Lesson 7: Congestione di rete e mappatura

Premessa

Nei capitoli precedenti abbiamo dato ampio risalto ai problemi che possono scaturire a fronte di configurazioni non appropriate di apparati e devices di rete. Questi argomenti sono molto legati alla sicurezza e alla protezione della rete, problematiche in grado di creare danni all'immagine dell'Azienda. La lezione attuale si concentra sulla disponibilità e produttività della rete aziendale e di come, la riduzione o la mancanza di uno o di entrambi gli elementi, costituisca un grave danno per l'organizzazione.

All'interno di questo documento analizzeremo le modalità di progettazione e implementazione di una "corretta architettura di rete" in grado di garantire la continuità di servizio. Evidenzieremo nel contempo come la funzione di "monitoring" applicata alla stessa diventi parte fondamentale della sua gestione. Per gestione non si intende solo la sua amministrazione quotidiana, ma anche la "prevenzione attiva" dei problemi e il rilievo delle performances.

Uno dei problemi maggiormente evidenziato durante gli audit è relativo a errori di collegamento o configurazione degli apparati di rete che ne possono mettere a repentaglio la stabilità. Grazie a sistemi di controllo, "**come quello proposto in allegato alla lezione"**, abbiamo evidenziato colli di bottiglia tra apparati o tra questi e Key device (server applicativi o sistemi Core). In prima analisi questi errori provocavano un crollo delle prestazioni della rete, ma alle volte andavano a variare le operazioni di Back-up alterandone le finestre temporali.

E' di fondamentale importanza mappare gli utenti connessi (Network Assessment) tracciando con precisione la loro connessione in modo da sapere sempre ed esattamente da dove si connettono e verso quale risorsa/applicazione di rete. Tale operazione consente di identificare e isolare i problemi molto rapidamente ottimizzando così i tempi di intervento e di DOWN della rete o di parte delle sue risorse.

Una volta tracciata la mappatura della rete è fondamentale controllarla continuamente ed eventualmente aggiornarla possibilmente in tempo reale. Questa operazione è ad appannaggio del sistema di monitoring.

Il sistema di monitor può essere indifferentemente implementato all'interno o all'esterno dell'azienda, fondamentale è il suo settaggio (tuning) attraverso il quale è possibile rendere il sistema **proattivo** profilandolo sulle policy aziendali e sulla propria architettura di rete. A tal proposito è fondamentale ricordare che le policy di rete così come la sicurezza non sono un prodotto finito, ma un progetto che si trasforma nel tempo. Credere di installare un sistema di monitoraggio una volta per tutte senza aggiornarlo costantemente **significa gettare quattrini, tempo ed esporre il proprio sistema informativo a rischi enormi.**

Architettura di rete

Alta affidabilità

Il tema della continuità di servizio è particolarmente sentito nelle reti e soprattutto in quelle Ethernet (IEEE802.3) che rappresentano circa il **99,8%** del totale installato nel mondo. Nonostante questa diffusione uno degli aspetti ancora oggi purtroppo sottovalutato in fase di progettazione è quello relativo alla messa in sicurezza dell'infrastruttura. Per sicurezza si intende la protezione della rete rispetto agli incidenti che possono impattare sulla continuità di servizio. Solo una minima parte (**meno del 4%**) delle reti è progettata per "resistere" in caso di guasti su uno o più componenti che la costituiscono. Da una recente indagine condotta sulle cause di disservizio alla rete locale, compaiono, in ordine di frequenza, il guasto all'alimentazione (Power Supply) e l'errore di configurazione (Misconfiguration).

Di seguito riportiamo una lista delle problematiche più comuni che si possono rilevare:

Blocco delle operazioni – Incidenti al Centro Stella

- **Mancata alimentazione** - Failure dell'alimentatore Centro stella.
- **Mancata alimentazione** – Interruzione nella erogazione dell'energia elettrica (assenza UPS).
- **OverTemp** (temperatura eccessiva) – Guasto alla ventola del Centro stella.
- **Errata tensione di alimentazione** – VA difformi dovuti al provider dell'energia elettrica (assenza stabilizzatore).
- **OverTemp** (temperatura eccessiva) – Guasto al condizionamento wiring closet (circuito elettrico).
- **Guasto della switch fabric** del Centro stella.
- **Guasto sul modulo** porte utenti o server.
- **Guasto sulla porta** del downlink verso utenti o server.
- **Interruzione della connessione** dovuta al cablaggio (agenti esterni o operazioni accidentali).
- **Interruzione della connessione** sul Patch Panel o sulla porta switch dovuta al cablaggio (tensione e curve cavi nel rack).
- **Reboot del sistema** – dovuto a Loop di pacchetti o frame (software).
- **Misconfiguration** – dovuto ad errore nella configurazione dello Spanning Tree o del VRRP.

