M.Nanni – F.Tinarelli – S.Tubertini

Le VLAN dell'Area di Ricerca di Bologna

IRA 340/03

Introduzione

La rete di trasmissione dati dell'Area della Ricerca di Bologna e' stata disegnata nei primi anni 90 partendo da un progetto che prevedeva una struttura articolata su piu' livelli. E' stata predisposta una dorsale primaria in fibra ottica, in grado di collegare i quattro edifici che costituiscono il campus, sono presenti dorsali di secondo livello, interne ai singoli edifici, per connettere gli armadi di concentrazione degli istituti, ed infine e' stato realizzato un sistema di cablaggio strutturato che, a partire dagli armadi di concentrazione, raggiunge tutti i laboratori e gli uffici dell'Area.

Gli apparati attivi presenti nel progetto originale mettevano a disposizione una banda di 100 Mbit/sec sulla dorsale primaria (concentratori ottici FDDI) e offrivano una velocita' di 10 Mbit/sec negli uffici e laboratori (bridge e hub Ethernet).

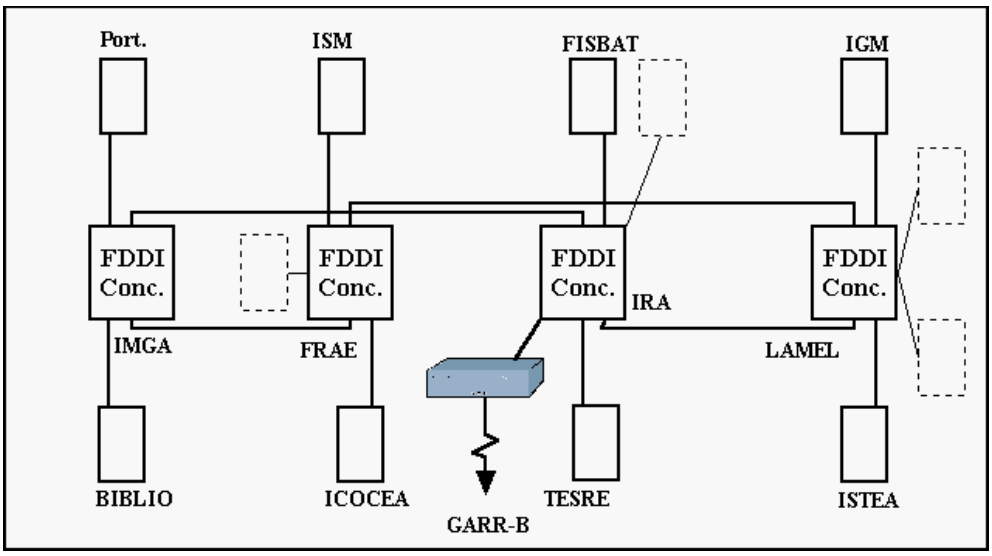


Figura 1

La struttura della Figura 1 e' stata attiva nell'Area della Ricerca di Bologna dal 1993 al 2001 quando, su proposta della Commissione Informatica e con finanziamenti su capitoli centralizzati CNR, sono stati sostituiti gli apparati attivi. Si e' arrivati cioe' ad una situazione come quella descritta nella **Tavola-A** (in appendice), dove i concentratori FDDI sono stati sostituiti da Switch Matrix "E5" e ogni istituto dispone nei propri armadi di uno o piu' Switch "VH-24" connessi ai Matrix della dorsale attraverso collegamenti in fibra ottica.

La realizzazione della nuova dorsale, basata su dispositivi Giga Ethernet, ha consentito di adeguare la velocita' di trasmissione alle attuali esigenze degli Istituti e di contenere i costi di manutenzione attraverso l'eliminazione di apparati ormai obsoleti. Attualmente, la rete di Area dispone di una banda a 1GB sulla dorsale e a 10/100/1000 MB negli Istituti.

Ma se questa operazione ha rappresentato un miglioramento notevole per quello che riguarda la pura capacita' trasmissiva, dal punto di vista logico la struttura conserva la stessa topologia della LAN progettata negli anni 90. L'intera rete di Area viene cioe' vista come un'unica grande rete locale indifferenziata su cui sono collocate le macchine degli istituti, e non vi e' modo di distinguere e/o separare ad esempio le macchine poste in Biblioteca da quelle dell'istituto IMM, . anche se possiedono classi di indirizzi di rete IP differenti.

