an enabled multicast address. If no matches are found, the packet is dropped.

During the DAD process, the number of DAD NS packets to be transmitted is defined by ***NX_IPV6_DAD_TRANSMITS****, which defaults to 3, and by default there is a one second delay between each DAD NS message is sent. Therefore, in a system with DAD enabled, after an IPv6 address is assigned (and assuming this is not a duplicated address), there is approximately 3 seconds delay before the IP address is in a VALID state and is ready for communication.*

Applications may want to receive notifications when IPv6 addresses in the system are changed. To enable the IPv6 address change notification feature, the NetX Duo library must be built with the symbol **NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY** defined. Once the feature is enabled, applications may install the callback function by using the ***nxd_ipv6_address_change_notify*** service.

Once an IPv6 address is changed, or becomes invalid, the user-supplied callback function is invoked with the following information:

ip_ptr	Pointer to the IP instance
interface_index	Index to the network interface that this IPv6 address is associated with
ipv6_addr_index	Index to the IPv6 address table
ipv6_address	Pointer to the IPv6 address, in the form of an array of four ULONG integers. Pv6 addresses are presented in host byte order.

IPv6 Multicast Support In NetX Duo

Multicast addresses specify a dynamic group of hosts on the Internet. Members of the multicast group may join and leave whenever they wish. NetX Duo implements several ICMPv6 protocols, including Duplicate Address Detection, Neighbor Discovery, and Router Discovery, which require IP multicast capability. Therefore, NetX Duo expects the underlying device driver to support multicast operations.

When NetX Duo needs to join or leave a multicast group (such as the all-node multicast address, and the *solicited-node* multicast address), it issues a driver command to the device driver to join or leave a multicast MAC address. The driver command for joining the multicast address is ***NX_LINK_MULTICAST_JOIN***. To leave a multicast address, NetX Duo issues the driver command ***NX_LINK_MULTICAST_LEAVE***. The device driver must implement these two commands for ICMPv6 protocols to work properly.

Applications may join an IPv6 multicast group by using the service ***nxd_ipv6_multicast_interface_join*.** This service registers the multicast address with the IP stack, and then notifies the specified device driver of the IPv6 multicast address. To leave a multicast group, applications use the service ***nxd_ipv6_multicast_interface_leave.***

Neighbor Discovery (ND)

Neighbor Discovery is a protocol in IPv6 networks for mapping physical addresses to the IPv6 addresses (global address or link-local address). This mapping is maintained in the Neighbor Discovery Cache (ND Cache). The ND process is the equivalent of the ARP process in IPv4, and the ND Cache is similar to the ARP table. An IPv6 node can obtain its neighbor's MAC address using the Neighbor Discovery (ND) protocol. It sends out a neighbor solicitation (NS) message to the all-node solicited node multicast address, and waits for a corresponding neighbor advertisement (NA) message. The MAC address obtained through this process is stored in the ND Cache.

Each IP instance has one ND cache. The ND Cache is maintained as an array of entries. The size of the array is defined at compilation time by setting the option ***NX_IPV6_NEIGHBOR_CACHE_SIZE*** which in ***nx_user.h***. Note that all interfaces attached to an IP instance share the same ND cache.

The entire ND Cache is empty when NetX Duo starts up. As the system runs, NetX Duo automatically updates the ND Cache, adding and deleting entries as per ND protocol. However, an application may also update the ND Cache by manually adding and deleting cache entries using the following NetX Duo services:

nxd_nd_cache_entry_delete
nxd_nd_cache_entry_set
nxd_nd_cache_invalidate

When sending and receiving IPv6 packets, NetX Duo automatically updates the ND Cache table.

Internet Control Message Protocol in IPv6 (ICMPv6)

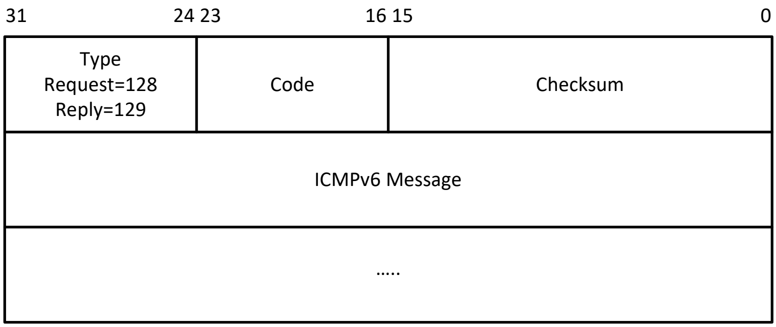
The role of ICMPv6 in IPv6 has been greatly expanded to support IPv6 address mapping and router discovery. In addition, NetX Duo ICMPv6 supports echo request and response, ICMPv6 error reports, and ICMPv6 redirect messages.

ICMPv6 Enable

Before ICMPv6 messages can be processed by NetX Duo, the application must call the ***nxd_icmp_enable*** service to enable ICMPv6 processing as explained previously.

ICMPv6 Messages

The ICMPv6 header structure is similar to the ICMPv4 header structure. As shown below, the basic ICMPv6 header contains the three fields, type, code, and checksum, plus variable length of ICMPv6 option data.



(Note: IPv6 header is prepended)

FIGURE 10. Basic ICMPv6 Header

Field	Size (bytes)	Description
Type	1	Identifies the ICMPv6 message type; 1 Destination Unreachable 2 Packet Too Big 3 Time Exceeded 4 Parameter Problem 128 Echo Request 129 Echo Reply 133 Router Solicitation 134 Router Advertisement 135 Neighbor Solicitation 136 Neighbor Advertisement 137 Redirect Message
Code	1	Further qualifies the ICMPv6 message type. Generally used with error messages. If not used, it is set to zero. Echo request/reply and NS messages do not use it.

Field	Size (bytes)	Description
Checksum	2	16-bit checksum field for the ICMP Header. This is a 16-bit complement of the entire ICMPv6 message, including the ICMPv6 header. It also includes a pseudo-header of the IPv6 source address, destination address, and packet payload length.

An example Neighbor Solicitation header is shown below.

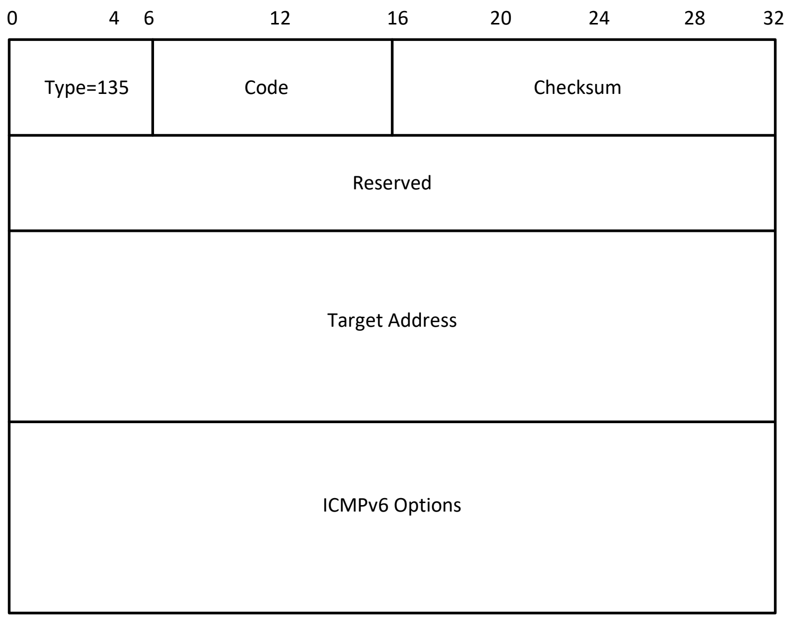


FIGURE 11. ICMPv6 Header for a Neighbor Solicitation Message

Field	Size (bytes)	Description
Type	1	Identifies the ICMPv6 message type for neighbor solicitation messages. Value is 135.
Code	1	Not used. Set to 0.

Field	Size (bytes)	Description
Checksum	2	16-bit checksum field for the ICMPv6 header.
Reserved	4	4 reserved bytes set to 0.
Target Address	16	IPv6 address of target of the solicitation. For IPv6 address resolution, this is the actual unicast IP address of the device whose link layer address needs to be resolved.
Options	Variable	Optional information specified by the Neighbor Discovery Protocol.

ICMPv6 Ping Request

In NetX Duo applications use ***nxd_icmp_ping*** to issue either IPv6 or IPv4 ping requests, based on the destination IP address specified in the parameters.

ICMPv6 Ping Response

An ICMPv6 ping response is another type of ICMPv6 message that is generated internally by the ICMPv6 component in response to an external ICMPv6 ping request. In additional to acknowledgement, the ICMPv6 ping response also contains a copy of the user data supplied in the ICMPv6 ping request.

Thread Suspension

Application threads can suspend while attempting to ping another network member. After a ping response is received, the ping response message is given to the first thread suspended and that thread is resumed. Like all NetX Duo services, suspending on a ping request has an optional timeout.

Other ICMPv6 Messages

ICMPv6 messages are required for the following features:

Neighbor Discovery
Stateless Address Autoconfiguration

Router Discovery
Neighbor Unreachability Detection

Neighbor Unreachability, Router and Prefix Discovery

Neighbor Unreachability Detection, Router Discovery, and Prefix Discovery are based on the Neighbor Discovery protocol and are described below.

Neighbor Unreachability Detection: An IPv6 device searches its Neighbor Discovery (ND) Cache for the destination link layer address when it wishes to send a packet. The immediate destination, sometimes referred to as the ‘next hop,’ may be the actual destination on the same link or it may be a router if the destination is off link. An ND cache entry contains the status on a neighbor’s reachability.

A REACHABLE status indicates the neighbor is considered reachable. A neighbor is reachable if it has recently received confirmation that packets sent to the neighbor have been received. Confirmation in NetX Duo take the form of receiving an NA message from the neighbor in response to an NS message sent by the NetX Duo device. NetX Duo will also change the state of the neighbor status to REACHABLE if the application calls the NetX Duo service ***nxd_nd_cache_entry_set*** to manually enter a cache record.

Router Discovery: An IPv6 device uses a router to forward all packets intended for off link destinations. It may also use information sent by the router, such as router advertisement (RA) messages, to configure its global IPv6 addresses.

A device on the network may initiate the Router Discovery process by sending a router solicitation (RS) message to the all-router multicast address

(FF01::2). Or it can wait on the all-node multicast address (FF::1) for a periodic RA from the routers.

An RA message contains the prefix information for configuring an IPv6 address for that network. In NetX Duo, router solicitation is by default enabled and can be disabled by setting the configuration option ***NX_DISABLE_ICMPV6_ROUTER_SOLICITATION*** in ***nx_user.h***. See Configuration Options in the "Installation and Use of NetX Duo" chapter for more details on setting Router Solicitation parameters.

Prefix Discovery: An IPv6 device uses prefix discovery to learn which target hosts are accessible directly without going through a router. This information is made available to the IPv6 device from RA messages from the router. The IPv6 device stores the prefix information in a prefix table. Prefix discovery is matching a prefix from the IPv6 device prefix table to a target address. A prefix matches a target address if all the bits in the prefix match the most significant bits of the target address. If more than one prefix covers an address, the longest prefix is selected.

ICMPv6 Error Messages

The following ICMPv6 error messages are supported in NetX Duo:

Destination Unreachable
Packet Too Big
Time Exceed
Parameter Problem

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) provides the simplest form of data transfer between network members (RFC 768). UDP data packets are sent from one network member to another in a best effort fashion; i.e., there is no built-in mechanism for acknowledgement by the packet recipient. In addition, sending a UDP packet does not require any connection to be established in advance. Because of this, UDP packet transmission is very efficient.

For developers migrating their NetX applications to NetX Duo there are only a few basic changes in UDP functionality between NetX and NetX Duo. This is because IPv6 is primarily concerned with the underlying IP layer. All NetX Duo UDP services can be used for either IPv4 or IPv6 connectivity.

UDP Header

UDP places a simple packet header in front of the application's data on transmission, and removes a similar UDP header from the packet on reception before delivering a received UDP packet to the application. UDP utilizes the IP protocol for sending and receiving packets, which means there is an IP header in front of the UDP header when the packet is on the network. Figure 12 shows the format of the UDP header.

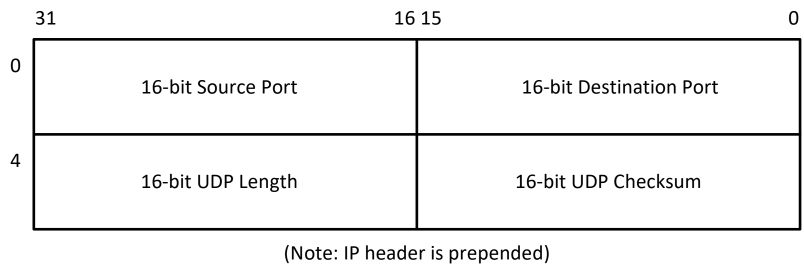


FIGURE 12. UDP Header

*All headers in the UDP/IP implementation are expected to be in **big endian** format. In this format,* *the most significant byte of the word resides at the lowest byte address.*

The following describes the UDP header format:

Header Field	Purpose
16-bit source port number	This field contains the port on which the UDP packet is being sent from. Valid UDP ports range from 1 through 0xFFFF.
16-bit destination port number	This field contains the UDP port to which the packet is being sent to. Valid UDP ports range from 1 through 0xFFFF.
16-bit UDP length	This field contains the number of bytes in the UDP packet, including the size of the UDP header.
16-bit UDP checksum	This field contains the 16-bit checksum for the packet, including the UDP header, the packet data area, and the pseudo IP header.

UDP Enable

Before UDP packet transmission is possible, the application must first enable UDP by calling the ***nx_udp_enable*** service. After enabled, the application is free to send and receive UDP packets.

UDP Socket Create

UDP sockets are created either during initialization or during runtime by application threads. The initial type of service, time to live, and receive queue depth are defined by the ***nx_udp_socket_create*** service. There are no limits on the number of UDP sockets in an application.

UDP Checksum

IPv6 protocol requires a UDP header checksum computation on packet data, whereas in the IPv4 protocol it is optional.

UDP specifies a one's complement 16-bit checksum that covers the IP pseudo header (consisting of the source IP address, destination IP address, and the protocol/length IP word), the UDP header, and the UDP packet data. The only differences between IPv4 and IPv6 UDP packet header checksums is that the source and destination IP addresses are 32 bit in IPv4 while in IPv6 they are 128 bit. If the calculated UDP checksum is 0, it is stored as all ones (0xFFFF). If the sending socket has the UDP checksum logic disabled, a zero is placed in the UDP checksum field to indicate the checksum was not calculated.

If the UDP checksum does not match the computed checksum by the receiver, the UDP packet is simply discarded.

On the IPv4 network, UDP checksum is optional. NetX Duo allows an application to enable or disable UDP checksum calculation on a per-socket basis. By default, the UDP socket checksum logic is enabled. The application can disable checksum logic for a particular UDP socket by calling the ***nx_udp_socket_checksum_disable*** service. On the IPv6 network, however, UDP checksum is mandatory. Therefore, the service ***nx_udp_socket_checksum_disable*** would not disable UDP checksum logic when sending a packet through the IPv6 network.

Certain Ethernet controllers are able to generate the UDP checksum on the fly. If the system is able to use hardware checksum computation feature, the NetX Duo library can be built without the checksum logic. To disable UDP software checksum, the NetX Duo library must be built with the following symbols defined: ***NX_DISABLE_UDP_TX_CHECKSUM*** and ***NX_DISABLE_UDP_RX_CHECKSUM*** (described in

Chapter two). The configuration options remove UDP checksum logic from NetX Duo entirely, while calling the ***nx_udp_socket_checksum_disable*** service allows the application to disable IPv4 UDP checksum processing on a per socket basis.

UDP Ports and Binding

A UDP port is a logical end point in the UDP protocol. There are 65,535 valid ports in the UDP component of NetX Duo, ranging from 1 through 0xFFFF. To send or receive UDP data, the application must first create a UDP socket, then bind it to a desired port. After binding a UDP socket to a port, the application may send and receive data on that socket.

UDP Fast Path™

The UDP Fast Path™ is the name for a low packet overhead path through the NetX Duo UDP implementation. Sending a UDP packet requires just a few function calls: ***nx_udp_socket_send***, ***nx_ip_packet_send***, and the eventual call to the network driver. ***nx_udp_socket_send*** is available in NetX Duo for existing NetX applications and is only applicable for IPv4 packets. The preferred method, however, is to use ***nxd_udp_socket_send*** service discussed below. On UDP packet reception, the UDP packet is either placed on the appropriate UDP socket receive queue or delivered to a suspended application thread in a single function call from the network driver's receive interrupt processing. This highly optimized logic for sending and receiving UDP packets is the essence of UDP Fast Path technology.

UDP Packet Send

Sending UDP data over IPv6 or IPv4 networks is easily accomplished by calling the ***nxd_udp_socket_send*** function. The caller must set the IP version in the *nx_ip_version* field of the NXD_ADDRESS pointer parameter. NetX Duo will determine the best source address for transmitted

UDP packets based on the destination IPv4/IPv6 address. This service places a UDP header in front of the packet data and sends it out onto the network using an internal IP send routine. There is no thread suspension on sending UDP packets because all UDP packet transmissions are processed immediately.

For multicast or broadcast destinations, the application should specify the source IP address to use if the NetX Duo device has multiple IP addresses to choose from. This can be done with the services ***nxd_udp_socket_source_send.***

*If **nx_udp_socket_send** is used for transmitting multicast or broadcast packets, the IP address of the first enabled interface is used as source address.*

If UDP checksum logic is enabled for this socket, the checksum operation is performed in the context of the calling thread, without blocking access to the UDP or IP data structures.

The UDP payload data residing in the NX_PACKET structure should reside on a long-word boundary. The application needs to leave sufficient space between the prepend pointer and the data start pointer for NetX Duo to place the UDP, IP, and physical media headers.

UDP Packet Receive

Application threads may receive UDP packets from a particular socket by calling ***nx_udp_socket_receive***. The socket receive function delivers the oldest packet on the socket's receive queue. If there are no packets on the receive queue, the calling thread can suspend (with an optional timeout) until a packet arrives.

The UDP receive packet processing (usually called from the network driver's receive interrupt handler) is responsible for either placing the packet on the UDP socket's receive queue or delivering it to the first suspended thread waiting for a packet. If the packet is queued, the receive processing also checks the maximum receive queue depth associated with the socket. If this newly queued packet exceeds the queue depth, the oldest packet in the queue is discarded.

UDP Receive Notify

If the application thread needs to process received data from more than one socket, the ***nx_udp_socket_receive_notify*** function should be used. This function registers a receive packet callback function for the socket. Whenever a packet is received on the socket, the callback function is executed.

The contents of the callback function is application-specific; however, it would most likely contain logic to inform the processing thread that a packet is now available on the corresponding socket.

Peer Address and Port

On receiving a UDP packet, application may find the sender's IP address and port number by using the service ***nx_udp_packet_info_extract***. On successful return, this service provides information on the sender's IP address, sender's port number, and the local interface through which the packet was received.

Thread Suspension

As mentioned previously, application threads can suspend while attempting to receive a UDP packet on a particular UDP port. After a packet is received on that port, it is given to the first thread suspended and that thread is then resumed. An optional timeout is available when suspending on a UDP receive packet, a feature available for most NetX Duo services.

UDP Socket Statistics and Errors

If enabled, the NetX Duo UDP socket software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP/UDP instance:

Total UDP Packets Sent
Total UDP Bytes Sent
Total UDP Packets Received
Total UDP Bytes Received
Total UDP Invalid Packets
Total UDP Receive Packets Dropped
Total UDP Receive Checksum Errors
UDP Socket Packets Sent
UDP Socket Bytes Sent
UDP Socket Packets Received
UDP Socket Bytes Received
UDP Socket Packets Queued
UDP Socket Receive Packets Dropped
UDP Socket Checksum Errors

All these statistics and error reports are available to the application with the ***nx_udp_info_get*** service for UDP statistics amassed over all UDP sockets, and the ***nx_udp_socket_info_get*** service for UDP statistics on the specified UDP socket.

UDP Socket Control Block NX_UDP_SOCKET

The characteristics of each UDP socket are found in the associated NX_UDP_SOCKET control block. It contains useful information such as the link to the IP data structure, the network interface for the sending and receiving paths, the bound port, and the receive packet queue. This structure is defined in the ***nx_api.h*** file.

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) provides reliable stream data transfer between two network members (RFC 793). All data sent from one network member are verified and acknowledged by the receiving member. In addition, the two members must have established a connection prior to any data transfer. All this results in reliable data transfer; however, it does require substantially more overhead than the previously described UDP data transfer.

Except where noted, there are no changes in TCP protocol API services between NetX and NetX Duo because IPv6 is primarily concerned with the underlying IP layer. All NetX Duo TCP services can be used for either IPv4 or IPv6 connections.

TCP Header

On transmission, TCP header is placed in front of the data from the user. On reception, TCP header is removed from the incoming packet, leaving only the user data available to the application. TCP utilizes the IP protocol to send and receive packets, which means there is an IP header in front of the TCP header when the packet is on the network. Figure 13 shows the format of the TCP header.

The following describes the TCP header format:

Header Field	Purpose
16-bit source port number	This field contains the port the TCP packet is being sent out on. Valid TCP ports range from 1 through 0xFFFF.
16-bit destination port number	This field contains the TCP port the packet is being sent to. Valid TCP ports range from 1 through 0xFFFF.

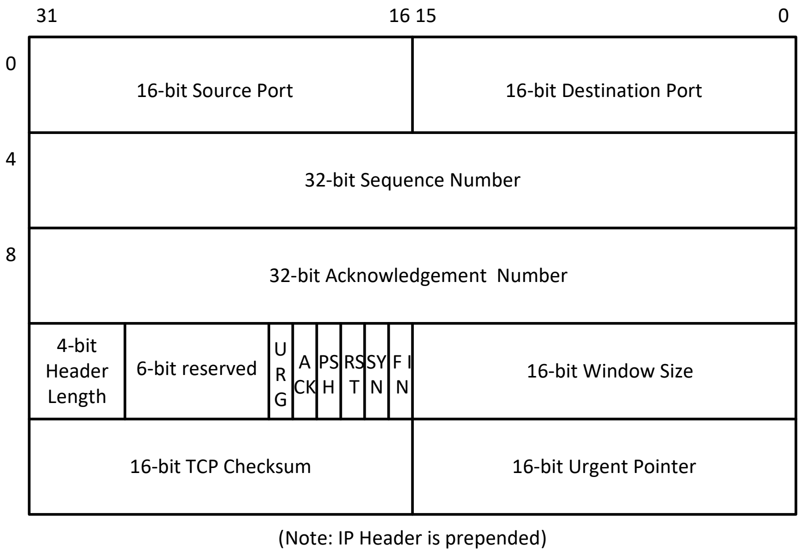


FIGURE 13. TCP Header

Header Field	Purpose
32-bit sequence number	This field contains the sequence number for data sent from this end of the connection. The original sequence is established during the initial connection sequence between two TCP nodes. Every data transfer from that point results in an increment of the sequence number by the amount bytes sent.
32-bit acknowledgment number	This field contains the sequence number corresponding to the last byte received by this side of the connection. This is used to determine whether or not data previously sent has successfully been received by the other end of the connection.

<table>
<tr><th>Header Field</th><th>Purpose</th></tr>
<tr><td>4-bit header length</td><td>This field contains the number of 32-bit words in the TCP header. If no options are present in the TCP header, this field is 5.</td></tr>
<tr><td>6-bit code bits</td><td>This field contains the six different code bits used to indicate various control information associated with the connection. The control bits are defined as follows:
<table>
<tr><th>Name</th><th>Bit</th><th>Meaning</th></tr>
<tr><td>URG</td><td>21</td><td>Urgent data present</td></tr>
<tr><td>ACK</td><td>20</td><td>Acknowledgement number is valid</td></tr>
<tr><td>PSH</td><td>19</td><td>Handle this data immediately</td></tr>
<tr><td>RST</td><td>18</td><td>Reset the connection</td></tr>
<tr><td>SYN</td><td>17</td><td>Synchronize sequence numbers (used to establish connection)</td></tr>
<tr><td>FIN</td><td>16</td><td>Sender is finished with transmit (used to close connection)</td></tr>
</table></td></tr>
<tr><td>16-bit window</td><td>This field is used for flow control. It contains the amount of bytes the socket can currently receive. This basically is used for flow control. The sender is responsible for making sure the data to send will fit into the receiver’s advertised window.</td></tr>
</table>

Header Field	Purpose
16-bit TCP checksum	This field contains the 16-bit checksum for the packet including the TCP header, the packet data area, and the pseudo IP header.
16-bit urgent pointer	This field contains the positive offset of the last byte of the urgent data. This field is only valid if the URG code bit is set in the header.

All headers in the TCP/IP implementation are expected to be in ***big endian*** *format. In this format, the most significant byte of the word resides at the lowest byte address.*

TCP Enable

Before TCP connections and packet transmissions are possible, the application must first enable TCP by calling the ***nx_tcp_enable*** service. After enabled, the application is free to access all TCP services.

TCP Socket Create

TCP sockets are created either during initialization or during runtime by application threads. The initial type of service, time to live, and window size are defined by the ***nx_tcp_socket_create*** service. There are no limits on the number of TCP sockets in an application.

TCP Checksum

TCP specifies a one's complement 16-bit checksum that covers the IP pseudo header, (consisting of the source IP address, destination IP address, and the protocol/length IP word), the TCP header, and the TCP packet data. The only difference between IPv4 and IPv6 TCP packet header checksums is that the source and destination IP addresses are 32 bit in IPv4 and 128 bit in IPv6.

Certain network controllers are able to perform TCP checksum computation and validation in hardware. For such systems, applications may want to use hardware checksum logic as much as possible to reduce runtime overhead. Applications may disable TCP checksum computation logic from the NetX Duo library altogether at build time by defining ***NX_DISABLE_TCP_TX_CHECKSUM*** and ***NX_DISABLE_TCP_RX_CHECKSUM***. This way, the TCP checksum code is not compiled in. However one should exercise caution if the optional NetX Duo IPsec package is installed, and the TCP connection may need to traverse through a secure channel. In this case, data in packets belonging to the TCP connection is already encrypted, and most hardware TCP checksum modules present in the network driver are unable to generate correct checksum value from the encrypted TCP payload.

To address this issue, application shall keep the TCP checksum logic available in the library and use the interface capability feature. With interface capability feature enabled, the TCP module knows how to properly handle the TCP checksum if the driver is also able to compute the checksum value:

(1) If the TCP packet is not subject to IPsec process, the network interface hardware is able to compute the checksum. Therefore the TCP module does not attempt to compute the checksum;

(2) If IPsec package is installed, and the TCP packet is subject to IPsec process, the TCP module computes checksum in software before sending the packet to IPsec layer.

TCP Port

A TCP port is a logical connection point in the TCP protocol. There are 65,535 valid ports in the TCP component of NetX Duo, ranging from 1 through

0xFFFF. Unlike UDP in which data from one port can be sent to any other destination port, a TCP port is connected to another specific TCP port, and only when this connection is established can any data transfer take place—and only between the two ports making up the connection.

TCP ports are completely separate from UDP ports; e.g., UDP port number 1 has no relation to TCP port number 1.

Client-Server Model

To use TCP for data transfer, a connection must first be established between the two TCP sockets. The establishment of the connection is done in a client-server fashion. The client side of the connection is the side that initiates the connection, while the server side simply waits for client connection requests before any processing is done.

For multihome devices, NetX Duo automatically determines the source address to use for the connection, and the next hop address based on the destination IP address of the connection. Because TCP is limited to sending packets to unicast (e.g.non-broadcast) destination addresses, NetX Duo does not require a "hint" for choosing the source IPv6 address.

TCP Socket State Machine

The connection between two TCP sockets (one client and one server) is complex and is managed in a state machine manner. Each TCP socket starts in a CLOSED state. Through connection events each socket’s state machine migrates into the ESTABLISHED state, which is where the bulk of the data transfer in TCP takes place. When one side of the connection no longer wishes to send data, it disconnects. After the other side disconnects, eventually the TCP socket returns to the CLOSED state. This process repeats each time a TCP client and server establish and close a connection. Figure 14 on page 138 shows the various states of the TCP state machine.

TCP Client Connection

As mentioned previously, the client side of the TCP connection initiates a connection request to a TCP server. Before a connection request can be made, TCP must be enabled on the client IP instance. In addition, the client TCP socket must next be created with the ***nx_tcp_socket_create*** service and bound to a port via the ***nx_tcp_client_socket_bind*** service.

After the client socket is bound, the ***nxd_tcp_client_socket_connect*** service is used to establish a connection with a TCP server. Note the socket must be in a CLOSED state to initiate a connection attempt. Establishing the connection starts with NetX Duo issuing a SYN packet and then waiting for a SYN ACK packet back from the server, which signifies acceptance of the connection request. After the SYN ACK is received, NetX Duo responds with an ACK packet and promotes the client socket to the ESTABLISHED state.

Applications should use ***nxd_tcp_client_socket_connect*** *for either IPv4 and IPv6 TCP connections. Applications can still use* ***nx_tcp_client_socket_connect*** *for IPv4 TCP connections, but developers are encouraged to use* ***nxd_tcp_client_socket_connect*** *since* ***nx_tcp_client_socket_connect*** *will eventually be deprecated.*

Similarly, ***nxd_tcp_socket_peer_info_get*** *works with either IPv4 or IPv6 TCP connections. However,* ***nx_tcp_socket_peer_info_get*** *is still available for legacy applications. Developers are encouraged to use* ***nxd_tcp_socket_peer_info_get*** *going forward.*

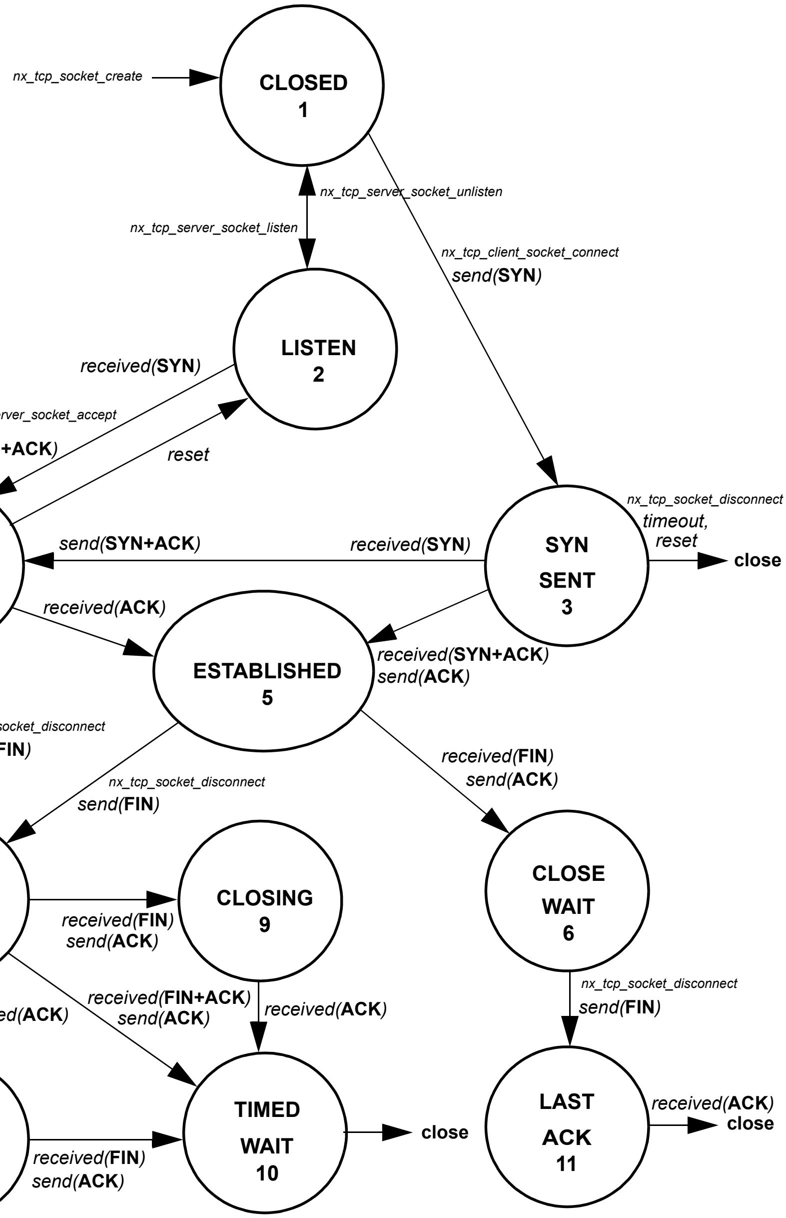


FIGURE 14. States of the TCP State Machine

TCP Client Disconnection

Closing the connection is accomplished by calling ***nx_tcp_socket_disconnect***. If no suspension is specified, the client socket sends a RST packet to the server socket and places the socket in the CLOSED state. Otherwise, if a suspension is requested, the full TCP disconnect protocol is performed, as follows:

- If the server previously initiated a disconnect request (the client socket has already received a FIN packet, responded with an ACK, and is in the CLOSE WAIT state), NetX Duo promotes the client TCP socket state to the LAST ACK state and sends a FIN packet. It then waits for an ACK from the server before completing the disconnect and entering the CLOSED state.
- If on the other hand, the client is the first to initiate a disconnect request (the server has not disconnected and the socket is still in the ESTABLISHED state), NetX Duo sends a FIN packet to initiate the disconnect and waits to receive a FIN and an ACK from the server before completing the disconnect and placing the socket in a CLOSED state.

If there are still packets on the socket transmit queue, NetX Duo suspends for the specified timeout to allow the packets to be acknowledged. If the timeout expires, NetX Duo empties the transmit queue of the client socket.

To unbind the port from the client socket, the application calls ***nx_tcp_client_socket_unbind***. The socket must be in a CLOSED state or in the process of disconnecting (i.e., TIMED WAIT state) before the port is released; otherwise, an error is returned.

Finally, if the application no longer needs the client socket, it calls ***nx_tcp_socket_delete*** to delete the socket.

TCP Server Connection

The server side of a TCP connection is passive; i.e., the server waits for a client to initiate connection request. To accept a client connection, TCP must first be enabled on the IP instance by calling the service ***nx_tcp_enable***. Next, the application must create a TCP socket using the ***nx_tcp_socket_create*** service.

The server socket must also be set up for listening for connection requests. This is achieved by using the ***nx_tcp_server_socket_listen*** service. This service places the server socket in the LISTEN state and binds the specified server port to the socket.

i

To set a socket listen callback routine the application specifies the appropriate callback function for the tcp_listen_callback argument of the ***nx_tcp_server_socket_listen*** *service. This application callback function is then executed by NetX Duo whenever a new connection is requested on this server port. The processing in the callback is under application control.*

To accept client connection requests, the application calls the ***nx_tcp_server_socket_accept*** service. The server socket must either be in a LISTEN state or a SYN RECEIVED state (i.e., the server is in the LISTEN state and has received a SYN packet from a client requesting a connection) to call the accept service. A successful return status from ***nx_tcp_server_socket_accept*** indicates the connection has been set up and the server socket is in the ESTABLISHED state.

After the server socket has a valid connection, additional client connection requests are queued up to the depth specified by the *listen_queue_size, passed into the* ***nx_tcp_server_socket_listen*** service. In order to process subsequent connections on a server port, the application must call ***nx_tcp_server_socket_relisten*** with an available socket (i.e., a socket in a CLOSED state). Note that the same server socket could be used if the previous connection associated with the socket is now finished and the socket is in the CLOSED state.

TCP Server Disconnection

Closing the connection is accomplished by calling ***nx_tcp_socket_disconnect***. If no suspension is specified, the server socket sends a RST packet to the client socket and places the socket in the CLOSED state. Otherwise, if a suspension is requested, the full TCP disconnect protocol is performed, as follows:

- If the client previously initiated a disconnect request (the server socket has already received a FIN packet, responded with an ACK, and is in the CLOSE WAIT state), NetX Duo promotes the TCP socket state to the LAST ACK state and sends a FIN packet. It then waits for an ACK from the client before completing the disconnect and entering the CLOSED state.
- If on the other hand, the server is the first to initiate a disconnect request (the client has not disconnected and the socket is still in the ESTABLISHED state), NetX Duo sends a FIN packet to initiate the disconnect and waits to receive a FIN and an ACK from the client before completing the disconnect and placing the socket in a CLOSED state.

If there are still packets on the socket transmit queue, NetX Duo suspends for the specified timeout to allow those packets to be acknowledged. If the timeout expires, NetX Duo flushes the transmit queue of the server socket.

After the disconnect processing is complete and the server socket is in the CLOSED state, the application must call the ***nx_tcp_server_socket_unaccept*** service to end the association of this socket with the server port. Note this service must be called by the application even if ***nx_tcp_socket_disconnect*** or ***nx_tcp_server_socket_accept*** return an error status. After the ***nx_tcp_server_socket_unaccept*** returns, the socket can be used as a client or server socket, or even deleted if it is no longer needed. If accepting another client connection on the same server port is desired, the ***nx_tcp_server_socket_relisten*** service should be called on this socket.

The following code segment illustrates the sequence of calls a typical TCP server uses:

```
/* Set up a previously created TCP socket to listen on port
   12 */
nx_tcp_server_socket_listen()

/* Loop to make a (another) connection. */
while(1)
{
   /* Wait for a client socket connection request for 100
      ticks.  */
   nx_tcp_server_socket_accept();

   /* (Send and receive TCP messages with the TCP client)
       */

   /* Disconnect the server socket.  */
   nx_tcp_socket_disconnect();

   /* Remove this server socket from listening on the
      port.  */
   nx_tcp_server_socket_unaccept(&server_socket);

   /* Set up server socket to relisten on the same port for
      the next client. */
   nx_tcp_server_socket_relisten();

}
```

MSS Validation

The Maximum Segment Size (MSS) is the maximum amount of bytes a TCP host can receive without being fragmented by the underlying IP layer. During TCP connection establishment phase, both ends exchanges its own TCP MSS value, so that the sender does not send a TCP data segment that is larger than the receiver's MSS. NetX Duo TCP module will optionally validate its peer's advertised MSS value before establishing a connection. By default NetX Duo does not enable such a check. Applications wishing to perform MSS validation shall define ***NX_ENABLE_TCP_MSS_CHECK*** when building the NetX Duo library, and the minimum value shall be defined in ***NX_TCP_MSS_MINIMUM***. Incoming TCP connections with MSS values below ***NX_TCP_MSS_MINIMUM*** are dropped.

Stop Listening on a Server Port

If the application no longer wishes to listen for client connection requests on a server port that was previously specified by a call to the ***nx_tcp_server_socket_listen*** service, the application simply calls the ***nx_tcp_server_socket_unlisten*** service. This service places any socket waiting for a connection back in the CLOSED state and releases any queued client connection request packets.

TCP Window Size

During both the setup and data transfer phases of the connection, each port reports the amount of data it can handle, which is called its window size. As data are received and processed, this window size is adjusted dynamically. In TCP, a sender can only send an amount of data that fits into the receiver's window. In essence, the window size provides flow control for data transfer in each direction of the connection.

TCP Packet Send

Sending TCP data is easily accomplished by calling the ***nx_tcp_socket_send*** function. If the size of the data being transmitted is larger than the MSS value of the socket or the current peer receive window size, whichever is smaller, TCP internal logic carves off the data that fits into min (MSS, peer receive Window) for transmission. This service then builds a TCP header in front of the packet (including the checksum calculation). If the receiver's window size is not zero, the caller will send as much data as it can to fill up the receiver window size. If the receive window becomes zero, the caller may suspend and wait for the receiver's window size to increase enough for this packet to be sent. At any given time, multiple threads may suspend while trying to send data through the same socket.

The TCP data residing in the NX_PACKET structure should reside on a long-word boundary. In addition, there needs to be sufficient space between the prepend pointer and the data start pointer to place the TCP, IP, and physical media headers.

TCP Packet Retransmit

Previously transmitted TCP packets sent actually stored internally until an ACK is returned from the other side of the connection. If transmitted data is not acknowledged within the timeout period, the stored packet is re-sent and the next timeout period is set. When an ACK is received, all packets covered by the acknowledgement number in the internal transmit queue are finally released.

Application shall not reuse the packet or alter the contents of the packet after nx_tcp_socket_send() returns with NX_SUCCESS. The transmitted packet is eventually released by NetX Duo internal processing after the data is acknowledged by the other end.

TCP Keepalive

TCP Keepalive feature allows a socket to detect whether or not its peer disconnects without proper termination (for example, the peer crashed), or to prevent certain network monitoring facilities to terminate a connection for long periods of idle. TCP Keepalive works by periodically sending a TCP frame with no data, and the sequence number set to one less than the current sequence number. On receiving such TCP Keepalive frame, the recipient, if still alive, responses with an ACK for its current sequence number. This completes the keepalive transaction.

By default the keepalive feature is not enabled. To use this feature, NetX Duo library must be built with ***NX_ENABLE_TCP_KEEPALIVE*** defined. The symbol ***NX_TCP_KEEPALIVE_INITIAL*** specifies the number of seconds of inactivity before the keepalive frame is initiated.

TCP Packet Receive

The TCP receive packet processing (called from the IP helper thread) is responsible for handling various connection and disconnection actions as well as transmit acknowledge processing. In addition, the TCP receive packet processing is responsible for placing packets with receive data on the appropriate TCP socket's receive queue or delivering the packet to the first suspended thread waiting for a packet.

TCP Receive Notify

If the application thread needs to process received data from more than one socket, the ***nx_tcp_socket_receive_notify*** function should be used. This function registers a receive packet callback function for the socket. Whenever a packet is received on the socket, the callback function is executed.

The contents of the callback function are application-specific; however, the function would most likely contain logic to inform the processing thread that a packet is available on the corresponding socket.

Thread Suspension

As mentioned previously, application threads can suspend while attempting to receive data from a particular TCP port. After a packet is received on that port, it is given to the first thread suspended and that thread is then resumed. An optional timeout is available when suspending on a TCP receive packet, a feature available for most NetX Duo services.

Thread suspension is also available for connection (both client and server), client binding, and disconnection services.

TCP Socket Statistics and Errors

If enabled, the NetX Duo TCP socket software keeps track of several statistics and errors that may be useful to the application. The following statistics and error reports are maintained for each IP/TCP instance:

Total TCP Packets Sent
Total TCP Bytes Sent
Total TCP Packets Received
Total TCP Bytes Received
Total TCP Invalid Packets
Total TCP Receive Packets Dropped
Total TCP Receive Checksum Errors
Total TCP Connections
Total TCP Disconnections
Total TCP Connections Dropped
Total TCP Packet Retransmits
TCP Socket Packets Sent
TCP Socket Bytes Sent
TCP Socket Packets Received
TCP Socket Bytes Received
TCP Socket Packet Retransmits
TCP Socket Packets Queued
TCP Socket Checksum Errors
TCP Socket State
TCP Socket Transmit Queue Depth

TCP Socket Transmit Window Size
TCP Socket Receive Window Size

All these statistics and error reports are available to the application with the ***nx_tcp_info_get*** service for total TCP statistics and the ***nx_tcp_socket_info_get*** service for TCP statistics per socket.

TCP Socket Control Block NX_TCP_SOCKET

The characteristics of each TCP socket are found in the associated *NX_TCP_SOCKET* control block, which contains useful information such as the link to the IP data structure, the network connection interface, the bound port, and the receive packet queue. This structure is defined in the ***nx_api.h*** file.

Chapter 4: Description of NetX Duo Services

This chapter contains a description of all NetX Duo services in alphabetic order. Service names are designed so all similar services are grouped together. For example, all ARP services are found at the beginning of this chapter.

There are numerous new services in NetX Duo introduced to support IPv6-based protocols and operations. IPv6-enabled services in Net Duo have the prefix ***nxd****,* indicating that they are designed for IPv4 and IPv6 dual stack operation.

Existing services in NetX are fully supported in NetX Duo. NetX applications can be migrated to NetX Duo with minimal porting effort.

Note that a BSD-Compatible Socket API is available for legacy application code that cannot take full advantage of the high-performance NetX Duo API. Refer to Appendix D for more information on the BSD-Compatible Socket API.

In the "Return Values" section of each description, values in **BOLD** are not affected by the NX_DISABLE_ERROR_CHECKING option used to disable the API error checking, while values in non-bold are completely disabled. The "Allowed From" sections indicate from which each NetX Duo service can be called.

nx_arp_dynamic_entries_invalidate

Invalidate all dynamic entries in the ARP cache

Prototype

```
UINT  nx_arp_dynamic_entries_invalidate(NX_IP *ip_ptr);
```

Description

This service invalidates all dynamic ARP entries currently in the ARP cache.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful ARP cache invalidate.
NX_NOT_ENABLED	(0x14)	ARP is not enabled.
NX_PTR_ERROR	(0x07)	Invalid IP address.
NX_CALLER_ERROR	(0x11)	Caller is not a thread.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Invalidate all dynamic entries in the ARP cache. */
status =  nx_arp_dynamic_entries_invalidate(&ip_0);

/*  If status is NX_SUCCESS the dynamic ARP entries were
    successfully invalidated.  */
```

See Also

nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_dynamic_entry_set

Set dynamic ARP entry

Prototype

```
UINT  nx_arp_dynamic_entry_set(NX_IP *ip_ptr,
                               ULONG ip_address,
                               ULONG physical_msw,
                               ULONG physical_lsw);
```

Description

This service allocates a dynamic entry from the ARP cache and sets up the specified IP to physical address mapping. If a zero physical address is specified, an actual ARP request is sent to the network in order to have the physical address resolved. Also note that this entry will be removed if ARP aging is active or if the ARP cache is exhausted and this is the least recently used ARP entry.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address to map.
physical_msw	Top 16 bits (47-32) of the physical address.
physical_lsw	Lower 32 bits (31-0) of the physical address.

Return Values

NX_SUCCESS	(0x00)	Successful ARP dynamic entry set.
NX_NO_MORE_ENTRIES	(0x17)	No more ARP entries are available in the ARP cache.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP instance pointer.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Setup a dynamic ARP entry on the previously created IP
    Instance 0. */
status = nx_arp_dynamic_entry_set(&ip_0, IP_ADDRESS(1,2,3,4),
                                  0x1022, 0x1234);

/*  If status is NX_SUCCESS, there is now a dynamic mapping between
    the IP address of 1.2.3.4 and the physical hardware address of
    10:22:00:00:12:34. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_enable

Enable Address Resolution Protocol (ARP)

Prototype

```
UINT nx_arp_enable(NX_IP *ip_ptr, VOID *arp_cache_memory,
                   ULONG arp_cache_size);
```

Description

This service initializes the ARP component of NetX Duo for the specific IP instance. ARP initialization includes setting up the ARP cache and various ARP processing routines necessary for sending and receiving ARP messages.

Parameters

ip_ptr	Pointer to previously created IP instance.
arp_cache_memory	Pointer to memory area to place ARP cache.
arp_cache_size	Each ARP entry is 52 bytes, the total number of ARP entries is, therefore, the size divided by 52.

Return Values

NX_SUCCESS	(0x00)	Successful ARP enable.
NX_PTR_ERROR	(0x07)	Invalid IP or cache memory pointer.
NX_SIZE_ERROR	(0x09)	User supplied ARP cache memory is too small.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_ALREADY_ENABLED	(0x15)	This component has already been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Enable ARP and supply 1024 bytes of ARP cache memory for
    previously created IP Instance ip_0.  */
status =  nx_arp_enable(&ip_0, (void *) pointer, 1024);

/*  If status is NX_SUCCESS, ARP was successfully enabled for this
    IP
    instance.*/
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_entry_delete

Delete an ARP entry

Prototype

```
UINT nx_arp_entry_delete(NX_IP *ip_ptr, ULONG ip_address);
```

Description

This service removes an ARP entry for the given IP address from its IP internal ARP table.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	ARP entry with the specified IP address should be deleted.

Return Values

NX_SUCCESS	(0x00)	Successful ARP enable.
NX_ENTRY_NOT_FOUND	(0x16)	No entry with the specified IP address can be found.
NX_PTR_ERROR	(0x07)	Invalid IP or cache memory pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_IP_ADDRESS_ERROR	(0x21)	Specified IP address is invalid.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Delete the ARP entry with the IP address 1.2.3.4. */
status =  nx_arp_entry_delete(&ip_0, IP_ADDRESS(1, 2, 3, 4));

/*  If status is NX_SUCCESS, ARP entry with the specified IP address
    is deleted.*/
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_gratuitous_send

Send gratuitous ARP request

Prototype

```
UINT  nx_arp_gratuitous_send(NX_IP *ip_ptr,
                             VOID (*response_handler)
                               (NX_IP *ip_ptr,
                                NX_PACKET *packet_ptr));
```

Description

This service goes through all the physical interfaces to transmit gratuitous ARP requests as long as the interface IP address is valid. If an ARP response is subsequently received, the supplied response handler is called to process the response to the gratuitous ARP.

Parameters

ip_ptr	Pointer to previously created IP instance.
response_handler	Pointer to response handling function. If NX_NULL is supplied, responses are ignored.

Return Values

NX_SUCCESS	(0x00)	Successful gratuitous ARP send.
NX_NO_PACKET	(0x01)	No packet available.
NX_NOT_ENABLED	(0x14)	ARP is not enabled.
NX_IP_ADDRESS_ERROR	(0x21)	Current IP address is invalid.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Caller is not a thread.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Send gratuitous ARP without any response handler. */
status =  nx_arp_gratuitous_send(&ip_0, NX_NULL);

/*  If status is NX_SUCCESS the gratuitous ARP was successfully
    sent.  */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_hardware_address_find

Locate physical hardware address given an IP address

Prototype

```
UINT nx_arp_hardware_address_find(NX_IP *ip_ptr,
                                   ULONG ip_address,
                                   ULONG *physical_msw,
                                   ULONG *physical_lsw);
```

Description

This service attempts to find a physical hardware address in the ARP cache that is associated with the supplied IP address.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address to search for.
physical_msw	Pointer to the variable for returning the top 16 bits (47-32) of the physical address.
physical_lsw	Pointer to the variable for returning the lower 32 bits (31-0) of the physical address.

Return Values

NX_SUCCESS	(0x00)	Successful ARP hardware address find.
NX_ENTRY_NOT_FOUND	(0x16)	Mapping was not found in the ARP cache.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP or memory pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Search for the hardware address associated with the IP address
    of 1.2.3.4 in the ARP cache of the previously created IP
    Instance 0.   */
status = nx_arp_hardware_address_find(&ip_0, IP_ADDRESS(1,2,3,4),
                                      &physical_msw,
                                      &physical_lsw);

/*  If status is NX_SUCCESS, the variables physical_msw and
    physical_lsw contain the hardware address.*/
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_info_get

Retrieve information about ARP activities

Prototype

```
UINT nx_arp_info_get(NX_IP *ip_ptr,
                     ULONG *arp_requests_sent,
                     ULONG *arp_requests_received,
                     ULONG *arp_responses_sent,
                     ULONG *arp_responses_received,
                     ULONG *arp_dynamic_entries,
                     ULONG *arp_static_entries,
                     ULONG *arp_aged_entries,
                     ULONG *arp_invalid_messages);
```

Description

This service retrieves information about ARP activities for the associated IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
arp_requests_sent	Pointer to destination for the total ARP requests sent from this IP instance.
arp_requests_received	Pointer to destination for the total ARP requests received from the network.
arp_responses_sent	Pointer to destination for the total ARP responses sent from this IP instance.
arp_responses_received	Pointer to the destination for the total ARP responses received from the network.
arp_dynamic_entries	Pointer to the destination for the current number of dynamic ARP entries.
arp_static_entries	Pointer to the destination for the current number of static ARP entries.

arp_aged_entries	Pointer to the destination of the total number of ARP entries that have aged and became invalid.
arp_invalid_messages	Pointer to the destination of the total invalid ARP messages received.

Return Values

NX_SUCCESS	(0x00)	Successful ARP information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Pickup ARP information for ip_0.  */
status =  nx_arp_info_get(&ip_0, &arp_requests_sent,
                           &arp_requests_received,
                           &arp_responses_sent,
                           &arp_responses_received,
                           &arp_dynamic_entries,
                           &arp_static_entries,
                           &arp_aged_entries,
                           &arp_invalid_messages);

/*  If status is NX_SUCCESS, the ARP information has been stored in
    the supplied variables.  */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_ip_address_find

Locate IP address given a physical address

Prototype

```
UINT nx_arp_ip_address_find(NX_IP *ip_ptr, ULONG *ip_address,
                            ULONG physical_msw, ULONG physical_lsw);
```

Description

This service attempts to find an IP address in the ARP cache that is associated with the supplied physical address.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	Pointer to return IP address, if one is found that has been mapped.
physical_msw	Top 16 bits (47-32) of the physical address to search for.
physical_lsw	Lower 32 bits (31-0) of the physical address to search for.

Return Values

NX_SUCCESS	(0x00)	Successful ARP IP address find
NX_ENTRY_NOT_FOUND	(0x16)	Mapping was not found in the ARP cache.
NX_PTR_ERROR	(0x07)	Invalid IP or memory pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_INVALID_PARAMETERS	(0x4D)	Physical_msw and physical_lsw are both 0.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Search for the IP address associated with the hardware address
    of 0x0:0x01234 in the ARP cache of the previously created IP
    Instance ip_0. */
status = nx_arp_ip_address_find(&ip_0, &ip_address, 0x0, 0x1234);

/*  If status is NX_SUCCESS, the variables ip_address contains the
    associated IP address. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_static_entries_delete

Delete all static ARP entries

Prototype

```
UINT nx_arp_static_entries_delete(NX_IP *ip_ptr);
```

Description

This service deletes all static entries in the ARP cache.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Static entries are deleted.
NX_PTR_ERROR	(0x07)	Invalid *ip_ptr* pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Delete all the static ARP entries for IP Instance 0, assuming
    "ip_0" is the NX_IP structure for IP Instance 0.  */
status =  nx_arp_static_entries_delete(&ip_0);

/*  If status is NX_SUCCESS all static ARP entries in the ARP cache
    have been deleted.  */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_static_entry_create

Create static IP to hardware mapping in ARP cache

Prototype

```
UINT nx_arp_static_entry_create(NX_IP *ip_ptr,
                                ULONG ip_address,
                                ULONG physical_msw,
                                ULONG physical_lsw);
```

Description

This service creates a static IP-to-physical address mapping in the ARP cache for the specified IP instance. Static ARP entries are not subject to ARP periodic updates.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address to map.
physical_msw	Top 16 bits (47-32) of the physical address to map.
physical_lsw	Lower 32 bits (31-0) of the physical address to map.

Return Values

NX_SUCCESS	(0x00)	Successful ARP static entry create.
NX_NO_MORE_ENTRIES	(0x17)	No more ARP entries are available in the ARP cache.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_INVALID_PARAMETERS	(0x4D)	Physical_msw and physical_lsw are both 0.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Create a static ARP entry on the previously created IP
    Instance 0.  */
status =  nx_arp_static_entry_create(&ip_0, IP_ADDRESS(1,2,3,4),
                                     0x0, 0x1234);

/*  If status is NX_SUCCESS, there is now a static mapping between
    the IP address of 1.2.3.4 and the physical hardware address of
    0x00:0x1234.  */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_arp_static_entry_delete

Delete static IP to hardware mapping in ARP cache

Prototype

```
UINT nx_arp_static_entry_delete(NX_IP *ip_ptr,
                                ULONG ip_address,
                                ULONG physical_msw,
                                ULONG physical_lsw);
```

Description

This service finds and deletes a previously created static IP-to-physical address mapping in the ARP cache for the specified IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address that was mapped statically.
physical_msw	Top 16 bits (47 - 32) of the physical address that was mapped statically.
physical_lsw	Lower 32 bits (31 - 0) of the physical address that was mapped statically.

Return Values

NX_SUCCESS	(0x00)	Successful ARP static entry delete.
NX_ENTRY_NOT_FOUND	(0x16)	Static ARP entry was not found in the ARP cache.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_INVALID_PARAMETERS	(0x4D)	Physical_msw and physical_lsw are both 0.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Delete a static ARP entry on the previously created IP
    instance ip_0.  */
status =  nx_arp_static_entry_delete(&ip_0, IP_ADDRESS(1,2,3,4),
                                     0x0, 0x1234);

/*  If status is NX_SUCCESS, the previously created static ARP entry
    was successfully deleted.  */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nx_icmp_enable

Enable Internet Control Message Protocol (ICMP)

Prototype

```
UINT nx_icmp_enable(NX_IP *ip_ptr);
```

Description

This service enables the ICMP component for the specified IP instance. The ICMP component is responsible for handling Internet error messages and ping requests and replies.

*This service only enables ICMP for IPv4 service. To enable both ICMPv4 and ICMPv6, applications shall use the **nxd_icmp_enable** service.*

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful ICMP enable.
NX_ALREADY_ENABLED	(0x15)	ICMP is already enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Enable ICMP on the previously created IP Instance ip_0.  */
status =  nx_icmp_enable(&ip_0);

/* If status is NX_SUCCESS, ICMP is enabled.  */
```

See Also

nx_icmp_info_get, nx_icmp_ping, nxd_icmp_enable, nxd_icmp_ping, nxd_icmp_source_ping, nxd_icmpv6_ra_flag_callback_set

nx_icmp_info_get

Retrieve information about ICMP activities

Prototype

```
UINT nx_icmp_info_get(NX_IP *ip_ptr,
                      ULONG *pings_sent,
                      ULONG *ping_timeouts,
                      ULONG *ping_threads_suspended,
                      ULONG *ping_responses_received,
                      ULONG *icmp_checksum_errors,
                      ULONG *icmp_unhandled_messages);
```

Description

This service retrieves information about ICMP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
pings_sent	Pointer to destination for the total number of pings sent.
ping_timeouts	Pointer to destination for the total number of ping timeouts.
ping_threads_suspended	Pointer to destination of the total number of threads suspended on ping requests.
ping_responses_received	Pointer to destination of the total number of ping responses received.
icmp_checksum_errors	Pointer to destination of the total number of ICMP checksum errors.
icmp_unhandled_messages	Pointer to destination of the total number of un-handled ICMP messages.

