Netfinity Director
Technical Tips and Information

Craig Elliott

Draft Version 0.2

July 23, 2000

Table of Contents

Chapter 1 – Uninstalling Netfinity Director v2.11

Overview

According to the README1.TXT file, Netfinity Director v2.11 Management Server must be uninstalled before installing Netfinity Director v2.12 Management Server. This is due to product changes including database engine modifications. Unfortunately, the uninstall process for v2.11 doesn't completely uninstall all components. Chapter 1 will document the procedure for identifying the files and registry changes remaining after an uninstall of v2.11 that should be manually deleted prior to installation of v2.12.

Methodology

This information was gathered using `SYSDIFF.EXE` included in the Windows NT Resource Kit. Basically, a snapshot was taken of the system prior to installing Netfinity Director and the UM Server Extensions, and another snap-shot was taken after UM Server Extensions and Netfinity Director were uninstalled. Then the two snap-shots were compared to identify the files / registry entries that were created but not deleted by the Netfinity Director uninstall program.

Recreation Steps

The specifics steps followed to determine the remaining files and registry entries are listed below:

1. Build the test system
   Install Windows NT 4.0 on a Netfinity 5500, configured as a Stand Alone server
   Install SP6a 128-bit
   Install IE 5.0 from the Resource Kit Supplement 4
   Install Resource Kit Supplement 4
2. Take a snapshot of the system
   Execute the command `C:\NTRESKIT\SYSDIFF /SNAP SYSDIFF.SNAP`
3. Install Netfinity Director
   Install the Management Server using the default components.
   Enable Director Remote Control
   Do not enable the TMR Gateway
   Use the default Jet database
   Reboot the system
4. Install the UM Server Extensions
   Stop the Management Server using the command `NET STOP TWGIPC`
   Install the Server Extensions
   Reboot the system
5. Uninstall the UM Server Extensions
   Stop the Management Server using the command `NET STOP TWGIPC`
   Uninstall the UM Server Extensions using the utility provided on the Start menu.
   Reboot the system
6. Uninstall Netfinity Director
   Stop the Management Server using the command `NET STOP TWGIPC`
   Uninstall the Management Server using Control Panel ✍ Add/Remove Programs
   Reboot the system
7. Take a second snapshot of the system
   Execute the command `C:\NTRESKIT\SYSDIFF /DIFF SYSDIFF.SNAP SYSDIFF.DIFF`
8. Dump the results to a text file
   Execute the command `C:\NTRESKIT\SYSDIFF /DUMP SYSDIFF.DIFF SYSDIFF.DUMP`

Testing Results

The results of the testing showed Netfinity Director left a substantial number of files and registry entries remaining following the uninstall. In fact, there were approximately 12,000 lines of changes in the resulting `SYSDIFF.DUMP` file created using `SYSDIFF.EXE`. While it isn't practical to list the entire results within this document, select entries can be found in Figure 3 – `SYSDIFF.EXE` Results on page 6. Please note that some of the remaining files and registry entries pertain to ODBC, WMI, Java Classes, etc. – items that may also be installed by other applications. Because of this, specific testing must be performed for each environment to ensure any manual deletion doesn't affect other applications.

Chapter 2 – Agent Discovery in a Multi-Management Server Environment

Overview

Netfinity Director has a limit of 1,500 managed devices (Agents) per Management Server. Because of this limitation, most enterprise customers must implement multiple Management Servers in order to manage all of their Netfinity servers. Chapter 2 will explain Netfinity Director discovery and how it can be configured to limit which Agents are discovered by each Management Server.

Discovery Process

Netfinity Director has the ability for the Management Server to discover systems running the Netfinity Director Agent. The Agents are listening on UDP port 14247 for communication requests. Discovery sends broadcast and/or multicast packets using UDP port 14247 to automatically discover the Agent systems.

In order for the remote Agents (those on a different IP subnet than the management server) to be discovered, the routers must be configured to allow the broadcast and/or multicast packets to pass. Typically, routers are configured to block the broadcast and/or multicast packets to minimize network traffic. The network administrator must verify the routers are properly configured for discovery to be successful.

