FACOLTÀ DI INGEGNERIA
UNIVERSITÀ DEGLI
STUDI DI PALERMO

Corso di Laurea Specialistica
Ingegneria Gestionale

Sistemi ICT per il Business Networking

Value-Added Networks (VANs)

Docente: **Vito Morreale** (vito.morreale@eng.it)

Value-Added Network (VAN)

- A **specialized application service provider (ASP)** that acts as an **intermediary** between trading partners sharing data or business processes
- **Data transmission** between business partners
- Usually for a given vertical domain or industry
- Provides **value-added services**
  - such as **data transformation** between formats (EDI↔XML, EDI↔EDI, …)
- Pre-defined **integration capabilities** (e.g. data synchronization services) and **applications** (e.g., supply chain order visibility)
- Traditionally, most VANs primarily only supported general-purpose B2B integration capabilities focused on **EDI**, but these service providers are **quickly evolving** to become more process- and industry-specific over time, particularly in industries such as retail and hi-tech manufacturing

Value-Added Network (VAN)

- Simply stated, the VAN is structured into three main components:
  - the **technical component**, which provides
    - message formatting,
    - establish communications protocol,
    - and determines and maintains line speeds;
  - the **mail component**, which establish the electronic mailbox in which EDI transactions are held before they are forwarded to their intended destinations;
  - the **link component**, which coordinates the transmission of data through the VAN network

Why VANs?

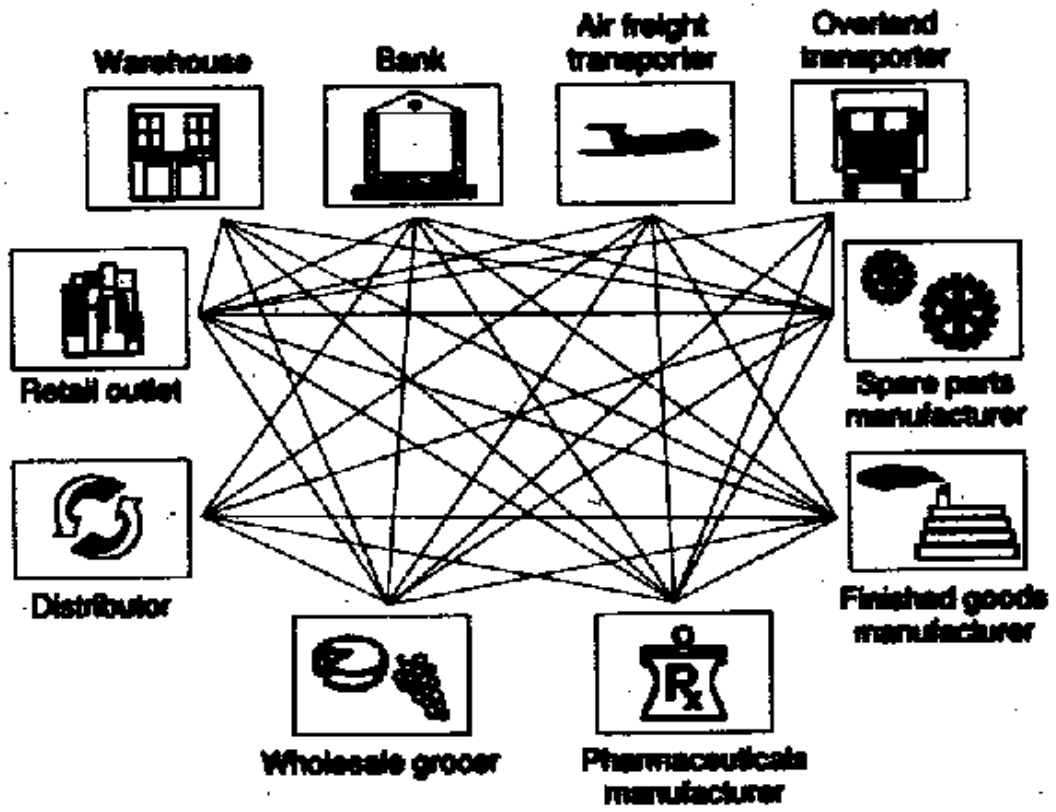
- Why not all partners can communicate each other through the **telephone**?
  - Because **the telephone cannot provide the additional features and services** that VANs can provide
- **Why not connect directly the both parts** involved in the communication with a point-to-point connection?
  - **Not all partners use the same computer environment**, and the VAN can easily make all this necessary conversions

VAN: benefits and features

- A **direct communication link** to any trading partner
- Knowledge of **EDI standards** and evolving **EDI technologies**
- Ability to support **multiple data format standards**
- Value-added components: **training**, **software**, **consulting**, etc.
- **Mailbox** services
- Ability to support **varied protocols** and access methods
- **24-hour** a day message transmission
- Ability to provide **tracking** and **control** information
- …

