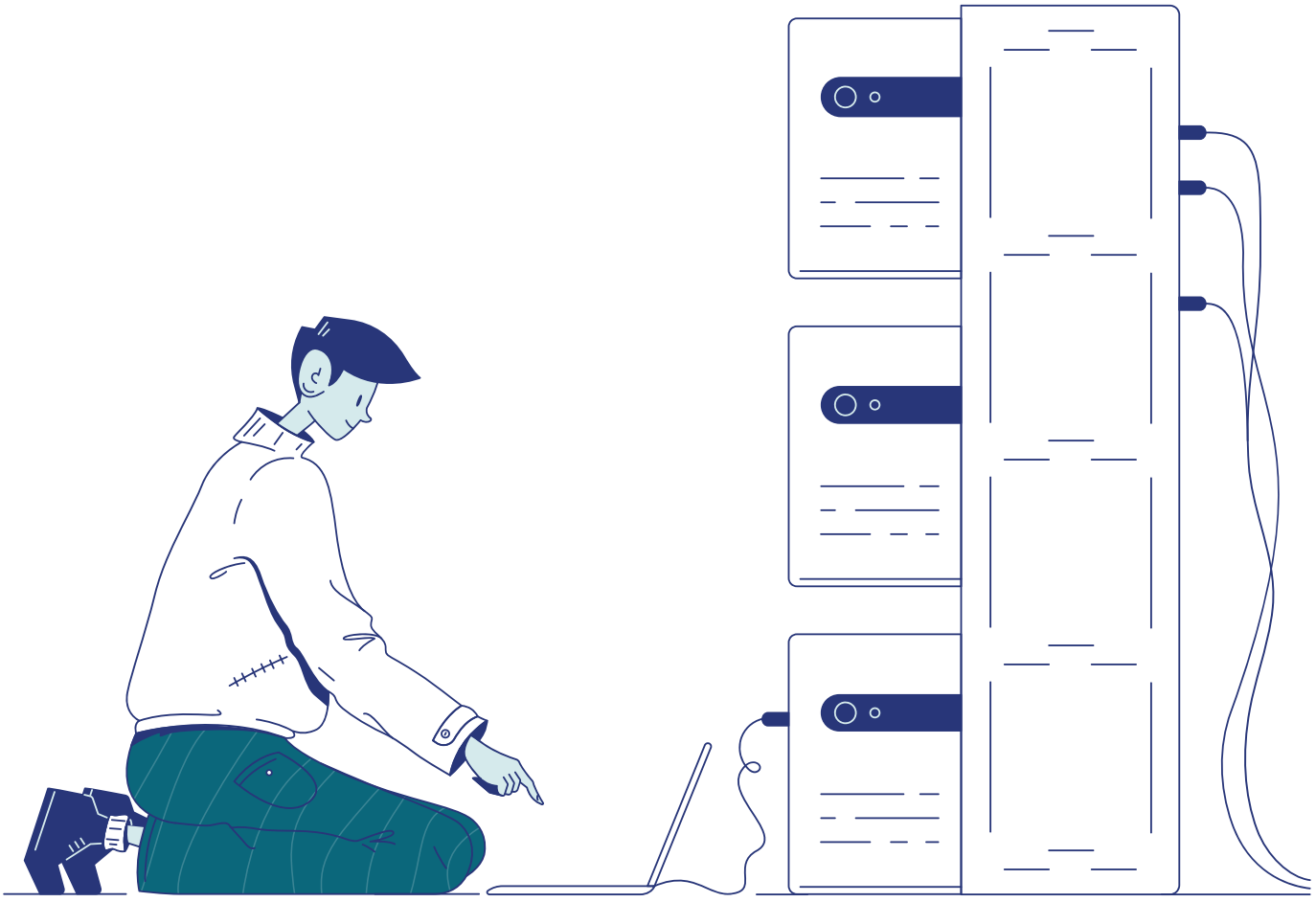
OYSTER™ NEXT

INFRASTRUCTURE NETWORK INSTALLATION

Manual for secure installation of the ON® network



ON® Technology

INDEX

1. Topics covered

This manual addresses the technical figure of the installer and explains how to better prepare the network infrastructure to accommodate the next ON infrastructure.

2. The steps of installing an ON infrastructure

The installer must take care of a series of procedures that can be divided into three macro-phases:

- Network construction: the implementation of the network infrastructure where ON devices will operate and communicate with each other
- Installation of ON devices: the connection of ON devices to the network that is predisposed to the infrastructure.
- ON infrastructure configuration: configuration and possibly programming of the ON infrastructure.

This manual will deal mainly with the first of the three phases.

3. Introduction to the systemic part of ON

To connect devices, ON is based on a LAN (Ethernet and/or Wi-Fi)

Each ON device can be free to communicate with any other via direct TCP and/or UDP connections without going through an intermediary, since ON has a strongly decentralised architecture and therefore uses a mesh network topology for inter-device communication.

