WHITE PAPER

IP-based Networks: Basics

TABLE OF CONTENTS

1. Introduction

Modern digital technology allows different sectors, e.g. telecom, data, radio and television, to be merged together. This occurrence, commonly known as convergence, is happening on a global scale and is drastically changing the way in which both people and devices communicate. At the center of this process, forming the backbone and making convergence possible, are IP-based networks.

Services and integrated consumer devices for purposes such as telephony, entertainment, security or personal computing are constantly being developed, designed and converged towards a communication standard that is independent from the underlying physical connection. The cable network, for instance, first designed for transmitting television to the consumer, can now also be utilized for sending e-mail, surfing the Web or even monitoring a network camera sending live pictures from another continent. Furthermore, these features are also available over other physical networks, e.g. telephone, mobile phone, satellite and computer networks.

This white paper introduces the central components of IP-based network technology, and in doing so it will demonstrate the tremendous benefits this new technology has to offer.

2. Basics in network communication

The Internet has become the most powerful factor guiding the ongoing convergence process. This is mainly due to the fact that the *Internet protocol suite* has become a shared standard used with almost any service. The Internet protocol suite consists primarily of the *Internet Protocol (IP)* and the *Transport Control Protocol (TCP)*; consequently, the term *TCP/IP* commonly refers to the whole protocol family.

IP-based networks are of great importance in today's information society. At first glance, this technology might appear a bit confusing and overwhelming. Therefore, we'll start by presenting the underlying network components upon which this technology is built.

A network is comprised of two fundamental parts, the nodes and the links. A node is some type of network device, such as a computer. Nodes are able to communicate with other nodes through links, like cables. There are basically two different network techniques for establishing communication between nodes on a network: the *circuit-switched network* and the *packet-switched network* techniques. The former is used in a traditional telephone system, while the latter is used in IP-based networks.

A circuit-switched network creates a closed circuit between two nodes in the network to establish a connection. The established connection is thus dedicated to the communication between the two nodes. One of the immediate problems with dedicated circuits is wasted capacity, since almost no transmission uses the circuit 100 percent of the time. Also, if a circuit fails in the middle of a transmission, the entire connection must be dropped and a new one established. For illustration purposes, take a look at a telephone connection over a circuit-switched network (Figure 1).

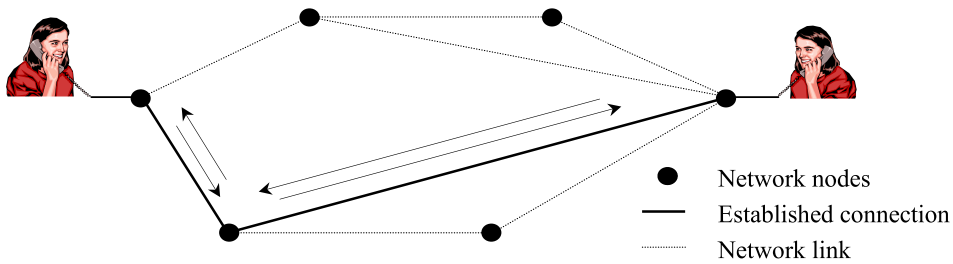

Figure 1: *A circuit-switched network utilizes a dedicated closed circuit*

IP-based networks on the other hand utilize a packet-switched network technology, which uses available capacity much more efficiently and minimizes the risk of possible problems, such as a disconnection. Messages sent over a packet-switched network are first divided into packets containing the destination address. Then, each packet is sent over the network with every intermediate node and router in the network determining where the packet goes next. A packet does not need to be routed over the same links as previous related packets. Thus, packets sent between two network devices can be transmitted over different routes in the event of a link breakdown or node malfunction (Figure 2).

