Rethinking the power of packet switching in the coming cyber threats era

Manfred Sneps-Sneppe, Dmitry Namiot

***Abstract*— The article is devoted to the discussion of the telecommunications development strategy. Communication specialists all around the world are facing the same problem: shifting from circuit switching (CS) to packet switching (CS). We will provide examples to illustrate the difficulties that complicate the transition from CS to PS and the move to hybrid CS+PS solutions. We start with the basics of routers and switches. Then we discuss the Defense Information System Network move from circuits to packets, namely, "Joint Vision 2010" - the implementation of signaling protocol SS7 and Advanced Intelligent Network, and "Joint Vision 2020" - the transformation from SS7 to IP protocol. We describe some packet switching shortcomings in the implementation of Joint Vision 2020, namely, Joint Information Environment as a beautiful but unattainable dream, GSM-O contract, and Joint regional security stacks failures, as well as give some critics regard Joint Enterprise Defense Infrastructure Cloud Strategy and Artificial Intelligence Initiative. An example of a hybrid solution: a unified packet and circuit switched network are shown. We describe a new trend in microelectronics, namely, a network-on-a-chip orientation from packet to circuit switching. We conclude that the long channel-packet coexistence seems inevitable, especially in the face of growing cyber threats.**

***Keywords*— circuit switching; packet switching; Joint Vision 2010; Joint Vision 2020; SS7; IP; softswitch; DISN; DRSN; hybrid packet-circuit solution; network-on-a-chip.**

I. Introduction

This paper is an extension of work originally presented in the 23d Open Association FRUCT Conference (2018) [1]. It is devoted to the discussion of the telecommunications development strategy. Communication specialists around the world are facing the same problem: shifting from circuit switching (CS) to packet switching (PS). We will provide examples to illustrate the difficulties that complicate the transition from CS to PS and give some examples of hybrid CS+PS solutions.

A. On DoD obsolete networks: the AT&T view

According to the AT&T experts' view [1], the Department of Defense (DoD) today still has analog, fixed, premises-based, time-division multiplexing (TDM) and even asynchronous transfer mode (ATM) infrastructure that drains billions of dollars in legacy operations and maintenance expenses from the DoD's annual budget, while unnecessarily exposing the DoD to cybersecurity risks. This aging network architecture is based on point-to-point circuits that require constant hardware maintenance and upgrades. The current situation is partially a result of defense contracting, not network providers. The roughly 15,000 separate networks that comprise the DoD's network were built by hundreds of different companies that are not in the business of networking. Why should the DoD outsource the operation of networks to contractors whose networks are then managed by AT&T? "The existing TDM environment is 30 years behind current commercial technologies", - such is the harsh rebuke of AT&T [2].

B. US Army Regulator fights for IP technology

The similar kind harsh sentence of the DoD's activities flows from the Army Regulation document [3] of 2017 regarding Telecommunications Systems and Services. The Army regulator recognizes that there is 'old' equipment on the network: Time-division multiplex equipment, Integrated services digital networking, channel switching Video telecommunication services. All these services will use IP technology. Name the few of instructive claims:

4–2.d. Commands that have requirements to purchase or replace existing Multilevel Secure Voice (previously known as Defense Red Switched Network (DRSN)) switches will provide a detailed justification and impact statement to the CIO/G–6 review authority.

4–2.e. The moratorium on investment in legacy voice-switching equipment and the requirement to submit requests for waivers to purchase voice-switching equipment applies to all TDM voice-switching equipment that is not capable of providing unclassified and/or secret IP voice services. The Army will migrate as soon as practical to an almost-everything-over-Internet Protocol architecture, to include Unified Capabilities (UC) and collaboration, with an end state of end-to-end IP.

4–4. All Army organizations will cease investment in (nonemergency) integrated services digital network (ISDN) supported technology, equipment, and transport. All Army organizations will transition from ISDN to a compatible IP-supported technology or service including, but not limited to, video, facsimile, voice, and other network capabilities.

7–4. Secret IP voice is the Army-preferred means of providing secret-only voice communications. The latest UCR will provide guidance for the implementation of secret IP voice capabilities. The UCR requires that classified IP voice migrates to multivendor equipment using the Assured Services Session Initiation Protocol (AS–SIP).

Received: Jun 21, 2019.
Manfred Sneps-Sneppe - Ventspils University of Applied Sciences, Latvia (email:manfreds.sneps@gmail.com)
Dmitry Namiot - Lomonosov Moscow State University, Russia (email: dnamiot@gmail.com)

C. *Cyber threats: what GAO found*

Cyber threats are another hard obstacle in a move to IP world. In October of 2018, the Government Accounting Office (GAO) has reported [4], the United States weapons systems developed between 2012 and 2017 have severe, even "mission critical" cyber vulnerabilities, and that the federal information security (i.e. cybersecurity) needs to improve "the abilities to detect, respond to, and mitigate cyber incidents", increase its cyber workforce and increase cybersecurity training efforts.

DOD weapon systems are more software dependent and more networked than ever before (Fig. 1). From ships to aircraft, the weapons made available to the Department of Defense are becoming more advanced technologically and uses more software and less hardware to control everything from navigation to weapons systems. The F-35 Lighting II software (aircraft) contains eight million lines of code and controls everything from flight controls to radar functionality, communications, and weapons deployment [4].

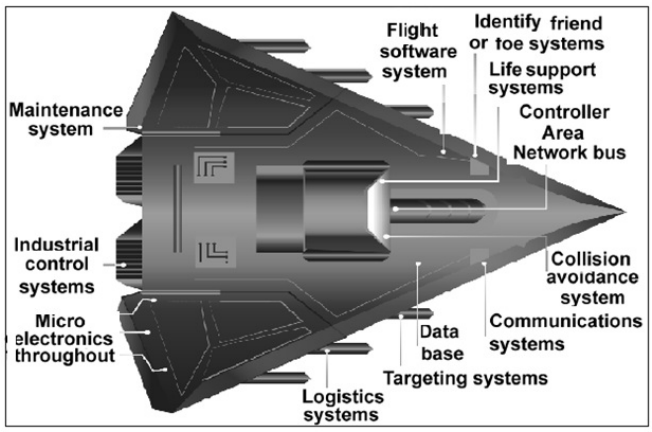

Fig. 1: Embedded software and information technology systems in weapon systems (represented via fictitious weapon system for classification reasons) [4]

The rest of the text is the following. Section 2 refers to the basics of routers and switches. Section 3 describes the Defense Information System Network (DISN) move from circuits to packets, namely, "Joint Vision 2010" - the implementation of signaling protocol SS7 and Advanced Intelligent Network, and "Joint Vision 2020" - the transformation from SS7 to IP protocol. In Section 4, we describe some packet switching shortcomings in the framework of Joint Vision 2020 implementation, namely, Joint Information Environment as a beautiful but unattainable dream, GSM-O contract and Joint regional security stacks failures, as well as Joint Enterprise Defense Infrastructure Cloud Strategy and Artificial Intelligence Initiative critics. Section 5 shows an example of a hybrid solution: unified packet and circuit switched network. In Section 6, we describe a new trend in microelectronics, namely, a network-on-a-chip orientation from packet to circuit switching.

Therefore, the long channel-packet coexistence seems inevitable, especially in the face of growing cyber threats.

