

Lamberto Celaia

Responsabile Servizio Elaborazione Dati

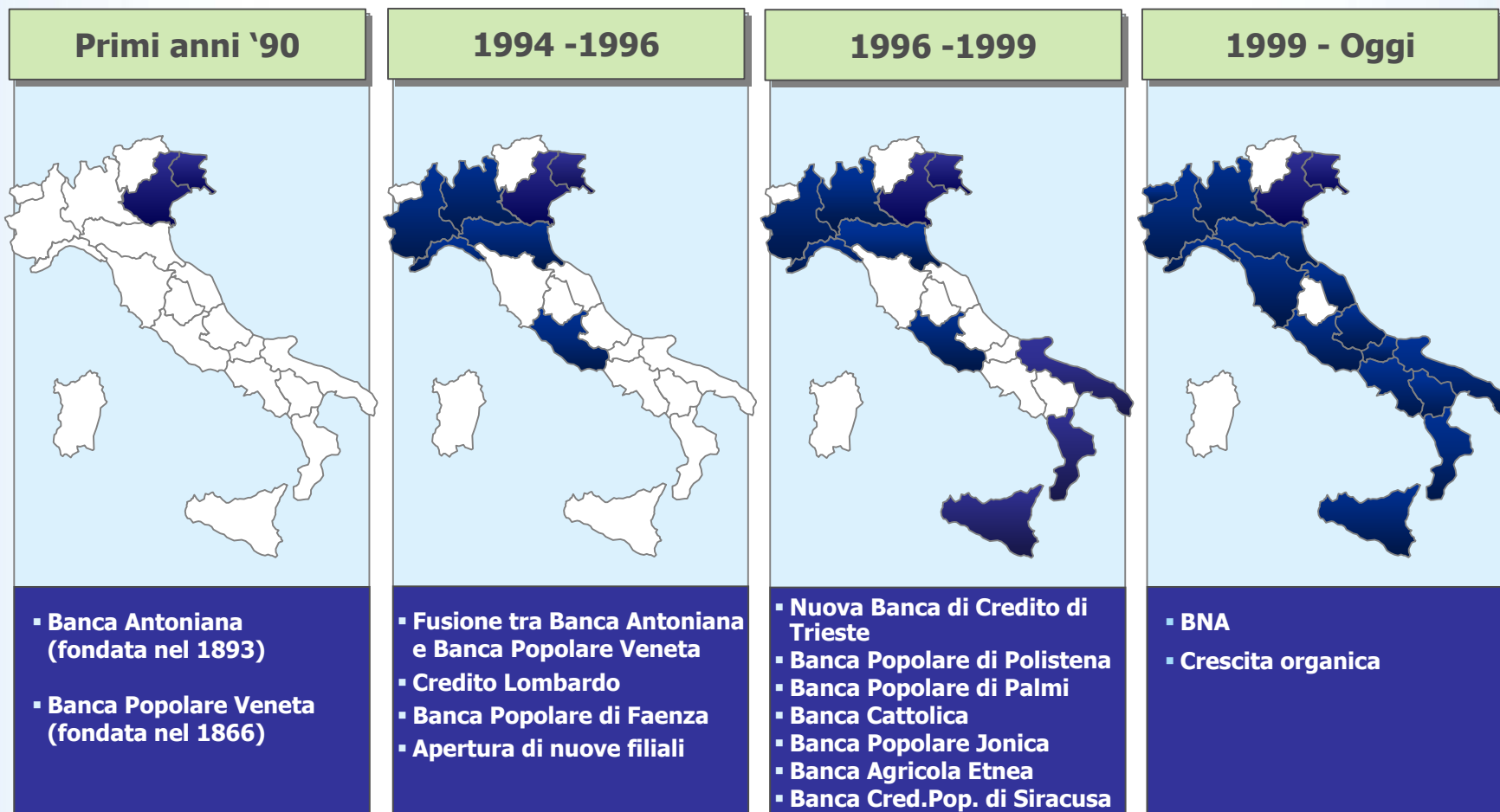
BUSINESS CONTINUITY

14 Febbraio 2003

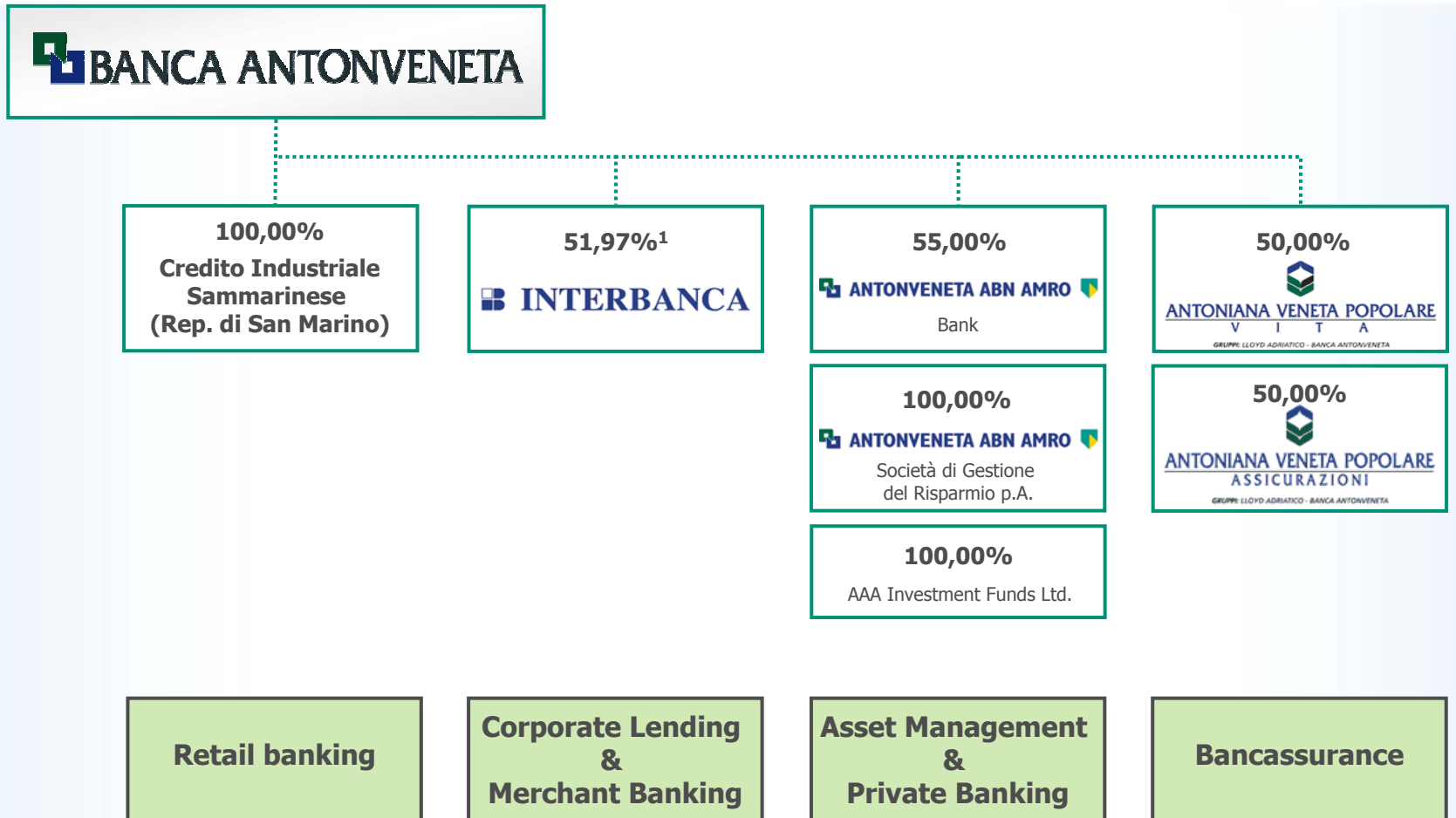
Da banca locale a banca nazionale mono-brand



Espansione della rete principalmente tramite acquisizioni



Struttura del Gruppo



¹ Il dato non tiene conto di una quota del 6,7% detenuta al servizio di un convertibile Banca Antonveneta in Interbanca e di una quota del 6% detenuta al servizio del warrant Interbanca.



