SOLUZIONE

Premessa e ipotesi aggiuntive

L'analisi del testo contiene qualche ambiguità che deve essere ben specificata.
La più evidente è che non è stato specificato quali servizi tale rete deve fornire pubblicamente, pur richiedendo scambio di informazioni pubbliche (dalla frase «progetto transnazionale»).
Date le richieste del testo, si decide di rendere i seguenti servizi pubblici tramite la rete:

1. scambio di documenti del progetto «transnazionale», documenti in gestione ai due laboratori;
2. sito Web del progetto «transnazionale», in carico ai due laboratori;
3. scambio di documenti amministrativi del progetto «transnazionale» a cura degli uffici amministrativi.

Nulla è specificato per il servizio di posta elettronica, anch'esso necessario per lo scambio di informazioni pubbliche circa il progetto «transnazionale», pertanto si decide di utilizzare un servizio di posta elettronica gestito dall'esterno e non internamente come i suddetti.

Infine l'accenno a un'eventuale rete preesistente, nella sua vaghezza, è un'indicazione che si decide di escludere dallo svolgimento.

Per sufficiente genericità si decide di riferirsi al progetto prescindendo dal sistema operativo server adottato, ovvero dal sistema operativo che gestisce utenti, routing e servizi. Per quanto possibile si daranno indicazioni circa entrambi i sistemi operativi più diffusi, Microsoft Windows Server (2000/2003) e Linux.

Per quanto assunto sia dal testo sia dalle ipotesi aggiuntive, verrà adottato un modello di rete comprendente una rete locale isolata (TRUST), una rete locale perimetrale (DMZ) e una porzione di rete pubblica (INTERNET) servita da un collegamento DSL flat a 2Mbit/s in ingresso e in uscita.

Progettazione Livelli 1 e 2 OSI

Per quanto riguarda la rete TRUST, vengono immessi in questa rete gli elaboratori degli uffici (in tutto 10, come dal testo), gli elaboratori della Presidenza e Vicepresidenza (2), della Biblioteca (4) e dei due laboratori (10). In tutto 26 calcolatori, ovvero 26 host.

Il livello Fisico e Dati (OSI 1 e 2) delle connessioni viene realizzato in tecnologia Ethernet 802.3u (FastEthernet 10/100/1Gb/s) secondo il modello di rete «switched».

Nessun dato prevede tratte superiori ai 90m classici per la portata del mezzo 100BaseT, quindi nessuna assunzione particolare viene fatta in merito.

Vengono considerati i seguenti domini di collisione da mantenere separati tramite switch:

a. uffici + Presidenza-Vicepresidenza;
b. biblioteca;
c. laboratori.

La scelta è stata fatta in base alla qualità del traffico circolante sui relativi segmenti di rete locale.

Il dominio **a.** sarà connesso con 2 switch (in cascata) a 8 porte per i 10 host.
Il dominio **b.** sarà connesso con 1 switch a otto porte per i 4 host.
Il dominio **c.** sarà connesso con 2 switch (in cascata) a 8 porte per i 10 host.

Le tre porte di upload dei tre domini convergeranno su uno switch «stella» (a 8 porte) per ottenere la completa interconnessione delle macchine. Tale switch sarà contenuto in adeguato armadio di commutazione dotato di gruppo di continuità e quanto necessario.

Per quanto riguarda la rete DMZ, la scelta ricade di nuovo su Ethernet 802.3u, con un solo switch a 8 porte. Su questa rete, accessibile pubblicamente, saranno disposte le macchine server di servizi pubblici, come descritto nella premessa.

La porzione di rete pubblica INTERNET invece è costituita dal modem/router DSL che riceve in ingresso dalla rete pubblica geografica il segnale DSL con le caratteristiche offerte dal provider (ISP) e si affaccia sulla rete scolastica tramite una connessione Ethernet 802.3u.

Progettazione Livello 3 OSI e Servizi di rete

Le interconnessioni delle tre reti previste dal progetto, TRUST, DMZ e INTERNET, avviene con un router opportunamente dislocato. Per semplicità consideriamo un router costituito da un elaboratore PC con tre interfacce di rete: una sulla rete TRUST, una sulla rete DMZ, una verso la rete INTERNET (cioè verso il modem DSL).

Il modello di riferimento per il livello 3 è IP dello stack TCP/IP della rete omonima.

