http://dx.doi.org/10.15414/isd2016.s9.02

University network with security aspects and redundancy to ISP

Pavel Beňo
Trnava university in Trnava
Centre of information systems
Hornopotočná 23, 91843 Trnava
Trnava, Slovakia
Pavel.Beno@truni.sk

Abstract
In this paper, we want to show the use of modern technologies for communication among individual DTCs, especially for the communication model and the technique, based on the fiber optics. This new concept, so called Wavelength division multiplexing (WDM), uses multi wavelength approach for the communication on a single optical fiber. Further, we deal with the main causes of a possible communication breakdown among DTCs and to ISP and suggest corresponding solutions for their elimination. We consider the cloud consisting of the whole bulk of communication, among its all blocks, virtualized machines (VMs), data processing, their content, sharing and access planning to individual communication. At present the most spread model of the failure elimination is the artificial built in redundancy of active and passive component parts of the communication network.

Keywords: *availability, communication, datacenters, network, security*

JEL classification: *L86, D85, L63*

1. Modern datacenters and Cloud virtualized services

The last decade has seen the rise of the DTC computing in practically every application domain. The move to DTC has been powered by two separate trends. In parallel, functionality and data usually associated with personal computing has moved into the DTC; users continuously interact with remote sites while using local computers, whether to run intrinsically online applications such as email, chat, or to manipulate data traditionally stored locally, such as documents, spreadsheets, videos and photos. In effect, modern architectures are converging towards cloud computing, a paradigm where all user activity is funneled into large DTC via high-speed networks. Simply speaking, cloud computing is a set of computers, services or infrastructure. Delivering services is reducing every day work of users (clients), service providers, but also IT specialists. Cloud allows to offer more access services, reduces infrastructure delivery time from weeks to hours and reimbursement for really provided sources and services only [1].

Let us give some typical services provided in modern cloud computing DTC [2]:

- Infrastructure as a service (IaaS),
- Platform as a service (PaaS),
- Software as a service (SaaS),
- Storage as a service (STaaS) ,
- Security as a service (SECaaS),
- Data as a service (DaaS),
- Business process as a service (BPaaS),
- Test environment as a service (TEaaS),
- Desktop as a service (DaaS),

http://dx.doi.org/10.15414/isd2016.s9.02

- API as a service (APIaaS),

A critical implication of the DTC computing model is that the user of the online service expects the same performance of the application as that, running on the desktop computer, immediately responsive as a desktop application. User expects the service to store data reliably and always and immediately available. For service providers, delivering on this expectation, it is an engineering task of immense proportions. DTC are composed of thousands of failure-prone components and exhibit a bewildering array of failure models. Each level of the SW and HW stack has its own litany of error models, ranging from simple to byzantine – hung machines, blown fans, corrupted disks, bad network cards, overloaded routers and switches, bugs in SW, rogue malware, partitioned networks - this list is endless. When faults occur, enterprises have to react extremely quickly to prevent service down-time.

Existing reliable communication protocols are reactive, and have an associated cost and latency of reaction. In many cases, they react too slowly to the packet loss. And often, they over-react – flooding the system with recovery traffic that potentially causes further data loss, as well as throttling back excessively on sending speeds to avoid more loss. Protocols such as TCP/IP were designed for congested public networks and do not work well in the high-speed networks deployed within and between DTCs.

2. Trnava university network

Let us show first the general scheme of communication among individual DTCs on example of DTCs in Trnava University. Trnava University has three locally separated DTCs, connected via fiber optic connection. Network connectivity is designed on the Cisco technology with security from the same company and application firewall from Checkpoint company. Let us touch first the problem about general topology, connectivity and all special features of the communication system among DTCs.

2.1 Transmission lines aggregation (TRUNKING)

If we want to speak about the communication among individual DTCs, we must first show, how is network balanced. Cisco technology enables the setup of the network for excessive data transfer. Our project requires a good and stable network backbone, with the conservation of the required security level. One interesting part of the networking and communication setup is aggregation in form of trunking. The task of the aggregation of the transmission lines is to provide availability with divided communication network among more physical transmission lines. If one line exhibits failure, communication is continued on other lines. Aggregation is formulated in the standard IEEE 802.3ad [3], where there is described the compatibility of this solution with different network components from different producers as well.

In the aggregation (Figure 1) the logical MAC address is used that is assignment to more physical ports. This logical address is moved on the third layer, what is input Address Resolution Protocol (ARP). All ports who are in aggregation are in one interface Data Link Provider Interface (DLPI) ports of the router, which looks and behaves as one port and thus the Spanning Tree Protocol (STP) does not block it how a topology loop.