Spesso si verificano incidenti in successione che paiono spesso concatenati tra di loro in una sorta di effetto domino difficile da risolvere in tempi accettabili utili per non impattare negativamente sulla operatività dell'organizzazione.

Facciamo un esempio:

Si guasta il condizionamento del wiring closet e le temperature di esercizio causano un guasto alla fabric (il componente più fragile e sofisticato del centro stella). Potrebbe succedere che, ancora prima della segnalazione di guasto al condizionamento, l'amministratore di rete venga travolto dalle problematiche relative al blocco del centro stella causato dal crash della Fabric.

Ma cosa sta succedendo nella realtà:

- **L'attenzione dell'amministratore è distolta dal guasto principale** in quanto quello secondario sta provocando il fermo della rete.
- La sostituzione della Fabric non ha risolto ma è servita solo ad eliminare uno degli effetti del problema principale. **La causa è rimasta**.
- Si manifesta a questo punto il secondo effetto. L'amministratore di rete si accorge dell'aumento della temperatura dovuto al bocco del condizionatore.
- Si provvede al ripristino dell'elettricità in modo che il condizionatore riprenda a funzionare. **Adesso si è eliminato il problema principale**.

E se nel frattempo la temperatura non scendesse abbastanza velocemente in modo da scongiurare il guasto della Fabric appena installata?

Oppure:

si verifica uno spike sulla rete elettrica (sovratensione) con la conseguenza attivazione delle protezioni del Power supply e il blocco dell'alimentazione. Alla ripartenza, eseguita in modalità automatica senza prevedere la disinserzione delle utenze e la loro progressiva riattivazione, si verifica un problema sulle ventole e…….

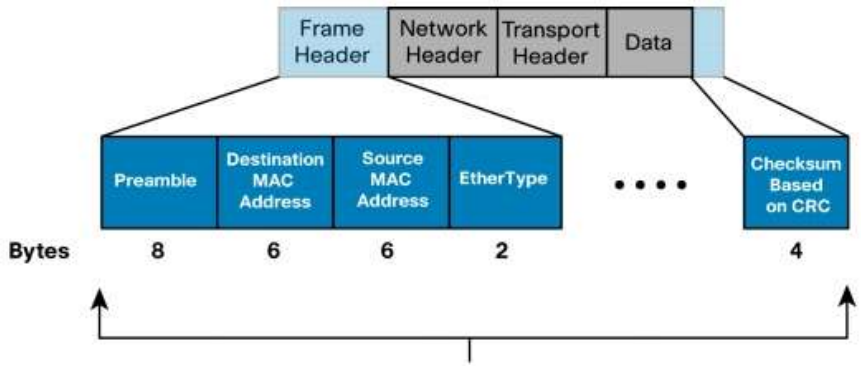
della serie, i guai non si presentano mai soli!!!!!!!!!!!!!

Ma è solo causa della malasorte oppure anche noi abbiamo le nostre responsabilità? Andiamo con ordine.

L'infrastruttura tradizionale

La maggior parte delle topologie di rete disegnate dai progettisti risente ancora oggi di nozioni e metodiche apprese negli anni '90, quando il design di rete imponeva delle scelte pressoché obbligate. Il modello dominante per certi versi si ricollega ancora all'epoca in cui la maggior parte delle funzioni di rete venivano espletate da un router o meglio da "one armed router" che svolgeva principalmente le seguenti attività:

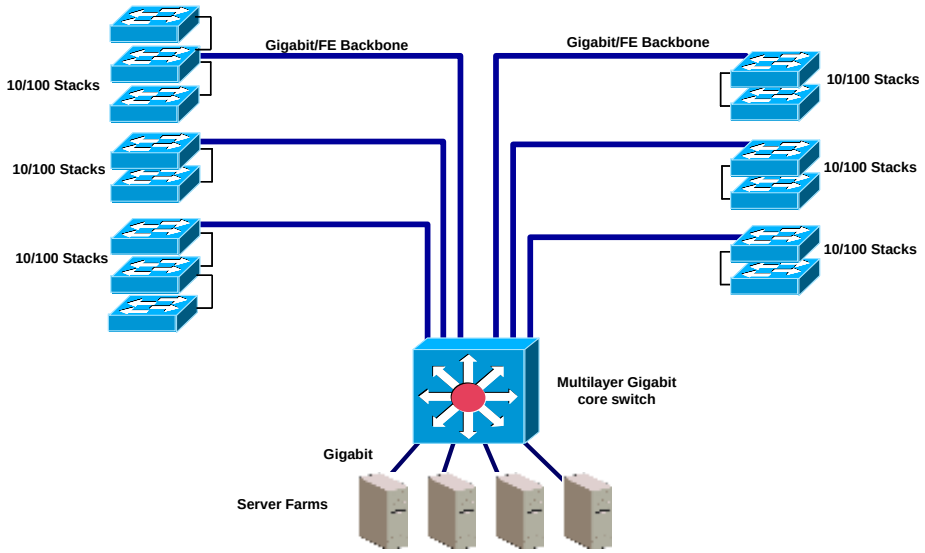
esaminare pacchetti di livello 2 e instradarli alle Subnet o alle VLAN di riferimento.



Peccato che, per tale attività, fosse impiegata una tecnologia che ispezionava il pacchetto alla ricerca non solo della destinazione e del mittente, ma pure del contenuto stesso

dell'informazione. Questa procedura veniva ripetuta per ogni frame e su ogni pacchetto nella sessione attiva a detrimento delle velocità di smaltimento delle trame Ethernet che vanno da e verso il centro stella. La logica era appunto quella di **creare una rete intelligente in uno solo dei componenti** (l'elemento al centro della rete) circondandolo da una serie di dispositivi più o meno stupidi. Tale metodologia ha subito poche variazioni anche quando la stupidità della "periferia" si è andata tramutando in una sempre maggiore sofisticazione, al punto di processare direttamente tutte le operazioni inerenti il riconoscimento degli utenti e il tagging (etichettatura) delle applicazioni. In seguito sono stati sostituiti i Router con i ben più agili "Switch Layer 3" (**1997**) che oggi rappresentano la totalità degli apparati posti al centro stella di una rete locale.

Possiamo quindi sintetizzare l'approccio "conservatore" in un disegno come quello sotto riportato, che vede appunto la "periferia stupida" totalmente asservita ad un solo chassis di centro stella che si rende di proposito il più possibile "robusto" attraverso l'adozione di doppia CPU e doppia alimentazione.



(fig. 1) La progettazione tradizionale

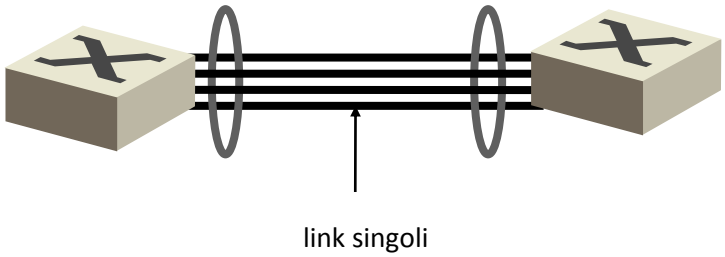
E' evidente nella rete rappresentata in fig.1 la somma dei "vizi" progettuali ereditati dal periodo pionieristico delle reti, allorquando la loro robustezza era decisamente meno importante rispetto all'elemento sperimentale che ne caratterizzava l'implementazione. Vediamo infatti che gli switch periferici sono connessi con una sola scheda in fibra al centro stella. In tal modo si penalizzano le prestazioni e, soprattutto, si determina un pericoloso "vulnus" costituito appunto da quell'unica scheda che è in grado di isolare, nel caso di guasto, tutti i client attestati in periferia. Questo modo di progettare è contro le più elementari regole che sovrintendono una rete con **Mission Criticality superiore al 99,99%**.

Link Aggregation (IEEE 802.3ad)

Altrimenti conosciuto come "trunking", la link aggregation opera a livello 2 del modello Open Systems Interconnection (OSI) ed è in grado di aggregare link multipli Fast Ethernet o Gigabit

Ethernet tra diversi dispositivi quali Client, Server e Switch, creando di fatto un unico "trunk" che moltiplica la banda passante disponibile per il numero di porte che vengono così aggregate.

