UNIT-1
SUPPLY CHAIN COMMUNICATION NETWORKS

ROLE OF COMMUNICATION NETWORKS IN SUPPLY CHAINS

Supply chains are complex networks of organizations, people and systems with communication playing a definitive role in effective coordination. In the past, telecommunications involved *visual signals* such as beacons, smoke signals, optical telegraphs or heliographs and *audio signals* such as drum beats, horns and whistles. With the advent of electricity and electronics, now the telecommunications include use of the following:

a. electrical devices like telegraphs, telephones and tele printers
b. radio wave, microwave communications and fiber optics associated electronics
c. orbiting satellites and the Internet

Given the competitive environment, communication networks make or break supply chains. The following case let provides an overview of how communication networks helped a fast moving consumer goods (FMCG) enterprise increase market share:

FMCG industry in India is facing a tough competition with international brands presence. Given the vast geographic spread of the country, communication and coordination between the regional offices is a major challenge. Even frustrating aspect is the complexity of wide spread distribution network and the speed of data collection & processing from the unorganized retailer networks. For the brand owner (FMCG products), the key success factor to become competitive in the market is to capture the stock information across distribution centers (primary sales) and more importantly atretailer outlets (secondary sales) under each distribution center. During the early days of competition, the primary sales information was used to be collected and processed at the end of every week to enable planning. And the information about retailer stock position (secondary sales) was always a mystery. The stock levels at retailers were invisible leading to inaccurate forecasts and incorrect reading about product performance. Any communication from retailer's end to the brand owner used to take about fifteen to thirty days crossing multiple hierarchies of people. For the competitors the communication lag was the best opportunity to occupy the retailer's shelf spaces. There were three important reasons for communication lag:

1. Though there was telecommunication network usage, data collection and presentationconsumed time at primary and secondary sales level
2. While the brand owners could extend their enterprise systems to capture primary sales data using telecom networks, secondary sales data capture had structural issues.
3. The extension of enterprise systems to secondary sales level required new functionality tobe added to enterprise systems and the process of change was very slow

2.2 OVERVIEW OF TELECOMMUNICATION NETWORKS

A telecommunication network has following basic components:

1. The sender who transmits data to a destination point in the network (e.g. Voice call overtelephone).
2. The carrier who transmits the data to the destination point in the network (e.g. Telephoneoperator enterprise).
3. The receiver who receives the data at the destination point in the network (e.g. Audiomessage over telephone).

Small telecommunication networks that comprise of individual connections called "nodes" (e.g. Home or office telephone connection) are connected to "regional telephone exchange" and the regional telephone exchanges are linked to "trunks or back bone".

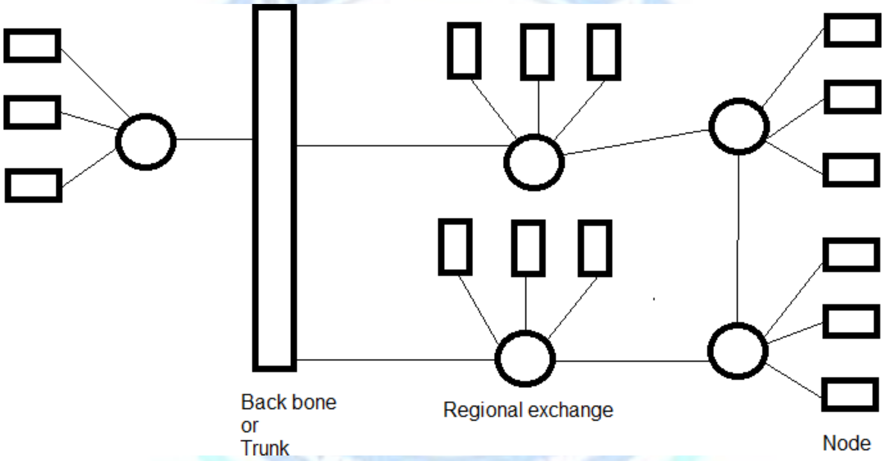

Figure 2.1: Telecommunication network

The worldwide interconnected telecommunications network consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all inter-connected by switching centers. It is also known as public switched telephone network (PSTN), a network of world's public circuit-switched telephone networks.

Network operators do the task of building telecommunication networks and selling services to customers. In India till telecom sector was opened to private operators, the government used to build and manage telecommunication services. BSNL is the government owned telecommunication network and service provided. Bharti Airtel, Reliance telecom, Tata teleservices, Idea are few private players in Indian telecommunications industry.

With the advent of computers and their convergence with telecommunications, the PSTN adapted digital technology to provide improved services. The "Internet" came into existence as a massive network of networks, a networking infrastructure. It connects millions of computers together

globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. The “Internet” leverages PSTN for long distance transmission and thus most of the Internet service providers (ISPs) rely on the telecommunication providers. Data communication over telecommunication networks was made possible with new technology protocols like Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP).