BUSINESS CONTINUITY

Assicurare l'erogazione dei servizi alla clientela anche a fronte di malfunzionamenti (eventi disastrosi e non) presso le infrastrutture ICT



STUDIO PRELIMINARE

Linee di indirizzo:

- **Coerenza con le strategie di business della Banca**
- **Elevata disponibilità (ripristino del servizio in tempi brevi)**
- **Affidabilità elevata in emergenza**
- **Onerosità gestionale limitata**
- **Impatto organizzativo sostenibile**
- **Attenzione ai costi**



STUDIO PRELIMINARE

Perimetro di azione:

- **Ambiente mainframe**
- **Ambiente open**
- **Rete trasmissione dati :**
 - Filiali
 - Direzione Centrale
 - Enti esterni



AMBIENTE MAINFRAME

Linee di intervento:

- Ottimizzare l'esistente
- Fronteggiare il disastro



▪OTTIMIZZARE L'ESISTENTE



OTTIMIZZARE L'ESISTENTE

Interventi:

APPLICAZIONI DI FRONT-OFFICE E BACK-OFFICE

- CONSEGUIRE *ALTA AFFIDABILITA'* PER IL 65% DELLE TRANSAZIONI CON LA POSSIBILITA' DI ESTENSIONE FINO ALL' 80%
- ACCRESCERE LA *DISPONIBILITA'* MEDIANTE LA RIDUZIONE DEGLI IMPATTI DI RECOVERY/RESTART E LA MIGLIORE DISTRIBUZIONE DEI CARICHI APPLICATIVI

APPLICAZIONI DI INTERNET BANKING su piattaforma MAINFRAME WEBSHERE - CICS

- AUMENTARE L' *AFFIDABILITA'* ATTRAVERSO LA RIMOZIONE DI SINGLE POINT OF FAILURE



OTTIMIZZARE L'ESISTENTE

Interventi:

INFRASTRUTTURA TECNOLOGICA HARDWARE - ELABORATORI E RISORSE STORAGE

- AUMENTARE L'*AFFIDABILITA'* MEDIANTE RIDUZIONE DELLE DIPENDENZE TRA COMPONENTI HARDWARE
- PROTEGGERE LA *DISPONIBILITA'* ATTUANDO POLITICHE MIRATE DI SICUREZZA PER LE RISORSE DEI SISTEMI ELABORATIVI



- **FRONTEGGIARE IL DISASTRO**



FRONTEGGIARE IL DISASTRO

Analisi delle alternative possibili

Valutazione su 5 aree :

- Tecnologie
- Organizzazione
- Applicazioni
- Utenti
- Costi



FRONTEGGIARE IL DISASTRO

SOLUZIONE SCELTA:

Backup a caldo presso un service esterno distante 12 Km:

- Gli archivi sono duplicati presso il Centro di backup e tutti gli aggiornamenti vengono riportati in modalità sincrona
- I collegamenti tra i due Centri sono realizzati con fibre ottiche e apparecchiature DWDM



FRONTEGGIARE IL DISASTRO

IL CENTRO DI DISASTER RECOVERY:

Apparati tutti dedicati

- Sistemi storage per la duplicazione sincrona dei dati
- Sistema di elaborazione in modalità "stand-by"
- Sistemi storage aggiuntivi per l'effettuazione delle prove
- Due prove l'anno in configurazione "piena"
- Collegamento ad alta velocità con il CED principale

PLUS DEL SERVIZIO:

- Crescita annuale per potenza elaborativa e storage contrattualmente garantita
- Adeguamento tecnologico (allineamento al CED primario)
- Ruolo tra i due Centri intercambiabile (bidirezionalità) per il ripristino del CED primario dopo un evento disastroso



AMBIENTE OPEN UNIX

- Consolidamento della base dati (Storage Area Network)
- Consolidamento degli Application Server
- Strutture di recovery a freddo presso il sito di back-up

