Dispensa e video per FAD: stima durata del lavoro complessivo pari a 4 ore.

Verifica con test a risposta multipla in data da definire alla fine della sospensione delle attività didattiche

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

Prof.ssa Agnese Di Donato

Video
MODULO 5 SEZIONE 3_SICUREZZA IN RETE
https://www.youtube.com/watch?v=1Cgyl91m_Ig
Durata: 21:37 min

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

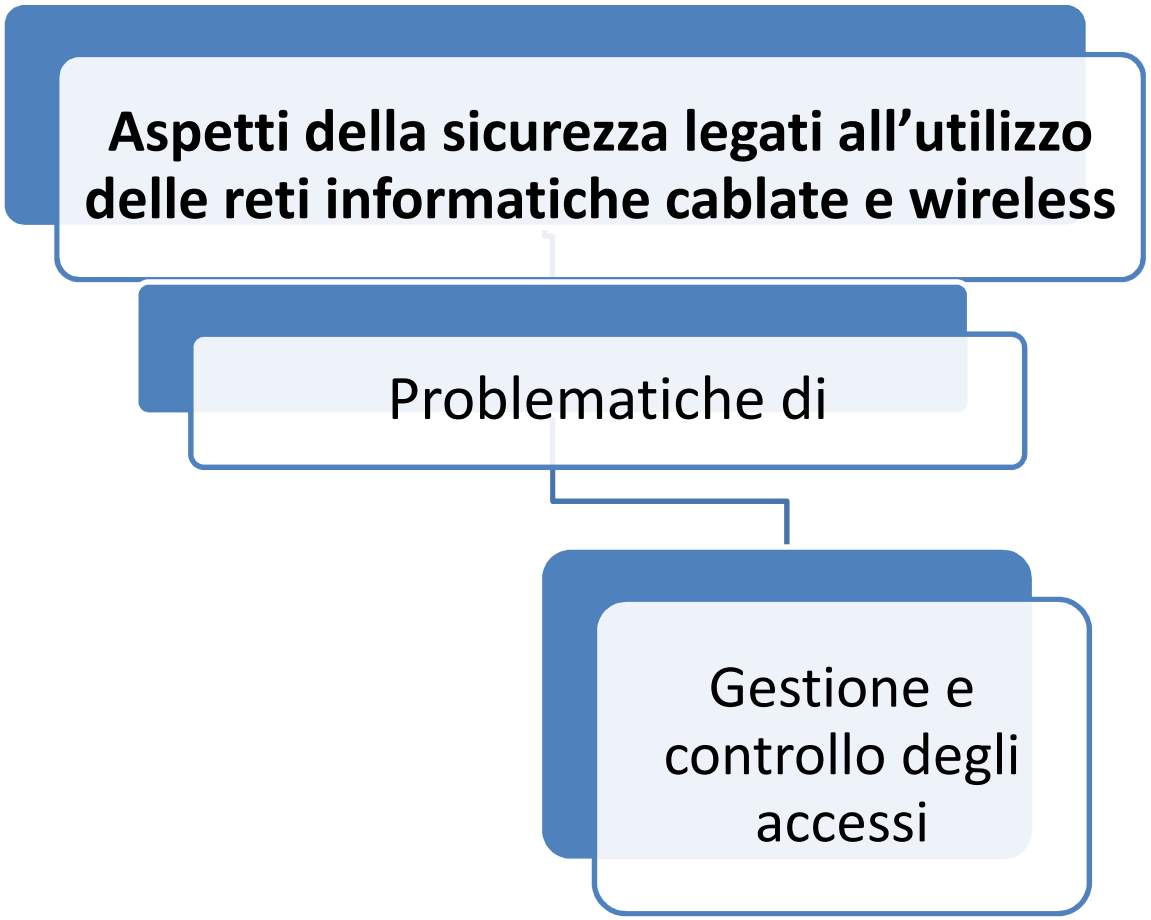
1. CONCETTI DI SICUREZZA
2. MALWARE
3. SICUREZZA IN RETE
4. CONTROLLO DI ACCESSO
5. USO SICURO DEL WEB
6. COMUNICAZIONI
7. GESTIONE SICURA DEI DATI

