Lesson 4: Protezione reti wireless

La rete wireless

L'introduzione di tecnologie wireless all'interno delle reti LAN rappresenta ormai da qualche anno una consuetudine tale che risulta difficile trovare una rete dati priva di un'estensione senza fili. Questa tecnologia, nonostante i tanti detrattori, è in costante crescita. Le "reti senza fili" infatti rappresentano un sistema economico e flessibile adatto ad ogni realtà comprese le piccole e medie imprese. Per realizzare una rete wireless non sono necessari lavori di muratura o di posa dei cavi per il fissaggio delle infrastrutture. Gli apparati che le costituiscono sono di facile reperibilità e di basso costo se confrontati con gli apparati che compongono una rete Wired. Una rete wireless infine si adatta alla crescita e al dinamismo di qualsiasi azienda. In pratica la realizzazione di una tale struttura all'interno della propria azienda consente di mettere in campo le sole risorse per la realizzazione del servizio di trasmissione dati necessario in quel momento.

Come per gli apparati di rete LAN risultano di fondamentale importanza alcune operazioni di seguito riportate:

- Installazione,
- Configurazione,
- Aggiornamento del firmware o del sistema operativo,
- Amministrazione,
- Monitoraggio,
- Sicurezza.

Quali sono i sistemi che compongono una rete Wireless

La crescente proliferazione di dispositivi portatili con connettività wireless e i recenti sviluppi delle stesse tecnologie, hanno aperto un nuovo scenario agli utenti che oltre a fruire dei tradizionali servizi Internet, quali il web o e-mail, hanno la possibilità di beneficiare anche di servizi collaborativi avanzati. I nuovi servizi consentono agli utenti di comunicare all'interno delle proprie organizzazioni ovunque si trovino, in qualunque momento e condizione (fermi o in movimento).
Per realizzare una rete wireless così strutturata si utilizza una grande tipologia di apparati di cui i più conosciuti sono:

- router wireless,
- modem wireless,
- access point,
- network card,
- chiavette USB,
- adattatori wireless.

Gli standard

Le wireless LAN sono state standardizzate nel giugno 1997 dal Comitato IEEE. Lo standard include requisiti dettagliati per la trasmissione fisica dei pacchetti di dati attraverso le onde radio. Nel 1999, IEEE pubblica le due versioni dello standard **802.11**: **802.11a e 802.11b**. Nel 2003 viene ratificato lo standard **802.11g** e nel 2009 viene rilasciata la versione dello standard **802.11n.**

NB: Per la propagazione via radio dei segnali, **sono state liberalizzate** le frequenze intorno ai 2.4 Ghz e non occorre quindi richiedere licenze specifiche per l'installazione di punti di accesso Wi-Fi (anche quelli domestici).

La famiglia 802.11 consta di tre protocolli dedicati alla trasmissione delle informazioni (a, b, g), la sicurezza è stata inclusa in uno standard a parte, **802.11i**. Gli altri standard della famiglia (c, d, e, f, h, …) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo protocollo largamente diffuso è stato il b; in seguito si sono diffusi il protocollo a e soprattutto il protocollo g.

I protocolli **802.11b e 802.11g** utilizzano lo spettro di frequenze (banda ISM) intorno ai 2,4 GHz. Si tratta di una banda di frequenze regolarmente assegnata dal piano di ripartizione nazionale (e internazionale) ad altro servizio, e lasciato di libero impiego solo per le applicazioni che prevedono potenze EIRP (Massima Potenza Equivalente Irradiata da antenna Isotropica) di non più di 20 dBm da utilizzare all'interno di una proprietà privata (è vietato l'attraversamento del suolo pubblico). Trovandosi però ad operare in bande di frequenze ove già lavorano altri apparecchi, i dispositivi b e g possono essere influenzati negativamente durante la loro trasmissione. Possono infatti risentire, anche in modo pesante, della vicinanza con telefoni cordless, ripetitori audio/video per distribuire programmi televisivi satellitari o altri apparecchi all'interno di un appartamento o ufficio che utilizzano quella banda di frequenze.