Aggregation must be supported on both sides of the communication channel what is ensured by the protocol Link Aggregation Control Protocol (LACP). Communication is started by the messages of the type “query”, where assigned for aggregation ports on both sides are. That is the way for creating a trunk with a sent message “start group”, where there are the identifying

http://dx.doi.org/10.15414/isd2016.s9.02

lines to ports. The collector compiles the communication from other ports and the distributor separates dataflow between ports in trunk or aggregation group.

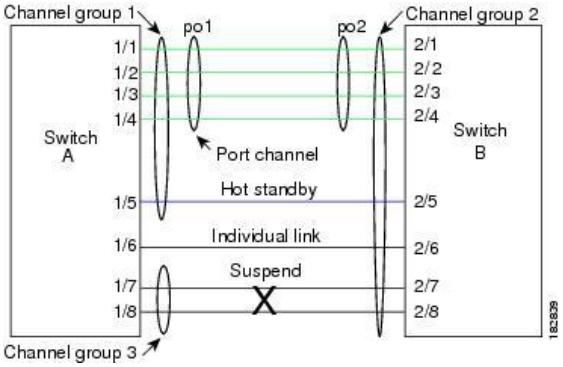

Figure 1 Scheme of transmission lines aggregation (TRUNKING) [4]

2.2 Data and WDM technology

Next part that we want to show for the support of the communication among individual DTCs is technology based on the multiplexing and demultiplexing transmition wavelength via fiber optic cable [5]. In fiber-optic communications, wavelength division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths of a laser radiation. This technique enables bidirectional communications over one strand of the fiber, as well as multiplication of its capacity. The WDM system uses a multiplexer at the transmitter side to combine the signals together and a demultiplexer at the receiver side to split them apart again. With the right type of fiber it is possible to have a device that does both simultaneously, and can function as an optical add-drop multiplexer.

2.2.1 Course WDM

Originally, the term "coarse wavelength division multiplexing" was fairly generic, and meant a number of different things. In general, these things shared the fact that the choice of channel spacings and frequency stability was such that erbium doped fiber amplifiers (EDFAs) could not be utilized. Prior to the relatively recent ITU standardization of the term, one common meaning for coarse WDM meant two (or possibly more) signals multiplexed onto a single fiber, where one signal was in the 1550 nm band, and the other in the 1310 nm band [6].

An interesting and relatively recent development relating coarse WDM is the creation of GBIC and small form factor pluggable (SFP) transceivers utilizing standardized CWDM wavelengths. GBIC and SFP optics allow for something very close to a seamless upgrade in even legacy systems that support SFP interfaces. Thus, a legacy switch system can be easily "converted" to allow wavelength multiplexed transport over a fiber simply by judicious choice of transceiver wavelengths, combined with an inexpensive passive optical multiplexing device.

2.2.2 Dense WDM

Dense wavelength division multiplexing (DWDM) [7] refers originally to optical signals multiplexed within the 1550 nm band so as to leverage the capabilities (and cost) of erbium doped fiber amplifiers (EDFAs), which are effective for wavelengths between approximately 1525–1565 nm (C band), or 1570–1610 nm (L band). EDFAs were originally developed to replace SONET/SDH optical-electrical-optical (OEO) regenerators, which they had made them practically obsolete. EDFAs can amplify any optical signal in their operating range, regardless of the bit rate. In terms of multi-wavelength signals, so long as the EDFA has

http://dx.doi.org/10.15414/isd2016.s9.02

enough pump energy available , it can amplify as many optical signals as can be multiplexed into its amplification band (though signal densities are limited by choice of modulation format). EDFAs therefore allow a single-channel optical link to be upgraded in bit rate by replacing only equipment at both ends of the link, while retaining the existing EDFA or series of EDFAs through a long haul route. Furthermore, single-wavelength links using EDFAs can similarly be upgraded to WDM links at reasonable cost. The EDFA's cost is thus leveraged across as many channels as can be multiplexed into the 1550 nm band.

2.2.3 Load DWDM at Trnava university

Let us show, how is Trnava university using DWDM technology (Figure 2). This communication is set up between two datacenters. The first is situated in Hornopotočná street (the rectorate of the university), the second is in Holleho street (Albertinum center). Among this two individual DTCs is DWDM connected via Small Factor Pluggable (SFP) installed in Cisco Catalist 4507. DWDM using four wavelengths. Two of them are used for the standard communication between DTCs, one is used for phone lines and last one is used for Storage area network (SAN) connection between DTCs. SAN connection is very important, because this allows a higher functionality in virtualization or cloud computing. This higher functionality is in the first place migration of the VMs between ESX servers and datastores in the DTCs.