Return Values

NX_SUCCESS	(0x00)	Successful ICMP information retrieval.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Retrieve ICMP information from previously created IP
    instance ip_0. */
status =  nx_icmp_info_get(&ip_0, &pings_sent, &ping_timeouts,
                           &ping_threads_suspended,
                           &ping_responses_received,
                           &icmp_checksum_errors,
                           &icmp_unhandled_messages);

/*  If status is NX_SUCCESS, ICMP information was retrieved.  */
```

See Also

nx_icmp_enable, nx_icmp_ping, nxd_icmp_enable, nxd_icmp_ping, nxd_icmp_source_ping, nxd_icmpv6_ra_flag_callback_set

nx_icmp_ping

Send ping request to specified IP address

Prototype

```
UINT nx_icmp_ping(NX_IP *ip_ptr,
                  ULONG ip_address,
                  CHAR *data, ULONG data_size,
                  NX_PACKET **response_ptr,
                  ULONG wait_option);
```

Description

This service sends a ping request to the specified IP address and waits for the specified amount of time for a ping response message. If no response is received, an error is returned. Otherwise, the entire response message is returned in the variable pointed to by response_ptr.

To send a ping request to an IPv6 destination, applications shall use the ***nxd_icmp_ping*** or ***nxd_icmp_source_ping*** service.

If NX_SUCCESS is returned, the application is responsible for releasing the received packet after it is no longer needed.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address, in host byte order, to ping.
data	Pointer to data area for ping message.
data_size	Number of bytes in the ping data
response_ptr	Pointer to packet pointer to return the ping response message in.
wait_option	Defines the number of ThreadX timer ticks to wait for a ping response. The wait options are defined as follows: NX_NO_WAIT (0x00000000) timeout value in ticks (0x00000001 through 0xFFFFFFFE) NX_WAIT_FOREVER0xFFFFFFFF

Return Values

NX_SUCCESS	(0x00)	Successful ping. Response message pointer was placed in

		the variable pointed to by response_ptr.
NX_NO_PACKET	(0x01)	Unable to allocate a ping request packet.
NX_OVERFLOW	(0x03)	Specified data area exceeds the default packet size for this IP instance.
NX_NO_RESPONSE	(0x29)	Requested IP did not respond.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP or response pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Issue a ping to IP address 1.2.3.5 from the previously created
    IP Instance ip_0.  */
status =  nx_icmp_ping(&ip_0, IP_ADDRESS(1,2,3,5), "abcd", 4,
                       &response_ptr, 10);

/*  If status is NX_SUCCESS, a ping response was received from IP
    address 1.2.3.5 and the response packet is contained in the
    packet pointed to by response_ptr. It should have the same
    "abcd" four bytes of data.  */
```

See Also

nx_icmp_enable, nx_icmp_info_get, nxd_icmp_enable, nxd_icmp_ping, nxd_icmp_source_ping, nxd_icmpv6_ra_flag_callback_set

nx_igmp_enable

Enable Internet Group Management Protocol (IGMP)

Prototype

```
UINT nx_igmp_enable(NX_IP *ip_ptr);
```

Description

This service enables the IGMP component on the specified IP instance. The IGMP component is responsible for providing support for IP multicast group management operations.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IGMP enable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_ALREADY_ENABLED	(0x15)	This component has already been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Enable IGMP on the previously created IP Instance ip_0.  */
status =  nx_igmp_enable(&ip_0);

/* If status is NX_SUCCESS, IGMP is enabled.  */
```

See Also

nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_info_get

Retrieve information about IGMP activities

Prototype

```
UINT nx_igmp_info_get(NX_IP *ip_ptr,
                      ULONG *igmp_reports_sent,
                      ULONG *igmp_queries_received,
                      ULONG *igmp_checksum_errors,
                      ULONG *current_groups_joined);
```

Description

This service retrieves information about IGMP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
igmp_reports_sent	Pointer to destination for the total number of ICMP reports sent.
igmp_queries_received	Pointer to destination for the total number of queries received by multicast router.
igmp_checksum_errors	Pointer to destination of the total number of IGMP checksum errors on receive packets.
current_groups_joined	Pointer to destination of the current number of groups joined through this IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IGMP information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Retrieve IGMP information from previously created IP Instance
ip_0. */
status =  nx_igmp_info_get(&ip_0, &igmp_reports_sent,
                           &igmp_queries_received,
                           &igmp_checksum_errors,
                           &current_groups_joined);

/* If status is NX_SUCCESS, IGMP information was retrieved.  */
```

See Also

nx_igmp_enable, nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_loopback_disable

Disable IGMP loopback

Prototype

```
UINT  nx_igmp_loopback_disable(NX_IP *ip_ptr);
```

Description

This service disables IGMP loopback for all subsequent multicast groups joined.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IGMP loopback disable.
NX_NOT_ENABLED	(0x14)	IGMP is not enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Caller is not a thread or initialization.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Disable IGMP loopback for all subsequent multicast groups
    joined. */
status =  nx_igmp_loopback_disable(&ip_0);

/*  If status is NX_SUCCESS IGMP loopback is disabled.  */
```

See Also

nx_igmp_enable, nx_igmp_info_get, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_loopback_enable

Enable IGMP loopback

Prototype

```
UINT  nx_igmp_loopback_enable(NX_IP *ip_ptr);
```

Description

This service enables IGMP loopback for all subsequent multicast groups joined.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IGMP loopback disable.
NX_NOT_ENABLED	(0x14)	IGMP is not enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Caller is not a thread or initialization.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Enable IGMP loopback for all subsequent multicast
   groups joined. */
status =  nx_igmp_loopback_enable(&ip_0);

/* If status is NX_SUCCESS IGMP loopback is enabled.  */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_multicast_interface_join

Join IP instance to specified multicast group via an interface

Prototype

```
UINT nx_igmp_multicast_interface_join(NX_IP *ip_ptr,
                                      ULONG group_address,
                                      UINT  interface_index)
```

Description

This service joins an IP instance to the specified multicast group via a specified network interface. An internal counter is maintained to keep track of the number of times the same group has been joined. After joining the multicast group, the IGMP component will allow reception of IP packets with this group address via the specified network interface and also report to routers that this IP is a member of this multicast group. The IGMP membership join, report, and leave messages are also sent via the specified network interface. To join an IPv4 multicast group without sending IGMP group membership report, application shall use the service ***nx_ipv4_multicast_interface_join***.

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Class D IP multicast group address to join in host byte order.
interface_index	Index of the Interface attached to the NetX Duo instance.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_NO_MORE_ENTRIES	(0x17)	No more multicast groups can be joined, maximum exceeded.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.
NX_IP_ADDRESS_ERROR	(0x21)	Multicast group address provided is not a valid class D address.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

NX_NOT_ENABLED	(0x14)	IP multicast support is not enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Previously created IP Instance joins the multicast group
    244.0.0.200, via the interface at index 1 in the IP interface
    list.   */
#define INTERFACE_INDEX 1
status = nx_igmp_multicast_interface_join
                                  (&ip IP_ADDRESS(244,0,0,200),
                                   INTERFACE_INDEX);

/*  If status is NX_SUCCESS, the IP instance has successfully joined
    the multicast group. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_multicast_interface_leave

Leave specified multicast group via an interface

Prototype

```
UINT nx_igmp_multicast_interface_leave(NX_IP *ip_ptr,
                                       ULONG group_address,
                                       UINT  interface_index)
```

Description

This service leaves the specified multicast group via a specified network interface. An internal counter is maintained to keep track of the number of times the same group has been a member of. After leaving the multicast group, the IGMP component will send out proper membership report, and may leave the group if there are no members from this node. To leave an IPv4 multicast group without sending IGMP group membership report, application shall use the service ***nx_ipv4_multicast_interface_leave***.

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Class D IP multicast group address to leave. The IP address is in host byte order.
interface_index	Index of the Interface attached to the NetX Duo instance.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_ENTRY_NOT_FOUND	(0x16)	The specified multicast group address cannot be found in the local multicast table.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.
NX_IP_ADDRESS_ERROR	(0x21)	Multicast group address provided is not a valid class D address.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

NX_NOT_ENABLED	(0x14)	IP multicast support is not enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Leave the multicast group 244.0.0.200. */
#define INTERFACE_INDEX 1
status = nx_igmp_multicast_interface_leave
                                   (&ip IP_ADDRESS(244,0,0,200),
                                    INTERFACE_INDEX);

/*  If status is NX_SUCCESS, the IP instance has successfully leaves
    the multicast group 244.0.0.200. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_multicast_join

Join IP instance to specified multicast group

Prototype

```
UINT nx_igmp_multicast_join(NX_IP *ip_ptr, ULONG group_address);
```

Description

This service joins an IP instance to the specified multicast group. An internal counter is maintained to keep track of the number of times the same group has been joined. The driver is commanded to send an IGMP report if this is the first join request out on the network indicating the host's intention to join the group. After joining, the IGMP component will allow reception of IP packets with this group address and report to routers that this IP is a member of this multicast group. To join an IPv4 multicast group without sending IGMP group membership report, application shall use the service ***nx_ipv4_multicast_interface_join***.

To join a multicast group on a non-primary device, use the service ***nx_igmp_multicast_interface_join.***

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Class D IP multicast group address to join.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_NO_MORE_ENTRIES	(0x17)	No more multicast groups can be joined, maximum exceeded.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP group address.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Previously created IP Instance ip_0 joins the multicast group
    224.0.0.200. */
status =  nx_igmp_multicast_join(&ip_0, IP_ADDRESS(224,0,0,200);

/*  If status is NX_SUCCESS, this IP instance has successfully
    joined the multicast group 224.0.0.200.  */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_igmp_multicast_leave

Cause IP instance to leave specified multicast group

Prototype

```
UINT nx_igmp_multicast_leave(NX_IP *ip_ptr, ULONG group_address);
```

Description

This service causes an IP instance to leave the specified multicast group, if the number of leave requests matches the number of join requests. Otherwise, the internal join count is simply decremented. To leave an IPv4 multicast group without sending IGMP group membership report, application shall use the service ***nx_ipv4_multicast_interface_leave***.

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Multicast group to leave.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_ENTRY_NOT_FOUND	(0x16)	Previous join request was not found.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP group address.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Cause IP instance to leave the multicast group 224.0.0.200.  */
status =  nx_igmp_multicast_leave(&ip_0, IP_ADDRESS(224,0,0,200);

/*  If status is NX_SUCCESS, this IP instance has successfully left
    the multicast group 224.0.0.200. */
```

See Also

nx_igmp_enable, nx_igmp_info_get, nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_ip_address_change_notifiy

Notify application if IP address changes

Prototype

```
UINT  nx_ip_address_change_notify(NX_IP *ip_ptr,
                                  VOID(*change_notify)(NX_IP *,
                                  VOID *),VOID *additional_info);
```

Description

This service registers an application notification function that is called whenever the IPv4 address is changed.

Parameters

ip_ptr	Pointer to previously created IP instance.
change_notify	Pointer to IP change notification function. If this parameter is NX_NULL, IP address change notification is disabled.
additional_info	Pointer to optional additional information that is also supplied to the notification function when the IP address is changed.

Return Values

NX_SUCCESS	(0x00)	Successful IP address change notification.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Register the function "my_ip_changed" to be called whenever the
    IP address is changed. */
status =  nx_ip_address_change_notify(&ip_0, my_ip_changed,
                                      NX_NULL);

/*  If status is NX_SUCCESS, the "my_ip_changed" function will be
    called whenever the IP address changes. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_address_get

Retrieve IPv4 address and network mask

Prototype

```
UINT nx_ip_address_get(NX_IP *ip_ptr,
                       ULONG *ip_address,
                       ULONG *network_mask);
```

Description

This service retrieves IPv4 address and its subnet mask of the primary network interface.

*To obtain information of the secondary device, use the service **nx_ip_interface_address_get**.*

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	Pointer to destination for IP address.
network_mask	Pointer to destination for network mask.

Return Values

NX_SUCCESS	(0x00)	Successful IP address get.
NX_PTR_ERROR	(0x07)	Invalid IP or return variable pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Get the IP address and network mask from the previously created
    IP Instance ip_0.  */
status =  nx_ip_address_get(&ip_0, &ip_address, &network_mask);

/*  If status is NX_SUCCESS, the variables ip_address and
    network_mask contain the IP and network mask respectively.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_address_set

Set IPv4 address and network mask

Prototype

```
UINT nx_ip_address_set(NX_IP *ip_ptr,
                       ULONG ip_address,
                       ULONG network_mask);
```

Description

This service sets IPv4 address and network mask for the primary network interface.

To set IP address and network mask for the secondary device, use the service ***nx_ip_interface_address_set****.*

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	New IP address.
network_mask	New network mask.

Return Values

NX_SUCCESS	(0x00)	Successful IP address set.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Set the IP address and network mask to 1.2.3.4 and 0xFFFFFF00
    for the previously created IP Instance ip_0.  */
status =  nx_ip_address_set(&ip_0, IP_ADDRESS(1,2,3,4),
                             0xFFFFFF00UL);

/*  If status is NX_SUCCESS, the IP instance now has an IP address of
    1.2.3.4 and a network mask of 0xFFFFFF00.   */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_auxiliary_packet_pool_set

Configure an auxiliary packet pool

Prototype

```
UINT nx_ip_auxiliary_packet_pool_set(NX_IP *ip_ptr,
                                         NX_PACKET_POOL *aux_pool);
```

Description

This service configures an auxiliary packet pool in the IP instance. For a memory-constrained system, the user may increase memory efficiency by creating the default packet pool with packet size of MTU, and creating an auxiliary packet pool with smaller packet size for the IP thread to transmit small packets with. The recommended packet size for the auxiliary pool is 256 bytes, assuming IPv6 and IPsec are both enabled.

By default the IP instance does not accept the auxiliary packet pool. To enable this feature, *NX_DUAL_PACKET_POOL_ENABLE* must be defined when compiling the NetX Duo library.

Parameters

ip_ptr	Pointer to previously created IP instance.
aux_pool	The auxiliary packet pool to be configured for the IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP address set.
NX_NOT_SUPPORTED	(0x4B)	The dual packet pool feature is not compiled in the library.
NX_PTR_ERROR	(0x07)	Invalid IP pointer or pool pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define SMALL_PAYLOAD_SIZE 256
NX_PACKET small_pool;


nx_packet_pool_create(&small_pool, "small pool", SMALL_PAYLOAD_SIZE,
                      small_pool_memory_ptr, small_pool_size);

/* Add the small packet pool to the IP instance. */
status =  nx_ip_auxiliary_packet_pool_set(&ip_0, &small_pool);

/*  If status is NX_SUCCESS, the IP instance now is able to use the
    small pool for transmitting small datagram.   */
```

See Also

nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_ip_create

Create an IP instance

Prototype

```
UINT nx_ip_create(NX_IP *ip_ptr, CHAR *name, ULONG ip_address,
                  ULONG network_mask, NX_PACKET_POOL *default_pool,
                  VOID (*ip_network_driver)(NX_IP_DRIVER *),
                  VOID *memory_ptr, ULONG memory_size,
                  UINT priority);
```

Description

This service creates an IP instance with the user supplied IP address and network driver. In addition, the application must supply a previously created packet pool for the IP instance to use for internal packet allocation. Note that the supplied application network driver is not called until this IP's thread executes.

Parameters

ip_ptr	Pointer to control block to create a new IP instance.
name	Name of this new IP instance.
ip_address	IP address for this new IP instance.
network_mask	Mask to delineate the network portion of the IP address for sub-netting and super-netting uses.
default_pool	Pointer to control block of previously created NetX Duo packet pool.
ip_network_driver	User-supplied network driver used to send and receive IP packets.
memory_ptr	Pointer to memory area for the IP helper thread's stack area.
memory_size	Number of bytes in the memory area for the IP helper thread's stack.
priority	Priority of IP helper thread.

Return Values

NX_SUCCESS	(0x00)	Successful IP instance creation.

NX_NOT_IMPLEMENTED	(0x4A)	NetX Duo library is configured incorrectly.
NX_PTR_ERROR	(0x07)	Invalid IP, network driver function pointer, packet pool, or memory pointer.
NX_SIZE_ERROR	(0x09)	The supplied stack size is too small.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_IP_ADDRESS_ERROR	(0x21)	The supplied IP address is invalid.
NX_OPTION_ERROR	(0x21)	The supplied IP thread priority is invalid.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Create an IP instance with an IP address of 1.2.3.4 and a network
    mask of 0xFFFFFF00UL. The "ethernet_driver" specifies the entry
    point of the application specific network driver and the
    "stack_memory_ptr" specifies the start of a 1024 byte memory
    area that is used for this IP instance's helper thread. */
status = nx_ip_create(&ip_0, "NetX IP Instance ip_0",
                        IP_ADDRESS(1, 2, 3, 4),
                        0xFFFFFF00UL, &pool_0, ethernet_driver,
                        stack_memory_ptr, 1024, 1);

/*  If status is NX_SUCCESS, the IP instance has been created. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_delete

Delete previously created IP instance

Prototype

```
UINT nx_ip_delete(NX_IP *ip_ptr);
```

Description

This service deletes a previously created IP instance and releases all of the system resources owned by the IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP deletion.
NX_SOCKETS_BOUND	(0x28)	This IP instance still has UDP or TCP sockets bound to it. All sockets must be unbound and deleted prior to deleting the IP instance.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

Yes

Example

```
/*  Delete a previously created IP instance. */
status = nx_ip_delete(&ip_0);

/*  If status is NX_SUCCESS, the IP instance has been deleted.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_driver_direct_command

Issue command to network driver

Prototype

```
UINT nx_ip_driver_direct_command(NX_IP *ip_ptr,
                                 UINT command,
                                 ULONG *return_value_ptr);
```

Description

This service provides a direct interface to the application's primary network interface driver specified during the ***nx_ip_create*** call. Application-specific commands can be used providing their numeric value is greater than or equal to NX_LINK_USER_COMMAND.

To issue command for the secondary device, use the ***nx_ip_driver_interface_direct_command*** *service.*

Parameters

ip_ptr	Pointer to previously created IP instance.
command	Numeric command code. Standard commands are defined as follows: NX_LINK_GET_STATUS (10) NX_LINK_GET_SPEED (11) NX_LINK_GET_DUPLEX_TYPE (12) NX_LINK_GET_ERROR_COUNT (13) NX_LINK_GET_RX_COUNT (14) NX_LINK_GET_TX_COUNT (15) NX_LINK_GET_ALLOC_ERRORS (16) NX_LINK_USER_COMMAND (50)
return_value_ptr	Pointer to return variable in the caller.

Return Values

NX_SUCCESS	(0x00)	Successful network driver direct command.
NX_UNHANDLED_COMMAND	(0x44)	Unhandled or unimplemented network driver command.

NX_PTR_ERROR	(0x07)	Invalid IP or return value pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Make a direct call to the application-specific network driver
    for the previously created IP instance. For this example, the
    network driver is interrogated for the link status.  */
status = nx_ip_driver_direct_command(&ip_0, NX_LINK_GET_STATUS,
                                      &link_status);

/*  If status is NX_SUCCESS, the link_status variable contains a
    NX_TRUE or NX_FALSE value representing the status of the
    physical link.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_driver_interface_direct_command

Issue command to network driver

Prototype

```
UINT nx_ip_driver_interface_direct_command(NX_IP *ip_ptr,
                                           UINT command,
                                           UINT interface_index,
                                           ULONG *return_value_ptr);
```

Description

This service provides a direct command to the application's network device driver in the IP instance. Application-specific commands can be used providing their numeric value is greater than or equal to *NX_LINK_USER_COMMAND*.

Parameters

ip_ptr	Pointer to previously created IP instance.
command	Numeric command code. Standard commands are defined as follows: NX_LINK_GET_STATUS (10) NX_LINK_GET_SPEED (11) NX_LINK_GET_DUPLEX_TYPE (12) NX_LINK_GET_ERROR_COUNT (13) NX_LINK_GET_RX_COUNT (14) NX_LINK_GET_TX_COUNT (15) NX_LINK_GET_ALLOC_ERRORS (16) NX_LINK_USER_COMMAND (50)
interface_index	Index of the network interface the command should be sent to.
return_value_ptr	Pointer to return variable in the caller.

Return Values

NX_SUCCESS	(0x00)	Successful network driver direct command.
NX_UNHANDLED_COMMAND	(0x44)	Unhandled or unimplemented network driver command.
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index

NX_PTR_ERROR	(0x07)	Invalid IP or return value pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Make a direct call to the application-specific network driver
    for the previously created IP instance. For this example, the
    network driver is interrogated for the link status.  */

/*  Set the interface index to the primary device. */
UINT interface_index = 0;

status = nx_ip_driver_interface_direct_command(&ip_0,
                                               NX_LINK_GET_STATUS,
                                               interface_index,
                                               &link_status);

/*  If status is NX_SUCCESS, the link_status variable contains a
    NX_TRUE or NX_FALSE value representing the status of the
    physical link.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_forwarding_disable

Disable IP packet forwarding

Prototype

```
UINT nx_ip_forwarding_disable(NX_IP *ip_ptr);
```

Description

This service disables forwarding IP packets inside the NetX Duo IP component. On creation of the IP task, this service is automatically disabled.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP forwarding disable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads, timers

Preemption Possible

No

Example

```
/*  Disable IP forwarding on this IP instance.  */
status = nx_ip_forwarding_disable(&ip_0);

/*  If status is NX_SUCCESS, IP forwarding has been disabled on the
    previously created IP instance.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_forwarding_enable

Enable IP packet forwarding

Prototype

```
UINT nx_ip_forwarding_enable(NX_IP *ip_ptr);
```

Description

This service enables forwarding IP packets inside the NetX Duo IP component. On creation of the IP task, this service is automatically disabled.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP forwarding enable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads, timers

Preemption Possible

No

Example

```
/*  Enable IP forwarding on this IP instance.  */
status = nx_ip_forwarding_enable(&ip_0);

/*  If status is NX_SUCCESS, IP forwarding has been enabled on the
    previously created IP instance.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_fragment_disable

Disable IP packet fragmenting

Prototype

```
UINT nx_ip_fragment_disable(NX_IP *ip_ptr);
```

Description

This service disables IPv4 and IPv6 packet fragmenting and reassembling functionality. For packets waiting to be reassembled, this service releases these packets. On creation of the IP task, this service is automatically disabled.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP fragment disable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	IP Fragmentation is not enabled on the IP instance.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Disable IP fragmenting on this IP instance.  */
status = nx_ip_fragment_disable(&ip_0);

/*  If status is NX_SUCCESS, disables IP fragmenting on the
    previously created IP instance.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_fragment_enable

Enable IP packet fragmenting

Prototype

```
UINT nx_ip_fragment_enable(NX_IP *ip_ptr);
```

Description

This service enables IPv4 and IPv6 packet fragmenting and reassembling functionality. On creation of the IP task, this service is automatically disabled.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP fragment enable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	IP Fragmentation features is not compiled into NetX Duo.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Enable IP fragmenting on this IP instance.  */
status = nx_ip_fragment_enable(&ip_0);

/*  If status is NX_SUCCESS, IP fragmenting has been enabled on the
    previously created IP instance.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_gateway_address_clear

Clear the IPv4 gateway address

Prototype

```
UINT nx_ip_gateway_address_clear(NX_IP *ip_ptr)
```

Description

This service clears the IPv4 gateway address configured in the IP instance. To clear an IPv6 default router from the IP instance, applications shall use the service ***nxd_ipv6_default_router_delete.***

Parameters

ip_ptr	IP control block pointer

Return Values

NX_SUCCESS	(0x00)	Successfully cleared the IP gateway address.
NX_PTR_ERROR	(0x07)	Invalid IP control block
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Clear the gateway address of IP instance. */
status = nx_ip_gateway_address_clear(&ip_0);

/* If status == NX_SUCCESS, the gateway address was successfully
   cleared from the IP instance. */
```

See Also

nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nx_ip_gateway_address_get

Get the IPv4 gateway address

Prototype

```
UINT nx_ip_gateway_address_get(NX_IP *ip_ptr, ULONG *ip_address)
```

Description

This service retrieves the IPv4 gateway address configured in the IP instance.

Parameters

ip_ptr	IP control block pointer
ip_address	Pointer to the memory where the gateway address is stored

Return Values

NX_SUCCESS	(0x00)	Successful get
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer or ip address pointer
NX_NOT_FOUND	(0x4E)	Gateway address not found
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
ULONG  ip_address;

/* Get the gateway address of IP instance. */
status = nx_ip_gateway_address_get(&ip_0, &ip_address);

/* If status == NX_SUCCESS, the gateway address was successfully
   got. */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nx_ip_gateway_address_set

Set Gateway IP address

Prototype

```
UINT  nx_ip_gateway_address_set(NX_IP *ip_ptr, ULONG ip_address);
```

Description

This service sets the IPv4 gateway IP address. All out-of-network traffic are routed to this gateway for transmission. The gateway must be directly accessible through one of the network interfaces. To configure IPv6 gateway address, use the service ***nxd_ipv6_default_router_add.***

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_address	IP address of the gateway.

Return Values

NX_SUCCESS	(0x00)	Successful Gateway IP address set.
NX_PTR_ERROR	(0x07)	Invalid IP instance pointer.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, thread

Preemption Possible

No

Example

```
/*  Setup the Gateway address for previously created IP
    Instance ip_0. */
status = nx_ip_gateway_address_set(&ip_0, IP_ADDRESS(1,2,3,99);

/*  If status is NX_SUCCESS, all out-of-network send requests are
    routed to 1.2.3.99. */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nx_ip_info_get

Retrieve information about IP activities

Prototype

```
UINT nx_ip_info_get(NX_IP *ip_ptr,
                    ULONG *ip_total_packets_sent,
                    ULONG *ip_total_bytes_sent,
                    ULONG *ip_total_packets_received,
                    ULONG *ip_total_bytes_received,
                    ULONG *ip_invalid_packets,
                    ULONG *ip_receive_packets_dropped,
                    ULONG *ip_receive_checksum_errors,
                    ULONG *ip_send_packets_dropped,
                    ULONG *ip_total_fragments_sent,
                    ULONG *ip_total_fragments_received);
```

Description

This service retrieves information about IP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
ip_total_packets_sent	Pointer to destination for the total number of IP packets sent.
ip_total_bytes_sent	Pointer to destination for the total number of bytes sent.
ip_total_packets_received	Pointer to destination of the total number of IP receive packets.
ip_total_bytes_received	Pointer to destination of the total number of IP bytes received.
ip_invalid_packets	Pointer to destination of the total number of invalid IP packets.
ip_receive_packets_dropped	Pointer to destination of the total number of receive packets dropped.
ip_receive_checksum_errors	Pointer to destination of the total number of checksum errors in receive packets.
ip_send_packets_dropped	Pointer to destination of the total number of send packets dropped.

ip_total_fragments_sent	Pointer to destination of the total number of fragments sent.
ip_total_fragments_received	Pointer to destination of the total number of fragments received.

Return Values

NX_SUCCESS	(0x00)	Successful IP information retrieval.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Retrieve IP information from previously created IP
    Instance 0. */
status =  nx_ip_info_get(&ip_0,
                         &ip_total_packets_sent,
                         &ip_total_bytes_sent,
                         &ip_total_packets_received,
                         &ip_total_bytes_received,
                         &ip_invalid_packets,
                         &ip_receive_packets_dropped,
                         &ip_receive_checksum_errors,
                         &ip_send_packets_dropped,
                         &ip_total_fragments_sent,
                         &ip_total_fragments_received);

/* If status is NX_SUCCESS, IP information was retrieved.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_interface_address_get

Retrieve interface IP address

Prototype

```
UINT nx_ip_interface_address_get (NX_IP *ip_ptr,
                                  UINT   interface_index,
                                  ULONG *ip_address,
                                  ULONG *network_mask)
```

Description

This service retrieves the IPv4 address of a specified network interface. To retrieve IPv6 address, application shall use the service ***nxd_ipv6_address_get***

The specified device, if not the primary device, must be previously attached to the IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.
interface_index	Interface index, the same value as the index to the network interface attached to the IP instance.
ip_address	Pointer to destination for the device interface IP address.
network_mask	Pointer to destination for the device interface network mask.

Return Values

NX_SUCCESS	(0x00)	Successful IP address get.
NX_INVALID_INTERFACE	(0x4C)	Specified network interface is invalid.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define INTERFACE_INDEX 1
/*  Get device IP address and network mask for the specified
    interface index 1 in IP instance list of interfaces).  */
status =  nx_ip_interface_address_get(ip_ptr,INTERFACE_INDEX,
                                      &ip_address,
                                      &network_mask);

/*  If status is NX_SUCCESS the interface address was successfully
    retrieved. */
```

See Also

nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_get, nx_ip_interface_capability_set,
nx_ip_interface_detach, nx_ip_interface_info_get,
nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get,
nx_ip_interface_physical_address_set, nx_ip_interface_status_check,
nx_ip_link_status_change_notify_set

nx_ip_interface_address_mapping_configure

Configure whether address mapping is needed

Prototype

```
UINT nx_ip_interface_address_mapping_configure(NX_IP *ip_ptr,
                                                UINT  interface_index,
                                                UINT  mapping_needed)
```

Description

This service configures whether IP address to MAC address mapping is needed for the specified network interface. This service is typically called from the interface device driver to notify the IP stack whether the underlying interface requires IP address to layer two (MAC) address mapping.

Parameters

ip_ptr	IP control block pointer
interface_index	Index to the network interface
mapping_needed	NX_TRUE -- address mapping needed NX_FALSE -- address mapping not needed

Return Values

NX_SUCCESS	**(0x00)**	**Successful configure**
NX_INVALID_INTERFACE	(0x4C)	Device index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Thread

Preemption Possible

No

Example

```
#define      PRIMARY_INTERFACE 0
UCHAR        mapping_needed = NX_TRUE;

/* Configure address mapping needed specified interface. */
status = nx_ip_interface_address_mapping_configure(&ip_0,
                                                PRIMARY_INTERFACE,
                                                mapping_needed);

/* If status == NX_SUCCESS, the address mapping needed was
   successfully configured. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_set, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_address_set

Set interface IP address and network mask

Prototype

```
UINT nx_ip_interface_address_set(NX_IP *ip_ptr,
                                 UINT  interface_index,
                                 ULONG ip_address,
                                 ULONG network_mask)
```

Description

This service sets the IPv4 address and network mask for the specified IP interface. To configure IPv6 interface address, application shall use the service ***nxd_ipv6_address_set.***

The specified interface must be previously attached to the IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.
interface_index	Index of the interface attached to the NetX Duo instance.
ip_address	New network interface IP address.
network_mask	New interface network mask.

Return Values

NX_SUCCESS	(0x00)	Successful IP address set.
NX_INVALID_INTERFACE	(0x4C)	Specified network interface is invalid.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid pointers.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define INTERFACE_INDEX 1
/*  Set device IP address and network mask for the specified
    interface index 1 in IP instance list of interfaces).  */
status =  nx_ip_interface_address_set(ip_ptr, INTERFACE_INDEX,
                                      ip_address,
                                      network_mask);

/*  If status is NX_SUCCESS the interface IP address and mask was
    successfully set. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_attach

Attach network interface to IP instance

Prototype

```
UINT  nx_ip_interface_attach(NX_IP *ip_ptr, CHAR *inter-
                             face_name,          ULONG ip_address,
                             ULONG network_mask,
                             VOID(*ip_link_driver)
                                  (struct NX_IP_DRIVER_STRUCT *));
```

Description

This service adds a physical network interface to the IP interface. Note the IP instance is created with the primary interface so each additional interface is secondary to the primary interface. The total number of network interfaces attached to the IP instance (including the primary interface) cannot exceed **NX_MAX_PHYSICAL_INTERFACES**.

If the IP thread has not been running yet, the secondary interfaces will be initialized as part of the IP thread startup process that initializes all physical interfaces.

If the IP thread is not running yet, the secondary interface is initialized as part of the ***nx_ip_interface_attach*** service.

ip_ptr must point to a valid NetX Duo IP structure. ***NX_MAX_PHYSICAL_INTERFACES*** *must be configured for the number of network interfaces for the IP instance. The default value is one.*

Parameters

ip_ptr	Pointer to previously created IP instance.
interface_name	Pointer to interface name string.
ip_address	Device IP address in host byte order.
network_mask	Device network mask in host byte order.
ip_link_driver	Ethernet driver for the interface.

Return Values

NX_SUCCESS	(0x00)	Entry is added to static routing table.
NX_NO_MORE_ENTRIES	(0x17)	Max number of interfaces. NX_MAX_PHYSICAL_INTERFACES is exceeded. If IPv6 is enabled,

		this error may also indicate that the driver may not have enough resource to handle IPv6 multicast operations.
NX_DUPLICATED_ENTRY	(0x52)	The supplied IP address is already used on this IP instance.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid pointer input.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address input.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Attach secondary device for device IP address 192.168.1.68 with
    the specified Ethernet driver. */
status = nx_ip_interface_attach(ip_ptr, "secondary_port",
                                IP_ADDRESS(192,168,1,68),
                                0xFFFFFF00UL,
                                nx_etherDriver);

/*  If status is NX_SUCCESS the interface was successfully added to
    the IP instance interface table. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_address_set, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_capability_get

Get interface hardware capability

Prototype

```
UINT nx_ip_interface_capability_get(NX_IP *ip_ptr,
                                    UINT  interface_index,
                                    ULONG *interface_capability_flag)
```

Description

This service retrieves the capability flag from the specified network interface. To use this service, the NetX Duo library must be built with the option ***NX_ENABLE_INTERFACE_CAPABILITY*** enabled.

Parameters

ip_ptr	IP control block pointer
interface_index	Index of the network interface
interface_capability_flag	Pointer to memory space for the capability flag

Return Values

NX_SUCCESS	(0x00)	Successfully obtained interface capability information.
NX_NOT_SUPPORTED	(0x4B)	Interface capability feature is not supported in this build.
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer or Invalid capability flag pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
ULONG       capability_flag;

/* Get the hardware capability flag of specified interface. */
status = nx_ip_interface_capability_get(&ip_0,
                                        PRIMARY_INTERFACE,
                                        &capability_flag);

/* If status == NX_SUCCESS, the capability flag from the primary
   interface was successfully retrieved. */
```

See Also

nx_ip_interface_address_get,
nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_set, nx_ip_interface_detach,
nx_ip_interface_info_get, nx_ip_interface_mtu_set,
nx_ip_interface_physical_address_get,
nx_ip_interface_physical_address_set, nx_ip_interface_status_check,
nx_ip_link_status_change_notify_set

nx_ip_interface_capability_set

Set the hardware capability flag

Prototype

```
UINT nx_ip_interface_capability_set(NX_IP *ip_ptr,
                                    UINT   interface_index,
                                    ULONG  interface_capability_flag)
```

Description

This service is used by the network device driver to configure the capability flag for a specified network interface. To use this service, the NetX Duo library must be compiled with the option ***NX_ENABLE_INTERFACE_CAPABILITY*** defined.

Parameters

ip_ptr	IP control block pointer
interface_index	Index of network interface
interface_capability_flag	Capability flag for output

Return Values

NX_SUCCESS	(0x00)	Successfully set interface hardware capability flag.
NX_NOT_SUPPORTED	(0x4B)	Interface capability feature is not supported in this build.
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
ULONG capability_flag = \
                 NX_INTERFACE_CAPABILITY_IPV4_TX_CHECKSUM |\
                 NX_INTERFACE_CAPABILITY_IPV4_RX_CHECKSUM;
UINT device_index = 0;

/* Set the hardware capability flag of specified interface. */
status = nx_ip_interface_capability_set(&ip_0,
                                        PRIMARY_INTERFACE,
                                        capability_flag);

/* If status == NX_SUCCESS, the hardware capability flag was
   successfully set. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_address_set, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_detach

Detach the specified interface from the IP instance

Prototype

```
UINT nx_ip_interface_address_set(NX_IP *ip_ptr, UINT index)
```

Description

This service detaches the specified IP interface from the IP instance. Once an interface is detached, all connected TCP sockets closed, and ND cache and ARP entries for this interface are removed from their respective tables. IGMP memberships for this interface are removed.

Parameters

ip_ptr	Pointer to previously created IP instance.
index	Index of the interface to be removed.

Return Values

NX_SUCCESS	(0x00)	Successfully removed a physical interface.
NX_INVALID_INTERFACE	(0x4C)	Specified network interface is invalid.
NX_PTR_ERROR	(0x07)	Invalid pointers.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define INTERFACE_INDEX 1
/*  Detach interface 1. */
status = nx_ip_interface_detach(&IP_0, INTERFACE_INDEX);

/*  If status is NX_SUCCESS the interface is successfully detached
    from the IP instance. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_address_set, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_info_get

Retrieve network interface parameters

Prototype

```
UINT nx_ip_interface_info_get(NX_IP *ip_ptr,
                              UINT   interface_index,
                              CHAR **interface_name,
                              ULONG *ip_address,
                              ULONG *network_mask,
                              ULONG *mtu_size,
                              ULONG *physical_address_msw,
                              ULONG *physical_address_lsw);
```

Description

This service retrieves information on network parameters for the specified network interface. All data are retrieved in host byte order.

! *ip_ptr must point to a valid NetX Duo IP structure. The specified interface, if not the primary interface, must be previously attached to the IP instance.*

Parameters

ip_ptr	Pointer to previously created IP instance.
interface_index	Index specifying network interface.
interface_name	Pointer to the buffer that holds the name of the network interface.
ip_address	Pointer to the destination for the IP address of the interface.
network_mask	Pointer to destination for network mask.
mtu_size	Pointer to destination for maximum transfer unit for this interface.
physical_address_msw	Pointer to destination for top 16 bits of the device MAC address.
physical_address_lsw	Pointer to destination for lower 32 bits of the device MAC address.

Return Values

NX_SUCCESS	(0x00)	Interface information has been obtained.
NX_PTR_ERROR	(0x07)	Invalid pointer input.

NX_INVALID_INTERFACE	(0x4C)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Retrieve interface parameters for the specified interface (index
    1 in IP instance list of interfaces).  */
#define INTERFACE_INDEX 1
status =  nx_ip_interface_info_get(ip_ptr, INTERFACE_INDEX,
                                   &name_ptr, &ip_address,
                                   &network_mask,
                                   &mtu_size,
                                   &physical_address_msw,
                                   &physical_address_lsw);

/*  If status is NX_SUCCESS the interface information is
    successfully retrieved. */
```

See Also

nx_ip_interface_address_get,
nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_get, nx_ip_interface_capability_set,
nx_ip_interface_detach, nx_ip_interface_mtu_set,
nx_ip_interface_physical_address_get,
nx_ip_interface_physical_address_set, nx_ip_interface_status_check,
nx_ip_link_status_change_notify_set

nx_ip_interface_mtu_set

Set the MTU value of a network interface

Prototype

```
UINT nx_ip_interface_mtu_set(NX_IP *ip_ptr,
                             UINT interface_index,
                             ULONG mtu_size)
```

Description

This service is used by the device driver to configure the IP MTU value for the specified network interface.

Parameters

ip_ptr	IP control block pointer
interface_index	Index to the network interface
mtu_size	IP MTU size

Return Values

NX_SUCCESS	(0x00)	Successfully set MTU value
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
ULONG       mtu_size = 1500;

/* Set the MTU size of specified interface. */
status = nx_ip_interface_mtu_set(&ip_0,
                                 PRIMARY_INTERFACE, mtu_size);

/* If status == NX_SUCCESS, the MTU size was successfully set. */
```

See Also

nx_ip_interface_address_get,
nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_get, nx_ip_interface_capability_set,
nx_ip_interface_detach, nx_ip_interface_info_get, ,
nx_ip_interface_physical_address_get,
nx_ip_interface_physical_address_set, nx_ip_interface_status_check,
nx_ip_link_status_change_notify_set

nx_ip_interface_physical_address_get

Get the physical address of a network device

Prototype

```
UINT nx_ip_interface_physical_address_get(NX_IP *ip_ptr,
                                          UINT   interface_index,
                                          ULONG  *physical_msw,
                                          ULONG  *physical_lsw)
```

Description

This service retrieves the physical address of a network interface from the IP instance.

Parameters

ip_ptr	IP control block pointer
interface_index	Index of the network interface
physical_msw	Pointer to destination for top 16 bits of the device MAC address
physical_lsw	Pointer to destination for lower 32 bits of the device MAC address

Return Values

NX_SUCCESS	(0x00)	Successful get
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer or physical address pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
ULONG   physical_msw;
ULONG   physical_lsw;

/* Get the physical address of specified interface. */
status = nx_ip_interface_physical_address_get(&ip_0,
                                              PRIMARY_INTERFACE,
                                              &physical_msw,
                                              &physical_lsw);

/* If status == NX_SUCCESS, the physical address was successfully
   retrieved. */
```

See Also

nx_ip_interface_address_get,
nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_get, nx_ip_interface_capability_set,
nx_ip_interface_detach, nx_ip_interface_info_get,
nx_ip_interface_mtu_set, nx_ip_interface_physical_address_set,
nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_physical_address_set

Set the physical address for a specified network interface

Prototype

```
UINT nx_ip_interface_physical_address_set(NX_IP *ip_ptr,
                                          UINT   interface_index,
                                          ULONG  physical_msw,
                                          ULONG  physical_lsw,
                                          UINT   update_driver)
```

Description

This service is used by the application or a device driver to configure the physical address of the MAC address of the specified network interface. The new MAC address is applied to the control block of the interface structure. If the ***update_driver*** flag is set, a driver-level command is issued so the device driver is able to update its MAC address programmed into the Ethernet controller.

In a typical situation, this service is called from the interface device driver during initialization phase to notify the IP stack of its MAC address. In this case, the ***update_driver*** flag should not be set.

This routine can also be called from user application to reconfigure the interface MAC address at run time. In this use case, the ***update_driver*** flag should be set, so the new MAC address can be applied to the device driver.

Parameters

ip_ptr	IP control block pointer
interface_index	Index to the network interface
physical_msw	Pointer to destination for top 16 bits of the device MAC address
physical_lsw	Pointer to destination for lower 32 bits of the device MAC address

Return Values

NX_SUCCESS	(0x00)	Successful set
NX_UNHANDLED_COMMAND	(0x4B)	Command not recognized by the driver

NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
ULONG       physical_msw = 0x00CF;
ULONG       physical_lsw = 0x01020304;

/* Set the physical address of specified device. */
status = nx_ip_interface_physical_address_set(&ip_0,
                                              PRIMARY_INTERFACE,
                                              physical_msw,
                                              physical_lsw,
                                              NX_TRUE);

/* If status == NX_SUCCESS, the physical address was successfully
   set. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_address_set, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_status_check, nx_ip_link_status_change_notify_set

nx_ip_interface_status_check

Check status of an IP instance

Prototype

```
UINT nx_ip_interface_status_check(NX_IP *ip_ptr,
                                  UINT interface_index
                                  ULONG  needed_status,
                                  ULONG *actual_status,
                                  ULONG  wait_option);
```

Description

This service checks and optionally waits for the specified status of the network interface of a previously created IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.
interface_index	Interface index number
needed_status	IP status requested, defined in bit-map form as follows: NX_IP_INITIALIZE_DONE (0x0001) NX_IP_ADDRESS_RESOLVED(0x0002) NX_IP_LINK_ENABLED (0x0004) NX_IP_ARP_ENABLED (0x0008) NX_IP_UDP_ENABLED (0x0010) NX_IP_TCP_ENABLED (0x0020) NX_IP_IGMP_ENABLED (0x0040) NX_IP_RARP_COMPLETE(0x0080) NX_IP_INTERFACE_LINK_ENABLED (0x0100)
actual_status	Pointer to destination of actual bits set.
wait_option	Defines how the service behaves if the requested status bits are not available. The wait options are defined as follows: NX_NO_WAIT (0x00000000) timeout value (0x00000001 through 0xFFFFFFFE) NX_WAIT_FOREVER 0xFFFFFFFF

Return Values

NX_SUCCESS	(0x00)	Successful IP status check.
NX_NOT_SUCCESSFUL	(0x43)	Status request was not satisfied within the timeout specified.
NX_PTR_ERROR	(0x07)	IP pointer is or has become invalid, or actual status pointer is invalid.
NX_OPTION_ERROR	(0x0a)	Invalid needed status option.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_INVALID_INTERFACE	(0x4C)	Interface_index is out of range. or the interface is not valid.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Wait 10 ticks for the link up status on the previously created IP
    instance.   */
status = nx_ip_interface_status_check(&ip_0, 1, NX_IP_LINK_ENABLED,
                                      &actual_status, 10);

/*  If status is NX_SUCCESS, the secondary link for the specified IP
    instance is up.  */
```

See Also

nx_ip_interface_address_get,
nx_ip_interface_address_mapping_configure,
nx_ip_interface_address_set, nx_ip_interface_attach,
nx_ip_interface_capability_get, nx_ip_interface_capability_set,
nx_ip_interface_detach, nx_ip_interface_info_get,
nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get,
nx_ip_interface_physical_address_set,
nx_ip_link_status_change_notify_set

nx_ip_link_status_change_notify_set

Set the link status change notify callback function

Prototype

```
UINT nx_ip_link_status_change_notify_set(NX_IP *ip_ptr,
          VOID(*link_status_change_notify(NX_IP *ip_ptr,
                     UINT interface_index, UINT link_up))
```

Description

This service configures the link status change notify callback function. The user-supplied *link_status_change_notify* routine is invoked when either the primary or secondary interface status is changed (such as IP address is changed.) If *link_status_change_notify* is NULL, the link status change notify callback feature is disabled.

Parameters

ip_ptr	IP control block pointer
link_status_change_notify	User-supplied callback function to be called upon a change to the physical interface.

Return Values

NX_SUCCESS	(0x00)	Successful set
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer or new physical address pointer
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Configure a callback function to be used when the physical
   interface status is changed. */
status = nx_ip_link_status_change_notify_set(&ip_0,
                                              my_change_cb);

/* If status == NX_SUCCESS, the link status change notify function
   is set. */
```

See Also

nx_ip_interface_address_get, nx_ip_interface_address_mapping_configure, nx_ip_interface_address_set, nx_ip_interface_attach, nx_ip_interface_capability_get, nx_ip_interface_capability_set, nx_ip_interface_detach, nx_ip_interface_info_get, nx_ip_interface_mtu_set, nx_ip_interface_physical_address_get, nx_ip_interface_physical_address_set, nx_ip_interface_status_check

nx_ip_max_payload_size_find

Compute maximum packet data payload

Prototype

```
UINT nx_ip_max_payload_size_find(NX_IP *ip_ptr,
                                 NXD_ADDRESS *dest_address,
                                 UINT if_index,
                                 UINT src_port,
                                 UINT dest_port,
                                 ULONG protocol,
                                 ULONG *start_offset_ptr,
                                 ULONG *payload_length_ptr)
```

Description

This service finds the maximum application payload size that will not require IP fragmentation to reach the destination; e.g., payload is at or below the local interface MTU size. (or the Path MTU value obtained via IPv6 Path MTU discovery). IP header and upper application header size (TCP or UDP) are subtracted from the total payload. If NetX Duo IPsec Security Policy applies to this end-point, the IPsec headers (ESP/AH) and associated overhead, such as Initial Vector, are also subtracted from the MTU. This service is applicable for both IPv4 and IPv6 packets.

