Technical Information

DAQSTATION online in three days

TI 04L01A01-41E

YOKOGAWA

80 Years of Innovative Technology

YOKOGAWA

TI 04L01A01-41E

1st Edition Nov. 2002

DAQSTATION Online in Three Days - A Tutorial

This textbook is prepared for those who want to know more about technologies supporting DAQSTATION network-oriented paperless recorders. Yokogawa Electric Corporation and its group funded this textbook to encourage users in adopting DAQSTATION with its full range of state-of-art networking technologies.

For additional information, contact

Yokogawa Electric Corporation
2-9-32 Nakacho
Musashino, Tokyo 180-8758, JAPAN
http://www.yokogawa.com/tm

Yokogawa Corporation of America
2 Dart Road
Newnan, GA 30265, U.S.A
http://www.us.yokogawa.com/

Yokogawa Europe B.V.
Databanksweg 20
3821 AL Amersfoort, The Netherlands
http://www.yokogawa-europe.com/

Yokogawa Electric Asia Pte. Ltd.
5 Bedok South Road
Singapore 469270, Singapore
http://www.yokogawa.com.sg/

DAQSTATION online in three days

TI 04L01A01-41E 1st Edition

CONTENTS

Introduction

This document is prepared for those who are going to work with Yokogawa paperless recorder, DAQSTATION family, especially with its Ethernet* communication capability to maximize the benefits of this recorder family but have little or no communication/networking experiences. The goal of this document is to make them understand DAQSTATION networking and be capable to plan/design their own DAQSTATION network in three days.

You might wonder if you need whole days in working with this document. Don't worry. A couple of hours would be enough if you have necessary equipments and documents listed at the first section of each day. The program consists of:

Getting Started: The first day is an "experiencing day." You will get experienced with DAQSTATION and network. As an ancient philosopher said, "Seeing is believing," the real experience is the best and shortest path to be knowledgeable of DAQSTATION online. You will see that networking is much easier than you were afraid before. You can skip this and go to the next chapter if you have already experiences in using DAQSTATION over communication network.

Network Technologies: The second day is a "learning day." You will be given an overview of the latest network technologies. You may have had a time scared of hearing unfamiliar, or even alien words on communication technology from a network freak's mouth. It would never happen again to you if you learn fundamentals in this chapter written in easy and familiar words. If you are a very beginner, it is better for you to read them one by one. If you know some part of them, you can skip items you already know. If you are very busy, just skip this chapter and come back when you need to know the word and technology.

Building Your Network: The third day is a "designing day." You will plan your own DAQSTATION network since you already got necessary experience and knowledge. You will find a procedure and guidelines to build a communication network in a professional way and make DAQSTATION and PC ready to serve your business. Standard configuration tables are provided to simplify the design effort so that you have only to pick up the appropriate one to bring the system operational quickly.

It is recommended to have user's manual of your DAQSTATION next to you when you are working with network. Are you ready? OK, let get started.

* Ethernet is a trademark of Xerox Corporation.

DAQSTATION Online

This chapter is to brief you what DAQSTATION online means. DAQSTATION is the second generation of paperless recorders and allows you enjoy the state-of-art communication technology in improving your business and making it much more productive and effective. The first-generation of paperless recorders freed you from supplying and managing chart paper and ink, which had bothered you in managing paper recorders. It is true that it injected another inconvenience to your business to compensate missing functions. DAQSTATION is introduced to address this inconvenience by maximizing the use of communication capabilities as its standard feature. It does not only resolve the problems but also allow you to utilize more sophisticated capability in recording and monitoring. Here is a short summary of such enhancements.

Automatic File Transfer

Recorded data must be stored for years and be able to be retrieved when it is necessary. You needed paper storage of controlled temperature and humidity to make charts survive long. Once data is stored on an electronic medium as a file, its capacity and lifetime became much larger, even boundless in a practical sense. You can manage and manipulate data much easier than before.

Though DAQSTATION has embedded data storage of disk or memory card, its capacity is not large enough to record data of months. They must be transferred onto much larger and less expensive media for long-term storage. File transfer function of DAQSTATION does this automatically to secure data.

Email Notification

DAQSTATION is able to record data without human intervention. However, your instrument needs human services when it experiences a hardware problem. A chemical process needs operator's intervention when its temperature becomes too high. You may want to be notified when such interaction becomes necessary. DAQSTATION has a capability to send an email to you or your people in those cases. It comes to your PC in the office. Or it comes to your pager or cellar phone if you want to get it even when you are out of office.

Display Image Transfer

It is quite common to show the data in your verbal report or written document. With paper recorders, you made a copy of the chart, or even removed the chart from a recorder for this purpose. DAQSTATION allows you to the same thing. A PC on the network can get current display image from DAQSTATION to make a printout. Or you can embed display image into your electronic documents.

PC Software for Monitoring

Yokogawa has PC software packages to manipulate data from DAQSTATION for monitoring, group display and analysis. There are third-party software packages for further manipulation in the marketplace. DAQSTATION and PC software provide connectivity to them via network. You do not have to bring data media by yourself.

You have had a glimpse of networking features that replace chart paper and do more for your business. They make DAQSTATION need-no-paper-any-more recorder rather than paperless. Thanks to the latest networking technologies and convenient network components of hardware and software, network planning is not so tough as it was a decade ago. You should be able to bring DAQSTATION online in three days.

Day 1: Getting Started

The first day is an “experiencing day.” You will get experienced with DAQSTATION and network. As an ancient philosopher said, “Seeing is believing,” the real experience is the best and shortest path to be knowledgeable of DAQSTATION online. You will see that networking is much easier than you were afraid before. You can skip this chapter and go to the Day 2 if you already have experiences in using DAQSTATION over communication network.

You will configure PC and DAQSTAION as instructed. Use configuration parameters as abracadabra instead of asking why. It is much more important for you to experience today than to know details. They will be explained on the second day.

1.1 What you need are ...

First of all, collect all necessary instruments on your workbench. They are DAQSATION, PC and network components. This hands-on system requires three or four AC power outlets (one or two for PC, depending it has an integrated LCD display or separate CRT). Make sure you have instruction manuals of DAQSTATION and PC operating system (you may need operating system CD-ROM).

DAQSTATION

You need a paperless recorder of DAQSTATION family. It can be one of DX100, DX200, MV100, MV200, CX1000 or CX2000, which have Ethernet connectivity as a standard feature. Instructions are given assuming you have DX200. Additional explanations will follow if some recorders need different procedure.

DAQSTATION is accompanied with either dedicated AC power cable or a power supply terminal mounted near the right-top corner of the back panel. If you find a power supply terminal, prepare a power cable with AC plug to connect to L and N terminals with screws. If your power cable has a grounding wire, connect it to the ground terminal of DAQSTATION indicated as ↓.

Windows PC

You need a PC with Windows operating system installed. Operating system can be one of Windows98, Windows-Me, Windows NT 4.0, Windows2000, Windows-XP or later. It is recommended to have a professional operating system such as Windows2000 and Windows-XP Professional for stable operation and file transfer training. Instructions are given assuming you have Windows2000 Professional. Additional explanations will follow if some other operating systems need different procedure by referencing operating systems. A personal operating system such as Windows98, Windows-Me and Windows-XP Home can be used in this training but not recommended because they lack some functions or become astable in some cases.

Administrator privilege is necessary to configure a network function of a professional operating system, such as Windows-NT 4.0, Winsow2000 and Windows-XP Professional. Ask administrator password to the PC vendor or whomever you get this PC from. A personal operating system requires user name and password if its network is already configured.

PC must have Ethernet connectivity. Typical hardware are network interface card (NIC) for an extension slot, a PCMCIA card or build-in network interface on the motherboard. Many PCs are Ethernet-ready when you purchase them. Some PCMCIA card needs “adaptor” cable to accept RJ45 LAN cable.

Network Components

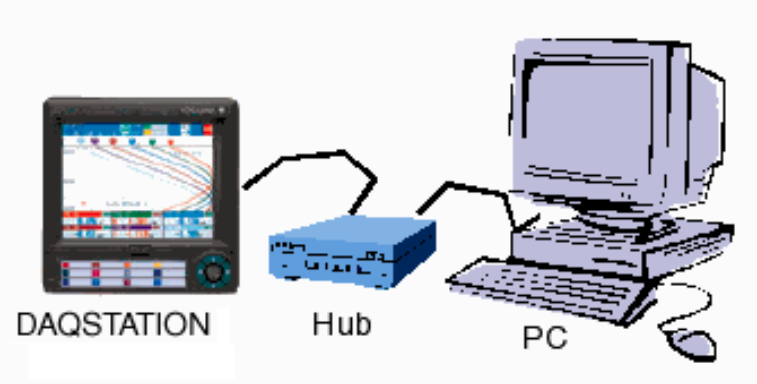
You need an Ethernet hub and two network cables. Select a hub with four or more ports, which supports 10BASE-T. You can also use a hub of automatic speed selection from 10BASE-T and 100BASE-TX.

Prepare two “straight (or patch)” UTP cables (often referred as LAN cables) of “category 3” or higher, e.g. category 4, category 5 and so on. These attributes are indicated on the package when you purchase them. Cable length should be 1m (3 ft) or longer. A UTP cable has RJ45 plastic connectors (see right) on the both ends, which is similar but a little larger than a telephone line (RJ11) connector.

Here is a confusing situation. A “cross cable” is often used for Ethernet connection between PC and another device directly, e.g., without using a hub. We are not going to use this cable in this hands-on training. It is better for you to avoid using cross cables, which would cause a plug-but-won’t-play nightmare. If you are not sure you have a straight cable or a cross cable, they can be distinguished as follows. Grip ends of the cable with your both hands, one in right and the other in left. An RJ45 connector has a locking clip. Look at the transparent surface on the other side of the clip; you will see eight contacts and thin wires. Wires have different colors. Compare the orders of colors on both connectors. If their orders are completely same, it is a straight cable. Some wires are disordered in a cross cable.

1.2 Connect your PC to DAQSTATION

Since you have all necessary hardware, you can connect cables to devices. Place DAQSTATION, hub and PC from left to right on your workbench. This arrangement is good if you use a mouse.



Equipment Configuration

Connect Network Cables

Make sure power cables are disconnected from AC outlet. Touch a metal (not painted) part of the workbench by your hand to discharge your body. Wiring should be done quickly.

Locate LAN connector of the DAQSTATION. It is near the right or left top corner of the back panel and indicated as “10Base-T.” It is covered with a soft-plastic cap when shipped. Pull the cap straight out of the place to reveal LAN connector. LAN connector has a rectangular hole with a hollow on a side. Grip a cable connector to align the clip to the hollow and insert the cable connector into LAN connector slowly until the clip fits in with clicking sound. This locks the cable into DAQSTATION. When you want to disconnect the cable, push down the locking clip and pull out the cable holding the connector (do not pull the cable part) carefully.

The other side of the cable should go to the hub. The hub has several female connectors and the port number is indicated near each connector. Select #2 port and insert the cable connector in the same manner. Now DAQSTATION and hub are connected with a cable.

Connect PC and #3 port of the hub with another cable. If your PCMCIA card has an adaptor cable, insert it to the card before connecting the RJ45 cable.

Connect Power Cables

Make sure that the power switches are off (on ○ side or not pushed in) before connecting its AC cable to AC outlet. DAQSTATION power switch is located at the left-bottom of the front panel or behind the switch cover at the bottom of the front panel if it has one. Some DAQSTATION recorders have no power switch. In this case, leave AC cable unplugged. Connect power cables of the PC (and display if needed) to AC outlet after connecting peripherals (e.g., keyboard, mouse and CRT). Then connect hub to AC outlet. Some hubs have no power switch and turn on immediately.

Start DAQSTATION and PC

Turn on the hub first. If it has no power switch, its power indicator (or a LED) is already illuminated when you connected the AC cable.

Then, turn on the DAQSTATION by pushing on the power switch or connect AC cable to an AC outlet. The LCD display panel should be on and initialization message comes up. Look at the LED indicator of #2 port on the hub. It should be on to show that the device hooked to #2 port is alive. If it remains off, check the LAN cable connection to DAQSTATION and the hub. RJ45 connector may not be locked. LED remains off if the LAN cable is not a straight cable but a cross cable.

Power on the PC to confirm #3 LED of the hub is on. Check the cable connection if the LED does not turn on.

Some operating systems for PC ask you to log in. For professional operating system, like Windows-NT4.0, Windows200 or Windows-XP Professional, login as administrator and type password for administrator. You should have been given the password when you acquire the PC. For home/personal operating system, use existing user name and password. You may be able to select “cancel” to login as an anonymous user for some personal operating systems.

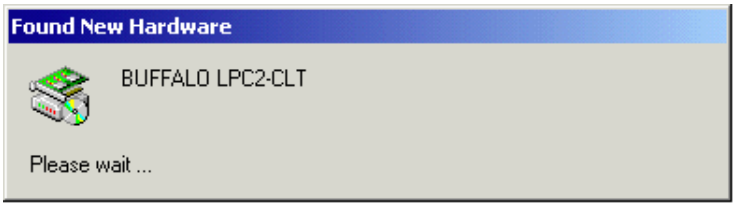
1.3 Configuring the PC

Your PC may show the message that it detected a new hardware, when you turn on the PC first time after you installed the network card. In that case, the operating system needs an appropriate device driver installed. Follow the procedure in the next section "NIC recognition." You can skip this section if you do not get the message.

NIC Recognition

This section explains the procedure to install device driver for the network card. Insert "device driver" floppy disk or CD-ROM, which should be accompanied with the card.

An interactive window indicating "device recognition wizard" or "Install device driver" comes up. Select "Search for optimal driver for this device" and click "Next (N)>." The operating system asks the place to find the driver. Floppy disk and CD-ROM are in the default search path. Click "Go (G)" and the operating system looks for the device driver on the floppy disk or CD-ROM and shows the name of the network card if found.



If the operating system fails to find the driver, go back to the previous window and click "Browse (B)" to give the folder (directory) that contains the device driver. In some cases, the disk contains several folders for different operating systems. Select your operating system from folders to find the driver file, which has extension "`inf`." A typical file name is `oemsetup.inf`. Most of Microsoft operating systems do not show the file name extension until you select View option of Windows Explorer to show the extension.

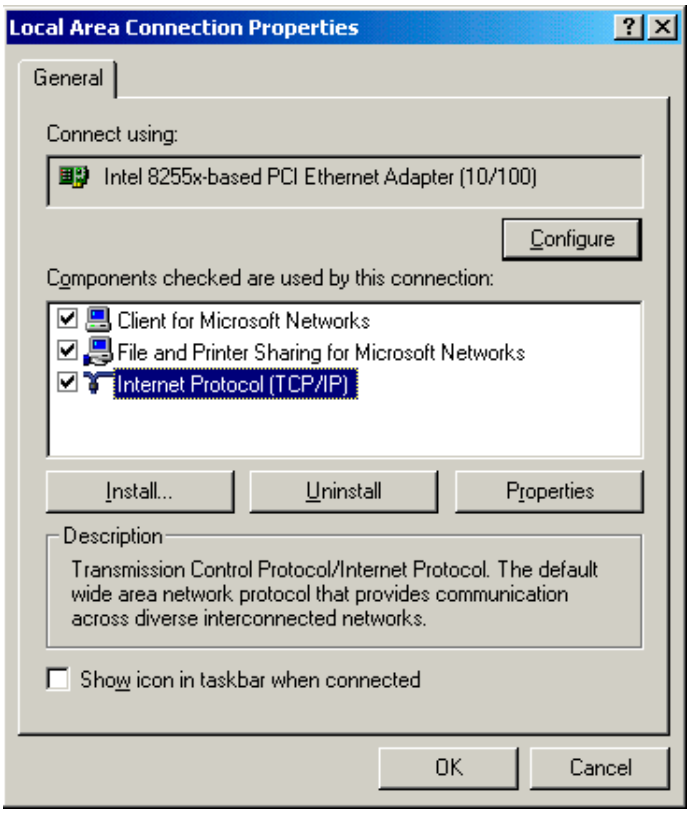
Highlight appropriate driver showing the card type/name and click "Next (N) >>" to install that driver. It will take a few moments and click "Finish" when the installation is completed. If the operating system requires the reboot, follow the instruction to make driver operational.

LAN Configuration

Since the operating system has correct device driver, you should be able to configure the network card. Follow the path *Start* → *Settings* → *Network* and *Dial-up Connections*. In case of a home/personal operating system, follow the path *Start* → *Settings* → *Control Panel*, and double-click "Network" in the Control Panel window.

If you find a "Local Area Network Connection" icon, right-click this icon and select "Properties" to show the network configuration. If you see no such icon, double click "Create a new connection" icon and select network card and TCP/IP. Some home/personal operating system does not install TCP/IP if you choose "standard" installation. It requires you to insert Windows CD-ROM to install TCP/IP. Follow the instructions.

The "Connection Properties" window shows available network components. Highlight "Internet Protocols TCP/IP" and click "Properties." In case of a home/personal operating system, highlight "TCP/IP -> <*network card name*>" and click "Properties." You should have "TCP/IP Properties" window shown below.