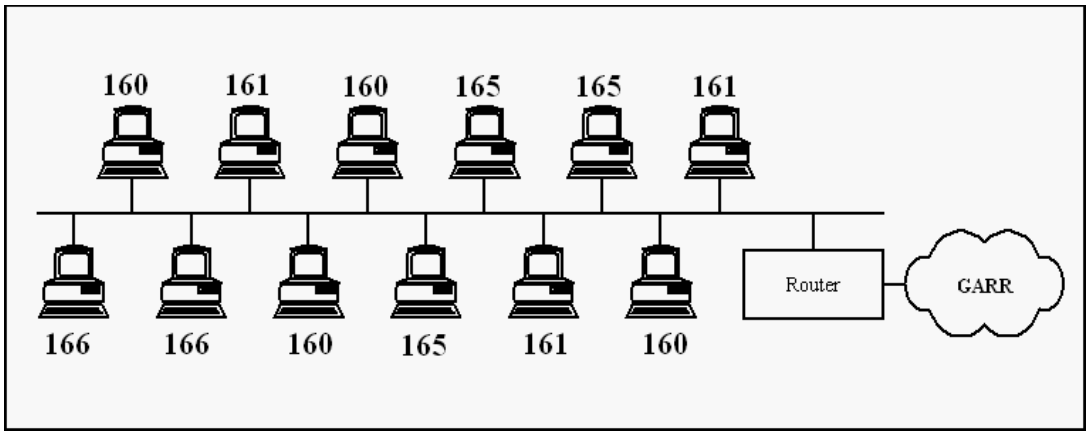


Figura 2

Questa situazione presenta l'indiscusso vantaggio di poter spostare una macchina in qualunque punto della rete senza doversi minimamente preoccupare dell'indirizzo IP, della configurazione del router e della visibilita' della macchina in Windows, ma proprio per garantire queste funzionalita' il traffico di controllo (broadcast) generato da ogni personal computer o apparato deve potersi propagare in tutti i rami della rete. Considerando che i sistemi presenti nell'Area sono ormai un migliaio, il traffico di controllo generato iniziava a rappresentare un fastidioso rumore di fondo presente in ogni ramo della rete.

Il contenimento del traffico di broadcast e' stata la ragione principale per cui la Commissione Informatica di Area ha iniziato a studiare l'opportunita' di separare le reti dei differenti Istituti utilizzando la tecnica delle Vlan.

Le Vlan

Gli switch "Matrix" e "Vertical Horizon" installati sulla dorsale e negli istituti supportano il protocollo 802.1Q che permette di realizzare le "**reti locali virtuali**" (VLAN), cioe' mostrare i differenti dispositivi (stazioni di lavoro, server etc) come se facessero parte di reti locali fisicamente separate. e in grado di comunicare tra di loro unicamente attraverso un router.

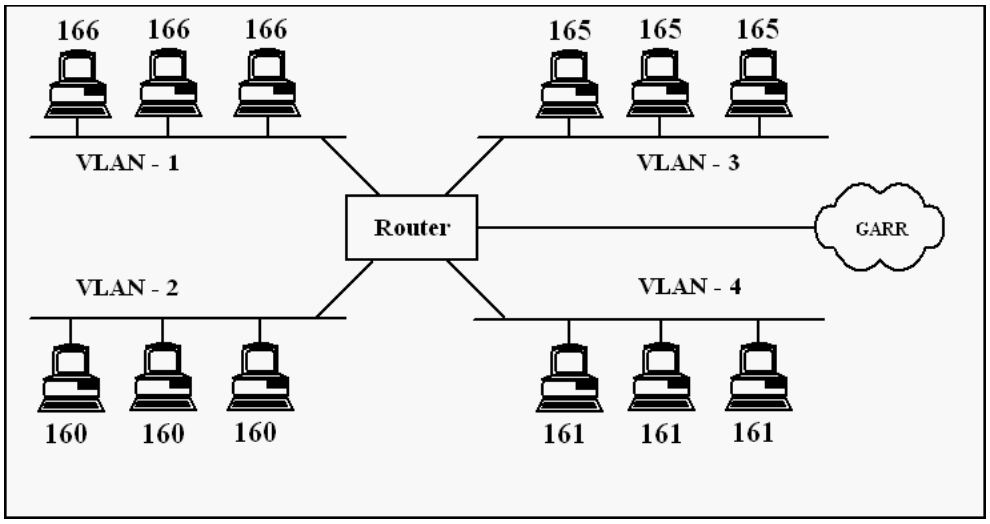


Figura 3

Gli switch e gli apparati utilizzati nella realizzazione di Vlan sono estremamente versatili nel permettere di associare i dispositivi alle diverse reti virtuali. Possono appartenere alla stessa Vlan stazioni di lavoro connesse a switch collocati agli estremi della dorsale o, al contrario, due porte dello stesso switch possono essere assegnate a Vlan diverse.

La comunicazione tra macchine appartenenti a Vlan diverse avviene unicamente attraverso il router, e questo porta a miglioramenti dal punto di vista delle prestazioni, versatilita' e sicurezza sull'intera rete.

