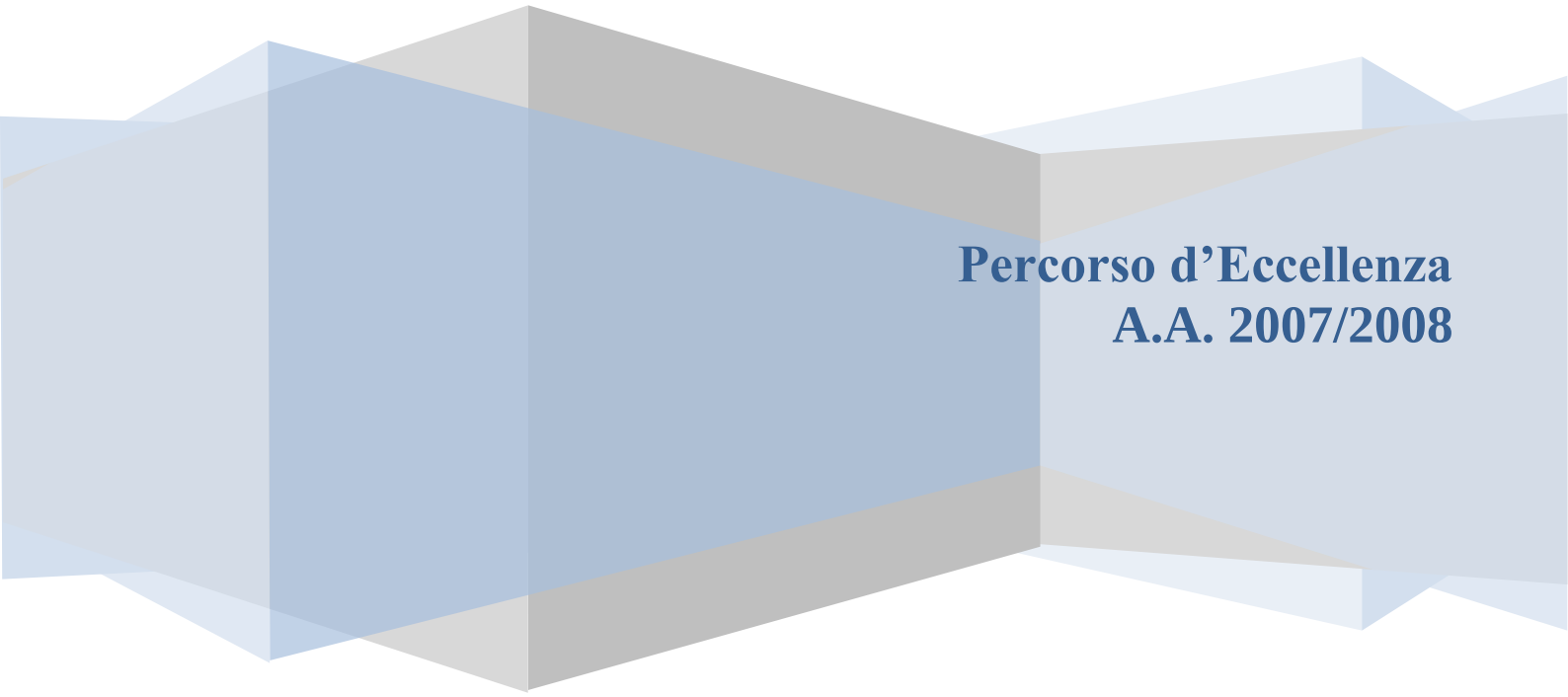
UNIVERSITÀ DI PISA

Corso di Laurea in Ingegneria Informatica

PROGETTO DI LABORATORIO DI RETI

Giovanni Accongiagioco
Simone Brienza
Daniele Giannetti



Percorso d'Eccellenza
A.A. 2007/2008

Sommario

1. Scenario di progetto

La WWAS (WorldWide Advanced Software) Spa, è un'azienda di sviluppo di software applicativo in rapida espansione. Per questo motivo ha programmato il trasferimento in nuovi locali delle tre sedi di Padova, Roma e Pisa.
Gli uffici logistici aziendali, dopo una prima analisi degli immobili, hanno già individuato gli uffici in cui si desidera siano forniti punti di connessione all'infrastruttura dati, e stabilito le caratteristiche di ciascun punto di presenza dell'infrastruttura dati (vedi planimetrie allegate). E' stato valutato che, prevalentemente, la direzione del traffico dati sarà interno alla singola sede o indirizzato fuori dalle sedi aziendali. Per quanto riguarda la componente geografica della rete, è stato deciso che le sedi di Pisa e Padova saranno connesse con link permanenti (fatturati secondo una tariffa flat) alla sede di Roma, secondo una topologia hub-and-spoke. Inoltre, per motivi di sicurezza, l'azienda ha stabilito di avere un unico punto di connessione con la rete Internet attraverso i servizi forniti da un operatore specializzato. In particolare, presso la sede di Roma sarà installato un router che fungerà da frontiera dell'intera rete aziendale verso l'esterno, a cui saranno connessi (attraverso link di tipo appropriato) i router locali alle singole sedi. Inoltre, allo scopo di fornire una soluzione di backup in caso di fallimento dei link principali, i router locali alle tre sedi saranno collegati tra loro con ulteriori link per i quali sarà attivato un contratto di servizio senza CIR e con una tariffa prevalentemente basata sul traffico che li attraversa. La topologia logica complessiva della rete geografica descritta sopra è rappresentata in Figura 0.1. Da un punto di vista produttivo l'azienda è organizzata secondo le funzioni aziendali: Direzione e Amministrazione (DA), Supporto Sistemi (SS), Marketing (M), Ricerca e Sviluppo (RS). Ciascuna funzione è presente in ciascuna delle sedi aziendali.
Il settore Ricerca e Sviluppo è strutturato, al suo interno, in gruppi di progetto che possono estendersi, ciascuno, sulle tre sedi e che hanno la durata dello specifico progetto a cui gli appartenenti al gruppo sono assegnati: una volta terminato il progetto, gli appartenenti al gruppo possono essere riassegnati a progetti diversi senza dover cambiare postazione di lavoro. La stessa cosa può accadere durante la durata di ciascun progetto in relazione alle esigenze di maggiore o minore apporto di lavoro della specifica fase progettuale.
Il settore Supporto Sistemi si occupa della gestione sistemistica della rete e, in generale, del sistema informatico aziendale.

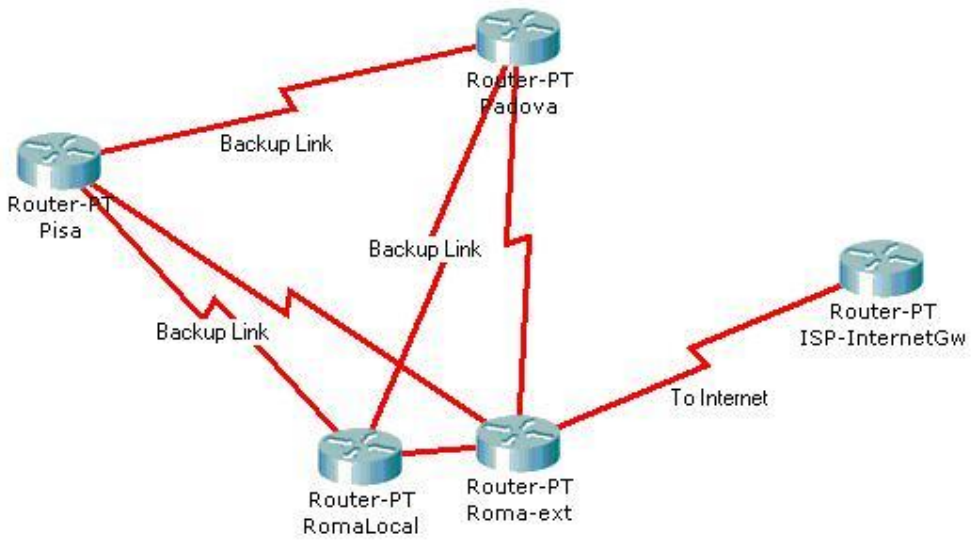


FIG 0.1 – Mappa Logica della nuova rete di WWAS

L'azienda ha quindi stabilito di commissionare ad un fornitore specializzato la realizzazione delle infrastrutture di rete degli immobili e la progettazione/messa a punto della loro interconnessione.

Sono stati fissati i seguenti requisiti generali:

1. la presenza su Internet dell'azienda sarà garantita da tre server web, due server per il DNS e due per il servizio di smistamento della posta con l'uso del protocollo SMTP: i server web saranno installati uno in ciascuna sede, i DNS a Roma e Pisa, gli SMTP a Pisa e Padova;
2. le comunicazioni esterne alla singola sede aziendale passeranno, di preferenza, attraverso *i link* principali (quelli fatturati flat) e, solo in caso di fallimento di uno di questi, attraverso le connessioni con tariffazione basata sul traffico (backup);
3. sulla rete è ammesso solo traffico appartenente ai protocolli dello *stack TCP/IP*.
4. per motivi di costo, il numero di indirizzi pubblici, per i server che devono essere raggiungibili da Internet e l'interconnessione a Internet, deve essere pari al minimo necessario;
5. il protocollo di routing utilizzato in tutta la rete aziendale è 1'OSPF.

Inoltre, le reti locali delle sedi aziendali dovranno soddisfare i requisiti che seguono:

a) ciascun punto di presenza dell'infrastruttura dovrà mettere a disposizione 4 prese di rete associate a cablaggio almeno in cat. 5e UTP. Salvo dove specificato diversamente, ogni stanza dovrà ospitare fino a 6 postazioni di lavoro, per ciascuna dovrà essere disponibile una banda minima di 1 Mbps fino ai server aziendali presenti nella medesima sede. Le stanze da cablare sono indicate dalla presenza, nella pianta dell'edificio, di un carattere ‘1’ cerchiato e/o di una lettera alfabetica; quando presente, a ciascuna lettera alfabetica corrisponde una sola postazione di lavoro. Le stanze destinate ad ospitare i server, due per ciascuna sede scelte tra quelle individuate sopra, dovranno essere in grado di ospitare fino a 24 macchine per stanza. I server ospitati in queste stanze saranno di due tipi: *enterprise server* (fino a un massimo di 40, di cui uno con funzione di server POP) *e workgroup server* (fino a un massimo di 3 per ciascuno dei gruppi di lavoraldominio di sicurezza);
   l'insieme dei due tipi di server non supererà, comunque, le 48 unità.
b) si richiede alla struttura e all'organizzazione della rete dati di riprodurre la flessibilità dell'organizzazione aziendale permettendo di configurare, in modo flessibile, domini di sicurezza associati a ciascun settore aziendale e, per il settore Ricerca e Sviluppo a ciascun gruppo di progetto per il tempo della sua durata. Nel tempo, si ritiene che il numero di progetti RS contemporaneamente attivi possa variare tra 1 e il massimo di 3.
c) *Le macchine di ciascun dominio di sicurezza di ciascuna sede potranno accedere, senza limitazioni, a quelle dello stesso dominio di sicurezza nelle altre sedi. Le macchine del dominio di sicurezza SS potranno aprire connessioni con protocolli basati su TCP verso macchine di tutti gli altri domini (dispositivi di rete compresi). Solo le macchine del dominio DA potranno accedere a Internet.* Il protocollo UDP non deve, salvo giustificate eccezioni, oltrepassare i confini di ciascun dominio di sicurezza (att.ne: ricordare che i server DNS utilizzano la porta UDP/53 e quelli DHCP la porta UDP/67, mentre i client DHCP usano la porta UDP/68)
d) Le macchine che forniscono i servizi di posta elettronica e di presenza nel World Wide Web, dovranno essere accessibili alle macchine di tutti e quattro i domini (e da Internet), con il minimo livello di esposizione: ad esempio, i server di posta elettronica dovranno permettere di ricevere la posta indirizzata all'azienda (e spedire quella da essa originata, protocollo SMTP) ma non leggere la posta (protocollo POP) da una postazione all'esterno della rete aziendale.

Il vostro datore di lavoro (un'azienda che gestisce una infrastruttura di rete geografica diffusa sull'intero territorio nazionale) ha deciso di presentare un'offerta per la realizzazione della nuova rete di "WWAS SpA", e ve ne ha affidato la progettazione suddividendola nei task che seguono. In particolare ha assegnato all'intero progetto oltre 16.000 indirizzi IP nella rete 172.16.192.0/18 su cui applicare il subnetting (eventualmente con tecnica VLSM), chiedendovi di utilizzarli nel modo più efficiente possibile. A tal fine, considerare attentamente eventuali implicazioni della presenza di tre sedi, ed eventualmente stabilire un partizionamento preventivo, tra le tre sedi, dello spazio degli indirizzi.
Al fine di dimostrare il progetto proposto, è richiesto di produrre, usando il Packet Tracer, una simulazione della porzione di rete assegnata alla vostra responsabilità, nell'ipotesi che siano attivi due progetti RS.

2.1 Task A

Progettazione e realizzazione della rete della sede di Padova e della sua connessione con le reti delle altre due sedi e con la rete pubblica.

Sulla base delle indicazioni fornite nello scenario:

1. *Progettare l'infrastruttura fisica, con particolare riferimento al cablaggio verticale, della rete della sede di Padova*, necessaria al supporto delle funzionalità richieste, tenendo conto che:
    - le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x;
    - il backbone della rete **di sede** deve garantire tempi di interruzione della connessione non superiori al centinaio di secondi;
    - devono essere scelti i mezzi di cablaggio (rame o fibra) che permettono di soddisfare i requisiti funzionali e le buone norme di cablaggio ai costi più bassi (si ricordi che il cablaggio UTP ha costi molto minori di quello in fibra ma anche specifiche limitazioni: di lunghezza, di eventuali interferenze, ecc.);
    - il progetto deve essere realizzato nel rispetto degli standard TIA/EIA-568-A e TIA/EIA-569.

    Per quanto riguarda questo punto, si richiede che venga fornita la seguente documentazione di progetto:
    - collocazione dei punti di distribuzione della rete (MDF e IDF);
    - mappa logica e mappa fisica dettagliata dei percorsi del cablaggio verticale (tra xDF);

    Tutte le scelte di progetto dovranno essere adeguatamente giustificate.
2. *Progettare e descrivere la realizzazione delle funzionalità di switching e routing della rete* di cui sopra tenendo conto che le postazioni di lavoro (macchine client) che potranno appartenere al dominio DA sono **al massimo** 11, quelle che potranno appartenere al dominio M sono **al massimo** 4, quelle del dominio SS **al massimo** 7.
   Le scelte effettuate dovranno essere adeguatamente giustificate (in termini di costi, funzionalità, ecc.) e dovrà essere fornita tutta la documentazione del caso:
    - numero e tipo degli switch/router installati in ciascuna delle Distribution Facilities;
    - configurazione di uno degli switch, a scelta, a cui faccia capo almeno almeno una macchina per ciascuno dei domini di sicurezza descritti sopra.
    - configurazione di **tutti i router** di interesse per la gestione del traffico della sede di Padova.

Non è richiesta, ma non è vietata, la configurazione di dispositivi non appartenenti alla rete dell'azienda (ad esempio nodi FR utilizzati per implementare i link geografici).

2.2 Task B

Progettazione e realizzazione della rete della sede di Roma e della sua connessione con le reti delle altre due sedi e con la rete pubblica.

Sulla base delle indicazioni fornite nello scenario:

1. *Progettare l'infrastruttura fisica, con particolare riferimento al cablaggio verticale, della rete della sede di Roma***,** necessaria al supporto delle funzionalità richieste, tenendo conto che:
    - le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x;
    - il backbone della rete **di sede** deve garantire tempi di interruzione della connessione non superiori al centinaio di secondi;
    - devono essere scelti i mezzi di cablaggio (rame o fibra) che permettono di soddisfare i requisiti funzionali e le buone norme di cablaggio ai costi più bassi (si ricordi che il cablaggio UTP ha costi molto minori di quello in fibra ma anche specifiche limitazioni: di lunghezza, di eventuali interferenze, ecc.);
    - il progetto deve essere realizzato nel rispetto degli standard TIA/EIA-568-A e TIA/EIA-569.

    Per quanto riguarda questo punto, si richiede che venga fornita la seguente documentazione di progetto:
    - collocazione dei punti di distribuzione della rete (MDF e IDF);
    - mappa logica e mappa fisica dettagliata dei percorsi del cablaggio verticale (tra xDF);

    Tutte le scelte di progetto dovranno essere adeguatamente giustificate.
2. *Progettare e descrivere la realizzazione delle funzionalità di switching e routing della rete* di cui sopra tenendo conto che le postazioni di lavoro (macchine client) che potranno appartenere al dominio DA sono **al massimo** 27, quelle che potranno appartenere al dominio M sono **al massimo** 5, quelle del dominio SS **al massimo** 8.

    Le scelte effettuate dovranno essere adeguatamente giustificate (in termini di costi, funzionalità, ecc.) e dovrà essere fornita tutta la documentazione del caso:
    - numero e tipo degli switch/router installati in ciascuna delle Distribution Facilities;
    - configurazione di uno degli switch, a scelta, a cui faccia capo almeno almeno una macchina per ciascuno dei domini di sicurezza descritti sopra.
    - configurazione di **tutti i router** di interesse per la gestione del traffico della sede di Roma.

Non è richiesta, ma non è vietata, la configurazione di dispositivi non appartenenti alla rete dell'azienda (ad esempio nodi FR utilizzati per implementare i link geografici).

2.2 Task C

Progettazione e realizzazione della rete della sede di Pisa e della sua connessione con le reti delle altre due sedi e con la rete pubblica.

Sulla base delle indicazioni fornite nello scenario:

1. *Progettare l'infrastruttura fisica, con particolare riferimento al cablaggio verticale, della rete della sede di Pisa***,** necessaria al supporto delle funzionalità richieste, tenendo conto che:
    - le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x;
    - il backbone della rete **di sede** deve garantire tempi di interruzione della connessione non superiori al centinaio di secondi;
    - devono essere scelti i mezzi di cablaggio (rame o fibra) che permettono di soddisfare i requisiti funzionali e le buone norme di cablaggio ai costi più bassi (si ricordi che il cablaggio UTP ha costi molto minori di quello in fibra ma anche specifiche limitazioni: di lunghezza, di eventuali interferenze, ecc.);
    - il progetto deve essere realizzato nel rispetto degli standard TIA/EIA-568-A e TIA/EIA-569.

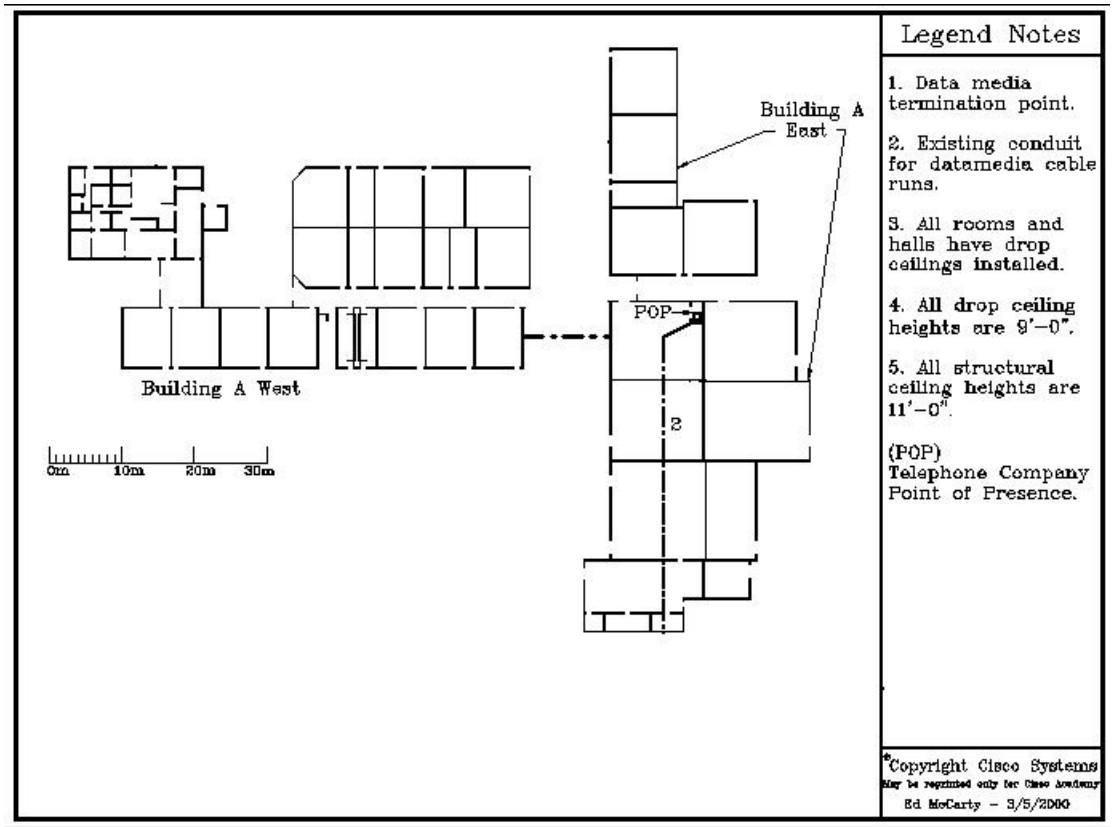
    Per quanto riguarda questo punto, si richiede che venga fornita la seguente documentazione di progetto:
    - collocazione dei punti di distribuzione della rete (MDF e IDF);
    - mappa logica e mappa fisica dettagliata dei percorsi del cablaggio verticale (tra xDF);

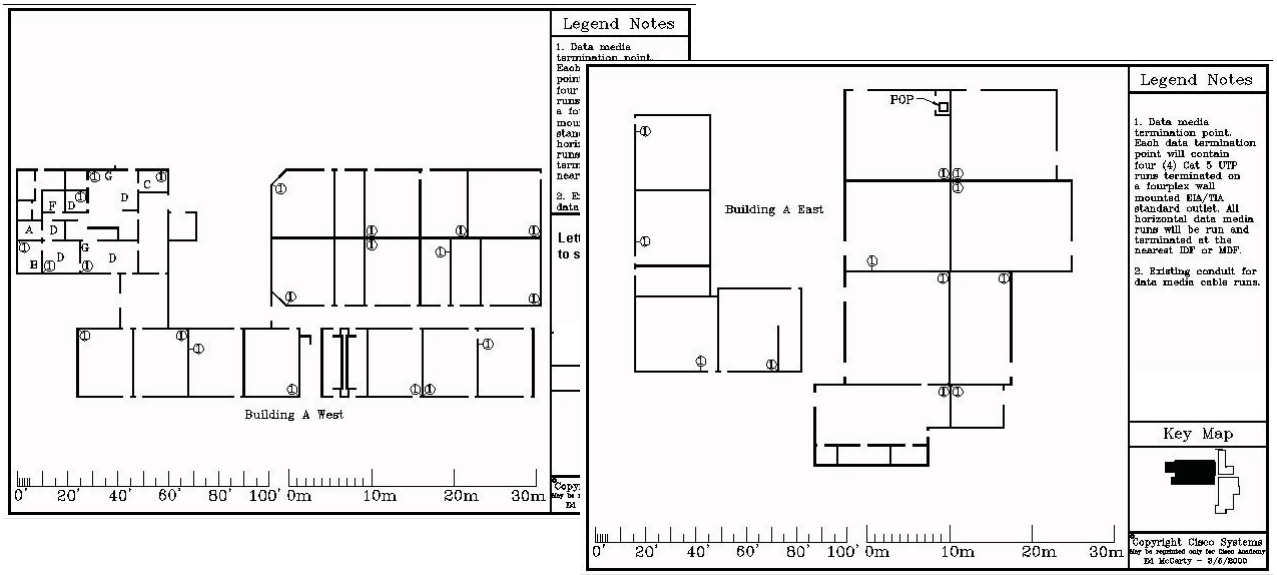
    Tutte le scelte di progetto dovranno essere adeguatamente giustificate.
2. *Progettare e descrivere la realizzazione delle funzionalità di switching e routing della rete* di cui sopra tenendo conto che le postazioni di lavoro (macchine client) che potranno appartenere al dominio DA sono **al massimo** 5, quelle che potranno appartenere al dominio M sono **al massimo** 3, quelle del dominio SS **al massimo** 2.

    Le scelte effettuate dovranno essere adeguatamente giustificate (in termini di costi, funzionalità, ecc.) e dovrà essere fornita tutta la documentazione del caso:
    - numero e tipo degli switch/router installati in ciascuna delle Distribution Facilities;
    - configurazione di uno degli switch, a scelta, a cui faccia capo almeno almeno una macchina per ciascuno dei domini di sicurezza descritti sopra.
    - configurazione di **tutti i router** di interesse per la gestione del traffico della sede di Pisa.

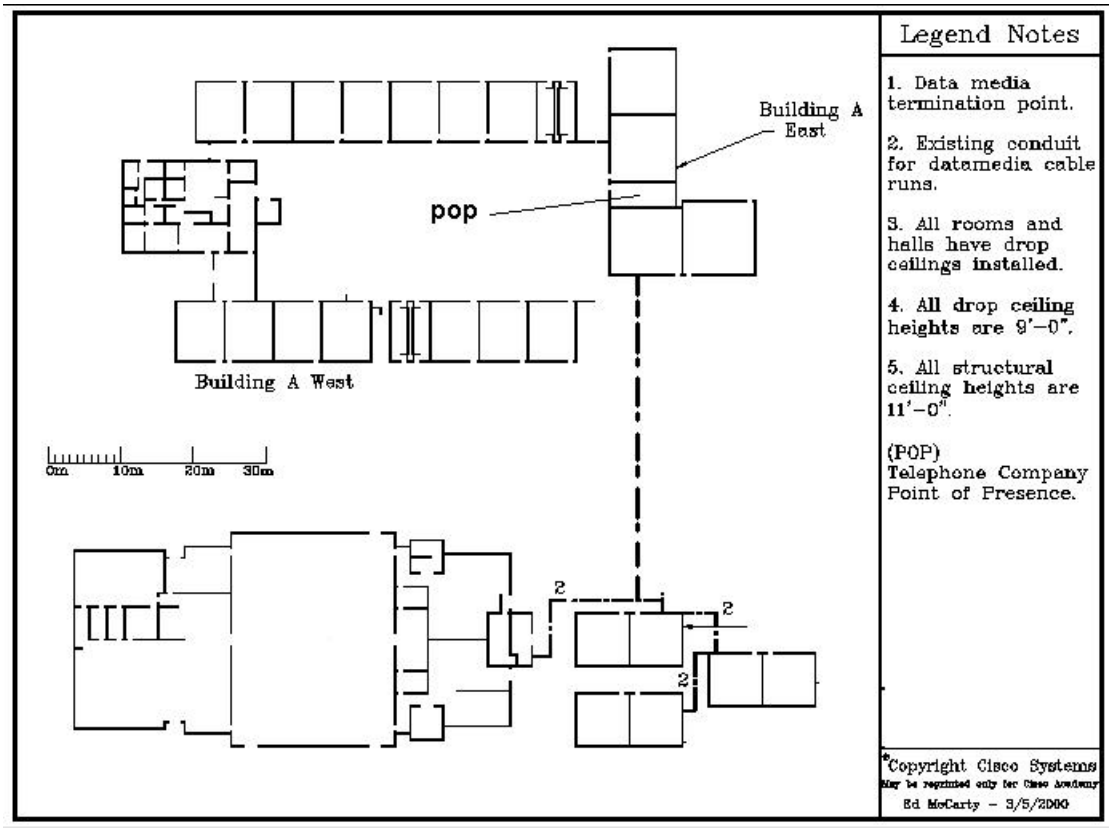
Non è richiesta, ma non è vietata, la configurazione di dispositivi non appartenenti alla rete dell'azienda (ad esempio nodi FR utilizzati per implementare i link geografici).

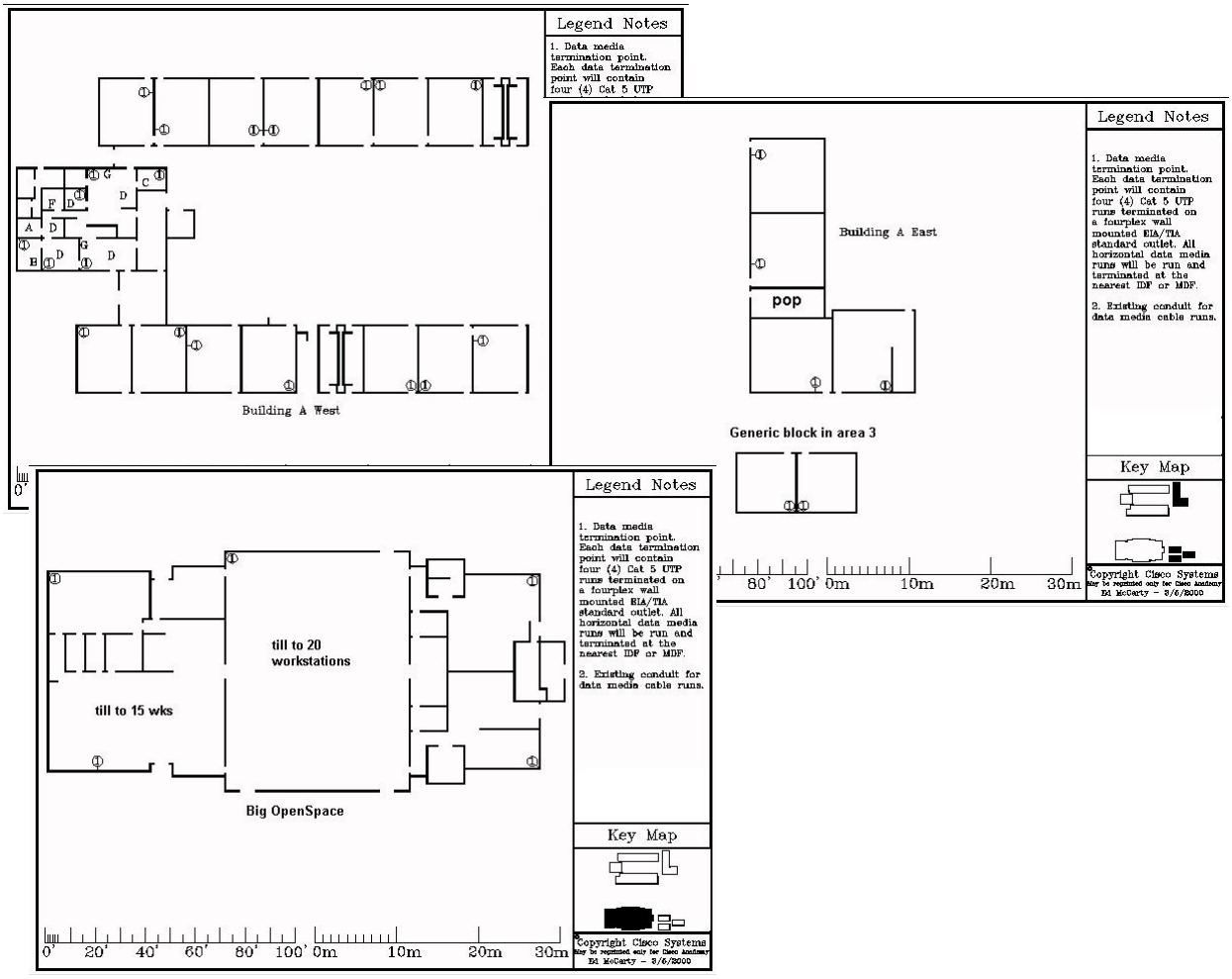
3.1 Padova


Legend Notes
1. Data media termination point.
2. Existing conduit for datamedia cable runs.
3. All rooms and halls have drop ceilings installed.
4. All drop ceiling heights are 9'-0".
5. All structural ceiling heights are 11'-0".
(POP)
Telephone Company Point of Presence.
Building A East
Building A West
POP
0m 10m 20m 30m
Copyright Cisco Systems
Ed McCarty - 3/5/2000

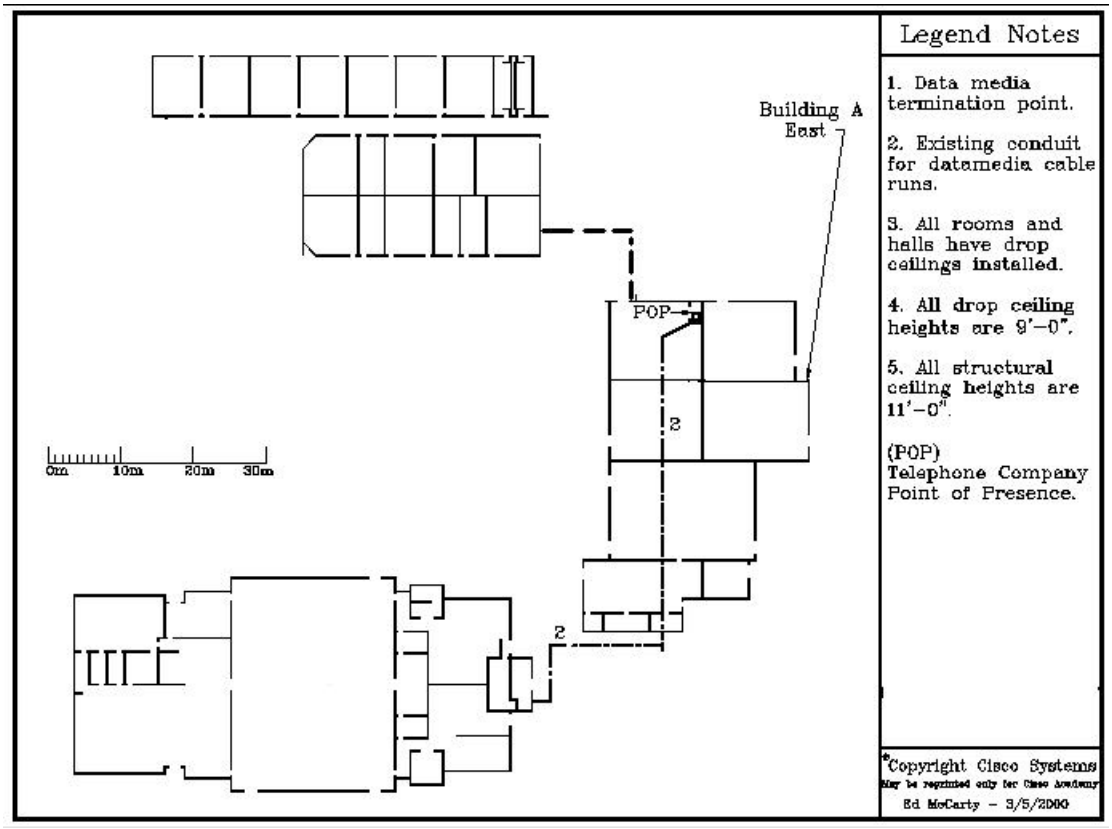

Legend Notes
Building A West
0' 20' 40' 60' 80' 100' 0m 10m 20m 30m
Legend Notes
1. Data media termination point. Each data termination point will contain four (4) Cat 5 UTP runs terminated on a fourplex wall mounted EIA/TIA standard outlet. All horizontal data media runs will be run and terminated at the nearest IDF or MDF.
2. Existing conduit for data media cable runs.
POP
Building A East
Key Map
0' 20' 40' 60' 80' 100' 0m 10m 20m 30m
Copyright Cisco Systems
Ed McCarty - 3/5/2000

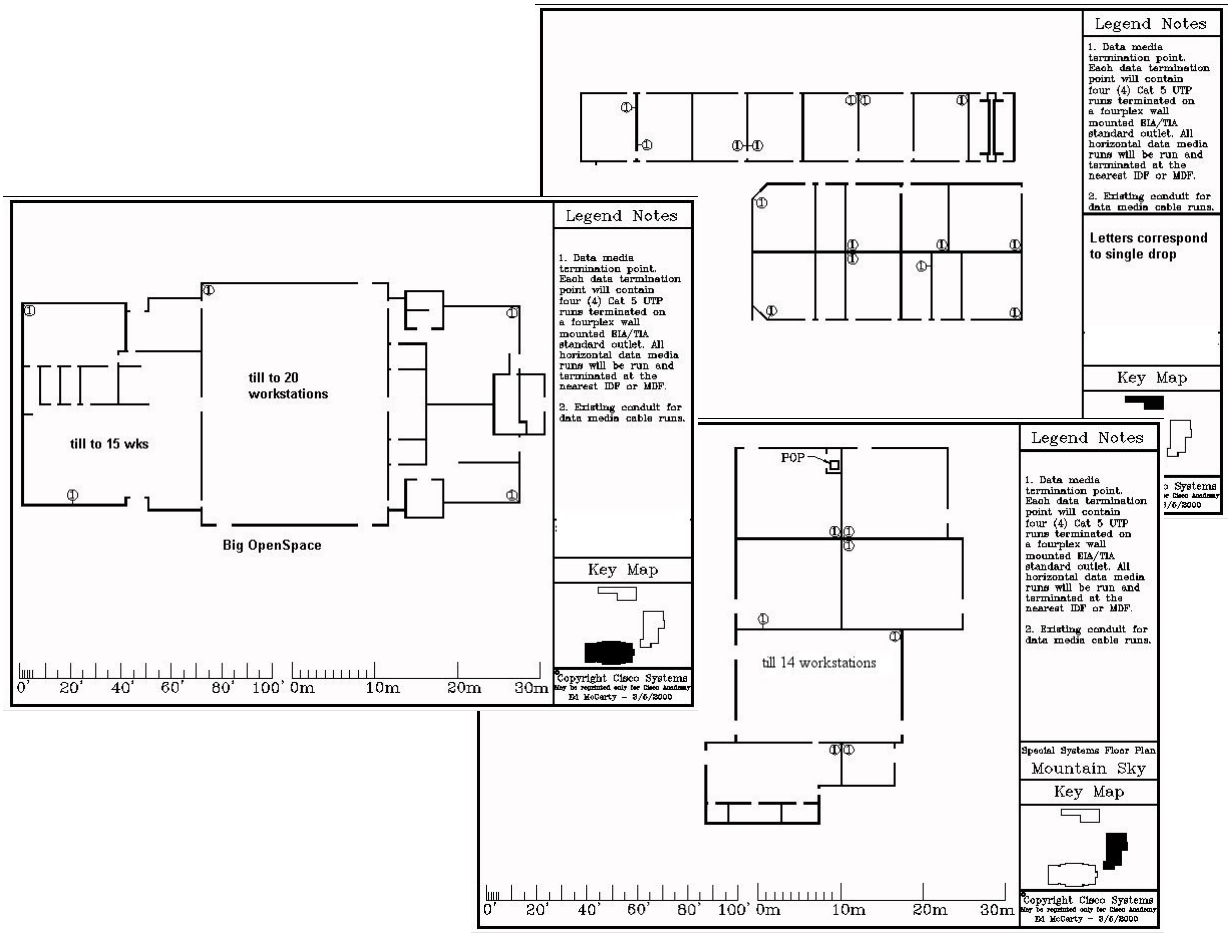
3.2 Roma


Legend Notes
1. Data media termination point.
2. Existing conduit for datamedia cable runs.
3. All rooms and halls have drop ceilings installed.
4. All drop ceiling heights are 9'-0".
5. All structural ceiling heights are 11'-0".
(POP) Telephone Company Point of Presence.
Building A East
pop
Building A West
0m 10m 20m 30m
2
2
2
Copyright Cisco Systems
May be reprinted only for Cisco Academy
Ed McCarty - 3/5/2000


Legend Notes
1. Data media termination point. Each data termination point will contain four (4) Cat 5 UTP
Building A West
Legend Notes
1. Data media termination point. Each data termination point will contain four (4) Cat 5 UTP runs terminated on a fourplex wall mounted EIA/TIA standard outlet. All horizontal data media runs will be run and terminated at the nearest IDF or MDF.
2. Existing conduit for data media cable runs.
Building A East
pop
Generic block in area 3
Key Map
80' 100' 0m 10m 20m 30m
Legend Notes
1. Data media termination point. Each data termination point will contain four (4) Cat 5 UTP runs terminated on a fourplex wall mounted EIA/TIA standard outlet. All horizontal data media runs will be run and terminated at the nearest IDF or MDF.
2. Existing conduit for data media cable runs.
till to 20 workstations
till to 15 wks
Big OpenSpace
Key Map
0' 20' 40' 60' 80' 100' 0m 10m 20m 30m
Copyright Cisco Systems
May be reprinted only for Cisco Academy
Ed McCarty - 3/6/2000

3.3 Pisa


Legend Notes
1. Data media termination point.
2. Existing conduit for datamedia cable runs.
3. All rooms and halls have drop ceilings installed.
4. All drop ceiling heights are 9'-0".
5. All structural ceiling heights are 11'-0".
(POP) Telephone Company Point of Presence.
Building A East
POP
0m 10m 20m 30m
Copyright Cisco Systems
Ed McCarty - 3/5/2000


Legend Notes
Letters correspond to single drop
Key Map
till to 20 workstations
till to 15 wks
Big OpenSpace
0' 20' 40' 60' 80' 100' 0m 10m 20m 30m
POP
till 14 workstations
Special Systems Floor Plan
Mountain Sky
Copyright Cisco Systems
Ed McCarty - 3/6/2000

1. Considerazioni su Indirizzi IP e Interfacciamento

Per quanto riguarda la parte a comune tra i progettisti, partiamo con alcune riflessioni di carattere generale: gli indirizzi IP forniti sono un gruppo di indirizzi privati, sono stati preventivamente suddivisi in 4 gruppi di indirizzi con una maschera /20, e 3 di questi gruppi sono stati assegnati alle 3 sedi.
La decisione è stata guidata dal fatto che, avendo a disposizione così tanti indirizzi per ciascuna sede, si ha la possibilità di una crescita locale enorme senza dover associare alle sedi dei gruppi di indirizzi disgiunti (e questo è un vantaggio per evitare di complicare la architettura logica della rete nel caso di una crescita locale alle sedi).
Il gruppo restante è stato suddiviso con tecnica VLSM al fine di fornire le subnet indispensabili per le interfacce dei collegamenti geografici. Per quanto riguarda il collegamento (tramite rete locale) tra il router Roma-ext e RomaLocal (deciso dalla WWAS), abbiamo deciso di rendere maggiormente robusta la struttura duplicando il collegamento e le interfacce necessarie: tali collegamenti saranno in rame, con cavo UTP cat5e, crossover (essendo le interfacce dei router delle semplici fastEthernet). Nonostante i collegamenti fastEthernet fra RomaLocal e Roma-ext siano locali alla sede di Roma, abbiamo deciso, per quanto riguarda gli indirizzi IP assegnati alle interfacce, di utilizzare due nuove sottoreti ottenute dal blocco di indirizzi rimasto libero: infatti tutta la sede di Roma è connessa direttamente al router RomaLocal, dunque, logicamente, Roma-ext funge da centro stella per la rete intersede in situazione di funzionamento senza guasti e sarebbe formalmente inadeguato assegnare ai link in esame IP provenienti dal blocco assegnato a Roma.
La decisione di utilizzare due collegamenti fastEthernet e non collegamenti a maggiore velocità è stata guidata da due considerazioni:

1) I collegamenti vengono utilizzati, se non si sono verificati dei fallimenti dei link geografici permanenti, solamente per far comunicare la sede di Roma con le altre sedi e con Internet, e dal momento che tipicamente i link geografici non hanno una velocità paragonabile a quella della fastEthernet allora due collegamenti di quel tipo dovrebbero essere sufficienti.
2) Nel caso in cui invece alcuni dei link di backup siano stati attivati a seguito di un fallimento di uno o più link permanenti allora sul collegamento tra Roma-ext e RomaLocal verrà deviato anche il traffico verso Internet delle altre sedi (eventualmente però alleviandolo del traffico verso la sede di Roma oppure diretto verso le altre sedi da Roma); ma, per le stesse riflessioni sopra, un doppio collegamento fastEthernet dovrebbe essere più che sufficiente.

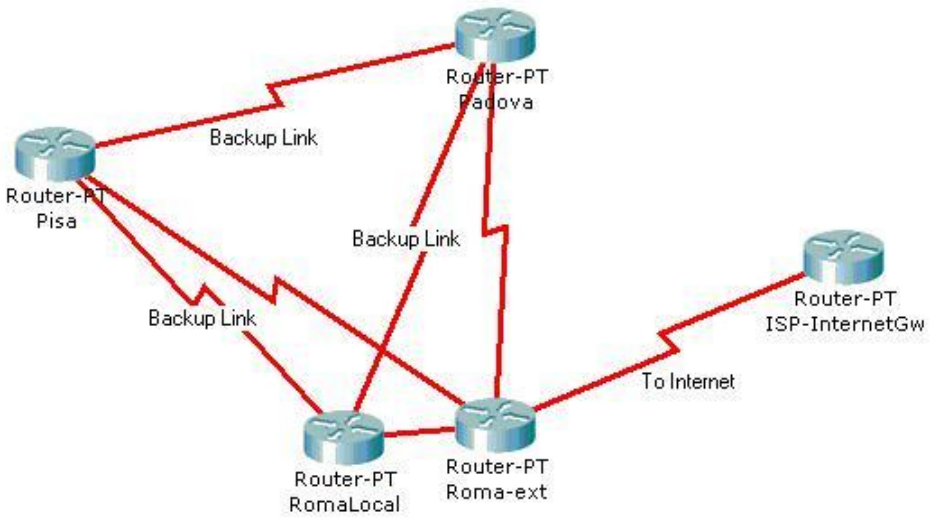


FIG 1.1

Osservando la mappa logica fornita dalla WWAS (fig. 1.1) si vede che i collegamenti (logici) di tipo geografico sono tutti punto-punto e (per le specifiche) vengono implementati con tecnologia Frame Relay. Per questioni di costo i tre collegamenti logici di backup in figura sono stati realizzati da un punto di vista fisico in modo diverso dalla topologia logica.
In ogni router interessato dai collegamenti di backup (tutti i router in figura escluso Roma-ext) è stata prevista una unica interfaccia fisica per realizzare entrambi i collegamenti di backup uscenti dal router, ad ogni interfaccia fisica sono state poi fatte corrispondere due sottointerfacce logiche per realizzare i due collegamenti. Ad ogni sottointerfaccia è stato associato l'appropriato DLCI per raggiungere il corrispettivo del collegamento punto-punto.
I router RomaLocal, Pisa e Padova hanno anche un collegamento interno verso le reti della sede: a tale scopo abbiamo previsto due interfacce fisiche gigabitEthernet che operino su fibra ottica, questa volta però la ridondanza non si è inserita per motivi di robustezza effettiva, ma per questioni di bilanciamento di carico.
La scelta di utilizzare delle interfacce capaci di supportare un gigabit di velocità e del cablaggio in fibra ottica deriva dal fatto che, secondo le specifiche, vi deve essere una banda disponibile pari a 1 Mbit per postazione fino ai server della sede in cui si trova[1].
Riassumendo, le interfacce dei router sono:

1. Router Pisa
    - 1 interfaccia fisica seriale per il link geografico permanente verso Roma-ext;
    - 1 interfaccia fisica seriale con due sottointerfacce per i link geografici di backup verso Padova e RomaLocal;
    - 2 interfacce fisiche gigabitEthernet per la rete della sede di Pisa.
2. Router Padova
    - 1 interfaccia fisica seriale per il link geografico permanente verso Roma-ext;
    - 1 interfaccia fisica seriale con due sottointerfacce per i link geografici di backup verso Pisa e RomaLocal;
    - 2 interfacce fisiche gigabitEthernet per la rete della sede di Padova.
3. Router RomaLocal
    - 1 interfaccia fisica seriale con due sottointerfacce per i link geografici di backup verso Pisa e Padova;
    - 2 interfacce fisiche fastEthernet verso Roma-ext;
    - 2 interfacce fisiche gigabitEthernet per la rete della sede di Roma.
4. Router Roma-ext
    - 1 interfaccia fisica seriale per il link geografico permanente verso Padova;
    - 1 interfaccia fisica seriale per il link geografico permanente verso Pisa;
    - 2 interfacce fisiche fastEthernet verso RomaLocal;
    - 1 interfaccia fisica seriale verso l'ISP.

Inoltre riportiamo la tabella di partizionamento degli indirizzi IP (che ovviamente deve essere completata con quella delle reti interne alle sedi, ma che al momento si esamina da un punto di vista "di alto livello"), Tabella 1.1.

[1] Si rimanda alle sezioni a seguire per maggiori dettagli su questo aspetto.

Sottorete	Dimensione	Indirizzo di Rete	Lunghezza Maschera	Maschera di Rete	Spazio di Indirizzamento
Roma	4094	172.16.192.0	/20	255.255.240.0	172.16.192.1 - 172.16.207.254
Padova	4094	172.16.208.0	/20	255.255.240.0	172.16.208.1 - 172.16.223.254
Pisa	4094	172.16.224.0	/20	255.255.240.0	172.16.224.1 - 172.16.239.254
Pisa_Roma-ext	2	172.16.240.0	/30	255.255.255.252	172.16.240.1 - 172.16.240.2
Padova_Roma-ext	2	172.16.240.4	/30	255.255.255.252	172.16.240.5 - 172.16.240.6
Pisa_Padova	2	172.16.240.8	/30	255.255.255.252	172.16.240.9 - 172.16.240.10
Pisa_RomaLocal	2	172.16.240.12	/30	255.255.255.252	172.16.240.13 - 172.16.240.14
Padova_RomaLocal	2	172.16.240.16	/30	255.255.255.252	172.16.240.17 - 172.16.240.18
RomaLocal_Roma-ext_a	2	172.16.240.20	/30	255.255.255.252	172.16.240.21 - 172.16.240.22
RomaLocal_Roma-ext_b	2	172.16.240.24	/30	255.255.255.252	172.16.240.25 - 172.16.240.26

TAB 1.1

2. Implementazione Frame Relay

Per quanto riguarda la scelta dei DLCI, abbiamo ovviamente previsto soltanto collegamenti Frame Relay di tipo punto-punto, inoltre il DLCI assegnato alla connessione logica per andare da un router al corrispettivo partner Frame Relay è il numero 100+O, dove O e' l'ultimo ottetto dell'indirizzo di rete della rete livello 3 interessata dal collegamento (che ovviamente ospita solo 2 indirizzi utili), ed e' lo stesso DLCI utilizzato dal router di destinazione per tornare al mittente (questo solo per semplicità).
Uno dei requisiti di progetto era quello di utilizzare i link di backup solamente in caso di fallimento dei link permanenti: questa funzionalità è stata implementata utilizzando il particolare tipo di calcolo che il protocollo di routing utilizzato (OSPF) esegue per valutare la metrica (il quale tiene conto della Bandwidth per valutare la convenienza di un collegamento). In pratica sono state assegnati in modo convenzionale alle interfacce e sottointerfacce dei link geografici delle Bandwidth tali da "guidare" il protocollo di routing verso la scelta dei giusti collegamenti (se disponibili): quelli con CIR e fatturati flat.

La topologia logica risultante è la seguente, dove la Bandwidth è stata scritta per chiarezza di disegno sul collegamento, intendendo che comunque è stata assegnata alle interfacce (o sottointerfacce) da entrambi i lati. Inoltre le connessioni Frame Relay di backup sono state disegnate come una "stella" attorno alla Frame Relay Cloud centrale nel disegno, ricordando però che in questa stella sono in realtà presenti 3 collegamenti punto-punto da un punto di vista logico, costruiti mediante un adeguato mapping dei DLCI sulle connessioni (fig. 1.2).

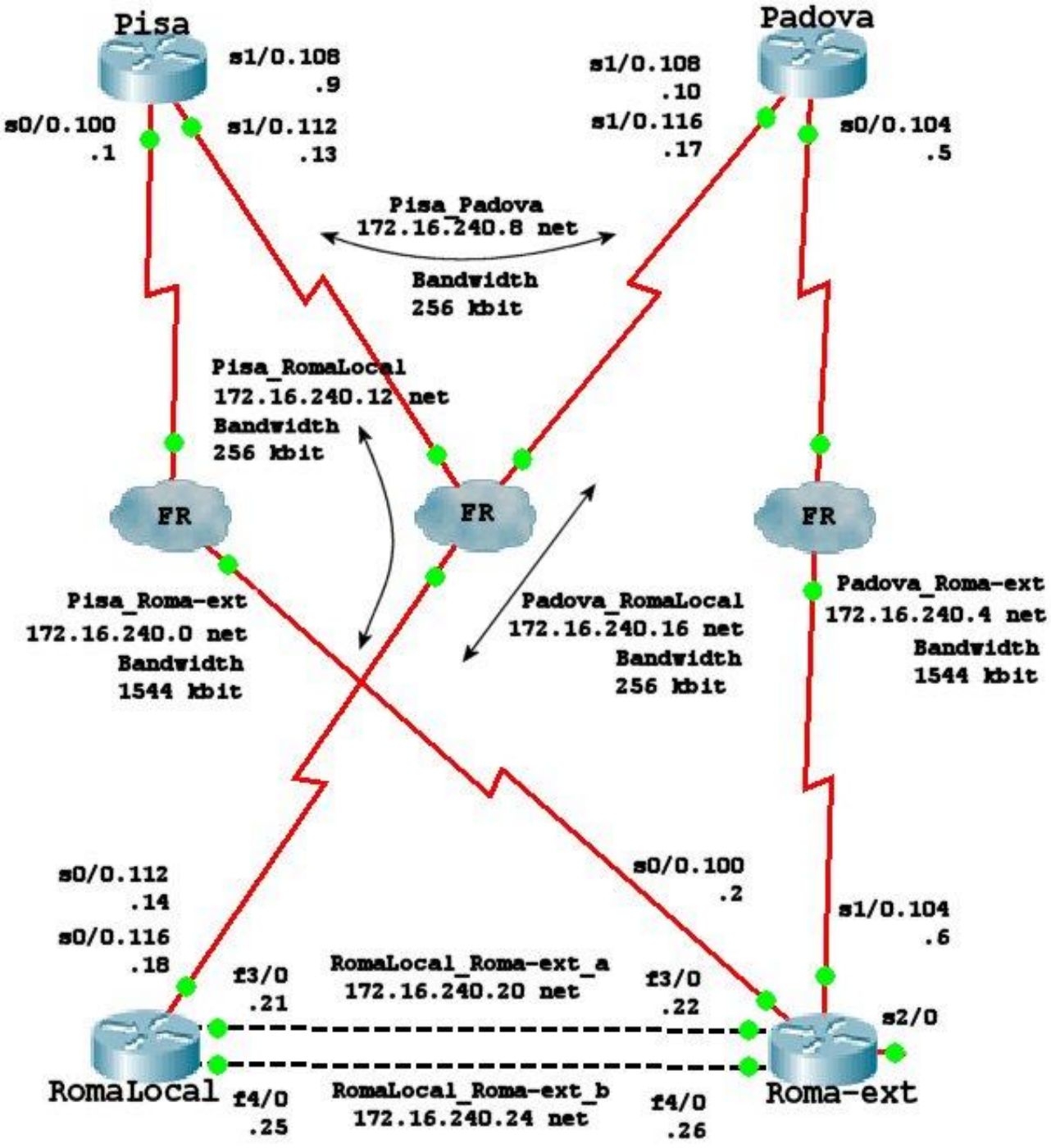


FIG 1.2 MAPPA LOGICA

I router RomaLocal, Padova e Pisa hanno due interfacce gigabitEthernet disponibili per la connessione alla rete delle rispettive sedi. All'interno di ogni sede sono presenti i 4 domini di sicurezza descritti nelle specifiche, tuttavia:

- Al dominio Ricerca e Sviluppo (RS) corrispondono in realtà da 1 a 3 sottodomini a seconda di quanti gruppi di progetto sono attivi ad un dato istante.
- Gli Enterprise Server si considerano facenti parte di un dominio di sicurezza separato, in questo modo si possono specificare delle regole di protezione apposite.
- I Server accessibili da Internet costituiscono anch'essi un dominio di sicurezza separato, in quanto necessitano di regole di protezione su misura, da ora in poi questi Server si indicheranno con il nome di Server globali (Global Server).
- I Workgroup Server invece, facendo capo ad una particolare funzione/gruppo di lavoro, si includono all'interno del dominio di sicurezza associato alla funzione o al gruppo di lavoro.