The parameter *if_index* specifies the interface to use for sending out the packet. For a multihome system, the caller needs to specify the *if_index* parameter if the destination is a broadcast (IPv4 only), multicast, or IPv6 link-local address.

This service returns two values to the caller:

(1) start_offset_ptr: This is the location after the TCP/UDP/IP/IPsec headers;

(2) payload_length_ptr: the amount of data application may transfer without exceeding MTU.

There is no equivalent NetX service.

Restrictions

The IP instance must be previously created.

Parameters

ip_ptr	Pointer to IP instance
dest_address	Pointer to packet destination address

if_index	Indicates the index of the interface to use
src_port	Source port number
dest_port	Destination port number
protocol	Upper layer protocol to be used
start_offset_ptr	Pointer to the start of data for maximum packet payload
payload_length_ptr	Pointer to payload size excluding headers

Return Values

NX_SUCCESS	(0x00)	Payload successfully computed
NX_INVALID_INTERFACE	(0x4C)	Interface index is invalid, or the interface is not valid.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_PTR_ERROR	(0x07)	Invalid IP pointer, or invalid destination address
NX_IP_ADDRESS_ERROR	(0x21)	Invalid address supplied
NX_NOT_SUPPORTED	(0x4B)	Invalid protocol (not UDP or TCP)
NX_CALLER_ERROR	(0x11)	Service is not called from system initialization or thread context.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  The following example determines the maximum payload for UDP
    packet to remote host. */
#define PRIMARY_INTERFACE 0
status = nx_ip_max_payload_size_find(&ip_0,
                                     &dest_ipv6_address,
                                     PRIMARY_INTERFACE,
                                     source_port,
                                     dest_port, NX_PROTOCOL_UDP,
                                     &start_offset,
                                     &payload_length);

/*  A return value of NX_SUCCESS indicates the packet payload
    payload_length starting at the offset start_offset is
    successfully computed. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ip_raw_packet_disable

Disable raw packet sending/receiving

Prototype

```
UINT nx_ip_raw_packet_disable(NX_IP *ip_ptr);
```

Description

This service disables transmission and reception of raw IP packets for this IP instance. If the raw packet service was previously enabled, and there are raw packets in the receive queue, this service will release any received raw packets.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP raw packet disable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Disable raw packet sending/receiving for this IP instance.  */
status = nx_ip_raw_packet_disable(&ip_0);

/*  If status is NX_SUCCESS, raw IP packet sending/receiving has
    been disabled for the previously created IP instance.  */
```

See Also

nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_packet_enable

Enable raw packet processing

Prototype

```
UINT nx_ip_raw_packet_enable(NX_IP *ip_ptr);
```

Description

This service enables transmission and reception of raw IP packets for this IP instance. Incoming TCP, UDP, ICMP, and IGMP packets are still processed by NetX Duo. Packets with unknown upper layer protocol types are processed by raw packet reception routine.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful IP raw packet enable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Enable raw packet sending/receiving for this IP instance.  */
status = nx_ip_raw_packet_enable(&ip_0);

/*  If status is NX_SUCCESS, raw IP packet sending/receiving has
    been enabled for the previously created IP instance.  */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_packet_filter_set

Set raw IP packet filter

Prototype

```
UINT nx_ip_raw_packet_filter_set(NX_IP *ip_ptr,
                                 UINT (*raw_packet_filter)
                                      (NX_IP *, ULONG,
                                       NX_PACKET *))
```

Description

This service configures the IP raw packet filter. The raw packet filter function, implemented by user application, allows an application to receive raw packets based on user-supplied criteria. Note that NetX Duo BSD wrapper layer uses the raw packet filter feature to handle raw socket in the BSD layer. To use this service, the NetX Duo library must be built with the option ***NX_ENABLE_IP_RAW_PACKET_FILTER*** defined.

Parameters

ip_ptr	IP control block pointer
raw_packet_filter	Function pointer of the raw packet filter

Return Values

NX_SUCCESS	(0x00)	Successfully set the raw packet filter routine
NX_NOT_SUPPORT	(0x4B)	Raw packet support is not available
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
UINT raw_packet_filter(NX_IP *ip_ptr, ULONG protocol,
                       NX_PACKET *packet_ptr)
{

    /* Simply filter protocol. */
    if(protocol == NX_IP_RAW)
       return NX_SUCCESS;
    else
       return NX_NOT_SUCCESSFUL;
}

void raw_packet_thread_entry(ULONG id)
{

    /* Set the raw packet filter of IP instance. */
    status = nx_ip_raw_packet_filter_set(&ip_0,
                                         raw_packet_filter);

    /* If status == NX_SUCCESS, the raw packet filter of IP instance
       was successfully set. */
}
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_packet_receive

Receive raw IP packet

Prototype

```
UINT nx_ip_raw_packet_receive(NX_IP *ip_ptr,
                              NX_PACKET **packet_ptr,
                              ULONG wait_option);
```

Description

This service receives a raw IP packet from the specified IP instance. If there are IP packets on the raw packet receive queue, the first (oldest) packet is returned to the caller. Otherwise, if no packets are available, the caller may suspend as specified by the wait option.

If NX_SUCCESS, is returned, the application is responsible for releasing the received packet when it is no longer needed.

Parameters

ip_ptr	Pointer to previously created IP instance.
packet_ptr	Pointer to pointer to place the received raw IP packet in.
wait_option	Defines how the service behaves if packets are not available. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful IP raw packet receive.
NX_NO_PACKET	(0x01)	No packet was available.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.

NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_PTR_ERROR	(0x07)	Invalid IP or return packet pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Receive a raw IP packet for this IP instance, wait for a maximum
    of 4 timer ticks.  */
status = nx_ip_raw_packet_receive(&ip_0, &packet_ptr, 4);

/*  If status is NX_SUCCESS, the raw IP packet pointer is in the
    variable packet_ptr.  */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_packet_send

Send raw IP packet

Prototype

```
UINT nx_ip_raw_packet_send(NX_IP *ip_ptr,
                           NX_PACKET *packet_ptr,
                           ULONG destination_ip,
                           ULONG type_of_service);
```

Description

This service sends a raw IPv4 packet to the destination IP address. Note that this routine returns immediately, and it is therefore not known whether the IP packet has actually been sent. The network driver will be responsible for releasing the packet when the transmission is complete.

For a multihome system, NetX Duo uses the destination IP address to find an appropriate network interface and uses the IP address of the interface as the source address. If the destination IP address is broadcast or multicast, the first valid interface is used. Applications use the ***nx_ip_raw_packet_source_send*** in this case.

To send a raw IPv6 packet, application shall use the service ***nxd_ip_raw_packet_send,*** or ***nxd_ip_raw_packet_source_send.***

Unless an error is returned, the application should not release the packet after this call. Doing so will cause unpredictable results because the network driver will release the packet after transmission.

Parameters

ip_ptr	Pointer to previously created IP instance.
packet_ptr	Pointer to the raw IP packet to send.
destination_ip	Destination IP address, which can be a specific host IP address, a network broadcast, an internal loop-back, or a multicast address.
type_of_service	Defines the type of service for the transmission, legal values are as follows: NX_IP_NORMAL (0x00000000) NX_IP_MIN_DELAY (0x00100000) NX_IP_MAX_DATA (0x00080000)

NX_IP_MAX_RELIABLE	(0x00040000)
NX_IP_MIN_COST	(0x00020000)

Return Values

NX_SUCCESS	(0x00)	Successful IP raw packet send initiated.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_NOT_ENABLED	(0x14)	Raw IP feature is not enabled.
NX_OPTION_ERROR	(0x0A)	Invalid type of service.
NX_UNDERFLOW	(0x02)	Not enough room to prepend an IP header on the packet.
NX_OVERFLOW	(0x03)	Packet append pointer is invalid.
NX_PTR_ERROR	(0x07)	Invalid IP or packet pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Send a raw IP packet to IP address 1.2.3.5.  */
status = nx_ip_raw_packet_send(&ip_0, packet_ptr,
                               IP_ADDRESS(1,2,3,5),
                               NX_IP_NORMAL);

/*  If status is NX_SUCCESS, the raw IP packet pointed to by
    packet_ptr has been sent.  */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_packet_source_send

Send raw IP packet through specified network interface

Prototype

```
UINT  nx_ip_raw_packet_source_send(NX_IP *ip_ptr,
                                   NX_PACKET *pack-
                                   et_ptr,
                                   ULONG     destination_ip,
                                   UINT      address_index,
                                   ULONG     type_of_service);
```

Description

This service sends a raw IP packet to the destination IP address using the specified local IPv4 address as the source address, and through the associated network interface. Note that this routine returns immediately, and it is, therefore, not known if the IP packet has actually been sent. The network driver will be responsible for releasing the packet when the transmission is complete. This service differs from other services in that there is no way of knowing if the packet was actually sent. It could get lost on the Internet.

! *Note that raw IP processing must be enabled.*

! *This service is similar to **nx_ip_raw_packet_send,** except that this service allows an application to send raw IPv4 packet from a specified physical interfaces.*

Parameters

ip_ptr	Pointer to previously created IP task.
packet_ptr	Pointer to packet to transmit.
destination_ip	IP address to send packet.
address_index	Index of the address of the interface to send packet out on.
type_of_service	Type of service for packet.

Return Values

NX_SUCCESS	(0x00)	Packet successfully transmitted.
NX_IP_ADDRESS_ERROR	(0x21)	No suitable outgoing interface available.
NX_NOT_ENABLED	(0x14)	Raw IP packet processing not enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid pointer input.
NX_OPTION_ERROR	(0x0A)	Invalid type of service specified.
NX_OVERFLOW	(0x03)	Invalid packet prepend pointer.
NX_UNDERFLOW	(0x02)	Invalid packet prepend pointer.
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index specified.

Allowed From

Threads

Preemption Possible

No

Example

```
#define ADDRESS_IDNEX 1
/*  Send packet out on interface 1 with normal type of service.  */
status = nx_ip_raw_packet_source_send(ip_ptr, packet_ptr,
                                      destination_ip,
                                      ADDRESS_INDEX,
                                      NX_IP_NORMAL);

/*  If status is NX_SUCCESS the packet was successfully
    transmitted. */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_raw_receive_queue_max_set

Set maximum raw receive queue size

Prototype

```
UINT nx_ip_raw_receive_queue_max_set(NX_IP *ip_ptr, ULONG queue_-
                                     max)
```

Description

This service configures the maximum depth of the IP raw packet receive queue. Note that the IP raw packet receive queue is shared with both IPv4 and IPv6 packets. When the raw packet receive queue reaches the user-configured maximum depth, newly received raw packets are dropped. The default IP raw packet receive queue depth is 20.

Parameters

ip_ptr	IP control block pointer
queue_max	New value for the queue size

Return Values

NX_SUCCESS	(0x00)	Successfully set raw receive queue maximum depth
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization and threads

Preemption Possible

No

Example

```
ULONG queue_max = 10;

/* Set the maximum size of the IP raw packet receive queue. */
status = nx_ip_raw_receive_queue_max_set (&ip_0,
                                          queue_max);

/* If status == NX_SUCCESS, the maximum size of the IP raw packet
   receive queue was successfully set. */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nxd_ip_raw_packet_send, nxd_ip_raw_packet_source_send

nx_ip_static_route_add

Add static route to the routing table

Prototype

```
UINT nx_ip_static_route_add(NX_IP *ip_ptr,
                            ULONG network_address,
                            ULONG net_mask,
                            ULONG next_hop);
```

Description

This service adds an entry to the static routing table. Note that the *next_hop* address must be directly accessible from one of the local network devices.

Note that ip_ptr must point to a valid NetX Duo IP structure and the NetX Duo library must be built with NX_ENABLE_IP_STATIC_ROUTING defined to use this service. By default NetX Duo is built without NX_ENABLE_IP_STATIC_ROUTING defined.

Parameters

ip_ptr	Pointer to previously created IP instance.
network_address	Target network address, in host byte order
net_mask	Target network mask, in host byte order
next_hop	Next hop address for the target network, in host byte order

Return Values

NX_SUCCESS	(0x00)	Entry is added to the static routing table.
NX_OVERFLOW	(0x03)	Static routing table is full.
NX_NOT_SUPPORTED	(0x4B)	This feature is not compiled in.
NX_IP_ADDRESS_ERROR	(0x21)	Next hop is not directly accessible via local interfaces.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid *ip_ptr* pointer.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Specify the next hop for 192.168.1.68 through the gateway
    192.168.1.1.  */
status =  nx_ip_static_route_add(ip_ptr, IP_ADDRESS(192,168,1,0),
                                   0xFFFFFF00UL,
                                   IP_ADDRESS(192,168,1,1));

/* If status is NX_SUCCESS the route was successfully added to the
    static routing table.  */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nx_ip_static_route_delete

Delete static route from routing table

Prototype

```
UINT nx_ip_static_route_delete(NX_IP *ip_ptr,
                               ULONG network_address,
                               ULONG net_mask);
```

Description

This service deletes an entry from the static routing table.

Note that ip_ptr must point to a valid NetX Duo IP structure and the NetX Duo library must be built with NX_ENABLE_IP_STATIC_ROUTING defined to use this service. By default NetX Duo is built without NX_ENABLE_IP_STATIC_ROUTING defined.

Parameters

ip_ptr	Pointer to previously created IP instance.
network_address	Target network address, in host byte order.
net_mask	Target network mask, in host byte order.

Return Values

NX_SUCCESS	(0x00)	Successful deletion from the static routing table.
NX_NOT_SUCCESSFUL	(0x43)	Entry cannot be found in the routing table.
NX_NOT_SUPPORTED	(0x4B)	This feature is not compiled in.
NX_PTR_ERROR	(0x07)	Invalid *ip_ptr* pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Remove the static route for 192.168.1.68 from the routing
    table.*/
status =  nx_ip_static_route_delete(ip_ptr,
                                    IP_ADDRESS(192,168,1,0),
                                    0xFFFFFF00UL,);

/*  If status is NX_SUCCESS the route was successfully removed from
    the static routing table.  */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nx_ip_status_check

Check status of an IP instance

Prototype

```
UINT nx_ip_status_check(NX_IP *ip_ptr,
                        ULONG  needed_status,
                        ULONG *actual_status,
                        ULONG  wait_option);
```

Description

This service checks and optionally waits for the specified status of the primary network interface of a previously created IP instance. To obtain status on secondary interfaces, applications shall use the service ***nx_ip_interface_status_check.***

Parameters

ip_ptr	Pointer to previously created IP instance.
needed_status	IP status requested, defined in bit-map form as follows: NX_IP_INITIALIZE_DONE (0x0001) NX_IP_ADDRESS_RESOLVED(0x0002) NX_IP_LINK_ENABLED (0x0004) NX_IP_ARP_ENABLED (0x0008) NX_IP_UDP_ENABLED (0x0010) NX_IP_TCP_ENABLED (0x0020) NX_IP_IGMP_ENABLED (0x0040) NX_IP_RARP_COMPLETE(0x0080) NX_IP_INTERFACE_LINK_ENABLED (0x0100)
actual_status	Pointer to destination of actual bits set.
wait_option	Defines how the service behaves if the requested status bits are not available. The wait options are defined as follows: NX_NO_WAIT 0x00000000) timeout value in ticks (0x00000001 through 0xFFFFFFFE) NX_WAIT_FOREVER 0xFFFFFFFF

Return Values

NX_SUCCESS	(0x00)	Successful IP status check.
NX_NOT_SUCCESSFUL	(0x43)	Status request was not satisfied within the timeout specified.
NX_PTR_ERROR	(0x07)	IP pointer is or has become invalid, or actual status pointer is invalid.
NX_OPTION_ERROR	(0x0a)	Invalid needed status option.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Wait 10 ticks for the link up status on the previously created IP
    instance.   */
status = nx_ip_status_check(&ip_0, NX_IP_LINK_ENABLED,
                            &actual_status, 10);

/*  If status is NX_SUCCESS, the link for the specified IP instance
    is up.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_ipv4_multicast_interface_join

Join IP instance to specified multicast group via an interface

Prototype

```
UINT nx_ipv4_multicast_interface_join(NX_IP *ip_ptr,
                                      ULONG group_address,
                                      UINT  interface_index)
```

Description

This service joins an IP instance to the specified multicast group via a specified network interface. Once the IP instance joins a multicast group, the IP receive logic starts to forward data packets from the give multicast group to the upper layer. Note that this service joins a multicast group without sending IGMP reports.

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Class D IP multicast group address to join in host byte order.
interface_index	Index of the Interface attached to the NetX Duo instance.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_NO_MORE_ENTRIES	(0x17)	No more multicast groups can be joined, maximum exceeded.
NX_PTR_ERROR	(0x07)	Invalid pointer to IP instance, or the IP instance is invalid
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_EANABLED	(0x14)	IGMP is not enabled in this IP instance
NX_IP_ADDRESS_ERROR	(0x21)	Multicast group address provided is not a valid class D address.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Previously created IP Instance joins the multicast group
    224.0.0.200, via the interface at index 1 in the IP interface
    list.   */
#define INTERFACE_INDEX 1
status = nx_ipv4_multicast_interface_join
                                  (&ip IP_ADDRESS(224,0,0,200),
                                   INTERFACE_INDEX);

/*  If status is NX_SUCCESS, the IP instance has successfully joined
    the multicast group. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_ipv4_multicast_interface_leave

Leave specified multicast group via an interface

Prototype

```
UINT nx_ipv4_multicast_interface_leave(NX_IP *ip_ptr,
                                       ULONG group_address,
                                       UINT  interface_index)
```

Description

This service leaves the specified multicast group via a specified network interface. After leaving the group, this service does not trigger IGMP messages being generated.

Parameters

ip_ptr	Pointer to previously created IP instance.
group_address	Class D IP multicast group address to leave. The IP address is in host byte order.
interface_index	Index of the Interface attached to the NetX Duo instance.

Return Values

NX_SUCCESS	(0x00)	Successful multicast group join.
NX_ENTRY_NOT_FOUND	(0x16)	The specified multicast group address cannot be found in the local multicast table.
NX_INVALID_INTERFACE	(0x4C)	Device index points to an invalid network interface.
NX_IP_ADDRESS_ERROR	(0x21)	Multicast group address provided is not a valid class D address.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid pointer to IP instance, or the IP instance is invalid

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Leave the multicast group 224.0.0.200. */
#define INTERFACE_INDEX 1
status = nx_ipv4_multicast_interface_leave
                                  (&ip, IP_ADDRESS(224,0,0,200),
                                   INTERFACE_INDEX);

/*  If status is NX_SUCCESS, the IP instance has successfully leaves
    the multicast group 244.0.0.200. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nxd_ipv6_multicast_interface_join, nxd_ipv6_multicast_interface_leave

nx_packet_allocate

Allocate packet from specified pool

Prototype

```
UINT nx_packet_allocate(NX_PACKET_POOL *pool_ptr,
                        NX_PACKET **packet_ptr,
                        ULONG packet_type,
                        ULONG wait_option);
```

Description

This service allocates a packet from the specified pool and adjusts the prepend pointer in the packet according to the type of packet specified. If no packet is available, the service suspends according to the supplied wait option.

Parameters

pool_ptr	Pointer to previously created packet pool.
packet_ptr	Pointer to the pointer of the allocated packet pointer.
packet_type	Defines the type of packet requested. See "Packet Pools" on page 63 in Chapter 3 for a list of supported packet types.
wait_option	Defines the wait time in ticks if there are no packets available in the packet pool. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful packet allocate.
NX_NO_PACKET	(0x01)	No packet available.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_INVALID_PARAMETERS	(0x4D)	Packet size cannot support protocol.
NX_OPTION_ERROR	(0x0A)	Invalid packet type.
NX_PTR_ERROR	(0x07)	Invalid pool or packet return pointer.
NX_CALLER_ERROR	(0x11)	Invalid wait option from non-thread.

Allowed From

Initialization, threads, timers, and ISRs (application network drivers). Wait option must be *NX_NO_WAIT* when used in ISR or in timer context.

Preemption Possible

No

Example

```
/*  Allocate a new UDP packet from the previously created packet
    pool and suspend for a maximum of 5 timer ticks if the pool is
    empty. */
status = nx_packet_allocate(&pool_0, &packet_ptr,
                            NX_UDP_PACKET, 5);

/*  If status is NX_SUCCESS, the newly allocated packet pointer is
    found in the variable packet_ptr.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_copy

Copy packet

Prototype

```
UINT  nx_packet_copy(NX_PACKET *packet_ptr,
                     NX_PACKET **new_packet_ptr,
                     NX_PACKET_POOL *pool_ptr,
                     ULONG wait_option);
```

Description

This service copies the information in the supplied packet to one or more new packets that are allocated from the supplied packet pool. If successful, the pointer to the new packet is returned in destination pointed to by **new_packet_ptr**.

Parameters

packet_ptr	Pointer to the source packet.
new_packet_ptr	Pointer to the destination of where to return the pointer to the new copy of the packet.
pool_ptr	Pointer to the previously created packet pool that is used to allocate one or more packets for the copy.
wait_option	Defines how the service waits if there are no packets available. The wait options are defined as follows:

NX_NO_WAIT	(0x00000000)
NX_WAIT_FOREVER	(0xFFFFFFFF)
timeout value in ticks	(0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful packet copy.
NX_NO_PACKET	(0x01)	Packet not available for copy.
NX_INVALID_PACKET	(0x12)	Empty source packet or copy failed.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to tx_thread_wait_abort.

NX_INVALID_PARAMETERS	(0x4D)	Packet size cannot support protocol.
NX_PTR_ERROR	(0x07)	Invalid pool, packet, or destination pointer.
NX_UNDERFLOW	(0x02)	Invalid packet prepend pointer.
NX_OVERFLOW	(0x03)	Invalid packet append pointer.
NX_CALLER_ERROR	(0x11)	A wait option was specified in initialization or in an ISR.

Allowed From

Initialization, threads, timers, and ISRs

Preemption Possible

No

Example

```
NX_PACKET *new_copy_ptr;

/* Copy packet pointed to by "old_packet_ptr" using packets from
   previously created packet pool_0. */
status = nx_packet_copy(old_packet, &new_copy_ptr, &pool_0, 20);

/* If status is NX_SUCCESS, new_copy_ptr points to the packet copy.
   */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_data_append

Append data to end of packet

Prototype

```
UINT nx_packet_data_append(NX_PACKET *packet_ptr,
                           VOID *data_start, ULONG data_size,
                           NX_PACKET_POOL *pool_ptr,
                           ULONG wait_option);
```

Description

This service appends data to the end of the specified packet. The supplied data area is copied into the packet. If there is not enough memory available, and the chained packet feature is enabled, one or more packets will be allocated to satisfy the request. If the chained packet feature is not enabled, *NX_SIZE_ERROR* is returned.

Parameters

packet_ptr	Packet pointer.
data_start	Pointer to the start of the user's data area to append to the packet.
data_size	Size of user's data area.
pool_ptr	Pointer to packet pool from which to allocate another packet if there is not enough room in the current packet.
wait_option	Defines how the service behaves if there are no packets available. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful packet append.
NX_NO_PACKET	(0x01)	No packet available.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.

NX_INVALID_PARAMETERS		
	(0x4D)	Packet size cannot support protocol.
NX_UNDERFLOW	(0x02)	Prepend pointer is less than payload start.
NX_OVERFLOW	(0x03)	Append pointer is greater than payload end.
NX_PTR_ERROR	(0x07)	Invalid pool, packet, or data Pointer.
NX_SIZE_ERROR	(0x09)	Invalid data size.
NX_CALLER_ERROR	(0x11)	Invalid wait option from non-thread.

Allowed From

Initialization, threads, timers, and ISRs (application network drivers)

Preemption Possible

No

Example

```
/*  Append "abcd" to the specified packet.  */
status = nx_packet_data_append(packet_ptr, "abcd", 4, &pool_0, 5);

/*  If status is NX_SUCCESS, the additional four bytes "abcd" have
    been appended to the packet.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_data_extract_offset

Extract data from packet via an offset

Prototype

```
UINT nx_packet_data_extract_offset(NX_PACKET *packet_ptr,
                                   ULONG offset,
                                   VOID *buffer_start,
                                   ULONG buffer_length,
                                   ULONG *bytes_copied);
```

Description

This service copies data from a NetX Duo packet (or packet chain) starting at the specified offset from the packet prepend pointer of the specified size in bytes into the specified buffer. The number of bytes actually copied is returned in *bytes_copied.* This service does not remove data from the packet, nor does it adjust the prepend pointer or other internal state information.

Parameters

packet_ptr	Pointer to packet to extract
offset	Offset from the current prepend pointer.
buffer_start	Pointer to start of save buffer
buffer_length	Number of bytes to copy
bytes_copied	Number of bytes actually copied

Return Values

NX_SUCCESS	(0x00)	Successful packet copy
NX_PACKET_OFFSET_ERROR	(0x53)	Invalid offset value was supplied
NX_PTR_ERROR	(0x07)	Invalid packet pointer or buffer pointer

Allowed From

Initialization, threads, timers, and ISRs

Preemption Possible

No

Example

```
/*  Extract 10 bytes from the start of the received packet buffer
    into the specified memory area. */
status = nx_packet_data_extract_offset(my_packet, 0, &data[0], 10,
                                        &bytes_copied) ;

/*  If status is NX_SUCCESS, 10 bytes were successfully copied into
    the data buffer. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_data_retrieve

Retrieve data from packet

Prototype

```
UINT  nx_packet_data_retrieve(NX_PACKET *packet_ptr,
                              VOID *buffer_start,
                              ULONG *bytes_copied);
```

Description

This service copies data from the supplied packet into the supplied buffer. The actual number of bytes copied is returned in the destination pointed to by **bytes_copied**.

Note that this service does not change internal state of the packet. The data being retrieved is still available in the packet.

! *The destination buffer must be large enough to hold the packet's contents. If not, memory will be corrupted causing unpredictable results.*

Parameters

packet_ptr	Pointer to the source packet.
buffer_start	Pointer to the start of the buffer area.
bytes_copied	Pointer to the destination for the number of bytes copied.

Return Values

NX_SUCCESS	(0x00)	Successful packet data retrieve.
NX_INVALID_PACKET	(0x12)	Invalid packet.
NX_PTR_ERROR	(0x07)	Invalid packet, buffer start, or bytes copied pointer.

Allowed From

Initialization, threads, timers, and ISRs

Preemption Possible

No

Example

```
UCHAR                   buffer[512];
ULONG                   bytes_copied;

/*  Retrieve data from packet pointed to by "packet_ptr". */
status = nx_packet_data_retrieve(packet_ptr, buffer,
    &bytes_copied);

/*  If status is NX_SUCCESS, buffer contains the contents of the
    packet, the size of which is contained in "bytes_copied." */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_length_get

Get length of packet data

Prototype

```
UINT nx_packet_length_get (NX_PACKET *packet_ptr, ULONG *length);
```

Description

This service gets the length of the data in the specified packet.

Parameters

packet_ptr	Pointer to the packet.
length	Destination for the packet length.

Return Values

NX_SUCCESS	(0x00)	Successful packet length get.
NX_PTR_ERROR	(0x07)	Invalid packet pointer.

Allowed From

Initialization, threads, timers, and ISRs

Preemption Possible

No

Example

```
/*  Get the length of the data in "my_packet." */
status = nx_packet_length_get(my_packet, &my_length);

/*  If status is NX_SUCCESS, data length is in "my_length". */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_pool_create

Create packet pool in specified memory area

Prototype

```
UINT nx_packet_pool_create(NX_PACKET_POOL *pool_ptr,
                           CHAR *name,
                           ULONG payload_size,
                           VOID *memory_ptr,
                           ULONG memory_size);
```

Description

This service creates a packet pool of the specified packet size in the memory area supplied by the user.

Parameters

pool_ptr	Pointer to packet pool control block.
name	Pointer to application's name for the packet pool.
payload_size	Number of bytes in each packet in the pool. This value must be at least 40 bytes and must also be evenly divisible by 4.
memory_ptr	Pointer to the memory area to place the packet pool in. The pointer should be aligned on an ULONG boundary.
memory_size	Size of the pool memory area.

Return Values

NX_SUCCESS	(0x00)	Successful packet pool create.
NX_PTR_ERROR	(0x07)	Invalid pool or memory pointer.
NX_SIZE_ERROR	(0x09)	Invalid block or memory size.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Create a packet pool of 32000 bytes starting at physical
    address 0x10000000.  */
status = nx_packet_pool_create(&pool_0, "Default Pool", 128,
                               (void *) 0x10000000, 32000);

/*  If status is NX_SUCCESS, the packet pool has been successfully
    created.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_pool_delete

Delete previously created packet pool

Prototype

```
UINT NX_PACKET_POOL *pool_ptr);
```

Description

This service deletes a previously created packet pool. NetX Duo checks for any threads currently suspended on packets in the packet pool and clears the suspension.

Parameters

pool_ptr	Packet pool control block pointer.

Return Values

NX_SUCCESS	(0x00)	Successful packet pool delete.
NX_PTR_ERROR	(0x07)	Invalid pool pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

Yes

Example

```
/*  Delete a previously created packet pool.  */
status = nx_packet_pool_delete(&pool_0);

/*  If status is NX_SUCCESS, the packet pool has been successfully
    deleted. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_pool_info_get

Retrieve information about a packet pool

Prototype

```
UINT nx_packet_pool_info_get(NX_PACKET_POOL *pool_ptr,
                             ULONG *total_packets,
                             ULONG *free_packets,
                             ULONG *empty_pool_requests,
                             ULONG *empty_pool_suspensions,
                             ULONG *invalid_packet_releases);
```

Description

This service retrieves information about the specified packet pool.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

pool_ptr	Pointer to previously created packet pool.
total_packets	Pointer to destination for the total number of packets in the pool.
free_packets	Pointer to destination for the total number of currently free packets.
empty_pool_requests	Pointer to destination of the total number of allocation requests when the pool was empty.
empty_pool_suspensions	Pointer to destination of the total number of empty pool suspensions.
invalid_packet_releases	Pointer to destination of the total number of invalid packet releases.

Return Values

NX_SUCCESS	(0x00)	Successful packet pool information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads, and timers

Preemption Possible

No

Example

```
/*  Retrieve packet pool information.  */
status = nx_packet_pool_info_get(&pool_0,
                                 &total_packets,
                                 &free_packets,
                                 &empty_pool_requests,
                                 &empty_pool_suspensions,
                                 &invalid_packet_releases);

/*  If status is NX_SUCCESS, packet pool information was
    retrieved. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_low_watermark_set, nx_packet_release, nx_packet_transmit_release

nx_packet_pool_low_watermark_set

Set packet pool low watermark

Prototype

```
UINT nx_packet_pool_low_watermark_set(NX_PACKET_POOL *pool_ptr,
                                      ULONG low_watermark);
```

Description

This service configures the low watermark for the specified packet pool. Once the low watermark value is set, TCP or UDP will not queue up the received packets if the number of available packets in the packet pool is less than the packet pool's low watermark, preventing the packet pool from being starved of packets. This service is available if the NetX Duo library is built with the option ***NX_ENABLE_LOW_WATERMARK*** defined.

Parameters

pool_ptr	Pointer to packet pool control block.
low_watermark	Low watermark value to be configured

Return Values

NX_SUCCESS	(0x00)	Successfully set the low watermark value.
NX_NOT_SUPPORTED	(0x4B)	The low watermark feature is not built into NetX Duo.
NX_PTR_ERROR	(0x07)	Invalid pool pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Set pool_0 low watermark value to 2.  */
status = nx_packet_pool_create(&pool_0, 2);

/*  If status is NX_SUCCESS, the low watermark value is set for
    pool_0.*/
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_release, nx_packet_transmit_release

nx_packet_release

Release previously allocated packet

Prototype

```
UINT nx_packet_release(NX_PACKET *packet_ptr);
```

Description

This service releases a packet, including any additional packets chained to the specified packet. If another thread is blocked on packet allocation, it is given the packet and resumed.

The application must prevent releasing a packet more than once, because doing so will cause unpredictable results.

Parameters

packet_ptr	Packet pointer.

Return Values

NX_SUCCESS	(0x00)	Successful packet release.
NX_PTR_ERROR	(0x07)	Invalid packet pointer.
NX_UNDERFLOW	(0x02)	Prepend pointer is less than payload start.
NX_OVERFLOW	(0x03)	Append pointer is greater than payload end.

Allowed From

Initialization, threads, timers, and ISRs (application network drivers)

Preemption Possible

Yes

Example

```
/*  Release a previously allocated packet.  */
status = nx_packet_release(packet_ptr);

/*  If status is NX_SUCCESS, the packet has been returned to the
    packet pool it was allocated from.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_transmit_release

nx_packet_transmit_release

Release a transmitted packet

Prototype

```
UINT nx_packet_transmit_release(NX_PACKET *packet_ptr);
```

Description

For non-TCP packets, this service releases a transmitted packet, including any additional packets chained to the specified packet. If another thread is blocked on packet allocation, it is given the packet and resumed. For a transmitted TCP packet, the packet is marked as being transmitted but not released till the packet is acknowledged. This service is typically called from the application's network driver after a packet is transmitted.

The network driver should remove the physical media header and adjust the length of the packet before calling this service.

Parameters

packet_ptr	Packet pointer.

Return Values

NX_SUCCESS	(0x00)	Successful transmit packet release.
NX_PTR_ERROR	(0x07)	Invalid packet pointer.
NX_UNDERFLOW	(0x02)	Prepend pointer is less than payload start.
NX_OVERFLOW	(0x03)	Append pointer is greater than payload end.

Allowed From

Initialization, threads, timers, Application network drivers (including ISRs)

Preemption Possible

Yes

Example

```
/*  Release a previously allocated packet that was just transmitted
    from the application network driver.  */
status = nx_packet_transmit_release(packet_ptr);

/*  If status is NX_SUCCESS, the transmitted packet has been
    returned to the packet pool it was allocated from.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_packet_allocate, nx_packet_copy, nx_packet_data_append, nx_packet_data_extract_offset, nx_packet_data_retrieve, nx_packet_length_get, nx_packet_pool_create, nx_packet_pool_delete, nx_packet_pool_info_get, nx_packet_pool_low_watermark_set, nx_packet_release

nx_rarp_disable

Disable Reverse Address Resolution Protocol (RARP)

Prototype

```
UINT nx_rarp_disable(NX_IP *ip_ptr);
```

Description

This service disables the RARP component of NetX Duo for the specific IP instance. For a multihome system, this service disables RARP on all interfaces.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful RARP disable.
NX_NOT_ENABLED	(0x14)	RARP was not enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Disable RARP on the previously created IP instance.  */
status = nx_rarp_disable(&ip_0);

/*  If status is NX_SUCCESS, RARP is disabled.  */
```

See Also

nx_rarp_enable, nx_rarp_info_get

nx_rarp_enable

Enable Reverse Address Resolution Protocol (RARP)

Prototype

```
UINT nx_rarp_enable(NX_IP *ip_ptr);
```

Description

This service enables the RARP component of NetX Duo for the specific IP instance. The RARP components searches through all attached network interfaces for zero IP address. A zero IP address indicates the interface does not have IP address assignment yet. RARP attempts to resolve the IP address by enabling RARP process on that interface.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful RARP enable.
NX_IP_ADDRESS_ERROR	(0x21)	IP address is already valid.
NX_ALREADY_ENABLED	(0x15)	RARP was already enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads, timers

Preemption Possible

No

Example

```
/*  Enable RARP on the previously created IP instance.  */
status = nx_rarp_enable(&ip_0);

/*  If status is NX_SUCCESS, RARP is enabled and is attempting to
    resolve this IP instance's address by querying the network.  */
```

See Also

nx_rarp_disable, nx_rarp_info_get

nx_rarp_info_get

Retrieve information about RARP activities

Prototype

```
UINT nx_rarp_info_get(NX_IP *ip_ptr,
                      ULONG *rarp_requests_sent,
                      ULONG *rarp_responses_received,
                      ULONG *rarp_invalid_messages);
```

Description

This service retrieves information about RARP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
rarp_requests_sent	Pointer to destination for the total number of RARP requests sent.
rarp_responses_received	Pointer to destination for the total number of RARP responses received.
rarp_invalid_messages	Pointer to destination of the total number of invalid messages.

Return Values

NX_SUCCESS	(0x00)	Successful RARP information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Retrieve RARP information from previously created IP
    Instance 0. */
status =  nx_rarp_info_get(&ip_0,
                             &rarp_requests_sent,
                             &rarp_responses_received,
                             &rarp_invalid_messages);

/*  If status is NX_SUCCESS, RARP information was retrieved.  */
```

See Also

nx_rarp_disable, nx_rarp_enable

nx_system_initialize

Initialize NetX Duo System

Prototype

```
VOID nx_system_initialize(VOID);
```

Description

This service initializes the basic NetX Duo system resources in preparation for use. It should be called by the application during initialization and before any other NetX Duo call are made.

Parameters

None

Return Values

None

Allowed From

Initialization, threads, timers, ISRs

Preemption Possible

No

Example

```
/*  Initialize NetX Duo for operation.  */
nx_system_initialize();

/*  At this point, NetX Duo is ready for IP creation and all
    subsequent network operations.  */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nx_tcp_client_socket_bind

Bind client TCP socket to TCP port

Prototype

```
UINT nx_tcp_client_socket_bind(NX_TCP_SOCKET *socket_ptr,
                               UINT port,
                               ULONG wait_option);
```

Description

This service binds the previously created TCP client socket to the specified TCP port. Valid TCP sockets range from 0 through 0xFFFF. If the specified TCP port is unavailable, the service suspends according to the supplied wait option.

Parameters

socket_ptr	Pointer to previously created TCP socket instance.
port	Port number to bind (1 through 0xFFFF). If port number is NX_ANY_PORT (0x0000), the IP instance will search for the next free port and use that for the binding.
wait_option	Defines how the service behaves if the port is already bound to another socket. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket bind.
NX_ALREADY_BOUND	(0x22)	This socket is already bound to another TCP port.
NX_PORT_UNAVAILABLE	(0x23)	Port is already bound to a different socket.
NX_NO_FREE_PORTS	(0x45)	No free port.

NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_INVALID_PORT	(0x46)	Invalid port.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Bind a previously created client socket to port 12 and wait for
    7 timer ticks for the bind to complete.  */
status = nx_tcp_client_socket_bind(&client_socket, 12, 7);

/*  If status is NX_SUCCESS, the previously created client_socket is
    bound to port 12 on the associated IP instance.  */
```

See Also

nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_client_socket_connect

Connect client TCP socket

Prototype

```
UINT nx_tcp_client_socket_connect(NX_TCP_SOCKET *socket_ptr,
                                  ULONG server_ip,
                                  UINT server_port,
                                  ULONG wait_option)
```

Description

This service connects the previously created and bound TCP client socket to the specified server's port. Valid TCP server ports range from 0 through 0xFFFF. If the connection does not complete immediately, the service suspends according to the supplied wait option.

Parameters

socket_ptr	Pointer to previously created TCP socket instance.
server_ip	Server's IP address.
server_port	Server port number to connect to (1 through 0xFFFF).
wait_option	Defines how the service behaves while the connection is being established. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket connect.
NX_NOT_BOUND	(0x24)	Socket is not bound.
NX_NOT_CLOSED	(0x35)	Socket is not in a closed state.
NX_IN_PROGRESS	(0x37)	No wait was specified, the connection attempt is in progress.
NX_INVALID_INTERFACE	(0x4C)	Invalid interface supplied.

NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid server IP address.
NX_INVALID_PORT	(0x46)	Invalid port.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Initiate a TCP connection from a previously created and bound
    client socket. The connection requested in this example is to
    port 12 on the server with the IP address of 1.2.3.5. This
    service will wait 300 timer ticks for the connection to take
    place before giving up.  */
status = nx_tcp_client_socket_connect(&client_socket,
                                      IP_ADDRESS(1,2,3,5),
                                      12, 300);

/*  If status is NX_SUCCESS, the previously created and bound
    client_socket is connected to port 12 on IP 1.2.3.5.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_client_socket_port_get

Get port number bound to client TCP socket

Prototype

```
UINT nx_tcp_client_socket_port_get(NX_TCP_SOCKET *socket_ptr,
                                    UINT *port_ptr);
```

Description

This service retrieves the port number associated with the socket, which is useful to find the port allocated by NetX Duo in situations where the NX_ANY_PORT was specified at the time the socket was bound.

Parameters

socket_ptr	Pointer to previously created TCP socket instance.
port_ptr	Pointer to destination for the return port number. Valid port numbers are (1 through 0xFFFF).

Return Values

NX_SUCCESS	(0x00)	Successful socket bind.
NX_NOT_BOUND	(0x24)	This socket is not bound to a port.
NX_PTR_ERROR	(0x07)	Invalid socket pointer or port return pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Get the port number of previously created and bound client
    socket.  */
status = nx_tcp_client_socket_port_get(&client_socket, &port);

/*  If status is NX_SUCCESS, the port variable contains the port
    this socket is bound to.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_client_socket_unbind

Unbind TCP client socket from TCP port

Prototype

```
UINT nx_tcp_client_socket_unbind(NX_TCP_SOCKET *socket_ptr)
```

Description

This service releases the binding between the TCP client socket and a TCP port. If there are other threads waiting to bind another socket to the same port number, the first suspended thread is then bound to this port.

Parameters

socket_ptr	Pointer to previously created TCP socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful socket unbind.
NX_NOT_BOUND	(0x24)	Socket was not bound to any port.
NX_NOT_CLOSED	(0x35)	Socket has not been disconnected.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

Yes

Example

```
/*  Unbind a previously created and bound client TCP socket.
status = nx_tcp_client_socket_unbind(&client_socket);

/*  If status is NX_SUCCESS, the client socket is no longer
    bound.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_enable

Enable TCP component of NetX Duo

Prototype

```
UINT nx_tcp_enable(NX_IP *ip_ptr);
```

Description

This service enables the Transmission Control Protocol (TCP) component of NetX Duo. After enabled, TCP connections may be established by the application.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful TCP enable.
NX_ALREADY_ENABLED	(0x15)	TCP is already enabled.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Initialization, threads, timers

Preemption Possible

No

Example

```
/*  Enable TCP on a previously created IP instance ip_0. /*
status = nx_tcp_enable(&ip_0);

/*  If status is NX_SUCCESS, TCP is enabled on the IP instance.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_free_port_find

Find next available TCP port

Prototype

```
UINT nx_tcp_free_port_find(NX_IP *ip_ptr,
                           UINT port,
                           UINT *free_port_ptr);
```

Description

This service attempts to locate a free TCP port (unbound) starting from the application supplied port. The search logic will wrap around if the search happens to reach the maximum port value of 0xFFFF. If the search is successful, the free port is returned in the variable pointed to by *free_port_ptr*.

This service can be called from another thread and have the same port returned. To prevent this race condition, the application may wish to place this service and the actual client socket bind under the protection of a mutex.

Parameters

ip_ptr	Pointer to previously created IP instance.
port	Port number to start search at (1 through 0xFFFF).
free_port_ptr	Pointer to the destination free port return value.

Return Values

NX_SUCCESS	(0x00)	Successful free port find.
NX_NO_FREE_PORTS	(0x45)	No free ports found.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_INVALID_PORT	(0x46)	The specified port number is invalid.

Allowed From

Threads

Preemption Possible

No

Example

```
/*  Locate a free TCP port, starting at port 12, on a previously
    created IP instance.  */
status = nx_tcp_free_port_find(&ip_0, 12, &free_port);

/*  If status is NX_SUCCESS, "free_port" contains the next free port
    on the IP instance.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_info_get

Retrieve information about TCP activities

Prototype

```
UINT nx_tcp_info_get(NX_IP *ip_ptr,
                     ULONG *tcp_packets_sent,
                     ULONG *tcp_bytes_sent,
                     ULONG *tcp_packets_received,
                     ULONG *tcp_bytes_received,
                     ULONG *tcp_invalid_packets,
                     ULONG *tcp_receive_packets_dropped,
                     ULONG *tcp_checksum_errors,
                     ULONG *tcp_connections,
                     ULONG *tcp_disconnections,
                     ULONG *tcp_connections_dropped,
                     ULONG *tcp_retransmit_packets);
```

Description

This service retrieves information about TCP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
tcp_packets_sent	Pointer to destination for the total number of TCP packets sent.
tcp_bytes_sent	Pointer to destination for the total number of TCP bytes sent.
tcp_packets_received	Pointer to destination of the total number of TCP packets received.
tcp_bytes_received	Pointer to destination of the total number of TCP bytes received.
tcp_invalid_packets	Pointer to destination of the total number of invalid TCP packets.
tcp_receive_packets_dropped	Pointer to destination of the total number of TCP receive packets dropped.
tcp_checksum_errors	Pointer to destination of the total number of TCP packets with checksum errors.

tcp_connections	Pointer to destination of the total number of TCP connections.
tcp_disconnections	Pointer to destination of the total number of TCP disconnections.
tcp_connections_dropped	Pointer to destination of the total number of TCP connections dropped.
tcp_retransmit_packets	Pointer to destination of the total number of TCP packets retransmitted.

Return Values

NX_SUCCESS	(0x00)	Successful TCP information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/*  Retrieve TCP information from previously created IP Instance
    ip_0. */
status =  nx_tcp_info_get(&ip_0,
                              &tcp_packets_sent,
                              &tcp_bytes_sent,
                              &tcp_packets_received,
                              &tcp_bytes_received,
                              &tcp_invalid_packets,
                              &tcp_receive_packets_dropped,
                              &tcp_checksum_errors,
                              &tcp_connections,
                              &tcp_disconnections
                              &tcp_connections_dropped,
                              &tcp_retransmit_packets);

/*  If status is NX_SUCCESS, TCP information was retrieved. */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_server_socket_accept

Accept TCP connection

Prototype

```
UINT nx_tcp_server_socket_accept(NX_TCP_SOCKET *socket_ptr,
                                 ULONG wait_option);
```

Description

This service accepts (or prepares to accept) a TCP client socket connection request for a port that was previously set up for listening. This service may be called immediately after the application calls the listen or re-listen service or after the listen callback routine is called when the client connection is actually present. If a connection cannot not be established right away, the service suspends according to the supplied wait option.

*The application must call **nx_tcp_server_socket_unaccept** after the connection is no longer needed to remove the server socket's binding to the server port.*

Application callback routines are called from within the IP's helper thread.

Parameters

socket_ptr	Pointer to the TCP server socket control block.
wait_option	Defines how the service behaves while the connection is being established. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful TCP server socket accept (passive connect).
NX_NOT_LISTEN_STATE	(0x36)	The server socket supplied is not in a listen state.

NX_IN_PROGRESS	(0x37)	No wait was specified, the connection attempt is in progress.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_PTR_ERROR	(0x07)	Socket pointer error.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
NX_PACKET_POOL          my_pool;
NX_IP                   my_ip;
NX_TCP_SOCKET           server_socket;

void   port_12_connect_request(NX_TCP_SOCKET *socket_ptr, UINT port)
{

    /* Simply set the semaphore to wake up the server thread.  */
    tx_semaphore_put(&port_12_semaphore);
}

void  port_12_disconnect_request(NX_TCP_SOCKET *socket_ptr)
{
    /* The client has initiated a disconnect on this socket. This
       example doesn't use this callback.  */
}

void   port_12_server_thread_entry(ULONG id)
{

NX_PACKET   *my_packet;
UINT        status, i;

    /* Assuming that:
         "port_12_semaphore" has already been created with an
         initial count of 0 "my_ip" has already been created and the
         link is enabled "my_pool" packet pool has already been
         created
    */

    /* Create the server socket.  */
    nx_tcp_socket_create(&my_ip, &server_socket,
                         "Port 12 Server Socket",
```

```
                        NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                        NX_IP_TIME_TO_LIVE, 100,
                        NX_NULL, port_12_disconnect_request);

    /* Setup server listening on port 12.  */
    nx_tcp_server_socket_listen(&my_ip, 12, &server_socket, 5,
                                port_12_connect_request);

    /* Loop to process 5 server connections, sending
       "Hello_and_Goodbye" to each client and then disconnecting.*/
    for (i = 0; i < 5; i++)
    {

        /* Get the semaphore that indicates a client connection
           request is present.  */
        tx_semaphore_get(&port_12_semaphore, TX_WAIT_FOREVER);

        /* Wait for 200 ticks for the client socket connection to
           complete.*/
        status =  nx_tcp_server_socket_accept(&server_socket, 200);

        /* Check for a successful connection.  */
        if (status == NX_SUCCESS)
        {

            /* Allocate a packet for the "Hello_and_Goodbye"
               message */
            nx_packet_allocate(&my_pool, &my_packet, NX_TCP_PACKET,
                                         NX_WAIT_FOREVER);

            /* Place "Hello_and_Goodbye" in the packet.  */
            nx_packet_data_append(my_packet, "Hello_and_Goodbye",
                                  sizeof("Hello_and_Goodbye"),
                                  &my_pool, NX_WAIT_FOREVER);

            /* Send "Hello_and_Goodbye" to client.  */
            nx_tcp_socket_send(&server_socket, my_packet, 200);

            /* Check for an error.  */
            if (status)
            {

                /* Error, release the packet.  */
                nx_packet_release(my_packet);
            }

            /* Now disconnect the server socket from the client.  */
             nx_tcp_socket_disconnect(&server_socket, 200);
        }

       /* Unaccept the server socket.  Note that unaccept is called
           even if disconnect or accept fails.  */
        nx_tcp_server_socket_unaccept(&server_socket);

        /* Setup server socket for listening with this socket
           again.  */
        nx_tcp_server_socket_relisten(&my_ip, 12, &server_socket);
    }

    /* We are now done so unlisten on server port 12.  */
    nx_tcp_server_socket_unlisten(&my_ip, 12);

    /* Delete the server socket.  */
    nx_tcp_socket_delete(&server_socket);
}
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_server_socket_listen

Enable listening for client connection on TCP port

Prototype

```
UINT nx_tcp_server_socket_listen(NX_IP *ip_ptr, UINT port,
                                 NX_TCP_SOCKET *socket_ptr,
                                 UINT listen_queue_size,
                                 VOID (*listen_callback)
                                      (NX_TCP_SOCKET *socket_ptr,
                                       UINT port));
```

Description

This service enables listening for a client connection request on the specified TCP port. When a client connection request is received, the supplied server socket is bound to the specified port and the supplied listen callback function is called.

The listen callback routine's processing is completely up to the application. It may contain logic to wake up an application thread that subsequently performs an accept operation. If the application already has a thread suspended on accept processing for this socket, the listen callback routine may not be needed.

If the application wishes to handle additional client connections on the same port, the ***nx_tcp_server_socket_relisten*** must be called with an available socket (a socket in the CLOSED state) for the next connection. Until the re-listen service is called, additional client connections are queued. When the maximum queue depth is exceeded, the oldest connection request is dropped in favor of queuing the new connection request. The maximum queue depth is specified by this service.

i *Application callback routines are called from the internal IP helper thread.*

Parameters

ip_ptr	Pointer to previously created IP instance.
port	Port number to listen on (1 through 0xFFFF).
socket_ptr	Pointer to socket to use for the connection.
listen_queue_size	Number of client connection requests that can be queued.
listen_callback	Application function to call when the connection is received. If a NULL is

specified, the listen callback feature is disabled.

