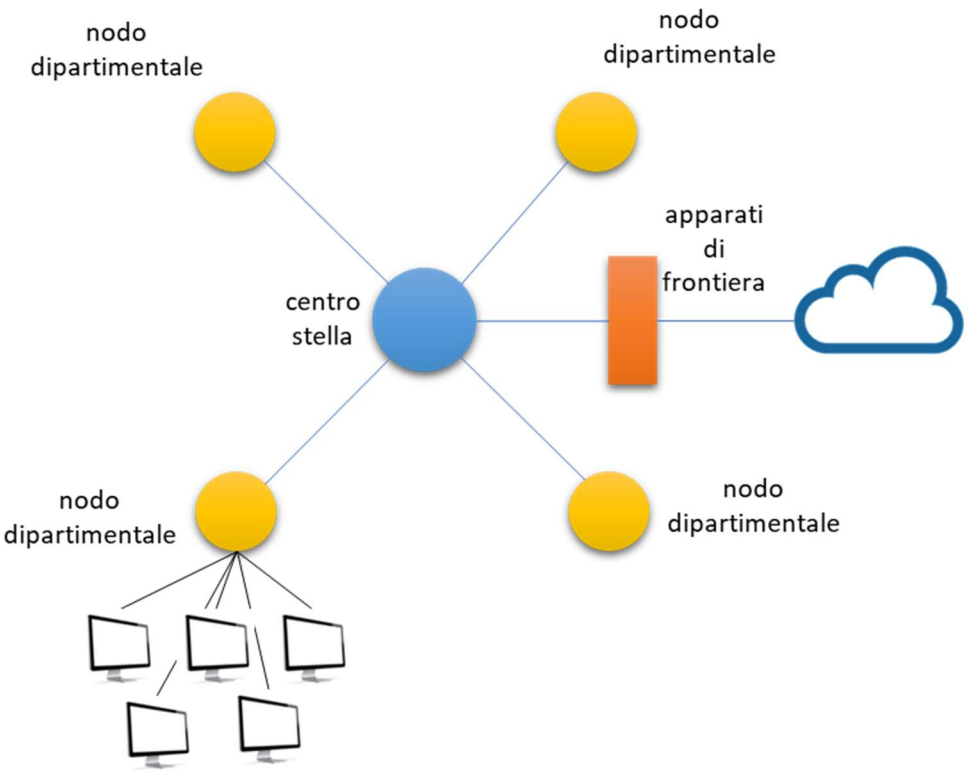
Le reti telematiche sono un vero e proprio ecosistema sul quale insistono moltissime componenti: attive, passive, topologiche, di mezzi trasmissivi, di architettura etc.

Non è mia intenzione entrare nel merito di ognuna di esse, né tantomeno farne dissertazioni tecniche.

Vorrei, invece, far emergere alcuni aspetti fondamentali in termini di resilienza e sicurezza delle reti. Questo perché è oramai irrinunciabile per ogni azienda definire a priori gli impatti di una indisponibilità (sulla rete o su una sua parte, sia interna che di comunicazione verso il Web) così come lo è garantire il massimo della riservatezza e sicurezza nella trasmissione dei dati, anche in virtù degli specifici obblighi normativi (ad es. il GDPR)

Limitiamoci pertanto ad alcuni scenari caratteristici e partiamo da uno schema che dovrebbe essere noto ai più