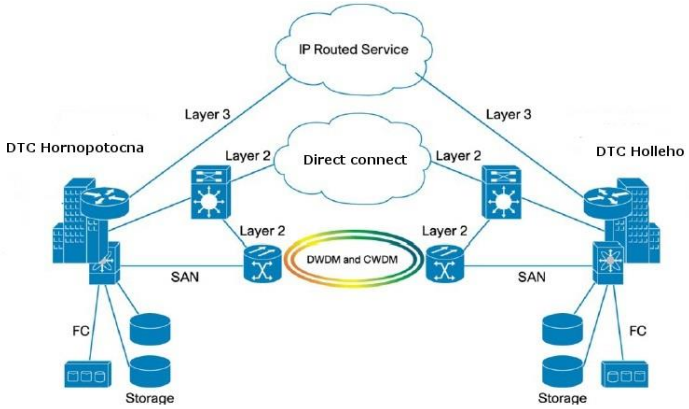

Figure 2 DWDM between DTCs in Trnava university

3 Security on the network

Firstly, it is proper to show schematically the main topology of the Trnava University network. We can start from Figure 3, where is the topology of the Trnava University network. University network is designed with respect to the organization structure of the university. Structure of the network consists of two main parts. The first part is the rectorate part, where is Internet service provider (ISP) connected, DMZ core switch in redundancy mode and firewalls – Cisco ASA and Checkpoint application firewall. The second part of the network is designed for faculties´ communication. Every faculty of the university is equipped with identical component parts designed to cooperate with the rectorate core switch, distribution and access switches in faculties buildings.

http://dx.doi.org/10.15414/isd2016.s9.02

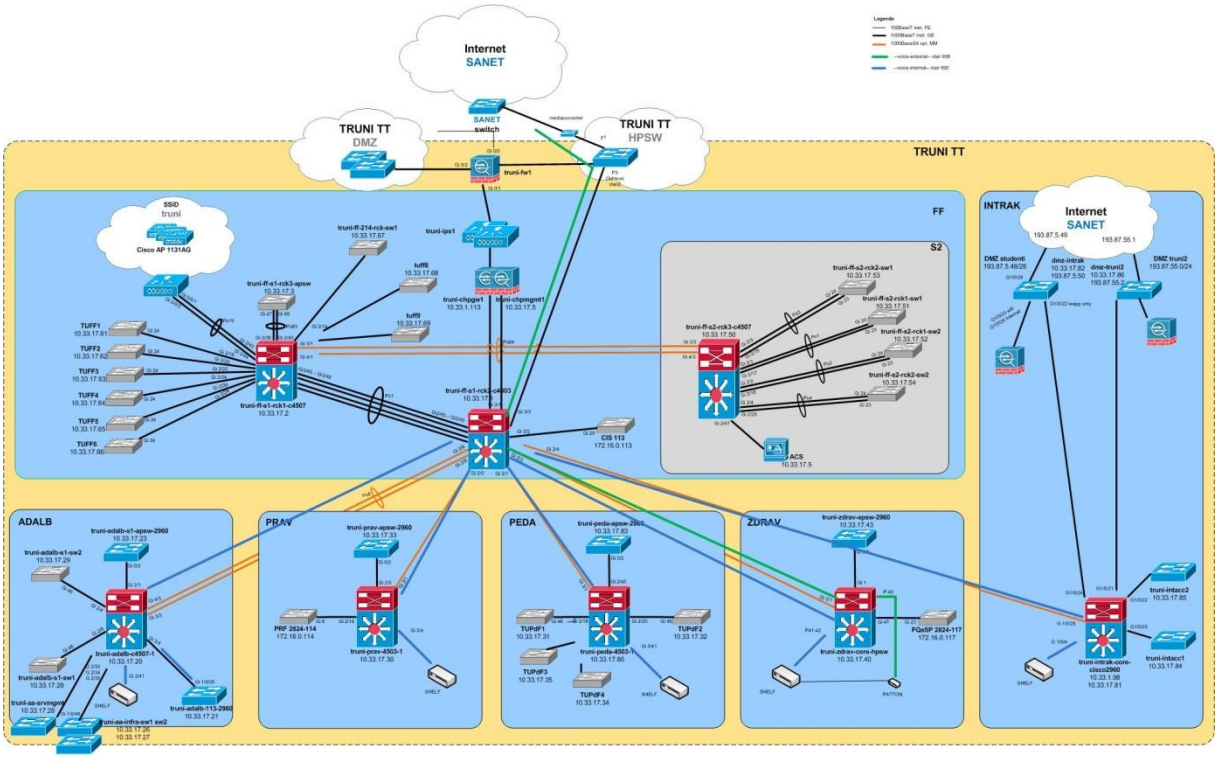

Figure 3 Topology of the Trnava University data communication network

The security of the university network is secured by four layers system. The first layer is the security provided by university's firewall. Cisco ASA is a good firewall choice, which enables to adjust the main security policy, for example blocking input/output communication with server or ports by the primary network antivirus – TrendMicro [8]. The second level, or second firewall rules is load of the application firewall. University using the Checkpoint firewall, for application control on the network. The third level of the security is the access list on the core switch, where route policy for all faculties and buildings is set. The third part of the security is Intrusion Detection System (IDS) [9] system for detecting problems and port security on the network. The last part is the security policy on the distribution switches, where is set the policy for every building and faculty. This is the network security element. On top of this, the university is protected with antivirus in all Windows servers and users end nodes. All networks are designed with VLAN modes for all faculties and primary applications. For example this VLAN is defined for every faculty:

- Sunray – for thin client,
- User – for all users and end nodes,
- Management – for management and monitoring on network,
- Phone – for telephone central,
- Wifi – for APs and clients in the building,
- Elab – for communication of the our experiments with servers in DTCs.

Approximately 90% of the university communication is in crypt mode. Every page, every communication between servers is protected for cybercrime. Connection to the network from outer word, from other providers is just in VPN mode authenticated to IDM system of the university.

http://dx.doi.org/10.15414/isd2016.s9.02

4 Redundancy of the connectivity to ISP

Very important part and goal of this work is redundant connectivity to ISP. Trnava university have a primary ISP, like every universities in Slovakia, SANET – Slovak academic network. Old way to Internet is oriented to MTF STU. This line is secured with Cisco ASA firewall on L2, L3 and with Checkpoint firewall on L7.

Next way to Internet is from new building Students hostel on Rybnikova Street. Security from this line is built with Cisco ASA firewall on L2 and L3 layer. Using L3 rules it is possible to manage and route all communication from redundancy to each line.

Primary line is routed on the IP network 193.87.54.0/24 and secondary line is routed on 193.87.55.0/24. Each line is active for primary IP address range and stand-by for the other. This is easy way to rerouting all of communication to one line to ISP.

5 Conclusion

In this contribution we tried to show the communication among DTCs of the Trnava University with all the progressive parts, including virtualized. Our three DTCs are geographically distributed in Trnava town, connected via Fiber optic (FO) . All transmission lines is design to transfer at minimum 1Gbps on one wavelengths λ=1310 or 1550 nm. Between DTCs Hornopotočná a Hollého is used DWDM connection for the separate communication. Under separate communication we mean the connection where different wavelengths for different communication are used. This approach enabled for the connection of the SAN (storage array network) between a both DTCs that is substantial contribution for virtualization, bringing migration among servers or datastores in both DTCs, resulting in many assets, the savings in the first place.

And what is really benefit from this work? Separated line to ISP is very important, because demands on the network connectivity and availability of the organizations are still increased. Lost connectivity for few days can have liquidation proceedings. Every organization, not just university with students and research, must have plan for business continuity and disaster recovery. Without these plans, organizations are still in vulnerable.

The paper was published with the financial support of the EUNIS Slovakia.

References

[1] K. T. Beno P., “Cloud computing. This is it!,” in *Cloud computing workshop 2011*, Bratislava, 2011.

[2] B. Pavel, “PhD thesis,” in *Thesis*, Zlin, FAI TBU, 2016.

[3] Frazier H., Doorn SV., Hays R., Muller S., Tolley B., Kolesar P., Thompson G., Turner B., “IEEE 802.3ad Link Aggregation (LAG),” in *what is it, and what is not*, Ottawa, 2007.

[4] C. corp., “Portchannel,” Cisco, [Online]. Available: http://cisco.sitecelerate.com/en/US/docs/switches/datacenter/sw/6_x/nxos/interfaces/configuration/guide/if_portchannel.html. [Accessed 10 10 2015].

[5] F. Optic, “Wavelenght-division multiplexing,” Fiber Optic, [Online]. Available: http://www.fiberoptic.com/adt_cwdm.htm. [Accessed 2 3 2016].

[6] [Online]. Available: http://cdn.ttgtmedia.com/ITKE/uploads/blogs.dir/58/files/2009/01/etherchannel7.jpg. [Accessed 10 3 2015].

[7] R. Margaret, “dense wavelength division multiplexing,” in *CIO Trends*, TechTarget, 2007.

[8] T. Micro, "Trend Micro," Trend Micro (UK) Limited, [Online]. Available: http://www.trendmicro.co.uk. [Accessed 10 1 2016].

[9] SANS, "IDFAQ: What is Intrusion Detection?," SANS, [Online]. Available: https://www.sans.org/security-resources/idfaq/wah-is-intrusion-detection/1/1. [Accessed 2 2 2016].

* Online full-text paper availability: doi:http://dx.doi.org/10.15414/isd2016.s9.02