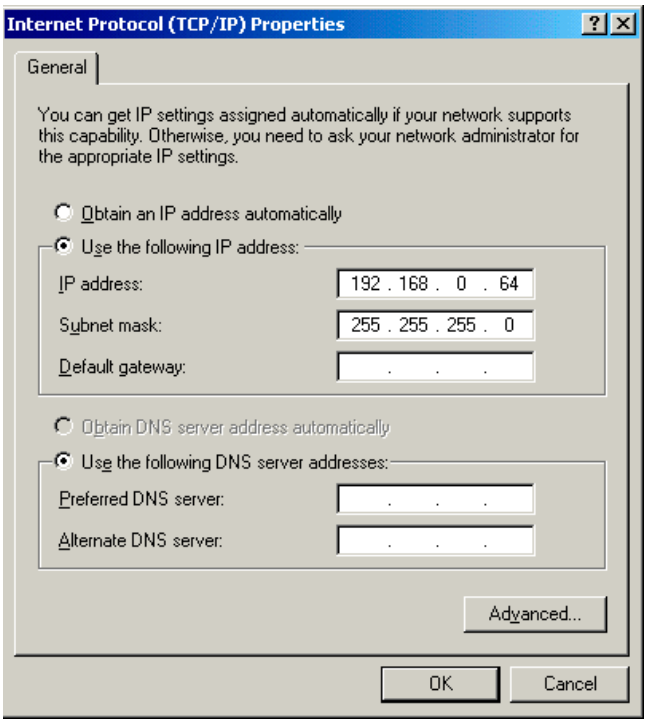


LAN Connection Properties (select TCP/IP Properties)

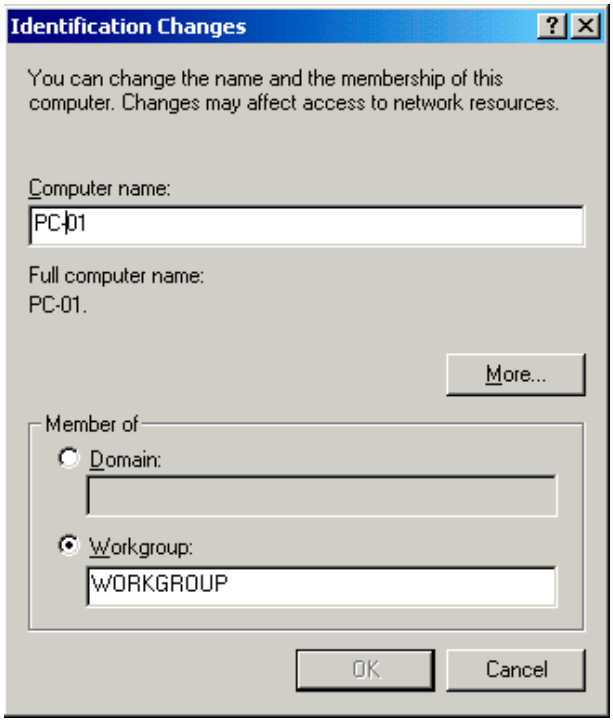
It shows "Obtain IP address automatically" option is selected during the installation. Select another choice "Use the following IP address" option to put following configuration in. Other field can be left blank. "TCP/IP Properties" window of some operating system has multiple pages. Select "IP Address" in that case.

```
IP Address:  192.168.0.64
Subnet Mask: 255.255.255.0
```

Typical windows display is shown below (left). Click OK to close "Properties" windows. If the operating system requires the reboot, follow the instructions to make IP address effective.



TCP/IP Properties



Computer Name and Workgroup

Set Your Host Name

You can give a name to the PC to select it by name instead of IP Address. This name is called "Computer Name" or "Host Name."

Follow the path *Start* → *Settings* → *Control Panel* and double-click the "System" icon in the Control Panel window. It will show you the network-visible attributes of the PC. Highlight "Network ID" to click "Properties" to open a window shown right in the previous page. Type `PC-01` in "Computer Name" field. The membership field below it shows this PC is a member of "WORKGROUP" workgroup. Leave it as it is. Click "OK" to close the two windows. If the operating system requires the reboot, follow the instruction to make this change effective. Your PC should be ready for Ethernet communication.

1.4 Configuring the DAQSTATION

Before you configure netw STOP key and look at the display. If the recording function is running, you have a dialog window that asks, “What do you want to stop?” Select a field showing the most items like “Mem+Math” and press DISP/ENTER button. If you see no dialog window, recording function was not running and you are ready for network configuration.

Open Basic Setting Menu

Press MENU key to get “Set mode” display. Then press FUNC key for more than three seconds to have “Basic Setting mode” display.

Select “Communication” soft key and press it. If “Communication” menu is in another page, press “Next” soft key to go to that page. Press soft key associated with “Ethernet, Serial” menu.

Use cursor keys to select a configuration parameter (field is highlighted when selected) and press “Input” soft key to give the value. DAQSTATION family has different methods for different types in giving alphanumerical text. Refer the instruction manual for your DAQSTATION. After finishing the text input, press DISP/ENTER button to give the value to parameter. Cursor moves to the next field.

IP Address and Subnet Mask

Give following values to parameters. Other parameters may be left blank or as they are.

```
IP-address          192.168.0.71
Subnet mask         255.255.255.0
Default gateway     0.0.0.0
DNS On/Off          Off
```

A parameter field of new entry is shown in different (yellow) color. Press DISP/ENTER button one more time to confirm all entries and bring all parameter field in white or blue color. Press ESC key twice to go back to “Basic setting mode” menu.

Press soft key associated with “Web, Email” menu and select “Web” soft key. Give following values to Web parameters and confirm them by pressing DISP/ENTER button one more time.

```
Use/Not             Use
Page type           Monitor
  On/Off            On
  Access control    Off
```

Press ESC key twice to come back to “Basic setting mode” menu. Press soft key associated with “End” menu, and you will get a dialog window that asks, “Do you want to store and make the new settings take effect?” Select “Yes” and press DISP/ENTER button. Within seconds, the screen changes to the recorder display and the communication should be running.

Press START key to start recording.

1.5 First Call to DAQSTATION

Now DAQSTATION and PC should be ready for online. Let us confirm this by sending a short message from PC to DAQSTATION and receiving a reply over the network.

Open Command Prompt Window

Go to the PC and open DOS window for command prompt by following the path *Start* → *Programs* → *Accessories* → *Command Prompt*. Some personal operating system shows *Command Prompt* just after *Programs* menu. A command prompt window has a black background with white characters in default. You can give a DOS command after `C:\>` prompt.

Ping to DAQSTATION

Give following command to the prompt and press ↵ Enter key. It will show you the process of PC trying to communicate with DAQSTATION on the screen.

```
ping 192.168.0.71 ↵
```

Reply should come back in 10ms or less if the network is properly configured. You will have following display:

```
Microsoft Windows 2000 [Version 5.00.2195]
(c) Copyright 1985-1999 Microsoft Corp.

C:\> ping 192.168.0.71

Pinging 192.168.0.71 with 32 bytes of data:

Reply from 192.168.0.71: byte=32 time<10ms TTL=255
Reply from 192.168.0.71: byte=32 time<10ms TTL=255
Reply from 192.168.0.71: byte=32 time<10ms TTL=255
Reply from 192.168.0.71: byte=32 time<10ms TTL=255

Ping statistics for 192.168.0.71:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

If you get successful result, you can go to the next section. You will have following display if network is not operating properly. You need to fix the problem before going to the next section. Follow the procedure below.

```
Microsoft Windows 2000 [Version 5.00.2195]
(c) Copyright 1985-1999 Microsoft Corp.

C:\> ping 192.168.0.71

Pinging 192.168.0.71 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.71:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss).
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Make sure that you gave correct IP address of DAQSTATION (`192,168.0.71`) to the prompt. Simplest cause of the problem is a wrong number or wrong order of numbers, or commas instead of periods.

If you gave IP address correctly, problem may be in PC, DAQSTATION or cabling. In order to separate causes, try to call NIC from your PC by giving the following command:

`ping 192.168.0.64` ↵

If this resulted time out again, PC should have a problem. Repeat procedure for NIC recognition and PC configuration. Possible causes might be wrong driver, wrong IP address/subnet mask or faulty NIC hardware.

If you have reply from `192.168.0.64`, problem should be in either cabling or DAQSTATION. Check if the LED displays for port #2 and #3 of the hub. If one is not illuminated, the cabling has a problem. Possible causes might be loose or incomplete mating of connectors, wrong (cross) cable or faulty hardware.

If you are still unable to succeed ping, check DAQSTATION configuration. Possible causes might be wrong IP address/subnet mask or you did not save configuration when leaving the Basic Setting mode.

1.6 Open DAQSTATION Web Page

Since your PC and DAQSTATION are able to communicate each other, you can browse DAQSTATION web page.

Start Internet Explorer

Locate and double click Internet Explorer icon (shown in blue ***e***) at the left-bottom corner of the screen or on the wallpaper. If you do not see the icon, follow the path *Start → Programs → Internet Explorer*.

If you are using Internet Explorer for the first time after Windows installation, Internet Connection Wizard shows up to configure the connection. Select options saying, "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and "I connect through a local area network (LAN)" in the next page. Remove checkmarks from "Automatic discovery of proxy server," "Use automatic configuration script" and "Manual Proxy server" before clicking "Next." Select "No" to a question asking, "Do you wan to set up an Internet mail account now?" (You do not have to make email account at this moment). Internet Explorer should be ready when you click "Finish."

Web Page and File Folder

DAQSTATION Web Page

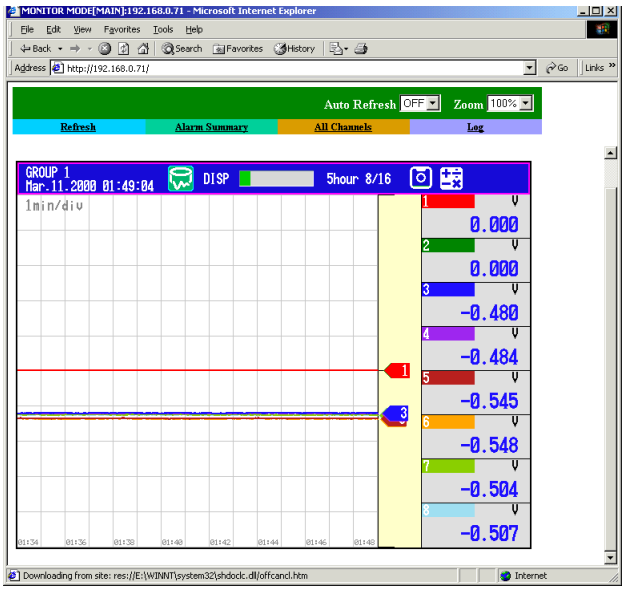
Type following string into the "Address (or URL)" field:

`http://192.168.0.71/monitor.htm` ↵

This will bring DAQSTATION display image into the browser. You can get a new display by clicking "Refresh" icon at the left-top corner of the web page. Turn on the "Auto Refresh" at the right-top corner of DAQSTATION web page, and display should refresh automatically.

Go to the DAQSTATION to change its display. Press DISP/ENTER button, and display menu comes to left side of the display. Switch to new display, say DIGITAL and press DISP/ENTER button to get new display. Your browser will show the new display very soon.

Click "Alarm Summary" and "Log" at the top of the web page to open new windows showing alarms and logs. If DAQSTATION has no entry to show, you will see only headers. Close those windows and click "All Channels." A new window will show the current measured value of all channels.



DAQSTATION Web Page

DAQSTATION File Folder

Type following string into the “Address (or URL)” field:

`ftp://192.168.0.71/` ↵

This will bring DAQSTATION file system into the browser. You may see folder data0 where recorded files are stored. Double click this to see its content. It is empty until DAQSTATION creates file. If there are files, you are able to download them into your PC by double-clicking a file one by one.

Now you are confident to see DAQSTATION display and important information via network. It would be a good idea to take a break now. Was it tough for you or much easier than you had been afraid? As you see, making DAQSTATION online is neither complicated nor difficult if you follow the correct procedure.

The next training may take a considerable time in installing necessary software. If you are so busy, you may skip it or come back on the other day. Again, you should be proud that you have successfully brought DAQSTATION online.

1.7 Try File Transfer with ftp

DAQSTATION stores recorded data as files, which you can handle with a computer. They are stored in an external medium (disk or memory card) automatically. Though you have an option to bring the medium to your computer by yourself, it is much easier and safer to do that via network. You do not have to touch the medium. One easiest method is to use ftp client of DAQSTATION to transfer files automatically to a computer of huge storage media. This stores a file in the two places, DAQSTATION and computer, and decreases the risk of losing it by an accident.

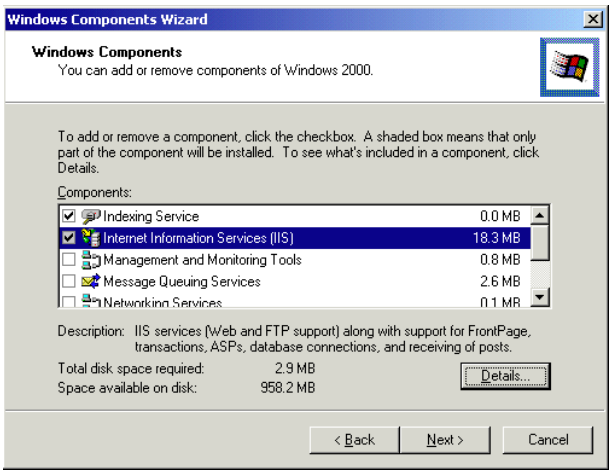
This method allows DAQSTATION to transfer a file automatically to the server computer when it is created. The process is initiated by DAQSTATION and therefore called "push" transfer. The computer must have a function called "ftp server" to accept the file using "File Transfer Protocol (ftp)." It is recommended to use professional operating system such as Unix and Windows2000 for safe and secure operation. Though there are ftp servers, distributed as a free software or shareware for personal operating systems like Windows98, many of those servers are neither secure nor stable and are not recommended for business use.

This section uses an ftp server bundled with Windows2000 operating system. Windows-XP Professional can be used in place of it. You may skip this section if you do not have such operating system on your PC.

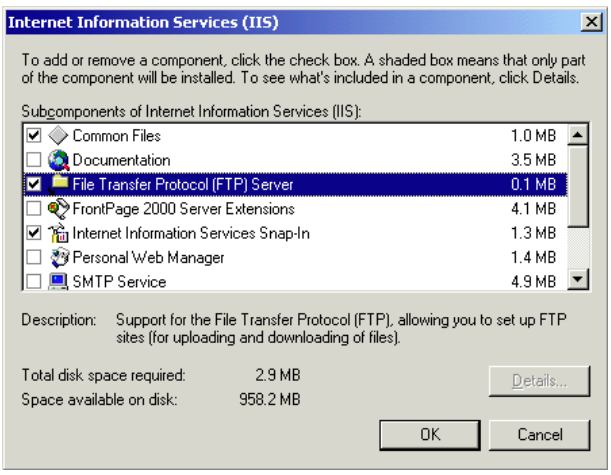
Install ftp Server into your PC

This section installs Internet Information Service (IIS) to your PC to activate ftp server. If you plan to have many DAQSTATION recorders to transfer files, you need Windows2000 Server operating system. In case of few recorders, server function of Windows2000 Professional is good enough. But neither ftp server nor IIS are installed when you install Windows2000 Professional operating system into your PC if you follow the standard installation procedure. Prepare Window2000 CD-ROM ready to use. Log in Windows2000 as administrator.

Follow the path *Start* → *Settings* → *Control Panel*, and double-click "Add/Remove Programs" icon in Control Panel window. Select " Add/Remove Windows Components" in the new window to open "Windows Components Wizard" as shown left below. Highlight "Internet Information Services (IIS) and click "Details..." to open IIS window shown right below. Check "File Transfer Protocol (FTP) Server," and two more items are automatically selected. They are "Common Files" and "Internet Information Services Snap-In." Click OK to return "Windows Components Wizard" window and see IIS is grayed out. Click "Next" to start installation and insert Windows2000 CD-ROM when requested. Click "Finished" of the Wizard to activate ftp server.



Windows Components Wizard



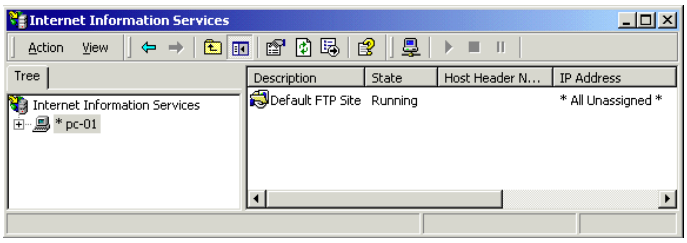
Install ftp Server and IIS Components

You may wonder where is the ftp server because you cannot find any indication on wallpaper, task bar or even in menu! Do not worry. It is working. Let us find the clue. Open Control Panel by following the path *Start* → *Settings* → *Control Panel*, and double-click "Administrative Tools" icon to open new window showing software tools to manage Windows2000. Double-click "Internet Service Manager" to see IIS status. Highlight the PC icon accompanied with "* pc-01" in the left half of the window, and you will see the "Default FTP Site" is "Running" in the right half of the window. An example screen is shown in the left top on the next page.

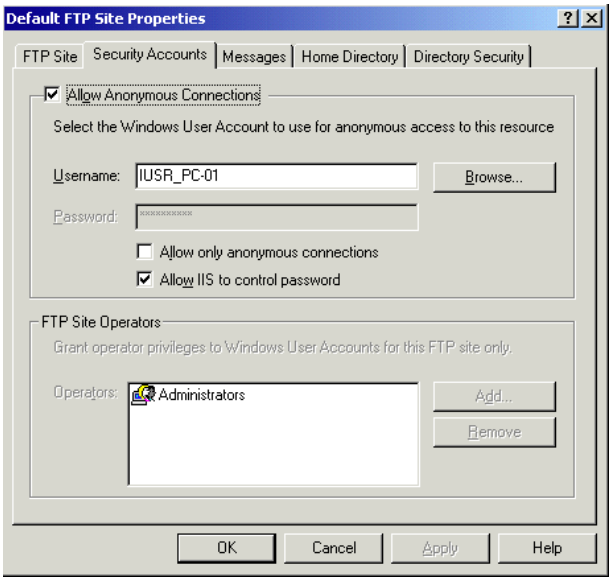
Disable Anonymous ftp

This ftp site accepts request from anybody (mentioned as “anonymous”) without any authentication. This is not good for security and the ftp server should be dedicated for DAQSTATION. Highlight “Default FTP Site” in the right half of the window. Press the right button of the mouse when cursor is within this window and select “Properties” to see “Default ftp site Properties” window shown in top right on the next page. Select “Security Accounts” tab and clear check in “Allow Anonymous Connections.” The system will ask if you are sure you want to continue. Answer “Yes.”

Then select “Home Directory” tab to select folder for ftp. System already selected “a directory located on this computer” and gave a Local path name C:\Inetpub\ftproot to be created. Check “Write” and confirm “Read” and “Log visits” are already checked. Directory listing style should be “MS-DOS.” Click OK to allow only authorized users use this ftp site. Close IIS status window.