Il protocollo **802.11a** utilizza la banda ISM dei 5,4 GHz. Tuttavia non risponde alla normativa europea ETSI EN 301 893[1] che prevede DFS (Dynamic Frequency Selection), TPC (Transmit Power Control) e radar meteorologici; tale normativa di armonizzazione europea è valida in Italia su indicazione del Ministero delle Comunicazioni con il decreto ministeriale del 10 gennaio 2005.
Per ovviare al problema in Europa è stato introdotto nel 2004 il protocollo **802.11h**, che risponde ai requisiti richiesti. Un apparato WIFI per trasmettere su suolo pubblico in Italia a 5.4 GHz deve obbligatoriamente utilizzare questo standard.

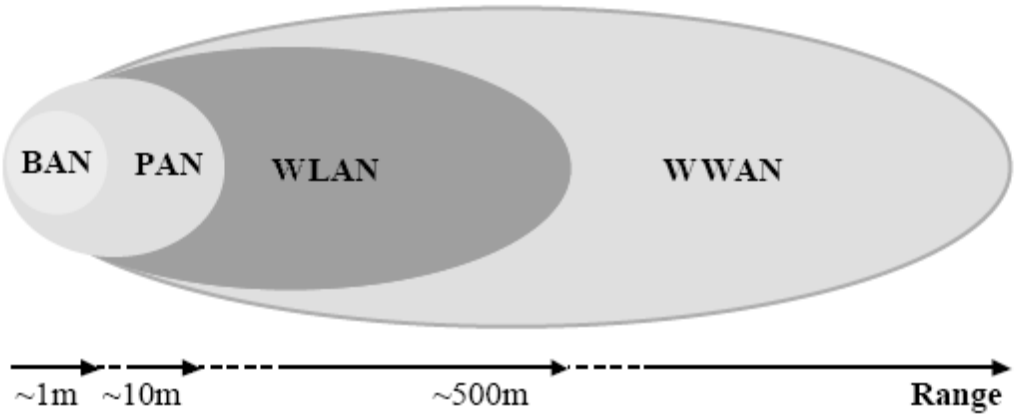
Implementazione dei protocolli WIFI

Il susseguirsi delle continue evoluzioni dei protocolli WIFI, frutto delle continue richieste del mercato, ha creato un po' di confusione, per cui, con la tabella riportata nella pagina seguente proviamo a fare chiarezza riassumendo brevemente le caratteristiche principali che identificano i vari standard.

Standard	Frequenza	Velocità di trasferimento (Mbit/s)
802.11 legacy	FHSS, 2,4 GHz, IR	1, 2
802.11a	5,2, 5,4, 5,8 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	2,4 GHz	1, 2, 5.5, 11
802.11g	2,4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
802.11n	2,4 GHz, 5,4 GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 125

Topologia di rete wireless

Possiamo indicativamente classificare le reti wireless in base all'area coperta dal segnale trasmesso dai dispositivi, in diverse categorie: **BAN, PAN, WLAN e WWAN**.



Body Area Network

Le BAN sono reti il cui raggio di trasmissione copre all'incirca le dimensioni di un corpo umano, tipicamente 1-2 metri, e consentono di connettere dispositivi indossabili quali auricolari, palmari, lettori MP3, telefoni cellulari etc.
Tra le caratteristiche principali delle reti WIFI BAN troviamo la capacità di connettere dispositivi eterogenei accompagnata a quella di auto-configurarsi, rendendo di fatto trasparenti

all'utente operazioni come la rimozione o l'aggiunta di un nuovo dispositivo.
La connessione wireless è considerata la soluzione naturale per una BAN in quanto l'utilizzo di fili risulterebbe estremamente scomodo.

Personal Area Network

Il raggio di comunicazione delle PAN è tipicamente superiore ai 10 metri. Le PAN consentono a dispositivi vicini di condividere dinamicamente le informazioni. E' possibile perciò connettere dispositivi portatili con altri oppure con stazioni fisse, ad esempio per accedere ad Internet. Tecnologie ad infrarossi e radio rendono nelle PAN notevolmente più pratiche le operazioni quotidiane di sincronizzazione fra portatile, desktop e palmare, ma anche il download delle immagini dalla macchina fotografica digitale, l'upload di musiche nel riproduttore di MP3, ecc.
Tra gli standard più usati per realizzare le BAN e le PAN ricordiamo il protocollo IrDA e il protocollo Bluetooth.

