

1 Purpose

This document describes the basics of networks from a theoretical point of view. The different notions will be more practically described by means of some examples.

More information on how to use an eWON in the network topologies can be found in the Technical Notes 15, 16 and especially 17, that you can find on our web site <http://www.ewon.biz> (**Support/Documentation/Technical Notes**).

1.1 Structure of the document

A first part will describe what an IP address is, both for hosts and networks. This first section will also describe the concepts of sub-networks and their advantages.

The next section briefly explains the principle of name resolution.

A third section explains how to connect networks to each others. Gateways, Port Forwarding and Firewalls are also described.

The last section describes a specific but very frequent type of connection used by particulars. The Dynamic DNS mechanism is also explained.

2 Host and Network Address

A host is a device that has a network interface. Most of the time, it will be a computer, but it can also be an embedded device like the eWON, or a PLC.

2.1 Host Address

A host IP address is a 32 bits number that identifies a unique host on a network. The address must therefore be unique on the network. To make the addresses more readable by humans, they are often represented by four numbers from 0 to 255, separated by a dot.

For example, the address:

11000000	10101000	00000000	00000001
----------	----------	----------	----------

Table 1: IP address - bit representation

Can be translated into:

192	168	0	1
-----	-----	---	---

Table 2: P address - decimal representation

The address will therefore be written "192.168.0.1".

For all eWON® types

A simple network can present the following topology:

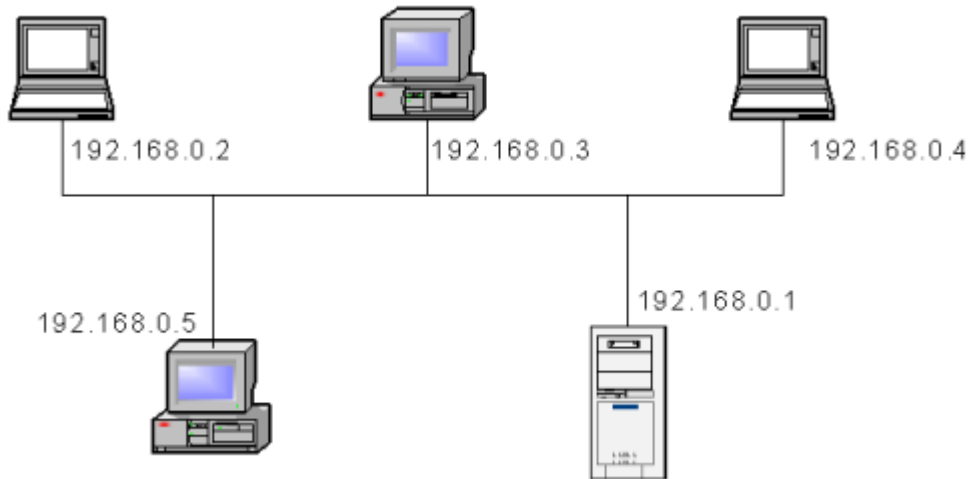


Table 3: Simple Network topology

In this figure, the wires shows the connection. In practice, this will often be achieved by using a hub or a switch. Each of the IP packets that are sent on the network contains both the sender address and the recipient address. The sender address is necessary for the recipient to be able to respond. When receiving a packet, the network interface of each host on the network will check the recipient's address. If this IP address is equal to its own address, then the packet is read and is sent to the TCP/IP stack; otherwise, it is discarded.

2.2 Network Address

Before defining a network address, we must explain what it is useful for. We have seen that a host address can be any address from 0.0.0.0 to 255.255.255.255, which gives 4.228.250.625 potential addresses! Theoretically, we could connect this amount of machine with a long cable, and each of those hosts could speak to any other... It is practically unfeasible, because four billion hosts speaking at the same time would result in an unmanageable amount of packets collisions on the network, and this would result to that not a single communication would work, exactly the same as if we were four billion of persons speaking at the same time in a huge room.

