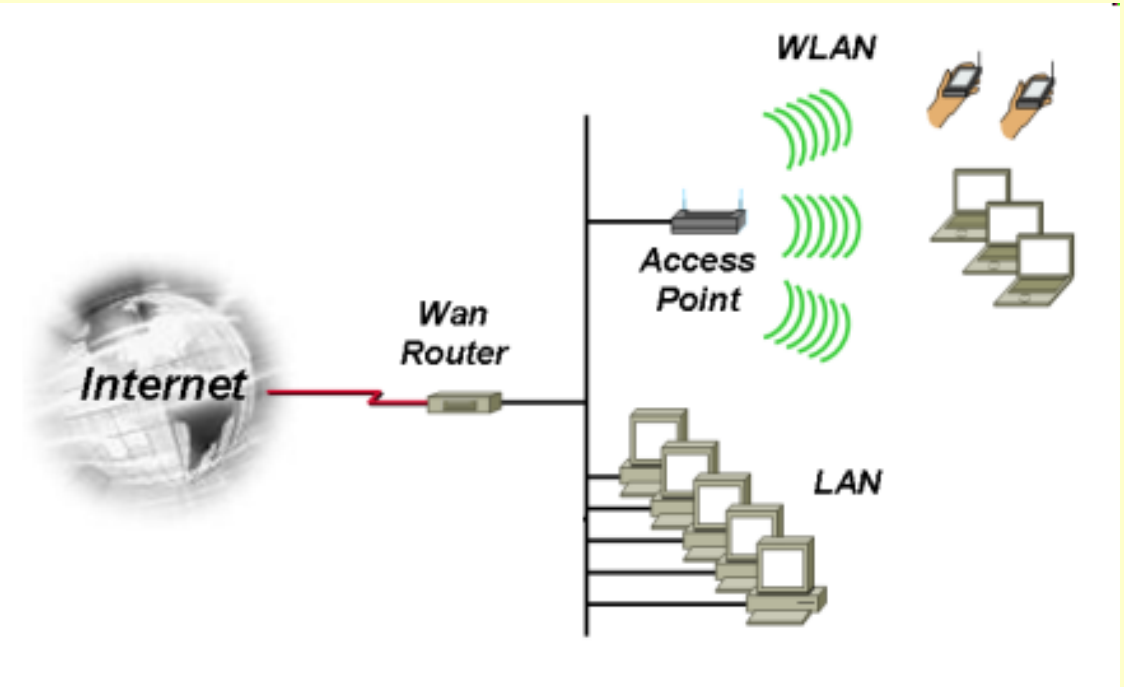
Sicurezza e Internet 05

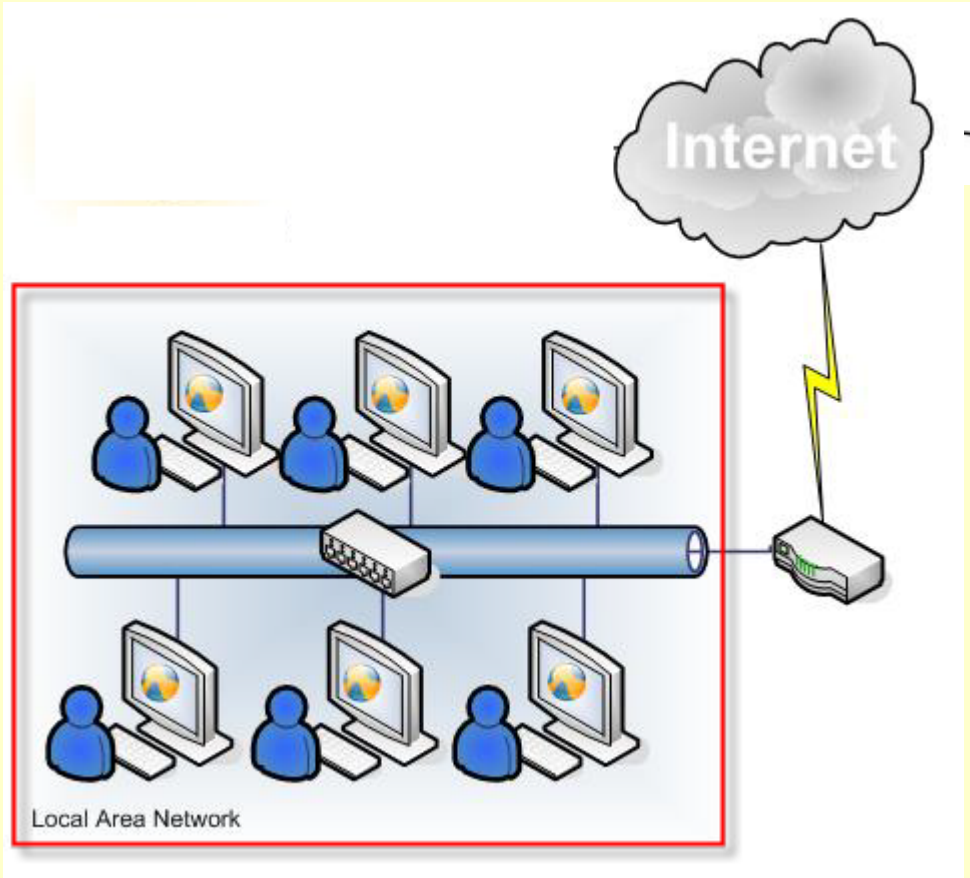

The 12 Layer Matrix
Building a Cyber Fortress
OCTAVE
Chief Security Officer
Policy Management Software
Proper Systems Administration
Firewall
Authentication
Incident Response Plan
Virus Scanners
Intrusion Detection Systems (IDS)
Cyber Intelligence
Encyrption
Active Content Filtering