Wireless Local Area Network

Le WLAN hanno un raggio di comunicazione di 100, 500 metri tipico dell'area mediamente occupata da un singolo palazzo. Nelle WLAN troviamo gli stessi requisiti delle tradizionali wired LAN, come la connessione fra le stazioni che ne fanno parte e la capacità di inviare messaggi broadcast. Le WLAN si trovano però a dover affrontare alcuni problemi specifici di questo ambiente, come la sicurezza dovuta al mezzo trasmissivo (trasmissioni via etere), il consumo energetico, la mobilità dei nodi e la limitata larghezza di banda.
Esistono due differenti approcci all'implementazione di una wireless LAN, uno basato sull'infrastruttura e uno su reti strutturate ad hoc.

L'architettura basata su un'infrastruttura prevede l'esistenza di un controller centralizzato chiamato "Access Point" solitamente connesso con la rete fissa, che realizza l'accesso tra i sistemi aziendali e i dispositivi mobili.

Una rete ad hoc è invece una rete "peer-to-peer" formata da nodi mobili posti all'interno dei reciproci raggi di trasmissione. Detti nodi si configurano sino a formare una rete temporanea gestita da un controller dinamicamente eletto tra tutti i nodi partecipanti alla comunicazione.

Wireless Wide Area Network

Le **WWAN** (Wireless Wide Area Network) sono le reti wireless che dispongono del range più ampio oggi disponibile, e vengono, nella maggior parte dei casi, installate nell'infrastruttura della fonia cellulare. Le **WWAN** offrono anche la possibilità di trasmettere dati.
Le **WWAN** sono estese su vaste aree geografiche e hanno un raggio di trasmissione dell'ordine dei km, tipicamente compreso tra 1,5 e 8 Km. Sono state concepite per rispondere all'esigenza di collegare utenti che si trovano a grandi distanze tra loro. Sfruttando questa loro caratteristica, tale tipologia di rete viene usata anche per collegare diverse LAN situate in località distanti tra loro.
Le soluzioni **WWAN**, che si basano su un'infrastruttura a rete cellulare, o su trasmissione satellitare, rappresentano il futuro della comunicazione dei dati.
Le "Wireless Wide Area Network" forniscono accesso alle informazioni anytime & anywhere in presenza di copertura di rete cellulare.

Le reti wireless di tipo **WLan,** molto diffuse ormai nelle aziende, rappresenteranno l'oggetto della presente lezione.

Quando si utilizza una rete wireless è di fondamentale importanza sapere che:

- gli apparati wireless vengono venduti con tutte le misure di sicurezza disattivate, per cui chiunque si può collegare e fare danni: **è necessario l'intervento dell'utente per attivare le protezioni**;
- la sicurezza delle reti wireless è molto più debole di quanto nella realtà viene dichiarato dai produttori;
- le prestazioni reali sono di gran lunga inferiori a quelle pubblicizzate.

Partendo da queste considerazioni e dalla conoscenza dei limiti imposti dalla tecnologia, è possibile realizzare reti dati correttamente funzionanti. Vediamo allora come mettere a Vostra disposizione la nostra esperienza maturata in anni di analisi e di realizzazioni di reti Wireless.

Implementazione rete wireless

In funzione dell'estensione dell'area da coprire possono essere utilizzate due diverse architetture wireless:

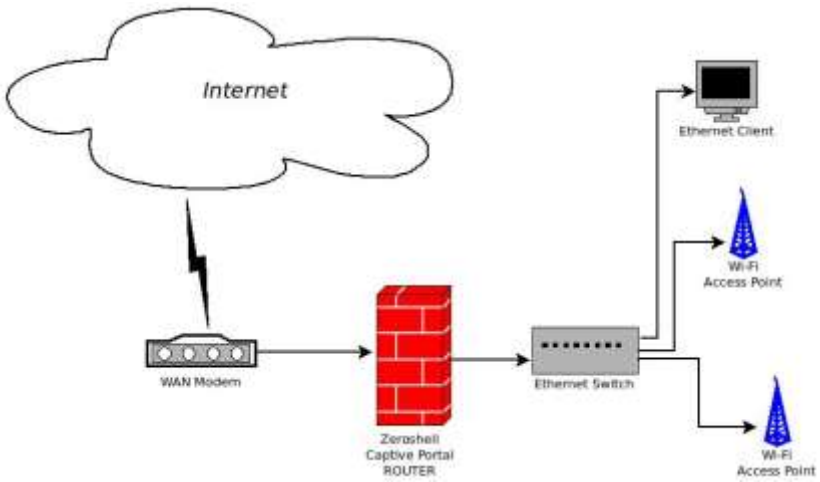
- stand-alone;
- con controller.