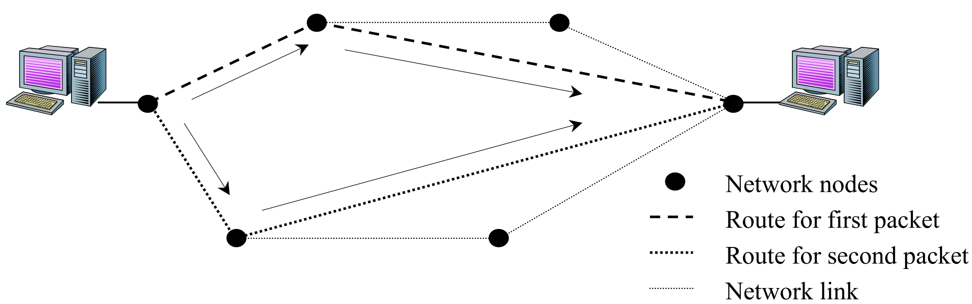

Figure 2: *A packet-switched network routes each packet independently*

3. Transmission Fundamentals

IP-based network solutions are both flexible and economical substitutes for solutions that utilize old network technologies. The diverse properties between these technologies result from how information is represented, transmitted and managed. Information is simply structured collections of data, and thus takes its meaning from the interpretation we give it. There are two fundamental types of data, analog and digital, and both possess different behaviors and characteristics.

Analog data is expressed as continuously variable waves and thus takes on continuous values. Examples include voice and video.

Digital data on the other hand is represented as a sequence of bits, or *ones* and *zeros*. This digitization allows any kind of information to be measured and represented as digital data. So, text, sound and pictures can be represented as a sequence of bits. Digital data can also be compressed to allow higher transmission rates and it can be encrypted for secure transmissions. In addition, a digital signal is exact and any related noise can easily be filtered out. Digital data can be transmitted through three general types of media—metal such as copper; optical fiber or radio waves.

The techniques represented below offer the first building block for digital communications, the *cable and antenna layer* (Figure 3). This layer allows us to send and receive digital data over a wide variety of media. However, more building blocks are required for successful digital communication.

Cable and antenna layer

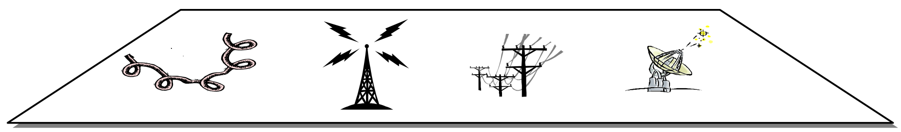

Figure 3: *Cable and antenna layer – the first building block*

4. The Local Area Network Infrastructure

This section will go one step further by discussing digital *communication*. You might ask, “What is the difference between transmission and communication?” Consider an analogy from human speech. Think about the acoustic waves in the air generated by speaking. These waves are transmitted, but they are a long way from communicating. The words that come out must be organized to make any sense. If they come out to quickly or too slowly, the speaker will not be understood. If many people speak simultaneously no one is understood. If someone speaks a language you don’t understand, information is lost. Speaking generates information, but it is not necessarily communicated, or understood.

Digital communication has similar problems that need to be overcome. The receiver must know how message bits are organized to understand the message. The receiver must know the rate at which the bits are arriving to interpret the message. Additionally, some rules must specify what will happen if many network devices try to use a shared media simultaneously. The best way to ensure that network devices send and receive in compatible ways is to adhere to standardized *protocols* that define the rules and the manner in which the devices initiate and carry on communication.

We have until now focused on communication between two network devices. However, several different connection strategies and protocols exist that can be used to maintain communication among many network devices.

Local Area Networks (LANs) are used for connecting network devices over a relatively short distance. Typically, a LAN operates in a limited space, such as an office building, a school or a home. LANs are usually owned and managed by a single person or organization. They also use certain specific connectivity technologies, often some type of shared media.

An important feature of a LAN is its topology, where the term *topology* refers to the layout of connected network devices on a network. We can think of topology as a network's shape. Network topologies can be categorized into the following basic types:

- The **bus topology** uses a shared communication medium, often referred to as a common bus, to connect all network devices (Figure 4). A device that wants to communicate with another device on the network sends the packet onto the bus. All devices that are connected to the bus will receive the sent packet but the intended recipient is the only device that actually accepts and processes the packets.