Vantaggi offerti dalle Vlan

- **Confinamento del traffico di broadcast.** Il traffico di broadcast rimane confinato all'interno delle singole Vlan in quanto non puo' essere propagato attraverso il router. Questo porta, oltre ad un minor impegno di banda in assoluto, ad una minore sollecitazione delle interfacce di rete dei calcolatori e quindi ad una generale diminuzione dei tempi di latenza dei servizi.
- **Servizi indipendenti.** All'interno delle singole Vlan e' possibile realizzare specifici servizi (Bootp, DHCP etc) definendo quindi differenti politiche di sicurezza rispetto ai numeri che vengono assegnati dinamicamente. Questa possibilita' permette tra l'altro di assoggettare a regole particolari i numeri IP assegnati in aree pubbliche (Biblioteca, sale convegni, regioni wi-fi etc). Inoltre i servizi basati su protocolli non-IP (Netbeui, Novel-IPX, Mac) saranno visibili solo all'interno della Vlan.
- **Nat e reti nascoste.** Per ogni Vlan vi e' la possibilita' di utilizzare in modo autonomo e indipendente le reti nascoste (10.0.0.0, 192.168.0.0 etc) per servizi, apparecchiature scientifiche e per creare isole di stazioni di lavoro protette da NAT; si e' riscontrato pero' che alcuni protocolli di comunicazione utilizzati dalle stampanti HP non vengono filtrati e passano liberamente attraverso le Vlan.
- **Controllo sui numeri IP assegnati.** All'interno di una Vlan si possono utilizzare solo gli indirizzi IP assegnati al singolo istituto. Cio' limita la possibilita' di configurare erroneamente macchine con i numeri IP assegnati ad altri e facilita quindi la ricerca e l'individuazione di macchine con traffico anomalo.

Per contro la realizzazione di una Vlan comporta un impegno organizzativo e di gestione e porta ad una struttura piu' rigida.

Svantaggi delle Vlan

- **Maggiore rigidita' nella configurazione degli apparati.** La definizione delle differenti VLAN richiede una fase di analisi sulla disposizione fisica dei singoli servizi di rete e delle stazioni di lavoro e la conseguente configurazione degli apparati. La sostituzione di dispositivi e l'inserimento di nuovi servizi richiede quindi un maggior lavoro che puo' anche comportare temporanea assenza di connettivita'.
- **Minore visibilita' dei servizi.** I servizi Windows che si trovano su una Vlan differente dalla propria non sono piu' visibili con il semplice "sfoglia la rete". Si puo' comunque ricercare il server che li ospita con la funzione "trova" indicando il nome completo o il numero IP. I servizi basati su protocolli diversi dall'IP non sono piu' visibili.
- **Duplicazione dei servizi centralizzati.** Nel caso di servizi basati su Bootp e DHCP ogni istituto dovra' provvedere in proprio a dotarsi di opportuni server in quanto non e' possibile utilizzare server che si trovano su altre Vlan.

- **Minore flessibilita' nel monitoraggio.** Il monitoraggio del traffico sulle singole reti non puo' piu' essere realizzato in modo centralizzato, ma deve essere effettuato su ogni singola Vlan.

Le Vlan dell'Area di Ricerca di Bologna

Nella definizione del disegno delle Vlan dell'Area della Ricerca di Bologna sono stati presi in esame la disposizione fisica degli istituti, i numeri di rete IP tradizionalmente utilizzati, le capacita' del router di Area di gestire VLAN ed il numero di porte Ethernet di cui e' dotato, oltre ovviamente alle caratteristiche tecniche degli switch presenti sulla dorsale e negli Istituti.

La prima operazione e' stata quella di definire il numero di Vlan che sarebbe stato conveniente assegnare all'interno dell'Area di Bologna, e questo dipende dalle reti IP in uso e dalla dislocazione fisica di istituti e reparti. Tradizionalmente, a ogni istituto/sezione o servizio sono state assegnate almeno una rete IP pubblica (cioe' visibile sull'Internet globale) e una rete IP privata, non visibile da Internet ma accessibile soltanto dall'interno del campus. Altre reti pubbliche (192.168.0.0 e 10.0.0.0) possono essere utilizzate dai singoli Istituti ma non avranno visibilita' esterna, sara' anzi compito dello stesso Istituto realizzare (o richiedere sul router) il "gateway" con le altre reti in uso all'interno dell'Istituto.