Connecting each computer to each other is useless, since a host located in your office will communicate a lot more often to the server next room than to a computer located on another continent. A solution to avoid packet collisions is by separating this huge network in smaller sub-networks. This is what network addresses are useful for: instead of considering the 32 bit address of a host as one long identifier, we separate it in two parts: the network number and the host number. A machine is then identified as host X on network Y.

All the networks don't need to contain the same amount of hosts. A home network will rarely contain more than ten hosts, while an insurance company needs several thousands. Network can therefore be classified following the number of hosts they involve. On a small network, a host IP address will have a long network number and a small host number, on the other hand, a host on a big network will have a small network number and a big host number.

For all eWON® types

Three sizes are predefined and separate networks in class A, B and C. The following table describes those three classes:

Class	Network bits	Host bits	Host Range Address	Address			
A	8	24	0.0.0.0 – 127.255.255.255				
B	16	16	128.0.0.0 – 191.255.255.255				
C	24	8	192.0.0.0 – 223.255.255.255				

Table 4: the three main IP classes

As we can see, there are a lot more class C networks than class A ones. The ranges have been distributed like this to allow their recognition from the first bits (00 for class A, 01 for class B and 11 for class C)

A network address consists in the IP address from any of the hosts on the network, where the host number has been replaced by zero. For instance, a class C network address will be 192.168.1.0. A class A network can be 10.0.0.0. Note that it is perfectly legal to have a class C network address 192.168.0.0. It just means that the hosts of that network will have an address 192.168.0.x where x is the host number and the 0 is part of the network address.

2.2.1 Public and Private Networks

With the evolution of Internet, it has become impossible for every company to have a fixed IP address, unique in the world, for each of its hosts. The number of computers is simply too big. Some smaller ranges of addresses have therefore been assigned for internal use, while the other ranges remain public. It means that several computers in the world have the same IP address. This is not a problem as far as the two internal networks are not connected to each other. We will see later how it is possible for computers from those two networks to communicate with each other.

One private range of addresses has been defined for each of the three classes:

Class	Private Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Table 5: Private ranges of addresses

A home host must therefore be in the range [192.168.0.0 -> 192.168.255.255], while an insurance company will have its hosts in the range [10.0.0.0 -> 10.255.255.255].

The networks out of this range are public, it means that they have a known, fixed IP address on the Internet.

2.2.2 Netmask

Let us consider a company that wants to host its own web server, its pop3 mail server and an ftp server. Those three hosts must be accessible from Internet and therefore, the company must obtain three fixed IP addresses. The addresses the company will receive will be, for instance, 129.128.5.191 (actually, this address corresponds to www.openbsd.org), 129.128.5.192 and 129.128.5.193. Those addresses are part of the class B network, 129.128.0.0. The three machines will maybe need to communicate with each other, but they don't need to communicate with hosts with addresses 129.128.4.x. The class B network must be spitted in smaller entities or sub-networks, so that the traffic can be decreased (see §2.3.1). The net mask is the key.

A net mask is a 32 bits number and is, as the IP addresses, often represented by four decimal numbers in the range of 0 to 255. Each bit of the net mask signifies if the corresponding bit of the IP address is part of the network number or part of the host number. While the number is more easily remembered as four decimal number, the meaning of the net mask is better seen looking at its binary format.

Let us imagine we have ordered three successive fixed IP addresses. Only the three last bits of our addresses could be different (the addresses received will always be successive addresses). Only the three last bits define the host number. We will therefore receive a net mask of 255.255.255.248. Indeed, 248 is 11111000 in binary format. With this net mask, however our addresses are part of a class B network, the machine number is only three bits long, and not 16 as it is by default.

2.2.3 Network Traffic

Using sub-networks can decrease considerably the network traffic by:

- **Avoiding hosts of different sub-networks to communicate**
- **Reducing the range of broadcast messages**

2.2.3.1 Communication Restriction

Hosts can only communicate with hosts of the same sub-network. For example, let's say we have a class C internal network with the address 192.168.1.0. If we apply a net mask of 255.255.255.128, we have separated the initial network in two sub-networks, each containing 128 hosts. Indeed, the network number is now 25 bits long while the host number becomes 7 bits long (allowing decimal values from 0 to 127). The first sub-network will have the addresses from 0 to 127, and the second the addresses from 128 to 255.