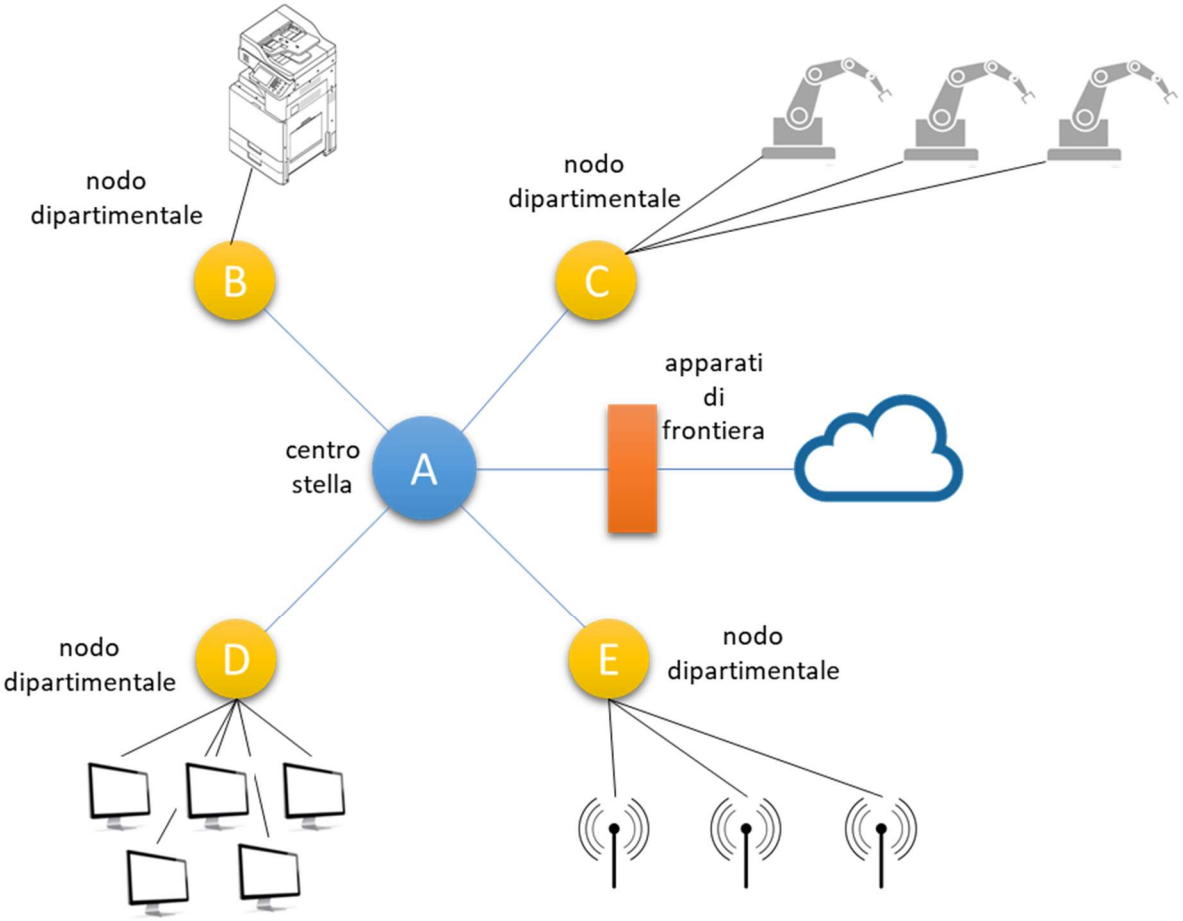


Si tratta di una rete disegnata “a stella”, dove un apparato controlla e gestisce il flusso dati da e per i nodi dipartimentali, cui sono collegati gli utenti e altri device di utilità. Al centro stella afferisce anche l’unità di comunicazione da e verso internet (il router), solitamente protetta da un firewall.

Aggiungiamo pochi elementi: un insieme di access point per costituire una rete wireless (sia essa in produzione, o in magazzino o semplicemente quella che eroga il servizio agli ospiti in sala riunioni) ed alcuni apparati interconnessi alla rete e gestiti dai fornitori (es: una multifunzione monitorata e gestita dal fornitore di servizi di

copia, oppure alcuni macchinari di produzione, anch'essi interconnessi con i sistemi aziendali e gestiti da remoto dal fornitore per le operazioni di manutenzione e/o assistenza)

La nostra rete ha assunto questo aspetto



Proviamo ad ipotizzare alcuni scenari di disfunzioni ("fault") che impattino parzialmente sulla disponibilità delle comunicazioni e sulla loro sicurezza oltre a un vero e proprio "Digital Disaster".

Scenario 1

Si rende indisponibile a causa di un guasto la linea di comunicazione tra centro stella "A" e nodo dipartimentale "C". In tal caso i sistemi di produzione non potranno più comunicare i propri dati al server (dati di avanzamento produzione, conteggi dei pezzi lavorati, …), né questo potrà inviare dati alle macchine (ad es. i part program, o i dati del gestionale relativi al lotto da produrre).