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

SEZIONE 3
SICUREZZA IN RETE

Prof.ssa Agnese Di Donato

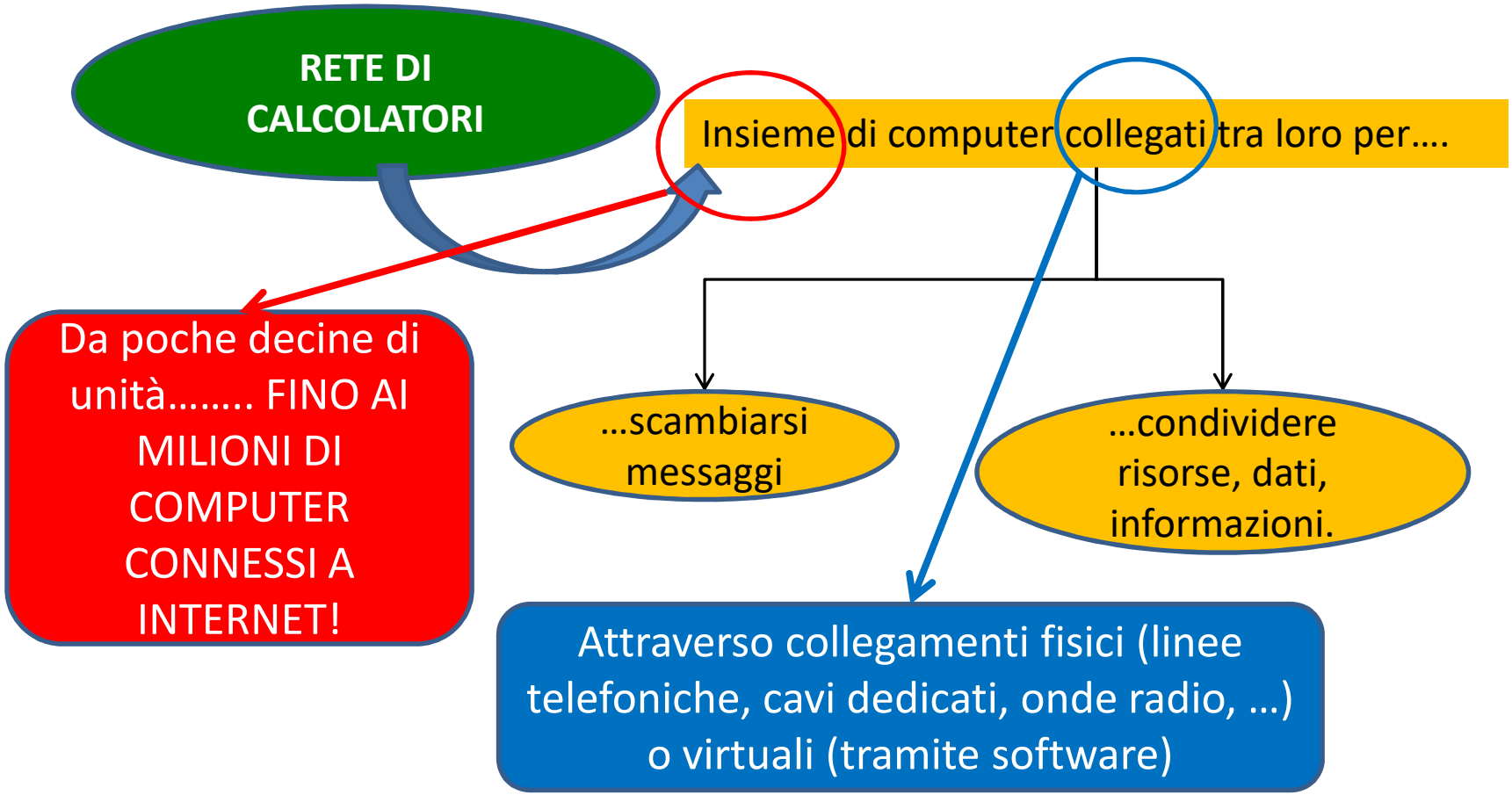
SEZIONE 3 – SICUREZZA IN RETE



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete



SEZIONE 3 – SICUREZZA IN RETE

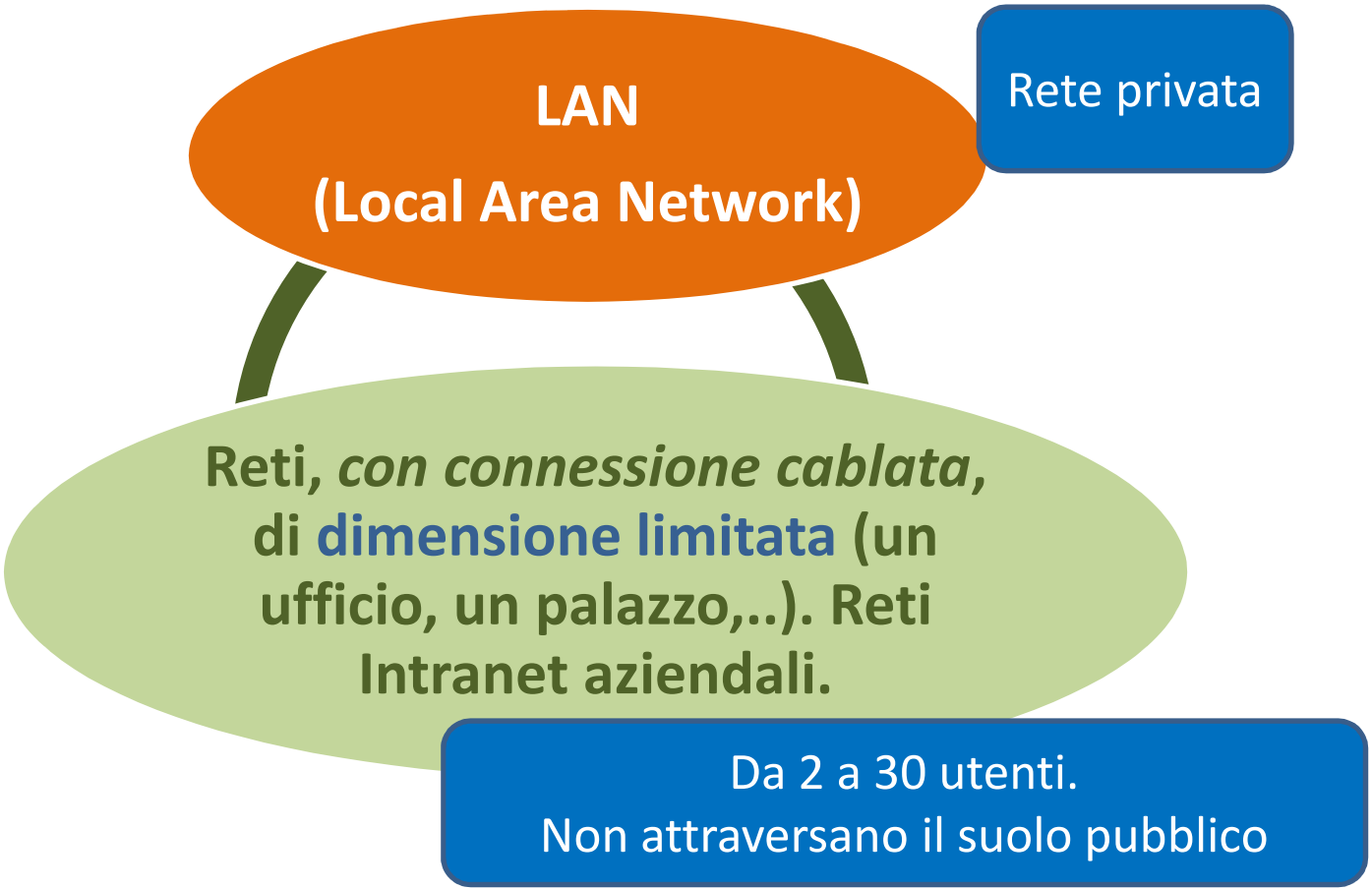
TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

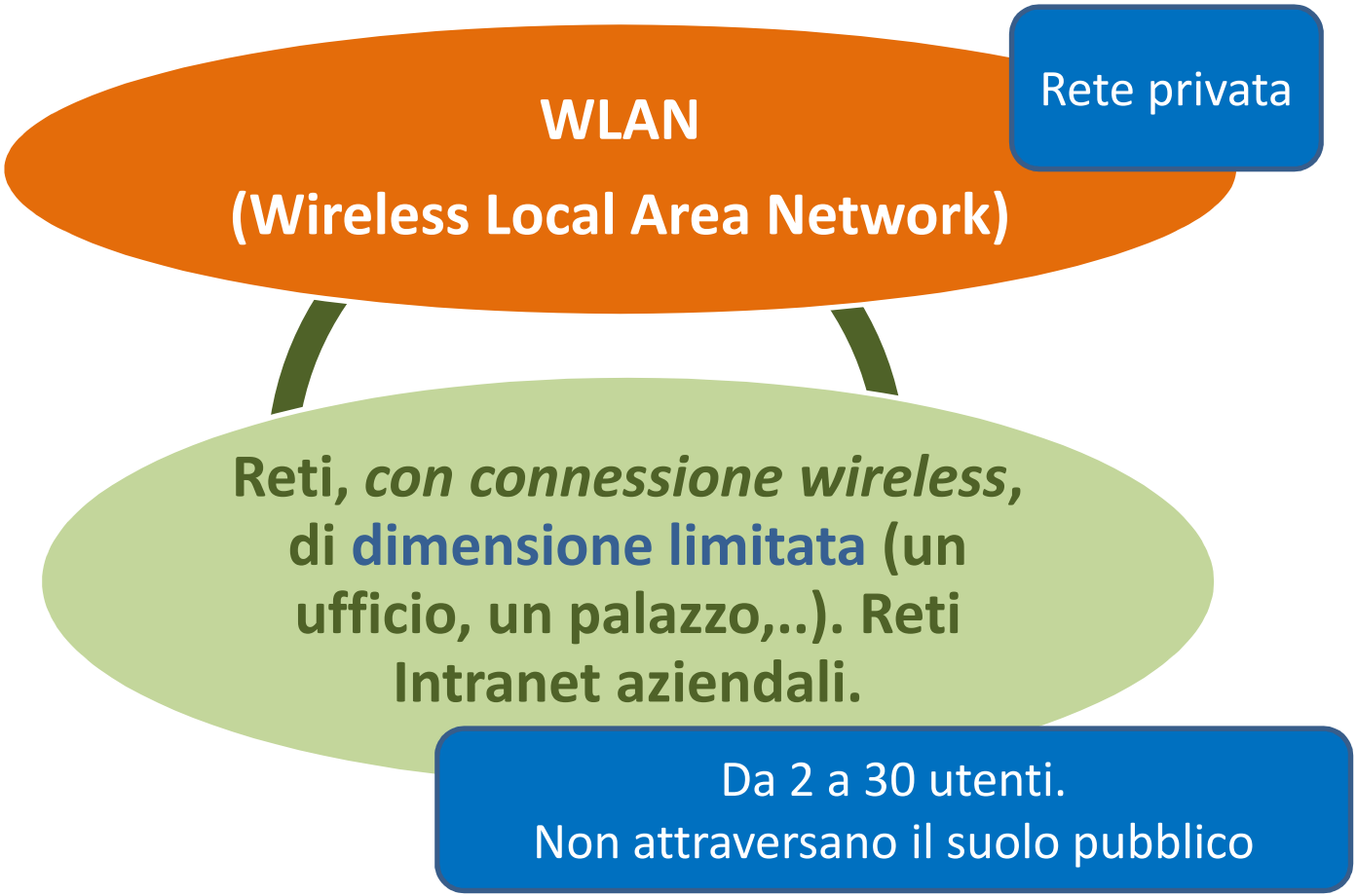
Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete



SEZIONE 3 – SICUREZZA IN RETE

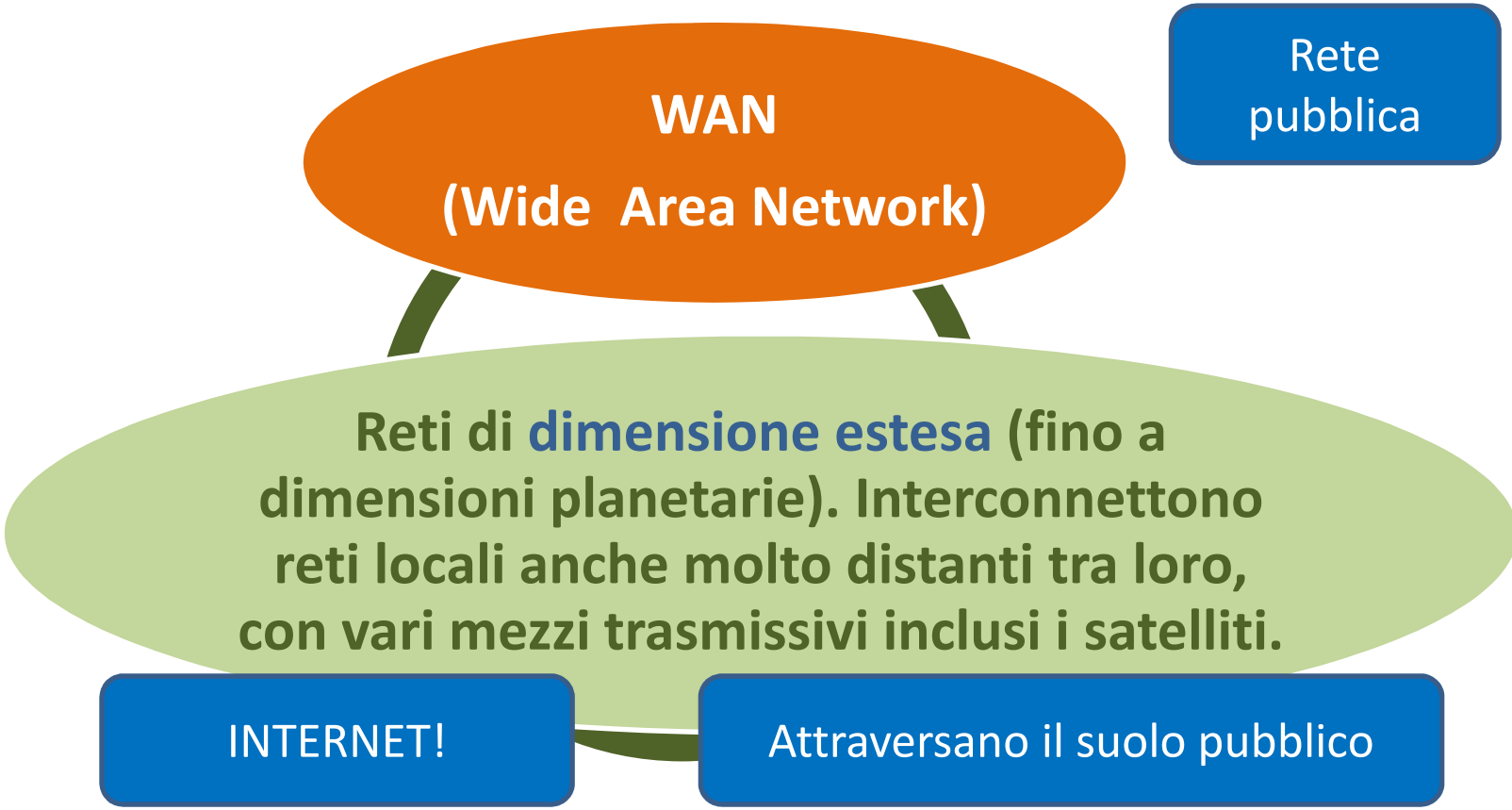
TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.1 Comprendere il termine “rete” e riconoscere i più comuni tipi di rete

VPN

(Virtual Private Network)

Rete privata che sfrutta una rete pubblica (Internet)

Virtuale, perché non c’è connessione fisica tra le reti, bensì virtuale, tramite software

Collegano, tramite un protocollo di comunicazione *con connessione cifrata*, reti locali geograficamente distanti utilizzando una rete WAN come mezzo di collegamento

Possono attraversare il suolo pubblico

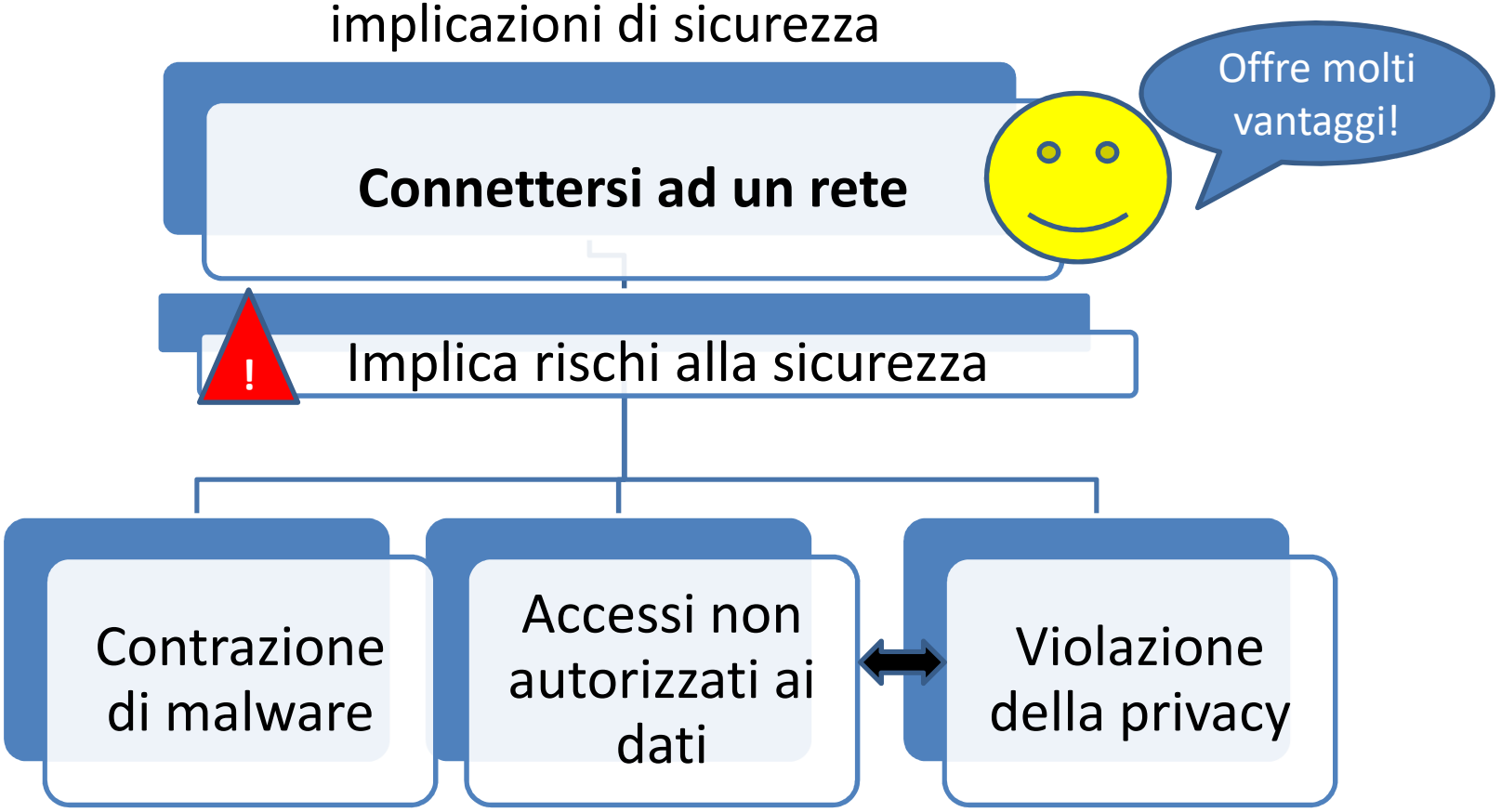
Privata: necessita di *autenticazione all’accesso,* in modo che l’utilizzo sia concesso solo ad utenti autorizzati

Es.: azienda che permette di lavorare da casa tramite client VPN, con stessi diritti di accesso, come se si fosse in ufficio; o collegamento tra uffici di stessa azienda in luoghi diversi,...

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.2 Comprendere che la connessione ad una rete ha implicazioni di sicurezza



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete

Cos'è un dominio?

Un dominio è un **nome globalmente unico e distinto** per un settore di internet ben determinato, per esempio un sito web. Agli utenti i domini appaiono in questa forma:

www.esempio.com

Come parte essenziale di un URL (abbreviazione di Uniform Resource Locator) il dominio indica dove si trova una risorsa all'interno di un **DNS** (in italiano "**sistema dei nomi di dominio**") gerarchicamente strutturato. La traduzione dei domini negli indirizzi IP avviene grazie ai cosiddetti name server. Si tratta di web server specializzati a cui è affidata la **risoluzione del nome di indirizzi IP**. Questo servizio funziona in modo simile a un normale servizio telefonico: un utente inserisce il dominio *www.esempio.com* nella maschera di ricerca del suo browser e questo invia una richiesta al name server di competenza. Qui viene richiamata la voce inserita *www.esempio.com* dalla banca dati e viene trasmesso al browser l'indirizzo IP digitato.

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete

Ogni persona che utilizza il computer all'interno di un dominio riceve un account o un nome utente univoco e ad ogni account può essere assegnato il grado di accesso alle risorse disponibili all'interno del dominio secondo dei criteri di gruppo assegnati dall'amministratore di sistema.

Attraverso un dominio web possiamo avere un nostro sito ospitato su un computer, detto server, che resta acceso perennemente per permettere ai visitatori di accedervi. Servono potenti linee adsl che permettano la navigazione di più persone contemporaneamente e che diano nello stesso tempo una certa velocità di navigazione.