Configuring Discovery

To configure Discovery, select the **Discovery Preferences...** item from the **Options** menu as shown in Figure 1 – Opening Discovery Preferences on page 5. This will open the **Discovery Preferences** window.

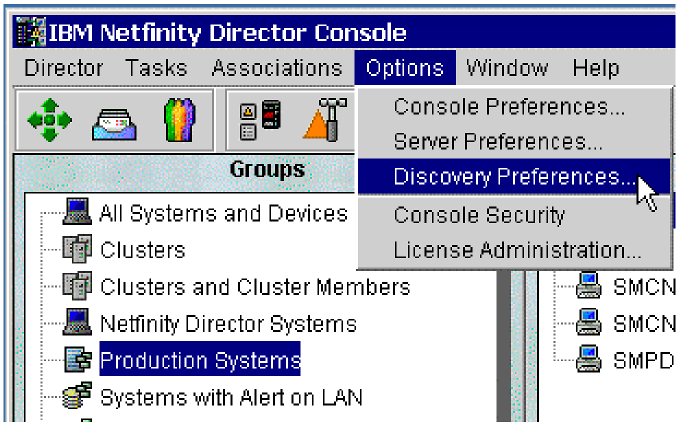
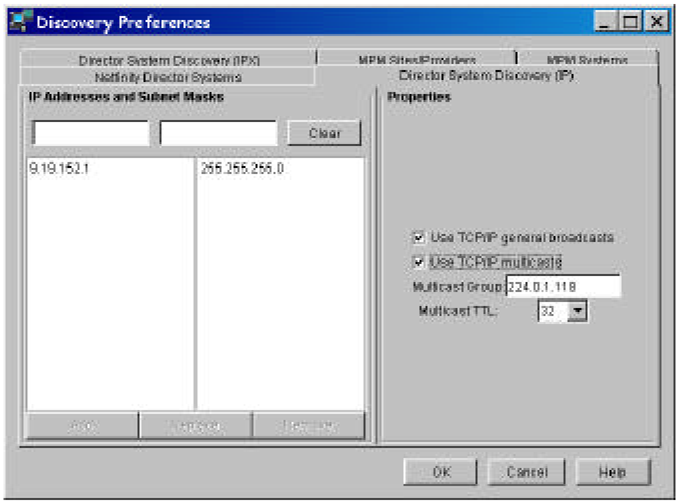


Figure 1 – Opening Discovery Preferences

In the **Discovery Preferences** window, the different types of discovery can be configured. These are shown in Figure 2 – Discovery Preferences on page 6.

The **IP Addresses and Subnet Masks** pane on the left side of the window allows multiple subnets to be discovered. In the **Properties** pane on the right side of the window are the options **Use TCP/IP general broadcasts** and **Use TCP/IP multicasts**. All three will be discussed below.


Discovery Preferences
Director System Discovery (IPX)
MPM Sites/Providers
MPM Systems
Netfinity Director Systems
Director System Discovery (IP)
Clear
OK
Cancel
Help

IP Addresses and Subnet Masks

9.19.152.1	255.255.255.0

Properties

☑ Use TCP/IP general broadcasts

☑ Use TCP/IP multicasts

Multicast Group: 224.0.1.118

Multicast TTL: 32

Figure 2 – Discovery Preferences

General Broadcasts

The **Use TCP/IP general broadcasts** option will allow the Management Server to discover all Netfinity Director Agents running on the local subnet only. This sends one 58-byte all routes broadcast packet, using UDP port 14247, to address 255.255.255.255 (see Figure 4 – General Broadcast on page 11 for a sample network trace).

Multicast

The **Use TCP/IP multicasts** option will allow the Management Server to discover Netfinity Director Agents on the local subnet as well as on remote subnets, assuming the routers will forward the multicast packet. This sends one 58-byte all routes broadcast packet, using UDP port 14247, to the default multicast group address 224.0.1.118 (see Figure 6 – TCP/IP Multicast on page 12 for a sample network trace).

Remote Subnet Broadcast

To discover system in remote subnets using broadcasts, a valid IP address and corresponding subnet mask must be specified for each subnet to be discovered. Using these two values, the Management Server will calculate the correct broadcast address for each subnet, and generate one 58-byte all routes broadcast packet, using UDP port 14247, to these addresses (see Figure 8 – Subnet Broadcast on page 13 for a sample network trace).