- Combina due o più Fast Ethernet (nell'esempio 4) links con un unico link da 800Mbps tra 2 switch (i link sono da 100Mbps ed essendo full duplex portano la banda supportabile a 200Mbps ciascuno).
- Combina due o più Gigabit Ethernet link tra due apparati attivi.
- È uno standard (IEEE 802.3ad) dal 6 Marzo 2000.



(fig. 2) Link Aggregation – schema

Se uno dei link fisici (cavo) o una delle porte dello switch dovesse guastarsi, il trunk realizzato manterrebbe in vita le connessioni pur riducendo il data rate. In questa modalità la banda tra due switch può essere incrementata aggiungendo un link ulteriore, senza dover sostituire il dispositivo con un più moderno switch dotato di connessioni high speed.

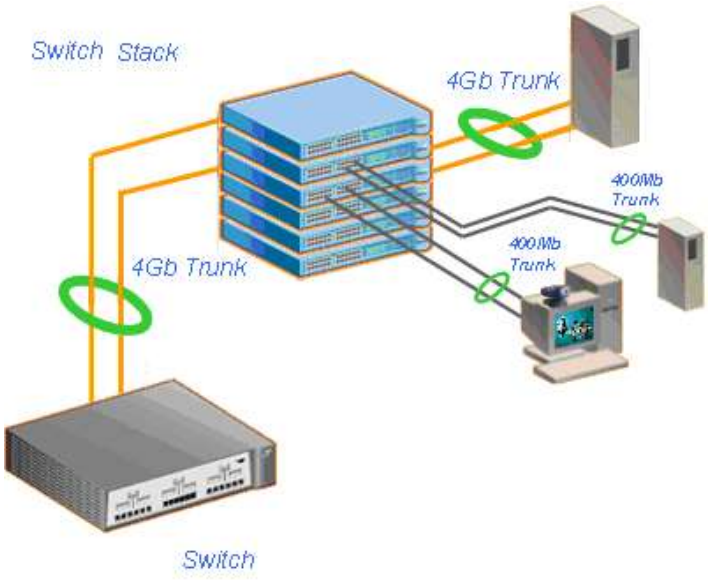
Attenzione però al conto economico, perché con la riduzione dei prezzi relativi alla tecnologia Gigabit, l'esercizio del truncking sta iniziando a mostrare la corda. Il costo incrementale di una connessione nativa Gigabit su 1000BaseT è già inferiore rispetto ad una doppia connessione Fast Ethernet 100BaseT. Il risultato è evidentemente sfavorevole al trunking nel momento in cui si debbano "aggregare" due o più link Fast Ethernet. Con il prezzo di due porte Ethernet (che poi diventano 4 considerando i due lati della connessione) si può acquistare un "Uplink Gigabit" come modulo opzionale, in dotazione ormai a tutti gli Switch di ultima generazione.

Se la Link Aggregation viene vista invece come resilienza, il quadro cambia in quanto rientra in una corretta politica di gestione delle risorse di rete. Nelle soluzioni odierne il Trunking 802.3ad è utilizzato per connettere in modo "sicuro" gli switch periferici verso un server piuttosto che verso il centro stella Layer 3. In quest'ultimo caso è bene rimarcare un'importante prerogativa che hanno alcuni switch rispetto ad altri apparati.

Trunking multistack

Con questo termine si configura un comportamento particolare che consente a una pila di switch collegati tra loro di poter comunicare in modo contemporaneo attraverso due o più

"calate"(connessioni) verso il centro stella.