Proteggere i propri PC

Si prende come esempio un sito dotato di alcuni PC collegati in LAN tramite cavo ethernet oppure wireless

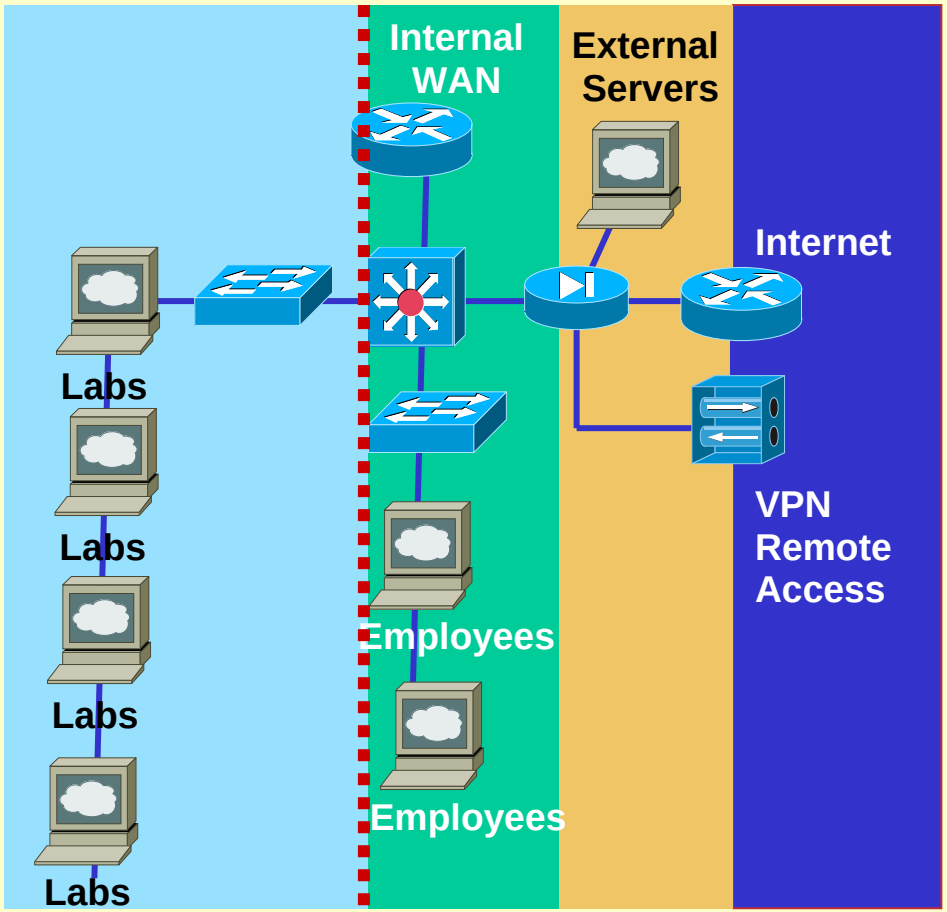


Intrusioni esterne



- Se le Intrusioni vengono dall'esterno del perimetro, si deve costruire un muro
  - Firewall
  - Antivirus, antispy
  - Antispam
  - Anti intrusione (IDS, IPS)

Intrusioni interne



Se le Intrusioni vengono dall'interno del perimetro, si deve costruire un muro tra i reparti