Let's say you have a host with the address 192.168.1.1. If you try to ping the host 192.168.1.223, a message will appear telling you "network unreachable". This can look more like something annoying then something positive, but we must be aware of the fact that, for example, windows file sharing protocol sends a lot of messages on the network, just to keep the file explorer up to date. Several protocols like this can quickly overload your network.

2.2.3.2 Broadcast Range

A special address can be used to send a packet to every host from the network. This mechanism is called broadcasting. The broadcast address can be set to be limited to the local sub-network. How to set the broadcast address is better shown with some examples as follows:

IP Address	Netmask	Broadcast Address
192.168.1.1	255.255.255.0	255.255.255.255
192.168.1.1	255.255.255.252	255.255.255.3

Table 6: broadcast range examples

With the first configuration, a broadcast message will be accepted by every machine with the address 192.168.1.x. With the second configuration, the address will be accepted only by three hosts.

For all eWON® types

Now, if we have computers connected to each other with a hub, the broadcast message -whatever its address is- will be sent to every host, so we haven't won anything. If we use a gateway between sub-networks, as it will be explained in a coming section, the broadcast message will not be forwarded to the other sub-networks and we decrease the network traffic.

While most web, mail and other public servers do not use broadcasting often, desktop computers do. Limiting the range of the broadcast messages can decrease considerably the network traffic.

2.3 Name Resolution

If we had to enter the IP address of the web server in our browser, we would need a big book (like an earth-wide telephone book) containing company names and the corresponding IP addresses and we should check at each connection because addresses are not that easy to remember! Indeed, it is easier to enter `www.google.com` than `216.239.51.99`.

When we enter `www.google.com` in our browser, a mechanism, called Name Resolution, is needed to translate this name into the IP address.

Several computers on Internet, called DNS (Dynamic Name Server), maintain a huge table of correspondence (like phone books). When we enter `www.google.com` and press enter in our browser, our computer sends a request to a DNS server which responds with the corresponding IP address. The name server is said to be dynamic because the entries of the translation table are regularly updated. Of course, the IP address of a DNS must be entered as is, and no names can be used.

2.4 Connecting Networks

So far, we have seen isolated networks or sub-networks. We have also seen that internal networks have addresses that are not unique in the world and that they may not be directly connected to the Internet. We thus need a way to interconnect networks and hide the internal networks. This section will explain the different ways to achieve this.

2.5 Gateways

A gateway is a host connected to two networks which serve as a common gate to every packet that needs to go from one network to another. The following figure shows a standard topology of two internal networks connected by a gateway.