L’impatto potrebbe essere pesante ed impattante, in particolare se tali dati vengono poi elaborati per sviluppare i processi trasversali alla logistica, all’area commerciale e all’amministrazione.

Scenario 2

Si rende indisponibile la connessione internet. Ciò significa incapacità di comunicare dati verso l’esterno o di riceverne. Se è vero che opportune configurazioni di sincronizzazione con gli apparati mobili come gli smartphone potrebbero mettere gli utenti nelle condizioni di gestire, almeno parzialmente, le proprie mail, l’impatto sarebbe comunque di rilievo per tutti quei servizi in outsourcing (si pensi ad esempio a quelli “in cloud”) o per gli utenti remoti che hanno bisogno di accesso ai dati aziendali (ad esempio le forze vendita distribuite sul territorio).

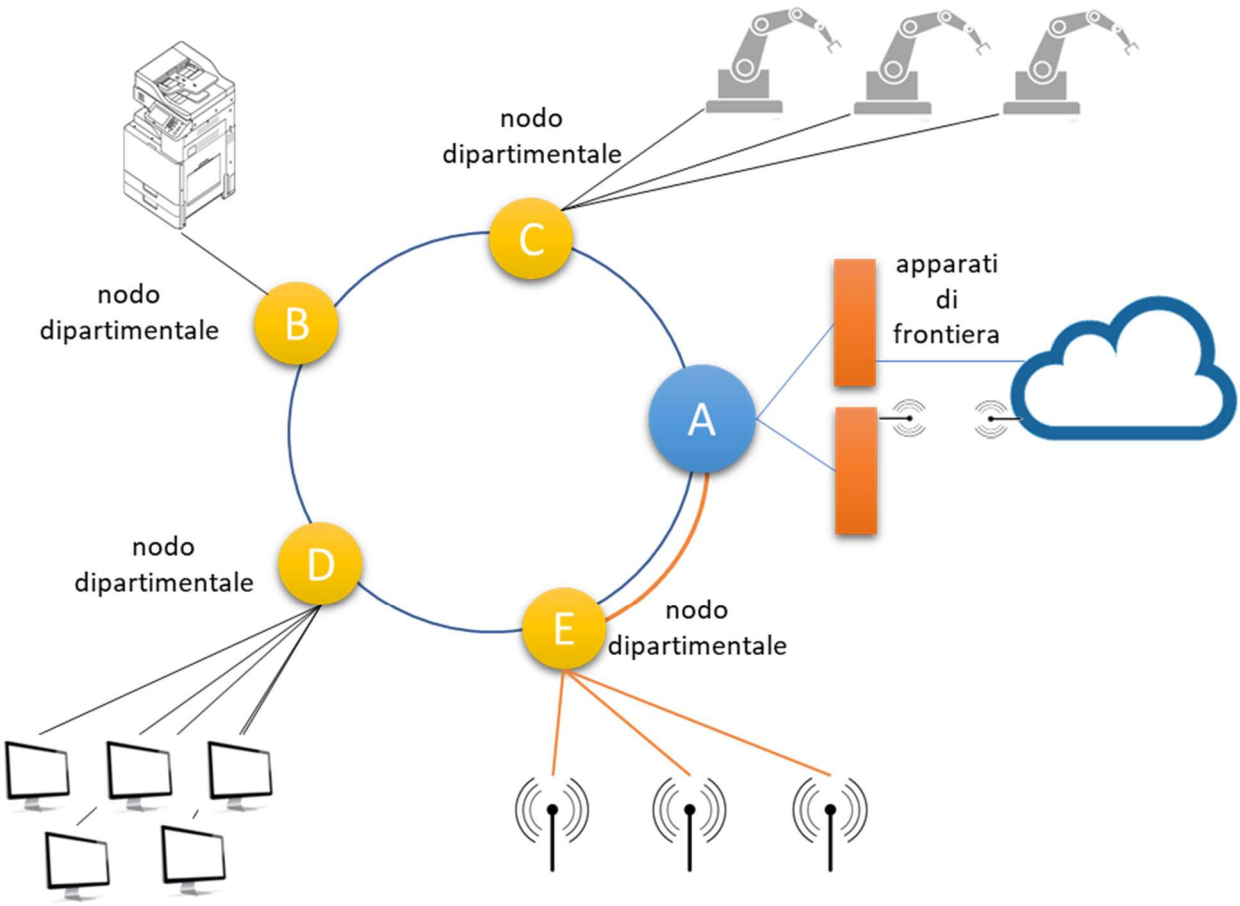
Scenario 3

Il nodo focale della rete, il centro stella, subisce un danno e diviene indisponibile. In questo caso le conseguenze sono facilmente intuibili: praticamente nessuno dei servizi aziendali risulta operativo e l’impatto sarebbe quasi devastante.

Come progettare, pertanto, una rete telematica che possa far fronte a situazioni di questo tipo limitando al massimo gli impatti, correlando tali eventi con i rischi che essi si manifestino, bilanciando il tutto con le esigenze strategiche e di budget dell’azienda ?

L’esperienza che Fill In The Blanks ha maturato sul campo, i progetti realizzati, le situazioni cui i sistemi sviluppati han dovuto reagire ci permette di dire che la scelta non è mai meramente tecnologica o economica o strategica o normativa. Si tratta invece di un **mix** opportunamente studiato e calibrato di ciascuna di queste componenti. Un mix che, quasi sempre, si concretizza in una soluzione su misura.

Cominciamo pertanto a dare delle risposte agli scenari sopra illustrati e pensiamo ad una rete progettata, ad esempio, in questo modo:



Innanzi tutto il disegno topologico è divenuto ad “anello”. Non è la soluzione a massima resilienza ma si tratta di un buon compromesso. Ogni nodo dipartimentale ha sempre due percorsi fisicamente distinti verso il centro di distribuzione delle informazioni (il nodo “A”). Particolari nodi dipartimentali che richiedano forti workload possono inoltre essere serviti da dorsali a più alta