AMBIENTE OPEN INTEL

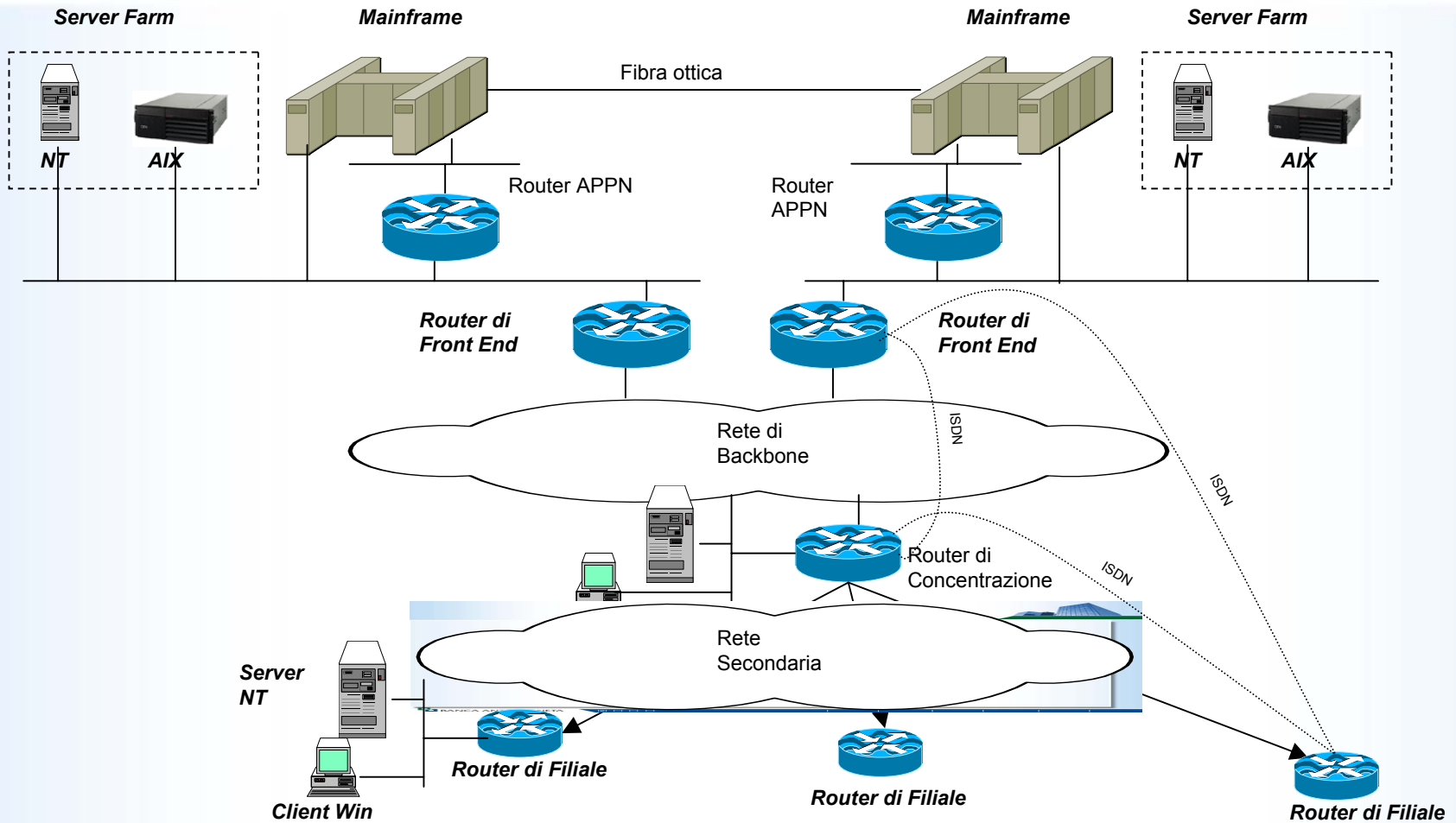
- Limitare al massimo le applicazioni "corporate" in questo ambiente
- Consolidamento della base dati (Storage Area Network)
- Scelte di recovery singole



RETE TRASMISSIONE DATI

- I sistemi di elaborazione raggiungono gli utenti finali attraverso due Data Center contemporaneamente attivi
- La rete è interna è basata su una architettura a due livelli con doppio livello di back up (ISDN)

Rete TD BAPV - schema logico





DA "ALTA DISPONIBILITA'" AD "ALTA AFFIDABILITA'"

Fase 1: mirroring delle base dati vitali in modalità sincrona

- garantire la ripartenza in tempi brevissimi in caso di evento disastroso evitando qualsiasi perdita di dati
- impostare l'architettura del sistema per le fasi successive