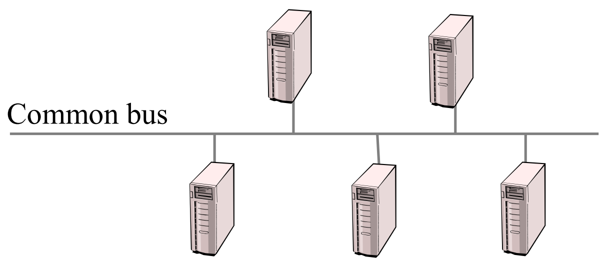

Figure 4: *Bus topology uses a common bus to connect network devices*

- The **ring topology** is structured in such a way that every network device on the network has exactly two neighbors for their communication purposes. All packets travel along a ring in the same direction (Figure 5).

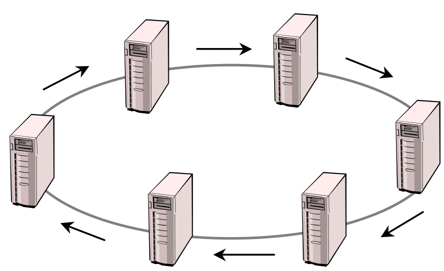

Figure 5: *Ring topology uses a ring structure to connect network devices*

- The **star topology** features a logical communication center to which all network devices are directly connected. Each device requires a separate cable to the central point and consequently all packets will travel through the communication center (Figure 6).

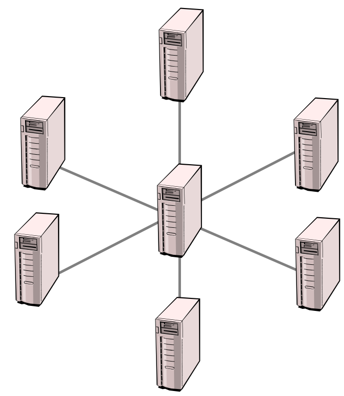

Figure 6: *Star topology uses a star-shaped network to connect network devices*

There are several different protocols that can be utilized together with each network topology. Aside from identifying the standards of communications between the network devices, a protocol sets the technical specifications needed to transmit data within a network. To transmit a message to another device in a network, the message is split into *data packets*. These data packets are then transmitted via the communication media and are reassembled again at the receiving end.

The standardized protocols utilize different network topologies together with the cable and antenna layer to build different LAN architectures that are either wired or wireless. These protocols offer the second building block for successful digital communications, the *transmission layer* (Figure 7).

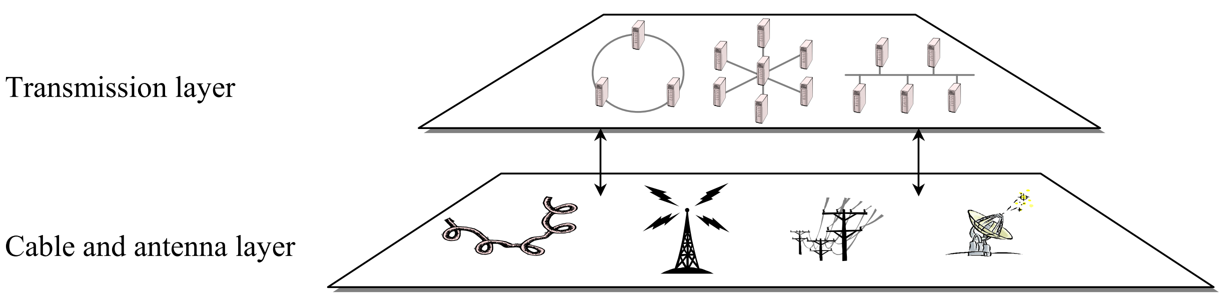

Figure 7: *Transmission layer – the second building block*

5. Interconnecting LANs in an IP-based Architecture

So far, we have described how network devices can communicate over different types of LANs. However, different LANs are designed for different goals and needs. Hence, every so often it is necessary to interconnect several LANs to allow communication over the network boundaries. Such a geographically scattered, interconnected collection of LANs is commonly referred to as a *Wide Area Network (WAN)*. Probably the most familiar WAN is the Internet, which spans most of the globe.

Shared communication architecture is required for all users, such as private persons, enterprises, public administration offices and other organizations, to be able to exchange digital information with one another over a WAN. This architecture should be an open standard and support different transmission layer protocols, particularly those that can be used over a variety of transmission media. Fortunately, the Internet protocol suite provides a well-designed solution that fits these requirements.