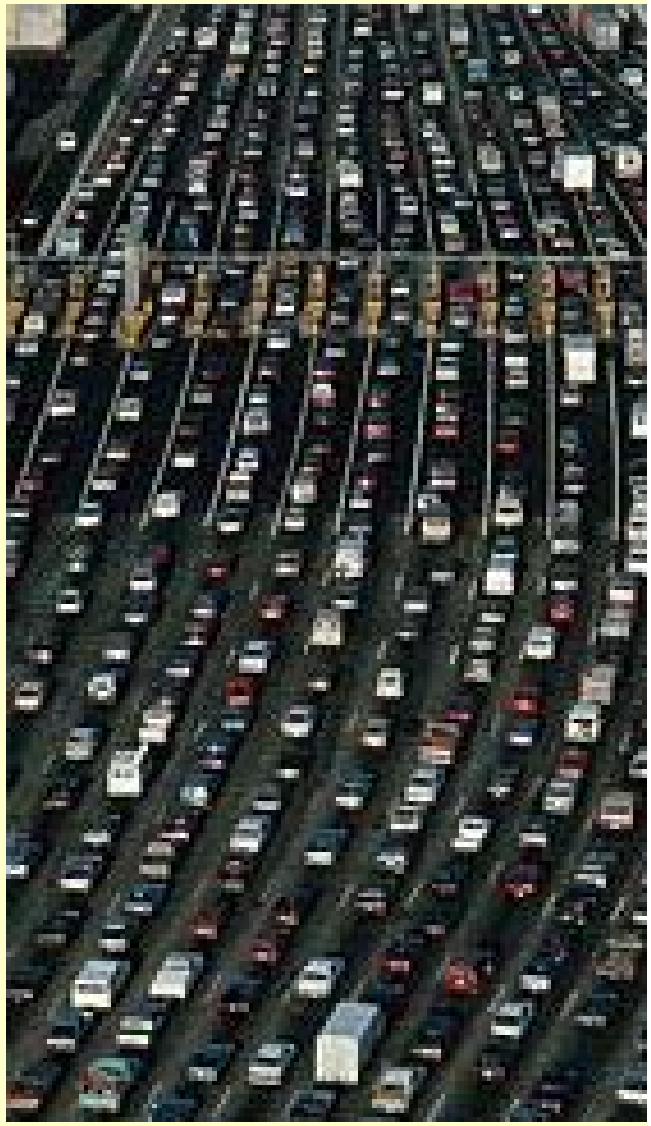
- Firewall
- Anti intrusione (IDS, IPS)

Filtering Network Traffic

Examining the flow of data (traffic) across a network

Types of flows:

- Packets
- Connections
- State



La sicurezza del singolo PC

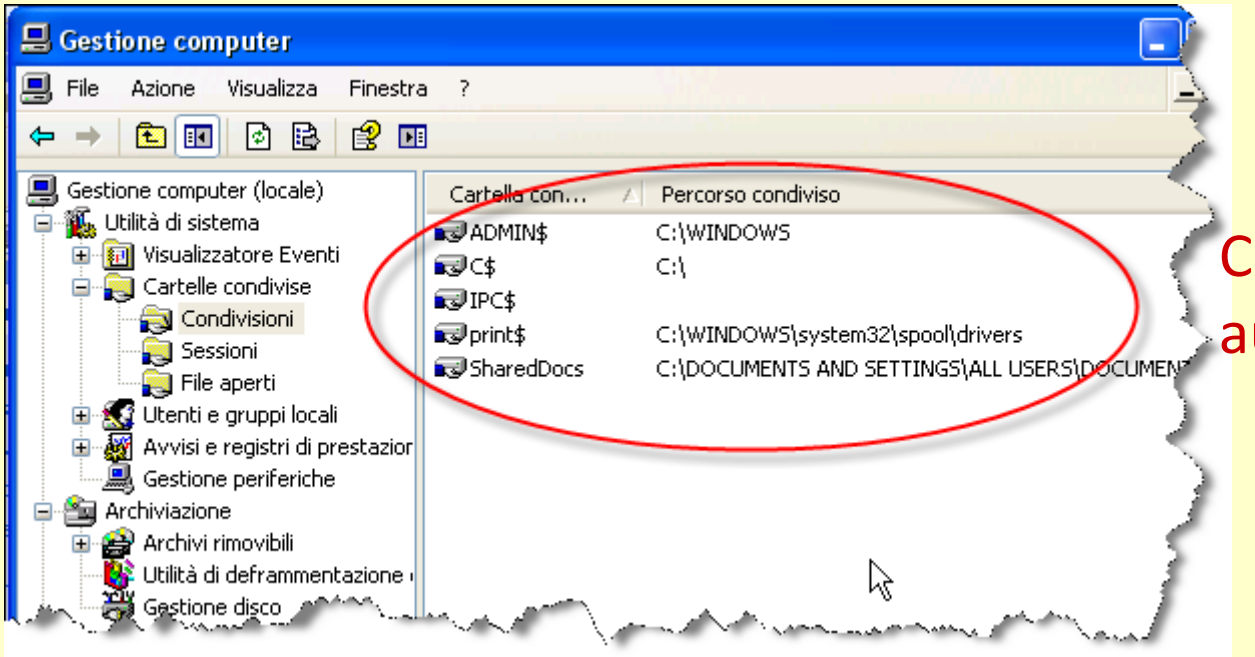
Riservatezza: occorre impedire che possano essere intercettati i dati trasmessi sul canale trasmissivo

Controllo degli accessi: occorre evitare l'accesso alla rete da parte di utenti non autorizzati

Integrità dei dati: occorre assicurarsi che i dati trasmessi non possano essere modificati