II. On basics of routers and switches

In order to understand the technological trends [5], one has to know the functions that packet and circuit switches do, and the technology used to perform them. Fig. 2 shows the functional blocks of a packet switch, also called a router. When information arrives at the ingress linecard, the framing module extracts the incoming packet from the link-level frame. The packet then has to go through a route lookup to determine its next hop, and the egress port. Right after the lookup, any required operations on the packet fields are performed, such as decrementing the Time-To-Live (TTL) field, updating the packet checksum, and processing any IP options. After these operations, the packet is sent to the egress port using the router's interconnect, which is rescheduled every packet time. Several packets destined to the same egress port could arrive at the same time. Thus, any conflicting packets have to be queued in the ingress port, the output port, or both.

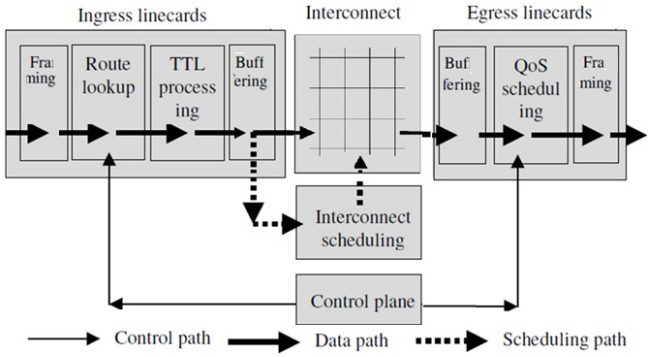

Fig. 2. The functionality of a packet switch [5].

In the output linecard, some routers perform additional scheduling that is used to police or shape traffic, so that quality of service (QoS) guarantees are not violated. Finally, the packet is placed in a link frame and sent to the next hop. In addition to the data path, routers have a control path that is used to populate the routing table, to set up the parameters in the QoS scheduler, and to manage the router in general. The signaling of the control channel is in-band, using packets just as in the data channel. The control plane might obtain the signaling information through a special port attached to the interconnect.

The main distinction between a router and a circuit switch is when information may arrive to the switch. In packet switching, packets may come at any time, and so routers resolve any conflicts among the packets by buffering them. In contrast, in circuit switching information belonging to a flow can only arrive in a predetermined channel, which is reserved exclusively for that particular flow. No conflicts or unscheduled arrivals occur, which allows circuit switches to do away with buffering, the online scheduling of the interconnect, and most of the data-path processing. Fig. 3 shows the equivalent functions in a circuit switch. As one can see, the data path is much simpler.

In contrast, the control plane becomes more complex: it requires new signaling for the management of circuits, a state associated with the circuits, and the off-line scheduling of the arrivals based on the free slots in the interconnect.

The tighter the control, the more signaling and state that will be needed. However, in circuit switching, as in packet switching, a slowdown in the control plane does not directly affect the data plane, as all on-going information transmissions can continue at full speed. In general, its data path determines the capacity of the switch.

Another important difference between a router and a circuit switch is the time scale in which similar functions need to be performed. For example, in both types of switches the interconnect needs to be scheduled. A packet switch needs to do it for every packet slot, while a circuit switch only does it when new flows arrive.

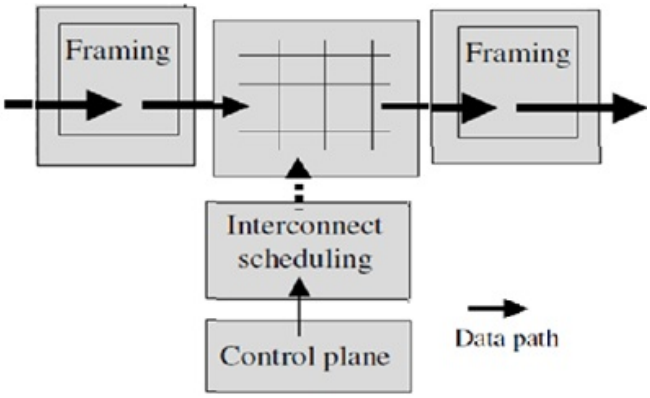

Fig. 3. Functionality of a circuit switch [5].

Comments on future circuit switching technology from Stanford University [5]. Compare the switches of equal throughput. It is reasonable to expect that since packet switches do much more work, it would come at the cost power and price. Compare two high capacity switches: packet switch Cisco CRS-1 and Ciena TDM switch; the former consumes 7 times the power and costs 10 times more (to multiple cost numbers with $1000 to get absolute values). Note that the throughput is equal to 10 million telephone calls (64 Kbps x 10 M = 640 Gbps). The software running in a typical transport switch is based on about three million lines of the source code, whereas Cisco's Internet Operating System (IOS) is based on eight million, over twice as many.

III. On DISN move from circuits to packets

A. *Joint Vision 2010: Bell Labs heritage*

In 1996, DISA approved "Joint Vision 2010" - a strategic development plan for US military departments for a 15-year period, which the GAO harshly criticized [6]. In 1998, GAO pointed out the following.

“Although Defense has been implementing the DISN program for 7 years, numerous networks continue to exist without DISA’s knowledge. Our own survey found that the military services are operating at least 87 independent networks that support a variety of long-haul telecommunications requirements.”

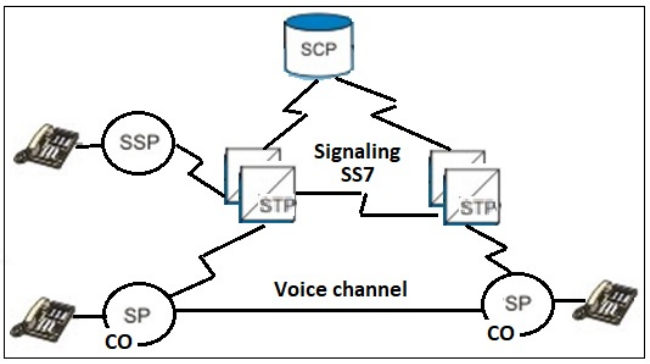

Fig. 4. Intelligent Network basics

SS7 is an architecture for performing out-of-band signaling in support of the call establishment, routing, and information exchange functions of the Publish Switch Telephone Network (PSTN). The Intelligent Network (IN) architecture (Fig. 4) allows operators to provide value-added services in addition to the standard telecom services such as PSTN, ISDN and GSM services on mobile phones. IN is supported by the Signaling System #7 (SS7) protocol between telephone network switching centers and other network nodes owned by network operators. The basic IN design is including STP (Signaling Transfer Point), SSP (Service Switching Point), SCP-DB (Service Control Point with Database), each Central Office (CO) contains Signaling Point (SP). The functional structure of the SS7 makes it possible to create the AIN by putting together functional parts.

The AIN details for defense we found in one paper from Lockheed Martin Missiles & Space [7] – the well-known Defense contractor. Fig. 5 describes the AIN components that operate in the worldwide telecommunication network, as well as how they are deployed in SS7 backbone, the space Wide Area Network (WAN), circuit switched voice network and the packet switched terrestrial WAN. The AIN components include the Service Creation Environment (SCE), Service Management System (SMS), Service Control Point (SCP), Service Switching Point (SSP), Intelligent Peripheral (IP), Adjunct, and the Network Access Point (NAP).

