CBC GROUP

comnet
Communication Networks

PORT GUARDIAN

Tecnologia Port Guardian

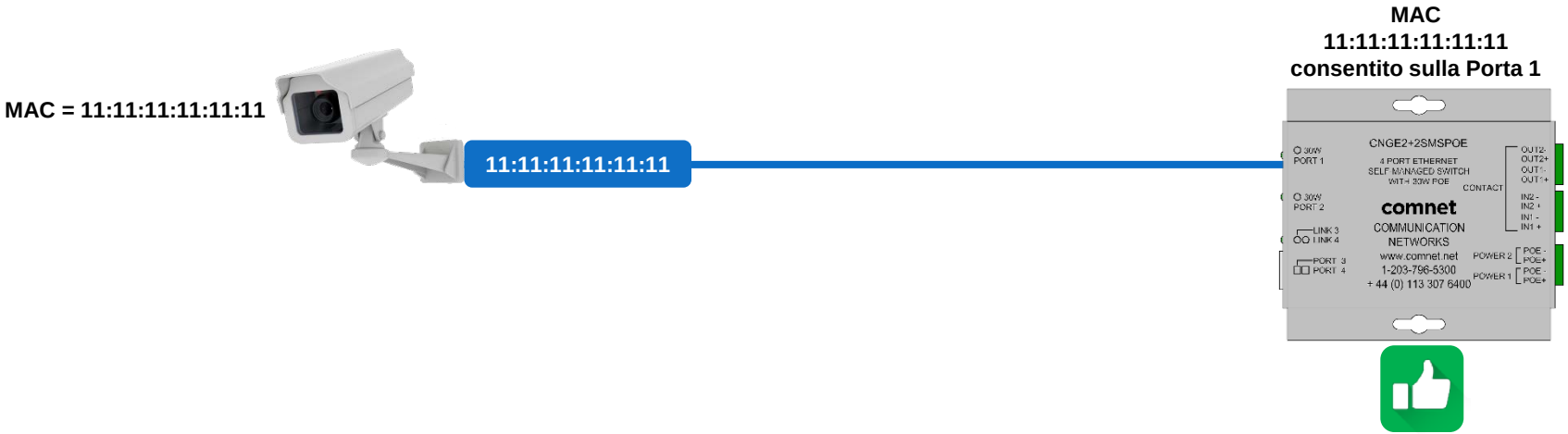
La Cyber Security sta diventando un fattore sempre più importante nella progettazione delle moderne reti Ethernet. ComNet ha lanciato una funzionalità di sicurezza di primo livello nel settore che è allo stesso tempo intuitiva, sicura e semplice da configurare e utilizzare.
L'esclusiva funzione Port Guardian di ComNet ha la capacità di disabilitare fisicamente una porta qualora venisse rilevato un accesso non autorizzato.

Il valore della tecnologia Port Guardian si evidenzia in situazioni in cui si verifica un'intromissione all'interno della rete con conseguente disconnessione di un dispositivo IP per connettersi alla rete. Quando Port Guardian rileva questa disconnessione, invia una notifica SNMP al gestore e la porta interessata viene fisicamente bloccata, impedendo qualsiasi accesso. L'amministratore di rete può riabilitare la porta una volta eliminata la minaccia. Questa funzionalità ostacola anche accessi tramite *Spoofing,* disabilitando la porta non appena viene rilevata un'interruzione.

Sicurezza tradizionale della porta switch

Gli switch di layer 2 sono generalmente in grado di implementare la sicurezza della porta, abbinando i pacchetti in entrata con il MAC address corrispondente.

Se una porta riceve un pacchetto con un MAC address valido, lo switch consentirà l'attraversamento del dato.



Sicurezza tradizionale della porta switch

Se la porta dello switch dovesse ricevere un pacchetto con un MAC address non valido, questo verrebbe bloccato dallo switch che non ne permetterebbe il passaggio. Ciò fornisce un livello di sicurezza base in quanto soltanto il traffico proveniente dal MAC address definito dall'utente sarebbe consentito su quella porta.

