Migliorare l’affidabilità delle reti di controllo Ethernet

RIEPILOGO

La proliferazione in stabilimento delle periferiche compatibili Ethernet - dai PLC alle schede di I/O fino ai sensori - a supporto dell’Industrial Internet of Things” (IIoT), della comunicazione e di altre necessità a livello dati richiede una vigilanza costante contro le perturbazioni del traffico, perturbazioni che possono avere serie conseguenze sulla rete di controllo. Il presente suggerimento tecnico offre una visione generale dei tipi di traffic storms o tempeste di traffico su Ethernet che si possono verificare, nonché di alcune tecniche idonee a prevenirle ed attenuarle.

Panoramica

Dato che le reti di controllo dipendono sempre piu’ da Ethernet per le comunicazioni, diviene vitale saper configurare e servirsi correttamente delle reti Ethernet al fine di evitare problemi potenzialmente gravi causati dai traffic storms. Benché le tempeste di trasmissione (broadcast) siano la preoccupazione principale, il traffico monodiffusione (unicast) e multidiffusione (multicast) puo’ a volte raggiungere dei livelli capaci di compromettere la performance del sistema di controllo. La misura piu’ importante che potete adottare per assicurare il buon funzionamento della rete é di configurarla correttamente da subito. Tuttavia, anche se la rete é stata configurata correttamente esistono altri motivi per i quali c’e’ il rischio di incontrare problemi di traffico rete. Il presente suggerimento tecnico vi aiuterà a capire i tipi di traffico Ethernet, i problemi creati da un traffico eccessivo nonché alcuni modi per ridurre tali problemi.

Tipi di traffico Ethernet

Per diagnosticare i problemi di affidabilità della rete, é importante conoscere i tipi di pacchetti Ethernet trasportabili dalla rete. Esistono tre tipi di traffico su rete Ethernet comuni ad ogni rete Ethernet ed essenziali per il suo buon funzionamento : monodiffusione (unicast), multidiffusione (multicast) e diffusione (broadcast).

. traffico unicast : i pacchetti Ethernet indirizzati direttamente all'indirizzo MAC di una periferica specifica

. traffico multicast : i pacchetti Ethernet per i quali l'indirizzo di destinazione é un indirizzo del gruppo multicast. Le periferiche Ethernet atte a processare questi pacchetti sono configurate per recepire l'indirizzo di un gruppo particolare

. traffico broadcast : i pacchetti Ethernet per i quali l'indirizzo di destinazione é l'indirizzo di diffusione. Le apparecchiature collegate alla medesima rete Ethernet ricevono pacchetti broadcast.

Questi tre tipi di traffico Ethernet sono comuni a tutte le reti Ethernet, ma un traffico eccessivo di qualunque genere puo' creare problemi alla rete Ethernet stessa, in particolare ad una rete di controllo industriale caratterizzata da grandi volumi di traffico messaggi.

Puo' una cosa valida risultare eccessiva ?

Il traffico Ethernet eccessivo é spesso indicato come « tempesta di traffico ». Il tipo piu' comune di tempesta di traffico é una tempesta di diffusione o broadcast, ma anche il traffico multicast e unicast possono creare problemi alla rete di controllo. Svariati protocolli moderni Ethernet I/O si basano su messaggi multicast e, allorché la rete contiene un gran numero di dispositivi che utilizzano protocolli multicast, il carico in rete puo' aumentare a dismisura. Nelle situazioni ove vari sistemi SCADA interrogano grandi quantità di dati, anche il traffico unicast puo' raggiungere a volte un livello problematico.

I paragrafi seguenti trattano i vari tipi di tempeste di traffico in rete ed i mezzi per prevenirle ed attenuarle. Al fine di determinare quale tipo di traffico (e quale periferica) é all'origine di una certa tempesta di traffico, in genere é necessario utilizzare un analizzatore di protocolli o 'packet sniffer', in grado di catturare e ed analizzare il traffico in rete. A CTI ci si serve di Wireshark, un analizzatore di protocolli di rete open-source. Il presente documento non intende dare informazioni sull'impiego di Wireshark, esiste già una quantità di informazioni in merito su internet. Vi suggeriamo a questo proposito la lettura dell'articolo di Brian Hill : www.arstechnica.com/information-technology/2016/09/the-power-of-protocol-analyzers/.

Traffico unicast : come possono livelli elevati impattare il sistema di controllo ?

