**Network trends:**

* BYOD (Bring your own device)
* Online collaboration (Cisco webex)
* Video
* In casa:
  + Smart casa
  + Smart auto
* Esistono possibilità del passaggio dati, cablati, appoggiandoci alla rete elettrica, tramite degli scatolotti (Powerline Networking).

**Cloud computing:**

Utilizzare dei server che sono nella rete, i quali sono acquistati dalle aziende per inserire i dati (es: bilanci). Questi server permettono di utilizzare delle macchine virtuali da remoto. Ci sono molte tipologie di dati segreti che non si vogliono far conoscere, e quindi da proteggere, dati che difficilmente le aziende lasciano ai Cloud computing. Anche perchè questi Cloud oltre ad immagazzinare dati vanno pure ad elaborarli.

Ci sono 4 tipologie di server remoto:

1. Public Clouds: Servizi pubblici che ci permettono di immagazzinare dei dati, che possono essere free or not.
2. Private Clouds: Inteso per una specifica organizzazione
3. Hybrid Clouds: Una parte pubblica e una parte privata
4. Custom Clouds

**Domotica:**

Smart home, utilizzati per comunicare con gli elettrodomestici e renderli domotici. Da remoto si può comandare la casa, per diversi elettrodomestici, es: antifurto, forno, ecc. Qui si utilizza sempre un Cloud computing perchè lavora ed elabora i dati.

**Wireless Broadband:**

Trasmissione a banda larga, detta anche Wi-Max. Significa portare internet in zone dove non è possibile portare ADSL o altre tipologie di connessioni. L’istallazione è molto semplice da effettuare e chi dal servizio viene chiamato WISP (Wireless Internet Service Provider) stile EOLO.

CONTRO: La connessione dipende dal meteo e dall’ambiente in cui è inserito l’access point.

1. Wireless Locale
2. Wireless Broadcast (velocità minore da quella locale)

**Sicurezza:**

I dati sono molto importanti nel 21esimo secolo, perchè essi possono essere utilizzati per capire i trend della società. Gli attacchi si possono effettuare sia interni che esterni. Il firewall è colui che blocca i dati che non vogliamo ricevere, esso è messo a metà tra i dati e decide se accettare o meno i dati.

* Minacce esterne: Virus (Malware), gli spyware (pop-up), Attacchi che mandano fuori dei server (es: Zero-Day attacks), Attacchi che intercettano i dati (per evitare ciò si utilizza la cifratura, che tramite algoritmi ci permettono di criptare i dati. Quest’ultimi possono essere cifrati solo da chi possiede la chiave). Possibilità di rubare l’identità di qualcuno.
* Minacce interne: Perdere o rubare un device, errori accidentali da lavoratori ed errori maliziosi.

SOLUZIONI:

* Utilizzo dei firewall, hardware e software
* Utilizzo degli antivirus o antispyware.
* Utilizzo delle ACL cioè regole contenute nel firewall
* Utilizzo delle VPN, è usare una rete privata all’interno di internet (dominio pubblico).

**Comunicazione Fondamentale:**

Ci sono tre elementi nella comunicazione:

* Sender 🡺 chi manda
* Un Destinatario 🡺 reciver
* Media 🡺 Mezzo fisico utilizzato per il passaggio delle informazioni

Troviamo dei protocolli, che regolano la comunicazione, essi mettono delle regole per la comunicazione. Queste regole dipendono dalla tipologia del protocollo. Nei computer troviamo il trasmettitore che va a tradurre il segnale per il reciver.

