



APPARATI DI INTERNETWORKING

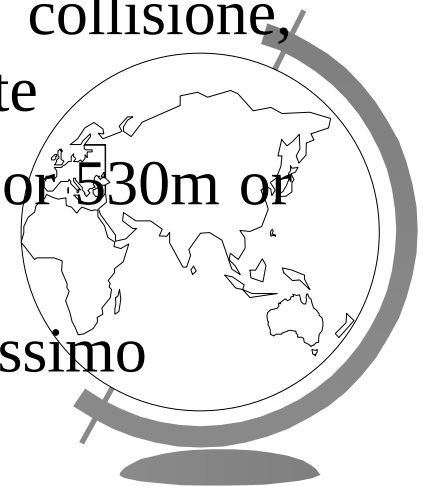
Prof. Ing. Maurizio Casoni



**Dipartimento di Ingegneria “Enzo Ferrari”
Università degli Studi di Modena e Reggio Emilia**

REPEATERS

- ➡ Apparato attivo che collega 2 o più mezzi di trasmissione
- ➡ Estende il mezzo di trasmissione
- ➡ Amplificazione del segnale : ripete i segnali verso tutte le porte di uscita
- ➡ Decodifica i flussi di bit entranti, li ricodifica e li sincronizza
- ➡ Gestisce la collisione: dopo aver rilevato una collisione, trasmette la sequenza di jamming su tutte le porte
- ➡ Rigenera il sincronismo ma con ritardo (5.3 μ s or 530m or 53bits)
- ➡ Oppure non lo rigenera ma ‘taglia’ l’header: massimo numero di repeaters in cascata



INTERCONNESSIONE di LANs

LANs hanno limiti

- ➡ Distanze massime
- ➡ Carico massimo
- ➡ Numero massimo di workstations

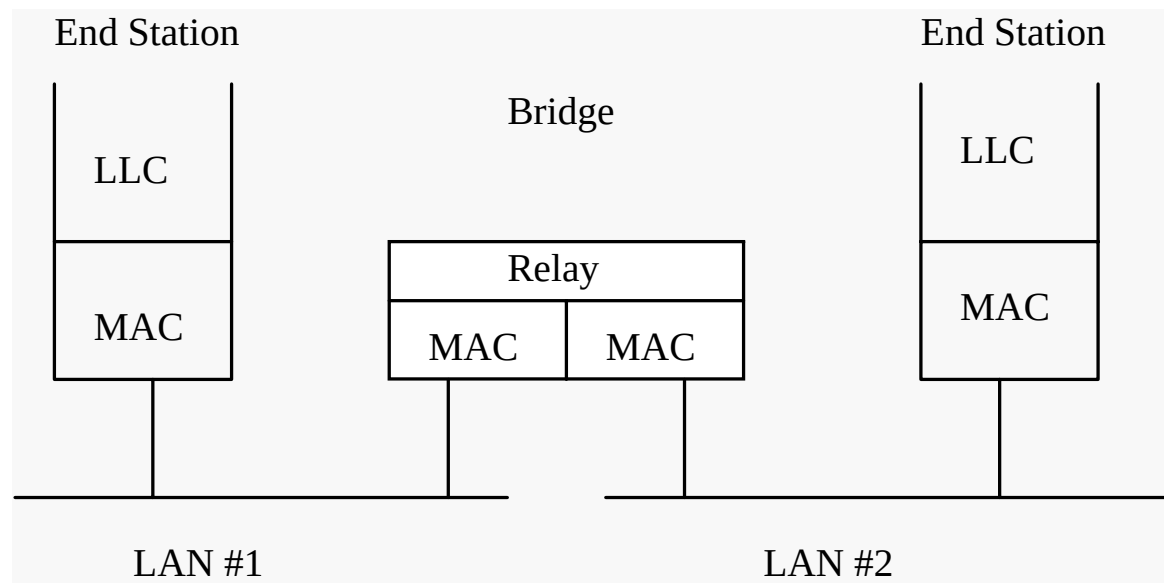
Per superare questi limiti è necessario creare una