Quando scegliere una modalità invece di un'altra? Se la necessità è quella di offrire un accesso in un'area aziendale ben definita o comunque connettere un numero limitato di access point, la soluzione **stand-alone** è quella più indicata. Nel caso invece di implementazioni più complesse, con un numero elevato di aree aziendali da coprire e di access point, l'adozione di una rete **con controller** è mandatory.

Vediamo le principali differenze tra i due sistemi:

Autenticazione

Entrambi i sistemi supportano autenticazione mediante **MAC** o server radius **802.1x**, in alcuni casi le controller hanno già implementati sistemi di autenticazione o di "captive portal" oggi sostituiti dalla modalità "Hot Spot Router" per utenti guest.



Encryption

Gli **access point stand-alone** criptano la comunicazione che intercorre tra loro e i device, archiviano le chiavi di criptografia in un proprio data base interno evitando la loro trasmissione in rete e quindi la loro lettura da parte di terze parti non autorizzate. Le reti **con controller** consentono invece la criptazione dell'intera architettura che intercorre tra access point, device e controller, partendo da un unico punto centralizzato con minore possibilità di errore.

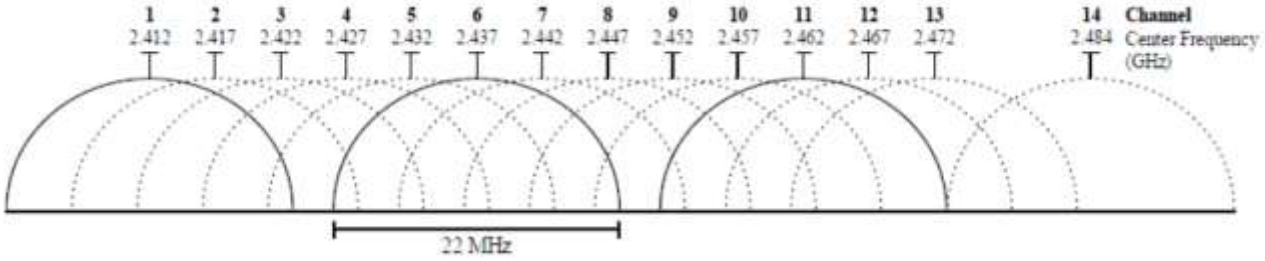
SSID/VLAN

Nel caso degli **access point stand-alone** la configurazione dei SSID e di eventuali VLAN avviene su ciascun dispositivo e in dipendenza della configurazione ereditata dalla rete locale cablata. Nella rete **con controller** invece si può avere funzionalità di Layer 3 e implementare quindi servizi indipendenti dalla rete a cui la rete wireless è connessa.

Radio Management/ Channel Management

La modalità **con controller** consente la gestione dei canali radio in modo da evitare le interferenze dovute a trasmissioni adiacenti alla rete su frequenze identiche (sovrapposizione di canali).

Il funzionamento di un sistema wireless infatti permette di utilizzare 13 canali (regolamentazione per lo stato italiano), di cui però solo 3 alla volta per non interferire tra di loro. Infatti, come si può notare dallo schema successivo, molti canali vanno in sovrapposizione di altri generando disturbi che abbassano le performance dell'infrastruttura e, in alcuni casi, bloccandone il corretto funzionamento.



Ogni canale ha un ampiezza di 22MHz, per cui vista l'ampiezza totale di banda dedicata ai sistemi WIFI, ogni canale va a sovrapporsi a quelli contigui. Ne risulta che, i canali realmente utilizzabili sono sempre a gruppi di 3 (1,6,11 o 2,7,12 o 3,8,13). Siccome ci sono dispositivi che non supportano i canali 12 e 13, per ovviare a qualsiasi problema, è stato deciso che i canali veramente utilizzabili sono solamente 3 (1,6,11).

