

Networks in Brief



Imprint

Manufacturer

Eaton Automation AG
Spinnereistrasse 8-14
CH-9008 St. Gallen
Schweiz
www.eaton-automation.com
www.eaton.com

Support

Region North America

Eaton Corporation
Electrical Sector
1111 Superior Ave.
Cleveland, OH 44114
United States
877-ETN-CARE (877-386-2273)
www.eaton.com

Other regions

Please contact your supplier or send an E-Mail to:
automation@eaton.com

Original instructions

The German version of this document is the original instructions.

Editor

Manfred Hüppi

Brand and product names

All brand and product names are trademarks or registered trademarks of the owner concerned.

Copyright

© Eaton Automation AG, CH-9008 St. Gallen

All rights reserved, also for the translation.

None of this document may be reproduced or processed, duplicated or distributed by electronic systems in any form (print, photocopy, microfilm or any other process) without the written permission of Eaton Automation AG, St. Gallen.

Subject to modifications.

Contents

1	Purpose of this document.....	5
2	Network topology.....	6
2.1	Hub.....	6
2.2	Switch.....	6
2.3	Router.....	6
2.4	Firewall.....	6
3	Settings.....	7
3.1	Introduction.....	7
3.2	IP address.....	7
3.3	Subnet mask.....	8
3.4	Gateway.....	8
3.5	DNS (domain name server).....	9
3.6	DHCP (obtain IP address automatically).....	9
3.7	WINS.....	9
3.8	Example of a network.....	10
4	Client server communication.....	11
4.1	Port.....	11
4.2	Server.....	11
4.3	Client.....	12
4.4	Peer to peer (P2P).....	12
4.5	Client in the intranet - server on the internet.....	12
4.6	Server in the intranet - client on the internet.....	12
4.7	Example.....	13
4.8	Static or dynamic IP address.....	13
5	Useful commands.....	14
5.1	PING.....	14
5.2	IPCONFIG.....	14
5.3	TRACERT.....	14
5.4	NETSTAT.....	14

Contents

1

Purpose of this document

This document is intended as an aid to integrate computers and panels in networks.
It contains information on:

- networks in general
- the integration of computers and panels in networks.

2 Network topology

2.1 Hub

A hub is a device that is used as a connection between different network stations. All data is distributed to all connected devices (via patch cables).

2.2 Switch

Switches are a further development of hubs. The difference is in their "integrated intelligence" by which they can ensure the optimum distribution of data packets. Several data packets can pass through the switch simultaneously. The total band width (data throughput) is considerably higher than on a hub. Switches learn gradually which stations are connected to which ports and thus with further data transfers do not burden other connections unnecessarily, but only the connection linking the destination station. Apart from being more expensive, switches only have advantages over hubs.

2.3 Router

This device is used to route or forward calls within a network to the Internet (or another network). This makes it impossible for a remote computer outside of the intranet to determine from which computer in the intranet it is requesting data. All computers within the intranet appear on the Internet with the same IP address.

2.4 Firewall

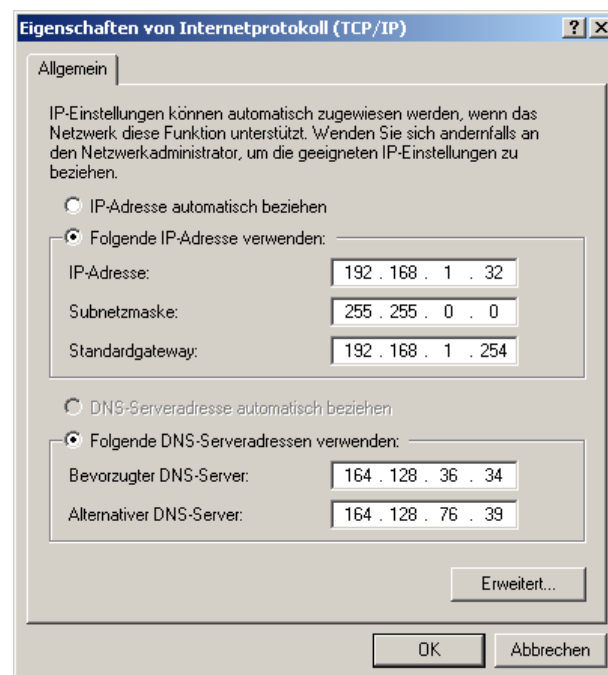
A firewall is used to prevent remote accesses to IP addresses within the intranet. It therefore protects internal data. When suitably configured, it can also be used to exclude URLs from being called by means of rules or lists, for example, when they contravene company ethics.