Extended LAN

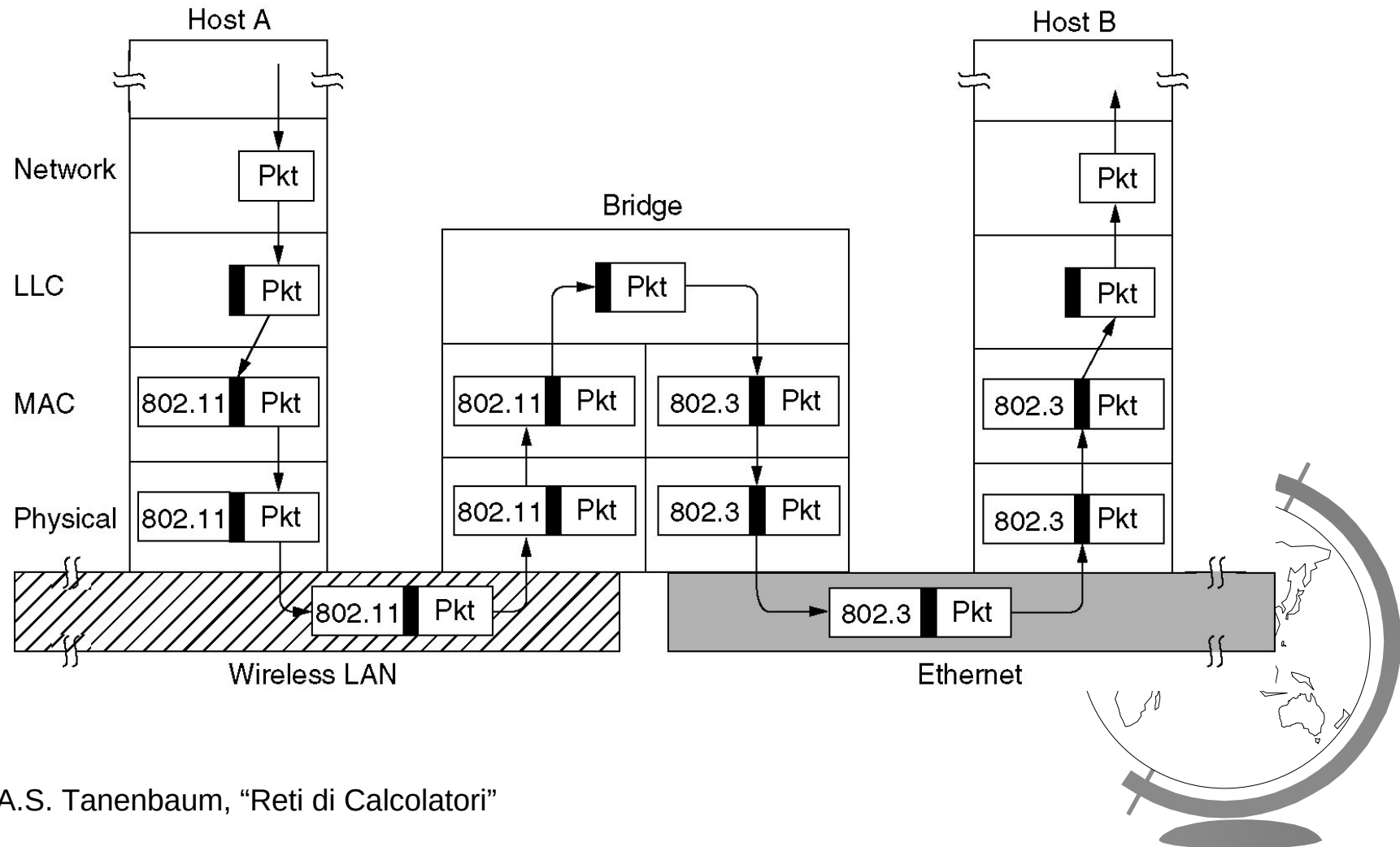


BRIDGE

- ➡ Filtraggio
- ➡ Store & forward



BRIDGE



Da A.S. Tanenbaum, "Reti di Calcolatori"

BRIDGE

- ☞ Eseguono semplici algoritmi di routing e calcolano le tabelle di routing

Due tipi principali:

- ☞ Transparent bridge: tabelle di routing sono sui bridges
- ☞ Source routing bridge: tabelle sono nelle workstations che devono specificare l'intero percorso da seguire all'atto della trasmissione

Transparent bridges:

- ☞ packet forwarding
- ☞ learning process
- ☞ Spanning Tree algorithm per la rimozione dei cicli



ALGORITMO SPANNING TREE

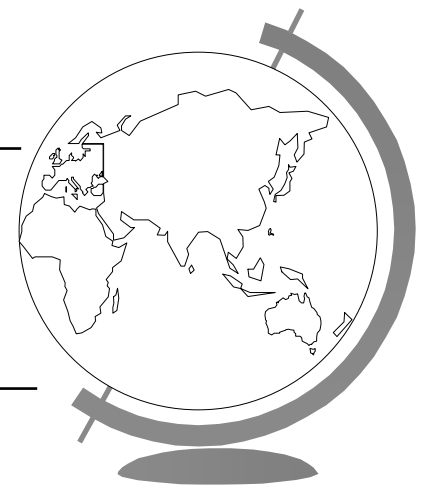
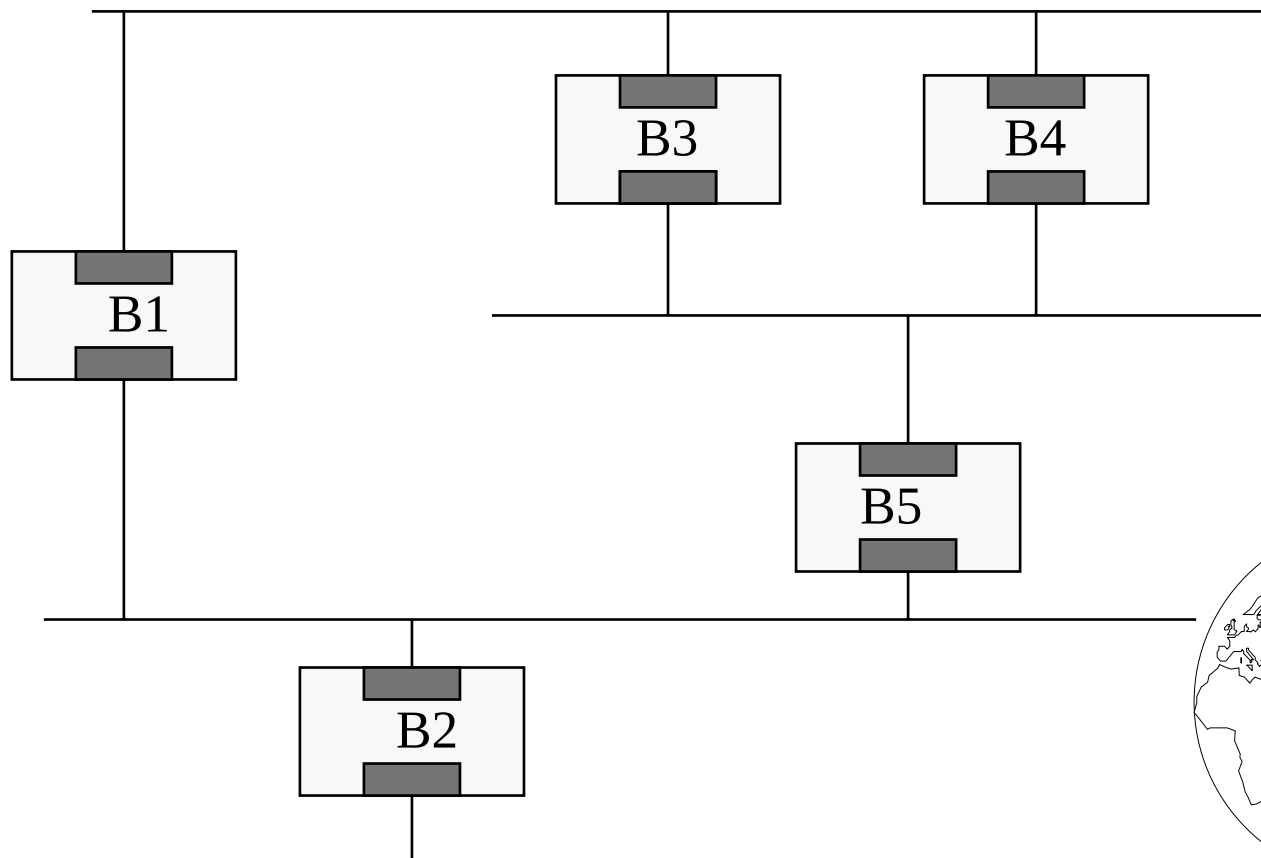
- ➡ Tabelle di routing si creano partendo da un processo di apprendimento processando i pacchetti entranti: nuovi entry points si creano nella tabella
- ➡ Spanning tree integra il processo di apprendimento, crea una struttura ad albero rimuovendo i cicli disabilitando alcune porte di uscita
- ➡ In caso di guasti, deve riconfigurare la topologia della rete nel minor tempo possibile