La scelta e' stata quella di assegnare una Vlan per Istituto (o sezione); sono state assegnate inoltre una Vlan per la Biblioteca e una per i Servizi Informatici di Area . E' stata riproposta cioe' la scelta fatta dieci anni fa nell'assegnazione delle reti IP, che ha dato buoni risultati e che e' riassunta nella tabella seguente:

Sezione/Istituto	**Rete IP pubblica**	**Rete IP privata**	**Edificio**	**VLAN**
AREA	192.167.160.0	192.168.160.0	1 (Esa)	**10**
BIBLIOTECA	192.167.161.0	192.168.161.0	1 (Esa)	**12**
ISOF	192.167.162.0	192.168.162.0	2 (Sud)	**4**
	192.167.163.0	192.168.163.0	2 (Sud)	**4**
ISMN	192.167.164.0	192.168.164.0	2 (Sud)	**8**
IRA	192.167.165.0	192.168.165.0	3 (Centrale)	**3**
IASF	192.167.166.0	192.168.166.0	3 (Centrale)	**7**
ISAC	192.167.167.0	192.168.167.0	3 (Centrale)	**6**
	192.167.171.0	192.168.171.0	1 (Esa)	**6**
ISMAR	192.167.168.0	192.168.168.0	4 (Nord)	**9**
IBIMET	192.167.169.0	192.168.169.0	4 (Nord)	**11**
IMM	192.167.170.0	192.168.170.0	4 (Nord)	**5**

Un elemento da tenere in considerazione e' la topologia della rete fisica dell'Area della Ricerca, che deriva dall'anello FDDI del disegno degli anni 90. Questo comporta che presso il centro calcolo del'IRA, dove e' installato il router di Area, arrivino 4 coppie di fibre che trasportano rispettivamente il traffico complessivo degli edifici a Sud, il traffico complessivo dell'edificio a Nord e il collegamento degli istituti ISAC e IASF. Il router dispone di 8 porte Ethernet a 100 Mbit/sec per il collegamento "interno", e porte ATM per il collegamento verso il Garr. Si e'valutato che la scelta piu' efficiente fosse quella di utilizzare 5 porte del router realizzando un "collegamento

virtuale diretto" tra ogni fibra in arrivo e una porta del router. In questo modo, considerando i 4 collegamenti piu' l' accesso dell'IRA, si dispone sul router di un troughtput totale di 500Mbit/sec.

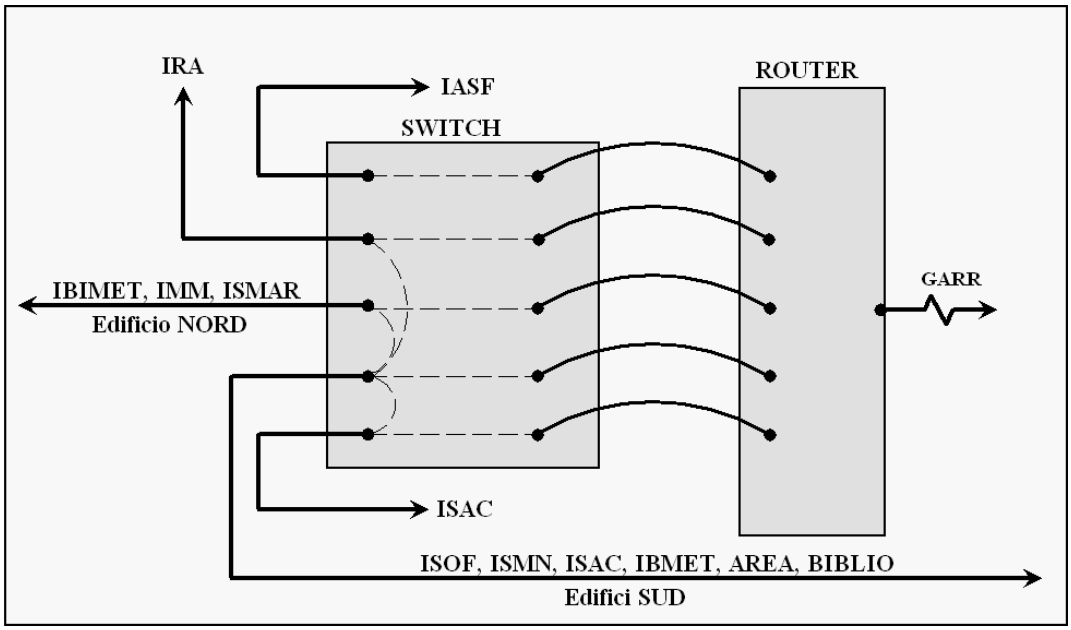


Figura 4

Le tecniche di Vlan permettono di realizzare questi collegamenti diretti virtuali tra le porte in arrivo sullo switch ed una corrispondente porta del router. Se si volessero ottenere solo 5 Vlan, una per ogni porta in ingresso, sarebbe sufficiente configurare questo switch centrale in modo "statico".