A firewall primarily decides whether to grant or refuse access by means of the information on source, destination IP and port contained in a packet. In this way, packets that are not allowed are also prevented from burdening the network, and prevent packets from the intranet reaching the Internet.

3 Settings

3.1 Introduction

The following section shows the required network settings to ensure effective communication via Ethernet. The figure shows an example of settings made using Windows 2000. Similar entry screens appear with other operating systems.



3.2 IP address

An IP address is 32 bits (4 bytes) long and is used for the unique identification networks, subnets and individual computers operating with the TCP/IP protocol.

Private address areas for local networks: (intranet)

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Examples:

172.16.1.22
192.168.128.132

Public addresses: (Internet)

Examples:

198.175.96.33 www.intel.com

3.3

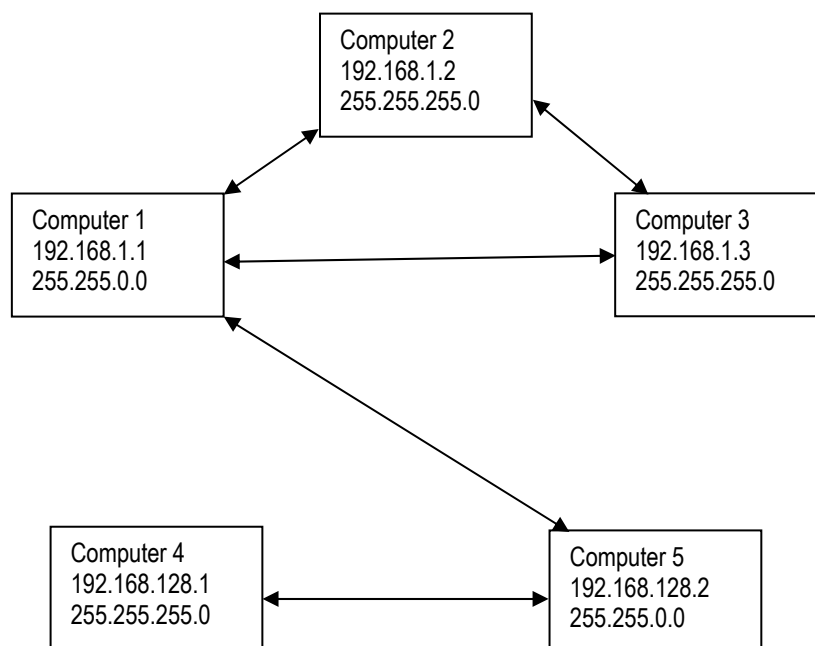
Subnet mask

The subnet mask is an IP address “filter” and has the same structure as an IP address. This mask defines which computers can exchange data with each other within a network. It therefore also defines the maximum size within a network.

Subnet mask	No. of computers	Possible IP addresses
255.255.255.0	254	aaa.bbb.ccc.0 – aaa.bbb.ccc.255
255.255.0.0	65534	aaa.bbb.0.0 – aaa.bbb.255.255

Configuration examples:

 The arrows indicate which computers can communicate with each other. All computers must be physically interconnected.



3.4

Gateway

If two computers in different networks wish to communicate with each other, these networks must be connected via a router. For example, when surfing on the Internet, the data packet must be routed from the Internet to the intranet and vice versa.

The subnet mask enables a computer to know whether to search for the recipient in the same network or another one. If this computer is outside of the network, it sends the data packet to the router that is specified by the IP address in the gateway entry.

3.5 DNS (domain name server)

If an address such as `www.intel.com` is entered in a browser or an FTP client, the computer cannot do anything with it. It first has to ask for the IP address that is assigned to this name. This information is provided by a Domain Name Server. Each Internet provider offers this service.

Providers usually offer a second DNS should a DNS fail.

The DNS entries are the IP addresses of these servers.

