Mobilita' in ESA
ESACOM WLAN

esa

Andrea Baldi ESA/ESRIN

V Incontro GARR

Roma 25.11.2003

esa

Informatics Department
Directorate of Administration

Contenuti

- ESA ed i suoi requisiti di mobilita’
- Prima e dopo l’avvento delle reti wireless
- La ESACOM Wireless LAN
- Il progetto ESACOM WLAN
- Le scommesse tecniche
- Il Disegno della ESACOM WLAN
- Conclusioni

ESA
EUROPEAN SPACE AGENCY

- ESA e' un' organizzazione internazionale con lo scopo di promuovere l' utilizzo di scienza, ricerca & sviluppo e applicazioni nel campo spaziale
- ESA ha sedi in tutto il mondo con grande concentrazione in Europa
  - Oltre 30 siti interconnessi in Wide Area Network
  - Oltre 4000 utenti della rete
  - Manager, ricercatori, tecnici, amministrativi e visitatori

esa

Informatics Department
Directorate of Administration

	D	B	F	I	NL	GB	DK	SP	S	CH	IRL	A	N	FIN	P	
2000	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	ESA
1995	●	●	●	●	●	●	●	●	●	●	●	●	●	●		
1987	●	●	●	●	●	●	●	●	●	●	●	●	●			
1975	●	●	●	●	●	●	●	●	●	●	●					
1973	●	●	●	●	●	●	●	●	●	●						
1962	●	●	●	●	●	●	●	●	●	●						ESRO
1962	●	●	●	●	●	●										ELDO

- Establishments
- Offices
- ESA ground stations
- Ground stations used by ESA
- Ariane downrange stations

Kiruna
ESTEC (Noordwijk)
Brussels
ESA Paris
Toulouse
Redu
EAC Cologne
ESOC (Darmstadt)
Villafranca
ESRIN (Frascati)
Fucino
CDN
Washington
Houston
Maspalomas
Moscow
Libreville
Kourou
Natal
Malindi
Perth
Ascension

Requisiti di Mobilita' in ESA

- Mobilita' Interna al campus
  - Movimento di personale dagli uffici in sale riunioni ed aree dedicate a progetti per lavoro collaborativo
  - Visitatori che regolarmente fanno business con ESA
- Altissima mobilita' fra i siti principali
  - 25.000 missioni l'anno con 50 persone in missione con frequenza settimanale
  - Per riunioni, seminari, attivita' di progetto, eventi
- ESA staff in visita ad altre organizzazioni
  - Agenzie spaziali o partner nazionali ed Internazionali come Nasa, ASI, DLR, CNES
- ESA organizza workshop e confererenze con massiccia partecipazione di esterni

Prima della Wireless LAN

- Prima della Wireless LAN
  - Ci si doveva spostare con raccoglitori pieni di carta, dischetti e cdrom
  - Si doveva pianificare con grande anticipo spostamenti, installazioni e dimostrazioni da fare
  - Si doveva conoscere il luogo esatto delle riunioni e quali attrezzature erano disponibili sul sito
  - Molto spesso le informazioni necessarie per svolgere il proprio lavoro non erano a disposizione in tempo o mancava sempre qualche cosa
- La Wireless LAN fornisce una risposta precisa ai requisiti precedentemente esposti ed una soluzione pratica ai problemi elencati

Con la Wireless LAN

- Gli utenti oggi si spostano con il loro laptop ed hanno accesso a tutti i servizi esistenti sulla rete esattamente come nel proprio ufficio (posta, database, agenda, applicazioni, Internet).
- Tutto cio' si traduce in
  - Efficienza ed incremento della produttivita'
  - Sfruttamento di tempi morti nelle riunioni
  - FIessibilita'
  - Accesso ai servizi ed alle informazioni indipendentemente dal luogo
  - ..... ma anche nuovi problemi da affrontare

La ESACOM WLAN

- La ESACOM WLAN e' la rete Wireless installata nei 4 siti principali dell' ESA per rispondere ai requisiti di mobilita' del proprio personale e dei suoi visitatori.
- Copre al momento 60 sale pubbliche destinate a riunioni e conferenze e sale dedicate a progetti
- Altre 20 sale sono gia' fase di allestimento
  - molte delle quali dedicate a progetti per lavoro collaborativo
- Nuovi siti pianificati nel 2004
- Conta ad oggi 500 utenti
- 1000 utenti, previsti per il 2004

