CAPITOLO 6 – PROTOCOLLI DI RETE E SERVIZI DI COMUNICAZIONE

Obiettivi del Capitolo

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

- Comprendere il concetto di protocollo di rete.
- Distinguere protocolli orientati alla connessione e non orientati alla connessione.
- Comprendere il funzionamento di TCP e UDP.
- Analizzare il ruolo di ARP, ICMP, DNS e DHCP.
- Comprendere il funzionamento dei principali protocolli applicativi.
- Interpretare il flusso di comunicazione tra client e server.

6.1 Cos'è un protocollo di rete

Un protocollo è un insieme di regole che definisce come i dispositivi devono comunicare.

Senza protocolli comuni, due dispositivi non sarebbero in grado di scambiarsi informazioni.

Analogia

Quando due persone conversano utilizzano una lingua comune.

Nelle reti informatiche la "lingua" è rappresentata dai protocolli.

Essi definiscono:

- formato dei dati;
- modalità di trasmissione;
- gestione degli errori;
- procedure di controllo.

6.2 La suite TCP/IP

La maggior parte delle reti moderne utilizza la suite di protocolli TCP/IP.

Non si tratta di un singolo protocollo ma di un insieme di protocolli che collaborano tra loro.

Tra i principali troviamo:

- IP
- TCP
- UDP
- ARP
- ICMP
- DNS
- DHCP
- HTTP
- HTTPS
- FTP
- SMTP

6.3 Il Protocollo IP

IP (Internet Protocol) è il protocollo responsabile dell'indirizzamento e dell'instradamento dei pacchetti.

Ogni pacchetto contiene:

- indirizzo IP sorgente;
- indirizzo IP destinazione;
- dati.

Funzioni

- Identificazione degli host
- Routing
- Consegna dei pacchetti

IP non garantisce che il pacchetto arrivi correttamente.

Per questo motivo si appoggia a TCP o UDP.

6.4 TCP – Transmission Control Protocol

TCP è un protocollo orientato alla connessione.

Prima di trasmettere i dati stabilisce una connessione tra mittente e destinatario.

Caratteristiche

- Affidabile
- Controllo degli errori
- Conferma di ricezione
- Ritrasmissione automatica
- Ordinamento dei dati

6.5 Il Three-Way Handshake

Prima della trasmissione TCP esegue una procedura chiamata:

Three-Way Handshake

Fase 1:

Client → SYN

Fase 2:

Server → SYN-ACK

Fase 3:

Client → ACK

Solo dopo questo scambio inizia la trasmissione dei dati.

6.6 Vantaggi e Svantaggi di TCP

Vantaggi

- Elevata affidabilità
- Correzione degli errori
- Integrità dei dati

Svantaggi

- Maggiore overhead
- Velocità inferiore rispetto a UDP

6.7 UDP – User Datagram Protocol

UDP è un protocollo non orientato alla connessione.

Invia i dati senza verificare la ricezione.

Caratteristiche

- Molto veloce
- Minimo overhead
- Nessuna conferma
- Nessuna ritrasmissione

6.8 Utilizzo di UDP

UDP viene utilizzato quando la velocità è più importante dell'affidabilità.

Esempi:

- Streaming video
- Streaming audio
- Gaming online
- VoIP
- Sensori IoT

6.9 Confronto TCP e UDP

Caratteristica	TCP	UDP
Connessione	Sì	No
Affidabilità	Alta	Bassa
Velocità	Inferiore	Maggiore

Controllo errori	Sì	Limitato
Applicazioni	Web, Email, FTP	VoIP, Streaming, Gaming

6.10 Porte di Comunicazione

Per consentire a più applicazioni di utilizzare la rete contemporaneamente vengono utilizzate le porte.

Una porta identifica un servizio.

Esempio:

IP → identifica il dispositivo

Porta → identifica l'applicazione

6.11 Porte più comuni

Protocollo	Porta
HTTP	80
HTTPS	443
FTP	21
SSH	22
SMTP	25
DNS	53
DHCP	67/68
POP3	110
IMAP	143

Queste porte devono spesso essere autorizzate dal firewall.

6.12 ARP – Address Resolution Protocol

ARP permette di associare un indirizzo IP ad un indirizzo MAC.

Problema

Il computer conosce l'IP del destinatario ma non il suo MAC Address.

Soluzione

Invia una richiesta ARP:

"Chi possiede questo indirizzo IP?"

Il dispositivo interessato risponde comunicando il proprio MAC Address.

6.13 Cache ARP

Per evitare continue richieste, il sistema memorizza temporaneamente le associazioni IP-MAC.