The SCE provides design and implementation tools needed to assist in creating and customizing services in the SCP. The SMS is a database management system used to manage the master database that controls the AIN warfighter services. The Intelligent Peripheral (IP) services include the authentication of users and much more. The Adjunct provides the same operation as the SCP, but is configured for one or fewer services for a single switch. The Network Access Point (NAP) is a switch that has no AIN functions. It is connected off a SSP, and interfaces to trunks with SS7 messages. It will route the call to its attached SSP or AIN services based on the called and calling number received.

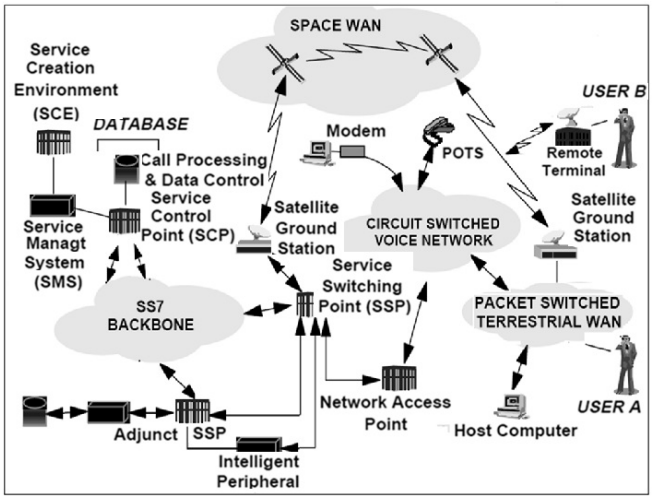

Fig. 5. Advanced Intelligent Network Military Service Architecture [7]

To illustrate the current DISN architecture we refer to the certification of Avaya Private Branch Exchange (PBX) S8300D in 2012 [8]. The SS7 network is, figuratively speaking, the nervous system of a DISN (Defense Information System Network) network up to resent time. That is, within the DISN network, the connections are established by means of SS7 signaling and, in the periphery, devices of any type are used. The presence of the SS7 network is not an obstacle to the transition to IP protocol.

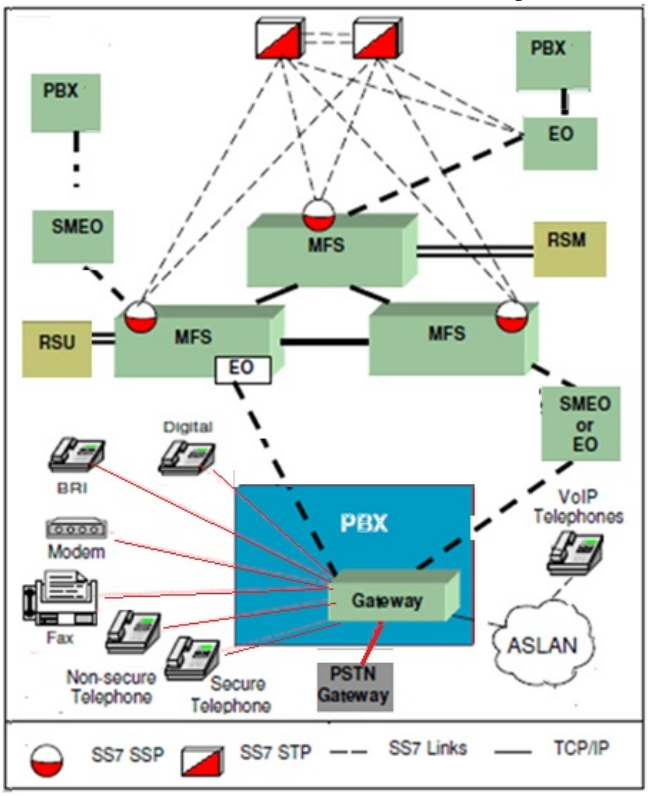

Fig. 6. The simplified DISN view: the current state [8] Here MFS (Multifunctional switch) stands for electronic exchange.

B. Joint Vision 2020: All-over-IP

In 2007, "Joint Vision 2020" appeared. Pentagon published a fundamental program [9], in which we find the most important point: Global Information Grid (GIG) must be built on basis of IP protocol (Fig. 7) as the only means of communication between the transport layer and applications.

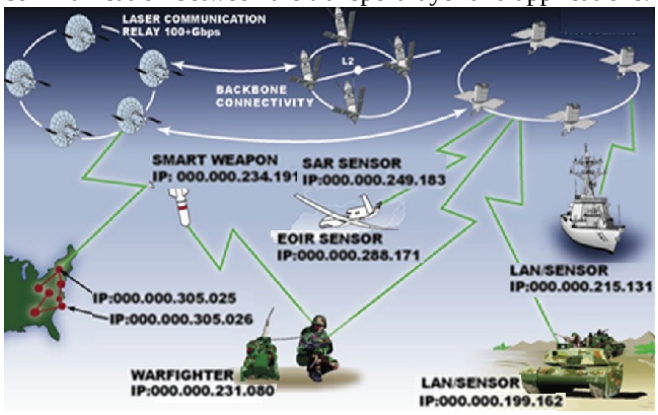

Fig. 7. Each warfare object has own IP address

Up to now, the main military communications networks of the Pentagon are circuit-switched networks (Fig. 8): (1) DSN - Defense Switched Network; (2) DRSN (Defense Red Switched Network) - for the top-secret government communications; (3) DVS - video conferencing network (DISN VIDEO). In addition, Fig. 8 shows two highly important classified military networks built on ATM switches: (4) JWICS (Joint Worldwide Intelligence Communications System), and (5) AFSCN (Air Force Satellite Control Network). There are also two widely known messaging networks: (6) SIPRNet (Secret Internet Protocol Router Network) - to transmit sensitive information over TCP/IP protocols, and (7) NIPRNet (Non-classified Internet Protocol Router Network) - a network used to exchange unclassified but important service information between "internal" users.

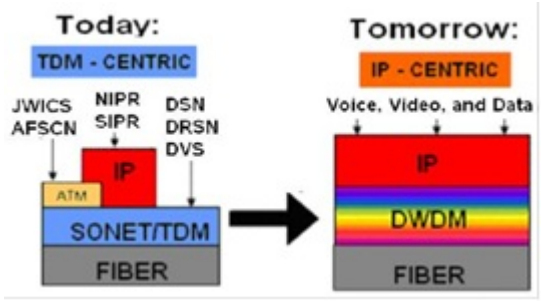

Fig. 8. DISN: from circuit switching to packet switching.

The most important step for DISN modernization is the replacing of channel switching electronic Multifunctional switches (MFS) by packet switching routers. The transition phase is based on the use of Multifunctional SoftSwiches (Fig. 9).

