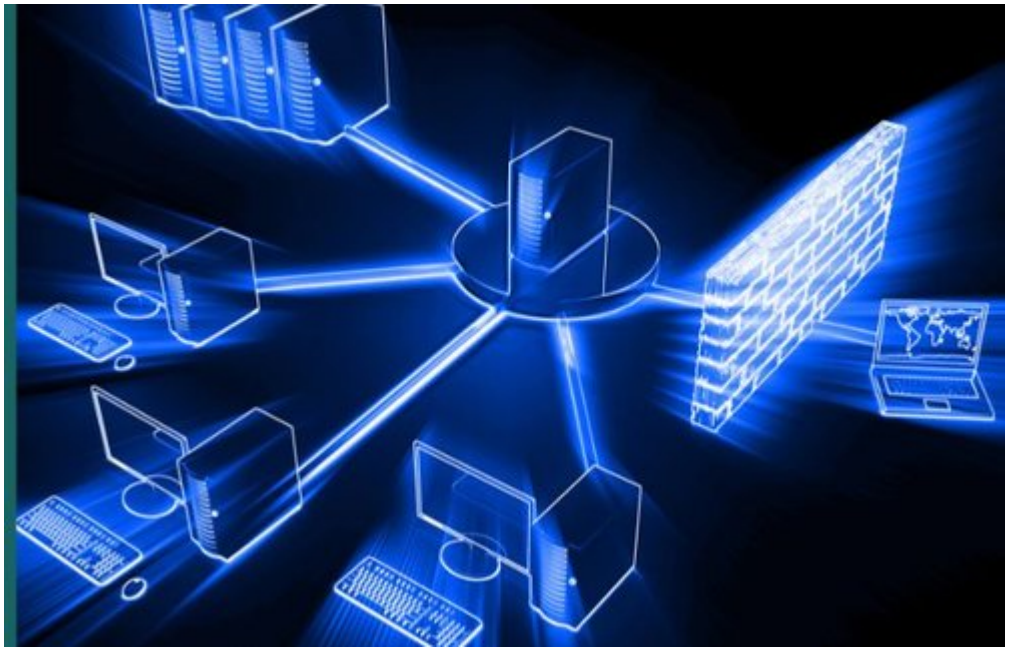
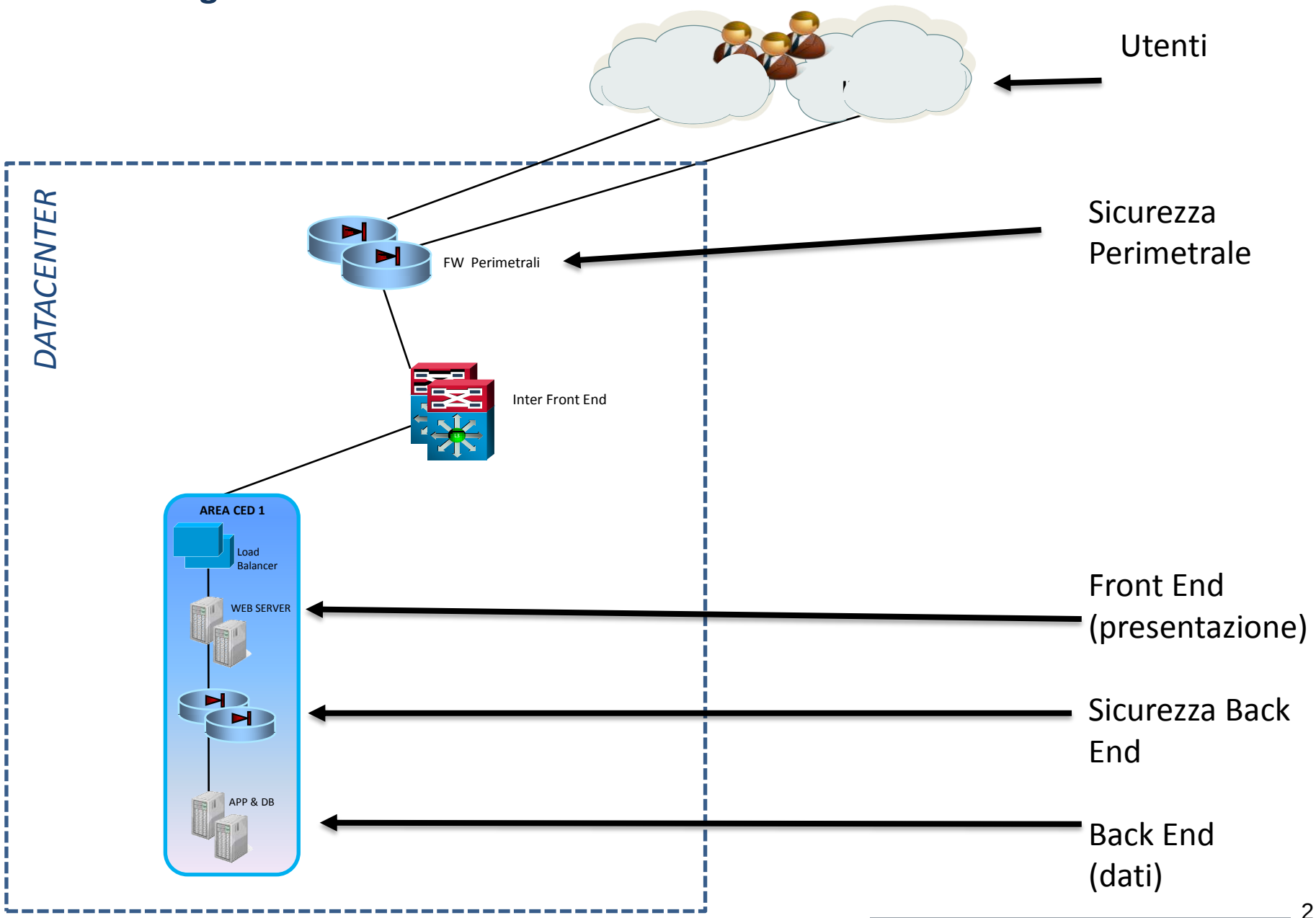
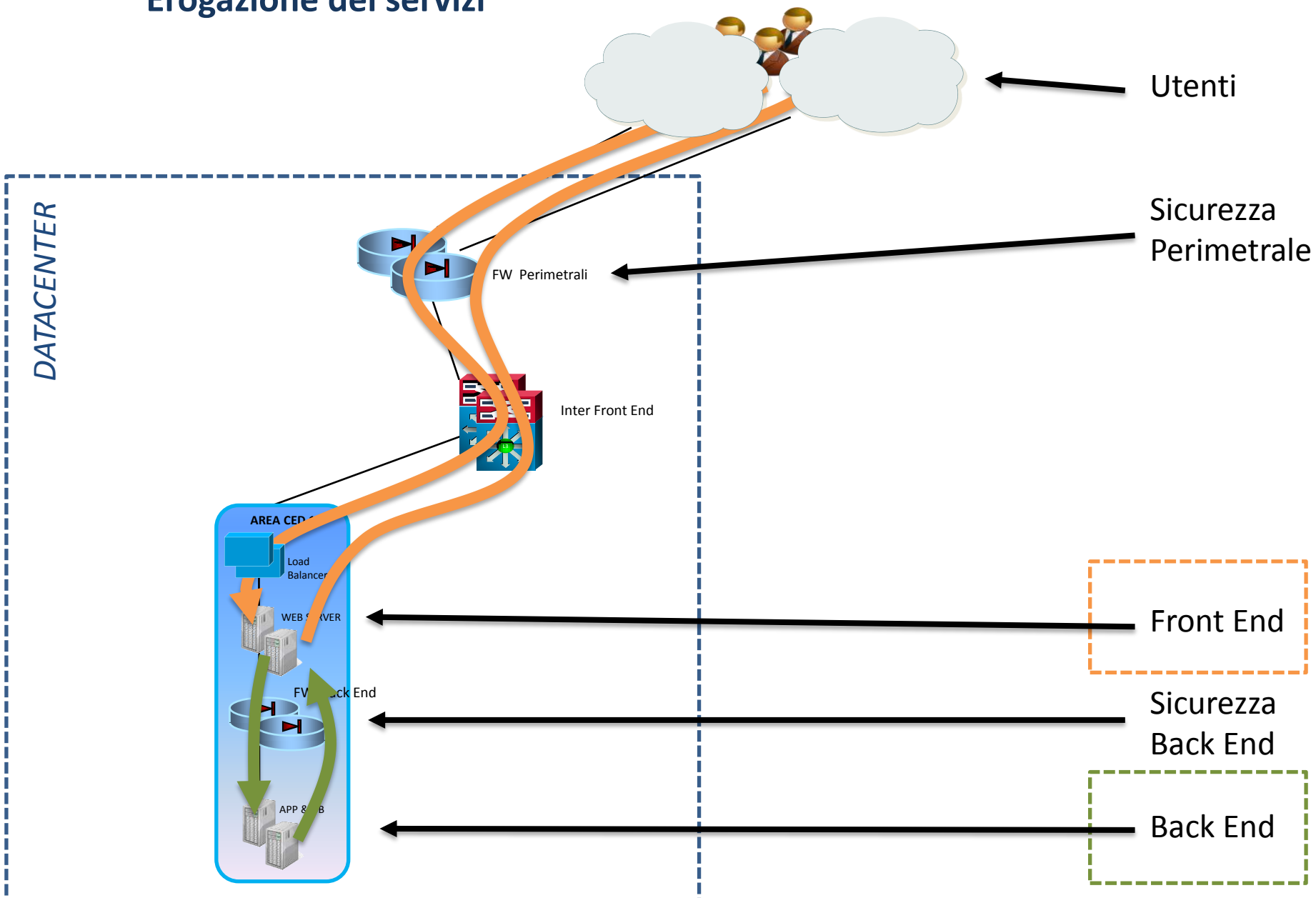


Networking

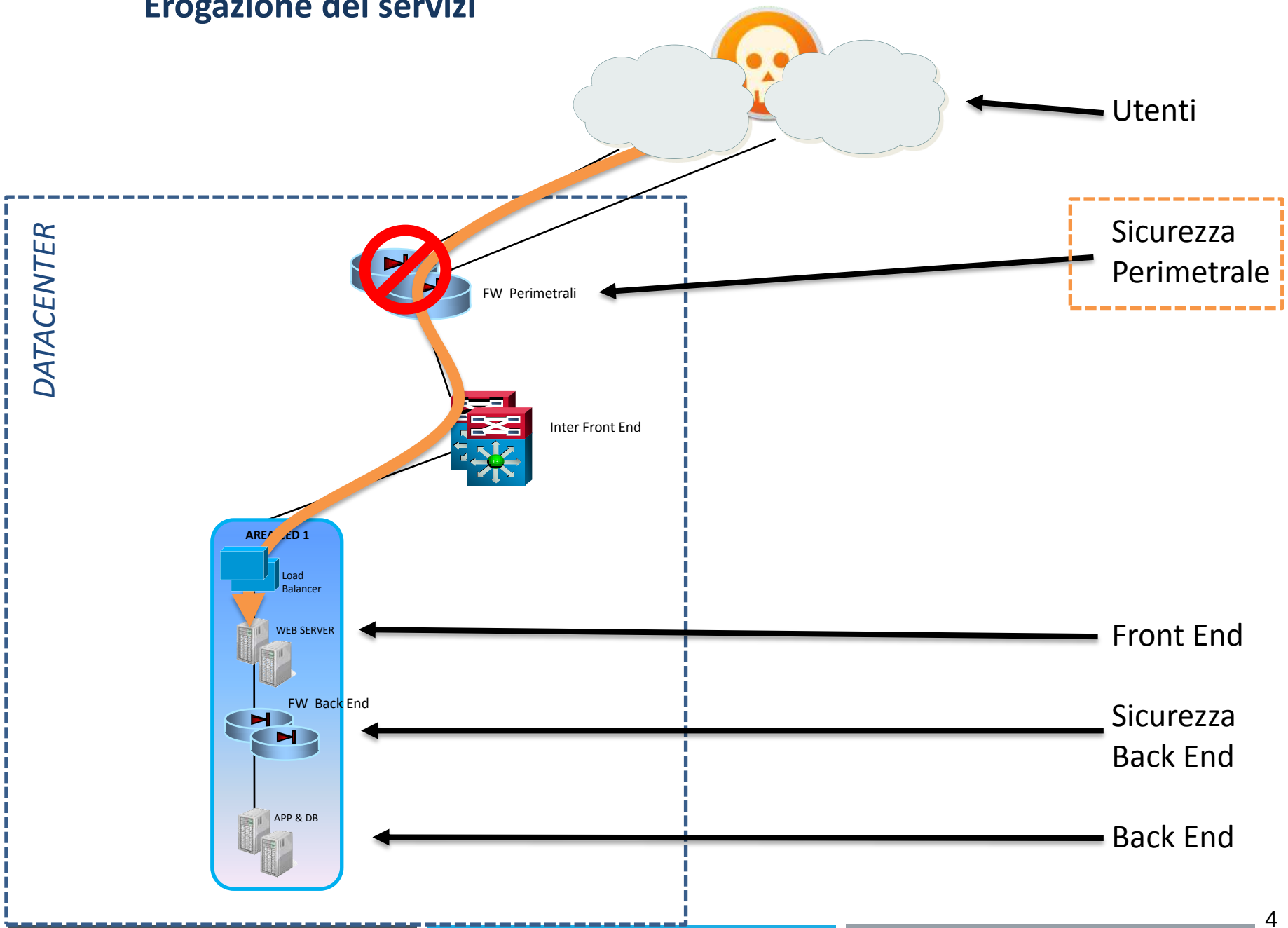
Erogazione dei servizi



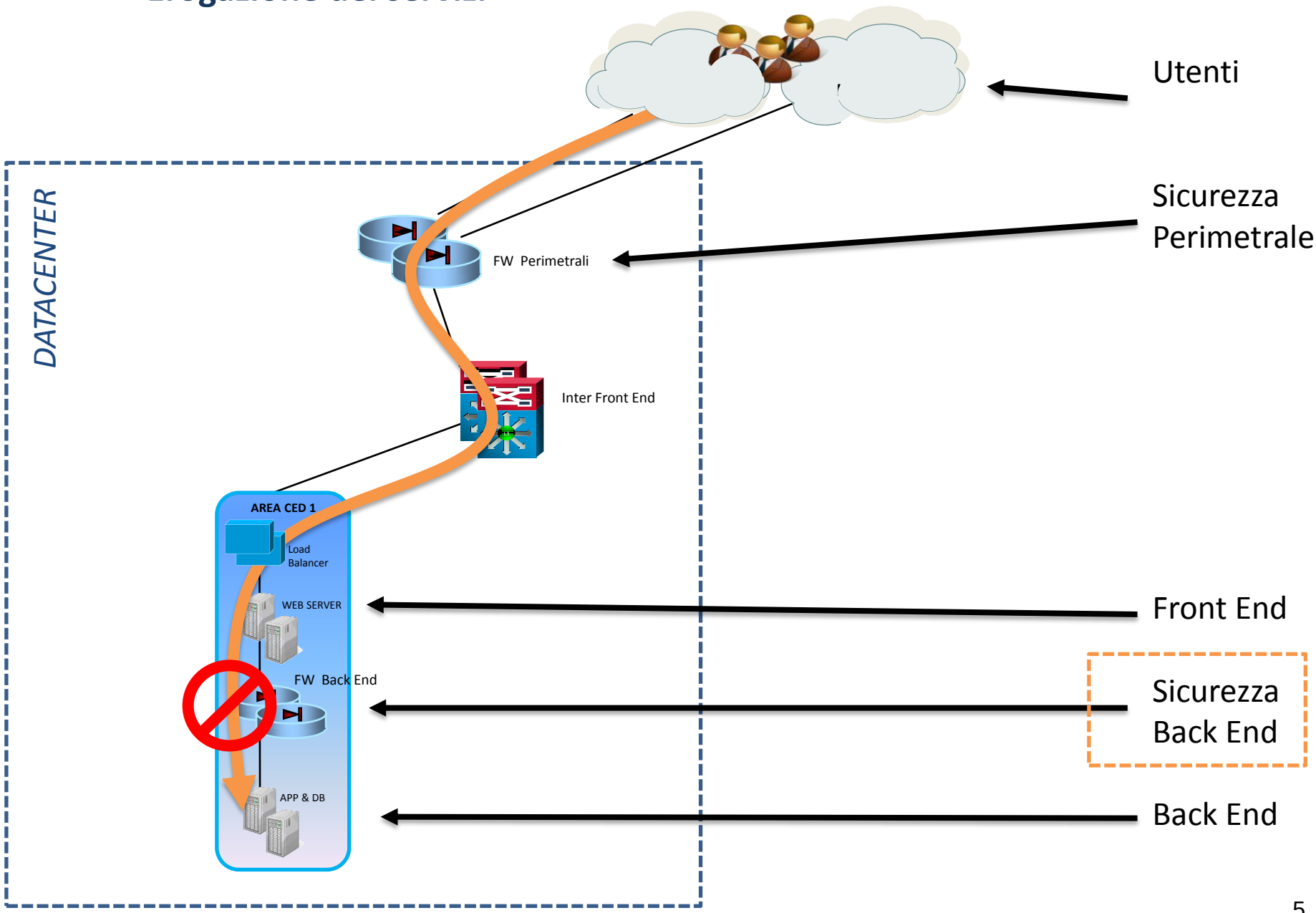
Erogazione dei servizi



Erogazione dei servizi



Erogazione dei servizi



ELEMENTI DI NETWORKING – *Definizione di reti*

Una rete locale o geografica è un insieme di apparati attivi e passivi che consentono a più computer di comunicare fra di loro.