Questa memoria prende il nome di:

ARP Cache

Vantaggi:

- Riduzione del traffico
- Maggiore velocità

6.14 ICMP – Internet Control Message Protocol

ICMP viene utilizzato per:

- diagnostica;
- segnalazione errori;
- test di connettività.

Non trasporta dati applicativi.

6.15 Il comando Ping

Ping utilizza ICMP.

Invia un messaggio Echo Request.

Il destinatario risponde con:

Echo Reply

Esempio:

ping 8.8.8.8

Permette di verificare:

- raggiungibilità;
- latenza;
- continuità della connessione.

6.16 Traceroute

Traceroute utilizza ICMP per individuare il percorso seguito dai pacchetti.

Mostra:

- router attraversati;
- tempi di risposta;
- eventuali problemi di instradamento.

È uno strumento fondamentale per il troubleshooting.

6.17 DNS – Domain Name System

Gli utenti ricordano facilmente nomi come:

www.openai.com

ma i computer utilizzano indirizzi IP.

Il DNS traduce il nome nel relativo indirizzo IP.

6.18 Funzionamento del DNS

Quando un utente inserisce un indirizzo web:

1. Il client contatta il server DNS.
2. Il DNS ricerca il record.
3. Restituisce l'indirizzo IP.
4. Il browser contatta il server corretto.

Senza DNS sarebbe necessario ricordare gli indirizzi IP di tutti i siti.

6.19 DHCP – Dynamic Host Configuration Protocol

DHCP assegna automaticamente:

- indirizzo IP;
- subnet mask;
- gateway;
- DNS.

6.20 Processo DHCP

Il processo utilizza quattro fasi:

1. Discover
2. Offer
3. Request
4. Acknowledge

Questo meccanismo è chiamato:

DORA

6.21 HTTP – HyperText Transfer Protocol

HTTP è il protocollo utilizzato per la navigazione web.

Opera secondo il modello:

Client → Server

Il browser invia una richiesta.

Il server restituisce una risposta.

6.22 HTTPS

HTTPS è la versione sicura di HTTP.

Utilizza:

TLS/SSL

per cifrare le comunicazioni.

Vantaggi:

- Protezione dei dati
- Riservatezza
- Integrità delle informazioni

6.23 FTP – File Transfer Protocol

FTP viene utilizzato per trasferire file tra client e server.

Funzioni:

- Upload
- Download
- Gestione file remoti

Limite principale:

trasmissione non cifrata.

Per questo motivo oggi viene spesso sostituito da:

- SFTP
- FTPS

6.24 SMTP – Invio della posta elettronica

SMTP significa:

Simple Mail Transfer Protocol

È utilizzato per:

- inviare email;
- trasferire messaggi tra server di posta.

6.25 POP3 e IMAP

Entrambi permettono di ricevere posta elettronica.

POP3

Scarica i messaggi sul dispositivo.

Vantaggi:

- semplicità;
- utilizzo offline.

IMAP

Mantiene i messaggi sul server.

Vantaggi:

- sincronizzazione tra dispositivi;
- gestione centralizzata.

È il protocollo più utilizzato nelle organizzazioni moderne.

6.26 Caso pratico: apertura di un sito web

Un utente apre:

www.azienda.it

Fasi:

1. DNS traduce il nome.
2. Viene individuato l'IP.
3. TCP stabilisce la connessione.
4. HTTPS protegge la comunicazione.
5. HTTP richiede la pagina.
6. Il server risponde.
7. Il browser visualizza il contenuto.

Tutto avviene in pochi millisecondi.

6.27 Caso pratico: invio di una email

Quando un utente invia una email:

1. Il client utilizza SMTP.
2. Il server inoltra il messaggio.
3. Il destinatario lo riceve tramite IMAP o POP3.

Durante il percorso possono intervenire:

- DNS
- TCP
- Firewall
- Router

Riepilogo

In questo capitolo abbiamo analizzato:

- TCP
- UDP
- Porte di comunicazione
- ARP
- ICMP
- DNS
- DHCP
- HTTP
- HTTPS
- FTP
- SMTP
- POP3
- IMAP

Questi protocolli costituiscono il linguaggio attraverso cui avvengono tutte le comunicazioni nelle reti moderne.

Domande di verifica

1. Cos'è un protocollo di rete?
2. Quali differenze esistono tra TCP e UDP?
3. Cos'è il Three-Way Handshake?
4. A cosa serve ARP?
5. Qual è il ruolo di ICMP?
6. Come funziona il DNS?
7. Qual è il ruolo del DHCP?
8. Quali differenze esistono tra HTTP e HTTPS?
9. A cosa serve SMTP?
10. Quali differenze esistono tra POP3 e IMAP?