*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 4, Ver. II (Jul - Aug .2015), PP 63-71*
*www.iosrjournals.org*

# A new Telecom Architecture for the Convergence of TDM with IP and usage in Internet of Things

Engr. Irfan Khan
*(Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan)*

***Abstract:*** *Historically, Telecom Networks were a Mixture of TDM/Circuit Switched and Packet/Datagram based and used techniques such as TDMoIP and IPoTDM for internetwork communication. Voice and Data Networks were separate. NGN was envisioned as a pathway towards a converged ALL-IP network capable to cater to Voice, Video and Data services. Around 2005, newer services such as SAN's, NAS's, CDN's, WSNs, Location Aware Services, BYOD, Data Centers, Cloud-Based Services, Big Data, XaaS, Internet of Things, Over-the-Top Content etc. were developed that required a more Flexible and Scalable network infrastructure. These services are Application Focused and require the network to be more Service-Centric than Infrastructure-Centric. This gave rise to the Concept of Software Defined Networks (SDNs) and Network Function Virtualization (NFV). However, these concepts saw strong opposition from Telecom Equipment Manufacturers and it was not until late 2010 that Telecom OEMs started adopting SDN and NFV. This research tries to develop a Simple and Modular Router/Protocol that implements Telecom Functions as opposed to the more complicated and complex concurrent telecom networks.*

***Keywords:*** *Internet of Things, Next Generation Networks, Routing Tables, SCADA, XaaS (Anything as a Service)*

## I. Introduction

NGN contains a plethora of Protocols and Sub-protocols which makes NGN sophisticated and complicated day by day with the addition of newer technologies beyond Triple-Play i.e. Voice, Video and Data. At times, the number of protocols required to perform a simple task such as transfer a single SMS message over an NGN network is very large. The network is very much complicated and sophisticated. It requires a very large setup for Operations and Maintenance as well as Troubleshooting. The need for a simpler network is thus imminent. With the addition of more sophisticated technologies to NGN it became more complex. The problem is complicated by the fact that NGN also has to be backward compatible with older technologies. NGN cannot discard reliance upon the protocols required to connect with Legacy Networks. Thus NGN has become a set of Hundreds of Protocols further subdivide into many sub-protocols.

Further amalgamation of NGN with PSTN and PLMN resulted in a Hybrid Network referred to as the Intelligent Network or simply the IN. With the arrival of newer technologies such as IP Multimedia Subsystem or IMS, NGN became one of the most sophisticated technologies ever deployed by mankind. This complication can be removed with the Introduction of a new and simple protocol which is the main objective of this research.

## II. The Proposed System for Simple Telecommunications

This research paper tries to propose a new telecom architecture which is very simple and is robust enough to carry out all the functions of the concurrent telecom networks deployed. It is especially suitable to be deployed in and Internet of Things environment because of its simplicity and low consumption of equipment resources such as processing power and memory. From this point onwards, a set of terminologies would be used to refer to the following items as, until or unless otherwise indicated:

1. The proposed equipment would be referred to as THE MACHINE.
2. The proposed protocol would be referred to as THE PROTOCOL.
3. The Information/Data/Message that passes from one node to another would be referred to as The Message or The Stream.
4. The information used to route the message would be referred to as SIGNALLING.

The Machine runs a Protocol on Hardware that performs the following two distinctive functions:

1. It directly communicates with its peer Machines and exchanges Streams and Signaling.
2. It Translates the Messages between Legacy and IP Networks and then does the reverse at the receiving end.

The Proposed Machine can transfer four types of Streams or Data, namely:

1. Different types of Broadband and Narrowband Data and Streams including but not limited to Voice, Video, Text, Files etc data which is the actual payload
2. Signaling data required for the transmission/reception, end to end delivery and format conversion of the payload data
3. Command Tool chains that are different types Commands delivered to end devices for Network of Things or Internet of Things Services.
4. Commands for the Human Network Interface (HNI) that are delivered for end devices for the Human Layer Services.

## III. Modular Design of the System

The main theme of this Router System is that it doesn't actually consist of a strict routing protocol in the real sense. It is a mere set of Rules which define how Proprietary Protocols and Buses can be used inside a router to control and populate a Routing Table, Manipulate the Data Stream and then the same Routing Table can be used to Route and Change the Transmitted and Received Data. Thus using Proprietary Protocols inside a Router, It can be used to Interact with Standardized protocols interfaced from the outside world with the Router. The use of proprietary protocols will enable vendors to accelerate all the processes in a much efficient manner while still keeping the interfaces compatible for both data and signaling.