Il Progetto e Le Sue Fasi

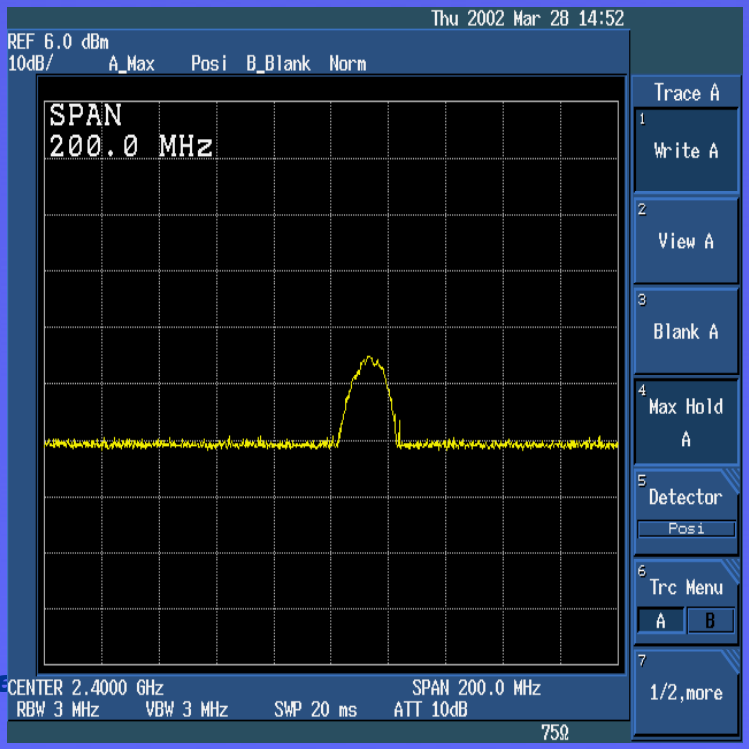
- Un progetto IT tradizionale:
  - Definizione
  - Approvazione
  - Analisi
  - Implementazione Pilota
  - Disegno
  - Implementazione
  - Test e Accettazione
  - Roll out
  - Operazioni
  - Evoluzione

Attivita' Importanti

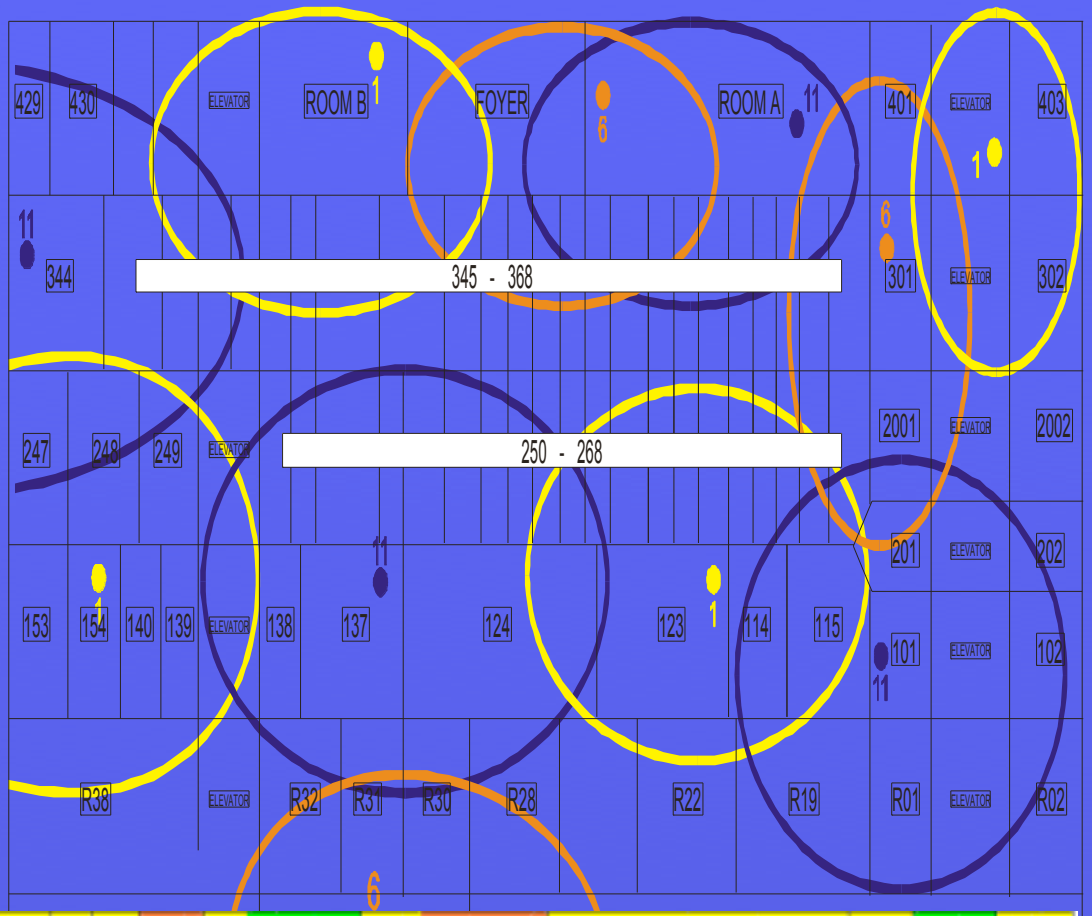
- Studio della tecnologia Wireless
- Definizione dei requisiti con il supporto di un working group sulla mobilita'
- Realizzazione di un pilota
- Analisi dei costi e del ritorno dell' investimento (ROI)
- Identificazione delle risorse umane e pianificazione
- Definizione del concetto operativo e delle policy di accesso
- Survey dei siti e installazione
- Analisi dei rischi legati agli aspetti di sicurezza