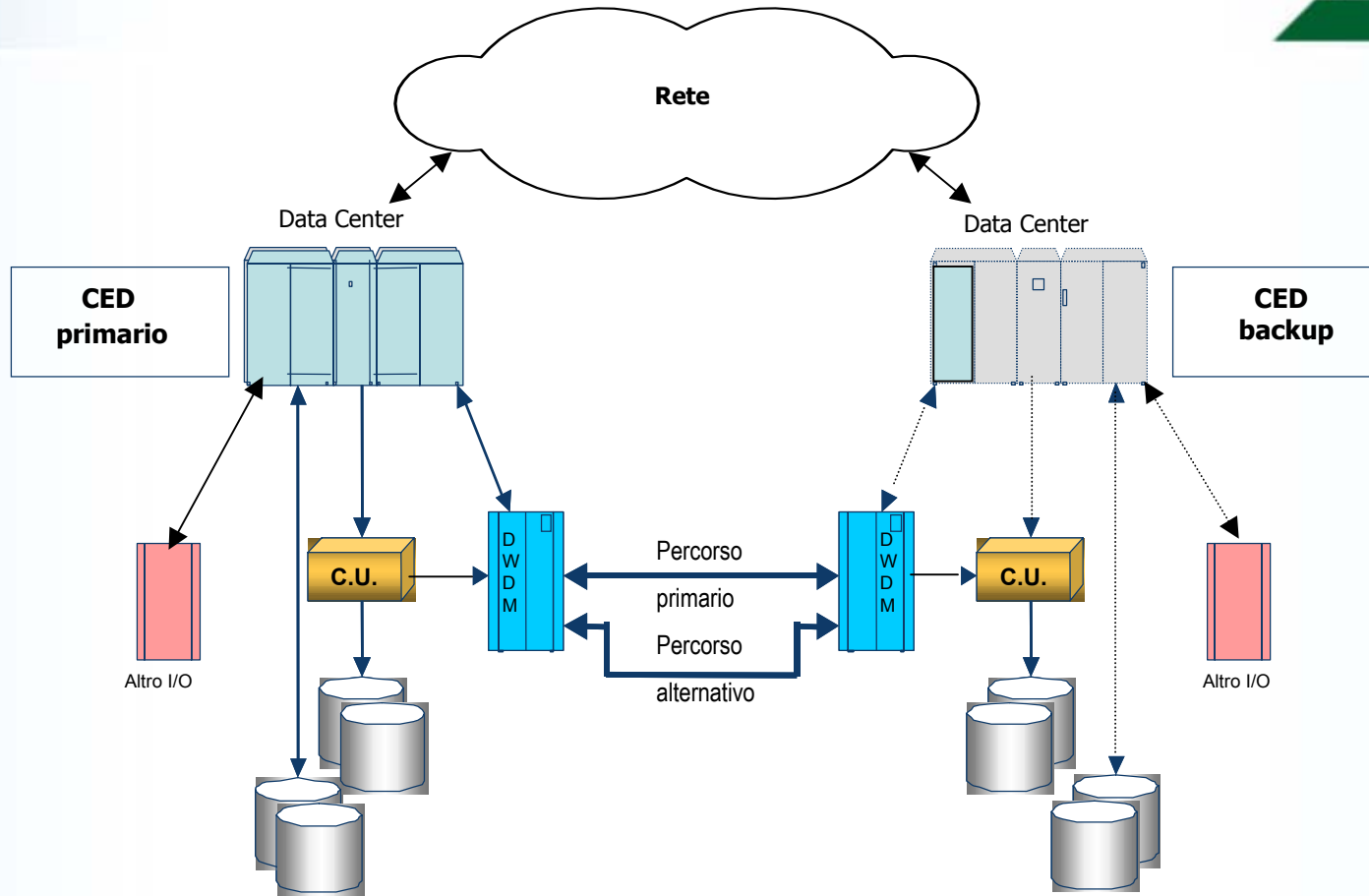
Fase 2: realizzazione di un GDPS (geographically dispersed parallel sysplex) tra ambienti non "mission critical"