Dalle riflessioni sopra ne discende che i domini di sicurezza presenti all'interno di ogni singola sede variano in numero da 6 a 8 a seconda del numero dei gruppi di ricerca e sviluppo (gruppi RS, anche detti gruppi di progetto) attivi ad un dato istante.

Per tenere separati i domini di sicurezza, sebbene fisicamente il personale possa trovarsi in qualunque postazione della sede, si ricorre alla tecnologia delle reti locali virtuali (VLAN).
In pratica ad ogni dominio di sicurezza si associa una VLAN caratterizzata da un identificatore; si è previsto un diverso identificatore per ogni VLAN e per ogni sede, la numerazione utilizzata è la seguente:

VLAN id = X+Y

dove

X è uguale a

- 10 per Roma
- 20 per Padova
- 30 per Pisa

Y è uguale a

- 1 per la VLAN dei Server globali (raggiungibili da internet) [GlobalVLAN]
- 2 per la VLAN degli Enterprise Server [ServerVLAN]
- 3 per la VLAN della funzione direzione e amministrazione [DominioDA]
- 4 per la VLAN della funzione marketing [DominioM]
- 5 per la VLAN della funzione supporto sistemi [DominioSS]
- 6 per la VLAN del primo gruppo di progetto, funzione ricerca e sviluppo [DominioRS1]
- 7 per la VLAN del secondo gruppo di progetto, funzione ricerca e sviluppo [DominioRS2]
- 8 per la VLAN del terzo gruppo di progetto, funzione ricerca e sviluppo [DominioRS3]

Realizzando la rete interna ad ogni singola sede esclusivamente utilizzando dispositivi di livello 2 (switch con l'appropriata configurazione delle 8 VLAN necessarie), il singolo router di frontiera deve fungere da default gateway per dispositivi terminali appartenenti a diverse VLAN, dunque ad ogni VLAN viene associata una sottointerfaccia di una delle interfacce fisiche gigabitEthernet del router che si affacciano verso la sede, da utilizzare come default gateway.

Questo criterio di progetto non assicura una maggiore robustezza del collegamento tra router di frontiera e sede, infatti se una delle interfacce fisiche cade tutte le VLAN che la utilizzavano come default gateway rimangono isolate. Tuttavia procedendo in questo modo si ha una migliore ripartizione del traffico sulle due interfacce del router.

- Sulla gigabitEthernet 2/0 di Pisa e Padova e sulla gigabitEthernet 1/0 di RomaLocal vengono create le sottointerfacce relative ai seguenti domini di sicurezza:
  - GlobalVLAN
  - ServerVLAN
  - DominioDA
  - DominioM
  - DominioSS
- Sulla gigabitEthernet 3/0 di Pisa e Padova e sulla gigabitEthernet 2/0 di RomaLocal vengono create le sottointerfacce relative ai seguenti domini di sicurezza:
  - DominioRS1
  - DominioRS2
  - DominioRS3

In ogni caso il numero della sottointerfaccia creata (ad esempio gigabitEthernet 2/0.xxx) corrisponde al VLAN id della VLAN che la utilizza come default gateway (diverso per ogni VLAN e sede aziendale).

La scelta di questo tipo di ripartizione delle VLAN deriva sia dalla quantità di personale facente parte dei diversi domini che dal numero delle persone che possono cercare di contattare macchine dall'esterno del dominio (come accade nel contattare i domini dei Server globali ed Enterprise).

Prima di implementare le politiche di sicurezza per i diversi domini è necessario conoscere esattamente a quali sottoreti corrispondono nelle diverse sedi i vari domini.
A tal proposito è necessario fare alcune riflessioni, in relazione alle singole sedi.

4.1 ROMA

Postazioni complessive:
95 (Edificio Nord) + 89 (Edificio Sud) + 12 (Edificio Centro) = 196
- Direzione e Amministrazione: 27
- Marketing: 5
- Supporto Sistemi: 8

Oltre alle postazioni suddette, sono presenti 2 stanze in cui collocare i Server:
- Workgroup Server + Enterprise Server + Global Server: 48

Per un totale di 244 macchine potenzialmente connesse.
Alla funzione RS, nel caso in cui le postazioni dei domini di cui sopra non fossero occupate da alcun impiegato, potrebbero appartenere potenzialmente tutte le 196 macchine.
Siccome se ho un solo progetto attivo tutte le macchine della funzione RS potrebbero far parte di tale progetto, potenzialmente ciascun gruppo di progetto deve essere in grado di ospitare 196 macchine.
Vediamo allora quanti sono gli indirizzi necessari:
- Global server: 2 + **1** (gateway) = 3
- Enterprise Server: 40 + **1**(gateway) = 41
- Direzione e Amministrazione: 27 + **3** (wg server) + **1** (gateway) = 31
- Marketing: 5 + **3** (wg server) + **1** (gateway) = 9
- Supporto Sistemi: 8 + **3** (wg server) + **1** (gateway) + **15** (switch) = 27
- Gruppo Ricerca e Sviluppo 1: 196 (potenzialmente) + **3** (wg server) + **1** (gateway) = 200
- Gruppo Ricerca e Sviluppo 2: 196 (potenzialmente) + **3** (wg server) + **1** (gateway) = 200
- Gruppo Ricerca e Sviluppo 3: 196 (potenzialmente) + **3** (wg server) + **1** (gateway) = 200

In generale si è deciso di adottare la regola che gli switch, che costituiscono i dispositivi (oltre al router) ai quali è concesso l'accesso solamente al dominio SS, abbiano la loro interfaccia di configurazione all'interno di tale dominio di sicurezza.
La tabella 1.2 mostra la suddivisione con tecnica VLSM del blocco degli indirizzi di Roma.

Indirizzi dei gruppi di Roma

Sottorete	Dimensione	Indirizzo di Rete	Lunghezza Maschera	Maschera	Spazio di Indirizzamento
DominioRS1_ Roma	254	172.16.192.0	/24	255.255.255.0	172.16.192.1 – 172.16.192.254
DominioRS2_ Roma	254	172.16.193.0	/24	255.255.255.0	172.16.193.1 – 172.16.193.254
DominioRS3_ Roma	254	172.16.194.0	/24	255.255.255.0	172.16.194.1 – 172.16.194.254
ServerVLAN_ Roma	62	172.16.195.0	/26	255.255.255.192	172.16.195.1 – 172.16.195.62
DominioDA_ Roma	62	172.16.195.64	/26	255.255.255.192	172.16.195.65 – 172.16.195.126
DominioSS_ Roma	30	172.16.195.128	/27	255.255.255.224	172.16.195.129 – 172.16.195.158
DominioM_ Roma	14	172.16.195.160	/28	255.255.255.240	172.16.195.161 – 172.16.195.174
GlobalVLAN_ Roma	6	172.16.195.176	/29	255.255.255.248	172.16.195.177 – 172.16.195.182

TAB 1.2

4.2 PADOVA

Postazioni complessive:
60 (Edificio Est) + 101 (Edificio Ovest) = 161
- Direzione e Amministrazione: 11
- Marketing: 4
- Supporto Sistemi: 7

Oltre alle postazioni suddette, sono presenti 2 stanze in cui collocare i Server:
- Workgroup Server + Enterprise Server + Global Server: 48

Per un totale di 209 macchine potenzialmente connesse.
Alla funzione RS, nel caso in cui le postazioni dei domini di cui sopra non fossero occupate da alcun impiegato, potrebbero appartenere potenzialmente tutte le 161 macchine.
Siccome se ho un solo progetto attivo tutte le macchine della funzione RS potrebbero far parte di tale progetto, ho che potenzialmente ciascun gruppo di progetto deve essere in grado di ospitare 161 macchine.
Vediamo allora quanti sono gli indirizzi necessari:
- Global server: 2 + **1** (gateway) = 3
- Enterprise Server: 40 + **1** (gateway) = 41
- Direzione e Amministrazione: 11 + **3** (wg server) + **1** (gateway) = 15
- Marketing: 4 + **3** (wg server) + **1** (gateway) = 8
- Supporto Sistemi: 7 + **3** (wg server) + **1** (gateway) + **12** (switch) = 23
- Gruppo Ricerca e Sviluppo 1: 161 (potenzialmente) + **3** (wg server) + **1** (gateway) = 165
- Gruppo Ricerca e Sviluppo 2: 161 (potenzialmente) + **3** (wg server) + **1** (gateway) = 165
- Gruppo Ricerca e Sviluppo 3: 161 (potenzialmente) + **3** (wg server) + **1** (gateway) = 165

In generale si è deciso di adottare la regola che gli switch, i quali costituiscono i dispositivi (oltre al router) ai quali è concesso l'accesso solamente al dominio SS, abbiano la loro interfaccia di configurazione all'interno di tale dominio di sicurezza.
La tabella 1.3 mostra la suddivisione con tecnica VLSM del blocco degli indirizzi di Padova.

Indirizzi dei gruppi di Padova

Sottorete	Dimensione	Indirizzo di Rete	Lunghezza Maschera	Maschera	Spazio di Indirizzamento
DominioRS1_ Padova	254	172.16.208.0	/24	255.255.255.0	172.16.208.1 - 172.16.208.254
DominioRS2_ Padova	254	172.16.209.0	/24	255.255.255.0	172.16.209.1 - 172.16.209.254
DominioRS3_ Padova	254	172.16.210.0	/24	255.255.255.0	172.16.210.1 - 172.16.210.254
ServerVLAN_ Padova	62	172.16.211.0	/26	255.255.255.192	172.16.211.1 - 172.16.211.62
DominioSS_ Padova	30	172.16.211.64	/27	255.255.255.224	172.16.211.65 - 172.16.211.94
DominioDA_ Padova	30	172.16.211.96	/27	255.255.255.224	172.16.211.97 - 172.16.211.126
DominioM_ Padova	14	172.16.211.128	/28	255.255.255.240	172.16.211.129 - 172.16.211.142
GlobalVLAN_ Padova	6	172.16.211.144	/29	255.255.255.248	172.16.211.145 - 172.16.211.150

TAB 1.3

4.3 PISA

Postazioni complessive:
38 (Edificio Est) + 90 (Edificio Nord) + 53 (Edificio Sud) = 181
- Direzione e Amministrazione: 5
- Marketing: 3
- Supporto Sistemi: 2

Oltre alle postazioni suddette, sono presenti 2 stanze in cui collocare i Server:
- Workgroup Server + Enterprise Server + Global Server: 48

Per un totale di 229 macchine potenzialmente connesse.
Alla funzione RS, nel caso in cui le postazioni dei domini di cui sopra non fossero occupate da alcun impiegato, potrebbero appartenere potenzialmente tutte le 181 macchine.
Siccome se ho un solo progetto attivo tutte le macchine della funzione RS potrebbero far parte di tale progetto, ho che potenzialmente ciascun gruppo di progetto deve essere in grado di ospitare 181 macchine.
Vediamo allora quanti sono gli indirizzi necessari:
- Global Server: 3 + **1** (gateway) = 4
- Enterprise Server: 40 + **1** (gateway) = 41
- Direzione e Amministrazione: 5 + **3** (wg server) + **1** (gateway) = 9
- Marketing: 3 + **3** (wg server) + **1** (gateway) = 7
- Supporto Sistemi: 2 + **3** (wg server) + **1** (gateway) + **12** (switch) = 18
- Gruppo Ricerca e Sviluppo 1: 181 (potenzialmente) + **3** (wg server) + **1** (gateway) = 185
- Gruppo Ricerca e Sviluppo 2: 181 (potenzialmente) + **3** (wg server) + **1** (gateway) = 185
- Gruppo Ricerca e Sviluppo 3: 181 (potenzialmente) + **3** (wg server) + **1** (gateway) = 185

In generale si è deciso di adottare la regola che gli switch, che costituiscono i dispositivi (oltre al router) ai quali è concesso l'accesso solamente al dominio SS, abbiano la loro interfaccia di configurazione all'interno di tale dominio di sicurezza.
La tabella 1.4 mostra la suddivisione con tecnica VLSM del blocco degli indirizzi di Pisa.

Indirizzi dei gruppi di Pisa

Sottorete	Dimensione	Indirizzo di Rete	Lunghezza Maschera	Maschera	Spazio di Indirizzamento
DominioRS1_ Pisa	254	172.16.224.0	/24	255.255.255.0	172.16.224.1 - 172.16.224.254
DominioRS2_ Pisa	254	172.16.225.0	/24	255.255.255.0	172.16.225.1 - 172.16.225.254
DominioRS3_ Pisa	254	172.16.226.0	/24	255.255.255.0	172.16.226.1 - 172.16.226.254
ServerVLAN_ Pisa	62	172.16.227.0	/26	255.255.255.192	172.16.227.1 - 172.16.227.62
DominioSS_ Pisa	30	172.16.227.64	/27	255.255.255.224	172.16.227.65 - 172.16.227.94
DominioDA_ Pisa	14	172.16.227.96	/28	255.255.255.240	172.16.227.97 - 172.16.227.110
DominioM_ Pisa	14	172.16.227.112	/28	255.255.255.240	172.16.227.113 - 172.16.227.126
GlobalVLAN_ Pisa	6	172.16.227.128	/29	255.255.255.248	172.16.227.129 - 172.16.227.134

TAB 1.4

Una volta definite le varie reti per ogni gruppo di lavoro, è possibile dare la configurazione delle interfacce del router, come si evince dalle Tabelle da 1.5 a 1.8.

Si noti che anche nel caso delle connessioni Frame Relay punto-punto con interfaccia seriale fisica dedicata abbiamo utilizzato delle sottointerfacce: questo rende più leggibile la configurazione in quanto il numero della sottointerfaccia è corrispondente al DLCI utilizzato.
Dove non indicato esplicitamente, la Bandwidth resta quella di default.
Dove non è stato assegnato un nome alla rete, allora questo non è importante in questa sezione, riferirsi alla sezione del progettista responsabile per eventuali osservazioni o rettifiche.

ROUTER ROMALOCAL

Interfaccia/ SottoInterfaccia	Descrizione	Band width	Nome Rete	Indirizzo Rete	Indirizzo IP Interfaccia	Maschera di Rete
Serial 0/0.112	To Pisa (Backup)	256	Pisa_ RomaLocal	172.16.240.12	172.16.240.14	255.255.255.252
Serial 0/0.116	To Padova (Backup)	256	Padova_ RomaLocal	172.16.240.16	172.16.240.18	255.255.255.252
gigabitEthernet 1/0.11	GlobalVLAN_R oma	-	-	172.16.195.176	172.16.195.177	255.255.255.248
gigabitEthernet 1/0.12	ServerVLAN_Ro ma	-	-	172.16.195.0	172.16.195.1	255.255.255.192
gigabitEthernet 1/0.13	DominioDA_Ro ma	-	-	172.16.195.64	172.16.195.65	255.255.255.192
gigabitEthernet 1/0.14	DominioM_Ro ma	-	-	172.16.195.160	172.16.195.161	255.255.255.240
gigabitEthernet 1/0.15	DominioSS_Ro ma	-	-	172.16.195.128	172.16.195.129	255.255.255.224
gigabitEthernet 2/0.16	DominioRS1_R oma	-	-	172.16.192.0	172.16.192.1	255.255.255.0
gigabitEthernet 2/0.17	DominioRS2_R oma	-	-	172.16.193.0	172.16.193.1	255.255.255.0
gigabitEthernet 2/0.18	DominioRS3_R oma	-	-	172.16.194.0	172.16.194.1	255.255.255.0
fastEthernet 3/0	To Roma-ext (A)	100. 000	RomaLocal_ Roma-ext_a	172.16.240.20	172.16.240.21	255.255.255.252
fastEthernet 4/0	To Roma-ext (B)	100. 000	RomaLocal_ Roma-ext_b	172.16.240.24	172.16.240.25	255.255.255.252

TAB 1.5

ROUTER PADOVA

Interfaccia/ SottoInterfaccia	Descrizione	Band width	Nome Rete	Indirizzo Rete	Indirizzo IP Interfaccia	Maschera di Rete
Serial 0/0.104	To Roma-ext	1.544	Padova_ Roma-ext	172.16.240.4	172.16.240.5	255.255.255.252
Serial 1/0.108	To Pisa (Backup)	256	Pisa_ Padova	172.16.240.8	172.16.240.10	255.255.255.252
Serial 1/0.116	To RomaLocal (Backup)	256	Padova_ RomaLocal	172.16.240.16	172.16.240.17	255.255.255.252
gigabitEthernet 2/0.21	GlobalVLAN_Padova	-	-	172.16.211.144	172.16.211.145	255.255.255.248
gigabitEthernet 2/0.22	ServerVLAN_Padova	-	-	172.16.211.0	172.16.211.1	255.255.255.192
gigabitEthernet 2/0.23	DominioDA_ Padova	-	-	172.16.211.96	172.16.211.97	255.255.255.224
gigabitEthernet 2/0.24	DominioM_ Padova	-	-	172.16.211.128	172.16.211.129	255.255.255.240
gigabitEthernet 2/0.25	DominioSS_ Padova	-	-	172.16.211.64	172.16.211.65	255.255.255.224
gigabitEthernet 3/0.26	DominioRS1_ Padova	-	-	172.16.208.0	172.16.208.1	255.255.255.0
gigabitEthernet 3/0.27	DominioRS2_ Padova	-	-	172.16.209.0	172.16.209.1	255.255.255.0
gigabitEthernet 3/0.28	DominioRS3_ Padova	-	-	172.16.210.0	172.16.210.1	255.255.255.0

TAB 1.6

ROUTER PISA

Interfaccia/ SottoInterfaccia	Descrizione	Band width	Nome Rete	Indirizzo Rete	Indirizzo IP Interfaccia	Maschera di Rete
Serial 0/0.100	To Roma-ext	1.544	Pisa_ Roma-ext	172.16.240.0	172.16.240.1	255.255.255.252
Serial 1/0.108	To Padova (Backup)	256	Pisa_ Padova	172.16.240.8	172.16.240.9	255.255.255.252
Serial 1/0.112	To RomaLocal (Backup)	256	Pisa_ RomaLocal	172.16.240.12	172.16.240.13	255.255.255.252
gigabitEthernet 2/0.31	GlobalVLAN_Pisa	-	-	172.16.227.128	172.16.227.129	255.255.255.248
gigabitEthernet 2/0.32	ServerVLAN_Pisa	-	-	172.16.227.0	172.16.227.1	255.255.255.192
gigabitEthernet 2/0.33	DominioDA_ Pisa	-	-	172.16.227.96	172.16.227.97	255.255.255.240
gigabitEthernet 2/0.34	DominioM_ Pisa	-	-	172.16.227.112	172.16.227.113	255.255.255.240
gigabitEthernet 2/0.35	DominioSS_ Pisa	-	-	172.16.227.64	172.16.227.65	255.255.255.224
gigabitEthernet 3/0.36	DominioRS1_ Pisa	-	-	172.16.224.0	172.16.224.1	255.255.255.0
gigabitEthernet 3/0.37	DominioRS2_ Pisa	-	-	172.16.225.0	172.16.225.1	255.255.255.0
gigabitEthernet 3/0.38	DominioRS3_ Pisa	-	-	172.16.226.0	172.16.226.1	255.255.255.0

TAB 1.7

ROUTER ROMA-EXT

Interfaccia/ SottoInterfaccia	Descrizione	Band width	Nome Rete	Indirizzo Rete	Indirizzo IP Interfaccia	Maschera di Rete
Serial 0/0.100	To Pisa	1544	Pisa_ Roma-ext	172.16.240.0	172.16.240.2	255.255.255.252
Serial 1/0.104	To Padova	1544	Padova_ Roma-ext	172.16.240.4	172.16.240.6	255.255.255.252
Serial 2/0	To ISP-InternetGw	-	Roma-ext_ ISP-InternetGW	Vedere la sezione sul NAT		
fastEthernet 3/0	To RomaLocal (A)	100.000	RomaLocal_ Roma-ext_a	172.16.240.20	172.16.240.22	255.255.255.252
fastEthernet 4/0	To RomaLocal (B)	100.000	RomaLocal_ Roma-ext_b	172.16.240.24	172.16.240.26	255.255.255.252

TAB 1.8

Una volta decisa la suddivisione degli indirizzi, si può immediatamente configurare il router di confine di ogni sede aziendale per fungere da Server DHCP.
Tale configurazione serve per realizzare la dinamicità richiesta dalle specifiche, infatti si richiede che gli appartenenti a ciascun gruppo di progetto possano essere riassegnati ad un altro gruppo se il progetto termina o anche se semplicemente lo si ritiene necessario.
Inoltre in generale la rete deve riprodurre la flessibilità dell'organizzazione aziendale permettendo di configurare, in modo flessibile, domini di sicurezza associati a ciascun settore aziendale e ai gruppi di progetto del dominio RS.

Implementando allora, sui router di frontiera, delle politiche per assegnare la configurazione IP alle macchine che si connettono a seconda della loro VLAN di appartenenza (stabilita dalla porta dello switch a cui si connettono), si ottiene la massima adattabilità alle esigenze in quanto se si necessita di un cambio di dominio di sicurezza per una macchina connessa ad uno switch è sufficiente cambiare la VLAN a cui è associata tale porta. Tutta la configurazione IP viene fornita in automatico dal router di confine tramite l'utilizzo di DHCP.
Dobbiamo notare però che alcuni indirizzi non possono essere assegnati dinamicamente alle macchine, in particolare quelli dei Server e quelli relativi agli switch (necessari per la configurazione).

I Server sono:
- Enterprise Server
- Workgroup Server
- Global Server (Server accessibili dall'esterno dell'azienda)

Inoltre consideriamo:
- Indirizzi assegnati alle interfacce di configurazione degli switch
- Indirizzi assegnati alle sottointerfacce del router

Si definiscono allora 6 pool di indirizzi IP dai quali il router ricava gli indirizzi da assegnare ai client DHCP: ogni pool ha un default-gateway diverso a seconda della VLAN in considerazione.
Il Server DHCP andrà inoltre ad assegnare l'indirizzo del Server DNS ad ogni client. Per le sedi di Roma e Pisa tale DNS è quello interno alla sede, mentre per la sede di Padova, dal momento che dalle specifiche si evince che manca un server DNS interno alla sede, il router di confine andrà ad assegnare uno fra i due server DNS di Roma o di Pisa.

In particolare si è deciso di assegnare ai domini
- *DominioDA_Padova*
- *DominioM_Padova*
- *DominioSS_Padova*
- *DominioRS1_Padova*

il server DNS di Roma, mentre ai domini
- *DominioRS2_Padova*
- *DominioRS3_Padova*

il server DNS di Pisa. Questo per cercare di bilanciare il lavoro dei Server.

In tabella 1.9 sono riportati gli indirizzi assegnati ai diversi Global Server della azienda.

Global Server

Città	Server	Indirizzo IP
Roma	Web	172.16.195.182
	DNS	172.16.195.181
Padova	Web	172.16.211.150
	SMTP	172.16.211.149
Pisa	Web	172.16.227.134
	DNS	172.16.227.133
	SMTP	172.16.227.132

TAB 1.9

Si danno allora le tabelle relative alla configurazione dei router di confine come Server DHCP (Tabelle da 1.10 a 1.12).

Tabella DHCP router RomaLocal

Indirizzi Esclusi	*172.16.195.124 – 172.16.195.126 (Workgroup Server DA)* *172.16.195.172 – 172.16.195.174 (Workgroup Server M)* *172.16.195.141 – 172.16.195.158 (Workgroup Server SS + Switch)* *172.16.192.252 – 172.16.192.254 (Workgroup Server RS1)* *172.16.193.252 – 172.16.193.254 (Workgroup Server RS2)* *172.16.194.252 – 172.16.194.254 (Workgroup Server RS3)*				
Nome del pool	**Rete**	**Maschera di rete**	**Default router**	**Server DNS**	**Indirizzi disponibili**
DominioDA_Roma	172.16.195.64	255.255.255.192	172.16.195.65	172.16.195.181	172.16.195.66-172.16.195.123
DominioM_Roma	172.16.195.160	255.255.255.240	172.16.195.161	172.16.195.181	172.16.195.162-172.16.195.171
DominioSS_Roma	172.16.195.128	255.255.255.224	172.16.195.129	172.16.195.181	172.16.195.130-172.16.195.140
DominioRS1_Roma	172.16.192.0	255.255.255.0	172.16.192.1	172.16.195.181	172.16.192.2-172.16.192.251
DominioRS2_Roma	172.16.193.0	255.255.255.0	172.16.193.1	172.16.195.181	172.16.193.2-172.16.193.251
DominioRS3_Roma	172.16.194.0	255.255.255.0	172.16.194.1	172.16.195.181	172.16.194.2-172.16.194.251

TAB 1.10

Tabella DHCP router Padova

Indirizzi Esclusi	*172.16.211.124 – 172.16.211.126 (Workgroup Server DA)* *172.16.211.140 – 172.16.211.142 (Workgroup Server M)* *172.16.211.80 – 172.16.211.94 (Workgroup Server SS + Switch)* *172.16.208.252 – 172.16.208.254 (Workgroup Server RS1)* *172.16.209.252 – 172.16.209.254 (Workgroup Server RS2)* *172.16.210.252 – 172.16.210.254 (Workgroup Server RS3)*				
Nome del pool	**Rete**	**Maschera di rete**	**Default router**	**Server DNS**	**Indirizzi disponibili**
DominioDA_Padova	172.16.211.96	255.255.255.224	172.16.211.97	172.16.195.181	172.16.211.98-172.16.211.123
DominioM_ Padova	172.16.211.128	255.255.255.240	172.16.211.129	172.16.195.181	172.16.211.130-172.16.211.139
DominioSS_ Padova	172.16.211.64	255.255.255.224	172.16.211.65	172.16.195.181	172.16.211.66-172.16.211.79
DominioRS1_ Padova	172.16.208.0	255.255.255.0	172.16.208.1	172.16.195.181	172.16.208.2-172.16.208.251
DominioRS2_ Padova	172.16.209.0	255.255.255.0	172.16.209.1	172.16.227.133	172.16.209.2-172.16.209.251
DominioRS3_ Padova	172.16.210.0	255.255.255.0	172.16.210.1	172.16.227.133	172.16.210.2-172.16.210.251

TAB 1.11

Tabella DHCP router Pisa

Indirizzi Esclusi	*172.16.227.108 – 172.16.227.110 (Workgroup Server DA)* *172.16.227.124 – 172.16.227.126 (Workgroup Server M)* *172.16.227.80 – 172.16.227.94 (Workgroup Server SS + Switch)* *172.16.224.252 – 172.16.224.254 (Workgroup Server RS1)* *172.16.225.252 – 172.16.225.254 (Workgroup Server RS2)* *172.16.226.252 – 172.16.226.254 (Workgroup Server RS3)*				
Nome del pool	**Rete**	**Maschera di rete**	**Default router**	**Server DNS**	**Indirizzi disponibili**
DominioDA_Pisa	172.16.227.96	255.255.255.240	172.16.227.97	172.16.227.133	172.16.227.98-172.16.227.107
DominioM_ Pisa	172.16.227.112	255.255.255.240	172.16.227.113	172.16.227.133	172.16.227.114-172.16.227.123
DominioSS_ Pisa	172.16.227.64	255.255.255.224	172.16.227.65	172.16.227.133	172.16.227.66-172.16.227.79
DominioRS1_ Pisa	172.16.224.0	255.255.255.0	172.16.224.1	172.16.227.133	172.16.224.2-172.16.224.251
DominioRS2_ Pisa	172.16.225.0	255.255.255.0	172.16.225.1	172.16.227.133	172.16.225.2-172.16.225.251
DominioRS3_ Pisa	172.16.226.0	255.255.255.0	172.16.226.1	172.16.227.133	172.16.226.2-172.16.226.251

TAB 1.12

Una volta suddivisi i domini di sicurezza/gruppi di lavoro in diverse VLAN corrispondenti a diverse sottoreti, risulta semplice implementare le politiche di protezione, a tale proposito si utilizzano i seguenti principi generali:

- Si utilizzano Access Control List (ACL) di tipo esteso, e named.
- Gli accessi non consentiti vengono bloccati il prima possibile (in particolare sulla interfaccia del gateway, in ingresso).
- Non si effettuano controlli all'uscita dei pacchetti dai router di sede, si suppone infatti che se un pacchetto ha superato la ACL in ingresso al suo default gateway allora il traffico relativo sia consentito.
- Non si effettuano controlli all'ingresso delle interfacce che si affacciano verso gli altri router in quanto se un pacchetto ha superato tale router allora il traffico era consentito.
- Anche per il traffico proveniente da internet, eventuali controlli vengono fatti all'ingresso dell'interfaccia del router Roma-ext che si affaccia verso l'ISP.
- A tutti i domini eccetto il dominio Supporto Sistemi è precluso l'accesso a tutti i dispositivi di rete.
- In generale le regole vengono realizzate in modo tale da essere più stringenti possibile.
- Si cerca sempre di scrivere prima le regole che matchano il maggior numero di pacchetti, per risparmiare tempo di elaborazione del router, ovviamente alcune regole devono essere necessariamente precedute da altre, anche se matcherebbero più pacchetti (perché la ACL sia corretta).

Non è specificato dalla WWAS il tipo di traffico che si avrà verso i Server Enterprise, l'ipotesi che facciamo è allora che l'accesso a tali Server deve essere consentito a tutta l'azienda, e che il traffico sia di tipo TCP.

Dalle specifiche è possibile ricavare le regole desiderate per la protezione e la segretezza, queste si possono classificare per dominio e riassumere come segue:

DA (Direzione e Amministrazione):

- deve essere consentito il traffico verso altri domini DA di altre sedi.
- deve essere consentito il traffico verso Internet.
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.
- deve essere consentito il traffico TCP verso i Server Enterprise.

RS1 (primo Gruppo di Progetto):

- deve essere consentito il traffico verso altri domini RS1 (ossia il medesimo gruppo di progetto) di altre sedi.
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.
- deve essere consentito il traffico TCP verso i Server Enterprise.

RS2 (secondo Gruppo di Progetto):

- deve essere consentito il traffico verso altri domini RS2 (ossia il medesimo gruppo di progetto) di altre sedi.
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.
- deve essere consentito il traffico TCP verso i Server Enterprise.

RS3 (terzo Gruppo di Progetto):
- deve essere consentito il traffico verso altri domini RS3 (ossia il medesimo gruppo di progetto) di altre sedi.
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.
- deve essere consentito il traffico TCP verso i Server Enterprise.

M (Marketing):
- deve essere consentito il traffico verso altri domini M di altre sedi.
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.
- deve essere consentito il traffico TCP verso i Server Enterprise.

SS (Supporto Sistemi):
- deve essere consentito il traffico verso altri domini SS di altre sedi.
- deve essere consentito il traffico TCP verso l'intera azienda (dispositivi di rete compresi).
- deve essere consentito il traffico verso i Server globali sulle giuste porte / protocolli.

GlobalVLAN:
- deve essere consentito il traffico sulle giuste porte / protocolli verso tutti (per consentire alle risposte dei server globali di raggiungere coloro che li hanno contattati)

ServerVLAN:
- deve essere consentito il traffico verso altri domini di Server Enterprise di altre sedi.
- deve essere consentito il traffico TCP verso l'intera azienda.

Notare che per quanto riguarda la GlobalVLAN l'unico traffico Web[2] consentito in uscita dalla rete sarà quello di tipo TCP established, in questo modo si ha che i server web possono solamente essere contattati dall'esterno e non possono essere loro ad aprire connessioni TCP.
Qualunque macchina di qualunque dominio dovrà inoltre essere in grado di rispondere ad un operatore della funzione SS che intenda connettersi, questo si fa facendo in modo che il traffico TCP verso i domini SS sia consentito, solo di tipo established, da tutte le macchine.
In ogni caso le macchine dei vari domini (eccetto GlobalVLAN e ServerVLAN) devono poter acquisire un indirizzo IP tramite l'utilizzo del protocollo DHCP, dunque bisogna prevedere regole appropriate, per evitare che le richieste vengano scartate.

Si riporta adesso un esempio di configurazione generica che rispecchia la configurazione dei tre router RomaLocal, Pisa e Padova. Si utilizzano i seguenti formalismi:

Dominio XX-a	→	Dominio XX locale alla sede.
Dominio XX-b e XX-c	→	Domini XX delle altre sedi.
Azienda	→	Blocco degli indirizzi IP privati della azienda.
any	→	ogni indirizzo è riconosciuto.
Server YY-a	→	Server globale locale alla sede.
Server YY-b e YY-c	→	Server globale YY delle altre sedi.
Broadcast	→	indirizzo IP di broadcast.
This	→	host 0.0.0.0.

Le ACL sotto riportate verranno applicate sulle sotto-interfacce dei router che si affacciano sulle sedi e filtreranno il traffico in ingresso. Per la ACL afferente al router connesso all'ISP si veda il paragrafo seguente.

[2] Per traffico Web si intende traffico sia di tipo HTTP (Porta 80) che HTTPS (Porta 443).

Esempio di configurazione:

DA:

```
permit ip DA-a DA-b
permit ip DA-a DA-c
permit tcp DA-a Enterprise-a
permit tcp DA-a DNS-a (non per Padova, che non ha un proprio server DNS)
permit udp DA-a DNS-b (solo per Padova)
permit udp DA-a DNS-c (solo per Padova)
permit tcp DA-a Web-a
permit tcp DA-a SMTP-a (non per Roma, che non ha un proprio server SMTP)
permit tcp DA-a SMTP-b (solo per Roma)
permit tcp DA-a SMTP-c (solo per Roma)
permit tcp DA-a Enterprise-b
permit tcp DA-a Enterprise-c
permit tcp DA-a Web-b
permit tcp DA-a Web-c
permit tcp DA-a SMTP-b (non per Roma)
permit udp DA-a DNS-b (non per Padova)
permit tcp DA-a SS-a established
permit tcp DA-a SS-b established
permit tcp DA-a SS-c established
deny ip DA-a Azienda
permit ip DA-a any
permit udp This eq 68 Broadcast eq 67
```

RSX (per X = 1,2,3):

```
permit ip RSX-a RSX-b
permit ip RSX-a RSX-c
permit tcp RSX-a Enterprise-a
permit udp RSX-a DNS-a (non per Padova, che non ha un proprio server DNS)
permit udp RSX-a DNS-b (solo per Padova)
permit udp RSX-a DNS-c (solo per Padova)
permit tcp RSX-a Web-a
permit udp RSX-a SMTP-a (non per Roma, che non ha un proprio server SMTP)
permit tcp RSX-a SMTP-b (solo per Roma)
permit tcp RSX-a SMTP-c (solo per Roma)
permit tcp RSX-a Enterprise-b
permit tcp RSX-a Enterprise-c
permit tcp RSX-a Web-b
permit tcp RSX-a Web-c
permit udp RSX-a SMTP-b (non per Roma)
permit udp RSX-a DNS-b (non per Padova)
permit tcp RSX-a SS-a established
permit tcp RSX-a SS-b established
permit tcp RSX-a SS-c established
permit udp This eq 68 Broadcast eq 67
```

M:

```
permit ip M-a M-b
permit ip M-a M-c
permit tcp M-a Enterprise-a
permit udp M-a DNS-a (non per Padova, che non ha un proprio server DNS)
permit udp M-a DNS-b (solo per Padova)
permit udp M-a DNS-c (solo per Padova)
permit tcp M-a Web-a
permit tcp M-a SMTP-a (non per Roma, che non ha un proprio server SMTP)
permit tcp M-a SMTP-b (solo per Roma)
permit tcp M-a SMTP-c (solo per Roma)
permit tcp M-a Enterprise-b
permit tcp M-a Enterprise-c
permit tcp M-a Web-b
permit tcp M-a Web-c
permit tcp M-a SMTP-b (non per Roma)
permit udp M-a DNS-b (non per Padova)
permit tcp M-a SS-a established
permit tcp M-a SS-b established
permit tcp M-a SS-c established
permit udp This 68 Broadcast 67
```

SS:

```
permit tcp SS-a Azienda
permit ip SS-a SS-b
permit ip SS-a SS-c
permit udp SS-a DNS-a (non per Padova, che non ha un proprio server DNS)
permit udp SS-a DNS-b
permit udp SS-a DNS-c (solo per Padova)
permit udp This 68 Broadcast 67
```

GlobalVLAN:

```
permit tcp Web-a any established
permit udp DNS-a any (non per Padova)
permit tcp SMTP-a any (non per Roma)
permit tcp GlobalVLAN-a SS-a established
permit tcp GlobalVLAN-a SS-b established
permit tcp GlobalVLAN-a SS-c established
```

ServerVLAN:

```
permit tcp ServerVLAN-a Azienda
permit ip ServerVLAN-a ServerVLAN-b
permit ip ServerVLAN-a ServerVLAN-c
```

8. Indirizzi pubblici

Secondo i requisiti di progetto è necessario utilizzare il minimo numero di indirizzi pubblici possibile (per motivi di costo). Il minimo numero è 3, infatti almeno 3 indirizzi devono essere disponibili sulla porta 80 per l'accesso ai 3 Server Web dall'esterno. 3 indirizzi sono inoltre sufficienti ad accomodare i server DNS e SMTP sulle corrette porte. Con la tecnica del PAT dinamico si possono poi utilizzare le altre porte disponibili per tutti i client che intendono connettersi ad internet (dominio DA).
A tutti i client che necessitano di una traduzione dinamica dell'indirizzo, si associa come indirizzo inside global uno dei tre indirizzi pubblici acquistati dalla azienda con una porta opportuna generata dal meccanismo di traduzione.

L'indirizzo della interfaccia Serial 2/0 del router Roma-ext coincide con uno dei tre indirizzi pubblici, ed è il seguente: `213.140.19.100/29`[3]

Per quanto riguarda il router Roma-ext, si prevede una ACL posizionata sull'interfaccia che si affaccia verso l'ISP, sempre per effettuare filtraggio in ingresso; tale ACL dovrà assicurare che pacchetti che portano come indirizzo IP di destinazione un indirizzo privato dell'azienda non vengano lasciati passare verso la rete aziendale. Per il principio dell'utilizzo di ACL più stringenti possibile si è allora deciso di scrivere regole che lascino passare solamente pacchetti verso i tre indirizzi pubblici della azienda. Inoltre, si dovrà accertare che i pacchetti siano diretti ad una porta prevista o derivino da una connessione già stabilita da utenti dell'azienda con l'esterno. Un esempio di ACL, scritta per essere applicata all'interfaccia Serial 2/0 di Roma-ext, in ingresso, è il seguente:

```
permit tcp any host <IP Pubblico 1> eq 80/443    (web)
permit tcp any host <IP Pubblico 2> eq 80/443
permit tcp any host <IP Pubblico 3> eq 80/443

permit tcp any host <IP Pubblico 2> eq 25        (SMTP)
permit tcp any host <IP Pubblico 3> eq 25

permit tcp any host <IP Pubblico 1> eq 53        (DNS)
permit tcp any host <IP Pubblico 3> eq 53
```

[3] Si veda oltre.

```
permit tcp any host <IP Pubblico 1> established  (traffico di risposta)
permit tcp any host <IP Pubblico 2> established
permit tcp any host <IP Pubblico 3> established
```

Per semplicità nell'esposizione a seguire supponiamo che i 3 indirizzi pubblici che la azienda ha comprato dal proprio ISP siano i seguenti (Tabella 1.13):

Indirizzi pubblici	Maschera di rete
213.140.19.100	255.255.255.248
213.140.19.101	255.255.255.248
213.140.19.102	255.255.255.248

TAB 1.13

Dove abbiamo supposto che alla rete tra il router Roma-ext e l'ISP sia stata associata una maschera /29, ossia tale da contenere 6 indirizzi pubblici[4].

Notiamo inoltre che sul router Roma-ext è stata definita una rotta di default statica per permettere al traffico diretto verso Internet di raggiungere l'ISP, questo implica che è necessario evitare che pacchetti non autorizzati vadano su Internet.

Facendo l'ipotesi che il protocollo di routing OSPF non sia ancora andato a regime, si potrebbe avere il problema che pacchetti diretti verso indirizzi privati aziendali arrivino sul router Roma-ext ma (per la mancanza di una rotta verso la destinazione indicata) vengano inoltrati su Internet (ovviamente senza traduzione degli indirizzi).
Per evitare che la situazione descritta sopra si presenti è necessario definire una ulteriore ACL sul router Roma-ext, applicata all'interfaccia Serial 2/0, in uscita.

La ACL definita per lo scopo avrà il seguente formato:

```
deny ip any Azienda
permit ip any any
```

Dove la sintassi utilizzata è rimasta la stessa.

Notare infatti che i pacchetti che verrebbero diretti su Internet grazie al fatto che OSPF non è ancora andato a regime hanno sempre come indirizzo di destinazione indirizzi aziendali. Se così non fosse sarebbero già stati filtrati in precedenza dai router delle diverse sedi (a meno che non si parli del dominio DA o dei Server globali, che devono poter accedere ad Internet).

Riferirsi alle appendici A.1, A.2, A.3 e A.4 per la configurazione esatta delle ACL.

[4] Il resto degli indirizzi pubblici consentiti dalla maschera, disposibili all'ISP, saranno probabilmente assegnati ad altre aziende sulla medesima rete.

Al fine di garantire un utilizzo minimo di indirizzi IP si è scelto quindi di utilizzare la tecnica del NAT, in particolare un mix di Port Address Translation statico e dinamico.
La comunicazione verso l'esterno da parte dell'azienda è legata esclusivamente ai 7 Global Server ed ai partecipanti del dominio DA.
In particolare i 7 Global Server sono di 3 tipi (Web di cui 3, DNS di cui 2 ed SMTP di cui 2), risulta pertanto conveniente usare il PAT statico dal momento che consente di utilizzare 3 indirizzi IP (il minimo indispensabile) per la gestione dei Server Globali.
Per quanto riguarda la gestione dei partecipanti al dominio DA, si utilizza il PAT dinamico per garantire massima flessibilità sugli indirizzi delle macchine client (ottenuti dinamicamente mediante DHCP), e la traduzione viene fatta su uno dei tre indirizzi pubblici disponibili (scelto dal router stesso).

Notare che l'indirizzo inside global associato ad alcuni dei Server globali della azienda coincide con quello della interfaccia Serial 2/0 del router Roma-ext. Questa scelta è dovuta al fatto che è necessario utilizzare il minimo numero di IP pubblici possibile. Una conseguenza è che se dall'interno della azienda si tenta di accedere ad uno di quei Server utilizzando l'indirizzo pubblico l'accesso viene bloccato in quanto il router si riconosce come destinatario. Questo non costituisce un problema per l'accesso ai Server da Internet, tuttavia è necessario che i dipendenti utilizzino l'indirizzo privato (aziendale) per accedere ai Server (cosa che peraltro deve essere prevista per i domini che non hanno accesso ad Internet).

La configurazione del NAT è stata effettuata presso il router che connette la rete aziendale verso l'esterno (Roma-ext) dal momento che è il router di confine della stub network.
Come già indicato nella sezione sulle ACL, tale router scarta tutti i pacchetti in ingresso da Internet che non hanno come destinazione un IP pubblico aziendale. Viceversa, gli accessi esterni su IP pubblico vengono "filtrati" direttamente dal NAT come segue:

- per i Server globali è garantito l'accesso verso le sole porte / protocolli supportati grazie alla traduzione statica;
- per il dominio DA, è garantita la protezione dall'esterno grazie al fatto che la traduzione dinamica avviene solo su iniziativa delle macchine interne, quindi dall'esterno non è possibile contattare direttamente DA, ma solo dopo che questi ha iniziato il colloquio.

La Tabella 1.14 mette in evidenza la configurazione del NAT.

Tabella NAT router Roma-ext

PAT dinamico	**Città**	**Dominio**	**Source List**	**Pool**
	Roma	DA	permit 172.16.195.64 0.0.0.63 permit 172.16.211.96 0.0.0.31 permit 172.16.227.96 0.0.0.15	213.140.19.100 - 213.140.19.102 netmask 255.255.255.248
	Padova			
	Pisa			
PAT statico	**Città**	**Server**	**Inside Local**	**Inside Global**
	Roma	WEB	IP: 172.16.195.182 PORTA: TCP 80 PORTA: TCP 443	IP: 213.140.19.100 PORTA TCP:80 PORTA: TCP 443
		DNS	IP: 172.16.195.181 PORTA: UDP 53	IP: 213.140.19.100 PORTA: UDP 53
	Padova	WEB	IP: 172.16.211.150 PORTA: TCP 80 PORTA: TCP 443	IP: 213.140.19.101 PORTA: TCP 80 PORTA: TCP 443
		SMTP	IP: 172.16.211.149 PORTA: TCP 25	IP: 213.140.19.101 PORTA: TCP 25
	Pisa	WEB	IP: 172.16.227.134 PORTA: TCP 80 PORTA: TCP 443	IP: 213.140.19.102 PORTA: TCP 80 PORTA: TCP 443
		DNS	IP: 172.16.227.133 PORTA: UDP 53	IP: 213.140.19.102 PORTA: UDP 53
		SMTP	IP: 172.16.227.132 PORTA: TCP 25	IP: 213.140.19.102 PORTA: TCP 25

TAB 1.14

Riferirsi alla appendice A.4 per esaminare in dettaglio la configurazione del NAT sul router Roma-ext.

10. Considerazioni finali

Abbiamo deciso di disabilitare il protocollo CDP su tutti i router presi in considerazione in questa sezione, i motivi di tale scelta sono molteplici e si possono riassumere nei seguenti punti:

- Il protocollo CDP genera overhead (traffico aggiuntivo non utile) sulla rete, e non è necessario per il suo funzionamento.
- Il protocollo CDP distribuisce informazioni riguardo alla rete aziendale su Internet.
- Bisogna evitare che CDP utilizzi inutilmente i collegamenti WAN di backup, infatti questi sono link a tariffazione basata sul traffico.

Qualora la funzione SS ritenesse appropriato attivare CDP su alcuni dispositivi al fine della manutenzione e configurazione, basterà dare l'appropriato comando.

Sotto è riportata la lista dei comandi che l'addetto (della funzione SS) dovrebbe dare per attivare CDP su un dispositivo (router o switch).

```
[accesso]
enable
[digitare la password]
configure terminal
cdp run
end
exit
```

Si danno adesso le informazioni necessarie per la gestione dei dispositivi introdotti fino ad ora.

Quando avviene l'accesso al dispositivo viene visualizzato un messaggio del tipo seguente:

```
Router WWAS <Nome router>: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile
```

Questo assicura che, se qualcuno danneggia la rete in qualunque modo e si riesce a capire di chi è la responsabilità, sia possibile perseguire per legge coloro che hanno causato il danno.

La password da utilizzare per l'accesso tramite telnet (su qualunque interfaccia dei router) e anche tramite console è:

```
class
```

La password da inserire per passare dalla modalità utente alla modalità privilegiata è:

```
cisco
```

Allegata al documento vi è una simulazione della rete che connette le sedi (rete intersede). Date le potenzialità dello strumento utilizzato per la simulazione (Packet Tracer 4.11) e visto che la simulazione deve avvicinarsi all'aspetto funzionale della rete più che agli aspetti di ottimizzazione, vi sono alcune considerazioni da fare.

- Ovviamente le reti delle tre sedi sono del tutto ipotetiche, fare riferimento alle sezioni 2, 3 e 4 per maggiori informazioni al riguardo.
- Le interfacce gigabitEthernet sono state sostituite (al fine della simulazione) con interfacce fastEthernet e i cavi in fibra ottica con semplici cavi in rame di tipo UTP cat 5e.
- Le regole ACL contenenti established (tutte di tipo permit) sono state incluse correttamente nella simulazione, tuttavia Packet Tracer 4.11 ignora la presenza della keyword `established`.
- Si suppone che l'IOS assegni di default la bandwidth pari a 1544 Kbps alle interfacce seriali e 100000 Kbps alle interfaccie fastEthernet.
- In Packet Tracer 4.11 vi sono dei problemi di overload sul NAT tra le traduzioni dinamiche e quelle impostate staticamente se si ricorre alla configurazione riportata in appendice A.4, quindi ai fini della simulazione la traduzione dinamica con overload avviene solamente sul primo dei tre indirizzi pubblici acquistati dalla azienda (quello associato alla interfaccia Serial 2/0 di Roma-ext).

Il file della simulazione è: "`Simulazione_Intersede.pkt`"
Si riporta una immagine della rete simulata, presa direttamente dal programma Packet Tracer 4.11 (figura 1.3).

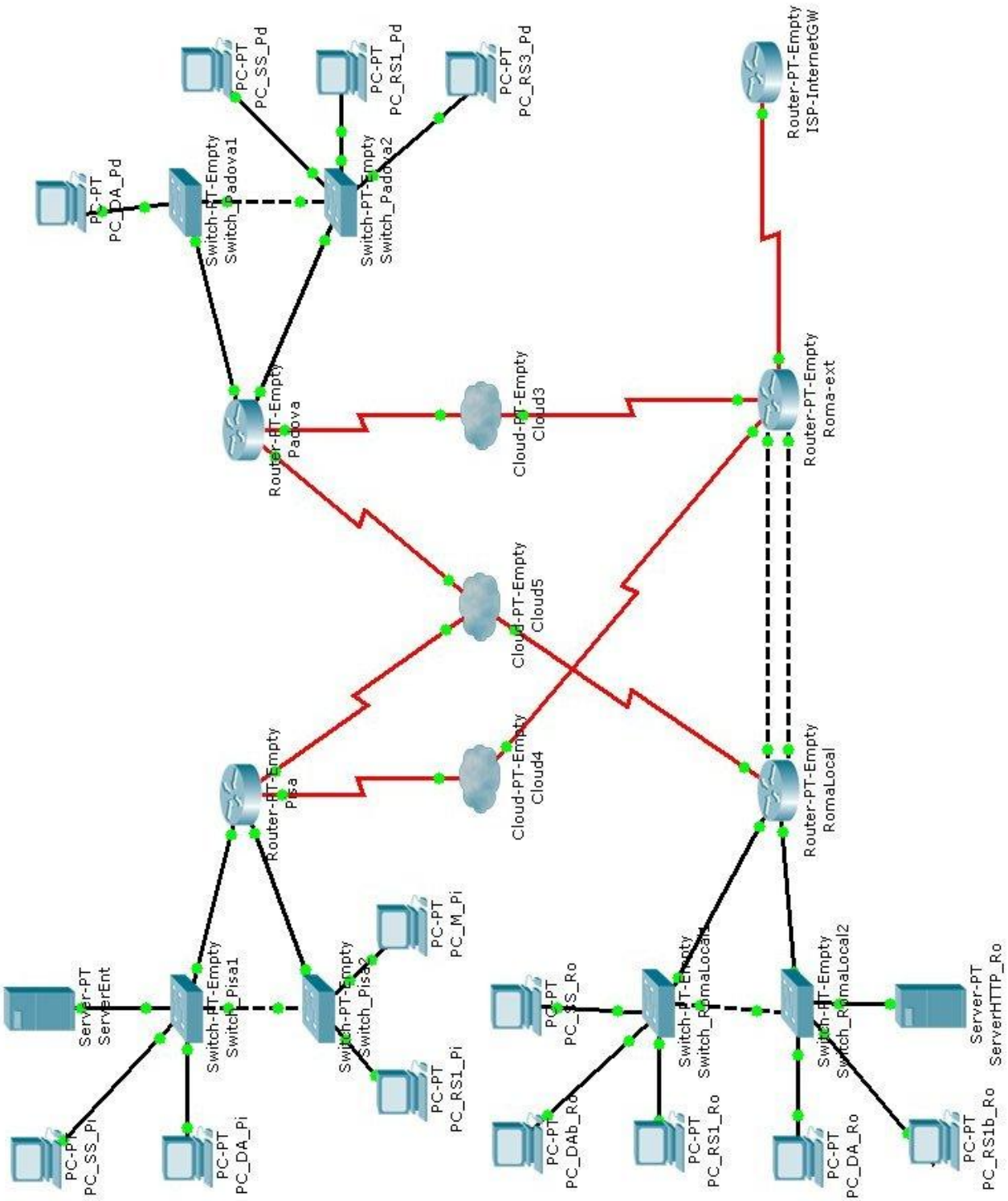


FIG 1.3 SIMULAZIONE INTERSEDE

1. Collocazione Armadi e Cablaggio

Come primo passo nella progettazione della sede di Roma, si vanno ad identificare in modo univoco le stanze presenti al suo interno, per favorire una migliore descrizione dei vari collegamenti delle stanze nelle fasi successive di progetto. Si collocano inoltre i punti di distribuzione della rete.
In particolare, vista la conformazione degli edifici, risulta conveniente collocare:

- 1 MDF, armadio principale, nella struttura centrale in corrispondenza del POP. Il nome assegnato a detta Distribution Facility è Roma_MDF;
- 2 IDF, armadi secondari, uno nella struttura a nord ed un altro nella struttura a sud. I nomi assegnati saranno, rispettivamente, Roma_IDF-Nord e Roma_IDF-Sud.

In figura 2.1 vi è la distribuzione delle stanze per l'edificio centrale, inoltre sono state riportate con colore diverso le stanze scelte per la collocazione dei Server aziendali. Difatti, come vedremo a breve, risulta conveniente porre questi ultimi nel punto più vicino possibile al "cuore" della rete aziendale.

Mappa stanze – Roma Centro

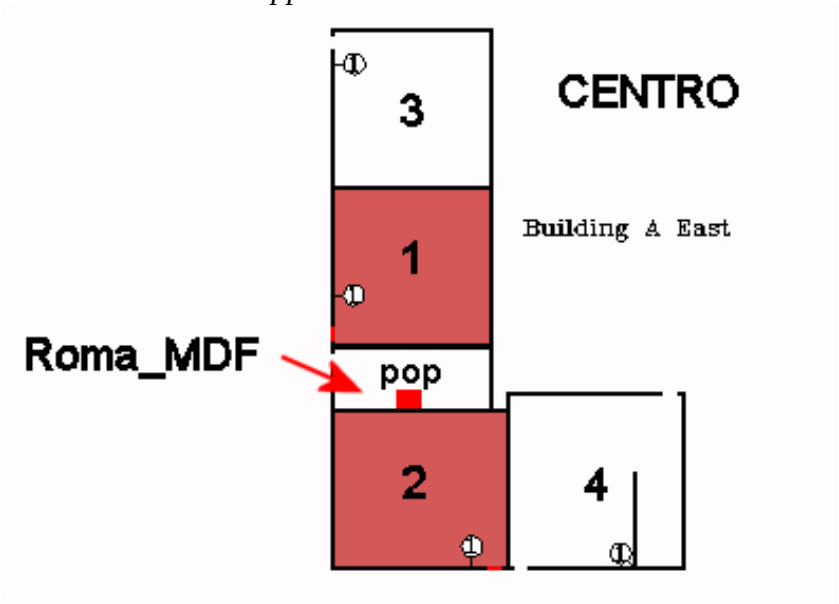


FIG 2.1

Nelle successive figure (da 2.2 a 2.4) troviamo invece la numerazione delle stanze nei restanti edifici della sede di Roma. Si da inoltre la collocazione degli armadi di distribuzione secondari. Vedremo in seguito che la scelta di utilizzare tre Distribution Facilities e collocarle come in queste figure, consente di ottenere cablaggi aderenti con gli standard TIA/EIA-568-B e TIA/EIA-569-A, che prevedono una lunghezza massima di 90 metri per cavi in rame UTP cat. 5e nel caso di cablaggi verticali e/o orizzontali.