Sicurezza tradizionale della porta switch

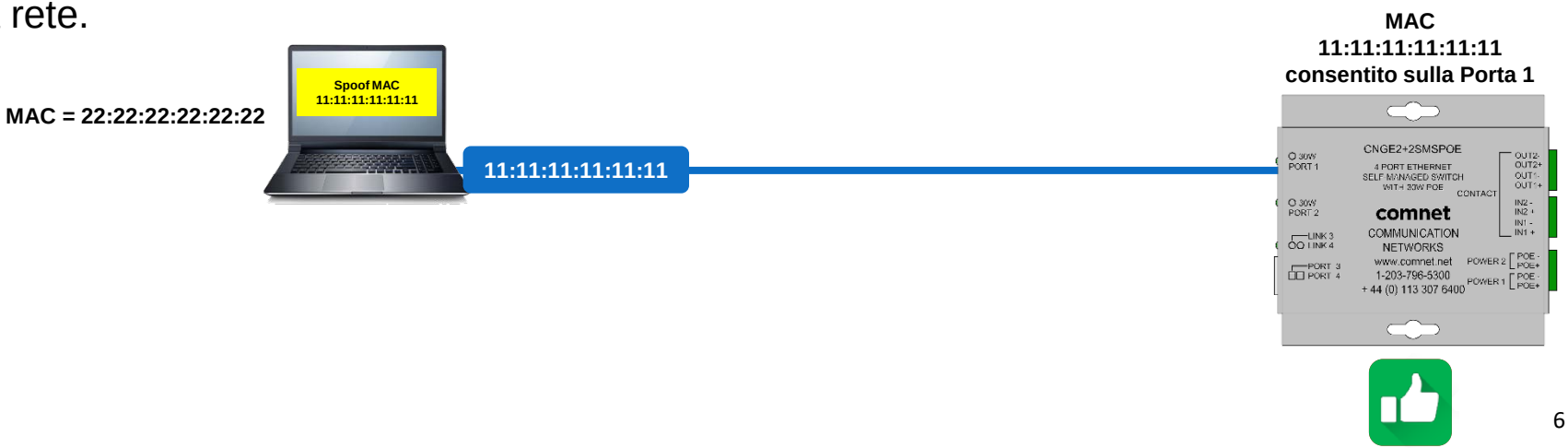
Con questo metodo è possibile implementare facilmente la sicurezza di base della porta contro un potenziale intruso ma, basterà sostituire il dispositivo originale con uno progettato per l'intrusione tagliando il cavo che va al dispositivo originale e collegandolo al dispositivo dedicato all'intrusione, per accedere alla rete.
Questo livello di protezione è comune tra la maggior parte dei managed switch di layer 2 disponibili sul mercato ed infatti tutti gli switch gestiti da ComNet supportano questa funzionalità come standard.

Questa funzione viene chiamata in molti modi a seconda del produttore:

- Port Locking
- MAC Locking
- Port Security
- MAC Filtering

Cosa manca alla sicurezza tradizionale della porta switch?

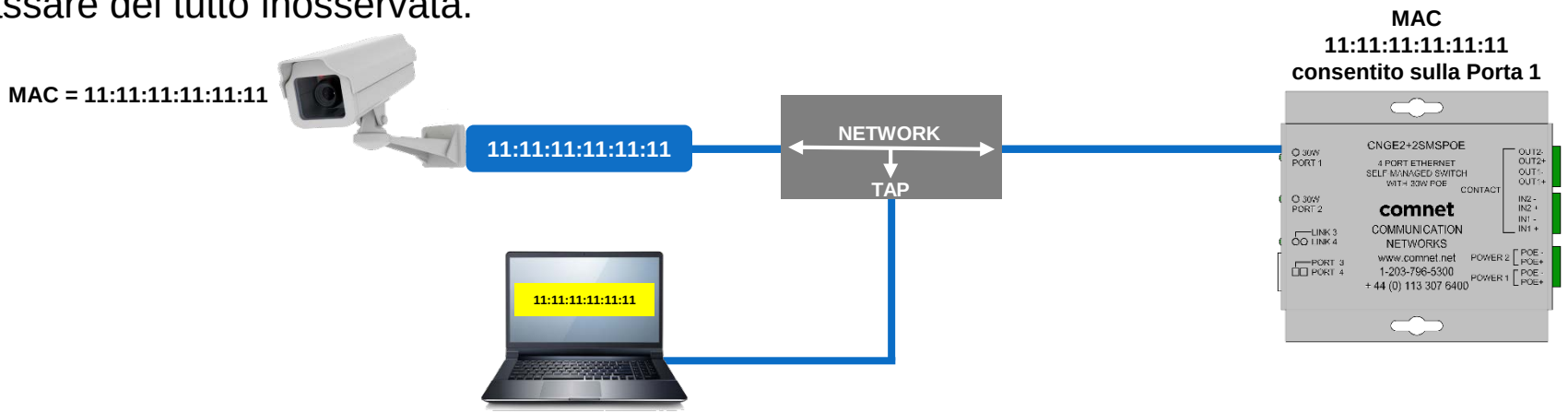
Il problema con il tradizionale filtraggio/blocco del MAC address di layer 2, come descritto in precedenza, è che può essere facilmente bypassato in pochi minuti tramite un software in grado di alterare artificialmente il MAC address del mittente, abbinandolo a qualsiasi potenziale intruso. Nell'esempio sottostante si evidenzia che l'intruso falsifica il MAC address del proprio laptop, utilizzando quello della telecamera autorizzata, ottenendo così l'accesso alla rete.



