CAPITOLO 5 – DISPOSITIVI DI RETE

Obiettivi del Capitolo

Al termine di questo capitolo il corsista sarà in grado di:

- Identificare i principali dispositivi di rete.
- Comprendere il ruolo di ciascun apparato nell'infrastruttura.
- Distinguere hub, bridge, switch e router.
- Comprendere il funzionamento delle reti wireless.
- Analizzare le funzioni di modem e firewall.
- Progettare una semplice infrastruttura di rete aziendale.

5.1 Introduzione ai dispositivi di rete

Una rete informatica non è composta soltanto da computer e server.

Per consentire la comunicazione tra dispositivi sono necessari apparati specializzati che gestiscono:

- il traffico dati;
- l'instradamento;
- la sicurezza;
- la connettività verso Internet;
- la comunicazione wireless.

Questi apparati vengono definiti dispositivi di rete.

Ogni dispositivo opera principalmente su uno o più livelli del modello OSI e svolge funzioni specifiche.

I principali dispositivi di rete sono:

- Scheda di rete (NIC)
- Hub
- Bridge
- Switch
- Router
- Access Point
- Modem
- Firewall

5.2 La Scheda di Rete (NIC)

NIC significa:

Network Interface Card

La scheda di rete rappresenta l'interfaccia che collega un dispositivo alla rete.

Senza una NIC un computer non sarebbe in grado di comunicare con altri dispositivi.

Funzioni principali

- Connessione fisica alla rete
- Trasmissione e ricezione dei dati
- Gestione dell'indirizzo MAC
- Conversione dei dati in segnali trasmissibili

Tipologie

NIC Ethernet

Utilizza un cavo di rete.

Velocità comuni:

- 100 Mbps
- 1 Gbps
- 2.5 Gbps
- 10 Gbps

NIC Wireless

Utilizza onde radio.

Supporta gli standard Wi-Fi.

5.3 Indirizzo MAC e NIC

Ogni scheda di rete possiede un indirizzo MAC univoco.

Esempio:

00:1A:2B:3C:4D:5E

L'indirizzo MAC è assegnato dal produttore.

È utilizzato per identificare il dispositivo all'interno della rete locale.

Analogia

Possiamo immaginare il MAC Address come il numero di telaio di un'automobile.

5.4 Hub

L'hub è uno dei primi dispositivi utilizzati nelle reti Ethernet.

Opera al:

Livello 1 (Fisico) del modello OSI

Quando riceve un segnale, lo replica su tutte le porte.

Esempio

Se il PC A invia dati al PC B:

l'hub trasmette il traffico a:

- PC B
- PC C
- PC D
- tutti gli altri dispositivi collegati

Vantaggi

- Semplicità
- Costi ridotti

Svantaggi

- Basse prestazioni
- Elevato traffico inutile
- Nessuna sicurezza

- Collisioni frequenti

Per questi motivi gli hub sono ormai obsoleti.

5.5 Collisioni di rete

Nelle reti basate su hub più dispositivi possono trasmettere contemporaneamente.

Quando ciò accade si verifica una collisione.

Le collisioni provocano:

- ritrasmissioni;
- rallentamenti;
- perdita di efficienza.

L'introduzione degli switch ha praticamente eliminato questo problema.

5.6 Bridge

Il bridge è stato introdotto per migliorare le prestazioni delle reti.

Opera al:

Livello 2 (Data Link)

È in grado di leggere gli indirizzi MAC.

Funzioni

- Segmentazione della rete
- Riduzione del traffico
- Filtraggio dei frame

Il bridge può decidere se inoltrare o meno un frame.

5.7 Switch

Lo switch è oggi il dispositivo più importante nelle reti LAN.

Opera principalmente al:

Livello 2 del modello OSI

Esistono anche switch Layer 3 che integrano funzionalità di routing.

5.8 Come funziona uno Switch

Lo switch costruisce una tabella chiamata:

MAC Address Table

Questa tabella associa:

MAC Address → Porta fisica

Esempio:

MAC	Porta
00:AA	1
00:BB	2
00:CC	3

Quando riceve un frame, lo switch consulta la tabella e lo inoltra solo alla porta corretta.

5.9 Vantaggi dello Switch

Rispetto all'hub offre:

- Maggiore velocità
- Maggiore sicurezza
- Assenza di collisioni
- Minore traffico inutile
- Maggiore scalabilità

Per questo motivo è presente praticamente in ogni rete moderna.

5.10 Switch Gestiti e Non Gestiti

Switch Non Gestiti

Configurazione automatica.

Ideali per:

- reti domestiche;
- piccoli uffici.

Switch Gestiti

Consentono configurazioni avanzate.

Funzionalità:

- VLAN
- QoS
- Monitoring
- Sicurezza
- Ridondanza

Sono ampiamente utilizzati in ambito aziendale.