5.1 The Internet protocol suite

The Internet protocol suite is a layered protocol family where each layer builds upon the layer below it, adding new functionality. The lowest layer is concerned purely with sending and receiving data utilizing the transmission layer. At the top are protocols designed for specific tasks, such as sending and receiving motion pictures, sound and control information. The protocols in between handle things such as dividing the message data into packets and forwarding them reliably between network devices.

5.2 Internet Protocol

The Internet Protocol (IP) is the basis of the Internet protocol suite and is the single most popular network protocol in the world. IP enables data to be transmitted across and between local area networks, hence the name: Inter-net Protocol. Data travels over an IP-based network in the form of *IP packets* (data units). Each IP packet includes both a header and the message data itself, where the header specifies the source, the destination, and other information about the data.

IP is a connectionless protocol where each packet is treated as a separate entity, like a postal service. Any mechanisms for ensuring that sent data arrives in a correct and intact manner are provided by higher-layer protocols in the suite.

Each network device has at least one IP address that uniquely identifies it from all other devices on the network. In this manner, intermediate nodes can correctly guide a sent packet from the source to the destination.

5.3 Transport Protocol

The Transport Control Protocol (TCP) is the most common protocol for assuring that an IP packet arrives in a correct and intact manner. TCP provides reliable transmission of data for upper layer applications and services in an IP environment. TCP offers reliability in the form of a connection-oriented, end-to-end packet delivery through an interconnected network.

5.4 An Internet Protocol suite summary

The Internet Protocol suite provides an adaptation to the transmission layer protocols and offers a standardized architecture for communication over an interconnected collection of LANs, i.e. a WAN. This is a tremendous advance, mainly because we're able to connect and communicate over different physical connections in a standardized way. With IP as the basis, the Internet Protocol suite provides the third building block for successful digital communications, the *IP layer* (Figure 8).

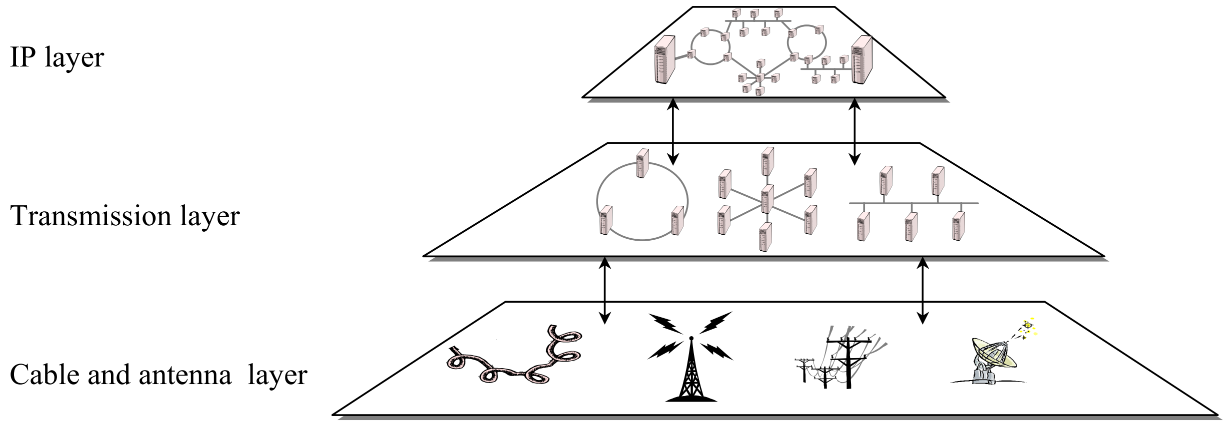

Figure 8: *IP layer – the third building block*

6. Benefit from the IP-based Architecture

The Internet Protocol suite brings together all transmission layer protocols into a single, standardized protocol architecture, which can be utilized by applications for different communication purposes. As a direct result, any application that supports TCP/IP will also be able to communicate over any IP-based network.