Opera in 3 passi:

- ➡ Elezione del Root bridge
- ➡ Selezione della Root port
- ➡ Selezione del Designated bridge

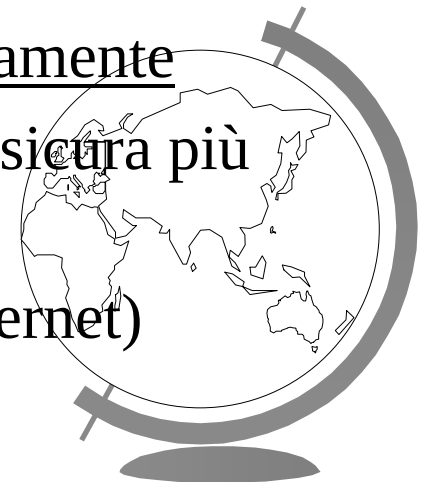


ESEMPIO



BRIDGE vs. ROUTER

- ➡ Entrambi consentono un incremento del numero di stazioni collegate e di suddividere il traffico di rete aumentando le prestazioni
- ➡ **Bridge** collega fisicamente reti differenti ma logicamente sono la stessa: le regole di cablaggio si applicano separatamente per ogni rete ma il protocollo di rete vede un'unica rete
- ➡ **Router** separa una rete sia fisicamente sia logicamente
- ➡ Router è più robusto (percorsi ridondanti) ed assicura più sicurezza (firewalls)
- ➡ Routers impiegati principalmente in WANs (Internet)



ROUTING o BRIDGING ?

- ➡ Davvero pochi apparati sono bridges puri o routers puri (brouters, multi-protocol routers,...)
- ➡ Bridge: data link layer
- ➡ Router: network layer
- ➡ Bridge: single hop packet forwarding
- ➡ Router: multi hop packet forwarding

Bridge non esegue:

- ➡ hop count
- ➡ fragmenting and reassembling
- ➡ congestion notification
- ➡ intermediate addressing



Indirizzi:

- ➡ Bridge: usa solo indirizzi IEEE 802 (MAC); non hanno significati topologici e sono preassegnati dai costruttori
- ➡ Router: usa indirizzi (IP p.es.) assegnati e gestiti nelle singole LANs

Packet forwarding:

- ➡ Bridge: non esegue riordino dei pacchetti
- ➡ Router: esegue riordino dei pacchetti



BRIDGES: PROS

- ➡ “Plug & play” mentre routers devono essere attentamente configurati
- ➡ Meno costosi
- ➡ Inoltrano protocolli non instradabili: alcuni vecchi protocolli di comunicazione (LAT) non sono gestibili dai router sicché occorre usare i bridge per inoltrare i relativi pacchetti da LAN a LAN



ROUTERS: PROS

- ➡ Calcolano il miglior percorso sorgente-destinazione (bridge sfrutta solo un sottoinsieme dell'intera rete con lo spanning tree)
- ➡ Consentono una riconfigurazione veloce e robusta dell'intera rete
- ➡ Non hanno limiti nel numero massimo di stazioni (indirizzi di rete sono WAN, geografici)
- ➡ Usati per gestire la sicurezza nelle reti (firewalls): protezione contro accessi non autorizzati e contro “broadcast storm”
- ➡ Frammentano e riassemblano i pacchetti (bridge non lo fanno e perciò scartano i pacchetti)
- ➡ Gestione della congestione