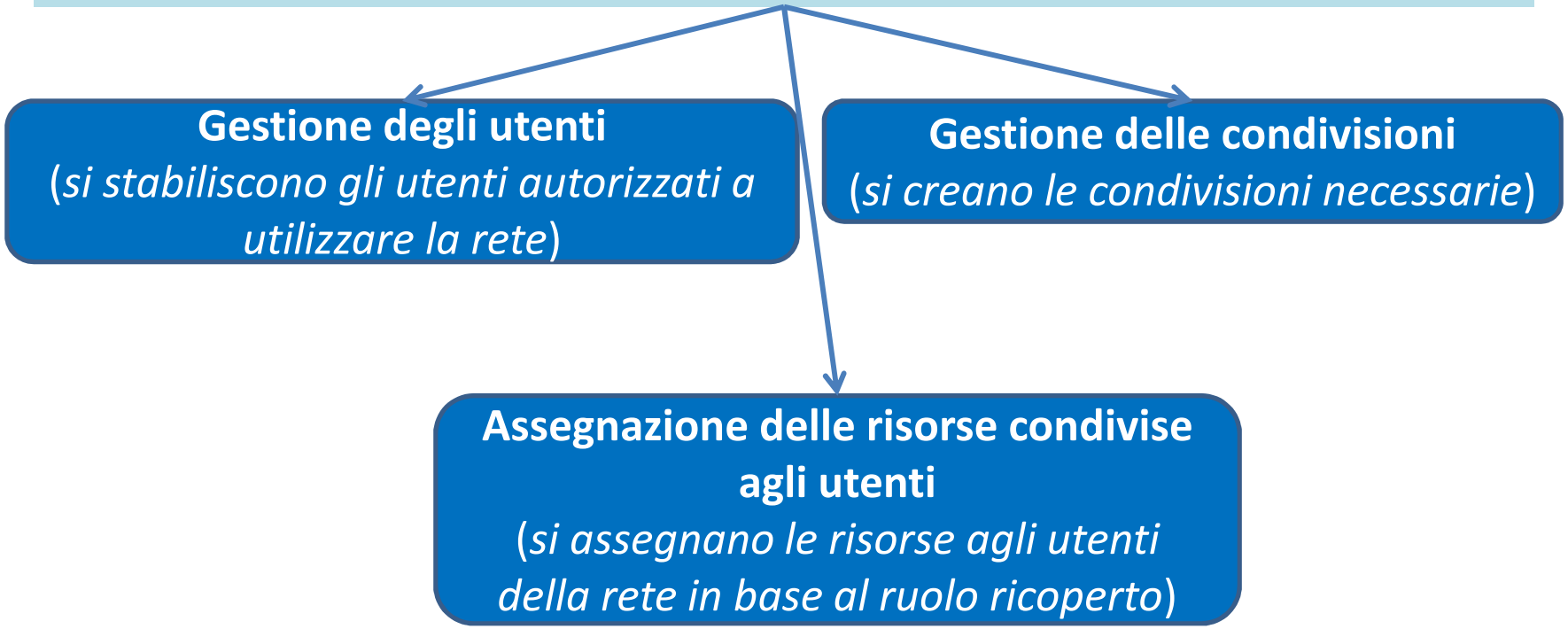
Un **domain controller** (DC) è un server che, nell'ambito **di un dominio**, gestisce le richieste di autenticazione per la sicurezza (login, controllo dei permessi, ecc.) e organizza la struttura del **dominio.**

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete

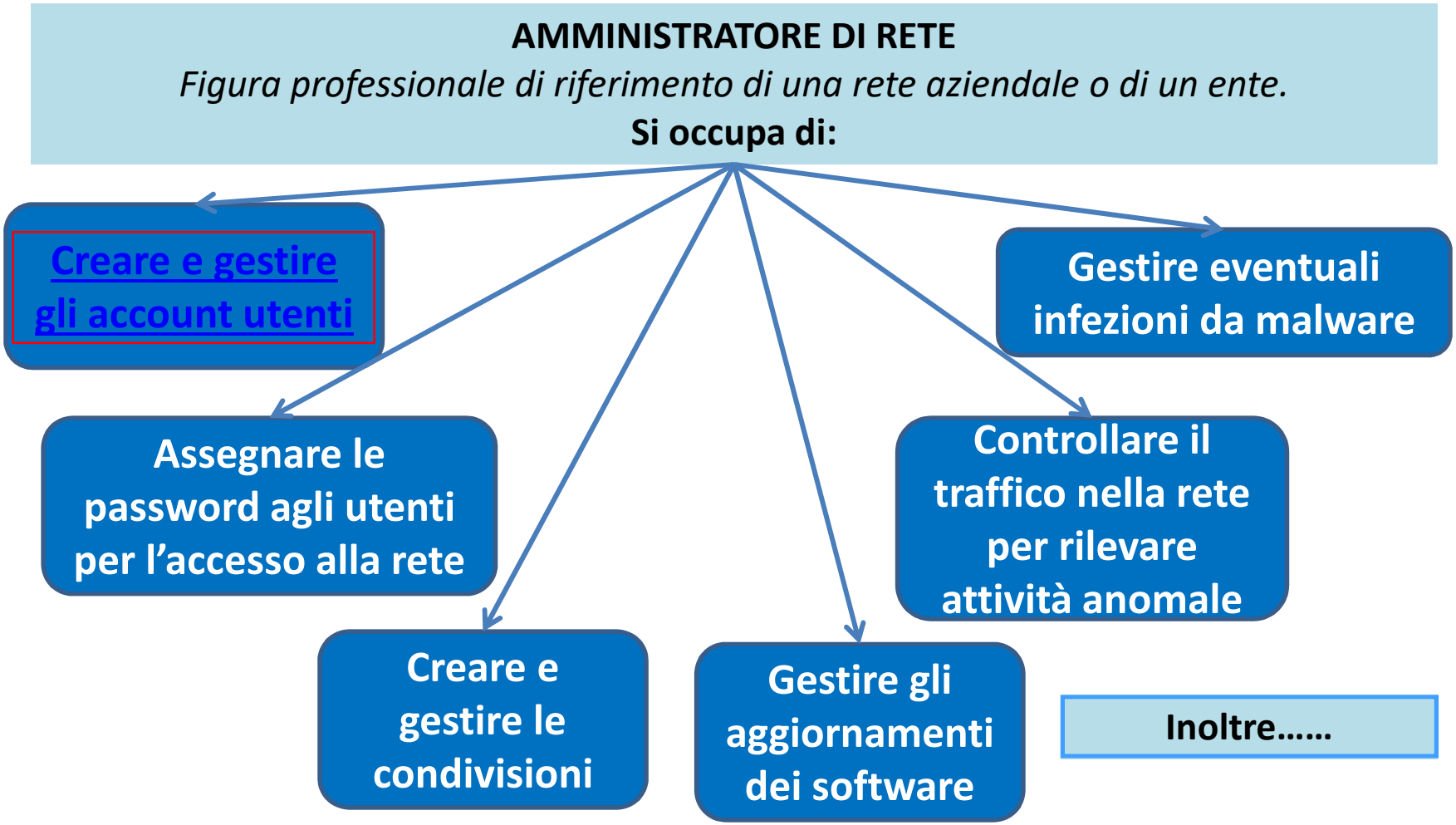
Le **reti locali** sono realizzate utilizzando apposite strutture centralizzate (**DC**) che consentono di effettuare **tre operazioni**:



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete

Creare e gestire gli account utenti

Un ACCOUNT è composto da:

NOME UTENTE (USERNAME) – *serve ad identificare l'utente*

PASSWORD – *serve ad autenticare l'utente*

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.3 Comprendere il ruolo dell'amministratore di rete

Inoltre……

AMMINISTRATORE DI RETE

È l'unica persona ad avere il controllo delle impostazioni di configurazione di una rete