Mappa stanze – Roma Nord

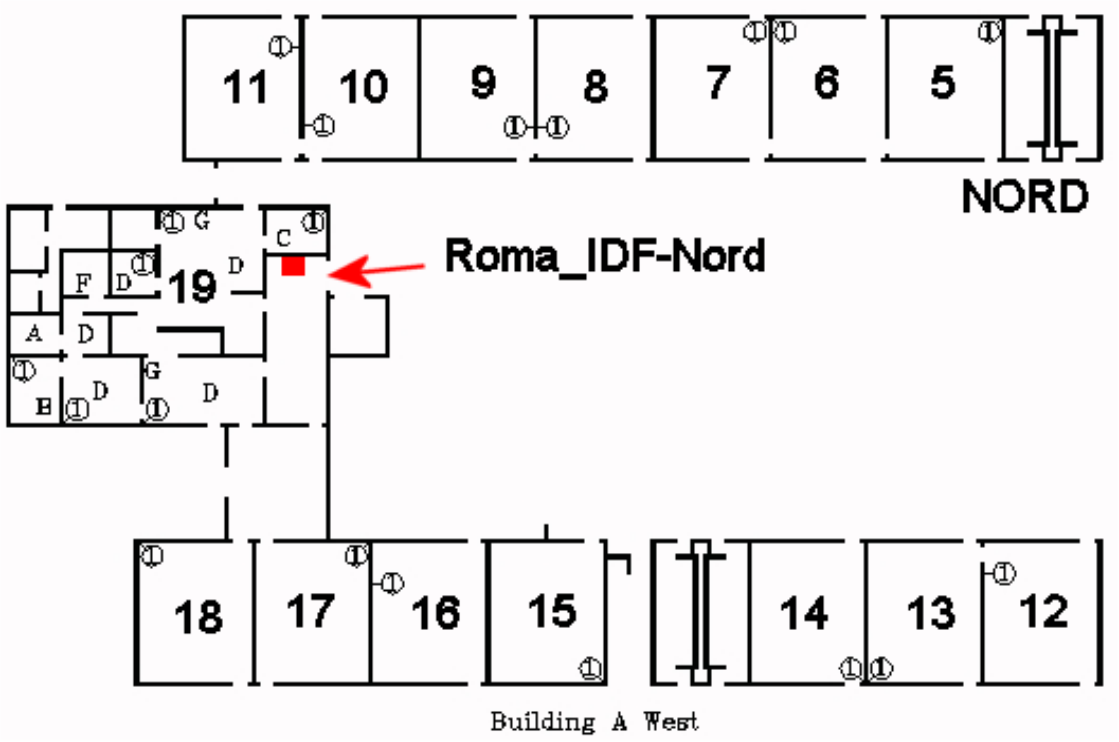


FIG 2.2

Alle stanze più piccole (evidenziate dalla presenza di lettere oltre che numeri) è stato assegnato un unico numero identificativo, dato che il numero totale di postazioni è relativamente basso.

Mappa stanze – Roma Sud

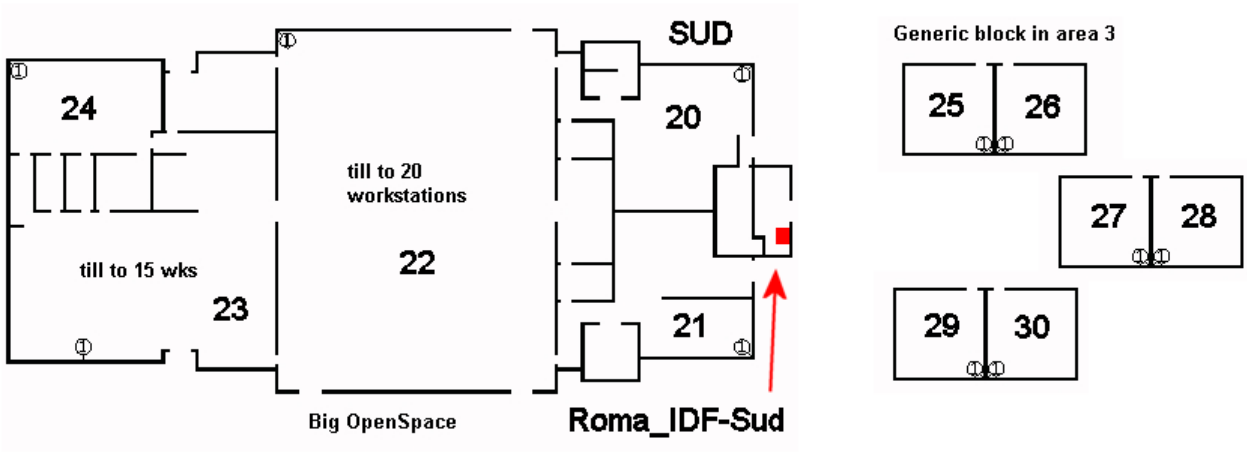


FIG 2.3

All'edificio di sud appartengono, oltre alla parte compresa sulla mappa dettagliata fornita, anche i blocchi presenti nella mappa che era stata fornita per Roma centro. La scelta è dettata semplicemente dal fatto che è molto più semplice raggiungere queste strutture dall' IDF di sud piuttosto che dall' MDF centrale.

La posizione delle Distribution Facilities è stata in ogni caso scelta, per motivi di sicurezza, la dove non sono previste postazioni di lavoro. Un possibile cablaggio verticale che interconnetta fra loro gli xDF è a questo punto riportato in figura 2.4

Mappa fisica – Cablaggio verticale

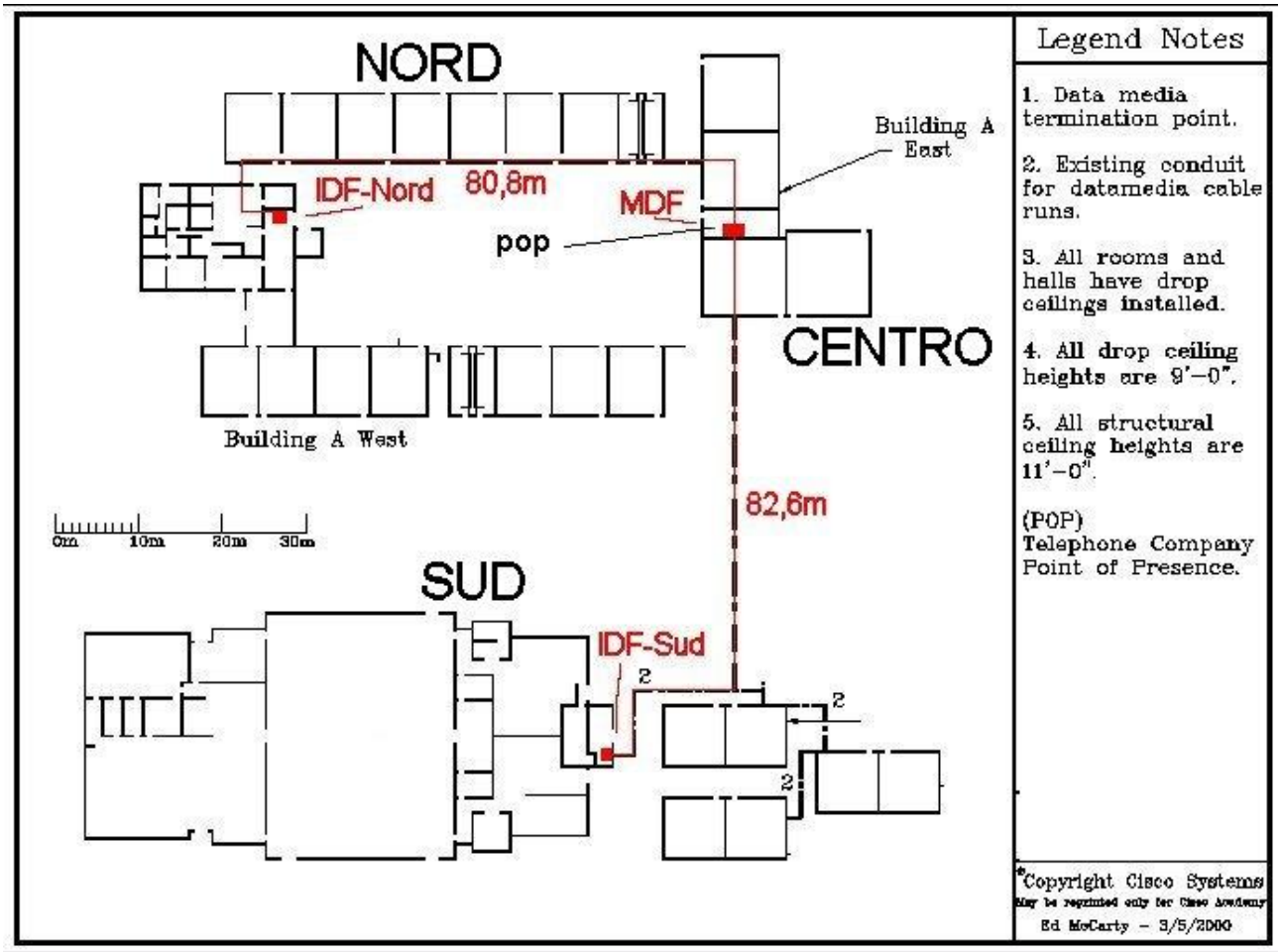


FIG. 2.4

I punti di collocazione degli armadi di rete consentono la stesura di cavi di lunghezza inferiore ai 90m (si faccia riferimento alla figura, eventualmente tenendo conto di un margine di tolleranza del 5% sul calcolo). Questo consente la stesura di cavi UTP cat. 5e, meno costosi di un'eventuale fibra ottica (la scelta non si effettua comunque in questa fase perché dipende dalla banda richiesta).

Con riferimento al cablaggio verticale:

- I cavi verso Roma_IDF-Nord partono dall'armadio di distribuzione principale, salgono lungo una canalina fino a raggiungere la controsoffittatura, da qui si muovono verso il condotto esterno che connette edificio centro e nord, quindi proseguono lungo il controsoffitto fino a raggiungere l'armadio secondario.
- I cavi verso Roma_IDF-Sud partono dall'armadio di distribuzione principale, salgono lungo una canalina fino a raggiungere la controsoffittatura, da qui si muovono verso il condotto esterno che connette edificio centro e nord, quindi proseguono lungo il controsoffitto fino a raggiungere l'armadio secondario.

L' efficacia del posizionamento degli xDF verrà dimostrata in seguito, dopo aver visto per ogni Distribution Facility quali e quanti dispositivi vengono introdotti, oltre al modo in cui questi dispositivi vanno ad interconnettere tutte le macchine terminali previste.

2. Roma_IDF-Nord

L' armadio di rete deve permettere l'interconnessione di tutte le macchine presenti nell'edificio Nord, oltre a fornire connettività verso l'armadio di distribuzione principale.
Si ricorda che, secondo i requisiti di progetto, ogni stanza (ove non indicato esplicitamente) contenente dei Data Media Termination Point, avrà sei postazioni di lavoro e, per ciascuna di esse, quattro prese di rete.
Quindi una stanza generica (ma il discorso può essere facilmente esteso) verrà collegata mediante 6x4 = 24 cavi ad un patch panel (HCC) interno all'armadio di distribuzione. Saranno poi presenti 6 macchine connesse mediante dei patch cord a queste prese di rete, corrispondenti a 6 porte di uno switch per ogni 24 porte del patch panel.
In generale quindi, a parte discorsi di ridondanza dovuti al cablaggio, ogni switch avrà tante porte occupate quante sono le postazioni di lavoro che va ad interconnettere alla rete della sede aziendale.

Vista la specifica funzione di accesso che svolgono questi switch il loro nome sarà del tipo "RomaAccessNordX", con X numero incrementale. Gli switch qui presenti dovranno fornire connettività a 95 postazioni, inoltre dovranno essere previsti dei collegamenti (2 per ogni switch, per questioni di robustezza) verso l' MDF, oltre che verso altri switch della stessa Distribution Facility, sempre per questioni di robustezza.
In particolare si prevede di sfruttare una topologia a ring che interconnetta fra loro i vari switch RomaAccessNord, per cui ogni switch dovrà prevedere due collegamenti verso gli altri switch limitrofi.

Per bilanciare il meglio possibile robustezza e costo, si prevede l'acquisto di switch a 24 porte, dal costo sufficientemente basso da consentire l'acquisto di un loro discreto numero (cosa che va ad incrementare la robustezza della rete).
Dal momento che 4 porte sono occupate per connettere dispositivi intermedi, restano a disposizione delle macchine terminali, 20 porte per ogni switch. Con 5 dispositivi potremmo allora collegare 100 postazioni di lavoro rispetto alle 95 richieste. Tuttavia in previsione di una futura espansione aziendale, si acquista per sicurezza un'ulteriore switch, arrivando così a quota 6.

Una volta deciso il tipo ed il numero degli switch, vanno definiti cavi ed interfacce, che ovviamente dipendono dalla banda minima richiesta.
Per la scelta delle interfacce, il requisito di progetto più stringente è quello che ad ogni postazione di lavoro deve essere garantita una banda di 1Mbps verso i Server aziendali, che come detto sono il più vicino possibile all'MDF, cuore della rete di sede:

- per quanto riguarda il cablaggio orizzontale, ogni postazione è connessa in modo indipendente ad una porta dello switch, quindi interfacce Ethernet 10Mbps sono più che sufficienti;
- per quanto riguarda quello verticale, gli switch presenti in Roma_IDF-Nord vanno ad interconnettere, verso l' MDF, 95 postazioni totali, quindi la banda complessiva, nel caso peggiore in cui tutti i dati viaggino attraverso la stessa interfaccia, deve essere di 95Mbps. Una interfaccia fastEthernet a 100Mbps è dunque sufficiente.

Per questioni di realizzazione fisica risulta altresì conveniente l'acquisto di switch a 24 porte tutte fastEthernet, più che sufficienti per i requisiti di progetto imposti.
Per la scelta dei cavi, bisogna tener presente una possibile crescita aziendale di un fattore 10x (questa scelta non va ad influire sulla scelta dei dispositivi perché si prevede una loro obsolescenza più rapida rispetto a quella del cablaggio), per cui i link di collegamento devono garantire una banda minima di 10Mbps da ogni postazione verso i Server aziendali:

- per quanto riguarda il cablaggio orizzontale, valgono tutte le considerazioni già viste sopra, per cui si prevede la stesura di cavi UTP cat. 5e che non hanno problemi nel supportare una banda di 10Mbps;
- per quanto riguarda il cablaggio verticale, i requisiti di banda salgono a 950Mbps (fattore 10x), tuttavia si ricorda che la velocità massima supportata da cavi in rame UTP cat. 5e è di 1Gbps, quindi sufficiente anche in questo caso. Si ricorda inoltre che tali cavi dovranno essere di tipo crossover, dal momento che vanno ad interconnettere dei dispositivi di tipo intermedio.

Come già evidenziato in fase di cablaggio verticale, la lunghezza dei cavi fra MDF ed IDF-Nord è di 80,8m, quindi visto che sia gli standard di cablaggio TIA/EIA che i requisiti di banda ce lo consentono, si sfruttano per l'interconnessione verticale fra l' MDF e l'IDF-Nord i cavi in rame sopra descritti.
Si può a questo punto verificare la funzionalità nel posizionamento dell'armadio Roma_IDF-Nord, semplicemente andando a vedere se questo consente la stesura dei cavi in rame previsti sopra anche per il cablaggio orizzontale verso le postazioni di lavoro.
Il cablaggio orizzontale verso le postazioni ritenute più remote a partire dall' IDF-Nord è riportato in figura 2.5.

Mappa Fisica – Roma Nord

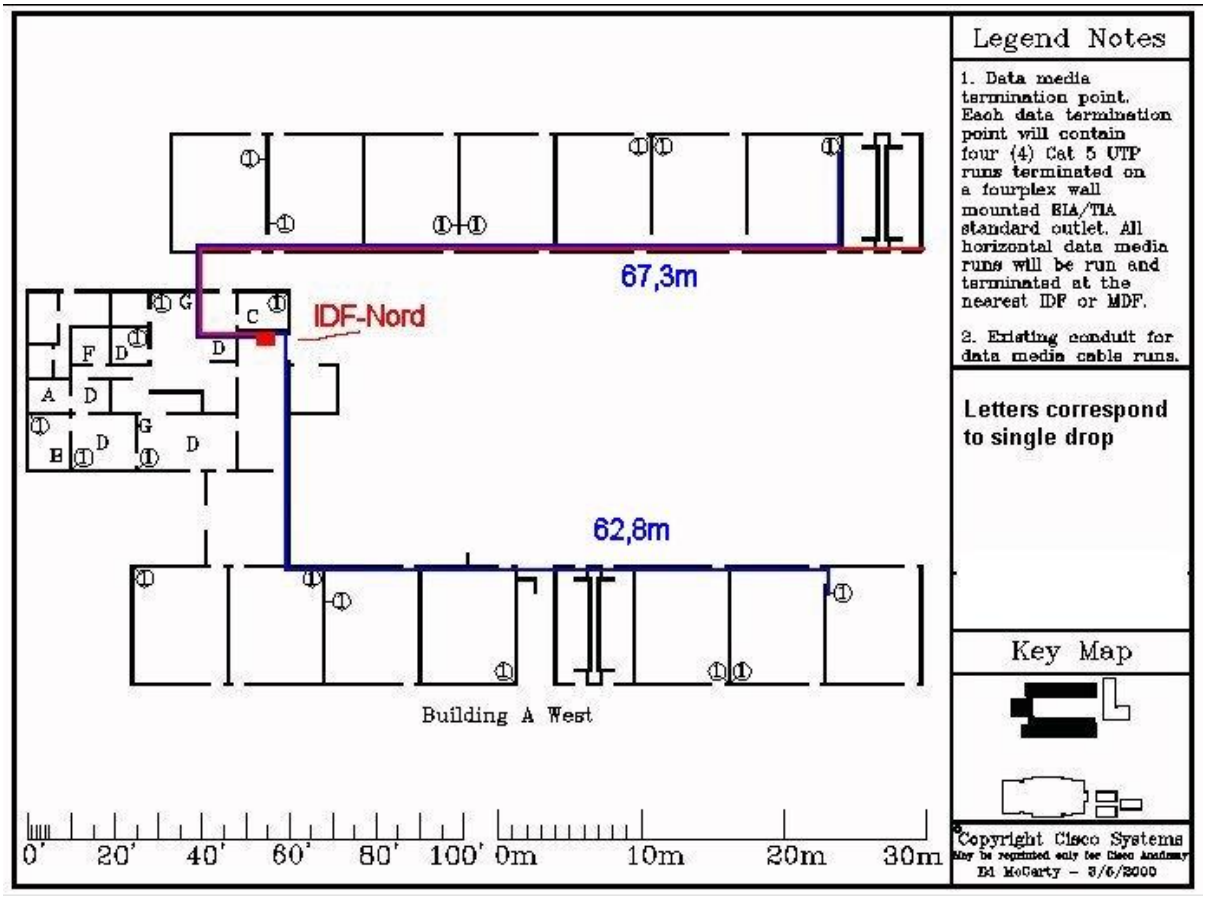


FIG 2.5

Sfruttando ancora una volta la controsoffittatura, la stesura di cavi che interconnettano l'intero edificio nord di Roma non comporta problemi, in quanto un cavo orizzontale può essere al più lungo 67,3 metri: anche considerando una tolleranza del 5% tale lunghezza è di molto inferiore ai 90 metri massimi previsti dagli standard.

Si dà allora, secondo le numerazioni delle stanze già elencate, l'elenco dei dispositivi presenti nella Distribution Facility posta nell' edificio nord della sede di Roma, oltre alle interfacce ed i cavi previsti per le interconnessioni:

1. RomaAccessNord1 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord6;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord2;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 5;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 6.
2. RomaAccessNord2 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord1;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord3;
    - 11 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 19.
3. RomaAccessNord3 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord2;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord4;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 7;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 8;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 9.
4. RomaAccessNord4 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord3;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord5;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 10;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 11;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 18.

5. RomaAccessNord5 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord4;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord6;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 12;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 13;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 14;
6. RomaAccessNord6 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord5;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessNord1;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 15;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 16;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 17.

Si forniscono quindi, per ogni switch, le tabelle che specificano la situazione per ogni interfaccia (TAB da 2.1 fino a 2.6). In particolare per il cablaggio verticale si specifica la porta del patch panel (VCC2) cui è connesso, oltre al nome della rete che identifica per ogni porta del VCC2 a quale porta del VCC1 (patch panel dell'MDF) dovrà essere connesso il cavo steso nella fase di cablaggio verticale. Per il significato della colonna switchport si guardi oltre, per il momento basti sapere che tutte le postazioni terminali hanno in questa colonna il valore "access".

SWITCH ROMAACCESSNORD1

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port1	100M	RomaVCC1/1_ RomaVCC2/1	Trunk
fastEthernet 0/2	To VCC2/Port12	100M	RomaVCC1/13_ RomaVCC2/12	Trunk
fastEthernet 0/3	To RomaAccessNord6	100M	RomaAccessNord6_ RomaAccessNord1	Trunk
fastEthernet 0/4	To RomaAccessNord2	100M	RomaAccessNord1_ RomaAccessNord2	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 5	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 6	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.1

SWITCH ROMAACCESSNORD2

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port2	100M	RomaVCC1/2_ RomaVCC2/2	Trunk
fastEthernet 0/2	To VCC2/Port11	100M	RomaVCC1/14_ RomaVCC2/11	Trunk
fastEthernet 0/3	To RomaAccessNord1	100M	RomaAccessNord1_ RomaAccessNord2	Trunk
fastEthernet 0/4	To RomaAccessNord3	100M	RomaAccessNord2_ RomaAccessNord3	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 19	100M	-	Access
fastEthernet 0/13 - 0/17	To Stanza 19	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.2

SWITCH ROMAACCESSNORD3

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port3	100M	RomaVCC1/3_ RomaVCC2/3	Trunk
fastEthernet 0/2	To VCC2/Port10	100M	RomaVCC1/15_ RomaVCC2/10	Trunk
fastEthernet 0/3	To RomaAccessNord2	100M	RomaAccessNord2_ RomaAccessNord3	Trunk
fastEthernet 0/4	To RomaAccessNord4	100M	RomaAccessNord3_ RomaAccessNord4	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 7	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 8	100M	-	Access
fastEthernet 0/19 – 0/24	To Stanza 9	100M	-	Access

TAB 2.3

SWITCH ROMAACCESSNORD4

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port4	100M	RomaVCC1/4_ RomaVCC2/4	Trunk
fastEthernet 0/2	To VCC2/Port9	100M	RomaVCC1/16_ RomaVCC2/9	Trunk
fastEthernet 0/3	To RomaAccessNord3	100M	RomaAccessNord3_ RomaAccessNord4	Trunk
fastEthernet 0/4	To RomaAccessNord5	100M	RomaAccessNord4_ RomaAccessNord5	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 10	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 11	100M	-	Access
fastEthernet 0/19 – 0/24	To Stanza 18	100M	-	Access

TAB 2.4

SWITCH ROMAACCESSNORD5

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port5	100M	RomaVCC1/5_ RomaVCC2/5	Trunk
fastEthernet 0/2	To VCC2/Port8	100M	RomaVCC1/17_ RomaVCC2/8	Trunk
fastEthernet 0/3	To RomaAccessNord4	100M	RomaAccessNord4_ RomaAccessNord5	Trunk
fastEthernet 0/4	To RomaAccessNord6	100M	RomaAccessNord5_ RomaAccessNord6	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 12	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 13	100M	-	Access
fastEthernet 0/19 – 0/24	To Stanza 14	100M	-	Access

TAB 2.5

SWITCH ROMAACCESSNORD6

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC2/Port6	100M	RomaVCC1/6_ RomaVCC2/6	Trunk
fastEthernet 0/2	To VCC2/Port7	100M	RomaVCC1/18_ RomaVCC2/7	Trunk
fastEthernet 0/3	To RomaAccessNord5	100M	RomaAccessNord5_ RomaAccessNord6	Trunk
fastEthernet 0/4	To RomaAccessNord1	100M	RomaAccessNord6_ RomaAccessNord1	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 15	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 16	100M	-	Access
fastEthernet 0/19 – 0/24	To Stanza 17	100M	-	Access

TAB 2.6

L' armadio di rete deve permettere l'interconnessione di tutte le macchine presenti nell'edificio Sud, oltre a fornire connettività verso l'armadio di distribuzione principale.
Si ricorda che, secondo i requisiti di progetto, ogni stanza (ove non indicato esplicitamente) contenente dei Data Media Termination Point, avrà sei postazioni di lavoro e, per ciascuna di esse, quattro prese di rete.
Quindi una stanza generica (ma il discorso può essere facilmente esteso) verrà collegata mediante 6x4 = 24 cavi ad un patch panel (HCC) interno all'armadio di distribuzione. Saranno poi presenti 6 macchine connesse mediante dei patch cord a queste prese di rete, corrispondenti a 6 porte di uno switch per ogni 24 porte del patch panel.
In generale quindi, a parte discorsi di ridondanza dovuti al cablaggio, ogni switch avrà tante porte occupate quante sono le postazioni di lavoro che va ad interconnettere alla rete della sede aziendale.

Vista la specifica funzione di accesso che svolgono questi switch il loro nome sarà del tipo "RomaAccessSudX", con X numero incrementale. Gli switch qui presenti dovranno fornire connettività a 89 postazioni, inoltre dovranno essere previsti dei collegamenti (2 per ogni switch, per questioni di robustezza) verso l' MDF, oltre che verso altri switch della stessa Distribution Facility, sempre per questioni di robustezza.
In particolare si prevede di sfruttare una topologia a ring che interconnetta fra loro i vari switch RomaAccessSud, per cui ogni switch dovrà prevedere due collegamenti verso altri switch limitrofi.

Per bilanciare il meglio possibile robustezza e costo, si prevede l'acquisto di switch a 24 porte, dal costo sufficientemente basso da consentire l'acquisto di un loro discreto numero di essi (cosa che va ad incrementare la robustezza della rete).
Dal momento che 4 porte sono occupate per connettere dispositivi intermedi, restano a disposizione delle macchine terminali, 20 porte per ogni switch. Con 5 dispositivi potremmo allora collegare 100 postazioni di lavoro rispetto alle 89 richieste. Tuttavia in previsione di una futura espansione aziendale, si acquista per sicurezza un'ulteriore switch, arrivando così a quota 6.

Una volta deciso il tipo ed il numero degli switch, vanno definiti cavi ed interfacce, che ovviamente dipendono dalla banda minima richiesta.
Per la scelta delle interfacce, il requisito di progetto più stringente è quello che ad ogni postazione di lavoro deve essere garantita una banda di 1Mbps verso i Server aziendali, che come detto sono vicini all'MDF, cuore della rete di sede:

- per quanto riguarda il cablaggio orizzontale, ogni postazione è connessa in modo indipendente ad una porta dello switch, quindi interfacce Ethernet 10Mbps sono più che sufficienti;
- per quanto riguarda quello verticale, gli switch presenti in Roma_IDF-Sud vanno ad interconnettere, verso l'MDF, 89 postazioni totali, quindi la banda complessiva, nel caso peggiore in cui tutti i dati passino attraverso la stessa interfaccia, deve essere di 89Mbps. Una interfaccia fastEthernet a 100Mbps è dunque sufficiente.

Per questioni di realizzazione fisica risulta altresì conveniente l'acquisto di switch a 24 porte tutte fastEthernet, più che sufficienti per i requisiti di progetto imposti.
Per la scelta dei cavi, bisogna tener presente una possibile crescita aziendale di un fattore 10x (questa scelta non va ad influire sulla scelta dei dispositivi perché si prevede una loro obsolescenza più rapida rispetto a quella del cablaggio), per cui i link di collegamento devono garantire una banda minima di 10Mbps da ogni postazione verso i Server aziendali:

- per quanto riguarda il cablaggio orizzontale, valgono tutte le considerazioni già viste sopra, per cui si prevede la stesura di cavi UTP cat. 5e che non hanno problemi nel supportare una banda di 10Mbps;
- per quanto riguarda il cablaggio verticale, i requisiti di banda salgono a 890Mbps (fattore 10x), tuttavia si ricorda che la velocità massima supportata da cavi in rame UTP cat. 5e è di 1Gbps, quindi sufficiente anche in questo caso. Si ricorda inoltre che tali cavi dovranno essere di tipo crossover, dal momento che vanno ad interconnettere dei dispositivi di tipo intermedio.

Come già evidenziato in fase di cablaggio verticale, la lunghezza dei cavi fra MDF ed IDF-Sud è di 82,6m, quindi visto che sia gli standard di cablaggio TIA/EIA che i requisiti di banda ce lo consentono, si sfruttano per l'interconnessione verticale fra l'MDF e l'IDF-Sud i cavi in rame sopra descritti.
Si può a questo punto verificare la funzionalità nel posizionamento dell'armadio Roma_IDF-Sud, semplicemente andando a vedere se questo consente la stesura dei cavi in rame previsti sopra anche per il cablaggio verticale verso le postazioni di lavoro.
Il cablaggio orizzontale verso le postazioni ritenute più remote a partire dall' IDF-Sud è riportato in figura 2.6.

Mappa Fisica – Roma Sud

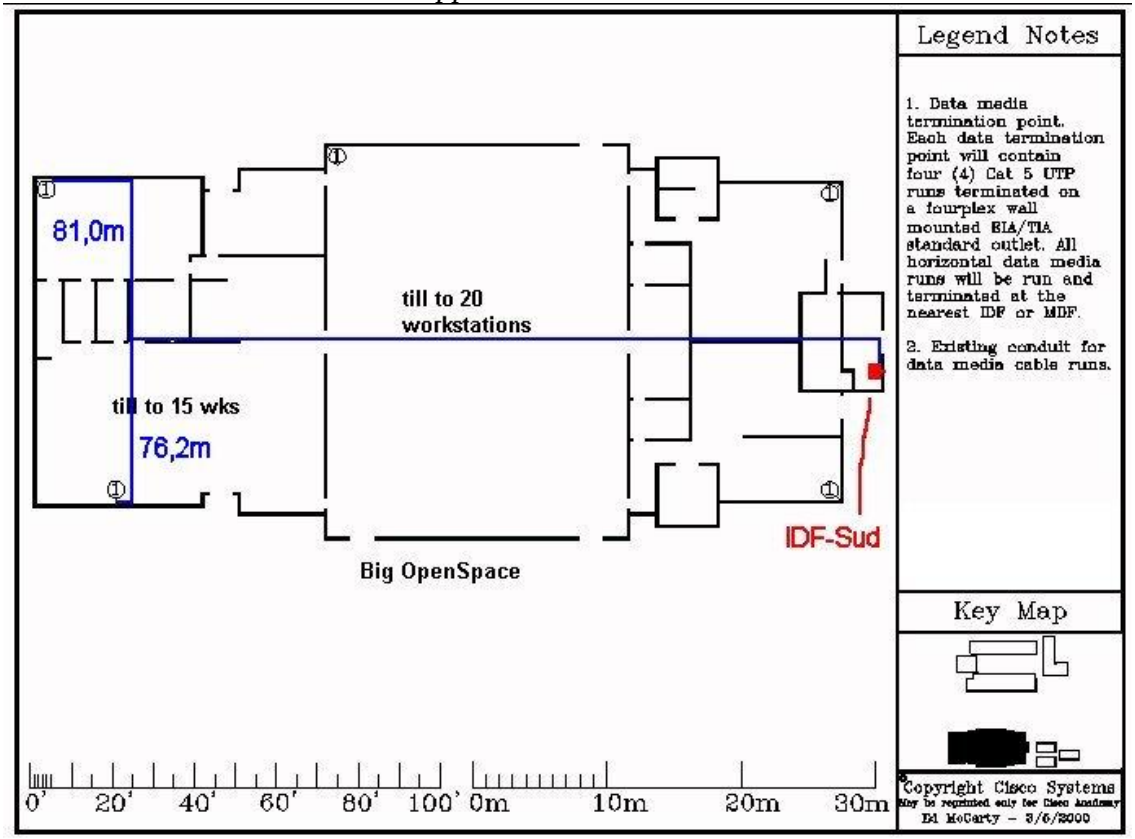


FIG 2.6

Su Roma Sud, il cablaggio orizzontale è ancora possibile, ma va scelto accuratamente il percorso dei cavi. Nell'esempio di figura, si fanno procedere i cavi lungo il controsoffitto tagliando la struttura più o meno al centro. In questo modo con circa 80 metri di cavo (più la solita tolleranza del 5%) è possibile connettere efficacemente le postazioni più remote.

Si dà allora, secondo le numerazioni delle stanze già elencate, l'elenco dei dispositivi presenti nella Distribution Facility posta nell' edificio nord della sede di Roma, oltre alle interfacce ed i cavi previsti per le interconnessioni:

1. RomaAccessSud1 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud6;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud2;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 20;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 21;
    - 5 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 22;
2. RomaAccessSud2 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud1;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud3;
    - 15 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 22.
    - 3 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 23.
3. RomaAccessSud3 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud2;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud4;
    - 12 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 23;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 24;
4. RomaAccessSud4 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud3;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud5;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 25;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 26;
5. RomaAccessSud5 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud4;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud6;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 27;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 28;

6. RomaAccessSud6 (tutto su fastEthernet)
    - 2 cavi UTP cat. 5e crossover verso l'MDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud5;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessSud1;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 29;
    - 6 cavi UTP cat. 5e straight-through verso il patch panel che interconnette la stanza numero 30;

Si forniscono quindi, per ogni switch, le tabelle che specificano la situazione per ogni interfaccia (TAB da 2.7 fino a 2.12). In particolare per il cablaggio verticale si specifica la porta del patch panel (VCC3) cui è connesso, oltre al nome della rete che identifica per ogni porta del VCC3 a quale porta del VCC1 (patch panel dell'MDF) dovrà essere connesso il cavo steso nella fase di cablaggio verticale. Per il significato della colonna switchport si guardi oltre, per il momento basti sapere che tutte le postazioni terminali hanno in questa colonna il valore "access".

SWITCH ROMAACCESSSUD1

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port1	100M	RomaVCC1/7_ RomaVCC3/1	Trunk
fastEthernet 0/2	To VCC3/Port12	100M	RomaVCC1/19_ RomaVCC3/12	Trunk
fastEthernet 0/3	To RomaAccessSud6	100M	RomaAccessSud6_ RomaAccesSud1	Trunk
fastEthernet 0/4	To RomaAccessSud2	100M	RomaAccessSud1_ RomaAccessSud2	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 20	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 21	100M	-	Access
fastEthernet 0/19 – 0/23	To Stanza 22	100M	-	Access
fastEthernet 0/24	Inutilizzata	100M	-	-

TAB 2.7

SWITCH ROMAACCESSSUD2

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port2	100M	RomaVCC1/8_ RomaVCC3/2	Trunk
fastEthernet 0/2	To VCC3/Port11	100M	RomaVCC1/20_ RomaVCC3/11	Trunk
fastEthernet 0/3	To RomaAccessSud1	100M	RomaAccessSud1_ RomaAccessSud2	Trunk
fastEthernet 0/4	To RomaAccessSud3	100M	RomaAccessSud2_ RomaAccessSud3	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/21	To Stanza 22	100M	-	Access
fastEthernet 0/22 - 0/24	To Stanza 23	100M	-	Access

TAB 2.8

SWITCH ROMAACCESSSUD3

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port3	100M	RomaVCC1/9_ RomaVCC3/3	Trunk
fastEthernet 0/2	To VCC3/Port10	100M	RomaVCC1/21_ RomaVCC3/10	Trunk
fastEthernet 0/3	To RomaAccessSud2	100M	RomaAccessSud2_ RomaAccessSud3	Trunk
fastEthernet 0/4	To RomaAccessSud4	100M	RomaAccessSud3_ RomaAccessSud4	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/18	To Stanza 23	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 24	100M	-	Access

TAB 2.9

SWITCH ROMAACCESSSUD4

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port4	100M	RomaVCC1/10_ RomaVCC3/4	Trunk
fastEthernet 0/2	To VCC3/Port9	100M	RomaVCC1/22_ RomaVCC3/9	Trunk
fastEthernet 0/3	To RomaAccessSud3	100M	RomaAccessSud3_ RomaAccessSud4	Trunk
fastEthernet 0/4	To RomaAccessSud5	100M	RomaAccessSud4_ RomaAccessSud5	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 25	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 26	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.10

SWITCH ROMAACCESSSUD5

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port5	100M	RomaVCC1/11_ RomaVCC3/5	Trunk
fastEthernet 0/2	To VCC3/Port8	100M	RomaVCC1/23_ RomaVCC3/8	Trunk
fastEthernet 0/3	To RomaAccessSud4	100M	RomaAccessSud4_ RomaAccessSud5	Trunk
fastEthernet 0/4	To RomaAccessSud6	100M	RomaAccessSud5_ RomaAccessSud6	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 27	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 28	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.11

SWITCH ROMAACCESSSUD6

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To VCC3/Port6	100M	RomaVCC1/12_ RomaVCC3/6	Trunk
fastEthernet 0/2	To VCC3/Port7	100M	RomaVCC1/24_ RomaVCC3/7	Trunk
fastEthernet 0/3	To RomaAccessSud5	100M	RomaAccessSud5_ RomaAccessSud6	Trunk
fastEthernet 0/4	To RomaAccessSud1	100M	RomaAccessSud6_ RomaAccessSud1	Trunk
fastEthernet 0/5 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 29	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 30	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.12

E’ stata così definita l’intera topologia logica degli armadi di distribuzione secondari posti negli edifici nord e sud della sede di Roma.
I risultati ottenuti sono riassunti schematicamente nella mappa logica di figura 2.7.

Mappa Logica – Roma Nord e Sud

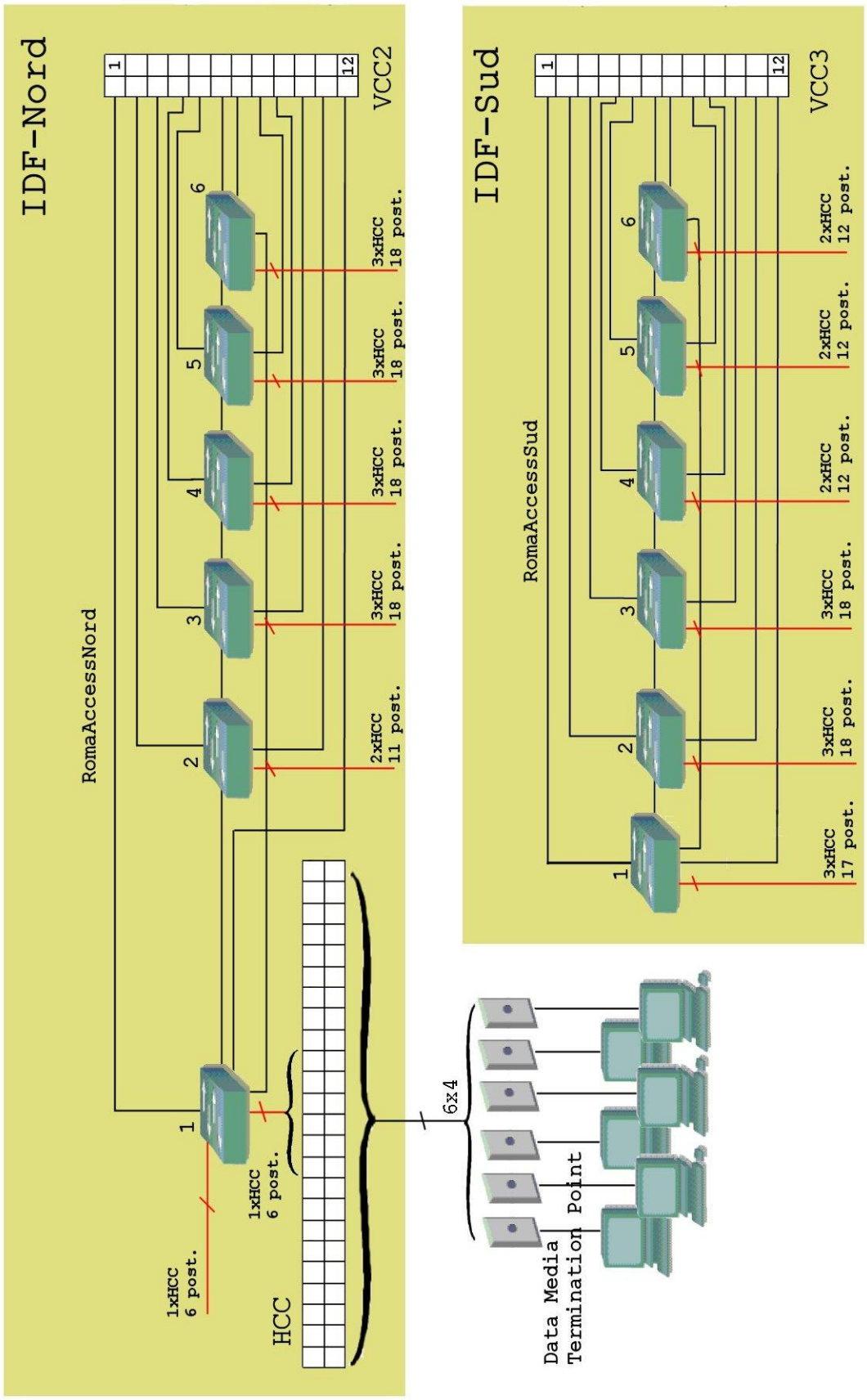


FIG 2.7

L' armadio di rete principale, oltre a permettere l'interconnessione di tutte le macchine presenti nell'edificio centrale (fra cui i Server aziendali), deve collegare anche gli armadi secondari e la rete dell'intera azienda a quella della singola sede. Inoltre nella sede di Roma deve essere presente anche il router Roma-ext, che consente la connessione ad Internet.
In questo caso oltre alle due stanze (3 e 4) per cui vale il discorso delle 6 postazioni già visto nelle sezioni nord e sud, nelle stanze 1 e 2 sono presenti i Server aziendali, 24 per ogni stanza.

In particolare a livello dell'MDF, la funzione di interconnessione con le macchine terminali è ben distinta da quella di collegamento con gli IDF e con la rete aziendale.
Progettando la rete secondo un modello gerarchico, buona norma per ottenere proprietà di efficienza ed efficacia della rete, si distinguono tre livelli:

- Livello core: backbone di switching ad alta velocità
- Livello distribution: definizione di domini
- Livello access: connessione delle macchine terminali

Nel nostro caso la rete risulta non eccessivamente estesa, per cui una configurazione più snella prevede di affidare al router di frontiera la funzione del livello distribuzione (definizione dei domini, regole di accesso, inter-VLAN routing) e quindi suddividere le funzioni di switching nei livelli core ed access.
In particolare tutti gli switch presenti negli IDF sono di tipo access (come si può intuire anche dal nome scelto) perché si occupano dell' interconnessione di macchine terminali.
A livello dell' MDF useremo ancora una volta switch di livello access per l' interconnessione di macchine terminali, e switch di livello core per collegare fra loro tutti gli switch di livello access. Gli switch di livello core saranno infine interconnessi con il router di frontiera RomaLocal.

Per quanto riguarda i Server, si adotta la scelta di posizionarli sugli switch a livello core invece che su quelli a livello access, dal momento che la maggior parte del traffico è destinato a loro e la banda disponibile calerebbe se li si andasse ad annidare sotto ulteriori livelli gerarchici.

Lo switch di livello access previsto nell'MDF è uno solo, di nome RomaAccessCentral1. Tale switch dovrà fornire connettività a 12 postazioni e, seguendo i ragionamenti visti per gli altri switch access, uno switch di 24 porte fastEthernet collegato mediante cavi UTP cat. 5e è più che sufficiente per i nostri scopi.

Per il livello core si prevede viceversa l'acquisto di due switch (come già visto nella sezione 1, questa scelta garantisce maggior robustezza e miglior divisione di carico).
Vista la loro funzione i loro nomi saranno RomaCore1 e RomaCore2.
Ciascun switch sarà connesso ad ogni switch di livello access presente nella rete (ridondanza che consente di ottenere un notevole incremento di robustezza), per un totale di 13 collegamenti per ogni switch di livello core. Entrambi gli switch saranno inoltre connessi ad un'interfaccia del router, e per irrobustire ulteriormente la struttura saranno connessi fra di loro con due cavi su due interfacce. Infine ciascuno switch sarà connesso a 24 dei 48 server aziendali.
Si noti in proposito, che la connessione fra i due switch di livello core è essenziale per il corretto funzionamento della rete, dal momento che il router "parla" con uno solo di loro a seconda della VLAN di appartenenza del pacchetto. Tuttavia la ridondanza introdotta nei collegamenti consente eventuali percorsi fra i due switch core attraverso switch di livello access. Questo consente alla rete di continuare a funzionare anche nel caso di rottura dei link diretti fra gli switch core, tuttavia ne riduce notevolmente le prestazioni. Per questo motivo il collegamento fra gli switch di livello core è doppio.

Il minimo numero di porte richiesto è dunque pari a :
24 (server) + 13 (access) + 2 (core) + 1 (router) = 40 porte.

I dispositivi scelti per il livello access, risultano dunque non efficaci per il livello core.
Prima di addentrarsi nella scelta dei dispositivi per questo livello, vanno definiti cavi ed interfacce richieste, in conseguenza della necessità di banda.
Per la scelta delle interfacce, il requisito di progetto più stringente è quello che ad ogni postazione di lavoro deve essere garantita una banda di 1Mbps verso i Server aziendali:

- per quanto riguarda il cablaggio di tutti gli switch di livello access (IDF e RomaCentralAccess1) vale il discorso già fatto, per cui interfacce fastEthernet a 100Mbps sono sufficienti;
- per quanto riguarda il cablaggio dei Server aziendali, ogni switch di livello core può potenzialmente accumulare il traffico di tutte le postazioni presenti nella sede. In totale ho un numero di postazioni pari a: 95 (nord) + 89 (sud) + 12 (centro senza i Server) = 192. La banda disponibile deve quindi essere pari a 192Mbps, per cui sono necessarie interfacce di tipo gigabitEthernet;
- per quanto riguarda il cablaggio fra gli switch del livello core stesso e con il router, bisogna prevedere gli stessi requisiti di banda che hanno i Server, dal momento che questi ultimi non appartengono necessariamente allo stesso dominio di sicurezza della postazione che vi accede, e quindi il traffico va smistato tramite router.
  In realtà il discorso potrebbe cambiare tenendo conto dell'esistenza di Workgroup Server, tuttavia dai requisiti di progetto si desume che il numero di tali Server è altamente variabile, cosa che non consente di fare stime precise sulla riduzione dei requisiti di banda. Nel caso peggiore non è comunque possibile ridurre i requisiti rispetto a quelli attualmente imposti.

Per la scelta dei cavi, bisogna tener presente una possibile crescita aziendale di un fattore 10x (questa scelta non va ad influire sulla scelta dei dispositivi perché si prevede una loro obsolescenza più rapida rispetto a quella del cablaggio), per cui i link di collegamento devono garantire una banda minima di 10Mbps da ogni postazione verso i Server aziendali:

- per quanto riguarda il cablaggio di tutti gli switch di livello access (IDF e RomaCentralAccess1) vale il discorso già fatto, per cui cavi in rame UTP cat. 5e sono più che sufficienti;
- per quanto riguarda il cablaggio dei Server aziendali, i requisiti di banda salgono a 1920Mbps (fattore 10x), per cui si rendono necessari cablaggi in fibra ottica;
- per quanto riguarda il cablaggio fra gli switch del livello core stesso e con il router, vale il discorso visto in relazione alla banda necessaria verso i Server, per cui si rende necessario un cablaggio in fibra ottica.

Si metterà dunque in preventivo l'acquisto dei seguenti componenti:

- Cavi in fibra ottica. In particolare si utilizza lo standard 1000Base-SX su fibra multimodale, che consente di raggiungere alte velocità su percorsi relativamente brevi (tali sono quelli che interconnettono l'MDF con le stanze dei server)
- Due switch di livello core, costituiti da (i moduli scelti riflettono il fatto che il progetto dovrà essere in seguito fisicamente realizzabile):
  - Un modulo fastEthernet a 24 porte compatibile con lo standard 1000Base-T;
  - Un modulo gigabitEthernet a 48 porte compatibile con lo standard 1000Base-SX.

A partire dall' MDF è possibile cablare senza alcuna difficoltà tutto l'edificio della zona centrale, come si desume dalla figura 2.8.

Mappa Fisica – Roma Centro

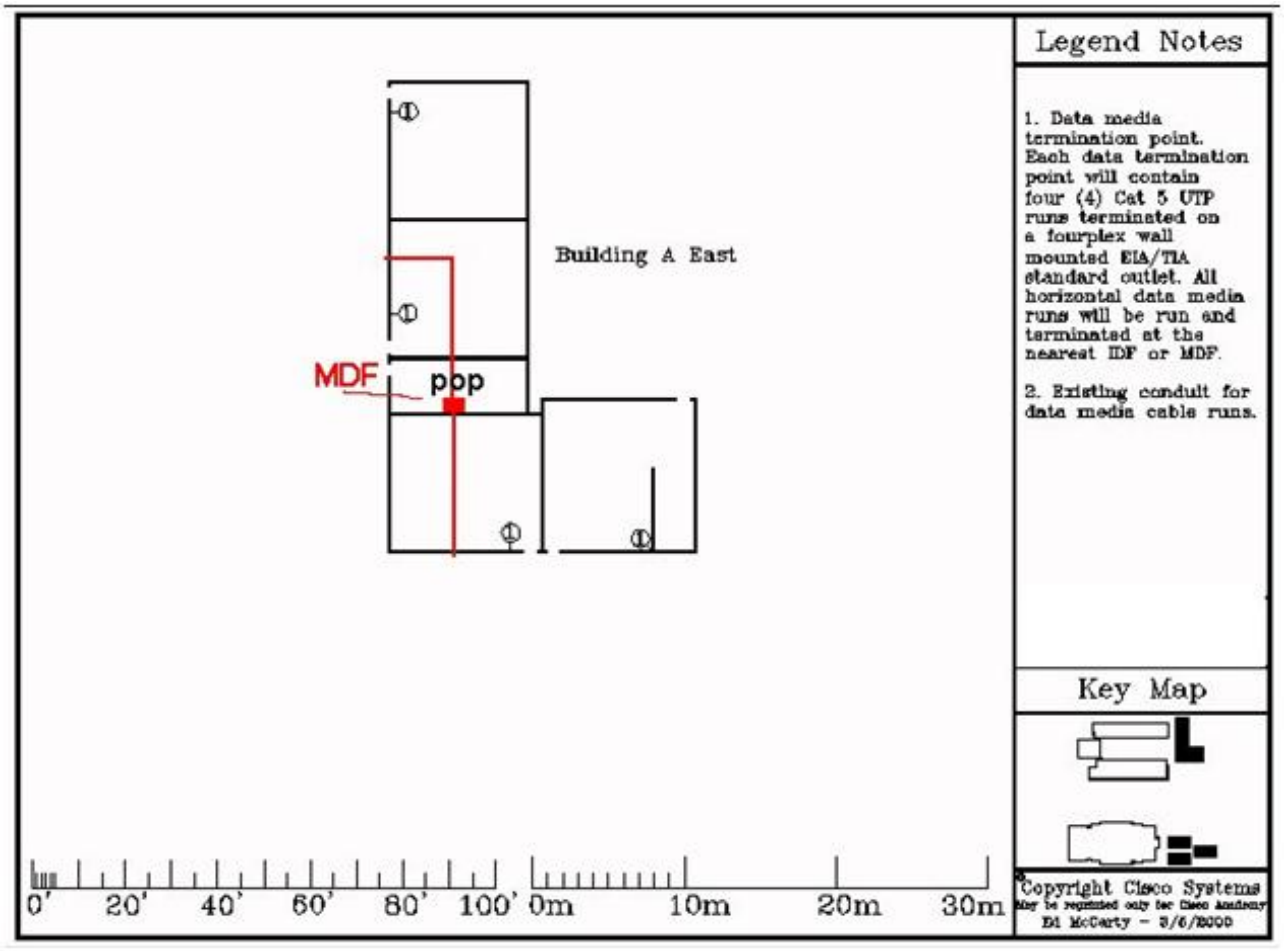


FIG 2.8

Si dà allora, secondo le numerazioni delle stanze già elencate, l'elenco dei dispositivi presenti nella Distribution Facility posta nell' edificio centrale della sede di Roma, oltre alle interfacce ed i cavi previsti per le interconnessioni:

1. Router Roma-ext
   - 1 cavo seriale per l'interconnessione con l'ISP;
   - 2 cavi seriali per l'interconnessione con le sedi di Pisa e Padova;
   - 2 cavi UTP cat. 5e crossover su interfacce fastEthernet per l'interconnessione con il router RomaLocal.
2. Router RomaLocal
   - 1 cavo seriale per l'interconnessione di Backup con le sedi di Pisa e Padova;
   - 2 cavi UTP cat. 5e crossover su interfacce fastEthernet per l'interconnessione con il router Roma-ext;
   - 2 cavi in fibra multimodale su interfacce gigabitEthernet per l'interconnessione con gli switch RomaCore.

3. RomaCore1
    - 1 cavo in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con il router RomaLocal;
    - 2 cavi in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con lo switch RomaCore2;
    - 24 cavi in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con i Server aziendali (Stanza 1);
    - 12 cavi UTP cat. 5e crossover verso gli IDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessCentral1;
4. RomaCore2
    - 1 cavo in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con il router RomaLocal;
    - 2 cavi in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con lo switch RomaCore1;
    - 24 cavi in fibra multimodale su interfaccia gigabitEthernet per l'interconnessione con i Server aziendali (Stanza 2);
    - 12 cavi UTP cat. 5e crossover verso gli IDF;
    - 1 cavo UTP cat. 5e crossover verso RomaAccessCentral1;

Si forniscono quindi, per ogni switch, le tabelle che specificano la situazione per ogni interfaccia (TAB da 2.13 fino a 2.15). In particolare per il cablaggio verticale si specifica la porta del patch panel (VCC1) cui è connesso, oltre al nome della rete che identifica per ogni porta del VCC1 a quale porta degli altri VCC (patch panel degli IDF) dovrà essere connesso il cavo steso nella fase di cablaggio verticale. Per il significato della colonna switchport si guardi oltre, per il momento basti sapere che tutte le postazioni terminali hanno in questa colonna il valore "access".