Return Values

NX_SUCCESS	(0x00)	Successful TCP port listen enable.
NX_MAX_LISTEN	(0x33)	No more listen request structures are available. The constant NX_MAX_LISTEN_REQUESTS in ***nx_api.h*** defines how many active listen requests are possible.
NX_NOT_CLOSED	(0x35)	The supplied server socket is not in a closed state.
NX_ALREADY_BOUND	(0x22)	The supplied server socket is already bound to a port.
NX_DUPLICATE_LISTEN	(0x34)	There is already an active listen request for this port.
NX_INVALID_PORT	(0x46)	Invalid port specified.
NX_PTR_ERROR	(0x07)	Invalid IP or socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
NX_PACKET_POOL          my_pool;
NX_IP                   my_ip;
NX_TCP_SOCKET           server_socket;

void   port_12_connect_request(NX_TCP_SOCKET *socket_ptr, UINT port)
{
```

```
    /* Simply set the semaphore to wake up the server thread.*/
    tx_semaphore_put(&port_12_semaphore);
}

void  port_12_disconnect_request(NX_TCP_SOCKET *socket_ptr)
{
    /* The client has initiated a disconnect on this socket.
       This example doesn't use this callback.  */
}

void   port_12_server_thread_entry(ULONG id)
{

NX_PACKET   *my_packet;
UINT        status, i;

    /* Assuming that:
       "port_12_semaphore" has already been created with an
       initial count of 0 "my_ip" has already been created
       and the link is enabled "my_pool" packet pool has already
       been created.
    */

    /* Create the server socket.  */
    nx_tcp_socket_create(&my_ip, &server_socket, "Port 12 Server
                         Socket",
                         NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                         NX_IP_TIME_TO_LIVE, 100,
                         NX_NULL, port_12_disconnect_request);

    /* Setup server listening on port 12.  */
    nx_tcp_server_socket_listen(&my_ip, 12, &server_socket, 5,
                                port_12_connect_request);

    /* Loop to process 5 server connections, sending
       "Hello_and_Goodbye" to
       each client and then disconnecting.  */
    for (i = 0; i < 5; i++)
    {

         /* Get the semaphore that indicates a client connection
            request is present. */
        tx_semaphore_get(&port_12_semaphore, TX_WAIT_FOREVER);

        /* Wait for 200 ticks for the client socket connection
           to complete. */
        status =  nx_tcp_server_socket_accept(&server_socket, 200);

        /* Check for a successful connection.  */
        if (status == NX_SUCCESS)
        {

            /* Allocate a packet for the "Hello_and_Goodbye"
               message.  */
            nx_packet_allocate(&my_pool, &my_packet, NX_TCP_PACKET,
                               NX_WAIT_FOREVER);

            /* Place "Hello_and_Goodbye" in the packet.  */
            nx_packet_data_append(my_packet, "Hello_and_Goodbye",
                                  sizeof("Hello_and_Goodbye"),
                                  &my_pool,
                                  NX_WAIT_FOREVER);
```

```
            /* Send "Hello_and_Goodbye" to client.  */
            nx_tcp_socket_send(&server_socket, my_packet, 200);

            /* Check for an error.  */
            if (status)
            {

                /* Error, release the packet.  */
                nx_packet_release(my_packet);
            }

             /* Now disconnect the server socket from the client.  */
            nx_tcp_socket_disconnect(&server_socket, 200);
        }

       /* Unaccept the server socket.  Note that unaccept is called even
          if disconnect or accept fails.  */
        nx_tcp_server_socket_unaccept(&server_socket);

        /* Setup server socket for listening with this socket
           again.  */
        nx_tcp_server_socket_relisten(&my_ip, 12, &server_socket);
    }

    /* We are now done so unlisten on server port 12.  */
    nx_tcp_server_socket_unlisten(&my_ip, 12);

    /* Delete the server socket.  */
    nx_tcp_socket_delete(&server_socket);
}
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_server_socket_relisten

Re-listen for client connection on TCP port

Prototype

```
UINT nx_tcp_server_socket_relisten(NX_IP *ip_ptr, UINT port,
                                   NX_TCP_SOCKET *socket_ptr);
```

Description

This service is called after a connection has been received on a port that was setup previously for listening. The main purpose of this service is to provide a new server socket for the next client connection. If a connection request is queued, the connection will be processed immediately during this service call.

The same callback routine specified by the original listen request is also called when a connection is present for this new server socket.

Parameters

ip_ptr	Pointer to previously created IP instance.
port	Port number to re-listen on (1 through 0xFFFF).
socket_ptr	Socket to use for the next client connection.

Return Values

NX_SUCCESS	(0x00)	Successful TCP port re-listen.
NX_NOT_CLOSED	(0x35)	The supplied server socket is not in a closed state.
NX_ALREADY_BOUND	(0x22)	The supplied server socket is already bound to a port.
NX_INVALID_RELISTEN	(0x47)	There is already a valid socket pointer for this port or the port specified does not have a listen request active.
NX_CONNECTION_PENDING	(0x48)	Same as NX_SUCCESS, except there was a queued

		connection request and it was processed during this call.
NX_INVALID_PORT	(0x46)	Invalid port specified.
NX_PTR_ERROR	(0x07)	Invalid IP or listen callback pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
NX_PACKET_POOL          my_pool;
NX_IP                   my_ip;
NX_TCP_SOCKET           server_socket;

void   port_12_connect_request(NX_TCP_SOCKET *socket_ptr, UINT port)
{

    /* Simply set the semaphore to wake up the server thread.*/
    tx_semaphore_put(&port_12_semaphore);
}

void  port_12_disconnect_request(NX_TCP_SOCKET *socket_ptr)
{
    /* The client has initiated a disconnect on this socket. This
       example doesn't use this callback.  */
}

void   port_12_server_thread_entry(ULONG id)
{

NX_PACKET   *my_packet;
UINT        status, i;

    /* Assuming that:
       "port_12_semaphore" has already been created with an initial
        count of 0.
       "my_ip" has already been created and the link is enabled.
       "my_pool" packet pool has already been created.   */

    /* Create the server socket.  */
    nx_tcp_socket_create(&my_ip, &server_socket, "Port 12 Server
Socket",
                                 NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                                 NX_IP_TIME_TO_LIVE, 100,
```

```
                                        NX_NULL,
        port_12_disconnect_request);

            /* Setup server listening on port 12.  */
            nx_tcp_server_socket_listen(&my_ip, 12, &server_socket, 5,
                                        port_12_connect_request);

              /* Loop to process 5 server connections, sending
                 "Hello_and_Goodbye" to each client then disconnecting.  */
              for (i = 0; i < 5; i++)
              {

                 /* Get the semaphore that indicates a client connection
                    request is present.  */
                 tx_semaphore_get(&port_12_semaphore, TX_WAIT_FOREVER);

                  /* Wait for 200 ticks for the client socket connection to
                     complete.  */
                  status =  nx_tcp_server_socket_accept(&server_socket,
200);

                 /* Check for a successful connection.  */
                 if (status == NX_SUCCESS)
                 {

                      /* Allocate a packet for the "Hello_and_Goodbye"
                         message.  */
                     nx_packet_allocate(&my_pool, &my_packet, NX_TCP_PACKET,
                                        NX_WAIT_FOREVER);

                      /* Place "Hello_and_Goodbye" in the packet.  */
                      nx_packet_data_append(my_packet, "Hello_and_Goodbye",
                                            sizeof("Hello_and_Goodbye"),
                                            &my_pool, NX_WAIT_FOREVER);

                      /* Send "Hello_and_Goodbye" to client.  */
                      nx_tcp_socket_send(&server_socket, my_packet, 200);

                      /* Check for an error.  */
                      if (status)
                      {

                          /* Error, release the packet.  */
                          nx_packet_release(my_packet);
                      }

                       /* Now disconnect the server socket from the client.
*/
                      nx_tcp_socket_disconnect(&server_socket, 200);
                  }

                  /* Unaccept the server socket.  Note that unaccept is
                     called even if disconnect or accept fails.  */
                  nx_tcp_server_socket_unaccept(&server_socket);

                  /* Setup server socket for listening with this socket
                     again.  */
                 nx_tcp_server_socket_relisten(&my_ip, 12, &server_socket);
              }

              /* We are now done so unlisten on server port 12.  */
              nx_tcp_server_socket_unlisten(&my_ip, 12);
```

```
/* Delete the server socket.  */
nx_tcp_socket_delete(&server_socket);
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_server_socket_unaccept

Remove socket association with listening port

Prototype

```
UINT nx_tcp_server_socket_unaccept(NX_TCP_SOCKET *socket_ptr);
```

Description

This service removes the association between this server socket and the specified server port. The application must call this service after a disconnection or after an unsuccessful accept call.

Parameters

socket_ptr	Pointer to previously setup server socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful server socket unaccept.
NX_NOT_LISTEN_STATE	(0x36)	Server socket is in an improper state, and is probably not disconnected.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
NX_PACKET_POOL          my_pool;
NX_IP                   my_ip;
NX_TCP_SOCKET           server_socket;

void   port_12_connect_request(NX_TCP_SOCKET *socket_ptr, UINT port)
{

    /* Simply set the semaphore to wake up the server thread.  */
    tx_semaphore_put(&port_12_semaphore);
}

void  port_12_disconnect_request(NX_TCP_SOCKET *socket_ptr)
{
    /* The client has initiated a disconnect on this socket. This
example
       doesn't use this callback.  */
}

void   port_12_server_thread_entry(ULONG id)
{

NX_PACKET   *my_packet;
UINT        status, i;

    /* Assuming that:
       "port_12_semaphore" has already been created with an initial
count
       of 0 "my_ip" has already been created and the link is enabled
       "my_pool" packet pool has already been created
    */

    /* Create the server socket.  */
    nx_tcp_socket_create(&my_ip, &server_socket, "Port 12 Server
                         Socket",NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                         NX_IP_TIME_TO_LIVE, 100,NX_NULL,
                         port_12_disconnect_request);

    /* Setup server listening on port 12.  */
    nx_tcp_server_socket_listen(&my_ip, 12, &server_socket, 5,
                                port_12_connect_request);

    /* Loop to process 5 server connections, sending "Hello_and_Goodbye"
       to
       each client and then disconnecting.  */
    for (i = 0; i < 5; i++)
    {

        /* Get the semaphore that indicates a client connection request
           is present.  */
        tx_semaphore_get(&port_12_semaphore, TX_WAIT_FOREVER);

        /* Wait for 200 ticks for the client socket connection to
           complete.*/
        status =  nx_tcp_server_socket_accept(&server_socket, 200);

        /* Check for a successful connection.  */
        if (status == NX_SUCCESS)
        {

           /* Allocate a packet for the "Hello_and_Goodbye" message.  */
```

```
                nx_packet_allocate(&my_pool, &my_packet, NX_TCP_PACKET,
                                   NX_WAIT_FOREVER);

                /* Place "Hello_and_Goodbye" in the packet.  */
                nx_packet_data_append(my_packet,
                           "Hello_and_Goodbye",sizeof("Hello_and_Goodbye"),
                           &my_pool, NX_WAIT_FOREVER);

                /* Send "Hello_and_Goodbye" to client.  */
                nx_tcp_socket_send(&server_socket, my_packet, 200);

                /* Check for an error.  */
                if (status)
                {

                    /* Error, release the packet.  */
                    nx_packet_release(my_packet);
                }

                 /* Now disconnect the server socket from the client.  */
                 nx_tcp_socket_disconnect(&server_socket, 200);
           }

           /* Unaccept the server socket.  Note that unaccept is called even
              if disconnect or accept fails.  */
           nx_tcp_server_socket_unaccept(&server_socket);

           /* Setup server socket for listening with this socket again.  */
           nx_tcp_server_socket_relisten(&my_ip, 12, &server_socket);
        }

        /* We are now done so unlisten on server port 12.  */
        nx_tcp_server_socket_unlisten(&my_ip, 12);

        /* Delete the server socket.  */
        nx_tcp_socket_delete(&server_socket);
}
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_server_socket_unlisten

Disable listening for client connection on TCP port

Prototype

```
UINT nx_tcp_server_socket_unlisten(NX_IP *ip_ptr, UINT port);
```

Description

This service disables listening for a client connection request on the specified TCP port.

Parameters

ip_ptr	Pointer to previously created IP instance.
port	Number of port to disable listening (0 through 0xFFFF).

Return Values

NX_SUCCESS	(0x00)	Successful TCP listen disable.
NX_ENTRY_NOT_FOUND	(0x16)	Listening was not enabled for the specified port.
NX_INVALID_PORT	(0x46)	Invalid port specified.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
NX_PACKET_POOL          my_pool;
NX_IP                   my_ip;
NX_TCP_SOCKET           server_socket;

void   port_12_connect_request(NX_TCP_SOCKET *socket_ptr, UINT port)
{

    /* Simply set the semaphore to wake up the server thread.  */
    tx_semaphore_put(&port_12_semaphore);
}

void  port_12_disconnect_request(NX_TCP_SOCKET *socket_ptr)
{
    /* The client has initiated a disconnect on this socket. This example
       doesn't use this callback.*/
}

void   port_12_server_thread_entry(ULONG id)
{

NX_PACKET   *my_packet;
UINT        status, i;

    /* Assuming that:
       "port_12_semaphore" has already been created with an initial count
       of 0 "my_ip" has already been created and the link is enabled
       "my_pool" packet pool has already been created
    */

    /* Create the server socket.  */
    nx_tcp_socket_create(&my_ip, &server_socket, "Port 12 Server Socket",
                         NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                         NX_IP_TIME_TO_LIVE, 100,
                         NX_NULL, port_12_disconnect_request);

    /* Setup server listening on port 12.  */
    nx_tcp_server_socket_listen(&my_ip, 12, &server_socket, 5,
                                port_12_connect_request);

    /* Loop to process 5 server connections, sending "Hello_and_Goodbye" to
       each client and then disconnecting.  */
    for (i = 0; i < 5; i++)
    {

       /* Get the semaphore that indicates a client connection request is
          present.  */
       tx_semaphore_get(&port_12_semaphore, TX_WAIT_FOREVER);

        /* Wait for 200 ticks for the client socket connection to
complete.*/
       status =  nx_tcp_server_socket_accept(&server_socket, 200);

       /* Check for a successful connection.  */
       if (status == NX_SUCCESS)
       {

            /* Allocate a packet for the "Hello_and_Goodbye" message.  */
            nx_packet_allocate(&my_pool, &my_packet, NX_TCP_PACKET,
                               NX_WAIT_FOREVER);

            /* Place "Hello_and_Goodbye" in the packet.  */
```

```
            nx_packet_data_append(my_packet, "Hello_and_Goodbye",
                                  sizeof("Hello_and_Goodbye"), &my_pool,
                                  NX_WAIT_FOREVER);

            /* Send "Hello_and_Goodbye" to client.  */
            nx_tcp_socket_send(&server_socket, my_packet, 200);

            /* Check for an error.  */
            if (status)
            {

                /* Error, release the packet.  */
                nx_packet_release(my_packet);
            }

             /* Now disconnect the server socket from the client.  */
             nx_tcp_socket_disconnect(&server_socket, 200);
        }

        /* Unaccept the server socket.  Note that unaccept is called even if
           disconnect or accept fails.  */
        nx_tcp_server_socket_unaccept(&server_socket);

        /* Setup server socket for listening with this socket again.  */
        nx_tcp_server_socket_relisten(&my_ip, 12, &server_socket);
    }

    /* We are now done so unlisten on server port 12.  */
    nx_tcp_server_socket_unlisten(&my_ip, 12);

    /* Delete the server socket.  */
    nx_tcp_socket_delete(&server_socket);
}
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_bytes_available

Retrieves number of bytes available for retrieval

Prototype

```
UINT nx_tcp_socket_bytes_available(NX_TCP_SOCKET *socket_ptr,
                                    ULONG *bytes_available);
```

Description

This service obtains the number of bytes available for retrieval in the specified TCP socket. Note that the TCP socket must already be connected.

Parameters

socket_ptr	Pointer to previously created and connected TCP socket.
bytes_available	Pointer to destination for bytes available.

Return Values

NX_SUCCESS	(0x00)	Service executes successfully. Number of bytes available for read is returned to the caller.
NX_NOT_CONNECTED	(0x38)	Socket is not in a connected state.
NX_PTR_ERROR	(0x07)	Invalid pointers.
NX_NOT_ENABLED	(0x14)	TCP is not enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Get the bytes available for retrieval on the specified socket. */
status =
nx_tcp_socket_bytes_available(&my_socket,&bytes_available);

/* Is status = NX_SUCCESS, the available bytes is returned in
   bytes_available. */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_create

Create TCP client or server socket

Prototype

```
UINT nx_tcp_socket_create(NX_IP *ip_ptr, NX_TCP_SOCKET *socket_ptr,
            CHAR *name, ULONG type_of_service, ULONG fragment,
            UINT time_to_live, ULONG window_size,
            VOID (*urgent_data_callback)(NX_TCP_SOCKET *socket_ptr),
            VOID (*disconnect_callback)(NX_TCP_SOCKET *socket_ptr));
```

Description

This service creates a TCP client or server socket for the specified IP instance.

> *Application callback routines are called from the thread associated with this IP instance.*

Parameters

ip_ptr	Pointer to previously created IP instance.
socket_ptr	Pointer to new TCP socket control block.
name	Application name for this TCP socket.
type_of_service	Defines the type of service for the transmission, legal values are as follows: NX_IP_NORMAL(0x00000000) NX_IP_MIN_DELAY(0x00100000) NX_IP_MAX_DATA(0x00080000) NX_IP_MAX_RELIABLE(0x00040000) NX_IP_MIN_COST(0x00020000)
fragment	Specifies whether or not IP fragmenting is allowed. If NX_FRAGMENT_OKAY (0x0) is specified, IP fragmenting is allowed. If NX_DONT_FRAGMENT (0x4000) is specified, IP fragmenting is disabled.
time_to_live	Specifies the 8-bit value that defines how many routers this packet can pass before being thrown away. The default value is specified by NX_IP_TIME_TO_LIVE.

window_size	Defines the maximum number of bytes allowed in the receive queue for this socket
urgent_data_callback	Application function that is called whenever urgent data is detected in the receive stream. If this value is NX_NULL, urgent data is ignored.
disconnect_callback	Application function that is called whenever a disconnect is issued by the socket at the other end of the connection. If this value is NX_NULL, the disconnect callback function is disabled.

Return Values

NX_SUCCESS	(0x00)	Successful TCP client socket create.
NX_OPTION_ERROR	(0x0A)	Invalid type-of-service, fragment, invalid window size, or time-to-live option.
NX_PTR_ERROR	(0x07)	Invalid IP or socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization and Threads

Preemption Possible

No

Example

```
/* Create a TCP client socket on the previously created IP instance,
   with normal delivery, IP fragmentation enabled, 0x80 time to
   live, a 200-byte receive window, no urgent callback routine, and
   the "client_disconnect" routine to handle disconnection initiated
   from the other end of the connection.  */
status =  nx_tcp_socket_create(&ip_0, &client_socket,
                               "Client Socket",
                               NX_IP_NORMAL, NX_FRAGMENT_OKAY,
                               0x80, 200, NX_NULL
                               client_disconnect);

/* If status is NX_SUCCESS, the client socket is created and ready
   to be bound.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_delete

Delete TCP socket

Prototype

```
UINT nx_tcp_socket_delete(NX_TCP_SOCKET *socket_ptr);
```

Description

This service deletes a previously created TCP socket. If the socket is still bound or connected, the service returns an error code.

Parameters

socket_ptr	Previously created TCP socket

Return Values

NX_SUCCESS	(0x00)	Successful socket delete.
NX_NOT_CREATED	(0x27)	Socket was not created.
NX_STILL_BOUND	(0x42)	Socket is still bound.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Delete a previously created TCP client socket.  */
status =  nx_tcp_socket_delete(&client_socket);

/* If status is NX_SUCCESS, the client socket is deleted.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_disconnect

Disconnect client and server socket connections

Prototype

```
UINT nx_tcp_socket_disconnect(NX_TCP_SOCKET *socket_ptr,
                              ULONG wait_option);
```

Description

This service disconnects an established client or server socket connection. A disconnect of a server socket should be followed by an un-accept request, while a client socket that is disconnected is left in a state ready for another connection request. If the disconnect process cannot finish immediately, the service suspends according to the supplied wait option.

Parameters

socket_ptr	Pointer to previously connected client or server socket instance.
wait_option	Defines how the service behaves while the disconnection is in progress. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket disconnect.
NX_NOT_CONNECTED	(0x38)	Specified socket is not connected.
NX_IN_PROGRESS	(0x37)	Disconnect is in progress, no wait was specified.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.

NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

Yes

Example

```
/* Disconnect from a previously established connection and wait a
   maximum of 400 timer ticks.  */
status =  nx_tcp_socket_disconnect(&client_socket, 400);

/* If status is NX_SUCCESS, the previously connected socket (either
   as a result of the client socket connect or the server accept) is
   disconnected.  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_disconnect_complete_notify

Install TCP disconnect complete notify callback function

Prototype

```
UINT nx_tcp_socket_disconnect_complete_notify(
                    NX_TCP_SOCKET  *socket_ptr,
                    VOID (*tcp_disconnect_complete_notify)
                              (NX_TCP_SOCKET *socket_ptr))
```

Description

This service registers a callback function which is invoked after a socket disconnect operation is completed. The TCP socket disconnect complete callback function is available if NetX Duo is built with the option ***NX_ENABLE_EXTENDED_NOTIFY_SUPPORT*** defined.

Parameters

socket_ptr	Pointer to previously connected client or server socket instance.
tcp_disconnect_complete_notify	The callback function to be installed.

Return Values

NX_SUCCESS	(0x00)	Successfully registered the callback function.
NX_NOT_SUPPORTED	(0x4B)	The extended notify feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Install the disconnect complete notify callback function. */
status =  nx_tcp_socket_disconnect_complete_notify(&client_socket,
                                                   callback);
```

See Also

nx_tcp_enable, nx_tcp_socket_create, nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get, nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set,nx_tcp_socket_receive_notify, nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure, nx_tcp_socket_window_update_notify_set

nx_tcp_socket_establish_notify

Set TCP establish notify callback function

Prototype

```
UINT nx_tcp_socket_establish_notify(NX_TCP_SOCKET *socket_ptr,
        VOID (*tcp_establish_notify)(NX_TCP_SOCKET *socket_ptr))
```

Description

This service registers a callback function, which is called after a TCP socket makes a connection. The TCP socket establish callback function is available if NetX Duo is built with the option ***NX_ENABLE_EXTENDED_NOTIFY_SUPPORT*** defined.

Parameters

socket_ptr	Pointer to previously connected client or server socket instance.
tcp_establish_notify	Callback function invoked after a TCP connection is established.

Return Values

NX_SUCCESS	(0x00)	Successfully sets the notify function.
NX_NOT_SUPPORTED	(0x4B)	The extended notify feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP has not been enabled by the application.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Set the function pointer "callback" as the notify function NetX
   Duo will call when the connection is in the established state. */
status =  nx_tcp_socket_establish_notify(&client_socket, callback);
```

See Also

nx_tcp_enable, nx_tcp_socket_create, nx_tcp_socket_disconnect_complete_notify, nx_tcp_socket_mss_get, nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify, nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure, nx_tcp_socket_window_update_notify_set

nx_tcp_socket_info_get

Retrieve information about TCP socket activities

Prototype

```
UINT nx_tcp_socket_info_get(NX_TCP_SOCKET *socket_ptr,
                            ULONG *tcp_packets_sent,
                            ULONG *tcp_bytes_sent,
                            ULONG *tcp_packets_received,
                            ULONG *tcp_bytes_received,
                            ULONG *tcp_retransmit_packets,
                            ULONG *tcp_packets_queued,
                            ULONG *tcp_checksum_errors,
                            ULONG *tcp_socket_state,
                            ULONG *tcp_transmit_queue_depth,
                            ULONG *tcp_transmit_window,
                            ULONG *tcp_receive_window);
```

Description

This service retrieves information about TCP socket activities for the specified TCP socket instance.

i *If a destination pointer is NX_NULL, that particular information is not returned to the caller.*

Parameters

socket_ptr	Pointer to previously created TCP socket instance.
tcp_packets_sent	Pointer to destination for the total number of TCP packets sent on socket.
tcp_bytes_sent	Pointer to destination for the total number of TCP bytes sent on socket.
tcp_packets_received	Pointer to destination of the total number of TCP packets received on socket.
tcp_bytes_received	Pointer to destination of the total number of TCP bytes received on socket.
tcp_retransmit_packets	Pointer to destination of the total number of TCP packet retransmissions.
tcp_packets_queued	Pointer to destination of the total number of queued TCP packets on socket.
tcp_checksum_errors	Pointer to destination of the total number of TCP packets with checksum errors on socket.
tcp_socket_state	Pointer to destination of the socket's current state.
tcp_transmit_queue_depth	Pointer to destination of the total number of transmit packets still queued waiting for ACK.
tcp_transmit_window	Pointer to destination of the current transmit window size.
tcp_receive_window	Pointer to destination of the current receive window size.

Return Values

NX_SUCCESS	(0x00)	Successful TCP socket information retrieval.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Retrieve TCP socket information from previously created
   socket_0.*/
status =  nx_tcp_socket_info_get(&socket_0,
                                 &tcp_packets_sent,
                                 &tcp_bytes_sent,
                                 &tcp_packets_received,
                                 &tcp_bytes_received,
                                 &tcp_retransmit_packets,
                                 &tcp_packets_queued,
                                 &tcp_checksum_errors,
                                 &tcp_socket_state,
                                 &tcp_transmit_queue_depth,
                                 &tcp_transmit_window,
                                 &tcp_receive_window);

/* If status is NX_SUCCESS, TCP socket information was retrieved. */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_mss_get

Get MSS of socket

Prototype

```
UINT  nx_tcp_socket_mss_get(NX_TCP_SOCKET *socket_ptr, ULONG *mss);
```

Description

This service retrieves the specified socket's local Maximum Segment Size (MSS).

Parameters

socket_ptr	Pointer to previously created socket.
mss	Destination for returning MSS.

Return Values

NX_SUCCESS	(0x00)	Successful MSS get.
NX_PTR_ERROR	(0x07)	Invalid socket or MSS destination pointer.
NX_NOT_ENABLED	(0x14)	TCP is not enabled.
NX_CALLER_ERROR	(0x11)	Caller is not a thread or initialization.

Allowed From

Initialization and threads

Preemption Possible

No

Example

```
/* Get the MSS for the socket "my_socket". */
status =  nx_tcp_socket_mss_get(&my_socket, &mss_value);

/* If status is NX_SUCCESS, the "mss_value" variable contains the
   socket's current MSS value.  */
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify,
nx_tcp_socket_establish_notify, nx_tcp_socket_mss_peer_get,
nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get,
nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify,
nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_mss_peer_get

Get MSS of the peer TCP socket

Prototype

```
UINT  nx_tcp_socket_mss_peer_get(NX_TCP_SOCKET *socket_ptr,
                                 ULONG *mss);
```

Description

This service retrieves the Maximum Segment Size (MSS) advertised by the peer socket.

Parameters

socket_ptr	Pointer to previously created and connected socket.
mss	Destination for returning the MSS.

Return Values

NX_SUCCESS	(0x00)	Successful peer MSS get.
NX_PTR_ERROR	(0x07)	Invalid socket or MSS destination pointer.
NX_NOT_ENABLED	(0x14)	TCP is not enabled.
NX_CALLER_ERROR	(0x11)	Caller is not a thread or initialization.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Get the MSS of the connected peer to the socket "my_socket". */
status =  nx_tcp_socket_mss_peer_get(&my_socket, &mss_value);

/* If status is NX_SUCCESS, the "mss_value" variable contains the
   socket peer's advertised MSS value.  */
```

See Also

nx_tcp_enable, nx_tcp_socket_create, nx_tcp_socket_disconnect_complete_notify, nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get, nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify, nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure, nx_tcp_socket_window_update_notify_set

nx_tcp_socket_mss_set

Set MSS of socket

Prototype

```
UINT  nx_tcp_socket_mss_set(NX_TCP_SOCKET *socket_ptr, ULONG mss);
```

Description

This service sets the specified socket's Maximum Segment Size (MSS). Note the MSS value must be within the network interface IP MTU, allowing room for IP and TCP headers.

This service should be used before a TCP socket starts the connection process. If the service is used after a TCP connection is established, the new value has no effect on the connection.

Parameters

socket_ptr	Pointer to previously created socket.
mss	Value of MSS to set.

Return Values

NX_SUCCESS	(0x00)	Successful MSS set.
NX_SIZE_ERROR	(0x09)	Specified MSS value is too large.
NX_NOT_CONNECTED	(0x38)	TCP connection has not been established
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_NOT_ENABLED	(0x14)	TCP is not enabled.
NX_CALLER_ERROR	(0x11)	Caller is not a thread or initialization.

Allowed From

Initialization and threads

Preemption Possible

No

Example

```
/* Set the MSS of the socket "my_socket" to 1000 bytes. */
status =  nx_tcp_socket_mss_set(&my_socket, 1000);

/* If status is NX_SUCCESS, the MSS of "my_socket" is 1000 bytes. */
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify,
nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get,
nx_tcp_socket_mss_peer_get, nx_tcp_socket_peer_info_get,
nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify,
nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_peer_info_get

Retrieve information about peer TCP socket

Prototype

```
UINT nx_tcp_socket_peer_info_get(NX_TCP_SOCKET *socket_ptr,
                                 ULONG *peer_ip_address,
                                 ULONG *peer_port);
```

Description

This service retrieves peer IP address and port information for the connected TCP socket over IPv4 network. The equivalent service that also supports IPv6 network is ***nxd_tcp_socket_peer_info_get.***

Parameters

socket_ptr	Pointer to previously created TCP socket.
peer_ip_address	Pointer to destination for peer IP address, in host byte order.
peer_port	Pointer to destination for peer port number, in host byte order.

Return Values

NX_SUCCESS	(0x00)	Service executes successfully. Peer IP address and port number are returned to the caller.
NX_NOT_CONNECTED	(0x38)	Socket is not in a connected state.
NX_PTR_ERROR	(0x07)	Invalid pointers.
NX_NOT_ENABLED	(0x14)	TCP is not enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Obtain peer IP address and port on the specified TCP socket. */
status = nx_tcp_socket_peer_info_get(&my_socket, &peer_ip_address,
                                     &peer_port);

/* If status = NX_SUCCESS, the data was successfully obtained. */
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify,
nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get,
nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set,
nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify,
nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_queue_depth_notify_set

Set the TCP transmit queue notify function

Prototype

```
UINT nx_tcp_socket_queue_depth_notify_set(
            NX_TCP_SOCKET *socket_ptr,
            VOID(*tcp_socket_queue_depth_notify)(NX_TCP_SOCKET *))
```

Description

This service sets the transmit queue depth update notify function specified by the application, which is called whenever the specified socket determines that it has released packets from the transmit queue such that the queue depth is no longer exceeding its limit. If an application would be blocked on transmit due to queue depth, the callback function serves as a notification to the application that it may start transmitting again. This service is available only if the NetX Duo library is built with the option ***NX_ENABLE_TCP_QUEUE_DEPTH_UPDATE_NOTIFY*** defined.

Parameters

socket_ptr	Pointer to the socket structure
tcp_socket_queue_depth_notify	The notify function to be installed

Return Values

NX_SUCCESS	(0x00)	Successfully installed the notify function
NX_NOT_SUPPORTED	(0x4B)	The TCP socket queue depth notify feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid pointer to the socket control block or the notify function
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
VOID tcp_socket_queue_depth_notify(NX_TCP_SOCKET *socket_ptr)
{
    /* Notify the application to resume sending. */

}
/* Install the TCP transmit queue notify function .*/
status = nxd_tcp_socket_queue_depth_notify_set(&tcp_socket,
                                    tcp_socket_queue_depth_notify);

/* If status == NX_SUCCESS, the callback function is successfully
    installed. */
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify,
nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get,
nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set,
nx_tcp_socket_peer_info_get, nx_tcp_socket_receive_notify,
nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_receive

Receive data from TCP socket

Prototype

```
UINT nx_tcp_socket_receive(NX_TCP_SOCKET *socket_ptr,
                           NX_PACKET **packet_ptr,
                           ULONG wait_option);
```

Description

This service receives TCP data from the specified socket. If no data is queued on the specified socket, the caller suspends based on the supplied wait option.

If NX_SUCCESS is returned, the application is responsible for releasing the received packet when it is no longer needed.

Parameters

socket_ptr	Pointer to previously created TCP socket instance.
packet_ptr	Pointer to TCP packet pointer.
wait_option	Defines how the service behaves if do data are currently queued on this socket. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket data receive.
NX_NOT_BOUND	(0x24)	Socket is not bound yet.
NX_NO_PACKET	(0x01)	No data received.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_NOT_CONNECTED	(0x38)	The socket is no longer connected.

NX_PTR_ERROR	(0x07)	Invalid socket or return packet pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Receive a packet from the previously created and connected TCP
   client socket. If no packet is available, wait for 200 timer
   ticks before giving up.  */
status =  nx_tcp_socket_receive(&client_socket, &packet_ptr, 200);

/* If status is NX_SUCCESS, the received packet is pointed to by
   "packet_ptr".  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_receive_notify

Notify application of received packets

Prototype

```
UINT nx_tcp_socket_receive_notify(NX_TCP_SOCKET *socket_ptr, VOID
                                   (*tcp_receive_notify)
                                   (NX_TCP_SOCKET *socket_ptr));
```

Description

This service configures the receive notify function pointer with the callback function specified by the application. This callback function is then called whenever one or more packets are received on the socket. If a NX_NULL pointer is supplied, the notify function is disabled.

Parameters

socket_ptr	Pointer to the TCP socket.
tcp_receive_notify	Application callback function pointer that is called when one or more packets are received on the socket.

Return Values

NX_SUCCESS	(0x00)	Successful socket receive notify.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Setup a receive packet callback function for the "client_socket"
   socket. */
status = nx_tcp_socket_receive_notify(&client_socket,
                                      my_receive_notify);

/* If status is NX_SUCCESS, NetX Duo will call the function named
   "my_receive_notify" whenever one or more packets are received for
   "client_socket". */
```

See Also

nx_tcp_enable, nx_tcp_socket_create, nx_tcp_socket_disconnect_complete_notify, nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get, nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure, nx_tcp_socket_window_update_notify_set

nx_tcp_socket_send

Send data through a TCP socket

Prototype

```
UINT nx_tcp_socket_send(NX_TCP_SOCKET *socket_ptr,
                        NX_PACKET *packet_ptr,
                        ULONG wait_option);
```

Description

This service sends TCP data through a previously connected TCP socket. If the receiver's last advertised window size is less than this request, the service optionally suspends based on the wait option specified. This service guarantees that no packet data larger than MSS is sent to the IP layer.

Unless an error is returned, the application should not release the packet after this call. Doing so will cause unpredictable results because the network driver will also try to release the packet after transmission.

Parameters

socket_ptr	Pointer to previously connected TCP socket instance.
packet_ptr	TCP data packet pointer.
wait_option	Defines how the service behaves if the request is greater than the window size of the receiver. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket send.
NX_NOT_BOUND	(0x24)	Socket was not bound to any port.
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface found.
NX_NOT_CONNECTED	(0x38)	Socket is no longer connected.
NX_WINDOW_OVERFLOW	(0x39)	Request is greater than receiver's advertised window size in bytes.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_INVALID_PACKET	(0x12)	Packet is not allocated.
NX_TX_QUEUE_DEPTH	(0x49)	Maximum transmit queue depth has been reached.
NX_OVERFLOW	(0x03)	Packet append pointer is invalid.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_UNDERFLOW	(0x02)	Packet prepend pointer is invalid.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Send a packet out on the previously created and connected TCP
   socket. If the receive window on the other side of the connection
   is less than the packet size, wait 200 timer ticks before giving
   up.  */
status =  nx_tcp_socket_send(&client_socket, packet_ptr, 200);

/* If status is NX_SUCCESS, the packet has been sent!  */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_state_wait

Wait for TCP socket to enter specific state

Prototype

```
UINT nx_tcp_socket_state_wait(NX_TCP_SOCKET *socket_ptr,
                              UINT desired_state,
                              ULONG wait_option);
```

Description

This service waits for the socket to enter the desired state. If the socket is not in the desired state, the service suspends according to the supplied wait option.

Parameters

socket_ptr	Pointer to previously connected TCP socket instance.
desired_state	Desired TCP state. Valid TCP socket states are defined as follows: NX_TCP_CLOSED(0x01) NX_TCP_LISTEN_STATE(0x02) NX_TCP_SYN_SENT (0x03) NX_TCP_SYN_RECEIVED(0x04) NX_TCP_ESTABLISHED (0x05) NX_TCP_CLOSE_WAIT(0x06) NX_TCP_FIN_WAIT_1(0x07) NX_TCP_FIN_WAIT_2 (0x08) NX_TCP_CLOSING (0x09) NX_TCP_TIMED_WAIT (0x0A) NX_TCP_LAST_ACK (0x0B)
wait_option	Defines how the service behaves if the requested state is not present. The wait options are defined as follows: NX_NO_WAIT (0x00000000) timeout value in ticks (0x00000001 through 0xFFFFFFFF)

Return Values

NX_SUCCESS	(0x00)	Successful state wait.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.

NX_NOT_SUCCESSFUL	(0x43)	State not present within the specified wait time.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_OPTION_ERROR	(0x0A)	The desired socket state is invalid.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Wait 300 timer ticks for the previously created socket to enter
   the established state in the TCP state machine. */
status =  nx_tcp_socket_state_wait(&client_socket,
                                   NX_TCP_ESTABLISHED, 300);

/* If status is NX_SUCCESS, the socket is now in the established
   state! */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nxd_tcp_client_socket_connect, nxd_tcp_socket_peer_info_get

nx_tcp_socket_timed_wait_callback

Install callback for timed wait state

Prototype

```
UINT nx_tcp_socket_timed_wait_callback(NX_TCP_SOCKET *socket_ptr,
                    VOID (*tcp_timed_wait_callback)
                         (NX_TCP_SOCKET *socket_ptr))
```

Description

This service registers a callback function which is invoked when the TCP socket is in timed wait state. To use this service, the NetX Duo library must be built with the option ***NX_ENABLE_EXTENDED_NOTIFY*** defined.

Parameters

socket_ptr	Pointer to previously connected client or server socket instance.
tcp_timed_wait_callback	The timed wait callback function

Return Values

NX_SUCCESS	(0x00)	Successfully registers the callback function socket
NX_NOT_SUPPORTED	(0x4B)	NetX Duo library is built without the extended notify feature enabled.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Install the timed wait callback function  */
nx_tcp_socket_timed_wait_callback(&client_socket, callback);
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify, nx_tcp_socket_establish_notify,
nx_tcp_socket_mss_get, nx_tcp_socket_mss_peer_get,
nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get,
nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify,
nx_tcp_socket_transmit_configure,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_transmit_configure

Configure socket's transmit parameters

Prototype

```
UINT  nx_tcp_socket_transmit_configure(NX_TCP_SOCKET *socket_ptr,
                                        ULONG max_queue_depth,
                                        ULONG timeout,
                                        ULONG max_retries,
                                        ULONG timeout_shift);
```

Description

This service configures various transmit parameters of the specified TCP socket.

Parameters

socket_ptr	Pointer to the TCP socket.
max_queue_depth	Maximum number of packets allowed to be queued for transmission.
timeout	Number of ThreadX timer ticks an ACK is waited for before the packet is sent again.
max_retries	Maximum number of retries allowed.
timeout_shift	Value to shift the timeout for each subsequent retry. A value of 0, results in the same timeout between successive retries. A value of 1, doubles the timeout between retries.

Return Values

NX_SUCCESS	(0x00)	Successful transmit socket configure.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_OPTION_ERROR	(0x0a)	Invalid queue depth option.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Configure the "client_socket" for a maximum transmit queue depth
   of 12, 100 tick timeouts, a maximum of 20 retries, and a timeout
   double on each successive retry. */
status = nx_tcp_socket_transmit_configure(&client_socket,12,100,20,
                                          1);

/* If status is NX_SUCCESS, the socket's transmit retry has been
   configured. */
```

See Also

nx_tcp_enable, nx_tcp_socket_create,
nx_tcp_socket_disconnect_complete_notify,
nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get,
nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set,
nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set,
nx_tcp_socket_receive_notify, nx_tcp_socket_timed_wait_callback,
nx_tcp_socket_window_update_notify_set

nx_tcp_socket_window_update_notify_set

Notify application of window size updates

Prototype

```
UINT nx_tcp_socket_window_update_notify_set(NX_TCP_SOCKET
                                        *socket_ptr,
                                        VOID (*tcp_window_update_notify)
                                        (NX_TCP_SOCKET *socket_ptr))
```

Description

This service installs a socket window update callback routine. This routine is called automatically whenever the specified socket receives a packet indicating an increase in the window size of the remote host.

Parameters

socket_ptr	Pointer to previously created TCP socket.
tcp_window_update_notify	Callback routine to be called when the window size changes. A value of NULL disables the window change update.

Return Values

NX_SUCCESS	(0x00)	Callback routine is installed on the socket.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_PTR_ERROR	(0x07)	Invalid pointers.
NX_NOT_ENABLED	(0x14)	TCP feature is not enabled.

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Set the function pointer to the windows update callback after creating the
   socket. */
status = nx_tcp_socket_window_update_notify_set(&data_socket,
                                                my_windows_update_callback);
/* Define the window callback function in the host application. */
void    my_windows_update_callback(&data_socket)
{

    /* Process update on increase TCP transmit socket window size. */
    return;
}
```

See Also

nx_tcp_enable, nx_tcp_socket_create, nx_tcp_socket_disconnect_complete_notify, nx_tcp_socket_establish_notify, nx_tcp_socket_mss_get, nx_tcp_socket_mss_peer_get, nx_tcp_socket_mss_set, nx_tcp_socket_peer_info_get, nx_tcp_socket_queue_depth_notify_set, nx_tcp_socket_receive_notify, nx_tcp_socket_timed_wait_callback, nx_tcp_socket_transmit_configure

nx_udp_enable

Enable UDP component of NetX Duo

Prototype

```
UINT nx_udp_enable(NX_IP *ip_ptr);
```

Description

This service enables the User Datagram Protocol (UDP) component of NetX Duo. After enabled, UDP datagrams may be sent and received by the application.

Parameters

ip_ptr	Pointer to previously created IP instance.

Return Values

NX_SUCCESS	(0x00)	Successful UDP enable.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_ALREADY_ENABLED	(0x15)	This component has already been enabled.

Allowed From

Initialization, threads, timers

Preemption Possible

No

Example

```
/* Enable UDP on the previously created IP instance.  */
status =  nx_udp_enable(&ip_0);

/* If status is NX_SUCCESS, UDP is now enabled on the specified IP
   instance.  */
```

See Also

nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_free_port_find

Find next available UDP port

Prototype

```
UINT nx_udp_free_port_find(NX_IP *ip_ptr, UINT port,
                           UINT *free_port_ptr);
```

Description

This service looks for a free UDP port (unbound) starting from the application supplied port number. The search logic will wrap around if the search reaches the maximum port value of 0xFFFF. If the search is successful, the free port is returned in the variable pointed to by free_port_ptr.

This service can be called from another thread and can have the same port returned. To prevent this race condition, the application may wish to place this service and the actual socket bind under the protection of a mutex.

Parameters

ip_ptr	Pointer to previously created IP instance.
port	Port number to start search (1 through 0xFFFF).
free_port_ptr	Pointer to the destination free port return variable.

Return Values

NX_SUCCESS	(0x00)	Successful free port find.
NX_NO_FREE_PORTS	(0x45)	No free ports found.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.
NX_INVALID_PORT	(0x46)	Specified port number is invalid.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Locate a free UDP port, starting at port 12, on a previously
   created IP instance.  */
status = nx_udp_free_port_find(&ip_0, 12, &free_port);

/* If status is NX_SUCCESS pointer, "free_port" identifies the next
   free UDP port on the IP instance.  */
```

See Also

nx_udp_enable, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_info_get

Retrieve information about UDP activities

Prototype

```
UINT nx_udp_info_get(NX_IP *ip_ptr,
                     ULONG *udp_packets_sent,
                     ULONG *udp_bytes_sent,
                     ULONG *udp_packets_received,
                     ULONG *udp_bytes_received,
                     ULONG *udp_invalid_packets,
                     ULONG *udp_receive_packets_dropped,
                     ULONG *udp_checksum_errors);
```

Description

This service retrieves information about UDP activities for the specified IP instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

ip_ptr	Pointer to previously created IP instance.
udp_packets_sent	Pointer to destination for the total number of UDP packets sent.
udp_bytes_sent	Pointer to destination for the total number of UDP bytes sent.
udp_packets_received	Pointer to destination of the total number of UDP packets received.
udp_bytes_received	Pointer to destination of the total number of UDP bytes received.
udp_invalid_packets	Pointer to destination of the total number of invalid UDP packets.
udp_receive_packets_dropped	Pointer to destination of the total number of UDP receive packets dropped.
udp_checksum_errors	Pointer to destination of the total number of UDP packets with checksum errors.

Return Values

NX_SUCCESS	(0x00)	Successful UDP information retrieval.
NX_PTR_ERROR	(0x07)	Invalid IP pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads, and timers

Preemption Possible

No

Example

```
/* Retrieve UDP information from previously created IP Instance
   ip_0.  */
status =  nx_udp_info_get(&ip_0, &udp_packets_sent,
                          &udp_bytes_sent,
                          &udp_packets_received,
                          &udp_bytes_received,
                          &udp_invalid_packets,
                          &udp_receive_packets_dropped,
                          &udp_checksum_errors);

/* If status is NX_SUCCESS, UDP information was retrieved.  */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_packet_info_extract

Extract network parameters from UDP packet

Prototype

```
UINT nx_udp_packet_info_extract(NX_PACKET *packet_ptr,
                                ULONG *ip_address,
                                UINT *protocol,
                                UINT *port,
                                UINT *interface_index);
```

Description

This service extracts network parameters, such as IPv4 address, peer port number, protocol type (this service always returns UDP type) from a packet received on an incoming interface. To obtain information on a packet coming from IPv4 or IPv6 network, application shall use the service ***nxd_udp_packet_info_extract.***

Parameters

packet_ptr	Pointer to packet.
ip_address	Pointer to sender IP address.
protocol	Pointer to protocol (UDP).
port	Pointer to sender's port number.
interface_index	Pointer to receiving interface index.

Return Values

NX_SUCCESS	(0x00)	Packet interface data successfully extracted.
NX_INVALID_PACKET	(0x12)	Packet does not contain IPv4 frame.
NX_PTR_ERROR	(0x07)	Invalid pointer input
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Extract network data from UDP packet interface.*/
status = nx_udp_packet_info_extract( packet_ptr, &ip_address,
                                     &protocol, &port,
                                     &interface_index)

/* If status is NX_SUCCESS packet data was successfully
   retrieved. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_bind

Bind UDP socket to UDP port

Prototype

```
UINT nx_udp_socket_bind(NX_UDP_SOCKET *socket_ptr, UINT port,
                        ULONG wait_option);
```

Description

This service binds the previously created UDP socket to the specified UDP port. Valid UDP sockets range from 0 through 0xFFFF. If the requested port number is bound to another socket, this service waits for specified period of time for the socket to unbind from the port number.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.
port	Port number to bind to (1 through 0xFFFF). If port number is NX_ANY_PORT (0x0000), the IP instance will search for the next free port and use that for the binding.
wait_option	Defines how the service behaves if the port is already bound to another socket. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket bind.
NX_ALREADY_BOUND	(0x22)	This socket is already bound to another port.
NX_PORT_UNAVAILABLE	(0x23)	Port is already bound to a different socket.
NX_NO_FREE_PORTS	(0x45)	No free port.

NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.
NX_INVALID_PORT	(0x46)	Invalid port specified.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Bind the previously created UDP socket to port 12 on the
   previously created IP instance. If the port is already bound,
   wait for 300 timer ticks before giving up. */
status = nx_udp_socket_bind(&udp_socket, 12, 300);

/* If status is NX_SUCCESS, the UDP socket is now bound to
   port 12.*/
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_bytes_available

Retrieves number of bytes available for retrieval

Prototype

```
UINT nx_udp_socket_bytes_available(NX_UDP_SOCKET *socket_ptr,
                                   ULONG *bytes_available);
```

Description

This service retrieves number of bytes available for reception in the specified UDP socket.

Parameters

socket_ptr	Pointer to previously created UDP socket.
bytes_available	Pointer to destination for bytes available.

Return Values

NX_SUCCESS	(0x00)	Successful bytes available retrieval.
NX_NOT_SUCCESSFUL	(0x43)	Socket not bound to a port.
NX_PTR_ERROR	(0x07)	Invalid pointers.
NX_NOT_ENABLED	(0x14)	UDP feature is not enabled.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Get the bytes available for retrieval from the UDP socket. */
status = nx_udp_socket_bytes_available(&my_socket,
                                       &bytes_available);

/* If status == NX_SUCCESS, the number of bytes was successfully
   retrieved.*/
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_checksum_disable

Disable checksum for UDP socket

Prototype

```
UINT nx_udp_socket_checksum_disable(NX_UDP_SOCKET *socket_ptr);
```

Description

This service disables the checksum logic for sending and receiving packets on the specified UDP socket. When the checksum logic is disabled, a value of zero is loaded into the UDP header's checksum field for all packets sent through this socket. A zero-value checksum value in the UDP header signals the receiver that checksum is not computed for this packet.

Also note that this has no effect if **NX_DISABLE_UDP_RX_CHECKSUM** and **NX_DISABLE_UDP_TX_CHECKSUM** are defined when receiving and sending UDP packets respectively,

Note that this service has no effect on packets on the IPv6 network since UDP checksum is mandatory for IPv6.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful socket checksum disable.
NX_NOT_BOUND	(0x24)	Socket is not bound.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads, timer

Preemption Possible

No

Example

```
/* Disable the UDP checksum logic for packets sent on this socket.  */
status = nx_udp_socket_checksum_disable(&udp_socket);

/* If status is NX_SUCCESS, outgoing packets will not have a checksum
   calculated.  */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_checksum_enable

Enable checksum for UDP socket

Prototype

```
UINT nx_udp_socket_checksum_enable(NX_UDP_SOCKET *socket_ptr);
```

Description

This service enables the checksum logic for sending and receiving packets on the specified UDP socket. The checksum covers the entire UDP data area as well as a pseudo IP header.

Also note that this has no effect if **NX_DISABLE_UDP_RX_CHECKSUM** and **NX_DISABLE_UDP_TX_CHECKSUM** are defined when receiving and sending UDP packets respectively.

Note that this service has no effect on packets on the IPv6 network. UDP checksum is mandatory in IPv6.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful socket checksum enable.
NX_NOT_BOUND	(0x24)	Socket is not bound.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads, timer

Preemption Possible

No

Example

```
/* Enable the UDP checksum logic for packets sent on this socket.
*/
status = nx_udp_socket_checksum_enable(&udp_socket);

/* If status is NX_SUCCESS, outgoing packets will have a checksum
   calculated.  */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_create

Create UDP socket

Prototype

```
UINT nx_udp_socket_create(NX_IP *ip_ptr,
                          NX_UDP_SOCKET *socket_ptr, CHAR *name,
                          ULONG type_of_service, ULONG fragment,
                          UINT time_to_live, ULONG queue_maximum);
```

Description

This service creates a UDP socket for the specified IP instance.

Parameters

ip_ptr	Pointer to previously created IP instance.
socket_ptr	Pointer to new UDP socket control bloc.
name	Application name for this UDP socket.
type_of_service	Defines the type of service for the transmission, legal values are as follows: NX_IP_NORMAL (0x00000000) NX_IP_MIN_DELAY (0x00100000) NX_IP_MAX_DATA (0x00080000) NX_IP_MAX_RELIABLE (0x00040000) NX_IP_MIN_COST (0x00020000)
fragment	Specifies whether or not IP fragmenting is allowed. If NX_FRAGMENT_OKAY (0x0) is specified, IP fragmenting is allowed. If NX_DONT_FRAGMENT (0x4000) is specified, IP fragmenting is disabled.
time_to_live	Specifies the 8-bit value that defines how many routers this packet can pass before being thrown away. The default value is specified by NX_IP_TIME_TO_LIVE.
queue_maximum	Defines the maximum number of UDP datagrams that can be queued for this socket. After the queue limit is reached, for every new packet received the oldest UDP packet is released.

Return Values

NX_SUCCESS	(0x00)	Successful UDP socket create.