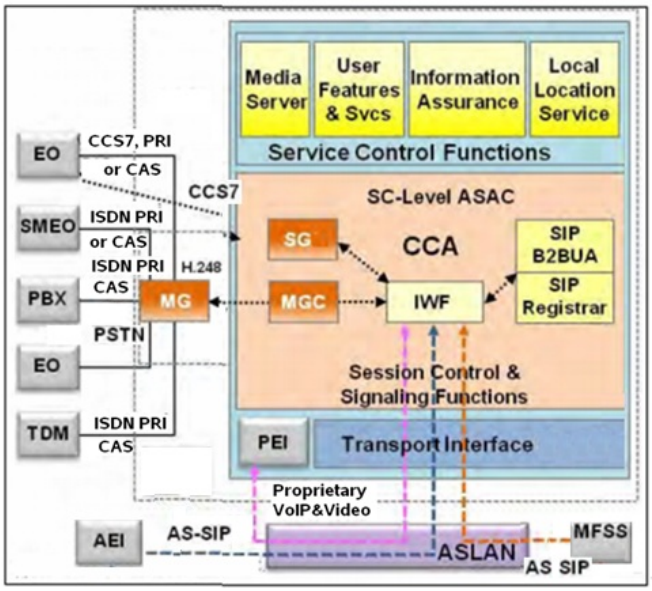

Fig. 9. Reference model for Multifunction SoftSwitch (MFSS) [10].

The left side of MFSS shows the traditional telephony protocols CCS7, ISDN PRI, and CAS (Channel Associated Signalling) used for connections with the "old" channel switching networks. MFSS interfaces the circuit switched based external TDM network and the IP backbone network also control the calls that are originating from the external Public Switched Telecommunications Network (PSTN)/Integrated Services Digital Network (ISDN). So, MFSS will also needs to provide ISUP-SIP inter-networking function (IWF). It is expected that TDM switching portion of the MFSS will be retired as soon as all users/systems migrate to IP.

A signalling gateway (SG) deals with all signalling protocols such as ISUP, CCS7/SS7, and CAS. The MFSS also operates as a media gateway (MG) between TDM circuits switching and IP packet switching under the control of the media gateway controller (MGC) while communications control protocol like H.248 is used between MG and MGC.

The main drawbacks of the SIP protocol are the difficulties in securing secrecy (under cyber warfare) and servicing priority calls, which is important for military applications, for emergency service. Therefore, by order of the Department of Defense, a secure AS-SIP protocol was developed [11]. The AS-SIP protocol turned out to be very cumbersome. If ordinary SIP uses 11 other RFC standards, then AS-SIP uses the services of almost 200 RFC standards.

Note the leading role of the Session Controller as an essential part of MFSS. The Session Controller is the most complex software package that performs the same functions in packet switching networks as a traditional telephone exchange. To implement the all currently existing services and plenty protocols: Session Controller contains as many as 19 servers for different services [10].

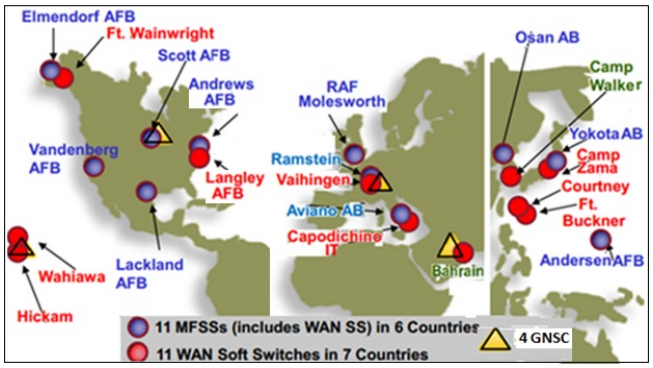

Fig. 10. DISN Joint Vision 2020: 22 SoftSwitches and 4 Global Network Support Centres [10]

The target DISN infrastructure contains two level switching nodes: Tier0 and Tier1 (Fig. 11). Tier0 geographic cluster typically consists of at least three Tier0 SoftSwitches (SSs). As the distance between the clustered SSs must be planned so that the RTT does not exceed 40 ms and propagation delay equals 6 μs/km thus the distance between Tier0 should not exceed 6,600 km. The classified signaling environment is unique in that it will use a mix of existing vendor-based H.323 and AS-SIP signaling during the transition period to all DISN CVVoIP (Classified VoIP and Video). In addition, a unique MG capability exists as part of a Tier0 SS. Classified VVoIP interfaces to the TDM Defense RED Switch Network (DRSN) via a proprietary PRI.

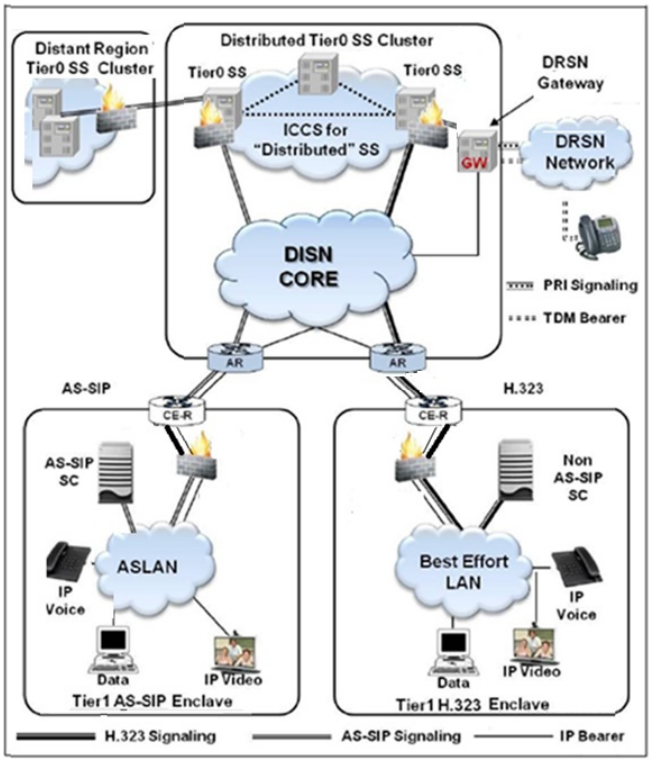

Fig. 11. DISN Classified VoIP and Video Signalling Design [10]

It is still difficult to predict the time during which the DISN network will finally switch to the AS-SIP protocol. Obviously, TDM and ISDN equipment could stay for an unpredictable time, especially considering cyber-security threats.

No reason to be surprised that the Defense Red Switch Network (DRSN) uses 40 years old ISDN technology. DRSN is a dedicated telephone network, which provides global secure communication services for the command and control structure of the United States Armed Forces (Fig. 12). The network is maintained by DISA and is secured for communications up to the level of Top Secret. Note the slot at the bottom right serves for a crypto-card and four buttons at the top - to select the priority of communications. The STE is the primary device for enabling secure communications over the Defense Switched Network (DSN). It may be used for secure voice, data, video, or facsimile.

Fig. 12. Secure Terminal Equipment, STE; note slot in front for Crypto PC Card (left). The DRSN architecture (right).

IV. Joint Vision 2020: on some packet switching shortcomings

A. Joint Information Environment: a beautiful but unattainable dream

In 1987 there was an article by J.A. Zachman "A Framework for Information Systems Architecture" and for the first time introduced the concept of "enterprise architecture". Following Zachman's model, the Joint Information Environment (JIE) of DISN and the DoDAF metamodel (Department of Defense Meta-Model) are being built. It has been developed since 1990. The JIE documentation consists of 52 volumes (too many for software developers).

The development of DoDAF – it is really a big multi-billion deal - has been going on for more than 25 years, but it obviously cannot be completed. The conclusion is that the very idea of creating a single information system for such a complex enterprise as the US Department of Defense today is an impossible task or the Zachman's model development method itself is erroneous at all.