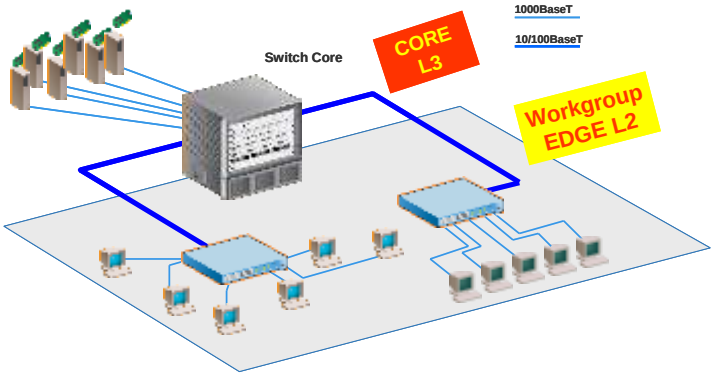


(fig. 3) LACP 802.3ad – le capacità degli switch intelligenti

Nell'esempio in Fig. 3 vediamo che la "pila" o stack che dir si voglia, costituita da 5 switch è in grado di gestire un totale di otto connessioni verso dispositivi esterni alla "pila" attraverso la metodologia **802.3ad.** Con questa modalità si assicura un doppio link verso lo switch di centro stella e un doppio link verso il server dotato di due schede Gigabit "Dual Homing" (in grado cioè di bilanciare il carico sulle due diverse interfacce).

La progettazione Core Chassis tradizionale

La rete rappresentata in fig. 4 ha un numero elevato di "single point of failure". Generalmente il progettista di tale soluzione si limita a rinforzare il centro stella con un doppio Power Supply e una Fabric supplementare (molto costosa). In pratica si realizza un raddoppio di CPU, che subentra nel caso in cui la fabric principale dovesse guastarsi. Con questa configurazione si pagano due engine (fabric) molto costose e si finisce per usarne una sola che è quella in produzione. L'altra engine, infatti, rimane in stand by, ed entra in azione solo a fronte in di un evento infausto che causa la disattivazione della principale. In pratica funzionano solo una alla volta. Le workstation hanno una singola scheda di rete connessa a un unico switch di Layer 2. Anche lo switch ha un'unica connessione verso "**l'unico**" centro stella 3.



(fig. 4) Progettazione ONE Core CHASSIS – l'approccio tradizionale

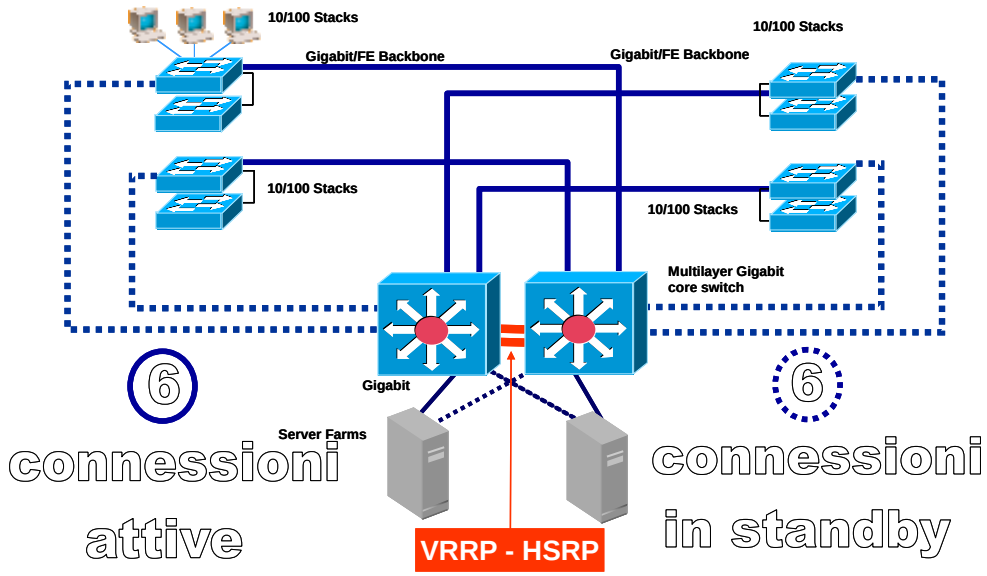
Questa rete non garantisce la continuità operativa delle 12 condizioni sotto riportate che definiscono la Mission Criticality di una rete distribuita di classe enterprise. Le condizioni che è in grado di sopportare a livello di eventi negativi sono solo le due evidenziate in grassetto, la numero 9 e la numero 10:

1. Rottura di una scheda di rete nella WST.
2. Interruzione della connessione tra WST e Switch di Periferia (Workgroup L4).
3. Guasto di una porta nello switch di periferia.
4. Rottura di uno switch di periferia.
5. Guasto dell'interfaccia di collegamento tra periferia e centro stella.
6. Interruzione di un link fisico tra periferia e centro stella.
7. Guasto di una porta/modulo del centro stella su cui è attestato il link alla periferia.
8. Rottura di uno switch di centro stella.
9. **Guasto della scheda principale (Fabric) del Centro stella.**
10. **Guasto di un Power Supply del Centro stella.**
11. Interruzione di un link tra centro stella e Server.
12. Rottura di una scheda server.