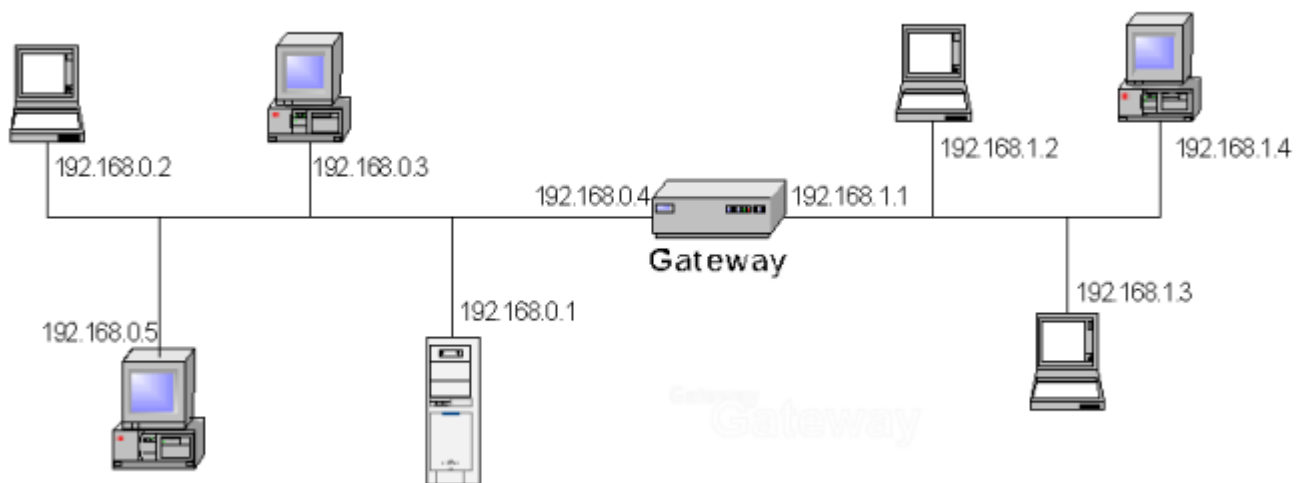


Figure 1: Gateway topology

On this figure, you can see that the network on the left has the address 192.168.0.0 and the network on the right has the address 192.168.1.0. The host named Gateway has two network interfaces, one connected to each network. The hosts of the network 192.168.0.0 must be configured to have the host 192.168.0.4 as a gateway to the 192.168.1.0 network. The hosts of the network 192.168.1.0 must have the host 192.168.1.1 as a gateway to the network 192.168.0.0.

The figure showed the connection of two networks. A gateway can also be used to connect two sub-networks (remember the broadcasting range discussion (See "Broadcast Range" on page 4) or more than two networks.

2.5.1 Default Gateways

In the topology of the Figure 2, every host knows about the other network. Often, we want a machine that relays every packet that is not for the local network. This topology arises generally with Internet connections, as we will see later.

The following figure shows such a topology:

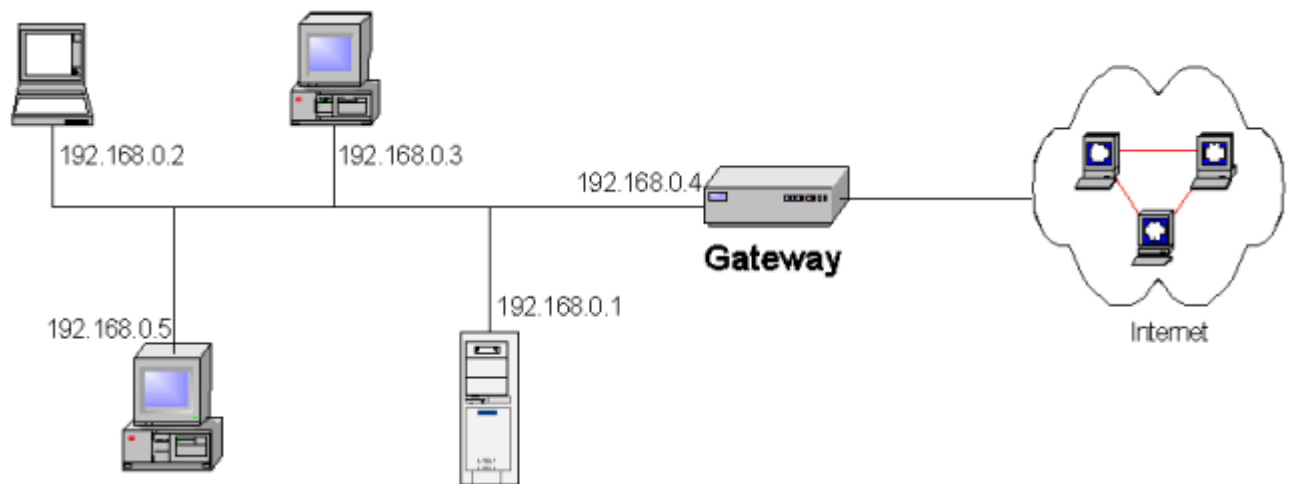


Figure 2: Default Gateway

Windows operating systems only allow to configure default gateways. It is not possible to configure several gateways to different networks or sub-networks.

2.6 Network Address Translation

We have seen that internal network cannot be directly connected to Internet. So, how can you reach Internet from your office desktop machine? The key is to have a special host that serves as a default gateway while masking the sender IP address.