It should be easy to see that this standardized architecture has revolutionized network communication. An ever-increasing number of applications that transfer text, sound, live pictures and more utilize IP-based architecture. All these applications and application protocols constitute the *application layer* and provide the fourth, and final, building block for successful digital communications (Figure 9)[1].

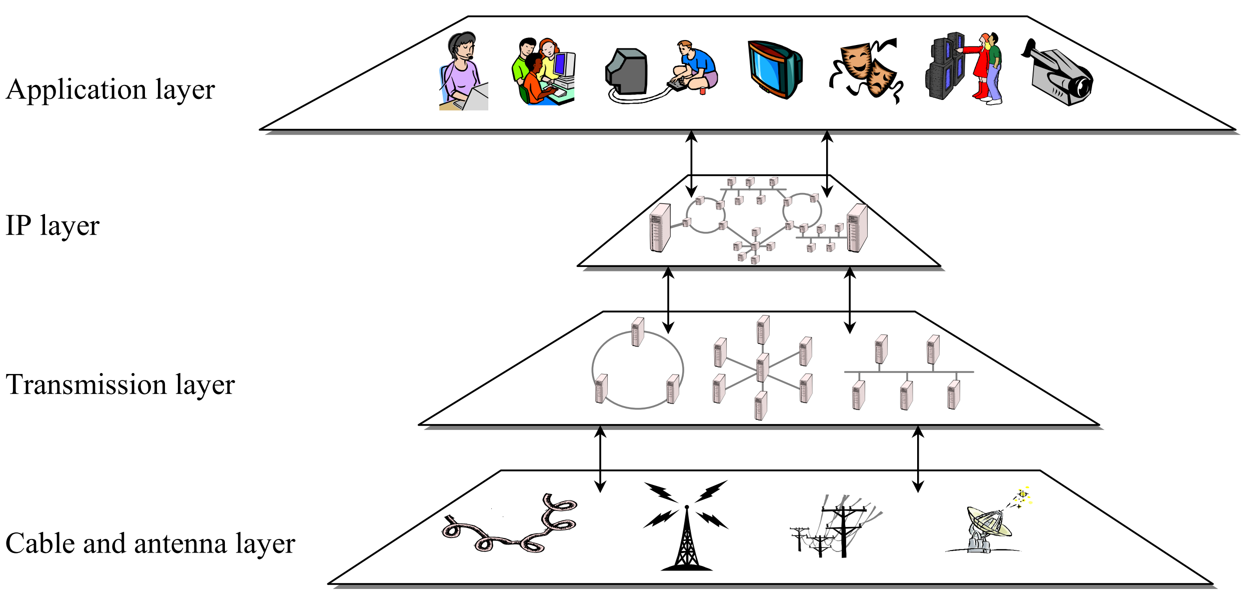

Figure 9: *Application layer – the fourth building block*

[1] Please note that this is a simplification of the Internet Protocol suite. Visit IETF for full details. http://www.ietf.org/

7. Convergence

Modern digital technology allows for convergence where different services, and combinations of these services, can be provided through infrastructures that formerly accommodated only one type of service. There are three major factors that create the conditions for convergence: digital technology, transmission technology and standardized communication protocols. Digital technology allows all information—text, sound and motion pictures, for example—to be represented as bits and transmitted as sequences of ones and zeros. Transmission technology enables better utilization of available capacity in different infrastructures. Consequently, services that require high capacity can be provided by infrastructures previously able to deliver only simpler services.

We have already seen how IP-based technology provides an excellent architecture for the process of ongoing convergence. At the heart of the Internet Protocol suite is the Internet Protocol, which represents the building block that uniformly connects different physical networks with a variety of applications. In addition, presently available IP-based solutions can be fully integrated with other available systems.

7. Case Study

So far we have discussed the structure of the IP-based architecture, especially in comparison with traditional circuit-switched networks. However, the preceding sections have not contained any real applications that take advantage of this architecture. IP-based architecture creates great opportunities for new application domains. Hence, applications that previously could not be realized can now be successfully implemented. Additionally, application domains built upon older technologies derive increased functionality when utilizing IP-based technology. For illustration, consider an application domain that has clearly taken advantage of IP-based architecture: visual surveillance systems.