The above proposition enables the router to be very much modular. Thus the main theme of this architecture is that it is very much modular enabling the modules to be very much versatile in their Physical Form and Scale. Depending upon the Scale and Traffic Load of The Router, the modules may be Independent units such as Hybrid ASICs, DSPs, FPGAs, Microprocessors, Microcontrollers or even Individual Computers. Also the same router can be implemented in Software on a Single IC or Computer so that each module is a Logical Software Module performing the same exact hardware functions. The machine can also be implemented on boards such as Raspberry Pie, Beagle-Board, and Arduino etc.

This modular scheme also enables the designer to create multiple systems within a single hardware equipment by using various available technologies of Virtualization. The hardware can then accelerate the system according to its various proprietary features. The concept of modularity enables the MACHINE to support both Centralized Architecture and Distributed Architecture. In a Distributed Architecture, some of the modules may be located at geographically remote locations while performing the same function [1]. Modularity also enables the machine to support Redundancy. This is advantageous as failure of one module would not support the whole Machine. Redundant modules can be used as Backup in Machines catering to Critical and Real-time networks such as SCADA or Telemetry etc.

This new Protocol is the soul of a Router Machine that will revolutionize the connectivity of non-compatible Protocols/Equipment. In order to manage and run different parts of the protocol on the machine, we require an Operating System which must be capable of running and scheduling all the tasks in real-time. Several Open Source Real Time Operating Systems are available. Specialized Network Operating Systems are also available which can cater to the needs of a particular networking task [2]. This selection of modularity and Open Network RTOS makes the proposed machine closer to the concepts of Software Defined Networking and Network Function Virtualization.

## IV. General System Architecture

In order to make the system more modular, the Machine been divided into smaller components or modules. There are Five Core Components of the proposed Protocol that maybe implemented in Hardware or Software. Each of these core components is connected via buses to other components. Thus these Core Components work together by coordinating through the buses and performing different functions. Additional components may be added depending upon the requirements of the system. However, following core components are a bare minimum requirement for the proposed system:

1. Main System Controller
2. Router
3. Codec or Trans-Coder(Compression and Decompression)
4. Protocol/Format Converter
5. Interfaces
6. Firewall/NAT

Fig. 1 shows the proposed Architecture with Core Modules, Buses and the Timing Module. Examples of additional components may include:

1. Input and Output User Interface Modules such as LEDs/LCDs and Keyboards/Push Buttons etc.
2. Clock/Synchronization Module
3. IDS and Honeypots( may be incorporated into the Firewall)
4. Power Supply and Power Supply Controllers
5. Environmental Sensor Modules (Temperature, Humidity etc.)
6. Proximity Sensors such as door sensors etc.

