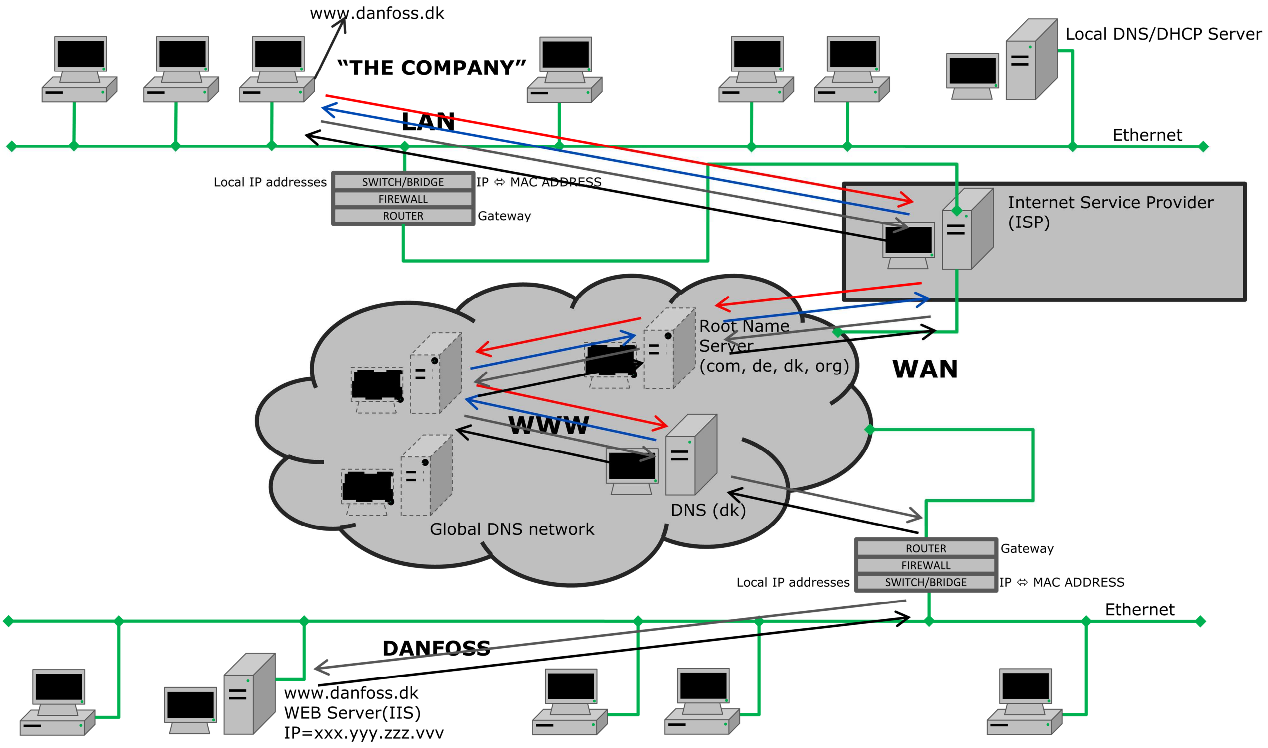
4.2.5 Ethernet and TCP/IP addressing

A typical network



This is a typical picture how companies or their Local Area Networks (LAN) are connected to the Internet(WAN).