Due condizioni su 12 sono davvero troppo poche per potersi proporre con efficacia in una logica di Mission Critical e sono da considerarsi a tutti gli effetti totalmente inadeguate alle odierne richieste di continuità operativa.

La progettazione DUAL Core Chassis tradizionale

La rete rappresentata in fig. 5 abbassa il numero di single point of failure, in quanto raddoppia i "CORE SWITCH modulari", evitando peraltro l'inserzione di un doppio Power Supply e di una Fabric supplementare su ognuno degli switch di centro stella.



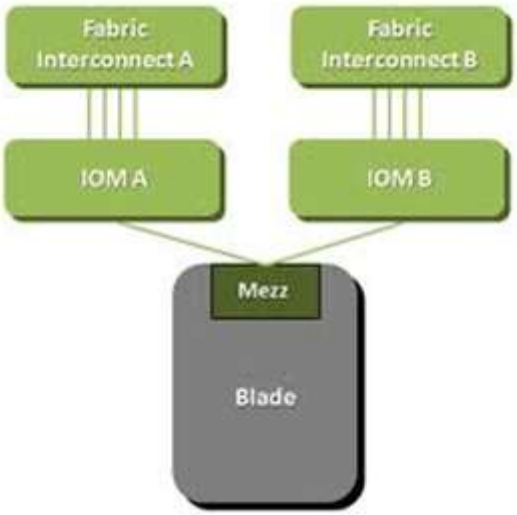
(fig.5) Progettazione DUAL Core CHASSIS – l'approccio tradizionale

Le linee tratteggiate danno l'idea di come questa topologia funzioni. Di solito, per evitare complicazioni nella configurazione, si mettono in stand by le connessioni tratteggiate in modo tale da non usarle effettivamente (tali connessioni sono a tutti gli effetti in grado di spostare pacchetti esattamente come le connessioni "piene"). Questa condizione impiega i protocolli VRRP o HSRP per attivare la "ridondanza" tra i Core switch.

La rete con due chassis ha un minore numero di single point of failure e continua a funzionare anche quando le condizioni enumerate qui di seguito si realizzano:

1. rottura di una scheda di rete nella WST.
2. Interruzione della connessione tra WST e Switch di Periferia (Workgroup L4).
3. Guasto di una porta nello switch di periferia.
4. Rottura di uno switch di periferia.
5. Guasto dell'interfaccia di collegamento tra periferia e centro stella.
6. Interruzione di un link fisico tra periferia e centro stella.
7. Guasto di una porta/modulo del centro stella su cui è attestato il link alla periferia.
8. Rottura di uno switch di centro stella.
9. Guasto della scheda principale (Fabric) del Centro stella.
10. Interruzione della connessione VRRP.
11. Guasto di un Power Supply.
12. Interruzione di un link tra centro stella e Server.
13. Rottura di una scheda server.

Oltre a questo approccio ne esiste uno ulteriore che prevede doppio Chassis e che inserisce doppia CPU, Doppio Power Supply e doppio FAN su ognuno degli Chassis. Decisamente antieconomico e statisticamente poco probabile quest'ultimo approccio è destinato soltanto a chi non ha problemi di Budget.



Software di gestione SNMP

Switch Center

Switch Center è una suite completa di gestione che aiuta a scoprire, monitorare e analizzare la connettività di rete e le prestazioni. Rappresenta una valida soluzione per la manutenzione della rete stessa. Tutte le sue funzionalità operano in tempo reale.

Il software mappa l'esatta ubicazione dei nodi di rete e la loro attività. Analizza il traffico in percentuali di utilizzo, di pacchetti broadcast e di eventuali errori tenendo aggiornato l'utente sui potenziali malfunzionamenti della rete.