5.11 VLAN

VLAN significa:

Virtual Local Area Network

Permette di dividere logicamente una rete fisica.

Esempio:

VLAN 10 → Amministrazione

VLAN 20 → Produzione

VLAN 30 → Direzione

Anche se i computer sono collegati allo stesso switch, appartengono a reti differenti.

Vantaggi

- Sicurezza
- Organizzazione
- Riduzione del traffico broadcast

5.12 Router

Il router è il dispositivo che collega reti differenti.

Opera al:

Livello 3 (Network)

Utilizza gli indirizzi IP.

5.13 Funzionamento del Router

Il router riceve un pacchetto e decide quale percorso utilizzare per raggiungere la destinazione.

Per prendere questa decisione utilizza:

- tabella di routing;
- protocolli di routing;
- metriche.

Esempio

Rete Aziendale

↓

Router

↓

Internet

Il router rappresenta il punto di uscita verso le reti esterne.

5.14 Routing

Il routing è il processo di scelta del percorso migliore.

Esistono:

Routing Statico

Configurato manualmente.

Routing Dinamico

Aggiornato automaticamente.

Protocolli utilizzati:

- RIP
- OSPF
- EIGRP
- BGP

5.15 Access Point

L'Access Point permette ai dispositivi wireless di collegarsi alla rete.

Opera principalmente ai livelli:

- 1
- 2

del modello OSI.

5.16 Funzionamento di un Access Point

L'Access Point:

- riceve traffico Wi-Fi;
- lo converte in traffico Ethernet;
- consente la comunicazione con la rete cablata.

È il dispositivo che crea la rete wireless visibile agli utenti.

5.17 SSID

Ogni rete Wi-Fi possiede un identificativo chiamato:

SSID

Esempio:

- Azienda_WiFi
- Guest_WiFi

Gli utenti selezionano l'SSID per collegarsi alla rete.

5.18 Modem

Il modem collega la rete locale alla rete del provider Internet.

Il termine deriva da:

MODulatore-DEModulatore

Funzioni

- Conversione dei segnali
- Connessione verso l'ISP
- Accesso a Internet

Tecnologie comuni

- ADSL
- VDSL
- Fibra ottica
- FWA
- 5G

5.19 Firewall

Il firewall rappresenta uno dei principali strumenti di sicurezza.

Può essere:

- hardware;
- software.

5.20 Funzioni del Firewall

Il firewall analizza il traffico di rete e decide se:

- consentirlo;
- bloccarlo.

Lavora attraverso regole chiamate:

Policy

Esempio

Consentire:

- HTTP
- HTTPS

Bloccare:

- connessioni non autorizzate

5.21 Firewall Tradizionali e Next Generation Firewall

Firewall Tradizionale

Analizza:

- indirizzi IP
- porte
- protocolli

Next Generation Firewall (NGFW)

Analizza anche:

- applicazioni
- utenti
- contenuti
- minacce avanzate

Offre livelli di protezione molto superiori.

5.22 IDS e IPS

Molti firewall moderni integrano:

IDS

Intrusion Detection System

Rileva attività sospette.

IPS

Intrusion Prevention System

Blocca automaticamente gli attacchi.

5.23 Appliance UTM

UTM significa:

Unified Threat Management

Integra:

- Firewall
- Antivirus
- Antispam
- VPN
- IDS/IPS

in un unico dispositivo.

5.24 Architettura di una rete aziendale moderna

Una tipica rete aziendale comprende:

Internet

↓

Firewall

↓

Router

↓

Switch Core

↓

Switch Access

↓

PC – Server – Stampanti – Access Point

Questa struttura garantisce:

- sicurezza;
- scalabilità;
- affidabilità.

5.25 Caso di studio

Un'azienda con 100 dipendenti dispone di:

- 1 firewall NGFW
- 2 router ridondati
- 6 switch gestiti
- 12 access point
- 1 connessione in fibra

Le VLAN separano:

- Amministrazione
- Produzione
- Ospiti
- Server

Questo approccio migliora sicurezza e prestazioni.

Riepilogo

In questo capitolo abbiamo analizzato:

- NIC
- Hub
- Bridge
- Switch
- VLAN
- Router
- Routing
- Access Point
- Modem
- Firewall
- IDS/IPS
- UTM

Questi dispositivi costituiscono l'infrastruttura fondamentale delle reti moderne.

Domande di verifica

1. Qual è la funzione di una scheda di rete?
2. Quali differenze esistono tra hub e switch?
3. Come funziona una MAC Address Table?

4. Cos'è una VLAN?
5. Qual è il ruolo di un router?
6. Quali differenze esistono tra routing statico e dinamico?
7. Qual è la funzione di un Access Point?
8. A cosa serve un modem?
9. Qual è il compito di un firewall?
10. Quali vantaggi offrono i Next Generation Firewall?