SWITCH ROMAACCESSCENTRAL1

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To RomaCore1	100M	RomaCore1_ RomaAccesCentral1	Trunk
fastEthernet 0/2	To RomaCore2	100M	RomaCore2_ RomaAccesCentral1	Trunk
fastEthernet 0/3 - 0/6	Inutilizzate	100M	-	-
fastEthernet 0/7 - 0/12	To Stanza 3	100M	-	Access
fastEthernet 0/13 - 0/18	To Stanza 4	100M	-	Access
fastEthernet 0/19 – 0/24	Inutilizzate	100M	-	-

TAB 2.13

SWITCH ROMACORE1

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To RomaCentral Access1	100M	RomaCore1_ RomaCentral Access1	Trunk
fastEthernet 0/2	To VCC1/Port1	100M	RomaVCC1/1_ RomaVCC2/1	Trunk
fastEthernet 0/3	To VCC1/Port2	100M	RomaVCC1/2_ RomaVCC2/2	Trunk
fastEthernet 0/4	To VCC1/Port3	100M	RomaVCC1/3_ RomaVCC2/3	Trunk
fastEthernet 0/5	To VCC1/Port4	100M	RomaVCC1/4_ RomaVCC2/4	Trunk
fastEthernet 0/6	To VCC1/Port5	100M	RomaVCC1/5_ RomaVCC2/5	Trunk
fastEthernet 0/7	To VCC1/Port6	100M	RomaVCC1/6_ RomaVCC2/6	Trunk
fastEthernet 0/8	To VCC1/Port7	100M	RomaVCC1/7_ RomaVCC3/1	Trunk
fastEthernet 0/9	To VCC1/Port8	100M	RomaVCC1/8_ RomaVCC3/2	Trunk
fastEthernet 0/10	To VCC1/Port9	100M	RomaVCC1/9_ RomaVCC3/3	Trunk
fastEthernet 0/11	To VCC1/Port10	100M	RomaVCC1/10_ RomaVCC3/4	Trunk
fastEthernet 0/12	To VCC1/Port11	100M	RomaVCC1/11_ RomaVCC3/5	Trunk
fastEthernet 0/13	To VCC1/Port12	100M	RomaVCC1/12_ RomaVCC3/6	Trunk
fastEthernet 0/14 – 0/24	Inutilizzate	100M	-	-
gigabitEthernet 1/1	To Router RomaLocal	1G	RomaCore1_ RomaLocal	Trunk
gigabitEthernet 1/2	To RomaCore2	1G	RomaCore1_ RomaCore2	Trunk
gigabitEthernet 1/3	To RomaCore2	1G	RomaCore1_ RomaCore2 (b)	Trunk
gigabitEthernet 1/4 – 1/27	To Server (Stanza 1)	1G	-	Access
gigabitEthernet 1/28 – 1/48	Inutilizzate	1G	-	-

TAB 2.14

SWITCH ROMACORE2

Interfaccia	Descrizione	Velocità	Nome Rete	Switchport
fastEthernet 0/1	To RomaCentral Access1	100M	RomaCore2_ RomaCentral Access1	Trunk
fastEthernet 0/2	To VCC1/Port13	100M	RomaVCC1/13_ RomaVCC2/12	Trunk
fastEthernet 0/3	To VCC1/Port14	100M	RomaVCC1/14_ RomaVCC2/11	Trunk
fastEthernet 0/4	To VCC1/Port15	100M	RomaVCC1/15_ RomaVCC2/10	Trunk
fastEthernet 0/5	To VCC1/Port16	100M	RomaVCC1/16_ RomaVCC2/9	Trunk
fastEthernet 0/6	To VCC1/Port17	100M	RomaVCC1/17_ RomaVCC2/8	Trunk
fastEthernet 0/7	To VCC1/Port18	100M	RomaVCC1/18_ RomaVCC2/7	Trunk
fastEthernet 0/8	To VCC1/Port19	100M	RomaVCC1/19_ RomaVCC3/12	Trunk
fastEthernet 0/9	To VCC1/Port20	100M	RomaVCC1/20_ RomaVCC3/11	Trunk
fastEthernet 0/10	To VCC1/Port21	100M	RomaVCC1/21_ RomaVCC3/10	Trunk
fastEthernet 0/11	To VCC1/Port22	100M	RomaVCC1/22_ RomaVCC3/9	Trunk
fastEthernet 0/12	To VCC1/Port23	100M	RomaVCC1/23_ RomaVCC3/8	Trunk
fastEthernet 0/13	To VCC1/Port24	100M	RomaVCC1/24_ RomaVCC3/7	Trunk
fastEthernet 0/14 – 0/24	Inutilizzate	100M	-	-
gigabitEthernet 1/1	To Router RomaLocal	1G	RomaCore1_ RomaLocal	Trunk
gigabitEthernet 1/2	To RomaCore1	1G	RomaCore1_ RomaCore2	Trunk
gigabitEthernet 1/3	To RomaCore1	1G	RomaCore1_ RomaCore2 (b)	Trunk
gigabitEthernet 1/4 – 1/27	To Server (Stanza 2)	1G	-	Access
gigabitEthernet 1/28 – 1/48	Inutilizzate	1G	-	-

TAB 2.15

Le tabelle elencate mostrano i collegameti fra gli switch degli IDF e quelli dell'MDF mettendo in evidenza per ogni interfaccia la porta sul patch panel (VCC) cui è connessa. Per capire quindi ad ogni switch access quali interfacce degli switch core sono associate basta incrociare le tabelle, in particolare sfruttando il nome della rete, che è univoco.
Si noti il fatto che il cablaggio verticale fra i patch panel relativo a RomaCore2 è "incrociato", cioè ad una porta "bassa" del VCC1 corrisponde una porta "alta" dei VCC2/3 (es. alla VCC1/Port13 corrisponde la VCC2/Port12).
La mappa logica dell'MDF e quella globale, sono presentate nelle figure 2.9 e 2.10.

Mappa Logica – Roma Centro

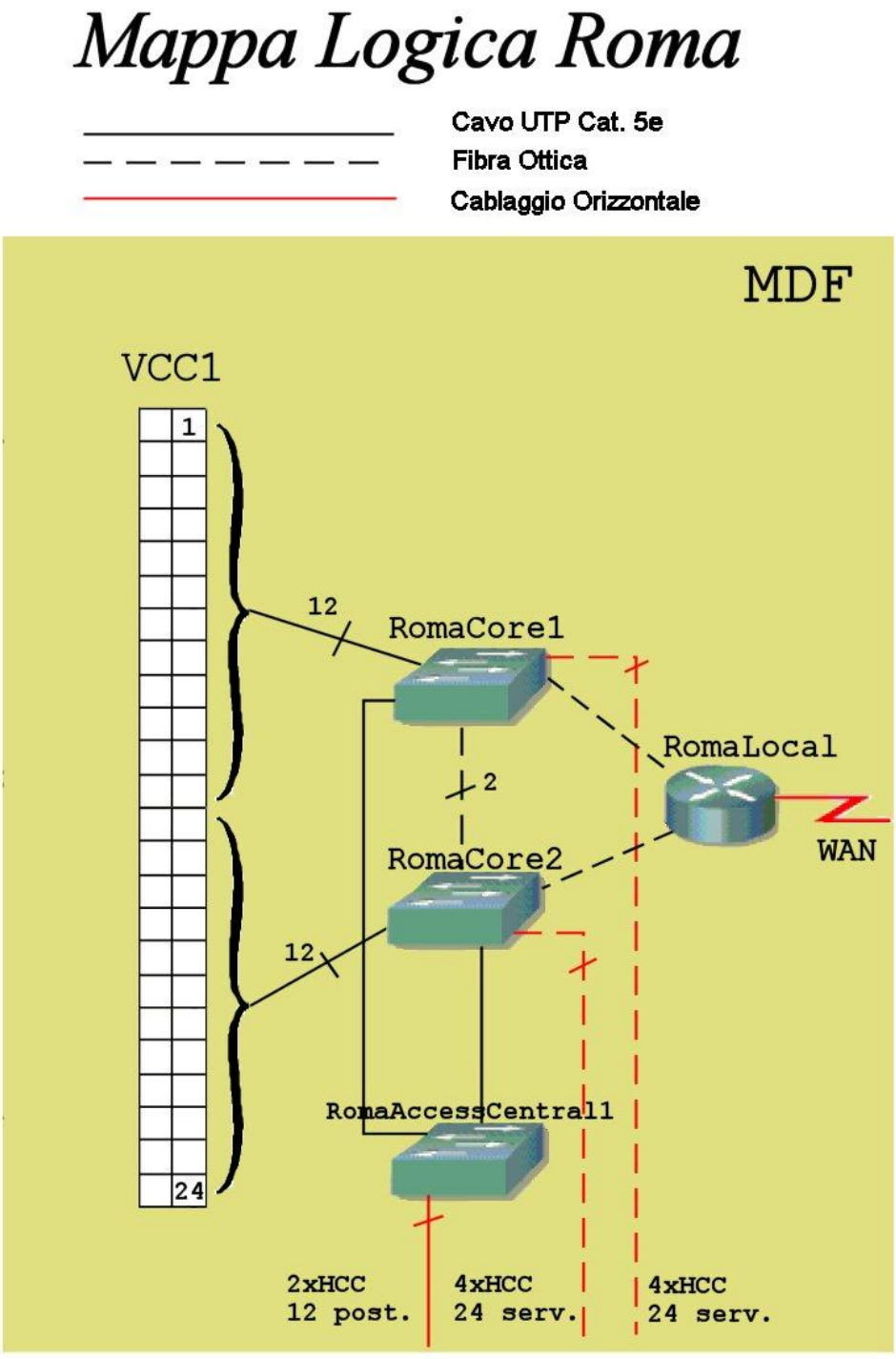


FIG 2.9

Mappa Logica – Roma

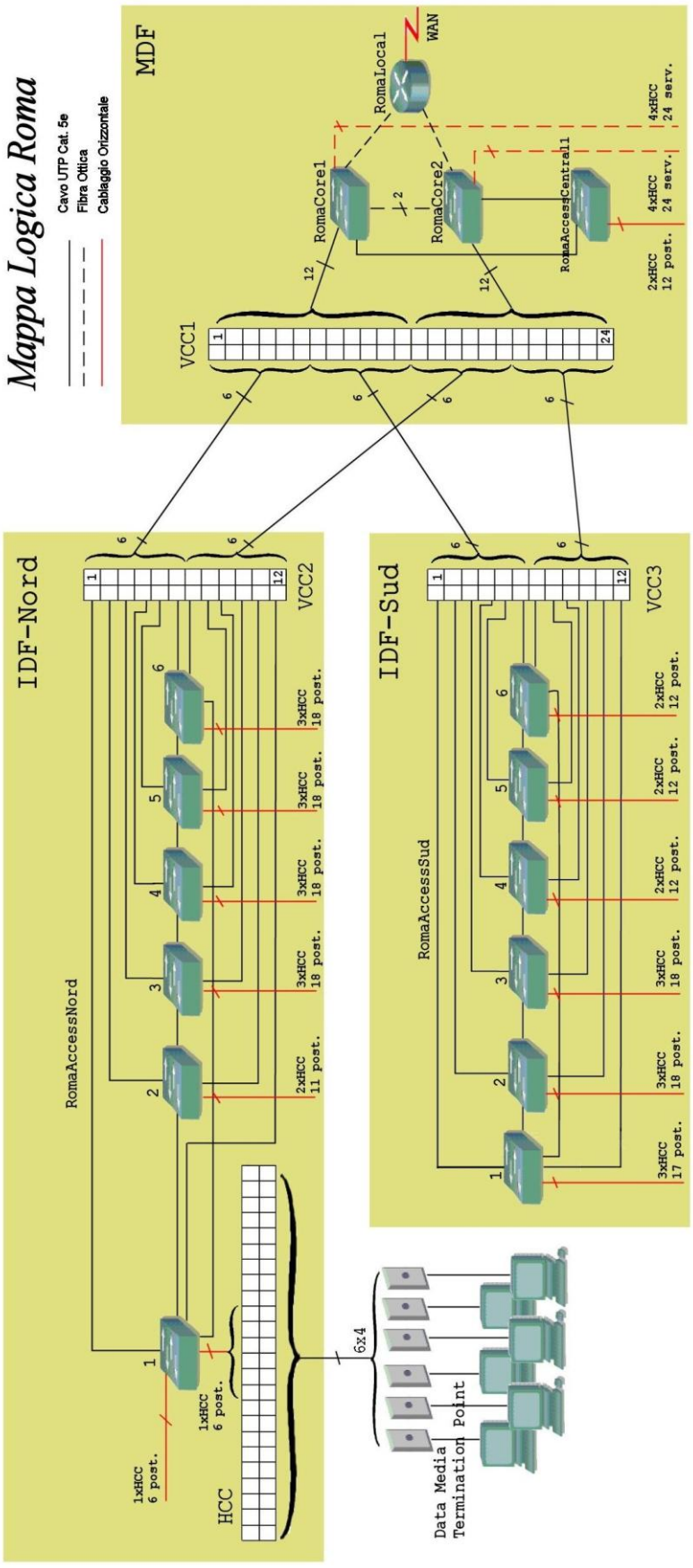


FIG 2.10

Andiamo ora a vedere come devono essere configurati i dispositivi della rete per garantirne il corretto funzionamento, oltre che il rispetto delle specifiche di progetto. Si ricorda di fare riferimento alla sezione a comune fra i progettisti per la configurazione del router di frontiera.
Viceversa si forniscono qui i requisiti di configurazione per gli switch della sede aziendale, in particolare con riferimento alle seguenti problematiche:

1. separazione dei domini, per mezzo di VLAN;
2. ridondanza, che può essere sfruttata grazie all'STP;
3. configurabilità, per mezzo di opportuni indirizzi di configurazione;
4. sicurezza, implementata per mezzo di password, port-security e DHCP snooping.

5.1 Impostazione delle VLAN

Come già visto nella sezione 1 del progetto, si è deciso di separare i gruppi di lavoro/domini di sicurezza della sede aziendale per mezzo delle LAN virtuali. Per precisi riferimenti sugli identificativi delle VLAN implementate si faccia riferimento alla sezione 1 o alle appendici di configurazione.
Per un corretto uso delle VLAN è necessario configurare correttamente le modalità di funzionamento delle porte degli switch. In particolare, facendo riferimento alle tabelle di configurazione, nella colonna switchport notiamo che tutte le macchine terminali sono connesse a porte di tipo access, mentre le restanti porte sono connesse a porte di tipo trunk.
In questo modo si ottiene la separazione dei vari domini, in quanto sui link access possono circolare solo pacchetti appartenenti al dominio (VLAN) opportuno, mentre sui link trunk possono circolare pacchetti di più domini di sicurezza. In particolare è inutile un'eventuale configurazione che impedisca su dei link trunk il passaggio di determinate VLAN, quindi si lascia attiva l'opzione di default (che pertanto non è riportata in fase di configurazione):

```
switchport trunk allowed vlan all
```

Un'altra opzione sfruttata per questioni di aderenza agli standard e non riportata perché attiva di default è l'incapsulamento usato sui link trunk (dot1q).
La configurazione delle porte è stata definita in modo completo, quindi non serve (anzi, riduce le performance della rete) lasciare attivo il Dynamic Trunking Protocol, che quindi verrà disattivato su ogni switch.

Protocollo di cui risulta invece utile l'attivazione, per incrementare ulteriormente la flessibilità della rete e snellire la configurazione manuale dei dispositivi, è il Virtual Trunking Protocol.
In particolare si configura il VTP version 1, dando come Server di dominio i due switch di livello core. In questo modo, se anche uno dei due dovesse non funzionare più, resterebbe l'altro a garantire la corretta configurazione delle VLAN sugli switch di livello access.
Per irrobustire la sicurezza si aggiunge alla configurazione un dominio ed una password per l'interazione fra gli switch (la password scelta è la classica "cisco").

Una funzionalità molto interessante offerta dall'uso del VTP è il VLAN Pruning, che consente di ridurre notevolmente il traffico di rete. Grazie al pruning difatti, il Server negozia con gli altri switch la disabilitazione del transito di pacchetti di alcune VLAN su link trunk, in relazione ai domini di sicurezza effettivamente attivi su tale link. La configurazione è riservata al solo Server primario (switch RomaCore1).

Per ulteriori informazioni sulla configurazione delle VLAN, si veda l' appendice B di configurazione degli switch.

5.2 Configurazione dell' STP

Al fine di garantire tempi di interruzione della connessione per il backbone di sede non superiori ai 100 secondi è stata implementata nella costruzione della rete una notevole ridondanza.
Tale ridondanza va a creare numerosi cicli, per cui la rete non è esente dal tipico fenomeno delle "tempeste di broadcast". La soluzione sta ovviamente nell'uso dello Spanning Tree Protocol.
Si osserva tuttavia che una configurazione non corretta di quest'ultimo, potrebbe portare a delle situazioni di regime in cui la rete si comporta in modo non efficiente, in particolare potrebbero venir bloccate porte che consentono percorsi più brevi fra le macchine terminali.
L' approccio seguito per ottenere una configurazione il più possibile ottimizzata dell'STP si fonda sui seguenti principi:

- gli switch RomaCore costituiscono il fulcro del traffico della sede aziendale, saranno pertanto candidati ad essere dei root switch;
- lo switch RomaCore1 è connesso al router con link trunk sulle VLAN che vanno da 11 a 15: si presume pertanto che sia meglio far convergere verso esso il traffico di queste VLAN;
- lo switch RomaCore2 è connesso al router con link trunk sulle VLAN che vanno da 16 a 18: si presume pertanto che sia meglio far convergere verso esso il traffico di queste VLAN.

Sulla base di questi principi, si assegna:

- Allo switch RomaCore1, priorità 4096 sulle VLAN da 11 a 15. In questo modo sarà sicuramente il root switch per queste VLAN (gli altri switch hanno per default priorità di 32768);
- Allo switch RomaCore2, priorità 4096 sulle VLAN da 16 a 18. In questo modo sarà sicuramente il root switch per queste VLAN.

Si prevede inoltre che in caso di fallimento di uno switch di livello core, il primo candidato a diventare root switch per le altre VLAN resta comunque l'altro dello stesso livello, per cui si assegna:

- Allo switch RomaCore1, priorità 8192 sulle VLAN da 16 a 18. In questo modo sarà sicuramente il root switch per queste VLAN in caso di fallimento del root switch primario.
- Allo switch RomaCore2, priorità 8192 sulle VLAN da 11 a 15. In questo modo sarà sicuramente il root switch per queste VLAN in caso di fallimento del root switch primario.

Un' opzione abbastanza utile per ridurre i tempi di convergenza dello spanning-tree, prevista dal protocollo proprietario CISCO che sarà quello effettivamente implementato, è l'utilizzo della modalità "portfast". Grazie a questa modalità, tutte le macchine terminali hanno la loro porta access direttamente attiva (è possibile farlo in quanto nella rete non sono presenti cicli di livello 1).
Per attivarlo si usa il comando:

```
spanning-tree portfast
```

sulle interfacce opportune.

Non si effettuano ulteriori configurazioni in quanto quelle già apportate garantiscono tempi di convergenza della rete sufficientemente rapidi (secondo quanto descritto nelle specifiche di progetto).

Per ulteriori informazioni sulla configurazione dell' STP, si veda l' appendice B di configurazione degli switch.

5.3 Configurazione degli indirizzi

Secondo i requisiti di progetto, gli switch devono essere configurabili da parte delle macchine appartenenti al dominio Supporto Sistemi. Per questo motivo si è scelto, già in fase di configurazione globale, di porre le interfacce di configurazione degli switch all'interno di questa specifica subnet, ovvero nella VLAN 15.
Nella seguente tabella (2.16) è possibile vedere per ogni switch quale indirizzo di configurazione gli è stato associato:

Tabella Indirizzi Switch

Locazione	Switch	Indirizzo di configurazione
Roma_ MDF	RomaCore1	172.16.195.141
	RomaCore2	172.16.195.142
	RomaAccessCentral1	172.16.195.143
Roma_ IDF-Nord	RomaAccessNord1	172.16.195.144
	RomaAccessNord2	172.16.195.145
	RomaAccessNord3	172.16.195.146
	RomaAccessNord4	172.16.195.147
	RomaAccessNord5	172.16.195.148
	RomaAccessNord6	172.16.195.149
Roma_ IDF-Sud	RomaAccessSud1	172.16.195.150
	RomaAccessSud2	172.16.195.151
	RomaAccessSud3	172.16.195.152
	RomaAccessSud4	172.16.195.153
	RomaAccessSud5	172.16.195.154
	RomaAccessSud6	172.16.195.155

TAB 2.16

Gli indirizzi da 172.16.195.156 a 172.16.195.158 sono poi riservati ai Server di Workgroup, per cui i restanti (da 172.16.195.130 a 172.16.192.140) sono disponibili per le macchine del gruppo di Supporto Sistemi (come già indicato nella parte della sezione 1 relativa al DHCP).

Per ulteriori informazioni sulla configurazione dell' interfaccia di configurazione per gli switch, perdonando il gioco di parole, si veda l' appendice B.

5.4 Impostazioni di sicurezza

Le opzioni di sicurezza basilari che sono state implementate sono le seguenti:

- Anzitutto sono state disabilitate le porte che non vengono utilizzate, secondo quanto descritto nella mappa logica;
- è stato altresì disabilitato il protocollo CDP, oltre che per problemi di sicurezza anche per ridurre il traffico di overhead;
- sono state ovviamente inserite password di login e di enable per la configurazione dei dispositivi. A fine puramente dimostrativo, le password sono quelle viste a lezione ("class" per il login e "cisco" per la modalità enable).
  Nella reale implementazione va prevista una loro modifica;
- è stato previsto un motd per ogni dispositivo, al fine di evidenziare che si sta agendo su dispositivi privati aziendali ed eventuali manomissioni da parte di non addetti ai lavori sono legalmente perseguibili.

Opzioni più avanzate di sicurezza includono il DHCP snooping ed il port-security.

Per quanto riguarda il DHCP, si cerca di evitare lo spoofing ed eventuali attacchi di flooding. Dal momento che, come già evidenziato in sezione 1, l'unico server DHCP presente nella sede è il router, si configura sugli switch l'opzione DHCP snooping come segue:

- Si configurano come "trusted" le porte degli switch di livello core rivolte verso il router e verso lo switch dello stesso livello, in quanto da tutte e tre le porte può potenzialmente transitare un pacchetto DHCP proveniente dal Server valido.
- Si configurano come "trusted" le porte degli switch di livello access rivolte verso gli switch di livello core e verso gli switch dello stesso livello, in quanto da tutte può potenzialmente transitare un pacchetto DHCP proveniente dal Server valido.
- Non si pongono limiti sulle porte trusted, e si configurano come untrusted (cosa che avviene automaticamente se la porta non è trusted) tutte le altre porte.

Il port-security costituisce il metodo di protezione più potente implementato.
In particolare attraverso quest' opzione, lo switch può riconoscere eventuali intrusioni e disabilitare la porta su cui è stata generata la violazione.
L' implementazione utilizzata si basa sullo sticky learning dinamico dei secure mac, effettuata su tutte le porte degli switch in modalità access. Gli switch presi in considerazione attivano automaticamente, assieme alle opzioni di port security e di sticky learning le seguenti:

```
switchport port-security maximum 1
switchport port-security violation shutdown
```

Qual che si ottiene dunque, è che gli switch apprendono dinamicamente il MAC address della macchina terminale che per prima si connette su una loro porta.
Successivamente, se sulla stessa porta viene riscontrata la presenza di un secondo MAC address (il massimo è per default 1) la porta entra in stato di shutdown per violazione (di default).

Tuttavia stringenti opzioni di sicurezza comportano necessità di gestione. In particolare quando si verifica la violazione, diventa compito della funzione SS intervenire e, in ultima istanza, andare a riattivare la porta compromessa. In particolare se fosse necessario dover sostituire le macchine (e di conseguenza i MAC address) delle varie postazioni della sede, si dovrebbe procedere come segue:

1. disabilitazione dello sticky learning, che ormai ha associato ad ogni porta uno specifico MAC address;
2. salvataggio della attuale configurazione dello switch;
3. riavvio dello switch;
4. riesecuzione del comando di sticky learning per riassociare il MAC corretto.
   ATTENZIONE: bisogna assicurarsi in questa fase che il MAC che si va ad associare sia veramente quello desiderato e non quello di un eventuale intruso.

Per maggior dettaglio sulle configurazioni della sicurezza, ed in generale degli switch di tipo core ed access, si faccia riferimento alle appendici B (sezione di Roma).

6. Simulazione con Packet Tracer 4.11

Una simulazione pratica delle funzionalità del progetto della sede di Roma sopra descritto, si trova in allegato al documento con il nome *"Simulazione_Roma.pkt"* ed è stata realizzata mediante Packet Tracer 4.11.

L' uso dello specifico strumento ed il fatto che la simulazione è a scopo puramente dimostrativo, comporta le seguenti limitazioni:

- Gli switch presenti sono tutti a 24 porte fastEthernet, in particolare questo provoca delle differenze nella configurazione degli switch core.
- A causa della limitazione di cui sopra, non sono previsti cablaggi in fibra ottica.
- Non è supportato il protocollo proprietario CISCO per lo spanning-tree, per cui non è prevista l'opzione portfast.
- Non è supportato il DHCP snooping.
- Non è supportato il VTP pruning.
- Non viene disabilitato il CDP, utile in simulazione per scopi di debug.
- Lo shutdown è dato solo sulle interfacce che non vengono mai usate su nessun switch di livello access o core (questo vuol dire che gli switch sono generici e non personalizzati in base alla stanza che devono interconnettere).
- I Server ed i computer connessi sono in numero ridotto rispetto alla situazione reale.
- E' riportata solo la topologia della sede di Roma, per quanto riguarda la connessione intersede si faccia riferimento al file specificato in sezione 1.
- L' appartenenza delle varie macchine ai diversi gruppi di lavoro è del tutto ipotetica, tant'è che non viene riportata una descrizione per le interfacce.

In figura 2.11 è possibile visualizzare uno screenshot della simulazione della rete di sede mediante PT.

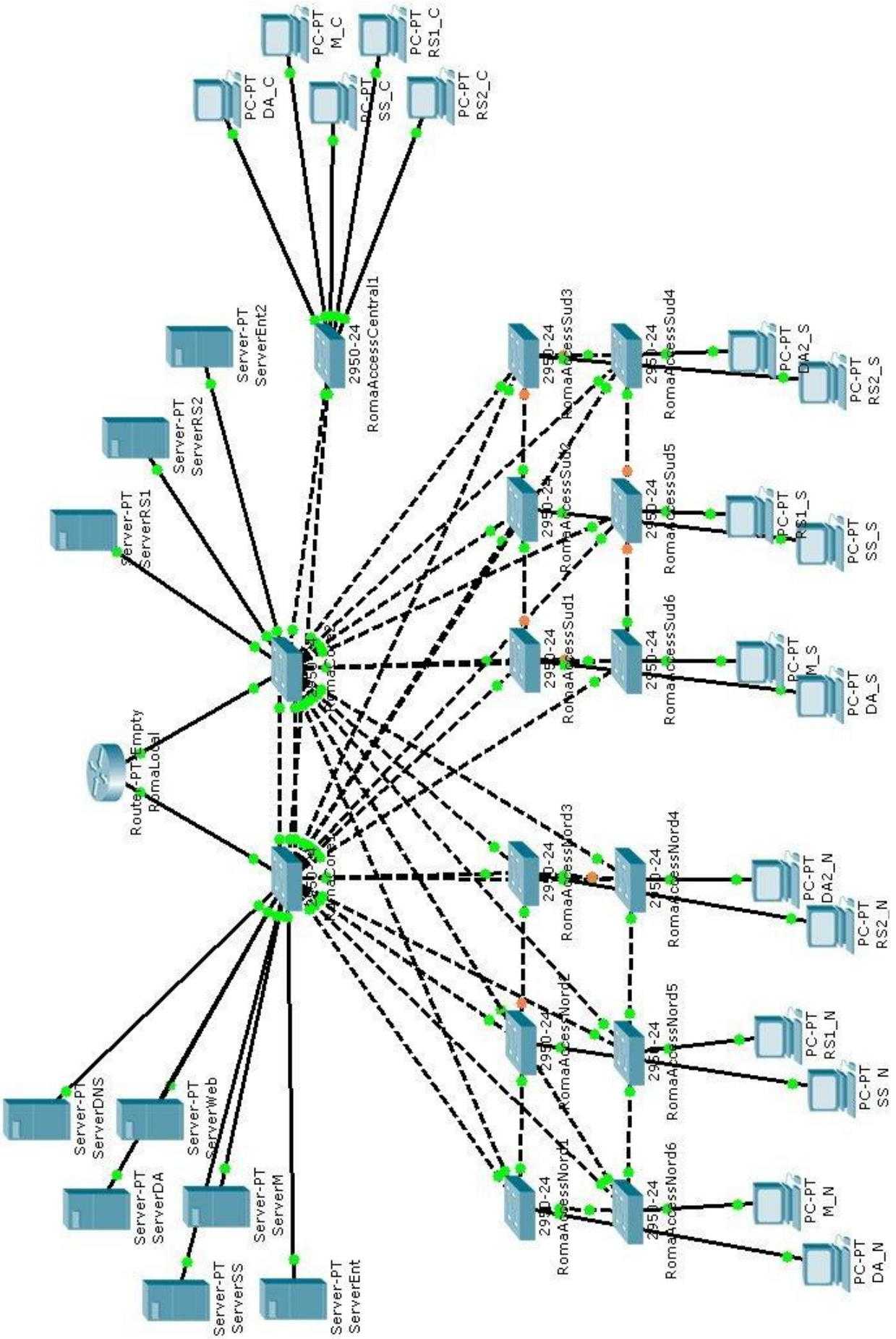

PC-PT M_C
PC-PT RS1_C
PC-PT DA_C
PC-PT SS_C
PC-PT RS2_C
Server-PT ServerEnt2
2950-24 RomaAccessCentral1
Server-PT ServerRS2
Server-PT ServerRS1
2950-24 RomaAccessSud3
2950-24 RomaAccessSud4
PC-PT DA2_S
PC-PT RS2_S
2950-24 RomaAccessSud2
2950-24 RomaAccessSud5
PC-PT RS1_S
PC-PT SS_S
2950-24 RomaAccessSud1
2950-24 RomaAccessSud6
PC-PT M_S
PC-PT DA_S
Router-PT-Empty RomaLocal
2950-24 RomaAccessNord3
2950-24 RomaAccessNord4
PC-PT DA2_N
PC-PT RS2_N
2950-24 RomaAccessNord2
2950-24 RomaAccessNord5
PC-PT RS1_N
PC-PT SS_N
2950-24 RomaAccessNord1
2950-24 RomaAccessNord6
PC-PT M_N
PC-PT DA_N
Server-PT ServerDNS
Server-PT ServerWeb
Server-PT ServerDA
Server-PT ServerM
Server-PT ServerSS
Server-PT ServerEnt

FIG. 2.11

1. Considerazioni preliminari

Come passo iniziale attribuiamo ad ogni stanza un'etichetta identificativa per potervisi più agilmente riferire durante le fasi di stesura dei cavi, configurazione delle interfacce, etc...
Si premette che si manterrà la divisione, applicata nelle mappe forniteci, degli stabili appartenenti alla sede di Padova, tra un'area Ovest ed Est.
Come è chiaro dalla mappa in figura 3.1 la società di telecomunicazioni ha posto il suo punto di presenza nella stanza in cui compare la sigla 'POP', pertanto essa diventa la posizione dove più vantaggiosamente possiamo collocare il Main Distribution Facility.
Per le etichette si è pensato conseguentemente di adottare un formato del tipo 'R-XY', dove X è una lettera e Y un numero: X diventa l'identificativo dell'edificio, Y della stanza all'interno dell'edificio. Sia X che Y sono in funzione della distanza dal MDF, assumendo valori crescenti all'aumentare della stessa; in particolare Y assume valori che partono da 1 per ogni stabile.
Questa nomenclatura permette così di ricavare già dall'etichetta della stanza importanti informazioni circa la sua collocazione: tale funzione 'mnemonica' potrà risultare utile per esempio qualora si vadano ad analizzare i collegamenti degli switch presenti nei Distribution Facilities.

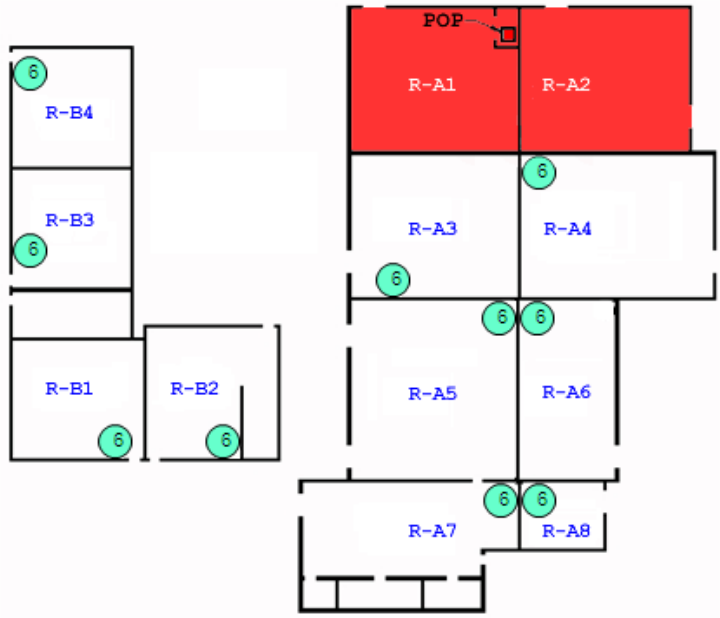


FIG. 3.1 – Padova Est

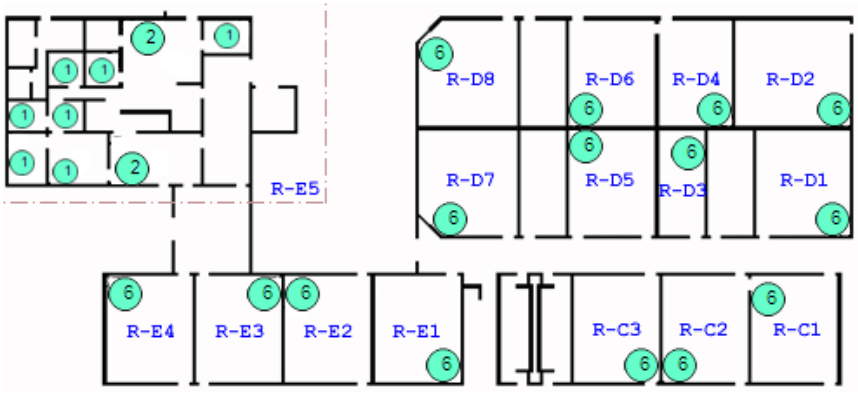


FIG. 3.2 – Padova Ovest

Si è evitato di dare un nome a quei vani che non necessitano di punti di presenza con l'infrastruttura. Inoltre, per semplicità di attribuzione, l'intera area delimitata dalla linea tratto-punto assume un singolo identificativo.

Oltre alle etichette ottenute, dalle precedenti immagini possiamo ricavare:

- gli ambienti destinati ad ospitare i server aziendali, corrispondenti alle zone evidenziate in rosso;
- l'eventuale presenza di Data Media Termination Point in una stanza (cerchio celeste) e il numero di postazioni di lavoro che devono essere ospitate (cifra interna).

Come da specifiche, ognuna delle stanze contenente il simbolo ⓵ nelle mappe datoci, è stata considerata da cablare in modo da fornire il supporto per 6 postazioni di lavoro; eccezion fatta per i vani predisposti ad accogliere la server farm aziendale e per quelle stanze contenenti lettere oltre o in sostituzione al simbolo ⓵: nel primo caso, come esplicitamente richiesto, le stanze devono poter ospitare ciascuna 24 macchine; nel secondo caso il numero delle postazioni di lavoro è rappresentato dalla cardinalità delle lettere presenti in ogni vano.

Si ricorda infine che ciascun punto di presenza dell'infrastruttura dovrà mettere a disposizione 4 prese di rete. Quindi, data la corrispondenza fra punti di presenza e postazioni di lavoro, ne deriva che per ottenere il numero di telecommunication outlet (e cavi) presenti in una stanza si deve moltiplicare per quattro il numero contenuto nel cerchio corrispondente nelle figure sopra.

2. Distribution Facilities

A questo punto è necessario disporre gli armadi di distribuzione: mentre per il MDF la collocazione è scontata (come visto è da posizionarsi nella stanza R-A1 dove la società di telecomunicazioni ha posto il POP), diverse considerazioni devono essere fatte circa gli armadi secondari o IDF.
Per quanto riguarda l'area Est del complesso aziendale, risulta che devono essere servite in totale 60 postazioni di lavoro, un numero cioè gestibile mediante un singolo Distribution Facility che pertanto viene a coincidere con il MDF stesso (cui sono connessi anche i server, al massimo 48). Questa scelta è inoltre permessa e suggerita dalla vicinanza degli immobili A e B, separati da una distanza inferiore ai 3 metri.

Un armadio secondario deve essere invece necessariamente posizionato per servire la parte Ovest della sede, al fine di poter fornire il servizio anche all'intero edificio E, il più lontano rispetto al MDF. Tenendo presente lo standard TIA/EIA 568 B, che stabilisce a 90 metri la lunghezza massima per un cablaggio orizzontale con cavo UTP cat. 5e (più 5 metri di patch cord e altrettanti per i work area station cable), si è scelto di collocare l'IDF come in figura 3.3, tra la stanza R-D5 e R-D7.

La scelta della stanza è stata supportata da diverse considerazioni:

- la (quasi) centralità della stessa rispetto al complesso degli edifici C, D, E e quindi la possibilità di conformarsi senza particolari difficoltà agli standard summenzionati (per valutazioni quantitative vedere in seguito);
- le specifiche di progetto, non prevedendo al suo interno postazioni di lavoro, fanno supporre che non risulti occupata da dipendenti della società. Questo è innegabilmente un vantaggio: per questioni di sicurezza infatti si deve concedere l'accesso ai dispositivi dell'armadio di distribuzione (e possibilmente all'armadio stesso) solamente ad addetti specializzati, o quantomeno limitare la libera circolazione delle persone nella stanza.

- risulta essere la migliore scelta anche in relazione ai cavi che devono raggiungere l'IDF, provenienti dagli edifici C ed E, e alle condotte che devono essere necessariamente utilizzate (sia preesistenti che nuove). Infatti dovranno pervenire nella stanza dell'IDF 140 cavi dallo stabile E e 72 dal C (risultato ottenuto semplicemente moltiplicando il numero delle postazioni di lavoro per quattro, numero di prese di rete che ogni postazione fornisce), più i cavi del cablaggio verticale.
  Come linea generale di comportamento, per permettere il collegamento fra due edifici, si è deciso di sfruttare le condotte preesistenti e limitare la realizzazione di nuove, eventuali condotte, al minimo indispensabile.
  È comunque evidente come, risultando E e D isolati dal resto della sede (mentre ricordiamo che C è collegata ad A tramite un condotto), sia necessario aggiungerne almeno una. È stato introdotto perciò il raccordo evidenziato in figura 3.3.
  In questo modo si utilizza il condotto già presente per portare fino a D i cavi di E, e il nuovo per portare quelli di C e del cablaggio verticale; chiaramente i cavi relativi alle postazioni di lavoro di D sono connessi in loco all'IDF e non devono attraversare altri edifici. Altre scelte potevano essere fatte, per esempio si poteva collocare l'IDF nello stabile C nella stanza accanto alla R-C3, ma sarebbe risultato sconveniente, in quanto avremmo dovuto posizionare due nuove condotte per unire C a D ed E, oppure, installandone una sola nuova tra C e D o E, avremmo dovuto farvi passare tutti i cavi dei due stabili (in totale 192 + 140 = 332). Come si nota la scelta fatta risulta essere la più proficua, considerando che ad un minor numero di cavi corrisponde un minor numero di condotte da installare o comunque di diametro minore; si tenga conto peraltro che non è noto il diametro del condotto preesistente fra gli edifici D ed E e pertanto è da preferirsi la scelta che prevede di occuparlo di meno.

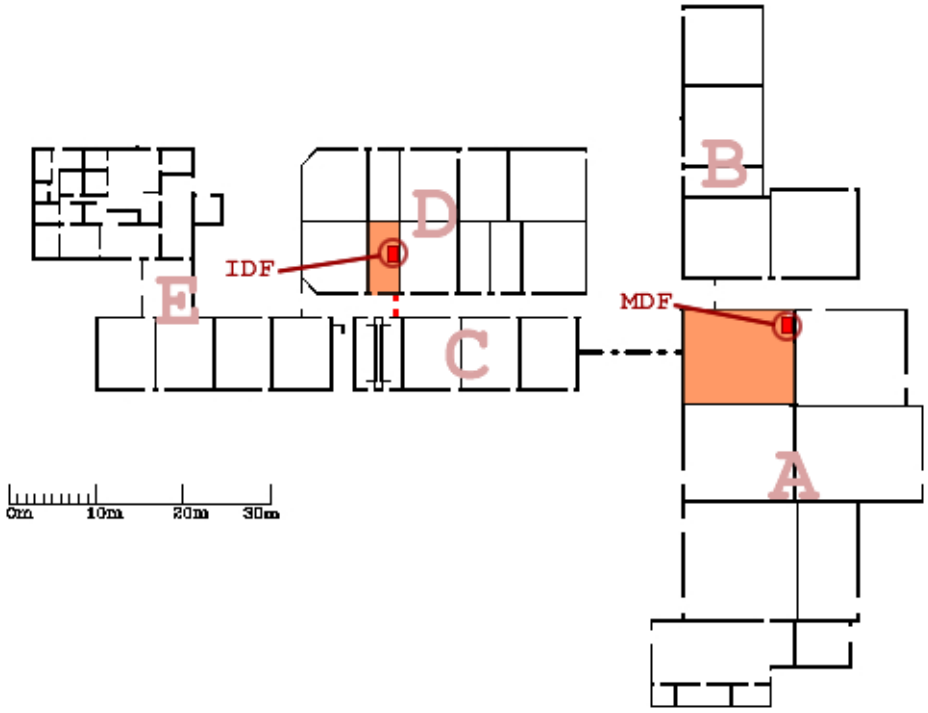


FIG. 3.3 – Distribution Facilities

Stabilita la posizione esatta degli armadi di distribuzione, si passa adesso ad una valutazione più precisa delle distanze massime che i cavi del cablaggio orizzontale (UTP cat. 5e) dovranno coprire, per poter così verificare la conformità di questa disposizione agli standard TIA/EIA-568-B e TIA/EIA-569.
Pertanto è sufficiente misurare la lunghezza dei due percorsi più lunghi a partire dai due armadi.

Per completezza però riportiamo per ogni edificio la distanza che separa il punto da cablare più lontano dall'xDF più vicino (tali percorsi sono rappresentati nella figura 3.4):

A.	R-A7	-	MDF	→	~58.2 m
B.	R-B4	-	MDF	→	~51.9 m
C.	R-C1	-	IDF	→	~38.8 m
D.	R-D2	-	IDF	→	~34.2 m
E.	R-E5	-	IDF	→	~63,7 m

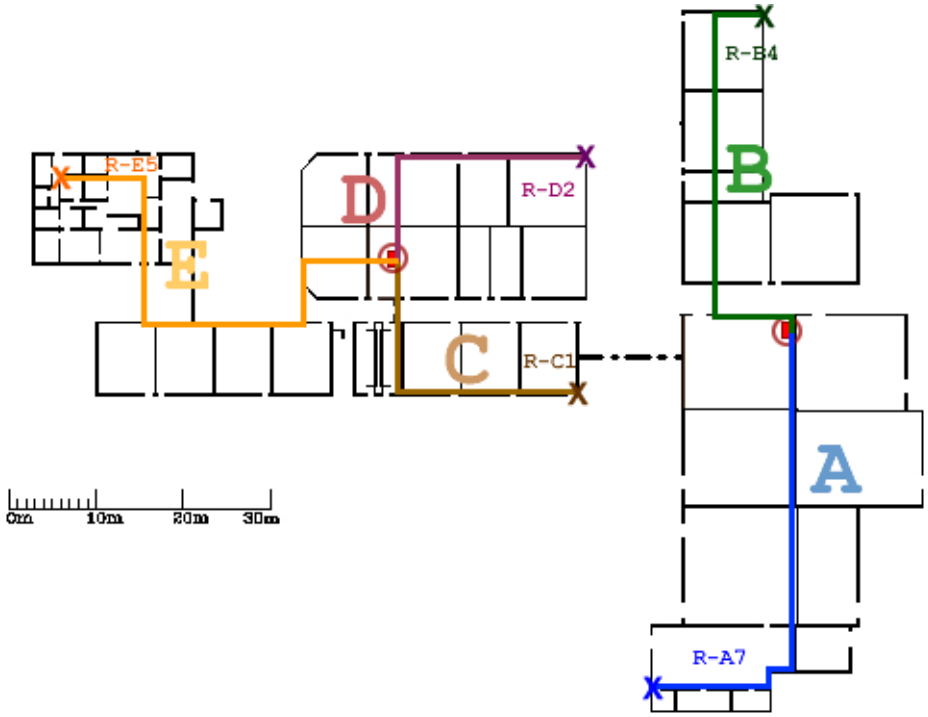


FIG. 3.4 – Percorsi di lunghezza massima per il cablaggio orizzontale

Come si evince facilmente dai risultati, rientriamo abbondantemente all'interno della soglia dei 90 metri anche considerando un margine di errore del 5% nel calcolo e eventuali curve o disposizioni all'interno della controsoffittatura dei cavi (che andrebbero ad aggiungere circa 6/8 metri per salire e scendere lungo la parete).

Oltre al rispetto degli standard TIA/EIA nelle specifiche di progetto sono richiesti due ulteriori requisiti, relativi alla banda da rendere disponibile, che devono essere tenuti in considerazione in questa fase di progettazione:

1) *"per ciascuna [postazione di lavoro] dovrà essere disponibile una banda minima di 1Mpbs fino ai server aziendali presenti nella medesima sede";*
2) *"Le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x".*

3.1 Cablaggio Orizzontale

Per collegare le postazioni di lavoro all'xDF più vicino abbiamo stabilito, come già anticipato, di stendere cavi UTP cat. 5e. Essi sono capaci di sostenere una banda fino a 1Gbps e pertanto sono più che sufficienti per soddisfare le richieste progettuali: ogni cavo che unisca un armadio di distribuzione con l'host di un end-user dovrà infatti supportare una banda massima di 10Mbps, 100 volte inferiore a quella realmente sostenibile.
Procediamo con un calcolo dei cavi che dovranno raggiungere il MDF e l'IDF (escludiamo i server delle stanze R-A1 e R-A2 analizzati in seguito), ricordando che ad ogni postazione di lavoro corrispondono quattro prese di rete (e quindi cavi):

- nell'edificio A ci sono 36 postazioni di lavoro, per un totale di $36 \cdot 4 = 144$ cavi che devono raggiungere il MDF;
- nell'edificio B ci sono 24 postazioni di lavoro, per un totale di $24 \cdot 4 = 96$ cavi che devono raggiungere il MDF (passando attraverso il condotto tra A e B);
- nell'edificio C ci sono 18 postazioni di lavoro, per un totale di $18 \cdot 4 = 72$ cavi che devono raggiungere l'IDF (passando attraverso il condotto tra C e D);
- nell'edificio D ci sono 48 postazioni di lavoro, per un totale di $48 \cdot 4 = 192$ cavi che devono raggiungere l'IDF;
- nell'edificio E ci sono 35 postazioni di lavoro, per un totale di $35 \cdot 4 = 140$ cavi che devono raggiungere l'IDF (passando attraverso il condotto tra E e D).

Complessivamente 240 cavi UTP raggiungono il MDF e 404 l'IDF. Ogni cavo è connesso, dalla parte dell'armadio di distribuzione, ad un patch panel, da cui, come da specifiche, partirà, diretto allo switch, un unico patch cord per postazione di lavoro (i patch cord saranno quindi in numero pari ad un quarto della somma appena calcolata).
Sia i work area station cable, che i cavi del cablaggio orizzontale, che i patch cord sono dotati da entrambe le estremità dei soliti plug RJ-45.
Considerandone il numero considerevole, per la stesura dei cavi si immagina di impiegare il controsoffitto (che fornisce un'intercapedine di ben 2 piedi): dalle postazioni di lavoro, tramite una canalina saranno dunque portati verso il soffitto, da cui scenderanno presso la stanza dell'armadio di distribuzione o nel caso fosse previsto il passaggio in una condotta.
Si noti come le distanze che separano i vari edifici interessati siano molto brevi: i condotti non superano i 3 metri di estensione pertanto si ritiene che i cavi non abbiano bisogno di particolari schermature.

Considerazioni diverse vanno compiute invece per connettere i server aziendali alla rete. Qui i vincoli di banda si fanno più stringenti, infatti il collegamento tra ciascun server e il MDF deve poter sostenere una banda pari al traffico massimo generato da ogni host della sede, ossia 10 Mbps (considerando già la previsione di crescita), moltiplicato per il numero complessivo delle postazioni (161), per un totale di 1610 Mbps. Un requisito che quindi impone l'utilizzo di mezzi trasmissivi alternativi ai cavi basati su doppino telefonico, come per esempio le fibre ottiche.
Si è deciso di utilizzare dunque un totale di $48 \cdot 2 = 96$ fibre ottiche multimodali 62.5/125, che permettono il collegamento con velocità in banda superiori a quelle richieste (sicuramente fino ai 10 Gbps) per brevi distanze. Si ricorda che per ottenere un collegamento full duplex sono necessarie due fibre, una impiegata in trasmissione e una in ricezione (per questo se ne installa un numero doppio rispetto al numero massimo di server). Come per i cavi UTP sarà presente un patch panel nel MDF cui andranno collegati i cavi provenienti dai server. È da notare come la scelta delle stanze, le più vicine rispetto alla distribution facility, comporti l'attraversamento di distanze molto brevi da parte delle fibre e quindi risulti conveniente in fase di installazione delle stesse. Per quanto riguarda i connettori, per patch panel e Telecommunication outlet si prevede l'utilizzo di comuni jack SC/PC.

Per la la messa in posa delle fibre, vista la vicinanza con l'armadio, si evita l'uso della controsoffittatura: per R-A1 si utilizzano canaline in materiale plastico che le collegano direttamente al pannello di permutazione; per R-A2 si usano ancora canaline fino alla parete divisoria che la separa dall'adiacente MDF e che sarà opportunamente forata e attraversata dai cavi.

3.2 Cablaggio Verticale

Resta da indicare come effettuare il cablaggio fra il MDF e l'IDF.
Si ritiene sia preferibile l'installazione di fibre ottiche in quanto presentano innumerevoli vantaggi rispetto ai cavi in rame; nel nostro caso siamo interessati fondamentalmente a due aspetti:

- ✓ risultano immuni alle interferenze elettromagnetiche;
- ✓ comportano bassi valori di BER.

In particolare la prima caratteristica le rende particolarmente utili nel caso di uso esterno agli edifici; nel nostro caso i cavi devono infatti attraversare una condotta, fra gli edifici A e C, della lunghezza di circa 12,5 metri (non trascurabile come per le altre). La bassa percentuale di errore in trasmissione rende la fibra comunque preferibile rispetto ai cavi in rame per collegamenti che, costituendo il backbone delle rete interna alla sede, devono risultare affidabili.
La fibra ottica è in grado di sostenere elevate velocità trasmissive per cui non dovrebbero porsi problemi relative alla banda, effettuiamo tuttavia una verifica per scrupolo.
Si consideri dunque il requisito di 10Mbps da ciascun host verso i server: ne risulta allora che, per le 101 postazioni di lavoro dell'area Ovest, si devono poter avere 1010 Megabit/secondo nella comunicazione verso il MDF; si tenga inoltre presente che questa capacità trasmissiva deve essere fornita dall'insieme di tutti i collegamenti che uniscono Intermediate e Main DF. Non solo dunque la fibra è più che idonea per l'utilizzo ma basterebbe che fossero presenti almeno due collegamenti fra i due distribution facilities per permettere il traffico anche su cavo UTP (che può sostenere come già ricordato un traffico di 1000Mbps).
Si applicano quindi ancora una volta fibre multimodali di tipo 62.5/125, economicamente le più vantaggiose.

Una volta decisa la tipologia di linea trasmissiva si deve stabilire il numero esatto di fibre da piazzare e per questo è necessario sapere quanti switch dovranno essere collocati nell'IDF.
Il calcolo può essere fatto in modo semplice e, per quanto serve adesso, non accurato:
si premette che verranno usati (per motivi che saranno chiariti in seguito) switch a 24 porte, pertanto, considerando di collegare ad un singolo switch non più di 18 postazioni (numero equivalente a tre stanze marcate col simbolo ⓵ e che permette di avere una discreta quantità di porte libere sul dispositivo per collegamenti ridondanti e/o per poter sostenere un'eventuale espansione dell'azienda), ne risultano necessari almeno $101 \div 18 \sim 6$.
Dunque, ipotizzando di rendere la rete più stabile tramite connessioni ridondanti, poniamo a due il numero di collegamenti tra ciascun switch dell'IDF e il MDF, ottenendo un totale di $6 \cdot 2 \cdot 2 = 24$ fibre ottiche da stendere. Per poter far fronte comunque ad eventuali future espansioni aziendali, danneggiamenti, usi non pianificati, etc si ritiene opportuna la messa in posa di ulteriori fibre, in numero arbitrariamente stabilito pari a 8, per un totale di 32 fibre (il costo dell'acquisto di queste soprannumerarie linee di trasmissione si ritiene trascurabile vista anche la brevità del percorso da coprire).

In figura 3.5 si riporta il percorso del cablaggio verticale.