VAN vs. Point-to-Point

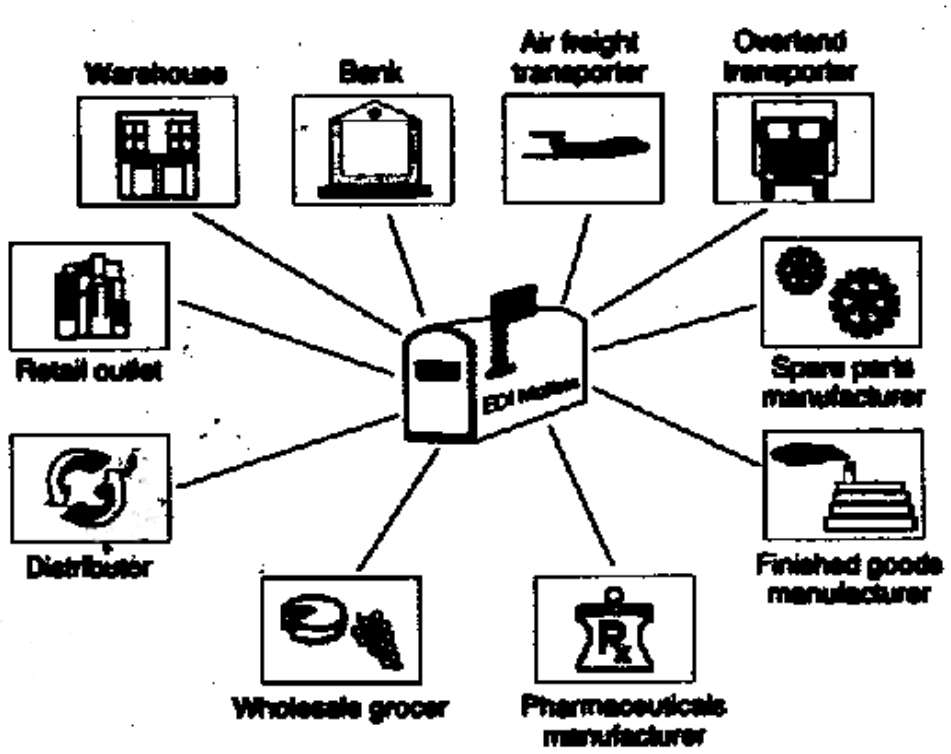
- In a **point-to-point network**, all computers are linked directly



Point-to-point EDI network.

VAN vs. Point-to-Point

VANs do not require to create own communication subsystems and the competition among them ensures subscribers **lower communications costs**, **assistance**, **education**, and access to **professional EDI support**



EDI messaging via a VAN mailbox service.

VAN: internal control

- **Access Control**
- **Data Integrity**
  - Message Authentication Code
  - Encryption
- **Transmission Security**
  - Message Authorization
  - Message Authentication
  - Message Delivery
  - Message Protection

VAN: internal control – access control

- The VAN have to ensure that an **unauthorized user** do not gain access to company data
- All data that pass through a third-party network are routed via the **receiver identification codes** in the outer EDI envelopes. The outer envelope is called the **interchange envelope**
- Access to a mailbox normally requires both a specific mailbox **identification code** and a **password**

VAN: internal control – data integrity

- **Message authentication code (MAC)** is a cryptographic checksum value
  - In an EDI transaction, **the sender calculates the MAC** and **appends it to the message** prior to transmission
  - **The receiver's software recalculates the MAC** upon receipt of the EDI message and **compares it to the original MAC**
    - **If the MACs agree**, the EDI message is processed
    - **If do not agree**, something of the message has been changed
  - This technique is **useful to know if messages have been modified, deleted or added**
- **Encryption** is the conversion of plain text into cipher-text data and is performed with a **cryptographic algorithm and key**
  - The only who can access the message is that **who has the key**

VAN: internal control – Transmission Security

- The VANs systems **have to** provide **security in the transmission** of all messages
- **The message won't be read by anyone else** than the authorized person
  - The message will arrive to his **correct destination**
  - **Nobody unauthorized** can access to the network

VAN: internal control – Transmission Security

- **Message Authorization:** security procedures that ensure the authenticity of a transmission
  - Validate the **originating workstation**
  - That it's authorized to transmit **at the specified time**
  - **Validate the message format**
  - Verify the operator or workstation's **authority to transmit the message type**
  - Test to ensure that the **correct authorization codes are embedded in the message**

VAN: internal control – Transmission Security

- Once an authorized originator has entered a message into the system, the ensuing procedures should address the parameters for the **message authentication**
  - **Positional edits** for correct control, characters, address, data fields, and for line and format constraints
  - **Validation** for routing numbers, addresses, type codes, and user-specific, content-oriented information

VAN: internal control – Transmission Security

- **Message delivery** controls help ensure that a message was received properly and remained accurate
  - **The destination is a valid node** on the network and is **authorized to receive the type** of traffic involved
  - **A positive connection is made** with the station and validated before and after message transmission
  - **Verification of receipt of the message** is secured
  - A **log of all messages transmitted** is kept and reviewed for adequacy
  - The **queuing and routing algorithms** enable traffic to be processed efficiently

VAN: internal control – Transmission Security

- **Message protection**:
  - Message **encryption**
  - **Multiplexed** transmission lines
  - **Synchronous, continuous** data streams
  - The **highest-speed transmission** facilities feasible or available
  - **Alternate paths** and rotary-line configurations
  - **Satellite** transmission

References

- **EDI** (provided by the teacher)