La sicurezza del singolo PC

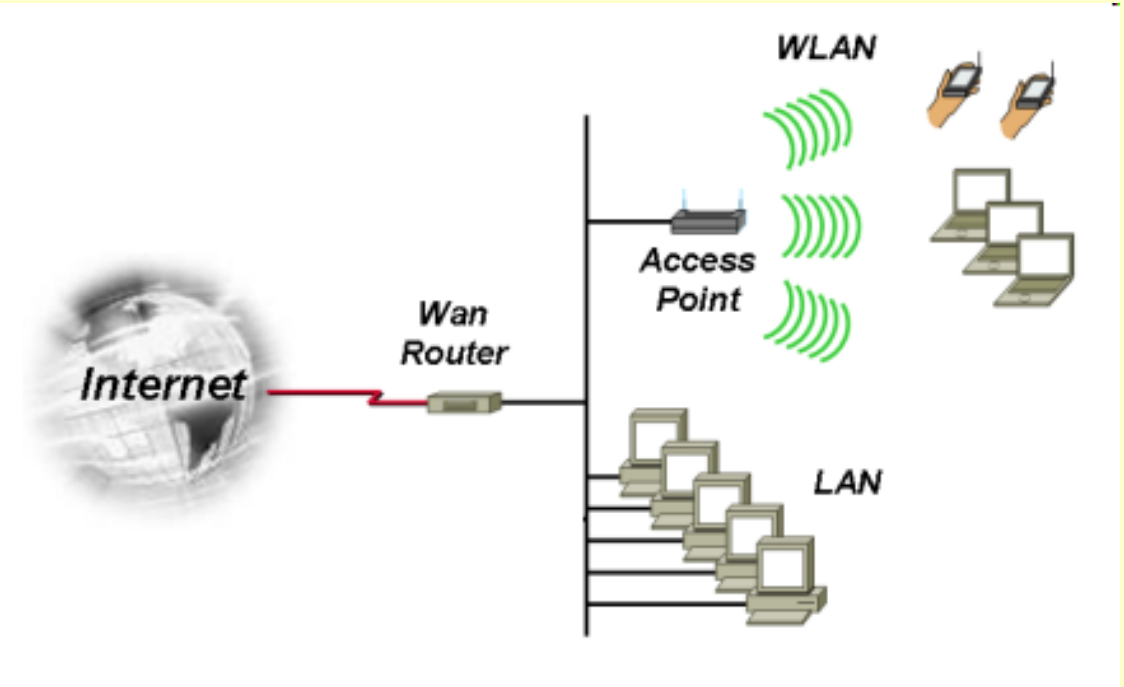
Disabilitare il routing



Controllare gli SHARE automatici

Proteggere i propri PC

- Se però c’è un access point wireless il muro di cinta non funziona più !!!!!