Come fa un intruso a conoscere il MAC da falsificare?

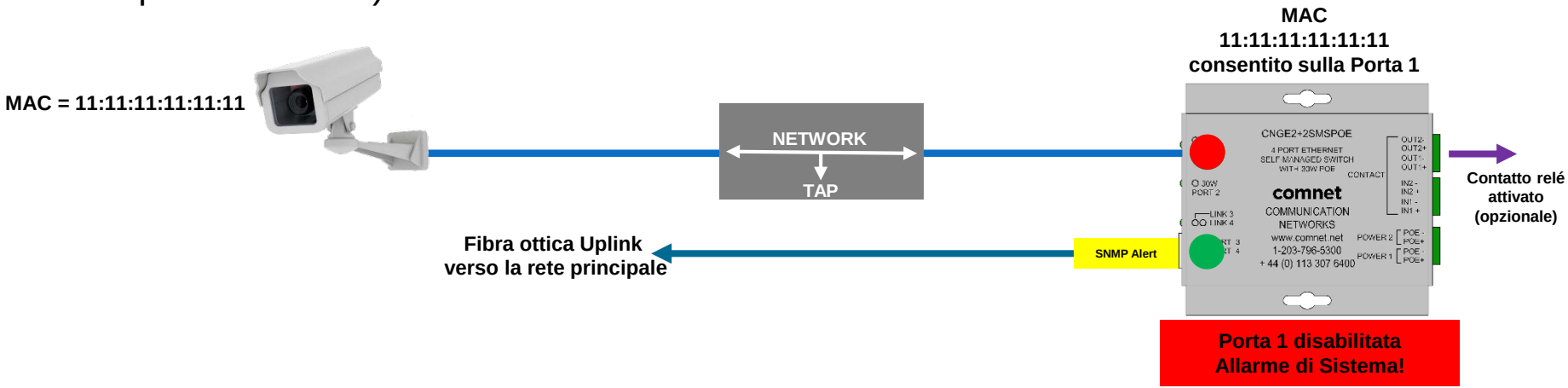
Come potrebbe un potenziale intruso conoscere il MAC address della telecamera per falsificarlo con il proprio laptop, ottenendo così l'accesso alla rete?

Il modo più semplice è quello di utilizzare un *tap device* di rete a basso costo. La telecamera verrà temporaneamente scollegata dalla rete e collegata al *tap*, per poi essere ricollegata rapidamente alla rete. La perdita del video della durata di pochi secondi, molto probabilmente, non verrà ricondotta ad una possibile intrusione o addirittura potrebbe passare del tutto inosservata.



In che modo il Port Guardian previene tali intrusioni?

Il Port Guardian funziona come un sistema di protezione di layer 1, quindi i dati inviati alla porta non sono considerati rilevanti dallo Switch, che pertanto li ignora. Port Guardian monitora costantemente le porte abilitate e, non appena rileva che un cavo viene scollegato, disabilita immediatamente la porta, inviando una notifica SNMP all'amministratore di rete, relativa alla potenziale intrusione (e, opzionale, attiva un contatto relè locale se supportato dallo specifico switch).



Cosa succede quando Port Guardian blocca una porta?