Limiting Discovery

In environments with more than 1,500 systems, multiple Management Servers must be deployed. However, these must be configured to prevent each Management Server from discovering the same Netfinity Director Agents. This can be accomplished in one of two ways – specifying the subnet broadcasts or specifying the multicast address. Each will be discussed in the following sections.

Subnet Broadcasts

The easiest method of restricting the Netfinity Director Agents discovered is by configuring the **IP Addresses and Subnet Masks** on each Management Server. For example, if a customer had systems deployed in two subnets – 9.19.128.0 and 9.19.152.0 – one Management Server could be configured with 9.19.141.1 255.255.240.0 and the other Management Server could be configured with 9.19.152.1 255.255.255.0. Therefore, one Management Server would manage the systems in one subnet, and the other Management Server would manage the systems in the other subnet.

Multicast Addresses

While limiting the Netfinity Director Agents discovered by Subnet Mask is an option, it may not always be feasible. For instance, in the previous example, the first subnet has far more systems than the 1,500 limit. The systems wouldn't be evenly distributed amongst Management Servers. Another example where subnet discovery isn't an option is if the customer wants the servers managed by one Management Server and the workstations managed by another Management Server. If the servers and workstations reside on the same subnet, limiting discovery by subnet will not achieve the desired results.

To overcome this limitation, Netfinity Director has the ability to discover Agents based on a Multicast Group Address. By default, it uses 224.0.1.118. However, this address can be changed. One each Management Server, specify a unique **Multicast Group Address** (see Figure 2 – Discovery Preferences on page 6). On the Agent systems, create a file `\IBM\UMS\DIRECTOR\BIN\TCPIP.INI` that contains the statement `MULTICASTADDR=`*`multicastgroupaddress`* where *`multicastgroupaddr`* is the Multicast Group Address specified in the Management Server that should discover the Agent. Now, each Management Server will only discover the Netfinity Director Agents it should manage.

Chapter 3 – Deploying Netfinity Director v2.12 in an NT Master Domain

Overview

Many customers have followed the advice of Microsoft and deployed Windows NT using a Master Domain model. While Netfinity Director recognizes and supports the authentication provided by this model, there are certain considerations when deploying the Management Server in this environment. Chapter 3 will discuss the configuration required to accomplish this.

Master Domain Explained

The Master Domain architecture uses a single Accounts domain and multiple Resource domains. The Accounts domain contains user accounts for all users within the corporation. Resource domains are comprised of the actual systems or “resources” within the corporation. This includes workstations, file servers, application servers, infrastructure servers, etc. Multiple Resource domains are typically deployed. This can be based on the number of departments, sites, or even workstations. A one-way trust is established between each of the Resource domains and the Account domain to allow users defined in the Accounts domain to access the resources defined in the Resource domain.

Application to Netfinity Director

Through definition, the system acting as the Management Server will be a member of a Resource domain. However, the account used to start the Netfinity Director service must belong to the Accounts domain. Therefore, there are a few account considerations when deploying Netfinity Director in a Master Domain environment. This includes the following:

1. The service account used by the Director support program service on the Management Server must:
   ?? have access to the Accounts Database of the Accounts domain to allow console security to authorize existing Windows NT user accounts as valid Netfinity Director users,
   ?? be able to create the special TWGAdmins and TWGSuperAdmins domain groups that are used by Netfinity Director,
   ?? be able to assign users to Windows NT groups
   Therefore, the service account should be a member of the Domain Admins group in the Accounts domain.
2. Additionally, the service account must:
   ?? be used as the log-on account during Netfinity Director installation to ensure the Director support program service is created correctly and
   ?? be a member of the local system’s Administrators group to allow registry changes to be made at install time.
3. The user accounts of the authorized Management Console users must have authority to read / write Netfinity Director configuration files on the Management Server. Therefore, the TWGAdmins and TWGSuperAdmins domain groups should be members of the local Users group on the Management Server.