Each ON device uses DHCP for automatic IP assignment and communication with a given device is done only by knowing the device-ID* when each device can set its hostname within the network: once a device has established the connection and received its IP, it can be reached on the network by pointing to the host with the name "on-<id device>".

**an integer that uniquely defines a given device*

4. Network construction

The network that will host ON can be built either using the network devices offered by Oyster (routers, firewalls, VPNs, etc.), which greatly simplify this first stage since all are already provided with a preconfiguration can offer the basic features to be able to move immediately to the next stage, both using any other third-party solution.

Regardless of how the network is implemented, the installer must ensure that it meets the following requirements:

- **Have the DHCPv4 implemented:** DHCPv6 is not supported;

- **Have the DNS server implemented:** the installer must pay attention to the possible presence of the FQDN set arbitrarily by the DNS server;

- **All hosts affected by the ON ecosystem must be able to communicate with all others:** being a decentralized architecture it is important that the technician ensures that each device can be able to start TCP connections (or UDP broadcast for some functions) to the other devices;

- **The network shall be wiretap-proof:** ON does not use cryptography at the application level in intra-network communication between devices, given the superfluity and the inability to offer real security in the intra-network context (the technical reasons will be explained in the following chapters), and also to allow smoothly third-party implementations. However, encryption is used (and is mandatory), instead, when it must interface outwards, so it will be the installer's task to manage security from the network (the procedures related to this point will be explained later). In essence, the internal network must prevent any man-in-the-middle attack through physical (and not only) access to network devices and ON devices.

5. Guidelines on Cybersecurity

Guidelines to build a network that offers robust security in the face of potential attacks will now be presented. These networks can be either wired networks or Wi-Fi networks.
Cybersecurity within the ON ecosystem can be divided into two macro-levels:

- Application security: Refers to the level of security for applications implemented by Oyster. In this case, the responsibility lies with Oyster.
- Network security: Refers to the level of security related to any or potential cyber attacks. In this case, the installer is responsible for security.

In order to know exactly where the responsibility of the technician lies in managing safety (or in which macro-level the responsibility falls) it is sufficient that at least one of the following conditions is true:

- Security can be breached through physical access to infrastructure;
- Security can be breached by intercepting network traffic (even passively);
- Security depends on credentials.

5.a In all cases

ON devices and network devices should not be easily accessible to the public* as sabotage of any networked equipment could compromise the integrity of the entire infrastructure, regardless of any security measures implemented at the software level.

The first rule that the installer must follow in the design and implementation of this network is that in addition to the ON devices and network devices capable of composing the functionality of that network, No other device outside the ON infrastructure shall be connected to this network. All third-party implementations will fall under the exclusive responsibility of the installer.

If within the same network there is ON and there are also the computers of the employees of a company, the network is considered compromised at the start.

**all persons who do not have the role of administrator of an infrastructure*

An exception can be made in a "home environment" where the end user does not have particular security needs and its possible home wireless network still has a minimum of security thanks to the standard use of WPA2, then it is the user's responsibility to decide what to connect to their home network, if of course you decide to install ON directly in the network where smarphone and various computers are connected all together (however not optimal approach, we recommend instead the implementation of a DMZ).

The use of IDS (Intrusion Detection System) and network equipment that already have built-in security measures (many switches have systems to counter attacks such as ARP Poisoning) should not be considered as safe as the rules described in this manual. If for some reason you want to violate some security rules present in this documentation, to integrate other solutions considered more secure, the responsibility will be exclusively of the installer.

5.a.1 Ethernet wired network (LAN) case

In order to create a secure network, it is essential not to leave the RJ45 ports of ON devices and network devices easily accessible to outsiders.

In fact, even if strong encryption is used in network communications, access to a simple switch by a malicious user is enough to completely tamper with the ON infrastructure through dos (Denial of Service) attacks working on ISO/OSI level 2 (e.g. ARP Poisoning).

Thus, within the case of the wired ethernet network, security will have to be managed physically.

Here are some practical examples:

- No switches available to the public: cables should be allowed through walls, avoiding leaving entry points or "flying cables" lying around;

- Try as much as possible to make the RJ45 connector of connected devices difficult to reach and, consequently, to sabotage.

5.a.2 Wi-Fi (WLAN) case

In this case, the essential element is that the **Wi-Fi network must be strongly encrypted**.
Solutions like the WPA2 Personal are considered adequate and represent the best choice (safe and at the same time simple).

On the other hand, solutions such as WEP, or others that use encryption protocols considered weak, are strongly discouraged.

We recommend that you pay close attention to repeaters and access points, which could create security problems with the poorly integrated WPS. Finally, as stated also for the previous case, avoid leaving the RJ45 ports (many access points have the integrated switch) easily accessible.

6. Note