IIS Status Window



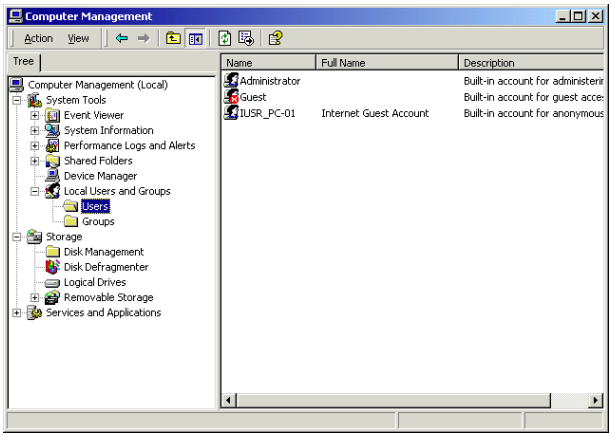
Default ftp Site Properties

Create a User Account for ftp Client

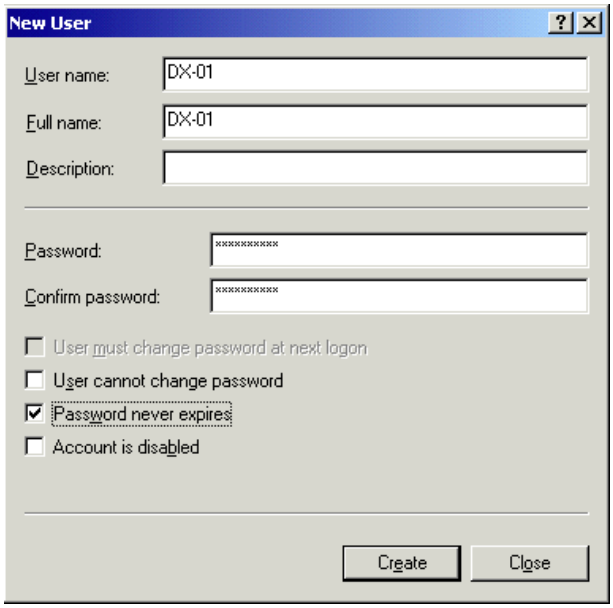
The next step is creating ftp user accounts. Go back to “Administrative Tools” window to double-click “Computer Management” icon.

The new window (see left below) shows managed items in a tree in left half and member of the selected group in the right half. Double-click “Local Users and Groups” to show “Users” and “Groups” folders. Select Users, and you will see registered users in the right half. We are going to add DAQSTATION as a new user. Press “Action” in the menu bar and then select “New User...” to open a new window to register a new user shown in right below.

Type DX-01 into “User name” and “Full Name” fields. User name is a keyword to identify ftp user. Type DAQSTATION into both “Password” and “Confirm Password” fields, where input characters are not visible but replaced with asterisks. Be careful in tying of upper cases. Remove check for “User must change password at next login” and give check to “Password never expires.” They are necessary because DAQSTATION never login to change password. Click “Create” to create account and close it by clicking “Close” for another account. The new user *DX-01* shows up in the right half of “Computer Management Window.”



Computer Management Window (User)

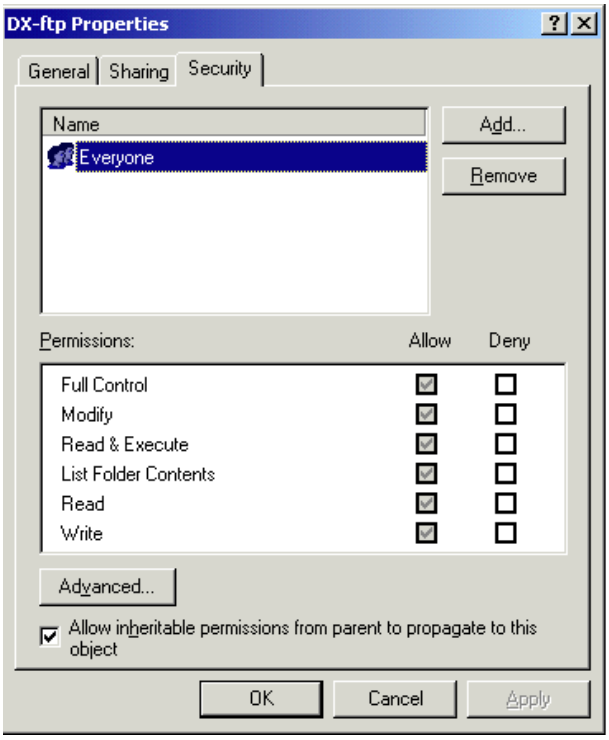


Add a new user window.

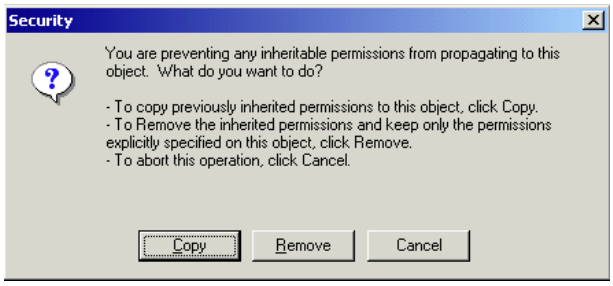
Create File Folder for DAQSTATION

Let us create a file folder in your PC for DAQSTATION and give access right to DAQSTATION. Open Windows Explorer by following the path *Start* → *Programs* → *Accessories* → *Windows Explorer* to see `C:\Inetpub` and `C:\Inetpub\ftproot` folders under My Computer. Create a folder `DX-ftp` for DAQSTATION by highlighting the latter folder and following the Explorer menu *File* → *New* → *Folder*. Give folder name `DX-ftp` to "New Folder" field of the created folder.

Highlight `DX-ftp` folder and press mouse right button to select "Properties." Select "Security" tab to see the access control to this folder (see left below). Remove check from "Allow inheritable permissions from parent to propagate to this object." Answer "Remove" to a long warning message shown in right below. This will remove "Everyone" from the name list. At this moment, nobody is entitled to have an access to this folder.



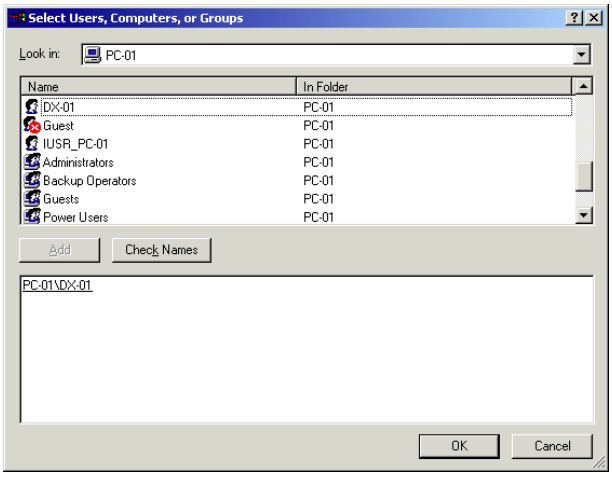
File Folder Properties



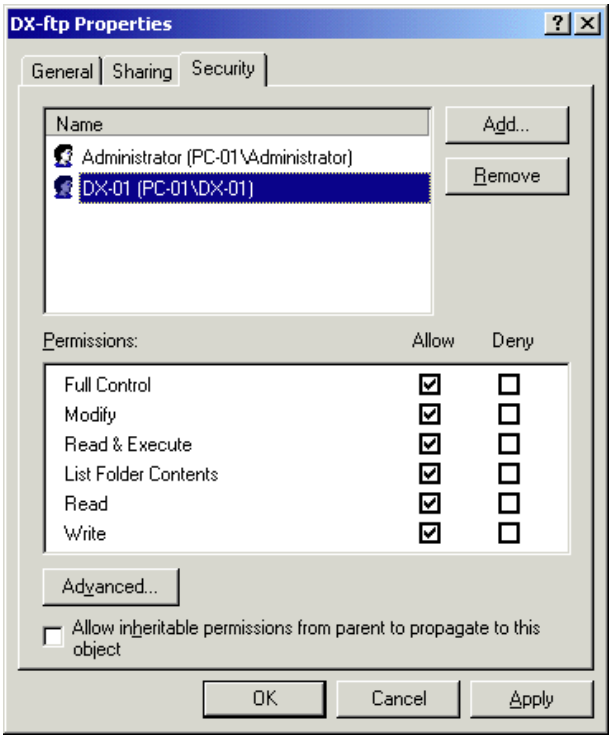
Waning to disable Permission Inheritance

Click “Add” to open “Select Users, Computers, or Groups” window shown in left on the next page. Locate `DX-01` in the upper half of the window to highlight it. Click “Add” to have `PC-01\DX-01` in the bottom half of the window. Click “OK” and you will come back to “DX-01 Properties” window. Check “Full Control” in “Permissions” list. This gives all access permission to DAQSTATION.

Add one more user, Administrator, with full access permission. Final result is shown in right on the next page. You can create other account only with Read permission to retrieve file from the server if needed. Click OK to close this window.



DX-01 is added as a new user.



This folder has two users.

File folder is now ready for ftp service. If you have two or more DAQSTATION recorders, create similar folder for each recorder so that it will transfer files to the different folder. This is important to know which DAQSTATION this file came from, because it is impossible to do that only with a file name consisting of a number string.

Close remaining windows started from “Administrative Tools.”

Configure DAQSTATION ftp Client

Since ftp server is ready, we can configure ftp client in DAQSTATION. Press STOP key and look at the display. If the recording function is running, you have a dialog window that asks, “What do you want to stop?” Select a field showing the most items like “Mem+Math” and press DISP/ENTER button. If you see no dialog window, recording function was not running and you are ready for ftp configuration.

Press MENU key to get “Set mode” display. Then press FUNC key for more than three seconds to have “Basic Setting mode” display. Select “Communication” soft key and press it. If “Communication” menu is in another page, press “Next” soft key to go to that page. Press soft key associated with “FTP client” menu.

Use cursor keys to select a configuration parameter (field is highlighted when selected) and press “Input” soft key to give the value. DAQSTATION family has different methods for different types in giving alphanumerical text. Refer the instruction manual for your DAQSTATION. After finishing the text input, press DISP/ENTER button to give the value to parameter. Cursor moves to the next field.

FTP transfer file		
	Disp & Event Data	On
	Report	On
FTP connection		
	Primary	
	FTP server name	192.168.0.64
	Port number	21
	Login name	DX-01
	Password	DAQSTATION
	Account	(blank)
	PASV mode	Off
	Initial path	DX-ftp

T001.eps

A parameter field of new entry is shown in different (yellow) color. Press DISP/ENTER button one more time to confirm all entries and bring all parameter field in white or blue color. Press ESC key twice to go back to “Basic setting mode” menu. Press soft key associated with “End” menu, you will get a dialog window that asks, “Do you want to store and make the new settings take effect?” Select “Yes” and press DISP/ENTER button. Within seconds, the screen changes to the recorder display and the communication should be running.

First ftp Test

Now you are ready to test ftp transfer. Go to DAQSTATION and press FUNC key to see soft menu. Press soft key showing "FTP test" and then press soft key showing "Primary." You may need to press "Next" key to find "FTP test" key. Once test is started, a small window comes up to the DAQSTATION display showing "Execution is complete." It tells you that ftp service test was successful. Go to the PC and see the content of `DX-ftp` folder. A file `DX_FTPC.TXT` should be there (If your Windows Explorer is configured to "hide extension of know file type," the file is displayed as `DX_FTPC` without extension). If you open this file with Notepad, you will see date and time of the test.

If you get a message "FTP control connection error" during the test, DAQSTATION failed to transfer `Dx_FTPC.TXT` file to the ftp server. Possible causes are wrong user name, wrong password or wrong folder name in PC configuration, or wrong IP address of primary ftp server, wrong user name, wrong password or wrong initial path in DAQSTATION configuration. Make sure they are configured correctly.

Transfer Data Files

We are going to see how automatic file transfer takes place. Press START key of DAQSTATION to start recording. It may take several minutes or more to correct data for one file. Wait until you see a message on DAQSTATION display "Data are being stored to media." This waiting time depends on the measurement configuration. When DAQSTATION creates a file in its local medium, it is also transferred to ftp server.

Go to the PC to see the content of `DX-ftp` folder. There should be files of measured data (of .DDS extension) and/or report file (of .DHR extension).

1.8 Experience Yokogawa Software Package

Now you should be confident DAQSTATION is online. The final training is to experience Yokogawa software package for PC, DAQSTANDARD, which DAQSTATION is accompanied with.

Install DAQSTANDARD into your PC

Insert DAQSTANDARD CD-ROM and the installation starts automatically. If it does not start, double-click `Setup.exe` (`or Setup` if extension is hidden) file icon in the root folder of the CD-ROM. Follow the instruction.

Start DAQSTANDARD

Start DAQSTANDARD by following the path *Start* → *Programs* → *DAQSTANDARD Software* → *Launcher*. DAQSTANDARD tries to reach DAQSTATION. When failed, Network Configuration window comes up. Select “Ethernet” to give `192.168.0.71` to “Address” field and click OK. Once succeeded, a small launcher window comes up.

Double-click the “CONFIG” icon to open “Hardware Configuration” window. Select “Comm” in the top menu bar and then “Receive Setting.” **Warning**: Do not select “Send Setting,” which would erase all configurations you made for DAQSTATION. Answer “Yes” to confirmation dialog for receiving and the complete message. Received information should be visible in DAQSTANDARD window. Save configuration to a file by selecting “File” in the top menu bar and “Save as” to give the path.

You can configure measurement channels on DAQSTANDARD by referencing the instruction manual and download it to DAQSTATION. This makes configuration and maintenance easier. You can save configuration in the PC for management purpose.

Available PC Software Packages

DAQSTANDARD configures DAQSTATION via network. Yokogawa offers other software packages to monitor, save and analyze data. If you have purchased software such as DAQEXPLORER, DAQLOGGER, ADDMULTI and ADDOBSERVER, install and try them by following the instruction manual. It must be easy because DAQSTATION is already online and you should not have any communication problem.

Day 2: Day Two: Network Technologies

The second day is a “learning day.” You will be given an overview of the latest network technologies. You may have had a time scared of hearing unfamiliar, or even alien words on communication technology from a network freak’s mouth. It would never happen again to you if you learn fundamentals in this chapter written in easy and familiar words. If you are a very beginner, it is better for you to read them one by one. If you know some part of them, you can skip items you already know. If you are very busy, just skip this chapter and come back when you need to know the word and technology.

No additional material is necessary in reading this chapter. You may read this chapter whenever and wherever you find a chance to do so. It would be interesting if you try examples in this chapter with your PC that can go to Internet.

2.1 Networking and Protocol Fundamentals

A network consists of basic elements and their interactions, which is capable to do something further than what each element can do. Your brain is an assembly of billions of neuron cells and their interconnections through synapses. Neurons and synapses are rather simple and their biochemical behavior is well known. But the overall system is really complex and it is the place where intelligence exists. A technology field called “neural network” was studied since 1980s to simulate intelligence by a man-made network. This network is capable to “store” knowledge and even “discover” solution of a problem without a help of human beings.

Another example is people’s networks to help victims of war or natural disaster, save Nature and wild life, and keep peace. An individual can do just a very little. But contributions could be quite comprehensive; soothe an injured child, cook and distribute lunch, collect garbage on a shore or a hill, remove starfish from a coral reef, sweep mines, express opinions, sign on an appeal, or even donate a bill. Once combined, those contributions acquire much power and become a higher movement to achieve their goal for the world and human life.

This scope of network needs more investigation and is too general for this small document. Instead, we should concentrate in a network of DAQSTATION and computers, which still have a plenty of issues to learn. Connect your DAQSTATION and computers with LAN cables to see what happens... Nothing would happen unless you allow communication as experienced in the previous chapter yesterday. Communication makes DAQSTATION and computer share the data and utilize mutual capabilities to manipulate data. It could result advanced data acquisition/ manipulation of higher level, which either DAQSTATION or computer cannot achieve individually. This is a network.

Communication Protocol and Interoperability

Communication is a mechanism to transfer a meaning data from function A (producer of the data) to function B (user of the data) in a mutually understandable form. Data transfer can be from A to B (uni-directional), or between A and B (bi-directional). Most important thing is, B understands what A says. Suppose you speak only English and your friend talks to you in Latin. There would be no communication between the two of you, if you do not trust body language. The definition of data structure (words) and procedure (grammar) to transfer data is called “communication protocol” or simply “protocol.” If you have watched Star Wars movie, you may recall C3-PO “protocol droid.” His role is to translate millions of languages and keep etiquette and procedure in diplomatic negotiation, which is protocol.

The benefit of networking comes from the interaction and cooperation of DAQSTATION and computers. Suppose they have a capability to talk the same communication protocol. It is absolutely necessary. But is it good enough to achieve the goal? The answer is no. They must have software running in them, which understand the meaning of the data, request and/or reply from others, and what the others expect to behave appropriately. Such software, combined with communication protocol, is called “Application Process” or simply “Application.”

A device with Application(s) is called “host.” Interoperability is a capability of hosts to work together serving for higher functionality. We need three conditions to achieve interoperability:

(1) Same communication protocol is running in hosts,
(2) Applications, which understand data and protocol, are running in hosts, and
(3) There is a coherent method to organize hosts and Applications.

DAQSTATION family has a standard communication protocol as well as common applications (see the last section of this chapter) in the world to achieve interoperability to various applications.

LAN and WAN

Hosts can be installed in different places, causing a physical spread of the network. How wide is your network? If it is a network within your office or business place, it is local and is called Local Area Network (LAN). Hosts are distributed in an area of a few meters or hundreds of meters in diameter. Number of hosts is from a few to hundreds. A network of several DAQSTATION recorders and a PC is an example of LAN. LAN is often mixed up with Ethernet (explained in the next section). It is true most of LANs are built with Ethernet but Ethernet is just a physical medium to build a LAN.

If your network connects buildings and facilities distributed in cities or states, it is called Wide Area Network (WAN). They are connected with dedicated lines, public telephone lines, radio, or through Internet. The network spreads in kilometers or over the globe. Number of hosts can be thousands or more. The word WAN is also used to distinguish connection to an Internet provider for broadband communication from a LAN.

Internet connects Networks

The idea of WAN can be extended to connect every host in the world to result Internet. This concept was developed to connect networks (inter-net) for military purposes as ARPANET by Defense Advanced Research Project Agency (DARPA) of United States. It was a network to connect four universities and national institutes with 56Kbps in early 1970s. When the project split into two, ARPANET for research and MILNET for military communication, more universities, institutes and companies became interested in having connection to this network to form a loose-connected global network maintained by their voluntary efforts. Email was exchanged with other academic networks like UUCP (Unix-to-Unix Copy Program) network among Unix operating system users.