NX_OPTION_ERROR	(0x0A)	Invalid type-of-service, fragment, or time-to-live option.
NX_PTR_ERROR	(0x07)	Invalid IP or socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization and Threads

Preemption Possible

No

Example

```
/* Create a UDP socket with a maximum receive queue of 30 packets.*/
status = nx_udp_socket_create(&ip_0, &udp_socket, "Sample UDP
                              Socket",
                              NX_IP_NORMAL, NX_FRAGMENT_OKAY, 0x80,
                              30);

/* If status is NX_SUCCESS, the new UDP socket has been created and
   is ready for binding.  */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_delete

Delete UDP socket

Prototype

```
UINT nx_udp_socket_delete(NX_UDP_SOCKET *socket_ptr);
```

Description

This service deletes a previously created UDP socket. If the socket was bound to a port, the socket must be unbound first.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful socket delete.
NX_STILL_BOUND	(0x42)	Socket is still bound.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Delete a previously created UDP socket.  */
status = nx_udp_socket_delete(&udp_socket);

/* If status is NX_SUCCESS, the previously created UDP socket has
   been deleted.  */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_info_get

Retrieve information about UDP socket activities

Prototype

```
UINT nx_udp_socket_info_get(NX_UDP_SOCKET *socket_ptr,
                            ULONG *udp_packets_sent,
                            ULONG *udp_bytes_sent,
                            ULONG *udp_packets_received,
                            ULONG *udp_bytes_received,
                            ULONG *udp_packets_queued,
                            ULONG *udp_receive_packets_dropped,
                            ULONG *udp_checksum_errors);
```

Description

This service retrieves information about UDP socket activities for the specified UDP socket instance.

If a destination pointer is NX_NULL, that particular information is not returned to the caller.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.
udp_packets_sent	Pointer to destination for the total number of UDP packets sent on socket.
udp_bytes_sent	Pointer to destination for the total number of UDP bytes sent on socket.
udp_packets_received	Pointer to destination of the total number of UDP packets received on socket.
udp_bytes_received	Pointer to destination of the total number of UDP bytes received on socket.
udp_packets_queued	Pointer to destination of the total number of queued UDP packets on socket.
udp_receive_packets_dropped	Pointer to destination of the total number of UDP receive packets dropped for socket due to queue size being exceeded.
udp_checksum_errors	Pointer to destination of the total number of UDP packets with checksum errors on socket.

Return Values

NX_SUCCESS	(0x00)	Successful UDP socket information retrieval.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Initialization, threads, and timers

Preemption Possible

No

Example

```
/* Retrieve UDP socket information from socket 0.*/
status =  nx_udp_socket_info_get(&socket_0,
                                 &udp_packets_sent,
                                 &udp_bytes_sent,
                                 &udp_packets_received,
                                 &udp_bytes_received,
                                 &udp_queued_packets,
                                 &udp_receive_packets_dropped,
                                 &udp_checksum_errors);

/* If status is NX_SUCCESS, UDP socket information was retrieved.*/
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_port_get

Pick up port number bound to UDP socket

Prototype

```
UINT nx_udp_socket_port_get(NX_UDP_SOCKET *socket_ptr,
                            UINT *port_ptr);
```

Description

This service retrieves the port number associated with the socket, which is useful to find the port allocated by NetX Duo in situations where the NX_ANY_PORT was specified at the time the socket was bound.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.
port_ptr	Pointer to destination for the return port number. Valid port numbers are (1- 0xFFFF).

Return Values

NX_SUCCESS	(0x00)	Successful socket bind.
NX_NOT_BOUND	(0x24)	This socket is not bound to a port.
NX_PTR_ERROR	(0x07)	Invalid socket pointer or port return pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Get the port number of created and bound UDP socket. */
status = nx_udp_socket_port_get(&udp_socket, &port);

/* If status is NX_SUCCESS, the port variable contains the port this
   socket is bound to. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_receive

Receive datagram from UDP socket

Prototype

```
UINT nx_udp_socket_receive(NX_UDP_SOCKET *socket_ptr,
                           NX_PACKET **packet_ptr,
                           ULONG wait_option);
```

Description

This service receives an UDP datagram from the specified socket. If no datagram is queued on the specified socket, the caller suspends based on the supplied wait option.

If NX_SUCCESS is returned, the application is responsible for releasing the received packet when it is no longer needed.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.
packet_ptr	Pointer to UDP datagram packet pointer.
wait_option	Defines how the service behaves if a datagram is not currently queued on this socket. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket receive.
NX_NOT_BOUND	(0x24)	Socket was not bound to any port.
NX_NO_PACKET	(0x01)	There was no UDP datagram to receive.
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to *tx_thread_wait_abort*.

NX_PTR_ERROR	(0x07)	Invalid socket or packet return pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

No

Example

```
/* Receive a packet from a previously created and bound UDP socket.
   If no packets are currently available, wait for 500 timer ticks
   before giving up. */
status = nx_udp_socket_receive(&udp_socket, &packet_ptr, 500);

/* If status is NX_SUCCESS, the received UDP packet is pointed to by
   packet_ptr. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_receive_notify

Notify application of each received packet

Prototype

```
UINT nx_udp_socket_receive_notify(NX_UDP_SOCKET *socket_ptr,
                                  VOID (*udp_receive_notify)
                                       (NX_UDP_SOCKET *socket_ptr));
```

Description

This service sets the receive notify function pointer to the callback function specified by the application. This callback function is then called whenever a packet is received on the socket. If a NX_NULL pointer is supplied, the receive notify function is disabled.

Parameters

socket_ptr	Pointer to the UDP socket.
udp_receive_notify	Application callback function pointer that is called when a packet is received on the socket.

Return Values

NX_SUCCESS	(0x00)	Successfully set socket receive notify function.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.

Allowed From

Initialization, threads, timers, and ISRs

Preemption Possible

No

Example

```
/* Setup a receive packet callback function for the "udp_socket"
   socket. */
status = nx_udp_socket_receive_notify(&udp_socket,
                                       my_receive_notify);

/* If status is NX_SUCCESS, NetX Duo will call the function named
   "my_receive_notify" whenever a packet is received for
   "udp_socket". */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_send

Send a UDP Datagram

Prototype

```
UINT nx_udp_socket_send(NX_UDP_SOCKET *socket_ptr,
                        NX_PACKET *packet_ptr,
                        ULONG ip_address,
                        UINT port);
```

Description

This service sends a UDP datagram through a previously created and bound UDP socket for IPv4 networks. NetX Duo finds a suitable local IP address as source address based on the destination IP address. To specify a specific interface and source IP address, the application should use the **nxd_udp_socket_source_send** service.

Note that this service returns immediately regardless of whether the UDP datagram was successfully sent. The NetX Duo (IPv4/IPv6) equivalent service is ***nxd_udp_socket_send*****.**

The socket must be bound to a local port.

Parameters

socket_ptr	Pointer to previously created UDP socket instance
packet_ptr	UDP datagram packet pointer
ip_address	Destination IPv4 address
port	Valid destination port number between 1 and 0xFFFF), in host byte order

Return Values

NX_SUCCESS	(0x00)	Successful UDP socket send
NX_NOT_BOUND	(0x24)	Socket not bound to any port
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface can be found.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid server IP address
NX_UNDERFLOW	(0x02)	Not enough room for UDP header in the packet

NX_OVERFLOW	(0x03)	Packet append pointer is invalid
NX_PTR_ERROR	(0x07)	Invalid socket pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	UDP has not been enabled
NX_INVALID_PORT	(0x46)	Port number is not within a valid range

Allowed From

Threads

Preemption Possible

No

Example

```
ULONG  server_address;

/* Set the UDP Client IP address. */
server_address = IP_ADDRESS(1,2,3,5);

/* Send a packet to the UDP server at server_address on port 12. */
status = nx_udp_socket_send(&client_socket, packet_ptr,
                            server_address, 12);

/* If status == NX_SUCCESS, the application successfully transmitted
   the packet out the UDP socket to its peer. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_source_send

Send datagram through UDP socket

Prototype

```
UINT nx_udp_socket_source_send(NX_UDP_SOCKET *socket_ptr,
                               NX_PACKET *packet_ptr,
                               ULONG ip_address,
                               UINT port,
                               UINT address_index);
```

Description

This service sends a UDP datagram through a previously created and bound UDP socket through the network interface with the specified IP address as the source address. Note that service returns immediately, regardless of whether or not the UDP datagram was successfully sent.

nxd_udp_socket_source_send works for both IPv4 and IPv6 networks.

Parameters

socket_ptr	Socket to transmit the packet out on.
packet_ptr	Pointer to packet to transmit.
ip_address	Destination IP address to send packet.
port	Destination port.
address_index	Index of the address associated with the interface to send packet on.

Return Values

NX_SUCCESS	(0x00)	Packet successfully sent.
NX_NOT_BOUND	(0x24)	Socket not bound to a port.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IP address.
NX_NOT_ENABLED	(0x14)	UDP processing not enabled.
NX_PTR_ERROR	(0x07)	Invalid pointer.
NX_OVERFLOW	(0x03)	Invalid packet append pointer.
NX_UNDERFLOW	(0x02)	Invalid packet prepend pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.

NX_INVALID_INTERFACE	(0x4C)	Invalid address index.
NX_INVALID_PORT	(0x46)	Port number exceeds maximum port number.

Allowed From

Threads

Preemption Possible

No

Example

```
#define ADDRESS_INDEX 1
/* Send packet out on port 80 to the specified destination IP on the
   interface at index 1 in the IP task interface list.  */

status = nx_udp_packet_source_send(socket_ptr, packet_ptr,
                                   destination_ip, 80,
                                   ADDRESS_INDEX);

/* If status is NX_SUCCESS packet was successfully transmitted. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_socket_unbind

Unbind UDP socket from UDP port

Prototype

```
UINT nx_udp_socket_unbind(NX_UDP_SOCKET *socket_ptr);
```

Description

This service releases the binding between the UDP socket and a UDP port. Any received packets stored in the receive queue are released as part of the unbind operation.

If there are other threads waiting to bind another socket to the unbound port, the first suspended thread is then bound to the newly unbound port.

Parameters

socket_ptr	Pointer to previously created UDP socket instance.

Return Values

NX_SUCCESS	(0x00)	Successful socket unbind.
NX_NOT_BOUND	(0x24)	Socket was not bound to any port.
NX_PTR_ERROR	(0x07)	Invalid socket pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service.
NX_NOT_ENABLED	(0x14)	This component has not been enabled.

Allowed From

Threads

Preemption Possible

Yes

Example

```
/* Unbind the previously bound UDP socket.  */
status = nx_udp_socket_unbind(&udp_socket);

/* If status is NX_SUCCESS, the previously bound socket is now
   unbound. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nx_udp_source_extract

Extract IP and sending port from UDP datagram

Prototype

```
UINT nx_udp_source_extract(NX_PACKET *packet_ptr,
                           ULONG *ip_address, UINT *port);
```

Description

This service extracts the sender's IP and port number from the IP and UDP headers of the supplied UDP datagram. Note that the service ***nxd_udp_source_extract*** works with packets from either IPv4 or IPv6 network.

Parameters

packet_ptr	UDP datagram packet pointer.
ip_address	Valid pointer to the return IP address variable.
port	Valid pointer to the return port variable.

Return Values

NX_SUCCESS	(0x00)	Successful source IP/port extraction.
NX_INVALID_PACKET	(0x12)	The supplied packet is invalid.
NX_PTR_ERROR	(0x07)	Invalid packet or IP or port destination.

Allowed From

Initialization, threads, timers, ISR

Preemption Possible

No

Example

```
/* Extract the IP and port information from the sender of the UPD
   packet.  */
status = nx_udp_source_extract(packet_ptr, &sender_ip_address,
&sender_port);

/* If status is NX_SUCCESS, the sender IP and port information has
   been stored in sender_ip_address and sender_port respectively.*/
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nxd_icmp_enable

Enable ICMPv4 and ICMPv6 Services

Prototype

```
UINT nxd_icmp_enable(NX_IP *ip_ptr);
```

Description

This service enables both ICMPv4 and ICMPv6 services and can only be called after the IP instance has been created. The service can be enabled either before or after IPv6 is enabled (see *nxd_ipv6_enable*). ICMPv4 services include Echo Request/Reply. ICMPv6 services include Echo Request/Reply, Neighbor Discovery, Duplicate Address Detection, Router Discovery, and Stateless Address Auto-configuration. The IPv4 equivalent in NetX is *nx_icmp_enable*.

i *If the IPv6 address is manually configured prior to enabling ICMPv6, the manually configured IPv6 is not subject to Duplicate Address Detection process.*

nx_icmp_enable starts ICMP services for IPv4 operations only. Applications using ICMPv6 services must use *nxd_icmp_enable* instead of *nx_icmp_enable*.

To utilize IPv6 router solicitation and IPv6 stateless auto-address configuration, ICMPv6 must be enabled.

Parameters

ip_ptr	Pointer to previously created IP instance

Return Values

NX_SUCCESS	(0x00)	ICMP services are successfully enabled
NX_PTR_ERROR	(0x07)	Invalid IP pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/* Enable ICMP on the IP instance.  */
status = nxd_icmp_enable(&ip_0);

/* A status return of NX_SUCCESS indicates that the IP instance is
   enabled for ICMP services. */
```

See Also

nx_icmp_enable, nx_icmp_info_get, nx_icmp_ping, nxd_icmp_ping, nxd_icmp_source_ping, nxd_icmpv6_ra_flag_callback_set

nxd_icmp_ping

Perform ICMPv4 or ICMPv6 Echo Requests

Prototype

```
UINT nxd_icmp_ping(NX_IP *ip_ptr, NXD_ADDRESS *ip_address,
                   CHAR *data_ptr, ULONG data_size,
                   NX_PACKET **response_ptr, ULONG wait_option)
```

Description

This service sends out an ICMP Echo Request packet through an appropriate physical interface and waits for an Echo Reply from the destination host. NetX Duo determines the appropriate interface, based on the destination address, to send the ping message . Applications shall use the service ***nxd_icmp_source_ping*** to specify the physical interface and precise source IP address to use for packet transmission.

The IP instance must have been created, and the ICMPv4/ICMPv6 services must be enabled (see ***nxd_icmp_enable***).

If NX_SUCCESS is returned, the application is responsible for releasing the received packet after it is no longer needed.

Parameters

ip_ptr	Pointer to IP instance
ip_address	Destination IP address to ping, in host byte order
data_ptr	Pointer to ping packet data area
data_size	Number of bytes of ping data
response_ptr	Pointer to response packet pointer
wait_option	Time to wait for a reply. The wait options are defined as follows: NX_NO_WAIT (0x00000000) timeout value in ticks (0x00000001 through 0xFFFFFFFE) NX_WAIT_FOREVER 0xFFFFFFFF

Return Values

NX_SUCCESS	(0x00)	Successful sent and received ping
NX_NOT_SUPPORTED	(0x4B)	IPv6 is not enabled
NX_OVERFLOW	(0x03)	Ping data exceeds packet payload
NX_NO_RESPONSE	(0x29)	Destination host did not respond
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by tx_thread_wait_abort
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface can be found.
NX_PTR_ERROR	(0x07)	Invalid IP or response pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	IP or ICMP component is not enabled
NX_IP_ADDRESS_ERROR	(0x21)	Input IP address is invalid

Allowed From

Threads

Preemption Possible

No

Example

```
/* The following two examples illustrate how to use this API to send
   ping packets to IPv6 or IPv4 destinations.  */

/* The first example:  Send a ping packet to an IPv6 host
   2001:1234:5678::1 */

/* Declare variable address to hold the destination address. */
NXD_ADDRESS  ip_address;

char *buffer = "abcd";
UINT  prefix_length = 10;

/* Set the IPv6 address. */
ip_address.nxd_ip_address_version   = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0]     = 0x20011234;
ip_address.nxd_ip_address.v6[1]     = 0x56780000;
ip_address.nxd_ip_address.v6[2]     = 0;
ip_address.nxd_ip_address.v6[3]     = 1;

status = nxd_icmp_ping(&ip_0, &ip_address, buffer,
                       strlen(buffer),&response_ptr,
                       NX_WAIT_FOREVER);

/* A return value of NX_SUCCESS indicates a ping reply has been
   received from IP address 2001:1234:5678::1 and the response
   packet is contained in the packet pointed to by response_ptr.It
   should have the same "abcd" four bytes of data. */

/* The second example: Send a ping packet to an IPv4 host 1.2.3.4 */

/* Program the IPv4 address. */
ip_address.nxd_ip_address_version   = NX_IP_VERSION_V4;
ip_address.nxd_ip_address.v4[0]     = 0x01020304;

status = nxd_icmp_ping(&ip_0, &ip_address, buffer,
                       strlen(buffer),&response_ptr, 10);

/* A return value of NX_SUCCESS indicates a ping reply was received
   from IP address 1.2.3.4 and the response packet is contained in
   the packet pointed to by response_ptr. It should have the same
   "abcd" four bytes of data. */
```

See also

nx_icmp_enable, nx_icmp_info_get, nx_icmp_ping, nxd_icmp_enable, nxd_icmp_source_ping, nxd_icmpv6_ra_flag_callback_set

nxd_icmp_source_ping

Perform ICMPv4 or ICMPv6 Echo Requests

Prototype

```
UINT nxd_icmp_source_ping(NX_IP *ip_ptr, NXD_ADDRESS *ip_address,
                          UINT address_index,
                          CHAR *data_ptr, ULONG data_size,
                          NX_PACKET **response_ptr,
                          ULONG wait_option);
```

Description

This service sends out an ICMP Echo Request packet using the specified index of an IPv4 or IPv6 address, and through the network interface the source address is associated with, and waits for an Echo Reply from the destination host. This service works with both IPv4 and IPv6 addresses. The parameter *address_index* indicates the source IPv4 or IPv6 address to use. For IPv4 address, the *address_index* is the same index to the attached network interface. For IPv6, the *address_index* indicates the entry in the IPv6 address table.

The IP instance must have been created, and the ICMPv4 and ICMPv6 services must be enabled (see *nxd_icmp_enable*).

! *If NX_SUCCESS is returned, the application is responsible for releasing the received packet after it is no longer needed.*

Parameters

ip_ptr	Pointer to IP instance
ip_address	Destination IP address to ping, in host byte order
address_index	Indicates the IP address to use as source address
data_ptr	Pointer to ping packet data area
data_size	Number of bytes of ping data
response_ptr	Pointer to response packet pointer

wait_option	Time to wait for a reply. The wait options are defined as follows: NX_NO_WAIT (0x00000000) timeout value in ticks (0x00000001 through 0xFFFFFFFE NX_WAIT_FOREVER 0xFFFFFFFF)

Return Values

NX_SUCCESS	(0x00)	Successful sent and received ping
NX_NOT_SUPPORTED	(0x4B)	IPv6 is not enabled
NX_OVERFLOW	(0x03)	Ping data exceeds packet payload
NX_NO_RESPONSE	(0x29)	Destination host did not respond
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by *tx_thread_wait_abort*
NX_NO_INTERFACE_ADDRESS		
	(0x50)	No suitable outgoing interface can be found
NX_PTR_ERROR	(0x07)	Invalid IP or response pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	IP or ICMP component is not enabled
NX_IP_ADDRESS_ERROR	(0x21)	Input IP address is invalid

Allowed From

Threads

Preemption Possible

No

Example

```
/* The following two examples illustrate how to use this API to send ping
   packets to IPv6 or IPv4 destinations.  */

/* The first example:  Send a ping packet to an IPv6 host
   FE80::411:7B23:40dc:f181 */

/* Declare variable address to hold the destination address. */

#define PRIMARY_INTERFACE 0
#define GLOBAL_IPv6_ADDRESS  1

NXD_ADDRESS  ip_address;
char *buffer = "abcd";
UINT  prefix_length = 10;

/* Set the IPv6 address. */
ip_address.nxd_ip_address_version   = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0]     = 0xFE800000;
ip_address.nxd_ip_address.v6[1]     = 0x00000000;
ip_address.nxd_ip_address.v6[2]     = 0x04117B23;
ip_address.nxd_ip_address.v6[3]     = 0x40DCF181;

status = nxd_icmp_source_ping(&ip_0, &ip_address,
                              GLOBAL_IPv6_ADDRESS,
                              buffer,
                              strlen(buffer),
                              &response_ptr,
                              NX_WAIT_FOREVER);

/* A return value of NX_SUCCESS indicates a ping reply has been received
   from IP address FE80::411:7B23:40dc:f181 and the response packet is
   contained in the packet pointed to by response_ptr.  It should have the
   same "abcd" four bytes of data. */

/* The second example:  Send a ping packet to an IPv4 host 1.2.3.4 */

/* Program the IPv4 address. */
ip_address.nxd_ip_address_version   = NX_IP_VERSION_V4;
ip_address.nxd_ip_address.v4        = 0x01020304;

status = nxd_icmp_source_ping(&ip_0, &ip_address,
                             PRIMARY_INTERFACE,
                             buffer,
                             strlen(buffer),
                             &response_ptr,
                             NX_WAIT_FOREVER);

/* A return value of NX_SUCCESS indicates a ping reply was received from
   IP address 1.2.3.4 and the response packet is contained in the packet
   pointed to by response_ptr. It should have the same "abcd" four bytes
   of data. */
```

See also

nx_icmp_enable, nx_icmp_info_get, nx_icmp_ping, nxd_icmp_enable, nxd_icmp_ping, nxd_icmpv6_ra_flag_callback_set

nxd_icmpv6_ra_flag_callback_set

Set the ICMPv6 RA flag change callback function

Prototype

```
UINT nxd_icmpv6_ra_flag_callback_set(NX_IP *ip_ptr, VOID(*ra_call-
                                     back) (NX_IP*ip_ptr, UINT ra_-
                                     flag))
```

Description

This service sets the ICMPv6 Router Advertisement flag change callback function. The user-supplied callback function is invoked when NetX Duo receives a router advertisement message.

Parameters

ip_ptr	Pointer to IP instance
ra_callback	User-supplied callback function

Return Values

NX_SUCCESS	(0x00)	Successful set the RA flag callback function
NX_NOT_SUPPORTED	(0x4B)	IPv6 is not enabled
NX_PTR_ERROR	(0x07)	Invalid IP
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
VOID icmpv6_ra_flag_callback(NX_IP *ip_ptr, UINT ra_flag)
{

   /* RA flag has changed. The updated value is passed in via the
      ra_flag parameter. */

}


/* Configure the user-defined ICMPv6 RA flag change callback
      function. */
status = nxd_icmpv6_ra_flag_callback_set(&ip_0,
                                          icmpv6_ra_flag_callback);



/* A status return of NX_SUCCESS indicates the callback function has
   been successfully configured. */
```

See Also

nx_icmp_enable, nx_icmp_info_get, nx_icmp_ping, nxd_icmp_enable, nxd_icmp_ping, nxd_icmp_source_ping

nxd_ip_raw_packet_send

Send Raw IP Packet

Prototype

```
UINT nxd_ip_raw_packet_send(NX_IP *ip_ptr, NX_PACKET *packet_ptr,
                            NXD_ADDRESS *destination_ip,
                            ULONG protocol, UINT ttl, ULONG tos)
```

Description

This service sends a raw IPv4 or IPv6 packet (no transport-layer protocol headers). On a multihome system, if the system is unable to determine an appropriate interface (for example, if the destination IP address is IPv4 broadcast, multicast or IPv6 multicast address), the primary device is selected. The service ***nxd_ip_raw_packet_source_send*** can be used to specify an outgoing interface. The NetX equivalent is ***nx_ip_raw_packet_send*****.**

The IP instance must be previously created and raw IP packet handling must be enabled using the ***nx_ip_raw_packet_enable*** service.

Parameters

ip_ptr	Pointer to the previously created IP instance
packet_ptr	Pointer to packet to transmit
destination_ip	Pointer to destination address
protocol	Packet protocol stored to the IP header
ttl	Value for TTL or hop limit
tos	Value for TOS or traffic class and flow label

Return Value

NX_SUCCESS	(0x00)	Raw IP packet successfully sent
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface can be found
NX_NOT_ENABLED	(0x14)	Raw IP handling not enabled
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IPv4 or IPv6 address
NX_UNDERFLOW	(0x02)	Not enough room for IPv4 or IPv6 header in the packet
NX_OVERFLOW	(0x03)	Packet append pointer is invalid
NX_PTR_ERROR	(0x07)	Invalid IP pointer or packet pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_PARAMETERS	(0x4D)	Not valid IPv6 address input

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  dest_address;

/* Set the destination address,in this case an IPv6 address. */
dest_address.nxd_ip_address_version   = NX_IP_VERSION_V6;
dest_address.nxd_ip_address.v6[0]     = 0x20011234;
dest_address.nxd_ip_address.v6[1]     = 0x56780000;
dest_address.nxd_ip_address.v6[2]     = 0;
dest_address.nxd_ip_address.v6[3]     = 1;

UINT ttl, tos;

ttl = 128;

tos = 0;

/* Enable RAW IP handling on the previously created IP instance.*/
status = nx_raw_ip_packet_enable(&ip_0);

/* Allocate a packet pointed to by packet_ptr from the IP packet
   pool. */
/* Then transmit the packet to the destination address. */

status = nxd_ip_raw_packet_send(&ip_0, packet_ptr,  dest_address,
                                NX_PROTOCOL_UDP, ttl, tos);

/* A status return of NX_SUCCESS indicates the packet was
   successfully transmitted. */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_source_send

nxd_ip_raw_packet_source_send

Send raw packet using specified source address

Prototype

```
UINT nxd_ip_raw_packet_source_send(NX_IP *ip_ptr,
                                   NX_PACKET *packet_ptr,
                                   NXD_ADDRESS *destination_ip,
                                   UINT address_index,
                                   ULONG protocol,
                                   UINT ttl,
                                   ULONG tos)
```

Description

This service sends a raw IPv4 or IPv6 packet using the specified IPv4 or IPv6 address as source address. This service is typically used on a multihome system, if the system is unable to determine an appropriate interface (for example, if the destination IP address is IPv4 broadcast, multicast or IPv6 multicast address). The parameter *address_index* allows the application to specify the source address to use when sending this raw packet.

The IP instance must be previously created and raw IP packet handling must be enabled using the ***nx_ip_raw_packet_enable*** service.

Parameters

ip_ptr	IP instance pointer
packet_ptr	Pointer to packet to send
destination_ip	Destination IP address
address_index	Index to the IPv4 or IPv6 addresses to use as source address.
protocol	Value for the protocol field
ttl	Value for ttl or hop limit
tos	Value for tos or traffic class and flow label

Return Values

NX_SUCCESS	(0x00)	Packet is sent successfully
NX_UNDERFLOW	(0x02)	Not enough room for IPv4 or IPv6 header in the packet
NX_OVERFLOW	(0x03)	Packet append pointer is invalid

NX_PTR_ERROR	(0x07)	Invalid pointer to IP control block, packet, or destination_ip
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	Raw processing not enabled
NX_IP_ADDRESS_ERROR	(0x21)	Address error
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index
NX_INVALID_PARAMETERS	(0x4D)	Not valid IPv6 address input

Allowed From

Thread

Preemption Possible

No

Example

```
#define SOURCE_ADDRESS_INDEX 2
/* Send a raw packet from specified interface. */
status = nxd_ip_raw_packet_source_send(&ip_0, packet_ptr,
                                       dest_ip,
                                       SOURCE_ADDRESS_INDEX,
                                       NX_IP_RAW,
                                       NX_IP_TIME_TO_LIVE,
                                       NX_IP_NORMAL);

/* If status == NX_SUCCESS, raw packet has been sent out on the
    specified interface. */
```

See Also

nx_ip_raw_packet_disable, nx_ip_raw_packet_enable, nx_ip_raw_packet_filter_set, nx_ip_raw_packet_receive, nx_ip_raw_packet_send, nx_ip_raw_packet_source_send, nx_ip_raw_receive_queue_max_set, nxd_ip_raw_packet_send

nxd_ipv6_address_change_notify

Set ipv6 address change notify

Prototype

```
UINT nxd_ipv6_address_change_notify(NX_IP *ip_ptr,
                 VOID (*ip_address_change_notify)(NX_IP *, UINT, UINT,
                                                  UINT, ULONG *))
```

Description

This service registers an application callback routine that NetX Duo calls whenever the IPv6 Address is changed.

This service is available if the NetX Duo library is built is the option ***NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY*** defined.

Parameters

ip_ptr	IP control block pointer
ip_address_change_notify	Application callback function

Return Values

NX_SUCCESS	(0x00)	Successful set
NX_NOT_SUPPORTED	(0x4B)	IPv6 address change notify feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	IPv6 address change notify is not compiled

Allowed From

Thread

Preemption Possible

No

Example

```
VOID ip_address_change_notify(NX_IP *ip_ptr, UINT status,
                              UINT interface_index,
                              UINT address_index,
                              ULONG *ip_address)
{

    /* Do something when ip address changed. */
}

void ip_address_thread_entry(ULONG id)
{

    /* Set the ip address change notify of IP instance. */
    status = nxd_ipv6_address_change_notify (&ip_0,

    ip_address_change_nofity);

/* If status == NX_SUCCESS, the ip address change notify of IP
   instance was successfully set. */
}
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_address_delete

Delete IPv6 Address

Prototype

```
UINT nxd_ipv6_address_delete(NX_IP *ip_ptr, UINT address_index);
```

Description

This service deletes the IPv6 address at the specified index in the IPv6 address table of the specified IP instance. There is no NetX equivalent.

Parameters

ip_ptr	Pointer to the previously created IP instance
address_index	Index to IP instance IPv6 address table

Return Values

NX_SUCCESS	(0x00)	Address successfully deleted
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface can be found
NX_PTR_ERROR	(0x07)	Invalid IP pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
NXD_ADDRESS ip_address;
UINT        address_index;

/* Delete the IPv6 address at the specified address table index.  */
address_index = 1;
status = nxd_ipv6_address_delete(&ip_0, address_index);

/* A status return of NX_SUCCESS indicates that the IP instance
   address is successfully deleted. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_address_get

Retrieve IPv6 Address and Prefix

Prototype

```
UINT nxd_ipv6_address_get(NX_IP *ip_ptr, UINT
                          address_index, NXD_ADDRESS
                          *ip_address,
                          ULONG *prefix_length,
                          UINT *interface_index);
```

Description

This service retrieves the IPv6 address and prefix at the specified index in the address table of the specified IP instance. The index of the physical interface the IPv6 address is associated with is returned in the *interface_index* pointer. The NetX equivalent services are ***nx_ip_address_get*** and ***nx_ip_interface_address_get***.

Parameters

ip_ptr	Pointer to the previously created IP instance
address_index	Index to IP instance address table
ip_address	Pointer to the address to set
prefix_length	Length of the address prefix (subnet mask)
interface_index	Pointer to the index of the interface

Return Values

NX_SUCCESS	(0x00)	IPv6 is successfully enabled
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_NO_INTERFACE_ADDRESS	(0x50)	No interface address, or invalid address_index
NX_PTR_ERROR	(0x07)	Invalid IP pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
NXD_ADDRESS ip_address;
UINT        address_index;
ULONG       prefix_length;
UINT        interface_index;

/* Get the IPv6 address at the specified address table index. If
   found, the address network interface is returned in the
   interface_index input, as well as the address prefix in the
   prefix_length input.  */

address_index = 1;
status = nxd_ipv6_address_get(&ip_0, address_index, &ip_address,
                              &prefix_length, &interface_index);

/* A status return of NX_SUCCESS indicates that the IP instance
   address is successfully retrieved. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_address_set

Set IPv6 Address and Prefix

Prototype

```
UINT nxd_ipv6_address_set(NX_IP *ip_ptr, UINT interface_index,
                          NXD_ADDRESS *ip_address,
                          ULONG prefix_length,
                          UINT *address_index);
```

Description

This service sets the supplied IPv6 address and prefix to the specified IP instance. If the *address_index* argument is not null, the index into the IPv6 address table where the address is inserted is returned. The NetX equivalent services are ***nx_ip_address_set*** and ***nx_ip_interface_address_set***.

Parameters

ip_ptr	Pointer to the previously created IP instance
interface_index	Index to the interface the IPv6 address is associated with
ip_address	Pointer to the address to set
prefix_length	Length of the address prefix (subnet mask)
address_index	Pointer to the index into the address table where the address is inserted

Return Values

NX_SUCCESS	(0x00)	IPv6 is successfully enabled
NX_NO_MORE_ENTRIES	(0x15)	IP address table is full
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_DUPLICATED_ENTRY	(0x52)	The supplied IP address is already used on this IP instance
NX_PTR_ERROR	(0x07)	Invalid IP pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IPv6 address
NX_INVALID_INTERFACE	(0x4C)	Interface points to an invalid network interface

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
NXD_ADDRESS ip_address;
UINT        address_index;
UINT        interface_index;

ip_address.nxd_ip_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0] = 0x20010000;
ip_address.nxd_ip_address.v6[1] = 0;
ip_address.nxd_ip_address.v6[2] = 0;
ip_address.nxd_ip_address.v6[3] = 1;

/* First create an IP instance with packet pool, source address, and
   driver.*/
status = nx_ip_create(&ip_0, "NetX IP Instance 0",
                      IP_ADDRESS(1,2,3,4),
                      0xFFFFFF00UL, &pool_0,_nx_ram_network_driver,
                      pointer, 2048, 1);

/* Then enable IPv6 on the IP instance. */
status = nxd_ipv6_enable(&ip_0);

/* Set the IPv6 address (a global address as indicated by the 64 bit
   prefix) using the IPv6 address just created on the primary device
   (index zero). The index into the address table is returned in
   address_index. */
interface_index = 0;
status = nxd_ipv6_address_set(&ip_0, interface_index, &ip_address,
                               64,&address_index);

/* A status return of NX_SUCCESS indicates that the IPv6 address is
   successfully assigned to the primary interface (interface 0). */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_default_router_add

Add an IPv6 Router to Default Router Table

Prototype

```
UINT nxd_ipv6_default_router_add(NX_IP *ip_ptr,
                                 NXD_ADDRESS *router_address,
                                 ULONG router_lifetime,
                                 UINT index_index);
```

Description

This service adds an IPv6 default router on the specified physical interface to the default router table. The equivalent NetX IPv4 service is ***nx_ip_gateway_address_set***.

router_address must point to a valid IPv6 address, and the router must be directly accessible from the specified physical interface.

Parameters

ip_ptr	Pointer to previously created IP instance
router_address	Pointer to the default router address, in host byte order
router_lifetime	Default router life time, in seconds. Valid values are: 0xFFFF: No time out 0-0xFFFE: Timeout value, in seconds
index_index	Pointer to the valid memory location for the network index index through which the router can be reached

Return Values

NX_SUCCESS	(0x00)	Default router is successfully added
NX_NO_MORE_ENTRIES	(0x17)	No more entries available in the default router table.
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IPv6 address
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.

NX_INVALID_PARAMETERS	(0x4D)	Not valid IPv6 address input
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_INTERFACE	(0x4C)	Invalid router interface index

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/* This example adds a default router for the primary interface at
   fe80::1219:B9FF:FE37:ac to the default router table. */

#define PRIMARY_INTERFACE 0

NXD_ADDRESS  router_address;

/* Set the router address version to IPv6 */
router_address.nxd_ip_version    = NX_IP_VERSION_V6;

/* Set the IPv6 address, in host byte order. */
router_address.nxd_ip_address[0] = 0xfe800000;
router_address.nxd_ip_address[1] = 0x0;
router_address.nxd_ip_address[2] = 0x1219B9FF;
router_address.nxd_ip_address[3] = 0xFE3700AC;

/* Set IPv6 default router. */
status = nxd_ipv6_default_router_add(ip_ptr, &router_address,
                                      0xFFFF, PRIMARY_INTERFACE);

/* Unless invalid pointer input is detected by the error checking
   Service, status return is always NX_SUCCESS. */
```

See also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nxd_ipv6_default_router_delete

Remove IPv6 Router from Default Router Table

Prototype

```
UINT nxd_ipv6_default_router_delete (NX_IP *ip_ptr,
                                     NXD_ADDRESS *router_address);
```

Description

This service deletes an IPv6 default router from the default router table. The equivalent NetX IPv4 service is ***nx_ip_gateway_address_clear***.

Restrictions

The IP instance has been created. *router_address* must point to valid information.

Parameters

ip_ptr	Pointer to a previously created IP instance
router_address	Pointer to the IPv6 default gateway address

Return Values

NX_SUCCESS	(0x00)	Router successfully deleted
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_NOT_FOUND	(0x4E)	The router entry cannot be found
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_PARAMETERS	(0x82)	Invalid non pointer input

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/*This example removes a default router:fe80::1219:B9FF:FE37:ac */

NXD_ADDRESS  router_address;

/* Set the router_address version to IPv6 */
router_address.nxd_ip_version    = NX_IP_VERSION_V6;

/* Program the IPv6 address, in host byte order. */
router_address.nxd_ip_address[0] = 0xfe800000;
router_address.nxd_ip_address[1] = 0x0;
router_address.nxd_ip_address[2] = 0x1219B9FF;
router_address.nxd_ip_address[3] = 0xFE3700AC;

/* Delete the IPv6 default router. */
nxd_ipv6_default_router_delete(ip_ptr, &router_address);
```

See also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nxd_ipv6_default_router_entry_get

Get default router entry

Prototype

```
UINT nxd_ipv6_default_router_entry_get(NX_IP *ip_ptr,
                                       UINT interface_index,
                                       UINT entry_index,
                                       NXD_ADDRESS *router_addr,
                                       ULONG *router_lifetime,
                                       ULONG *prefix_length,
                                       ULONG *configuration_method)
```

Description

This service retrieves a router entry from the default IPv6 routing table that is attached to a specified network device.

Parameters

ip_ptr	IP control block pointer
interface_index	Index of the network interface
entry_index	Entry Index
router_addr	Router IPv6 Address
router_lifetime	Pointer to router life time
prefix_length	Pointer to prefix length
configuration_method	Pointer to the information on how the entry was configured

Return Values

NX_SUCCESS	(0x00)	Successful get
NX_NOT_FOUND	(0x4E)	Router entry not found
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
NXD_ADDRESS            router_addr;
ULONG                  router_lifetime;
ULONG                  prefix_length;
ULONG                  configuration_method;

/* Get the router entry of specified interface. */
status = nxd_ipv6_default_router_entry_get (&ip_0,
                                            PRIMARY_INTERFACE,
                                            entry_index,
                                            &router_addr,
                                            &router_lifetime,
                                            &prefix_length,
                                            &configuration_method);

/* If status == NX_SUCCESS, the router entry was successfully
   got. */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_get, nxd_ipv6_default_router_number_of_entries_get

nxd_ipv6_default_router_get

Retrieve an IPv6 Router from Default Router Table

Prototype

```
UINT nxd_ipv6_default_router_get(NX_IP *ip_ptr, UINT interface_in-
                                 dex
                                 NXD_ADDRESS *router_address,
                                 ULONG *router_lifetime,
                                 ULONG *prefix_length);
```

Description

This service retrieves an IPv6 default router address, lifetime and prefix length on the specified physical interface from the default router table. The equivalent NetX IPv4 service is ***nx_ip_gateway_address_get*.**

router_address must point to a valid NXD_ADDRESS structure, so this service can fill in the IPv6 address of the default router.

Parameters

ip_ptr	Pointer to previously created IP instance
interface_index	The index to the network interface that the router is accessible through
router_address	Pointer to the storage space for the return value of the default router address, in host byte order.
router_lifetime	Pointer to the router lifetime
prefix_length	Pointer to the router address prefix length

Return Values

NX_SUCCESS	(0x00)	Default router is successfully added
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_NOT_FOUND	(0x4E)	Default router not found
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_INTERFACE	(0x4C)	Invalid router interface index
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/* This example retrieves a default router for the primary device from the
   default router table. */

#define PRIMARY_INTERFACE 0


NXD_ADDRESS  router_address;
ULONG        router_lifetime;
ULONG        prefix_length;

/* Get IPv6 default router. */
status = nxd_ipv6_default_router_get(ip_ptr, PRIMARY_INTERFACE,
                                     &router_address, &router_lifetime,
                                     &prefix_length);

/* If status returns NX_SUCCESS, the router address and related information
   is returned successfully. */
```

See also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_number_of_entries_get

nxd_ipv6_default_router_number_of_entries_get

Get number of default IPv6 routers

Prototype

```
UINT nxd_ipv6_default_router_number_of_entries_get(NX_IP *ip_ptr,
                                                   UINT   interface_index,
                                                   UINT  *num_entries)
```

Description

This service retrieves the number of IPv6 default routers configured on a given network interface.

Parameters

ip_ptr	IP control block pointer
interface_index	Index of the network interface
num_entries	Destination for number of IPv6 routers on a specified network device

Return Values

NX_SUCCESS	(0x00)	Successful get
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_INVALID_INTERFACE	(0x4C)	Device index value is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer or *num_entries* pointer

Allowed From

Thread

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
UINT                   num_entries;

/* Get the router entries of specified interface. */
status = nxd_ipv6_default_router_number_of_entries_get(&ip_0,

    PRIMARY_INTERFACE,

    &num_entries);

/* If status == NX_SUCCESS, the router entries was successfully
   retrieved. */
```

See Also

nx_ip_gateway_address_clear, nx_ip_gateway_address_get, nx_ip_gateway_address_set, nx_ip_info_get, nx_ip_static_route_add, nx_ip_static_route_delete, nxd_ipv6_default_router_add, nxd_ipv6_default_router_delete, nxd_ipv6_default_router_entry_get, nxd_ipv6_default_router_get

nxd_ipv6_disable

Disable the IPv6 feature

Prototype

```
UINT nxd_ipv6_disable(NX_IP *ip_ptr)
```

Description

This service disables the IPv6 for the specified IP instance. It also clears the default router table, ND cache and IPv6 address table, leaves the all multicast groups, and resets the router solicitation variables. This service has no effect if IPv6 is not enabled.

Parameters

ip_ptr	IP instance pointer

Return Values

NX_SUCCESS	(0x00)	Successful disable
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_NOT_SUPPORT	(0x4B)	IPv6 module is not compiled
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* Disable IPv6 feature on this IP instance. */
status = nxd_ipv6_disable(&ip_0);

/* If status == NX_SUCCESS, disables IPv6 feature on IP instance.*/
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_enable

Enable IPv6 Services

Prototype

```
UINT nxd_ipv6_enable(NX_IP *ip_ptr);
```

Description

This service enables IPv6 services. When the IPv6 services are enabled, the IP instance joins the all-node multicast group (FF02::1). This service does not set the link local address or global address. Applications should use *nxd_ipv6_address_set* to configure the device network addresses. There is no NetX equivalent.

Parameters

ip_ptr	Pointer to the previously created IP instance

Return Values

NX_SUCCESS	(0x00)	IPv6 is successfully enabled
NX_ALREADY_ENABLED	(0x15)	IPv6 is already enabled
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library.
NX_PTR_ERROR	(0x07)	Invalid IP pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/* First create an IP instance with packet pool, source address, and
   driver.*/
status = nx_ip_create(&ip_0, "NetX IP Instance 0",
                      IP_ADDRESS(1,2,3,4),
                      0xFFFFFF00UL, &pool_0,_nx_ram_network_driver,
                      pointer, 2048, 1);

/* Then enable IPv6 on the IP instance. */
status = nxd_ipv6_enable(&ip_0);

/* A status return of NX_SUCCESS indicates that the IP instance is
   enabled for IPv6 services. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_stateless_address_autoconfig_disable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_multicast_interface_join

Join an IPv6 multicast group

Prototype

```
UINT nxd_ipv6_multicast_interface_join(NX_IP *ip_ptr,
                                       NXD_ADDRESS *group_address,
                                       UINT interface_index)
```

Description

This service allows an application to join a specific IPv6 multicast address on a specific network interface. The link driver is notified to add the multicast address. This service is available if the NetX Duo library is built with the option ***NX_ENABLE_IPV6_MULTICAST*** defined.

Parameters

ip_ptr	IP instance pointer
group_address	IPv6 multicast address
interface_index	The index to the network interface associated with the multicast group

Return Values

NX_SUCCESS	(0x00)	Successfully enables receiving on IPv6 multicast address
NX_NO_MORE_ENTRIES	(0x17)	No more entries in the IPv6 multicast table.
NX_OVERFLOW	(0x03)	No more group addresses available in the device driver
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature or IPv6 multicast feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IPv6 address
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid

Allowed From

Threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
/* Join multicast group on this IP instance. */
status = nxd_ipv6_multicast_interface_join(&ip_0,
                                           &group_address,
                                           PRIMARY_INTERFACE);

/* If status == NX_SUCCESS, interface of index on IP instance
   has joined the multicast group. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_leave

nxd_ipv6_multicast_interface_leave

Leave an IPv6 multicast group

Prototype

```
UINT nxd_ipv6_multicast_interface_leave(NX_IP *ip_ptr,
                                         NXD_ADDRESS *group_address,
                                        UINT interface_index)
```

Description

This service removes the specific IPv6 multicast address from the specific network device. The link driver is also notified of the removal of the IPv6 multicast address.This service is available if the NetX Duo library is built with the option ***NX_ENABLE_IPV6_MULTICAST*** defined.

Parameters

ip_ptr	IP instance pointer
group_address	IPv6 multicast address
interface_index	The index to the network interface associated with group

Return Values

NX_SUCCESS	(0x00)	Successful multicast leave
NX_ENTRY_NOT_FOUND	(0x16)	Entry not found
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature or IPv6 multicast feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_IP_ADDRESS_ERROR	(0x21)	Invalid IPv6 address
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid

Allowed From

Threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
/* Leave multicast address on this IP instance. */
status = nxd_ipv6_multicast_interface_leave(&ip_0,
                                            &group_address,
                                            primary_interface);

/* If status == NX_SUCCESS, interface of index on IP instance
   has left the multicast group. */
```

See Also

nx_igmp_enable, nx_igmp_info_get,nx_igmp_loopback_disable, nx_igmp_loopback_enable, nx_igmp_multicast_interface_join, nx_igmp_multicast_join, nx_igmp_multicast_interface_leave, nx_igmp_multicast_leave, nx_ipv4_multicast_interface_join, nx_ipv4_multicast_interface_leave, nxd_ipv6_multicast_interface_join

nxd_ipv6_stateless_address_autoconfig_disable

Disable stateless address autoconfiguration

Prototype

```
UINT nxd_ipv6_stateless_address_autoconfig_disable(NX_IP *ip_ptr,
                                                   UINT interface_index)
```

Description

This service disables the IPv6 stateless address auto configuration feature on a specified network device. It has no effect if the IPv6 address has been configured.

This service is available if the NetX Duo library is built with the option ***NX_IPV6_STATELESS_AUTOCONFIG_CONTROL*** defined.

Parameters

ip_ptr	IP instance pointer
interface_index	The index to the network interface that the IPv6 stateless address autoconfiguration should be disabled.

Return Values

NX_SUCCESS	(0x00)	Successfully disables stateless address autoconfigure feature.
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature or IPv6 stateless address autoconfig control feature is not built into the NetX Duo library
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE 0
/* Disable stateless address auto configuration on this IP instance. */
status = nxd_ipv6_stateless_address_autoconfig_disable(&ip_0,
                                                         PRIMARY_INTERFACE);

/* If status == NX_SUCCESS, disables stateless address auto
   configuration on IP instance. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_enable

nxd_ipv6_stateless_address_autoconfig_enable

Enable stateless address autoconfiguration

Prototype

```
UINT nxd_ipv6_stateless_address_autoconfig_enable(NX_IP *ip_ptr,
                                                  UINT interface_index)
```

Description

This service enables the IPv6 stateless address auto configuration feature on a specified network device.

This service is available if the NetX Duo library is built with the option ***NX_IPV6_STATELESS_AUTOCONFIG_CONTROL*** defined.

Parameters

ip_ptr	IP instance pointer
interface_index	The index to the network interface that the IPv6 stateless address autoconfiguration should be enabled.

Return Values

NX_SUCCESS	(0x00)	Successfully enables stateless address autoconfig feature.
NX_ALREADY_ENABLED	(0x15)	Already enabled
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature or IPv6 stateless address autoconfig control feature is not built into the NetX Duo library
NX_INVALID_INTERFACE	(0x4C)	Interface index is not valid
NX_PTR_ERROR	(0x07)	Invalid IP control block pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
#define PRIMARY_INTERFACE
/* Enable stateless address auto configuration on this
   IP instance. */
status = nxd_ipv6_stateless_address_autoconfig_enable(&ip_0,

    PRIMARY_INTERFACE);

/* If status == NX_SUCCESS, enables stateless address auto
   configuration on IP instance. */
```

See Also

nx_ip_auxiliary_packet_pool_set, nx_ip_address_change_notify, nx_ip_address_get, nx_ip_address_set, nx_ip_create, nx_ip_delete, nx_ip_driver_direct_command, nx_ip_driver_interface_direct_command, nx_ip_forwarding_disable, nx_ip_forwarding_enable, nx_ip_fragment_disable, nx_ip_fragment_enable, nx_ip_info_get, nx_ip_max_payload_size_find, nx_ip_status_check, nx_system_initialize, nxd_ipv6_address_change_notify, nxd_ipv6_address_delete, nxd_ipv6_address_get, nxd_ipv6_address_set, nxd_ipv6_disable, nxd_ipv6_enable, nxd_ipv6_stateless_address_autoconfig_disable

nxd_nd_cache_entry_delete

Delete IPv6 Address entry in the Neighbor Cache

Prototype

```
UINT nxd_nd_cache_entry_delete(NX_IP *ip_ptr, ULONG *ip_address)
```

Description

This service deletes an IPv6 neighbor discovery cache entry for the supplied IP address. The equivalent NetX IPv4 function is ***nx_arp_static_entry_delete***.

Parameters

ip_ptr	Pointer to previously created IP instance
ip_address	Pointer to IPv6 address to delete, in host byte order

Return Values

NX_SUCCESS	(0x00)	Successfully deleted the address
NX_ENTRY_NOT_FOUND	(0x16)	Address not found in the IPv6 neighbor cache
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Initialization, threads

Preemption Possible

No

Example

```
/* This example deletes an entry from the neighbor cache table. */

NXD_ADDRESS ip_address;

ip_address.nxd_ip_address_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0]   = 0x20011234;
ip_address.nxd_ip_address.v6[1]   = 0x56780000;
ip_address.nxd_ip_address.v6[2]   = 0;
ip_address.nxd_ip_address.v6[3]   = 1;


/* Delete an entry in the neighbor cache table with the specified
   IPv6 address and hardware address. */
status = nxd_nd_cache_entry_delete(&ip_0,

 &ip_address.nxd_ip_address.v6[0]);

/* If status == NX_SUCCESS, the entry was deleted from the neighbor
   cache table. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nxd_nd_cache_entry_set

Add an IPv6 Address/MAC Mapping to Neighbor Cache

Prototype

```
UINT nxd_nd_cache_entry_set(NX_IP *ip_ptr, NXD_ADDRESS *dest_ip,
                            UINT interface_index, char *mac);
```

Description

This service adds an entry to the neighbor discovery cache for the specified IP address *ip_address* mapped to the hardware MAC address on the specified network interface index (interface_index). The equivalent NetX IPv4 service is ***nx_arp_static_entry_create***.

Parameters

ip_ptr	Pointer to previously created IP instance
dest_ip	Pointer to IPv6 address instance
interface_index	Index specifying physical network interface where the destination IPv6 address can be reached
mac	Pointer to hardware address.

Return Values

NX_SUCCESS	(0x00)	Entry successfully added
NX_NOT_SUCCESSFUL	(0x43)	Invalid cache or no neighbor cache entries available
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index value.