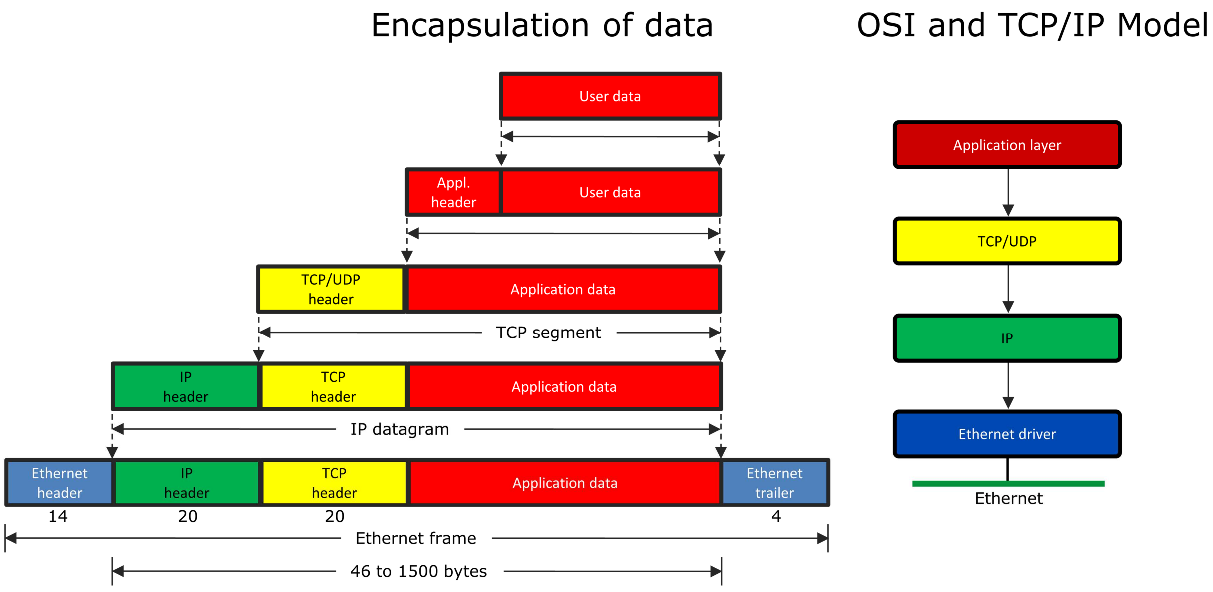
Let's assume that an employee in "The Company" wants' to access the Danfoss homepage www.danfoss.dk.

By doing this he actually initiates a whole series of requests and answers trough several computers and servers. To actually access any computer or web page your computer must know the IP address of the destination computer or server, but you only typed in www.danfoss.dk not the IP address hence a translation from name to IP address must take place. This is handled by Domain Name Servers(DNS) which is a global database network holding information on all domain names and their corresponding IP addresses.

1. When typing in the web address of Danfoss in the internet browser and hitting enter, the first thing that happens is that your request is routed to your Internet Service Provider(ISP)
2. The ISP routes your request to a DNS Root Name Server which is keeping track of all the other DNS servers that holds information on, like in this example, domain names in DK, because your request ended with ".dk". The Root Name Server only know about top level domains like .com, .org, .dk, .de, .uk and so on.
3. The DNS for .dk now searches it's database for danfoss.dk to find the IP address
4. Once if has found the IP address it returns the IP address again trough the same route as the request came from finally ending up at your computer.
5. Now your computer knows the actual IP address of the Server which runs the www.danfoss.dk.
6. Now your computer (by itself) calls the Danfoss web server to fetch the page. But, again, the message is routed through several Servers along the road depending form where in the world you are placed.
7. Finally the WEB server returns the requested page.

Ethernet frame

- Ethernet is standardized as IEEE 802.3 which comprises the physical description of the network, cabling etc. and the frame protocol



This is a picture of how your data (email, web page, TLX PRO data) eventually ends up on the Ethernet. As you can see data are packed in several layers of protocols before being transmitted. User data ends up being wrapped into several layers/protocols to ensure as reliable a transmission as possible
Again comparing to the OSI model you can see how the complete frame is being build.

Ethernet cabling

Network speed, cabling and definitions

Speed [Mbit/Sec]	Distance[m]	Name	Connector	Rec.cable
10	100	10BASE-T	*RJ45	*CAT5, CAT5e, CAT6
100	100	100BASE-T	RJ45	CAT5, CAT5e, CAT6
1000	100	1000BASE-T	RJ45	CAT5e, CAT6
10000	10	10GBASE-T	RJ45	CAT7

- The main difference between CAT5e and CAT6 is internal cable design
  - CAT6 is certified for 1000 Mbit, CAT5e is not but still recommended
  - CAT6 is more immune to crosstalk due to the cable design hence capable of higher speeds like 10Gbit
  - For 1000Mbit CAT5e is sufficient
  - CAT6 only for future proofing
  - CAT7 unnecessary

The table shows the basic specifications for Ethernet cabling. The most common speed today is either 100 Mbit or 1000 Mbit.