Commercial offer of Internet Service Providers (ISPs) changed everything dramatically. They own and share long-distance lines of high-speed high-capacity transmission to allow people to have an access to Internet just by calling an access point. Local phone call and ISP fare are cheap and one can get data from a computer located on the other side of the globe with the same cost to call another computer in the immediate neighbors. This opened the real information age.

Cheap Internet connection changed business communications by providing secure communication over public Internet instead of costly dedicated lines. Confidential data is encrypted before going into Internet so that the only authenticated users can decode and read it. This is called Virtual Private Network (VPN). Many VPNs were proprietary by vendors but a standard method called IPSec (Internet Protocol Security) was developed and is becoming common.

One field of Internet communication is very hot these days. It is called “last one mile” problem to connect homes and offices to Internet high-speed backbone. Common methods are 56Kbps analog line and 64Kbps ISDN, which are too slow to transfer data we use today. Digital Subscriber Line (ADSL and others) is improving this problem and 100Mbps fiber line is growing. Mobile phone starts from 9600bps of GSM (Global System for Mobile Communications) and is coming to 3GSM (W-CDMA) of up to 2Mbps. Wireless LAN is another alternative and will be discussed later.

2.2 IEEE802.3 Ethernet

This section explains Ethernet, which all DAQSTATION family has as a standard feature.

Palo Alto in 1970s

In early 1970s researchers were trying to connect computers at Xerox laboratory in Palo Alto, a town in southern California, where coaxial cables crawled around the laboratory to transfer data. They imagined such network would be at any places in the world soon and christened their network “Ethernet” from the ubiquity of “Ether” postulated in 19th century as a medium of light wave. Ether was considered to exist at any place in the universe because light travels through the space until the negative experimental result to detect Ether by Michelson and Morley in1887, which germinated Albert Einstein’s special relativity in 1905.

Ethernet specification was disclosed in 1976 and then standardized by IEEE (Institute of Electrical and Electronic Engineers) of United States as IEEE802.3. Three companies, Digital Equipment (DEC) Intel and Xerox, proposed extended specification (DIX for their initials) and DIX specification is well adopted in TCP/IP Ethernet.

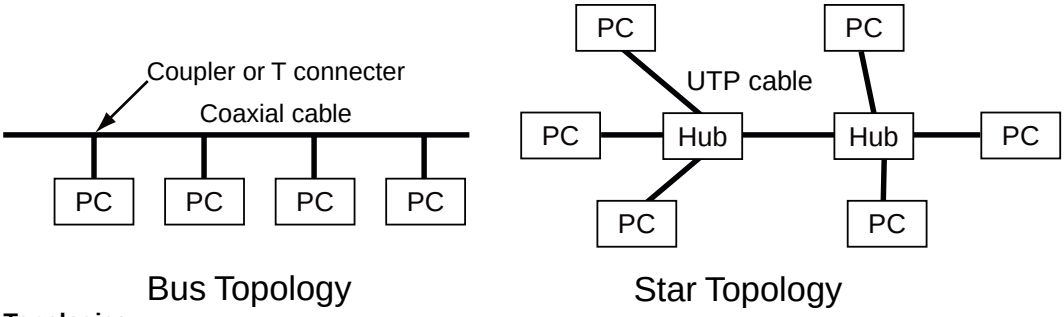
Wire and Optical Media

A medium transfers communication signals; electric, optical or radio. Early Ethernet in Palo Alto used a thick coaxial cable. We now have variable media of various speeds. The following table shows only a few examples of electric media. Maximum cable length depends on transmission speed (or “bandwidth”) and signal modulation. A medium name starts with a number showing transmission speed in Mbps unit and terminates with another number or character indicating the cable type. For your reference, Mbps stands for “Megabit per second.”

Media	Bandwidth	Cable	Maximum Cable Length
10BASE-5		Coaxial cable (12mmϕ)	500m
10BASE-2	10Mbps	Coaxial cable (5mmϕ)	185m
10BASE-T		UTP cable (category 3)	100m
100BASE-TX	100Mbps	UTP cable (category 5)	100m
1000BASE-T	1000Mbps	UTP cable (category 5)	100m

T002.eps

Electric Ethernet cables are coaxial cables and UTP (Unshielded Twisted Pair) cables. Connection diagram of cables is called “cable topology” or simply “topology.” Following figure shows typical topologies. Coaxial cables have branching points using a coupler (10BASE-5) or a T-connector (10BASE-2) to go to hosts and other network devices. This is “bus topology” and is used in connecting buildings and/or floors because of its reliability and noise immunity. A UTP cable connects a host to a concentrating network device, called “hub” for multiple connecting ports, points to connect UTP cables. This is “star topology” with hubs at the centers and is used in a small network on a floor because of simple and quick installation. A hub repeats (or re-transmits) signal coming to a port to other ports. Latest hubs can detect if the host interface is 10BASE-T or 100BASE-TX, and adapt its speed automatically to allow host interfaces of both speeds in the same Ethernet. When the network has more hosts than the number of ports of a hub, you can cascade hubs as shown below. Since an electric signal is delayed when it goes through a hub, number of hubs between any two hosts must not exceed four.



Topologies

A DAQSTATION has one 10BASE-T port, which is physically a modular RJ45 connector for eight wires. An RJ45 cable is similar to RJ11 telephone connector but is a little larger than it. Eight wires are used as four twisted pairs of signal and ground; two pairs for transmission and reception, the others for collision detection explained in the next subsection. There are two cable assemblies in the market. One is a “straight cable” (or sometimes, “patch cable”) where same wire is connected to the same pin of connectors at the both end of the cable. The other is “cross cable” where transmission and reception pins are exchanged. The latter is used to connect computers directly for some purposes. It would cause a wrong-cable problem if you store straight and cross cables in the same place. It is recommended to use only straight cables. Some hubs have “cascade port” to cascade them to another hub with cross cables. Such port are indicated with “X” symbol. Avoid using these ports to eliminate cross cables, and use pots indicated with “II” symbol for straight cable.

“Category” of UTP cables specifies characteristics of the cable. 100BASE-TX interface requires category-5 cable, while 10BASE-T interface can use both category-3 and category-5 cables. Cable specification of category and straight/cross should be indicated as well as cable length on the package when you purchase it.

Media Access Control

When a host transmits an electric signal to a coaxial cable (in case of 10BASE-2 or 10BASE-5), the signal goes along the cable and reaches to every hosts connected to the cable. In case of UTP cable Ethernet, hub repeats a signal from one port to others so that every host receives the same signal. It must be prohibited for two or more hosts transmit signal at the same time otherwise electric signals are superposed making it impossible to retrieve individual signal or data at receiving hosts. A network must have a mechanism to avoid this multiple transmission, called “Media Access Control (MAC).”

There are different MAC mechanisms. Following table shows some examples.

Examples of Media Access Control

Method	Explanation
Collision Detection (Ethernet)	A device transmits signal at any time. There is a mechanism to detect multiple transmissions (called “collision”) and stop transmission. Signals are re-transmitted after different time intervals.
Token Rotation	A device transmits signal when it has a right (called “token”) to do so. When it finishes transmission, it transfers token to the next device so that every device on the network has a chance to send signal.
Master/Slave	A directing device (called “Master”) has a role to control medium access. It sends instruction to one of other devices (called “Slave”) so that the slave transmits only one train of signal.

T003.eps

Ethernet deploys one of collision detection methods, Carrier Sense Multiple Access/Collision Detection (CSMA/CD) technology. In case of coaxial cable, a device applies DC voltage to the wire additively when transmitting signal so that this voltage is doubled when two devices transmit signal simultaneously. In case of UTP cable, hub can detect collision when it receives signal from two ports at the same time. In either case, a device observes the cable before transmission to know if there is a signal. If there is, it waits until signal disappears and starts transmission. When two devices are waiting, there is a chance of collision. Transmitting devices stop transmission when they detect or are notified collision and start re-transmission after a different time intervals to minimize the risk of another collision.

CSMA/CD technology gives a good throughput when signal is rare on the wire. When signal exists more than 30% of the time, throughput becomes worse because of increased chance of collision. To avoid this problem in a network of many devices, it is common to divide the whole network into multiple “collision domains,” which is a spread of network a signal is repeated. A “switch” is a device sharing the same position of hub in the topology and isolates collision domain. A switch does not repeat signals directly but stores them as data within it and transmits them one by one only to the port where receiver of the signal exists by referencing MAC address (see next subsection). This prevents collision over a switch. This type of switch is often called Layer-2 switch.

MAC Address

Data transfer needs information on the “sender” and the “receiver” of the data. A device gets data only when it is receiver of the data so that it can ignore other signals for effective communication. It also identifies the sender of the data so that it can maintain communication with a partner or reject requests from unwanted sender.

On Ethernet, such information on sender and receiver is six-bytes long “MAC address.” Each Ethernet port has its MAC address assigned to the hardware, which is unique in the world. Note that a MAC address does not belong to the device but the port hardware. A device can be identified with two or more MAC addresses if it has multiple ports. MAC address bound to a device changes when you replace its Ethernet Interface card.

A MAC address has two fields; first three bytes are assigned to a hardware manufacturer, while the manufacturer assigns the others before the hardware is shipped. This rule guarantees there is no duplicated MAC address in the world. For example DAQSTATION has a MAC address starting 00.00.64 in a hexadecimal expression (show a byte with a pair of 0~9 or A~F, with period between bytes). Yokogawa is responsible to give unique MAC address 00.00.64.XX.XX.XX to a DAQSTATION, where XX.XX.XX is unique to that DAQSTATION. Other examples are 08.00.5A for IBM and 40.00.AA for Xerox.

Following figure shows the structure of data (called “frame”) transferred over Ethernet. MAC addresses are shown near the head of the frame so that recognition becomes easy and quick. Numbers in parenthesis show the size of each data field in byte (8 bits) unit. When user data is bigger than 1500 bytes, it is divided into small portions to be fit into an Ethernet frame and then re-constructed by the receiver.

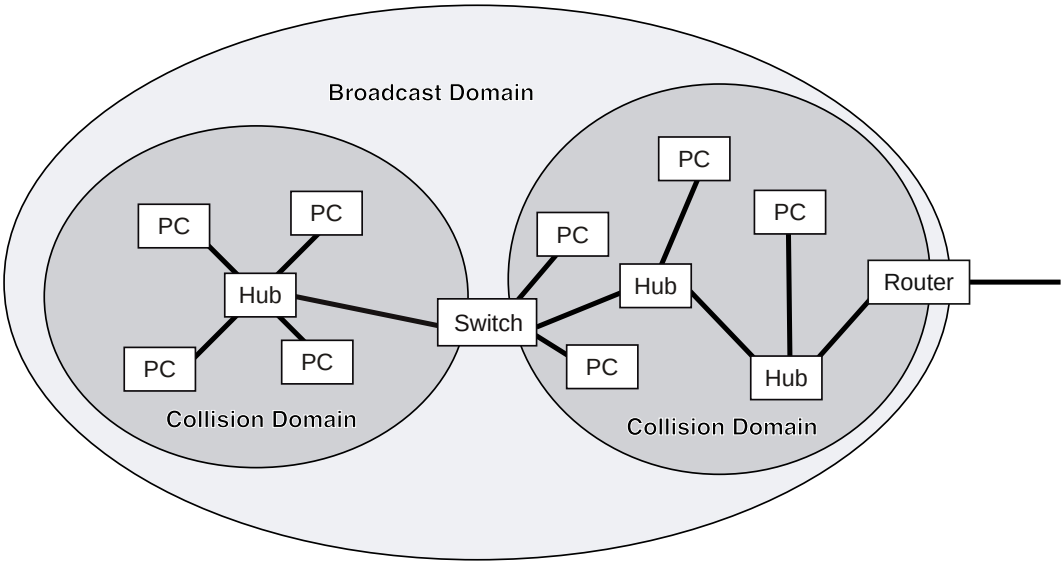
Preamble (8)	Receiver’s MAC Address (6)	Sender’s MAC Address (6)	Frame Type (2)	User Data (46~1500)	Frame Check Sequence (4)

T004.eps

Ethernet Frame Structure

Existing hardware has an Ethernet chip, which filters received frame without help of CPU for high throughput. It transfers received frame to the memory and notifies this to the CPU when Receiver’s MAC address is its MAC address or broadcast (sent to all hardware). It discards other frames to prevent unnecessary interrupt to the CPU.

A broadcast frame goes to all devices in the “broadcast domain.” Since hubs simply repeat frames, collision domain is same to broadcast domain if it does not contain any switch. Since a switch transmits a broadcast frame received at a port to other ports, broadcast domain is bigger than collision domain if it contains a switch. See following figure.



Collision Domain and Broadcast Domain

2.3 TCP/IP Protocol Suite

DAQSTATION deploys TCP/IP communication protocol used in Internet. It consists of several important protocols and therefore is often called TCP/IP "protocol suite". Internet Protocol (IP) delivers data units to receivers. Transfer Control Protocol (TCP) provides error-free data transmission between hosts by using IP delivery services. User Datagram Protocol (UDP) is similar to TCP but provide simpler transmission mechanism and facility to send data to many hosts. This section explains TCP/IP protocol suite.

Communication Technology in Military Activities

TCP/IP has a history related to military activities. Actually it was developed as a part of ARPANET project explained before. ARPANET has layered protocol architecture (explained at the end of this section) and a reliable message delivery facility over less reliable network. The latter was necessary because cables or a relay station could be destroyed by an attack. TCP/IP was developed to maximize the reliability of message delivery even under such environment.

TCP/IP is specified independent form transmission line or media. This made TCP/IP goes over not only Ethernet but also telephone line, optical fiber, microware, undersea cable, satellite channel and more. This extended the horizon of global network.

TCP/IP history tells another epoch related to military in 1990-1991. Commander Norman Schwarzkopf reported to US House after the Gulf War that TCP/IP was the only communication that survived against the Iraqi efforts to disrupt communication. He once expressed a concern of developing such an important technology by non-military society but later became understood that TCP/IP would not be such good without Internet community.

Internet Protocol

Internet Protocol (IP) delivers data to the correct receiver even beyond Ethernet. Every device in IP network has an "IP Address" of four bytes length (new IPv6 will be discussed in the next section). A device with IP address is often called a "node." IP delivers a data packet to the node of destination (receiving) IP address. This may sound similar to MAC address. MAC address is usable only on an Ethernet network, while IP address can be used beyond Ethernet and goes over various media. Another difference is, IP address is a logical address, therefore it can be assigned by configuration and stay unchanged even when you replace Ethernet interface card.

IP packs an amount of data with additional information for the protocol including IP addressed of sender and receiver into an "IP packet" after dividing original data into relatively small segments. The maximum data size can be large when the quality of data transmission is good between nodes. It should be small if IP packet goes over the unreliable transmission medium to minimize the penalty of lost packets.

The route to deliver IP packet from the sender to the receiver can be redundant by selecting the actual delivery route at "routers." A router has multiple ports and relays IP packet to an appropriate node or router. It has two "routing" algorithms. One is "static routing" where routing is predetermined by configuration. The other is "dynamic routing" where routers exchange information of network availability to determine the most reliable route using Routing Information Protocol (RIP) or its enhancement. (RIP-II) When a transmission line or a router fails, other routers try to avoid sending IP packet to it and use another possible route to the destination. When such re-routing takes place frequently, there is a chance an IP packet is routed back and forth in the network. Such "stray" IP packets are erased from the network when they go through routers by predefined times (called "hops") to avoid they fill up the network.

In connecting headquarters and branch offices by dedicated lines, routers take static routing algorithm for better throughput and easier trouble-shooting. A router has a "routing table" to decide which packet should be forwarded to where for static routing. Routing does not take place when an IP packet goes only through hubs and switches of an Ethernet. A router isolates broadcast domain as well as collision domain.

Here is a question. Before a node sends an Ethernet frame, it has to know the MAC address of receiver to build the frame. How can it get it when IP address is given by an application? There is a mechanism to do that using Address Resolution Protocol (ARP). The sender broadcasts another frame to all nodes on the Ethernet telling he wants to know the MAC address of the hardware of "this IP address." All nodes compare that IP address with its own IP address.

When and only when a node finds they are same, it sends back the answer to the requester, whose MAC address is shown in the broadcast frame. When the requester receives the answer, the MAC address he wanted to know is shown there and he is able to send the frame given by the application. IP memorizes this relationship (pair of MAC address and IP address) for a certain period of time so that it does not have to repeat this resolution process when another frame is given. When the host of destination IP address is outside the Ethernet broadcast domain (e.g., beyond a router), the router responds to ARP request and forwards IP packet according to the routing information. Therefore, many IP addresses can be related to MAC address of the router because the router seems to have many IP addresses in IP level.

TCP provides reliable data transfer

IP delivers IP packets as discussed above. It implies the chance of lost packet or delivery of packets in a wrong order after routing over an unreliable network. A mechanism to recover lost or unordered packets is necessary for reliable communication. Transfer Control Protocol (TCP) is used for this purpose.

TCP is a one-to-one communication between nodes and requests IP to send a “TCP frame” to its destination. Before starting data exchange, TCP pair on both nodes establishes mutual “connection” to share the information of reliable data transfer. Every TCP frame is accompanied with a “sequence number” of the connection to identify its position in the data transfer flow. When a loss or disorder takes place, discontinued sequence number indicates it and TCP requests to re-transmit the necessary TCP frame for recovery. This mechanism provides a very reliable data transfer over unreliable transmission line or route.

Since a host has many applications that communicate to other applications on other hosts, TCP carries another information on which application the data should go to. A sixteen-bit number called “port number” is used for this purpose. It is a kind of local address within a host. When a host application wants to use the function of anther host, it needs the port number of that application. For that purpose, “well known” port numbers are defined for typical applications in the range between 0 and 1023. Following table shows examples.

Example of well-known ports

Port Number	Application	Port Number	Application	Port Number	Application
20	ftp (data)	23	telnet	53	DNS
21	ftp (control)	25	SMTP	80	WWW http

T005.eps

A TCP connection is identified with a pair of port numbers and IP addresses of both hosts. This enables an application can handle multiple requests from various applications at a time because the port number and IP address identify the requester. When a TCP needs to establish a connection to one of these applications, it sends connection request to that port with requesting port number larger than 1024 avoiding duplication within the host.