Il tipico PLC compatibile con Ethernet individua svariate fonti di traffico unicast, tra cui :
. sistemi SCADA che interrogano il PLC per ottenere dati
. pannelli HMI che interrogano il PLC per ottenere dati
. altri PLC che interrogano per ottenere dati
. PC che effettuano operazioni di programmazione

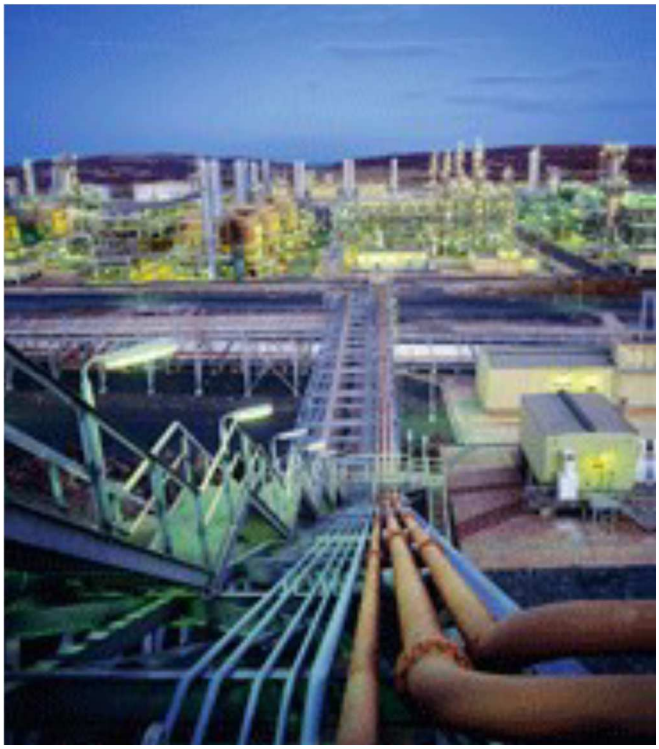
Ogni pacchetto Ethernet ricevuto dal PLC provoca una « interruzione » la quale necessita delle risorse del processore per rimuovere il pacchetto stesso dal buffer di ricezione e salvarlo per un trattamento successivo durante la comunicazione. Se sopravvengono flussi elevati di pacchetti unicast, il PLC si trova a dover passare parecchio tempo a gestire il trattamento dell'interruzione. Se la quantità di pacchetti da gestire diviene eccessiva, i tempi di trattamento aumentano considerevolmente e cio' porta a una degradazione dei compiti di controllo di processo e alla perdita dei pacchetti Ethernet.

Gli switch Ethernet sono informati dell'indirizzo MAC delle periferiche che comunicano con ciascuna porta degli switch. Una volta informato dell'indirizzo MAC, lo switch inoltra alla porta corrispondente soltanto i pacchetti unicast che dispongono di una determinata destinazione unicast. L'interfaccia di rete di un dispositivo Ethernet blocca la ricezione di tutti i pacchetti unicast tranne quelli il cui indirizzo di destinazione é uguale all'indirizzo MAC dell'interfaccia. Per tali motivi é meno probabile che si verifichi un carico eccessivo a causa dei pacchetti unicast. Tuttavia puo' comunque verificarsi in certe condizioni, tipo:

.1 Un gran numero di dispositivi, come i sistemi SCADA/HMI, interrogano velocemente i dati. Il flusso medio dei pacchetti é spesso accettabile, ma il traffico di questi sistemi tende a essere a discontinuo, cioé una sorta di raffica di pacchetti seguiti da un periodo senza pacchetti. Man mano che il numero di periferiche aumenta, le raffiche di varie periferiche si accavallano e creano picchi di traffico considerevoli.
.2 Periferiche mal configurate che inviano per errore all'indirizzo IP della periferica.
.3 Attacchi DoS (servizio negato – denial of service) nei quali una raffica di pacchetti é inviata all'indirizzo unicast al fine di degradare le operazioni.

Attenuazione dei problemi di traffico unicast

A seconda della situazione, le azioni seguenti possono risolvere i problemi di traffico unicast :
. Ridurre il tasso di interrogazione dei sistemi SCADA/HMI quando possibile. La maggioranza di questi sistemi interrogano piu' velocemente del necessario (due volte piu' velocemente del tempo di aggiornamento richiesto).
. Localizzare e riconfigurare/disattivare le periferiche incriminate
. Collegare il dispositivo ad uno switch capace di limitare il flusso. Configurare lo stesso in modo da limitare il trasferimento di pacchetti ad un flusso accettabile. Dato che limitare il flusso puo' mettere i pacchetti Ethernet nel buffer, i picchi di traffico risulteranno equiparati.
. Utilizzare una scheda di comunicazione CTI, tipo la 2572-B o la 2500P-ECC1, per le comunicazioni in rete.