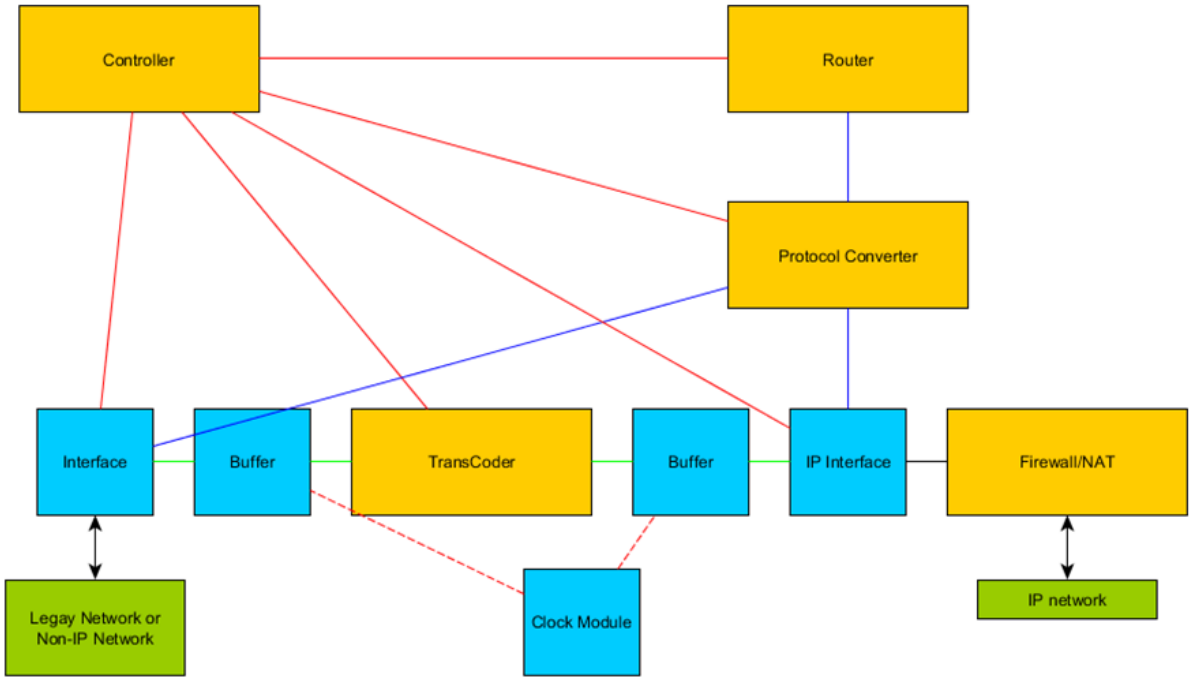


**Figure: 1.** The Modules and Buses used in the Machine along with the Clock/Timing Module and Bus

### 4.1 Main System Controller

As the name implies, the main task of the System Controller is to Control and Coordinate the overall function of the system including but not limited to:

- Running the Network RTOS (on standalone units)
- System boot and initialization
- System Reboot (Warm & Cold)
- System Maintenance
- Power Control
- Module Coordination
- Alarm Collection
- The controller interrogates all the components for Status
- System Watchdog
- System Configuration, its Storage and Retrieval
- SNMP Agent
- User Access and Management Control
- It is also responsible to coordinate partly in WAN Acceleration.

Another key and most important function of the System Controller is the Synchronization of the overall Machine. It will thus generate a Reference Signal by itself or retrieve it from some external module and then distribute the signal via the Clock Bus for Intra-Module Synchronization. It can also Distribute the same signal for clock synchronization via the External Timing Interface or via the Data Links for Inter-Router Synchronization. An External Clock Source may be a GPS derived clock or another Router.

The Controller also maintains user credential schemes used to Authentic other Routers or Users. It also maintains session logs for security purposes.

**4.2 Router**

The primary Duty of the Router is to gather data from Legacy/No-IP Protocols and then use the same data to Populate a Routing Table. Afterwards, it uses the same table to deliver the data to its destination. The router also uses contemporary IP protocols to obtain information about Destination Routers such as OSPF, RIP, BGP etc. The Router contains a number of Tables that are used to maintain the routing information. There are different types of tables which are used for the end-to-end and hope-to-hope delivery of the streams. Also there are tables which are used for the manipulation of stream data and signaling data from one format to another for use in different types of equipment and scenarios.

The router is also responsible to coordinate with other routers in order to keep info about the status of the various available links. It may get following information about a link:

- Link Status
- Link Availability
- Link reliability
- Link Latency
- Link Throughput/Speeds etc.

The Router can also get information from other neighboring routers via the BEACON Signals by listening to them on specific ports. It then uses this data to manage the end-to-end links for data transfer keeping in view the data requirements in an optimized manner. The router also carries out advanced functions such as WAN Acceleration and Multi-homing of Data Links via the INTERFACEs. The router can set priority of different links towards the same destination i.e. it can Prioritize links and also manage multiple links for same destination.

The router also takes care of Traffic Shaping and Bandwidth Management by controlling the INETRFACEs. It can attach different priorities to different types of traffics. For example it can give more bandwidth to real-time time traffic such as SCADA, Voice Streams, Video Conferencing, IP Telephony and IP TV. It can allot lower bandwidths to non-interactive services such as FTP, HTTP and Torrents etc. In order to do so, it must maintain and manage different traffic queues for different types of traffic. The Router does Latency Compensation via the Buffers. The router also uses the Buffers to manage Jitter and Wander. The overall data routing is thus managed by the router.

**4.3 Codec**

The Codec performs various functions related to the transformation of the Payload i.e. it manipulates the stream in a way which is much efficient for its transfer across the network. This may be performed in a number ways but these methods are specific to different forms of Data/Streams. For example we may compress text messages and HTML files on the fly. We may change a Bitmap Image to a JPEG Image which will reduce its size. We may change the Audio Format of an Audio Message or Audio Stream. The same is true for a Video File or Video Stream.