When an application wants to send data to multiple applications at a time, another protocol, User Datagram Protocol (UDP), is used instead of TCP. Since UDP does not maintain connection, e.g., sequence numbers, its processing time is shorter than TCP and it is good for applications that need fast throughput. One drawback is, it does not guarantee reliable data delivery. Usually user does not worry about selecting TCP or UDP because each application does it by weighing their advantages and disadvantages.

ISO Open System Interconnection Model

We have discussed Ethernet, IP and TCP, which provide different “level” of communication. Their role can be well summarized by referring Open System Interconnection (OSI) model proposed by International Standards Organization (ISO). The OSI model is an approach to study the method in designing a network-based system using various devices from different vendors (often referred as “multi-vendor system”). Though its original intention was to provide a guideline of software implementation of communication for an open system, it is used for theoretical study of interoperability rather than the real implementation. It is therefore often called OSI reference model.

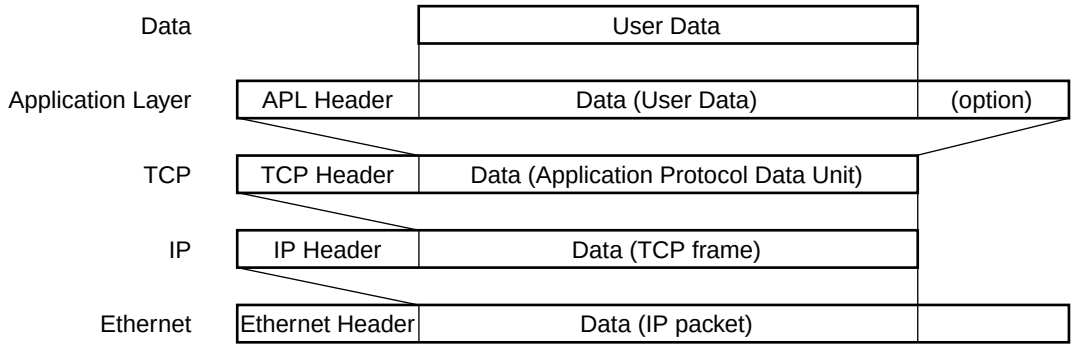
OSI model defines seven “layers” of different level of communication. A layer uses the functions provided by the next lower (of smaller level number) layer to perform higher-level functions. Following table shows the functions of layers and examples in Internet.

OSI reference model and examples

No	Layer	Functionality	Examples
7	Application Layer	Provide software interface to application software	ftp, SMTP
6	Presentation Layer	Defines common data structure among devices	
5	Session Layer	Controls order of send/receive data	
4	Transport Layer	Provide data transfer facility of high quality	TCP, UDP
3	Network Layer	Delivers data through routes	IP, ARP, RIP
2	Data Link Layer	Controls medium access and detects transmission error	Ethernet
1	Physical Layer	Transmits data as a signal onto medium and retrieves data from received signal	10BASE-T

T006.eps

In our case of communication over Ethernet, Ethernet serves as Data Link layer and Physical Layer. IP and TCP serve as Network Layer and Transport Layer, respectively. A lower layer handles higher-layer frame as its data. See following figure.



Wrapping of higher layer data

2.4 IP Address

This section discusses IP address a little further. All nodes in a network (not restricted to Ethernet) have at least one IP address.

IP Address in IPv4 Technology

IP common in TCP/IP networks is “version 4” of IP protocol (IPv4) using IP address of 32 bits (4 bytes) length. Though IP address is specified as bit string, it is often expressed in hexadecimal expression of bytes for better visibility. For example, IP address in bit string `11000000.10101000.00000000.00000001` is expressed as `192.168.0.1`. Number of available IP addresses in IPv4 is more than four billion (4,294,967,296).

Your home address is a combination of building/block number and town/street name, *1020 Cedar Street* as an example. IP address should have a similar structure of two parts, one to identify host and the other to identify network. Higher part of IP address is dedicated to identify network (network address) and lower part identifies the host (host address). There are five “classes” of IP addresses shown in the table below, each of which has boundary of network and host addresses at different places. Since each class use different IP address range, reading bit string from the beginning can recognize the class. In real networks, IP addresses in classes A thru C are used. Class A, B and C addresses are designed for large, medium- and small-scale networks respectively.

IP Address Classes

Class	Bits for network address	Number of identifiable networks	Bits for host address	Number of identifiable hosts	Range of IP addresses
A	8	126	24	16,777,214	1.0.0.0 to 126.255.255.255
B	16	16,384	16	65,536	128.0.0.0 to 191.255.255.255
C	24	2,097,152	8	254	192.0.0.0 to 223.255.255.255
C	0	0	32	268,400,000	224.0.0.0 to 236.255.255.255
E	Reserved for future use				Other than above

T007.eps

Some parts of IP address range are used for special purposes. IP address 0.0.0.0 means the host itself (this host). IP address of network address of all zeros means the network where the host is connected (this network). IP address of host address of all ones means the broadcast expecting all hosts in this network receive it. IP address of 127 in the first byte is used for testing the network.

Subnet mask was introduced to separate network address from an IP address. It is a 32-bit number with ones in network address part and zeros in host address part. Making a logical AND of IP address and subnet mask, you will get the network address. Making a logical AND of IP address and inverse of subnet address, you will get host address. Following figure shows an example of IP address `192.168.2.12` and subnet mask `255.255.255.0`.

```
                IP Address:  11000000.10101000.00000010.00001100  = 192.168.2.12
               Subnet Mask:  11111111.11111111.11111111.00000000  = 255.255.255.0
Inversed subnet mask:        00000000.00000000.00000000.11111111
            Network Address = 11000000.10101000.00000010.00000000  = 192.168.2.0
               Host Address = 00000000.00000000.00000000.00001100  = 0.0.0.12
```

T008.eps

Calculation of network address and host address using subnet mask

Following table shows subnet mask of IP address classes.

Subnet masks

Class	Subnet mask	
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.255.0
C	11111111.11111111.11111111.00000000	255.255.255.0

T009.eps

Subnet mask is often expressed in number of ones combined with IP address. For example, class-C subnet mask is expressed as /24 instead of 11111111.11111111.111111111.00000000 for simplicity. A class-C private network is expressed as 192.168.2.0/24, which means network address is 192.168.2.0 and host address range is between 192.168.2.1 to 192.168.2.254.

There is an approach to use subnet mask other than above for special purposes discussed later.

Global and Private Addresses

Since a host on Internet is identified by its IP address, it must be unique in the global Internet. Organizations got their unique network addresses and were responsible to give unique host addresses. For example, Yokogawa got class-B network addresses of 133.140.0.0/16. These IP addresses are unique in the global Internet and called “global addresses.” Internet Assigned Numbers Authority (IANA) controls global addresses.

Some ranges in IP addresses are dedicated private networks, which are not explicitly visible in the Internet. They are called “private addresses.” Following table shows ranges of private addresses. Since these addresses do not exist on Internet but are visible only within the private network, the same private IP address can be used in many private networks. The idea of private address has another advantage that same configuration including IP address can be duplicated to many private networks for simple and systematic network designing. We will see how it works in the next chapter (tomorrow).

Private IP addresses

Class	Number of Networks	Network Address	Range of IP address
A	1	10.0.0.0	10.0.0.0 to 10.255.255.255
B	16	172.16.0.0 to 172.31.0.0	172.16.0.0 to 172.31.255.255
C	256	192.168.0.0 to 192.168.255.0	192.168.0.0 to 192.168.255.255

T010.eps

Routing a Private Address

When IPv4 technology was developed, nobody wondered if four billion IP address is not many enough. However, the concern of IP address shortage is coming to reality as Internet using TCP/IP becomes more and more popular. In case of Yokogawa, 65,536 host addresses are not many enough to cover PCs, workstations and other nodes within the company and Yokogawa switched its intranet to class-A private addresses.

Now here is a question. Suppose you are looking at a PC in Yokogawa intranet of 10.0.233.193. How can you browse a web page on Internet and receive its content from the web server? The answer is, the router connecting the private network to Internet takes care. The router has global IP address(s) on the port to Internet while it has another private IP address on the port(s) to the private network. When your PC sends a request to a web page on Internet, the router answers to address resolution protocol (RIP) and receives the request on behalf of the web server. It then forwards this request to Internet with one of its own global IP addresses (say `133.140.80.100`) and memorizes this action. When the page contents come back to `133.140.80.100` (e.g., router), it forwards to `10.0.233.193` in the private network by recalling the last action. This is a lease of IP address to the private host and called Network Address Translation (NAT) technology.

Another technology, IP masquerade, is useful for private networks where number of hosts going to Internet is much more than that of global IP address of the router. In this technology, the router leases same global IP address to multiple hosts by giving different TCP port number. When contents come back from the web server to the router, it uses destination TCP port number to know to which host the contents should go.

Automatic IP Address Assignment through DHCP

Even within a private network, IP address must be unique. If you give IP address to hosts manually, there is a chance of mistake to give the same IP address to two hosts. The more hosts you have in the network, the more risk of address duplication becomes. It is much better and safer to do it automatically using Dynamic Host Configuration Protocol (DHCP). You have this in TCP/IP property discussed in section 1.3, where is an option to “Obtain an IP address automatically.”

With DHCP, your PC obtains its IP address from DHCP server (IP address manager) every time it joins the network. IP address may change each time (DHCP gives the same IP address if your PC comes back to the network within a short time after it left network. This time interval is configurable in DHCP server). If your PC is a server to which other hosts may want to have access, it is not a good idea to change IP address so frequently. DAQSTATION require a “fixed’ IP address for this reason. When you configure a DHCP server, be careful to make ranges of DHCP address and fixed address do not overlap.

For more Nodes

An intermediate idea to have more nodes was proposed to use “fragment” subnet mask. Suppose you have a class-C network and want to have more than 256 nodes. You could do that by decreasing the number of networks by using subnet mask of `255.255.254.0` (`11111111.11111111.11111110.00000000`), where number of host can be up to 511, as an example is `192.168.0.0/23`. This should be avoided unless it is absolutely necessary because the IP management becomes more complicated.

Toward the IPv6

The final solution to IP address shortage is IPv6 (IP version 6) or IPng (IP next generation) developed by The Internet Engineering Task Force (IETF) as RFC2460. IPv6 deploys IP address of 128 bits length resulting possible 3.4×10^{38} IP addresses. This sounds as infinite at least in next decades. This technology is being adopted in the Internet communities. DAQSTATION supports IPv4 today and this needs to be reconsidered when IPv6 becomes popular.

2.5 Important Network Devices

You have already seen many network devices. Following table summarizes them with some additions. Devices with asterisk (*) are explained in this chapter. The table describes only basic definitions regardless the fact that latest hubs have some functionality of switches, and latest switches have some functionality of routers.

Important Network Devices

Device	Explanation	Domain	
Network Interface Card (NIC)*	Hardware to connect your PC to the network	Collision Domain	Broadcast Domain
Hub*	Device to transmit signal from a port to other ports		
Repeater	A hub with only two ports to extend cable length		
Switch*	Device to relay Ethernet frame to the port where the destination is		
Bridge	A switch with only two port to isolate collision domains		
Router*	Device to relay IP packet from a network to another network.		
Dialup router*	A router with telephone line to call destination when necessary		
Firewall	A device to protect network hosts and information from outside		

T011.eps

2.6 Host Name Management

IP address is so powerful to identify hosts but it is not so good for humans to memorize because it is just a series of numbers. This would be more serious when we migrate to IPv6. It is much better to call a host with name that means something to you. Host name must be unique by the same reason for IP address.

Identifying a Host on the Network

Since Internet is an assembly of many networks, you need to specify not only host name but also network name (called “domain”). For example, you can specify Yokogawa web server as www.yokogawa.com. Your request is parsed from the tail; (1) interpret “com” as a commercial organization, (2) finds Yokogawa as a registered commercial organization to reach Yokogawa domain (yokogawa.com). Then your request goes to the host registered as the web server.

You have used ping to test if you can reach the host of assigned IP address in section 1.5 (yesterday). If you have a PC connected to Internet, try following command to reach a host with host name. Your result may be different from this depending on your Internet connection. This will translate famous host names into IP addresses. Notes some servers do not respond to ping by security reasons.

```
Microsoft Windows 2000 [Version 5.00.2195]
(c) Copyright 1985-1999 Microsoft Corp.

C:\> ping www.ieee.org

Pinging www.ieee.org [140.98.193.38] with 32 bytes of data:

Reply from 140.98.193.38: byte=32 time=271ms TTL=52
Reply from 140.98.193.38: byte=32 time=240ms TTL=52
Reply from 140.98.193.38: byte=32 time=241ms TTL=52
Reply from 140.98.193.38: byte=32 time=240ms TTL=52

Ping statistics for 140.98.193.38:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
   Minimum = 240ms, Maximum = 271ms, Average = 248ms

C:\>
```

Section 1.3 (yesterday) of this document explains the method to give a host name to your PC. A host name is a combination of alphanumeric characters and hyphen plus underscore. Use alphabet for the first character of a host name.

DNS: Domain Name System

How does your PC know the IP address of a host given as a host name? The easiest solution is to have a translation table in your PC. Search a file, hosts, in your PC to open it with Notepad. Following is an example. It is a table to relate IP addresses to host names as used in the past. You will find it empty because it is there only for backward compatibility. It is very hard, if not impossible, to have every host names listed in this table. You may recognize this approach is not useful for hosts assigned IP address through DHCP.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

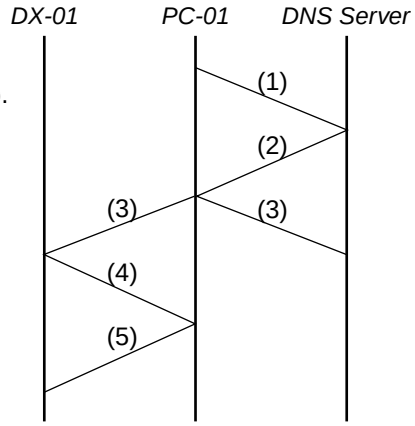
Domain Name System (DNS) resolves host name into IP address over the network. A computer called "domain name server" or simple "name server" keeps information on host name and IP address. There is a hierarchy of name servers distributed in Internet. When you ask for IP address of a host to the name server on your network, it returns IP address if the host exist on the same network. If it does not, the request goes up and down the hierarchy by analyzing domain name from the tail to retrieve correct information. If name servers are unable to resolve host name, it will return the answer "Unknown host." Go back to ping with host name experiment and try to ping to `daqstation.yokogawa.com`, which should fail.

DHCP gives not only IP address of your PC but also IP address of your name server. If you have a professional operating system, input "`ipconfig -all`" to the command prompt to see network configuration information. If you have a personal operating system, use "`winipcfg -all`" for the same purpose. You will see "DNS Server" entry showing IP address of your name server. If you have a personal operating system, click "Start" then "Run" and then "Run a program." Type "WINIPCFG" and click "OK" to open IP configuration window. Highlight network interface card, and click "Detail>>" to see IP addresses of DHCP and DNS servers. It is common to have redundant (two) name servers so that you can enjoy DNS service even when one server failed.

Address Resolution

Here is a review of address resolution processes. Suppose your PC (host name = *PC-01*, IP address = `192.168.0.64`, MAC address = `08.00.5A.2A.10.CD`) is going to send a request to DAQSTATION (host name = *DX-01*, IP address = `192.168.0.71`, MAC address = `00.00.64.00.B2.14`) using name server (IP address `192.168.0.254`). Address resolution flow is like this (assuming PC-01 already knows MAC address of name server):

(1) *PC-01* at (`192.168.0.64`) sends a name resolution request for *DX-01* to DNS server at (`192.168.0.245`).
(2) DNS server returns IP address (`192.168.0.71`) to *PC-01* at (`192.168.0.64`).
(3) *PC-01* broadcasts an ARP request of *DX-01* for (`192.168.0.71`) to all nodes at (`192.168.0.255`).
(4) *DX-01* at (`00.00.64.00.B2.14: 192.168.0.71`) sends reply for the ARP request to (`08.00.5A.2A.10.CD: 192.168.0.64`)
(5) *PC-01* at (`192.168.0.64`) sends an application request to *DX-01* at (`00.00.64.00.B2.14: 192.168.0.71`).



Flow of Address Resolution

It would be a waste of network traffic if this resolution took place for every transfer request from applications. Instead, TCP/IP protocol software has a cash table to keep relation of host name, IP address and MAC address so that only step (5) repeats after the resolution process. If you have a professional operating system, type `ipconfig -displaydns` at command prompt you tested ping. It would show all current entries for host name and IP address.

2.7 Wireless LAN

This section is prepared for those who need wireless connection in some part of your Ethernet network. Only radio medium is discussed though infrared light is an alternative. Network devices for wireless LAN have IP address and MAC addresses, and therefore undistinguishable from application point of view.

Regional Regulation of Radio Bands

Regional (or national) government strictly controls radio band for communication. In general, you need to get license from the government before you install a radio station. It would need certain weeks, if not in months, and paper works. Some bands are assigned to avoid this complexity so that you can use radio instruments in these bands without license. Since regulation varies from region to region, keep in mind a radio instrument purchased in a region may not be allowed for use in another region.

IEEE802.11b Wireless LAN

Institute of Electrical and Electronic Engineering (IEEE) standardized wireless LAN (IEEE802.11) as well as Ethernet (IEEE802.3). Popular medium is 2.4GHz “industrial scientific medical” band specified as IEEE802.11b. An American organization, Wireless Ethernet Compatibility Alliance (WECA), promotes this technology by testing compatibility and interoperability of devices to call passed devices “Wireless Fidelity (Wi-Fi).” Other bands are also standardized. They are IEEE802.11a using 5GHz band and IEEE802.11g for higher communication.

IEEE802.11b uses radio of power less than 10mW and frequency between 2.4GHz and 2.4835GHz for which license is not necessary. Since a microwave oven and some other instruments uses the same band, it is necessary to avoid IEEE802.11b network coexist with those instruments. This band was divided into “channels.” Number of channels is 11 in US and Canada, 13 in Europe and 14 in Japan. Because some channels are overlapped and may interfere to each other, you should avoid using those channels at the same time and place.

IEEE802.11b has 11Mbps transmission rate in its peak. It also allows slower transmission of 5.5Mbps, 2Mbps or 1Mbps where radio field is not strong enough to achieve 11Mbps.

