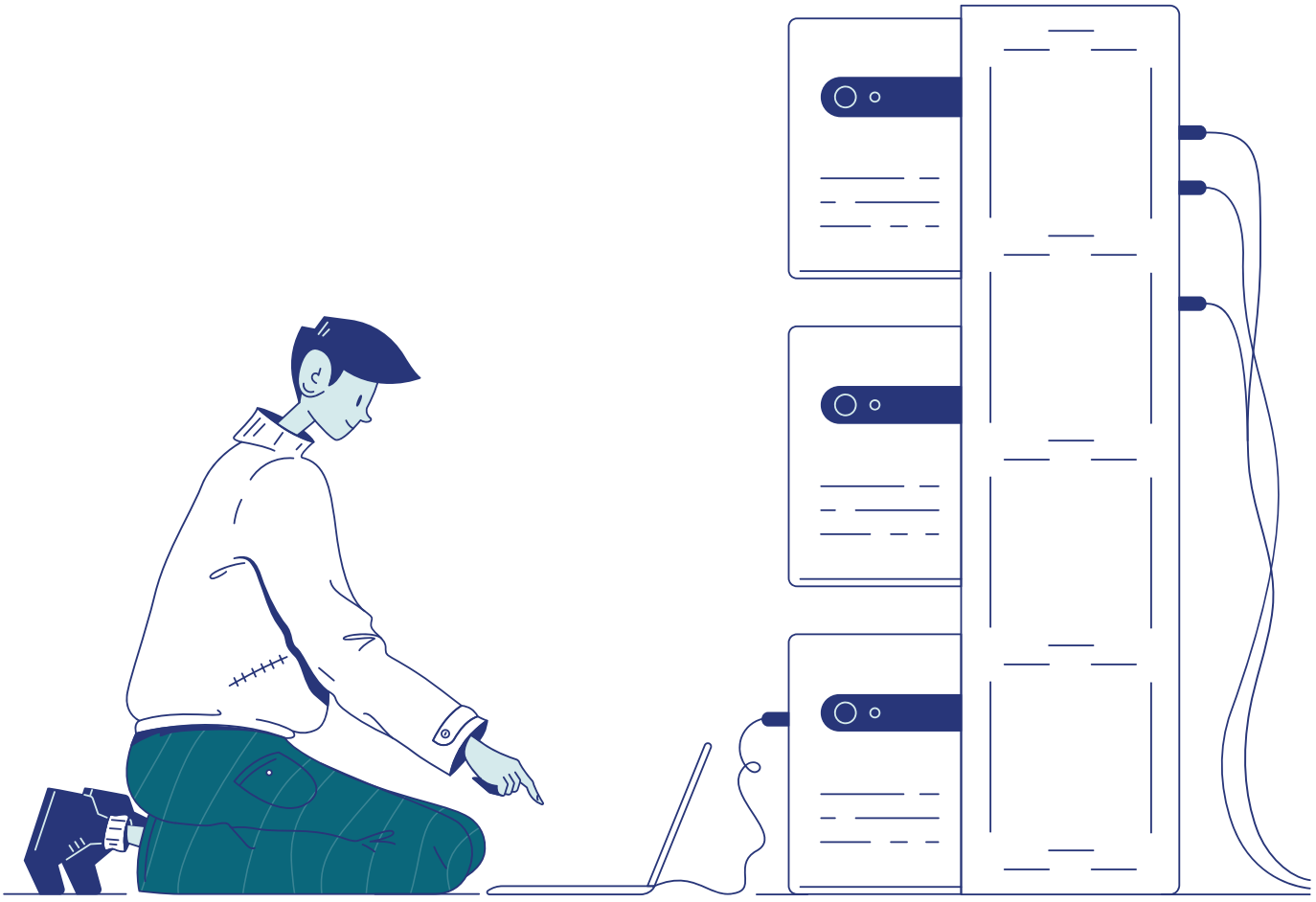
OYSTER™ NEXT

INSTALLAZIONE INFRASTRUTTURA DI RETE

Manuale per l'installazione sicura della rete ON®



ON® Technology

INDICE

1. Temi trattati

Questo manuale si rivolge alla figura tecnica dell'installatore e spiega come preparare al meglio l'infrastruttura di rete per accogliere la successiva infrastruttura ON.