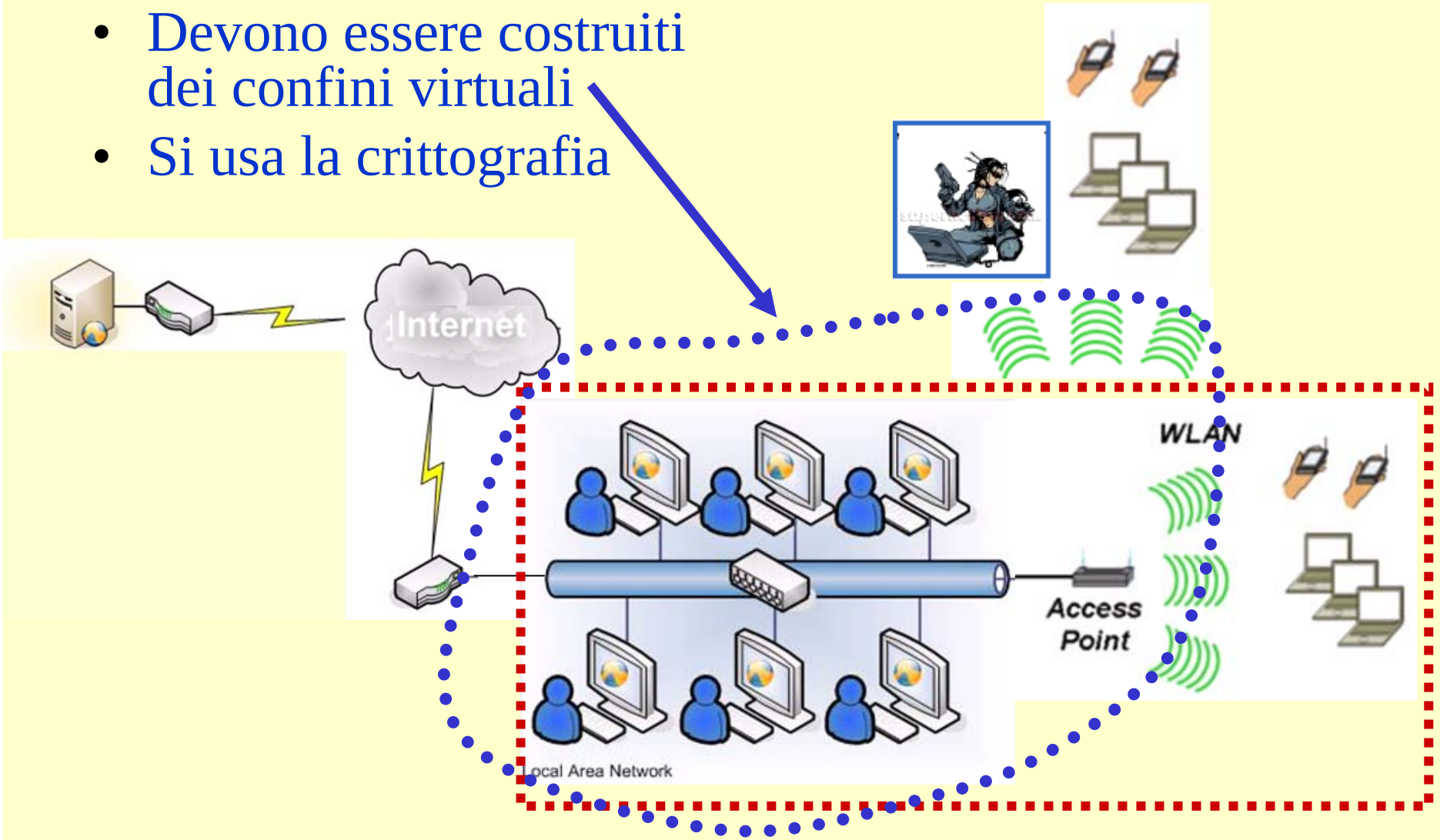


Inserimento in rete

- Via etere non ci sono confini

Inserimento in rete

- Devono essere costruiti dei confini virtuali
- Si usa la crittografia



Due tipi di tecnica

non esclusivi

Crittografia WIFI

- Tutto il traffico di rete wireless è crittografato
- Si usano chiavi simmetriche
- Le chiavi vengono cambiate spesso

VPN

- Si usa crittografare “peer to peer”
- Si costituisce un “tunnel” chiamato Virtual Private Network

Elementi di una rete wireless

Gli elementi che costituiscono una rete wireless sono essenzialmente tre:

Access point (AP)

Gli *access point* sono gli apparati che realizzano il punto di accesso alla rete wireless e collegano la rete wireless con la rete cablata.

Wireless Terminal (WT)

I *Wireless Terminal* sono i dispostivi che usufruiscono direttamente dei servizi di rete, tramite opportune schede di rete RF (integrate nei notebook o disponibili su bus PCI, PCMCIA oppure dotate di interfaccia USB).

Sistema di autenticazione

Il sistema di autenticazione integra un RADIUS (Remote Authentication Dial-In User Service) Server in grado di dialogare con gli access point per consentire o negare l'accesso alla rete ai wireless terminal che ne fanno richiesta.

Elementi di una rete wireless

Gli elementi che costituiscono una rete wireless sono essenzialmente tre:

Access point (AP)

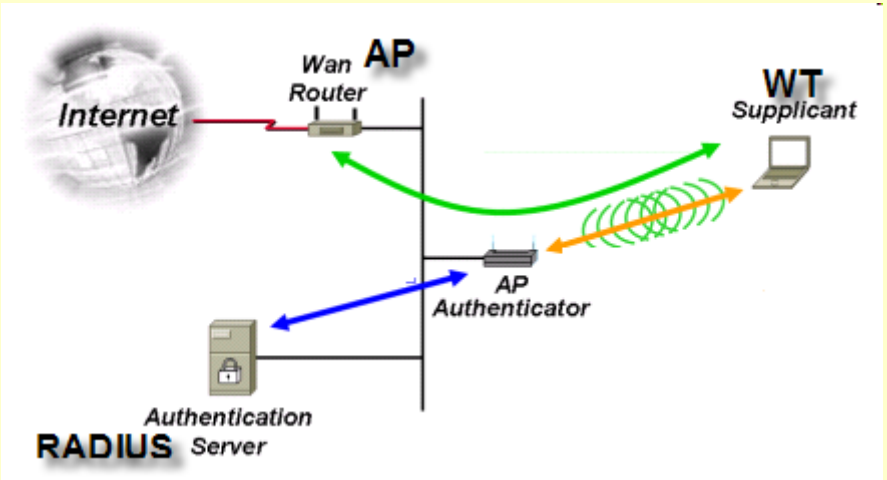
Gli *access point* sono gli apparati che realizzano il punto di accesso alla rete wireless e collegano la rete wireless con la rete cablata.

Wireless Terminal (WT)

I *Wireless Terminal* sono i dispostivi che usufruiscono direttamente dei servizi di rete, tramite opportune schede di rete RF (integrate nei notebook o disponibili su bus PCI, PCMCIA oppure dotate di interfaccia USB).

Sistema di autenticazione

Il sistema di autenticazione integra un RADIUS (Remote Authentication Dial-In User Service) Server in grado di dialogare con gli access point per consentire o negare l'accesso alla rete ai wireless terminal che ne fanno richiesta.



Gli standard Wifi

Crittografia con Chiave WEP

- Il meccanismo per la protezione dei dati originariamente previsto dallo standard IEEE 802.11 è il **WEP** (*"Wired Equivalent Privacy"*).
- Il WEP prevede che ogni pacchetto scambiato tra l'*access point* e l'apparato dell'utente sia codificato con l'agoritmo di cifratura **RC4**, utilizzando una *chiave segreta* di 40 o 104 bit, preceduta da un'ulteriore sequenza casuale di 24 bit (*Initialization Vector*) diversa per ogni pacchetto trasmesso.
- La chiave segreta deve essere comunicata a tutti gli utenti che accedono al corrispondente *access point*.
  - Nel **2001** alcuni ricercatori hanno però dimostrato la debolezza dell'algoritmo RC4, nonché altre debolezze intrinseche del meccanismo WEP.
  - È stato quindi istituito un gruppo di lavoro, chiamato *"Task Group i"*, per correggere i noti problemi del WEP e definire un nuovo standard di sicurezza, l'**IEEE 802.11i**.