Una volta attivato il Port Guardian su una determinata porta, quest'ultima si troverà in uno stato di blocco permanente e verrà visualizzata da eventuali intrusi come disattivata (no LED ecc). La porta rimarrà in questa condizione di arresto anche in caso di collegamento del dispositivo originale. Lo stato di blocco potrà essere cancellato soltanto dall'amministratore di rete, tramite una delle 3 seguenti procedure:

- Invio di comando SNMP di ripristino;
- comando di ripristino del Port Guardian avviato da USB locale della porta serial CLI
- chiusura del contatto d'ingresso (disponibile soltanto sui modelli predisposti)

L'utilizzo dei contatti è configurabile dall'utente e non è abilitato tra le impostazioni predefinite.

Gli stati di blocco della porta possono essere impostati in modo da essere azzerati ad ogni ciclo di alimentazione oppure per entrare in condizione di blocco in caso di spegnimento (questa sarebbe l'opzione più sicura).

Come posso utilizzare il Port Guardian nelle mie reti?

Esistono due modalità distinte per l'impiego della tecnologia Port Guardian. La corretta implementazione dipende da quanto è sicura la posizione in cui si trova lo switch Edge ComNet remoto (con funzionalità di Port Guardian).
Segue una descrizione ed un esempio per entrambe le ipotesi.

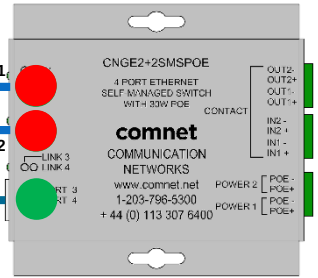
Switch Edge posizionato in luogo sicuro

Se lo stesso switch Edge è installato all'interno di un luogo sicuro non è probabile l'accesso di personale non autorizzato. Sarà pertanto sufficiente abilitare il Port Guardian sulle porte alle quali sono collegati i dispositivi periferici che si trovano al di fuori dell'area sicura e, viceversa, disabilitarlo sulle porte uplink appartenenti alla rete protetta. Per questa ipotesi è altresì possibile impostare l'opzione per lo sblocco delle porte al riavvio, in quanto l'ipotesi di un potenziale intruso in grado di riavviare lo switch non è plausibile.

Di seguito un esempio.

Esempio di Switch Edge in posizione sicura

Switch Edge
(con Port Guardian)



Porta 1 = Port Guardian ON
Porta 2 = Port Guardian ON
Porta 3 = N/A (Porta disabilitata come non in uso)
Porta 4 = Port Guardian OFF
Ciclo alimentazione = rimozione blocco porta

Se la porta 4 rileva una caduta nel collegamento, la porta rimane abilitata, quindi l'accesso remoto viene mantenuto per reimpostare tutte le condizioni di blocco del Port Guardian sulle porte 1 o 2

Qualsiasi switch (Port Guardian non richiesto)

Se una delle due porte del dispositivo 1 o 2 rileva una caduta nel collegamento, la porta verrà bloccata fino a ripristino da parte dell'amministratore di rete.

Area sicura
Punto di demarcazione

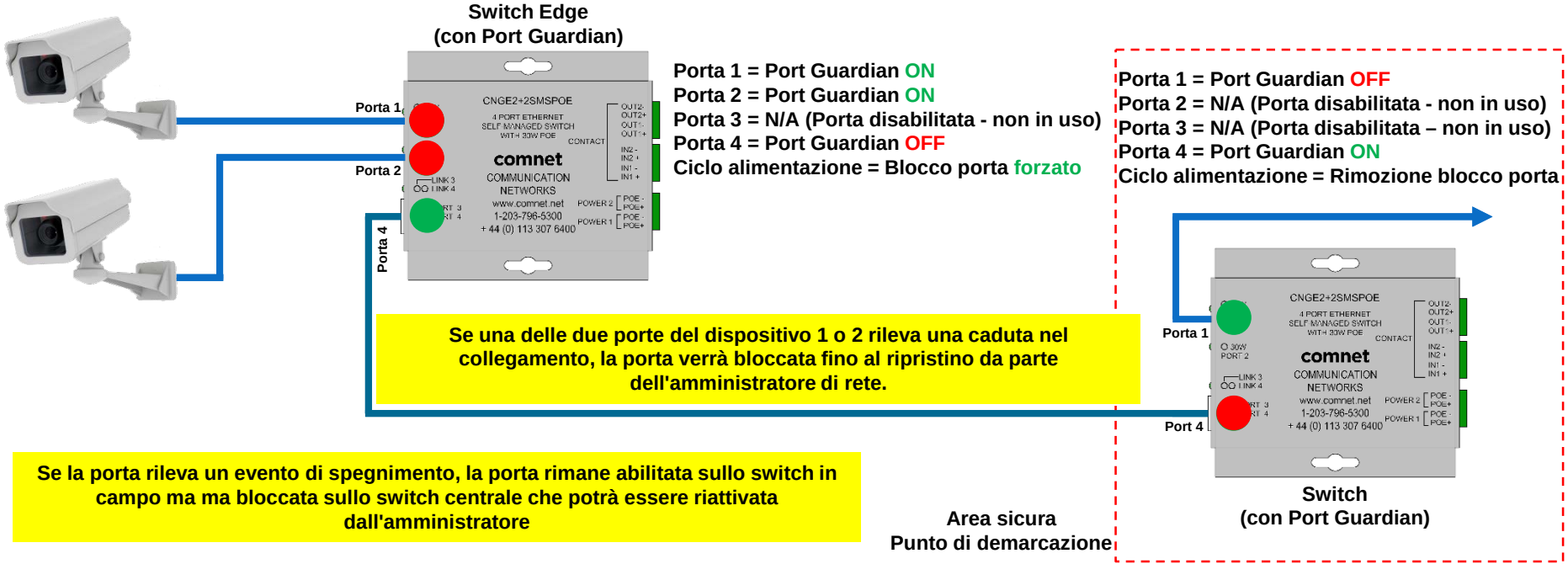
Come posso utilizzare il Port Guardian nei miei Network?