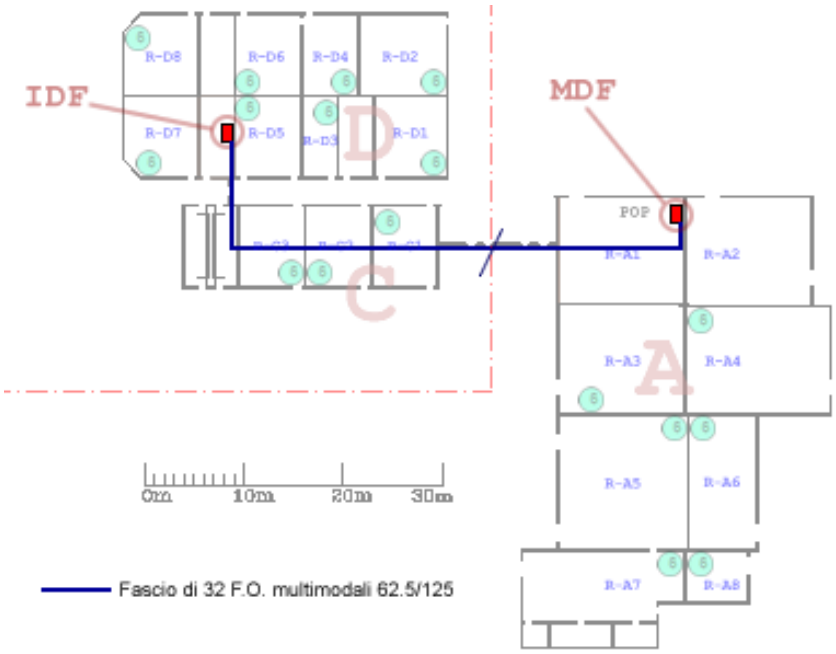


FIG. 3.5 – Cablaggio verticale (mappa fisica)

La lunghezza complessiva è pari a circa 60,5 metri, ben al di sotto dei limiti imposti da qualsiasi tecnologia funzionante su fibra ottica multimodale 62.5/125 (per il 1000BASE-SX che useremo il limite è posto a 275 metri per questo tipo di linea trasmissiva).
Per quanto concerne la disposizione dei cavi si è pensato di impiegare ancora il controsoffitto sia per le stanze R-A1 che R-C1/3 (vedi figura 3.4), tuttavia visto l'esiguo numero e ingombro delle fibre da collocare si potrebbe in alternativa pensare di inserirle in canaline che seguano i muri esterni delle suddette stanze.
Presso ciascuno dei due punti di distribuzione della rete sarà presente un patch panel per il cablaggio verticale, costituito da 16 porte con connettori SC/PC (un collegamento in full duplex fra due dispositivi, ricordiamo, richiede due fibre ottiche e due fibre perciò entreranno in ciascuna porta tramite due plug anch'essi di tipo Standard Connector/PC).

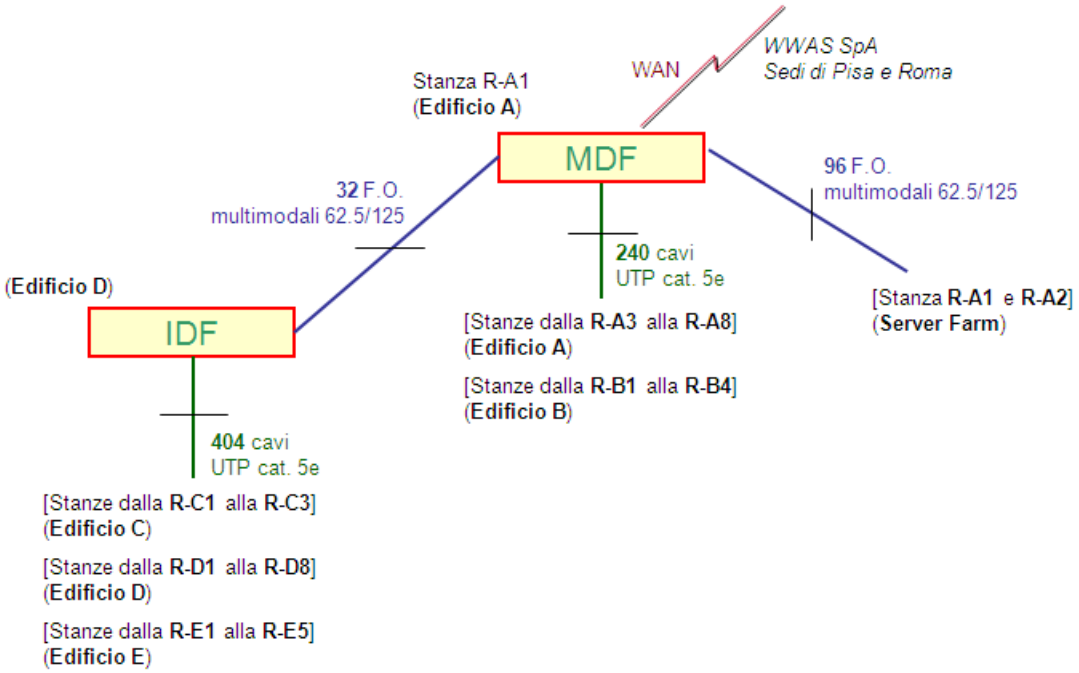


FIG. 3.6 – Sintesi della distribuzione orizzontale e verticale

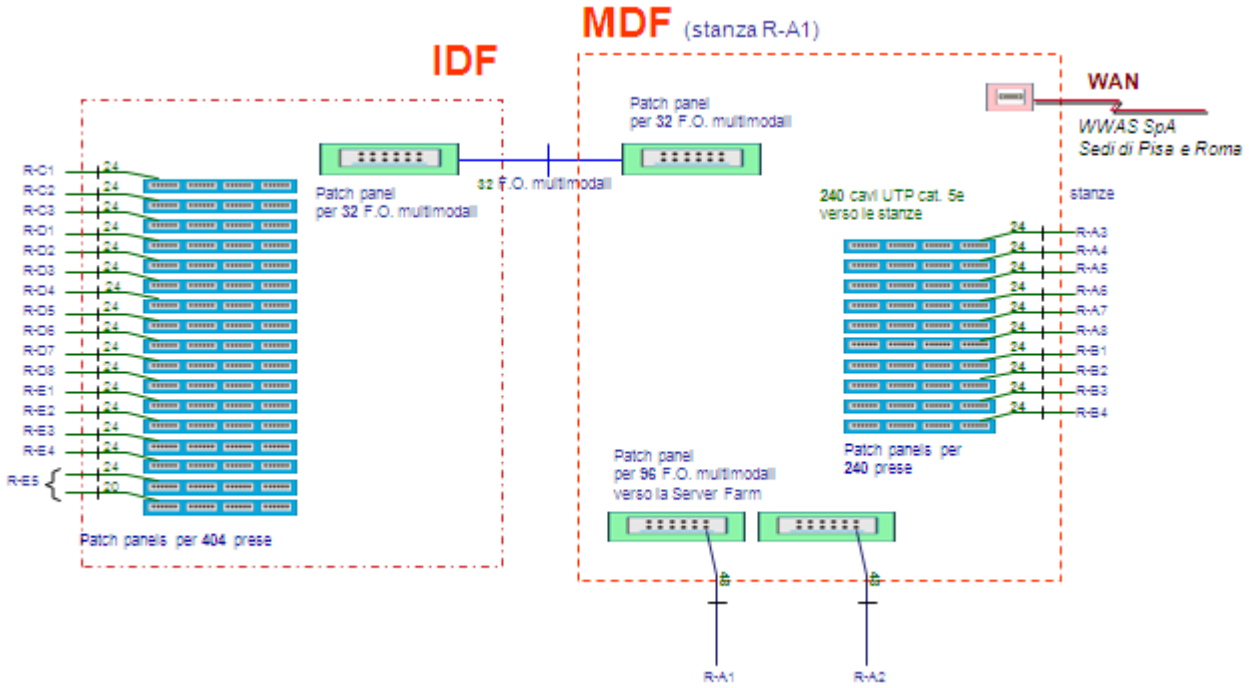


FIG. 3.7 – Distribuzione orizzontale e verticale del cablaggio strutturato

Come risulta chiaramente in figura abbiamo dedicato un patch panel per ognuna delle stanze da connettere alla rete (due per la stanza R-E5).

4. Switch

Diamo un quadro sintetico e qualitativo della topologia logica della rete prima di analizzare in dettaglio i due Distribution Facilities.
Ogni postazione di lavoro fornisce quattro prese di rete ed è perciò unita al patch panel con quattro cavi a quattro porte, di queste però solamente una è collegata allo switch tramite patch cord.
Nei due armadi di distribuzione abbiamo pertanto switch che forniscono l'accesso alla rete a 101 (area Ovest) + 60 (area Est) device terminali.
Questi dispositivi di livello data link sono collegati ad altri switch collocati nel MDF che rispondono a diverse funzionalità:

1. definizione dei domini di sicurezza/broadcast;
2. aggregazione delle connessioni verso gli end-user device (e gli altri switch);
3. collegamento con i server della sede (scelta chiarita in seguito);

sono inoltre collegati al router con accesso alla rete geografica.

Volendo individuare i livelli caratteristici della struttura gerarchica di una rete LAN, vediamo come ci siano dispositivi che svolgono funzioni tipiche di più layer e pertanto, come esemplificato in figura 3.7, su alcuni di essi si sovrappongono più livelli:

- le postazioni di lavoro hanno accesso alla rete tramite switch che forniscono funzionalità di livello **access**;
- questi switch sono a loro volta connessi ad altri che implementano le succitate funzioni 1 e 2 di livello **distribution**, ma che connettono anche i server all'infrastruttura, realizzando anch'essi funzionalità di tipo **access**;
- il router fornisce sia il collegamento tramite WAN al backbone che unisce Padova con le sedi aziendali di Pisa e Roma (livello **core**), sia la funzionalità di inter-VLAN routing (livello **distribution**).

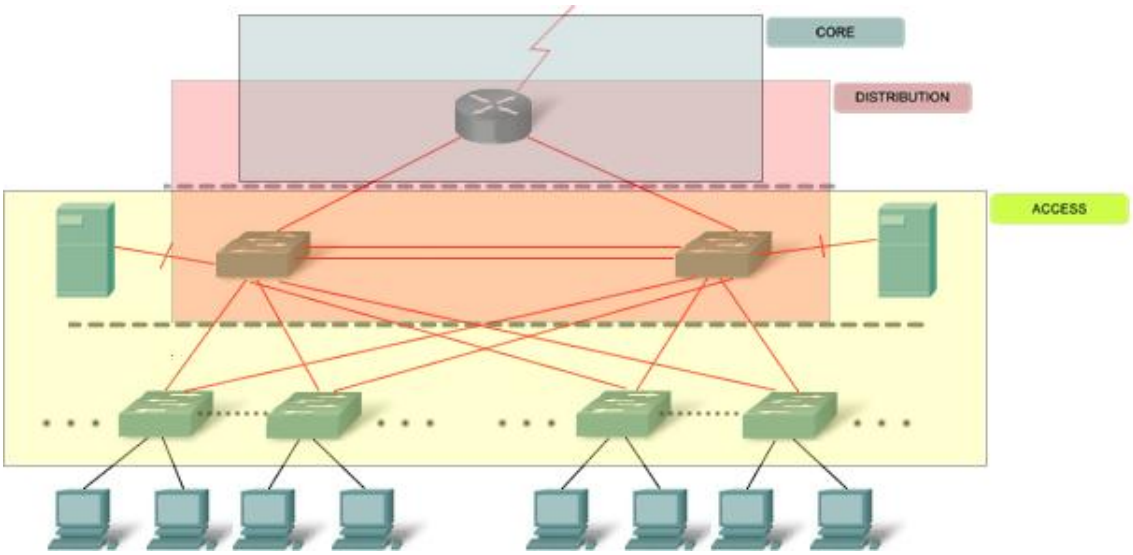


FIG. 3.8 – Topologia logica e struttura gerarchica

La situazione per ogni armadio di distribuzione è stata chiarita nei termini di cablaggio orizzontale e verticale, resta da determinare in dettaglio il numero e il tipo di dispositivi contenuti al loro interno nonché caratteristiche e collegamenti delle interfacce.
Ricordiamo ancora che dei 24 cavi che giungono da ciascuna stanza ad un pannello di commutazione, solo 6 (1 per ogni postazione di lavoro) devono essere collegati a switch.

4.1 Intermediate DF

Si è optato per l'impiego di dispositivi a 24 porte (più 2 di uplink) in quanto disponibili a costi ragionevolmente contenuti ed essenzialmente inferiori, anche in proporzione, rispetto ad altri dotati di un numero maggiore di porte (vedi listino fornito). L'utilizzo di più device comporta, in aggiunta, che l'eventuale guasto di un apparecchio implichi l'isolamento dalla rete solamente di un numero limitato di host.
La scelta è ricaduta sul modello 2950SX-24 CISCO: esso permette la connessione di 24 postazioni di lavoro, grazie a 24 porte Fast Ethernet con l'usuale jack RJ45 (tecnologia 100BASE-T); mette inoltre a disposizione 2 porte Gigabit Ethernet di uplink per la connessione agli switch del MDF tramite tecnologia 1000BASE-SX. La comunicazione su fibra ottica è permessa mediante connettori di tipo MTRJ.
Si rende necessario di conseguenza l'uso di bretelle bifibra multimodali 62.5/125 duplex con connettori misti: MTRJ ad un'estremità e SC all'altra.

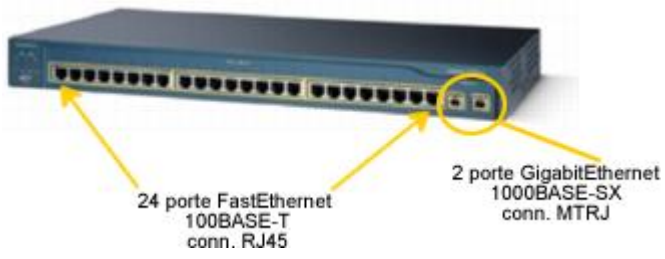


FIG. 3.9 – Lo switch CISCO 2950SX-24

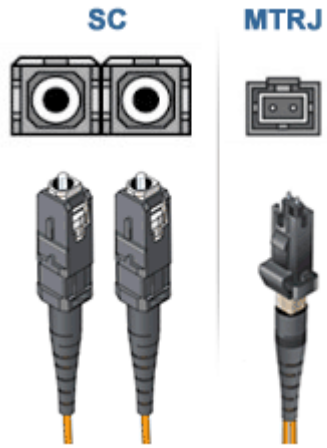


FIG. 3.10 – Connettori SC/PC e MTRJ

La presenza delle due porte Gigabit Ethernet permette poi la realizzazione di collegamenti doppi con gli switch del MDF: tutti i dispositivi dell'IDF risultano pertanto connessi tramite le fibre del cablaggio verticale a due switch dell'armadio principale (che in seguito vedremo essere MDF1 e MDF2).
Si fa presente che per quanto detto, potremmo pensare di usare anche collegamenti su fibra del tipo 100BASE-FX, in quanto anch'essi capaci di soddisfare le richieste di banda; tuttavia è parso preferibile adottare una soluzione tecnologica più avanzata a fronte di un risparmio economico trascurabile (addirittura il modello CISCO 2950C-24, con tale dotazione, a causa del software installatovi, risulta meno conveniente di quello scelto).

Delle 24 porte disponibili ne usiamo al massimo 18 per connettere apparati terminali: in tal modo è possibile collegare tutte le postazioni di lavoro di una work area ad un unico switch, fornendo dunque un elemento di chiarezza che può risultare vantaggioso durante la manutenzione dei dispositivi. In particolare ad ogni switch connettiamo dalle 2 alle 3 stanze complete.
Inoltre si prevede di aumentare la robustezza della rete effettuando dei collegamenti, secondo una tipologia a ring, tra i dispositivi interni all'IDF: significa che ogni switch è collegato ad altri due tramite cavi UTP cat. 5e crossover, con un massimo quindi di 20 porte occupate su 24 (le rimanenti sono a disposizione dell'azienda per usi futuri).
Il numero degli switch da collocare è, come peraltro già anticipato, pari a 6, ossia l'approssimazione intera per eccesso della divisione 101 ÷ 18, dove il dividendo corrisponde al numero totale delle postazioni e il divisore alle porte utili su ciascuno switch.
In seguito ci riferiremo ad essi utilizzando un'etichetta del tipo 'IDFX' dove X è un numero progressivo a partire da 1.

Riepilogo dei cavi collegati ad ogni switch
(le ultime due voci si riferiscono alle porte Gigabit Ethernet, tutte le altre a porte FastEthernet):

1. **IDF1**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-C1;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-C2;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-C3;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF2;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF6;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

2. **IDF2**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D1;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D2;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D3;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF3;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

3. **IDF3**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D4;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D5;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D6;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF4;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF2;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

4. **IDF4**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D7;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-D8;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF5;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF3;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

5. **IDF5**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-E1;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-E2;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-E3;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF6;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF4;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

6. **IDF6**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-E4;
   - 11 cavi UTP cat. 5e straight-through diretti ai due patch panel della stanza R-E5;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF1;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch IDF5;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

È evidente come alcuni switch rimangano con un discreto numero di porte libere (in particolare IDF4 e IDF6), la soluzione scelta tuttavia permette il collegamento di tutta una work area ad uno stesso switch; inoltre, la rimozione di IDF4, portando il numero degli switch a 5, causerebbe l'occupazione di tutte le porte eccetto 9, numero troppo esiguo per fornire la sicurezza di poter far fronte ad eventuali futuri guasti o espansioni dell'azienda in termini di nuove connessioni.

Riepilogo dell'utilizzo delle interfacce di ogni switch
(le porte non indicate sono inutilizzate; per il significato delle colonne 'Modalità' e 'Snooping' ci si riferisca alla sezione successiva):

IDF1

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-C1	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-C2	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-C3	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF2	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF6	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/1	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/1	1000	Trunk	trusted

TAB 3.1

IDF2

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-D1	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-D2	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-D3	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF3	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF1	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/2	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/2	1000	Trunk	trusted

TAB 3.2

IDF3

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-D4	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-D5	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-D6	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF4	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF2	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/3	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/3	1000	Trunk	trusted

TAB 3.3

IDF4

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-D7	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-D8	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF5	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF3	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/4	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/4	1000	Trunk	trusted

TAB 3.4

IDF5

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-E1	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-E2	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-E3	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF6	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF4	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/5	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/5	1000	Trunk	trusted

TAB 3.5

IDF6

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-E4	NIC dell'host	100	access	untrusted
FastEthernet 0/7-17	To R-E5	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To IDF1	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To IDF5	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/6	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/6	1000	Trunk	trusted

TAB 3.6

4.1 Main DF

Iniziamo determinando numero e tipo degli switch connessi alle work area degli stabili A e B.

Per gli stessi principi che hanno guidato la scelta dei dispositivi dell'IDF, optiamo per switch a 24 porte e decidiamo di connettere non più di 18 postazioni a ciascuno di essi, pertanto si rende necessario l'acquisto di 4 switch (approssimazione intera per eccesso della divisione 60 ÷ 18).
Premettiamo che il requisito di banda impone che sia prevista una crescita fino a 10Mbps per il traffico da ciascun host verso i server; questo significa che per le 60 postazioni di lavoro presenti nell'area Ovest dobbiamo garantire una velocità di 600Mbps. In particolare per uno switch (del tipo definito access) con collegati 18 host, l'uplink verso i dispositivi di livello superiore (del tipo definito distribution/access) dovrà poter sostenere una banda di 180Mbps (in realtà vedremo che le connessioni di questo genere sono due per ogni switch access, tuttavia in questo caso subentra il protocollo STP e si aggiungono considerazioni sulle VLAN coinvolte dai trasferimenti. È lecito comunque prendere per valida questa richiesta di banda per ognuno dei due collegamenti).

È chiaro comunque che in ogni caso i cavi in rame di tipo UTP cat. 5e sono più che sufficienti, in quanto un singolo cavo è in grado di sostenere un traffico dell'ordine di 1Gbps.

Rimane da determinare la tipologia delle interfacce interessate dai collegamenti fra gli switch di diverso livello. Sebbene infatti il vincolo in banda sia circoscritto al cablaggio si ritiene doveroso capire se sia possibile, a costi ragionevoli, tradurlo in termini di livello data link.
In pratica possiamo decidere di realizzare i collegamenti di uplink tramite Fast o Gigabit Ethernet: nel primo caso ipotizziamo che la reale esigenza di crescita sia posposta ad un futuro imprecisato e pertanto si realizza solo il vincolo più stringente di 1Mbps per postazione; nel secondo caso si ipotizza una crescita più rapida, tale da non rendere conveniente la sostituzione in tempi brevi degli switch installati con altri dotati di porte più veloci.
Per la precisione le alternative sono tre: Fast Ethernet, Gigabit Ethernet su rame e Gigabit Ethernet su fibra. Analizziamo pertanto rapidamente i pro e i contro di ciascuna soluzione.

- La versione su fibra comporta l'acquisto di switch del modello usato nell'IDF, più i moduli SFP per i due switch di livello superiore (si veda in seguito) per un totale calcolato di 14316 €, supponendo la spesa per le fibre ottiche irrisoria (si tratta di cavi che devono collegare dispositivi all'interno di uno stesso armadio). Avremmo già implementato il requisito della crescita 10x.
- La versione Gigabit Ethernet su rame comporta l'acquisto di switch con almeno due porte Gigabit Ethernet 1000BASE-T (come il modello 2950T-24), più una line card di porte 10/100/1000 BASE-T per ognuno degli switch di livello distribution/access, per un totale calcolato di 18306 €. Avremmo già implementato il requisito della crescita 10x.
- La versione Fast Ethernet comporta l'acquisto di usuali switch a porte 10/100 BASE-T, più una line card di porte 10/100 BASE-T per ognuno degli switch di livello distribution/access, per un totale calcolato di 11560 €. NON Avremmo implementato il requisito della crescita 10x.

(Più avanti la descrizione dei dispositivi di livello distribution/access. Il dettaglio dei costi è presentato nello predisposto capitolo.)

Esclusa la seconda soluzione, fra le rimanenti si è scelta la prima: anzitutto la spesa aggiuntiva di 2756 € pare non difficilmente sostenibile a fronte anche delle migliori prestazioni fornite; si è considerato poi che un'effettiva rapida crescita del traffico, con conseguente sostituzione dei dispositivi, verrebbe a costare considerevolmente di più.
Si procede così all'acquisto di 4 switch del modello 2950SX-24 CISCO descritto in precedenza.
E come in precedenza, si usano le due porte di uplink per effettuare un collegamento ridondante con i due switch di livello superiore, aumentando la robustezza dell'infrastruttura.
Delle 24 porte disponibili ne usiamo al massimo 18 per connettere apparati terminali così da collegare tutte le postazioni di lavoro di una work area ad un unico switch. Ad ogni dispositivo layer 2 quindi corrispondono dalle 2 alle 3 stanze complete.
Aumentiamo la robustezza della rete effettuando dei collegamenti, secondo una tipologia a ring, tra i dispositivi interni all'IDF.
Le porte rimaste libere garantiscono una adeguata precauzione nel caso di sviluppo dell'azienda o di guasti.

<u>Infine trattiamo degli switch di livello distribution/access.</u>

Ne abbiamo fissato il numero a due unità (li chiameremo in seguito MDF1 e MDF2), il minimo che permetta la connessione a tutti i server e switch access, un buon bilanciamento di carico nella comunicazione verso il router, l'indicazione di almeno due server per il protocollo VTP e due Root Bridge per lo STP, etc.

Risultano quindi collegati a MDF1 e MDF2 gli switch di livello access, l'intera server farm e il router (il quale ricordiamo essere già stato analizzato nel capitolo 'Router e Rete intersede').
In particolare si è deciso di connettere ad essi i server, piuttosto che ad un altro switch dedicato, in modo da ridurre la latenza, cioè il tempo che un pacchetto impiega per giungere a destinazione, che aumenta aggiungendo dispositivi lungo il percorso del pacchetto stesso.
In realtà la situazione è più complicata: quando infatti un host invia un pacchetto diretto ad un server, se questi non è uno dei workgroup server, cioè non fa parte della stessa sottorete, è necessaria la comunicazione con una VLAN differente da quella di partenza. Entra dunque in gioco il router, in quanto una delle sue sottointerfacce sarà il default gateway dell'host in questione, il quale inoltrerà il tutto all'interfaccia corrispondente alla VLAN 21 o 22 (la Global VLAN e la Server VLAN discusse nel capitolo 'Router e Rete intersede'), raggiungendo così lo switch collegato ad essa (MDF1). Se ora il server di destinazione fosse connesso a MDF2 si avrebbe comunque l'attraversamento di un nodo in più rispetto a quanto strettamente necessario. Una possibile soluzione è quella di connettere i server globali (SMTP e HTTP) ed enterprise, accessibili da tutta l'azienda, allo switch MDF1 e i workgroup allo switch della corrispondente VLAN (quello che, per tale VLAN, è stato definito Root Bridge per il protocollo STP). È chiaro che questo porterebbe però ad una disparità nel numero di dispositivi connessi a ciascuno dei due switch, con problemi per l'acquisto di slot con un adeguato numero di porte. Si è scelta pertanto per semplicità una soluzione intermedia, decidendo di collegare a MDF1 e MDF2 massimo 24 server a testa.
Altra riflessione da fare concerne i requisiti di banda: la solita richiesta espressa per il cablaggio comporterebbe il sostenimento di una velocità di 1610Mbps (10 Mbps per ogni postazione di lavoro) verso ciascuno dei server. Ciò legittima l'uso della fibra ottica nel collegamento fra questi e gli switch, tuttavia richiederebbe, se trasportassimo il problema a livello data link, interfacce più prestanti rispetto alle Gigabit Ethernet. Ci limiteremo a installare pertanto porte basate su tecnologia 1000BASE-SX, lasciando l'acquisto delle interfacce a 10 Gbps per il futuro: risultando considerevolmente costose infatti non sono ritenute convenienti nell'immediato. Questa soluzione provvisoria ci permette peraltro di realizzare il vincolo qualora lo si intenda rivolto non al singolo server ma all'insieme dei server.
Colleghiamo fra loro MDF1 e MDF2 tramite due (per robustezza) cavi bifibra: saranno utili per la comunicazione verso i server, non workgroup, connessi a MDF2 e, comunque, nel caso un collegamento tra uno switch access e gli switch di livello superiore dovesse presentare malfunzionamenti. Li colleghiamo inoltre anche al router. Queste quattro connessioni sono tutte effettuate con cavi bifibra. Per le interfacce valgono le considerazioni fatte in merito alla banda diretta verso i server, dato che il traffico che le può teoricamente interessare è dello stesso ordine di grandezza (ciascuna postazione di lavoro per inviare un pacchetto ad un server globale o enterprise dovrà necessariamente inoltrarlo al suo default gateway, cioè ad una sottointerfaccia del router): quindi si applicano porte Gigabit Ethernet rimandando eventualmente al futuro l'installazione di porte da 10Gbps. Si tenga presente poi che sulla sottointerfaccia del router associata alla Global VLAN sarà indirizzato anche il traffico extra-sede diretto ai server HTTP e SMTP.
Infine per come abbiamo realizzato il cablaggio verticale e per la scelta dei dispositivi di livello access, dobbiamo fornire il supporto per la tecnologia 1000BASE-SX anche per il collegamento con tutti gli altri switch.

Stabilite queste condizioni, un modello confacente alle nostre necessità è il 4503 CISCO, integrato con la line card WS-X4448-GB-SFP, che fornisce 48 porte 1000BASE-X. Chiaramente per ciascuna porta che si vorrà utilizzare è necessario acquistare anche il relativo modulo SFP 1000BASE-SX. Per ognuno dei due switch serviranno pertanto

24 (server) + 6 (IDF) + 4 (MDF3/6) + 2 (MDF1/2) + 1 (router) = 37 transceiver SFP

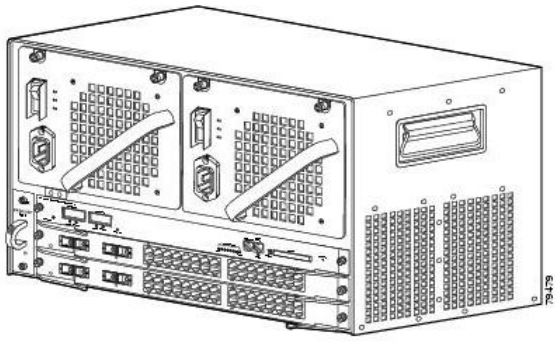


FIG. 3.11 – Lo switch CISCO Catalyst 4503 Chassis (3-slot)

FIG. 3.12 – La line card 48-Port 1000Base-X (SFPs Optional)

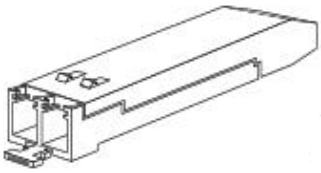


FIG. 3.13 – Transceiver SFP Module

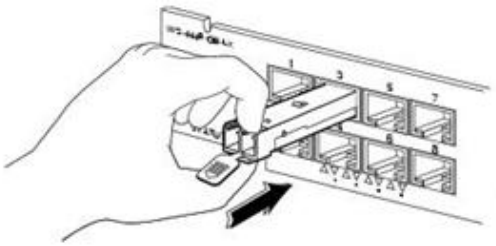


FIG. 3.14 – Inserimento di un modulo SFP

L'interfaccia utilizzata presenta porte con connettori di tipo Lucent (LC) avremo bisogno dunque di patch cord verso i pannelli di permutazione con connettori LC da un capo e SC dall'altro, mentre i cavi che collegano MDF1 e MDF2 hanno entrambi connettori LC.

FIG. 3.15 – Double LC Connector

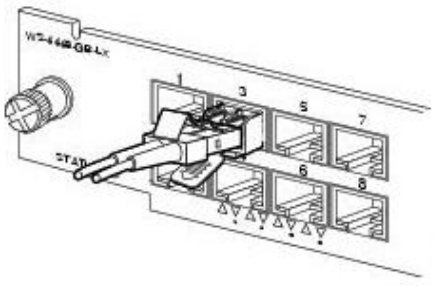


FIG. 3.16 – Collegamento di Connettori LC al Modulo SFP

Infine sul router, per permettere la comunicazione di tipo 1000BASE-SX, installiamo due interfacce Gigabit Interface Converter (GBIC), che supportano connettori di tipo SC. Saranno necessari due cavi bifibra duplex con connettori LC – SC per collegare il router con MDF1 e MDF2.

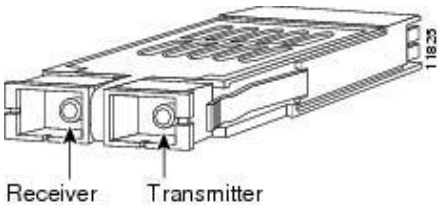


FIG. 3.17 – GBIC (GigaBit Interface Converter)

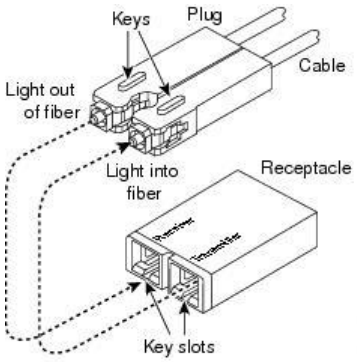


FIG. 3.18 – Connettore per fibra ottica di tipo SC

In seguito ci riferiamo ai dispositivi del Main Distribution Facility utilizzando un'etichetta del tipo 'MDFX' dove X è un numero progressivo a partire da 1 (MDF1 e MDF2 sono gli switch di livello distribution/access, gli altri 4 sono di livello access).

Riepilogo dei cavi collegati ad ogni switch:

1. **MDF1 (tutto su Gigabit Ethernet)**
   - 6 bretelle MMF dirette ai patch panel per la connessione agli switch IDF1 – IDF6;
   - 4 bretelle MMF dirette ai patch panel per la connessione agli switch MDF3 – MDF6;
   - 24 bretelle MMF dirette ai patch panel per la connessione a 24 server (e.g. R-A1);
   - 1 bretella MMF diretta verso il router;
   - 2 bretelle MMF dirette verso MDF2;

2. **MDF2 (tutto su Gigabit Ethernet)**
   - 6 bretelle MMF dirette ai patch panel per la connessione agli switch IDF1 – IDF6;
   - 4 bretelle MMF dirette ai patch panel per la connessione agli switch MDF3 – MDF6;
   - 24 bretelle MMF dirette ai patch panel per la connessione a 24 server (e.g. R-A2);
   - 1 bretella MMF diretta verso il router;
   - 2 bretelle MMF dirette verso MDF1;

(le ultime due voci si riferiscono alle porte Gigabit Ethernet, tutte le altre a porte FastEthernet):

3. **MDF3**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A3;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A4;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A5;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF4;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF6;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

4. **MDF4**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A6;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A7;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-A8;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF5;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF3;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

5. **MDF5**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-B1;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-B2;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF6;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF4;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

6. **MDF6**
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-B3;
   - 6 cavi UTP cat. 5e straight-through diretti al patch panel della stanza R-B4;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF3;
   - 1 cavo UTP cat. 5e cross-over diretto allo switch MDF5;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF1;
   - 1 bretella MMF diretta al patch panel per la connessione allo switch MDF2;

Riepilogo dell'utilizzo delle interfacce di ogni switch
(le porte non indicate sono inutilizzate; per il significato delle colonne 'Modalità' e 'Snooping' ci si riferisca alla sezione successiva):

MDF1

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
Gigabit Ethernet 0/1-6	To IDF1 – IDF6	Gigabit Ethernet 1/1	1000	trunk	untrusted
Gigabit Ethernet 0/7-10	To MDF3 – MDF6	Gigabit Ethernet 1/1	1000	trunk	untrusted
Gigabit Ethernet 0/22-45	To Server R-A1	NIC del server	1000	access	untrusted
Gigabit Ethernet 0/46-47	To MDF2	Gigabit Ethernet 0/46-47	1000	trunk	trusted
Gigabit Ethernet 0/48	To Router	Gigabit Ethernet 2/0	1000	trunk	trusted

TAB 3.7

MDF2

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
Gigabit Ethernet 0/1-6	To IDF1 – IDF6	Gigabit Ethernet 1/2	1000	trunk	untrusted
Gigabit Ethernet 0/7-10	To MDF3 – MDF6	Gigabit Ethernet 1/2	1000	trunk	untrusted
Gigabit Ethernet 0/22-45	To Server R-A2	NIC del server	1000	access	untrusted
Gigabit Ethernet 0/46-47	To MDF1	Gigabit Ethernet 0/46-47	1000	trunk	trusted
Gigabit Ethernet 0/48	To Router	Gigabit Ethernet 3/0	1000	trunk	trusted

TAB 3.8

MDF3

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-A3	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-A4	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-A5	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To MDF4	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To MDF6	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/7	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/7	1000	Trunk	trusted

TAB 3.9

MDF4

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-A6	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-A7	NIC dell'host	100	access	untrusted
FastEthernet 0/13-18	To R-A8	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To MDF5	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To MDF3	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/8	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/8	1000	Trunk	trusted

TAB 3.10

MDF5

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-B1	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-B2	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To MDF6	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To MDF4	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/9	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/9	1000	Trunk	trusted

TAB 3.11

MDF6

Interfaccia/e	Descrizione	Interfaccia del vicino	Velocità (Mbps)	Modalità	Snooping
FastEthernet 0/1-6	To R-B3	NIC dell'host	100	access	untrusted
FastEthernet 0/7-12	To R-B4	NIC dell'host	100	access	untrusted
FastEthernet 0/23	To MDF3	FastEthernet 0/24	100	trunk	trusted
FastEthernet 0/24	To MDF5	FastEthernet 0/23	100	trunk	trusted
Gigabit Ethernet 1/1	To MDF1	Gigabit Ethernet 0/10	1000	trunk	trusted
Gigabit Ethernet 1/2	To MDF2	Gigabit Ethernet 0/10	1000	Trunk	trusted

TAB 3.12

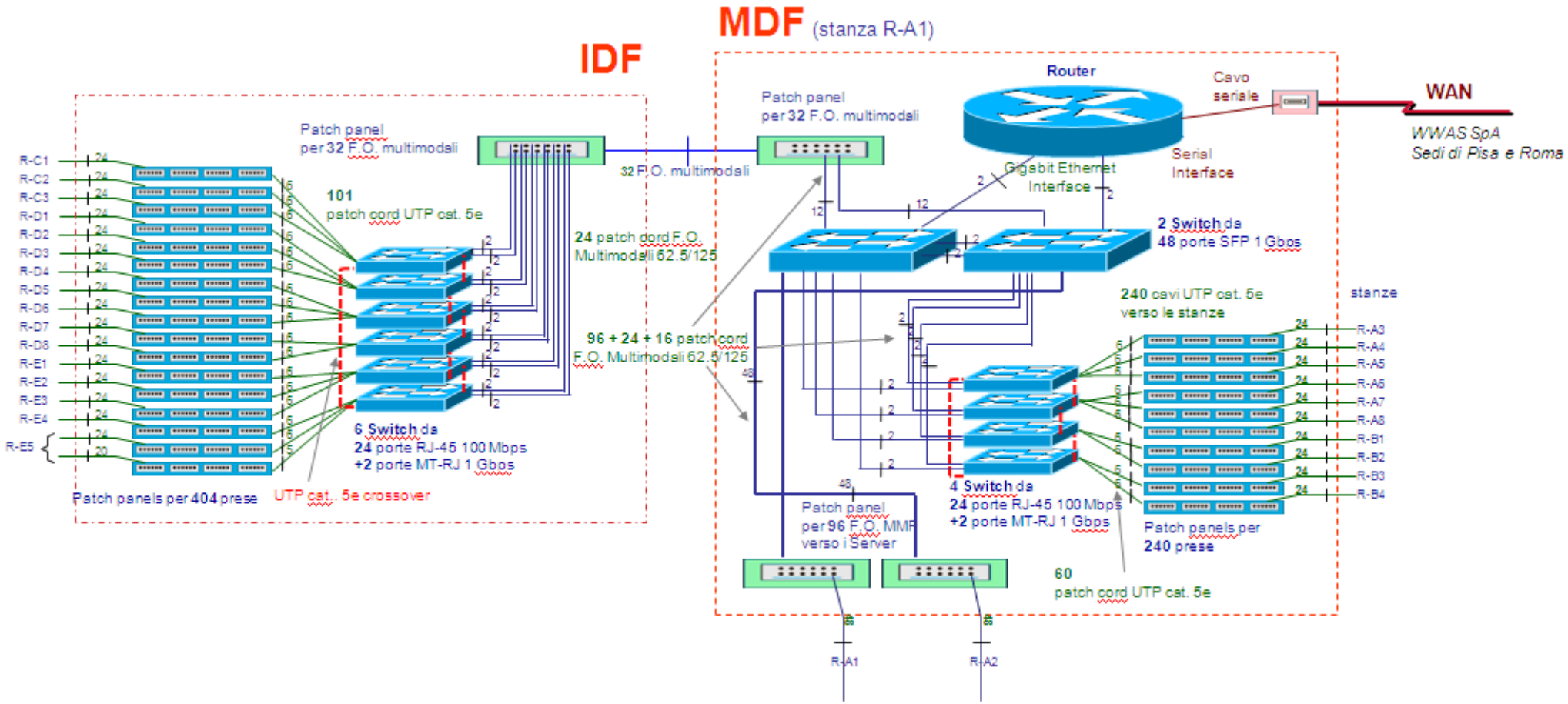


FIG. 3.19 – Cablaggio e apparati attivi (switch e router)

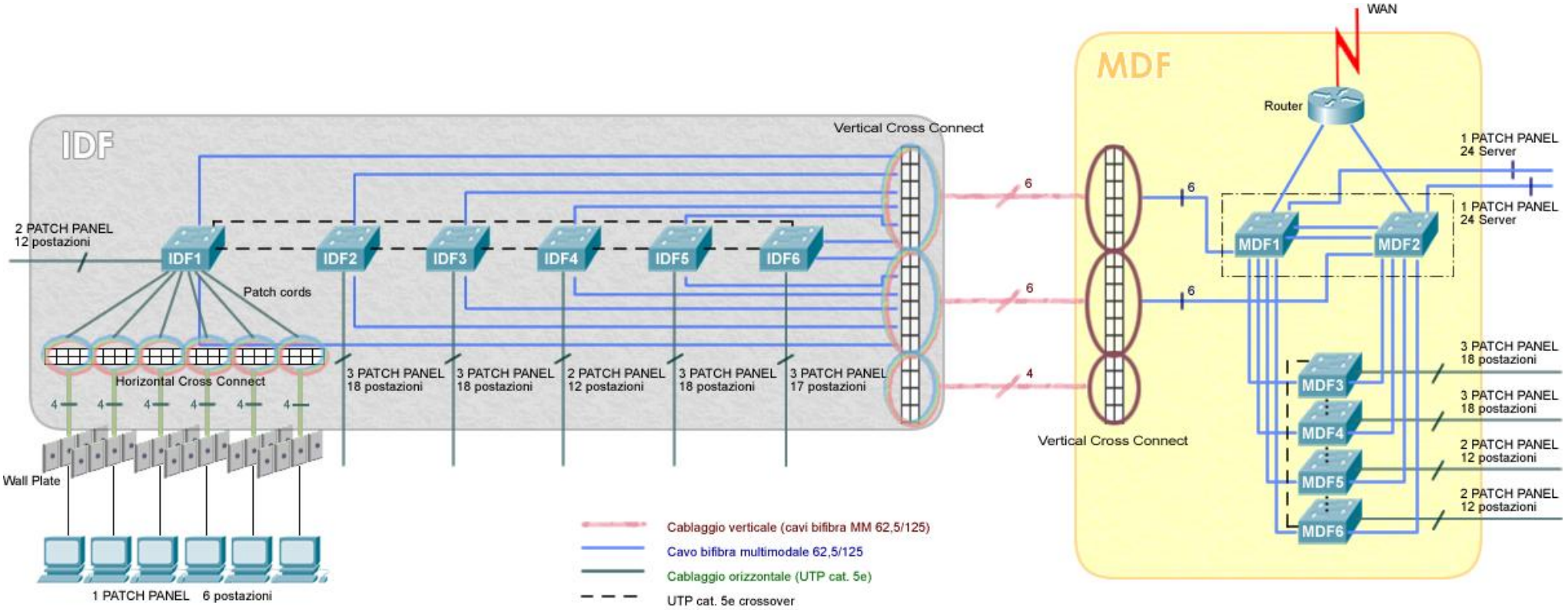


FIG. 3.20 – Mappa Logica

I dispositivi collocati nei due armadi di distribuzione devono essere opportunamente configurati.
A tal proposito si rimanda al capitolo 'Router e Rete intersede' per la configurazione del router e per la descrizione delle VLAN create.
Si premette che ora presentiamo solo descrizioni e spiegazioni circa le configurazioni esposte nella relativa appendice.

5.1 Domini di sicurezza (VLAN)

Come presentato nelle precedenti sezioni, impostiamo delle Virtual LAN per implementare il requisito dei domini di sicurezza/gruppi di lavoro: abbiamo già stabilito le 8 VLAN necessarie e gli ID per ciascuna sede, oltre a ciò, per consentire l'inter-VLAN routing, abbiamo attribuito le VLAN dalla 21 alla 25 (Global, Server, Marketing, Supporto Sistemi, Direzione e Amministrazione VLANs) all'interfaccia 2/0 del router e quelle dalla 26 alla 28 (i tre gruppi di progetto di Ricerca e Sviluppo) all'interfaccia 3/0.
Per il traffico inter-switch, si è deciso di adottare la soluzione di frame tagging, classificando e suddividendo le porte di ciascuno, in **access**, qualora vi siano connessi dispositivi terminali, o **trunk**, qualora vi siano connesse macchine layer 2 o 3 (per maggiore chiarezza ci si riferisca alle precedenti tabelle). Non abbiamo ritenuto necessario dover indicare per ciascun link quali siano le Virtual LAN i cui pacchetti sono abilitati alla trasmissione, in quanto il protocollo VTP che attiviamo fornisce già questa funzionalità (grazie alla funzione di *pruning*).
Proprio per rendere più agevoli le modalità di aggiunta, modifica, eliminazione delle VLAN, nonché la gestione degli scambi di pacchetti afferenti a diversi domini di sicurezza tra gli switch, sfruttiamo il *Virtual Trunking Protocol*. Questo protocollo, proprietario CISCO, prevede l'elezione a server VTP di due switch, che abbiamo pertanto individuato in MDF1 e MDF2. La scelta di più dispositivi permette l'aggiornamento delle informazioni sulle VLAN anche qualora si verificasse un guasto in uno dei due; in caso di malfunzionamento poi, con un solo server, perderemmo ogni impostazione sulle macchine client al loro primo riavvio.
Il principale vantaggio introdotto da questo protocollo è però un altro, il già menzionato 'VLAN pruning': evita che si verifichi il fenomeno del *broadcast flooding*, ovverosia ogni qual volta un pacchetto di una qualche VLAN giunga ad uno switch, da cui debba essere trasmesso in modalità broadcast, questo lo inoltra esclusivamente su quei link da cui è effettivamente possibile raggiungere (eventualmente attraversando altri switch) host appartenenti a quella VLAN; il risparmio in banda risulta evidente.
Per i link di tipo trunk impieghiamo l'incapsulamento previsto dallo standard 802.1Q dell'IEEE
(in seguito presupporremo che il sistema operativo installato sugli switch abbia questa impostazione di default).

Dobbiamo dunque:

- creare un dominio VTP (unico per l'intera sede di Padova);
- stabilire la versione VTP da utilizzare nel dominio (si è deciso per la versione 1);
- scegliere una password di sicurezza ("*cisco"*);
- abilitare MDF1 e MDF2 come server VTP;
- impostare tutti gli altri switch come *client*;
- attivare il *VLAN pruning* su uno dei due server;
- disabilitare il *Dynamic Trunking Protocol* (DTP) in quanto è già stato indicato per ogni dispositivo quali sono le porte di tipo trunk.

5.2 Spanning Tree Protocol

I molti collegamenti ridondanti che abbiamo presentato nella fase di scelta e collocamento degli switch, se da un lato accrescono la robustezza dell'infrastruttura, dall'altra costituiscono dei loop, dei cicli, che la sottopongono al problema dei *broadcast storm*. Per evitare che pacchetti di tipo broadcast attraversino per un numero tendenzialmente infinito la nostra rete, attiviamo il protocollo STP.
In aggiunta a queste ragioni lo STP ci permette di soddisfare il requisito di progetto secondo cui

> *"il backbone della rete **di sede** deve garantire tempi di interruzione della connessione non superiori al centinaio di secondi"*.

Infatti qualora per un guasto dello switch o di un link, su una porta non dovessero più arrivare BPDU, il protocollo provvederebbe autonomamente a far passare la porta su cui abbiamo realizzato il collegamento ridondante, dallo stato di *'blocking'* a quello di *'forwarding'* (passando dalle fasi intermedie di *'listening'* e *'learning'*), in un tempo previsto di circa 50 secondi, ossia la metà di quanto richiesto.
Pertanto non ci pare opportuno modificare i parametri relativi al diametro della rete: sebbene i valori standard (diametro pari a 7) ipotizzino una rete di dimensioni più grandi della nostra, il protocollo opererà in modo solo leggermente subottimale, con svantaggi trascurabili.
Dobbiamo invece stabilire i *Root Bridge* e ancora una volta li individuiamo in MDF1 e MDF2 (sono infatti di livello superiore agli altri). Dobbiamo osservare anche che lo STP può essere configurato diversamente per le varie Virtual LAN, pertanto è opportuno tenere conto di come queste possano influire sull'azione del protocollo stesso.
Si considerino infatti le VLAN attribuite alle varie sottointerfacce del router nelle Gigabit Ethernet 2/0 e 3/0: per ciascuna VLAN evidentemente converrà rendere Root Bridge lo switch che è connesso alla relativa interfaccia sul router; questo infatti permetterà una più rapida comunicazione fra host e default gateway, oltre a un bilanciamento del carico tra i due dispositivi. L'altro switch in ogni caso è elevato a livello di Root Bridge secondario.
Pertanto

- MDF1 diventa Root Bridge primario per le VLAN 21, 22, 23, 24, 25;
- MDF2 diventa Root Bridge primario per le VLAN 26, 27, 28.

Lo si ottiene stabilendo un'alta priorità per lo switch. Nella fattispecie la priorità è stabilita a 4096 per quelle VLAN per cui il dispositivo è Root Bridge primario, a 8192 per tutte le altre. Gli altri switch invece mantengono il valore di default, 32768 (in seguito presupporremo che il sistema operativo installato sugli switch abbia questa impostazione di default).

Mediante l'utilizzo della versione proprietaria CISCO del protocollo, PVST+, è possibile usare la modalità *PortFast* nella configurazione delle porte di uno switch. Essa è particolarmente utile in quanto permette un passaggio istantaneo dalla fase di 'blocking' a quella di 'forwarding', rendendo rapidamente la porta in grado di funzionare, ricevendo e trasmettendo pacchetti. Chiaramente questa opzione la si può usare in sicurezza solo su quelle porte per cui è prevista la connessione con dispositivi terminali (esclusi i casi dove siano presenti cicli di livello 1; in pratica il collegamento deve essere diretto ad un singolo host).

La figura 3.21 riassume la situazione delle VLAN per quanto riguarda il numero e la descrizione degli host, l'inter-VLAN routing, il protocollo STP.

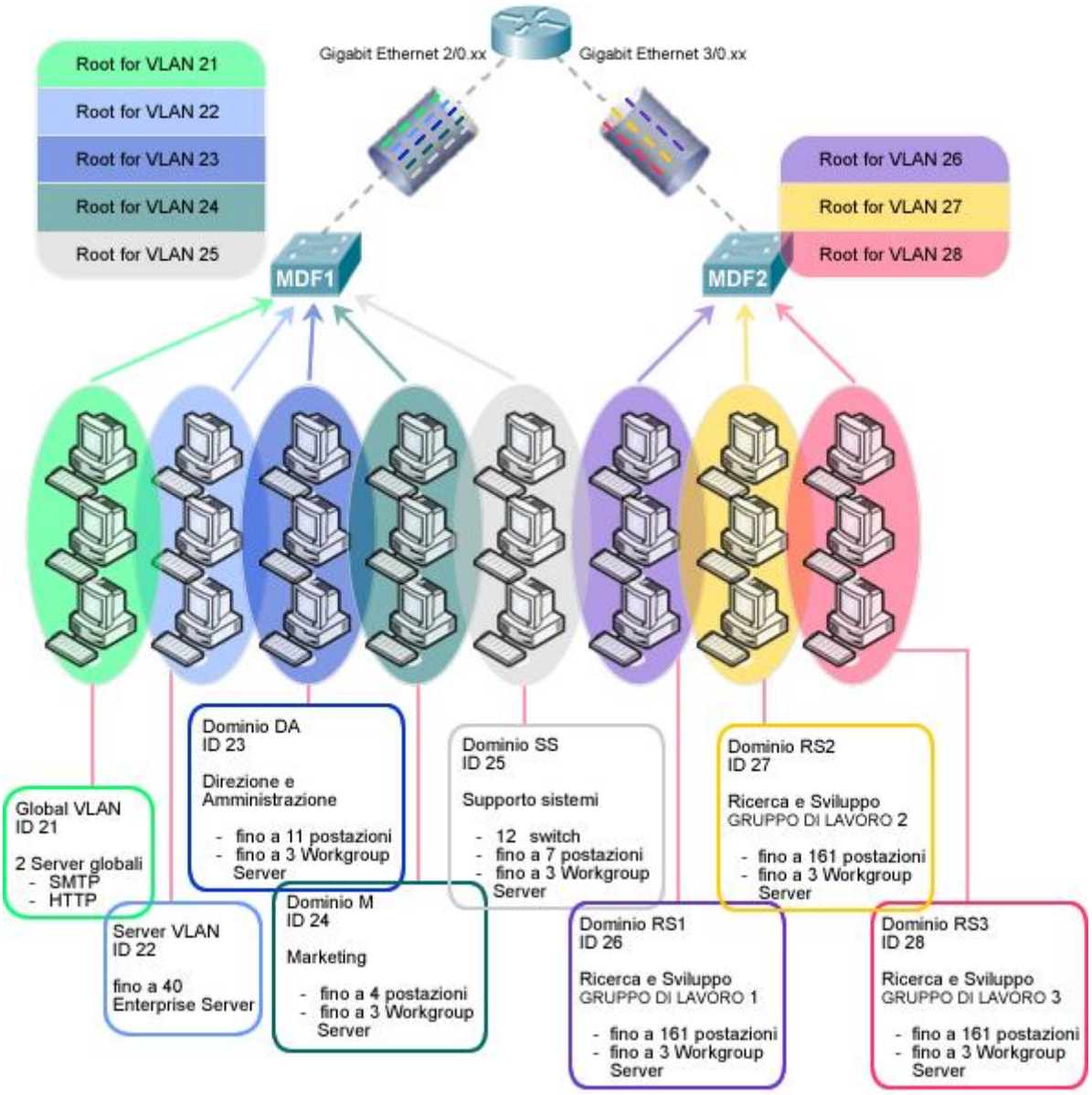


FIG. 3.21 – VLAN, STP e inter-VLAN routing

5.3 Indirizzi degli switch

Come da specifiche, il settore 'Supporto Sistemi' deve poter accedere a tutti i dispositivi: si rende pertanto necessario attribuire indirizzi IP anche agli switch, prelevandoli dal pool a disposizione del dominio SS (VLAN 25). La scelta deve essere consistente con le considerazioni fatte sul DHCP nel capitolo 'Router e Rete intersede'. Le tabelle seguenti riassumono lo stato delle interfacce di configurazione (i 3 indirizzi riservati rimanenti sono per i Workgroup Server del dominio SS).

Switch	Indirizzo	Subnet Mask
MDF1	172.16.211.80	255.255.255.224
MDF2	172.16.211.81	255.255.255.224
MDF3	172.16.211.82	255.255.255.224
MDF4	172.16.211.83	255.255.255.224
MDF5	172.16.211.84	255.255.255.224
MDF6	172.16.211.85	255.255.255.224

TAB 3.13

Switch	Indirizzo	Subnet Mask
IDF1	172.16.211.86	255.255.255.224
IDF2	172.16.211.87	255.255.255.224
IDF3	172.16.211.88	255.255.255.224
IDF4	172.16.211.89	255.255.255.224
IDF5	172.16.211.90	255.255.255.224
IDF6	172.16.211.91	255.255.255.224

TAB 3.14

5.4 Sicurezza

È necessario adottare alcune misure per garantire la sicurezza della rete:

i. fissare il banner di apertura;
ii. stabilire le password;
iii. disabilitare il protocollo CDP;
iv. disattivare le porte non utilizzate;
v. implementare il DHCP *snooping*;
vi. stabilire e impostare una politica di *port security*.

Analizziamo singolarmente ciascun punto.

- Il banner di apertura avverte un utente che si connetta ad un dispositivo, che sta accedendo ad un'infrastruttura di rete privata e pertanto ogni tentativo di manomissione o alterazione è legalmente perseguibile. La frase scelta:
  "Swicth WWAS Padova *nome dispositivo**: l'accesso e' vietato ai non autorizzati, ogni abuso e' legalmente perseguibile"*.

- Stabiliamo in *'class'* la password per il login tramite console e telnet e in *'cisco'* la password per l'accesso alla modalità di configurazione.

- Il *Cisco Discovery Protocol* è, come suggerisce il nome, un protocollo proprietario CISCO, che permette l'individuazione dei dispositivi CISCO adiacenti a quello in uso. Sebbene di indubbia utilità in fase di *troubleshooting*, lo scambio di informazioni sensibili tra i vari dispositivi e verso l'esterno della rete, rende particolarmente vulnerabile l'infrastruttura ad attacchi di utenti malintenzionati, sconsigliandone l'attivazione.

- Come risulta evidente dalla fase di collegamento degli switch con i rispettivi dispositivi terminali, l'utilizzo di talune porte non è previsto, pertanto devono essere disabilitate. In seguito sarà la funzione Supporto Sistemi a decidere per un eventuale loro impiego e quindi per la loro abilitazione. Lo stesso facciamo per tutte quelle porte per cui sia stata prevista una connessione con un host ma il collegamento non sia stato ancora realizzato.