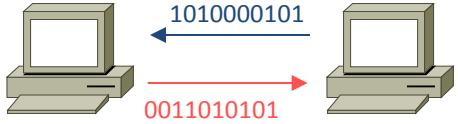
Una rete si definisce locale quando interessa una limitata area topologica (un piano, un edificio, ecc..) mentre si definisce geografica quando per la sua estensione collega computer dislocati su un territorio diverso da un edificio.

Distanza	Ambito	Tipo di rete
10 m	Ufficio	Rete locale (LAN)
100 m	Edificio	Rete locale (LAN)
1 km	Campus	Rete locale di Campus (LAN)
10 km	Città	Rete metropolitana (MAN)
100 km	Regione	Rete geografica (WAN)
1000 km	Nazione	Rete geografica (WAN)
10.000 km	Pianeta	Internet

ELEMENTI DI NETWORKING – *i protocolli*

Scambiare dati fra computer significa scambiare una serie di numeri che in binario corrispondono ad una serie significativa di impulsi elettrici.

Per far si che la serie sia significativa occorre utilizzare uno standard di comunicazione condiviso fra il computer mittente e il destinatario della comunicazione, analogamente all'uso della stessa lingua per la comunicazione umana.



I protocolli di comunicazione sono dei linguaggi standard di comunicazione fra apparati che definiscono il formato degli impulsi in partenza o in arrivo e il significato degli stessi.

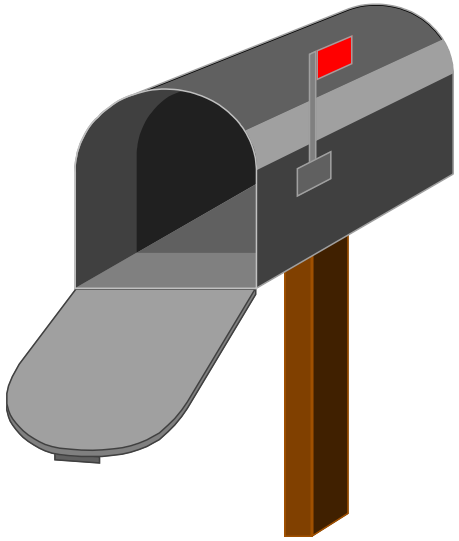
Un protocollo di comunicazione aggiunge dei dati rispetto a quelli originari, dati che sono utili alla sola comunicazione.

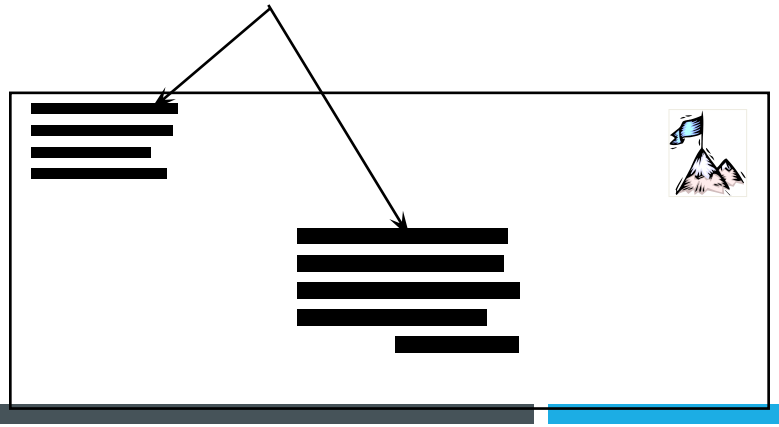
ELEMENTI DI NETWORKING – *i protocolli*

Immaginiamo di voler inviare un documento via lettera.

Cosa dobbiamo preparare :

- **Il documento (i dati)**
- **Una Busta (il protocollo)**
- **Scrivere l'indirizzo del destinatario e del mittente sulla busta**





A chi e a cosa serve l'indirizzo del destinatario e del mittente ?

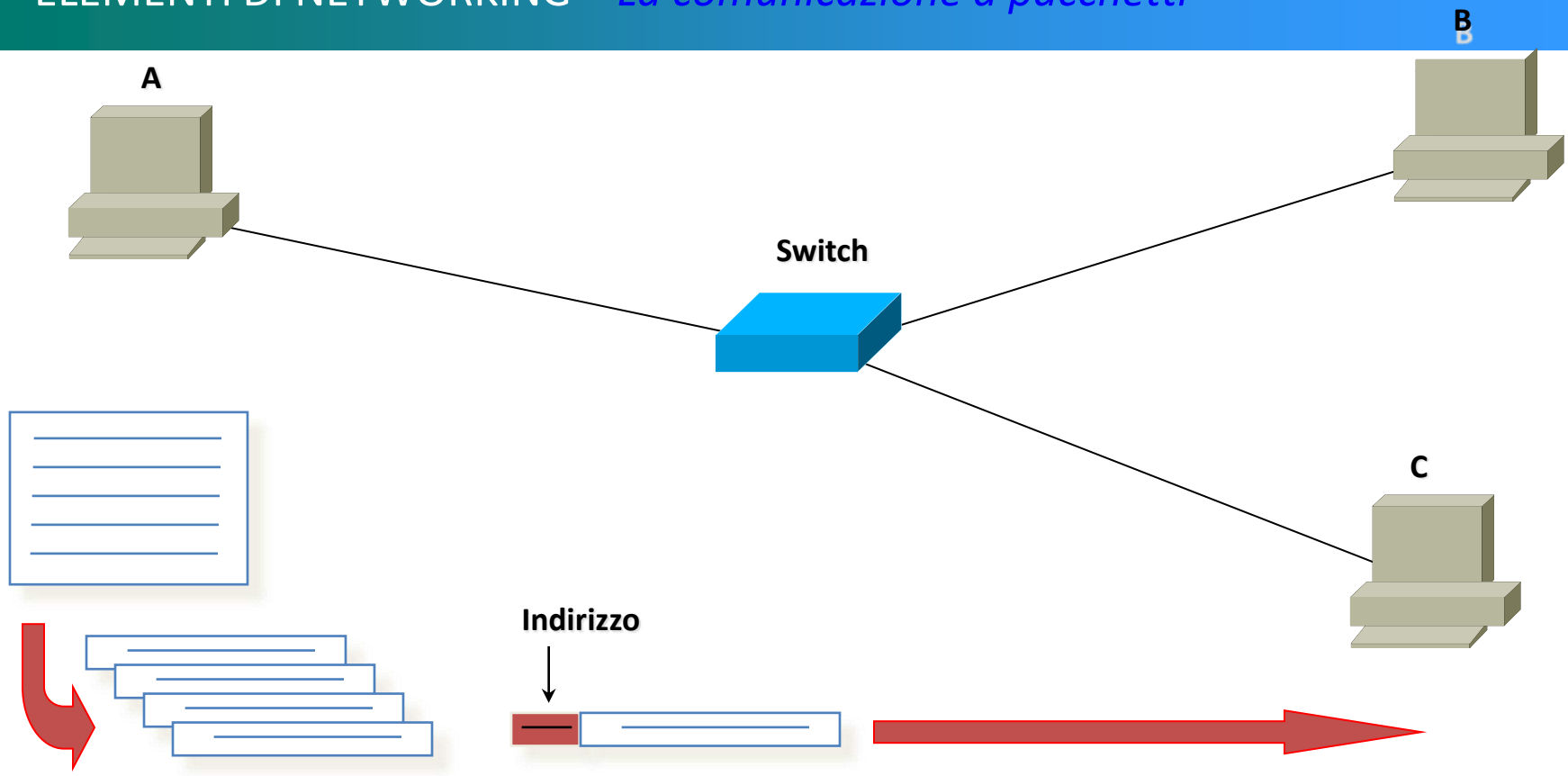
ELEMENTI DI NETWORKING – *i protocolli*

L'indirizzo del destinatario e del mittente servono al postino per recapitare la lettera e…

- **Non aggiungono nessun valore al documento che il mittente ha spedito**
- **Sono significativi solo se scritti in vista sulla busta e non se nascosti all'interno**

- **Sono dati utili e significativi solo per far recapitare la busta.**
- **Sono quindi dati aggiunti a quelli che il mittente vuole che siano recapitati che hanno la sola funzione di far si che il contenuto della busta arrivi effettivamente al destinatario.**
- **Sono Istruzioni che vengono fornite al mezzo che trasporta i dati significativi (il postino) per potergli far compiere il suo dovere.**

ELEMENTI DI NETWORKING – *La comunicazione a pacchetti*



Se A deve trasmettere dei dati a C accade questo :

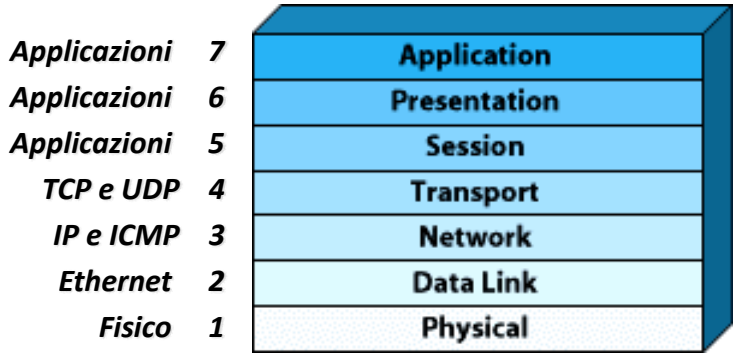
- **I Dati vengono divisi in pacchetti di lunghezza uguale (il nostro documento)**
- **Ai dati vengono aggiunti l'indirizzo del destinatario e e del mittente (busta con indirizzo)**
- **I dati vengono inviati e lo Switch (il postino) legge l'indirizzo e consegna il pacchetto a C**

ELEMENTI DI NETWORKING – *La pila ISO/OSI*

Ogni pacchetto inviato da un computer è imbustato più volte in quanto gli apparati e le macchine in gioco che necessitano di istruzioni, i postini, sono più di un tipo e utilizzano informazioni diverse.

Per ogni pacchetto esiste quindi una "pila" di protocolli che consentono di recapitare il pacchetto a destinazione.

La "pila" di riferimento principale si chiama ISO/OSI, e ha sette livelli:



I livelli che ci interessano sono il 2 ed il 3 e un po' anche il 4.

Il livello 2 della pila ISO/OSI

Il protocollo più usato nelle LAN: Ethernet

• L2 Switch

- ***Gli switch sono apparati che operano a livello 1 e 2 della pila ISO/OSI***
- ***Sono utilizzati oggi per realizzare reti locali a cablaggio stellare***

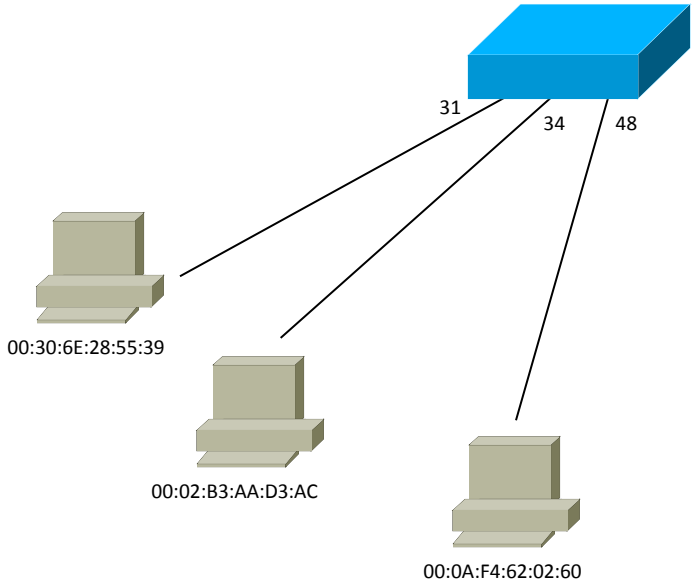
IL LIVELLO 2 - *il protocollo Ethernet*

La scheda di rete ha un suo indirizzo attribuito dal costruttore: si chiama *MAC ADDRESS* ed è composto da 16 cifre esadecimali. Questo è un indirizzo di livello 2 della pila ISO/OSI.

Al livello 2 lavorano gli Switch.