Let's say we have a host with the address 192.168.0.2 and a default gateway with a local address 192.168.0.1 and a public address 194.194.194.1. We want to send a packet to a Web server with address 15.15.15.1. When we send our packet, it has a sender address 192.168.0.2 and a destination address 15.15.15.1. The default gateway sees the packet and notices it is not for the local network, so it forwards it on Internet through its other TCP/IP interface. If the sender address remains 192.168.0.2, the Web server will respond with packets that have 192.168.0.2 as the destination address, which doesn't exist on Internet, and the response will be lost. Therefore, when the default gateway forwards the packet to the Internet, it must change the sender address with its own public address. The Web server 15.15.15.1 will then respond to the 194.194.194.1 address, which is well known on Internet.

For all eWON® types

Of course, the default gateway needs to keep track of the exchange, so that it can redirect the response to our original host. This process is called Network Address Translation, or simply NAT.

The following diagram synthesizes the packets address modifications using NAT.

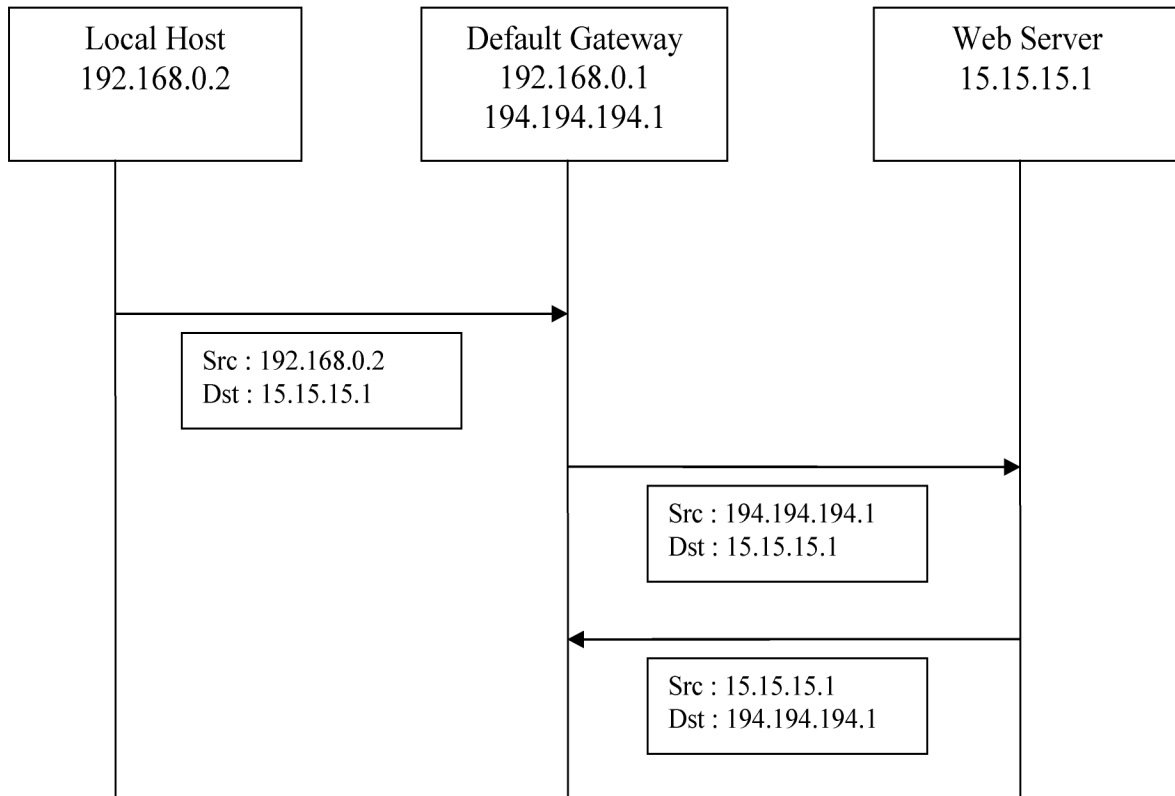


Figure 3: NAT Process

2.7 Port Forwarding

We have seen in the previous section how to access a host with a public address from an internal host. We will now see how to access an internal host from any machine.