- mettere a punto le procedure tecniche ed i processi operativi

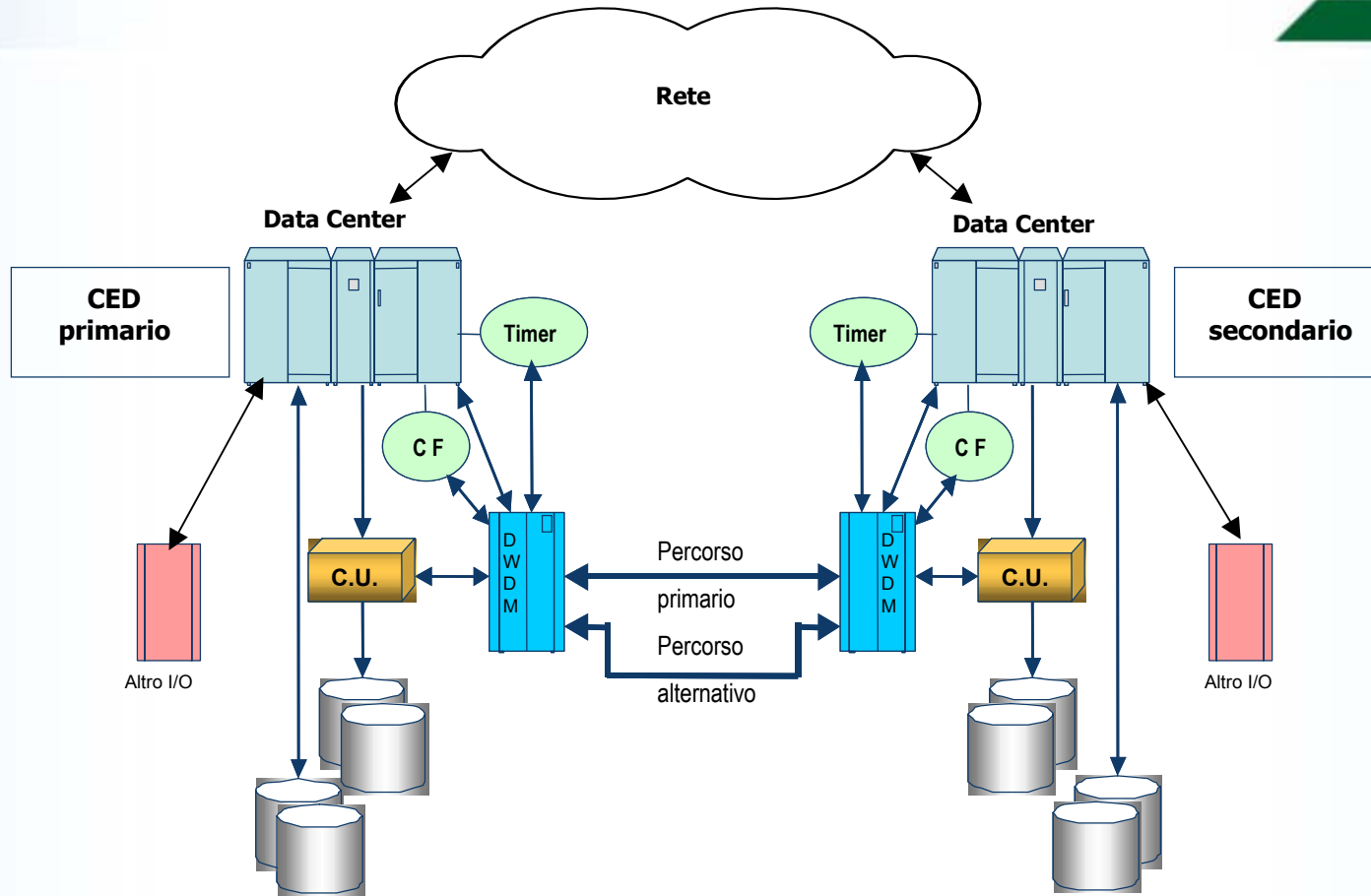
Fase 3: creazione di un ambiente unico ad Alta Affidabilità tra i due Centri

- garantire la continuità del servizio anche in caso di indisponibilità totale o parziale di qualsiasi componente del sistema in quanto i servizi possono essere erogati indifferentemente dai due Centri

Schema di riferimento logico fase 1



Schema di riferimento logico fase 2



Schema di riferimento logico fase 3