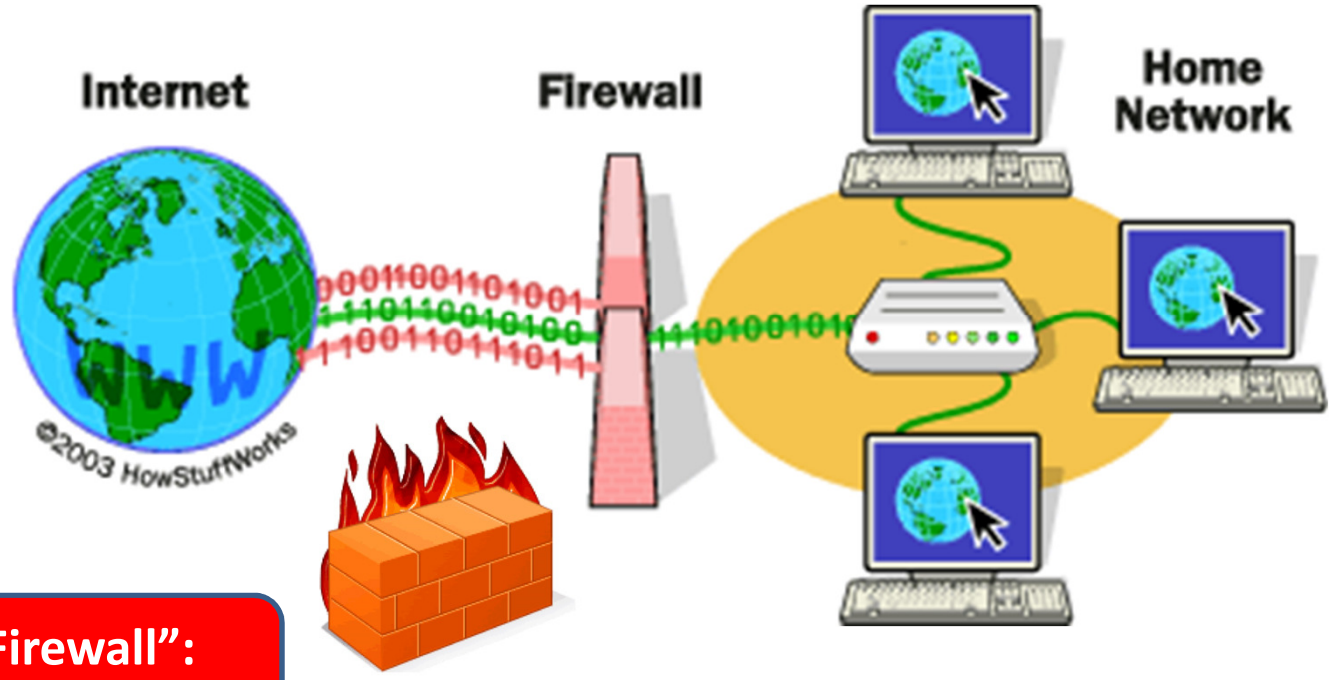
Si occupa di:

Attuare le politiche di sicurezza dell'azienda, configurando il sistema in modo da soddisfare i requisiti di sicurezza stabiliti

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.4 Comprendere la funzione ed i limiti di un firewall in ambiente domestico e di lavoro



"Firewall": muro di fuoco

Componente, hardware o software, collocato fra la rete e l'esterno, che filtra e seleziona i pacchetti in ingresso ed in uscita dalla rete

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.4 Comprendere la funzione ed i limiti di un firewall in ambiente domestico e di lavoro

“Firewall”

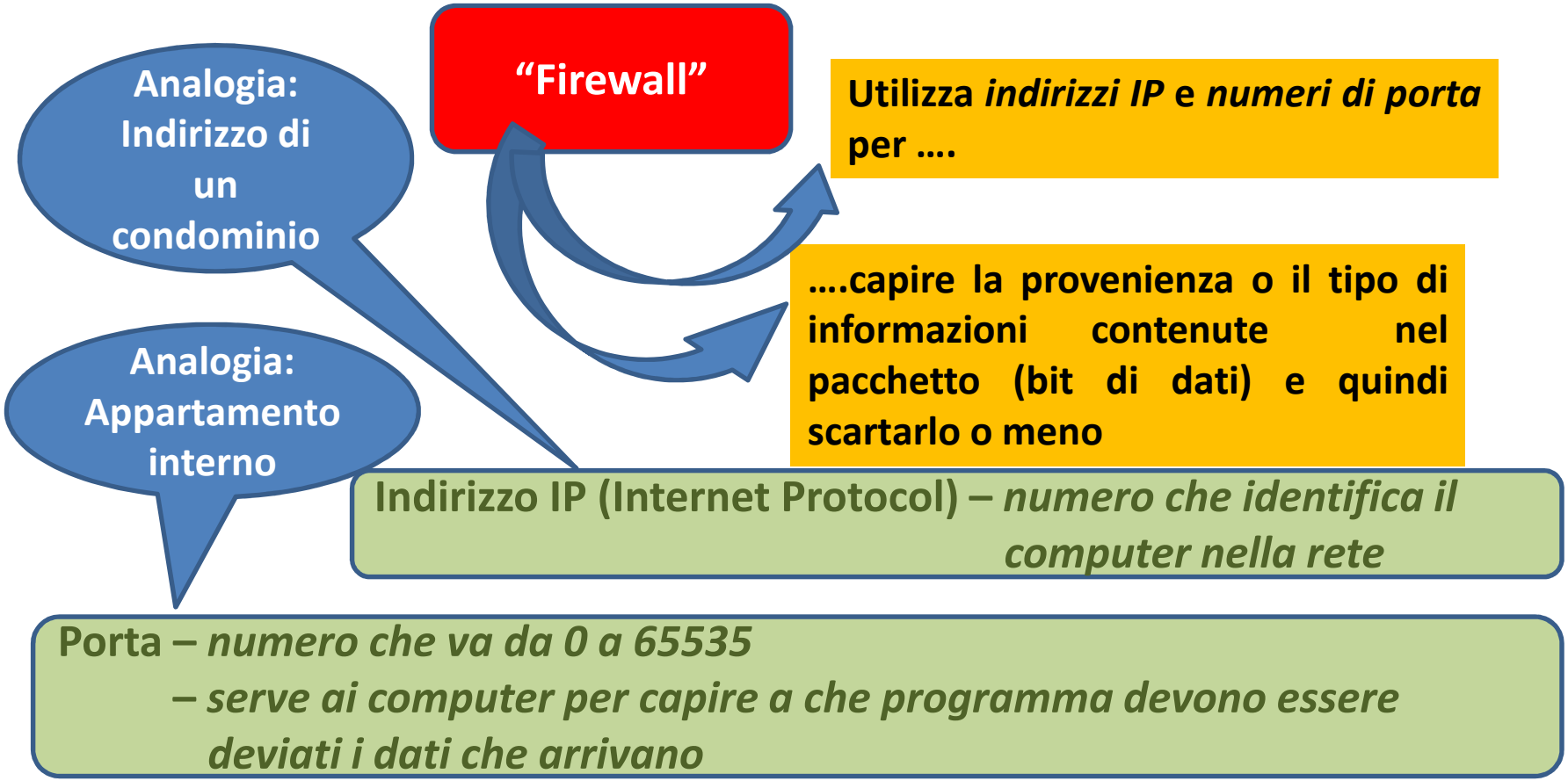
Personale: realizzato tramite software, in genere incluso nel Sistema Operativo; direttamente gestito dall’utente.
Utilizzato in ambito domestico a protezione di un PC.

Di rete o perimetrale: realizzato con apparati dedicati a protezione della LAN; gestito dall’amministratore di rete.
Utilizzato per proteggere una rete aziendale

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.4 Comprendere la funzione ed i limiti di un firewall in ambiente domestico e di lavoro



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.1 RETI E CONNESSIONI

Argomento 3.1.4 Comprendere la funzione ed i limiti di un firewall in ambiente domestico e di lavoro

LIMITI DEI FIREWALL

Configurazione: gestita da impostazioni predefinite, poco flessibili

Funzionalità dell'intero sistema e vulnerabilità: funzionalità compromessa se un attacco esterno, anche da malware, va a buon fine, dato che il firewall è installato nel sistema stesso.

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

RETE CABLATA: - richiede un collegamento fisico (doppini telefonici, cavi coassiali, fibre ottiche) agli apparati di rete;

https://goo.gl/Sw7CNj

- è quasi impossibile collegare un dispositivo senza l'autorizzazione dell'amministratore di rete.

RETE WIRELESS: - non ha collegamento fisico agli apparati di rete, ma si collega tramite onde radio o, a volte, IR, sfruttando ponti radio o satellitari;

- può essere agganciata da un dispositivo mobile , anche esterno all'edificio, fin dove arriva il segnale.

Se la rete non avesse la password, tutti potrebbero connettersi all'insaputa dell'amministratore!