2. Le fasi dell'installazione di un'infrastruttura ON

L'installatore dovrà incaricarsi di una serie di procedure che si possono suddividere in tre macro-fasi:

- **Costruzione della rete:** l'implementazione dell'infrastruttura di rete dove i dispositivi ON opereranno e comunicheranno tra loro
- **Installazione dei dispositivi ON:** la connessione dei dispositivi ON alla rete che è predisposta all'infrastruttura.
- **Configurazione dell'infrastruttura ON:** la configurazione ed eventualmente la programmazione dell'infrastruttura ON.

In questo manuale verrà trattata principalmente la prima delle tre fasi.

3. Introduzione alla parte sistemistica di ON

Per la connessione dei dispositivi, ON si appoggia su una rete LAN (Ethernet e/o Wi-Fi).

Ogni dispositivo ON può essere libero di comunicare con qualsiasi altro tramite connessioni TCP e/o UDP dirette senza passare per un intermediario, dal momento che ON ha un'architettura fortemente decentralizzata e quindi utilizza applicativamente una topologia di rete a maglia per la comunicazione tra dispositivi.

Ogni dispositivo ON utilizza il DHCP per l'assegnazione automatica dell'IP e la comunicazione con un dato dispositivo avviene tramite la sola conoscenza dell'ID-dispositivo* qual'ora ogni dispositivo riesca a settare il proprio hostname all'interno della rete: una volta che un dispositivo ha stabilito la connessione e ha ricevuto il suo IP, potrà essere raggiungibile sulla rete puntando all'host con nome "on-<id dispositivo>".

*****un numero intero che definisce in modo univoco un dato dispositivo*

4. Costruzione della rete

La rete che ospiterà ON può essere costruita sia utilizzando i dispositivi di rete offerti da Oyster (router, firewall, VPN, ecc.), che semplificano enormemente questa prima fase dal momento che tutti vengono già forniti con una preconfigurazione in grado di offrire le features base per poter passare subito alla fase successiva, sia utilizzando qualsiasi altra soluzione di terze parti.

Indipendentemente da come verrà implementata la rete, l'installatore si dovrà assicurare che essa rispetti le seguenti caratteristiche:

- **Avere il DHCPv4 implementato:** il DHCPv6 non è supportato;

- **Avere il DNS server implementato:** l'installatore dovrà prestare attenzione ell'eventuale presenza dell'FQDN impostato arbitrariamente dal DNS server;

- **Tutti gli host interessati dall'ecosistema ON devono poter comunicare con tutti gli altri:** essendo un'architettura decentralizzata è importante che il tecnico si assicuri che ogni dispositivo possa essere in grado di avviare delle connessioni TCP (o UDP broadcast per alcune funzioni) verso gli altri dispositivi;

- **La rete deve essere a prova di intercettazione:** ON non fa utilizzo della crittografia a livello applicativo nella comunicazione intra-rete tra dispositivi, data la superfluità e l'incapacità di offrire reale sicurezza nel contesto intra-rete (le ragioni tecniche verranno esposte nei capitoli successivi), e anche per consentire agevolmente implementazioni di terze parti. La crittografia è però utilizzata (ed è obbligatoria), invece, quando deve interfacciarsi verso l'esterno, pertanto sarà compito dell'installatore gestire la sicurezza a partire dalla rete (le procedure relative a questo punto verranno esposte in seguito). In sostanza, la rete interna deve impedire qualsiasi **attacco man-in-the-middle tramite accesso fisico (e non solo)** ai dispositivi di rete e ai dispositivi ON.

5. Linee guida sulla sicurezza informatica

Verranno ora esposte delle linee guida da seguire per costruire una rete in grado di offrire una robusta sicurezza di fronte a dei potenziali attacchi.
Le reti in questione possono essere sia reti cablate, sia reti Wi-Fi.

La sicurezza informatica all'interno dell'ecosistema ON si può dividere in due macro-livelli:

- **Sicurezza applicativa:** fa riferimento al livello di sicurezza riguardante le applicazioni implementate da Oyster. In questo caso, la responsabilità è a carico di Oyster.
- **Sicurezza della rete:** fa riferimento al livello di sicurezza riguardante eventuali o potenziali attacchi informatici. In questo caso, la sicurezza è a carico dell'installatore.