- Il DHCP snooping è una impostazione di sicurezza che verifica la provenienza da fonte ritenuta attendibile, di ogni risposta DHCP che perviene alla porta di uno switch.
  Come evidenziato nelle tabelle dalla 3.1 alla 3.12, per ogni dispositivo si devono indicare le porte su cui la consegna di un riscontro DHCP è considerabile affidabile (trusted) o meno (untrusted). In particolare tenendo presente che l'unico server DHCP interno alla sede coincide col router di frontiera abbiamo che:
  - tutte le porte direttamente connesse a macchine terminali sono da considerarsi *untrusted*;
  - le porte di MDF1 e MDF2 collegate agli switch di livello access sono *untrusted*, mentre sono *trusted* quelle rivolte verso il router o verso l'altro switch di pari livello;
  - le porte degli switch access connesse ad altri switch sono tutte *trusted*.

  Questa opzione previene dunque il fenomeno dello *spoofing*, ossia il sostituirsi, da parte di un utente malintenzionato, al previsto server DHCP, fornendo false informazioni ai client o proponendosi come default gateway o server DNS.

- La configurazione della port security consente l'accertamento dei dispositivi terminali connessi alla rete, mediante la memorizzazione degli indirizzi MAC. Ciò significa che per ogni switch salviamo gli indirizzi delle macchine end-user collegate (evidentemente su porte

di tipo *access*), in modo da poter riconoscere eventuali connessioni inaspettate: nel caso siano individuati host non previsti la porta automaticamente si disabilita; in questa maniera si evita il collegamento con device di intrusi o comunque non programmati in fase di progettazione. Pertanto stabiliamo che il numero massimo di indirizzi MAC riscontrabili su ciascuna porta sia al massimo uno.
Inoltre gli indirizzi che pervengono allo switch, al primo utilizzo, vengono prima memorizzati nella running-configuration (apprendimento detto *sticky*) ed in seguito salvati nella startup-configuration ad opera degli addetti alla funzione Supporto Sistemi, in modo da renderli validi anche ai successivi riavvii dei dispositivi.
Chiaramente nel caso si dovesse provvedere a sostituzione o aggiunta di host alla rete sarà necessario prima liberare la tabella degli indirizzi MAC della running-configuration dello switch interessato (disabilitando l'apprendimento sticky) e salvare la stessa in NVRAM, effettuare il reload sullo switch e solo infine connettere il nuovo dispositivo, salvando poi nuovamente nella startup-configuration.

6. Simulazione con Packet Tracer 5

Alleghiamo la simulazione della rete di Padova realizzata con Packet Tracer 5.
Le limitazioni del programma hanno imposto alcune variazioni rispetto a quanto enunciato finora:

- I pochi switch messi a disposizione non hanno un sufficiente numero di porte per la comunicazione tramite fibra ottica o comunque con tecnologia Gigabit Ethernet, pertanto sono stati utilizzati dispositivi dotati solamente di porte FastEthernet;
- Non ci sono dispositivi con 48 porte, dunque MDF1 e MDF2 sono stati rappresentati con switch a 24 porte;
- Globalmente l'uso nella simulazione di switch diversi da quelli previsti ha comportato una diversa distribuzione dei collegamenti tra le varie porte, rispetto a quanto presentato;
- Si sono considerati un numero simbolico di macchine terminali e server, a titolo di esempio, con lo scopo di verificare/mostrare la funzionalità del progetto;
- La simulazione riguarda esclusivamente la sede di Padova;
- Non è supportato il DHCP snooping;
- Non è supportato il VTP pruning.

La figura seguente chiarisce la topologia della rete simulata.

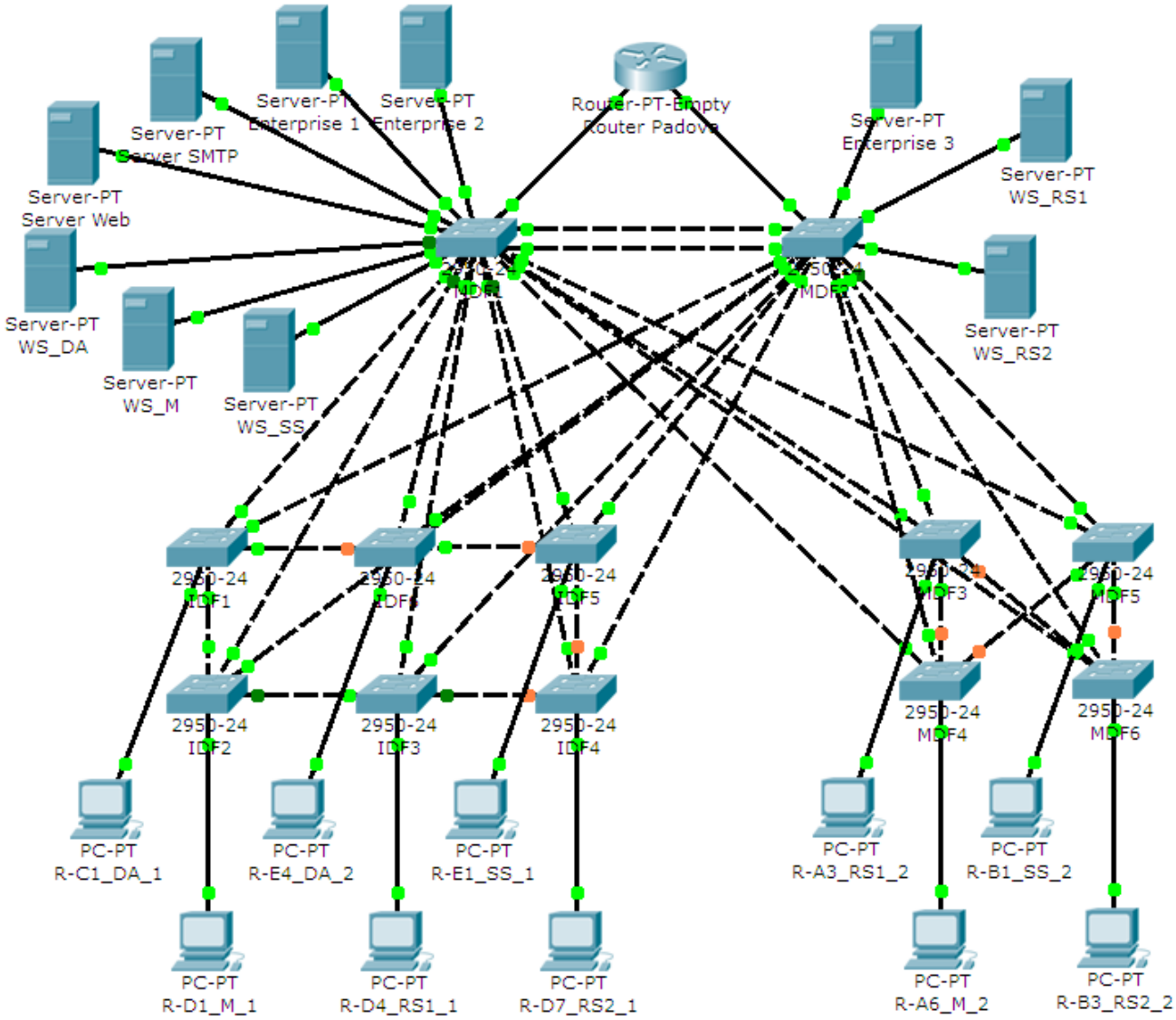


FIG. 3.22 – Simulazione della rete di Padova con Packet Tracer 5

1. Collocazione Armadi e Cablaggio

Cominciamo ora con la progettazione della rete della sede di Pisa.
Per adesso ignoriamo quali dispositivi siano presenti negli xDF e concentriamoci sulla collocazione degli stessi.
Il MDF (Main Distribution Facility) si troverà, come di consueto, in corrispondenza del POP ossia del punto di connessione alla rete WAN.
Il MDF conterrà i dispositivi necessari alla connessione alla rete telematica di tutte le macchine presenti nell'edificio Pisa-Est, il nome assegnatoli è **Pisa-MDF**.
Sono state scelte le stanze destinate ad ospitare i server, evidenziate in figura 4.1.
Nelle figure a seguire viene evidenziata la numerazione delle stanze: i numeri in grassetto presenti al centro delle stanze da cablare costituiscono la numerazione utilizzata in questa sezione del progetto.

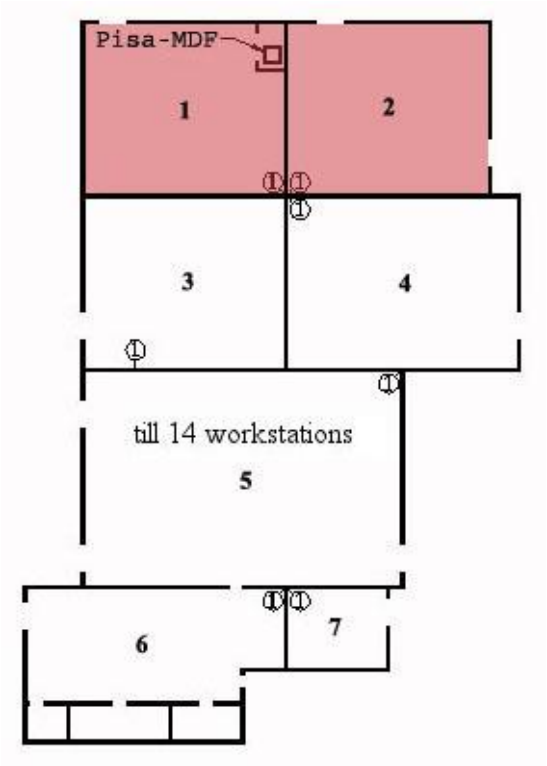


FIG 4.1 PISA-EST

Secondo gli standard TIA/EIA-568-B (il più recente per il cablaggio degli edifici) e TIA/EIA-569, i collegamenti orizzontali e verticali possono avere la lunghezza massima (dalla Telecommunications Room alle Work Area per il cablaggio orizzontale, dalla Telecommunication Room ad altre Telecommunications Room per il cablaggio verticale) pari a 90m (se si usano collegamenti in rame di tipo UTP cat5e).
Questo limite massimo di lunghezza implica che, considerando i percorsi obbligati dei cavi, conviene fare dell'MDF il centro di connessione alla rete telematica del solo edificio Pisa-est (per gli altri edifici prevediamo altre Distribution Facility).
Notiamo dalle mappe fornite dalla WWAS che vi è un condotto preesistente per far passare i cavi per il cablaggio verticale verso l'Edificio Pisa-sud, conviene allora mettere un IDF come centro della rete telematica dell'edificio Pisa-sud all'uscita di tale condotto, la sua posizione viene evidenziata in figura 4.2.
Il nome dato a questo IDF è **Pisa-IDF-sud**, i dispositivi contenuti verranno illustrati in seguito.

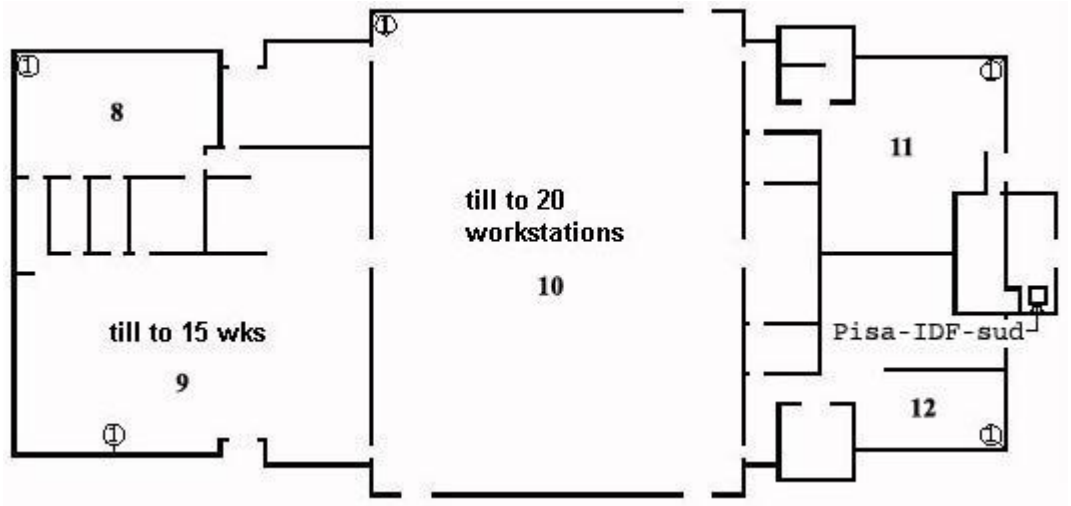


FIG 4.2 PISA-SUD

Per il terzo edificio da cablare, si prevede di far correre i cavi per il cablaggio verticale all'interno del condotto preesistente che collega l'edificio Pisa-est all'edificio Pisa-nord, e si posiziona un secondo IDF (**Pisa-IDF-nord**) nel punto indicato in figura 4.3.
La scelta di non metterlo direttamente davanti all'uscita del condotto è stata guidata dal fatto che la stanza 27 è una stanza dove 6 persone (al massimo) lavorano alle loro postazioni, e dunque operazioni di manutenzione o controlli dei dispositivi nell'IDF risultano più complessi perché potrebbero dover essere effettuati durante il lavoro degli impiegati, inoltre lasciando l'IDF-nord in una stanza di lavoro (come la 27) risulta più difficile impedire al personale di causare danni alle apparecchiature.

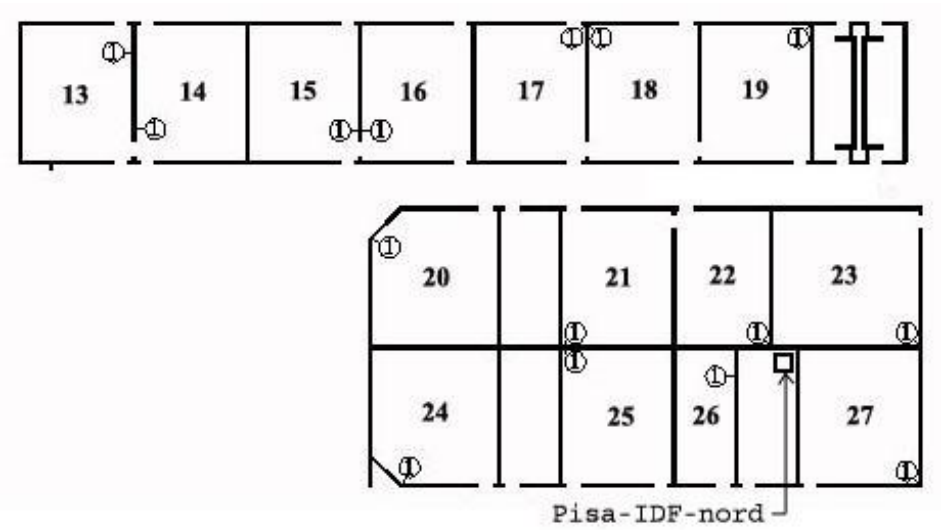


FIG 4.3 PISA-NORD

La scelta delle posizioni degli IDF negli edifici interessati è stata guidata dal criterio di bilanciare la distanza che il cavo deve percorrere per arrivare dall'IDF al MDF e quella che invece deve percorrere per arrivare alle diverse Work Area (partendo dall'IDF o dall'MDF), in modo da rispettare lo standard TIA/EIA-568-B.

Indipendentemente dall'xDF, i cavi per il cablaggio orizzontale (cavi che si stendono dagli xDF alle work area) che partono dai patch panel nella Telecommunication Room vengono fatti passare nello spazio disponibile tra il controsoffitto e il soffitto della struttura (2 piedi, circa 60 cm).
Si possono bucare le pareti che separano le camere e far scendere i cavi lungo i muri (eventualmente coperti da canali di materiale plastico, oppure all'interno della parete), fino ai punti di presenza, ognuno dei quali conta 4 prese di rete.
Invece, come si è visto, tutti i cavi per il cablaggio verticale che mettono in comunicazione le Telecommunications Room si fanno passare nei condotti preesistenti della sede di Pisa.
Notiamo che il canale preesistente che collega l'edificio Pisa-est all'edificio Pisa-nord si interrompe quando arriva alla stanza 27. Da questa i cavi per il cablaggio verticale devono essere portati all'IDF-nord, e questo si può fare facendoli correre lungo la parete interna della stanza 27 e sfruttando lo spazio dovuto al controsoffitto per portare i cavi nella stanza dell'IDF (forando le pareti sul percorso).

Per la connessione dei server all'infrastruttura di rete, i cavi nella stanza 1 vengono portati direttamente all'MDF, facendoli passare in canali di materiale plastico applicati alle pareti; i cavi della stanza 2 vengono anch'essi connessi direttamente all'MDF, eventualmente si può pensare di forare la parete che separa la stanza 1 dalla stanza 2 piuttosto che far passare i cavi nello spazio dovuto al controsoffitto (specialmente perché, come si vedrà in seguito, questi cavi sono in fibra ottica e dunque è necessario maneggiarli con cura).

Per connettere i dispositivi terminali all'IDF-nord si devono collegare i due fabbricati di cui si compone l'edificio Pisa-nord tramite un canale in materiale plastico (mostrato nella figura 4.4 a seguire).

Si può allora dare la mappa fisica, completa dei percorsi del cablaggio verticale (FIG 4.4).

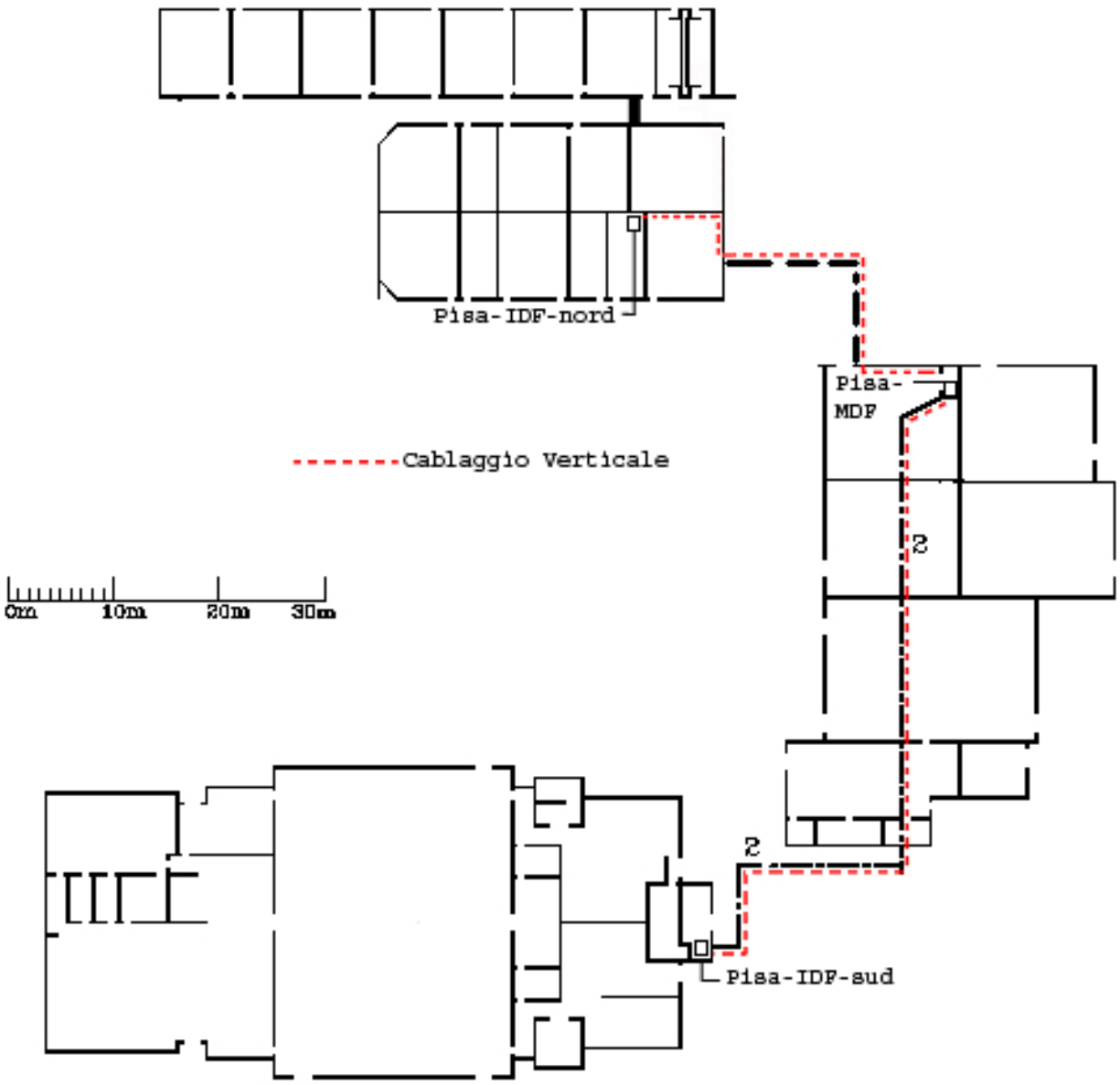


FIG 4.4 MAPPA FISICA (PERCORSI)

Notare che per adesso non si hanno informazioni sul numero o sul tipo dei cavi che costituiscono le linee evidenziate in figura.

Cerchiamo adesso di capire quali dispositivi verranno contenuti negli IDF e nel MDF.
In generale si è scelto di utilizzare come switch per il livello access della rete il modello 2950-24 (sigla completa WS-C2950-24) della CISCO, il quale fornisce 24 porte fastEthernet, seguendo il seguente principio:

- Per aumentare la robustezza della rete è preferibile comprare molti dispositivi con poche porte ognuno
- Per diminuire i costi della rete è preferibile comprare pochi dispositivi con molte porte ognuno

Cercando di arrivare ad un compromesso, è stata individuata nel modello 2950-24 la miglior soluzione.
Si può inoltre fare la seguente riflessione: Lo switch 2950-24 viene venduto completo di tutte le porte sopra indicate, ad un prezzo relativamente basso; siccome le porte sono disponibili, e i cavi in rame di cat5e hanno basso costo, conviene allora cercare di fruttare al meglio le interfacce presenti aggiungendo ridondanza tramite l'utilizzo di cavi UTP in rame di categoria 5e (questo è inoltre necessario per garantire una certa robustezza alla rete, richiesta dalle specifiche).

La figura 4.5 descrive le porte presenti sullo switch 2950-24.

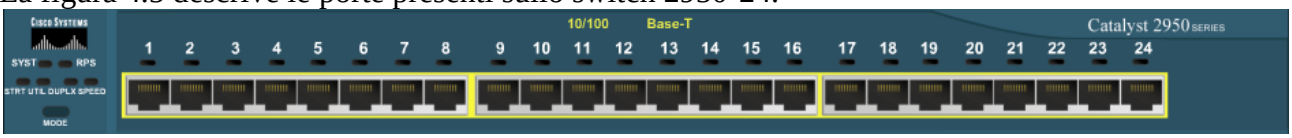


FIG 4.5 SWITCH MODELLO 2950-24

Il modello di progettazione gerarchica classico (a 3 livelli: Access - Distribution - Core) nel caso della rete per la sede di Pisa risulta eccessivo, infatti in questo caso il routing inter-VLAN (che tipicamente è affidato al livello Distribution) è effettuato dal router (che sta "sopra" il livello core, nel senso che la sua unica funzione è quella di interconnettere le sedi), si è deciso allora di comprimere la struttura a 3 livelli in una gerarchia a 2 livelli (core – access) la quale risulta più snella.

In questa ottica si considerano facenti parte del livello core:

- Il router Pisa
- Lo switch Pisa-MDF-S1 direttamente connesso al router (si veda oltre)
- Lo switch Pisa-MDF-S2 direttamente connesso al router (si veda oltre)

Si deve offrire connettività a tutte le macchine presenti nell'edificio Pisa-sud.
I cavi che provengono dalle 4 prese di rete per ogni punto di presenza (cablaggio orizzontale) vengono portati ad un patch panel (diverso per ogni stanza) residente nella Telecommunication Room dove è contenuto l'IDF-sud, dal patch panel si dirama un cavo (patch cord) per ogni punto di presenza, il quale va verso lo switch associato alla postazione (che verrà opportunamente configurato sulla porta a seconda del dominio di sicurezza al quale appartiene la macchina).

Seguendo allora la numerazione presente in figura 4.2 si prevedono i seguenti dispositivi (dove non specificato, con cavo UTP categoria 5e si intende un cavo straight-through)

- Pisa-IDF-sud-S1 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 8 (connessi alle porte fastEthernet da 0/1 a 0/6).
  - 15 cavi UTP cat5e provenienti dal patch panel per la stanza 9 (connessi alle porte fastEthernet da 0/7 a 0/21).
  - La porta fastEthernet 0/22 viene lasciata libera per futuri utilizzi.
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).
- Pisa-IDF-sud-S2 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 20 cavi UTP cat5e provenienti dal patch panel per la stanza 10 (connessi alle porte fastEthernet da 0/1 a 0/20).
  - Le porte fastEthernet da 0/21 a 0/22 vengono lasciate libere per futuri utilizzi.
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).
- Pisa-IDF-sud-S3 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 11 (connessi alle porte fastEthernet da 0/1 a 0/6).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 12 (connessi alle porte fastEthernet da 0/7 a 0/12).
  - Le porte fastEthernet da 0/13 a 0/22 vengono lasciate libere per futuri utilizzi
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).

Notare che secondo i requisiti vi deve essere una banda disponibile di 1Mbit da ogni postazione verso i server della sede di Pisa, questo è garantito per l'edificio Pisa-sud dal fatto che vi sono 6 cavi in rame che vanno verso il MDF (verso i server) ognuno capace di sostenere velocità di 1000Mbps, i quali vengono connessi ad interfacce fastEthernet, che forniscono una banda di 100Mbps ognuna.
Nell'edificio Sud vi sono punti di presenza capaci di ospitare fino a 53 postazioni, il che significa che 53 Mbps devono essere disponibili sul collegamento verso il MDF, e dunque il requisito è rispettato in quanto vi sono ben 6 collegamenti che (con le interfacce attuali) supportano ognuno 100Mbps di banda (notare che in realtà alcuni collegamenti verranno disattivati, e sarà il protocollo STP a scegliere quali).

Vi è anche il seguente requisito: “le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x”.

Permettere una tale crescita significa garantire che il cablaggio verticale verso l’MDF renda disponibile una banda di 530 Mbps, il che è garantito dal fatto che un cavo UTP di categoria 5e può funzionare collegato ad interfacce gigabit Ethernet, dunque fino a 1000Mbps.
Nel caso tale crescita fosse però effettivamente necessaria, si dovrebbero cambiare i modelli degli switch (non si inseriscono subito modelli più performanti per il semplice motivo che la vita utile di un dispositivo è bassa rispetto a quella del cablaggio, e potrebbe essere una spesa inutile installare subito dispositivi più costosi).

La ridondanza prevista nei collegamenti è stata pensata con il seguente criterio: Si fa l’ipotesi che la rete debba essere in grado di funzionare (possibilmente senza degrado delle prestazioni) anche quando si verifica un guasto nella rete, ma che il guasto debba essere riparato il prima possibile.
La ridondanza ha un costo, quindi il criterio che si segue è porre la ridondanza nei collegamenti dove risulta più efficace ed efficiente, e non aggiungere ridondanza in modo tale che la rete sia in grado di resistere a innumerevoli guasti.

Le tabelle da 4.1 a 4.3 riflettono la situazione degli switch dell’IDF-sud
Per informazioni sul significato delle colonne [Modalità] e [Snooping] si veda oltre.

Pisa-IDF-sud-S1

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 8	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/21	Collegamenti Stanza 9	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/1	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/1	100Mbps	trunk	trusted

TAB 4.1

Pisa-IDF-sud-S2

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/20	Collegamenti Stanza 10	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/2	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/2	100Mbps	trunk	trusted

TAB 4.2

Pisa-IDF-sud-S3

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 11	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 12	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/3	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/3	100Mbps	trunk	trusted

TAB 4.3

La topologia per questi switch è riportata nella figura 4.6.

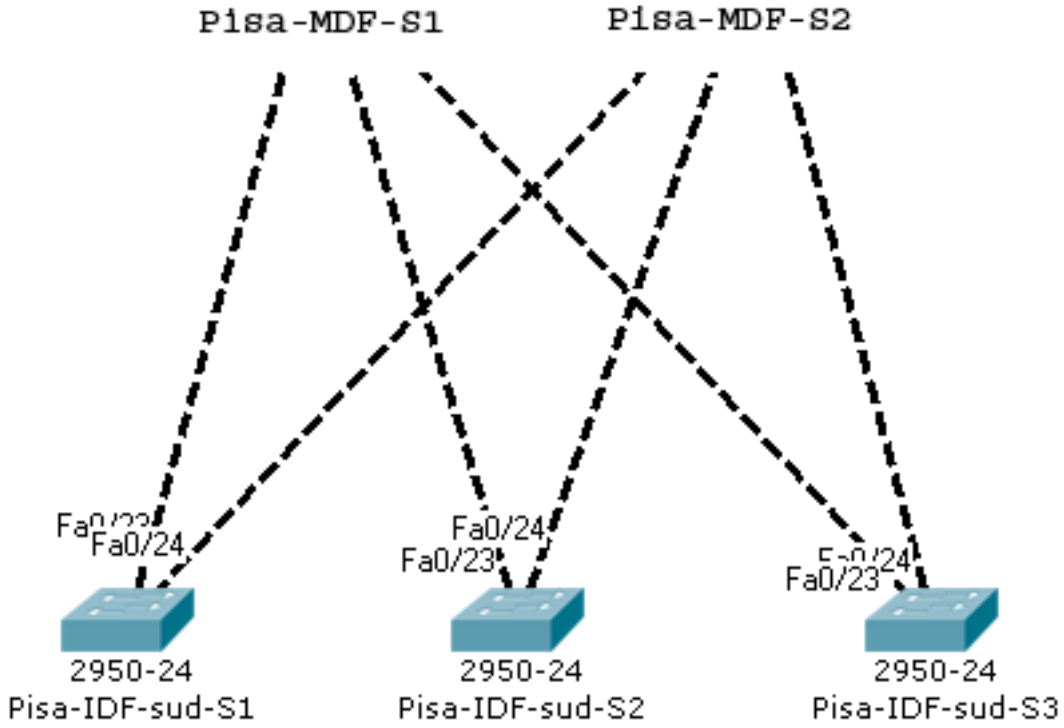


FIG 4.6 TOPOLOGIA IDF-SUD

Si deve offrire connettività a tutte le macchine presenti nell'edificio Pisa-nord.
I cavi che provengono dalle 4 prese di rete per ogni punto di presenza (cablaggio orizzontale) vengono portati ad un patch panel (diverso per ogni stanza) residente nella Telecommunication Room dove è contenuto l'IDF-nord, dal patch panel si dirama un cavo (patch cord) per ogni punto di presenza, il quale va verso lo switch associato alla postazione (che verrà opportunamente configurato sulla porta a seconda del dominio di sicurezza al quale appartiene la macchina).

Seguendo allora la numerazione presente in figura 4.3 si prevedono i seguenti dispositivi (dove non specificato, con cavo UTP categoria 5e si intende un cavo straight-through)

- Pisa-IDF-nord-S1 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 13 (connessi alle porte fastEthernet da 0/1 a 0/6).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 14 (connessi alle porte fastEthernet da 0/7 a 0/12).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 15 (connessi alle porte fastEthernet da 0/13 a 0/18).
  - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).
- Pisa-IDF-nord-S2 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 16 (connessi alle porte fastEthernet da 0/1 a 0/6).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 17 (connessi alle porte fastEthernet da 0/7 a 0/12).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 18 (connessi alle porte fastEthernet da 0/13 a 0/18).
  - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).
- Pisa-IDF-nord-S3 = Switch modello 2950-24 [livello access] al quale verranno connessi:
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 19 (connessi alle porte fastEthernet da 0/1 a 0/6).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 20 (connessi alle porte fastEthernet da 0/7 a 0/12).
  - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 21 (connessi alle porte fastEthernet da 0/13 a 0/18).
  - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
  - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).

- Pisa-IDF-nord-S4 = Switch modello 2950-24 [livello access] al quale verranno connessi:
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 22 (connessi alle porte fastEthernet da 0/1 a 0/6).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 23 (connessi alle porte fastEthernet da 0/7 a 0/12).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 24 (connessi alle porte fastEthernet da 0/13 a 0/18).
    - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
    - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
    - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).
- Pisa-IDF-nord-S5 = Switch modello 2950-24 [livello access] al quale verranno connessi:
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 25 (connessi alle porte fastEthernet da 0/1 a 0/6).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 26 (connessi alle porte fastEthernet da 0/7 a 0/12).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 27 (connessi alle porte fastEthernet da 0/13 a 0/18).
    - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
    - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23, si veda oltre).
    - 1 cavo UTP cat5e crossover che va verso lo switch Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24, si veda oltre).

Notare che secondo i requisiti vi deve essere una banda disponibile di 1Mbit da ogni postazione verso i server della sede di Pisa, questo è garantito dal fatto che vi sono 10 cavi in rame che vanno verso il MDF (verso i server) ognuno capace di sostenere velocità di 1000Mbps, i quali vengono connessi ad interfacce fastEthernet, che forniscono una banda di 100Mbps ognuna.
Nell'edificio Nord vi sono punti di presenza capaci di ospitare fino a 90 postazioni, il che significa che 90 Mbps devono essere disponibili sul collegamento verso il MDF, e dunque il requisito è rispettato in quanto vi sono ben 10 collegamenti che (con le interfacce attuali) supportano ognuno 100Mbps di banda (notare che in realtà alcuni collegamenti verranno disattivati, e sarà il protocollo STP a scegliere quali).

Vi è anche il seguente requisito: "le caratteristiche del cablaggio della rete dati dovranno essere adeguate ai requisiti di banda descritti e permettere la loro crescita fino a un fattore 10x".

Permettere una tale crescita significa garantire che il cablaggio verticale verso l'MDF renda disponibile una banda di 900 Mbps, il che è garantito dal fatto che un cavo UTP di categoria 5e può funzionare collegato ad interfacce gigabit Ethernet, dunque fino a 1000Mbps.
Nel caso tale crescita fosse però effettivamente necessaria, si dovrebbero cambiare i modelli degli switch (non si inseriscono subito modelli più performanti per il semplice motivo che la vita utile di un dispositivo è bassa rispetto a quella del cablaggio, e potrebbe essere una spesa inutile installare subito dispositivi più costosi).

Valgono ancora le riflessioni fatte durante la descrizione dell'IDF-sud per quanto riguarda la ridondanza.

Le tabelle da 4.4 a 4.8 riflettono la situazione degli switch dell'IDF-nord
Per informazioni sul significato delle colonne [Modalità] e [Snooping] si veda oltre.

Pisa-IDF-nord-S1

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 13	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 14	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 15	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/4	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/4	100Mbps	trunk	trusted

TAB 4.4

Pisa-IDF-nord-S2

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 16	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 17	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 18	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/5	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/5	100Mbps	trunk	trusted

TAB 4.5

Pisa-IDF-nord-S3

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 19	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 20	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 21	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/6	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/6	100Mbps	trunk	trusted

TAB 4.6

Pisa-IDF-nord-S4

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 22	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 23	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 24	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/7	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/7	100Mbps	trunk	trusted

TAB 4.7

Pisa-IDF-nord-S5

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 25	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 26	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 27	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/8	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/8	100Mbps	trunk	trusted

TAB 4.8

La topologia per questi switch è riportata nella figura 4.7.

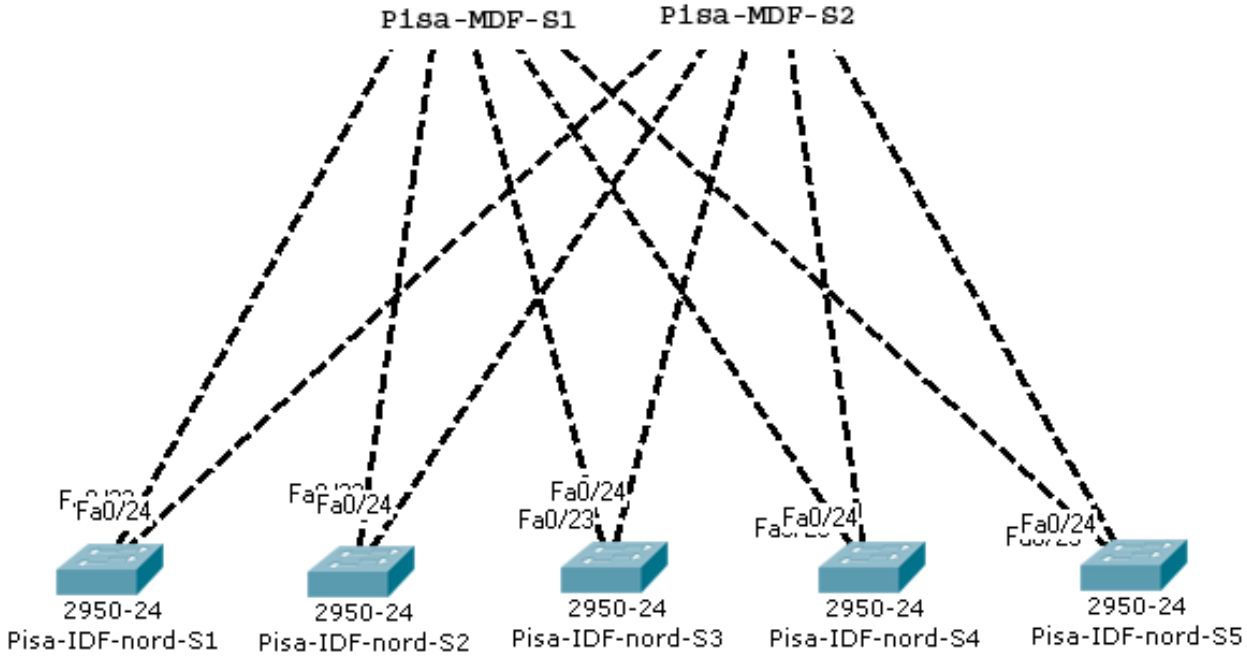


FIG 4.7 TOPOLOGIA IDF-NORD

Si deve offrire connettività a tutte le macchine presenti nell'edificio Pisa-est.
Bisogna considerare che nel MDF sono presenti anche i due switch facenti parte del livello core della rete della sede di Pisa, questi switch dovranno essere direttamente connessi ai server della sede, in modo tale da evitare che la comunicazione con questi server debba (dopo essere arrivata necessariamente fino al livello core) tornare verso il basso nella organizzazione gerarchica della rete (il che causerebbe un maggior ritardo).

Si ricorda che nelle due stanze individuate per contenere i server vi sono al massimo 48 macchine, e in questo insieme si includono anche i tre server globali (come descritto nella sezione intersede).

Si prevede allora di acquistare, per fungere da dispositivi di livello core, switch più costosi, che offrano più di 24 porte (il modello 2950-24 risulta inefficace sia per capienza che per prestazioni).
Una scelta di questo tipo porta anche ad un vantaggio economico, infatti più dispositivi con minor numero di porte costano di più rispetto ad un dispositivo con molte porte, ovviamente questa scelta diminuisce la robustezza della rete, per questo bisogna assicurarsi che gli switch scelti per lo scopo siano sufficientemente affidabili.

Notiamo che la connessione verso ogni singolo server deve essere in grado di accomodare tutto il traffico dovuto ai client di sede (in realtà andrebbe considerato anche il traffico generato da client esterni alla sede, ma questo sarà molto minore), garantendo una banda di 1Mbps per ogni postazione, e cavi in grado di accomodare 10 volte tale traffico[5].

Considerando allora che complessivamente le postazioni (non server) che devono accedere ai server sono, per la sede di Pisa, in numero pari a 181, allora conviene usare delle interfacce gigabitEthernet sullo switch e sulla scheda di rete dei server.

Postazioni:
- Nord: 6*15 = 90
- Sud: 20+15+6*3 = 53
- Est: 14+4*6 = 38 (non si considerano le stanze dedicate ai server)

Totale: 90+53+38 = 181
Banda da offrire: 181Mbps (in realtà esattamente questa non sarebbe sufficiente, perché al traffico intrasede si somma quello proveniente dall'esterno della sede di Pisa, anche se più piccolo, e l'overhead di rete, causato dai protocolli).

Un altro fatto da notare è che tale traffico non interessa solamente i link tra lo switch e i server, ma anche i link tra lo switch e il router, infatti quando un utente desidera (ad esempio) accedere ad un enterprise server è necessario che cambi VLAN, e per fare una cosa del genere è necessario che il pacchetto arrivi fino al router della sede.

Gli switch di livello core della rete della sede di Pisa sono, come già detto, in numero pari a 2.

[5] Bisognerebbe inoltre considerare che per i server di workgroup (come descritto nella sezione relativa alla rete intersede) gli utenti sono in numero più limitato, probabilmente basterebbero collegamenti e interfacce con minori prestazioni.
Essendo però che l'azienda non ha fornito un numero esatto di server dell'uno o dell'altro tipo, si prevede di considerare tutti i server come "uguali" considerando che ogni postazione deve avere 1Mbps di banda disponibile verso ogni server, sia esso globale, enterprise o di workgroup.

Si aggiunge un collegamento tra i due switch di livello core, realizzato per robustezza mediante due cavi.

La ridondanza viene aggiunta perché è fondamentale che questo collegamento non cada (se ciò accadesse le prestazioni della rete sarebbero altamente degradate).

Notare che questo collegamento tra gli switch di livello core è interessato da un traffico paragonabile a quello dei server, infatti i pacchetti prima di arrivare ai server (e per tornare ai client) devono arrivare al default gateway della loro VLAN (una delle interfacce gigabitEthernet del router), e questo può implicare di percorrere il collegamento in questione.

Per i requisiti di banda del cablaggio, è necessario prevedere che in futuro la banda richiesta potrebbe salire ad oltre 1800Mbps, questo significa che non basta un collegamento con cavo UTP cat5e in quanto si deve superare la velocità di 1Gbps.
È necessario allora ricorrere a cavi in fibra ottica per connettere

- Gli switch di livello core ai server aziendali.
- Gli switch di livello core al router di frontiera della sede.
- Gli switch di livello core tra di loro

Sempre per la durata limitata della vita utile dei dispositivi, per una prima realizzazione della rete della sede di Pisa si utilizzano interfacce con connettori appositi per la fibra ottica, ma dalla velocità di 1Gbps e non 10Gbps, in particolare si scelto di utilizzare lo standard 1000Base-SX su fibra multimode (infatti i tratti da percorrere sono veramente corti e non è dunque necessario ricorrere a standard che supportino la fibra single-mode).
I connettori ovviamente non saranno i classici RJ-45 del cavo UTP cat5e, si è scelto invece di utilizzare connettori Duplex Multimode Lucent Connector per il collegamento alle interfacce, in modo tale da operare Full Duplex anche sulla fibra ottica.

I nomi assegnati ai due switch di livello core sono Pisa-MDF-S1 e Pisa-MDF-S2.

La scelta per gli switch di livello core è ricaduta (per motivi di disponibilità di apparecchiature che soddisfino i requisiti e costo dei componenti) sulla serie 4500 della CISCO, si dovranno acquistare i seguenti moduli[6]:

- Un modulo con 24 interfacce fastEthernet su cavo in rame UTP cat5e
- Un modulo con 48 interfacce gigabitEthernet su cavo in fibra ottica

Allora le connessioni di questi due switch avranno le seguenti caratteristiche (dove non specificato, con cavo UTP categoria 5e si intende un cavo straight-through).

[6] Si veda il capitolo ‘Scelta dei dispositivi e valutazione dei costi’ per conoscere esattamente i componenti utilizzati, ed il loro prezzo.

- Pisa-MDF-S1 = Switch di livello core al quale verranno connessi:
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S1 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/1).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S2 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/2).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S3 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/3).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S1 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/4).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S2 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/5).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S3 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/6).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S4 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/7).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S5 [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/8).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-MDF-S3[7] [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/9).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-MDF-S4[8] [fastEthernet 0/23] (connesso sulla porta fastEthernet 0/10).
    - Le porte fastEthernet da 0/11 a 0/24 vengono lasciate libere per futuri utilizzi.
    - 24 cavi in fibra provenienti dal patch panel per la stanza numerata con 1 (server) in figura 4.1 (connessi alle porte gigabitEthernet da 0/1 a 0/24)
    - Le porte gigabitEthernet da 0/25 a 0/45 vengono lasciate libere per futuri utilizzi.
    - 2 cavi in fibra provenienti dallo switch Pisa-MDF-S2 (connessi alle porte gigabitEthernet da 1/46 a 1/47).
    - 1 cavo in fibra proveniente dal router Pisa (connesso sulla porta gigabitEthernet 1/48).

[7] Per maggiori informazioni sugli switch Pisa-MDF-S3 e Pisa-MDF-S4 si veda oltre.
[8] Si veda nota 5.

- Pisa-MDF-S2 = Switch di livello core al quale verranno connessi:
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S1 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/1).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S2 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/2).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-sud-S3 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/3).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S1 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/4).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S2 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/5).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S3 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/6).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S4 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/7).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-IDF-nord-S5 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/8).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-MDF-S3 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/9).
    - 1 cavo UTP cat5e crossover proveniente dallo switch Pisa-MDF-S4 [fastEthernet 0/24] (connesso sulla porta fastEthernet 0/10).
    - Le porte fastEthernet da 0/11 a 0/24 vengono lasciate libere per futuri utilizzi.
    - 24 cavi in fibra provenienti dal patch panel per la stanza numerata con 2 (server) in figura 4.1 (connessi alle porte gigabitEthernet da 1/1 a 1/24).
    - Le porte gigabitEthernet da 1/25 a 1/45 vengono lasciate libere per futuri utilizzi.
    - 2 cavi in fibra provenienti dallo switch Pisa-MDF-S1 (connessi alle porte gigabitEthernet da 1/46 a 1/47).
    - 1 cavo in fibra proveniente dal router Pisa (connesso sulla porta gigabitEthernet 1/48).

Oltre agli switch di livello core, ovviamente l'MDF conterrà anche il router denominato "Pisa", il quale ha le connessioni già descritte nella sezione a comune, sulle quali non ci dilunghiamo.

- Pisa: Router di frontiera della sede di Pisa

Nell'edificio Pisa-est vi sono ancora da collegare alla rete telematica tutte le stanze diverse da quelle dei server, a tale scopo all'interno dell'MDF si prevedono altri 2 switch (di livello access, si utilizza il solito modello 2950-24) per la connessione degli altri dispositivi terminali.

Questi due ulteriori switch avranno connessioni verso gli switch di livello core simili a quelle che hanno gli switch di livello access negli IDF appena esaminati.

- Pisa-MDF-S3 = Switch modello 2950-24 [livello access] al quale verranno connessi:
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 3 (connessi alle porte fastEthernet da 0/1 a 0/6).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 4 (connessi alle porte fastEthernet da 0/7 a 0/12).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 6 (connessi alle porte fastEthernet da 0/13 a 0/18).
    - Le porte fastEthernet da 0/19 a 0/22 vengono lasciate libere per futuri utilizzi.
    - 1 cavo UTP cat5e crossover che va verso lo switch di livello core Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23).
    - 1 cavo UTP cat5e crossover che va verso lo switch di livello core Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24).
- Pisa-MDF-S4 = Switch modello 2950-24 [livello access] al quale verranno connessi:
    - 14 cavi UTP cat5e provenienti dal patch panel per la stanza 5 (connessi alle porte fastEthernet da 0/1 a 0/14).
    - 6 cavi UTP cat5e provenienti dal patch panel per la stanza 7 (connessi alle porte fastEthernet da 0/15 a 0/20).
    - Le porte fastEthernet da 0/21 a 0/22 vengono lasciate libere per futuri utilizzi.
    - 1 cavo UTP cat5e crossover che va verso lo switch di livello core Pisa-MDF-S1 (connesso alla porta fastEthernet 0/23).
    - 1 cavo UTP cat5e crossover che va verso lo switch di livello core Pisa-MDF-S2 (connesso alla porta fastEthernet 0/24).

Cumulando il traffico delle 5 stanze non dedicate ai server, si vede che esso è originato da un totale di 38 postazioni, dunque anche in questo caso basta utilizzare interfacce fastEthernet per la connessione dei due switch Pisa-MDF-S3 e Pisa-MDF-S4 verso gli switch di livello core (a cui sono connessi i server) perché il requisito della banda disponibile verso i server venga rispettato (al solito stendendo cavi in rame di categoria 5e ci si assicura anche che, comprando nuove interfacce, la velocità possa raggiungere 1Gbps, rispettando il requisito di banda richiesta al cablaggio per una futura crescita).

Le tabelle da 4.9 a 4.12 riflettono la situazione degli switch del MDF[9].
Per informazioni sul significato delle colonne [Modalità] e [Snooping] si veda oltre.

Pisa-MDF-S1

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1	Collegamento con Pisa-IDF-sud-S1	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/2	Collegamento con Pisa-IDF-sud-S2	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/3	Collegamento con Pisa-IDF-sud-S3	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/4	Collegamento con Pisa-IDF-nord-S1	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/5	Collegamento con Pisa-IDF-nord-S2	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/6	Collegamento con Pisa-IDF-nord-S3	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/7	Collegamento con Pisa-IDF-nord-S4	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/8	Collegamento con Pisa-IDF-nord-S5	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/9	Collegamento con Pisa-MDF-S3	fastEthernet 0/23	100Mbps	trunk	untrusted
fastEthernet 0/10	Collegamento con Pisa-MDF-S4	fastEthernet 0/23	100Mbps	trunk	untrusted
gigabitEthernet 1/1-1/24	Collegamenti Stanza 1 (server)	gigabitEthernet del server	1000Mbps	access	untrusted
gigabitEthernet 1/46	Collegamento con Pisa-MDF-S2	gigabitEthernet 1/46	1000Mbps	trunk	trusted
gigabitEthernet 1/47	Collegamento con Pisa-MDF-S2	gigabitEthernet 1/47	1000Mbps	trunk	trusted
gigabitEthernet 1/48	Collegamento con Router Pisa	gigabitEthernet 2/0	1000Mbps	trunk	trusted

TAB 4.9

[9] Per conoscere in dettaglio la situazione del router Pisa fare riferimento alla sezione dedicata alla rete intersede (capitolo 'Router e Rete intersede').

Pisa-MDF-S2

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1	Collegamento con Pisa-IDF-sud-S1	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/2	Collegamento con Pisa-IDF-sud-S2	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/3	Collegamento con Pisa-IDF-sud-S3	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/4	Collegamento con Pisa-IDF-nord-S1	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/5	Collegamento con Pisa-IDF-nord-S2	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/6	Collegamento con Pisa-IDF-nord-S3	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/7	Collegamento con Pisa-IDF-nord-S4	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/8	Collegamento con Pisa-IDF-nord-S5	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/9	Collegamento con Pisa-MDF-S3	fastEthernet 0/24	100Mbps	trunk	untrusted
fastEthernet 0/10	Collegamento con Pisa-MDF-S4	fastEthernet 0/24	100Mbps	trunk	untrusted
gigabitEthernet 1/1-1/24	Collegamenti Stanza 2 (server)	gigabitEthernet del server	1000Mbps	access	untrusted
gigabitEthernet 1/46	Collegamento con Pisa-MDF-S1	gigabitEthernet 1/46	1000Mbps	trunk	trusted
gigabitEthernet 1/47	Collegamento con Pisa-MDF-S1	gigabitEthernet 1/47	1000Mbps	trunk	trusted
gigabitEthernet 1/48	Collegamento con Router Pisa	gigabitEthernet 3/0	1000Mbps	trunk	trusted

TAB 4.10

Pisa-MDF-S3

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/6	Collegamenti Stanza 3	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/7-0/12	Collegamenti Stanza 4	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/13-0/18	Collegamenti Stanza 6	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/9	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/9	100Mbps	trunk	trusted

TAB 4.11

Pisa-MDF -S4

Interfaccia/Interfacce	Descrizione	Interfaccia del vicino	Velocità	Modalità	Snooping
fastEthernet 0/1-0/14	Collegamenti Stanza 5	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/15-0/20	Collegamenti Stanza 7	fastEthernet del dispositivo terminale	100Mbps	access	untrusted
fastEthernet 0/23	Collegamento con Pisa-MDF-S1	fastEthernet 0/10	100Mbps	trunk	trusted
fastEthernet 0/24	Collegamento con Pisa-MDF-S2	fastEthernet 0/10	100Mbps	trunk	trusted

TAB 4.12

Per avere una idea della topologia risultante si faccia riferimento alla figura 4.8.