Lo Switch ha una tabella interna dove è scritta la corrispondenza tra un indirizzo di MAC ADDRESS e la porta dove è connesso (ovvero una tabella di conversione tra il livello 1 e il livello 2 della pila ISO/OSI):

Mac	Port List
00:30:6E:28:55:39	31
00:0A:F4:62:02:60	48
00:02:B3:AA:D3:AC	34

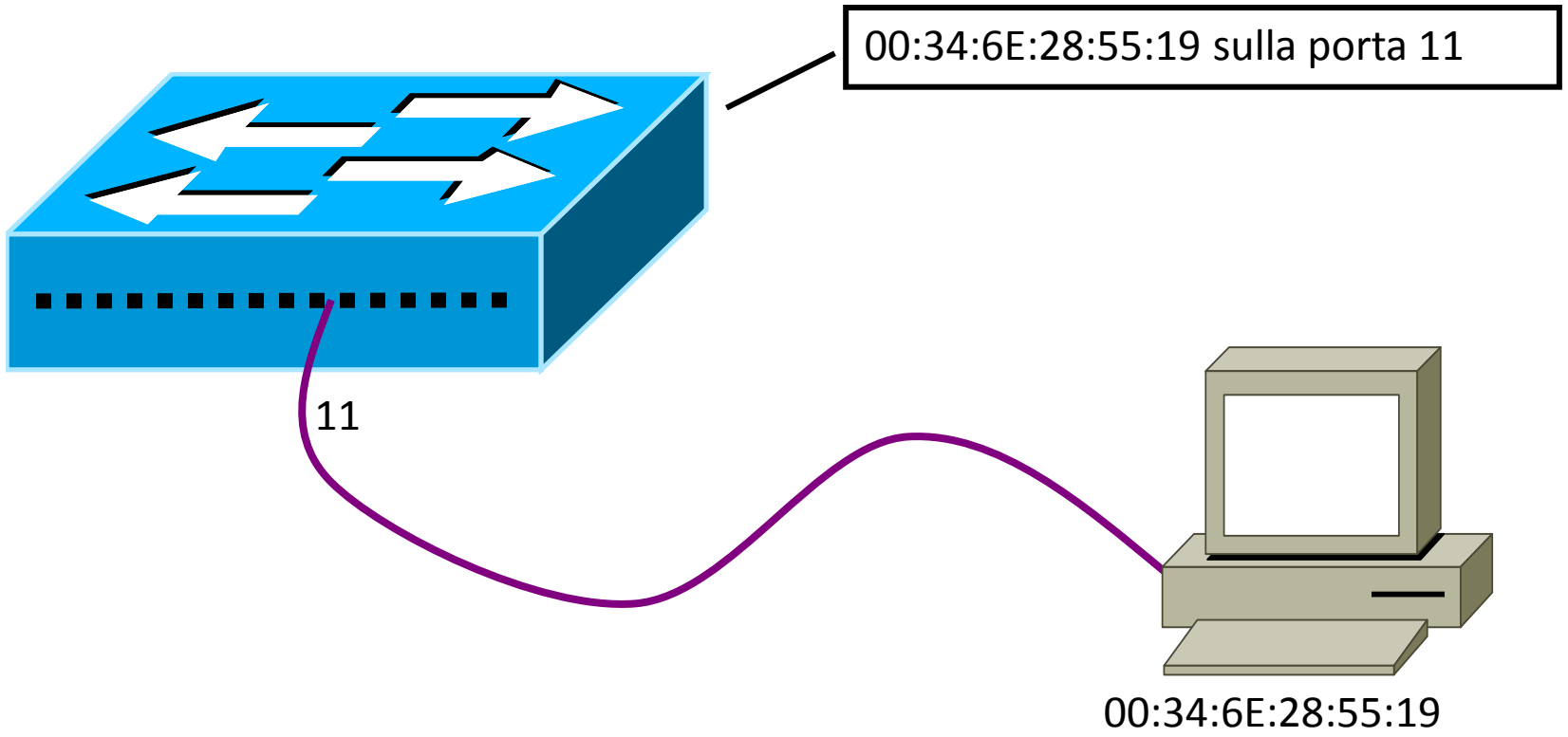


Questo protocollo di livello 2 si chiama Ethernet

IL LIVELLO 2 - *il protocollo Ethernet*

Ricapitolando:

- **ogni PC ha un suo indirizzo MAC ADDRESS**
- **Gli Switch sanno su quale loro porta è connesso questo MAC ADDRESS e sanno recapitargli i messaggi**



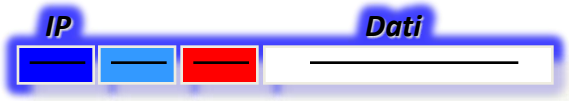
Il livello 3 della pila ISO/OSI

Il protocollo IP e il protocollo ICMP

IL LIVELLO 3 - *il protocollo IP*

Il livello 3 della pila ISO/OSI che ci interessa è l'*Internet Protocol*, o più brevemente IP.

Visto che sarebbe troppo difficile individuare l'indirizzo MAC ADDRESS della macchina con cui vogliamo scambiare i dati (solo FS ha oltre 100.000 utenze, pensate Internet!), si è reso necessario utilizzare un altro protocollo, dove gli indirizzi vengono assegnati dagli amministratori delle singole reti. Appunto il protocollo IP.



L'indirizzo IP identifica, in modo univoco, un elaboratore (host) in una rete (net). Esso è rappresentato con una stringa di 32 bit, divisa in 4 byte (ottetti di 8 bit) tradotti in forma decimale puntata.

Esempio: 192.168.149.12 (che sarebbe 00001010.11101001.10010101.00001100)

Regola : gli ottetti vanno da 0 a 255 (tutti i bit a 0 fino a tutti i bit a 1).

La possibilità di parlare tutti con tutti creerebbe dei grossi problemi di "confusione", così si inseriscono all'interno di una stessa "net" o rete solo i computer che vogliamo parlino tra loro (attraverso uno Switch) direttamente. Gli altri computer faranno parte di altre net e solo in caso di necessità verrà stabilito il colloquio tra net diverse.

IL LIVELLO 3 - *il protocollo IP*

La net è individuata dalla *classe* di appartenenza dell'IP che dipende dal primo ottetto:

xxx.yyy.zzz.qqq

Ci interessano 3 classi:

- **Classe A = da 1 a 127 (il primo ottetto è la net, il resto gli host, oltre 16M)**
- **Classe B = da 128 a 191 (i primi due byte sono la net, gli altri due l'host, 65534)**
- **Classe C = da 192 a 223 (solo l'ultimo byte individua uno dei 254 host)**

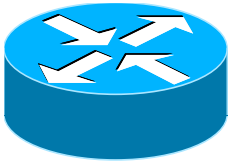
In un IP 10.233.149.1, 10 è la net e .233.149.1 è l'identificativo dell'host.

In un IP 172.16.5.44, 172.16 è la net e .5.44 è l'identificativo dell'host.

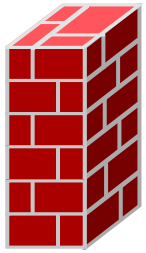
In un IP 192.168.11.67 invece la net è 192.168.11 mentre l'host il .67

IL LIVELLO 3 - *il protocollo IP*

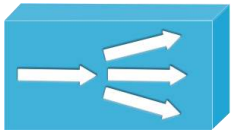
Al livello 3 lavorano i Router



Eseguono routing anche: i Firewall



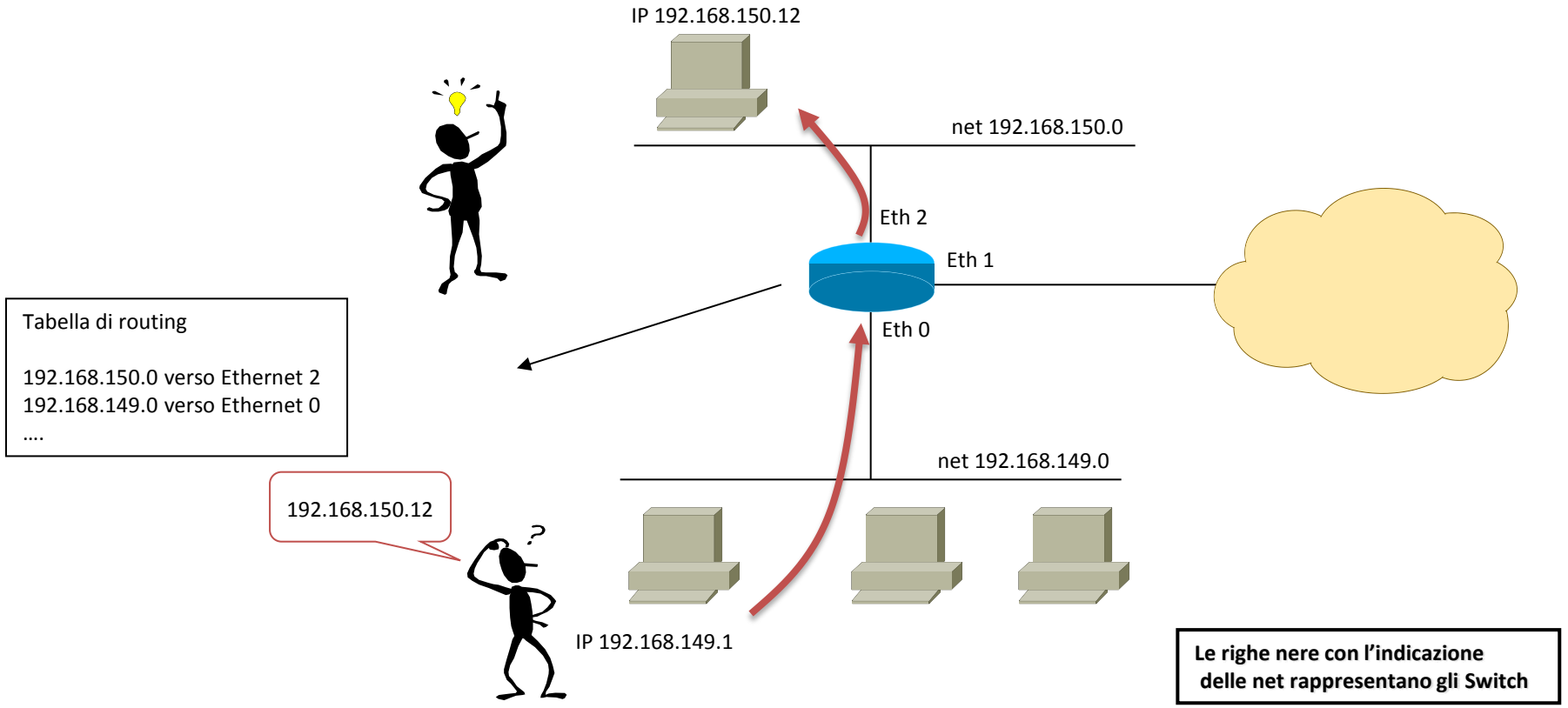
ed i bilanciatori



Quando due computer si trovano su due net differenti, se autorizzati, parlano attraverso i questi apparati.

IL LIVELLO 3 – *i Router*

Nel momento in cui un host deve parlare con una net che non conosce (quindi sicuramente non sua) invia il pacchetto IP al suo *default gateway*, un apparato di livello 3 che si trova sulla sua net, che ha una tabella di traduzione tra le net di destinazione e una delle sue interfacce (tabella di routing).



IL LIVELLO 3 – *i Router*

Se la net di destinazione non è direttamente connessa ad una interfaccia del Router, sulla tabella di routing si può scrivere il salto ("hop") che deve effettuare il pacchetto verso un altro Router:

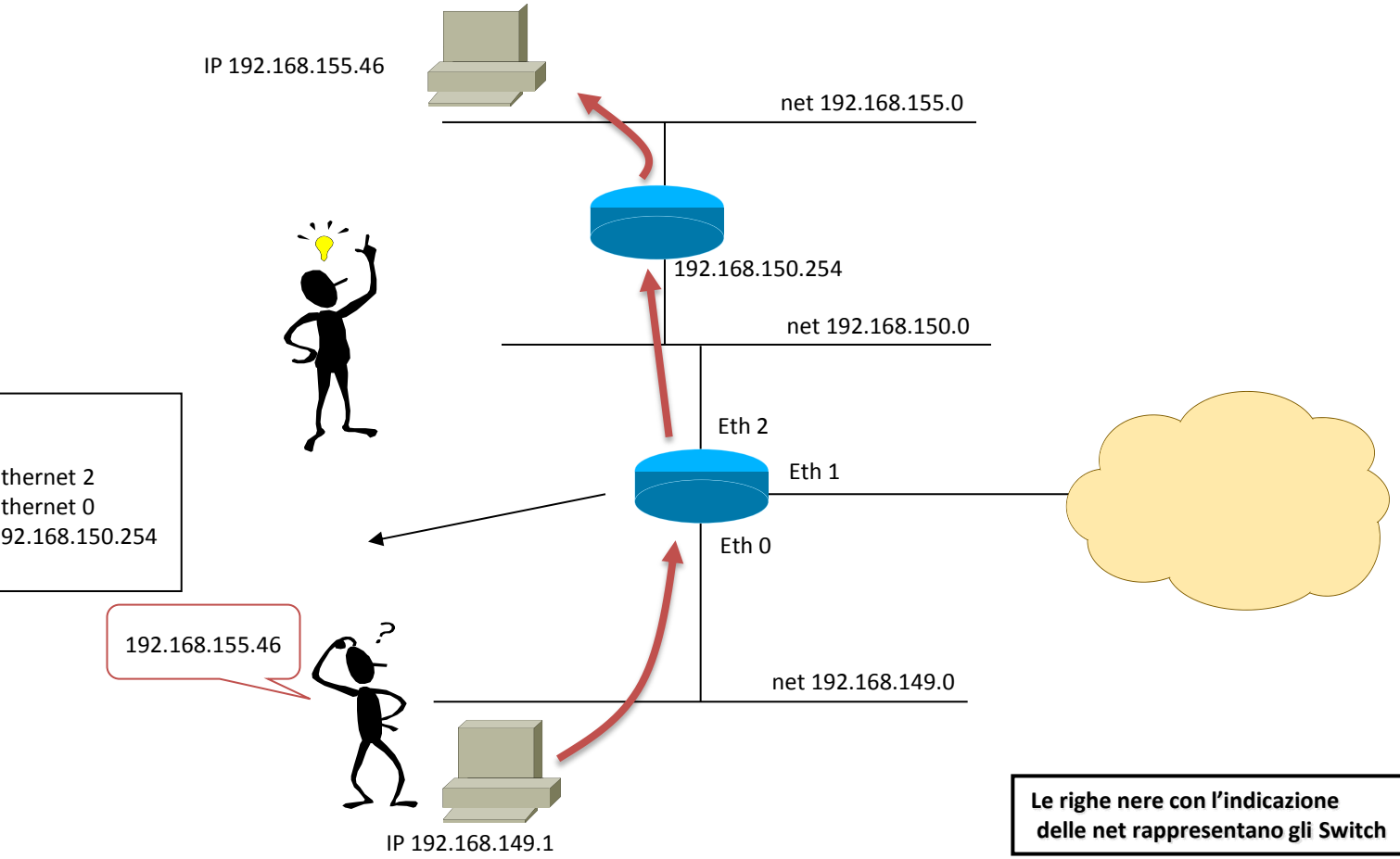


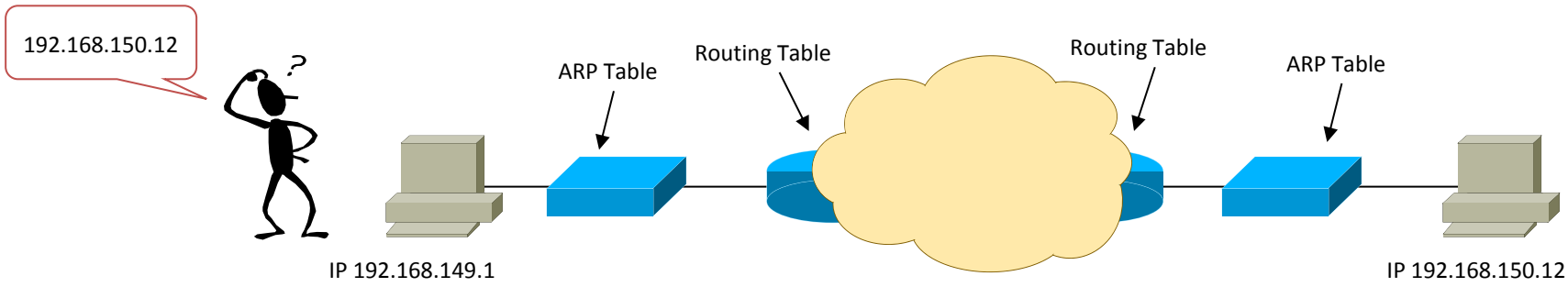
Tabella di routing

192.168.150.0 verso Ethernet 2
192.168.149.0 verso Ethernet 0
192.168.155.0 verso 192.168.150.254
....