Alla luce di quanto detto sopra, per evitare segnali interferenti, generati dagli access point impiegati per la copertura, sarà necessario riconfigurare su tutti i moduli radio il canale da utilizzare e fissarlo, in modo da evitare ogni interferenza con i segnali generati dagli access point adiacenti. Nello schema a lato è rappresentata la miglior configurazione delle frequenze dei canali su cui è bene fissare gli access point.

La configurazione suggerita consente infatti di non avere
canali interferenti sovrapposti, garantendo il miglior SNR **Signal-to-noise ratio** e aumentando nel contempo le performance della rete WIFI.

Group configuration

Una rete wireless con controller, mediante gestione centralizzata, consente di realizzare configurazioni di gruppo agevolando di fatto le operazioni di manutenzione quali la distribuzione delle configurazioni o gli aggiornamenti del firmware.

Bandwidth/ Load balancing

Una rete wireless con controller consente di limitare la larghezza di banda massima che gli utenti possono utilizzare oltre a bilanciare il traffico in zone ad alta densità di connessione facendo transitare i dati tra più access point.

Redundancy

Il sistema basato su controller rappresenta un single "point of failure" che in caso di fault bloccherebbe tutti gli access point ad esso connesso. Per questo motivo è consigliato adottare una doppia controller in modo da garantire la continuità del servizio.

Network Access Control

Sempre tramite le controller è consentita l'implementazione di policy d'utente o di gruppo per l'accesso alla rete o alle singole applicazioni.

Security

Alcuni access point integrano sistemi di IDS (intrusion detection system) che sono limitati alla propria funzionalità in rete, mentre una controller implementa criteri di sicurezza su tutta l'architettura wireless. Può essere dedicato un canale radio per il rilevamento delle intrusioni wireless e monitorata la rete wireless per il controllo di minacce, attacchi di spoofing, attacchi Denial of Service, di reti ad-hoc, ecc.

Quality of Service

Sia i sistemi stand-alone che quelli basati su controller sono in grado di assegnare delle priorità al traffico, in base alle applicazioni e ai protocolli, ma solo la controller è in grado di garantire il roaming tra i vari access point per poter offrire servizi multimediali efficienti quali voce, video etc.

Mesh Networking

Entrambe le tecnologie consentono la creazione di topologie magliate, sia tramite l'utilizzo del cavo che dell'etere. In questo ultimo caso però si riduce la disponibilità della banda che risente in modo diretto del numero di hop che il pacchetto dati deve passare. La controller, al contrario della stand-alone, è in grado di modificare in automatico la magliatura, in base a precise esigenze definite da parametri quali la priorità, il protocollo, il tipo di traffico, la congestione di rete, ecc.

Live monitoring of Wireless network and location based services

La controller consente un monitoraggio in tempo reale della rete wireless e di eventuali servizi basati sulla localizzazione. E' possibile integrare le planimetrie dei locali con l'architettura

wireless implementata per individuare i singoli device e l'area entro la quale stanno operando con lo scarto di qualche metro.

SNMP Comunity

Come evidenziato nella precedente lezione, anche per i device wireless è fondamentale la configurazione corretta dell'SNMP. L'insieme degli apparati di rete gestiti da SNMP appartiene a una **comunità** (*community*). La comunità rappresenta un **identificativo** che permette di garantire la sicurezza delle interrogazioni SNMP. Un agent SNMP risponde **solo** alle 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 agent (il nome di comunità deve corrisponde a quello della management station che ne ha fatto la richiesta);
- **control**: permette tramite gli agent SNMP di effettuare delle operazioni in lettura/scrittura sul dispositivo, quindi di variarne le impostazioni sempre previo controllo di sicurezza;
- **trap**: permette a un agent di inviare un messaggio trap SNMP alla management station secondo la propria configurazione.

La sicurezza

Come premesso all'inizio, una volta installati i device wireless, spesso vengono lasciati in funzione con i parametri di default. Pessima abitudine.