What is the difference between 10BASE-T, 100BASE-T and 1000BASE-T?
10BASE-T is the IEEE standard that defines the requirement for sending information at 10 Mbps on unshielded twisted-pair cabling, and defines various aspects of running Ethernet on this cabling.

100BASE-T is the IEEE standard that defines the requirement for sending information at 100 Mbps on unshielded twisted-pair cabling, and defines various aspects of running baseband Ethernet on this cabling.

1000BASE-T (also called gigabit Ethernet) is the IEEE standard that defines the requirement for sending information at 1000 Mbps on unshielded twisted-pair cabling, and defines various aspects of running baseband Ethernet on this cabling

The most commonly used cabling today is CAT5e. The specification of the different cable types is done to enable higher data rates, not due to crosstalk or EMC problems on the same data rate.

Using CAT7 on a 100Mbit or 1000Mbit network doesn't give any performance enhancements.

If you experience problems with noise you should consider revising your installation instead.

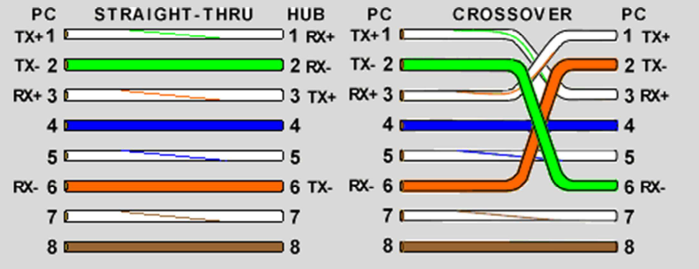
Main diff. compared to CAT5e

- CAT7 Shielding on twisted pairs and the cable as a whole
- CAT6 Internal design, twisting etc. Cable comes shielded and unshielded

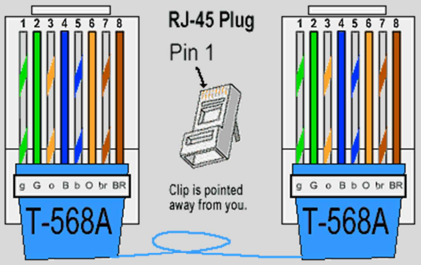
Ethernet cabling plugs

TIA/EIA-568A/B Straight-Through/Crossover Ethernet Cable

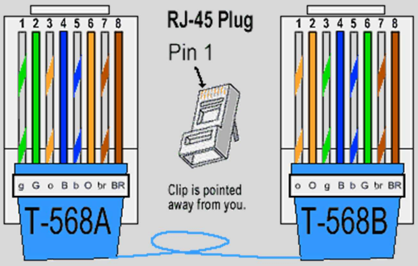
RJ-45 Ethernet Cable colors



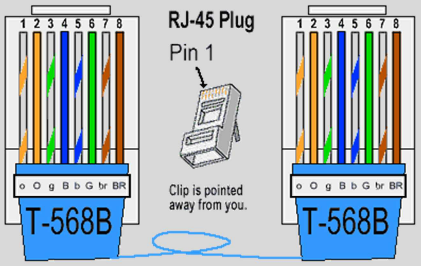
T-568A Straight-Through Ethernet Cable



RJ-45 Crossover Ethernet Cable



T-568B Straight-Through Ethernet Cable



The TIA/EIA 568-A standard which was ratified in 1995 was replaced by the TIA/EIA 568-B standard in 2002 and has been updated since. Both standards define the T-568A and T-568B pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity. The standards and pin-out specification appear to be related and interchangeable, but are not the same and should not be used interchangeably.

Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections. If you require a cable to connect two Ethernet devices directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable instead.