Nel nostro caso pero' vogliamo ottenere 11 Vlan, una per ogni istituto piu' i servizi. Come si puo' vedere dalla **Tavola-B** (in appendice), che mostra la dislocazione delle differenti Vlan nell'Area, abbiamo 3 diverse Vlan nell'edificio Nord e 6 negli edifici a Sud. Inoltre abbiamo alcuni casi particolari:

- l'IBIMET e' presente nell'edificio Nord e nell'edificio ESA;
- l' ISAC e' presente nell'edificio centrale e nell'ESA e ha una macchina presso l'IRA;
- l'AREA .ha i server presso l'IRA ed e' presente presso l'ESA.

Quindi una semplice configurazione statica dello switch centrale non era sufficiente, ed e' stato necessario agire anche su altri apparati della dorsale. Inoltre anche il router deve essere in grado di gestire le Vlan. Analizzando gli indirizzi IP di destinazione dei pacchetti il router non deve solo scegliere la corretta porta Ethernet di uscita, ma deve anche inserire il "tag" relativo alla Vlan a cui la rete IP appartiene.

La configurazione degli apparati

Nella configurazione degli apparati si e' scelto di intervenire sul minor numero di switch e di porte, al fine di evitare inutili complicazioni. Si e' preferito quindi, per quanto possibile, configurare le porte degli apparati che appartengono alla dorsale piuttosto che gli apparati periferici. Grazie a questa scelta, la maggioranza degli switch utilizzati dagli Istituti dell'Area non ha richiesto alcuna particolare configurazione per quello che riguarda le Vlan.

La **Tabella-1** descrive la configurazione delle porte sugli apparati di rete. I rami di rete ed i sistemi che si trovano a valle delle porte configurate su una particolare Vlan verranno a far parte di quella specifica rete privata virtuale.

TABELLA 1: CONFIGURAZIONE DELLE PORTE SUGLI APPARATI DI RETE

Matrix IRA

Interfaccia	Porta	Connessa a	VLAN	Tagged/Untagged
Giga-1	3	VHorizon IASF-1	7	UNTAGGED
Giga-1	4	VHorizon ISAC-2	6	UNTAGGED
Giga-1	6	VHorizon ISAC-1	6	UNTAGGED
Giga-2	3	Matrix IMM	5,11	TAGGED
Giga-2	4	Matrix ISOF	4,6,8,10,11,12	TAGGED
Giga-2	6	VHorizon IRA-1	3,4,5,6,7,8,9,10,11,12	TAGGED
10/100 48P-2	26	JRouter porta 1	4,8,10,12	TAGGED
10/100 48P-2	28	JRouter porta 2	5,9,11	TAGGED
10/100 48P-2	30	JRouter porta 3	7	TAGGED
10/100 48P-2	32	JRouter porta 4	6	TAGGED
10/100 48P-2	34	JRouter porta 5	3	TAGGED

Matrix IMM

Interfaccia	Porta	Connessa a	VLAN	Tagged/Untagged
Giga-1	3	Matrix IRA	5,9,11	TAGGED
Giga-1	4	VH ISMAR-2	9	UNTAGGED
Giga-1	5	VH ISMAR-1	9	UNTAGGED
Giga-1	6	VH IBIMET-1	11	UNTAGGED
Giga-2	3	VH IMM-2	5	UNTAGGED
Giga-2	4	VH IMM-1	5	UNTAGGED

Matrix ISOF

Interfaccia	Porta	Connessa a	VLAN	Tagged/Untagged
Giga-1	3	Matrix IRA	4,6,8,10,11,12	TAGGED
Giga-1	4	VH ESA-1	10,11,12	TAGGED
Giga-1	5	VH ESA-2 (ISAC ex IMGA)	6,10	TAGGED
Giga-2	3	VH ISOF-1	4	UNTAGGED
Giga-2	4	VH ISMN-1	8	UNTAGGED
Giga-2	5	VH ISOF ex ICoCEA-1	4	UNTAGGED

VHorizon ESA-1

Porta	Connessa a	VLAN	Tagged/Untagged
24	VHorizon ESA-3	4000-TRUNK	TAGGED
25	Matrix ISOF	4000-TRUNK	TAGGED
26	VH BIBLIO-1	12	UNTAGGED

VHorizon ESA-2

Porta	Connessa a	VLAN	Tagged/Untagged
25	Matrix ISOF	4000-TRUNK	TAGGED
26	VH PORTINERIA-1	10	UNTAGGED

VHorizon ESA-3

Porta	Connessa a	VLAN	Tagged/Untagged
1-12	IBIMET	11	UNTAGGED
13-23	AREA	10	UNTAGGED
24	VH ESA-1	4000-TRUNK	TAGGED

VHorizon IRA-1

Su questo switch sono state riservate 10 porte (UNTAGGED) alle 10 VLAN esistenti sulla rete di Area: le porte vengono utilizzate sia per il monitoraggio della rete, sia per la connessione al router di backup in caso di emergenza.
La porta 25 (collegamento alla dorsale) e' TRUNK ENABLED per permettere il transito di piu' Vlan.