Gli standard Wifi

Dal WEP all'802.11i: WPA

- IEEE e Wi-Fi Alliance hanno quindi dato vita ad un progetto per sostituire il WEP come meccanismo di sicurezza nei prodotti commerciali esistenti.
- Il nuovo meccanismo, denominato WPA (*Wireless Protected Access*), è stato concepito sin dall'inizio come soluzione temporanea, in attesa che lo sviluppo di 802.11i giungesse a maturazione.

- Per WPA è stato progettato un nuovo protocollo, denominato TKIP (*Temporal Key Integrity Protocol*), sempre basato sull'algoritmo RC4, che aggiunge un meccanismo di cifratura *software* preliminare a quello utilizzato dal WEP (eseguito invece in hardware) per ogni pacchetto inviato.

- WPA si basa su TKIP per la codifica dei messaggi, mentre si è aggiunto un meccanismo di autenticazione *per utente*, in luogo dello scambio della chiave WEP segreta, basato sul protocollo 802.1x (illustrato piu' avanti).

Gli standard Wifi

WPA2 (802.11i)

- **L'802.11i, rilasciato nel luglio 2004, è ora comunemente indicato con il nome di WPA2.**

- **Anche WPA2 utilizza 802.1x per la gestione delle politiche di autenticazione.**
- **Per la cifratura dei dati invece, è definito un nuovo protocollo, CCMP (*Counter Mode with CBC-MAC Protocol*), che utilizza l'algoritmo crittografico AES al posto dell'RC4.**
- **La maggiore robustezza di AES (e di CCMP) si paga con una maggior potenza di calcolo richiesta agli apparati rispetto a WEP e TKIP, e richiede quindi una modifica dell'hardware.**
- **Riepilogando:**

  WPA = TKIP + 802.1x

  WPA2 = CCMP + 802.1x

L’autenticazione

802.1x

- **Per evitare gli accessi non autorizzati in rete si è deciso di adottare il protocollo di autenticazione port-based denominato IEEE 802.1x, il quale prevede che l'autenticazione avvenga sia in fase di primo accesso alla rete sia ad intervalli periodici di tempo.**
- **Per l'autenticazione l'access point si deve appoggiare ad un server esterno tramite il protocollo RADIUS (*Remote Authentication Dial-In User Service*).**
- **L'architettura 802.1x applicata alla tecnologia wireless prevede quindi la presenza delle seguenti entità:**

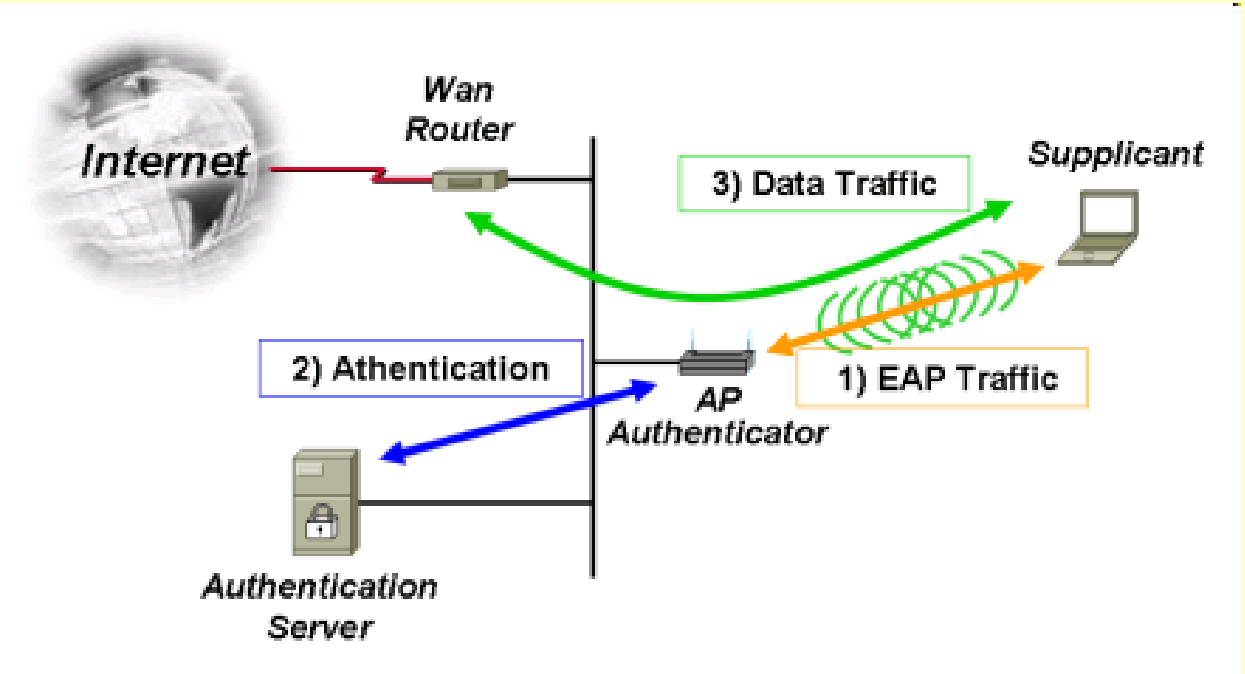
  Supplicant = client che intende accedere alla rete