B. GSM-O contract failure

In June 2012, Lockheed Martin won the largest tender for managing the DISN network (Global Services Management-Operations, GSM-O). The essence of the GSM-O contract is the modernization of the management system for cybersecurity requirements. The cost of work is a huge amount - 4.6 billion dollars for 7 years. The first deal was to upgrade the GIG management system: to consolidate the operating centers - from four to two. GIG network management centers are expanding at the AB Scott (Illinois) and Hickam in Hawaii, but the centers in Bahrain and Germany are being closed (see Fig. 10).

In 2015, the telecommunications world was shocked by the news: Lockheed Martin is not coping with the upgrade of the DISN network management and sells its division “LM Information and Global Solutions” to the competing firm Leidos. The failure of the work was most likely due to the inability to recruit developers capable of combining the "old" circuit switching equipment with the latest packet switching systems as well as taking into account the new cybersecurity requirements [12].

C. Joint regional security stacks

The very concept of the Joint Information Environment is extremely complex, and the requirements of cybersecurity make it even more difficult. The essence of the JIE concept is to create a common military infrastructure, provide corporate services and a unified security architecture, and Joint regional security stacks (JRSS) are the main components of the JIE environment that provide a unified approach to the structure of cybersecurity and the protection of computers and networks in all military organizations.

Currently, JRSS stacks are installed for the NIPRNet. It is planned also to install the stacks for the SIPRNet. The total amount of works includes the installation of 23 JRSS stacks on the NIPRNet service network and 25 JRSS stacks on the secret SIPRNet network. By 2019, it is planned to transfer to these stacks cybersecurity programs, which are now deployed in more than 400 locations [13].

During several last years, the Government Accounting Office (GAO) has been paying attention to Pentagon’s budget, particularly to Joint Regional Security Stacks (JRSS) budget [10]. In January 2018, under the pressure of GAO critics, the Pentagon’s chief weapons tester said the DoD should stop deploying its new network security platform JRSS. Why? The Pentagon’s weapon tester said that during a test last year the version of the program in use by the Air Force did not help protect the network [14].

Can the Pentagon fulfill this grandiose plan? The complexity of the task, in particular, characterizes the set of requirements for potential JRSS developers, named in the job invitations by Pentagon’s contractors. Requires work experience of 12-14 years and knowledge of at least two or more products from ArcSight, TippingPoint, Sourcefire, Argus, Bro, Fidelis XPS, Niksun FPCAP, Lancope, NetCool, InfoVista, and Riverbed. Note these companies provide the full complex software for cyber defense. How to combine them? How to hire the software experts able to do such a sophisticated job?

More importantly, is the project worth be doing? Why? The crucial JRSS failure is extremely important: JRSS is too S-L-O-W (!).It sounds like a sentence on the fate of the JRSS project [15].

D. JEDI Cloud Strategy and its critics

The Defense Department's newly released cloud strategy positions the general-purpose Joint Enterprise Defense Infrastructure (JEDI) cloud initiative as the foundation [16].

The strategy emphasizes a cloud hierarchy at DOD, with JEDI on top. Fit-for-purpose clouds, which includes MilCloud 2.0 run by the Defense Information Services Agency (DISA), will be secondary to the commercially run JEDI general-purpose cloud.

During testimony at a Senate Armed Services cybersecurity subcommittee hearing Jan. 29, DOD CIO Dana Deasy said that DOD needs to stop debating over mission-specific tools and focus entirely on implementation. Note some unexplainable rush with the JEDI project forgetting about recent shortcomings with JRSS deal.

April 10, 2019. The Department of Defense confirms that Amazon and Microsoft are the winners. Oracle and IBM are officially out of the race for a key $10 billion defense cloud contract as Amazon and Microsoft move ahead. Note Amazon was in the best position to win the government contract, and they were considered the favorite by most.

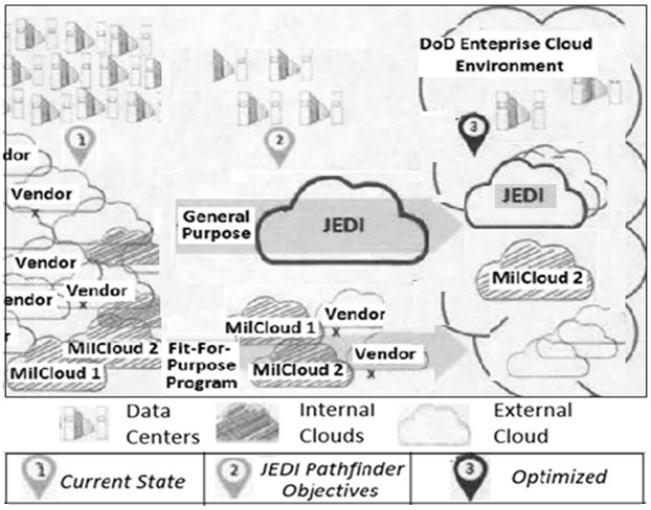

Fig. 13. DoD Pathfinder to Hybrid Cloud Environments [15]

Could be the JEDI Cloud Strategy successful? A key technological difficulty for the JEDI project is interoperability of clouds (Fig. 13). The interoperability of a technology (getting different parts to function in combination) can be divided into three main categories: internal, external, and iterative. Unfortunately, in each category, the Pentagon's JEDI cloud strategy leaves a series of unanswered questions that could spell disaster in the future [17].

For internal interoperability the strategy lays out the correct goal, stating that common data and application standards such as tagging, transport protocols, and interfaces, will be developed to navigate DoD away from custom approaches. However, it does not mention the enormous logistical hurdles to this data-normalization process. First, both the military's legacy IT systems and the 500+ clouds already used within the Pentagon will each need to have their data formatted and migrated onto the JEDI platform.

The second unanswered question regards the JEDI cloud's external interoperability. This sounds simple on paper, but the reality is far more uncertain. In a future conflict situation, would America's allies need to use the same cloud provider (e.g., Microsoft or Oracle) and the same data-formatting practices as the DoD? The strategy does not discuss these long-term concerns including security flaws.

E. Artificial Intelligence Initiative

The Defense Innovation Unit (DIU) is a DoD organization founded to help the U.S. military make faster use of emerging commercial technologies. Launched in 2015, the organization has been called "the Pentagon's Innovation Experiment". DIU is staffed by civilian and both active duty and reserve military personnel. The organization is headquartered in Mountain View, California — Silicon Valley — with offices in Boston, Austin, and some more. The Joint Artificial Intelligence Center is a focal point of the DoD Artificial Intelligence Strategy [18]. The DoD has created this Cloud Strategy to strengthen the security and resilience of the networks and systems that contribute to the Department's military advantage.

Underscoring the potential magnitude of AI's impact on the whole of society, and the urgency of this emerging technology race, President Trump signed the executive order, Maintaining American Leadership in Artificial Intelligence, on February 11, 2019, launching the American AI Initiative. This was immediately followed by the release of DoD's first-ever AI strategy [19].

The DoD strategy identifies how artificial intelligence can manage the understanding of all the Department's data to free information from the current system of "disjointed stovepipes." This is really one great idea - artificial intelligence, if it happens to be successful. Could it have more success than JRSS initiative?