The Codec also preforms the Reverse function at the Receiver's End so that the messaging process is completed. However, it is not necessary in some cases to perform the reverse process as it may save time by not performing it. Also the reverse process may not be possible in certain cases. Some of the performed functions may include:

- Compression/Decompression of Plain Text
- Raster to Vector Conversion
- Format Change of Images
- Format Change of Audio & Video Streams
- Compression/Decompression of Audio and Video Streams

Another feature of the codec is that it is also modular or accepts pluggable modules for different types of messages and media. We can add modules or plugins for the different functions that it can perform. Thus codec on one machine may have modules for Image Compression and another one may have modules for Audio Compression. However, in order to communicate in a proper manner, both the sending and the receiving machines should have same or corresponding Modules in their Codecs. Each Machine also has a Capability Table which is used to store the types of Modules present in the Codec of that Machine.

**4.4 Protocol Converter**

The Protocol Converter Modifies the Signaling information of the message. The Protocol Converter obtains Signaling/Routing information from the receiver and then uses it to send the data to the destination. It has the following main functions while sending data from Legacy Networks to IP Networks:

- It obtains Signaling/Routing Information from the sender of Legacy Protocols.
- It obtains information about the Destination Routers from the Routing Table and adds it to the Message data.

While sending data from IP Networks to Legacy Networks, it does the reverse of the above process i.e. it uses address information from the IP header with the routing table and adds the info to the outbound message so that it may successfully reach its destination. It is not necessary that the machine sends streams between Legacy and IP Networks as it may be used to connect one type of Non-IP Network to another Type of Non-IP network. So, the Protocol Converter should also be capable to cater to these needs.

### 4.5 Difference between Codec and Protocol Converter

The main difference between the Codec and Protocol Converter is that the Codec is used to modify the Actual message or the Payload while the Protocol Converter is used only to modify the different types of Address information or Headers. However, both obtain the required manipulation information from the various types of modules present in the Machine. The Codec obtains the necessary information from the Capabilities Table while the Protocol Converter obtains information from the Interfaces.

### 4.6 Interfaces

As clear from the name, the Interface modules interface the machine with different types of Networks/Environments. Depending upon the types of these networks, the Interfaces may be divided into several types.

**According to the type of protocols, an interface may be:**

- An IP Interface
- A Non-IP Interface

**Interfaces may also be:**

- Analog Interface
- Digital Interface

**Also, an Interface may be:**

- Simplex
- Half Duplex
- Full Duplex

**According to another classification, an Interface may be:**

- Unidirectional/One Way
- Bidirectional/Two Way

The Machine may utilize different type of GPIO interfaces nowadays being used by the different types of open-source boards and DSP Processors such as Arduino, Beagle-Board, and Raspberry-Pie etc. The Interface is not a just a Physical Connector but is in fact a fully functional module which supports all the functions required to send or receive data over a Physical link or Network. It can also support functions such as Error Correction. Chip Manufacturers generally refer to these modules as PHYs [3]. The Openness in usage of different types of Interfaces and Payload Data brings us closer to the concepts of Internet of Things and Anything Over IP [4].

### 4.7 Buses used in the System

The system consists of three essential buses used for the exchange of data between the modules. There is also another Timing Bus but it is optional and not necessary in each system. The following is the description of each bus:

1. The Control Bus is used to pass control data and alarms on the system. It serves to pass on the telemetry data about the overall system status and performance by the different modules to the system controller. The system controller uses it to collect the alarm data from each module as well. It's shown as red lines in Fig. 1.
2. The Signaling Bus is used to share Legacy Signaling information between the Input Interface Module and the Protocol Converter module. It is also used to share the routing Protocol info between the Output Interface, the Protocol Converter and the Router. It's shown as Blue lines in Fig. 1.

3. The Data Bus is used to carry the Payload Data between Input Interface Module to the Output Interface Module. The Data Bus carries the data in both the formats while is being converted in the Transcoder. It's shown as Green lines in Fig. 1.
4. The Timing Bus is used to carry the Timing and Clock Sync information between from the Optional Timing module to the Buffers. It's shown as red dotted lines in Fig. 1.

The Concept of Bus is somehow comparable to the concept Northbound and Southbound Interfaces used in Software defined Networking.

