Lesson 3: Protezione apparati di rete

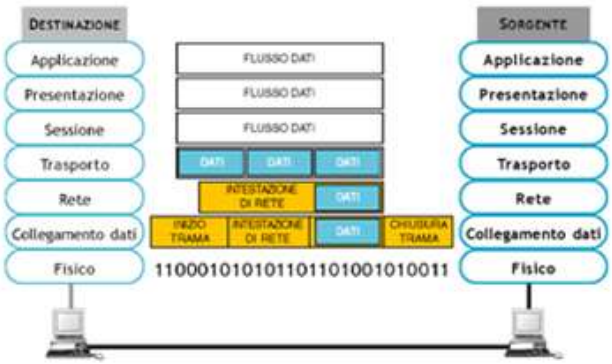
Gli Apparati di Rete

Prendiamo ora in considerazione le apparecchiature che realizzano, una volta connesse tra di loro la struttura della nostra rete informatica. Col termine apparati di rete attivi ci si riferisce comunemente ai dispositivi che gestiscono il traffico e la struttura del flusso dati nelle reti informatiche. Lo scopo principale di questa lezione è quello di verificare se gli apparati di rete sono stati installati e configurati in modo corretto tra di loro o verso il mondo esterno risultando di fatto una struttura informatica sicura come spiegato nelle lezioni precedenti. Nell'ambito di un progetto di rete sono di fondamentale importanza le modalità con le quali la rete stesse viene concepita, realizzata, e mantenuta efficiente. In particolare, rappresentano per quanto riguarda gli apparati che la compongono risultano determinanti le seguenti fasi:

- l'installazione,
- la configurazione,
- l'aggiornamento del firmware o del sistema operativo,
- l'amministrazione,
- un' accurata politica di sicurezza,
- il monitoraggio.

Quali sono gli apparati di rete

Gli apparati di rete più diffusi e normalmente impiegati all'interno delle reti, vanno a posizionarsi all'interno della pila di protocolli ISO/OSI in funzione della funzionalità che svolgono nel processo di trasporto dei dati e sono:



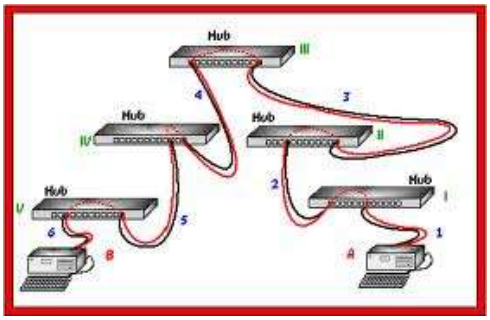
- Repeater
- Hub
- Bridge
- Switch
- Router

Repeater

Sono dispositivi elettronici che rigenerano il segnale elettrico che si è attenuato per perdita di potenza a causa della lunghezza del cavo. Dopo averlo rigenerato lo ritrasmettono su di un nuovo segmento di rete. In questo modo garantiscono un livello di segnale ottimale su ognuno dei segmenti di rete che interconnettono. Possono essere connessi in modo seriale sino ad un massimo di 4 repeater. La distanza che possono coprire dipende dalla tipologia di cavo impiegato nella realizzazione della rete. Lavorano al livello più basso "fisico" della pila ISO/OSI,

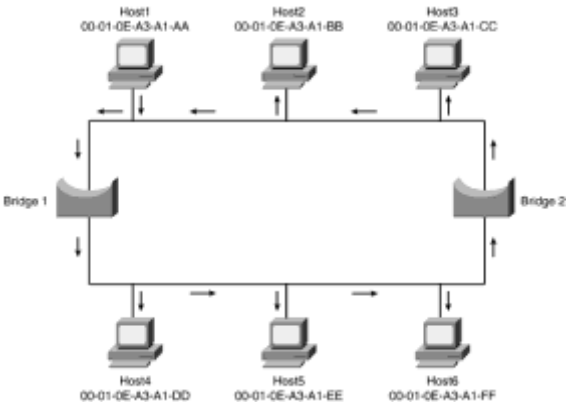
e non prevedono nessun meccanismo atto alla gestione dei dati, pertanto non delimitano né i domini di collisione né quelli di broadcast (ormai raramente utilizzati).