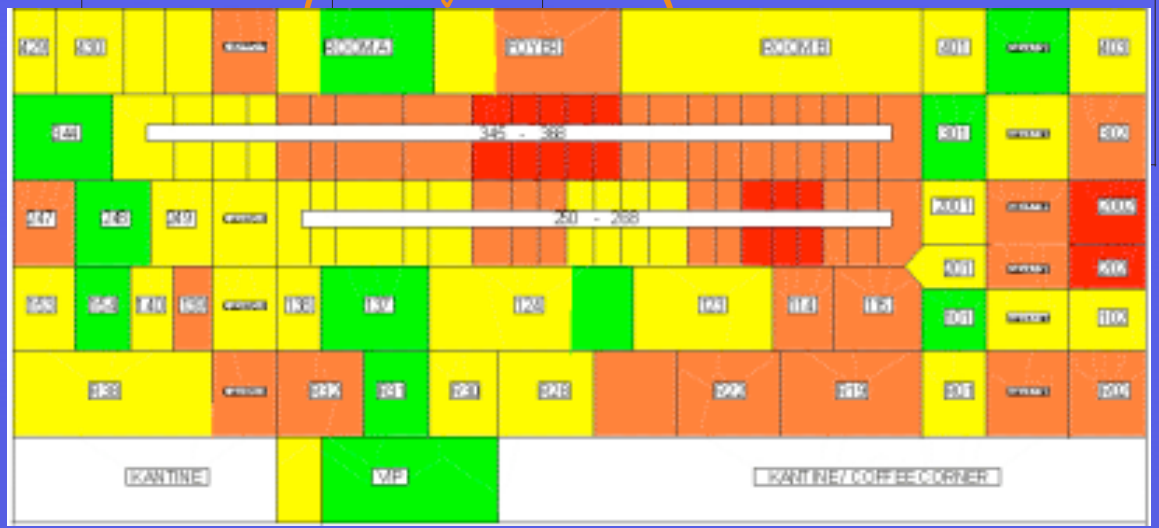
Survey Dei Siti

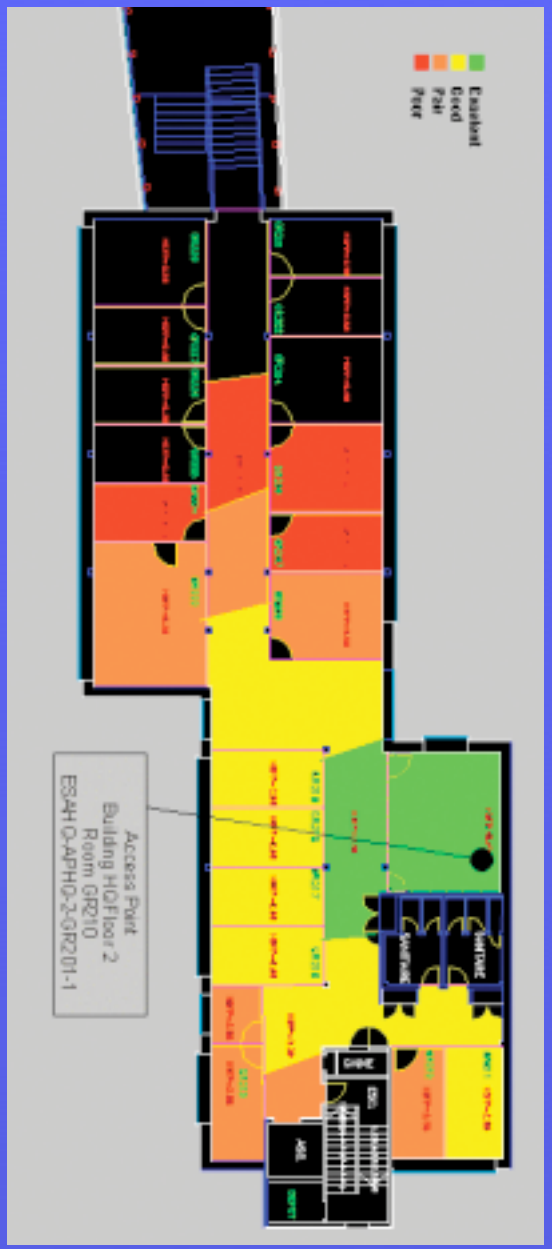
- Essenziale per produrre le specifiche dettagliate
  - Definizione e disegno dei canali
  - Selezione dell'antenna appropriata
  - Determinazione dei parametri radio
  - Analisi delle interferenze RF
  - Roaming
  - Requisiti di cablaggio
  - Requisiti alimentazione
    - Power over the Ethernet
  - Fotografia dell'ambiente



esa


ROOM B
FOYER
ROOM A
ELEVATOR
345 - 368
250 - 268
429
430
401
403
344
301
302
247
248
249
2001
2002
201
202
153
154
140
139
138
137
124
123
114
115
101
102
R38
R32
R31
R30
R28
R22
R19
R01
R02


345 - 368
250 - 268
KANTINE
KANTINE/COFFEE CORNER


Access Point
Building HQ/Floor 2
Room GR210
ES4H 0-APH0-2-GR201-1

Sicurezza

- Il WEP (Wired Equivalent Protocol), parte dello standard 802.11, e' insicuro
  - Progettato per indirizzare sia l'autenticazione che la criptografia risulta carente su entrambi i fronti
  - Confidenzialita'
    - riutilizzo dello stream cifrato
    - vettore di Inizializzazione non cifrato
    - la stessa chiave usata per tutte le stazioni
  - Integrita'
    - il CRC usato come controllore dell'integrita' non e' crittograficamente sicuro
  - Autenticazione
    - basata su indirizzo Mac e non su credenziali
    - si autentica solo il cliente (rouge access point)

Sicurezza

- Lo standard 802.11b fallisce nel definire come devono essere distribuite le chiavi
  - La distribuzione statica delle chiavi non scala oltre poche unita'
    - va bene per casa
    - ma impossibile da gestire gia' in una piccola azienda
  - Se chi possiede la chiave lascia l'organizzazione o un PC viene perduto/rubato e' necessario cambiare le chiavi per tutti.
- WEP e' stato violato
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Sicurezza

- Nelle reti Wireless esiste il requisito per un piu' elevato livello di sicurezza
  - Mutua Autenticazione
    - Utente --> Rete,
    - Rete --> Utente
  - Gestione dinamica delle chiavi
    - diverse per ogni utente,
    - per ogni sessione
    - ed uso limitato net tempo
  - Controllo degli accessi alla rete
  - Monitoraggio
  - Accounting (per WISP)