La **Tabella-2** illustra invece la configurazione delle porte sul router Juniper.

TABELLA 2: CONFIGURAZIONE DELLE PORTE SUL ROUTER JUNIPER

Porta	Connessa a	VLAN	Tagged/Untagged
JRouter porta 1	Matrix IRA 48P2 - porta 26	4,8,10,12	TAGGED
JRouter porta 2	Matrix IRA 48P2 - porta 28	5,9,11	TAGGED
JRouter porta 3	Matrix IRA 48P2 - porta 30	7	TAGGED
JRouter porta4	Matrix IRA 48P2 - porta 32	6	TAGGED
JRouter porta5	Matrix IRA 48P2 - porta 34	3	TAGGED

Piano di emergenza in caso di guasto del router

Come si e' gia' fatto presente, la realizzazione di una VLAN impone una maggiore rigidita' alla struttura di rete e rende piu' complessa la sostituzione degli apparati, e del router in particolare. Se, nella precedente situazione, a fronte di un guasto del router Juniper si poteva prevedere una sostituzione temporanea con altri apparati, oggi questo richiederebbe anche la completa deconfigurazione di tutte le VLAN dell'Area.

Data la disponibilita' del vecchio router di Area (Cisco 4700) che, anche se obsoleto, e'ancora funzionante, e' stato preparato un piano per ripristinare una situazione in cui, con un intervento minimo, si possa garantire la connettivita' dell'Area.

Poiche' il vecchio router e' dotato di 6 porte Ethernet e non riesce a gestire differenti Vlan sulla stessa porta, il piano di emergenza prevede di accorpare differenti reti virtuali secondo lo schema della **Tavola-C** (in appendice).
Sul sito web di Area, all' indirizzo *http://www.bo.cnr.it/servinfo/Comminf/vlan-conf/piano-di-emergenza.htm,* si possono trovare le istruzioni dettagliate sul modo di procedere per realizzare il collegamento dell'Area di Ricerca alla rete Garr attraverso il vecchio router Cisco.