V. Network Optimization for Unified Packet and Circuit Switched Networks

The SDN-(Software Defined Network) based unified architecture is coming from Stanford University [20] and co-authorized by prof. Nick McKoewn, the inventor of SDN technology. In this architecture, backbone routers are replaced with less expensive hybrid optical-circuit/electrical-packet switches that have both circuit-switching and packet-switching capabilities. These hybrid switches are logically connected in a fully-meshed network where each hybrid switch implements an IP node, and where each IP node is logically connected to each and every other IP node via a single direct circuit-switched hop. This unified packet and circuit-switched network can then be managed using a single converged control plane. Fig. 14 depicts this unified fully-meshed IP network architecture. The actual underlying optical transport network can be dynamically allocated to provide different circuit capacities to implement each logical connection in the full-mesh, for example based on estimated traffic demands. For example, a logical connection from San Francisco (SF) to New York (NY) may be implemented as an optical circuit-switched path via Seattle and Chicago.

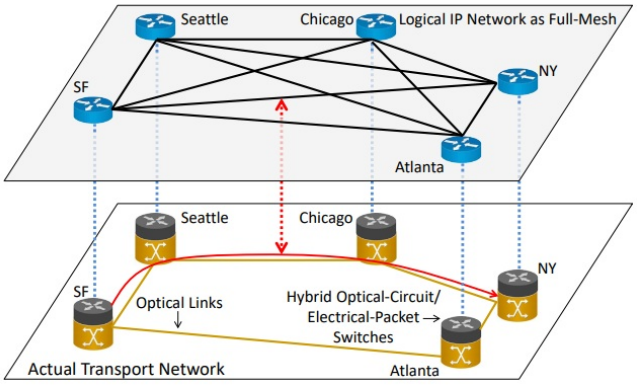

Fig. 14. IP network logically as a full-mesh, with logical connections implemented over an optical circuit-switched transport network and logical routers implemented as part of hybrid optical circuit/electrical-packet switches [21]

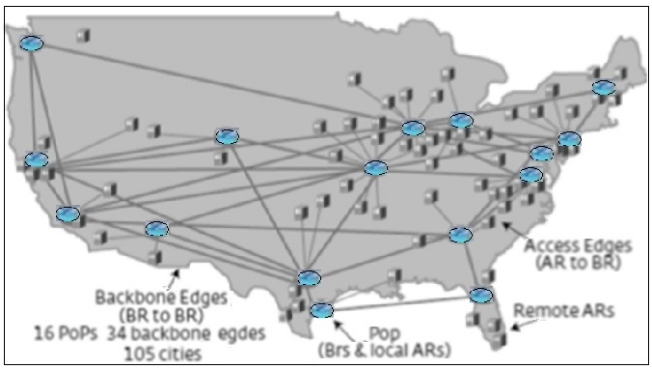

Fig. 15. AT&T US IP core network: 16 PoPs across the U.S. are aggregating the traffic from 89 other cities [20]

The efficiency of Unified Packet and Circuit Switched Network has proven by data of AT&T US IP core network (Fig. 15). Two architectures were compared: (1) traditional All-IP version used MPLS backbone routers (BR) and (2) the hybrid packet and circuit core with hybrid MPLS-OTN (packet optical) switch, building on the ideas from SDN and replacing BRs in core PoPs with hybrid MPLS-OTN switches (Fig. 16). The overall number of core ports was reduced significantly in IP-and-DCS (Dynamic Circuit Switching) when compared to the reference design (from 2564 to 1480). As a result, nearly 60% in overall Capex savings have been achieved when compared to the reference IP-over-WDM design. Most of these savings come in the backbone switches, which see an 85% reduction in cost. A key problem that must be solved in this unified architecture approach is the allocation of optical circuits between adjacent IP nodes in the logical full-mesh (i.e., between every pair of ingress and egress nodes).

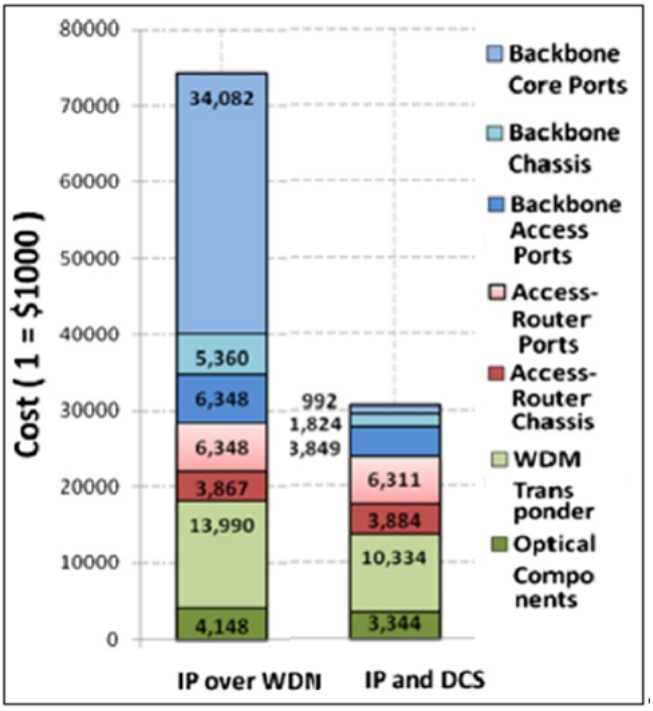

Fig. 16. Capex results for two AT&T US IP core network designs [20]

These results have led to the following:

(1) Packet switching will continue to exist at the edge of the network. The packet-switched network should ideally gather traffic from disparate sources, and multiplex it together.

(2) At the core of the network, the circuit switched transport network should remain as a means to interconnect the packet switched routers, and as a means to provide high reliability and performance guarantees.

VI. NETWORK-ON-A-CHIP: CS VERSUS PS

A. NoC basics

Consider the confrontation of CS and PS supporters in one particular but very important area, namely — microelectronics. NoC schemes were developed for packet switching, while considering circuit switching as a side option. However, in the latest years, there are works denoting the opposite: in the NoC market, circuit switching products can take the field from packet switching products. Fig. 17 shows an example of a complex circuit: a so-called network on a chip (NoC) [1]. A single crystal houses a lot of familiar elements: the central processing unit (CPU); the memory (MEM); the input/output (I/O); and the USB interface, Ethernet, and others. They mainly communicate using buses, but the question that relates to the topic of this article is how to build the central part — the switching network between the buses.

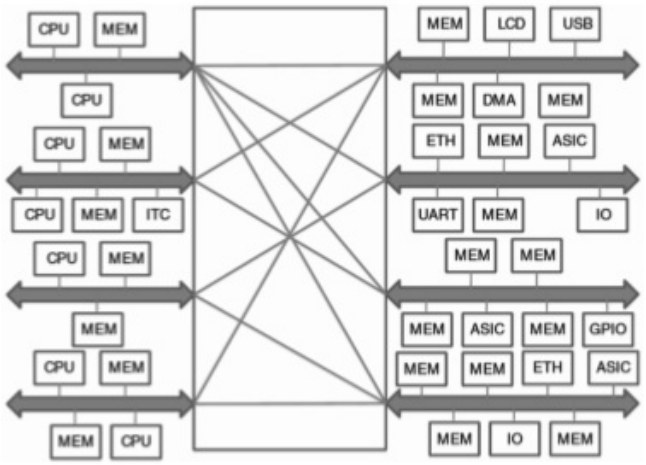

Fig. 17. Single-crystal microchip (NoC) example [22]

Fig. 18 shows a NoC network for packet switching. Each node S comprising a 4x4 switch board is a router; it has four inputs, four outputs, and a certain resource (CPU, memory, I/O device) that communicates with the S node via the resource network interface (RNI). In the packet switching (PS) mode, there is a buffer allocated for each input. The S node is controlled by Arbiter. The operation of message sending is the consistent transmission of packets through a chain of routers.