Alternative al WEP

- SSH o IPSEC
  - Solo per la criptografia
    - Sicuro ma difficile da implementare
    - Piu' alto costo, prestazioni meno scalabili, roaming problematico
- 802.1x (LAN port authentication) e EAP (Extensible Authentication Protocol)
  - Mutua autenticazione
    - dell'utente da parte della rete
    - della rete da parte dell'utente
  - trasportabile su ogni link protocol
  - Supporta diversi tipi di autenticazione
    - EAP-TLS, TTLS, PEAP, LEAP

802.1x

EAPOW

EAP
Over
Radius

Authentication
Server
Radius

Authenticator

EAPOL

Supplicant

Window Domain
Controller

esa

Informatics Department
Directorate of Administration

Autenticazione

- PEAP: Protected Extensible Authentication Protocol
  - PEAP usa un tunnel sicuro per il metodo EAP
  - Mutua autenticazione ma non supporta metodi tradizionali come PAP e CHAP
- EAP-TLS
  - Mutua autenticazione ma richiede certificati sia sul server che sui clienti.
  - Complessa da gestire senza un' infrastruttura PKI
  - I clienti si autenticano sulla rete con un metodo EAP o con un metodo tradizionale come PAP,CHAP, MS CHAP, o MS CHAP V2.