  Authenticator = punto di accesso alla rete (access-point)

  Authentication Server = server esterno a cui l'autenticatore invia le richieste di autenticazione provenienti da un supplicant

Architettura di autenticazione prevista dal protocollo 802.1x:

Schema applicativo 802.1x



- The authenticator role is either performed by
  - the access point itself via a pre-shared key (referred to as WPA2-PSK) or
  - for larger enterprises, by a third-party entity, such as a RADIUS server.

EAP

Alcuni termini che porteste trovare

- *Il sistema di autenticazione utilizza il protocollo di trasporto **EAP** (Extensible Authentication Protocol), il quale non specifica un meccanismo di autenticazione fisso, bensì definisce una piattaforma di autenticazione estensibile, consentendo quindi di poter variare il meccanismo di autenticazione nel caso in cui in quest'ultimo venisse scoperta una qualche vulnerabilità.*

Metodi di autenticazione

Tra i vari metodi di autenticazione impiegati in EAP (oltre 40) è possibile segnalare:

***EAP-MD5**: (MD5-Challenge), equivalente al PPP, richiede username/password. Non prevede mutua autenticazione o scambio di chiavi quindi è poco adatto in ambiente wireless.*

***LEAP**: (Lightweight EAP) sviluppato da Cisco, prevede l'invio di username/password ad un server di autenticazione (RADIUS). Considerato poco sicuro è in fase di abbandono.*

***EAP-TLS**: crea un sessione TLS (tunnel) tra il Supplicant e l'Authentication Server. Sia il server che il supplicant richiedono l'utilizzo di un certificato (x509). Questo metodo fornisce una mutua autenticazione.*

***EAP-TTLS**: crea una sessione TLS cifrata, all'interno della quale è possibile utilizzare qualsiasi metodo di autenticazione.*

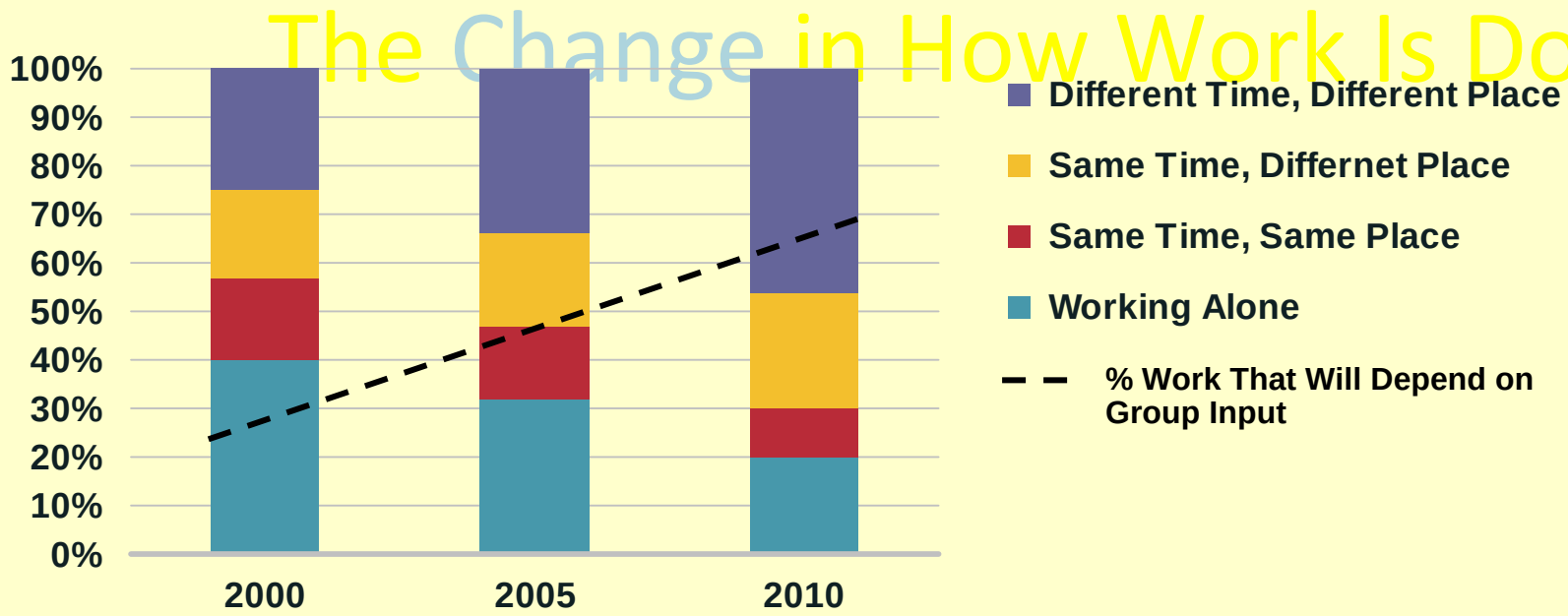
***PEAP**: (Protected EAP) crea una sessione TLS cifrata. Sia in PEAP che in TTLS il certificato del supplicant è opzionale, mentre è obbligatorio quello dell'Authentication Server.*