capacità (es. la fibra). La rottura della dorsale ipotizzata nello scenario 1 non costituisce più un problema. I sistemi attivi della rete dirottano i flussi sull’altra linea di comunicazione, senza impatto alcuno sull’operatività e in modalità automatica (“unattended”). A maggior ragione questa soluzione risponde alle esigenze di Disaster Recovery presentate nello scenario 3, visto che non esiste più un nodo “centro stella”.

La presenza nel progetto di due apparati di frontiera distinti e connessi a due linee di comunicazione verso il WEB, diversificate per supporto trasmissivo (ad esempio una linea in Fibra ed un link radio) permette l’implementazione di molteplici funzioni di ottimizzazione dei flussi come il bilanciamento di carico tra i due apparati o lo spostamento dei protocolli band-intensive sulla linea più performante. In modo particolare, però, questo progetto consente di dirottare tutti i flussi su una delle due linee di comunicazione qualora la seconda risultasse indisponibile. Anche in questo caso l’operazione può essere effettuata automaticamente e senza intervento di alcun operatore.

Infine: come offrire la disponibilità di connessione Internet agli ospiti, senza però intaccare la riservatezza della rete aziendale? Come rappresentato nel progetto – dorsale “rossa”- si delega ai sistemi di rete la gestione di una rete “virtuale” separata (VLAN). Dal punto di vista fisico essa è implementata sulla stessa infrastruttura di quella aziendale, dal punto di vista logico, invece, essa costituisce una rete assolutamente autonoma. Ciò avrebbe senso anche per tutti gli attori che interagiscono con i sistemi aziendali, come ad esempio i manutentori degli apparati di copia o dei sistemi informatizzati di reparto.

Pochi cambiamenti al progetto di rete originale, pertanto, hanno indotto grandi vantaggi in termini di resilienza e di sicurezza oltre a fattori, non trascurabili, di riservatezza delle informazioni private o riservate.

Ce ne sono molti altri che possono essere declinati in funzione delle specifiche esigenze di ogni cliente e che gli esperti di Networking di Fill In The Blanks potranno descrivervi.

La prossima puntata la dedicherò al Backup e al Disaster Recovery dei dati.

Stay connected!

Andrea Bertoni

CEO di Fill In The Blanks srl