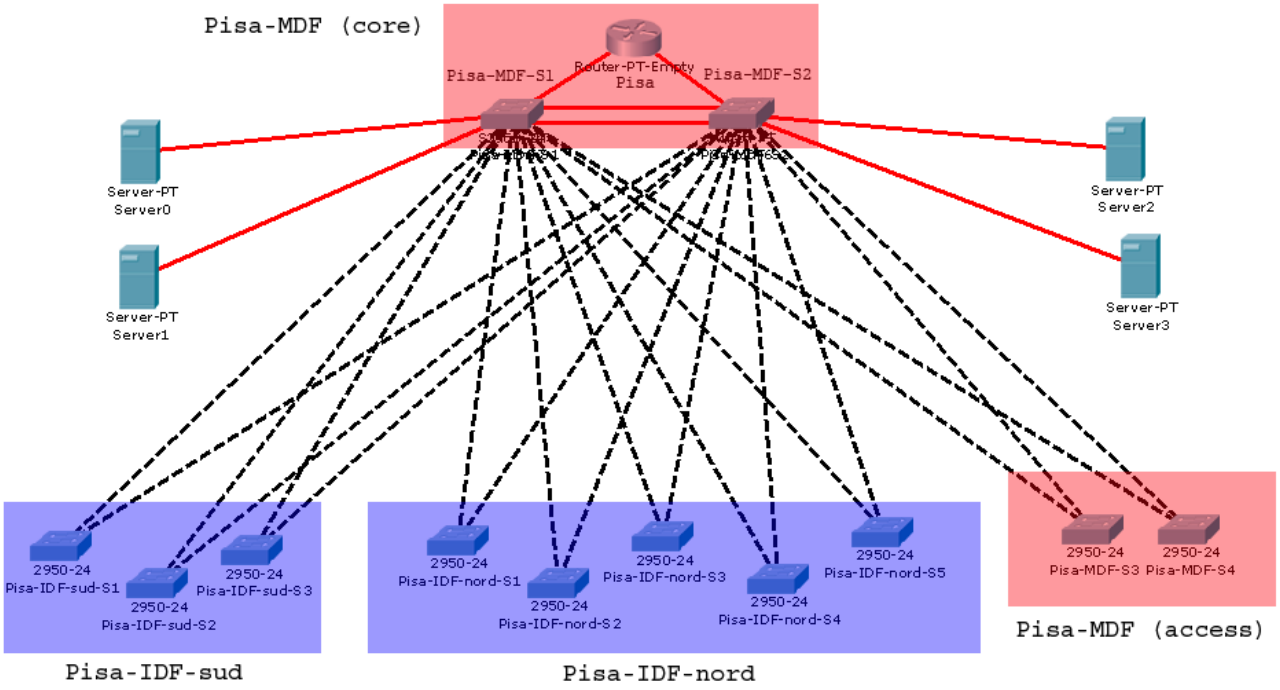


FIG 4.8 TOPOLOGIA

Ora che è noto il numero e il tipo dei collegamenti verticali, si può dare una mappa fisica con valutazioni sul numero dei cavi e sulla loro lunghezza (figura 4.9)

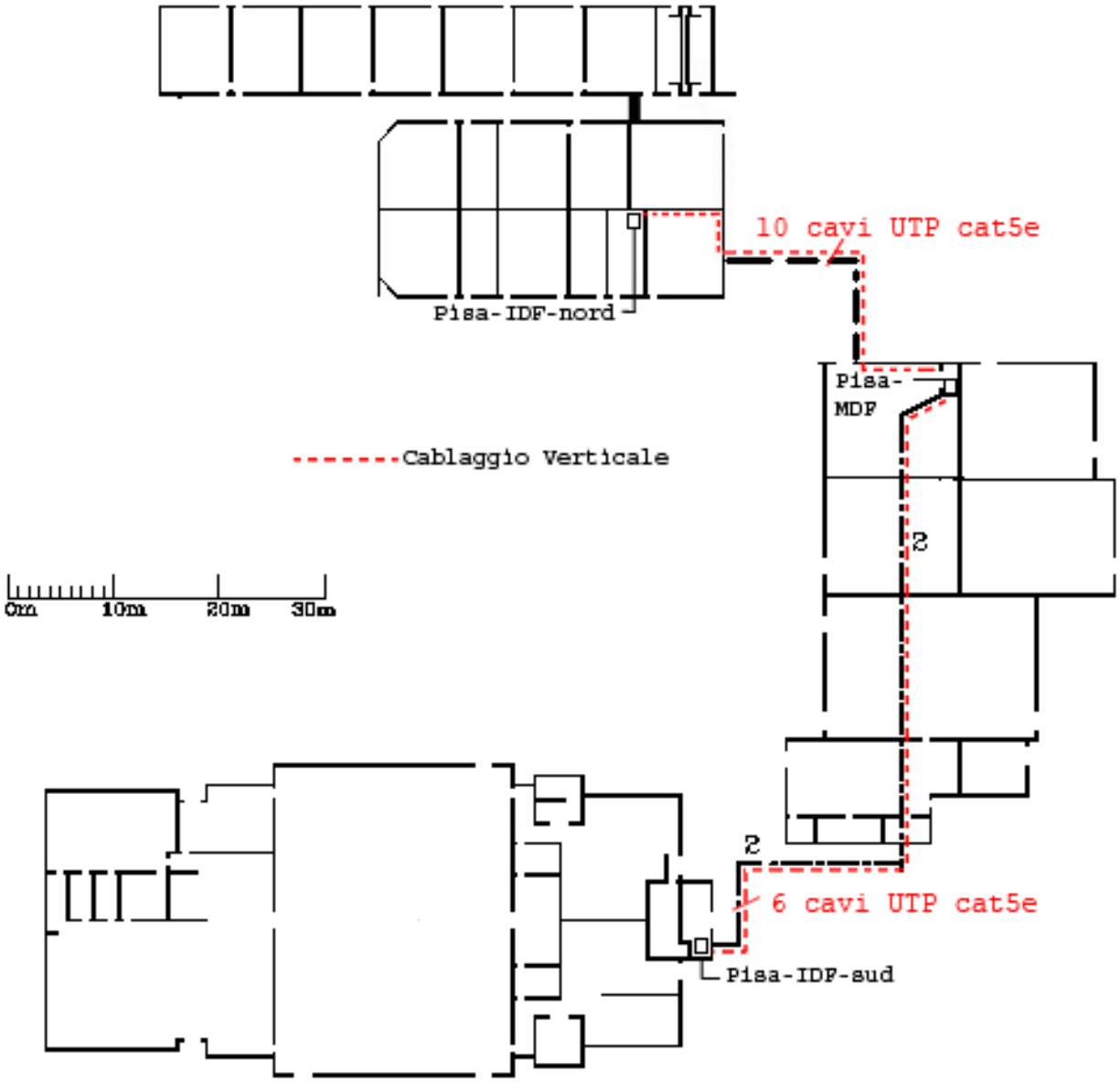


FIG 4.9 MAPPA FISICA

Nella figura è presente anche una scala per la misurazione della lunghezza dei collegamenti.

I cavi evidenziati nella figura saranno tutti di tipo crossover.

Se si ritenesse necessario, si può pensare di ricorrere (per il cablaggio verticale) a cavi schermati per difesa contro le interferenze esterne.

Nella trattazione presentata, si suppone che dei cavi non schermati (UTP) siano sufficienti per lo scopo.

Facciamo allora alcune considerazioni per mostrare che il progetto rispetta gli standard TIA-EIA 568-B e 569 (in realtà deve essere considerata una certa incertezza in quanto ci si basa sulla mappa e non su misurazioni effettive).

- I cavi per il cablaggio verticale dall'MDF all'IDF-sud sono UTP cat5e e hanno, secondo lo standard, una lunghezza massima di 90m. Misurando tramite la mappa fornita, la lunghezza viene di circa 71.2m. Considerando una incertezza di misura di 5 metri si rientra comunque negli standard.
- I cavi per il cablaggio verticale dall'MDF all'IDF-nord sono UTP cat5e e hanno, secondo lo standard, una lunghezza massima di 90m. Misurando tramite la mappa fornita, la lunghezza viene di circa 44.6m senza considerare il tratto in cui il filo scorre lungo il muro interno della stanza 27 per raggiungere il controsoffitto. Supponendo che il condotto preesistente arrivi alla altezza del pavimento, si ha che la lunghezza verticale da percorrere è circa 2.8m. Considerando una incertezza di misura di 5 metri si rientra comunque negli standard.

Anche per il cablaggio orizzontale lo standard prevede per cavi in rame di tipo UTP cat5e una lunghezza massima di 90m.

- Per quanto riguarda il cablaggio orizzontale dall'MDF alle stanze dell'edificio Pisa-est, si ha che le stanze più lontane risultano la 6 e la 7, supponendo allora di far correre i cavi (UTP cat5e) secondo il percorso indicato in figura 4.10 si ha una lunghezza complessiva di circa 47.3m Considerando una incertezza di misura di 5 metri si rientra comunque negli standard.

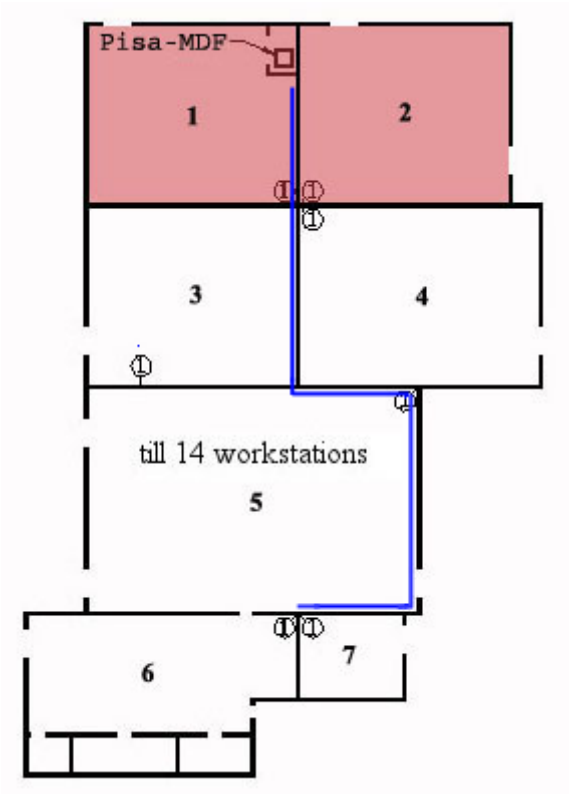


FIG 4.10

- Per quanto riguarda il cablaggio orizzontale dall'IDF-sud alle stanze dell'edificio Pisa-sud, si ha che la stanza più lontana risulta la 9, supponendo allora di far correre i cavi (UTP cat5e) secondo il percorso indicato in figura 4.11 si ha una lunghezza complessiva di circa 81.0m Considerando una incertezza di misura di 5 metri si rientra comunque negli standard.

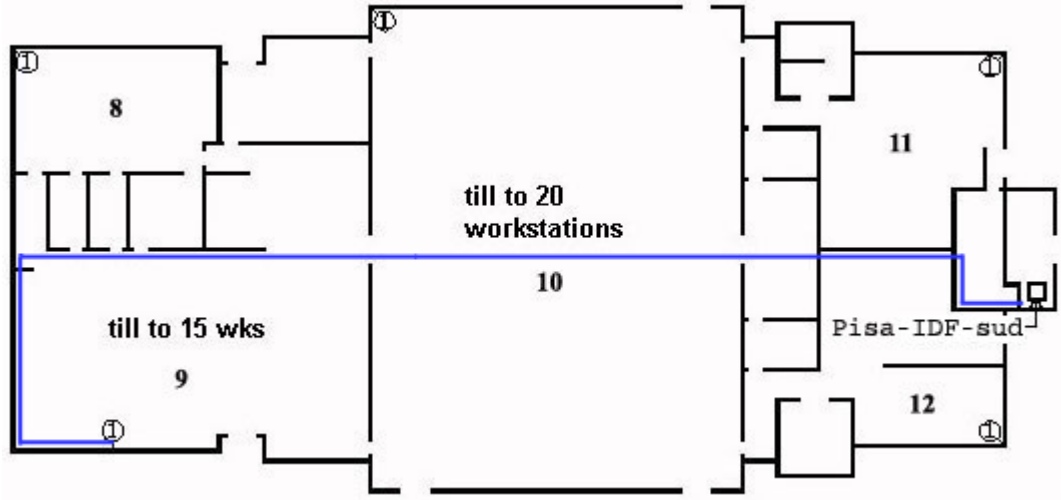


FIG 4.11

- Per quanto riguarda il cablaggio orizzontale dall'IDF-nord alle stanze dell'edificio Pisa-nord, si ha che la stanza più lontana risulta la 13, supponendo allora di far correre i cavi (UTP cat5e) secondo il percorso indicato in figura 4.12 si ha una lunghezza complessiva di circa 56.6m. Considerando una incertezza di misura di 5 metri si rientra comunque negli standard.

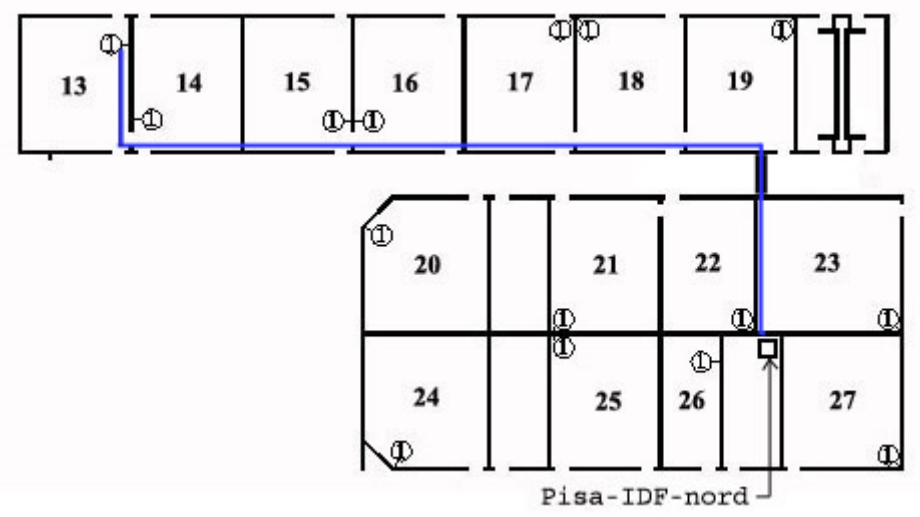


FIG 4.12

In appendice D.1 sono riportate le mappe dei tre edifici che costituiscono la sede di Pisa, dove vengono mostrati in modo completo i percorsi del cablaggio orizzontale.

Come spiegato nella sezione dedicata alla rete intersede, la divisione dei domini di sicurezza si basa sull'utilizzo della tecnologia delle VLAN. Questo implica che (siccome si usa la tecnica del frame tagging) ogni interfaccia di ogni singolo switch dovrà essere configurata in modo appropriato a seconda del dispositivo connesso[10].

Per porte configurate trunk si permette la circolazione di pacchetti di qualunque VLAN, questa scelta è stata guidata da quanto segue: in realtà potrebbe essere utile limitare le VLAN 31 e 32 ai soli switch core, evitando che pacchetti taggati con questi identificatori attraversino i link di tipo trunk verso il livello access; questa soluzione limiterebbe i domini di broadcast, evitando traffico inutile sulla rete, si può però ottenere lo stesso effetto (se non uno migliore) con la funzionalità di pruning di VTP (come verrà spiegato in seguito), si è dunque scelto di utilizzare questa seconda soluzione.
Quando si utilizza una porta in modalità trunk si utilizza l'incapsulamento definito dallo standard della IEEE, ossia l'incapsulamento 802.1Q.

Si faccia riferimento alle tabelle da 4.1 a 4.12 per sapere in che modalità operano le porte degli switch della sede di Pisa (colonna [Modalità]).

Ricordiamo che la funzione Supporto Sistemi (SS) deve essere in grado di agire su questi switch per la configurazione e la manutenzione, per questo si è deciso di inserire l'interfaccia di configurazione degli switch all'interno della VLAN riservata a questa funzione aziendale (ossia all'interno del dominio di sicurezza Supporto Sistemi).
Per fare questo bisogna creare una interfaccia di configurazione (ulteriore a quella di default appartenente alla VLAN 1, ineliminabile) su ogni switch, e associarle un indirizzo appartenente al dominio di sicurezza della funzione Supporto Sistemi di Pisa.
Questa interfaccia prende il nome di Vlan35 su ogni switch e gli indirizzi IP assegnati sono riportati nella tabella 4.13.

Locazione	Switch	Interfaccia	Indirizzo IP	Maschera di Rete
Pisa-MDF	Pisa-MDF-S1	Vlan35	172.16.227.90	255.255.255.224
	Pisa-MDF-S2	Vlan35	172.16.227.91	255.255.255.224
	Pisa-MDF-S3	Vlan35	172.16.227.88	255.255.255.224
	Pisa-MDF-S4	Vlan35	172.16.227.89	255.255.255.224
Pisa-IDF-sud	Pisa-IDF-sud-S1	Vlan35	172.16.227.85	255.255.255.224
	Pisa-IDF-sud-S2	Vlan35	172.16.227.86	255.255.255.224
	Pisa-IDF-sud-S3	Vlan35	172.16.227.87	255.255.255.224
Pisa-IDF-nord	Pisa-IDF-nord-S1	Vlan35	172.16.227.80	255.255.255.224
	Pisa-IDF-nord-S2	Vlan35	172.16.227.81	255.255.255.224
	Pisa-IDF-nord-S3	Vlan35	172.16.227.82	255.255.255.224
	Pisa-IDF-nord-S4	Vlan35	172.16.227.83	255.255.255.224
	Pisa-IDF-nord-S5	Vlan35	172.16.227.84	255.255.255.224

TAB 4.13 INTERFACCE DI CONFIGURAZIONE

Notare che questi indirizzi sono coerenti con la tabella relativa al DHCP nella sede di Pisa, riportata nella sezione intersede (sezione 1, tabella 1.12).

[10] Si faccia riferimento alle appendici D.2 e D.3 per alcuni esempi di configurazione delle interfacce degli switch.

Un requisito di progetto è il seguente: “il backbone della rete di sede deve garantire tempi di interruzione della connessione non superiori al centinaio di secondi”.

Per rispettare il requisito (oltre a prevedere la ridondanza, come si è fatto) è necessario configurare gli switch perché in caso di cambiamenti si abbia un adeguamento automatico con tempi inferiori ai 100 secondi, per fare questo si ricorre al protocollo STP (Spanning Tree Protocol).

Tipicamente, almeno in dispositivi CISCO, il protocollo STP è attivo di default; conoscendo la rete in modo approfondito è però possibile configurare il protocollo perché si comporti in modo ottimizzato.
In particolare si utilizza la versione proprietaria della CISCO PVST+, la quale supporta l’incapsulamento 802.1Q, permette di lavorare correttamente in presenza di diverse VLAN e supporta interessanti estensioni al protocollo STP, come PortFast.

Si è scelto allora di configurare come Root Bridge uno dei due switch Pisa-MDF-S1 o Pisa-MDF-S2 per ogni VLAN, e come Root Bridge secondario quello che non è stato scelto come primario.
Con questa scelta si ha un buon sfruttamento della ridondanza prevista a livello fisico, e un minor tempo di convergenza (infatti le notifiche di cambiamento topologico devono sempre arrivare al Root Bridge per essere rese effettive).

La suddivisione delle VLAN sui due Root Bridge è stata effettuata seguendo la posizione delle interfacce del router che costituiscono il default gateway per le varie VLAN (è infatti preferibile che tali interfacce vengano connesse al Root Bridge primario).

Si faccia riferimento alla seguente tabella per conoscere quale è il ruolo dei due switch nelle diverse VLAN (tabella 4.14)

VLAN	VLAN id	Root Bridge primario	Root Bridge secondario
GlobalVLAN_Pisa	31	Pisa-MDF-S1	Pisa-MDF-S2
ServerVLAN_Pisa	32	Pisa-MDF-S1	Pisa-MDF-S2
DominioDA_Pisa	33	Pisa-MDF-S1	Pisa-MDF-S2
DominioM_Pisa	34	Pisa-MDF-S1	Pisa-MDF-S2
DominioSS_Pisa	35	Pisa-MDF-S1	Pisa-MDF-S2
DominioRS1_Pisa	36	Pisa-MDF-S2	Pisa-MDF-S1
DominioRS2_Pisa	37	Pisa-MDF-S2	Pisa-MDF-S1
DominioRS3_Pisa	38	Pisa-MDF-S2	Pisa-MDF-S1

TAB 4.14 ROOT BRIDGES

Notare che il protocollo STP si basa su alcuni ritardi che descrivono il tempo di convergenza della rete, ossia il tempo di permanenza delle interfacce interessate nei vari stati verso la stabilità.

Questi ritardi vengono impostati automaticamente dagli switch considerando il diametro della rete pari a 7. Nel nostro caso invece il diametro (inteso come numero di switch che un frame deve attraversare per viaggiare tra le due macchine più distanti presenti nel dominio) è pari a 4 per tutte le VLAN con id diverso da 31 e 32.
Per le VLAN 31 e 32 invece le macchine (server) si possono collegare solamente agli switch Pisa-MDF-S1 e Pisa-MDF-S2 (come deciso precedentemente) e principalmente dialogano con il router Pisa, il diametro per queste VLAN è pari a 2.

Quanto appena detto vale nell'ipotesi che il collegamento in fibra ottica che connette Pisa-MDF-S1 e Pisa-MDF-S2 (previsto con ridondanza per robustezza) sia sempre disponibile, in caso contrario i diametri sarebbero maggiori (ma questo sarebbe il problema minore, visto che in tale situazione le prestazioni risulterebbero profondamente deteriorate).

Una volta che è noto il diametro, si possono ottimizzare le prestazioni dando la configurazione opportuna al Root Bridge.
Si veda l'appendice D.2 e D.3 per una configurazione dettagliata di due switch, notare che il diametro configurato in questo caso è esattamente quello presente, bisogna quindi essere sicuri che non sia possibile per i dipendenti collegare ulteriori dispositivi intermedi (switch), che potenzialmente potrebbero aumentare il diametro.
Notare inoltre che il diametro viene configurato anche sul Root Bridge secondario, questo per fare in modo che, se si avesse un fallimento del Root Bridge primario, rimanga l'ottimizzazione delle prestazioni.

La versione PVST+ permette di utilizzare la modalità PortFast, tale modalità consente (se attivata su porte di tipo access) di ridurre drasticamente il tempo necessario a portare la porta in stato forwarding, il che è utile al momento della connessione del dispositivo (soprattutto quando i PC devono inoltrare richieste DHCP), ma è sicuro solo su porte direttamente connesse a dispositivi terminali, nel nostro caso ai client e ai server di sede.

Si è allora deciso di utilizzare la modalità PortFast ovunque essa sia sicura (porte access connesse direttamente a server o macchine client).

Con la ottimizzazione del protocollo sul diametro della rete, e con l'utilizzo della modalità PortFast il tempo di interruzione della connessione (se fisicamente possibile, grazie alla ridondanza) è limitato e sicuramente al di sotto del centinaio di secondi (infatti in realtà anche con i timer standard il protocollo STP risulta soddisfare il requisito, perché il tempo complessivo da quando ci si accorge di una variazione topologica a quando le porte giuste passano in stato forwarding sarebbe dell'ordine dei 50 secondi).

È già stato descritto, nella sezione dedicata alla rete intersede (sezione 1), come si procede ad implementare la dinamicità della rete, ossia tramite il protocollo DHCP.
Si faccia riferimento a tale sezione per maggiori approfondimenti al riguardo.

Un'altra funzionalità che si è scelto di implementare sugli switch della sede di Pisa è quella dello snooping.
Fondamentalmente lo snooping è un metodo di difesa verso gli attacchi di spoofing delle risposte DHCP, con cui un utente malintenzionato fornisce informazioni potenzialmente dannose ad un client DHCP, fingendo di essere un server DHCP aziendale. L'intruso potrebbe anche generare molte richieste DHCP verso il router Pisa, il quale si troverebbe a rispondere nel caso venissero generati indirizzi MAC sempre diversi, esaurendo la disponibilità di indirizzi; anche per questo lo snooping fornisce un metodo di protezione[11].

Si faccia riferimento alle tabelle da 4.1 a 4.12 per sapere come vengono configurate le porte dei dispositivi (colonna [Snooping]).

[11] Notare che anche la Port Security (descritta in seguito) fornisce una protezione contro questo secondo tipo di azione di disturbo.

Lo snooping in realtà può venire configurato anche solo per alcune VLAN, tuttavia nel nostro caso questa opzione non ci interessa.
Le porte configurate come untrusted andranno down automaticamente se viene ricevuta un risposta DHCP; viene inoltre costruita una tabella di binding DHCP su tali porte, che viene utilizzata per filtrare il traffico DHCP potenzialmente dannoso.

Un'altra funzionalità che si è scelto di implementare per questioni di sicurezza è la cosiddetta "Port Security", in particolare si è ritenuto che una configurazione degli switch tale che i dispositivi riconoscano i giusti indirizzi MAC (e solo quelli) fosse una ottima protezione per la rete, pertanto gli obiettivi che si vogliono raggiungere sono i seguenti:

- Permettere che solo una macchina venga collegata agli switch di livello access, sulle interfacce configurate in modalità access. La cosa più sicura possibile sarebbe utilizzare una configurazione statica degli indirizzi MAC sicuri, tuttavia questo risulta poco efficace, perché in tal modo si avrebbe un lavoro molto oneroso gravante sulla funzione SS della WWAS, si è deciso allora di configurare indirizzi MAC sicuri appresi dinamicamente dagli switch e salvati nella Running-Configuration (Sticky) e poi nella Startup-Configuration (grazie funzione aziendale SS) in modo tale che solo quei calcolatori siano ammessi nella rete.
- Fare in modo che se viene riconosciuto un indirizzo MAC diverso l'accesso alla rete venga precluso e rimanga una traccia dell'intrusione nello switch[12].

Utilizzare un apprendimento dinamico degli indirizzi MAC sicuri senza che vengano salvati nella Running-Configuration e nella Startup-Configuration risulta inutile, perché un dipendente potrebbe semplicemente collegare qualsiasi cosa alla rete nel momento in cui si ha un restart generale.
Utilizzando un apprendimento Sticky invece si ha il vantaggio che si può (dopo il primo collaudo della rete) salvare nella Startup-Configuration gli indirizzi MAC riconosciuti come sicuri, e da quel momento in poi solo tali indirizzi MAC saranno considerati sicuri.
Notiamo che se fossero necessari cambiamenti delle macchine, come nuove schede di rete, allora dovrebbe essere la funzione SS della WWAS ad occuparsi di azzerare la lista dei MAC-address sicuri presenti nella Running-Configuration, e salvare le nuove informazioni ottenute dopo un riavvio dello switch interessato, copiandole nella Startup-Configuration.

I comandi che l'addetto a questo tipo di operazione dovrebbe dare sono i seguenti:

```
[accesso]
enable
[digitare la password]
configure terminal
[entrare modalità di configurazione della interfaccia desiderata]
no switchport port-security mac-address sticky
end
copy running-config startup-config
reload
[accesso]
enable
[digitare la password]
configure terminal
[entrare modalità di configurazione della interfaccia desiderata]
switchport port-security mac-address sticky
end
[attendere l'apprendimento]
copy running-config startup-config
exit
```

[12] (con riferimento alla nota 11) Ecco che allora si capisce che se un utente malintenzionato cercasse di sovraccaricare il router di richieste DHCP modificando il proprio indirizzo MAC si vedrebbe precluso l'accesso alla rete.

Eventualmente, per una istruzione minimale del personale della funzione SS della WWAS, alcuni esperti della nostra azienda potranno fornire supporto tecnico per un periodo di tempo precedentemente accordato.

L'azione scelta in conseguenza della violazione della sicurezza è di porre l'interfaccia in stato down, in tal modo si impedisce a colui che ha causato la violazione di connettersi alla rete, e si ha anche l'effetto che l'accaduto viene scritto in un file di log salvato nello switch.

Notare che con questo tipo di configurazione della sicurezza sugli indirizzi MAC, si ha anche l'effetto che, nel caso in cui un dipendente della WWAS collegasse uno switch o un hub ad uno switch aziendale di livello access allo scopo di fornire connettività ad ulteriori dispositivi (aumentando il diametro della rete), la porta interessata dello switch aziendale verrebbe automaticamente posta nello stato down, preservando la sicurezza aziendale e le funzionalità del protocollo STP.

La funzione aziendale SS, per connettersi agli switch allo scopo di configurare le VLAN o la Port Security, deve aprire una sessione telnet verso l'indirizzo IP dell'interfaccia di configurazione dello switch (per la sede di Pisa tali indirizzi sono stati già presentati in tabella 4.13, fare riferimento alle sezioni 2 e 3 per sapere gli indirizzi per i dispositivi di Roma e Padova).

Un'altra funzionalità offerta dai dispositivi CISCO è il protocollo VTP (Virtual Trunking Protocol) la sua utilità si presenta sotto diversi punti di vista:

- Permette di configurare le VLAN presenti nella sede di Pisa esclusivamente sugli switch che assumono (nel dominio VTP specificato) il ruolo di server, i client vengono automaticamente tenuti aggiornati dai server.
  - Questa caratteristica incrementa ulteriormente la flessibilità della rete.
- Permette di attivare la funzionalità di pruning, che risulta particolarmente appetibile per il progetto in questione: il VTP pruning è in grado di prevenire il flooding di frame in broadcast quando non necessario.
  - Questo riduce moltissimo il traffico overhead sulla rete, ottimizzando le prestazioni.

La versione del protocollo VTP che si è deciso di utilizzare è la 1.

Il ruolo di server nel dominio (unico) della sede di Pisa viene dato ai 2 switch

- Pisa-MDF-S1
- Pisa-MDF-S2

In quanto dovrebbero essere più affidabili degli switch livello access.

Si utilizzano due server per far si che il VTP continui a funzionare anche se uno dei due dovesse fallire. Se in un dominio VTP non vi sono più server infatti si ha l'effetto che non si possono più modificare le VLAN presenti in quanto i client non possono aggiungere/rimuovere/modificare informazioni al riguardo, inoltre essendo che i client non memorizzano le VLAN in NVRAM si ha che la configurazione andrebbe persa.
Quindi il motivo fondamentale che spinge ad usare due server è quello della ridondanza.

Si è deciso di configurare il dominio della WWAS di Pisa, chiamato "wwas", in modalità sicura, questo fa si che gli switch interagiscano tra loro con una password.
La password scelta per lo scopo è la seguente:

```
cisco
```

Per configurare il pruning VTP (che è il motivo fondamentale per cui si è deciso di adottare tale protocollo) è sufficiente utilizzare l'appropriato comando su un solo switch del dominio configurato come server.
Lo switch scelto per lo scopo è Pisa-MDF-S1 (si veda l'appendice D.2).

Alcuni criteri da seguire durante l'installazione e configurazione della nuova rete della sede di Pisa sono i seguenti.

- Conviene sempre portare down le interfacce degli switch che risultano inutilizzate. Quando poi sarà necessario effettuare la connessione sarà la funzione SS a dare il comando per portare up l'interfaccia. Questo serve da protezione contro malintenzionati che si connettono fisicamente agli switch senza autorizzazione.
- Dopo la prima installazione e il testing della rete di Pisa, si deve disabilitare su tutti gli switch e sul router di Pisa il protocollo CDP, questo incrementa la performance della rete di sede in quanto riduce il traffico "overhead", inoltre così facendo si evita di mandare ai dipendenti della WWAS informazioni sulla rete aziendale. Disabilitandolo si ha anche l'effetto che si preclude la possibilità che i collegamenti WAN di backup possano essere utilizzati senza necessità.
- Dato il fatto che la rete è stata progettata per intero, risulta inutile effettuare la negoziazione della modalità delle porte trunk tramite il protocollo DTP – Dynamic Trunking Protocol, il quale potrebbe (nel caso non fossero tutti dispositivi CISCO) confondere i dispositivi collegati alle porte, ed inoltre genera traffico inutile sulla rete. La configurazione della modalità sulla porta avviene dunque staticamente, e si è scelto di disabilitare il dialogo DTP tra gli switch su tutte le porte destinate ad operare in modalità trunk.

Tutti gli switch e il router Pisa sono stati configurati perché all'accesso mostrino un messaggio del seguente tipo:

```
[Switch|Router] WWAS <Nome switch o router>: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile
```

Questo assicura che, se qualcuno danneggia la rete in qualunque modo e si riesce a capire di chi è la responsabilità, sia possibile perseguire per legge coloro che hanno causato il danno.

La password da utilizzare per l'accesso tramite telnet (o anche tramite console) è:

```
class
```

La password da inserire per passare dalla modalità utente alla modalità privilegiata è:

```
cisco
```

Fare riferimento alle appendici

- D.2 per osservare come dovrebbe venir configurato lo switch Pisa-MDF-S1
- D.3 per osservare come dovrebbe venir configurato lo switch Pisa-IDF-nord-S1

Allegata al documento vi è una simulazione della rete della sede di Pisa. Date le potenzialità dello strumento utilizzato per la simulazione (Packet Tracer 4.11) e visto che la simulazione deve avvicinarsi all'aspetto funzionale della rete più che agli aspetti di ottimizzazione, vi sono alcune considerazioni da fare.

- Non vi sono switch nel simulatore idonei a rappresentare gli switch del livello core della rete della sede di Pisa, quindi (prescindendo dai cavi effettivamente utilizzati e dalle interfacce effettivamente presenti) si utilizzano solamente cavi UTP cat5e e interfacce fastEthernet, si suppone inoltre che tutti gli switch siano modelli CISCO 2950-24.
- Non è possibile sfruttare funzionalità avanzate del protocollo proprietario CISCO PVST+, quindi non sono presenti le funzionalità della modalità PortFast e non è possibile regolare il diametro della rete.
- Lo snooping non è supportato da Packet Tracer 4.11.
- Vi è solo un tipo possibile di encapsulation su link di tipo trunk, e questa è la dot1q ossia 802.1Q, che peraltro è quella che si è deciso di utilizzare.
- Le porte che collegano gli switch Pisa-MDF-S1 e Pisa-MDF-S2 non saranno
  - gigabitEthernet 1/46
  - gigabitEthernet 1/47

  ma
  - fastEthernet 0/22
  - fastEthernet 0/23

  e la porta che collega gli switch Pisa-MDF-S1 e Pisa-MDF-S2 al router non sarà
  - gigabitEthernet 1/48

  ma
  - fastEthernet 0/24
- Le porte che collegano il router Pisa agli switch Pisa-MDF-S1 e Pisa-MDF-S2 non saranno
  - gigabitEthernet 2/0
  - gigabitEthernet 3/0

  ma
  - fastEthernet 2/0
  - fastEthernet 3/0
- I server connessi in ogni stanza si riducono, per la simulazione con Packet Tracer, ad un massimo di 6.
- I server avranno interfacce di rete fastEthernet, non su fibra ottica e si collegheranno agli switch core tramite cavo in rame UTP cat5e, la connessione con gli switch avverrà sulle porte fastEthernet da 0/11 a 0/16.
- Ovviamente l'appartenenza delle macchine ai diversi domini è soltanto ipotetica.
- Le interfacce inutilizzate non sono state portate down come specificato in precedenza.
- I collegamenti WAN di backup verso le altre sedi non sono presenti.
- La topologia delle reti nelle altre sedi (Padova e Roma) è del tutto ipotetica, come pure la configurazione dei dispositivi al loro interno. Si faccia riferimento alle sezioni 2 e 3 per maggiori informazioni al riguardo.
- Il protocollo VTP in Packet Tracer è parzialmente implementato, pertanto sono stati configurati i dispositivi client e server, ma non è stato possibile configurare il pruning.
- Il Protocollo CDP non è stato disabilitato: visto che è solo una simulazione, può essere di aiuto nel validare la configurazione.
- La descrizione data alle interfacce serve solo per capire la simulazione, non è la descrizione che si darebbe alle interfacce in fase di prima configurazione della rete.
- Come descritto nelle specifiche, la simulazione include due soli gruppi di lavoro.

Il numero di macchine però effettivamente presenti nei gruppi è del tutto arbitrario ed è stato scelto in modo da poter valutare la funzionalità della rete, rimanendo nelle possibilità dello strumento utilizzato (Packet Tracer).

- Per una simulazione più accurata della situazione della rete intersede si rimanda al file di Packet Tracer apposito, come descritto nella sezione 1.

Il file della simulazione è: "`Simulazione_Pisa.pkt`"

In figura 4.13 vi è una immagine della rete simulata, presa direttamente dal programma Packet Tracer 4.11.

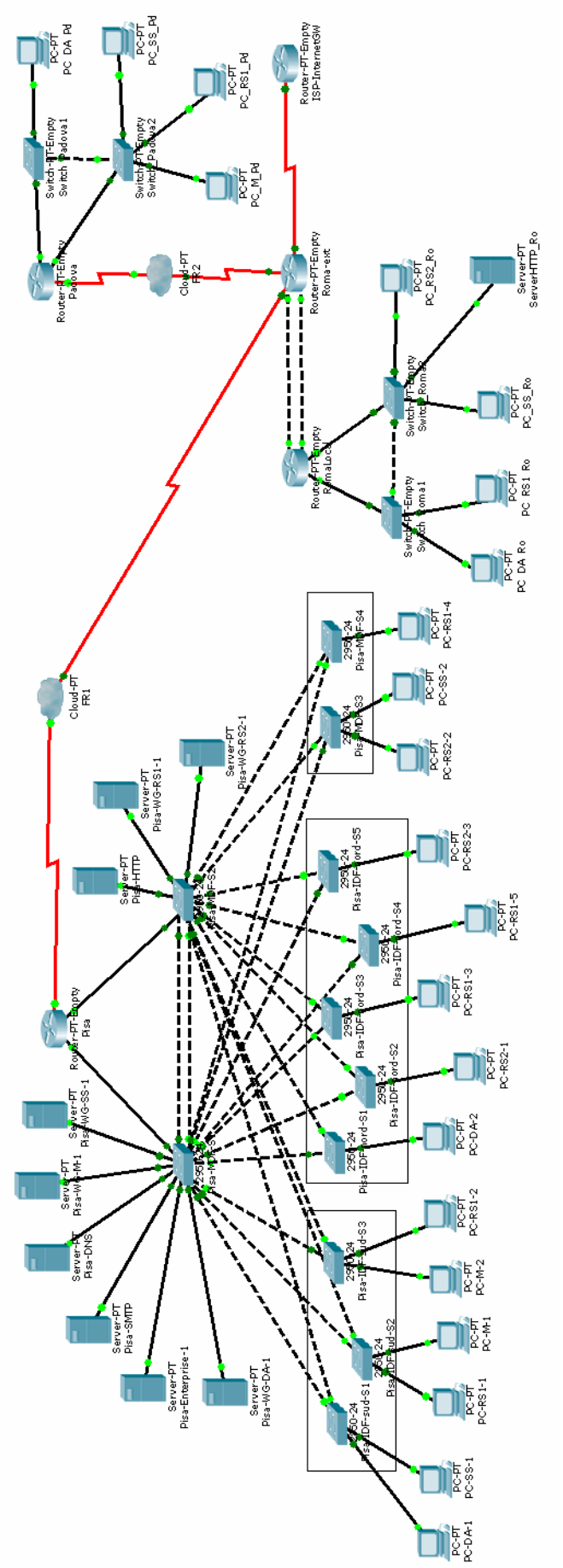


FIG 4.13 SIMULAZIONE SEDE DI PISA

1. Router

I router di Pisa e Padova, come già visto in sezione 1, devono possedere:

- 2 interfacce seriali per la connessione alla rete WAN.
- 2 interfacce gigabitEthernet su fibra ottica per le reti di sede.

Il router più economico presente in listino che supporti i moduli richiesti per velocità di trasmissione e numero è il CISCO 3745 della serie 3700. Si ricorda che l'acquisto di un Network Module Gigabit Ethernet comporta anche quello di un GBIC adeguato alla tecnologia che si vuole implementare (in questo caso la 1000BASE-SX).

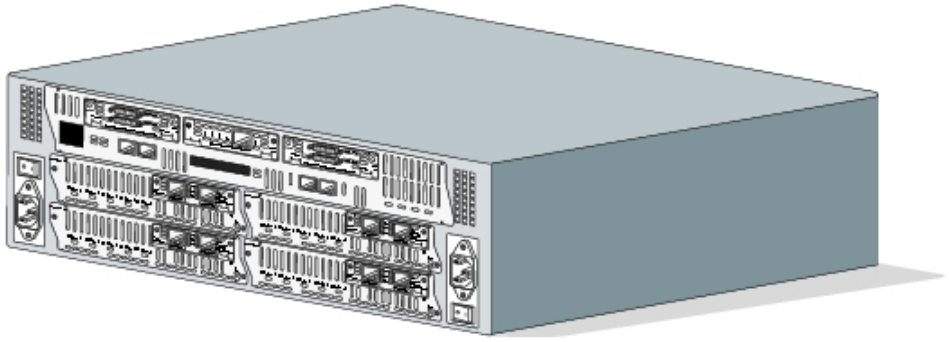


FIG 5.1 – Il Router CISCO 3745 e le interfacce che mette a disposizione

In particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x CISCO3745 – € 15678.00
- ✓ 2 x Porta seriale WIC-1T – 2 x € 523.00 = € 1046.00
- ✓ 2 x Porta gigabitEthernet NM-1GE – 2 x € 5879.00 = € 11768.00
- ✓ 2 x 1000BASE-SX GBIC WS-G5484 – 2 x € 653.00 = € 1306.00

TOTALE = € 29798.00

Dunque per i due router di Pisa e Padova si arriva ad un costo complessivo di € 59596.00.

Il router RomaLocal, come già visto nel capitolo 'Router e Rete intersede', deve possedere:

- 1 interfaccia seriale per la connessione alla rete WAN
- 2 interfacce fastEthernet per la connessione con il router Roma-ext
- 2 interfacce gigabitEthernet su fibra ottica per le reti di sede

La scelta è ancora una volta ricaduta sulla serie 3700 della CISCO, in particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x Chassis CISCO3745 – € 15678.00
- ✓ 1 x Porta seriale WIC-1T – € 523.00
- ✓ 2 x Porta gigabitEthernet NM-1GE – 2 x € 5879.00 = € 11768.00

[13] Notare che gli identificatori associati dall'IOS alle porte descritte in seguito potrebbero differire da quelli che sono stati utilizzati nella descrizione della rete e nelle configurazioni esemplificative.

- ✓ 2 x 1000BASE-SX GBIC WS-G5484 – 2 x € 653.00 = € 1306.00

TOTALE = € 29275.00

Il router Roma-ext, come già visto in sezione 1, deve possedere:

- 3 interfacce seriali per la connessione alla rete WAN ed all'ISP
- 2 interfacce fastEthernet per la connessione con il router RomaLocal

La scelta è ancora una volta ricaduta sulla serie 2600XM della CISCO, in particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x Chassis CISCO2621XM – € 4044.00
- ✓ 1 x Porta seriale WIC-1T – € 523.00
- ✓ 1 x Porta seriale WIC-2T – € 915.00

TOTALE = € 5482.00

Possiamo allora calcolare il costo complessivo dei router:

TOTALE = € 94353.00

Gli switch di livello core di Roma, come già visto in sezione 2, devono possedere:

- 24 interfacce fastEthernet per la connessione agli switch di livello access;
- 48 interfacce gigabitEthernet su fibra ottica per la connessione ai server, al router e tra gli switch di livello core.

La scelta è quindi ricaduta sulla serie Catalyst 4500 della CISCO. Si ricorda che l'acquisto di una line card WS-X4448-GB-SFP comporta anche quello di un numero, pari a quello delle porte impiegate, di moduli SFP per la tecnologia che si vuole implementare (in questo caso la 1000BASE-SX).
In particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x Chassis WS-C4503 – € 1300.00
- ✓ 1 x Alimentatore PWR-C45-1400AC – € 1953.00
- ✓ 1 x Modulo fastEthernet WS-X4124-RJ45 – € 3260.00
- ✓ 1 x Modulo gigabitEthernet WS-X4448-GB-SFP – € 21551.00
- ✓ 27 x Transceiver 1000BASE-SX SFP – 27 x € 653.00 = € 17631.00

TOTALE = € 45695.00

Dunque per i due switch di livello core della sede di Roma si arriva ad un costo complessivo di € 91390.00.

Gli switch di livello access della sede di Roma, come già visto in sezione 2, devono possedere:

- 24 interfacce fastEthernet per la connessione ai dispositivi terminali, agli switch di livello core e tra gli switch di livello access.

La scelta è ricaduta sulla serie Catalyst 2950 della CISCO, in particolare si mette in preventivo l'acquisto del seguente modello:

- ✓ 1 x Switch WS-C2950-24 – € 1260.00

Dunque per i tredici switch di livello access della sede di Roma si arriva ad un costo complessivo di € 16380.00.

Possiamo allora calcolare il costo complessivo degli switch per la sede di Roma:

TOTALE = € 107770.00

Gli switch di livello distribution/access di Padova, come già visto in sezione 3, devono possedere:

- 48 interfacce gigabitEthernet su fibra ottica per la connessione ai server, al router, ai 10 switch di livello access e tra MDF1 e MDF2.

La scelta è quindi ricaduta sulla serie Catalyst 4500 della CISCO. Si ricorda che l'acquisto di una line card WS-X4448-GB-SFP comporta anche quello di un numero, pari a quello delle porte impiegate, di moduli SFP per la tecnologia che si vuole implementare (in questo caso la 1000BASE-SX).
In particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x Chassis WS-C4503 – € 1300.00
- ✓ 1 x Alimentatore PWR-C45-1400AC – € 1953.00
- ✓ 1 x Modulo gigabitEthernet WS-X4448-GB-SFP – € 21551.00
- ✓ 37 x Transceiver 1000BASE-SX SFP – 37 x € 653.00 = € 24161.00

TOTALE = € 48965.00

Dunque per i due switch MDF1 e MDF2 della sede di Padova si arriva ad un costo complessivo di € 97930.00.

Gli switch di livello access della sede di Padova, come già visto in sezione 3, devono possedere:

- 24 interfacce fastEthernet per la connessione ai dispositivi terminali;
- 2 interfacce gigabitEthernet per la connessione agli switch di livello superiore.

La scelta è ricaduta sulla serie Catalyst 2950 della CISCO, in particolare si mette in preventivo l'acquisto del seguente modello:

- ✓ 1 x Switch WS-C2950SX-24 – € 2273.00

Dunque per i dieci switch di livello access della sede di Pisa si arriva ad un costo complessivo di € 22730.00.

Possiamo allora calcolare il costo complessivo degli switch per la sede di Pisa:

TOTALE = € 120660.00

Presentiamo i costi delle tre alternative (come anticipato nella sezione 3) relative alla scelta dei dispositivi di livello access all'interno dell'armadio principale:

1) *gigabit Ethernet su fibra (soluzione adottata):*
   - ✓ *4 x Switch WS-C2950SX-24* – *4 x € 2273.00 = € 9092.00*
   - ✓ *8 x Transceiver 1000BASE-SX SFP* – *8 x € 653.00 = € 5224.00*

   TOTALE = € 14316.00

2) gigabit Ethernet su rame:
   - ✓ 2 x Mod. gigabitEthernet WS-X4524-GB-RJ45V – 2 x € 5873.00 = €11746
   - ✓ 4 x Switch WS-C2950T-24 – 4 x € 1640.00 = € 6560.00

   TOTALE = € 18306.00

3) fastEthernet:
   - ✓ 2 x Modulo fastEthernet WS-X4124-RJ45 – 2 x € 3260.00 = €6520.00
   - ✓ 4 x Switch WS-C2950-24 – 4 x € 1260.00 = € 5040.00

   TOTALE = € 11560.00

Gli switch di livello core di Pisa, come già visto in sezione 4, devono possedere:

- 24 interfacce fastEthernet per la connessione agli switch di livello access;
- 48 interfacce gigabitEthernet su fibra ottica per la connessione ai server, al router e tra gli switch di livello core.

La scelta è quindi ricaduta sulla serie Catalyst 4500 della CISCO. Si ricorda che l'acquisto di una line card WS-X4448-GB-SFP comporta anche quello di un numero, pari a quello delle porte impiegate, di moduli SFP per la tecnologia che si vuole implementare (in questo caso la 1000BASE-SX).
In particolare si mette in preventivo l'acquisto dei seguenti componenti:

- ✓ 1 x Chassis WS-C4503 – € 1300.00
- ✓ 1 x Alimentatore PWR-C45-1400AC – € 1953.00
- ✓ 1 x Modulo fastEthernet WS-X4124-RJ45 – € 3260.00
- ✓ 1 x Modulo gigabitEthernet WS-X4448-GB-SFP – € 21551.00
- ✓ 27 x Transceiver 1000BASE-SX SFP – 27 x € 653.00 = € 17631.00

TOTALE = € 45695.00

Dunque per i due switch di livello core della sede di Pisa si arriva ad un costo complessivo di € 91390.00.

Gli switch di livello access della sede di Pisa, come già visto in sezione 4, devono possedere:

- 24 interfacce fastEthernet per la connessione ai dispositivi terminali ed agli switch di livello core.

La scelta è ricaduta sulla serie Catalyst 2950 della CISCO, in particolare si mette in preventivo l'acquisto del seguente modello:

- ✓ 1 x Switch WS-C2950-24 – € 1260.00

Dunque per i dieci switch di livello access della sede di Pisa si arriva ad un costo complessivo di € 12600.00.

Possiamo allora calcolare il costo complessivo degli switch per la sede di Pisa:

TOTALE = € 103990.00

A.1 Router RomaLocal

```
!
service password-encryption
!
hostname RomaLocal
!
!
enable secret cisco
!
!
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial0/0.112 point-to-point
 description To Pisa (Backup)
 bandwidth 256
 ip address 172.16.240.14 255.255.255.252
 frame-relay interface-dlci 112
!
interface Serial0/0.116 point-to-point
 description To Padova (Backup)
 bandwidth 256
 ip address 172.16.240.18 255.255.255.252
 frame-relay interface-dlci 116
!
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet1/0.11
 description GlobalVLAN_Roma
 encapsulation dot1Q 11
 ip address 172.16.195.177 255.255.255.248
 ip access-group GlobalVLAN_Roma in
!
interface GigabitEthernet1/0.12
 description ServerVLAN_Roma
 encapsulation dot1Q 12
 ip address 172.16.195.1 255.255.255.192
 ip access-group ServerVLAN_Roma in
!
interface GigabitEthernet1/0.13
 description DominioDA_Roma
 encapsulation dot1Q 13
 ip address 172.16.195.65 255.255.255.192
 ip access-group DominioDA_Roma in
!
interface GigabitEthernet1/0.14
 description DominioM_Roma
 encapsulation dot1Q 14
 ip address 172.16.195.161 255.255.255.240
 ip access-group DominioM_Roma in
!
interface GigabitEthernet1/0.15
 description DominioSS_Roma
 encapsulation dot1Q 15
```

```
 ip address 172.16.195.129 255.255.255.224
 ip access-group DominioSS_Roma in
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet2/0.16
 description DominioRS1_Roma
 encapsulation dot1Q 16
 ip address 172.16.192.1 255.255.255.0
 ip access-group DominioRS1_Roma in
!
interface GigabitEthernet2/0.17
 description DominioRS2_Roma
 encapsulation dot1Q 17
 ip address 172.16.193.1 255.255.255.0
 ip access-group DominioRS2_Roma in
!
interface GigabitEthernet2/0.18
 description DominioRS3_Roma
 encapsulation dot1Q 18
 ip address 172.16.194.1 255.255.255.0
 ip access-group DominioRS3_Roma in
!
interface FastEthernet3/0
 description To Roma-ext (A)
 ip address 172.16.240.21 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet4/0
 description To Roma-ext (B)
 ip address 172.16.240.25 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.16.240.12 0.0.0.3 area 0
 network 172.16.240.16 0.0.0.3 area 0
 network 172.16.240.20 0.0.0.3 area 0
 network 172.16.240.24 0.0.0.3 area 0
 network 172.16.192.0 0.0.15.255 area 0
!
!
ip access-list extended DominioDA_Roma
 permit ip 172.16.195.64 0.0.0.63 172.16.211.96 0.0.0.31
 permit ip 172.16.195.64 0.0.0.63 172.16.227.96 0.0.0.15
 permit tcp 172.16.195.64 0.0.0.63 172.16.195.0 0.0.0.63
 permit udp 172.16.195.64 0.0.0.63 host 172.16.195.181 eq 53
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.195.182 eq 80
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.195.182 eq 443
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.227.132 eq 25
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.211.149 eq 25
 permit tcp 172.16.195.64 0.0.0.63 172.16.227.0 0.0.0.63
 permit tcp 172.16.195.64 0.0.0.63 172.16.211.0 0.0.0.63
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.227.134 eq 80
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.227.134 eq 443
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.211.150 eq 80
 permit tcp 172.16.195.64 0.0.0.63 host 172.16.211.150 eq 443
 permit udp 172.16.195.64 0.0.0.63 host 172.16.227.133 eq 53
 permit tcp 172.16.195.64 0.0.0.63 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.195.64 0.0.0.63 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.195.64 0.0.0.63 172.16.227.64 0.0.0.31 established
 deny ip 172.16.195.64 0.0.0.63 172.16.192.0 0.0.63.255
```

```
 permit ip 172.16.195.64 0.0.0.63 any
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioM_Roma
 permit ip 172.16.195.160 0.0.0.15 172.16.211.128 0.0.0.15
 permit ip 172.16.195.160 0.0.0.15 172.16.227.112 0.0.0.15
 permit tcp 172.16.195.160 0.0.0.15 172.16.195.0 0.0.0.63
 permit udp 172.16.195.160 0.0.0.15 host 172.16.195.181 eq 53
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.195.182 eq 80
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.195.182 eq 443
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.227.132 eq 25
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.211.149 eq 25
 permit tcp 172.16.195.160 0.0.0.15 172.16.227.0 0.0.0.63
 permit tcp 172.16.195.160 0.0.0.15 172.16.211.0 0.0.0.63
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.227.134 eq 80
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.227.134 eq 443
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.211.150 eq 80
 permit tcp 172.16.195.160 0.0.0.15 host 172.16.211.150 eq 443
 permit udp 172.16.195.160 0.0.0.15 host 172.16.227.133 eq 53
 permit tcp 172.16.195.160 0.0.0.15 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.195.160 0.0.0.15 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.195.160 0.0.0.15 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS1_Roma
 permit ip 172.16.192.0 0.0.0.255 172.16.224.0 0.0.0.255
 permit ip 172.16.192.0 0.0.0.255 172.16.208.0 0.0.0.255
 permit tcp 172.16.192.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit udp 172.16.192.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.192.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.192.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.192.0 0.0.0.255 host 172.16.211.150 eq 443
 permit udp 172.16.192.0 0.0.0.255 host 172.16.227.133 eq 25
 permit tcp 172.16.192.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.192.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.192.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS2_Roma
 permit ip 172.16.193.0 0.0.0.255 172.16.225.0 0.0.0.255
 permit ip 172.16.193.0 0.0.0.255 172.16.209.0 0.0.0.255
 permit tcp 172.16.193.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit udp 172.16.193.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.193.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.193.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.193.0 0.0.0.255 host 172.16.211.150 eq 443
 permit udp 172.16.193.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.193.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.193.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.193.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS3_Roma
 permit ip 172.16.194.0 0.0.0.255 172.16.226.0 0.0.0.255
 permit ip 172.16.194.0 0.0.0.255 172.16.210.0 0.0.0.255
 permit tcp 172.16.194.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit udp 172.16.194.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.227.132 eq 25
```

```
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.194.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.194.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.194.0 0.0.0.255 host 172.16.211.150 eq 443
 permit udp 172.16.194.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.194.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.194.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.194.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioSS_Roma
 permit tcp 172.16.195.128 0.0.0.31 172.16.192.0 0.0.63.255
 permit ip 172.16.195.128 0.0.0.31 172.16.211.64 0.0.0.31
 permit ip 172.16.195.128 0.0.0.31 172.16.227.64 0.0.0.31
 permit udp 172.16.195.128 0.0.0.31 host 172.16.195.181 eq 53
 permit udp 172.16.195.128 0.0.0.31 host 172.16.227.133 eq 53
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended GlobalVLAN_Roma
 permit tcp host 172.16.195.182 eq 80 any established
 permit tcp host 172.16.195.182 eq 443 any established
 permit udp host 172.16.195.181 eq 53 any gt 1
 permit tcp 172.16.195.176 0.0.0.7 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.195.176 0.0.0.7 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.195.176 0.0.0.7 172.16.227.64 0.0.0.31 established
ip access-list extended ServerVLAN_Roma
 permit tcp 172.16.195.0 0.0.0.63 172.16.192.0 0.0.63.255
 permit ip 172.16.195.0 0.0.0.63 172.16.227.0 0.0.0.63
 permit ip 172.16.195.0 0.0.0.63 172.16.211.0 0.0.0.63
!
ip dhcp excluded-address 172.16.195.124 172.16.195.126
ip dhcp excluded-address 172.16.195.172 172.16.195.174
ip dhcp excluded-address 172.16.195.141 172.16.195.158
ip dhcp excluded-address 172.16.192.252 172.16.192.254
ip dhcp excluded-address 172.16.193.252 172.16.193.254
ip dhcp excluded-address 172.16.194.252 172.16.194.254
!
ip dhcp pool DominioDA_Roma
 network 172.16.195.64 255.255.255.192
 default-router 172.16.195.65
 dns-server 172.16.195.181
ip dhcp pool DominioM_Roma
 network 172.16.195.160 255.255.255.240
 default-router 172.16.195.161
 dns-server 172.16.195.181
ip dhcp pool DominioSS_Roma
 network 172.16.195.128 255.255.255.224
 default-router 172.16.195.129
 dns-server 172.16.195.181
ip dhcp pool DominioRS1_Roma
 network 172.16.192.0 255.255.255.0
 default-router 172.16.192.1
 dns-server 172.16.195.181
ip dhcp pool DominioRS2_Roma
 network 172.16.193.0 255.255.255.0
 default-router 172.16.193.1
 dns-server 172.16.195.181
ip dhcp pool DominioRS3_Roma
 network 172.16.194.0 255.255.255.0
 default-router 172.16.194.1
 dns-server 172.16.195.181
!
no cdp run
!
banner motd #Router WWAS RomaLocal: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
```

```
 login
line vty 0 4
 password class
 login
!
!
end
```