Non è sufficiente impostare una password di accesso al device, occorre anche modificare la community di appartenenza. Ottimo suggerimento.

Spesso i nomi di community di default predefiniti sono "public" per le comunità di sola lettura e "write" o "private" per quelle in lettura/scrittura. Ovviamente è bene modificare queste impostazioni di default per motivi di sicurezza. Assolutamente da fare.

E' necessario schermare le onde radio che attraversano aree di non pertinenza propria mediante l'utilizzo di apposite antenne direzionali o con accorgimenti quali carta stagnola o simili.

Il firmware obsoleto può rappresentare una minaccia, occorre costantemente verificare le documentazioni inerenti i nuovi rilasci di release, controllare se contengono unicamente aspetti innovativi o risolvono problemi che possono mettere a rischio la stabilità della nostra rete. Spesso per i più esperti.

NB: 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 agli apparati di rete wireless, consente di acquisire fondamentali informazioni, esattamente come per gli apparati di rete wired.

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,
- WEP.

Protocolli sicuri:

- HTTP abbinato ad SSL,
- SSH (non basato su SSL ma concettualmente similare),
- SNMP ver.3,
- WPA e WPA2.

Mettere in sicurezza gli apparati di rete

Sicurezza degli accessi:

Anche gli apparati di rete wireless sono soggetti al controllo accesso da parte degli amministratori di sistema che la normativa richiede alle aziende. A questo proposito occorre definire e controllare:

- chi può accedere agli apparati;
- a quale livello e funzioni;
- disabilitare le interfacce non usate;
- disabilitare i protocolli;
- disabilitare i servizi non necessari.

In particolare, occorre prevedere:

- di restringere le modalità di accesso (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 l'utente che accede (singoli, gruppi, servizi offerti);
- di limitare il numero di tentativi di login imponendo una pausa tra i tentativi successivi;
- di autorizzare le azioni (singole funzioni o "views") che ogni utente può svolgere;
- di proteggere i dati archiviati localmente o in transito sulle linee dati da copia e alterazione.

L'accesso amministrativo può avvenire in locale, tramite cavo console (preferibile) o da remoto con vari protocolli tra i quali è bene preferire quelli che cifrano il traffico a quelli in chiaro, come indicato nei punti precedenti.

Ad es. è meglio usare:

- SSH Secure SHell invece di Telnet sulla CLI;
- HTTPS invece di http sulla GUI;
- SNMP v3 invece di SNMP v1-2.

Inoltre è consigliabile anche:

- definire l'Host o la rete da cui si accetta l'accesso remoto;
- definire le interfacce su cui esso è accettato;
- definire i protocolli ammissibili.

Occorre poi impostare protocolli di criptazione dei dati sicuri, appositamente studiati per reti wireless. Poiché i segnali radio vengono inviati via etere, è possibile che vengano rilevati anche da dispositivi o utenti non autorizzati ad accedere alla rete WIFI, compromettendo quindi la sicurezza della rete e delle informazioni veicolate al suo interno. Per tale motivo, all'interno degli standard di trasmissione wireless, sono stati implementati protocolli e misure rivolte all'aumento della sicurezza delle reti.

Chiave di Autenticazione Pubblica (WEP)

Questo tipo di autenticazione (Wired Equivalent Privacy) presente nello standard IEEE 802.11, è stato progettato per fornire una sicurezza comparabile a quella delle reti LAN via cavo, e richiede che l'access point invii ad ogni stazione una chiave pubblica (a 64 o 128 bit) che viene trasmessa su un canale indipendente.

Chiave di crittografia WPA

Il **WPA** (WIFI Protected Access) è progettato, a differenza del **WEP**, per utilizzare l'autenticazione delle postazioni e la distribuzione di differenti chiavi per ogni utente. Tale operazione è effettuabile attraverso una Pre-Shared Key (PSK), che presenta una sola password d'accesso per qualsiasi utente ne richieda l'accesso. Una delle modifiche che introducono maggiore robustezza rispetto alla chiave WEP è l'utilizzo del metodo di criptaggio dei dati basato sul **TKIP** (Temporal Key Integrity Protocol) che, cambiando periodicamente la chiave (ora fino a 256 bit) in uso tra gli apparati Wi-Fi in modo dinamico e criptato, consente di ottenere una maggiore efficacia contro i tentativi di accesso non autorizzato alla rete wireless.