When Netfinity Director is installed in the manner listed above, all members of the Domain Admin group are enabled within console security automatically. This is true even though those ID’s aren’t added to the TWGAdmins or TWGSuperAdmins groups. Domain Administrators cannot be unauthorized using console security. To restrict their access to Netfinity Director, their individual profiles must be edited.

The default profile allows all privileges with the exception of console security. Therefore, all Domain Admin’s, even though they are authorized users, will not have console security access.

Initially, the only account with console security access is the one used during Netfinity Director installation. To enable other Management Console users to perform console security functions, log on using the ID used during installation and grant the console security privilege to additional users.

Appendix A – Figures & Tables

Remaining Directories

```
d:\IBM\Director and it's subdirectories
d:\WINNT\Profiles\All Users\Start Menu\Programs\IBM UM Server Extensions
C:\WINNT\system32\drivers\i2cnt.sys
C:\WINNT\system32\drivers\smbios.sys
```

Remaining Registry entries

```
HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
  TWGMachineID: binary data of type 3
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\Cornhusker Client
  EventMessageFile: REG_SZ/REG_EXPAND_SZ %SystemRoot%\System32\NTEventViewerFormater.exe
HKLM\SOFTWARE\IBM\IBM Netfinity Director Extension Installer
HKLM\SOFTWARE\IBM\ICSM  and its sub-keys and values
```

Figure 3 – SYSDIFF.EXE Results

```
Frame: Base frame properties
    Frame: Time of capture = 6/20/2000 12:18:2.187
    Frame: Time delta from previous physical frame: 0 microseconds
    Frame: Frame number: 5
    Frame: Total frame length: 58 bytes
    Frame: Capture frame length: 58 bytes
    Frame: Frame data: Number of data bytes remaining = 58 (0x003A)
TOKENRING: Length =  58, Priority Normal (No token) LLC Frame, Routed.
    TOKENRING: Access control = 16 (0x10) Original, Frame, Priority: Normal (No token)
        TOKENRING: .....000   Reservation bits: Reservation = Normal, No token needed.
        TOKENRING: ....0...   Monitor bit = Original (non-repeated)
        TOKENRING: ...1....   Token bit = Frame
        TOKENRING: 000.....   Priority bits: Priority = Normal, No token needed.
    TOKENRING: Frame control = 64 (0x40), LLC Frame
        TOKENRING: ....0000   Control bits = Normal Buffered
        TOKENRING: 01......   Frame type = LLC Frame
    TOKENRING: Destination address : FFFFFFFFFFFF
        TOKENRING: Destination Address I/G Bit        = Group address
        TOKENRING: Destination Address U/L bit        = Locally administered address
        TOKENRING: Destination Address Functional bit = Group address
    TOKENRING: Source address      : 80062917CF56
        TOKENRING: Source Address Routing bit = Routing information present
        TOKENRING: Source Address U/L bit     = Universally administered address
    TOKENRING: Frame length : 58 (0x003A)
    TOKENRING: Routing control 1 = 0x82, length 2, All Routes Broadcast
        TOKENRING: ...00010   Routing length = 2 bytes.
        TOKENRING: 100.....   Broadcast indicator = All Routes Broadcast B'100'
    TOKENRING: Routing control 2 = 0x70, Forward, All-routes broadcast.
        TOKENRING: Direction indicator = Forward (left-to-right) direction.
        TOKENRING: Largest frame = All-routes broadcast.
    TOKENRING: Tokenring data: Number of data bytes remaining = 42 (0x002A)
LLC: UI DSAP=0xAA SSAP=0xAA C
    LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
    LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
    LLC: Frame Category: Unnumbered Frame
    LLC: Command = UI
    LLC: LLC Data: Number of data bytes remaining = 39 (0x0027)
SNAP: ETYPE = 0x0800
    SNAP: Snap Organization code = 00 00 00
    SNAP: Snap etype : 0x0800
    SNAP: Snap Data: Number of data bytes remaining = 34 (0x0022)
IP: ID = 0x8268; Proto = UDP; Len: 34
    IP: Version = 4 (0x4)
    IP: Header Length = 20 (0x14)
    IP: Precedence = Routine
    IP: Type of Service = Normal Service
    IP: Total Length = 34 (0x22)
    IP: Identification = 33384 (0x8268)
    IP: Flags Summary = 0 (0x0)
        IP: .......0 = Last fragment in datagram
        IP: ......0. = May fragment datagram if necessary
    IP: Fragment Offset = 0 (0x0) bytes
    IP: Time to Live = 128 (0x80)
    IP: Protocol = UDP - User Datagram
    IP: Checksum = 0x2160
    IP: Source Address = 9.19.141.240
    IP: Destination Address = 255.255.255.255
    IP: Data: Number of data bytes remaining = 14 (0x000E)
UDP: IP Multicast: Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 14
(0xE)
    UDP: Source Port = 0x37A7
    UDP: Destination Port = 0x37A7
    UDP: Total length = 14 (0xE) bytes
    UDP: UDP Checksum = 0x60A7
    UDP: Data: Number of data bytes remaining = 6 (0x0006)
```