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

Hotspot Wi-Fi – diffusi negli ultimi anni;

- punti di accesso ad internet, con tecnologia wireless, aperti al pubblico;
- aree, create da dispositivi programmati per offrire *un servizio* sicuro e controllato, nelle quali è possibile accedere ad internet tramite il proprio dispositivo WiFi

"WiFi": Wireless Fidelity (fedeltà senza fili)…..*ma non tutti concordano (potrebbe essere solo un marchio commerciale)*

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

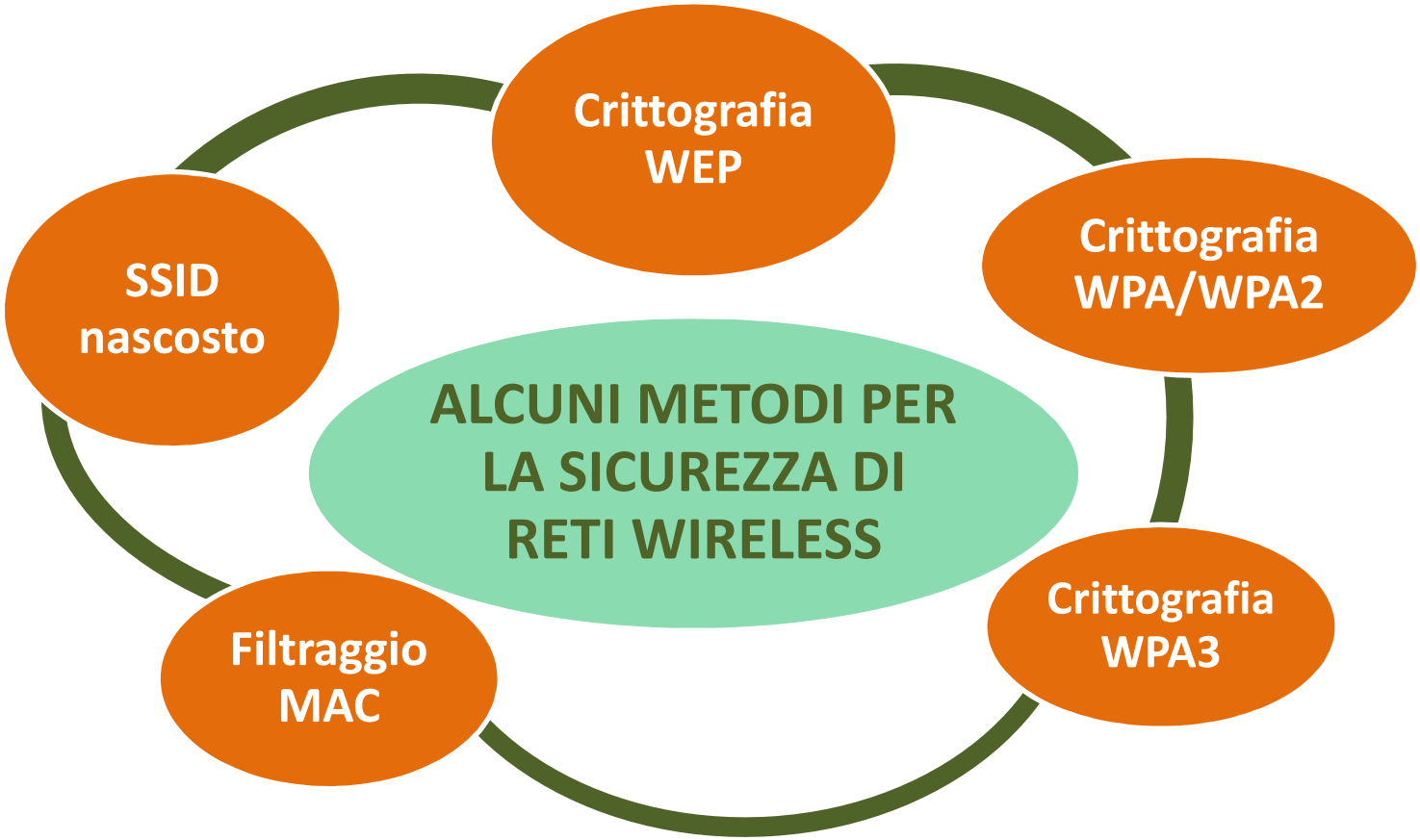
Router

Un **instradatore** (dall'inglese **router**) è un dispositivo di rete che, in una rete informatica, si occupa di instradare i dati, suddivisi in pacchetti, fra sottoreti diverse. L'instradamento può avvenire verso sottoreti direttamente connesse, su interfacce fisiche distinte, oppure verso altre sottoreti non limitrofe che, grazie alle informazioni contenute nelle *tabelle di instradamento*, siano raggiungibili attraverso altri nodi della rete. Il tipo di indirizzamento operato è detto *indiretto* contrapposto invece all'*indirizzamento diretto* tipico del trasporto all'interno delle sottoreti. Esso può essere visto dunque come un dispositivo di interfacciamento tra diverse sottoreti eterogenee e non.

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

SSID
(Service Set Identifier)

Più sicuro rendere non visibile l'SSID della nostra rete WiFi!

È una stringa di testo mediante la quale una rete WiFi indica il suo nome ai propri utenti (= *il nome della rete*).

Quando un dispositivo mobile rileva una rete WiFi, il suo SSID viene aggiunto nell'elenco delle reti disponibili.

Se non ci sono meccanismi di autenticazione, la rete è Open.
Chiunque può connettersi!

Alto rischio di malware e intrusioni con fini criminosi!

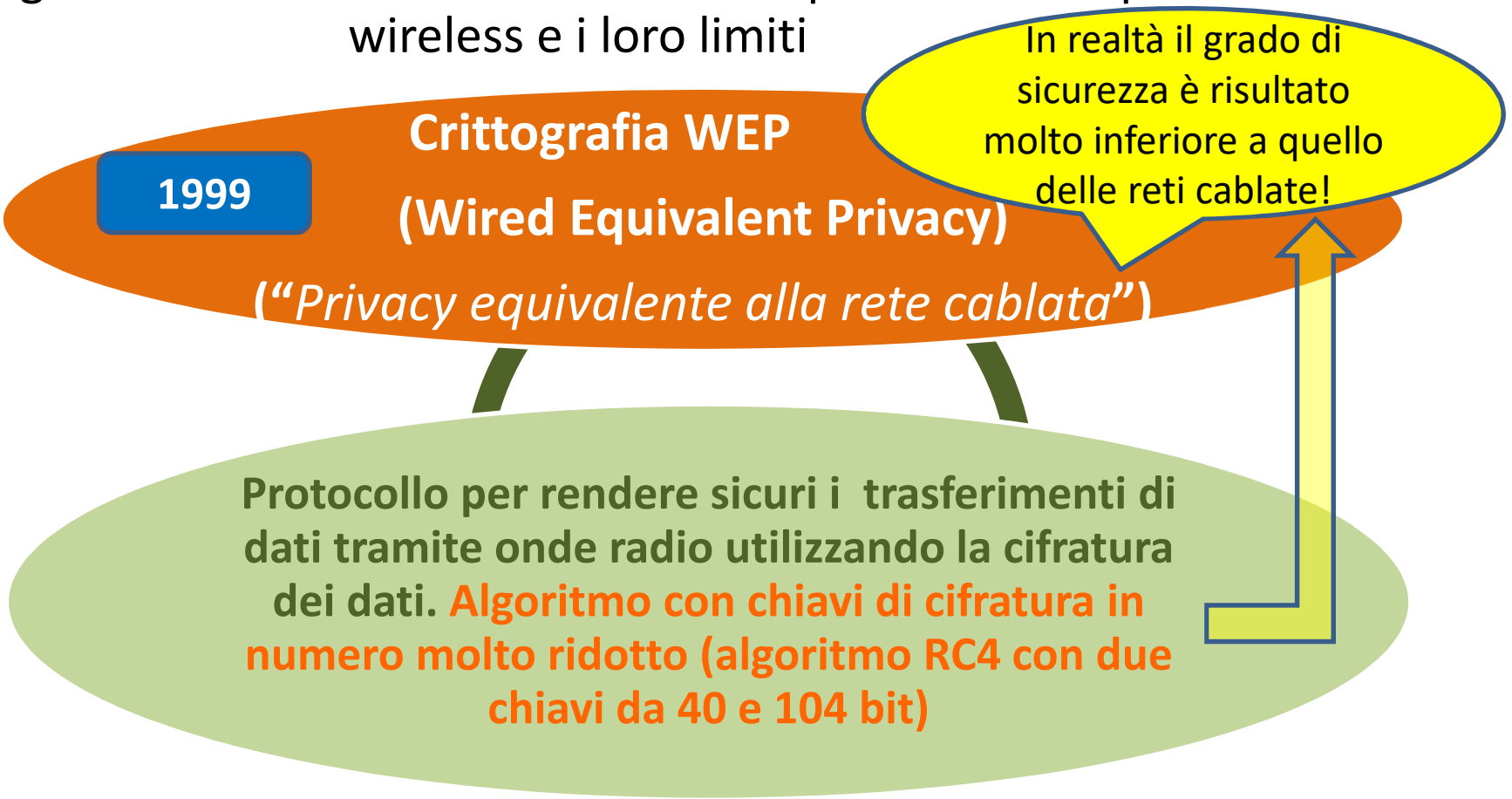
Se ci sono meccanismi di autenticazione, la connessione alla rete è possibile solo con la "Chiave di sicurezza"!

Codice che impedisce la connessione a chi non la possiede e permette di crittografare i dati inviati da un computer della rete ad un altro.