Traffico multicast : una causa spesso ignorata circa i problemi della rete di controllo

Correttamente implementata, la messaggeria multicast é un metodo di comunicazione efficace per i sistemi di controllo allorché gli stessi dati devono essere trasmessi a svariati destinatari.
Ethernet/IP utilizza spesso il multicast per la comunicazione tra PLC e le periferiche di I/O.
Tuttavia, in alcune circostanze il traffico multicast puo' creare problemi. Il traffico multicast tende ad avere flussi di pacchetti piu' elevati rispetto allo unicast perché non occorre attendere la risposta della periferica. Per default Ethernet inonda le porte dello switch di pacchetti multicast, propagandoli cosi' sulla rete Ethernet. Combinati ad elevati flussi di traffico multicast (per esempio con I/O in Ethernet/IP), la situazione puo' impattare negativamente il funzionamento delle periferiche di rete.
La maggior parte delle periferiche consente sempre al traffico multicast di passare via rete Ethernet. Tale traffico include pacchetti con indirizzi multicast legati al controllo di rete e alla gestione stessa del gruppo multicast. Di conseguenza é sempre possibile per il traffico multicast creare interruzioni alla periferica.

Attenuazione dei problemi di rete in multicast

Il traffico multicast non crea alcun problema al processore CTI modello 2500-Cxxx : esso infatti non supporta il multicast ed é configurato per bloccare la ricezione di tutti i messaggi multicast.
Per impedire al traffico multicast indesiderato di inondare altri prodotti CTI esistono varie soluzioni. Se non volete servirvi dei prodotti CTI compatibili Ethernet per le comunicazioni multicast, potete collegarli ad uno switch che supporta il monitoraggio IGMP (Internet Group Management Protocol). Si tratta di una funzionalità che individua le richieste IGMP per unirsi poi ad un gruppo multicast particolare e trasmetterne il flusso solo verso la porta collegata alla periferica che ha lanciato la richiesta. La maggioranza degli switch che supportano IGMP si possono configurare affinché ignorino un flusso multicast sconosciuto. Se invece volete che il vostro prodotto CTI riceva flussi multicast, questa soluzione non funzionerà correttamente, in quanto il prodotto CTI deve rispondere ad una domanda IGMP proveniente da un router e gli attuali prodotti CTI non rispondono a richieste IGMP da router. Sono infatti stati concepiti per la comunicazione multicast solo in rete locale.

Una soluzione alternativa se si vuole che il proprio prodotto CTI riceva messaggi multicast é quella di usare uno switch Ethernet che supporti il Bridge Multicast Filtering. Si tratta di una funzionalità che consente di definire in modo statico come vengono trasferiti i pacchetti multicast. Se volete ricevere pacchetti multicast con un determinato indirizzo di gruppo, potete assegnare in modo statico l'indirizzo del gruppo alla porta. Potete anche scegliere di impedire ai pacchetti multicast di essere trasferiti verso le porte designate.
Se non volete aggiungere uno switch esterno, un'altra possibilità é quella di usare un prodotto CTI come la scheda 2500P-ECC1 e/o la scheda 2500P-ACP1 che adoperano switch integrati ; essi limitano il tasso di pacchetti multicast (e broadcast). Questa soluzione si rivela efficace il piu' delle volte, tuttavia esiste un rischio di perdita dei pacchetti che si vogliono ricevere in quanto l'algoritmo limite comincia a ignorare i pacchetti non appena si supera la soglia massima.

Una soluzione piu' globale consiste nel segmentare la propria rete Ethernet come indicato piu' sotto.

Traffico broadcast : il colpevole piu' frequente delle perturbazioni in rete

Il traffico broadcast é necessario al buon funzionamento di TCP/IP su Ethernet. Per esempio l'Address Resolution Protocol (ARP), che rileva l'indirizzo MAC di una periferica con indirizzo IP conosciuto, é richiesto al fine di trasmettere messaggi unicast TCP/IP via collegamento Ethernet. Come indicato in precedenza, tutti i dispositivi su di una rete Ethernet consumano risorse per processare il pacchetto broadcast.

Dato che alla rete sono aggiunte sempre piu' periferiche, il numero di comunicazioni aumenta naturalmente. Le tempeste broadcast si verificano quando un numero anormalmente elevato di messaggi viene inviato in un breve lasso di tempo, congestionando i dispositivi in rete e provocando spesso ingombri e pacchetti persi negli switch di rete. Mentre le tempeste broadcast possono essere un semplice disturbo in una rete di ufficio, possono rivelarsi catastrofiche in una rete di controllo. A causa di vincoli di dimensione, costo ed alimentazione, le periferiche di una rete di controllo hanno in genere una potenza di trattamento limitata rispetto al computer da ufficio. Inoltre queste risorse limitate devono restare dedicate al compito primario di controllo, cosi' da assicurare le corrette operazioni delle apparecchiature.