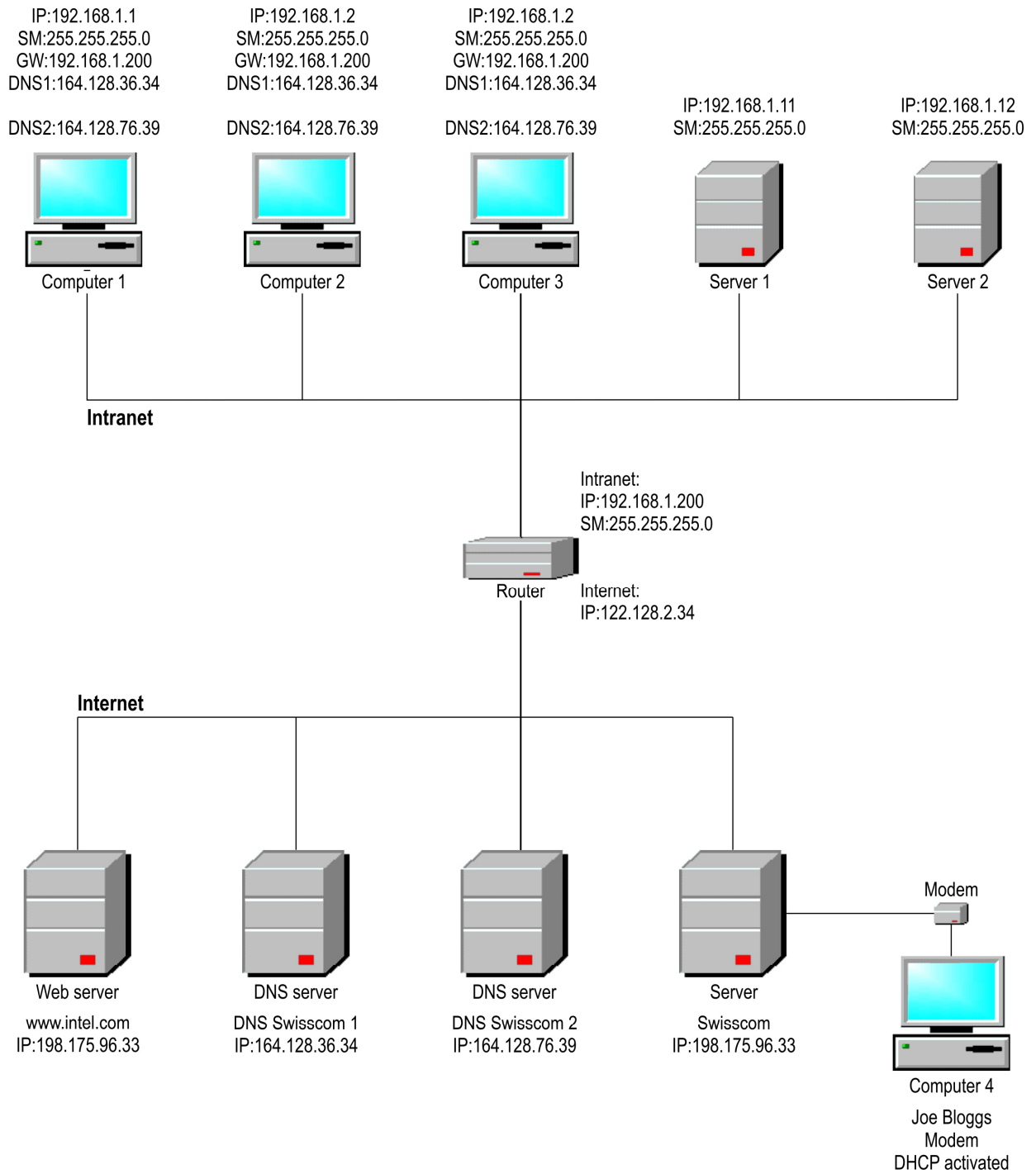
3.6 DHCP (obtain IP address automatically)

This setting can be activated if you do not wish to configure every computer within a network, and if there is a DHCP server within the network. The computer then obtains the necessary information such as IP address, subnet mask, gateway and DNS from the DHCP server. The router in the network usually also contains a DHCP server.