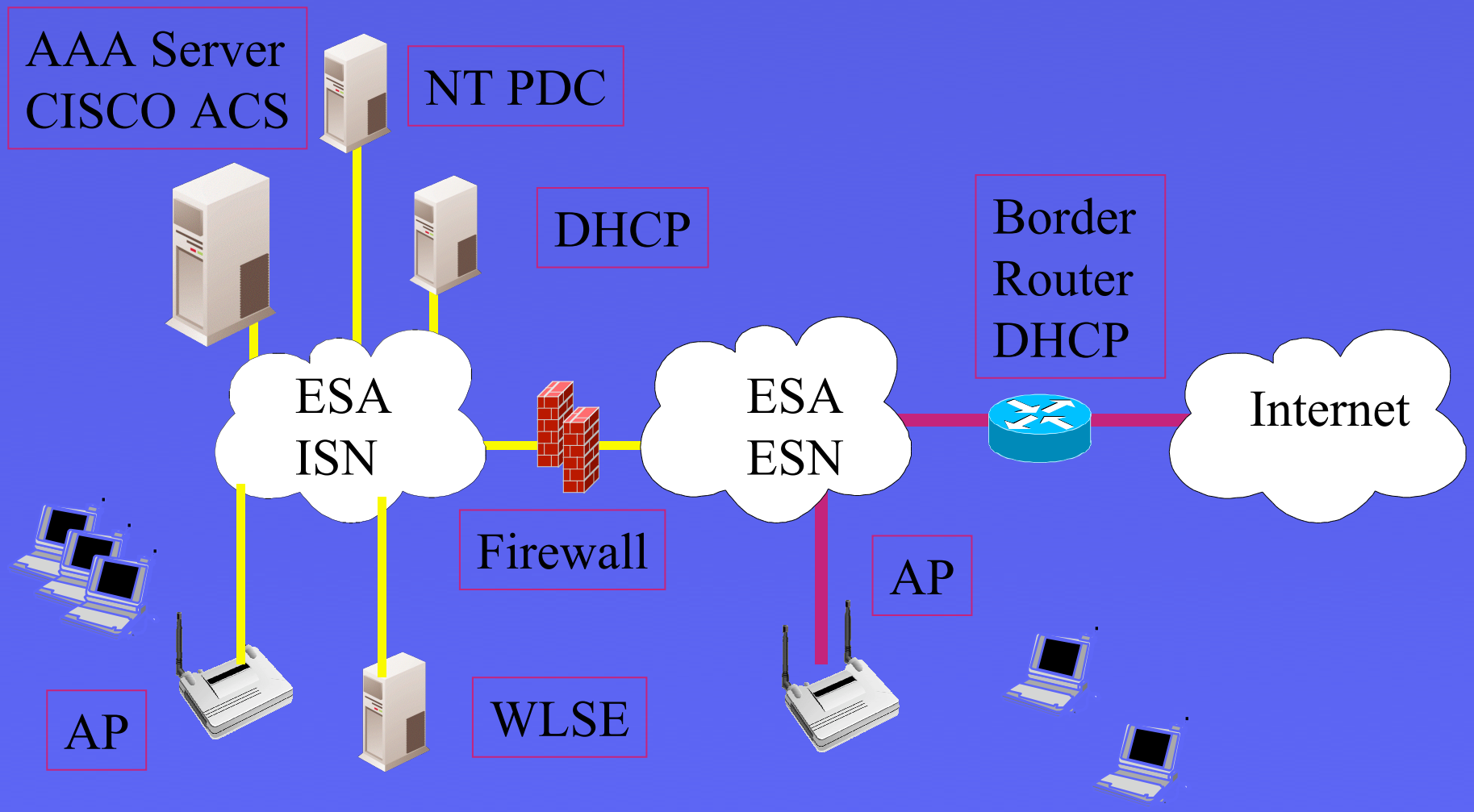
Autenticazione

- TTLS (Tunneled Transport Layer Security)
  - simile a TLS ma senza la distribuzione di certificati sui clienti. Il certificato risiede solo sul server
  - i clienti autenticano il server sul tunnel criptato
  - dopo l' autenticazine il dialogo prosegue utilizzando le chiavi scambiate in fase di autenticazione
- LEAP proprietario CISCO (Lighweight Extensible Authentication Protocol)
  - Altamente diffuso, e' stato il primo metodo disponibile sul mercato a rispondere ai problemi del WEP
  - CISCO ha messo le specifiche a disposizione dei piu' importanti produttori WiFi (supportato da Apple Airport, Intel Centrino)

Scelte Per ESACOM WLAN

- Tecnologia basata su IEEE standards
  - Standard 802.11b come Wireless LAN
  - Autenticazione 802.1x con CISCO LEAP
    - Unica soluzione completa ragionevolmente sicura disponibile nel 2002
- Soluzione basata su fornitore unico
  - Cisco
    - PC Cards: Cisco Aironet 350
      - Supporto per MAC OS X, Linux oltre a Windows
    - Access points: Cisco Aironet 350/1200
    - AAA Servers: CISCO ACS
    - Gestione , aggiornamento, monitoraggio Wireless LAN
      - Cisco Wireless LAN Solution Engine