The convergence of voice, data, audio and video has become a reality with the proliferation of Internet, wireless technologies and digital audio-video communication. Today, enterprises leverage telecommunication carriers’ abilities to transmit high speed multi-media content from head office to executives in the field.

While the Internet is information super highway, the World Wide Web (WWW) became the standard for accessing information over the Internet. WWW is an information sharing model that isbuilt on top of the Internet. It uses the Hyper Text Transfer Protocol (HTTP) to transfer data.

Classification of data networks: The data networks can be characterized and classified in different ways as follows:

1. Spatial distance, such as Local Area Network (LAN), Metropolitan Area Network(MAN),and Wide Area Network (WAN);
2. Topology or general configurations of networks, such as the ring, bus, star, tree, mesh,hybrid, and others;
3. Network ownership, such as public, private or virtual private;
4. Type of switching technology such as circuit, message, packet, or cell switching;
5. Type of computing model, such as centralized or distributed computing; and
6. Type of information it carries such as voice, data, or both kinds of signals.

From the supply chain domain perspective, we will study two important classifications, the spatialdistance and the network ownership.

Classification by Spatial Distance

The geographic spread of a network determines other factors like speed and ownership. There three types of networks: Wide area network (WAN), Metropolitan area network (MAN), Local area network (LAN). A WAN covers large geographical area and uses common telecom carrier to connect intermediate nodes. The WAN may be global or may cover only few cities. The WAN uses leased communication circuits from telecom companies or other communication carriers.

A MAN covers an area of between 5 and 50 km in diameter, about the size of a city. A

MAN is not generally owned by a single organization, but rather a consortium of users or by a single

network provider who sells the service to the users. Its customers are enterprises that need a lot ofhigh speed connectivity within a city.

A LAN is most common type of data network seen in industrial plants, office buildings, universities or similar locations. LAN is developed by organizations that want their own high quality, high speed communication links. E.g.an organization creates LAN to share its computer related resources like Enterprise resource planning system, collaboration portal… in its head officebuilding. The organization can share computer resources to its branches by connecting to MAN or WAN. The following table summarizes data networks classification by spatial distance:

	LAN	MAN	WAN
Geographic Spread	Less than 5 km	5 to 50 km	More than 50 km
Ownership	Private	Private / Public	Private / Public
Data Transmission Rate	Mbps to Gbps	Kbps to Mbps	Kbps to Mbps
Example	Industrial plants, Corporate offices, College campuses, Single departments	Chennai Metropolitan Water Supply and Sewage Board connects its offices across the city	Life insurance Corporation of India connects offices in different cities using leased lines
Supply chain application	Connecting computers in side corporate back office	Connecting retail outlet branches inside city	Connecting branch offices across cities

Classification by ownership

Data networks are classified according to ownership in three types: Public networks, Private networks and Virtual private networks (VPN).

A *Public Network* refers to a network owned by a common carrier for use by its customers. PSTN is a public network generally operated by government owned company or recognized private company. The capital and operational costs of the network are shared by number of users making the carrier achieve good network utilization and high quality service at a reasonable cost. Example of public network application is usage of internet service provided by BSNL for transmitting emails to trade partners.

A *Private network* is developed exclusively for use of a single organization, typically when traffic among organization business locations is very high. This may save data transmission cost and gives the organization full control of the network's operation and high security. Example of a private network is connecting a retail chain's internal auditing department's computers for high volume data processing.

A *Virtual private network* combines the advantages of both private and public networks. VPNs are secured channels through a shared private or public network that transmit data over shared or dedicated leased lines. It provides the security of a private network through encryption of data and savings in cost through public and shared infrastructure for data transmission. However, highly sensitive corporate information may not be shared over VPNs as they can pose potential security challenges. Example of the VPN application is a multinational company's enterprise system connecting various offices and supply chain partners across countries.

2.3 DATA SECURITY IN SUPPLY CHAIN NETWORKS

Efficient and effective supply chain management requires sharing of information about orders, shipments, products, designs, demand forecasts and inventory in any form of media (voice, print ordigital). Enterprises often create communication networks with supply chain partners to share such information. Research [3] indicates that there three types of threats that may arise while sharing information in supply chain communication networks:

a. Direct loss of proprietary information to rivals
b. Compromised bidding systems
c. Supply chain IT system malfunction

Direct loss of proprietary information to rivals: It can lead a company to forfeit its competitive advantage. It can occur through competitive business theft, inference by suppliers, and transfer of information by employees or general hacking.