3.7 WINS

WINS is the abbreviation for the Windows Internet Name Service. This service is responsible for resolving names in the intranet of Microsoft networks. However, to use this service a WINS server must be in place. Otherwise the name is resolved via broadcasts and other mechanisms. The IP address can be assigned to a fixed name in the WINS server so that the computer is still detected if the IP changes.

3.8 Example of a network



4

Client server communication

4.1

Port

A port is a type of virtual mailbox for data packets. A computer can communicate with other computers on 65536 different ports. This can be understood as follows:

If Internet Explorer wishes to open a web page it requests a port from the operating system. The operating system then provides it with a suitable port, such as port 1000. Internet Explorer then sends a packet to the web server. This contains the sender IP address, the sender port (port 1000), the receiver IP address, the receiver port (for web pages port 80 as standard) as well as user data (the request for a particular web page). This enables the data packet to know where it should be sent. The web server detects the data packet in its port, processes it and sends a response to the sender.

Each "important" protocol has a "well-known" port. The port numbers 1 to 1024 should only be used for well-known server services.

Important port numbers:

Port No.	Service	Description
20	FTP Data	File transfer (data transfer from server to client)
21	FTP	File transfer (session initiation and sending of FTP control commands by the client)
23	Telnet	Terminal emulation
25	SMTP	E-mailing
80	HTTP	Web server
110	POP3	Client access for e-mail server
143	IMAP	Access and management of mail boxes
443	HTTPS	Encrypted web server transmission, mostly by SSL or TLS encryption

4.2

Server

A server is normally the term given to a computer that offers services in a network. However, this not exactly correct, since servers are really the applications in a computer that have the task of presenting or processing data. Any computer can offer these services.

A server is inherently inactive. It waits until it is addressed by a client and then executes its tasks. Every server application offers its service in the network via a port.

Typical servers:

■ Web server	Port 80	■ SMTP server	Port 25
■ FTP server	Port 21	■ POP server	Port 110
■ Telnet server	Port 23		

4.3

Client

A client is normally the term given to an application which requests certain services from a server.

Typical clients:

- Internet Explorer
- WS-FTP
- Outlook

4.4

Peer to peer (P2P)

Peer-to-Peer is a term given to computers that are connected together, each of which can take on the role of server and client. Famous P2P applications are Napster, Kazaa, eDonkey etc.

4.5

Client in the intranet - server on the internet

This type of access is normally the case for an Internet user.

Example: (see Chap. 4.7)

User no. 2 with IP address 192.168.1.11 opens a web page with Internet Explorer. The operating system assigns port 1000 to Internet Explorer. The data packets are then sent to the gateway or router. This automatically makes an entry in the routing table, specifying that the user with IP address 192.168.1.11 and port 1000 wishes to access the Internet. It assigns a new port number 1002 to this entry. The router sends the data packet under the new sender IP address 129.232.123.8, port 1002 to the web server. This processes the request and sends back a response to the router. The router searches for port 1002 in the routing table and receives back the definitive IP address 192.168.1.11 port 1000 of User no. 2. This enables the router to know where it should forward the data packet. Internet Explorer is waiting longingly for a response in port 1000.