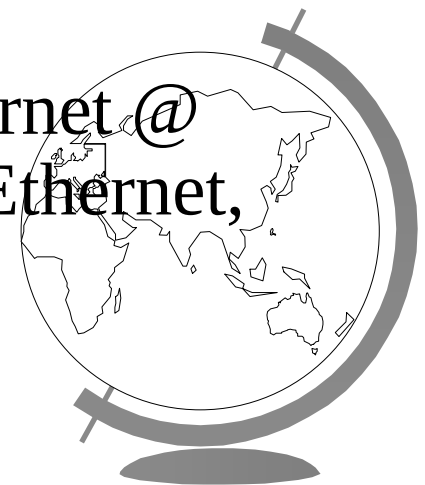
BROUTERS

- ➡ Router che può agire pure come bridge
- ➡ Se il protocollo di rete è noto allora i pacchetti sono processati dal router, altrimenti dalla parte bridge dell'apparato
- ➡ Brouter = router e bridge implementati nel modo “ship in the night”



SWITCH

- ☞ Utile per *superare colli di bottiglia della banda disponibile*
- ☞ Divide le reti in più piccoli collision domains (Ethernet) or anelli (Token Ring) al fine di fornire ad ogni stazione di lavoro più banda
- ☞ E' un bridge multiporta con talvolta caratteristiche dei routers
- ☞ Usato per connettere reti tradizionali (Ethernet @ 10Mbps) a reti ad alta velocità come Fast Ethernet, FDDI, Gigabit Ethernet,...



SWITCH

Sono di due tipi principali:

- ☞ Store & Forward
- ☞ Cut-through

Switches Cut-through hanno tempi di latenza inferiori (μsec vs. msec) ma possono propagare pacchetti danneggiati