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

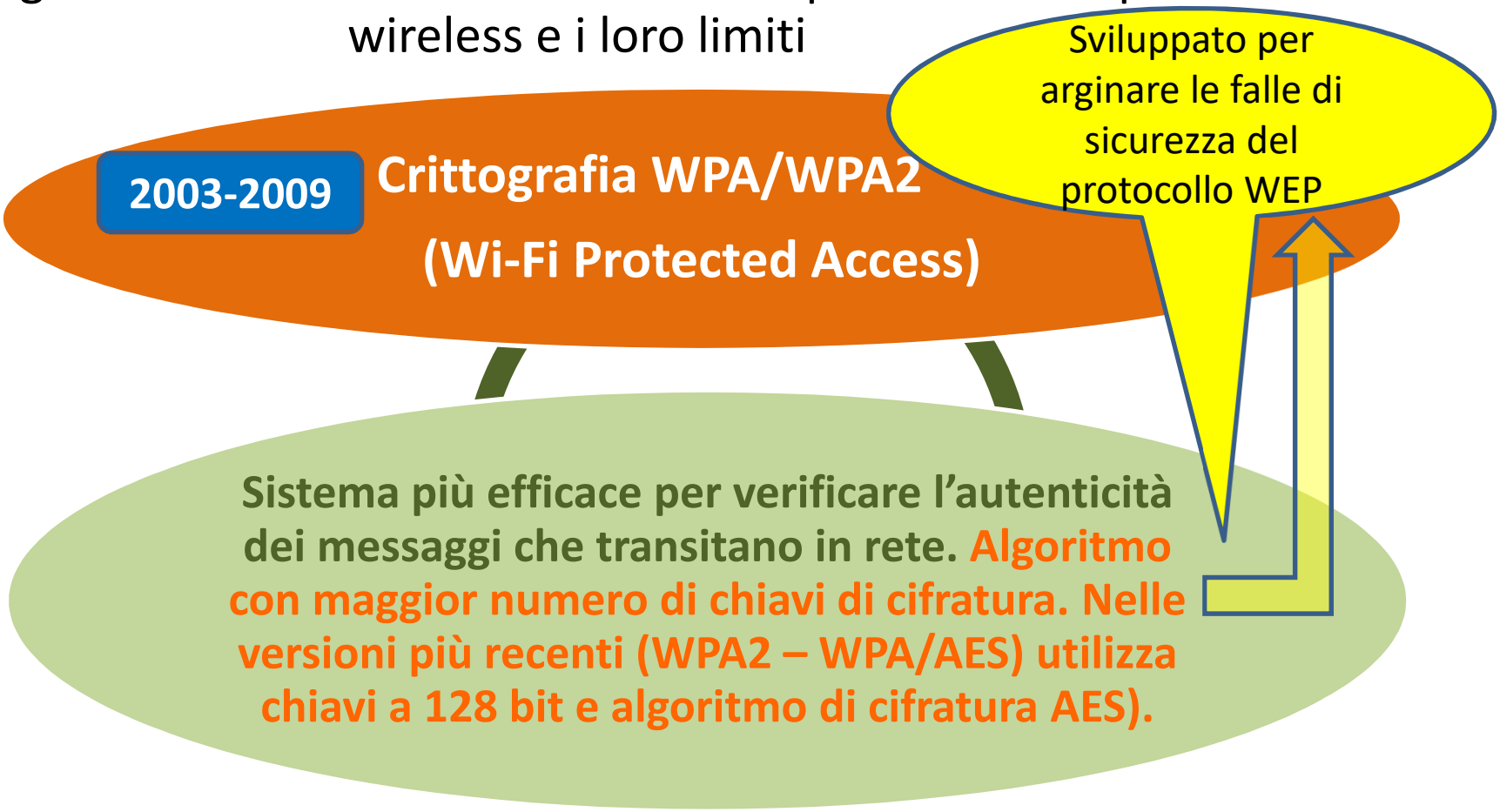
Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

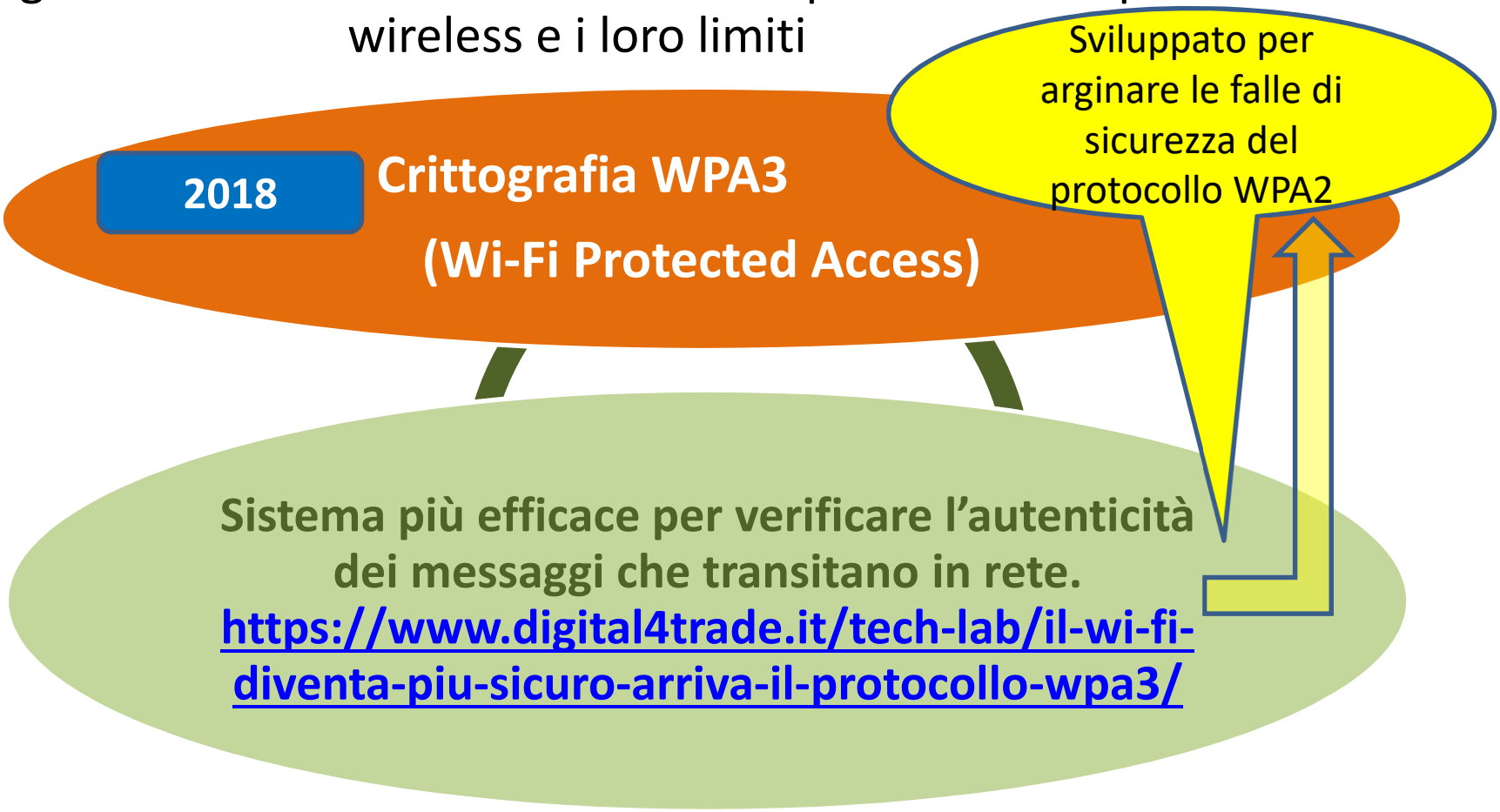
Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

I problemi di WPA2

WPA2, in realtà, da tempo considerato non sicuro a causa di un problema, ossia le reti Wi-Fi aperte, non criptate, che consentono a chiunque si trovi sulla stessa rete WiFi di intercettare le connessioni con altri dispositivi.

Le nuove funzionalità di WPA3

Sono quattro le nuove funzionalità previste in WPA3:

1) La protezione dagli attacchi di Brute Forcing.

2) La possibilità di utilizzare i dispositivi abilitati WiFi nelle vicinanze come pannello di configurazione per altri dispositivi.

3) Un sistema di crittografia unica per ogni dispositivo connesso.

4) La possibilità di utilizzare una suite di sicurezza aderente agli standard del CNSA (Committee on National Security Systems) che potrà essere utilizzata per le reti Wi-Fi più “sensibili” (enti pubblici, settore industriale,...)

Un passaggio non immediato

Ovviamente il passaggio al nuovo standard non avverrà dall’oggi al domani: per essere abilitati al nuovo standard occorrerà acquistare un router di nuova generazione. E, almeno per il momento, non esiste nessun obbligo che imponga ai produttori di equipaggiare i propri nuovi prodotti con questo nuovo protocollo.

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

Protocollo di basso livello

Nelle trasmissioni via internet i protocolli utilizzati contemporaneamente agiscono a livelli differenti: il livello più alto è quello dell'applicazione usata dall'utente (browser, programma per la posta elettronica, etc.), quello più basso è usato dalle apparecchiature di trasmissione elettroniche che inviano i segnali sul mezzo fisico di trasmissione (fibre ottiche, linee telefoniche, etc.)