Le righe nere con l'indicazione delle net rappresentano gli Switch

IL LIVELLO 3 – *i Router*

Quindi, tra le informazioni del Router e le informazioni dello Switch il percorso è completo:

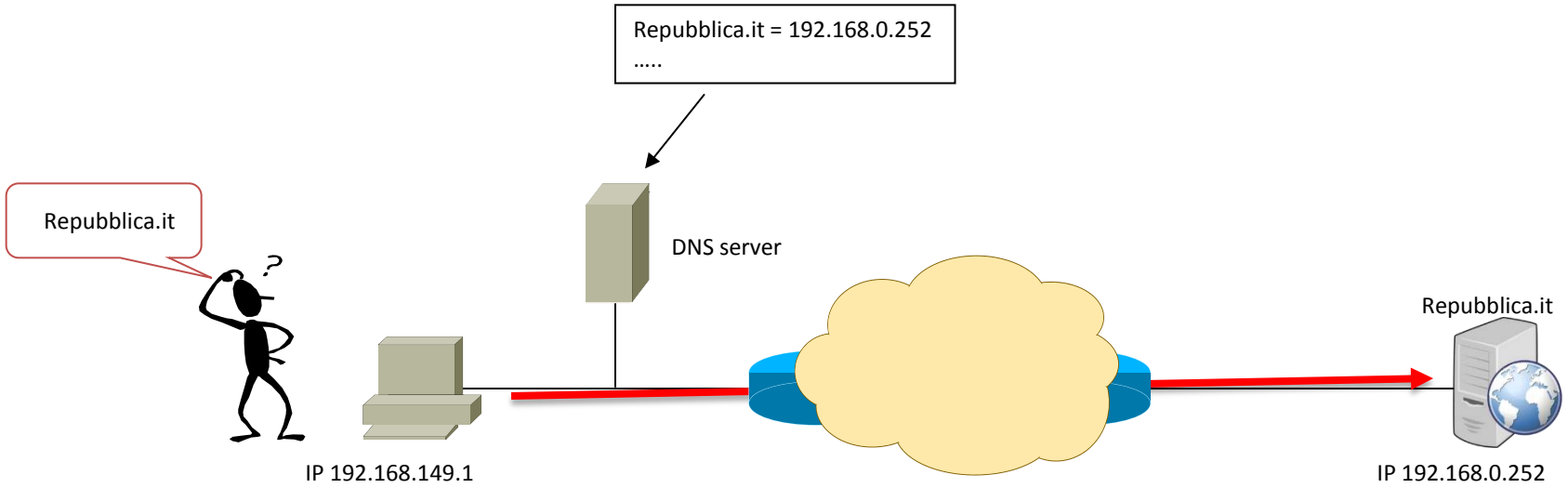


IL LIVELLO 3 – *i Router*

Visto che chiamare tutti i destinatari per indirizzo IP non è proprio semplice è stato creato un servizio di risoluzione dei nomi, il DNS.

Il servizio DNS non fa altro che associare un nome a un indirizzo IP. E' un server al cui interno c'è una semplice tabella di conversione.

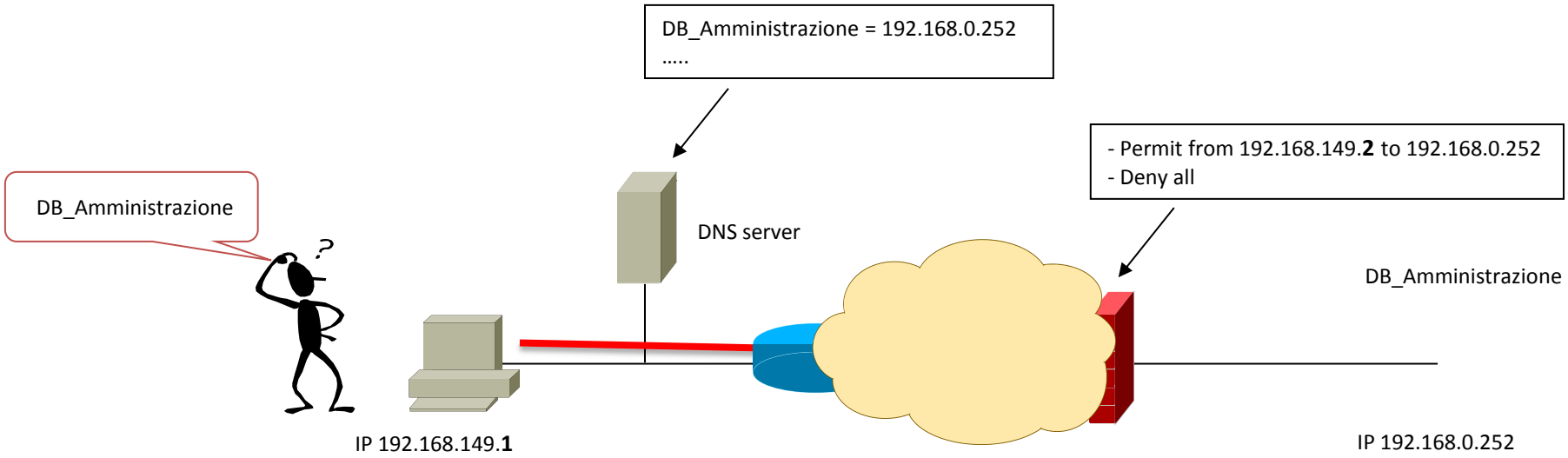
Nelle proprietà di rete dei PC si indica a quale server DNS puntare.



IL LIVELLO 3 – *i Firewall*

I router uniscono mentre i firewall impediscono la comunicazione.

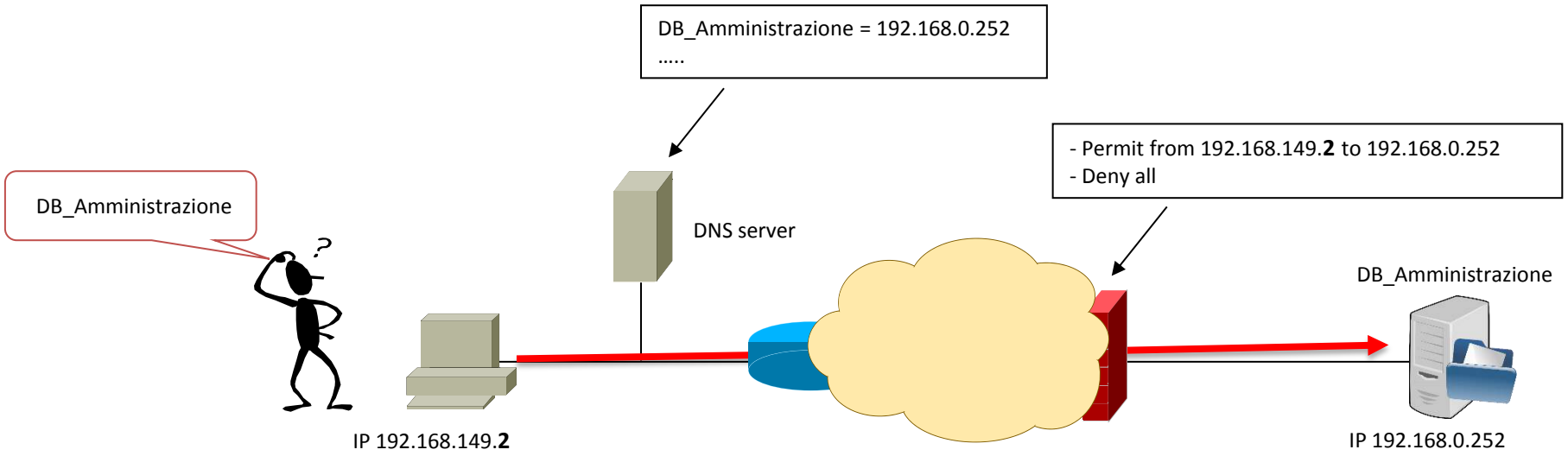
La regola è che i firewall negano l'accesso a tutti tranne che agli autorizzati.



IL LIVELLO 3 – *i Firewall*

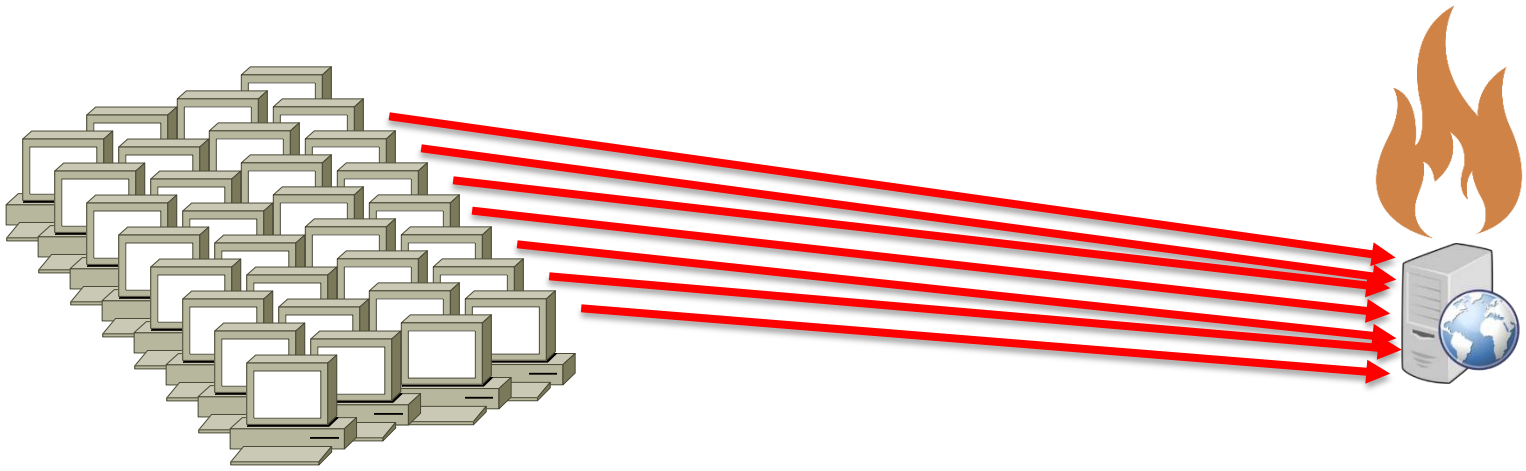
I router uniscono mentre i firewall impediscono la comunicazione.

La regola è che i firewall negano l'accesso a tutti tranne che agli autorizzati.



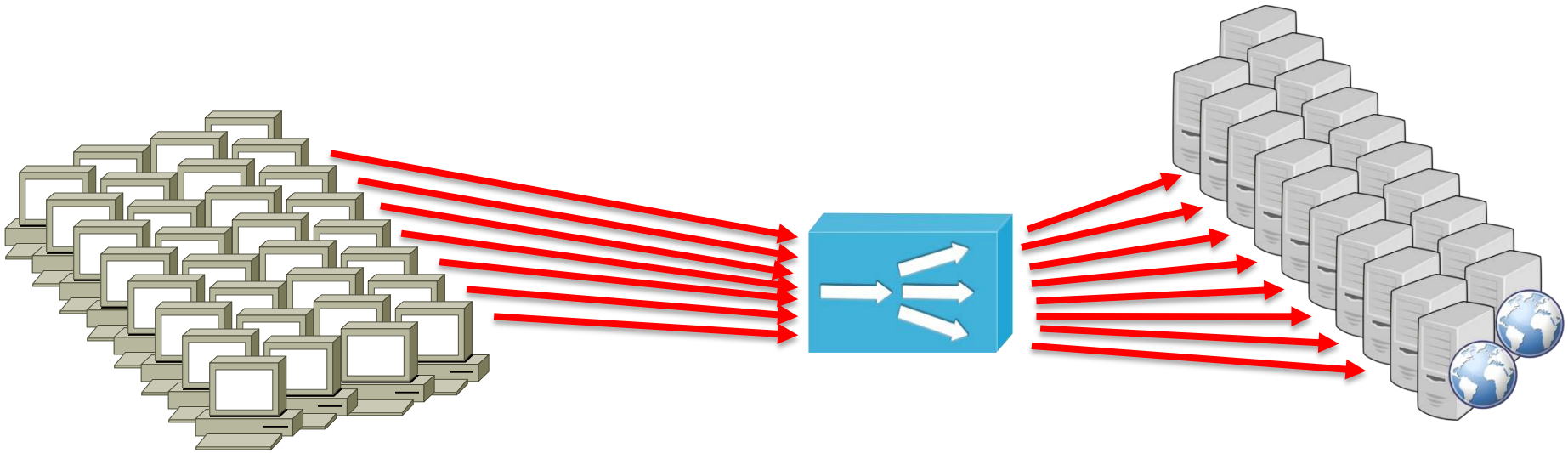
IL LIVELLO 3 – *i Bilanciatori*

- ***I servizi e le applicazioni possono essere esposti sia sulla Intranet che su Internet***
- ***In entrambi i casi, occorre effettuare una stima, in fase progettuale, del numero di accessi che l'infrastruttura può sopportare***
- ***Un solo server può essere in grado di esporre un servizio***
- ***Per il principio della ridondanza occorre avere più di un server che esponga lo stesso servizio***
- ***Esigenza di ridondanza (high-availability) + esigenza di potenza elaborativa (scaling) = presenza di due o più server (riuniti nella cosiddetta 'farm')***
- ***Come posso rendere il servizio, presente su più di una entità fisica, fruibile come una sola entità logica verso l'utente finale ?***



IL LIVELLO 3 – *i Bilanciatori*

- ***Rappresenta una server farm con un singolo indirizzo IP (public IP address, virtual IP address)***
- ***I client risolvono l'indirizzo IP attraverso una request DNS***
- ***Il Network Load Balancer gira il traffico sui server della farm***
- ***La scelta del server di destinazione avviene in base ad algoritmi preimpostati, e personalizzabili***
- ***Permette la distribuzione di un enorme carico di lavoro (connessioni) su più server fisici***
- ***L'NLB monitora costantemente la presenza e la vitalità dei server fisici, e li esclude dal pool se necessario; tale comportamento è a vantaggio della high-availability***