INDICE DELLE TAVOLE

TAVOLA "A"
Topologia della rete di Area

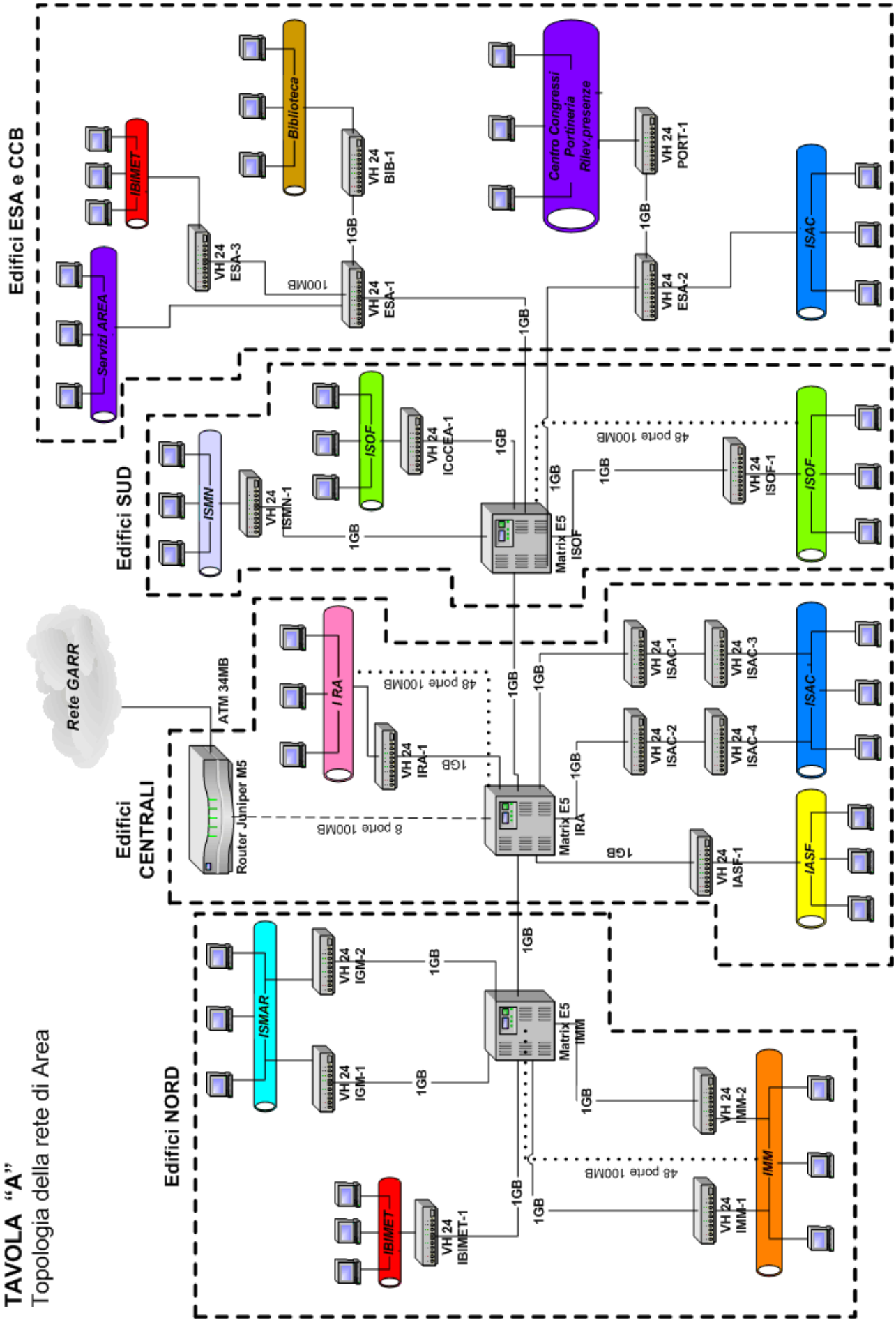


TAVOLA "B"
Configurazione delle VLAN

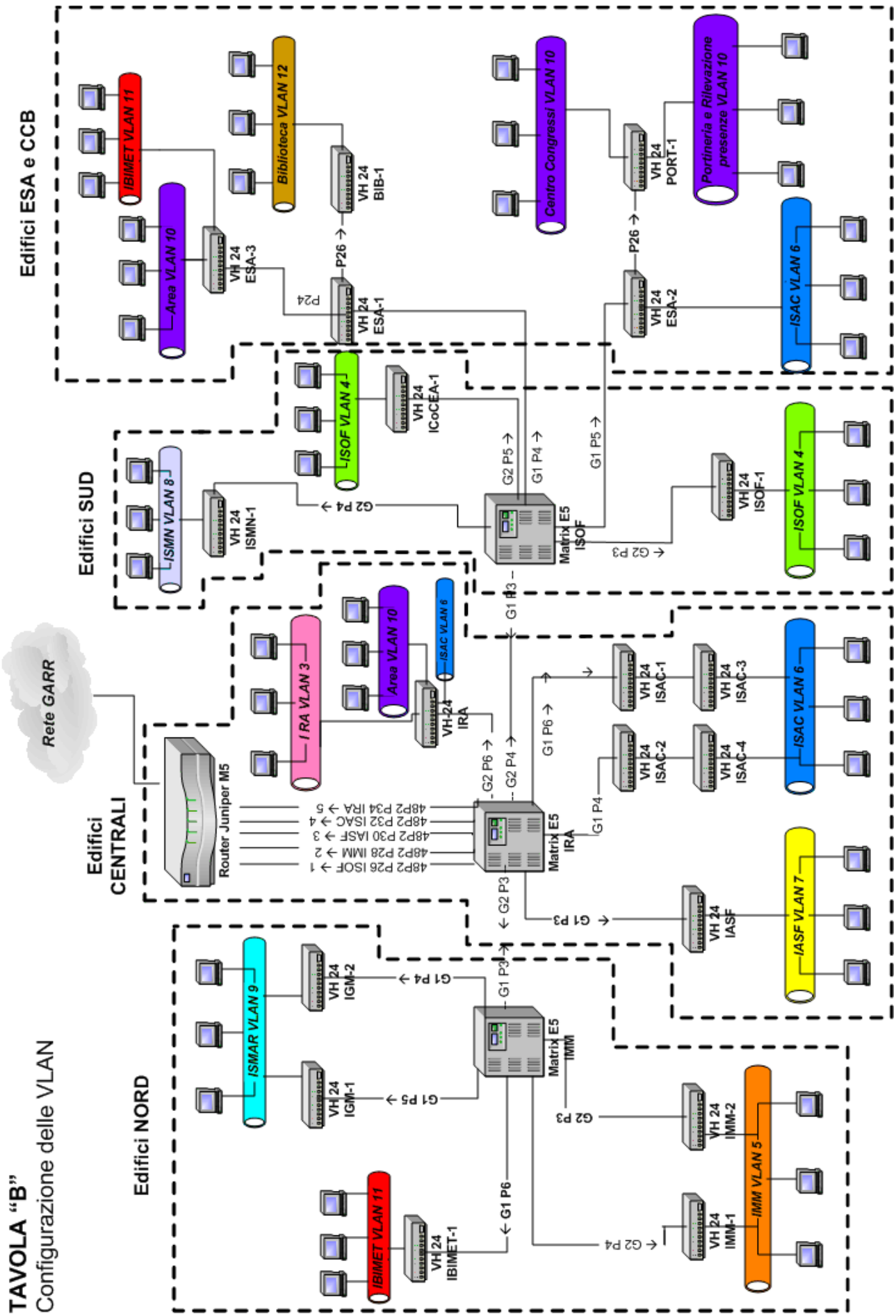
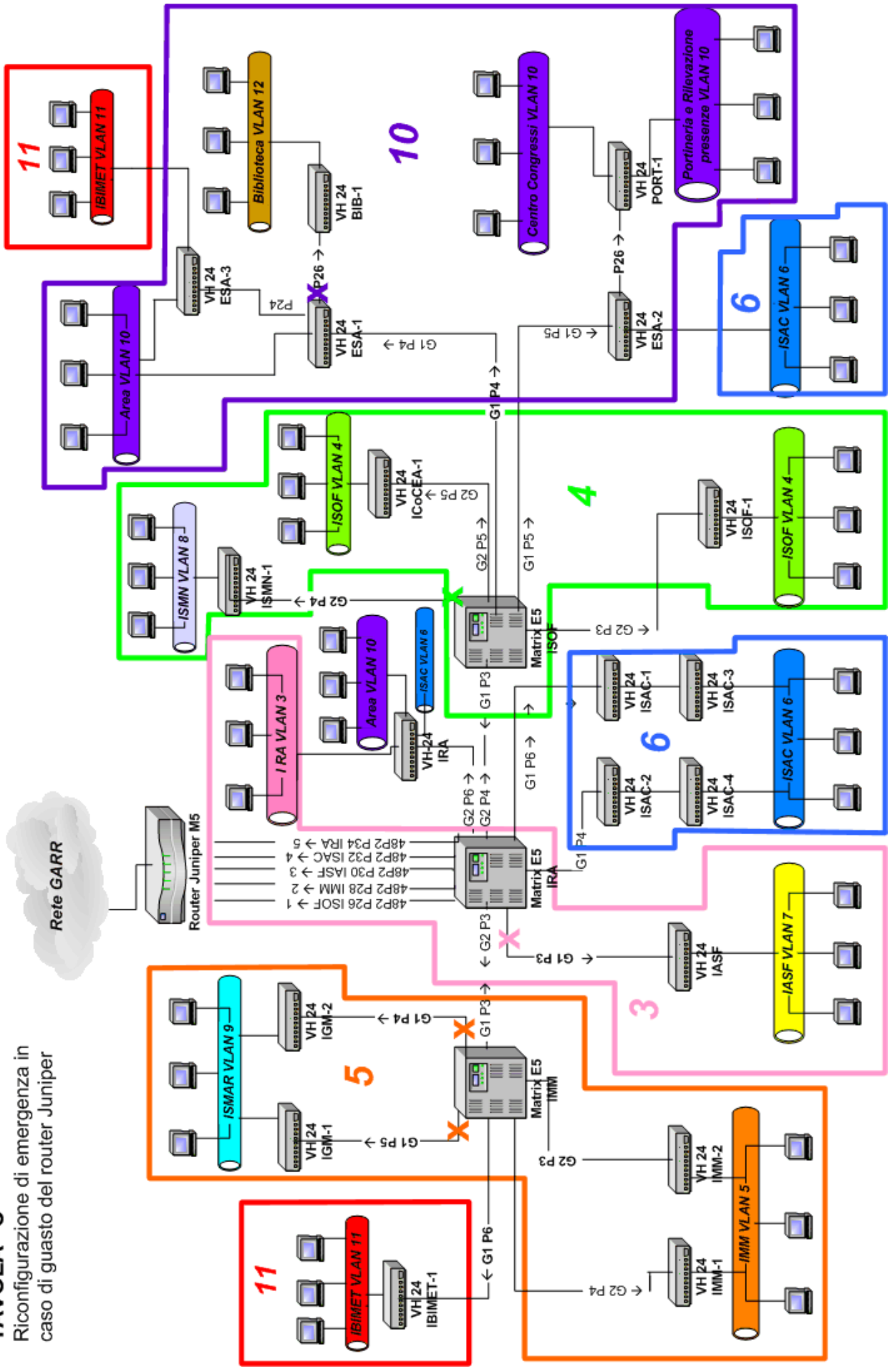


TAVOLA "C"
Riconfigurazione di emergenza in caso di guasto del router Juniper



Questo rapporto tecnico, in versione PDF, e' disponibile in rete all'indirizzo
http://www.bo.cnr.it/servinfo/Comminf/vlan-rapp-interno.pdf