Today, a lot of equipment supports autosense that automatically detects whether straight-trough or crossover cable is applied and adapts accordingly.

A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard. Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires. Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white

- Ethernet Cable Tips:
  - A straight-thru cable has identical ends
  - A crossover cable has different ends
  - A straight-thru is used as a patch cord in Ethernet connections
  - A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs
  - A crossover has one end with the Orange set of wires switched with the Green set
  - Odd numbered pins are always striped, even numbered pins are always solid colored
  - Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left
  - No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk
  - Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

Ethernet cabling recommendations

- Proper installation techniques **must** be applied
  - This is more important than using CAT6 or CAT7 cables
- When connecting cable to the plug do not untwist more wires than absolutely necessary, you open up a door to noise
- Do not:
  - Deform, Bend, Stretch, loop, staple, sharp kinks
  - run parallel with power cables
  - run Ethernet cables near noise inducing components
- Don’t place communication cables closer to power lines than 200mm, preferably in a separate cable tray
- Communication cables can cross power cables when doing so in a 90°angle if necessary (still observing the 200 mm distance)
- Max. Cable length 100 m by standard, but going above 80-90 m EMC problems can arise.
- Shielding to be connected at both ends(if applied)

CONCLUSION
PROPER INSTALLATION TECHNIQUES
MUST BE APPLIED!!!

IP Addressing

IPv4 is the most commonly used addressing format that you see in daily use. Due to the limited address area of IPv4, a new format has been defined the IPv6 which is a 128 bit address
We will not cover IPv6, but this opens up for an almost unlimited no. of addresses, we could all get our own IP address and there would still be plenty left.

- The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. http://www.iana.org/
  - The most commonly used IP addressing version is IPv4
  - IPv4 is the one you always see e.g. 10.5.35.187
  - IPv4 uses 4 bytes (32 bit's) for addressing
  - That enables 4,294,967,296 (2^{32}) possible addresses
    - IPv6(128 bit's)=3,4028×10^{38}= 340282366920938463463374607431768211456 addresses
- The IP address is defined by 4 .(dot) separated bytes
  - The format ranges from 0.0.0.0 to 255.255.255.255

The format enables the definition or segmentation of networks into classes

- 5 classes are defined: A, B, C, D, E
- Within these 5 classes special use addresses are specified where the private network areas are of particular interest
- Local host address range: 127.0.0.0–127.255.255.255 (loopback)

CLASS	IP Address	Network ID	Host Id	Range from	Range To	Default subnet masks	
A	a.b.c.d	a	b.c.d	1.0.0.0	126.255.255.255	255.0.0.0	Large scale networks 2,147,483,648 addresses
B	a.b.c.d	a.b	c.d	128.0.0.0	191.255.255.255	255.255.0.0	Medium sized networks 1,073,741,824 addresses
C	a.b.c.d	a.b.c	d	192.0.0.0	223.255.255.255	255.255.255.0	Small networks 536,870,912 addresses
D	a.b.c.d			224.0.0.0	239.255.255.255		Multicast addresses
E	a.b.c.d			240.0.0.0	254.255.255.255		Reserved for future use

- Class A uses one subnet masking (255.0.0.0)
- Class B uses two subnet masking (255.255.0.0)
- Class C uses three subnet masks (255.255.255.0)

Class A class is for very large networks, such as a major international company might have. IP addresses with a first octet from 1 to 126 are part of this class. The other three octets are used to identify each host.

Class B is used for medium-sized networks. IP addresses with a first octet from 128 to 191 are part of this class. Class B addresses also includes the second octet as part of the Net identifier. The other two octets are used to identify each host.

Class C addresses are commonly used for small to networks. IP addresses with a first octet from 192 to 223 are part of this class. Class C addresses also include the second and third octets as part of the Net identifier. The last octet is used to identify each host.

D and E, we leave out.