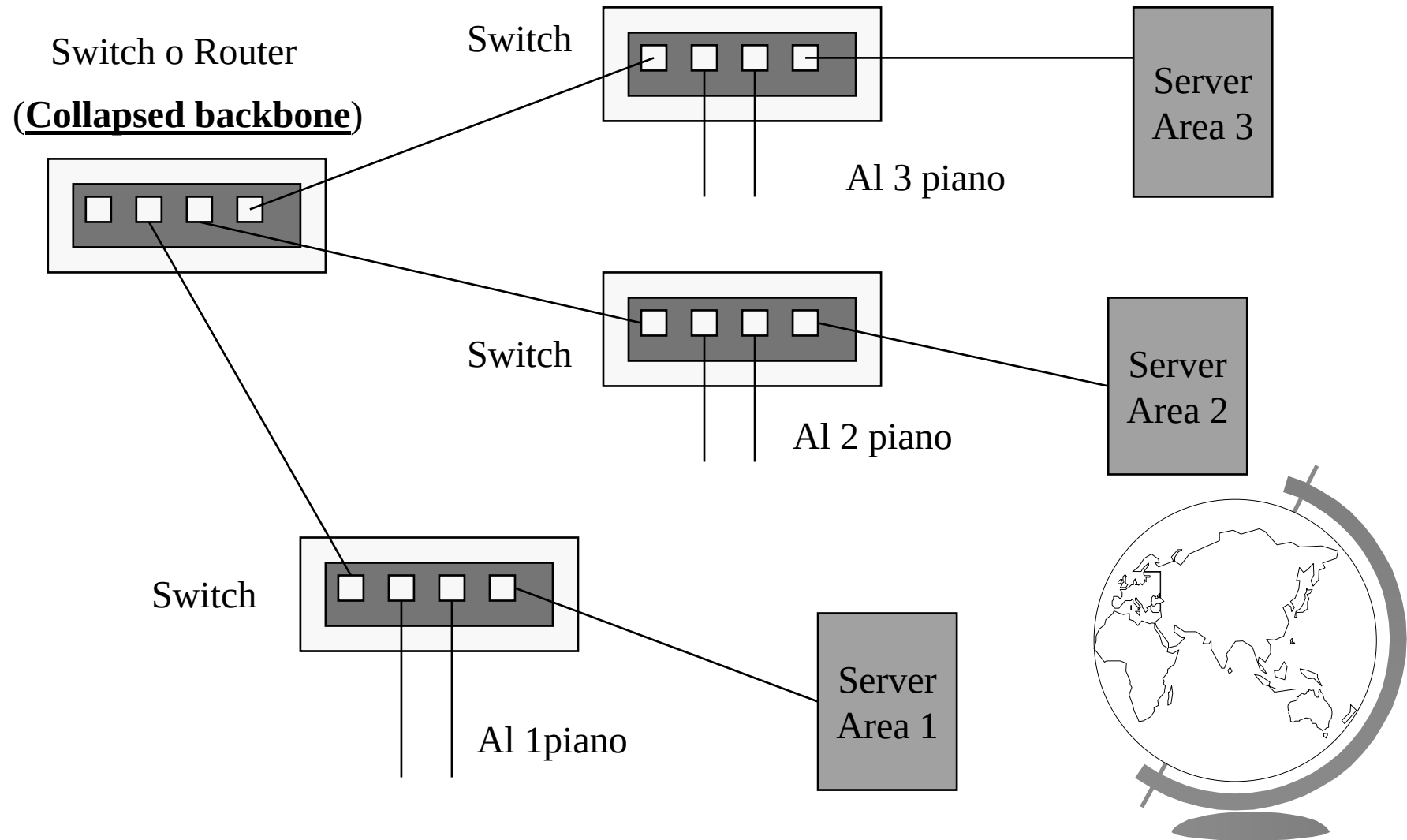


SWITCH STORE & FORWARD

- ➡ Problemi carico elevato a causa del trabocco del buffer: switch deve rigettare nuovi pacchetti in ingresso
- ➡ Indirizzamento viene eseguito mediante tabelle: se traboccano o nuovi pacchetti vengono rigettati oppure indirizzi in uso devono essere scartati
- ➡ Alcuni switches sono ibridi (**threshold detection** o **adaptive**): cominciano come cut-through tenendo sotto controllo la bit error rate; quando una certa soglia viene raggiunta diventano store & forward



ESEMPIO



VIRTUAL LANs

- ➡ Una VLAN è un dominio di trasmissione che collega un sottoinsieme di stazioni secondo determinati criteri
- ➡ Migliore utilizzo della banda disponibile: una rete viene logicamente suddivisa in domini distinti cosicché i pacchetti da una stazione sono inoltrati solo ai membri della VLAN a cui la stazione stessa appartiene
- ➡ Migliorata sicurezza della rete: il traffico tra distinti domini deve passare attraverso un router
- ➡ Gestione più semplice della rete



VLAN: REALIZZAZIONE

Costruttori hanno finora definito 3 metodi per le VLANs:

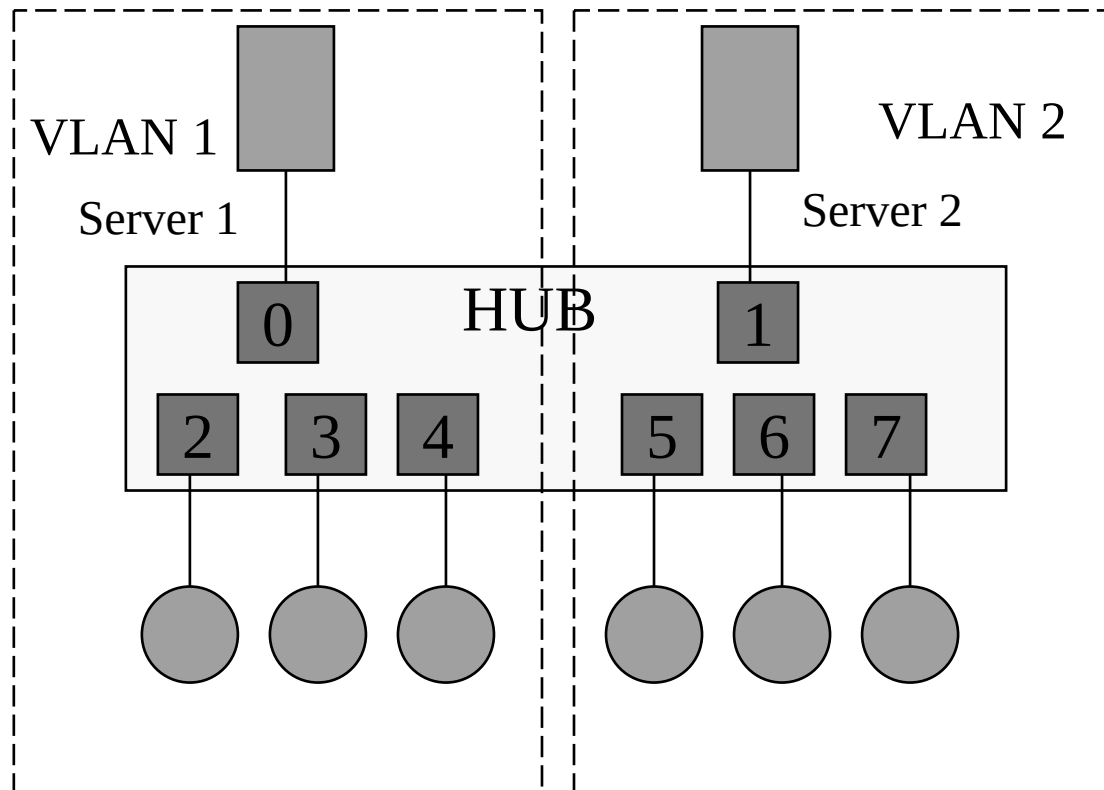
1. Basati su porta
2. Basati su indirizzi MAC
3. Basati sullo strato di Rete OSI

Ognuno di questi metodi esegue compiti tipici di differenti strati OSI



VLAN BASATE SU PORTE

- ☞ Un dominio viene creato collegando logicamente le porte di un apparato
- ☞ Comunicazioni tra domini distinti richiedono l'uso di un router



VLAN BASATE SU PORTE

- ➡ Switches sono usati per realizzare questo metodo
- ➡ Switches possono scambiarsi informazioni per estendere una VLAN

CONS:

- ➡ quando si sposta una stazione la configurazione della VLAN muta: si rende necessario operare da console
- ➡ appartenenza a VLAN è on-off: solo una VLAN per porta è supportata



VLAN BASATE SU INDIRIZZO MAC

- ➡ HUB mantiene una tabella con le associazioni indirizzi MAC vs. VLAN
- ➡ Soluzione più flessibile: se una stazione viene spostata, l'hub automaticamente se ne accorge e modifica l'associazione indirizzo MAC-numero di porta
- ➡ Una stazione può appartenere a più di una VLAN
- ➡ Occorre prestare attenzione alla configurazione dell'hub
- ➡ Per il traffico inter-dominio occorre o un server con 2 porte (2 schede di rete) o un router



VLAN BASATE SUL LIVELLO RETE

- ➡ Occorrono routers o switches che supportano l'inoltro dei pacchetti a livello 3
- ➡ Simile al modo in cui operano i routers: è possibile creare sottoreti IP, numeri di rete IPX, domini AppleTalk,...

PROS:

- ➡ Flessibilità: riconfigurazione automatica delle VLANs
- ➡ Facilità di configurazione
- ➡ Supporto delle comunicazioni inter-dominio : con una porta globale un router può gestire molte sottoreti



IEEE 802.1Q

- ➡ IEEE ha creato un gruppo di lavoro, 802.1Q, per definire uno standard per VLANs, al fine di consentire ad apparati di costruttori differenti di cooperare
- ➡ Si studiano campi dedicati nell' header dei frames di livello 2 per la gestione delle VLANs

Aspetti ancora da definire:

- ➡ Registrazione di una stazione ad una VLAN
- ➡ Gestione dei frames “regolari”
- ➡ Compatibilità dei frames estesi con apparati non standard
- ➡



ETHERNET: FORMATO TRAMA PER SUPPORTO IEEE 802.1Q

- Supporto QoS in ethernet è implementato mediante VLAN identificate da etichette (tag) che contengono bit di priorità
- Apparati bridge/switch processano trame entranti basandosi sull'indirizzo MAC di destinazione e sull'etichetta di VLAN