Evoluzione della sicurezza IT

1988

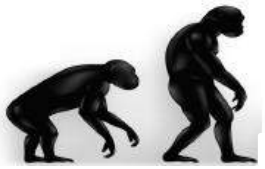
Physical Security…

Prevent the bad guys to enter the computers room

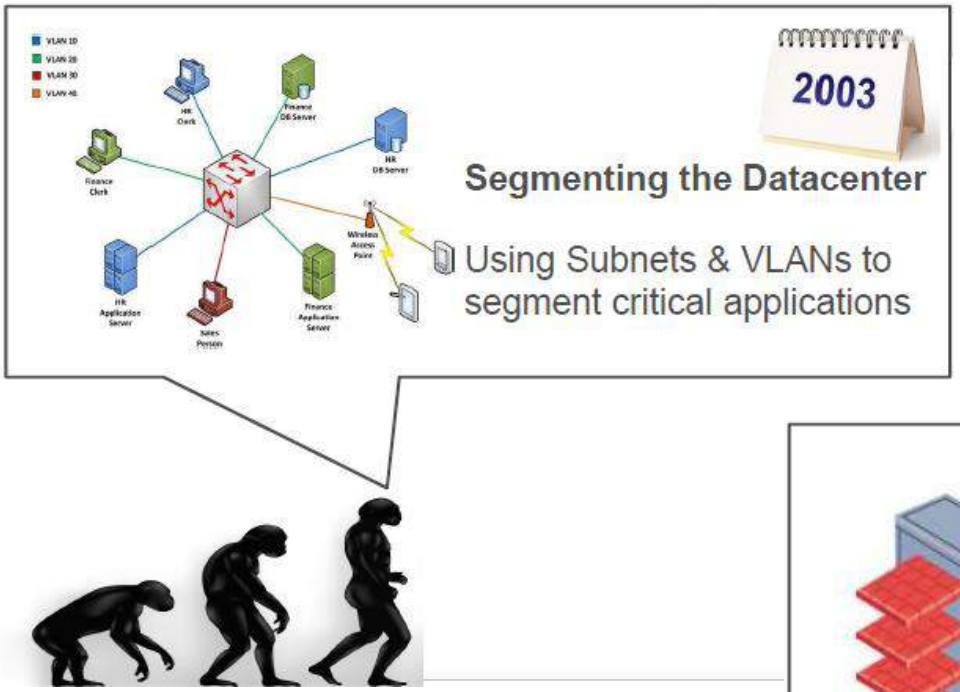
1998

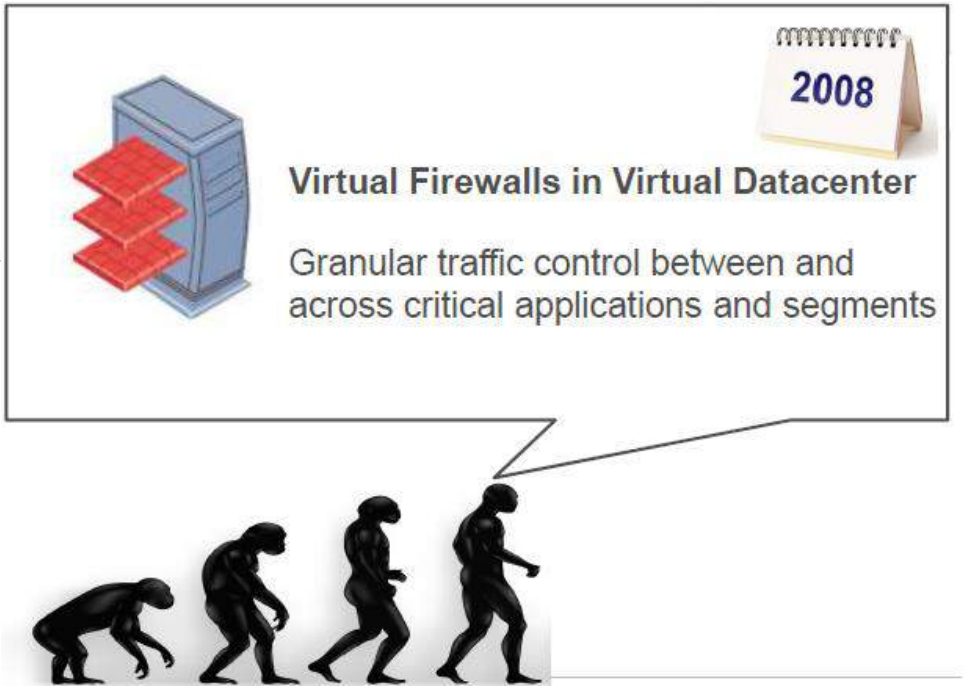
Internet & DMZ Firewalls…

Traffic Control to the Datacenter

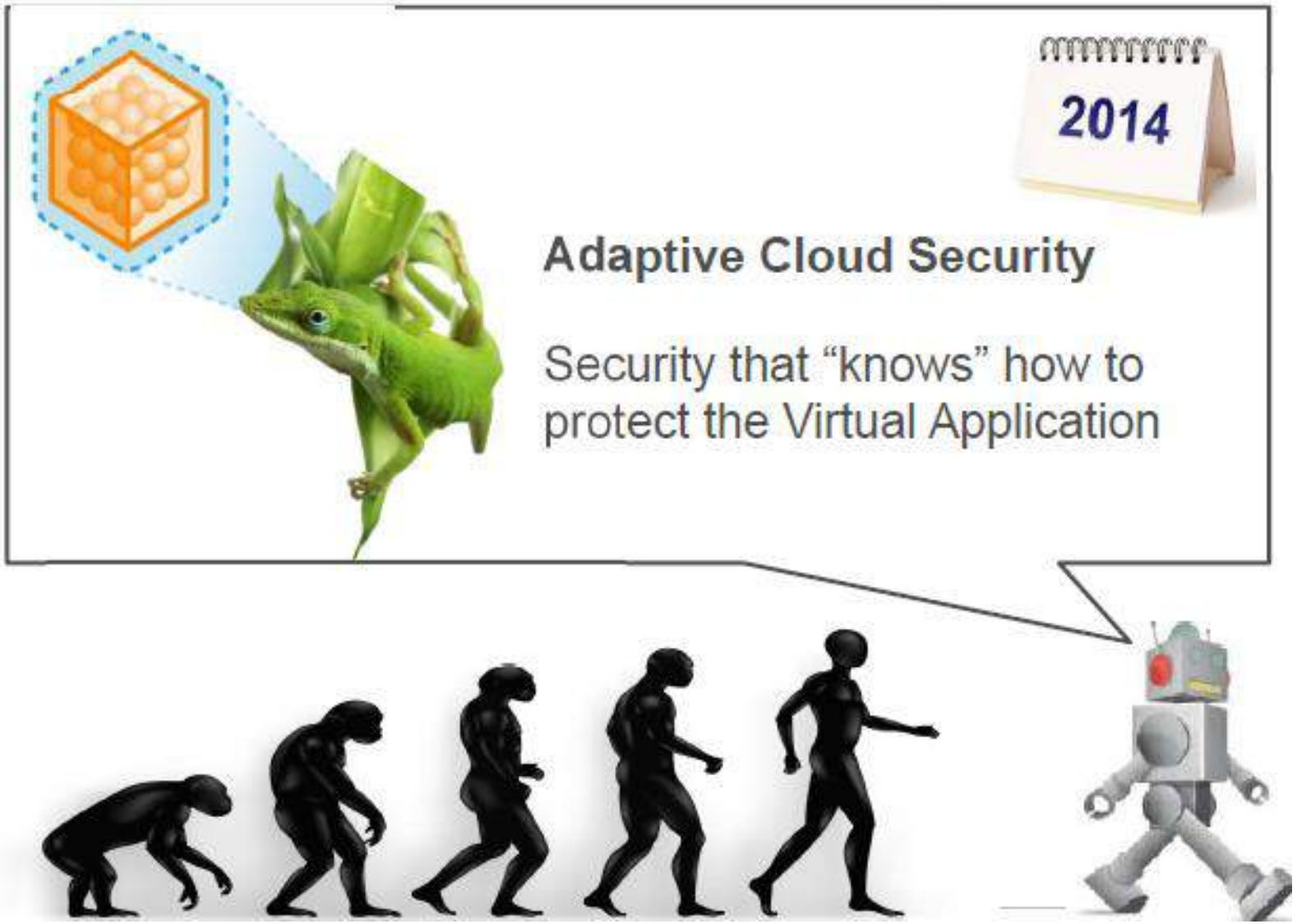


Evoluzione della sicurezza IT





Evoluzione della sicurezza IT



Evoluzione della sicurezza IT

A causa del cambiamento dei target del cyber crime, dello spionaggio e dell'hacktivism, gli attacchi diventano sempre più vari, come ad esempio l'hackeraggio di un sito di news dove è stata riportata la notizia falsa di bombe alla Casa Bianca: **la borsa è crollata** in pochi minuti.

CheckPoint ha eseguito nel 2013 uno studio sulle maggiori minacce alla sicurezza, attraverso l'analisi dei dati reali rilevati su 888 aziende clienti.

L'analisi ha evidenziato che:

- Il 61% delle aziende aveva traffico peer to peer
- Il 53% era vulnerabile ad attacchi sulle postazioni di lavoro
- Il 54% avevano dipendenti che hanno perso informazioni
- Il 63% aveva postazioni di lavoro infettate da BOT
- Il 43% presentava l'uso di anonymizers

Evoluzione della sicurezza IT

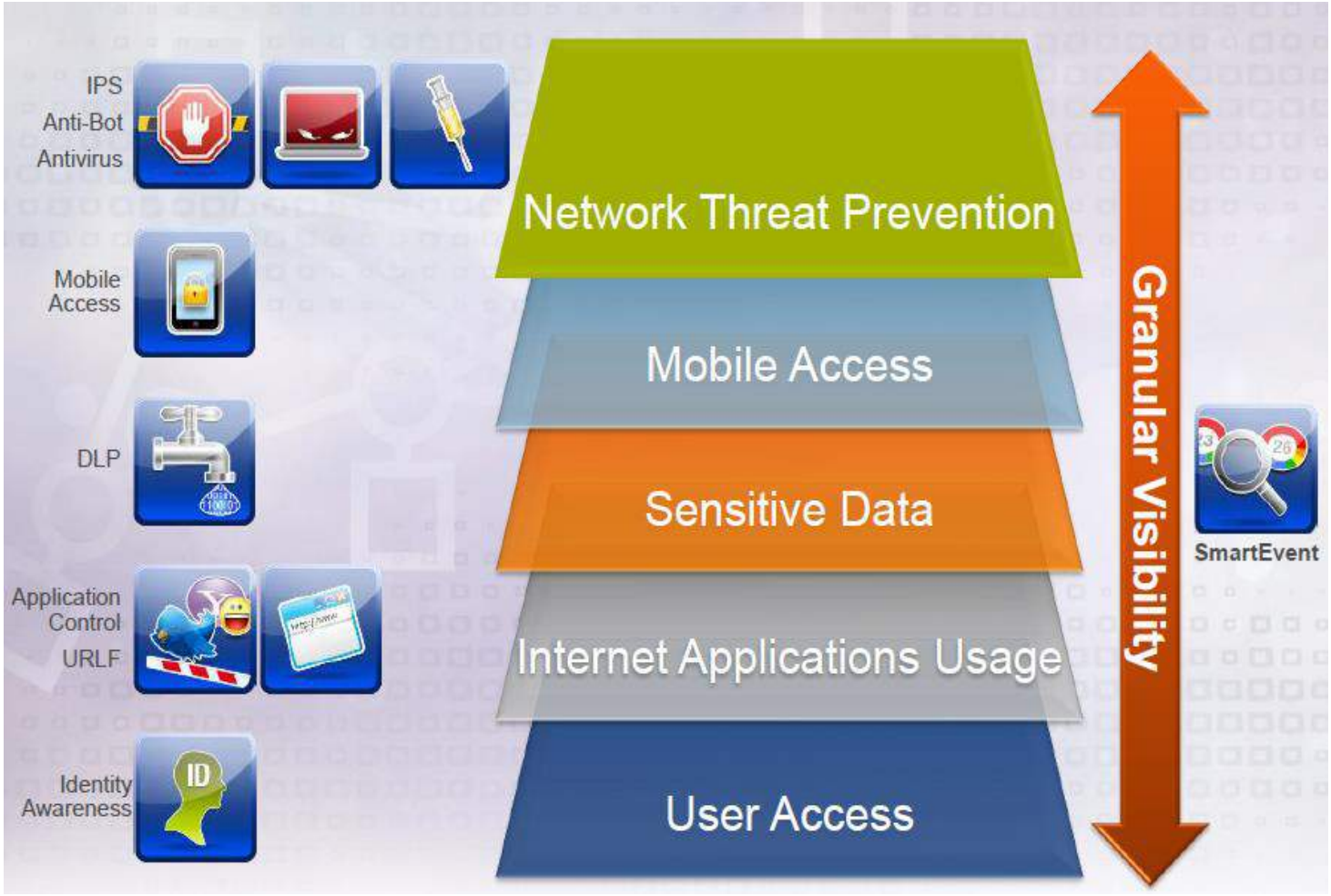
Le soluzioni tecnologiche per affrontare queste minacce sono:

- **Software Blade Architecture**: consente l'implementazione delle policies mediante l'estensione sullo stesso hardware delle componenti software di sicurezza disponibili, gestite centralmente ed in maniera modulare

- **Threat Cloud**: è una rete collaborativa tra gli utenti CheckPoint per la costituzione di una base di conoscenza in tempo reale delle minacce e per il relativo aggiornamento automatico delle protezioni sui singoli apparati

Evoluzione della sicurezza IT

Software Blade: Implementa una architettura di sicurezza multistrato integrando i vari prodotti come indicato nella figura seguente:



Evoluzione della sicurezza IT

Le blade software più interessanti ed innovative sono:

- **Mobile Access**: rende sicuro l'utilizzo privato/aziendale dei dispositivi mobili, creando un ambiente isolato e criptato accessibile solo dietro autenticazione. Implementa inoltre una VPN tra il dispositivo dell'utente ed i servizi Corporate
- **DLP** (data loss prevention): regola l'invio fuori dall'azienda di email (testo ed allegati) con informazioni classificate, come ad esempio numeri di carte di credito, fogli di budget…
- **Threat Emulation**: apre ed esamina il comportamento degli allegati delle email entranti in un'area protetta prima di inviarli all'utente, o bloccarli, nel caso siano dannosi.

- **Application Control**: consente di regolare l'uso di un gran numero di applicazioni che sfuggono ai tradizionali controlli dei firewall (esempio Emule, Torrent, Skype…)
- **URL Filtering** e **Identity Awareness**: prevedono la connessione con Active Directory per identificazione ed autorizzazione alla navigazione, propedeutico a eliminazione proxy

Evoluzione della sicurezza IT

Threat Cloud

Oggi contiene:

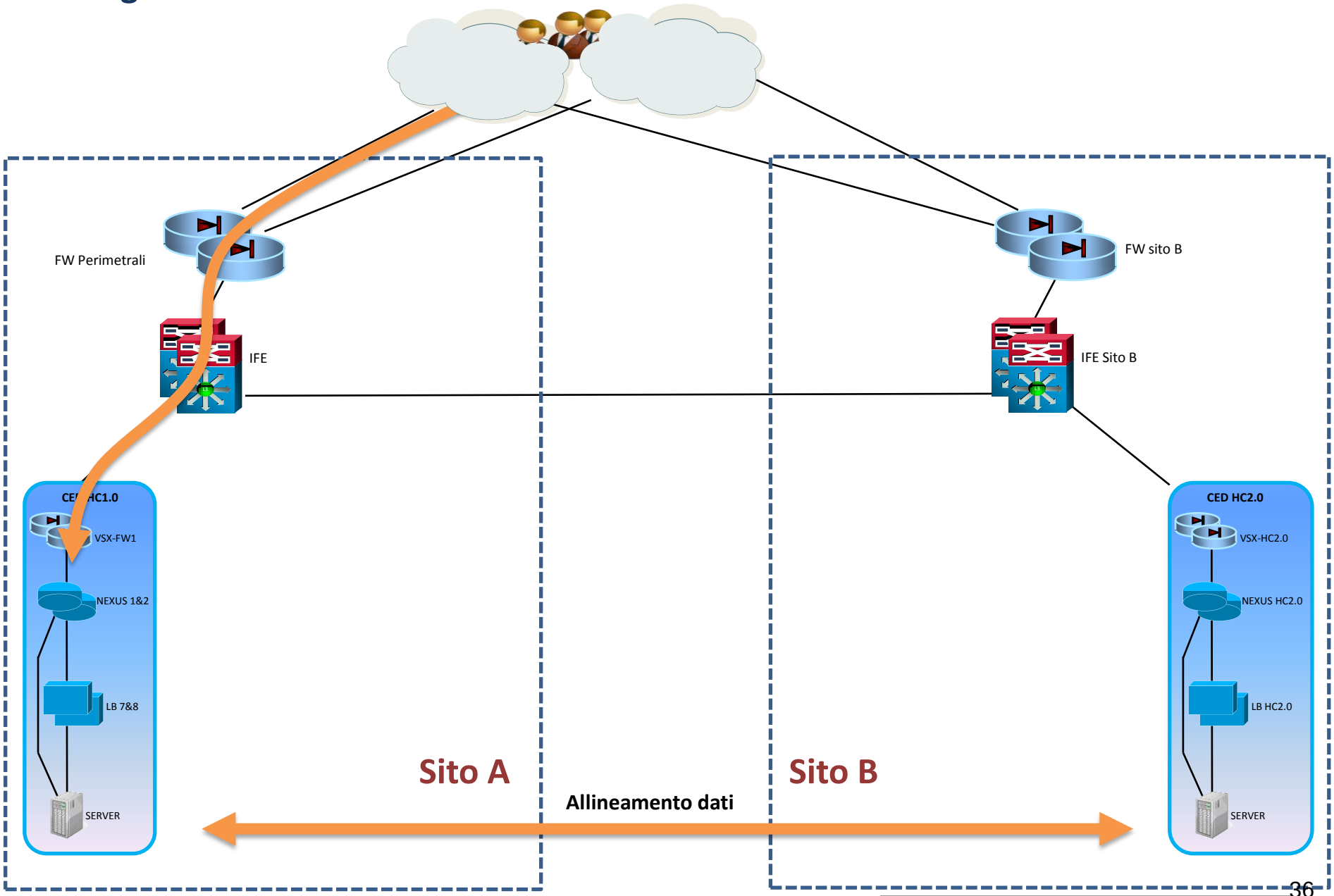
- Oltre 250M di indirizzi analizzati per la BOT discovery
- Oltre 4,5M di firme malware
- Oltre 300k siti affetti da malware