Allowed From

Initialization, Threads

Preemption Possible

No

Example

```
/* This example adds an entry on the primary network interface to
   the neighbor cache table. */

#define PRIMARY_INTEFACE 0

NXD_ADDRESS ip_address;
UCHAR   hw_address[6] = {0x0, 0xcf,0x01,0x02, 0x03, 0x04};
CHAR    *mac;

mac = (CHAR *)&hw_address[0];

ip_address.nxd_ip_address_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0]   = 0x20011234;
ip_address.nxd_ip_address.v6[1]   = 0x56780000;
ip_address.nxd_ip_address.v6[2]   = 0;
ip_address.nxd_ip_address.v6[3]   = 1;


/* Create an entry in the neighbor cache table with the specified
   IPv6 address and hardware address. */
status = nxd_nd_cache_entry_set(&ip_0,
                                &ip_address.nxd_ip_address.v6[0],
                                PRIMARY_INTERFACE, mac);

/* If status == NX_SUCCESS, the entry was added to the neighbor
   cache table. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nxd_nd_cache_hardware_address_find

Locate Hardware Address for an IPv6 Address

Prototype

```
UINT nxd_nd_cache_hardware_address_find(NX_IP *ip_ptr,
                                        NXD_ADDRESS *ip_address,
                                        ULONG *physical_msw,
                                        ULONG *physical_lsw
                                        UINT *interface_index);
```

Description

This service attempts to find a physical hardware address in the IPv6 neighbor discovery cache that is associated with the supplied IPv6 address. The index of the network interface through which the neighbor can be reached is also returned in the parameter *interface_index.* The equivalent NetX IPv4 service is ***nx_arp_hardware_address_find***.

Parameters

ip_ptr	Pointer to previously created IP instance
ip_address	Pointer to IP address to find, host byte order
physical_msw	Pointer to the top 16 bits (47-32) of the physical address, in host byte order
physical_lsw	Pointer to the lower 32 bits (31-0) of the physical address in host byte order
interface_index	Pointer to the valid memory location for the interface index specifying the network device on which the IPv6 address can be reached.

Return Values

NX_SUCCESS	(0x00)	Successfully found the address
NX_ENTRY_NOT_FOUND	(0x16)	Mapping not in the neighbor cache
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_INVALID_PARAMETERS	(0x4D)	The supplied IP address is not version 6.
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space

NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
/* This example inputs an IP address on the primary network in order
   to obtain the hardware address it is mapped to in the neighbor
   cache able. */

NXD_ADDRESS  ip_address;
ULONG physical_msw, physical_lsw;
UINT  interface_index;

ip_address.nxd_ip_address_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0]   = 0x20011234;
ip_address.nxd_ip_address.v6[1]   = 0x56780000;
ip_address.nxd_ip_address.v6[2]   = 0;
ip_address.nxd_ip_address.v6[3]   = 1;

/* Obtain the hardware address mapped to the supplied global IPv6
   address. */
status = nxd_nd_cache_hardware_address_find(&ip_0, &ip_address,
                                              &physical_msw,
                                              &physical_lsw
                                              &interface_index);

/* If status == NX_SUCCESS, a matching entry was found in the
   neighbor cache table and the hardware address returned in
   variables physical_msw and physical_lsw, the index of the network
   interface through which the neighbor can be reached is stored in
   interface_index. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_invalidate, nxd_nd_cache_ip_address_find

nxd_nd_cache_invalidate

Invalidate the Neighbor Discovery Cache

Prototype

```
UINT nxd_nd_cache_invalidate(NX_IP *ip_ptr);
```

Description

This service invalidates the entire IPv6 neighbor discovery cache. This service can be invoked either before or after ICMPv6 has been enabled. This service is not applicable to IPv4 connectivity, so there is no NetX equivalent service.

Parameters

ip_ptr	Pointer to IP instance

Return Values

NX_SUCCESS	(0x00)	Cache successfully invalidated
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP instance
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
/* This example invalidates the host neighbor cache table. */

/* Invalidate the cache table bound to the IP instance. */
status = nxd_nd_cache_invalidate (&ip_0);

/* If status == NX_SUCCESS, all entries in the neighbor cache table
   are invalidated. */
```

See also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_ip_address_find

nxd_nd_cache_ip_address_find

Retrieve IPv6 Address for a Physical Address

Prototype

```
UINT nxd_nd_cache_ip_address_find(NX_IP *ip_ptr,
                                  NXD_ADDRESS *ip_address,
                                  ULONG  physical_msw,
                                  ULONG  physical_lsw,
                                  UINT  *interface_index);
```

Description

This service attempts to find an IPv6 address in the IPv6 neighbor discovery cache that is associated with the supplied physical address. The index of the network interface through which the neighbor can be reached is also returned. The equivalent NetX IPv4 service is ***nx_arp_ip_address_find***.

Parameters

ip_ptr	Pointer to previously created IP instance
ip_address	Pointer to valid NXD_ADDRESS structure
physical_msw	Top 16 bits (47-32) of the physical address to find, host byte order
physical_lsw	Lower 32 bits (31-0) of the physical address to find, host byte order
interface_index	Pointer to the network device index through which the IPv6 address can be reached

Return Values

NX_SUCCESS	(0x00)	Successfully found the address
NX_ENTRY_NOT_FOUND	(0x16)	Physical address not found in the neighbor cache
NX_NOT_SUPPORTED	(0x4B)	IPv6 feature is not built into the NetX Duo library
NX_PTR_ERROR	(0x07)	Invalid IP instance or storage space

NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_INVALID_PARAMETERS	(0x4D)	MAC address is zero.

Allowed From

Threads

Preemption Possible

No

Example

```
/* This example inputs a hardware address to search on for the
   matching IPv6 global address in the neighbor cache table. */

NXD_ADDRESS ip_address;
ULONG physical_msw = 0xcf;
ULONG physical_lsw = 0x01020304;
UINT  interface_index;


/* Obtain the IPv6 address mapped to the supplied hardware
   Address on the primary device. */
status = nxd_nd_cache_ip_address_find(&ip_0, &ip_address,
                                      physical_msw, physical_lsw,
                                      &interface_index);

/* If status == NX_SUCCESS, a matching entry was found in the
   neighbor cache table and the global IPv6 address returned in
   variable ip_address. */
```

See Also

nx_arp_dynamic_entries_invalidate, nx_arp_dynamic_entry_set, nx_arp_enable, nx_arp_entry_delete, nx_arp_gratuitous_send, nx_arp_hardware_address_find, nx_arp_info_get, nx_arp_ip_address_find, nx_arp_static_entries_delete, nx_arp_static_entry_create, nx_arp_static_entry_delete, nxd_nd_cache_entry_delete, nxd_nd_cache_entry_set, nxd_nd_cache_hardware_address_find, nxd_nd_cache_invalidate

nxd_tcp_client_socket_connect

Make a TCP Connection

Prototype

```
UINT nxd_tcp_client_socket_connect(NX_TCP_SOCKET *socket_ptr
                                   NXD_ADDRESSS *server_ip,
                                   UINT  server_port,
                                   ULONG wait_option)
```

Description

This service makes TCP connection using a previously created TCP client socket to the specified server's port. This service works on either IPv4 or IPv6 networks. Valid TCP server ports range from 0 through 0xFFFF. NetX Duo determines the appropriate physical interface based on the server IP address. The NetX IPv4 equivalent is ***nx_tcp_client_socket_connect***.

The socket must have been bound to a local port.

Parameters

socket_ptr	Pointer to previously created TCP socket
server_ip	Pointer to IPv4 or IPv6 destination address, in host byte order
server_port	Server port number to connect to (1 through 0xFFFF), in host byte order
wait_option	Wait option while the connection is being established. The wait options are defined as follows: NX_NO_WAIT (0x00000000) NX_WAIT_FOREVER (0xFFFFFFFF) timeout value in ticks (0x00000001 through 0xFFFFFFFE)

Return Values

NX_SUCCESS	(0x00)	Successful socket connect
NX_WAIT_ABORTED	(0x1A)	Requested suspension was aborted by a call to tx_thread_wait_abort
NX_IP_ADDRESS_ERROR	(0x21)	Invalid server IPv4 or IPv6 address
NX_NOT_BOUND	(0x24)	Socket is not bound
NX_NOT_CLOSED	(0x35)	Socket is not in a closed state
NX_IN_PROGRESS	(0x37)	No wait was specified, connection attempt is in progress
NX_INVALID_INTERFACE	(0x4C)	Invalid interface index.
NX_NO_INTERFACE_ADDRESS	(0x50)	The network interface does not have valid IPv6 address
NX_NOT_ENABLED	(0x14)	TCP not enabled
NX_INVALID_PORT	(0x46)	Invalid port
NX_PTR_ERROR	(0x07)	Invalid socket pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_CONNECTED	(0x38)	Connection fails.

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  peer_ip_address;
ULONG        peer_port;


/* Set Peer IPv6 address */
peer_ip_address.nxd_ip_version = NX_IP_VERSION_V6;
peer_ip_address.nxd_ip_address.v6[0] = 0x20010000;
peer_ip_address.nxd_ip_address.v6[1] = 0;
peer_ip_address.nxd_ip_address.v6[2] = 0;
peer_ip_address.nxd_ip_address.v6[3] = 0x101;

/* Set peer port number */
peer_port = 2563;

/* Connect to the peer */
status = nxd_tcp_client_socket_connect(socket_ptr,
                                       &peer_ip_address,
                                       peer_port, NX_WAIT_FOREVER);
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_socket_peer_info_get

nxd_tcp_socket_peer_info_get

Retrieves Peer TCP Socket IP Address and Port Number

Prototype

```
UINT nxd_tcp_socket_peer_info_get(NX_TCP_SOCKET *socket_ptr,
                                  NXD_ADDRESS *peer_ip_address,
                                  ULONG *peer_port);
```

Description

This service retrieves peer IP address and port information for the connected TCP socket over either IPv4 or IPv6 network. The equivalent NetX IPv4 service is ***nx_tcp_socket_peer_info_get***.

Note that *socket_ptr* must point to a TCP socket that is already in the connected state.

Parameters

socket_ptr	Pointer to TCP socket connected to peer host
peer_ip_address	Pointer to IPv4 or IPv6 peer address. The returned IP address is in host byte order.
peer_port	Pointer to peer port number. The returned port number is in host byte order.

Return Values

NX_SUCCESS	(0x00)	Socket information successfully retrieved
NX_NOT_CONNECTED	(0x38)	Socket not connected to peer
NX_NOT_ENABLED	(0x14)	TCP not enabled
NX_PTR_ERROR	(0x07)	Invalid pointer input
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  peer_ip_address;
ULONG        peer_port;


/* Get TCP socket information. */
status = nxd_tcp_socket_peer_info_get(socket_ptr, &peer_ip_address,
                                      &peer_port);

/* If status == NX_SUCCESS, the service returns valid peer info: */
if(peer_ip_address.nxd_ip_version == NX_IP_VERSION_V4)
    /* Peer IP address is stored in
       peer_ip_address.nxd_ip_address.v4 */

if(peer_ip_address.nxd_ip_version == NX_IP_VERSION_V6)
    /* Peer IP address is stored in
       peer_ip_address.nxd_ip_address.v6 */
```

See Also

nx_tcp_client_socket_bind, nx_tcp_client_socket_connect, nx_tcp_client_socket_port_get, nx_tcp_client_socket_unbind, nx_tcp_enable, nx_tcp_free_port_find, nx_tcp_info_get, nx_tcp_server_socket_accept, nx_tcp_server_socket_listen, nx_tcp_server_socket_relisten, nx_tcp_server_socket_unaccept, nx_tcp_server_socket_unlisten, nx_tcp_socket_bytes_available, nx_tcp_socket_create, nx_tcp_socket_delete, nx_tcp_socket_disconnect, nx_tcp_socket_info_get, nx_tcp_socket_receive, nx_tcp_socket_receive_queue_max_set, nx_tcp_socket_send, nx_tcp_socket_state_wait, nxd_tcp_client_socket_connect

nxd_udp_packet_info_extract

Extract network parameters from UDP packet

Prototype

```
UINT nxd_udp_packet_info_extract(NX_PACKET *packet_ptr,
                                 NXD_ADDRESS *ip_address,
                                 UINT *protocol,
                                 UINT *port,
                                 UINT *interface_index);
```

Description

This service extracts network parameters from a packet received on either IPv4 or IPv6 UDP networks. The NetX equivalent service is ***nx_udp_packet_info_extract.***

Parameters

packet_ptr	Pointer to packet.
ip_address	Pointer to sender IP address.
protocol	Pointer to protocol to be returned.
port	Pointer to sender's port number.
interface_index	Pointer to the index of the network interface from which this packet is received

Return Values

NX_SUCCESS	(0x00)	Packet interface data successfully extracted.
NX_INVALID_PACKET	(0x12)	Packet is neither IPv4 or IPv6.
NX_PTR_ERROR	(0x07)	Invalid pointer input
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
/* Extract network data from UDP packet interface.*/
status = nxd_udp_packet_info_extract(packet_ptr, &ip_address,
                                     &protocol, &port,
                                     &interface_index)

/* If status is NX_SUCCESS packet data was successfully retrieved.*/
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_socket_send, nxd_udp_socket_source_send, nxd_udp_source_extract

nxd_udp_socket_send

Send a UDP Datagram

Prototype

```
UINT nxd_udp_socket_send(NX_UDP_SOCKET *socket_ptr,
                         NX_PACKET *packet_ptr,
                         NXD_ADDRESS *ip_address,
                         UINT port);
```

Description

This service sends a UDP datagram through a previously created and bound UDP socket for either IPv4 or IPv6 networks. NetX Duo finds a suitable local IP address as source address based on the destination IP address. To specify a specific interface and source IP address, the application should use the ***nxd_udp_socket_source_send*** service.

Note that this service returns immediately regardless of whether the UDP datagram was successfully sent. The NetX (IPv4) equivalent service is ***nx_udp_socket_send*.**

The socket must be bound to a local port.

Parameters

socket_ptr	Pointer to previously created UDP socket instance
packet_ptr	UDP datagram packet pointer
ip_address	Pointer to destination IPv4 or IPv6 address
port	Valid destination port number between 1 and 0xFFFF), in host byte order

Return Values

NX_SUCCESS	(0x00)	Successful UDP socket send
NX_IP_ADDRESS_ERROR	(0x21)	Invalid server IPv4 or IPv6 address
NX_NOT_BOUND	(0x24)	Socket not bound to any port
NX_NO_INTERFACE_ADDRESS	(0x50)	No suitable outgoing interface can be found.

NX_UNDERFLOW	(0x02)	Not enough room for UDP header in the packet
NX_OVERFLOW	(0x03)	Packet append pointer is invalid
NX_PTR_ERROR	(0x07)	Invalid socket pointer, address pointer, or packet pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	UDP has not been enabled
NX_INVALID_PORT	(0x46)	Port number is not within a valid range

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  ip_address, server_address;

/* Set the UDP Client IPv6 address. */
ip_address.nxd_ip_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0] = 0x20010000;
ip_address.nxd_ip_address.v6[1] = 0;
ip_address.nxd_ip_address.v6[2] = 0;
ip_address.nxd_ip_address.v6[3] = 1;

/* Set the UDP server IPv6 address to send to. */
server_address.nxd_ip_version = NX_IP_VERSION_V6;
server_address.nxd_ip_address.v6[0] = 0x20010000;
server_address.nxd_ip_address.v6[1] = 0;
server_address.nxd_ip_address.v6[2] = 0;
server_address.nxd_ip_address.v6[3] = 2;

/* Set the global address (indicated by the 64 bit prefix) using the
   IPv6 address just created on the primary device (index 0). We
   don't need the index into the address table, so the last argument
   is set to null. */

interface_index = 0;
status = nxd_ipv6_address_set(&client_ip, interface_index,
                              &ip_address, 64, NX_NULL);

/* Create the UDP socket client_socket with the ip_address and */
/* allocate a packet pointed to by packet_ptr (not shown). */

/* Send a packet to the UDP server at server_address on port 12. */
status = nxd_udp_socket_send(&client_socket, packet_ptr,
                             &server_address, 12);

/* If status == NX_SUCCESS, the UDP host successfully transmitted
    the packet out the UDP socket to the server. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_source_send, nxd_udp_source_extract

nxd_udp_socket_source_send

Send a UDP Datagram

Prototype

```
UINT nxd_udp_socket_source_send(NX_UDP_SOCKET *socket_ptr,
                                NX_PACKET *packet_ptr,
                                NXD_ADDRESS *ip_address,
                                UINT port, UINT address_index);
```

Description

This service sends a UDP datagram through a previously created and bound UDP socket for either IPv4 or IPv6 networks. The parameter *address_index* specifies the source IP address to use for the outgoing packet. Note that the function returns immediately regardless of whether the UDP datagram was successfully sent.

The socket must be bound to a local port.

The NetX (IPv4) equivalent service is ***nx_udp_socket_source_send***.

Parameters

socket_ptr	Pointer to previously created UDP socket instance
packet_ptr	UDP datagram packet pointer
ip_address	Pointer to destination IPv4 or IPv6 address
port	Valid destination port number between 1 and 0xFFFF), in host byte order
address_index	Index specifying the source address to use for the packet

Return Values

NX_SUCCESS	(0x00)	Successful UDP socket send
NX_IP_ADDRESS_ERROR	(0x21)	Invalid server IPv4 or IPv6 address
NX_NOT_BOUND	(0x24)	Socket not bound to any port
NX_NO_INTERFACE_ADDRESS		

	(0x50)	No suitable outgoing interface can be found.
NX_NOT_FOUND	(0x4E)	No suitable interface can be found
NX_PTR_ERROR	(0x07)	Invalid socket pointer, address, or packet pointer.
NX_CALLER_ERROR	(0x11)	Invalid caller of this service
NX_NOT_ENABLED	(0x14)	UDP has not been enabled
NX_INVALID_PORT	(0x46)	Port number is not within valid range.
NX_INVALID_INTERFACE	(0x4C)	Specified network interface is valid
NX_UNDERFLOW	(0x02)	Not enough room for UDP header in the packet
NX_OVERFLOW	(0x03)	Packet append pointer is invalid

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  ip_address, server_address;
UINT address_index;

/* Set the UDP Client IPv6 address. */
ip_address.nxd_ip_version = NX_IP_VERSION_V6;
ip_address.nxd_ip_address.v6[0] = 0x20010000;
ip_address.nxd_ip_address.v6[1] = 0;
ip_address.nxd_ip_address.v6[2] = 0;
ip_address.nxd_ip_address.v6[3] = 1;

/* Set the UDP server IPv6 address to send to. */
server_address.nxd_ip_version = NX_IP_VERSION_V6;
server_address.nxd_ip_address.v6[0] = 0x20010000;
server_address.nxd_ip_address.v6[1] = 0;
server_address.nxd_ip_address.v6[2] = 0;
server_address.nxd_ip_address.v6[3] = 2;

 /* Set the global address (indicated by the 64 bit prefix) using the IPv6
    address just created on the primary device (index 0). The address index
    is needed for nxd_udp_socket_source_send. */

 status = nxd_ipv6_address_set(&client_ip, 0,
                               &ip_address, 64, &address_index);

/* Create the UDP socket client_socket with the ip_address and */
/* allocate a packet pointed to by packet_ptr (not shown). */

/* Send a packet to the UDP server at server_address on port 12. */
status = nxd_udp_socket_source_send(&client_socket, packet_ptr,
                                    &server_address, 12, address_index);

/* If status == NX_SUCCESS, the UDP host successfully transmitted the
   packet out the UDP socket to the server. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_source_extract

nxd_udp_source_extract

Retrieve UPD Packet Source Information

Prototype

```
UINT nxd_udp_source_extract(NX_PACKET *packet_ptr,
                            NXD_ADDRESS *ip_address, UINT *port)
```

Description

This service extracts the source IP address and port number from a UDP packet received through the host UDP socket. The NetX (IPv4) equivalent is ***nx_udp_source_extract***.

Parameters

packet_ptr	Pointer to received UDP packet
ip_address	Pointer to NXD_ADDRESS structure to store packet source IP address
port	Pointer to UDP socket port number

Return Values

NX_SUCCESS	(0x00)	Successful source extract
NX_INVALID_PACKET	(0x12)	Packet is not valid
NX_PTR_ERROR	(0x07)	Invalid socket pointer
NX_CALLER_ERROR	(0x11)	Invalid caller of this service

Allowed From

Threads

Preemption Possible

No

Example

```
NXD_ADDRESS  ip_address;
UINT          port;

/* Create the UDP socket client_socket and */
/* allocate the packet pointed to by packet_ptr (not shown). */

/* Extract the IP address and port of the packet received on the UDP
   socket specified in the packet interface. */
status = nxd_udp_source_extract(&packet_ptr, &ip_address, &port);

/* If status == NX_SUCCESS, the source IP address and port of the
   packet received on the UDP socket was successfully extracted. */
```

See Also

nx_udp_enable, nx_udp_free_port_find, nx_udp_info_get, nx_udp_packet_info_extract, nx_udp_socket_bind, nx_udp_socket_bytes_available, nx_udp_socket_checksum_disable, nx_udp_socket_checksum_enable, nx_udp_socket_create, nx_udp_socket_delete, nx_udp_socket_info_get, nx_udp_socket_port_get, nx_udp_socket_receive, nx_udp_socket_receive_notify, nx_udp_socket_send, nx_udp_socket_source_send, nx_udp_socket_unbind, nx_udp_source_extract, nxd_udp_packet_info_extract, nxd_udp_socket_send, nxd_udp_socket_source_send

Chapter 5: NetX Duo Network Drivers

This chapter contains a description of network drivers for NetX Duo. The information presented is designed to help developers write application-specific network drivers for NetX Duo. The following topics are covered:

The NX_IP structure contains everything to manage a single IP instance. This includes general TCP/IP protocol information as well as the application-specific physical network driver's entry routine. The driver's entry routine is defined during the ***nx_ip_create*** service. Additional devices may be added to the IP instance via the ***nx_ip_interface_attach*** service.

Communication between NetX Duo and the application's network driver is accomplished through the **NX_IP_DRIVER** request structure. This structure is most often defined locally on the caller's stack and is therefore released after the driver and calling function return. The structure is defined as follows:

```
typedef struct NX_IP_DRIVER_STRUCT
{
      UINT           nx_ip_driver_command;
      UINT           nx_ip_driver_status;
      ULONG          nx_ip_driver_physical_address_msw;
      ULONG          nx_ip_driver_physical_address_lsw;
      NX_PACKET      *nx_ip_driver_packet;
      ULONG          *nx_ip_driver_return_ptr;
      NX_IP          *nx_ip_driver_ptr;
      NX_INTERFACE   *nx_ip_driver_interface;
} NX_IP_DRIVER;
```

Driver Entry

NetX Duo invokes the network driver entry function for driver initialization and for sending packets and for various control and status operations, including initializing and enabling the network device. NetX Duo issues commands to the network driver by setting the ***nx_ip_driver_command*** field in the **NX_IP_DRIVER** request structure. The driver entry function has the following format:

```
VOID my_driver_entry(NX_IP_DRIVER *request);
```

Driver Requests

NetX Duo creates the driver request with a specific command and invokes the driver entry function to execute the command. Because each network driver has a single entry function, NetX Duo makes all requests through the driver request data structure. The ***nx_ip_driver_command*** member of the driver request data structure (**NX_IP_DRIVER**) defines the request. Status information is reported back to the caller in the member ***nx_ip_driver_status***. If this field is **NX_SUCCESS**, the driver request was completed successfully.

NetX Duo serializes all access to the driver. Therefore, the driver does not need to handle multiple threads asynchronously calling the entry function. Note that the device driver function executes with the IP mutex locked. Therefore the device driver internal function shall not block itself.

Typically the device driver also handles interrupts. Therefore, all driver functions need to be interrupt-safe.

Driver Initialization

Although the actual driver initialization processing is application specific, it usually consists of data structure and physical hardware initialization. The information required from NetX Duo for driver initialization is the IP Maximum Transmission Unit (MTU), which is the number of bytes available to the IP-layer payload, including IPv4 or IPv6 header) and if the physical interface needs logical-to-physical mapping. The driver configures the interface MTU value by calling ***nx_ip_interface_mtu_set***.

The device driver needs to call ***nx_ip_interface_address_mapping_configure*** to inform NetX Duo whether or not interface address mapping is required. If address mapping is needed, the driver is responsible for configuring the interface with valid MAC address, and supply the MAC address to NetX via ***nx_ip_interface_physical_address_set***.

When the network driver receives the NX_LINK INITIALIZE request from NetX Duo, it receives a pointer to the IP control block as part of the NX_IP_DRIVER request control block shown above.

After the application calls ***nx_ip_create***, the IP helper thread sends a driver request with the command set to NX_LINK_INITIALIZE to the driver to initialize its physical network interface. The following NX_IP_DRIVER members are used for the initialize request.

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_INITIALIZE
nx_ip_driver_ptr	Pointer to the IP instance. This value should be saved by the driver so that the driver function can find the IP instance to operate on.
nx_ip_driver_interface	Pointer to the network interface structure within the IP instance. This information should be saved by the driver. On receiving packets, the driver shall use the interface structure information when sending the packet up the stack. The interface index (device index) can be obtained by reading the member nx_interface_index inside this data structure.
nx_ip_driver_status	Completion status. If the driver is not able to initialize the specified interface to the IP instance, it will return a non-zero error status.

The driver is actually called from the IP helper thread that was created for the IP instance. Therefore the driver routine should avoid performing blocking operations, or the IP helper thread could stall, causing unbounded delays to applications that rely on the IP thread.

Enable Link

Next, the IP helper thread enables the physical network by setting the driver command to NX_LINK_ENABLE in the driver request and sending the request to the network driver. This happens shortly after the IP helper thread completes the initialization request. Enabling the link may be as simple as setting the *nx_interface_link_up* field in the interface instance. But it may also involve manipulation of the physical hardware. The following NX_IP_DRIVER members are used for the enable link request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_ENABLE
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to enable the specified interface, it will return a non-zero error status.

Disable Link

This request is made by NetX Duo during the deletion of an IP instance by the ***nx_ip_delete*** service. Or an application may issue this command in order to temporarily disable the link in order to save power. This service disables the physical network interface on the IP instance. The processing to disable the link may be as simple as clearing the *nx_interface_link_up* flag in the interface instance. But it may also involve manipulation of the physical hardware. Typically it is a reverse operation of the ***Enable Link*** operation. After the link is disabled, the application request ***Enable Link*** operation to enable the interface.

The following NX_IP_DRIVER members are used for the disable link request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_DISABLE
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to disable the specified interface in the IP instance, it will return a non-zero error status.

Uninitialize Link

This request is made by NetX Duo during the deletion of an IP instance by the ***nx_ip_delete*** service. This request uninitialize the interface, and release any resources created during initialization phase. Typically it is a reverse operation of the ***Initialize Link*** operation. After the interface is uninitalized, the device cannot be used until the interface is initialized again.

The following NX_IP_DRIVER members are used for the disable link request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_UNINITIALZE
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to uninitialize the specified interface to the IP instance, it will return a non-zero error status.

Packet Send

This request is made during internal IPv4 or IPv6 send processing, which all NetX Duo protocols use to transmit packets (except for ARP, RARP). On receiving the packet send command, the *nx_packet_prepend_ptr* points to the beginning of the packet to be sent, which is the beginning of the IPv4 or IPv6 header. *nx_packet_length* indicates the total size (in bytes) of the data being transmitted. If *nx_packet_next* is valid, the outgoing IP datagram is stored in multiple packets, the driver is required to follow the chained packet and transmit the entire frame. Note that valid data area in each chained packet is stored between *nx_packet_prepend_ptr* and *nx_packet_append_ptr*.

The driver is responsible for constructing physical header. If physical address to IP address mapping is required (such as Ethernet), the IP layer already resolved the MAC address. The destination MAC address is passed from the IP instance, stored in *nx_ip_driver_physical_address_msw and nx_ip_driver_physical_address_lsw.*

After adding the physical header, the packet send processing then calls the driver's output function to transmit the packet.

The following NX_IP_DRIVER members are used for the packet send request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_PACKET_SEND
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_packet	Pointer to the packet to send
nx_ip_driver_interface	Pointer to the interface instance.
nx_ip_driver_physical_address_msw	Most significant 32-bits of physical address (only if physical mapping needed)
nx_ip_driver_physical_address_lsw	Least significant 32-bits of physical address (only if physical mapping needed)
nx_ip_driver_status	Completion status. If the driver is not able to send the packet, it will return a non-zero error status.

Packet Broadcast (IPv4 packets only)

This request is almost identical to the send packet request. The only difference is that the destination physical address fields are set to the Ethernet broadcast MAC address. The following NX_IP_DRIVER members are used for the packet broadcast request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_PACKET_BROADCAST
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_packet	Pointer to the packet to send

NX_IP_DRIVER member	Meaning
nx_ip_driver_physical_address_msw	0x0000FFFF (broadcast)
nx_ip_driver_physical_address_lsw	0xFFFFFFFF (broadcast)
nx_ip_driver_interface	Pointer to the interface instance.
nx_ip_driver_status	Completion status. If the driver is not able to send the packet, it will return a non-zero error status.

ARP Send

This request is also similar to the IP packet send request. The only difference is that the Ethernet header specifies an ARP packet instead of an IP packet, and destination physical address fields are set to MAC broadcast address. The following NX_IP_DRIVER members are used for the ARP send request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_ARP_SEND
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_packet	Pointer to the packet to send
nx_ip_driver_physical_address_msw	0x0000FFFF (broadcast)
nx_ip_driver_physical_address_lsw	0xFFFFFFFF (broadcast)
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to send the ARP packet, it will return a non-zero error status.

i

If physical mapping is not needed, implementation of this request is not required.

Although ARP has been replaced with the Neighbor Discovery Protocol and the Router Discovery Protocol in IPv6, Ethernet network drivers must still *be compatible with IPv4 peers and routers. Therefore, drivers must still handle ARP packets.*

ARP Response Send

This request is almost identical to the ARP send packet request. The only difference is the destination physical address fields are passed from the IP instance. The following NX_IP_DRIVER members are used for the ARP response send request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_ARP_RESPONSE_SEND
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_packet	Pointer to the packet to send
nx_ip_driver_physical_address_msw	Most significant 32-bits of physical address
nx_ip_driver_physical_address_lsw	Least significant 32-bits of physical address
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to send the ARP packet, it will return a non-zero error status.

i

If physical mapping is not needed, implementation of this request is not required.

RARP Send

This request is almost identical to the ARP send packet request. The only differences are the type of packet header and the physical address fields are not required because the physical destination is always a broadcast address.

The following NX_IP_DRIVER members are used for the RARP send request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_RARP_SEND
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_packet	Pointer to the packet to send
nx_ip_driver_physical_address_msw	0x0000FFFF (broadcast)
nx_ip_driver_physical_address_lsw	0xFFFFFFFF (broadcast)
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to send the RARP packet, it will return a non-zero error status.

i

Applications that require RARP service must implement this command.

Multicast Group Join

This request is made with the ***nx_igmp_multicast_interface join*** and ***nx_ipv4_multicast_interface_join*** service in IPv4, ***nxd_ipv6_multicast_interface_join*** service in IPv6, and various operation required by IPv6. The network driver takes the supplied multicast group address and sets up the physical media to accept incoming packets from that multicast group address. Note that for drivers that don't support multicast filter, the driver receive logic may have to be in promiscuous mode. In this case, the driver may need to filter incoming frames based on destination MAC address, thus reducing the amount of traffic passed into the IP instance. The following NX_IP_DRIVER members are used for the multicast group join request.

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_MULTICAST_JOIN
nx_ip_driver_ptr	Pointer to IP instance

NX_IP_DRIVER member	Meaning
nx_ip_driver_physical_address_msw	Most significant 32-bits of physical multicast address
nx_ip_driver_physical_address_lsw	Least significant 32-bits of physical multicast address
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to join the multicast group, it will return a non-zero error status.

IPv6 applications will require multicast to be implemented in the driver for ICMPv6 based protocols such as address configuration. However, for IPv4 applications, implementation of this request is not necessary if multicast capabilities are not required.

If IPv6 is not enabled, and multicast capabilities are not required by IPv4, implementation of this request is not required.

Multicast Group Leave

This request is invoked by explicitly calling the ***nx_igmp_multicast_interface_leave*** or ***nx_ipv4_multicast_interface_leave*** services in IPv4, ***nxd_ipv6_multicast_interface_leave*** service in IPv6, or by various internal NetX Duo operations required for IPv6. The driver removes the supplied Ethernet multicast address from the multicast list. After a host has left a multicast group, packets on the network with this Ethernet multicast address are no longer received by this IP instance. The following

NX_IP_DRIVER members are used for the multicast group leave request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_MULTICAST_LEAVE
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_physical_address_msw	Most significant 32 bits of physical multicast address
nx_ip_driver_physical_address_lsw	Least significant 32 bits of physical multicast address
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to leave the multicast group, it will return a non-zero error status.

If multicast capabilities are not required by either IPv4 or IPv6, implementation of this request is not required.

Attach Interface

This request is invoked from the NetX Duo to the device driver, allowing the driver to associate the driver instance with the corresponding IP instance and the physical interface instance within the IP. The following NX_IP_DRIVER members are used for the attach interface request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_INTERFACE_ATTACH
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance.
nx_ip_driver_status	Completion status. If the driver is not able to detach the specified interface to the IP instance, it will return a non-zero error status.

Detach Interface

This request is invoked by NetX Duo to the device driver, allowing the driver to disassociate the driver instance with the corresponding IP instance and the physical interface instance within the IP. The following NX_IP_DRIVER members are used for the attach interface request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_INTERFACE_DETACH
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance.
nx_ip_driver_status	Completion status. If the driver is not able to attach the specified interface to the IP instance, it will return a non-zero error status.

Get Link Status

The application can query the network interface link status using the NetX Duo service ***nx_ip_interface_status_check*** service for any interface on the host. See Chapter 4, “Description of NetX Duo Services” on page 149, for more details on these services.

The link status is contained in the *nx_interface_link_up* field in the NX_INTERFACE structure pointed to by *nx_ip_driver_interface* pointer. The following NX_IP_DRIVER members are used for the link status request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_STATUS
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the status.

NX_IP_DRIVER member	Meaning
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get specific status, it will return a non-zero error status.

i *__nx_ip_status_check__ is still available for checking the status of the primary interface. However, application developers are encouraged to use the interface specific service:* ***nx_ip_interface_status_check.***

Get Link Speed

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's line speed in the supplied destination. The following NX_IP_DRIVER members are used for the link line speed request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_SPEED
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the line speed
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get speed information, it will return a non-zero error status.

i *This request is not used internally by NetX Duo so its implementation is optional.*

Get Duplex Type

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's duplex type in the supplied destination. The following NX_IP_DRIVER members are used for the duplex type request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_DUPLEX_TYPE
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the duplex type
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get duplex information, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Get Error Count

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's error count in the supplied destination. To support this feature, the driver needs to track operation errors. The following NX_IP_DRIVER members are used for the link error count request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_ERROR_COUNT
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the error count

NX_IP_DRIVER member	Meaning
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get error count, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Get Receive Packet Count

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's receive packet count in the supplied destination. To support this feature, the driver needs to keep track of the number of packets received. The following NX_IP_DRIVER members are used for the link receive packet count request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_RX_COUNT
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the receive packet count
nx_ip_driver_interface	Pointer to the physical network interface
nx_ip_driver_status	Completion status. If the driver is not able to get receive count, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Get Transmit Packet Count

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's transmit packet count in the supplied destination. To support this feature, the driver needs to keep track of each packet it transmits on each interface. The following NX_IP_DRIVER members are used for the link transmit packet count request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_TX_COUNT
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the transmit packet count
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get transmit count, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Get Allocation Errors

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver stores the link's packet pool allocation error count in the supplied destination. The following NX_IP_DRIVER members are used for the link allocation error count request:

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_GET_ALLOC_ERRORS
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	Pointer to the destination to place the allocation error count
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to get allocation errors, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Driver Deferred Processing

This request is made from the IP helper thread in response to the driver calling the ***_nx_ip_driver_deferred_processing*** routine from a transmit or receive ISR. This allows the driver ISR to defer the packet receive and transmit processing to the IP helper thread and thus reduce the amount to process in the ISR. The *nx_interface_additional_link_info* field in the NX_INTERFACE structure pointed to by *nx_ip_driver_interface* may be used by the driver to store information about the deferred processing event from the IP helper thread context. The following NX_IP_DRIVER members are used for the deferred processing event.

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_DEFERRED_PROCESSING
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance

Set Physical Address

This request is made from within the ***nx_ip_interface_physical_address_set*** service. This service allows an application to change the interface physical address at run time. On receiving this command, the driver is required to re-configure the hardware address of the network interface to the supplied physical address. Since the IP instance already has the new address, there is no need to call the ***nx_ip_interface_address_set*** service from this command.

The following NX_IP_DRIVER members are used for the user command request.

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_SET_PHYSICAL_ADDRESS
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_physical_address_msw	Most significant 32-bits of the new physical address
nx_ip_driver_physical_address_lsw	Least significant 32-bits of the new physical address
nx_ip_driver_status	Completion status. If the driver is not able to reconfigure the physical address, it will return a non-zero error status.

User Commands

This request is made from within the ***nx_ip_driver_direct_command*** service. The driver processes the application specific user commands. The following NX_IP_DRIVER members are used for the user command request.

NX_IP_DRIVER member	Meaning
nx_ip_driver_command	NX_LINK_USER_COMMAND
nx_ip_driver_ptr	Pointer to IP instance
nx_ip_driver_return_ptr	User defined
nx_ip_driver_interface	Pointer to the interface instance
nx_ip_driver_status	Completion status. If the driver is not able to execute user commands, it will return a non-zero error status.

This request is not used internally by NetX Duo so its implementation is optional.

Unimplemented Commands

Commands unimplemented by the network driver must have the return status field set to NX_UNHANDLED_COMMAND.

Driver Capability

Some network interfaces offer checksum offload features. Device drivers may take advantage of the hardware accelerations to free up CPU time from running various checksum computations.

Depending the level of hardware checksum support from the hardware, the device driver needs to inform the IP instance which hardware feature is enabled. This way, the IP instance is aware of the hardware feature, and offload as much computation to the hardware as possible. The driver should use the API ***nx_ip_interface_capability_set*** to set all the features the physical interface is able to handle.

The following features can be used:

```
NX_INTERFACE_CAPABILITY_IPV4_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_IPV4_RX_CHECKSUM
NX_INTERFACE_CAPABILITY_TCP_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_TCP_RX_CHECKSUM
NX_INTERFACE_CAPABILITY_UDP_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_UDP_RX_CHECKSUM
NX_INTERFACE_CAPABILITY_ICMPV4_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_ICMPV4_RX_CHECKSUM
NX_INTERFACE_CAPABILITY_ICMPV6_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_ICMPV6_RX_CHECKSUM
NX_INTERFACE_CAPABILITY_IGMP_TX_CHECKSUM
NX_INTERFACE_CAPABILITY_IGMP_RX_CHECKSUM
```

For a checksum computation that can be performed in hardware, the driver must set up the hardware or the buffer descriptors correctly so the checksum for an out-going packet can be generated and inserted into the header by the hardware. On receiving a packet, the hardware checksum logic should be able to verify the checksum value. If the checksum value is incorrect, the received frame should be discarded.

Even with the capability of performing checksum computation in hardware, the IP instance still maintains the checksum capability. In certain scenarios, for example a UDP datagram going through IPsec protection, the UDP checksum must be computed in software before passing the UDP frame down the stack. Most hardware checksum feature does not support checksum computation for a segment of data protected by IPsec. For a UDP or ICMP frame that needs to be fragmented, the UDP or ICMP checksum needs to be computed in software. Most hardware checksum logic does not handle the case where the data is split into multiple frames.

Driver Output

All previously mentioned packet transmit requests require an output function implemented in the driver. Specific transmit logic is hardware specific, but it usually consists of checking for hardware capacity to send the packet immediately. If possible, the packet payload (and additional payloads in the packet chain) are loaded into one or more of the hardware transmit buffers and a transmit operation is initiated. If the packet won't fit in the available transmit buffers, the packet should be queued, and be transmitted when the transmission buffers become available.

The recommended transmit queue is a singly linked list, having both head and tail pointers. New packets are added to the end of the queue, keeping the oldest packet at the front. The *nx_packet_queue_next* field is used as the packet's next link in the queue. The driver defines the head and tail pointers of the transmit queue.

Because this queue is accessed from thread and interrupt portions of the driver, interrupt protection must be placed around the queue manipulations.

Most physical hardware implementations generate an interrupt upon packet transmit completion. When the driver receives such an interrupt, it typically releases the resources associated with the packet just being transmitted. In case the transmit logic reads data directly from the NX_PACKET buffer, the driver should use the ***nx_packet_transmit_release*** service to release the packet associated with the transmit complete interrupt back to the available packet pool. Next, the driver examines the transmit queue for additional packets waiting to be sent. As many of the queued transmit packets that fit into the hardware transmit buffer(s) are de-queued and loaded into the buffers. This is followed by initiation of another send operation.

As soon as the data in the NX_PACKET has been moved into the transmitter FIFO (or in case a driver supports zero-copy operation, the data in NX_PACKET has been transmitted), the driver must move the nx_packet_prepend_ptr to the beginning of the IP header before calling ***nx_packet_transmit_release.*** Remember to adjust *nx_packet_length* field accordingly. If an IP frame is made up of multiple packets, only the head of the packet chain needs to be released.

Driver Input

Upon reception of a received packet interrupt, the network driver retrieves the packet from the physical hardware receive buffers and builds a valid NetX Duo packet. Building a valid NetX Duo packet involves setting up the appropriate length field and chaining together multiple packets if the incoming packet's size is greater than a single packet payload. Once properly built, the prepend_ptr is moved after the physical layer header and the receive packet is dispatched to NetX Duo.

NetX Duo assumes that the IP (IPv4 and IPv6) and ARP headers are aligned on a ULONG boundary. The NetX Duo driver must, therefore, ensure this alignment. In Ethernet environments this is done by starting the Ethernet header two bytes from the beginning of the packet. When the *nx_packet_prepend_ptr* is moved beyond the Ethernet header, the underlying IP (IPv4 and IPv6) or ARP header is 4-byte aligned.

See the section “Ethernet Headers” below for important differences between IPv6 and IPv6 Ethernet headers.

There are several receive packet functions available in NetX Duo. If the received packet is an ARP packet, ***_nx_arp_packet_deferred_receive*** is called. If the received packet is an RARP packet, ***_nx_rarp_packet_deferred_receive*** is called. There are several options for handling incoming IP packets. For the fastest handling of IP packets, ***_nx_ip_packet_receive*** is called. This approach has the least overhead, but requires more processing in the driver’s receive interrupt service handler (ISR). For minimal ISR processing ***_nx_ip_packet_deferred_receive*** is called.

After the new receive packet is properly built, the physical hardware’s receive buffers are setup to receive more data. This might require allocating NetX Duo packets and placing the payload address in the hardware receive buffer or it may simply amount to changing a setting in the hardware receive buffer. To minimize overrun possibilities, it is important that the hardware’s receive buffers have available buffers as soon as possible after a packet is received.

The initial receive buffers are setup during driver initialization.

Deferred Receive Packet Handling

The driver may defer receive packet processing to the NetX Duo IP helper thread. For some applications this may be necessary to minimize ISR processing as well as dropped packets.

To use deferred packet handling, the NetX Duo library must first be compiled with ***NX_DRIVER_DEFERRED_PROCESSING*** defined. This adds the deferred packet logic to the NetX Duo IP helper thread. Next, on receiving a data packet, the driver must call *_nx_ip_packet_deferred_receive():*

```
_nx_ip_packet_deferred_receive(ip_ptr, packet_ptr);
```

The deferred receive function places the receive packet represented by *packet_ptr* on a FIFO (linked list) and notifies the IP helper thread. After executing, the IP helper repetitively calls the deferred handling function to process each deferred packet. The deferred handler processing typically includes removing the packet's physical layer header (usually Ethernet) and dispatching it to one of these NetX Duo receive functions:

_nx_ip_packet_receive
_nx_arp_packet_deferred_receive
_nx_rarp_packet_deferred_receive

Ethernet Headers

One of the most significant differences between IPv6 and IPv4 for Ethernet Headers is the frame type setting. When sending out packets, the Ethernet driver is responsible for setting the Ethernet frame type in outgoing packets. For IPv6 packets, the frame type should be 0x86DD; for IPv4 packets, the frame type should be 0x0800.

The following code segment illustrates this process:

```
NX_PACKET *packet_ptr;
packet_ptr = driver_req_ptr -> nx_ip_driver_packet;
if (packet_ptr -> nx_packet_ip_version == NX_IP_VERSION_V4)
{
    /* Set Ethernet frame type to IPv4  /*
    ethernet_frame_ptr -> frame_type = 0x0800;

    /* Swap endian-ness for little endian targets.*/
    NX_CHANGE_USHORT_ENDIAN(ethernet_frame_ptr -> frame_type);
}
else if (packet_ptr -> nx_packet_ip_version == NX_IP_VERSION_V6)
{
    /* Set Ethernet frame type to IPv6. /*
    ethernet_frame_ptr -> frame_type = 0x86DD;

    /* Swap endian-ness for little endian targets.*/
    NX_CHANGE_USHORT_ENDIAN(ethernet_frame_ptr -> frame_type);
}
else
{
    /* Unknown IP version. Free the packet we will not send. */
    nx_packet_transmit_release(packet_ptr);
}
```

Similarly, for incoming packets, the Ethernet driver should determine the packet type from the Ethernet frame type. It should be implemented to accept IPv6 (0x86DD), IPv4 (0x0800), ARP (0x0806), and RARP (0x8035) frame types.

Example RAM Ethernet Network Driver

The NetX Duo demonstration system is delivered with a small RAM-based network driver, defined in the file ***nx_ram_network_driver.c.*** This driver assumes the IP instances are all on the same network and simply assigns virtual hardware addresses (MAC addresses) to each device instance as they are created. This file provides a good example of the basic structure of NetX Duo physical network drivers. Users may develop their own network drivers using the driver framework presented in this example.

The entry function of the network driver is ***_nx_ram_network_driver(),*** which is passed to the IP instance create call. Entry functions for additional network interfaces can be passed into the *nx_ip_interface_attach()* service. After the IP instance starts to run, the driver entry function is invoked to initialize and enable the device (refer to the case **NX_LINK_INITIALIZE** and **NX_LINK_ENABLE**). After the **NX_LINK_ENABLE** command is issued, the device should be ready to transmit and receive packets.

The IP instance transmits network packets via one of these commands:

NX_LINK_PACKET_SEND	An IPv4 or IPv6 packet is being transmitted,
NX_LINK_ARP_SEND	An ARP request or ARP response packet is being transmitted,
NX_LINK_ARP_RARP_SEND	A Reverse ARP request or response packet is being transmitted,

On processing these commands, the network driver needs to prepend the appropriate Ethernet frame header, and then send it to the underlying hardware for transmission. During the transmission process, the network driver has the exclusive ownership of the packet buffer area. Therefore once the data is being transmitted (or once the data has been copied into the driver internal transfer buffer), the network driver is responsible for releasing the packet buffer by first moving the prepend pointer past the Ethernet header to the IP header (and adjust packet length accordingly), and then by calling the ***nx_packet_transmit_release()*** service to release the packet. Not releasing the packet after data transmission will cause packets to leak.

The network device driver is also responsible for handling incoming data packets. In the RAM driver example, the received packet is processed by the function ***_nx_ram_network_driver_receive()***. Once the device receives an Ethernet frame, the driver is responsible for storing the data in NX_PACKET structure. Note that NetX Duo assumes the IP header starts from 4-byte aligned address. Since the length of Ethernet header is 14-byte, the driver needs to store the starting of the Ethernet header at 2-byte aligned address to guarantee that the IP header starts at 4-byte aligned address.

Appendix A: NetX Duo Services

Address Resolution Protocol (ARP)

```
UINT    nx_arp_dynamic_entries_invalidate(NX_IP
           *ip_ptr);

UINT    nx_arp_dynamic_entry_set(NX_IP *ip_ptr, ULONG
           ip_address, ULONG physical_msw, ULONG
           physical_lsw);

UINT    nx_arp_enable(NX_IP *ip_ptr, VOID
           *arp_cache_memory,
           ULONG arp_cache_size);

UINT    nx_arp_gratuitous_send(NX_IP *ip_ptr,
           VOID (*response_handler)(NX_IP *ip_ptr,
           NX_PACKET *packet_ptr));

UINT    nx_arp_hardware_address_find(NX_IP *ip_ptr,
           ULONG ip_address, ULONG*physical_msw,
           ULONG *physical_lsw);

UINT    nx_arp_info_get(NX_IP *ip_ptr, ULONG
           *arp_requests_sent, ULONG
           *arp_requests_received,
           ULONG *arp_responses_sent,
           ULONG*arp_responses_received,
           ULONG *arp_dynamic_entries,
           ULONG *arp_static_entries,
           ULONG *arp_aged_entries,
           ULONG *arp_invalid_messages);

UINT    nx_arp_ip_address_find(NX_IP *ip_ptr,
           ULONG *ip_address, ULONG physical_msw,
           ULONG physical_lsw);

UINT    nx_arp_static_entries_delete(NX_IP *ip_ptr);

UINT    nx_arp_static_entry_create(NX_IP *ip_ptr,
           ULONG ip_address,
           ULONG physical_msw, ULONG physical_lsw);

UINT    nx_arp_static_entry_delete(NX_IP *ip_ptr,
           ULONG ip_address, ULONG physical_msw,
           ULONG physical_lsw);
```

Internet Control Message Protocol (ICMP)

```
UINT    nx_icmp_enable(NX_IP *ip_ptr);

UINT    nx_icmp_info_get(NX_IP *ip_ptr, ULONG
           *pings_sent,
           ULONG *ping_timeouts, ULONG
           *ping_threads_suspended,
           ULONG *ping_responses_received,
           ULONG *icmp_checksum_errors,
           ULONG *icmp_unhandled_messages);

UINT    nx_icmp_ping(NX_IP *ip_ptr,
           ULONG ip_address, CHAR *data,
           ULONG data_size, NX_PACKET **response_ptr,
           ULONG wait_option);
```

```
UINT      nxd_icmp_enable(NX_IP *ip_ptr)

UINT      nxd_icmp_ping(NX_IP *ip_ptr, NXD_ADDRESS
             *ip_address, CHAR *data_ptr, ULONG
             data_size, NX_PACKET **response_ptr, ULONG
             wait_option)

UINT      nxd_icmp_interface_ping(NX_IP *ip_ptr,
             NXD_ADDRESS *ip_address, UINT source_index,
             CHAR *data_ptr, ULONG data_size, NX_PACKET
             **response_ptr, ULONG wait_option);
```

Internet Group Management Protocol (IGMP)

```
UINT      nx_igmp_enable(NX_IP *ip_ptr);

UINT      nx_igmp_info_get(NX_IP *ip_ptr, ULONG
             *igmp_reports_sent, ULONG
             *igmp_queries_received,
             ULONG *igmp_checksum_errors,
             ULONG *current_groups_joined);

UINT      nx_igmp_loopback_disable(NX_IP *ip_ptr);

UINT      nx_igmp_loopback_enable(NX_IP *ip_ptr);

UINT      nx_igmp_multicast_interface_join(NX_IP
             *ip_ptr,
             ULONG group_address, UINT interface_index);

UINT      nx_igmp_multicast_join(NX_IP *ip_ptr,
             ULONG group_address);

UINT      nx_igmp_multicast_leave(NX_IP *ip_ptr,
             ULONG group_address);
```

Internet Protocol (IP)

```
UINT      nx_ip_address_change_notify(NX_IP *ip_ptr,
             VOID (*change_notify)(NX_IP *, VOID *),
             VOID *additional_info);

UINT      nx_ip_address_get(NX_IP *ip_ptr, ULONG
             *ip_address, ULONG *network_mask);

UINT      nx_ip_address_set(NX_IP *ip_ptr, ULONG
             ip_address, ULONG network_mask);

UINT      nx_ip_create(NX_IP *ip_ptr, CHAR *name,
             ULONG ip_address,
             ULONG network_mask, NX_PACKET_POOL
             *default_pool, VOID
             (*ip_network_driver)(NX_IP_DRIVER *),
             VOID *memory_ptr, ULONG memory_size, UINT
             priority);

UINT      nx_ip_delete(NX_IP *ip_ptr);

UINT      nx_ip_driver_direct_command(NX_IP *ip_ptr,
             UINT command, ULONG *return_value_ptr);
```

```
UINT    nx_ip_driver_interface_direct_command(NX_IP
           *ip_ptr, UINT command, UINT
           interface_index, ULONG *return_value_ptr);

UINT    nx_ip_forwarding_disable(NX_IP *ip_ptr);

UINT    nx_ip_forwarding_enable(NX_IP *ip_ptr);

UINT    nx_ip_fragment_disable(NX_IP *ip_ptr);

UINT    nx_ip_fragment_enable(NX_IP *ip_ptr);

UINT    nx_ip_gateway_address_set(NX_IP *ip_ptr,
           ULONG ip_address);

UINT    nx_ip_info_get(NX_IP *ip_ptr,
           ULONG *ip_total_packets_sent,
           ULONG *ip_total_bytes_sent,
           ULONG *ip_total_packets_received,
           ULONG *ip_total_bytes_received,
           ULONG *ip_invalid_packets,
           ULONG *ip_receive_packets_dropped,
           ULONG *ip_receive_checksum_errors,
           ULONG *ip_send_packets_dropped,
           ULONG *ip_total_fragments_sent,
           ULONG *ip_total_fragments_received);