Figure 4 – General Broadcast

```
Frame: Base frame properties
    Frame: Time of capture = 6/20/2000 12:8:45.327
    Frame: Time delta from previous physical frame: 0 microseconds
    Frame: Frame number: 6
    Frame: Total frame length: 58 bytes
    Frame: Capture frame length: 58 bytes
    Frame: Frame data: Number of data bytes remaining = 58 (0x003A)
TOKENRING: Length =  58, Priority Normal (No token) LLC Frame, Routed.
    TOKENRING: Access control = 16 (0x10) Original, Frame, Priority: Normal (No token)
        TOKENRING: .....000   Reservation bits: Reservation = Normal, No token needed.
        TOKENRING: ....0...   Monitor bit = Original (non-repeated)
        TOKENRING: ...1....   Token bit = Frame
        TOKENRING: 000.....   Priority bits: Priority = Normal, No token needed.
    TOKENRING: Frame control = 64 (0x40), LLC Frame
        TOKENRING: ....0000   Control bits = Normal Buffered
        TOKENRING: 01......   Frame type = LLC Frame
    TOKENRING: Destination address : C00000040000
        TOKENRING: Destination Address I/G Bit        = Group address
        TOKENRING: Destination Address U/L bit        = Locally administered address
        TOKENRING: Destination Address Functional bit = Functional address
    TOKENRING: Source address      : 80062917CF56
        TOKENRING: Source Address Routing bit = Routing information present
        TOKENRING: Source Address U/L bit     = Universally administered address
    TOKENRING: Frame length : 58 (0x003A)
    TOKENRING: Routing control 1 = 0x82, length 2, All Routes Broadcast
        TOKENRING: ...00010   Routing length = 2 bytes.
        TOKENRING: 100.....   Broadcast indicator = All Routes Broadcast B'100'
    TOKENRING: Routing control 2 = 0x70, Forward, All-routes broadcast.
        TOKENRING: Direction indicator = Forward (left-to-right) direction.
        TOKENRING: Largest frame = All-routes broadcast.
    TOKENRING: Tokenring data: Number of data bytes remaining = 42 (0x002A)
LLC: UI DSAP=0xAA SSAP=0xAA C
    LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
    LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
    LLC: Frame Category: Unnumbered Frame
    LLC: Command = UI
    LLC: LLC Data: Number of data bytes remaining = 39 (0x0027)
SNAP: ETYPE = 0x0800
    SNAP: Snap Organization code = 00 00 00
    SNAP: Snap etype : 0x0800
    SNAP: Snap Data: Number of data bytes remaining = 34 (0x0022)
IP: ID = 0x802A; Proto = UDP; Len: 34
    IP: Version = 4 (0x4)
    IP: Header Length = 20 (0x14)
    IP: Precedence = Routine
    IP: Type of Service = Normal Service
    IP: Total Length = 34 (0x22)
    IP: Identification = 32810 (0x802A)
    IP: Flags Summary = 0 (0x0)
        IP: .......0 = Last fragment in datagram
        IP: ......0. = May fragment datagram if necessary
    IP: Fragment Offset = 0 (0x0) bytes
    IP: Time to Live = 32 (0x20)
    IP: Protocol = UDP - User Datagram
    IP: Checksum = 0xA227
    IP: Source Address = 9.19.141.240
    IP: Destination Address = 224.0.1.118
    IP: Data: Number of data bytes remaining = 14 (0x000E)
UDP: IP Multicast: Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 14
(0xE)
    UDP: Source Port = 0x37A7
    UDP: Destination Port = 0x37A7
    UDP: Total length = 14 (0xE) bytes
    UDP: UDP Checksum = 0x7F30
    UDP: Data: Number of data bytes remaining = 6 (0x0006)
```