Hub



E' un ripetitore multi porta che mette in comunicazione più pc sulla stessa LAN. Anche lui, come il repeater precedente, non consente una connettività seriale oltre i 5 apparati. Realizza un nodo direte all'interno del quale realizza la concentrazione degli host connessi alle sue porte (**rete a stella**). Nell'hub i dati entrano in una "**porta**" e vengono replicati ed instradati verso tutte le altre esclusion fatta per quella di provenienza. Viene usato come centro-stella e consente di connettere le periferiche e di estendere le connessioni di rete. Questo apparato non contiene al proprio interno nessun meccanismo decisionale nei confronti dei dati. Per questo motivo tutti i dispositivi connessi all'hub ricevono, senza nessun filtro, tutto il traffico che attraversa l'apparato. Opera al livello più basso "fisico" della pila ISO/OSI. (Ormai raramente utilizzati).

Bridge



E' un apparato di rete più sofisticato dell'hub, e viene utilizzato per connettere due segmenti di LAN diverse tra loro (per questo viene chiamato bridge "ponte"). Questi apparati esistono per supporto di tecnologie diverse (non solo ethernet). Realizza la connessione di 2 segmenti di rete, replicando i pacchetti dati indirizzandoli intelligentemente secondo le indicazioni di una tabella di instradamento che implementa in maniera automatica in "autodescovery mode" al momento dell'accensione. Tale tabella viene poi aggiornata ogni qualvolta all'interno delle due reti connesse viene attivato un nuovo utente. Il Bridge può implementare logiche intelligenti in modo da intervenire sul passaggio dei dati da un segmento all'altro realizzando di fatto veri e propri blocchi di utenti da una LAN verso l'altra (Work Group locali). Nasce in origine dalla necessità di ridurre le lan in segmenti più piccoli, più facilmente gestibili e performanti. Implementa al suo interni protocolli intelligenti quali lo "Spanning Tree" che permette la connessione tra due reti in alta affidabilità(doppio path tra le stesse reti) evitando il loop del traffico. Il bridge opera a livello 2 "data link" della pila ISO/OSI. (Ormai raramente utilizzati).

Switch

Lo switch è un apparecchio di rete che mette in comunicazione diretta un host A con un altro host B senza che ,come accade con un hub tutti gli altri ascoltino. Viene definito anche come "bridge multi porta", in grado cioè di connettere più segmenti di rete realizzando di fatto una gestione più efficiente dei dati con conseguente incremento delle performance di rete (velocità e bandwidth o ampiezza di banda). Non realizza nessuna conversione diretta sui dati. Per la determinazione della destinazione dei dati utilizza delle "forwarding table". Al contrario dell'hub può supportare funzionalità avanzate come le VLAN (Virtual LAN). Questi apparati a seconda del S/W implementato sopra possono operare a vari livelli del modello ISO/OSI. Principalmente lavorano a livello 2, occupandosi appunto del Forwarding dei dati intervenendo al più sulle priorità dei pacchetti "802.3X". Gli Switch più evoluti invece implementano anche funzionalità di livello 3 e 4 normalmente appannaggio di altri apparati. Gli switch di Layer 2 utilizzano una tabella nella quale sono riportati i numeri che corrispondono alle porte dello switch accanto ai quali vengono associati i "mac address" degli apparati a loro connessi. Per gli switch di Layer 3 rimandiamo invece alla descrizione del Router.(Comunemente utilizzati nella realizzazione delle reti dati).

Host MAC Address	Port
00 00 80 45 FE 21	5
00 00 80 45 DA 47	3
00 40 00 80 45 FE	2
00 40 80 10 AA 21	1
00 00 80 00 FF AB	5

Router

Sono utilizzati principalmente per estendere ed interconnettere tra di loro Reti locali geograficamente distanti tra loro. Sono di solito posizionata alla periferia della rete in quanto ne rappresentano di solito la porta d'ingresso o di uscita. Sono apparati più lenti rispetto ai Bridge ed agli Switch, in quanto, dovendo essere messi in grado di prendere decisioni critiche su come instradare i pacchetti ricevuti verso le altre reti sulla base di tabelle di instradamento, hanno la necessità di leggere ed elaborare una quantità superiore di dati per cui il loro tempo di latenza è più alto. Realizzando la funzionalità di connessione tra reti diverse i routers al contrario dei bridge che possono solo connettere una rete ad un'altra possono interconnettere centinaia di reti diverse decidendone anche i percorsi in funzione di parametri quali il traffico, la qualità della connessione, la variata situazione della rete, un preciso piano di indirizzamento, etc, etc. Per questo motivo i router racchiudono al loro interno un po' tutte le funzionalità degli altri apparati di rete come concentratori, ripetitori, convertitori di dati, gestori di traffico. Un router può a seconda dell'esigenza disporre di interfacce sia di tipo LAN che WAN e può così estendere segmenti di reti locali anche tecnologicamente diverse tra loro su aree più estese (WAN). All'interno di una LAN può anche essere usato per scopi di segmentazione in modo da proteggere per esempio l'area server dall'utenza, oppure in un contesto WAN come dispositivo di interconnessione e interfacciamento tra tecnologie diverse. I routers utilizzano tabelle di routing sia costruite staticamente vedi ad esempio dall'amministratore di rete, oppure dinamicamente tramite gli automatismi forniti da appositi protocolli "routing protocols". Il router lavora a livello 3 "rete" della pila ISO/OSI. Sostanzialmente analizza i pacchetti di livello 3 cioè di indirizzi IP. L'operazione di routing, a differenza dell'operazione di switching, decide in base alle informazioni di