Switch Edge posizionato in luogo NON sicuro

Se lo Switch Edge ComNet NON è posizionato in un luogo sicuro, sussisterebbe il rischio che un intruso riesca ad accedere fisicamente allo switch, con un potenziale ingresso all'interno della rete. In questo caso vi sono 2 opzioni possibili per la configurazione del sistema:

1. abilitazione del Port Guardian su tutte le porte dello Switch Edge e impostazione dell'opzione di riavvio per forzare il blocco della porta. Ciò offrirebbe protezione su tutte le porte; tuttavia lo svantaggio è che in caso di interruzione della corrente, l'unico modo per avere accesso allo switch sarebbe reimpostarlo tramite la porta seriale USB CLI;
2. utilizzando due switch su che dispongono della funzione Port Guardian. Lo switch in campo dovrebbe essere abilitato solo sulle porte con periferiche collegate all'Edge, mentre lo switch centrale dovrebbe essere abilitato solo sulla porta di uplink che si collega allo switch Edge. Ciò offre una protezione completa e consente il ripristino dopo un'interruzione di corrente in quanto 1 porta avrà sempre accesso abilitato.

Esempio di Switch Edge in area sicura



Quali prodotti sono dotati di tecnologia Port Guardian?

Di seguito è riportato un elenco di prodotti ComNet che presentano l'esclusiva funzione Port Guardian:

- CNGE2+2SMS
- CNGE2+2SMSPOE
- CNGE2+2SMSPOEHO
- CNGE4+2SMS
- CNGE4+2SMSPOE
- CNGE4+2SMSPOEHO

Nel 2019 saranno rilasciati molti altri prodotti ComNet con funzione Port Guardian. In caso di applicazioni urgenti, ed i prodotti selezionati non supportano la tecnologia Port Guardian, contattate gli uffici CBC per un'eventuale implementazione di questa funzione ai prodotti richiesti.

Riassumendo…

- Port Guardian blocca fisicamente una porta se rileva una disconnessione dalla porta Edge;
- se un dispositivo IP su Edge viene disconnesso con l'intenzione di accedere alla rete collegandosi ad una porta Ethernet Edge, Port Guardian rileva la disconnessione e blocca fisicamente la porta;
- invia automaticamente un alert SNMP all'amministratore del sistema, notificando la porta che è stata disconnessa, il quale potrà quindi ripristinarla dopo che la minaccia sarà risolta;
- disabilità fisicamente le porte in caso di sospetta intrusione;
- è immune alla falsificazione degli indirizzi IP;
- disponibile sui prodotti SMS Gen2, CNGE2+2SMS(PoE), CNGE4+2SMS(PoE);
- disponibile su CNGE11FX3TX8MS(PoE), CNGE3FE8MS(PoE), CNGE24FX12TX12MS(POE) con firmware aggiornato all'ultima versione.

Grazie per l'attenzione.