Address 127 is local host; 127.0.0.0–127.255.255.255 is used for self test. Try ping this address on your computer and you will get an answer regardless whether you are connected to a network or not. Addresses within this range should never appear outside a host computer and packets sent to this address are returned as incoming packets on the same virtual network device (loopback)

Address masks

Address masks is a property or a tool for network administrators to administer very large networks e.g. the public structure on the Internet or in other large scale networks in companies.

Address mask is used to determine which part is the NETWORK PART and which is the HOST PART.

- Class A uses one subnet masking (255.0.0.0)
- Class B uses two subnet masks (255.255.0.0)
- Class C uses three subnet masks (255.255.255.0)

CLASS	IP Address	Network ID	Host Id	Range from	Range To	Default Address masks	
A	a.b.c.d	a	b.c.d	1.0.0.0	126.255.255.255	255.0.0.0	Large scale networks 2,147,483,648 addresses
B	a.b.c.d	a.b	c.d	128.0.0.0	191.255.255.255	255.255.0.0	Medium sized networks 1,073,741,824 addresses
C	a.b.c.d	a.b.c	d	192.0.0.0	223.255.255.255	255.255.255.0	Small networks 536,870,912 addresses
D	a.b.c.d			224.0.0.0	239.255.255.255		
E	a.b.c.d			240.0.0.0	254.255.255.255		

- Under normal circumstances you will only work in class C networks with the default address mask using the private network area 192.168.0.ddd subnet 255.255.255.0

If you need to apply sub netting you should enter with a network specialist to design the network.

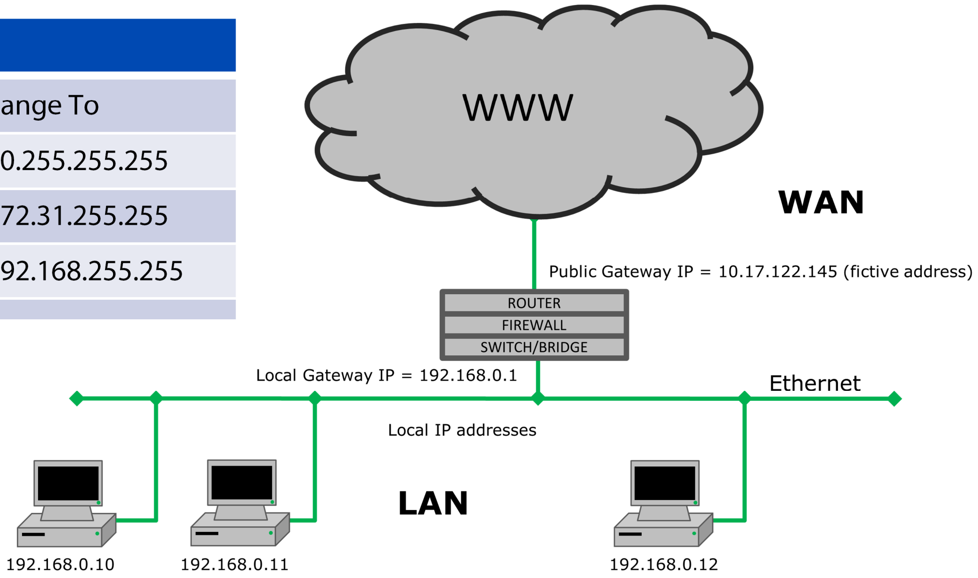
Private network areas

Private network areas are used on the LAN side of a network and are not visible on the Internet because any IP address from the private network areas are automatically blocked by the Router.

- 3 ranges of addresses are reserved for use in private networks
- These ranges are not routable outside of private networks and private machines cannot directly communicate with public networks
- They can, however, do so through network address translation (NAT)

E.g. any address in the area 192.168.ccc.ddd cannot be seen in the Internet.

PRIVATE NETWORK AREAS		
CLASS	Range from	Range To
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



Routers and NAT tables

How can a computer on the LAN side then access the Internet?

Because the Router stores or readdresses the local IP address in a table called Network Access Table (NAT) and then transmits the request but with the IP address from the Routers public side (WAN).