A.2 Router Padova

```
!
service password-encryption
!
hostname Padova
!
!
enable secret cisco
!
!
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial0/0.104 point-to-point
 description To Roma-ext
 ip address 172.16.240.5 255.255.255.252
 frame-relay interface-dlci 104
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial1/0.108 point-to-point
 description To Pisa (Backup)
 bandwidth 256
 ip address 172.16.240.10 255.255.255.252
 frame-relay interface-dlci 108
!
interface Serial1/0.116 point-to-point
 description To RomaLocal (Backup)
 bandwidth 256
 ip address 172.16.240.17 255.255.255.252
 frame-relay interface-dlci 116
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet2/0.21
 description GlobalVLAN_Padova
 encapsulation dot1Q 21
 ip address 172.16.211.145 255.255.255.248
 ip access-group GlobalVLAN_Padova in
!
interface GigabitEthernet2/0.22
 description ServerVLAN_Padova
 encapsulation dot1Q 22
 ip address 172.16.211.1 255.255.255.192
 ip access-group ServerVLAN_Padova in
!
interface GigabitEthernet2/0.23
 description DominioDA_Padova
 encapsulation dot1Q 23
 ip address 172.16.211.97 255.255.255.224
 ip access-group DominioDA_Padova in
!
interface GigabitEthernet2/0.24
 description DominioM_Padova
 encapsulation dot1Q 24
 ip address 172.16.211.129 255.255.255.240
 ip access-group DominioM_Padova in
!
```

```
interface GigabitEthernet2/0.25
 description DominioSS_Padova
 encapsulation dot1Q 25
 ip address 172.16.211.65 255.255.255.224
 ip access-group DominioSS_Padova in
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet3/0.26
 description DominioRS1_Padova
 encapsulation dot1Q 26
 ip address 172.16.208.1 255.255.255.0
 ip access-group DominioRS1_Padova in
!
interface GigabitEthernet3/0.27
 description DominioRS2_Padova
 encapsulation dot1Q 27
 ip address 172.16.209.1 255.255.255.0
 ip access-group DominioRS2_Padova in
!
interface GigabitEthernet3/0.28
 description DominioRS3_Padova
 encapsulation dot1Q 28
 ip address 172.16.210.1 255.255.255.0
 ip access-group DominioRS3_Padova in
!
router ospf 1
 log-adjacency-changes
 network 172.16.240.4 0.0.0.3 area 0
 network 172.16.240.8 0.0.0.3 area 0
 network 172.16.240.16 0.0.0.3 area 0
 network 172.16.208.0 0.0.15.255 area 0
!
!
ip access-list extended DominioDA_Padova
 permit ip 172.16.211.96 0.0.0.31 172.16.195.64 0.0.0.63
 permit ip 172.16.211.96 0.0.0.31 172.16.227.96 0.0.0.15
 permit tcp 172.16.211.96 0.0.0.31 172.16.211.0 0.0.0.63
 permit udp 172.16.211.96 0.0.0.31 host 172.16.195.181 eq 53
 permit udp 172.16.211.96 0.0.0.31 host 172.16.227.133 eq 53
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.211.150 eq 80
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.211.150 eq 443
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.211.149 eq 25
 permit tcp 172.16.211.96 0.0.0.31 172.16.195.0 0.0.0.63
 permit tcp 172.16.211.96 0.0.0.31 172.16.227.0 0.0.0.63
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.195.182 eq 80
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.195.182 eq 443
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.227.134 eq 80
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.227.134 eq 443
 permit tcp 172.16.211.96 0.0.0.31 host 172.16.227.132 eq 25
 permit tcp 172.16.211.96 0.0.0.31 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.211.96 0.0.0.31 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.211.96 0.0.0.31 172.16.227.64 0.0.0.31 established
 deny ip 172.16.211.96 0.0.0.31 172.16.192.0 0.0.63.255
 permit ip 172.16.211.96 0.0.0.31 any
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioM_Padova
 permit ip 172.16.211.128 0.0.0.15 172.16.195.160 0.0.0.15
 permit ip 172.16.211.128 0.0.0.15 172.16.227.112 0.0.0.15
 permit tcp 172.16.211.128 0.0.0.15 172.16.211.0 0.0.0.63
 permit udp 172.16.211.128 0.0.0.15 host 172.16.195.181 eq 53
 permit udp 172.16.211.128 0.0.0.15 host 172.16.227.133 eq 53
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.211.150 eq 80
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.211.150 eq 443
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.211.149 eq 25
 permit tcp 172.16.211.128 0.0.0.15 172.16.195.0 0.0.0.63
```

```
 permit tcp 172.16.211.128 0.0.0.15 172.16.227.0 0.0.0.63
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.195.182 eq 80
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.195.182 eq 443
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.227.134 eq 80
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.227.134 eq 443
 permit tcp 172.16.211.128 0.0.0.15 host 172.16.227.132 eq 25
 permit tcp 172.16.211.128 0.0.0.15 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.211.128 0.0.0.15 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.211.128 0.0.0.15 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS1_Padova
 permit ip 172.16.208.0 0.0.0.255 172.16.224.0 0.0.0.255
 permit ip 172.16.208.0 0.0.0.255 172.16.192.0 0.0.0.255
 permit tcp 172.16.208.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit udp 172.16.208.0 0.0.0.255 host 172.16.195.181 eq 53
 permit udp 172.16.208.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.208.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.208.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.208.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.208.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.208.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.208.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS2_Padova
 permit ip 172.16.209.0 0.0.0.255 172.16.225.0 0.0.0.255
 permit ip 172.16.209.0 0.0.0.255 172.16.193.0 0.0.0.255
 permit tcp 172.16.209.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit udp 172.16.209.0 0.0.0.255 host 172.16.195.181 eq 53
 permit udp 172.16.209.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.209.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.209.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.209.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.209.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.209.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.209.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS3_Padova
 permit ip 172.16.210.0 0.0.0.255 172.16.226.0 0.0.0.255
 permit ip 172.16.210.0 0.0.0.255 172.16.194.0 0.0.0.255
 permit tcp 172.16.210.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit udp 172.16.210.0 0.0.0.255 host 172.16.195.181 eq 53
 permit udp 172.16.210.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.211.149 eq 25
 permit tcp 172.16.210.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.210.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.210.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.210.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.210.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.210.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
```

```
ip access-list extended DominioSS_Padova
 permit tcp 172.16.211.64 0.0.0.31 172.16.192.0 0.0.63.255
 permit ip 172.16.211.64 0.0.0.31 172.16.195.128 0.0.0.31
 permit ip 172.16.211.64 0.0.0.31 172.16.227.64 0.0.0.31
 permit udp 172.16.211.64 0.0.0.31 host 172.16.195.181 eq 53
 permit udp 172.16.211.64 0.0.0.31 host 172.16.227.133 eq 53
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended GlobalVLAN_Padova
 permit tcp host 172.16.211.150 eq 80 any established
 permit tcp host 172.16.211.150 eq 443 any established
 permit tcp host 172.16.211.149 eq 25 any gt 1
 permit tcp 172.16.211.144 0.0.0.7 172.16.211.64 0.0.0.31 established
 permit tcp 172.16.211.144 0.0.0.7 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.211.144 0.0.0.7 172.16.227.64 0.0.0.31 established
ip access-list extended ServerVLAN_Padova
 permit tcp 172.16.211.0 0.0.0.63 172.16.192.0 0.0.63.255
 permit ip 172.16.211.0 0.0.0.63 172.16.195.0 0.0.0.63
 permit ip 172.16.211.0 0.0.0.63 172.16.227.0 0.0.0.63
!
ip dhcp excluded-address 172.16.211.124 172.16.211.126
ip dhcp excluded-address 172.16.211.140 172.16.211.142
ip dhcp excluded-address 172.16.211.76 172.16.211.94
ip dhcp excluded-address 172.16.208.252 172.16.208.254
ip dhcp excluded-address 172.16.209.252 172.16.209.254
ip dhcp excluded-address 172.16.210.252 172.16.210.254
!
ip dhcp pool DominioDA_Padova
 network 172.16.211.96 255.255.255.224
 default-router 172.16.211.97
 dns-server 172.16.195.181
ip dhcp pool DominioM_Padova
 network 172.16.211.128 255.255.255.240
 default-router 172.16.211.129
 dns-server 172.16.195.181
ip dhcp pool DominioSS_Padova
 network 172.16.211.64 255.255.255.224
 default-router 172.16.211.65
 dns-server 172.16.195.181
ip dhcp pool DominioRS1_Padova
 network 172.16.208.0 255.255.255.0
 default-router 172.16.208.1
 dns-server 172.16.195.181
ip dhcp pool DominioRS2_Padova
 network 172.16.209.0 255.255.255.0
 default-router 172.16.209.1
 dns-server 172.16.227.133
ip dhcp pool DominioRS3_Padova
 network 172.16.210.0 255.255.255.0
 default-router 172.16.210.1
 dns-server 172.16.227.133
!
no cdp run
!
banner motd #Router WWAS Padova: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
line vty 0 4
 password class
 login
!
!
end
```

A.3 Router Pisa

```
!
service password-encryption
!
hostname Pisa
!
!
enable secret cisco
!
!
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial0/0.100 point-to-point
 description To Roma-ext
 ip address 172.16.240.1 255.255.255.252
 frame-relay interface-dlci 100
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial1/0.108 point-to-point
 description To Padova (Backup)
 bandwidth 256
 ip address 172.16.240.9 255.255.255.252
 frame-relay interface-dlci 108
!
interface Serial1/0.112 point-to-point
 description To RomaLocal (Backup)
 bandwidth 256
 ip address 172.16.240.13 255.255.255.252
 frame-relay interface-dlci 112
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet2/0.31
 description GlobalVLAN_Pisa
 encapsulation dot1Q 31
 ip address 172.16.227.129 255.255.255.248
 ip access-group GlobalVLAN_Pisa in
!
interface GigabitEthernet2/0.32
 description ServerVLAN_Pisa
 encapsulation dot1Q 32
 ip address 172.16.227.1 255.255.255.192
 ip access-group ServerVLAN_Pisa in
!
interface GigabitEthernet2/0.33
 description DominioDA_Pisa
 encapsulation dot1Q 33
 ip address 172.16.227.97 255.255.255.240
 ip access-group DominioDA_Pisa in
!
interface GigabitEthernet2/0.34
 description DominioM_Pisa
 encapsulation dot1Q 34
 ip address 172.16.227.113 255.255.255.240
 ip access-group DominioM_Pisa in
!
```

```
interface GigabitEthernet2/0.35
 description DominioSS_Pisa
 encapsulation dot1Q 35
 ip address 172.16.227.65 255.255.255.224
 ip access-group DominioSS_Pisa in
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet3/0.36
 description DominioRS1_Pisa
 encapsulation dot1Q 36
 ip address 172.16.224.1 255.255.255.0
 ip access-group DominioRS1_Pisa in
!
interface GigabitEthernet3/0.37
 description DominioRS2_Pisa
 encapsulation dot1Q 37
 ip address 172.16.225.1 255.255.255.0
 ip access-group DominioRS2_Pisa in
!
interface GigabitEthernet3/0.38
 description DominioRS3_Pisa
 encapsulation dot1Q 38
 ip address 172.16.226.1 255.255.255.0
 ip access-group DominioRS3_Pisa in
!
router ospf 1
 log-adjacency-changes
 network 172.16.240.0 0.0.0.3 area 0
 network 172.16.240.8 0.0.0.3 area 0
 network 172.16.240.12 0.0.0.3 area 0
 network 172.16.224.0 0.0.15.255 area 0
!
!
ip access-list extended DominioDA_Pisa
 permit ip 172.16.227.96 0.0.0.15 172.16.195.64 0.0.0.63
 permit ip 172.16.227.96 0.0.0.15 172.16.211.96 0.0.0.31
 permit tcp 172.16.227.96 0.0.0.15 172.16.227.0 0.0.0.63
 permit udp 172.16.227.96 0.0.0.15 host 172.16.227.133 eq 53
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.227.134 eq 80
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.227.134 eq 443
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.227.132 eq 25
 permit tcp 172.16.227.96 0.0.0.15 172.16.195.0 0.0.0.63
 permit tcp 172.16.227.96 0.0.0.15 172.16.211.0 0.0.0.63
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.195.182 eq 80
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.195.182 eq 443
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.211.150 eq 80
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.211.150 eq 443
 permit tcp 172.16.227.96 0.0.0.15 host 172.16.211.149 eq 25
 permit udp 172.16.227.96 0.0.0.15 host 172.16.195.181 eq 53
 permit tcp 172.16.227.96 0.0.0.15 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.227.96 0.0.0.15 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.227.96 0.0.0.15 172.16.211.64 0.0.0.31 established
 deny ip 172.16.227.96 0.0.0.15 172.16.192.0 0.0.63.255
 permit ip 172.16.227.96 0.0.0.15 any
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioM_Pisa
 permit ip 172.16.227.112 0.0.0.15 172.16.195.160 0.0.0.15
 permit ip 172.16.227.112 0.0.0.15 172.16.211.128 0.0.0.15
 permit tcp 172.16.227.112 0.0.0.15 172.16.227.0 0.0.0.63
 permit udp 172.16.227.112 0.0.0.15 host 172.16.227.133 eq 53
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.227.134 eq 80
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.227.134 eq 443
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.227.132 eq 25
 permit tcp 172.16.227.112 0.0.0.15 172.16.195.0 0.0.0.63
 permit tcp 172.16.227.112 0.0.0.15 172.16.211.0 0.0.0.63
```

```
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.195.182 eq 80
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.195.182 eq 443
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.211.150 eq 80
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.211.150 eq 443
 permit tcp 172.16.227.112 0.0.0.15 host 172.16.211.149 eq 25
 permit udp 172.16.227.112 0.0.0.15 host 172.16.195.181 eq 53
 permit tcp 172.16.227.112 0.0.0.15 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.227.112 0.0.0.15 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.227.112 0.0.0.15 172.16.211.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS1_Pisa
 permit ip 172.16.224.0 0.0.0.255 172.16.192.0 0.0.0.255
 permit ip 172.16.224.0 0.0.0.255 172.16.208.0 0.0.0.255
 permit tcp 172.16.224.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit udp 172.16.224.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.224.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.224.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.224.0 0.0.0.255 host 172.16.211.149 eq 25
 permit udp 172.16.224.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.224.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.224.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.224.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS2_Pisa
 permit ip 172.16.225.0 0.0.0.255 172.16.193.0 0.0.0.255
 permit ip 172.16.225.0 0.0.0.255 172.16.209.0 0.0.0.255
 permit tcp 172.16.225.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit udp 172.16.225.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.225.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.225.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.225.0 0.0.0.255 host 172.16.211.149 eq 25
 permit udp 172.16.225.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.225.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.225.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.225.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended DominioRS3_Pisa
 permit ip 172.16.226.0 0.0.0.255 172.16.194.0 0.0.0.255
 permit ip 172.16.226.0 0.0.0.255 172.16.210.0 0.0.0.255
 permit tcp 172.16.226.0 0.0.0.255 172.16.227.0 0.0.0.63
 permit udp 172.16.226.0 0.0.0.255 host 172.16.227.133 eq 53
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.227.134 eq 80
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.227.134 eq 443
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.227.132 eq 25
 permit tcp 172.16.226.0 0.0.0.255 172.16.195.0 0.0.0.63
 permit tcp 172.16.226.0 0.0.0.255 172.16.211.0 0.0.0.63
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.195.182 eq 80
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.195.182 eq 443
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.211.150 eq 80
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.211.150 eq 443
 permit tcp 172.16.226.0 0.0.0.255 host 172.16.211.149 eq 25
 permit udp 172.16.226.0 0.0.0.255 host 172.16.195.181 eq 53
 permit tcp 172.16.226.0 0.0.0.255 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.226.0 0.0.0.255 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.226.0 0.0.0.255 172.16.211.64 0.0.0.31 established
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
```

```
ip access-list extended DominioSS_Pisa
 permit tcp 172.16.227.64 0.0.0.31 172.16.192.0 0.0.63.255
 permit ip 172.16.227.64 0.0.0.31 172.16.195.128 0.0.0.31
 permit ip 172.16.227.64 0.0.0.31 172.16.211.64 0.0.0.31
 permit udp 172.16.227.64 0.0.0.31 host 172.16.227.133 eq 53
 permit udp 172.16.227.64 0.0.0.31 host 172.16.195.181 eq 53
 permit udp host 0.0.0.0 eq 68 host 255.255.255.255 eq 67
ip access-list extended GlobalVLAN_Pisa
 permit tcp host 172.16.227.134 eq 80 any established
 permit tcp host 172.16.227.134 eq 443 any established
 permit udp host 172.16.227.133 eq 53 any gt 1
 permit tcp host 172.16.227.132 eq 25 any gt 1
 permit tcp 172.16.227.128 0.0.0.7 172.16.227.64 0.0.0.31 established
 permit tcp 172.16.227.128 0.0.0.7 172.16.195.128 0.0.0.31 established
 permit tcp 172.16.227.128 0.0.0.7 172.16.211.64 0.0.0.31 established
ip access-list extended ServerVLAN_Pisa
 permit tcp 172.16.227.0 0.0.0.63 172.16.192.0 0.0.63.255
 permit ip 172.16.227.0 0.0.0.63 172.16.195.0 0.0.0.63
 permit ip 172.16.227.0 0.0.0.63 172.16.211.0 0.0.0.63
!
ip dhcp excluded-address 172.16.227.108 172.16.227.110
ip dhcp excluded-address 172.16.227.124 172.16.227.126
ip dhcp excluded-address 172.16.227.80 172.16.227.94
ip dhcp excluded-address 172.16.224.252 172.16.224.254
ip dhcp excluded-address 172.16.225.252 172.16.225.254
ip dhcp excluded-address 172.16.226.252 172.16.226.254
!
ip dhcp pool DominioDA_Pisa
 network 172.16.227.96 255.255.255.240
 default-router 172.16.227.97
 dns-server 172.16.227.133
ip dhcp pool DominioM_Pisa
 network 172.16.227.112 255.255.255.240
 default-router 172.16.227.113
 dns-server 172.16.227.133
ip dhcp pool DominioSS_Pisa
 network 172.16.227.64 255.255.255.224
 default-router 172.16.227.65
 dns-server 172.16.227.133
ip dhcp pool DominioRS1_Pisa
 network 172.16.224.0 255.255.255.0
 default-router 172.16.224.1
 dns-server 172.16.227.133
ip dhcp pool DominioRS2_Pisa
 network 172.16.225.0 255.255.255.0
 default-router 172.16.225.1
 dns-server 172.16.227.133
ip dhcp pool DominioRS3_Pisa
 network 172.16.226.0 255.255.255.0
 default-router 172.16.226.1
 dns-server 172.16.227.133
!
no cdp run
!
banner motd #Router WWAS Pisa: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
line vty 0 4
 password class
 login
!
!
end
```

A.4 Router Roma-ext

```
!
service password-encryption
!
hostname Roma-ext
!
!
enable secret cisco
!
!
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial0/0.100 point-to-point
 description To Pisa
 ip address 172.16.240.2 255.255.255.252
 frame-relay interface-dlci 100
 ip nat inside
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no shutdown
!
interface Serial1/0.104 point-to-point
 description To Padova
 ip address 172.16.240.6 255.255.255.252
 frame-relay interface-dlci 104
 ip nat inside
!
interface Serial2/0
 description To ISP-InternetGW
 ip address 213.140.19.100 255.255.255.248
 ip access-group EXTERNAL in
 ip access-group INTERNET out
 ip nat outside
 no shutdown
!
interface FastEthernet3/0
 description To RomaLocal (A)
 ip address 172.16.240.22 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet4/0
 description To RomaLocal (B)
 ip address 172.16.240.26 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.16.240.0 0.0.0.3 area 0
 network 172.16.240.4 0.0.0.3 area 0
 network 172.16.240.20 0.0.0.3 area 0
 network 172.16.240.24 0.0.0.3 area 0
 default-information originate
!
ip nat pool external 213.140.19.100 213.140.19.102 netmask 255.255.255.248
ip nat inside source list 3 pool external overload
ip nat inside source static tcp 172.16.195.182 80 213.140.19.100 80
```

```
ip nat inside source static tcp 172.16.227.134 80 213.140.19.102 80
ip nat inside source static tcp 172.16.211.150 80 213.140.19.101 80
ip nat inside source static tcp 172.16.195.182 443 213.140.19.100 443
ip nat inside source static tcp 172.16.227.134 443 213.140.19.102 443
ip nat inside source static tcp 172.16.211.150 443 213.140.19.101 443
ip nat inside source static udp 172.16.195.181 53 213.140.19.100 53
ip nat inside source static udp 172.16.227.133 53 213.140.19.102 53
ip nat inside source static tcp 172.16.227.132 25 213.140.19.102 25
ip nat inside source static tcp 172.16.211.149 25 213.140.19.101 25
ip route 0.0.0.0 0.0.0.0 Serial2/0
!
access-list 3 permit 172.16.195.64 0.0.0.63
access-list 3 permit 172.16.211.96 0.0.0.31
access-list 3 permit 172.16.227.96 0.0.0.15
ip access-list extended EXTERNAL
 permit tcp any host 213.140.19.100 eq 80
 permit tcp any host 213.140.19.100 eq 443
 permit tcp any host 213.140.19.101 eq 80
 permit tcp any host 213.140.19.101 eq 443
 permit tcp any host 213.140.19.102 eq 80
 permit tcp any host 213.140.19.102 eq 443
 permit tcp any host 213.140.19.101 eq 25
 permit tcp any host 213.140.19.102 eq 25
 permit tcp any host 213.140.19.100 eq 53
 permit tcp any host 213.140.19.102 eq 53
 permit tcp any host 213.140.19.100 established
 permit tcp any host 213.140.19.101 established
 permit tcp any host 213.140.19.102 established
ip access-list extended INTERNET
 deny ip any 172.16.192.0 0.0.63.255
 permit ip any any
!
!
!
no cdp run
!
banner motd #Router WWAS Roma-ext: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
line vty 0 4
 password class
 login
!
!
end
```

B.1 Switch livello Core

A scopo di esempio si fornisce la configurazione dello switch RomaCore1. Ovviamente per poter implementare concretamente quanto sinora descritto è necessario fare alcune ipotesi.
In particolare per gli switch di livello core si suppone che:

- I Server Web e DNS siano connessi allo switch RomaCore1, sulle porte gigabitEthernet 1/4 ed 1/5
- I Server di Workgroup al momento connessi siano 2 per ogni dominio di sicurezza, connessi come segue:
  - dalla porte gigabitEthernet 1/6 a 1/11 per i domini DA, M ed SS sullo switch RomaCore1;
  - dalla porte gigabitEthernet 1/4 a 1/7 per i due domini RS attualmente attivi;
  - le restanti porte saranno occupate da server di tipo Enterprise.

```
!
service password-encryption
!
hostname RomaCore1
!
enable secret cisco
!
!
spanning-tree vlan 11 priority 4096
spanning-tree vlan 12 priority 4096
spanning-tree vlan 13 priority 4096
spanning-tree vlan 14 priority 4096
spanning-tree vlan 15 priority 4096
spanning-tree vlan 16 priority 8192
spanning-tree vlan 17 priority 8192
spanning-tree vlan 18 priority 8192
!
interface FastEthernet0/1
 description To RomaAccessCentral1
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/2
 description To RomaAccessNord1
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/3
 description To RomaAccessNord2
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/4
 description To RomaAccessNord3
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
```

```
interface FastEthernet0/5
 description To RomaAccessNord4
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/6
 description To RomaAccessNord5
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/7
 description To RomaAccessNord6
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/8
 description To RomaAccessSud1
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/9
 description To RomaAccessSud2
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/10
 description To RomaAccessSud3
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/11
 description To RomaAccessSud4
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/12
 description To RomaAccessSud5
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/13
 description To RomaAccessSud6
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
```

```
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet1/1
 description To Router RomaLocal
 switchport mode trunk
 ip dhcp snooping trust
 no shutdown
!
interface GigabitEthernet1/2
 description To RomaCore2 (A)
 switchport mode trunk
 ip dhcp snooping trust
 no shutdown
!
interface GigabitEthernet1/3
 description To RomaCore2 (B)
 switchport mode trunk
 ip dhcp snooping trust
 no shutdown
!
interface GigabitEthernet1/4
 description To Web Server
 switchport access vlan 11
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/5
 description To DNS Server
 switchport access vlan 11
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/6
 description To WorkGroupDA 1
 switchport access vlan 13
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/7
 description To WorkGroupDA 2
 switchport access vlan 13
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
```

```
!
interface GigabitEthernet1/8
 description To WorkGroupM 1
 switchport access vlan 14
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/9
 description To WorkGroupM 2
 switchport access vlan 14
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/10
 description To WorkGroupSS 1
 switchport access vlan 15
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/11
 description To WorkGroupSS 2
 switchport access vlan 15
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/12
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/13
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/14
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/15
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

```
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/16
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/17
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/18
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/19
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/20
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/21
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/22
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/23
 description To Enterprise
 switchport access vlan 12
 switchport mode access
```

```
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/24
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/25
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/26
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/27
 description To Enterprise
 switchport access vlan 12
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet1/28
 shutdown
!
interface GigabitEthernet1/29
 shutdown
!
interface GigabitEthernet1/30
 shutdown
!
interface GigabitEthernet1/31
 shutdown
!
interface GigabitEthernet1/32
 shutdown
!
interface GigabitEthernet1/33
 shutdown
!
interface GigabitEthernet1/34
 shutdown
!
interface GigabitEthernet1/35
 shutdown
!
interface GigabitEthernet1/36
 shutdown
!
interface GigabitEthernet1/37
 shutdown
```

```
!
interface GigabitEthernet1/38
 shutdown
!
interface GigabitEthernet1/39
 shutdown
!
interface GigabitEthernet1/40
 shutdown
!
interface GigabitEthernet1/41
 shutdown
!
interface GigabitEthernet1/42
 shutdown
!
interface GigabitEthernet1/43
 shutdown
!
interface GigabitEthernet1/44
 shutdown
!
interface GigabitEthernet1/45
 shutdown
!
interface GigabitEthernet1/46
 shutdown
!
interface GigabitEthernet1/47
 shutdown
!
interface GigabitEthernet1/48
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan15
 ip address 172.16.195.141 255.255.255.224
!
vlan 11
 name GlobalVLAN_Roma
vlan 12
 name ServerVLAN_Roma
vlan 13
 name DominioDA_Roma
vlan 14
 name DominioM_Roma
vlan 15
 name DominioSS_Roma
vlan 16
 name DominioRS1_Roma
vlan 17
 name DominioRS2_Roma
vlan 18
 name DominioRS3_Roma
!
vtp version 1
vtp domain wwas_roma
vtp mode server
vtp password cisco
vtp pruning
!
ip default-gateway 172.16.195.129
ip dhcp snooping
!
no cdp run
!
banner motd #Switch WWAS RomaCore1: l'accesso e'
```

```
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
!
line vty 0 4
 password class
 login
line vty 5 15
 password class
 login
!
!
end
```

B.2 Switch livello Access

A scopo di esempio si fornisce la configurazione dello switch RomaAccessNord3. Ovviamente per poter implementare concretamente quanto sinora descritto è necessario fare alcune ipotesi.
In particolare per questo switch di livello access si suppone che:

- siano connesse 3 postazioni del dominio di Direzione ed Amministrazione, dalla porte fastEthernet 0/7 alla 0/9;
- sia connessa una postazione del dominio di Marketing, alla porte fastEthernet 0/10;
- siano connesse 2 postazioni del dominio di Supporto Sistemi, dalla porte fastEthernet 0/11 alla 0/12;
- siano connesse 6 postazioni del primo gruppo di Ricerca e Sviluppo, dalla porte fastEthernet 0/13 alla 0/18;
- siano connesse 6 postazioni del secondo gruppo di Ricerca e Sviluppo, dalla porte fastEthernet 0/19 alla 0/24.

```
!
service password-encryption
!
hostname RomaNordAccess3
!
enable secret cisco
!
!
!
interface FastEthernet0/1
 description To RomaCore1
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/2
 description To RomaCore2
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/3
 description To RomaAccessNord4
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/4
 description To RomaAccessNord2
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
 no shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 description To DominioDA 1
 switchport access vlan 13
```

```
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/8
 description To DominioDA 2
 switchport access vlan 13
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/9
 description To DominioDA 3
 switchport access vlan 13
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/10
 description To DominioM 1
 switchport access vlan 14
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/11
 description To DominioSS 1
 switchport access vlan 15
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/12
 description To DominioSS 2
 switchport access vlan 15
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/13
 description To DominioRS1 1
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/14
 description To DominioRS1 2
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/15
```

```
 description To DominioRS1 3
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/16
 description To DominioRS1 4
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/17
 description To DominioRS1 5
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/18
 description To DominioRS1 6
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 description To DominioRS2 1
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/20
 description To DominioRS2 2
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/21
 description To DominioRS2 3
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/22
 description To DominioRS2 4
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
```

```
!
interface FastEthernet0/23
 description To DominioRS2 5
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/24
 description To DominioRS2 6
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 spanning-tree portfast
 no shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan15
 ip address 172.16.195.146 255.255.255.224
!
vtp version 1
vtp domain wwas_roma
vtp mode client
vtp password cisco
!
ip default-gateway 172.16.195.129
ip dhcp snooping
!
no cdp run
!
banner motd #Switch WWAS RomaNordAccess1: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
!
line vty 0 4
 password class
 login
line vty 5 15
 password class
 login
!
!
end
```

C.1 MDF1 (livello distribution/access)

In questo esempio di configurazione abbiamo assunto preventivamente e arbitrariamente che:

- il Server Web è connesso alla porta gigabitEthernet 0/22;
- il Server SMTP è connesso alla porta gigabitEthernet 0/23;
- sulle porte gigabitEthernet 0/24 – 30 sono connessi Enterprise Server;
- sulle porte gigabitEthernet 0/31 – 32 sono connessi due Workgroup Server per la funzione Direzione e Amministrazione;
- sulle porte gigabitEthernet 0/33 – 34 sono connessi due Workgroup Server per la funzione Marketing;
- sulle porte gigabitEthernet 0/35 – 36 sono connessi due Workgroup Server per la funzione Supporto Sistemi.

I server globali sono indicati col nome 'Web Server' e 'SMTP Server'.
I server enterprise sono indicati col nome 'Enterprise X', dove X è un numero progressivo a partire da 1.
I workgroup server sono indicati col nome 'WS_[dominio]_X', dove *dominio* è la sigla di una/tre lettere rappresentante la funzione aziendale (DA, M, SS, RS1, RS2, RS3) e X è un numero progressivo a partire da 1.

```
!
service password-encryption
!
hostname MDF1
!
enable secret cisco
!
!
banner motd #Switch WWAS Padova MDF1: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
!
line con 0
 password class
 login
!
line vty 0 15
 password class
 login
!
no cdp run
!
vtp version 1
vtp domain wwas_pad
vtp mode server
vtp password cisco
vtp pruning
!
vlan 21
 name GlobalVLAN_Padova
vlan 22
 name ServerVLAN_Padova
vlan 23
 name DominioDA_Padova
vlan 24
 name DominioM_Padova
vlan 25
 name DominioSS_Padova
```

```
vlan 26
 name DominioRS1_Padova
vlan 27
 name DominioRS2_Padova
vlan 28
 name DominioRS3_Padova
!
spanning-tree vlan 21 priority 4096
spanning-tree vlan 22 priority 4096
spanning-tree vlan 23 priority 4096
spanning-tree vlan 24 priority 4096
spanning-tree vlan 25 priority 4096
spanning-tree vlan 26 priority 8192
spanning-tree vlan 27 priority 8192
spanning-tree vlan 28 priority 8192
!
ip dhcp snooping
!
interface GigabitEthernet0/1
 description To IDF1
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/2
 description To IDF2
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/3
 description To IDF3
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/4
 description To IDF4
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/5
 description To IDF5
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/6
 description To IDF6
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/7
 description To MDF3
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/8
 description To MDF4
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/9
 description To MDF5
 switchport mode trunk
 switchport nonegotiate
```

```
 no shutdown
!
interface GigabitEthernet0/10
 description To MDF6
 switchport mode trunk
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/11
 shutdown
!
interface GigabitEthernet0/12
 shutdown
!
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
 shutdown
!
interface GigabitEthernet0/22
 description To Web Server
 switchport access vlan 21
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/23
 description To SMTP Server
 switchport access vlan 21
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/24
 description To Enterprise 1
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
```

```
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/25
 description To Enterprise 2
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/26
 description To Enterprise 3
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/27
 description To Enterprise 4
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/28
 description To Enterprise 5
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/29
 description To Enterprise 6
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/30
 description To Enterprise 7
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
```

```
interface GigabitEthernet0/31
 description To WS_DA_1
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/32
 description To WS_DA_2
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/33
 description To WS_M_1
 switchport access vlan 24
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/34
 description To WS_M_2
 switchport access vlan 24
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/35
 description To WS_SS_1
 switchport access vlan 25
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/36
 description To WS_SS_2
 switchport access vlan 25
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/37
 shutdown
!
interface GigabitEthernet0/38
```

```
 shutdown
!
interface GigabitEthernet0/39
 shutdown
!
interface GigabitEthernet0/40
 shutdown
!
interface GigabitEthernet0/41
 shutdown
!
interface GigabitEthernet0/42
 shutdown
!
interface GigabitEthernet0/43
 shutdown
!
interface GigabitEthernet0/44
 shutdown
!
interface GigabitEthernet0/45
 shutdown
!
interface GigabitEthernet0/46
 description To MDF2_1
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/47
 description To MDF2_2
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet0/48
 description To Router Padova
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan25
 ip address 172.16.211.80 255.255.255.224
!
!
end
```

C.2 IDF1 (livello access)

In questo esempio di configurazione abbiamo assunto preventivamente e arbitrariamente che:

- sulle porte fastEthernet 0/1 – 4 sono connesse 4 postazioni della funzione Direzione e Amministrazione;
- sulla porta fastEthernet 0/5 è connessa 1 postazione della funzione Marketing;
- sulle porte fastEthernet 0/11 – 12 sono connesse 2 postazioni della funzione Supporto Sistemi;
- sulle porte fastEthernet 0/7 – 10 sono connesse 4 postazioni della funzione Ricerca e Sviluppo, gruppo di lavoro 1;
- sulle porte fastEthernet 0/15 – 18 sono connesse 4 postazioni della funzione Ricerca e Sviluppo, gruppo di lavoro 2;

Gli host sono indicati col nome '[stanza]_[dominio]_X', dove *stanza* è l'etichetta della stanza dove è collocato l'host, *dominio* è la sigla di una/tre lettere rappresentante la funzione aziendale (DA, M, SS, RS1, RS2, RS3) e X è un numero progressivo a partire da 1.

```
!
service password-encryption
!
hostname IDF1
!
enable secret cisco
!
!
banner motd #Switch WWAS Padova IDF1: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#
line con 0
 password class
 login
!
line vty 0 15
 password class
 login
!
no cdp run
!
vtp version 1
vtp domain wwas_pad
vtp mode client
vtp password cisco
!
ip dhcp snooping
!
interface FastEthernet0/1
 description To R-C1_DA_1
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/2
 description To R-C1_DA_2
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
```

```
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/3
 description To R-C1_DA_3
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/4
 description To R-C1_DA_4
 switchport access vlan 23
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/5
 description To R-C1_M_1
 switchport access vlan 24
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 description To R-C2_RS1_1
 switchport access vlan 26
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/8
 description To R-C2_RS1_2
 switchport access vlan 26
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/9
 description To R-C2_RS1_3
 switchport access vlan 26
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
```

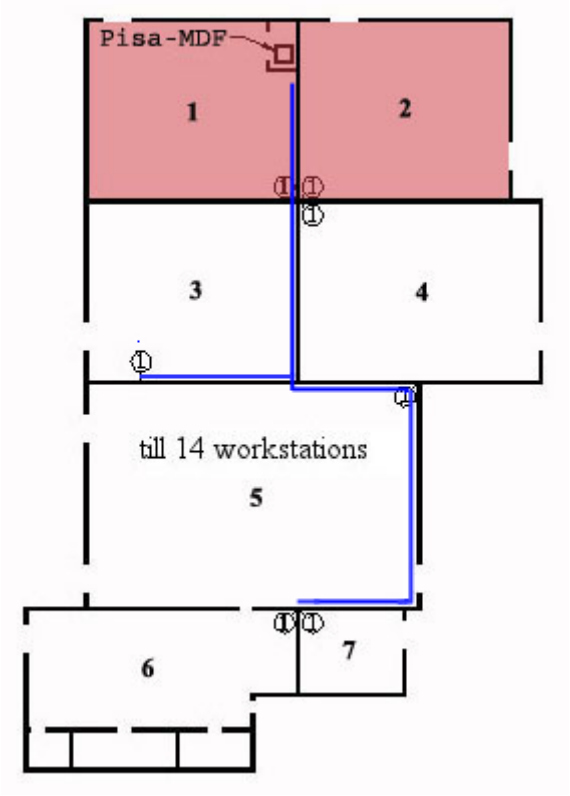
```
 no shutdown
!
interface FastEthernet0/10
 description To R-C2_RS1_4
 switchport access vlan 26
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/11
 description To R-C2_SS_1
 switchport access vlan 25
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/12
 description To R-C2_SS_2
 switchport access vlan 25
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 description To R-C3_RS2_1
 switchport access vlan 27
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/16
 description To R-C3_RS2_2
 switchport access vlan 27
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/17
 description To R-C3_RS2_3
 switchport access vlan 27
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
```

```
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/18
 description To R-C3_RS2_4
 switchport access vlan 27
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 description To IDF2
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface FastEthernet0/24
 description To IDF6
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet1/1
 description To MDF1
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface GigabitEthernet1/2
 description To MDF2
 switchport mode trunk
 ip dhcp snooping trust
 switchport nonegotiate
 no shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan25
 ip address 172.16.211.86 255.255.255.224
!
!
end
```

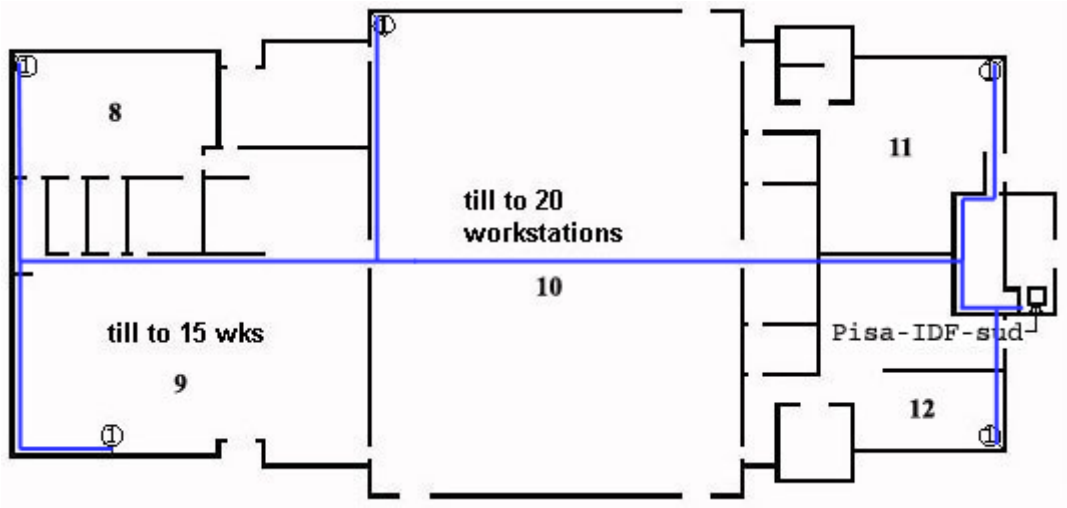
Per la configurazione del router Pisa, si rimanda alla appendice A.3.

D.1 Mappe fisiche per il cablaggio orizzontale

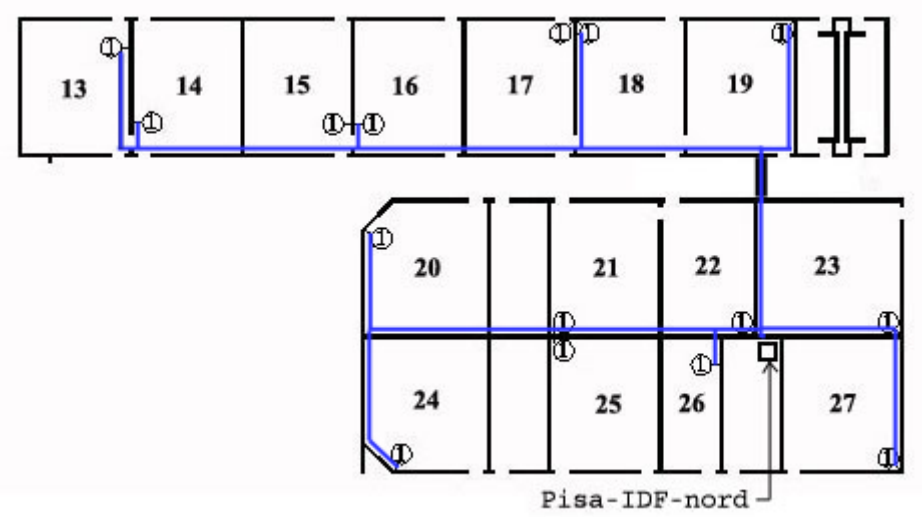
Le mappe riportate sotto illustrano i percorsi che il cablaggio orizzontale dovrebbe seguire



PISA-EST



PISA-SUD



PISA-NORD

Per conoscere il numero e il tipo dei cavi fare riferimento alla descrizione della rete della sede di Pisa (sezione 4).

D.2 Switch Pisa-MDF-S1

Per questa configurazione esemplificativa si fanno le seguenti ipotesi:

- Sulla porta gigabitEthernet 1/1 è stato connesso il server Web sella sede di Pisa.
- Sulla porta gigabitEthernet 1/2 è stato connesso il server DNS della sede di Pisa.
- Sulle porte gigabitEthernet da 1/3 a 1/10 sono connessi dei server Enterprise.
- Sulla porta gigabitEthernet 1/13 è stato connesso un server di workgroup appartenente alla funzione Marketing.
- Sulla porta gigabitEthernet 1/14 è stato connesso un server di workgroup appartenente al primo gruppo di progetto della funzione ricerca e sviluppo (DominioRS1_Pisa).

Si suppone inoltre che la versione del sistema operativo di networking dello switch sia tale da

- Utilizzare come incapsulamento di default (per link di tipo trunk) l'incapsulamento 802.1Q.
- Associare allo switch una Bridge Priority di default pari a 32768 (per ogni VLAN).

Nei commenti riportati nella configurazione si utilizza la seguente terminologia:

- PORTE NON UTILIZZATE = porte alle quali non è stato collegato alcun dispositivo e che, per quanto detto in sezione 4, sono state portate down. Una configurazione minimale è stata fornita per queste porte per ridurre il lavoro di configurazione se fosse necessaria una attivazione.
- PORTE NON UTILIZZABILI = porte alle quali non è collegato alcun dispositivo e che non dovrebbero, secondo le specifiche, essere utilizzate in alcun modo. Per utilizzare queste porte è necessario dare una configurazione completa.

La descrizione data alle interfacce è stata stabilita arbitrariamente, la WWAS potrà poi modificarla a piacere.

```
service password-encryption
hostname Pisa-MDF-S1
enable secret cisco

banner motd #Switch WWAS Pisa-MDF-S1: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#

! LINEE
line con 0
password class
login
exit
line vty 0 15
password class
login
exit

! CONFIGURO VTP
vtp version 1
vtp domain wwas
vtp mode server
vtp password cisco
vtp pruning

! CREO LE VLAN
vlan 31
name GlobalVLAN_Pisa
exit
vlan 32
name ServerVLAN_Pisa
exit
vlan 33
name DominioDA_Pisa
```

```
exit
vlan 34
name DominioM_Pisa
exit
vlan 35
name DominioSS_Pisa
exit
vlan 36
name DominioRS1_Pisa
exit
vlan 37
name DominioRS2_Pisa
exit
vlan 38
name DominioRS3_Pisa
exit

! IMPOSTO LE BRIDGE PRIORITY PER STP
spanning-tree vlan 31 priority 4096
spanning-tree vlan 32 priority 4096
spanning-tree vlan 33 priority 4096
spanning-tree vlan 34 priority 4096
spanning-tree vlan 35 priority 4096
spanning-tree vlan 36 priority 8192
spanning-tree vlan 37 priority 8192
spanning-tree vlan 38 priority 8192
!

! IMPOSTO I DIAMETRI PER STP
spanning-tree vlan 31 root primary diameter 2
spanning-tree vlan 32 root primary diameter 2
spanning-tree vlan 33 root primary diameter 4
spanning-tree vlan 34 root primary diameter 4
spanning-tree vlan 35 root primary diameter 4
spanning-tree vlan 36 root primary diameter 4
spanning-tree vlan 37 root primary diameter 4
spanning-tree vlan 38 root primary diameter 4
!

! SNOOPING
ip dhcp snooping

! DISABILITO CDP
no cdp run

! INTERFACCE VERSO ALTRI SWITCH
interface FastEthernet0/1
description Collegamento con Pisa-IDF-sud-S1
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/2
description Collegamento con Pisa-IDF-sud-S2
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/3
description Collegamento con Pisa-IDF-sud-S3
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/4
description Collegamento con Pisa-IDF-nord-S1
switchport mode trunk
```

```
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/5
description Collegamento con Pisa-IDF-nord-S2
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/6
description Collegamento con Pisa-IDF-nord-S3
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/7
description Collegamento con Pisa-IDF-nord-S4
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/8
description Collegamento con Pisa-IDF-nord-S5
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/9
description Collegamento con Pisa-MDF-S3
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown
!
interface FastEthernet0/10
description Collegamento con Pisa-MDF-S4
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
no shutdown

! PORTE NON UTILIZZABILI
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
```

```
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown

! INTERFACCE VERSO SERVER GLOBALI
interface GigabitEthernet1/1
description Collegamento server-Web
switchport mode access
switchport access vlan 31
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/2
description Collegamento server-DNS
switchport mode access
switchport access vlan 31
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! INTERFACCE VERSO SERVER ENTERPRISE
interface GigabitEthernet1/3
description Collegamento server enterprise-Pisa-1
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/4
description Collegamento server enterprise-Pisa-2
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/5
description Collegamento server enterprise-Pisa-3
switchport mode access
switchport access vlan 32
switchport port-security
```

```
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/6
description Collegamento server enterprise-Pisa-4
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/7
description Collegamento server enterprise-Pisa-5
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/8
description Collegamento server enterprise-Pisa-6
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/9
description Collegamento server enterprise-Pisa-7
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface GigabitEthernet1/10
description Collegamento server enterprise-Pisa-8
switchport mode access
switchport access vlan 32
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! PORTE NON UTILIZZATE
interface GigabitEthernet1/11
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
```

```
!
interface GigabitEthernet1/12
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown

! SERVER DI WORKGROUP DOMINIO M
interface GigabitEthernet1/13
description Collegamento server workgroup-M-Pisa-1
switchport mode access
switchport access vlan 34
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! SERVER DI WORKGROUP DOMINIO RS1
interface GigabitEthernet1/14
description Collegamento server workgroup-RS1-Pisa-1
switchport mode access
switchport access vlan 36
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! PORTE NON UTILIZZATE
interface GigabitEthernet1/15
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/16
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/17
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/18
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
```

```
!
interface GigabitEthernet1/19
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/20
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/21
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/22
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/23
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface GigabitEthernet1/24
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown

! PORTE NON UTILIZZABILI
interface GigabitEthernet1/25
shutdown
!
interface GigabitEthernet1/26
shutdown
!
interface GigabitEthernet1/27
shutdown
!
interface GigabitEthernet1/28
shutdown
!
interface GigabitEthernet1/29
shutdown
```

```
!
interface GigabitEthernet1/30
shutdown
!
interface GigabitEthernet1/31
shutdown
!
interface GigabitEthernet1/32
shutdown
!
interface GigabitEthernet1/33
shutdown
!
interface GigabitEthernet1/34
shutdown
!
interface GigabitEthernet1/35
shutdown
!
interface GigabitEthernet1/36
shutdown
!
interface GigabitEthernet1/37
shutdown
!
interface GigabitEthernet1/38
shutdown
!
interface GigabitEthernet1/39
shutdown
!
interface GigabitEthernet1/40
shutdown
!
interface GigabitEthernet1/41
shutdown
!
interface GigabitEthernet1/42
shutdown
!
interface GigabitEthernet1/43
shutdown
!
interface GigabitEthernet1/44
shutdown
!
interface GigabitEthernet1/45
shutdown

! INTERFACCE VERSO Pisa-MDF-S2
interface GigabitEthernet1/46
description Collegamento con Pisa-MDF-S2
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
ip dhcp snooping trust
no shutdown
!
interface GigabitEthernet1/47
description Collegamento con Pisa-MDF-S2
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
ip dhcp snooping trust
no shutdown

! INTERFACCIA VERSO ROUTER PISA
interface GigabitEthernet1/48
description Collegamento con Router Pisa
switchport mode trunk
```

```
switchport trunk allowed vlan all
switchport nonegotiate
ip dhcp snooping trust
no shutdown
!

! INTERFACCE DI CONFIGURAZIONE
interface Vlan1
no ip address
shutdown
!
interface Vlan35
ip address 172.16.227.90 255.255.255.224
no shutdown
exit
!

end
```

D.3 Switch Pisa-IDF-nord-S1

Per questa configurazione esemplificativa si fanno le seguenti ipotesi:

- Sulle porte fastEthernet da 0/1 a 0/3 sono stati collegati computer del dominio Direzione e Amministrazione della sede di Pisa
- Sulle porte fastEthernet da 0/4 a 0/6 sono stati collegati computer del dominio Marketing della sede di Pisa
- Sulle porte fastEthernet da 0/7 a 0/8 sono stati collegati computer del dominio Supporto Sistemi della sede di Pisa
- Sulla porta fastEthernet 0/13 sia connesso un computer della funzione Ricerca e Sviluppo (primo gruppo di progetto)
- Sulla porta fastEthernet 0/14 sia connesso un computer della funzione Ricerca e Sviluppo (secondo gruppo di progetto)
- Sulla porta fastEthernet 0/15 sia connesso un computer della funzione Ricerca e Sviluppo (terzo gruppo di progetto)

Si suppone inoltre che la versione del sistema operativo di networking dello switch sia tale da:

- Utilizzare come incapsulamento di default (per link di tipo trunk) l'incapsulamento 802.1Q.
- Associare allo switch una Bridge Priority di default pari a 32768 (per ogni VLAN).

Nei commenti riportati nella configurazione si utilizza la seguente terminologia

- PORTE NON UTILIZZATE = porte alle quali non è stato collegato alcun dispositivo e che, per quanto detto sopra, sono state portate down. Una configurazione minimale è stata fornita per queste porte per ridurre il lavoro di configurazione se fosse necessaria una attivazione.
- PORTE NON UTILIZZABILI = porte alle quali non è collegato alcun dispositivo e che non dovrebbero, secondo le specifiche, essere utilizzate in alcun modo. Per utilizzare queste porte è necessario dare una configurazione completa.

Nel dare la descrizione alle interfacce connesse a macchine client si è utilizzata la seguente sintassi:

```
description Collegamento con PC-XX-YY-Z
```

dove:

- XX è il numero della stanza che contiene il PC
- YY è il dominio di sicurezza / gruppo di lavoro a cui appartiene la macchina
- Z è il numero (sequenziale) della macchina nel proprio dominio

```
service password-encryption
hostname Pisa-IDF-nord-S1
enable secret cisco

banner motd #Switch WWAS Pisa-IDF-nord-S1: l'accesso e'
vietato ai non autorizzati, ogni
abuso e' legalmente perseguibile#

! LINEE
line con 0
password class
login
exit
line vty 0 15
password class
login
exit

! CONFIGURO VTP
vtp version 1
```

```
vtp domain wwas
vtp mode client
vtp password cisco

! LE VLAN VERRANNO IMPORTATE DAL VTP SERVER

! UTILIZZO PRIORITÀ DI DEFAULT PER STP

! I DIAMETRI SI IMPOSTANO SOLO SUL ROOT BRIDGE

! SNOOPING
ip dhcp snooping

! DISABILITO CDP
no cdp run

! INTERFACCE VERSO MACCHINE CLIENT
interface FastEthernet0/1
description Collegamento con PC-13-DA-1
switchport mode access
switchport access vlan 33
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/2
description Collegamento con PC-13-DA-2
switchport mode access
switchport access vlan 33
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/3
description Collegamento con PC-13-DA-3
switchport mode access
switchport access vlan 33
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/4
description Collegamento con PC-13-M-1
switchport mode access
switchport access vlan 34
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/5
description Collegamento con PC-13-M-2
switchport mode access
switchport access vlan 34
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
```

```
no shutdown
!
interface FastEthernet0/6
description Collegamento con PC-13-M-3
switchport mode access
switchport access vlan 34
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/7
description Collegamento con PC-14-SS-1
switchport mode access
switchport access vlan 35
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/8
description Collegamento con PC-14-SS-2
switchport mode access
switchport access vlan 35
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! PORTE NON UTILIZZATE
interface FastEthernet0/9
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface FastEthernet0/10
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface FastEthernet0/11
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface FastEthernet0/12
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
```

```
shutdown

! INTERFACCE VERSO MACCHINE CLIENT
interface FastEthernet0/13
description Collegamento con PC-15-RS1-1
switchport mode access
switchport access vlan 36
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/14
description Collegamento con PC-15-RS2-1
switchport mode access
switchport access vlan 37
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown
!
interface FastEthernet0/15
description Collegamento con PC-15-RS3-1
switchport mode access
switchport access vlan 38
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
no shutdown

! PORTE NON UTILIZZATE
interface FastEthernet0/16
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface FastEthernet0/17
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown
!
interface FastEthernet0/18
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
spanning-tree portfast
shutdown

! PORTE NON UTILIZZABILI
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
```

```
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!

! INTERFACCIA VERSO Pisa-MDF-S1
interface FastEthernet0/23
description Collegamento con Pisa-MDF-S1
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
ip dhcp snooping trust
no shutdown

! INTERFACCIA VERSO Pisa-MDF-S2
interface FastEthernet0/24
description Collegamento con Pisa-MDF-S2
switchport mode trunk
switchport trunk allowed vlan all
switchport nonegotiate
ip dhcp snooping trust
no shutdown

! INTERFACCE DI CONFIGURAZIONE
interface Vlan1
no ip address
shutdown
!
interface Vlan35
ip address 172.16.227.80 255.255.255.224
no shutdown
exit
!

end
```