Figure 6 – TCP/IP Multicast

```
Frame: Base frame properties
    Frame: Time of capture = 6/20/2000 12:8:45.327
    Frame: Time delta from previous physical frame: 93750 microseconds
    Frame: Frame number: 3
    Frame: Total frame length: 58 bytes
    Frame: Capture frame length: 58 bytes
    Frame: Frame data: Number of data bytes remaining = 58 (0x003A)
TOKENRING: Length =  58, Priority Normal (No token) LLC Frame, Routed.
    TOKENRING: Access control = 16 (0x10) Original, Frame, Priority: Normal (No token)
        TOKENRING: .....000   Reservation bits: Reservation = Normal, No token needed.
        TOKENRING: ....0...   Monitor bit = Original (non-repeated)
        TOKENRING: ...1....   Token bit = Frame
        TOKENRING: 000.....   Priority bits: Priority = Normal, No token needed.
    TOKENRING: Frame control = 64 (0x40), LLC Frame
        TOKENRING: ....0000   Control bits = Normal Buffered
        TOKENRING: 01......   Frame type = LLC Frame
    TOKENRING: Destination address : FFFFFFFFFFFF
        TOKENRING: Destination Address I/G Bit        = Group address
        TOKENRING: Destination Address U/L bit        = Locally administered address
        TOKENRING: Destination Address Functional bit = Group address
    TOKENRING: Source address      : 80062917CF56
        TOKENRING: Source Address Routing bit = Routing information present
        TOKENRING: Source Address U/L bit     = Universally administered address
    TOKENRING: Frame length : 58 (0x003A)
    TOKENRING: Routing control 1 = 0x82, length 2, All Routes Broadcast
        TOKENRING: ...00010   Routing length = 2 bytes.
        TOKENRING: 100.....   Broadcast indicator = All Routes Broadcast B'100'
    TOKENRING: Routing control 2 = 0x70, Forward, All-routes broadcast.
        TOKENRING: Direction indicator = Forward (left-to-right) direction.
        TOKENRING: Largest frame = All-routes broadcast.
    TOKENRING: Tokenring data: Number of data bytes remaining = 42 (0x002A)
LLC: UI DSAP=0xAA SSAP=0xAA C
    LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
    LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
    LLC: Frame Category: Unnumbered Frame
    LLC: Command = UI
    LLC: LLC Data: Number of data bytes remaining = 39 (0x0027)
SNAP: ETYPE = 0x0800
    SNAP: Snap Organization code = 00 00 00
    SNAP: Snap etype : 0x0800
    SNAP: Snap Data: Number of data bytes remaining = 34 (0x0022)
IP: ID = 0x8027; Proto = UDP; Len: 34
    IP: Version = 4 (0x4)
    IP: Header Length = 20 (0x14)
    IP: Precedence = Routine
    IP: Type of Service = Normal Service
    IP: Total Length = 34 (0x22)
    IP: Identification = 32807 (0x8027)
    IP: Flags Summary = 0 (0x0)
        IP: .......0 = Last fragment in datagram
        IP: ......0. = May fragment datagram if necessary
    IP: Fragment Offset = 0 (0x0) bytes
    IP: Time to Live = 128 (0x80)
    IP: Protocol = UDP - User Datagram
    IP: Checksum = 0x8A8E
    IP: Source Address = 9.19.141.240
    IP: Destination Address = 9.19.143.255
    IP: Data: Number of data bytes remaining = 14 (0x000E)
UDP: Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 14 (0xE)
    UDP: Source Port = 0x37A7
    UDP: Destination Port = 0x37A7
    UDP: Total length = 14 (0xE) bytes
    UDP: UDP Checksum = 0xC794
    UDP: Data: Number of data bytes remaining = 6 (0x0006)
```

Figure 8 – Subnet Broadcast