Auto-apprende:

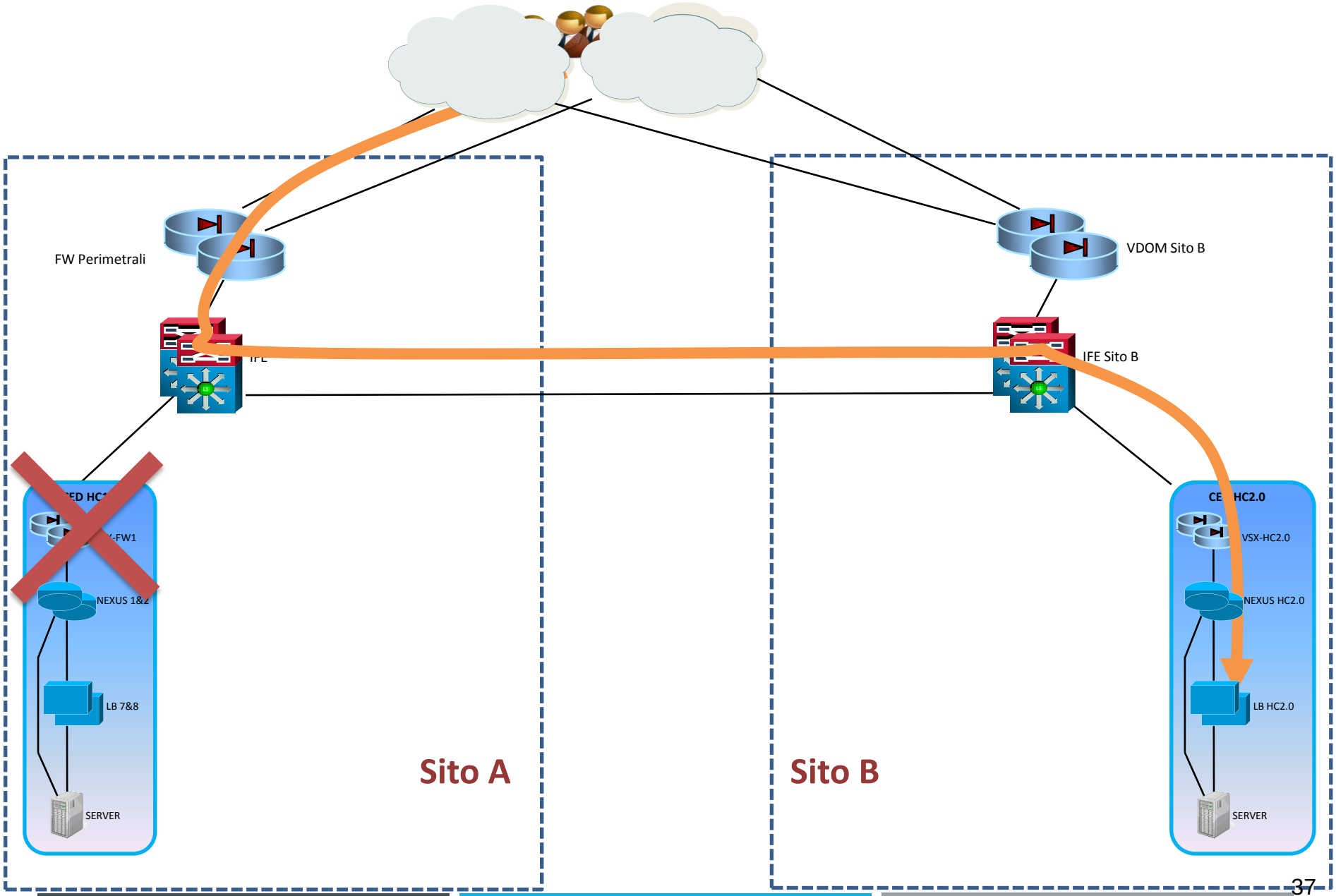
- Dinamicamente dalla rete dei sensori CheckPoint (che sono i dispositivi installati presso i clienti)
- Da analisti CheckPoint
- Da fonti esterne

Distribuisce in real-time le informazioni per l'adeguamento automatico delle configurazioni degli apparati cliente

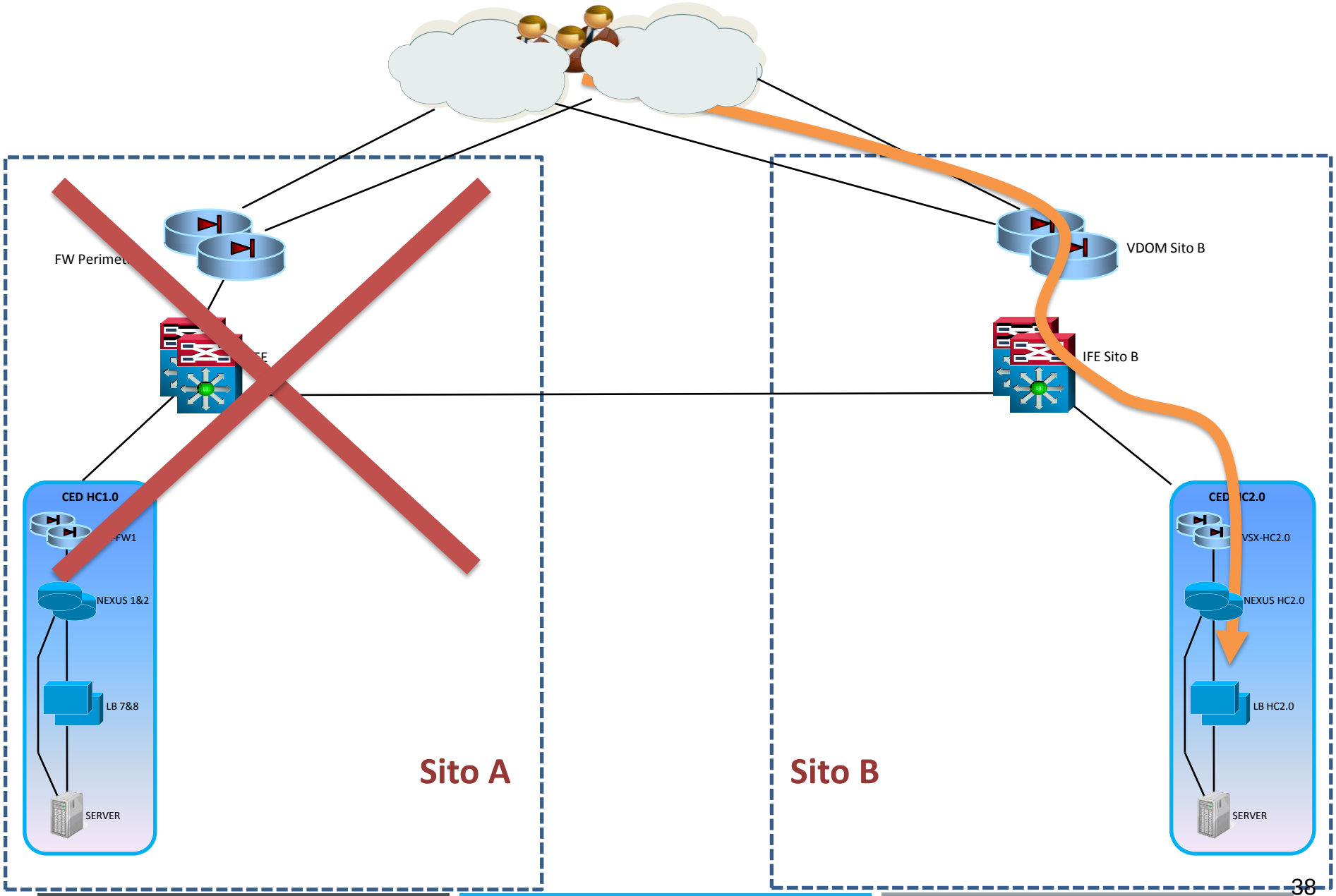
Erogazione del servizio in condizioni normali



Erogazione del servizio da Sito B



Erogazione del servizio da Sito B in caso di Disastro

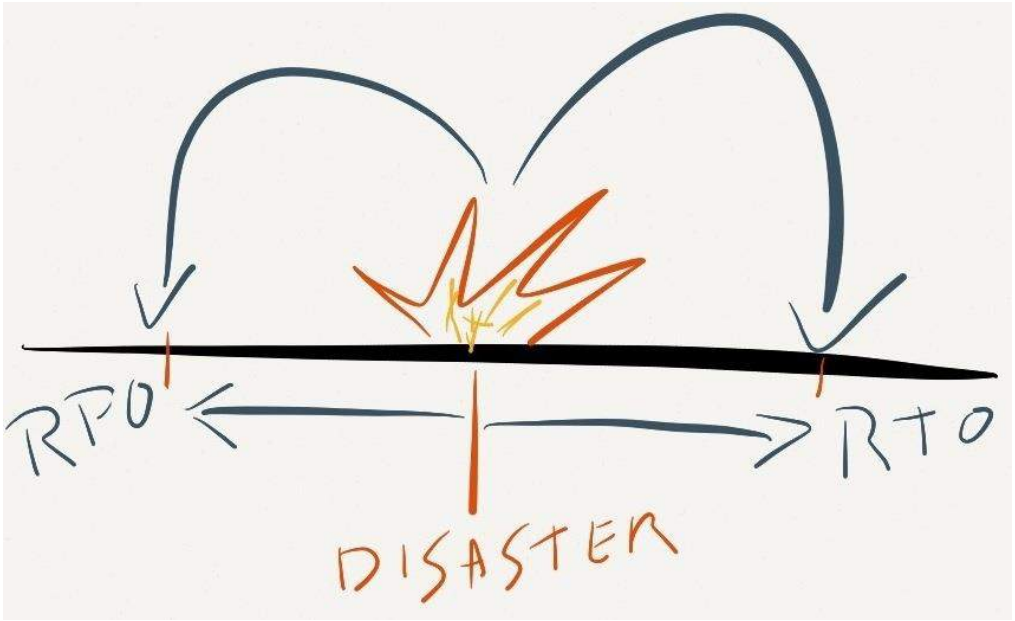


Erogazione del servizio da Sito B in caso di Disastro

Due parametri fondamentali:

RPO: quanti dati ho perso?

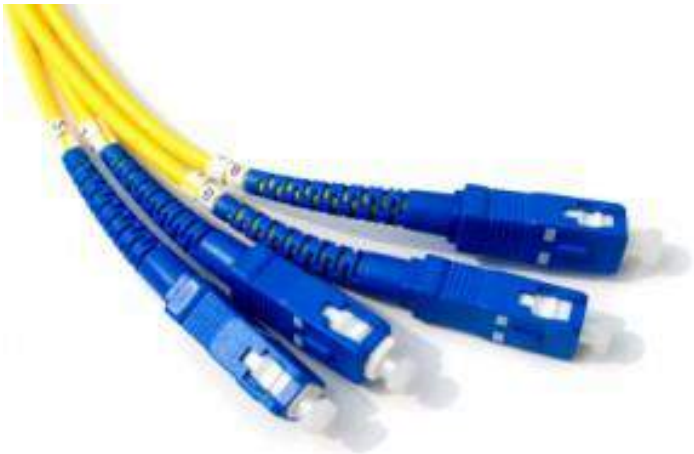
RTO: dopo quanto tempo ho di nuovo il servizio?



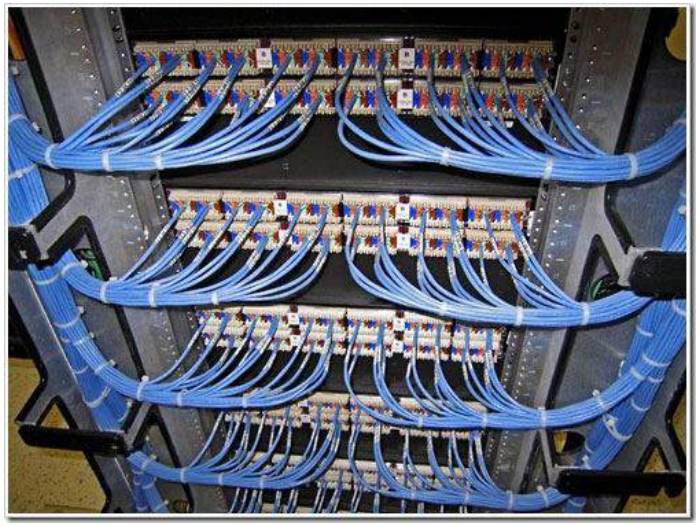
Cabling: il cablaggio strutturato

Nei Data Center vengono realizzati impianti di cablaggio strutturato, basati su cavi in rame di categoria 6 o superiore e connettori RJ-45 oppure in fibra ottica.
I cavi hanno una lunghezza massima di 90 m per il rame e 300 metri per la fibra.

Per ogni apparato IT da servire, vengono posati uno o più cavi in apposite canalizzazioni nelle pareti, nei controsoffitti o nei sottopavimenti dell'edificio, fino a raggiungere un armadio di distribuzione di piano (rack standard da 19 pollici) che ospita sia permutatori che apparati attivi (switch, router, server, dischi, etc.).