Network Architecture and Antennae

Nodes of wireless LAN are classified into “access points” and “stations.” An access point is similar to hub and converts electric signals and radio signals. Once installed in a fixed place and properly configured, an access point continues to transmit radio signal and waits for stations to join the network. A station is similar to nodes and can be fixed in a place or mobile within the range of access point. It can join network when it receives signal from the access point.

There are two networking mode for wireless LAN. One is “infrastructure” mode and the other is “ad hoc” mode. Access point is the key component of infrastructure mode. Any station can join the network through the most convenient access point to form a flexible network. It is also applicable to connect two Ethernet domains with radio signal. One of important applications is connection of networks installed in different buildings without cable installed between them. Ad hoc mode is for smaller networks where stations communicate each other promiscuously. DAQSTATION network should use infrastructure mode.

Distance from a station to the access point can be up to 100m as long as the station is directly visible through the air from the access point. It is the limit of small dipole antennae of poor directivity installed in access point or radio interface card. If you want to extend the distance or transmit through window glasses, more directional antennae are necessary. Some vendors provide planer antenna or Yagi antenna for longer transmission. Consult such vendor if necessary.

Secure Communication over wireless LAN

Radio wave has a risk of leakage to undesired area where somebody could listen to the communication or even hack into the network. IEEE802.11b has mechanisms to protect your network.

IEEE802.11b uses spread spectrum (SS) or more precisely, Direct Sequence Spread Spectrum (DSSS) technology with wide-band frequency for noise-resistive secure communication. A keyword called SSID (Service Set Identifier) or ESSID (Extended SSID) is used in modulating SS signal. Some person may insist this is a mechanism to secure wireless LAN but unfortunately it is wrong. Some wireless LAN interface card accepts “ANY” as SSID. Windows-XP injected another concern by introducing “automatic SSID detection” for easy configuration. These make it possible to connect a PC to an operating wireless LAN without knowing the SSID.

Encryption using Wired Equivalent Privacy (WEP) technology is necessary to protect your wireless LAN from a wire-tapper or destructive hackers. WEP encrypts data with 40- or 128- bit shared key. This is rather safe and secure. Once an outsider finds shared key, however, your network is not secure any more. Shared key must be kept confidential.

Pros and Cons

Here is a short summary of pros and cons of wireless LAN. It should be useful when you consider a wireless LAN by weighting each item.

Pros and Cons of wireless LAN

Pros	Cons
No cable or cabling space	Limited reach of low-power radio signal
LAN can be built very quickly	Can tap very easily
Flexible node installation. Mobile network is possible	Concrete or metal wall prevents radio penetration
Can connect buildings or outdoor nodes	Transmission is affected by weather

T012.eps

2.8 Application Layer Protocols

This section gives an overview of application layer protocols common and important for DAQSTATION networking.

Client/Server model

Application protocols in this section are all based on Client/Server model, where client and server are applications software running in hosts. When a “client” application needs service of a “server,” client sends a service request to the server and the server returns the result of the service to client. The role of client or server is not an attribute of host itself but depends on the functionality (program code) of the software. Your PC can work as ftp server while it contains clients for email and web browsing. It is not a good idea to run many server functions on a not-so-powerful hardware because it would slow down the overall throughput of the system.

Telnet

Telnet is a simple protocol to exchange text strings between client and server. It has been used with a classic Teletype and its simulations are developed as “terminal emulator” software. A popular one is “Hyper Terminal” bundled to Windows operating system. Other sharewares are available.

Hyper Text Transfer Protocol (http)

Another text-based protocol is Hyper Test Transfer Protocol (http) to transfer web contents described in Hyper Text Markup Language (html). Http clients are called “browser.” Popular browsers are Internet Explorer and Netscape. Http servers are IIS (Internet Information Service) for Windows and Apache for Unix operating system. DAQSTATION has http server as a standard feature.

File Transfer Protocol (ftp)

File Transfer Protocol (ftp) is another important protocol to transfer files. Ftp transfers file in two modes. One is “text” mode to transfer text file, which solves the problem of different text delimiters between Windows and Unix. The other is Binary (or Image) mode to transfer binary file as it is. A binary data file must be transferred in this mode. Command prompt of Windows provides ftp client functionality. More convenient clients like winsock are available. A web browser can be used as an ftp client to download files from a server. DAQSTATION is equipped with ftp server and client. It uses ftp client function for automatic file transfer.

Simple Mail Transfer Protocol (SMTP)

SMTP (Simple Mail Transfer Protocol) is used in sending an email as a text. A client called “mailer” in your PC calls SMTP server, when it wants to send an email, to send texts for attention, sender, subject and email body and receive acknowledge to each part. The server forwards this email to another SMTP server that knows where it should go. Your mailer encodes attached binary file into text before transmission and the receiving mailer decodes it. There are several decoding methods; base64 is an examples.

Your mailer uses another protocol to retrieve received emails from mail server (or post office). Most mailers are able to handle two common protocols, POP3 (Post Office Protocol) and IMAP (Internet Message Access Protocol). SMTP server and POP3/IMAP server can sit in different hosts of different names.

DAQSTATION is equipped with SMTP client to send emails when necessary but it has no POP3/IMAP client.

Day 3: Day Three: Building your Network

The third day is a “designing day.” You will plan your own DAQSTATION network since you already got necessary experience and knowledge. You will find a procedure and guidelines to build a communication network in a professional way and make DAQSTATION and PCs ready to serve your business. Standard configuration tables are provided to simplify the design effort so that you have only to pick up the appropriate one to bring the system operational quickly.

Here is an **important advice**: Consult network/system administrators of your company or organization from the early stage of planning and work with them, if you want to maximize the benefits of DAQSTATION with the help of internal network of your company or organization (intranet). It should be much easier to utilize existing ftp server and mail server than to install them by yourself. Network backbone allows you to read DAQSTATION data at your office. You would not be able to enjoy them without permission and assistance of administrators. You should also be careful and sensitive to network security and throughput, especially protecting network from viruses, hackers and cyber terrorism, for which administrators are working everyday. Cooperation with them is the key to success. Refer “DAQSTATION networking white paper” to understand what DAQSTATION does and is equipped with from network management point of view.

3.1 Your DAQSTATION network

Study purposes and environments in which you are going to have DAQSTATION network. Imagine how it will evolve in the future expecting your business growth. That will help you in deciding what network domain you are going to build. Chances are:

1. Isolated DAQSTATION network,
2. DAQSTATION on your Intranet,
3. DAQSTATION network over WAN, and
4. DAQSTATION network over Internet.

As discussed below, you have two options: Choose 2 to work with intranet administrators, or develop your own network from 1 to 3 or 4 by yourself. It will be difficult to go to domain 2 after you chose one of the others. Discuss pros and cons with your administrator.

Isolated DAQSTATION Network

Your DAQSTATION network is a small isolated domain consisting of recorders, PCs and some peripherals such as a printer. You need to bring data stored in a disk or memory card if you want to manipulate data with computers located in other places. Email service is not available in this domain. Standard network configuration at the end of this chapter suggests sending emails through cellar phone connection to a mail server provided by a carrier or an Internet Provider.

This domain may sound very simple and suitable to your small network. Once you built this network, however, it is very difficult to connect it to your intranet when you become to want intranet services. It would cause many technical conflicts and inject security concerns. So if you have a plan or even hope to use intranet services in the future, select intranet domain discussed below.

If this domain is located at a remote site and you want to receive email when needed, consider it as a remote site connected over Internet. It may need remote access service.

DAQSTATION on your Intranet

DAQSTATION network is a segment of your intranet. You can enjoy functions provided by existing servers and backbone.

Professional administrators manage your intranet. Consult them and follow the management policy, their instructions and suggestions. If you do not want DAQSTATION network and intranet interfere traffic each other (heavy communication increases the chance of collision and decreases throughput), install switch between them so that they become independent collision domains.

DAQSTATION network over WAN

If DAQSTATION is installed at a remote site from your office (no Ethernet connection between) from which you want to have an access to it at your office, network needs to go over WAN. Ask your system/network administrator if there is an intranet connection using dedicated or public line, or VPN (Virtual Private Network). If not, ask them to install one for your business. Start this quickly because it would take weeks or months.

If this installation is temporary for demonstration, experiment or trial, you may consider connection with cellar phone. It will also be viable if the site is too remote (deep in mountains) to have a telephone line.

If the number of remote sites is so many or the sites are so distant that the cost of telephone connection between sites and the office becomes a concern, you should seriously consider Internet.

DAQSTATION network over Internet

If DAQSTATION network is routed to Internet, it is truly global and you can collect data from recorders distributed in a very wide area. Each site needs an Internet access, e.g., contact with an Internet Provider.

On-demand (dial up) Internet connection is safe (and cheap in many cases) and good for DAQSTATION client functions to transfer data files to a server and/or send emails. If you want DAQSTATION server functions exposed to Internet, you need continuous Internet connection and a router configuration to expose DAQSTATION. You have to protect DAQSTATION and PC from potential evil invasions. Consult security expert. This section describes configuration only for client functions.

3.2 Network Installation Design

This section discusses network devices and cabling by estimating the size of DAQSTATION network and the number of necessary network components including cables. The approach in this section is not common in network experts but simpler and easier for those who have experiences in cabling and installing devices.

Estimate how big your Network will be

First step is to determine how big your DAQSTATION network is and will be. It is better to consider not only this installation plan but also future expansion plan so that your network would not be obsolete in a short period of time. Yokogawa representative would be more than happy to assist you in counting number of recorders and measurement points.

Estimate number of DAQSTATION recorders. It is ideal if you are able to estimate the number of measurement points and the period of measurement of each point. Prepare a table or spreadsheet as shown below to fill with your estimation. If you have a difficulty to predict the detailed future plan, just estimate the number of measurement points and period.

Calculate number of point per second to fill in the table. Fill with the number of points if the measurement is once each second. Double it if the measurement is in every half a second (500ms). Multiply by four if it is in every quarter second. Divide with two if it is in every two seconds, vice versa.

Make a table for each site if your network extends to multiple sites connected with WAN or Internet.

Network Size Estimation Table

	This installation Plan		Final Plan	
	# of devices	Measurement point/ Period	# of devices	Measurement point/ Period
DX102	A_1	M_1		
DX104	A_2	M_2		
:				
CX2016	A_n	M_n		
PC for applications	A_{n+1}	-		-
PC for management	A_{n+2}	-		-
Peripherals	A_{n+3}	-		-
TOTAL	$N = \sum A_n$	$L = \sum (A_n \times M_n)$		

T013.eps

Make a sum of number of devices (N). Multiply number of devices and measurement point/period and calculate the sum of them (L). The value L gives an estimation of measured data created in every second. If it becomes more than 10,000, you should be better to separate network into collision domains within which L-value is less than 10,000. Number of Application PCs depends on the total L-value.

Value of N gives the number of hosts in this network. You need IP addresses for them. Especially, DAQSTATION and server PCs need fixed IP addresses. You must ask for their allocation if your network will be a part of intranet.

Define DAQSTATION Network Domains

A network grows as large as you want by adding hosts and hubs. However if a large network is too homogeneous, network throughput becomes worse and the network is so difficult to manage. Hosts of applications interacting tightly should be near each other, while a server to which a client has less frequent access can stay in a distant place for easier management. The concept of “near” and “distant” does not mean physical distance but “network distance” defined by the amount of interactions. See collision domain and broadcast domain in section 2.2 of this document.

A collision domain has worse throughput, if the network load becomes 30% or more. A value of 10,000 measured points every second, discussed above, comes from this criterion. You need to divide it into multiple collision domains with a switch if the network load is such high. A cheap switch may not have a good throughput in forwarding frames, resulting communication over a switch slower. This is a “distance” in network.

Group your recorders and PCs into domains. DAQSTATION recorders and PC with low-level interaction (e.g., ftp server, DAQSTANDARD, DAQEXPLORER or DAQLOGGER) with them should sit in the same domain, while other clients and mail server can stay “distant.” One switch may be enough for many cases.

Locate Stations to draw a Cabling Diagram

Locate the places where DAQSTATION recorders and PCs (e.g., hosts) are installed. Make sure you have a space for future expansion. Select places for switches and hubs. Major criteria are (1) power is available, (2) there is very small risk of somebody to touch a switch/hub or cable connector intentionally or unintentionally, and (3) easy access to maintain the switch/hub. A host must be within 100m of cable length from hub. If a group of recorders and PCs is installed within a small distance, place a hub for the group so that you can minimize the overall cable length and chance of problems. Since a hub is very cheap today, it is much more important to reduce such risk than having less hubs.

If you are connecting this network to your intranet, decide the place of connection with the help of administrator. There must be an unused port of a switch or router. If not, ask for another switch.

If you are connecting this network to outside by telephone or cellar phone, locate a good place to install a dialup router. Make sure the radio field is strong enough at the place. Since a metal plate shields the field, put an antenna outside of a metal cabinet.

Now you have located all hosts, switch and hubs, you are able to draw a cabling diagram for connecting a host to a hub, between hubs, and hubs to switch. There must not be a “loop” of cables, which means a redundant path from one device to another. From this drawing, you can determine the length of each cable by considering installation height, cable rack and wire routing with an enough margin. It is easier to purchase cables from the shelf of a shop by determining their length according to the commercial practice (1m, 2m, 3m, 5m, 10m, etc.). You do not have to determine cable length for future expansion as far as it is less than 100m.

In determining cable length between hubs, it must not exceed 100m. If this is the case, repeat cable with another hub or wireless LAN. Make sure that number of hubs between any two hosts within the collision domain is equal or less than four. If this condition is not satisfied, redesign cabling scheme. Use another switch if needed.

Order and Install Devices including Cables

Count number of cables for each hub location. The hub must have ports equal or more than that. It is a good idea for having less stock that all hubs have same number of ports.

Reserve some ports for future expansion. It is ridiculous to reconfigure the network by unplugging existing cables when you add more devices. It should be achieved only by plugging new cables to add devices.

If you have many nodes concentrated in a small area and a hub does not have so many ports enough to concentrate all nodes, you may need cascading hubs to increase number of ports. You must count this again: the number of hubs between any nodes must not exceed four.

It is a good practice to give a tag (identifier) to devices for management. For recorders and PCs, it could be same to their host names. Give tags to hubs and switches to identify them, too. It is recommended to make a “wiring table” like below and attach tags or markers of “Cable Tag” identifying the cable at both ends of a cable. This will help you in maintaining the network and prevent unplugging a wrong cable.

An Example of Wiring Table

No.	Cable Tag	From: Hub/Switch Tag	To: Node/Hub Tag	Length (m)	Note
1	UTP100-01-5	HUB-001-P1	DX1001-01	5	10BASE-T
2	UTP100-01-10	HUB-001-P2	DX1002-01	10	10BASE-T
:					
30	UTP300-20-50	SW001-P3	HUB001-P16	50	100BASE-TX(category 5)

T014.eps

When you finished, make a list of necessary hubs, switches and cables to order them. Do not forget to order housings, cable ties and/or clamps, cable guides, ducts and/or conduits for device/ cable installation. Prepare instructions if you order installation to a third party.

An Example of Device List

No.	Quantity	Name	Specification	Vendor	Tags
1	1	Switch	8 ports 10/100 Mbps	C	SW001
2	3	Hub	8 ports, 10/100 Mbps	C	HUB-001, HUB-002, HUB-003
:					
40	12	UTP Cable	Straight, Category 5, 5m	X	UTP100-01-5, ...

T015.eps

You do not have to order devices for future expansion at this time. Make sure they are available by the scheduled day you install them. It is recommended to attach a plate indicating its tag to the device before installation.

3.3 Managing IP Addresses

This section gives an idea for managing IP addresses. DAQSTATION recorders need fixed IP address. It is necessary to give fixed IP address to server PCs if your network has no domain name server. If DAQSTATION network is going to be a part of your intranet, ask administrator fixed addresses for them.

This section assumes the case you are managing IP address by yourself. Though you have a plenty degree of freedom in doing this like a tyrant, it is recommended to set up a simple scheme and follow it. It would be a waste of time if you set up different schema every time you manage a new network. Scheme in this section is suggested for your "standard" configuration. It is just one of possible ideas and may not be optimal in some rare case, but can be used repeatedly because of its simplicity.

Private addressing strategy

Your DAQSTATION domain consists of 100 or less nodes in most of cases. Choose class-C private address, `192.168.0.0/24` for your domain (`192.168.0.1 ~ 192.168.0.254`). If you have remote sites connected with routers, they should have different network addresses (`192.168.1.0/24, 192.168.2.0/24 ~ 192.168.10.0/24`). They shall be expressed with a parameter, `N` (`192.168.N.0/24`), and means a central site if `N` is equal to zero (`192.168.0.0/24`).

Within a network, divide host addresses into following groups:

Grouping of IP Addresses

IP address range	Number of nodes	Fixed/ assignable	Usage
`192.168.N.1 to 63`	63	Fixed	Router to connecting sites or to Internet
`192.168.N.64 to 70`	7	Fixed	Servers (ftp, SMTP) and peripherals
`192.168.N.71 to 127`	57	Fixed	DAQSTATION recorders
`192.168.N.128 to 191`	64	Assignable	For temporary PCs through DHCP
`192.168.N.192 to 222`	31	Assignable	PCs logging in via remote access
`192.168.N.223 to 253`	31	Fixed	Router for remote access

T016.eps

This addressing group guarantees same host address is used for the same function. Standard configuration in section 3.5 allocates this IP addresses in more restrictive scheme.

Fixed IP Addresses

Allocate IP address for DAQSTATION recorders in the central site from `192.168.0.71` increasingly up to `192.168.0.127`. Allocate IP address for DAQSTATION recorders in the remote site `N` from `192.168.N.71` increasingly up to `192.168.N.127`.

Allocate IP address of `192.168.0.64` (primary) and `192.168.0.65` (secondary if exists) to ftp server(s) located in the central site. Other servers in the central site should have IP addresses allocated from `192.168.0.66`. If you need ftp server in the remote site `N`, allocate `192.168.N.64` to it.

Give host names to DAQSTATION recorders and PCs regardless you have a domain name server. It is recommended to give a name consisting of alphanumeric characters (uppercase only), hyphen and underscore, starting with an alphabet. Attach a plate or tape showing host name to them so that you can identify hosts by reading the plate or tape. If you give tags to field instruments in your facilities, follow the same rule to give host names.