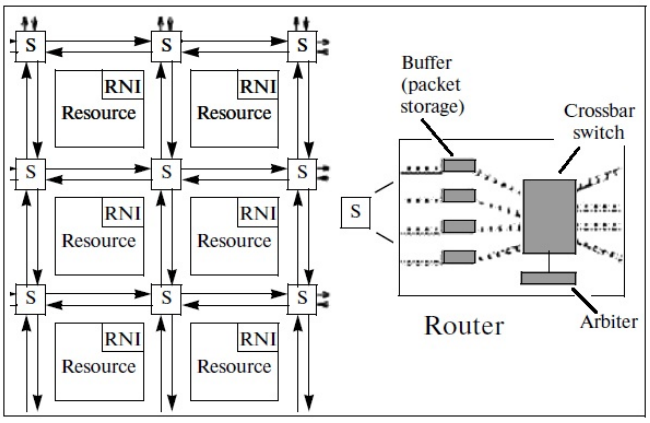

Fig. 18. Network on a chip with six nodes (left); each node S represents a router with 4 inputs and outputs (right) [22]

To transmit messages received by the chip input, they are divided into smaller parts due to the numbers of bits for the devices (usually, that is the number of parallel wires between blocks). The messages are divided into packets, and those in turn are divided into smaller units: Flit and Phit (often, the lengths of Flit and Phit are the same). Phit is a unit of data transferred between nodes in a single cycle of the chip.

In the circuit switched mode, the physical channel (from the network input to the output) is reserved until data transmission starts. When the message subject is being transmitted through the network, it reserves (occupies) the path for the message transmission. Furthermore, this method, as compared with packet switching, eliminates the need to transmit the service information (head flit and tail flit) for each packet. The essence of circuit switching is the following: the Arbiter controller determines the input, and the multiplexer, the output of the bit stream (Flit) in this cycle of the chip.

B. On CS NOC advantages: some examples

MPEG-4 decoder (Taiwan). Let's start with a specific mass product—an MPEG-4 decoder. The international standard MPEG-4 was introduced in 1998. The MPEG-4 standard is mainly used for broadcasting (video streaming), recording movies onto a CD, and for video telephony (videophones) and broadcasting, which actively use digital video and audio compression.

In 2006, the engineers of a Taiwan university presented MPEG-4 decoder prototypes in two implementations: CS NoC and PS NoC based on 0.18 μm technology [23]. The test results clearly show the advantage of circuit switching for NoC. The CS NoC option surpasses PS NoC in all the indices (Table 1). The most notable is the difference in power consumption — by 45 times.

Table 1. Experimental results for two different MPEG-4 decoder architectures

	CS NoC	PS NoC
Surface (μm^2)	56.26×10^3	649.27×10^3
Power consumption (μW)	260.6	11793.69
Delay (ns)/switch	3.48	29.66
Bandwidth (10^6 ns)	2.16	12.04

A Stockholm experience. In 2013, Swedish engineers (the Royal Institute of Technology, Sweden) presented the results of comparing three NoC solutions [24]: (1) CS NoC with a 4 x 4 switching field; (2) PS NoC with the same field: 4 virtual channels and 4 buffers (PS_v4_b4); and (3) PS NoC: 16 virtual channels and 16 buffers (PS_v16_b16).

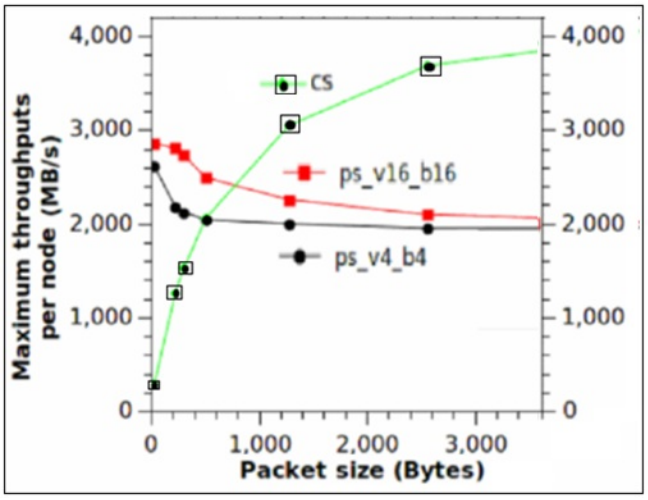

Fig. 19. In a vast range of loads, circuit-switched CS NoC is more effective than packet-switched PS NoC.[17]

The measurements have shown (Fig. 19) that, in a vast range of loads, circuit-switched CS NoC is more effective. If the packets are longer than 500–800 bytes, then circuit-switched CS NoC is more effective. The first packet

switching PS NoC option (PS_v4_b4) has the advantage in case of packets of only 500 bytes, while the second PS NoC option (PS_v16_b16) retains its advantage for packet lengths up to 800 bytes. At a packet length of 5120 bytes, the capacity of both PS NoC options is the same.

Intel's crazy efficient, crazy fast network-on-chip. In February 2014 [25], Intel announced the development of a phenomenal chip that contains a network consisting of a matrix of 256 nodes (16 × 16 mesh network-on-chip). This network is a high-performance hybrid switch board with 20.2 terabit/s bandwidth. This chip is based on 22-nm trigate CMOS technology. It is important that this chip is able to switch not only packets (as a standard now) but circuits as well.

The Intel's NoC achieves a lot (Fig. 20):

(i) 20.2 Tb/s total throughput at 0.9 V, 25 °C;

(ii) hybrid packet/circuit switching for a 62% latency improvement and 55% increase in energy efficiency to 7.0 Tb/s/W, compared to packet switching;

(iii) a peak energy efficiency of 18.3 Tb/s/W for near-threshold operation at 430 mV, 25 °C;

(iv) ultra-low-voltage operation down to 340 mV, 25 °C, with router power scaling to 363 μW.

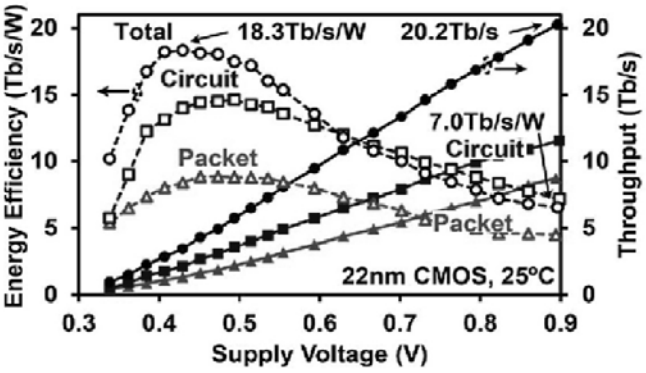

Fig. 20. Voltage scaling and throughput measurements [25]

Hybrid circuit-switched router as intelligent network prototype. The paper [26] proposes a hybrid circuit-switched router that interleaves circuit- and packet-switched flits on the same physical network with the low area and power overhead. Combining space (SDM) and time (TDM) division multiplexing techniques in a router (Fig. 21) allows taking advantages of the abundance of wires resulting from the increased level of circuits. We then have two degrees of freedom to optimize the router; one can increase either the number of subchannels in an SDM-TDM Channel or the number of time slots per subchannel. In both cases, the number of available channels increases in the network, thereby increasing the possibilities of establishing paths through the network.