livello 3 "IP Address" quale strada fare prendere ad un pacchetto dati.

Non affrontiamo in questa fase le funzionalità di un firewall che saranno oggetto di una futura trattazione, ma consideriamo lo stesso parte integrante della sicurezza perimetrale della nostra rete.

Topologia di rete

Le reti odierne sono costituite principalmente da switch di Layer 2/3/4. Solitamente quelli con funzionalità di routing sono posti al centro stella e connettono gli apparati di layer 2 ubicati in periferia. A fronte di connessioni così realizzate la topologia di rete migliore da realizzare risulta essere di tipo stellare. Esistono svariate tipologie di apparati alcuni dei quali sono di tipo "intelligente" perché dotati di un S/W di management. Questa loro peculiarità li rende i più indicati in quanto consentono di monitorare la rete e le sue performances.

Il protocollo standard utilizzato per realizzare i sistemi di Network Management è l' **SNMP** ed è utilizzato di fatto per la gestione dell'intera infrastruttura di rete.

SNMP

"Simple Network Managment Protocol" (SNMP), permette il monitoraggio (statistiche sullo stato dei sistemi) ed il controllo (modifica delle impostazioni) di dispositivi di rete quali Server, Router, Switch, Hub ecc. Grazie a questo protocollo è possibile conoscere il throughput (carico, dati sulle interfacce di rete) e le intere prestazioni di un sistema di trasmissione dati.

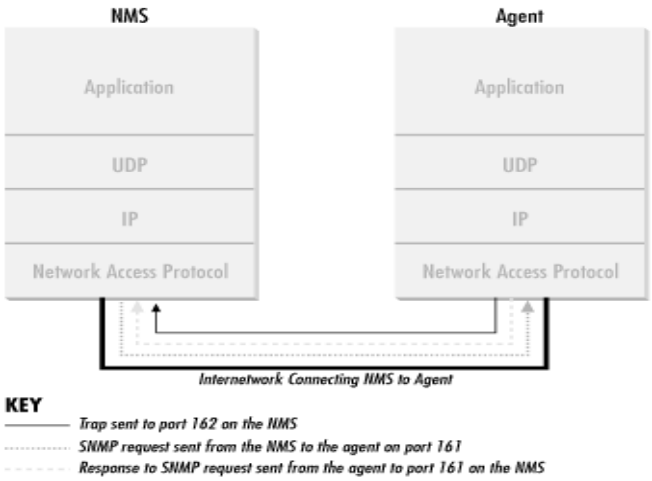
SNMP è passato attraverso alcune revisioni fino all'attuale versione 3:

- **SNMPv1**: descritto nelle **RFC 1155-1157** rappresenta la prima versione, utilizza l'invio dei nomi di community (utilizzati come password) in **chiaro**;
- **SNMPv2**: descritto nelle **RFC 1441-1452** è la seconda versione a cui sono state aggiunte nuove funzionalità tra cui la crittografia tramite **MD5**;
- **SNMPv3**: descritto nelle **RFC 2571-2575** è lo standard finale ed opera con protocolli sicuri cifrati ma è al momento raramente utilizzato.

Sostanzialmente un framework SNMP è composto da una o più Stazioni di Gestione (Management Station) e dagli agenti SNMP (SNMP Agent) installati sui devices di rete. Le Management Station interrogano gli agents i quali inviano le informazioni richieste. Solitamente gli agent SNMP di un apparato di rete sono implementati nel firmware dello stesso, mentre per quanto riguarda i server, vengono implementate tramite dei S/W aloro volti operanti sui server come servizi. Gli variabili gestite dagli agents, che rappresentano le caratteristiche e gli stati in cui si trovano gli oggetti monitorati , sono raccolti, in ogni singolo device, in un database chiamato MIB (Management Information Base) secondo la struttura definita nella SMI (Structure Management Information)che descrive l'oggetto stesso.