DHCP Server

It is very convenient to activate DHCP server so that any DHCP client PC can get IP address to join the network very easily. Such temporary PCs are useful for maintenance and troubleshooting. Since DHCP request is broadcast in the network, you need one DHCP in each broadcast domain separated with a router.

It is easiest to use a router as DHCP server. If you have two or more routers in a network, use one of smallest host address. Even if your DAQSTATION network is an isolated network, it is a good idea to have a router (with no routing configuration) just as a DHCP server, because a simple router is very cheap today.

Configure DHCP server to allocate 64 IP addresses starting from `192.168.N.128.`

Domain Name Server

It is nice to have a domain name server in your network. If your network is a part of intranet, give its IP address to PCs and DAQSTATION recorders so that you can use host name of servers instead of their IP addresses. It is better to register host names of your servers (DAQSTATION and PC) to DNS.

If you have an Internet connection through a router, give IP address of name server notified by the Internet Provider to that router. Give router's IP address to recorders and PCs so that the router can relay the DNS request to the name server.

In other cases, it is recommended to use only IP addresses, because it might be a tough challenge for you to manage operating systems, like Linux and Windows2000 Server, which are equipped with the name server function.

Configuring DAQSTATION

Go to Basic Setting mode as experienced in section 1.4 and give IP address, subnet mask, ftp server info and mail server address using "standard configuration" menu. Read next section for mail servers.

Configuring PC

If you are going to use Windows, it is recommended to select a professional operating system instead of personal one for stable operation. It is also recommended to reboot periodically (at least once each year) Windows operating system to free resources and reset counters.

Configure TCP/IP properties of a PC by giving IP address, subnet mask, default gateway, and name server, if applicable, as experienced in section 1.3.

If you need ftp server function, install ftp server as experienced in section 1.7. Create account and folder for each DAQSTATION. Data from different DAQSTATION must be stored in different folders because it is not possible to identify DAQSTATION from the filename consisting only numbers related to date and time. Set password to avoid undesired invasion.

If you are going to use an existing ftp server on the intranet, ask administrator to create accounts, folders and password in the same manner.

Configuring Router

Consult the instruction manual of the router to find its IP address when it is shipped. Many routers have IP address of `192.168.0.1` as a shipping address. There are exceptions in the market and this could cause a problem!

Configure a PC to give it a fixed IP address of the same class of the router but other than that of the router. Subnet mask must be same. Connect the router and PC through a hub and turn on this small network.

Start a browser and open homepage of the router, which most of routers provide. If the router has an IP address of `192.168.0.1`, its URL should be `http://192.168.0.1/`. Configure DHCP server and give an IP address. This may require reboot of the router. After this is done, reconfigure the PC to acquire IP address through DHCP. Open the configuration web page with new URL (e.g., router's new IP address) to continue configuration.

Give configurations in the standard menu following the instruction manual.

3.4 Sending an Email

DAQSTATION is able to send an email when it finds a defect in its functionality or abnormal measured value, or when it issues a reporting file. A periodic email as heartbeat is also available. You can register two receivers' account and define which email should go to which. Emails are sent to mail server (SMTP server), which you need in the DAQSTATION extended network (e.g., intranet or Internet).

Possible Mail Servers

There are possible choices of having a mail server. A criterion is:

1. If the DAQSTATION is a part of your intranet, use intranet mail server.
2. If the DAQSTATION is isolated from intranet or Internet, consider cellar phone.
3. Consider mail server of an Internet provider.

Mail server on your intranet

Ask administrator to create an account for DAQSTATION. Each recorder should have individual email account to trace the delivery route when a problem is detected. Ask administrator to configure those accounts to forward received emails to another "managing account" before deleting them. This would prevent mailboxes overflow because DAQSTATION does not read emails.

Mail server for cellar phones

If a cellar phone carrier in your region provides SMTP service, it would be a convenient method to send emails. Since DAQSTATION email is not so big and is sent not so frequently, it does not require high-speed communication. GSM should work just fine.

Ask carrier to forward received email to another account or simply disable mailbox (send only) because DAQSTATION does not read received emails.

Mail server of an ISP

When you make a contract with an Internet provider, it also provides email service in addition to Internet access. Ask provider to forward received email to another account or simply disable mailbox (send only) because DAQSTATION does not read received emails.

Use telephone number of an access point given by the provider when sending emails. Some providers reject SMTP request from places other than their access points unless you open your mailbox before sending an email.

It is not recommended to use a "free email service" on Internet for business.

Managing Mail Addresses

When DAQSTATION, with account name `DX-01`, sends an email through a mail server in a domain, `inetdomain.net`, the sender of this email is identified as `DX-01@inetdomain.net`. It is shown in “FROM:” field of the message. When an error is detected at the receiving side, an error message is sent back to this address. Forwarding received email provides you an access to those messages.

DAQSTATION has a mechanism to replace the content of “FROM:” field. If you give another name to “Sender” field of “Basic Email settings” menu of configuration, given string replaces `DX-01@inetdomain.net.`

It is a good practice to have a short string to identify recorders in “Subject:” field or in the first line of the message.

DAQSTATION keeps email addresses in two fields of “Recipient 1” and “Recipient 2” of “Basic Email settings” menu so that you can configure to which address each email should go. These fields can store up to 150 characters and you can specify multiple addresses separated with a space.

There is a method to deliver an email to multiple receivers by sending it to a single email account, called “mailing list.” Suppose George, Patty and John are working together in maintaining a process observed by DAQSTATION. You can create a mailing list, `SGP-group@ml.inetdomain.net`, having their email account.
When DAQSTATION sends an email to `SGP-group@ml.inetdomain.net`, mail server in `inetdomain.net` will forward it to mail accounts of George, Patty and John. This is useful to avoid typing a long string of email accounts for each DAQSTATION. It is also useful to have a longer list of addresses. Ask your postmaster (email administrator) to create mailing list(s) for your convenience.

3.5 Standard Network Configurations for your Convenience

This section gives a “standard configuration” of DAQSTATIN network nodes. Use lists in section 3.2 for hubs and cables because they are not listed here.

Configurations in this section are simplest “examples” and are not intended to give any restriction in using DAQSTATION recorders. Neither author nor distributor of this document is responsible for any loss of damage arising out or resulting from any defect, error or omission in the standard configurations.

Assumptions, Restrictions and Examples

Standard configuration is given for several DAQSTATION network domains discussed in section 3.1, by referencing configuration tables defined at the end of this section. Configuration shown in a bracket (‘<‘ and ‘>’) shows an example of the value, which should be replaced with the value given by your network administrator or Internet provider. Configuration parameter in Italic does not give an example but requests you to define appropriate value.

This configuration assumes following restriction of network size and gives values only for them. If your network needs to be bigger, you can add more by the limits shown below.

Network Size Restriction

Item	Limit in this configuration	Extendable to
Number of remote sites	10	53
Number of DAQSTATION recorders in a network segment	10	57
Number of Remote Access Service routers	1	31

T017.eps

A remote site is identified by parameter `N (N = 1 ~ 10)` and router talking to this site at the central site is identified by another parameter `N’ (N’ = N+10 = 11 ~ 20)`.

Grouping of IP Addresses

IP address range	Number of nodes	Fixed/ assignable	Usage
192.168.0.1	1	Fixed	Router to connecting to Internet
192.168.N.1 (N≠0)	1 on each	Fixed	Router at remote sites to go to the center
192.168.0.N'	10	Fixed	Routers connecting to remote sites
192.168.N.64 to 70	7	Fixed	Servers (ftp, SMTP) and peripherals
192.168.N.71 to 80	10	Fixed	DAQSTATION recorders
192.168.N.128 to 191	64	Assignable	For temporary PCs through DHCP
192.168.N.192	1	Assignable	PC logging in via remote access
192.168.N.223	1	Fixed	Router for remote access

T018.eps

Remote Access is prepared in case you need to login the network remotely over a phone line. It is your choice to have one access point or not.

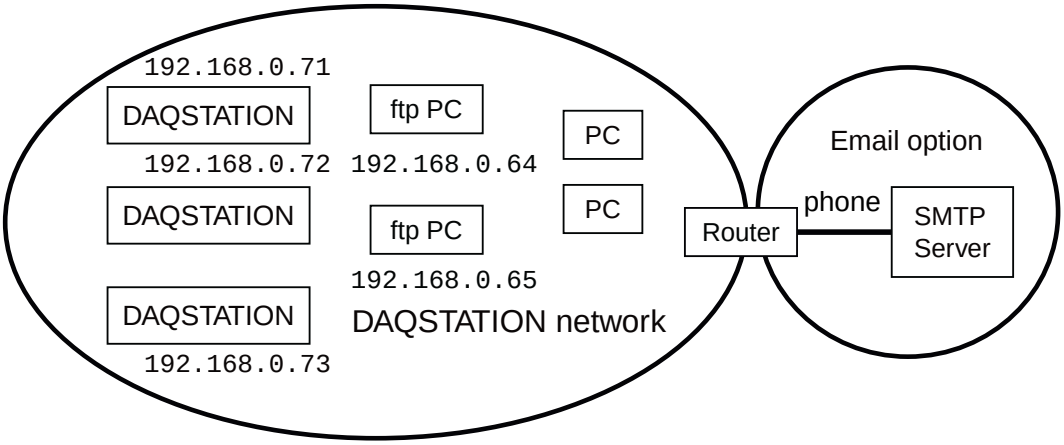
Account and folder names for ftp server are given as an example. You can choose any other names but you are responsible to give same names to both server and clients (e.g., DAQSTATION).

This configuration uses two mailing lists, one is an operating group, `opr@ml.daq.com`, and the other is maintaining group, `mt@ml.daq.com`.

Intranet configuration should follow the administrator’s network management policy. This example assumes your intranet (daq.com) uses class-B private address and network address `172.18.100.0/16` is allocated for DAQSTATION network. Domain name servers are `172.16.20.100` and `172.16.20.101`. Internet proxy is `proxy.daq.com`, ftp servers are ftp.daq.com and `ftp2.daq.com`, and SMTP server is `smtp.daq.com`.

Standard configuration uses class-C private address, `192.168.X.0/24`, for domains other than intranet. It assumes an Internet provider, if applicable, informed you domain name, `ispd.net`, user accounts, `dx-a-01 ~ dx-a-10`, domain name servers, `10.2.3.50` and `10.2.3.51`, ftp server `ftp1.ispd.net` and `ftp2.ispd.net`, and SMTP server, `smtp.ispd.net`.

Isolated DAQSTATION network



Isolated DAQSTATION network (with email option)

Completely isolated network

Node	Configuration
DAQSTATION	E1 + F1
ftp server	S1 + S2
PC for Yokogawa software	P1
PC for maintenance	P2
Router (recommended to have)	R1

T019.eps

Routing table of R1 is not necessary for this network.

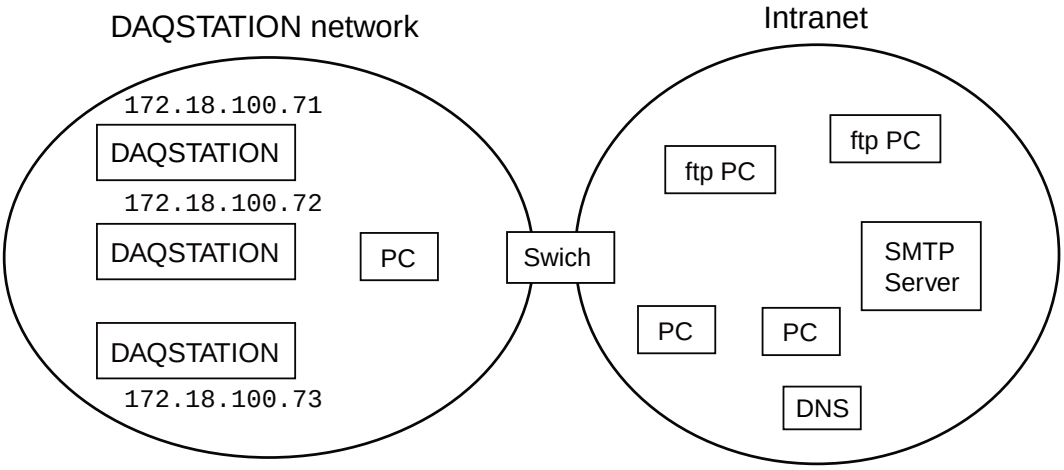
Isolated network with email

Node	Configuration
DAQSTATION	E2 + F1 + M1
ftp server	S1 + S2
PC for Yokogawa software	P1
PC for maintenance	P2
Router to Internet	R1
Router to Remote Access Service	R4 (N=0)

T020.eps

Routing table of R1 is not necessary for this network.

DAQSTATION in your Intranet



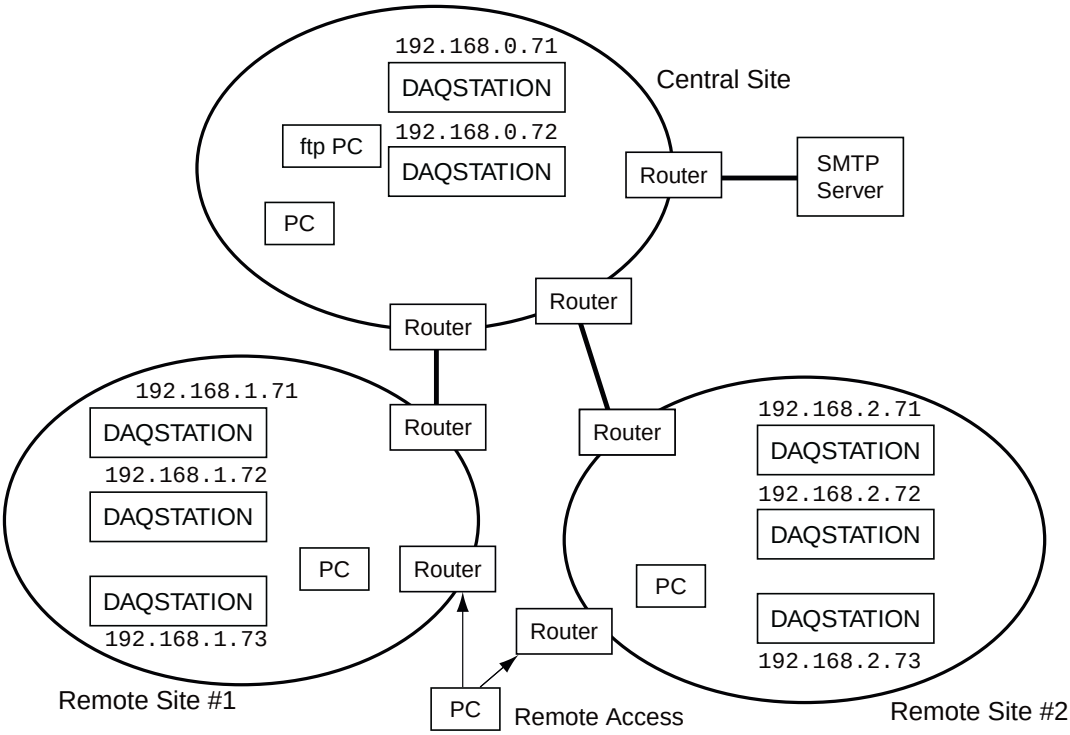
DAQSTATION network as a part of your Intranet

This configuration is just an example. Your network/system administrator must provide real configuration.

Node	Configuration
DAQSTATION	E3 + F2 + M2
ftp server	Intranet ftp server + S2
PC for Yokogawa software	P1
PC for maintenance	P2
Router	(not used)

T021.eps

DAQSTATION over WAN



DAQSTATION network distributed in multiple sites and connected over WAN or public line

Central Site

Node	Configuration
DAQSTATION	E2 + F1 + M1
ftp server	S1 + S2
PC for Yokogawa software	P1
PC for maintenance	P2
Router to Internet	R1
Router to remote site	R2
Router for Remote Access Service	R4 (N = 0)

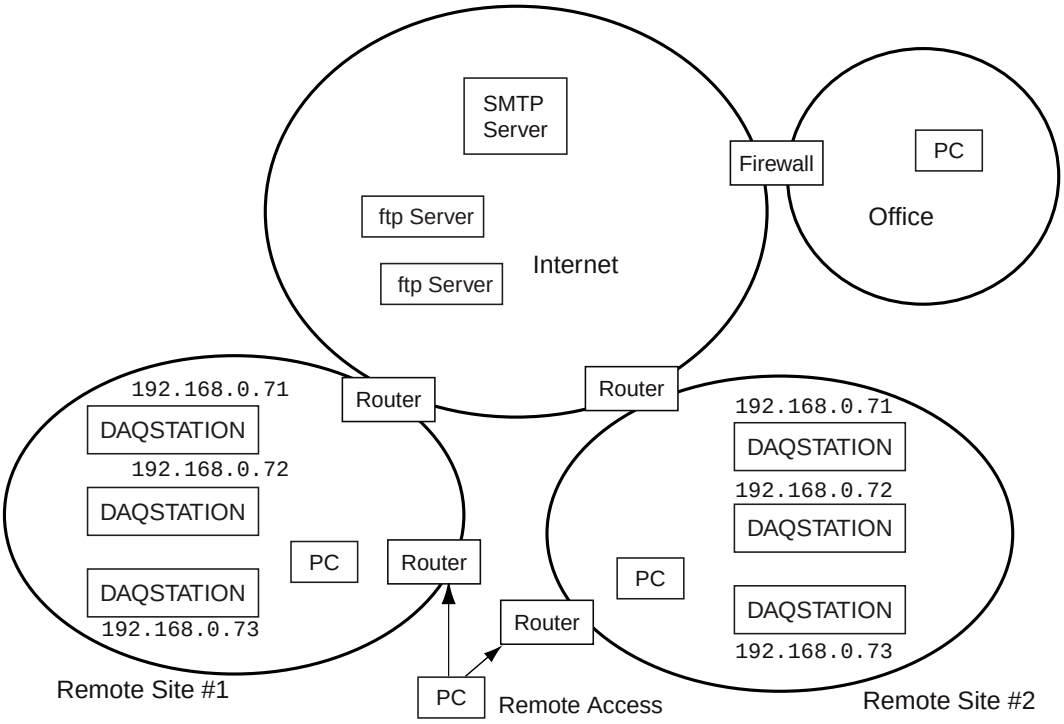
T022.eps

Remote Site

Node	Configuration
DAQSTATION	E4 + F1 + M1
ftp server (if exist)	(not used)
PC for Yokogawa software (if exist)	P1
PC for maintenance	P2
Router to central site	R3
Router for RAS (if exists)	R4

T023.eps

DAQSTATION over Internet



DAQSTATION network distributed in multiple sites and concentrated over Internet

Your intranet can be used to go to Internet as central site. If you use Internet only for email delivery, refer isolated network with email option. This configuration assumes ftp server on Internet. Since all remote sites are independent, common IP addressing scheme (`N = 0`) is applicable to all sites.