In today's society, the demand for visual surveillance systems has been steadily increasing. Different camera solutions are used for monitoring activities in a variety of environments, such as shops, enterprise buildings and prisons. Up until recently, Closed Circuit Television systems (CCTV systems) were the only alternative for such monitoring. These dedicated systems typically require their own communication link between the camera and the monitor. This separate link is expensive to buy, install and maintain. Camera images are transmitted over the dedicated cabling network to time-lapse video recorders or dedicated monitors at a control center.

A modern IP-based visual surveillance system on the other hand is not limited in the same way as a traditional CCTV system. Enterprises can install *network cameras,* IP-based visual surveillance cameras that plug directly into the enterprise network. Such cameras have their own IP address, much like any network device. The main differences between these systems and CCTV systems are that video digitization is performed at the camera level and the Internet Protocol suite is utilized for transferring the pictures onto the network. This is beneficial since IP-based networks are generally available in most buildings, and because TCP/IP can be utilized with almost any existing network, there is probably no need for extra cabling. A network camera system, in comparison with a CCTV system, also saves money by reducing the amount of dedicated equipment needed to manage the security system. For example, no dedicated monitors are required.

An IP-based solution also allows images to be remotely stored and monitored over any interconnected network, such as the Internet. This alone creates huge advantages for enterprises that wish to outsource the monitoring of their offices and facilities to a third party surveillance and monitoring center. This center simply needs a password and the IP-address to access live pictures, via the Internet, from a camera placed anywhere in the world. Moreover, the IP-based architecture creates a new world in which different applications can be completely integrated. For instance, motion pictures can be distributed to other network solutions, such as factory control management systems and access control systems.

8. Conclusion

The Internet Protocol suite has rapidly grown into a widespread, fundamental building block for information exchange. As communication technology becomes increasingly important, there is growing pressure to use this technology to reduce costs without sacrificing any capabilities or benefits. IP-based networks address many of the problems faced in this complex environment, while providing an elegant solution that meets present needs, as well as those to come. Ultimately, all forms of communications, including data, voice, motion pictures and entertainment, will converge into a common transporting network.

The primary benefits of an IP-based network strategy are the cost savings and operational improvements from using one converged network instead of several smaller networks dedicated to specific purposes, like data, voice and motion pictures. The second most important group of benefits from network convergence is in enabling new applications. New applications not only drive cost reductions; they can also be a source of new revenue as they provide value essential to enterprises and users.

Convergence is here and the benefits are real. Now it’s time to pick strategic partners--those who understand the broad scope of needs and are committed to meeting them--and take the first step towards an IP-based future.

Axis Communications

Axis develops solutions for user-friendly and secure communication over wired and wireless networks. The company is a worldwide market leader in network connectivity, with products for office, facility and industrial environments. Axis was founded in 1984 and is listed on the O-list (Attract 40) of Stockholmsbörsen (XSSE:AXIS). With more than 300 employees, and offices in 14 countries, Axis operates globally in cooperation with distributors and OEM partners in some 70 countries. Markets outside Sweden account for more than 95 percent of sales.

Information about Axis can be found at www.axis.com

Contact Axis

info@axis.com

Head office, Lund

Axis Communications AB
Emdalavägen 14
SE-223 69 Lund
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

Subsidiaries

BOSTON:
Phone:+1 978 614 20 00

MIAMI:
Phone:+1 305-860-8226

LONDON:
Phone:+44 20 7553 9200

MADRID:
Phone:+34 91 803 46 43

MUNICH:
Phone:+49 811 555 0810

PARIS:
Phone:+33 1 49 69 15 50

ROTTERDAM:
Phone:+31 10 444 34 34

TURIN:
Phone:+39 011 841 321

HONG KONG:
Phone:+852 2836 0813

SEOUL:
Phone:+82 2 780 9636

SHANGHAI:
Phone:+86 21 6431 1690

SINGAPORE:
Phone:+65 836 2777

TAIPEI:
Phone:+886 2 2546 9668

TOKYO:
Phone:+81-3-5531-8041

SYDNEY:
Phone:+61 2 9967 5700

KUALA LUMPUR:
Phone:+60 3 2474 582