Le regole servono per far capire i messaggi, siccome il linguaggio deve essere comune. Oppure ci possono essere su regole su come avviene la comunicazione. Queste regole vanno sotto il nome di protocolli. Quest’ultimi devono essere riconosciuti a livello internazionale siccome devono esssere standard (indipendenti da SO e HW). Ci sono i linguaggi prioritari che però non essendo standard non possono comunicare con altri device che non conoscono quel linguaggio, senza utilizzare un traduttore (GATEWAY)

REQUISITI PRINCIPALI:

* Il mittende e il destinatario devono essere identificati (es: indirizzi IP)
* Linguaggio e grammatica comune (i PDU (protocol data unit)).
* Velocità e il tempo di invio
* Protocollo che conferma o non i dati inviati. (ad esempio: nei protocolli che trasmettono dati di video streaming NON utilizzano quelli confermati siccome sennò il dato bisognerebbe rimandarlo in caso di errore e questo non si può avere in uno streaming).

ENCODING:

* È il processo di conversione delle informazioni per renderle accettabili ad un altro dispositivo. Esempio: TTL (computer 0-1). Encoder è il dispositivo che in trasmissione converte il segnale in TTL a Manchester, rendendolo compatibile per il mezzo fisico.

DECODING:

* È il processo inverso della conversione di informazioni (Encoding) e servono per renderle interpretate. Decoder va a decodificare il segnale da Manchester a TTL per renderlo compatibile al dispositivo al device.

FORMATTAZIONE DEI DATI INVIATI:

I dati vengono inviati in uno specifico formato o struttura, le quali dipendono dal tipo di messaggio e dal canale usato per inviare il messaggio. Ad esempio, il protocollo IP: ci permette di instradare i dati, esso è costituito come: esso è diviso in vari campi (es:version, ecc).

L’incapsulamento serve per capire l’indirizzo del destinatario e del mittente.

DIMENSIONI DEL MESSAGGIO:

Se il messaggio è molto grande allora esso viene frammentato e quindi ci permette di uilizzare tante applicazioni collegate alla rete assieme. Questo viene fatto siccome la trasmissione è seriale, quindi questo seve per far si che non ci sia una monopolizzazione della applicazione, ma renderla così in pseudoparallelismo.

TEMPO DEL MESSAGGIO:

La velocità di trasmissione definisce quanti bit al secondo invio. Parametro che deve essere uguale sia tra mittente che ricevente. Il concetto di bit in trasmissione significa un’unità del tempo del bit trasmesso, se avessimo una velocità di trasmissione differente riceveremmo meno dati rispetto all’altra macchina.

Questa velocità di trasmissione deve tener conto delle differenze tra le macchine, siccome chi riceve deve effuttare più operazioni (es: correzzione di dati con il CRC oppure la memorizzazione dei dati), rispetto al mandante. Il ricevente potrebbe andare in OverRan siccome NON è in grado di elaborare i dati che arrivano, siccome il suo buffer e pieno, questo è regolato dal CONTROLLO DI FLUSSO. Quindi prima che esso vada in overRan lui si ferma, finche il trasmettitore non libera il buffer per ricevere i dati. Per regolamentarlo vengono utilizzati algoritmi (es: XON-XOFF [XON resume trasmission] e XOFF[stop trasmission]).

Il controllo dell’errore consiste nel verificare se i dati solo arrivati correttamenti, questo controllo viene fatto dalla scheda di rete: la quale se trova un errore nel dato lo va a eliminare. Nel caso di protocollo confermato, esso va a creare un TIMEOUT che viene attivato quando mandiamo il messaggio, se la conferma del messaggio non arriva entro la fine del timeout allora manda un messaggio di errore, così il mittente può capire se ci sono o meno errori nei dati inviati.

METODI DI ACCESSO: spesso si utilizza un mezzo comune tra device, e siccome ci sono molte macchine che hanno intenzione di accedere allo stesso device, quindi per questo bisogna regolamentare l’accesso per evitare una collisione tra segnali. Si suddividono in due categorie:

|  |  |
| --- | --- |
| I device si accorgono che sono andati in collissione cercano di gestire la collissione. | Wireless, fa si che non avvenga, quindi va a prevenire la collissione. |

MESSAGGI INVIATI:

* Unicast
* Multicast
* BroadCast