Cabling



Power & Cooling: Efficienza ed efficacia

Efficienza:

P.U.E.(Power Usage Effectivness)= Fattore di efficienza energetica

$$\textbf{P.U.E.} = \frac{\text{Potenza Elettrica Assorbita dall'intero impianto}}{\text{Potenza Elettrica impegnata dalle apparecchiature informatiche}}$$

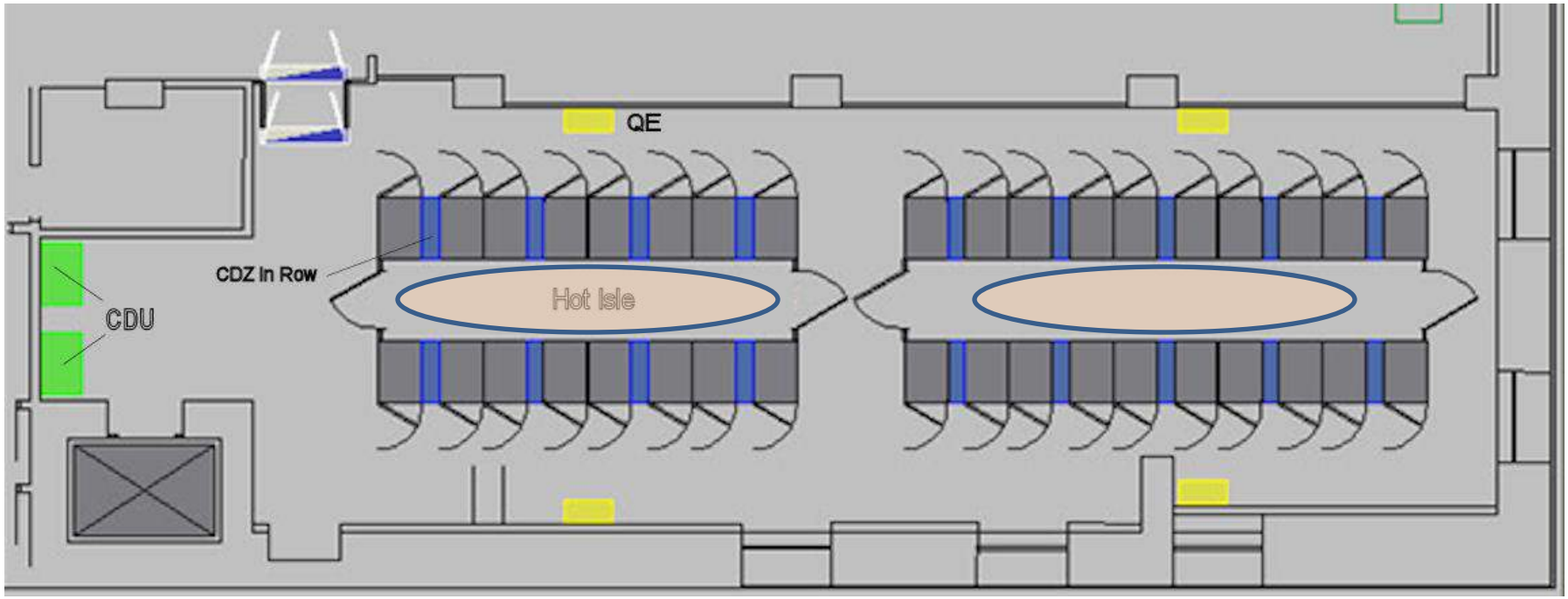
Valore	1,2	1,5	2	2,5	3
Livello	Molto efficiente	Efficiente	In Media	Inefficiente	Molto Inefficiente

Efficacia:

TIER:Fattore di Classificazione di disponibilità di servizio (Uptime Institute,Inc-USA)

Livello	TIER I	TIER II	TIER III	TIER IV
Disponibilità	99,671%	99,749%	99,982%	99,995%

I nuovi CED alta densità

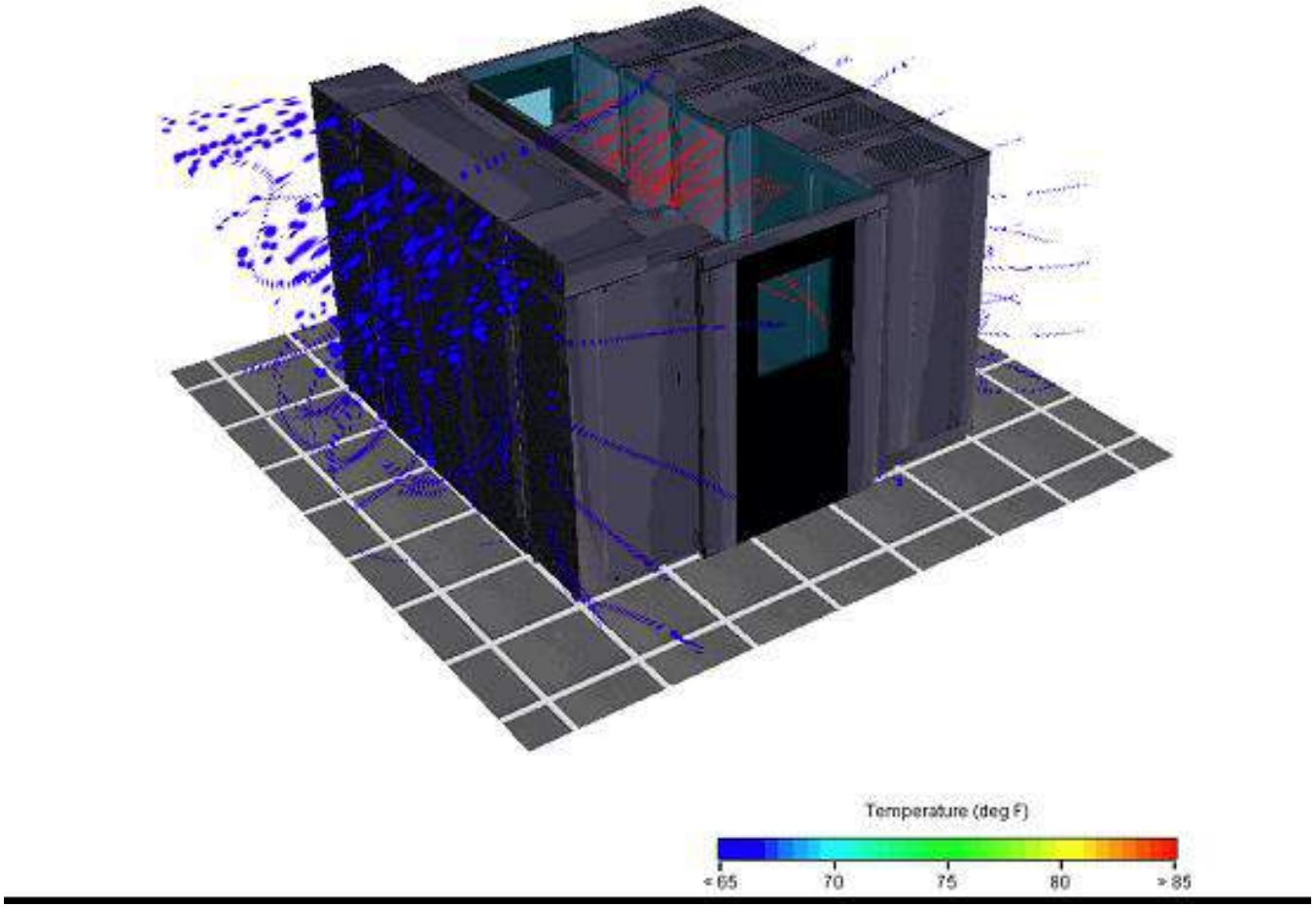


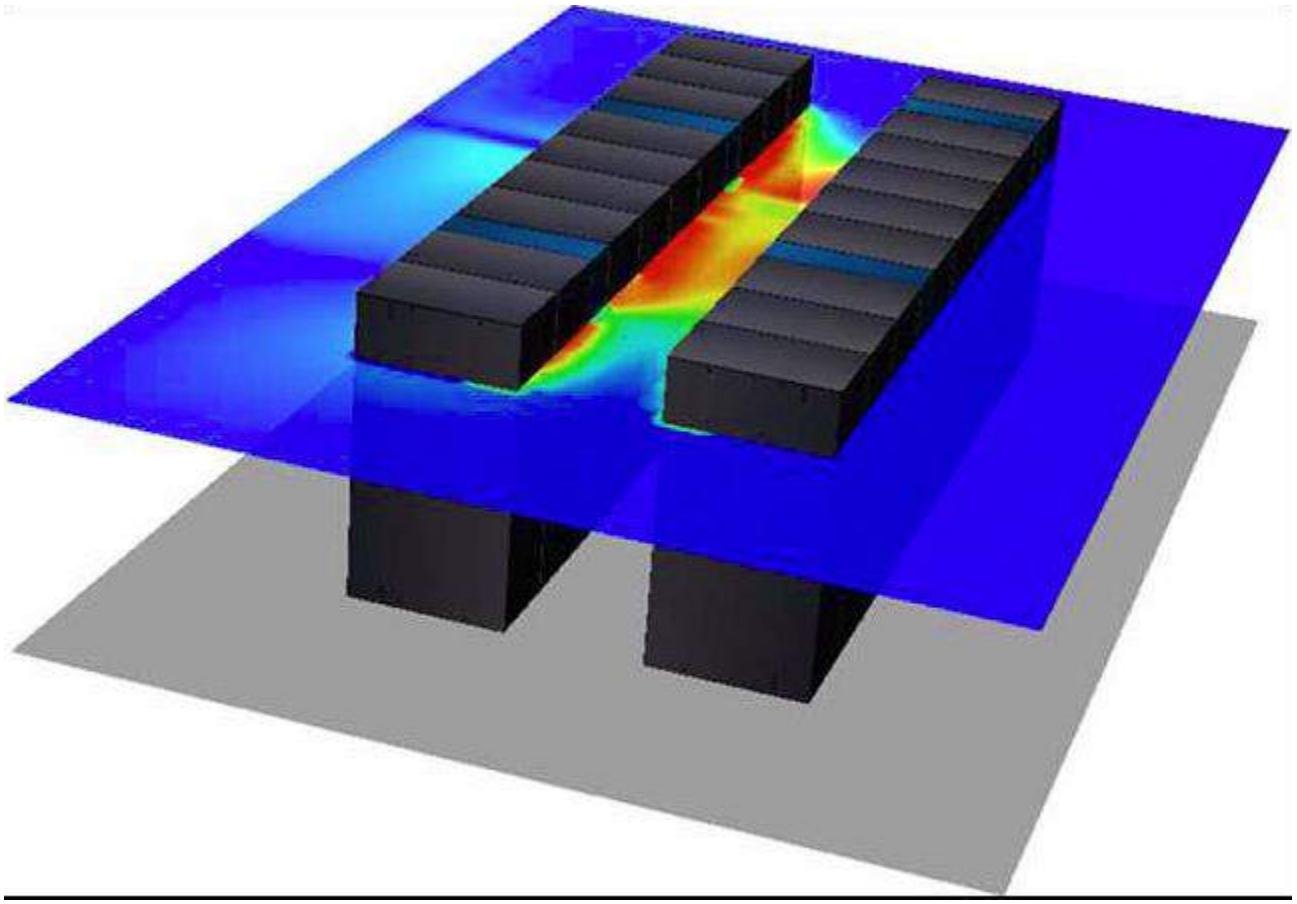
Superficie: 165 m^2
N° Rack: 36
CDZ: 10 x 22KW InRow
Pot. Elettrica: 4 x 160KW
Dens. Pot.: 4 KW/m^2

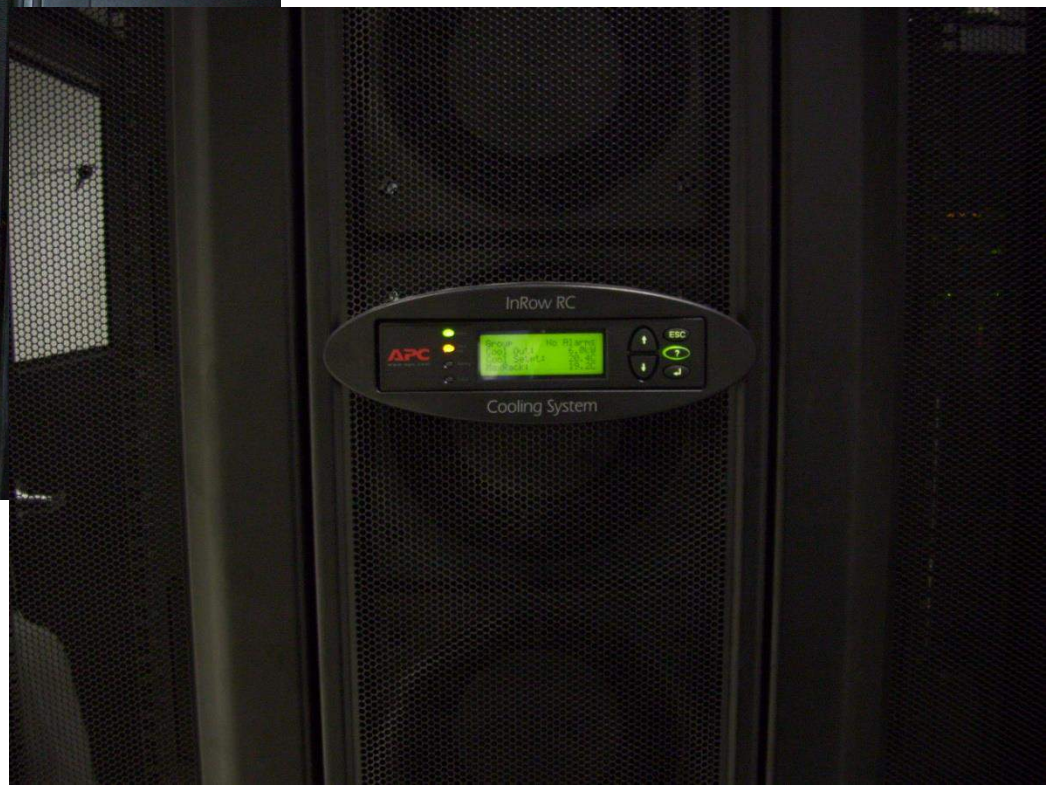
“IN ROW” Cooling System

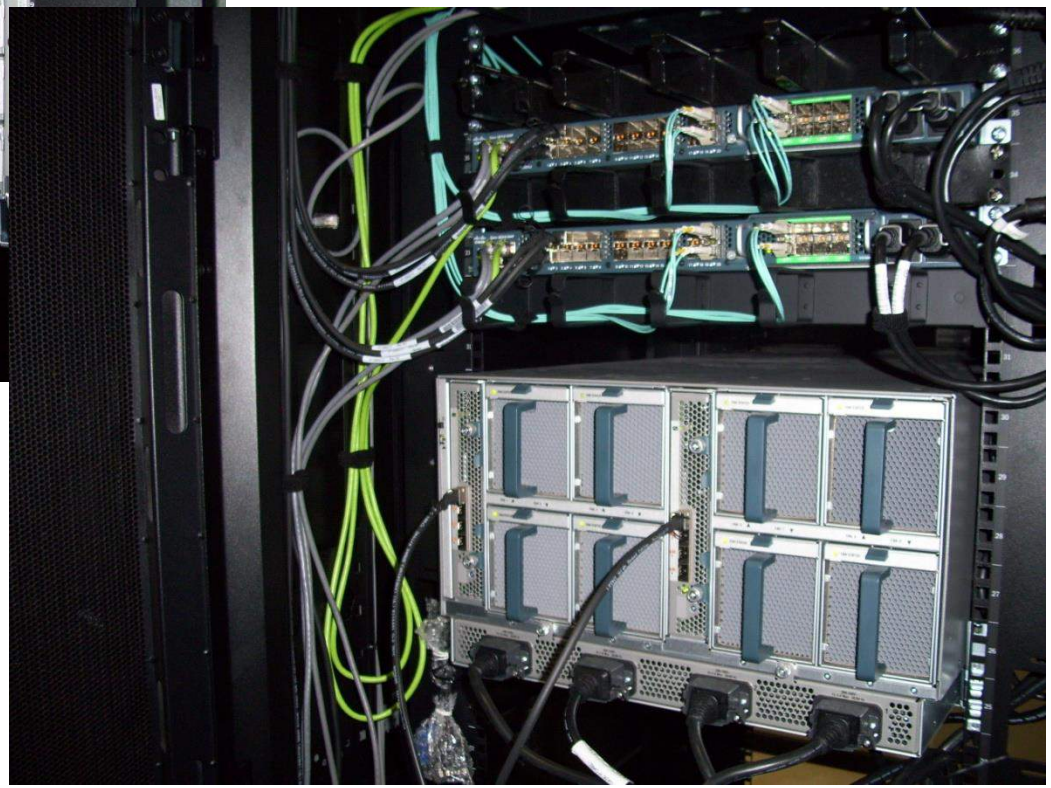
uses an innovative cooling systems with a uniform thermal distribution that allows to dissipate up to 30 KWatts per rack for a high density rack.

The adopted on-demand architecture that integrates Power, Cooling, Rack, management and services, allows the selection of standardized components to create a solution through modular and mobile configurations.