Per sapere con precisione dove ricade la responsabilità del tecnico nel gestire la sicurezza (ovvero in quale macro-livello ricade la responsabilità) è sufficiente che almeno una delle seguenti condizioni sia vera:

- La sicurezza può essere violata grazie all'accesso fisico all'infrastruttura;
- La sicurezza può essere violata intercettando il traffico di rete (anche in modo passivo);
- La sicurezza dipende dalle credenziali.

5.a In tutti i casi

I dispositivi ON e i dispositivi di rete **non devono essere facilmente raggiungibili dal pubblico*** dal momento che il sabotaggio di un qualsiasi apparato connesso in rete potrebbe compromettere l'integrità di tutta l'infrastruttura, indipendentemente dalle eventuali misure di sicurezza implementate a livello software.

La prima regola in assoluto che l'installatore deve seguire nella progettazione e nell'implementazione di questa rete è che oltre ai dispositivi ON e ai dispositivi di rete atti a comporre le funzionalità di tale rete, **nessun altro dispositivo fuori dell'infrastruttura ON deve essere collegato a questa rete.** Tutte le implementazioni di terze parti ricadranno sotto l'esclusiva resposabilità dell'installatore.

Se all'interno di una stessa rete è presente ON e sono presenti anche i computer degli impiegati di un'azienda, la rete è da considerarsi **compromessa in partenza.**

**tutte le persone che non hanno il ruolo di amministratore di un'infrastruttura*

Un'eccezione può essere fatta in un "ambiente domestico" dove l'utente finale non ha particolari esigenze in termini di sicurezza e la sua eventuale rete wireless domestica possiede comunque un minimo di sicurezza grazie all'utilizzo standard del WPA2, allora è responsabilità dell'utente decidere cosa connettere alla propria rete domestica, qualora ovviamente si deciderà di installare ON direttamente nella rete dove smarphone e computer vari sono connessi tutti insieme (approccio comunque non ottimale, si consiglia invece l'implementazione di una DMZ).

L'utilizzo di IDS (Intrusion Detection System) e apparati di rete che hanno già delle misure di sicurezza integrate (molti switch hanno sistemi per contrastare attacchi come l'ARP Poisoning) non devono essere ritenuti sicuri quanto le regole descritte in questo manuale. Se per qualche ragione si vuole violare alcune regole di sicurezza presenti all'interno di questa documentazione, per integrare altre soluzioni reputate maggiormente sicure, **la responsabilità sarà esclusivamente dell'installatore.**

5.a.1 Caso di rete cablata ethernet (LAN)

Per creare una rete sicura è fondamentale **non lasciare le porte RJ45 dei dispositivi ON e dei dispositivi di rete facilmente accessibili** agli estranei.

Infatti, anche se si utilizzasse la crittografia forte nelle comunicazioni di rete, l'accesso ad un semplice switch da parte di un utente malevolo è sufficiente per manomettere completamente l'infrastruttura ON tramite attacchi DoS (Denial of Service) che lavorano sul livello 2 dell'ISO/OSI (ad es. ARP Poisoning).

Quindi, all'interno del caso della rete cablata ethernet, la sicurezza dovrà essere gestita a livello fisico.

Si presentano di seguito alcuni esempi pratici:

- Assenza di switch a disposizione del pubblico: i cavi dovrebbero essere fatti entrare attraverso i muri, evitando di lasciare punti di ingresso o "cavi volanti" in giro;

- Cercare quanto più possibile di rendere il connettore RJ45 dei dispositivi connessi difficile da raggiungere e, di conseguenza, da sabotare.

5.a.2 Caso di Wi-Fi (WLAN)

In questo caso, l'elemento imprescindibile è che **la rete Wi-Fi deve essere criptata in modo forte**. Soluzioni come il **WPA2 Personal** sono ritenute adeguate e rappresentano la scelta migliore (sicura e al tempo stesso semplice).

D'altra parte, soluzioni come il WEP, o altre che utilizzano protocolli di cifratura considerati deboli, sono fortemente sconsigliate.

Si consiglia di prestare grande attenzione ai ripetitori e agli access point, i quali potrebbero creare problemi di sicurezza con il WPS integrato male. Infine, come precisato anche per il caso precedente, evitare di lasciare le porte RJ45 (molti access point abbiano lo switch integrato) facilmente accessibili.

6. Note