Controllo Access-List ristretta

Sull'access point è possibile abilitare soltanto alcune determinate postazioni utente mediante uno specifico elenco dei **Mac-Address** relativi alle schede di rete wireless. In tal modo, soltanto le schede WIFI, con i Mac-Address specificati nella lista, saranno abilitati ad accedere alla rete wireless.

Nome della rete WIFI (SSID) nascosto

Sull'apparato che trasmette il segnale wireless (access point), è possibile configurare il nome della rete wireless in modalità nascosta. Tale modalità, consente di evitare che i dispositivi rilevino in modo automatico la rete wireless. Gli utenti autorizzati potranno connettersi alla rete solo specificando, con la configurazione in modo manuale, il nome dell'access point (SSID).

VLAN (Virtual LAN)

La creazione di una Vlan di Layer 3 di management consente di mettere in sicurezza gli apparati di rete wireless. Le VLAN sono reti logiche e vengono implementate quando è necessario suddividere il traffico o le reti (vedi lezione precedente sugli apparati di rete).

Applicazione utile

Oltre alle debolezze riscontrate nelle configurazioni dei sistemi di rete wireless, abbiamo sovente riscontrato un problema legato alla gestione dei nostri device nei confronti delle connessioni di rete disponibili. Durante gli audit in aziende, dove è stata implementata una rete wireless per consentire mobilità in ufficio, abbiamo riscontrato lentezze di trasmissione molto significative nonostante gli utenti fossero connessi alla rete cablata. Facendo dei test di velocità di trasmissione, non si riusciva ad andare oltre il 20% delle potenzialità della rete dati e questo perché l'utente, che si era sconnesso dalla LAN per recarsi in sala riunioni, agganciava la rete wireless per questioni di mobilità. Una volta però tornato alla propria postazione e riconnesso alla LAN, restava di fatto ancora connesso alla rete wireless senza accorgersene.

Tutto ciò accade perché il client non è in grado di discriminare o di assegnare delle priorità alle network cards. Essendo molti gli utenti mobili, o meglio diventandolo con questa modalità operativa, si viene ad accumulare un numero decisamente elevato di utenti connessi in WIFI con conseguente degrado delle performance di rete.

Chi ha scaricato questa lezione può anche scaricare un tool trial che una volta installato sul proprio client consente di disabilitare in modalità automatica la rete wireless una volta connessi alla rete LAN.

Conclusioni

Il wireless, oltre che di fondamentale importanza per i servizi aziendali, sta diventando una delle più grandi rivoluzioni del mondo dell'elettronica. Oltre agli impieghi visti durante la lezione, la rete wireless può collegare un computer ad internet e ad apparecchi come:

- stampanti;
- telefoni;
- tablet;
- videocamere e telecamere;
- console videogiochi;
- Hard Disk portatili;
- DVD player;
- impianti hi-fi;

- TV di nuova generazione;
- sistemi per l'automobile;
- domotica.

Questo vuol dire che è possibile ascoltare in ogni stanza della casa i file MP3 contenuti nel computer fisso e, per chi parcheggia nei pressi della propria casa, scaricare direttamente nello stereo i file audio che intende ascoltare durante il viaggio.

I segnali video, come quelli provenienti da un ricevitore satellitare, possono essere visti su qualsiasi tv di casa, così come le stazioni radio, che trasmettono su Internet, possono essere ascoltate su qualsiasi impianto hi-fi. Allo stesso modo, la centralina del riscaldamento e tutti gli elettrodomestici di casa possono essere telecontrollati da una apparecchiatura adatta allo scopo.

Insomma, l'unico limite all'applicazione della tecnologia WIFI sembra davvero essere la fantasia, motivo in più per applicare idonee politiche di sicurezza per evitare spiacevoli inconvenienti e una volta tanto…….…… **fate attenzione**:

non sempre una rete wireless aperta è solo un'opportunità per navigare gratis, potrebbe rivelarsi invece un mezzo per acquisire le vostre informazioni.

Il Tuo EterNet Team