I servizi di rete necessari per tale progetto sono:

- Servizio di Dominio per consentire l'accesso con autenticazione agli utenti sulla rete.
- Servizio DHCP per permettere la configurazione automatica degli host della rete TRUST.
- Servizio di Firewall, per impedire accessi dall'esterno sulla rete TRUST e accessi indesiderati sulla rete DMZ.
- Servizio di NAT, in particolare sNAT per consentire agli host della rete TRUST di accedere ai servizi pubblici standard (HTTP, POP3, SMTP, FTP, NNTP).
- Servizio di NAT, in particolare dNAT, per rendere raggiungibili dall'esterno gli host sulla rete DMZ.
- Servizio DNS privato per consentire la risoluzione dei nomi interna alla rete TRUST e DMZ.
- Servizio di Condivisione disco e stampanti (NBT) per consentire la condivisione di spazi disco e stampanti all'interno delle reti TRUST e DMZ.
- Servizio FTP pubblico (come da premessa).
- Servizio HTTP pubblico (come da premessa).
- Servizio di DNS pubblico per risolvere i nomi pubblici della rete Internet mondiale.

Tutti questi servizi saranno dislocati su macchine server individuate sulla rete.

Schema di indirizzamento (livello 3 OSI)

Dati i presupposti, si vengono a determinare due sottoreti isolate (TRUST e DMZ) su cui distribuire un pool di indirizzi.

Viene deciso di usare la classe di indirizzi dedicata alle reti isolate e previste dal modello IP 192.168.0.0 e un subnetting con 4 bit per le sottoreti, sui 16 a disposizione dal modello.

In questo caso la notazione è 192.168.0.0/20 o netmask 255.255.240.0.

Questo modello consente 2^4 subnet differenti, ognuna con 2^12 host indirizzabili (in realtà sarebbero 2^12-2 host indirizzabili, dato che il primo e l'ultimo indirizzo della subnet sono riservati alla subnet stessa e al broadcast).

Lo schema scelto è ridondante, dato che le subnet reali sono solo 2 (TRUST e DMZ): 14 subnet rimangono inutilizzate.

Assegniamo quindi la subnet 192.168.0.0 alla rete TRUST.

Assegniamo poi la subnet 192.168.16.0 alla rete DMZ.

La rete TRUST avrà a disposizione quindi gli indirizzi 192.168.0.1 – 192.168.0.254; 192.168.1.1 – 192.168.1.254; 192.168.2.1 – 192.168.2.254; ecc. fino a 192.168.15.1 – 192.168.15.254.

In totale: 254*16 = 4064 indirizzi utilizzabili.

La rete DMZ avrà a disposizione quindi gli indirizzi 192.168.16.1 – 192.168.16.254; 192.168.17.1 – 192.168.17.254; 192.168.18.1 – 192.168.18.254; ecc. fino a 192.168.31.1 – 192.168.31.254.

In totale: 254*16 = 4064 indirizzi utilizzabili.

(Per conferma, verificare che tutti gli indirizzi possibili della rete TRUST in AND con la netmask danno sempre 192.168.0.0, mentre tutti gli indirizzi possibili per la rete DMZ in AND con la netmask danno come risultato 192.168.16.0).

Dislocazione dei servizi e routing (livello 7 e 3 OSI)

Per una corretta e bilanciata dislocazione dei servizi è necessario aggiungere al progetto almeno tre macchine server:

a. un server router (SR) con interfacce sulle reti TRUST, DMZ e INTERNET;

b. un server locale di sistema (PDC) con interfaccia sulla rete TRUST;
c. un server pubblico di servizio (SP) con interfaccia sulla rete DMZ.

A questo punto si possono dislocare i servizi elencati precedentemente.
Sul server SR saranno collocati: Routing, Firewall, NAT, eventuale Proxy.
Questo server deve:

1. fare sNAT per tutte le macchine ir
2. fare dNAT per le macchine su DM
3. bloccare il traffico proveniente dal
4. controllare il traffico proveniente d
5. consentire il traffico tra TRUST e I
6. DNS.

Sul server PDC sono collocati i servi:

1. DHCP per la distribuzione delle c :te TRUST.
2. Dominio, per l'autenticazione degli utenti e delle macchine.
3. DNS privato, per risolvere i nomi delle reti TRUST e DMZ.

Sul server SP devono essere collocati i servizi:

1. FTP, per consentire lo scambio pubblico dei documenti del progetto «transnazionale».
2. HTTP, per gestire un sito a servizio del progetto «transnazionale».