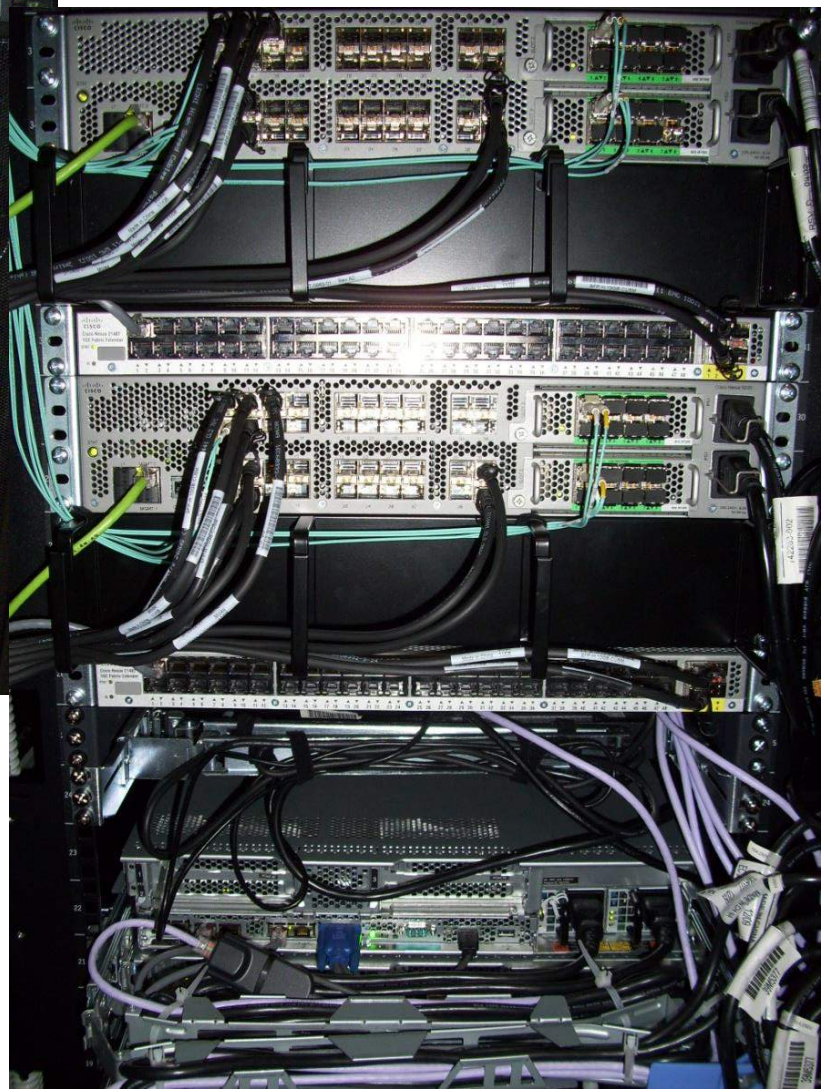

Temperature (deg F)
< 65
70
75
80
> 85




InRow RC
APC
ESC
Cooling System



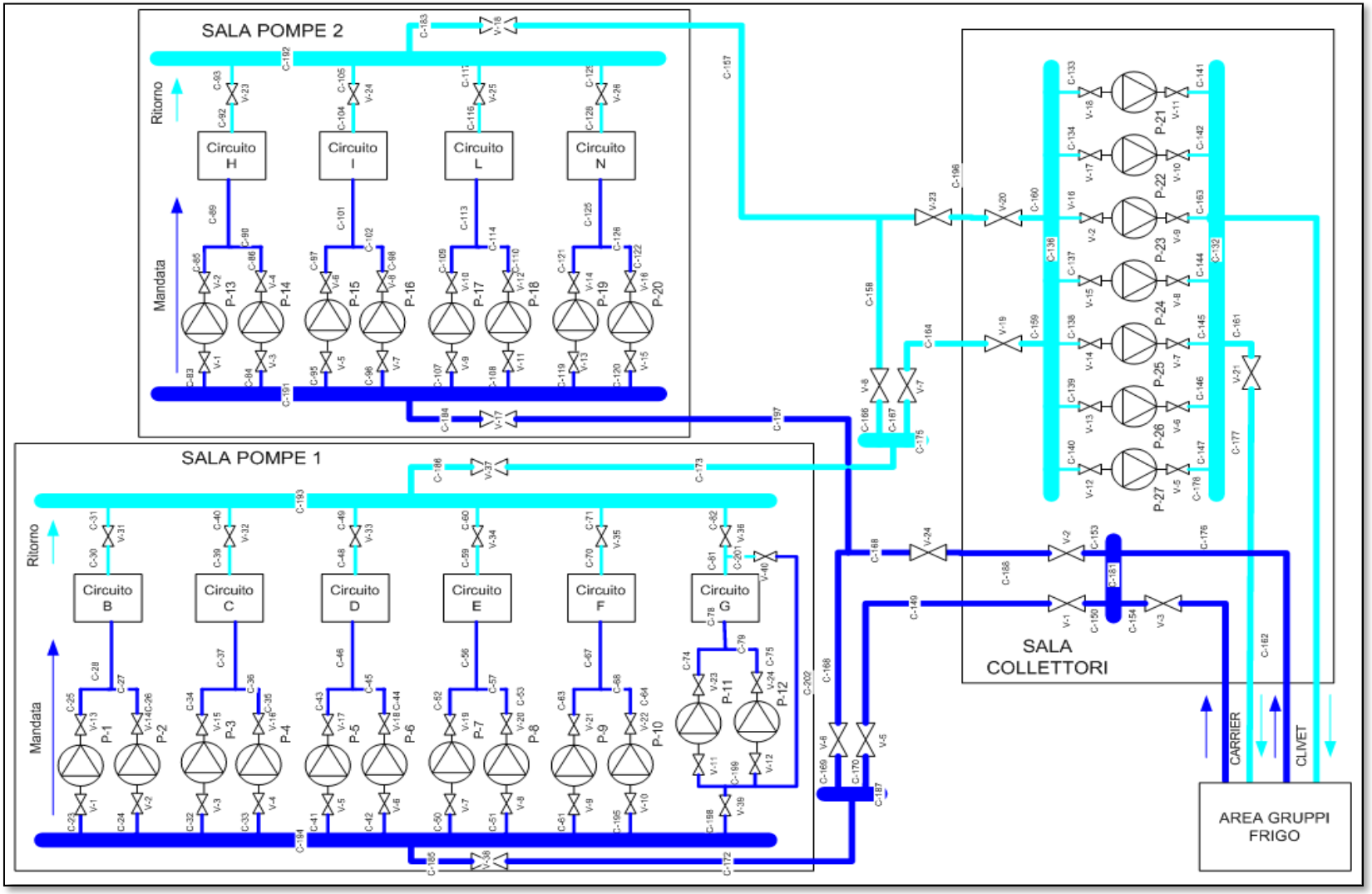

APC
Cooling System



Metodo tradizionali

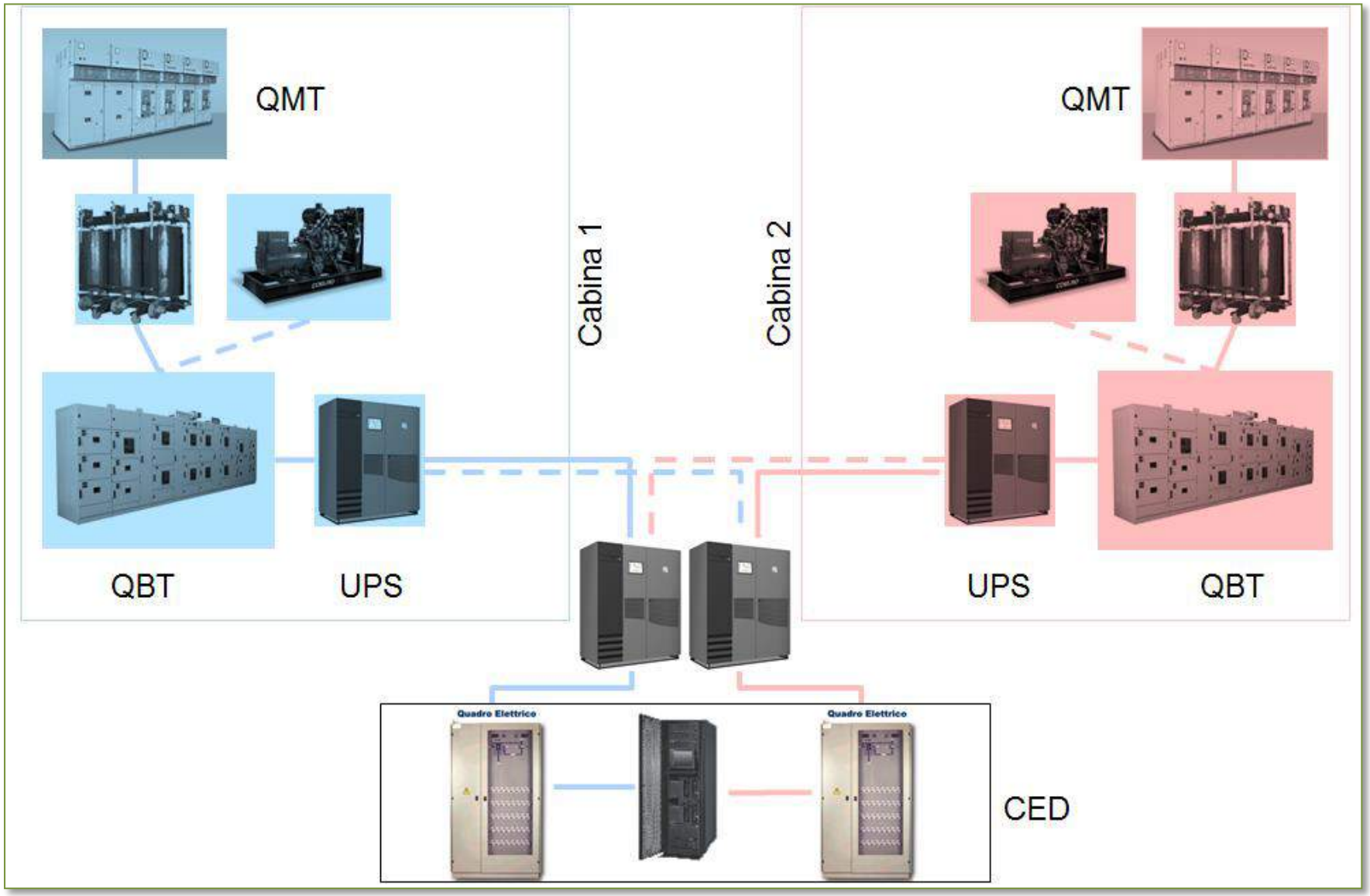
Data Center facilities

Circuiti di distribuzione del condizionamento



Data Center facilities

distribuzione elettrica



Impianti: conoscere per migliorare

- *Trend di contesto*
- *Trend di utilizzo*
- *Correlazioni tra condizioni di contesto e utilizzo dei componenti*
- *Correlazioni tra utilizzo dei componenti e consumi*

Analizzare

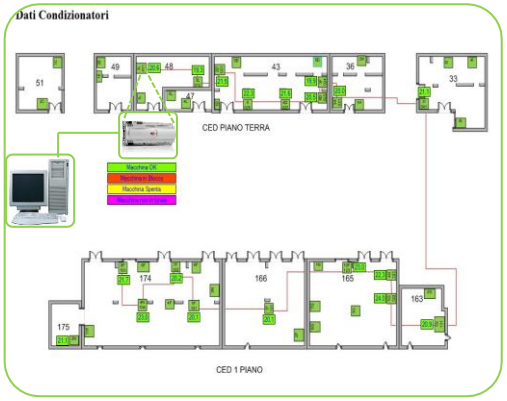
Intervenire

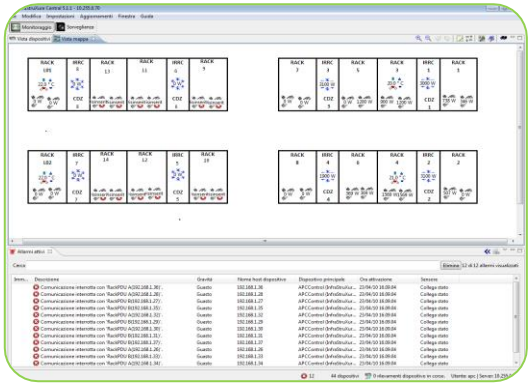
Conoscere

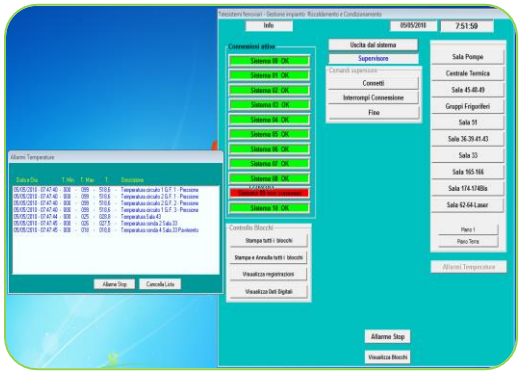
- *Regolazioni*
- *Manutenzioni*
- *Modifiche all'impianto*
- *Aggiornamento tecnologico*

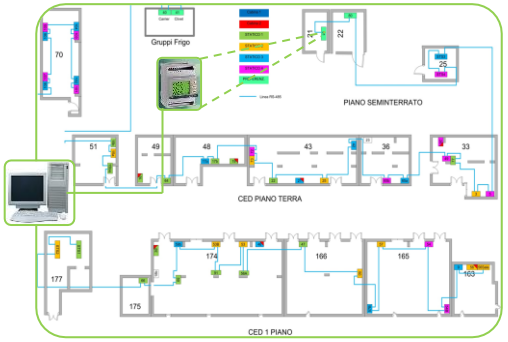
- *Caratteristiche dei componenti*
- *Profilo di efficienza dei componenti nel contesto reale*
- *Profilo di utilizzo dei componenti*
- *Condizioni di contesto*

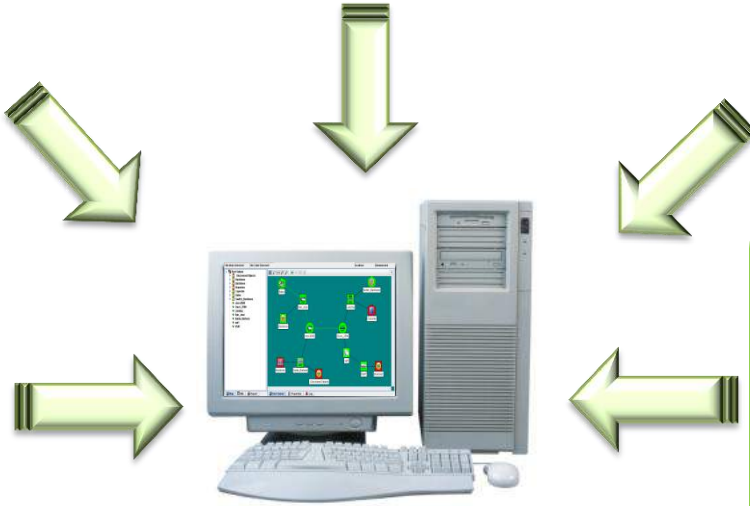
Impianti: sistemi di monitoraggio

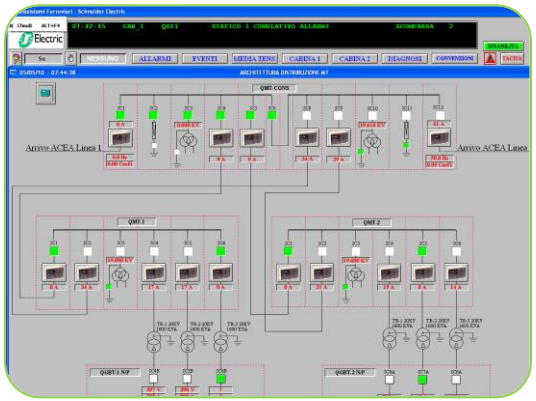












Gestione centralizzata