Gli apparati di rete possono anche settati in modalità tale da non dover essere interrogati, ma di essere allertati per inviare in autonomia determinati messaggi di allarme alle Management Station al raggiungimento di una soglia precedentemente impostata. E' infatti possibile configurare gli agents impostando le così dette trap. Grazie all'impostazione delle trap è

possibile ad esempio sapere quando un'interfaccia di rete smette di funzionare, in quanto al verificarsi del guasto precedentemente configurato, l'agent SNMP, che esegue il monitoraggio dell'apparato invia alla Management Station un allert che identifica il problema specifico. SNMP utilizza come protocollo di trasmissione lo stack TCP/IP e nel particolare il "UDP" in modo da ottenere migliori performance e minore overhead della rete. Ricordiamo che UDP al contrario del TCP non effettua controlli e non iserusce bit ridondati all'interno del Frame il chè aumenta l'efficienza e la velocità di trasmissione. In particolare viene utilizzata la porta UDP 161 per le interrogazioni e le risposte, e la porta UDP 162 come destinazione dei messaggi trap SNMP generati dagli agents.



SNMP COMMUNITY

L'insieme degli apparati di rete gestiti da SNMP appartengono ad una **comunità** "community". La comunità rappresenta un **identificativo** che permette di garantire la sicurezza delle interrogazioni SNMP. Un agent SNMP risponde **solo** alla richieste di informazioni effettuate da una Management Station appartenente alla **stessa** comunità. I nomi di comunità sono formati da 32 caratteri e sono di tipo case sensitive.

Esistono tre tipi di comunità:

- **monitor**: permette di lavorare in sola lettura, quindi di effettuare solamente interrogazioni agli agents (il cui nome di comunità deve corrisponde a quello della management station che ne ha fatto la richiesta);
- **control:** permette tramite gli agents SNMP di effettuare delle operazioni in lettura/scrittura sul dispositivo, quindi di variarne le impostazioni sempre previo controllo di sicurezza;
- **trap:** permette ad un agent di inviare un messaggio trap SNMP alla management station secondo la propria configurazione.

La sicurezza

Purtroppo è uso abbastanza comune dare poca importanza agli apparati di rete, una volta installati vengono lasciati in funzione con i parametri di default. Se si vuole perseguire la sicurezza non è sufficiente impostare la password di accesso al device, occorre anche modificare la community di appartenenza.

I nomi di community di default predefiniti sono public per le comunità di sola lettura e write o private per quelle in lettura/scrittura. Se questi vengono lasciati così anche dopo l'installazione è stupido poi lamentarsi perché qualche male intenzionato ha approfittato di questa leggerezza per carpire informazioni relative ai dati trasportati dai nostri apparati. E' bene modificare queste impostazioni di default con password e nomi scelti con cura.

Lo stesso firmware obsoleto, perché mai aggiornato può rappresentare una minaccia, occorre costantemente verificare la documentazioni inerente i nuovi rilasci di release per appurare se contengono unicamente aspetti innovativi o risolvono invece problemi che possono mettere a rischio la stabilità della nostra rete.

Quanto sopra non è comunque sufficiente a garantirci la sicurezza. Se riprendiamo la metodologia di attacco descritta nel primo capitolo "Man in the Middle", ci rendiamo conto che se applicata nei confronti degli apparati di rete ci consente di acquisire informazioni fondamentali. Come per le altre applicazioni aziendali, anche in questi casi i protocolli maggiormente utilizzati per accedere ai sistemi di rete sono da suddividere in sicuri e non sicuri.

Protocolli insicuri:

- http,
- Telnet,
- SNMP ver.1 e 2

Protocolli sicuri:

- HTTP abbinato ad SSL,
- SSH (non basato su SSL ma concettualmente similare),
- SNMP ver.3

Mettere in sicurezza gli apparati di rete

Sicurezza fisica:

E' consigliabile installare gli apparati in un locale controllato e possibilmente chiuso a chiave, al riparo da scariche elettrostatiche o altre interferenze radio o elettromagnetiche. Il locale dovrebbe essere attrezzato con sistemi antincendio, controllo della temperatura e umidità ed alimentazione ridondata con gli apparati, in caso di centro stella, connessi a due distinti UPS.