At the router (2, 3), the allocator reserves the requested time slot at the unique subchannel; in this case, it is the time slot number 3. Then the ACK packet is generated and routed through the packet-switched subrouter from the destination to the source. Upon reception of the ACK packet, the source node then starts transferring streaming data at the time slot specified by the allocator EAST at the router (2,1).

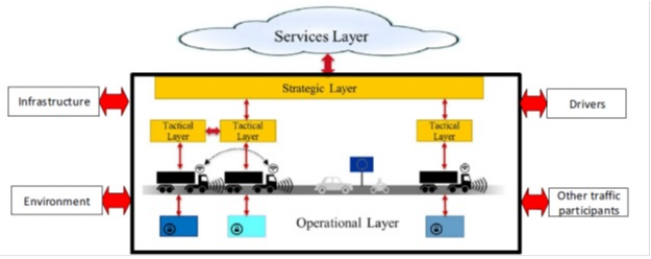

Fig. 21. SDM-TDM path between the source (2,1) and the destination (2,3) [26]

This NoC recalls the Intelligent Network architecture (see Fig. 4): the upper part is similar to the packet switching SS7 network, the bottom part is channel switching.

VII. Conclusion

The article is devoted to the discussion of the telecommunications development strategy. We will provide examples to illustrate the difficulties that complicate the transition from circuit switching to packet switching, and the move to hybrid CS+PS solutions. We start with the basics of routers and switches. Then we discuss the Defense Information System Network move from circuits to packets, namely, "Joint Vision 2010" - the implementation of signaling protocol SS7 and Advanced Intelligent Network, and "Joint Vision 2020" - the transformation from SS7 to IP protocol. We describe some packet switching shortcomings in the implementation of Joint Vision 2020, namely, Joint Information Environment as a beautiful but unattainable dream, GSM-O contract and Joint regional security stacks failures, as well as give some critics regard Joint Enterprise Defense Infrastructure Cloud Strategy and Artificial Intelligence Initiative. An example of a hybrid solution: a unified packet and circuit switched network are shown. We describe a new trend in microelectronics, namely, a network-on-a-chip orientation from packet to circuit switching. We conclude that the long channel-packet coexistence seems inevitable, especially in the face of growing cyber threats.

References

[1] M. Sneps-Sneppe, D. Namiot. "Time to Rethink the Power of Packet Switching". In Proc, 14-16 Nov. 2018, Bologna, Italy.

[2] The Defense Network of Tomorrow—Today. AT&T White paper. 2018

[3] Army Regulation 25–13 Information Management. Army Telecommunications and Unified Capabilities. Headquarters Department of the Army Washington, DC. 11 May 2017

[4] GAO-19-128. Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities. Report to the Committee on Armed Services, U.S. Senate. United States Government Accountability Office. October 2018

[5] P.M. Fernandez. "Circuit switching in the internet". Dissertation. Stanford University. June 2003

[6] Defense Networks. Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals. US General Accounting Office. GAO/AIMD-98-202. July 30, 1998

[7] William W. Chao. "Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters". MILICOM, 1999. IEEE

[8] Special Interoperability Test Certification of Avaya S8300D with Gateway 450 (G450). DISA, Joint Interoperability Test Command, 17 Apr 2012

[9] U.S. Department of Defense. Global Information Grid. Architectural Vision, Version 1.0. June 2007
[10] US Army Unified Capabilities (UC) Reference Architecture (RA). Version 1.0. 11 October 2013.
[11] Department of Defense Assured Services (AS) Session Initiation Protocol (SIP). Errata-1, July 2013 http://www.defense.gov/news/newsarticle.aspx?id=122949/ Retrieved: Jun, 2019
[12] A. Corrin. "Leidos-Lockheed merger changes the face of federal IT". Federal Times. February 5, 2016. Web: https://www.federaltimes.com/it-networks/2016/02/05/leidos-lockheed-merger-changes-the-face-of-federal-it/ Retrieved: Jun, 2019
[13] S. Meloni. "The Future of the Joint Information Environment (JIE)", Sept 24, 2014. Web: http://blog.immixgroup.com/2014/09/24/the-futureof-the-joint-information-environment-jie/ Retrieved: Apr, 2019.
[14] Cyberscoop. Web: https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/ Retrieved: Jun, 2019
[15] L. C. Williams Is it time to rethink JRSS? Feb 01, 2019 https://defensesystems.com/articles/2019/02/01/jrss-pause-report-williams.aspx/ Retrieved: Jun, 2019
[16] L. C. Williams. "DOD cloud strategy puts JEDI at the center". Feb 05, 2019. Web: https://defensesystems.com/articles/2019/02/06/dod-cloud-strategy.aspx/ Retrieved: Jun, 2019.
[17] T. Keelan. "The Pentagon's JEDI cloud strategy is ambitious, but can it work?" March 21 2019. Web: https://www.c4isrnet.com/opinion/2019/03/21/the-pentagons-jedi-cloud-strategy-is-ambitious-but-can-it-work/ Retrieved: Jun, 2019.
[18] Department of Defense. DoD Cloud Strategy Readiness for Artificial Intelligence (Al). December 2018.
[19] U.S. Department of Defense. Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity, (February 12, 2019). Web: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf/ Retrieved: Jun, 2019
[20] Saurav Das, Guru Parulkar, and Nick McKeown. Rethinking IP core networks. Journal of Optical Communications and Networking, 5(12):1431–1442, 2013.
[21] Ping Yin, Steven Diamond, Bill Lin, Stephen Boyd. "Network Optimization for Unified Packet and Circuit Switched Networks". 22 May 2019. https://arxiv.org/abs/1808.00586/ Retrieved: Jun, 2019
[22] S. Pasricha, and N. Dutt, "On-Chip Communication Architectures," Elsevier, 2008.
[23] Kuei-chung Chang, Jih-sheng Shen and Tien-fu Chen, "Evaluation and design trade-offs between circuit-switched and packet-switched NoCs for application-specific SoCs," Proc. Design Autom. Conf., San Francisco, 2006, pp. 143--148.
[24] L. Shaoteng, A. Jantsch and Z. Lu, "Analysis and evaluation of circuit switched NoC and packet switched NoC," Proc. Euromicro Conf. on Digital System Design (DSD), 2013.
[25] Chen, G., Anders, M.A., Kaul, H., Satpathy, S.A., Mathew, S.K., Hsu, S.K., Agarwal, A., Krishnamurthy,R.K., Borkar, S., and De, V., A 340mV_to_0.9V 20.2Tb/s source_synchronous hybrid packet/circuit_switched 16 × 16 network_on_chip in 22 nm tri_gate CMOS, Proc. Solid_State Circuits Conf. Digest of Technical Papers (ISSCC), IEEE International, 2014.