UINT    nx_ip_interface_address_get(NX_IP *ip_ptr,
           ULONG interface_index,
           ULONG *ip_address,
           ULONG *network_mask);

UINT    nx_ip_interface_address_set(NX_IP *ip_ptr,
           ULONG interface_index, ULONG ip_address,
           ULONG network_mask);

UINT    nx_ip_interface_attach(NX_IP *ip_ptr, CHAR*
           interface_name, ULONG ip_address, ULONG
           network_mask,
           VOID (*ip_link_driver)(struct
           NX_IP_DRIVER_STRUCT *));

UINT    nx_ip_interface_info_get(NX_IP *ip_ptr, UINT
           interface_index, CHAR **interface_name,
           ULONG *ip_address,
           ULONG *network_mask, ULONG *mtu_size,
           ULONG *phsyical_address_msw, ULONG
           *physical_address_lsw);

UINT    nx_ip_interface_status_check(NX_IP *ip_ptr,
           UINT interface_index, ULONG needed_status,
           ULONG *actual_status, ULONG wait_option);

UINT    nx_ip_max_payload_size_find(NX_IP *ip_ptr,
           NXD_ADDRESS *dest_address, UINT if_index,
           UINT src_port,
           UINT dest_port, ULONG protocol,
           ULONG *start_offset_ptr,
           ULONG *payload_length_ptr)

UINT    nx_ip_raw_packet_disable(NX_IP *ip_ptr);
```

```
UINT     nx_ip_raw_packet_enable(NX_IP *ip_ptr);

UINT     nx_ip_raw_packet_interface_send(NX_IP *ip_ptr,
            NX_PACKET *packet_ptr, ULONG
            destination_ip,
            UINT interface_index, ULONG
            type_of_service);

UINT     nx_ip_raw_packet_receive(NX_IP *ip_ptr,
            NX_PACKET **packet_ptr,
            ULONG wait_option);

UINT     nx_ip_raw_packet_send(NX_IP *ip_ptr,
            NX_PACKET *packet_ptr,
            ULONG destination_ip, ULONG
            type_of_service);

UINT     nx_ip_static_route_add(NX_IP *ip_ptr, ULONG
            network_address, ULONG net_mask, ULONG
            next_hop);

UINT     nx_ip_static_route_delete(NX_IP *ip_ptr, ULONG
            network_address, ULONG net_mask);

UINT     nx_ip_status_check(NX_IP *ip_ptr, ULONG
            needed_status, ULONG *actual_status, ULONG
            wait_option);

UINT     nxd_ipv6_default_router_add(NX_IP *ip_ptr,
            NXD_ADDRESS *router_address, ULONG
            router_lifetime, UINT if_index)

UINT     nxd_ipv6_default_router_delete(NX_IP *ip_ptr,
            NXD_ADDRESS *router_address)

UINT     nxd_ipv6_default_router_get(NX_IP *ip_ptr,
            UINT if_index, NXD_ADDRESS *router_address,
            ULONG *router_lifetime, ULONG
            *prefix_length)

UINT     nxd_ipv6_enable(NX_IP *ip_ptr)

UINT     nxd_ip_raw_packet_send(NX_IP *ip_ptr,
            NX_PACKET *packet_ptr, NXD_ADDRESS
            *destination_ip, ULONG protocol)

UINT     nxd_ip_raw_packet_interface_send(NX_IP
            *ip_ptr, NX_PACKET *packet_ptr, NXD_ADDRESS
            *destination_ip, UINT if_index, ULONG
            protocol);

UINT     nxd_ipv6_address_delete(NX_IP *ip_ptr, UINT
            address_index);

UINT     nxd_ipv6_address_get(NX_IP *ip_ptr, UINT
            address_index, NXD_ADDRESS *ip_address,
            ULONG *prefix_length, UINT *if_index);

UINT     nxd_ipv6_address_set(UINT
            nxd_ipv6_address_set(NX_IP *ip_ptr, UINT
            address_index);
```

Neighbor Discovery

```
UINT    nxd_nd_cache_entry_delete(NX_IP ip_ptr, ULONG
           *ip_address)

UINT    nxd_nd_cache_entry_set(NX_IP *ip_ptr, ULONG
           *ip_address, char *mac)

UINT    nxd_nd_cache_hardware_address_find(NX_IP
           *ip_ptr, NXD_ADDRESS *ip_address, ULONG
           *physical_msw,
           ULONG *physical_lsw)

UINT    nxd_nd_cache_invalidate(NX_IP *ip_ptr)

UINT    nxd_nd_cache_ip_address_find(NX_IP *ip_ptr,
           NXD_ADDRESS *ip_address,ULONG
           physical_msw, ULONG physical_lsw, UINT
           *if_index)
```

Packet Management

```
UINT    nx_packet_allocate(NX_PACKET_POOL *pool_ptr,
           NX_PACKET **packet_ptr, ULONG packet_type,
           ULONG wait_option);

UINT    nx_packet_copy(NX_PACKET *packet_ptr,
           NX_PACKET **new_packet_ptr, NX_PACKET_POOL
           *pool_ptr,
           ULONG wait_option);

UINT    nx_packet_data_append(NX_PACKET *packet_ptr,
           VOID *data_start, ULONG data_size,
           NX_PACKET_POOL *pool_ptr, ULONG
           wait_option);

UINT    nx_packet_data_extract_offset(NX_PACKET
           *packet_ptr,
           ULONG offset, VOID *buffer_start, ULONG
           buffer_length, ULONG *bytes_copied);

UINT    nx_packet_data_retrieve(NX_PACKET *packet_ptr,
           VOID *buffer_start, ULONG *bytes_copied);

UINT    nx_packet_length_get(NX_PACKET *packet_ptr,
           ULONG *length);

UINT    nx_packet_pool_create(NX_PACKET_POOL
           *pool_ptr,
           CHAR *name, ULONG block_size, VOID
           *memory_ptr, ULONG memory_size);

UINT    nx_packet_pool_delete(NX_PACKET_POOL
           *pool_ptr);

UINT    nx_packet_pool_info_get(NX_PACKET_POOL
           *pool_ptr, ULONG *total_packets, ULONG
           *free_packets,
           ULONG *empty_pool_requests,
           ULONG *empty_pool_suspensions,
           ULONG *invalid_packet_releases);
```

```
UINT    nx_packet_release(NX_PACKET *packet_ptr);

UINT    nx_packet_transmit_release(NX_PACKET
           *packet_ptr);
```

Reverse Address Resolution Protocol (RARP)

```
UINT    nx_rarp_disable(NX_IP *ip_ptr);

UINT    nx_rarp_enable(NX_IP *ip_ptr);

UINT    nx_rarp_info_get(NX_IP *ip_ptr,
           ULONG *rarp_requests_sent,
           ULONG *rarp_responses_received,
           ULONG *rarp_invalid_messages);
```

System Management

```
VOID    nx_system_initialize(VOID);
```

Transmission Control Protocol (TCP)

```
UINT    nx_tcp_client_socket_bind(NX_TCP_SOCKET
           *socket_ptr, UINT port, ULONG wait_option);

UINT    nx_tcp_client_socket_connect(NX_TCP_SOCKET
           *socket_ptr, ULONG server_ip, UINT
           server_port,
           ULONG wait_option);

UINT    nx_tcp_client_socket_port_get(NX_TCP_SOCKET
           *socket_ptr, UINT *port_ptr);

UINT    nx_tcp_client_socket_unbind(NX_TCP_SOCKET
           *socket_ptr);

UINT    nx_tcp_enable(NX_IP *ip_ptr);

UINT    nx_tcp_free_port_find(NX_IP *ip_ptr, UINT
           port,
           UINT *free_port_ptr);

UINT    nx_tcp_info_get(NX_IP *ip_ptr, ULONG
           *tcp_packets_sent, ULONG *tcp_bytes_sent,
           ULONG *tcp_packets_received, ULONG
           *tcp_bytes_received, ULONG
           *tcp_invalid_packets, ULONG
           *tcp_receive_packets_dropped,
           ULONG *tcp_checksum_errors,ULONG
           *tcp_connections, ULONG
           *tcp_disconnections,
           ULONG *tcp_connections_dropped,
           ULONG*tcp_retransmit_packets);

UINT    nx_tcp_server_socket_accept(NX_TCP_SOCKET
           *socket_ptr, ULONG wait_option);
```

```
UINT     nx_tcp_server_socket_listen(NX_IP *ip_ptr,
            UINT port, NX_TCP_SOCKET *socket_ptr,
            UINT listen_queue_size,
            VOID (*tcp_listen_callback)(NX_TCP_SOCKET
            *socket_ptr, UINT port));

UINT     nx_tcp_server_socket_relisten(NX_IP *ip_ptr,
            UINT port, NX_TCP_SOCKET *socket_ptr);

UINT     nx_tcp_server_socket_unaccept(NX_TCP_SOCKET
            *socket_ptr);

UINT     nx_tcp_server_socket_unlisten(NX_IP *ip_ptr,
            UINT port);

UINT     nx_tcp_socket_bytes_available(NX_TCP_SOCKET
            *socket_ptr, ULONG *bytes_available);

UINT     nx_tcp_socket_create(NX_IP *ip_ptr,
            NX_TCP_SOCKET *socket_ptr, CHAR *name,
            ULONG type_of_service, ULONG fragment,
            UINT time_to_live, ULONG window_size,
            VOID
            (*tcp_urgent_data_callback)(NX_TCP_SOCKET
            *socket_ptr),
            VOID
            (*tcp_disconnect_callback)(NX_TCP_SOCKET
            *socket_ptr));

UINT     nx_tcp_socket_delete(NX_TCP_SOCKET
            *socket_ptr);

UINT     nx_tcp_socket_disconnect(NX_TCP_SOCKET
            *socket_ptr,
            ULONG wait_option);

UINT     nx_tcp_socket_info_get(NX_TCP_SOCKET
            *socket_ptr,
            ULONG *tcp_packets_sent, ULONG
            *tcp_bytes_sent,
            ULONG *tcp_packets_received, ULONG
            *tcp_bytes_received,
            ULONG *tcp_retransmit_packets, ULONG
            *tcp_packets_queued,
            ULONG *tcp_checksum_errors, ULONG
            *tcp_socket_state,
            ULONG *tcp_transmit_queue_depth, ULONG
            *tcp_transmit_window,
            ULONG *tcp_receive_window);

UINT     nx_tcp_socket_mss_get(NX_TCP_SOCKET
            *socket_ptr,
            ULONG *mss);

UINT     nx_tcp_socket_mss_peer_get(NX_TCP_SOCKET
            *socket_ptr, ULONG *peer_mss);

UINT     nx_tcp_socket_mss_set(NX_TCP_SOCKET
            *socket_ptr,
            ULONG mss);
```

```
UINT    nx_tcp_socket_peer_info_get(NX_TCP_SOCKET
           *socket_ptr, ULONG *peer_ip_address, ULONG
           *peer_port);

UINT    nx_tcp_socket_receive(NX_TCP_SOCKET
           *socket_ptr, NX_PACKET **packet_ptr, ULONG
           wait_option);

UINT    nx_tcp_socket_receive_notify(NX_TCP_SOCKET
           *socket_ptr, VOID
           (*tcp_receive_notify)(NX_TCP_SOCKET
           *socket_ptr));

UINT    nx_tcp_socket_send(NX_TCP_SOCKET *socket_ptr,
           NX_PACKET *packet_ptr, ULONG wait_option);

UINT    nx_tcp_socket_state_wait(NX_TCP_SOCKET
           *socket_ptr, UINT desired_state, ULONG
           wait_option);

UINT    nx_tcp_socket_transmit_configure(NX_TCP_SOCKET
           *socket_ptr, ULONG max_queue_depth, ULONG
           timeout, ULONG max_retries, ULONG
           timeout_shift);

UINT    nx_tcp_socket_window_update_notify_set
           (NX_TCP_SOCKET *socket_ptr,
           VOID (*tcp_window_update_notify)
           (NX_TCP_SOCKET *socket_ptr));

UINT    nxd_tcp_client_socket_connect(NX_TCP_SOCKET
           *socket_ptr, NXD_ADDRESS *server_ip,  UINT
           server_port, ULONG wait_option)

UINT    nxd_tcp_socket_peer_info_get(NX_TCP_SOCKET
           *socket_ptr, NXD_ADDRESS *peer_ip_address,
           ULONG *peer_port)
```

User Datagram Protocol (UDP)

```
UINT    nx_udp_enable(NX_IP *ip_ptr);

UINT    nx_udp_free_port_find(NX_IP *ip_ptr, UINT
           port,
           UINT *free_port_ptr);

UINT    nx_udp_info_get(NX_IP *ip_ptr, ULONG
           *udp_packets_sent, ULONG *udp_bytes_sent,
           ULONG *udp_packets_received, ULONG
           *udp_bytes_received,
           ULONG *udp_invalid_packets,
           ULONG *udp_receive_packets_dropped,
           ULONG *udp_checksum_errors);

UINT    nx_udp_packet_info_extract(NX_PACKET
           *packet_ptr,
           ULONG *ip_address, UINT *protocol, UINT
           *port,
           UINT *interface_index);
```

```
UINT     nx_udp_socket_bind(NX_UDP_SOCKET *socket_ptr,
            UINT  port, ULONG wait_option);

UINT     nx_udp_socket_bytes_available(NX_UDP_SOCKET
            *socket_ptr, ULONG *bytes_available);

UINT     nx_udp_socket_checksum_disable(NX_UDP_SOCKET
            *socket_ptr);

UINT     nx_udp_socket_checksum_enable(NX_UDP_SOCKET
            *socket_ptr);

UINT     nx_udp_socket_create(NX_IP *ip_ptr,
            NX_UDP_SOCKET *socket_ptr, CHAR *name,
            ULONG type_of_service, ULONG fragment,
            UINT time_to_live, ULONG queue_maximum);

UINT     nx_udp_socket_delete(NX_UDP_SOCKET
            *socket_ptr);

UINT     nx_udp_socket_info_get(NX_UDP_SOCKET
            *socket_ptr,
            ULONG *udp_packets_sent, ULONG
            *udp_bytes_sent,
            ULONG *udp_packets_received, ULONG
            *udp_bytes_received,
            ULONG *udp_packets_queued,
            ULONG *udp_receive_packets_dropped,
            ULONG *udp_checksum_errors);

UINT     nx_udp_socket_interface_send(NX_UDP_SOCKET
            *socket_ptr, NX_PACKET *packet_ptr, ULONG
            ip_address, UINT port, UINT address_index);

UINT     nx_udp_socket_port_get(NX_UDP_SOCKET
            *socket_ptr,
            UINT *port_ptr);

UINT     nx_udp_socket_receive(NX_UDP_SOCKET
            *socket_ptr,
            NX_PACKET **packet_ptr, ULONG wait_option);

UINT     nx_udp_socket_receive_notify(NX_UDP_SOCKET
            *socket_ptr, VOID
            (*udp_receive_notify)(NX_UDP_SOCKET
            *socket_ptr));

UINT     nx_udp_socket_send(NX_UDP_SOCKET *socket_ptr,
            NX_PACKET *packet_ptr, ULONG ip_address,
            UINT port);

UINT     nx_udp_socket_unbind(NX_UDP_SOCKET
            *socket_ptr);

UINT     nx_udp_source_extract(NX_PACKET *packet_ptr,
            ULONG *ip_address, UINT *port);

UINT     nxd_udp_packet_info_extract(NX_PACKET
            *packet_ptr, NXD_ADDRESS *ip_address, UINT
            *protocol, UINT *port, UINT
            *interface_index);
```

```
UINT      nxd_udp_source_extract (NX_PACKET *packet_ptr,
             NXD_ADDRESS *ip_address, UINT *port)

UINT      nxd_udp_socket_interface_send(NX_UDP_SOCKET
             *socket_ptr, NX_PACKET *packet_ptr,
             NXD_ADDRESS *ip_address, UINT port, UINT
             address_index)

UINT      nxd_udp_socket_send(NX_UDP_SOCKET *socket_ptr,
             NX_PACKET *packet_ptr, NXD_ADDRESS
             *ip_address, UINT port)
```

Appendix B: NetX Duo Constants

Alphabetic Listing

NX_ALL_HOSTS_ADDRESS	0xFE000001
NX_ALL_ROUTERS_ADDRESS	0xFE000002
NX_ALREADY_BOUND	0x22
NX_ALREADY_ENABLED	0x15
NX_ALREADY_RELEASED	0x31
NX_ALREADY_SUSPENDED	0x40
NX_ANY_PORT	0
NX_ARP_EXPIRATION_RATE	0
NX_ARP_HARDWARE_SIZE	0x06
NX_ARP_HARDWARE_TYPE	0x0001
NX_ARP_MAX_QUEUE_DEPTH	4
NX_ARP_MAXIMUM_RETRIES	18
NX_ARP_MESSAGE_SIZE	28
NX_ARP_OPTION_REQUEST	0x0001
NX_ARP_OPTION_RESPONSE	0x0002
NX_ARP_PROTOCOL_SIZE	0x04
NX_ARP_PROTOCOL_TYPE	0x0800
NX_ARP_TIMER_ERROR	0x18
NX_ARP_UPDATE_RATE	10
NX_ARP_TABLE_SIZE	0x2F
NX_ARP_TABLE_MASK	0x1F
NX_CALLER_ERROR	0x11
NX_CARRY_BIT	0x10000
NX_CONNECTION_PENDING	0x48
NX_DELETE_ERROR	0x10
NX_DELETED	0x05
NX_DISCONNECT_FAILED	0x41
NX_DONT_FRAGMENT	0x00004000
NX_DRIVER_TX_DONE	0xDDDDDDDD
NX_DUPLICATE_LISTEN	0x34
NX_ENTRY_NOT_FOUND	0x16
NX_FALSE	0
NX_FOREVER	1

NX_FRAG_OFFSET_MASK	0x00001FFF
NX_FRAGMENT_OKAY	0x00000000
NX_ICMP_ADDRESS_MASK_REP_TYPE	18
NX_ICMP_ADDRESS_MASK_REQ_TYPE	17
NX_ICMP_DEBUG_LOG_SIZE	100
NX_ICMP_DEST_UNREACHABLE_TYPE	3
NX_ICMP_ECHO_REPLY_TYPE	0
NX_ICMP_ECHO_REQUEST_TYPE	8
NX_ICMP_FRAMENT_NEEDED_CODE	4
NX_ICMP_HOST_PROHIBIT_CODE	10
NX_ICMP_HOST_SERVICE_CODE	12
NX_ICMP_HOST_UNKNOWN_CODE	7
NX_ICMP_HOST_UNREACH_CODE	1
NX_ICMP_NETWORK_PROHIBIT_CODE	9
NX_ICMP_NETWORK_SERVICE_CODE	11
NX_ICMP_NETWORK_UNKNOWN_CODE	6
NX_ICMP_NETWORK_UNREACH_CODE	0
NX_ICMP_PACKET (IPv6 enabled	56
NX_ICMP_PACKET (IPv6 disabled	36
NX_ICMP_PARAMETER_PROB_TYPE	12
NX_ICMP_PORT_UNREACH_CODE	3
NX_ICMP_PROTOCOL_UNREACH_CODE	2
NX_ICMP_REDIRECT_TYPE	5
NX_ICMP_SOURCE_ISOLATED_CODE	8
NX_ICMP_SOURCE_QUENCH_TYPE	4
NX_ICMP_SOURCE_ROUTE_CODE	5
NX_ICMP_TIME_EXCEEDED_TYPE	11
NX_ICMP_TIMESTAMP_REP_TYPE	14
NX_ICMP_TIMESTAMP_REQ_TYPE	13
NX_ICMPV6_ADDRESS_UNREACHABLE_CODE	3
NX_ICMPV6_BEYOND_SCOPE_OF_SOURCE_ADDRESS_CODE	2
NX_ICMPV6_COMMUNICATION_WITH_DESTINATION_PROHIBITED_CODE	1
NX_ICMPV6_DEST_UNREACHABLE_CODE	4
NX_ICMPV6_DEST_UNREACHABLE_TYPE	1
NX_ICMPV6_ECHO_REPLY_TYPE	129

NX_ICMPV6_ECHO_REQUEST_TYPE	128
NX_ICMPV6_MINIMUM_IPV4_PATH_MTU	576
NX_ICMPV6_MINIMUM_IPV6_PATH_MTU	1280
NX_ICMPV6_NEIGHBOR_ADVERTISEMENT_TYPE	136
NX_ICMPV6_NEIGHBOR_SOLICITATION_TYPE	135
NX_ICMPV6_NO_ROUTE_TO_DESTINATION_CODE	0
NX_ICMPV6_NO_SLLA	1
NX_ICMPV6_OPTION_TYPE_PREFIX_INFO	3
NX_ICMPV6_OPTION_REDIRECTED_HEADER	4
NX_ICMPV6_OPTION_TYPE_MTU	5
NX_ICMPV6_OPTION_TYPE_SRC_LINK_ADDR	1
NX_ICMPV6_OPTION_TYPE_TRG_LINK_ADDR	2
NX_ICMPV6_PACKET_TOO_BIG_TYPE	2
NX_ICMPV6_PARAMETER_PROBLEM_TYPE	4
NX_ICMPV6_PATH_MTU_INFINITE_TIMEOUT	0xFFFFFFFF
NX_ICMPV6_REDIRECT_MESSAGE_TYPE	137
NX_ICMPV6_REJECT_ROUTE_TO_DESTINATION_CODE	6
NX_ICMPV6_ROUTER_ADVERTISEMENT_TYPE	134
NX_ICMPV6_ROUTER_SOLICITATION_TYPE	133
NX_ICMPV6_SOURCE_ADDRESS_FAILED_I_E_POLICY_CODE	5
NX_ICMPV6_TIME_EXCEED_TYPE	3
NX_IGMP_HEADER_SIZE	8
NX_IGMP_HOST_RESPONSE_TYPE	0x02000000
NX_IGMP_HOST_V2_JOIN_TYPE	0x16000000
NX_IGMP_HOST_V2_LEAVE_TYPE	0x17000000
NX_IGMP_HOST_VERSION_1	1
NX_IGMP_HOST_VERSION_2	2
NX_IGMP_MAX_RESP_TIME_MASK	0x00FF0000
NX_IGMP_MAX_UPDATE_TIME	10
NX_IGMP_PACKET	36
NX_IGMP_ROUTER_QUERY_TYPE	0x01000000
NX_IGMP_TTL	1
NX_IGMP_TYPE_MASK	0x0F000000
NX_IGMP_VERSION	0x10000000
NX_IGMPV2_TYPE_MASK	0xFF000000
NX_IN_PROGRESS	0x37

NX_INIT_PACKET_ID	1
NX_NOT_IMPLEMENTED	0x4A
NX_NOT_SUPPORTED	0x4B
NX_INVALID_INTERFACE	0x4C
NX_INVALID_PACKET	0x12
NX_INVALID_PORT	0x46
NX_INVALID_RELISTEN	0x47
NX_INVALID_SOCKET	0x13
NX_IP_ADDRESS_ERROR	0x21
NX_IP_ADDRESS_RESOLVED	0x0002
NX_IP_ALIGN_FRAGS	8
NX_IP_ALL_EVENTS	0xFFFFFFFF
NX_IP_ARP_ENABLED	0x0008
NX_IP_ARP_REC_EVENT	0x00000010
NX_IP_CLASS_A_HOSTID	0x00FFFFFF
NX_IP_CLASS_A_MASK	0x80000000
NX_IP_CLASS_A_NETID	0x7F000000
NX_IP_CLASS_A_TYPE	0x00000000
NX_IP_CLASS_B_HOSTID	0x0000FFFF
NX_IP_CLASS_B_MASK	0xC0000000
NX_IP_CLASS_B_NETID	0x3FFF0000
NX_IP_CLASS_B_TYPE	0x80000000
NX_IP_CLASS_C_HOSTID	0x000000FF
NX_IP_CLASS_C_MASK	0xE0000000
NX_IP_CLASS_C_NETID	0x1FFFFF00
NX_IP_CLASS_C_TYPE	0xC0000000
NX_IP_CLASS_D_GROUP	0x0FFFFFFF
NX_IP_CLASS_D_HOSTID	0x00000000
NX_IP_CLASS_D_MASK	0xF0000000
NX_IP_CLASS_D_TYPE	0xE0000000
NX_IP_DEBUG_LOG_SIZE	100
NX_IP_DONT_FRAGMENT	0x00004000
NX_IP_DRIVER_DEFERRED_EVENT	0x00000800
NX_IP_DRIVER_PACKET_EVENT	0x00000200
NX_IP_FRAGMENT_MASK	0x00003FFF

NX_IP_ICMP	0x00010000
NX_IP_ICMP_EVENT	0x00000004
NX_IP_ID	0x49502020
NX_IP_IGMP	0x00020000
NX_IP_IGMP_ENABLE_EVENT	0x00000400
NX_IP_IGMP_ENABLED	0x0040
NX_IP_IGMP_EVENT	0x00000040
NX_IP_INITIALIZE_DONE	0x0001
NX_IP_INTERNAL_ERROR	0x20
NX_IP_LENGTH_MASK	0x0F000000
NX_IP_LIMITIED_BROADCAST	0xFFFFFFFF
NX_IP_LINK_ENABLED	0x0004
NX_IP_LOOPBACK_FIRST	0x7F000000
NX_IP_LOOPBACK_LAST	0x7FFFFFFF
NX_IP_MAX_DATA	0x00080000
NX_IP_MAX_RELIABLE	0x00040000
NX_IP_MIN_COST	0x00020000
NX_IP_MIN_DELAY	0x00100000
NX_IP_MORE_FRAGMENT	0x00002000
NX_IP_MULTICAST_LOWER	0x5E000000
NX_IP_MULTICAST_MASK	0x007FFFFF
NX_IP_MULTICAST_UPPER	0x00000100
NX_IP_NORMAL	0x00000000
NX_IP_NORMAL_LENGTH	5
NX_IP_OFFSET_MASK	0x00001FFF
NX_IP_PACKET (IPv6 enabled	56
NX_IP_PACKET (IPv6 disabled	36
NX_IP_PACKET_SIZE_MASK	0x0000FFFF
NX_IP_PERIODIC_EVENT	0x00000001
NX_IP_PERIODIC_RATE	100
NX_IP_PROTOCOL_MASK	0x00FF0000
NX_IP_RARP_COMPLETE	0x0080
NX_IP_RARP_REC_EVENT	0x00000020
NX_IP_RECEIVE_EVENT	0x00000008
NX_IP_TCP	0x00060000

NX_IP_TCP_CLEANUP_DEFERRED	0x00001000
NX_IP_TCP_ENABLED	0x0020
NX_IP_TCP_EVENT	0x00000080
NX_IP_TCP_FAST_EVENT	0x00000100
NX_IP_TIME_TO_LIVE	0x00000080
NX_IP_TIME_TO_LIVE_MASK	0xFF000000
NX_IP_TIME_TO_LIVE_SHIFT	24
NX_IP_TOS_MASK	0x00FF0000
NX_IP_UDP	0x00110000
NX_IP_UDP_ENABLED	0x0010
NX_IP_UNFRAG_EVENT	0x00000002
NX_IP_VERSION	0x45000000
NX_IPV6_ADDRESS_INVALID	0
NX_IPV6_ADDRESS_LINKLOCAL	0x00000001
NX_IPV6_ADDRESS_SITELOCAL	0x00000002
NX_IPV6_ADDRESS_GLOBAL	0x00000004
NX_IPV6_ALL_NODE_MCAST	0x00000010
NX_IPV6_ALL_ROUTER_MCAST	0x00000020
NX_IPV6_SOLICITED_NODE_MCAST	0x00000040
NX_IPV6_ADDRESS_UNICAST	0x80000000
NX_IPV6_ADDRESS_MULTICAST	0x40000000
NX_IPV6_ADDRESS_UNSPECIFIED	0x20000000
NX_IPV6_ADDRESS_LOOPBACK	0x10000000
NX_IPV4_ICMP_PACKET	36
NX_IPV4_IGMP_PACKET	36
NX_IPV4_TCP_PACKET	56
NX_IPV4_UDP_PACKET	44
NX_IPV6_ICMP_PACKET	56
NX_IPV6_IGMP_PACKET	56
NX_IPV6_TCP_PACKET	76
NX_IPV6_UDP_PACKET	64
NX_IPV6_PROTOCOL_NEXT_HEADER_HOP_BY_HOP	0
NX_IPV6_PROTOCOL_NEXT_HEADER_ROUTING	43
NX_IPV6_PROTOCOL_NEXT_HEADER_FRAGMENT	44
NX_IPV6_PROTOCOL_NEXT_HEADER_ICMPV6	58

NX_IPV6_PROTOCOL_NO_NEXT_HEADER	59
NX_IPV6_PROTOCOL_NEXT_HEADER_DESTINATION	60
NX_IPV6_PROTOCOL_TCP	6
NX_IPV6_PROTOCOL_UDP	17
NX_IPV6_PROTOCOL_ICMPV6	58
NX_IPV6_PROTOCOL_ICMP	1
NX_IPV6_PROTOCOL_IPV4	4
NX_IPV6_PROTOCOL_IPV6	41
NX_IPV6_ADDR_STATE_UNKNOWN	0x00
NX_IPV6_ADDR_STATE_TENTATIVE	0x01
NX_IPV6_ADDR_STATE_PREFERRED	0x02
NX_IPV6_ADDR_STATE_DEPRECATED	0x03
NX_IPV6_ADDR_STATE_VALID	0x04
NX_IPV6_ROUTE_TYPE_NOT_ROUTER	0x00
NX_IPV6_ROUTE_TYPE_SOLICITATED	0x01
NX_IPV6_ROUTE_TYPE_UNSOLICITATED	0x02
NX_IPV6_ROUTE_TYPE_STATIC	0x04
NX_IPV6_ROUTE_TYPE_DEFAULT	0x40
NX_IPV6_ROUTE_TYPE_VALID	0x80
NX_LINK_ARP_RESPONSE_SEND	6
NX_LINK_ARP_SEND	5
NX_LINK_DEFERRED_PROCESSING	18
NX_LINK_DISABLE	3
NX_LINK_ENABLE	2
NX_LINK_GET_ALLOC_ERRORS	16
NX_LINK_GET_DUPLEX_TYPE	12
NX_LINK_GET_ERROR_COUNT	13
NX_LINK_GET_RX_COUNT	14
NX_LINK_GET_SPEED	11
NX_LINK_GET_STATUS	10
NX_LINK_GET_TX_COUNT	15
NX_LINK_INITIALIZE	1
NX_LINK_INTERFACE_ATTACH	19
NX_LINK_MULTICAST_JOIN	8
NX_LINK_MULTICAST_LEAVE	9

NX_LINK_PACKET_BROADCAST	4
NX_LINK_PACKET_SEND	0
NX_LINK_RARP_SEND	7
NX_LINK_UNINITIALIZE	17
NX_LINK_USER_COMMAND	50
NX_LOWER_16_MASK	0x0000FFFF
NX_MAX_LISTEN	0x33
NX_MAX_LISTEN_REQUESTS	10
NX_MAX_MULTICAST_GROUPS	7
NX_MAX_PORT	0xFFFF
NX_MORE_FRAGMENTS	0x00002000
NX_NO_FREE_PORTS	0x45
NX_NO_MAPPING	0x04
NX_NO_MORE_ENTRIES	0x17
NX_NO_PACKET	0x01
NX_NO_RESPONSE	0x29
NX_NO_WAIT	0
NX_NOT_BOUND	0x24
NX_NOT_CLOSED	0x35
NX_NOT_CONNECTED	0x38
NX_NOT_CREATED	0x27
NX_NOT_ENABLED	0x14
NX_NOT_IMPLEMENTED	0x4A
NX_NOT_LISTEN_STATE	0x36
NX_NOT_SUCCESSFUL	0x43
NX_NULL	0
NX_OPTION_ERROR	0x0a
NX_OVERFLOW	0x03
NX_PACKET_ALLOCATED	0xAAAAAAAA
NX_PACKET_DEBUG_LOG_SIZE	100
NX_PACKET_ENQUEUED	0xEEEEEEEE
NX_PACKET_FREE	0xFFFFFFFF
NX_PACKET_POOL_ID	0x5041434B
NX_PACKET_READY	0xBBBBBBBB
NX_PHYSICAL_HEADER	16

NX_PHYSICAL_TRAILER	4
NX_POOL_DELETED	0x30
NX_POOL_ERROR	0x06
NX_PORT_UNAVAILABLE	0x23
NX_PTR_ERROR	0x07
NX_RARP_HARDWARE_SIZE	0x06
NX_RARP_HARDWARE_TYPE	0x0001
NX_RARP_MESSAGE_SIZE	28
NX_RARP_OPTION_REQUEST	0x0003
NX_RARP_OPTION_RESPONSE	0x0004
NX_RARP_PROTOCOL_SIZE	0x04
NX_RARP_PROTOCOL_TYPE	0x0800
NX_RECEIVE_PACKET	0
NX_RESERVED_CODE0	0x19
NX_RESERVED_CODE1	0x25
NX_RESERVED_CODE2	0x32
NX_ROUTE_TABLE_MASK	0x1F
NX_ROUTE_TABLE_SIZE	32
NX_SEARCH_PORT_START	49152
NX_SHIFT_BY_16	16
NX_SIZE_ERROR	0x09
NX_SOCKET_UNBOUND	0x26
NX_SOCKETS_BOUND	0x28
NX_STILL_BOUND	0x42
NX_SUCCESS	0x00
NX_TCP_ACK_BIT	0x00100000
NX_TCP_ACK_TIMER_RATE	5
NX_TCP_CLIENT	1
NX_TCP_CLOSE_WAIT	6
NX_TCP_CLOSED	1
NX_TCP_CLOSING	9
NX_TCP_CONTROL_MASK	0x00170000
NX_TCP_EOL_KIND	0x00
NX_TCP_ESTABLISHED	5
NX_TCP_FAST_TIMER_RATE	10

NX_TCP_FIN_BIT	0x00010000
NX_TCP_FIN_WAIT_1	7
NX_TCP_FIN_WAIT_2	8
NX_TCP_HEADER_MASK	0xF0000000
NX_TCP_HEADER_SHIFT	28
NX_TCP_HEADER_SIZE	0x50000000
NX_TCP_ID	0x54435020
NX_TCP_KEEPALIVE_INITIAL	7200
NX_TCP_KEEPALIVE_RETRIES	10
NX_TCP_KEEPALIVE_RETRY	75
NX_TCP_LAST_ACK	11
NX_TCP_LISTEN_STATE	2
NX_TCP_MAXIMUM_RETRIES	10
NX_TCP_MAXIMUM_TX_QUEUE	20
NX_TCP_MSS_KIND	0x02
NX_TCP_MSS_OPTION	0x02040000
NX_TCP_MSS_SIZE	1460
NX_TCP_NOP_KIND	0x01
NX_TCP_OPTION_END	0x01010100
NX_TCP_PACKET (IPv6 enabled)	76
NX_TCP_PACKET (IPv6 disabled)	56
NX_TCP_PORT_TABLE_MASK	0x1F
NX_TCP_PORT_TABLE_SIZE	32
NX_TCP_PSH_BIT	0x00080000
NX_TCP_RETRY_SHIFT	0
NX_TCP_RST_BIT	0x00040000
NX_TCP_SERVER	2
NX_TCP_SYN_BIT	0x00020000
NX_TCP_SYN_HEADER	0x70000000
NX_TCP_SYN_RECEIVED	4
NX_TCP_SYN_SENT	3
NX_TCP_TIMED_WAIT	10
NX_TCP_TRANSMIT_TIMER_RATE	1
NX_TCP_URG_BIT	0x00200000
NX_TRUE	1

NX_TX_QUEUE_DEPTH	0x49
NX_UDP_ID	0x55445020
NX_UDP_PACKET (IPv6 enabled)	64
NX_UDP_PACKET (IPv6 disabled)	44
NX_UDP_PORT_TABLE_MASK	0x1F
NX_UDP_PORT_TABLE_SIZE	32
NX_UNDERFLOW	0x02
NX_UNHANDLED_COMMAND	0x44
NX_WAIT_ABORTED	0x1A
NX_WAIT_ERROR	0x08
NX_WAIT_FOREVER	0xFFFFFFFF
NX_WINDOW_OVERFLOW	0x39

Listings by Value

NX_ANY_PORT	0
NX_ARP_EXPIRATION_RATE	0
NX_FALSE	0
NX_ICMP_ECHO_REPLY_TYPE	0
NX_ICMP_NETWORK_UNREACH_CODE	0
NX_ICMPV6_NO_ROUTE_TO_DESTINATION_CODE	0
NX_IPV6_ADDRESS_INVALID	0
NX_IPV6_PROTOCOL_NEXT_HEADER_HOP_BY_HOP	0
NX_LINK_PACKET_SEND	0
NX_NO_WAIT	0
NX_NULL	0
NX_RECEIVE_PACKET	0
NX_TCP_RETRY_SHIFT	0
NX_IPV6_ADDR_STATE_UNKNOWN	0x00
NX_IPV6_ROUTE_TYPE_NOT_ROUTER	0x00
NX_SUCCESS	0x00
NX_TCP_EOL_KIND	0x00
NX_FRAGMENT_OKAY	0x00000000
NX_IP_CLASS_A_TYPE	0x00000000
NX_IP_CLASS_D_HOSTID	0x00000000
NX_IP_NORMAL	0x00000000
NX_FOREVER	1
NX_ICMP_HOST_UNREACH_CODE	1
NX_ICMPV6_COMMUNICATION_WITH_DESTINATION_PROHIBITED_CODE	1
NX_ICMPV6_DEST_UNREACHABLE_TYPE	1
NX_ICMPV6_NO_SLLA	1
NX_ICMPV6_OPTION_TYPE_SRC_LINK_ADDR	1
NX_IGMP_HOST_VERSION_1	1
NX_IGMP_TTL	1
NX_INIT_PACKET_ID	1
NX_IPV6_PROTOCOL_ICMP	1
NX_LINK_INITIALIZE	1
NX_TCP_CLIENT	1

NX_TCP_CLOSED	1
NX_TCP_TRANSMIT_TIMER_RATE	1
NX_TRUE	1
NX_IP_PERIODIC_EVENT	0x00000001
NX_IPV6_ADDRESS_LINKLOCAL	0x00000001
NX_ARP_HARDWARE_TYPE	0x0001
NX_ARP_OPTION_REQUEST	0x0001
NX_IP_INITIALIZE_DONE	0x0001
NX_RARP_HARDWARE_TYPE	0x0001
NX_IPV6_ADDR_STATE_TENTATIVE	0x01
NX_IPV6_ROUTE_TYPE_SOLICITATED	0x01
NX_NO_PACKET	0x01
NX_TCP_NOP_KIND	0x01
NX_ICMP_PROTOCOL_UNREACH_CODE	2
NX_ICMPV6_BEYOND_SCOPE_OF_SOURCE_ADDRESS_CODE	2
NX_ICMPV6_OPTION_TYPE_TRG_LINK_ADDR	2
NX_ICMPV6_PACKET_TOO_BIG_TYPE	2
NX_IGMP_HOST_VERSION_2	2
NX_LINK_ENABLE	2
NX_TCP_LISTEN_STATE	2
NX_TCP_SERVER	2
NX_IP_UNFRAG_EVENT	0x00000002
NX_IPV6_ADDRESS_SITELOCAL	0x00000002
NX_ARP_OPTION_RESPONSE	0x0002
NX_IP_ADDRESS_RESOLVED	0x0002
NX_IPV6_ADDR_STATE_PREFERRED	0x02
NX_IPV6_ROUTE_TYPE_UNSOLICITATED	0x02
NX_TCP_MSS_KIND	0x02
NX_UNDERFLOW	0x02
NX_ICMP_DEST_UNREACHABLE_TYPE	3
NX_ICMP_PORT_UNREACH_CODE	3
NX_ICMPV6_ADDRESS_UNREACHABLE_CODE	3
NX_ICMPV6_OPTION_TYPE_PREFIX_INFO	3
NX_ICMPV6_TIME_EXCEED_TYPE	3
NX_LINK_DISABLE	3

NX_TCP_SYN_SENT	3
NX_RARP_OPTION_REQUEST	0x0003
NX_IPV6_ADDR_STATE_DEPRECATED	0x03
NX_OVERFLOW	0x03
NX_ARP_MAX_QUEUE_DEPTH	4
NX_ICMP_FRAMENT_NEEDED_CODE	4
NX_ICMP_SOURCE_QUENCH_TYPE	4
NX_ICMPV6_DEST_UNREACHABLE_CODE	4
NX_ICMPV6_OPTION_REDIRECTED_HEADER	4
NX_ICMPV6_PARAMETER_PROBLEM_TYPE	4
NX_IPV6_PROTOCOL_IPV4	4
NX_LINK_PACKET_BROADCAST	4
NX_PHYSICAL_TRAILER	4
NX_TCP_SYN_RECEIVED	4
NX_IP_ICMP_EVENT	0x00000004
NX_IPV6_ADDRESS_GLOBAL	0x00000004
NX_IP_LINK_ENABLED	0x0004
NX_RARP_OPTION_RESPONSE	0x0004
NX_ARP_PROTOCOL_SIZE	0x04
NX_IPV6_ADDR_STATE_VALID	0x04
NX_IPV6_ROUTE_TYPE_STATIC	0x04
NX_NO_MAPPING	0x04
NX_RARP_PROTOCOL_SIZE	0x04
NX_ICMP_REDIRECT_TYPE	5
NX_ICMP_SOURCE_ROUTE_CODE	5
NX_ICMPV6_OPTION_TYPE_MTU	5
NX_ICMPV6_SOURCE_ADDRESS_FAILED_I_E_POLICY_CODE	5
NX_IP_NORMAL_LENGTH	5
NX_LINK_ARP_SEND	5
NX_TCP_ACK_TIMER_RATE	5
NX_TCP_ESTABLISHED	5
NX_DELETED	0x05
NX_ICMP_NETWORK_UNKNOWN_CODE	6
NX_ICMPV6_REJECT_ROUTE_TO_DESTINATION_CODE	6
NX_IPV6_PROTOCOL_TCP	6

NX_LINK_ARP_RESPONSE_SEND	6
NX_TCP_CLOSE_WAIT	6
NX_ARP_HARDWARE_SIZE	0x06
NX_POOL_ERROR	0x06
NX_RARP_HARDWARE_SIZE	0x06
NX_ICMP_HOST_UNKNOWN_CODE	7
NX_LINK_RARP_SEND	7
NX_MAX_MULTICAST_GROUPS	7
NX_TCP_FIN_WAIT_1	7
NX_PTR_ERROR	0x07
NX_ICMP_ECHO_REQUEST_TYPE	8
NX_ICMP_SOURCE_ISOLATED_CODE	8
NX_IP_ALIGN_FRAGS	8
NX_LINK_MULTICAST_JOIN	8
NX_TCP_FIN_WAIT_2	8
NX_IGMP_HEADER_SIZE	8
NX_IP_RECEIVE_EVENT	0x00000008
NX_IP_ARP_ENABLED	0x0008
NX_WAIT_ERROR	0x08
NX_ICMP_NETWORK_PROHIBIT_CODE	9
NX_LINK_MULTICAST_LEAVE	9
NX_TCP_CLOSING	9
NX_SIZE_ERROR	0x09
NX_ARP_UPDATE_RATE	10
NX_ICMP_HOST_PROHIBIT_CODE	10
NX_IGMP_MAX_UPDATE_TIME	10
NX_LINK_GET_STATUS	10
NX_MAX_LISTEN_REQUESTS	10
NX_TCP_FAST_TIMER_RATE	10
NX_TCP_KEEPALIVE_RETRIES	10
NX_TCP_MAXIMUM_RETRIES	10
NX_TCP_TIMED_WAIT	10
NX_IPV6_ALL_NODE_MCAST	0x00000010
NX_OPTION_ERROR	0x0A
NX_ICMP_NETWORK_SERVICE_CODE	11

NX_ICMP_TIME_EXCEEDED_TYPE	11
NX_LINK_GET_SPEED	11
NX_TCP_LAST_ACK	11
NX_ICMP_HOST_SERVICE_CODE	12
NX_ICMP_PARAMETER_PROB_TYPE	12
NX_LINK_GET_DUPLEX_TYPE	12
NX_ICMP_TIMESTAMP_REQ_TYPE	13
NX_LINK_GET_ERROR_COUNT	13
NX_ICMP_TIMESTAMP_REP_TYPE	14
NX_LINK_GET_RX_COUNT	14
NX_LINK_GET_TX_COUNT	15
NX_LINK_GET_ALLOC_ERRORS	16
NX_PHYSICAL_HEADER	16
NX_SHIFT_BY_16	16
NX_IP_ARP_REC_EVENT	0x00000010
NX_IP_UDP_ENABLED	0x0010
NX_DELETE_ERROR	0x10
NX_ICMP_ADDRESS_MASK_REQ_TYPE	17
NX_IPV6_PROTOCOL_UDP	17
NX_LINK_UNINITIALIZE	17
NX_CALLER_ERROR	0x11
NX_ARP_MAXIMUM_RETRIES	18
NX_ICMP_ADDRESS_MASK_REP_TYPE	18
NX_LINK_DEFERRED_PROCESSING	18
NX_INVALID_PACKET	0x12
NX_INVALID_SOCKET	0x13
NX_LINK_INTERFACE_ATTACH	19
NX_TCP_MAXIMUM_TX_QUEUE	20
NX_NOT_ENABLED	0x14
NX_ALREADY_ENABLED	0x15
NX_ENTRY_NOT_FOUND	0x16
NX_NO_MORE_ENTRIES	0x17
NX_IP_TIME_TO_LIVE_SHIFT	24
NX_ARP_TIMER_ERROR	0x18
NX_RESERVED_CODE0	0x19

NX_WAIT_ABORTED	0x1A
NX_ARP_MESSAGE_SIZE	28
NX_RARP_MESSAGE_SIZE	28
NX_TCP_HEADER_SHIFT	28
NX_ROUTE_TABLE_MASK	0x1F
NX_TCP_PORT_TABLE_MASK	0x1F
NX_UDP_PORT_TABLE_MASK	0x1F
NX_ROUTE_TABLE_SIZE	32
NX_TCP_PORT_TABLE_SIZE	32
NX_UDP_PORT_TABLE_SIZE	32
NX_IPV6_ALL_ROUTER_MCAST	0x00000020
NX_IP_RARP_REC_EVENT	0x00000020
NX_IP_TCP_ENABLED	0x0020
NX_IP_INTERNAL_ERROR	0x20
NX_IP_ADDRESS_ERROR	0x21
NX_ALREADY_BOUND	0x22
NX_PORT_UNAVAILABLE	0x23
NX_ICMP_PACKET	36
NX_IGMP_PACKET	36
NX_IP_PACKET	36
NX_IPV4_ICMP_PACKET	36
NX_IPV4_IGMP_PACKET	36
NX_NOT_BOUND	0x24
NX_RESERVED_CODE1	0x25
NX_SOCKET_UNBOUND	0x26
NX_NOT_CREATED	0x27
NX_SOCKETS_BOUND	0x28
NX_NO_RESPONSE	0x29
NX_IPV6_PROTOCOL_IPV6	41
NX_IPV6_PROTOCOL_NEXT_HEADER_ROUTING	43
NX_IPV4_UDP_PACKET	44
NX_IPV6_PROTOCOL_NEXT_HEADER_FRAGMENT	44
NX_UDP_PACKET	44
NX_POOL_DELETED	0x30
NX_ALREADY_RELEASED	0x31

NX_LINK_USER_COMMAND	50
NX_RESERVED_CODE2	0x32
NX_MAX_LISTEN	0x33
NX_DUPLICATE_LISTEN	0x34
NX_NOT_CLOSED	0x35
NX_NOT_LISTEN_STATE	0x36
NX_IN_PROGRESS	0x37
NX_NOT_CONNECTED	0x38
NX_IPV4_TCP_PACKET	56
NX_IPV6_ICMP_PACKET	56
NX_IPV6_IGMP_PACKET	56
NX_TCP_PACKET	56
NX_WINDOW_OVERFLOW	0x39
NX_IPV6_PROTOCOL_NEXT_HEADER_ICMPV6	58
NX_IPV6_PROTOCOL_ICMPV6	58
NX_IPV6_PROTOCOL_NO_NEXT_HEADER	59
NX_IPV6_PROTOCOL_NEXT_HEADER_DESTINATION	60
NX_IPV6_UDP_PACKET	64
NX_IPV6_SOLICITED_NODE_MCAST	0x00000040
NX_IP_IGMP_EVENT	0x00000040
NX_IP_IGMP_ENABLED	0x0040
NX_ALREADY_SUSPENDED	0x40
NX_IPV6_ROUTE_TYPE_DEFAULT	0x40
NX_DISCONNECT_FAILED	0x41
NX_STILL_BOUND	0x42
NX_NOT_SUCCESSFUL	0x43
NX_UNHANDLED_COMMAND	0x44
NX_NO_FREE_PORTS	0x45
NX_INVALID_PORT	0x46
NX_INVALID_RELISTEN	0x47
NX_CONNECTION_PENDING	0x48
NX_TX_QUEUE_DEPTH	0x49
NX_NOT_IMPLEMENTED	0x4A
NX_NOT_SUPPORTED	0x4B
NX_TCP_KEEPALIVE_RETRY	75

NX_INVALID_INTERFACE	0x4C
NX_IPV6_TCP_PACKET	76
NX_ARP_DEBUG_LOG_SIZE	100
NX_ICMP_DEBUG_LOG_SIZE	100
NX_IGMP_DEBUG_LOG_SIZE	100
NX_IP_DEBUG_LOG_SIZE	100
NX_IP_PERIODIC_RATE	100
NX_PACKET_DEBUG_LOG_SIZE	100
NX_RARP_DEBUG_LOG_SIZE	100
NX_TCP_DEBUG_LOG_SIZE	100
NX_UDP_DEBUG_LOG_SIZE	100
NX_IP_TCP_EVENT	0x00000080
NX_IP_TIME_TO_LIVE	0x00000080
NX_IP_RARP_COMPLETE	0x0080
NX_IPV6_ROUTE_TYPE_VALID	0x80
NX_NOT_IMPLEMENTED	0x4A
NX_IP_CLASS_C_HOSTID	0x000000FF
NX_IP_MULTICAST_UPPER	0x00000100
NX_IP_TCP_FAST_EVENT	0x00000100
NX_IP_DRIVER_PACKET_EVENT	0x00000200
NX_IP_IGMP_ENABLE_EVENT	0x00000400
NX_IP_DRIVER_DEFERRED_EVENT	0x00000800
NX_ARP_PROTOCOL_TYPE	0x0800
NX_RARP_PROTOCOL_TYPE	0x0800
NX_IP_TCP_CLEANUP_DEFERRED	0x00001000
NX_ICMPV6_ECHO_REQUEST_TYPE	128
NX_ICMPV6_ECHO_REPLY_TYPE	129
NX_ICMPV6_ROUTER_SOLICITATION_TYPE	133
NX_ICMPV6_ROUTER_ADVERTISEMENT_TYPE	134
NX_ICMPV6_NEIGHBOR_SOLICITATION_TYPE	135
NX_ICMPV6_NEIGHBOR_ADVERTISEMENT_TYPE	136
NX_ICMPV6_REDIRECT_MESSAGE_TYPE	137
NX_ICMPV6_MINIMUM_IPV4_PATH_MTU	576
NX_ICMPV6_MINIMUM_IPV6_PATH_MTU	1280
NX_TCP_KEEPALIVE_INITIAL	7200

NX_FRAG_OFFSET_MASK	0x00001FFF
NX_IP_OFFSET_MASK	0x00001FFF
NX_IP_MORE_FRAGMENT	0x00002000
NX_MORE_FRAGMENTS	0x00002000
NX_IP_FRAGMENT_MASK	0x00003FFF
NX_TCP_MSS_SIZE	16384
NX_DONT_FRAGMENT	0x00004000
NX_IP_DONT_FRAGMENT	0x00004000
NX_SEARCH_PORT_START	49152
NX_IP_CLASS_B_HOSTID	0x0000FFFF
NX_IP_PACKET_SIZE_MASK	0x0000FFFF
NX_LOWER_16_MASK	0x0000FFFF
NX_MAX_PORT	0xFFFF
NX_IP_ICMP	0x00010000
NX_TCP_FIN_BIT	0x00010000
NX_CARRY_BIT	0x10000
NX_IP_IGMP	0x00020000
NX_IP_MIN_COST	0x00020000
NX_TCP_SYN_BIT	0x00020000
NX_IP_MAX_RELIABLE	0x00040000
NX_TCP_RST_BIT	0x00040000
NX_IP_TCP	0x00060000
NX_IP_MAX_DATA	0x00080000
NX_TCP_PSH_BIT	0x00080000
NX_IP_MIN_DELAY	0x00100000
NX_TCP_ACK_BIT	0x00100000
NX_IP_UDP	0x00110000
NX_TCP_CONTROL_MASK	0x00170000
NX_TCP_URG_BIT	0x00200000
NX_IP_MULTICAST_MASK	0x007FFFFF
NX_IP_PROTOCOL_MASK	0x00FF0000
NX_IP_TOS_MASK	0x00FF0000
NX_IGMP_ROUTER_QUERY_TYPE	0x01000000
NX_TCP_OPTION_END	0x01010402
NX_IGMP_HOST_RESPONSE_TYPE	0x02000000

NX_TCP_MSS_OPTION	0x02040000
NX_IGMP_TYPE_MASK	0x0F000000
NX_IP_LENGTH_MASK	0x0F000000
NX_IGMP_MAX_RESP_TIME_MASK	0x00FF0000
NX_IP_CLASS_A_HOSTID	0x00FFFFFF
NX_IP_CLASS_D_GROUP	0x0FFFFFFF
NX_IGMP_VERSION	0x10000000
NX_IPV6_ADDRESS_LOOPBACK	0x10000000
NX_IGMP_HOST_V2_JOIN_TYPE	0x16000000
NX_IGMP_HOST_V2_LEAVE_TYPE	0x17000000
NX_IPV6_ADDRESS_UNSPECIFIED	0x20000000
NX_IP_CLASS_C_NETID	0x1FFFFF00
NX_IP_CLASS_B_NETID	0x3FFF0000
NX_IPV6_ADDRESS_MULTICAST	0x40000000
NX_IP_VERSION	0x45000000
NX_IP_ID	0x49502020
NX_TCP_HEADER_SIZE	0x50000000
NX_PACKET_POOL_ID	0x5041434B
NX_TCP_ID	0x54435020
NX_UDP_ID	0x55445020
NX_IP_MULTICAST_LOWER	0x5E000000
NX_IP_CLASS_A_NETID	0x7F000000
NX_TCP_SYN_HEADER	0x70000000
NX_IP_LOOPBACK_FIRST	0x7F000000
NX_IP_LOOPBACK_LAST	0x7FFFFFFF
NX_IP_CLASS_A_MASK	0x80000000
NX_IP_CLASS_B_TYPE	0x80000000
NX_IPV6_ADDRESS_UNICAST	0x80000000
NX_PACKET_ALLOCATED	0xAAAAAAAA
NX_PACKET_READY	0xBBBBBBBB
NX_IP_CLASS_B_MASK	0xC0000000
NX_IP_CLASS_C_TYPE	0xC0000000
NX_DRIVER_TX_DONE	0xDDDDDDDD
NX_IP_CLASS_C_MASK	0xE0000000
NX_IP_CLASS_D_TYPE	0xE0000000

NX_PACKET_ENQUEUED	0xEEEEEEEE
NX_IGMP_VERSION_MASK	0xF0000000
NX_IP_CLASS_D_MASK	0xF0000000
NX_TCP_HEADER_MASK	0xF0000000
NX_ALL_HOSTS_ADDRESS	0xFE000001
NX_IGMPV2_TYPE_MASK	0xFF000000
NX_IP_TIME_TO_LIVE_MASK	0xFF000000
NX_ICMPV6_PATH_MTU_INFINITE_TIMEOUT	0xFFFFFFFF
NX_IP_ALL_EVENTS	0xFFFFFFFF
NX_IP_LIMITIED_BROADCAST	0xFFFFFFFF
NX_PACKET_FREE	0xFFFFFFFF
NX_WAIT_FOREVER	0xFFFFFFFF

Appendix C: NetX Duo Data Types