When recorders at a remote site save data locally and use Internet only for email delivery, you may want a router not only to send emails but also accept remote access (e.g., combine R1 and R5 configurations). It is possible because the frequency of email is not so high. You must, however, realize the chances of loosing emails during you are logging in the network through the router.

Remote Site via Internet

Node	Configuration
DAQSTATION	E5 (N=0)+ F3 + M1
ftp server	Internet ftp server + S2
PC for Yokogawa software (if exist)	P1
PC for maintenance	P2
Router to Internet	R1
Router for RAS (if exists)	R5 (N=0)

T024.eps

Routing configuration of R1 is not necessary for this network.

Standard DAQSTATION Configurations

This subsection gives configuration of DAQSTATION under various network environments.

Ethernet Configuration

Configuration E1: Isolated DAQSTATION network (no email/Internet)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Ethernet				
IP-address	192.168.0.71	192.168.0.72		192.168.0.80
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0
Default gateway	0.0.0.0	0.0.0.0		0.0.0.0
DNS On/Off	Off	Off		Off
Primary	0.0.0.0	0.0.0.0		0.0.0.0
Secondary	0.0.0.0	0.0.0.0		0.0.0.0
Host name	<DX-A-01>	<DX-A-02>		<DX-A-10>
Domain suffix search				
Primary	(blank)	(blank)		(blank)
Secondary	(blank)	(blank)		(blank)

T025.eps

Configuration E2: Isolated DAQSTATION network (with email/Internet option)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Ethernet				
IP-address	192.168.0.71	192.168.0.72		192.168.0.80
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0
Default gateway	0.0.0.0	0.0.0.0		0.0.0.0
DNS On/Off	Off	Off		Off
Primary	0.0.0.0	0.0.0.0		0.0.0.0
Secondary	0.0.0.0	0.0.0.0		0.0.0.0
Host name	<DX-A-01>	<DX-A-02>		<DX-A-10>
Domain suffix search				
Primary	(blank)	(blank)		(blank)
Secondary	(blank)	(blank)		(blank)

T025.eps

Configuration E3: DAQSTATION in your Intranet (Configuration in bracket shall be provided by administrator)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Ethernet				
IP-address	<172.18.100.71>	<172.18.100.72>		<172.18.100.80>
Subnet mask	<255.255.0.0>	<255.255.0.0>		<255.255.0.0>
Default gateway	<172.18.100.1>	<172.18.100.1>		<172.18.100.1>
DNS On/Off	Off	Off		Off
Primary	<172.16.20.100>	<172.16.20.100>		<172.16.20.100>
Secondary	<172.16.20.101>	<172.16.20.101>		<172.16.20.101>
Host name	<DX-A-01>	<DX-A-02>		<DX-A-10>
Domain suffix search				
Primary	<daq.com>	<daq.com>		<daq.com>
Secondary	(blank)	(blank)		(blank)

T027.eps

Configuration E4: DAQSTATION network at remote site N (N=1…63) (no DNS)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Ethernet				
IP-address	192.168.N.71	192.168.N.72		192.168.N.80
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0
Default gateway	192.168.N.1	192.168.N.1		192.168.N.1
DNS On/Off	Off	Off		Off
Primary	0.0.0.0	0.0.0.0		0.0.0.0
Secondary	0.0.0.0	0.0.0.0		0.0.0.0
Host name	<DX-N-01>	<DX-N-02>		<DX-N-10>
Domain suffix search				
Primary	(blank)	(blank)		(blank)
Secondary	(blank)	(blank)		(blank)

T028.eps

Configuration E5: DAQSTATION network at remote site N (N=1…10) (with DNS)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Ethernet				
IP-address	192.168.N.71	192.168.N.72		192.168.N.80
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0
Default gateway	192.168.N.1	192.168.N.1		192.168.N.1
DNS On/Off	Off	Off		Off
Primary	0.0.0.0	0.0.0.0		0.0.0.0
Secondary	0.0.0.0	0.0.0.0		0.0.0.0
Host name	<DX-N-01>	<DX-N-02>		<DX-N-10>
Domain suffix search				
Primary	(blank)	(blank)		(blank)
Secondary	(blank)	(blank)		(blank)

T028.eps

FTP Client Configuration

Configuration F1: FTP client to private ftp server (for remote site N, replace 'a' in login name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
FTP transfer file				
Disp & Event data	<On>	<On>		<On>
Report	<On>	<On>		<On>
FTP connection (primary)				
FTP server name	192.168.0.64	192.168.0.64		192.168.0.64
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank)	(blank)		(blank)
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>
FTP connection (secondary)				
FTP server name	192.168.0.65	192.168.0.65		192.168.0.65
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank>	(blank>		(blank>
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>

T030.eps

Configuration F2: FTP client to Intranet ftp server (for remote site N, replace 'a' in login name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
FTP transfer file				
Disp & Event data	<On>	<On>		<On>
Report	<On>	<On>		<On>
FTP connection (primary)				
FTP server name	<ftp.daq.com>	<ftp.daq.com>		<ftp.daq.com>
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank>	(blank>		(blank>
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>
FTP connection (secondary)				
FTP server name	<ftp2.daq.com>	<ftp2.daq.com>		<ftp2.daq.com>
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank>	(blank>		(blank>
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>

T031.eps

Configuration F3: FTP client to ISP ftp server (for remote site N, replace 'a' in login name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
FTP transfer file				
Disp & Event data	<On>	<On>		<On>
Report	<On>	<On>		<On>
FTP connection (primary)				
FTP server name	<ftp1.ispd.net>	<ftp1.ispd.net>		<ftp1.ispd.net>
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank)	(blank)		(blank)
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>
FTP connection (secondary)				
FTP server name	<ftp2.ispd.net>	<ftp2.ispd.net>		<ftp2.ispd.net>
Port number	21	21		21
Login name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Password	*<Password>*	*<Password>*		*<Password>*
Account	(blank>	(blank>		(blank>
PASV mode	Off	Off		Off
Initial path	<dxa01>	<dxa02>		<dxa10>

T032.eps

Email Basic Configuration

Configuration M1: Email for ISP SMTP server (for remote site N, replace 'a' in login name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Basic E-mail settings				
SMTP server name	<smtp.ispd.net>	<smtp.ispd.net>		<smtp.ispd.net>
Port number	25	25		25
Recipient 1	<opr@ml.daq.com>	<opr@ml.daq.com>		<opr@ml.daq.com>
Recipient 2	<mt@ml.daq.com>	<mt@ml.daq.com>		<mt@ml.daq.com>
Sender	<dxa01@ispd.net>	<dxa02@ispd.net>		<dxa10@ispd.net>

T033.eps

Configuration M2: Email for intranet SMTP server (for remote site N, replace 'a' in login name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
Basic E-mail settings				
SMTP server name	<smtp.daq.com>	<smtp.daq.com>		<smtp.daq.com>
Port number	25	25		25
Recipient 1	<opr@ml.daq.com>	<opr@ml.daq.com>		<opr@ml.daq.com>
Recipient 2	<mt@ml.daq.com>	<mt@ml.daq.com>		<mt@ml.daq.com>
Sender	<dxa01@ispd.net>	<dxa02@ispd.net>		<dxa10@ispd.net>

T034.eps

Standard PC Configuration

PC for private ftp Server

Configuration S1: Network configuration (open "Local Area Connection" properties, then TCP/IP properties)

Configuration	Primary	Secondary (backup)
Computer (host) name	<ftp>	<ftp2>
Workgroup	<DAQSTATION>	<DAQSTATION>
IP address	192.168.0.64	192.168.0.65
Subnet mask	255.255.255.0	255.255.255.0
Default gateway	192.168.0.1	192.168.0.1
Preferred DNS server	192.168.0.1	192.168.0.1

T035.eps

Configuration S2: ftp account (for remote site N, replace 'a' in file folder and user name with N)

Configuration	1st DAQSTATION	2nd DAQSTATION	....	10th DAQSTATION
User name	<dx-a-01>	<dx-a-02>		<dx-a-10>
Full name	(blank)	(blank)		(blank)
Password	*<Password>*	*<Password>*		*<Password>*
File folder	<dxa01>	<dxa02>		<dxa10>

T036.eps

PC for Yokogawa PC Software Packages

Configuration P1: Network configuration (open "Local Area Connection" properties, then TCP/IP properties)

Configuration	1st host	2nd host	....	5th host
Computer (host) name	<host1>	<host2>		<host5>
Workgroup	<DAQSTATION>	<DAQSTATION>		<DAQSTATION>
IP address	192.168.0.66	192.168.0.67		192.168.0.70
Subnet mask	255.255.255.0	255.255.255.0		255.255.255.0
Default gateway	192.168.0.1	192.168.0.1		192.168.0.1
Preferred DNS server	192.168.0.1	192.168.0.1		192.168.0.1

T037.eps

If you want PCs at remote site N, give IP addresses 192.168.N.64 and 192.168.N.65 to ftp servers and 192.168.N.66 through 192.168.N.70 to others. Configuration PC software packages for your network is not provided here.

PC for maintenance

Configuration P2: Network configuration (open "Local Area Connection" properties, then TCP/IP properties)

Configuration	1st PC	2nd PC	....	5th PC
Computer (host) name	<maint1>	<maint2>		<maint5>
Workgroup	<DAQSTATION>	<DAQSTATION>		<DAQSTATION>
IP address	Obtain an IP address automatically			

T038.eps

These PCs are used directly connected to DAQSTATION network or via remote access. Configuration PC software for your network is not provided here.

Standard Router Configuration

Configuring routers is a little complicated because terminology and methods depend on the vendor. Read instruction manual of the router in giving values below.

Configuration R1-R5: Basic configuration (IP address of RAS router in the central network shall be 192.168.0.253)

Configuration	**R1**: Internet	**R2**: Central site	**R3**: Remote site	**R4**: RAS
Network		(N'= N + 10)		
IP Address	192.168.0.1	192.168.0.N'	192.168.N.1	192.168.N.253
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default gateway	192.168.0.1	192.168.0.1	192.168.0.1	192.168.0.1
DHCP server	Enabled	Disabled	Enabled	Disabled
Start address	192.168.0.128		192.168.N.128	
No of addresses	64		64	
DNS server				
Primary	<given by ISP>	192.168.0.1	192.168.0.1	192.168.0.1
Secondary	<given by ISP>			
Routing	Static	Static	Static	Static
NAT/Masquerade	Enabled	Disabled	Disabled	Disabled
My Telephone No.	*<center0>*	*<center N>*	*<remote N>*	*<RAS N>*
My user ID	*<ISP user ID>*	*<center N ID>*	*<remote N ID>*	
My password	*<ISP password>*	*<remote N PW>*	*<remote N PW>*	
Partner Telephone	*<ISP AP>*	*<remote N>*	*<center N>*	
Partner user ID		*<remote N ID>*	*<center N ID>*	*<RAS N ID>*
Partner Password		*<remote N PW>*	*<center N PW>*	*<RAS N PW>*
Partner IP address		192.168.N.1	192.168.0.N'	192.168.N.192
Protocols				
Authentication		CHAP	CHAP	CHAP
Routing		(RIP)	(RIP)	(RIP)

T039.eps

Configuration R1: Static routing table for Router to Internet

No	Destination	Next hop	Metric	Interface
1	192.168.1.0/24	192.168.0.11	3	Ethernet
2	192.168.2.0/24	192.168.0.12	3	Ethernet
3	192.168.3.0/24	192.168.0.13	3	Ethernet
4	192.168.4.0/24	192.168.0.14	3	Ethernet
5	192.168.5.0/24	192.168.0.15	3	Ethernet
6	192.168.6.0/24	192.168.0.16	3	Ethernet
7	192.168.7.0/24	192.168.0.17	3	Ethernet
8	192.168.8.0/24	192.168.0.18	3	Ethernet
9	192.168.9.0/24	192.168.0.19	3	Ethernet
10	192.168.10.0/24	192.168.0.20	3	Ethernet
11	0.0.0.0	dynamic		WAN

T040.eps

Configuration R2: Static routing table for a central Router to remote site N

No	Destination	Next hop	Metric	Interface
1	192.168.N.0/24	192.168.N.1	2	WAN
2	0.0.0.0	192.168.0.1	1	Ethernet

T041.eps

Configuration R3: Static routing table for a remote Router at site N to central site.

No	Destination	Next hop	Metric	Interface
1	0.0.0.0	192.168.N'	1	WAN

T042.eps

Configuration R4: Static routing table for a Remote Access Service Router at site N (including central site)

No	Destination	Next hop	Metric	Interface
1	0.0.0.0	192.168.N.1	1	Ethernet

T043.eps

3.6 When you need Wireless Connection

This section discusses an additional configuration of your DAQSTATION network, a wireless LAN to repeat Ethernet with radio. You may consider a wireless LAN in the following cases:

- DAQSTATION recorders are installed in multiple buildings, between which it is difficult to install an Ethernet cable.
- DAQSTAION is being installed in an operating clean room. You are not allowed to install Ethernet cable but you want communication through a glass window.
- DAQSTATION is installed in a remote site, which is visible from your office.
- You plan to record data in a trial or an experimental plant. Since it is a temporary site, you do not want to install many cables among facilities.

IEEE802.11b wireless LAN (Wi-Fi) is very useful for those cases and will be discussed in this section.

Network Configuration

Wireless LAN should be in "*infrastructure mode*" and you need an access point. You can extend Ethernet cable with the pair of two access points, one configured as an "*access point*" and the other as "*station.*" This configuration is safe because some access points support communication between *access points* and the others do not. A PC with wireless LAN interface card can join this network as a *station* from any place within the radio reach.

Since an access point separates a collision domain, you can treat it as a node when you count hubs between nodes (should not exceed four). For your information, it does not separate a broadcast domain. Two Ethernet segments connected with wireless LAN form one network. Since DHCP service is relayed via wireless LAN, a DHCP server on one segment gives an IP address to a node on another segment.

Access points need an IP addresses for management. It is better to give them fixed address to identify them easier. Use a part from 2 to 9 of fixed address range for routers.

Antennae Installation

Radio signal goes straight as long as 100m. If access point and stations are installed within a building, wireless LAN works fine with antennae installed in access points and interface cards as long as stations are visible from the access point. Glass, plastic or wood does not prevent radio. Wireless LAN does not work beyond floors or fire-resistant walls because radio cannot penetrate through metal or concrete.

If you want to connect two buildings, locate antennae inside of glass windows of buildings visible each other. When distance between access points is within 100m, antennae embedded to the access points would work fine. If the radio field is not strong enough with such antennae because of distance, window material or a bad weather (especially rain), consult a vendor to supply planer antennae.

If you want to relay Ethernet segments in more distant places, say a mile, you need much more effective antennae (Yagi or parabola). Consult an antenna vendor if it works within your distance. You may need to consider the cable length from a hub to the access point installed near the roof of the building.

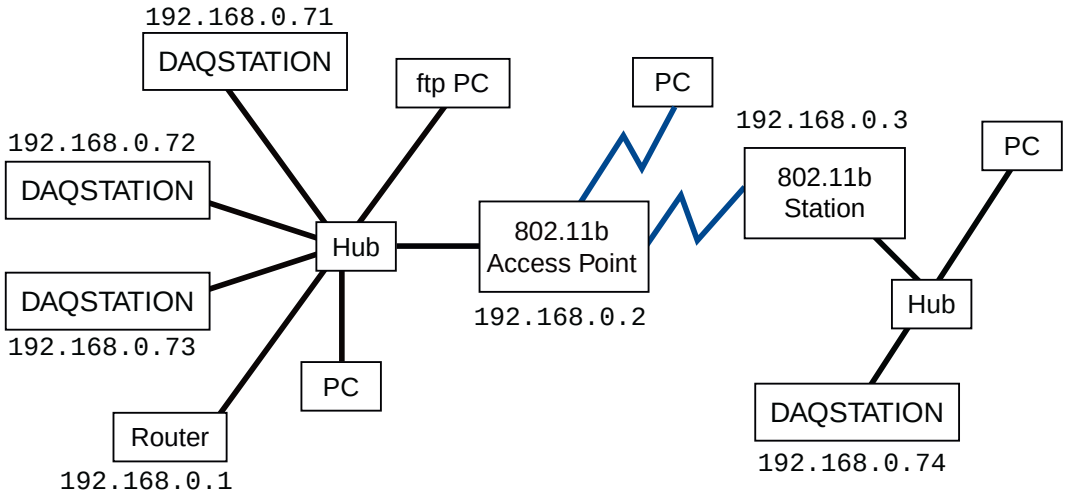
Radio Configuration

Choose radio channel not used in your site. Radio band of adjacent channel may have an overlap and should be avoided.

Do not forget to set SSID and WEP encryptions for security reasons. They should be secret to people other than the LAN manager. This section does not suggest any key code by this reason and you must choose them by yourself.

Node Configuration

Here is a standard configuration to have a wireless part within your DAQSTATION network. IP addresses are chosen for a private network `192.168.N.0/24`. WEP key code handling depends on the device vendor.



DAQSTATION network with IEEE802.11b connection

Wireless LAN configurations

Item	Access Point #1	Access Point #2	PC Interface
IP Address	`192.168.N.2`	`192.168.0.3`	`<Obtain by DHCP>`
Subnet mask	`255.255.255.0`	`255.255.255.0`	`<Obtain by DHCP>`
Administrator password	*<Admin password>*	*<Admin password2>*	
Mode	`Infrastructure`	`Infrastructure`	`Infrastructure`
Operation	`Access Point`	`Station`	`(Station)`
Channel	*<select one>*	*<select one>*	`automatic`
SS ID (ESS ID)	*<SSID>*	*<SSID>*	*<SSID>*
Security	`WEP40`	`WEP40`	`WEP40`
WEP key code	*<WEP key code>*	*<WEP key code>*	*<WEP key code>*

T044.eps

DAQSTATION online in three days

TI 04L01A01-41E 1st Edition

INDEX