Competitive business theft can happen while sharing the proprietary data shared with suppliers that may reach business rivals in the industry. For example, Siemens Westing House Power Generation (SWHPG) has partnered with its rivals for reduced costs and overseas expansion. It shared sensitive designs with them which were then found copied by some unauthorized people leading tofinancial loss.

Transfer of information through human resources occurs by acquisition of employees of rival company specifically because of their knowledge (experience, training and proprietary information). Though such transfer could be limited through non-disclosure agreements or non-competitive contracts, enforcement is the not easy. For example, General Motors employee was employed by Volkswagen for sensitive design, purchasing and sales information causing financial loss to General Motors. Even the highly trusted employees can leak proprietary information unknowingly or for a price. This is one form of competitive business theft called as "social engineering". For example, a highly trusted employee of Ellery systems in Colorado transferred a million dollar worth software to a competing Chinese company.

Generalized hacking or computer penetration is a serious form of threat. Generalized hacking of large information systems that contain proprietary information could be done by disinterested thirdparty not for stealing proprietary data, but for causing damage or loss of data. For example, the hacking attacks on Sony Records, Amazon and Burger King lead to either website damage or denial of service or both.

Compromised bidding systems: The compromised bidding systems can lead to significant cost increases due to artificially high bid from suppliers. This may happen while using e-procurement systems to facilitate reverse auctions. Each supplier is naturally inclined to know their rivals bids. For example, the US General Services Administration online bidding system had a security flaw. One of the authenticated bidders had access to access and even to change competitor bids of rival contractors. The online system was shut down for almost a week to rectify the security flaw.

System malfunction: The system malfunction or system freeze of supply chain information technology can cause delays and ordering mistakes. For example, Nike encountered major difficulties in implementing i2 forecasting and supply chain software. The result was poorly placed orders for East Asian suppliers leading to financial loss. Another example is from the digitally operated railways. CRX rail transportation was forced to shut down its central control dispatching center because of computer virus leading to disruption in transportation of goods in many supply chains.

[3] Darian Unger and Rajni Goel, "Sharing and guarding information: managing data security in supply chainnetworks, Alliance journal of business research.

Framework for data security

High degree of care should be taken about the degree of information sharing and protecting data security. Increasing the level of information sharing with supply chain partners may increase efficiency, but selective sharing will increase the effectiveness. It requires an intelligent systemthat controls the degree of information sharing. The above mentioned categories of threats can be countered using a combination of information technology security tools usage and HR / Business policies enforcement. The IT security tools include access controls, firewalls, encryption, intrusion detection systems and authentication. The HR and business policies include non-disclosure, non- competitive agreements and monitoring of individuals and suppliers to avoid competitive business thefts and supplier inference.

Security standards like the British standard for information security management (BS 7799) should be implemented. Following such standards will ensure compliance with legal requirements and allows enterprises to achieve level of trust required to trade securely with supply chain partners. The use of BS7799 allows enterprises to develop information security management system (ISMS)in three steps:

1. Set goals and direction of information security through management framework for

information and security policy. Involve supply chain partners in developing the security policy.

2. Assess the risks related to information security and allocate contingent budgets. The impactof loss can be directly on the focal enterprise or indirectly in the form of risks to its customers and suppliers.
3. Implement security measures to keep the risk levels down to the acceptable level. Focal enterprise should be cautious while considering the comfort level of customers and suppliers in adhering to security measures.

The practical way of developing and implementing information security management systems is asfollows:

1. **Classify the data based on value:** The data can be classified in three levels of security as follows:

Security level 1 (low security classification)	Non-critical data that can be accessed by all employees, customers and suppliers through a password protected website. Example: inventory information.
Security level 2 (medium security classification)	Business critical data that should be kept confidential within the company or shared with select customers and suppliers. Such data has limited access through passwords and similar measures. Example: mailing lists, financial information
Security level 3 (high security classification)	Private information, access to be strictly controlled. It may be necessary store this information in encrypted format. Example: Credit card details

2. **Identify threats:** The threats come in two basic forms – malicious threats and accidental threats. Malicious threats include hackers, disgruntled employees and supplier inference. Accidental threats include system failures, internet born viruses. In highly networked supply chains that share electronic information, security threats from supply chain partner's systems shall also be considered.
3. **Identify weaknesses:** Collaborative supply chains require trust. In addition, it's necessary to be aware of the vulnerabilities in the supply chain. The supply chain is as strong as its weakest partner. Weaknesses should be identified in the light of risks considered. Some of the areas to be questioned are backups, regulations and accessibility from both the focal enterprise and its supply chain partners' perspectives.
4. **Establish countermeasures:** These include external backups, firewalls, virus protection programs, token passwords, software to monitor internet and extranet traffic.
5. **Managing risk:** The security policy must include regular reviews of the situation. Key supply chain partners should be involved in any reviews as truly effective security measures work for the whole supply chain.