```
typedef struct NX_ARP_STRUCT
{

    UINT                                    nx_arp_route_static;
    UINT                                    nx_arp_entry_next_update;
    UINT                                    nx_arp_retries;
    struct NX_ARP_STRUCT                    *nx_arp_pool_next,
                                            *nx_arp_pool_previous;
    struct NX_ARP_STRUCT                    *nx_arp_active_next,
                                            *nx_arp_active_previous,
                                            **nx_arp_active_list_head;
    ULONG                                   nx_arp_ip_address;
    ULONG                                   nx_arp_physical_address_msw;
    ULONG                                   nx_arp_physical_address_lsw;
    struct NX_INTERFACE_STRUCT              *nx_arp_ip_interface;
    struct NX_PACKET_STRUCT                 *nx_arp_packets_waiting;
} NX_ARP;


typedef struct NX_INTERFACE_STRUCT
{
    CHAR                                    *nx_interface_name;
    UCHAR                                   nx_interface_valid;
    UCHAR                                   nx_interface_address_mapping_needed;
    UCHAR                                   nx_interface_link_up;
    UCHAR                                   nx_interface_index;
    UCHAR                                   nx_interface_link_status_change;
    UCHAR                                   nx_interface_reserved[3];
    struct NX_IP_STRUCT                     *nx_interface_ip_instance;
    ULONG                                   nx_interface_physical_address_msw;
    ULONG                                   nx_interface_physical_address_lsw;
    ULONG                                   nx_interface_ip_address;
    ULONG                                   nx_interface_ip_network_mask;
    ULONG                                   nx_interface_ip_network;
    struct NXD_IPV6_ADDRESS_STRUCT          *nxd_interface_ipv6_address_list_head;
    ULONG                                   nx_interface_ip_mtu_size;
#ifndef NX_DISABLE_ICMPV6_ROUTER_SOLICITATION
    ULONG                                   nx_ipv6_rtr_solicitation_max;
    ULONG                                   nx_ipv6_rtr_solicitation_count;
    ULONG                                   nx_ipv6_rtr_solicitation_interval;
    ULONG                                   nx_ipv6_rtr_solicitation_timer;
#endif /* NX_DISABLE_ICMPV6_ROUTER_SOLICITATION */

#ifdef NX_IPV6_STATELESS_AUTOCONFIG_CONTROL
    ULONG                                   nx_ipv6_stateless_address_autoconfig_status;
#endif /* NX_IPV6_STATELESS_AUTOCONFIG_CONTROL    */
    VOID                                    *nx_interface_additional_link_info;
    VOID                                    (*nx_interface_link_driver_entry)
                                                    (struct NX_IP_DRIVER_STRUCT *);
#ifdef NX_ENABLE_INTERFACE_CAPABILITY
    ULONG                                   nx_interface_capability_flag;
#endif /* NX_ENABLE_INTERFACE_CAPABILITY */
    ULONG                                   nx_interface_arp_defend_timeout;
    CHAR                                    *nx_interface_name;
    UCHAR                                   nx_interface_valid;
    UCHAR                                   nx_interface_address_mapping_needed;
    UCHAR                                   nx_interface_link_up;
    UCHAR                                   reserved;
    struct NX_IP_STRUCT                     *nx_interface_ip_instance;
    ULONG                                   nx_interface_physical_address_msw;
    ULONG                                   nx_interface_physical_address_lsw;
    ULONG                                   nx_interface_ip_address;
    ULONG                                   nx_interface_ip_network_mask;
    ULONG                                   nx_interface_ip_network;
    struct NXD_IPV6_ADDRESS_STRUCT          *nxd_interface_ipv6_address_list_head;
    ULONG                                   nx_interface_ip_mtu_size;
    VOID                                    *nx_interface_additional_link_info;
    VOID                                    (*nx_interface_link_driver_entry)
                                                    (struct NX_IP_DRIVER_STRUCT *);
} NX_INTERFACE;
```

```
typedef struct NX_IP_STRUCT
{
    ULONG                                   nx_ip_id;
    CHAR                                    *nx_ip_name;

#define nx_ip_address                       nx_ip_interface[0].nx_interface_ip_address
#define nx_ip_driver_mtu                    nx_ip_interface[0].nx_interface_ip_mtu_size
#define nx_ip_driver_mapping_needed         nx_ip_interface[0].nx_interface_address_mapping_needed
#define nx_ip_network_mask                  nx_ip_interface[0].nx_interface_ip_network_mask
#define nx_ip_network                       nx_ip_interface[0].nx_interface_ip_network
#define nx_ip_arp_physical_address_msw      nx_ip_interface[0].nx_interface_physical_address_msw
#define nx_ip_arp_physical_address_lsw      nx_ip_interface[0].nx_interface_physical_address_lsw
#define nx_ip_driver_link_up                nx_ip_interface[0].nx_interface_link_up
#define nx_ip_link_driver_entry             nx_ip_interface[0].nx_interface_link_driver_entry
#define nx_ip_additional_link_info          nx_ip_interface[0].nx_interface_additional_link_info

    ULONG                                   nx_ip_gateway_address;
    struct NX_INTERFACE_STRUCT              *nx_ip_gateway_interface;
#ifdef FEATURE_NX_IPV6
    struct NXD_IPV6_ADDRESS_STRUCT          nx_ipv6_address[NX_MAX_IPV6_ADDRESSES];
#endif /* FEATURE_NX_IPV6 */
    ULONG                                   nx_ip_total_packet_send_requests;
    ULONG                                   nx_ip_total_packets_sent;
    ULONG                                   nx_ip_total_bytes_sent;
    ULONG                                   nx_ip_total_packets_received;
    ULONG                                   nx_ip_total_packets_delivered;
    ULONG                                   nx_ip_total_bytes_received;
    ULONG                                   nx_ip_packets_forwarded;
    ULONG                                   nx_ip_packets_reassembled;
    ULONG                                   nx_ip_reassembly_failures;
    ULONG                                   nx_ip_invalid_packets;
    ULONG                                   nx_ip_invalid_transmit_packets;
    ULONG                                   nx_ip_invalid_receive_address;
    ULONG                                   nx_ip_unknown_protocols_received;
    ULONG                                   nx_ip_transmit_resource_errors;
    ULONG                                   nx_ip_transmit_no_route_errors;
    ULONG                                   nx_ip_receive_packets_dropped;
    ULONG                                   nx_ip_receive_checksum_errors;
    ULONG                                   nx_ip_send_packets_dropped;
    ULONG                                   nx_ip_total_fragment_requests;
    ULONG                                   nx_ip_successful_fragment_requests;
    ULONG                                   nx_ip_fragment_failures;
    ULONG                                   nx_ip_total_fragments_sent;
    ULONG                                   nx_ip_total_fragments_received;
    ULONG                                   nx_ip_arp_requests_sent;
    ULONG                                   nx_ip_arp_requests_received;
    ULONG                                   nx_ip_arp_responses_sent;
    ULONG                                   nx_ip_arp_responses_received;
    ULONG                                   nx_ip_arp_aged_entries;
    ULONG                                   nx_ip_arp_invalid_messages;
    ULONG                                   nx_ip_arp_static_entries;
    ULONG                                   nx_ip_udp_packets_sent;
    ULONG                                   nx_ip_udp_bytes_sent;
    ULONG                                   nx_ip_udp_packets_received;
    ULONG                                   nx_ip_udp_bytes_received;
    ULONG                                   nx_ip_udp_invalid_packets;
    ULONG                                   nx_ip_udp_no_port_for_delivery;
    ULONG                                   nx_ip_udp_receive_packets_dropped;
    ULONG                                   nx_ip_udp_checksum_errors;
    ULONG                                   nx_ip_tcp_packets_sent;
    ULONG                                   nx_ip_tcp_bytes_sent;
    ULONG                                   nx_ip_tcp_packets_received;
    ULONG                                   nx_ip_tcp_bytes_received;
    ULONG                                   nx_ip_tcp_invalid_packets;
    ULONG                                   nx_ip_tcp_receive_packets_dropped;
    ULONG                                   nx_ip_tcp_checksum_errors;
    ULONG                                   nx_ip_tcp_connections;
    ULONG                                   nx_ip_tcp_passive_connections;
```

```
    ULONG                                   nx_ip_tcp_active_connections;
    ULONG                                   nx_ip_tcp_disconnections;
    ULONG                                   nx_ip_tcp_connections_dropped;
    ULONG                                   nx_ip_tcp_retransmit_packets;
    ULONG                                   nx_ip_tcp_resets_received;
    ULONG                                   nx_ip_tcp_resets_sent;
    ULONG                                   nx_ip_icmp_total_messages_received;
    ULONG                                   nx_ip_icmp_checksum_errors;
    ULONG                                   nx_ip_icmp_invalid_packets;
    ULONG                                   nx_ip_icmp_unhandled_messages;
    ULONG                                   nx_ip_pings_sent;
    ULONG                                   nx_ip_ping_timeouts;
    ULONG                                   nx_ip_ping_threads_suspended;
    ULONG                                   nx_ip_ping_responses_received;
    ULONG                                   nx_ip_pings_received;
    ULONG                                   nx_ip_pings_responded_to;
    ULONG                                   nx_ip_igmp_invalid_packets;
    ULONG                                   nx_ip_igmp_reports_sent;
    ULONG                                   nx_ip_igmp_queries_received;
    ULONG                                   nx_ip_igmp_checksum_errors;
    ULONG                                   nx_ip_igmp_groups_joined;
#ifndef NX_DISABLE_IGMPV2
    ULONG                                   nx_ip_igmp_router_version;
#endif
    ULONG                                   nx_ip_rarp_requests_sent;
    ULONG                                   nx_ip_rarp_responses_received;
    ULONG                                   nx_ip_rarp_invalid_messages;
    VOID                                    (*nx_ip_forward_packet_process)
                                                    (struct NX_IP_STRUCT *, NX_PACKET *);
#ifdef NX_NAT_ENABLE
    UINT                                    (*nx_ip_nat_packet_process)(struct NX_IP_STRUCT *,
                                                                       NX_PACKET *);
    UINT                                    (*nx_ip_nat_port_verify)(struct NX_IP_STRUCT *, UINT
                                                                    protocol, UINT port);
#endif
    ULONG                                   nx_ip_packet_id;
    struct NX_PACKET_POOL_STRUCT            *nx_ip_default_packet_pool;
#ifdef NX_ENABLE_DUAL_PACKET_POOL
    struct NX_PACKET_POOL_STRUCT            *nx_ip_auxiliary_packet_pool;
#endif /* NX_ENABLE_DUAL_PACKET_POOL */
    TX_MUTEX                                nx_ip_protection;
    UINT                                    nx_ip_initialize_done;
    NX_PACKET                               *nx_ip_driver_deferred_packet_head,
                                            *nx_ip_driver_deferred_packet_tail;
    VOID                                    (*nx_ip_driver_deferred_packet_handler)(struct
                                                      NX_IP_STRUCT *, NX_PACKET *);
    NX_PACKET                               *nx_ip_deferred_received_packet_head,
                                            *nx_ip_deferred_received_packet_tail;
    UINT                                    (*nx_ip_raw_ip_processing)(struct NX_IP_STRUCT *,
                                                                      ULONG, NX_PACKET *);
#ifdef NX_ENABLE_IP_RAW_PACKET_FILTER
    UINT                                    (*nx_ip_raw_packet_filter)(struct NX_IP_STRUCT *,
                                                                      ULONG, NX_PACKET *);
#endif /* NX_ENABLE_IP_RAW_PACKET_FILTER */
    NX_PACKET                               *nx_ip_raw_received_packet_head,
                                            *nx_ip_raw_received_packet_tail;
    ULONG                                   nx_ip_raw_received_packet_count;
    ULONG                                   nx_ip_raw_received_packet_max;
    TX_THREAD                               *nx_ip_raw_packet_suspension_list;
    ULONG                                   nx_ip_raw_packet_suspended_count;
    TX_THREAD                               nx_ip_thread;
    TX_EVENT_FLAGS_GROUP                    nx_ip_events;
    TX_TIMER                                nx_ip_periodic_timer;
    VOID                                    (*nx_ip_fragment_processing)(struct
                                                      NX_IP_DRIVER_STRUCT *);
    VOID                                    (*nx_ip_fragment_assembly)(struct NX_IP_STRUCT *);
    VOID                                    (*nx_ip_fragment_timeout_check)
                                                       (struct NX_IP_STRUCT *);
    NX_PACKET                               *nx_ip_timeout_fragment;
```

```
    NX_PACKET                               *nx_ip_received_fragment_head,
                                            *nx_ip_received_fragment_tail;
    NX_PACKET                               *nx_ip_fragment_assembly_head,
                                            *nx_ip_fragment_assembly_tail;
    VOID                                    (*nx_ip_address_change_notify)(struct NX_IP_STRUCT *,
                                                                           VOID *);
    VOID                                    *nx_ip_address_change_notify_additional_info;

#ifdef FEATURE_NX_IPV6
#ifdef NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY
    VOID                                    (*nx_ipv6_address_change_notify)(struct NX_IP_STRUCT *,
                                                                             UINT, UINT, UINT,
                                                                             ULONG*);
#endif /* NX_ENABLE_IPV6_ADDRESS_CHANGE_NOTIFY */
#endif /* FEATURE_NX_IPV6 */
    NX_IPV4_MULTICAST_ENTRY                 nx_ipv4_multicast_entry[NX_MAX_MULTICAST_GROUPS];
    UINT                                    nx_ip_igmp_global_loopback_enable;
    void                                    (*nx_ip_igmp_packet_receive)(struct NX_IP_STRUCT *,
                                                                        struct NX_PACKET_STRUCT *);
    void                                    (*nx_ip_igmp_periodic_processing)
                                                      (struct NX_IP_STRUCT *);
    void                                    (*nx_ip_igmp_queue_process)(struct NX_IP_STRUCT *);
    NX_PACKET                               *nx_ip_igmp_queue_head;
    ULONG                                   nx_ip_icmp_sequence;
#ifdef NX_ENABLE_IPV6_MULTICAST
    NX_IPV6_MULTICAST_ENTRY                 nx_ipv6_multicast_entry[NX_MAX_MULTICAST_GROUPS];
    ULONG                                   nx_ipv6_multicast_groups_joined;
#endif /* NX_ENABLE_IPV6_MULTICAST  */
    void                                    (*nx_ip_icmp_packet_receive)(struct NX_IP_STRUCT *,
                                                                     struct NX_PACKET_STRUCT *);
    void                                    (*nx_ip_icmp_queue_process)(struct NX_IP_STRUCT *);
    void                                    (*nx_ip_icmpv4_packet_process)(struct NX_IP_STRUCT *,
                                                                           NX_PACKET *);
#ifdef FEATURE_NX_IPV6
    void                                    (*nx_ip_icmpv6_packet_process)(struct NX_IP_STRUCT *,
                                                                           NX_PACKET *);
    void                                    (*nx_icmpv6_process_router_advertisement)(struct
                                                                 NX_IP_STRUCT *, NX_PACKET *)
    void                                    (*nx_nd_cache_fast_periodic_update)(struct
                                                                                NX_IP_STRUCT *);
    void                                    (*nx_nd_cache_slow_periodic_update)(struct
                                                                                NX_IP_STRUCT *);
    void                                    (*nx_icmpv6_ra_flag_callback)(struct NX_IP_STRUCT *,
                                                                          UINT);

#ifdef NX_ENABLE_IPV6_PATH_MTU_DISCOVERY
    void                                    (*nx_destination_table_periodic_update)(struct
                                                                           NX_IP_STRUCT *);
#endif

#endif /* FEATURE_NX_IPV6 */
    NX_PACKET                               *nx_ip_icmp_queue_head;
    TX_THREAD                               *nx_ip_icmp_ping_suspension_list;
    ULONG                                   nx_ip_icmp_ping_suspended_count;
    struct NX_UDP_SOCKET_STRUCT             *nx_ip_udp_port_table[NX_UDP_PORT_TABLE_SIZE];
    struct NX_UDP_SOCKET_STRUCT             *nx_ip_udp_created_sockets_ptr;
    ULONG                                   nx_ip_udp_created_sockets_count;
    void                                    (*nx_ip_udp_packet_receive)(struct NX_IP_STRUCT *,
                                                                        struct NX_PACKET_STRUCT *);
    UINT                                    nx_ip_udp_port_search_start;
    struct NX_TCP_SOCKET_STRUCT             *nx_ip_tcp_port_table[NX_TCP_PORT_TABLE_SIZE];
    struct NX_TCP_SOCKET_STRUCT             *nx_ip_tcp_created_sockets_ptr;
    ULONG                                   nx_ip_tcp_created_sockets_count;
    void                                    (*nx_ip_tcp_packet_receive)(struct NX_IP_STRUCT *,
                                                                        struct NX_PACKET_STRUCT *);
    void                                    (*nx_ip_tcp_periodic_processing)
                                                                         (struct NX_IP_STRUCT *);
    void                                    (*nx_ip_tcp_fast_periodic_processing)(struct
                                                                                NX_IP_STRUCT *);
```

```
    void                                    (*nx_ip_tcp_queue_process)(struct NX_IP_STRUCT *);
    NX_PACKET                               *nx_ip_tcp_queue_head,
                                            *nx_ip_tcp_queue_tail;
    ULONG                                   nx_ip_tcp_received_packet_count;
    struct NX_TCP_LISTEN_STRUCT             nx_ip_tcp_server_listen_reqs[NX_MAX_LISTEN_REQUESTS];
    struct NX_TCP_LISTEN_STRUCT             *nx_ip_tcp_available_listen_requests;
    struct NX_TCP_LISTEN_STRUCT             *nx_ip_tcp_active_listen_requests;
    UINT                                    nx_ip_tcp_port_search_start;
    UINT                                    nx_ip_fast_periodic_timer_created;
    TX_TIMER                                nx_ip_fast_periodic_timer;
    struct NX_ARP_STRUCT                    *nx_ip_arp_table[NX_ARP_TABLE_SIZE];
    struct NX_ARP_STRUCT                    *nx_ip_arp_static_list;
    struct NX_ARP_STRUCT                    *nx_ip_arp_dynamic_list;
    ULONG                                   nx_ip_arp_dynamic_active_count;
    NX_PACKET                               *nx_ip_arp_deferred_received_packet_head,
                                            *nx_ip_arp_deferred_received_packet_tail;
    UINT                                    (*nx_ip_arp_allocate)(struct NX_IP_STRUCT *, struct
                                                                  NX_ARP_STRUCT **, UINT);
    void                                    (*nx_ip_arp_periodic_update)(struct NX_IP_STRUCT *);
    void                                    (*nx_ip_arp_queue_process)(struct NX_IP_STRUCT *);
    void                                    (*nx_ip_arp_packet_send)(struct NX_IP_STRUCT *, ULONG
                                                                     destination_ip, NX_INTERFACE
                                                                     *nx_interface);
    void                                    (*nx_ip_arp_gratuitous_response_handler)(struct
                                                                 NX_IP_STRUCT *, NX_PACKET *);
    void                                    (*nx_ip_arp_collision_notify_response_handler)
                                                                                       (void *);
    void                                    *nx_ip_arp_collision_notify_parameter;
    ULONG                                   nx_ip_arp_collision_notify_ip_address;
    struct NX_ARP_STRUCT                    *nx_ip_arp_cache_memory;
    ULONG                                   nx_ip_arp_total_entries;
    void                                    (*nx_ip_rarp_periodic_update)(struct NX_IP_STRUCT *);
    void                                    (*nx_ip_rarp_queue_process)(struct NX_IP_STRUCT *);
    NX_PACKET                               *nx_ip_rarp_deferred_received_packet_head,
                                            *nx_ip_rarp_deferred_received_packet_tail;
    struct NX_IP_STRUCT                     *nx_ip_created_next,
                                            *nx_ip_created_previous;
    void                                    *nx_ip_reserved_ptr;
    void                                    (*nx_tcp_deferred_cleanup_check)
                                                                  (struct NX_IP_STRUCT *);
    NX_INTERFACE                            nx_ip_interface[NX_MAX_IP_INTERFACES];
    void                                    (*nx_ipv4_packet_receive)(struct NX_IP_STRUCT *,
                                                                      NX_PACKET *);
#ifdef NX_ENABLE_IP_STATIC_ROUTING
    NX_IP_ROUTING_ENTRY                     nx_ip_routing_table[NX_IP_ROUTING_TABLE_SIZE];
    ULONG                                   nx_ip_routing_table_entry_count;
#endif /* NX_ENABLE_IP_STATIC_ROUTING */
#ifdef FEATURE_NX_IPV6
    USHORT                                  nx_ipv6_default_router_table_size;
    NX_IPV6_DEFAULT_ROUTER_ENTRY  nx_ipv6_default_router_table[NX_IPV6_DEFAULT_ROUTER_TABLE_SIZE];
    UINT                                    nx_ipv6_default_router_table_round_robin_index;
    NX_IPV6_PREFIX_ENTRY          nx_ipv6_prefix_list_table [NX_IPV6_PREFIX_LIST_TABLE_SIZE];
    NX_IPV6_PREFIX_ENTRY *nx_ipv6_prefix_list_ptr;
    NX_IPV6_PREFIX_ENTRY *nx_ipv6_prefix_entry_free_list;

    /* Define the IPv6 packet receive processing routine */
    void                                    (*nx_ipv6_packet_receive)(struct NX_IP_STRUCT *,
                                                                      NX_PACKET *);
    ULONG                                   nx_ipv6_retrans_timer_ticks;
    ULONG                                   nx_ipv6_reachable_timer;
    ULONG                                   nx_ipv6_hop_limit;
#endif /* FEATURE_NX_IPV6 */

#ifdef NX_IPSEC_ENABLE
    UINT                                    (*nx_ip_ipsec_authentication_header_receive)(struct
                                               NX_IP_STRUCT *, NX_PACKET *, ULONG *, NX_PACKET **);
    UINT                                    (*nx_ip_ipsec_authentication_header_transmit)(struct
                                                NX_IP_STRUCT *, NX_PACKET **, UINT, UINT);
```

```
    UINT                                    (*nx_ip_ipsec_encapsulating_security_payload_receive)
                                               (struct NX_IP_STRUCT *, NX_PACKET *, ULONG *,
                                                        NX_PACKET **);
    UINT                                    (*nx_ip_ipsec_encapsulating_security_payload_transmit)
                                                (struct NX_IP_STRUCT *, NX_PACKET **, UINT);
    UINT                                    (*nx_ip_packet_egress_sa_lookup)(struct NX_IP_STRUCT
                                                         *ip_ptr, NXD_ADDRESS *src_address,
                                                         NXD_ADDRESS *dst_address, UCHAR protocol,
                                                         ULONG src_port, ULONG dest_port,
                                                         ULONG *data_offset, VOID **sa_ptr, UINT
                                                         option);
    VOID                                    *nx_ip_ipsec_ingress_sa_ptr;
    VOID                                    *nx_ip_ipsec_egress_sa_ptr;
    VOID                                    *nx_ip_ipsec_ikev2_ptr;
    NX_PACKET                               *nx_ip_hw_done_packet_header_ptr;
    NX_PACKET                               *nx_ip_hw_done_packet_tail_ptr;
#endif /* NX_IPSEC_ENABLE */
    VOID                                    (*nx_ip_link_status_change_callback)(struct
                                                                  NX_IP_STRUCT *, UINT, UINT);
#ifdef NX_ENABLE_IP_PACKET_FILTER
    UINT                                    (*nx_ip_packet_filter)(VOID *, UINT);
#endif /* NX_ENABLE_IP_PACKET_FILTER */
} NX_IP;

typedef struct NX_IP_DRIVER_STRUCT
{
    UINT                                    nx_ip_driver_command;
    UINT                                    nx_ip_driver_status;
    ULONG                                   nx_ip_driver_physical_address_msw;
    ULONG                                   nx_ip_driver_physical_address_lsw;
    NX_PACKET                               *nx_ip_driver_packet;
    ULONG                                   *nx_ip_driver_return_ptr;
    struct NX_IP_STRUCT                     *nx_ip_driver_ptr;
    NX_INTERFACE                            *nx_ip_driver_interface;
} NX_IP_DRIVER;

typedef struct NX_IP_ROUTING_ENTRY_STRUCT
{
    ULONG                                   nx_ip_routing_dest_ip;
    ULONG                                   nx_ip_routing_net_mask;
    ULONG                                   nx_ip_routing_next_hop_address;
    NX_INTERFACE                            *nx_ip_routing_entry_ip_interface;
} NX_IP_ROUTING_ENTRY;

typedef struct NX_IPV6_DEFAULT_ROUTER_ENTRY_STRUCT
{
    UCHAR                                   nx_ipv6_default_router_entry_flag;
    UCHAR                                   nx_ipv6_default_router_entry_reserved;
    USHORT                                  nx_ipv6_default_router_entry_life_time;
    ULONG                                   nx_ipv6_default_router_entry_router_address[4];
    struct NX_INTERFACE_STRUCT              *nx_ipv6_default_router_entry_interface_ptr;
    VOID                                    *nx_ipv6_default_router_entry_neighbor_cache_ptr;
} NX_IPV6_DEFAULT_ROUTER_ENTRY;
#endif /* FEATURE_NX_IPV6 */


typedef struct NX_IPV6_PREFIX_ENTRY_STRUCT
{
    ULONG                                   nx_ipv6_prefix_entry_network_address[4];
    ULONG                                   nx_ipv6_prefix_entry_prefix_length;
    ULONG                                   nx_ipv6_prefix_entry_valid_lifetime;
    struct NX_IPV6_PREFIX_ENTRY_STRUCT      * nx_ipv6_prefix_entry_prev;
    struct NX_IPV6_PREFIX_ENTRY_STRUCT      * nx_ipv6_prefix_entry_next;
} NX_IPV6_PREFIX_ENTRY;

typedef  struct NX_PACKET_STRUCT
{
    struct NX_PACKET_POOL_STRUCT            *nx_packet_pool_owner;
#ifndef NX_DISABLE_PACKET_CHAIN
```

```
    struct NX_PACKET_STRUCT                 *nx_packet_next;
#endif /* NX_DISABLE_PACKET_CHAIN */
    UCHAR                                   *nx_packet_prepend_ptr;
    UCHAR                                   *nx_packet_append_ptr;
    UCHAR                                   *nx_packet_data_start;
    UCHAR                                   *nx_packet_data_end;
#ifndef NX_DISABLE_PACKET_CHAIN
    struct NX_PACKET_STRUCT                 *nx_packet_last;
    struct NX_PACKET_STRUCT                 *nx_packet_queue_next;
    union
    {
        struct NX_PACKET_STRUCT             *nx_packet_tcp_queue_next;

#ifndef NX_DISABLE_FRAGMENTATION
        struct NX_PACKET_STRUCT             *nx_packet_fragment_next;
#endif /* NX_DISABLE_FRAGMENTATION */
    } nx_packet_union_next;
    ULONG                                   nx_packet_length;
#ifndef NX_DISABLE_FRAGMENTATION
    ULONG                                   nx_packet_reassembly_time;
#endif /* NX_DISABLE_FRAGMENTATION */
#ifdef FEATURE_NX_IPV6
    UCHAR                                   nx_packet_option_state;
    UCHAR                                   nx_packet_destination_header;
    USHORT                                  nx_packet_option_offset;
#endif /* FEATURE_NX_IPV6 */
    UCHAR                                   nx_packet_ip_version;
    UCHAR                                   nx_packet_identical_copy;
    UCHAR                                   nx_packet_reserved[2];
    union
    {
        struct NX_INTERFACE_STRUCT          *nx_packet_interface_ptr;
        struct NXD_IPV6_ADDRESS_STRUCT      *nx_packet_ipv6_address_ptr;
    } nx_packet_address;

#define nx_packet_ip_interface nx_packet_address.nx_packet_interface_ptr

    UCHAR                                   *nx_packet_ip_header;

#ifdef NX_ENABLE_INTERFACE_CAPABILITY
    ULONG                                   nx_packet_interface_capability_flag;
#endif /* NX_ENABLE_INTERFACE_CAPABILITY */
#ifdef NX_IPSEC_ENABLE
    VOID                                    *nx_packet_ipsec_sa_ptr;
    USHORT                                  nx_packet_ipsec_op;
    USHORT                                  nx_packet_ipsec_state;
#endif /* NX_IPSEC_ENABLE */
#ifdef NX_ENABLE_PACKET_DEBUG_INFO
    CHAR                                    *nx_packet_debug_thread;
    CHAR                                    *nx_packet_debug_file;
    ULONG                                   nx_packet_debug_line;
#endif /* NX_ENABLE_PACKET_DEBUG_INFO */

#ifdef NX_PACKET_HEADER_PAD
    ULONG                                   nx_packet_packet_pad[NX_PACKET_HEADER_PAD_SIZE];
#endif
    struct NX_PACKET_POOL_STRUCT            *nx_packet_pool_owner;
    struct NX_PACKET_STRUCT                 *nx_packet_queue_next;
    struct NX_PACKET_STRUCT                 *nx_packet_tcp_queue_next;
    struct NX_PACKET_STRUCT                 *nx_packet_next;
    struct NX_PACKET_STRUCT                 *nx_packet_last;
    struct NX_PACKET_STRUCT                 *nx_packet_fragment_next;
    ULONG                                   nx_packet_length;
    struct NX_INTERFACE_STRUCT              *nx_packet_ip_interface;
    ULONG                                   nx_packet_next_hop_address;
    UCHAR                                   *nx_packet_data_start;
    UCHAR                                   *nx_packet_data_end;
    UCHAR                                   *nx_packet_prepend_ptr;
    UCHAR                                   *nx_packet_append_ptr;
#ifdef NX_PACKET_HEADER_PAD
```

```
    ULONG                                 nx_packet_packet_pad;
#endif
    ULONG                                 nx_packet_reassembly_time;
    UCHAR                                 nx_packet_option_state;
    UCHAR                                 nx_packet_destination_header;
    USHORT                                nx_packet_option_offset;
    ULONG                                 nx_packet_ip_version;
#ifdef FEATURE_NX_IPV6
    ULONG                                 nx_packet_ipv6_dest_addr[4];
    ULONG                                 nx_packet_ipv6_src_addr[4];
    struct                                NXD_IPV6_ADDRESS_STRUCT *nx_packet_interface;
#endif /* FEATURE_NX_IPV6 */
    UCHAR                                 *nx_packet_ip_header;
} NX_PACKET;

typedef struct NX_PACKET_POOL_STRUCT
{
    ULONG                                 nx_packet_pool_id;
    CHAR                                  *nx_packet_pool_name;
    ULONG                                 nx_packet_pool_available;
    ULONG                                 nx_packet_pool_total;
    ULONG                                 nx_packet_pool_empty_requests;
    ULONG                                 nx_packet_pool_empty_suspensions;
    ULONG                                 nx_packet_pool_invalid_releases;
    struct NX_PACKET_STRUCT               *nx_packet_pool_available_list;
    CHAR                                  *nx_packet_pool_start;
    ULONG                                 nx_packet_pool_size;
    ULONG                                 nx_packet_pool_payload_size;
    TX_THREAD                             *nx_packet_pool_suspension_list;
    ULONG                                 nx_packet_pool_suspended_count;
    struct NX_PACKET_POOL_STRUCT          *nx_packet_pool_created_next,
                                          *nx_packet_pool_created_previous;

#ifdef NX_ENABLE_LOW_WATERMARK
    UINT                                  nx_packet_pool_low_watermark;
#endif /* NX_ENABLE_LOW_WATERMARK */
} NX_PACKET_POOL;

typedef struct NX_TCP_LISTEN_STRUCT
{
    UINT                                  nx_tcp_listen_port;
    VOID                                  (*nx_tcp_listen_callback)(NX_TCP_SOCKET *socket_ptr,
                                                                    UINT port);
    NX_TCP_SOCKET                         *nx_tcp_listen_socket_ptr;
    ULONG                                 nx_tcp_listen_queue_maximum;
    ULONG                                 nx_tcp_listen_queue_current;
    NX_PACKET                             *nx_tcp_listen_queue_head,
                                          *nx_tcp_listen_queue_tail;
    struct NX_TCP_LISTEN_STRUCT           *nx_tcp_listen_next,
                                          *nx_tcp_listen_previous;

} NX_TCP_LISTEN;

typedef struct NX_TCP_SOCKET_STRUCT
{
    ULONG                                 nx_tcp_socket_id;
    CHAR                                  *nx_tcp_socket_name;
    UINT                                  nx_tcp_socket_client_type;
    UINT                                  nx_tcp_socket_port;
    ULONG                                 nx_tcp_socket_mss;
    NXD_ADDRESS                           nx_tcp_socket_connect_ip;
    UINT                                  nx_tcp_socket_connect_port;
    ULONG                                 nx_tcp_socket_connect_mss;
    struct NX_INTERFACE_STRUCT            *nx_tcp_socket_connect_interface;
    ULONG                                 nx_tcp_socket_next_hop_address;
    ULONG                                 nx_tcp_socket_connect_mss2;
    ULONG                                 nx_tcp_socket_tx_slow_start_threshold;
    UINT                                  nx_tcp_socket_state;
    ULONG                                 nx_tcp_socket_tx_sequence;
    ULONG                                 nx_tcp_socket_rx_sequence;
    ULONG                                 nx_tcp_socket_rx_sequence_acked;
    ULONG                                 nx_tcp_socket_delayed_ack_timeout;
```

```
    ULONG                                   nx_tcp_socket_fin_sequence;
    USHORT                                  nx_tcp_socket_fin_received;
    USHORT                                  nx_tcp_socket_fin_acked;
    ULONG                                   nx_tcp_socket_tx_window_advertised;
    ULONG                                   nx_tcp_socket_tx_window_congestion;
    ULONG                                   nx_tcp_socket_tx_outstanding_bytes;
    ULONG                                   nx_tcp_socket_tx_sequence_recover;
    ULONG                                   nx_tcp_socket_previous_highest_ack;
    ULONG                                   nx_tcp_socket_ack_n_packet_counter;
    UINT                                    nx_tcp_socket_duplicated_ack_received;
    ULONG                                   nx_tcp_socket_rx_window_default;
    ULONG                                   nx_tcp_socket_rx_window_current;
    ULONG                                   nx_tcp_socket_rx_window_last_sent;
    ULONG                                   nx_tcp_socket_packets_sent;
    ULONG                                   nx_tcp_socket_bytes_sent;
    ULONG                                   nx_tcp_socket_packets_received;
    ULONG                                   nx_tcp_socket_bytes_received;
    ULONG                                   nx_tcp_socket_retransmit_packets;
    ULONG                                   nx_tcp_socket_checksum_errors;
    ULONG                                   nx_tcp_socket_zero_window_probe_failure;
    ULONG                                   nx_tcp_socket_zero_window_probe_sequence;
    UCHAR                                   nx_tcp_socket_zero_window_probe_has_data;
    UCHAR                                   nx_tcp_socket_zero_window_probe_data;
    UCHAR                                   nx_tcp_socket_fast_recovery;
    UCHAR                                   nx_tcp_socket_reserved;
    struct NX_IP_STRUCT                     *nx_tcp_socket_ip_ptr;
    ULONG                                   nx_tcp_socket_type_of_service;
    UINT                                    nx_tcp_socket_time_to_live;
    ULONG                                   nx_tcp_socket_fragment_enable;
    ULONG                                   nx_tcp_socket_receive_queue_count;
    NX_PACKET                               *nx_tcp_socket_receive_queue_head,
                                            *nx_tcp_socket_receive_queue_tail;
    ULONG                                   nx_tcp_socket_transmit_queue_maximum;
    ULONG                                   nx_tcp_socket_transmit_sent_count;
    NX_PACKET                               *nx_tcp_socket_transmit_sent_head,
                                            nx_tcp_socket_transmit_sent_tail;
#ifdef NX_ENABLE_LOW_WATERMARK
    ULONG                                   nx_tcp_socket_receive_queue_maximum;
#endif /* NX_ENABLE_LOW_WATERMARK */
    ULONG                                   nx_tcp_socket_timeout;
    ULONG                                   nx_tcp_socket_timeout_rate;
    ULONG                                   nx_tcp_socket_timeout_retries;
    ULONG                                   nx_tcp_socket_timeout_max_retries;
    ULONG                                   nx_tcp_socket_timeout_shift;
#ifdef NX_ENABLE_TCP_WINDOW_SCALING
    ULONG                                   nx_tcp_socket_rx_window_maximum;
    ULONG                                   nx_tcp_rcv_win_scale_value;
    ULONG                                   nx_tcp_snd_win_scale_value;
#endif /* NX_ENABLE_TCP_WINDOW_SCALING */
    ULONG                                   nx_tcp_socket_keepalive_timeout;
    ULONG                                   nx_tcp_socket_keepalive_retries;
    struct NX_TCP_SOCKET_STRUCT             *nx_tcp_socket_bound_next,
                                            *nx_tcp_socket_bound_previous;
    TX_THREAD                               *nx_tcp_socket_bind_in_progress;
    TX_THREAD                               *nx_tcp_socket_receive_suspension_list;
    ULONG                                   nx_tcp_socket_receive_suspended_count;
    TX_THREAD                               *nx_tcp_socket_transmit_suspension_list;
    ULONG                                   nx_tcp_socket_transmit_suspended_count;
    TX_THREAD                               *nx_tcp_socket_connect_suspended_thread;
    TX_THREAD                               *nx_tcp_socket_disconnect_suspended_thread;
    TX_THREAD                               *nx_tcp_socket_bind_suspension_list;
    ULONG                                   nx_tcp_socket_bind_suspended_count;
    struct NX_TCP_SOCKET_STRUCT             *nx_tcp_socket_created_next,
                                            *nx_tcp_socket_created_previous;
    VOID                                    (*nx_tcp_urgent_data_callback)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);

#ifndef NX_DISABLE_EXTENDED_NOTIFY_SUPPORT
     UINT                                   (*nx_tcp_socket_syn_received_notify)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr,
                                                           NX_PACKET *packet_ptr);
```

```
    VOID                                    (*nx_tcp_establish_notify)(struct NX_TCP_SOCKET_STRUCT
                                                           *socket_ptr);
    VOID                                    (*nx_tcp_disconnect_complete_notify)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);
    VOID                                    (*nx_tcp_timed_wait_callback)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);
#endif
    VOID                                    (*nx_tcp_disconnect_callback)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);
    VOID                                    (*nx_tcp_receive_callback)(struct NX_TCP_SOCKET_STRUCT
                                                           *socket_ptr);
    VOID                                    (*nx_tcp_socket_window_update_notify)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);
#ifdef   NX_ENABLE_TCP_QUEUE_DEPTH_UPDATE_NOTIFY
    VOID                                    (*nx_tcp_socket_queue_depth_notify)(struct
                                                           NX_TCP_SOCKET_STRUCT *socket_ptr);
#endif
    void                                    *nx_tcp_socket_reserved_ptr;
    ULONG                                   nx_tcp_socket_transmit_queue_maximum_default;
    UINT                                    nx_tcp_socket_keepalive_enabled;
#ifdef FEATURE_NX_IPV6
    struct NXD_IPV6_ADDRESS_STRUCT          *nx_tcp_socket_ipv6_addr;
#endif /* FEATURE_NX_IPV6 */
#ifdef NX_IPSEC_ENABLE
    VOID                                    *nx_tcp_socket_egress_sa;
    UINT                                    nx_tcp_socket_egress_sa_data_offset;
#endif /* NX_IPSEC_ENABLE */
} NX_TCP_SOCKET;

typedef struct NX_UDP_SOCKET_STRUCT
{
    ULONG                                   nx_udp_socket_id;
    CHAR                                    *nx_udp_socket_name;
    UINT                                    nx_udp_socket_port;
    struct NX_IP_STRUCT                     *nx_udp_socket_ip_ptr;
    ULONG                                   nx_udp_socket_packets_sent;
    ULONG                                   nx_udp_socket_bytes_sent;
    ULONG                                   nx_udp_socket_packets_received;
    ULONG                                   nx_udp_socket_bytes_received;
    ULONG                                   nx_udp_socket_invalid_packets;
    ULONG                                   nx_udp_socket_packets_dropped;
    ULONG                                   nx_udp_socket_checksum_errors;
    ULONG                                   nx_udp_socket_type_of_service;
    UINT                                    nx_udp_socket_time_to_live;
    ULONG                                   nx_udp_socket_fragment_enable;
    UINT                                    nx_udp_socket_disable_checksum;
    ULONG                                   nx_udp_socket_receive_count;
    ULONG                                   nx_udp_socket_queue_maximum;
    NX_PACKET                               *nx_udp_socket_receive_head,
                                            *nx_udp_socket_receive_tail;
    struct NX_UDP_SOCKET_STRUCT             *nx_udp_socket_bound_next,
                                            *nx_udp_socket_bound_previous;
    TX_THREAD                               *nx_udp_socket_bind_in_progress;
    TX_THREAD                               *nx_udp_socket_receive_suspension_list;
    ULONG                                   nx_udp_socket_receive_suspended_count;
    TX_THREAD                               *nx_udp_socket_bind_suspension_list;
    ULONG                                   nx_udp_socket_bind_suspended_count;
    struct NX_UDP_SOCKET_STRUCT             *nx_udp_socket_created_next,
                                            *nx_udp_socket_created_previous;
    VOID                                    (*nx_udp_receive_callback)(struct NX_UDP_SOCKET_STRUCT
                                                                       *socket_ptr);
    void                                    *nx_udp_socket_reserved_ptr;

} NX_UDP_SOCKET;
typedef struct NXD_IPV6_ADDRESS_STRUCT
{
    UCHAR                                   nxd_ipv6_address_valid;
    UCHAR                                   nxd_ipv6_address_type;
    UCHAR                                   nxd_ipv6_address_state;
    UCHAR                                   nxd_ipv6_address_prefix_length;
```

```
    struct NX_INTERFACE_STRUCT              *nxd_ipv6_address_attached;
    ULONG                                   nxd_ipv6_address[4];
    struct                                  NXD_IPV6_ADDRESS_STRUCT *nxd_ipv6_address_next;
    CHAR                                    nxd_ipv6_address_DupAddrDetectTransmit;
    CHAR                                    nxd_ipv6_address_ConfigurationMethod;
    UCHAR                                   nxd_ipv6_address_index;
    UCHAR                                   reserved;
} NXD_IPV6_ADDRESS;

typedef struct NXD_ADDRESS_STRUCT
{
    ULONG                                   nxd_ip_version;
    union
    {
        ULONG                               v4;
#ifdef FEATURE_NX_IPV6
        ULONG                               v6[4];
#endif
    } nxd_ip_address;
} NXD_ADDRESS;
```

Appendix D: BSD-Compatible Socket API

BSD-Compatible Socket API

The BSD-Compatible Socket API supports a subset of the BSD Sockets API calls (with some limitations) by utilizing NetX Duo® primitives underneath. Both IPv6 and IPv4 protocols and network addressing are supported. This BSD-Compatible Sockets API layer should perform as fast or slightly faster than typical BSD implementations because this API utilizes internal NetX Duo primitives and bypasses unnecessary NetX error checking.

Configurable options allow the host application to define the maximum number of sockets, TCP maximum window size, and depth of listen queue.

Due to performance and architecture constraints, this BSD-Compatible Sockets API does not support all BSD Sockets calls. In addition, not all BSD options are available for the BSD services, specifically the following:

- ***select***() call works with only fd_set *readfds, other arguments in this call e.g., writefds, exceptfds are not supported.
- The “int flags” argument is not supported for ***send()***, ***recv()***, ***sendto(),*** and ***recvfrom ()*** calls.
- The BSD-Compatible Socket API supports only limited set of BSD Sockets calls.

The source code is designed for simplicity and is comprised of only two files, ***nxd_bsd.c*** and ***nxd_bsd.h***. Installation requires adding these two files to the build project (not the NetX library) and creating the host application which will use BSD Socket service calls. The ***nxd_bsd.h*** file must also be included in your application source. Sample demo files for both IPv4 and IPv6 based applications are included with the distribution which is freely available with NetX Duo. Further details are available in the help and Readme files bundled with the BSD-Compatible Socket API package.

The BSD-Compatible Sockets API supports the following BSD Sockets API calls:

INT	*bsd_initialize (NX_IP *default_ip, NX_PACKET_POOL *default_pool, CHAR *bsd_memory_not_used);*
INT	*getpeername(INT sockID, struct sockaddr *remoteAddress, INT *addressLength);*
INT	*getsockname(INT sockID, struct sockaddr *localAddress, INT *addressLength);*
INT	*recvfrom(INT sockID, CHAR *buffer, INT buffersize, INT flags,struct sockaddr *fromAddr, INT *fromAddrLen);*
INT	*recv(INT sockID, VOID *rcvBuffer, INT bufferLength, INT flags);*
INT	*sendto(INT sockID, CHAR *msg, INT msgLength, INT flags, struct sockaddr *destAddr, INT destAddrLen);*
INT	*send(INT sockID, const CHAR *msg, INT msgLength, INT flags);*
INT	*accept(INT sockID, struct sockaddr *ClientAddress, INT *addressLength);*
INT	*listen(INT sockID, INT backlog);*
INT	*bind (INT sockID, struct sockaddr *localAddress, INT addressLength);*
INT	*connect(INT sockID, struct sockaddr *remoteAddress, INT addressLength);*
INT	*socket(INT protocolFamily, INT type, INT protocol);*
INT	*soc_close (INT sockID);*
INT	*select(INT nfds, fd_set *readfds, fd_set *writefds, fd_set *exceptfds, struct timeval *timeout);*
VOID	*FD_SET(INT fd, fd_set *fdset);*
VOID	*FD_CLR(INT fd, fd_set *fdset);*
INT	*FD_ISSET(INT fd, fd_set *fdset);*
VOID	*FD_ZERO(fd_set *fdset);*

Appendix E: ASCII Character Codes in HEX

ASCII Character Codes in HEX

most significant nibble

least significant nibble

<table>
<tr><th></th><th>0_</th><th>1_</th><th>2_</th><th>3_</th><th>4_</th><th>5_</th><th>6_</th><th>7_</th></tr>
<tr><td>_0</td><td>NUL</td><td>DLE</td><td>SP</td><td>0</td><td>@</td><td>P</td><td>'</td><td>p</td></tr>
<tr><td>_1</td><td>SOH</td><td>DC1</td><td>!</td><td>1</td><td>A</td><td>Q</td><td>a</td><td>q</td></tr>
<tr><td>_2</td><td>STX</td><td>DC2</td><td>"</td><td>2</td><td>B</td><td>R</td><td>b</td><td>r</td></tr>
<tr><td>_3</td><td>ETX</td><td>DC3</td><td>#</td><td>3</td><td>C</td><td>S</td><td>c</td><td>s</td></tr>
<tr><td>_4</td><td>EOT</td><td>DC4</td><td>$</td><td>4</td><td>D</td><td>T</td><td>d</td><td>t</td></tr>
<tr><td>_5</td><td>ENQ</td><td>NAK</td><td>%</td><td>5</td><td>E</td><td>U</td><td>e</td><td>u</td></tr>
<tr><td>_6</td><td>ACK</td><td>SYN</td><td>&</td><td>6</td><td>F</td><td>V</td><td>f</td><td>v</td></tr>
<tr><td>_7</td><td>BEL</td><td>ETB</td><td>'</td><td>7</td><td>G</td><td>W</td><td>g</td><td>w</td></tr>
<tr><td>_8</td><td>BS</td><td>CAN</td><td>(</td><td>8</td><td>H</td><td>X</td><td>h</td><td>x</td></tr>
<tr><td>_9</td><td>HT</td><td>EM</td><td>)</td><td>9</td><td>I</td><td>Y</td><td>i</td><td>y</td></tr>
<tr><td>_A</td><td>LF</td><td>SUB</td><td>*</td><td>:</td><td>J</td><td>Z</td><td>j</td><td>z</td></tr>
<tr><td>_B</td><td>VT</td><td>ESC</td><td>+</td><td>;</td><td>K</td><td>[</td><td>K</td><td>}</td></tr>
<tr><td>_C</td><td>FF</td><td>FS</td><td>,</td><td><</td><td>L</td><td>\</td><td>l</td><td>|</td></tr>
<tr><td>_D</td><td>CR</td><td>GS</td><td>-</td><td>=</td><td>M</td><td>]</td><td>m</td><td>}</td></tr>
<tr><td>_E</td><td>SO</td><td>RS</td><td>.</td><td>></td><td>N</td><td>^</td><td>n</td><td>~</td></tr>
<tr><td>_F</td><td>SI</td><td>US</td><td>/</td><td>?</td><td>O</td><td>_</td><td>o</td><td>DEL</td></tr>
</table>

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

N

Q

R

S

T

U

V

W

Z