***EAP-MSCHAPv2**: richiede username/password, ed è fondamentalmente un'incapsulamento dell'MS-CHAP-v2 in EAP.*

Wireless LAN: La normativa italiana

* Dal 2001 al luglio 2005
  * Il decreto Pisanu (27 luglio 2005)
  * Il decreto Landolfi (4 ottobre 2005)
  * Il decreto legge n. 248 (27 dicembre 2007)
  * La direttiva europea 2006/24/CE (15 marzo 2006)
  * Il decreto legislativo n. 109 (30 maggio 2008)
  * Il decreto legge n. 207 (30 dicembre 2008)
  * I limiti di potenza attuali

The Changing Business Environment



- An increasing percentage of an employee's work output will be the result of collaboration with others
- Working with others, but not face-to-face
- Maintaining productivity requires supporting this trend

Source: Gartner Group

Nuovi stili di vita, nuovi mezzi di informazione

Il lavoro a casa, la casa - ufficio
L'education e l'entertainment (edutainment)
I cataloghi elettronici ipertestuali
Gli acquisti elettronici
L'accesso alle banche dati informative
I giornali elettronici
Le teleprenotazioni
La scelta dei programmi TV (Pay per view e Vod)
L'emergenza ed il teleallarme
La gestione centralizzata della casa, la casa cablata
Le e-mail ad amici, a radio e TV, ai giornali
La Voice over IP
Gli elettrodomestici intelligenti

Secure Connectivity

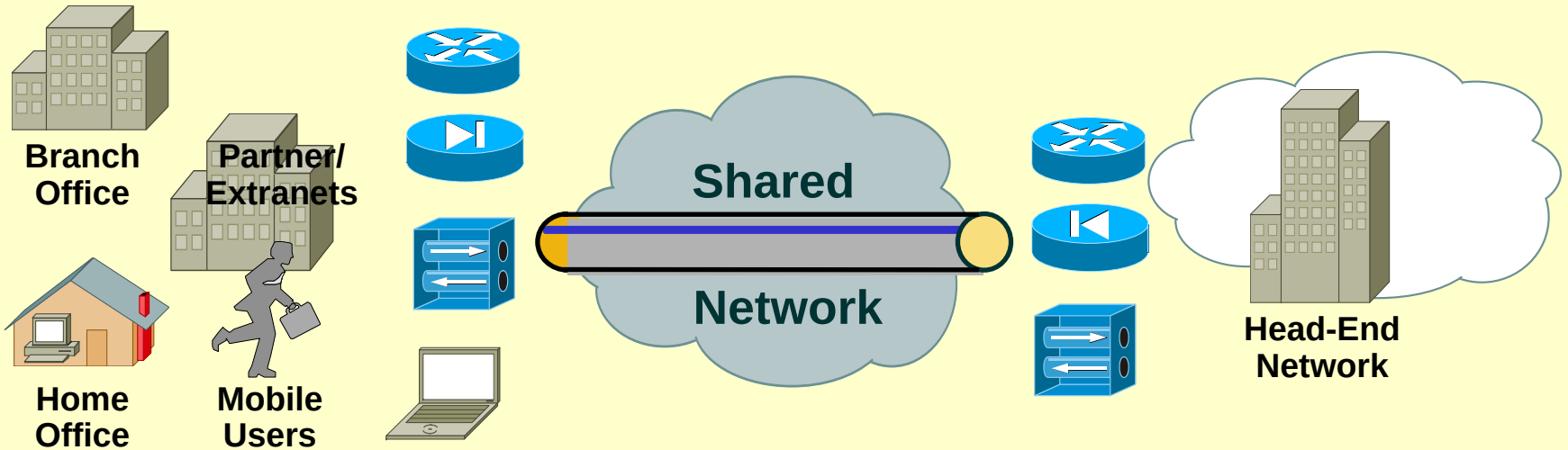
Protocols to Encrypt Network Traffic

Two Main Protocol Suites

- IPSec (IP security)
  - Built directly on the IP layer (protocol 50)
  - Uses IKE (Internet Key Exchange) to exchange keys, and ESP (Encapsulated Security Protocol) to encrypt traffic
  - Requires both end points to run special software that understands IPSec (most routers and security appliances currently support high-speed IPSec)
- SSL (Secure Socket Layer)
  - Built on top of the TCP layer (port 443)
  - Used extensively to provide confidentiality for Web traffic (often called HTTPS)
  - All major browsers can be used to communicate over SSL

Virtual Private Network (VPN)

- Virtual Private Network (VPN): A network built on a less expensive shared infrastructure with the same policies and performance as a private network
- Connects two peers via a tunnel that ignores network complexity between them



Altro?