I servizi NBT (NetBIOS) per spazio disco e condivisioni stampanti è disponibile su tutte le macchine con opportuna impostazione dei diritti di accesso forniti dal Dominio.

Si osserva che i tre server dovrebbero essere duplicati, per questioni di fault tolerance (i loro servizi devono sempre essere disponibili). Inoltre i loro indirizzi locali dovranno essere impostati manualmente (statici).

Configurazioni di rete (livello 3 OSI)

Gli host della rete TRUST avranno la seguente configurazione, ottenuta via DHCP:

Indirizzo IP: come da schema.
Default Gateway: indirizzo IP della macchina SR (sulla sua interfaccia in TRUST).
DNS: indirizzo IP della macchina PDC.

Gli host della rete DMZ avranno la seguente configurazione (statica):

Indirizzo IP: come da schema.
Default Gateway: indirizzo IP della macchina SR (sulla sua interfaccia in DMZ).
DNS: indirizzo IP della macchina SR (sulla sua interfaccia in DMZ).

Consultare lo schema per un esempio numerico, compresi gli indirizzi pubblici ottenuti dall'ISP e opportunamente distribuiti con dNAT sugli host della rete DMZ.

Risposte ai quesiti

I punti 1. e 2. contenuti nel testo sono stati affrontati nello svolgimento.

Dei punti esplicitamente ricordati, invece, rimangono esclusi:

- presenza di eventuali reti preesistenti;
- numero di stampanti da installare;
- sicurezza dati sensibili.

Per quanto riguarda la «presenza di eventuali reti preesistenti», data la vaghezza, non è possibile una risposta esauriente.

Nello schema proposto si potrebbe considerare una serie di host generici presenti nella scuola, magari distribuiti sui vari laboratori. Essi farebbero parte della rete TRUST e ne condividerebbero le scelte, sempre considerando di separare i domini di collisione opportunamente (magari tra i vari laboratori).

Lo schema degli indirizzi non cambierebbe (con più di 4000 indirizzi a disposizione il problema non sus-

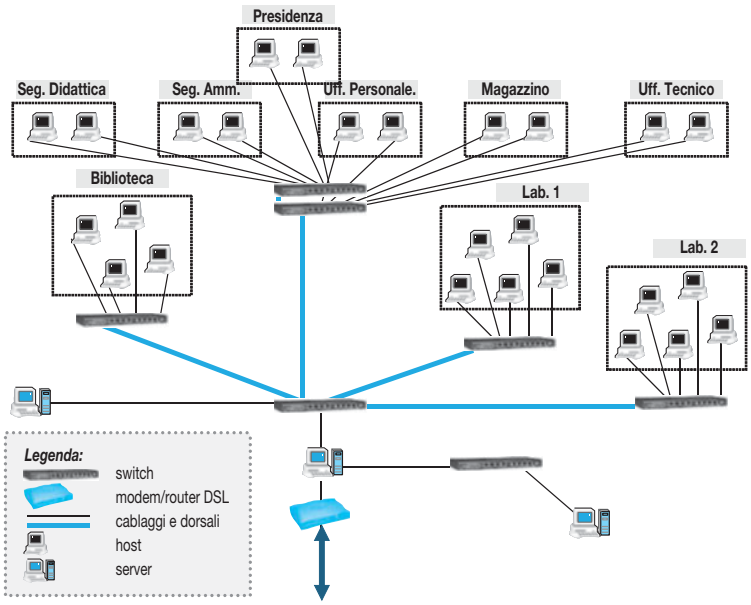
siste). Eventualmente si potrebbero individuare macchine Server di servizi interni, come per esempio server Dati (SQL Server o analoghi) presso i quali accedere dai vari client per esigenze didattiche o altro ancora.

Per quanto riguarda il «numero di stampanti da installare» si può affermare che il quesito è debole: tante quante ne servono, con opportune condivisioni NBT.

Infine per quanto riguarda i «dati sensibili» è necessario che i documenti che li contengono siano protetti all'accesso e consultabili solo dagli utenti del dominio autorizzati. Sarà cura dell'Amministratore della rete (e del Dominio) concedere i diritti d'accesso opportuni per la protezione di tali informazioni, utilizzando i servizi già presenti nel Sistema Operativo adottato.

Schemi

Schema cablaggio strutturato



Schema topologia e indirizzamento