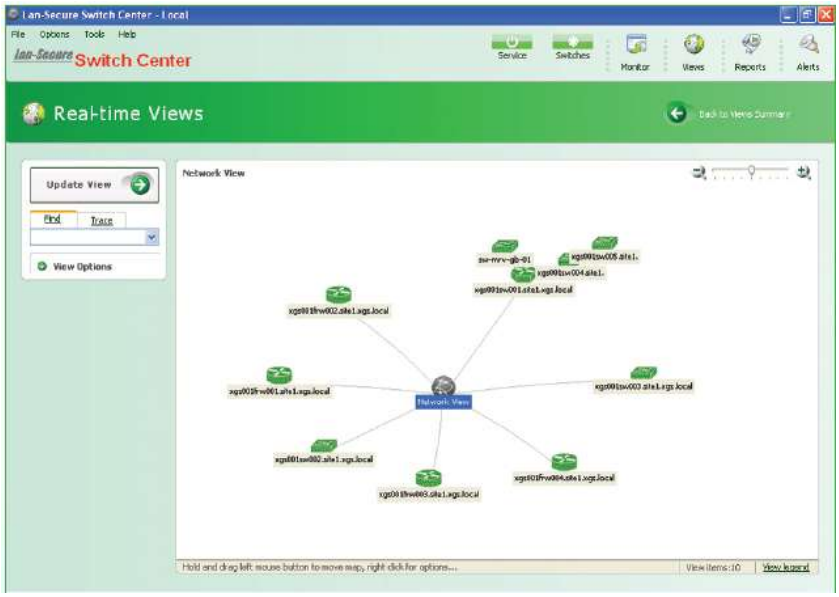
In automatico viene effettuato il "discovery" degli apparati di rete dotati di agent SNMP (vedi importanza nella lezione inerente gli apparati attivi di rete). Presenta in modalità grafica interattiva la mappatura e le connessioni della rete. Evidenzia la tipologia delle connessioni, in modo da poter individuare con un semplice colpo d'occhio incongruenze di connessione.

Cliccando sui singoli devices mostra il dettaglio relativo all'utente selezionato, evidenziando la tipologia di connessione, la sua ubicazione e i dati relativi quali Mac Address, IP Address, etc..

Nel caso di Monitor su di un device non SNMP viene evidenziata l'intera nuvola delle connessioni presenti sulla singola porta dello switch. Il non utilizzo dell'SNMP è fortemente sconsigliato in quanto rappresenta una connessione non gestibile.

Se settato appositamente il sistema avvisa ad ogni nuova connessione di un nuovo device fornendone immediatamente l'identità e l'ubicazione. L'amministratore di rete troverà questa funzione estremamente utile in quanto lo porrà nella condizione di controllare in tempo reale se la nuova connessione rappresenta un pericolo per la sua struttura o una nuova connessione/utente da registrare. In questo secondo caso verrà automaticamente modificata la

mappatura della rete



E' possibile esportare la mappa in Visio mediante appositi tools in modo tale da poter disporre sempre e velocemente l'esatta istantanea della propria rete.

E' possibile fare attente analisi e statistiche con sistemi di business intelligence in grado di interfacciarsi con il sistema. Tutti i dati raccolti possono essere salvati su DB Access o SQL, in modo da poterli riutilizzare per effettuare analisi o una reportistica puntuale e aggiornata. E' anche possibile verificare le performances della propria rete a livello grafico identificando così immediatamente eventuali problemi o colli di bottiglia.

Conclusioni

Durante le fasi di Audit questi strumenti vengono utilizzati per fare una fotografia della rete a livello di architettura, per rilevare tutti gli apparati di rete SNMP e verificarne lo stato.

Grazie al software impiegato è possibile fornire all'amministratore di rete la mappatura di quali siano i device connessi e dove siano ubicati. Qualora ci fossero problemi di broadcast, multicast o unicast che rallentano le performance della rete sarebbero immediatamente evidenziati. Anche la presenza di eventuali errori quali allineamento, CRC, etc. verrebbero evidenziati con l'indicazione del device incriminato. Infine per alcune problematiche quali i colli di bottiglia verranno forniti suggerimenti per eliminarli.

Come risulta evidente da quanto sopra esposto l'importanza dell'utilizzo di un software di monitoring e di gestione è fondamentale per tenere sotto controllo il nostro patrimonio informatico.

Ed è proprio per questa ragione che alleghiamo alla presente lezione un Link attraverso il quale è possibile scaricare un'applicazione che una volta installata permetterà all'amministratore della rete di toccare con mano l'importanza del Monitoring e di verificare che:

Lavorare senza informazioni, o peggio ancora con quelle sbagliate, **è come operare al buio**.

Lavorare invece con le informazioni giuste e aggiornate in tempo reale……..

E' tutta un'altra cosa!!!

Il Tuo EterNet Team