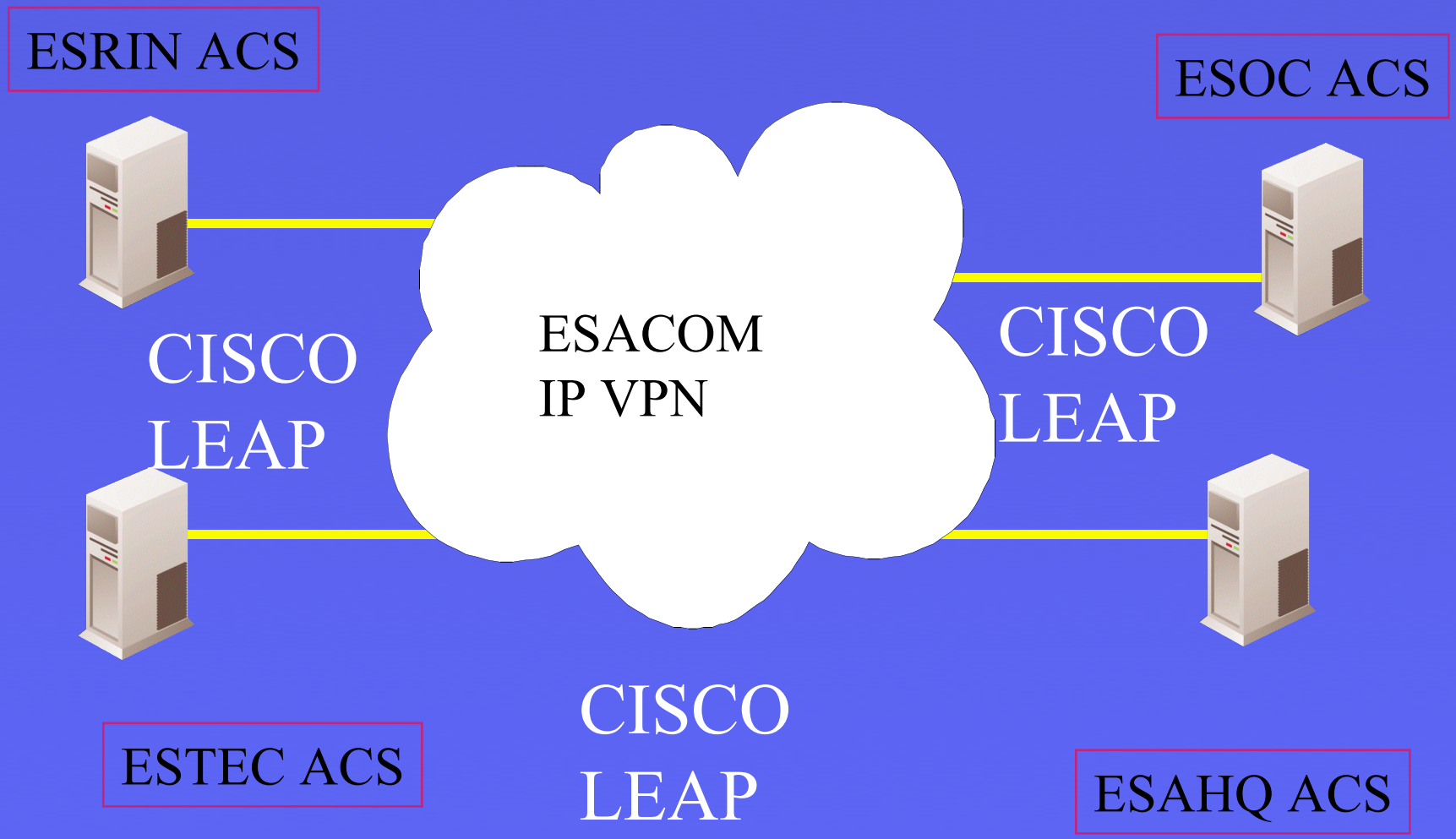
Disegno Di ESACOM WLAN



esa

Informatics Department
Directorate of Administration

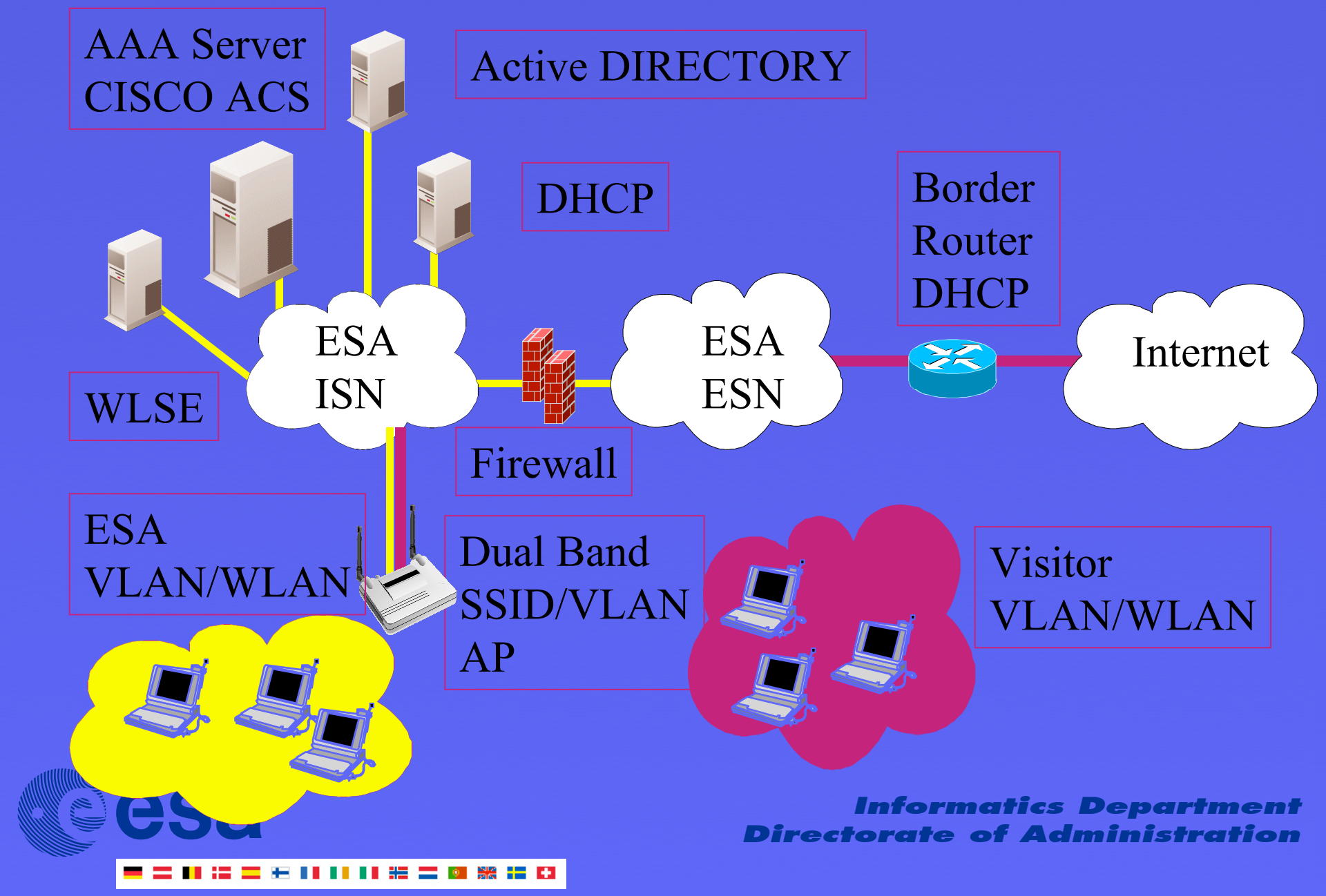
ESACOM WLAN AAA Servers



esa

Informatics Department
Directorate of Administration

NUOVA ESACOM WLAN



esa

Informatics Department
Directorate of Administration

Operazioni

- Operazioni della Rete Wireless effettuate attraverso una stazione di management dedicata
  - Gestione e mantenimento dell'infrastruttura
    - Aggiornamento del firmware e delle configurazioni
    - riconfigurazione veloce degli apparati per eventi particolari
  - Supporto all' utente
    - Sito WEB
    - Helpdesk
    - Tecnici
  - Procedure Operative
  - Evoluzione

Nuove Scommesse

- Analisi ed integrazione di nuovi standard
  - 54Mbps: 802.11G 2.4 GHz, & 802.11A GHz,
  - 802.11E Qualita del Servizio (QoS)
  - 802.11F Inter Access Point Protocol (IAPP)
  - 802.11I Sicurezza (WPA: WiFi Protected Access)
- WiFi Hotspot per utenti spesso fuori sede con accesso via IPSEC e https
- Ad hoc networking & Zerooconf
- Voce su WLAN (VoWLAN)

Conclusioni