## V. Routing Table Architecture and The Entity

The Real Essence of this Protocol is the definition an Entity. An Entity Defines an Individual Item that can be addressed by the Routing Table and with which it can Establish a Connection and Send or Receive a message. In other words an Entity can Transmit or Receive a Data Stream. Entities can be Sub-scaled or super-Scaled. Individual Entities can be subdivided into smaller Sub-Entities or they can be combined to form a Super Entity. This would help in clustering networks. It may be especially useful in services such as SANs and Computer Grids etc. Sub-Entities may refer to Logical or Physical Ports on the Same Super Entity. Thus a single Machine itself can comprise of several entities i.e. Interface Ports. The smallest possible entity can be a:

- TCP port + IP
- UDP port + IP
- VPN ID + IP
- Physical Ethernet Port + IP
- Physical Ethernet Port + MAC Address
- Physical Ethernet Port+ VPN ID
- Physical Ethernet Port+ VoIP ID

Thus an entity may refer to an Single Machine, a Collection of Machines or an entire Network. An entity may also refer to a single port of a machine or a collection of similar ports.

### 5.1 The Entity ID

An Entity ID is an ID used to refer to a specific Entity within the routing table of a router. It is thus the Name or Alias of an Entity within a certain router's routing table. Each Entity will have a unique ID in the routing table of a specific system. However, each Entity may be represented by a Different Entity ID in the routing table of another router. The Entity ID is thus only an Index or Reference to the Location of the Entity in the Routing Table. The Entity ID is a Pointer to a Register/Memory Location which can be either Local or Remote. One purpose to use Entity IDs instead of Real Entity Addresses is to reduce the size of the Routing Table. Thus the Routing Table will only store a pointer to the address of the Entity stored in the Entity Table. Another advantage of using Pointers to remote Registers for Entity IDs is that it enables the Machine to get addressing information from remote Routing Tables.

We will use the Notation En for an Entity, Pn for an Interface and Nn for a Network in the various tables. A particular interface of a particular machine may also be denoted by En.Pn.

### 5.2 The Routing Table

As the name implies, the routing table holds all the routing information required for estimating path metrics, establishing a connection and then successfully transferring the data from one node to another. The data may be transferred from one node to the next one or the data transfer may be end to end, depending upon the scenario. There can be two type of routing Tables depending upon the requirement of the Network Operator/Owner of the Router:

1. Local Routing Table
2. Remote Routing Table

As the names imply, the local routing table is stored on the local machine while the remote routing table can be stored on a trusted remote machine. The concept of remote routing table will enable the machines in a network to share the same routing table. Thus a single machine can Analyze the network trends and populate an efficient routing table. It can then share the same routing table with other machines in the network. This can be helpful to avoid network congestion and can help in network disaster recovery. It can also help in routing in networks where the Machines turn ON or OFF rapidly such e.g. sensor node networks or mesh networks [5].

The Routing Table stores the Entity IDs. Thus the Routing Table is actually an Array of Pointers. In other words, instead of holding the actual entity addresses, it holds the pointers to memory locations of those addresses.

### 5.3 The Routing Table and Example Scenarios

Table 1 is an example Routing Table of Machine with Entity ID E0. The remarks field is only used for explanation. It is not present in an actual Routing Table. We can later on Add Columns/Fields such as Status, Reliability however these fields form the basis of the Link Status Table and Capability Table etc.

**Table: 1 The Routing Table**

| No. | Metric/ Priority | Local Port | Route/ Network | Destination Entity | Destination Network Port | Next Hope H1 | Next Hope Hn | Remarks |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | P1 | N1 | E1 | E1.P1 | | | 1st path to E1 |
| 2 | 2 | P2 | N1 | E1 | E1.P2 | | | 2nd Path to E1, used for redundancy or low priority traffic |
| 3 | 3 | P3 | N2 | E1 | E1.P3 | | | 3rd path to E1via Network N2, used for redundancy or lowest priority traffic |
| 4 | 1 | P4 | N4 | E2 | E2.P1 | | | 1st Path to E2 via Network N4 |
| 5 | 1 | P5 | N5 | E2 | E2.P2 | | | 2nd path to E2 but with same priority, used simultaneously for Load Balancing as well as Redundancy |
| 6 | 1 | P6 | N6 | N6 | | | | Port used for Broadcast/Multicast to Network N6 |
| 9 | | | | | | + | + | + The Next Hope fields are used when we wish to use Strict Routing |
| 10 | | *Pn= E0.Pn | | | | | | * In the PORT column we can use Pn or E0.Pn |