The receiver of the request then transmits back the data that the Router requested. When the Router receives the message it is using the rules stored in the translation tables to transmit the data to the local computer, done.

This method, however, only allows traffic originating from the LAN side since this establishes the translation tables.

A web browser outside could not browse a web site in the masqueraded network. However, most NAT devices today allow the network administrator to configure translation table entries for permanent use.
This feature is often referred to as static NAT or port forwarding and allows traffic from the outside network to reach hosts on the inside.

NAT is like the receptionist in an office. Let's say you have left instructions with the receptionist not to forward any calls to you unless you request it. Later on, you call a potential and leave a message for them to call you back. You tell the receptionist that you are expecting a call from this client and to put them through.

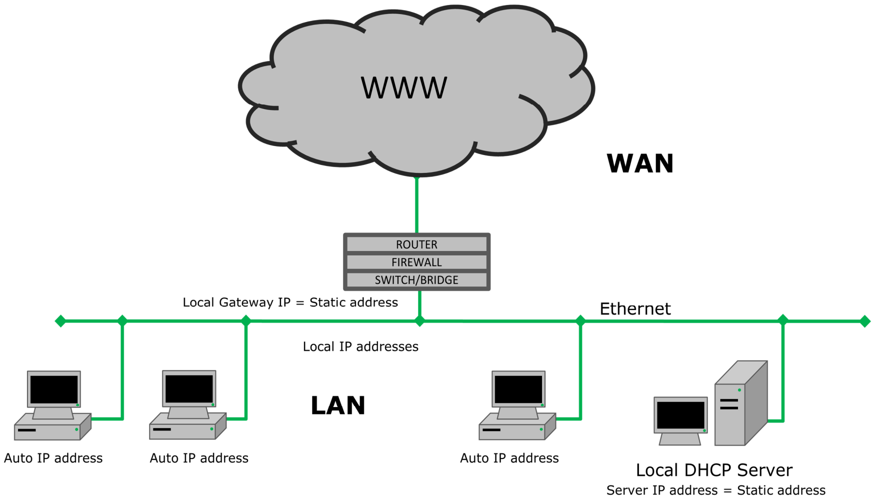
The client calls the main number to your office, which is the only number the client knows. When the client tells the receptionist who they are looking for, the receptionist checks a lookup table that matches up the person's name and extension. The receptionist knows that you requested this call, therefore the receptionist forwards the caller to your extension.

- NAT devices "hide" an entire, private network behind a single public IP address, permitting the use of private addresses within the private network
- Routers typically support this feature
- LAN side components can access the WAN side trough the automatic readdressing done by the Router
- WAN side components can NOT access LAN side without the network administrator configuring a NAT table for permanent use

DHCP servers

Computers that are connected to IP networks must be configured before they can communicate with other computers. **Dynamic Host Configuration Protocol** (**DHCP**) is an auto configuration protocol used on IP networks.

- DHCP is a service running on a Server which automatically configures the Hosts with:
    - IP Address
    - Subnet mask
    - Gateway
    - Others



In the drawing the DHCP Server assigns IP addresses to the Hosts (computers) connected to the local network. The DHCP server has a pool of IP addresses from which it assigns the IP addresses. The addresses can be assigned dynamic or static.

In dynamic addressing the Host most likely will get a different address each time they boot and need an IP address. In static addressing the DHCP Server is configured in such a way that the Hosts on the network are configured with the same IP address always.

In the absence of a DHCP server, the Hosts must be configured with a static IP address of they can use APIPA (**A**utomatic **P**rivate **IP A**ddress)