Quali sono le cause di una tempesta broadcast ?

Svariati fattori, ma i piu' frequenti sono :

Combinare la rete dello stabilimento con la rete informatica

Le reti IT generano spesso un ingente traffico broadcast. Questo livello é accettabile per la rete informatica, ma puo' danneggiare seriamente le prestazioni dei sistemi di controllo, per i quali occorrono operazioni in tempo reale.

Reti di controllo eccessivamente estese

Anche se isolate dalla rete informatica, reti di controllo estese possono generare un traffico broadcast troppo importante a causa del numero delle periferiche collegate in rete e dei protocolli impiegati.

Protocolli mal concepiti

Non é raro trovare comunicazioni Ethernet e protocolli I/O non autorizzati che si servono del broadcast come principale mezzo di trasmissione dati. Si tratta in genere di protocolli 'ereditati', che sono stati sviluppati nelle prime fasi dell'adozione di Ethernet.

Guasto hardware/Switch difettoso

Uno switch, un router o una interfaccia di rete difettosa puo' inondare la rete di traffico broadcast. Vale la pena investire in materiale di qualità equipaggiato di funzioni di prevenzione contro le tempeste.

Errore umano

Un errore umano frequente si verifica quando un loop é creato inavvertitamente, il che produce una ripetizione continua di di traffico broadcast in rete. Si puo' creare un loop collegando le estremità di un cavo su due porte dello stesso switch oppure creando un loop tra diversi switch.

Prevenzione o attenuazione delle tempeste broadcast

Esistono numerosi metodi per ridurre l'incidenza di tempeste e/o per attenuarne i disturbi.

.1 Isolare la rete IT dalla rete di controllo

Assicuratevi che la vostra rete aziendale IT sia fisicamente isolata dalla rete di controllo o separata da quest'ultima per mezzo di router e firewall correttamente configurati. I router trasmettono i pacchetti TCP/IP multicast e unicast designati, ma non trasmettono quelli broadcast. I firewall limitano ulteriormente i pacchetti TCP/IP che saranno accettati. Questi componenti di rete permettono la comunicazione tra gli uffici amministrativi e lo stabilimento, impedendo nel contempo ai pacchetti broadcast/unicast e multicast indesiderati di entrare nella rete di controllo.

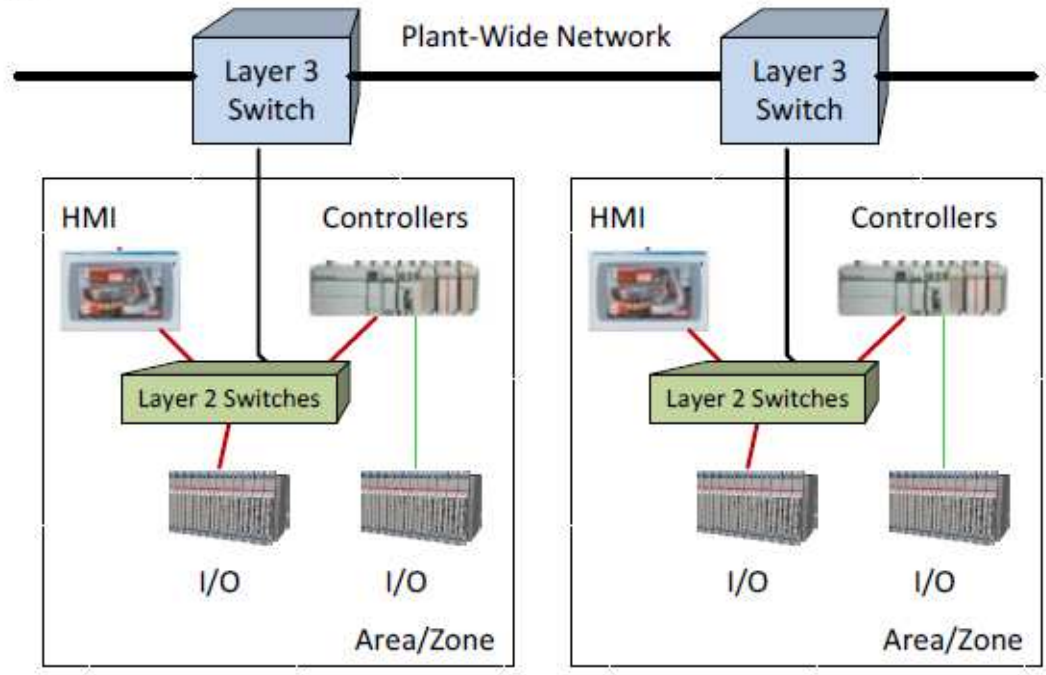
.2 Suddividere la rete di stabilimento in segmenti piu' ridotti