### 5.4 The Entity Address Table

An Entity Address Table is the Storage Location of the Real Addresses of the different entities or machines. It is actually an Array of Addresses. Since the Entity IDs are actually Pointers so they point to the location of an Entity in the Entity Table. Table 4.2 is an example of an Entity Address Table:

**Table: 2 The Entity Address Table**

| Memory Register/Location | Entity Address |
|---|---|
| X | 192.168.1.10 |
| X+1 | 210.56.22.216 |
| X+2 | 210.56.20.21 |
| X+3 | 10.60.90.4 |
| X+4 | 10.50.60.2 |

Thus the Routing table is an Array of Pointers while the Entity Address Table is an Array of Addresses. The Memory Register/Location column is not a part of the Entity Address Table but has been shown to explain the memory location of the addresses.

### 5.5 The Connection Status/Session Table

The Session table or the Connection Status Table holds the all Information related to the Current Stream Queue being processed by the router or waiting in for being processed. Table 4.3 is an example of the Connection Status/Session Table:

**Table: 3 The Connection Status/Session Table**

| Message No. | Local Port | Remote Port | Queue Status | Initiation | Timeout |
|---|---|---|---|---|---|
| 1 | P1 | E1.P1 | Processing | Local | 60 Sec |
| 2 | P2 | E2.P1 | Waiting | Remote | 30 Sec |
| 3 | P3 | E3.P1 | Processing | Local | 60 Sec |

### 5.6 The Entity Capability Table

An Entity Capability table is used to store the capabilities of the Codec of a machine. The Machine can advertise its Capability table whenever it is queried by another Machine before establishing a connection. The remote machine then sends Streams according to the capabilities of the local machine. Table 4.4 is an example Capability Table of a Machine with Analog Audio, Analog Video and Ethernet Interfaces [6].

**Table: 4.4 The Entity Capability Table**

| No. | Capability |
|---|---|
| 1 | NTSC/PAL to MPEG(Bitrate, FPS, Resolution) |
| 2 | NTSC/PAL to AVI(Bitrate, FPS, Resolution) |
| 3 | Analog Audio to PCM(Bitrate, Sampling) |
| 4 | Analog Audio to MP3(Bitrate, Sampling) |

## VI. Example Configurations of the Machine

Since the machine is very much modular so, it can be used in a number of ways in different types of networks and different scenarios. This chapter shows some typical possible scenarios in which the machine can be used. Different types of modules can used inside the machine to fulfill the requirement of the network. By using different types of Hardware and Software modules in the machine, it can be used in a number of roles including but not limited to:

1. Media Converter
2. Router
3. Bridge
4. Gateway
5. Multiplexer
6. Address Register

Following example explains the scenario first and is then followed by the required modules/sub-modules and their configurations. This scenario uses an Analog CCTV camera and its transmission and storage over IP Network. It serves to connect an Analog Device to an IP-Network and also adds a few other features such as Camera Movement Control known as PTZ (Pan, Tilt and Zoom) and Video Storage. An operator sitting in a remote location can use and control the camera. He can also use a SAN [7] Server to store and retrieve video. These features are related to Remote Telemetry/SCADA [8], Internet of Things, Anything Over IP and SANs etc.

Following is the configuration of the modules in the machine # 01:

- Controller: The controller will have the capability to store/process/log user-credentials and perform user authentication for Security. It shall also be able to keep a record of user sessions.
- Router: The router will have the capability to maintain a routing table that can store the IPs of far end Machines. The router may have sub-modules for Standardized Video Streaming Protocols. The router should also support Multicasting and Broadcasting of the Video Stream.
- Codec: A codec is required that can convert the Analog Video from interface # 01 to a Digital Video Format for transmission on the IP-Network. The Analog Interface may be PAL or NTSC and the Digital Video Format may be MPEG, AVI etc. The Codec should support video compression according to the desired bit rate of the IP-Network.
- Interface #1: This interface is an Analog Video Interface. Any standard such as PAL/NTSC may be used to connect with a compatible Analog camera.
- Interface #2: This interface is an RS-485 Interface which is used to connect the PTZ (Pan-Tilt-Zoom) Movement Controller of the Camera Chassis/Assembly.
- Interface #3: This interface is an IEEE 802.3 Ethernet Interface for connectivity with the IP Cloud.