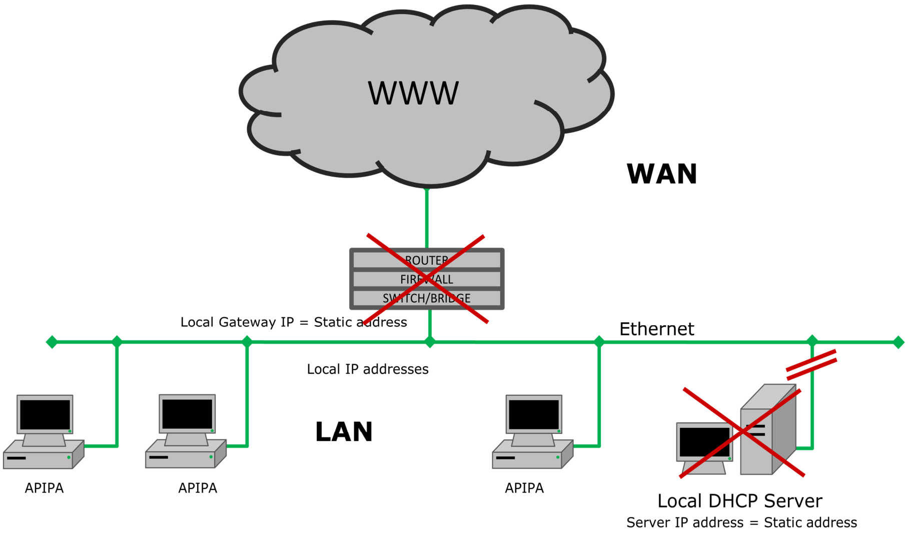
APIPA (Automatic Private IP Address)

When no DHCP server is present in a network IP addresses must be assigned statically by means of APIPA or link-local addressing

With APIPA each host negotiates its own IP address from a predefined pool of IP addresses

- 169.254.1.0 through 169.254.254.255

- Be aware of that your Router most likely isn't a member of the addressing pool for APIPA hence no access to the Internet.



In the absence of a DHCP server, the Hosts must be configured with a static IP address or they can use APIPA (**A**utomatic **P**rivate **IP A**ddress)

When no DHCP server present the Host starts to negotiate IP addresses until all of them has found a address that is unique. Then the network functions, with what is called limited access.

On your computer this will appear on the network Icon below right on Windows computers. An exclamation mark will be visible on the Icon.

This function can be used on the TLX PRO in a local network without DHCP or static addressing

The IANA has reserved the address block 169.254.1.0 through 169.254.254.255 for link-local addressing in IPv4. They are assigned to interfaces by host-internal, i.e. stateless, address auto configuration when other means of address assignment are not available.

In the automatic address configuration process, network hosts select a random candidate address within the reserved range and use Address Resolution Protocl (ARP) probes to ascertain that the address is not in use by another host.

Otherwise, a new address is selected. When a globally routable or a private address become available after a link-local address has been assigned, the use of the link-local address must be discontinued. Microsoft refers to this address auto configuration method as **Automatic Private IP Addressing** (**APIPA**). It is sometimes also casually referred to as **auto-IP**.

Danfoss Solar Inverters A/S

Danfoss Solar Inverters offers a comprehensive range of advanced grid-connected inverters for residential and commercial solar energy applications. The product range also includes solutions for monitoring the solar system in order to achieve optimal energy output and return on investment.

Energy–saving products and solutions have always been a core competence and now renewable energy generation is added to the Danfoss portfolio of products making modern living possible. Danfoss has 40 years of experience in power electronics technology; solar inverters and frequency converters are technologically closely related.

Contact information

Main web page
www.danfoss.com/solar

Service and hotline information

http://www.danfoss.com/BusinessAreas/Solar+Energy/Service/

Call our Hotline and let us take care of the rest.
We speak five languages – English, German, French, Spanish and Italian – and know exactly how to provide the technical support you need.

High speed inverter Exchange Service
If an exchange inverter is required, we guarantee that it is shipped as soon as possible and within no more than 24 hours.

On-Site Service
If the service issue cannot be solved by our Hotline guidance or Exchange Service, our experienced On-Site service teams are prepared for the task, which is initiated within 24 hours.

Call our Hotline and we will find the easiest and fastest way ensuring that your system is up and running.

Hotline numbers

English:	+ 45 7488 1349
German:	+ 49 (0) 69 8902 454
Italian:	800 29 10 60
French:	0820201043
Spanish:	+34 91 383 0455