- ESACOM WLAN ha rivoluzionato il modo di lavorare degli utenti ESA ed e' uno fra i servizi piu' apprezzati nel 2003
- Le scommesse tecniche da affrontare per la realizzazione di una rete wireless sicura richiedono competenze su tutti i fronti IT
  - Standard, Sicurezza, IP , LAN, RF, Cablaggio
- La Sicurezza ha un ruolo fondamentale
- C'e' differenza fra installare la rete wireless a casa o in una realta' aziendale
- Si apriranno nuove ed entusiasmanti possibilita' per avvicinarsi al concetto di ubiquita'

Riferimenti

WiFi Alleance	http://www.wi-fi.org/
Cisco Wireless	http://www.cisco.com/en/US/tech/tk722/tech_topology_and_network_serv_and_protocol_suite_home.html
Zeroconf	http://www.zeroconf.org/
WiFi planet	http://www.wi-fiplanet.com/
IEEE	http://www.ieee802.org/
Oreilly	http://wireless.oreilly.com/
WEP	http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
802.1x	http://www.mtghouse.com/
802.1x	http://www.funk.com/
Apple Airport	http://www.apple.com/airport
AirDefense	http://www.airdefense.net/
TERENA Mobilty	http://www.terena.nl/tech/index_mobility.html
WiFi hotspots	http://www.wi-fihotspotlist.com/
AAA	http://www.surfnet.nl/innovatie/wlan/