At the remote end, we use a machine that acts as an Operator Console used to Control and View the Camera Video. It is also used to Store the video on a SAN and retrieve the video whenever required. Following is the configuration of the modules in the machine # 02:

- Controller: The controller will have the capability to store/process/log user-credentials and perform user authentication for Security. It shall also be able to keep a record of user sessions.
- Router: The router will have the capability to maintain a routing table that can store the IPs of far end Machines. The router may have sub-modules for Standardized Video Streaming Protocols. The router should also support Multicasting and Broadcasting of the Video Stream. The router will support different types SAN Protocols to connect with Video Storage Devices.

- Codec: The codec should be able to convert Digital Video from the IP Network to Analog Video which can be transmitted to an Analog NTSC/PAL monitor connected on Interface # 01. It should also be able to Convert the video from the IP-Network for Storage on the SAN Storage Device attached on Interface # 03. Also it should be able to convert the Digital Video retrieved from the Storage device to be Played-Back on the Analog Monitor. The Codec should support the proper video compression and decompression.
- Interface #1: This interface is an Analog Video Interface. It is used to connect to an Analog Monitor supporting either PAL or NTSC video Standard for displaying the streaming video from the remote camera or the video storage server.
- Interface #2: This interface is an RS-485 Interface which is used to connect the PTZ (Pan-Tilt-Zoom) Desktop-Controller Console Device. This device is used by the Operator to issue Pan-Tilt-Zoom commands to the remote analog camera.
- Interface #3: This interface is a Digital Video Interface such as DVI or HDMI. It should be able to connect to Video Storage Devices or SANs complying to DLNA or other such standards.
- Interface #4: This interface is an IEEE 802.3 Ethernet Interface for connectivity with the IP Cloud.

Thus the operating at Machine # 02 can control the camera attached to Machine # 01 and also control the Video Storage attached to Machine # 02.

## VII. Conclusion

Initially an all IP network was envisioned take over the Telecom Networks. In order to do the transition towards this all IP Network, NGN was designed and it supposed to be the interim transition network. However, NGN proved to be more Robust and it seemed as if NGN would be the future network. With the passage of time, problems arose with NGN because of its Complexity of Protocols. Although newer and more simplified hardware was introduced into NGN but the Software protocols were still complex. In this paper, we have proposed a protocol that would try to overcome the complexity of NGN by simplifying the communication systems involved for multiple types of scenarios. This protocol would greatly simplify the involved software and hardware required and would modularize the communication system. It will be useful in utilization in resource constraint systems such as Wireless Sensor Networks or other Internet of Things nodes.

The Example Scenario defined in this paper can be implemented on hardware platforms. Nowadays some open source hardware boards are available in Market. These boards use open source software and hardware. These boards are generally low cost platforms and very large user forum is available for software development. These facilities can be used to implement the communication scenarios in this book. Also special boards can be designed to implement this router by utilizing ASICs, FPGAs, SOCs etc.

## References

[1] Moindze, S.M. ; Konate, K. "A survey of the distributed network management models and architectures: Assessment and challenges", IEEE 6th International Conference on Adaptive Science & Technology (ICAST), 2014.

[2] Zhibo Pang ; Kan Yu ; Akerberg, J. ; Gidlund, M. , "An RTOS-based architecture for industrial wireless sensor network stacks with multi-processor support " IEEE International Conference on Industrial Technology (ICIT), 2013.

[3] Wang, Guixin ; Kang, Guixia ; Wang, Hao "Design and FPGA Implementation of MAC-PHY Interface Based on PCI Express for Next-Generation WLANs " 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

[4] Subin Shen ; Carugi, M. "Standardizing the Internet of Things in an evolutionary way ", Proceedings of the ITU Kaleidoscope Academic Conference: Living in a converged world - Impossible without standards, 2014.

[5] Stepanenko, A. and Constantinou, C. "Novel Topological Framework for Adaptive Routing ", IEEE Global Telecommunications Conference-GLOBECOM, 2009.

[6] Grubitzsch, P. and Schuster, D. "Hosting and Discovery of Distributed Mobile Services in an XMPP Cloud" IEEE International Conference on Mobile Services (MS), 2014.

[7] Pranggono, B. ; Elmirghani, J.M.H. "Traffic statistics in WDM storage area networks", 10th International Conference on Transparent Optical Networks, ICTON 2008, Volume: 3.

[8] Mollah, M.B. and Islam, S.S. "Towards IEEE 802.22 based SCADA system for future distributed system ", International Conference on Informatics, Electronics & Vision (ICIEV), 2012.