Sicurezza degli accessi:

Anche gli apparati di rete così come gli applicativi, i Data Base ed i dati in genere, sono oggetto di controllo da parte della normativa sulla sicurezza che chiede agli amministratori di rete delle aziende di effettuare un rigoroso controllo degli accessi effettuati ai sistemi. Occorre quindi definire e controllare chi può accedere agli apparati, a quale livello di funzionalità, e quale sia la funzione degli utenti che Vi accedono. E' necessario disabilitare le interfacce non usate e i protocolli e i servizi non necessari.

in particolare, occorre prevedere:

- **di restringere** le modalità d'accesso (su quali porte, da quali utenti o IP, con quali protocolli);
- **di registrare** (log) chi ha avuto accesso, quando l'ha avuto, e che cosa ha fatto;
- **di autenticare** chi accede (singoli, gruppi, servizi offerti);
- **di limitare** il numero di tentativi di login e imporre una pausa tra tentativi successivi;

- **di autorizzare** le azioni (singole funzioni o "views") che ogni utente può svolgere;
- **di visualizzare** una nota legale (scritta con un consulente) che appaia prima delle sessioni interattive;
- **di proteggere** i dati archiviati localmente, o in transito sulle linee dati, da copia e alterazione.

L'accesso agli apparati per scopi amministrativi può avvenire in locale, con cavo console (preferibile), e se da remoto attraverso l'impiego di protocolli tra i quali preferire quelli che cifrano il traffico a quelli in chiaro come indicato nei punti precedenti. Per esemplificare in caso di connessione remota è meglio usare **SSH** Secure SHell invece di un comando **Telnet** sulla **CLI** (comand line interface). E ancora: è preferibile il protocollo **HTTPS** invece di **http** sulla **GUI**(guide user interface). Ed infine in caso di Network management è preferibile **SNMP v3** invece di **SNMP v1-2**. Un'altra accortezza da applicare è quella di definire l'Host o la rete da cui si accetta l'accesso remoto, le interfacce su cui esso è accettato, e i protocolli ammissibili prima di attivare la connessione remota.

VLAN (Virtual LAN)

Prima di effettuare operazioni di monitoring è sempre bene realizzare una **Vlan di Layer 3** appositamente dedicata al management che consente una maggior sicurezza alle informazioni in arrivo dagli apparati di rete.
Le VLAN sono reti logiche e vengono implementate quando è necessario suddividere il traffico o le reti. Pe questo motivo, se ne dedichiamo una al management, realizzeremo di fatto una divisione tra i dati in transito sulla rete e gli allerts o i comandi in arrivo o verso gli apparati di rete(maggior sicurezza).

Benefici e Vantaggi

L'implementazione delle VLAN porta scalabilità, un miglioramento delle performance di rete e di conseguenza una migliore disponibilità del servizio (availability).

Dettagliamone i vantaggi :

- **Migliore utilizzo della banda:** le VLAN risolvono il problema della scalabilità in reti molto complesse e grandi suddividendo la rete in domini di broadcast minori;
- **Sicurezza:** le VLAN implementano un livello minimo di sicurezza permettendo la separazione di frame particolarmente sensibili inserendoli in VLAN differenti;
- **Isolamento degli errori in un dominio di broadcast:** forse la ragione più importante per implementare le VLAN, il loro impiego riduce notevolmente l'impatto dei malfunzionamenti sulla rete limitando le problematiche di un unico dominio di broadcast.

Conclusioni

La corretta configurazione degli apparati di rete e l'implementazione di una VLAN di management, rappresentano le due operazioni principali da effettuare per perseguire la sicurezza direttamente correlata agli apparati di rete. L'impiego delle VLAN dividendo i domini di broadcast e le tipologie di traffico oltre ad aumentare l'efficienza del monitoring è in grado di evitare pratiche di hacking purtroppo molto diffuse a livello 2 della rete.

Tutte le reti sono realizzate tramite l'impiego degli apparati sopra descritti per cui è inevitabile che, **se si vogliono proteggere i dati, bisogna prima di tutto proteggere gli apparati.**

Se i dati rappresentano il denaro e gli apparati la cassaforte è bene che la combinazione di quest'ultima non sia ne conosciuta ne di facile reperibilità, ma soprattutto…… è inutile nascondere la combinazione nella cassaforte se quest'ultima può essere…… **facilmente rubata !!!!!**

Il Tuo
EterNet Team