Indirizzo IP di default:
192.168.1.1
MENO SICURO DI ALTRI!

Indirizzo IP	Indirizzo MAC
Definito a livello software	Definito a livello hardware
Può anche cambiare ad ogni connessione alla rete	Assegnato dal produttore; non cambia mai nel tempo.

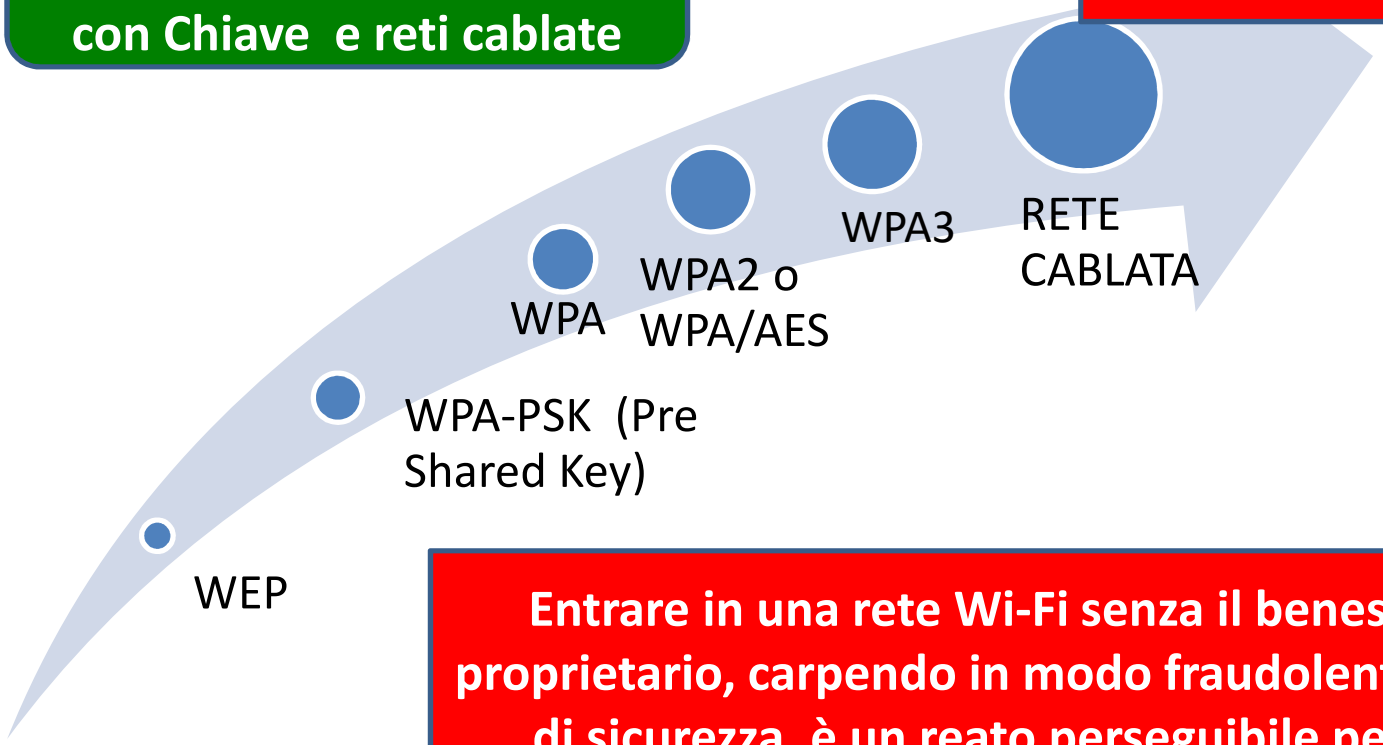
SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

GRADO DI SICUREZZA : confronto tra reti Wireless con Chiave e reti cablate

Nessun metodo è sicuro al 100%



Entrare in una rete Wi-Fi senza il benestare del proprietario, carpendo in modo fraudolento la chiave di sicurezza, è un reato perseguibile per legge!

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi di vario tipo

Hotspot Wi-Fi – punti di accesso ad internet, con tecnologia wireless, aperti al pubblico

Se non ci sono meccanismi di autenticazione, la rete è Open.
Chiunque può connettersi!

RISCHI DI ATTACCHI INFORMATICI DA "SPIE DIGITALI" PER INTERCETTAZIONE DI INFORMAZIONI

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi di vario tipo

SEZIONE 3 – SICUREZZA IN RETE

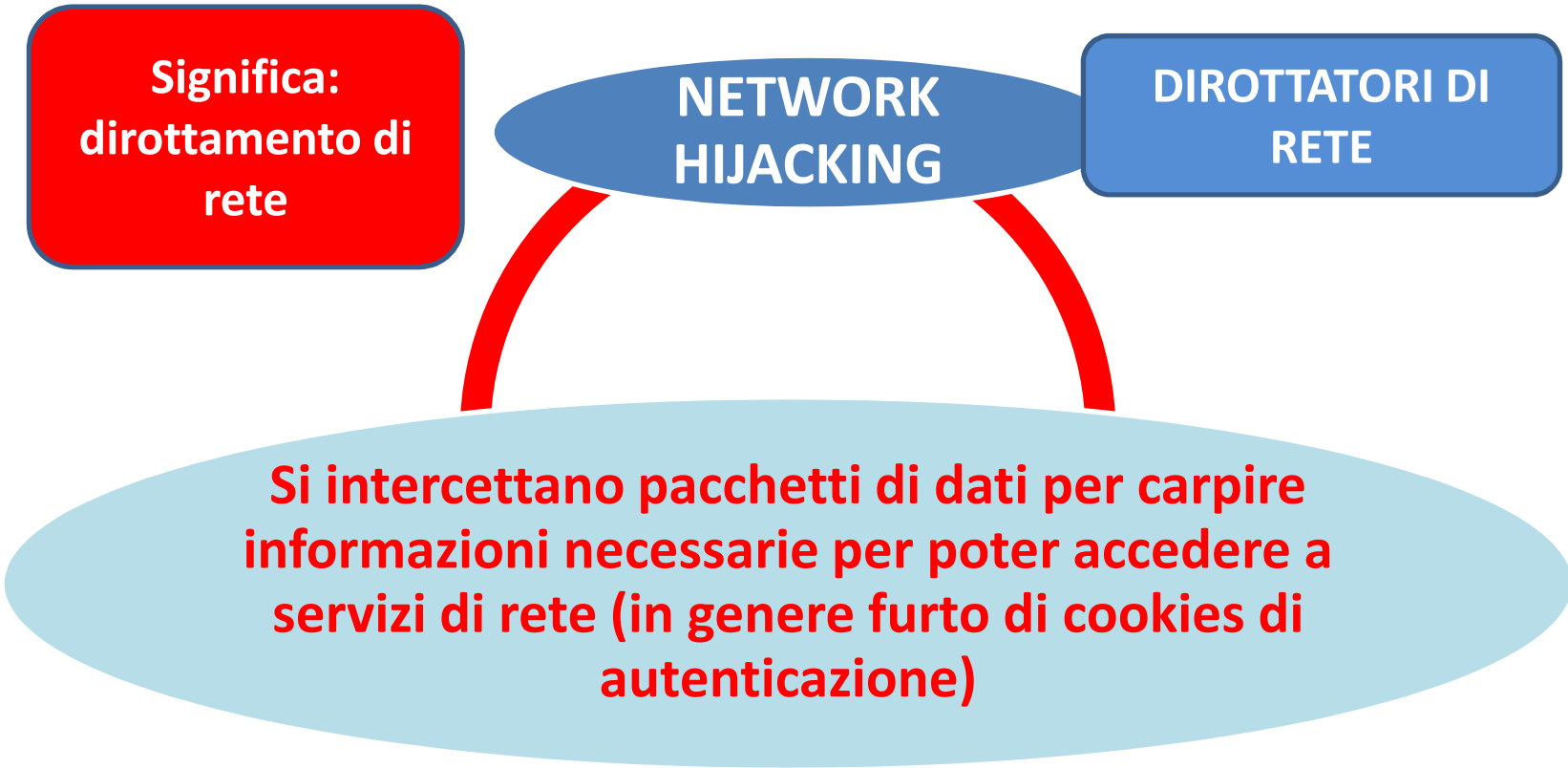
TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi di vario tipo

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi di vario tipo



SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi di vario tipo

SEZIONE 3 – SICUREZZA IN RETE

TEMA 3.2 SICUREZZA SU RETI WIRELESS

Argomento 3.2.3 Comprendere il termine “hotspot personale”

Hotspot Wi-Fi – punti di accesso ad internet, con tecnologia wireless, aperti al pubblico

...è diverso da.....

Hotspot personale – dispositivo che consente di condividere la connessione dati di uno smartphone, di un tablet o di una chiavetta USB per connettere a Internet altri dispositivi fissi o portatili dotati di interfaccia Wi-Fi.