Uno dei modi migliori per gestire il traffico broadcast e multicast consiste nel suddividere la rete in zone di diffusione ridotte. La maggior parte degli ambienti produttivi puo' essere naturalmente divisa in aree di lavoro automatizzate da uno o piu' controllori con gli I/O associati. Ciascun dominio broadcast consisterebbe in una rete Ethernet locale (LAN) collegata alla rete dello stabilimento via uno switch di livello 3. Lo switch di livello 3 assicura il routing dei pacchetti TCP/IP tra la rete locale e la rete principale, fornendo nel contempo le funzioni di switching Ethernet (livello 2). Di conseguenza i pacchetti broadcast provenienti dalla rete piu' estesa non saranno trasmessi alla rete locale (Figura 1).

.3 Implementare il controllo di tempesta broadcast

Uno dei metodi piu' semplici ed efficaci per minimizzare gli effetti delle tempeste e dei flussi di pacchetti elevati é quello di installare un managed switch. I managed switch hanno la capacità di definire limiti di flusso per il traffico broadcast. Altri switch permettono di limitare il flusso per il traffico unicast e multicast. A titolo di esempio, l'illustrazione piu' sotto (Figura 2) mostra la pagina web di configurazione dello Storm Control per un managed switch Cisco ad 8 porte. Tale switch consente di definire i limiti di flusso di pacchetti indipendenti per il traffico broadcast, unicast e multicast. I limiti di flusso sono definiti in % della banda larga di rete o in pacchetti per secondo (pps). Per le porte collegate ai prodotti CTI, si raccomanda di limitare la porta a 1000 pacchetti broadcast /multicast per secondo (l'1% di un collegamento a 100Mb).

Figure 1: Subdivided plant network.



.4 Implementare la protezione dai ritorni di loop (loopback) dello switch

Molti switch Ethernet moderni prevedono la possibilità di individuare i ritorni di loop, cosa che mette al riparo dalla creazione accidentale di un loop. Questa funzionalità prevede l'invio periodico di pacchetti di protocollo di loop a partire da una porta attivata per l'individuazione del ritorno di loop. Se la porta riceve successivamente lo stesso pacchetto, essa viene disattivata automaticamente e il diffondersi in loop dei pacchetti é bloccato. Molti switch odierni supportano il protocollo RSTP (Rapid Spanning Tree Protocol) per poter conservare la topologia di rete priva di loop allorché si utilizzano reti ridondanti. L'RSTP, i loop e la ridondanza di rete sono argomenti piu' avanzati, non approfonditi dal presente suggerimento tecnico.

Figure 2: Storm Control configuration page for a Cisco 8-port managed switch.

Storm Control

Storm Control Table

			Broadcast Storm Control			Multicast Storm Control			Unicast Storm Control		
	Entry No.	Port	Mode	Threshold	Threshold Type	Mode	Threshold	Threshold Type	Mode	Threshold	Threshold Type
○	1	g1	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	2	g2	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	3	g3	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	4	g4	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	5	g5	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	6	g6	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	7	g7	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	8	g8	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps

.5 Formazione del personale

Per ridurre la possibilità di errore umano é importante formare in modo corretto il personale che interviene a livello di rete. Disporre di conoscenze di base sul funzionamento della rete, nonché saper riconoscere i tipi di tempeste di traffico e saperli prevenire, puo' evitare possibili errori, puo' aiutare a riconoscere i problemi piu' comuni e migliorare quindi la capacità di segnalare in modo preciso eventuali anomalie. Disporre di tecnici in grado di servirsi di un programma di cattura di rete, tipo Wireshark, per registrare gli eventi di rete, puo' notevolmente migliorare la capacità del supporto clienti di CTI a contribuire alla soluzione di un determinato problema di comunicazione.

Conclusione

Ethernet rivoluziona senza sosta i sistemi di controllo industriale. Man mano che i produttori esplorano l'Industrial Internet of Things (IIoT) ed installano sempre piu' dispositivi collegati ad Ethernet, diventa vitale saper capire e gestire i rischi dovuti alle tempeste di traffico Ethernet. Questo suggerimento tecnico fornisce giusto una veduta d'insieme sui rischi legati alle tempeste di traffico e sulle misure da adottare per prevenirle o attenuarle.