4.6

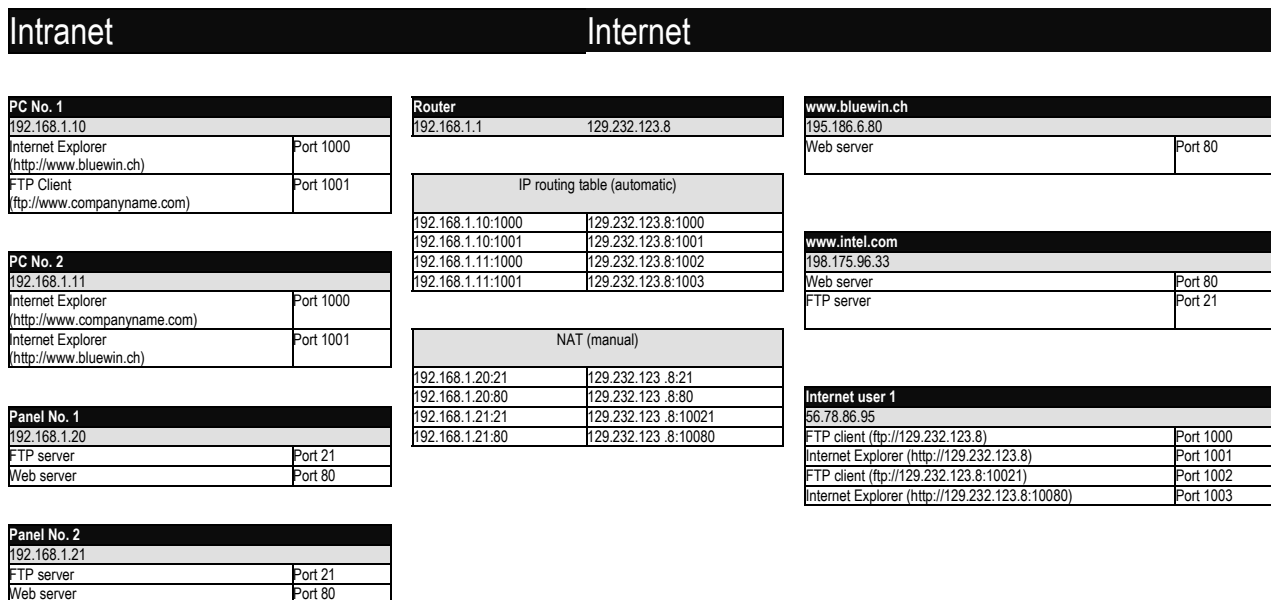
Server in the intranet - client on the internet**Example: (see Chap. 4.7)**

Internet user 1 wishes to access the FTP server of a panel No. 1 which is connected in the intranet of company XYZ. The entire company is only visible to the Internet under IP address 129.232.123.8. The IP address 192.168.1.20 of the panel would not be successful for access from the Internet because this is a private IP address. The user confidently opens connection 129.232.123.8 with an FTP client, unfortunately in vain. The router did not know what it should do with the data packet. The network administrator first had to make a manual entry in the NAT of the router, in which the router is notified to forward a data packet to the IP address 192.168.1.20 port 21 when a data packet is sent to the router port 21. What would happen, however, if a second panel is set up in the intranet? This cannot be assigned to the same port on the router. A new port must be defined, such as port 10021. When accessed with the FTP client, IP address 129.232.123.8 port 10021 must then be specified explicitly.



Apart from the router, any firewall must also be configured so that external access is possible. Ask your network administrator about this.

4.7 Example



4.8 Static or dynamic IP address

Accessing the intranet from outside is not a problem if the company intranet has a dedicated line with a static IP address. With DSL connections, the router is assigned a new IP address several times during the day. A server in the intranet can only be accessed if the network administrator notifies the Internet user of the current IP address. This is very complicated. However, it is possible to use a Dynamic Domain Name Server service on the Internet.

If you wish to know more about this, visit the website at www.dyndns.org.

It should be remembered that some providers disconnect the DSL connection if it is not active. The company intranet cannot then be accessed. As a countermeasure, an application should be run in the intranet that continuously accesses the Internet so that the Internet connection is kept active. The routers can in part be configured so that this maintains this connection.

A connection is virtually impossible if the company intranet is connected to the Internet via a dial-up connection. The Internet connection must be established manually from the intranet.

5 Useful commands

The following commands can be entered in the command prompt of a Windows PC or partly also in Windows CE. For information which commands are available, see the system description of the used operating system.



The following commands may possibly only work inside the intranet, because the firewall in your company network does not permit these kinds of accesses to the Internet. If necessary ask your network administrator.

5.1 PING

The PING command can be used to test whether a network connection can be established to another computer.

Examples:

PING 192.168.1.1

PING www.intel.com

5.2 IPCONFIG

The IPCONFIG command is used to obtain the network settings of your own computer.

Examples:

IPCONFIG Displays information.

IPCONFIG /all Displays detailed information.

5.3 TRACERT

The TRACERT command is used to display the route taken by a data packet.

Examples:

TRACERT 192.168.1.1

TRACERT www.intel.com

5.4 NETSTAT

Displays protocol statistics and the current TCP/IP network connections.

Examples:

NETSTAT Displays the status of all client connections.

NETSTAT -a Displays the status of all connections.

NETSTAT -n Displays addresses and port numbers in numerical order.