2.7.1 Ports

Using only a sender and a destination IP address, it is possible for a single program running on a host A to communicate with a single program running on a host B. However, it should be nice if several programs running on a host could use the network at the same time. This can be achieved by using ports.

A port is an unsigned number which is used with the IP address to communicate with a specific program on a certain host. Ports can be seen as specifying the person when we send a letter to a company instead of just specifying the name and address of the company.

For example, a FTP server (program) can be accessed on port 21, while HTTP server (program) are generally accessed on port 80*. With those two different ports, it is possible to simultaneously download a file via FTP and browse the web pages that are delivered by the same server.

For all eWON® types

A (more) complete IP packet contains four information: the sender IP address and port, and the destination address and port.

Imagine that two applications are running on different hosts. The first application runs on the host with the address 192.168.0.1 and uses the port 1234. The second application runs on the host with the address 192.168.0.2 and uses the port 5678. A packet sent from the first application to the second one will contain the following information:

	Sender	Destination
IP Address	192.168.0.1	192.168.0.2
Port	1234	5678

Table 7: Port forwarding example

The reply will contain the same information with the Sender and Destination swapped.

* Port value for HTTP Web Server, FTP Server, Modbus/TCP Server and Ethernet/IP Server can be redefined since firmware version 4 (**System Setup/Communication/IP Services**).

2.7.2 Redirection

The only way to access an internal host from Internet is to go through a known host with a public address and to be redirected. Imagine we have the following topology:

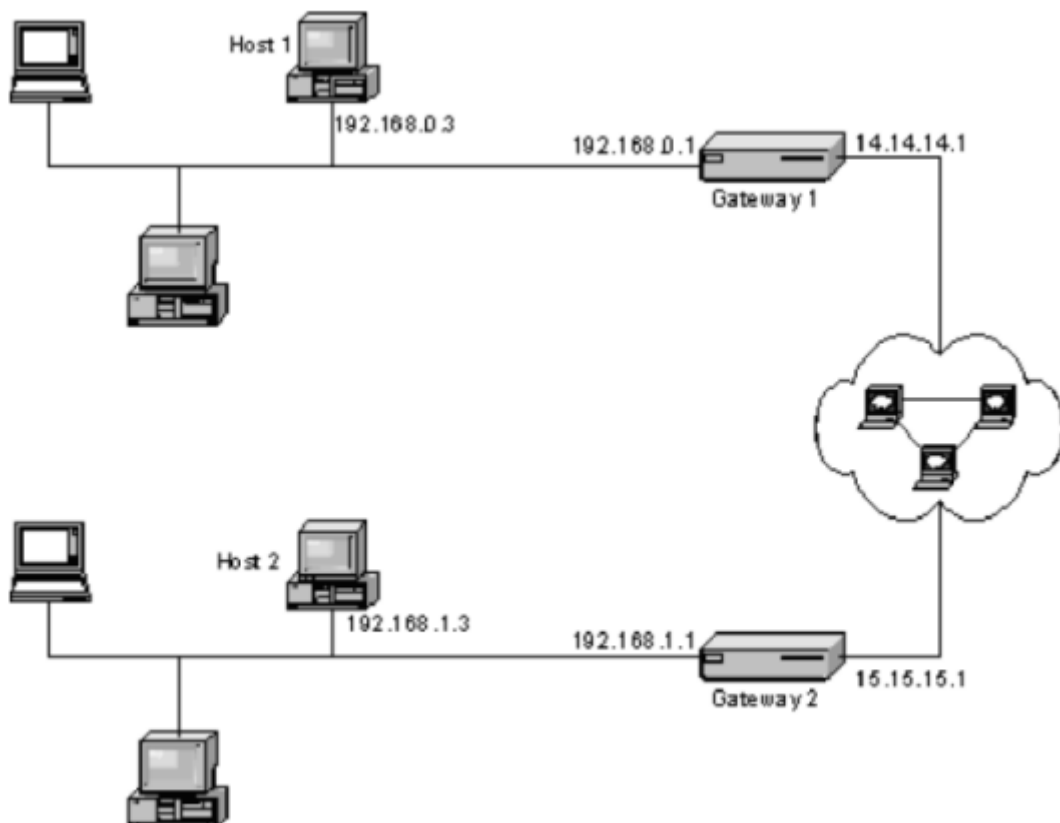


Table 8: Internal host to internal host topology

For all eWON® types

We would like an application running on Host 1 to communicate with Host 2. A way to achieve this would be to configure the Gateway 2 so that whenever it receives a packet from Internet with its address as the destination address, it changes the destination address to 192.168.1.3 and forwards the packet on the internal network. In this way, the destination address given in parameter to the application on Host 1 is simply the Internet address of Gateway 2.

This solution is simple to configure but is not ideal. Indeed, since every packet is forwarded, there is no way to reach Gateway 2 from Internet anymore. It would also be better if we could reach other hosts rather than Host 2 only.

A better technique is for gateway 2 to choose the address to forward the packets to, depending on the destination port. In this way, we could build a rule as: if the destination port is less than 1000, do not forward; if it is in the range 1000 to 5000, forward to Host 2; otherwise, forward to Host 3. This mechanism is called Port Forwarding.

More complicated rules can be set up so that the destination port is changed as well. This can be useful, for example, if we want to reach a web server on Host 2 listening on the standard port 80. We could set up a rule that does the following forwarding:

	Original		Forwarded	
	Sender	Destination	Sender	Destination
IP Address	14.14.14.1	15.15.15.1	14.14.14.1	192.168.1.3
Port	80	1080	80	80

Table 9: Changing port destination value

Notice that the Sender address is 14.14.14.1. This is because Gateway 1 has processed a network address translation. The original destination port is 1080. When forwarded, the destination port becomes 80.

Note: that Host 2 must have Gateway 2 as a default gateway. If not the case, the packet will arrive to Host 2, but when this one will respond, the same "unreachable network" will appear, or (that is worse), it will come with no message!

Some gateway systems (like the eWON) provide an intermediate port forwarding scheme which consists in forwarding every port excepted one. The port which is not forwarded is used to control the gateway itself.

2.8 Firewalls

A firewall is a host that can block and redirect packets following user definable rules. The rules can involve the sender and destination IP address and port. The term "firewall" is often associated with security only, but it can also provide security against intrusion by blocking ports or addresses, and also NAT and port forwarding.

The general rule when setting up a firewall is to block everything excepted the required information. In this way, if we have forgotten something in the configuration, we will not able to act anymore (because the firewall will block our packets), but at least, we don't let an opened door for intruders.

2.9 PPP(oE) Connections

While companies are interested by a fixed IP address on Internet, particulars generally don't need it. Obtaining a fixed IP address and the related quality of service from an Internet Service Provider is rather expensive for particulars (small web sites can be hosted for free or almost). Let's say we are at home and we connect to Internet by calling our ISP with a modem. What happens after the server picks up the phone? First, some hardware parameters like speed will be discussed between the modems, then, an IP connection is established and our desktop computer receives an IP address from the server. You can notice that this address is different *at each connection*. It means that other persons on Internet cannot reach our desktop computer since they don't know our address.

The ADSL or cable modem connections (PPP over Ethernet or PPPoE) have the same limitation since, even if they provide a permanent connection, it is reset at least every 24h by the provider.

2.10 Dynamic DNS

To solve the dynamic IP addressing problem, a special kind of name resolution called *Dynamic DNS* has been set up. Dynamic DNS works like this: an account with a username, a password and an URL (ex: myname.no-ip.org) is created on a dedicated server (ex: no-ip, dyn-dns, ...). The username correspond to your machine. A small program runs in background on your machine and checks the Internet side IP address. If it has changed (the connection has been reset or we have just called the ISP), the program connects to the Dynamic DNS server and informs it of the new IP address. As the username and password are used by the program to log in, the Dynamic DNS knows what URL must be altered and updates its name to the address correspondance table. The standard DNS will see the change and update a few minutes later.

Using Dynamic DNS, it is then possible to have an URL that always points to our home desktop, whatever its address is.